Intent-Based Networking

Building the bridge between business and IT

Introduction

Networks are at the heart of the unstoppable evolution to a digital economy. Digitalization is changing the way businesses, partners, employees, and consumers interact at an unprecedented pace. Products and services can be customized, ordered and delivered at the click of a button using web-based applications. Business data can be acquired, analyzed and exchanged in near-real time. Geographic boundaries between businesses and consumers are diminishing. And the network is at the center of communication to and between the applications driving the digital economy.

Increasingly, traditional enterprise and data center network architectures are being stressed to adapt quickly to these dynamic requirements. Applications are moving to public-, private-, and hybrid-cloud environments and are now consumed as services, blurring the well-defined boundaries between the enterprise's network and untrusted domains. Developers, empowered by the movements toward open-source software, containers, microservices and agile development processes, can bring applications from concept to production in days rather than months or even years. Employees and customers expect connectivity from anywhere, on any device, to access information at any time. And increasingly, sensors and autonomous devices are being connected as the Internet of Things (IoT) expands. At the same time, cyber-threats across the network are becoming more sophisticated and dangerous to the brand reputation and financial welfare of all organizations.

Traditional enterprise and data center network architectures and their respective operational procedures need to evolve to keep pace with these trends. Specifically, the new network needs to:

- Enable new digital business initiatives, not hold them back. It needs to have the flexibility to quickly change in alignment with rapidly changing business objectives.
- Be easier to configure, operate and maintain in the face of growing scale and complexity. Current operational models are not scalable or sustainable.
- Provide full visibility in terms of how a network is operating and providing assurance that it is supporting the desired business initiatives and achieving compliance. Identify any discrepancies and recommend fixes
- Identify and neutralize security threats before they cause harm. Multi-cloud, IoT and mobile adoption open up new threat vectors that the network needs to constantly protect against.

Contents

This is driving the IT industry's growing interest in more intelligent networks, commonly termed "Intent-based Networks".

Intent-based networking (IBN) offers a significant paradigm shift in how networks are planned, designed, and operated. In the past, tools were not available to declare intent and translate it into the device-level configurations required to realize a desired outcome. Instead, the network designer or operator had to manually derive individual network-element configurations to support the desired intent, such as, "I want these servers to be reachable from these branches; therefore, I need to configure specific VLAN, subnet, and security rules on each device in my network."

Intent-based networking solutions enable conventional practices that require the alignment of manually derived individual network-element configurations to be replaced by controller-led and policy-based abstractions that easily enable operators to express intent (desired outcome) and subsequently validate that the network is doing what they asked of it.

Scale, agility and security demands associated with digital transformation require that element-by-element network configuration be replaced by automated systemwide programming of network elements with consistent intent-based policies. Furthermore, the contextual analysis of data before, during, and after deployment enables continuous verification to help assure that the network is delivering the desired outcome and protection at any point in time. Continuous gathering of telemetry and other forms of data from a multitude of diverse sources provides a rich context of information to optimize a system and ensure it is secure.

Intent-based policy extends beyond the access control of clients or applications. It broadens to expressions of the desired user experience, application prioritization, service-chaining network functions that need to be applied to an application flow, or even operational service-level agreement (SLA) rules, such as, "I want to deploy only golden images on my network devices."

