思科软件定义的接入 (SD-Access)

步入崭新的网络新时代。网络·全智慧

如今，策略维护工作的难度不断加大，配置流程也变得越来越复杂。随着用户和终端数量持续增长，网络分段变得愈发困难。通常，IT 会对有线和无线网络制定互相独立的用户策略，而且在进行故障排除时无法找到具体的用户。用户越多，策略越多，复杂性必然会随之增加。因此，您需要一种以体验为基础，能够将情景转化为情报的网络，一种响应速度更快、更为人性化的网络：网络·全智慧。

如果您能为 IT 节省更多时间，结果会怎样？如果您能在几分钟内为任何用户或任何设备提供对任何应用的网络访问权限，而且丝毫不会影响安全性，结果又会怎样？借助我们提供的业内首个全面涵盖从网络边缘到云的策略型自动化接入解决方案，您可以获得所有这些优势。思科® 软件定义的接入 (SD-Access) 可以为您的全数字化网络奠定坚实基础。它采用了思科全数字化网络架构（思科 DNA™）的设计理念，是业内首个涵盖从边缘到云的策略型自动化接入解决方案。SD-Access 可提供端到端的网络分段，确保您无需重新设计网络，即可将用户、设备和应用流量分离。它可以自动实施用户访问策略，因此组织可以确保为网络中访问任何应用的任何用户或设备设置正确的策略。所有操作都由单一网络交换矩阵执行，以确保在不影响安全性的情况下，为任何位置的用户提供一致的用户体验。这意味着局域网、广域网和云将采用共同的用户策略。

优势

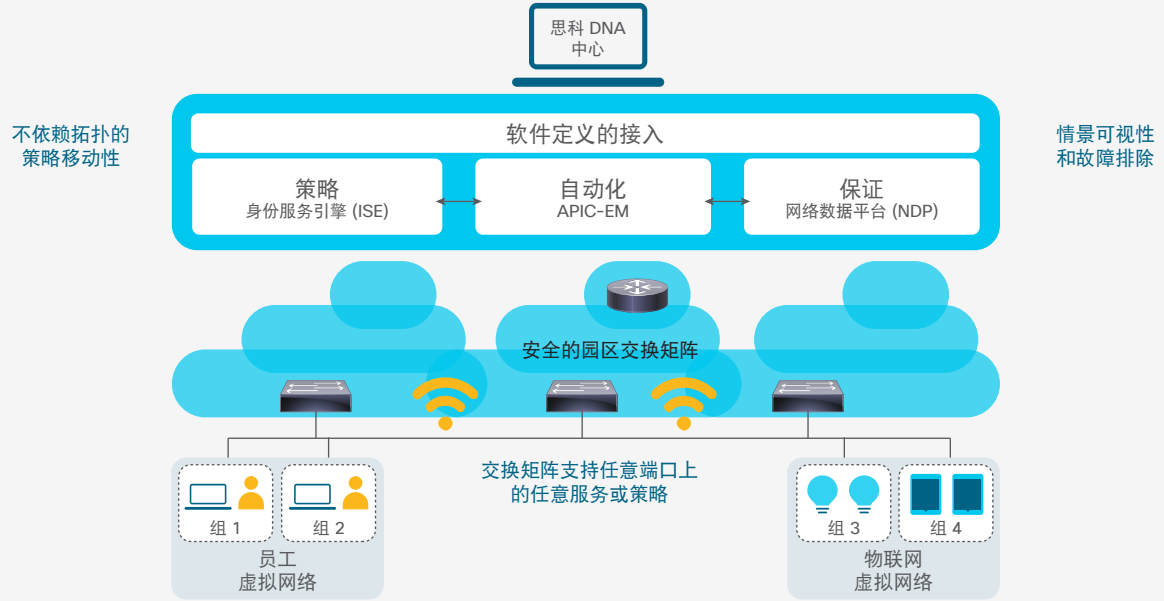
- 从边缘到云端**实现基于策略的自动化网络调配**
- 通过在整个服务生态系统中使用统包自动化解决方案和开放式 API，**快速提供服务**
- **获得对整个网络的可视性**，将有线网络、无线网络和广域网作为单一实体进行管理
- 在现有基础设施之上进行构建，不仅可以提高效率，而且能**降低运营成本**

