



Cisco Distributed Research and Development Solution Deployment Guide for PTC Windchill

Cisco Validated Design

February 20, 2009

Contents

Solution Overview	4
Product Lifecycle Management Applications	5
Solution Benefits	6
Scope of the Solution	7
Solution Features	7
Solution Architecture	9
Solution Framework	9
Application Layer	9
Core Common Services Layer	10
Physical Infrastructure	10
Solution Use Cases	11
User Types	11
Locations	12
Solution Components	13
PTC-Windchill Application Overview	13
Windchill Multi-Tier Architecture	14
Content Storage: Remote File Servers and Replication	15
Pro/ENGINEER Communication Protocols	16
Application Networking Services	17
WAAS Features and Design	18



Corporate Headquarters:

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

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

WAAS Mobile Features and Design	20
ACE Features and Design	22
Enterprise Data Center	24
Enterprise Branch/WAN	25
A Mobile/VPN Connected User	26
WAAS Implementation and Configuration	26
Implementation Overview	26
Network Topology	26
Scalability and Capacity Planning	28
High Availability	28
Configuration Task Lists	29
Central Manager	29
Data Center WCCP Interception	30
HTTP Acceleration	34
WAAS Implementation Caveats or Limitations	35
WAAS and ACE Compression	35
Troubleshooting Commands	35
Cisco WAE Commands	35
WCCP Router Commands	36
WAAS Mobile Implementation and Configuration	37
Network Topology	37
WAAS Mobile Server	38
Create a Client Distribution	39
WAAS Mobile Configuration for Pro/ENGINEER	41
WAAS Mobile Client Installation	42
Client Software Configuration	43
Cisco ASA Configuration	43
Cisco VPN Client	43
System Reports	44
ACE Implementation and Configuration	45
Network Topology	46
Features and Design Considerations	47
High Availability and Load Balancing Features	47
Configuration Task Lists	47
Catalyst 6500	47
Remote Management Access	49
Interfaces and Default Gateway	49
Redundant ACE Appliances	51
Real Server and Serverfarm	52

Session Persistence (Stickiness)	53
Health Monitoring	54
Layer 7 Load Balancing	55
ACE Compression	56
FlashForward Acceleration	57
ACE Implementation Caveats or Limitations	58
WAAS and ACE Compression	58
FlashForward	59
Troubleshooting Commands	60
Testing Results and Conclusions	60
Test Methodology	61
Pro/ENGINEER Testing	61
Application Test Results	61
WAN Simulation	62
HTTP Operations—WAAS	62
HTTP Content Operations—WAAS	65
Folder Browsing Operations —WAAS	67
Pro/ENGINEER Testing—WAAS	69
WAAS Mobile Test Results	71
HTTP Operations—WAAS Mobile	71
HTTP Content Operations—WAAS Mobile	71
Folder Operations—WAAS Mobile	72
Pro/ENGINEER—WAAS Mobile	73
Appendix A—Test Environment	75
Hardware and Software Releases	76
Appendix B—Reference Documents	78
Appendix C—Device Configurations	78
Cisco ACE Configurations	78
PLM Context	80
Cisco WAAS Configurations	82
Engineering Site WAE	82
Data Center WAE	83
Central Manager WAE	84
Catalyst Switches	85
Data Center Core Switch 1	85
Data Center Core Switch 2	87
Data Center Distribution Switch 1	89
Data Center Distribution Switch 2	93
Data Center Access Switch 1	97

Data Center Access Switch 2	98
Engineering Site Access Switch	99
Cisco ISR Routers	100
Branch Router	100
Data Center WAN Router	101
Internet Router 1	101
Internet Router 2	102
Cisco ASA	103
ASA for Remote VPN Users	103
Cisco Validated Design	105

Solution Overview

For many manufacturing companies, increasing the rate of innovation has become a top priority. Driven by demands from increasingly sophisticated customers, by growth in emerging markets that often require localized products, and the need to maintain a competitive edge, companies are looking for ways to develop new products faster. According to a recent study by Forrester, “*slow response to changing market conditions in today’s hyper-competitive environment places companies at a distinct disadvantage relative to competitors.*”

To address these issues, manufacturers are expanding their global research and development footprint both internally and through outsourced partners, committing additional resources to drive faster innovation. This enables them to accelerate time-to-market by adding resources, capturing local knowledge and talent, and minimizing the costs of development.

Successfully implementing a global product development organization, however, brings its own significant challenges, which must be addressed to gain the full benefits of a global design chain and achieve business objectives. One of the most important of these challenges is coordinating and synchronizing product development data and business processes. Managing innovation processes on a global basis requires consistent access to applications and data throughout the development process.

To enable these distributed and extended relationships, organizations are increasingly using product lifecycle management (PLM) applications across global locations to manage product development. By relying on the capabilities of PLM applications, manufacturers ensure that design activities are in synch, engineering processes remain consistent, and design and production teams are always working from the latest information.

However, delivering these large-scale applications and data to globally dispersed locations challenges manufacturers to optimize information sharing and availability while remaining cost-effective and secure. The Cisco Distributed Research and Development solution with Parametric Technology Corporation’s (PTC) Windchill PDMLink solution addresses this challenge by combining the power of Cisco’s Application Network Services (ANS) with proven Pro/ENGINEER CAD and Windchill PDMLink PLM applications from PTC. Based on this powerful technology, manufacturers are better able to capture the benefits of an expanded global research and development footprint through capabilities including:

- Improved management and visibility of the global product development process through consistent, reliable, highly available PLM capabilities.
- Improved productivity for engineers at global design centers and remote locations due to improved application performance and faster data transfers.

- Efficient deployment and operation through data center infrastructure and WAN bandwidth optimization
- Comprehensive security to protect the confidentiality of critical design data, applications, and infrastructure

The Cisco Distributed Research and Development solution with PTC's solutions improves visibility into the product development process, allowing manufacturers to become more efficient and accelerate product development and lifecycle management based on consistent access to information and applications. Based on such capabilities, manufacturers can streamline product lifecycle management functions to achieve a competitive edge and greater profitability.

Product Lifecycle Management Applications

Product lifecycle management is the process of overseeing the entire lifecycle of a product from its conception through design, manufacture, and service. PLM applications help manufacturers to create and manage engineering information, implement changes, support communication and collaboration between distributed teams, and automate and control consistent processes across the distributed global development teams. Such applications help reduce time to market, improve product quality, lower prototyping costs, repurpose data for greater efficiency, and reduce waste.

However, the success of deployments can vary. Many companies choose to centralize their data and applications as part of the installation, which can help them to achieve significant savings, improved security, and more flexible deployments. However, centralization can also result in slower application performance issues for engineers in remote design centers and even slower performance for remote and mobile personnel. This in turn lowers adoption of the application, making PLM deployments less effective. Common problems with global infrastructures include:

- **Network performance**— Limited WAN bandwidth negatively affects end-user productivity for global users of centralized PLM applications. In addition, PLM applications handle large volumes of content data that may be demanding on these distributed networks. This can be a time-consuming portion of the user experience and require significant bandwidth. PLM applications address this through the use of their own replication technologies as an attempt to offset those effects, but network bandwidth limitations can still make data availability a challenge for some manufacturers with distributed design practices.
- **Application availability**—Increasing business dependence on fewer but large applications deployed in a central location requires a more careful examination of combined network and application architecture, including single points of failure and product stability, to achieve availability objectives.
- **Application security**—Keeping applications and data secure can be challenging in any environment. Extending access and distributing important data to global users and partners not only increases the complexity and potential security risks, but also increases the impact of security incidents.
- **Application infrastructure ownership costs**—The increasing complexity of applications and expanding geographic footprint requires a new approach to cost- effectively deliver the performance, availability, and security needed for globally dispersed users.

Solution Benefits

The Cisco Distributed Research and Development (DRD) solution with PTC significantly improves the performance of the Windchill PLM application and Pro/ENGINEER CAD data transfers over a wide area network (WAN). This allows companies deploying these applications to achieve the benefits of centralized application performance, including lower deployment and operational costs, quicker deployment times, and increased flexibility. The solution also optimizes data center resources for centralized Windchill PLM deployments through capabilities such as load balancing and application health monitoring.

The combination of optimized application performance and data transfers across a WAN along with data center infrastructure optimization enables manufacturers to derive significant benefits, including the following:

- Improved productivity and increased data sharing between global teams in various remote locations through accelerated application performance across the WAN
- Increased availability of information and PLM applications through the use of load balancing, failover switching, and other advanced capabilities
- Reduced costs of deployment due to server and data replication avoidance, services offload, virtualized services, and multiple form factors
- Reduced costs, with fewer remote servers and applications, transparent network integration, and reduced maintenance and management costs
- Complete security for mission-critical product development projects by maintaining centralized deployments in highly secure data centers

Table 1 shows a summary of the test results obtained for WAAS and WAAS Mobile and the level of improvement experienced in the lab testing. The [“Testing Results and Conclusions” section on page 60](#) explains in detail how these results were obtained.

Table 1 **Summary Test Results**

WAAS		
	Improvement Range	x Times Faster
HTTP Operations	8% to 92%	6
HTTP Content Operations	69% to 99%	41
Folder Browsing Testing	33 to 90%	5
Pro/ENGINEER Operations	90 to 92%	11
WAAS Mobile		
HTTP Operations	20% to 90%	4
HTTP Content Operations	64% to 100%	95
Folder Browsing Testing	47% to 90%	5
Pro/ENGINEER Operations	91% to 97%	25

Scope of the Solution

The Cisco DRD solution with PTC is based on the Cisco Application Networking Services (ANS) solutions, including the Cisco Wide Area Application Services (WAAS) and Application Control Engine (ACE) product families. The applications from PTC, specifically Windchill PDMLink Version 9.0 and Pro/ENGINEER Wildfire 3, were tested along with the Cisco ANS products to determine the optimal architecture and product configurations and to validate the potential performance improvements. The testing performed for this solution did not include every scenario or application function, but focused on a range of scenarios, use cases, and application functions that were considered to be representative of common deployment scenarios.

The primary application functions included a number of different browser-based transactions using PTC Windchill 9.0, various document upload and download scenarios using the Microsoft® Internet Explorer. Various Pro/ENGINEER workspace operations and data transfers were also performed. These functions were baselined using a standard LAN configuration and comparison tested with remote engineering centers (based on Cisco's branch architecture) with different WAN configurations and for a remote user with the WAAS Mobile client. Testing was also completed to validate the data center architecture for this solution, using the Cisco ACE for data center optimization and application performance improvements in an asymmetric deployment scenario (i.e., when WAAS is not deployed in the remote engineering center or for the remote user).

The solution did not focus on scalability testing with a large number of users or remote locations. For more information on the scalability of the key components, refer to the *WAAS Enterprise Data Center Wide Area Application Services (WAAS) Design Guide* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/WAASDC11.html

Solution Features

The Cisco DRD solution with PTC's Windchill PDMLink product builds on existing Cisco architectures and solutions with a recommended Windchill deployment configuration from PTC. The Application Networking Services (ANS) products used in the Cisco DRD solution were deployed on the Cisco branch, WAN, and data center architectures. These architectures offer a foundation that provides consistent, high performance networking services and capabilities and have been tested, validated, and documented as part of the Cisco validated design(CVD) program.

The specific Cisco ANS products used in the Cisco DRD solution include the following:

- Cisco Application Control Engine (ACE) 4710 appliance
- Cisco Wide Area Application Engine (WAE) appliance
- Cisco Wide Area Application Services (WAAS) Mobile server and client software

