2020全球网络趋势报告

目录

序言: 数字时代的网络状况 4

IT网络日益重要 7

催生网络需求的全球趋势 9

- 全球化 9
- 数字业务的转型 9
- 业务自动化 10
- 业务和运营弹性 10
- 可持续性 10

推动网络发展的技术趋势 11

- 不断发展的应用程序领域 11
- 物联网 (IoT) 12
- 人工智能 (AI) 13
- 移动性 13
- 安全性 14
- 沉浸式体验 14

对新型网络的需求 16

- 思科专家对新兴网络架构的展望 17
- 网络架构的状态 19

网络技术的趋势 20

大规模网络自动化 23

- 软件定义网络: 刚刚开始 25
- 基于意图的网络: 关闭回路 25
- 网络功能虚拟化 27
- 作为网络基础的可编程性 27

网络技术的趋势 (续)

开放平台IBN控制器: IT流程及业务整合 28

从客户到工作负载的跨域策略和保障到位 29

AI驱动保障 30

何为AI、ML和MR? 31

网络复杂性推动了AI的应用 32

如何将ML和MR用于网络情境? 34

AI在网络保障中的当前及未来状况 34

未来AI考虑 36

多云环境下的数据和应用程序网络 37

改变应用程序模型的网络影响 39

优化用户与多云的连接 41

用于"无处不在"数据中心的网络 45

构建多云网络时的考虑 48

网络接入与无线 49

为移动用户提供愉快的体验 51

让IT为无线的成功做好准备 53

网络接入就绪度的当前和未来状况 53

实现数字时代接入和无线技术的考虑 55

不断改变的网络安全角色 56

网络安全挑战 59

用智能网络应对安全挑战 61

网络安全的当前和未来状况 64

网络运营趋势 65

网络运营的当前和未来状况 69

网络进步如何改变网络运营 69

网络运营集成至IT流程中 69

完全符合IT和业务意图 71

实现自动化以减少网络运营复杂性 72

预防性与被动反应问题及事故管理 72

为网络运营带来连接性 73

引入下一代网络运营框架 73

生命周期管理 74

策略管理 75

保障管理 76

网络运营的未来——展望2025 77

网络人才趋势 78

为正在改变的网络技能做好准备 82

信息技术领域最为缺乏的技能 82

最为缺乏的网络技能 83

日益增长的业务和软件技能需求 84

跨领域职位在未来越来越重要 84

网络策略师的新职责 85

未来的策略师: 提供超越网络的价值 85

网络从业者的新职责 87

未来的网络工程师: 提供超越连接性的价值 87

IT领导者: 采取措施弥补网络人才的缺乏 88

对IT领导者如何构建未来网络团队的建议 90

序言: 数字时代的网络状况

章节摘要

要点

- 全球化、数字化转型、业务自动化和弹性，以及可持续性等趋势正在塑造着对于新型网络的需求。
- 不断发展的技术领域——新兴的云原生模型、物联网、人工智能（AI）、手机、网络安全威胁，及沉浸式应用程序——都对IT网络的架构和运营带来了显著的影响。
- 这些需求的规模、复杂性和动态性几近超出人类操作者的应对能力。
- 新型网络正通过人工智能（AI）、机器学习及自动化等新兴技术简化和保障运营，实现快速适应性，并提高人类的决策能力。

催生新型网络的全球业务和技术趋势

7亿	50%	146亿	42%	53%	12倍
到2021年的边缘托管容器数量[1]	到2021年，企业数据中心之外的工作负载占比[2]	到2022年，物联网（IoT）设备数量[3]	2017至2022年，业务移动流量每年增加量[3]	导致超过50万美元损失的网络安全攻击占比[4]	到2022年，增强现实（AR）/虚拟现实（VR）使用量增长[3]

章节摘要 (续)

重要指南

- IT领导者和网络策略师应基于自动化和AI技术逐步将每个网络域发展为基于控制器的模型。
- IT领导者应构建匹配业务优先级并贯穿架构、技术、运营及人才的业务和技术计划。
- 网络策略师和网络从业者应确定可为他们带来领导此次网络转型并提升自身价值所需技能的职业和学习路径。

高层前瞻

“到2025年，领先的网络团队将跨域（园区、分支机构、WAN、数据中心、云、服务提供商和安全等）运行基于意图的网络。他们的网络将能够理解业务和应用的需求，并将这些需求转化为网络和安全策略。藉由网络的智能自动化，其灵活性会得到显著提高，网络将以强大的反馈环运行，提供持续的监控、保障和优化。基于意图的网络将确保不间断提供业务服务并进行保护。这些进步将为企业乃至整个社会带来巨大益处。”

——思科企业网络首席技术官 (CTO)
John Apostolopoulos

序言: 数字时代的网络状况

美国国防高级研究计划局 (Defense Advanced Research Projects Agency) 局长J.C.R. Licklider在其1962年写下的一系列备忘录中提出了“星际计算机网络” (Intergalactic Computer Network) 的构想，即将全球的计算机相互连接在一起，让人们从任何地方都能快速访问数据和程序。[5]

就在几年后的1965年，Leonard Kleinrock与Lawrence Roberts和Thomas Merrill用电话线将四台计算机连在一起，组成了第一个实际意义上的广域网，互联网由此诞生。[6]

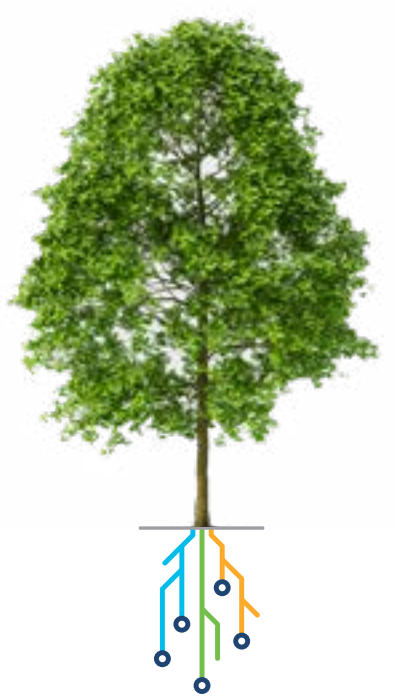
此后50多年，互联网一如Licklider当初的设想，不断地将全球客户的信息和服务连接到应用程序和数据资源。

但除此之外，一切均已改变。

IT网络日益重要

当今世界在技术性能迅猛增长的推动下，变得日益互联、数字化、广分布而多样化。几乎每个“事物”都具备数据处理能力，计算机模型的分布性和网络化更加显著。按照梅特卡夫定律 (Metcalfe’s law)，随着设备和用户的加入，网络的价值和重要性将不断以几何级数增加。

数字业务继续推动网络创新。据IDC估计，到2023年，全球联网设备将达489亿台，[7] 且*《2018年思科可视化网络指数完整预测》*预计，网络中每台个人计算机每月的平均数据用量会接近60GB。[3]

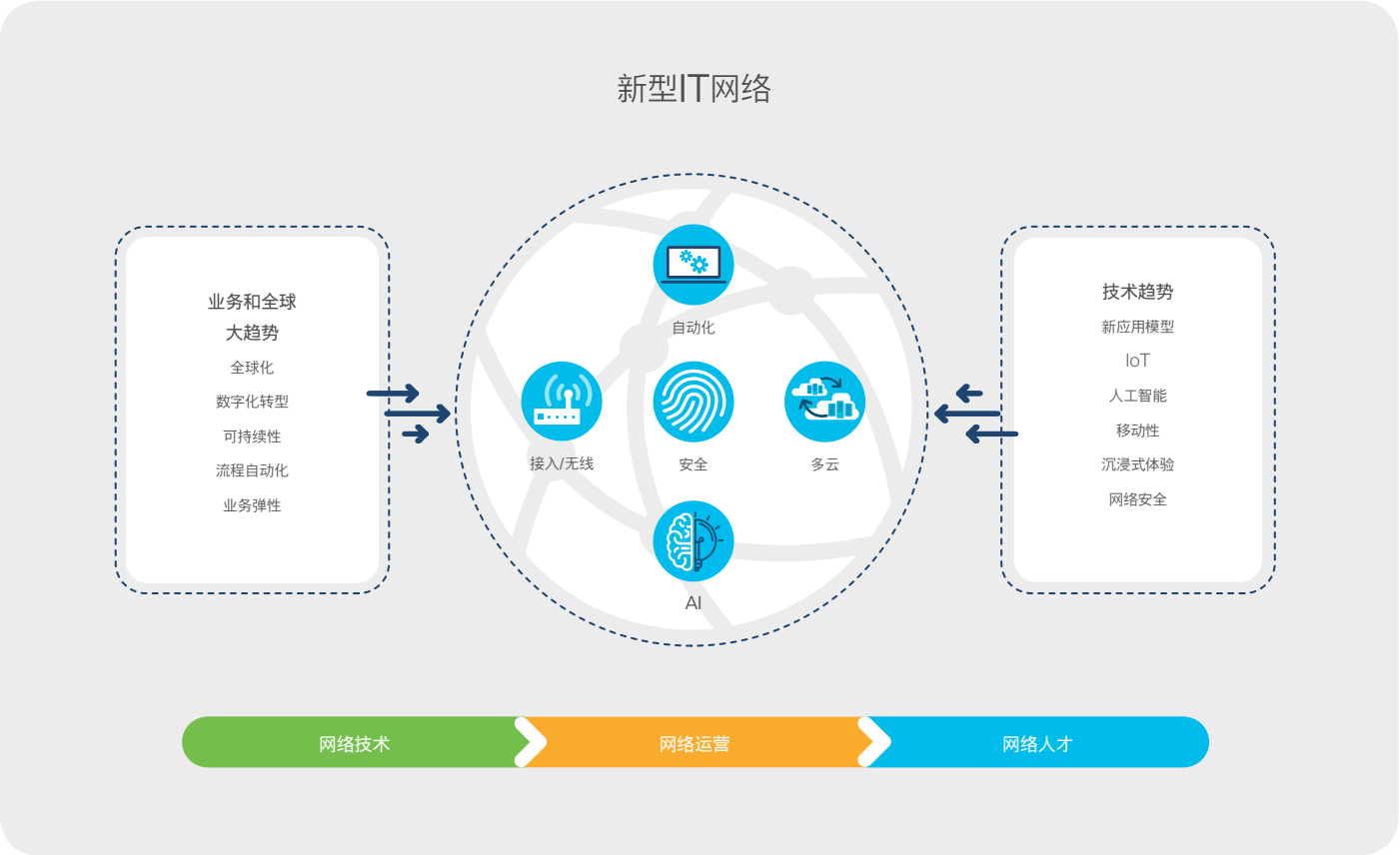


如果照此持续增长，可以想见，网络的庞大规模和复杂性将超出IT团队有效管理网络并确保其安全的能力。目前，我们所需的是能够将机器学习、机器推理和自动化等技术结合在一起的新系统，以简化运营，提高人类的决策能力。

当前，我们正处于迈入网络新时代的关口。IT将打破网络构建和运行的传统方式，拥抱未来技术，以全新方式解决这些挑战。

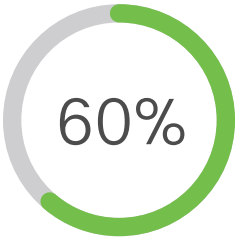
在审视构成这种新型网络基础的新兴网络技术、运营和人才趋势之前，让我们先简要了解一下推动这种发展的全球业务和技术趋势。

图1　催生新型网络的全球业务和技术趋势



催生网络需求的全球趋势

许多全球业务趋势正在塑造着网络在组织中所扮演的角色。了解这些趋势可帮助IT领导者更好地做好准备，满足业务领导者对网络日益升高的期望。



据Gartner公司统计，到2023年，60%以上的企业会将网络视为其数字化策略的核心，而当前仅有不到20%的企业将其视为“策略推手”。[8]

简单地了解一下这些全球大趋势，便会发现它们可能会对网络提出的要求。

全球化

按照世界经济论坛 (World Economic Forum) 的说法，目前我们正进入一个被称为“全球化4.0”的以数字驱动的全球化新时代。在这个时代，通过数字功能和人工智能实现的数字产品和服务成为主要输出品。[9]

网络影响力

随着系统、人员、流程、位置和设备间的连接性变得愈加分布和复杂，网络对企业的经济价值将增加，保护和管理网络将变得更为重要和困难。

数字业务的转型

越来越多的企业正在使用分析、移动、云解决方案和物联网等数字技术作为其业务转型的基础。据IMD和*思科数字漩涡2019*报告，88%的高管认为，数字化颠覆将对其行业产生重大或变革性影响，而在2015年，持此观点的人仅为27%。[10]

网络影响力

业务固有的不可预测性要求网络能够快速适应不断变化的需求，实现新的业务、流程和模式。

业务自动化

未来，随着企业寻求提高质量、劳动力生产率、客户满意度等，自动化和机器人的使用将继续激增。据Capgemini研究院预计，到2022年，自动化技术的大规模采用会使汽车、零售、公共事业和制造业节省高达4710亿美元的成本。[11]

网络影响力

因为流程自动化的核心旨在时间敏感性和任务关键性，所以网络需要确保按时可靠地交付数据包。

业务和运营弹性

由于全球化和数字化转型，当今的企业依赖于日趋复杂的技术、系统、流程、供应链和基础设施网络。有效的业务弹性需要持续不断且积极主动地评估运营风险、制定和审核应急预案，并进行事件响应培训。

网络影响力

灵活、安全、有弹性的网络架构对保护员工、客户和合作伙伴，及恢复数据并快速重建服务与访问至关重要。

可持续性

当今世界的互联性日益紧密，企业在环保可持续性方面的发展正面临挑战。除标准指标外，企业需要接受在减少温室气体排放、保护生物多样性和自然资源，以及最大程度地降低产品设计上的浪费和废物回收利用方面的审查。

网络影响力

先进的网络在几乎所有业务环节，从能源消耗到资源利用和减排等，均可提供更具效率的前景。

推动网络发展的技术趋势

目前，许多新兴趋势正明显改变着IT领域。仔细研究其中一些关键趋势，会发现它们可能对企业网络产生的影响。

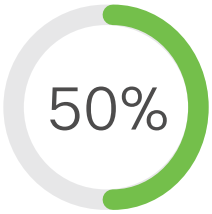
不断发展的应用程序领域

应用程序和数据无疑是数字业务的核心。为满足新的业务需求，研发、托管和使用应用程序的方式时刻在变。

以下为应用程序发展演变及在某些方面重塑网络的一些方式：

应用程序和数据正迁离本地：应用程序和数据正被模块化为微服务，并移至多个公共云。在某些情况下，它们也被分发到网络边界，且被多个软件即服务（SaaS）提供商越来越多地使用。

应用程序是模块化的，并跨多个环境分布：在很多情况下，整体式应用程序正在分解为相互连接的微服务，并通过跨整个企业的一系列虚拟和物理工作负载（包括容器）交付。



据Uptime Institute估计，到2021年，所有工作负载的一半会在企业数据中心之外的云和数据中心基础设施内或网络边缘运行。[2]

应用程序得到持续高速构建：对于在内部开发和托管的应用程序，IT必需加速自身基础设施服务的创建和交付，以满足应用程序和用户的需求，同时控制运营成本。

应用程序正从物理向虚拟，再向容器和无服务器迁移：容器的兴起将应用程序的设计和部署模式置于更颠覆性的技术，即无服务器架构，该架构正迫使企业重新审视构建应用程序的方式、基础设施的作用，以及运营流程的设计。

据估计，到2021年，已安装和正在使用的容器将超过35亿，其中20%以上运行在分布式位置，服务于边缘和物联网工作负载。[1]

网络影响力

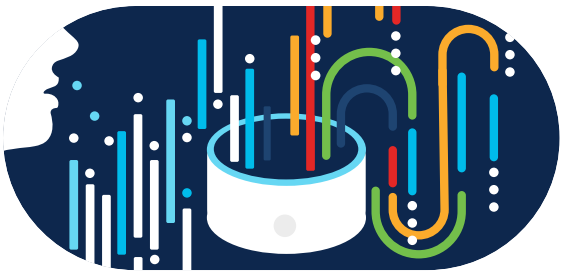
随着应用程序和微服务在所有领域如雨后春笋般涌现，更应将网络视为一组正在生长的互连“神经簇”，它们位于数据所在的位置，并可出现在边缘云统一体的任何位置。新型网络需能够稳固地连接在这些互连的“神经簇”之内和之间，并对这些新应用模型的工作方式有基本的了解，同时将整个网络的应用程序政策动态地扩展到托管应用程序的任何地方。

物联网

物联网设备、应用程序及相关数据的爆炸式使用正推动新型分布式计算机模型的建立，这些模型的规模和复杂性都呈指数级增长。据思科“VNI Forecast Highlights Tool”，到2022年，机对机 (M2M) 设备将占全球所有联网设备的51% (146亿)。[12]

网络影响力

除为极其多样的物联网设备提供连通性和安全性外，网络管理员还需要找到可扩展的高效方式，自动识别、分类和应用策略，并对它们进行监控，确保功能正常，不会影响或损害在网络上运行的其他设备。

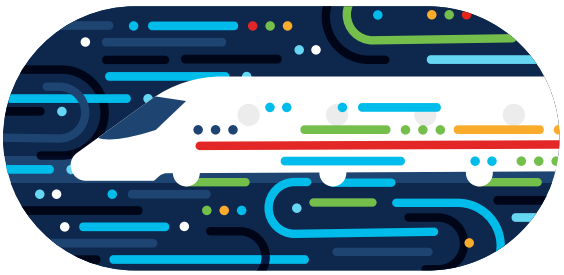


AI

以AI驱动的应用程序（无论面向业务还是消费者）的出现正引领人们迈入一个互联、智能和自动化设备无处不在的全新世界。

网络影响力

要释放AI在业务中的全部潜力，需要在更靠近边缘的地方完成更多的计算处理和决策。AI处理和数据的布置包括云到内部数据中心，再到网络边缘，取决于其性能、容量、隐私性，甚至成本考虑。

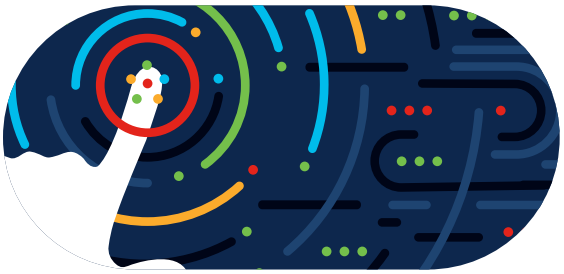


移动性

据思科"VNI Forecast Highlights Tool"，从2017年到2022年，全球业务移动数据流量将增长六倍，年增长率为42%。[12] 业务移动用户仍期待通过Wi-Fi及公共4G和5G网络在任何地点、任何时间和任何设备上实现即时高性能连接。同时，无线物联网设备会越来越普遍地出现在我们生活的各个方面。

网络影响力

使用公司和个人设备访问云应用程序的员工如果离开网络，会导致缺乏可见性和控制力，这是网络和安全管理员未曾面临的情况。物联网设备的涌现在规模、不同的流量模式和安全性方面增加了对无线网络的要求。



安全

网络安全威胁变得日益复杂和危险，受攻击面更为广泛，且不再包含在明确并受保护的边界内。尤其是随着工作负载的向外迁移，IT有失去可见性的危险。

网络影响力

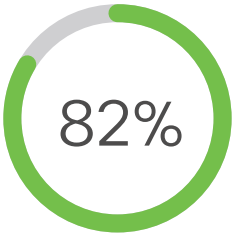
尽管在识别和遏制威胁方面网络仍是强大的同盟，但网络和安全运营需要分享数据、集成工具和工作流，以最佳方式抗击数量及复杂性不断增加的攻击。另外，网络能将IT的触及范围扩展到云环境中，以帮助保护应用程序和数据——即便不在这些环境的直接控制之下。

沉浸式体验

为提升合作、培训、生产效率和远程工作体验，视频的使用日渐增加，虚拟现实 (VR) 和增强现实 (AR) 技术也随之兴起，这些都对企业的网络提出更高的要求。

网络影响力

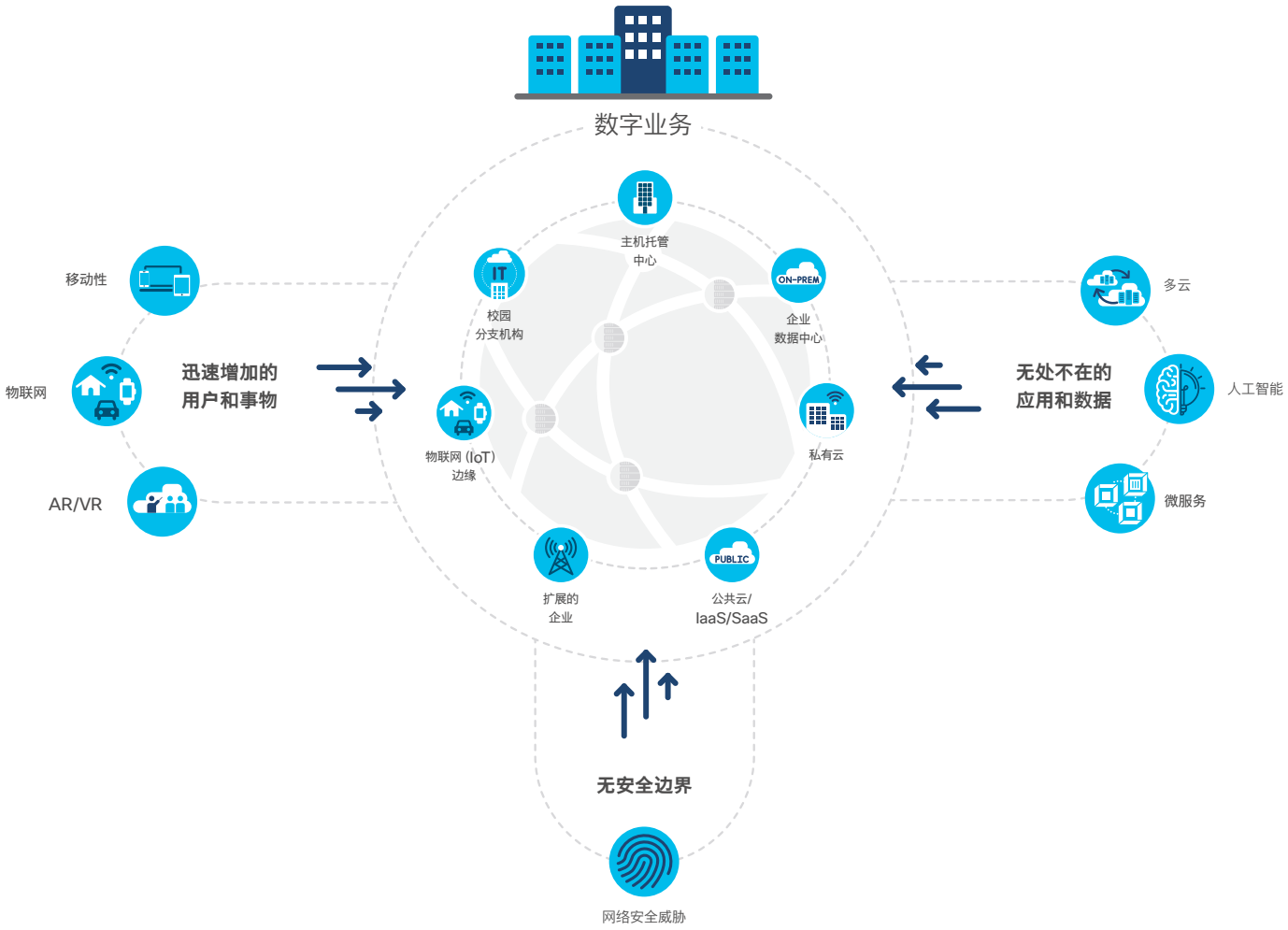
网络需要提供实现上述沉浸式体验所需的端到端宽带和低延时通信及动态性能控制。



到2022年，互联网视频将占互联网全部业务流量的82%，VR/AR流量将增长12倍，互联网视频监视流量将增长7倍。[13]

