

Networking and Cloud: An Era of Change

What You Will Learn

As you deploy cloud infrastructure and operating models in your organization, the role that networking plays and the impact of these models on your networks may not always be clear. This document discusses the importance of the network to cloud computing, why the network must change, and what Cisco is doing to lead these changes.

CLOUD MODELS

CLOUD SERVICE MODELS

- Infrastructure as a service (IaaS) provides users with processing, storage, networks, and other computing infrastructure resources. The user does not manage or control the infrastructure, but has control over operating systems, applications, and programming frameworks.
- Platform as a service (PaaS) enables users to deploy applications developed using specified programming languages or frameworks and tools on the cloud infrastructure. The user does not manage or control the underlying infrastructure, but has control over deployed applications.
- Software as a service (SaaS) enables users to access applications running on a cloud infrastructure from various end-user devices (generally through a web browser). The user does not manage or control the underlying cloud infrastructure or individual application capabilities other than through limited user-specific application settings.

CLOUD DEPLOYMENT MODELS

- Private clouds are operated solely for one organization. They may be managed by the organization itself or by a third party, and they may exist on or off premises.
- Public clouds are open to the general public or to a large industry group and are owned and managed by a cloud service provider.
- Hybrid clouds combine two or more clouds (private or public) that remain unique entities but are bound together by technology that enables data and application portability.
- Community clouds have infrastructure that is shared by several organizations and supports a specific community. They may be managed by the organizations or a third party and may exist on or off premises.

Source: NIST
(<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>)

The Network Is Critical to Cloud Computing

Cloud computing is a model in which IT resources and services are abstracted from the underlying infrastructure and provided on demand and at scale in a multi-tenant environment.

Cisco uses the U.S. National Institute of Standards (NIST) cloud framework, differentiating between service and deployment models (see sidebar).

From a networking standpoint, each service model requires the cloud provider to expose more or less of the network and provide more or fewer networking capabilities to cloud users. Conversely, each service model requires cloud users to understand and design more or less of the network to which they are exposed. The network is most exposed in the IaaS model and least in the SaaS model.

The essential technological difference between the deployment models is derived from the networking relationship between the cloud user and the cloud provider. In a private cloud, the user and provider are within the same trusted network boundary. In a public cloud, they are on different networks. In a hybrid cloud, a secured connection may exist between the user's and provider's networks, or the user's network may extend into the provider's cloud (or the reverse). In a community cloud, the structure depends on the charter and architecture of the organizations operating the cloud.

Every cloud is some combination of a service and deployment model. Regardless of the type of cloud, however, one fact remains true: no network means no cloud. Without networks, users cannot access their cloud services. Without networks, applications, data, and users cannot move between clouds. Without networks, the infrastructure components that must work together to create a cloud

cannot.

Networking Has to Change

Networking must change because the rise of cloud models is changing what is happening on the network:

- New **infrastructure**: For example, everything is becoming virtualized, infrastructure is becoming programmable, and servers and applications have mobility
- New **applications**: For example, data-intensive analytics, parallel and clustered processing, telemedicine, remote experts, and community cloud services
- New **access**: For example, mobile device-based access to everything and virtual desktops
- New **traffic**: For example, predominantly server-to-server traffic patterns and location-independent endpoints on both sides of a service or transaction

What you need to do with and to data has not changed. Data still needs to travel between the computing and storage components of an application and then to the user of the application. Security still must be applied to help make sure that the right users, devices, and systems have access to the right data at the right time while protecting against attacks, intrusions, breaches, and leaks. Different kinds of data and traffic have different levels of importance and network resource needs that still must be met across the entire network with quality-of-service (QoS) capabilities.

However, how you do these things has to change:

- Network architecture needs to be flexible, instead of being a static stumbling block
- Network services need to be location independent: delivered wherever data, applications, and users are and whenever the services are needed
- Network resources need to be abstracted so that provisioning can be automated and actions orchestrated through common interfaces

