Cisco Virtual Workspace (VXI) Smart Solution 2.7 Reference Architecture

April 2, 2013

What You Will Learn

Enterprise IT departments are increasingly looking to desktop virtualization as a way to reduce operating expenses, improve manageability, enhance security, and accelerate the deployment of new capabilities. However, desktop virtualization also presents a number of critical challenges in terms of cost, performance, and scalability. Many projects stall in the pilot stage, as organizations struggle to provide a consistent user experience while achieving return-on-investment goals. Desktop virtualization impacts every part of the enterprise IT infrastructure, from the end user to the data center, and successful deployment requires a well-planned, end-to-end solution. This document describes the Cisco Virtual Workspace (VXI) Smart Solution architecture, which provides a foundation for addressing the challenges associated with desktop and application virtualization.

Introduction

The solution is a scalable, high performance, end-to-end architecture for desktop and application virtualization. A core component of the Cisco Unified Workspace, this solution unites proven Cisco architectures in the data center, the network, and the user workspace to provide a comprehensive system for deploying virtualization across the enterprise. It offers a superior collaboration and rich media experience with best in class return-on-investment (ROI), by delivering a fully integrated, open, and validated desktop virtualization system. It also leverages industry-leading ecosystem partners for storage, virtualization, client, and management technology.

This reference architecture document defines the building blocks and services of the solution. Enterprises evaluating desktop virtualization can use this reference architecture to identify the critical products and technologies needed to deploy a successful system. This reference architecture is a companion to the Cisco Validated Design (CVD) Guide for the Cisco Virtual Workspace (VXI) Smart Solution, and provides a foundation for understanding the best practices and design techniques described in that document.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Architecture Goals

Given the end-to-end nature of desktop virtualization systems, the solution architecture is designed to achieve these goals –

- Host virtual desktops at very high densities and readily scale to accommodate additional users
- Efficiently transport virtual desktop-related traffic, including rich media, across various networks and media to provide a high quality user experience
- Enable users to access virtual desktops and collaborate using a wide range of devices from diverse locations
- Maximize flexibility, security, resilience, manageability, and cost-effectiveness

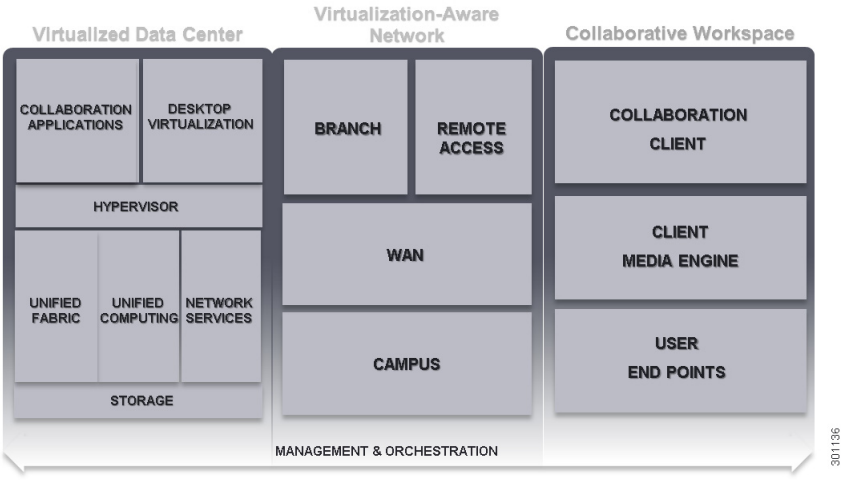
Achieving these goals requires a robust and far-reaching architecture that addresses the full range of an organization's requirements. Data centers, for example, must provide not only the computing resources required to accommodate virtual machines and desktops, but also the networking, services, and storage elements to support virtualization. The network must deliver desktop traffic throughout the enterprise and to various remote locations, while ensuring that voice and video traffic meet user expectations. Accomplishing this task requires a full range of networking technologies for campus, WAN, branch offices, and teleworkers, as well as specialized tools for bandwidth optimization, application acceleration, and more. The user workspace must seamlessly accommodate both virtualized and native collaboration capabilities, while enabling users to seamlessly transition between operating modes.

Unlike other approaches to desktop virtualization, this architecture uniquely assembles the full range of products, technologies, and services needed for a successful deployment.

Architecture Overview

The architecture is based on three foundational pillars – the Virtualized Data Center, the Virtualization-Aware Network, and the Collaborative Workspace (see Figure 1). Together, these architectural elements deliver an end-to-end workspace solution that provides secure, scalable, flexible desktop virtualization, along with the voice and video collaboration capabilities needed by today's users. Management and orchestration tools from Cisco and ecosystem partners simplify the provisioning and administration of virtual desktops, resulting in greater operational efficiencies.

Figure 1 Cisco Virtual Workspace (VXI) Smart Solution Architecture



Virtualized Data Center Overview

The Virtualized Data Center is based on Cisco's Unified Data Center architecture, which is designed to create data centers that are efficient, agile, and transformative. The Virtualized Data Center provides the resources required to host virtual desktops and applications while simplifying deployment and manageability. It can easily scale to accommodate extremely large deployments with tens of thousands of virtual desktops.

Cisco has also developed a portfolio of data center architectures and designs with innovative storage and I/O technologies to make sure a broad set of virtual desktop delivery models, scalability requirements, and performance needs are supported. The full portfolio of data center designs for desktop virtualization can be accessed here: www.cisco.com/go/vdi

The Virtualized Data Center comprises these functional elements:

- **Unified Computing**: the Cisco UCS B-Series blade server system and the UCS C-Series rack mount servers provide the processing, memory, and storage needed to run virtual machines and desktops.
- **Unified Fabric**: provides connectivity for the Virtualized Data Center, unifying storage, data networking, and network services. It delivers architectural flexibility and consistent networking across physical and virtual environments. Cisco Nexus and MDS switches provide the foundation for the Unified Fabric.
- **Network Services**: the data center provides head-end functionality for many network services such as bandwidth optimization, VPNs, firewalls, and load balancing. Products such as Cisco WAAS, Cisco ASA, Cisco ACE and their virtual equivalents provide these functions.
- **Storage**: with desktop virtualization, user data, applications, and desktop images are centralized in the data center. The architecture leverages centralized shared storage arrays from ecosystem partners, server-based local storage options such as SSDs and flash, and a wide range of storage optimization technologies to provide needed performance, flexibility, and cost efficiency.
- **Hypervisor**: the data center is hypervisor-agnostic, and has been architected to support industry-leading hypervisors from VMware, Microsoft, and Citrix. These hypervisors run on Cisco UCS servers and are used to create virtual machines, which in turn will host virtual desktops and applications.
- **Desktop Virtualization**: this architectural element includes the components needed to create, access, and manage virtual desktops. The architecture accommodates both Citrix and VMware solutions for desktop/application virtualization.
- **Collaboration Applications**: the data center architecture supports the collaboration applications often required for virtual desktop users, including Cisco Unified Contact Center Enterprise, Cisco Unified Communications Manager, and Cisco Jabber. These applications enable the architecture to host agent desktops with full unified communications support.

