# Virtualized Multi-Tenant Data Center Solution for Infrastructure-as-a-Service

Cloud computing is one of the fastest growing opportunities for enterprises and service providers. Enterprises use the Infrastructure-as-a-service (IaaS) model to build private clouds and virtual private clouds that reduce operating and capital expenses and increase the agility and reliability of their critical information systems. Service providers build public clouds to offer on-demand, secure, multi-tenant, pay-per-use IT infrastructure to businesses and government agencies that use cloud services to offload, or augment, their internal resources using a public cloud infrastructure.

## What You Will Learn

Cisco uses its comprehensive understanding of networks and its ecosystem of partners to develop a trusted approach to cloud computing, which includes advancements in cloud security and automation. Cisco architectures for cloud computing help service providers build secure public clouds and help enterprises and other organizations build private clouds, which combine the flexible, on-demand qualities of a cloud with the control and stability of a traditional data center.

This document describes the Cisco® Virtualized Multi-Tenant Data Center (VMDC) architecture, version 2.0, to build an end-to-end IaaS cloud computing infrastructure for the following deployments:

- Enterprise private clouds
- Service provider public clouds

This document is a shorter version of a Cisco design implementation guide, which provides more detail about the architecture, platforms, network design, and implementation of a cloud computing IaaS deployment.

## Cloud Computing Solutions to Business Challenges

IT departments face several business challenges today, including the following:

- High capital and operating expenditures and overhead caused by resource needs
- Low responsiveness to business needs due to complex IT operations; tasks such as manual configuration and resource provisioning are complicated and time consuming to streamline
- Inefficient resource use in dedicated physical infrastructures; resource pools are customized per application, resulting in fewer shared resources
- Difficulty in scaling resources up and down dynamically, resulting in longer deployment times
- Difficulty in integrating elements of the cloud with other operational elements in the data center (operations, change request management, etc.), resulting in higher operating expenses

Cloud computing offers several capabilities to users and network administrators. These capabilities provide several tangible benefits for enterprises, detailed in Table 1.

**Table 1.** Benefits of Cloud Capabilities

| Cloud Capabilities | Benefits |
|---|---|
| **Flexible resource allocation**<br>**Efficient resource allocation**<br>**Democratization of resource allocation** | Agile IT service delivery<br>Rapid provisioning<br>Reduced deployment times<br>Optimized cost<br>Higher server and storage utilization<br>Lower power and cooling costs<br>Reduced capital expenditures (CapEx) and operating expenses (OpEx)<br>Reduced total cost of ownership (TCO) |

## Logical Building Blocks for Cloud

Logical building blocks for cloud computing include the following (Figure 1):

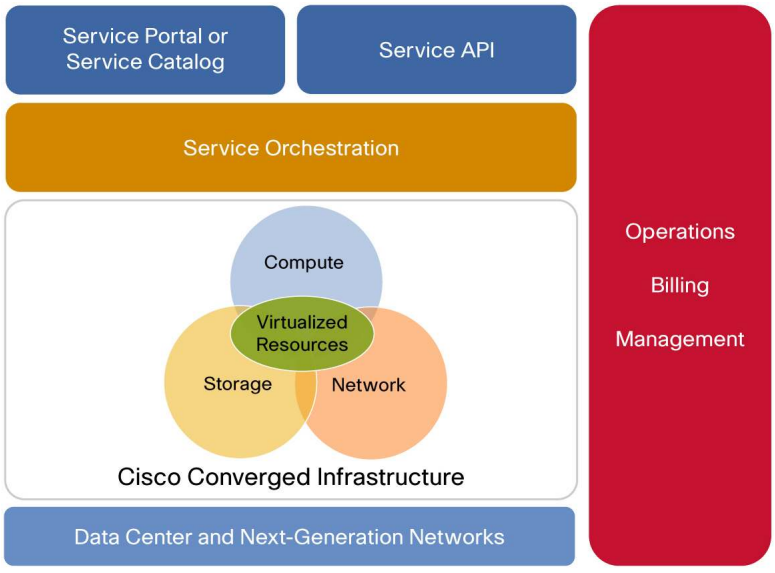
**Virtualized resources:** Network, compute, and storage resources are the building blocks of a cloud deployment. The virtualized resources are shared by users and applications, and they promote efficiency in resource allocation.