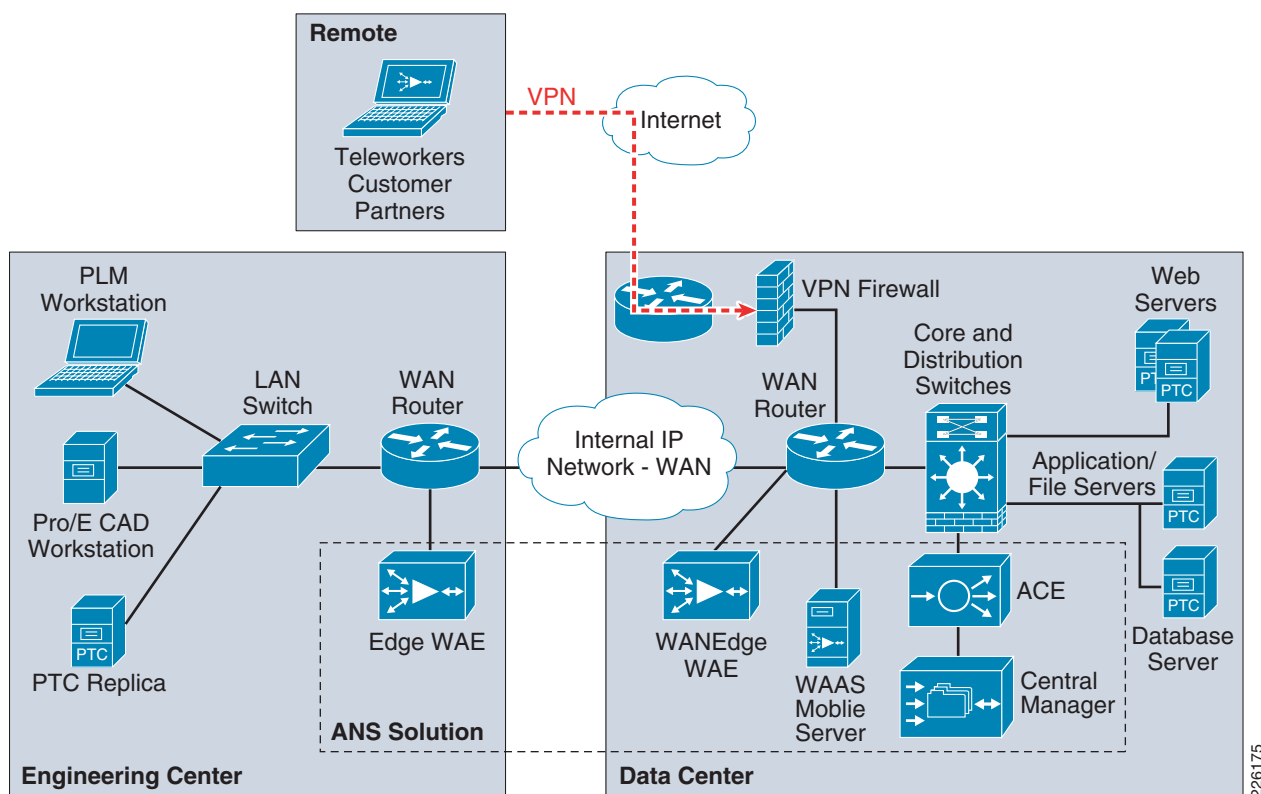
The overall solution architecture was then validated using PTC Windchill PDMLink 9.0 and Pro/ENGINEER Wildfire 3 for the testing scenarios described in this document. The PTC Windchill PDMLink application is one of the leading products in the market for creating, controlling, collaborating, communicating, and configuring engineering data. It offers a range of information management capabilities on an integrated, web-based architecture that supports the globally distributed environment. Modular in design for greater reliability and extensibility, it shares a single database business object and process model, and is used through a consistent and unified web-based user interface. Integral with Windchill PDMLink is the Pro/ENGINEER Wildfire CAD package which provides integrated, parametric, and 3D capabilities for product design and development.

The DRD solution consists of a set of network capabilities that allow manufacturers to take advantage of the solution benefits. These capabilities include the following:

- The Cisco ANS enabling reliable, accelerated and secure application delivery to users around the world, including:
 - Cisco WAAS-enable seamless access over the WAN to centrally hosted applications, storage, and rich media.
 - Cisco WAAS Mobile which extends Cisco WAAS application acceleration benefits to mobile employees.
 - Cisco ACE delivers virtualized application services providing security, acceleration, availability, message mediation, and switching with dedicated engines for messages and advanced applications.
- An enterprise data center network environment based upon a layered design to improve scalability, performance, flexibility, resiliency, and maintenance.
- A Branch-WAN network to securely and reliably deliver the same enterprise applications and collaboration capabilities to remote engineering locations.
- A Mobile/VPN connected user to securely and reliably deliver the same enterprise applications and collaboration capabilities to remote and mobile engineers.

The Cisco DRD solution overview shown in [Figure 1](#) depicts these capabilities and how they integrate to form a complete, end-to-end solution.

Figure 1 *Distributed Research and Development Solution*



226175

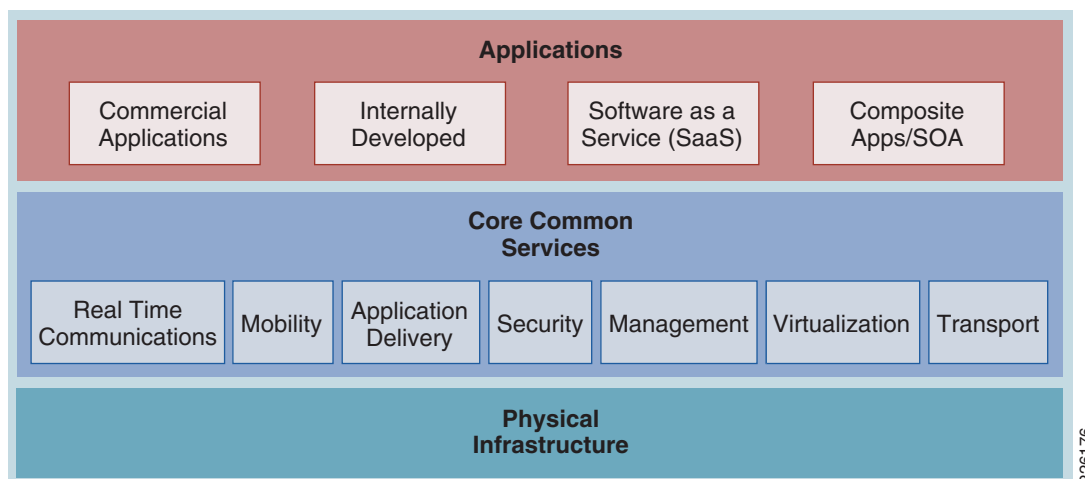
Windchill PDMLink is configured in a standard multi-tier configuration consisting of a pair of web servers and an application server with a corresponding database server. The DRD solution did not focus on testing a fully redundant configuration. The web servers were configured in a load-balanced configuration to demonstrate the ACE load balancing capabilities during the solution testing. While a remote replication server is available for remote environments, the solution only focused on accessing content from the central data center.

Solution Architecture

Solution Framework

The Cisco Services-Oriented Network Architecture (SONA) framework provides a standard paradigm for designing current and next generation solutions that link network-based services with enterprise applications to drive business results. The SONA framework shown in [Figure 2](#) illustrates the components of the solution from the infrastructure providing network-based services and the applications that use them.

Figure 2 **The SONA Framework**



Application Layer

The top layer of the SONA framework includes the applications that are part of the Distributed Research and Development (DRD) solution. The SONA framework identifies commercial products, applications developed internally, or sourced externally (software as a service) or a combination of types in the form of a composite, mash-up, or SOA applications. The DRD solution focuses on PLM applications that are typically commercial products versus any of the other application types. This deployment guide focuses on PTC's Windchill PDMLink and Pro/ENGINEER Wildfire applications.

Core Common Services Layer

The primary layer of the SONA framework provides common network-based services for security, mobility, real-time communications, application delivery, management, virtualization, and transport. Common services that are shared across the network increases operational efficiency and compliance requirements of the entire system. The SONA framework outlines the following services:

- Real-time communication services offer session and media management capabilities, contact center services, and presence functions.
- Mobility services provide location information and device dependent functionality.
- Application delivery services use application awareness to optimize performance.
- Security services help protect the infrastructure, data, and application layers from constantly evolving threats, and also offer access control and identity functions.
- Management services offer configuration and reporting capabilities.
- Virtualization services deliver abstraction between physical and functional elements in the infrastructure, allowing for more flexible and reliable service operation and management.
- Transport services help with resource allocation and deliver on the overall quality-of-service (QoS) requirements of the application, as well as routing and topology functions.

The DRD solution focuses on the use of the application delivery services to the PLM applications. The solution assumes the existence of transport (for example, WAN and LAN) and security services in the various locations and only considers how the application delivery services integrate into these functions. The solution also considers the management aspects of the application delivery services. The other services listed are not a focus or particular consideration for the solution, but may provide other value or service to the PLM applications.

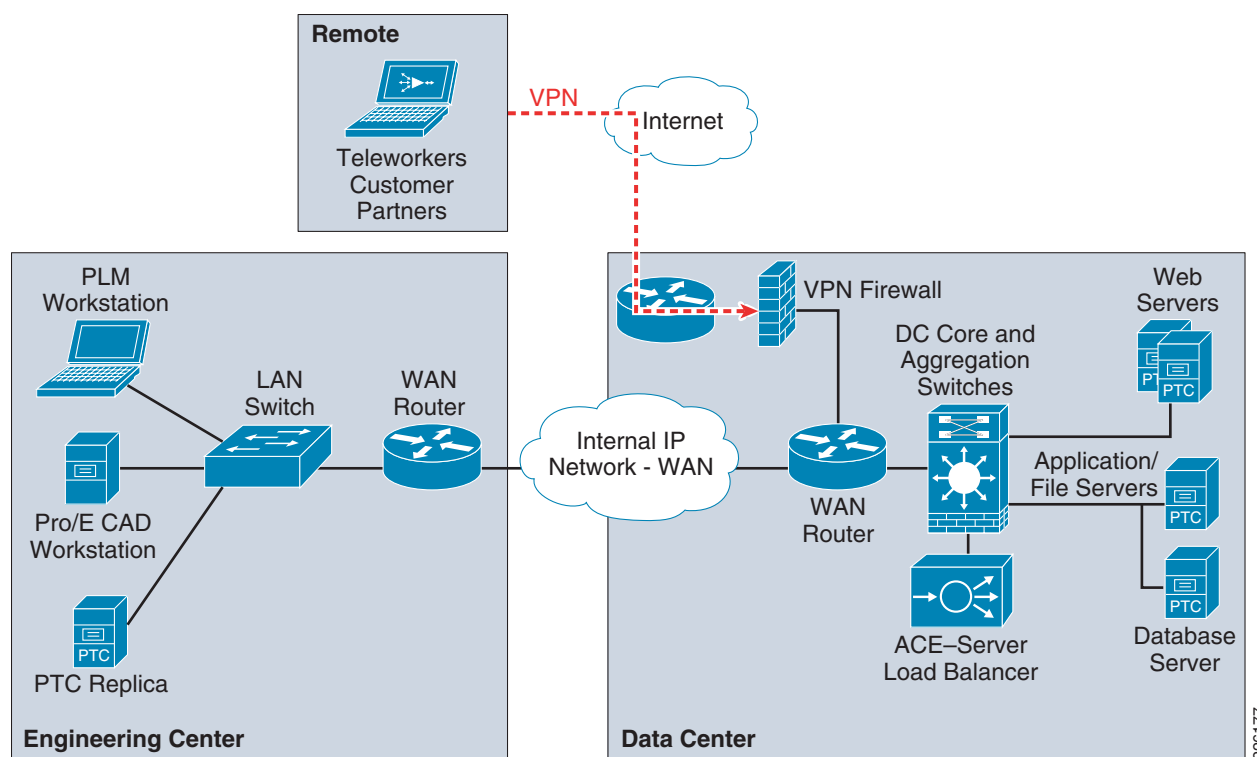
Physical Infrastructure

The foundation layer of the SONA framework covers the various network locations and network resources that internal, partner, and customer users may access as part of the DRD solution. This solution uses the following places in the network (PINs), shown in [Figure 3](#):

- A remote engineering branch where a significant number of engineers reside.
- A centralized data center housing the PLM applications servers, database and core components.
- Wide area networks (WANs) connecting branches to the data center.
- Remote engineers accessing the enterprise network via an encrypted internet connection.

These PINs outline a wide variety of network infrastructure options to support a location. This solution assumes that these solutions are in place, but does not explain them in detail.

Figure 3 *Places in the Network*



Solution Use Cases

The solution use cases describe how the users benefit from the DRD solution. The use cases are the key scenarios where the functional requirements are defined. The DRD solution and pertinent testing to support the solution were designed around these use cases. For this solution, PLM users and engineers or designers were simulated in two types of locations: distributed engineering centers on the enterprise WAN and remote users through a secure Internet connection.

User Types

PLM Users

PLM users rely on the product management features of the application. These users may be engineers, but may also be product managers, designers, management, or other people involved in the product lifecycle. They typically access the PTC Windchill with a web browser.

Engineers or Designers

Engineers typically use more advanced design and engineering features of the PLM solution. Pro/ENGINEER Wildfire 3 provides access to Windchill PDMLink through an embedded browser. One of the main features used involves downloading large engineering files to be worked on locally and uploading those changes when work is complete.

Locations

Distributed Engineering Centers

Since engineering centers and resources can be distributed around the globe, limited bandwidth and overall network latency may have a negative impact on application performance. The number of remote engineers also has an impact on the network and application designs.

PTC offers replication services designed to reduce the time required to upload and download files at remote locations to improve application performance for content operations that would otherwise consume bandwidth and add a significant burden of time to the end users daily responsibilities.

The focus of this solution is to improve the performance of the replication transfers and reduce the network bandwidth used by accelerating the associated traffic between the end users and the data center. PTC recommends the use of remote file servers for replication purposes for customers managing CAD data of remote sites. For customers that manage very small data sets or single files such as Microsoft office documents can use the benefits of WAAS without replication services. A remote file server reduces the overall footprint for accessing content not yet available at the remote site and reduces bandwidth consumption during application accesses, content transfers, etc.

The test results presented in this guide can also be extended to the replication services offered by PTC since the replication relies on similar protocols and requirements as the client application.

Since WAN bandwidth and latency have a significant impact on application performance, the tests were performed with different types of WAN connectivity for the distributed engineering centers.

The size of the engineering center impacts the decision to deploy a key component of the solution, the Cisco WAAS platform. That decision is typically based on the following:

- The number and type of users that will benefit from the application acceleration
- The reduction in network bandwidth used by the application acceleration
- The cost of deployment and operations
- The volume and size of content to be transferred regularly
- The current amount of available bandwidth and latency

The solution recognizes that, even without the deployment of the WAAS services, the solution provides some application acceleration for small engineering centers due to the deployment of the ACE in the data center as explained in the [“Testing Results and Conclusions” section on page 60](#).