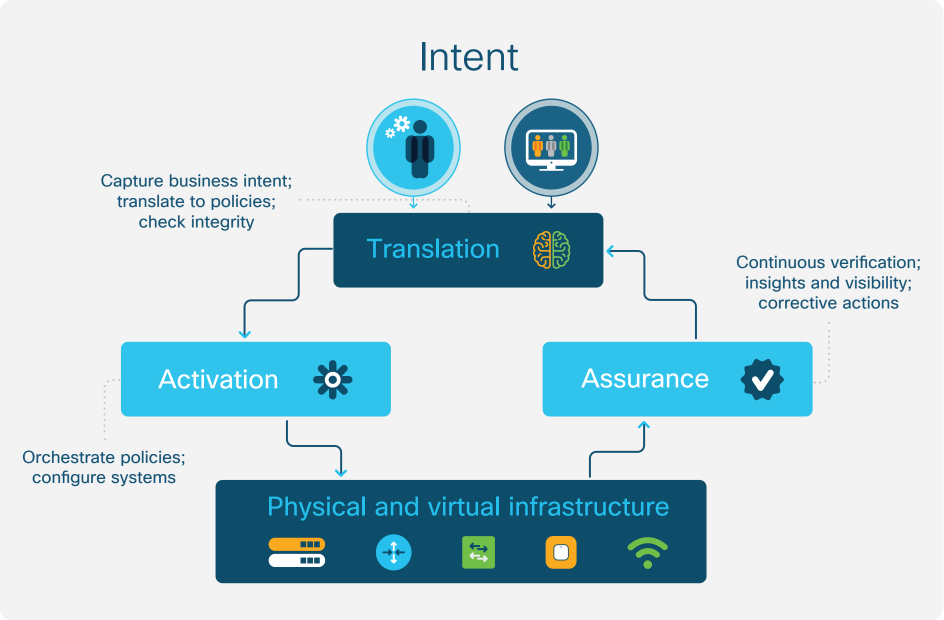
> **“Gartner sees the biggest benefits from IBNS are improving network agility and availability, and supporting unified intent and policy across multiple infrastructures.”**
>
> **–Gartner, 2017**

Gartner, Innovation Insight: Intent-Based Networking Systems, Andrew Lerner, Joe Skorupa, Sanjit Ganguli, 07 February 2017

In Cisco’s view, a complete intent-based network (Figure 1) needs to deliver on a number of essential functions:

- **Translation:** The Translation function is about the characterization of intent. It enables network operators to express intent in a declarative and flexible manner, expressing **what** the expected networking behavior is that will best support the business objectives, rather than **how** the network elements should be configured to achieve that outcome.
- **Activation:** The captured intent then needs to be interpreted into policies that can be applied across the network. The Activation function installs these policies into the physical and virtual network infrastructure using networkwide automation.
- **Assurance:** In order to continuously check that the expressed intent is honored by the network at any point in time, the Assurance function maintains a continuous validation-and-verification loop. Context derived from telemetry data is used to check alignment of operation with intent.

Figure 1. Intent-based network functions


Intent
Capture business intent; translate to policies; check integrity
Translation
Continuous verification; insights and visibility; corrective actions
Activation
Assurance
Orchestrate policies; configure systems
Physical and virtual infrastructure

This paper provides Cisco’s point of view on the evolution toward intent-based networking by outlining the vision for it and its architecture and benefits for network strategists and architects. The paper provides an overview of the main functional building blocks of an intent-based network and offers concrete examples from both a data center and an enterprise networking perspective.

Intent: Bridging the gap between business and IT

Today, implementing business requirements requires a lot of human interpretation and manual intervention to ensure the IT systems are meeting these needs. In most cases the process is lengthy, very resource intensive, and error prone. It does not meet the criteria for an agile digital business environment that has increasing numbers of systems, devices, applications, and services that need to be served.

Intent-based networking captures the business intent, in business language, and translates this intent into IT policies that can be applied and constantly monitored across the network. Figure 2 provides examples of the difference between intent (the "what") and execution (the "how").

