

Application Networking—Optimizing Oracle E-Business Suite 12i Across the WAN

October 6, 2008

Introduction

This document presents network design practices to enhance an Oracle E-Business Suite 12i application environment across the WAN. It introduces key concepts and options regarding application deployment and detailed design strategies available to a data center leveraging Cisco application and networking technologies.

Today's organizations face a host of challenges from the new global economy. With Oracle E-Business Suite Release 12, applications and technology come together to ensure that your company can compete effectively in the worldwide marketplace.

Oracle E-Business Suite Release 12 enables businesses to think globally to make better decisions, work globally to be more competitive, and manage globally to lower costs and increase performance. With a new user experience and hundreds of cross-industry capabilities spanning enterprise resource planning, customer relationship management, and supply chain planning, this new release helps you manage the complexities of global business environments.

The enterprise data center is an intricate system of computing power and storage resources that supports enterprise business applications. A data center is not simply a facility, but represents a competitive edge that is strategic to achieving the real business objectives that the associated applications collectively address. The physical and logical design of the data center network must provide a flexible, secure, and highly available environment to optimize critical business applications and to assist the enterprise in achieving its goals; goals that are not confined to the local data center campus, but extend to encompass remote locations and users.

Enterprises are addressing IT infrastructure and management costs through the consolidation of branch and data center resources. Consolidation centralizes application environments and storage assets in the data center to make them accessible to remote users via the WAN. The introduction of detached applications to the enterprise is significant because *distance* might negatively affect performance, availability, and the overall end-user experience.



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

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

Scope

Cisco data center and Cisco branch architectures are established enterprise designs that deliver highly available and robust network infrastructures. This document describes the deployment of the Oracle E-Business Suite in a Cisco data center through the use of services available in the Cisco branch and local LAN. This end-to-end solution design employs many integrated network services—including load balancing, security, and application optimization.

Enterprise Architecture

This section describes the application architecture of the Oracle E-Business Suite 12i.

Enterprise Application Overview

The data center is a repository for enterprise software applications that are continuously changing to meet business requirements and to accommodate the latest technological advances and methods. Consequently, the logical and physical structure of the data center server farm and of the network infrastructure hosting associated software applications is also continuously changing.

The server farm has evolved from the classic client/server model to an *N*-tier approach, where *N* implies any number, such as two-tier or four-tier—any number of distinct tiers used in the architecture. The *N*-tier model logically or physically separates the enterprise application by creating functional areas. These areas are generally defined as the web frontend, the application business logic, and the database tiers.

Figure 1 and Figure 2 illustrate the progression of the enterprise application from the client/server to *N*-tier paradigm.

Figure 1 Client/Server Model

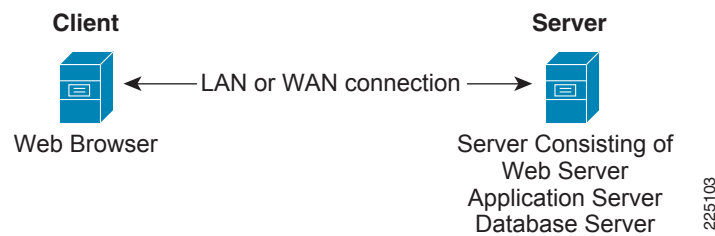
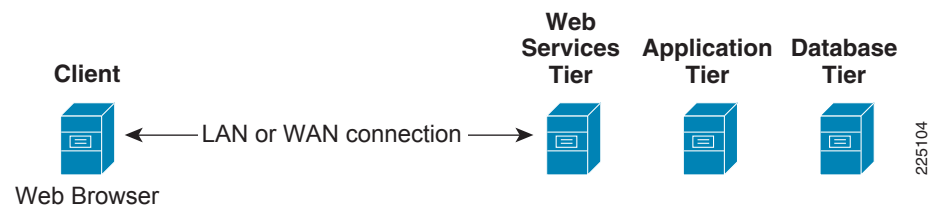


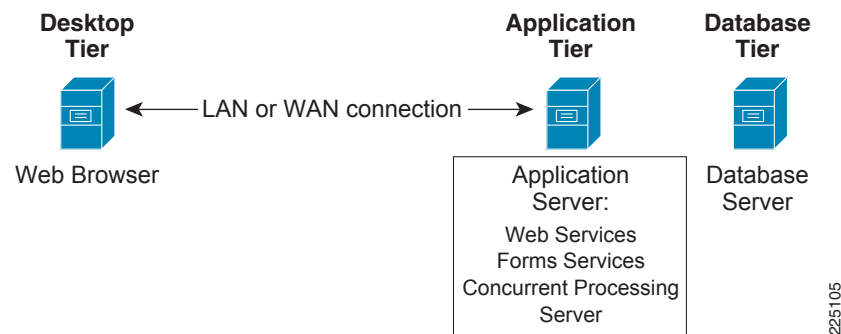
Figure 2 The N-Tier Model



The *N*-tier model provides a more scalable and manageable enterprise application environment because it creates distinct serviceable areas in the software application. The application is distributed and becomes more resilient as single points of failure are removed from the design.

The Oracle application architecture uses the *N*-tier model by distributing application services across nodes in the server farm. The Oracle application architecture, as shown in [Figure 3](#), uses the logical separation of tiers as desktop, application, and database. It is important to remember that each tier can consist of one or more physical host(s) to provide the enterprise with the required performance or application availability.

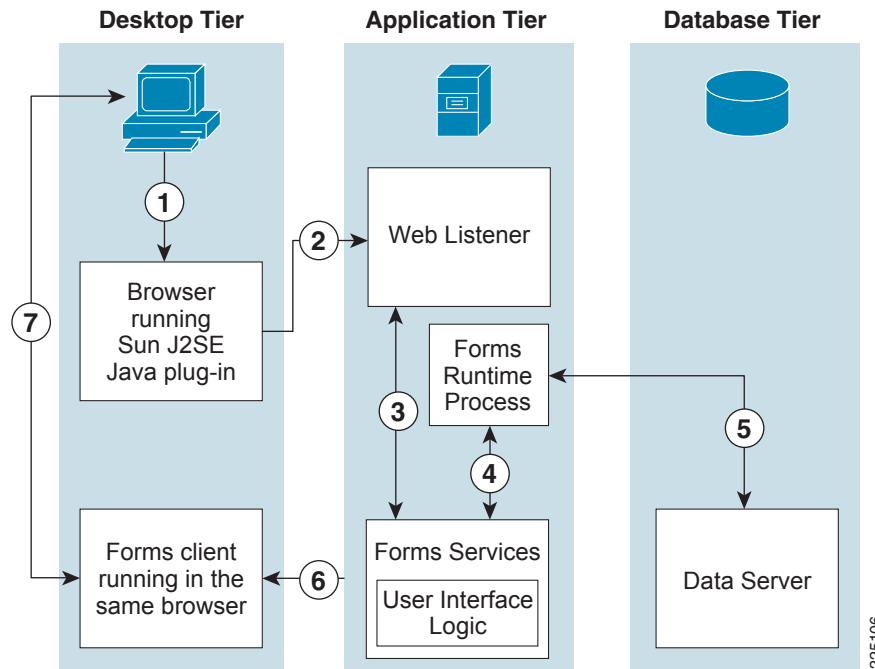
Figure 3 *N-Tier Oracle Model*



Desktop Tier

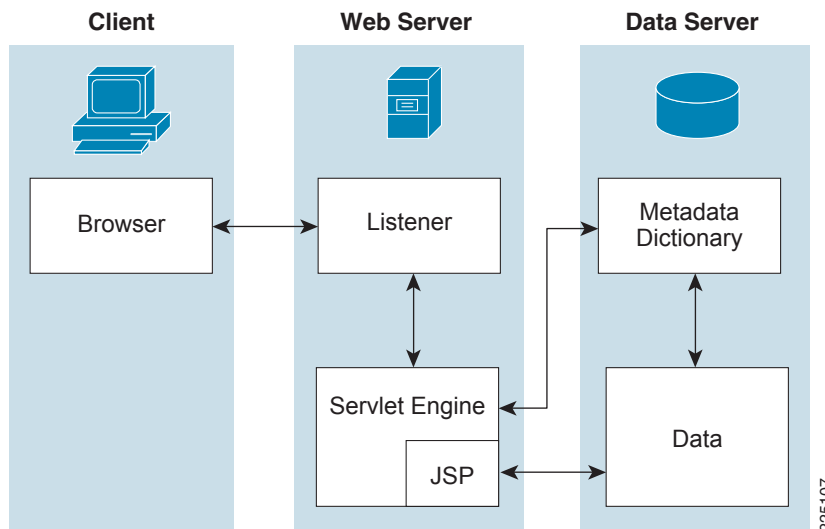
The desktop tier, traditionally called the presentation layer, consists of the client user interface (a web browser). The browser connects to the application tier via HTTP or HTTPS to the web server or the forms server. Historically, the forms server required the use of a client-side applet, Oracle JInitiator, which runs as an Active-X or plug-in on the client browser using a direct socket connection to the forms server. This direct-connect environment requires two logical connections to the applications tier: one connection to the web server listener and the other to the forms services (see [Figure 4](#)). This exposes an enterprise to potential security risks when connectivity is allowed beyond the confines of the corporate LAN or WAN by requiring *holes* in firewalls. These holes must open another port in the firewall—in addition to HTTP port allowing the connection between the client and the forms server. This becomes more of a security risk when Secure Socket Layer (SSL) is used. In the SSL environment, additional certificate requirements are necessary because certificates are required for the HTTP traffic and forms server.

Figure 4 Traditional Desktop to Form Server Connections



In 2002, Oracle E-Business Suite offered a more Internet-friendly forms server application by allowing a Java forms-listener servlet to intercept forms server requests via the web listener. The forms listener servlet allows a single HTTP or HTTPS connection between the client, desktop tier, and the application tier. Figure 5 shows the more secure forms-listener servlet deployment model, which can also take advantage of standard SSL offload and load balancing approaches.

Figure 5 Forms Listener Servlet Architecture



Note

The forms-listener servlet deployment model is now common in enterprise data centers. The remainder of this document assumes the use of this forms strategy.

Application Tier

The application tier of the Oracle E-Business Suite provides administrative services and business logic, allowing end users at the desktop tier to make use of the information found at the database tier.

Figure 3 shows the primary servers residing in this layer:

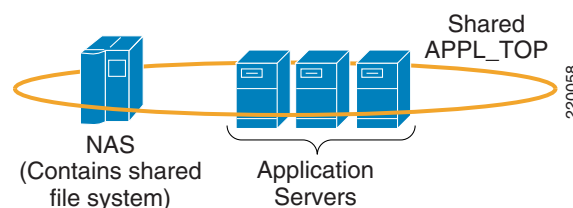
- Web server
- Forms server
- Concurrent processing server
- Administration server
- Daily business intelligence

Each of the application servers provides business process logic or management services to the Oracle E-Business Suite-enabled enterprise. The desktop tier communicates with the application tier via the web server listener (see Forms Listener Servlet Architecture).

The application tier is commonly referred to as the APPL_TOP. The APPL_TOP is a file system that can reside on a single physical node or span multiple nodes in a *shared* multi-node application tier deployment. A shared APPL_TOP resides on a common disk mounted by each node in the Oracle 12i installation. A shared APPL_TOP allows any of the nodes to invoke the five primary server functions, such as the web server and forms server. The primary advantage to a shared application tier deployment is the ability to patch and/or modify a single file system in a multi-node deployment, propagating those changes to all nodes simultaneously.

In addition, the use of a single file system requires the backup of only a single file system despite the use of multiple nodes. The shared application file system shows three server nodes sharing the application file system via NFS. The shared mount point in this case is a storage device located in the network.

Figure 6 Shared Application File System



Note

Windows systems do not support a shared application tier in an Oracle 12i environment. For more information on shared application tier file systems, see Oracle Metalink Document 384248.1.

Database Tier

The database tier contains the Oracle database server that stores all the data maintained by Oracle applications. The database also stores the Oracle applications online help information. More specifically, the database tier contains the Oracle data server files and Oracle applications database executables that physically store the tables, indexes, and other database objects for your system. The database server does not communicate directly with the desktop clients, but rather with the servers on the application tier that mediate the communications between the database server and the clients. To provide increased performance, scalability, and availability, Oracle offers real application clusters (RAC) that allow multiple nodes to support a single database instance.

Enterprise Network Architecture

Data Center Network Components

The logical topology of the data center infrastructure can be divided into the frontend network and the backend network, depending on their role:

- The frontend network provides the IP routing and switching environment, including client-to-server, server-to-server, and server-to-storage network connectivity.
- The backend network supports the storage area network (SAN) fabric and connectivity between servers and other storage devices, such as storage arrays and tape drives.

