LOGICALIS
Architects of Change

White Paper

Intent-based Networking

How it works. Why you need it.
Where to get it.

CISCO Partner
Global Gold Certified

Most users and more than a few IT professionals have been yelling at their networks for years. Users can't log into an application that worked fine yesterday. Network technicians spend days troubleshooting the same outages that they spent days solving last week. Sales executives preparing for a meeting with an important client discover they can't access their Salesforce account.
For all that yelling, until recently, networks just sat there. There was a communications gap. Users spoke business productivity and networks spoke command line interface (CLI) configurations. Manually troubleshooting network issues, as a result, have caused major frustrations among IT Professionals.

Software defined networking (SDN) launched a transformation of network infrastructure from hardware-centric, manually-operated networks to software-centric and fully-automated networks. With SDN, networks have been given the ability to take direction, verify policies, and keep you continuously updated on their progress.

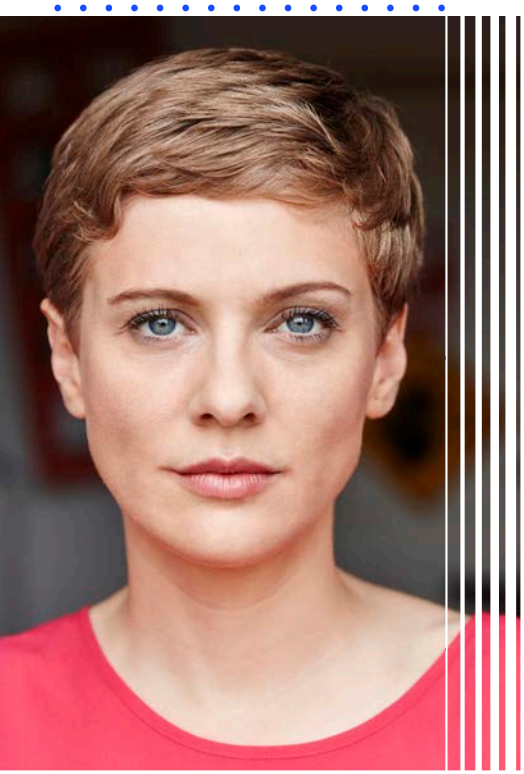
Intent-based networking (IBN) builds on SDN and adds context, learning, and assurance capabilities that can comprehend business and application requirements and translate them into network and security policies. IBN enables enterprise networks to follow complex instructions, including the ability to distribute and automate changes throughout the entire system. This promises to fundamentally change the relationship between users, IT professionals and their ever-expanding network environments.

How It Works

Intent-based networks capture business intent and use analytics, predictive analysis, machine learning, and automation to continuously and dynamically apply and ssure application performance requirements. They are designed to automate user, security, compliance, and IT operations policies across multiple domains, including campus, branch, WAN, data center, cloud, and service provider.

Integrated with other IT and business systems, intent-based networks will enable organizations to:

- **Adapt to new application and service requirements:** An intent-based network makes it easier to deploy new applications, prioritize applications, and integrate with IT services and processes through APIs.
- **Reduce risk:** Through continuous gathering of telemetry, combined with machine learning, you can provide context to identify and neutralize security threats, and proactively address performance issues.
- **Increase operational efficiently:** Applying automated policy across users, devices, branches, WAN, campus, data centers, and clouds helps you respond faster to business needs.
- **Support exceptional customer experience:** Intent-based networks improve the user experience by translating desired operational Service-Level Agreements (SLAs) and applying them consistently across the network.



Why You Need It

Traditional networks are no match for the increasing demands that global business and technology trends are making on corporate networks. For example:

700M

edge hosted containers will be online by 2021[1]

14.6B

IoT devices will be connected to the network by 2022[3]

50%

of workloads will be outside the enterprise data center by 2021[2]

42%

annual growth is expected in mobile traffic from 2017 to 2022[3]

12X

increase is expected in AR and VR traffic by 2022[3]

Against this tsunami of demand, traditional networks are already struggling with:

- A lack of network visibility
- Underperforming WANs
- An inability to control network access and segment traffic
- A lack of analytics to proactively address issues
- An inability to respond quickly to changing business needs

Software defined networking only provides part of the solution. IBN adds translation and assurance functionality. In other words, an administrator, or even an authorized application, tells the network an intent, and the intent-based network translates that purpose into policy and device configurations that are automatically deployed, validated, and monitored.

Consider this example: an organization needs to deploy new IoT devices across several manufacturing plants—a process that involves creating new virtual local area networks (VLANs), adding access lists and configuring ports across the entire network.

With IBN, administrators define the business intent: “I want these IoT devices to only be accessible to this application and/or server.” Then, the IBN platform automatically interprets that intent into IT policies, defines the configuration changes needed across different network devices, applies those changes and constantly monitors them—a process that takes minutes instead of hours or days.

