Cisco Application Networking for Citrix Presentation Server Deployment Guide

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

Preface

Document Purpose

This document provides implementation and configuration information for the Cisco ACE and WAAS to provide performance and load balancing to the Citrix Presentation Server application.

Prerequisites

The following prerequisites are required to understand, configure and deploy the Citrix Presentation Server application solution:

- Working knowledge of Citrix Presentation Server application.
- Experience with basic networking and troubleshooting.
- Experience with installation and acceptance of the products covered by this network design.
- Working knowledge of the Cisco Internetworking Operating System (IOS).

Document Organization

The following table provides a brief description of each section.

Section	Description
Solution Overview	A high-level introduction to the solution. Introduces the solution, historical aspects, potential benefits, and scope and limitations.
Solution Architecture	Describes the architecture of the Joint Solution.
Implementing and Configuring the Cisco ACE Solution	Describes configuration and implementation of Cisco ACE within the Joint Solution.
Implementing and Configuring the WAAS Solution	Describes configuration and implementation of WAAS within the Joint Solution.
Network Management	Describes the network management software used in the Joint Solution.

Solution Overview

Solution Description

The Joint Solution offers optimized Citrix Presentation Server application availability, performance, security, and costs by providing application optimization services as follows:

- Application Availability

  Cisco ACE product family application optimization services for high Citrix Presentation Server availability:

  - Application health monitoring—Continuously and intelligently monitors application and database availability
  - Server load balancing—Efficiently routes end user and web services requests to the best available server
  - Network platform health monitoring—Ensures continuity of business operations through mirroring end user transaction states across pairs of network devices

- Application Performance

  Cisco ACE and WAAS product family application optimization services for Citrix Presentation Server high performance:

  - WAN optimization—Provides intelligent caching, compression, and protocol optimization that yields up to 30percent less bandwidth (see Results and Conclusions, page 40).
  - Server offloading—Specialized hardware that offers greater processing efficiency for application optimization services listed below, which frees up significant application server processing time and memory to focus on business logic computations.
  - Data center load balancin—Replaces DNS server
  - Server load balancing—Substitutes for Citrix Presentation Server native load balancing
  - Secure Socket Layer (SSL) termination—Terminates 15,000 connections per second.

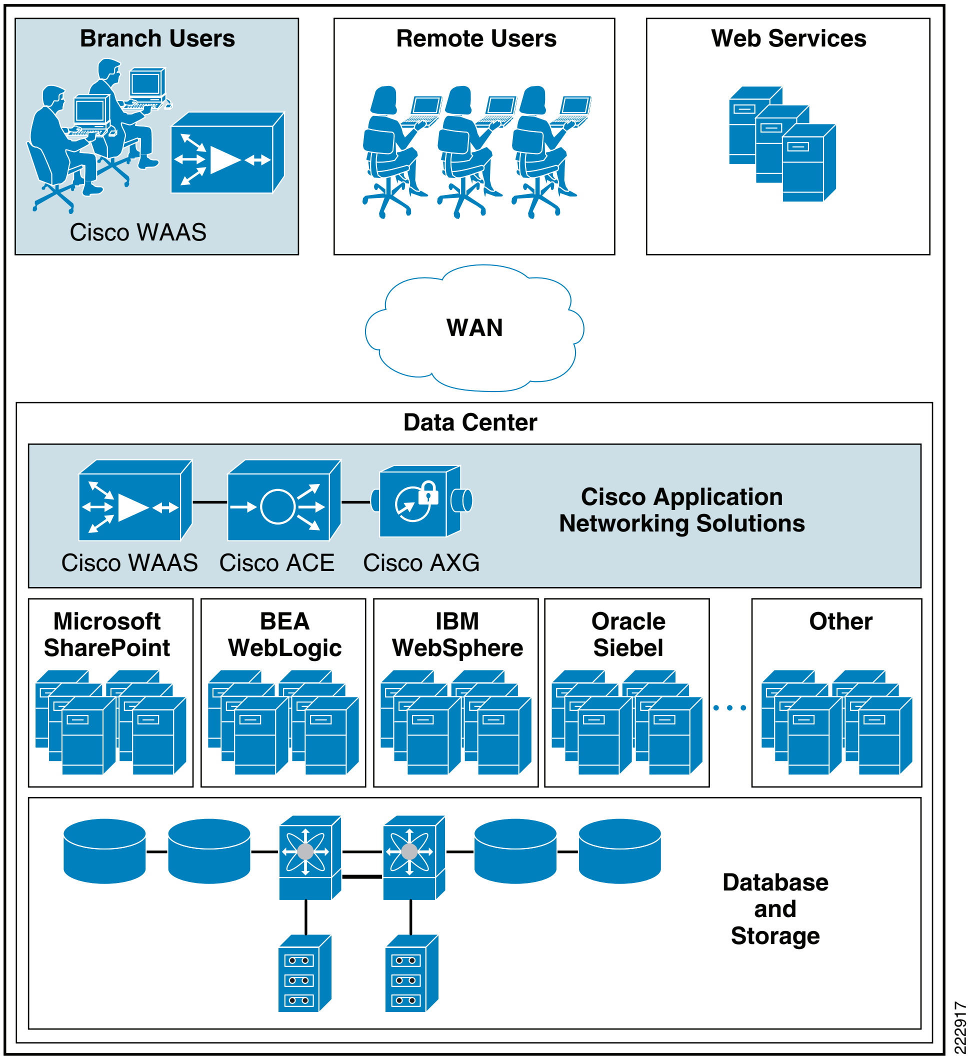
  - Transmission Control Protocol (TCP) connection management—Reduces the number of TCP connections to server.
  - Server health monitoring—Substitutes for Citrix Presentation Server native server health monitoring
  - Traffic compression—Scalable gzip functionality
  - Object caching—Reduce requests to server
- Application Security

  Cisco ACE product family application optimization services for optimized Citrix Presentation Server data security:

  - SSL termination—Efficiently encrypts and decrypts SSL enabled traffic which facilitates the use of intrusion detection and prevention solutions before traffic reaches the servers
  - End user access control—Provides access control lists (ACLs) to protect client-to-server traffic from worms and intruders that attack vulnerable open server ports not used by the application
- Virtualization of Application Optimization Services

  Virtualization of application optimization services herein supplies such services for multiple Citrix Presentation Server solutions as well as other enterprise applications (see Figure 1)

Figure 1 Virtualization of Application Optimization Services



The Application optimization services of the Joint Solution reside both in the data center and the branch to offer end-to-end value, from branch and remote users, all the way through to the database and information storage.

- Data Center Application Optimization Services

  Cisco ACE and WAAS reside in the data center and are arranged to provide virtualized application optimization services for multiple Citrix Presentation Server deployments as well as other enterprise applications.

  Because of their unique location, these solutions can take intelligent action on the end user traffic before it is routed to the Citrix Presentation Server application servers, including load balancing, server health monitoring, SSL decryption, TCP connection consolidation, and security access control.

  While some of these functions could be provided natively by the Citrix Presentation Server application or third party server based solutions, Cisco networking provides these services cost-effectively, freeing up server processing and memory needs to focus on business logic computation.

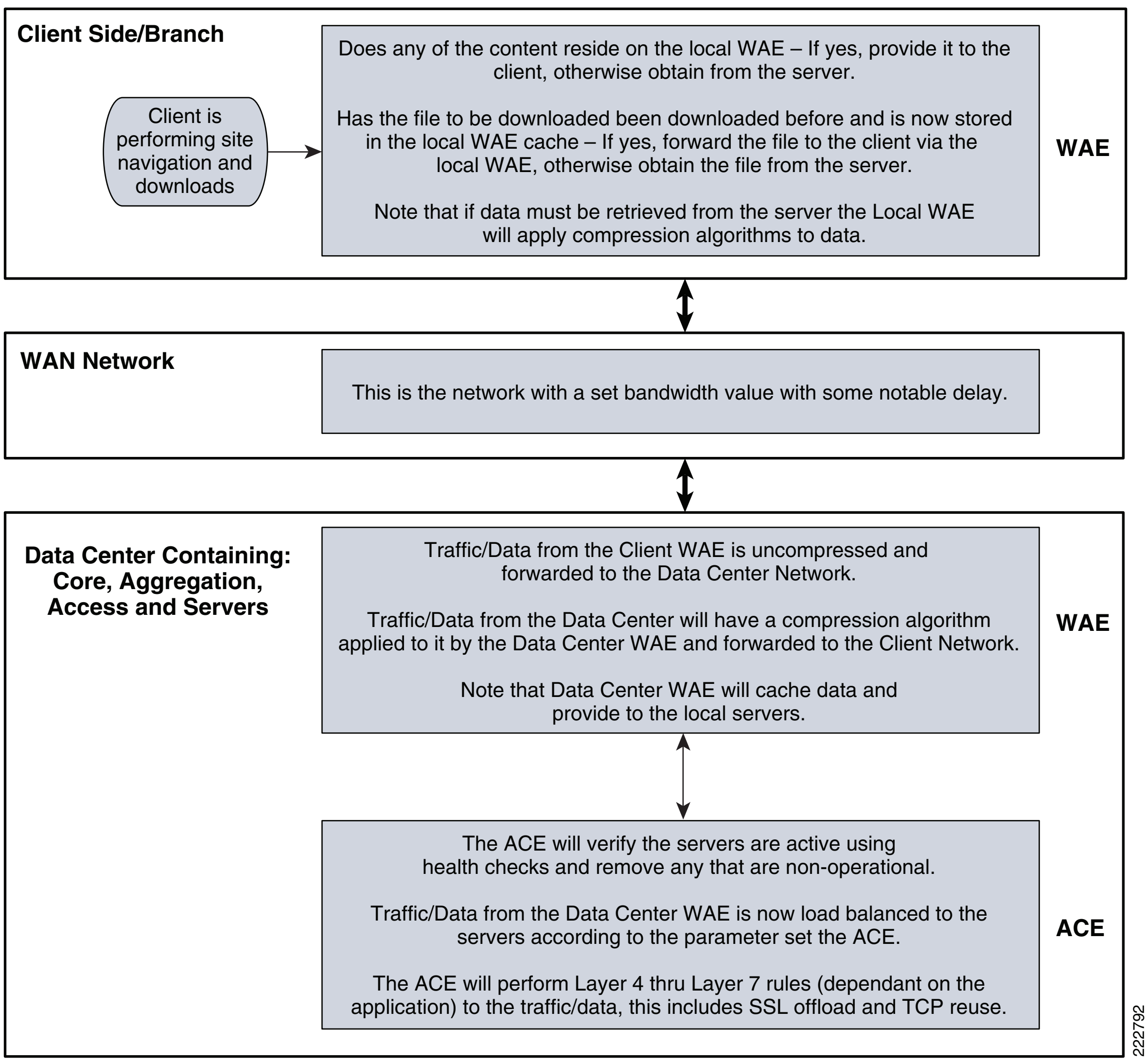
- Wide Area Application Optimization Services

  Cisco WAAS also resides in the branch office and is arranged to provide virtualized application optimization services for all application users in that location. Together with the data center WAAS deployment, the two offer a WAN optimization service through the use of intelligent caching, compression, and protocol optimization.

  When the Citrix Presentation Server application servers respond to end user requests, the response is compressed and then most efficiently passed across the WAN, with minimal bandwidth usage and maximum speed. Commonly used information is cached both at the WAAS solution in the branch as well as in the Cisco ACE solution in the data center, which significantly reduces the burden on the servers and the WAN. (See Figure 2).

Process Flow

Figure 2 Process Flow



Solution Architecture

Citrix Presentation Application Overview

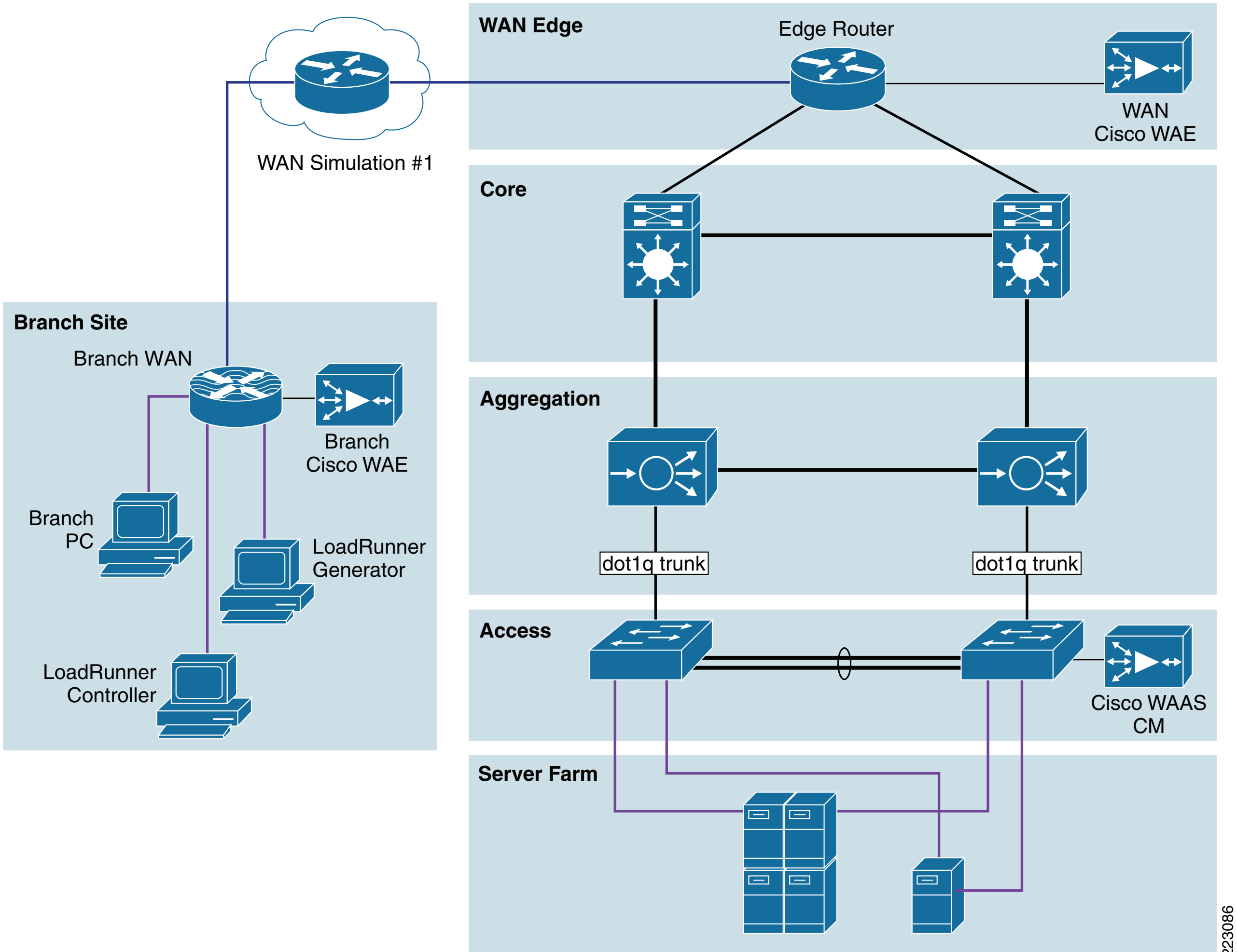
The scope of the solution is to provide performance benefits and reduce resource loading on the server farms for the Citrix Present Server running on the application. The Citrix Presentation Server is a remote access/application publishing product that allows people to connect to applications available from central servers. The advantage of publishing applications using Presentation Server is that it lets people connect to these applications remotely, from their homes, smart phones, and other devices outside of their corporate networks.