**Service orchestration:** Orchestration software automates and orchestrates routine tasks and functions that operators perform. It coordinates the activities of configuration automation solutions across servers, clients, and network devices, resulting in faster provisioning of resources. It automates processes across multiple applications and tools, as well as across multiple IT groups, such as support and operations, making cross-silo integration easier, faster, and more reliable. Orchestration is critical to the basic definition of cloud as it enables on-demand and scalable IT resources in a multi-tenant environment.

**Service portal and service APIs:** To transform cloud services into a utility computing model, you must define and expose a service catalog as a portal or set of service APIs to clients who consume cloud resources. Using the catalog, clients select resources based on requirements and initiate record keeping to track costs, or chargebacks, for those resources.

**Operations and management:** This building block includes systems for billing, asset and configuration management, software license management, change and release management, service desk, and, service-level management.

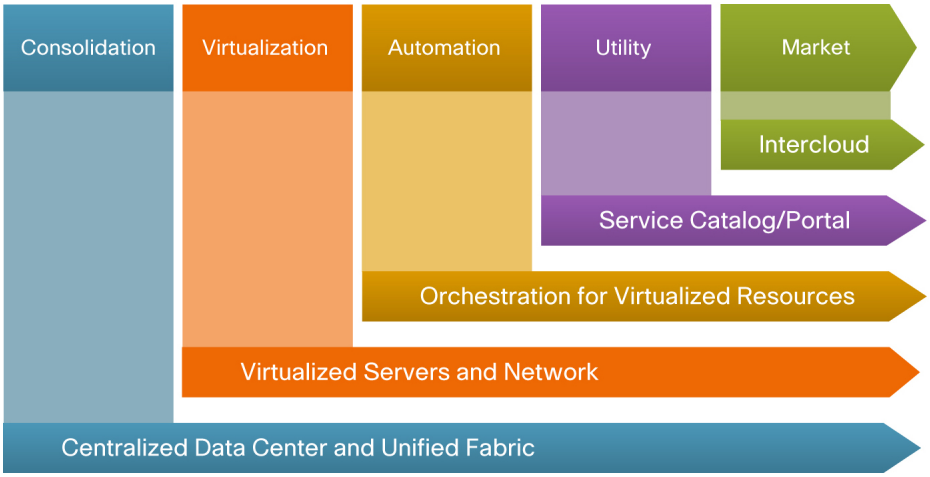
**Figure 1.** Logical Building Blocks for a Cloud Build-out



## Incremental Value at Each Step in the Journey toward the Cloud

Enterprises that want to deploy private clouds can work in stages, secure in the knowledge that incremental value and return on investment (ROI) exists at each stage. To serve their customers and generate additional revenues, service providers can build an end-to-end public cloud infrastructure that is scalable, secure, multi-tenant and resilient (Figure 2).

**Figure 2.** Steps Toward Deploying an Enterprise Private Cloud




**Consolidation:** Many large enterprises are consolidating to reduce data center and server sprawl, reduce power and cooling costs, or implement a unified fabric using Cisco Nexus® Family data center switches.

**Virtualization:** Virtualization is a great enabler of consolidation. Server virtualization enables consolidation because more applications run on fewer compute resources. Network path isolation virtualization allows a single common network infrastructure to carry traffic from multiple customers or compute environments and helps ensure that the traffic remains separated.

**Automation:** Automation of resource element manager and service orchestration tasks reduces provisioning time and simplifies management and optimization of resource pools. Presenting resources as a utility empowers clients to choose the resources and services they need, which results in flexibility, efficiency, and democratization of resource allocation that reduces OpEx.

**The Cisco Advantage:** The Cisco Unified Computing System™ with unified fabric dramatically reduces the number of network adapters, blade-server switches, and cables needed as it passes network traffic to parent fabric interconnects. These interconnects process and centrally manage the traffic to improve performance. They also reduce the number of devices that need to be powered, cooled, secured, and managed. With multiple-role management embedded in the interconnects to manage configuration and operation, separate element managers are no longer required for each component. In addition, Cisco VN-Link Virtualization support gives network links connected to virtual machines the same status as physical links. I/O configurations and network profiles move with the virtual machines, increasing security and efficiency while reducing complexity. This virtual network interface card (vNIC) feature improves performance and reduces NIC infrastructure.

