Cisco DNA Application Experience

Intent-Based Networking for Applications in the Enterprise

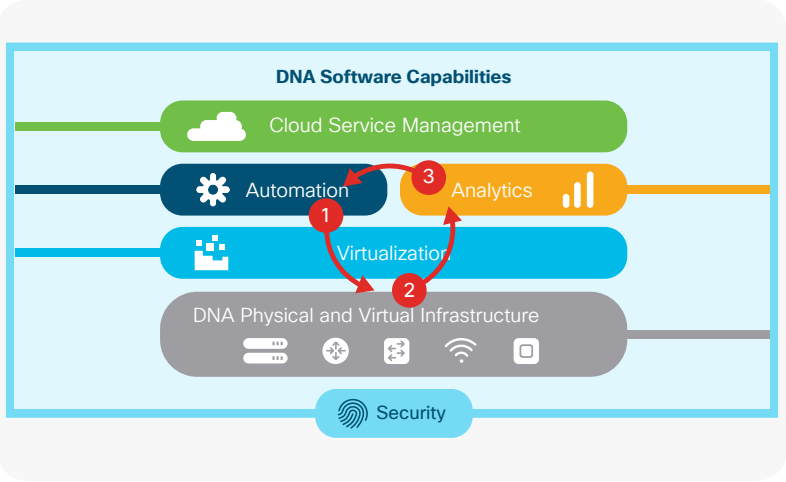
Requirements of intent-based networks

The primary functions of intent-based networks are:

- **Translation and validation of intent:** Business-level intent is expressed by an operator and is translated into validated platform-specific configurations.
- **Automation:** Network device configurations are deployed at scale by a controller.
- **Analytics:** The network operational state is continually monitored via telemetry.
- **Assurance:** The system validates that the expressed intent is being delivered via quantitative metrics OR recognizes that the intent is not being met and then guides or automates remediation actions.

The Cisco® Digital Network Architecture (Cisco DNA™), illustrated in **Figure 1**, meets all of these requirements for intent-based application networking in the enterprise.

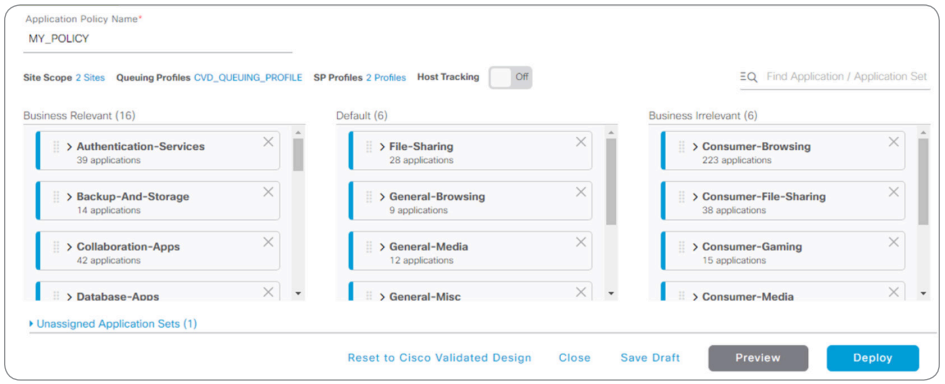
Figure 1. Cisco Digital Network Architecture



Cisco DNA delivers intent-based networking for applications via the following three main components:

- **Cisco DNA Application Policy** (item 1 in Figure 1) is an application within Cisco DNA Center™ that solicits business intent, **translates and validates** this **intent**, and **automates** the deployment of Cisco Validated Design configurations to network devices.
- **Cisco Programmable Infrastructure** (item 2 in Figure 1): Programmable hardware enables powerful infrastructure software solutions to **recognize** and **prioritize** application traffic, as well as **report** on application treatment across the enterprise routing, switching, and wireless network; this capability includes advanced application recognition for hundreds of encrypted applications, without compromising privacy or confidentiality.
- **Cisco DNA Application Assurance** (item 3 in Figure 1) is an application within DNA Center that ingests telemetry data from the network and adjacent data sources and performs contextual correlation and **analytics** to determine the network state in the context of the expressed intent. This application provides **assurance** either by confirming that the intent is being met (and supplying quantitative metrics to support such a validation) or by identifying that the intent is not being met and then initiating guided remediation workflows.

Figure 2. Creating an intent-based Cisco DNA Application Policy



Cisco DNA Application Policy

Network operators can deploy application policies across their routed, switched, and wireless enterprise infrastructure with just three easy steps:

1. Name their policy.
2. Select a site scope (to which their policy will apply).
3. Assign business relevance to their applications.

Note: Operators can also perform optional steps, such as tuning bandwidth allocations and/or service provider profiles, as well as previewing and testing the policy prior to deployment.

