Network Programmability and Automation with Cisco Nexus 9000 Series Switches

White Paper

November 2013

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

What You Will Learn

This document examines the increased importance of automation and programmability capabilities in the network. It explores the various trends in the data center that necessitate flexible control of the underlying infrastructure: from the emergence of modern self-service IT to increased use of continuous integration using development and operations (DevOps) models. It discusses the automation and programmability demands on the network as a result of these trends and describes the comprehensive support for these capabilities on the new Cisco Nexus® 9000 Series Switches.

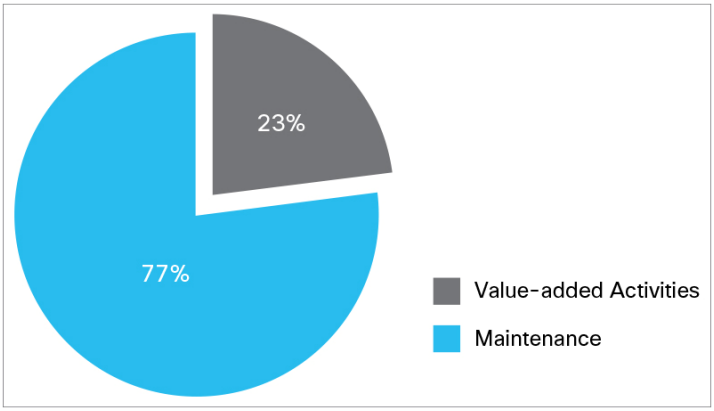
Automation and Programmability

Data center strategy has become a critical part of business strategy overall. Today, more than ever, the ways and means of IT deployment can make the difference between an efficient, successful organization and an inefficient one. That is because today IT applications and services support increasing numbers of business operations and create competitive differentiation in many industries. However, the resulting proliferation of applications and their underlying server, storage, and networking technologies is placing increasingly greater burdens on IT staff, demanding more from IT than ever before. One of the major burdens is the management of this complex IT environment, with considerable staff time needed to configure, deploy, and manage application infrastructure.

A recent IDC study shows just how heavy this burden has become. IT decision makers report that approximately three-quarters (76.8 percent) of IT staff time and resources is spent maintaining existing environments, and less than one-quarter (23.2 percent) of staff time is spent on value-added activities (Figure 1). Analysis of the maintenance portion reveals the following:

- 24 percent of staff time and resources is consumed by presystem deployment.
- 23 percent of staff time and resources is consumed by turning on and preparing systems for applications.
- 29 percent of the remaining time is spent monitoring and maintaining the IT infrastructure, including performing patch management, health monitoring, software and application updating, analysis, and troubleshooting.[1]

Figure 1. IT Staff Time and Resources Distribution



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Concurrent with the challenges of adapting to these changes in the IT industry is the continued challenge for IT to do more with flat or decreasing budgets. This confluence of factors has caused IT managers to become eager to identify and adopt new technologies and solutions that deliver efficiency for those maintenance activities that are consuming more than three-quarters of staff time. The goal of IT managers is to deliver excellent maintenance service with less staff effort and increase the focus on deployment of new services for the organization. This trend is the focal point of evolving data center strategy. Therefore, enterprises are seeking data center solutions that deliver on the efficiency promises of unified infrastructure and management products.

The adoption of converged infrastructure solutions, such as Cisco® Unified Fabric and Cisco Unified Computing System™ (Cisco UCS®), has been increasing because converged infrastructure that spans computing, networking, and storage resources can improve IT agility, protect business investments into the future, streamline deployment, and significantly increase asset utilization. Converged infrastructure helps reduce floor space needs and energy costs and provides operation benefits by creating a virtualized pool of resources. However, the real reduction in the total cost of ownership (TCO) occurs when converged infrastructure is combined with end-to-end, simplified, automated management.

Automation and programmability capabilities in the components of the data center - computing, networking, storage, and services resources - enable this end-to-end automated management. A modern network device, be it a switch or a router or a service appliance, has to support a wide range of automation features and provide robust APIs for external tools, both off-the-shelf and custom-built, to be able to automatically provision network resources, provide bandwidth allocation and latency guarantees to support network service-level agreements (SLAs), and monitor the network for performance and compliance needs.

This document describes the various use cases for network automation and programmability and discusses the features of the Cisco Nexus® 9000 Series Switches that enable these use cases.

IT as a Service

IT is increasingly being delivered as a service, with private cloud models, to provide the speed, flexibility, and competitive innovation needed by modern businesses. IT as a service (ITaaS) aims to achieve these goals:

- Accommodate rapid business growth without adding IT staff.
- Standardize the IT environment while providing the capability to expand the size, scope, and scale of services delivered to customers.
- Increase the customer base and global presence as a result of the nimbleness and agility of the IT environment.
- Increase collaboration among the development and IT teams, resulting in new automation use cases to foster even greater innovation.

ITaaS typically is implemented in several phases.

Private Cloud

The first phase of ITaaS implementation requires several building blocks:

- Self-service portal and standardized menu of services
- Service-delivery automation
- Operation-process automation
- Resource-management automation
- Service lifecycle automation

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Traditional networks use manual configuration and management mechanisms. The command-line interface (CLI), an interface designed for interactive human use, is the primary mechanism in such networks. The range of automation needed for a private cloud deployment, however, cannot be accomplished with the CLI and Simple Network Management Protocol (SNMP)-based scripts and tools. To help IT environments transition from human-led network operations to automated network operations, IT needs:

- New network automation capabilities such as Power-On Auto Provisioning (POAP) and intent-led automation using the Puppet and Chef tools
- Programming capabilities such as Representational State Transfer (REST) and JavaScript Object Notation (JSON)-based interfaces
- APIs with comprehensive language support such as that offered by the Cisco Open Network Environment (ONE) Platform Kit (onePK)

Chargeback

After implementing a private cloud infrastructure, IT departments focus on implementing chargeback models that allow business units to allocate, account for, monitor, and report resource use and associated costs. Business units get visibility into the amount they are paying for resources and the amount of their resources that is unused, allowing them to optimize resource consumption and costs. Such self-service optimizations depend on automation capabilities in the network: automated resource tracking and reporting with detailed statistics and analytics, automated resource provisioning and deprovisioning, automated tuning of quality-of-service (QoS) capabilities, etc.

