Cisco Application Networking Services for VMware Virtual Desktop Infrastructure

Deployment Guide

Contents

Introduction

Document Purpose

Customers use desktop virtualization solutions such as VMware® Virtual Desktop Infrastructure (VDI) to replace traditional PCs with virtual machines that are managed from the data center to reduce operational costs, increase control of desktop management, and extend business continuity and disaster recovery to enterprise desktops.

However, when desktop virtualization solutions are deployed over the WAN, latency and bandwidth constraints limit their effectiveness. Customers face the following challenges in deploying virtual desktop solutions for the enterprise:

- Poor performance of display protocols over the WAN, affecting employee productivity
- High bandwidth consumption, increasing costs
- Limited scalability, reducing the number of users that can be supported
- Poor performance of centralized printing and increased costs of printing at the branch
- Large amount of time and bandwidth required to back up data center virtual desktop infrastructure for disaster recovery

To address the challenges associated with today's complex user desktops, Cisco in collaboration with VMware offers a joint solution for VMware VDI, an enterprise network architecture for deploying VMware VDI with Cisco® Application Networking Services (ANS) with design best practices and implementation guidance that optimizes desktop delivery to all type of users in the enterprise.

Cisco and VMware have worked together to deliver this joint solution, including collaboration on the lab setup, solution testing, and validation of test results. Cisco and VMware jointly validate that the lab setup and solution testing represent best efforts in creating a realistic customer deployment and accurate documentation of such deployment.

The joint Cisco and VMware solution optimizes VMware VDI delivery, offering the following benefits:

- Near-LAN performance for virtual desktops over the WAN, improving performance by 70 percent
- Increase scalability of the number of VMware VDI clients by 2 to 4 times and provide massive scalability of VMware VDI and VMware VDM data center infrastructure
- Reduce costly WAN bandwidth required by 60 to 70 percent
- Optimize printing over the WAN by 70 percent and provide the option of a local print server hosted on the Cisco Wide Area Application Services (WAAS) appliance
- Improve business continuity by accelerating virtual image backups by more than 10 times, with bandwidth reductions exceeding 90 percent.

The purpose of this document is to provide a design best practices and deployment guide for the joint Cisco and VMware solution to optimize desktop delivery to all type of users in the enterprise.

Prerequisites

The following prerequisites are required to deploy the joint Cisco and VMware solution:

- Working knowledge of VMware VDI
- Experience with basic networking and troubleshooting
- Experience installing the Cisco products covered by this network design, including the Cisco WAAS and Cisco Application Control Engine (ACE) product families
- Working knowledge of Cisco IOS® Software

Document Organization

Table 1 provides a brief description of each section.

Table 1. Document Organization

Section	Description
Solution Overview	Provides a high-level introduction to the solution; introduces the solution, historical aspects, potential benefits, scope, and limitations
Solution Architecture	Describes the architecture of the joint solution
Implementing and Configuring the Cisco WAAS Solution	Describes configuration and implementation of Cisco WAAS within the joint solution
Implementing and Configuring the Cisco ACE Solution	Describes configuration and implementation of Cisco ACE within the joint solution
Network Monitoring with NetQoS	Describes the network monitoring software used for the solution testing
Solution Testing and Results	Describes the test methodology used and presents the results

Solution Overview

Cisco WAAS and ACE with VMware VDI reduces the cost and complexity of managing desktops by optimizing virtual desktop delivery over the WAN while avoiding costly bandwidth upgrades.

- This jointly validated solution improves employee productivity by combining VMware VDI for virtualizing and centralizing desktops and Cisco WAAS for compressing and accelerating VMware VDI traffic and optimizing branch office printing.
- Cisco WAAS increases the scalability and number of VMware VDI users supported over the WAN, and Cisco ACE improves the availability and scalability of data center VMware VDI infrastructure.
- Enterprise business continuity is improved by reducing the time required for backup and replication of datacenter VMware VDI infrastructure.

Solution Description

The joint Cisco and VMware solution offers optimized and scalable enterprise network architecture to deploy VMware VDI using Cisco ANS products. Cisco ANS provides optimization services and application scalability for VMware VDI deployments in the data center and branch offices. Following are the main components of this solution:

- VMware VDI and VMware Virtual Desktop Manager (VDM), to virtualize and centralize desktops

Step 1. Virtual desktops are hosted on VMware Infrastructure 3 ESX Server in the data center.

Step 2. VMware VDM Connection Server allows remote branch users to connect to their virtual desktops in the data center running VMware ESX Server.

- Cisco WAAS, to accelerate virtual desktop performance, reduce bandwidth demands, and provide faster backup

Step 3. Cisco WAAS, deployed on both sides of the WAN, optimizes display protocol traffic between the end users and the data center using a sophisticated combination of TCP optimizations that reduce the effects on the WAN, providing persistent session-based compression and data redundancy elimination. Cisco WAAS optimizes display protocol delivery, including delivery of Microsoft Remote Desktop Protocol (RDP), the underlying protocol used by the current version of VMware VDM and currently the predominant protocol used by the various virtual desktop implementations.

Step 4. The branch-office Cisco WAAS appliance provides print services locally to branch-office users by running Microsoft Windows print services.

Step 5. Cisco WAAS can also be deployed between data centers to optimize backup of VMware VDI infrastructure for disaster recovery.

- Cisco ACE, to improve the scalability and availability of data center VMware VDI infrastructure

Step 6. The Cisco ACE appliance provides load balancing among multiple VMware VDM Connection Servers, providing scalability and resiliency to the VMware VDI solution.

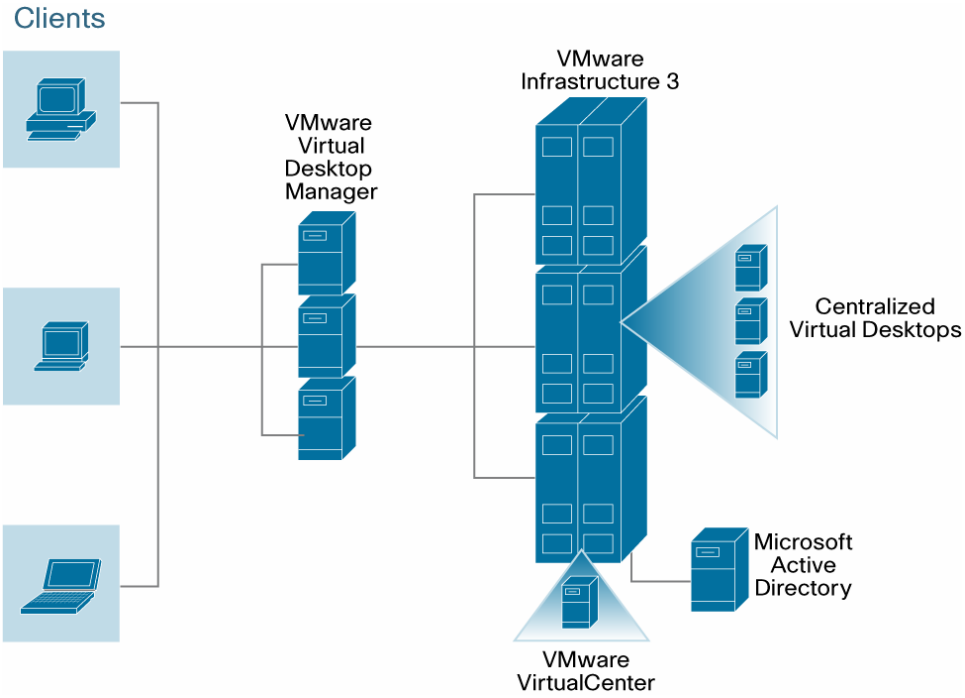
VMware Virtual Desktop Infrastructure

VMware VDI is an integrated desktop virtualization solution that delivers enterprise-class control and manageability. VMware VDI, built on VMware's industry leading virtualization platform, provides an efficient and reliable environment for virtual desktops.

The VMware VDI solution includes the following components (Figure 1):

- VMware Infrastructure 3 software, which provides a platform for hosting virtual desktops including the VMware ESX and VMware ESXi software
- VMware VDM, a desktop management server that securely connects users to virtual desktops in the data center and provides an easy-to-use web-based interface for managing the centralized environment
- VMware VDM Client, which runs on a windows PC and allows users to connect to virtual desktops through VMware VDM; clients can use Microsoft RDP or the VMware VDM Client software

Figure 1. VMware VDI Solution Components



VMware VDI enables users to run desktop operating systems and applications on virtual machines that reside on servers in the data center. These desktop systems running on virtual machines are called virtual desktops. Users access virtual desktops and applications from a desktop PC client or thin client (called VMware VDI clients) using a remote display protocol.

VMware VDI clients first connect to the VMware VDM Connection Server. The VMware VDM server then sends the connections to the end virtual desktops. VMware VDM servers maintain a central inventory of virtual desktops running on VMware ESX Server. Administrators provision virtual desktops on VMware ESX Servers and then register them to the VMware VDM server. In a large environment, multiple VMware VDM servers can be used to share client requests. In such cases, VMware VDM servers are replicated, with one primary VMware VDM server.

VMware VDI offers the following main benefits:

- Desktop environments are isolated.
- Data is secure in the data center.
- All applications work on a virtual machine.
- Normal management tools work on a virtual machine.
- Images are managed centrally.
- Hardware can be consolidated.
- Desktops are always on and always connected.
- Users have access to their desktops from anywhere.

Cisco Application Networking Services

Cisco ANS is a comprehensive portfolio of application networking solutions and technologies that supports the application delivery network in both the data center and the branch office. The Cisco ANS product portfolio includes these components:

- **Cisco WAAS:** Provides accelerated delivery of centralized applications to remote users, helping consolidate resources, optimize the WAN, and locally host critical applications
- **Cisco ACE:** Optimizes overall application availability, security, and performance by delivering application switching and load balancing

Cisco Wide Area Application Services

Cisco WAAS is a comprehensive WAN optimization solution that accelerates applications over the WAN, delivers video to the branch office, and provides local hosting of branch-office IT services. Cisco WAAS enables IT departments to centralize applications and storage in the data center while maintaining LAN-like application performance and to rapidly deliver local branch-office IT services while reducing the branch-office device footprint through the following application acceleration and WAN optimization features:

- **Transport Flow Optimization (TFO):** TFO addresses TCP performance limitations in high-latency, high-loss, and high-bandwidth networks. TFO employs the following main optimizations:
  - **Selective acknowledgement (SACK) and extensions:** Reduces the amount of data that must be retransmitted when a loss is detected
  - **Large initial windows:** Reduces the amount of time each connection spends in slow-start mode to enable more timely use of available bandwidth
  - **Virtual window scaling of TCP windows:** Enables end nodes to transmit and receive larger amounts of data by increasing the amount of data that can be outstanding and unacknowledged in the network at any given time
  - **Advanced congestion avoidance:** Reduces the performance effects on throughput when a loss is detected by more intelligently managing the congestion window of each TCP connection; this congestion avoidance mode also enables “fill-the-pipe” optimization to enable applications that are TCP throughput bound to make better use of available bandwidth capacity
- **Data Redundancy Elimination (DRE):** DRE is a bidirectional database of blocks of data seen within TCP byte streams. DRE inspects incoming TCP traffic and identifies data patterns. Patterns are identified and added to the DRE database, and they can then be used in the future as a compression history, and repeated patterns are replaced with very small signatures that tell the distant device how to rebuild the original message. With DRE, bandwidth consumption is reduced, as is latency associated with data transfer because fewer packets need to be exchanged. DRE maintains full application and protocol coherency and correctness because the original message rebuilt by the distant Cisco Wide Area Application Engine (WAE) device is always verified for accuracy at multiple levels and is application independent. Patterns that have been learned from one application flow can be used when another flow is seen, even when using a different application. DRE can provide from 2:1 to 100:1 compression depending on the application, data, and workload.

- **Persistent Lempel-Ziv (LZ) compression:** Cisco WAAS implements LZ compression with a connection-oriented compression history to further reduce the amount of bandwidth consumed by a TCP connection. Persistent LZ compression, which can be used independently or in conjunction with DRE, provides from 2:1 to 5:1 compression depending on the application used and data transmitted, in addition to any compression offered by DRE.

Cisco Application Control Engine

Cisco ACE application switches provide core server load-balancing services, advanced application acceleration, and security services to increase application availability, performance, and security. Cisco ACE application switches provide a virtualized hardware platform, application-specific intelligence, powerful performance, and granular role-based administration. Cisco ACE application switches are typically deployed in the data center in an asymmetric solution.

Cisco ACE application switches are part of the Cisco family of Data Center 3.0 solutions and help to:

- Increase application availability
- Scale application performance
- Secure application delivery
- Facilitate data center consolidation

Cisco ACE achieves these goals through a broad set of intelligent Layer 4 load-balancing and Layer 7 content-switching technologies integrated with leading acceleration and security capabilities. To increase application availability, Cisco ACE uses best-in-class application-switching algorithms and highly available system software and hardware. Cisco ACE provides industry-leading scalability and throughput for application traffic. Cisco ACE greatly improves server efficiency through highly flexible application traffic management and offloading of CPU-intensive tasks such as SSL encryption and decryption processing and TCP session management.

Solution Benefits

The joint solution offers optimized virtual desktop availability, performance, security, and costs by providing virtual desktops to users.

Virtual Desktop Performance

The Cisco WAAS product family provides application optimization services for virtual desktop delivery to support VMware VDI client high performance:

- **WAN optimization:** Provides intelligent caching, compression, and protocol optimization that yields, for example, 3 to 25 times faster printing and 90 percent traffic reduction
- **Traffic compression:** Provides scalable LZ compression
- **Object caching:** Reduces requests to the server
- **Print optimization:** Reduces print data traversing the WAN and improves print latency

Virtual Desktop Availability

The Cisco ACE product family provides load-balancing services for VMware VDM connection brokers:

- **Server and application health monitoring:** Continuously and intelligently monitors availability of VMware VDM Connection Server
- **Server load balancing:** Efficiently routes end-user desktop connection requests to the best available VMware VDM Connection Server

Solution Architecture

In this solution, virtual desktops run on VMware ESX Servers, and two VMware ESX Servers are used in this architecture. These servers are connected to shared storage to take advantage of VMware VMotion, VMware Distributed Resource Scheduler (DRS), and high-availability features. VMware ESX Servers and virtual machines running on them are managed by VMware VirtualCenter, which runs on separate servers.

A VMware VDM connection broker server holds the inventory of all virtual desktops. Two VMware VDM connections broker servers are used in this architecture. User requests to these servers are load balanced by the Cisco ACE load balancer.

