NETWORKWORLD
FROM IDG

THE CONNECTED ENTERPRISE
INSIDER EXCLUSIVE

GETTING GROUNDED IN INTENT-BASED NETWORKING

Learn about this trending technology that stands to **streamline management**, **access control** and **security**

INTENT-BASED NETWORKING made a big splash in 2017 when Cisco announced its intent to create an IBN advanced automation and orchestration system over the next few years.

The vision the company expressed has widespread implications for reducing the manual work needed to establish and maintain the desired state of a network.

Editor's NOTE

Once it is mature, IBN would let network admins define what they want the network to do – the intent – and after that the system would configure the network to fulfill that intent. Once the desired state is set, the system would monitor the network for changes that might disrupt that state. If it finds any, it could then take action to restore the expressed intent.

Cisco isn't the only player in IBN. Others include Juniper Networks, Apstra, Forward Networks and Veriflow. Each has a slightly different spin on what IBN is and how their products fit into the picture. For example, Apstra's big push is to enable IBN via its platform of overlay software that can incorporate devices in multivendor environments into a coherent IBN system.

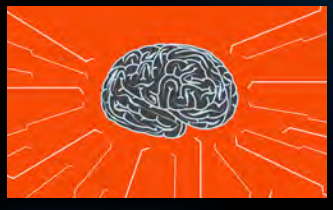
By contrast, Cisco's model incorporates much of its own legacy hardware and software as well as gear it plans to roll out. Juniper says its gear can support many IBN features but the company doesn't have a published IBN roadmap.

Forward creates software models of networks on which admins can dry-run network configurations to see their ramifications before going live in the network. It's not IBN, but the company claims it's a way to get a taste of IBN. Veriflow monitors traffic through the network to verify that the intent of the network configuration is being carried out.

This package of articles provides essential definitions, descriptions and roadmaps that can help networking pros weigh if and when they want to jump into IBN. ◆

TIM GREENE, *executive editor, Network World*

INSIDE



What is Intent-Based Networking? 3

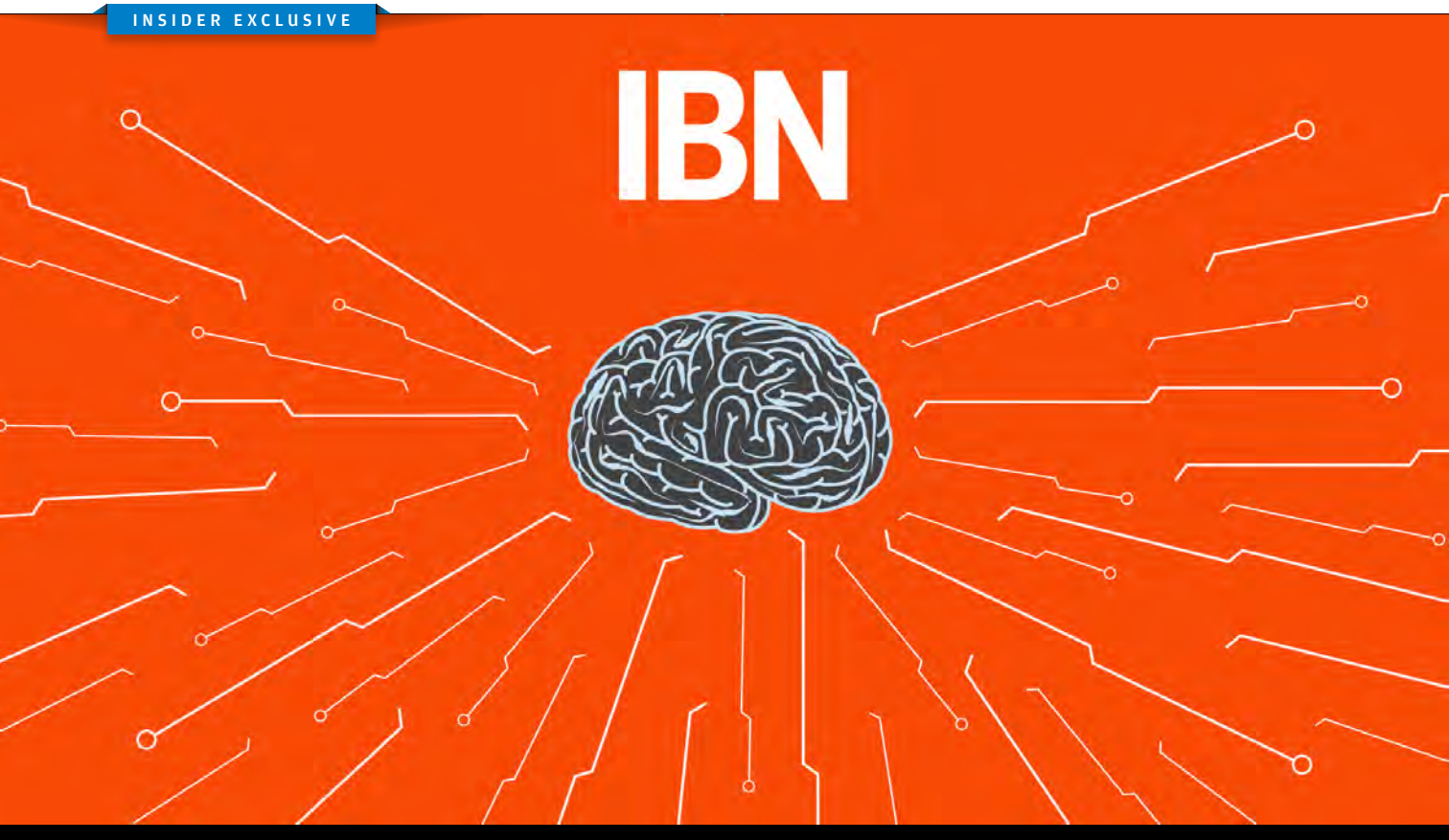
Why Cisco's New Intent-Based Networking Could Be a Big Deal 5