For those looking to increase efficiency and decrease risk, this is huge. According to Gartner: “We believe a full IBNS implementation can reduce network infrastructure delivery times to business leaders by 50 percent to 90 percent, while simultaneously reducing the number and duration of outages by at least 50 percent.”

The Functional Building Blocks of IBN

There are three functional building blocks for IBN:

1. **Translation:** Translation literally translates intent (business or technical) from a network administrator into actions or policies and checks their integrity. Endpoints on the network are identified and placed into groups so that policies can be applied to them. From a security standpoint, this is useful for segmenting the network traffic of certain devices (like IoT and mobile) from other mission-critical devices on the network.

2. **Activation:** Activation instantly implements configuration changes across the network (both physical and virtual devices) with minimal errors, using automation and/or network orchestration. For example: automation allows policy updates to be rolled out in minutes with a single command, thereby minimizing the impact of network changes.

3. **Assurance:** Assurance continuously monitors the network to ensure the original intent is being met, proactively identifies any degradation of performance or accessibility, and recommends corrective action. Recent studies have shown that IT administrators spend 43 percent of their time troubleshooting network issues, and 4x more time collecting data than they do analyzing and resolving issues. Because IBN platforms continuously collect data from the network and store it for troubleshooting, an intent-based network assurance solution can greatly reduce the time spent troubleshooting network issues.

The Benefits of IBN

Before we talk about how to begin to implement IBN, let's take a deeper dive into the benefits it promises:

Increased business agility — The abstractions and the fully automated nature of an intent-based network supported by open APIs ensures that the network is responsive to the dynamics expected in a digital economy. New applications can be quickly on-boarded in the network wherever most appropriate (the enterprise data center, a Virtual Private Cloud (VPC), or even consumed as-a-service).

The capability of an intent-based system to capture and act upon the intent of a new application simplifies the process of providing connectivity and security to such applications. Sophisticated integrity checks, automated configuration of the network policies relating to the application, and ongoing assurance allow infrastructure teams to confidently support the rapid pace of application development.

Improved operational efficiencies — The functionality offered by an intent-based network promises operational efficiencies and even reductions in operating expenses (OpEx). Network operators will be able to significantly reduce the time spent on network design, implementation, testing, and troubleshooting. An intent-based network is fully model driven: Operators can express intent in an intuitive manner with easy translation into model-based policies.

Once the intent is captured in a model, sophisticated consistency and integrity checks can be applied to ensure that new intent is consistent with previously expressed intent, or that intent expressed by different operational groups is consistent.

As a result, translation of model-based policies into standard network element configurations can be fully automated, increasing the consistency in the network. IBN offers a stark simplification of the conventional process of manually deriving command line interface (CLI) configurations for a policy for every network element in the architecture, repeating this manual process every time a new application or device type is on-boarded, and ensuring that any configuration changes do not break or violate previous policies.

The level of abstraction and automation in an intent-based model also supports the anticipated scale increases in a digitized network architecture. For example, intent and policy are typically expressed at a group level. Grouping applications, devices, and users and expressing intent with respect to associated groups supports a simplified operational model. As new employees join the company or application tiers scale out, new endpoints can simply be created within existing groups, thereby leveraging previously expressed intent and policies.

An intent-based network also reduces—or in some cases eliminates—complex troubleshooting scenarios that occur in networks today. As assurance processes verify the alignment of network configuration with intent, they can surface potential problems to identify the root cause of emerging issues quickly and efficiently. Standard changes to commonly recurring issues can even be automated while preserving the integration with IT Service Management (ITSM) systems, potentially yielding further significant OpEx savings.

IBN can drive transformation from an operator-curated knowledge base (i.e.: a help-desk tool or configuration management database) to a systemic or machine-learned knowledge base that covers “preapproved” changes as the path towards closed-loop automation.

