An Independent Competitive Assessment:

Cisco Data Center Network Manager (DCNM 11)
Arista CloudVision Portal (CVP)

April 2020

DR200204E

Miercom

Miercom.com

Contents

1.0 Executive Summary

The modern-day data center has evolved from managing a few switches to the complex task of overseeing data center fabrics, compounded by multi-site, multi-cloud implementations. An administrator who once managed a handful of physical switches, now must handle a more complicated, dispersed physical network that includes virtualized workloads and public clouds. Given that data center elements each require a high-standard of compliance for integrity and reliable functionality, the administrator needs to have visibility into every detail of this complex network from a single pane-of-glass.

Introduction to Cisco Data Center Network Manager

Cisco Systems, Inc. offers the Data Center Network Manager (DCNM) solution as a comprehensive way to aid customers looking to easily deploy, manage, monitor, operate and maintain modern data center deployments. By using automation, extensive visibility and reliable operations, DCNM offers the most powerful data center manager Cisco has produced to date, simplifying network operations while lowering costs. It is the recommended management solution for data center NX-OS deployments, premiering also as a storage network management tool.

The DCNM solution includes Cisco's best practices and advanced fabric tools to handle growing networks. Customers look to DCNM for its unparalleled VXLAN EVPN fabric deployment and management – discovering and connecting existing or new unprovisioned Nexus switches, help customers quickly and easily build new VXLAN-EVPN fabrics using the DCNM fabric builder in minutes. A complicated process such as a switch RMA and replacement, requires only a few clicks – with no manual configuration changes.

DCNM provides granular, scalable visibility for deep-dive troubleshooting, functionality and maintenance operations that data center customers can truly benefit from. The Topology View shows not only the network switches but also other connected entities such as virtual machines, container workloads, physical servers, multiple fabrics, inter-fabric connectivity, switch health and search functions. Customers can view these metrics in real-time to identify bottlenecks for optimized resource allocation for a smoother network experience.

Deployment consistency and configuration compliance is fully supported by DCNM, which constantly checks for proper switch-to-fabric configurations with autocorrections for any errors. The bottom line: DCNM makes fabric management simple and reliable.

What We Tested

By engaging with Miercom, an independent, comparative analysis was performed by comparing two data center network management packages: Cisco DCNM, with latest version 11.3(1), and an offering by Arista Networks – the CloudVision Portal (CVP), version 2019.1.1. These solutions were assessed for functionality regarding configuration and deployment, change control, network visibility, and real-time fault identification.

Summary of Brownfield Deployment Observations

What customers need is a management platform to address issues incurred by upgrading or adding to an existing network – known as brownfield deployment, as opposed to a new, greenfield deployment. Despite data center complexity, this management solution should intuitively accelerate deployment while ensuring operational compliance to help continue operations without downtime or cost.

We find for brownfield deployments, Cisco DCNM excels beyond its competition:

- ✓ Provides intelligent configuration and resource usage inference
- ✓ Validates all configurations
- ✓ Ensures there is no resource conflict
- ✓ Simple, two-click process

Arista CVP did not offer the same service, showing poor brownfield deployment:

- × No transparency during importing
- × Lack of resource tracking
- × Lacks understanding and validation of switch configurations
- × No detection, or alert, of an IP address conflict between an interface or loopback of an imported and existing switch – resulting in possibly disastrous effects on the network
- × Does not "understand" the network deployment per se; it essentially just reads the running configuration from the switches as a bunch of ASCII EOS CLIs

Key features of these packages were tested using comparable configurations of each vendor's network devices and respective network management package installations. Many features were fully supported by Cisco DCNM but were either not offered or only partially available on the Arista CVP. These features truly benefit customers looking to simplify and automate the complex processes of data center provisioning and policing through a centralized management solution.

Key Findings of the Cisco DCNM

- **Configuration & Deployment.** Exceptional support of extendable web-based GUI, topology-based provisioning, link awareness, resource visibility and management and "one touch" automated configurations for not only devices, but the entire fabric – including physical, virtual, containers and multi-cloud.
- **Policy Templates.** DCNM allows users to pre-provision internally or externally connecting physical and logical fabric links using link policy templates supporting Cisco's best practices for the most common deployment scenarios. The links are automatically associated with real-time health statistics for each interface; this data can be exported to daily or weekly reports. These policy templates can be easily customized specifically for the data center's needs.
- **Day 0 Installation.** With Cisco DCNM, this is easily done through its GUI interface and one touch option using one of two views – the default Topology View or the List View. The Topology View shows devices on the network, allowing for multiple, simultaneous switch deployment.

- **Fabric Building.** The DCNM fabric builder outperforms the Arista Fabric Builder by offering the ability to compare new and old configuration scripts to accept or correct the CLI scripts for the deployment process. The DCNM fabric builder allows switches to be associated with specific roles that, in turn, result in appropriate configuration generation for those specific switches. The configuration generation process in the fabric builder employs various resources such as IP addresses, loopback IDs, VLANs, VNIs etc. that are derived from user-defined resource pools.
- **Change-Control Workflows.** Cisco DCNM offers customizable change-control workflows for operations such as VXLANs and multi-site, tenant-routed multicast services. The DCNM fabric builder includes an embedded, integrated Configuration Compliance to validate and synchronize all configurations within the underlay, overlay, interfaces and others driven through the DCNM policies based on user-intent. This feature further builds on customization of Cisco's best practices policy templates. Configuration Compliance can be run periodically or on-demand to immediately trigger a compliance check.
- **VXLAN Management of Cloud Services.** Easy management of VXLAN BGP EVPN fabric to the public cloud was achieved with Cisco DCNM using IPSec tunneling between on-premise and Azure cloud services with management similar to any other Nexus device. It offers discovery, visibility, configuration control and compliance, built-in best practice templates, license management, upgrades and more.
- **Layer 4-7 Application Service Integration.** DCNM also provided topology visualization, control and integration of L4-7 service appliances attached to a VXLAN EVPN fabric, as well as defining custom service policies for traffic redirection.
- **Application Framework.** The DCNM infrastructure supports an extensible microservices based framework that readily supports scale-out. The DCNM App center offers applications, either as default for standard functionality or for licensed download. These applications collect data for each switch, coordinating data, to assist the customer with provisioning and visibility as a user-friendly way to approach what would have been an overwhelming, complex infrastructure.
- **Network Visibility.** The Network Insights applications on DCNM actively monitor complete flows for fabric-wide views, data correlation, and diagnosis. Topology overlay and awareness provide greater visibility and provisioning, as well as native switch-role awareness. Deep VXLAN visibility supports operation and maintenance for virtual machines.
- **Real-time Fault Identification.** The device analyzer locates network endpoints related to the underlay and overlay fabrics for useful troubleshooting, showing a green or red status for systems that are up or down.
- **Inline Controller Upgrades.** Cisco DCNM inline upgrades enable customers to upgrade to the latest release by imposing the newest version to the existing DCNM.
- **In-Service Software Upgrade (ISSU).** Cisco DCNM allows for switch software upgrades and patches while maintaining minimal traffic disruption.

- **Virtual Machine Manager.** Cisco DCNM allows for native integration with Virtual Machine Managers (VMM) to provide a correlated view of compute + network. Arista does not support this feature.

Based on our hands-on testing of both the Cisco Data Center Network Manager and Arista CloudVision Portal, we found Cisco's product offered superior capabilities and ease of use, and automated, "one-touch" provisioning based on templates and best practices. We estimate a trained technician can perform tasks with the Cisco package 50 to 300 percent faster than when using Arista's offering. As a result, we proudly award Cisco's Data Center Network Manager the ***Miercom Performance Verified*** certification.

