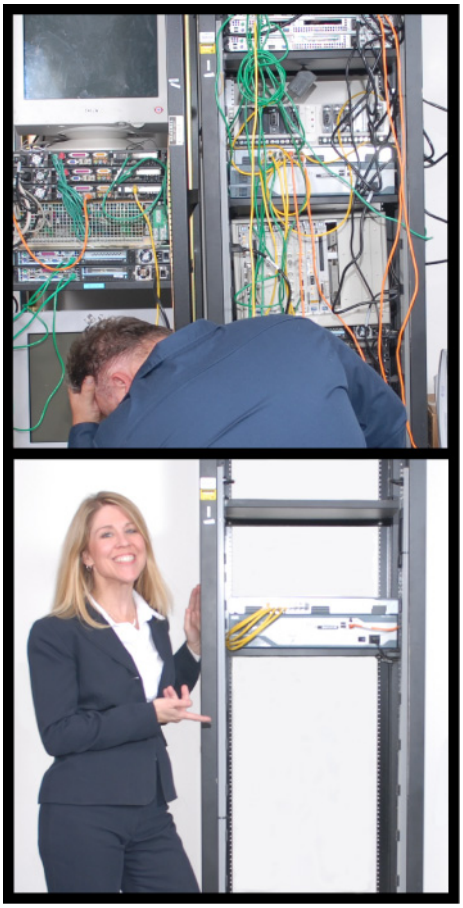


Cisco Lean Retail Architecture—Oracle Store Inventory Management Application Deployment Guide

Cisco Validated Design

February 9, 2009

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

Contents

Solution Overview

This document provides best practices to enhance the Oracle Store Inventory Management application within a Cisco Lean Retail environment. It introduces key concepts and options regarding the application deployment and detailed designs strategies available to multiple store footprints and data center leveraging Cisco application and networking technologies.

Solution Description

Cisco's Lean Retail Oracle Store Inventory Management solution provides best practices and implementation guidance that optimizes Oracle's SIM application availability, performance, scalability, and security while lowering application ownership costs. Cisco's Lean Retail architecture provides accelerated application performance and improved access to information. Data center-based applications and hosted managed services can have their performance accelerated to LAN-like speeds. Oracle Store Inventory Management is a strategic business application developed to assist enterprise class retailers in addressing in-store supply/inventory challenges. Cisco's Lean Retail architecture includes:

- Application and collaboration services
- Integrated networking services
- Reference network designs

A key Lean Retail integrated network service is Cisco's Application Networking Service (ANS). This service includes the Cisco Application Control Engine (ACE) and Wide Area Application Services (WAAS) product families. It provides data center, retail store, and remote end-user application optimization services. This service addresses the following Oracle SIM deployment challenges:

- Application availability
- Application response time over limited WAN connections
- Application scalability

The value of Cisco's Lean Retail is accomplished through five key benefits:

- Application availability—When an application server fails in a store, only that store is impacted. When an application fails in a data center, many stores are impacted. A core tenet of Cisco's Lean Retail is the centralization of application services. Through server virtualization and application load balancing, greater application uptime is achieved. Virtualized server resources in the data center leverage clustering and load balancing to share and distribute application load across a larger pool of resources. A single failure does not impact overall accessibility of the application users.
- Performance improvement—Traditionally, retailers use low bandwidth links. Many retailers have hundreds to thousands of stores. The incremental addition of WAN bandwidth per store significantly increases OPEX costs due to economies of scale. Retailers get more for less through the use of virtualized servers, load balancing, and WAAS. Performance is significantly improved for the end-user (both in stores and across the Web). Servers are more fully utilized when loads are balanced across larger clusters. WAN performance is improved by locally caching content and accelerating the TCP protocol.
- Application scalability—As additional users log in and begin executing transactions through an application, it is important that the performance of each user remains constant. By providing linear scalability through the RDBMS, the application and the underlying servers, retailers can achieve that goal. Cisco ACE provides server load-balancing services that spread the application load across a pool of servers.

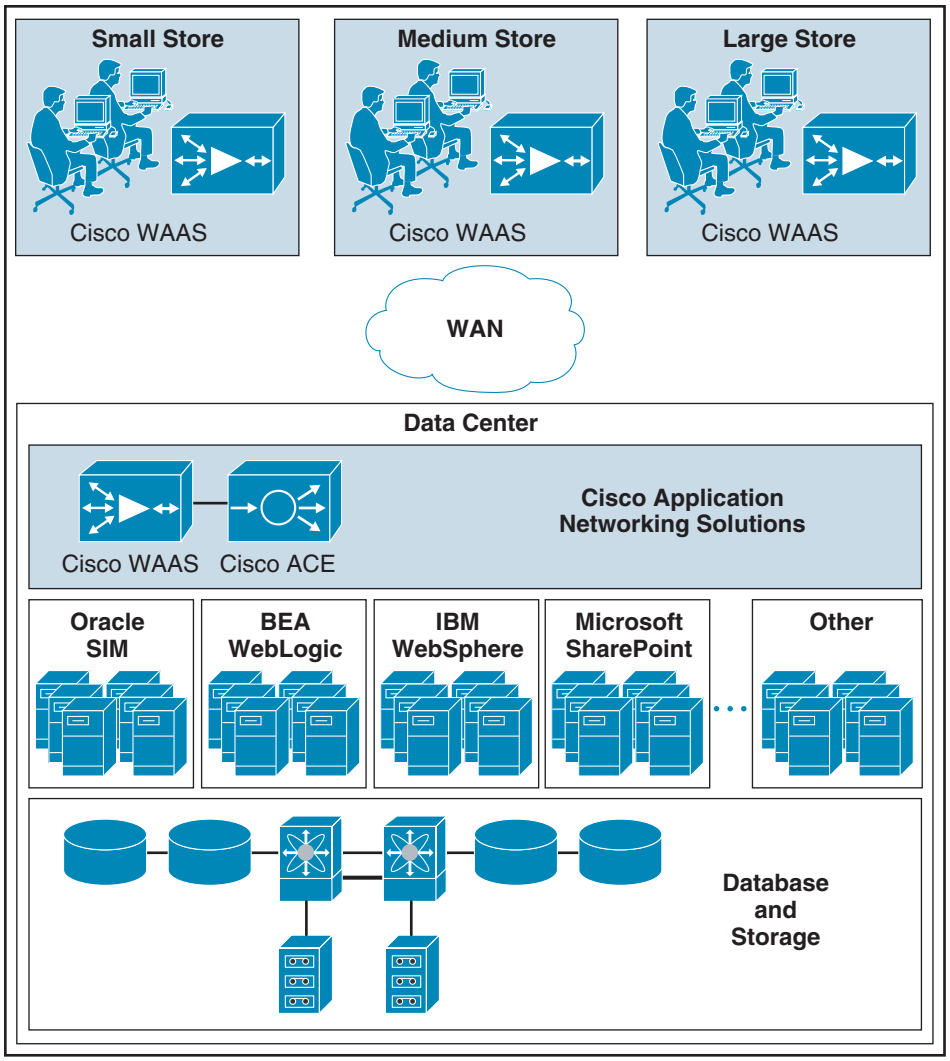
- Increased security—Retailers need to comply with industry and regulatory requirements (e.g., PCI, HIPPA, and SOX to avoid fines and penalties). Security features including encryption, segmentation, and authentication address many of these requirements. Cisco ACE applies stateful inspection rules that explicitly allow or deny specified traffic patterns. Cisco ACE also uses role-based access control to give independent access to both security and load-balancing policies.
- Lowering hardware and software TCO—Many retailers have hundreds to thousands of stores. Typically they have several servers in each store. For both existing and new applications, the incremental costs per store are significant. By removing servers from the stores, retailers are able to reduce OPEX costs on average of 16%[1].

Deploying new applications and capabilities quickly and effectively are key IT metrics that improve an organization's business agility. Cisco's Lean Retail enables more applications to be deployed centrally, cutting down dramatically on the time and cost of deployment. Deploying centrally also reduces the costs of opening new stores and of integrating acquisitions. While many retailers will choose to deploy some applications in the stores, the Lean Retail architecture improves the capabilities of a central deployment model. To learn more about the Cisco Lean Retail, refer to the following URL:

http://www.cisco.com/web/strategy/retail/lean-retail.html

1. Gartner: Server consolidation can save money 12/2005.

Figure 1 Virtualization of Application Optimization Services



The application optimization services of this solution reside both in the data center and the stores to offer end-to-end value, from store 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 Oracle deployments as well as other enterprise applications. Because of their unique location, these solutions can take intelligent action on the end-user traffic before it is routed to the Oracle application servers, including load balancing, server health monitoring, and security access control.

  While some of these functions could be provided natively by the Oracle 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.

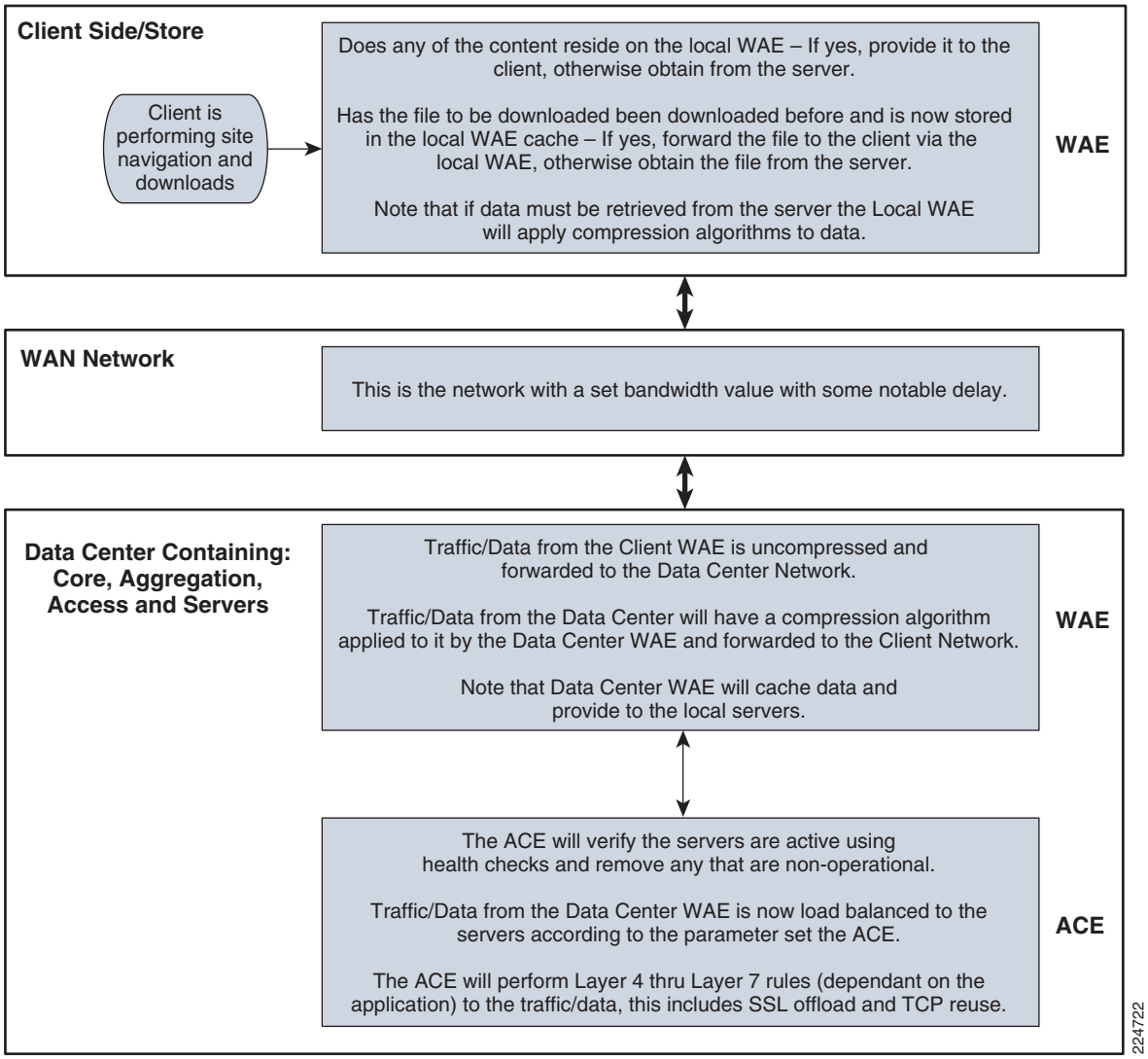
- Wide Area Application Optimization Services

  Cisco WAAS also resides in the store (WAAS appliance and WAAS mobile) and is arranged to provide application acceleration services for all application users in that location in addition to server consolidation. 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 Oracle application servers respond to end-user requests, the response is compressed and then most efficiently passed across the WAN, with minimal bandwidth usage and maximum speed. Commonly used information is cached both at the Cisco WAAS solution in the store as well as in the Cisco ACE/WAAS solution in the data center, which reduces the burden on the servers and the WAN.

Process Flow

Figure 2 Process Flow



Objective

The objectives of the Lean Retail Oracle Store Inventory Management solution testing are to:

- Ensure interoperability (functional testing) between Oracle's Store Inventory Management application, an Oracle RDBMS and Cisco's networking components that comprise the overall Lean Retail Architecture—routers, switches, firewalls, load balancer, and application enhancement engines.
- Enhance Oracle SIM performance in several areas—client download, log on, inventory transaction, and log off.
- Demonstrate bandwidth savings across several different recommended store designs ranging from small to large with respective varying bandwidth wide area networks.
- Detail deployment and lessons learned.

Cisco and Oracle cooperated in all phases of the Cisco Lean Retail Architecture—Oracle Retail Store Inventory Management testing and validation project, including lab setup at Cisco offices, solution functional and performance testing, and in writing this deployment guide. Cisco and Oracle jointly validate that the lab setup and this joint solution testing represents best efforts in creating a realistic customer deployment and accurate documentation of such deployment.

Scope

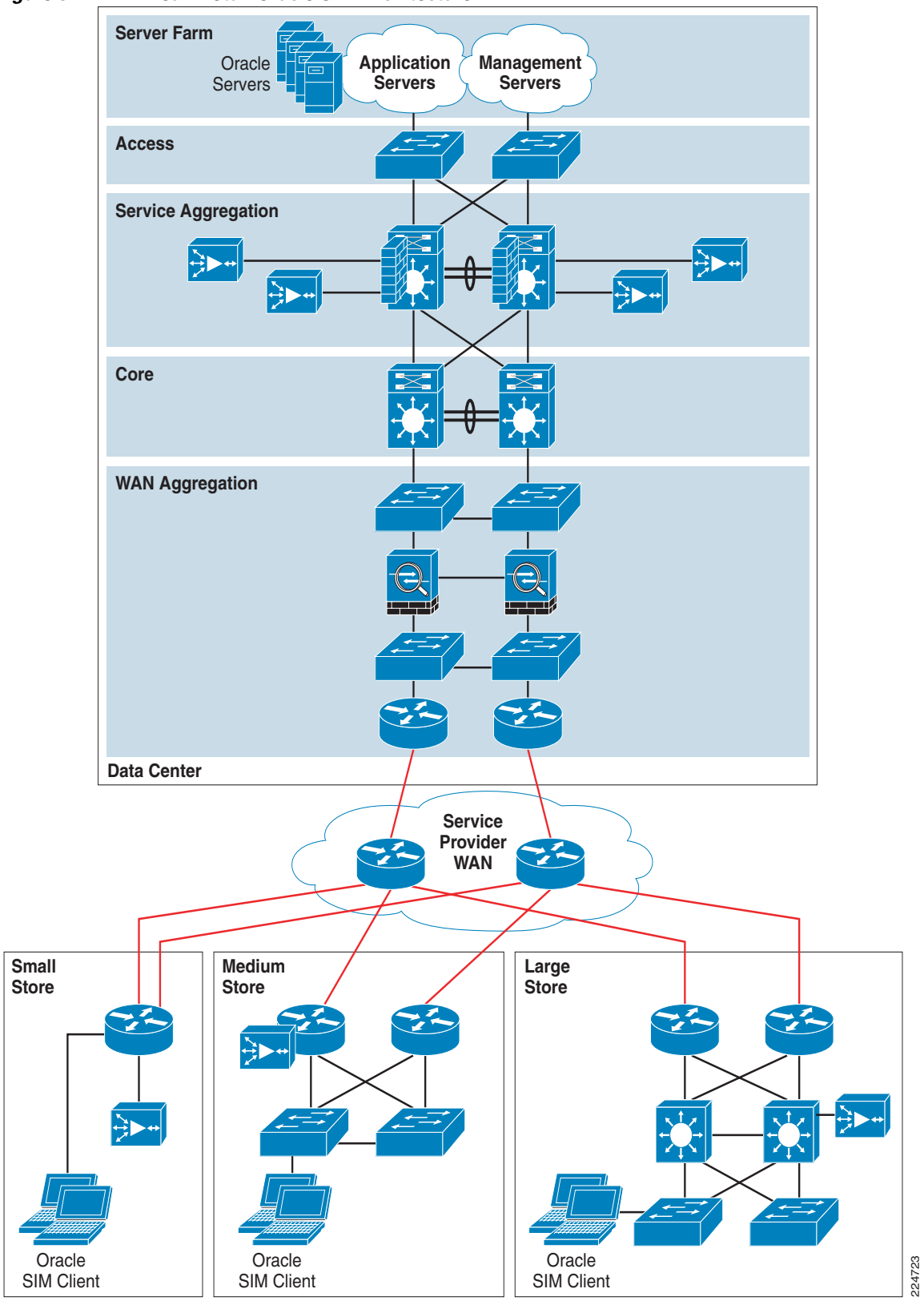
Cisco data center and store architectures are established enterprise designs that deliver highly available and robust network infrastructures. This document describes the deployment of the Oracle Store Inventory Management application in a Cisco data center, while leveraging services available in multiple store footprints. This end-to-end solution design employs many integrated network services, including load balancing, security, and application optimization.

- Only specific features of the Oracle SIM application were tested; Oracle provided a detailed list of transactions that were to be tested based on traditional performance seen in low speed links of customers.
- Testing of the Oracle SIM application was limited to three store deployment scenarios connected to a central data center.
- The range of applications running, within the Cisco lab, did not emulate a production-level data center. The size of the server farm and SAN in the testing environment do not accurately represent the typical breadth deployed in enterprise retail data centers today. Given this inherent limitation, the comprehensive benefits of the Lean Retail Architecture could not be fully demonstrated during this validation project. The use of server and storage virtualization reduces the need for server hardware and adds the ability to provide dynamic provisioning of server capacity. By deploying Cisco's ACE product across a server farm that is executing a full range of retail applications, there should be significant economies of scale in increased performance and scalability, as well as failover capabilities should a server stop running.

Solution Technical Architecture

Figure 3 shows the Lean Retail Oracle SIM architecture.

Figure 3 Lean Retail Oracle SIM Architecture



Oracle Store Inventory Management Technology Stack

Oracle SIM has an *N*-tier architecture consisting of a client-tier, a server-tier, and a data-tier. The client-tier contains a PC client (a Java desktop application) and handheld devices. The server-tier contains the SIM server (deployed as a J2EE application inside the Oracle Application Server) and the Wavelink server (a standalone server for the handheld devices). The data-tier consists of an Oracle 10g database and an LDAP directory.

Advantages of the Architecture

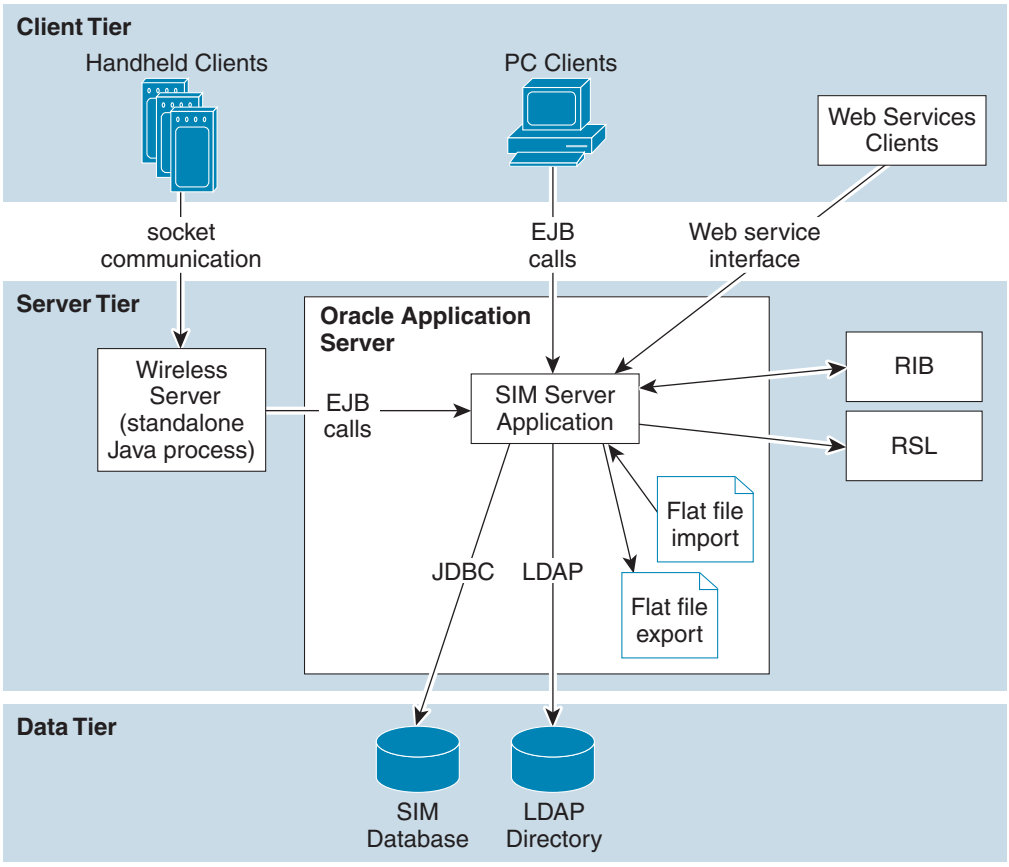
Oracle SIM's robust distributed computing platform enables enhanced performance and allows for scalability. The *N*-tier architecture of SIM allows for the encapsulation of business logic, shielding the client from the complexity of the backend system. Any given tier need not be concerned with the internal functional tasks of any other tier. The following is a summary of the advantages that accompany SIM's use of an *N*-tier architectural design:

- Scalability—Hardware and software can be added to meet retailer requirements for each of the tiers.
- Maintainability—The separation of presentation, business logic, and data makes the software cleaner, more maintainable, and easier to modify.
- Platform independence—The code is written once but can run anywhere that Java can run.
- Cost effectiveness—Open source market-proven technology is utilized, while object-oriented design increases reusability for faster development and deployment.
- Ease of integration—The reuse of business objects and function allows for faster integration to enterprise subsystems. *N*-tier architecture has become an industry standard.
- High availability—Middleware is designed to run in a clustered environment or on a low-cost blade server.
- Endurance—Multi-tiered physically distributed architecture extends the life of the system.
- Flexibility—The system allocates resources dynamically based on the workload.

Oracle SIM Technical Architecture Overview

This section provides a high-level overview of Oracle SIM's technical architecture. Figure 4 illustrate the major parts of the typical three-tiered SIM implementation.

Figure 4 Oracle SIM's Technical Architecture



Client Tier

SIM can be deployed on a wide variety of clients, including a desktop computer, a handheld wireless device, and so on. The GUI is responsible for presenting data to the user and for receiving data directly from the user through the "frontend". The presentation-tier only interacts with the middle application-tier (as opposed to the database-tier). To optimize performance, the SIM PC frontend facilitates robust client-side processing. The PC side of SIM is built upon a fat client architecture, which was developed using Swing, a toolkit for creating rich graphical user interfaces (GUIs) in Java applications. The fat Java client is downloaded to each store PC via a browser URL. The handheld communication infrastructure piece, known as the Oracle Retail Wireless Foundation Server, enables the handheld devices to communicate with the SIM server. The handheld devices "talk" to the Oracle Retail Wireless Foundation Server, which in turn makes calls as a client to the SIM server.

Middle Tier

By providing the link between the SIM client and the database, the middle application-tier handles virtually all of the business logic processing that occurs within SIM's multi-tiered architecture. The middle-tier is comprised of services, most of which are related to business functionality. For example, an item service gets items, and so on. Within SIM, business objects are beans (that is, Java classes that have one or more attributes and corresponding set/get methods) that represent a functional entity. Most business objects have very few operations; in other words, business objects can be thought of as data containers, which by themselves have almost no business functionality.

Although the PC client and the handheld client use the middle-tier's functionality differently, the middle-tier is the same for both clients. For example, the handheld device, used 'on the fly', performs frequent commits to the database, while the PC performs more infrequent commits. The application is flexible in that it accommodates the different styles of client-driven processing. The middle-tier is designed to operate in a 'stateless' manner, meaning it receives whatever instruction it needs to access the database from the client and does not retain any information between client calls. Further, SIM has failover abilities; if a specific middle-tier server fails, processing can roll over to another SIM server for continued processing. If the workload warrants, SIM can be vertically scaled by adding additional application servers. Because SIM servers are running on multiple application servers in a stateless system, work can be seamlessly distributed among the servers. The result of this feature is that SIM clients do not need to know that additional application servers have been added to help with the workload. SIM application servers can contain multiple containers, each of which is related to a unique Java Virtual Machine (JVM). Each container corresponds to a specific SIM instance. Introducing multiple instances of a container allows SIM retailers to more effectively distribute the processing among several containers and thereby horizontally scale the platform. As the request load for a service increases, additional instances of the service are automatically created to handle the increased workload.