Virtualization-Aware Network Overview

The Cisco Virtualization-Aware Network architecture is designed to reduce operational complexity and provide the services needed to connect anyone, anywhere, on any device. To that end, the network employs bandwidth optimization, load balancing, quality of service, security, and other technologies from Cisco's industry-leading networking portfolio to ensure that traffic flows securely, reliably, and efficiently between users and desktops. The network includes the following elements:

- **Campus/DC Edge**: connects the end-users and devices in the corporate network with the data center, WAN, and Internet. In this architecture, the campus network leverages the Cisco Enterprise Campus 3.0 architecture. In addition to high-speed connectivity, the campus network provides a rich set of services such as Power over Ethernet, access control and authentication, Quality of Service, and more.
- **WAN**: connects workers in branch and regional offices with their data-center-based virtual desktops. In many virtual desktop environments, bandwidth-constrained WANs take a heavy toll on user satisfaction. In this architecture, the WAN leverages several optimization products and technologies, such as Cisco WAAS and performance routing to ensure a quality experience for end users.
- **Branch Office**: connects remote office locations to the enterprise network. In the branch, users access their virtual desktops across the corporate WAN, and may be subject to delays associated with bandwidth constraints, latency, and packet loss. In this architecture, branch offices deploy Cisco routers and switches to handle inter- and intra-office traffic, and leverage optimization technologies such as compression and caching. The branch also supports Unified Communications survivability, which is important for delivering a complete workspace.
- **Remote Access**: users such as teleworkers can be fixed or mobile. Fixed teleworkers are usually located in a home office and use solutions such as Cisco Virtual Office to communicate. Mobile teleworkers access their desktops from almost anywhere, using a suitably equipped device such as a laptop or tablet computer. Both types of user will employ Cisco VPN and WAAS client software.

Collaborative Workspace Overview

The Collaborative Workspace builds on the Cisco Collaboration architecture, extending virtual desktop access to a wide range of end points while supporting critical collaboration capabilities hosted in the data center. The Collaborative Workspace supports both corporate-owned and personal assets for those organizations interested in Bring Your Own Device (BYOD) programs. This architectural subsystem is composed of the following elements:

- **Collaboration Client Software**: The architecture is designed to support collaboration on virtually any device. Pervasive unified communications support is enable by Cisco Jabber, which can run natively on the device, in the user's hosted virtual desktop, or even as a hosted virtual application.
- **Media Engine Software**: The Collaborative Workspace architecture separates unified communications traffic (both voice and video) from normal virtual desktop traffic. This separation reduces latency, conserves data center resources and network bandwidth, and provides a higher quality user experience. The Cisco Virtualization Experience Media Engine (VXME), which runs on Cisco and 3rd party clients, works with Cisco Jabber to terminate local media at the user end point. This interaction enables media to flow directly from end point to end point, and eliminates the need for hair-pinning traffic through the data center.
- **User End Points**: End points can be Cisco or 3rd party clients zero or thin clients, or devices such as smart phones, tablets, and laptop computers running VMware or Citrix client software.

Virtualized Data Center

The Virtualized Data Center, based on Cisco Unified Data Center (UDC), plays a critical role in the solution architecture. The data center hosts the processing, storage, network, and other associated systems needed to support server, desktop, and application virtualization. The data center is designed to provide a simplified, secure, and scalable platform for desktop and application virtualization.

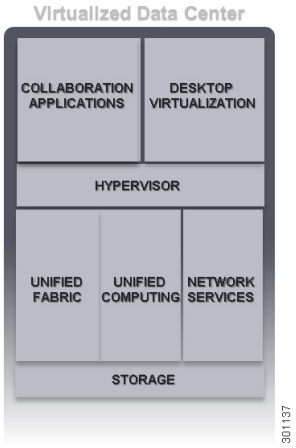
- The Virtualized Data Center provides very high desktop densities, a unified management system, and the opportunity to leverage pre-packaged and validated infrastructure solutions. It requires fewer servers, fewer cables, and is simpler to deploy and manage.
- It provides enhanced security through virtualization-aware access and control policies, virtualization-aware networking, on-demand provisioning, and end-to-end segmentation.
- The data center provides scalable, predictable performance with a superior user experience. It can scale to support thousands of virtual desktops in a single domain, and new desktops can be rapidly provisioned through service profiles.

The architecture leverages these attributes to deliver a data center that provides a faster return-on-investment and a lower Total Cost of Ownership. The Virtualized Data Center enables organization to simplify deployments, increase productivity, and improve agility while reducing risk.

Since desktop virtualization projects come with a broad range of scale, deployment model and performance requirements, the data center architecture and design can vary to meet these needs. Cisco offers four different data center architectures and associated designs to meet these different needs: On-board architecture; simplified architecture; scalable architecture and converged infrastructure. You can find more details on these architectures at www.cisco.com/go/vdi

This paper focuses on the scalable architecture and converged infrastructure architectures that are most appropriate to larger virtual desktop deployments. The Virtualized Data Center, based on Cisco UDC can integrate the functions shown in Figure 2.

Figure 2 Virtualized Data Center Architecture

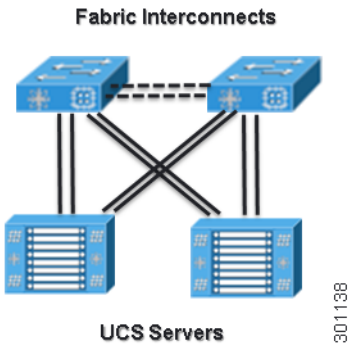


Unified Computing

The Cisco Unified Computing System provides the processing capabilities needed to host virtual machines and virtual desktops, collaboration software and other applications in the data center. The Cisco UCS servers deliver a high-performance computing resource built especially for virtualized environments. The Cisco UCS system comprises a broad range of Intel Xeon x86-based servers offering a variety of memory, storage, interface, and form factor options. This solution has validated both Cisco UCS B-Series blade servers and C-Series rack servers to provide maximum flexibility for enterprise IT organizations. The Cisco Unified Computing System comprises these elements:

- **Cisco UCS B-Series Blade Servers**: Cisco UCS B Series servers (see Figure 3) are based on Intel Xeon processors and offer exceptional performance and memory capacity. Each blade server's front panel provides direct access to video connections, USB ports, and console connections. The Cisco UCS B-Series blade servers connect to the chassis by means of converged network adapter (CNA) cards, such as the Cisco VIC 1240 and 1280.
- **Cisco UCS 5100 Series Blade Server Chassis**: The chassis provides an enclosure for Cisco UCS B-Series Blade Servers. It is six rack units (6RU) in height, can mount in an industry-standard 19-inch rack, and uses standard front-to-back cooling. Each chassis can accommodate up to eight half-width or four full-width Cisco UCS B-Series Blade Servers. The chassis also supports up to four single-phase, hot-swappable power supplies.
- **Cisco UCS C-Series Rack Servers**: The Cisco UCS C-Series extends Cisco UCS innovations to an industry-standard rack-mount form factor. The Cisco UCS C-Series servers can operate both in standalone environments and as part of the Cisco Unified Computing System. The Cisco UCS C-Series servers can be deployed incrementally according to an organization's timing and budget.
- **Cisco UCS C-Series**: Servers interface with the Cisco Unified Communications System through network adapters such as the Cisco UCS P81E VIC. This card is a dual-port, 10 Gigabit Ethernet, PCI Express (PCIe) adapter that provides dynamically configurable virtual interfaces.
- **Cisco Fabric Extenders**: The Cisco UCS 2100 and 2200 Series Fabric Extenders reside in the Cisco UCS 5100 Series Blade Server Chassis and provide 10 Gigabit Ethernet connections between servers and fabric interconnects. The fabric extenders function as distributed line cards and are managed as extensions of the fabric interconnects. The Cisco Nexus® 2000 Series Fabric Extenders connect rack servers to the fabric interconnects. Like the Cisco UCS fabric extenders, the Cisco Nexus fabric extenders function as line cards for the parent switch.
- **Cisco UCS Fabric Interconnects**: Typically deployed in pairs to provide highly available network connectivity and management capabilities for Cisco UCS, the fabric interconnects offer line-rate, low-latency, lossless 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions. All chassis and servers attached to the fabric interconnects become part of a single, highly available management domain. The fabric interconnects provide connectivity between Cisco UCS and the rest of the data center network.
- **Cisco UCS Manager**: Cisco UCS Manager provides embedded management of all software and hardware components of Cisco UCS across multiple chassis and rack-mount servers and thousands of virtual machines. It manages the system as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API. Cisco UCS Manager is embedded on a pair of Cisco UCS 6100 or 6200 Series Fabric Interconnects using a clustered, active-standby configuration for high availability. The manager participates not only in server provisioning, but also in device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection.