**Note**

For more information on Cisco data center designs or other places in the network, refer to the following URL: http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html. Content at that location provides an introduction to data center designs.

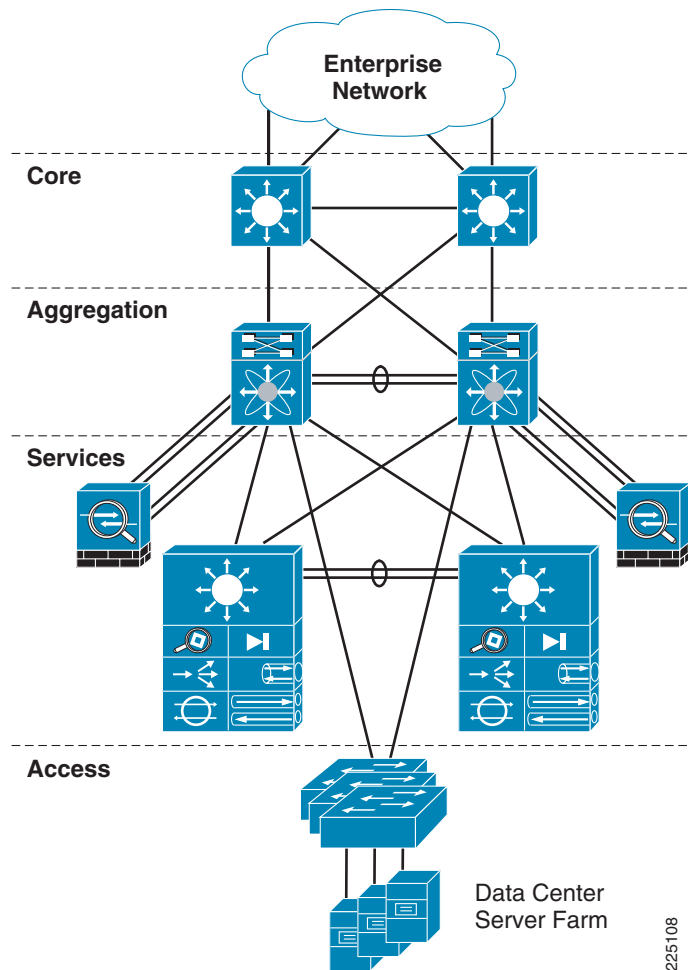
Frontend Network

The frontend network contains three distinct functional layers:

- Core
- Aggregation
- Access

Figure 7 shows a multi-tier frontend network topology and a variety of services that are available at each of these layers.

Figure 7 Data Center Multi-Tier Model Topology



Core Layer

The core layer is a gateway that provides high-speed connectivity to external entities such as the WAN, intranet, and extranet of the campus. The data center core is a Layer-3 domain where efficient forwarding of packets is the fundamental objective. To this end, the data center core is built with high-bandwidth links (10-Gigabit Ethernet) and uses routing best practices to optimize traffic flows. The data center core is connected to the WAN (Internet) edge; this is where acceleration devices can be placed.

Aggregation Layer

The aggregation layer is a point of convergence for network traffic that provides connectivity between the services layer and the server farms at the access layer to the rest of the enterprise. The aggregation layer supports Layer 2 and Layer 3 functionality.

Services Layer

The services layer provides services that are shared across the access layer server farms. It provides common services in a way that is efficient, scalable, predictable, and deterministic. The services layer provides a comprehensive set of features for the data center. The following devices support these features:

- Multilayer aggregation switches
- Load balancing devices
- Firewalls
- Wide area application acceleration
- Intrusion detection systems
- Content engines
- SSL offloaders
- Network analysis devices

Access Layer

The primary role of the access layer is to provide the server farms with the required port density. In addition, the access layer must be a flexible, efficient, and predictable environment to support client-to-server and server-to-server traffic. A Layer-2 domain meets these requirements by providing the following:

- Layer-2 adjacency between servers and service devices
- A deterministic, fast converging, loop-free topology

Layer-2 adjacency in the server farm lets you deploy servers or clusters that require the exchange of information at Layer 2 only. It also readily supports access to network services in the services layer, such as load balancers and firewalls. This enables an efficient use of shared, centralized network services by the server farms.

In contrast, if services are deployed at each access switch, the benefit of those services is limited to the servers directly attached to the switch. Through access at Layer 2, it is easier to insert new servers into the access layer. The services layer is responsible for data center services, while the Layer-2 environment focuses on supporting scalable port density.

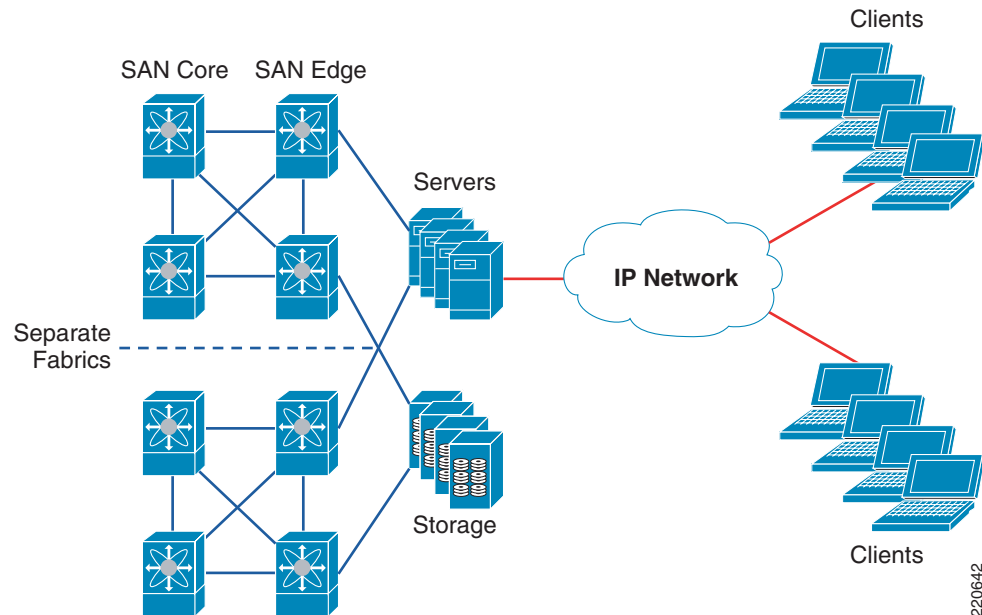
Layer-3 access designs are not widely deployed in current data centers. However, to minimize fault domains and provide rapid convergence, network administrators are seeking to leverage the benefits of Layer 3. Layer-3 designs do not exclude the introduction of network services, but the transparency of the service at the services layer is more difficult to maintain. As with all access layer designs, the requirements of the application environments drive the decision for either model. The access layer must provide a deterministic environment to ensure a stable Layer-2 domain regardless of its size. A predictable access layer allows spanning tree to converge and recover quickly during failover and fallback.

Backend Network

The backend SAN consists of core and edge SAN storage layers to facilitate high-speed data transfers between hosts and storage devices. SAN designs are based on the FiberChannel (FC) protocol. Speed, data integrity, and high availability are key requirements in an FC network. In some cases, in-order delivery must be guaranteed. Traditional routing protocols are not necessary on FC. Fabric Shortest Path First (FSFP), similar to Open Shortest Path First (OSPF), runs on all switches for fast fabric convergence and best path selection. Redundant components are present from the hosts to the switches and to the

storage devices. Multiple paths exist and are in use between the storage devices and the hosts. Completely separate physical fabrics are a common practice to guard against control plane instability, ensuring high availability in the event of any single component failure. Figure 8 illustrates a general SAN topology.

Figure 8 SAN Topology



SAN Core Layer

The SAN core layer provides high-speed connectivity to the edge switches and external connections. Connectivity between core and edge switches are 10 Gbps links or trunking of multiple full-rate links for maximum throughput. Core switches also act as master devices for selected management functions, such as the primary zoning switch and Cisco fabric services. In addition, advanced storage functions such as virtualization, continuous data protection, and iSCSI reside in the SAN core layer.

SAN Edge Layer

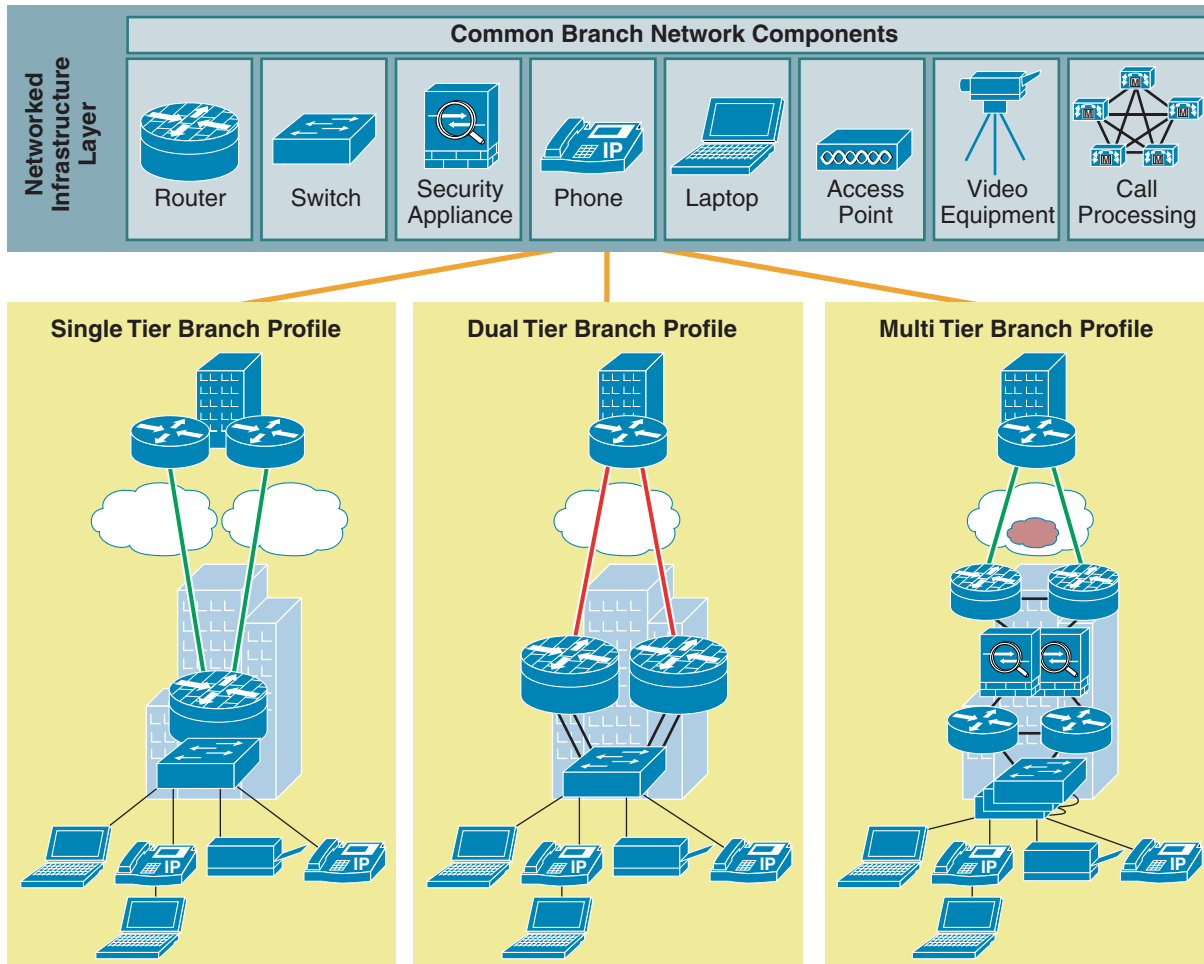
The SAN edge layer is analogous to the access layer in an IP network. End devices such as hosts, storage, and tape devices connect to the SAN edge layer. Compared to IP networks, SANs are much smaller in scale, but the SAN must still accommodate connectivity from all hosts and storage devices in the data center. Over-subscription and planned core-to-edge fan out ratio result in high port density on SAN switches. On larger SAN installations, it is common to segregate the storage devices to additional edge switches.

Branch Network Components

The enterprise branch provides remote users connectivity to corporate resources such as the centralized application services residing in the enterprise data center. The architectural design of the enterprise branch varies depending on the availability, scalability, security, and other service requirements of the organization.

The Cisco enterprise branch architecture framework defines the network infrastructure, network services, and application optimization capabilities of three typical branch deployment models. Figure 9 shows these three common branch solutions. Each of these profiles provides varying degrees of scalability and resiliency in addition to integrated network and application services.

