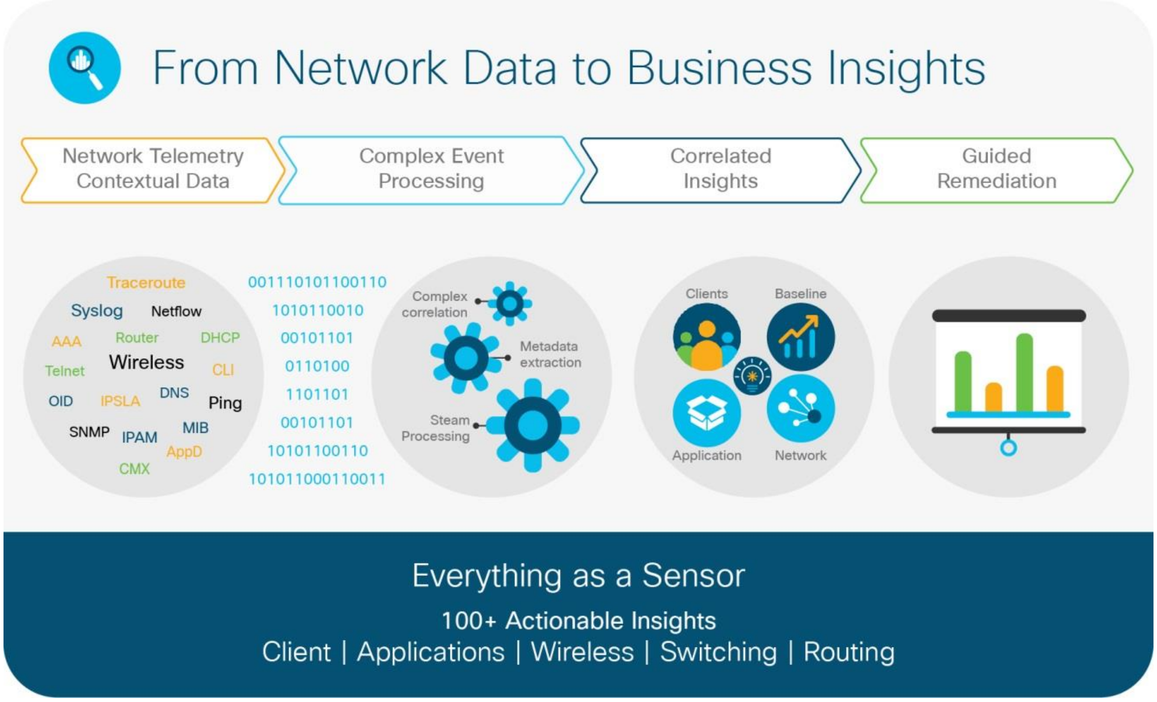
Data Sheet

Cisco DNA Center 1.1

Closing the loop with context

Cisco DNA Center™ is the foundational controller and analytics platform at the heart of Cisco's intent-based network. DNA Center 1.0 supported the expression of intent for multiple use cases, including base automation capabilities, fabric provisioning, and policy-based segmentation in the enterprise network. DNA Center 1.1 adds context to this journey through the introduction of Analytics and Assurance. Version 1.1 provides end-to-end visibility into the network with full context through data and insights (Figure 1).

Figure 1. Cisco DNA Center 1.1



Introducing Cisco DNA Assurance

Problem: Traditional network management tools are limited and do not address network needs