What Cisco Is Doing to Evolve the Network

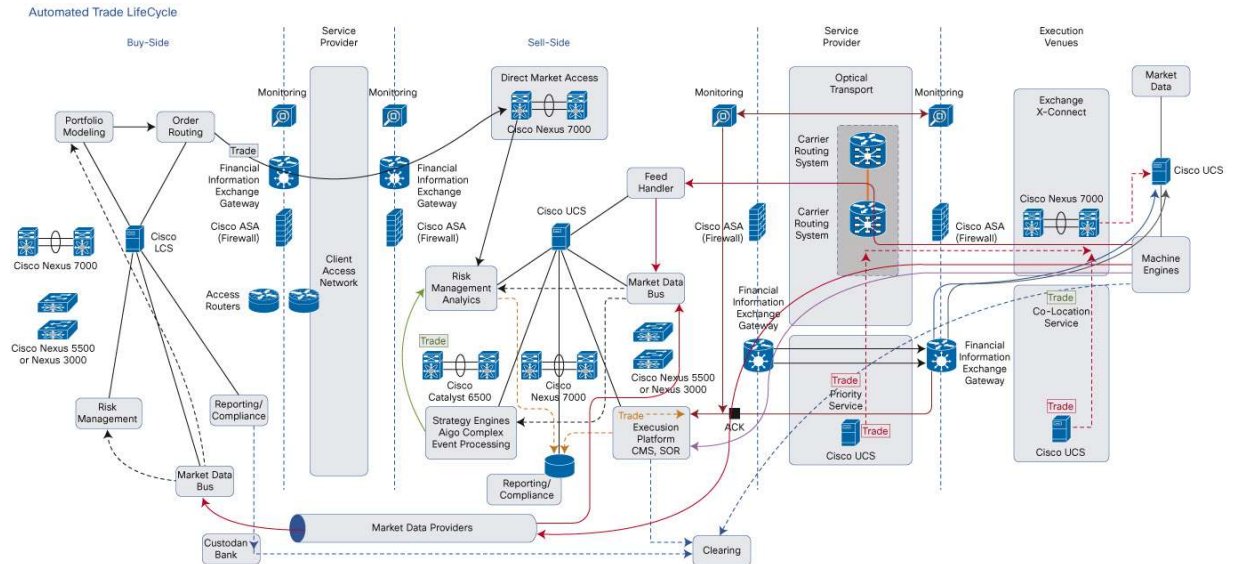
In addition to enabling open, resilient, secure, and scalable networks, Cisco is helping make networks more flexible, integrated, mobile, and automated.

Flexibility

There is no single, fundamental architecture or design pattern that will satisfy the requirements of all cloud models, all applications, all users, or all of Cisco's customers. Through the breadth and depth of its innovations, Cisco is making sure that there is a solution for every use and that there is the correct mix of products and capabilities so that your investment is protected for the longest term possible while maintaining performance competitiveness:

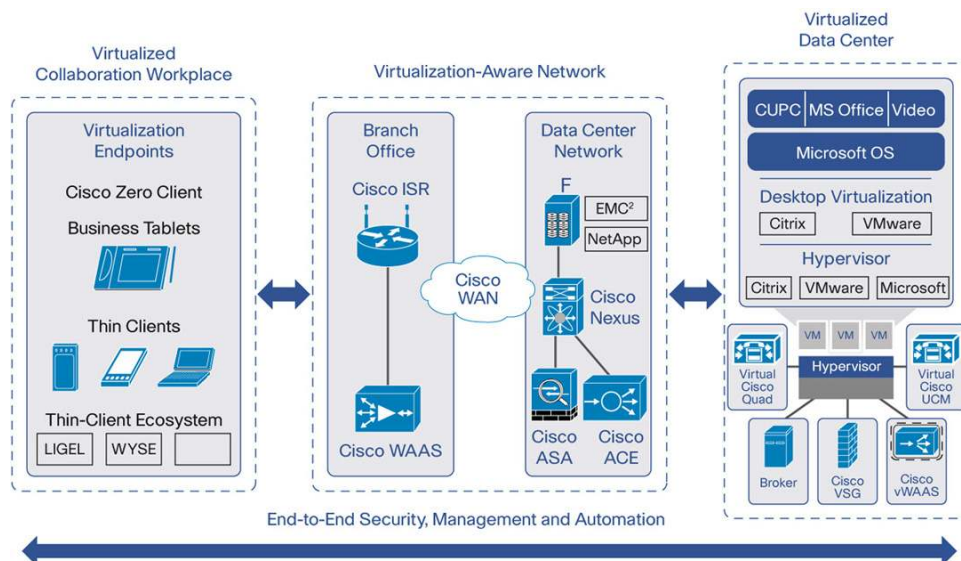
- One-, two-, or multiple-layered network designs with flexible placement of boundaries between Layer 2, Layer 3, and higher-level services
- Designs for comprehensive performance at scale across the entire network underlying a transaction or application, instead of designs for single steps or subparts within that process (Figure 1)