Figure 9 Network Infrastructure Layer -Three Models



Note

This document does not focus on enterprise branch design. For more information on Cisco data center designs or other places in the network, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html.

Technology Overview

This section provides an overview of the significant Cisco products and technologies leveraged in this design. The following products are addressed:

- Cisco Wide Area Application Engine, page 11
- Cisco Application Control Engine, page 12
- Firewall Services Module, page 17

Cisco Wide Area Application Engine

To appreciate how Wide Area Application Services (WAAS) provides WAN and application optimization benefits to the enterprise, consider the basic types of centralized application messages that are transmitted between remote branches. For simplicity, two basic types are identified:

- *Bulk transfer applications*—Transfer of files and objects, such as FTP, HTTP, and IMAP. In these applications, the number of round-trip messages may be few and may have large payloads with each packet. Examples include web portal or thin client versions of Oracle, SAP, Microsoft (SharePoint, OWA) applications, e-mail applications (Microsoft Exchange, Lotus Notes), and other popular business applications.
- *Transactional applications*—High number of messages transmitted between endpoints. Chatty applications with many round-trips of application protocol messages that may or may not have small payloads. Examples include Microsoft Office applications (Word, Excel, PowerPoint, and Project).

WAAS uses the technologies described in the following subsections to provide a number of features, including application acceleration, file caching, print service, and DHCP to benefit both types of applications.

Advanced Compression using DRE and Lempel-Ziv Compression

Data Redundancy Elimination (DRE) is an advanced form of network compression that allows Cisco WAAS to maintain an application-independent history of previously-seen data from TCP byte streams. Lempel-Ziv (LZ) compression uses a standard compression algorithm for lossless storage. The combination of using DRE and LZ reduces the number of redundant packets that traverse the WAN, thereby conserving WAN bandwidth, improving application transaction performance, and significantly reducing the time for repeated bulk transfers of the same application.

Transport File Optimizations

Cisco WAAS Transport File Optimizations (TFO) uses a robust TCP proxy to safely optimize TCP at the WAE device by applying TCP-compliant optimizations to shield the clients and servers from poor TCP behavior because of WAN conditions. Cisco WAAS TFO improves throughput and reliability for clients and servers in WAN environments through increases in the TCP window sizing and scaling enhancements as well as implementing congestion management and recovery techniques to ensure that the maximum throughput is restored if there is packet loss.

Common Internet File System Caching Services

Common Internet File System (CIFS), used by Microsoft applications, is inherently a highly chatty transactional application protocol where it is not uncommon to find several hundred transaction messages traversing the WAN just to open a remote file. WAAS provides a CIFS adapter that can inspect and to some extent predict what follow-up CIFS messages are expected. By doing this, the local WAE caches these messages and sends them locally, significantly reducing the number of CIFS messages traversing the WAN.

Print Services

WAAS provides native SMB-based Microsoft print servers locally on the WAE device. Along with CIFS optimizations, this allows for branch server consolidation at the data center. Having full-featured local print services means less traffic transiting the WAN. Without WAAS print services, print jobs are sent from a branch client to the centralized server(s) across the WAN, then back to the branch printer(s), thus transiting the WAN twice for a single job. WAAS eliminates the need for either WAN trip.

Cisco Application Control Engine

Overview

The Cisco Application Control Engine (ACE) provides a highly available and scalable data center solution from which the Oracle E-Business Suite application environment may benefit. Currently, the ACE is available as an appliance or integrated service module in the Catalyst 6500 platform. ACE features and benefits include the following:

- Device partitioning (up to 250 virtual ACE contexts)
- Load balancing services (up to 16 Gbps of throughput capacity, 345,000 L4 connections/second)
- Security services via deep packet inspection, access control lists (ACLs), unicast reverse path forwarding (URPF), Network Address Translation (NAT)/Port Address Translation (PAT) with fix-ups, syslog, and so on
- Centralized role-based management via Application Network Manager (ANM) GUI or CLI
- SSL Offload (up to 15,000)
- URL rewrite
- SSL sessions via licensing
- Support for redundant configurations (intra-chassis, inter-chassis, inter-context)

The ACE support the following modes of operation:

- Transparent
- Routed
- One-armed

The following sections describe some of the features and functionalities found on the ACE and employed in the Oracle E-Business Suite application environment.

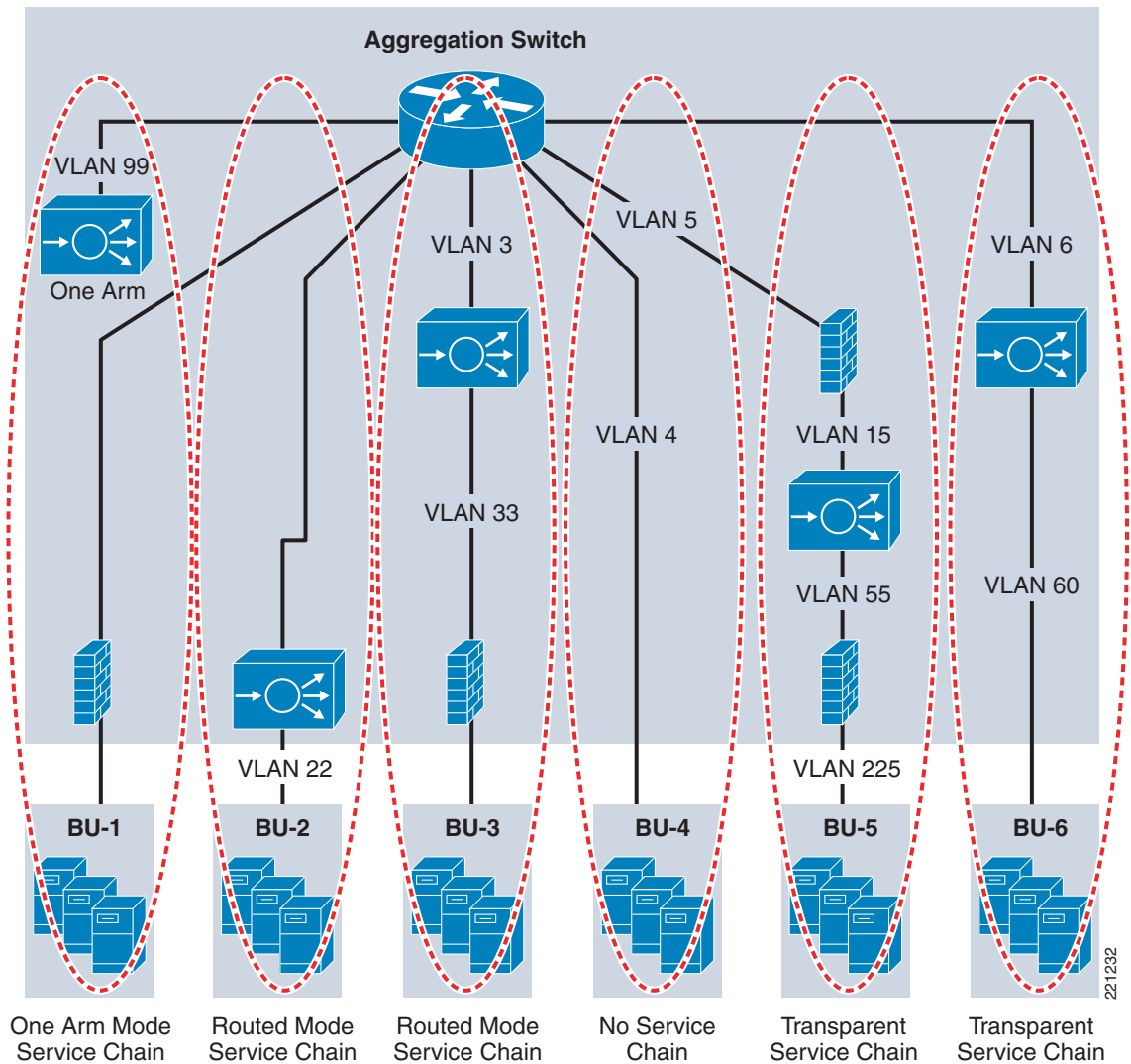
ACE Virtualization

Virtualization is a prevalent trend in the enterprise today. From virtual application containers to virtual machines, the ability to optimize the use of physical resources and provide logical isolation is gaining momentum. The advancement of virtualization technologies includes the enterprise network and the intelligent services it offers.

The ACE supports device partitioning where a single physical device may provide multiple logical devices. This virtualization functionality allows system administrators to assign a single virtual ACE device to a business unit or application to achieve application performance goals or service-level agreements (SLAs). The flexibility of virtualization allows the system administrator to deploy network-based services according to the individual business requirements of the customer and technical requirements of the application. Service isolation is achieved without purchasing another dedicated appliance that consumes more space and power in the data center.

Figure 10 shows the use of virtualized network services afforded via the ACE and Cisco Firewall Services Module (FWSM). In **Figure 10**, a Catalyst 6500 housing a single ACE and FWSM supports the business processes of five independent business units. The system administrator determines the requirements of the application and assigns the appropriate network services as virtual contexts. Each context contains its own set of policies, interfaces, resources, and administrators. The ACE and FWSMs allow routed, one-arm, and transparent contexts to co-exist on a single physical platform.

Figure 10 Service Chaining via Virtualized Network Services



Note

For more information on ACE virtualization, see the *Application Control Engine Module Virtualization Configuration Guide* at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/virtualization/guide/config.html

Session Persistence

Session persistence is the ability to forward client requests to the same server for the duration of a session. Oracle recommends HTTP session persistence for their E-Business Suite environment via the following:

- IP sticky
- Cookie sticky

ACE supports each of these methods, but given the presence of proxy services in the enterprise, Cisco recommends using the cookie sticky method to guarantee load distribution across the server farm. HTTP Header Insertion Example shows the *ACEOptimized* cookie inserted into the client E-Business request.

In addition, ACE supports the replication of sticky information between devices and their respective virtual contexts. This provides a highly available solution that maintains the integrity of each session.

Transparent Interception

Load balancers typically perform a NAT function to conceal the real server IP addresses residing in the enterprise data center, which means that the virtual IP address (VIP) is transformed and the request is forwarded to a real server. In addition to supporting this functionality, the ACE allows the system administrator to disable NAT for particular server farms, which is a desirable behavior for both firewall load balancing deployments and WAAS server farms.



Note

Transparent interception allows the WAE devices to perform their application optimization functionality without changing the Layer 3 information of the session.

Health Monitoring

The ACE device is capable of tracking the state of a server and determining its eligibility for processing connections in the server farm. The ACE uses a simple pass/fail verdict but has many recovery and failures configurations, including probe intervals, timeouts, and expected results. Each of these features contributes to an intelligent load balancing decision by the ACE context.

Following are the predefined probe types currently available on the ACE module:

- ICMP
- TCP
- UDP
- Echo (TCP/UDP)
- Finger
- HTTP
- HTTPS
- FTP
- Telnet
- DNS
- SMTP
- IMAP
- POP
- RADIUS
- Scripted (TCL support)

Note that the potential probe possibilities available via scripting make the ACE an even more flexible and powerful application-aware device. In terms of scalability, the ACE module can support 1000 open probe sockets simultaneously.

**Note**

In the E-Business Suite environment, the HTTP probe verified the state of the entire application stack by requesting a page requiring APPL_TOP and database services.

Untested Cisco ACE Features

The following additional features of the Cisco ACE that were not tested with Oracle 12i EBS during the creation of this document:

- [TCP Reuse](#)
- [HTTP Header Insertion](#)
- [MAC Sticky](#)
- [Allowed Server Connections](#)
- [Route Health Injection](#)

These features are described briefly in the following subsections.

TCP Reuse

TCP reuse allows the ACE to recycle TCP connections to the server farm, essentially reducing the load on the application servers. Servers use RAM to open and maintain connections to clients. RAM is a finite resource that directly impacts server performance. The ACE module allows persistent TCP connections to the application server and reclaims them for use by multiple clients.

**Note**

It is important to verify that the MSS and TCP options on the server and ACE are identical. For logging consistency, use HTTP header insertion to maintain the source IP address of clients when TCP reuse is in use.

HTTP Header Insertion

The ACE HTTP header insertion feature allows a system administrator to insert a generic string value or to capture the following request specific values:

- Source IP address
- Destination IP address
- Source port
- Destination port

HTTP header insertion is especially useful when TCP reuse or the source address of the request may be determined via NAT. HTTP header insertion allows service logs to reflect the original source IP address of the request. [Figure 11](#) shows the insertion of an HTTP header under the name *X-forwarder*, reflecting the source IP address of the request.

