Cisco Application Networking for IBM WebSphere Portal Deployment Guide

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

Preface

Document Purpose

To address challenges associated with today's mission critical enterprise application deployments, Cisco offers an enterprise network architecture for the ANS WebSphere solution with best practices and implementation guidance that optimizes application availability, performance, and security and lowers application ownership costs.

Featuring the Cisco Application Control Engine (ACE) and Wide Area Application Services (WAAS) product families, collectively known as Cisco Application Networking Services (ANS), that provide data center, branch, and remote end user application optimization services, the solution addresses the following challenges for ANS WebSphere deployments:

- Recovery time and point objectives for business continuity
- End user performance over limited Wide Area Network (WAN) connections
- Security for service-oriented application architectures (SOA)
- Reduced capital and operational costs

The purpose of this document is to describe the ANS WebSphere Solution enterprise network architecture and deployment best practices and guidance.

Prerequisites

The following prerequisites are required to deploy the IBM WebSphere Solution:

- Working knowledge of the WebSphere application
- Experience with basic networking and troubleshooting
- Experience installing the Cisco products covered by this network design, including the Cisco ACE and WAAS product families
- Working knowledge of Cisco's 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 ANS WebSphere Solution.
Implementing and Configuring the Cisco ACE Solution	Describes configuration and implementation of Cisco ACE within the ANS WebSphere Solution.

Section	Description
Implementing and Configuring the Cisco WAAS Solution	Describes configuration and implementation of WAAS within the ANS WebSphere Solution.
Network Management	Describes the network management software used in the ANS WebSphere Solution.

Solution Overview

Solution Description

The ANS WebSphere Solution offers optimized WebSphere application availability, performance, security, and costs by providing application optimization services as follows:

- Application availability

  Cisco ACE product family application optimization services for high WebSphere 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 WebSphere high performance:

  - WAN optimization—Provides intelligent caching, compression, and protocol optimization.
  - Server offloading—Specialized hardware that offers greater processing efficiency for application optimization services listed below, such as server load balancing, Secure Socket Layer termination, and traffic compression, which frees up to 50 percent of application server processing and memory to focus on business logic computations.
  - Server load balancing—Substitutes for WebSphere 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 WebSphere native server health monitoring.
  - Traffic compression—Scalable LZ compression functionality.
  - Object caching—Reduce requests to server.

- Application security

  Cisco ACE product family application optimization services for optimized WebSphere data security:

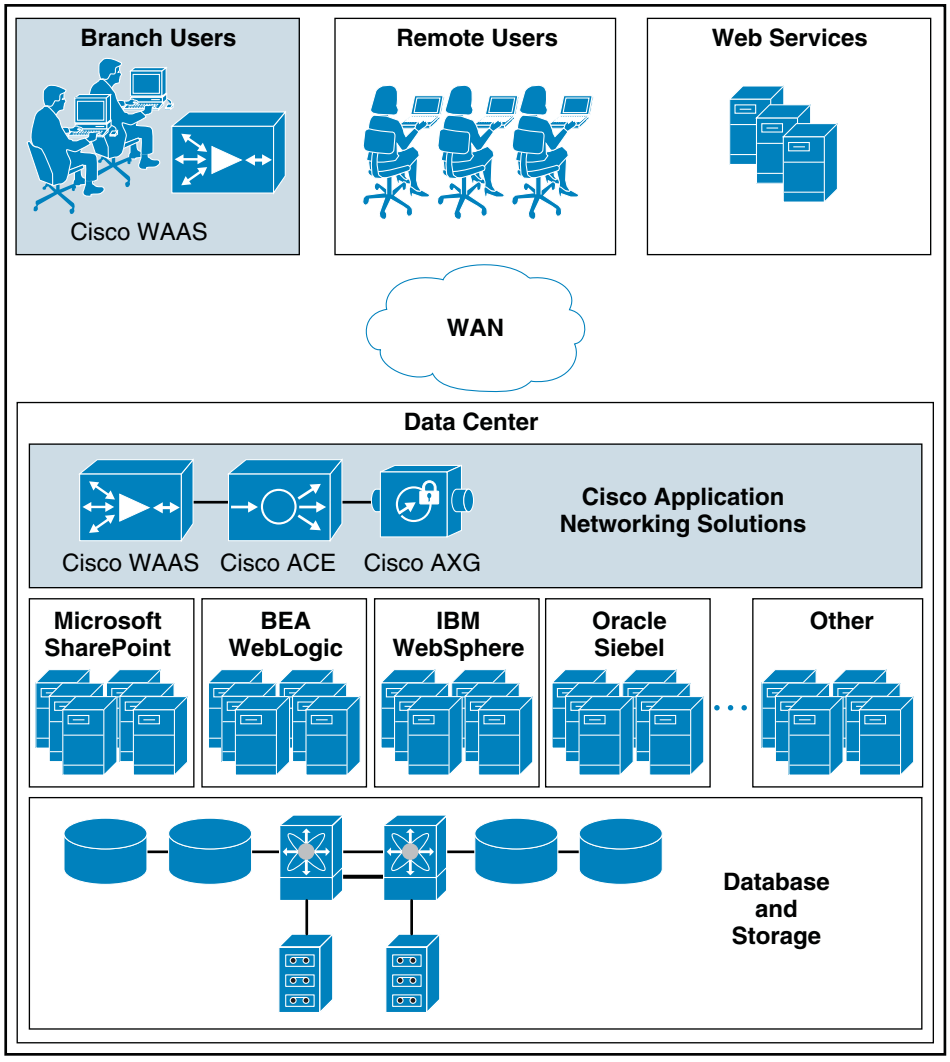
  - SSL termination—Efficiently encrypts and decrypts SSL enabled traffic, which facilitates the use of intrusion detection and prevention solutions before traffic reaches the servers.

  - 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 supplies such services for multiple WebSphere instances as well as other enterprise applications (see Figure 1). Specifically, a single physical Cisco ACE can be virtualized into multiple logical Cisco ACEs in which application traffic can traverse between virtualized Cisco ACEs. This virtualization of load balancing is an exclusive Cisco feature.

Figure 1 Virtualization of Application Optimization Services



The application optimization services of the ANS WebSphere Solution reside in both 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 WebSphere instances 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 WebSphere Portal application servers, including server 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 WebSphere Portal 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.

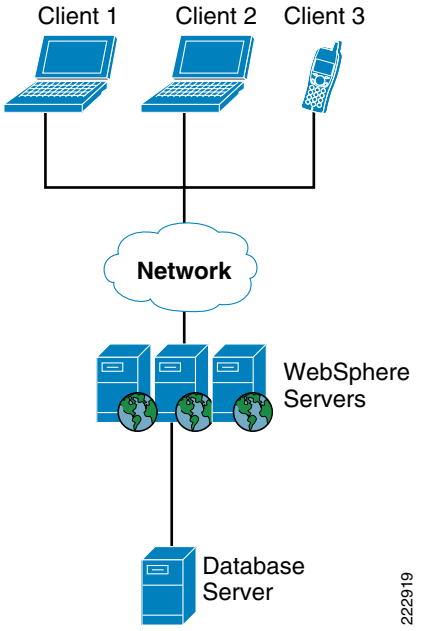
- Wide area application optimization services

  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 WebSphere Portal application servers respond to end-user requests, Cisco WAAS compresses the response and then most efficiently passes it 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.

WebSphere refers to a broad category of IBM software products. It sets up and integrates enterprise applications across multiple computers using Web technologies. It includes both the run-time components and the development tools for applications. Enterprise applications are often deployed in a three-tier approach: client tier, middle tier, and data tier (see Figure 2). WebSphere software manages the middle tier.

Figure 2 WebSphere Manages the Middle Tier in a Three-Tier Model

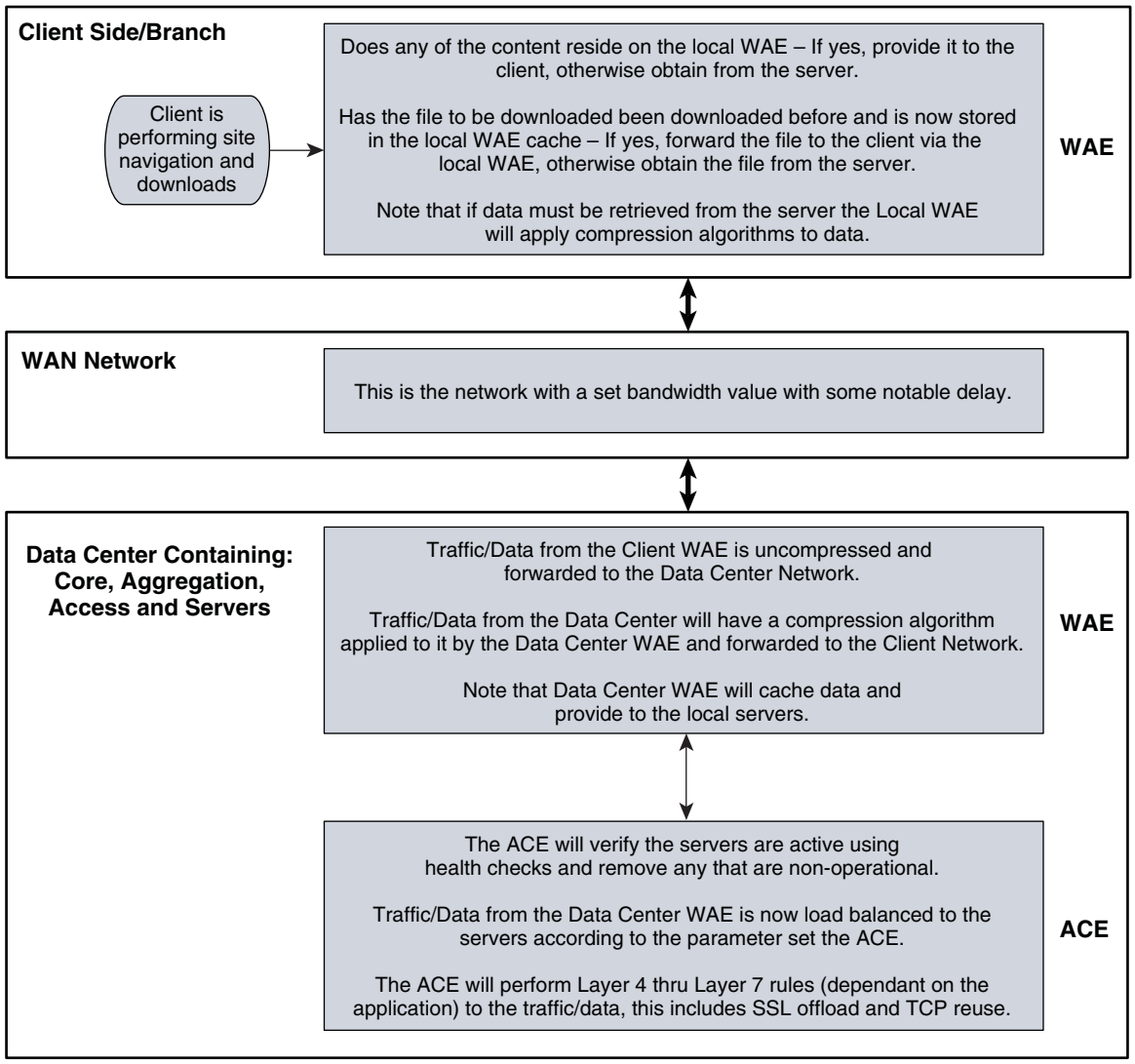


One of the WebSphere products, WebSphere Portal, manages a variety of enterprise applications and supports application development and delivery. In the ANS WebSphere Solution, content development and document management functions of WebSphere Portal were tested.

Note The Cisco Wide Area Application Services (WAAS) software runs on the Cisco Wide-Area Application Engine (WAE).

