Network Considerations to Optimize Virtual Desktop Deployment

What You Will Learn

Enterprises today strive to improve productivity, increase operating efficiency, and offer competitive advantages by enabling communication, collaboration, and computing technologies. The enterprise workspace is rapidly evolving to adapt to these changing business requirements. Several notable trends in the workspace are:

- Wide adoption of collaboration and real-time applications such as IP Telephony, instant messaging, Web 2.0, Cisco WebEx®, and peer-to-peer applications
- Increased use of video applications, including desktop video, video conferencing, video surveillance, and digital signage
- Ubiquitous mobility and proliferation of Wi-Fi–enabled clients such as dual-mode phones, laptops, and radio-frequency identification (RFID) devices
- Emerging workspace virtualization technologies including several forms of desktop virtualization solutions

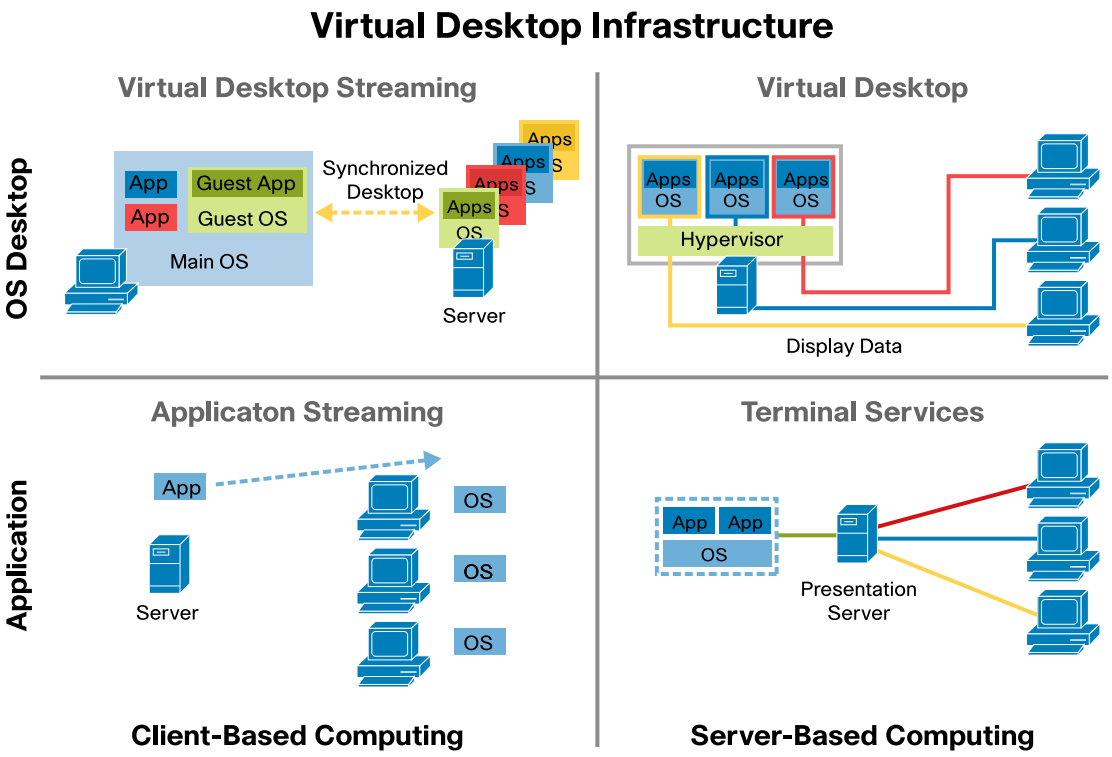
As the workspace continues to evolve, enterprise IT departments must prepare their network infrastructure to meet the future demands. This document examines the effects of desktop virtualization technologies on the network and provides infrastructure design considerations for such deployments.

Desktop Virtualization Technologies

The current distributed desktop computing environment gives corporate users ample client computing power and flexibility to enable productivity applications at work, at home, and at remote locations with flexible user control and a good user experience. However, this model also presents enterprise IT departments with challenges such as high operating costs for desktop configuration, patch management, and application support; compliance with regulations that demand security and data protection; and the capability to scale in the event of a merger or acquisition or the need for disaster recovery.