Rob Smithers, CEO

Miercom

2.0 Test Summary

	Cisco DCNM	Arista CVP
Graphical User Interface (GUI)	Supported+	Partially Supported
	Provides extendable web-based GUI and supplies extensions for other vendors (not tested). Multi-faceted and varied GUI appropriate for each management task performed. CLI is also a supported option if desired.	Pre-built Configlet called Fabric Builder interface is written in Python, downloadable from github.com. It is quicker than manually creating management CLI files. Third-party devices are supported via CLI only. However, this interface is not an *interactive* GUI, applying scripts only to specifically building VXLAN fabric.
Topology-based Provisioning	Supported	Not Supported
	Supports topology-based provisioning and is link-aware.	No topology-based provisioning supported. Managed nodes are arranged in groups. CVP also lacks link awareness.
Resource Management	Supported	Not Supported
	Provides management and visibility of resources, including IP addresses, Loopback IDs, Port-channel IDs, subnets, VNI and VLAN numbers.	No support of resource management. The user is unable to check VLANs or IP addresses; for example, there is no visibility of which IP addresses or VLAN numbers are in use.
Configuration Automation	Supported+	Not Supported
	Provides impressive "one touch" capability for configuring new devices. With little required user input, the DCNM system can apply a board range of templates and best practices – producing device configurations, as well as configuration of network links and connections.	Primarily CLI-based configuration; CVP's role in configuration automation is used mainly to push command-string configurations to switches. Arista offers a pre-built Configlet Builder application downloadable from github.com to automatically import configurations. While this Configlet facilitates device configuration generation via widgets and Python scripts, applying these configurations to new switches still requires a fair amount of manual intervention.

	Cisco DCNM	Arista CVP
Virtual Machine Manager (VMM) Integration	Supported	Not Supported
	Provides capable VMM facility, organizing virtual machines (VMs) into appropriate domains and provides a correlated network and compute view. The Cisco package also provides high-level visibility of virtual machines.	No facility for managing a data center's VMs (e.g. VMware, RedHat) is supported.
Brownfield Configuration Import	Supported	Not Supported
	Provides real import of brownfield configurations, including associated resources used on every device within that deployment. The network can then be managed as if provisioned by the DCNM in the first place. Additionally, the Cisco package handles multi-site network deployments as well as multi-tenant operations.	Cannot import all the data of a previous configuration, to aid in generating a new or re-worked configuration. New or revised configurations must be manually re-entered or previous command strings must be edited.
Customizable Change-Control Workflows	Supported	Partially Supported
	Supports GUI-generated workflows for network operations (e.g. adding VXLANs, multi-site and tenant-routed multicast services). Supports integration of L4-7 service appliances attached to a VXLAN EVPN fabric, as well as defining custom service policies for traffic redirection. Supports ISSU for multiple endpoints with minimal downtime, customizable to the smallest number of fixes per upgrade package. Native change control is planned for a future DCNM release, as well as integration with ServiceNow.	Offers basic change-control; it is typically necessary to disable a device by putting it in maintenance or health-check mode before any change can be applied. Changes cannot be performed across multiple switches as ISSU is not supported. Supports Smart System Upgrade (SSU) that allows system software upgrades in small maintenance windows.
Data Plane Visibility	Supported+	Partially Supported
	Network Insights, an optional component of DCNM, actively monitors complete network flows including per flow latency, flow path, flow drops etc. It also provides fabric-wide flow views, with data correlation and diagnosis.	In the latest version, CVP can display traffic flows. This is based on sFlow, a standard (IETF RFC 3176) that monitors flows based on a sampling of transmitted data between endpoints.

	Cisco DCNM	Arista CVP
Device Analyzer	Supported+	Not Supported
	Offers ability to search for endpoints in real-time; an endpoint locator is part of a tool that provides correlated visibility for fabric (underlay/overlay, as well as endpoints) to provide a useful troubleshooting starting point. While not observed during testing, DCNM version 11.3 offers endpoint scalability.	The ability to find a network device is limited to a MAC-address search.
Topology Overlay Views	Supported+	Not Supported
	Supports various network topology views – including L2VNI, VRF and L3VNI. Third-party integration is included as of its last major release of DCNM in December 2019; one of the first supported vendors is Arista.	Topology overlay views, showing high-level fabric connectivity, are not supported in Arista's CVP. For example, CVP is unable to collect the necessary information to show what Layer-2 Virtual Network Interface (L2VNI) is deployed on which leaf node.
Third-Party Device Visibility	Supported*	Supported
	Planned third-party device integration for both provisioning and visibility for DCNM 11.3(1) and Network Insights Resources (NIR) following release 2.1. **While not observed during testing, DCNM version 11.3 offers this capability.*	Pulls standard-format data from third-party devices via SNMP.
Native Switch-Role Awareness	Supported	Not Supported
	Fully supports switch-role awareness.	Unaware of the role (e.g. leaf, spine) that a switch performs.
Topology Awareness	Supported	Not Supported
	Aware of both topology and switch for provisioning purposes.	Unaware of fabric or links. Changes to links or fabric members require that the configuration on related switches be manually added or removed.
Deep VXLAN Visibility for OAM	Supported	Not Supported
	Supports Operations and Maintenance functions via deep VXLAN visibility.	Does not support OAM functions. Lacks deep visibility of VXLANs.
In-Service Software Upgrades (ISSU)	Supported	Partially Supported
	Supports disruptive and non-disruptive ISSU options for minimal downtime.	Supports SSU since ISSU packages are unreliable – resulting in downtime.

3.0 Products Tested

The objective of this project was to compare the sophistication, functionality and ease of use of two data center network management platforms: Cisco DCNM and Arista CVP. To accomplish this, we acquired and built separate albeit functionally comparable configurations for each platform, employing current data center-class switch and router devices from both vendors.

The two network-management software packages we examined were:

- **Cisco Data Center Network Manager (DCNM)**, version 11.3(1). In our test environment the software was used to manage an infrastructure of varied Cisco Nexus 9000 switch models.
- **Arista CloudVision Portal (CVP)**, version 2019.1.1. The software was used to manage an infrastructure of mixed Arista 7000 Series switches.

Cisco Data Center Network Manager

Cisco DCNM is among the most comprehensive network-management offerings to collectively address all aspects of fabric management – although it is primarily for managing higher-end Cisco switches. Specifically, DCNM addresses all NX-OS (Nexus Operating System) and Cisco Multilayer Distributed Switching (MDS) network deployments – spanning LAN fabrics, SAN fabrics, and IP Fabric for Media (IPFM) networking in the data center. DCNM provides provisioning, management, control, automation of network operations, monitoring, visualization, and troubleshooting of Cisco Nexus and MDS infrastructures. This modular package has more than 200 discrete software modules distinguished by:

- **Management of LAN or SAN (storage-area network) environments.** A DCNM environment handling both LAN and SAN fabrics can also be assembled. Another aspect of DCNM, called IP Fabric for Media (IPFM), addresses the visibility and policy management of flows.
- **Support for specific Cisco device models.** Many of the software modules contain all the specific details for the in-depth management of particular devices. Most are for Nexus switches (Nexus 3000 through 9000-series switches) or MDS 9000 series switches.

Yet other software modules for DCNM integrate additional management functions and applications, such as those that incorporate Network Insights Resources and Cisco Device Manager.

The server environment required for DCNM – one or more 8- or 16-vCPU platforms – depends on whether for LAN and/or WAN environments. LAN operations are delivered via an OVA (Open Virtual Application) or ISO (Integrated Operating System) virtual system atop: VMware vCenter, Red Hat 7 KVM, or Cisco UCS C-Series platform. SAN management software is delivered in ISO CD format and runs on Microsoft Windows 2012 or Red Hat Enterprise Linux 7 platforms.

See the data sheet for more details on the Cisco DCNM software and hardware requirements.

Arista CloudVision Portal (CVP)

CloudVision Portal (CVP) is the web-based GUI for the CloudVision platform – a turnkey package addressing automation of certain network operations, network-device provisioning, compliance, change management,

and network monitoring of Arista switches. The package includes APIs to enable the customer to integrate with third-party or in-house management applications.

CVP is delivered as a packaged OVA (Open Virtual Application) file that includes most of the base software modules. The package runs on any x86 hypervisor, but the vendor recommends either VMware ESX 5.5 or Red Hat Linux 6.5 to 7. Similar to the Cisco DCNM platform requirements, Arista CVP needs either one or a cluster of 8- or 16-vCPU platforms. Similar to Cisco's, the Arista CVP server software is accessed via a web-based GUI.

After an Arista device (switch) is imported into CVP, it can be configured and monitored using the various CVP applications. Devices must enable streaming of status and data to send this information to the CVP platform for generating events, as appropriate, from the streamed data and state changes it receives from devices.

