IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Cisco

Intent-Based Networking (IBN) is increasingly being used to provide policy-based automation, service assurance, and security enforcement. But the full potential of IBN can only be realized if it can exchange intelligence with the applications, systems, and processes around it. Turning the intent-based network into an open platform allows IT to meet the needs of dynamic business and IT objectives continuously and efficiently.

Why Intent-Based Networking Demands an Open Platform

June 2018

Written by: Brandon Butler, Senior Research Analyst, Network Infrastructure

Networking Strategies for the Digital Era

The network has never been a more critical enabler of new technologies. Networking is at the center of connecting to the cloud, supporting the rise of the mobile revolution, and leading to a world made up of an Internet of Things. IDC refers to these tectonic shifts as third-platform technologies, and while they enable efficiencies, new business opportunities, and advanced security, third-platform technologies also put tremendous strain on the network. To take full advantage of third-platform technologies, organizations must embrace automated management of their networks.

Far too often though, IT departments are required to control disparate systems as silos. This leads to manual, ad-hoc management of the network. IT today acts more as human middleware rather than enablers of exciting new technology. Inefficient operations lead to security vulnerabilities, and reduced service levels for end users and applications. Human middleware that needs to correlate and exchange information between multiple systems often ends up missing important trends and events that fall between the cracks.

AT A GLANCE

KEY THEME

IT is burdened with managing complex environments and ensuring the needs of the business are met.

WHAT'S IMPORTANT

Intent-Based Networking brings new levels of automation, visibility, and assurance.

KEY TAKEAWAYS

By creating an open network platform, IBN becomes an innovation engine and integration point for IT and non-IT applications and systems across the organization.

Achieving the full value of the network requires an open platform that streamlines automated management of IT and non-IT systems.

In recent years there has been robust innovation in the networking industry to alleviate these issues. Network platforms have been developed that run at machine speed for exchanging intelligence and correlating information. Network platforms enable substantial efficiency gains and allow IT to focus on delivering services and improved user experiences. Integrations with security systems allow the network to become a powerful security platform, rather than a vulnerability. Increased levels of automation are required to help enable a platform, support new applications, and provide higher levels of network programmability. Controller-based network automation as delivered by software-defined networking (SDN) and to an even greater extent by the all-encompassing vision of an Intent-Based Network can elevate IT's role and cope with the strains of digital business.

This is borne out by an IDC survey of more than 1,000 enterprises in the last quarter of 2017, where more than two-thirds of organizations expected to deploy some elements of software-defined networking in their enterprise campus environment within the next year. The top reason for using SDN, ranked by more than 55% of respondents, was to increase network agility and support virtualized applications; the second most important reason – cited by half of respondents – was to enable programmability of the network with the goal of gaining operational IT efficiencies. These statistics clearly show the desire by organizations for higher levels of automation and the benefits they expect to gain.

Centralized alignment of application and process policy throughout the enterprise allows IT to take advantage of the intelligence of the network to support and secure the business. But for business and IT apps to deliver the desired outcomes and fully take advantage of network intelligence requires an open network platform. The open platform uses published application programming interfaces (APIs) to integrate and exchange intelligence with adjacent network and IT services. It integrates with other IT resources, security tools, line of business applications and third-party infrastructure. An open network platform must be able to take inputs from these sources and automatically deliver the network resources needed.