Hybrid Cloud Models

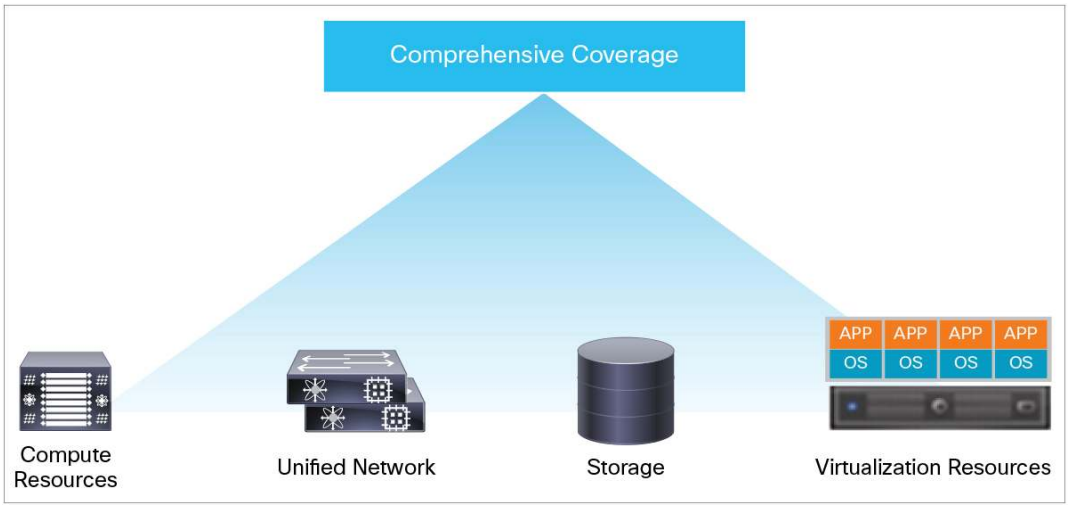
As IT departments move from these private cloud ITaaS models to hybrid cloud models that use capacity bursting and cloud-based disaster recovery, automation features become even more important: to enable automated capacity management, workload mobility, and disaster recovery. Automated VLAN and Virtual Extensible LAN (VXLAN), route injection, security configuration, analytics collection, and error reporting are critical for successful hybrid cloud deployment. In addition, programmability features with comprehensive API and language support are needed for different orchestration and management frameworks in the public and private cloud domains to enable automatic configuration and management of the network.

Infrastructure Provisioning and Operations

Organizations endeavor to automate every aspect of their infrastructure: bare-metal, virtualized computing, networking, and storage resources and services (Figure 2). Automation of infrastructure provisioning can bring immense benefits by reducing the infrastructure light-up time: the amount of time that capital investments stay unused. This strategy also allows time-consuming, error-prone manual tasks to be replaced by automated tasks that are completed in dramatically faster times with increased accuracy. Similarly, after the infrastructure is operational, automation of day-to-day management, monitoring, and configuration changes can increase the efficiency of infrastructure operations teams.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 2. Goal of Organizations: Comprehensive Automation of Infrastructure



Tasks that can be automated include:

- Autodiscovery and provisioning of devices
- Role-based and policy-based management of infrastructure
- Configuration management, event management, power management, and availability management of all devices and their components
- Autodiscovery of all components of a device, such as chassis, servers, fans, modules, memory units, and disks
- Dynamic provisioning of device resources (interfaces, VLANs, switch and port profiles, routes, etc.)
- Inventory, operation, and licensing status reports for all devices
- Continuous monitoring of resource utilization and capacity

Network automation is a crucial aspect of this comprehensive automation strategy. Features such as POAP and intent-based automation with the Puppet and Chef tools dramatically reduce network deployment and configuration times. Programming tools such as Python scripting and APIs such as Cisco NX-API and Cisco onePK enable instantaneous provisioning and automated monitoring through integration with existing tools and frameworks.

Development and Operations Models and Continuous Integration

Development and operations (DevOps) models of software development and deployment, with their agility in deploying new features and patches and their resulting business benefits, have become increasingly popular over the past few years. DevOps environments enable rapid enhancement and tuning of applications with continuous deployments: applications with rates ranging from tens of deployments per day to thousands of deployments per day, depending on the application and organization. With this rate of change, to enable a DevOps model, automation of infrastructure operations and management is not just desirable but required. Network devices, as critical parts of the infrastructure, need to support automation and programmability features.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

As new applications are deployed, the infrastructure resources need to be provisioned to enable the applications. From a network perspective, various configuration tasks may need to be automated: provisioning of new VLANs, VXLANs, Virtual Routing and Forwarding (VRF) instances, and QoS policies; injection of new routes into the network; etc. In ongoing deployments, network parameters may need to be changed to allow or restrict communications between components of the application or to tune networks for performance, based on application needs. Modification of routing parameters, addition and removal of access control lists (ACLs), modification of QoS parameters, etc. may need to be accomplished in the network.

Network devices need to provide comprehensive automation capabilities and APIs to support the new configuration change and operation model and to integrate with agile software development methodologies and tools that are prevalent in such environments.

Monitoring and Advanced Analytics

Network administrators seek a holistic view of the way that the network is performing and the ways that users are experiencing the delivery of applications and services. Comprehensive visibility empowers the network administrator to:

- Optimize network resources by characterizing application performance and use of network resources
- Troubleshoot problems with quick access to critical network information across bare-metal, virtual, and cloud environments
- Deliver consistent performance levels by assessing the impact of changes, such as server consolidation and virtual machine migration, on network performance

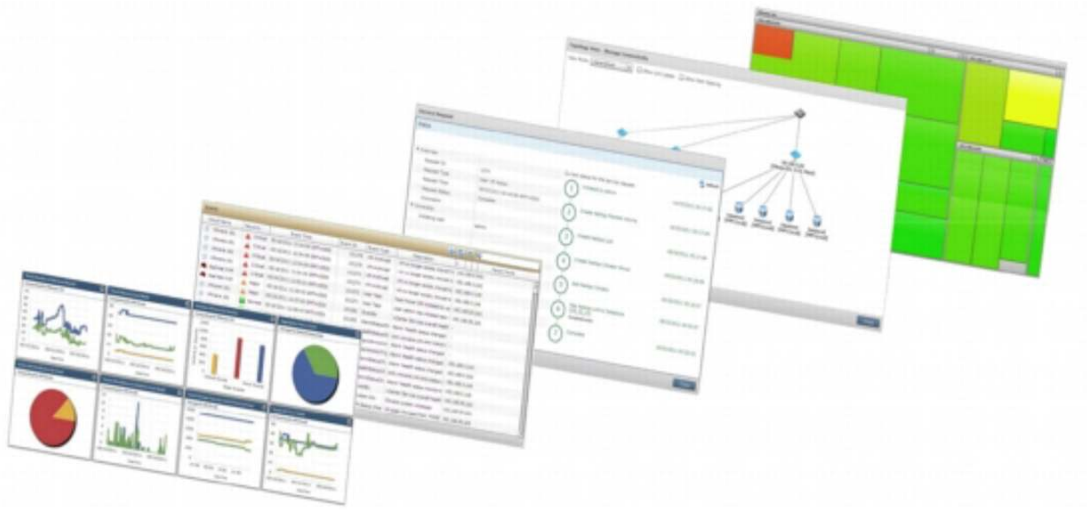
Tools that enable these capabilities depend on the APIs and interfaces exposed by network devices to gather information and identify events of interest and trends. They present information to the user in context-relevant reports with:

- Comprehensive traffic statistics and application, voice, and video performance metrics
- Detailed troubleshooting with insightful packet captures, advanced filters, and error scanning
- Centralized management and reporting

Traditional monitoring and analytics tools could use only basic features of network devices such as SNMP, CLI, syslogs, and remote monitoring (RMON) capabilities. Modern tools can provide more powerful monitoring and analytics by using new capabilities such as REST APIs, Python scripting, and comprehensive APIs such as Cisco NX-API and Cisco onePK. These APIs enable a variety of all-encompassing views of the network to be exposed to the administrator and also role-based, context-sensitive views to end users (Figure 3). The APIs also allow the tools to, optionally, modify certain network parameters automatically based on trends derived from the analytics: for example, migrate traffic to a different route if a specific route is congested.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 3. Examples of Monitoring Views Provided by Cisco UCS Director



Security and Compliance

With the increased pace of infrastructure convergence with cloud models, it is increasingly common for multiple tenant, organizations, and applications to share the same infrastructure. In such an environment, it is very important to gain visibility across the entire infrastructure to help ensure not just the security goals of the infrastructure team, but also the security and compliance expectations of the individual tenants and organizations.

The visibility and audit requirements from the network require the network to embody certain characteristics. The network must be:

- Observable: The network needs to provide visibility into resource use, secure resource segmentation, statistics, and performance across tenants and organizations.
- Controllable: The network should provide capabilities to change security parameters to meet security, compliance, and visibility needs.
- Automatable: The scale and complexity of today's networks dictate automated collection and monitoring of information for security and compliance needs. The same level of collection and monitoring cannot be accomplished with manual intervention.

To meet these needs, networks need to expose a very large amount of very detailed configuration and operation information to external tools and entities. A robust set of APIs, such as that exposed by Cisco onePK and Cisco NX-API, that tools can use to query network information can be critical for a secure data center. Automation capabilities such as those provided by Python scripting and Puppet and Chef integration, can help ensure that the network stays in compliance throughout the duration of its operation, even in the event of new threats and requirements.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco Nexus 9000 Series: Automation and Programmability Capabilities

To meet the numerous demands of the network in the modern data center, a network device - or more particularly, the operating system that powers that device - must be:

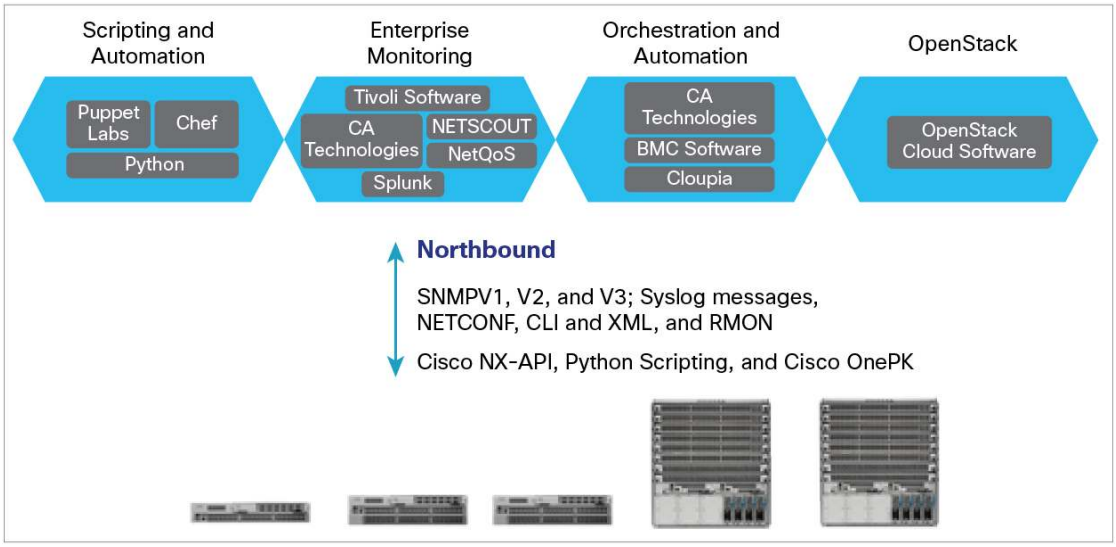
- Resilient: To provide critical business-class availability
- Modular: To be capable of extension to evolve with business needs and provide an extended lifecycle
- Highly programmable: To allow rapid automation and orchestration through APIs
- Secure: To protect and preserve data and operations
- Flexible: To integrate and enable new technologies
- Scalable: To accommodate and grow with the business and its requirements
- Easy to use: To reduce the amount of learning required, simplify deployment, and ease manageability

The enhanced Cisco NX-OS Software is designed to meet all these criteria while running on the Cisco Nexus 9000 Series Switches. The Cisco Nexus 9000 Series consists of Cisco Nexus 9500 platform modular switches and Cisco Nexus 9300 platform fixed-configuration switches.

Equipped with enhanced Cisco NX-OS as the operating system, Cisco Nexus 9000 Series Switches function in unified fabric mode to provide network connectivity through traditional means but with exceptional performance, resiliency, and programmable automation functions.

Enhanced Cisco NX-OS on the Cisco Nexus 9000 Series integrates with a variety of open source software (OSS) and commercial technologies to provide comprehensive automation, orchestration, programmability, monitoring, and compliance support (Figure 4).

Figure 4. Cisco Nexus 9000 Series: Comprehensive Ecosystem Integration



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Standard Network Manageability Features

The Cisco Nexus 9000 Series supports standard network manageability features that are widely used by network administrators and operators for automation (Figure 5):

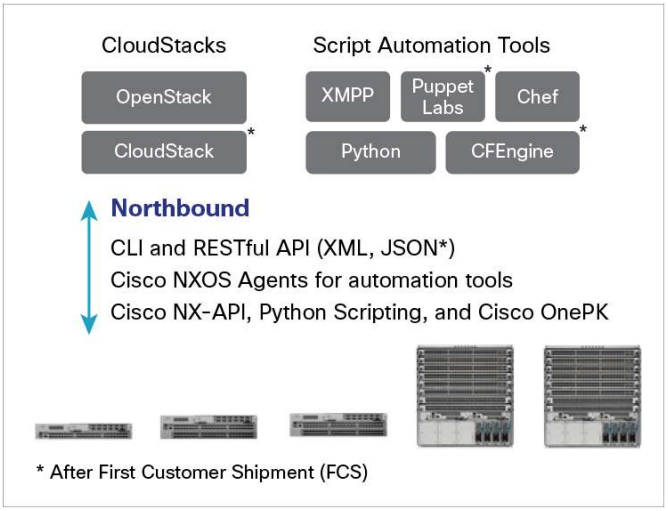
- SNMPv1, v2, and v3
- Syslog
- RMON
- Network Configuration Protocol (NETCONF)
- CLI and CLI scripting

Figure 5. Core Management Features

Advanced Automation Features

Enhanced Cisco NX-OS on the Cisco Nexus 9000 Series supports numerous capabilities to aid with automation. The platform incorporates comprehensive APIs that expose an extensive set of functions, providing investment protection with the capability to add support for new automation capabilities in the future (Figure 6).