Process Flow

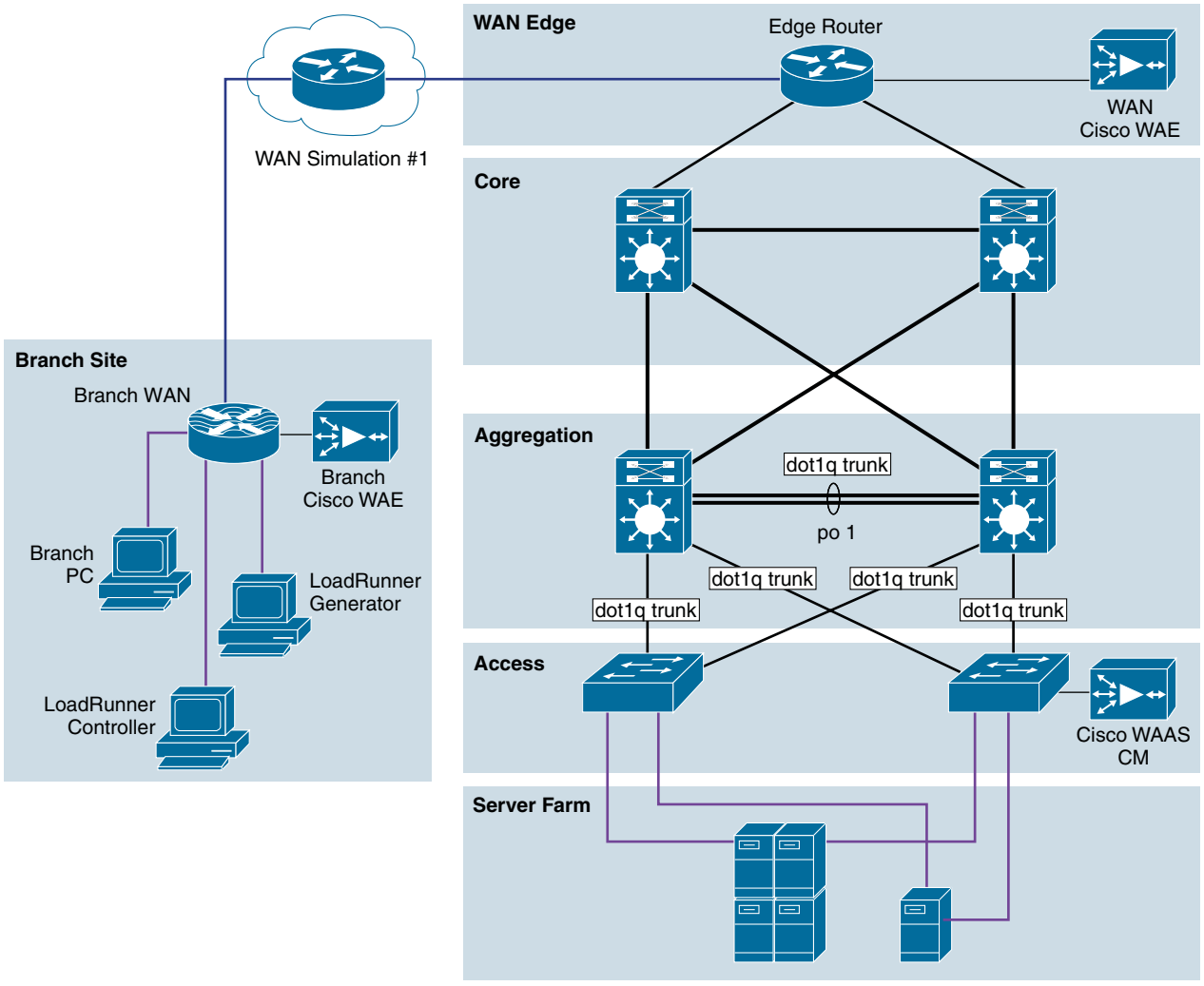
Figure 3 Process Flow



Solution Architecture

Application and Application Networking Architecture

Figure 4 Application and Application Networking Architecture



The ANS solution uses WAAS to enhance performance and Cisco ACE to reduce the load on resources in the server farm. The 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 ANS Solution architecture is based on the Enterprise Branch Wide Area Application Services Design Guide (Enterprise Branch Design) and the Data Center Infrastructure Design Guide 2.1, both found at www.cisco.com/go/srnd.

In the ANS 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 via 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 provides simulations of the following WAN links:

1. WAN Type 1 (Intracontinental or T1)
   a. Bandwidth - 1.544 Mbps, ESF, B8ZS, Delay - 100 mS, Loss - drop one packet in every 1000 packets (0.1%)
2. WAN Type 2 (Intercontinental)
   a. Bandwidth - 512 Kbps, ESF, B8ZS, Delay - 200 mS, Loss - drop one packet in every 500 packets (0.2%)

Data Center

The data center (DC) follows the design guidelines found in the 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, and access Ethernet switching, and the server farm where the application resides. In this document, the focus is on the DC WAN router, aggregation, and the server farm. The core Ethernet switching provides routing to and from the DC WAN router and the aggregation. The access Ethernet switching provides Layer 2 connectivity for the server farms to the aggregation.

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

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

Included in the data center is the Cisco WAAS central manager (CM), which runs on the Cisco WAE Appliance. The Cisco WAAS CM provides a centralized mechanism for configuring Cisco WAAS features and 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 CM 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 central management system (CMS). The CMS process provides SSL-encrypted bidirectional configuration synchronization of the Cisco WAAS CM 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 WAEs. Cisco WAEs that are not available to receive the changes will receive them the next time the appliances become available.

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

- Virtualization—Virtualization is device partitioning into multiple contexts, where each context can be configured for different applications and is independent of any others. In the Joint Solution, Cisco ACE is configured with the Admin context and the SharePoint context. Note that the Cisco ACE can support up to 250 contexts.
- Session persistence—Session persistence is the ability to forward client requests to the same server for the duration of the session. MOSS requires either source Internet Protocol (IP) based session persistence or Hypertext Transfer Protocol (HTTP) cookie based session persistence.
- Transparent interception—Transparent interception performs a Network Address Translation (NAT) function to conceal the real server IP address that is residing in the server farm. The SharePoint context is configured with a Virtual IP (VIP) that provides a single address that users use to connect to the server farm. This allows users to access the MOSS application by placing a single IP in the Web browser.
- Allowed server connections—Allowed server connections is the maximum number of active connections value on a per-server basis and/or globally to the server farm.
- Health monitoring—Health monitoring is used to track the state of the server and determine its ability to process connections in the server farm. The SharePoint context used a compound probe to determine if servers are operational and responding to HTTP requests.

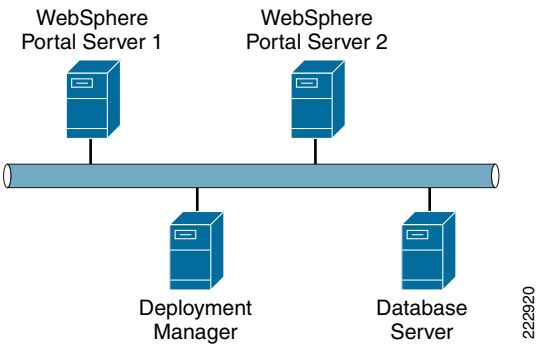
Cisco ACE provides load balancing of the traffic to the server farm using one of the following methods: Round Robin, Weighted Round Robin, Least Connections, Hash address, Hash cookie, Hash Header, and Hash URL. In the Joint Solution, Least Connections was used, which selects the server with the fewest number of server connections. Cisco ACE is also used to provide SSL offload and TCP reuse.

Inter-chassis Cisco ACE redundancy was used, in which a Cisco ACE module in one Cisco Catalyst 6500 Series Switch chassis is protected by a Cisco ACE module in a peer Cisco Catalyst 6500 Series Switch chassis connected by a fault tolerant (FT) VLAN. The FT VLAN is used to transmit flow-state information, configuration synchronization information, and the redundancy heartbeat.

Server Farm

The server farm consisted of two IBM WebSphere Portal servers, a deployment manager, and an IBM DB2 database (see Figure 5). The two WebSphere portal servers are not only connected to the database server, but also to the deployment manager. A deployment manager acts as a coordinator of the multiple WebSphere portal servers. If there is only one portal server, a deployment manager is not needed. If there is more than one portal server, a deployment manager is required.

Figure 5 Server Farm



The WebSphere Portal servers run IBM WebSphere Portal Express v6.0. Each of the WebSphere Portal servers resides on the Windows 2003 enterprise server operating system. Dual Xeon processors running at 2.33 Ghz with 4 G of RAM and 4 80 G SATA hard drives were used.

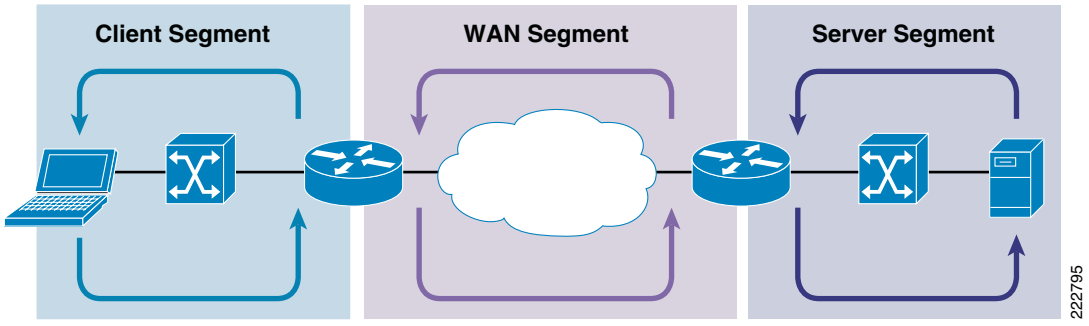
The IBM WebSphere deployment manager runs IBM WebSphere Application Server Network Deployment version 6.0. The deployment manager resides on the Windows 2003 enterprise server operating system. Dual Xeon processors running at 2.33 Ghz with 4 G of RAM and 4 80 G SATA hard drives were used.

The IBM DB2 database version is 8.1.7. The IBM DB2 resides on the Windows 2003 enterprise server operating system. Dual Xeon processors running at 2.33 Ghz with 4 G of RAM and 4 80 G SATA hard drives were used. The gigabit network interface cards are “nic-teamed” for redundancy.

Packet Flow Without Cisco WAAS and Cisco ACE

Application packet flow from a remote site can be categorized into three segments, client, WAN, and server.

Figure 6 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 residing 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 service level agreement (SLA). The WAN inherently introduces delay and packet loss to the data traffic (packets).