Remote Users

While manufacturers try to concentrate users at remote engineering centers, other users may need to access the PLM applications while external to the enterprise network. These users may be home office employees, employees that are working as a contractor at a remote customer facility, or even remote contractor resources.

This solution supports accelerating the access of the PLM and engineering applications from external, Internet-based remote locations. This use case is supported by the deployment of the Cisco WAAS Mobile application. The solution assumes that the remote user has enterprise network access through a secure virtual private network (VPN) connection.

Solution Components

The DRD solution includes networking technology that takes full advantage of application delivery features to optimize the PTC applications. The main components of the DRD solution include the following:

- PTC's Windchill PDMLink 9.0 and Pro/ENGINEER Wildfire 3 applications
- Cisco ANS, including the following:
 - Cisco WAAS Version 4.1.1
 - Cisco WAAS Mobile Version 3.3.4
 - Cisco ACE Version A3(1.0)
- An enterprise data center network
- A branch WAN
- A Mobile VPN connected user

PTC-Windchill Application Overview

The Windchill architecture is a production-proven set of integral, modular solutions for rapid distributed collaborative development of customer driven products. Windchill was the first and remains the only proven PLM solution with the purest and most sophisticated architecture that is integral, pure Internet, and interoperable.

Integral

- Modular solutions sharing a common database schema, business object, and process model
- Consistent web-based user interface
- Provides customization to customer-specific needs

Pure Internet

- 100 percent web-based anytime, anywhere team management and information access across intranet/extranet deployments
- Written 100 percent in Java with the broadest and most sophisticated support of J2EE and internet standards
- Integrates with existing IT, Internet, and security infrastructure
- Support high scalability and availability, without redundant infrastructure layers
- Industry-standard J2EE, Internet, and web-services interfaces

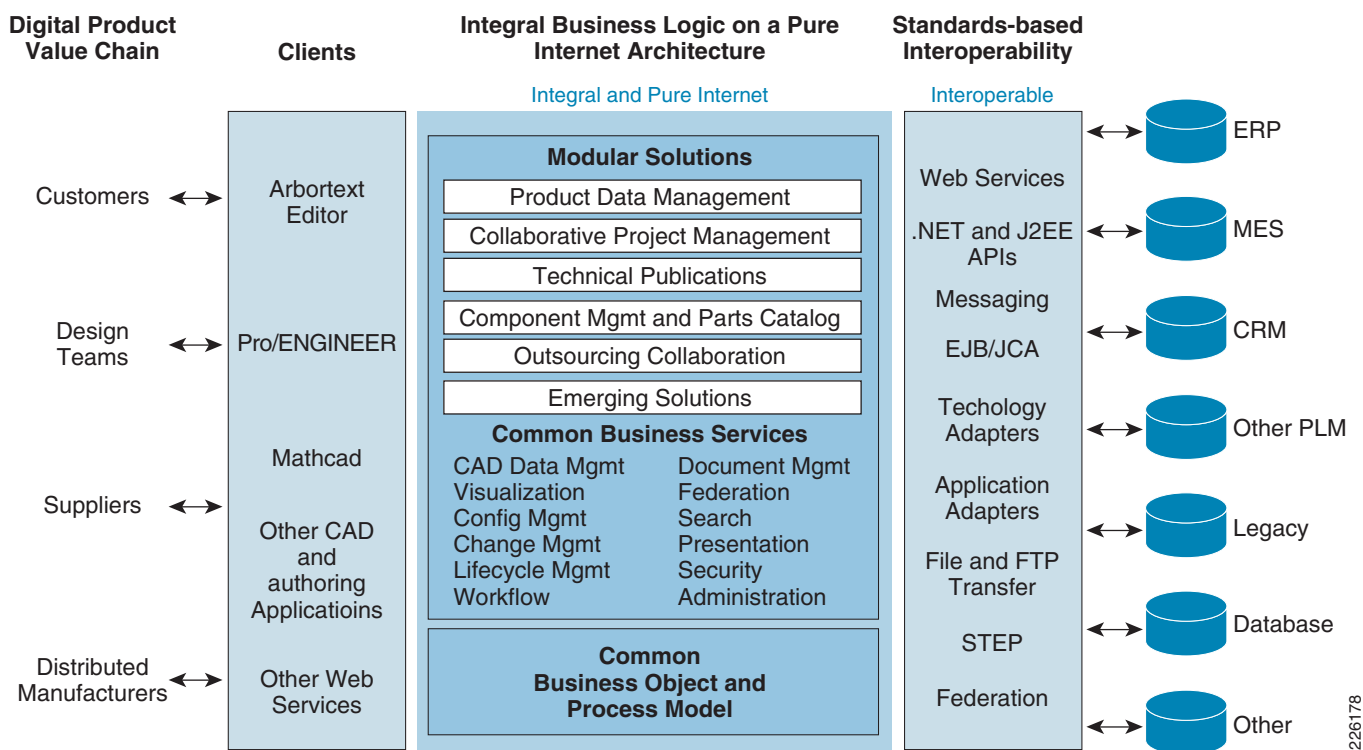
Interoperable

- Seamless interoperability with heterogeneous CAD systems
- Powerful federation for maintaining data with other systems
- Standards-based integration with commercial EAI vendors and turnkey process integration with Tibco

- Full web services connectivity with Pro/ENGINEER Wildfire and Microsoft .NET web-service applications

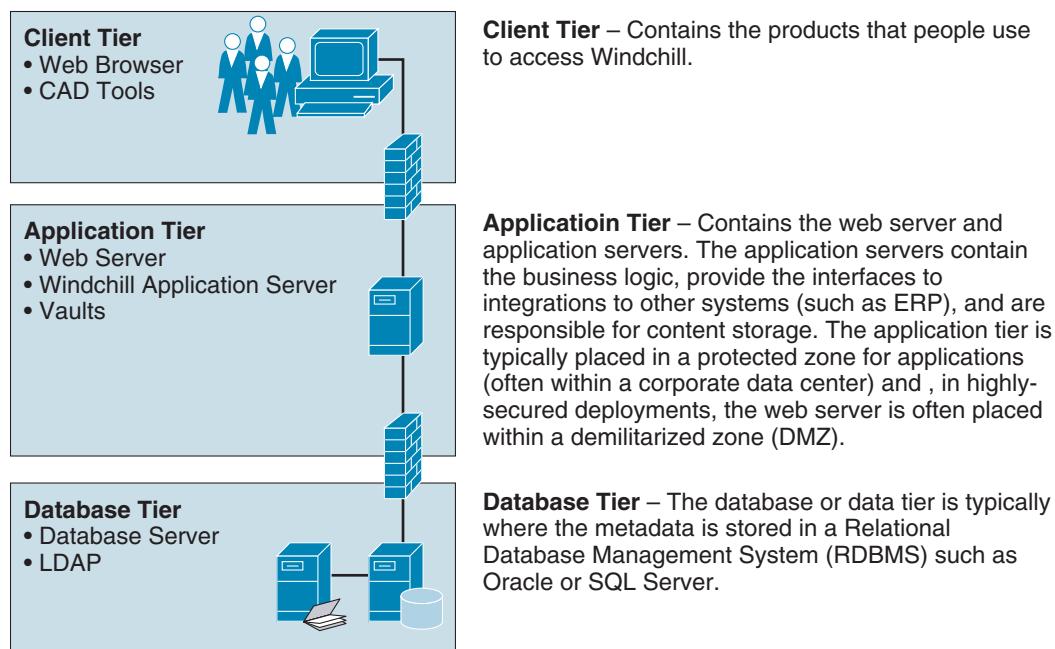
Figure 4 shows an overview of the Windchill architecture. The left-hand side of the diagram shows the various methods available for users to interact with the system. The middle portion of Figure 4 shows the foundation of the Windchill integral architecture, and the far-right side illustrates types of systems that can be easily integrated using the Windchill standards-based interoperability features.

Figure 4 *Windchill Architecture Overview*



Windchill Multi-Tier Architecture

Windchill is a multi-tier architecture that can be deployed in a configuration small enough to run on a single server (for small workgroup teams), as well as in a configuration as large and complex as a highly redundant clustered system serving thousands of end users on a global scale. The architecture is commonly represented as three tiers as shown in Figure 5.

Figure 5 Windchill Multi-tier Architecture

The Windchill multi-tier architecture offers the flexibility and options to be deployed with an infrastructure that can support the most demanding distributed collaborative product development processes. This architecture can support users from various departments within the company, as well as users from supplier, manufacturing partner, and customer communities.

The core components of the Windchill runtime architecture reside in the application and database tiers:

- Web servers to provide access to the application through web browsers or through web-enabled applications. The web-server hosts static content and provides access to dynamic content delivered by the application server. Two or more web servers can be configured behind a content switch to provide additional redundancy
- The Windchill Application Server combines several components that work together to provide dynamic capabilities of the application. Some of these components include a Servlet Engine, a Server Manager, and a Method Server.
- A database server is required to store the application's pertinent metadata. Windchill is certified with both Oracle and Microsoft SQL.
- An LDAP directory service provides user and group administration and stores application-specific configuration information.

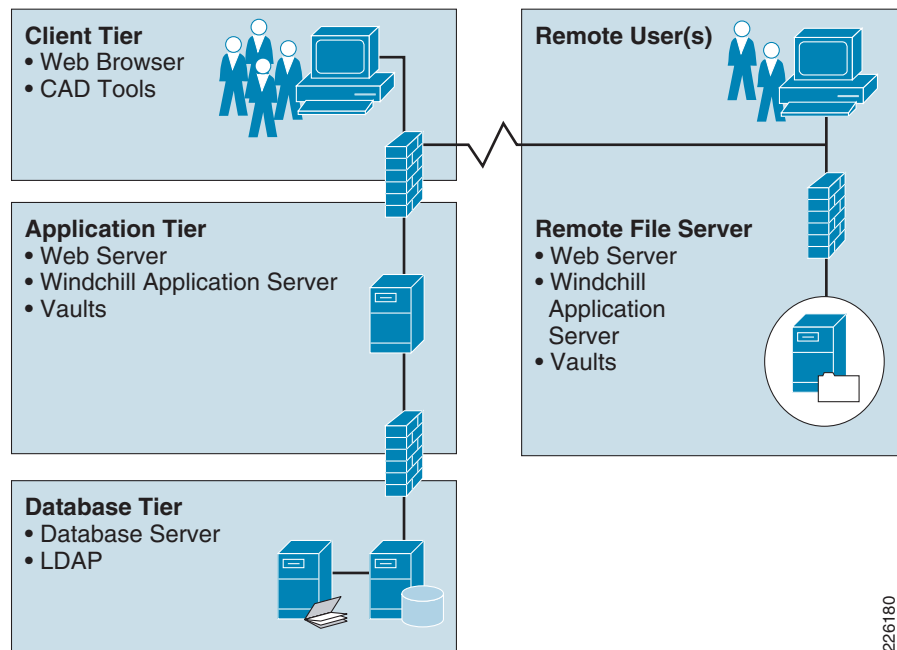
Content Storage: Remote File Servers and Replication

Customers often have users in multiple locations across the globe. To address performance concerns around uploading and downloading large amounts of content (such as CAD files) over a WAN, PTC provides the remote file server functionality. The remote file servers support the local upload and download of content at end user locations as well as the means to replicate data from location to location.

Replication is used to offset multiple downloads of the same data and reduce consumption of valuable WAN resources while providing a near LAN-like experience to the end users for content handling. This allows all users of the system to access the same information globally while maintaining the level of performance that is demanded by remote users.

Figure 6 shows how the remote file servers are deployed at a remote location.