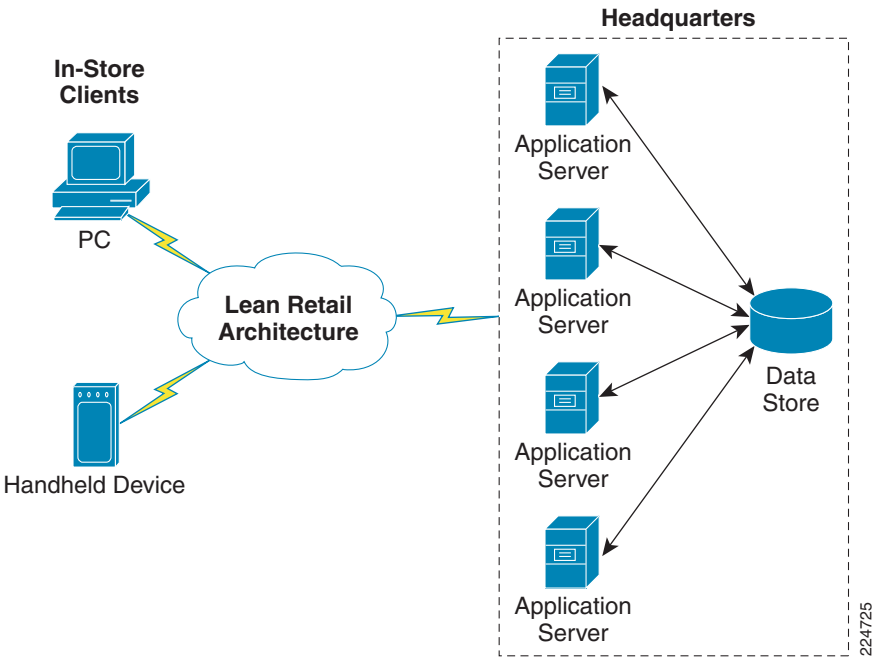
The middle-tier consists of the following core components, which allow it to make efficient and reliable calls to the SIM database:

- Server services contain the pertinent business logic.
- DAO objects handle database interaction.
- Databeans contain the SQL necessary to retrieve data from and save data to the database. 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.

Note There is at least one databean for every table and view in the database, but there may be more used for different specific purposes.

The Oracle Application Architecture (see Figure 5) uses the *N*-tier model by distributing application services across nodes in the server farm.

Figure 5 Oracle Application Architecture



SIM 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 hosts to provide the enterprise with the required performance or application availability.

Data Access Objects (DAO)

DAOs are classes that contain the logic necessary to find and maintain data persistence. They are used by services when database interaction is required.

Java Database Connectivity (JDBC)

DAOs communicate with the database via the industry standard Java database connectivity (JDBC) protocol. In order for the SIM client to retrieve the desired data from the database, a JDBC connection must exist between the middle-tier and the database. JDBC facilitates the communication between a Java application and a relational database. In essence, JDBC is a set of application programming interfaces APIs that offer a database-independent means of extracting and/or inserting data to or from a database. To perform those insertions and extractions, SQL code also resides in this tier facilitating create, read, update, and delete actions.

Data Tier

Note The SIM data model includes some tables and columns that are SIM-specific and some that derive their names from the Association for Retail Technology Standards (ARTS) data model. Note, though, that SIM uses but does not fully conform to the ARTS standard. The data-tier is the application's storage platform, containing the physical data used throughout the application. The database houses data in tables and views; the data is used by the SIM server and then passed to the client. The database also houses stored procedures to do data manipulation in the database itself.

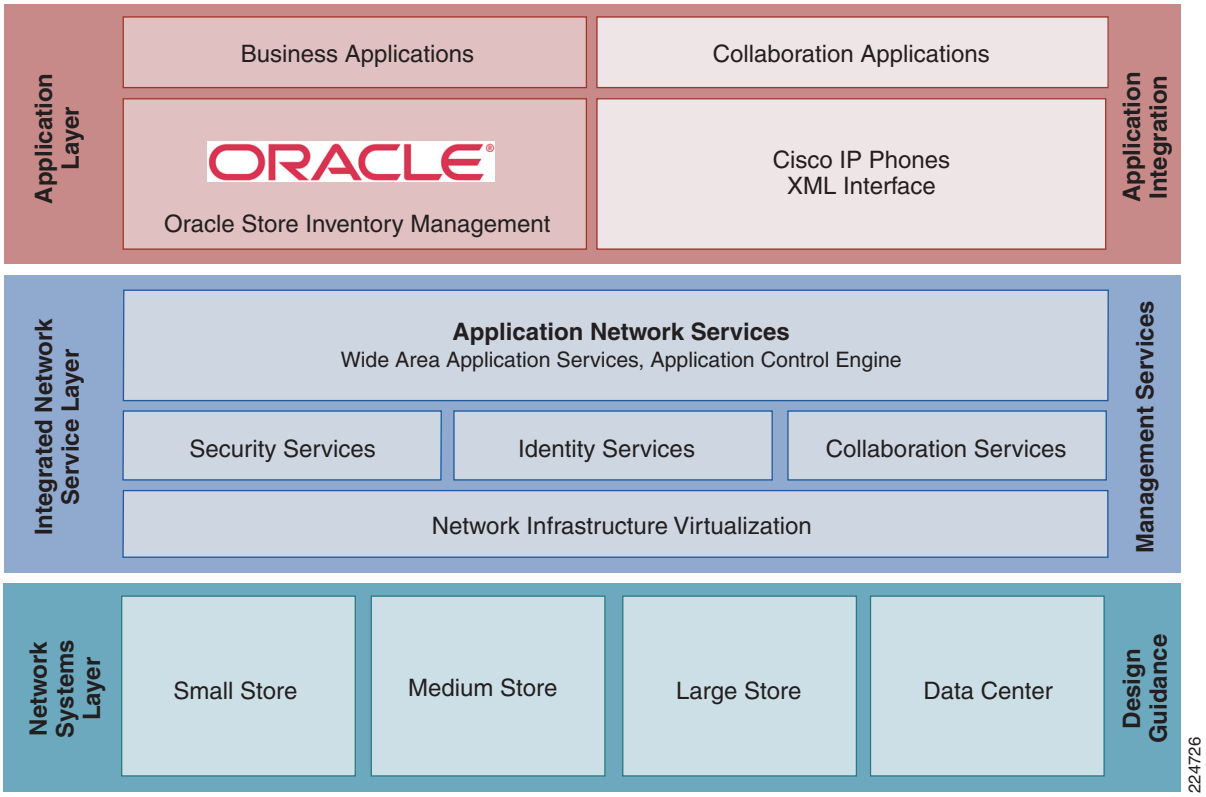
Distributed Topology

One of SIM's most significant advantages is its flexible distributed topology. SIM offers complete location transparency because the location of data and/or services is based upon the retailer's business requirements, not upon technical limitations. SIM's client server communication is an EJB call (which uses RMI). Because the server does not have to be in the same store as the in-store clients, the clients log onto the server 'over the wire'. SIM's client code makes use of helper and framework classes that contain the logic to look up remote references to EJBs on the server and make calls to them. These helper and framework contain no business logic but contain only enough code to communicate with the server. For example, if a helper class is called by the client to perform the method 'update shipment', the helper class appears to have that capability, though in reality it only behaves as a passage to the EJB remote reference, which is looked up from the server. The EJB remote reference communicates across the network with the server to complete the business-logic driven processing. The server performs the actual 'update shipment' business logic and returns any return values or errors to the client. Connectivity between the SIM client and the middle-tier is achieved via the Java Naming and Directory Interface (JNDI), which the SIM client accesses with the necessary IP address and port. JNDI contains the means for the client to look up services available on the application server.

Cisco's Lean Retail Network Architecture

Cisco's Lean Retail Store Inventory Management solution was developed and tested using Cisco's Connected Retail Framework. This model depicts the relationships between applications such as Oracles SIM application and the network infrastructure. Figure 6 represents the solution framework.

Figure 6 Connected Retail Framework



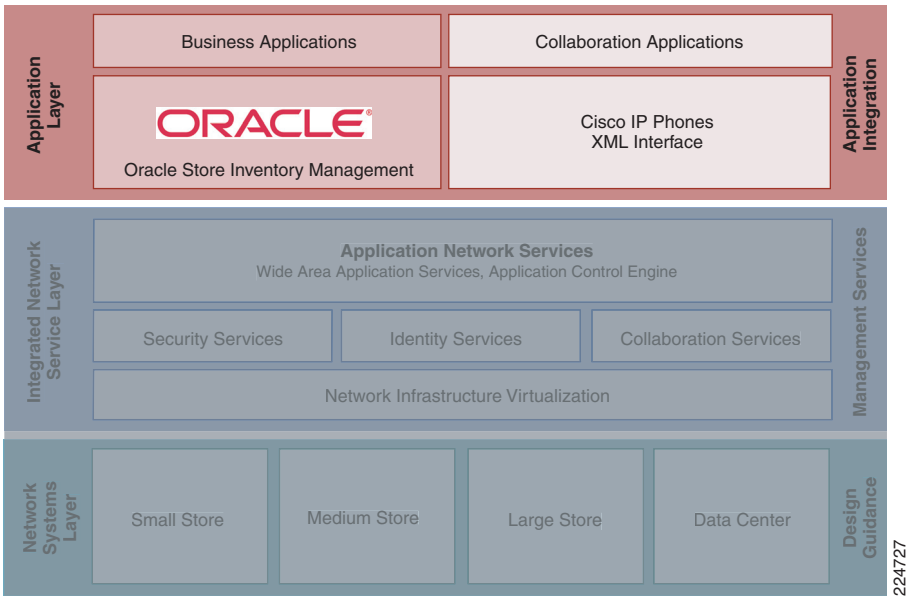
The solution framework is divided into three functional layers:

- *Application*—Business and collaboration applications connect users and business process to the infrastructure.
- *Integrated Network Services*—Application Networking Services (ANS), Unified Communications, Identity, and Security services extend and virtualize from the network to the applications.
- *Network Systems*—Connected Retail Store architectures serve as the adaptable, secure platform.

Application Layer

Business and collaboration applications connect users and business processes to the infrastructure. The application layer (see Figure 7) of the framework includes the business and collaboration applications from Oracle and Cisco.

Figure 7 Application Layer



Oracle SIM Application

Oracle Retail Store Inventory Management is part of Oracle Retail's In-Store Operations solution group. Oracle Retail Store Inventory Management allows store personnel to quickly and easily perform an array of in-store operations to receive merchandise, manage physical inventories, conduct stock counts, order stock, or transfer stock.

Oracle Retail Store Inventory Management enables retailers to streamline in-store activities, improve merchandise management and productivity, reduce labor costs, support remote store processes, and manage true store-level profit and loss.

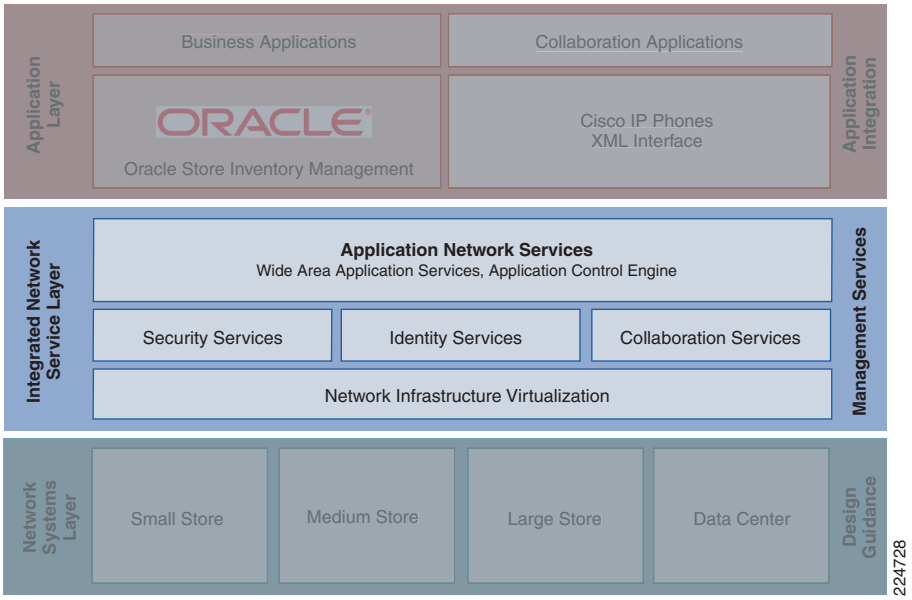
- Fully integrated with the Oracle Retail Merchandising System to provide instantaneous, real-time data communications between stores and the corporate office, eliminating the need for batch processing systems.
- Real-time access to the same store data unites the whole organization in a customer-centric approach, allowing better monitoring progress, ability to respond immediately to customer needs and adjust buys for continual improvement.

- Oracle Retail Store Inventory Management, coupled with the Oracle Retail Merchandising System, provides the power and processes behind a retailer's day-to-day buying and selling activities. It can record and analyze inventory results and merchandise processes daily to help retailers know that the business decisions are based on timely, accurate information.
- Easy-to-use features minimize the need for extensive training, IT experience, and expensive software or hardware investments.

Integrated Network Services Layer

Within the Connected Retail Framework, the Integrated Network Services layer (see Figure 8) is where filtering, caching, and protocol optimization interact with applications or application middleware services to optimize the performance from the network to the end-user. Process control is simplified by using common infrastructure services such as collaboration, security, and identity. These are key advantages that aid in operational reporting and security policy enforcements. Fewer services that are shared across more intelligent devices increases the operational efficiency of the whole system.

Figure 8 Integrated Network Services Layer



- *Application Networking Services*—WAAS and ACE provide application availability, decreased application response time, and increased performance.
- *Voice and collaboration services*—Created by adding the voice IOS service to the store routers, and adding Cisco Unified Communication Manager and application servers to the data center.
- *Network virtualization* —Cisco Integrated Services Routers (ISRs), virtualized store security appliances, routers, switches, and voice and application services into intelligent IT appliances that are centrally managed and monitored.
- *Security services* —Used extensively in the Connected Retail framework. These services are a combination of in-store security services shared across multiple physical devices, central management in the data center, and virtual access to the security control plane from anywhere in the retail network.

- *Identity services* —are used to ensure that access to each application is allowed only for authenticated and authorized management users. A central directory such as LDAP enhances secure identity services.

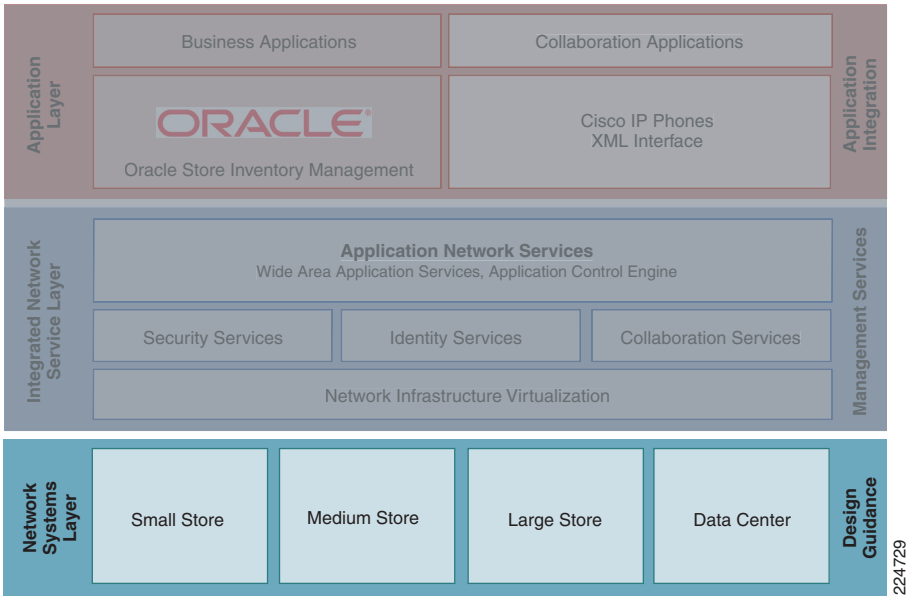
Note For more information about securing Connected Retail architectures, refer to the *PCI Solution for Retail Design and Implementation Guide* at the following URL: http://www.cisco.com/web/strategy/retail/pci_imp.html. This guide describes services that can be used to provide a secure posture for the Cisco Lean Retail Oracle SIM solution.

The Integrated Network Services layer provides services that are distributed across the infrastructure or Network Systems layer.

Network Systems Layer

The Network Systems layer (see Figure 9) is where the infrastructure resides. *Connected Retail* references architectures were used as a contextual backdrop to test the interoperability of the features and functionality of integration between Oracle's SIM application and the Cisco Lean Retail Services. The Lean Retail reference architectures serve as the foundation of the Network Systems Layer. These architectures exhibit best practices for retail networks and provide the robust foundation for higher-level services and applications. Each of these architectures contain additional products and features beyond what is necessary for the Lean Retail Oracle SIM solution (e.g., wireless products, kiosks and application acceleration), but are depicted because they are common in most enterprise networks.

Figure 9 Network Systems Layer



For more information about Connected Retail, see the following URL:

http://www.cisco.com/web/strategy/retail/irn.html.

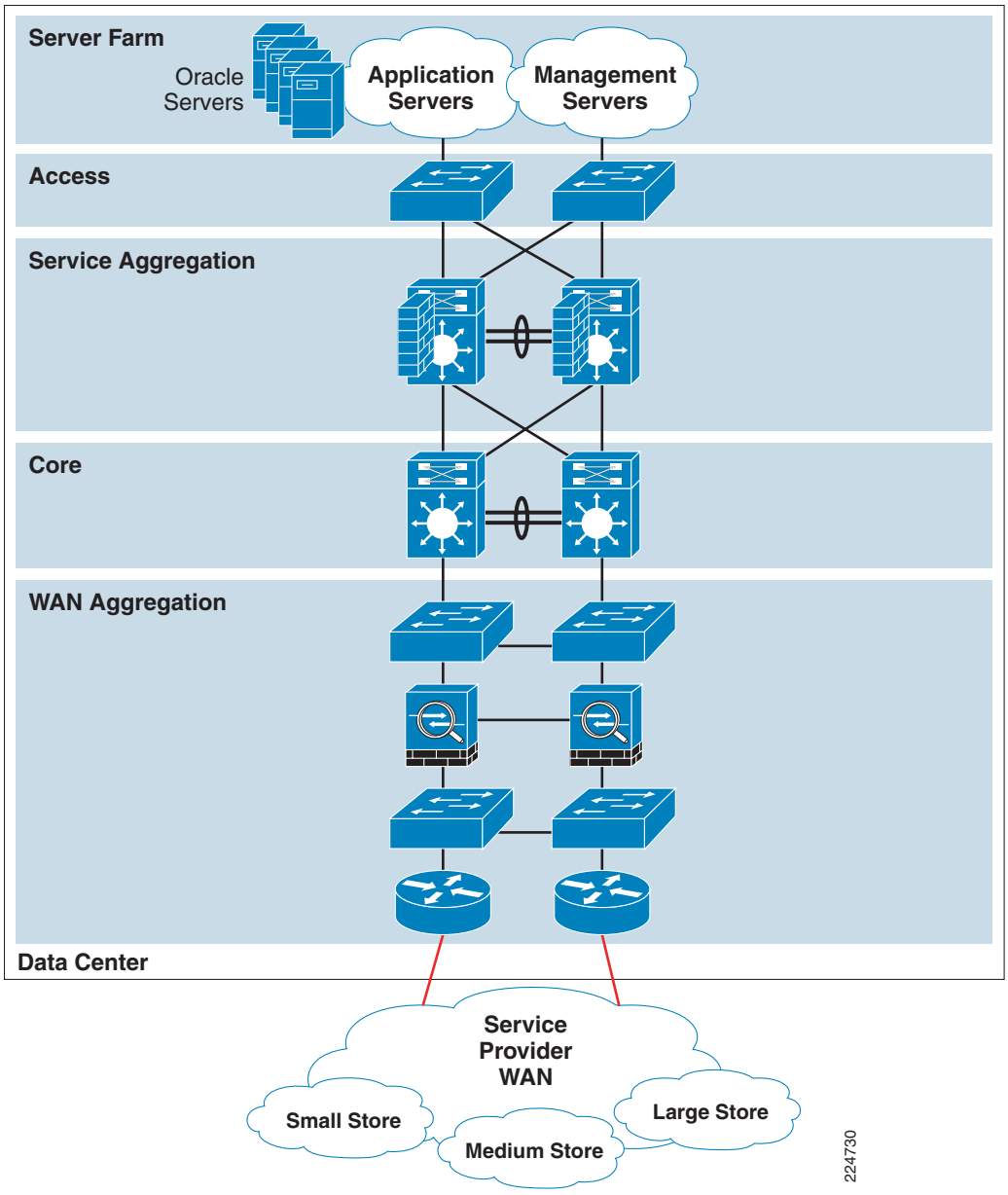
Connected Retail Reference Architecture

The following reference architectures depict Cisco's recommended retail store formats that range from small to large stores as well as the central data center. These architectures depict a platform that is adequately robust to support traditional retail applications such as point of sale, as well as integrated security, voice, video, wireless and data. These reference architectures are built out in Cisco's lab for testing of the Oracle SIM application. For specific design information, see Appendix A—Test Environment Diagrams, page 56.

Data Center

The data center network design is based on a proven *layered* approach, which has been tested and improved over the past several years in some of the largest data center implementations in the world. The layered approach is the basic foundation of the data center design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance. Figure 10 shows the basic layered design.

Figure 10 Data Center Architecture



The layers of the data center design are the *core, aggregation,* and *access* layers. These layers are referred to throughout this guide and are briefly described as follows:

- *Access layer*—Where the servers physically attach to the network. The server components consist of 1RU servers, blade servers with integral switches, blade servers with pass-through cabling, clustered servers, and mainframes with OSA adapters. The access layer network infrastructure consists of modular switches, fixed configuration 1 or 2RU switches, and integral blade server switches. Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.
- *Service Aggregation layer modules*—Provide important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy. Server-to-server multi-tier traffic flows through the aggregation layer and can use services, such as

firewall and server load balancing, to optimize and secure applications. The smaller icons within the aggregation layer switch in Figure 11 represent the integrated service modules. These modules provide services, such as content switching, firewall, SSL offload, intrusion detection, network analysis, and more.

- *Core layer*—Provides the high-speed packet switching backplane for all flows going in and out of the data center. The core layer provides connectivity to multiple aggregation modules and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as OSPF or EIGRP, and load balances traffic between the campus core and aggregation layers using Cisco Express Forwarding-based hashing algorithms.

Note For more information on data center infrastructure design best practices, see the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a008073377d.pdf

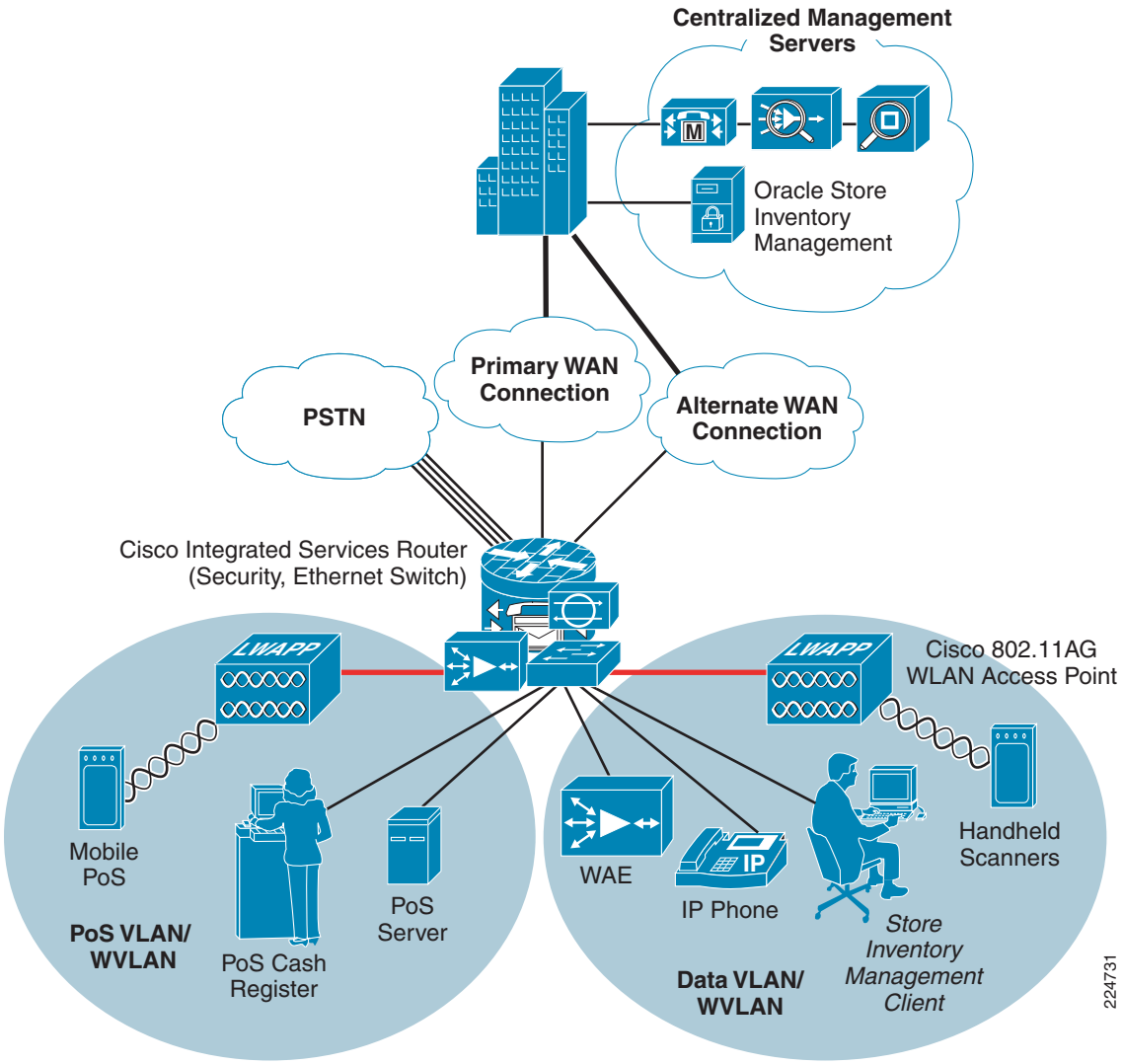
Small Store

The small store reference architecture (Figure 11) is a powerful platform for running an enterprise retail business that requires simplicity and a compact form factor. This combination appeals to many different retail formats that can include the following:

- Mall-based retail stores
- Quick-serve restaurants
- Convenience stores
- Specialty shops
- Discount retailers who prefer network simplicity over other factors

This network architecture is widely used, and consolidates many services into fewer infrastructure components. The small store also supports a variety of retail business application models because an integrated Ethernet switch supports high-speed LAN services.