Server Segment

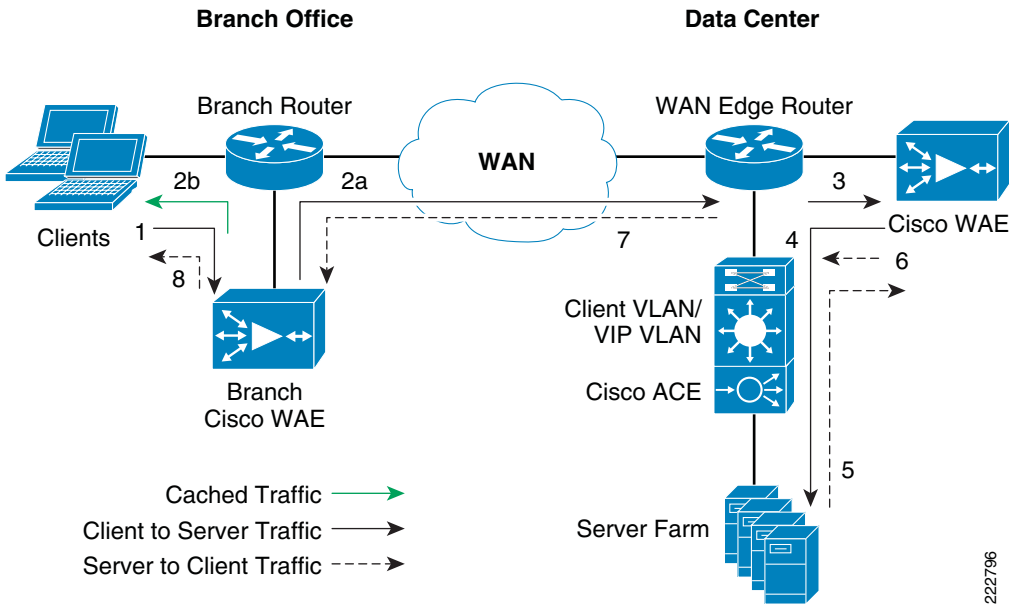
The server segment consists of a highly available and resilient core, aggregation, and access Ethernet switching. The core routes the data traffic to and from the WAN and the aggregation layer. The aggregation layer provides consolidation of multiple access layers and routes the access layer traffic 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 time consists of server response time and WAN round trip time. 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 Cisco WAAS and Cisco ACE

Figure 7 Packet Flow with Cisco WAAS and Cisco ACE



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

1. The client sends a TCP SYN (synchronize) 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.
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.
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.
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.
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.
6. The data center Cisco WAE sends the packet to the WAN edge router.
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.
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 module used in this solution is deployed in a Cisco Catalyst 6509 switch in the data center aggregation layer. The Cisco ACE module is deployed in routed mode where the client and server side VLANs each support unique IP subnets. In this deployment mode the Cisco ACE acts as the default gateway for the application servers.

What Was Implemented

Key features implemented on the Cisco ACE module to support this application are:

- Layer 4/Layer 7 load balancing
- Persistence based on source IP address, server cookie, or Cisco ACE-inserted cookie
- Server health monitoring
- Connection replication for stateful failover

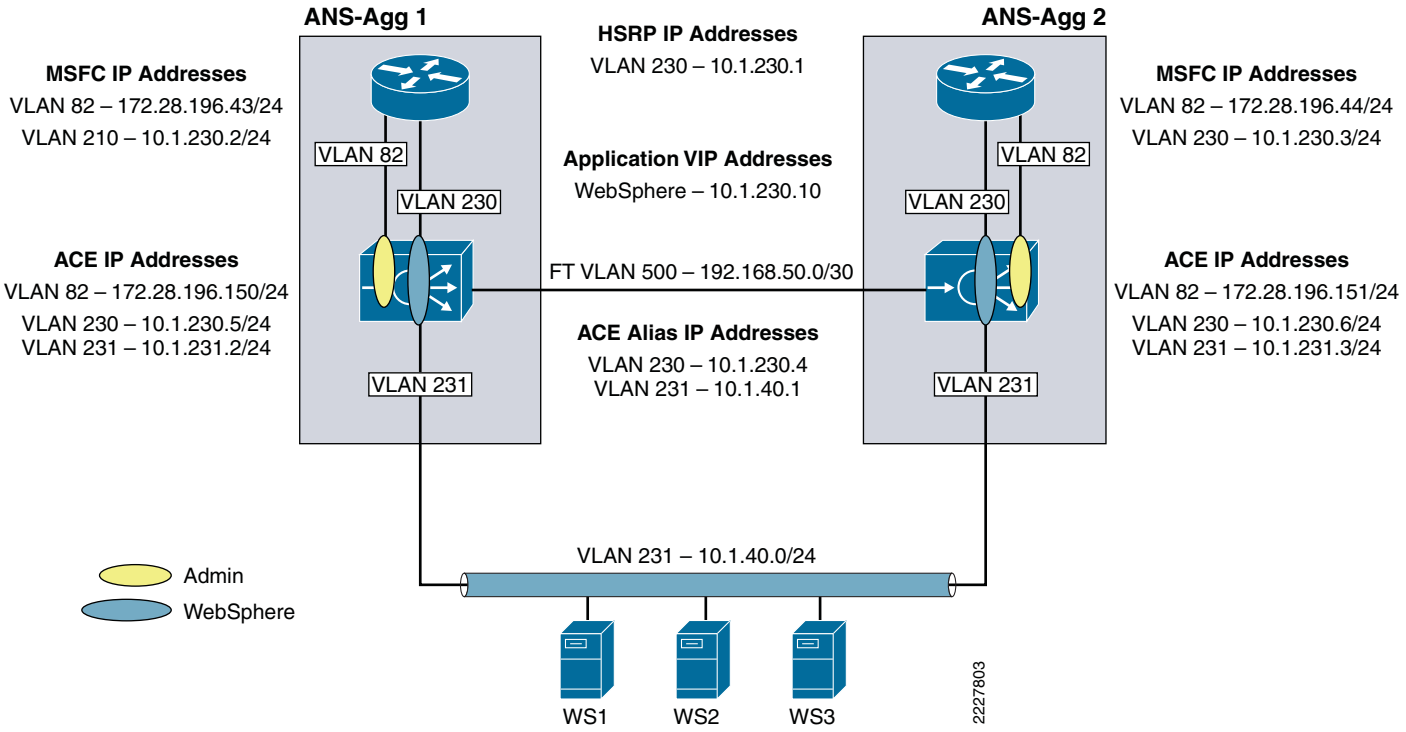
What Was Not Implemented/Tested

The following was not implemented in this solution:

- SSL offload
- TCP reuse

Network Topology

Figure 8 Network Topology



Hardware or Components

Table 1 Hardware

Product	Chassis	Modules	Interfaces	Memory
ACE20-MOD-K9	Must be inserted into a Cisco Catalyst 65XX chassis	N/A	Console port	957928 kB

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

Software

Table 2 Software

Product	Software/Code Version
SC6K-3.0.0A14-ACE	c6ace-t1k9-mz.3.0.0_A1_6_1.bin
ACE-VIRT-250	ACE-VIRT-250
ACE-SSL-20K-K9	ACE-SSL-20K-K9
ACE10-16G-LIC	ACE10-16G-LIC
ACE-08G-LIC	ACE-08G-LIC

Features and Functionality

Table 3 Features and Functionality

Product	Features and Functionality Used in the Solution
ACE20-MOD-K9	• Virtualization • Load balancing • Session persistence • Server health monitoring • SSL offload (up to 15,000 SSL sessions via licensing) • TCP reuse • Transparent interception support for redundant configurations (intra-chassis, inter-chassis, inter-context)

Features, Services, and Application Design Considerations

WebSphere servers support active cookie persistence, passive cookie persistence, and SSL persistence. In terms of the Cisco ACE, active cookie persistence is the Cisco ACE cookie insert feature which is used for the ANS WebSphere solution. The Cisco ACE inserts the cookie on behalf of the server upon the return request, so the Cisco ACE can perform cookie stickiness even when the servers are not configured to set cookies. The cookie contains information that the Cisco ACE uses to ensure persistence to a specific real server. Refer to Configuration Task Lists and Appendix A—Cisco ACE Configuration for configuration information.

High Availability, Scalability, and Redundancy

The Cisco ACE also offers multitiered redundancy, availability, and scalability for maximum protection. It is the only product in the industry that offers three types of high availability:

- Inter-chassis—A Cisco ACE in one Cisco Catalyst 6500 is protected by a Cisco ACE in a peer Cisco Catalyst 6500.
- Intra-chassis—A Cisco ACE in a Cisco Catalyst 6500 is protected by another Cisco ACE in the same Cisco Catalyst 6500 (the Cisco Catalyst 6500 has solid redundancy built in).
- Inter-partition—Cisco ACE supports high availability between virtual partitions configured across two modules to allow specific partitions to fail over without affecting the other partitions and applications on a given module.

All these application availability modes provide rapid, stateful application redundancy with replication of connection state and sticky tables.

Inter-chassis and Inter-partition redundancy is used in the ANS WebSphere solution. Refer to Configuration Task Lists and Appendix A—Cisco ACE Configuration for configuration information.

Configuration Task Lists

This section describes the steps necessary to configure the equipment.

Installing Cisco ACE and MSFC Configuration

A Cisco ACE module interacts with clients and servers via VLANs that are set up in Cisco Catalyst 6500 Series/Cisco 7600 Series Supervisor Engine 720 (Sup 720). These VLANs must be configured on Sup720 to be allowed to be sent to the Cisco ACE module. Without this configuration, by default Cisco ACE does not receive any traffic from any VLAN.

The following sample configuration steps are performed on the MSFC. Refer to Appendix A—Cisco ACE Configuration for a complete configuration.

Step 1 Add Cisco ACE VLANs and database server VLAN. For example:

```
vlan 230
 name ACE-CLIENT
!
vlan 231
 name ACE-SERVER
!
vlan 500
 name ACE-FT-VLAN
!
```

Step 2 Add the SVCLC configuration.

For this deployment, Cisco ACE is installed in slot 3 in the Cisco Catalyst 6500 chassis. The following configuration needs to be added to allow Cisco ACE-specific VLAN traffic to be directed towards Cisco ACE:

```
svclc multiple-vlan-interfaces
svclc module 3 vlan-group 1
svclc vlan-group 1 230,231,500
```

Step 3 Add the Switch Virtual Interface (SVI) configuration.

The SVI (interface VLAN) configuration defines Layer 3 instance on the router MSFC. The Cisco ACE client side VLAN SVI configuration is:

```
interface Vlan230
 description ACE Client Side VLAN
 ip address 10.1.230.2 255.255.255.0
```

```
standby 230 ip 10.1.230.1
standby 230 Priority 120
```

Virtualization

Virtualization is a method to allocate available resources into two or more contexts for security and management purposes. Up to 250 (5 with no additional license requirements) contexts can be configured on Cisco 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

Sample context configuration steps are:

Step 1 Configure resource-class(es):

```
ACE_1/Admin(config)# resource-class Gold
  <cr>  Carriage return.
```

The different resources that can be segmented are:

```
ACE_1/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 amount of regular expression memory
  sticky             Limit number of sticky entries
  xlates             Limit number of Xlate entries
```

Step 2 Configure context(s):

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

```
context websphere
  description WebSphere Testing
  allocate-interface vlan 230-231
  member Gold
```

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

```
ACE_1/Admin# changeto websphere
```

Redundancy/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.

```
ACE_1/Admin(config)# ft interface vlan 500 Create a VLAN interface for the FT traffic
ACE_1/Admin(config-ft-intf)# ip address 192.168.50.1 255.255.255.252
ACE_1/Admin(config-ft-intf)# peer ip address 192.168.50.2 255.255.255.252
ACE_1/Admin(config-ft-intf)# no shutdown
ACE_1/Admin(config)# ft peer 1  Configure FT peer for this ACE module
ACE_1/Admin(config-ft-peer)# ft-interface vlan 500  Assign FT VLAN to this peer
ACE_1/Admin(config-ft-peer)# heartbeat count 10
ACE_1/Admin(config-ft-peer)# heartbeat interval 300
ACE_1/Admin(config)# ft group 1  Create a fault tolerance group
ACE_1/Admin(config-ft-group)# peer 1
ACE_1/Admin(config-ft-group)# priority 200
ACE_1/Admin(config-ft-group)# preempt
ACE_1/Admin(config-ft-group)# associate-context Admin  Admin context, ACTIVE in this ACE
ACE_1/Admin(config-ft-group)# inservice  Enable this FT group
ACE_1/Admin(config)# ft group 3  Create a fault tolerance group
ACE_1/Admin(config-ft-group)# peer 1
ACE_1/Admin(config-ft-group)# priority 200
ACE_1/Admin(config-ft-group)# associate-context websphere WebSphere context, ACTIVE in
this ACE
ACE_1/Admin(config-ft-group)# inservice  Enable this FT group
```

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

Remote Management Access

To access the Cisco ACE module remotely using Telnet, SSH, SNMP, HTTP, or HTTPS or to allow ICMP access to the Cisco ACE module, a policy must be defined and applied to the interface(s) the access is entering.

The configuration steps in this section are required for both the Admin context and the application context. The following example is for the application context. Refer to Appendix A—Cisco ACE Configuration for a complete configuration.