Cisco's long-term vision is an open, public cloud network called the inter-cloud. It involves a long-term market transition marked by ubiquitous portable workloads and a rich cloud environment in which external and internal clouds share resources. The inter-cloud will allow secure and transparent movement of resources based on available capacity, power cost, and proximity to promote a new wave of innovation.

## End-to-End Architecture Design and Validation for Cloud-Based IaaS Deployment

Architectural blueprints for enterprise private clouds and service provider public clouds with the IaaS delivery model are quite similar. Both require transparent scaling to enable rapid on-demand deployment, lights-out management and automation, and integrated operations and monitoring of the underlying infrastructure systems. They differ in the importance of multi-tenancy controls and security, as well as the scale of service operations. The Cisco VMDC architecture is a validated design of a virtualized multi-tenant cloud infrastructure that confers several benefits:

**Proven design:** Building out a cloud computing environment with complex requirements and choices can be a challenging task. Numerous Cisco and ecosystem vendor technologies are interwoven to form the foundation of an end-to end cloud infrastructure. Cisco's efforts in integrating solutions from strategic partners allow administrators to use the knowledge and best practices gleaned from the integration efforts to make their processes smoother.

**Reduced deployment time and OpEx savings:** Cisco has addressed the cloud computing challenge with an end-to-end systems approach. We deliver a well-designed, fully tested, and documented solution that allows our customers to transition more rapidly and cost effectively to a virtualized, cloud-based infrastructure. This solution reduces the need for network administrators to start from the beginning in validating the architecture, saving time and money.

