# Intent-Based Networking
## WITH CISCO MERAKI

## Introduction

Businesses around the world are undergoing digitization at an unprecedented pace and networking is at the center of this unstoppable evolution. Businesses are facing increasing pressure from customers who desire the best-in-class customer service in every interaction. Traditional enterprise architecture is under immense stress to adapt and address these changing market demands.

The move towards cloud-based software services has reduced product development cycles to days instead of years, which has made any competitive advantage transient. Add to this, the steady and certain rise of widespread Internet-of-Things, Sensors and Autonomous devices that are bound to push traditional networks to the edge.

This combination of needs and threats is driving innovation in the area of "Intent-Based Networks". **Intent-based Networking (IBN)** is a powerful paradigm shift in the networking industry. IBN allows a business to express its intent for the network and translate that intent in device-level configurations instead of having to depend on the ability of an expert designer. IBN simplifies networking expertise and makes it available to everyone.

Cisco Meraki believes that a successful IBN is achieved through a closed-loop system built with the following functional building blocks:

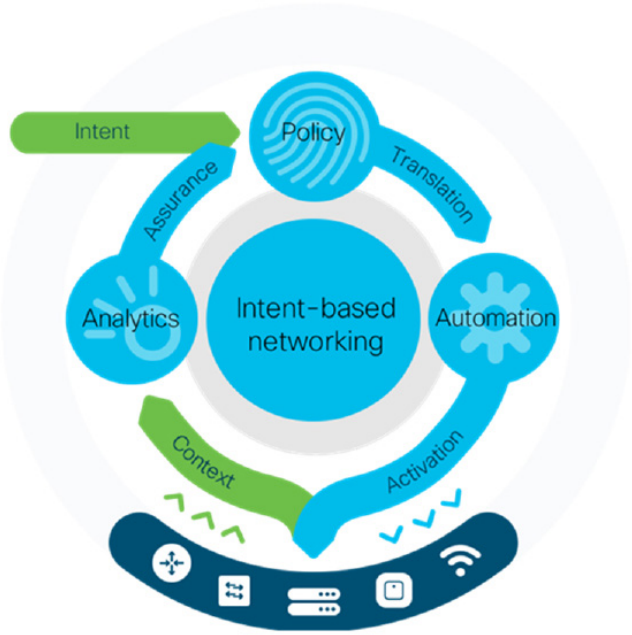



Figure 1. Intent-based networking

**1. Translation:** The capability to express the intent of the business to obtain the desired outcome by using verified policy settings that are seamlessly deployed on a network.

> Example: Translate a business intent for a branch Office location that wants to give Employees, Contractors, IT staff, Compliance different levels of security and access to different applications/resources using segmentation and dynamic policies.

**2. Activation:** To be truly intent-based, a network must go beyond the access-control of clients and applications by automating policy enforcement across the network to provide desired levels of user experience, application prioritization, and quality-of-service (QoS).

> Example: Assign QoS priority for business critical traffic and provision application access for different user groups in the Office across the entire network.

**3. Assurance:** The most important part of an IBN for an IT manager is the assurance that the network is running as intended. The network should be able to self-regulate in case of mismatched policies or other configurations using predictive analytics.

> Example: Use built-in analytics to monitor user access issues and assess network performance levels against desired business outcomes. Use recommendations to remediate issues wherever necessary.

IBN 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. Meraki simplifies IT management to deliver an intent-based network by enabling these three building blocks from a single dashboard which acts a controller and which can be accessed from anywhere on any device.

**"Gartner sees the biggest benefits from IBNS are improving network agility and availability, and supporting unified intent and policy across multiple infrastructures."**