Arista documentation asserts the support of a range of management processes: device management (mainly via telemetry reporting), network provisioning, network compliance, troubleshooting (mainly of log files and configuration command sequences), back-up, restore, and updates.

For more details, visit the Arista CVP Overview.

4.0 How We Did It

Test-bed Overview

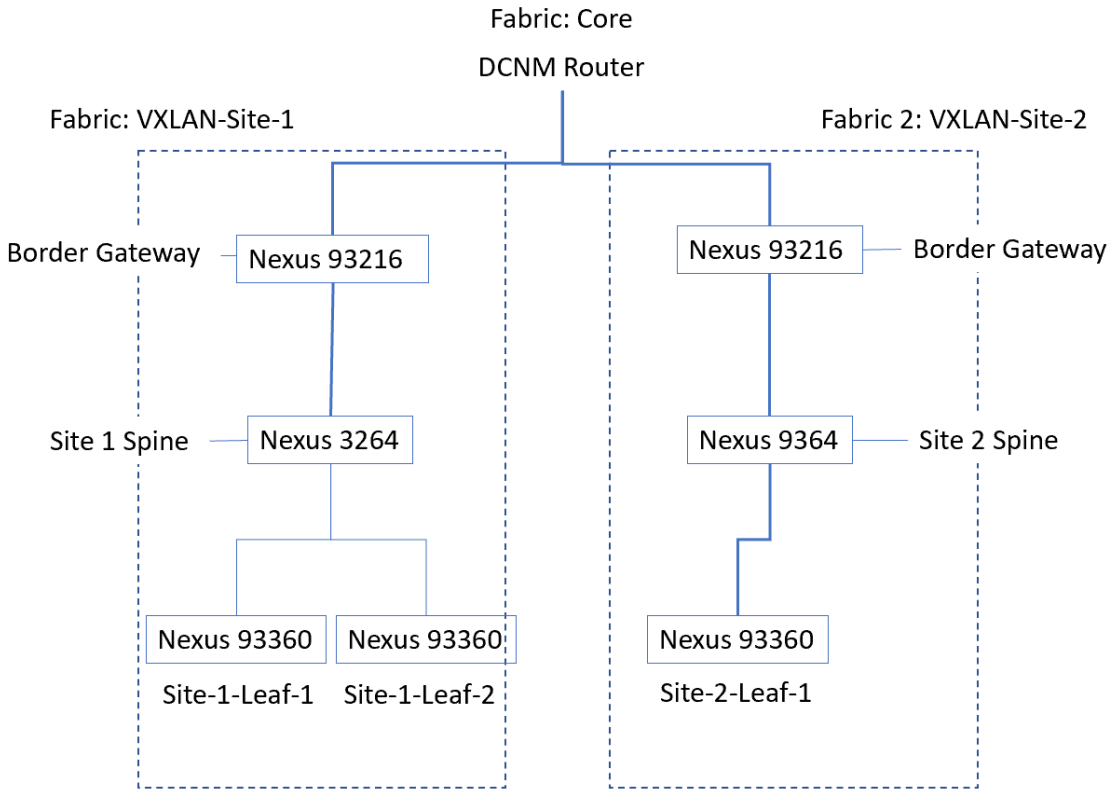
Two separate networks were assembled for this comparative testing: one of Arista switches running Arista's current operating software; the other of Cisco Nexus 9000 Series switches running the latest NX-OS release.

Cisco Test Bed

A Cisco DCNM server, running version 11.3(1) software, was installed and connected into a fully functional network of Nexus 9000 switches, comprising multiple network-infrastructure levels and fabric orientations.

The following Cisco Nexus switches were acquired and deployed:

- 2 x Nexus 93216, model N9K-C93216TC-FX2
- 3 x Nexus 93360, model N9K-C93360YC-FX2
- Nexus 9364, model N9K-C9364C
- Nexus 3264, model N3K-C3264C-E

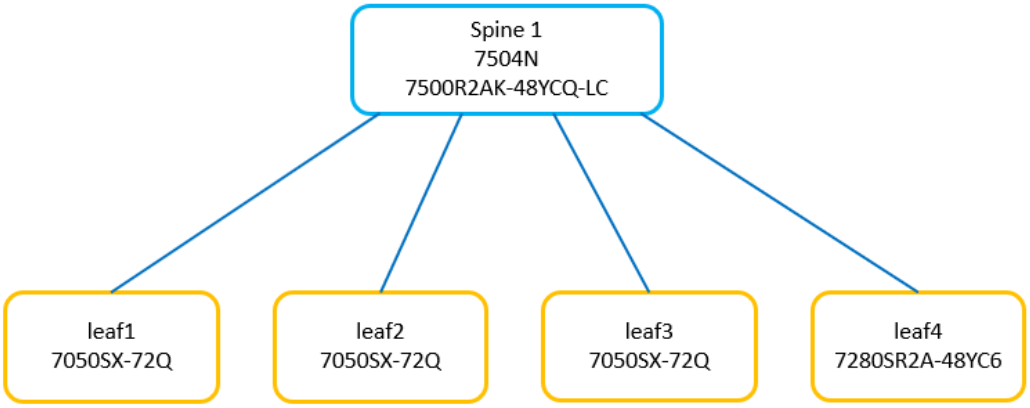


Source: Miercom

Arista Test Bed

An Arista CVP server was installed, running version 2019.1.1 software, and connected into a fully functional network of Arista multi-level switches: one serving as a spine switch, the others as leaf nodes. The following Arista 7000 Series switches were acquired and deployed, all running operating software version EOS 4.22.0.1F:

- 3 x 7050 Switch, model 7050SX-72Q
- 7280 Switch, model 7280SR2A-48YC6-M
- 7504N Switch, model 7500R2AK-48YCQ-LC



Source: Miercom

5.0 Configuration & Deployment

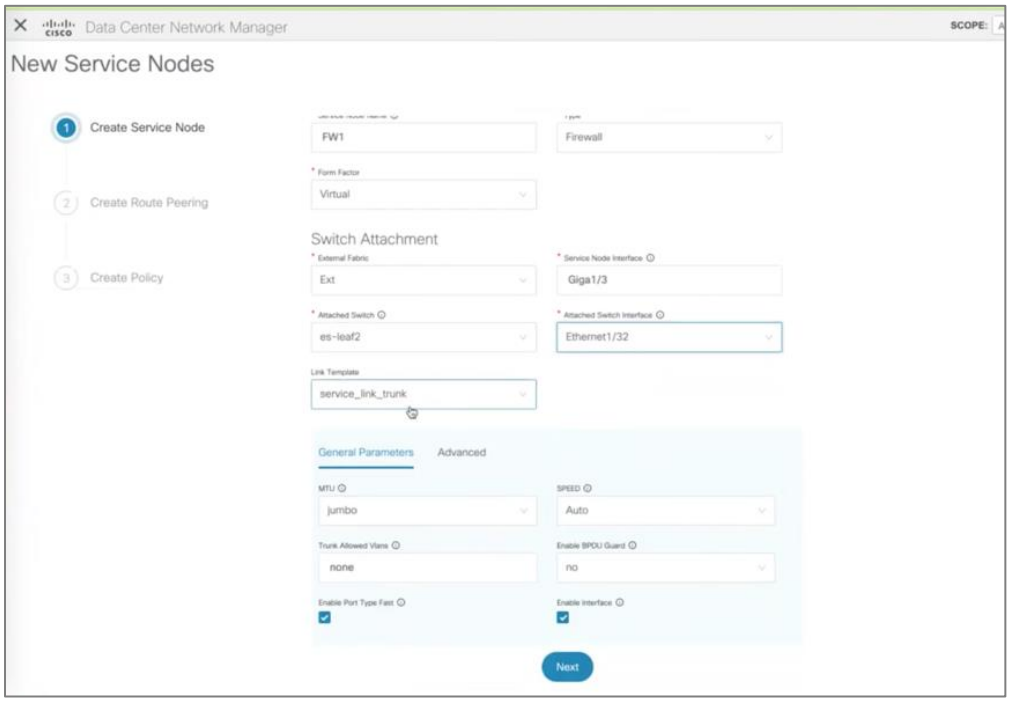
Why It Matters

Data centers consist of numerous switches, fabrics and endpoints – making configuration and deployment an overwhelming task. We evaluated Cisco DCNM and Arista CVP for their abilities to deploy large, realistic deployments that address custom business needs ("intent"), traditional and brownfield setups, and optimized overhead.