Apstra Intent-Based Networking Bridges the Physical, Virtual 8

How to Buy Intent-Based Networking Today 10

IDG / THINKSTOCK

INSIDER EXCLUSIVE



VIDEO: The networking industry's hottest new buzzword — intent-based networking — is the next evolution of network software management. Get up to speed fast with this visual explainer.

What is Intent-Based Networking?

Cisco has jumped into the intent-based networking market. **BY BRANDON BUTLER**

CISCO HAS JUMPED head-first into the intent-based networking market, saying the technology that uses machine learning and advanced automation to control networks could be a major shift in how networks are managed.

MORE ONLINE: Cisco CEO Chuck Robbins on intent-based network management

But what exactly is intent-based networking?

Gartner Research Vice President Andrew Lerner says intent-based networking (IBN) systems are not new, and in fact the ideas behind IBN have been around for years. What's new is that machine learning algorithms have advanced to a point where IBN could become a reality soon. Fundamentally, an IBN is the idea of a network administrator defining a desired state of the network and having automated network orchestration software implementing that definition as policies.

"IBN is a stark departure from the way enterprise networks are managed today," Lerner explains in a research note describing IBN. "Currently, translation is manual, and algorithmic validation is absent ... Intent-based networking systems monitor, identify and react in real time to changing network conditions."

Lerner says IBN has four characteristics:

IDG / THINKSTOCK

1 **Translation and validation**
One of the key tenets of IBN is its ability to translate commands from network administrators into actions the software performs. The idea is that network managers define a high-level business policy they want enforced in the network. The IBN verifies that the policy can be executed.

2 **Automated implementation**
After a network manager defines the desired state of the network, the IBN software manipulates network resources to create the desired state and enforce policies.

3 **Awareness of state**
Another key component of IBN is its gathering of data to constantly monitor the state of the network.

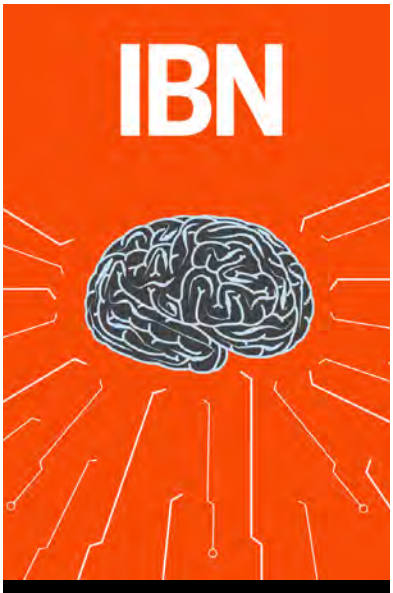
4 **Assurance and dynamic optimization/remediation**
The IBN constantly ensures the desired state of the network is maintained. It uses machine learning to choose the best way to implement the desired state and can take automated corrective action to maintain state.

In a nutshell, IBN is about giving network administrators the ability to define what they want the network to do, and having an automated network management platform create the desired state and enforce policies.

Cisco, along with a handful of startup companies, have laid out product roadmaps to create IBN platforms, but Lerner says none of them has a full-fledged IBN product on the market yet. IBNs are meant to be hardware-agnostic, although certain vendors, like Cisco, may make products that are integrated with their own hardware.