Figure 11 *HTTP Header Insertion Example*



MAC Sticky

The ACE is capable of Reverse Path Forwarding (RPF) based on the source MAC address on a VLAN interface of the request. This feature allows for transparency at Layer 3 and provides deterministic traffic flows at Layer 2 through the ACE. Cisco WAAS devices deployed as a server farm under the ACE take advantage of this feature, guaranteeing that the same WAE device consistently manages each TCP session.

**Note**

This feature is not compatible with Layer 3 (IP)-based Reverse Path Forwarding (RPF).

Allowed Server Connections

Enterprise data centers typically perform due diligence on all deployed server and network devices, determining the performance capabilities to create a more deterministic, robust, and scalable application environment. The ACE allows the system administrator to establish the maximum number of active connections values on a per-server basis and/or globally to the server farm. This functionality protects the end device, whether it is an application server or network application optimization device such as the WAE.

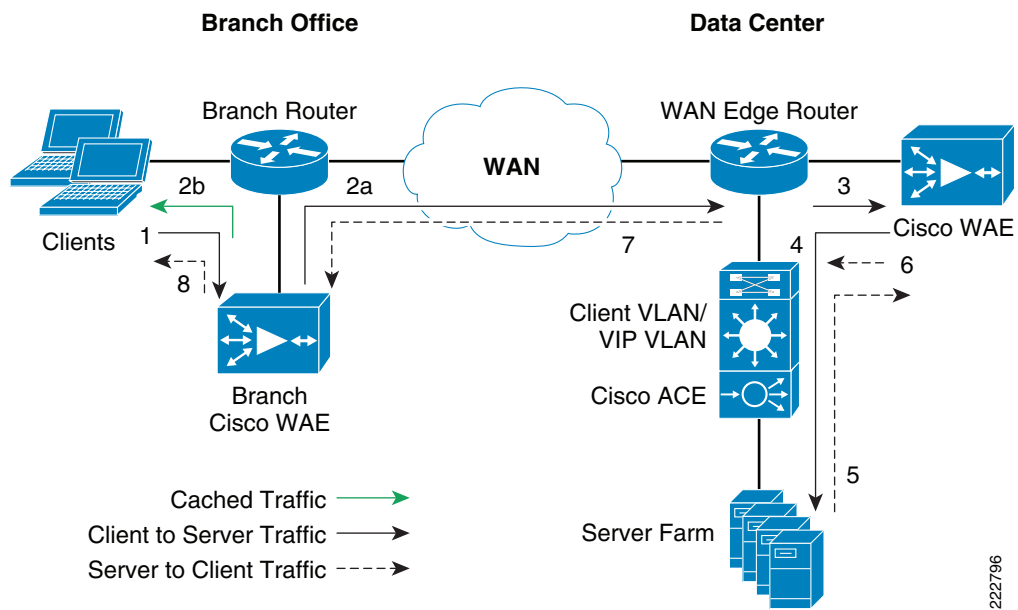
Route Health Injection

Route health injection (RHI) allows the ACE to advertise host routes to any number of virtual IP addresses hosted by the device. The injection of the host route to the remaining network offers Layer 3 availability and convergence capabilities to the application environment.

Packet Flow with WAAS and ACE

Figure 12 illustrates the handshake between a client and the server farm and the data transfer phase.

Figure 12 Packet Flow with WAAS and ACE



The following process description summarizes the steps illustrated in Figure 12:

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

2. 2a). The branch WAE applies a new TCP option (0x21) to the packet if the application is identified for optimization by an application classifier. The branch WAE adds its device ID and application policy support to the new TCP option field. This option is examined and understood by other WAEs in the path as the ID and policy fields of the initial WAE device. The initial ID and policy fields are not altered by another WAE. The packet is forwarded to the branch router and then to the WAN.
 2b). During the data transfer phase, if the requested data is in its cache, the branch WAE returns its cached data to the client. Traffic does not travel through the WAN to the server farm. Therefore, 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 WAE.
4. The data center 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 WAE forwards the packet to the WAN edge router. The edge router forwards it to the ACE. The 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 ACE performs load balancing to the data traffic. Other functions the 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 ACE and then to the WAN edge router. The WAN edge router forwards the packet to the data center WAE. The data center WAE marks the packet with TCP option 0x21. During the data transfer phase, the data center WAE caches the data if the data is not in its cache.
6. The data center 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 WAE. The branch WAE is aware of the 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 WAE compares its application-specific policy to that of its remote peer defined in the TCP option. At this point, the data center WAE and branch WAE have determined the application optimizations to apply on this specific TCP flow. During the data transfer phase, the branch 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.

Firewall Services Module

Overview

The Cisco Firewall Services Module (FWSM) is a stateful packet inspection engine that delivers access control security between network segments. The FWSM is an integrated service module available on the Catalyst 6500 platform that supports the following two modes of operation:

- *Routed mode*—The FWSM is considered a next hop in the network.
- *Transparent mode*—The FWSM bridges traffic between VLAN segments.

FWSM Virtualization

The FWSM supports device partitioning, allowing a single FWSM to be virtualized into multiple security contexts. The security contexts are logically isolated using independent security rules and routing tables. The system administrator can define up to 100 security contexts on a single FWSM. In

addition, security context deployments support either routed or transparent mode. Service Chaining via Virtualized Network Services shows several configuration options available with the security contexts of the FWSM. FWSM security contexts provide a flexible, scalable solution for data center application deployments.

**Note**

The Oracle E-Business Suite application environment set up for this test document used security contexts in front of the APPL_TOP and database servers.

Design and Implementation Details

Design Goals

The enterprise network is a platform constructed to support a myriad of business functions; more specifically, applications. The traditional perception of the network relegates its role to one of data transport, providing a reliable fabric for the enterprise. This is a fundamental responsibility of the network infrastructure and should be enhanced rather than neglected. In addition to transport, the ubiquitous nature of the enterprise network fabric allows the introduction of intelligent network services to support business applications. This evolution of the network as an enterprise service platform is natural and supports the following Oracle application objectives:

- High availability
- Scalability
- Security
- Optimization
- Manageability

The Cisco data center architecture is a holistic approach that allows the network and the applications it supports to work together. The primary goals of this design are to increase the performance, availability, scalability, and manageability of enterprise applications in the data center, while simultaneously providing a secure environment. In addition, this design reduces the complexity and implementation time of enterprise applications in the data center using virtualization technologies and network design best practices. The remainder of this document focuses on each of these objectives when deploying an Oracle E-Business Suite 12i application using the services of the Cisco data center infrastructure and Cisco empowered branch solutions.

Branch Designs

The WAAS solution requires a minimum of two WAE devices to auto-discover and deliver applicable application optimizations. To leverage these transparent optimizations across the WAN, deploy one or more WAEs at the remote branch and one or more WAEs at the enterprise data center, depending on availability and scalability requirements.

Within the existing branch topologies, the WAE devices may be positioned in one of the following models:

- Extended branch
- Consolidated branch

Figure 13 shows each of these design models. The extended services branch offloads the WAE device from the local branch router and leverages the available ports on a local switch. The consolidated branch model uses an integrated services router, providing a comprehensive solution within a single platform. Each of these models provides application optimization services. The enterprise must consider the scalability and availability requirements of each branch for WAAS and other network services before choosing a deployment model.

**Note**

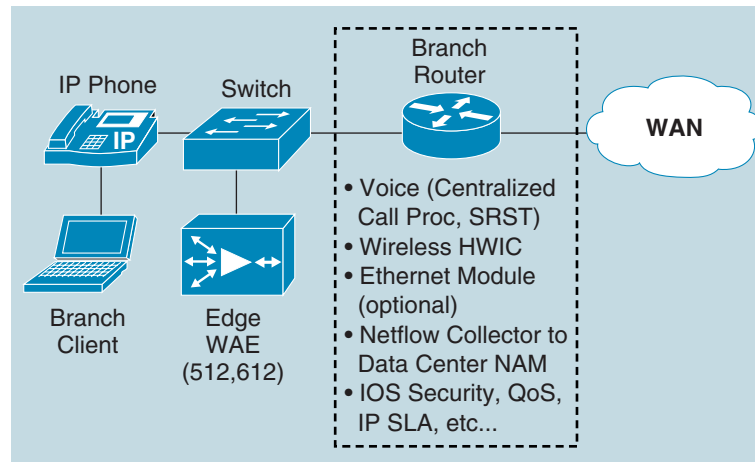
The testing performed to create this document used extended branch design model. For more information on Cisco WAE branch deployments, see *Enterprise Branch Wide Area Application Services Design Guide* at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c649/ccmigration_09186a008081c7d5.pdf

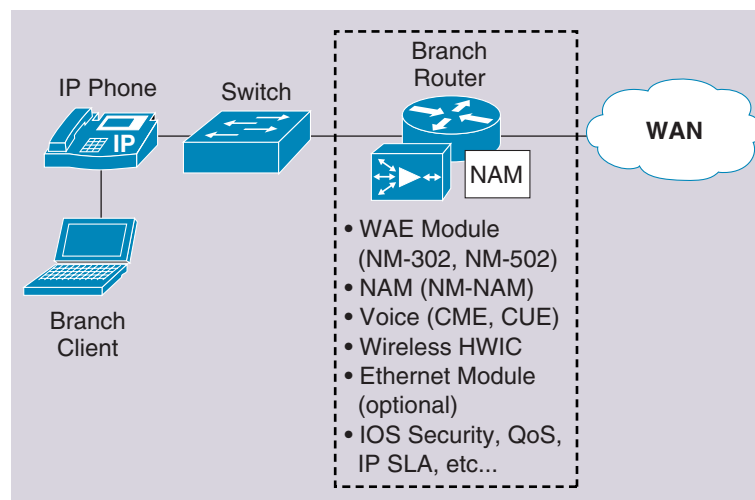
Figure 13 WAE Branch Deployment Models

Branch 1

Extended Services Branch

**Branch 2**

Consolidated Branch



220795

WAAS technology requires the efficient and predictable interception of application traffic to produce results. It is critical that the 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 ACE
- Inline hardware

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

Design Implementation

This section focuses on the different methods of deploying the ACE and FWSM in the Oracle 12i EBS environment. The Cisco Wide Area Application Engine (WAE) will not change, because it will be placed in the data center WAN edge and in the branch. The section is broken out as follows:

- [Design Architecture Details, page 20](#)
- [Bridged vs. Routed ACE and FWSM, page 22](#)
- [ACE Transparent Mode Design, page 23](#)
- [FWSM Transparent \(Bridged\) Design, page 25](#)
- [ACE Routed Mode Design, page 25](#)
- [FWSM Routed Design, page 27](#)
- [WAAS and ACE SSL Offload Performance Summary, page 27](#)

These designs specifically address a multi-tier deployment of the Oracle E-Business Suite application in the Cisco data center infrastructure architecture. The designs provide centralized load balancing, security, and optimization services for the application. In addition, the virtualization capabilities of both the FWSM and the ACE allow a single physical device to provide multiple logical devices to support a variety of application environments.

Design Architecture Details

This section describes the application and network components of the test bed and includes the following sub-topics:

- [Oracle E-Business Suite 12i Environment, page 20](#)
- [Oracle E-Business Suite 12i Environment with Integrated Network Services, page 21](#)
- [ACE Server Load Balancing \(SLB\) Algorithms, page 21](#)
- [Additional Integrated Service Options, page 21](#)

Oracle E-Business Suite 12i Environment

This subsection details the application environment used during testing as well as identify the hardware and software components of the test bed.

Hardware

- A single Penguin Altus 1300 server supports the Oracle 12i database. Accessing this database server is a set of three HP DL580 servers housing the APPL_TOP nodes of this deployment. NFS services at the APPL_TOP layer allowed for a *shared* environment across the nodes.

Software

- Red Hat Enterprise Linux AS Release 4 (Update 5) is the operating system used for all nodes in the test bed. The Oracle test environment consists of the following software packages:
 - E-Business Suite 12i version 12 r 4
 - Oracle Database version 10.1.2

The Oracle E-Business Suite contains a sample database named *Vision*. The Vision database allows the generation of valid application traffic in the test bed using production-ready applications in the Oracle 12i Suite.

Oracle E-Business Suite 12i Environment with Integrated Network Services

This section covers the introduction of network services into the Oracle E-Business Suite solution topology. The network-related hardware and software components are shown in [Table 1](#).