The Cisco Advantage

- **GUI-based workflows**. Cisco DCNM lets the user create automated-provisioning workflows, including for complex, high-level topologies: VXLANs (Virtual Extensible LANs), EVPNs (Ethernet Virtual Private Networks), multi-site, and TRM (tenant-routed multicast) configurations. (TRM enables multicast forwarding on the VXLAN fabric using a BGP-based EVPN control plane.)
- **Powerful "One Touch" Configuration**. Cisco DCNM also supports a one-touch option for configuring new additions to the network, a considerable time saver.
- **"Intent-based" configuration**. Cisco DCNM translates the user's network "intents" – discerned from various fabric-setting options – into appropriate command files for network configuration. To promote consistency and synchronization, DCNM then also checks configuration files to catch changes from previous files and highlights the differences.
- **Link-aware**. DCNM is link-aware and supports the management of interfaces individually at a per-device, fabric or data center level. This is done via the GUI or programmatically via an API. The tools within DCNM support all the same options for interface/link provisioning and configuration for device configuration, including best-practice, and interface-policy templates, which serve common deployment scenarios.
- **Topology-based provisioning and switch-role awareness**. Besides link-aware, DCNM is also topology-aware for provisioning. In addition, the Cisco package is native-switch role aware (i.e. whether it is leaf, spine, border leaf).
- **Real brownfield import**. Cisco DCNM can import a brownfield device or network configuration, and its resources, to be integrated with a new or revised network configuration.
- **Templates and best practices**. Besides user-specified fabric-setting parameters that define "intent," Cisco DCNM also applies best-practices rules and templates to the automated-configuration process. These serve the most common deployment scenarios. For more sophisticated or unusual use cases, the policy templates within DCNM can be readily customized to meet specific needs.

- **Configuration compliance and "intent" consistency checking**. DCNM periodically monitors the configurations running in the switches and tracks if any "Out-of-Band" change (via CLI or other method) was made in any function of the switch. If changes are found differing from the applied intent, DCNM will mark the switch as "Out-of-Sync," indicating a violation in compliance. This warns the user that the running configuration of a switch does not match the defined intent. The Out-of-Sync state is indicated by a color code in the topology view, and the switch Out-of-Sync state is tagged in the tabular view that lists all the switches in a fabric.
- **Layers 4-7 Services Integration**. DCNM facilities enable the network orchestration of L4-7 service appliances attached to a Virtual Extended LAN, Ethernet Virtual Private Network fabric. The first step is to select the appropriate fabric to which the L4-7-service node connects. Then, as the above interface shows, the user specifies the node's route peering and access policies. With the form all filled out, DCNM automatically integrates the service node. This L4-7 services-node integration capability lets the network manager view and monitor the service appliance's health, and see, for example, how much traffic is traversing the service node.



Adding a Service Appliance. *This interface page enables the user to define L4-7 service appliances and specify route-peering and apply policies for network access.*

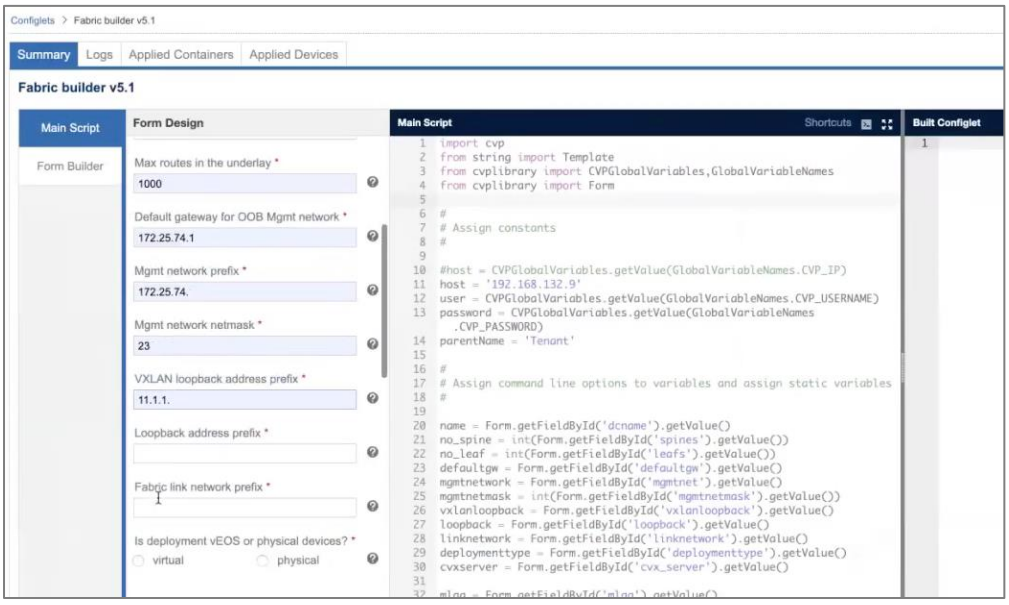
- **Public Cloud Connectivity**. DCNM supports integration of Public Cloud Connectivity into the managed network, using a Cloud Services Router (CSR) 1000v switch/router definition. In our testing we established DCNM Public Cloud Connectivity with Microsoft's Azure services. Users can provision virtual machines in the cloud using a virtual domain; IPsec tunneling is typically employed. Depending on configuration, a web server in the cloud is used, but data doesn't have to leave the

user's premises. The administrator can also establish different policies for different tenants with different VRF (Virtual Route Forwarding) routing tables.

- **Includes full version-control**. A Version Browser allows the user to peruse archived configurations, view and compare specific configuration versions, and merge changes from one version to another. After a configuration is modified by merging changes, it can be saved as a text file on a file system available to the computer running as the DCNM client. In a typical configuration, DCNM compares the old CLI configuration script with the new one and shows the differences. The user can accept or correct the CLI scripts as part of the configuration process.
- **Third-party device support.** The DCNM GUI is extendable, with extensions for a number of non-Cisco network systems and devices, so that network administrators can manage the Cisco and non-Cisco systems from one consistent interface.

How Arista Compares

- **Limited tools.** Arista's CVP supports two main mechanisms that contribute to provisioning: Fabric Builder and Configlet Builder. Both open-source tools enable portions of existing configurations (command-line scripts) to be re-applied to new device configuration files.



Arista's Open-Source Fabric Builder. *The application aids somewhat in command-line-based configuration but does no error checking of command scripts. Nor is there any auto-provisioning with Arista's CloudVision system.*

- **Mainly command-line based**. Device and network configuration are essentially CLI-based. CVP serves mainly to push configuration command-line scripts to switches.
- **No command-file diagnostics.** Arista CVP provides no help in resolving errors that occur in creating configuration command files. Troubleshooting and finding configuration errors is done by updating files via Fabric Builder, or by manually editing the faulty command file.
- **No version-control**. Arista provides no version-control for tracking configuration files, whether created manually or via the Fabric Builder tool. CVP creates command files anew each time it is run; the user must record and track the differences between old and new configuration files.
- **Auto-discovery, but no auto-configuration**. With appropriate password settings, Arista CVP can auto-discover Arista switches. These are identified to the CVP system and shown connected in a group. But no role – like leaf or spine switch – is determined or assigned, and no accurate auto topology is generated. No auto-configuration is supported after discovery.
- **New devices added manually.** To configure a new Arista device, the user could edit the configuration of a similar device in a similar role, or else create a new config file from scratch.
- **Third-party device configuration via CLI only.** Non-Arista systems being added are configured via CVP's command-line interface, using the CLI command structure of the non-Arista device. The user therefore needs to fully understand the Arista and the third-party configuration details.
- **No brownfield support.** Arista CVP is unable to import a partial or previous configuration, to be merged into a new, combined configuration or topology. The brownfield network must be defined from scratch or else be command-line edited.

Configuration & Deployment Summary

Cisco DCNM differs considerably from Arista CVP when it comes to the provisioning and configuration processes. While the Arista package uses 'power-assisted' coding of command-line files and has more limited configuration/provisioning functionality, we found Cisco DCNM to be comprehensive, considerably more sophisticated, innovative and timesaving.

