RESEARCH
社交媒体的影响与见解

2020 年 3 月

统一的有线和无线接入边缘是

影响业务的关键因素

白 皮 书

作者
Zeus Kerravala

ZK Research
Kerravala Consulting
附属公司

统一的有线和无线接入边缘是影响业务的关键因素

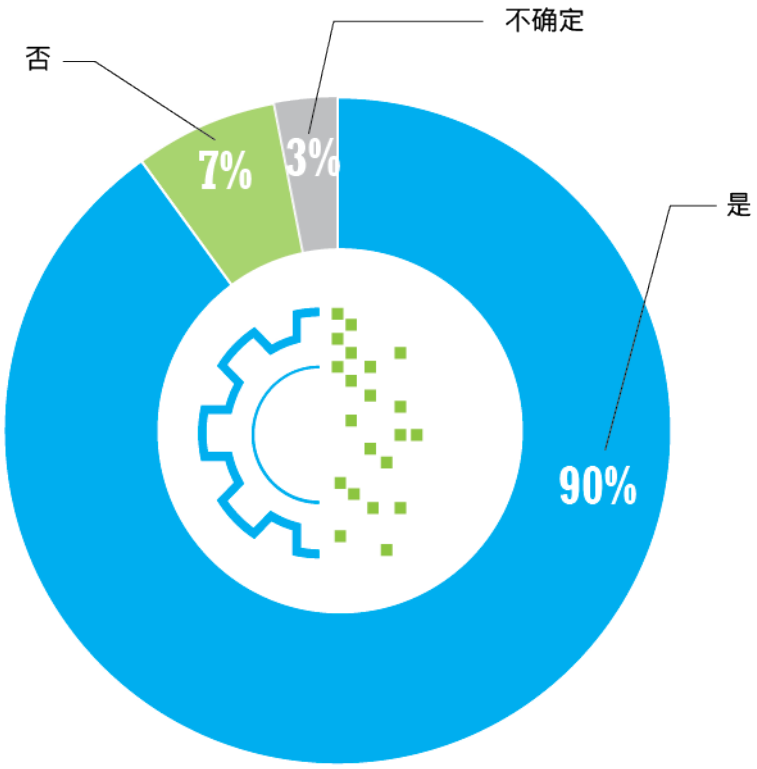
序言：接入边缘是全数字化转型取得成功的关键

全数字化业务时代已经来临，并且正在以前所未有的速度改变业务形势。大胆接受全数字化转型的企业获利越来越多，迅速成为市场领导者；而那些不敢尝试的企业则日渐衰落，逐渐失去影响力，因此，全数字化转型已成为几乎每一位 IT 和企业领导者的当务之急。ZK Research 的 “2019 年 IT 工作重点调查” (2019 IT Priorities Survey) 发现，90% 的企业目前正在开展全数字化转型计划（图 1），相比 2017 年的 84% 有所增加。

在全数字化业务时代，保持市场领先地位的关键不再关乎拥有最好的产品、最优惠的价格或最杰出的人才，而在于必须能够对市场转型了如指掌，且能够比竞争对手更快地利用这些转型机会。