Figure 6. Support for Integration of Comprehensive Orchestration and Automation Functions



Power-On Auto Provisioning

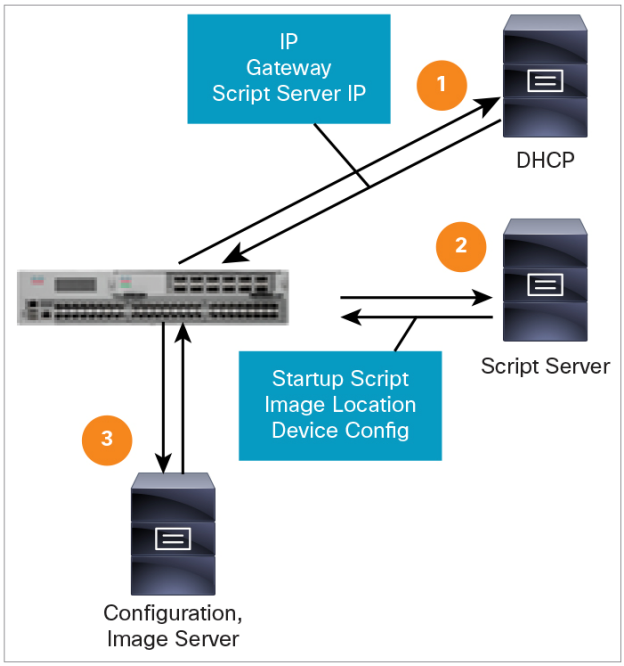
POAP automates the processes of installing and upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

When a Cisco Nexus switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode, locates a Domain Host Configuration Protocol (DHCP) server, and boots itself with its interface IP address, gateway, and Domain Name System (DNS) server IP address. The switch also obtains the IP address of a Trivial FTP (TFTP) server or the URL of an HTTP server and downloads a configuration script that enables the switch to download and install the appropriate software image and configuration file (Figure 7).

POAP enables touchless bootup and configuration of new Cisco Nexus 9000 Series Switches, reducing the need for time-consuming, error-prone, manual tasks to scale network capacity.

Figure 7. Automated Provisioning of Cisco Nexus 9000 Series with POAP



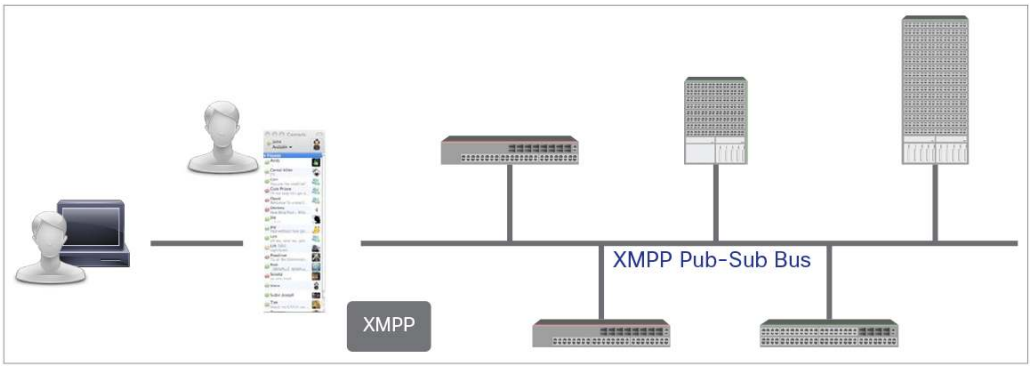
Extensible Messaging and Presence Protocol Support

Enhanced Cisco NX-OS on the Cisco Nexus 9000 Series integrates an Extensible Messaging and Presence Protocol (XMPP) client into the operating system. This integration allows a Cisco Nexus 9000 Series Switch to be managed and configured by XMPP-enabled chat clients, which are commonly used for human communication. XMPP support enables several useful capabilities:

- Group configuration: Add a set of Cisco Nexus 9000 Series devices to a chat group and manage a set of Cisco Nexus 9000 Series Switches as a group. This capability can be useful for pushing common configurations to a set of Cisco Nexus 9000 Series devices instead of configuring the devices individually.
- Single point of management: The XMPP server can act as a single point of management. Users authenticate with a single XMPP server and gain access to all the devices registered on the server.
- Security: The XMPP interface supports role-based access control (RBAC) and helps ensure that users can run only the commands that they are authorized to run.
- Automation: XMPP is an open, standards-based interface. This interface can be used by scripts and management tools to automate management of Cisco Nexus 9000 Series devices (Figure 8).

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 8. Automation with XMPP Support on Cisco Nexus 9000 Series



Puppet and Chef Integration

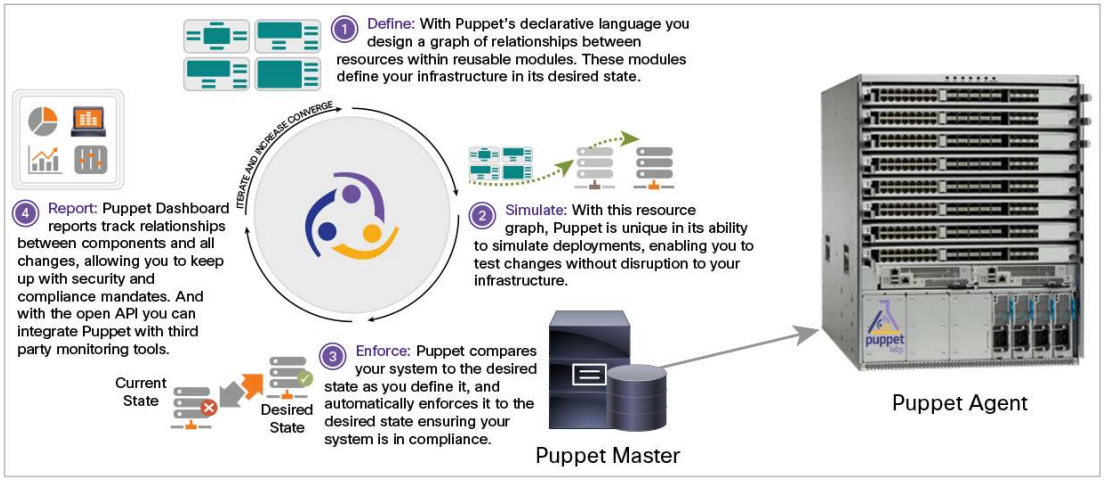
Puppet and Chef are two popular intent-based infrastructure automation frameworks.