The WAASs provided performance benefits to Citrix Presentation Server application by providing optimization to the traffic/data flowing across the WAN and caching data at the local WAASs. The cached data reduced the amount of traffic flowing across the WAN and allowing for more transactions/observations to take place.

The Cisco ACE reduced resource loading on the server farm by providing load balancing on the data that was bound for the server farm.

Application and Application Networking Architecture

Figure 3 Application and Application Networking Architecture



The Joint Solution uses the Cisco WAAS to enhance performance and the Cisco ACE to reduce the load on resources in the server farm. The Cisco WAAS and Cisco ACE each provide a unique benefit to the solution, however there are additional benefits when they are used together as the two solutions are complimentary. The Cisco ACE provides load balancing to the server farm. If the application uses SSL, then the Cisco ACE can provide SSL termination offload, thereby increasing efficiency by removing the load on the servers' resources and allowing the servers to process more transactions. Increased server efficiency also results if the Cisco ACE is used to provide TCP reuse.

The Joint Solution architecture is based on the *Enterprise Branch Wide Area Application Services Design Guide* architecture (Enterprise Branch Design) and the *Data Center Infrastructure Design Guide 2.1*, both found at www.cisco.com/go/srnd.

In the Joint Solution architecture, the WAAS Solution is installed within the Cisco Wide Area Application Engine (WAE) Appliances.

Enterprise Branch

The enterprise branch design shows the Cisco WAE Appliance connected to the local branch router, typically a Cisco Integrated Services Router (ISR). The design provides scalability and availability as compared to installing a Cisco WAAS Network Module within a Cisco ISR as the Cisco ISR must share its resources.

HP Mercury LoadRunner, running on a personal computer in the branch, simulates users that would perform certain tasks in the application.

The traffic is redirected to the Cisco WAE through the Web Cache Communications Protocol (WCCP) from the branch router. The Cisco WAE performs the following functions:

- Locally cached—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 server farm. This allows the WAN to become more efficient as only "needed data" requested.
- New data—If the data that is being forwarded to the server farm or coming from the server farm, the Cisco WAE performs compression algorithms on the data, allowing for the WAN to become more efficient.

WAN Simulation

The WAN simulator provide simulations of standard T1. The following simultions was used:

- WAN Type 1 (Intracontinental)
  - Bandwidth—1.544 Mbps, ESF, B8ZS
  - Delay—100 mS
  - Loss—Drop one packet in every 1000 packets
- WAN Type 2 (Intercontinental)
  - Bandwidth—512 Kbps
  - ESF, B8ZS, Delay—200 mS
  - Loss—drop one packet in every 500 packets

Data Center

The enterprise branch design shows the Cisco WAE appliance connected to the local branch router, typically a Cisco Integrated Services Router (ISR). The design provides scalability and availability as compared to installing a Cisco WAAS Network Module within a Cisco ISR as the Cisco ISR must share its resources.

HP Mercury LoadRunner, running on a personal computer in the branch, simulates users that would perform certain tasks in the application.

The traffic is redirected to the Cisco WAE through the Web Cache Communications Protocol (WCCP) from the branch router. The Cisco WAE performs the following functions:

- Locally cached—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 server farm. This allows the WAN to become more efficient as only "needed data" requested.
- New data—If the data that is being forwarded to the server farm or coming from the server farm, the Cisco WAE performs compression algorithms on the data, allowing for the WAN to become more efficient.

WAN Simulation

The WAN simulator provide simulations of standard T1. The following simulations was used:

- WAN Type 1 (Intracontinental)
  - Bandwidth: 1.544 Mbps, ESF, B8ZS
  - Delay: 100 mS
  - Loss: Drop one packet in every 1000 packets
- WAN Type 2 (Intercontinental)
  - Bandwidth: 512 Kbps, ESF, B8ZS
  - Delay: 200 mS
  - Loss: Drop one packet in every 500 packets

Data Center

For this design, the Cisco ACE Appliance is targeted for a small-to-medium data center (DC). The DC follows the design guidelines found in the *Data Center Infrastructure Design Guide* found at the following URL: http://www.cisco.com/go/srnd

The design consists of a DC WAN router, a collapsed core/aggregation, access, and the server farm (where the application resides). In this document, the focus will be on the DC WAN router, aggregation, and the server farm. The core provides routing to and from the DC WAN router and the aggregation. The access provide Layer 2 connectivity for the server farms to the aggregation. For larger deployments, one should consider a separate core and aggregation layer, or a one-arm deployment where the Cisco ACE Appliance connects to a Cisco 6500. For more information, refer to the following URL:

http://www.cisco.com/en/US/partner/products/ps7027/tsd_products_support_series_home.html

The DC WAN router performs the same function as the branch WAN router by redirecting traffic to the DC WAE. The DC WAE performs the following:

- Locally cached—If the data that is being requested is locally cache, the WAE responds to the requestor with the cached data and requests only required data from the branch. This allows the WAN to become more efficient as only "needed data" is requested.
- New data—If the data is being forwarded to the branch or coming from the branch, the WAE performs compression algorithms on the data, allowing for the WAN to become more efficient.

Within a Cisco WAAS topology, each Cisco WAE runs a process called central management system (CMS). The CMS process provides SSL-encrypted bidirectional configuration synchronization of the Cisco WAAS Central Manager and the Cisco WAE devices. 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 device or a group of Cisco WAE devices (a device group), the Cisco WAAS Central Manager automatically propagates the changes to each of the managed Cisco WAE devices. Cisco WAE devices that are not available to receive the update will receive the update the next time they become available.

The aggregation segment contains the Cisco ACE Appliance. The Cisco ACE Appliance provides the following:

- Virtualization—Device partitioning, where the Cisco ACE has multiple contexts. Each context can be configured for different applications and each context is independent of the other. The Cisco ACE is configured with Admin context and the Weblogic context. Note that the Cisco ACE can support up to 20 contexts (dependant on the license).
- Session Persistence—The ability to forward client requests to the same server for the duration of the session. The Citrix Presentation Server application requires source IP sticky session persistence.
- Transparent Interception—Performs a NAT function to conceal the real server IP address that is residing in the server farm. The Weblogic context is configured with a Virtual IP (VIP) that provides a single address for the users to use connect to the server farm with. This allows the users to access the Citrix Presentation Server application by placing a single IP in the web browser.
- Allowed Server Connections—The maximum number of active connections value on a per-server basis and/or globally to the server farm. In the Citrix Presentation Server application, the maximum number of connections where allowed. Note that this should be re-adjusted depending on the number of applications that will use the Cisco ACE.
- Health monitoring—Used to track the state of the server and determining its ability processing connections in the server farm. The Citrix context used TCP probes to verify if the Citrix Presentation Server servers were available to process application connections.

The Cisco ACE Appliance provides load balancing of the traffic bound to the server farm using one of the following methods:

- Round Robin
- Weighted Round Robin
- Least Connections
- Hash address
- Hash cookie
- Hash Header
- Hash URL

Least connections was used to provide load balancing for ANS solution for Citrix Presentation Server. Least connections selects the server with the fewest number of connections based on server weight. The Cisco ACE Appliance is also used to provide SSL offload and TCP reuse.

The Cisco ACE redundancy used was Inter-chassis. Inter-chassis is a Cisco ACE in one chassis protected by a Cisco ACE in a peer-chassis connected by a fault tolerant (FT) VLAN. The FT is used to transmit flow-state information, configuration synchronization information, and the redundancy heartbeat.

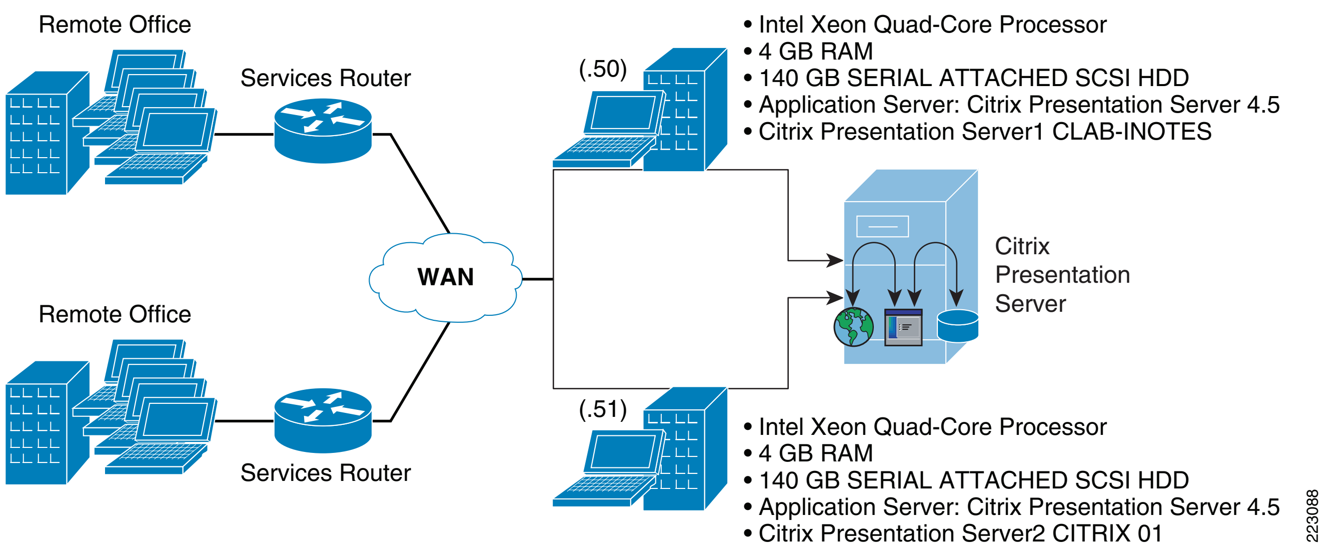
Server Farm

The server farm consisted of two Citrix Presentation Servers, version 4.5:

- The users uses a web interface to connect to the published application (i.e., Microsoft Word).
- The Citrix Presentation Server resides on the Windows 2003 Enterprise Server operating system.
- The hardware used is Quad Xeon processors, running at 1.6 Ghz with 4 GB of RAM and 140 GB SCSI hard drives.

Figure 4 illustrates the Citrix server configuration.

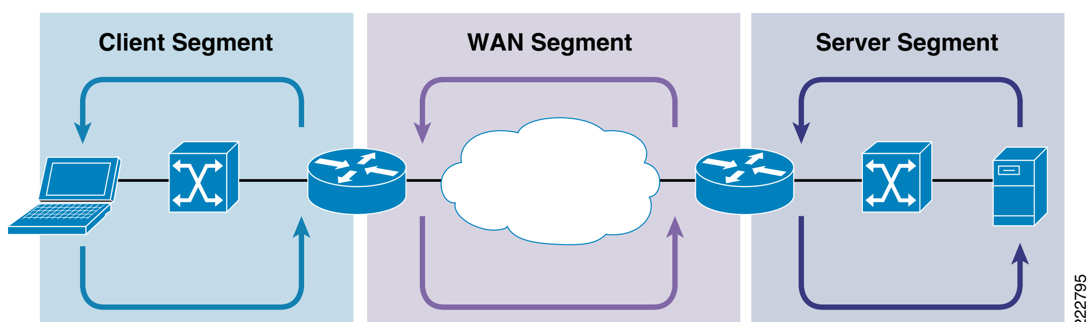
Figure 4 Citrix Server Configuration



Normal Packet Flow

Normal packet flow is broken down into three segments: Client, WAN, and server (see Figure 5). The overall result is that the user's transaction is successful.

Figure 5 Normal Packet Flow



Client Segment

The client segment is defined as the location into which users are connected that allows them to obtain or retrieve data from the application that resides on the server farm. Users have connected personal computers (PC) to a local external switch or an integrated switch/router. When a user opens a browser and provides a URL that points to the application residing on the server, the data is sent from the PC to the switch. The switch forwards the data to the router that connects to the wide area network (WAN).