Figure 6 *Remote Replication Servers*

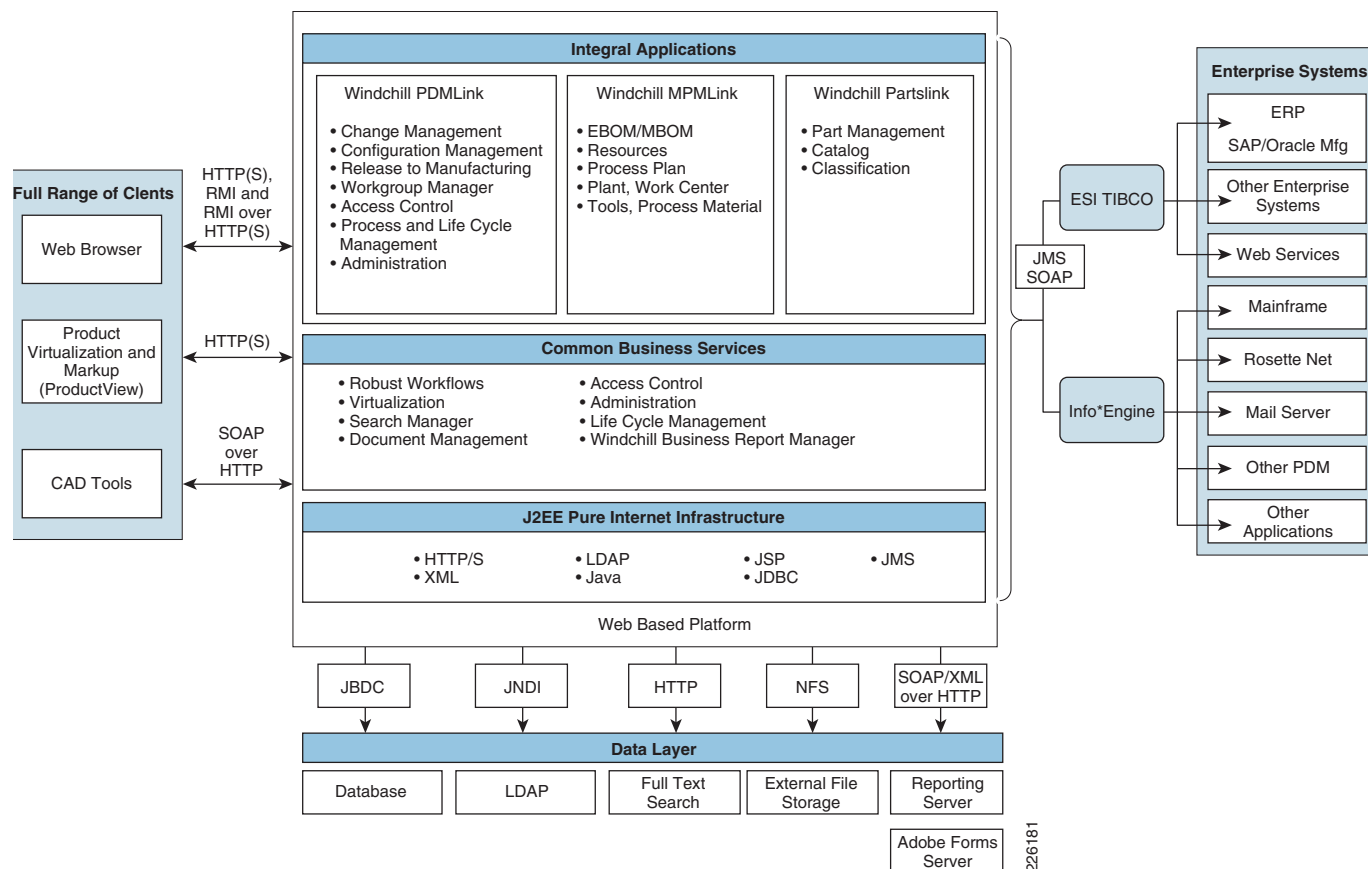


Pro/ENGINEER Communication Protocols

Windchill leverages web-based protocols for communication with clients. These protocols are primarily HTTP(S) over standard web ports. Clients are also able to interact with rich-client applications using RMI natively or they can be tunneled over HTTP(S). Other clients like Microsoft Office and the various Workgroup Managers support SOAP over HTTP communication with the servers.

Server-to-server and application-to-application communication uses a broader number of protocols and ports. Figure 7 illustrates the protocols and communication paths used within the Windchill architecture.

Figure 7 **Protocols and Communication Paths**



PTC's Windchill architecture is explained in further detail in the Windchill Architecture Overview available to current customers from PTC's Technical Support website:

<http://www.ptc.com/WCMS/files/83516/en/WindchillArchitectureOverview.pdf>

Prospective customers may obtain a copy by contacting a local PTC sales representative.

Application Networking Services

The Cisco ANS focuses on transforming the network infrastructure to improve application performance and availability while improving security and simplifying data center and branch infrastructures. The ANS products can be grouped into two functional families: application delivery and WAN optimization.

- Application delivery products ensure application availability in data centers and remote locations, including the Cisco ACE Appliance and the ACE Module.
- WAN optimization products focus on centralizing servers and storage in the data center and delivering on-demand local and branch services while maintaining LAN-like application performance. Products in this family include Cisco WAE appliances, Wide Area Application Engine network modules, and Wide Area Application Services module client software.

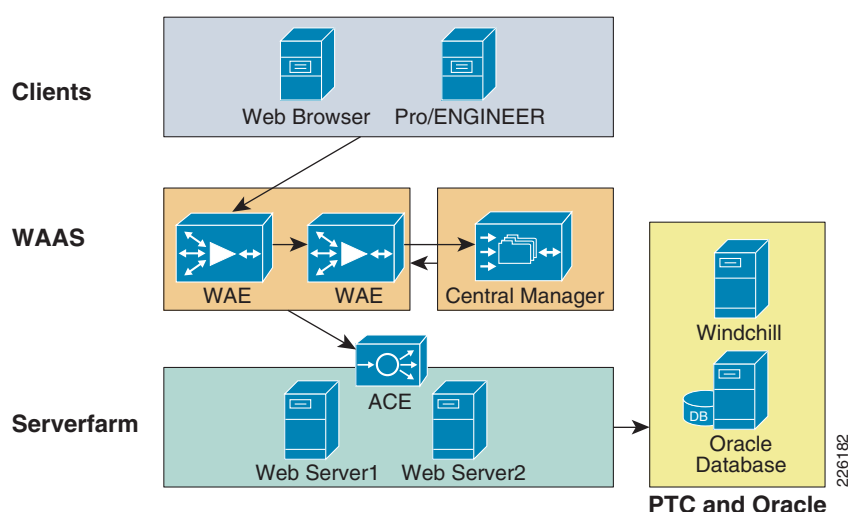
WAAS Features and Design

Cisco WAAS is a symmetric WAN optimization and application acceleration solution designed to improve the performance of applications over a WAN. Cisco WAAS can be deployed with a hardware device called the Cisco WAE deployed in each location or as a software solution called WAAS Mobile for VPN-connected users, or both.

The WAE can be either a standalone appliance or a router-integrated network module for the Cisco Integrated Services Router (ISR). This solution focused on testing the WAE appliances, but future versions may focus on the ISR network module.

By employing these performance-improving techniques, IT organizations are able to improve productivity, minimize WAN bandwidth consumption, and enable consolidation of costly and difficult-to-manage infrastructure such as servers, storage, and data protection hardware.

Figure 8 **WAAS Design**



The WAAS appliance-based architecture consists of the following hardware components, as shown in Figure 8:

- Cisco WAEs—Resides within the campus/data center or the branch. The WAE placed at the data center provides TCP optimization and caching proxy for the origin servers. The WAE placed at the branch provides the main TCP optimization and caching proxy for branch clients.
- WAAS Central Manager (CM)—Provides a unified management control over all the WAEs. The WAAS CM usually resides within the data center, although it can be at other locations, as long as it is able to communicate with the managed WAEs.

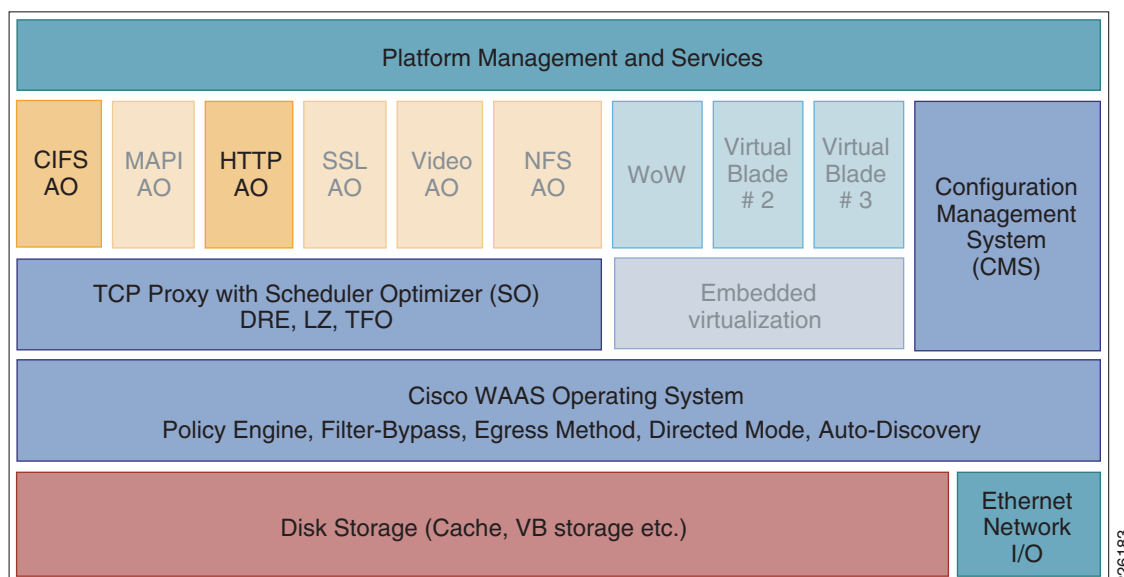
Cisco WAAS uses the following optimization techniques:

- Application acceleration—Refers to examination of user-to-server application message exchanges to identify ways of improving the performance of applications over the WAN. This involves read-ahead mechanisms, write-behind mechanisms, object caching, and pre-positioning.
- Data Redundancy Elimination (DRE)—DRE is a compression technology that examines TCP streams to build a compression history. As new data is identified, the new data is added to the compression history. As redundant data is identified, it is removed from the TCP stream and replaced with a small signature that tells the peer WAE what data to reinsert. DRE can commonly provide up to 95 percent or higher levels of compression on WAN links while ensuring consistency of messages and data.

- Persistent Lempel-Ziv Compression (PLZ)—PLZ is a compression algorithm that is effective on TCP stream data that has not been identified as redundant by DRE. PLZ is an adaptation of a traditional LZ compression algorithm, yet uses a longer persistent compression history, thereby allowing for potentially higher levels of compression. PLZ can generally provide 20%-80% compression depending on datasets and history.
- Transport Flow Optimization (TFO)—TFO is an optimized implementation of TCP that is used for connections that are being optimized by Cisco WAAS. TFO helps prevent WAN conditions from impacting end-node TCP behavior (such as packet loss and retransmissions) as part of its TCP proxy architecture. TFO provides the following optimizations:
 - Bandwidth scalability (fill the available pipe when safe to do so)
 - Loss mitigation (selective acknowledgement and adaptive congestion avoidance)
 - Slow-start mitigation (large initial windows)

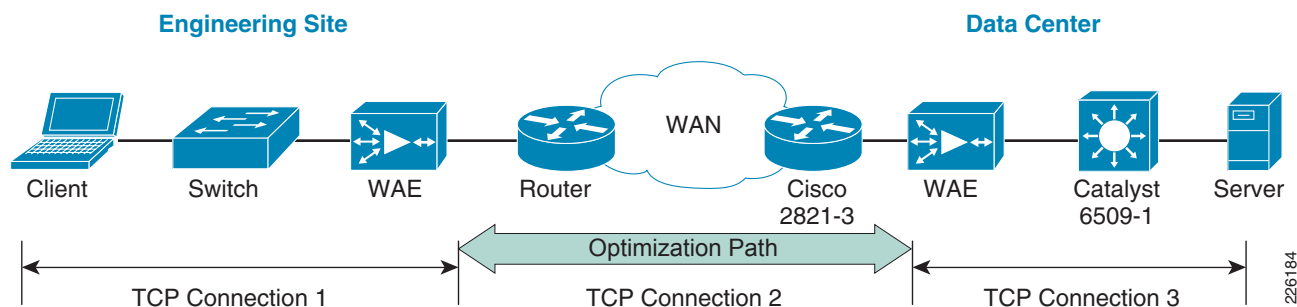
Figure 9 shows the Cisco WAAS product architecture features. The faded features provide significant benefits for many customer implementations, but were not tested in this solution.

Figure 9 **WAAS Architecture**



WAAS Optimization Path

Optimizations are performed between the core and edge WAE. The WAEs act as a TCP proxy for both clients and their origin servers within the data center. Other WAN optimization solutions create optimization tunnels, and the TCP header is modified between the caching appliances. With WAAS, the TCP headers are fully preserved. Figure 10 shows the three TCP connections used by WAAS.

Figure 10 **WAAS Optimization Path**

The optimization path between the two WAEs is used by the WAAS to optimize the transfer of data over the WAN connection, minimizing the data sent or received. WAAS optimization mechanism such as TFO, DRE, and LZ compression are also included in the optimization path.

Cisco WAAS relies on some form of network interception to integrate into the network and receive packets from flows that are to be optimized. This design guide focuses on the following methods of network interception:

- **Physical inline interception**—The Cisco WAE appliance is deployed physically between two network devices, most commonly between a router and a switch at the remote engineering office. This allows all traffic traversing the network toward the WAN or returning from the WAN to physically pass through the WAE, thereby giving it the opportunity to optimize traffic flows. Physical inline can be used in any type of location (branch office, regional office, and data center), but is commonly used for branch office implementations. A WAE provides fail-to-wire capabilities in case of power, hardware, or software failures.
- **Web Cache Communication Protocol version 2 (WCCPv2)**—Provides an off-path but virtually in-line deployment. With WCCPv2, WAE devices are deployed as appliances (nodes on the network and not physically in-line) on the network. WCCPv2 provides scalability to 32 WAE devices in a service group, load-balancing amongst WAEs, fail-through operation if all WAEs are unavailable, and allows the administrator to dynamically add or remove WAE devices to the cluster with little to no disruption.