Lerner expects, given the nascent nature of IBN, that it may not be mainstream until at least 2020. In the meantime, he believes IBNs are best implemented in pilot and proof-of-concept deployments. "We anticipate that adoption will be pragmatic, associated with new build-outs and/or network refresh initiatives," he notes. "Early rollouts will likely be for well-defined and specific use cases, such as a spine/leaf data center fabric or WAN – edge infrastructure." ◆

BRANDON BUTLER, *formerly a* Network World *senior editor, is an IDC analyst covering Ethernet switching, routing, wireless LAN and newer tech such as SDN and SD-WAN.*



VIDEO: Why should enterprises care about intent-based networking?
Panelists break down Cisco's intent-based networking strategy, which brings machine learning to the networking realm. Plus, they hash out the ramifications for the security industry. **[Tech Talk Ep 1, Pt 2]**

> **IBN is a stark departure from the way enterprise networks are managed today.** Currently, translation is manual, and algorithmic validation is absent ... Intent-based networking systems monitor, identify and react in real time to changing network conditions.
>
> **ANDREW LERNER,** VICE PRESIDENT, GARTNER RESEARCH

INSIDER EXCLUSIVE

Why Cisco's New Intent-Based Networking Could Be a Big Deal

Intent-driven networking uses **machine learning** to automatically enforce security policies and maintain network state. **BY BRANDON BUTLER**

SCENTSY, a $500 million manufacturer and seller of wickless candles, got an early look at what Cisco and some analysts are saying could be the next big thing in the network industry: intent-based networking.

"I think this could be a pretty big shift in terms of the paradigm of network management," says Kevin Tompkins, network architect at the company. "We're getting away from managing individual devices and into having a central, globally managed policy, all controlled from one place that pervades through the network."

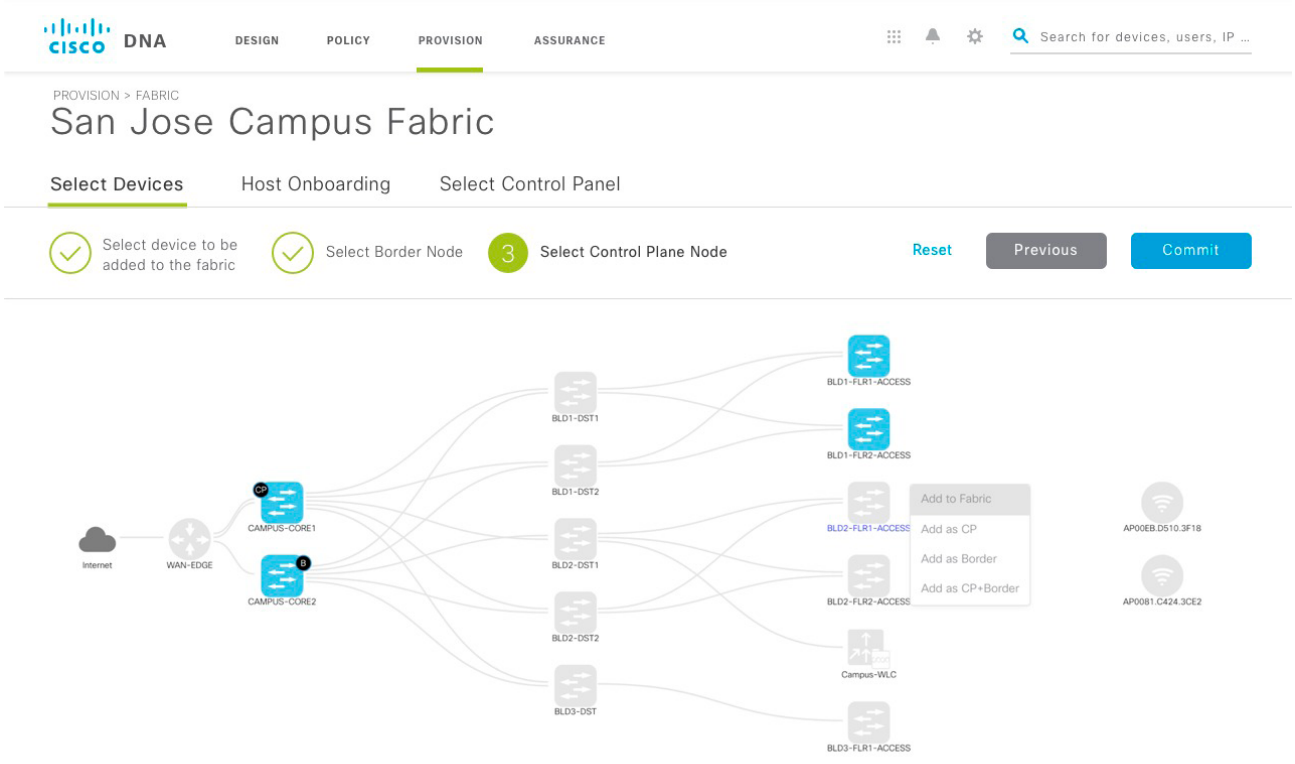
In 2017 Cisco released a series of new hardware and software capabilities that it says use machine learning technology to provide advanced network automation. The system allows users to express policies and have a software platform that executes and maintains the desired state of the network.