WAN Segment

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

Server Segment

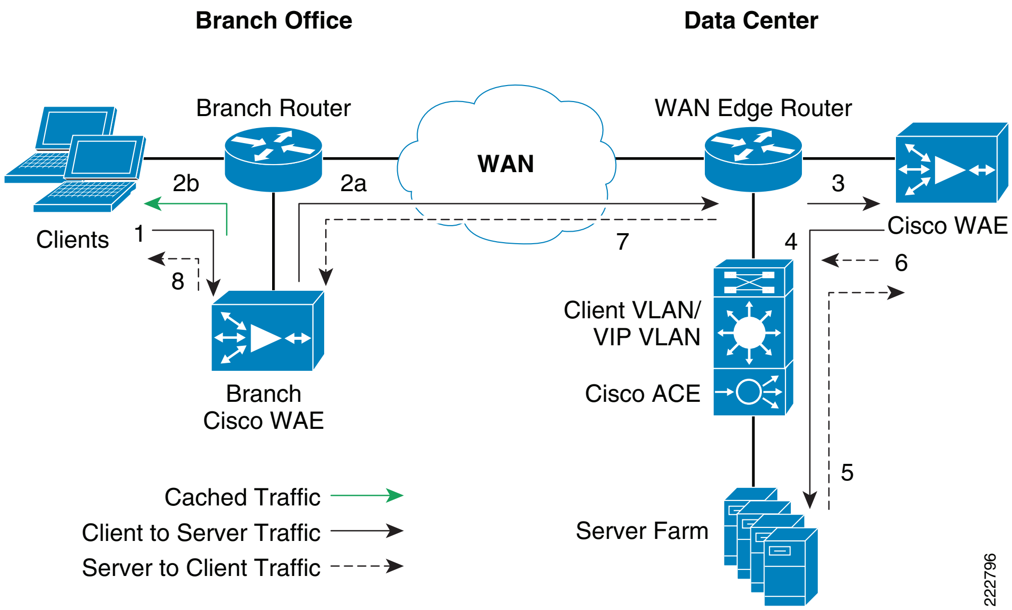
The server segment is the actual data center that consists of a highly available and resilient core, aggregation, and access. The core routes the data traffic to and from the WAN and the aggregation layer. The aggregation layer provides consolidation of multiple access layers and routes the access layer traffic into 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 server farm where the applications reside. The data traffic (URL, per the example) from the client segment transverses the data center until the data traffic is received by the appropriate server. The server's application responds to the request and responds back to the user by forwarding the appropriate data back the client segment.

Response Times

Transaction response times consists of server response time and WAN round trip time. Overall transaction time is directly affected by the WAN round trip time and the server response time. The transaction time correlates to the end-user experience. Delays in the WAN or the time to process a request on a server lead to a longer wait times for data to be viewed by the end-user.

Packet Flow with WAAS and Cisco ACE

Figure 6 Packet Flow with WAAS and Cisco ACE



The following sequence describes the handshake between a client and the server farm and the data transfer phase:

Step 1 The client sends a SYN packet to the server farm VIP address. The packet is forwarded to the branch router. The branch router intercepts the packet with WCCP and forwards it to the branch Cisco WAE appliance.

Step 2 2.a.) The branch Cisco WAE applies a new TCP option (0x21) to the packet if the application is identified for optimization by an application classifier. The branch 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 router and then to the WAN. b.) During the data transfer phase, if the requested data are in its cache, the branch Cisco WAE returns its cached data to the client. Traffic does not travel through the WAN to the server farm. Hence both response time and WAN link utilization are improved.

Step 3 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.

Step 4 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 (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 it to the Cisco ACE. The Cisco ACE forwards the packet to the server farm VLAN with TCP option 21 removed. TCP options are usually ignored by the server, even if it is still in place. The Cisco ACE performs load balancing to the data traffic. Other functions the Cisco ACE performs include SSL offload, TCP reuse, cookie and IP sticky pertinence.

Step 5 The following steps are for reverse traffic flow. The server farm sends the SYN/ACK packet back to the client with no TCP option. The packet from the server farm VLAN is matched 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 are not in its cache.

Step 6 The data center Cisco WAE sends the packet to the WAN edge router.

Step 7 The packet travels through the WAN and arrives at the branch router. The branch router intercepts the packet and forwards it to the branch Cisco WAE. The branch 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. The auto-negotiation of the policy occurs as the branch 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 Cisco WAE have determined the application optimizations to apply on this specific TCP flow. During the data transfer phase, the branch Cisco WAE caches the data if the data are not in its cache.

Step 8 The packet is forwarded to the branch router and then to the client.

Implementing and Configuring the Cisco ACE Solution

Implementation

Implementation Overview

The Cisco ACE Appliance used in this solution is deployed at data center aggregation layer. The Cisco ACE Appliance is deployed in *routed* mode, where the client and server side VLANs each support unique IP subnet. In this deployment mode, the Cisco ACE Appliance acts as the default gateway for the application servers.

What was Implemented

Key features implemented on the Cisco ACE Appliance to support this application are as follows.

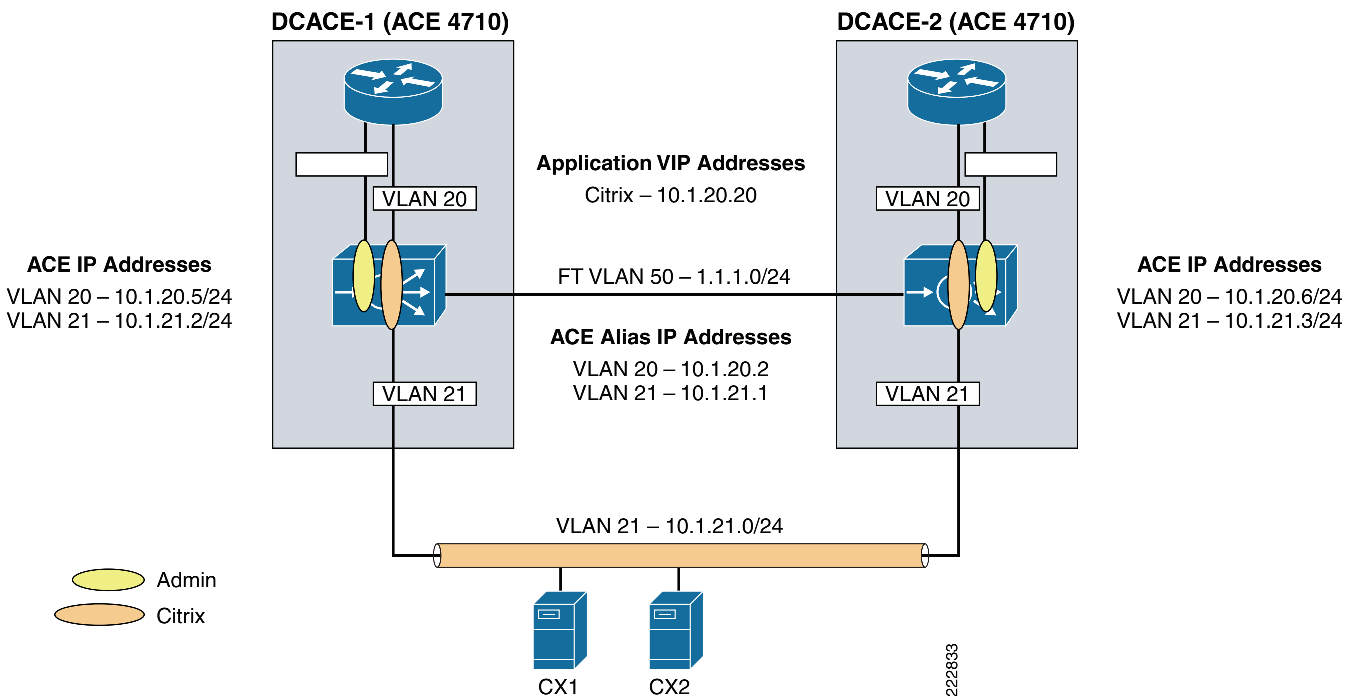
- Layer 4 load balancing
- Persistence based on source IP
- Server health monitoring
- Connection replication for stateful failover
- Least connections predictor used for load balancing

What was Not Implemented/Tested

TCP reuse was not implemented in this solution.

Network Topology

Figure 7 Cisco ACE Network Topology



Hardware Components

Table 1 Hardware Components

Product	Hardware Rev	Interfaces	Memory
ACE-4710-K9	1.1	Console port 4 - 10/100/1000	6226408 kB

Note For the data center infrastructure, refer to the *Data Center Infrastructure Design Guide*: http://www.cisco.com/go/srnd

Software Components

Table 2 Software Components

Product	Software/Code Version
System Image	build 3.0(0)AB0(0.500)
Performance Throughput	ACE-AP-02-LIC.lic
Virtualization Contexts	ACE-AP-VIRT-020.lic
SSL TPS	ACE-AP-SSL-10K-K9.lic
Application Acceleration	ACE-AP-OPT-LIC-K9
Compression Performance	ACE-AP-C-1000-LIC.lic

Features and Functionality

Table 3 Solution Features

Product	Features and Functionality
ACE-4710-K9	• Virtualization • Layer 4 load balancing • Session persistence with source IP sticky • Server health monitoring • Transparent interception • High availability • Least connections predictor used for load balancing

Features, Services, and Application Design Considerations

In terms of the Cisco ACE, source IP sticky is the Cisco ACE session persistence feature that is used for the Citrix Presentation Server solution. For configuration, refer to Configuration Task Lists and Appendix A—Cisco ACE Configuration.

Scalability and Capacity Planning

Server farms can increase application scalability and availability by load balancing applications services with multiple servers. In the event a server is down, other servers within the server farm can assume the load. Additional servers can be added to the server farm for scalability.

High Availability

Redundancy (or fault tolerance) uses a maximum of two Cisco ACE Appliances to ensure that the network remains operational, even if one of the appliances becomes unresponsive. Redundancy ensures that network services and applications are always available.

Redundancy provides seamless switchover of flows in case a Cisco ACE becomes unresponsive or a critical host or interface fails. Redundancy supports the following network applications that require fault tolerance:

- Mission-critical enterprise applications
- Banking and financial services
- E-commerce
- Long-lived flows such as FTP and HTTP file transfers

For more information on configuring HA on the Cisco ACE Appliance, refer to:
http://preview.cisco.com/en/US/products/ps7027/products_configuration_guide_chapter09186a00807c64d3.html

For specific HA setup for this design, refer to the the complete Admin context configuration in Appendix A—Cisco ACE Configuration.

Configuration Task Lists

Information required prior to configuration of the equipment:

Installing and Configuring Cisco ACE Appliance

Given the topology in Figure 7, the Cisco ACE Appliance is configured in *routed* mode with a client and a server side VLANs. The GigabitEthernet port connecting to the WAN router needs to be configured as a Layer 2 dot1q trunk carrying client vlans. The GigabitEthernet port connecting to the access switches should be configured as a Layer 2 dot1q trunk server VLANs. These are the first steps in configuring the ACE Appliance. Note that the following steps occur from within the Admin Context.

Step 1 Add client trunk to WAN router:

Example:

```
!interface gigabitEthernet 1/4
  description connection to WANRTR
  switchport trunk allowed vlan 10,20,30
  no shutdown
```

Step 2 Add server side trunk to access switches:

Example:

```
interface gigabitEthernet 1/1
  description 3750-1
  switchport trunk allowed vlan 11,21,31
  no shutdown
```

Virtualization

Virtualization is a method used in allocating available resources into two or more contexts for security and management purposes. Up to 20 contexts can be configured on ACE. Resources can be allocated to each context to avoid a single context consuming the entire pool of resources. This document only covers key virtualization configuration. Within each context, domains and role-base access controls (RBACs) can be further configured to provide additional security and access control to the resources.

Context Configuration

The following example shows the context configuration steps:

Step 1 Configure resource-class(es):

Example:

```
DCACE1/Admin(config)# resource-class CX-resource  <- Resource-class name
  <cr>  Carriage return.
```

Following are the different resources that can be segmented:

```
DCACE1/Admin(config-resource)# limit-resource ?
  acl-memory         Limit ACL memory
  all                Limit all resource parameters
  buffer             Set resource-limit for buffers
  conc-connections   Limit concurrent connections (thru-the-box traffic)
  mgmt-connections   Limit management connections (to-the-box traffic)
  proxy-connections  Limit proxy connections
  rate               Set resource-limit as a rate (number per second)
  regexp             Limit amout of regular expression memory
  sticky             Limit number of sticky entries
  xlates             Limit number of Xlate entries
```

Sample configuration:

```
DCACE1/Admin# show running-config resource-class
Generating configuration....

resource-class CX-resource
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 0.01 maximum unlimited
resource-class IN-resource
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 0.01 maximum unlimited
resource-class PS-resource
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 0.01 maximum unlimited
```

Step 2 Configure context(s).

A context is configured by giving it a name, allocating VLANs, and assigning it to a resource-class (See Step 1):

```
context citrix
  description CITRIX Testing
  allocate-interface vlan 20-21
  member CX-resource
```

Step 3 To configure per-context features and functionality, use the **changeto** command with the context created in Step 2. At that point, you have accessed a virtually new Cisco ACE context.

Example:

```
DCACE1/Admin# changeto citrix
DCACE1/testfeature# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

For more information on configuring virtualization, visit:
http://preview.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

Remote Management Access

To access the Cisco ACE Appliance remotely either via Telnet, SSH, SNMP, HTTP or HTTPS or to allow ICMP access to the Cisco ACE Appliance, a policy must be defined and applied to the interface(s) where the access will be entering from. The following example shows the configuration steps needed:

Step 1 Configure 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 <- Needed if XML Interface access
50 match protocol https any- via HTTP(S)
```

Step 2 Configure policy-map of type management:

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

Step 3 Apply policy-map to the VLAN interfaces:

```
interface vlan 30
  service-policy input REMOTE-ACCESS

interface vlan 31
service-policy input REMOTE-ACCESS
```

Configuring Interface(s) and Default Gateway

Interface VLANs need to be configured for Layer 3 connectivity to the Cisco ACE. Service policies for load balancing, security, and management access to the Cisco ACE are also applied at the interface VLAN level.