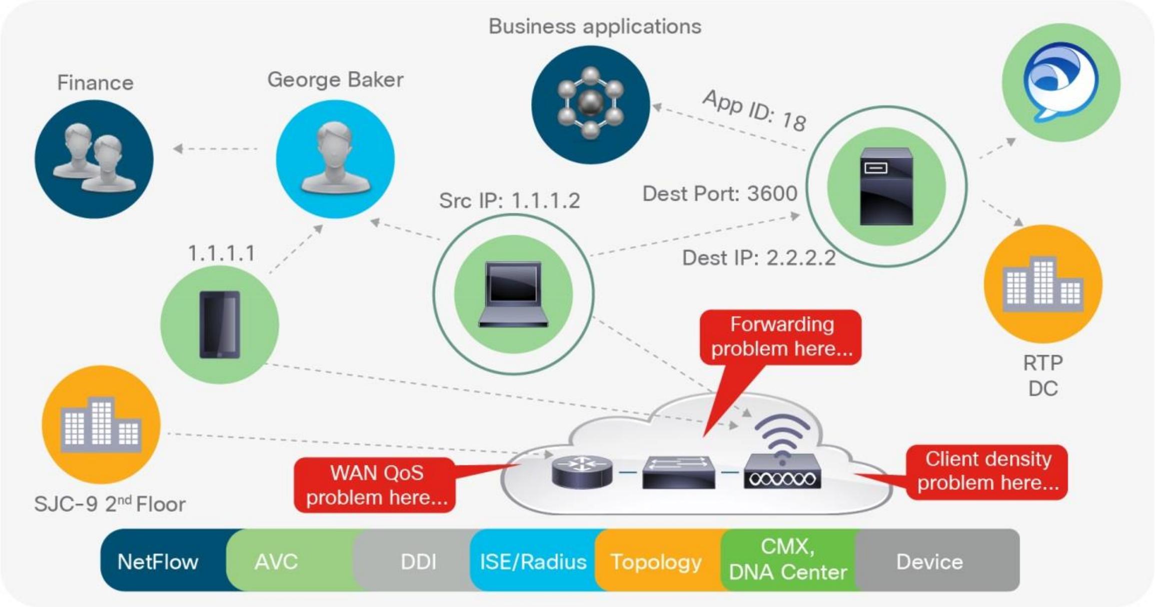
Too many tools with siloed views and nonstandard and closed interfaces provide limited and fragmented insights with little to no actionable data for IT.

Solution: How Cisco DNA Assurance helps

Cisco DNA Center drives innovation and simplicity over and above traditional monitoring tools by focusing on generating correlated insights rather than reporting. Cisco DNA Assurance collects multiple data sources for devices, applications, users, and endpoints, and then applies advanced analytics algorithms to uncover issues and suggest remediation.

Cisco DNA Assurance uses unique **network graph** technology developed by Cisco that draws from a combination of data sources, such as NetFlow; Application Visibility and Control (AVC); DNS, DHCP, and IP address management (DDI); Cisco Identity Services Engine (ISE) and RADIUS information; topology data; and Cisco Connected Mobile Experiences (CMX) and other device metrics to construct a unique real-time and historical capture of interrelationships among users, devices, applications, and network services across time and location (Figure 2).

Figure 2. Contextual correlation and property



Key features of Cisco DNA Center 1.1

- **Cisco DNA Assurance (New)**
  - Actionable insights and simplicity that transform network operations
  - End-to-end visibility: 360-degree views across network, historical views, ability to follow the network path
  - Network time travel
  - Proactive and predictive insights
  - Guided remediation
- **Cisco DNA Automation (new feature updates)**
  - Wireless automation: Simplified wireless design workflow
  - Enterprise Service Automation (ESA) for control of hardware hosting platforms and software services required in new branch deployments
  - Branch deployment automation: Support for physical and virtual branches; day-0 router and Network Functions Virtualization (NFV) design
  - Software Image Management (SWIM) updates: Intent-based network upgrades, pre- and post-checks, patching support

- **Cisco Software-Defined Access (SD-Access) solution for DNA Center 1.1**
  - Automated external connectivity handoff using Virtual Routing and Forwarding Lite (VRF-Lite), and Border Gateway Protocol Ethernet VPN (BGP-EVPN)
  - Fabric assurance, with key performance indicators (KPIs) and 360-degree views for clients, access points, Wireless Controllers (WLCs), and switches
  - Fabric wireless
- **Cisco Meraki® integration**
  - Starting point of integration between Cisco's access platforms
  - Provides hybrid (Cisco DNA™ and Meraki) customers a single management pane of glass
  - Uses existing Meraki API keys; no additional license required
- **Programmability and APIs:** Supports Representational State Transfer (REST) APIs at the northbound layer for programmability
- **Platform:** Single platform for both Automation and Assurance, designed for scale. Cisco DNA Center 1.1 also supports Role-Based Access Control (RBAC)