MORE ONLINE: Cisco brings intent based networking to the end-to-end network

An Emerging Technology

The first thing to know about Intent-based networking is that it is very early days. "Intent-based networking is nascent, but could be the next big thing in networking, as it

THINKSTOCK



Cisco's Digital Network Architecture is a central hub for managing policies

promises to improve network availability and agility, which are key as organizations transition to digital business," Gartner analyst Andrew Lerner wrote in a recent report.

A key component of IBN is that it provides mathematical validation that the expressed intent of the network can be and is implemented within the network, and that it has the ability to take real-time action if the desired state of the network is misaligned with the actual state.

IBN is, in theory, a software platform that can be agnostic to the hardware that it runs on.

The idea of IBN has been around for a couple of years, Lerner says, but there have been very few platforms that can enable it. A handful of startups, such as Apstra, Veriflow and Forward Networks have some early components of IBN in various product offerings. Lerner estimates there are less than 15 intent based-networking platforms in production deployments today, but the number could grow to more than 1,000 by 2020.

Cisco's Announcement

Cisco has jumped into the IBN market with a series of new software and hardware components that customers can purchase either as an integrated package or separately, with the software available a la carte via subscription. Many of these components are built on Cisco's Digital Network Architecture (DNA) and will be available as part of Cisco's ONE Software. These components include:

- **DNA Center:** A software dashboard where users manage policy creation and provisioning, and get validation that policies are in place.
- **SD-Access:** Software that manages automated policy enforcement and network segmentation.
- **Network Data Platform:** A new repository that categorizes and correlates network data.
- **Encrypted Traffic Analysis (ETA):** Software that analyzes metadata of encrypted traffic to detect vulnerabilities.

Cisco's new line of Catalyst 9000 switches

■ **New series of Catalyst 9000 hardware switches**, including the Catalyst 9300 and 9500 and the 9400. These switches are meant to be deployed throughout the campus.

Prashanth Shenoy, VP of enterprise network marketing at Cisco, says many of today's networks were designed for what he calls the Internet Era to run voice, video and data. Businesses now need the network to run mobile, cloud and IoT applications with advanced security. A new network platform is needed to manage the scale of devices connecting to the network, the threats posed to it and the explosion of data generated.

"What we've announced has fundamentally redesigned how we help our customers design, manage and scale their networks," says Shenoy. "We're calling that a network that is intuitive, one that can constantly learn from itself and from the data it sees, constantly adapt to the changing business demands and then constantly protect against advanced threats."

But Lerner, the Gartner analyst, says that all together, the software and hardware components Cisco talks about do not amount to a full-fledged IBN system. "It's a platform that should enable intent-driven network management in the future," he says. "Except for some discrete, tight use cases around configuration, it's not quite completely glued all together yet."

The system at this point, he says, lacks the ability to take a policy defined at a high level and have the system configure the network to match the desired state. As of now, Lerner believes the system still has a degree of network configuration intricacies and nuances that could make it difficult to onboard. As Cisco develops the product he expects more abstractions will be created to push it closer to true IBN.

How It Will Be Used

Tompkins, the Scentsy network architect, is optimistic the advanced automation capabilities Cisco has announced will benefit his 125-person IT shop that runs the company's development, ecommerce and logistics operations.

Scentsy was an early customer of Cisco's Unified Computing System (UCS), is running Cisco's Application Centric Infrastructure (ACI) and is one of the few customers that has trialed the intent-based networking gear.

During the Wannacry vulnerability scare, Tompkins wanted to ensure that a specific port was shut down throughout his network and an intent-based system could execute that policy change easily, he says. Doing that process manually is not only cumbersome, but a potential security risk because it's difficult to ensure the ports have been shut down on all devices.