WAAS Mobile Features and Design

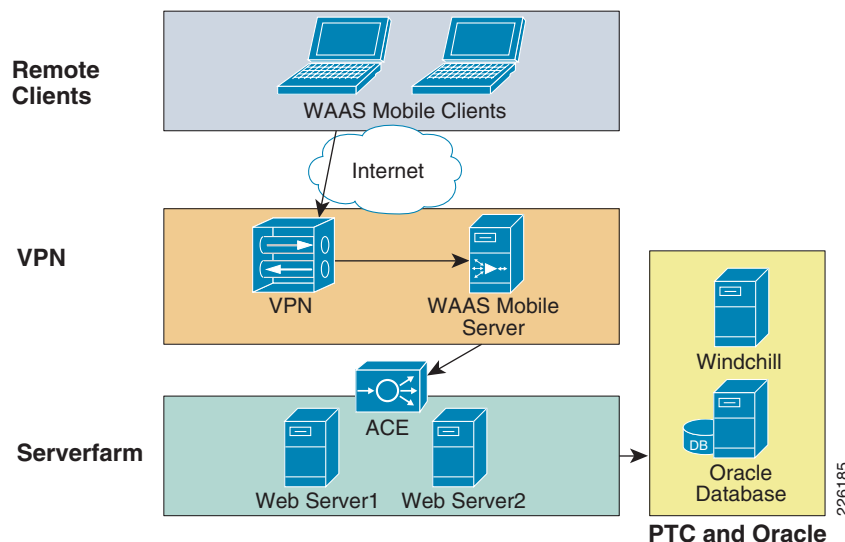
Cisco WAAS Mobile is a software solution that extends Cisco WAAS application acceleration benefits to any employee regardless of location. Cisco WAAS Mobile is a purpose-built, ready to use software solution consisting of client software for end users and software deployed on servers near existing VPN concentrators.

Cisco WAAS Mobile achieves industry-leading performance by extending Cisco WAAS acceleration technologies including:

- Advanced data transfer reduction using compression and bi-directional, cross-protocol byte caching.
- Application-specific acceleration for web-based applications, Microsoft Exchange, and Windows file servers applications.
- Transport optimization to handle the timing variations found in packet switched networks, the bandwidth and latency problems of broadband satellite links, and noisy Wi-Fi and DSL connections.

As shown in Figure 11, the Cisco WAAS Mobile software solution consists of client software for end users and server software deployed near existing VPN concentrators to extend the Cisco WAAS deployment.

Figure 11 **WAAS Mobile**



The client-side software is transparent and requires no user maintenance or local configuration changes:

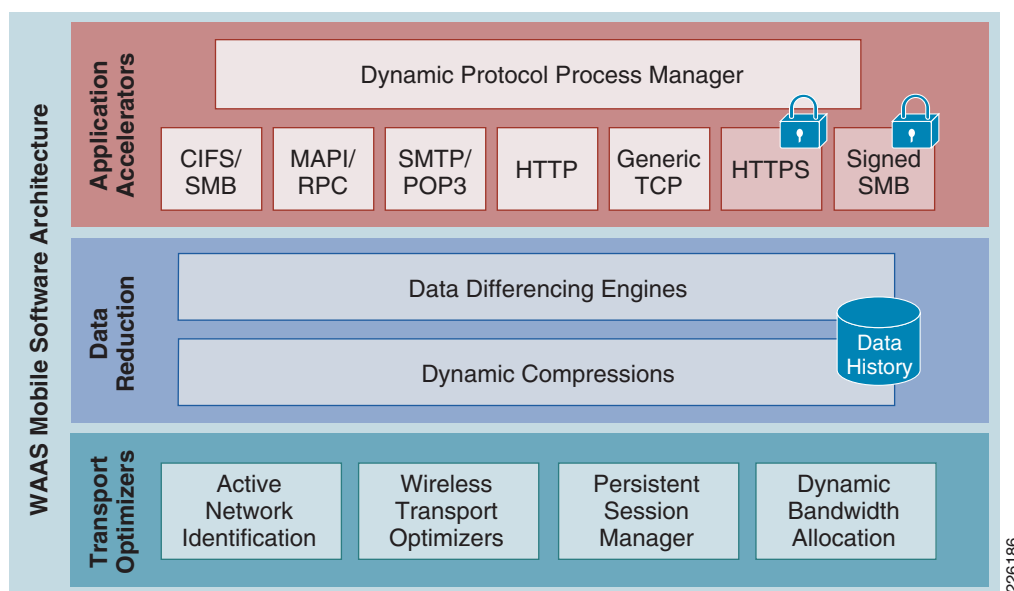
- Remote client configuration and installation—The Cisco WAAS Mobile client configuration is established by the system administrator, and the client software image can be loaded directly to remote devices using standard software distribution products.
- End-user self-installation—Although the Cisco WAAS Mobile client software can be installed and some configuration can be delegated to the end user, standard enterprise configurations can be used to help ensure that the client software is operational without any user interaction.
- No reconfiguration of applications—Cisco WAAS Mobile redirects data transparently to help ensure that no configuration changes are required for any application.
- No requirement to open incoming ports on client firewall or other local security software—Existing desktop security is fully preserved.
- Auto-detection of high-speed networks—Auto-detection allows users to automatically transition to the office network.

The server-side software also provides an easy deployment:

- No changes are required to the application or file servers.
- No changes are required in network resources such as routers, switches, and WAN accelerators.
- No changes to IP network topologies are required because the traffic is directed to the Cisco WAAS Mobile server through the client software.
- In the event of a server failure, the only effect is loss of optimization, not loss of connectivity.
- Cisco WAAS Mobile is fully compatible with standard load-balancing solutions such as the Cisco ACE for high-availability configurations.
- Cisco WAAS Mobile can be deployed with or without a Cisco WAE device, which provides branch-office user acceleration, enabling flexible deployment in enterprise environments

Figure 12 shows the WAAS Mobile architecture.

Figure 12 WAAS Mobile Architecture



ACE Features and Design

The Cisco ACE product family (see Figure 13), a comprehensive application delivery solution, helps ensure application availability, accelerate application performance, and protect applications while simultaneously reducing data center costs. Benefits of the Cisco ACE family products include the following:

- **Application Availability**—The Cisco ACE helps ensure business continuity and the best service to end users by taking advantage of availability through highly scalable Layer 4 load balancing and Layer 7 content switching, and minimizes effects of application, device, or site failure by providing a failover system with an extensive set of application health probes.
- **Accelerated Application Performance**—Accelerates performance of PTC's applications by using acceleration technologies and delivers highly efficient data compression to speed up application response times and improve server performance. Technologies such as compression and FlashForward improve performance and reduce latency and data transfers for applications.
- **Comprehensive application security**—The Cisco ACE protects against application threats and denial-of-service (DoS) attacks with features such as deep packet inspection, network and protocol security, and highly scalable access control capabilities.
- **Virtualization**—Architecturally, a single physical ACE can function as multiple virtual ACE devices. Up to 250 virtual devices can be configured in a single Cisco ACE. These virtual devices are secured and isolated from each other. Each virtual device can be configured with unique settings to provide different features or address different applications.

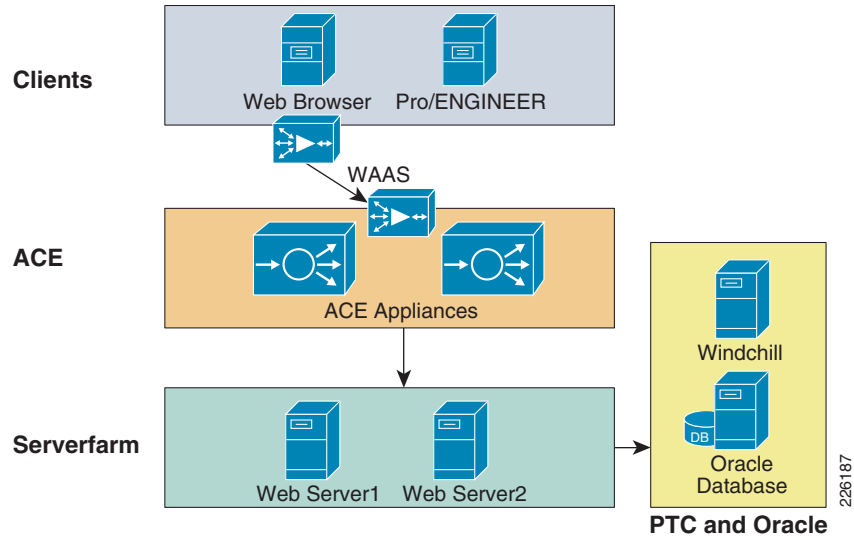
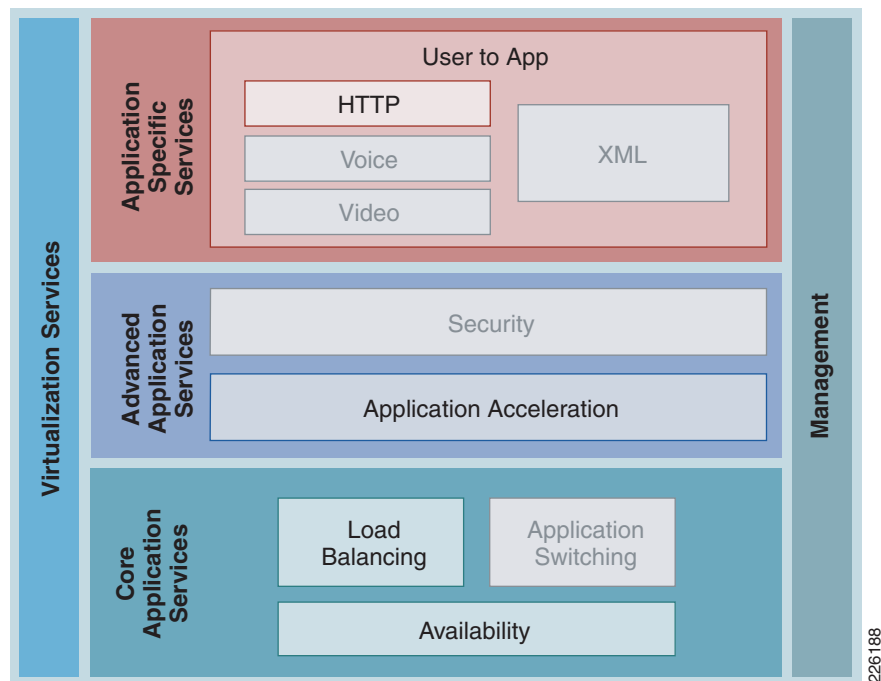
Figure 13 ACE Design

Figure 14 shows the ACE architecture and its key features. The features that were not tested in this solution are faded out in the diagram.

Figure 14 Cisco ACE Architecture

ACE Module vs. ACE 4710 Appliance

The Cisco ACE family of products includes highly scalable modules for the Cisco Catalyst 6500 Series Switches and standalone Cisco ACE 4710 appliances. Both products offer a full range of application delivery features, including Layer 4 and Layer 7 content switching as well as a set of application acceleration capabilities.

While both offer a similar feature set, the ACE module offers the highest performance in the market and supports up to 345,000 Layer 4 connection setups and teardowns per second, while the ACE 4710 supports up to 120,000 connections per second.

The ACE 4710 appliance software used for the solution guide includes unique acceleration features not available on the ACE module:

- Latency optimization, also known as FlashForward—FlashForward is a patented technology that enables the Cisco ACE 4710 appliance to eliminate unnecessary browser cache validation requests. This technology eliminates the network delays associated with embedded cacheable Web objects such as images, style sheets, and JavaScript files.
- Bandwidth optimization—Optimization includes hardware-accelerated GZIP and deflate compression and patented delta encoding. GZIP and deflate compression provide significant byte savings on transmitted files. The Cisco delta encoding technology enables the Cisco ACE 4710 appliance to send only the difference (or deltas) between a previous and new instance of a web page.

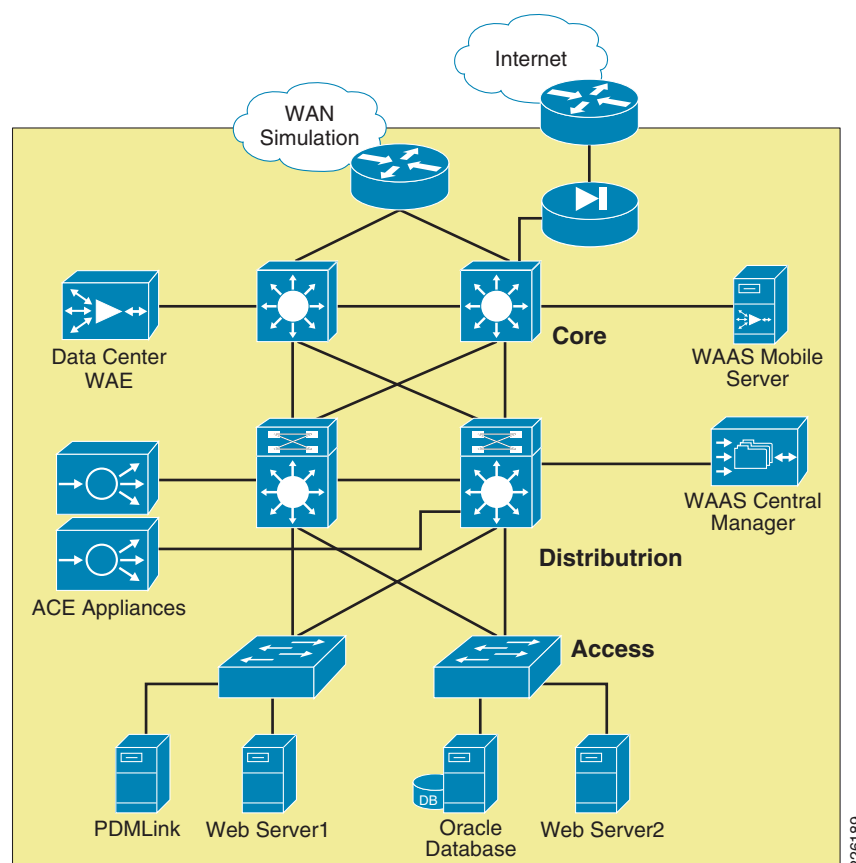
Since this solution focused on performance optimization and not in testing a large number of sessions, the test environment relied on the Cisco ACE 4710 appliances. This also allowed for testing the unique acceleration features of the appliance.