Cisco DNA Assurance detailed feature description

Table 1. Cisco DNA Assurance features and benefits

Feature	Description and benefits
Overall health	• Overall health summary of network and clients • Top 10 global issues • Views by sites/geos, list, or topology
Network and client health	An easy-to-use single dashboard for monitoring network health, identifying issue root causes, and remediating issues • Client health summary • Onboarding, RF, and client profile info • Network health summary • Control, data, policy plane, and health information
360-degree views of users and devices	Single dashboard for end-to-end visibility into all user information and user devices • History of performance for each user device • Proactive identification of any issues affecting the user experience • Connectivity graph with health score of all devices on the path • Application experience • Device KPIs
Network time travel	Go back in time to understand the network state when the issue occurred: • Rewind time to when the issue occurred • History shows critical events • All the information on the user or network device changes to the selected time
Proactive insights	**Insights with guided remediation** • Guided actions to help remediate issues quickly • Detailed drill-downs to identify the impact quickly **Proactive insights from sensors:** Ability to create a sensor test schedule and define the applications and tests to run • Sensor tests raise issues and provide insights • Detailed results shown at the floor level

Feature	Description and benefits
Streaming telemetry	Streaming telemetry enables network devices to send near-real-time telemetry information to DNA Center, reducing delays in data collection. Some of the other benefits of streaming telemetry include: • Low and quantifiable CPU overhead • Optimized data export (KPI, events) • Event-driven notifications
Wi-Fi analytics for iOS	• Support per-device-group policies and analytics ◦ Client details, such as iPhone model and iOS information • Insights into the clients' view of the network ◦ Basic Service Set Identifier (BSSID) ◦ Received Signal Strength Indication (RSSI) ◦ Channel number • Clarity regarding the reliability of connectivity ◦ Client reasons, such as error codes for last disconnection
Path trace	Troubleshoots issues along the network path • Run a path trace from source to destination to quickly get key performance statistics for each device along the network path • Identify Access Control Lists (ACLs) that may be blocking or affecting the traffic flow

Correlated insights

Table 2. List of correlated insights

Category	Insights
Wireless (Total insights: 66 issues in DNA Center 1.1)	**Client onboarding** • Association failures • Authentication failures • IP address failure • Client exclusion • Excessive onboarding time • Excessive authentication time • Excessive IP addressing time • Authentication, Authorization, and Accounting (AAA) and Dynamic Host Configuration Protocol (DHCP) reachability **Client experience** • Throughput analysis • Roaming pattern analysis • Sticky client • Slow roaming • Excessive roaming • RF, roaming pattern • Dual-band clients that prefer 2.4 GHz • Excessive interference **Network coverage and capacity** • Coverage hole • Access point license utilization • Client capacity • Radio utilization **Network device monitoring** • Availability • Crash, access point join failure • High availability • CPU, memory • Flapping access point, hung radio • Power supply failures

Category	Insights
Routing **(Total insights: 8 issues in DNA Center 1.1)**	**Router health** • High CPU utilization • High memory utilization **Routing technologies** • BGP AS mismatch, flaps • Open Shortest Path First (OSPF) adjacency failure • Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency failure **Connectivity** • Interface high utilization • LAN connectivity down/flap • IS SLA to service provider gateway connectivity
Switching (nonfabric)	**Client onboarding** • Client and device DHCP • Client and device DNS • Client authentication and authorization **Switch** • CPU, memory, temperature • Line card • Modules • Power over Ethernet (PoE) power • Ternary Content-Addressable Memory (TCAM) table
SD-Access **(Total insights: 38 issues in DNA Center 1.1)**	**Border and edge reachability** • Control plane reachability • Edge reachability • Border reachability • Routing protocol • MAP server **Data plane** • Border and edge connectivity • Border node health • Access node health • Network services DHCP, DNS, AAA **Policy plane** • ISE and pxGrid connectivity • Border node policy • Edge node policy **Client onboarding** • Client and device DHCP • Client and device DNS • Client authentication and authorization **Switch** • CPU, memory, temperature • Line card • Modules • PoE power • TCAM table