Connections between the branch office and data center are optimized by Cisco WAAS. Routers on the branch office and data center sides intercept Web Cache Communication Protocol (WCCP) traffic and use two Cisco WAAS appliances, one each on the branch-office side and the data center side, to optimize the traffic. One Cisco WAAS Central Manager on the data center side is used to monitor the traffic and configure the Cisco WAAS setup.

Various print options are available for users. Print servers in both the data center and the branch office accept the requests from virtual desktops. Additionally, VMware VDI clients at the branch office are connected to a local printer.

Installing and Configuring Virtual Desktop Machines

Virtual desktop machines run on VMware ESX Servers. Refer to the latest VMware documentation to create and provision virtual machines. The following steps were used in this solution to create virtual desktops:

Step 1. From VMware VirtualCenter, create a virtual machine. Figure 2 shows the sample configuration used in this solution.

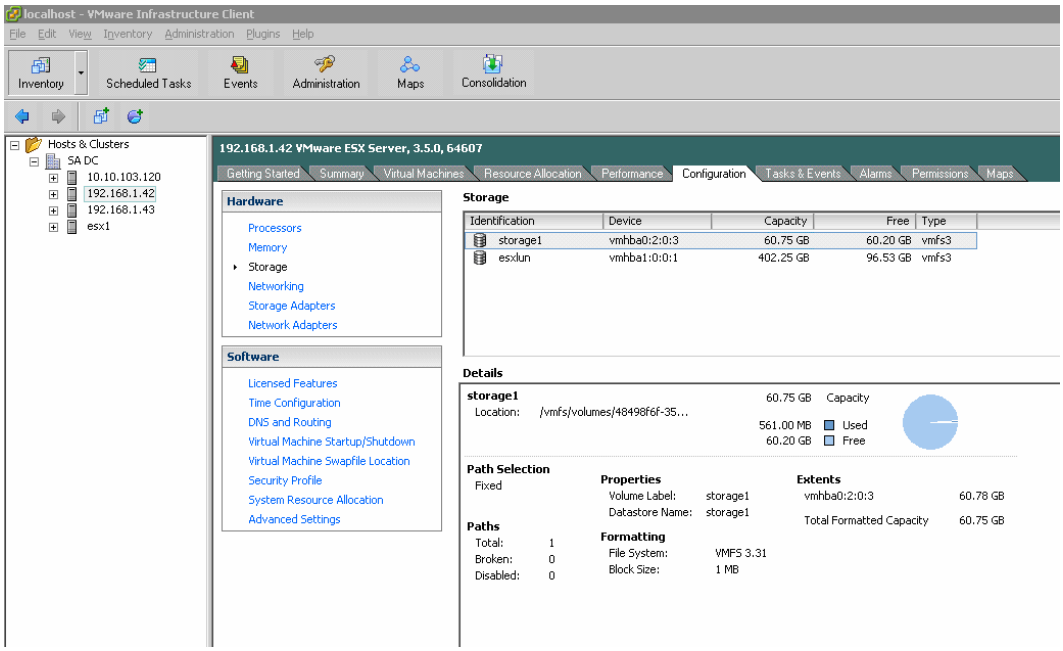
Step 2. Install Microsoft Windows XP on the virtual machine.

Step 3. Install VMware tools in the virtual machine.

Step 4. Download and install the latest VMware VDM agent on the Microsoft Windows XP virtual machine.

Step 5. Create a template of virtual machine to provision desktops in VMware VDM.

Figure 2. Sample Solution Configuration



Note: Refer to "Configuring Virtual Desktops for Optimization" to optimize the virtual machine for performance in this solution.

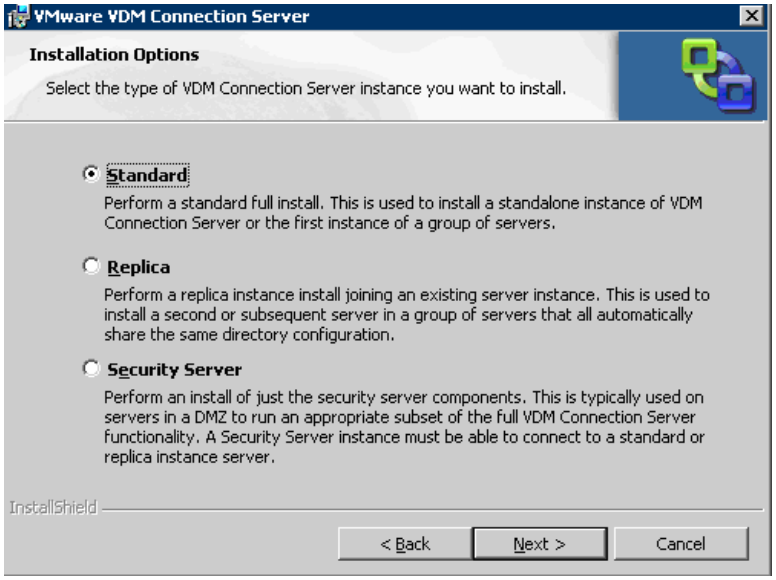
Installing and Configuring VMware VDM Connection Servers

Refer to the latest VMware documentation for installing and configuring VMware VDM Connection Server. The following steps were used in this solution to install VMware VDM Connection Server:

Step 1. Install Microsoft Windows Server 2003.

Step 2. Download and install the VMware VDM Connection Server executable file (VMware-vdmconnectionserver-2.1.0-<xxx>.exe). Install the first server as the standard server (Figure 3).

Figure 3. VMware VDM installation options



Step 3. Repeat the preceding steps for the second server, but this time select Replica.

Step 4. Next, a one-time configuration is required to configure VMware VDM Connection Servers.

Step 5. Launch http://hostname_or_ip.of.vdm.server/admin and log on with the appropriate credential. Typically, you can use any local administrator group user.

Step 6. In the Configuration section, add the license key.

Step 7. In the VirtualCenter Servers section, click Add and complete the details for the VMware VirtualCenters to be used with VMware VDM.

Step 8. Enable the VMware VDM Connection Server by selecting it from the list of VMware VDM servers and clicking Enable.

Provisioning Virtual Desktops

Desktops need to be provisioned for VMware VDM. The following steps were performed for this solution:

Step 1. Logon to VMware VDM Connection Server (as described in the preceding section) and click Inventory.

Step 2. In the All Desktops section, click the Desktops tab and click Add.

Step 3. Select Desktop Pool (persistent) and follow the steps to provision the required number of desktops. Select the virtual desktop template from the VMware VirtualCenter inventory when asked.

Step 4. When all the desktops are created and added to pool (this will take a while), name the desktops for the users. Select the user or group as required.

Installing and Connecting from the VMware VDI Client

Install and connect to the VMware VDI client. The following steps were performed for this solution:

Step 1. Download and run the VMware VDI client software (VMware-vdmclient-2.1.0-<xxx>.exe).

Step 2. Follow the standard installation steps to install the VMware VDI client software.

Step 3. Run the VMware VDI client software and enter the IP or hostname of the VMware VDM server to which you want to connect. From the list, choose the virtual machine to which you want to connect. If a hardware load balancer is used (such as in this solution), enter the IP or hostname of the load balancer in the VMware VDI Client window.

Server Hardware and Software

VMware ESX

VMware ESX Servers run all the desktop virtual machines. The tests use the following hardware:

- 2 VMware ESX 3 servers running host desktop virtual machine images
- 2 VMware VDM Connection Servers
- 1 VMware VirtualCenter Server

The VMware ESX Server environment consists of two physical servers running VMware ESX 3i with the following configuration:

- 2 dual-core Intel Xeon CPUs at 3.06 GHz
- 4 GB of RAM
- VMware ESX 3.5

VMware VDM Connection Server

VMware VDM Connection Servers are the middle clients to which users connect and authenticate. Users then select their desktops and connect to the end virtual desktop. The tests use the following hardware and software for VMware VDM Connection Servers:

- Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1
- 2 dual-core Intel Xeon processors at 3.06 GHz
- 1 GB of RAM
- Local storage

Storage for VMware VMotion

The physical VMware ESX Servers are connected to EMC Clariion storage over Fibre Channel. Both servers can write simultaneously to the Veritas File System (VxFS) on physical storage, a prerequisite for VMware VMotion.

Virtual Desktops

Each VMware ESX Server hosts 10 virtual machines running with the following configuration:

- 1 CPU
- 1 GB of RAM
- 8-GB hard disk
- Microsoft Windows XP OS with Service Pack 2.

Other Components

Microsoft Windows 2003 Server running as a VMware virtual machine serving the entire data center network includes the following:

- Microsoft Active Directory
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Printing

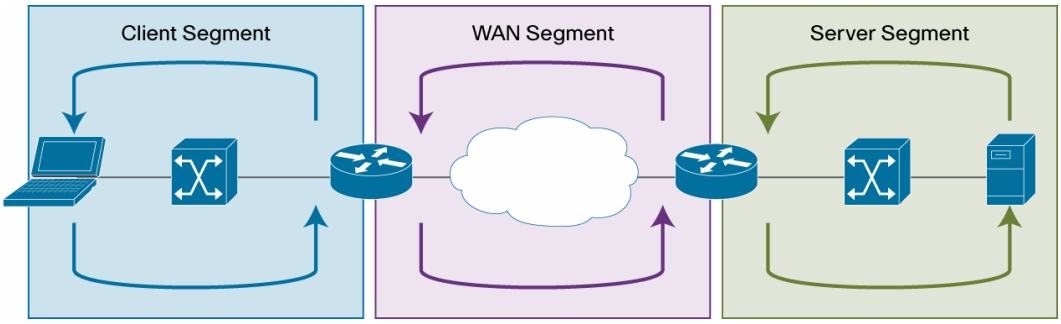
Depending on the printing scenario, the print server runs on either the branch-office or the data center side. More details can be found in the implementation sections. The following printer was used to test printing:

- HP LaserJet 4000 with Jetdirect network port

Solution Workflow without Cisco WAAS and Cisco ACE

Packet flow from a remote site can be categorized into three segments, client, WAN, and server (Figure 4).

Figure 4. Packet Flow



Client Segment

The client segment is the location to which users are connected that allows them to connect to virtual machines in the data center. Users connect PCs or thin clients to a local external switch or an integrated switch or router. When a user opens a VMware VDI client on the PC or thin client and connects to a virtual desktop running in the data center, the data is sent from the PC to the switch. The switch forwards the data to the router that is connected to the WAN.

WAN Segment

The WAN provides connectivity from the client location to the data center where the server farm is located. The WAN is provided by a service provider with a given service-level agreement (SLA). The WAN inherently introduces delay and packet loss to the data traffic (data packets).

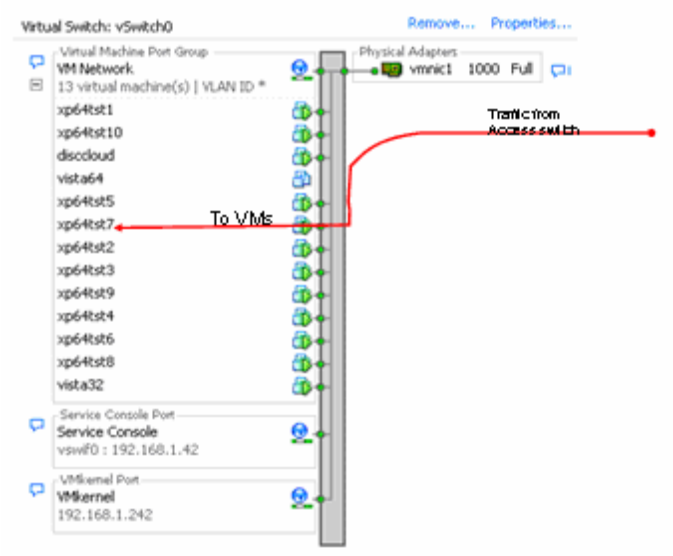
VMware ESX Server Segment

The server segment consists of a highly available and resilient core, aggregation layer, and access layer Ethernet switching. The core routes the data traffic to and from the WAN and the aggregation layer. The aggregation layer provides consolidation of multiple access layers and routes the access layer traffic to the core. The aggregation layer also takes the data traffic from the core layer and sends it to the appropriate access layer. The access layer provides connectivity to the VMware VDM Connection Servers and the VMware ESX Servers on which the virtual desktops reside. The data traffic from the client segment transverses the data center until it is received by the appropriate server.

Inside VMware ESX Server

Traffic from outside access switches is then redirected to a virtual switch inside VMware ESX Server. The virtual switch connects to the virtual machines and passes the traffic to them (Figure 5). Refer to the Cisco and VMware joint white paper for details.

Figure 5. Traffic flow inside VMware ESX Server



Cisco ANS Architecture for VMware VDI

Cisco ACE and WAAS reside in the data center and are configured to provide virtualized application optimization services for multiple VMware VDM server groups as well as other enterprise applications.

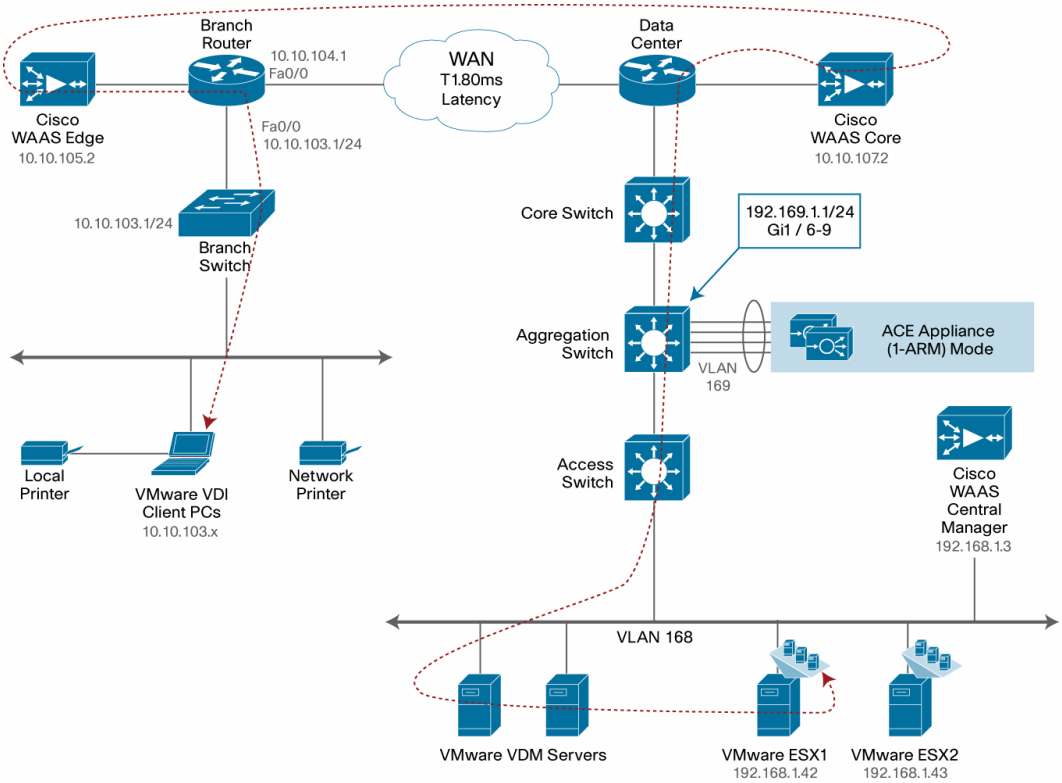
Because of their unique location, these solutions can take intelligent action on end-user traffic before it is routed to the end virtual desktops, including server load balancing, server health monitoring, and end-user access control.