图 1：全数字化转型已几乎无处不在

您的组织目前是否正在实施全数字化转型计划？



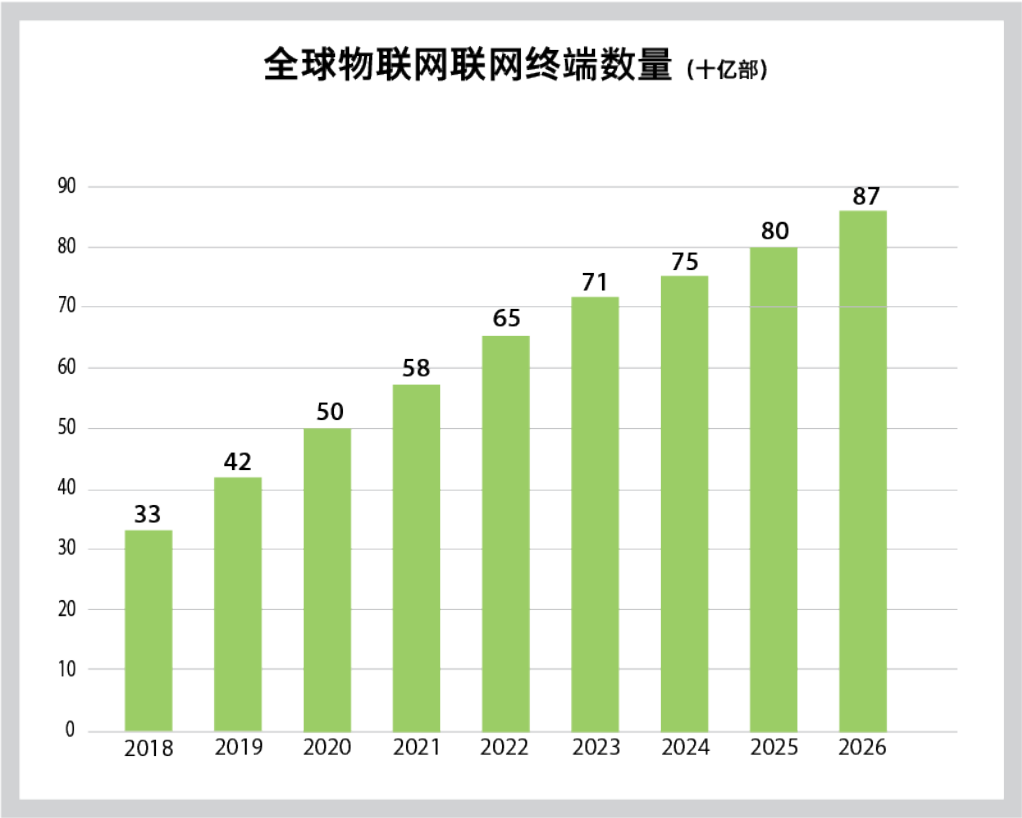
来源：ZK Research，“2019 年 IT 工作重点调查” (2019 IT Priorities Survey)

在向全数字化企业转型的过程中，关键的一步是成为敏捷性组织。为此，组织必须拥有能够根据需要灵活调整的动态 IT 基础设施。但是难题在于，组织的敏捷性受制于其最不敏捷的 IT 组件，而如今的组织敏捷性最差的 IT 组件就是网络，尤其是接入边缘。软件定义网络 (SDN) 的出现推动了数据中心转型，软件定义广域网 (SD-WAN) 则促进了广域网的现代化，但接入边缘仍几十年不变。

从历史上看，网络边缘一直被视为无足轻重。它用于将员工计算机、打印机和其他各种设备连接至主网络，但大多数用户数据和应用均位于计算机上。网络用于定期获取新信息或支持 “尽力而为” 的服务（例如邮件）。在这种情况下，因为接入边缘只起到基础连接的作用，所以被认为价值不大。如今，接入边缘的作用已与以前截然不同，应被视为影响业务的关键因素。以下是推动接入边缘价值增长的一些主要因素:

- **几乎所有应用都需要联网。**如果应用和数据位于用户工作站上，则即使网络性能不佳，也不会影响其工作效率。如今，越来越多的应用已迁移至数据中心、私有云、公共云和其他位置。这意味着网络边缘的质量和可靠性会直接影响应用性能。ZK Research 预测，在三年内，74% 的业务应用将驻留于公共云或私有云中，促使网络边缘的价值进一步提升。
- **物联网 (IoT) 现已成为主流。**物联网已不再只是适用于少数垂直行业的运营技术 (OT)，而已成为各行各业大多数企业全数字化转型战略的核心要素。随着物联网日益普及，联网终端的数量也将与日俱增。ZK Research “2019 年物联网设备预测” (2019 IoT Device Forecast) 预计，到 2026 年，联网的物联网终端数量将达到 870 亿部（图 2）。几乎所有这些设备均连接到网络边缘，因此边缘问题可能会严重影响物联网应用的性能。

图 2：物联网联网终端的增长



来源：ZK Research，“2019 年物联网设备预测”(2019 IoT Device Forecast)

- **Wi-Fi 已变得无处不在。**过去，员工必须在具有速度优势的有线连接和具有便利性优势的 Wi-Fi 连接之间做出选择。Wi-Fi 5 和 Wi-Fi 6 标准的出现使得员工从此不再两难，因为 Wi-Fi 速度现在已能媲美有线连接，他们能够同时享受有线和无线的优势。此外，许多移动和物联网设备都只支持无线连接，这意味着它们没有有线接口。许多企业已将 Wi-Fi 覆盖范围从封闭办公室扩展到各个地方，包括大堂、自助餐厅、户外场所，以及组织活动范围内的所有其他场所。在这些趋势的共同作用下，Wi-Fi 现已成为主要的接入网络，而网络边缘也成为所有这些设备与公司网络相连接的入口点。
- **传感器和信标的使用日益增长。**为了提供差异化服务，零售商、娱乐设施、机场、医院和其他拥有大量流通人员的场所纷纷开始构建移动应用。低功耗蓝牙 (BLE) 信标和其他类型的传感器可用于结合 Wi-Fi 三角测量技术提高定位服务精度，将误差从 30 英尺（9 米）缩小到不到 3 英尺（0.9 米）。这些信标和传感器连接到 Wi-Fi 无线接入点，提高了网络边缘的重要性。