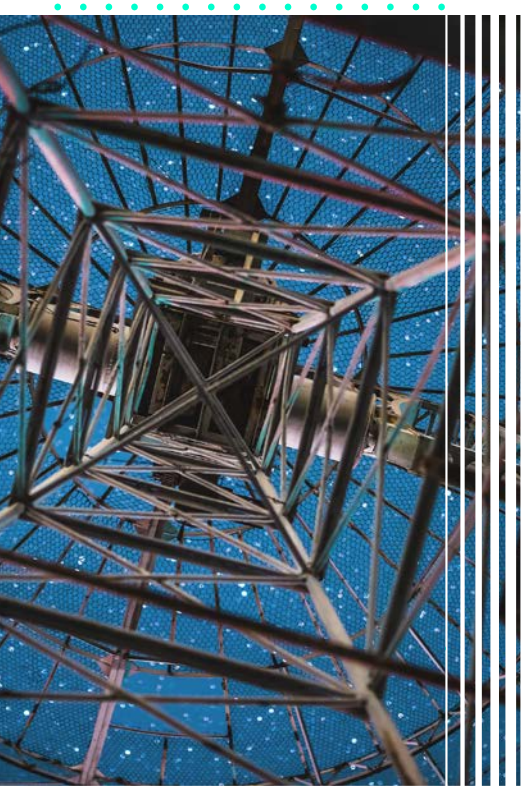
Continuous alignment of the network with business objectives — An intent-based network allows the desired behavior of the network to be expressed in abstract terms, putting the emphasis on the what instead of the how. This capability helps ensure the network is always fully aligned with business operations. Previously, the translation of business objectives into device configurations was a process performed by a highly skilled engineer.

For example, a business objective—application X is business critical—required in-depth knowledge of every network element to filter application X traffic, and configuration of the respective Quality of-Service (QoS) policies at every relevant node in the network. With IBN, the same expressed intent is translated into policy, and the configuration of the network elements is fully automated.

The feedback mechanism built into the IBN checks that the derived policies are always honored and can help automatically adjust the network configuration if the network is no longer aligned with the expressed intent.

Better compliance and security — Improved protection and rapid threat containment are primary benefits of IBN. Each of the building blocks in an intent-based network helps to substantially improve the overall security and compliance of the network through continuous alignment with security and compliance policies.

Alignment is achieved by making security an integral part of each of the IBN functional areas and delivering closed-loop policy enforcement and threat containment. Security policies can be expressed by the security operations team independently of other operations groups.



The integrity verification functions in the architecture check that policies are not counteracting each other. Also, the ongoing telemetry and assurance functions provide an up-to-date picture of the state of the network that is essential for security and regulatory compliance reports. Advanced segmentation techniques protect the availability of core assets by preventing the spread of lateral infections between endpoints, users, and applications.

Reduced risk — The abstractions, automation, and assurance introduced with IBN promise to reduce the overall operational risks of providing communication services between users, devices, and applications. Manual, error-prone CLI-based processes are minimized in an intent-based network.

For example, access control lists (ACLs) are typically configured throughout the network to filter traffic for security or traffic control purposes (QoS, path determination, etc.). Many ACLs have grown over time, and making any modifications risks the creation of a security hole or may counteract previously desired policies.

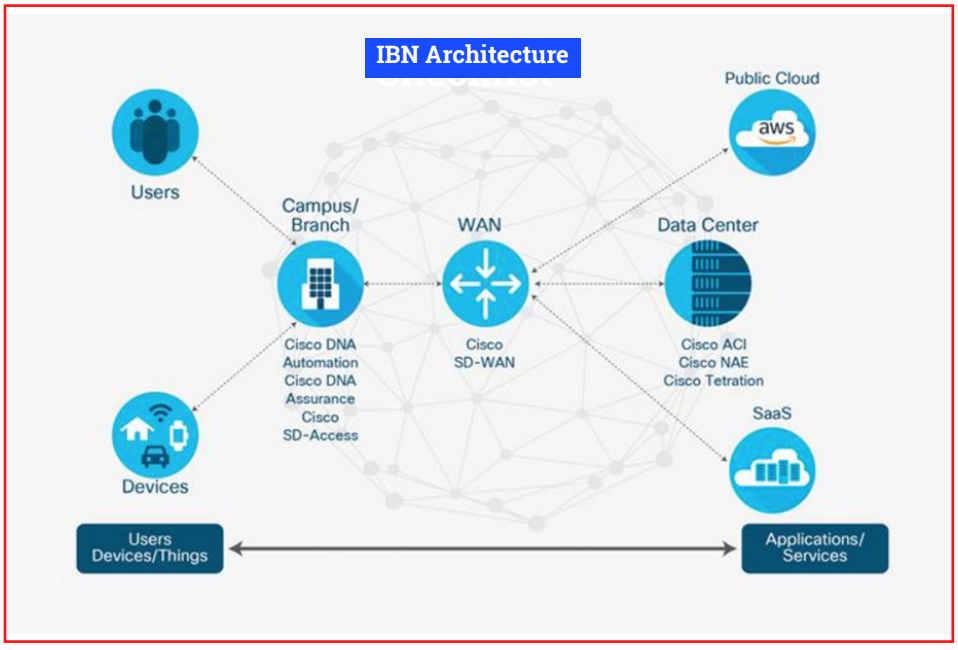
The predictable and coherent expression of intent-based policies in IBN, combined with the ability to apply consistency and integrity checks, and their standardized translation and deployment into network element configurations all increase consistency in the network—even in the face of multiple operator groups and disparate technologies.