Figure 2. Examples of intent expressions

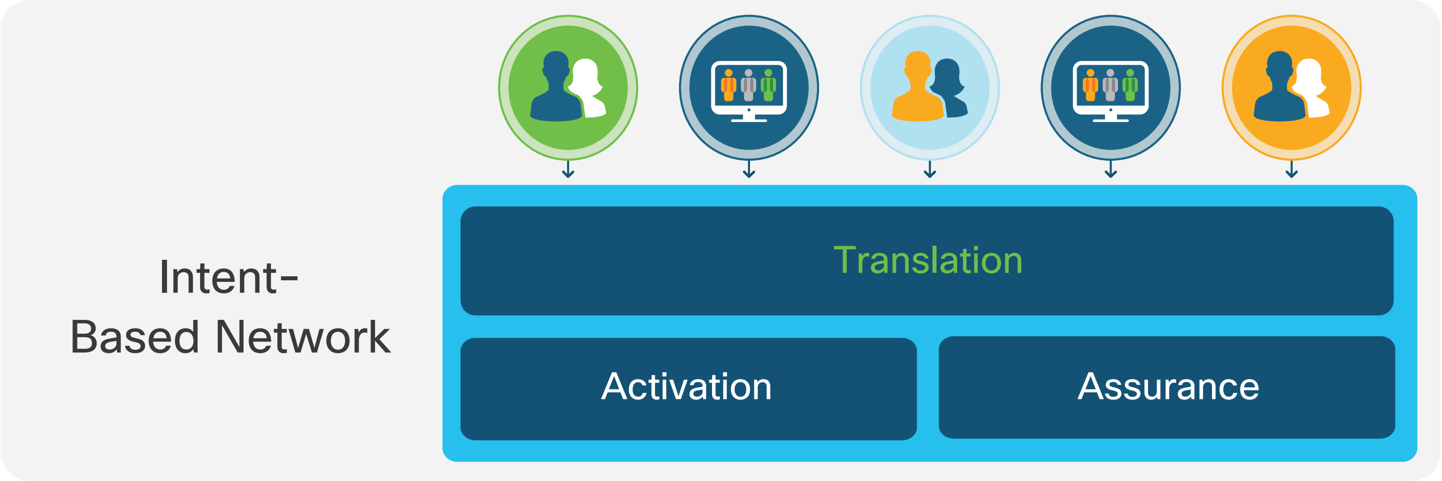
Intent	I need to scale out my application database	I have scheduled a telemedicine session at 10am	I am rolling out a new IoT app for factory equipment monitoring	I need to deploy a secure multi-tier application
Execution	Extend network segments; update load balancer configuration; configure QoS policies	Create HD video connection; prioritize with E2E QoS; validate performance; keep the communication safe; tear down connection after call	Create a new segment for all factory devices to connect to the IoT app; isolate from other traffic; apply SLA; validate SLA; optimize	Provision multiple networks and subnets; configure ACLs and firewall rules; advertise routing information

With an intent-based network, the administrator determines the 'what,' and the system then figures out the 'how'." –Zeus Kerravala

Building blocks of an intent-based enterprise network

An intent-based network provides three principal functional building blocks (Figure 3): capabilities to capture intent, functions to automate the deployment of the expressed intent throughout the network infrastructure, and the ability to assure that the desired intent is being realized.

Figure 3. Building blocks of Intent-Based Networks (IBN)



Translation

Translation involves several functions in an intent-based model. One or more operators, or groups of operators, have the capability to characterize their desired intent. This may take the form of an easy-to-use graphical user interface, an abstracted model (such as YANG or JSON/XML) that is intuitive and related to the business objectives, or even a predefined syntax or language. It may be defined by application developers as part of a continuous integration/continuous delivery (CI/CD) process, or in the future, it may even be achieved through text-to-speech expressions, in which operators verbally speak intent and the intent-based system executes and provides verbal or other feedback. This abstract and business-near expression of what the network should do differentiates an intent-based approach from traditional network architectures.

Another capability of Translation is to harmonize the captured intent into a common model-based policy (MBP), often with the help of a controller-based architecture. Intent expressed by various input mechanisms, potentially across multiple network domains, is translated into such standard MBPs—a foundational step to leverage automation and allow sophisticated consistency and integrity checks to be applied.

An important challenge relates to moving from a traditional network deployment to an IBN deployment. In this case there are already policies in affect in the current network, but the network operator may or may not have a list or full visibility of all of the currently deployed policies. Therefore, it is important to perform automatic host discovery and policy discovery to identify the policies in operation, to provide the operator with full visibility of all the running policies for review, and then to activate the desired policies automatically in the IBN deployment.