Chef allows users to define their intent through a recipe - a reusable set of configuration or management tasks - and allows the recipe to be deployed on numerous devices. The recipe, when deployed on a Cisco Nexus 9000 Series Switch, translates into network configuration settings and commands for collecting statistics and analytics information. The recipe allows automated configuration and management of a Cisco Nexus 9000 Series Switch.

Puppet provides a similar intent-definition construct, called a manifest. The manifest, when deployed on a Cisco Nexus 9000 Series Switch, translates into network configuration settings and commands for collecting information from the switch.

Both Puppet and Chef are widely deployed and receive significant attention in the infrastructure automation and DevOps communities. The Cisco Nexus 9000 Series supports both the Puppet and Chef frameworks, with clients for Puppet and Chef integrated into enhanced Cisco NX-OS on the switch (Figure 9).

Figure 9. Automation with Puppet Support on Cisco Nexus 9000 Series



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

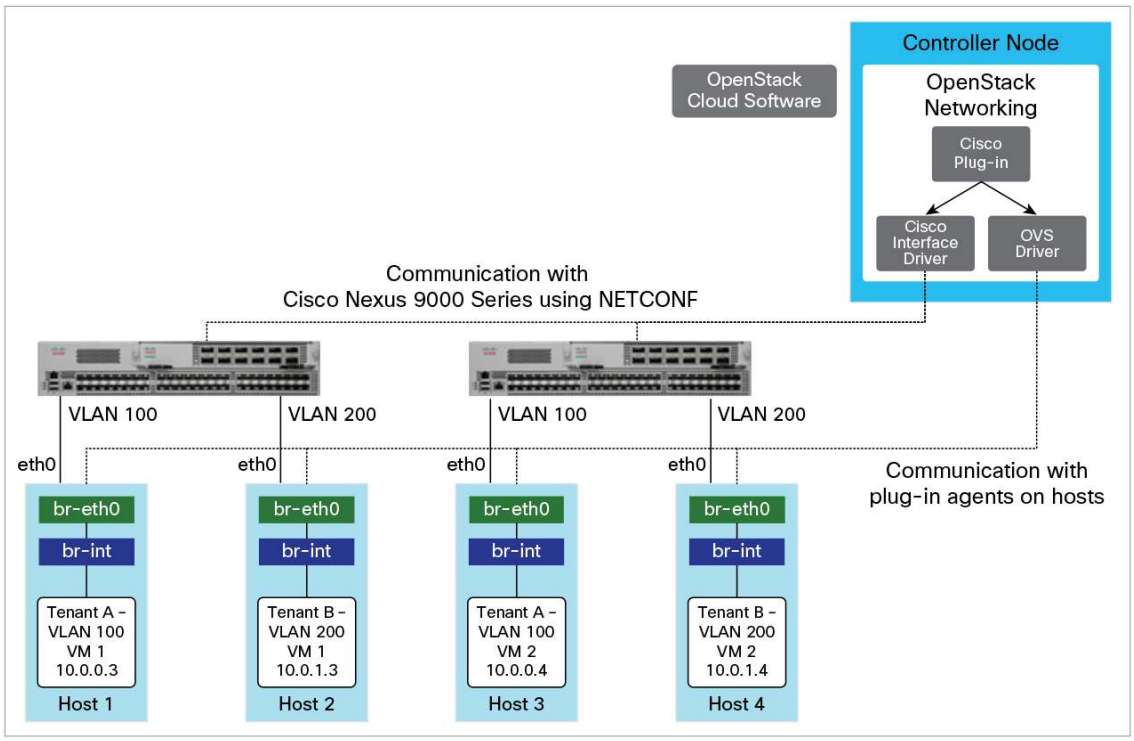
OpenStack Integration

The Cisco Nexus 9000 Series includes support for the Cisco Nexus plug-in for OpenStack Networking (Neutron). The plug-in allows customers to easily build their infrastructure-as-a-service (IaaS) networks using the industry's leading networking platform, delivering performance, scalability, and stability with familiar manageability and control. The plug-in helps bring operation simplicity to cloud network deployments. OpenStack's capabilities for building on-demand self-serve multitenant computing infrastructure are well known. However, implementing OpenStack's VLAN networking model across virtual and physical infrastructures can be difficult.

OpenStack Networking provides an extensible architecture that supports plug-ins for configuring networks directly. However, each network plug-in enables configuration of only that plug-in's target technology. When OpenStack clusters are run across multiple hosts with VLANs, a typical plug-in configures either the virtual network or the physical network, but not both.

The Cisco Nexus plug-in solves this problem by enabling the use of multiple plug-ins simultaneously. A typical deployment runs the Cisco Nexus plug-in in addition to the standard Open vSwitch (OVS) plug-in. The Cisco Nexus plug-in accepts OpenStack Networking API calls and directly configures Cisco Nexus switches as well as OVS running on the hypervisor. Not only will the Cisco Nexus plug-in configure VLANs on both the physical and virtual network, but it also intelligently allocates VLAN IDs, deprovisioning them when they are no longer needed and reassigning them to new tenants whenever possible. VLANs are configured so that virtual machines running on different virtualization (computing) hosts that belong to the same tenant network transparently communicate through the physical network. Moreover, connectivity from the computing hosts to the physical network is trunked to allow traffic only from the VLANs configured on the host by the virtual switch (Figure 10).

Figure 10. Cisco OpenStack Neutron Plug-in with Support for Cisco Nexus 9000 Series Switches



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 1. Cisco Nexus Plug-in for OpenStack Networking

Requirement	Challenge	Cisco Plug-in Resolution
Extension of tenant VLANs across virtualization hosts	VLANs must be configured on both physical and virtual networks. OpenStack Networking supports only a single plug-in at a time. The operator must choose which parts of the network to manually configure.	Accepts OpenStack Networking API calls and configures both physical and virtual switches
Efficient use of limited VLAN IDs	Static provisioning of VLAN IDs on every switch rapidly consumes all available VLAN IDs, limiting scalability and making the network more vulnerable to broadcast storms.	Efficiently uses limited VLAN IDs by provisioning and deprovisioning VLANs across switches as tenant networks are created and destroyed
Easy configuration of tenant VLANs in top-of rack (ToR) switch	Operators need to statically provision all available VLANs on all physical switches, a manual and error-prone process.	Dynamically provisions tenant-network-specific VLANs on switch ports connected to virtualization hosts through the Cisco Nexus plug-in driver
Intelligent assignment of VLAN IDs	Switch ports connected to virtualization hosts are configured to handle all VLANs, reaching hardware limits very soon.	Configures switch ports connected to virtualization hosts only for the VLANs that correspond to the networks configured on the host, enabling accurate port-to-VLAN associations
For large, multirack deployments, aggregation switch VLAN configuration	When computing hosts run in several racks, ToR switches need to be fully meshed, or aggregation switches need to be manually trunked.	Supports Cisco Nexus 2000 Series Fabric Extenders to enable large, multirack deployments and eliminate the need for aggregation-switch VLAN configuration