Figure 11 Small Store Network Design



Primary Requirements

Primary requirements are as follows:

- Store size averages between 2000 to 6000 square feet
- Fewer than 25 devices requiring network connectivity
- Single router, integrated Ethernet switch
- Preference for integrated services within fewer network components because of physical space requirements

Advantages

Advantages are as follows:

- Lower cost per store
- Fewer parts to spare
- Fewer software images to maintain
- Lower equipment maintenance costs

Limitations

Limitations are as follows:

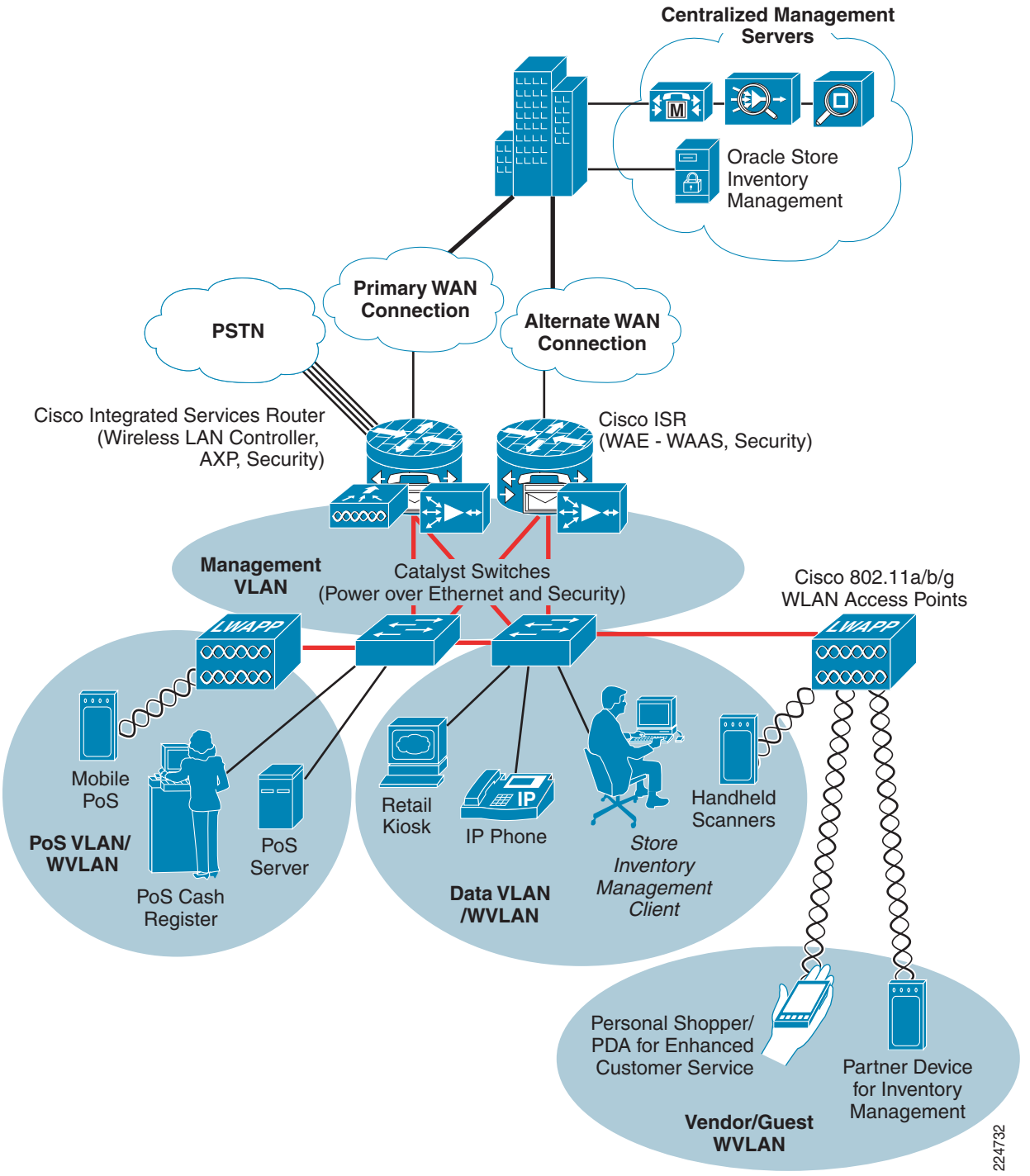
- Decreased levels of network resilience
- Greater potential downtime because of single points of failure

Medium Store

The medium retail store reference architecture (Figure 12) is designed for enterprise retailers who require network resilience and increased levels of application availability over the small store architecture and its simple, single-threaded approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium store supports these requirements. Each of the ISR routers can run Cisco IOS security services and other store communication services simultaneously. Each of the ISR routers is connected to a dedicated WAN connection. Hot-Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small store. The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small store.

Figure 12 Medium Store Network Design



Primary Design Requirements

Primary design requirements are as follows:

- Store size averages between 6,000 to 18,000 square feet
- Physical size of store is smaller than a large store, so a distribution layer of network switches is not required
- Number of devices connecting to the network averages between 25 and 100 devices

Advantages

- Multiple routers for primary and backup network requirements
- Adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, etc)
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

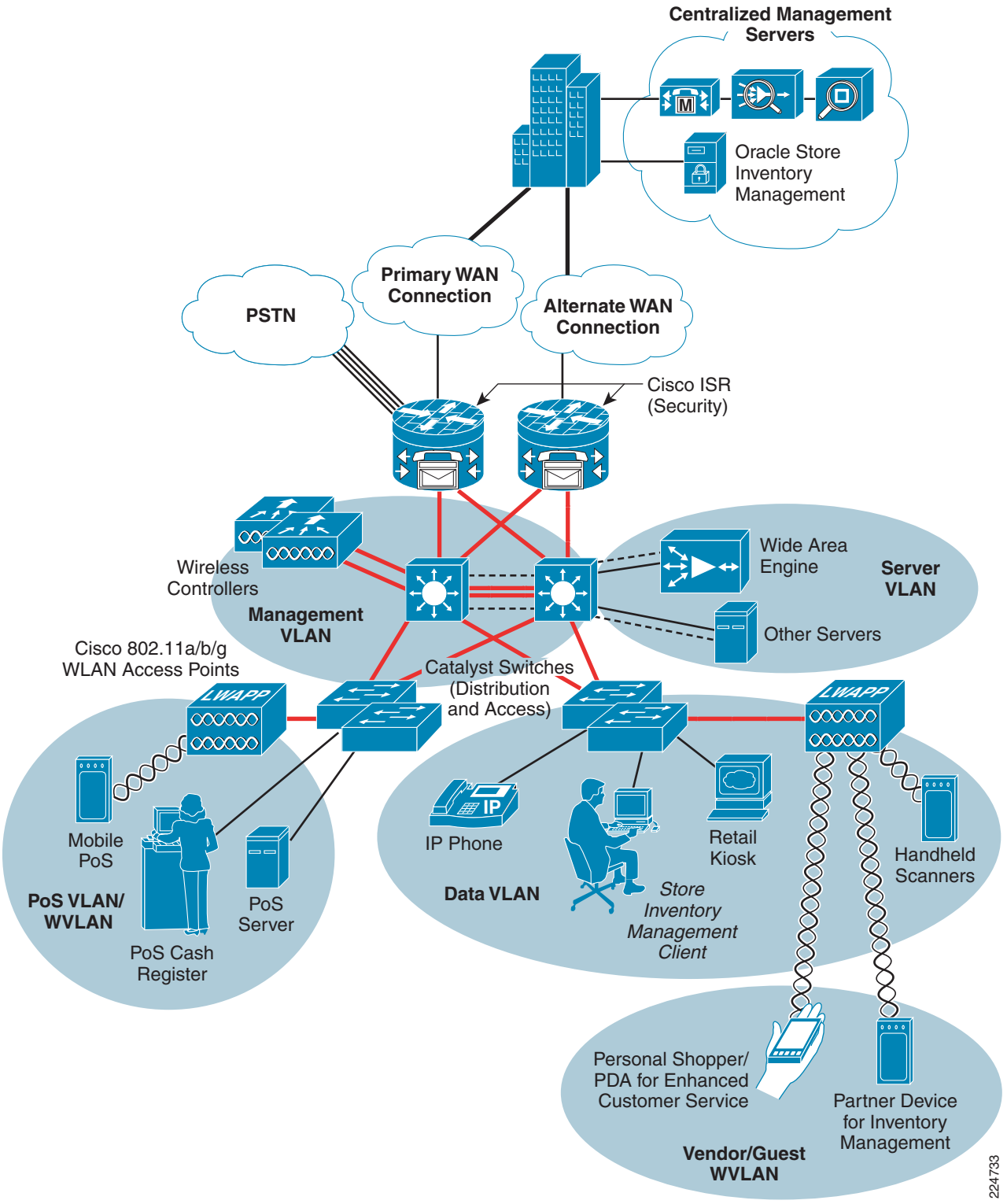
Limitations

The limitation is of this architecture is that there is no distribution layer between core layer (the ISR) and the access layer switches.

Large Store

The large retail store reference architecture (Figure 13) adapts the Cisco campus network architecture recommendations to a large retail store environment. Network traffic can be segmented (logically and physically) to meet business requirements. The distribution layer of the large store architecture improves LAN performance while offering enhanced physical media connections. A larger number of endpoints can be added to the network to meet business requirements. This type of architecture is widely used by large-format retailers globally. Dual routers and distribution layer media flexibility improves network serviceability because the network is highly available and scales to support the large retail store requirements. Routine maintenance and upgrades can be scheduled and performed more frequently, or during normal business hours, through this parallel path design.

Figure 13 Large Store Network Design



Primary Design Requirements

Primary design requirements are as follows:

- Store size averages between 15,000 to 150,000 square feet
- More than 100 devices per store requiring network connectivity
- Multiple routers for primary and backup network requirements
- Preference for a combination of network services distributed within the store to meet resilience and application availability requirements
- Three-tier network architecture within the store; distribution layer switches are used between the central network services core and the access layer connecting to the network endpoints (point-of-sale, wireless APs, servers, etc.)

Advantages

- Highest network resilience based on highly available design
- Port density and fiber density for large retail locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements in large retail stores

Limitations

The limitation of this architecture is the higher associated cost because of network resilience based on highly available design.

Application Networking Services Technology Overview

This section provides an overview of the significant Cisco products and technologies leveraged within the Lean Retail Architecture to enhance Oracle SIM. The following products are addressed:

- Cisco Application Control Engine (ACE)
- Cisco Wide Area Application Services (WAAS)

Although this section highlights features of these Cisco products, refer to Design and Implementation, page 34, for the specific test configurations used for Oracle SIM.

Application Control Engine

The Cisco Application Control Engine Module for Cisco Catalyst 6500 Series Switches is a member of the Cisco family of Data Center 3.0 solutions, and a critical component of Cisco ACE product family. Cisco ACE module represents state of the art in next-generation application switches that helps:

- Maximize application availability
- Scale application performance
- Secure application delivery
- Facilitate data center consolidation and reduce costs through the use of fewer servers, load balancers, and data center firewalls

The Cisco ACE Module achieves these goals through a broad set of intelligent Layer-4 load balancing and Layer-7 content switching technologies integrated with leading acceleration and security capabilities. A key design element of the module is its ability to use virtualized architecture and role-based administration, which enable IT to provision and deliver a broad range of multiple applications from a single module, bringing increased scalability for to the data center.

To maximize application availability, the module uses best-in-class application-switching algorithms and highly available system software and hardware. It provides industry-leading scalability and throughput for managing application traffic, up to 16Gbps in a single module and 64Gbps with four modules in a single Catalyst 6500 switch chassis. This is upgradeable through software licenses or new module additions, thus providing IT with long-term investment protection and scalability.

The Cisco ACE Module greatly improves server efficiency through both highly flexible application traffic management and offloading CPU-intensive tasks such as SSL encryption/decryption processing and TCP session management.

Overview

ACE provides a highly available and scalable data center solution for the Oracle SIM application environment. Currently, the ACE is available as an appliance or integrated service module in the Catalyst 6500 platform. The testing of the SIM application in this solution was restricted to the ACE service module in the Catalyst 6500. 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, etc.
- Centralized role-based management via Application Network Manager (ANM) GUI or CLI
- SSL Offload (up to 15,000 SSL sessions via licensing)
- Support for redundant configurations (intra-chassis, inter-chassis, inter-context)

Additional Integrated Service Options

This document addresses the integration of network services with the Oracle SIM application. 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 store. 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 (appliance only).

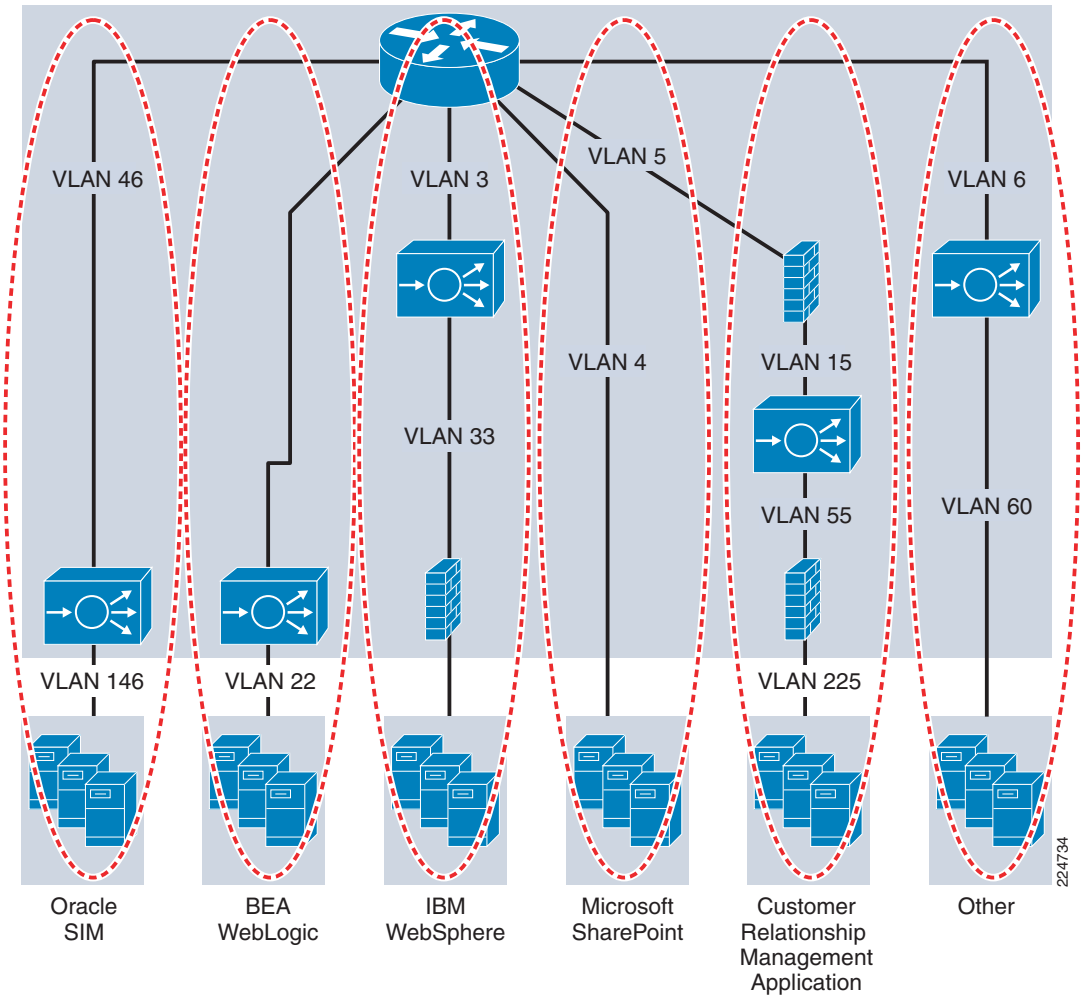
ACE Virtualization

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 applications, such as Oracle SIM, 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 14 shows the use of virtualized network services afforded via the ACE and Cisco Firewall Services Module (FWSM). In Figure 14, a Catalyst 6500, housing a single ACE and FWSM, supports the business processes of five independent business functions. 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 14 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/products/hw/modules/ps2706/products_configuration_guide_book09186a00806882c6.html

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.

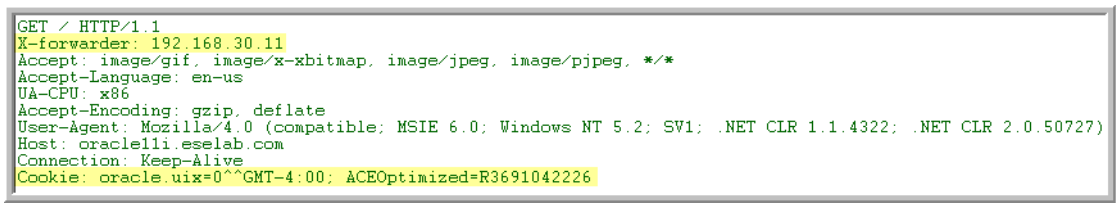
HTTP Header Insertion

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 15 shows the insertion of an HTTP header under the name “X-forwarder”, reflecting the source IP address of the request.

Figure 15 HTTP Header Insertion Example



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 ExampleHeader 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.

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 Wide Area Application Services (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 RPF.

Transparent Interception

Load balancers typically perform a NAT function to conceal the real server IP addresses residing in the retail 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.

Allowed Server Connections

Retail 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.

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.

Wide Area Application Services

Cisco Wide Area Application Services (WAAS) provides appliance/software-based performance optimizations for TCP-based traffic. WAAS is targeted at improving the performance of TCP-based applications across the WAN, while reducing the amount of repetitive data that traverses the WAN. A Wide Area Application Engine running WAAS is required on both sides of a WAN link to perform optimization. Each WAE device forms one or more peer relationships with other WAE devices in the flow path.

To appreciate how WAAS provides WAN and application optimization benefits to the enterprise, consider the basic types of centralized application messages that are transmitted between stores. 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 SIM's client download, 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. For example, Oracle SIM Warehouse Delivery.

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. For more information, refer to the following URL:

http://www.cisco.com/en/US/partner/prod/collateral/contnetw/ps5680/ps6474/product_data_sheet0900aecd80329e39.html

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) employs 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.

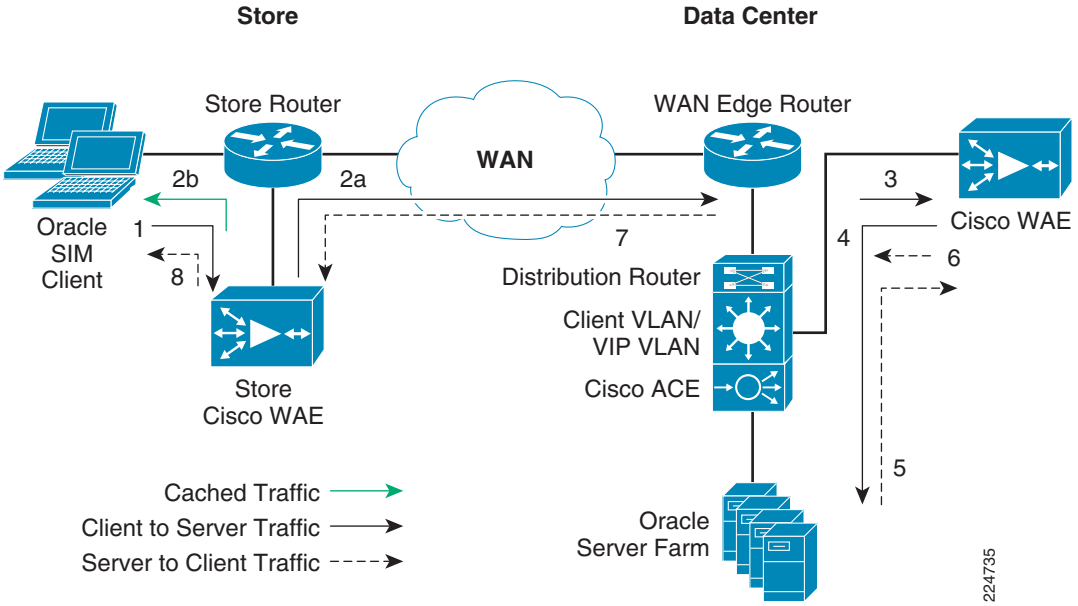
Print Services

WAAS provides native SMB-based Microsoft print servers locally on the WAE device. Along with CIFS optimizations, this allows for store 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 store client to the centralized server(s) across the WAN, then back to the store printer(s), thus transiting the WAN twice for a single job. WAAS eliminates the need for either WAN trip.

Note For more information on these enhanced services, see the *Cisco Wide Area Application Services (WAAS) V4.0 Technical Overview* at the following URL: http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml

Lean Retail Oracle SIM Packet Flow

Figure 16 Oracle SIM Packet Flow



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

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

Step 2 The following steps are for 2a and 2b in Figure 16 above:

a. The store WAE applies a new TCP option (0x21) to the packet if the application is identified for optimization by an application classifier. The store 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 store router and then to the WAN.

b. During the data transfer phase, if the requested data are in its cache, the store WAE returns its cached data to the client. Traffic does not travel through the WAN to the server farm. Hence both response time and WAN link utilization are improved.

Step 3 The packet arrives on the WAN edge router and is forwarded to the distribution router. The distribution router intercepts the packet with WCCP and forwards the packet to the data center WAE.

Step 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 back to the distribution router. The distribution router forwards it to the ACE. The ACE forwards the packet to the Oracle server farm VLAN with TCP option 0x21 removed. The ACE performs load balancing of the session data traffic. Other functions the ACE performs include IP sticky persistence.

The following steps are for reverse traffic flow:

Step 5 The Oracle server 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 distribution router. The distribution 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.

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

Step 7 The packet travels through the WAN and arrives at the store router. The store router intercepts the packet and forwards it to the store WAE. The store 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 store 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 store WAE have determined the application optimizations to apply on this specific TCP flow. During the data transfer phase the store WAE caches the data, if the data is not already in its cache.

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

WAAS Mobile Product Overview

Cisco WAAS Mobile provides significant application acceleration and bandwidth savings to telecommuters, mobile users, and home-office users accessing corporate HTTP applications, e-mail, and file servers. By default, Cisco WAAS Mobile proxies a range of applications including most web browsers, email clients, Windows Explorer for file shares, ftp clients, and thin clients like Citrix and Microsoft Remote Desktop Client (RDC). In addition, any generic application using TCP connections to content servers can be added via its process name. This list of accelerated applications is determined by comparing the name of the process running on the end-user's machine to a preconfigured list of "Accelerated Processes". TCP connections not in this list will be bypassed.

The Cisco WAAS Mobile Persistent Sessions feature maintains acceleration sessions even when web connectivity is lost or when a mobile client switches to a different network such as from Wi-Fi to cellular. When connectivity is restored, the current session is sustained to create a seamless access experience regardless of the changes in the underlying network structure. Downloads and uploads are resumed without loss of data, and no additional log-ins are required.

Persistent Sessions insulates the end-user from problems with RF coverage in wireless networks as well as from problems in poor quality dial-up access. It allows the acceleration system to support advanced wireless network features such as automated Wi-Fi/cellular switchover or hand-offs when roaming through different cellular networks.

The WAAS Mobile product is typically installed in a DMZ and used to support mobile workers, telecommuters, and SOHO workers, but has also been used by retailers internally to accelerate employee access to applications from smaller store footprints that may not justify the cost of an appliance-based solution.

Design and Implementation

Design Goals

The enterprise retail network is a platform constructed to support a extensive range 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. 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 Oracle application objectives: high availability, security, optimization, scalability, and manageability.

The Cisco Lean Retail 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.

Specific solution objectives were:

- Ensure interoperability (functional testing) between Oracle's Store Inventory Management application and Cisco's networking components that comprise the overall Lean Retail architecture—routers, switches, firewalls, load balancer, and application enhancement engines.
- Enhance Oracle SIM performance in several areas— client download, log on, inventory transaction, and log off.
- Enhance the ability for Oracle SIM to scale to many users across many hardware servers.
- Demonstrate bandwidth savings across several different recommended store designs ranging from small to large with respective varying bandwidth wide area networks.

The remainder of this document focuses on each of these objectives and detail specific deployments of an Oracle SIM application using the services of the Cisco Lean Retail data center infrastructure and Connected Retail store designs.

Design Considerations

This solution required several design considerations to achieve the goals list above.

PCI is a major concern for retailers. Several configurations were enabled to support this security standard:

- Disk Encryption of the WAAS devices was enabled to protect cached information PCI 3).
- The WAAS devices were configured to use user- and role-based authentication (PCI 8).
- 15 minute administrative session time out was configured (PCI 8.5.15).
- Banners were used to notify unauthorized access that legal prosecution would result.
- Sys logging was enabled (PCI 10.5.4).
- SNMP event notification was configured (PCI 10).

Security devices (ASAs) implemented in the WAN aggregation layer were used to terminate encryption tunnels and filter traffic for security and compliance concerns such as PCI, HIPAA, etc. These security devices must be configured to inspect WAAS traffic due to the optimization and manipulation performed by the WAAS protocol.

At the store level, routers running firewall feature sets will need to be configured using zone-based firewall methods. Zone-based firewalls possess the capability to inspect WAAS traffic. The use of zone-based firewalls was not tested in this solution validation.

The Cisco WAAS Mobile product tunnels all client traffic through TCP and UDP port 1182 to the WAAS mobile server. Security devices and QoS must account for this traffic as all client traffic will appear to be sourced from the WAAS mobile server. This may affect IP-based security policies for store user traffic.

WAAS Application Profiling

WAAS has default profiles for many known applications and their corresponding TCP ports. Oracle SIM is not currently one of those default profiles. A new profile must be created to optimize Oracle SIM. Creating an application profile for Oracle SIM has overlapping ports with the well known application "Napster" on port 7777. Either the Oracle implementation must be altered from the standard port of 7777 to some other high port, or the default profile of Napster must be modified to remove the TCP port 7777. In this implementation, Napster was modified to remove the port 7777 from its profile. This overlap of port 7777 should also be considered when implementing QoS. Many retailers may force Napster to be blocked or put as low prioritization within their application priority scheme. This would have a negative impact on a default Oracle SIM installation. For more information, see:

http://protocolinfo.org/wiki/Napster

Hardware-based load balancing of Oracle applications is typically used for high availability and scalability. The *Oracle High Availability Guide* identifies several methods, including using DNS, to direct client traffic to an appropriate application server. This DNS method was used in testing to redirect traffic sent to the Oracle SIM application servers to instead use the ACE VIP address created for the Oracle SIM solution.