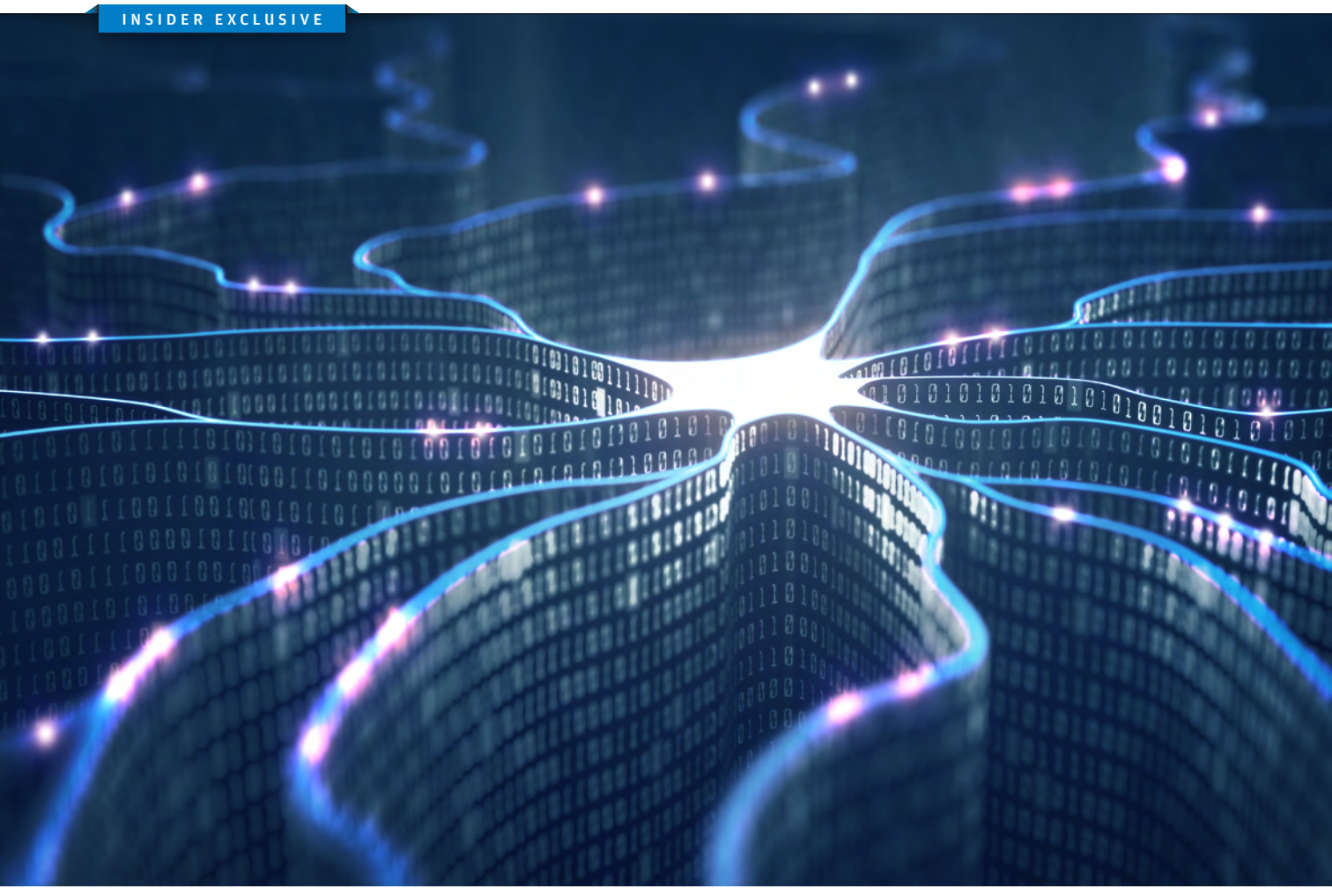
Tompkins is also excited about the ability to more granularly enforce policies based on user activity and role. A system like this could, for example, ensure that workers only have access to core company data during normal business hours. "These are decisions made at the policy level, and applied at the network level," and he says they're done without managing the "minutiae of access controls."

Rohit Mehra, vice president of network infrastructure at IDC says elements of intent-based networking, specifically around policies and context, have been around for a while. "This is taking policy enforcement to the next level," he says. "It uses a combination of intent and context, based on what the application is, who the user is, what the device is, and automates the network management to actually get to the desired state of what you want the network to do," he says.

Cisco has not released pricing details for the new software and hardware it has announced. ◆

To comment on this story, visit Network World's Facebook page.

> What we've announced has **fundamentally redesigned** how we help our customers design, manage and scale their networks.
>
> **PRASHANTH SHENOY,** VP OF ENTERPRISE NETWORK MARKETING, CISCO



OPINION

Apstra Intent-Based Networking Bridges the Physical, Virtual

Apstra's intent-based AOS 2.0 delivers agility across **physical/virtual networks** so they look like one. **BY ZEUS KERRAVALA**

INTENT-BASED SYSTEMS have been all the rage since Cisco announced its "Network Intuitive" solution in 2017. For Cisco customers, its solution is certainly interesting. But what about businesses that want an alternative to Cisco? Or companies that want to run a multi-vendor environment?

Over a year before Cisco's launch, a start-up called Apstra shipped a closed-loop, intent-based solution. It was designed to be multi-vendor in nature with support for Cisco but also Arista, Juniper, HP and others, including white-box. Apstra operates as an overlay to networks built on any of the leading vendors' gear to deliver intent-based networking in heterogeneous environments.