To meet these challenges, enterprise IT departments are looking for ways to centralize the control and management of client computing environments. Several client computing virtualization technologies in recent years have shown promise for creation of a new desktop computing model. Together with remote client delivery protocols and connection broker software solutions, they deliver a solution known as virtual desktop infrastructure (VDI). The scope of VDI is still in flux and quickly evolving, with a wide range of VDI products and solutions currently available on the market. Figure 1 categories the current solutions and approaches.

Figure 1. Virtual Desktop Infrastructure



Desktop Virtualization

In the desktop virtualization model, the entire client desktop environment is decoupled from the underlying physical hardware and host operating system. This approach allows the enterprise IT department to centrally provision and manage the client desktop environment. The client virtual desktop environment can be run at different places: on the server side or the client side.

Server-Based Desktop Virtualization

Server-based desktop virtualization allows execution of the client desktop environment on the data center servers and presentation of that desktop environment on the client side. The client desktop screen view is delivered from data center servers to the users through remote client display protocols such as Microsoft Remote Desktop (RDP) and Citrix Independent Computing Architecture (ICA). Remote execution allows the enterprise IT department to manage users' desktops centrally in the data center and control the applications and data within the data center. At the server side, server virtualization technologies are often deployed to allow multiple client environments to share the common server hardware resources. At the client side, dedicated thin clients (vendors such as Wyse) or repurposed PCs are deployed. The dedicated thin clients have limited hardware computing power and software functionalities, and their main purpose is to serve as terminals to receive the virtual desktop display. Representative examples of server-based desktop virtualization solutions are VMware VDI and Citrix XenDesktop solutions.

In addition to the benefits of central desktop management, server-based desktop virtualization offers strong benefits in data protection and disaster recovery. The dedicated thin-client hardware also provides power benefits at the workspace environment as thin clients typically consume less power than today's PCs and laptops.

Because of its heavy dependency on network connectivity, server-based desktop virtualization is not the best solution for users who need the flexibility of being able to work offline.

Client-Based Desktop Virtualization

Client-based desktop virtualization uses virtualization technology to separate the user's desktop environment from the physical hardware and host operation system. In this case, both the user's virtual desktop and the host OS run in parallel on the client hardware. The virtual desktop images can be centrally managed by the corporate IT department and streamed to the user's PC. Representative examples of client-hosted desktop virtualization are VMware View, Moka5 LivePC, and Microsoft Virtual PC with the Microsoft Enterprise Desktop Virtualization (MEDV) management solution.

The client-hosted desktop virtualization provides users more flexibility to have multiple computing environments for different purposes and to be able to work offline. It allows enterprise IT departments the benefits of central management of desktop images and applications. However, unlike server-based desktop virtualization, the user and application data are distributed at the client side.

Application Virtualization

Application virtualization technology packages and isolates specific applications from the underlying host operating system. This approach is useful for resolving application compatibility problems and supporting task workers who need to access only certain applications. Application virtualization helps corporate IT departments reduce the complexity of testing, deploying, updating, and removing applications. As with desktop virtualization, the application-computing environment can be executed at the server side or at the client side. This technology has been on the market for many years and is widely deployed for remote access and hosted applications.

Server-Based Application Virtualization (Terminal Services)

In server-based application virtualization, also called terminal services, the applications run on data center servers. Users receive the application environment display through a remote client display protocol such as Microsoft RDP or Citrix ICA. The most popular examples are Microsoft Terminal Services and Citrix Presentation Server.

Client-Based Application Virtualization (Application Streaming)

In client-based application virtualization, the target application is packaged and streamed to the client PC. It has its own application computing environment that is isolated from the client OS and other applications. A representative example is Microsoft SoftGrid.

VDI Technology Characteristics

Each VDI technology has its own networking connectivity, bandwidth, quality-of-service (QoS), and security characteristics, summarized in Table 1.