- **安全保护正在转移至接入边缘。**传统网络只有单个网络流量入口/出口点。要保护这种网络环境，只需在该单点位置设置大规模防火墙并扫描进出网络的所有流量。如今，移动设备、物联网终端和云计算已形成众多新的入口点，并促使入口点转移至接入边缘。因此，网络安全保护也必须向边缘转移，以便最大限度地提高效力。

全数字化转型提升了接入边缘的价值，因为接入边缘是用户、应用、云和物联网终端的第一个连接点。如今，网络边缘应被视为全数字化企业的基础。事实上，甚至可能有人主张，对大多数企业而言，接入边缘可以与业务划等号。静态、无差异的传统接入边缘已无法满足需求。企业和 IT 领导者必须专注于构建智能接入边缘，这就需要统一有线和无线网络环境。

第二部分：传统接入边缘面临的挑战

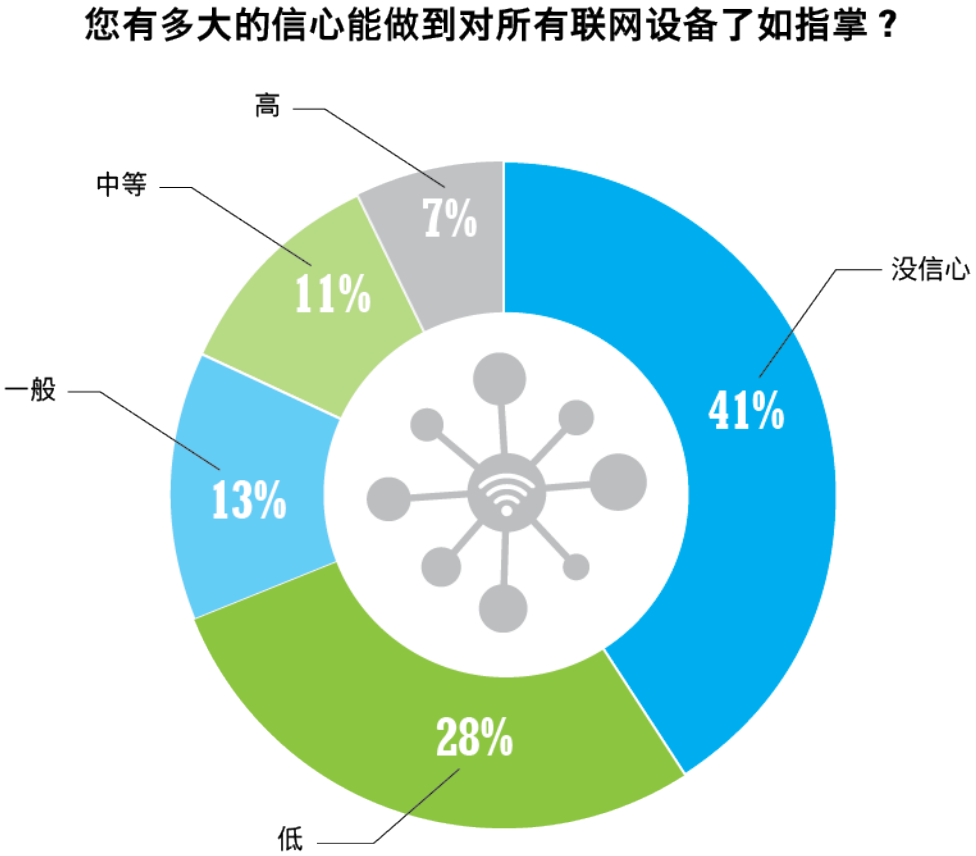
当前接入边缘架构和运营模式已有三十多年的历史。过去，这种设计足以满足需求，因为那时流量传输只要 “尽力而为”，连接只要 “足够好” 就算达到了标准，而且网络与应用性能几乎没有关系。如今，情况发生了变化，因为网络会对应用性能和可用性产生直接影响，而应用性能和可用性又直接影响员工的工作效率。

网络性能不佳会导致员工工作效率降低。ZK Research 在 “2019 年网络购买意向研究” (2019 Network Purchase Intention Study) 中对员工的工作效率降幅进行了量化：在应用性能不佳的情况下，员工工作效率平均降低 16%。IT 和企业领导者应考虑到这个因素，因为组织每年会在 IT 项目上花费数百万美元来提高员工的工作效率，但是通过确保现有应用始终保持最佳性能，可以使工作效率实现两位数的提升。
传统的接入边缘受到几个问题的困扰，如果不加以解决，将会阻碍企业的发展并加重企业的成本负担。以下是阻碍接入边缘成为全数字化推动力的首要问题:

- **缺乏创新:** 在过去 30 年里，接入边缘在创新方面乏善可陈。虽然连接速度有所提升，并引入了以太网供电 (PoE) 功能，但接入边缘的运作模式没有任何改变。
- **不可编程的基础设施:** 传统的网络基础设施缺乏可编程的应用编程接口 (API)，应用与网络之间的接口仅可通过自定义脚本或命令行接口 (CLI) 命令的输入来实现。应用部署和挑战需要与网络更改相协调。可编程基础设施可实现更高程度的协调。
- **缺少自动化功能:** 在传统的边缘基础设施中，网络交换机、无线接入点或其他边缘设备需要手动配置，一次配置一台设备。即使是简单的更改，也可能需要很长时间才能完成。ZK Research “2019 年网络购买意向研究” (2019 Network Purchase Intention Study) 发现，企业实施全网更改平均需要 110 天的时间，这对全数字化时代而言过于缓慢。更出色的自动化功能可减轻许多与网络运营相关的日常和重复性任务。

- **有线和无线网络采用独立的安全保护：**在传统网络中，有线和无线网络的安全保护是独立的。这可能会造成一些重大的安全问题，因为两种网络之间很难保持策略一致。在许多企业中，无线网络处于闭锁状态，没有凭证的个人无法访问。但是，有线网络一直没有受到保护，这意味着任何人只需从 IP 电话背面拔下以太网电缆，就能获得整个网络的访问权限。
- **可视性不足：**传统网络管理方法特定于设备，主要关注单个设备的状态。在这种模式下，管理员无法获得网络运行情况的端到端视图，因此很难了解应用性能。此外，网络管理工具使用的数据源约每 30 秒采样一次，而不是实时采样。这对于研究长期趋势是足够的，但数据上的断带留下了明显的盲点。缺乏可视性的另一个问题是，管理员难以了解哪些设备连接到网络。以前，IT 部门对连接到公司网络的每台设备一清二楚。随着自带设备 (BYOD) 和物联网的兴起，许多 IT 专业人士很难了解有哪些设备连接到他们的网络。在 ZK Research “2019 年网络购买意向研究” (2019 Network Purchase Intention Study) 中，69% 的受访者对网络中的所有设备没有或几乎没有信心（图 3）。IT 界有这样一条箴言：凡是看不到的对象，也就无法管理或保护。因此，充分了解网络中的设备对于管理正常运营至关重要。

图 3：缺乏可视性困扰着很多企业



来源：ZK Research，“2018 年网络购买意向研究” (2018 Network Purchase Intention Study)

- **Wi-Fi 的不可靠性：**对于大多数企业而言，Wi-Fi 网络是影响业务的关键因素。这是一个顽疾，因为在过去 Wi-Fi 一直不可靠。诸如连接丢失、网络饱和、在 Wi-Fi 网络下应用性能不佳等等，各种状况层出不穷。这不仅会降低用户的使用热情，而且会影响公司营收和利润。此外，在全数字化时代，许多公司开始利用 Wi-Fi 网络挖掘客户数据（例如社交信息）或提供基于位置的服务；因此，不可靠的 Wi-Fi 可能会让客户避而远之。现有技术虽然值得称赞，但问题在于设计和规划不佳，部分原因是对 Wi-Fi 的使用缺乏认识。众所周知，Wi-Fi 网络也很难进行故障排除，因为许多问题是间歇出现的。事实上，ZK Research “2019 年 Wi-Fi 故障排除调查” (2019 Wi-Fi Troubleshooting Survey) 显示，约 22% 的工程师每周至少花一天时间专门对 Wi-Fi 网络进行故障排除。
- **安全挑战：**传统网络通过将重叠网络设备置于网络中的特定点（例如隔离区 [DMZ]）实现安全保护。在所有流量都通过单个点进出组织时，这种方法是有效的。如今，云应用、物联网设备、移动用户和其他因素已使网络攻击面呈指数级增加。一个令人信服的相关数据点来自 ZK Research “2019 年安全调查” (2019 Security Survey)，该调查发现 71% 的安全支出集中于传统边界，但是仅 29% 的漏洞源自传统边界。显而易见的是，组织需要重新思考整个安全模式，并且需要首先在接入边缘应用安全。
- **缺乏敏捷性：**用于支持接入边缘的基础设施以硬件为中心，这样一来就变得非常死板。在大多数情况下，对于如何部署设备或如何管理设备，几乎没有选择的余地。传统基础设施尚未获益于软件创新或云。缺乏敏捷性使得网络专业人员很难跟上应用开发领域的快速变化。