Apstra has announced the AOS 2.0 release of its software, which addresses the gap that exists between physical-underlay and

THINKSTOCK

virtual-overlay networks, including VXLAN. I've discussed this topic with many network professionals, and there is a high degree of interest in using network virtualization, but the lack of visibility between the underlay and overlay is a huge deterrent. Without an understanding of the relationship between the two, network managers are faced with managing two separate networks — the physical network and the virtual overlay.

Also, with this model, troubleshooting becomes extremely difficult as the virtual network is one big blind spot. Any application problems that occur in the overlay are, for all intents and purposes, invisible to the engineers running the physical network. The lack of visibility also creates security problems because malware or other malicious traffic could spread like wildfire across the overlay and be hidden from the security tools attached to the physical network. There's an expression that you can't secure or manage what you can't see, and that's certainly true for overlay networks today.

Bringing the two environments together using traditional management models like CLI would be like trying to compute all the algorithms in an autonomous vehicle manually. People can't work fast enough to process huge volumes of data, analyze it and take action on the insights to make it practical. That is why the task is turned over to machine-learning systems. Similarly, with a physical network, trying to maintain an intended state is hard enough to do with a single network. Bring in the virtual overlay and all its dependencies, and the task would be so monumentally difficult that it's practically impossible, even for the largest network teams.

How It Works

Apstra's intent-based operation works off a closed-loop model where the intent is continuously validated. Virtual overlays introduce VXLAN segments that are used in conjunction with VLANs to segment virtual machines and containers in data centers at a more granular level. When these resources are put in motion and spun up and down dynamically, it becomes very difficult to maintain specific policies, such as "all workloads in VLAN1 are to be assigned to a specific VXLAN segment." Intent-based solutions continually gather data and automate the reconfiguration.

Also, Apstra's AOS self-documents, repairs itself and can maintain security. The term "intent-based security" is often bandied about, but that's more the effect of being able to understand, create and maintain policies in highly dynamic environments.

This latest release of AOS automates the full lifecycle of VXLAN-based, layer two network operations within, but also across racks, which is crucial today because east-west traffic flows are dominating data centers. The growth in east-west is driving the need to migrate from legacy, multi-tier, layer two networks to more dynamic and scalable, layer three leaf-spine architectures with an agile layer two overlay. Doing this with legacy configuration methodologies, such as scripting or CLI infusion, would require extensive application testing and possibly modification to account for the changes. Apstra's closed loop increases agility, so the transition to leaf-spine can be made without any modifications at the application layer.

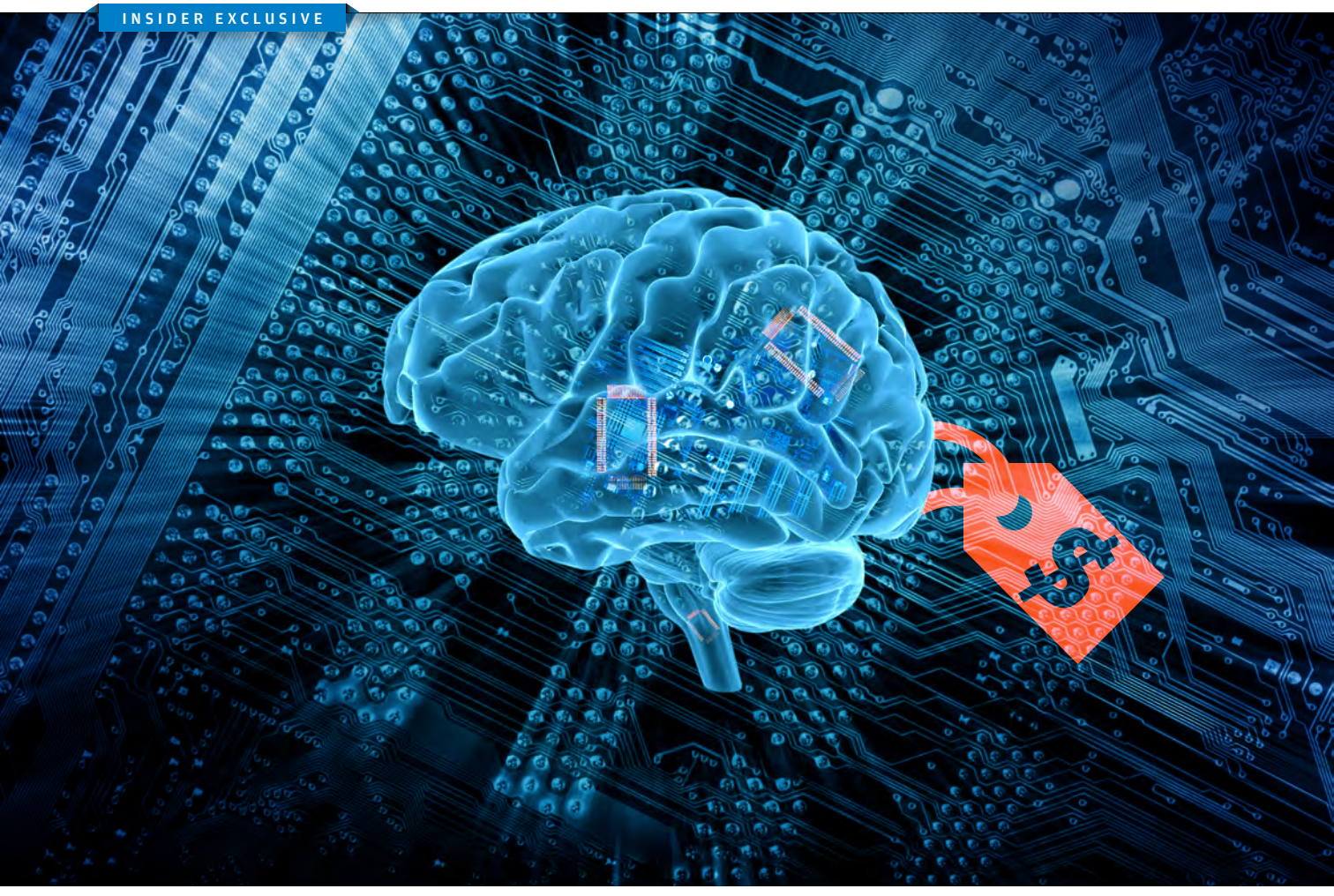
In a world where digital transformation is running amok, the infrastructure teams, including network operations, must find a way to respond to line-of-business requests faster. Intent-based networks reduce the amount of downtime caused by human error (still the largest cause) and cut operational expenses. They also increase network agility.