Table 1. Network Characteristics of VDI Technologies

VDI Technology	Networking Characteristics
Server-based desktop virtualization	• Relies on always-on network connectivity (some vendors offer offline mode) • RDP and ICA protocol traffic sent through the network between end users and data centers • Long-term variable bit rate; rendered video applications can consume high bandwidth • User experience subject to bandwidth availability and network latency • High data protection security
Client-based desktop virtualization	• Supports offline mode • Application traffic sent directly to the network • Bursty and bulky OS streaming traffic • No inherent data protection security
Server-based application virtualization (terminal services)	• Relies on always-on network connectivity • Long-term variable bit rate • RDP and ICA protocol traffic sent through the network between end users and data centers; possible for it to mix with other native application traffic from applications on the host OS • User experience subject to bandwidth availability and network latency • High data protection security

Client-based application virtualization (application streaming)	• Bursty application streaming traffic • Application traffic sent directly to the network; possible for it to mix with other native application traffic from applications on the host OS • No inherent data protection security

Since most organizations have a variety of user groups (task workers, knowledge workers, power users, etc.) with different application requirements and user-experience expectations, currently no one technology meets all VDI deployment needs. In many cases, enterprise IT departments deploy multiple technologies for different user groups.

Even with VDI deployment, the workspace environment will continue to be a heterogeneous environment for the foreseeable future. For example, a typical workspace environment can have all the following devices:

- Hardware thin clients
- Repurposed PCs that are deployed for VDI
- IP phones
- PCs for power users, guest users, etc.
- Other network devices such as printers, wireless access points, video surveillance cameras, and badge readers

Campus Network Considerations

The campus network connects the users and devices in the corporate workspace to the data center, WAN, and Internet. 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, and traffic monitoring and management. When planning a campus network, it is important to consider the trends in the workspace environment and design the infrastructure with performance, scalability, and services that will meet the requirements for both today and tomorrow. The Cisco® Enterprise Campus 3.0 Architecture at http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html provides an overall design recommendation for a campus network. This section highlights some design elements that should be considered in a VDI deployment.

Resiliency

As described earlier, the server-based desktop virtualization and application virtualization technologies rely on always-on network connectivity to the data center. Therefore, resilient network design should be considered throughout the campus and WAN:

- Network resiliency can be achieved by designing the campus network with topology, device, and link redundancy and an optimized routing control plane. Technologies such as the Cisco Catalyst® 6500 Virtual Switching System (VSS) with its Multi-Chassis Etherchannel, Equal Cost Multi-Path recovery can be used to help improve the resiliency of the network design to deliver a sub-second network convergence in a failure recovery.
- Device resiliency can be achieved with a combination of physical redundancy (such as redundant switch supervisors), device hardening (such as control plane policing), and other supporting software features such as nonstop forwarding (NSF) and stateful switchover (SSO).
- Operation resiliency reduces planned downtime to help ensure always-on connectivity. For example, the In-Service Software Upgrade (ISSU) on the Cisco Catalyst 4500 Series Switches provides for less than 200 milliseconds of traffic loss during a full Cisco IOS® Software upgrade.

Bandwidth

As shown in Table 1, different VDI technologies have different traffic patterns and network bandwidth requirements. In general, server-based desktop and virtualization have long-term variable bit rate (VBR) traffic patterns, mainly because of the characteristics of the RDP and ICA protocols, which use compression techniques. The maximum bandwidth requirement can vary greatly depending on user activities, which directly affect the complexity of the desktop display. For video applications, server-side image rendering can greatly increase the bandwidth requirement to several hundred Mbps. For client-based desktop virtualization or application streams, bursty bulk data transfers may occur when the OS and applications are streamed to the client.

Given these bandwidth considerations, ample network bandwidth should be allocated to handle various scenarios. Ethernet 10/100/1000-Mbps host-facing connectivity would provide bandwidth headroom. Correspondingly, bandwidth headroom should be planed in the campus distribution and core layers.

Security

Server-based desktop and application virtualization technologies provide good data protection. In addition, dedicated thin-client devices in general have less exposure to security vulnerabilities due to their simplicity. Client-based desktop virtualization and application streaming technologies with standard PCs have security requirements similar to those for today's PC environments. When planning for network security services, the overall workspace environment needs to be considered. In a mixed desktop environment, proper security services are required to protect the client and network infrastructure.