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
50 match protocol https any
```

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 230
  service-policy input REMOTE-ACCESS
```

```
interface vlan 231
service-policy input REMOTE-ACCESS
```

Configuring Interface(s) and Default Gateway

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

The configuration steps in this section are required for both the Admin context and the application context. The following example is for the application context. Refer to Appendix A—Cisco ACE Configuration for a complete configuration.

Step 1 Define an access-list to permit/deny traffic through Cisco ACE. For example:

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

Step 2 Configure IP address and network mask of the interface(s):

```
interface vlan 230
  ip address 10.1.230.5 255.255.255.0
  peer ip address 10.1.230.6 255.255.255.0
  alias 10.1.230.4 255.255.255.0

interface vlan 231
  ip address 10.1.50.2 255.255.255.0
  peer ip address 10.1.50.3 255.255.255.0
  alias 10.1.50.1 255.255.255.0
```

Step 3 Apply management access policy and access-group to the interface(s), no shut of the interface(s):

```
interface vlan 230
  access-group input ANYONE
  access-group output ANYONE
  service-policy input REMOTE-ACCESS
  no shutdown
interface vlan 231
  access-group input ANYONE
  access-group output ANYONE
  service-policy input REMOTE-ACCESS
 no shutdown
```

Step 4 Default gateway can be configured as:

```
ip route 0.0.0.0 0.0.0.0 10.1.230.1
```

Step 5 Verify interfaces are recognized by MSFC and operational.

Type **show interface** and verify the VLANs are up and assigned from the supervisor.

Here is an example of a working output:

```
vlan230 is up
  Hardware type is VLAN
  MAC address is 00:1b:d5:9b:88:ed
  Virtual MAC address is 00:0b:fc:fe:1b:02
  Mode : routed
  IP address is 10.1.230.5 netmask is 255.255.255.0
  FT status is active
  Description:Client side vlan
  MTU: 1500 bytes
```

```
  Last cleared: never
  Alias IP address is 10.1.230.4 netmask is 255.255.255.0
  Peer IP address is 10.1.230.6 Peer IP netmask is 255.255.255.0
  Assigned from the Supervisor, up on Supervisor
     53808467 unicast packets input, 17900167965 bytes
     7331701 multicast, 7776 broadcast
     0 input errors, 0 unknown, 0 ignored, 0 unicast RPF drops
     91028995 unicast packets output, 5455629020 bytes
     4 multicast, 5202 broadcast
     0 output errors, 0 ignored

vlan231 is up
  Hardware type is VLAN
  MAC address is 00:1b:d5:9b:88:ed
  Virtual MAC address is 00:0b:fc:fe:1b:02
  Mode : routed
  IP address is 10.1.231.2 netmask is 255.255.255.0
  FT status is active
  Description:Server side vlan
  MTU: 1500 bytes
  Last cleared: never
  Alias IP address is 10.1.231.1 netmask is 255.255.255.0
  Peer IP address is 10.1.231.3 Peer IP netmask is 255.255.255.0
  Assigned from the Supervisor, up on Supervisor
     83222640 unicast packets input, 95861661879 bytes
     1118208 multicast, 47974 broadcast
     0 input errors, 0 unknown, 0 ignored, 0 unicast RPF drops
     53089290 unicast packets output, 4304456323 bytes
     4 multicast, 14950 broadcast
     0 output errors, 0 ignored
```

Probes

Cisco ACE uses probe, one of the 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 Cisco ACE:

```
ACE_1/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 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 qualify a server to declared probe failed. faildetect is configured as a counter value. The default value is 3. Generally, the faildetect value is left at the default value.
- interval—Refers to how frequently Cisco ACE sends probe to a server. The interval is configured in seconds. The default value is 120 seconds. Generally, the interval is configured around 5-10 seconds depending upon the applications and size of the environment.
- passdetect—Determines how Cisco ACE re-probes the server after it has been declared failed. The passdetect variable has two attributes:
  - passdetect count—Refers to how many consecutive successful responses Cisco ACE needs 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 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 in the 15-30 seconds range.

These additional parameters should be configured for TCP, HTTP, and HTTPS probes:

- Open—Refers to the time (in seconds) that 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 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 as equal to or less than the value interval.
- Connection—This parameter determines how Cisco ACE closes the connection after it has successfully sent a probe. By default, Cisco ACE closes the connection gracefully, which means it sends TCP FIN to close the connection. Optionally, Cisco ACE can be configured to close the connection with a TCP RESET by configuring connection term forced.
- Port—TCP/UDP port number on which this probe is sent. The default values for various probes are:
  - TCP—port 80
  - UDP—port 53
  - HTTP—port 80
  - HTTPS—port 443
- Request—Used to configure the 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—Allows Cisco ACE to detect two values from the server:
  - expect status—The HTTP status code (or range) to expect from the server. There is no default HTTP return code expected; it has to be explicitly configured.
  - 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—Configured to define what cipher and SSL version Cisco ACE should use when sending an HTTPS probe. Ciphers and SSL versions supported on Cisco ACE are:

```
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.

The following are configurations for TCP and ICMP:

- TCP probe:

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

- ICMP probe:

```
probe icmp PING
  interval 2
  faildetect 2
```

Real Server

Load balancer selects the real servers (called rserver in 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 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 load balancer selects based on certain sets of criteria. As with real server, serverfarm name is also case sensitive.

Basic server farm configuration includes adding rservers and probes to the server farm.

Key configuration options within server farm sub-configuration mode are:

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

  A configurable option is failaction purge, which forces 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 are:
  - hash—Based on source/destination IP address, URL, cookie, and header
  - leastconns—Based on least number of connections. By default slow start is enabled for leastconns 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—Allows a probe to be applied to the server farm. Multiple probes can be applied to the same server farm.
- retcode—Used to configure server health-checks based on the HTTP return code. The configuration allows you 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—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—When configured, Cisco ACE does not NAT Layer 3 IP address from VIP to real server's IP address.

The following is an example of basic server farm configuration:

```
serverfarm host WEBSPHERE
  predictor leastconns
  probe ICMP
  rserver WL1
    inservice
  rserver WL2
    inservice
```

Layer 4 Load Balancing

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 address on a certain port can be used as classifiers for Layer 4 load balancing as the classification is only based on destination IP and destination port.

Note In the WebSphere configuration, Layer 4 load balancing was not used. Instead Layer 7 load balancing was used and is discussed in Layer 7 Load Balancing.

The following example shows the configuration steps needed:

Step 1 Configure virtual IP address (VIP) using class-map of type match-all:

```
class-map match-all VIP-HTTP-10
  2 match virtual-address 10.1.230.10 tcp eq 7041
```

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

```
policy-map type loadbalance first-match VIP-POLICY-10
  class class-default
    sticky-serverfarm SRC-IP-STICKY
```

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 LB-VIP
  class VIP-HTTP-10
    loadbalance vip inservice
    loadbalance policy VIP-POLICY-10
    loadbalance vip icmp-reply
```

Step 4 Apply policy-map to the interface VLAN:

```
interface vlan 230
  service-policy input LB-VIP
```

Layer 7 Load Balancing

Similar to Layer 4 policy, Cisco ACE uses class-map, policy-map, and service-policy to classify and enforce a Layer 7 policy. Cisco ACE uses additional information such as URL, HTTP header, or cookie to make a load balancing decision. The following example shows the configuration steps for URL-based matching. Similar steps can be used for cookie or header matching.

The following example shows the configuration steps needed:

Step 1 Configure class-map of type HTTP:

```
class-map type http loadbalance match-any L7-URL
2 match http url .*.htm
```

Step 2 Configure HTTP parameters (optional):

```
parameter-map type http L7-map
case-insensitive
```

Step 3 Configure virtual IP address (VIP) using class-map of type match-all:

```
class-map match-all VIP-HTTP-10
  2 match virtual-address 10.1.230.10 tcp eq 7041
```

Step 4 Configure policy-map of type loadbalance to associate server farm:

```
policy-map type loadbalance first-match L7-match
  class L7-URL
sticky-serverfarm STICKY-INSERT-COOKIE
  class class-default
    serverfarm WEBSPHERE
```

Step 5 Configure policy-map of type multi-match to associate class-map configured in step 1 above. See SSL Termination for configuring SSL VIP.

```
policy-map multi-match LB-VIP
class VIP-HTTP-10
    loadbalance vip inservice
    loadbalance policy L7-match
    loadbalance vip icmp-reply
```

Step 6 Apply policy-map to the interface VLAN:

```
interface vlan 230
  service-policy input LB-VIP
```

Stickiness (Session Persistence)

Session persistence or sticky configuration allows multiple connections from the same client to be sent to the same real server by Cisco ACE. Cisco ACE supports stickiness based on source/destination (or both) IP address and HTTP cookies. Cisco ACE insert cookie persistence is when the Cisco ACE inserts the cookie on behalf of the server upon the return request, so that the Cisco ACE can perform cookie stickiness even when the servers are not configured to set cookies. The cookie contains information that the Cisco ACE uses to ensure persistence to a specific real server.

The following are the sample configurations for various sticky types along with working demonstrations.

Cisco ACE Inserted Cookie Stickiness

The following steps are needed to configure stickiness based on Cisco ACE inserted cookie:

Step 1 Configure a sticky group:

```
sticky http-cookie acecookie STICKY-INSERT-COOKIE
  cookie insert
  serverfarm
```

Step 2 Apply sticky group to a loadbalance Layer 7 policy as a sticky-serverfarm:

```
policy-map type loadbalance first-match L7-MATCH
  class L7-URL
    sticky-serverfarm STICKY-INSERT-COOKIE
  class class-default
    serverfarm WEBSPHERE
```

Step 3 Apply load balance policy to a multimatch policy:

```
policy-map multi-match LB-VIP
  class VIP-HTTP-10
    loadbalance vip inservice
    loadbalance policy L7-MATCH
    loadbalance vip icmp-reply
```

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

```
interface vlan 230
  description Client side vlan
  ip address 10.1.230.5 255.255.255.0
  alias 10.1.230.4 255.255.255.0
  peer ip address 10.1.230.6 255.255.255.0
  access-group input ANYONE
  service-policy input LB-VIP
  service-policy input REMOTE-MANAGEMENT
  no shutdown
```

SSL Termination

SSL termination configuration on Cisco ACE provides SSL traffic termination on Cisco ACE instead of on the servers. This allows the offloading of server resources and also provides HTTP request inspection for various load balancing functionalities.

Front End SSL Termination

With SSL termination on the Cisco ACE, client to Cisco ACE traffic is SSL encrypted, but Cisco ACE to server traffic is clear-text. The configuration steps to implement front end SSL termination are:

Step 1 Generate key:

```
ACE_1/testfeature# crypto generate key 512 testkey.key
ACE_1/testfeature# show crypto key all
Filename                                 Bit Size Type
--------                                 -------- ----
testkey.key                              512      RSA
```

Step 2 Define CSR parameters set:

```
crypto csr-params testparams
  country US
  state California
  locality SJ
  organization-name AS
  organization-unit TAS
  common-name www.testssl.com
  serial-number cisco123
```

Step 3 Generate csr:

```
ACE_1/testfeature# crypto generate csr testparams testkey.key
-----BEGIN CERTIFICATE REQUEST-----
MIIBHjCByQIBADBkMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEL
MAkGA1UEBxMCU0oxCzAJBgNVBAoTAkFTMQwwCgYDVQQLEwNUQVMxGDAWBgNVBAMT
D3d3dy50ZXN0c3NsLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC+xphqQJn9
EOzOhkFfVCVO5SYJj7nVjWmaslVZOi7TYKzFgXtJexMt0Y1VyO7XY+U5XdZuvoxE
cO4rdAGzo84HAgMBAAGgADANBgkqhkiG9w0BAQQFAANBAAL9EzKcYyOrL3XYc7YG
STgpa1B8tTpCpJIVwrHwolyK3OzvfudLTbF7CQ2V3jUYS//sf2Cei8fe+voKIQE9
nI4=
-----END CERTIFICATE REQUEST-----
```

Step 4 Obtain certificate:

An SSL certificate can be obtained from various Certificate Authority (CA) companies like VERISIGN. The following example shows using a CISCO router as a CA:

```
OS-CA-SERVER#crypto pki server CDN-CA request pkcs10 terminal pem
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE REQUEST-----
MIIBHjCByQIBADBkMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEL
MAkGA1UEBxMCU0oxCzAJBgNVBAoTAkFTMQwwCgYDVQQLEwNUQVMxGDAWBgNVBAMT
D3d3dy50ZXN0c3NsLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC+xphqQJn9
EOzOhkFfVCVO5SYJj7nVjWmaslVZOi7TYKzFgXtJexMt0Y1VyO7XY+U5XdZuvoxE
cO4rdAGzo84HAgMBAAGgADANBgkqhkiG9w0BAQQFAANBAAL9EzKcYyOrL3XYc7YG
STgpa1B8tTpCpJIVwrHwolyK3OzvfudLTbF7CQ2V3jUYS//sf2Cei8fe+voKIQE9
nI4=
-----END CERTIFICATE REQUEST-----
Quit
```

```
% Granted certificate:
-----BEGIN CERTIFICATE-----
MIIB6TCCAVKgAwIBAgIBCTANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZDRE4t
Q0EwHhcNMDYwNDI2MTgxNjQzWhcNMDcwNDI2MTgxNjQzWjBkMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcm5pYTELMAkGA1UEBxMCU0oxCzAJBgNVBAoTAkFT
MQwwCgYDVQQLEwNUQVMxGDAWBgNVBAMTD3d3dy50ZXN0c3NsLmNvbTBcMA0GCSqG
SIb3DQEBAQUAA0sAMEgCQQC+xphqQJn9EOzOhkFfVCVO5SYJj7nVjWmaslVZOi7T
YKzFgXtJexMt0Y1VyO7XY+U5XdZuvoxEcO4rdAGzo84HAgMBAAGjQjBAMB8GA1Ud
IwQYMBaAFNKc5JGHmabT17tofs9CUD8mxVURMB0GA1UdDgQWBBQAL2ptyfN85SoV
NdEiGRav8nI8lTANBgkqhkiG9w0BAQQFAAOBgQAUHyfbs+aMapSEFXmdlKPh8F67
gGuYBdyWxmXjR7KVErDxde+4UqJCkNP4R2m11g30j6UveG2wLiP7C4IZHzGfFXUb
zdPhaZ1838qgZlFn+lXPtCrayto1PitWeuPbCwLTxmE2vWWLw6lwEzguVbF+6t0n
mLAkyiYsuz/MOiql/g==
-----END CERTIFICATE-----

IOS-CA-SERVER#
```

Step 5 Import certificate on Cisco ACE:

```
ACE_1/testfeature# crypto import terminal testcert.pem
Please enter PEM formatted data. End with "quit" on a new line.
 -----BEGIN CERTIFICATE-----
 MIIB6TCCAVKgAwIBAgIBCTANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZDRE4t
 Q0EwHhcNMDYwNDI2MTgxNjQzWhcNMDcwNDI2MTgxNjQzWjBkMQswCQYDVQQGEwJV
 UzETMBEGA1UECBMKQ2FsaWZvcm5pYTELMAkGA1UEBxMCU0oxCzAJBgNVBAoTAkFT
 MQwwCgYDVQQLEwNUQVMxGDAWBgNVBAMTD3d3dy50ZXN0c3NsLmNvbTBcMA0GCSqG
 SIb3DQEBAQUAA0sAMEgCQQC+xphqQJn9EOzOhkFfVCVO5SYJj7nVjWmaslVZOi7T
 YKzFgXtJexMt0Y1VyO7XY+U5XdZuvoxEcO4rdAGzo84HAgMBAAGjQjBAMB8GA1Ud
 IwQYMBaAFNKc5JGHmabT17tofs9CUD8mxVURMB0GA1UdDgQWBBQAL2ptyfN85SoV
 NdEiGRav8nI8lTANBgkqhkiG9w0BAQQFAAOBgQAUHyfbs+aMapSEFXmdlKPh8F67
 gGuYBdyWxmXjR7KVErDxde+4UqJCkNP4R2m11g30j6UveG2wLiP7C4IZHzGfFXUb
 zdPhaZ1838qgZlFn+lXPtCrayto1PitWeuPbCwLTxmE2vWWLw6lwEzguVbF+6t0n
 mLAkyiYsuz/MOiql/g==
 -----END CERTIFICATE-----
 quit
```

Step 6 Validate certificate using key:

```
ACE_1/testfeature# crypto verify testkey.key testcert.pem
Keypair in testkey.key matches certificate in testcert.pem.
```

Step 7 Configure SSL parameters and SSL proxy service:

a. SSL parameter configuration:

```
parameter-map type ssl sslparams
  cipher RSA_WITH_RC4_128_MD5
 version SSL3
```

b. SSL proxy service configuration:

```
ssl-proxy service testssl
  key testkey.key
  cert testcert.pem
  ssl advanced-options sslparams
```

Step 8 Configure class-map (for VIP) and policy-maps:

```
serverfarm host farm-3
  probe test-tcp
  rserver real40 80
    inservice
  rserver real41 80
    inservice
```

```
class-map match-all VIP-SSL-175
2 match virtual-address 10.74.1.175 tcp eq https

policy-map type loadbalance first-match vip-ssl-175
  class class-default
    serverfarm farm-3

policy-map multi-match LB-VIP
  class VIP-WEB-175
    loadbalance vip inservice
    loadbalance policy L7-match
    loadbalance vip icmp-reply
    appl-parameter http advanced-options L7-map
  class VIP-SSL-175
    loadbalance vip inservice
    loadbalance policy vip-ssl-175
    loadbalance vip icmp-reply
    ssl-proxy server testssl
```

Step 9 Apply multi-match policy-map to service-policy at interface level or globally:

```
interface vlan 749
  ip address 10.74.1.5 255.255.255.0
  access-group input everyone
  access-group output everyone
  service-policy input REMOTE-ACCESS
  service-policy input LB-VIP
  no shutdown
```

Configuration and Menus

See Appendix A—Cisco ACE Configuration for the configuration used to support WebSphere Portal.

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 good 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 Cisco WAAS Solution

Implementation

Implementation Overview

The Cisco WAAS solution requires a minimum of three Cisco Wide Area Application Engine (WAE) appliances 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 third Cisco WAE is used for the Central Manager. The architecture 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 for the solution.

What Was Implemented

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:

- Policy-based routing (PBR)
- Web Cache Communications Protocol (WCCP) v2
- Service policy with 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 Cisco WAEs "out of box" 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 Cisco WAEs.

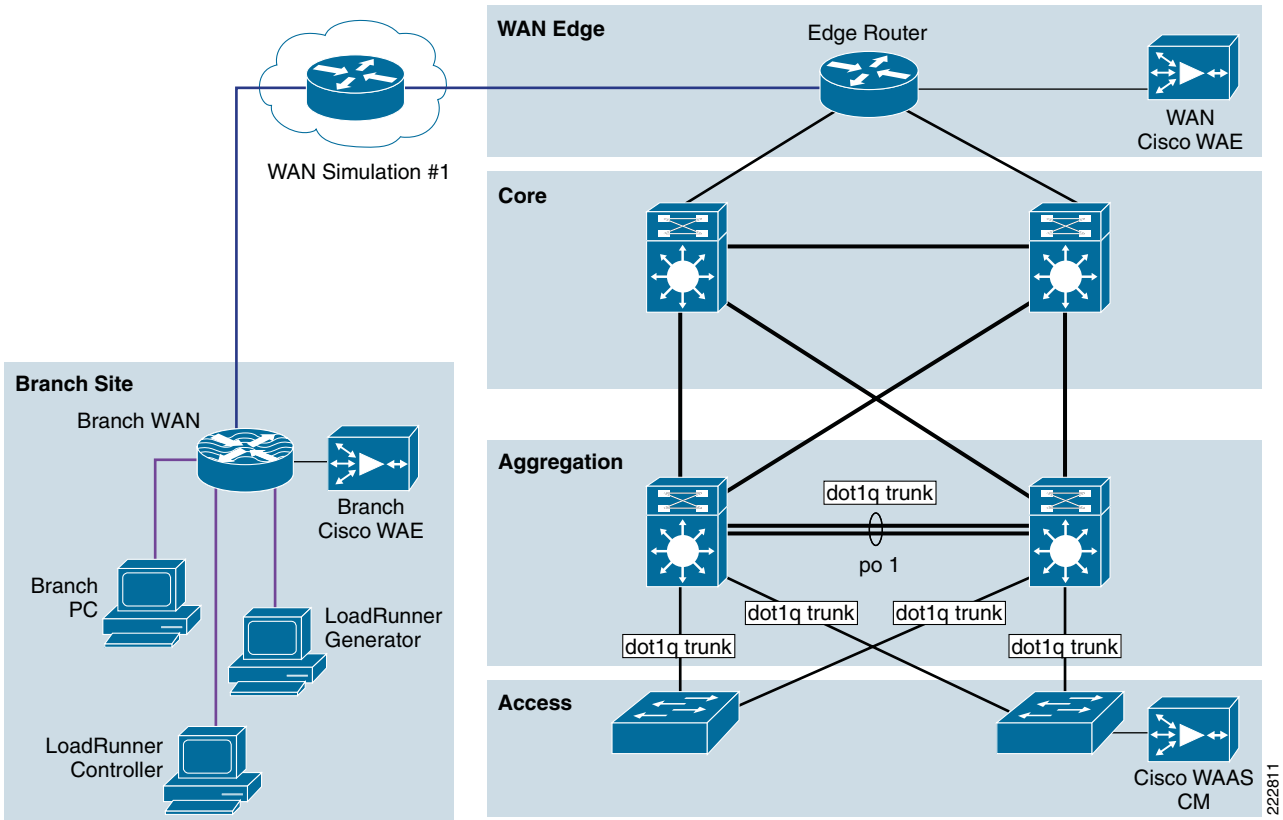
What Was Not Implemented

The following was not implemented in this solution:

- Cisco WAAS Network Module in which Cisco WAAS is installed in an integrated services router, providing a comprehensive solution within a single platform. This architecture provides less scalability and should be considered for use with a branch with a small number of users.

Network Topology

Figure 9 Network Topology



Hardware or Components

Table 4 Hardware

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

Table 5 Software

Product	Software/Code Version
SF-WAAS-4.0-SC-K9	4.0.13
WAAS-ENT-APL	Cisco WAAS Enterprise License for 1 Cisco WAE Appliance
SF-WAAS-4.0-SC-K9	4.0.13
WAAS-ENT-APL	Cisco WAAS Enterprise License for 1 Cisco 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 use port 80. 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 to 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 only traverse the Cisco WAEs once, at the ingress/egress of the data center. Further application communication between the Web servers, application servers, and database servers are within the data center and are not affected by Cisco WAAS.

Transport Flow Optimization (TFO), Data Redundancy Elimination (DRE), and Lempel-Ziv (LZ)-compression, the three key technologies of Cisco WAAS, are enabled by default. Each of these features and functionalities are described in Features and Functionality. 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:

- *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

Scalability and Capacity Planning

Cisco WAE farms can scale up to 32 devices with WCCP and up to 16000 with Cisco ACE load balancing. Cisco WAAS services scale linearly in a N+1 configuration. In addition to the Max Optimized TCP connections, the 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 Cisco 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 range from the NME-WAE-302 for very small offices to the 612-4GB or even higher models for bigger branch sites. WAE 7326 and up 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 if Cisco WAAS devices are not functioning, WCCP does not forward traffic to the Cisco WAEs, resulting in un-optimized traffic flow. This is the worse case scenario; traffic flow continues but is not optimized.

Device High Availability

The Cisco 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 Cisco 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 Cisco WAE and switch. When connected to separate switches in active/standby mode, the standby interface protects the Cisco 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 utilized, 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.

Central Manager

Central Manager (CM) is the management component of Cisco WAAS. CM provides a GUI for configuration, monitoring, and management of multiple branch and data center Cisco WAEs. CM can scale to support thousands of Cisco WAE devices for large-scale deployments. The CM is necessary for making any configuration changes via the Web interface. In the event of CM failure, Cisco WAEs continue to function, however changes cannot be made using the Web pages on the CM until the CM comes back online.

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

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

The following example shows the configuration steps needed to configure CM.

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- or WAN-facing segments.

Step 1 Configure the device to be Central Manager. It 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 10.1.21.2 255.255.255.0
```