Bridge mode design also requires configuration of BVI interfaces. Basic Interface configuration includes:

- An access-list to permit/deny traffic through ACE. For example:

```
access-list EVERYONE line 10 extended permit icmp any any
access-list EVERYONE line 20 extended permit ip any any
```

- IP address and network mask of the interface(s):

```
interface vlan 20
  ip address 10.1.20.5 255.255.255.0
  peer ip address 10.1.20.6 255.255.255.0
  alias 10.1.20.2 255.255.255.0
```

```
interface vlan 21
  ip address 10.1.21.2 255.255.255.0
  peer ip address 10.1.21.3 255.255.255.0
  alias 10.1.21.1 255.255.255.0
```

- Applying management access policy, and access-group to the interface(s), **no shutdown** of the interface(s):

```
interface vlan 20
  access-group input EVERYONE
  access-group output EVERYONE
  service-policy input remote-access
  no shutdown
interface vlan 21
  access-group input EVERYONE
  access-group output EVERYONE
  service-policy input remote-access
 no shutdown

interface vlan 20
  ip address 10.1.20.5 255.255.255.0
  alias 10.1.20.2 255.255.255.0
  peer ip address 10.1.20.6 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  service-policy input int20
  no shutdown
interface vlan 21
  ip address 10.1.21.2 255.255.255.0
  alias 10.1.21.1 255.255.255.0
  peer ip address 10.1.21.3 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  no shutdown
```

- Default gateway can be configured as following:

```
ip route 0.0.0.0 0.0.0.0 10.1.20.1
```

Redundancy / High Availability

To provide high availability and redundancy, the Cisco ACE Appliances can be setup and configured in a redundant mode. The Cisco ACE can be configured in a typical active/backup redundancy mode or active/active (per context) redundancy mode.

```
DCACE1/Admin(config)# ft ?
  auto-sync  Enable auto sync
  group      Configure Fault Tolerance Group
  interface  Configure FT VLAN
  peer       Configure Fault Tolerance Peer
  track      Configure Fault Tolerance tracking for switchover
DCACE1/Admin(config)# ft interface vlan 50  <- Create a VLAN interface for the FT traffic
DCACE1/Admin(config-ft-intf)# ip address 1.1.1.1 255.255.255.0
DCACE1/Admin(config-ft-intf)# peer ip address 1.1.1.2 255.255.255.0
DCACE1/Admin(config-ft-intf)# no shutdown
DCACE1/Admin(config)# ft peer 1  <- Configure FT peer for this ACE Appliance
DCACE1/Admin(config-ft-peer)# ?

Configure FT Peer parameters:
```

```
  do                EXEC command
  exit              Exit from this submode
  ft-interface      Specify interface used for exchanging FT related information
  heartbeat         Configure heartbeat
  no                Negate a command or set its defaults
  query-interface   Specify interface to obtain peer's health if FT vlan is down
DCACE1/Admin(config-ft-peer)# ft-interface vlan 50 <- Assign FT VLAN to this peer
DCACE1/Admin(config-ft-peer)# heartbeat ?
  count     Configure heartbeat interval count
  interval  Configure heartbeat interval
DCACE1/Admin(config-ft-peer)# heartbeat count ?
  <10-50>  Specify heartbeat interval count (default 10)
DCACE1/Admin(config-ft-peer)# heartbeat count 10

DCACE1/Admin(config-ft-peer)# heartbeat interval ?
  <100-1000>  Specify heartbeat interval frequency in milli-seconds
DCACE1/Admin(config-ft-peer)# heartbeat interval 1000

DCACE1/Admin(config)# ft group 2  <- Create a fault tolerance group
DCACE1/Admin(config-ft-group)# ?
Configure FT Group parameters:
  associate-context  Associate a context with this FT group
  do                 EXEC command
  exit               Exit from this submode
  inservice          Enable FT Group
  no                 Negate a command or set its defaults
  peer               Configure FT Group Peer parameters
  preempt            Enable FT preemption
  priority           Configure FT Group priority
DCACE1/Admin(config-ft-group)# peer 1
DCACE1/Admin(config-ft-group)# priority 99
DCACE1/Admin(config-ft-group)# preempt
DCACE1/Admin(config-ft-group)# associate-context admin  <- Admin context, ACTIVE in this 
ACE
DCACE1/Admin(config-ft-group)# inservice <- Enable this FT group
```

By assigning context(s) to an FT group, a network administration can create multiple groups for multiple contexts where the ACTIVE contexts can be distributed among the two Cisco ACE Appliances. This setup provides active/active redundancy setup for load sharing and high availability.

Probes

The Cisco ACE uses probe as one of available keep-alive methods to verify the availability of a real server. Probe is configured by defining its type and name. There are different types of probes that can be configured on the Cisco ACE, as shown in the following:

```
DCACE1/Admin(config)# probe ?
  dns       Configure dns probe
  echo      Configure echo probe
  finger    Configure finger probe
  ftp       Configure ftp probe
  http      Configure http probe
  https     Configure https probe
  icmp      Configure icmp probe
  imap      Configure imap probe
  ldap      Configure ldap probe
  pop       Configure pop probe
  radius    Configure radius probe
  scripted  Configure script probe
  smtp      Configure smtp probe
  tcp       Configure tcp probe
  telnet    Configure telnet probe
```

```
  udp        Configure udp probe
```

Some key timers and parameters need to be tuned when probes are configured. The value for these parameters influences how rapidly the Cisco ACE (or any load balancer) takes a server out of rotation and brings it back in service. The following parameters need to be tuned for probes of any type (ICMP, UDP, TCP, HTTP, HTTPS, Scripted)

- *Faildetect*—Refers to how many consecutive failed probes qualifies a server to declared probe failed. 'Faildetect' is configured as a counter value. The default value is 3. Generally, *faildetect* value is left at default value.
- *Interval*—Refers to how frequently the Cisco ACE sends probe to a server. *Interval* is configured in seconds. The default value is 120 seconds. Generally, interval is configured around 5-10 seconds depending upon the applications and size of the environment.
- *Passdetect*—This configuration determines how the Cisco ACE will re-probe the server after it has been declared failed. *Passdetect* variable has two attributes:
  - *Passdetect count*—Refers to how many consecutive successful responses ACE will need to see before declaring a server as OPERATIONAL. The default value is 3. This value can be tuned according to the requirements.
  - *Passdetect interval*—Refers to how many seconds the Cisco ACE waits to probe a server after it has been declared failed. The default value is 300 seconds. Generally, the value is changed to a much lower value of 15 to 30 seconds range.

Following additional parameters should be configured for TCP, HTTP, and HTTPS types of probes:

- *Open*—Refers to the time (in seconds) the Cisco ACE waits to keep a TCP connection open. The default value is 10 seconds. Generally this value is configured close to the interval value.
- *Receive*—Once a TCP SYN (for a probe) is sent to a server, the value for *receive* determines how long the Cisco ACE waits to receive a reply from the server. This value is configured in seconds and the default value is 10 seconds. Generally, it is configured to something equal to or less than the value interval.
- *Connection*—Determines how the Cisco ACE closes the connection after it has successfully sent a probe. By default, the Cisco ACE closes the connection gracefully, meaning, it sends TCP FIN to close the connection. Optionally, the Cisco ACE can be configured to close the connection with a TCP RESET by configuring the **connection term forced** command.
- *Port* —TCP/UDP port number on which this probe is sent. Following are the default values for various probes:
  - TCP port 80
  - UDP port 53
  - HTTP port 80
  - HTTPS port 443
- *Request*—This parameter is used to configure HTTP Request method (HEAD or GET) and URL for the probe. The default method is GET and default URL is '/'. Generally, method and URL are configured according to specific applications. This parameter is only applicable to HTTP/HTTPS probes.
- *Expect*—This parameter allows the Cisco ACE to detect two values from the server:
  - *Expect status* – Refers to what HTTP Status Code (or range) to expect from the server. There is no default HTTP return code expected. It has to be configured explicitly.
  - *Expect regex*—A *regex* can be configured to parse a specific field in the response data.

This parameter is only applicable to HTTP/HTTPS probes.

- *SSL*—This is configured to defined what cipher and SSL version the Cisco ACE should use when sending an HTTPS probe. Following is the list of ciphers and SSL versions supported on the Cisco ACE:
  - ssl cipher:
  - RSA_EXPORT1024_WITH_DES_CBC_SHA EXP1024-DES-CBC-SHA Cipher
  - RSA_EXPORT1024_WITH_RC4_56_MD5 EXP1024-RC4-MD5 Cipher
  - RSA_EXPORT1024_WITH_RC4_56_SHA EXP1024-RC4-SHA Cipher
  - RSA_EXPORT_WITH_DES40_CBC_SHA EXP-DES-CBC-SHA Cipher
  - RSA_EXPORT_WITH_RC4_40_MD5 EXP-RC4-MD5 Cipher
  - RSA_WITH_3DES_EDE_CBC_SHA 3DES-EDE-CBC-SHA Cipher
  - RSA_WITH_AES_128_CBC_SHA AES-128-CBC-SHA Cipher
  - RSA_WITH_AES_256_CBC_SHA AES-256-CBC-SHA Cipher
  - RSA_WITH_DES_CBC_SHA DES-CBC-SHA Cipher
  - RSA_WITH_RC4_128_MD5 RC4-MD5 Cipher
  - RSA_WITH_RC4_128_SHA RC4-SHA Cipher
  - ssl versions:
  - SSLv2 SSL Version 2.0
  - SSLv3 SSL Version 3.0
  - TLSv1 TLS Version 1.0

  This parameter is only applicable to HTTPS probes.

Following are sample configurations for TCP, HTTP, and HTTPS probes:

- TCP Probe:

```
probe tcp TEST-TCP
  interval 2
  faildetect 2
  passdetect interval 10
passdetect count 2
```

- HTTPS Probe:

```
probe https test-ssl
  interval 5
  faildetect 2
  passdetect interval 10
  passdetect count 2
  receive 2
  ssl cipher RSA_WITH_RC4_128_MD5
  expect status 200 201
open 2
```

Note The above sample configuration uses the default request method GET and default URI/.

- HTTP Probe:

```
probe http test-web
  interval 5
  faildetect 2
```

```
passdetect interval 10
passdetect count 2
receive 2
expect status 200 201
open 2
```

Real Server

Load balancer selects the real servers (called rserver in the Cisco ACE) to send the intended traffic based on certain sets of criteria. When configuring a real server, be aware that real server name is case sensitive. The minimum configuration needed for rserver configuration is the IP address and configuring the rserver as inservice.

The same rserver can be used in multiple server farms (shown later in the document). If an rserver is made no inservice at the rserver level, then it is taken out of rotation from every server farm on which it is configured. This provides the flexibility to take a server completely out of rotation with a single command.

To take a server out of rotation on a per-server farm basis, rserver should be made no inservice at the server farm level.

The following is an example of configuring rserver on the Cisco ACE:

```
rserver host WL1
ip address 10.1.50.51
inservice
```

Server Farm

A server farm is a logical collection of real servers (rservers) that the load balancer select base on certain sets of criteria. As with real server, server farm name is also *case sensitive*.

Basic server farm configuration includes adding rservers and probes to the server farm. In addition, some other parameters are also explained.

Following are the key configuration options along with explanation within server farm sub-configuration mode:

- *Failaction*—Defines what action ACE should take about currently established connections if a real is detected as probe_failed. The default behavior for the Cisco ACE is to take no action and allow the connections to close gracefully or timeout.

  The configurable option *failaction purge* forces the Cisco ACE to remove the connections established to that real and send TCP RST(s) towards the client(s) and real(s).

- *Predictor*—Refers to the Load Balancing Algorithm for the server farm. Options available are:
  - *Hash* –Is based on source/destination IP address, URL, Cookie, and Header
  - *Leastconns*—Is based on least number of connections. By default , slow start is enabled for l*eastconns* and its timing can be tuned using *predictor leastconns slowstart*?

    <1-65535> Specify slowstart duration in seconds
  - *roundrobin*—Load balance in a roundrobin fashion (default)
- probe —This parameter allows to apply a probe with the server farm. Multiple probes can be applied to the same server farm.

- retcode—This parameter is used to configure server health-checks based on HTTP return code. The configuration allows to define a range of HTTP return codes and take an action once a threshold is reached.

  retcode <*min*> <*max*> **check** <*remove|count|log*> <*threshold value*> **resume-service** <*value in seconds*>

- Rserver—This parameter is used to associate real server(s) with a server farm. Port address translation, maximum and minimum connections, and weight are some common configurations that can be done in rserver sub-configuration mode.
- Transparent—This parameter is equivalent to **no nat server** command on the CSM and type *transparent-cache* on the CSS. When configured, the Cisco ACE does not NAT Layer 3 IP address from VIP to real server's IP address.

Following is an example of basic server farm configuration:

```
serverfarm host PS1
  predictor leastconns
  probe TCP
  rserver PS2
    inservice
  rserver PS3
    inservice
```

Load Balancing

The Cisco ACE uses class-map, policy-map, and service-policy to classify, enforce, and take action on incoming traffic. Traffic trying to reach a virtual IP (VIP) on certain a port can be classify as a Layer 4 as the classification only based on destination IP and destination port.

The following example shows the configuration steps needed:

Step 1 Configure Virtual IP Address (VIP) using class-map of type match-any:

```
class-map match-any CX-VIP
  2 match virtual-address 10.1.20.10 any
```

Step 2 Configure policy-map of type loadbalance to associate sticky serverfarm:

```
policy-map type loadbalance first-match CX-VIP-l7slb
  class class-default
    sticky-serverfarm app-ipstky
```

Step 3 Configure policy-map of type multi-match to associate class-map configured in Step 1 above. Also apply ssl-proxy server under class maps for HTTPS traffic.

```
policy-map multi-match int20
  class CX-VIP
    loadbalance vip inservice
    loadbalance policy CX-VIP-l7slb
    loadbalance vip icmp-reply
```

Step 4 Apply policy-map to the interface VLAN:

```
interface vlan 20
  service-policy input int20
```

The following is a complete Layer 4 Load-balancing configuration:

```
!
probe tcp PROBE-TCP
  interval 2
  faildetect 2
  passdetect interval 10
  passdetect count 2

rserver host CX1
  ip address 10.1.21.50
  rserver host CX2
  ip address 10.1.21.51
  inservice
rserver host CX3
 ip address 10.1.21.52
 inservice

serverfarm host CX1
  predictor leastconns
  rserver CX1 80
  rserver CX2 80
    probe PROBE-TCP
    inservice
  rserver CX3 80
    probe PROBE-TCP
    inservice


class-map match-any CX-VIP
  2 match virtual-address 10.1.20.10 any

policy-map type loadbalance first-match CX-VIP-l7slb
  class class-default
    sticky-serverfarm app-ipstky

policy-map multi-match int20
  class CX-VIP
    loadbalance vip inservice
    loadbalance policy CX-VIP-l7slb
    loadbalance vip icmp-reply


interface vlan 20
  ip address 10.1.20.5 255.255.255.0
  alias 10.1.20.2 255.255.255.0
  peer ip address 10.1.20.6 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  service-policy input int20
  no shutdown
interface vlan 21
  ip address 10.1.21.2 255.255.255.0
  alias 10.1.21.1 255.255.255.0
  peer ip address 10.1.21.3 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.1.20.1
```

Stickiness (Session Persistence)

Session persistence or sticky configuration allows multiple subsequent connections from the same client to be sent to the same real server by the Cisco ACE. The Cisco ACE supports stickiness based on source/destination (or both) IP address, and HTTP cookies. For the Citrix proof-of-concept test effort, source IP sticky was chosen because of the nature of Citrix Presentation Server.