- Consider IEEE 802.1x-based identity services to prevent unauthorized access and gain visibility into user access to network resources. Consider layer 2 security services such as port security, dynamic ARP inspection, DHCP snooping and IP source guard to mitigate layer 2 threats.
- Consider NetFlow to gather telemetry data to detect and observe any anomalous or malicious activities. NetFlow will also help IT monitor performance and troubleshoot VDI delivery.
- Consider segmentation and network virtualization technologies such as VLAN and virtual routing and forwarding (VRF) in the campus to segment group of users and apply specialized policies.

Rich Media Support

Delivery of rich media, such as voice over IP (VoIP) and video (streaming video and bi-directional interactive video applications), is one of the biggest challenges in desktop virtualization deployment. VDI vendors today struggle to provide a good user experience for voice and video applications within the framework of existing remote protocols (RDP and ICA) that are not optimized for rich-media delivery. Some VDI vendors, such as Wyse TCX Multimedia 3.0, have started to introduce technologies to allow native VoIP and media delivery instead of tunneling the server-rendered media data into RDP and ICA transport. This approach could greatly improve the rich-media user experience. With this, the network-based QoS and multicast services delivered by the campus network infrastructure today to optimize the delivery of VoIP and video applications could eventually be used to assist in rich-media delivery in a VDI deployment.

PoE is required today to support IP phones in the workspace environment. Thin-client vendors are also planning to deliver PoE-enabled thin clients to take advantage of this technology, mitigating the need for separate power outlets. With the introduction of the PoE Plus (IEEE 802.3at) standard, which provides approximately 30-watt (W) PoE, the list of devices that can benefit from PoE is extended to new device types such as thin clients in point-of-sale kiosks with integrated display monitors.

Data Center Considerations

VDI deployments also bring changes in data center networking. Server virtualization technologies are used to host multiple virtual desktop computing environments on a single physical server or server blade. Each user's client

computing environment is a virtual machine running on top of the hypervisor, which allows the virtual machines to share the server hardware resources. Virtual machines are instantiated on demand as users log onto VDI management applications (known as connection brokers) to request connection to their virtual desktops. Logically, a user's desktop network entity really starts in the data center, rather than in the campus, bringing changes and new requirements to data center networking:

- The data center network infrastructure needs to support increased bandwidth; port density; and IP address use and DHCP services as a result of the large number of user virtual desktop instances and the corresponding application traffic.
- The data center network infrastructure needs to support highly scalable and resilient server virtualization deployment. VMware VMotion technology greatly improves the flexibility and availability of virtual machine deployments. It also poses new challenges to network infrastructure to support a larger Layer 2 domain and transparent policy mobility.
- As users' desktop environments instantiate in the data center, access services and user policies traditionally enforced in the campus access layer of the network now need to be considered in the data center.

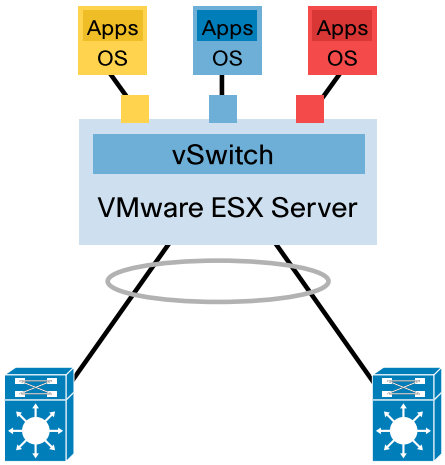
Bandwidth

More traffic and a higher port density are expected in the data center in a VDI deployment as users now move into the data center. The data center network should be designed to provide enough performance, scalability, and Gigabit Ethernet and 10 Gigabit Ethernet port density to accommodate this additional load.