思科优势

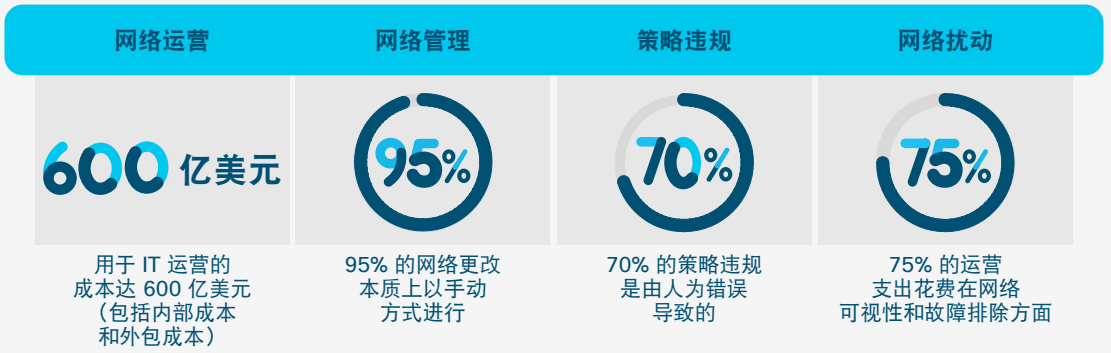
为什么需要采用 SD-Access？因为网络管理如今面临许多挑战，只有克服这些挑战，才能实现业务成果。而这些挑战的根源在于手动配置流程和相互独立的工具所固有的局限性。SD-Access 的优势在于：

- 为您提供革命性的管理解决方案，在降低运营成本的同时，提高业务灵活性
- 以一致的方式管理有线和无线网络的调配及策略实施
- 自动执行网络分段和基于组的策略
- 提供基于情景的洞察力，从而加快问题解决和容量规划的速度
- 采用开放式可编程接口，可与各种第三方解决方案实现集成

图 1. SD-Access 和全数字化网络架构



挑战



解决方案 – SD-Access

思科通过开发推动转型所需的重要技术，不断努力解决企业 IT 部门面临的主要挑战。

要了解 SD-Access 的根本优势，要了解该解决方案的基本原理和功能两个方面，这非常重要。

表 1. IT 转型目标（总结了 IT 的一些重要优先事项）

IT 优先诉求	网络基础设施要求
运营效益： ▪ 网络自动化 ▪ 网络保证 ▪ 网络融合 ▪ 与“云优先”战略保持一致	▪ 一致且基于标准的 API ▪ 策略自动化（安装和调配） ▪ 网络虚拟化和分段 ▪ 恢复能力、可扩展性和高可用性 ▪ 云连接安全
改善员工体验 ▪ 协作 ▪ 自带设备 (BYOD) 和移动性	▪ 智能流量工程（基于应用） ▪ 应用可视性与可控性、动态服务质量 (QoS) ▪ 网络访问控制和移动设备管理 (MDM) ▪ 网络虚拟化和分段
安全性和合规性	▪ 威胁可视性和基于身份验证的网络访问 ▪ 基于角色的内部网络分段 ▪ 动态服务插入

在网络部署和运营方面，都存在着根深蒂固的挑战：

网络部署

- **设置或部署单个网络交换机可能需要几个小时：**造成这个问题的原因是 IT 需要制定计划，或与不同的基础设施团队进行合作。在某些情况下，部署一批交换机可能需要数周时间。
- **安全性问题：**安全性是现代网络管理中的关键因素。为了实时响应各种需求，组织需要有效地实施变更。与此同时，组织需要以适当的方式保护资源。不过，要通过跟踪 VLAN、访问控制列表 (ACL) 和 IP 地址来确保策略和安全合规性达到最佳状态，可能是一项艰巨的任务。
- **分散的网络：**这个问题在组织中十分常见，因为不同的系统往往由不同的部门来管理。通常情况下，建筑物管理系统、安全系统和其他生产系统都会独立于主 IT 网络独立运行。这就造成了网络硬件重复采购以及管理措施不一致等问题。

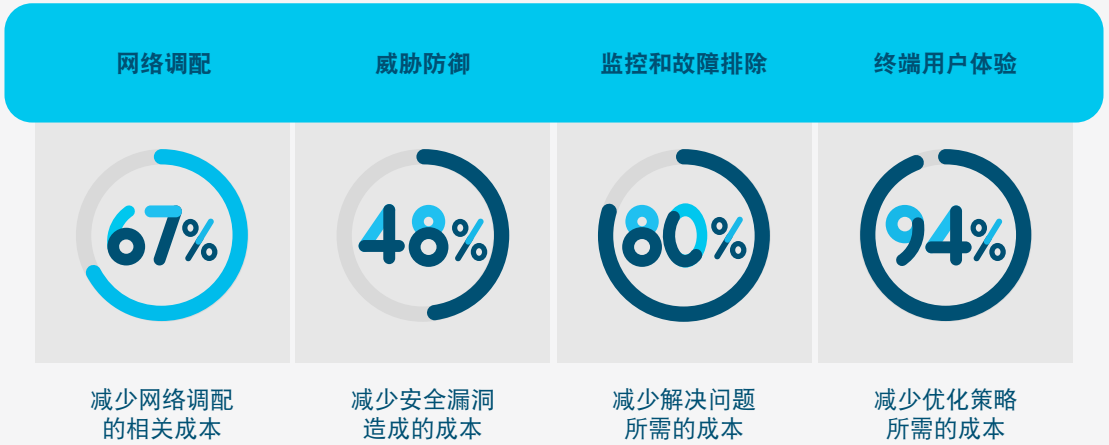
Cisco Capital

提供融资服务，助您实现目标

Cisco Capital® 可帮助您获得所需的技术来实现目标并保持竞争力。帮助您减少资本支出，加速业务发展，并优化投资和投资回报。借助 Cisco Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。Cisco Capital 可以为您提供一种可预测的支付方式。Cisco Capital 现已在 100 多个国家/地区推出。了解详情。