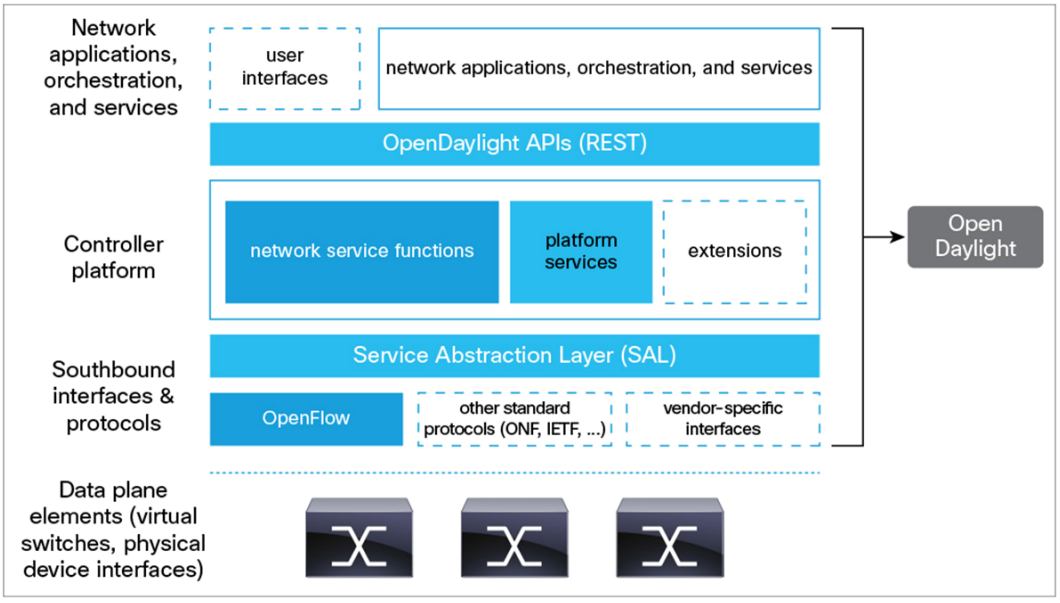
OpenDayLight Integration and OpenFlow Support

The Cisco Nexus 9000 Series will support integration with the open source OpenDayLight project championed by Cisco (Figure 11). OpenDayLight is gaining popularity in certain user groups because it helps meet some of their requirements from the infrastructure:

- Operators want affordable real-time orchestration and operation of integrated virtual computing, application, and networking resources.
- Application developers want a single simple interface for the network. Underlying details such as “router,” “switch,” or “topology” can be a distraction that they want to abstract and simplify.

The Cisco Nexus 9000 Series will integrate with the OpenDayLight controller though well-published, comprehensive interfaces such as Cisco onePK.

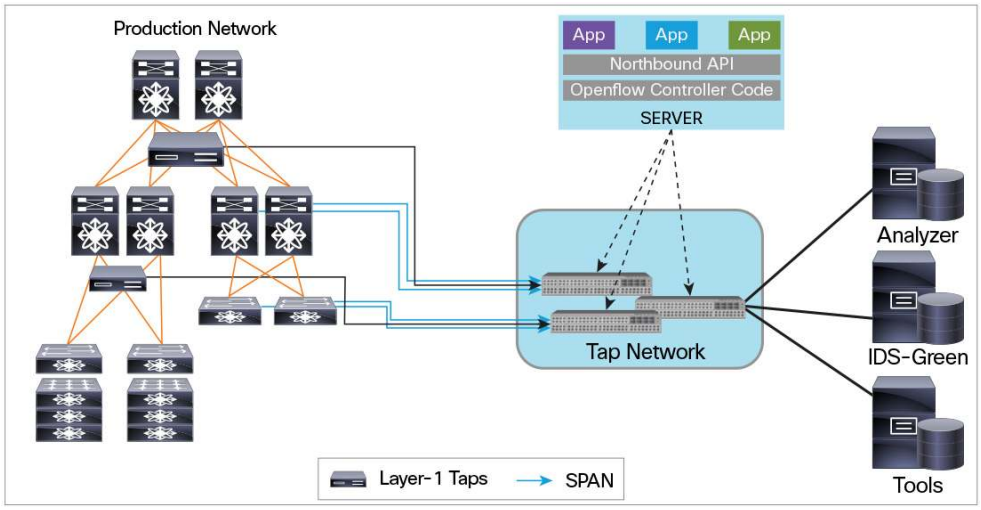
Figure 11. OpenDaylight: Future Support on Cisco Nexus 9000 Series



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

The Cisco Nexus 9000 Series will also support OpenFlow to enable use cases such as network tap aggregation (Figure 12).

Figure 12. Tap Aggregation Using OpenFlow Support on Cisco Nexus 9000 Series



Comprehensive Programmability Support

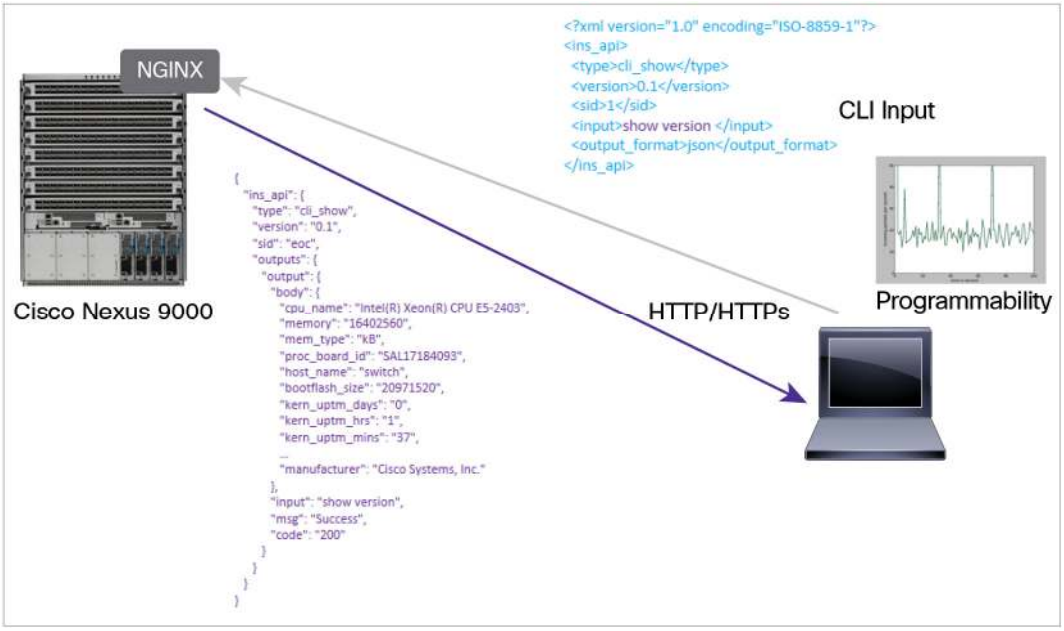
Comprehensive programmability features available on enhanced Cisco NX-OS on the Cisco Nexus 9000 Series enable custom automation and scripting.