Intent-based networks also significantly reduce the risk of network outages by predicting the impact of changes to the systemwide network state. For example, consider a situation where a primary site is functioning properly, but a secondary site, accessed only in the case of disaster recovery, is not. An IBN system would be able to identify such a latent misconfiguration and flag it to an operator (or correct it automatically) to avoid a potential network outage.

Inter-related solutions

IBN architecture consists of several inter-related solutions that span all networking domains: data center, campus, branch, WAN and multi-cloud. They are:

- Modern network hardware supporting automation and policy management
- Assurance – the IBN management platform
- Identity and Policy Management – Software Defined-Access (SD-Access)
- WAN Policies, SLA and redundancy – Software Defined-WAN (SD-WAN)



Small Steps

Very few organizations are able to take on IBN in one jump. A good place to start is with legacy networking servers and controllers that are approaching end of life. Upgrading them with new systems that support automation through the latest Internetworking Operating System (IOS-XE) helps you establish enhanced functionality that will allow you to migrate into IBN as resources allow. You can even update select segments that will run alongside legacy systems until you are able to upgrade them in turn.

It is also possible to implement aspects of IBN that provide short-term cost savings and increase operational efficiency. Starting with the Assurance building block, for example, provides broad and deep monitoring capabilities that will pay dividends immediately in terms of reduced time for troubleshooting. Assurance will also give you visibility into the network as you take the next steps toward IBN, and it works the same across both wired and wireless networks.

A logical next step once you are comfortable with Assurance is the implementation of SD-Access which allows you to push specific intent to the network and use automation to configure and activate the necessary devices.

If you are moving data centers to a third-party cloud or using a software-as-a-service (SaaS) app like Salesforce, SD-WAN might be the place to start. You know you will need reliable and redundant access over the Internet, and you also know you can't control the Internet. With SD-WAN, you can use multiple circuits and let SD-WAN decide which circuit is performing better at any given time. No need to manually configure load balancing at the command line. Once SD-WAN determines the best circuit, it will automatically configure the appropriate devices for you in the background.

Conclusion

While IBN will not perform magic tricks, it has the potential to translate intent into action. For example, your CFO will be able to tell the network your company is being audited and, when the auditors arrive, they will need authenticated secure access to the appropriate financial documents. IBN will translate this intent, implement the necessary policy and assure that the auditors have the required access to designated financial information, and nothing else within the network.

IBN is rapidly evolving. All the technologies and processes required to implement intent-based networks are becoming more robust and as they do, the scope and capabilities of IBN will expand. Key features to look forward to include:

- Continuous service alignment
- Automated provisioning of devices, self-diagnosing and dynamically updated networks
- Policy driven, automated, self-optimizing networks
- Automated and predictive insights

Organizations that launch an IBN initiative today will be exposed to the inevitable risk associated with any rapidly evolving technology. By starting early, however, organizations that commit to climbing the IBN learning curve will gain an important head start over competitors that continue to rely on manual networks.

Where To Get It & How To Begin

The scope of IBN can seem daunting, but it is possible to develop a roadmap that starts where you are and allows you to proceed step-by-step at a pace that suits your needs and fits your budget. Importantly, a well-designed roadmap ensures that you avoid functional cul de sacs and the need to backtrack and start over in another direction.

Logicalis offers IBN Workshops to organizations interested in exploring how IBN can work for them. Conducted by Logicalis IBN/networking experts, the workshops are high-level and consultative and are designed to foster an open and honest discussion about an organization's technological state as well as its future technology and business goals. Representatives from both the business and technology side of an organization are asked to attend. Basically, anyone from the CEO down who is tasked with making the company a more nimble, agile organization is welcome. Healthy debate is encouraged.

The workshops offer an organization's business and tech teams an opportunity to discuss objectives in a comfortable offsite atmosphere where they have access to IBN experts as questions arise. Attendees have said that one of the key benefits of the workshop is the ability for business and tech leaders to brainstorm together.

The workshops are also intended to familiarize Logicalis with an organization's goals and objectives and develop insights into how incremental implementation of IBN can help accomplish them. After the workshop, Logicalis develops a roadmap with clearly defined phases and a rough order of magnitude of pricing.

Logicalis + Cisco: Taking business transformation seriously

An award-winning, Cisco-certified partner, Logicalis is trusted to deliver the expertise you can count on to transform your organization and enable business outcomes. We bring unrivaled knowledge, skills and experience to deliver IoT, Cloud and security solutions that maximize existing investments, meet your needs and drive confidence.

What we can do for your organization?

Contact Logicalis to learn how we can help.

Visit
www.us.logicalis.com

Call
866 456 4422

LOGICALIS
Architects of Change

CISCO
Partner
Global Gold Certified