Table 1 Test Bed Network Components

Network Component	Hardware Model	Software Version
Aggregation/access switches	Catalyst 6500 w/Sup720	12.2(18)SXF10
Firewalls	WS-SVC-FWM-1	3.1(6)
Load balancer	ACE10-6500-K9	3.0(0)A2(1.0)
Wide Area Application Service	WAE-7326	4.0.13.12

ACE Server Load Balancing (SLB) Algorithms

The ACE virtual context determines the state of the Oracle environment via health probes. Using this information, the ACE context manages the workload for each Oracle server and the state of the VIP, making the environment highly available and scalable by potentially supporting thousands of E-Business servers. The ACE module currently supports the following load balancing algorithms:

- Round-robin
- Least connections
- Hash address
- Hash cookie
- Hash header
- Hash URL

For this test environment, least connections was used.

Additional Integrated Service Options

This document addresses the integration of network services with the Oracle enterprise class application, E-Business Suite 12i. Server load balancing and security are fundamental services that may be leveraged by data center applications. In addition, this document details the integration of network-based

application optimization services in the data center and remote branch. However, these are not the only integrated network services available for the enterprise. The following network services are also accessible as service modules or appliances:

- SSL offloading (hardware-based option integrated into the ACE platform)
- Intrusion prevention systems (IPS)
- Intrusion detection systems (IDS)
- Network analysis devices
- Caching devices
- Alternative WAN optimization systems such as the Application Velocity System

The management aspect of the data center and branch network environments is critical to the success of the enterprise. In the test bed, the following Cisco management tools were used to monitor and configure the network environment:

- Cisco Application Networking Manager (ANM) to monitor and manage the ACE module
- Cisco Fabric Manager for the SAN configurations
- Cisco Network Analysis Module (NAM)
- Cisco Application Analysis Solution (AAS)

Bridged vs. Routed ACE and FWSM

Both the ACE and the FWSM can be deployed in routed or bridged (transparent) mode. For this test, environment bridged mode was selected. The choice to use either method is dependent on the customer's design requirements. The following list summarizes some considerations to review when deciding whether to deploy the ACE and FWSM in either bridged or routed mode:

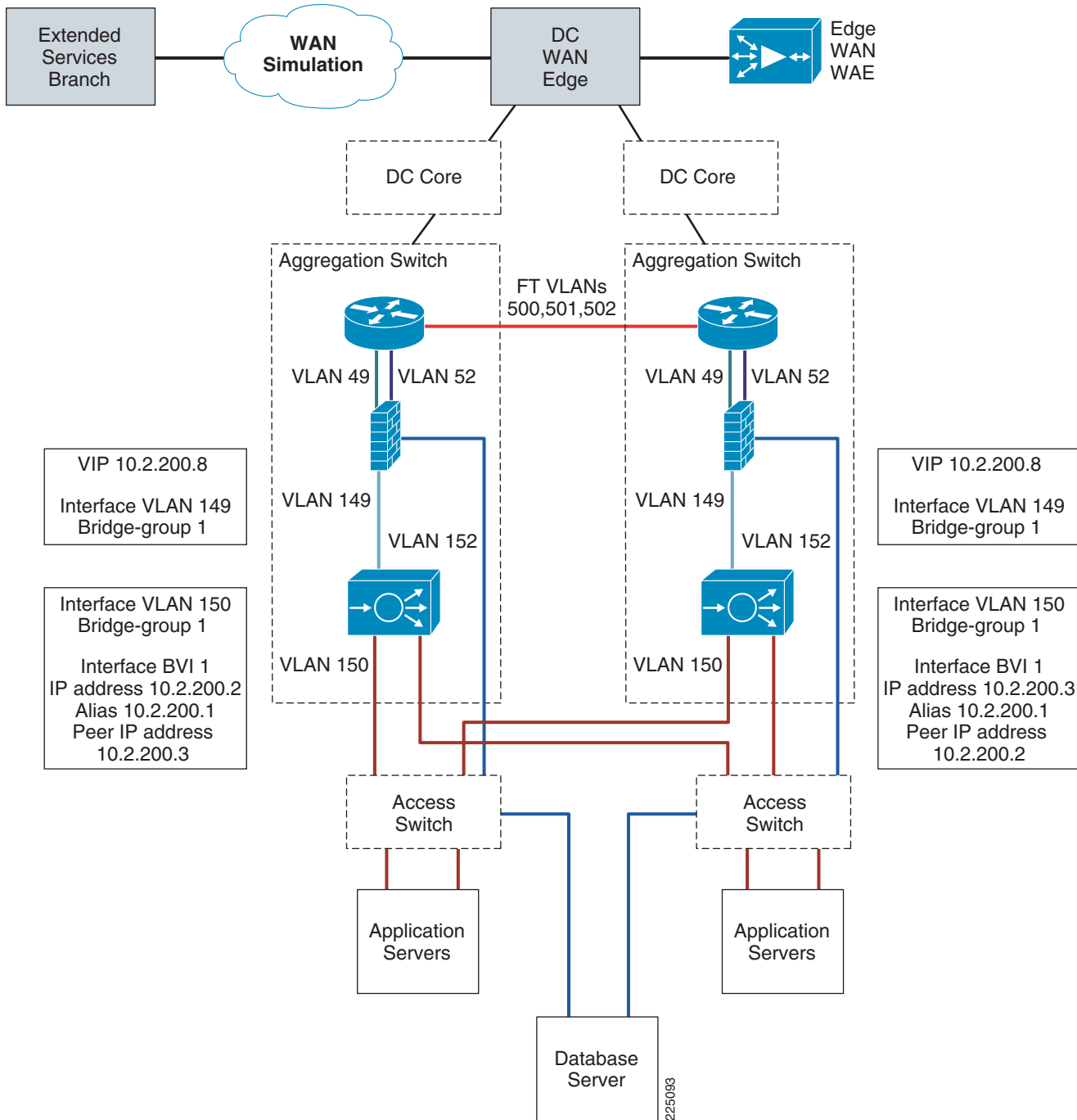
- Ease of configuration and deployment when using the ACE in bridge mode.
- The ACE does not support routing protocols, only static routes.
- The FWSM only supports OSPF and static routes when used in routed mode.
- By using bridged (transparent) mode for the ACE and the FWSM, there are no routing constraints as the Multilayer Switch Feature Card (MSFC) performs all the routing functions.
- Only a single IP address is required when using bridge mode, whereas multiple IPs are required for routing mode.
- The ACE can support multiple contexts (license dependent). Each context can be either routed or bridged.
- The FWSM can support bridged or routed but not both.
- The FWSM is limited to eight bridged interface pairs with FWSM version 3.1; if more than eight interfaces are required then routed mode must be used.
- If active-active is a requirement when using the service modules in bridged mode, the possibility of loops is introduced. This can happen when the heartbeat messages are lost due to the interswitch link (ISL) failure or a configuration error that causes both contexts to believe the other is down. This can be mitigated by forwarding Bridge Protocol Data Units (BPDU) across the service modules. However, to completely remove the possibility of a loop, one of the contexts (ACE or FWSM) must be placed in routed mode.

ACE Transparent Mode Design

Figure 14 details the data center networking topology used in the test Oracle application environment. The extended test branch connects to the data center across the WAN and leverage the services of the enterprise edge and data center core (not pictured here) that attach to the aggregation layer of the data center.

Best practices for the Cisco data center infrastructure offer predictable Layer-2 and Layer-3 traffic patterns, permitting the efficient application of network services. From a Layer-2 perspective, the data center must be scalable, flexible, and robust. Given current application clustering, network interface card (NIC) teaming, and virtual machine requirements, the presence of a Layer-2 redundancy protocol is required and will be for the foreseeable future. At this time, Cisco recommends the use of Rapid Per VLAN Spanning Tree (RPVST)+ to achieve sub-second Layer-2 convergences and deterministic flows in the data center.

Figure 14 Logical Topology using ACE in Transparent Mode



The Layer-3 devices in the aggregation layer use a redundancy protocol such as Hot Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) to create a robust IP network. The MSFC employs an Interior Gateway Protocol (IGP), for instance OSPF or Enhanced Interior Gateway Routing Protocol (IGRP), to distribute route information to the external network—including updates relative to the state of the E-Business Suite applications. This information is derived from the RHI messages received from the active ACE context. In addition to Layer-2 and Layer-3 functionality, the data center aggregation switches together create a natural convergence area in the network and therefore present an ideal location to apply intelligent network services.

**Note**

For more information on data center infrastructure design best practices, refer to the following URL: <http://www.cisco.com/go/designzone>.

The ACE virtual context in this design is in transparent mode and the default gateway of the APPL_TOP servers points to an IP address existing on a VLAN on the MSFC. This IP address is redundant (via HSRP) between the data center aggregation layer switches, offering a redundant Layer-3 topology for the server farms.

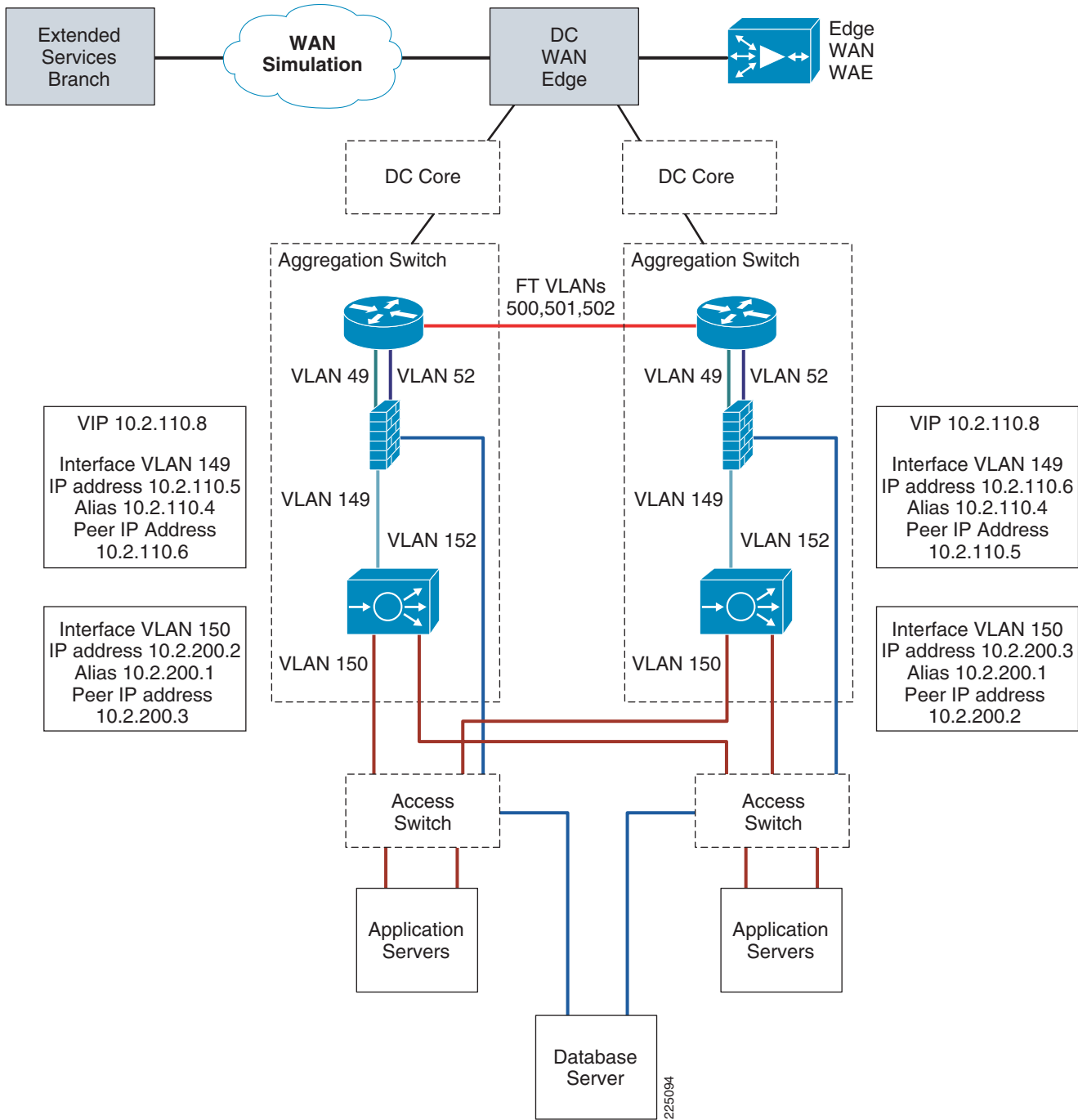
FWSM Transparent (Bridged) Design

In [Figure 14](#), multiple FWSM contexts provide security services to the Oracle APPL_TOP and database tiers. The segmented traffic patterns between tiers in the multi-tier Cisco data center infrastructure allows for granular security policies, as well as application services, to be applied at each layer of the stack. In this instance, there are two transparent firewall contexts deployed. Transparent firewalls are *bumps-in-the-wire*, bridging traffic between VLAN segments. Transparent firewalls allow the construction advanced Layer-2 topologies by passing Bridge Protocol Data Units (BPDUs) between VLAN segments.