Cisco WAAS also resides in the branch office and is configured to provide virtualized application optimization services for all application users in that location. 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 the virtual desktops through VMware VDM Servers, Cisco WAAS compresses the response and then efficiently passes it across the WAN with minimal bandwidth use and high speed. Commonly used information is cached at both the Cisco WAAS solution in the branch office and the data center, which significantly reduces the burden on the servers and the WAN.

Figure 6 shows the Cisco ANS architecture.

Figure 6. VMware VDI and Cisco WAAS Network Configuration



The VMware VDI and Cisco ANS solution consists of two main parts:

- Data center
- Enterprise branch office

Data Center

The data center follows the design guidelines in Data Center Infrastructure Design Guide 2.1, a Cisco Validated Design found at http://www.cisco.com/go/srnd. The design consists of a data center WAN router; core, aggregation layer, and access layer Ethernet switching; and the server farm where the application resides. This document focuses on the data center WAN router, aggregation layer, and server farm.

The core Ethernet switching provides routing to and from the data center WAN router and the aggregation layer. The access layer Ethernet switching provides Layer 2 connectivity for the server farms to the aggregation layer.

The data center WAN router performs the same function as the branch-office WAN router by redirecting traffic to the data center Cisco WAE. The data center Cisco WAE performs the following functions:

- **Locally cached data:** If the data that is being requested is locally cached, the Cisco WAE responds to the requestor with the cached data and requests only required data from the branch office. This process makes the WAN more efficient because only required data is requested.
- **New data:** If the data that is being forwarded to the branch office or coming from the branch office is new, the Cisco WAE runs compression algorithms on the data, enabling for the WAN to perform more efficiently.

Included in the data center is the Cisco WAAS Central Manager, which runs on the Cisco WAE appliance. The Cisco WAAS Central Manager provides a centralized mechanism for configuring Cisco WAAS features and for reporting and monitoring Cisco WAAS traffic. It can manage a topology containing thousands of Cisco WAE nodes and be accessed from any web browser using SSL. The Cisco WAAS Central Manager can be configured for high availability by deploying a pair of Cisco WAE appliances as central managers.

Within a Cisco WAAS topology, each Cisco WAE runs a process called the configuration management system (CMS). The CMS process provides SSL-encrypted bidirectional configuration synchronization of the Cisco WAAS Central Manager and the Cisco WAE appliances. The CMS process is also used to exchange reporting information and statistics at a configurable interval. When the administrator applies configuration or policy changes to a Cisco WAE appliance or a group of Cisco WAE appliances, the Cisco WAAS Central Manager automatically propagates the changes to each of the managed Cisco WAE appliances. Cisco WAE appliances that are not available to receive the changes will receive them the next time the appliances become available.

The aggregation layer contains Cisco ACE, which provides the following features:

- **Virtualization:** Virtualization partitions devices into multiple contexts, where each context can be configured for different applications and is independent of any others. In the joint solution, the Cisco ACE appliance is configured with the Admin context and the VMware VDM context.
- **Server load balancing:** The Cisco ACE VMware VDM context is configured to provide intelligent load balancing of the VMware VDM Connection Servers.
- **Session persistence:** Session persistence is the capability to forward client requests to the same server for the duration of a session. Cisco ACE is configured for source IP-based session persistence.

Enterprise Branch Office

In an enterprise branch-office setup, the Cisco WAE appliance is connected to the local branch-office router, typically a Cisco Integrated Services Router.

Users connect PCs or thin clients to a local external switch or an integrated switch or router. When a user opens a VMware VDI client on the PC or thin client and connects to the virtual desktop running in the data center, the data is sent from the PC to the switch. The switch forwards the data to the router that connects to the WAN.

The traffic is redirected from the branch-office router to the Cisco WAE by WCCP.

The Cisco WAE performs the following functions:

- **Locally cached data:** If the data that is being requested is locally cached, the Cisco WAE responds to the requestor with the cached data and requests only the required data from the server farm. This approach makes the WAN more efficient because only the necessary data is requested.
- **New data:** If the data that is being forwarded to the server farm or coming from the server farm is new, the Cisco WAE performs compression algorithms on the data, making the WAN more efficient.

WAN Simulation between Branch Office and Data Center

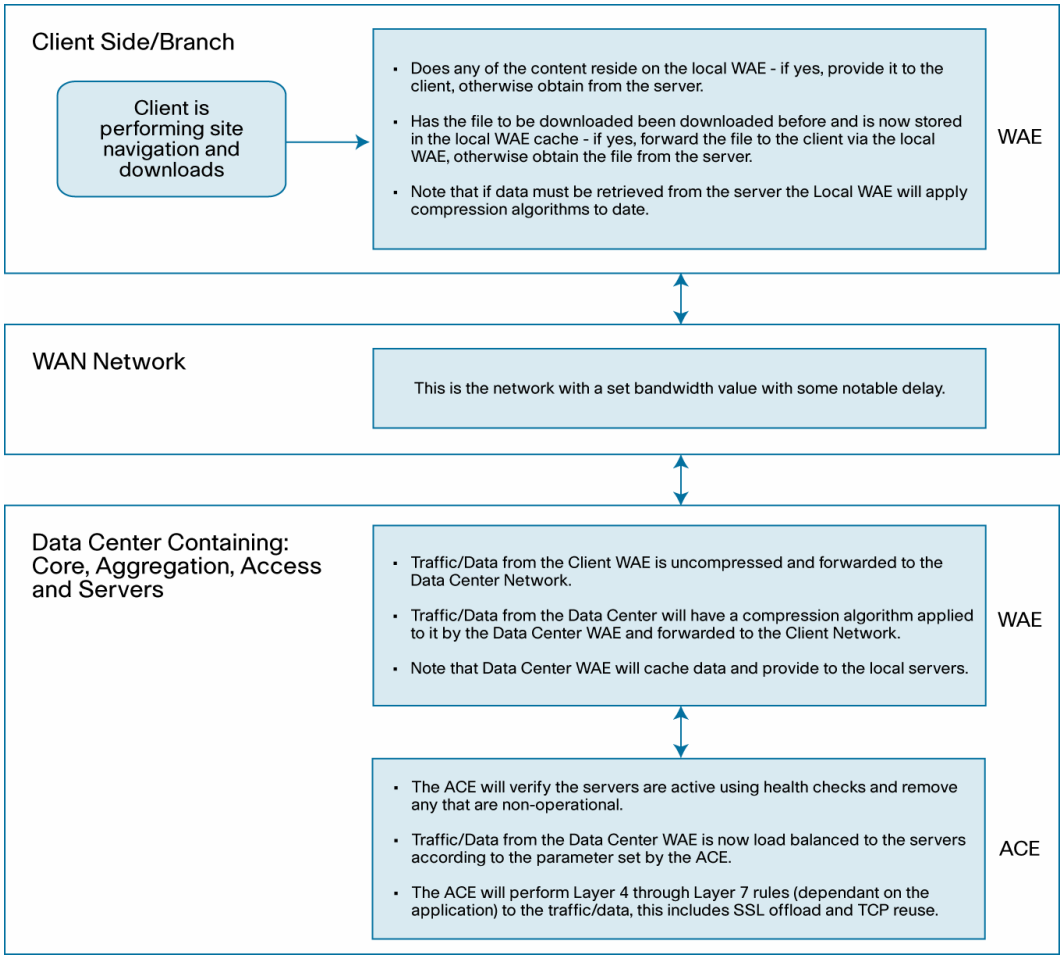
To provide a realistic WAN-like scenario for the solution test, a WAN bridge was used. The WAN simulator provided simulations of the following WAN links:

- WAN Type 1 T1
  - Bandwidth: 1.544 Mbps
  - Delay: 100 milliseconds (ms)
- WAN Type 2
  - Bandwidth: 10 Mbps
  - Delay: 50 ms

Process Flow with Cisco WAAS and Cisco ACE

Figure 7 shows the process in which data flows when Cisco ACE and Cisco WAAS are connected in the network.

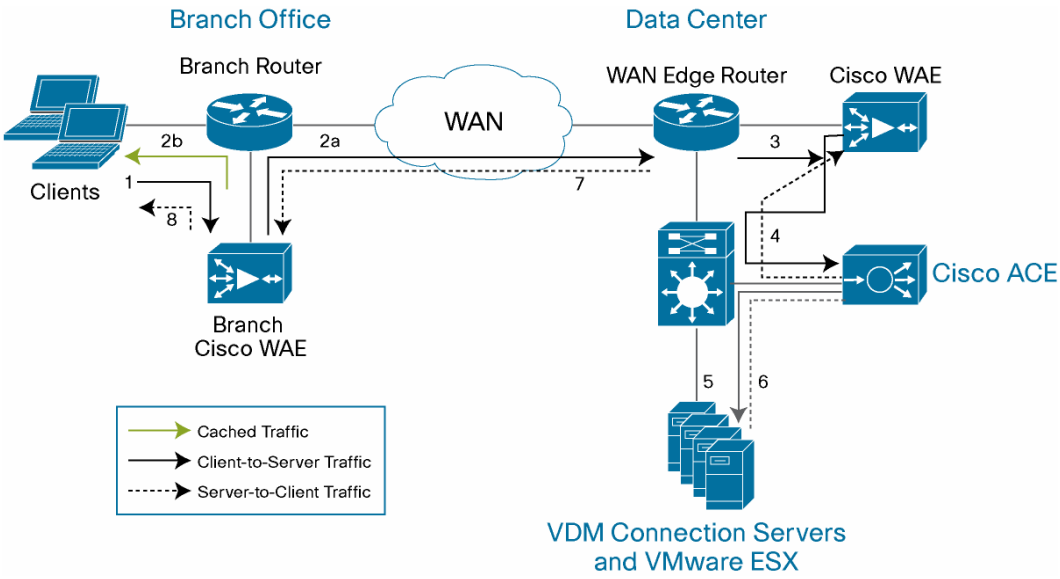
Figure 7. Cisco WAAS and Cisco ACE Process Flow



Packet Flow with Cisco WAAS and Cisco ACE

Figure 8 shows the sequence for the handshake between a client and the VMware ESX Servers and the data transfer phase.

Figure 8. Cisco WAAS and Cisco ACE Packet Flow



The following sequence describes the handshake between a client and the VMware ESX Servers and the data transfer phase:

1. The client sends a TCP synchronize (SYN) packet to the virtual IP address configured on the Cisco ACE for VMware VDM Connection Server load balancing. The packet is forwarded to the branch router. The branch router intercepts the packet with WCCP and forwards it to the branch-office Cisco WAE appliance.
2. The branch-office Cisco WAE applies a new TCP option (0x21) to the packet if the application is identified for optimization by an application classifier. The branch-office Cisco WAE adds its device ID and application policy support to the new TCP option field. This option is examined and understood by other Cisco WAEs in the path as the ID and policy fields of the initial Cisco WAE device. The initial ID and policy fields are not altered by another Cisco WAE. The packet is forwarded to the branch-office router and then to the WAN.
3. During the data transfer phase, if the requested data is in its cache, the branch-office Cisco WAE returns the cached data to the client. Traffic does not travel through the WAN to the server farm. Hence, both the response time and WAN link utilization are improved.
4. The packet arrives on the WAN edge router. The WAN edge router intercepts the packet with WCCP and forwards the packet to the data center Cisco WAE.
5. The data center Cisco WAE inspects the packet. Finding that the first device ID and policy is populated, it updates the last device ID field (the first device ID and policy parameters are unchanged). The data center Cisco WAE forwards the packet to the WAN edge router. The edge router forwards the packet to the aggregation switch, and the aggregation switch then forwards it to the Cisco ACE. The Cisco ACE load balances the connection on one of the VMware VDM Connection Servers in the server farm.

The following steps are for reverse traffic flow.

6. The VMware VDM Connection Server sends the SYN/ACK packet back to the client with no TCP option. The packet from the server is matched by a policy-based routing (PBR) rule on the aggregation switch and forwarded to the Cisco ACE and then to the WAN edge router. The WAN edge router forwards the packet to the data center Cisco WAE. The data center Cisco WAE marks the packet with TCP option 0x21. During the data transfer phase, the data center Cisco WAE caches the data if the data is not in its cache.
7. The data center Cisco WAE sends the packet to the WAN edge router.
8. The packet travels through the WAN and arrives at the branch-office router. The branch-office router intercepts the packet and forwards it to the branch-office Cisco WAE. The branch-office Cisco WAE is aware of the Cisco WAE in the data center because the SYN/ACK TCP option 0x21 contains an ID and application policy. Autonegotiation of the policy occurs as the branch-office Cisco WAE compares its application-specific policy to that of its remote peer defined in the TCP option. At this point, the data center Cisco WAE and branch-office Cisco WAE have determined the application optimizations to apply on this specific TCP flow. During the data transfer phase, the branch-office Cisco WAE caches the data if the data is not in its cache.
9. The packet is forwarded to the branch-office router and then to the VMware VDI client.

Implementing and Configuring the Cisco WAAS Solution

Implementation Overview

The Cisco WAAS solution requires a minimum of three Cisco WAE appliances to autodiscover and deliver applicable application optimizations. One Cisco WAE is placed in the enterprise data center and the other at the branch-office site. The enterprise data center Cisco WAE is placed on the WAN edge connected to the WAN router. The third Cisco WAE is used as the central manager. The architecture offloads the Cisco WAE device from the local branch-office router and uses the available ports on a local switch. This design provides scalability and availability for the solution.