6.0 Change-Control

Why It Matters

"Change Control" collectively includes all features of a management system that aid in tracking changes and assuring that changes to the network are made promptly, accurately and without unintentional disruption.

The Cisco Advantage

- **Configuration error checking**. As changes are defined for an existing configuration, they are compared to what is already up and running and conflicts are flagged to be fixed before the new changes are installed into the running fabric.
- **Ensures changes comply with intent**. DCNM learns user intent through various fabric-setting options selected by the user. These are reflected in appropriate commands in new network-configuration files. DCNM then checks configuration files to catch changes from previous files and highlights the differences.
- **Resources tracked**. DCNM provides for resource management: tracking, compiling and enabling the user to see what VLAN numbers, IP addresses, Virtual Network Interfaces, and so on have been used so far. This simplifies and eases changes and helps avoid errors in changed configurations.
- **Full version-control**. DCNM offers a Version Browser allowing the user to peruse archived configurations, view and compare specific configuration versions, and merge changes from one version to another.
- **Fallback protection**. If a new configuration file fails for any reason, the user can readily fall back to the last working configuration, while the new configuration is debugged. In a typical configuration, DCNM compares the old CLI configuration script with the new one and shows the differences. The user can accept or correct the CLI scripts as part of the configuration process.
- **Suspect configuration changes are automatically flagged**. DCNM periodically monitors the configurations running in the switches and tracks if any "Out-of-Band" change (via CLI or other method) was made. If changes are found differing from the applied intent, DCNM will mark the switch as "Out-of-Sync," indicating a violation in compliance. This warns the user that the running configuration of a switch does not match the defined intent. The Out-of-Sync state is indicated by a color code in the topology view, and the switch Out-of-Sync state is tagged in the tabular view that lists all the switches in a fabric.
- **In-Service Software Upgrades**. When a Cisco device's software is upgraded from DCNM, the user can select either disruptive or non-disruptive options for performing the software upgrade.

How Arista Compares

- **No command-file checking.** Arista CVP provides no help in spotting errors that occur in newly configured command files. Troubleshooting and finding configuration errors is done by updating files via Fabric Builder, or by manually editing the faulty command file. In our testing, an obscure error took a half a day to find and correct, with no help from Arista.
- **No version-control**. Arista provides no version control for tracking configuration files, whether created manually or via the Fabric Builder tool. CVP creates command files anew each time it is run; the user must record and track the differences between old and new configuration files.
- **Disruptive changes**. Any change on Arista fabric members or links entails a manual add or removal of the configuration on related switches. Before changes are made to a switch, it is effectively taken down – put in maintenance or health-check mode.
- **Limited ISSU (In-Service Software Upgrade).** Most of Arista's latest switch models do not support ISSU. Instead, Arista offers Smart System Upgrades (SSU) for software upgrades where switches are taken out of service during small maintenance windows.

Change-Control Test Summary

Based on the following observations, we regard Arista CVP's change-control functionality as minimal compared to Cisco DCNM's, which include numerous safeguards for assuring the integrity of changes made to the network.

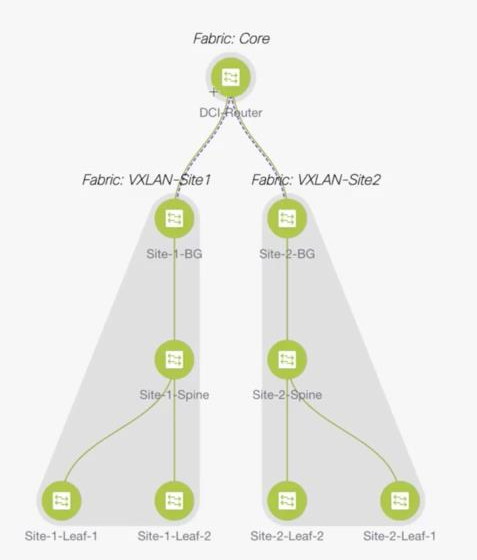
7.0 Network Visibility

Why It Matters

Being able to view a network topology dynamically, in real-time, and from different perspectives (i.e. the Denver-office network, or a Layer-2 "switch" display, or a specific node) are critical for an effective network-management system.

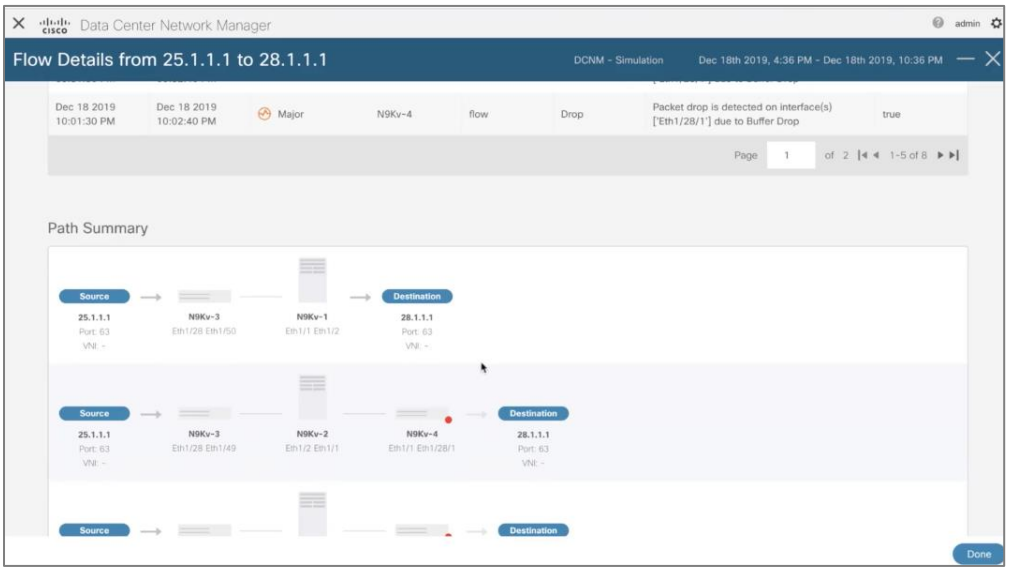
The Cisco Advantage

- **Network Insights**. A component of DCNM, Network Insights collects full flow data and provides fabric-wide flow views, along with data correlation and diagnostics.
- **GUI is rich and view-selectable**. Various topology views can be selected: fabric view, Layer-2, Layer-3, Virtual Extended LAN (VXLAN), overlay, underlay, and more.



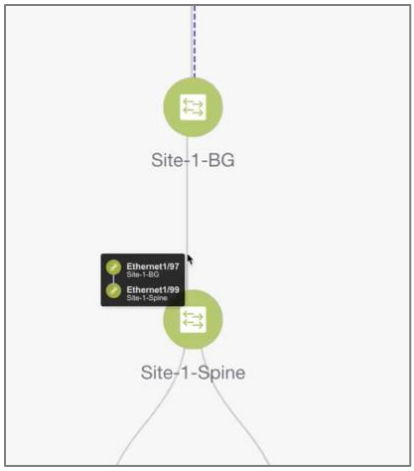
Cisco DCNM Topology Diagram: Fabric-level view. *This is a fabric view of the simplistic Cisco test-bed network, showing all devices are "green" and in sync. All nodes and links are selectable for additional, drill-down detail.*