When using DNS redirection, the Java client application is still tied to the application server host name. When starting a new session, it was noted that the client will be downloaded from each application server that the user is dynamically assigned to for that session, until all application servers in the server load balancing pool have been downloaded and cached in the local PC Java cache. As the client application Java components are all the same on each of the application servers, WAAS is able to supply these files in an accelerated manner from the DRE cache.

Another method to avoid the need to download the Java client for each host server would be to point the **JNDI url** in the **JNLP** file to the load-balancer host name of the VIP address. This method was not tested, as it would require a reinstall of the Oracle SIM application and changing that setting in the **ant.install.properties** file.

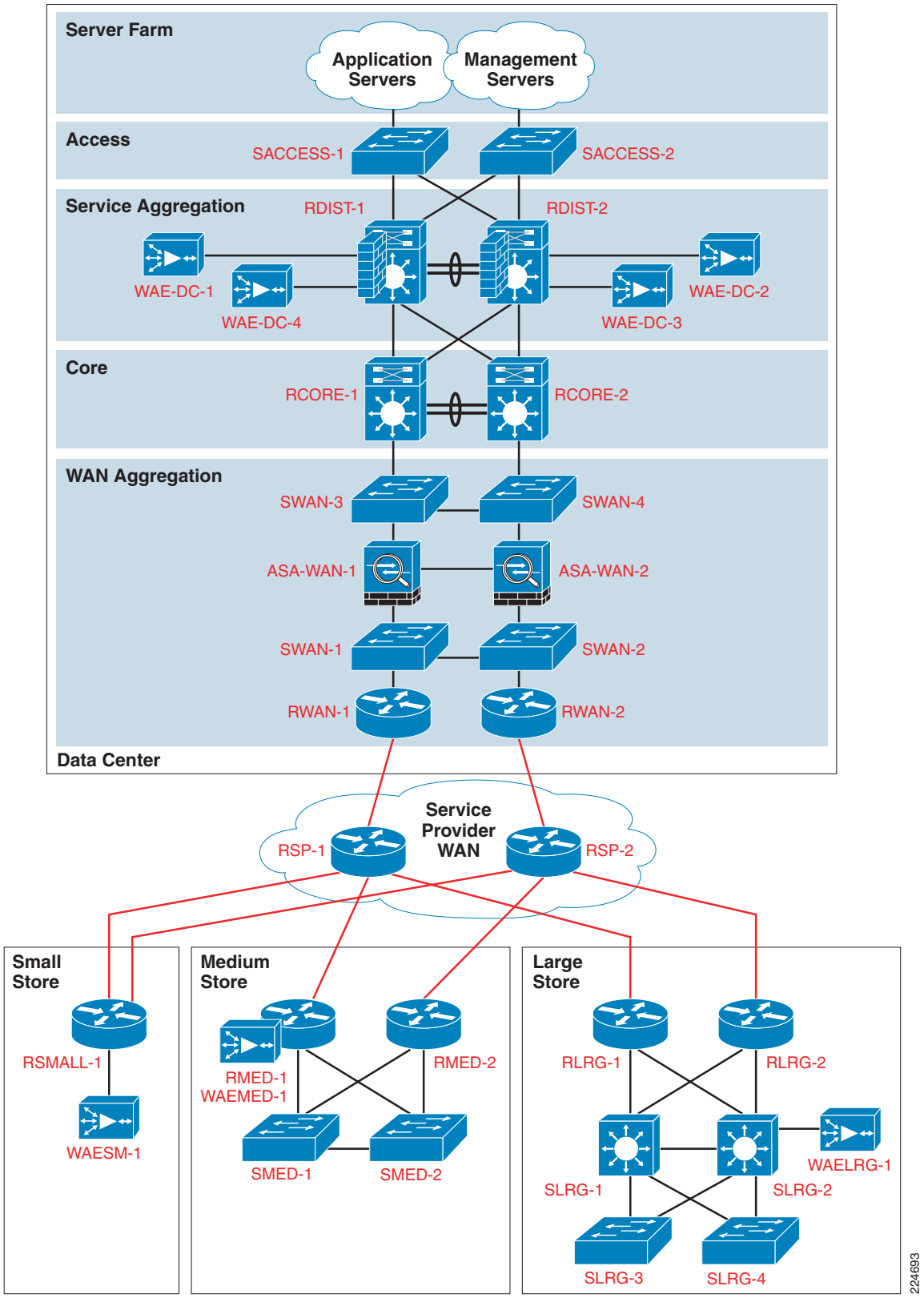
Traffic acceleration occurs when the application data traverses through the WAE. The redirection of traffic can be achieved through several methods. This design used WCCP v2 because it was the most scalable and resilient of the protocol choices available.

Application acceleration requires the implementation of a wide area engine (WAE) at each end of the wide area network (WAN) that connects the store to the data center. The Lean Retail reference design places a firewall behind the WAN aggregation router (see Figure 17) in the data center for filtering and VPN termination. This affects the placement of the WAEs given that they should be placed outside of the encrypted tunnel path to optimize the tunnel traffic. This design positioned the WAE appliances at the service aggregation layer, allowing the optimization of encrypted traffic between stores and the data center.

Design Implementation

This section focuses on the use of the Cisco Wide Area Application Engine (WAE) in conjunction with the Cisco Application Control Engine (ACE) in the retail enterprise network. These designs specifically address a multi-tier deployment of the Oracle SIM application in the Cisco data center infrastructure architecture. The designs provide centralized load balancing, security, and optimization services for the Oracle application.

Figure 17 Lean Network Architecture



Oracle Store Inventory Management

The Oracle SIM application was installed on two separate Oracle application servers which enabled independent testing of Cisco's hardware-based ACE load balancer. Each application server and the Oracle RDBMS database server were built ontop of Oracle's Enterprise Linux operating system (OEL). Oracle SIM and OEL were obtained from Oracle's E-Delivery website, and also include all available documentation: http://www.oracle.com/technology/software/index.html

The Oracle ORDBMS database was installed using default values as specified in the implementation guide. The creation of the SIM database tables were modified such that their maximum size was set to **UNLIMITED** to accommodate the import of the standard reference database content used for application testing.

```
CREATE TABLESPACE RETEK_INDEX DATAFILE
'/opt/oracle/oradata/$ORACLE_SID/retek_index01.dbf' SIZE 500M AUTOEXTEND ON NEXT 100M
MAXSIZE UNLIMITED
EXTENT MANAGEMENT LOCAL
SEGMENT SPACE MANAGEMENT AUTO
;
```

The Oracle Application servers were built using the basic installation type with Integrated Web Server, J2EE Server, and Process Management. These application servers were built individually and not clustered together as this implementation was to use a hardware load balancer in place of clustering, to provide high availability and per-client session load balancing. High availability was achieved using an active-active topology with Oracle HTTP Server and OC4J in the same Oracle home.

Load Balancing

Active-active topologies use a load balancer to direct requests to one of the Oracle Application Server instances in the topology. In other words, the Oracle Application Server instances are fronted by the load balancer. You configure the load balancer with virtual server names for HTTP and HTTPS traffic. Clients use the virtual server names in their requests. The load balancer directs requests to an available Oracle Application Server instance where the Oracle SIM client is the downloaded from. The architecture SIM currently uses allows the JNLP request to be load balanced, but then once that file is retrieved from a server, all communication from the client to the server is directly to the application server the JNLP was downloaded from. Refer to the *Oracle Application Server High Availability Guide* at the following URL for additional information:

http://www.oracle.com/technology/products/ias/hi_av/904ha.pdf

This implementation also tested the ability of Cisco ACE to load balance returning clients by session so that they were no longer tied to the JNLP server that the client is downloaded from. These tests were successful and significantly improve the availability on SIM during server maintenance and unexpected failure of a server.

The Oracle SIM application was installed on each of the application servers following the steps specified in the installation guide. SIM needed to be installed as standalone oc4j implementations instead of clustered instances. This was achieved by modifying the **ant.install.properties** file and changing the **deployer uri** as follows:

```
input.deployer.uri = deployer:oc4j:opmn://OracleSIM01.cisco-irn.com:6003/sim-oc4j-instance
```

For this deployment of Oracle SIM, authentication for users of the application used database authentication instead of the more common LDAP authentication which is configured during the default installation. Changing the method of authentication was achieved as follows:

```
Modify the following file:
            <SIM_INSTANCE>/sim-home/files/prod/config/dao.cfg
```

```
            Change the following line:
EMPLOYEE_DAO=oracle.retail.sim.shared.dataaccess.sim.ldap.dao.EmployeeLdapDAO
            To the following:
EMPLOYEE_DAO=oracle.retail.sim.shared.dataaccess.artsoracle.dao.EmployeeOracleDao

            And change the following line:
STORE_AUTHORIZATION_INFO_DAO=oracle.retail.sim.shared.dataaccess.sim.ldap.dao.StoreAuthori
zationInfoRSSLdapDao
            To this:
STORE_AUTHORIZATION_INFO_DAO=oracle.retail.sim.shared.dataaccess.artsoracle.dao.StoreAutho
rizationInfoOracleDao
```

After completion of these edits, the SIM oc4j instance was restarted.

This version of Oracle SIM did not include a configurable option in the management interface for enabling and disabling compression between the SIM client and the SIM server. This compression is built-in and normally enabled at all times. The testing methodology included tests that needed to be performed with compression set to OFF, so a script was developed to modify several class files enabling the capability of turning compression ON and OFF as needed.

The client PC's tested used Internet Explorer 6 SP1 and included Java JRE 6.0. From each client PC, the following URL was opened in the Internet Explorer browser to launch the SIM client: http://oraclesim01.cisco-irn.com:7777/sim-client/launch?template=sim_jnlp_template.vm.

Before SIM is opened, J2SE Runtime Environment 5.0 Update 15 is automatically downloaded from the Oracle Application server and installed on the client. After the client is downloaded, it is cached in the Java Web Start cache, which is different than IE's temporary space. Thereafter, it is only downloaded if a patch is applied to the client code on the server, and only changed resources are downloaded. Patches are typically sent out every few months. If the Java Web Start cache on the client PC is manually cleared, the full client must be downloaded again. For testing, the Java cache was cleared to initiate new client downloads by deleting the entire folder: "**C:\Documents and Settings\Administrator\Application Data\Sun\Java\Deployment\cache\6.0**"

As the SIM client is stored in the individual user's Java cache profile, each new user that logs in to the client PC will need to download or update the client before use.

ACE

The ACE module is a load balancer that is capable of creating virtual contexts within the confines of the single module. From the Admin context, an Oracle context is created. This allows the administrators of the Oracle SIM application to have a virtual load balancer created that is used specifically for the administration and performance enhancement of Oracle SIM.

The ACE modules were implemented in the service aggregation layer of the data center (RDIST-1 and RDIST-2). This is consistent with the underlying philosophy of the *Data Center C 2.5 Design Guide* that places services like load balancing in an aggregated area between the access and core layers.

Cisco ACE was installed using *Application Control Engine Module Getting Started Guide*, which can be found at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/quick/guide/GSGd.html

The load balancer was configured to use "round robin" method for distributing load. Predictor is round robin by default and does not show up in the running configuration under the serverfarm host section.

```
!
serverfarm host ORACLE
  probe PING
  probe SIM
```

```
  rserver oracle1
    inservice
  rserver oracle2
    inservice
!
```

Several probes were used for server farm health monitoring. Ping was used to verify that the application server was functional. An HTTP probe was used to verify that the Oracle SIM application was functioning.

Configuration within the Oracle Context of custom HTTP probe:

```
   probe http SIM
        port 7777
     interval 5
     faildetect 2
     request method get url /sim-ws/simWebService
     expect status 200 200
```

The Oracle application requires that the client maintains its session with the same application server within the server farm. The ACE load balancer is configured to "stick" the client to the application server for the entire session of that user until the application is closed. To enable sticky functionality, a resource class was defined in the admin context. The source IP sticky functionality for all IP addresses was configured and assigned in the Oracle context.

Configuration and assignment of resource in Admin context:

```
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

context oracle
  description Oracle SIM
  allocate-interface vlan 46
  allocate-interface vlan 146
  member Gold
```

Configuration and assignment of source IP sticky in Oracle context:

```
sticky ip-netmask 255.255.255.255 address source src-ip-sticky
  timeout 10
  serverfarm ORACLE

policy-map type loadbalance first-match VIP-POLICY-11
  class class-default
    sticky-serverfarm src-ip-sticky
policy-map multi-match LB-VIP
  class VIP-HTTP-11
    loadbalance vip inservice
    loadbalance policy VIP-POLICY-11
    loadbalance vip icmp-reply
```

The Oracle SIM client periodically sends keepalive packets to the Oracle SIM server while logged in and the client is open and running. These keepalives are sent every 90 seconds. This continuous communication helps to maintain state and synchronization through the load balancer which maintains client source IP sticky connectivity through 10 minutes of inactivity as specified by the **timeout** command.

WAAS

This design required a WAE for each of these functions: Central Manager, headend, in the data center, and per store. The Central Manager must have a minimum configuration of:

- Device mode as a Central Manager
- IP address of LAN interface for connectivity

Headend and Store WAEs

In order to use the Central Manager for management and scaled configuration, initial configuration must be performed via the CLI interface of the headend WAE and the store side WAEs. These settings are as follows:

- The device mode as an application accelerator
- IP address of the LAN interface for connectivity
- The IP address of the Central Manager

These initial configurations allow the use of the Central Manager for all subsequent configurations of the WAAS devices. Through the use of the device group capability, the common settings for all the devices were assigned (e.g., NTP, Disk Encryption, authentication, and SNMP).

Redirection of Oracle SIM Traffic To WAEs

WAEs

The WAEs were configured to retrieve WCCP redirection of the Oracle SIM traffic from the Cisco routers by using the Central Manager.

```
!
Specifies the data center router (RDIST-1) as source of WCCP traffic
wccp router-list 1 192.168.62.161
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
```

Routers

The data center routers at the service aggregation layer (RDIST1 and RDIST2) and the store routers were configured to redirect Oracle SIM traffic to the local WAE using WCCP v2. The following configurations demonstrate how the data center routers were configured.

Global Configuration:

```
!Enable WCCP services- WCCP version 2 is  default
ip wccp 61
ip wccp 62
ip wccp version 2
!
```

Interface Configuration:

```
interface Loopback62
ip address 192.168.62.161 255.255.255.255
!
!WCCP was implemented on the interfaces that Oracle SIM traffic flows through.
interface Vlan102
 description Uplink to RCORE-2
```

```
 ip address 192.168.10.18 255.255.255.252
 ip wccp 61 redirect in
!
!
interface Vlan46
 description ORACLE SIM NETWORK
 ip address 192.168.46.3 255.255.255.0
  ip wccp 62 redirect in
!
```

In the medium store, a network module was used (NME-WAE). The IP address of the WAE is assigned via the router NME (Integrated Service Engine) interface as follows:

```
!
interface Integrated-Service-Engine1/0
 ip address 10.10.46.41 255.255.255.252
 service-module ip address 10.10.46.42 255.255.255.252
 service-module ip default-gateway 10.10.46.41
 no keepalive
!
```

For more information regarding WCCP, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf018.html

WAAS Oracle Application Profile

WAAS devices come with a large amount of application profiles built into the application. The Oracle SIM application is not a default application that is characterized within this portfolio. There are two ramifications of this that must be configured within the WAEs:

1. Creation of the Oracle SIM profile within Cisco WAAS
2. Resolving the overlap of ports used by Oracle WAAS and the default profile used by the application Napster.

   Creation of Oracle SIM profile was achieved by creating an application profile, an application classifier and an application action. The following screenshots depict how to create an Oracle SIM application profile with the Central Manager that is pushed out to the headend and store WAEs (see Figure 18, Figure 19, and Figure 20).

Figure 18 New Application Policy

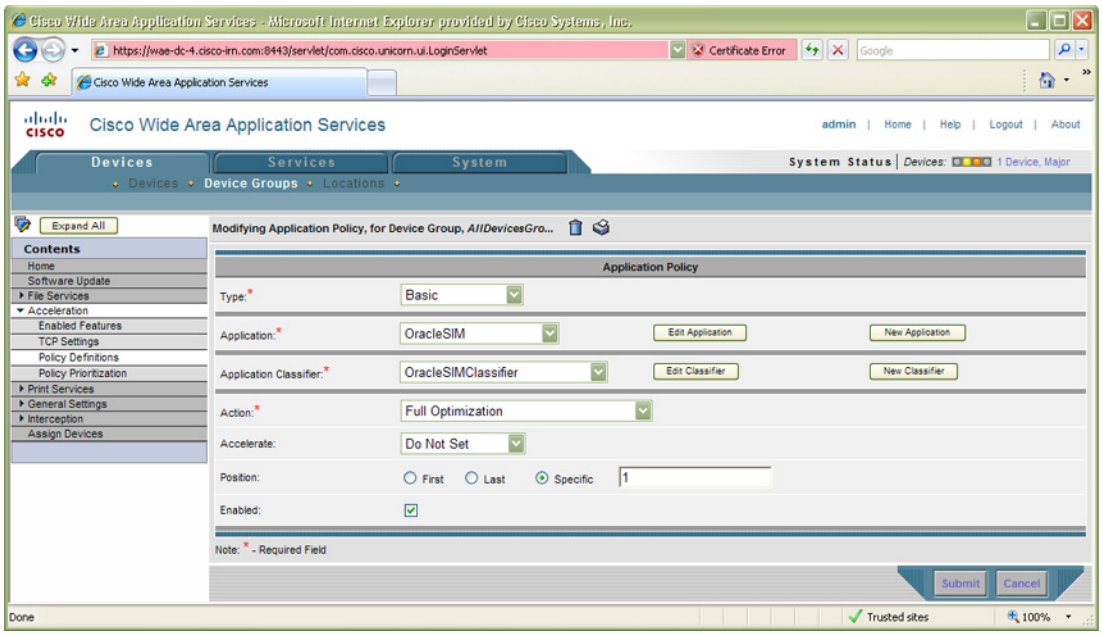


Figure 19 New Classifier for Oracle SIM TCP Ports

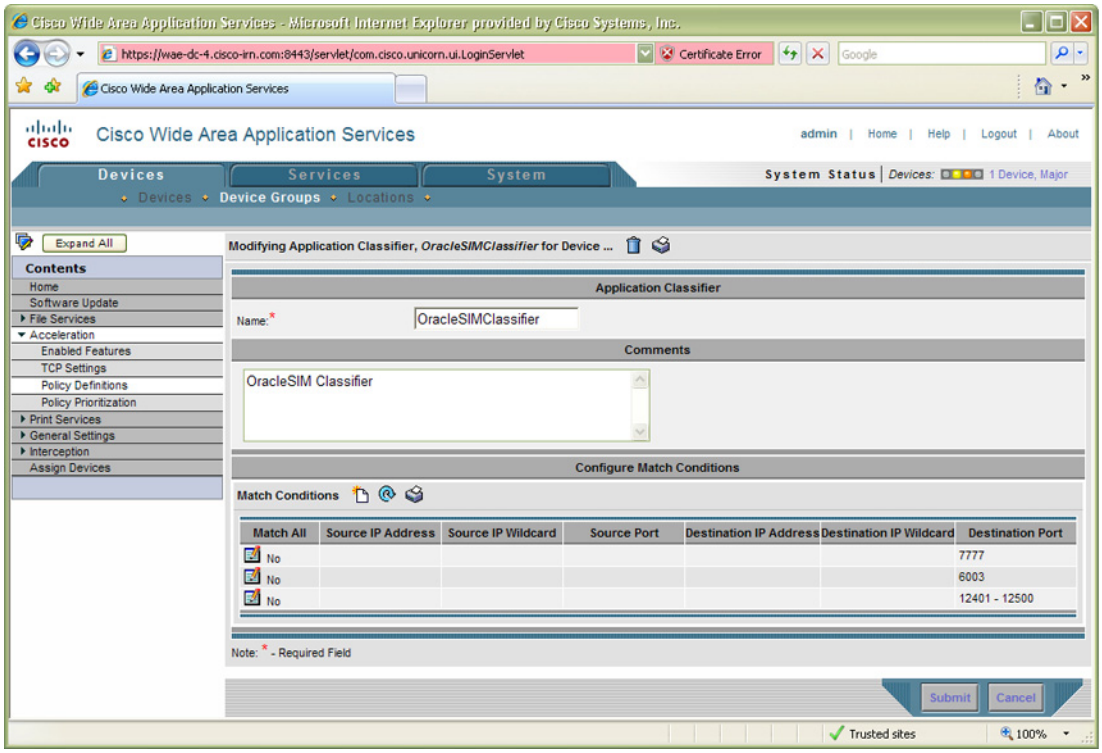
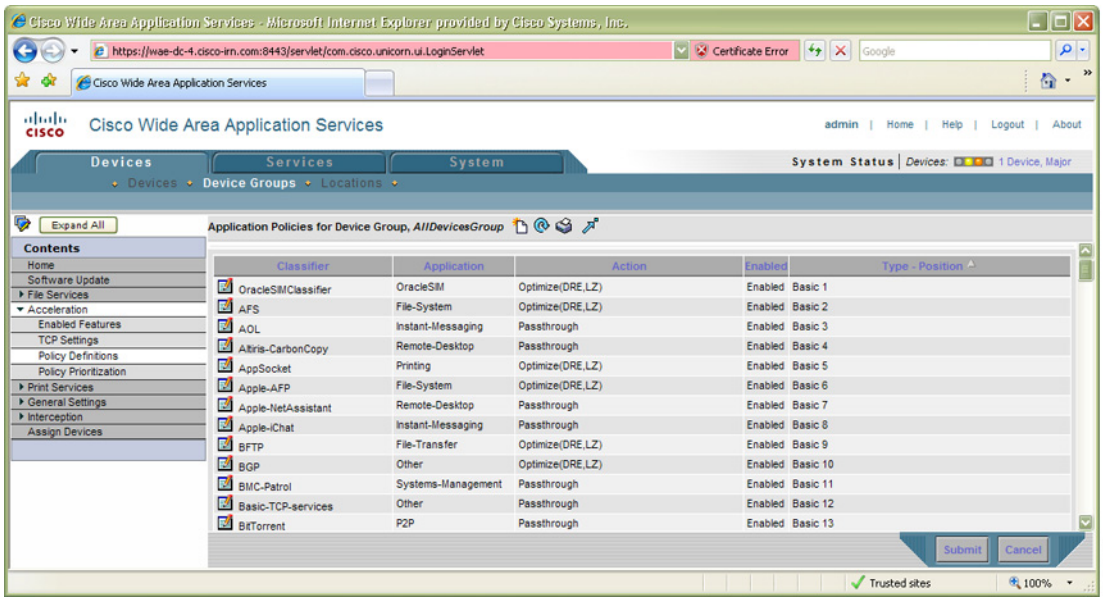


Figure 20 Application Oracle SIM Listed in the Application Policy Group



After this profile has been pushed to the enterprise WAEs, the following configurations are found within the WAEs:

```
!Oracle SIM application profile now appears at the end of the list of default application
policies.
policy-engine application
   name Authentication
… default policies excerpted for brevity
   name OracleSIM
!

!Oracle SIM classifier now appears using the standard Oracle SIM TCP ports
classifier OracleSIMClassifier
      match dst port range 12401 12500
      match dst port eq 7777
      match dst port eq 6003

! Oracle SIM now appears and is configured for full optimization
  map basic
      name OracleSIM classifier OracleSIMClassifier action optimize full
```

Oracle SIM was configured for full optimization, which includes TFO, DRE, and LZ compression.

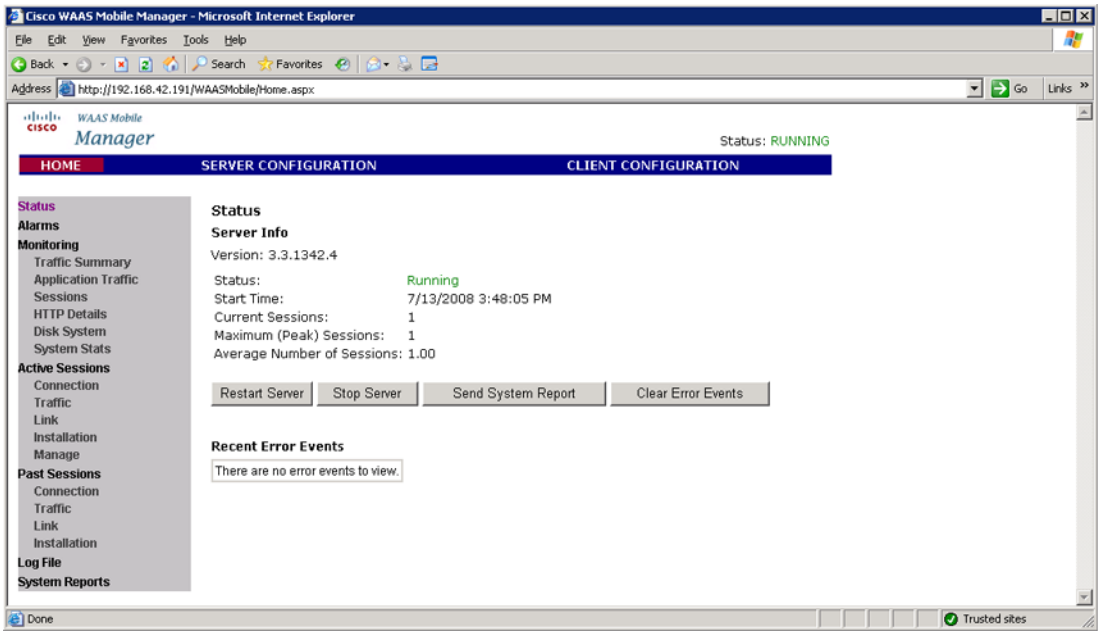
Napster

Under the Napster application profile, the Napster classifier was modified to remove TCP port 7777. This resolves the conflict that was introduced when creating the Oracle Store Inventory Management classifier.