网络运营

- **变更管理受限：**对网络运营而言，定期升级软件和配置是一项基本的例行活动。但是，在典型的网络中进行此类更改时，仅物流工作就需要 6 个月以上的时间。
- **工作效率低下：**如今，每家企业都在努力提供高质量的通信体验，以期提高员工的工作效率。但是在当前模式下，这项工作一直困难重重，费时费力。经验表明，改善服务质量可能需要数月时间进行规划和实施，而且如果实施过程中出现欠缺，还会导致业务关键应用出现性能问题。
- **问题解决缓慢：**在当前的网络管理模式下，网络不仅规模庞大，而且极其复杂。因此一旦出现故障，很可能需要投入大量的时间和精力来查明并解决问题。网络中可能还存在大量未正确关联的数据。这样，IT 就无法利用这些数据来了解网络情景和用户行为。



服务

通过思科软件定义的接入服务加快向全数字化就绪型网络迁移的步伐

思科服务可以为您提供专家指导，帮助您以更低的成本跨有线和无线环境创建更简单的运营模式。凭借可靠的经验、最佳实践和创新的工具，思科服务可协助您轻松管理、扩展和保护您的 SD-Access 解决方案。通过选择全面的生命周期服务（包括咨询、实施、优化和技术服务），您可以毫不费力且信心十足地迁移到安全且自动化的统一网络。了解详情。

- 制定与业务需求相符的 SD-Access 架构战略和规划图
- 通过迁移获得高性能、安全性和可靠性
- 通过优化实现卓越运营
- 保持可靠性，并加速 SD-Access 解决方案的投资回报
- 通过主动监控和管理减少网络中断
- 向您的 IT 员工传授知识并开展培训

基本概念

思科 SD-Access 旨在通过提高运营效率、改善员工体验，以及增强安全性与合规性来推动 IT 转型。构建这种下一代解决方案涉及一些关键的基本要素，包括：

- 基于控制器的协调器
- 网络交换矩阵
- 可编程的交换机

基于控制器的网络：传统网络需要按设备实施管理。这不仅需要大量时间，而且会产生许多复杂问题。而且，这种方法很容易出现人为错误。SD-Access 使用现代控制器架构，通过对网络元素进行协调和操作来促进实现业务目标。它能够在用户、设备和终端连接到网络时，立即配置与之相关的设备和策略。在这个过程中，控制器会提供一个网络抽象层，用于对各种网络元素的特性进行仲裁。如果使用思科 DNA 控制器，还可以连接到基于北向具象状态传输 (REST) 的 API，这有助于第三方或企业内部在网络中开发有意义的服务。

网络交换矩阵：设计好控制器要素后，下一步就要考虑在逻辑块（即交换矩阵）中构建网络。在 SD-Access 中，交换矩阵是设备的逻辑组，可作为单一实体在一个或多个位置进行管理。构建交换矩阵有助于实现多种功能，例如创建虚拟网络和用户及设备组、SD-WAN 集成和高级报告。不仅如此，交换矩阵还能提供用于应用识别、流量分析、流量优先级和流量控制的智能服务，从而帮助实现最佳性能和运营效益。

现代设备软件堆叠：为了构建现代化基础设施，思科将各种高级功能集成到已经推出和即将推出的交换机产品，以实现开放、基于标准和可扩展的完整生命周期管理。这些重要技术包括 (1) 自动化设备调配（用于支持各种广为人知的功能，如零接触调配、即插即用和预启动执行环境等）；(2) 开放式 API 接口（用于支持 NETCONF 和 YANG 模型）；(3) 精细可视性（用于支持 NetFlow 和 YANG 操作模型等遥测功能）；以及 (4) 通过实时软件补丁实现无缝软件升级。

特色功能

网络设计和部署：构建网络的第一步是安装设备和构建基础设施，以便为企业提供支持。思科 DNA 中心为网络架构师或管理员提供了一个设计中心，除了可以用于设计网络外，还能为相关设备生成配置命令。客户可以利用经过全面测试和认证的思科验证设计来满足各种部署需求和规模要求。