Figure 3 Cisco UCS B-Series and Fabric Interconnects



Unified Fabric

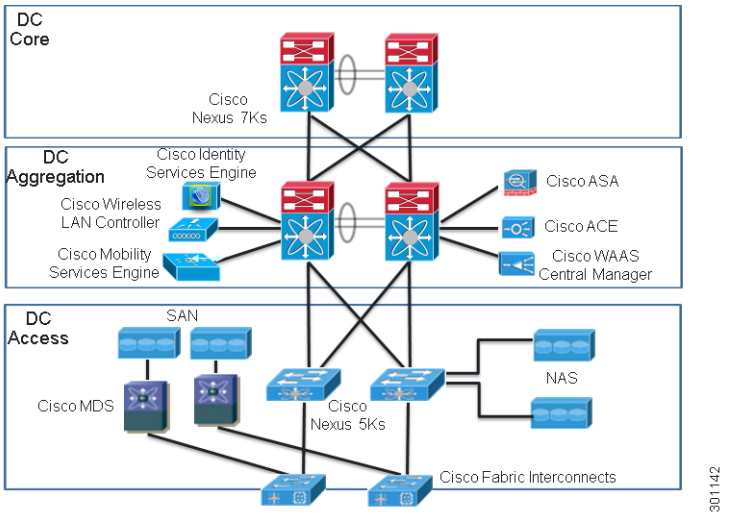
In the solution architecture, Cisco Unified Fabric provides foundational connectivity and unifies storage, data networking and network services. Through enhanced convergence, scalability, and network intelligence, the fabric optimizes resource usage, improves application performance, lowers operating costs, and speed application rollout. The Cisco Unified Fabric is based on Cisco Nexus and MDS switches, the NX-OS operating system, and fabric and network management solutions. The Virtualized Data Center deploys the following Cisco Unified Fabric components to build a hierarchical data center network that could easily be scaled to support even the largest deployments:

- **Cisco Nexus 7000 Series**: these modular switches are designed for the most mission critical deployments in data centers and enterprise campuses. It is available in 4, 9, 10, and 18 slot configurations, and can scale to extremely high port densities. The Cisco Nexus 7000 offers very high performance, scaling beyond 15 terabits per second. The switch can be logically partitioned into multiple virtual device contexts. The Cisco solution architecture leverages this capability to collapse two switching layers into a single physical switch.
- **Cisco Nexus 5000 Series**: these data center switches enable any transport over Ethernet, including Layer 2, Layer 3, and storage traffic. This reference architecture deploys the Cisco Nexus 5000 Series switches at the access layer, for connectivity to storage networks, the aggregation layer switches, and the Unified Computing System (via the Fabric Interconnects). The switches handle a broad range of connectivity and protocols, including Unified Ports, which support Ethernet and FCoE or native Fibre Channel.
- **Cisco MDS 9000 Series**: high performance, protocol-independent, director-class SAN switches, the Cisco MDS 9000 Series is used for connecting to block-based storage arrays via Fibre Channel, Fibre Channel over Ethernet, Fibre Channel over IP, and iSCSI.

The network architecture consists of three logical layers: core, aggregation, and access. As previously noted, the core and aggregation layers are logically separate, but have been physically collapsed within the Cisco Nexus 7000 switches (see Figure 3) using virtual contexts.

The core layer is based on a pair of Cisco Nexus 7000 Series switches. This layer provides highly available, high performance Layer 3 switching to the campus and other parts of the network. The aggregation layer provides connectivity for the access switches, and consolidates them into a smaller number of core connections. Services such as bandwidth optimization, load balancing, and firewalling are also deployed in the aggregation layer. The access layer provides connectivity for servers (and fabric interconnects) located in the data center and to network-based storage arrays.

Figure 4 Cisco Unified Fabric



Network Services

In this architecture, network services are deployed in the aggregation layer. Services can be deployed by means of standalone appliances, or as part of a Data Center Service Node (a Cisco Catalyst 6500 with service modules, connected to a Nexus 7000 Series switch). In this solution, the following services are particularly recommended:

- **Server Load Balancing**: Cisco recommends that connection brokers associated with virtual desktop solutions be deployed in redundant pairs and load balanced. Solutions such as Cisco Application Control Engine (ACE)) or Citrix NetScaler provide load balancing, health monitoring, and SSL offload to ensure users can get to their virtual desktops when they log in. In the solution architecture, load balancers are deployed in redundant pairs in one-arm mode.
- **Firewall/VPN Termination**: in this architecture, the aggregation layer service typically provides VPN concentration for the rest of the organization. As with Cisco ACE, the architecture assumes that the ASA 5500 will be deployed in redundant pairs.
- **WAN Optimization**: to ensure a satisfactory user experience, this solution calls for the use of Cisco Wide Area Application Services (WAAS). The enterprise WAN is usually a bandwidth constrained environment, and remote users often experience poor results when rich media traffic is transported over the wide area network. Cisco WAAS uses caching, compression, and protocol optimization to make the most efficient use of WAN links. Cisco WAAS Central Manager, which controls all WAAS devices in the network, is typically deployed in the DC aggregation layer. Cisco WAAS is commonly deployed in the WAN aggregation system (at the DC edge), as well as in remote locations. Cisco WAAS can also be deployed in the data center as a virtual appliance in a virtual machine.
- **Identity Services Engine (ISE)**: Cisco Identity Service Engine (ISE) is a component of the Cisco Trustsec architecture that can provide contextual based access policy enforcement. Cisco Trustsec provides many enhancements to standard identity based access policy enforcement model including Security Group Access (SGA). ISE and Trustsec are also foundational technologies for providing Bring Your Own Device Support.

Storage

Storage is a critical element in the virtualized data center, representing anywhere from 40% to 80% of the cost of a desktop virtualization investment. The storage system architecture has a major impact on desktop performance and user experience. Storage system design also influences the ability to scale to accommodate new users, as pilot programs expand to full-scale deployments. In short, the storage architecture is a significant factor in determining the success or failure of a virtualized desktop implementation.

Designing storage for desktop virtualization presents significant challenges in terms of cost and performance. It can be difficult to balance costs with capacity and IO access requirements. Organizations often over-provision their storage arrays, adding more disks than are needed to ensure sufficient levels of IO access. In virtualized environments, IO also tends to be highly random. These random IO operations have a significant impact on disk performance, and may introduce unacceptable levels of latency.

To that end, the storage architecture is designed to integrate a wide range of storage technologies and optimization techniques. The architecture is intended to be flexible, supporting multiple approaches that can be tailored to user environments. It is designed to be efficient, protecting customer ROI by ensuring that resources are optimized. Finally, the architecture is designed to offer high performance, delivering a superior end user experience.