**- Gartner, 2017**

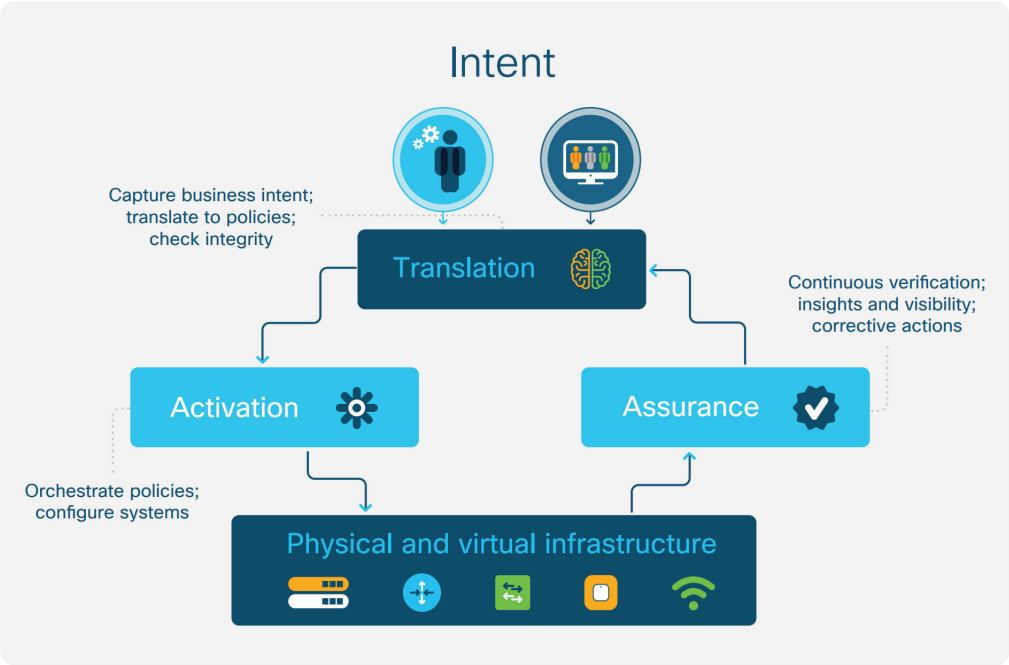
Gartner, Innovation Insight: Networking Systems, Andrew Joe Skorupa, Sanjit Ganguli, 07

Meraki

**"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: Networking Systems, Andrew Joe Skorupa, Sanjit Ganguli, 07




## Policy and Translation:

In a Meraki powered IBN, the dashboard helps the network operator translate business intent into policies. The dashboard captures these "business intentions" and helps translate them into custom templates and policies. These templates and policies are used across multiple sites to help sites/networks go-live in minutes rather than days. IT teams can set policies, which allow the dashboard (controller) to remotely configure multiple ports on a switch with a few simple clicks from the dashboard using Virtual Stacking. If the business directive is to be energy effective, then port scheduling policies are used to enable energy savings.

Security and SD-WAN come in a single box with Meraki. IT teams can easily create and apply multiple policies to shape business-critical and non-critical traffic to meet desired service level agreements. Additionally, Meraki Dashboard API is an interface for software to interact directly with the Meraki cloud platform and Meraki managed devices. The API endpoints are useful in building software and applications that communicate with the Meraki Dashboard for use cases such as setting policy, bulk configuration changes, and monitoring in real-time.

## Automation and Activation:

Meraki has a host of solutions to enforce intentions across the entire network through automated policy enforcement. Security and SD-WAN come in a single box with Meraki. IT teams can easily create and apply multiple policies to shape business-critical and non-critical traffic to meet desired service level agreements. The Systems Manager solution enables

the enforcement of several end-point management policies ranging from auto-device enrollment to sophisticated geofencing security options across all devices connecting to the network. The Dashboard also offers the ability to create custom device - tags and integrates with a RADIUS server to make device authentication simpler.

Scheduling automated updates over the cloud instead of being on-site at odd hours of the night helps always be updated and ensure minimal business disruption. Meraki switches also allow you the option of enabling policies based on user groups in your organization instead of cryptic individual IP addresses. MS390 series of Meraki switches simplifies the delivery of IBN across Branch locations, IoT devices, and Sensors.

Cisco SD-Access gives network operators the tools to perform key business functions like onboarding, secure segmentation, IoT integration, and guest access. Extended Nodes in the Cisco DNA architecture provide zero-touch configuration options to set group-based policies for users, cameras, and other IoT equipment. With Adaptive Policy, customers can deploy consistent, rich policies, across networks. With this customers who have Cisco Catalyst switches at the campus and sco Meraki switches at the Branch can deploy rich policies seamlessly.

### Analytics and Assurance:

While the ability to capture and enforce intent is important, an intent-based network fails if it does not have the ability to inform the IT administrator of deviations or conflicts between policies. The Meraki dashboard isolates root-causes and errors to ease troubleshooting. In the Meraki dashboard, WAN Health helps resolve WAN up-link issues across their entire networks proactively by providing real-time alerts to a network administrator in case of a failure. Wireless Health as provisions to send alerts over SMS and email to administrators when the performance of their APs drop below their desired thresholds.

Web App Health on Meraki Insight informs administrators when expected Quality-of-Service levels are not maintained on SaaS applications. It determines where the issue is at (LAN, WAN or Application level) before alerting the administrator, which helps in reducing response times. The Meraki Dashboard also allows remote packet capture (pCap file) on all Meraki appliances for remote troubleshooting. However, for large enterprise IBNs, the Cisco DNA center (Digital Network Architecture) acts as a single interface to monitor and troubleshoot at Cisco Catalyst devices. Additionally, all Meraki Access Points (APs) come with a dedicated scanning radio, which powers the Air Marshall feature to enforce security policies across the entire network and crack down on rogue SSIDs. Meraki also enables admins to create and deploy custom Radio-Frequency (RF) profiles to obtain the desired outcome from the wireless network.