ACE Routed Mode Design

[Figure 15](#) shows the Oracle E-Business Suite 12i application environment with the ACE virtual context in a routed mode design. The ACE context provides load balancing, session persistence, and security services to the application.

Figure 15 ACE Routed Mode Test Bed Topology



The routed mode design implies that the ACE is the default gateway for the APPL_TOP server farm. The gateway is accessible via the services of a transparent firewall context. The ACE and firewall context are deployed in an active/standby scenario with stateful failover. An independent pair of transparent virtual firewalls secures the database environment as well. The ability to segment and enforce granular traffic policies at each tier of the application topology is a powerful characteristic of this design.

At the foundation, the application leverages the high availability, scalability, and security features of the Cisco data center infrastructure at Layer 2 and Layer 3. The aggregation switch on the left in [Figure 15](#) represents the *root* of the spanning tree domain and the *active* HSRP Layer-3 interface. To provide efficient traffic patterns in the data center, we recommend keeping active network service contexts aligned with the Layer-2 and -3 topologies. This prevents overutilization of ISLs that might support fault-tolerant protocols in addition to traffic relevant to the application.

The ISLs in the test bed are all 10-Gigabit Ethernet. The access layer switches are dual-homed to the aggregation switches and carry the APPL_TOP and database subnets. The servers are dual-homed to the access layer using an active/standby NIC teaming configuration.

FWSM Routed Design

On the MSFC, static routes are used to push the traffic to the FWSM. These routes are redistributed into the dynamic routing protocol used by the enterprise and become external routes. The FWSM is configured to route traffic to the MSFC. The FWSM acts as a router between connected networks, and each interface requires an IP address on a different subnet. In single context mode, the routed firewall supports Routing Information Protocol (RIP) in passive mode and OSPF. Multiple context mode supports static routes only, although it is recommended that you use the advanced routing capabilities of the upstream and downstream routers instead of relying on the FWSM for extensive routing needs.

WAAS and ACE SSL Offload Performance Summary

This section describes performance testing conducted using the Oracle E-Business Suite application environment using the transparent mode design. The tests were conducted using the Mercury LoadRunner application test tool. Two LoadRunner scripts were created to determine the potential benefits of the Cisco WAAS solution in an Oracle E-Business deployment. The data center and branch environments described earlier provide the end-to-end network connectivity, while using Pagent to inject selected delays for each 30-minute test iteration. These tests simulate a remote branch user accessing applications homed in the data center. The tests used the following WAN variables: T1 and 512Kbps simulating a large branch office and a small branch office, respectively. [Figure 16](#) through [Figure 19](#) illustrate test results.

[Figure 16](#) illustrates the average performance impact on a non-optimized native WAN, and the improvements provided with the Cisco WAAS solution. As the charts in [Figure 17](#) and [Figure 19](#) illustrate, the non-optimized WAN has a negative impact on the user experience. The WAAS solution provides an improved user experience, as indicated by allowing more transactions to occur due to increased throughput. Note that the increased throughput and transactions result from the WAE caching data at the local and remote locations. In addition, the WAE compresses data that traverses the WAN—which also contributes to reduced overall total data being sent over the WAN.

Figure 16 *Total Throughput Summary Using a T1 with 100msec Delay, 0.1 Packet Loss, and 10 Users*

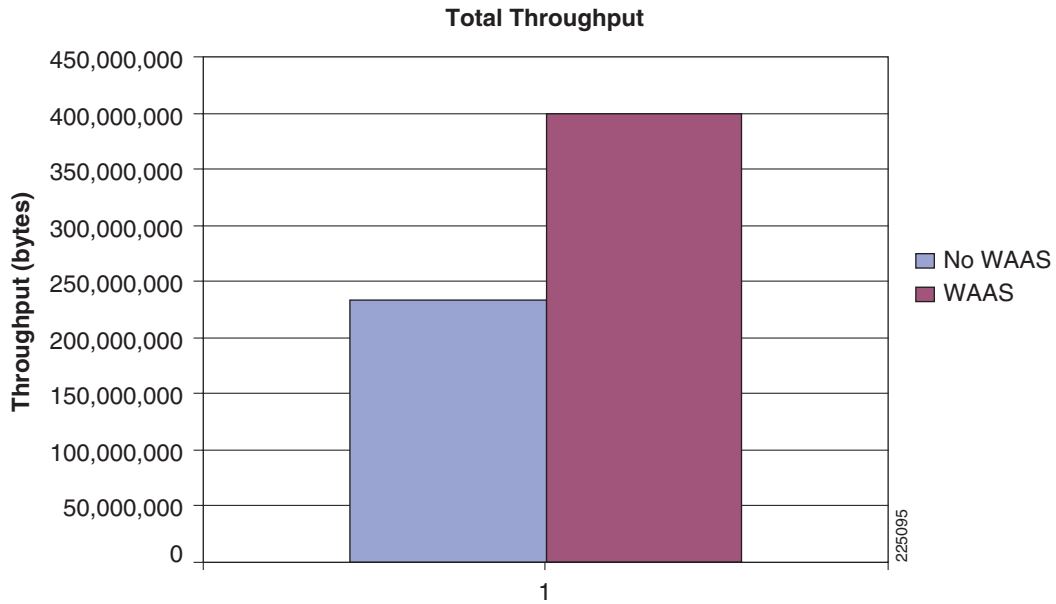


Figure 17 *Total Transaction Throughput Summary Using a T1 with 100msec Delay, 0.1 Packet Loss, and 10 Users*

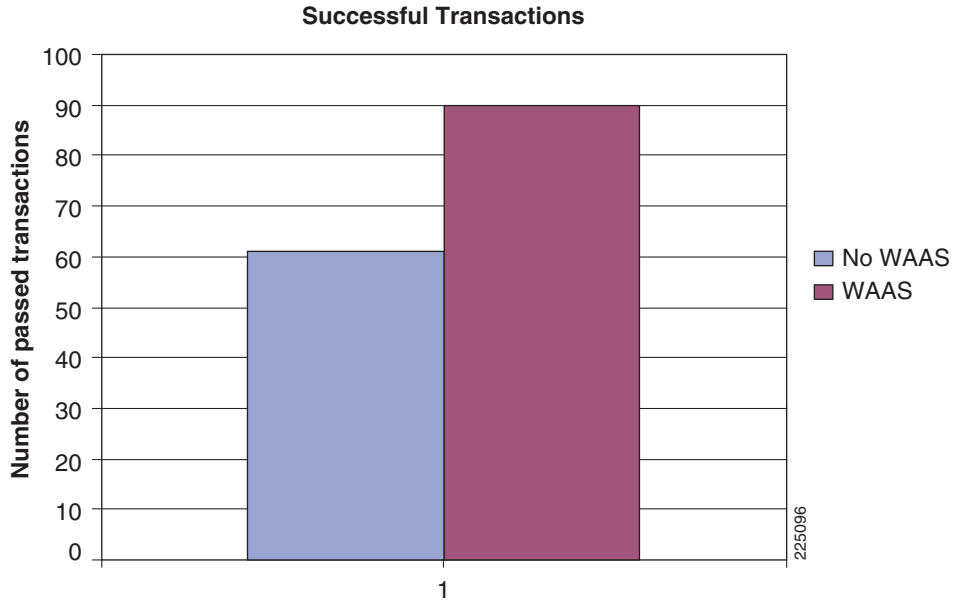


Figure 18 *Total Throughput Summary Using a 512Kbps Link with 200msec Delay, 0.2 Packet Loss, and 5 Users*

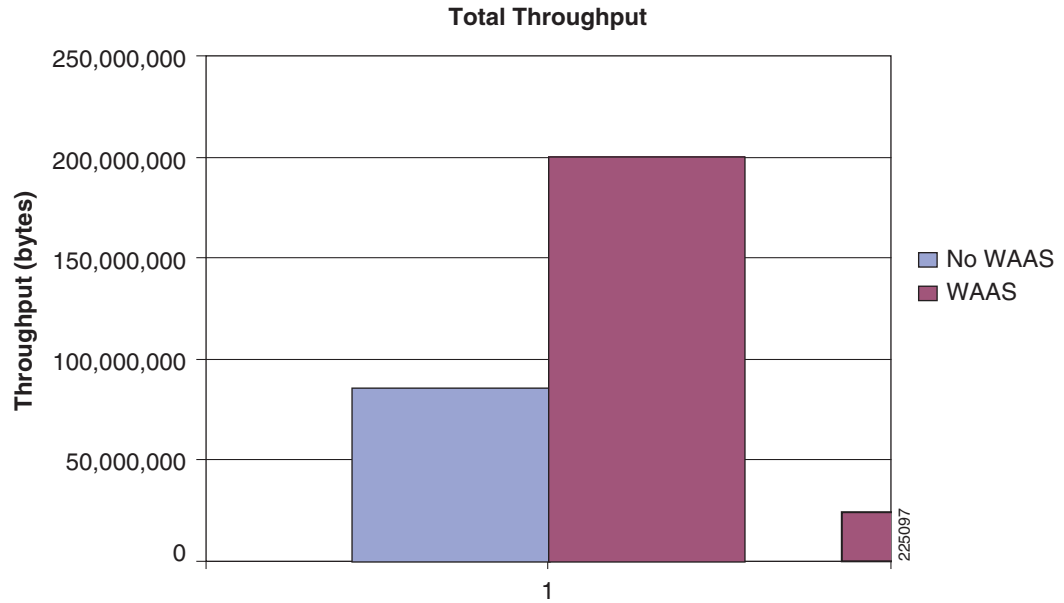
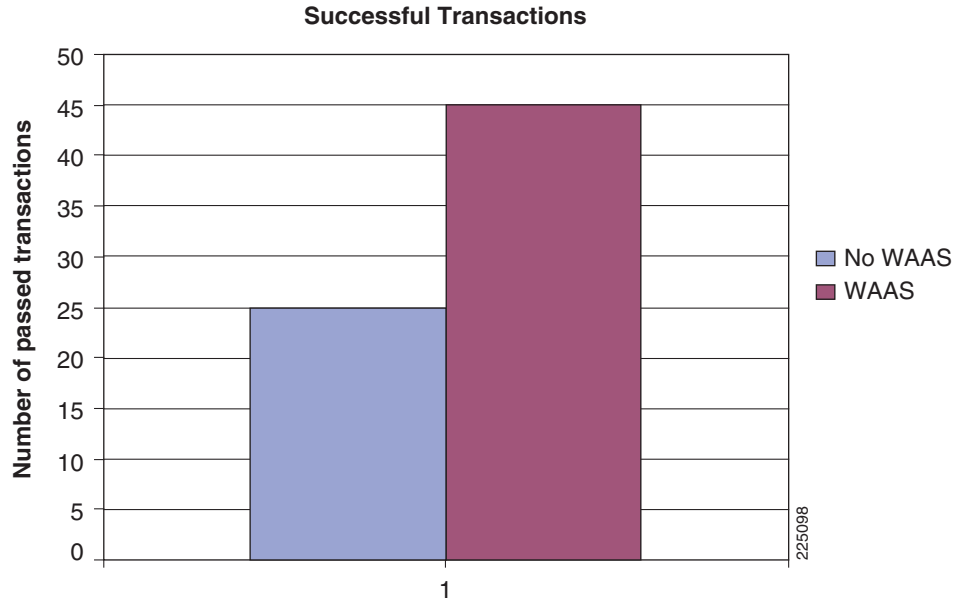


Figure 19 *Total Transaction Throughput Summary Using a 512K Link with 200msec Delay, 0.2 Packet Loss, and 5 Users*



The ACE was tested for Server Load Balancing (SLB) and SSL offload. When using the ACE to perform SSL offload, the ACE communicates with the clients via SSL and communicates with the servers in clear text. This allows the ACE to remove the additional workload that would be needed to be performed by the servers. The ACE performs the encryption and decryption of the SSL traffic between the clients and

the ACE. The test used a single Oracle 12i EBS application server configured for SSL using a load balancer. Table 2 summarizes the required changes when configuring SSL on the Oracle 12i EBS application server and connected to load balancer to perform SSL offload.