Step 3 Set up the default gateway:

```
ip default-gateway 10.1.21.1
```

Step 4 Set the primary interface. Cisco WAAS supports multiple network interfaces type, port channels, and standby interface. 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 NTP server. Traffic statistics are captured and forward 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:

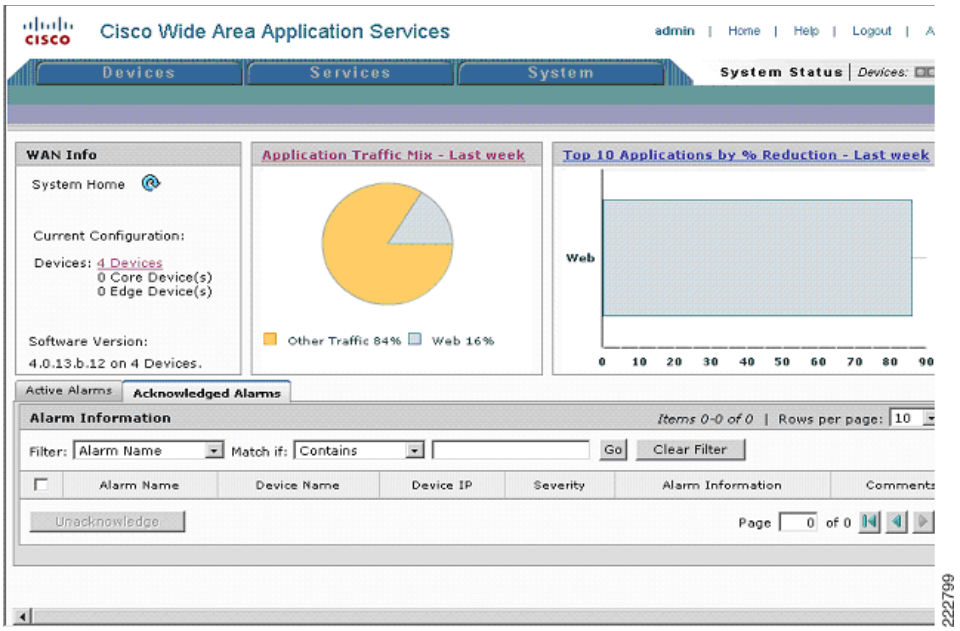
```
ntp server 10.1.6.20
```

Step 6 Initialize the Configuration Management System (CMS) database. The CMS contains configuration rules and information. The Central Manager is the repository of CMS data:

```
cms enable
```

Step 7 Login to the CM Web GUI on port 8443 after the CM is up and running. The initial CM screen is an overview of the health of the system. It contains information on number of devices, status, application traffic, and optimization rate.

Figure 10 Cisco WAAS Central Manager



Branch and Data Center Router

The branch and data center router provides WCCP interception points for Cisco WAAS. Without WCCP interception, Cisco WAAS does not know where to obtain and optimize traffic flow. Different methods of interception and redirection are supported by routers and switches. Redirection methods depend 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 the physical interfaces. Loopback interfaces are always available; there are no physical ties to them. Other routing protocols also use loopback interfaces as a preferred method for naming the router ID. With the IP address tied 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. Notice 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 Set device mode to accelerator. Cisco WAE can be set up as 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 10.1.20.2 255.255.255.0
```

Step 3 Set up the default gateway:

```
ip default-gateway 10.1.20.2
```

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

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

Step 5 Turn on WCCP version 2:

```
wccp version 2
```

Step 6 Add the router to the router list:

```
wccp router-list 1 10.1.20.1
```

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 NTP server. 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 10.1.20.1
```

Step 9 Set up Central Manager address. The Cisco WAE needs register to the Central Manager for statistics reporting and management. Configurations on a per device basis can be perform by the CLI and device GUI. Site wide or Cisco WAAS group have to be perform by the Central Manager. The Central Manager can run operations on thousands of Cisco WAEs at once, saving precious time managing the Cisco WAAS infrastructure:

```
central-manager address 10.1.21.2
```