Activation

Activation functions ensure that the derived MBPs are disseminated throughout any of the relevant network domains. The physical or virtual network functions in an IBN may be managed in different operational domains (data center, WAN, branches, campuses) by the same or different operational teams. The orchestration function in an intent-based network allows for the dissemination of MBPs into the relevant domains—meaning that policies can also be limited in scope to particular parts of the network.

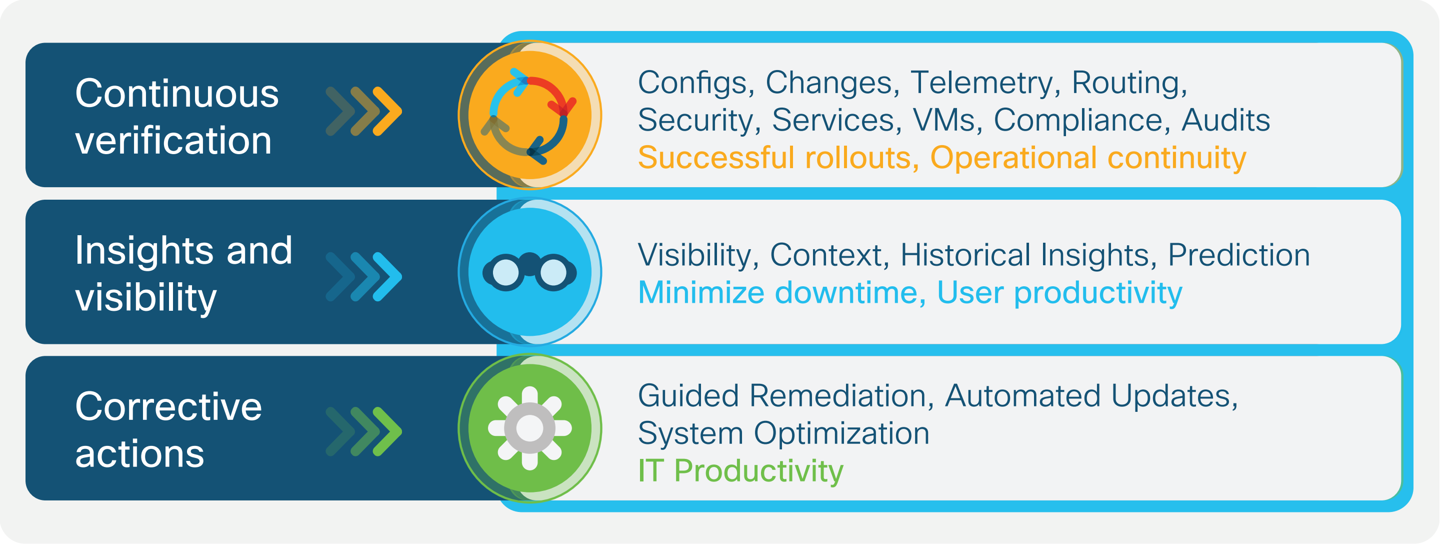
Activation may also employ additional functions to further derive the appropriate device configurations. A domain's controller can correlate the information about the network elements, their capabilities, and the topology with the expressed MBPs to establish the appropriate device configurations. Additional checks for consistency at the configuration level may also be applied before programming the network elements using standards-based APIs (such as Network Configuration Protocol [NETCONF] or YANG, or representational state transfer [REST]).

Assurance

Assurance is a critical function of intent-based networking. It uses contextual analysis of data to provide validation that the intent has been applied as intended, and also continuously verifies that the desired outcomes are actually being achieved. The Assurance capabilities of an intent-based network cover three main aspects, also highlighted in Figure 4:

- **Continuously verify the IBN system behavior before, during, and after deployment:** Check that the system behavior is aligned to the expressed intent at any point in time. This capability requires ongoing observation of the network element states and events. Intent-based telemetry data specifically measures the performance of the expressed intent, and is continuously collected and reported to the IBN Assurance functions. Assurance algorithms, ranging from formal mathematical models to approaches based on telemetry and machine learning, guarantee that the network state and behavior are coherent with the desired intent at both the domain and cross-domain levels.
- **Derive insights based on analytics (correlation of events and leveraging machine learning and artificial intelligence [ML/AI]) for validation, understanding, and prediction:** In addition to verifying the current network state and its alignment with the expressed intent, assurance functions can derive more sophisticated insights and visibility into the behavior of an intent-based network. For example, they may predict any violations of the expressed intent prior to changes being applied, understand or forecast trends, identify anomalies, predict and validate system-level network performance.
- **Leverage a closed-loop cycle to realize corrective action and optimization:** Anomalies, violations, and simple out-of-SLA (expressed intent) situations that are detected can be programmatically remediated leveraging the Activation building block to effect systemwide adjustment. An intent-based network thus enables a mechanism to automate the remediation of any intent-based policy violations, or to allow continuous optimizations to be automated to guarantee that the expressed intent is realized by the network at any point in time. Note that depending on the policy, the actions may be automatically executed or may be provided to the operator as recommendations, in which case the operator decides on execution.

Figure 4. Three main aspects of Assurance


Continuous verification
Configs, Changes, Telemetry, Routing, Security, Services, VMs, Compliance, Audits
Successful rollouts, Operational continuity
Insights and visibility
Visibility, Context, Historical Insights, Prediction
Minimize downtime, User productivity
Corrective actions
Guided Remediation, Automated Updates, System Optimization
IT Productivity

The main architecture, building block, and outcomes differences between a traditional network and an Intent-based network are captured in Table 1 below.

Table 1. Comparison of traditional and intent-based networks

Capabilities	Traditional network	Intent-based network
Architecture	· Device-by-device management · Unidirectional configuration · Nonprogrammable devices · Patchy network security	· Networkwide system-oriented management · Closed-loop automated configuration and assurance · Programmable physical and virtualized infrastructure · Security functions integrated systematically throughout the architecture · API-centric, model-based · Open hardware and software stack
Translation	· Ad hoc operator interpretation and ad hoc translation	· Yes, through intent capturing and translation system functions
Intent verification	· No support	· Yes, integrity and consistency checks
Policy support	· Limited, expressed by device commands	· Intent-based policies based on models
Activation	· Limited (scripting), device-by-device	· Automated, networkwide with controllers
Telemetry	· Limited support	· Extensive support
Assurance	· Manual, device-by-device	· Automated, full analytics with AI/ML or formal method support
Feedback loop	· Based on ad hoc, manual operator monitoring	· Yes, automated for either operator or system activation
Outcomes	· Limited, best effort business alignment · Complex and costly to manage at scale	· Continuous business alignment · Simplified, efficient management at scale