Figure 1. Cisco's High-Performance Trading Fabric



- Scalability from one rack to a whole data center to collections of data centers
- Services such as security and application acceleration delivered in the best form factor, physical or virtual, wherever needed (Figure 2)

Figure 2. Application Acceleration, WAN Acceleration, and Security Services Deployed as Appliances, Software Modules, and Virtualized Services working Directly with the Hypervisor in a Cisco Virtualization Experience Infrastructure (VXI) Architecture



- Virtualization and security to divide a single infrastructure into isolated “network containers” for different tenants, applications and data, and zones of security
- New approaches to building and operating networks, such as software-defined networking and controller-based networks

Integration

Integration is needed both out from and in to the network. Cisco is creating a fabric that presents diverse systems' capabilities as part of an integrated infrastructure, as a cloud, with networking as the fundamental platform:

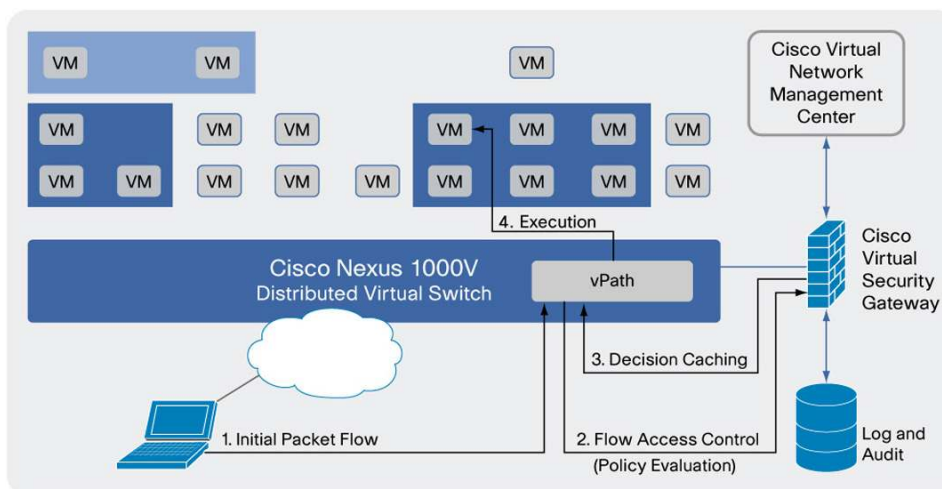
- A single network for all data and traffic in the cloud: one set of devices, one cable plant, and one management system (Figure 3)

Figure 3. Cisco Unified Fabric Using an End-to-End Fibre Channel over Ethernet (FCoE) Data Center Network with Unified Management



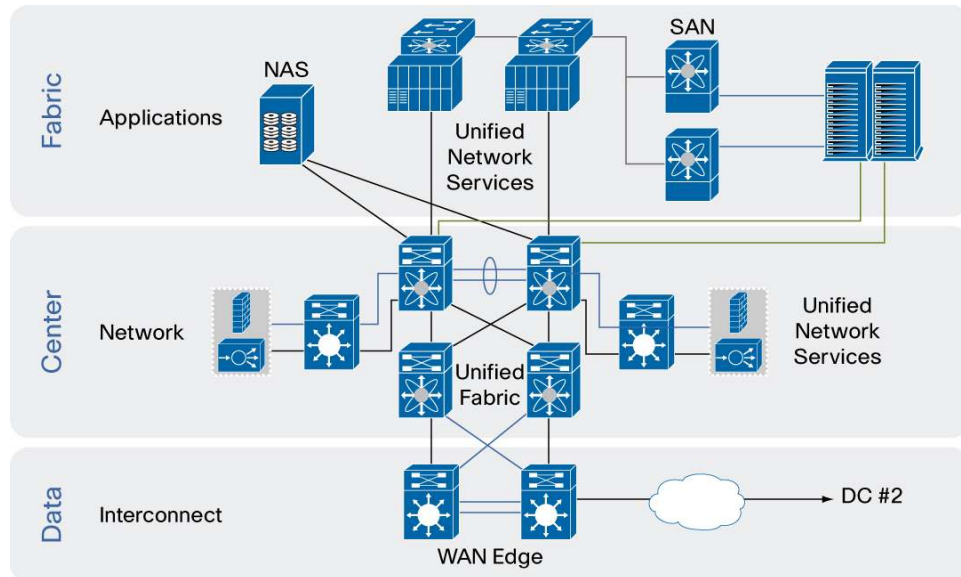
- Security and encryption for every kind of traffic and data, controlled and implemented through the network
- Advanced networking capabilities delivered deep into the servers and virtualization platforms running the cloud infrastructure (Figure 4)