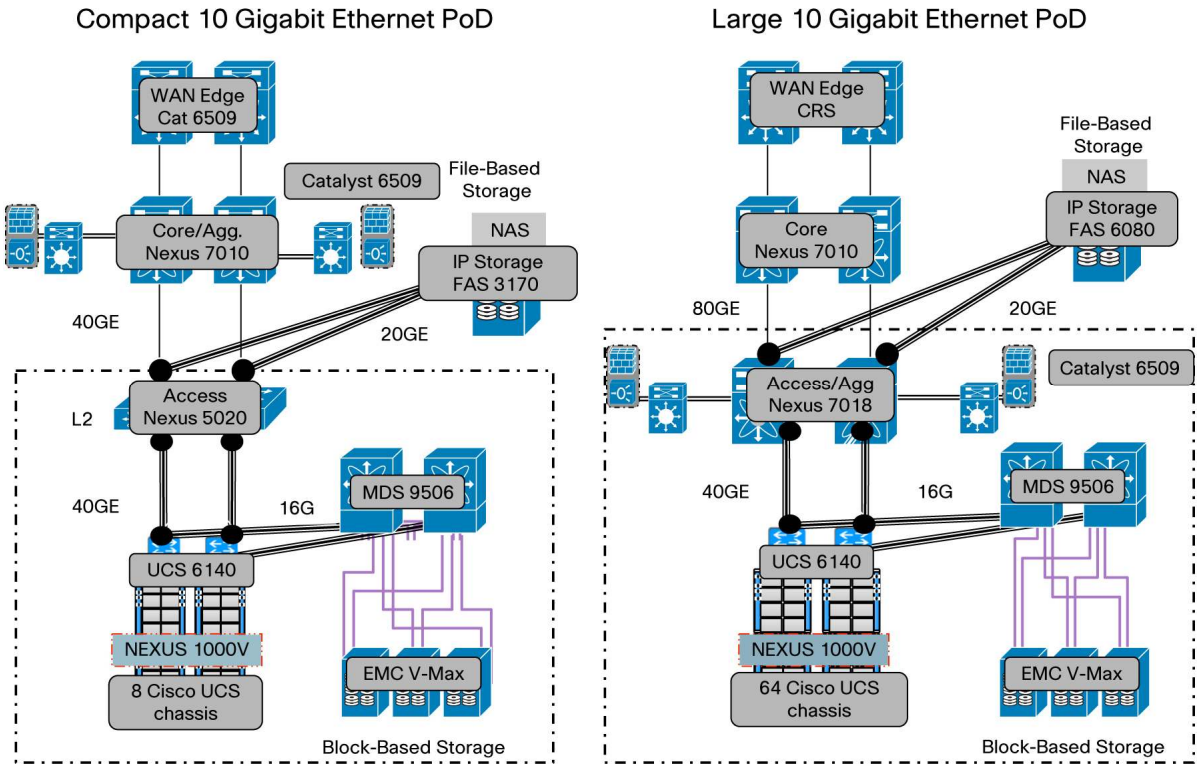
## Architecture Features

The Cisco VMDC architecture for IaaS consists of several components of a cloud design, from the infrastructure building blocks - compute, storage, and network - to the components that complete the solution, which include orchestration for automation and configuration management. This architecture is the latest in modular, multi-tenancy data center design, using Vblocks defined by the Virtual Computing Environment (VCE) coalition[1]. Vblocks offer a predesigned and prequalified virtual environment consisting of fabric, compute, hypervisor, security, storage, and management. With its verified security and layered design for the access, aggregation, and core data center layers, the architecture provides a clear roadmap that reduces cost and complexity and is faster to deploy. The architecture specifies two point-of-delivery (PoD) types, Large PoD and Compact PoD, which differ in their compute and storage scalability as well as in their access and aggregation layer designs (Figure 3).

This architecture is built on a service delivery framework that can be used to host other services besides IaaS on the same infrastructure, sharing a pool of compute, storage, and networking resources. This framework could be used by service providers to add applications to the same systems, should those services be valuable to external customers, or by enterprises that want to add other services for internal clients (for instance, virtual desktop infrastructure [VDI] services).

[1] http://www.cisco.com/en/US/partner/netsol/ns1027/index.html

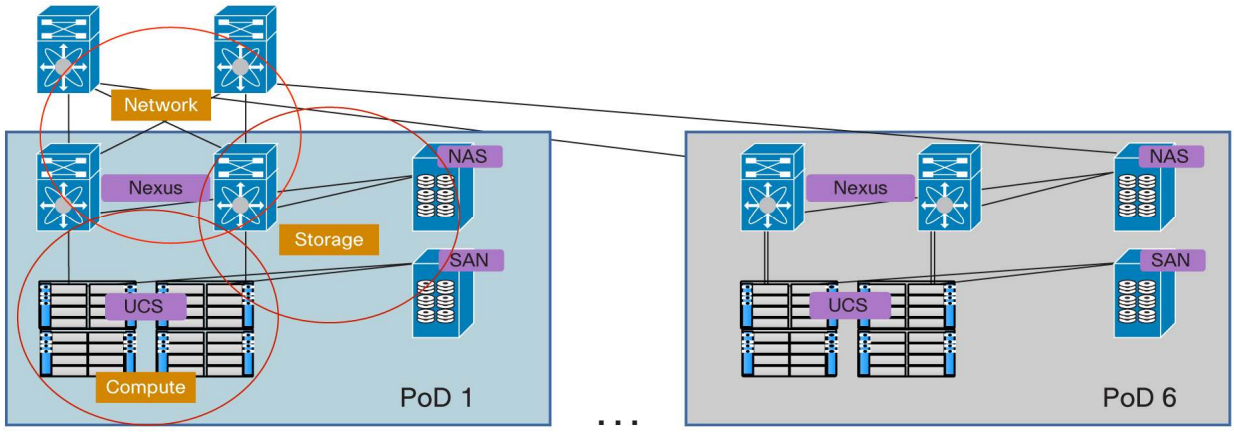
**Figure 3.** Topology for 10 Gigabit Ethernet Small and Large PoDs




**PoD Design: Add Capacity with Fully Integrated, Modular Building Blocks**

The Cisco architecture for the end-to-end IaaS solution includes support for either Gigabit Ethernet or 10 Gigabit Ethernet SAN and network-attached storage (NAS) deployments. The end-to-end system starts with a basic infrastructure module called the PoD. A PoD is a logical repeatable construct with predictable infrastructure characteristics and deterministic functions. Each PoD is discovered by the system, integrated into the resource pools, and assigned workloads as needed. PoDs allow you to scale compute, network, and storage in predictable increments (Figure 4). As mentioned earlier, the architecture specifies two PoD types: Large PoD and Compact PoD, which differ in their compute and storage scalability as well as in their access and aggregation layer designs. The PoD design incorporates Vblocks defined by the VCE coalition.