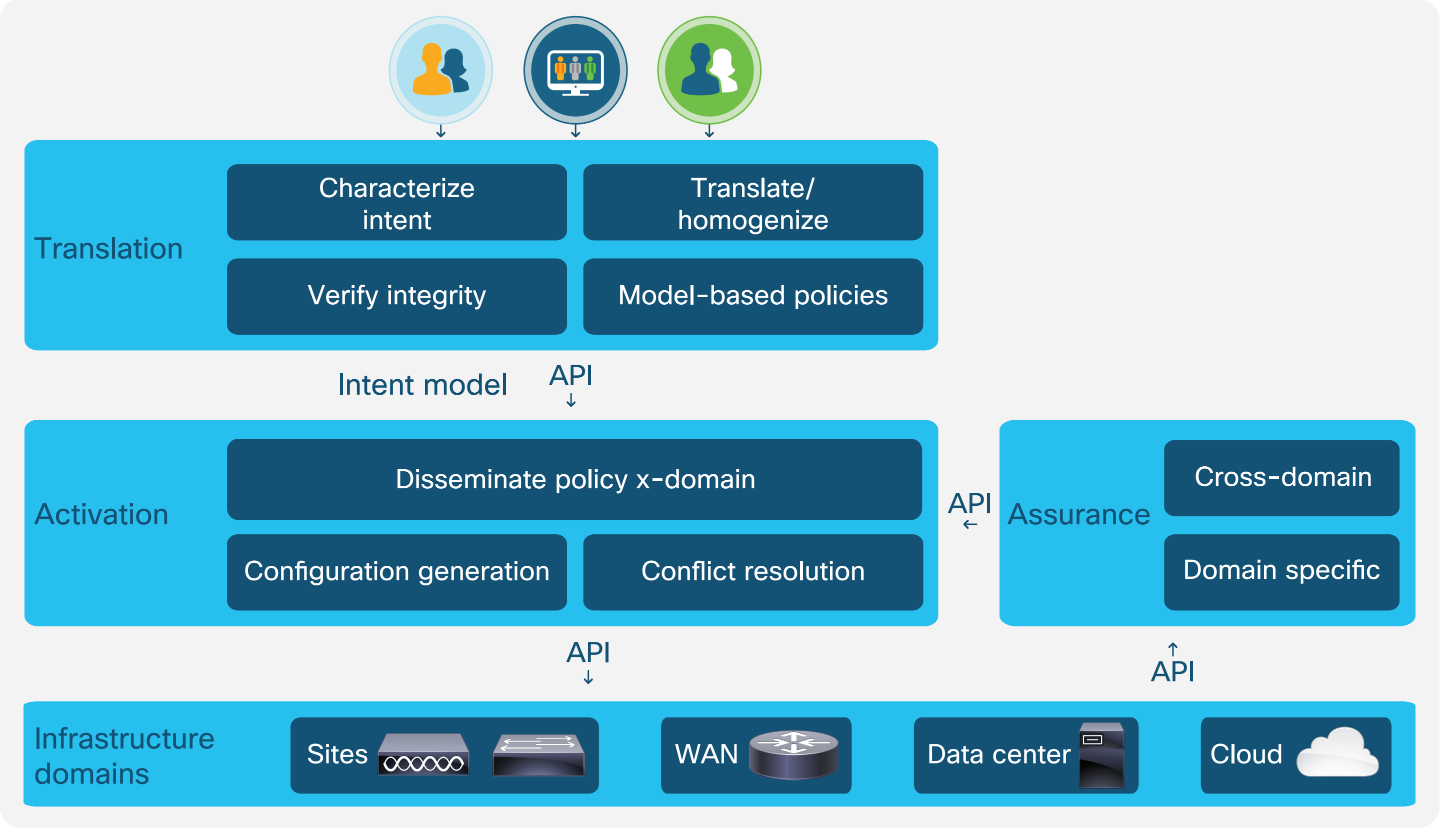
Intent-based networking in multi-domain environments

An enterprise's network infrastructure may be managed in different domains, separating the operational duties into campus and branch sites, WAN, data center, and the cloud. Applications hosted in the data center or cloud, as well as clients, may also have their own operational procedures, and thus be considered domains. In an IBN, one or more domains are expected to be governed by a controller, which provides a holistic view of the infrastructure and maintains a consistent state (configurations, software images, etc.).

The intent-based system accommodates this arrangement of network infrastructure into domains. Translation and orchestration capabilities are applied across domains, allowing for the characterization of networkwide intent-based policies across the campus and branch sites, WAN, data center and cloud. An orchestration function disseminates the captured policies to the relevant domains, which also enables restriction of some policies' scope by design. Automating the translation of the model-based policies into device-specific configurations, and instantiating these into the network infrastructure, is covered by the domain-specific controllers. IBN Assurance functions may apply to a particular domain to ensure adherence to the expressed intent-based policy. Additionally, Assurance functions operate across domains to check for compliance with the expressed intent networkwide and end-to-end (from application to application, regardless of where the apps are hosted).

Figure 5 illustrates additional functional details of the Translation, Activation, and Assurance building blocks of IBN, and how they relate to different infrastructure domains. The figure also highlights the feedback loop that sends insights gained by Assurance back into the Activation functions for ongoing optimization of the network.

Figure 5. Intent-based networking model and functional details



Benefits of an intent-based network

An intent-based approach to networking enables several benefits for business and IT leaders. These include improved business agility and operational efficiencies, better compliance and security, continuous IT and business alignment and reduced risk.