这一动态技术前景不仅是摆在所有企业及其客户面前的现实，而且也是数字经济的引擎。毫无疑问，IT行业需要开拓正确的网络技术策略、运营模式和人才来应对所有这些趋势，这让人感到压力。

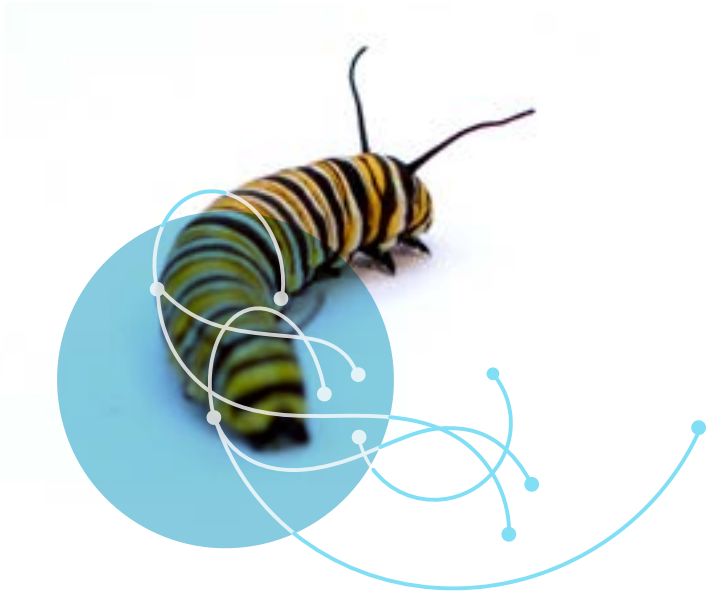
图2 驱动新型网络需求的技术



对新型网络的需求

在这个要求日益严苛的环境中，IT领导者们迫切需要迁移到一种全新的网络途径。

要使企业在数字经济中蓬勃发展，网络需要能够快速适应不断变化的业务要求。网络需要支持日益多样和快速变化的用户、设备、应用程序及服务，且需要安全无缝地承载这些多样化的设备，提供理想的用户和应用体验。



此外，网络还需确保对工作负载的快速安全访问，以及工作负载之间的访问，无论这些负载在哪里。为使网络发挥最佳功能，所有这些需跨每个网络域——园区、分支机构、远程家居、WAN、服务提供商、手机、数据中心、混合云以及多云等——在用户、设备、应用程序和服务间端到端实现。

这意味着组织需要为每个网络域提供新的集成架构。该架构是可以定制的，以满足相应网络域的特定需求，并提供跨所有域进行通信和强制执行一致策略的方法。

图3 新型网络的四个基本目标

满足业务需求	简化复杂性	确保性能	降低风险
• 启动新的数字业务计划 • 动态满足快速变化的应用需求	• 简化IT运营，应对日益增长的需求 • 让IT能够集中资源创造业务价值	• 始终满足服务性能和用户体验要求 • 防止网络中断	• 在网络威胁造成损害前加以预防和遏制 • 满足合规和法规要求

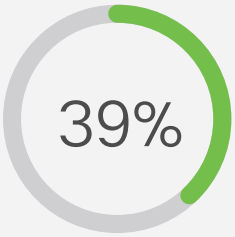
思科专家对新兴网络架构的展望

当今大多数网络并未做好满足新兴数字时代要求的准备。在我们的*《2019全球网络趋势调查》*中，我们发现，39%的IT领导者认为他们的网络能够很好地满足数字业务的需求，但只有19%的网络战略家持同样的观点。[14]

不过，仍有理由对此保持乐观。思科企业网络首席技术官（CTO）John Apostolopoulos预计，当今大部分僵化的、人工运行的基础设施经过相对较短的过度就能转变为更灵活的、以软件驱动的架构，后者可"不断进行适应，从而满足组织所依赖的应用程序和服务不断变化的需求。"

> "这种网络将作为一个系统运行，其自主水平会越来越高，并会考虑自己的状态、所有用户和应用程序的动态，同时还会考虑大量的可能选项。"
>
> – 思科企业网络工程高级副总裁Ravi Chandrasekaran

这种新兴网络架构是什么样的呢？思科企业网络工程高级副总裁Ravi Chandrasekaran表示，"这种网络将作为一个系统运行，其自主水平会越来越高，并会考虑自己的状态、所有用户和应用程序的动态，同时还会考虑大量的可能选项。"



我们发现，39%的IT领导者认为他们的网络能够很好地满足数字业务的需求，但只有19%的网络战略家持同样的观点。[14]

实现这种更为自主状态的关键是AI。无论是自动更改交通路线、请求更多带宽，还是要求改变策略，甚至拒绝新的服务请求，AI都会帮助IT团队对不断变化的网络状况做出快速响应。

假以时日，通过利用全系统的智能和自动化，这种网络会变得对用户完全透明，并以需要的层级随时随地为用户所需服务提供安全连接。

虽然Apostolopoulos承认，在网络具备实现这一前景的智能和力量前，还有很长的路要走，但他相信，将实现人工智能

的服务保障、基于控制器的自动化、自然语言处理和网络安全方面的重大改进汇集在一起所需要的技术进步正在顺利推进。

新型网络用例

到2025年，领先的企业网络将能够处理来自任何行业的、以自然语言表达的要求，并自动将其转化为一套政策和自动行动，确保网络持续满足业务需求，且所有这些均对任何其他现有服务无影响。具备这些能力的网络通常被称为基于意图的网络。

以下是基于意图的网络的一个假定用例。

简要介绍：一家企业想使用无线IoT光学传感器为一项通过AR应用程序交付的新业务创新提供支持。以下为业务需求和意图如何被转化成网络行动的过程。

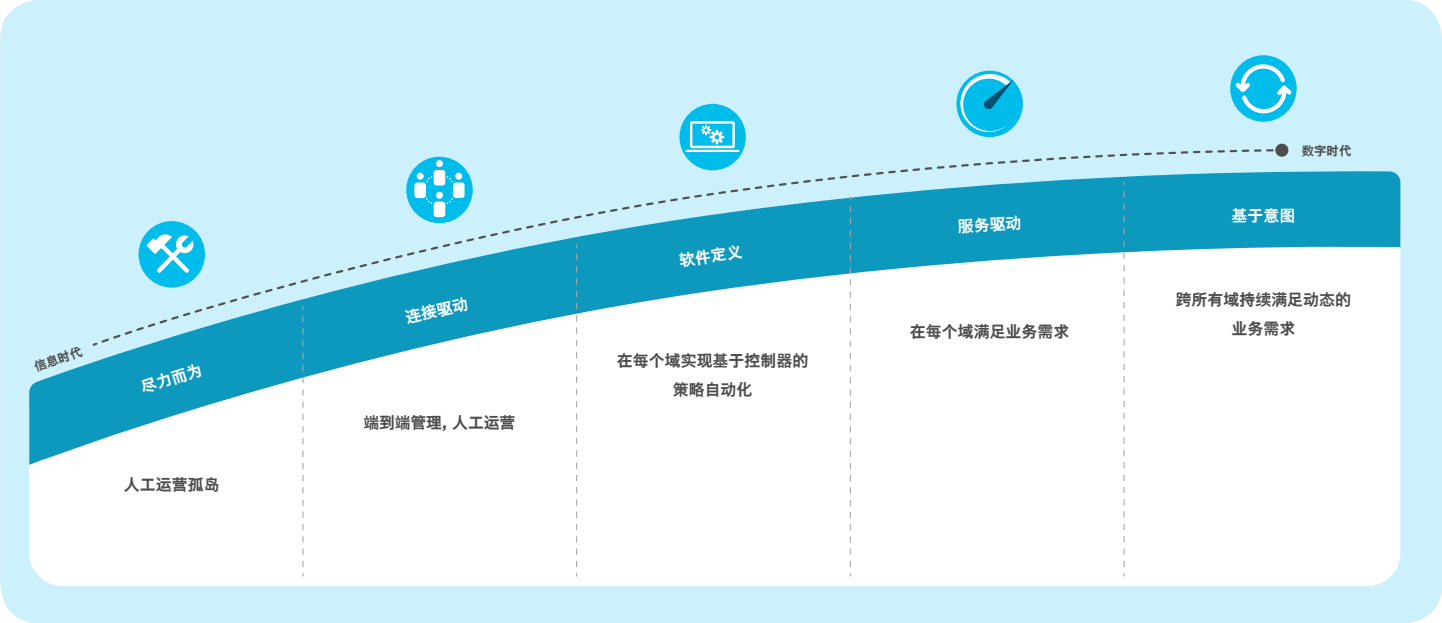
图4　新型网络用例

网络架构的状态

在迈向更先进的网络、以满足数字时代的需求的过程中，企业如今处于什么位置？思科数字网络就绪模型提供了标准的五级成熟度模型，帮助IT企业评估他们当前的网络就绪水平并助其制定未来发展的定位。

该模型可用于多个网络就绪类别，如架构、接入、WAN、保障、网络安全等。

图5　思科数字网络就绪模型



2020全球网络趋势报告

网络技术的趋势

催生新型网络的五大技术

目前，网络技术的许多重大进展正汇集融合成新型网络模式的基础。尤其是**自动化、AI、多云网络、无线**和**网络安全**这五个技术领域的进步会在数十年内兴起最大的网络转型浪潮。这些技术将支持市场对扩大规模、提高灵活性和安全性的需求，并促使正在改变我们世界的新兴趋势得以实现。

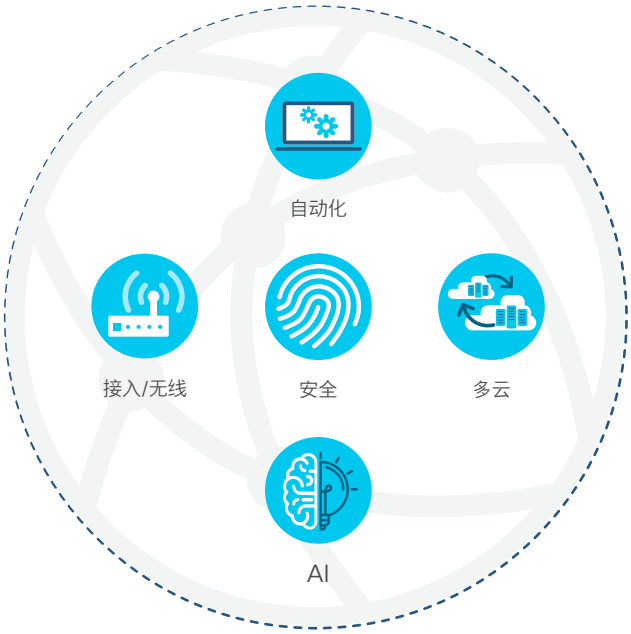
技术领域

- 自动化
- AI
- 多云网络
- 无线
- 网络安全

“全球企业都意识到进行数字转型的必要性，以跟上市场的发展，并满足员工、合作伙伴、客户及成员的要求。IT领导者也意识到，没有更为健全、安全和灵活的网络，他们企业的数字转型将面临风险，并将引发其网络多方面的同步重构。”—— IDC企业网络高级研究分析师Brandon Butler

仔细研究这些技术领域的状况，可深入了解它们重塑网络的方式、它们当前的应用情况，以及我们在不远的将来能够期待的变化。

图6 推动网络转型的五大技术



大规模网络自动化

章节摘要

要点

- 软件定义网络 (SDN)、基于意图的网络 (IBN)、网络虚拟化、可编程性和开放平台网络控制器正在共同促进网络服务自动适应业务需求和IT流程的实现。
- IBN提高了SDN的自动化能力，使其能够将意图转化为策略、收集数据、提供可见性、纠正问题，并确保策略按意图如实执行。
- IBN的目标是在整个网络中不断应用并保证服务性能要求、安全性及合规策略，以及IT运营流程。
- 开放平台控制器上的应用程序编程接口 (API) 允许控制器与相邻的网络及IT服务、其他IT域、业务应用和异构基础架构集成并交换智能。

关键调查结果

- IT领导者认为，网络自动化 (25%)、SDN (23%) 和IBN (16%) 是今后五年对网络影响最大的技术。
- 27%的IT领导者将接入、WAN、数据中心 (DC)、云和安全域孤立的设计和运营方式视为他们适应先进网络技术的障碍。
- 34%的IT领导者认为，与其他IT团队更好地进行网络协作和整合是改进的一个重要领域。
- 尽管当前仅4%的IT领导者和网络策略师认为他们的网络是基于意图的网络，但有35%计划在两年内将他们的网络改为基于意图的网络。

章节摘要 (续)

重要指南

- IT领导者应该评估他们的网络是否准备就绪以业务需要的速度提供网络服务。
- 探索制定路线图，在各网络域以每个步骤均为企业带来最佳ROI的增量步骤执行闭环且基于意图的网络策略。
- 确定与开放平台网络控制器集成后受益最大的IT流程和业务应用程序，并优先考虑它们。

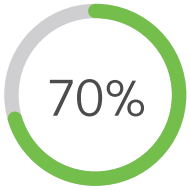
高层前瞻

“到2025年，执行端到端、基于意图的策略这一长期愿景将开始成为现实。网络团队将能够大规模跨域（接入、WAN、DC、多云、IoT）自动执行动态分段和服务优化策略——从客户端到应用程序，以及分布式工作负载之间。”

– 思科企业网络客户体验副总裁Ronnie Ray

大规模网络自动化

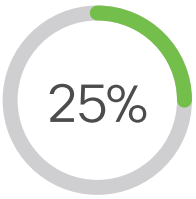
网络自动化就是使网络中物理和虚拟设备的配置、管理、测试、部署和运营实现自动化的过程。为创建持续的服务增强，甚至网络自动化本身也可自动化。



据Gartner统计，“近70%的数据中心网络任务由人工完成，这不仅增加了用时、成本、出错几率，而且降低了灵活性。”[15]

自动化可提高网络可用性，并将网络运营（NetOps）团队从耗时的日常任务中解脱出来，难怪当被问及未来五年哪些技术会对网络影响最大时，25%的IT领导者认为是网络自动化。[14]

如今，在SDN、基于意图的网络（IBN）、虚拟化、可编程性和开放平台控制器领域的创新正使网络自动化成为现实。



25%的IT领导者认为未来五年对网络影响最大的是自动化。[14]

软件定义网络: 刚刚开始

过去几年，SDN在实现全网自动化方面取得了长足进步。它可让网络团队将网络作为端到端系统进行管理，并将控制平面和转发平面加以分离而使管理更为高效和灵活。

因此，控制面可直接编程。它将底层设备和基础设施从应用程序和网络服务中提取出来。通过可编程SDN控制器，网络智能被逻辑中心化。

最初引入SDN的目的是简化复杂的数据中心环境，这些环境需要支持可移植动态工作负载迁移和服务器到服务器的通信。软件定义访问 (SD-Access) 和软件定义广域网 (SD-WAN) 都遵循同样的原则，前者有助于更有效地保护用户和设备的访问，后者可使用户在访问应用程序和云服务时得到更好的体验。

基于意图的网络: 关闭回路

网络团队的首要目标是为业务持续提供应用程序、服务性能和保护。因此，尽管SDN在自动化方面提供了重要的进步，但那只是解决方案的一部分。此外，企业还需要持续的网络监控和优化，以支持日益动态并以数字驱动的业务模式。

为实现这一点，网络必须了解不断变化的业务意图，并对动态的网络状况进行监控，这样才能不断顺应意图。据互联网工程任务组 (IETF) 的草案，“意图构成了全网范围的声明性策略。人类操作员定义的是预期，而网络计算出可满足要求的解决方案。”[16]

基于意图的网络是相对较新的网络模式，最早于2017年进入市场，现已被网络行业广泛采用。

使用时，系统还需不断核实是否符合意图，若不符合意图，应提供纠正指南。Gartner认为，“基于策略的配置将过渡到基于意图的网络(IBN)解决方案，并使用自动化进行自我监控，确保网络实际上满足在配置时设置的策略意图。”[15]

图7 IBN: 以SDN为基础构建

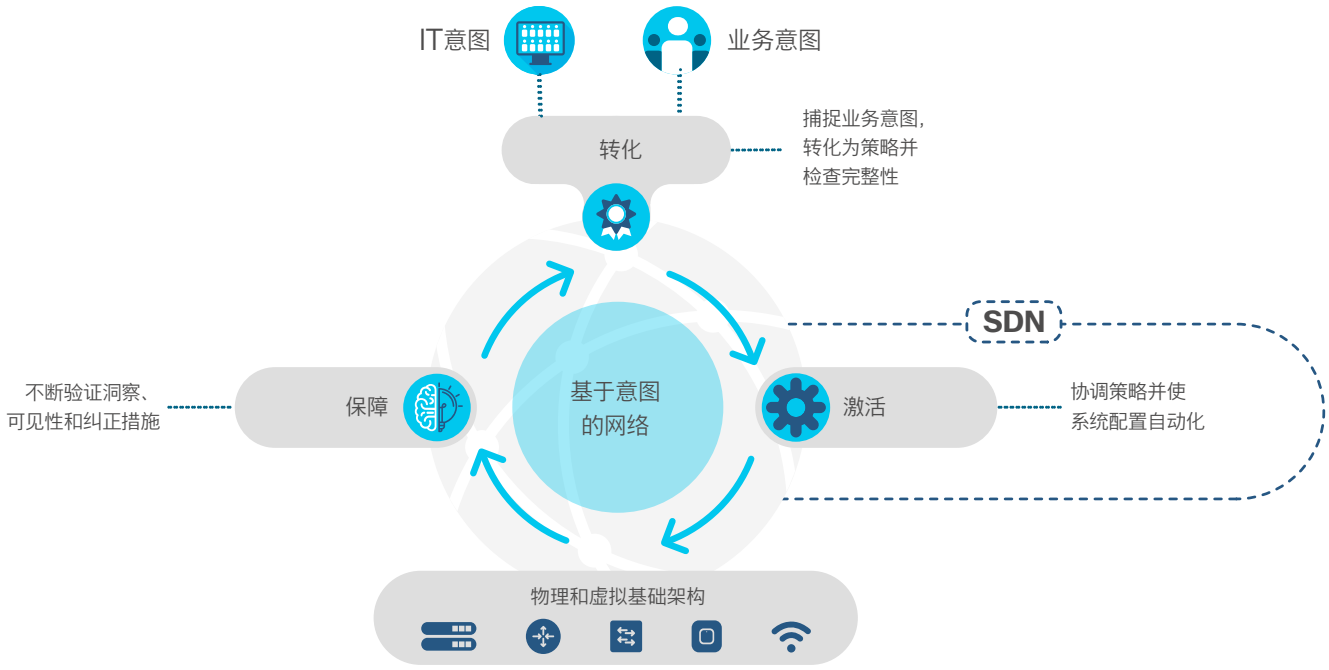
在我们的*《2019全球网络趋势调查》*中，我们发现，26%的网络策略师将在一个或多个领域部署基于意图的网络作为实现理想网络的技术优先项。尽管当前仅4.3%的受访者认为他们的网络是基于意图的网络，但有35%的人计划在两年内将他们的网络改为基于意图的网络。[14]

John Apostolopoulos解释说，IBN控制器对SDN进行了扩展，以提供更完整的系统，从而不断调整网络以实现所需的业务意图。它提升了SDN的自动化能力，使其能够将意图转化为策略、收集数据、提供可见性和相关见解，并确保网络按意图执行。IBN提供的闭环反馈是实现预期效益的基础。[17]

基于意图的网络可捕获业务的意图，并使用分析、机器学习、机器推理和自动化使网络持续动态地适应不断变化的业务需求，同时适应不断变化的网络负载和其他环境影响。这可能意味着要在整个网络中不断应用并保障服务性能要求及用户、安全、合规性和IT运营策略。

基于意图的网络是如何工作的呢？思科定义的IBN包含三个功能性构建模块: 转化、激活和保障。[18]

图8 基于意图的网络的构成



在与云服务的合作与竞争中，IT领导者不得不更快速、更有效地提供服务。从技术角度看，IBN所需的计算、处理能力和AI专业知识正变得越来越容易获得。

IDC的Rohit Mehra表示，“基于意图的网络是网络行业的重大进展。它不仅包含高级可见性、自动化和保障，而且是构建基于机器学习的新网络管理功能的平台。”[19]

网络功能虚拟化

从根本上改变计算服务的虚拟化模型已经以网络功能虚拟化（NFV）的形式应用于网络。它使NetOps能够快速交付或改变网络服务，并对其进行远程部署和管理。除了IT灵活性之外，NFV还可提供大量的物理整合，从而节省空间和能源，并减少潜在的故障点。

作为网络基础的可编程性

对于IBN控制器和系统而言，若想可扩展并发挥全部潜力，需要构建可编程的物理或虚拟网络基础设施。可编程设备和接口及专用集成电路（ASIC）形成了智能网络的根本基础。

为采用更高效的自动化系统，IT团队要继续抛弃传统的基于命令行接口 (CLI) 的人工管理方式，而以数据模型驱动接口 (DMI) 取而代之。这些标准的基于模型的接口提供一致性、开放性、结构和效率。