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 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 10.1.70.11
flow monitor tcpstat-v1 enable
```

Configuration and Menus

See Appendix B—Cisco WAE Configurations for the configuration used by WebSphere Portal.

Troubleshooting Configuration

Cisco WAE Commands

These show commands can help troubleshoot issues with the configuration:

- **sh wccp status**—Verifies WCCP V2 is enabled.
- **sh wccp services**—Verifies WCCP service 61 and 62 are active. Service 61 and 62 must be active.
- **sh wccp routers**—Verifies 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 tfo connection summary**—Verifies Cisco WAAS clients are using Cisco WAAS for connectivity. Show tfo connections show all optimize path in the Cisco WAE. The policy field indicates which optimization method is active for the specified link. F shows the link is fully optimized, which includes DRE, TFO (shown as TCP Optimization), and LZ compression. Pass-through connections are connections that are not optimized.
- **sh statistics dre**—Checks DRE usage. There are two sections in the statistics. One is encode, traffic coming in to the Cisco WAE from the client/server. The Cisco WAE needs to compress the incoming traffic with LZ compression then apply DRE. Another is the decode, traffic coming from the peering Cisco WAE, DRE lookup is performed and traffic uncompressed. These statistics are useful for finding compressibility of the data.

Router Commands

- **sh ip wccp 61**—Verifies WCCP service 61 and 62 are active. This command shows global wccp information and how the packets are redirected. Redirect and group access-list issues 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, namely the Cisco WAEs. sh ip wccp 61 shows global WCCP information; this command shows detailed WCCP client information. Hashing assignments (Cisco WAE bucket assignments), client ID, and client status are found in the output.
- **sh ip wccp interface detail**—Verifies which interface has WCCP configured. Identify 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. Check service 62 as well.

Results and Conclusions

Figure 11 Bandwidth Savings for 1.544 Mbps WAN Link

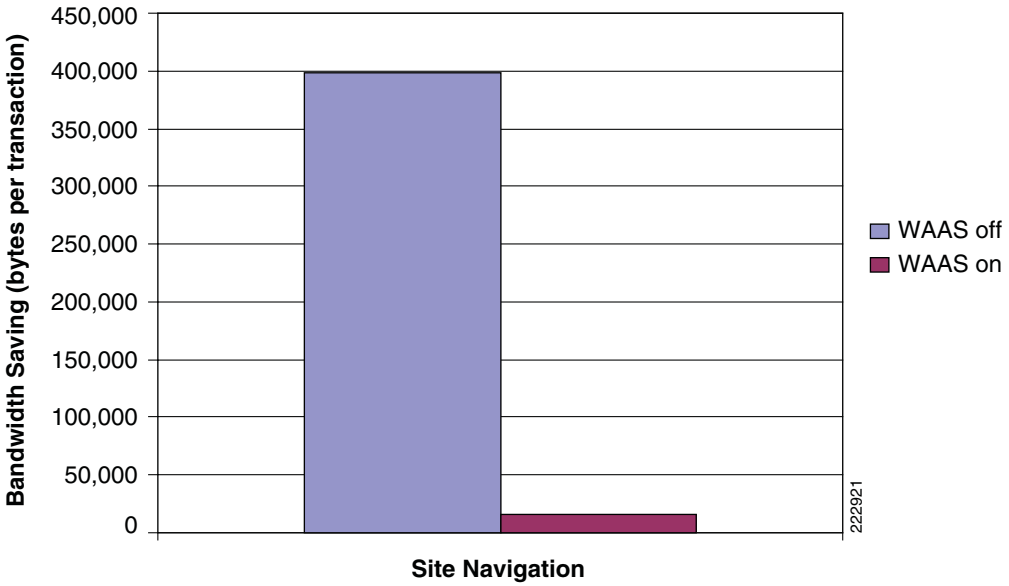


Figure 11 shows the amount data volume traversing the 1.544 Mbps WAN link with and without the Cisco WAAS device that was observed during in a 30 minute cycle with 40 users performing site navigation on the WebSphere Portal application. Figure 11 is based on the total amount data passing through the WAN divided by the total number of transactions under the conditions identified earlier.

The Cisco WAAS device reduces the amount of unnecessary data that traverses the WAN by locally caching data and using compression algorithms on the data the must traverse the WAN. As seen in Figure 11, the Cisco WAAS-enabled network becomes more efficient as less data must traverse the WAN.

With this efficiency, the end-user response time is faster and more transactions can occur, as shown in Figure 12 and Figure 13. Figure 12 shows the decreased average response time with Cisco WAAS enabled. This would result in the end-user obtaining quicker responses from the application and allowing more transactions to occur as the end-user is not waiting as long for the responses, as seen in the transaction summary charts.

Figure 12 Response Time for 1.544 Mbps WAN Link

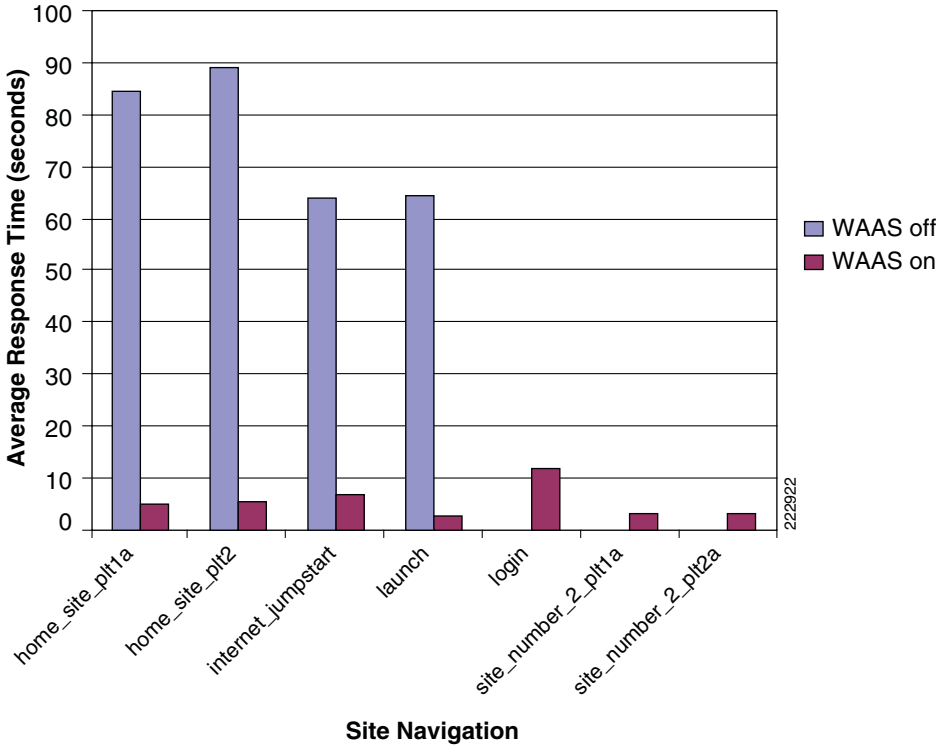


Figure 13 indicates the number of transactions that were observed for the same 30 minute cycle.

Figure 13 Number of Transactions for 1.544 Mbps WAN Link—With and Without Cisco WAAS

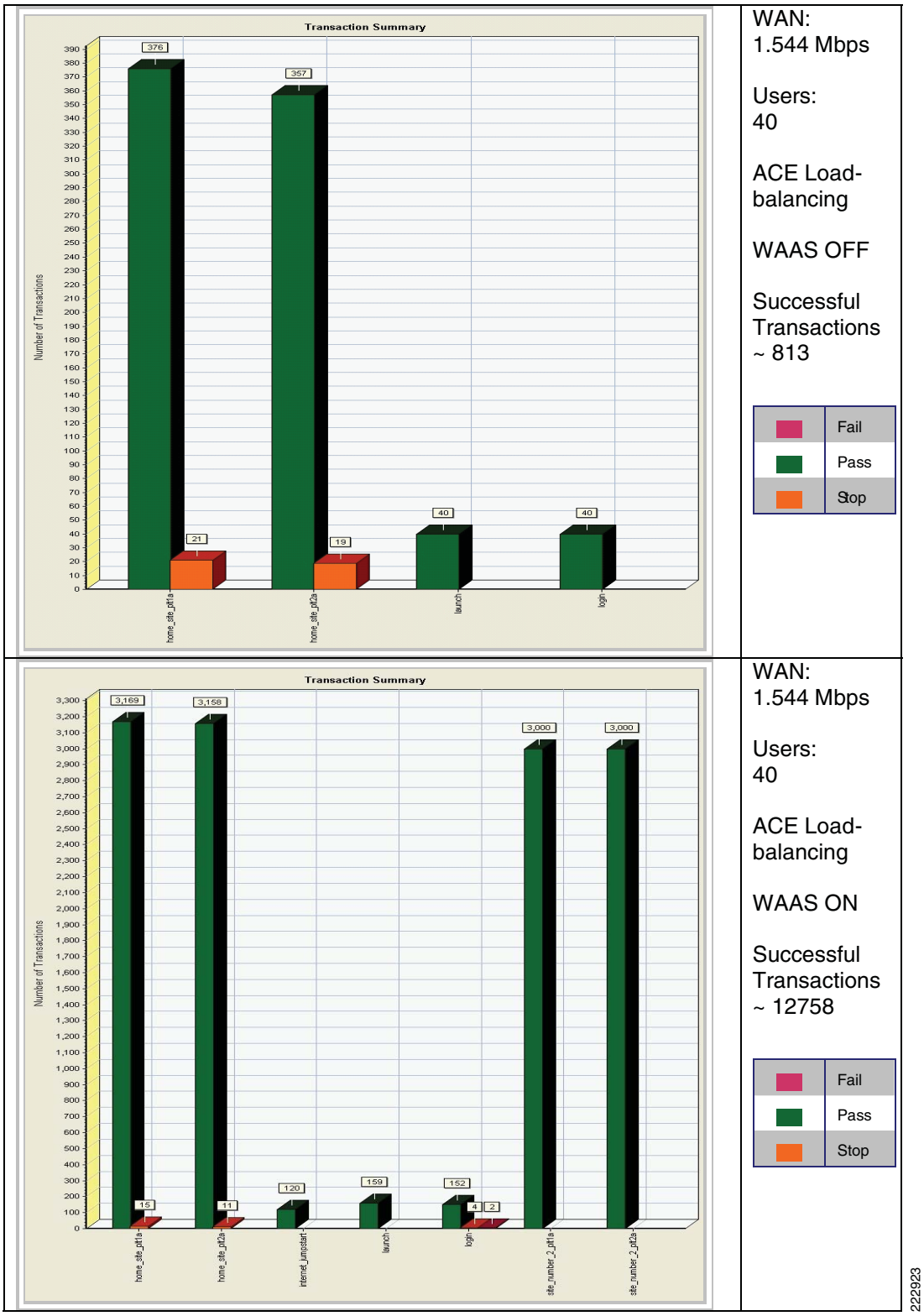
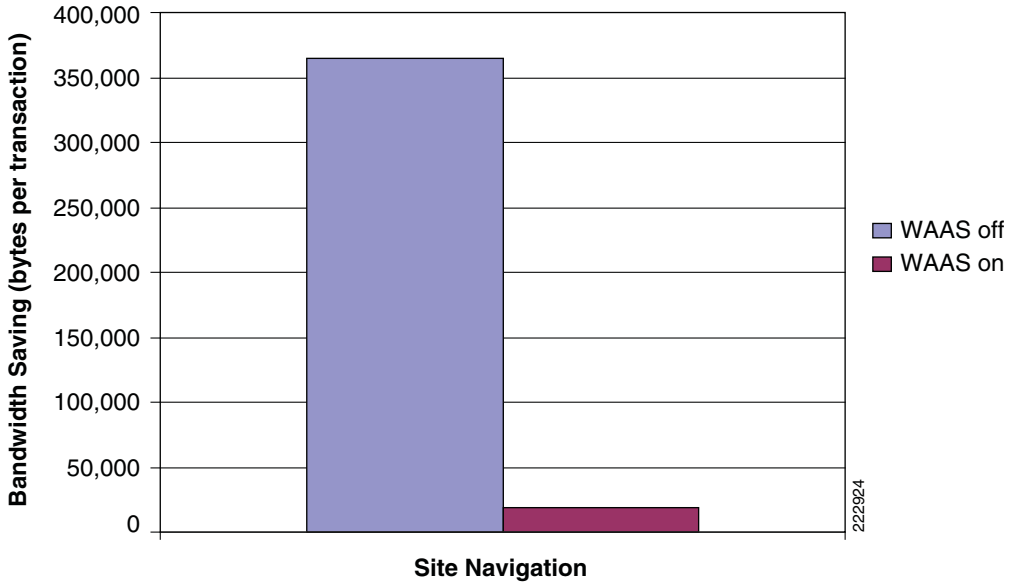


Figure 14 provides the amount data volume traversing the 512 Kbps WAN link with and without the Cisco WAAS device that was observed during in a 30 minute cycle with 40 users performing site navigation on the WebSphere Portal application. The chart is based on the total amount data passing through the WAN divided by the total number of transactions under the conditions identified earlier.

Figure 14 Bandwidth Savings for 512 Kbps WAN Link



The Cisco WAAS device reduces the amount of unnecessary data that traverses the WAN by locally caching data and using compression algorithms on the data the must traverse the WAN. As seen in Figure 14, the Cisco WAAS-enabled network becomes more efficient as less data must traverse the WAN.

With this efficiency, the end-user response time is faster and more transactions can occur, as shown in Figure 15 and Figure 16. Figure 15 shows the decreased average response time with Cisco WAAS enabled. This would result in the end-user obtaining quicker responses from the application and allowing more transactions to occur as the end-user is not waiting as long for the responses, as seen in the transaction summary charts.

Figure 15 Response Time for 512 Kbps WAN Link

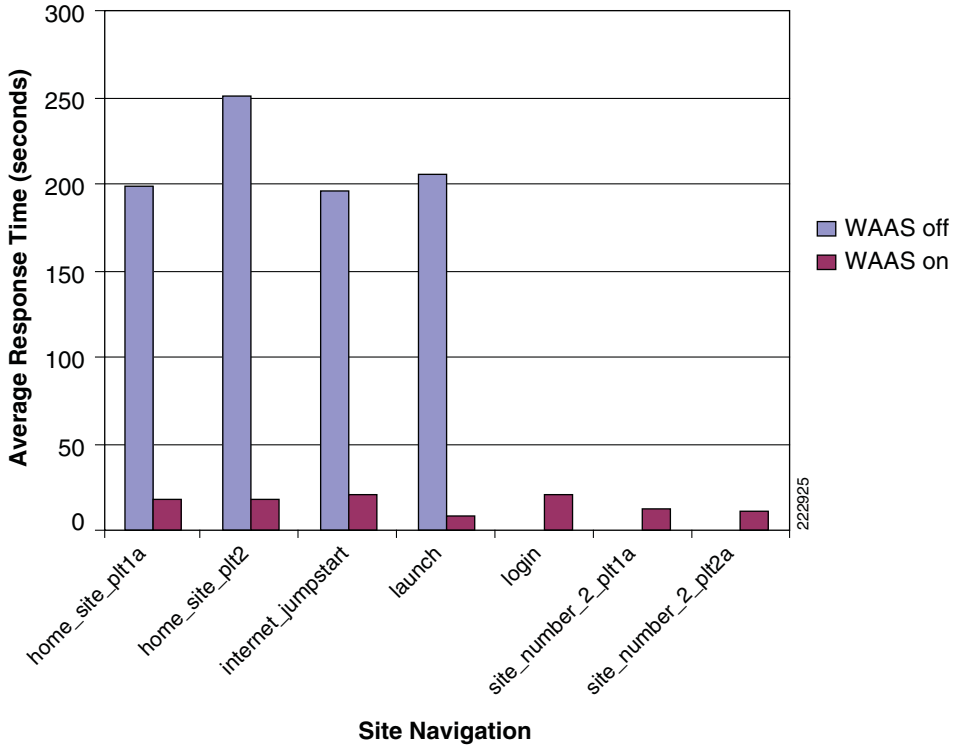
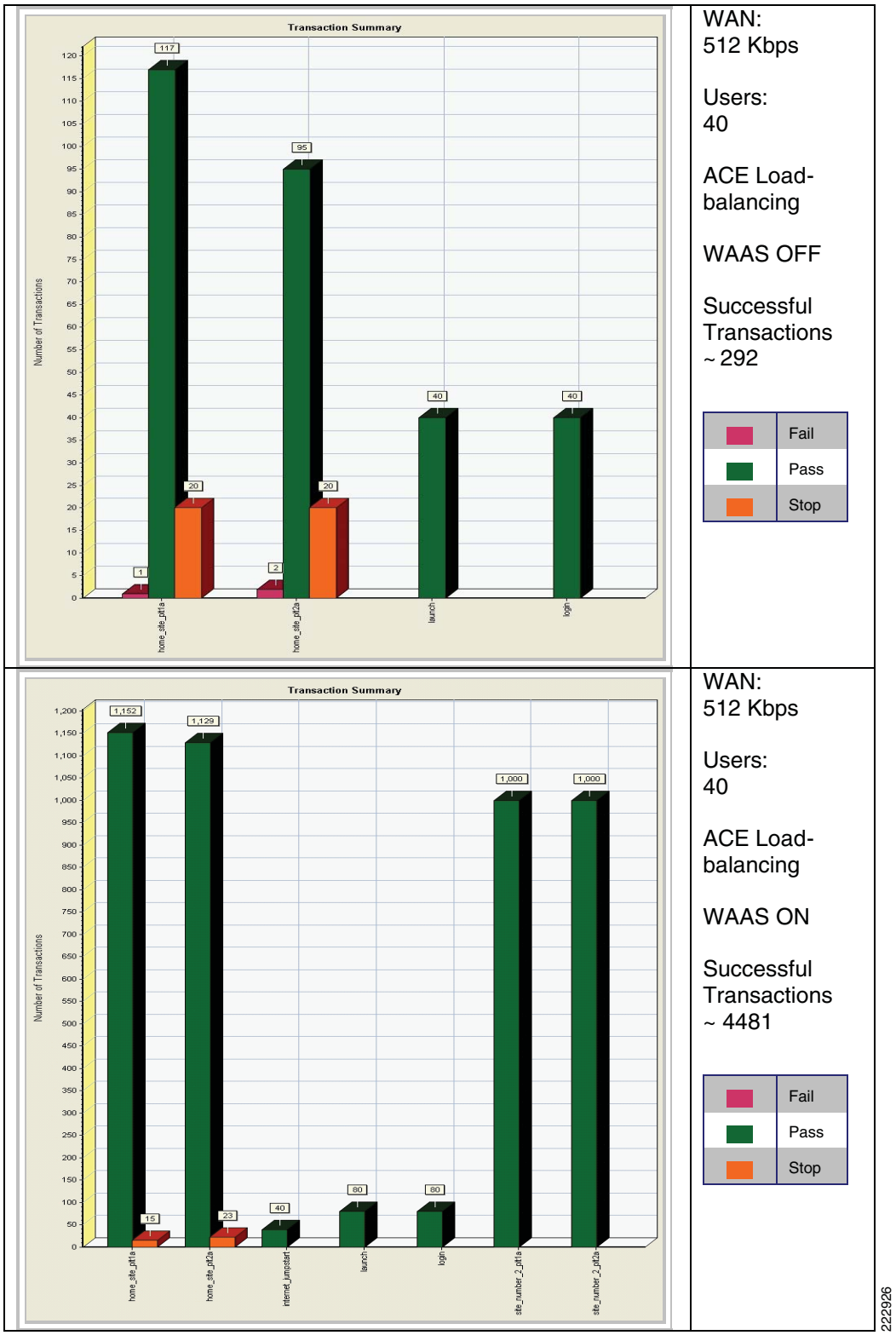


Figure 16 indicates the number of transactions that were observed for the same 30 minute cycle.

Because of the size of this WAN link, it became very congested with 40 users performing site navigation. Comparing to 1.544 Mbps WAN link, average response time is longer and the number of transactions are smaller, with and without Cisco WAAS.

Figure 16 Number of Transactions for 512 Kbps WAN Link—With and Without Cisco WAAS



In summary, with Cisco WAAS enabled the WAN link becomes more efficient, allowing transactions to respond to end-user requests. The Cisco WAAS devices remove the congestion by reducing the amount of unnecessary data traffic that traverses the WAN by locally caching data and using compression algorithms on the data the must traverse the WAN. More transactions are successful and more transactions are completed.

Network Management

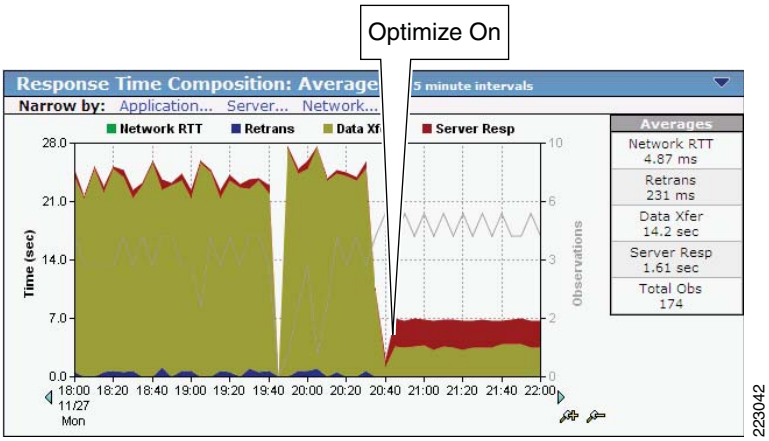
This section focuses on the network management system (NMS) that was used to monitor and provide results indicating the benefits of the Cisco WAAS optimization. The NMS tool used was NetQoS SuperAgent with NetQoS Collector and Reporter. NetQoS Collector gathers the pre-optimized traffic and reports the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

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

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

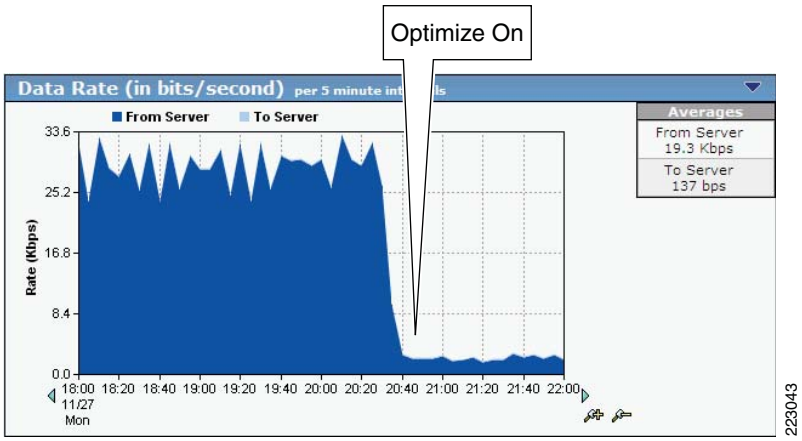
NetQoS Reporter gathers the optimized traffic and reports the data to NetQoS Super Agent. NetQoS Super Agent uses the data from the NetQoS Collector (un-optimized) and compares it to the optimized traffic, indicating the benefits of optimization using the Cisco WAAS as shown in the generic samples in Figure 17, Figure 18, and Figure 19.

Figure 17 Benefit of Optimization Using the Cisco WAAS—Application Response Time



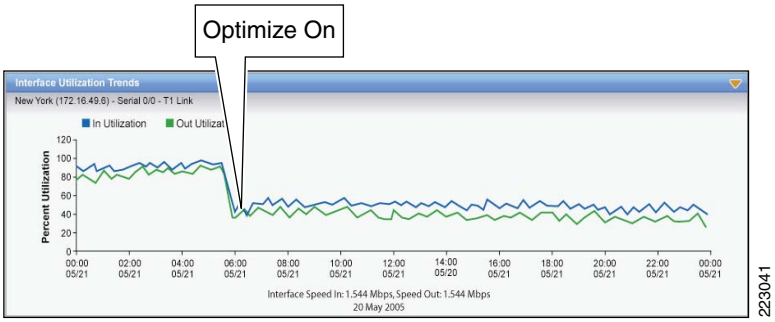
Application Response Time

Figure 18 Benefit of Optimization Using the Cisco WAAS—Application Data Rate



Application Data Rate

Figure 19 Benefit of Optimization Using the Cisco WAAS—Link Utilization



Link Utilization

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

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

Appendix A—Cisco ACE Configuration

Cisco ACE Admin Context