Network Integration

Cisco WAAS technology requires the efficient and predictable interception of application traffic to produce results. It is critical that the Cisco WAE device see the entire TCP conversation. At the WAN edge, Cisco routers support the following four methods of traffic interception:

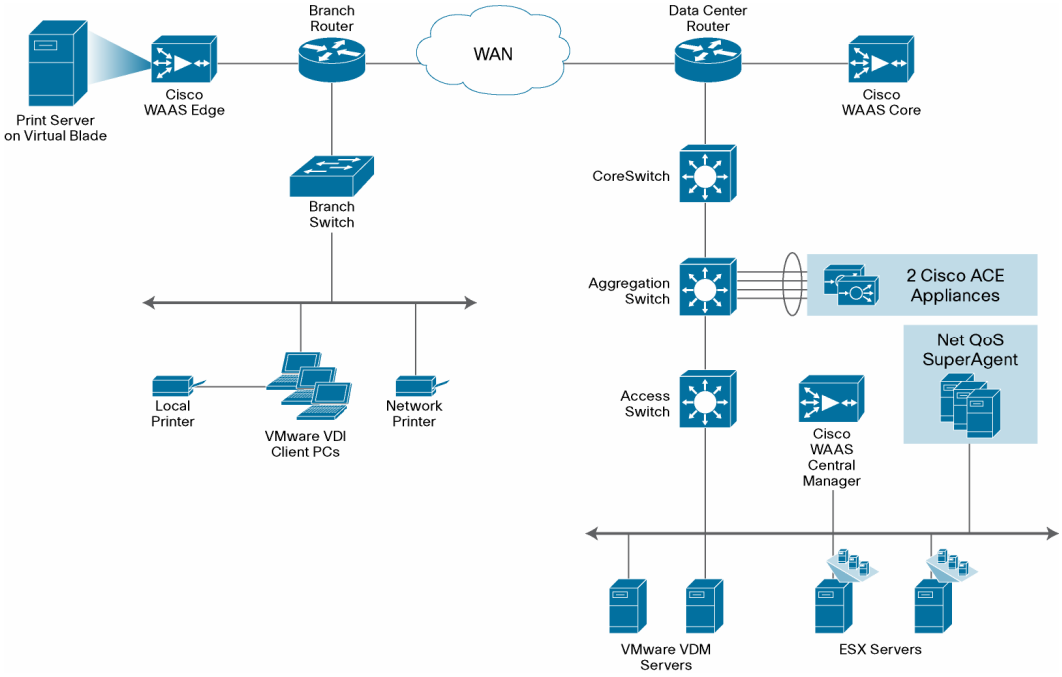
- Inline hardware
- WCCP Version 2
- Service policy with Cisco ACE
- PBR

WCCPv2 is the most common method used in the remote branch-office environment; therefore, WCCPv2 has been used for this solution.

Network Topology

Figure 9 shows the network topology used in this solution.

Figure 9. Network Topology for Cisco WAAS Solution



Hardware

- Cisco WAE-674-K9
- Cisco WAE-7341-K9
- Cisco WAE-612-K9

Software

- Cisco WAAS Software Version 4.1.1

Features, Services, and Application Design Considerations

The VMware VDI solution uses port 80 to send RDP connections from VMware VDI client machines to virtual machines. In the context of Cisco WAAS, port 80 is accelerated by default; no further configuration in the Cisco WAE is necessary unless the application requires ports that are not part of the default application profile. For applications that use TCP ports that are not defined in the default application profile, you must define ports in the existing application profile or create a new application profile with the associated ports.

With the recommended design of Cisco WAAS at the WAN edge, client data traverses the Cisco WAEs only once, at ingress or egress to the data center. The VMware VDM connection broker and virtual machines are in the data center, and communication between them stays in the data center network.

TFO, DRE, and LZ compression, the three main technologies of Cisco WAAS, are enabled by default. Each of these features is described in the “Cisco Wide Area Application Services” overview section earlier in this document. The net results are reduced traffic and decreased latency across the WAN. Since Cisco WAAS deployments are transparent to the network and application, applications do not need to be aware of the added functions and continue to work as-is, but with decreased response time and increased traffic throughput and transactions.

Scalability and Capacity Planning

Cisco WAE farms can scale up to 32 devices with WCCP and up to 16,000 with Cisco ACE load balancing. Cisco WAAS services scale linearly in an N+1 configuration. In addition to the maximum optimized TCP connections, the fan-out ratio between the data center Cisco WAE and branch-office Cisco WAE must be considered. The fan-out ratio is determined by several factors, such as the number of Cisco WAEs in the branch offices, the amount of network traffic, and the number of TCP connections. A sizing tool is available internally that can help automate sizing decisions. NetFlow, NetQoS, and other network analysis tools can provide additional traffic flow information for increased accuracy in scalability and capacity planning.

High Availability

Device High Availability

Cisco WAAS deployments are transparent to the application. The application client and server do not know that Cisco WAAS is optimizing traffic flows. High availability is built into the WCCP interception. If WCCP is not active or if Cisco WAAS devices are not functioning, WCCP does not forward traffic to the Cisco WAEs, resulting in unoptimized traffic flows: the worst-case scenario, where traffic flow continues but is not optimized.

N+1 Availability

Cisco WAEs and the network provide additional high-availability capabilities. Routers can be configured redundantly, providing Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) services. Cisco WAEs can be configured in an N+1 configuration, which provides scalability and availability. This design calls for N number of Cisco WAEs for a specific workload and then a standby Cisco WAE. Because the workload is always distributed evenly among the Cisco WAEs, the standby Cisco WAE is used, reducing the overall workload. If a Cisco WAE fails, the rest of the Cisco WAEs continue with the normal workload.

Configuration Tasks

Each Cisco WAE appliance can be configured either as an application accelerator or a central manager. As a best practice, Cisco recommends deploying a primary and a standby central manager. These devices will configure all other WAE devices on the network. Application accelerators are placed at the core and edge sites, and these devices perform the actual WAN acceleration.

The devices must be activated on the network in a specific order:

1. Configure the primary central manager on the network.
2. Configure the standby central manager on the network.
3. Configure the application accelerators.

After an application accelerator is configured on the network, it will then register with the central manager. With the central manager set up first, this registration will be successful.

Detailed Configuration Overview

Two types of configuration are applied to devices running Cisco WAAS:

- Base configuration
- Central manager configuration

The base configuration is the first configuration that is applied to each Cisco WAE through the console port using the command-line interface (CLI). The base configuration contains the minimum configuration settings to bring up the Cisco WAE on the network and register it with the central manager. The following information is configured on each Cisco WAE as part of the base configuration:

- Hostname
- Interface settings (speed, duplex, IP address, and subnet mask)
- Default gateway
- Domain name
- Domain Name Servers (DNSs)
- Primary interface
- Central manager address

After the base configuration is complete, the Cisco WAE can be registered with the central manager. Registration with the central manager requires that all base configuration steps be complete and that the Cisco WAE is able to connect to the central manager. After the Cisco WAE has been registered and activated with the central manager, all additional configuration options can be set through the central manager device groups.

The central manager configuration provides the remaining configuration for the entire Cisco WAAS deployment. The central manager configuration options can be applied at the device or device group level. To simplify the deployment and management of the Cisco WAAS solution, the solution uses device groups as the primary central manager configuration method.

Configuring the Central Manager

The central manager is the management component of Cisco WAAS. The central manager provides a GUI for configuration, monitoring, and management of multiple branch-office and data center Cisco WAEs. The central manager can scale to support thousands of Cisco WAE devices for large-scale deployments. The central manager is necessary for making any configuration changes through the web interface. In the event of central manager failure, Cisco WAEs continue to function; however, changes cannot be made using the webpages on the central manager until the central manager comes back online.

Cisco WAEs need to connect to the central manager at the initial setup. The registration process adds the Cisco WAE to the central manager and initializes the local Cisco WAE database. When disk encryption on the Cisco WAE is enabled, the central manager must be available to distribute the encryption key in the event that the Cisco WAE reboots.

Centralized reporting can be obtained from the central manager. Individually, the Cisco WAEs provide basic statistics through the CLI and local-device GUI. Systemwide application statistics are available from the central manager GUI. Detailed reports such as total traffic reduction, application mix, and pass-through traffic can be obtained from the central manager GUI.

The following example shows the configuration steps needed to configure the central manager for Cisco WAAS.

Note: At least one Cisco WAE must be the central manager. Adding backup central managers increases availability. Central managers should be installed in the data center with other critical servers, not near the branch-office- or WAN-facing segments.

Step 1. Configure the device to be the central manager. This device is set to application-accelerator mode by default.

```
device mode central-manager
```

Step 2. Configure the central manager IP address:

```
interface GigabitEthernet 1/0
ip address 192.168.1.3 255.255.255.0
```

Step 3. Set up the default gateway:

```
ip default-gateway 192.168.1.1
```

Step 4. Set the primary interface. Cisco WAAS supports multiple network interface types, PortChannels, and standby interfaces. Cisco WAAS uses the primary interface for traffic interception and delivery. The primary interface must defined.

```
primary-interface GigabitEthernet 1/0
```

Step 5. Define the Network Time Protocol (NTP) server. Traffic statistics are captured and forwarded to the central manager and NetQoS. The time stamp on each packet needs to be accurate. All Cisco WAEs and routers should synchronize to the same NTP server.

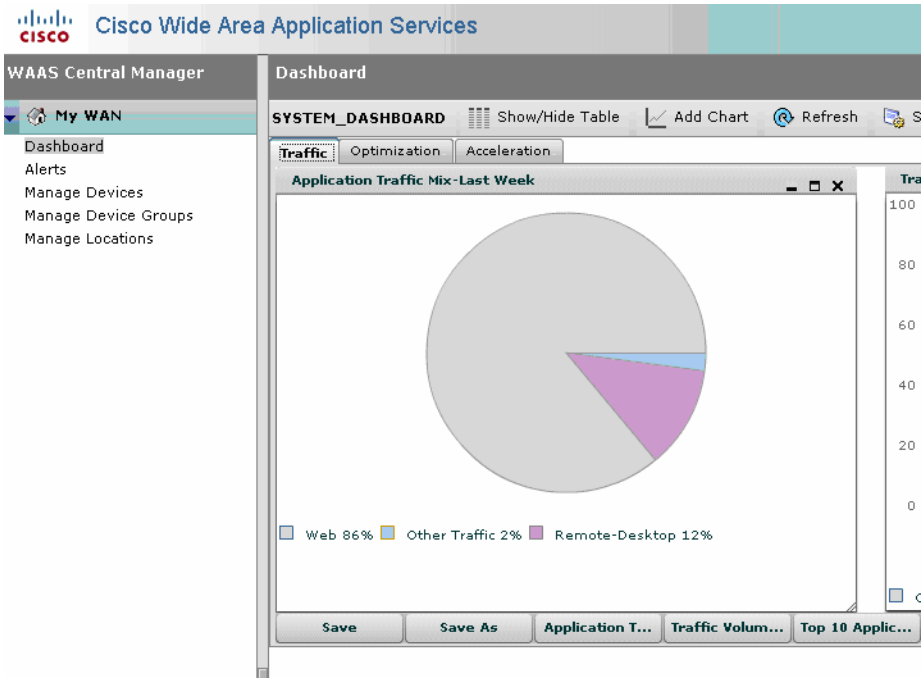
```
ntp server 192.168.1.20
```

Step 6. Initialize the CMS database. The CMS database contains configuration rules and information. The central manager is the repository of CMS data.

```
cms enable
```

Step 7. After the central manager is up and running, log in to the central manager web GUI on port 8443. The initial central manager screen is an overview of the health of the system. It contains information about the number of devices, status, application traffic, and optimization rate (Figure 10).

Figure 10. Cisco WAAS Central Manager Management Console



Configuring the Branch-Office and Data Center Router

The branch and data center router provides WCCP interception points for Cisco WAAS. WCCP redirection allows the router to redirect traffic to Cisco WAAS for optimization. Different methods of interception and redirection are supported by routers and switches. Redirection methods depend on the speed requirements and the router or switch platform. This deployment uses Generic Router Encapsulation (GRE) redirection.

The loopback interface on the router is essential for identifying the router ID. While any IP address can be used to identify the router ID, the loopback interface is preferred over the physical interfaces. Loopback interfaces are always available; there are no physical ties to them. Other routing protocols also use loopback interfaces as the preferred method for naming the router ID. With the IP address tied to a specific physical interface, if the physical interface fails, the IP address becomes unavailable, causing unexpected problems for WCCP groups.

The following example shows the steps for configuring the branch-office and data center routers.

Step 1. Configure the loopback interface:

```
interface Loopback0
ip address 10.1.6.21 255.255.255.255
```

WCCP service 61 and 62 direct the router to reroute traffic from the interface to the WCCP group. Service 61 redirects ingress traffic, and service 62 redirects egress traffic. Services 61 and 62 are both needed to redirect bidirectional traffic flow. WCCP is an open standard. Other equipment that implements the WCCP protocol can participate in the WCCP group. Passwords should be assigned to WCCP groups to prevent rogue traffic interception and redirection.

Step 2. Configure WCCP services 61 and 62 with a password:

```
ip wccp 61
ip wccp 62
```

Step 3. Configure the Cisco WAE VLAN. The Cisco WAE needs to reside in its own subnet for WCCP interception:

```
interface Vlan301
description WAE vlan - 301
ip address 10.1.12.1 255.255.255.0
```

Step 4. Exclude the WAE subnet from interception since this configuration uses a single interface to intercept incoming and outgoing packets. The interception exclusion is required because the router does not differentiate between traffic from the Cisco WAE for the client or server. Traffic from the Cisco WAE should not be redirected again by the router as this will create a loop.

```
ip wccp redirect exclude in
```

Step 5. Enable the NetFlow collection for outgoing traffic from the Cisco WAEs:

```
ip flow egress
```

Step 6. Assign the Cisco WAE VLAN to a physical port:

```
interface FastEthernet1/0
description WAE port
switchport access vlan 301
```

Step 7. Configure the client VLAN. This is the VLAN or interface for WCCP

```
interception:
  interface Vlan300
  description client vlan - 300
  ip address 10.1.11.1 255.255.255.0
```

Step 8. Configure WCCP interception services 61 and 62 on the client VLAN. All ingress and egress packets from this VLAN or interface are forwarded to the Cisco WAE for optimization.

```
ip wccp 61 redirect in
ip wccp 62 redirect out
```

Step 9. Configure NetFlow statistics for all outbound traffic:

```
ip flow egress
```

Step 10. Configure NTP to synchronize with a master clock. Traffic statistics are captured and forwarded to the central manager and NetQoS. The time stamp on each packet must be accurate. All Cisco WAEs and routers should synchronize with the same NTP server.

```
ntp server 192.168.1.20
```

Step 11. Configure NetFlow to send information to the collector. Notice that NetFlow also uses the loopback interface as the source address. NetFlow sends statistics from the Cisco WAE and router to the NetFlow aggregator. NetFlow statistics can be overwhelming for smaller connections so Cisco WAAS should optimize NetFlow transfers.

```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 192.168.1.163 9995
```

Configuring the Branch-Office and Data Center Cisco WAE

Follow these steps to configure the Cisco WAE-674-K9 for the branch office and data center.