For desktop virtualization, the virtual desktop computing environments are executed on virtual machines on the servers. Depending on the end-user performance requirements, each server blade can support one (for power users) or many (for task workers) virtual machines. To save costs and reduce server resource utilization, enterprise IT departments tend to deploy as many virtual machines as possible on a physical server. To deliver higher data throughput, Gigabit Ethernet server network interface cards (NICs) are often bundled through link aggregation technologies.

As shown in Figure 2, the multichassis EtherChannel technology from the Cisco Catalyst 6500 VSS or Cisco Nexus™ Family virtual PortChannels (vPCs) can be deployed in data center server access to greatly improve server bandwidth utilization and availability.

Figure 2. Multichassis EtherChannel



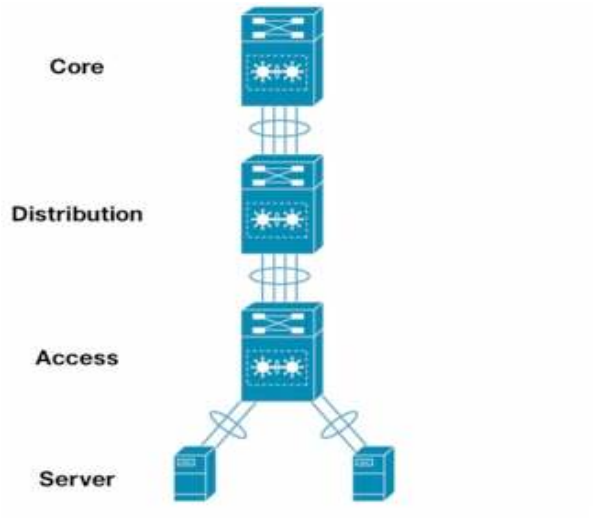
VMware VMotion

VMware VMotion technology allows virtual machines to move from one physical server to another without service interruption. The move can be within the same data center or across data centers for backup and disaster

avoidance. This new mobility application presents challenges to network infrastructure, requiring management of a large, scalable, Layer 2 domain and dynamic policy enforcement.

As shown in Figure 3, Cisco Catalyst 6500 VSS technology deployed at the data center server access and distribution layers help scale the network infrastructure to support a large, resilient, loop-free Layer 2 network within the data center. Refer to http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/vssdc_integrate.html for details.

Figure 3. Cisco Catalyst 6500 VSS Deployed in Data Center Network Core, Distribution, and Server Access Layers



To gain more flexibility, VMware VMotion across the data center is becoming a requirement. To support this new requirement from the data center infrastructure perspective, data center interconnect technologies need to be considered to be able to transport traffic across the Layer 2 topology.