Following are the sample configuration for IP source and destination sticky with the Cisco ACE.

ACE IP Stickiness

Following steps are needed to configure stickiness based on the source IP:

Step 1 Configure a sticky IP group:

```
sticky ip-netmask 255.255.255.0 address both app-ipstky
  serverfarm CX1
```

Step 2 Apply sticky group to a loadbalance L7 policy as a sticky-serverfarm:

```
policy-map type loadbalance first-match CX-VIP-l7slb
  class class-default
    sticky-serverfarm app-ipstky
```

Step 3 Apply load balance policy to a multimatch policy:

```
policy-map multi-match int20
  class CX-VIP
    loadbalance vip inservice
    loadbalance policy CX-VIP-l7slb
    loadbalance vip icmp-reply
```

Step 4 Apply multimatch policy as a service-policy to the interface VLAN:

```
interface vlan 20
  ip address 10.1.20.5 255.255.255.0
  alias 10.1.20.2 255.255.255.0
  peer ip address 10.1.20.6 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  service-policy input int20
  no shutdown
```

Configuration and Menus

Refer to Appendix A—Cisco ACE Configuration, page 48.

Troubleshooting Configuration

These show commands can help troubleshoot issues with the configuration:

- **show stats**—Displays the statistical information relating to the operation of the Cisco ACE.
- **show service-policy** *policy_name*—Displays the statistics for service policies enabled globally within a context or on a specific interface.

- **show serverfarm** *name* **detail**—Displays the summary or detailed server-farm statistics.
- **show rserver** *rserver_name* **detail—**Displays the summary or detailed statistics for a named real server or for all real servers.
- **show probe—**Displays the probe information including 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 auto-sync configuration of all contexts.
- **show ft group status—**Verifies FT status of all configured context in the Cisco ACE.
- **show ft peer detail**—Verifies the state of FT peering.
- **show resource usage—**Displays the resource usage for each context.
- **show np** *NP_number*—Displays the hardware information stored on the three network processors.

Configuration Rollback

Configuration rollback allows the administrator to revert back to a previous configuration when the new configuration does not work.

Step 1 Create a configuration checkpoint:

```
ACE_1/testfeature# checkpoint create name
```

Step 2 Rollback to the checkpoint defined in Step 1:

```
ACE_1/testfeature# show checkpoint all
ACE_1/testfeature# checkpoint rollback config-05-09-06
```

Implementing and Configuring the WAAS Solution

Implementation

Implementation Overview

The Cisco WAAS solution requires a minimum of three Cisco Wide Area Application Engine (WAE) devices to auto-discover and deliver applicable application optimizations. One Cisco WAE is placed in the enterprise data center and the other at the branch site. The enterprise data center Cisco WAE is placed on the WAN edge connected to the WAN router. The branch topology for the WAE uses the extended branch model. The extended services branch offloads the Cisco WAE device from the local branch router and leverages the available ports on a local switch. This design provides scalability and availability of the solution.

What was Implemented

The 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, the Cisco routers support the following four methods of traffic interception:

- Web Cache Communications Protocol (WCCP) v2
- Service policy with the Cisco ACE
- Inline hardware

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

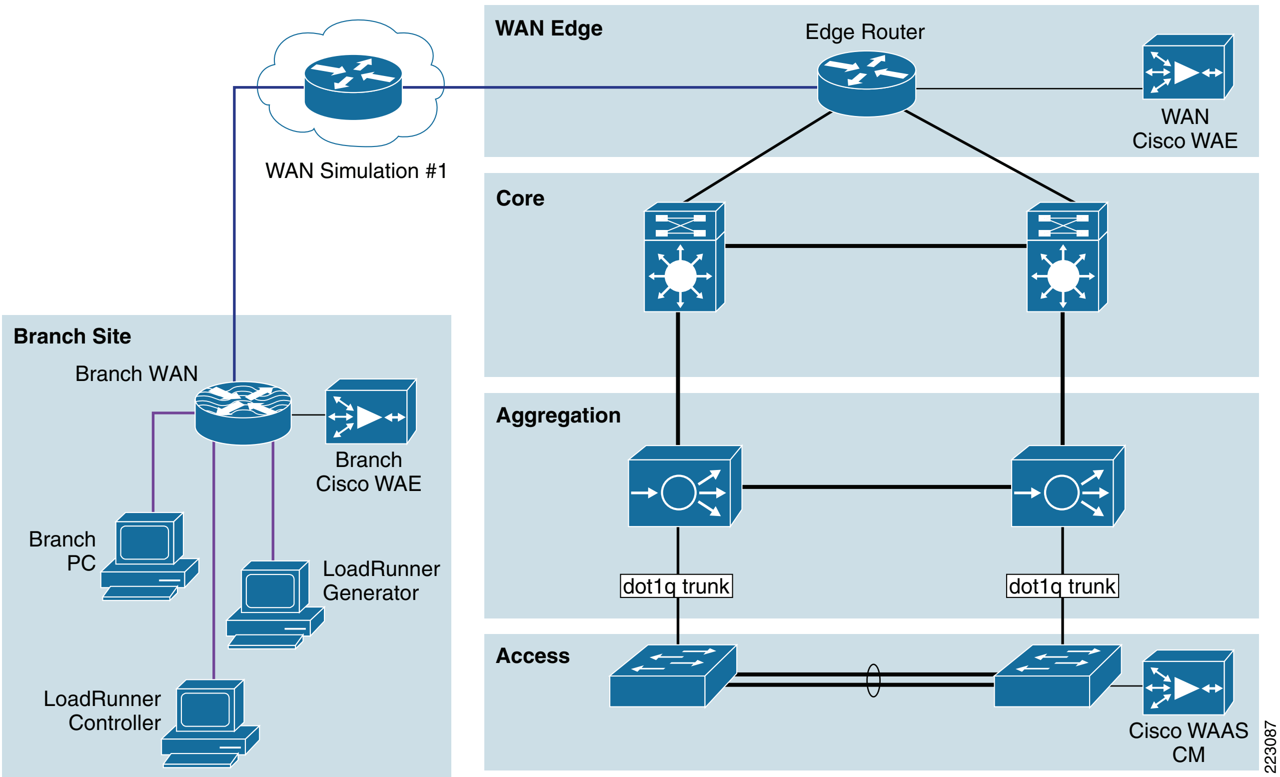
Note The "out-of-box" Cisco WAEs have a standard set of application variables and ports that are defined for optimization. In this solution no changes need to be made to the standard default configuration of the WAEs.

What was Not Implemented

Consolidated branch was not implemented in this solution. The consolidated branch model uses an integrated services router, providing a comprehensive solution within a single platform. The consolidated branch provides limited scalability and consider for use with a branch with small amount of users.

Network Topology

Figure 8 Cisco WAAS Network Topology



Hardware Components

Table 4

Product	Chassis	Modules	Interfaces	Memory
WAE-7326-K9	WAE-7326-K9	N/A	2 10/100/1000 Ethernet, serial port	4 Gbytes, 144 GB SCSI HD
WAE-612-K9	WAE-612-K9	N/A	2 10/100/1000 Ethernet, serial port	2 Gbytes, 144 GB SCSI HD

Software Components

Table 5 Software Components

Product	Software/Code Version
SF-WAAS-4.0-SC-K9	4.0.13
WAAS-ENT-APL	Cisco WAAS Enterprise License for 1 WAE Appliance

Table 5 Software Components

Product	Software/Code Version
SF-WAAS-4.0-SC-K9	4.0.13
WAAS-ENT-APL	Cisco WAAS Enterprise License for 1 WAE Appliance

Features and Functionality

Table 6 Features and Functionality

Product	Supported Features and Functionality used in the solution
WAE-7326-K9 WAE-612-K9	Transport Flow Optimization (TFO) Data Redundancy Elimination (DRE), LZ compression

Features, Services, and Application Design Considerations

Most multi-tiered applications support web-based clients in addition to native application clients. Web-based clients use port 80 to communicate to the web server. Applications in this test uses port 80. In the context of the Cisco WAAS, port 80 is accelerated by default, no further configuration in the WAE is necessary unless the application requires ports that are not part of the default application profile. For applications that use TCP ports that is not defined in the default application profile, defining ports to the existing application profile or create a new application profile with the associated ports is required. With the recommended design of Cisco WAAS at the WAN edge, client data only traverse the Cisco WAEs once, at the ingress/egress of the data center. Further application communications between the web servers, application servers and database servers are within the data center, and are not affected by WAAS. TFO, DRE and LZ-compression are enabled by default.

Note However, because Citrix Presentation Server network traffic patterns are small (<64 bytes), TFO only is the optimal Cisco WAAS setting. Careful baselining of each environment is needed to properly tune the Cisco WAAS for these environments.

Each of these features and functionalities are summarized in Table 6. 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 functionalities and continue to work as-is, but with decreased response time and increased traffic throughput and transactions.

Additional information on Cisco WAAS data center and branch designs are available at the following URLs:

- *WAAS Data Center De sign Guide*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c649/ccmigration_09186a008081c7da.pdf
- *WAAS Branch Design Guide*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c649/ccmigration_09186a008081c7d5.pdf

Scalability and Capacity Planning

The CIsco WAE farms can scale up to 32 devices with WCCP and up to 16000 devices with the Cisco ACE load balancing. The Cisco WAAS services scale linearly in a N+1 configuration. In addition to the maximum optimized TCP connections, *fan out ratio* between the DC Cisco WAE and branch Cisco WAE have to be considered. The *fan out ratio* is determined by a number of factors, such as the number of Cisco WAEs in the branch offices, amount of network traffic, and 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.

Table 7 WAE Family Performance and Scalability

Device	Max Optimized TCP Connections	Max CIFS Sessions	Single Drive Capacity [GB]	Max Drives	RAM [GB]	Max Recommended WAN Link [Mbps]	Max Optimized Throughput [Mbps]	Max Core Fan-out [Peers]	CM Scalability [Devices]
NME-WAE-302	250	N/A	80	1	0.5	4	90		
NME-WAE-502	500	500	120	1	1	4	150		
WAE-512-1GB	750	750	250	2	1	8	100	5	500
WAE-512-2GB	1500	1500	250	2	2	20	150	10	1000
WAE-612-2GB	2000	2000	300	2	2	45	250	30	2000
WAE-612-4GB	6000	2500	300	2	4	90	350	50	2500
WAE-7326	7500	2500	300	6	4	155	450	96	
WAE-7341	12000	12000	300	4	12	310	800	200	
WAE-7371	50000	32000	300	6	24	1000	1500	400	

Branch devices ranges from the NME-WAE-302 for very small offices to the 612-4GB or even higher models for bigger branch sites. Cisco WAE 7326 and later products are designed for data center installations.

High Availability

Cisco WAAS deployments are transparent to the application. The application client and server do not know Cisco WAAS is optimizing traffic flows. High availability is built into the WCCP interception. When WCCP is not active or in the events of Cisco WAAS devices not functioning, WCCP will not forward traffic to the WAEs, resulting in unoptimized traffic flow. This is the worse case scenario, traffic flow continues but unoptimized.

Device High Availability

The WAEs have many built-in high availability features. The disk subsystem is recommended to be configured with RAID 1 protection. RAID 1 is mandatory when two or more drives are installed in the WAE. With RAID 1, failure of the physical drive does not affect normal operations. Failed disks can be replaced during planned downtime. Multiple network interfaces are available. Standby interfaces can be configured for interface failover. A standby interface group guards against network interface failure on the WAE and switch. When connected to separate switches in active/standby mode, the standby interface protects the WAE from switch failure.

N+1 Availability

Cisco WAEs and the network provide additional high availability (HA) capabilities. Routers can be configured redundantly providing HSRP or GLBP services. Cisco WAEs can configured in a N+1 configuration. N+1 configuration provides scalability and availability. This design calls for N number of Cisco WAEs for a specific workload, then add a standby Cisco WAE. Since the workload always distributes evenly among the Cisco WAEs, the standby Cisco WAE is used, reducing overall workload. In the event that a Cisco WAE fails, the rest of Cisco WAEs can resume normal workload.

Configuration Task Lists

The following subsections describe the information required prior to configuration of the equipment.

Branch and Data Center Router

The branch and data center router provide WCCP interception points for the Cisco WAAS. Without WCCP interception, the Cisco WAAS does not know where to obtain and optimize traffic flow. Different methods of interception and redirection are support by routers and switches. Redirection methods depends on the speed requirement and router/switch platform. In this deployment, Generic Router Encapsulation (GRE) redirection is used.

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 physical interfaces. Loopback interfaces are always available, there are no physical-tie to them. Other routing protocols also use loopback interfaces as a preferred method for naming the router ID. With IP address tie to a specific physical interface, when the physical interface goes down, the IP address becoming unavailable, causing unexpected issues with WCCP groups.

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 re-route traffic from the interface to the WCCP group. Service 61 redirects ingress traffic and service 62 redirects egress traffic. Both service 61 and 62 are needed to complete redirect bi-directional 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 service 61 and 62 with a password:

```
ip wccp 61 password ANS
ip wccp 62 password ANS
```

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 WAW subnet from interception since we are using a single interface to intercept incoming and outgoing packets. The interception exclusion is required because the router does not discriminate traffic from the Cisco WAE for client/server. Traffic must be redirected to the Cisco WAE after it is optimized by the Cisco WAE; the effect would be forwarding 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 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 service 61 and 62 on the client VLAN. All ingress/egress packets from this VLAN/interface are forwarded to the Cisco WAE for optimization:

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

Step 9 NetFlow statistics is configured for all outbound traffic:

```
ip flow egress
```

Step 10 Configure NTP to synchronize to a master clock. Traffic statistics are captured and forwarded to 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 10.1.6.20
```

Step 11 Configure NetFlow to send information to the collector. Note that NetFlow also uses 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. It is recommended that Cisco WAAS optimize NetFlow transfers.