Cisco NX-API Support

Cisco NX-API on the Cisco Nexus 9000 Series Switches allows web-based programmatic access to the Cisco Nexus 9000 Series. This support is delivered through an open source web server, NGINX. Cisco NX-API exposes the complete configuration and management capabilities of the CLI through web-based APIs. The Cisco Nexus 9000 Series Switches can be instructed to publish the output of the API calls in either XML or JSON format. This comprehensive, easy-to-use API enables rapid development on the Cisco Nexus 9000 Series Switches (Figure 13).

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 13. Programmatic Access to Cisco Nexus 9000 Series Through Cisco NX-API



Python Scripting

Python is an easy-to-learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an excellent language for scripting and rapid application development in many areas on most platforms. The Python interpreter and the extensive standards library are freely available in source or binary form for all major platforms from the Python website: http://www.python.org/.

The same site also contains distributions of and pointers to many free third-party Python modules, programs, and tools and additional documentation.

The Cisco Nexus 9000 Series supports Python Release 2.7.5 in both interactive and noninteractive (script) modes.

The Python scripting capability on the Cisco Nexus 9000 Series Switches gives programmatic access to the switch CLI to perform various tasks and POAP and Cisco Embedded Event Manager (EEM) actions. Responses to Python calls that invoke a Cisco NX-OS CLI return a JSON output instead of just text output: a powerful feature that makes Python scripting easy and helps ensure that the scripts are forward compatible.

The Python interpreter is available by default in Cisco NX-OS.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Various repetitive, manual workflows that are error prone can be automated either on-device or off-device using the Python scripting capabilities on the Cisco Nexus 9000 Series (Figures 14 and 15).

Figure 14. Manual, Repetitive Troubleshooting Steps Used to Track a Node in the Network

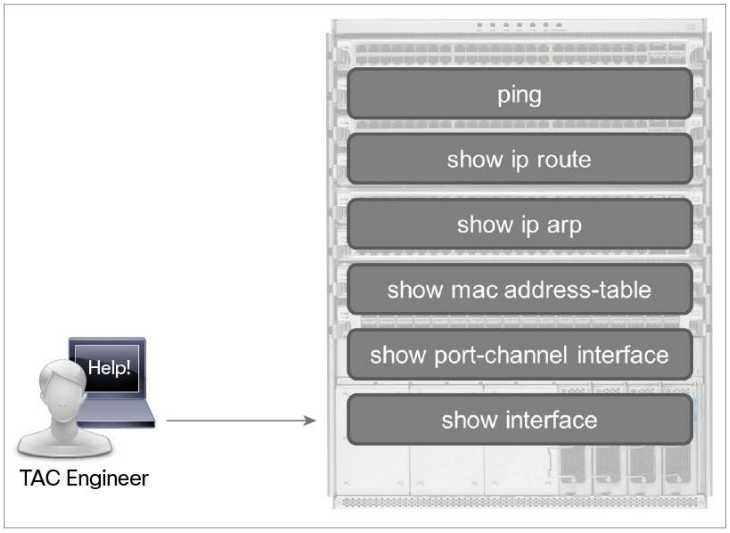
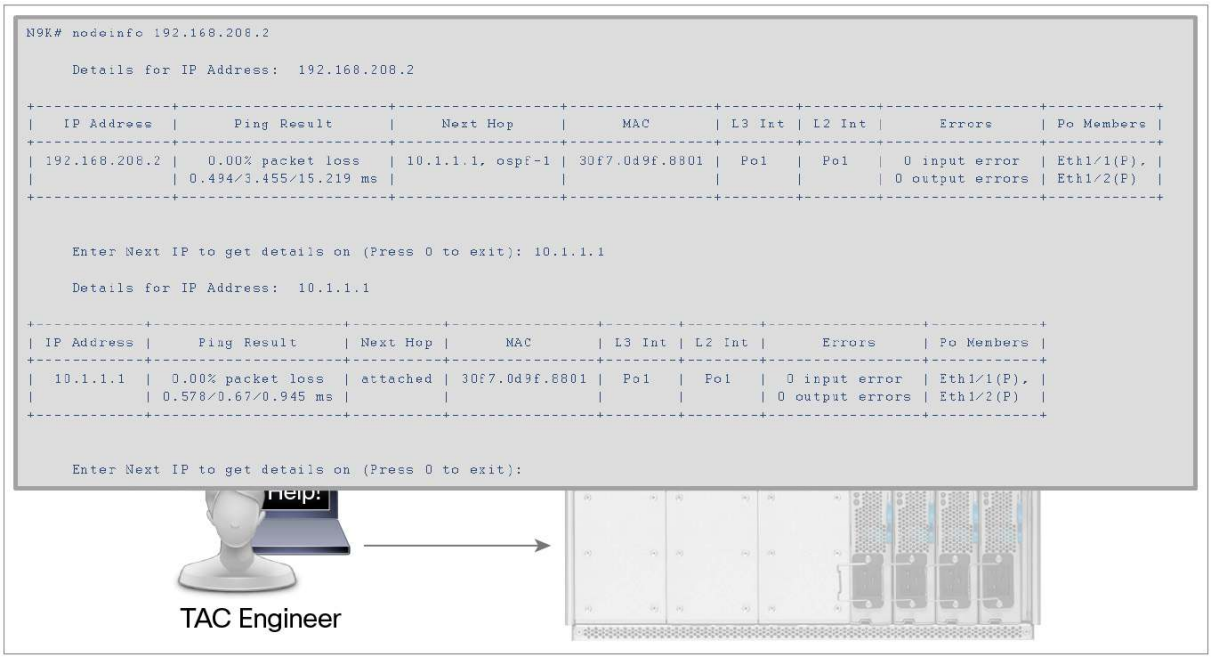


Figure 15. Automated Node Information Collection with Python Scripting Support on Cisco Nexus 9000 Series



Cisco onePK

Cisco onePK is a main element of the Cisco ONE software-defined networking (SDN) strategy. Cisco onePK is an easy-to-use toolkit for development, automation, rapid service creation, and more. It enables timely access to the valuable data in the network through easy-to-use, comprehensive APIs.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

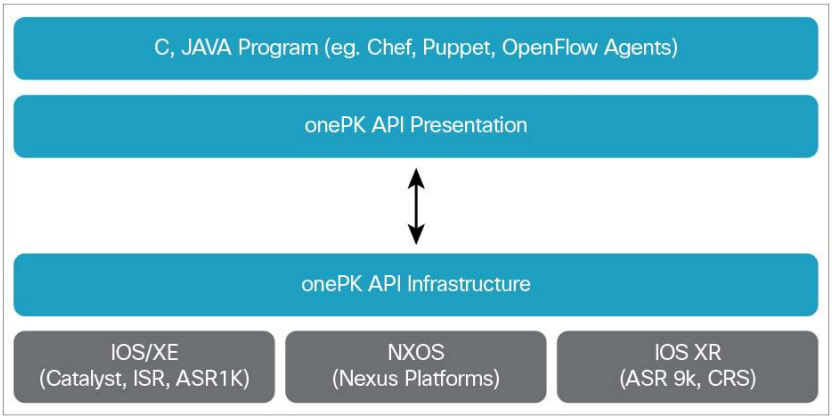
Cisco onePK provides the capability to build or extend applications across routers and switches to servers and new business platforms. It enables organizations to quickly automate current services or create new ones on demand when and where they are needed. Cisco onePK makes the network more powerful and flexible while providing detailed programmatic control.