IETF标准模型 (像YANG) 提供了一套完整的北向编程接口，打造易于使用、性能一致的可持续运营模型。

开放平台IBN控制器: IT流程及业务整合

该控制器上的应用程序编程接口 (API) 可使控制器将相邻网络及IT服务、其他IT域、业务应用程序和异构基础设施整合在一起并与之交换智能。

这将网络转变为开放的平台，该平台可接受来自应用程序和设备的策略规范，利用集中的跨域策略自动化，并确认系统是否满足业务需要。通过简化跨网络域工作流程、IT系统，以及用于独立管理的行业流程，改善了IT服务交付。

在我们的《*2019全球网络趋势调查*》中，34%的IT领导者认为，与其他IT团队更好地进行网络协作和整合是改进的一个重要领域。[14]

图9 用于整合业务应用程序、IT服务和网络域的开放平台控制器

借助API和软件开发工具包 (SDK) 的网络可扩展性，IT人员能够更好地满足业务及IT应用程序的需求、简化运营，并确保投资保护。

从客户到工作负载的跨域策略和保障到位

网络团队需要共同努力，使网络在端到端层面上正确执行业务意图。这意味着从客户或“物”与网络连接之处到服务或应用程序托管之处，无论在哪里，都可建立无缝链接。

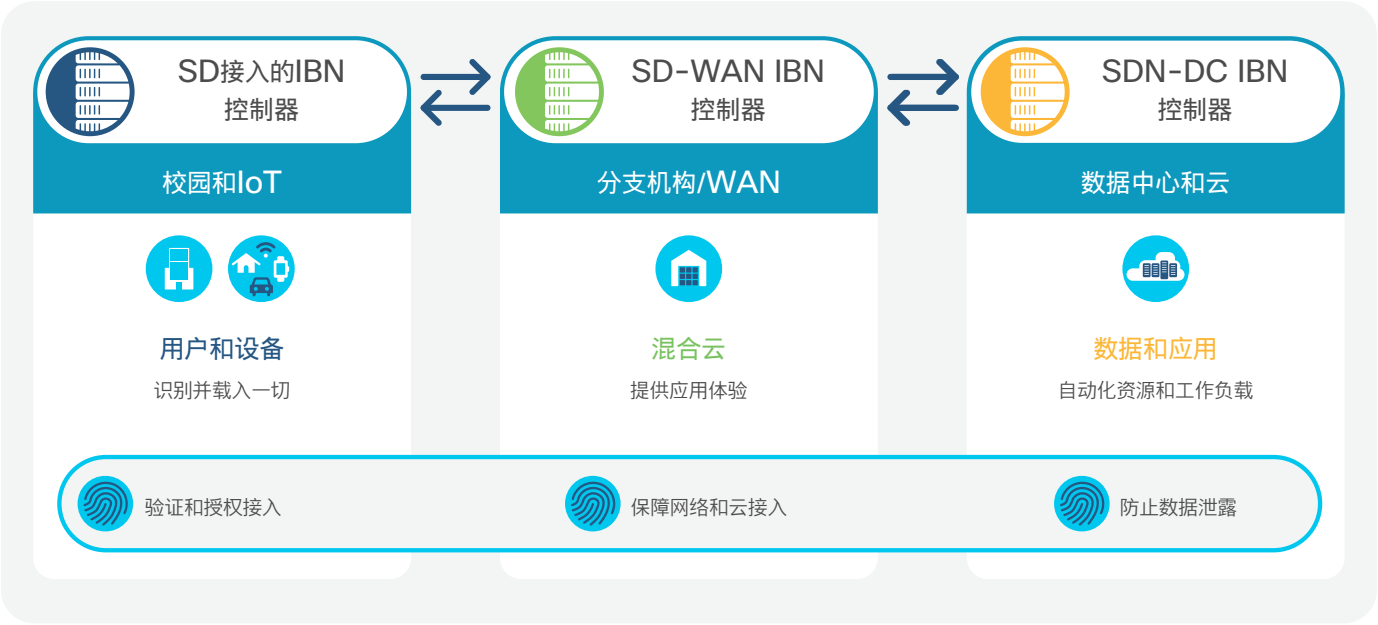
现状分析: 要使企业成功地实施基于意图的网络，它需要在数据中心、园区、广域网和分支机构中完全实现自动化。[20]

然而，在很多情况下，这并不容易实现。在我们的*《2019全球网络趋势调查》*中，27%的IT领导者将接入、WAN、DC、云和安全域孤立的设计和运营方式视为他们适应先进网络技术的障碍。[14]

在通常情况下，有充分的理由将网络分成各个域，而这些域通常围绕域的主要目标组织起来。然而，要实现业务意图的真正的端到端可见性、控制和验证，需要跨域协调策略和保障功能。

IT领导者正采取措施，力图实现这一点。26%的IT领导者将“集成的多域网络策略的实施和保障”作为增加投资的首要事项。[14]

图10 策略和保障: 所有IBN域的对齐



AI驱动保障

章节摘要

要点

- 人工智能 (AI) 的使用对运营、服务交付和网络保障日趋重要。将AI能力与运营结合在一起的AIOps (智能运营) 正日渐完善。
- 流量、连接的移动和IoT设备、互联的应用程序和微服务，以及日益增加的安全威胁都呈爆炸性增长，这些让网络团队不堪重负。
- 由网络支持的数量激增的设备和服务所产生的海量数据、遥测和事件超出了人类操作员应对的能力。
- AI是基于意图的网络(IBN)模型的基础，它使用大量的网络源数据探索环境的复杂性，并动态地提出网络调整的建议。
- 机器学习和机器推理相互补充，应对复杂的事件处理，提供关联洞察和指导性补救。

关键调查结果

- 超过50%的网络策略师将AI视为网络投资优先项。
- 仅17%的网络策略师认为AI技术的不成熟阻碍了网络现代化。
- 目前，仅22%的网络团队将AI用于网络保障，这可能是因为真正的AI驱动的工具的可用性仍为新概念所致。
- 72%的网络策略师计划在今后两年内采用AI驱动的预测性洞察或规范性补救。

重要指南

- 利用基于云的AI学习: 在某些情况下，企业数据策略的变化需要利用云驱动的AI工具带来的益处。
- 人和AI联锁: 渐进式定义AI在决策或采取行动方面走多远后需要人类操作员介入监控、批准或更改。
- AI知识: 网络专业知识将成为确认AI是否按意图实现IT和业务目标所必需的重要技能。

章节摘要 (续)

高层前瞻

“到2025年，AI驱动的网络保障工具将使若干定义明确的特定任务很好地完全实现自动化。然而，大多数要求更灵活和更情境化决策的运营任务仍需要人类操作员的专业知识和介入。”

– 思科研究员JP Vasseur

AI驱动保障

目前，AI正驱动各行各业的强力转型，对IT运营十分重要，AIOps (智能运营) 正日渐完善。

何为AI、ML和MR？

简而言之，AI是一个研究领域，在执行任务时，它能赋予计算机如人类般的智能。机器学习 (ML) 和机器推理 (MR) 是AI最重要的两个门类。机器学习可描述为无需显式编程便可从数据中进行“统计学习”的能力，而机器推理则是使用已获得的知识浏览一系列可能的选项，直至找到最佳结果。

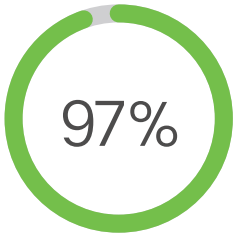
因此，ML能使系统审查数据并推断知识。它不再只是简单地学习或提取知识，而是随着时间的推移和经验的积累来利用和改进知识。从本质上说，ML的目标是识别和利用那些隐藏在“训练”数据中的模式。

MR很适于解决需要深厚专业知识的问题。为让推理机能够对新数据进行操作，人类需事先明确获取所有知识。MR是对ML的完美补充，这是因为它能根据ML得出的结论分析可能的原因和潜在的改进选择。

网络复杂性推动了AI的应用

有很多因素推动着AI驱动的网络的发展。由于网络复杂性和规模的空前增加，AI在帮助IT团队交付水平一致的网络和服务方面越来越必要。

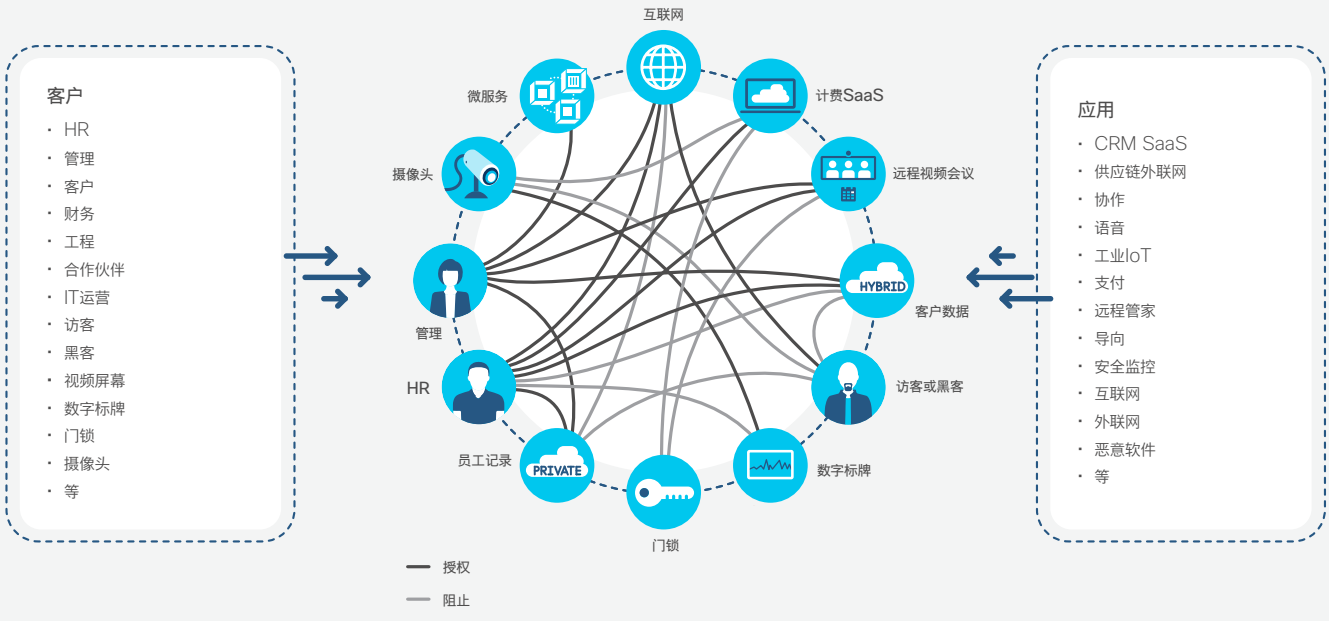
网络正支撑着流量、连接的移动和IoT设备、及互联的应用程序和微服务的爆炸性增长。同时，当今网络所产生的海量数据超出了只由人类操作员管理的能力，更不用说理解了。



网络故障造成的损失

在被调查的全球IT领导者中，有97%的人说，他们在过去6个月遇到过与关键业务应用程序相关的性能问题。每次网络故障的平均损失有多少呢？美国是402,542美元，英国是212,254美元。[21]

图11　超连接企业的网络复杂性



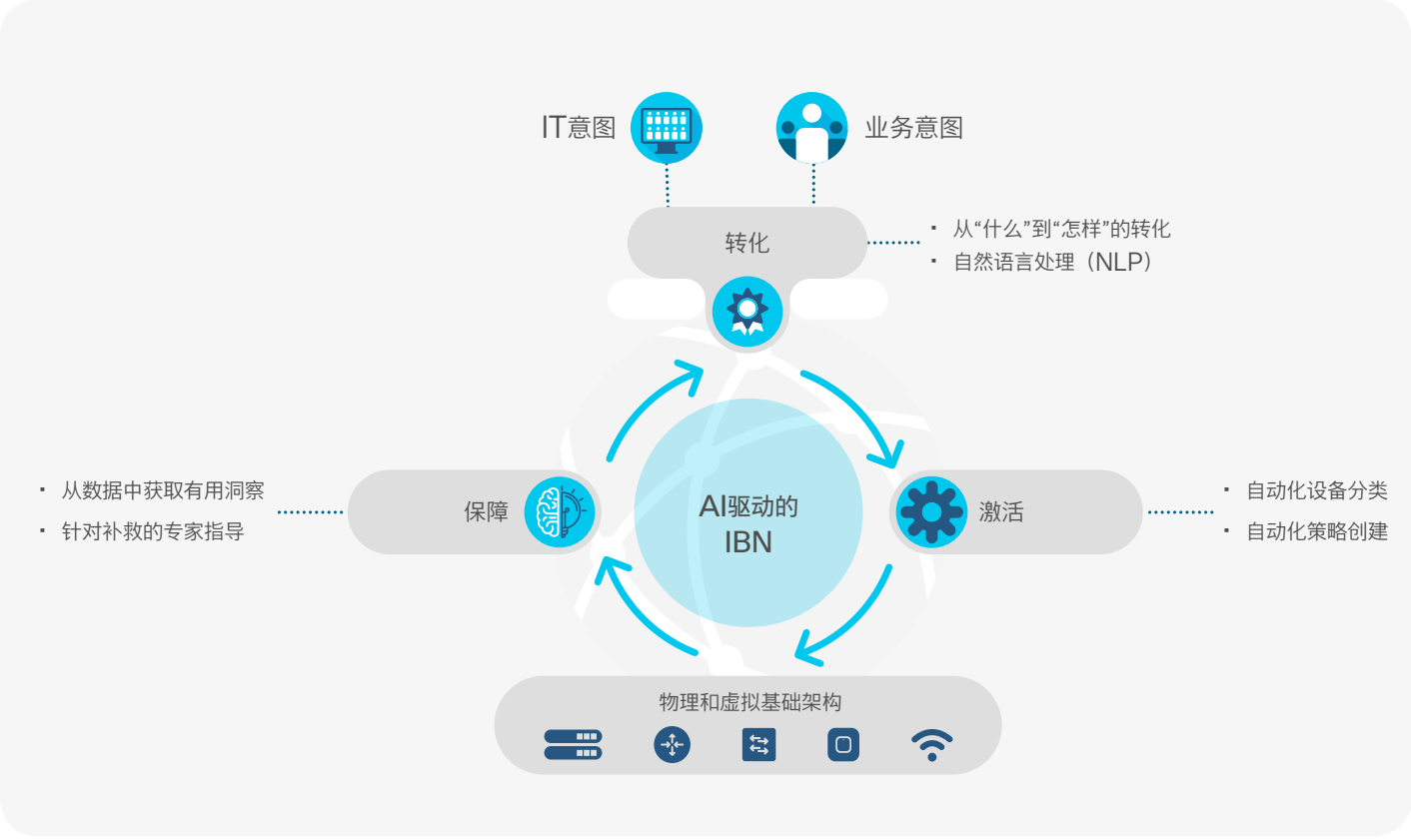
AI为网络团队更好地使用此数据提供了可能性，以确保他们的网络有效运行且持续满足业务需求。例如，它有助于建立更好的基准、准确地预测问题，并帮助对复杂系统排查故障。

网络策略师已认识到这一点。超过50%的策略师将AI看作打造理想网络所需的投资优先项，[14]而只有17%的策略师认为AI技术的不成熟阻碍了网络现代化。[14]

通过使用大量的网络源数据，AI可了解通信和网络环境的复杂性，并能动态地提出对网络的调整。这种能力使AI成为了IBN模型的基础。

AI及IBN这样的先进网络技术显然正在颠覆着事情执行的方式，对网络运营尤其如此。对新的应用程序的测试可分分钟完成，无需数周。保障引擎会找出问题的根本原因，并给出解决建议，这使网络问题排查变得容易不少。实际上，如果给未来的网络操作员配备上提供可执行洞察的强大面板，则其可能只需查看几个地方，而无需对众多可能的故障原因一一排查。

图12 由AI驱动的基于意图的网络



如何将ML和MR用于网络情境？

如上所述，网络运营和基于意图的网络的一个重要组成部分就是网络保障，它不断确认网络状态和行为是否与预期意图一致。机器学习和机器推理提供独特的功能，操作员可使用这些功能确保所需的网络性能，尤其在以下三个主要保障领域（见下图13）：

复杂事件处理：将ML用于网络遥测时，可建立对某个给定意图构成正常运营条件的动态基准。

关联洞察：ML可提供对网络运营更深刻的洞察和可见性，甚至能帮助预测未来何时可能出现异常情况。通过应用从排查类似问题的工作流程中获得的预加载专业知识，MR提升了ML的能力。

补救：通过使用由MR等提供的知识库找出最恰当的纠正措施，可使补救始终符合意图。[22]

AI在网络保障中的当前及未来状况

我们*《2019全球网络趋势调查》*的数据反映了企业采用AI驱动网络保障方面的进展。

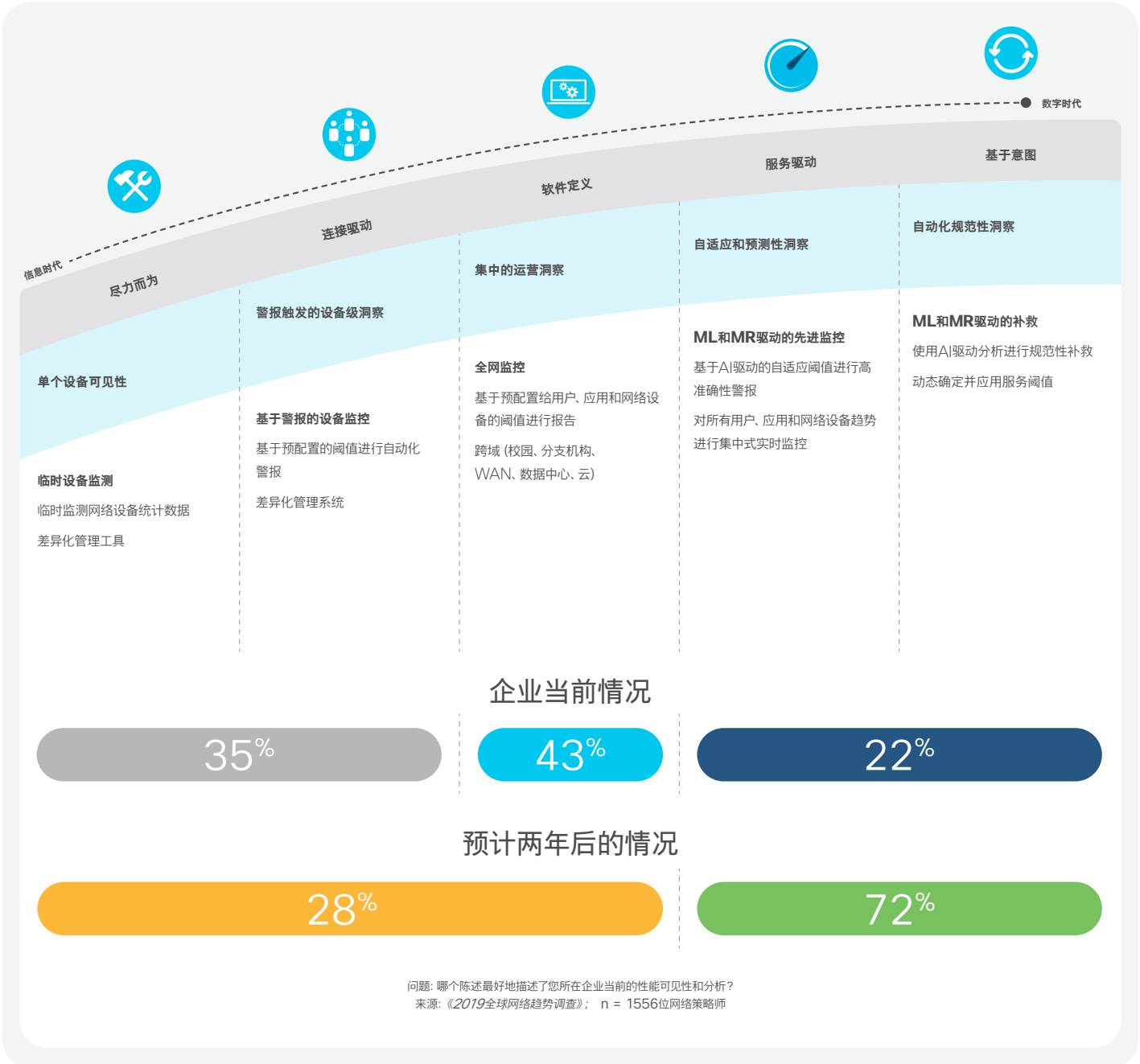
使用我们标准的五级就绪度模型衡量就绪度估计状态时，当前仅22%的受访网络策略师报告对网络保障使用了AI功能。

图13 ML和MR的网络保障用例

	机器学习	机器推理
技术途径	源于大数据集的数学模型	掌握人类知识、符号逻辑
适用性	预测性分析、异常检测、分类、回归	机器化可决策流程
网络保障功能	• 动态基线和问题识别 • 洞察和可见性 • 预测性分析	• 自动排查问题 • 自动补救

这可能是因为真正的基于AI的网络保障解决方案相对而言仍是新鲜事物所致。然而，72%的受访者计划在今后两年内使用AI驱动的预测性洞察或规范性补救。[14]

图14 AI驱动的保障就绪度



问题: 哪个陈述最好地描述了您所在企业当前的性能可见性和分析？
来源:《2019全球网络趋势调查》； n = 1556位网络策略师

未来AI考虑

思科研究员JP Vasseur认为，评估AI在网络基础设施中的使用时，需考虑以下方面:

1. **创建最佳运营实践:** 知道AI**不能**做什么和**不应做**什么与知道它**能**做什么一样重要。在确定哪个业务领域可从AI获益最大时，也一定要明辨那些会带来最高风险和危害的领域。

2. **定义明确的目标函数:** 如果ML团队没有清楚地指出目标，就没有算法可从数据集中提取出令人感兴趣的东西。在使用AI前，能够明确提出目标和性能指标至关重要。

3. **人和AI联锁:** 定义AI在决策或采取行动方面走多远后需要人类操作员介入监控、批准或更改，对于业务和网络团队保持控制能力十分重要。

4. **AI知识:** 对AI的日益依赖有可能造成知识缺口，因此，网络专业知识将成为如下操作所需的重要技能: 确认AI是否按意图实现IT和业务目标、帮助工作人员从AI系统推荐的选项中做出正确的选择。

5. **数据依赖:** 更好地收集数据。AI依靠数学计算创建可执行的建议，而这些计算取决于它们所使用数据的质量。网络专家需要跨职能和领域工作，确保AI项目的数据质量可信。