Cisco DNA Automation detailed feature description

Table 3. Cisco DNA Automation features and benefits

Feature	Description and benefits
Wireless automation	Intent-based workflows for simplified wireless deployment and automation ● Network profiles: A container of wireless properties that can represent single or multiple sites ● Simplified guest and SSID creation ● Advanced RF support for wireless networks ● A single workflow to enable flex or centralized wireless deployment ● Plug and Play (PnP) provisioning for access points ● Policy ◦ IP ACL support ◦ Access control policy for SD-Access wireless only
Branch deployment automation	Simplified workflows for physical and virtual branch automation; Day-0 router/NFV design. Onboard WAN devices and services via easy steps: 1. Configure network settings, service provider, and IP pools 2. Design a router or virtual profile 3. Assign to sites and provision network devices
SWIM and patch management	An easy to way to build a central repository of software images and Software Maintenance Updates (SMUs) and apply them to devices. Administrators can mark software images and patches as golden for a device family, allowing them to upgrade devices to the software image and patch versions that are in compliance with the golden versions defined in the repository. ● Golden images: Intent-based network upgrades allow for image standardization, much desired by network administrators ● Pre- and post-checks allow network administrators more control and visibility over network upgrades ● Patches are supported in DNA Center from intent to pre- and post-checks in the same way that we manage regular images
Discovery	Scans the devices and hosts in your network to build a centralized inventory database. The discovery function uses the following protocols and methods to retrieve device information, such as IP addresses, neighboring devices, and hosts connected to the device: ● Cisco Discovery Protocol ● Link Layer Discovery Protocol (LLDP) for endpoints ● IP Device Tracking (IPDT) and Address Resolution Protocol (ARP) entries for host discovery ● LLDP Media Endpoint Discovery (LLDP-MED) for discovering IP phones and some servers SNMP versions 2 and 3.
Network Information Database (NIDB)	Periodically scans the network to create a “single source of truth” for IT to build the network inventory. This inventory includes all network devices, along with an abstraction for the entire enterprise network. The NIDB allows applications to be device independent, so configuration differences between devices aren’t a problem.
Network design and profile-based management	Allows you to manage your network in a hierarchical fashion by letting you add areas and buildings on a geospatial map. You can start by defining your sites, then add buildings to sites, and finally add floors with detailed floor plans to the buildings. Cisco DNA Center lets the user define profiles, which consist of common network settings such as device credentials, DHCP, DNS server, AAA server, IP address pool, etc., Wireless settings such as SSIDs and RF profiles can be created globally and customized at site levels. These profiles form the basis for network automation.
SD-Access	Cisco SD-Access is the industry’s first intent-based networking solution for access networks and enables policy-based segmentation for users, devices, and things using an automated network fabric. DNA Center 1.1 brings several new enhancements to the SD-Access solution. Please refer to Table 4 for detailed features.

Cisco SD-Access 1.1 key new features

Table 4. SD-Access features and description

Feature	Description
Fabric infrastructure	• Automated external connectivity handoff using VRF-Lite, and BGP-EVPN
Fabric assurance	• KPIs, 360-degree views for clients, access points, WLCs, and switches ◦ Underlay and overlay correlation ◦ Device health: Fabric border and edge, CPU, memory, temperature, line cards, modules, stacking, PoE power, TCAM ◦ Data plane connectivity: Reachability to fabric border and edge, control plane, and DHCP, DNS, AAA ◦ Policy: Fabric border and edge policy, ISE/pxGrid connectivity ◦ Client onboarding: Client and device DHCP and DNS, client authentication and authorization
Fabric wireless	• Wireless guest with ISE (Central Web Authorization [CWA]) • Wireless guest support on separate guest border and control plane and wireless guest support as separate virtual network on enterprise border and control plane • Same SSID for traditional and fabric on same WLC (mixed mode) • WLC Single Sign-On (SSO) • Wireless multicast
Management	• Pre-check and post-check workflow validations • ISE administration (PAN) High Availability (HA) support (includes pxGrid, Monitoring and Troubleshooting [MnT]) • Distributed ISE Policy Service Node (PSN) support (2 per site) • Same ISE instance for fabric and traditional deployments • Cisco Secure Access Control System (ACS) and ISE for TACACS+ authentication of network devices • HA support for Cisco DNA Center • Policy-protected Command-Line Interface (CLI) configuration • Software image and patch management • License management • Backup and restore • Task scheduler

For more details on SD-Access, visit the SD-Access Solution page on Cisco.com.