```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.1.70.10 9995
```

WAE-612-K9, WAE-7326-K9

Step 1 Setup device mode to accelerator. WAE can be setup as application accelerator or Central Manager. Application-accelerator is enabled by default.

```
device mode application-accelerator
```

Step 2 Configure WAE IP address:

```
interface GigabitEthernet 1/0
ip address 13.1.12.2 255.255.255.0
```

Step 3 Setup default gateway:

```
ip default-gateway 13.1.12.1
```

Step 4 Setup primary interface. Cisco WAAS support many type of interfaces including local network failover. Designating a primary interface is required. The Cisco WAAS uses this interface for interception and redirection.

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

Step 5 Enable WCCP version 2:

```
wccp version 2
```

Step 6 Add the router to the router list:

```
wccp router-list 1 13.1.12.1
```

Step 7 setup 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 Setup NTP server. Traffic statistics are capture and forward to Central Manager and NetQoS. The time stamp on each packet needs to be accurate. All WAEs and routers should synchronize to the same NTP server.

```
ntp server 13.1.15.2
```

Step 9 Setup NetFlow to send Cisco WAAS statistics to the NetFlow Aggregator. Note that the host IP address is not the NetFlow Aggregator, but the management station. The management station opens another connection to the WAE to inform the IP address of the Aggregator.

```
flow monitor tcpstat-v1 host 10.1.71.11
flow monitor tcpstat-v1 enable
```

Configuration and Menus

Refer to Appendix A—Cisco ACE Configuration, page 48.

Troubleshooting Configuration

WAE Commands

The following **show** commands can help troubleshoot issues with the Cisco WAE configuration:

- **sh wccp status**—Verifies WCCP V2 is enabled. Example output:

```
WCCP version 2 is enabled and currently active
```

- **sh wccp services**—Verifies WCCP service 61 and 62 is active. Service 61 and 62 must be active. Example output:

```
Services configured on this File Engine
   TCP Promiscuous 61
   TCP Promiscuous 62
```

- **sh wccp routers**—Verifies router can see the WAE. Note that the router ID is the router loopback address. *Sent To* is the router interface on the WAE VLAN. All routers are defined and visible on the WAE. Example output:

```
Router Information for Service: TCP Promiscuous 61
        Routers Configured and Seeing this File Engine(1)
                Router Id       Sent To         Recv ID
                13.1.15.3       13.1.12.1       00040E89
        Routers not Seeing this File Engine
                -NONE-
        Routers Notified of but not Configured
                -NONE-
        Multicast Addresses Configured
                -NONE-

Router Information for Service: TCP Promiscuous 62
        Routers Configured and Seeing this File Engine(1)

                Router Id        Sent To        Recv ID
                13.1.15.3       13.1.12.1               00040E78
        Routers not Seeing this File Engine
                -NONE-
        Routers Notified of but not Configured
                -NONE-
        Multicast Addresses Configured
                -NONE-
```

- **sh tfo connections summary**—Verifies Cisco WAAS clients are using Cisco WAAS for connectivity. Show tfo connections show all optimize path in the WAE. The policy field indicates which optimization method is active for the specified link. F shows the link is fully optimized, that includes DRE, TFO (shown as TCP Optimization), and LZ compression. Pass-through connections are connections that are not optimized at all. Example output:

```
Optimized Connection List
Policy summary order: Our's, Peer's, Negotiated, Applied
F: Full optimization, D: DRE only, L: LZ Compression, T: TCP Optimization

Local-IP:Port         Remote-IP:Port        ConId   PeerId            Policy
13.1.11.3:49520       13.1.40.41:80         43357   00:14:5e:ac:3a:47 F,F,F,F
13.1.11.2:9146        13.1.40.41:80         55532   00:14:5e:ac:3a:47 F,F,F,F

Pass-Through Connections
Local-IP:Port         Remote-IP:Port        Conn Type
13.1.42.54:445        13.1.11.2:5401        PT In Progress
13.1.12.2:42708       13.1.50.6:7878        Internal Client
13.1.41.58:139        172.28.210.61:5425    PT In Progress
13.1.40.53:445        13.1.11.2:5491        PT In Progress
```

- **sh statistics dre**—Checks DRE usage. There are two sections of the statistics. One is encode, traffic coming in to the WAE from the client/server. The WAE needs to compress the incoming traffic with LZ compression then apply DRE. Another is the decode, traffic is coming from the peering WAE, DRE lookup is performed and traffic uncompressed. These statistics are useful for finding compressibility of the data. Example output:

```
Cache:
    Status: Usable, Oldest Data (age): 33d
    Total usable disk size: 118876 MB,  Used: 24.19%
      Hash table RAM  size:    475 MB,  Used: 18.00%

Connections:   Total (cumulative): 41038   Active: 2

Encode:
   Overall: msg:    4058742, in:    606 MB, out:    189 MB, ratio:  68.76%
```

```
        DRE: msg:    4037944, in:    602 MB, out:    484 MB, ratio:  19.56%
DRE Bypass: msg:      20798, in:   3791 KB
         LZ: msg:    1469108, in:    431 MB, out:    131 MB, ratio:  69.40%
 LZ Bypass: msg:    2589634, in:  58894 KB
    Avg latency:      0.180 ms
  Message size distribution:
    0-1K=99%  1K-5K=0%  5K-15K=0%  15K-25K=0%  25K-40K=0%  >40K=0%
Decode:
   Overall: msg:    5114308, in:  13123 MB, out:  15909 MB, ratio:  17.51%
       DRE: msg:    5086542, in:  13342 MB, out:  15908 MB, ratio:  16.13%
DRE Bypass: msg:      27766, in:    505 KB
         LZ: msg:    4490694, in:  11386 MB, out:  11605 MB, ratio:   1.89%
 LZ Bypass: msg:     623614, in:   1737 MB
    Avg latency:      0.244 ms
  Message size distribution:
    0-1K=20%  1K-5K=74%  5K-15K=3%  15K-25K=0%  25K-40K=0%  >40K=0%
```

Router Commands

The following **show** commands can help troubleshoot issues with the configuration:

- **sh ip wccp 61**—Verifies WCCP service 61 and 62 is active. This command shows global WCCP information and how the packets are redirected. Redirect and group access-list issues can easier troubleshoot with this output. Service 62 should also check with the **sh ip wccp 62** command. Example output:

```
Global WCCP information:
    Router information:
        Router Identifier:                    13.1.15.3
        Protocol Version:                     2.0

    Service Identifier: 61
        Number of Service Group Clients:      1
        Number of Service Group Routers:      1
        Total Packets s/w Redirected:         60434039
          Process:                            435
          Fast:                               0
          CEF:                                60433604
        Redirect access-list:                 -none-
        Total Packets Denied Redirect:        0
        Total Packets Unassigned:             414
        Group access-list:                    -none-
        Total Messages Denied to Group:       0
        Total Authentication failures:        9
        Total Bypassed Packets Received:      0
```

- **sh ip wccp 61 detail**—Checks WCCP client hash or Layer 2 assignments. This command also check the status of the WCCP client, namely the WAEs. sh ip wccp 61 shows global WCCP information, this command shows detailed WCCP client information. Hashing assignments (WAE bucket assignments), client ID, and client status are found on this output. Example output:

```
WCCP Client information:
        WCCP Client ID:          13.1.12.2
        Protocol Version:        2.0
        State:                   Usable
        Initial Hash Info:       FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:          256 (100.00%)
        Packets s/w Redirected:  15107709
```

```
Connect Time:            4d05h
Bypassed Packets
  Process:               0
  Fast:                  0
  CEF:                   0
  Errors:                0
```

- **sh ip wccp interface detail**—Verifies which interface has WCCP configured. Identify all interfaces within a router or switch that has WCCP configured with ingress or egress for exclude-in redirection. Another way to get this information is from sh run and look through each interface. Example output:

```
WCCP interface configuration details:
    Vlan300
        Output services: 1
        Static:          None
        Dynamic:         062
        Input services:  1
        Static:          None
        Dynamic:         061
        Mcast services:  0
        Exclude In:      FALSE

    Vlan301
        Output services: 0
        Input services:  0
        Mcast services:  0
        Exclude In:      TRUE
```

- **sh ip wccp 61 view**—Verifies WCCP group membership. Need to check service 62 as well. Example output:

```
WCCP Routers Informed of:
    13.1.15.3
WCCP Clients Visible:
    13.1.12.2
WCCP Clients NOT Visible:
    -none-
```

Results and Conclusions

The testing verified the following.

Figure 9 Bandwidth Savings—1.544 Mbps Circuit

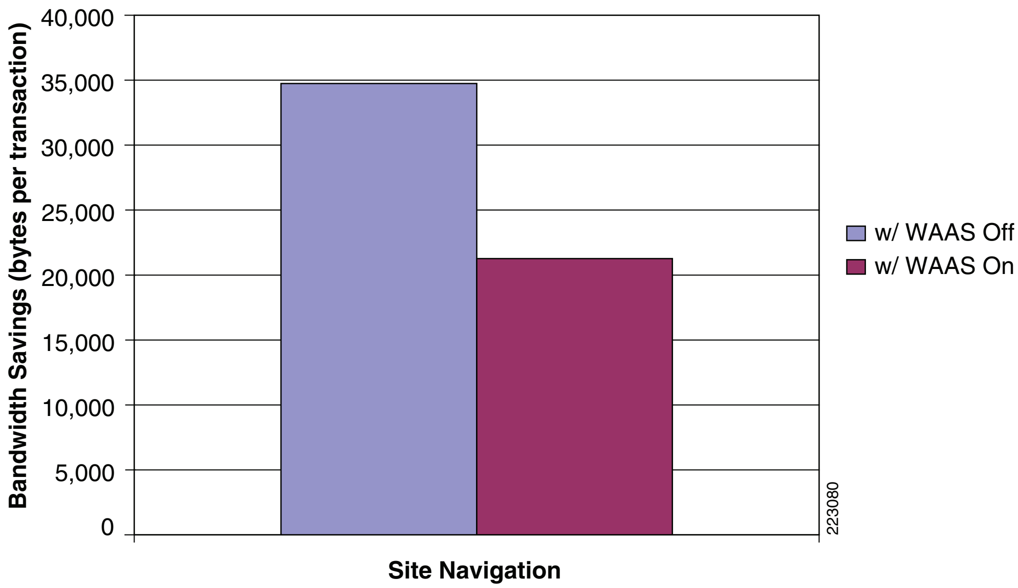
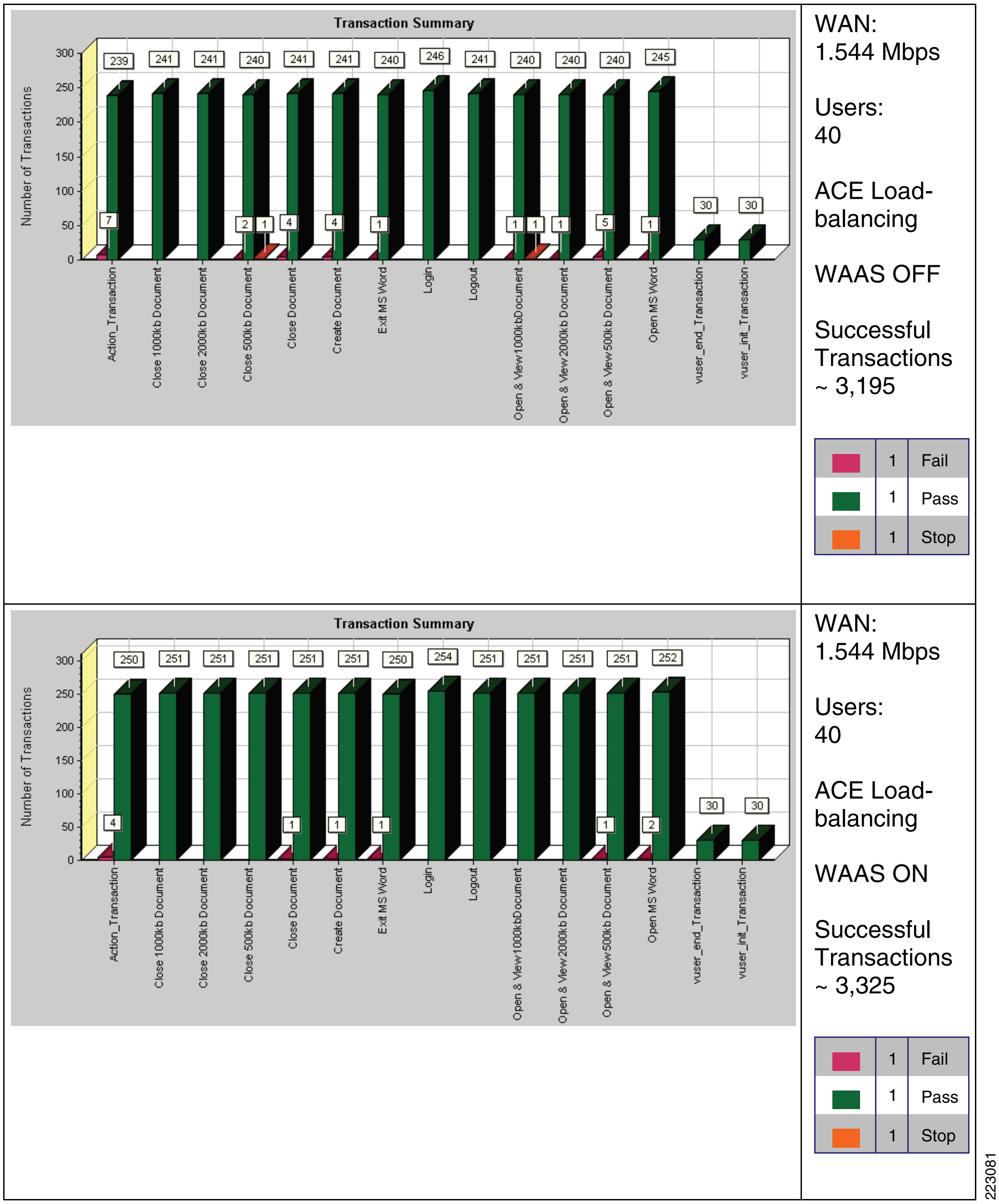


Figure 9 provides the amount data volume transversing the 1.544 Mbps WAN link with and without the WAAS device that was observed during in a 30-minute cycle with 40 users performing MS Word Navigation from Citrix Presentation Server. The Cisco WAAS device reduces the amount of unnecessary data volume that transverses the WAN by locally caching data and using compression algorithms on the data the must transverse the WAN. As shown in the Figure 9 above, the Cisco WAAS-enabled network becomes more efficient as less data must transverse the WAN.

With this efficiency, the end-user transaction times are faster and more transactions can occur as shown in Figure 10. Figure 10 illustrates the number of transactions that were observed for the same 30-minute cycle.

Figure 10 Transaction Summary—1.544 Mbps (WAAS Off)



The following characteristics apply to the chart provided in Figure 10 (top chart):

- WAN: 1.544 Mbps
- Users: 40
- Cisco ACE load-balancing
- WAAS OFF
- Successful Transactions: ~ 3195

The following characteristics apply to the chart provided in Figure 10 (bottom chart):

- WAN: 1.544 Mbps
- Users: 40
- Cisco ACE load-balancing
- WAAS ON
- Successful Transactions: ~ 3,325

Figure 11 Bandwidth Savings—512 Kbps Circuit

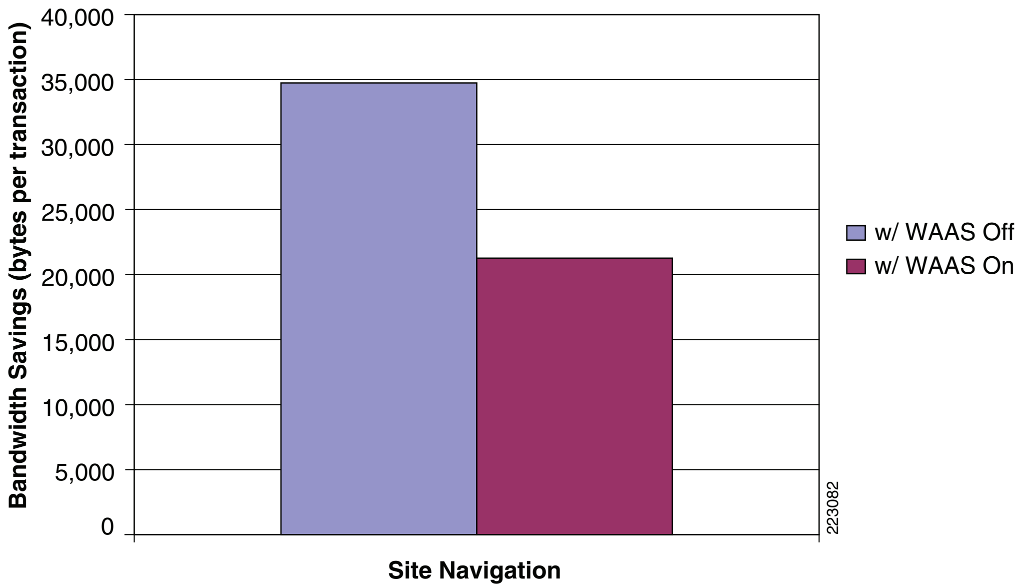
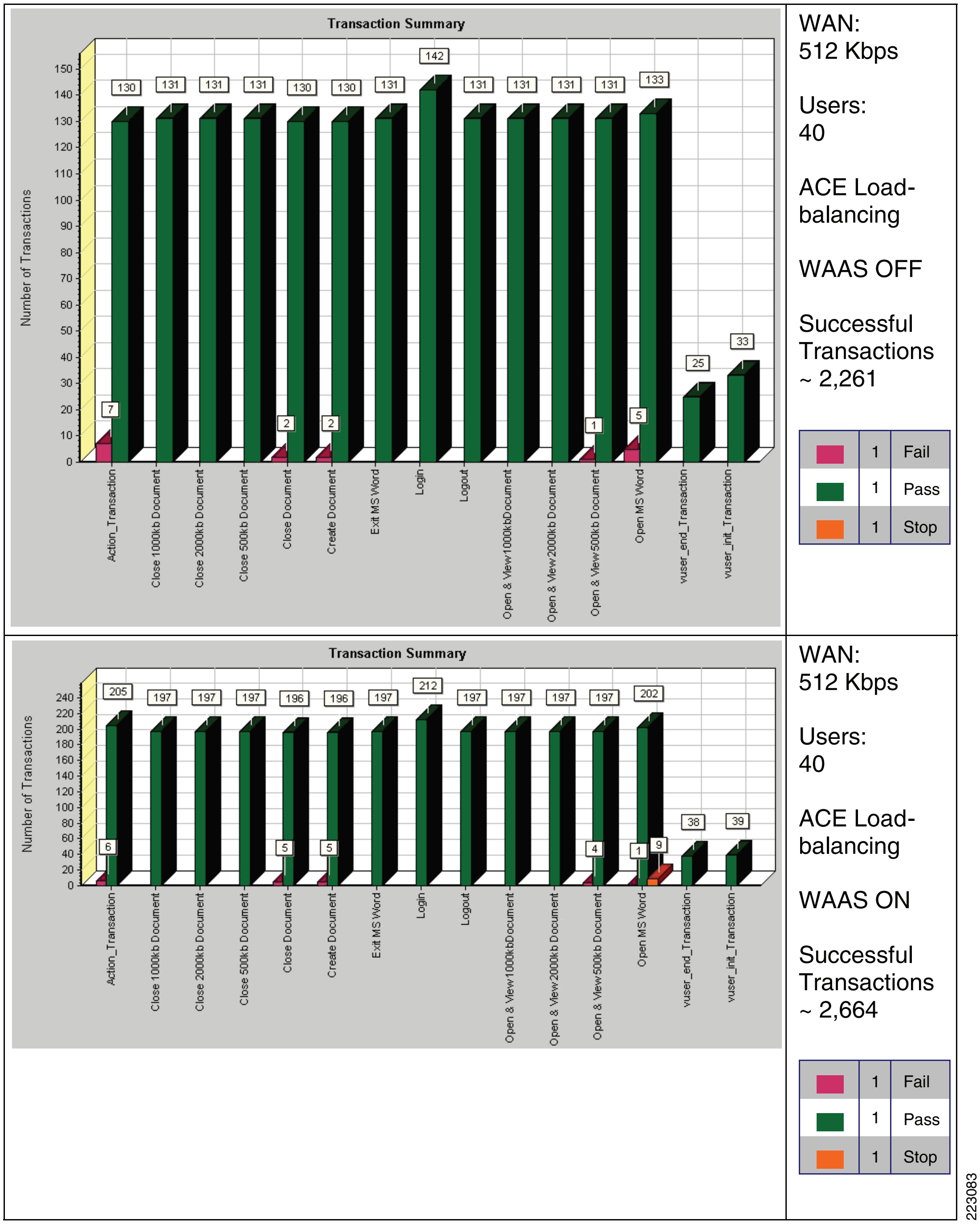


Figure 11 provides the amount data volume transversing the 512 Kbps WAN link with and without the Cisco WAAS device that was observed during a 30-minute cycle with 40 users performing MS Word Navigation from Citrix Presentation Server. The Cisco WAAS device reduces the amount of unnecessary data volume that will transverse the WAN by locally caching data and using compression algorithms on the data the must transverse the WAN. As shown in Figure 11 above, the Cisco WAAS-enabled network becomes more efficient as less data must transverse the WAN.

With this efficiency, the end-user transaction times are faster and more transactions can occur as shown in the Figure 12. Figure 12 illustrates the number of transactions that were observed for the same 30-minute cycle.

Figure 12 Transaction Summary—512 Kbps (WAAS Off)



The following characteristics apply to the chart provided in Figure 12 (top chart):

- WAN: 512 Kbps
- Users: 40
- Cisco ACE load-balancing
- WAAS OFF

- Successful Transactions: ~ 2261

The following characteristics apply to the chart provided in Figure 12 (bottom chart):

- WAN: 512 Kbps
- Users: 40
- Cisco ACE load-balancing
- WAAS ON
- Successful Transactions: ~ 2664

Figure 13 and Figure 14 illustrate the benefit of total transaction time of a user navigating the MS Word with or without Cisco WAAS optimization. The results indicate marginal speedup of transaction time on both circuits due to the majority of Citrix network traffic being keyboard entries and mouse clicks (send/acknowledgements). These packets are small and very chatty.

Figure 13 Transaction Time Savings—1.544 Mbsp Circuit

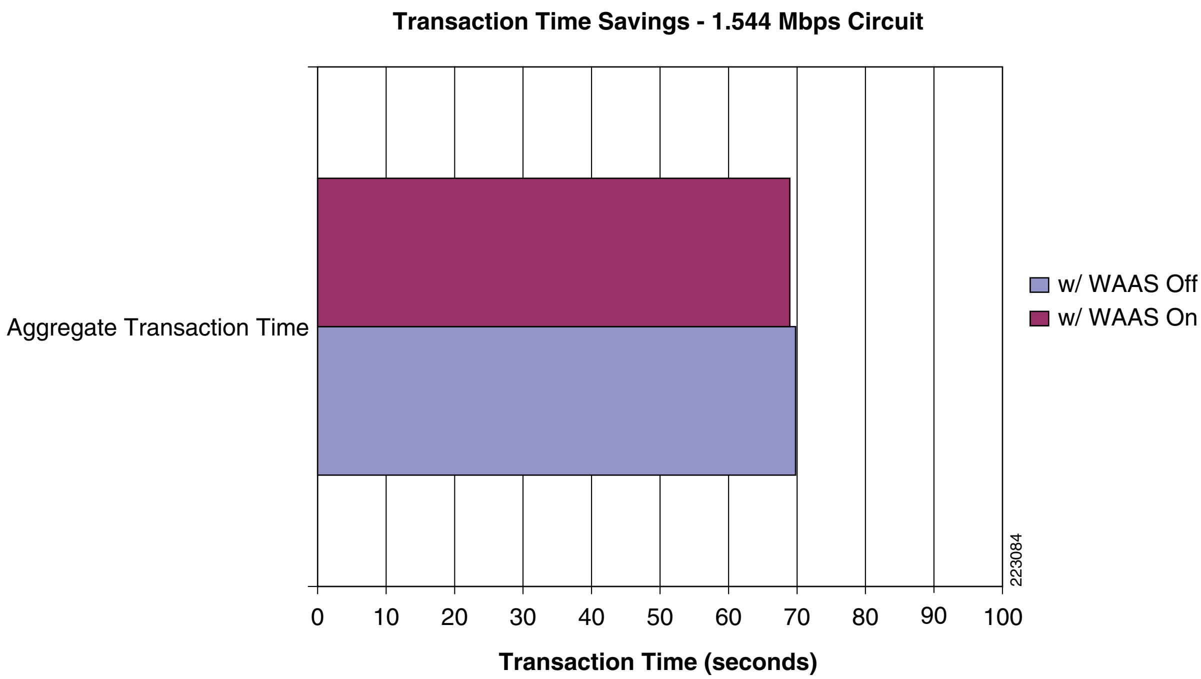
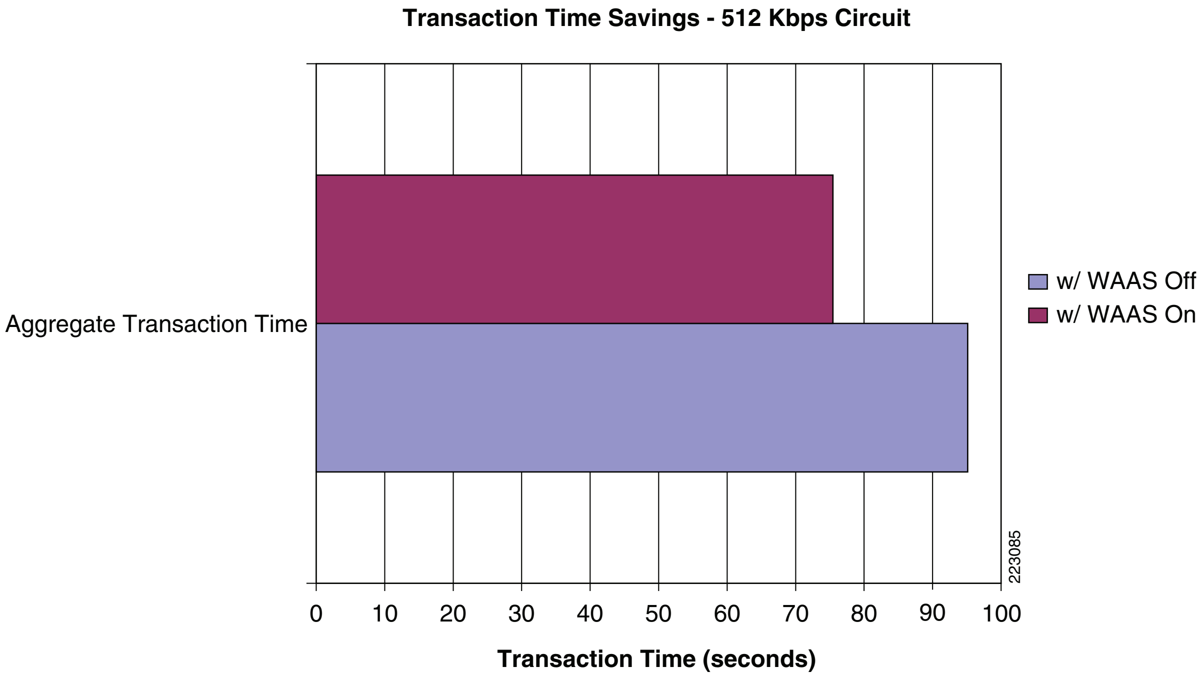


Figure 14 Transaction Time Savings—512Kbps Circuit



Network Management

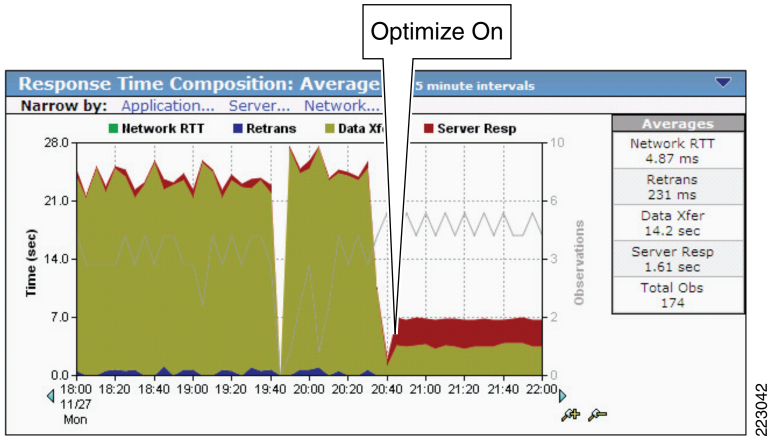
This section only focuses on the network management system (NMS) used to monitor and provide results indicating the benefits of Cisco WAAS optimization. The NMS tool used was NetQoS SuperAgent with NetQoS Collector and Reporter. NetQoS Collector gathers the pre-optimized traffic and reports the data to the NetQoS SuperAgent. The NetQoS SuperAgent provides details on the protocols and applications tranversing the network(s), including:

- Response Time
- Data Transfer Time
- Retransmission Delay
- Network Round Trip Time
- Effective Network Round Trip Time
- Performance by Server
- Performance by Network

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

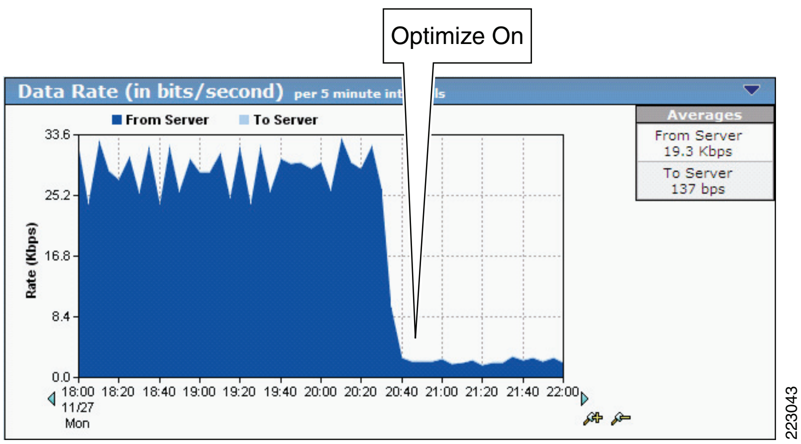
NetQoS Reporter gathers the optimized traffic and reports the data to the NetQoS Super Agent. NetQoS Super Agent uses the data from the NetQoS Collector (un-optimized) and compares it to the optimized traffic, showing the benefits of optimization using the Cisco WAAS as shown in Figure 15, Figure 16, and Figure 17.

Figure 15 Benefit of Optimization Using the Cisco WAAS—Application Response Time



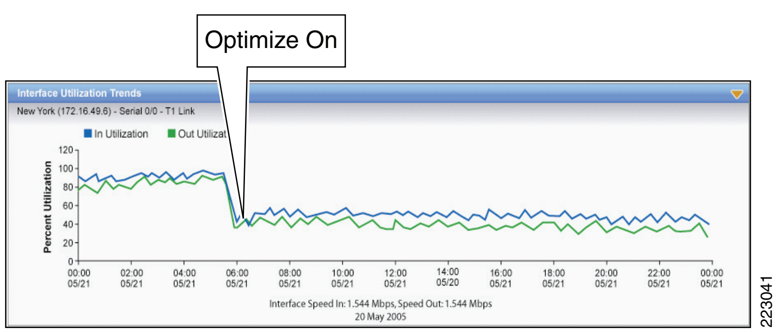
Application Response Time

Figure 16 Benefit of Optimization Using the Cisco WAAS—Application Data Rate



Application Data Rate

Figure 17 Benefit of Optimization Using the Cisco WAAS—Link Utilization



Link Utilization

NetQoS devices passively listen in by using the rspan feature of the Cisco routers and switches. They do not poll servers, hence do not add server load. For more information about this tool, refer to:

http://www.netqos.com/CiscoWAASSolutions/Cisco_WAAS_overview.html

Appendix A—Cisco ACE Configuration

ACE Admin Context