Cisco onePK brings numerous benefits to the data center:

- Build, automate, and improve: Create new or improve existing applications and services and increase productivity.
- Adapt quickly: Provide flexibility to meet rapidly changing business needs and reduce operating costs.
- Extend: Extend the capabilities of your network.
- Gain new revenue opportunities: Monetize new applications and services and create services more quickly with code that you can write once and run anywhere.

Cisco Nexus 9000 Series Switches incorporate support for Cisco onePK to enable programmatic access through a wide variety of programming languages (Figure 16).

Figure 16. Support for Cisco onePK Across a Variety of Platforms Including Cisco Nexus 9000 Series

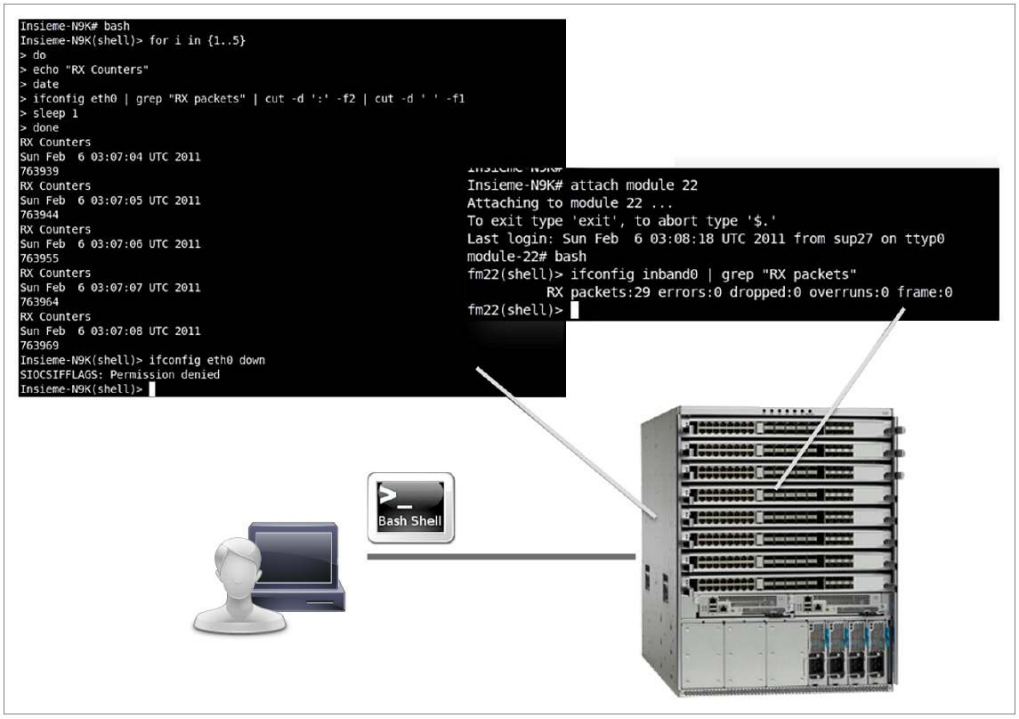


Bash Shell Access and Linux Container Support

Network operators in DevOps environments and modern enterprise data centers endeavor to use the comprehensive tool and scripting capabilities developed for the computing environment on network devices. To support our customers, Cisco has enabled support for direct Linux shell access and for Linux containers. With Linux shell access, customers can access the underlying Linux system on the Cisco Nexus 9000 Series Switches to use the Linux commands with which they are familiar and to manage the underlying system (Figure 17). Customers can also use support for Linux containers to install their own software in a relatively secure fashion to enhance the capabilities of the Cisco Nexus 9000 Series.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 17. Bash Access to Cisco NX-OS on the Supervisor and on Line Cards



Customers, for example, are installing bare-metal provisioning tools such as Cobbler on Cisco Nexus 9000 Series devices to enable automatic provisioning of bare-metal servers from the ToR switch.

Conclusion

Modern data centers require a highly available network that provides the bandwidth and service guarantees required by organizations and their applications. In addition to performance and resiliency characteristics, modern networks need to support several new capabilities: automated provisioning and monitoring of network resources, programmatic access to statistics and events to enable end-to-end visibility, and RBAC and policy management. The Cisco Nexus 9000 Series is powered by enhanced Cisco NX-OS, an open, Linux-based, modern operating system. The switches expose a comprehensive set of automation and programmability features to meet the requirements of data center operations teams. The capabilities are comprehensive in both their breadth, with support for a wide variety of technologies (commercial and OSS), and depth, with comprehensive automation features and APIs. They enable a wide variety of use cases (Table 2).

Table 2. Use Cases for Automation and Programmability Capabilities of Cisco Nexus 9000 Series

	ITaaS	Infrastructure Provisioning and Automation	DevOps	Monitoring	Security and Compliance
Automation					
POAP	Yes	Yes			Yes
Chef Integration	Yes	Yes	Yes	Yes	Yes
Puppet Integration	Yes	Yes	Yes	Yes	Yes
XMPP Support	Yes	Yes	Yes		
OpenStack Support	Yes	Yes			

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

	ITaaS	Infrastructure Provisioning and Automation	DevOps	Monitoring	Security and Compliance
Automation					
OpenDaylight	Yes	Yes			
OpenFlow				Yes	
Programmability					
Cisco NX-API	Yes	Yes	Yes	Yes	Yes
Python Scripting	Yes	Yes	Yes	Yes	
Cisco onePK	Yes	Yes	Yes	Yes	Yes
Bash Support	Yes	Yes	Yes	Yes	
Linux Containers	Yes	Yes	Yes	Yes	

Cisco understands that the needs of the market evolve rapidly as technologies evolve and new technologies emerge. Cisco has a long history of responding to customer needs and has designed enhanced Cisco NX-OS on the Cisco Nexus 9000 Series Switches to evolve rapidly with new features. Starting with a strong foundation, the Cisco Nexus 9000 Series provides a comprehensive set of automation and programmability features that can be built on in the future.

For More Information

Please visit http://www.cisco.com/go/nexus9000 for more information

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 www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-729385-00 11/13

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.