Figure 4. Cisco Virtual Security Gateway (VSG) Working with the Cisco Nexus® 1000V Switch with vPath to Provide Firewall Services Between Virtual Machines



- Policy enforcement that is context aware and performed from the network
- Integration of all the IT resources in a data center into a fabric for the cloud (Figure 5)

Figure 5. Cisco Data Center Fabric



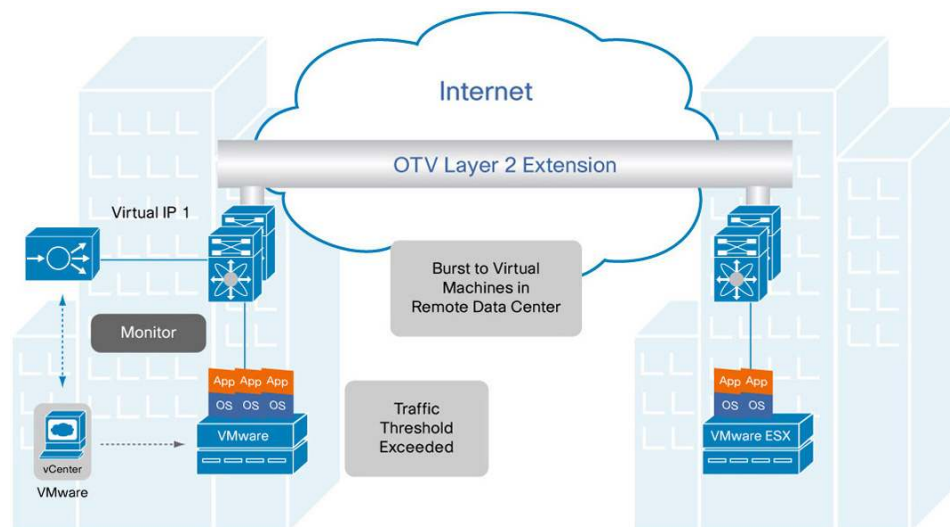
Mobility

There is an increasing proliferation of phones and other mobile devices that are being used to access applications and data from clouds across many different kinds of networks.

Until recently, “mobile” mainly referred to these devices and the networks that support them. Now, however, with cloud infrastructure, applications and servers also have become mobile: able to move from one part of a cloud to another or even from one cloud to another. Cisco is making the network aware of and accommodating to not just users accessing the cloud, but also the applications and data in the cloud:

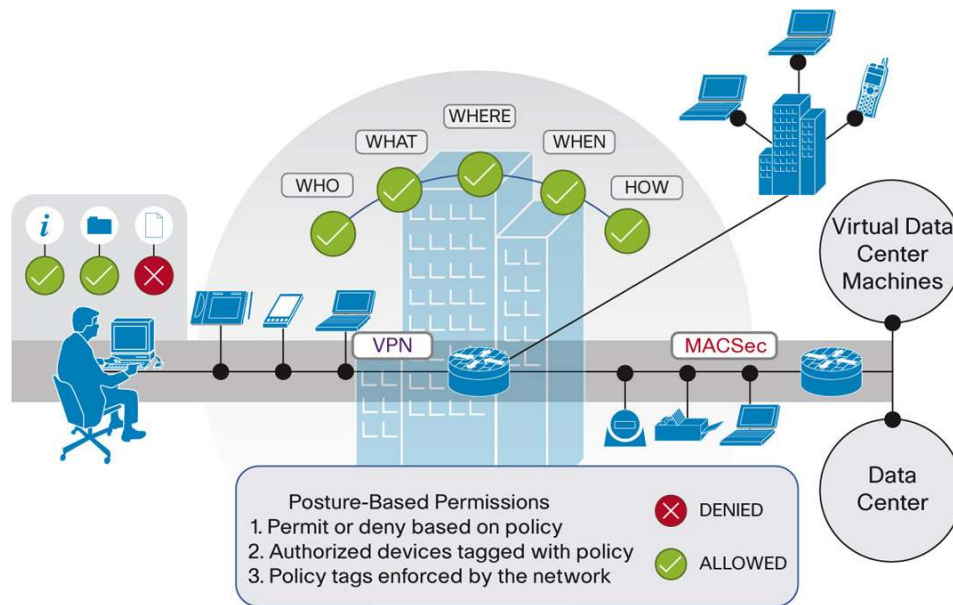
- Extending and interconnecting clouds, enabling application and data and user mobility between clouds (Figure 6)