Platform features

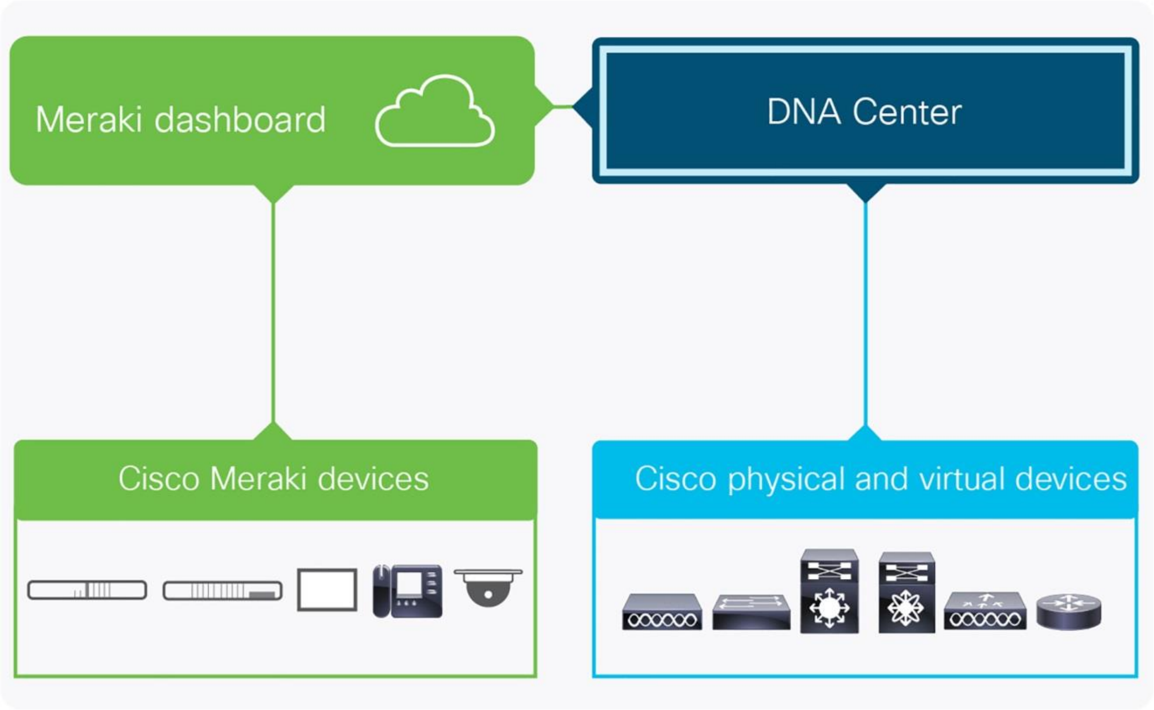
Table 5. Platform features

Role-Based Access Control (RBAC)	Allows users to be mapped to one of four predefined roles. The role determines what types of operations a user can perform within the system.
Programmability and APIs	Supports REST APIs at the northbound layer for programmability. The DNA Center 1.1 API provides support for the following features: • Discovery, device, and host inventory: The API provides basic details about the physical device chassis, such as its running software, as well as its interfaces, including up or down operational status • SWIM, PnP, system (file and Public Key Infrastructure [PKI]) APIs
Backup and restore	Supports complete backup and restore of the entire database for added protection.
ISE integration	Integrates with ISE through pxGrid/API for fabric overlay support.
IP Address Management (IPAM)	Integrates with Infoblox to allow applications built on top of the platform to leverage IPAM capabilities from Infoblox.

Meraki visibility in Cisco DNA Center

For existing Meraki branch customers that want to explore using Cisco DNA Center and the Cisco Catalyst® 9000 switching platform, or for customers with mixed environments, Cisco DNA Center now offers a single management pane of glass (Figure 3). This is an **API-driven dashboard integration** that supports all existing Meraki hardware and software at **no additional license cost**.

Figure 3. Cisco DNA Center integration with Meraki dashboard



Features and benefits

- Single dashboard inventory across all platforms (Cisco Meraki, Catalyst, Integrated Services Routers [ISRs], Aironet® access points)
- Up or down status of all devices in a single platform
- Use existing Meraki API keys; no additional license required

Cisco DNA Center 1.1 platform: Scale and hardware specifications

Tables 6 to 9 capture the scale information for Cisco DNA Center Release 1.1.