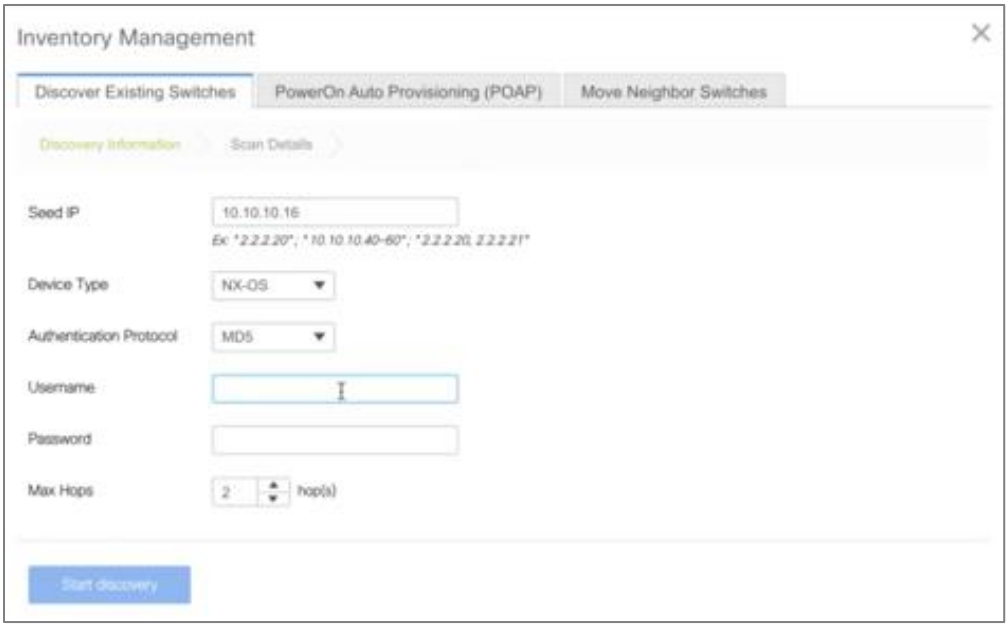
- **Flow visibility**. Another capability of DCNM management is IP Fabric for Media (IPFM), enabled by Network Insights, which provides visibility and policy management of flows. Unlike Arista, DCNM flows are based on full actual data and not just a sampling of packets, per sFlow. DCNM provides fabric-wide flow view with data correlation and diagnosis.



***Flow Analysis**. The above flow view shows both latency and packet drops.*

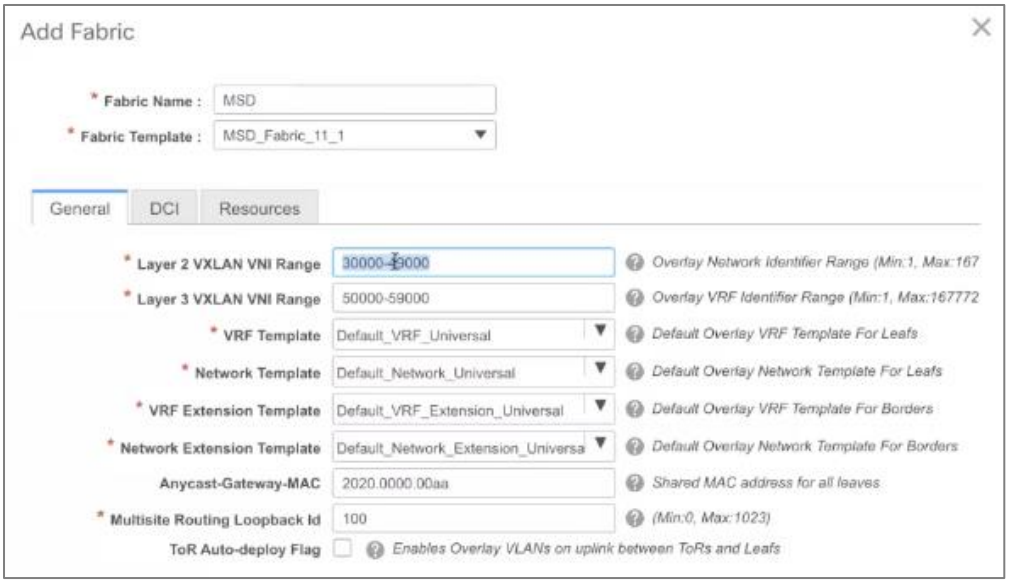
- **Real-time health**. DCNM provides "correlated visibility" – real-time health summaries for the fabric – overlay, underlay, endpoints. Another feature, called compute visibility, lets the user view VMware vCenter-managed hosts and their leaf switch connections in the topology page.
- **Link and switch-role aware**. DCNM is link- , topology- and native switch-role (leaf, spine, border leaf, etc.) -aware. These are separately definable, provisioned and monitored. As shown here, an individual link can be selected for additional information.
- **Third-party devices.** Visibility of third-party devices is supported in DCNM in several ways, including via OpenConfig, an industry working group developing standards for APIs and tools for configuring and managing network devices; and a software development kit (SDK) for integrating non-Cisco devices into DCNM.





Adding Non-Cisco Devices: Vendor agnostic. *This interface provides an "other" choice for defining non-Cisco equipment, which can be integrated in the same topologies, fabrics and views as Cisco devices. The same "Define, Save, Preview and Deploy" process is used for both Cisco and non-Cisco devices.*

- **Multi-site Manager**. Provides a high-level dashboard for tracking and synchronizing data with other DCNM deployments in local or remote data centers. Additionally, allows searches to query across the enterprise to locate elements that match search criteria (e.g. switch, virtual machine, MAC address, or segment ID).
- **Large, Multi-site Domains**. Multi-Site Domain (MSD) is a multi-fabric container that is created to manage multiple member fabrics. It is a single point of control for overlay networks and Virtual Routing and Forwarding (VRF) definitions that are shared across member fabrics. One DCNM can manage hundreds of data-center sites. Anything that is defined in an MSD doesn't have to be re-defined elsewhere but can be used as a template in further configurations.

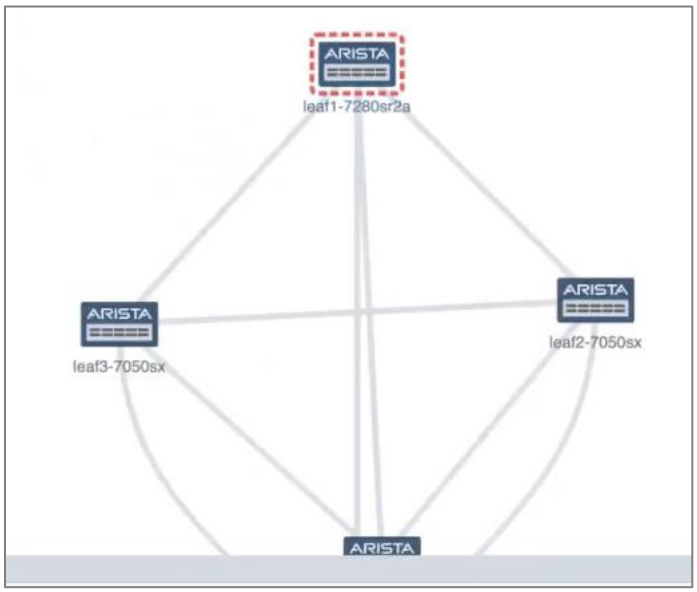


Adding Sites: Creating a Multi-Site Domain (MSD). *This interface invokes an MSD template from a previously defined template (at the MSD level). The previously defined ranges can be used in creating the next one. Values can be changed as desired/needed.*

- **Virtual Machine Manager (VMM)**. Shows to which switches virtual machine hosts are connected, as well as VRF tables. This helps the user quickly find where particular traffic is located in a large fabric.
- **Multi-search capabilities**. Arista offers an endpoint search by MAC address only. Cisco DCNM supports various search mechanisms for locating endpoints, including virtual machines. While not demonstrated during testing, DCNM version 11.3 offers the Kubernetes containers view.
- **Topology Overlay Views.** Unlike Arista's fairly static, basic topology display, DCNM supports multiple views, letting the user select among such topology views as Layer-2 Virtual Network Interface (L2VNI), and VRF Layer-3 (L3VNI). The user can hover the cursor over the diagram for additional detail of a particular fabric or device.
- **Operations and Maintenance (O&M).** Cisco DCNM includes an O&M capability, especially useful for deep visibility of Virtual Extended LANs (VXLANs). Arista CVP, by comparison, offers no O&M functionality.