**Figure 4.** PoD Build-out




The Cisco VMDC architecture allows you to add infrastructure to the whole system rather than for just a single service. The added infrastructure is dynamically discovered and comes online to meet any required demand.

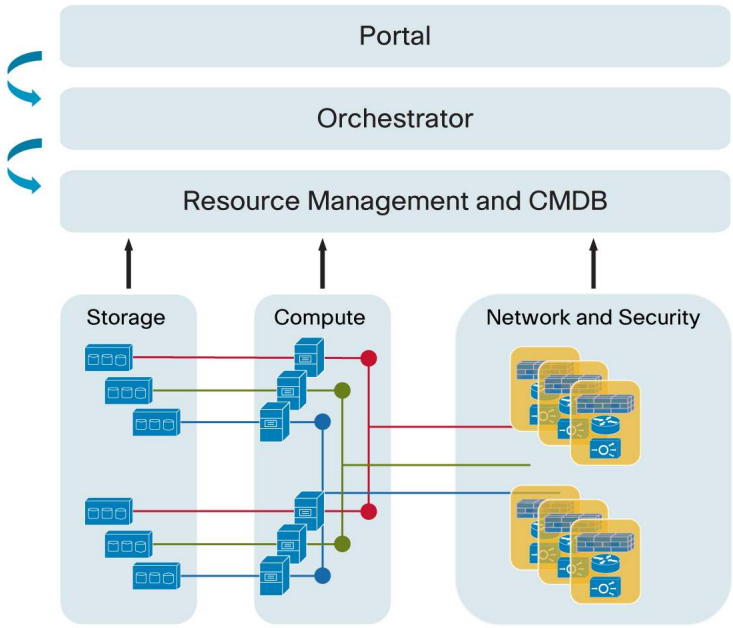
The PoD design offers a number of benefits:

- Enables administrators to scale their build-out in predictable, logical units
- Enables planning and rollout of capacity in a pay-as-you-grow model

### Service Orchestration: On-Demand Provisioning of Resources

The architecture enables on-demand provisioning of resources through service orchestration, which is a multi-domain configuration abstraction layer on top of the data center infrastructure. It enables a portal-based configuration model in which the subscriber can select from a defined number of service options and host applications as virtual machines (Figure 5).

**Figure 5.** Orchestration Layers




Based on these selections, configuration actions are performed on the devices to achieve the service represented in the portal. This self-service, portal-based model offers customization per customer and reduces the number of manual tasks required of the IT department. Service orchestration thus automates the configuration across many devices based on the services advertised through the portal. The orchestrator used in this architecture is a BMC Atrium Orchestrator.

Service orchestration offers a number of benefits:

- Significantly reduces the OpEx associated with IaaS
- Enables applications to be provisioned and put it into production more quickly; what can take months in a manual model is reduced to minutes with service orchestration

### Differentiated Services Using Service Tiers

The Cisco VMDC architecture allows enterprises to use differentiated service tiers to build data centers that support their internal clients based on differentiated requirements or that provide differentiated application support based on service tiers. Service providers can offer service tiers with differing support for customer segmentation based on desired service levels and capabilities (Table 2).