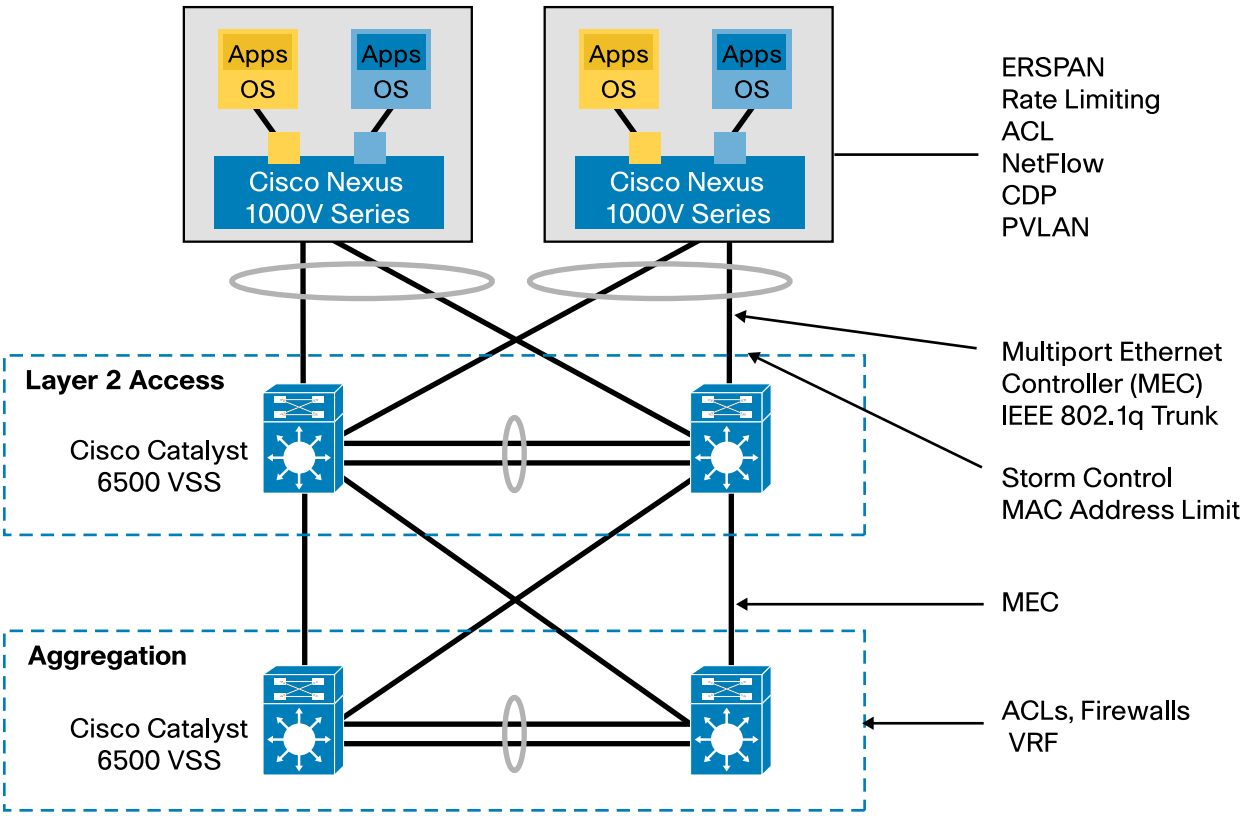
Network Services

With VDI deployment, the enterprise workspace is moving into the data center, which has been a relatively more controlled and secure environment with mainly application and data resources. Network and security services now must be considered to provide network-level traffic monitoring, troubleshooting, and QoS control; network infrastructure protection; and secure access control (Figure 4). The following are some network services to consider:

- Deploy virtual desktops and corporate applications and data resources on separate servers. Apply network segmentation, virtualization and firewall technologies to enforce proper access control policies between virtual desktops and corporate resources.
- Consider applying traditional campus access services in the data center access layer for infrastructure security: for example, access control lists (ACLs), QoS, layer 2 security such as port security, dynamical ARP inspection, IP source guard etc, private VLANs (PVLANs), and Switched Port Analyzer (SPAN).

Server virtualization presents new challenges to some of the Layer 2 network services designed for access-layer switches directly connecting to endpoints. In this case, the data center access switches no longer form the true access layer. Virtual switches (vSwitches) inside the hypervisors now serve as virtual access switches connecting the virtual machines. The data center access switches now see aggregated traffic from multiple virtual machines on each physical port. Cisco Nexus 1000V Series Switches provide the solution by allowing a set of network policies to be applied to the virtual machines directly at the hypervisor level. In addition, Cisco VN-Link technology enables consistent policies to follow the virtual machines in VMware VMotion events.

Figure 4. Network Services for Virtual Machines



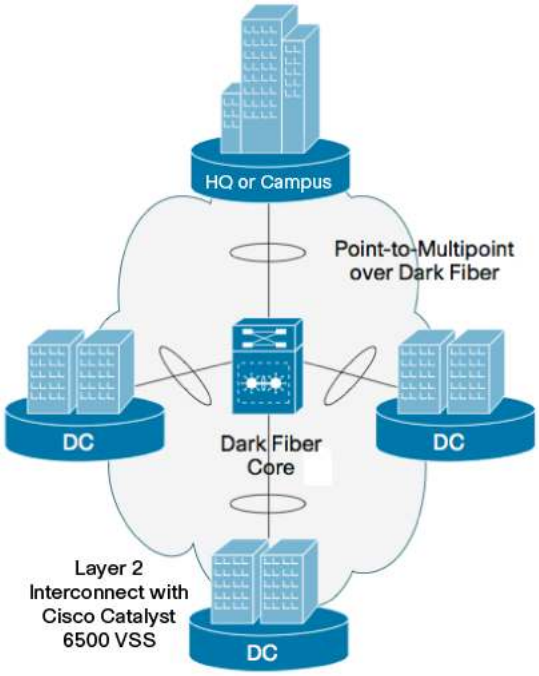
Resiliency

As in campus networks, resiliency is a critical design consideration for data center networks. The design considerations and technologies described earlier in this document for campus networks also apply here.