How Arista Compares

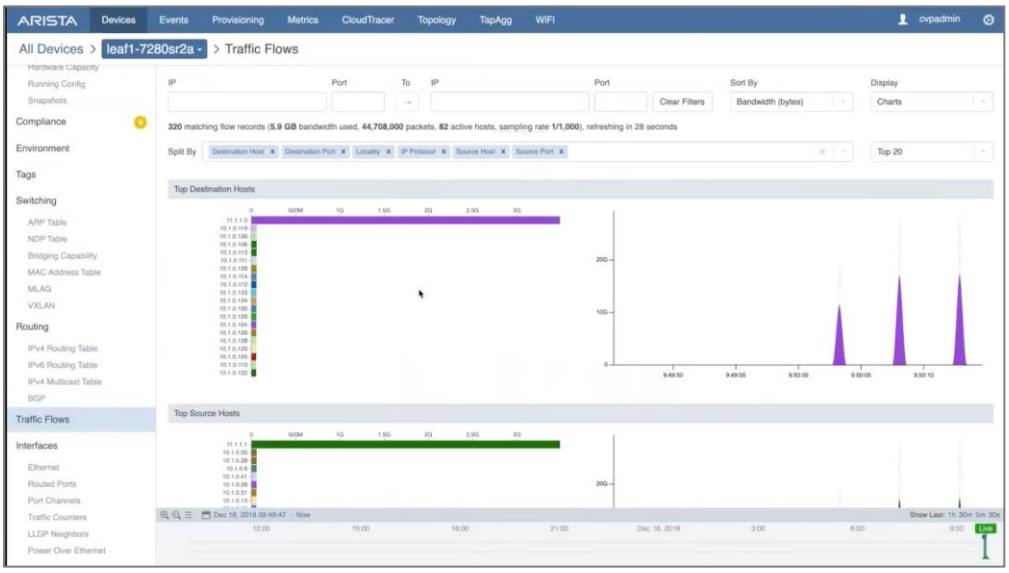
- **Static topology**. Arista CVP aggregates and displays interconnected switches in a group. There is limited capability to drill down for additional details.



***Arista CVP Single Topology View**. The above screenshot shows the topology displayed by Arista CVP. Clicking on a switch provides a list of devices attached, by MAC address.*

- **Discovery, but no auto-configuration**. Arista CVP does auto-discover interconnected Arista switches and displays them in a fairly static group. They are identified but no further auto-configuration on discovered switches is supported.
- **Limited locator**. Clicking on a switch shows MAC address, but no further details on attached devices. The user can try to find the node by entering the MAC address in the locator.
- **Third-party devices via SNMP**. Arista CVP interrogates and manages third-party devices and equipment via SNMP, which virtually all devices support. SNMP provides the ability to poll the device for current status and learn details of its configuration.

- **Data flow visibility**. The latest Arista CVP release does provide visibility of flows. CVP collects info on flows via sFlow, a standardized polling process based on sampling of traffic streams.



Arista Display of Traffic Flows. *The above screen shows the Arista display of traffic flows.*

- **No Virtual Machine integration**. Arista CVP offers no facility for displaying or monitoring the virtual machines that constitute the bulk of data center endpoints.
- **No Link or Switch-Role Awareness**. In displaying topology and provisioning, Arista CVP is unaware of switch role (i.e. whether switch is a leaf of spine) and unaware of individual links.

Network Visibility Test Summary

We found the visibility aspects of Cisco DCNM to be impressive, effective and state of the art. The network diagrams Arista CVP displays are rudimentary, not particularly insightful, and limited in terms of drilling down or changing perspective to see nodes, sites or flows of interest.

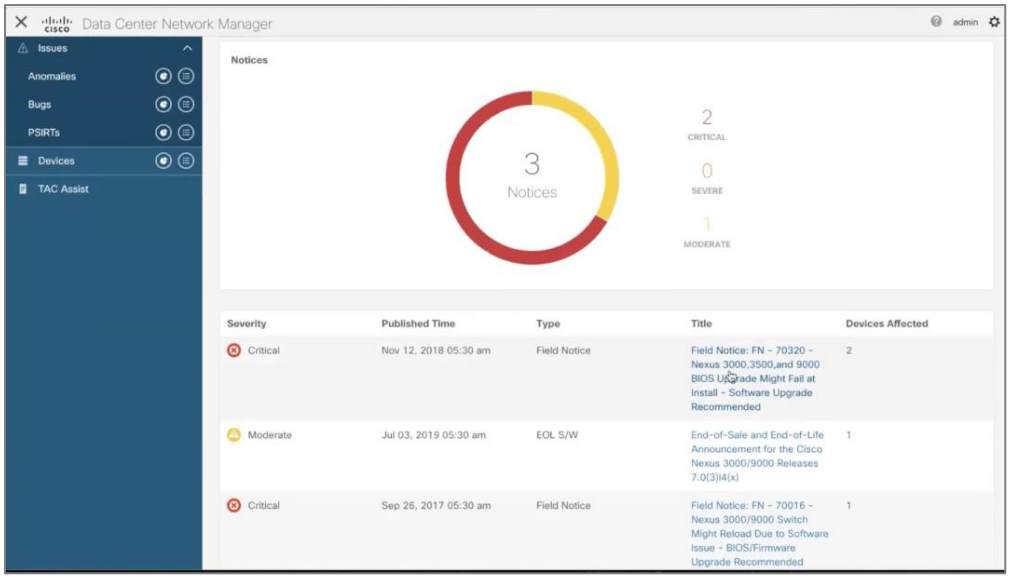
8.0 Real-time Fault Identification

Why It Matters

Event management is crucial for administrators to have control over individual network components. Each platform was expected to provide a system of real-time monitoring tools, health summaries, forwarded alerts and error identification for effective remediation.

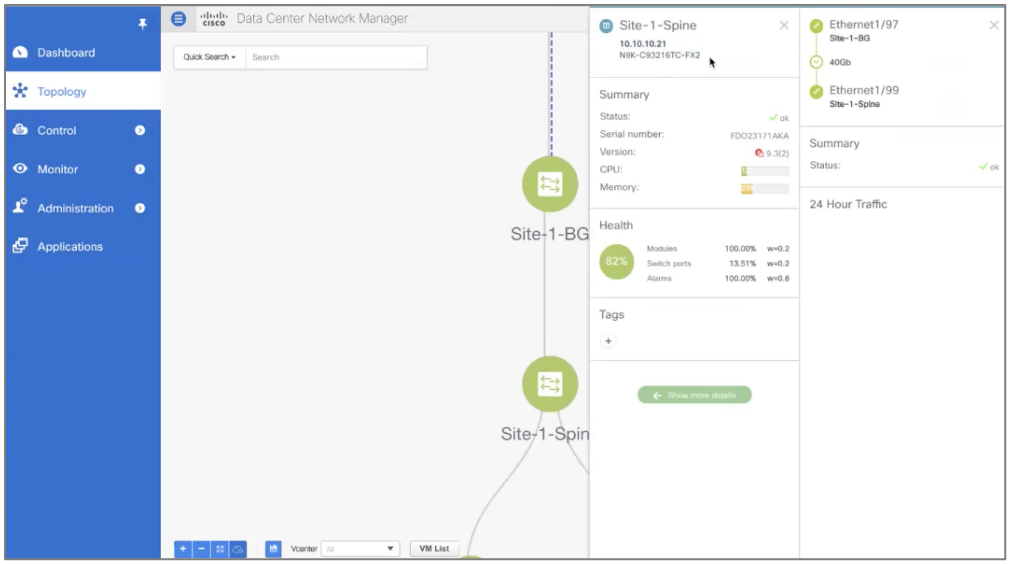
The Cisco Advantage

- **Alerts.** Alerts and alarms are issued by many different processes within DCNM. These are consolidated in a central alarm log.