Step 1. Set the device mode to application-accelerator. The Cisco WAE can be set up as an application accelerator or central manager. By default, application-accelerator is enabled.

```
device mode application-accelerator
```

Step 2. Configure the Cisco WAE IP addresses:

```
interface GigabitEthernet 1/0
ip address 10.10.105.3 255.255.255.0
```

Step 3. Set up the default gateway:

```
ip default-gateway 10.10.105.1
```

Step 4. Set up the primary interface. Cisco WAAS supports many type of interfaces, including local network failover. You must designate a primary interface. Cisco WAAS uses this interface for interception and redirection.

```
primary-interface GigabitEthernet 1/0
```

Step 5. Turn on WCCPv2:

```
wccp version 2
```

Step 6. Add the router to the router list:

```
wccp router-list 1 10.10.105.1
```

Step 7. Set up TCP promiscuous mode to accept all traffic from the interface. The WCCP password is the same for all devices in the WCCP group, including routers.

```
wccp tcp-promiscuous router-list-num 1 password cisco
```

Step 8. Set up the NTP server. Traffic statistics are captured and forwarded to the central manager and NetQoS. The time stamp on each packet must be accurate. All Cisco WAEs and routers should synchronize with the same NTP server.

```
ntp server 192.168.1.20
```

Step 9. Set up the central manager address. The Cisco WAE needs to register with the central manager for statistics reporting and management. Configurations on a per-device basis can be perform by the CLI and device GUI. Sitewide or Cisco WAAS group configurations must be performed by the central manager. The central manager can run operations on thousands of Cisco WAEs at once, saving considerable time in managing the Cisco WAAS infrastructure.

```
central-manager address 192.168.1.3
```

Step 10. Enable CMS. This command initializes the local database and connects to the central manager:

```
cms enable
```

Step 11. Set up NetFlow to send Cisco WAAS statistics to the NetFlow aggregator. Notice that the host IP address is not the NetFlow aggregator, but the management station. The management station opens another connection to the Cisco WAE to inform the IP address of the aggregator.

```
flow monitor tcpstat-v1 host 192.168.1.164
flow monitor tcpstat-v1 enable
```

Configuration and Menus

See Appendix A for the Cisco WAE configuration.

Troubleshooting the Configuration

You can use show commands to help troubleshoot problems with the configuration.

Cisco WAE Commands

- **sh wccp status:** Verifies that WCCP V2 is enabled.
- **sh wccp services:** Verifies that WCCP services 61 and 62 are active. Services 61 and 62 must be active.
- **sh wccp routers:** Verifies that the router can see the Cisco WAE. Notice that the router ID is the router loopback address. Sent To is the router interface on the Cisco WAE VLAN. All routers are defined and visible on the Cisco WAE.
- **sh stat connection optimized:** Verifies that Cisco WAAS clients are using Cisco WAAS for connectivity. Show TFO Connections shows all optimized paths in the Cisco WAE. The Policy field indicates the optimization method that is active for the specified link. F shows that the link is fully optimized; optimization includes DRE, TFO (shown as TCP Optimization), and LZ compression. Pass-through connections are connections that are not optimized.

- **sh statistics connection dre:** Checks DRE use. The statistics have two sections. The Encode section shows traffic coming into the Cisco WAE from the client or server; the Cisco WAE needs to compress the incoming traffic with LZ compression and then apply DRE. The Decode section shows traffic coming from the peering Cisco WAE; DRE lookup is performed and traffic uncompressed. These statistics are useful for determining the compressibility of the data.

Router Commands

- **sh ip wccp 61:** Verifies that WCCP services 61 and 62 are active. This command shows global WCCP information and how the packets are redirected. Redirect and group access list problems are easier to troubleshoot with this output. Service 62 should also check with sh ip wccp 62.
- **sh ip wccp 61 detail:** Checks WCCP client hash or Layer 2 assignments. This command also checks the status of the WCCP client: the Cisco WAEs. The sh ip wccp 61 command shows global WCCP information; this command shows detailed WCCP client information. The output includes hashing assignments (Cisco WAE bucket assignments), client ID, and client status.
- **sh ip wccp interface detail:** Verifies which interface has WCCP configured. This command identifies all interfaces within a router or switch that have WCCP configured with ingress or egress for exclude-in redirection. Another way to get this information is with sh run. Examine each interface.
- **sh ip wccp 61 view:** Verifies WCCP group membership. This command also checks service 62.

Implementing and Configuring the Cisco ACE Solution

Implementation Overview

Cisco ACE is deployed at the aggregation layer in the data center using the 1-ARM design; a minimum of two Cisco ACE 4710 appliances are required. Cisco ACE 4710 appliances are connected to Cisco Catalyst® 6500 Series Switches in the aggregation layer using a PortChannel and are enabled for high availability. The Cisco ACE 4710 appliances are not inline to the traffic flow and use VLAN 169 to connect to the aggregation switches. The Cisco ACE 4710 appliances load balance connections to the VMware VDM Connection Servers and provide session persistence.

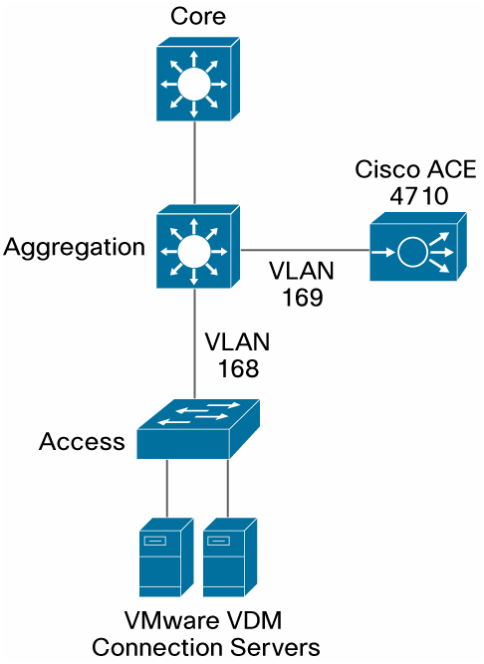
The main features implemented on the Cisco ACE appliance for this solution are:

- Load balancing of VMware VDM Connection Servers
- Health monitoring of VMware VDM Connection Servers
- Session persistence based on client IP address
- High availability

Network Topology

Figure 11 shows the network topology used in this solution.

Figure 11. Network Topology for Cisco ACE Solution



Hardware

Cisco ACE 4710

Software

Cisco ACE Software Version 3.0(0)A3(1.0)

Features, Services, and Application Design Considerations

When a user needs to access a virtual desktop in the data center, the user connects to a virtual IP address configured on the Cisco ACE. The Cisco ACE periodically checks the health of the VMware VDM application by querying the URL of the application and applying a regular expression to the retrieved results. Using this probe information, the Cisco ACE determines the VMware VDM Connection Server that can service the user request with the best performance and availability. Then the Cisco ACE forwards the request from the user to the VMware VDM Connection Server.

Cisco ACE supports several session persistence mechanisms between the client and the VMware VDM Connection Server so that a particular client session is always directed to the same server. In this topology, the Cisco ACE appliance is configured to perform session persistence based on the client IP address.

To provide high availability, the Cisco ACE is deployed in a stateful redundant active-standby design. The Cisco ACE replicates both connection and persistence information to the standby device and provides instant application service failover.

Cisco ACE Configuration

Admin Context Configuration

The Admin context is used to configure the following:

- Physical interfaces
- Management access
- Virtual context for load balancing VMware VDM Connection Servers
- High availability

Configuring Physical Interfaces

The Cisco ACE appliance interacts with clients and servers through VLANs that are set up in the Cisco Catalyst switch. These VLANs must be configured on the physical interfaces of the Cisco ACE. Without this configuration, by default the Cisco ACE will not process any traffic received from the switch.

Configure the Cisco ACE appliance physical interfaces in a PortChannel and set up the required VLANs as follows:

```
interface gigabitEthernet 1/1
  channel-group 200
  no shutdown
interface gigabitEthernet 1/2
  channel-group 200
  no shutdown
interface gigabitEthernet 1/3
  channel-group 200
  no shutdown
interface gigabitEthernet 1/4
  channel-group 200
  no shutdown
interface port-channel 200
  ft-port vlan 170
  switchport trunk allowed vlan 168-169
  port-channel load-balance src-dst-port
  no shutdown
```

Configuring Remote Management Access

To access the Cisco ACE remotely using Telnet, Secure Shell (SSH), Simple Network Management Protocol (SNMP), HTTP, or HTTPS or to allow Internet Control Message Protocol (ICMP) access to the Cisco ACE, a policy must be defined and applied to the interfaces that the access is entering.

The configuration steps in this section are required for both the Admin context and the VMware VDI context. The following example is for the Admin context.

Step 1. Configure a class map of type management:

```
class-map type management match-any REMOTE-MGMT
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
50 match protocol https any
```

Step 2. Configure a policy map of type management and invoke the management class map:

```
policy-map type management first-match REMOTE-ACCESS
  class REMOTE-MGMT
    permit
```

Step 3. Configure the IP address for the VLAN interface and a default gateway.

```
interface vlan 168
  ip address 192.168.1.40 255.255.255.0
  alias 192.168.1.41 255.255.255.0
  peer ip address 192.168.1.42 255.255.255.0
  no normalization
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Step 4. Apply the policy map to the VLAN interfaces:

```
interface vlan 168
  service-policy input REMOTE-MGMT
```

Configuring the Virtual Context for VMware VDI

Typically, when Cisco ACE is deployed, the Admin context is used for managing and provisioning other virtual contexts. In this design, a virtual context named VMware VDI is created for VMware VDM Connection Server load balancing.

Configure the virtual context and associate it with a resource class as follows:

```
resource-class STICKY
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
context VDI
  allocate-interface vlan 169
  member STICKY
```

Configuring Redundancy and High Availability

To provide high availability and redundancy, Cisco ACE can be set up and configured in a redundant mode. Cisco ACE can be configured in a typical active-backup redundancy mode or active-active (per context) redundancy mode.

Configure high availability as follows:

```
ft interface vlan 170
  ip address 192.170.1.1 255.255.255.0
  peer ip address 192.170.1.2 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
```

```
    heartbeat count 10
    ft-interface vlan 170
  ft group 1
    peer 1
    no preempt
    priority 200
    associate-context Admin
    inservice
  ft group 2
    peer 1
    no preempt
    priority 200
    associate-context VDI
    inservice
```

VMware VDI Context Configuration

Configuring the VLAN Interface, Routing, and Access List

Step 1. Configure the VLAN interface and a default static route with the IP address of VLAN 169 on the aggregation switch as the next hop:

```
interface vlan 169
  ip address 192.169.1.4 255.255.255.0
  alias 192.169.1.1 255.255.255.0
  peer ip address 192.169.1.5 255.255.255.0
  no normalization
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.169.1.2
```

Step 2. Configure an access list to permit IP traffic and apply it to the VLAN interface:

```
access-list 102 line 8 extended permit tcp any any eq www
access-list 102 line 24 extended permit icmp any any
interface vlan 169
  access-group input 102
```

Configuring the Real Servers and Server Farm

Step 1. Configure the real servers on the Cisco ACE is shown in this example:

```
rserver host CB1
  ip address 192.168.1.80
  inservice
rserver host CB2
  ip address 192.168.1.81
  inservice
```

Step 2. Configure a server farm and add the real servers under the server farm:

```
serverfarm host VDM_CB
  rserver CB1
    inservice
  rserver CB2
    inservice
```

Configuring Health Monitoring for VDM Connection Servers

Cisco ACE supports several health monitoring probes to determine the availability of the servers.

Step 1. To monitor the application running on the VMware VDM Connection Servers, use the following HTTP probe:

```
probe http VDM_PROBE
  interval 5
  faildetect 2
  passdetect interval 5
  passdetect count 2
  request method get url /admin/
  expect status 200 200
  open 1
  expect regex "VDM Administrator"
```

Step 2. Apply the health probe to the server farm to start monitoring the VMware VDM Connection Servers:

```
serverfarm host VDM_CB
  probe VDM_PROBE
```

Configuring the Load-Balancing Algorithm

Cisco ACE provides several load-balancing algorithms to distribute loads among the VMware VDM Connection Servers intelligently. In this design, the Least-Loaded algorithm is configured for the server farm. The Cisco ACE will load balance new connections to the VMware VDM Connection Server that has the fewest number of open connections.