Table 2 Changes When Using an SSL Accelerator

Variable	Non-SSL Value	SSL Value
s_url_protocol	http	http
s_local_url_protocol	http	http
s_webentryurlprotocol	http	https
s_active_webport	same as s_webport	Value of the SSL Accelerator’s external interfacing port
s_webentryhost	same as s_webhost	SSL Accelerator hostname
s_webentrydomain	same as s_domainname	SSL Accelerator domain name
s_enable_sslterminator	#	Remove the # symbol to use <i>ssl_terminator.conf</i> in SSL-terminated environments,
s_login_page	URL constructed with http protocol and s_webport	URL constructed with https protocol, s_webentryhost, s_webentrydomain, s_active_webport
s_external_url	URL constructed with http protocol and s_webport	URL constructed with https protocol, s_webentryhost, s_webentrydomain, s_active_webport



Note

For more information on configuring the Oracle 12i EBS application server for SSL offload, refer to the following URL:

https://metalink.oracle.com/metalink/plsql/f?p=130:14:9627043080427676175:::p14_database_id,p14_docid,p14_show_header,p14_show_help,p14_black_frame,p14_font:NOT,376700.1,1,1,1,Helvetica#midtier (requires Oracle Metalink access)

Table 3 and Figure 20 summarize results for an SSL direct environment, while Table 4 and Figure 21 summarize results for an SSL offload environment.

Table 3 Statistics Summary for SSL Direct

Statistics Summary	
Maximum Running Vusers	50
Total Throughput (bytes)	52,566,782
Average Throughput (bytes / second)	103,887
Total Hits	64,000
Average Hits per Second	12,648
Total Passed Transactions	300

Figure 20 Output Example Showing Statistics for SSL Direct

Color	Scale	Measurement	Minimum	Average	Maximum	Std. Deviation
Yellow	100	Average load (Unix Kernel Statistics):10.2.200.10	0	0.054	0.238	0.054
Purple	1	CPU Utilization (Unix Kernel Statistics):10.2.200.10	0	2.561	27.053	5.388
Green	1	Paging rate (Unix Kernel Statistics):10.2.200.10	3.334	17.671	67.348	13.772

Table 4 **Statistics Summary for SSL Offload**

Statistics Summary	
Maximum Running Vusers	50
Total Throughput (bytes)	1,148,910,133
Average Throughput (bytes / second)	3,273,248
Total Hits	139,328
Average Hits per Second	396,946
Total Passed Transactions	4,454

Figure 21 **Output Example Showing Statistics for SSL Offload**

Color	Scale	Measurement	Minimum	Average	Maximum	Std. Deviation
Yellow	10	Average load (Unix Kernel Statistics):10.2.200.10	0	5.791	9.879	2.102
Purple	1	CPU Utilization (Unix Kernel Statistics):10.2.200.10	3.431	59.854	68.753	11.753
Green	0.1	Paging rate (Unix Kernel Statistics):10.2.200.10	11.758	161.218	288.75	62.345

285100

Performance Observation Results

The performance test results indicate that with SSL offload, the number of transactions *increased*. Due to the increased transactions, the CPU utilization, average load, and paging rate increased as compared to SSL direct.

Application Configuration Details

Oracle E-Business Suite requires modifications to the APPL_TOP tier to employ network-based load balancing and SSL offload services. The autoconfiguration file retains the APPL_TOP tier configuration information and must be modified to support these advanced services.

- HTTP load balancing
- Forms listener servlet
- SSL acceleration (Configuration changes shown in the performance section)

Appendix A—Configurations

Note that the MFSC configuration section only indicates the service line card (SVCLC) configuration. The virtual LANs (VLAN) and routing must also be configured.

MFSC Configuration

```
svclc autostate
svclc multiple-vlan-interfaces
svclc module 3 vlan-group 1,3,4,5
svclc vlan-group 1 150,151,158-161,190,191,210,211,220,221,230,231,240,241
svclc vlan-group 1 500
svclc vlan-group 2 49,52,152
svclc vlan-group 3 82,105
svclc vlan-group 4 110
```

```

svclc vlan-group 5 149
firewall multiple-vlan-interfaces
firewall module 1 vlan-group 2,3,5

```

ACE Configuration

ACE Admin Context

```

logging enable
logging fastpath
logging standby
logging console 0
logging timestamp
logging trap 5
logging history 3
logging supervisor 6
logging buffered 3
logging persistent 3
logging monitor 3
logging device-id context-name
logging reject-newconn tcp-queue-full
logging reject-newconn rate-limit-reached
logging reject-newconn cp-buffer-full
logging host 172.28.196.75 udp/514 format emblem

login timeout 60
line vty
  session-limit 100
hostname ACE1-Slot3
boot system image:c6ace-t1k9-mz.A2_1.bin

resource-class Gold
  limit-resource all minimum 10.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
resource-class Silver
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum equal-to-min

access-list anyone line 10 extended permit ip any any
access-list anyone line 20 extended permit icmp any any

parameter-map type connection WAN
  tcp-options selective-ack allow

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
  31 match protocol https any
  32 match protocol snmp any

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
  peer ip address 172.28.196.142 255.255.255.0
  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

context ebs
  description Oracle 12i EBS
  allocate-interface vlan 82
  allocate-interface vlan 149-150
  member Gold

ft group 8
  peer 1
  no preempt
  peer priority 200
  associate-context ebs
  inservice

```

ACE Oracle12i Transparent Mode Context

Generating configuration....

```

crypto csr-params EBSPARMS
  country US
  state California
  locality SJ
  organization-name CMO
  organization-unit ANSteam
  common-name team
  serial-number cisco123
crypto csr-params EBPAPARMS
  country US
  state California
  locality SJ
  organization-name CMO

```

```

organization-unit ANSteam
common-name ebsvip
serial-number cisco123
crypto csr-params EPARMS
country US
state California
locality SJ
organization-name CMO
organization-unit ANSteam
common-name ebsvip.cisco.com
serial-number cisco123
access-list bdpu ethertype permit bpdu

access-list all line 10 extended permit icmp any any
access-list all line 20 extended permit ip any any

probe http web
description This is a basic HTTP Probe
port 8000
interval 5
faildetect 15
passdetect interval 15
receive 2
expect status 200 200
open 2

parameter-map type ssl SSLPARMS
cipher RSA_WITH_RC4_128_MD5
version SSL3

rserver host app1
ip address 10.2.200.10
inservice
rserver host app2
ip address 10.2.200.11
inservice
rserver host app3
ip address 10.2.200.12
inservice

ssl-proxy service SSLPROXY
ssl-proxy service sslproxy
key essl
cert ebsl
ssl advanced-options SSLPARMS

serverfarm host httpsebs
! The application servers listen on port 8000 by default.
serverfarm host httpsebs farm
description This is the httpsebs server farm
probe web
rserver app1 8000
inservice
rserver app2 8000
inservice
rserver app3 8000
inservice

! HTTP cookie sticky is employed for the httpsebs farm
sticky http-cookie acecookie sticky-insert-cookie
cookie insert
replicate sticky

```

```

serverfarm httppebs

class-map match-all ACL
  2 match access-list all

! Oracle httppebs HTTP VIP address
class-map match-all ebsVIP
  10 match virtual-address 10.2.200.8 tcp eq 8000

! Oracle httppebs HTTPS VIP address
class-map match-all ebssslvip
  10 match virtual-address 10.2.200.8 tcp eq 4443

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
class-map match-all server-initiated
  description server initiated connections
  2 match source-address 10.2.200.0 255.255.255.0
  3 match destination-address 10.2.200.8 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit

! This policy references the sticky server farm created to support the HTTP httppebs servers

policy-map type loadbalance first-match VIP-HTTP
  class class-default
    sticky-serverfarm sticky-insert-cookie

! This policy references the sticky server farm created to support the HTTPS httppebs
servers
policy-map type loadbalance first-match VIP-HTTPS
  class class-default
    sticky-serverfarm sticky-insert-cookie

! This policy map is enforced when the destination is the Oracle (HTTP or HTTPS) VIP
(10.2.200.8). Traffic matching that destination has the VIP-HTTP or VIP-HTTPS applied.
This policy references the sticky httppebs farm
policy-map multi-match HTTP-SLB
  class server-initiated
    nat dynamic 1 vlan 150
  class ebsVIP
    loadbalance vip inservice
    loadbalance policy VIP-HTTP
    loadbalance vip icmp-reply
  class ebssslvip
    loadbalance vip inservice
    loadbalance policy VIP-HTTPS
    loadbalance vip icmp-reply
    ssl-proxy server sslproxy

interface vlan 149
  description to the client side
  bridge-group 1
  access-group input bdpu
  access-group input all
  service-policy input remote-access
  service-policy input HTTP-SLB
  no shutdown

```

```

interface vlan 150
  description to the server side
  bridge-group 1
  access-group input bdpu
  access-group input all
  nat-pool 1 10.2.200.250 10.2.200.254 netmask 255.255.255.0 pat
  service-policy input remote-access
  service-policy input HTTP-SLB
  no shutdown

interface bvi 1 (Transparent Mode Bridge Connection)
  ip address 10.2.200.2 255.255.255.0
  alias 10.2.200.1 255.255.255.0
  peer ip address 10.2.200.3 255.255.255.0
  no shutdown

!Default Route to HSRP Address on the Aggregation Catalyst 6500's MSFC
ip route 0.0.0.0 0.0.0.0 10.2.200.4

```

ACE Oracle12i Routed Mode Context

Generating configuration....

```

crypto csr-params EBSPARMS
  country US
  state California
  locality SJ
  organization-name CMO
  organization-unit ANSteam
  common-name team
  serial-number cisco123
crypto csr-params EBPARMS
  country US
  state California
  locality SJ
  organization-name CMO
  organization-unit ANSteam
  common-name ebsvip
  serial-number cisco123
crypto csr-params EPARMS
  country US
  state California
  locality SJ
  organization-name CMO
  organization-unit ANSteam
  common-name ebsvip.cisco.com
  serial-number cisco123
access-list bdpu ethertype permit bdpu

access-list all line 10 extended permit icmp any any
access-list all line 20 extended permit ip any any

probe http web
  description This is a basic HTTP Probe
  port 8000

```

```

interval 5
faildetect 15
passdetect interval 15
receive 2
expect status 200 200
open 2

parameter-map type ssl SSLPARMS
  cipher RSA_WITH_RC4_128_MD5
  version SSL3

rserver host app1
  ip address 10.2.200.10
  inservice
rserver host app2
  ip address 10.2.200.11
  inservice
rserver host app3
  ip address 10.2.200.12
  inservice

ssl-proxy service SSLPROXY
ssl-proxy service sslproxy
  key essl
  cert ebsl
  ssl advanced-options SSLPARMS

serverfarm host httpsebs
  ! The application servers listen on port 8000 by default.
  serverfarm host httpsebs farm
  description This is the httpsebs server farm
  probe web
  rserver app1 8000
  inservice
  rserver app2 8000
  inservice
  rserver app3 8000
  inservice

! HTTP cookie sticky is employed for the httpsebs farm
sticky http-cookie acecookie sticky-insert-cookie
  cookie insert
  replicate sticky
  serverfarm httpsebs

class-map match-all ACL
  2 match access-list all

! Oracle httpsebs HTTP VIP address
class-map match-all ebsVIP
  10 match virtual-address 10.2.110.8 tcp eq 8000

! Oracle httpsebs HTTPS VIP address
class-map match-all ebssslvip
  10 match virtual-address 10.2.110.8 tcp eq 4443

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
class-map match-all server-initiated

```

```

description server initiated connections
2 match source-address 10.2.200.0 255.255.255.0
3 match destination-address 10.2.110.8 255.255.255.255

policy-map type management first-match remote-access
class remote-mgmt
    permit

! This policy references the sticky server farm created to support the HTTP httpbebs
servers

policy-map type loadbalance first-match VIP-HTTP
class class-default
    sticky-serverfarm sticky-insert-cookie

! This policy references the sticky server farm created to support the HTTPS httpbebs
servers
policy-map type loadbalance first-match VIP-HTTPS
class class-default
    sticky-serverfarm sticky-insert-cookie

! This policy map is enforced when the destination is the Oracle (HTTP or HTTPS) VIP
(10.2.200.8). Traffic matching that destination has the VIP-HTTP or VIP-HTTPS applied.
This policy references the sticky httpbebs farm
policy-map multi-match HTTP-SLB
class server-initiated
    nat dynamic 1 vlan 150
class ebsVIP
    loadbalance vip inservice
    loadbalance policy VIP-HTTP
    loadbalance vip icmp-reply
class ebsslvip
    loadbalance vip inservice
    loadbalance policy VIP-HTTPS
    loadbalance vip icmp-reply
    ssl-proxy server sslproxy

interface vlan 149
description to the client side
ip address 10.2.110.5 255.255.255.0
alias 10.2.110.1 255.255.255.0
peer ip address 10.2.110.6 255.255.255.0
access-group input bdpu
access-group input all
service-policy input remote-access
service-policy input HTTP-SLB
no shutdown

interface vlan 150
description to the server side
ip address 10.2.200.2 255.255.255.0
alias 10.2.200.1 255.255.255.0
peer ip address 10.2.200.3 255.255.255.0
access-group input bdpu
access-group input all
nat-pool 1 10.2.200.250 10.2.200.254 netmask 255.255.255.0 pat
service-policy input remote-access
service-policy input HTTP-SLB
no shutdown

!Default Route to HSRP Address on the Aggregation Catalyst 6500's MSFC
ip route 0.0.0.0 0.0.0.0 10.2.110.4