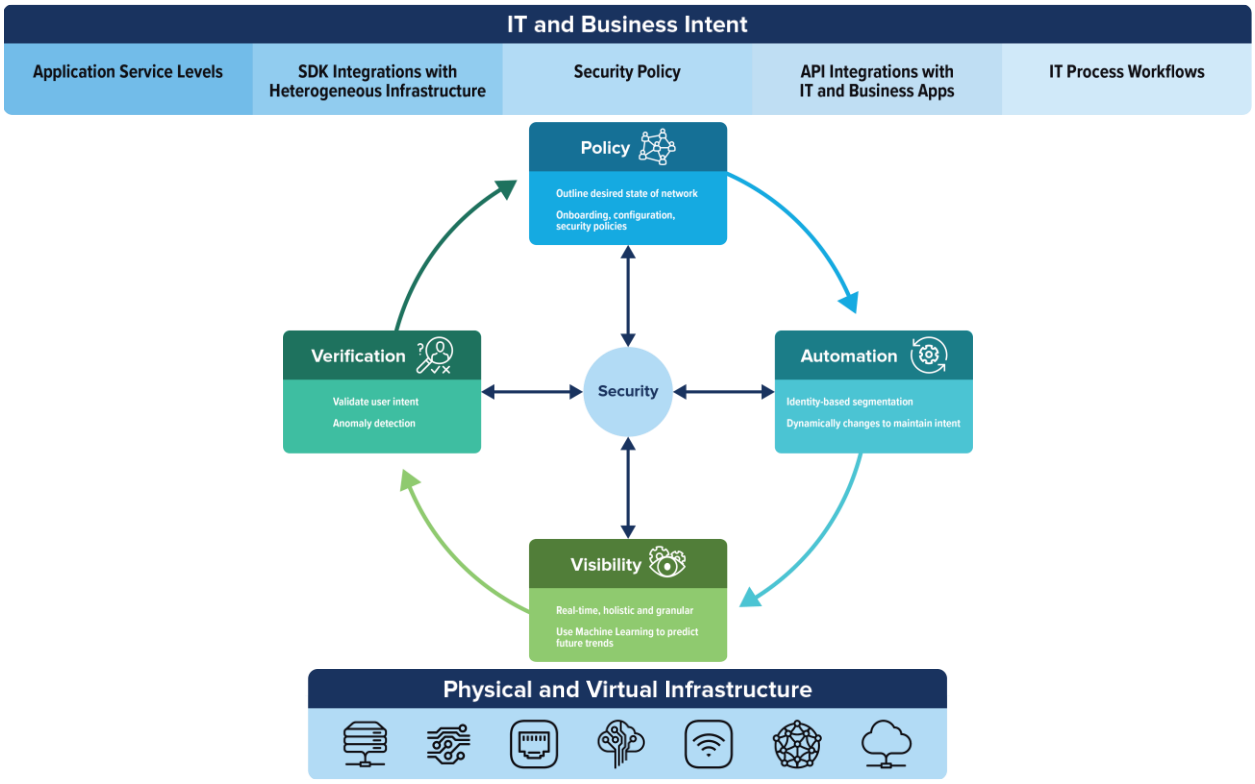
Intent-Based Networking Definition

Intent-Based Networking (IBN) is the industry model for creating an outcome-oriented network system that can automatically adapt to meet communicated or learned dynamic business and IT intent. Intent can be communicated as application service levels, security and compliance policies, IT operational processes, and any other intent that needs the support of the network (see Figure 1). Building on the automation capabilities of SDN, Intent-Based Networking relies on the interaction of policy-driven network-wide automation, with advanced visibility, analytics and assurance tools to implement, secure and dynamically maintain the state of the network required by constantly changing business and IT intent.

The full potential of Intent-Based Networking can only be realized if it can exchange intelligence with the applications, systems and processes around it.

The vision for IBN has come into play in recent years and has evolved from point-specific products, for example, around on-boarding users and devices to a network. It's advanced to become a network-wide automation system for managing the complete life cycle of enterprise networks. The next evolution of IBN is for it to become an open platform that can integrate with other IT and business applications and processes. An open IBN platform allows the network to dynamically ensure that the networking needs of the business are constantly being met.

FIGURE 1: THE INTENT-BASED NETWORKING MODEL



Source: IDC, 2018

Why Intent-Based Networking Requires an Open Platform

Can Intent-Based Networking be achieved without an open platform? By definition, an IBN system configures resources to ensure the needs of the business are met. But to do so, the IBN system must be able to receive data from business and IT applications. The IBN system needs to have comprehensive abilities to integrate with applications outside of the network engineer's domain. Without an open platform, the IBN system is not reaching its full potential.

Achieving the full value of the network requires an open platform that streamlines automated management of IT and non-IT systems.

For intent to be applied and assured end-to-end from clients and devices to any service anywhere, policy needs to be applied consistently and assured across all domains (campus, branch, WAN, cloud, datacenter, security). IBN requires open interfaces to communicate and align policy and assurance across domains.

An open platform is also needed for IBN systems to integrate into operational workflows. An open IBN platform automatically monitors for events or threats and activates intent policy across the system. When the network is an open platform, IT can centralize visibility, management, analytics, security, and troubleshooting across multiple applications, systems, and heterogeneous network devices to achieve better IT and user experience.

This is particularly important for security. There are growing interactions between networking and security operations, but too often these groups are still siloed. IBN systems

have the unique ability to ingest security policies and automatically execute them. In order to do so, however, the IBN must be an open platform to allow for integrations with security tools. An open IBN platform becomes a powerful distributed security policy enforcer, threat detector, and mitigator. The IBN provides a bridge between network and security operations to monitor and secure the business.