Data center interconnect technologies allow enterprise IT departments to establish backup data centers for the purposes of business continuity and flexible resource planning. Both LAN and SAN connectivity need to be considered. If VMware VMotion across data centers is a requirement, several data center interconnect technologies are available to maintain the Layer 2 connectivity across data centers interconnected with dark fiber connections or a service provider IP or Multiprotocol Label Switching (MPLS) network.

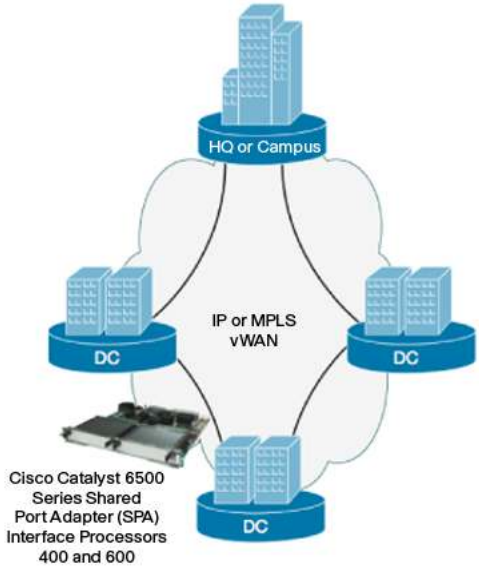
- Cisco Catalyst 6500 VSS or Cisco Nexus™ Family virtual PortChannels (vPCs) technology to interconnect data centers across a short distance physically connected over dark fiber connections (Figure 5)

Figure 5. Data Center Interconnect through Cisco Catalyst 6500 VSS or vPC Technology



- Ethernet over MPLS or Virtual Private LAN Services (VPLS) technology to interconnect data centers over an MPLS-based private IP network (Figure 6)

Figure 6. Data Center Interconnect over MPLS or IP Network



- Ethernet over a generic routing encapsulation (GRE) tunnel to interconnect data centers over an generic or service provider-provided IP-based network

WAN Considerations

Today, the quality of the virtual desktop experience is greatly affected by the available bandwidth, average latency, and packet loss of the transport network. As VDI is deployed in regional, international, and branch offices for its data protection benefits, virtual desktop traffic is often transported over WANs. Even in a large campus VDI deployment,

with the trend toward data center consolidation, VDI traffic often travels across a WAN to reach the remote data centers.

WAN optimization technologies should be considered to optimize the VDI delivery with the following benefits:

- Improved performance and user experience by reducing the latency of VDI traffic over WAN links
- Reduced bandwidth requirements
- Optimized printing over the WAN

For more information about the joint Cisco and VMware solution for optimizing VDI delivery with Cisco Wide Area Application Services (WAAS) Software and Cisco ACE Application Control Engine solutions at http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns377/white_paper_c11-494994.pdf.

For campus VDI deployment with users or applications that have very high latency and user experience requirements, consider positioning a local data center adjacent to the campus network.

Conclusion

Network architecture is evolving in response to a combination of new business requirements, technology changes, and growing end-user expectations. A new trend, virtual desktop infrastructure, offers the promise of simplified desktop management, data protection, and cost savings through green technologies. Its success will eventually be determined in large part by the user experience that it can deliver. Meanwhile, existing distributed desktop computing model will continue to be around and adding new collaboration applications for the years to come. Using both existing and new network technologies, the networking infrastructure, from the campus data center to branch offices and the WAN, can help scale and optimize virtual desktop delivery to improve the user experience and serve as a common platform for consistent policies in an increasingly heterogeneous desktop and application environment.

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 C11-531553-00 04/09