接入边缘日益重要，现已成为影响业务的关键因素。传统的接入边缘对于全数字化业务而言过于死板、缓慢而且不安全。坚持现状肯定会使企业面临风险。因此，将接入边缘转换为具有统一管理的以软件为中心的模式需要成为 IT 和业务领导者的首要任务。

第三部分：定义新的接入边缘

接入边缘的演进是几十年来网络中的最大变化，是一种全新的运营和架构模式。接入边缘专为全数字化业务而设计，为边缘带来前所未有的活力，并使其具有与其他 IT 领域相同的敏捷性。因此，网络将不再是阻碍组织发展的瓶颈。

新接入边缘的关键标准包括:

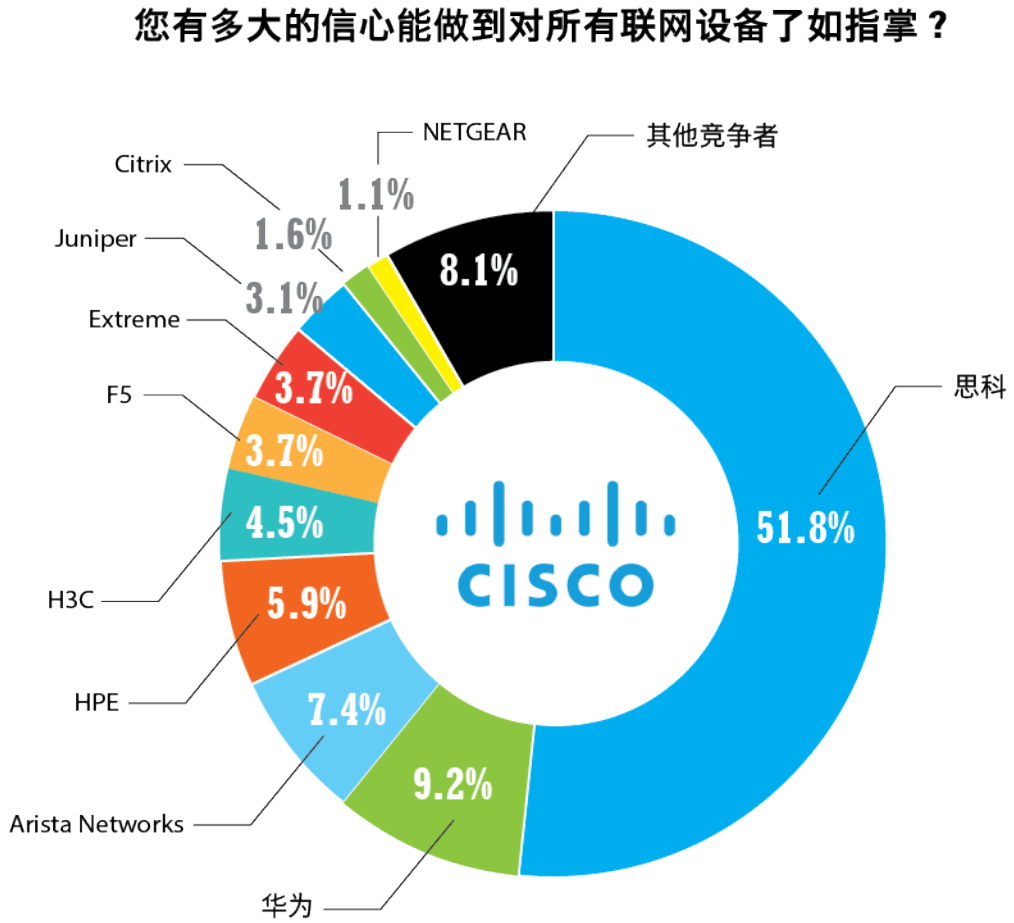
- **有线和无线的统一管理:** 各企业不能再将有线和无线网络视为不同的实体。相反，企业应采用单一接入边缘，部署可向整个网络推送的策略。这将确保整个统一边缘具有一致的性能和安全性。
- **以软件为中心的解决方案:** 全数字化企业需要保持敏捷性，而以硬件为中心的传统基础设施非常死板和脆弱。基于软件的解决方案使公司能够集中控制、实现任务管理自动化以及使用 API 与应用进行交互。最后，基于软件的解决方案可在设备、虚拟机或云中运行，以实现最大的灵活性。
- **分段无处不在:** 限制漏洞造成损害的最简单方法之一是分离关键资产。这种分离可以通过网络分段完成，类似于虚拟局域网 (VLAN)，但敏捷性更高。当今接入边缘高度动态变化，这就要求分段解决方案能覆盖整个网络，从园区核心到边缘，包括物联网设备。
- **集成式威胁防御:** 安全需要与网络紧密结合，而不是作为重叠层部署。网络应充当安全平台，能够集成广泛的安全工具生态系统，以提供集成的自动化合规检查以及威胁检测和规避。集成安全可从新设备自行激活到其会话终止全程保护网络。在有线和无线网络中实施一致的安全保护至关重要。此外，解决方案也必须值得信赖，这需要通过流程确保硬件和软件来自合法的供应商。
- **可自动化网络:** 全数字化企业需要快速发展。因此，等待网络操作更新 VLAN 或访问控制列表 (ACL) 会延迟创新。统一接入要求使困扰网络运营的所有常见和重复流程实现自动化。尽管有些人可能会将自动化视为一种威胁，但实际上它应被视为网络专业人员工具包中的重要工具，因为它可以消除人为错误，并让他们可以腾出更多宝贵时间来推动创新。
- **单一管理平台:** 网络运营基于 “转椅管理” 理念，即工程师坐在多个控制台中间，尝试手动关联数据。有效管理统一接入边缘需要采用单一管理控制台，网络管理员从这一个控制台即可查看所有信息，同时执行配置更改和更新。
- **基于标准的解决方案:** 许多终端与网络和接入边缘互通。基于标准的解决方案可确保最大灵活性和与广泛生态系统的互通性。
- **基于机器学习 (ML) 的智能:** 网络问题的故障排除主要是个被动应对过程。大多数问题是员工而不是 IT 部门报告的，这意味着网络工程师始终处于 “救火” 模式。事实上，许多工程师把大部分时间都花在故障排除上。现代化解决方案应使用机器学习持续分析网络信息，主动报告异常情况并在其对员工造成问题前予以解决。
- **基于意图的网络 (IBN):** IBN 是网络开发自主功能的全新网络范例。它使用闭环模型，网络不断分析端到端状态，以确保始终满足业务意图。