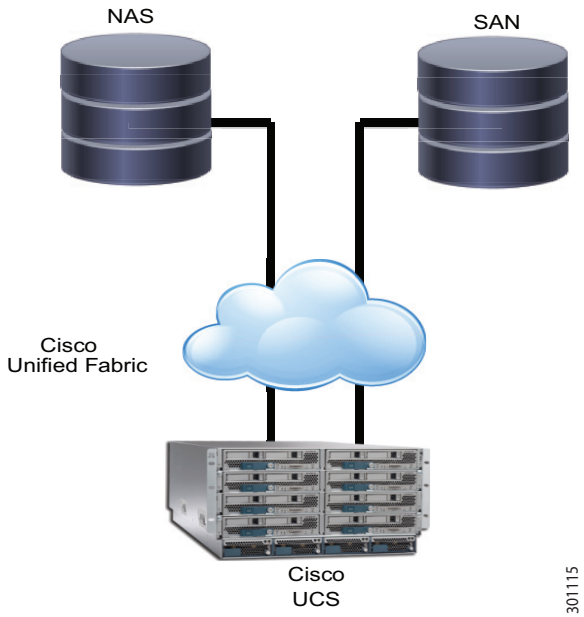
Desktop virtualization vendors traditionally have recommended the use of centralized shared storage arrays for customer deployments. These solutions offer a number of advantages in terms of flexibility, performance, and economies of scale. However, it has proven difficult to size these systems in some cases. Buying too little storage impacts performance and user experience, buying too much wastes money. The current trend is to augment shared storage with other caching or optimization technologies. This architecture supports the traditional centralized storage model, as well as a number of hybrid approaches that blend shared and local storage.

Centralized Shared Storage Model

In this deployment model, the shared storage system contains the user's machine environment, including the operating system, user profiles, and user data. These systems, based on high capacity storage arrays, offer centralized security, high performance, and resource sharing. Centralized shared storage also facilitates the use of advanced hypervisor features and aids in desktop migration.

This solution architecture supports both Network-Attached Storage (NAS) and Storage Area Networks (SAN). NAS is connected over high speed Ethernet, while SANs can be connected over native Fiber Channel, or the increasingly popular Fibre Channel over Ethernet (FCoE). Shared storage systems are provided by ecosystem partners EMC and NetApp. Each partner offers solutions that support both NAS and SAN.

Figure 5 Centralized, Shared Storage Architecture

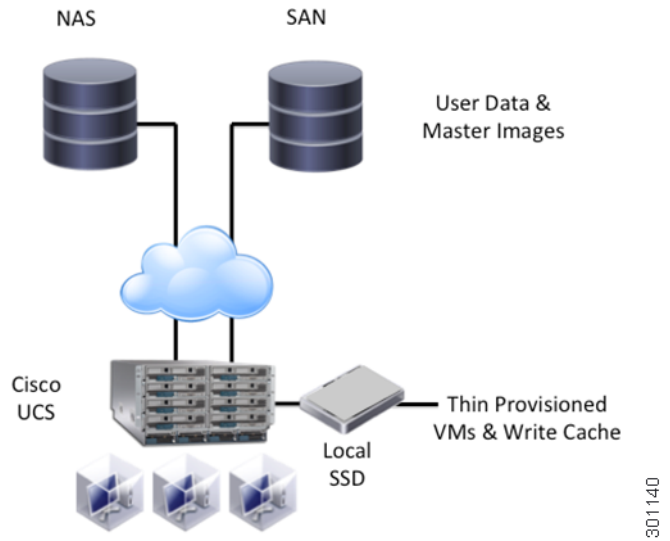


Centralized Shared Storage with Local SSD

This model leverages the solid-state drives (SSDs) available on Cisco UCS servers to complement the shared storage system. Non-persistent files and thin-provisioned VMs are stored locally on the Cisco UCS server SSDs. User data and master images are maintained on shared storage. This approach can reduce demand on the shared storage system by servicing many requests from the local SSD.

During steady state operations, Write IO tends to be the predominate workload for storage systems. Write IO is also more expensive than Read IO in terms of resource consumption. In production-class desktop virtualization environments, large numbers of random Write operations can negatively impact storage performance. By moving the Write cache to the server SSDs, these Write operations are offloaded and addressed locally for improved performance.

Figure 6 Shared Storage with Local SSD Hybrid Architecture

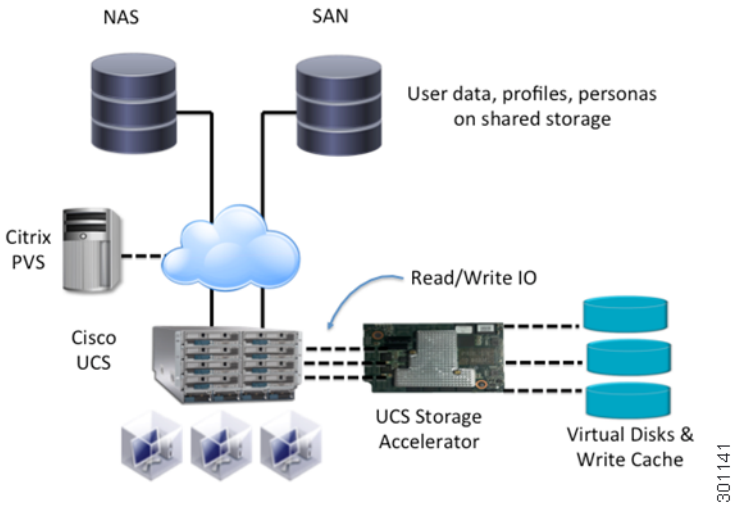


Centralized Shared Storage with Local Cisco UCS Storage Accelerator

The UCS Storage Accelerator is a Flash-based caching solution that resides on a Cisco UCS B200 M3 blade server. The accelerator is a 785 GB mezzanine card that delivers more IOPS than a typical shared storage system. This model is typically used with non-persistent desktops. IO requests are contained within the server, which reduces latency compared to traditional approaches. The model enables support for a guaranteed number of users at a lower cost, and with predictable performance.

In this model, a golden master image and all associated clone images are hosted on the Cisco UCS Storage Accelerator, which is installed on the blade server. A central copy of the golden master image is maintained on the shared storage system. User data, profiles, and personas are saved on the shared system. This approach may enable support for a greater number of users, while providing faster boot-up times.

Figure 7 Shared Storage with Cisco UCS Storage Accelerator



Hypervisor

The hypervisor abstracts the processor, memory, storage, and networking resources of its physical server into multiple virtual machines, and helps ensure that each virtual machine receives its appropriate share of these resources. The hypervisor is installed on each Cisco UCS server to allow virtualized desktops and servers to run as independent virtual machines.

Hypervisors include advanced tools for managing servers and associated virtual machines in high-density production environments. These tools enable IT administrators to identify overcommitted host machines, move virtual machines among pooled hosts, manage power-up sequences, consolidate active virtual machines on the fewest possible hosts, and more.