```

FWSM Administrative Configuration (Admin Context)

The following example shows the configuration for the FWSM:

```
FWSM(config)# show run
: Saved
:

FWSM Version 3.1(6) <system>
!
resource acl-partition 12
hostname FWSM-AGG1
enable password 8Ry2YjIyt7RRXU24 encrypted
!
interface Vlan49
!
interface Vlan52
  description bot_database
!
interface Vlan82
!
interface Vlan100
  shutdown
!
interface Vlan105
!
interface Vlan149
!
interface Vlan152
  description top_database
!
interface Vlan501
  description LAN Failover Interface
!
interface Vlan502
  description STATE Failover Interface
!
passwd 2KFQnbNIdI.2KYOU encrypted
class default
  limit-resource IPsec 5
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
failover lan interface failover Vlan501
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover replication http
failover link state Vlan502
failover interface ip failover 192.168.51.1 255.255.255.0 standby 192.168.51.2
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
```

```

    allocate-interface Vlan82
    config-url disk:/admin.cfg
!

context database
    allocate-interface Vlan152
    allocate-interface Vlan52
    config-url disk:/db.cfg
!

context apps
    allocate-interface Vlan149
    allocate-interface Vlan49
    config-url disk:/ap.cfg
!

prompt hostname context
Cryptochecksum:a0ac614cb829ab6933a5fd2889c17b2b
: end

```

FWSM Transparent Mode Configuration (Database Context)

The following example shows the configuration for the FWSM in transparent mode:

```

FWSM/db(config)# show run
: Saved
:
FWSM Version 3.1(6) <context>
!
firewall transparent
hostname db
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan152
nameif inside
bridge-group 1
security-level 100
!
interface Vlan152
nameif outside
bridge-group 1
security-level 0
!
interface BVI1
ip address 10.2.30.4 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list BPDU ethertype permit bpd
pager lines 35
logging enable
logging timestamp
logging buffered informational
logging trap informational

logging asdm informational

```

```

logging queue 0
logging device-id hostname
mtu outside 1500
mtu inside 1500
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group outside in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.2.30.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 360
ssh timeout 5
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect smtp
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect sqlnet
!
service-policy global_policy global
Cryptochecksum:c74e5affba450ceb83052cf618bf7996
: end

```

FWSM Transparent Mode Configuration (Applications Context)

The following example shows the configuration for the FWSM APPS context:

```

FWSM/appltop(config)# show run
: Saved
:
FWSM Version 3.1(6) <context>
!
firewall transparent
hostname apps
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted

```

```

names
!
interface Vlan49
nameif outside
bridge-group 1
security-level 0
!
interface Vlan149
nameif inside
bridge-group 1
security-level 100
!
interface BVI1
ip address 10.2.200.40 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list BPDU ethertype permit bpdu
pager lines 24
logging enable
logging timestamp
logging buffered informational
logging trap informational
logging asdm informational
logging queue 0
logging device-id hostname
mtu outside 1500
mtu inside 1500
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group outside in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.2.200.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect smtp

```

```
inspect sqlnet
inspect skinny
inspect sunrpc
```

```
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
!
service-policy global_policy global
Cryptochecksum:822088e52ddf41626a20bf206a13b80c
: end
```

WAE Configuration

```
! WAAS version 4.0.13 (build b12 Aug 9 2007)
!
device mode application-accelerator
!
!
hostname ANS-CoreWAE
!
!
clock timezone US/Pacific -7 0
!
!
ip domain-name cisco.com
!
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 ip address 10.1.20.2 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
!
ip default-gateway 10.1.20.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 171.70.168.183
!
!
logging console enable
!
ntp server 10.1.3.2
!
!
wccp router-list 1 10.1.20.1
wccp tcp-promiscuous router-list-num 1
```

```

wccp version 2
!
central-manager address 10.1.21.2
cms enable
!
tfo tcp optimized-send-buffer 8192
tfo tcp optimized-receive-buffer 8192
!
!
adapter epm enable
!
! The httpbebs traffic is traversing the WAN using port 8000. The default policy configured
on the WAE will be applied. Note that the httpbebs 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
  name Web
...
! Full optimization is applied to the APPL_TOP WAN traffic
map basic
  name Web classifier HTTP action optimize full

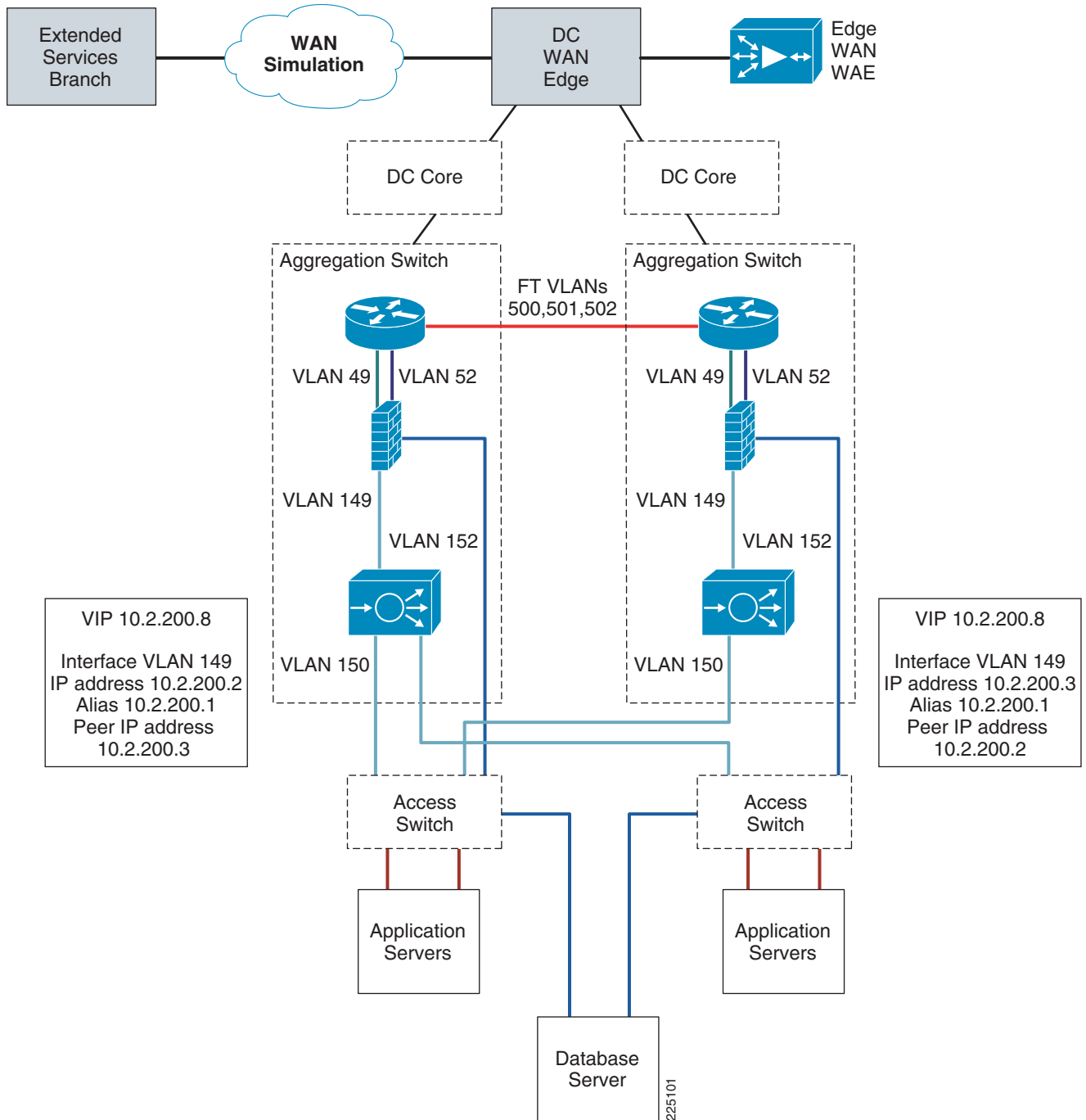
!
!
! End of WAAS configuration

```

Appendix B—One-Armed Mode Configuration

This topology is used when the device that makes the connection to the virtual IP address (VIP) enters the ACE on the same VLAN on which the servers reside. The server reply traffic must return to the ACE before it is sent to the device that initiated the connection. This can be done with either source NAT or policy based routing.

Figure 22 One-Armed Mode Design



Oracle One-Armed Context Configuration

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

probe http web
```

```

port 8081
interval 5
faildetect 15
passdetect interval 15
receive 2
expect status 200 200
open 2

parameter-map type http persist
persistence-rebalance
set header-maxparse-length 8096

rserver host test1
ip address 130.35.85.86
inservice
rserver host test2
ip address 130.35.85.131
inservice

serverfarm host oraclelab
predictor leastconns
probe web
rserver test1 8081
inservice
rserver test2 8081
inservice

sticky http-cookie acecookie sticky-cookie-insert
cookie insert
replicate sticky
serverfarm oraclelab

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
2 match virtual-address 10.2.200.8 tcp eq 8081

class-map match-all server-initiated
description server initiated connections
2 match source-address 10.2.220.0 255.255.255.0
3 match destination-address 10.2.220.8 255.255.255.255

policy-map type management first-match REMOTE-MANAGEMENT
class REMOTE-MANAGEMENT
permit

policy-map type loadbalance first-match vip-oracle
class class-default
sticky-serverfarm sticky-cookie-insert

policy-map multi-match lb-vip
class VIP-HTTP
loadbalance vip inservice
loadbalance policy vip-oracle
loadbalance vip icmp-reply
appl-parameter http advanced-options persist
nat dynamic 1 vlan 149

```

```

policy-map multi-match server-side
  class server-initiated
    nat dynamic 1 vlan 149

interface vlan 149
  description one armed mode
  ip address 10.2.220.2 255.255.255.0
  alias 10.2.220.1 255.255.255.0
  peer ip address 10.2.220.3 255.255.255.0
  access-group input ANYONE
  nat-pool 1 10.2.220.250 10.2.220.254 netmask 255.255.255.0 pat
  service-policy input REMOTE-MANAGEMENT
  service-policy input lb-vip
  service-policy input server-side
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.2.200.4

```

Appendix C—References

Application Networking Services documentation

<http://www.cisco.com/en/US/products/hw/contnetw/index.html>

Oracle Metalink document ID 384248.1—“Sharing the Application Tier File System in Oracle E-Business Suite Release 12.”

Oracle Applications Installation Guide: Using Rapid Install Release 12 (Part No. B31295-02)
http://download-west.oracle.com/docs/cd/B34956_01/current/acrobat/120oaig.pdf

Appendix D—Glossary

Table 5 *Glossary*

Term	Definition
Cisco Application Control Engine (ACE)	The Cisco Application Control Engine is a module within the Catalyst 6500 Series switch that allows applications resources to be distributed and managed via logical groups within a given physical platform. The ACE also provides high levels of Layer 4 through Layer 7 performance (16 Gbps and 345,000 connections per second) to optimize application performance and provide scalability.
Cisco Firewall Services Module (FWSM)	The Cisco Firewall Services Module (FWSM) is a high-speed, integrated firewall module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that provides the fastest firewall data rates in the industry: 5 Gbps throughput, 100,000 CPS, and 1M concurrent connections. Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis.

Table 5 **Glossary**

Term	Definition
Cisco Wide Area Application Engine (WAE)	The Cisco Wide Area Application Engine (WAE) platforms provide a portfolio of powerful, scalable network appliances that host WAN optimization and application acceleration solutions to enable branch office server consolidation and to provide performance improvements for centralized application. In addition, the WAEs provide remote users with LAN-like access to applications, storage, and content across the WAN.
Cisco WAAS Central Manager	Cisco WAAS is centrally managed by a scalable, secure, and simple function called the Cisco WAAS Central Manager that runs on Cisco WAE appliances. The central manager can be configured for high availability by deploying a pair of Cisco WAEs as central managers; configuration and monitoring data is automatically shared by the two central manager WAEs. The central manager provides a centralized mechanism for configuring features and reporting, and can manage a topology containing thousands of Cisco WAE nodes.