```
serverfarm host VDM_CB
   predictor leastconns
```

Configuring Load-Balancing Policy

The Cisco ACE uses class maps, policy maps, and service policy to classify, enforce, and take action on incoming traffic. The following steps are needed to configure the load-balancing policy.

Step 1. Configure a Layer 3 or 4 class with a virtual IP address that listens on port 80:

```
class-map match-all VDM_VIP_80
  2 match virtual-address 192.169.1.254 tcp eq www
```

Step 2. Configure a sticky group that performs persistence based on the source IP address and assign the VMware VDM Connection Server server farm to it:

```
sticky ip-netmask 255.255.255.255 address source VDM_IP_STICKY
  timeout 10
  replicate sticky
serverfarm VDM_CB
```

Step 3. Configure a load-balancing policy and enable load balancing for the sticky server farm created earlier:

```
policy-map type loadbalance first-match VDM_LB
  class class-default
    sticky-serverfarm VDM_IP_STICKY
```

Step 4. Configure a policy map of type multi-match and attach the load balancing to the virtual IP address:

```
policy-map multi-match VM_LB
  class VDM_VIP_80
    loadbalance vip inservice
    loadbalance policy VDM_LB
    loadbalance vip icmp-reply
```

Step 5. Apply the policy map to the interface VLAN 169:

```
interface vlan 169
  service-policy input VM_LB
```

Cisco Catalyst 6500 Multilayer Switch Feature Card PBR Configuration

Since the Cisco ACE appliance is deployed in a 1-ARM design, PBR must be configured on the Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) in the aggregation layer to help ensure that the return traffic from the VMware VDM Connection Servers is sent back to the Cisco ACE appliance.

Step 1. Configure an access list to match the return traffic:

```
ip access-list extended ACE_RETURN
permit tcp any eq www any
```

Step 2. Configure a route map and apply it to the Cisco Catalyst 6500 MSFC VLAN interface on which the return traffic from the VMware VDM Connection Server is seen:

```
route-map VM permit 10
 match ip address ACE_RETURN
 set ip next-hop 192.169.1.1
!
interface Vlan168
 ip policy route-map VM
```

Troubleshooting the Configuration

The following show commands can help troubleshoot problems with the configuration:

- **show stats:** Displays statistics relating to the operation of the Cisco ACE
- **show service-policy policy_name:** Displays statistics for service policies enabled globally within a context or on a specific interface
- **show serverfarm name detail:** Displays summary or detailed server farm statistics
- **show rserver rserver_name detail:** Displays summary or detailed statistics for a named real server or for all real servers
- **show probe:** Displays probe information, including information for script probes
- **show arp:** Displays the current active IP address–to–MAC address mapping in the ARP table, statistics, or inspection or timeout configuration

- **show arp statistics:** Displays the ARP statistics for all VLAN interfaces
- **show context:** Verifies the autosync configuration of all contexts
- **show ft group status:** Verifies the fault-tolerant (FT) status of all configured contexts in the Cisco ACE
- **show ft peer detail:** Verifies the state of FT peering
- **show resource usage:** Displays the resource utilization for each context
- **show np NP_number:** Displays the hardware information stored on the three network processors

Performance Measurement Using NetQoS

This section shows the network monitoring system used to monitor and provide results, demonstrating the benefits of the Cisco WAAS optimization. The tool used to measure network performance was NetQoS SuperAgent with NetQoS Collector and Reporter. NetQoS Collector gathers the preoptimized traffic and reports the data to the NetQoS SuperAgent. NetQoS SuperAgent provides details about the protocols and applications traversing the network, including:

- Response time
- Data transfer time
- Retransmission delay
- Network round-trip time (RTT)
- Effective network RTT
- Performance by the server
- Performance by the network

This information provides the baseline of the application under test with valid overall transaction times (the end-user experience).

NetQoS Reporter gathers the optimized traffic and reports the data to NetQoS SuperAgent. NetQoS SuperAgent uses the data from NetQoS Collector (unoptimized) and compares it to the optimized traffic, indicating the benefits of optimization using Cisco WAAS as shown in the generic samples in Figures 12, 13, and 14.

Figure 12. Benefits of Optimization Using Cisco WAAS: Application Response Time

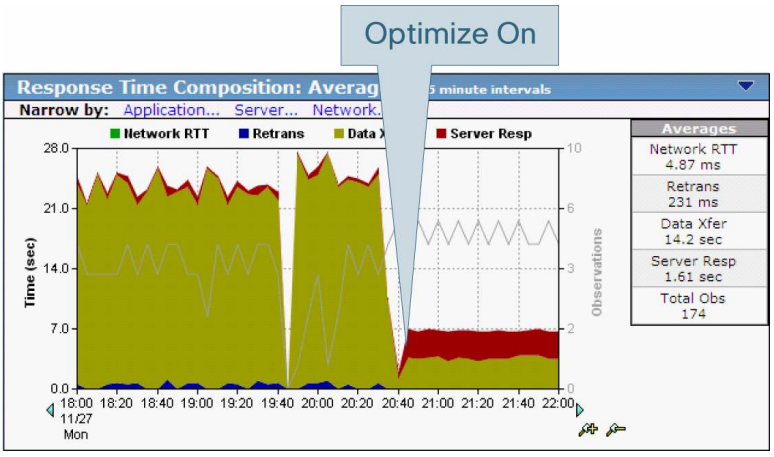


Figure 13. Benefits of Optimization Using Cisco WAAS: Application Data Rate

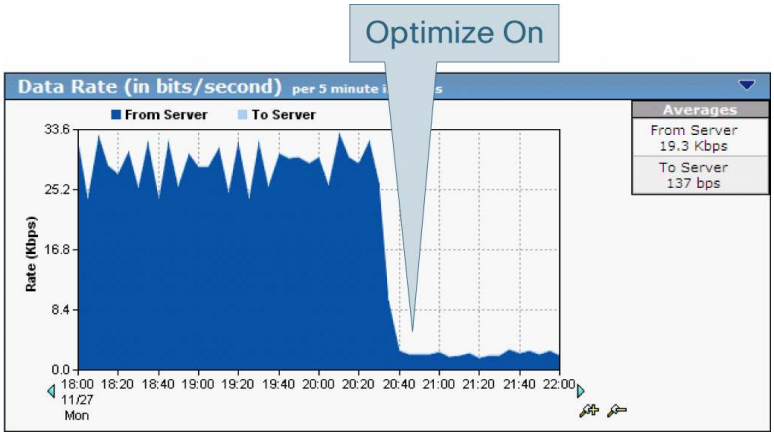
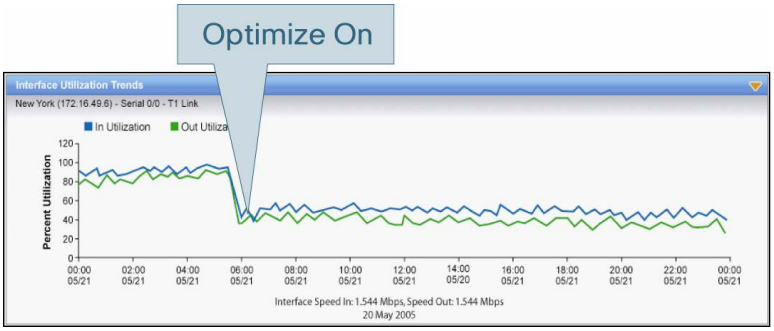


Figure 14. Benefits of Optimization Using Cisco WAAS: Link Utilization



NetQoS devices passively listen in by using the Remote Switched Port Analyzer (RSPAN) feature of Cisco routers and switches. They do not poll servers and hence do not add to the server load.

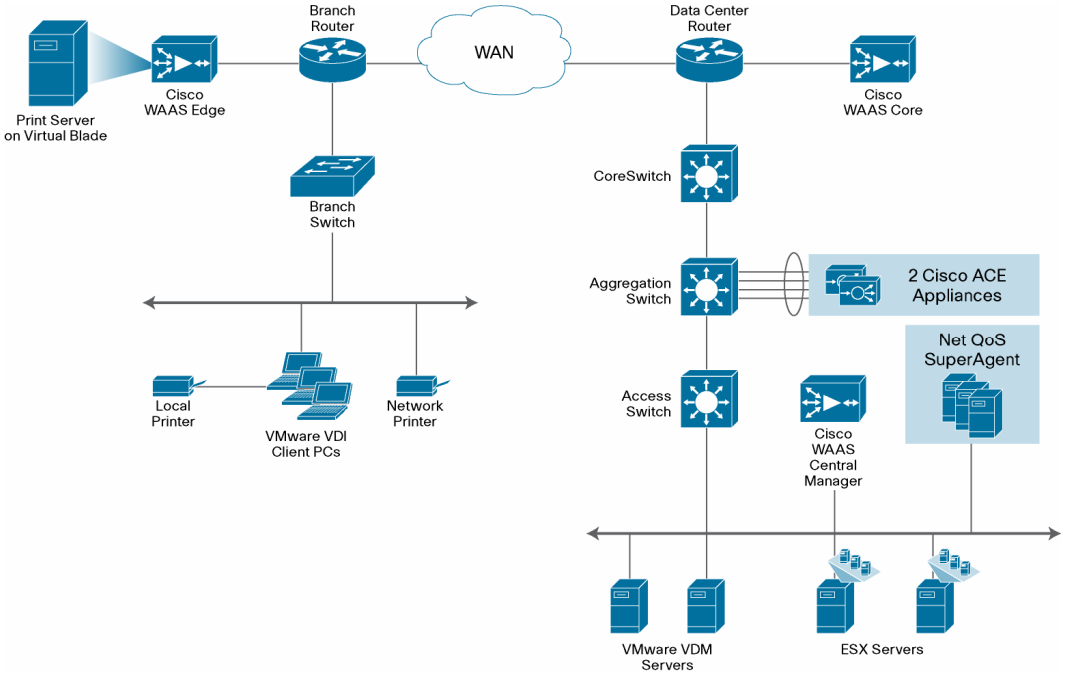
Solution Testing and Results

The following section details the test environment that was used for testing this joint Cisco and VMware solution and provides the results that were obtained.

Test Environment

Cisco and VMware have tested and validated the customer benefits of the joint solution. Figure 15 shows main key components of the test environment.

Figure 15. Test Environment Topology



Test Design

To compare the behavior and performance of an optimized environment to that of the baseline VMware VDI session, several test scenarios and networking environments were tested.

WAN Simulation

The following two WAN settings were used to simulate typical enterprise settings:

- Small branch office with a T1 link (1.5 Mbps) and an RTT of 100 ms
- Regional office with a larger connection of 10 Mbps and an RTT of 50 ms

Test Plan and Procedure

To get a clear understanding of the performance for various types of applications, the following sets of tests were conducted:

- **Internet browsing:** In these tests, several websites were accessed and their pages browses; tests were conducted on a variety of sites ranging in the amount of graphical content and animation.
- **Email and collaboration:** In these tests, using Microsoft Outlook, a corporate mail account was accessed, and several typical activities were tested, such as opening new email messages, including some with attachments; browsing the calendar and contacts; and creating new content.
- **Microsoft Office:** In these tests, Microsoft Office applications were tested by opening various Word, PowerPoint, and Excel documents; viewing presentation slideshows; creating new documents; and viewing the graphs on an Excel spreadsheet.
- **File transfers:** Because users in VMware VDI environments are remote from the files on their desktops, the transfer of files from the virtual desktop to end-user USB drives was tested.

- **Printing:** In VMware VDI environments, printing is conducted over the WAN, regardless of where the print server is located; because the virtual desktop and the printer are separated by the WAN, printing was tested.

Testing Tools and Procedures

In real-life situations, rarely will you have the entire WAN to yourself. In addition, deployments of VMware VDI typically migrate all the users in the branch office to VMware VDI. For these reasons, simulated traffic of additional VMware VDI workers was generated for the tests.

To simulate this traffic, multiple client connections running AutoIT scripts were generated. The operations conducted by the simulated users included all the tests mentioned here with the exception of file transfers and printing.

To increase the realism of the simulated VMware VDI users, several randomizations were introduced:

- Random selection of the test conducted next
- Random selection of the file, site, or email viewed or browsed
- Random selection of whether an operation includes addition of content or just reviewing of content
- Random spacing of the time between operations and suboperations

Configuring Virtual Desktops for Optimization

To optimize the VMware VDI traffic, the underlying protocol's encryption and compression should be disabled. Microsoft RDP is the underlying protocol used by the current version of VMware VDM and is currently the predominant protocol used by the various VMware VDI implementations.

To disable encryption on RDP, the settings on the virtual desktop must be changed. The changes can be made either by group policy settings or by changes to the registry. Both methods can also be distributed to large groups of virtual desktops using Microsoft Active Directory.

To disable compression, the settings on the VMware VDM client must be modified. These can be configured by group policy and thus can easily be deployed to large groups of clients using Microsoft Active Directory

Disabling Compression on the RDP File

To disable compression on the RDP configuration file, follow these steps:

Step 1. Open the RDP connection (.rdp) file in Notepad.

Step 2. Change the line compression:i:1 to compression:i:0.

Step 3. Save the file.

After the change is made, any new connection using the changed file will not use RDP compression.

Configuring VMware VDM to Use Uncompressed RDP Sessions

To configure VMware VDM to use uncompressed RDP sessions, follow these steps:

Step 1. Copy the c:\ Program Files\VMware\VMware VDM\Server\ADM\vdm_client.adm file from the connection broker server to the VMware VDI client PC.

Step 2. Import this file to the group policy object (GPO).

Step 3. In the GPO, choose User Configuration > VMware VDI Client and disable the Enable Compression policy.

Disabling Encryption

The following steps were used to disable encryption on Windows virtual desktops

Registry keys:

- Set HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\MinEncryptionLevel to 1.
- Create HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer as a DWORD value and set it to 0.

Large deployments should use Microsoft Active Directory to push these changes to the virtual desktops.

Note: On Windows XP 32 bit Virtual Desktop Machines, a hot-fix from Microsoft was used to add capability to disable RDP protocol encryption. However, this hot-fix was not required to disable RDP protocol encryption on Windows XP 64-bit and Windows Vista desktops

Test Results and Conclusions

For each metric tested, such as application performance, bandwidth consumed, scalability, and print optimization, baseline measurements using native protocol compression were first established, and these were then compared to performance with Cisco WAAS turned on (and native protocol compression turned off). For every metric tested, Cisco WAAS optimizes the display protocol substantially.

VMware VDI Remote Desktop Performance Results

Traffic Reduction

The traffic reduction tests looked at the overall amount of traffic sent over the WAN and compared the results of a baseline run (with the native encryption and compression enabled).

For each metric tested, such as application performance, bandwidth consumed, scalability, and print optimization, baseline measurements using native protocol compression were first established, and these were then compared to performance with Cisco WAAS turned on (and native protocol compression turned off). For every metric tested, Cisco WAAS optimizes the display protocol substantially.

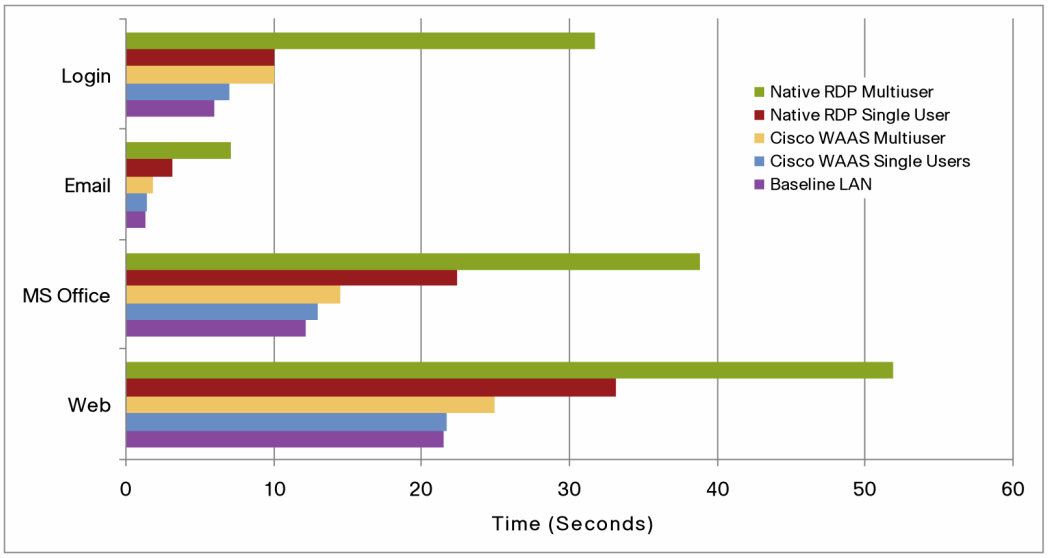
Performance Acceleration

Cisco WAAS improves display protocol performance by 70 percent, providing a near-LAN user experience.

Performance of various applications when using VMware VDI was tested, and the time required to complete tasks such as logging in to the virtual desktop, opening Microsoft Outlook, and viewing a Microsoft PowerPoint slideshow was measured (Figure 16).

- Using Cisco WAAS, the time to complete the tasks of the various applications was reduced by up to 70 percent both when comparing a single user and comparing multiple VMware VDI users.
- The performance achieved by VMware VDI sessions optimized with Cisco WAAS is within a small deviation from LAN performance even when there are additional users on the WAN.

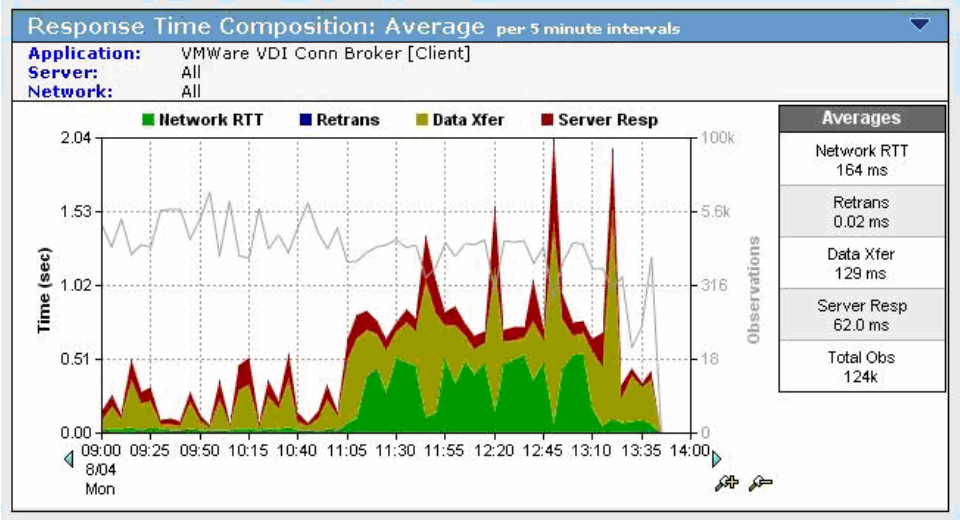
Figure 16. Task completion at 1.5 Mbps upstream and downstream and 100-ms RTT



The aggregate application performance information available from NetQoS, as provided by the NetQoS devices, and the Cisco WAAS integrated SuperAgent was also measured.

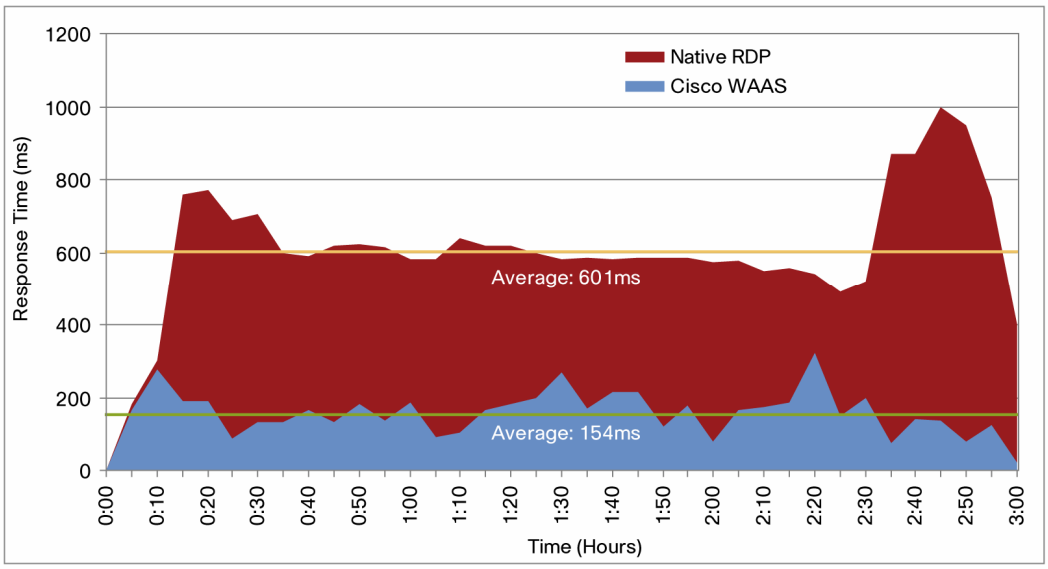
The response time as measured at the VMware VDM Connection Server for a single user was reduced by 4 to 6 times when Cisco WAAS optimization was used (9 a.m. to 11 a.m.) as compared to native VMware VDI (11 a.m. to 1:40 p.m.) (Figure 17).

Figure 17. NetQoS Response-Time Analysis: Single User



The response time measured at the remote branch office during a test of 15 simultaneous VMware VDI sessions shows a 4-times improvement. Cisco WAAS acceleration results in an average response time of 154 ms, and native VMware VDI achieves an average response time of 601 ms (Figure 18).

Figure 18. Response-Time Analysis: Multiuser



Bandwidth Optimization

Cisco WAAS reduces bandwidth demand by 60 to 70 percent, decreasing WAN bandwidth cost.

In the traffic reduction tests, the bandwidth consumed by VMware VDI traffic over the WAN was measured for the baseline with native protocol compression and then compared to tests using Cisco WAAS (Figure 19).

Figure 19. Traffic Reduction in Application Tests

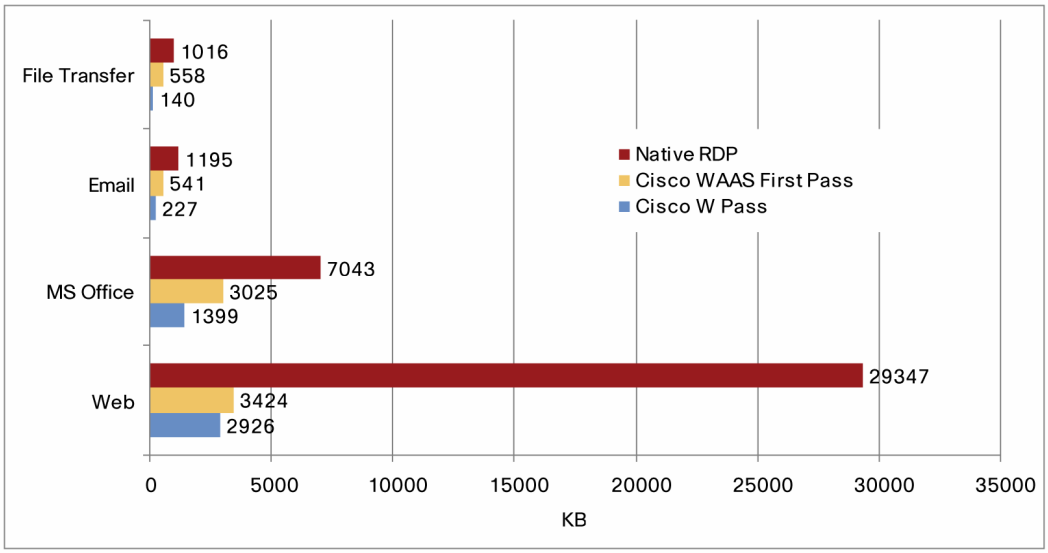
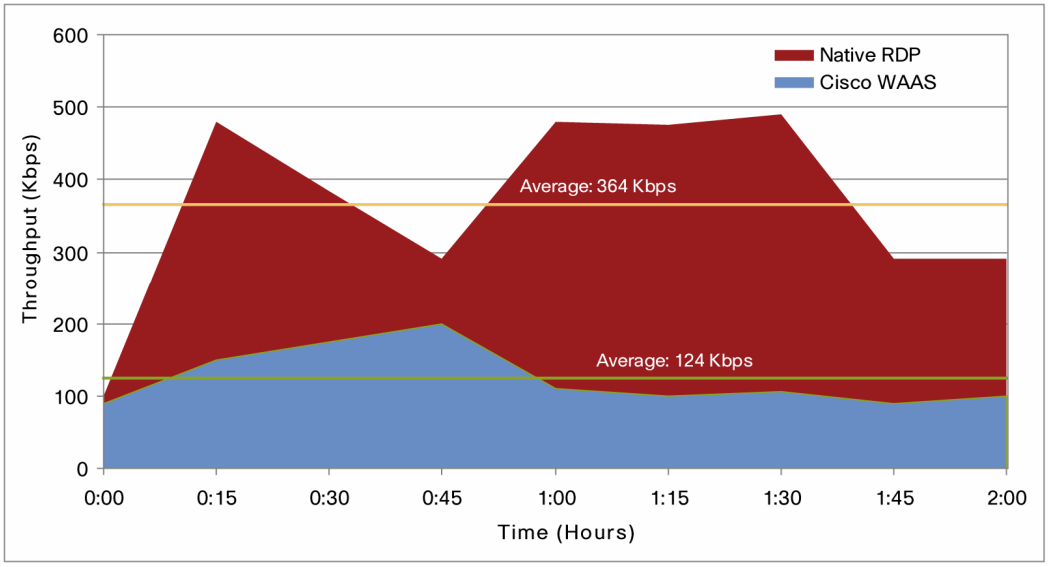


Figure 19 shows the traffic reduction achieved while running the application tests cases. These results show that the traffic reduction ranged from 54 percent to more than 90 percent, with an average reduction of 67 percent in the first pass and 84 percent in the second pass. Note that the file transfer results refer to copying files from the virtual desktop to a detachable drive connected to the client machine.

The traffic generated for a realistic single simulated VMware VDI session for a duration of 2 hours was compared before and after Cisco WAAS optimization. The average bandwidth per simulated session was reduced by 66 percent by using Cisco WAAS (Figure 20).

Figure 20. Two-Hour Simulated User Throughput



The results shown here reflect the superior compression capability of Cisco WAAS DRE, which outperforms the native protocol compression for the entire duration of the testing, and because of the reduction of repetitive data, reaches peaks of more than 90 percent compression.

Scalability of Number of Users

Cisco WAAS increases the number of users that can be supported on a given network by 2 to 4 times.

Cisco WAAS acceleration and data reduction technologies work together to increase the scalability of VMware VDI solutions. RDP tries to adjust to bandwidth and latency constraints by reducing the quality of the session, and as the results of the multiuser tests show, this causes a substantial decline in session quality: up to 10 times worse than the LAN experience (Figures 21 and 22).

Figure 21. Effect of Additional Users on Session Response Time

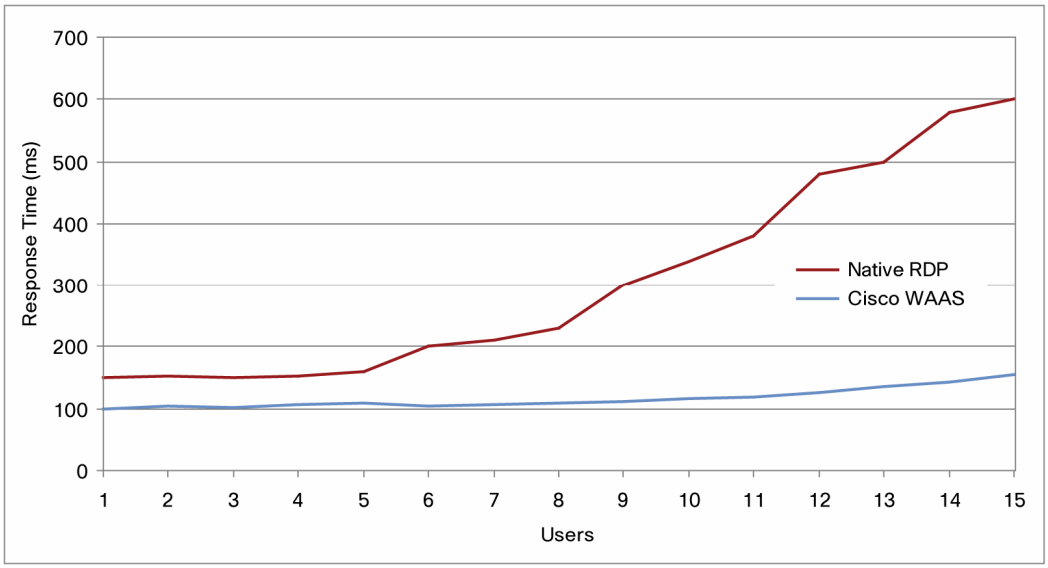
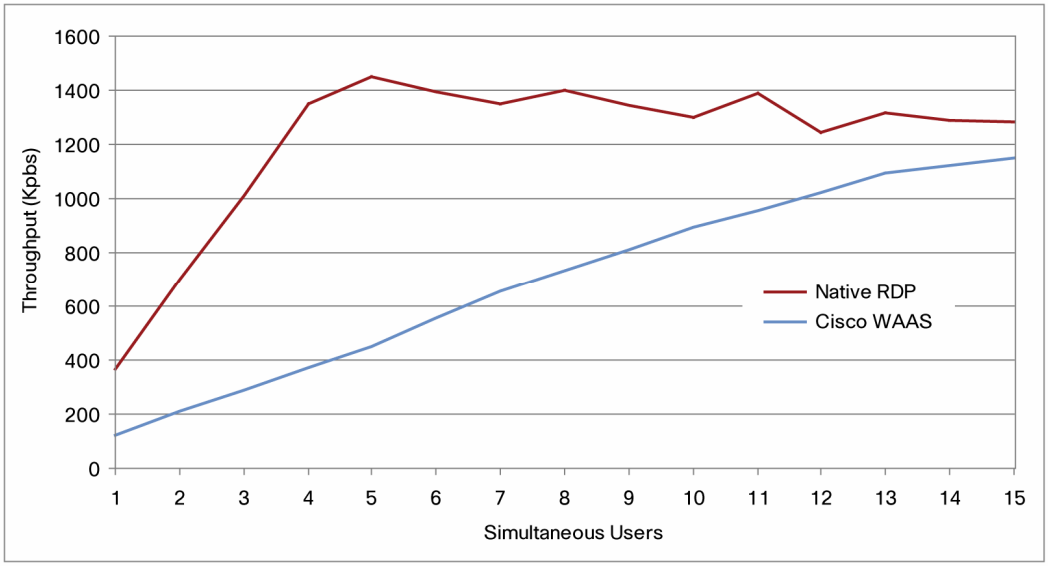


Figure 22. Effect of Additional Users on Throughput



Figures 21 and 22 show the results of the measured response times on the branch-office network and throughput when users are added to a 1.5-Mbps link with a 100-ms RTT.

- With the native protocol, the degradation in session quality starts with as few as six users on the network, and with nine users the system is almost unusable, with a measured response time of nearly 300 ms, or 3 times worse than for a single user over the WAN.
- With Cisco WAAS optimization, users can be added to the network with minimal negative effects, enabling up to 4 times more sessions on the same network with exceptional responsiveness and the same experience as a single user.

- The throughput results may seem counterintuitive, but they actually reflect the poor quality for the native protocol with the increasing number of users. The decreased throughput is due to RDP's built-in algorithms, which reduce session quality. Some of the mechanisms used include reduction in the number of screen refreshes, which tends to produce a work experience that is choppy and not user friendly.

Printing with VMware VDI

Cisco WAAS optimizes printing by 70 percent and provides a branch-office print server option without the need for additional servers.

Even as desktop machines are migrated to the data center, users still need to print on printers located in the remote branch office. Due to the nature of print spools, which can contain as much as 10 times the raw data, printing must be carefully designed in VMware VDI environments. Deployment considerations for printing in VMware VDI environments include:

- **Location of the print server:** The print server (print spooler) can be located at either end of the WAN, either in the remote branch office or in the data center.
- **Method of printing:** Two methods can be used:
  - **Direct printing:** The printer is defined on the virtual desktop and sends the print job directly to the spooler. Depending on the location of the print server, either Common Internet File System (CIFS) or RAW/PostScript printing traffic is sent across the WAN.
  - **RDP printing:** The printer is defined on the client machine and is virtualized by RDP on the virtual desktop. In this scenario, a print job is first sent to the client machine by RDP and then sent by the client computer to the spooler. If the print server is located at the data center, CIFS and RAW/PS print traffic is sent across the wire.

Cisco WAAS provides optimizations for all VMware VDI print environments: centralized and local.

- **Centralized printer:** Cisco WAAS includes printing-specific optimizations, data reduction, compression, and TCP optimizations to provide dramatic improvements.
- **Branch-office print server:** Cisco WAAS provides a virtualized Microsoft Windows print server on the Cisco WAAS appliance, providing a print server in the branch office without the need for additional servers.

Table 2 shows the results of printing a 10-page Microsoft Word document over a T1 line with a latency of 100 ms.

Table 2. Results of Printing a 10-Page Microsoft Word Document

Action	Baseline	With Cisco WAAS
Local printer on client using RDP	**50.1 sec/3.67 MB**	**16.1 sec/1.6 MB**
Data center print server		
RDP printing	287.1 sec/10.8 MB	62.6 sec/1.1 MB
Direct printing	140.1 sec/3.62 MB	94.3 sec/556 KB
Branch-office print server (virtualized Microsoft Windows print server on Cisco WAAS)		
RDP printing	42.5 sec/2.22 MB	22.1 sec/1.53 MB
Direct printing	520.7 sec/20.17 MB	21 sec/546 KB

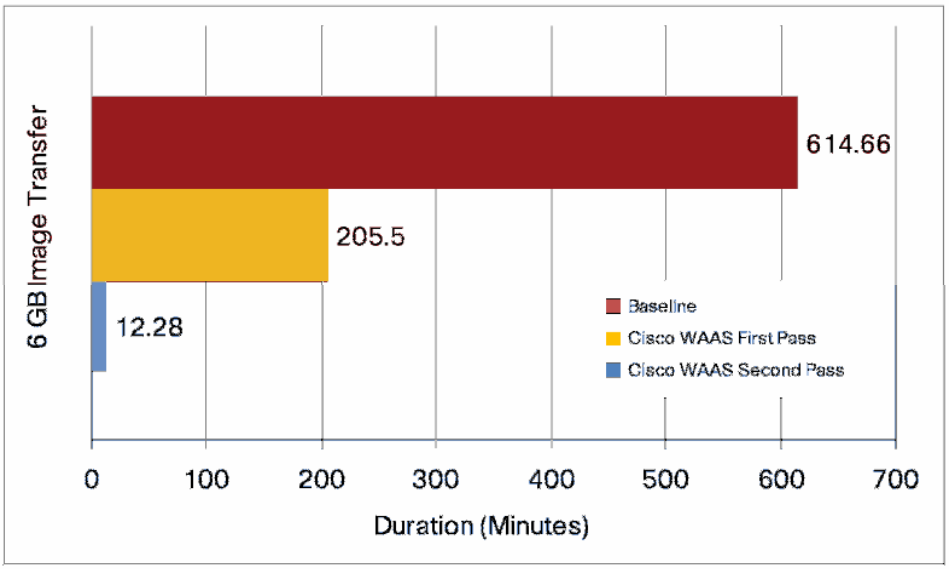
As Table 2 shows, Cisco WAAS greatly enhances the printing experience in every configuration by reducing the amount of bandwidth required to perform the print job, averaging traffic reduction of 70 percent and reaching peaks of 97 percent while also completing the print job 3 to 25 times faster.

Virtual Machine Image Copying Across the WAN

To facilitate enhanced deployments and management of a VMware VDI deployment, virtual machine images must periodically be transferred and backed up across the WAN.

Figure 23 shows the results of transferring a 6-GB virtual machine image for a Microsoft Windows XP desktop using the VMware Network File Copy (NFC) Protocol, achieving a 3-times faster transfer on the first transfer and a 50-times faster transfer on the second transfer.

Figure 23. Image Copying Using VMware NFC Protocol



Copying User Files To and From the Virtual Desktop

VDI users can transfer local files, such as files stored on their USB or CD drives, to the remote virtual desktop. When the local drives are mapped using VMware VDI, the file copy data flows over RDP.

Table 3 shows the user file copy results.

Table 3. File Transfers

	Time		Data		Second Pass	
	Baseline	**Cisco WAAS**	**Baseline**	**Cisco WAAS**	**Time Taken**	**Data over WAN**
Client to virtual desktop	**10.5 seconds**	**10 seconds**	1,054,596 bytes	1,160,398bytes		
Virtual desktop to client	**9 seconds**	**4.2 seconds**	520,544 bytes	281,216 bytes	3 seconds	71,815 bytes

Connections from clients to remote desktops are encrypted and hence are not optimized in this setup, so you should use CIFS file sharing if a large amount of data needs to be transferred from a Microsoft Windows PC to the virtual desktop. Cisco WAAS can optimize CIFS file transfers by applying CIFS optimizations to reduce latency and bandwidth consumption.

As Table 3 shows, file transfers from the virtual desktop to clients through VMware VDI are faster by more than 50 percent in the first run and by 66 percent in the second run.

Appendix A: Cisco WAE Configurations

Branch-Office Cisco WAE Configuration