An open network platform that builds on an Intent-Based Network tightens the gap between business and IT by continuously aligning the network to the needs of the business. This allows business and IT applications to take full advantage of the network's capabilities. To achieve all these goals, an open network platform should provide integration points across multiple components, including:

- **Intent-Based Application Programming Interfaces (APIs)**, which allow for applications and systems internal to IT and from lines of business and security teams to communicate their needs to the IBN. Data such as application policy, compliance settings, provisioning of necessary resources, software image management, and assurance that automation has been properly implemented can all be achieved through APIs. IT systems such as Active Directory and business applications such as SAP or Oracle can automatically communicate the network resources needed for optimal performance via Northbound APIs.
- **Multivendor Software Development Kits (SDKs)** allow organizations, or system integrator partners, to build customized integration between the open network platform and heterogenous infrastructure to map third party network devices to a data model. Doing so allows for Level 1 Operations support such as discovery, inventory, topology, availability and health scores for infrastructure from Cisco, Dell-EMC, Hewlett Packard Enterprise, and others. The SDKs also allow customized integration across heterogeneous network devices so they can be incorporated into the intent-based network.
- **Process integration APIs** enable integration with IT Service Management (ITSM) such as ServiceNow, IP Address Management (IPAM) such as InfoBlox, and IT reporting services such as Tableau for automating workflows across network and IT operations. Additional domain integration APIs allow intent and policy exchange across technology domains like campus and branch LANs, SD-WAN, and datacenters. Integrations with advanced threat detection systems allow IBN to enforce security policies consistently across the organization.

With API and SDK network extensibility, IT can better align to the needs of business and IT apps, streamline operations and ensure investment protection.

Benefits of an Open Network Platform

An open network platform enables an outcome-oriented network. It accepts policy specifications from applications and devices, takes advantage of centralized automation, and verifies that the system is meeting the needs of the business. It does all this not just for core networking infrastructure, but for other hardware devices, security tools, and line-of-

business applications, too. Continuous alignment through API and SDK integrations, means that the integrations are not point-in-time connections, but rather a two-way street supplying critical diagnostic, telemetry, and health status to the IBN system. In return, the IBN platform aligns the necessary resources to ensure the entire system runs securely and smoothly. This improves IT service delivery by streamlining workflows across network systems, IT apps, line-of-business processes and third-party apps that used to be managed independently.

Security services such as physical or virtual firewalls, identity-based authentication systems, Deep Packet Inspection, intrusion prevention, and many others can feed data into the open IBN system. The IBN in turn should be able to dynamically configure the network to monitor for threats and respond to them, even if the traffic is encrypted. The IBN system can also automatically ensure network services are always configured correctly to meet compliance with regulatory frameworks. It can make changes to the network as the environment changes to ensure compliance is met.

End users are excited about the opportunities an open network platform can deliver. One network manager for a U.S.-based healthcare provider that has about 15,000 users, 1,000 switches, and 60,000 ethernet ports has been automating various functions within the enterprise network. "It's a big environment, but the ability to not have to manually configure switch ports and give users automatic access to their appropriate resources is a huge benefit," the network manager said. This multifaceted environment includes systems from Cisco, CheckPoint, and F5. Opening the network to integrate with business applications, heterogenous infrastructure, and various systems throughout the enterprise will allow for even more ways to automate once-manual tasks and improve IT efficiency, the manager noted. "If we can manage all those components through a central platform, it would give us one solution to check everything, manage configurations, and reduce our time using separate management platforms."

Advanced levels of network automation have benefits beyond just IT – they can help enable new business opportunities, too.

Introducing this level of advanced network automation has significant benefits beyond just IT. Relying on manual processes for onboarding new applications, devices, or users slows the process of exploring new business opportunities. An open network enables more streamlined support for new technology. Imagine that a marketing department, for example, finds a compelling cloud-based application for finding new prospects. An open

Open IBN Use Case

Unified Communications (UC) applications have robust network requirements that can be difficult to predict. With an open IBN, UC apps can automatically communicate via APIs the network resources need to ensure a high quality of service for a VOIP call.

Through open integrations, the UC system aligns with Active Directory for authentication of meeting participants and makes API calls to ensure adequate bandwidth throughout the call. During the call, users provide real-time feedback, which the open network platform ingests, then makes automatic changes to optimize the quality of the call. After the call, the open network platform automatically executes a charge back to the department that initiated it.

All these processes would have required manual IT intervention without an open network platform. Instead, they're done through a smart IBN. Similar automated workflows can be created for a range of Enterprise Resource Planning (ERP) processes, billing, customer outreach, logistical operations, HR, and many other services in the enterprise.

network platform can automatically enable identity-based access policies so that only certain executives have access to the app. API integrations between the new app and back-end enterprise databases can be configured and managed with the IBN. Monitoring tools can be integrated into the system to track all communication between the app and the enterprise to ensure appropriate security checks are constantly in place. With an open network platform IT has become an enabler of this new app, as opposed to the reason it can't be supported.