WAAS Mobile Design Installation

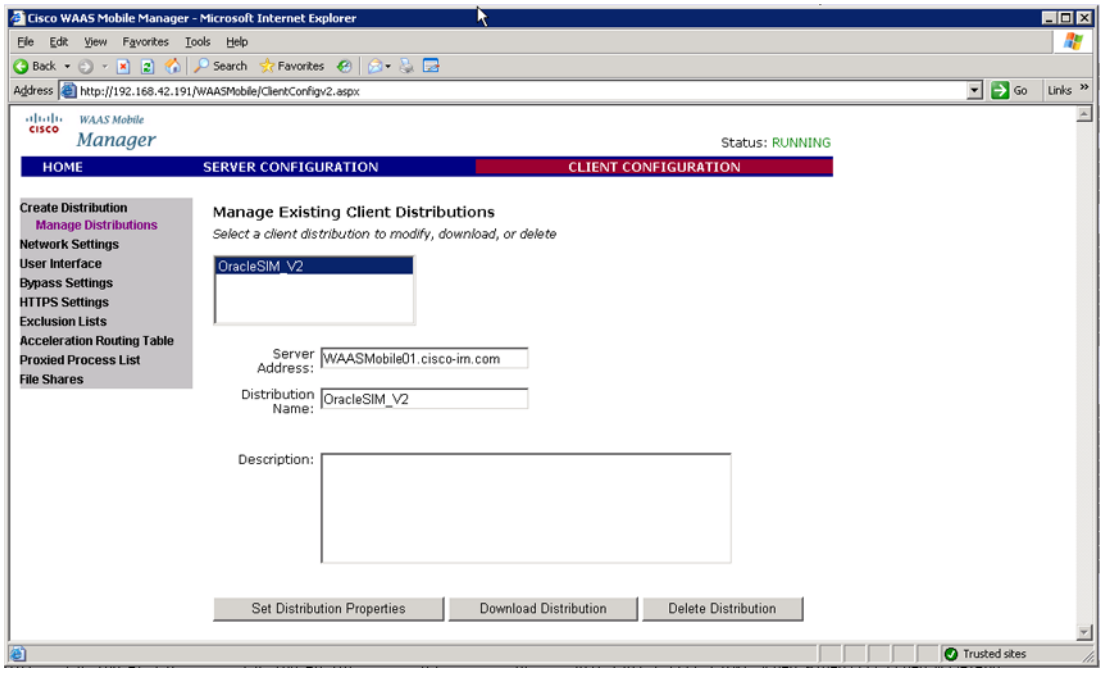
The Cisco WAAS Mobile server was installed on a Windows 2003 server with Service Pack 1 installed, IIS services and Windows .NET v2.0 as specified in the installation guide (see Figure 21).

Figure 21 WAAS Mobile SIM Distribution



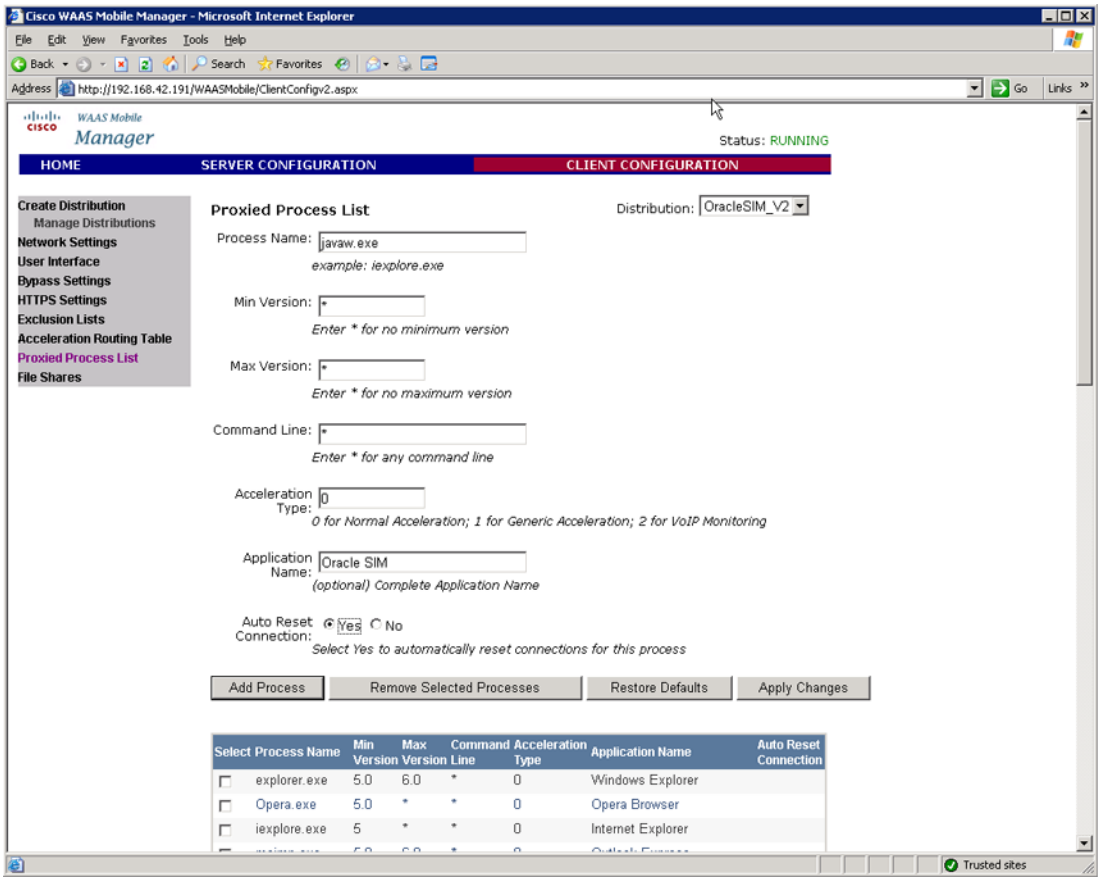
After completing installation and licensing, a new **Client Distribution** was created. This new client distribution was labeled as **OracleSIM_V2** (see Figure 22).

Figure 22 WAAS Mobile SIM Distribution



To enable acceleration and caching for the Oracle SIM client application, a new process needed to be added to the Proxied Process List. The Oracle SIM client is a Java application, so the process name that is used is **javaw.exe**. This new process was defined and the auto reset connection option was set to **Yes** as shown in Figure 23.

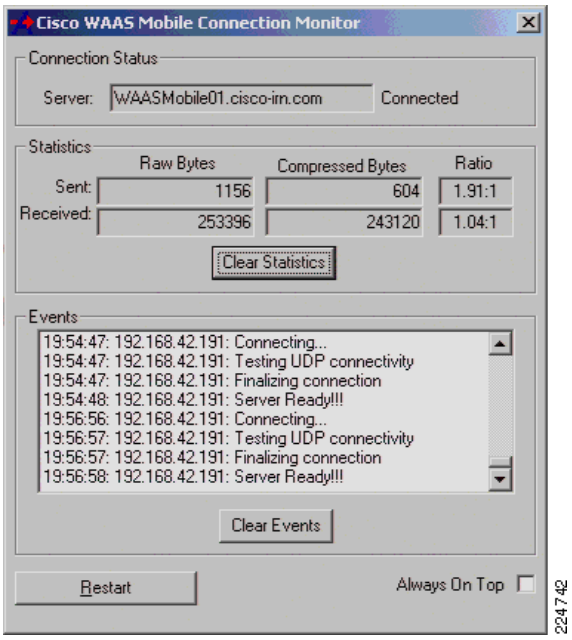
Figure 23 WAAS Mobile SIM Distribution



After the client distribution options have been assigned, it was then downloaded onto a client PC in the small store and installed. Once installed and enabled, all traffic from the defined processes is sent to the WAAS Mobile server using UDP port 1182. The mobile server then fully proxies the connection to the Oracle SIM application servers on behalf of the client.

The WAAS Mobile client application (see Figure 24) provides basic statistical information including; RAW Bytes and Compressed Bytes sent and received, and Events.

Figure 24 WAAS Mobile SIM Client



Cisco WAAS Mobile instructions for use and installation of this product are detailed in the following documents: *Cisco WAAS Mobile Integration Guide*, *Cisco WAAS Mobile System Administration Guide*, and *Cisco WAAS Mobile Client Software User Guide*. More information on WAAS Mobile can be found at the following URL: http://www.cisco.com/en/US/products/ps9523/index.html.

Connected Retail Store Designs

Several different store footprints were tested in this solution. Each store connected back to the central data center.

Table 1 Connected Retail Store Design Data

Location	WAAS Device	WAN Bandwidth	WAN Delay
Small	512 Appliance	128Kbps	100 ms
Small	WAAS Mobile Client	128Kbps	100 ms
Medium	NME-WAE-502	512Kbps	100 ms
Large	512 Appliance	1544Kbps	100 ms

Lean Retail Oracle Store Inventory Solution Environment

Table 2 details the application environment leveraged during testing, identifying the hardware, and software components of the test bed.

Table 2 Solution Components

Solution Component	Hardware Model	Software Version
Oracle Application Server	Cisco MCS 7845	10.1.3.3
Oracle SIM	Cisco MCS 7845	12.0.2
Oracle Database	Cisco MCS 7845	10.2
Oracle Enterprise Linux	Cisco MCS 7845	Release 4, Update 6
Load balancer	ACE20-MOD-K9	3.0(0)A1(6.3a)
Wide Area Application Service	WAE-7341	4.0.19 B14
WAE Appliance	WAE-512	4.0.19 B14
Router Network Module	NME-WAE-502	4.0.19 B14
WAE Appliance (Manager)	WAE-612	4.0.19 B14
WAAS Mobile	Cisco MCS 7845	3.3.1342.4

Testing

The Oracle SIM application was tested using a standard script which Oracle uses in QA testing of the product. Testing included a subset of the script, and tests were performed across each architecture in as consistent a manner as possible.

These test points describe typical Oracle SIM usage in a production environment:

- Download of the Oracle SIM Client—Typically the Oracle SIM client is downloaded once initially (a full client download). Thereafter it is only downloaded if a patch is applied to the client code on the server, and only changed resources are downloaded. If the Java Web Start cache on the client PC is cleared, the full client must be downloaded again. A different user performing a unique Windows logon into the same PC will have there own individual Java Web Start cache, and would require a full download as well, even if they use the same Oracle SIM client logon.
- Logging into the SIM application—Client login is performed by supplying the users employee ID and assigned password.
- Performing Warehouse Delivery Tasks—Warehouse delivery testing included four scenarios of receiving 500, 1000, 1500, and 10,000 items. All scenarios were executed in each store topology, though typically only very large stores would receive 10,000 item orders.
- Logging out of the SIM Application—Logout included exiting from client and closing it completely.

Figure 25 through Figure 28 show each of the application client screens.

Figure 25 SIM Client Download

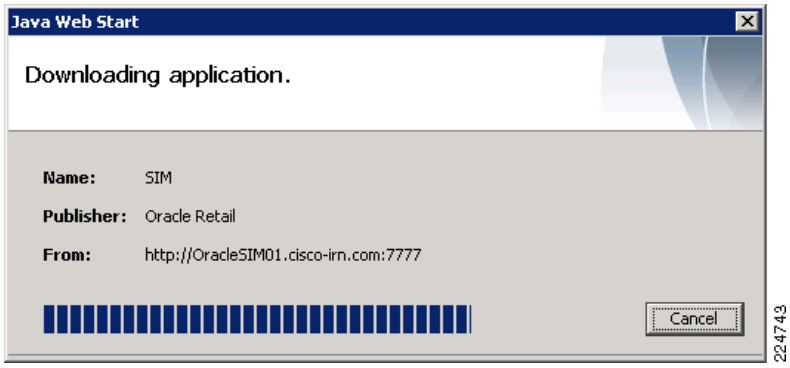
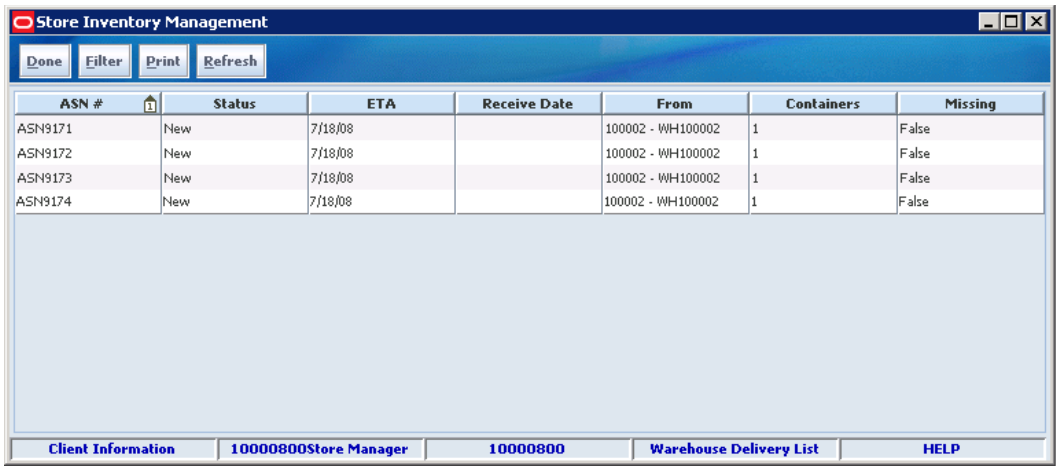


Figure 26 SIM Client Login

Figure 27 SIM Client Menu

Figure 28 SIM Client Warehouse Delivery List



Testing was performed with a combination of Cisco WAAS ON and OFF, with Oracle Compression ON and OFF, and with Cisco ACE enabled and performing load balancing for sessions. Only a small amount of additional traffic was running in the background on the network such as SNMP and Syslog events. All data captured was restricted to the Oracle SIM traffic flow.

Detailed testing results are available in Appendix B—Testing Results DATA, page 60.

Each of the following figures represents the testing results data for the small, medium, and large stores. Each data point represents a complete store user transaction which includes client startup, client login, perform a warehouse delivery of *X* number of skews, logout and close the Oracle SIM application.

Figure 29 and Figure 30 show the results obtained in the small store. Figure 29 depicts the transaction times in seconds and Figure 30 depicts the transaction data in bytes.

Figure 29 Small Store Transaction Time—128kbps

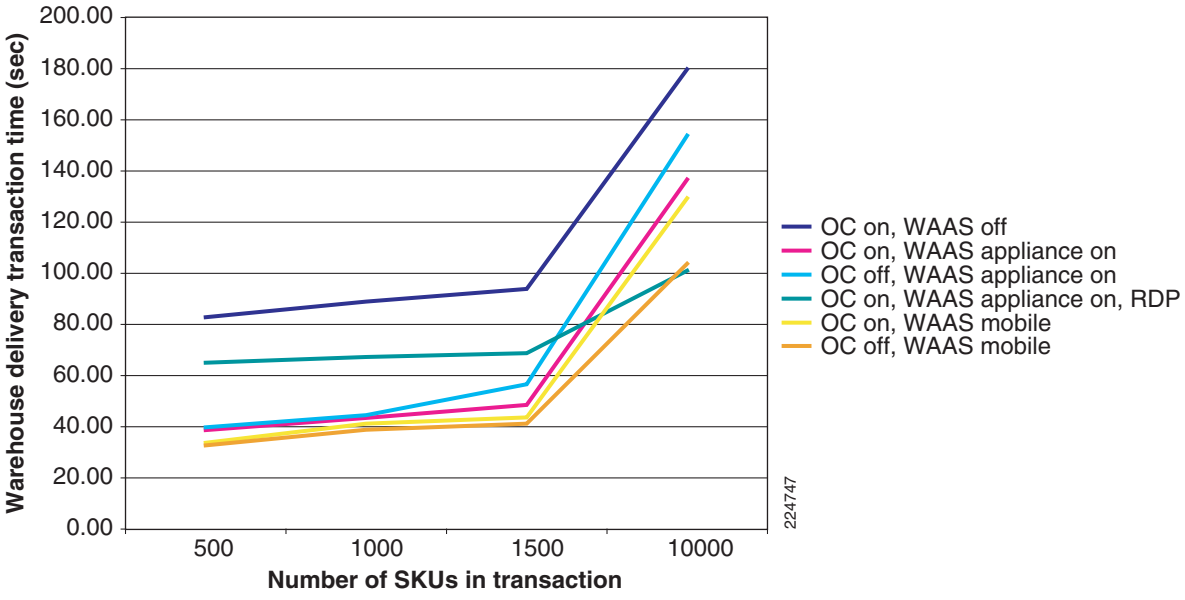


Figure 30 Small Store Transaction Bytes —128kbps

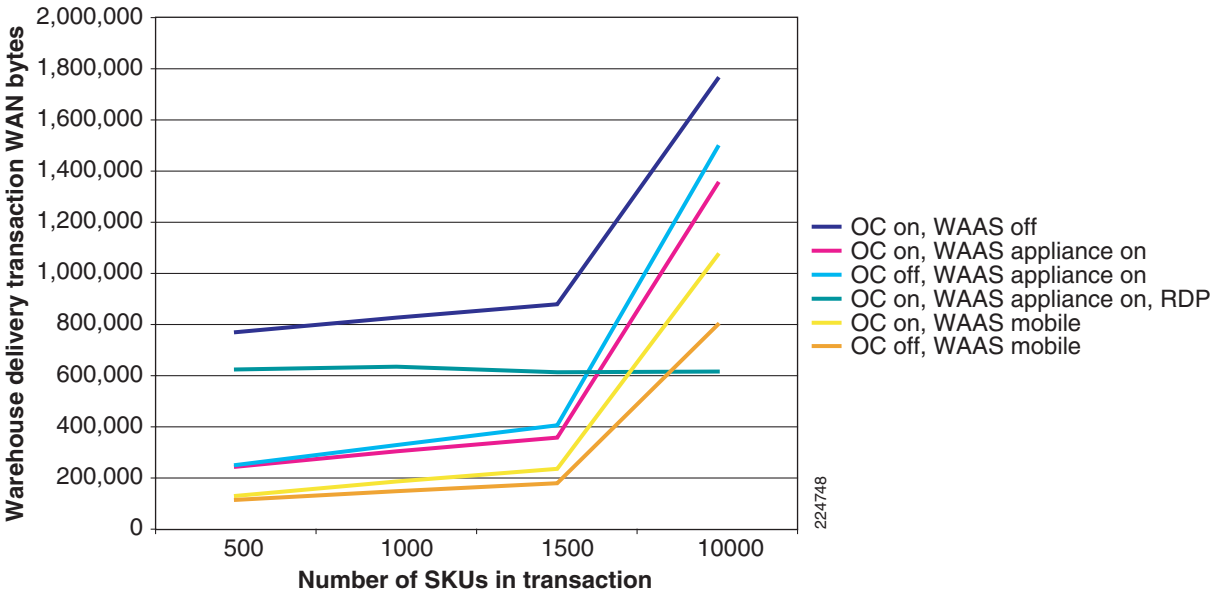


Figure 31 and Figure 32 show the results obtained in the medium store. Figure 31 depicts the transaction times in seconds and Figure 32 depicts the transaction data in bytes.

Figure 31 Medium Store Transaction Time—512Kbps

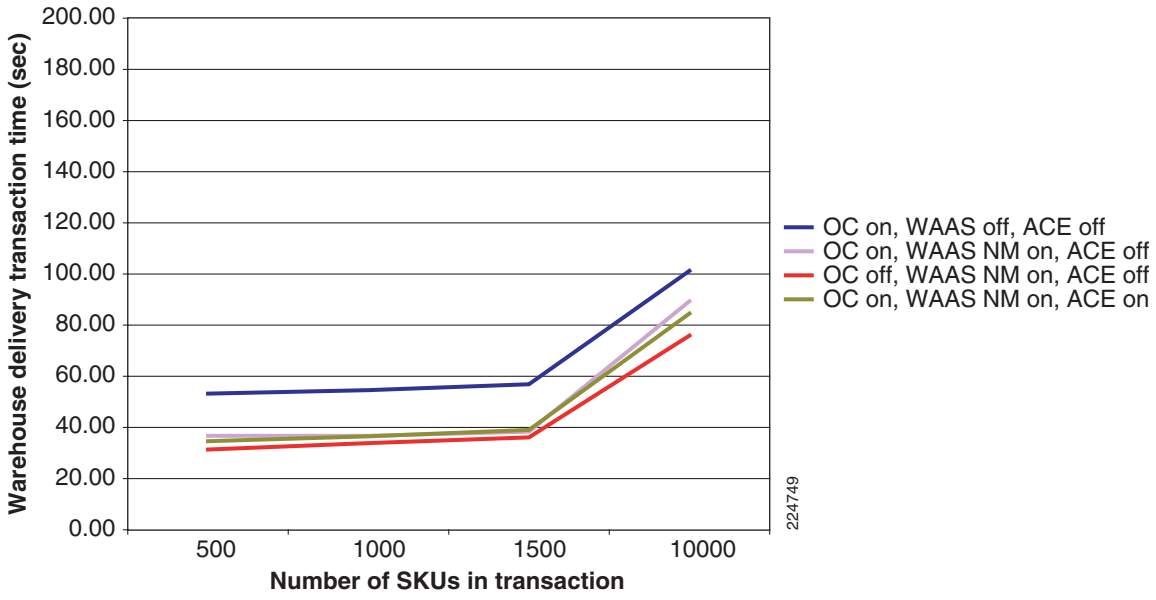


Figure 32 Medium Store Transaction Bytes—512Kbps

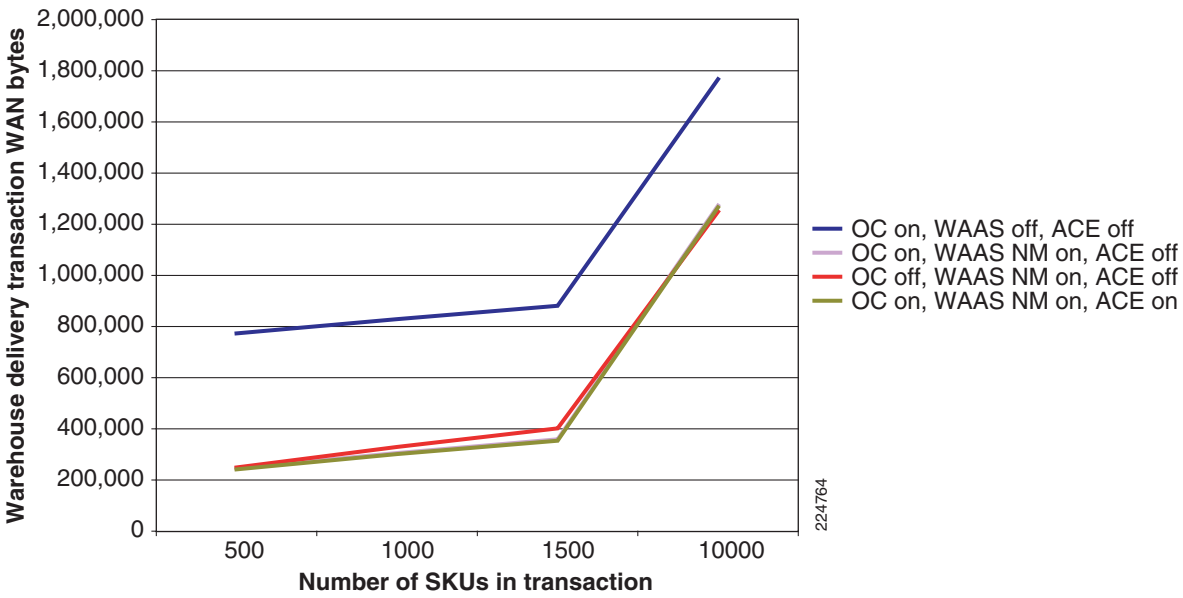


Figure 33 and Figure 34 show the results obtained in the large store. Figure 33 depicts the transaction times in seconds and Figure 34 depicts the transaction data in bytes.

Figure 33 Large Store Transaction Time—1544Kbps

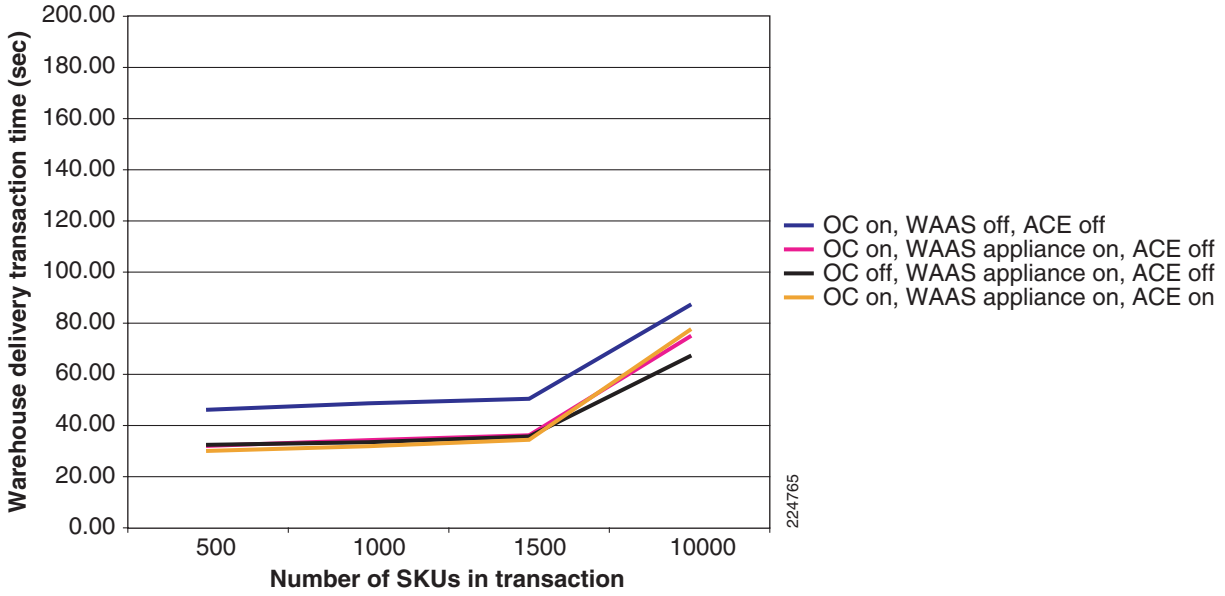
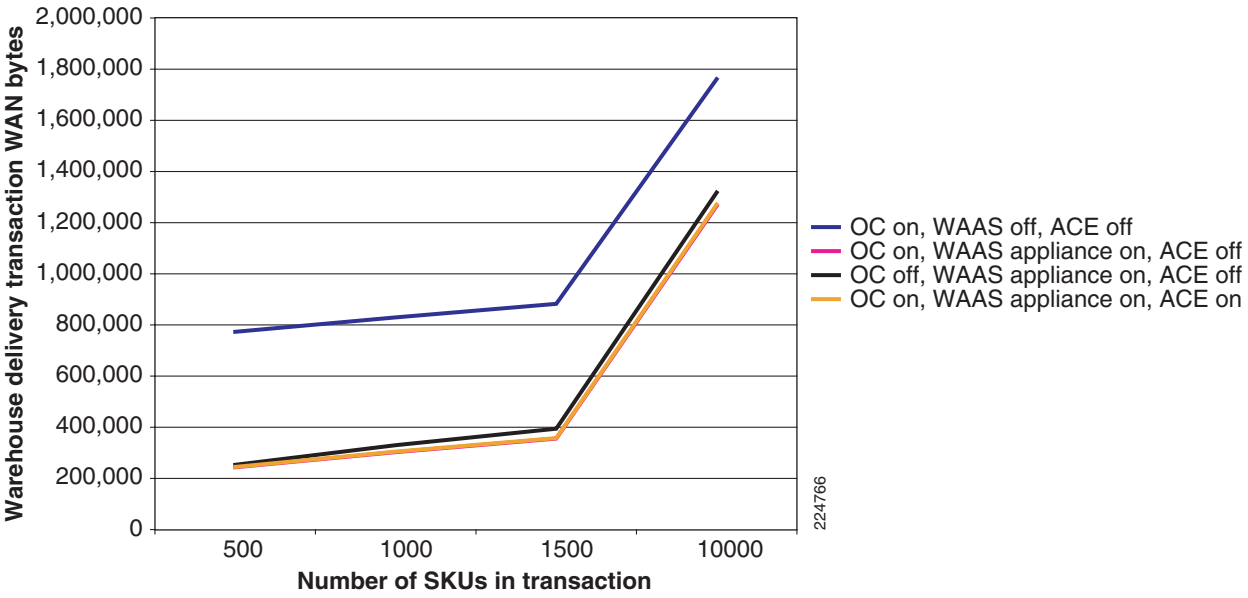


Figure 34 Large Store Transaction Bytes —1544Kbps



Summary and Conclusions

The Cisco Lean Retail Oracle Store Inventory Management solution demonstrates several benefits and considerations when deploying the Oracle SIM application within the Cisco Lean Retail environment.