第四部分：Cisco Catalyst 9000 系列促进接入边缘转型

总部位于圣何塞的思科数十年来一直是网络领域的市场领导者。据 Synergy Research Group 表示，思科目前在以太网交换方面的市场份额略高于 52%（图 4），在接入边缘动态变化方面积累了丰富经验。

图 4：思科是以太网交换领导者

来源：Synergy Research Group 和 ZK Research，2019 年



最近，思科升级了广泛部署的 Catalyst 系列接入交换机，并推出了新的 Catalyst 无线接入点和无线控制器系列。新 Catalyst 9000 系列采用当今的多种高级功能实现基于意图的网络的愿景，同时也为将来实现完全自主的网络提供了可能性。该系列包括以下产品：

- **Catalyst 9100：** 高容量 Wi-Fi 6 无线接入点 (AP)，外型设计可满足各种规模的企业的需求
- **Catalyst 9200：** 适用于分支机构和中小型企业的可堆叠规格
- **Catalyst 9300：** 适用于分支机构和大中园区的可堆叠规格
- **Catalyst 9400、9500 和 9600：** 适用于固定配置和模块化园区核心与分布层

- **Catalyst 9800 无线局域网控制器 (WLC)：**适用于 Catalyst 9100 无线接入点的高度安全可靠的控制器。部署十分灵活，支持包括云在内的各种部署模式。
- **Catalyst 嵌入式无线控制器 (EWC)：**适用于 Catalyst 无线接入点的嵌入式控制器，有助于轻松快捷地部署 Wi-Fi，免除使用独立控制器的需要
- **Catalyst 90W UPoE+：**对 IEEE 的增强型以太网供电 (PoE+) 标准进行了延伸，将供电功率增加了一倍，达到 90W。这意味着整个 Catalyst 9000 交换机系列可以通过以太网电缆为更多类型的设备供电。

产品亮点包括以下内容:

- 所有 Catalyst 产品均采用可编程统一接入数据平面专用集成电路 (UADP ASIC)，运行思科最新操作系统 Cisco IOS XE。该集成电路芯片由思科专门设计，以满足统一接入边缘的需求。Cisco IOS XE 是一个开放的可编程网络操作系统，已成为实质上的业界标准。
- 这些产品支持灵活管理，可通过 Cisco DNA Center 单一管理平台工具、本地 Web 用户界面 (UI) 或传统的命令行界面进行管理。
- 可通过堆叠、状态切换和冷修补最大限度减少停机时间并实现重启时 PoE，从而确保不间断运行。
- 集成威胁防御功能包括以下内容:
    - 基于策略的微分段和宏分段
    - 软件定义接入
    - MACsec 链路加密
    - 使用 Flexible NetFlow 检测异常
    - 可靠的解决方案
- Catalyst 产品提供应用识别（500 多个应用）和网络状态感知功能。
- 这些产品是支持物联网的解决方案，提供以下功能:
    - 不间断的快速 PoE、PoE+ 和通用 POE (UPOE)
    - IEEE 1588 音频视频网桥
    - 支持物联网特定协议