**Table 2.** Service-Tier Differences

| Service | Bronze | Silver | Gold |
|---|---|---|---|
| **CPU allocation** | 0.25<br>(32 virtual machines per server) | 0.5<br>(16 virtual machines per server) | 1<br>(8 virtual machines per server) |
| **Virtual machines per CPU core** | 4:1 | 2:1 | 1:1 |
| **Services** | No additional services | Firewall services | Firewall and load-balancing services |
| **Segmentation** | One VLAN per client and single virtual route forwarding (VRF) instance | Multiple VLANs per client and single VRF instance | Multiple VLANs per client and single VRF instance |
| **Data protection** | None | Snap: virtual copy (local site) | Clone: mirror copy (local site) |
| **Disaster recovery** | None | Remote replication (with specific recovery-point objective [RPO] or recovery-time objective [RPO]) | Remote replication (any-point-in-time recovery) |

The VMDC architecture enables differentiation in network services, compute capabilities, and storage protection. This solution specifies three service tiers: Bronze, Silver, and Gold. Different quality-of-service (QoS) attributes are associated with each service tier. On the compute side, the virtual machine - to - core ratio varies for each service tier. The network services differentiation is implemented through the data center services node (DSN), which offers firewall and server load-balancing capabilities. In the enterprise, different departments may use different kinds of services based on individual department requirements. Storage differentiation is implemented through data protection mechanisms such as cloning and snapshots.

Differentiated service tiers offer a number of benefits:

- Offers service tiers with differing capabilities
- Supports customer segmentation based on desired service levels and capabilities

### Layered Security

Secure access and resource protection are critical to the adoption of cloud architectures. The Cisco VMDC architecture embeds security at each layer of the data center, including the WAN edge, core, aggregation, access, virtual-access, compute, and storage layers. Several features on the network devices and on the compute infrastructure combine to provide the robust security desired to give organizations the confidence to use cloud computing infrastructure to address their business needs for application deployment (Table 3).

**Table 3.** Security Components by Solution Layer

| Layer | Embedded Security |
|---|---|
| **WAN edge** | • Secured access and perimeter firewall<br>• Multiprotocol Label Switching (MPLS) Layer 2 and 3 VPNs<br>• SSL and IP Security (IPsec) VPNs<br>• Infrastructure security to protect device, traffic plane, and control plane |
| **Aggregation and core**<br>**Storage and storage aggregation** | • Device virtualization for control-, data-, and management-plane segmentation<br>• Virtual service domains plus NetApp vFilers (NAS)<br>• Zoning<br>• Infrastructure security to protect device, traffic plane, and control plane |
| **Services** | • Server load balancing to mask servers and applications<br>• Application firewall to mitigate cross-site scripting (XSS), HTTP, SQL, and XML attacks<br>• Infrastructure security to protect device, traffic plane, and control plane |
| **Access and aggregation** | • Secure, authenticated connections<br>• Dynamic Address Resolution Protocol (ARP) inspection<br>• Dynamic Host Configuration Protocol (DHCP) snooping<br>• IP source guard<br>• Zone security (private VLANs, port switching, and port profiles with access control lists [ACLs])<br>• Infrastructure security to protect device, traffic plane, and control plane |

| Layer | Embedded Security |
|---|---|
| **Compute virtual access** | • Policy-based virtual machine connectivity<br>• Mobile virtual machine security and network policies<br>• Virtual firewall integration with Cisco Nexus 1000V Switch<br>• Application security |

Layered security offers a number of benefits:

- Provides secure access to the cloud
- Secures resources in the cloud
- Isolates clients and applications in the cloud

### Multi-Tenant Design with Workload Mobility and Disaster Recovery Capability

Multi-tenancy refers to the capability of the data center to host multiple customers, and it is a critical attribute of any cloud computing deployment. It is relevant in public clouds hosting multiple customers with different service-level requirements and in private clouds in which multiple departments or organizations share the same cloud infrastructure. Different degrees of multi-tenancy must be supported throughout the data center. The Cisco VMDC architecture balances logical and physical segmentation.

Unique resources are assigned to each tenant. These resources include different policies, pools, and QoS definitions. Virtualization at different layers of a network allows the infrastructure to provide logical isolation without dedicating physical resources to each customer. Some of the features used to implement multi-tenancy are VRF-lite to segregate customer traffic at Layer 3, multicontext Cisco Application Control Engine (ACE) and Cisco Catalyst® 6500 Series Firewall Service Module (FWSM) configuration to dedicate a service context to each client or customer, and VLANs to segregate Layer 2 traffic. On the compute side, virtual interfaces on the Cisco UCS adapters segregate traffic at the server NIC.