The discovery of the overlapping port usage of the Oracle SIM client download and Napster could have caused erratic application performance issues in Oracles existing customer deployments. Security and QoS policies regularly block and restrict traffic using this port, negatively affecting the performance of Oracle SIM. Current and future retail deployments need to account for the overlap of this TCP port.

The Cisco WAAS Mobile was effective in its ability to compress and optimize Oracle SIM traffic. This is a cost effective method of optimizing retail store applications where the deployment of a WAAS appliance or a WAAS network module is not practical.

The Oracle SIM testing was performed from a retail clerk's perspective that included login, receive shipment, and logout. Performance improvement was found in several areas:

- For normal day-to-day SIM warehouse delivery transactions with Cisco WAAS turned on, transaction time was reduced by 30% to 60%. The transaction time reduction delivered through WAAS is more pronounced for low bandwidth stores. Furthermore, the amount of WAN traffic was reduced by 30% to 80% for the warehouse delivery transaction.
- Most of the reduction in warehouse delivery transaction time came from the login step. For security purposes, Cisco and Oracle recommend that users log in, perform their transactions, and log out. Consequently, this testing reflects the desired real-world behavior.
- Through the use of DNS and Cisco ACE, Oracle SIM client sessions were successfully distributed within the server farm, providing scalability and client access high availability.
- Cisco WAAS Mobile reduced transaction times by about 5% more than the WAAS appliance because fewer WAN bytes were passed from the data center to the store. Most stores run multiple applications that must communicate over the WAN to a data center. The CapEx and OpEx cost of a single WAAS device would need to be compared to that of multiple WAAS Mobile clients to determine the most cost-effective approach.
- With Cisco WAAS turned on, there was a 3% to 5% reduction in initial client download times. Downloaded SIM clients are persistent in the client's Java Web Start cache. Subsequent client downloads only occur if a patch is applied to the client code on the server, and then, only changed resources are downloaded. Oracle sends out patches every few months, so initial client downloads occur infrequently.
- Oracle SIM's native compression provides about the same level of compression as Cisco WAAS. There is no need to turn Oracle compression on if WAAS is turned on. Oracle application server cycles are saved because the application servers are not performing compression computations.
- Common perception is that Windows Remote Desktop Protocol is a superior method of converting fat clients into thin. Remote Desktop protocol was tested as an alternative to the traditional in store Oracle SIM client. There was marginal time savings using Windows RDP and it less efficient in WAN usage for all but the largest of transactions.

The functional interoperability testing of Oracle's Store Inventory Management application within Cisco's small, medium, and large Lean Retail reference architectures was successful. This solution's validation enables retailers to confidently progress to a pilot testing stage for technology deployment and avoids additional costly testing.

Appendix A—Test Environment Diagrams

Figure 35 Data Center

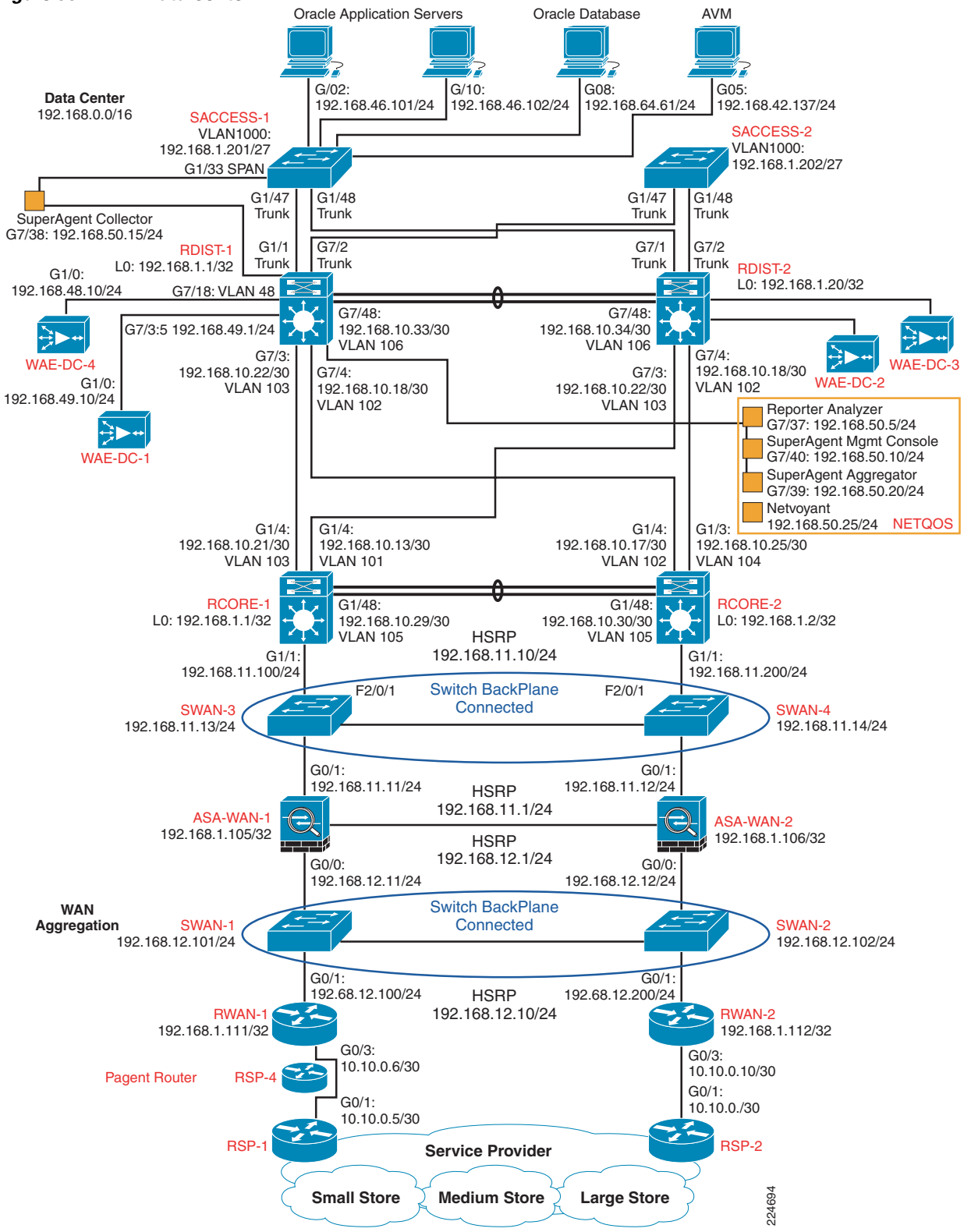


Figure 36 Small Store

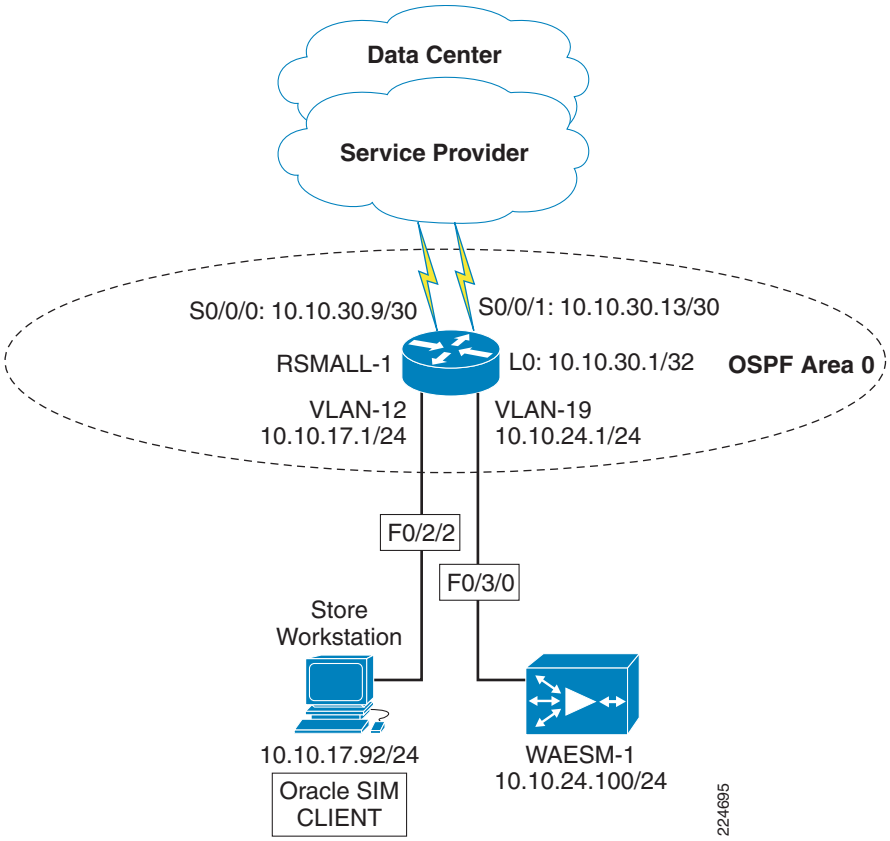


Figure 37 Medium Store

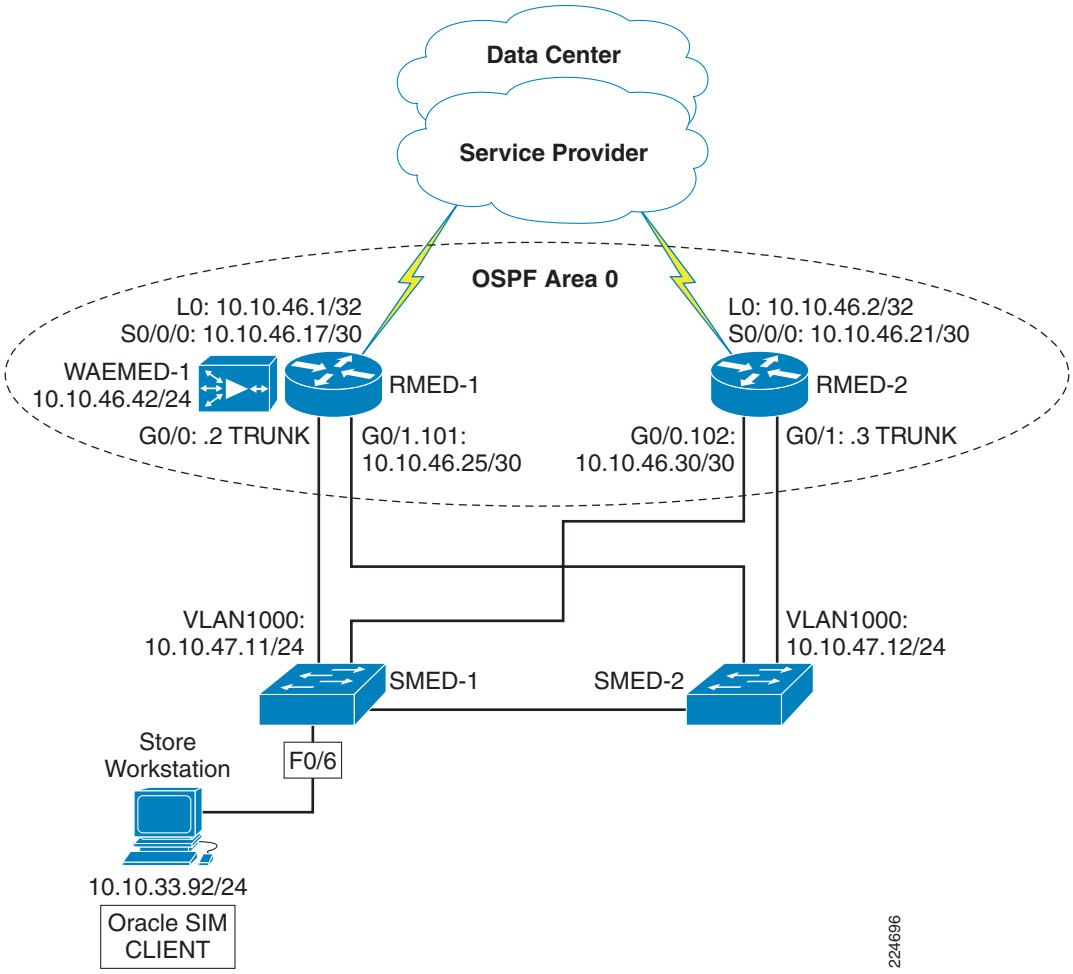
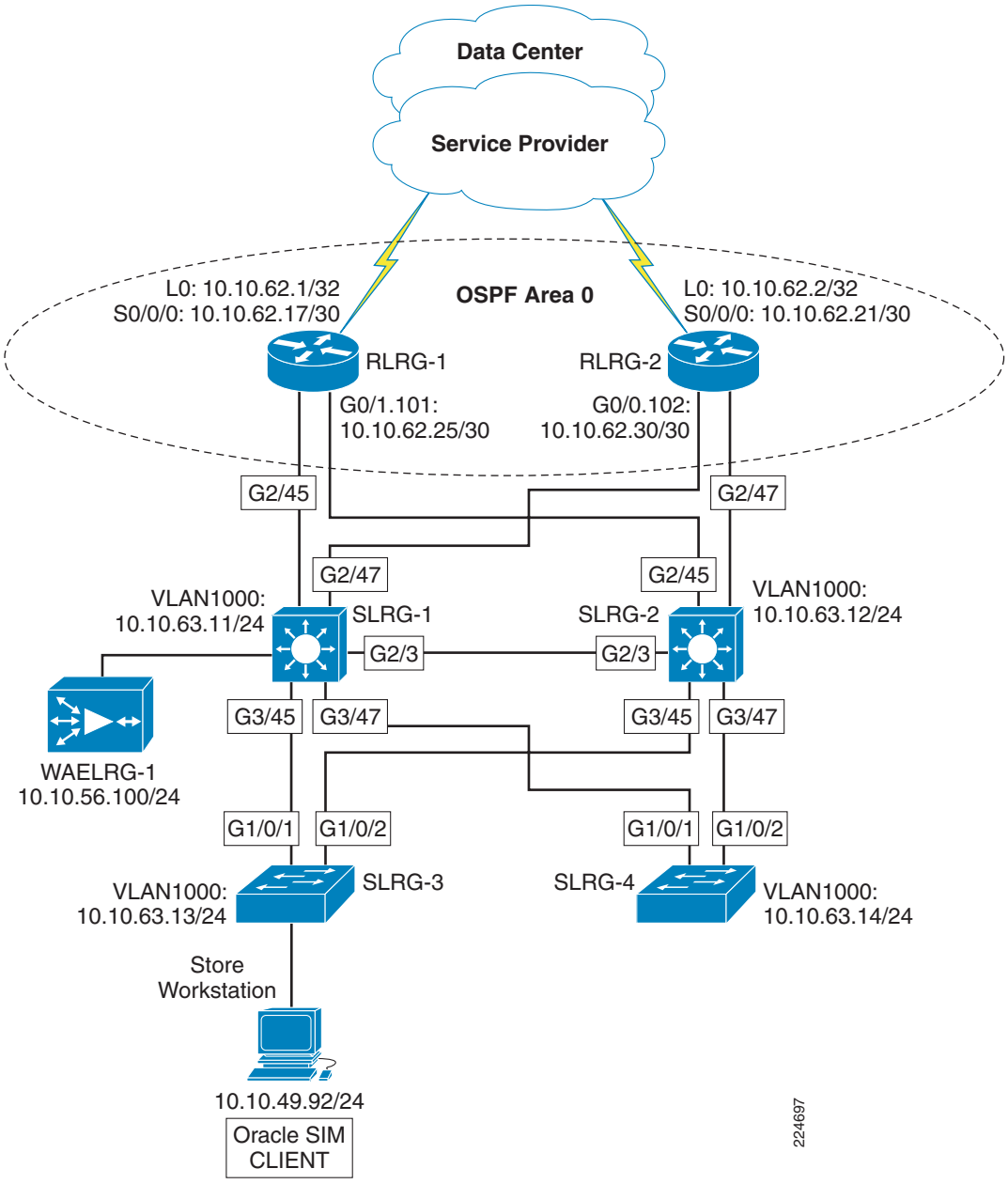


Figure 38 Large Store



Appendix B—Testing Results DATA

The following three test scenarios were performed as appropriate in each of the deployment types:

- T1—Clear Java web cache, IE cache, and clear WAAS DRE caches in data center and store (simulates initial client deployment).
- T2—Clear Client PC Java web and IE cache (simulates second PC or new windows user login being used in the store).
- T3—Do not clear any caches (simulates normal usage in a store for a repetitive user).

Table 3 through Table 5 are the recorded testing results. These results were compiled to create Figure 39 through Figure 47.

Table 3 Baseline Oracle SIM test results

Application: Oracle SIM								
End User Response Time	Baseline Tests Ace Off, Waas Off							
	Oracle Compression Off				Oracle Compression On			
Event	T1 Seconds	T1 Bytes	T3 Seconds	T3 Bytes	T1 Seconds	T1 Bytes	T3 Seconds	T3 Bytes
Data Center 1000Mbps	test024		test025		test016b		test017b	
Download SIM Client	11.91	17,010,916	1.13	39,380	12.25	17,444,720	1.11	39,380
Login to SIM	7.13	909,738	4.54	775,351	8.59	681,271	5.50	650,235
Perform QTP Script-500	5.50	1,492,492	5.62	1,494,137	6.50	63,276	6.11	64,899
Perform QTP Script-1000	6.72	2,893,241	7.45	2,895,996	6.82	123,813	6.91	121,117
Perform QTP Script-1500	8.57	4,290,817	8.36	4,294,001	8.93	173,767	8.90	173,787
Perform QTP Script-10,000	33.35	27,261,530	34.10	27,308,779	38.91	1,045,860	39.91	1,051,661
Logout of SIM	3.00	11,675	3.21	13,636	3.17	9,186	3.02	7,299
LAN Bytes (client side)		53,882,735		36,829,275		19,546,403		2,113,966
Small Store 128Kbps - WAAS Appliance	test022		test023		test010		test011	
Download SIM Client	1,067.03	17,052,392	4.82	45,784	1,100.28	17,544,607	4.91	39,380
Login to SIM	78.36	918,180	67.29	777,105	65.10	688,096	60.84	657,612
Perform QTP Script-500	104.27	1,513,628	103.58	1,513,686	13.40	65,682	11.64	65,976
Perform QTP Script-1000	194.03	2,928,151	193.97	2,928,215	17.28	123,034	17.74	123,004
Perform QTP Script-1500	287.13	4,346,495	287.84	4,346,943	22.36	175,306	22.69	174,632
Perform QTP Script-10,000	1,798.73	27,632,825	1,794.33	27,631,119	107.88	1,055,782	108.42	1,056,587
Logout of SIM	5.48	11,653	5.81	13,215	4.80	8,822	5.49	8,754
WAN Bytes (store link)		54,410,359		37,263,038		19,665,891		2,130,444
LAN Bytes (client side)		54,410,467		37,265,101		19,665,891		2,133,500
Small Store 128Kbps - WAAS Mobile	test022		test023		test010		test011	
Download SIM Client	1,067.03	17,052,392	4.82	45,784	1,100.28	17,544,607	4.91	39,380
Login to SIM	78.36	918,180	67.29	777,105	65.10	688,096	60.84	657,612
Perform QTP Script-500	104.27	1,513,628	103.58	1,513,686	13.40	65,682	11.64	65,976
Perform QTP Script-1000	194.03	2,928,151	193.97	2,928,215	17.28	123,034	17.74	123,004
Perform QTP Script-1500	287.13	4,346,495	287.84	4,346,943	22.36	175,306	22.69	174,632
Perform QTP Script-10,000	1,798.73	27,632,825	1,794.33	27,631,119	107.88	1,055,782	108.42	1,056,587
Logout of SIM	5.48	11,653	5.81	13,215	4.80	8,822	5.49	8,754
WAN Bytes		54,410,359		37,263,038		19,665,891		2,130,444
RAW Bytes		54,410,467		37,265,101		19,665,891		2,133,500
Small Store 128Kbps- Windows RDP - WAAS Appl	test039		test040		test037		test038	
RDP Login					26.00	329,726	28.26	330,225
Download SIM Client					15.26	61,969	4.52	45,512
Login to SIM					12.68	55,750	12.74	49,888
Perform QTP Script-500					13.92	97,379	14.37	78,387
Perform QTP Script-1000					12.70	80,546	15.75	80,720
Perform QTP Script-1500					17.31	83,469	15.23	74,683
Perform QTP Script-10,000					42.76	85,635	51.29	78,555
Logout of SIM					8.14	94,414	8.22	95,429
RDP Logout					5.57	14,194	4.57	12,438
WAN Bytes (store link)						1,073,168		1,010,688
LAN Bytes (client side)						1,073,170		1,010,692
Medium Store 512Kbps - WAAS NM Module	test020		test021		test012		test013	
Download SIM Client	277.57	16,931,388	1.92	39,380	285.59	17,387,142	1.76	39,380
Login to SIM	41.15	917,842	36.43	783,782	45.38	689,978	35.52	657,549
Perform QTP Script-500	33.45	1,514,690	33.33	1,518,851	10.99	63,661	11.12	66,590
Perform QTP Script-1000	57.04	2,934,705	56.20	2,933,394	12.99	123,869	12.42	122,329
Perform QTP Script-1500	82.55	4,360,157	80.54	4,356,373	14.84	174,760	14.72	174,316
Perform QTP Script-10,000	480.27	27,841,199	473.16	27,710,027	59.86	1,050,428	59.05	1,058,802
Logout of SIM	5.12	11,717	5.32	13,343	4.70	8,837	4.92	8,845
WAN Bytes (store link)		54,518,669		37,362,057		19,503,174		2,132,245
LAN Bytes (client side)		54,454,023		37,333,169		19,460,034		2,132,245
Large Store 1544Kbps - WAAS Appliance	test018		test019		test014		test015	
Download SIM Client	106.61	17,034,981	1.77	39,380	108.48	17,519,402	1.72	39,380
Login to SIM	35.68	917,154	32.59	783,746	34.36	687,561	31.54	658,309
Perform QTP Script-500	17.36	1,510,336	17.61	1,529,673	9.69	65,517	8.89	65,481
Perform QTP Script-1000	24.20	2,922,609	25.37	2,924,758	10.74	122,259	11.44	122,265
Perform QTP Script-1500	33.63	4,338,925	34.09	4,340,797	12.80	174,478	13.20	174,848
Perform QTP Script-10,000	184.28	27,608,367	182.20	27,609,803	47.53	1,053,629	49.69	1,052,177
Logout of SIM	5.33	13,093	6.35	55,341	4.28	9,019	3.93	8,758
WAN Bytes (store link)		54,352,436		37,314,825		19,637,477		2,125,724
LAN Bytes (client side)		54,352,436		37,314,825		19,637,477		2,125,724