Figure 6. Cisco Application Control Engine (ACE) Overlay Transport Virtualization (OTV) Dynamic Capacity Expansion: Bursting Traffic to a Standby Data Center or Virtual Private Cloud



- Providing consistent quality of service across the entire network
- Enforcing policies on devices, users, data, and applications regardless of location and making the policy enforcement points themselves mobile
- Providing a consistent policy infrastructure, centralized management, separation of duties, and the capability to deliver federated sign-on and policy enforcement across clouds (Figure 7)

Figure 7. Mobile Policy Enforcement Across Multiple Devices and Locations

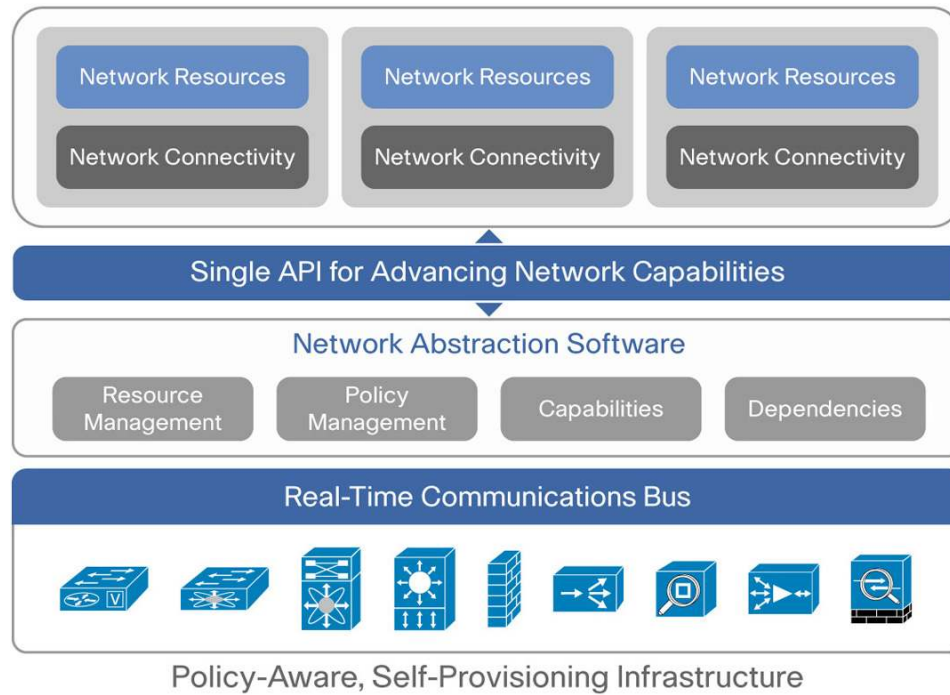


Automation

While virtualization and the capability to control parts of the infrastructure programmatically through APIs and automation are becoming standard, the network has lagged behind in affording the same manageability to developers, engineers, and operators. Cisco is bringing agility into the fabric through abstraction and automation of network resources:

- Creating an API to automate the provisioning of network resources for the fabric (Figure 8)

Figure 8. A Single API Across the Entire Network



- Creating self-service catalog, orchestration, and automation tools to provision all IT resources in the fabric
- Enabling the collection of metrics directly from the fabric for analysis and response
- Working with the OpenStack group to create an open-source network-as-a-service (NaaS) capability for provisioning networking resources in open cloud environments

What Does It Mean for Me?

The network is fundamental to cloud computing. However, networks have to change for the cloud. Cisco is leading this change to create networks that are more flexible, integrated, mobile, and automated. Ask yourself what your network should be doing for the cloud:

- Do you need to accelerate access to the cloud?
- Do you need to provide network security for virtual machines?
- Do you need to create virtual data centers for use by multiple customers?
- Do you need to operate a vast, flat, single-layer network for large clusters of virtual machines?
- Do you need to enable users to move from one cloud to another while maintaining the same credentials?

Cisco makes all these capabilities possible today while innovating to meet the future challenges of the network.

For More Information

As you begin your own journey to the cloud, we invite you to discuss the right approach for your organization with your Cisco account manager, channel partners, and other IT advisors. For additional information about cloud computing, please visit <http://www.cisco.com/go/cloud>.



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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

Printed in USA

C11-677946-00 08/11