```
! WAAS version 4.1.0 (build b87 Jul  7 2008)
!
device mode application-accelerator
!
!
hostname edge-2
!
!
clock timezone PST8PDT -7 0
!
!
interface GigabitEthernet 1/0
 ip address 10.10.105.3 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
!
ip default-gateway 10.10.105.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
wccp router-list 1 16.10.105.1 10.10.105.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE
7D891AB402CAF2E89CCDD33ED54333AC
!
!
!
!
windows-domain workgroup "SA"
windows-domain netbios-name "CORE"
!
authentication login local enable primary
authentication configuration local enable primary
```

```
!
!
!
!
central-manager address 192.168.1.3
cms enable
!
!
!
flow monitor tcpstat-v1 host 192.168.1.161
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
!
! The VMware VDI uses TCP port 80. The default Web Policy is applied
to this traffic
!
policy-engine application
   set-dscp copy
   service-class default weight 10
   name Web
   classifier HTTP
      match dst port eq 80
      match dst port eq 8080
      match dst port eq 8000
      match dst port eq 8001
      match dst port eq 3128
   exit
   classifier HTTPS
      match dst port eq 443
   exit
   classifier VMware-VMConsole
      match dst port eq 902
   exit
   classifier netqos
      match dst port eq 7878
   exit
! Full Optimization policy is applied to the VMware VDI traffic
traversing the WAN
   map basic
      name Web classifier HTTP action optimize full accelerate http
      name FlowAgent classifier netqos action optimize full
      name Remote-Desktop classifier VMware-VMConsole action optimize
full
   exit
   map other optimize full
exit
!
```

```
! kernel kdb is enabled in WAAS by default
!
!
! End of WAAS configuration
```

Core Cisco WAE Configuration

```
! WAAS version 4.1.0 (build b87 Jul  7 2008)
!
device mode application-accelerator
!
!
hostname Core
!
!
clock timezone PST8PDT -7 0
!
!
interface GigabitEthernet 1/0
 ip address 10.10.107.3 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
!
ip default-gateway 10.10.107.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
wccp router-list 1 16.10.107.1 10.10.107.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE
7D891AB402CAF2E89CCDD33ED54333AC
!
!
!
!
windows-domain workgroup "SA"
windows-domain netbios-name "CORE"
!
```

```
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
central-manager address 192.168.1.3
cms enable
!
!
!
flow monitor tcpstat-v1 host 192.168.1.161
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
! The VMware VDI uses TCP port 80. The default Web Policy is applied
to this traffic
!
!
policy-engine application
   set-dscp copy
   service-class default weight 10
   name Web
   classifier HTTP
      match dst port eq 80
      match dst port eq 8080
      match dst port eq 8000
      match dst port eq 8001
      match dst port eq 3128
   exit
   classifier HTTPS
      match dst port eq 443
   exit
   classifier VMware-VMConsole
      match dst port eq 902
   exit
   classifier netqos
      match dst port eq 7878
   exit
! Full Optimization policy is applied to the VMware VDI traffic
traversing the WAN
   map basic
      name Web classifier HTTP action optimize full accelerate http
      name FlowAgent classifier netqos action optimize full
      name Remote-Desktop classifier VMware-VMConsole action optimize
full
   exit
   map other optimize full
```

```
exit
!
! kernel kdb is enabled in WAAS by default
!
!
! End of WAAS configuration
```

Appendix B: Cisco ACE Configuration

Cisco ACE Admin Context

```
resource-class STICKY
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
boot system image:c4710ace-mzg.A1_8_0a.bin
peer hostname 4710_VDI_2
hostname 4710_VDI_1
interface gigabitEthernet 1/1
  channel-group 200
  no shutdown
interface gigabitEthernet 1/2
  channel-group 200
  no shutdown
interface gigabitEthernet 1/3
  channel-group 200
  no shutdown
interface gigabitEthernet 1/4
  channel-group 200
  no shutdown
interface port-channel 200
  ft-port vlan 170
  switchport trunk allowed vlan 168-169
  port-channel load-balance src-dst-port
  no shutdown
class-map type management match-any MGMT-TRAFFIC
  description "allowed mgmt traffic to ACE"
  2 match protocol http any
  3 match protocol https any
  4 match protocol icmp any
  5 match protocol ssh any
  6 match protocol telnet any
  7 match protocol xml-https any
policy-map type management first-match REMOTE-MGMT
  class MGMT-TRAFFIC
    permit
interface vlan 168
  ip address 192.168.1.220 255.255.255.0
  peer ip address 192.168.1.221 255.255.255.0
  alias 192.168.1.222 255.255.255.0
  service-policy input REMOTE-MGMT
  no shutdown
ft interface vlan 170
  ip address 192.170.1.1 255.255.255.0
  peer ip address 192.170.1.2 255.255.255.0
  no shutdown
ft peer 1
```

```
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 170
ft group 1
  peer 1
  no preempt
  priority 200
  associate-context Admin
  inservice
ip route 0.0.0.0 0.0.0.0 192.168.1.1
context VDI
  allocate-interface vlan 168-169
  member STICKY
ft group 2
  peer 1
  no preempt
  priority 200
  associate-context VDI
  inservice
```

Cisco ACE VMware VDI Context

```
access-list 102 line 8 extended permit tcp any any eq www
access-list 102 line 24 extended permit icmp any any
probe http VDM_PROBE
  interval 5
  faildetect 2
  passdetect interval 5
  passdetect count 2
  request method get url /admin/
  expect status 200 200
  open 1
rserver host CB1
  ip address 192.168.1.80
  inservice
rserver host CB2
  ip address 192.168.1.81
  inservice
serverfarm host VDM_CB
   probe VDM_PROBE
   predictor leastconns
  rserver CB1 80
    inservice
  rserver CB2 80
    inservice
sticky ip-netmask 255.255.255.255 address source VDM_IP_STICKY
  timeout 10
  replicate sticky
  serverfarm VDM_CB
class-map match-all VDM_VIP_80
```

```
  2 match virtual-address 192.169.1.254 tcp eq www
policy-map type loadbalance first-match VDM_LB
  class class-default
    sticky-serverfarm VDM_IP_STICKY
policy-map multi-match VM_LB
  class VDM_VIP_80
    loadbalance vip inservice
    loadbalance policy VDM_LB
    loadbalance vip icmp-reply
interface vlan 169
  ip address 192.169.1.4 255.255.255.0
  alias 192.169.1.1 255.255.255.0
  peer ip address 192.169.1.5 255.255.255.0
  no normalization
  access-group input 102
  service-policy input VM_LB
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.169.1.2
```

Appendix C: References

- Cisco ANS for VMware: http://www.cisco.com/go/optimizevmware
- Cisco ANS: http://www.cisco.com/go/applicationservices
- Cisco Application Networking partner portal: http://www.cisco.com/go/optimizemyapp
- Cisco WAAS Software product information: http://www.cisco.com/go/waas
- Cisco ACE product information: http://www.cisco.com/go/ace
- VMware virtual desktop product information http://vmware.com/products/desktop_virtualization.html
- VMware VDI product information: http://vmware.com/products/vdi/

Additional information about Cisco WAAS data center and branch-office designs is also available:

- Enterprise Data Center Wide Area Application Services (WAAS) Design Guide: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c649/ccmigration_09186a008081c7da.pdf
- Enterprise Branch Wide Area Application Services Design Guide (Version 1.1): http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c649/ccmigration_09186a008081c7d5.pdf

For additional information on VMware Virtual Desktop Manager and networking in the VMware ESX environment, visit:

- http://www.vmware.com/pdf/vdm21_manual.pdf
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns304/c649/ccmigration_09186a00807a15d0.pdf

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 C07-493981-00 09/08