Table 6. Scale and hardware specifications

Platform specifications
Single appliance for DNA Center (Automation and Assurance) • Centralized deployment, cloud tethered • 1 Rack Unit (RU), small form factor • 2x 10-Gbps data links • Built-in network telemetry collection (Flexible NetFlow, SNMP, syslog) • Built-in contextual connectors (ISE and pxGrid, IPAM, location)

Platform specifications
● 64-bit x86 processors ● Solid-state disks in RAID 10 ● Hardware MRAID controller ● Dual power supplies

Note: The scale numbers below remain the same whether DNA Center is deployed either as a single host (standalone cluster) or a three hosts cluster.

Table 7. DNA Center Area scale

Area	Supported scale
Total devices, including routers, switches, and WLCs (the individual physical switches deployed in the network)	1000 (500 of which can be fabric devices)
Wireless devices (access points)	4000
Total number of Clients (wired and wireless)	25,000
Total number of IP pools	500
Number of Site hierarchies	200 **Note A** site hierarchy can include sites, buildings, and floors.
Number of Fabric domains	10
Profiles	25
Parallel device upgrades/threads (SWIM)	25
Concurrent UI users	10

Table 8. DNA Center Fabric Domain Scale

Fabric Domain	Supported scale
Total number of clients	15,000
Total number of IP pools	500
Fabric nodes[1]	500
Control plane nodes	2
Border nodes	4

[1] A fabric node can consist of a single switch or a stack consisting of upto 8 switches

Table 9. DNA Center Policy Scale

Policy	Supported scale
Policies	1,000
Contracts	500
Scalable Groups	1,000
Virtual Networks	64
Traffic Copy Policies	10
SGACLs – IP Based (Device)	Device dependent, refer to the following: CTS Release Bulletin
SGACLs – Group Based (Device)	Device dependent, refer to the following: CTS Release Bulletin
SGT Group/Fabric Domain	1,000

Roles and privileges

Table 10. Role-based access control

Role	Privilege
Network-Admin-Role	Users with this role have full access to all of the network-related DNA Center functions. They do not have access to system-related functions, such as app management, users (except for changing their own passwords), and backup and restore.
Observer-Role	Users with this role have view-only access to all Cisco DNA functions.
Telemetry-Admin-Role	Users with this role can perform system-level functions within DNA Center.
Super-Admin-Role	Users with this role have full access to all of the DNA Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.

Device support

Cisco DNA Center provides coverage for Cisco enterprise switching, routing, and mobility products. See the support matrix for a complete list of Cisco products supported:

DNA Center Device Support Matrix

Cisco DNA Center Appliance physical specifications

The Cisco DNA Center Appliance is available in a single form factor and comes with the Cisco DNA Center application preinstalled on it. Table 9 shows the appliance specifications.

Table 11. Physical specifications

Part number: DN1-HW-APL

Attribute	Specification
Power supply	Dual 770W AC
Physical dimensions (H x W x D)	Height: 1.7 in. (4.32 cm) Width: 16.89 in. (43.0 cm); including handles:18.98 in. (48.2 cm) Depth: 29.8 in. (75.6 cm); including handles: 30.98 in. (78.7 cm)
Temperature: Operating	1° to 95°F (5° to 35°C) Derate the maximum temperature by 1°C per every 1000 ft. (305 m) of altitude above sea level
Temperature: Nonoperating	-40° to 149°F (–40° to 65°C)
Humidity: Operating	10% to 90%, noncondensing at 82°F (28°C)
Humidity: Nonoperating	5% to 93% at 82°F (28°C)
Altitude: Operating	0 to 3,000 m (0 to 10,000 ft)
Altitude: Nonoperating	0 to 12,192 m (0 to 40,000 ft)
Network and management I/O	Supported connectors: • One 1 Gigabit Ethernet dedicated management port • Two 1 Gigabit BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA2 connector • Two USB3 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector

Licensing and ordering

To enable the Cisco DNA Center features listed in Tables 1 and 3, you will need one Cisco DNA Essentials or Cisco DNA Advantage license for each network device. Both of these licenses are available for purchase with Cisco ONE™ Software or a la carte. Please contact your Cisco sales representative for the Cisco DNA Center Ordering Guide.

See how Cisco ONE makes software buying simple: Cisco One Software.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For more information

See how Cisco DNA Center helps you move faster, lower costs, and reduce risk: Cisco DNA Center.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-739686-02 03/18