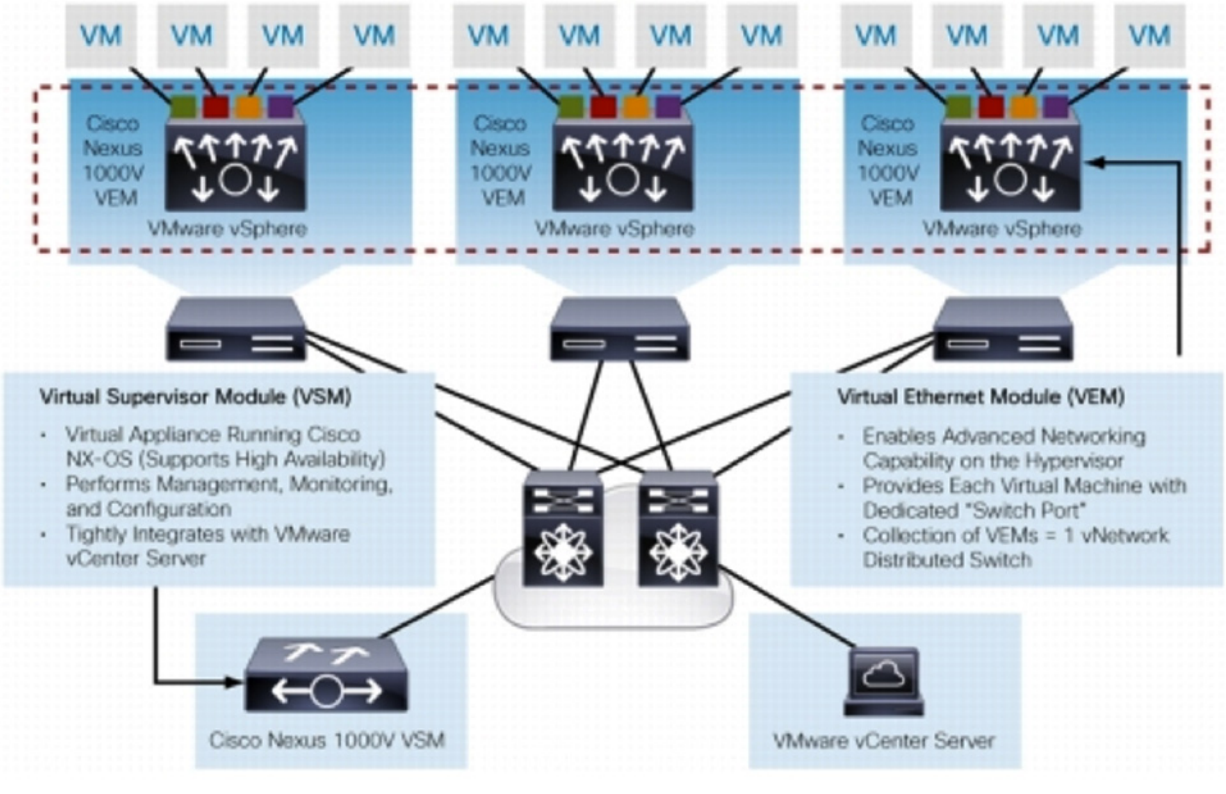
The solution supports the following industry-leading hypervisors, depending on the desktop virtualization solution to be deployed:

- VMware vSphere (VMware View, Citrix XenDesktop and XenApp)
- Citrix XenServer (Citrix XenDesktop and XenApp)
- Microsoft Hyper-V (Citrix XenDesktop and XenApp)

Virtualized Networking and Virtualized Network Services

While virtual machines are an effective mechanism for optimizing IT resources, they can be a challenge in terms of networking and visibility. Cisco, in partnership with VMware, has developed the Cisco Nexus 1000V virtual switch (see Figure 7). The solution runs the Nexus 1000V switch in the hypervisor for policy-based VM security, mobile VM security, and continuity between server and networking assets. With the Cisco Nexus 1000V, port profiles can be created and assigned to VMs through a hypervisor tool such as VMware vCenter. Network and security policies follow the VM throughout its lifecycle. The advanced edition of the Nexus 1000V also includes the Virtual Security Gateway, a virtual firewall that enables the creation of VM-based trust zones. In addition virtualized network services such as WAN optimization (vWAAS) and virtual security firewalls (vASA) can be deployed and scaled on demand.

Figure 8 VM Networking with the Cisco Nexus 1000V



Desktop Virtualization

Desktop virtualization solutions enable the creation of virtual desktops on virtual machines. Applications and Operating Systems are hosted in these desktops, which can be accessed by remote users via a wide range of end-points. A desktop virtualization session requires an endpoint, a hosted desktop running on a virtual machine housed in a data center, and a software agent running inside the virtual desktop. The client end-point initiates a connection to the virtual desktop agent, and interfaces with the desktop by means of a display protocol. Virtual desktop deployments also may position a connection broker between the endpoint and the desktop. The connection broker authenticates client requests, and connects users to appropriate desktops. For desktop virtualization, Cisco has validated desktop virtualization solutions from Citrix (XenDesktop, XenApp) and from VMware (View).

Collaboration Applications

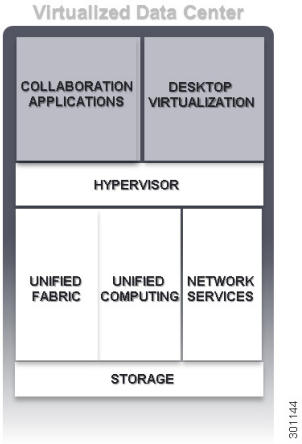
These are applications that can be run on a virtual server in the data center. For this solution, the most important of these are (1) Cisco Unified Communications Manager, (2) Cisco Unified Contact Center Enterprise, and (3) Cisco Jabber. The Virtualized Data Center can host these applications on virtual machines to enable maximum elasticity, scalability and survivability. This solution has validated each of these applications running on Cisco UDC in a virtual desktop environment. Refer to the Collaboration Architecture section for more details on these applications.

Modular Data Center Blocks

Cisco has partnered with key storage and virtualization partners to develop and deliver prepackaged, validated **converged infrastructure** solutions for data centers. These solutions provide computing, storage, server, management, and virtualization resources in an integrated, modular form (see Figure 8). The solution architecture supports the use of these solutions as effective data center building blocks. These packages simplify planning, facilitate acquisition, speed deployment, and reduce risk. Cisco has partnered on the following solutions:

- **Vblock**: the Virtual Computing Environment Company (VCE) was formed by Cisco and EMC, with investments by VMware and Intel. Vblock platforms integrate Cisco UCS and networking technology with VMware vSphere and EMC storage. VCE offers different size Vblocks for different deployment sizes.
- **Flexpod**: unites Cisco UCS and networking technologies with NetApp storage. These integrated platforms have been validated with hypervisors from VMware, Red Hat, and Microsoft. Flexpod solutions, too, have been pre-configured and validated to speed deployment.
- **VSPEX**: Cisco partners with EMC on the VSPEX solution, which integrates Cisco UCS and Nexus equipment with EMC storage and VMware vSphere for server virtualization. VSPEX is a pre-validated and modular platform that provides a complete end-to-end solution.

Figure 9 Prepackaged Infrastructure Integrates Data Center Functions



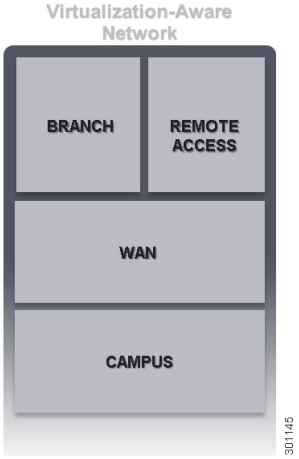
Virtualization-Aware Network

This solution leverages Cisco Unified Access infrastructure to transport traffic between users and virtual desktops or applications. The network architecture allows organizations to connect anyone, anywhere, anytime, to any device – and to do so reliably, securely, and seamlessly. It is designed to provide optimization, scale, and security for collaborative and virtualized environments, using an infrastructure of resilient and scalable hardware and software.

Cisco Unified Access supports virtual desktop users, bring-your-own-device (BYOD) capabilities, and the Internet of Everything (IoE). Cisco Unified Access connects people, processes, data, and things with greater intelligence, security, and efficiency than every before. Cisco Unified Access leverages one policy, one management, and one network to deliver an integrated and simplified intelligent network platform that empowers users to work their way.