```
Generating configuration....

interface gigabitEthernet 1/1
  description 3750-1
  switchport trunk allowed vlan 11,21,31,171
  no shutdown
interface gigabitEthernet 1/2
  description 3750-2
  no shutdown
interface gigabitEthernet 1/3
  switchport access vlan 50
  no shutdown
interface gigabitEthernet 1/4
  description connection to WANRTR
  switchport trunk allowed vlan 10,20,30,170,500
  no shutdown

resource-class CX-resource
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 0.01 maximum unlimited
resource-class IN-resource
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 0.01 maximum unlimited
resource-class CX-resource
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 0.01 maximum unlimited

boot system image:c4710ace-mz.3.0.0_AB0_0.500.bin
hostname DCACE1



access-list anyone line 10 extended permit ip any any
access-list anyone line 11 extended permit icmp any any
access-list anyone line 12 extended permit tcp any any






class-map type management match-any remote-access
  10 match protocol icmp any
  20 match protocol telnet any
  30 match protocol ssh any
  40 match protocol snmp any
  50 match protocol http any
  60 match protocol https any

policy-map type management first-match remote-mgt
```

```
  class remote-access
    permit

interface vlan 10
  ip address 10.1.10.7 255.255.255.0
  service-policy input remote-mgt
  no shutdown
interface vlan 20
  ip address 10.1.20.100 255.255.255.0
  no shutdown
interface vlan 30
  ip address 10.1.30.100 255.255.255.0
  peer ip address 10.1.30.200 255.255.255.0
  service-policy input remote-mgt
  no shutdown
interface vlan 100
  ip address 10.1.100.100 255.255.255.0
  no shutdown
interface vlan 500
  ip address 10.50.50.2 255.255.255.0
  no shutdown

ft interface vlan 50
  ip address 1.1.1.1 255.255.255.0
  peer ip address 1.1.1.2 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 50
ft group 2
  peer 1
  peer priority 99
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 10.1.30.1

context citrix
  description CITRIX Testing
  allocate-interface vlan 20-21
  member CX-resource
context inotes
  description INOTES Testing
  allocate-interface vlan 10-11
  member IN-resource
context peoplesoft
  description PEOPLESOFT Testing
  allocate-interface vlan 30-31
  member CX-resource



ft group 3
  peer 1
  peer priority 99
  associate-context inotes
  inservice
ft group 4
  peer 1
  peer priority 99
  associate-context citrix
  inservice
```

```
ft group 5
  peer 1
  peer priority 99
  associate-context peoplesoft
  inservice
username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/  role Admin domain
default-domain
username www password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/  role Admin domain de
fault-domain


DCACE1/Admin#
```

ACE Citrix Context

```
access-list anyone line 10 extended permit ip any any
access-list anyone line 11 extended permit icmp any any
access-list anyone line 12 extended permit tcp any any


probe tcp PROBE-TCP
  interval 2
  faildetect 2
  passdetect interval 10
  passdetect count 2



rserver host CX1
  ip address 10.1.21.50
  inservice
rserver host CX2
  ip address 10.1.21.51
  inservice
rserver host CX3
  ip address 10.1.21.52
  inservice

serverfarm host CX1
  predictor leastconns
  probe PROBE-TCP
  rserver CX1
    inservice
  rserver CX2
    inservice
  rserver CX3
    inservice

sticky ip-netmask 255.255.255.0 address both app-ipstky
  serverfarm CX1

class-map match-any CX-VIP
  2 match virtual-address 10.1.20.10 any
class-map type management match-any remote-access
  10 match protocol icmp any
  20 match protocol telnet any
  30 match protocol ssh any
  40 match protocol snmp any
  50 match protocol http any
  60 match protocol https any

policy-map type management first-match remote-mgt
```

```
  class remote-access
    permit
policy-map type loadbalance first-match CX-VIP-l7slb
  class class-default
    sticky-serverfarm app-ipstky
policy-map multi-match int20
  class CX-VIP
    loadbalance vip inservice
    loadbalance policy CX-VIP-l7slb
    loadbalance vip icmp-reply

interface vlan 20
  ip address 10.1.20.5 255.255.255.0
  alias 10.1.20.2 255.255.255.0
  peer ip address 10.1.20.6 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  service-policy input int20
  no shutdown
interface vlan 21
  ip address 10.1.21.2 255.255.255.0
  alias 10.1.21.1 255.255.255.0
  peer ip address 10.1.21.3 255.255.255.0
  access-group input anyone
  access-group output anyone
  service-policy input remote-mgt
  no shutdown

role RSERVER-MOD
  rule 1 permit modify feature rserver

ip route 0.0.0.0 0.0.0.0 10.1.20.1
username citrix password 5 $1$sr6JQVjF$P4cvnETg/9GDD08OoM6Of.  role RSERVER-MOD
domain default-domain
username cisco_test password 5 $1$6/390Zp/$nWVnDmC9uSp8gYIAT6mKV0  role Network-
Monitor domain default-domain
```

Appendix B—Cisco WAE Configurations

Branch Cisco WAE Configuration

```
! WAAS version 4.0.13 (build b12 Aug  9 2007)
! Configure this device to function as a WAAS Engine
device mode application-accelerator
!
!
hostname ANS-EDGE
!
!
clock timezone US/Pacific -7 0
!
!
ip domain-name cisco.com
!
!
!
primary-interface GigabitEthernet 1/0
!
```

```
!
! Connect to the branch router
interface GigabitEthernet 1/0
 ip address 10.1.101.2.2 255.255.255.0
 exit
!
! This is the address of interface vlan301 on the branch router.
ip default-gateway 10.1.101.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 171.70.168.183
!
!
! Designate the server for network time protocol
ntp server 10.1.10.1
!
!
wccp router-list 1 10.1.101.1
wccp tcp-promiscuous router-list-num 1 password ****
wccp version 2
!
!
!
snmp-server community ANSwerLab
!
!
!
windows-domain netbios-name "ANS-EDGE"
!
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
flow monitor tcpstat-v1 host 10.1.71.11
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
!
no adapter epm enable
!
! The application traffic is traversing the WAN using port 80. The default policy
configured on the WAE will be applied. Note that the application configuration can be
modified to any port.
policy-engine application
...
   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 NetQoS
```

```
      match dst port eq 7878
   exit
! Full optimization is applied to the application WAN traffic
   map basic
      name NetQoS classifier NetQoS action optimize full
...
      name Web classifier HTTP action optimize full
      name Web classifier HTTPS action optimize DRE no compression none
...
! End of WAAS configuration
```

Data Center Cisco WAE Configuration

```
! WAAS version 4.0.13 (build b12 Aug  9 2007)
! Configure this device to function as a WAAS Engine
device mode application-accelerator
!
!
hostname ANS-CoreWAE
!
!
clock timezone US/Pacific -7 0
!
!
ip domain-name cisco.com
!
!
!
primary-interface GigabitEthernet 1/0
!
!
! Connect to the data center WAN edge router
interface GigabitEthernet 1/0
 ip address 10.1.100.100.2 255.255.255.0
 exit
!
!
! This is the address of interface GigabitEthernet2/0 on data center WAN edge router.
ip default-gateway 10.1.100.100.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
!
! Designate the server for network time protocol
ntp server 10.1.10.1
!
!
wccp router-list 1 10.1.100.100.1
wccp tcp-promiscuous router-list-num 1 password ****
wccp version 2
!
!
!
snmp-server community ANSwerLab
!
!
!
windows-domain netbios-name "ANS-COREWAE"
!
```

```
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
!
flow monitor tcpstat-v1 host 10.1.71.11
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
! The application traffic is traversing the WAN using port 80. The default policy
configured on the WAE will be applied. Note that the application configuration can be
modified to any port.
policy-engine application
...
   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 NetQoS
      match dst port eq 7878
   exit
! Full optimization is applied to the application WAN traffic
   map basic
      name NetQoS classifier NetQoS action optimize full
...
      name Web classifier HTTP action optimize full
      name Web classifier HTTPS action optimize DRE no compression none
...
! End of WAAS configuration
```

Appendix C—References

Enterprise Data Center Wide Area Application Services Design Guide

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c649/ccmigration_09186a008081c7da.pdf

Cisco Advanced Services

Cisco Services Help Accelerate and Optimize ANS Deployments

Application deployments are complex projects. Cisco Services can help mitigate the risk of making changes to the environment and accelerate deployment of Cisco ANS solutions. Our product and technology expertise is constantly enhanced by hands-on experience with real-life networks and broad exposure to the latest technology and implementations. Cisco uses leading practices to help our customers define their IT and business requirements and help them deliver fast, secure and highly available application access in a scalable environment.

- The Cisco Application Control Engine Planning and Design Service helps customers accelerate deployment of a Cisco ACE solution for fast, secure application access in a scalable environment.
- The Cisco Application Control Engine Optimization Services help customers continuously update and optimize their Cisco Application Control Engine solution as their applications delivery environment changes.
- The Cisco Wide Area Application Services Planning and Design Service helps customers accelerate deployment of Cisco WAAS solutions and improve application responsiveness across their wide area networks.
- The Cisco Wide Area Application Services Optimization Services help customers maintain or improve application responsiveness across wide area network as their business changes and grows.
- The Cisco Application Profiling Service helps customers host and manage applications more effectively while preserving application performance, security, and availability.

Cisco ANS Services:

http://www.cisco.com/en/US/products/ps6892/serv_group_home.html

http://www.cisco.com/en/US/products/ps6894/serv_group_home.html