Digital businesses need to move with speed, but they are only as agile as the least-agile IT component. And that today is the network. Apstra's AOS 2.0 now delivers agility across the physical—virtual boundary, so now it looks like a single network instead of two distinct ones. ◆

ZEUS KERRAVALA *is the founder and principal analyst with ZK Research.*

In a world where digital transformation is running amok, the infrastructure teams, including network operations, must find a way to respond to line-of-business requests faster.

INSIDER EXCLUSIVE



How to Buy Intent-Based Networking Today

Network industry stalwarts and startups alike are jumping on the intent-based networking buzzword bandwagon. **BY BRANDON BUTLER**

CISCO MADE A BIG SPLASH last year when it revealed its vision for the future of networking: An intent-based networking system that allows users to specify what they want the network to do and management software that automatically orchestrates it.

Since Cisco's announcement, intent-based networking (IBN) has caught the networking industry's attention and has seemingly become the buzzword-du-jour. Some see it as a logical evolution of advanced network automation. Others believe it's a fundamental shift in how enterprises use machine learning to autonomously manage networks. Meanwhile, all types of vendors, from stalwarts of the industry to myriad startups are jumping on to the IBN bandwagon.

Analysts who track this market say it is nascent. Cisco says it has some IBN functionality in its Nexus line of switches and is rolling out intent features in its Catalyst line. Many vendors, particularly startups, offer parts of an IBN system.

"Make sure you understand what the vendor means when they say they offer intent-based networking," recommends IDC data center networking analyst Brad Casemore. "Interrogate them a bit, find out what they're proposing, whether it's applicable to your environment, how it will integrate in your environment and whether your staff can pick it up and run with it."

Refresher: What is Intent-Based Networking?

For an in-depth assessment of what intent-based networking is, check out Network World's explainer here. Research firm Gartner has defined intent-based networking systems as having four components:

- **Translation and validation:** This refers to the ability of IBN to translate what a network administrator wants the network to look like into actions the software takes to enforce those policies.
- **Automated implementation:** IBNs automatically create the desired state that has been requested by the network administrator.
- **Awareness of state:** A key component of an IBN is its ability to have a deep understanding of the state of the network and everything happening inside it.
- **Dynamic optimization and remediation:** IBN adapts to changes in the network to maintain the desired state of the network.

Here is a list of some of the different ways end users can begin using IBN systems today.

Cisco's Dual Approach

Cisco is integrating intent-based networking functionality into two of its product lines: Both the campus Catalyst switch line and the data center Nexus products. The announcement just before Cisco Live was all about new Catalyst 9000 switches that when combined with new functionality in the company's Digital Network Architecture (DNA) management platform will allow users to create an IBN that includes policy creation, provisioning and verification. Cisco says some of this functionality is available, and other features will be rolling out.