The Cisco network infrastructure delivers two primary sets of services. Network services are end-to-end services delivered by the infrastructure that encompass routing, switching, mobility, security, and WAN optimization components. Endpoint and user services define the user experience and enable the attributes of secure, reliable, and seamless performance on a broad range of devices and environments (for example, Cisco AnyConnect™ software for secure, persistent, policy-based access. All services are managed by a comprehensive and integrated management solution.

Figure 10 Virtualization-Aware Network Architecture Elements



Campus Network Architecture

The campus network connects the end-users and devices in the corporate network with the data center, WAN, and Internet. The Cisco Enterprise Campus 3.0 architecture provides an overview of the campus network architecture and includes descriptions of

design considerations, topologies, technologies, configuration design guidelines, and other factors relevant to the design of a highly available, full-service campus switching fabric. In addition to the high-speed connectivity service, the campus network, with its direct interaction with end-users and devices, provides a rich set of services, such as power over Ethernet (PoE), secure access control using IEEE 802.1x, intelligent and dynamic provisioning of DV clients into the correct VLANs (with appropriate QoS/Security policies), location tracking for endpoints, and traffic monitoring and management. To enable these services, end-points within the campus domain should be connected to a wiring closet switch. The campus network leverages these core technologies

Power over Ethernet: provides high availability, high efficiency, and easy-to-manage power. With the introduction of PoE+ and Universal PoE (UPoE) capable clients, organizations now can transition the entire employee work environment to a single power source, saving on both wiring and energy costs. The Cisco Catalyst 4500E, Catalyst 2000S, and Catalyst 3000-X are recommended campus access platforms. The Cisco Catalyst 4500E also supports Universal PoE, a Cisco technology that extends the IEEE 802.3 PoE standard to provide up to 60 watts of power over Ethernet cabling.

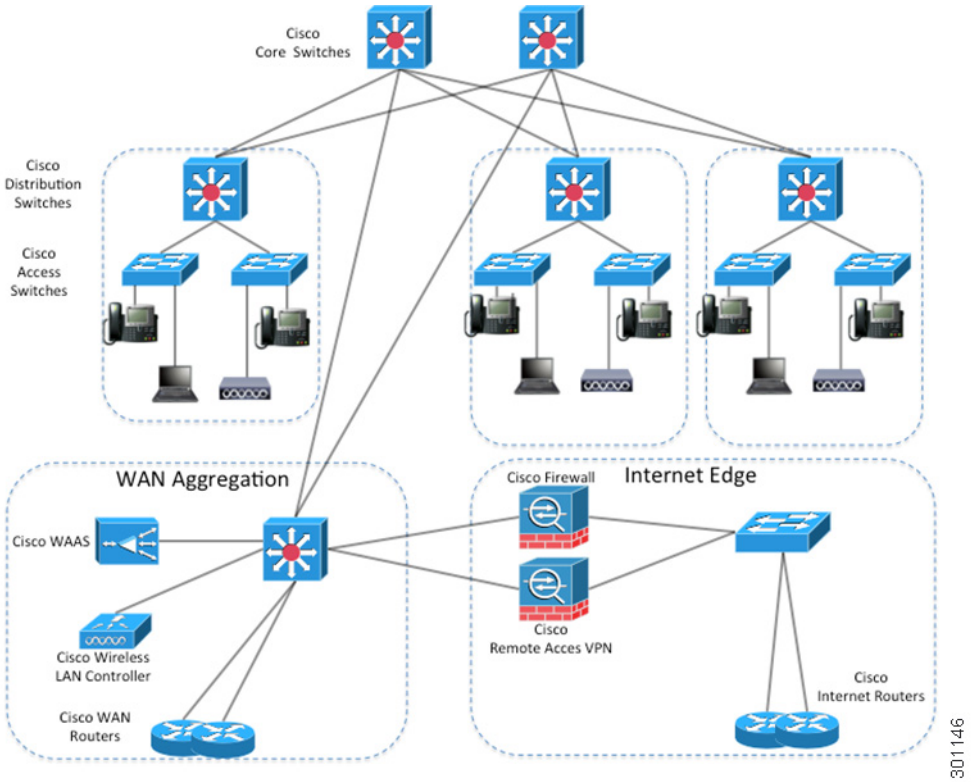
Auto SmartPorts: enable campus switches to dynamically provision clients by

automatically configuring a port based on device identification obtained through Cisco Discovery Protocol (CDP) or MAC addresses. Smartport macros are pre-defined customizable configuration scripts based on Cisco best practices that allow administrators to easily con common switch port configurations.

QoS: Display traffic is encapsulated in vendor proprietary protocols such as ICA, PCoIP and RDP. In the campus, use DSCP marking and Class of Service (CoS) values to prioritize traffic. Detailed recommendations around these settings for various types of data can be found in the Cisco Validated Design Guide.

802.1x: Cisco Catalyst® switches can authenticate devices via 802.1x, and map them to appropriate ACLs based on their credentials. For example, a contractor can connect to the network and be granted access to specific resources. The Cisco Catalyst 4500E and Catalyst 3000-X switches provide 802.1X and port security features for endpoint level security in the campus.

Figure 11 Campus Network Architecture



Wide Area Network Architecture

The WAN connects workers in branch and regional offices with their data-center-based virtual desktops. This solution is designed to deliver a high-quality user experience across a wide range of WAN architectures. Many of the display protocols used with desktop virtualization are not optimized for wide-area networking, and may not perform well in high-latency or bandwidth-constrained environments. At the same time, desktop virtualization users tend to be highly mobile, and they increasingly demand access across the WAN to their virtual desktops. To improve the performance and protect the integrity of virtual desktop traffic across a WAN, the solution leverages the following technologies:

- Cisco WAAS for Bandwidth Optimization and WAN Acceleration
- Performance Routing
- Dynamic Multipoint VPN

Cisco WAAS technology is deployed on either side of the WAN to optimize the traffic that crosses it. Cisco WAAS technology can improve application response time by reducing bandwidth consumption, thereby increasing application performance. This has the dual benefit of improving the user experience while allowing more users to be served by a given WAN link.

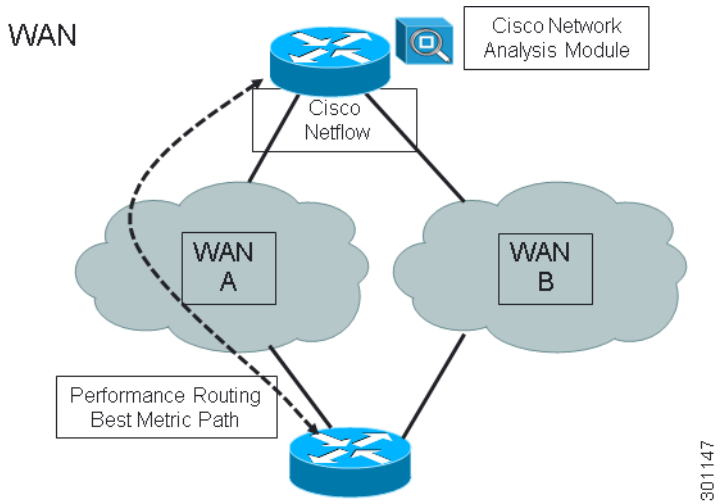
Performance Routing (PfR) improves application performance by selecting the best path across the WAN. PfR takes into account network metrics such as reachability, delay, loss, and jitter to help select the best path based on the application needs. It measures network performance and dynamically re-routes the traffic when the metrics do not satisfy the application needs. It has two logical components, the Master Controller (MC) and the Border Router (BR). The MC acts as a central processor and data collection point and reports events and measurements. The MC gathers network metrics from all the BRs and determines whether traffic classes are performing in accordance with policy. Based on these metrics, the MC can instruct the BR to stay on the current WAN link or change to an alternate path.