解决方案组件

SD-Access 采用行业领先的软件和硬件组件构建而成。

核心组成部分包括：

- 应用策略基础设施控制器企业模块 (APIC-EM) 2.0 版（包括思科 DNA 中心）
- 身份服务引擎 (ISE)
- 网络数据平台
- 网络设备：详见表 2

网络分段：许多大中型企业希望将多个网络整合到一个管理平面，并按照业务部门或职能板块对网络进行分段。利用 SD-Access 即可实现这一目标。

灵活的身份验证选项：设备和用户需要通过各种不同的身份验证方案安全地连接到企业网络。SD-Access 可提供灵活的身份验证选项，包括 802.1X、Active Directory 和静态身份验证方案。

基于组的策略：在传统网络中实现策略可能非常复杂。因此，不受 IP 地址或 VLAN 成员关系限制为用户或设备分组的功能至关重要。如果能实现这一点，就能从思科 DNA 中心策略屏幕创建策略，来描述各个组之间如何进行交互。SD-Access 使用行业领先且久经验证的思科 TrustSec® 技术，可在整个企业范围内实现这一功能。

网络保证：网络中断和用户连接问题会严重影响企业的收入和工作效率。企业必须能预测问题并采取主动的预防措施；当问题出现时，要能迅速将其解决。思科 DNA 中心保证功能可从网络中的多个来源（例如系统日志和 NetFlow）收集数据，对用户和网络活动提供基于情景的见解。

表 2. 支持的设备平台一览表（包括网络角色）

	接入	边界
非软件化	思科 Catalyst® 9300 系列 思科 Catalyst 3850 系列 Catalyst 3650 系列 第二代 802.11 无线接入点：思科 Aironet® 1800、2800 和 3800 系列 思科 5520 和 8540 无线控制器	思科 Catalyst 9500 系列 思科 Catalyst 3850 系列（10G 型号） 思科 Catalyst 4500-X 系列 思科 4000 系列集成多业务路由器 思科 ASR 1000 系列汇聚多业务路由器
软件化	思科 Catalyst 9400 系列（管理引擎 1） 思科 Catalyst 4500E 系列（管理引擎 8E、9E）	思科 Catalyst 9400 系列（管理引擎 1-XL） 思科 Catalyst 6807-XL（管理引擎 6T、2T） 思科 Catalyst 6500 系列 思科 Catalyst 6880-X 思科 Catalyst 6840-X 思科 Nexus® 7700（仅提供管理引擎 2E 和 M3 线卡）

SD-Access 使用案例

SD-Access 采用行业领先的功能构建而成，适用于各种促进企业发展的主要使用案例，帮助企业真正实现全数字化承诺，并降低总拥有成本（表 3）。

表 3. SD-Access 使用案例

使用案例	详细信息	优势
安全和分段	▪ 通过 802.1X、Active Directory 和静态身份验证实现用户自行注册 ▪ 通过思科 TrustSec（安全组标签）实现用户分组 ▪ 自动执行虚拟路由和转发 (VRF) 配置（业务板块、部门等）	▪ 减少调配网络分段和用户组所需的时间 ▪ 为实施网络安全策略提供基础
用户移动性	▪ 实现有线用户和无线用户的单点定义 ▪ 在有线网络和无线网络之间无缝漫游	▪ 利用单一界面（思科 DNA 中心）管理有线网络、无线网络和用户 ▪ 将无线数据路径分流到网络交换机（减少控制器上的负载）
访客接入	▪ 为访客用户定义专门的组 ▪ 创建访客用户的资源访问策略（例如互联网访问策略）	▪ 简化策略调配 ▪ 节省策略调配时间
物联网集成	▪ 对物联网设备进行分段和分组 ▪ 为物联网组定义接入和管理策略 ▪ 通过灵活的身份验证选项执行设备分析	▪ 简化物联网设备的部署 ▪ 通过设备分段减少网络的受攻击面
监控和故障排除	▪ 从多个数据点（如系统日志、统计信息等）收集网络行为数据 ▪ 针对每个用户和设备提供情景数据	▪ 显著缩短故障排除时间 ▪ 丰富的情景和分析方便决策

如何熟悉并使用 SD-Access

- 查看业务和技术决策者演示文稿
- 阅读 SD-Access 技术解决方案白皮书
- 联系销售代表，安排产品演示
- 通过 http://cisco.com/go/sd-access/tco 获得快速的总有用成本分析

使用案例	详细信息	优势
云集成	• 管理用户的应用访问策略 • 与思科云解决方案全面集成	• 管理员可从单一界面定义用户的应用访问策略 • 对整个企业进行端到端的策略管理
分支机构集成	• 创建涵盖多个区域性分支机构位置的单一交换矩阵 • 利用思科路由器作为交换矩阵边界节点	• 简化分支机构位置的调配和管理 • 企业范围的策略调配和实施

C22-739012-00 06/17