Cisco also has an IBN strategy for its popular Nexus data-center switches. Cisco's director of product management Mike Cohen says when customers combine Cisco's Application Centric Infrastructure (ACI) — its flagship software defined networking product — with its Tetration network analytics and visibility platform, then they get IBN functionality. He says ACI is fundamentally a way for users to automate the orchestration of their network.

"It allows users to describe the security policies, the connectivity policies your apps need, and that's what it will automate across the network," he says.

Tetration, the advanced network analytics product, can be used with ACI to monitor the network. "Tetration is really good at learning and discovering the application intent," Cohen says, adding that the analytics system uses sensors placed throughout the network to capture packet-level information about workloads running on the network. "ACI lets you identify the policies you want, Tetration can figure out the intent, based on observing the behavior pattern of the network."

VIDEO: The 10 Most Powerful Companies in Enterprise Networking
See what puts the top 10 heavyweights in the enterprise networking space at the very top of their market.

Juniper jumps on IBN

Some Cisco competitors are jumping in on the intent-based networking market, too. Juniper's CTO of engineering Kireeti Kompella argues that the company's open source Contrail software-defined networking controller has IBN-like functionality.

"The ability to express what you want at a high level, and then have automation implement that policy, that takes a huge burden off the operator," he says.

While that may not be a full-fledged IBN system, he argues that it meets most of the definitions of IBN as defined by Gartner. Juniper markets Contrail as working across any network hardware and OS models.

To comment on this story, visit Network World's Facebook page.

Apstra: An Original IBN Startup

Even before Cisco's entrance into the IBN market, some startups were already talking about the idea of allowing users to specify their intent and having a software platform orchestrate it.

Apstra, a startup founded in 2014 that released its first product in July

> **Make sure you understand what the vendor means when they say they offer intent based networking.** Interrogate them a bit, find out what they're proposing, whether it's applicable to your environment, how it will integrate in your environment and whether your staff can pick it up and run with it.
>
> **BRAD CASEMORE,** DATA CENTER NETWORKING ANALYST, IDC

of 2016, claims to be one of the original IBN companies that was developing this functionality before Cisco's announcement. Apstra CEO and Founder Mansour Karam likens the emergence of IBN to a self-driving car: The self-driving car looks just like any other car, but it's equipped with state of the art sensors and automation technology that offer the driver an autonomous experience.

"We've built a layer of software, an OS for your network," Karam explains. "It runs and operates the network in an intent-driven way. It delivers on the autonomous experience."

The company has developed the Apstra Operating System (AOS), which controls and orchestrates network resources. Apstra also has a distributed data system that monitors the current state of the network and analyzes changes that are being implemented in it. AOS is hardware-agnostic, meaning it's an overlay software that can run on any hardware vendor's products or on whitebox switches. AOS can design templates for what the network should look like, build blueprints for how that vision should be implemented, then control the resource and device management to deploy the configuration. As it does so, AOS gathers telemetry data to perform real-time analytics about the state of the network and to detect anomalies that are inconsistent with the desired network policies.

Startups Focusing on IBN Components

There is another set of startups that offers important components of an IBN system. David Erickson, co-founder and CEO at Forward Networks says he breaks the IBN market into two categories. One is the creation and enforcement of network configurations, which instantiate the desired policy on the network. He says this is primarily for net-new, so-called "greenfield" deployments of IBN, and companies like Apstra and Cisco are working on this.

The other side of the IBN coin, he says, is modeling the network to understand how the network is operating and how changes will impact it.

Forward Networks, which was founded in 2013 and has received multiple rounds of venture financing, creates a software copy of a customer's network. Using this copy, customers can test a potential change to the network before implementing it. They can verify that changes have been made and roll back changes that cause a problem. This can be done to existing networks, allowing customers to get a taste of IBN functionality without a full-fledged IBN deployment, he says.

Veriflow is another company that creates a predictive model of the network and analyzes all possible traffic flows through the network. "It's like a Google Maps for your network," says CEO James Brear. This allows users to verify and ensure that their business intent is being met in their network, and the company markets its products as helping to prevent outages and vulnerabilities.

"Verification is a critical part of the picture," Veriflow co-founder and CTO Brighten Godfrey says. "It may be the most important part because in a sense, if you automate without verification, then you're increasing your risk by taking actions faster than you know what is happening in your environment."

Both Forward Networks and Veriflow, though, do not claim to offer all the components of IBN; namely they do not yet offer an orchestration software that will implement intent-driven network policies. ◆

BRANDON BUTLER, *formerly a* Network World *senior editor, is an IDC analyst covering Ethernet switching, routing, wireless LAN and newer tech such as SDN and SD-WAN.*