Site-to-Site VPNs between the branches and the corporate head offices are secured IP security (IPSec) encrypted tunnels across the WAN. These tunnels can be deployed by means of certificates or pre-shared passwords for authentication of the tunnel endpoints.

This deployment model encrypts any site-to-site traffic to minimize data being captured along the route. The solution supports Easy VPN and Dynamic Multipoint VPN (DMVPN). The DMVPN solution is preferred and supports a variety of WAN links such

as T1/T3, WAN, xDSL etc. In this solution it can be implemented by configuring the ISR G2 router at each branch or fixed teleworker location to connect to a VPN head-end at the Data Center edge.

Figure 12 WAN Architecture



Branch Office Network Architecture

A remote branch office is an enterprise-controlled environment. The primary challenge in the delivery of hosted virtual desktops to branch offices is making sure that the WAN provides adequate performance to meet end-user experience expectations. When hosted virtual desktops are delivered over the WAN, the end user has to cope with limited WAN bandwidth, latency, and packet loss. Branch offices typically deploy:

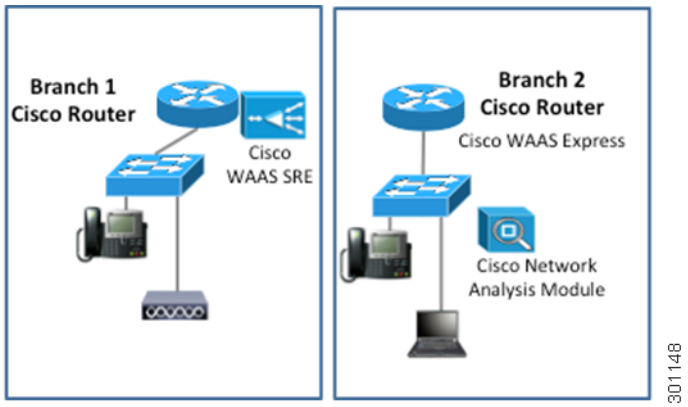
- Cisco Integrated Services Routers
- Cisco WAAS
- Catalyst Switches

In a branch office, the primary means of connectivity back to the central data center is typically via a Cisco Integrated Services Router (ISR). These routers are modular, and offer several interface options for LAN and WAN connectivity, as well as other optional service capabilities. The Cisco WAE appliance can be connected to the local router. The branch-office Cisco WAAS deployment, together with the data

center Cisco WAAS deployment, offers a WAN optimization service through the use of intelligent caching, compression, and protocol optimization. When end-users access their virtual desktops through the connection broker, Cisco WAAS compresses the response and then efficiently passes it across the WAN at high speed and with little bandwidth use. Commonly used information is cached at both the Cisco WAAS solution in the branch office and in the data center, which significantly reduces the burden on the servers and the WAN.

Since the branch will typically service its own local DHCP requests, access layer switches should employ DHCP Snooping, dynamic ARP inspection, and IP source guard. For device authentication, IEEE 802.1x or MAC Authentication Bypass (MAB) should also be deployed locally, via branch switches or switch modules within the Cisco ISR. In some cases (e.g., unencrypted RDP), traffic between the endpoint and the access switch might travel in the clear over the local network.

Figure 13 Branch Office Network Architecture

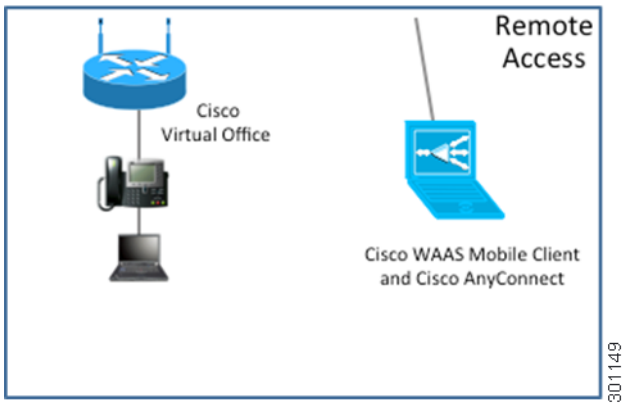


Remote Access Network Architecture

Teleworker remote access can be either fixed or mobile. A fixed teleworker, usually a home-office worker, uses a solution such as Cisco Virtual Office, which provides secure, rich network services to workers outside the traditional corporate office. Cisco Virtual Office is a small router that delivers extensible data, voice, video, and applications to create a complete office environment. The Cisco Virtual Office comprises the following:

- Cisco 800 series Integrated Services Router (ISR) and a Cisco Unified IP Phone.
- A data center presence that includes a VPN router and centralized management software for policy, configuration and identity controls.
- WAN optimization for teleworkers using DV clients that support WAAS mobile implementation.
- WAAS mobile pairs with the WAAS mobile server in the data center behind the VPN head-end.

Figure 14 Remote Access Architecture



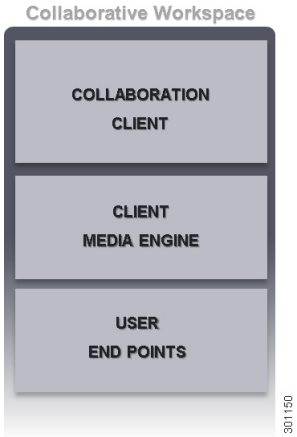
Collaborative Workspace

The Collaborative Workspace enables end-users to access corporate data and applications from a wide range of clients and from multiple locations. The end-point can be chosen from an ever-expanding list of devices, including tablet computing platforms, DV clients, laptop and desktop computers, all spanning a multitude of operating systems. These devices enable typical user desktop interactions, and may also support USB-based print and storage functions. With this solution, the enterprise can now offer a consistent user experience while allowing employees to work with the device that best suits their situations.

The guiding principle of the Collaborative Workspace is to provide a superior end user experience. This portion of the architecture therefore integrates technologies that both facilitate collaboration and support the separation of Unified Communications media from conventional desktop traffic. The architecture is also designed to eliminate hair-pinning, so that UC media flow from peer to peer rather than looping through the data center. The core components of the Collaborative Workspace architecture are:

- Cisco Collaboration Applications
- Cisco Virtualization Experience Media Engine
- User Endpoints

Figure 15 Cisco Virtual Workspace Smart Solution Collaborative Workspace



Collaboration Applications

These are applications that can be run on a virtual server in the data center. For this solution, the most important of these are (1) Cisco Unified Communications Manager, (2) Cisco Unified Contact Center Enterprise, and (3) Cisco Jabber.

Cisco Unified Communications Manager is an industry-leading call control platform that provides services such as session management, voice, video, messaging, mobility, and web conferencing. It can be deployed in a variety of ways, including public cloud, private cloud, on-premises, and hybrid blends of these.

Cisco Unified Contact Center Enterprise delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure. It combines automatic call distributor (ACD) functionality with IP telephony in a unified solution, enabling organizations to rapidly deploy a distributed contact center infrastructure.

Cisco Jabber provides presence, instant messaging, web conferencing, voice, and visual voicemail to laptops, notebooks, tablets, and smartphones. In virtual environments, Cisco Jabber can be run in the virtual desktop and accessed by a remote client.

This solution has validated each of these applications in a virtual desktop environment.