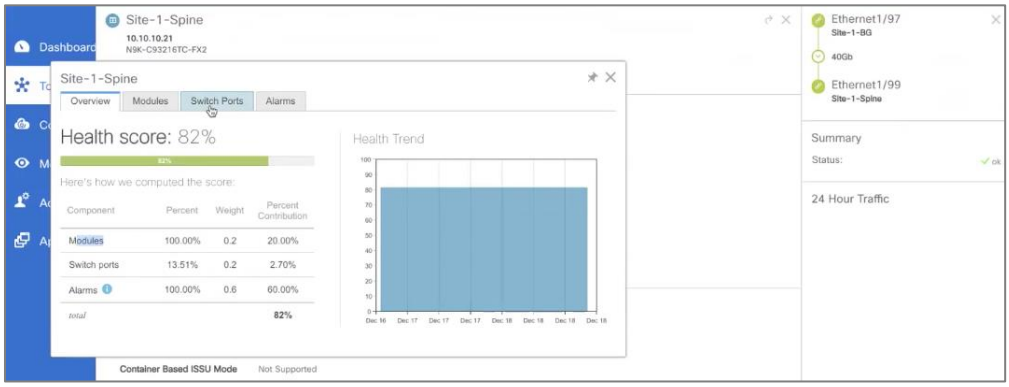


***Cisco Alarm Notification Detail**. The above interface shows the log of alarms from a high level. Each alarm shows its severity, when it was received, the type of alarm and the number of devices affected. The user can then drill down in any alarm notice for more detail, and an advisory about what to do about it.*

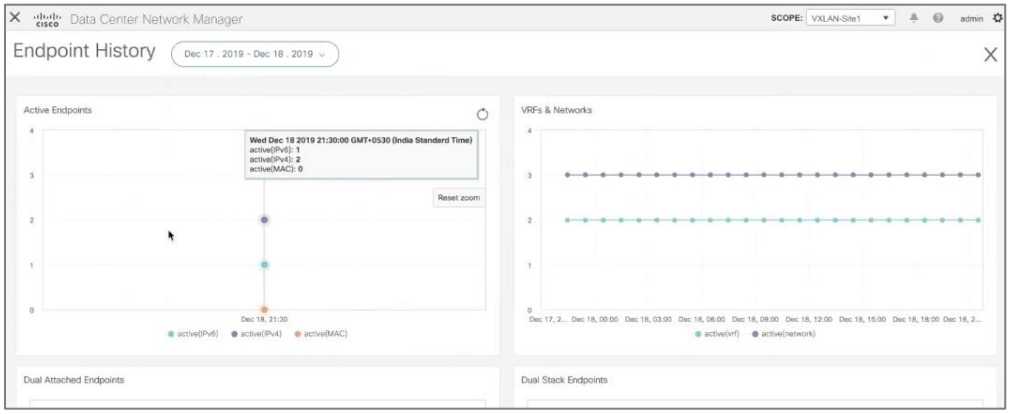
- **Configurations are continually monitored**. DCNM periodically monitors the configurations running in the Nexus switches and tracks if any "Out-of-Band" change (via CLI or other method) was made. If changes are found differing from the applied intent, DCNM will mark the switch as "Out-of-Sync," indicating a violation in compliance. This warns the user that the running configuration of a switch does not match the defined intent. The Out-of-Sync state is indicated by a color code in the topology view, and the switch Out-of-Sync state is tagged in the tabular view that lists all the switches in a fabric.
- **Monitoring and Health View**. Performance details on switches are readily available.



Cisco Topology View: Detailed Information on Switch Status.

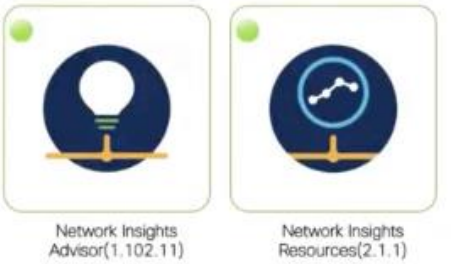


Cisco Topology View: Health Score.



Cisco Endpoint History.

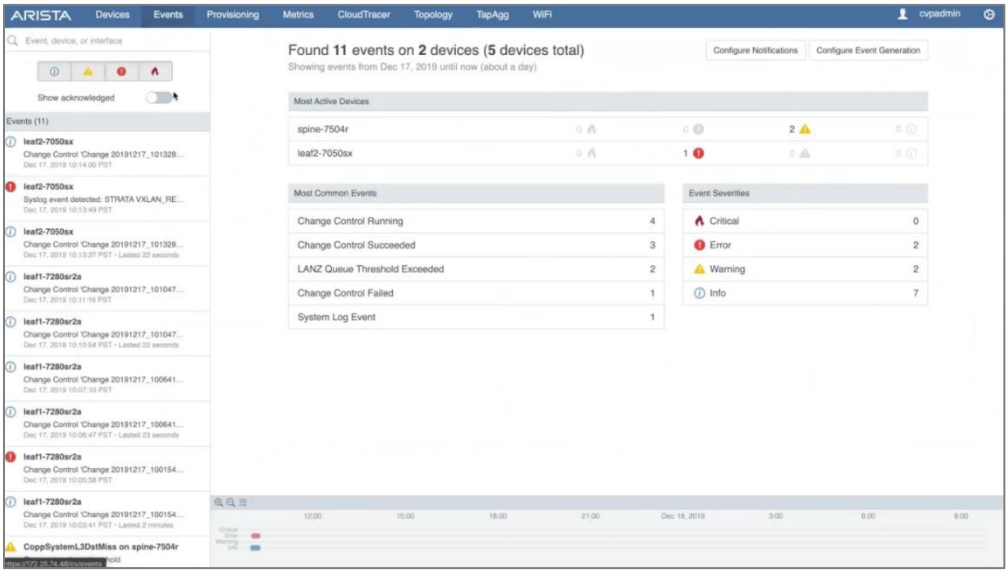
- **Topology Overlay Views.** Unlike Arista's fairly static, basic topology display, DCNM supports multiple views, letting the user select among such topology views as Layer-2 Virtual Network Interface (L2VNI), and VRF Layer-3 (VRF, L3VNI). The user can hover the cursor over the diagram for additional detail of a particular fabric or device.
- **Operations and Maintenance (O&M).** Cisco DCNM includes an O&M capability, especially useful for deep visibility of Virtual Extended LANs (VXLANs). Arista CVP, by comparison, offers no O&M functionality.
- **Network Insights.** Much of the switch data collection and fault-finding in DCNM is handled by Network Insights modules. They are: Network Insights Advisor and Network Insights Resources.



How Arista Compares

- **Telemetry.** Device-state data is streamed via NetDB State Streaming to the Arista CVP Analytics Engine – a component of Arista's Telemetry platform. All data is monitored and normalized for other applications to use, and data is stored in CVP. The CVP Analytics Engine Viewer (Aeris Browser) allows users to view device-state data.
- **Health Tracer.** The Arista CVP EOS Health Tracer increases infrastructure resiliency using a dedicated agent for software fault detection and real-time device monitoring of switch fabric and hardware integrity.
- **Path Tracer.** The Arista Path Tracer actively probes the network using synthetic packets to monitor and analyze all Layer-2 and ECMP (Equal Cost Multi-Pathing) networks. The Path Tracer can detect link issues, record packet loss and automate alerts. Responses are generated for easy detection, diagnosis and remediation for issues seen in large, scalable data center networks.
- **SNMP.** Arista CVP interrogates third-party devices via SNMP, and issues alert or alarms based on those responses.

- **Alarms and events.** Arista CVP maintains an alarm log, organized by most active alarm-generating devices and most common events and event severity.



Arista Alarm Notification. *Arista provides an effective alarm log, in which events are listed by most active devices. Events and devices can be selected for additional detail.*

- **Clients within Switches.** Client software running in Arista EOS switches continually monitors all operational aspects and automatically issues alerts and alarms to the CVP management system as appropriate.

Real-time Fault Identification Test Summary

Cisco DCNM features numerous impressive processes and corresponding displays for identifying network issues when, and ideally before, they become catastrophic. Arista CVP offers minimal fault identification. DCNM, by comparison, provides tools for continually monitoring flows, individual switches, endpoint history, and health views of fabrics, switches and endpoints.

Conclusion

Cisco DCNM outperforms its competition, the Arista CVP, in all test cases. Its provisioning and configuration go beyond basic CLI-based functionality with a user-friendly, automated process that can add multiple devices simultaneously to reduce error, time and cost.

Cisco DCNM's change-control has numerous safeguards for assuring the integrity of changes within the network, superior to the Arista CVP which offers minimal change-control functionality.

The impressive and effective network visibility of the Cisco DCNM outperforms the Arista CVP's extremely limited visibility when drilling down or changing perspectives to view nodes, sites or flows.

Identifying faults in real-time is no problem for Cisco DCNM, which offers a multitude of impressive ways to identify network issues before they affect the network. DCNM provides tools for continuous monitoring of flows, switches, and endpoints; it also gives the user visibility into heath of fabrics, switches and endpoints. Arista CVP, by comparison, offers little fault identification.

Return on Investment. As supported by our findings, Miercom concludes the Cisco DCNM enables a capable network technician or operator, through a single web-based management console, to measurably increase the overall uptime and reliability of a data center infrastructure of Cisco Nexus, Cisco MDS, and Cisco UCS (Unified Computing System) products.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied; Miercom accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.