224767

Table 4 Comparison Test Results with WAAS

Application: Oracle SIM												
End User Response Time	Comparison Tests Ace Off, Waas On											
	Oracle Compression Off						Oracle Compression On					
Event	T1 Seconds	T1 Bytes	T2 Seconds	T2 Bytes	T3 Seconds	T3 Bytes	T1 Seconds	T1 Bytes	T2 Seconds	T2 Bytes	T3 Seconds	T3 Bytes
Small Store 128Kbps - WAAS Appliance	test032		test033		test034		test007		test008		test009	
Download SIM Client	1,119.40	19,745,952	67.40	627,411	4.84	66,385	1,059.40	19,894,897	57.64	603,876	4.73	61,924
Login to SIM	32.10	161,394	24.23	115,494	22.16	119,315	30.64	164,247	31.07	119,792	21.49	115,909
Perform QTP Script-500	13.48	72,445	9.28	67,277	9.27	61,257	9.07	61,810	9.39	61,314	9.26	61,496
Perform QTP Script-1000	16.60	157,023	17.16	145,810	14.02	139,348	14.43	122,025	14.33	121,395	13.98	121,644
Perform QTP Script-1500	25.22	233,636	24.15	215,269	26.08	216,769	18.91	174,747	19.24	175,671	19.06	175,198
Perform QTP Script-10,000	129.05	1,534,253	107.76	1,131,078	123.19	1,304,547	107.90	1,174,147	106.65	1,163,188	107.08	1,168,666
Logout of SIM	2.91	6,254	2.73	3,828	3.58	5,044	3.95	5,942	3.20	6,606	3.31	6,164
WAN Bytes (store link)		21,914,722		2,307,954		1,914,333		21,602,356		2,254,405		1,713,609
LAN Bytes (client side)		53,826,438		53,895,215		37,018,453		18,794,559		18,813,433		2,141,416
Small Store 128Kbps - WAAS Mobile	test043		test044		test045		test046		test047		test048	
Download SIM Client	977.39	15,576,119	987.19	15,627,975	2.60	15,621	982.46	15,642,036	980.77	15,637,109	2.67	15,852
Login to SIM	28.59	105,536	22.41	103,513	14.73	53,131	23.92	99,103	21.10	96,987	16.69	55,442
Perform QTP Script-500	12.97	43,946	13.54	45,458	9.74	40,652	13.55	60,655	11.25	57,199	10.53	56,301
Perform QTP Script-1000	13.02	81,895	13.95	80,281	15.85	74,119	17.28	119,944	17.15	112,794	17.98	113,028
Perform QTP Script-1500	16.95	111,176	16.45	108,765	18.24	105,719	21.20	166,319	20.43	168,511	20.41	161,968
Perform QTP Script-10,000	84.81	760,526	80.10	755,945	80.65	725,047	108.71	1,060,955	107.83	1,040,142	106.03	997,976
Logout of SIM	4.75	6,462	5.84	4,717	5.73	6,645	4.83	6,289	4.27	6,213	3.93	3,765
WAN Bytes		16,700,429		16,738,567		1,045,434		17,139,306		17,143,441		1,427,497
RAW Bytes		54,058,008		54,064,369		36,734,673		19,370,880		19,377,587		2,124,057
Small Store 128Kbps- Windows RDP - WAAS Appliance	test041				test042		test035				test036	
RDP Login							24.63	328,764			25.08	329,497
Download SIM Client							39.07	78,200			6.02	56,570
Login to SIM							14.16	57,564			12.18	50,904
Perform QTP Script-500							11.97	90,505			10.50	81,670
Perform QTP Script-1000							12.60	74,662			12.74	92,775
Perform QTP Script-1500							14.29	85,577			14.25	70,745
Perform QTP Script-10,000							45.72	75,519			46.49	73,227
Logout of SIM							8.10	78,923			7.37	94,591
RDP Logout							3.67	13,908			3.91	12,565
WAN Bytes (store link)								1,081,676				1,042,703
LAN Bytes (client side)								1,081,666				1,042,693
Medium Store 512Kbps - WAAS NM Module	test029		test030		test031		test004		test005		test006	
Download SIM Client	280.63	16,898,103	25.45	576,775	1.88	63,129	282.83	16,890,245	25.29	578,801	1.93	63,154
Login to SIM	23.56	160,979	21.76	112,087	19.83	118,287	23.87	159,945	24.25	142,253	20.01	116,672
Perform QTP Script-500	6.41	69,936	6.50	60,965	6.43	63,925	10.53	59,924	10.03	60,684	10.65	60,606
Perform QTP Script-1000	9.28	152,643	8.91	139,716	8.92	143,670	13.01	119,248	12.93	119,869	10.65	119,430
Perform QTP Script-1500	12.25	228,161	11.93	205,958	11.11	216,436	13.43	172,136	15.45	173,696	12.28	173,238
Perform QTP Script-10,000	56.00	1,340,252	51.56	1,035,777	50.84	1,062,311	65.67	1,086,418	60.29	1,084,316	63.17	1,085,445
Logout of SIM	3.66	5,577	4.65	3,962	3.35	3,561	4.57	6,105	7.77	5,709	4.24	5,681
WAN Bytes (store link)		18,859,218		2,136,937		1,673,565		18,498,834		2,167,562		1,626,527
LAN Bytes (client side)		53,836,794		53,971,433		37,077,759		18,856,609		18,954,736		2,138,880
Large Store 1544Kbps - WAAS Appliance	test026		test027		test028		test001		test002		test003	
Download SIM Client	102.87	19,180,373	20.47	553,954	1.73	62,652	102.98	19,142,035	21.70	847,286	1.70	63,317
Login to SIM	23.07	159,608	22.85	117,223	21.35	118,771	21.81	152,729	21.60	143,431	18.77	113,227
Perform QTP Script-500	7.30	68,454	5.85	62,482	6.25	66,625	9.09	60,546	8.62	59,966	8.04	61,082
Perform QTP Script-1000	7.61	153,517	7.22	131,250	7.25	143,464	10.54	120,166	9.88	120,355	10.26	120,056
Perform QTP Script-1500	9.44	221,636	9.41	207,417	9.48	208,141	11.66	172,417	11.92	171,882	12.19	172,687
Perform QTP Script-10,000	40.89	1,395,393	38.99	1,103,876	40.75	1,129,991	50.01	1,100,828	48.37	1,099,192	50.60	1,080,985
Logout of SIM	2.89	5,393	2.52	3,509	3.07	4,658	3.90	5,796	3.61	5,180	3.48	5,905
WAN Bytes (store link)		21,188,535		2,181,436		1,735,968		20,759,044		2,449,532		1,619,361
LAN Bytes (client side)		53,555,105		53,870,137		36,838,307		18,808,976		19,009,226		2,126,982

224768

Table 5 Comparison Test Results with WAAS and ACE

Application: Oracle SIM						
End User Response Time	Comparison Tests					
	Ace On, Waas On					
	Oracle Compression On					
Event	T1 Seconds	T1 Bytes	T2 Seconds	T2 Bytes	T3 Seconds	T3 Bytes
Small Store 128Kbps - WAAS Appliance	test055		test056		test057	
Download SIM Client	1,057.73	19,653,124	70.25	684,725	4.71	65,016
Login to SIM	26.57	153,280	26.24	145,410	22.32	115,426
Perform QTP Script-500	9.07	61,293	8.63	61,850	8.87	62,238
Perform QTP Script-1000	13.95	121,473	13.44	121,569	13.38	121,909
Perform QTP Script-1500	18.79	174,755	18.76	173,756	19.91	175,986
Perform QTP Script-10,000	107.59	1,164,881	108.92	1,165,330	113.91	1,166,423
Logout of SIM	3.15	6,522	2.99	6,152	2.63	6,922
WAN Bytes (store link)		21,339,864		2,361,120		1,716,189
LAN Bytes (client side)		18,861,999		18,923,825		2,125,937
Small Store 128Kbps - WAAS Mobile	test058		test059		test060	
Download SIM Client	987.68	15,600,696	987.23	15,633,951	3.67	14,311
Login to SIM	20.20	98,621	18.98	97,520	15.49	57,570
Perform QTP Script-500	13.14	61,898	9.05	58,312	8.68	60,573
Perform QTP Script-1000	13.84	113,787	13.22	117,019	14.09	116,877
Perform QTP Script-1500	18.37	172,881	18.96	171,606	18.71	166,830
Perform QTP Script-10,000	104.78	1,051,370	103.55	1,033,387	100.17	979,231
Logout of SIM	3.67	5,024	3.77	4,225	4.68	4,338
WAN Bytes		17,120,897		17,129,259		1,409,404
RAW Bytes		19,384,291		19,376,864		2,122,626
Small Store 128Kbps- Windows RDP - WAAS Appliance	test061				test062	
RDP Login	19.39	220,776			19.51	221,528
Download SIM Client	34.54	66,082			4.13	42,833
Login to SIM	14.34	56,830			10.36	51,857
Perform QTP Script-500	11.80	75,659			11.06	75,720
Perform QTP Script-1000	12.45	67,881			11.12	63,248
Perform QTP Script-1500	13.41	62,993			13.53	72,514
Perform QTP Script-10,000	46.30	58,916			46.83	56,796
Logout of SIM	7.86	90,288			5.99	73,544
RDP Logout	4.50	11,060			3.93	9,935
WAN Bytes (store link)		850,372				814,130
LAN Bytes (client side)		850,362				814,120
Medium Store 512Kbps - WAAS NM Module	test052		test053		test054	
Download SIM Client	279.55	16,816,460	24.72	538,108	4.86	64,778
Login to SIM	23.46	150,083	22.34	113,571	20.17	110,635
Perform QTP Script-500	7.05	59,990	6.32	60,764	6.54	60,083
Perform QTP Script-1000	8.77	121,478	8.79	119,175	8.45	119,922
Perform QTP Script-1500	12.34	173,381	10.76	172,003	10.96	172,249
Perform QTP Script-10,000	60.52	1,079,608	56.47	1,084,077	56.36	1,083,238
Logout of SIM	3.71	5,770	3.58	5,918	3.14	5,825
WAN Bytes (store link)		18,411,305		2,095,850		1,618,817
LAN Bytes (client side)		19,321,934		19,499,344		2,136,991
Large Store 1544Kbps - WAAS Appliance	test049		test050		test051	
Download SIM Client	103.85	19,110,962	22.49	929,394	1.73	63,339
Login to SIM	24.68	155,499	20.92	139,355	19.14	115,127
Perform QTP Script-500	9.44	60,929	6.07	60,910	5.86	60,256
Perform QTP Script-1000	9.22	120,155	7.76	119,654	7.71	119,729
Perform QTP Script-1500	11.11	172,831	10.02	172,881	10.21	172,403
Perform QTP Script-10,000	55.13	1,082,644	54.27	1,085,723	53.02	1,084,316
Logout of SIM	2.81	5,932	2.87	6,344	3.28	6,092
WAN Bytes (store link)		20,713,486		2,516,508		1,623,500
LAN Bytes (client side)		18,723,620		19,045,700		2,120,628

224769

Each of the following twelve figures (Figure 39 through Figure 47) represent the testing results data for the small, medium, and large stores. Each data point represents a complete store user transaction which includes client startup, client login, perform a warehouse delivery of X number of skews, logout, and close the Oracle SIM application.