Cisco Virtualization Media Engine

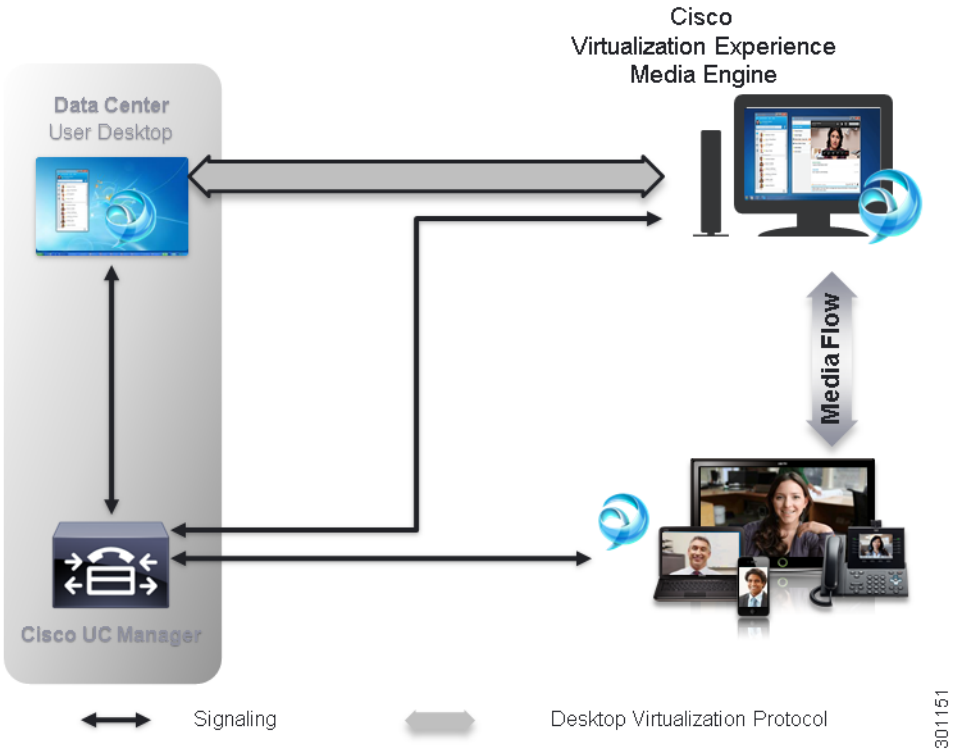
The Cisco VXME extends the Cisco Jabber unified collaboration experience to users in virtualized environments by enabling intelligent processing of real-time voice and video traffic on the local device. This local processing provides a seamless experience that fully leverages the capabilities of Cisco Jabber, and delivers secure high definition audio and video. Cisco VXME also supports a wide range of integrated Unified Communications accessories.

Cisco VXME provides full separation of media traffic from routine virtual desktop traffic, eliminating the hair-pinning of traffic through the data center. Call traffic flows directly from end point to end point. This functionality increases server scalability, reduces network bandwidth requirements, and improves the user experience.

User End Points

The architecture supports both Cisco and 3rd party client devices (e.g., thin clients), and a wide range of laptop computers, tablet computers, and smartphones.

Figure 16 Cisco Jabber and VXME Eliminate Hair-pinning



Management

This end-to-end solution requires a comprehensive management architecture that can provision, monitor, and troubleshoot the service for a large number of users on a continuous basis. Given the breadth of the solution, several applications and tools are available to assist administrators. Management functions can be broadly divided into the following functional areas:

- **Provisioning and configuration**: Provision end users, virtual desktops, and endpoints using batch provisioning tools and templates. Vendor-provided APIs (XML) can be used for automation and self-service provisioning. These tools include software image and application management on endpoints and virtual desktops. Proper configuration helps ensure that the proper policy is applied for access, and applications Cisco Intelligent Automation and Cloupia management products are examples of applications that integrate with UCS manager to automate provisioning of virtual desktops
- **Device monitoring**: Monitor the status of every element in real time and obtain diagnostics. Simple Network Management Protocol (SNMP), syslog, XML-based monitoring and HTTP-based interfaces are used to manage devices. This function also includes inventory and asset management (hardware and software) of endpoints and virtual desktops
- **Quality-of-service (QoS) monitoring**: Monitor and troubleshoot the status and quality of experience (QoE) of user sessions. This function includes the use of packet capture and monitoring tools such as Cisco Network Analysis Module (NAM), Cisco NetFlow, and Wireshark to monitor a session. It also enables the desktop virtualization administrator to remotely access the endpoint and virtual desktop to observe performance and collect bandwidth and latency measurements. These

tools also can measure computing, memory, storage, and network utilization in real time to identify bottlenecks or causes of service degradation. Session details records for a virtual desktop session can indicate connection failures and quality problems.

- **Statistics collection and reporting**: Collect quality and resource use measurements and generate reports useful for operations, infrastructure optimization, and capacity planning. Measurements include session volume, service availability, session quality, session detail records, resource utilization, and capacity across the system. The reports can be used for billing purposes and for service-level management

Cisco Desktop Virtualization Services

Complementing Cisco VDI and Virtual Workspace solutions, Cisco Desktop Virtualization Services deliver rich, expert-based services end to end that can help you rapidly realize a desktop virtualization solution of your choice anywhere, with any device, over any medium. These services also help provide the right fit with your existing investments and align your IT and business strategies. Our services can help you plan, build, and manage a secure desktop virtualization solution. These include:

Plan

- Desktop Virtualization Strategy Service: Develop a comprehensive business case and solution strategy for desktop virtualization. Assess operational and mobility services readiness. Create an architecture that may include desktop virtualization, collaboration, and innovation.
- Desktop Virtualization Assessment Service: Conduct a comprehensive feasibility study and total cost of ownership (TCO) analysis for desktop virtualization.
- Desktop Virtualization Planning and Design Service: Design a reliable desktop virtualization infrastructure that fits your IT strategy and user requirements.

Build

- Desktop Virtualization Pre-Production Pilot Service: Validate specific technical requirements for your proposed desktop virtualization design prior to full production.
- Desktop Virtualization Implementation Service: Smoothly implement your desktop virtualization solution, including creating an implementation plan and migrating users.

Manage

- Desktop Virtualization Optimization Service: Understand the performance and utilization of your desktop environment and evolve your VDI or VXI solution to assure operational excellence as you expand.
- Cisco Solution Support Service for VXI: Rapidly resolve operational issues with solution support that provides a single point of contact.

Conclusion

The Cisco Virtual Workspace (VXI) Smart Solution is a fully integrated, open, and validated desktop virtualization architecture that delivers a superior collaboration and rich media experience with best-in-class Return on Investment. The solution architecture facilitates rapid deployment of desktops

and improves control and security by increasing visibility at the virtual machine level. The modular, ecosystem-based architecture preserves customer flexibility and helps ensure long-term alignment with the industry.

For More Information

- Visit Cisco Virtual Workspace (VXI) Smart Solution on Cisco Design Zone:
  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns1100/landing_vxi.html
- Cisco Virtual Workspace (VXI) Smart Solution 2.7 with VMware View 5.1
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/CVD/VXI_CVD_VMware.html
- Cisco Virtual Workspace (VXI) Smart Solution 2.7 with Citrix XenDesktop 5.6
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/CVD/VXI_CVD_Citrix.html
- Cisco Introduction to End to End Desktop Virtualization (NO NAME or LINK CHANGE)
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/VXI_PRIMER.pdf
- Cisco Virtual Workspace (VXI) Smart Solution As-Built Reference Guide
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf
- Cisco Virtual Workspace (VXI) Smart Solution At-A-Glance
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/ATAG/VXI_ATAG.pdf