Operators can assign applications to one of three levels of business relevance, as shown in **Figure 2**.

- **Business relevant:** These applications are **known to contribute to the business objectives** of the organization.
- **Default:** These applications may or may not contribute to business objectives, or there is no business reason to justify explicit policy treatment.
- **Business irrelevant:** These applications are known to have no contribution to business-objectives.

Cisco DNA Programmable Infrastructure

The next set of requirements for enforcing application policy across the infrastructure is:

- Identifying the applications on the network, even though the majority of these are encrypted
- Grouping these applications into traffic classes
- Expressing the operator-selected business relevance of the applications
- Marking the traffic from end to end across the network
- Applying consistent congestion management and congestion avoidance to the traffic from end to end across the network

DNA Center abstracts heterogeneous platform-specific tools and features needed to implement these requirements across the network and deploys a consistent, cohesive, and comprehensive policy to express the intent from end to end, as shown in **Figure 3**.

A key technology used by Cisco DNA infrastructure is Next-Generation Network-Based Application Recognition (NBAR2). NBAR2 recognizes over 1400 applications, including more than 150 encrypted applications (without compromising confidentiality or privacy). NBAR2 is now supported not only on routing and wireless platforms, but also on switching platforms, such as the Cisco Catalyst® 9300 Series, because of its advanced Cisco Unified Access® Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC).

Figure 3. Cisco DNA infrastructure enabling and enforcing Cisco DNA Application Policy

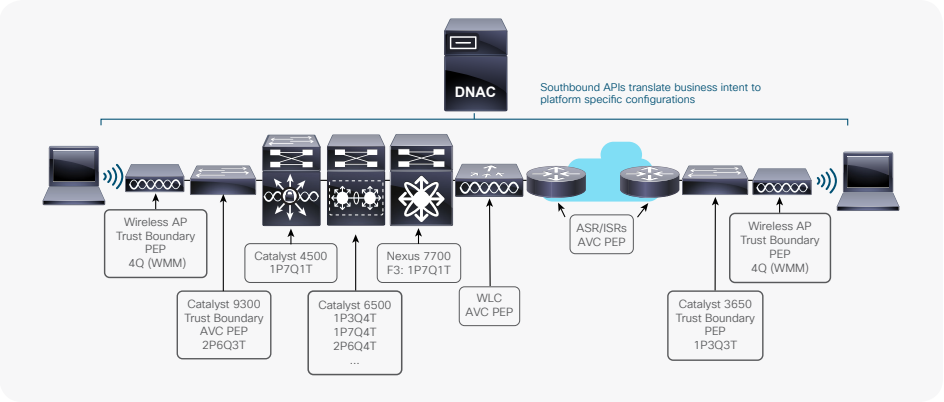
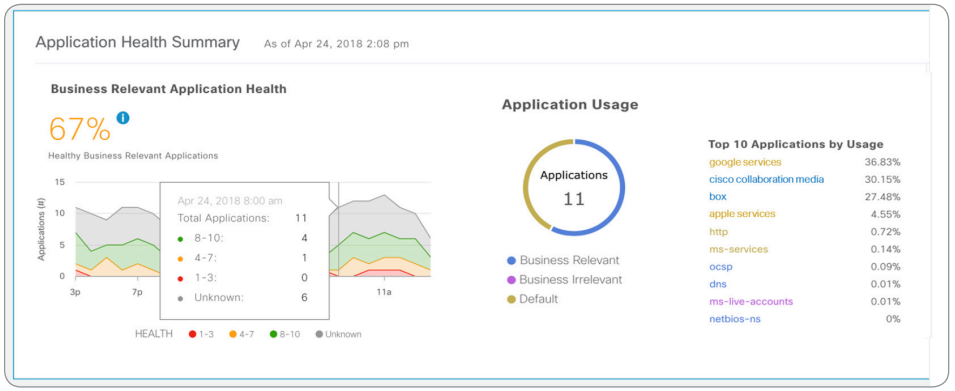


Figure 4. Cisco DNA Application Assurance—Application Health Summary



Cisco DNA Application Assurance

Cisco DNA Application Assurance closes the intent-based application experience loop illustrated in **Figure 1**.

Cisco DNA Application Assurance ingests telemetry data from the network, as well as from relevant non-network sources (such as application servers, peer-analytics systems, client devices, etc.) and performs contextual correlation and analysis of all such data to determine the operational state of applications on the enterprise network.

To do this, Cisco DNA Application Assurance monitors multiple application Key Performance Indicators (KPIs) and—by applying standards-based guidance—interprets these for the network operator. In such a manner, raw network data (such as latency, jitter, and packet-loss values) can be transformed into more meaningful information, such as the overall health score of an application, as shown in **Figure 4**.

Additionally, Cisco DNA Application Assurance flags issues with underperforming applications and presents actionable insights and guided remediation to the network operator.