Figure 39 Small Store Local Client Transaction Time, ACE Off —128Kbps

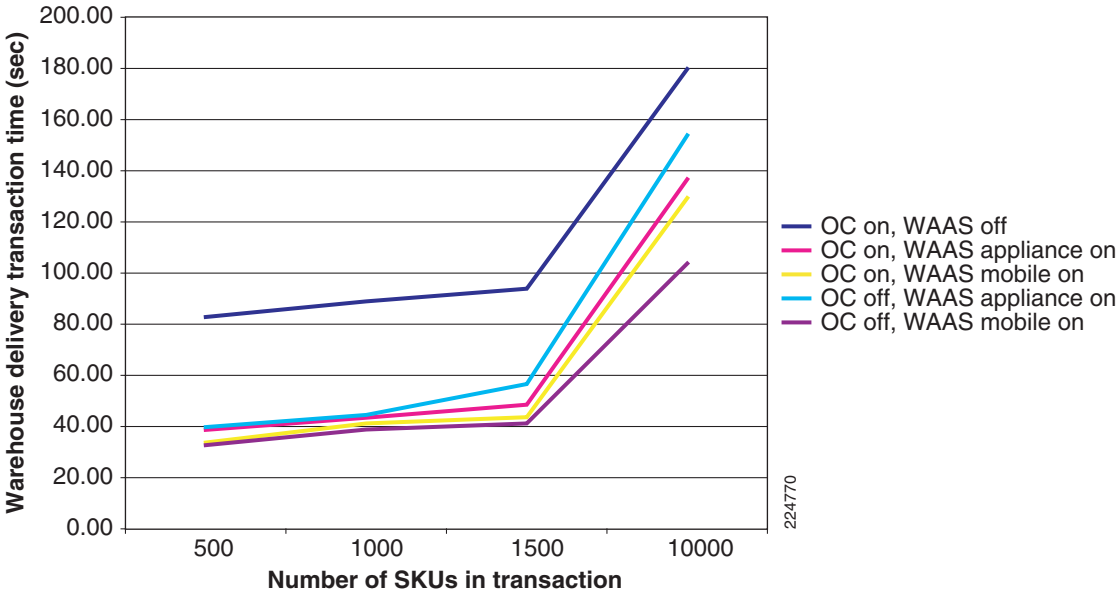


Figure 40 Small Store Local Client Transaction Bytes, ACE Off—128Kbps

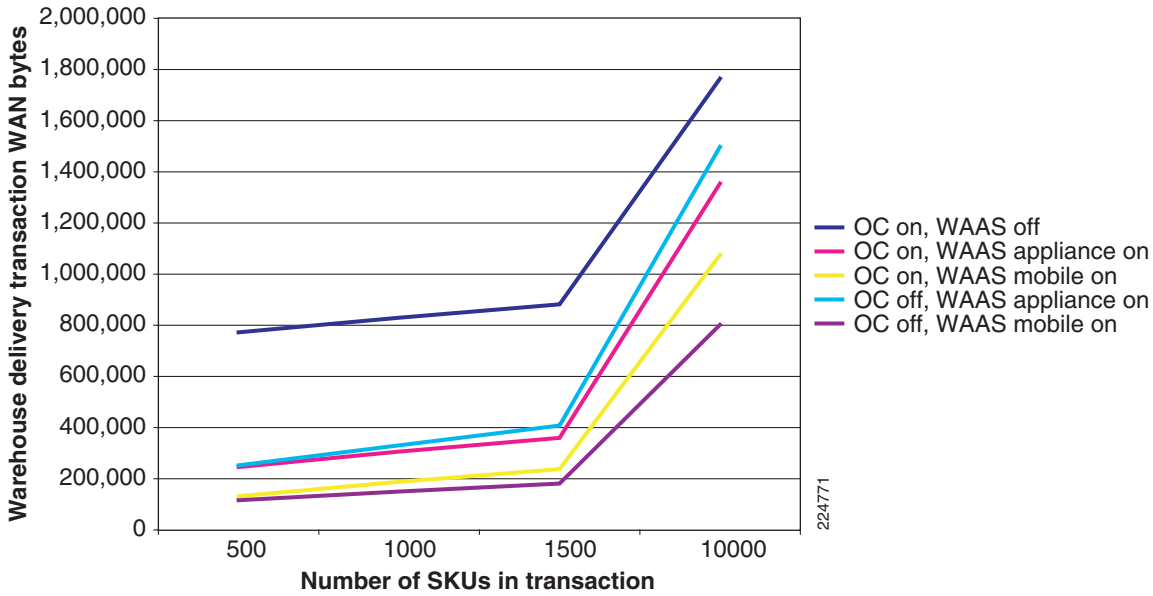


Figure 41 Small Store Windows RDP Transaction Time, ACE Off —128Kbps

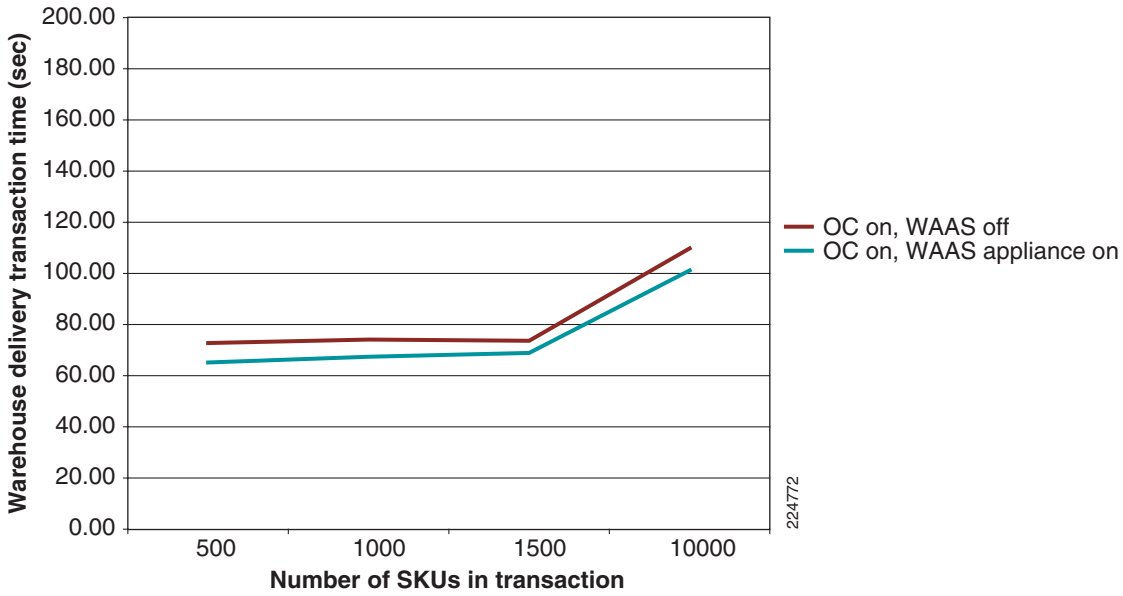


Figure 42 Small Store Windows RDP Transaction Bytes, ACE Off —128Kbps

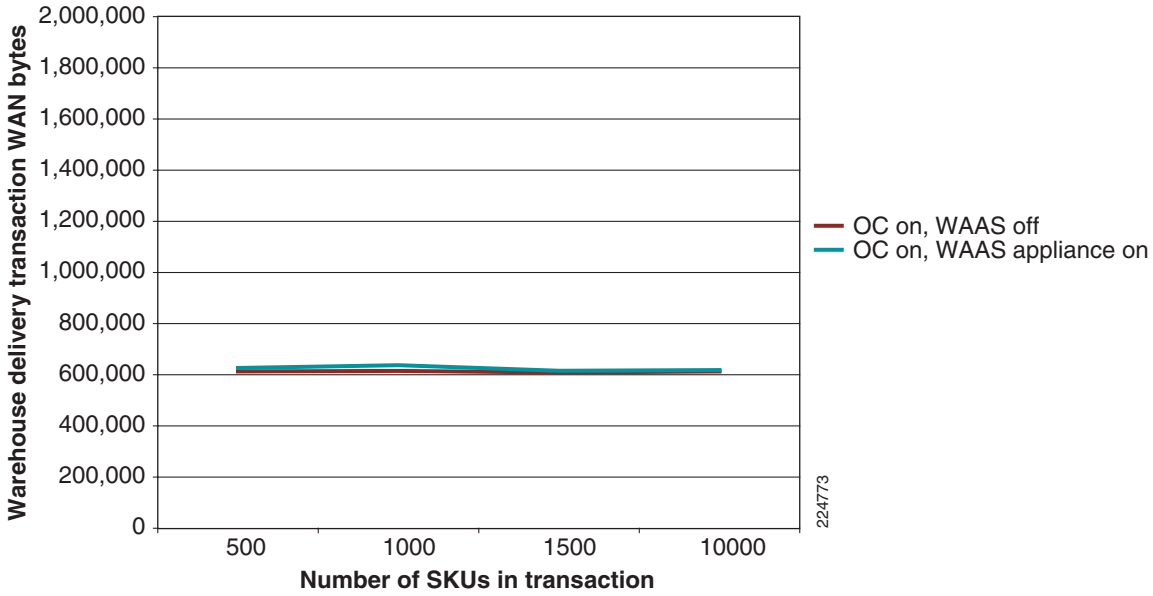


Figure 43 Small Store Local Client Transaction Time, ACE On—128Kbps

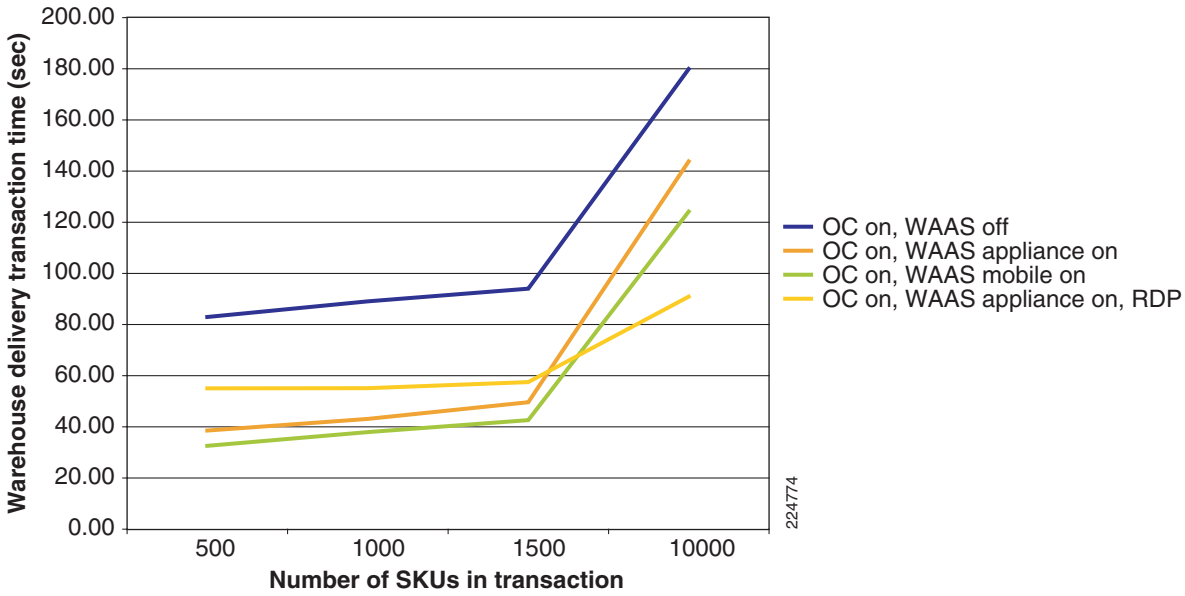


Figure 44 Small Store Local Client Transaction Bytes, ACE On—128Kbps

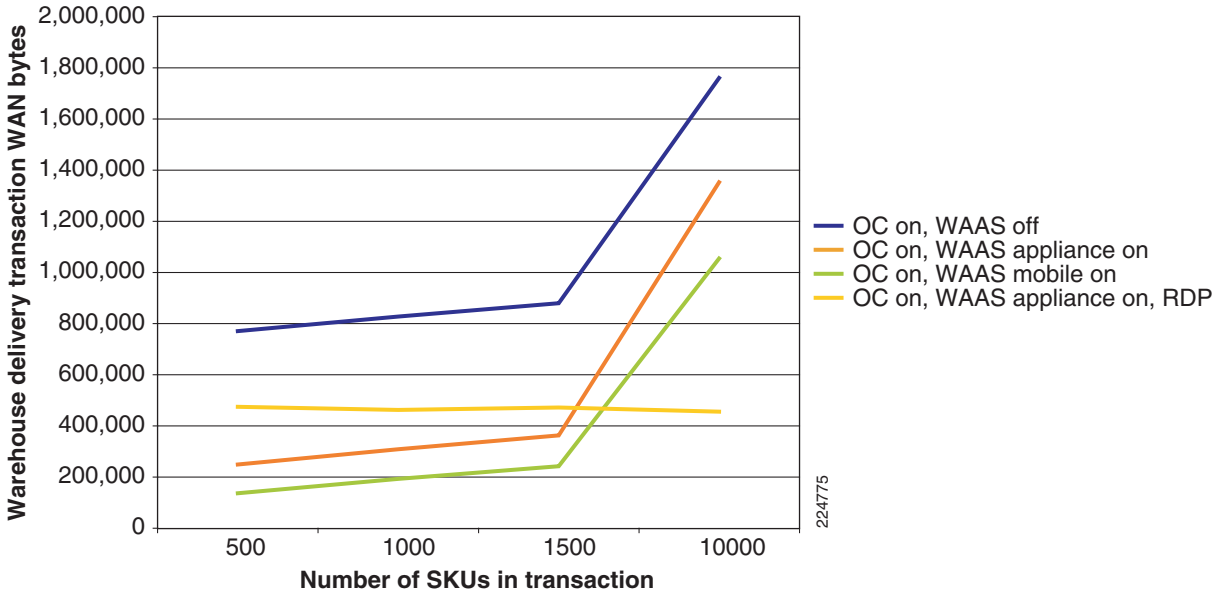


Figure 45 Small Store Transaction Time—128kbps

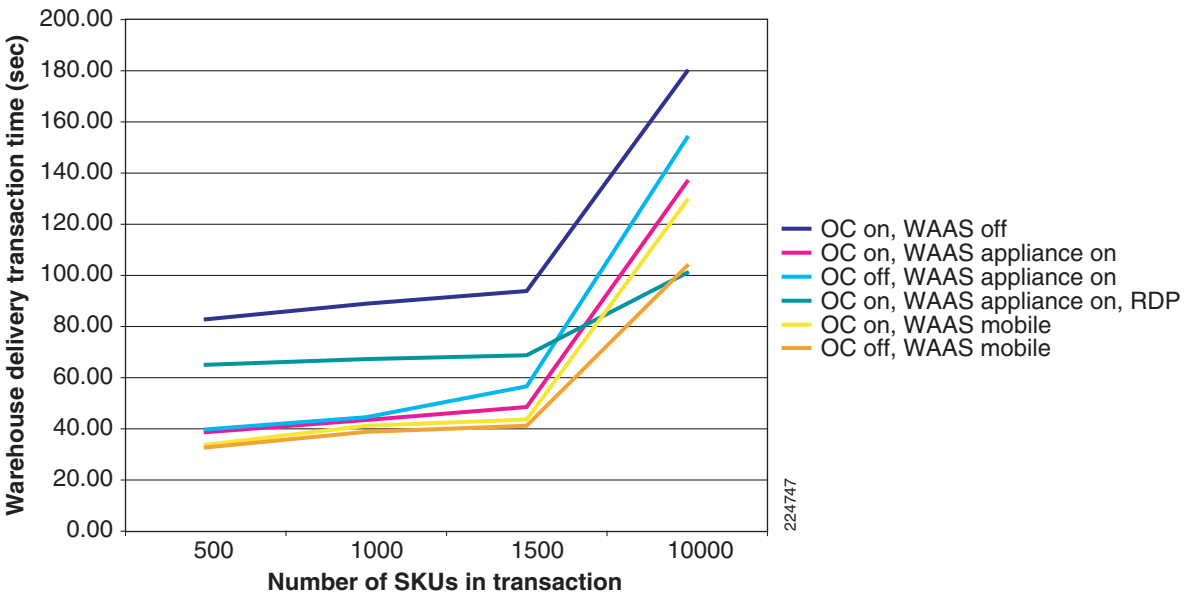


Figure 46 Small Store Transaction Bytes —128kbps

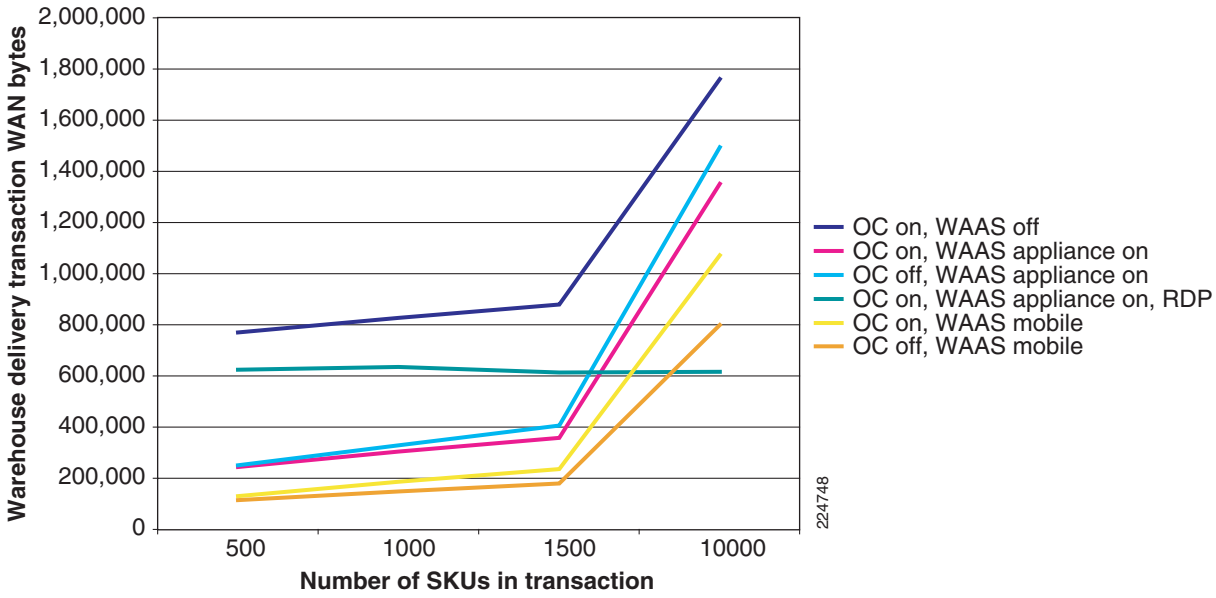


Figure 47 Medium Store Transaction Time—512Kbps

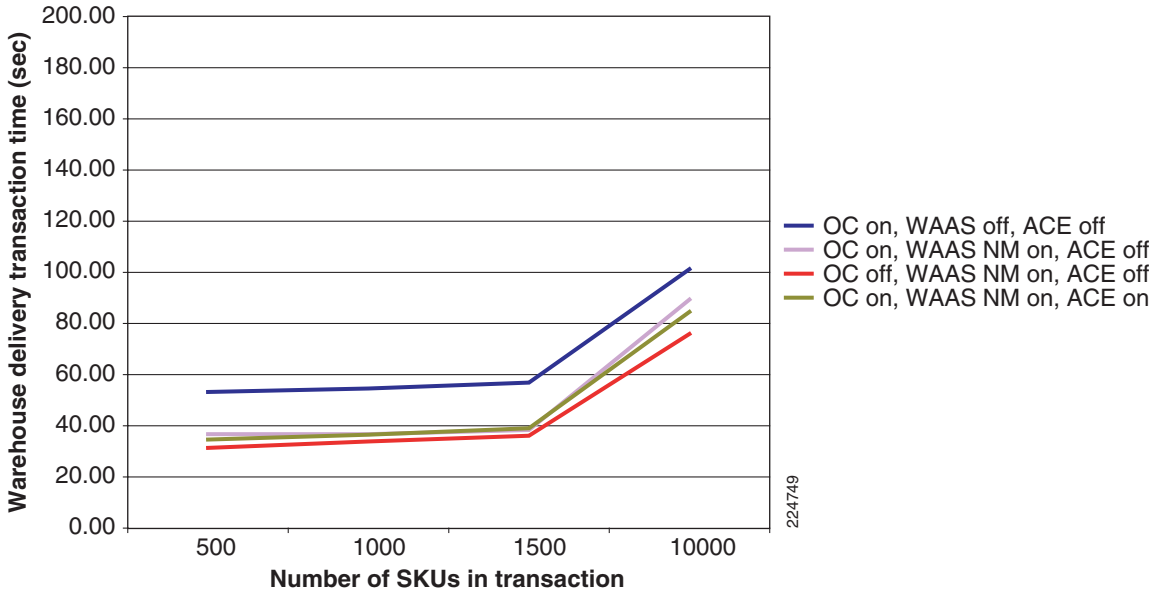


Figure 48 Medium Store Transaction Bytes—512Kbps

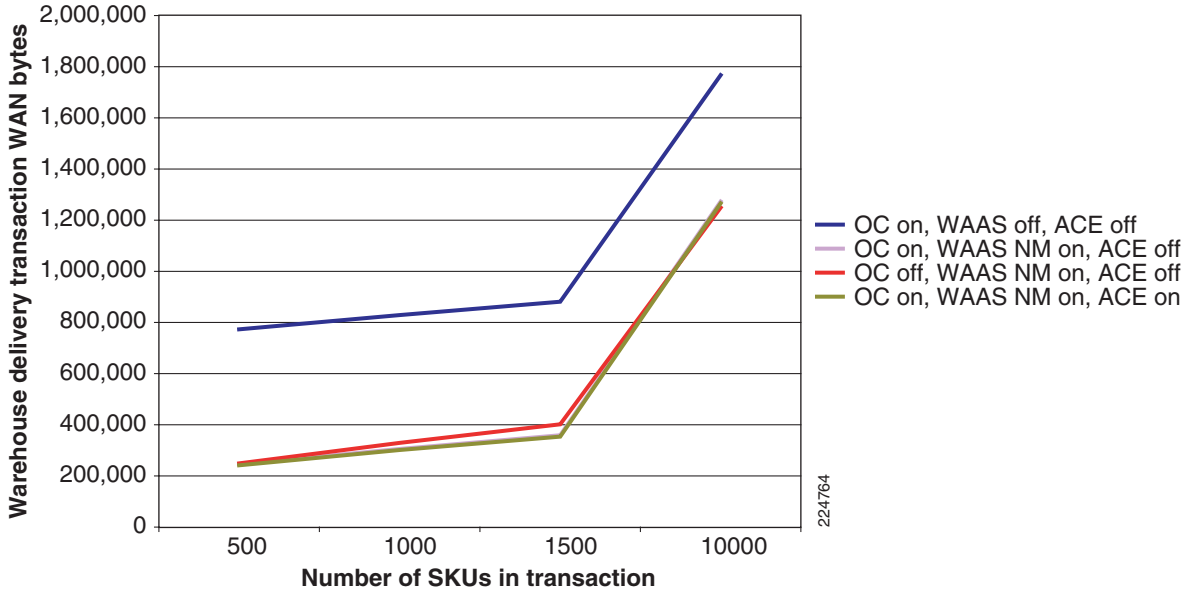


Figure 49 Large Store Transaction Time—1544Kbps

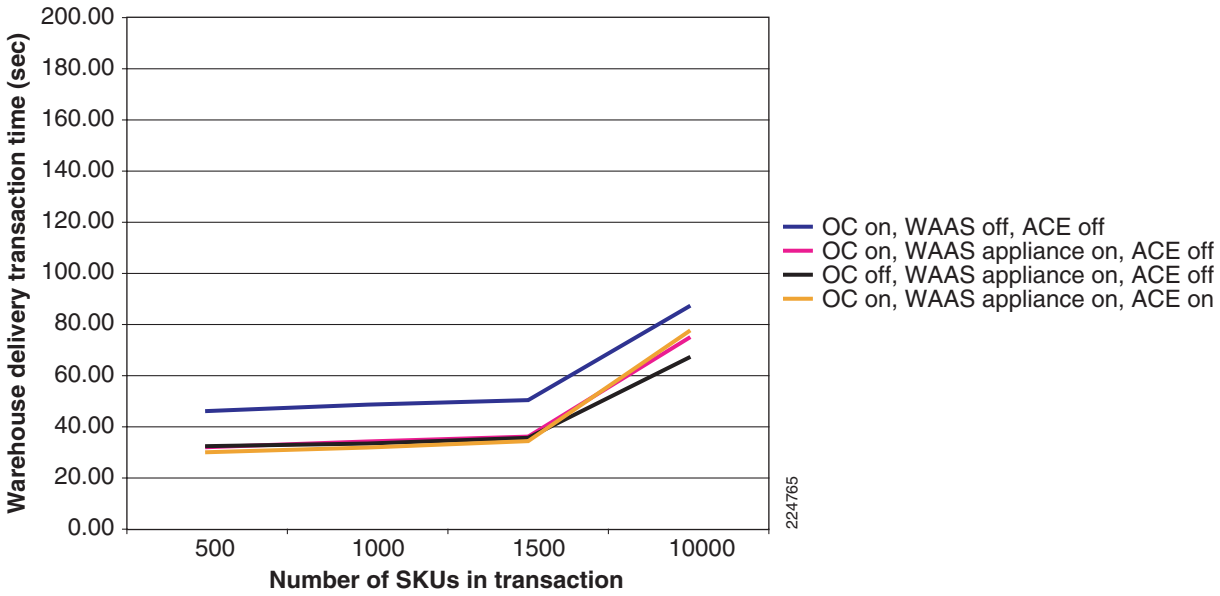
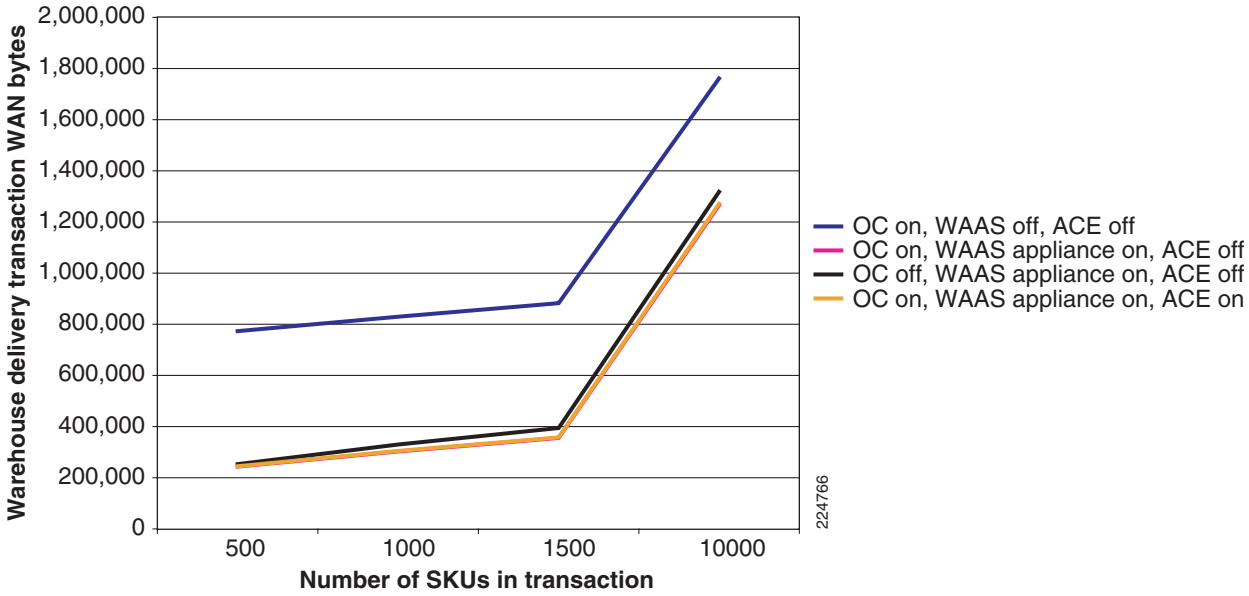


Figure 50 Large Store Transaction Bytes —1544Kbps



Appendix C—Configurations

Data Center Configurations

ACE Configurations

ACE Admin Context

```
ACE1-Slot4/Admin# sh run
Generating configuration....

login timeout 60
hostname ACE1-Slot4
boot system image:c6ace-t1k9-mz.3.0.0_A1_6_3a.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

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
  31 match protocol https any
  32 match protocol snmp any

policy-map type management first-match REMOTE-MGT
  class REMOTE-ACCESS
    permit

interface vlan 20
  ip address 192.168.2.3 255.255.255.0
  service-policy input REMOTE-MGT
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.2.1

context oracle
  description Oracle SIM
  allocate-interface vlan 46
  allocate-interface vlan 146
  member Gold

username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/  role Admin domain
default-domain
username www password 5 $1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/  role Admin domain de
fault-domain
```

ACE SIM Context

```
ACE1-Slot4/oracle# sh run
Generating configuration....



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


probe icmp PING
  interval 2
probe http SIM
  port 7777
  interval 5
  faildetect 2
  request method get url /sim-ws/simWebService
  expect status 200 200

rserver host oracle1
  ip address 192.168.46.101
  inservice
rserver host oracle2
  ip address 192.168.46.102
  inservice

serverfarm host ORACLE
  probe PING
  probe SIM
  rserver oracle1
    inservice
  rserver oracle2
    inservice

sticky ip-netmask 255.255.255.255 address source src-ip-sticky
  timeout 10
  serverfarm ORACLE

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
class-map match-all VIP-HTTP-11
  2 match virtual-address 192.168.46.100 any

policy-map type management first-match REMOTE-MGT
  class REMOTE-ACCESS
    permit
policy-map type loadbalance first-match VIP-POLICY-11
  class class-default
    sticky-serverfarm src-ip-sticky
policy-map multi-match LB-VIP
  class VIP-HTTP-11
    loadbalance vip inservice
    loadbalance policy VIP-POLICY-11
    loadbalance vip icmp-reply

interface vlan 46
  bridge-group 1
```

```
  access-group input ANYONE
  service-policy input REMOTE-MGT
  service-policy input LB-VIP
  no shutdown
interface vlan 146
  bridge-group 1
  access-group input ANYONE
  no shutdown

interface bvi 1
  ip address 192.168.46.10 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.46.1
```

WAE Configuration

Central Manager "WAE-DC4"

```
WAEDC-4#sh run
! WAAS version 4.0.19 (build b14 Jun 13 2008)
!
device mode central-manager
!
hostname WAEDC-4
!
clock timezone PST8PDT -7 0
!
ip domain-name cisco-irn.com
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 192.168.48.10 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
ip default-gateway 192.168.48.1
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.42.130
!
ntp server 192.168.62.162
ntp server 192.168.62.161
ntp server 192.168.0.1
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE 7D891AB40
2CAF2E89CCDD33ED54333AC
!
authentication login local enable primary
authentication configuration local enable primary
!
cms enable
!
```

```
! End of WAAS configuration
WAEDC-4#
```

Data Center WAE (Headend) "WAE-DC1"

```
WAEDC-1#sh run
! WAAS version 4.0.19 (build b14 Jun 13 2008)
!
device mode application-accelerator
!
hostname WAEDC-1
!
clock timezone PST8PDT -7 0
!
ip domain-name cisco-irn.com
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 192.168.49.10 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
interface InlineGroup 1/0
 inline vlan all
 shutdown
 exit
interface InlineGroup 1/1
 inline vlan all
 shutdown
 exit
!
ip default-gateway 192.168.49.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.42.130
!
logging facility syslog
logging host 192.168.42.134
logging console enable
!
ntp server 192.168.62.162
ntp server 192.168.62.161
ntp server 192.168.0.1
!
wccp router-list 1 192.168.62.161
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
egress-method negotiated-return intercept-method wccp
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE 7D891AB40
2CAF2E89CCDD33ED54333AC
!
snmp-server contact Christian Janoff
```

```
snmp-server location Croms Mountain
snmp-server enable traps config
snmp-server enable traps content-engine disk-read
snmp-server enable traps content-engine disk-write
snmp-server enable traps content-engine disk-fail
snmp-server enable traps content-engine overload-bypass
snmp-server enable traps content-engine transaction-log
snmp-server enable traps alarm raise-critical
snmp-server enable traps alarm clear-critical
snmp-server enable traps alarm raise-major
snmp-server enable traps alarm clear-major
snmp-server enable traps alarm raise-minor
snmp-server enable traps alarm clear-minor
snmp-server enable traps entity
snmp-server enable traps snmp authentication
snmp-server enable traps snmp cold-start
snmp-server enable traps event
snmp-server host 192.168.42.134 retaillab v3  priv
snmp-server community ciscoprivate rw
snmp-server community ciscopublic
!
tacacs key ****
tacacs host 192.168.42.131 primary
!
windows-domain netbios-name "WAEDC-1"
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
no telnet enable
!
no sshd version 1
sshd enable
!
flow monitor tcpstat-v1 host 192.168.50.10
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
policy-engine application
… policy engine configuration excerpted for brevity
   name OracleSIM
   … classifiers excerpted for brevity
   classifier OracleSIMClassifier
      match dst port range 12401 12500
      match dst port eq 7777
      match dst port eq 6003
   exit
   map basic
      name OracleSIM classifier OracleSIMClassifier action optimize full

…configuration excerpted for brevity
!
central-manager address 192.168.48.10
cms enable
!
!
disk encrypt enable
!
banner motd message "WARNING:  \n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR TH
```

```
E USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\
nANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \
nTO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
\nTO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRES
ENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTH
ER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL
 CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFI
CIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACC
ESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.\n"
banner login message "WARNING:\nTHIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF A
UTHORIZED USERS ONLY!"
banner exec message "WARNING:\n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE
USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\nA
NY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \nT
O MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY\n
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRESEN
TATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTHER
 NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL C
ONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFICI
ALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACCES
S IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS."
banner enable
!
! End of WAAS configuration
WAEDC-1#
```

Small Store Configurations

Small Store WAE Appliance "WAESM-1"

```
WAESM-1#sh run
! WAAS version 4.0.19 (build b14 Jun 13 2008)
!
device mode application-accelerator
!
hostname WAESM-1
!
clock timezone PST8PDT -7 0
!
ip domain-name cisco-irn.com
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.10.24.100 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
interface InlineGroup 1/0
 inline vlan all
 shutdown
 exit
interface InlineGroup 1/1
 inline vlan all
 shutdown
```

```
 exit
!
ip default-gateway 10.10.24.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.42.130
!
logging facility syslog
logging host 192.168.42.134
logging console enable
!
ntp server 192.168.42.130
!
wccp router-list 1 10.10.24.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
egress-method negotiated-return intercept-method wccp
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE 7D891AB40
2CAF2E89CCDD33ED54333AC
!
snmp-server contact Christian Janoff
snmp-server location Croms Mountain
!
tacacs key ****
tacacs host 192.168.42.131 primary
!
windows-domain netbios-name "WAESM-1"
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
no telnet enable
!
no sshd version 1
sshd enable
!
flow monitor tcpstat-v1 host 192.168.50.10
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
policy-engine application
… policy engine configuration excerpted for brevity
   name OracleSIM
   … classifiers excerpted for brevity
   classifier OracleSIMClassifier
      match dst port range 12401 12500
      match dst port eq 7777
      match dst port eq 6003
   exit
   map basic
      name OracleSIM classifier OracleSIMClassifier action optimize full
…configuration excerpted for brevity
```

```
!
central-manager address 192.168.48.10
cms enable
!
disk encrypt enable
!
banner motd message "WARNING:  \n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR TH
E USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\
nANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \
nTO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
\nTO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRES
ENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTH
ER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL
 CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFI
CIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACC
ESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.\n"
banner login message "WARNING:\nTHIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF A
UTHORIZED USERS ONLY!"
banner exec message "WARNING:\n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE
USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\nA
NY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \nT
O MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY\n
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRESEN
TATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTHER
 NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL C
ONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFICI
ALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACCES
S IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS."
banner enable
!
! End of WAAS configuration
WAESM-1#
```

Medium Store Configurations

Medium Store Router Configuration for the WAE Network Module

```
!
interface Integrated-Service-Engine1/0
 ip address 10.10.46.41 255.255.255.252
 service-module ip address 10.10.46.42 255.255.255.252
 service-module ip default-gateway 10.10.46.41
 no keepalive
!
```

Medium Store WAE Network Module

```
WAEMED-1#sh run
! WAAS version 4.0.19 (build b14 Jun 13 2008)
!
device mode application-accelerator
!
hostname WAEMED-1
!
clock timezone PST8PDT -7 0
!
ip domain-name cisco-irn.com
```

```
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.10.46.42 255.255.255.252
 no autosense
 bandwidth 1000
 full-duplex
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
ip default-gateway 10.10.46.41
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.42.130
!
logging facility syslog
logging host 192.168.42.134
logging console enable
!
ntp server 192.168.62.162
ntp server 192.168.62.161
ntp server 192.168.0.1
!
wccp router-list 1 10.10.46.41
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
egress-method negotiated-return intercept-method wccp
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE 7D891AB40
2CAF2E89CCDD33ED54333AC
!
snmp-server contact Christian Janoff
snmp-server location Croms Mountain
snmp-server enable traps config
snmp-server enable traps content-engine disk-read
snmp-server enable traps content-engine disk-write
snmp-server enable traps content-engine disk-fail
snmp-server enable traps content-engine overload-bypass
snmp-server enable traps content-engine transaction-log
snmp-server enable traps alarm raise-critical
snmp-server enable traps alarm clear-critical
snmp-server enable traps alarm raise-major
snmp-server enable traps alarm clear-major
snmp-server enable traps alarm raise-minor
snmp-server enable traps alarm clear-minor
snmp-server enable traps entity
snmp-server enable traps snmp authentication
snmp-server enable traps snmp cold-start
snmp-server enable traps event
snmp-server host 192.168.42.134 retaillab v3  priv
snmp-server community ciscoprivate rw
snmp-server community ciscopublic
!
tacacs key ****
tacacs host 192.168.42.131 primary
```

```
!
windows-domain netbios-name "WAEMED-1"
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
no telnet enable
!
no sshd version 1
sshd enable
!
flow monitor tcpstat-v1 host 192.168.50.10
flow monitor tcpstat-v1 enable
!
policy-engine application
… policy engine configuration excerpted for brevity
   name OracleSIM
   … classifiers excerpted for brevity
   classifier OracleSIMClassifier
      match dst port range 12401 12500
      match dst port eq 7777
      match dst port eq 6003
   exit
   map basic
      name OracleSIM classifier OracleSIMClassifier action optimize full
…configuration excerpted for brevity
!
central-manager address 192.168.48.10
cms enable
!
disk encrypt enable
!
banner motd message "WARNING:  \n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR TH
E USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\
nANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \
nTO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
\nTO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRES
ENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTH
ER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL
 CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFI
CIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACC
ESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.\n"
banner login message "WARNING:\nTHIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF A
UTHORIZED USERS ONLY!"
banner exec message "WARNING:\n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE
USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\nA
NY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \nT
O MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY\n
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRESEN
TATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTHER
 NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL C
ONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFICI
ALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACCES
S IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS."
banner enable
!
! End of WAAS configuration
WAEMED-1#
```

Large Store Configurations

Large Store WAE Appliance

```
WAELRG-1#sh run
! WAAS version 4.0.19 (build b14 Jun 13 2008)
!
device mode application-accelerator
!
hostname WAELRG-1
!
clock timezone PST8PDT -7 0
!
ip domain-name cisco-irn.com
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.10.56.100 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
interface InlineGroup 1/0
 inline vlan all
 shutdown
 exit
interface InlineGroup 1/1
 inline vlan all
 shutdown
 exit
!
ip default-gateway 10.10.56.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.42.130
!
logging facility syslog
logging host 192.168.42.134
logging console enable
!
ntp server 192.168.62.162
ntp server 192.168.0.1
ntp server 192.168.62.161
!
wccp router-list 1 10.10.62.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
egress-method negotiated-return intercept-method wccp
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE 7D891AB40
2CAF2E89CCDD33ED54333AC
```

```
!
snmp-server contact Christian Janoff
snmp-server location Croms Mountain
snmp-server enable traps config
snmp-server enable traps content-engine disk-read
snmp-server enable traps content-engine disk-write
snmp-server enable traps content-engine disk-fail
snmp-server enable traps content-engine overload-bypass
snmp-server enable traps content-engine transaction-log
snmp-server enable traps alarm raise-critical
snmp-server enable traps alarm clear-critical
snmp-server enable traps alarm raise-major
snmp-server enable traps alarm clear-major
snmp-server enable traps alarm raise-minor
snmp-server enable traps alarm clear-minor
snmp-server enable traps entity
snmp-server enable traps snmp authentication
snmp-server enable traps snmp cold-start
snmp-server enable traps event
snmp-server host 192.168.42.134 retaillab v3  priv
snmp-server community ciscoprivate rw
snmp-server community ciscopublic
!
tacacs key ****
tacacs host 192.168.42.131 primary
!
windows-domain netbios-name "WAELRG-1"
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
no telnet enable
!
no sshd version 1
sshd enable
!
flow monitor tcpstat-v1 host 192.168.50.10
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
!
policy-engine application
… policy engine configuration excerpted for brevity
   name OracleSIM
   … classifiers excerpted for brevity
   classifier OracleSIMClassifier
      match dst port range 12401 12500
      match dst port eq 7777
      match dst port eq 6003
   exit
   map basic
      name OracleSIM classifier OracleSIMClassifier action optimize full
…configuration excerpted for brevity
!
central-manager address 192.168.48.10
cms enable
!
!
disk encrypt enable
!
```

```
banner motd message "WARNING:  \n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR TH
E USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\
nANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \
nTO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
\nTO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRES
ENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTH
ER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL
 CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFI
CIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACC
ESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.\n"
banner login message "WARNING:\nTHIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF A
UTHORIZED USERS ONLY!"
banner exec message "WARNING:\n    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE
USE OF CISCO INC.****\n                    **** AUTHORIZED USERS ONLY! ****\n\nA
NY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT \nT
O MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY\n
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER \nREPRESEN
TATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT\nFURTHER
 NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER \nCRIMINAL C
ONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW \nENFORCEMENT OFFICI
ALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.        \n\nUNAUTHORIZED ACCES
S IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS."
banner enable
!
! End of WAAS configuration
WAELRG-1#
```

Appendix D—References

- Application Networking Services documentation—
  http://www.cisco.com/en/US/products/hw/contnetw/tsd_products_support_category_home.html

Appendix E—Troubleshooting

Troubleshooting Configuration

WAE Commands

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Connections:   Total (cumulative): 41038   Active: 2

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

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

Router Commands

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

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

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

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

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

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

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

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

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

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

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

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

Appendix F—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 4–7 performance (16 Gpbs and 345,000 connections per second) to optimize application performance and provide scalability. For more information on the ACE service module see the following URL: http://www.cisco.com/en/US/products/ps6906/index.html
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, and 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. For more information on the FWSM service module, see the following URL: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
Cisco Wide Area Application Engine (WAE)	The Cisco Wide Area Application Engine (WAE) platforms are a portfolio of powerful, scalable network appliances that host WAN optimization and application acceleration solutions that enable store server consolidation, performance improvements for centralized applications, and 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.

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.