This network-based automated management of applications, devices and processes is especially useful in large-scale environments, such as Internet of Things (IoT) deployments. Managing the life cycle of these devices — from onboarding to optimizing network connections to ensuring security policies are up to date — will require an automated network platform that supports a wide range of infrastructure, analytics tools, and connectivity methods. This process can be integrated directly into an open IBN platform. Devices can be automatically recognized by the network when they come online, then the system can install the proper configurations and run verification checks to ensure they are compliant. Once the devices are in the field, the open IBN platform can monitor diagnostic information and automatically configure network settings to facilitate the transfer of data from the devices to a central location, all via encrypted connections. Each of these processes could have required painstaking manual setup and execution. Instead, an open IBN platform enables a completely automated IoT workflow.

An open network platform can evolve in the future to support new applications and infrastructure, and integrate them into the IBN workflow.

As an open platform, the network also can evolve into the future. APIs and SDKs can be developed for a wide range of applications and services within the enterprise, and they can be changed at any time. As new applications, infrastructure and devices come into the network, they can communicate the network resources they need into the open IBN system. The open network becomes a way of future-proofing a network management platform to ensure it can meet the needs of the business not just today, but also as demands on the network increase in the future.

The open networking platform will extend across multiple domains under the control of IT, too. Increasingly there will be integrations between the datacenter, enterprise campus, the WAN, and into the cloud. Having consistent policies, automation, and analytics across these domains will lead to increased levels of visibility and assurance. An open IBN ensures the network is continuously meeting the needs of the business, no matter where the applications or processes are running.

Considering Cisco

In line with IT's growing need for a more dynamic and efficient infrastructure, Cisco has launched major initiatives to lead the industry's charge to delivering Intent-Based Networking systems across multiple technology domains. This includes delivering an open Intent-Based Networking model across the datacenter, private cloud, campus, WAN, and branch.

For datacenter and private cloud, Intent-Based Networking captures business intent by understanding the application requirements first with Cisco Tetration. IT policy can then be defined, orchestrated, and managed with Application Centric Infrastructure. And Network Assurance Engine delivers continous assurance through advanced analytics to keep the network operating in its desired state. IT teams are able to use their own tools within the

open and programmable environment. Cisco also provides a broad set of solutions through technology partners who form an extensive ecosystem of integrated solutions.

In addition, Cisco is delivering an open and extensible intent-based network platform across the campus, branch, and WAN named the Cisco Digital Network Architecture (DNA). At the core of DNA is DNA Center, which acts as the control center and delivers on all the elements of an enterprise-class, closed-loop intent-based network, including policy-based automation and segmentation and advanced levels of visibility, analytics, and assurance.

With the introduction of intent-based APIs, process and domain integration APIs, and multivendor SDKs, IT teams and developers can now build integrations and innovations on top of DNA Center's native automation, assurance, and analytics capabilities. IT teams can now use these open interfaces themselves, or work with Cisco's partner ecosystem to customize their network to serve their own specific IT and business objectives. DNA Center is delivering multiple cross-domain integrations, including Cisco ACI in the datacenter, Stealthwatch security, and Meraki networking.

Conclusion

Organizations require increased agility and deeper levels of visibility into what's happening in their environments. There is increased demand for automated processes that can replace manual, ad-hoc management of network systems. Furthermore, organizations need assurances that the system is being managed in a secure way that provides the optimal application and end-user experiences. The industry vision of Intent-Based Networking holds the promise to achieve this.

IT teams can only achieve the full value of Intent-Based Networking with an open platform approach that allows for integration with other IT and business applications, systems, and processes. This enables IBN principles to be used to align business needs with IT execution throughout the enterprise and ensure the entire enterprise receives reliable and secure network performance.

By using intent-based and integration APIs, SDKs, and customized integrations, organizations can streamline IT operations, ensure the security of their environments, and centralize management of disparate systems. This allows IT to move on from acting as human middleware, and allows for automated platforms to help make sure the network is meeting the needs of organizations both today and as they evolve in the future.

About the analyst:

Brandon Butler, *Senior Research Analyst, Enterprise Network*

Brandon is responsible for market and technology trends, forecasts and competitive analysis in Ethernet switching, routing, wireless LAN, and adjacent emerging segments such as SDN and SD-WAN. Prior to joining IDC, Brandon spent more than a decade as an accomplished technology and business journalist. He spent six years at Network World as a Senior Editor covering emerging networking technologies, including software-defined networking (SDN) and software-defined Wide Area Networking (SD-WAN).

IDC Custom Solutions

IDC Corporate USA

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