Enterprise Data Center

The data center design is based on a proven layered model with core, distribution and access layers. The solution includes the following:

- WAN edge routers
- Cisco Catalyst switches in the core, distribution, and access layers
- Redundant ACEs
- Enterprise edge router and firewall for remote users access
- Application acceleration and off-load server processing (WAAS and ACE appliance)
- Management applications
- Tiered, segmented applications servers (web, application, and database)

The data center architecture was not tested for this deployment guide. The application and management servers used to support PTC Windchill were incorporated in the testing of this solution. A data center environment similar to the one shown in [Figure 15](#) was configured to demonstrate the architecture and benefits of WAAS and ACE.

Figure 15 Data Center Infrastructure

Enterprise Branch/WAN

In order to provide services to distributed engineering resources, a branch WAN solution must be in place. The enterprise branch solution outlines a wide range of networking services for branch operations, including the following:

- Application acceleration
- IP communications (for example, voice)
- LAN
- WAN connectivity
- Security
- Network management

This solution does not focus or test the following features since they are sufficiently described in other branch WAN design guides. Information on the following topics can be found at the Cisco design zone website <http://www.cisco.com/go/designzone>.

- Wireless access
- Voice or video traffic
- Branch security

- Branch high availability
- Large branch design with an specific aggregation switches
- Various WAN interconnectivity technologies, including Internet or MPLS as the WAN interconnect

A Mobile/VPN Connected User

In order to provide services to mobile and single instance remote users who are not located in branch offices, a mobile VPN solution must be provided. The mobile VPN solution assumes an underlying infrastructure for VPN access into the enterprise network and the solution provides for application acceleration.

The DRD solution does not focus on or describe remote access solutions for the VPN as that topic is well covered in other guides that can be found at the Cisco design zone website <http://www.cisco.com/go/designzone>.

WAAS Implementation and Configuration

The following sections discuss the test configuration steps for Cisco WAAS, WAAS Mobile, and ACE used in the solution.

Implementation Overview

By default, Cisco WAAS accelerates web traffic (TCP port 80) and no additional configuration is required on the Cisco WAE to support PTC applications, unless other ports are required that are not part of the default application profile. TFO, DRE, and LZ compression are also enabled by default. Since Cisco WAAS deployments are transparent to the network, applications do not need to be aware of the added functionality and will benefit from the optimization provided by the Cisco WAEs.

Network Topology

The test environment contained one Cisco WAAS Central Manager and two Cisco WAEs managed by the WAAS Central Manager. The remote WAE was configured with a Cisco inline network adapter card and was deployed inline between the WAN router and the PTC clients or servers. The WAAS Central Manager runs on a dedicated appliance, located in the data center distribution switches, but can also be located at any layer, as long as it is able to reach the WAEs.

The following characteristics apply to WAAS deployment scenarios:

- As a general best practice, WAE devices should be placed as close to the WAN termination points as possible.
- A WAE running WAAS is required on both sides of the WAN link to perform optimization. Each device forms one or more peer relationships with other WAEs in the flow path.
- Each WAE must be placed on a dedicated subnet. Traffic to or from the subnet should not be configured for interception.
- Traffic in both directions of the flow must be seen by at least two WAEs for an optimized peer relationship to form. If both the request and response are not seen by a WAE, the traffic will pass through unoptimized.

- Policy-based routing (PBR)
- Web Cache Communications Protocol (WCCP) v2
- Inline hardware

Figure 16 **WAAS Topology**



WCCPv2 is the preferred mechanism for interception and redirection in networks that use WAAS for acceleration. PBR is usually recommended in branch deployments that cannot deploy WCCP for any reasons, which may include hardware or IOS versions deployed that do not support WCCPv2. WCCP is also preferred for the following reasons:

- Stateful, process-based availability monitoring—WAE availability is monitored continuously using WCCP keepalives. The WCCP processes on the WAE are more closely associated with the optimization components of the WAE, and as such, the availability metrics of the WAE is more accurate. PBR relies on CDP neighbor information, ICMP echo requests/responses or TCP connection requests/responses.
- Scalability and load-balancing—WCCPv2 allows up to 32 WAEs in a service group and up to 32 routers in a service group. PBR only provides failover and no scalability or load-balancing.

By default, WCCP redirects all traffic to the WAEs for inspection and optimization, unless an access list (ACL) is configured. Using WCCP ACL redirection may be beneficial for conserving WAAS processing, since it offloads the WAEs for inspecting pass-through traffic.

The following *Enterprise Branch Wide Area Application Services Design Guide* provides detailed design and deployment guidelines:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/WAASDC11.html

Scalability and Capacity Planning

Several factors play a role when selecting the proper WAE hardware model. For the branch, the number of estimated simultaneous TCP/CIFS connections, the estimated disk size for files to be cached, and the estimated WAN bandwidth are important. Cisco provides a WAAS sizing tool for guidance; [Table 2](#) shows a sample of the sizing information for WAEs.

Table 2 **WAE Hardware Sizing**

Device	Max Optimized TCP Connections	Max Recommended WAN Link (Mbps)	Max Optimized Throughput (Mbps)
WAE-512-1	750	8	100
WAE-512-2	1500	20	150
WAE-612-2	2000	45	250
WAE-612-4	6000	90	350
WAE-7326	7500	155	450
WAE-7341	12000	310	800

High Availability

The WAEs offer many built-in high-availability features. It is recommended to configure the disk subsystem with RAID 1 protection. RAID 1 is mandatory when two or more drives are installed in a WAE, so failure of a physical drive does not affect normal operations. Multiple network interfaces are also available, providing interface failover. When connected to separate switches in active/standby mode, the standby interface protects the WAE from switch failure.

WCCP provides load-balancing and high availability through a built-in load-balancing mechanism that distributes load amongst WAEs within a service group. The WCCP protocol can have up to 32 routers and 32 devices (WAEs) per service group.

Since Cisco WAAS deployments are transparent to the application, the PTC client and servers are not aware that the Cisco WAAS is optimizing traffic flows. High availability is built into the WCCP interception. If a WAE fails or WCCP is not active, traffic flows will continue to operate without being optimized.

Inline deployments allow the WAE to be physically inserted between two network devices such as the branch switch and the branch WAN router. The Cisco WAAS inline card has four 10/100/1000BaseT Ethernet ports in two port groups. Each port group provides a fail-to-wire bypass service with mechanical relays to ensure that network connectivity is not interrupted should a device fail or a software crash be encountered by the WAE.

Configuration Task Lists

Central Manager

The Central Manager is the main management component of the Cisco WAAS solution. It provides a GUI interface for configuration, monitoring, and management of the branch and data center WAEs. WAEs need to contact the CM during the initial setup. This registration process adds the WAEs to the CM and initializes the local WAE database.

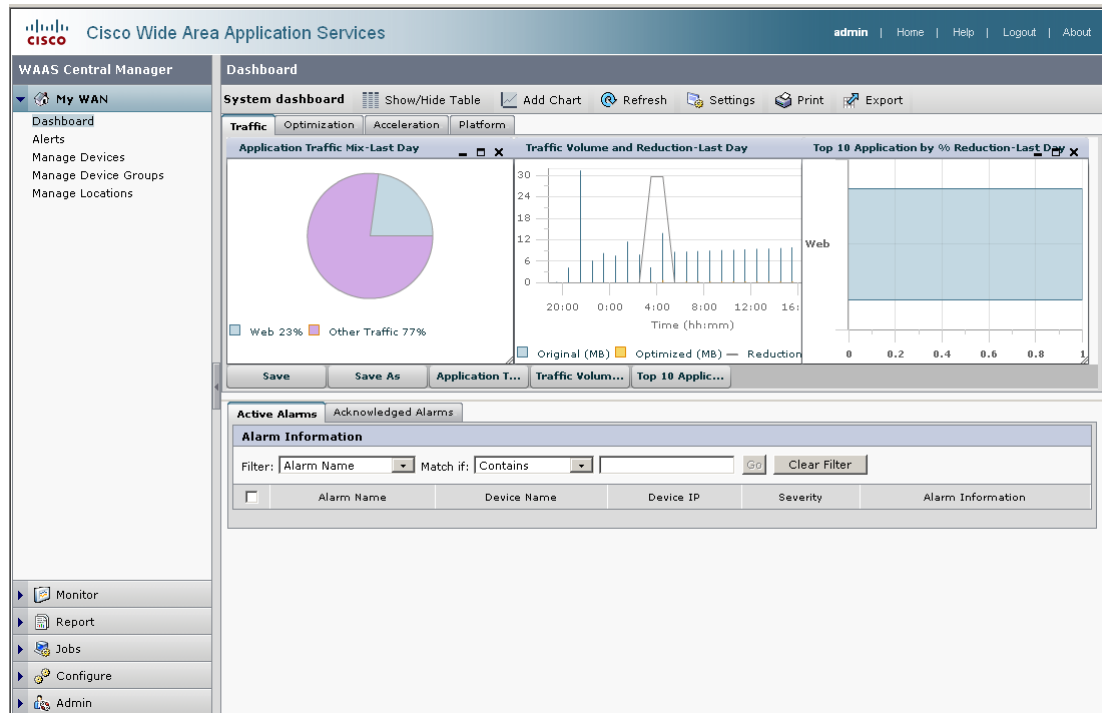
The Central Manager provides centralized reporting of the WAAS environment. Cisco WAEs also provide statistics through a local GUI or the CLI.

To configure the Central Manager, follow these steps:

-
- Step 1** Configure the IP address of the Central Manager and specify a default gateway:
- ```
interface GigabitEthernet 1/0
 ip address 10.1.52.5 255.255.255.0
 !
ip default-gateway 10.1.52.1
```
- Step 2** By default, the WAEs are configured in application-accelerator mode. To configure the device to act as a Central Manager, use the following command:
- ```
!
device mode central-manager
```
- Step 3** Using the **primary-interface** command, specify the interfaces used for traffic interception and delivery:
- ```
!
primary-interface GigabitEthernet 1/0
```
- Step 4** Specify the NTP server used by all Cisco WAEs and network devices to synchronize time. In the test environment, a Cisco Catalyst 6500 switch provides NTP clock to all devices.
- ```
ntp server 10.1.6.1
```
- Step 5** Enable the Centralized Management System (CMS) on the WAE using the **cms** configuration command. The **cns enable** command automatically registers the node in the database management tables and enables the CMS process.
- ```
!
cms enable
```
- Step 6** At this point, the Central Manager web user-interface should be available on port 8443. Point the web browser to the following URL: [https://CM\\_IP\\_address:8443](https://CM_IP_address:8443).

Figure 17 shows the initial CM screen with an overview of the system.

**Figure 17** WAAS Central Manager



226191

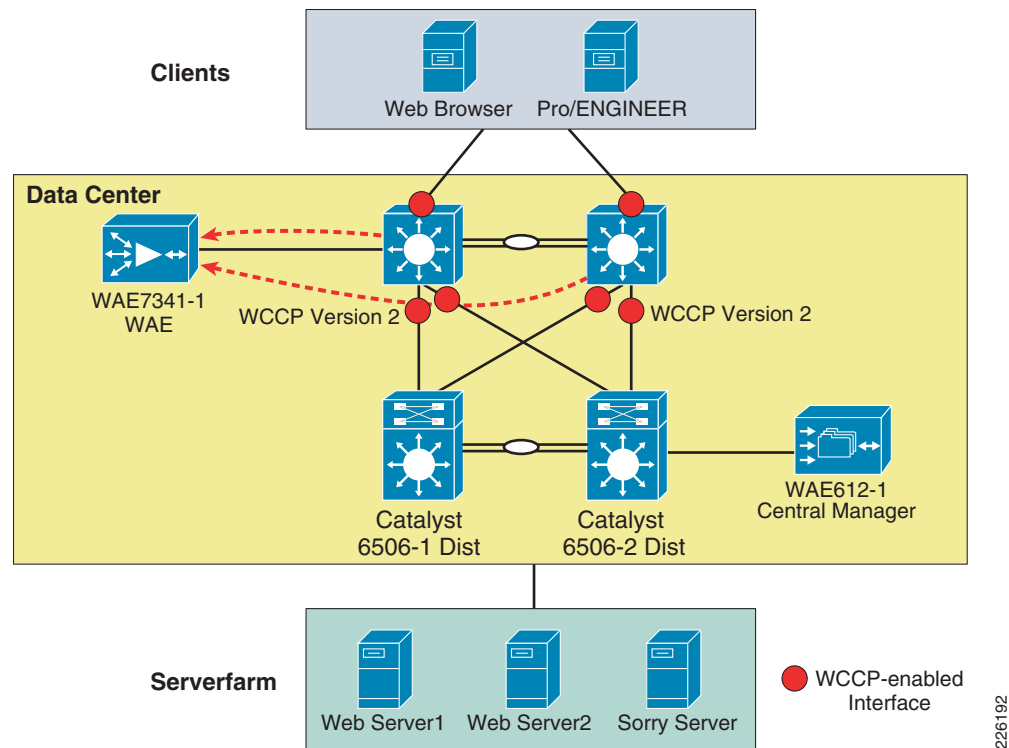
## Data Center WCCP Interception

In the test environment, WCCP interception was used at the data center. In data center environments, WCCP should be deployed on platforms that support redirection hardware to handle the high data rates from flow aggregation. To configure basic WCCP, the WCCP service must be enabled on at least one router and the WAEs.