6. **在哪里使用AI:** 在哪里使用AI取决于应用程序和数据的性能、安全性、数据容量和隐私性。尽管有一些内部模型训练的应用实例，但目前最常见的应用是基于云的机器学习。云提供计算和存储能力，从多个源的大量聚合匿名数据中学习和执行ML。在某些情况下，这可能会引起隐私方面的担忧，比如谁有权访问这些数据，甚至这些数据存储在哪个地理位置。此外，还要注意延迟的影响，这可能会影响对大型数据集的实时洞察，例如，对于产生大量数据的视频传感器，可能会发生这种情况。

7. **改变公司范式:** 调整公司的数据策略，充分利用基于云的AI。通过将数百万个系统捆绑到一个AI分析引擎，可获得理想的数据样本量，相较于由源于单一网络体验的数据支持的相同技术，其可提供好得多的结果。IT团队是今天播种的关键，这将带来云友好的策略，从而支持AI部署。

多云环境下的数据和应用程序网络

章节摘要

要点

- 所有公司都需要基于云的服务，但始终有必要将一些数据和工作负载保留在内部。
- 在很多情况下，整体式应用程序正分解为相互连接的微服务，并通过位于容器内、企业内部、云中和企业网络边缘的一系列虚拟和物理工作负载交付。
- 分布式数据中心与传统数据中心的运行方式不同，因此IT企业需适应并满足这种新型架构增加的应用程序和网络连接需求。
- SD-WAN、云直接访问、主机托管设施、云交换，以及更经济的高带宽宽带和5G服务，正逐渐成为重要的新构架元素，以确保云服务可按业务要求有效而实惠地交付。

关键调查结果

- SDN/NFV已在企业数据中心内传输了23%的流量，到2021年，有望增加到44%。
- 29%的IT领导者和网络策略师认为，两年内他们将在企业内部、混合云和多云环境中部署基于意图的网络能力。
- 对云的日益依赖驱动WAN流量上升，到2022年，全球商用IP WAN流量预计将增长2倍，达到每月5.3艾字节。
- 全球超过58%的企业已经以某种形式部署了SD-WAN，且超过94%的受访者相信，他们会在未来两年内部署基本或更高级的基于意图的SD-WAN。

重要指南

- 确定最关键的基于云的应用程序和服务，并优先考虑任何SD-WAN计划，以首先访问并保护这些应用程序。
- 跨混合云和多云扩展一致的、基于策略的自动化，仔细考虑跨任何位置和任何工作负载的任何平台、任何管理程序或任何容器框架（云原生、裸机、管理程序、容器和无服务器）。

章节摘要 (续)

- 将应用程序服务、工作负载和服务组件映射到“扩展的”网络，以对网络上有何应用程序、服务和微服务有更好的了解。
- 数据中心、云和网络团队应协作开发跨园区、分支机构、数据中心、边缘/IoT和公共云/SaaS提供商域的服务一致性。
- 应用程序和服务需要在企业内部和云工作负载之间进行持续集成和交付，执行运营流程以互连和支持此模型的企业将获得云所承诺的速度和灵活性。

高层前瞻

“到2025年，我预计会有20%的工作负载分布在企业和多云数据环境之外的网络边缘。这意味着，通常限于数据中心的五分之一的流量现在需要在企业和多云网络得到保障和保护。”

– 思科云平台和解决方案小组副总裁兼首席技术官 (CTO) Vijoy Pandey

多云环境下的数据和应用程序网络

人们对速度与创新的需求正推动着IT企业对现有应用程序进行现代化，并快速开发能随时访问任何设备上的信息的新应用程序。当前的应用程序开发者和业务用户欣赏云的灵活性、可扩展性和自服务性。

然而，尽管85%的IT企业正在评估或已经使用公共云，但向云端转移并不能完全解决问题。[23]实际上，“向云端转移”这种说法并未证明是完全准确的。思科云平台和解决方案小组副总裁兼CTO Vijoy Pandey认为，“在过去几年，虽然有价值的工作负载试图迁移到公共云，但有一些工作负载，特别是一些数据，需要留在本地，因此这显然不是二元情形。”[24]

在当前使用公共云的企业中，有85%正寻求多云策略，这一比例将在12个月内增加至94%。[25]

同时，Pandey也指出，将数据保持在内部的决定源于许多问题，包括规章和数据保护：“另一个问题是，如果你需要从数据中得到众多洞察，就要做很多数据处理工作。对所有这些工作负载来说，你需要本地计算和本地网络。尽管所有公司都对基于云的服务有需求，但对内部服务的需求绝不会消失。这就是为何我笃定多云和混合云是未来发展方向的原因。”

改变应用程序模型的网络影响

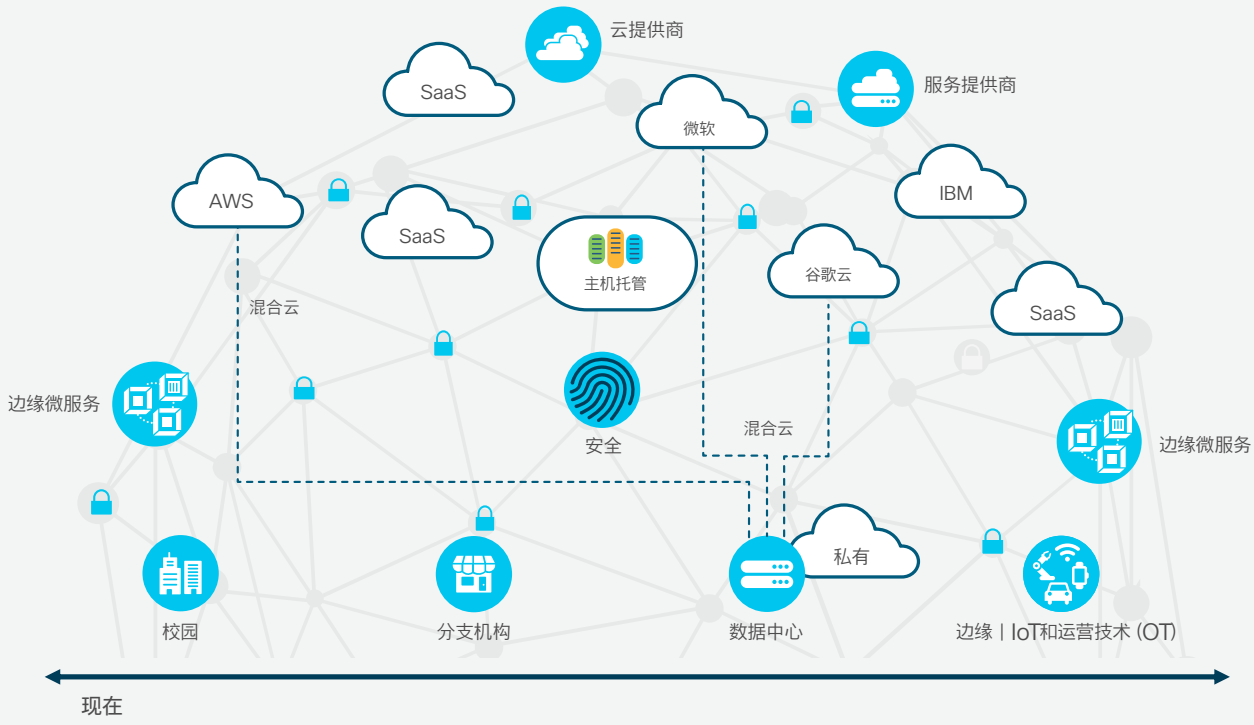
网络性能一般集中在两个主要方面:

- 客户与整体式服务或应用程序间的通信，通常托管于中央数据中心。
- 服务器和网络存储间的数据中心内部通信。

图15 以前: 客户与服务和工作负载间的通信

但这种方式已无法满足需求，因为应用程序团队不断采用更为灵活的应用程序模式，这些模式不再是单一的，而是由多个并非总是在一起的、更倾向于分散的、在数据中心和内部环境之外的工作负载或服务组件构成。

图16 以后: 客户与服务和工作负载间的通信



尽管有些IT团队或许认为，向云端转移意味着对网络的考虑减少，但事实并非如此。IT领导者已经认识到，数据中心和云团队无法再与网络团队分开工作。目前，他们将用于支持多云环境（公共云、基础设施即服务（IaaS）或SaaS）的网络投资视为最高优先项之一。[14]

图17 IT团队优先投资用于多云环境的网络

问题：如果能减少花在维持现状方面的时间，您会更侧重于以下哪些增值服务？
来源：*《2019全球网络趋势调查》*； n = 505位IT领导者

思科数据中心CTO及名誉顾问Tom Edsall认为，“随着应用程序、工作负载、服务和数据在整个边缘云统一体中分布得越来越多，IT作为一个整体，需要承担更多的责任，以确保安全可靠地并按所需性能交付服务，不管其物理位置在哪里。数据中心的专业人员现在必须比之前更为紧密地与负责分支机构/边缘、WAN和园区网络的团队合作。”

考虑到当前这些变化，如今的IT和网络领导者需要把力量集中于何处呢？

向混合云和多云领域的扩展意味着要管理那些涵盖企业每个领域且不断变化的变量（应用程序、数据、用户和设备）。因此，基础设施和运营 (I&O) 及网络团队必须携手合作，处理从公共云和SaaS提供商的网络影响到对其内部环境的影响等一切事项。

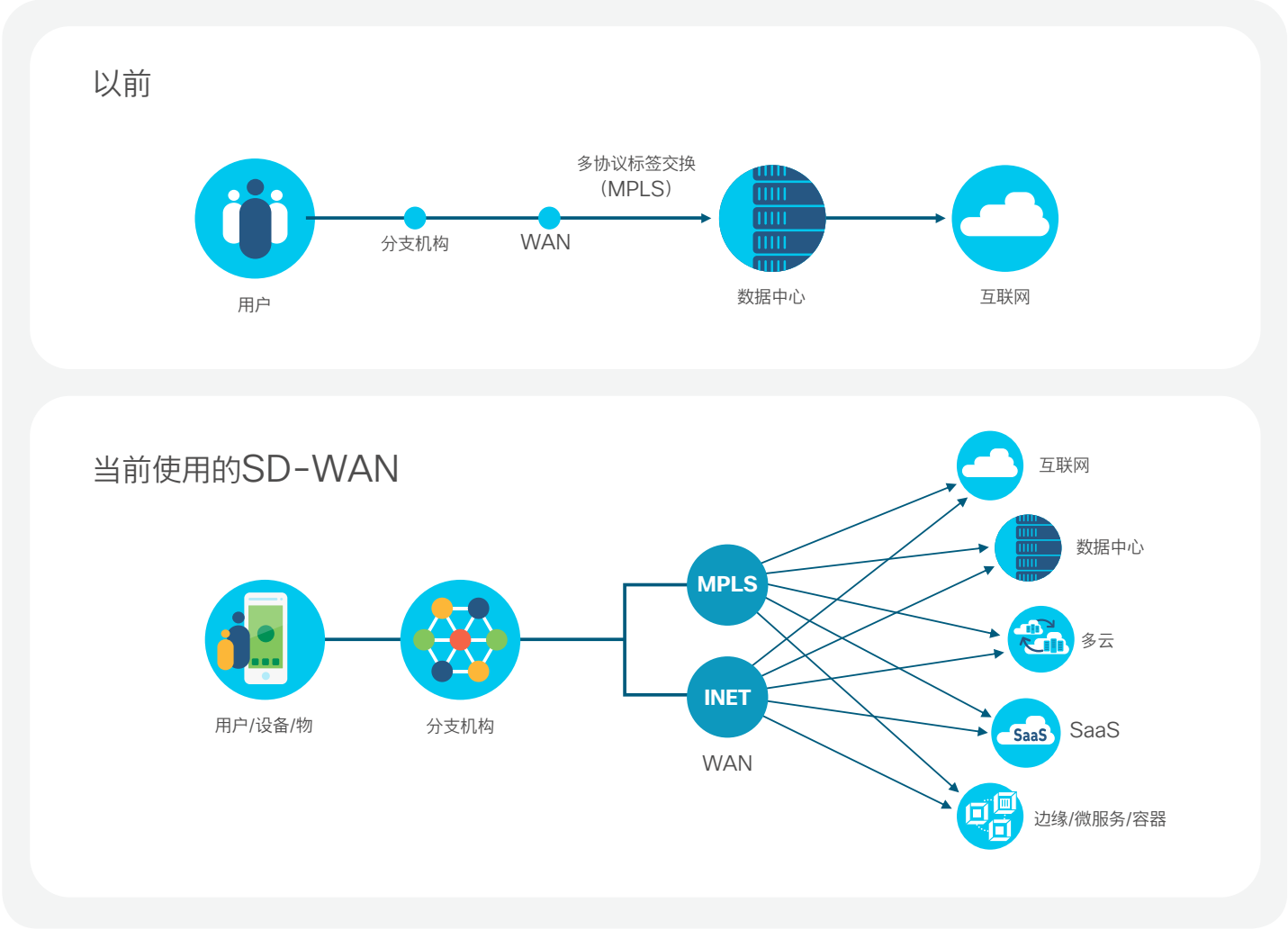
为帮助理解这种挑战，我们从两方面了解一下网络要求:

- 优化用户与多云的连接
- 用于“无处不在”数据中心的网络

优化用户与多云的连接

云服务的新兴优势意味着，与这些服务的远程连接变得比以往任何时候都更加重要。同时还意味着，侧重于连接远程站点与集中式数据中心的传统广域网架构不再是最佳架构。

图18 不断变化的WAN领域



既然SaaS、IaaS和分布式边缘服务可被托管在任何有网络连接的地方，那么遗留的中心辐射型WAN架构就可能阻碍企业的发展。

↑2X 对云的日益依赖也使WAN的流量上升，到2022年，全球商用IP WAN流量预计将增长2倍，达到每月5.3艾字节。[12]

SD-WAN、云直接访问、主机托管设施、云交换，以及更经济的高带宽宽带服务，正逐渐成为重要的新构架元素，以确保云服务可按业务要求实惠地交付。

IT团队需要在多云环境中的控制与自己网络中的相同，这样他们可以继续交付业务所期望的服务。

SD-WAN

SD-WAN是以软件定义的方式去管理WAN，这种方式可使集中控制器优化多云应用体验，大大简化WAN运营。

近来对SD-WAN的迅速采用表明，它为云日益增长的需求提供了很多解决方案。其实，云是采用SD-WAN最大的驱动器。在IDC对SD-WAN的调查中，近75%的受访者认为，SaaS/云服务对当前WAN的技术选择来说是重要的（或非常重要的）。[26]

这并不令人意外，因为用于连接由云服务提供商提供的虚拟私有云的传统选项和服务让企业网络团队在多云情境中控制受限。

据我们的*《2019全球网络趋势调查》*，全球超过58%的企业已经以某种形式部署了SD-WAN，且超过94%的受访者认为，他们会在未来两年内部署基本或更高级的SD-WAN。[14]

同时，随着5G服务的应用越来越广泛，SD-WAN会将它们无缝集成到一个与传输无关的框架中，以实现最大的灵活性和最佳性能，改进始终在线支持，并减少成本。

图19 多云就绪WAN

问题: 哪个陈述最好地描述了您所在企业当前对自己WAN架构的设计、部署和管理方式？

来源: *《2019全球网络趋势调查》*； n = 1556位网络策略师

云直接访问

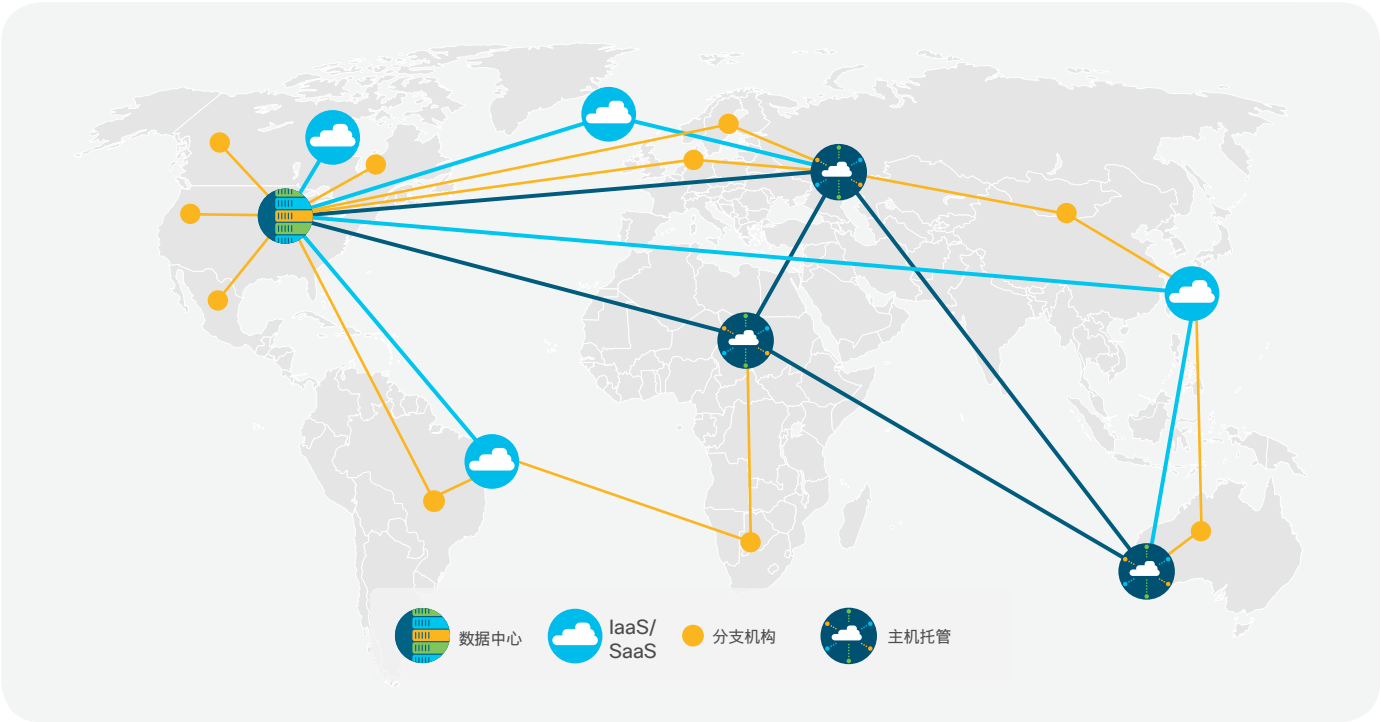
将分支机构流量通过昂贵的WAN电路回传至数据中心或通过中心辐射型架构回传至集中式互联网网关的传统方式可能阻碍向云服务的转变，同时还将增加费用并产生降低用户体验的延迟。

直到现在，网络架构师由于替代方法的成本和复杂性仍囿于这种方式，替代方案需要在每个分支机构路由器部署和管理分布式安全功能，如防火墙、URL过滤和DNS保护。

但“云直接访问”或“互联网直接访问”功能现在可将用户直接从分支机构安全连接到云服务。这简化了跨远程站点的策略

管理，并在数分钟内自动提供新的网络服务，同时实施了多层次安全防护，包括加密、认证、分段、防火墙和DNS保护。

图20　具有云直接访问和主机托管中心的安全SD-WAN



主机托管和云交换

虽然运营商中立主机托管 (colo) 设施并不是什么新东西，但它们在多云时代发挥了很大作用，并是新型云优化WAN构架的关键组件。实质上，由Equinix和其他互连服务等提供的colo设施成为了企业WAN的延伸，为多个SaaS和IaaS提供商提供可见性、高性能访问和集中式安全。(见上图20)

用于“无处不在”数据中心的网络

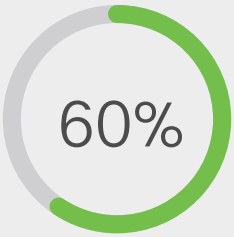
如今的数据中心不再是单一地点。新兴的“分布式数据中心”是应用程序和数据在混合、多云和边缘环境中共存的结果。但分布式数据中心与传统数据中心的运行方式不同，因此IT企业需适应并改变其技术和运营，以满足这种新型架构增加的应用程序和网络连接需求。

“无处不在”的数据中心需要IT团队在企业内部、企业边缘和混合云及多云环境中保持技术和运营的一致性。

自动化

数据中心内不断增加的规模、复杂性和工作负载的可移植性正迫使网络管理员撤换人工流程，并使用自动化工具管理网络策略和连接。

软件定义网络、自动化及用于4层至7层服务的NFV的采用将数据中心网络置于一个可行位置，以支持灵活的内部云环境。这实现了以工作负载为中心的网络与计算和存储服务的协调。其实，可以认为，仍未采用基于控制器且由API驱动的DevOps模型的数据中心网络已落后于时代。



近60%的IT领导者和网络策略师表示他们已在其数据中心部署了某种形式的SDN。[14]

近60%的IT领导者和网络策略师表示他们已在其数据中心部署了某种形式的SDN。[14]SDN/NFV已在数据中心内传输了23%的流量，到2021年，有望增加到44%。[23]那些未部署SDN的数据中心会为支持敏捷且灵活的应用程序模型而努力。

用于数据中心的基于意图的网络

基于意图的网络以SDN为基础构建，使数据中心团队获得了整体闭环验证构架，该构架可按既定策略实时分析数据中心的行为，并能使用有效且可靠的方法在网络内做出改变。这让IT团队能够跟上动态工作负载的变化，持续满足业务的应用需求。

在数据中心情境下，激活策略前对其进行验证也非常重要。使用IBN，可通过持续的、自动化的全网验证（包括合规性策略）来实现这一点。

将IBN扩展至多云环境

对当今企业而言，若想确保所需服务水平和安全，数据中心团队需将控制和可见性扩展到企业内部环境之外。IT团队可将IBN基于策略的自动化和实施扩展至多云环境，这样他们就能将策略一致地部署到工作负载，无论其在何处。

据我们的*《2019全球网络趋势调查》*显示，29%的受访者计划在两年内配置基于意图的网络能力，通过确保跨多云环境的自动化网络行动保持业务和意图的一致性。[14]

思科数据中心CTO Tom Edsall解释道: “IBN是网络界最大胆、最包罗万象的成果，其创建了一个系统范围的网络模型，可让敏捷企业应对所有最新技术趋势和瞬息万变的需求。”

> “基于意图的网络是网络界最大胆、最包罗万象的成果，其创建了一个系统范围的网络模型，可让敏捷企业应对所有最新技术趋势和瞬息万变的需求。”
>
> – 思科数据中心CTO兼名誉顾问Tom Edsall

内部云、多云或混合云成功实施的关键是使其简单化。为实现这一点，网络架构师应考虑:

- 云中无覆盖网络
- 无代理依赖，这对任何工作负载都具有广泛的适用性
- 对云规模的适应性

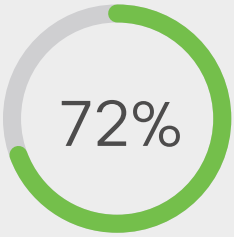
底层网络基础设施

在数据中心，底层网络基础设施需要提供开放的可编程性和遥测，以支持对IBN系统最为重要的自动化和分析。此外，数据中心网络基础设施还需要跟上流量的大幅增长。未来五年，