```
login timeout 60
line vty
  session-limit 100
hostname ACE1-Slot3
boot system image:c6ace-t1k9-mz.3.0.0_A1_5a.bin

resource-class Gold
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
```

```
! Define an access control list to include all IP and ICMP traffic
access-list anyone line 10 extended permit ip any any
access-list anyone line 20 extended permit icmp any any

class-map type management match-any REMOTE-ACCESS
  description remote access traffic match rule
  10 match protocol telnet any
  20 match protocol ssh any
  30 match protocol icmp any

! Define a policy to allow management traffic
policy-map type management first-match REMOTE-MGT
  class REMOTE-ACCESS
    permit

interface vlan 82
  description To OOB Management Network
  ip address 172.28.196.150 255.255.255.0
  access-group input anyone
  service-policy input REMOTE-MGT
  no shutdown

ft interface vlan 500
  ip address 192.168.50.1 255.255.255.252
  peer ip address 192.168.50.2 255.255.255.252
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 500
ft group 1
  peer 1
  no preempt
  priority 200
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 172.28.196.1

! Create a context for each application
context dicom
  description Dicom Testing
  allocate-interface vlan 240-241
context sharepoint
  description SharePoint Testing
  allocate-interface vlan 82
  allocate-interface vlan 210-211
context weblogic
  description Web Logic Testing
  allocate-interface vlan 220-221
  member Gold
context websphere
  description Web Sphere Testing
  allocate-interface vlan 230-231
  member Gold

snmp-server community ANSwerLab group Network-Monitor

! For each fault tolerance group, associate a context with it
ft group 2
  peer 1
  no preempt
```

```
  priority 200
  associate-context sharepoint
  inservice
ft group 3
  peer 1
  priority 200
  associate-context weblogic
  inservice
ft group 4
  peer 1
  priority 200
  associate-context websphere
  inservice
ft group 5
  peer 1
  priority 200
  associate-context dicom
  inservice
```

Cisco ACE WebSphere Context

```
login timeout 60

! Define an access control list to include all IP and ICMP traffic
access-list ANYONE line 10 extended permit ip any any
access-list ANYONE line 20 extended permit icmp any any

! Configure different types of probe to check if servers are healthy
probe icmp PING
  interval 2
  faildetect 2

probe tcp PROBE-WS
  port 10038
  interval 2
  faildetect 2
  passdetect interval 10
  passdetect count 2

! Configure WebSphere portal servers as real servers and place them in service
rserver host WS1
  ip address 10.1.40.13
  inservice
rserver host WS2
  ip address 10.1.40.14
  inservice

! Add real servers with port 10038 to a server farm and place them in service
serverfarm host WEBSPHERE
  predictor leastconns
probe PING
probe PROBE-WS
rserver WS1 10038
    inservice
rserver WS2 10038
    inservice

! The Cisco ACE inserts a cookie then loads balance among the server farm
sticky http-cookie acecookie STICKY-INSERT-COOKIE
  cookie insert
  serverfarm WEBSPHERE
```

```
! Define various classes for http traffic,
! for management traffic,
! for traffic destined to VIP with port 10038
class-map type http loadbalance match-any L7-URL
  2 match http url .*.*
class-map type management match-any REMOTE-MANAGEMENT
  2 match protocol telnet any
  3 match protocol icmp any
  4 match protocol ssh any
  5 match protocol snmp any
  6 match protocol http any
  7 match protocol https any
class-map match-all VIP-HTTP-10
  2 match virtual-address 10.1.230.10 tcp eq 10038

! Define various policies to allow management traffic,
! to insert a cookie and load balance for http traffic.
! to use a previously defined policy and enable the VIP to reply to ICMP requests
policy-map type management first-match REMOTE-MANAGEMENT
  class REMOTE-MANAGEMENT
    permit
policy-map type loadbalance first-match L7-RULE
  class L7-URL
    sticky-serverfarm STICKY-INSERT-COOKIE
  class class-default
    serverfarm WEBSPHERE
policy-map multi-match LB-VIP
class VIP-HTTP-10
    loadbalance vip inservice
    loadbalance policy L7-RULE
    loadbalance vip icmp-reply

! For the client side interface, define IP address for this Cisco ACE, the other Cisco ACE
and the shared alias address of the two Cisco ACEs. Load balance traffic destined to VIP
interface vlan 230
description Client side vlan
ip address 10.1.230.5 255.255.255.0
alias 10.1.230.4 255.255.255.0
peer ip address 10.1.230.6 255.255.255.0

access-group input ANYONE
  service-policy input LB-VIP
  service-policy input REMOTE-MANAGEMENT
no shutdown

! For the server side interface, define IP address for this Cisco ACE, the other Cisco ACE
and the shared alias address of the two Cisco ACEs, load balance.
interface vlan 231
description Server side vlan
ip address 10.1.40.2 255.255.255.0
alias 10.1.40.1 255.255.255.0
peer ip address 10.1.40.3 255.255.255.0

  access-group input ANYONE
  service-policy input REMOTE-MANAGEMENT
  no shutdown

! Default route to the HSRP address on aggregation routers
ip route 0.0.0.0 0.0.0.0 10.1.230.1
```

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 Cisco 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 10.1.12.2 255.255.255.0
 exit
!
! This is the address of interface vlan301 on the branch router.
ip default-gateway 10.1.12.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in Cisco WAAS by default
!
ip name-server 171.70.168.183
!
!
! Designate the server for network time protocol
ntp server 10.1.20.1
!
!
wccp router-list 1 10.1.12.1
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
!
!
! Enable central manager
central-manager address 10.1.21.2
cms enable
```

```
!
!
!
flow monitor tcpstat-v1 host 10.1.70.11
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 Cisco 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 Cisco 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 10.1.20.2 255.255.255.0
 exit
!
!
! This is the address of interface GigabitEthernet2/0 on data center WAN edge router.
ip default-gateway 10.1.20.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in Cisco WAAS by default
!
ip name-server 171.70.168.183
!
!
! Designate the server for network time protocol
ntp server 10.1.20.1
!
!
wccp router-list 1 10.1.20.1
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
!
!
! Enable central manager
central-manager address 10.1.21.2
cms enable
!
!
!
flow monitor tcpstat-v1 host 10.1.70.11
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 Cisco 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