Increased business agility

The abstractions and the fully automated nature of an IBN 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 the intent of a new application in the abstract 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 IBN promises operational efficiencies and even reductions in Operating Expenses (OpEx). Network operators are expected to 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. Translation of model-based policies into standard network element configurations can be fully automated, increasing the consistency in the network. An IBN thus 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. Furthermore, the standardized and automated nature of IBN inherently supports a higher scale than traditional manual, non-automated processes.

Through its closed-loop design, an intent-based network also greatly reduces—or in many 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 before they occur, or can quickly and efficiently identify the root cause of emerging issues.

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 (manifested today in, say, a help-desk tool or configuration management database) to a systemic or machine-learned knowledge base that covers more and more “preapproved” changes as the path towards closed-loop automation.

Continuous alignment of the network with the business objectives

An intent-based network system allows the desired behavior of the network to be expressed in abstract, business-near terms: the **what** instead of the **how**. This capability helps ensure that the network is always fully aligned with the 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 hop in the network. In an IBN, that 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

While sometimes over-looked, improved protection and rapid threat containment are actually one of the main benefits intent-based networking can deliver. Each of the building blocks in an IBN helps to substantially improve the overall security and compliance of the network. Continuous alignment to intent related to security and compliance policies should be a core objective of IBN. It 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 function provide an up-to-date picture of the state of the network that is essential for security and regulatory compliance reports. Advanced segmentation techniques prevent the spread of lateral infections between endpoints, users, and applications to protect the availability of core assets.

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 system. Consider, for example, the case of traffic filters in the network. Typically, Access Control Lists (ACLs) are configured throughout the network to filter traffic for security or traffic control purposes (QoS, path determination). Many ACLs have grown over time, and making any modifications risks the creation of a security hole, or may counteract previously desired policies. A predictable and coherent expression of intent-based policies in IBN, the ability to apply consistency and integrity checks (such as using formal mathematical methods), and their standardized translation and deployment into network element configurations all increase the consistency in the network—even in the face of multiple operator groups and disparate technologies.

Furthermore, intent-based networks 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.

The transition to intent-based networking

For many organizations, the evolution to a fully intent-based network will be a journey, requiring a combination of existing and new technologies and process changes. The full potential of IBN is ultimately recognized when it is deployed across all network domains, including data center, campus, branch, and WAN.

A number of initiatives across the industry are working to deliver on the promise of intent, and many of the functional building blocks contributing to an intent-based model are available today and already providing substantial benefits. Many foundational elements, including software-defined networking, virtualization, and analytics have matured to the point that they can be deployed today, as part of a longer-term intent-based strategy. The transition to IBN can also be dramatically simplified and accelerated by automatically discovering hosts and policies running on an organization's current network, and then providing the operator with the ability to review the running policies and identify which should be activated in their IBN.

Cisco is helping IT leaders embark on achieving an end-to-end intent-based network based on our open platforms for data center and enterprise networking, together with an ecosystem of third-party technologies.

In the data center, the Cisco® Application Centric Infrastructure (Cisco ACI™) solution provides a policy-based automated network fabric, covering the translation and activation phases of the intent-based framework, while Cisco Network Assurance Engine provides assurance in data center networks.

On the enterprise-networking side, the Cisco Digital Network Architecture (Cisco DNA™) offers similar services for enterprise campus, branch and WAN environments, providing translation, activation and assurance capabilities for wired and wireless, software-defined access, and software-defined WAN domains. Furthermore, Cisco's Identity Services Engine provides identify-based policy and rich contextual information.

The journey to elevate networks to an intent-based model is well under way!

For more information

Learn more about intent-based networking here: https://www.cisco.com/c/en/us/solutions/enterprise-networks/intent-based-networking.html

> **"We believe a full IBNS implementation can reduce network infrastructure delivery times to the business leaders by 50% to 90%, while simultaneously reducing the number and duration of outages by at least 50%."**
>
> **–Gartner, 2017**

Gartner, Innovation Insight: Intent-Based Networking Systems, Andrew Lerner, Joe Skorupa, Sanjit Ganguli, 07 February 2017