3倍

未来五年，全球数据中心IP流量将增长3倍。[23]

全球数据中心IP流量将增长3倍。总体而言，到2021年，数据中心IP流量将以25% (复合年均增长率) 的速度增长。[23]



到2021年，数据中心内的流量将占数据中心总流量的72%。[23]

网络基础设施需要灵活性和容量，以支持高性能的客户到应用程序流量 (南北流量) 和日益增长的服务器到服务器或VM到VM流量 (东西流量) 。目前，这一般是使用由一个或多个控制层覆盖协议支持的扁平“脊叶”架构完成的。

据《*思科全球云指数*》，到2021年，数据中心内的流量将占数据中心总流量的72%，将远远超过数据中心到用户 (15%) 和数据中心到数据中心 (14%) 的流量。[23]

对以太网交换性能的要求将不断提高，以支持计算流量及基于文件，甚至基于块的存储流量增长的需求。

当前，由于400 Gbp交换式以太网已成为主流，且IEEE正制定针对800 Gbp，甚至1.6 Tbp的规范，以太网诱人的资金和运营优势使它不可避免地成为某些工作负载下传统光纤通道交换的替代品。

构建多云网络时的考虑

在这种扩展的、更分布式的应用程序环境中，网络和云架构师、数据中心高管及基础设施和运营团队需制定可优化应用程序体验的网络策略。开始制定时，应考虑以下方面:

1. **深入了解企业的应用程序策略:** 从应用程序开始。IT和网路策略师应对企业不断扩展的工作负载和数据足迹有很好的了解。

2. **共同合作为多云提供一致性:** 企业需要其多云环境（包括企业内部）作为一个整体运行。正因所有这些复杂性，数据中心和网络团队应协作开发跨园区、分支机构、数据中心、边缘/IoT和公共云/SaaS提供商域的一致性，以实现最佳成本、性能、可见性、安全和用户体验。

3. **跨混合云和多云扩展基于策略的自动化一致性:** 团队应考虑跨任何平台、管理程序或容器框架、任何地点和任何工作负载（云原生、裸机、管理程序、容器和无服务器）实施基于策略的自动化。

4. **将应用程序服务和工作负载及服务组件映射到扩展的网络:** 网络策略师和从业者需对网络上有何应用程序、服务和微服务有深入了解。

5. **在SD-WAN策略中优先考虑应用程序性能:** 确定对任务最关键的、基于云的应用程序和服务，并优先考虑支持这些应用程序的SD-WAN计划。

6. **跨网络竖井对接访问策略和应用程序策略:** 为向各处交付基于策略的安全分段，应考虑IBN系统如何在不同的网络域（如WAN和数据中心）之间映射群组和策略。

7. **扩充NetDevOps技能集:** 由于工作负载和服务需要随需应变的网络服务(不仅是在数据中心内，而且在远程位置之间)，因此需要向网络明确表示自己的需求。这需要NetDevOps技能集，以了解如何将应用程序需求与网络策略对接起来。

8. **用AI成果提升SDN:** 使用AI功能加速问题排查，增强变更管理，保证合规性。

网络接入与无线

章节摘要

要点

- 开放漫游 (OpenRoaming) 等新兴功能将在不同的Wi-Fi 6网络和5G公共网络之间提供无缝、始终在线且安全的全球漫游。
- 网络团队需要增强的分析和AI功能，用于无线规划、健康监控、问题排查和补救。
- IT团队需要跨不同的接入网络自动管理、实施并传播一致的访问策略，以更好地保护应用程序、数据、用户和设备。
- 无线网络需要识别并动态支持新型沉浸式媒体应用程序和IoT设备的需求。

关键调查结果

- 在全球范围内，到2022年，无线设备将占到所有联网设备的43%。
- 到2022年，IoT M2M设备将占到全部联网设备的51%，其中大多数是无线连接。
- 35%的网络策略师认为，排查网络问题是当今网络运营中最耗资源和时间的活动。
- 34%的企业仍在使用人工方式管理有线和无线网络的访问。
- 40%的企业提供策略自动化和细分以减少威胁，而另外15%则使用AI驱动的访问解决方案。
- 27%的企业计划在两年内建立基于意图的网络访问模型。

重要指南

- 考虑Wi-Fi 6和5G将如何影响你所在企业的未来业务需求，并据此制定您的无线策略。
- 制定使所有移动和IoT设备的安全载入和细分实现自动化的路线图。
- 探索自动化设备分类的使用，实现各型IoT设备的大规模载入。
- 评估基于位置的服务和网络分析如何能为你的企业带来业务利益。

章节摘要 (续)

- 探索如何通过公共管理层来管理特定或高要求用例 (如蓝牙、Zigbee和Thread) 所需的任何专用无线技术。

高层前瞻

“到2025年，像开放漫游 (OpenRoaming) 这样的无线联合会将无处不在，IT企业和服务提供商由此可使用零信任访问系统，安全共享身份凭证，终端用户可安全无缝地在任何私人或公共无线接入网络上漫游。用户体验将是无摩擦和策略执行式的，不管用户在哪里访问都能为其提供最佳体验。”

– 思科无线技术CTO Matt MacPherson

“到2025年，基于IEEE 802.11ax标准的Wi-Fi 6网络将与计划中的Wi-Fi 6扩展网络一起成为无所不在的Wi-Fi的主要形式。大概在2024年，基于制定中的IEEE 802.11be标准的下一代Wi-Fi (可能作为Wi-Fi 7推出) 才会开始上市。”

– 思科董事、Wi-Fi联盟前主席和技术领导
Andrew Myles

网络接入与无线

到2022年，全球商用IP流量将达每月63.3艾字节，是2017年的3倍。[3]在以太网 (10Mbp) 、令牌环网 (16Mbp) 和FDDI (100Mbp) 等共享有线局域网处于相对简单的初始阶段，诞生了有线接入，其受益于半导体和光学领域的持续创新，已成为目前客户可以部署的用于LAN和城域网络环境的400Gbps交换式以太网的核心网络。

不断的创新预示着，针对确定性IoT应用程序的兆兆位以太网和时间敏感网络 (TSN) 等先进的新功能会在不远的将来变为现实。然而，在当今移动为主导的世界，无线接入才是瞩目的焦点。通过无线LAN (Wi-Fi) 或公共移动网络接入的无线网络将继续以人们难以想象的方式改变我们的生活。

“我们发现，数字业务的创新需要并推动无线创新的发展，同时，无线创新本身也为新的业务创新开辟了可能性。二者良性循环。”

––思科客户转型高级副总裁Guillermo Diaz

> “如今，“体验”是业务的重要部分，无线连接的进展将成为许多下一代体验的推动者。通过将最好的Wi-Fi 6和5G结合使用，网络团队有能力实现这些体验。”
>
> – 思科无线技术CTO Matt MacPherson

在全球范围内，到2022年，无线设备将占到所有联网设备的43%，而智能手机将占到全部联网设备的24% (67亿部)。同时，到2022年，IoT M2M设备的数量将增至146亿台，占到全部联网设备的51%，其中大多数是无线连接。[12]

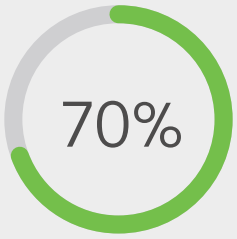
为移动用户提供愉快的体验

全世界的人们目前都已习惯于使用Ube、Waze和Webex®等移动应用程序，这些对他们的工作和私人生活发挥重要作用。人们希望他们的移动体验具有即时性——始终可用，不受约束，无处不在，且令人满意，并能通过IP不间断地访问无抖动的4K视频，进行超高速浏览，听到无比清晰的语音。

同样重要的是，无线网络需要支持新的业务创新。随着企业越来越多的使用高清视频、AR和VR等沉浸式媒体应用，领导们希望清楚网络是否具备支持新数字举措所需的性能、容量、覆盖范围和安全性，以便机会到来时，能够快速行动。

“想像一下，如果顾客能享受到由定位服务和AR驱动的个性化相关体验，或在仓库中安装数百万传感器，由自主式电动机器人和自动驾驶电动车辆执行指令并运送产品会怎样？”思科无线技术CTO Matt MacPherson解释说。

新型Wi-Fi 6和5G公共移动网络都承诺将提供更好的性能来支持这些要求。Wi-Fi 6具有更高的数据速率、更低的延迟、更高的设备密度和更好的整体性能。同样，到2022年，5G公共移动网络（计划于2020年在一些选定国家投入商用）要比4G的速度快4倍多。[12]



Wi-Fi被广泛用作一种移动卸载机制，在5G时代甚至更为必要。据预测，5G将卸载其流量的70%以上，相比于4G网络的59%有明显提升。[27]

此外，移动用户在访问企业、云和公共互联网应用程序时也希望有透明的体验。这包括登录和网络漫游。

Wi-Fi 6与5G的结合会让用户在私人和公共区域（无论室内还是室外）获得透明且始终在线的体验。这包括对新的大流量应用程序的支持，这些程序很容易突破许多用户移动数据计划的限制。

为实现这一愿景，OpenRoaming以Wi-Fi联盟的Passpoint技术为基础构建。[28]尽管仍处于早期阶段，但由思科和几个领先的无线企业共同组成的OpenRoaming基金会正致力于使跨私人和公共无线网络进行无缝、安全漫游的宏伟目标变为现实。

通过由接入网络和身份提供商，包括移动运营商组成的基于云的联盟，允许用户在不同的Wi-Fi 6网络和公共5G网络之间轻松安全地全球漫游。在最近召开的世界移动通信大会上，OpenRoaming得到了成功的演示。[28]

用户使用智能手机和平板电脑等双模设备能够在私人家庭或商用Wi-Fi网络、公共Wi-Fi热点和5G公共网络间无缝切换。

“有了OpenRoaming，移动用户再也无需猜测哪个Wi-Fi网络可用、忍受弹出式强制门户，或再次使用不安全的用户名和密码。无论他们身处何处都可以接入网络，下载、串流、视频聊天、玩游戏，甚至随心所欲地工作。”

– 思科无线技术CTO Matt MacPherson

让IT为无线的成功做好准备

由于部署和维护无线网络所用的传统方式不可持续，因此网络运营要走在这些新兴业务需求的前面。

特别是无线网路的问题排查，对大多数网络团队而言，这是一项被动、复杂且耗资源的工作。难怪网络领导者目前将排查网络问题视为网络运营中最耗时的作业。[14]

更为复杂的是，除了新兴的Wi-Fi 6和5G网络外，IoT设备还可通过包括BLE、Zigbee和Thread在内的多个利基无线协议通信。IT面临的挑战将是确保网络管理工作不会在这些不同的网络上分崩离析。

尽管许多IoT用例集中在主流Wi-Fi 6和5G网络上，但IT团队应考虑如何通过公共管理层来管理独特或高要求用例所需的更专业的无线技术。

若想先人一步，NetOps团队需要一种更主动的方法来进行无线规划、监控、问题排查和补救。这要求使用分析及AI驱动的监控更好地了解无线性能及其健康状况。

网络接入就绪度的当前和未来状况

IT不能依靠传统的人工接入网络运营来支持移动用户。相反，企业需要一种跨所有网络域的软件驱动方式。

网络管理系统要能够跨不同的接入网络自动管理、实施和传播一致的访问策略，即便当用户和工作负载继续移动时也是如此。这需要解锁数据和洞察力，从而使IT实时支持业务并利用AI更好地预测问题和实现日常工作的自动化。而且，鉴于IoT应用程序的日益普及，网络需对IoT设备进行自动识别和分类，并适用相关策略。

总之，这些功能会使员工、客户和业务领导者充分利用Wi-Fi 6和5G，并让IT不仅在无线大潮中生存下来，还要确保移动通信世界中的安全性和最佳用户体验。

在我们的《*2019全球网络趋势调查*》中，我们向网络策略师询问了他们在采用与五级就绪度模型相关的安全接入架构方面处于哪一阶段。72%的受访者计划在两年内部署AI驱动或基于意图的接入，而之前这一比例只有18%。这样做会让他们动态地创建并改变策略，并最终在用户和服务之间始终一致地将访问策略与业务意图端到端对齐，无论用户在何处漫游或位于何处。[14]

图21　安全接入就绪度

问题：哪个陈述最好地描述了您所在企业当前的网络安全方法？
来源：《*2019全球网络趋势调查*》；　n = 1556位网络策略师

实现数字时代接入和无线技术的考虑

1. **无线保障工具将成为必需品:** 在大多数行业中，无论对于客户还是物，无线连接都是主要的接入方式。网络策略师需准备好先进的无线保障系统和工具，以有能力在所有IT和IoT接入网络提供一致的无线体验。

2. **基于策略的有线和无线分段将省去很多麻烦:** 跨接入、核心和分支结构网络的基于策略的自动化可根据用户和应用程序动态创建和管理段和微段，以便网络形成动态的零信任屏障，拦阻攻击和威胁。

3. **在广泛部署IoT前使用AI驱动的设备分类:** 使用昂贵的安全解决方案保护便宜的IoT传感器、监视器和其他设备没有什么经济意义。然而，使用自动化设备分类和基于策略的自动化，可根据IoT设备和应用程序组动态地创建和管理IoT段和微段。

4. **为Wi-Fi 6、5G和OpenRoaming做准备:** 网络领导者应确保他们的无线路线图考虑到Wi-Fi 6和5G将如何互补，以及如何与设备、Wi-Fi运营商和服务提供商合作来提供OpenRoaming功能。

5. **考虑基于位置的服务:** 许多零售、卫生保健和教育领域的企业高管正利用室内基于地点的服务所带来的好处改善客户体验。根据我们的调查，51%的受访者已在使用位置感知无线技术，通过移动应用程序实现更为个性化的客户体验。另外40%则正在考虑时机。[14]

6. **为微服务在边缘网络设备的运行做准备:** 随着Kubernetes和其他管理和协调能力（用于基于容器的工作负载）的出现，将网络或应用程序服务组件托管到位于边缘的、具有工作负载能力的网络设备上这一举措，对应用程序团队越来越有吸引力。要考虑这将对您网络的策略、性能、安全性及分段要求有何影响。

不断改变的网络安全角色

章节摘要

要点

- 随着应用程序、数据和身份向云端和网络边缘的迁移，仅基于边界的安全无法有效防御当前的威胁。
- 许多不同类型的设备，以及从各处接入网络应用的移动客户，混杂的状态带来新的挑战，如可见性和控制的缺失。
- 将安全性与基于意图的网络功能集成在一起，可产生强大的组合，从而跨网络实现有效的策略执行、保护和修复。

关键调查结果

- 网络策略师将安全视为仅次于AI的重要投资领域。
- 43%的网络团队将提高嵌入式网络安全能力作为优先事项。
- 2019年，48%的首席信息安全官 (CISO) 将“补救时机”看作主要的关键性能指标 (KPI)，比2018年的30%有所上升。
- 近75%的网络领导者有信心在两年内拥有AI驱动的适应性或自动化的策略定义和实施。

重要指南

- 在五个关键领域开发网络安全能力: 可见性与威胁检测、零信任接入、持续保护、可信网络基础设施、安全运营 (SecOps) 和网络运营 (NetOps) 一体化工作流程。
- 确保将零信任安全策略包括在任何网络自动化和保障计划中，以有效管理安全威胁，不管它们存在于分布式网络的何处。
- 在升级基础设施和流程时，网络团队应考虑可信要求，确保网络本身可防篡改。
- SecOps和NetOps团队需要考虑如何分享数据，并应整合工具，以简化威胁防御、检测和响应工作流程。

章节摘要 (续)

高层前瞻

“到2025年，一些领先的IT企业会部署一系列有限的完全自动化的网络驱动安全工作流程，帮助提高补救速度，减少SecOps团队的工作负荷。随着IBN平台、AI/ML技术，及安全和网络工具间的集成日趋成熟，将使一些定义明确、不会给企业的安全态势或网络带来风险的用例实现自动化。”

– 思科CISO顾问团队负责人Wendy Nather

“虽然量子计算到2025年仍将处于早期阶段，但人们已经在努力应对量子计算被用于破坏当前加密方法的新危险。”

– 思科研究员David McGrew

不断改变的网络安全角色

移动、多云和IoT模型的采用正在产生新的网络安全挑战和机会。传统的企业网络边界目前只是一个更为分布的模型的一部分。在此模型中，必须对所有用户、物和应用程序的身份进行质疑，无论它们是否在园区或分支机构内、VPN上、公共网络上，或云中。

IT团队需要利用网络和安全的综合力量来有效应对网络安全挑战。网络策略师很容易认识到对网络安全进行投资的重要性。在我们的*《2019全球网络趋势调查》*中，当被问及网络团队如何才能更好地满足业务需求时，受访者将安全视为继AI之后的第二个重要投资领域，其中43%的网络团队将提高嵌入式网络安全能力作为优先事项。[14]

安全与基于意图的网络模型的结合能够使企业应用并实施业务角色策略，并对所有网络服务的威胁做出更快的响应。

在新形势下，NetOps团队与其所控制的网络在以下五个方面扮演至关重要的安全角色:

可见性: CISO关注的是在新型分布式应用程序和数据模型中保持可见性。

零信任接入: 网络是实现一致性信任模型必不可少的一部分。在该模型中，所有用户、设备和应用程序都同等可疑，不管他们在何处接入网络。

Forrester Research公司认为, 零信任网络模型必须做三件事情: [29]

1

对网络分段, 以应用粒度控制并防止横向移动。

2

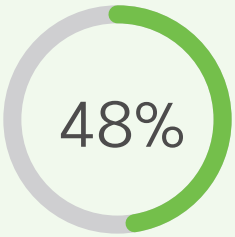
为威胁检测和响应提供网络粒度分析和可见性。

3

提供统一的网络安全可管理性并奠定自动化基础。

持续保护: 网络需要同时作为分布式检测机构和执行机构, 能够自动和快速地采取行动来遏制受感染的设备。

可信网络基础设施: 随着恶意分子寻找保密信息或试图破坏网络运营的威胁日益增加, 企业必须保证网络系统和各个网络设施免受攻击。



2019年, 48%的CISO将"补救时机"看作关键性能指标(KPI), 比2018年的30%有所上升。[30]

无缝的SecOps和NetOps工作流程: CISO将SecOps和NetOps视为合作伙伴, 95%的人表示他们很合作或特别合作。[30]但两个团队仍倾向于使用不同的数据、工作流程和工具去收集并分析数据。SecOps和NetOps团队要重新考虑如何能简化工作流程、分享数据和整合工具, 以实现自动化威胁防御、检测和响应这一共同目标。

据Gartner Research的研究, "对SecOps而言, 网络流量接入支持流量流的回顾性分析、渗漏企图的识别、网络取证和微分段工作流程。"[31]

网络安全挑战

规模和复杂性增加

面对更大、更复杂及快速变化的移动优先和云优先环境，以及防御难度日益增加的安全威胁，IT必须保护企业及其数据。

工作负载: 随着应用程序、数据和身份向云端和网络的迁移，IT模型继续拓展并超越传统的企业边界。混合云计算和多云计算以及边缘托管的微服务的兴起，要求我们改变保护工作负载的方式。仅基于边界的安全无法有效防御当前的威胁。

客户: 此外，许多不同类型的设备（用户设备和互联IoT设备）与从各处接入网络应用的各种不同用户（员工、承包商、第三方）的混合也使情况更为复杂。[30]

基础设施: 最后，随着威胁复杂性的发展，攻击者越来越多地试图颠覆底层交换和路由基础设施，以便窃听、窃取或操纵数据，并对网络的其他部分发起攻击。[32]

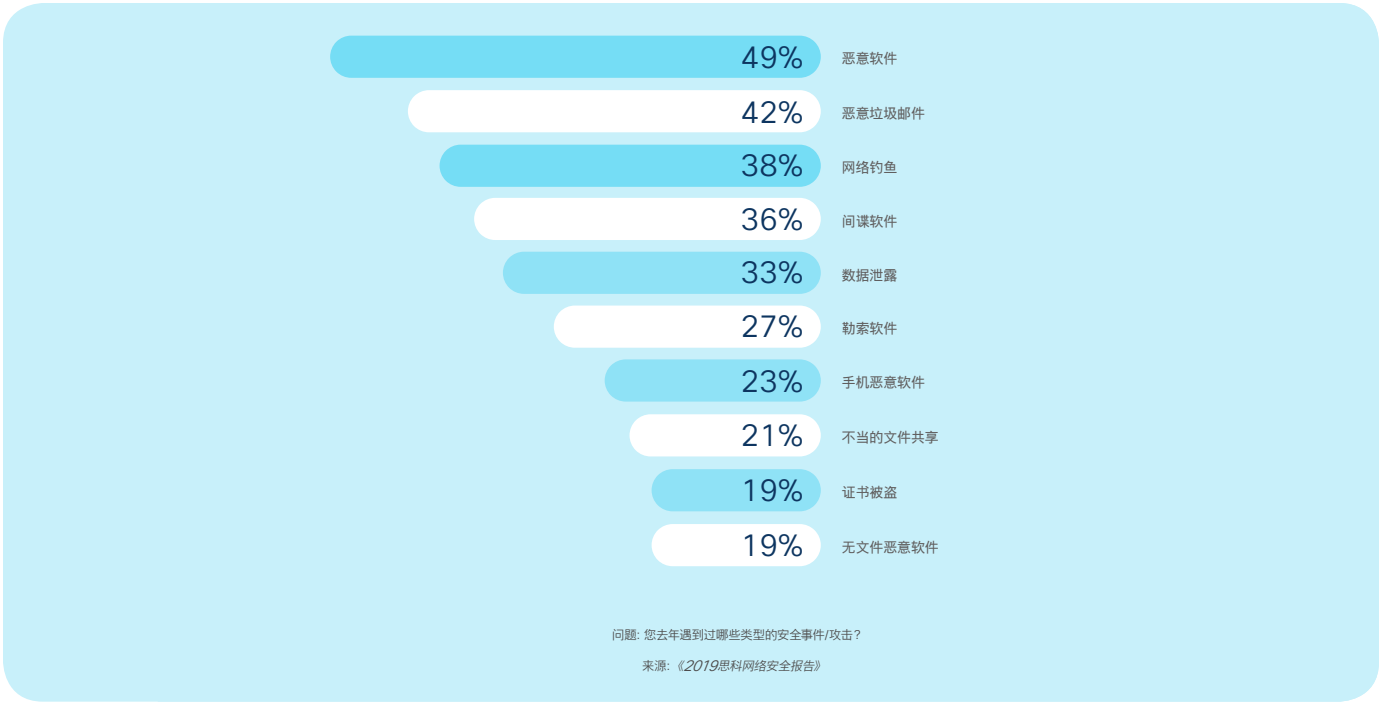
> “我们和任何其他大型企业一样，需要应对日益增加的复杂性。我们每天要检查47太字节的互联网流量，分析280亿次流动，记录1.2万亿个安全事件。”
>
> – 思科基础设施安全总监Marisa Chancellor