该系列还包括 Catalyst 9800 无线控制器，这是思科首个由与以太网交换机相同的 Cisco IOS XE 操作系统支持的控制器。其优势在于，从无线边缘到园区核心提供一致的端到端体验（图 5）。

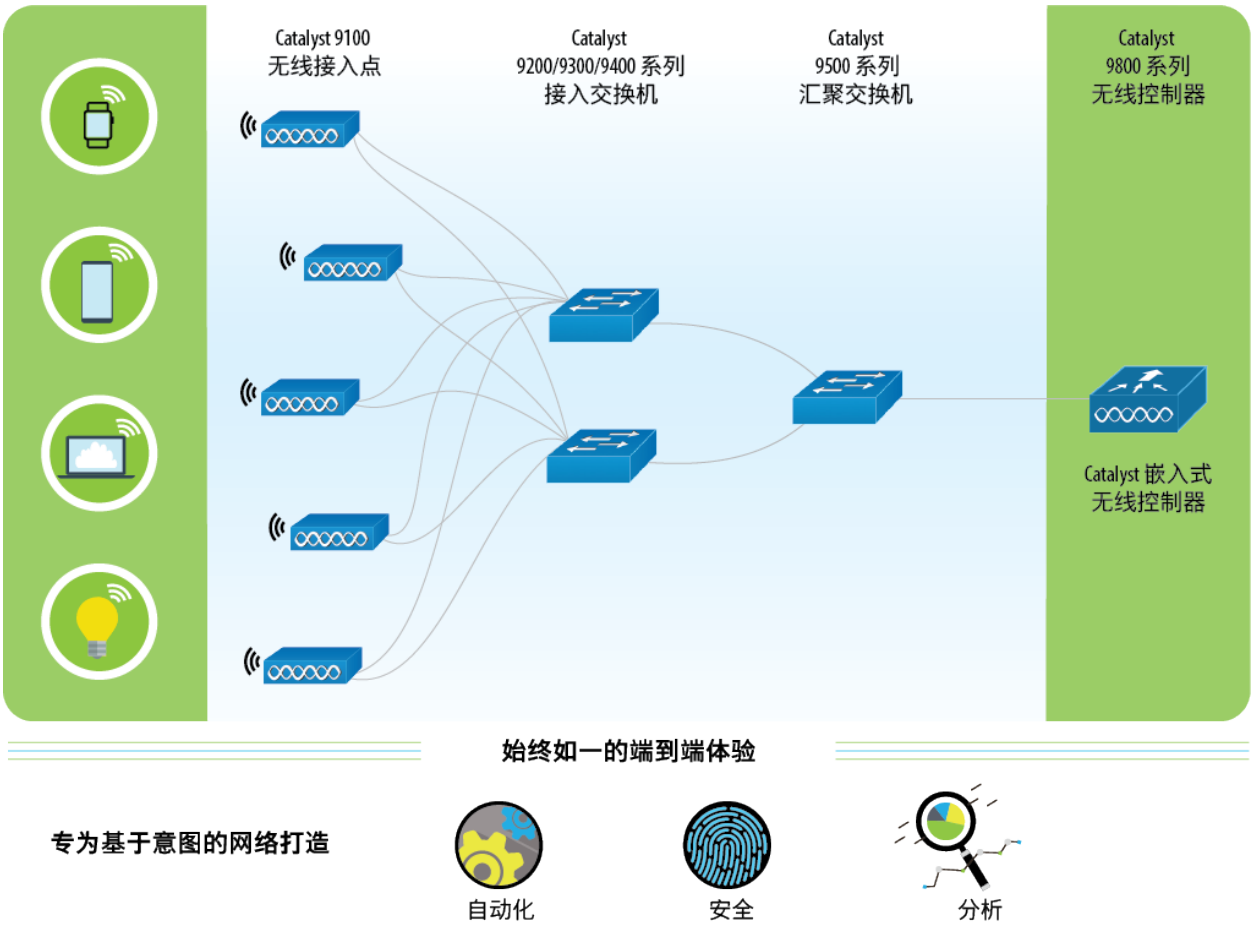
随着对 Wi-Fi 的需求不断增长，对企业级 Wi-Fi 的要求也越来越高。为达到这个要求，思科遵循以下三条原则设计了 Catalyst 9800 控制器:

- **不间断运行，消除停机时间：**控制器无需关闭或重启即可进行软件更新，从而消除计划内停机时间。此外，可升级或添加无线接入点 (AP)，而无需重新启动系统。

- **安全解决方案：**思科最近发布了一项称为加密流量分析 (ETA) 的功能，可以发现加密流量中的恶意软件。该功能现可通过 Catalyst 9800 控制器在 Wi-Fi 网络中使用。此外，还已实现微分段和宏分段自动化，从而将无线资产分开。
- **部署灵活性：**企业不断变化，客户需要有选择和灵活性。Catalyst 9800 控制器可以满足这一需求，既可部署在本地、私有云、公共云服务（例如 Amazon Web Services）中，也可嵌入思科以太网交换机中。无论客户偏好如何，思科都能满足其需求。

Catalyst 9800 控制器还具有高可扩展性，可支持最多 6000 个 AP，因此客户可从小型部署开始，然后根据需要进行扩展。

图 5：全数字化转型需要统一的接入边缘



来源：思科和 ZK Research，2020 年

选择利用新 Catalyst 9000 系列的客户将会实现以下几项业务和技术优势:

- **简化安全策略:** 只需创建一次安全策略，即可在有线和无线网络之间全面推送。
- **将策略扩展至数据中心:** 通过使用思科 ACI 控制器，可将安全策略扩展到数据中心，以实现 “从网络核心到用户” 的全面保护。
- **网络分段无处不在:** 通过利用 ACI，企业可在整个网络（包括数据中心）中利用微分段和宏分段。
- **通过自动化实现有线网络和无线网络的快速操作**，确保提供最佳的应用体验。
- **利用 Cisco DNA Center 在有线和无线网络中使用单一管理平台**，可确保消除管理或安全盲点。
- **物联网平台:** 无论协议如何，均可连接和保护任何类型的物联网设备。
- **自动化和网络状态感知**将减少操作时间并加快问题补救速度。此外，缩短停机时间将直接提升 IT 部门和员工工作效率。
- **可编程网络**可实现系统集成，并确保能在部署后快速添加新的特性和功能。
- **为基于意图的网络 (IBN) 奠定基础:** 目前，思科提供诸多 IBN 功能，例如自动分段、ETA 和自动操作。未来几年内，思科将提供更多智能功能，最终目标是让客户在准备就绪后能够转向完全自主的网络。

第五部分：总结与建议

全数字化转型时代已经来临，企业需要明白适者生存这一道理。现今，公司竞争优势取决于其敏捷地适应变化并做出快速转变以捕捉市场变化的能力。大多数支持全数字化的技术（如物联网、云和移动）均以网络为中心，这提高了网络（特别是接入边缘）的价值。如果企业要充分利用这些技术的潜力，则接入边缘必须不断发展，第一步是实现统一边缘。转向统一接入网络是当今 CIO 的当务之急，因为这是全数字化转型的基础。

为了帮助企业着手进行转型，ZK Research 提出了以下建议:

- **专注于首先发展接入边缘。**对于大多数企业而言，边缘是网络操作和复杂性的关键所在。边缘是物联网设备连接网络的入口，是云与企业的接口，也是从移动客户端提取的数据的来源。传统网络边缘架构不灵活、僵化死板，阻碍着组织成为全数字化组织。企业必须首先投资于统一接入网络，以实现更高水平的网络灵活性；需要注意的是，网络的其余部分需要在之后进行升级。Wi-Fi 5 和 Wi-Fi 6 标准将产生级联效应，要求园区核心进行更新升级，而且可能要求数据中心进行更新，但边缘是起点。

- **坚决彻底地实现网络进程自动化。**自动化并非网络工程师的敌人；相反，应将其视为一种可消除 Wi-Fi 故障排除等诸多日常任务的战略性工具，目前这些日常任务已让网络专业人员不堪重负。企业应使用人工智能 (AI) 和基于机器学习的自动化工具来简化网络运营，转向采用一种能够自我修复并提供更高安全性的前瞻性管理模式。自动化程度越高，IT 就越能专注于实现战略计划。
- **规划基于意图的网络转型过程。**自动化是网络转型的第一步，而不是最终目标。IT 领导者应专注于向基于意图的网络发展，这种网络将不断检查安全和管理策略，以确保实现业务目标。循序渐进地启动思科 ETA 等具有高影响力的功能，待其实现切实价值之后，再将其作为跳板以实现更广泛的 IBN 部署。