The key points of this deployment model include:

- WCCP interception is performed as close to the WAN access point as possible, typically in aggregation switches directly behind the WAN routers or in cases where the WAN access terminates directly in Catalyst 6500 switches, in the WAN access switches themselves.
- Inbound WCCP redirection is configured so that redirection happens in hardware.
- WAE devices must be Layer 2 adjacent to the switches performing WCCP redirection.

WCCP Version 2 must be used instead of WCCP Version 1, because WCCP Version 1 only supports web traffic (port 80). In the test environment, WCCP Version 2 was enabled on the core switches and the data center WAE, as shown in Figure 18. A redundant WAE would typically be connected to the 6509-2 in the diagram.

**Figure 18 WCCP Interception**

### Enable WCCP on the Data Center WAE

To install and configure WAE devices with WCCP, and register them with the WAAS Central Manager, follow these steps:

**Step 1** Configure the WAE IP address and default gateway:

```
!
interface GigabitEthernet 1/0
 ip address 10.1.53.5 255.255.255.0
!
ip default-gateway 10.1.53.1
```

**Step 2** Specify the primary interface and NTP server and enable the **cms** database command:

```
!
primary-interface GigabitEthernet 1/0
!
ntp server 10.1.6.1
!
cms enable
```

**Step 3** Specify the IP address of the Central Manager:

```
!
central-manager address 10.1.52.5
```

**Step 4** The following command configures the WAE to function as a WAAS accelerator. All edge WAEs and data center WAEs should be operating in this mode:

```
!
```

```
device mode application-accelerator
```

- Step 5** Enable WCCPv2 and specify which routers are providing WCCP interception. Up to 32 routers can be specified in the list. 10.1.53.1 is the IP address of 6509-1 core switch, while 10.1.6.12 is the loopback address of 6509-2.

```
!
wccp version 2
wccp router-list 1 10.1.53.1 10.1.6.12
```

- Step 6** Turn on TCP promiscuous mode service and associated this service with a router list defined in the previous step:

```
!
wccp tcp-promiscuous router-list-num 1
```

## Enable WCCP on the Data Center Catalyst Switches

- Step 1** For the 6509-1 core switch, configure a loopback interface to identify the router ID:

```
interface Loopback1
ip address 10.1.6.11 255.255.255.255
```

- Step 2** Enable WCCPv2 and WCCP services 61 and 62 (TCP promiscuous mode):

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

- Step 3** Configure the LAN interface for redirection. This interface is for traffic will be intercepted from when leaving the data center network toward the WAN.

```
!
interface GigabitEthernet2/3
description to 2821-3
ip address 10.1.7.1 255.255.255.252
ip wccp 62 redirect in
```

- Step 4** Enable WCCP service 62 redirection on the interfaces facing the distribution switches:

```
!
interface GigabitEthernet2/47
description to 6506-2 Distribution
ip address 10.1.5.2 255.255.255.252
ip wccp 61 redirect in
!
interface GigabitEthernet2/48
description to 6506-1 Distribution
ip address 10.1.5.10 255.255.255.252
ip wccp 61 redirect in
```

- Step 5** On interface VLAN 53, enter the **ip wccp redirect exclude in** command to specify that the core switch should not repeatedly redirect the same traffic to the local WAE:

```
!
interface Vlan53
ip address 10.1.53.1 255.255.255.0
ip wccp redirect exclude in
```



- Step 6** Besides IP addresses, the configuration for the 6509-2 is identical. [“Appendix C—Device Configurations” section on page 78](#) has the full configuration for both switches.

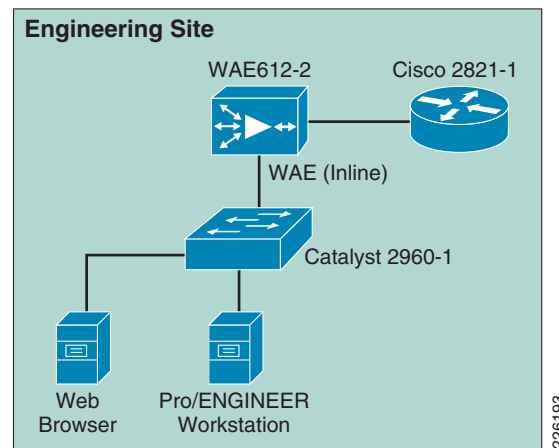
## Remote WAE

The remote engineering site does not rely on WCCP interception. Instead, a WAE Inline Network Adapter is installed. With inline interception that WAE is deployed physically between the WAN router and a switch at the remote engineering site. This allows all traffic traversing the network toward the WAN or returning from the WAN to physically pass through the WAE, giving it the opportunity to optimize traffic flows.

The Cisco PCI Inline Network Adapter provides two groups of fail-to-wire pairs, providing fail-to-wire capabilities during failure scenarios. If the WAE in [Figure 19](#) fails, connectivity to the site would continue, but no optimization would take place.

The Cisco PCI Inline Network Adapter provides two groups of fail-to-wire pairs, providing fail-to-wire capabilities during failure scenarios. If the WAE in [Figure 19](#) fails, connectivity to the site continues without optimization.

**Figure 19 Remote Engineering Site**



To configure the remote WAE for inline interception, follow these steps. No configuration changes are required to the switch or WAN router:

- Step 1** Define the common WAE settings:

```
!
device mode application-accelerator
!
ntp server 10.1.6.1
!
ip default-gateway 10.1.61.1
!
central-manager address 10.1.52.5
cms enable
```

- Step 2** Configure the interfaces that will participate in inline interception and define the primary interface:

```
!
primary-interface InlineGroup 1/0
```

```
!
interface InlineGroup 1/0
ip address 10.1.61.5 255.255.255.0
inline vlan all
exit
interface InlineGroup 1/1
inline vlan all
exit
```

## HTTP Acceleration

PTC's solution relies on HTTP or HTTPS traffic to communicate between the client and servers. WAAS is able to accelerate HTTP traffic on ports 80, 8080, 8000, 8001, and 3128. To verify that web application policies are in place, from the WAAS GUI, select **Configure > Acceleration > Policies > HTTP**. [Figure 20](#) shows the configurations used in the test environment.

**Figure 20** WAAS HTTP Policy

The screenshot displays the Cisco Wide Area Application Services (WAAS) GUI. The left sidebar shows the navigation menu with 'Configure' selected. The main content area is titled 'Modifying Application Policy, for Device Group, AllDevicesGro...'. The configuration form includes the following fields and values:

- Type: Basic
- Application: Web
- Application Classifier: HTTP
- Action: Full Optimization
- Accelerate: HTTP
- Position: First (radio button), Last (radio button), Specific (radio button, selected) with value 38
- DSCP Marking: inherit-from-name
- Enabled: ☒

A note at the bottom of the form states: 'Some or all configuration on this page may not have any effect on the WAE (individual or part of device group) until it is upgraded to version 4.1.x or above.' The 'Submit' and 'Cancel' buttons are located at the bottom right of the form.

## WAAS Implementation Caveats or Limitations

### WAAS and ACE Compression

Compression should not be enabled at both WAAS and ACE when both are part of the flow. When both WAAS and ACE are part of the traffic flow, compression should only be enabled on the WAAS and disabled on the ACE. In a future release, the ACE will be able to determine what packets have already been compressed by the WAAS and disable compression for those flows. The ACE may be manually configured to disable compression.

## Troubleshooting Commands

### Cisco WAE Commands

The following commands may be useful when troubleshooting the WAAS configuration:

- **sh wccp status**—Verifies WCCP V2 is enabled.
- **sh wccp services**—Verifies WCCP service 61 and 62 are active. Service 61 and 62 must be active.
- **sh wccp routers**—Verifies the router can see the Cisco WAE. Notice that the router ID is the router loopback address. Sent To is the router interface on the Cisco WAE VLAN. All routers are defined and visible on the Cisco WAE.
- **sh statistics dre**—This command displays the DRE general statistics for the WAE.
- **sh statistics tfo**—This commands displays the (TFO) statistics for a WAE.

The following are sample outputs of some of the previous commands:

```
WAE612-2-EDGE#show statistics tfo
Total number of connections : 324
No. of active connections : 2
No. of pending (to be accepted) connections : 0
No. of bypass connections : 116
No. of normal closed conns : 231
No. of reset connections : 91
Socket write failure : 49
Socket read failure : 0
WAN socket close while waiting to write : 0
AO socket close while waiting to write : 2
WAN socket error close while waiting to read : 0
AO socket error close while waiting to read : 40
DRE decode failure : 0
DRE encode failure : 0
Connection init failure : 0
WAN socket unexpected close while waiting to read : 0
Exceeded maximum number of supported connections : 0
Buffer allocation or manipulation failed : 0
Peer received reset from end host : 0
DRE connection state out of sync : 0
Memory allocation failed for buffer heads : 0
Unoptimized packet received on optimized side : 0
Data buffer usages:
 Used size: 0 B, B-size: 0 B, B-num: 0
 Cloned size: 36757 B, B-size: 52224 B, B-num: 67
Scheduler:
 Queue Size: IO: 0, Semi-IO: 0, Non-IO: 0
```

```

WAE7341-1#show statistics dre
Cache:
 Status: Usable, Oldest Data (age): 2h18m58s
 Total usable disk size: 503325 MB, Used: 0.00%
 Hash table RAM size: 2012 MB, Used: 0.00%

Connections: Total (cumulative): 321 Active: 1

Encode:
 Overall: msg: 8570, in: 83716 KB, out: 10982 KB, ratio: 86.88%
 DRE: msg: 8470, in: 83694 KB, out: 17236 KB, ratio: 79.41%
 DRE Bypass: msg: 4595, in: 22329 B
 LZ: msg: 4074, in: 9265 KB, out: 2962 KB, ratio: 68.02%
 LZ Bypass: msg: 4496, in: 7992 KB
 Avg latency: 0.327 ms Delayed msg: 17620
 Encode th-put: 29896 KB/s
 Message size distribution:
 0-1K=50% 1K-5K=10% 5K-15K=12% 15K-25K=10% 25K-40K=15% >40K=1%
Decode:
 Overall: msg: 1043, in: 187 KB, out: 665 KB, ratio: 71.86%
 DRE: msg: 967, in: 613 KB, out: 658 KB, ratio: 6.91%
 DRE Bypass: msg: 874, in: 6988 B
 LZ: msg: 776, in: 185 KB, out: 616 KB, ratio: 69.88%
 LZ Bypass: msg: 267, in: 1696 B
 Avg latency: 0.070 ms
 Decode th-put: 9144 KB/s
 Message size distribution:
 0-1K=76% 1K-5K=23% 5K-15K=0% 15K-25K=0% 25K-40K=0% >40K=0%

```

## WCCP Router Commands

- **sh ip wccp 61 [or 62]**—Verify that WCCP service 61 and 62 are active. The command shows global WCCP information and how the packets are redirected.
- **sh ip wccp 61 [or 62] detail**—Checks WCCP client hash or Layer 2 assignments. This command also checks the status of the WCCP client, the Cisco WAEs. The **sh ip wccp 61 detail** command shows detailed global WCCP information.
- **sh ip wccp interface detail**—Verifies which interface has WCCP configured. Identify all interfaces within a router or switch that have WCCP configured with ingress or egress for exclude-in redirection.
- **sh ip wccp 61 [or 62] view**—Verifies WCCP group membership.

The following is a sample output of the **show ip wccp** command executed on the 6509-1 core switch:

```

6509-1#show ip wccp
Global WCCP information:
 Router information:
 Router Identifier: 10.1.6.11
 Protocol Version: 2.0

 Service Identifier: 61
 Number of Service Group Clients: 1
 Number of Service Group Routers: 1
 Total Packets s/w Redirected: 14065
 Process: 0
 CEF: 14065
 Redirect access-list: -none-
 Total Packets Denied Redirect: 0
 Total Packets Unassigned: 0

```

```

Group access-list: -none-
Total Messages Denied to Group: 0
Total Authentication failures: 0
Total Bypassed Packets Received: 0

Service Identifier: 62
Number of Service Group Clients: 1
Number of Service Group Routers: 1
Total Packets s/w Redirected: 263
 Process: 0
 CEF: 263
Redirect access-list: -none-
Total Packets Denied Redirect: 0
Total Packets Unassigned: 87
Group access-list: -none-
Total Messages Denied to Group: 0
Total Authentication failures: 0
Total Bypassed Packets Received: 0

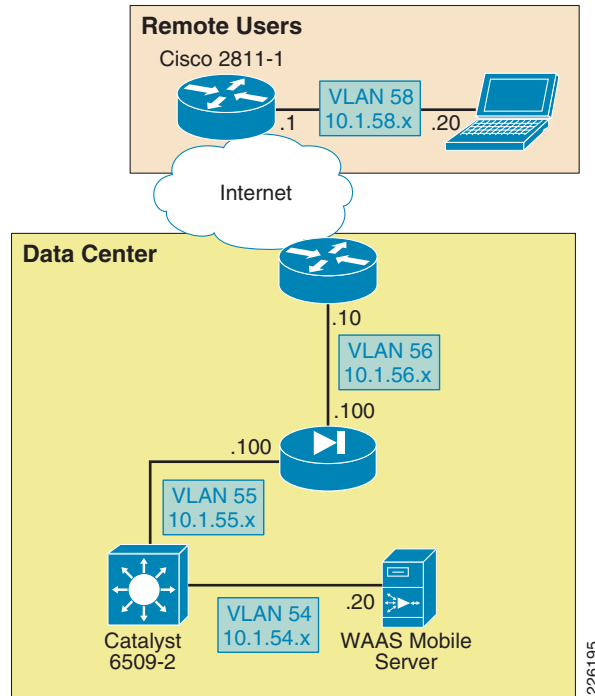
```

# WAAS Mobile Implementation and Configuration

## Network Topology

The test environment contains one WAAS Mobile server located in the data center and remote PTC clients connecting through a VPN service into a Cisco ASA appliance. The Internet connectivity is provided by a T1 connection. While several factors may impact Internet connectivity, the lab connection used 100ms delay and 1 percent packet drop to simulate a typical Internet connection. [Figure 21](#) shows the WAAS Mobile topology.