威胁趋势: 攻击者不断创新

由于网络攻击的潜在收益越来越具有诱惑力，因此攻击的类型也越来越复杂。一些更令人担忧的攻击趋势包括:

- 基于网络的自传播勒索软件
- 隐藏在加密流量内的加密恶意攻击，这种攻击方式竟占到了2017年所有恶意攻击的70%[4]
- 部署在有漏洞和不受监视的IoT设备上的IoT僵尸网络

图22 当前的网络安全威胁



欲了解与威胁趋势演变有关的最新信息，请参看当前的《思科网络安全系列威胁报告》。[33]

合规性

安全团队还面临遵守新颁法规的问题。这意味着要保证并证明有效的安全策略已经到位。

2018年生效的《欧盟通用数据保护条例》(GDPR) 要求对数据隐私采取积极的保护措施。同时，医疗保健、金融服务、零售、联邦政府和其他部门还在制定其他的合规标准，如若违反将受重罚。

IoT设备的激增扩大了受攻击面

联网IoT设备在没有充分安全保护的情况下继续迅速增加，这主要是因为它们经常不被IT所知或未受IT检测。对企业来说，每联网一台设备都会增大受攻击面。针对IoT设备的网络级攻击可能包括分布式阻断服务 (DDoS) 攻击、射频识别 (RFID) 电子欺骗、以密码为目标的软件威胁和恶意软件威胁。

可见性缺失

新的云端应用程序和微服务的大幅增加可导致IT可见性和受攻击面控制方面的缺乏。用户现在能够安装并自行启用可能不安全或要求过多访问权限的应用程序。

> “许多IoT设备本身的安全防护很有限，很少使用数字证书或凭证，所以易受到攻击。因此，设备识别、分类和网络接入策略激活的自动化成为了防止或遏制安全漏洞的重中之重。”
>
> – 思科IoT首席工程师Tim Szigeti

移动设备（公司或个人所有）的数量和种类将继续增加，且携带自己设备的趋势意味着更多个人所有的智能手机、笔记本电脑、平板电脑等在访问关键的应用程序，这进一步导致了可见性和控制的缺失。

用智能网络应对安全挑战

拥有智能网络的NetOps团队是SecOps团队的强大同盟，并与之并肩作战，确保企业及其数据的安全。通过采用以安全功能为基础的基于意图的网络模型，IT可帮助网络自动且有效地确定什么是新的、什么是重要的、什么是异常的，无论其存在于分布式网络何处。

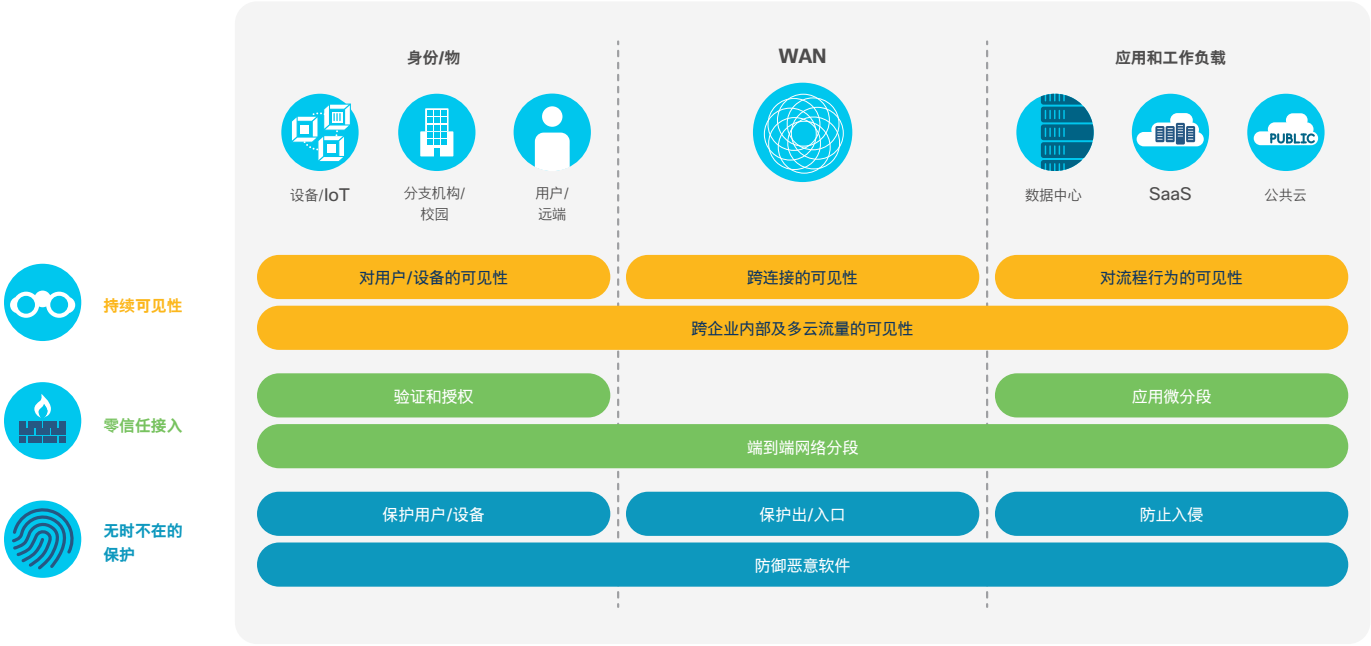
基于意图的网络与安全的结合最终将对网络上的人和事提供持续的可见性和控制，同时也有助于建立完整的零信任模型，并在网络内而非网络上构建威胁预防、检测和快速响应机制，提供无所不在的持续保护。（见下图23）

网络可见性和威胁检测

无法看到就无法保护，这千真万确。可见性对于IT团队保护网络资产和信息来说至关重要。这包括对用户、设备、应用程序和物的可见性，不管它们在哪里，以监控异常活动并制定策略。

> “我们正面临向SaaS的大规模迁移，并正在失去我们过去曾经拥有的传统的可见性和控制。”
>
> – 思科基础设施安全总监Marisa Chancellor

图23 集成的网络安全模型



对接入、WAN、数据、多云和IoT网络的完全可视性可使流过网络的每次流动映射出来，这样团队就能够确定正常网络行为的动态基准。有了可提供完全可视性的智能网络，网络团队就有了帮助安全团队更快更准确地（甚至在加密流量中）检测威胁并进行补救的宝贵资源。

零信任接入

无论可疑的设备和工作负载是何类型、在何处接入，NetOps团队都能借助建立在先进可视性基础上的整体式零信任安全模型对接入进行管理。若使用得当，它能保护私有云或公有云中的工作负载和数据以及工作人员，即便用户已离开网络也是如此。零信任模型的主要功能包括:

保障网络接入安全: 在零信任接入模型中，IT对有线和无线网络上的用户和IoT终端可在何时、何地、如何做什么实行精确控制。同时，还能借助基于群组的策略控制和端到端、客户到应用程序分段来应用零信任方式，从而限制对您网络上资源的访问。

主动遏制应用程序漏洞: IT工作人员可减缓数据中心内外工作负载间未经授权的横向运动，这有助于在攻击者已经进入时减少攻击面。

降低未经授权访问应用程序的风险: 不管是什么用户（员工、承包商、第三方等），当他们登录到任何内部或外部应用程序时，需使用双因素验证确认其身份及其设备的

安全性，降低因密码被盗或密码弱而导致的未经授权访问应用程序和数据的风险。

无时、无处不在的保护

要保护企业的所有用户和系统，网络需与时俱进，将保护拓展到传统边界之外。SD-WAN等基于意图的构架可提供集中控制平台，用于部署和管理将保护延伸到每个网络出入口的全边缘安全堆栈。要实现全方位保护，这种安全堆栈应包括网络分段、防火墙、安全网关、恶意软件防护和DNS层安全。

对于任何试图进入的恶意文件，恶意软件检测都能迅速指令网络将受感染设备自动移至受限制或隔离网段。通过持续更新威胁情报并阻断恶意文件，及将情报提供给终端和上传至云端，系统可在威胁再次来临时实施阻断。

构建可信网络基础设施

随着企业的数字化和威胁的逐步升级，验证网络基础设施和个人网络设备安全性及完整性的必要性在增加。

构建“可信”网络基础设施需要在产品的整个生命周期全面实施安全措施。这有助于防止在生产、分发、部署及持续运行期间受到篡改和操纵，这一点很重要，因为第三方分销商、系统集成商或服务管理提供商经常参与这些过程。

对设备进行升级时，网络团队应寻找多种重要能力，如硬件固定式安全启动、安全且唯一的设备标识，及销毁秘钥和激活工厂重置的能力等。

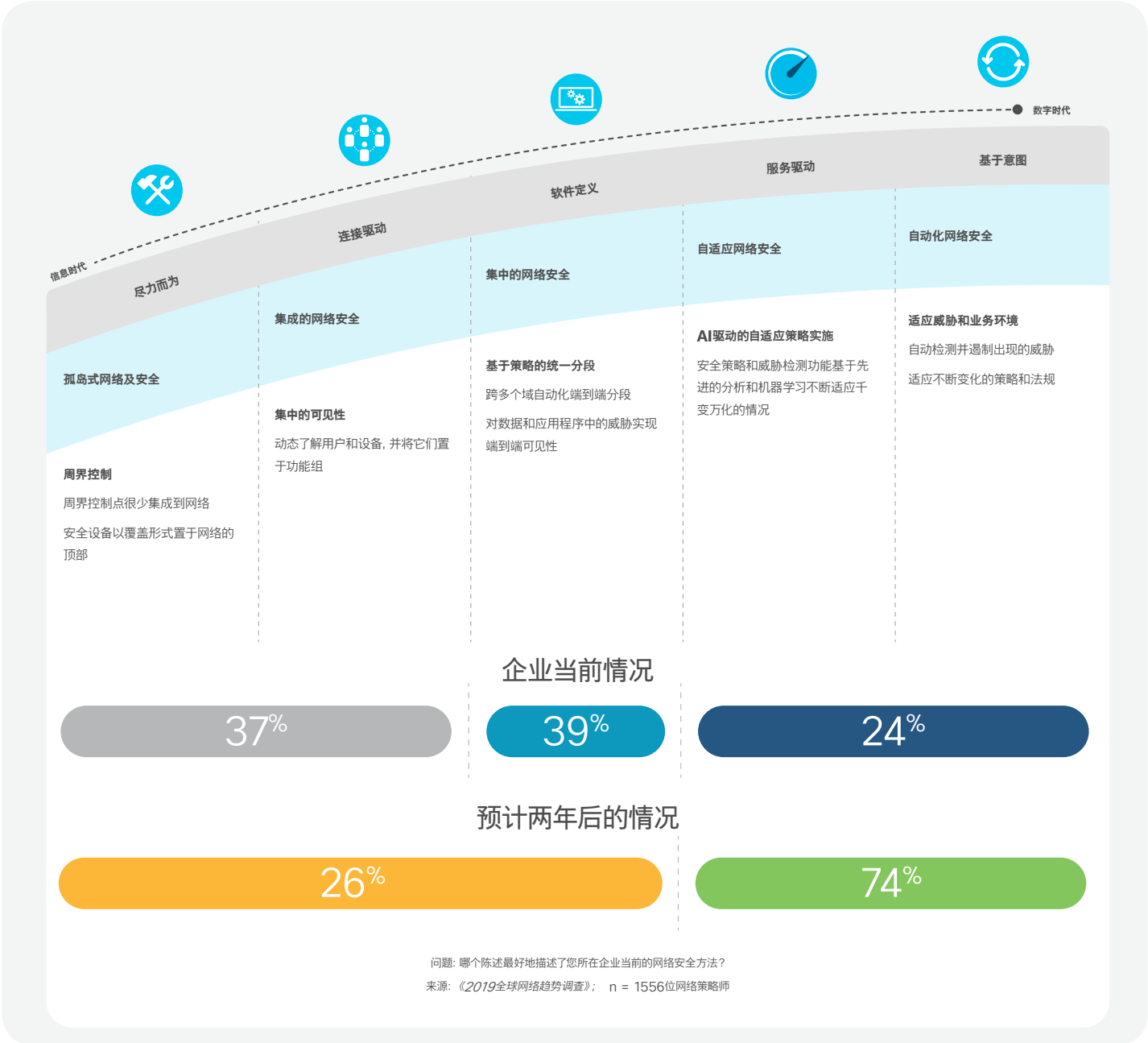
总之，网络正越来越善于应对当前及未来的威胁。NetOps和SecOps团队应采取行动将这些先进的安全能力融入其设计和运营中，携手合作，向实现持续可见性、保护和信任的目标前进。

网络安全的当前和未来状况

目前企业在为实现连续保护而建立全方位网络安全模型方面处于什么阶段呢？

在我们的《*2019全球网络趋势调查*》中，我们询问了网络领导者：如果按照我们的五级就绪度模型，会如何评价他们当前的网络安全状况。尽管企业当前在各个等级的分布相当平均，但有近四分之三的受访者表示，他们有信心在两年内建立某种形式的AI驱动的自动化安全策略定义并加以实施。[14]

图24 基于意图的网络安全就绪度



问题：哪个陈述最好地描述了您所在企业当前的网络安全方法？

来源：《*2019全球网络趋势调查*》； n = 1556位网络策略师

2020全球网络趋势报告

网络运营趋势

从被动反应到业务优化的转变

章节摘要

要点

- 面对不断增加的数字化需求，传统的网络运营模式已不足以支持所需的业务服务。
- IT团队正在对IT运营进行现代化，并正在采用DevOps方式，以利用基于控制器的系统和AI工具，实现或消除许多传统的重复性网络工作。
- 先进的新型开放式网络平台可更好地与其他IT和安全系统及运营流程整合，为业务应用程序开发商提供新机会。
- 下一代网络运营有利于领导者和团队脱离被动的运营模式，持续交付业务需要的准确服务。

关键调查结果

- 73%的团队为维持网络现状而花费了其一半以上的时间。
- 如果IT领导者能够将网络团队资源从日常维护任务中释放出来，那么他们将能够专注地投入到多云领域、加快应用程序部署、更好地保护网络应用程序和数据。
- 超过三分之一的IT领导者将实现与其他IT团队和行业更好的网络合作与整合作为重要事项优先考虑。

章节摘要 (续)

重要指南

- 当采用基于控制器的自动化和保障模式时，网络团队应将精力集中在三个关键的流程领域：生命周期管理、策略管理和保障管理。
- 为提高服务质量、灵活性、安全性并降低成本，网络管理员应从对单个设备的管理中抽身，将注意力集中在网络控制器及通过控制器管理端到端网络系统上来。
- 网络团队应采用开放式平台、DevOps主导的方法，将网络融入IT流程，并简化端到端工作流程，以提升效率并更快速响应业务需求。
- 网络运营团队应具备新兴的AIOps能力，以提供更好的网络和业务成果。

高层前瞻

将业务与IT连通：“团队将调整网络维护用时，注重如何使网络更好地满足企业需求和支持业务创新，并赋予运营新使命，将业务意图和应用程序需求转化为网络策略。”

NetOps将监控拓展到云：“随着多云业务服务成为常态，NetOps团队将跨WAN、公共网络拓展可视性和预测性监控，并将其拓展到云接入点。对于更深入的洞察，企业基于意图的网络系统将开始把来自服务提供商的数据与云提供商系统融合，以确保云服务体验质量的连续性。”

– 思科客户体验CTO Rich Plane

从被动反应到业务优化的转变

据思科研究，IT领导团队正在为他们的组织带头进行数字化转型。为此，他们正在推动一项独立但同等重要的转型——使IT基础设施和运营现代化，以满足新兴的数字化需求。[34]

通过采用开放式平台、DevOps主导的方法，网络团队首次拥有了将网络融入IT流程的工具和技术，简化了端到端工作流程，从而提高效率和对业务需求的更快响应。

这种方式还为在网络域间建立运营之桥并直接与应用程序融合提供了机会，更好地支持各行业不断变化的需求。

通过采用新的方式思考网络运营和新的工作方式，IT领导者和团队将能更好地交付各行业需要的精准服务，不管是更好的现有服务，还是业务驱动的新服务。

63%

据我们的*《2019全球网络趋势调查》*，63%的IT领导者计划在三年内建立可动态满足业务需求的先进网络。[14]

网络运营的当前和未来状况

支持数字化转型的运营就绪度

在我们的*《2019全球网络趋势调查》*中，我们就保障管理的五级成熟度（从被动反应到业务优化）询问了IT领导者和网络策略师如何将他们当前的网络运营就绪度分级。

虽然目前只有23%的受访者认为自己具有预测性或业务优化能力，但71%的人计划在两年内实现这一目标，这凸显出企业在准备应对企业网络日益增长的需求时感到的紧迫性。[14]

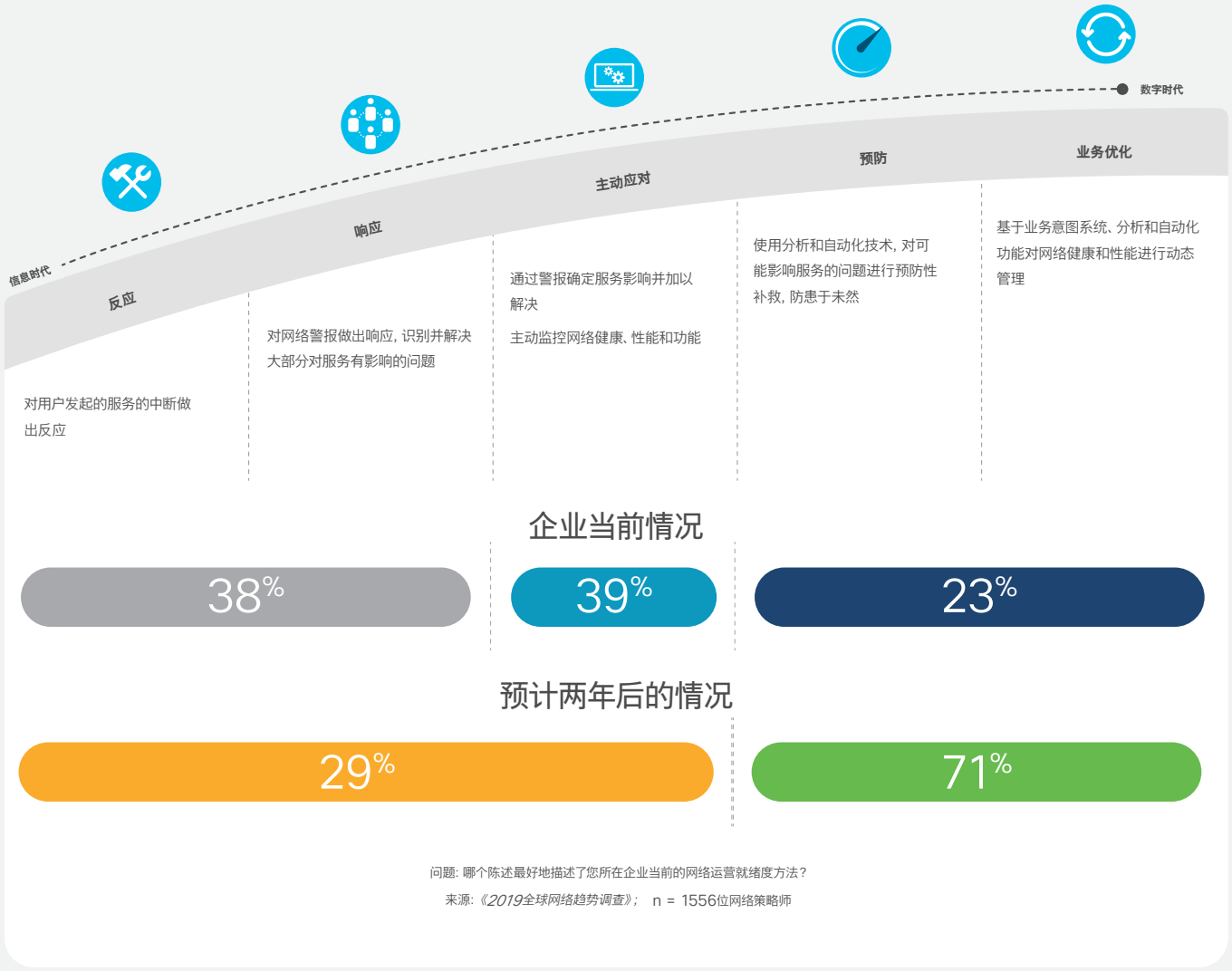
网络进步如何改变网络运营

近年来，先进网络技术的迅猛发展将改变网络运营的方方面面，预计在以下方面会出现重大变化：

网络运营集成至IT流程中

过去由主要具备某个领域专业知识的工程师在技术孤岛中运营网络的日子正在迅速消失。在我们的研究中，约三分之一的IT领导者强调了与其他IT团队进行更好的网络协作与整合的重

图25 网络运营就绪度: 保障管理



问题: 哪个陈述最好地描述了您所在企业当前的网络运营就绪度方法？

来源:《*2019全球网络趋势调查*》； n = 1556位网络策略师

要性，而26%则透露了提高与各行业合作能力的重要性。[14]另外27%则认为在不同网络域的孤立的设计和运营方式正在拖累他们。[14]

由于基于意图的网络控制器提供了开放式接口，所以NetOps团队将舍弃孤岛式运营，成为IT工作流程中完全整合的一部分。34%的IT领导者将这一改变视为最有助于网络团队更好地满足企业需求的举措。[14]

然而，为实现所需水平的IT灵活性并持续符合意图，NetOps团队将肩负起改善整个网络域（接入、WAN、数据中心、云等）及与其他IT域（如，IT服务管理（ITSM）和SecOps系统）进行整合的责任。