The architecture facilitates movement of workloads within the data center. Disaster recovery capability is also built into the design using VMware Site Recovery Manager and enables movement of workloads from one data center site to another.

### Architecture Components

Table 4 lists the components of the Cisco VDMC architecture.

**Table 4.** Components of the Cisco VDMC Architecture

| Feature | Components |
|---|---|
| **Network** | • Cisco Nexus 5020, 7010, and 7018 Switches<br>• Cisco Catalyst 6500 Series Switches and Cisco CRS-1 Modules (WAN edge)<br>• Data center services node: Cisco Catalyst 6509-E Switch (Virtual Switching System [VSS])<br>• Cisco Nexus 2148T Fabric Extender |
| **Compute** | • Cisco Unified Computing System<br>◦ Cisco UCS 5108 Blade Server Chassis<br>◦ Cisco UCS B200 M1 Blade Server<br>◦ Cisco UCS M71KR-E Emulex Converged Network Adapter<br>◦ Cisco UCS M81KR Virtual Interface Card<br>◦ Cisco UCS 6120XP 20-Port Fabric Interconnect and Cisco UCS 6140XP 40-Port Fabric Interconnect |
| **Virtualization** | • VMware vSphere<br>• VMware ESXi 4.0U1 Hypervisor<br>• Cisco Nexus 1000V (virtual access switch) |
| **Security** | • Cisco Catalyst 6500 Series FWSM and Cisco ACE<br>• VMware vShield<br>• NetApp vFiler and Virtual Service Domains<br>• Cisco Nexus 1000V Switch |

| Feature | Components |
|---|---|
| **Storage fabric and arrays** | • Cisco MDS 9506 and MDS 9513 Multilayer Directors and Cisco MDS 9148 and 9134 Multilayer Fabric Switches<br>• EMC Symmetrix V-Max with virtual provisioning<br>• NetApp FAS3170 and NetApp FAS6080 |
| **Orchestration and management** | • BMC Atrium Orchestrator<br>• VMware vCenter<br>• Cisco UCS Manager<br>• BMC BladeLogic for server and network<br>• BMC Remedy IT Service Management Suite |

## Conclusion

The cloud computing phenomenon is popular because of its lower TCO, scalability, competitive differentiation, and reduced complexity. Many types of services can be delivered from the cloud with stability, security, high performance, and flexibility to augment the existing infrastructure of IT departments.

IaaS is a cloud-based service expected to generate high demand among large and small enterprises because it is easy to deploy and cost effective. Cisco has designed, tested, and validated the VMDC architecture with intelligent technologies, platforms, and solutions at each level of the network. Service providers can use it to deploy IaaS-based public clouds to generate revenue by providing value-added services. Enterprises can use it to deploy private clouds that improve agility and turn the data center into a business enabler rather than a cost center.

## For More Information

For more information, visit the following links

- **Delivering IT as a Service for Virtualized Data Centers:** http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/Secure_Multi-tenancy_Overview.pdf
- **Cloud Computing Overlay for Unified Service Delivery: Delivering Infrastructure-as-a-Service:** http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns951/solution_overview_c22-539404.pdf
- **Cisco and VMware Deliver Solution to Simplify Management of Network Services for Cloud Environments:** http://newsroom.cisco.com/dlls/2009/prod_042109d.html
- **Cloud Computing:** http://www.cisco.com/en/US/netsol/ns976/index.html
- **Cisco Unified Computing System:** http://www.cisco.com/en/US/products/ps10265/index.html
- **Cisco Nexus 7000 Series Switches:** http://www.cisco.com/en/US/products/ps9402/index.html
- **Cisco Nexus 5000 Series Switches:** http://www.cisco.com/en/US/products/ps9670/index.html
- **Cisco Catalyst 6500 Series Switches:** http://www.cisco.com/en/US/products/ps9402/index.html
- **Cisco Blade Switches:** http://www.cisco.com/en/US/products/ps6746/Products_Sub_Category_Home.html
- **Cisco Storage Networking Products:** http://www.cisco.com/en/US/products/hw/ps4159/index.html

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.**



Printed in USA C11-604559-01 09/10