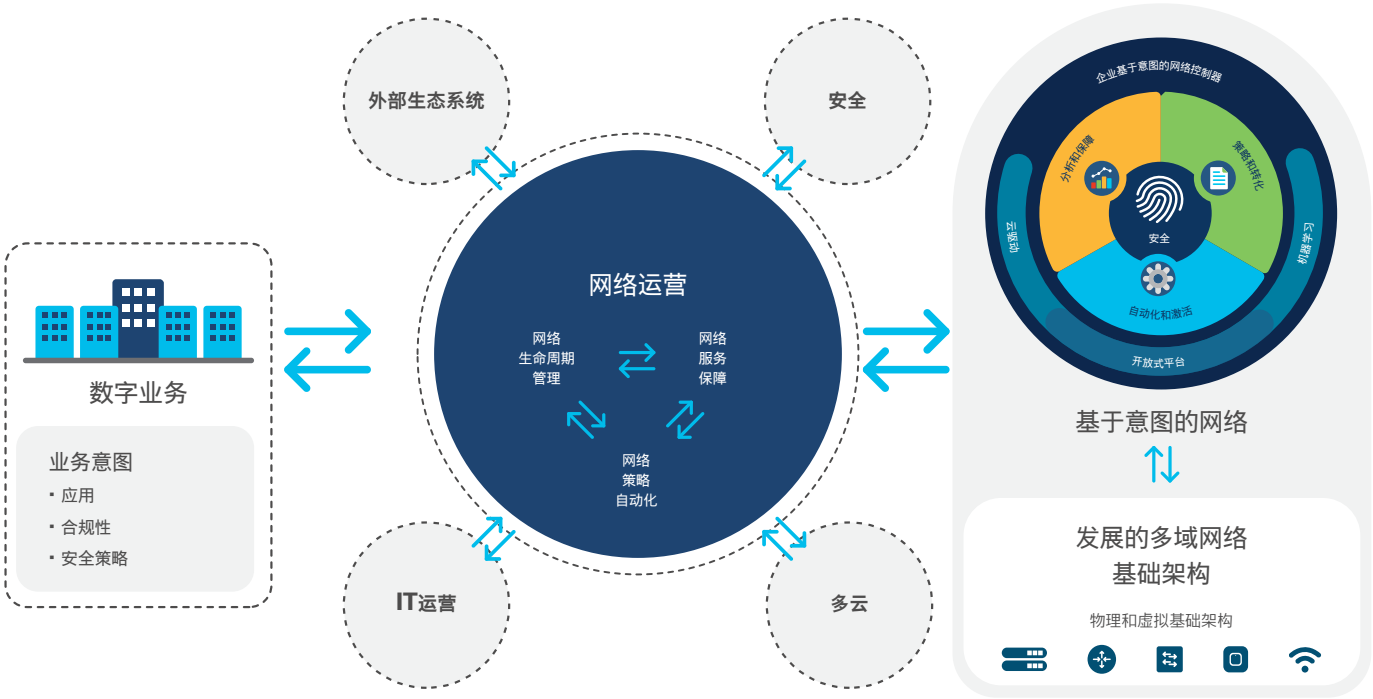
本图说明了NetOps如何能够使用开放式平台和网络DevOps方式将网络技术和流程与其他的内部，甚至外部系统进行整合。

完全符合IT和业务意图

从本质上讲，网络的存在是为了提供支持员工、客户和合作伙伴所需的服务，换言之，是为了运营业务。但实际情况是传统的人工运营方式通常难以满足动态的业务需求，这就需要改变。

使用基于意图的网络，网络运营将更为自动化和动态化，并由业务和IT意图直接通知。这些意图包括应用程序性能需求、安全策略与合规性及IT流程。

图26　使用开放式网络DevOps方式的整合机会



随着时间的推移，将业务和IT意图转换为网络策略将成为网络运营角色不可或缺的一部分。

实现自动化以减少网络运营复杂性

毫无疑问，运营任务的自动化正改变着网络运营的面貌。四分之一的IT领导者和网络策略师认为，自动化技术将在未来五年对他们的网络策略和设计产生最大的影响。[14]

然而，这将意味着要舍弃传统的人工配置和维护网络的方式。一些团队因此而惴惴不安，20%的IT领导者认为NetOps团队不愿采用自动化和AI技术是现代化的主要障碍。[14]

预防性与被动反应问题及事故管理

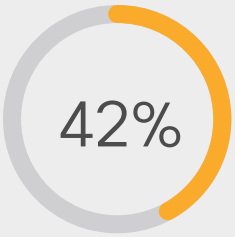
如前面所述，许多企业发现自己处于运营就绪度的被动反应阶段。这方面的挑战是，25%的受访者表示，被动反应的运营思维是他们实现其网络目标的拖累。[35]这同样需要改变。通过使用AI并与其他IT系统集成，NetOps团队将能够实现预见性维护状态，并可在问题变成事故并影响服务前将其解决。

人与人工智能协调工作

在应对网络复杂性方面，网络工程师需要获得一切帮助。

正因此，NetOps团队正在配备机器学习、机器推理等新的智能运营（AIOps）能力，它们可提供更准确的性能基准、异常检测、自动化根本原因分析、补救指南和预测性洞察。

NetOps团队将不再对成千上万的事件进行筛查，而是日益依靠这些技术准确地找出最重要的问题，提供最优补救选项。同时，AIOps团队还可对这种输出进行微调，丰富其内容，并将专业知识与关键业务和服务管理系统集成。



向AIOps转变的势头正在兴起，42%的IT领导者认为，在未来AI对他们的自动化运营影响最大。[35]

为网络运营带来连接性

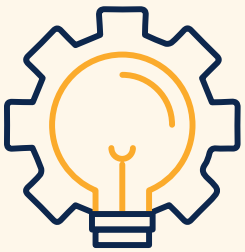
目前，IoT设备被视为业务资产，且其产生的运营数据对业务运营至关重要，这凸显了采用新方式进行基础设施管理的必要性。

- 在实时监控等IoT用例中，运营问题可能造成严重的、甚至危及生命的后果。
- 大型网络中的IoT设备可能达到数以百万计，因此自动化是有效管理这些设备的唯一方式。
- 在一些用例中，HQ与远端IoT设备间缺乏有保证的持续连接（这推动着对边缘分析和雾分析的投资）。

引入下一代网络运营框架

为迎接未来以基于意图的网络驱动的网络运营，思科客户体验技术专家已创建了一个框架，该框架可提供策略指南、最佳实践、经验证的设计、经证明的流程和推荐的调整。

该模型的核心是三个过程领域：生命周期管理、策略管理和保障管理。IBN提供的运营简化使围绕这些核心流程规划并建立运营转型成为可能。

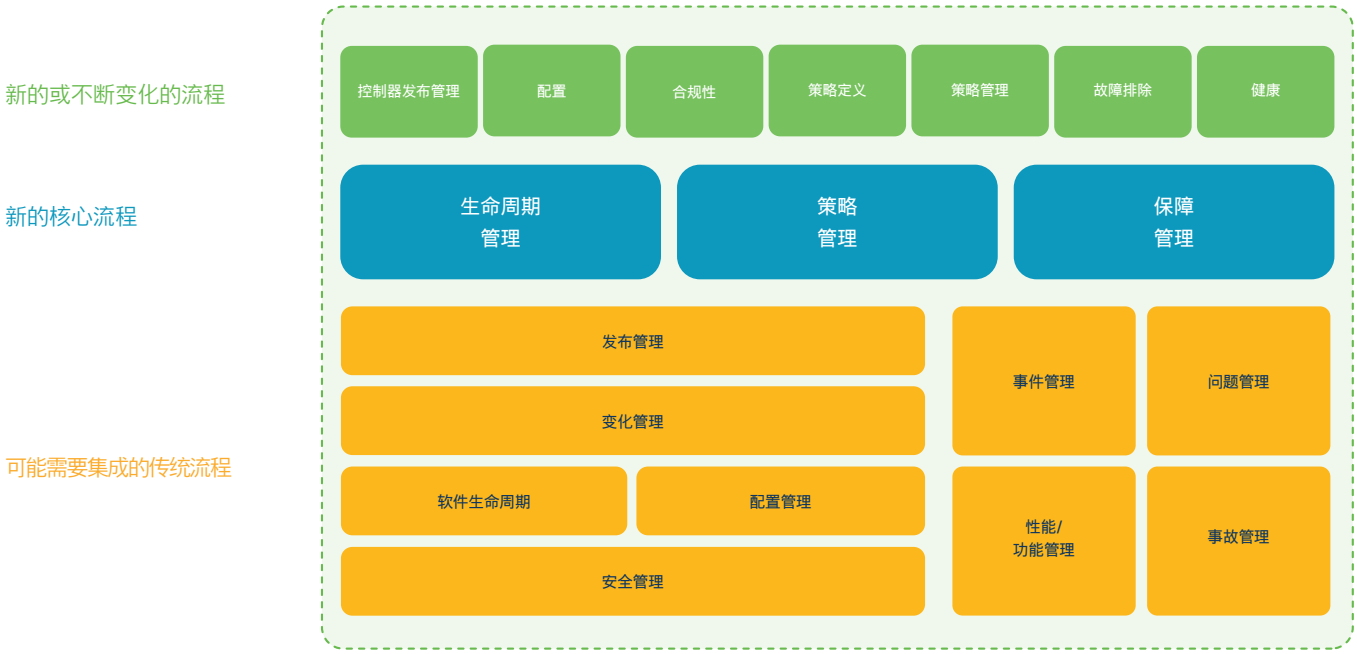


管理网络控制器的新思维

思科客户体验解决方案构架师Jake Hartinger认为，网络运营领域最为深刻的变化之一，将是关注点从设备转向控制器。到目前为止，网络管理员通常通过登录设备从网络提供并收集信息。

借助基于控制器的自动化和保障模式，管理员将侧重于管理控制器及与控制器相关的整合及流程。企业越能接受这种变化，就越能更快地提高服务质量、灵活性和安全性，并降低成本。[36]

图27 用于新型网络的新兴运营模式



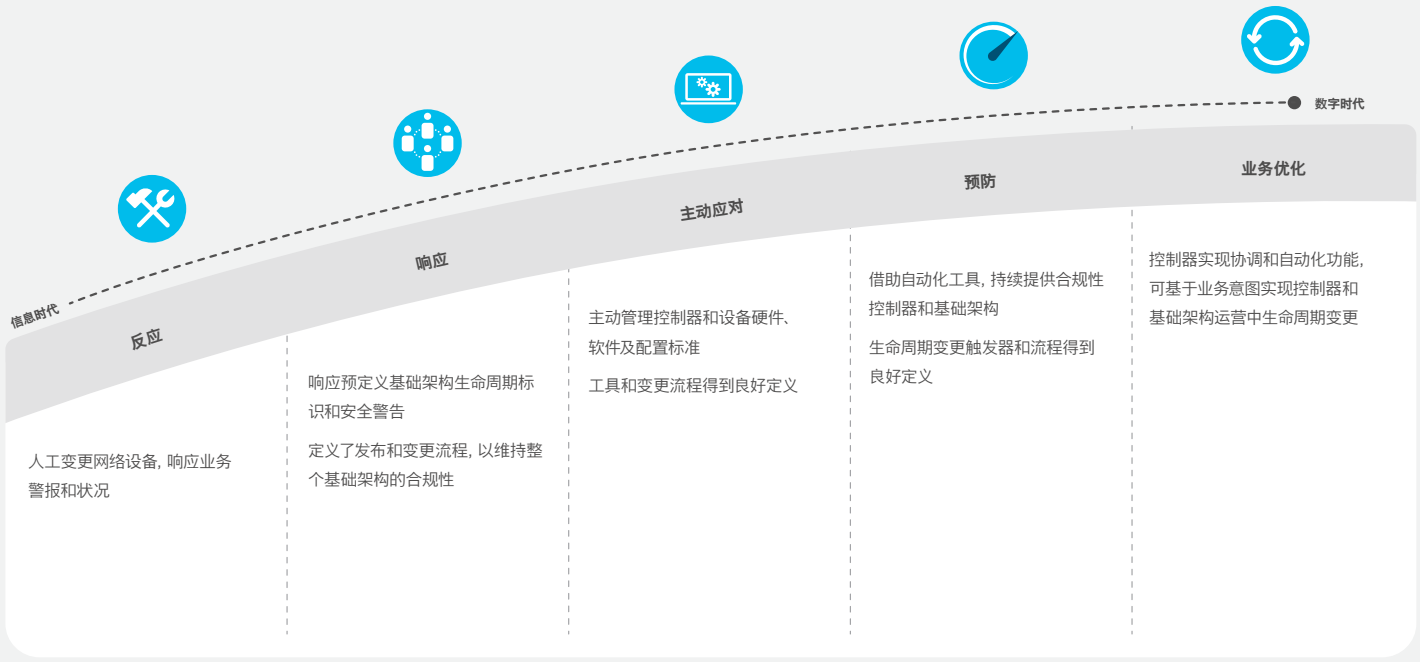
生命周期管理

向控制器主导的自动化和配置系统的转变要求更加严格地遵守硬件、软件和安全标准。更改命令行接口 (CLI) 的用户可能会发现，控制器会在后来的更新中覆盖此命令，这是因为它没有被定义为策略。

为避免这种情况，企业需围绕发布管理和变更管理建立明确的生命周期管理实践，尤其对于将网络或服务作为一个系统的自动化。

简言之，管理网络控制器涉及管理新控制器硬件、软件、集成点和API，以及用户界面配置 (其管理策略和保障功能)。在可预见的未来，控制器的功能会不断改变，因此为网络控制器和集成定义一个独特的生命管理流程是当务之急。

图28 网络运营就绪度: 生命周期管理

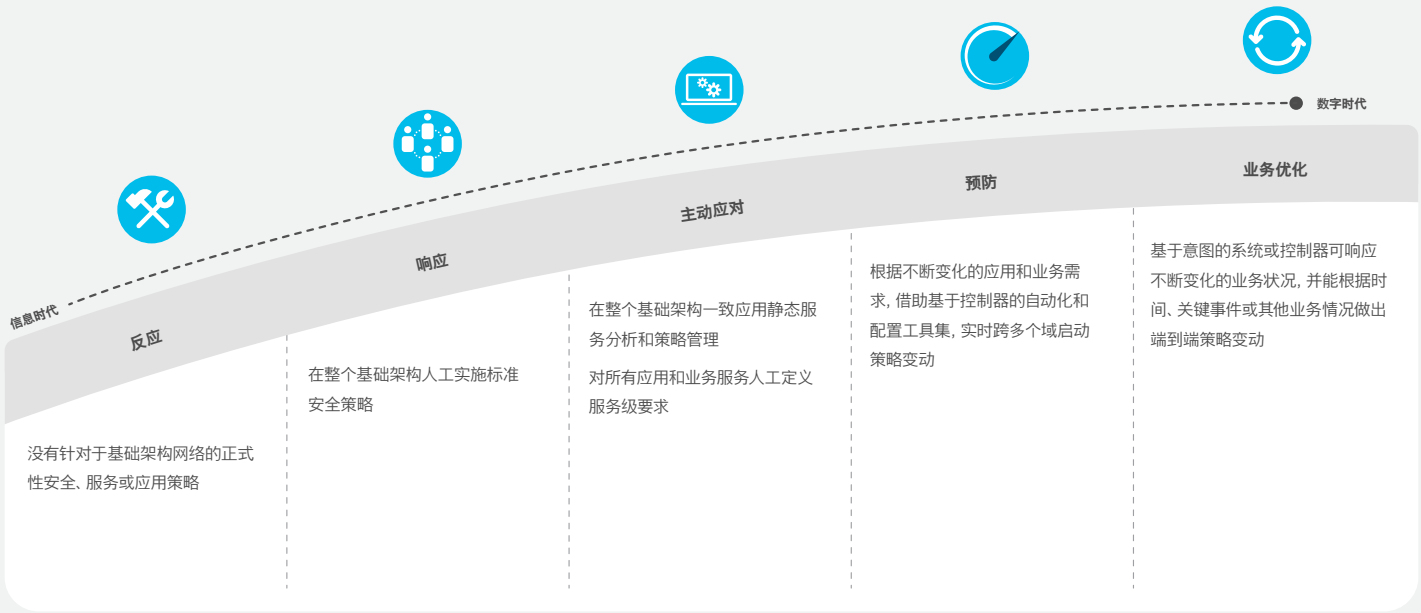


策略管理

要想取得成功并实现可持续性，对网络策略进行管理也十分重要。网络控制器将依赖于针对网络设备硬件、软件、配置，甚至集成的更为严格的标准和指南。必须首先定义策略，然后进行更新。同时，还必须在网络控制器内对其进行配置，以确保持续提供所定义的标准。另外，必须使用合规性验证方法对策略进行验证。

由于策略的更改会产生非常广泛的激活足迹，可能影响成千上万设备的配置，因此需要是规范性的，这样才能被测试和验证为有效并批准。最终，随着基于模型的策略验证模式（可在任何变化被激活前模拟它们）应用越来越普遍，配置选项将有更大的灵活性。

图29 网络运营就绪度: 策略管理



保障管理

小型网络易于人工管理，但对于大型网络，如果没有工具、网络数据和明确的流程，则难以管理。目前，仅有五分之一的运营团队能在影响服务的问题发生之前使用先进的分析对它们进行识别和补救。[14]

借助AI驱动的基于意图的网络模型，保障管理可改善这些资源，并将其与分析、API集成、关联能力、先进的清单和报告，及扩充进行整合。尤其是，分析和扩充可提供与网络故障相关的其他详细信息，有利于快速排故或改善网络健康状况。基于从大量其他部署获得的经验，预计AI驱动的系统将继续得以增强，运营团队也将继续获益。

在大型网络中，这将会使服务质量提高、问题快速解决、运营效率提升。AIOps团队可专注于过滤、扩充以及业务或服务管理系统API，以实现保障工作流程的完全自动化。

除这三个核心过程领域外，我们建议看一看与传统的ITSM流程、IT域和系统是否可以实现交互，以识别其他潜在的整合机会。

网络运营的未来——展望2025

思科客户体验CTO Rich Plane认为，在未来五年，网络运营团队会更有效地完成企业需要他们承担的任务。以下是他的预见。

1. **端到端的保障：** 网络运营团队可在任何客户（或设备）与任何业务服务（无论其托管在何处）之间，进行预测性问题检测和根本原因分析，并迅速确定网络是否是任何服务性能下降的原因，以及原因在哪里。

2. **连通业务与IT：** 网络运营将能够重新平衡关注点，把重点从几乎完全投入网络监控和问题排查，转到向外关注业务及网络如何最好地满足业务需求。运营的新使命是理解并将业务意图和应用需求转化为网络策略。

3. **NetOps和SecOps以单一可信来源开展运营：** NetOps和SecOps团队将开发集成且精简的工作流程，这通过数据分享及平台与工具间的自动切换和交互实现。

4. **NetOps将监控拓展到云：** 随着多云业务服务成为常态，NetOps团队将跨WAN、公共网络拓展可视性和预测性监控，并将其拓展到云接入点。对于更深入的洞察，企业IBN网络系统将开始把来自服务提供商的数据与云提供商系统融合，以确保云服务体验质量的连续性。

5. **基于模型的变化管理：** 更为先进的NetOps流程，如对网络上任何变化的假定分析，将扩展到数据中心之外，并越来越普遍。

6. **自我驱动、自我修复的工作流程：** 一些影响力稍逊的工作流程将实现全自动化，使网络可在无人类管理员干预的情况下自行采取补救措施，或进行生命周期管理。采用这种以数据驱动并以意图验证的方式，最大程度地减少了出错的几率，因而可获得更高水平的服务连续性。

2020全球网络趋势报告

网络人才趋势

现代网络需要的新技能

章节摘要

要点

- 新技术正在取代许多行业中大量人工完成的任务，IT行业也不例外。
- IT和网络行业的利好消息是，对于那些拥有当前所需新技能（如网络可编程性）的人而言，工作需求仍然旺盛。
- 随着网络运营越来越自动化，网络管理员的职责将是遵从网络生命周期、策略和保障相关的运营新规范。
- 网络策略师将承担以提高业务一致性、整合IT流程、提高安全性和更好地利用数据为目标的高价值职责。

关键调查结果

- 目前，网络维护任务平均占用了网络团队工作时间和资源的55%。
- 27%的IT领导者认为缺乏必要技能是向先进网络转变的主要障碍。
- 22%的IT领导者更愿意通过投资培训、继续教育和认证而提高技能。
- 网络策略师将AI、IT/OT集成、自动化和网络DevOps视为需提高技能的重要领域。

重要指南

策略师：考虑获取技术、业务和软件专业知识，使自己在以下一个或多个方向发展：

- 业务转化人员将专注于使IT性能符合动态的业务意图。
- 网络监护员将专注于连通网络和安全架构。
- 网络数据架构师将专注于利用网络分析和AI。
- 网络集成架构师将专注于跨网络与IT域的集成。

章节摘要 (续)

从业者: 积极主动获取技术与软件综合技能，使自己在以下一个或多个新兴领域发展:

- 网络负责人将专注于网络生命周期管理。
- 网络协调员将专注于策略的转化和自动化。
- 网络检测员将专注于服务保障和网络安全。

领导者: 考虑以下建议来构建未来的网络团队:

- 培育不断学习的文化氛围。
- 在再培训与雇用之间寻求平衡。
- 增加培训和研发投资。
- 进行人员轮换，提高业务敏锐性。
- 营造包容的工作环境。

高层前瞻

“到2025年，75%的网络团队会将不到三分之一的工作时间用于维持网络现状，而将三分之二的时间投入到创新和创造业务价值中去。”

——思科杰出工程师Joe Clarke

现代网络需要的新技能

未来两年，先进的网络技术将改变几乎每个网络岗位的职能。随着IT在业务转型中扮演更核心的角色，IT专业人员必须适应。

60%的业务领导者认为，IT是企业业务转型策略的引领者，但93%的高管认为，缺乏技能正导致他们难以足够快地转型。[34]

无论业务部门正在部署新的IoT应用、云服务，还是合规策略，IT专业人员都要清楚网络的需求及自己的职责，以便准时、安全地提供所需的网络服务。

在本报告的这一部分，我们将审视三类关键的IT人员——网络策略师、网络从业者和IT领导者——他们的角色是如何改变的，并确定这些专业人员为了管理快速变化的企业网络环境所需要的新技能。

IT领导者

- 全面的IT和网络监管
- 监督网络策略和预算

职务：CIO、IT基础设施副总裁、IT总监

网络策略师

- 负责制定网络策略、路线图、架构和技术偏好

职务：网络策略师、IT/网络架构师、网络经理

网络从业者

- 负责部署、配置、维护网络及排查网络故障

职务：网络工程师、网络管理员、网络支持工程师

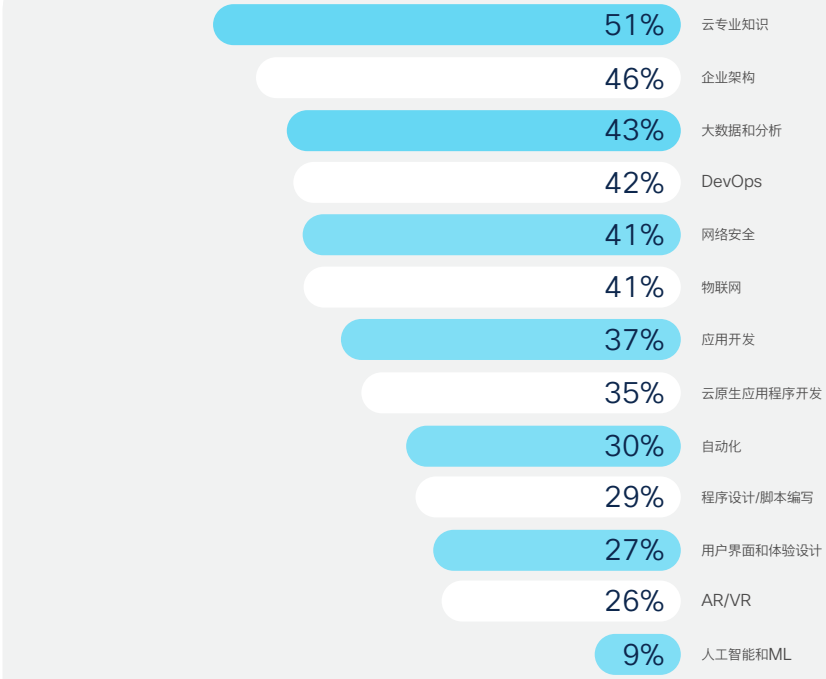
为正在改变的网络技能做好准备

如同企业网络的演变一样，构建和管理网络的技能也在变化，这不足为奇。在最近的两次调查中，IT领导者和网络策略师表示，他们在普通岗位和不那么普通的岗位上都看到了技能缺乏现象。

信息技术领域最为缺乏的技能

来自我们IT人才调查的数据表明，在整个IT领域，云专业知识、企业架构、大数据与分析、DevOps和网络安全等先进技术位居短缺技能和专业知识名单的前列。[34]顺便提一下，对位于技能缺乏前四位的领域（云、企业架构、数据分析和DevOps）的专业知识的需求为IT正在变化的职能提供了有力证据。

图30　最为短缺的IT技能



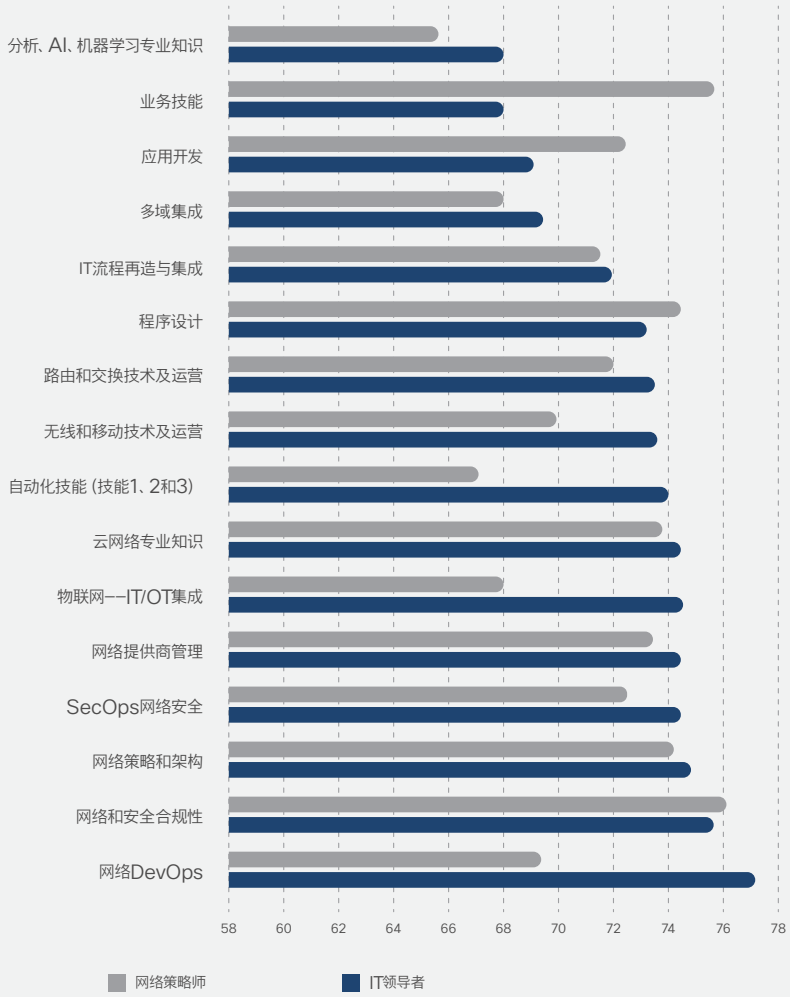
问题：您所在IT部门用于支持业务转型所需的最重要的技能或专业知识是什么？
来源：《下一代IT人才策略》，思科，2018年10月；n = 600位IT和公司高管

最为缺乏的网络技能

在我们的《*2019全球网络趋势调查*》中，我们请IT领导者和网络策略师评价他们团队在构建和维护满足其所在企业未来需求的网络方面的就绪度水平。

总体而言，这些领导者和策略师对他们网络团队的能力表现出相当程度的信心。IT领导者认为分析和AI，以及业务技能和应用程序开发技能最需要关注。尽管网络策略师也承认分析和AI技能的缺乏，但他们将IT/OT集成、自动化和网络DevOps看作需要提高的其他关键领域。[14]

图31　网络团队对不同技能就绪度的信心



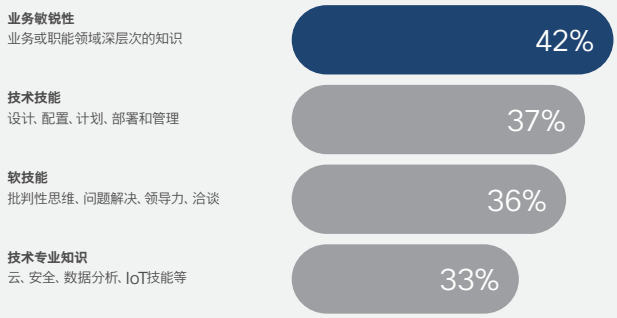
问题：想一想您网络团队当前的技能和能力，在构建和维护满足您所在企业未来需求的网络方面，您如何评价团队在以下各领域的就绪度水平？

来源：《*2019全球网络趋势调查*》；　n = 2061（505位IT领导者；1556位网络策略师）

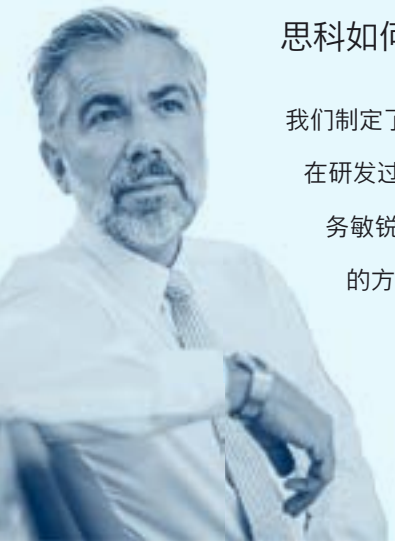
日益增长的业务和软件技能需求

我们的IT人才调查表明，缺乏业务敏锐性是IT业目前最短缺的技能。[34]由于企业正向基于意图的网络转变，因此填补这一缺乏至关重要。IT使用业务语言能够有效地将业务目标或意图转化为高水平的IT策略，从而可确定基础设施和设备配置。

图32 业务敏锐性被认为是最缺乏的技能



问题：业务转型需要但最短缺的IT技能和专业知识是什么？
来源：《下一代/T人才策略》，思科，2018年10月；n = 600位IT和公司高管



思科如何培养业务敏锐性

我们制定了“Customer Zero”计划，将IT专业人员投入研发。在研发过程中，他们可以培养批判性思维和深度解决问题等业务敏锐性和软件技能。这会激励员工以帮助我们保持竞争力的方式适应和转变。

跨领域职位在未来越来越重要

在不远的将来，一些IT职位会跨越不只一个领域。例如，额外掌握编程或数据分析能力的网络管理员，可填补新兴的职位，从而有效加大其贡献并提升其工作价值。

这些跨领域职位需要将分散的技术领域和基于语言的技能进行独特而受欢迎的结合。例如，从业者可使用API和编程语言为网络编程。再如，NetOps和SecOps合作，在两个团队间建立简单的运营工作流程。

“我们需要致力于设计、构建和运营任务关键型基础架构的网络和基础架构工程师。我们需要致力于编写创新应用程序（在基础架构上运行并使工作流程和任务自动化）的软件开发人员。最高效的企业会组建由软件和基础架构两个领域的专家组成的高效合作团队。”[37]

– 思科DevNet高级副总裁兼CTO Susie Wee

网络策略师的新职责

毫无疑问，对网络策略师而言，最紧要的工作是为更敏捷且与业务相符的网络架构制定高效而低风险的路线图。同时，策略师还需通过创建自助式网络服务目录、将网路与IT流程集成、整合NetOps和SecOps工作流程，及融合IT和运营技术（OT）来对IT进行优化。企业则需帮助筹划网络驱动的业务创新，如基于位置的个性化、工作场所利用优化，或远程专家应用程序。

未来的策略师: 提供超越网络的价值

思科杰出工程师Joe Clarke认为，网络策略师的岗位会越来越多地包含超出当前大多数策略师责任以外的职责。网络策略师的职责可能会按照以下一个或多个方向演变:

业务转化人员——专注于使IT性能符合业务意图:

转化人员致力于更好地将业务需求转化为可在网络上应用和监控的服务级别需求。同时，他们还将更好地将网络和网络数据用于业务价值和创新。

业务技能: 确定业务需求并将其转化为网络需求。

DevOps技能: 懂得网络平台API和自然语言处理（NLP）技术如何连通业务意图和IT。

网络集成架构师将专注于网络与IT域的集成:

集成人员致力于将网络融入IT流程并与外部系统整合。同时还负责网络域之间的整合，以确保向所有相关域传递意图。

IT流程重建与集成: 了解IT流程和工作流程，变更并集成网络运营以提高效率。

IT服务管理 (ITSM) 服务运营: 了解信息技术基础构架库 (ITIL) 流程，将网络保障系统高效链接至ITSM功能。

DevOps技能: 了解开放式网络平台提供的API，以及其如何使工作流程与其他IT系统集成。

网络监护员——专注于连通网络与安全架构:

网络监护员使网络的分布式智能成为安全架构和SecOps流程的一部分，并将在网络与安全的融合中扮演关键角色。

思科如何让员工不断学习知识与技能

我们围绕企业、安全、数据中心、服务提供商、合作、DevNet和其他高级主题建立了若干个学习IT知识与技能的途径，为工程师提供了发展前沿技能的机会。同时还为所有同事、专业人员和专家提供继续教育，并为员工提供免费或折扣培训和认证。

安全技能: 确定网络安全架构、部署网络安全技术、了解网络在促进整体安全方面所起的作用。

DevOps技能: 了解网络平台API如何实现与SecOps系统的集成。

网络数据架构师——专注于利用网络分析和AI:

网络数据架构师致力于更好地利用网络上的大量数据和新兴的AI驱动工具提高IT服务并通知业务。

分析和AI技能: 收集数据以便更快做出更好的决策。了解AI技术，以及如何将它们用于网络保障、如何将它们与其他IT系统集成，以实现全面的服务保障。

业务洞察技能: 了解业务，及其如何使用网上获得的数据提供决策并创造新机会。

网络从业者的新职责

随着数字化转型成为企业战略的核心，网络从业者需将重点从重复性管理工作转移至支持业务目标的增值服务。由于先进网络自动化水平的不断提高，IT工程师所做的更为耗时的工作开始被取代，因此更容易做到这一点。

> “如今，成功的网络工程师善于将新技术与传统技术相结合，并消除网络与软件开发间的隔阂。这要求既具备DevOps思维，也要对技术如何与业务目标结合有更好的理解。”
>
> ––思科杰出工程师Joe Clarke

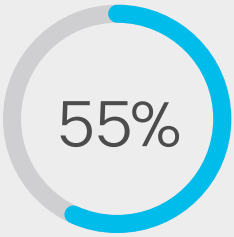
未来的网络工程师: 提供超越连接性的价值

随着基于意图的网络越来越盛行，网络从业者的职责不断发展，转变为支持一个或多个网络运营支柱: 生命周期、流程或保障。在这种情况下，网络从业者需培养承担其中一种或多种潜在职责的技能:

网络负责人––专注于网络生命周期管理:

网络负责人掌管确保网络控制器和底层网络全面健康并持续运营的流程和实践。

> **所需技能:** 在基于意图的网络环境中运行、维护和调整提供自动化和协调的控制器，确保平台与其他系统集成的可持续性。了解这些控制器的生命周期，并确保控制器和底层网络的持续健康、安全、合规及稳定。



目前，重复性管理工作可占用网络从业者55%的工作时间和资源。[14]

网络协调员——专注于策略转化和自动化：

协调员需懂得业务需求如何转化为网络策略，及如何管理这些策略的自动化，还要负责策略与其他网络和IT域的相符性。

> **所需技能：**掌握如何利用基础架构自动化工具、自动化协议和数据模型。熟练使用Linux、Python和网络可编程开发工具。了解常用数据格式，熟悉灵活的软件开发方法，娴熟使用API和工具包与网络控制器和设备交互。

网络检测员——专注于网络和服务保障：

网络检测员应擅长使用和调整依赖先进分析和AI的网络保障工具，确保网络提供承诺的业务意图，同时需与IT服务管理流程整合，并与SecOps团队密切合作，标记网络异常，堵住潜在的安全漏洞。

> **所需技能：**根据AI驱动的洞察识别并按优先次序排列趋势，以便企业主动采取措施。整理反馈并将其提供给分析系统，以不断改善异常检测和补救。将网络问题检测和解决流程与IT和安全流程整合。

IT领导者：采取措施弥补网络人才的缺乏

现在掌握技术技能是未来成功实现数字转型的关键。在我们的*《2019全球网络趋势调查》*中，我们邀请IT领导者分享他们目前的人才培养之道。再培训、扩大人才库和调整投入方向是三大举措。

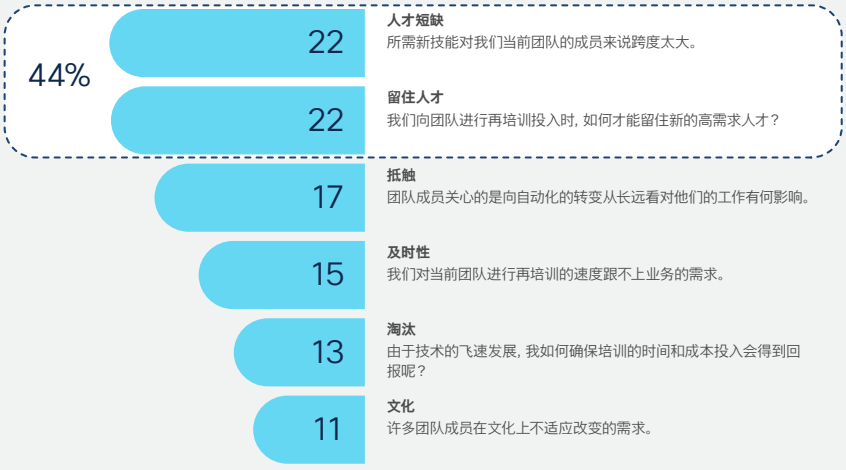
图33 解决网络技能缺乏的首选举措

问题：解决当前在规划、部署和维护未来网络需求方面所需人才的短缺问题时，您所在企业的IT领导层应优先采用的主要措施是什么？

来源：*《2019全球网络趋势调查》*； n = 505位IT领导者

尽管领导者对再培训有所顾虑，但其仍是提高IT业务技能和IT技术技能的首选方式。

图34 最受关注的再培训问题



问题：当您考虑对您所在企业的网络团队进行再培训、以更好地构建和支持更先进的网络时，您最关注的是什么？

来源：*《2019全球网络趋势调查》*； n = 505位IT领导者

对IT领导者如何构建未来网络团队的建议

思科客户转型高级副总裁Guillermo Diaz认为，以下五个策略能帮助IT领导者构建可推动数字化转型业务的网络团队。

1. **培育不断学习的文化氛围：** IT领导者培育不断学习的文化氛围是绝对必要的。这样可帮助网络从业者和策略师定期掌握他们适应新技术和运营流程所需的技能。要内外结合，为团队提供各种教育、体验和参与的机会。

2. **在再培训与雇用之间寻求平衡：** 我们的研究表明，领导者正日益依赖再培训来解决技能缺乏问题，但对新技术而言，情况可能正好相反。许多企业正为新兴技术岗位招募新人才，尤其是与AI和ML相关的岗位。在培养和雇用之间找到正确的平衡取决于业务和运营的目标，以及网络转型的时期。

> “再培训比向外部市场招聘新专业人员更节省成本，不仅在工资和招募费用方面，在新员工培训成本、传授企业隐性知识和流程熟悉方面也是如此。现有人员可能缺乏某些新技能和能力，但他们可能有不少让你占得先机的东西。”[38]
>
> – 思科欧洲、中东和俄罗斯CIO Colin Seward

3. **向培训和研发增加投入：** 在近来对IT领导者的调查中，我们发现，数字化转型更为成功的企业在IT工作人员培训和培养方面投入了近10%以上的资金。[34]如果IT能跟上技术发展的步伐，就能做出更快、更明智、更好的以数据驱动的决策，为实现业务目标提供支持。

满足新需求: 思科扩大认证套件

为帮助应对这些新的培训需求，网络课程和认证（如思科提供的课程和认证）正迅速更新。[37]

4 **进行人员轮换，提高业务敏锐性：**通过短期轮换，让IT人员和业务人员交换岗位可增进了解、扩大认知范围，这样可在以后实现更有效的互动。具体而言，轮换网络、应用程序和业务岗位可带来技术、可编程性和业务敏锐性的综合技能。

5 **营造包容的工作环境：**以上建议着重于人才。营造高度包容的工作环境意味着让人才尽情施展才能。在招聘、管理、发展和奖励员工方面，注重多样性和包容性的公司，其发展要好于未这样做的竞争对手。行政领导层要带头营造包容性企业环境，并致力于为实现这样的环境创造条件的行为规范、计划、政策和培训。下一代IT企业在其日常运营中必需践行多样包容的文化。

思科如何吸引新人才

找到优秀人才并非偶然。正因此，我们通过我们的IT大学、思科网络学院及思科国际实习生项目发现和雇用新人才，并通过思科退伍军人计划帮助我们培训和雇用对技术职业感兴趣的退伍军人。

关于本报告

*《2020全球网络趋势报告》*为IT领导者、策略师和从业者提供了对企业当前和未来网络趋势的洞察，并提供了针对网络技术、运营和人才的重要指南。本报告基于思科原创研究，并引用了*《2019全球网络趋势调查》*（对13个国家2061位IT领导者所做的调查）中的新数据。此外，思科的部门领导、研究员和杰出工程师也为向先进网络技术转型的企业提供了专家分析和建议。

谨以本报告给Cliff Apsey先生，他向客户交付最佳数字体验的热忱激励着我们让本报告为您带来良好体验。感谢Cliff与我们共事，我们将永远怀念他。

资料来源

1. *IDC FutureScape: Worldwide Enterprise Infrastructure 2018 Predictions*, IDC, 2017.
2. *Uptime Institute Annual Data Center Survey*, 2019.
3. *2018 Cisco Complete VNI Forecast, Cisco, 2018.*
4. *Cisco 2018 Annual Cybersecurity Report, Cisco, 2018.*
5. "J.C.R. Licklider," Internet Hall of Fame, 2013.
6. "History of Online Education," The Quad, 2019.
7. *IDC Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023*, IDC, May 2019.
8. Dennis Smith, Dale Kutnick, Lisa Pierce, Invest in Networks to Achieve Digital Business Success, Gartner, May 2019
9. "A Brief History of Globalization," World Economic Forum, January 2019.
10. *Digital Vortex 2019: Continuous and Connected Change, IMD, 2019.*
11. *Reshaping the Future* (automation use case survey), Capgemini Research Institute, 2018.
12. "VNI Forecast Highlights Tool," Cisco, 2017.
13. *Cisco Visual Networking Index: Forecast and Trends, 2017–2022 (white paper), Cisco, February 2019.*
14. *2019 Global Networking Trends Survey, Cisco, 2019.*
15. Jonathan Forest, Neil Rickard, 2019 Strategic Roadmap for Networking, Gartner, 10 April 2019
16. *Distinguishing Intent, Policy, and Service Models*, IETF, May 3, 2018.
17. "Why Is Intent-Based Networking Good News for Software-Defined Networking?" Cisco, June 1, 2018.
18. *Intent-Based Networking: Building the Bridge Between Business and IT, Cisco, January 2018.*
19. *Intent-Based Networking: Evolution of the Enterprise Campus Network*, IDC, June 2018.
20. "Enterprises Cannot Have Automation Commitment Issues and Be Successful," IT Connection, July 21, 2017.
21. "The Rise of AIOps: How Data, Machine Learning, and AI Will Transform Performance Monitoring," AppDynamics, December 17, 2018.
22. "Network Assurance with Machine Reasoning and Machine Learning," Cisco, July 25, 2019.
23. *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 (white paper), Cisco, November 19, 2018.*
24. "2019 Predictions: For Infrastructure," Cisco, February 11, 2019.
25. *Multicloud Is the New Normal*, IDC, March 2018.
26. *SD-WAN: Security, Application Experience and Operational Simplicity Drive Market Growth, IDC, April 2019.*
27. "Connecting the Unconnected: 5G and Wi-Fi 6 Will Play a Pivotal Role in Bridging the Digital Divide," Cisco, March 19, 2019.
28. "OpenRoaming: Automatic and Seamless Roaming Across Wi-Fi 6 and 5G," Cisco, April 29, 2019.
29. *The Zero Trust eXtended Ecosystem: Networks*, Forrester, January 2, 2019.
30. *Anticipating the Unknowns: Chief Information Security Officer Benchmark Study, Cisco, March 2019.*

31. Sanjit Ganguli, Lawrence Orans, Align NetOps and SecOps Tool Objectives With Shared Use Cases, Gartner, 24 July 2018
32. *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, CISA, April 16, 2018.*
33. "Cisco Cybersecurity Report Series," Cisco, 2019.
34. *Next-Generation IT Talent Strategies, Cisco, October 2018.*
35. *Transforming IT Operations, Cisco Connected Futures, 2018.*
36. *Next-Generation Network Operations, Cisco, September 2019.*
37. "Bringing Software Practices and Software Skills to Networking with Cisco Certifications and DevNet," Cisco, June 10, 2019.
38. *Evolving the IT Team, Cisco, 2019.*