**Figure 21** *WAAS Mobile Topology*



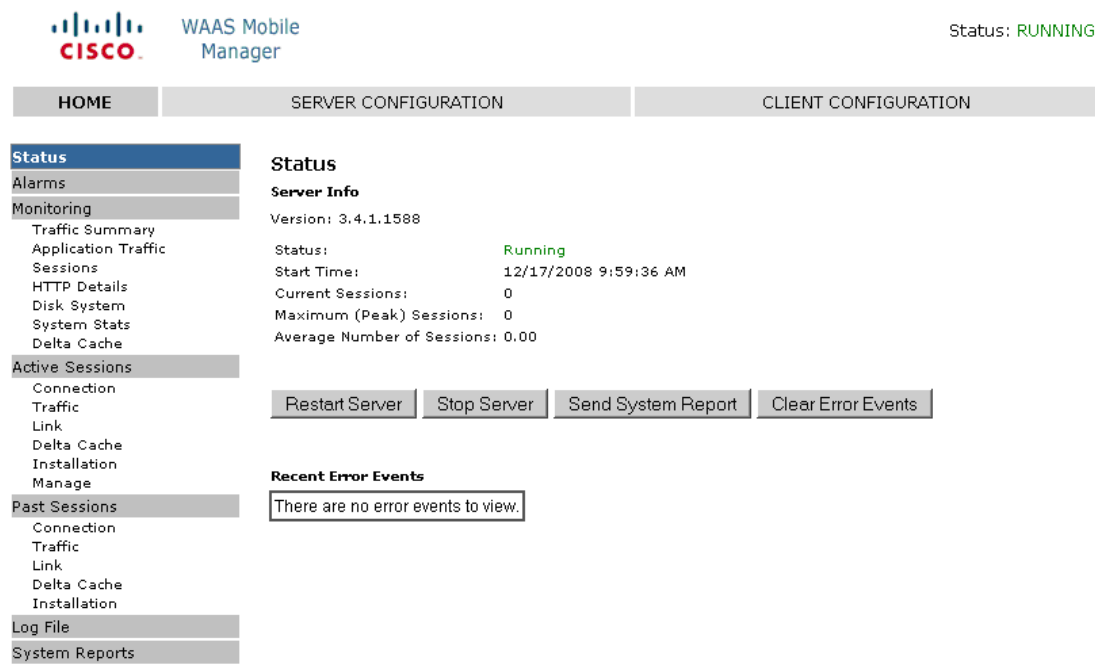
226195

## WAAS Mobile Server

The WAAS Mobile server was installed on a Windows 2003 Enterprise server following these steps:

- Step 1** Install the server software by double-clicking on the **ServerSetup.exe** file.
- Step 2** When installation completes, a browser window will open and display the WAAS Mobile Manager Home page.
- Step 3** Enter the license key by clicking on the **WAAS Mobile Manager Server Configuration > Licensing** page.
- Step 4** Verify Delta Cache size and location by navigating to the **WAAS Mobile Manager Server Configuration > Advanced Settings > Delta Cache** screen.
- Step 5** By default, WAAS Mobile will attempt to configure a 275 GB cache. If there is insufficient space available, a fallback cache of 50 GB will be attempted. A minimum of 5 GB of disk space is required.
- Step 6** Start the server. Navigate to the **WAAS Mobile Manager Home > Status** page and click the **Start Server** button. [Figure 22](#) shows the server status.

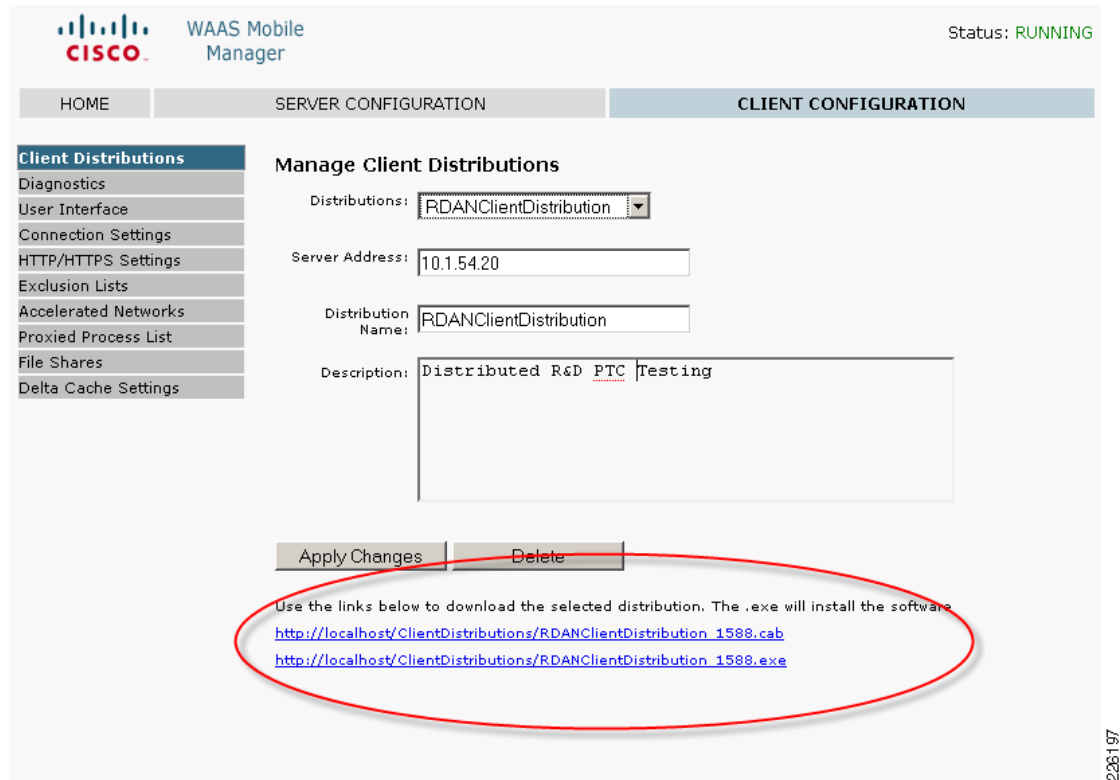
Figure 22 WAAS Mobile Manager Server



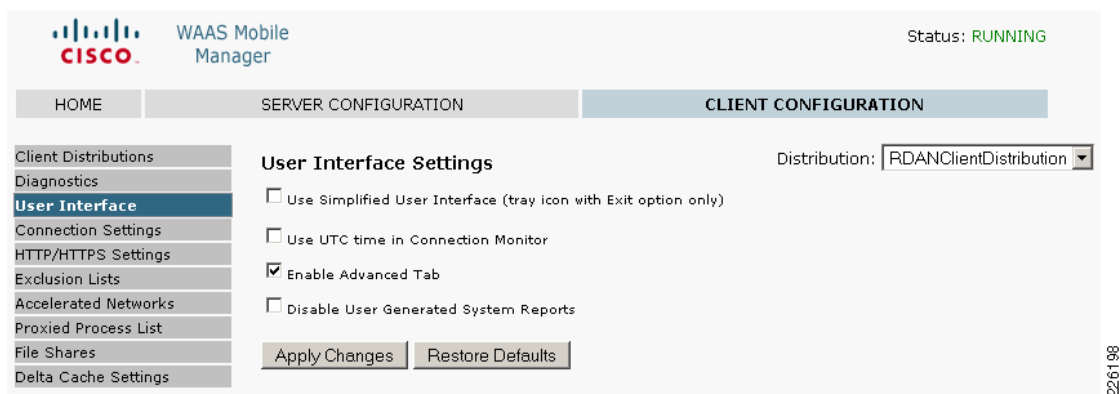
228196

## Create a Client Distribution

- Step 1** Go to the Client Configuration section of the WAAS Mobile Manager and click on **Client Distributions**.
- Step 2** From the pull-down menu in the *Distributions* field, select **Create New Distribution**.
- Step 3** Enter the IP or DNS host name of the server in the *Server Address* field.
- Step 4** Enter a name and description for the distribution and click **Create**; after the distribution has been created, new links will appear. Figure 23 shows the client distribution created for the test environment.

**Figure 23** WAAS Mobile Client Distribution

- Step 5** To distribute the client software, click on the **.exe** link at the bottom of the screen and save the distribution file. The link to the **.exe** file could also be emailed to users for self-install. To allow the client to view the **Advanced Tab**, go to **Client Configuration > User Interface** and select **Enable Advanced Tab**, as shown in [Figure 24](#).

**Figure 24** WAAS Mobile Advanced Tab

[Figure 25](#) shows the Delta Cache Settings configured for the user, with a 1GB local cache and the file location.



**Figure 25**      **Delta Cache Settings**

The screenshot displays the 'Delta Cache Settings' page in the Cisco WAAS Mobile Manager. The status is 'RUNNING'. The left sidebar lists various configuration sections, with 'Delta Cache Settings' selected. The main content area shows the following settings:

- Delta Cache Settings** (Distribution: RDANClientDistribution)
- Desired Delta Cache Size:** 1024 MB
- Maximum Delta Cache Size:** 10240 MB (Note: Client delta cache size may not exceed this value.)
- Reduced Size Enabled:** ☒
- Reduced Delta Cache Size:** 256 MB (Note: Size if desired size does not fit.)
- Delta Cache Location:** %ALLUSERSPROFILE%\Application Data\Cisco\WAASMobile\DeltaCache\ (Note: Paths can include Windows environment variables. For instance, %USERPROFILE%, %Temp%, ...)
- HTTPS Caching:** ☒
- Encryption:** ☐

Buttons at the bottom: **Apply Changes** and **Restore Defaults**.

226199

## WAAS Mobile Configuration for Pro/ENGINEER

While Cisco WAAS acts on TCP connections in general, Cisco WAAS Mobile acts on individual well-defined applications. In order to optimize Pro/ENGINEER, the application must be added to the *Proxied Process List* in the Cisco WAAS Mobile Manager.

Figure 26 shows the steps to add Pro/ENGINEER to the proxied list. Under **Client Configuration > Proxied Process List**, enter the following:

- Process name: **xtop.exe**. This is the name of the Windows process used by Pro/ENGINEER.
- Under **Application Type**, select **1 – Generic Acceleration**.
- Under **Auto Reset Connection**, click on **Yes**.



### Note

Make sure to click on both **Add Process** and **Apply Changes** buttons to make the entries appear in the process list.

**Figure 26** *Proxied Process List*

WAAS Mobile Manager

Status: **RUNNING**

HOME SERVER CONFIGURATION **CLIENT CONFIGURATION**

Client Distributions  
Diagnostics  
User Interface  
Connection Settings  
HTTP/HTTPS Settings  
Exclusion Lists  
Accelerated Networks  
**Proxied Process List**  
File Shares  
Delta Cache Settings

**Proxied Process List** Distribution: RDANClientDistribution

Process Name: xtop.exe  
xtop.exe

Min Version: \*  
*Enter \* for no minimum version*

Max Version: \*  
*Enter \* for no maximum version*

Command Line: \*  
*Enter \* for any command line*

Acceleration Type: 1 - Generic Acceleration

Application Name: Pro/Engineer  
*(optional) Complete Application Name*


Auto Reset Connection: ☒ Yes ☐ No  
*Select Yes to automatically reset connections for this process*

Add Process Remove Selected Processes Restore Defaults Apply Changes

226200

## WAAS Mobile Client Installation

To install the WAAS Mobile client, follow these steps:

- Step 1** Login to the client PC with administrator privileges and execute the previous generated **.exe** file.
- Step 2** Follow the install wizard and restart the computer when asked.
- Step 3** After registering, the client software will automatically start up and connect to WAAS Mobile Manager
- Step 4** Once connected, WAAS Mobile will start accelerating and the  icon will appear in the Windows System Tray and turn green.

The following icons are displayed in the Windows System Tray of the client PC to indicate the status of WAAS Mobile:



Connected—WAAS Mobile is accelerating applications



User Disabled—Application acceleration disabled by the user



Persistent Connection—The client lost connection to the WAAS Mobile server but acceleration session is still active

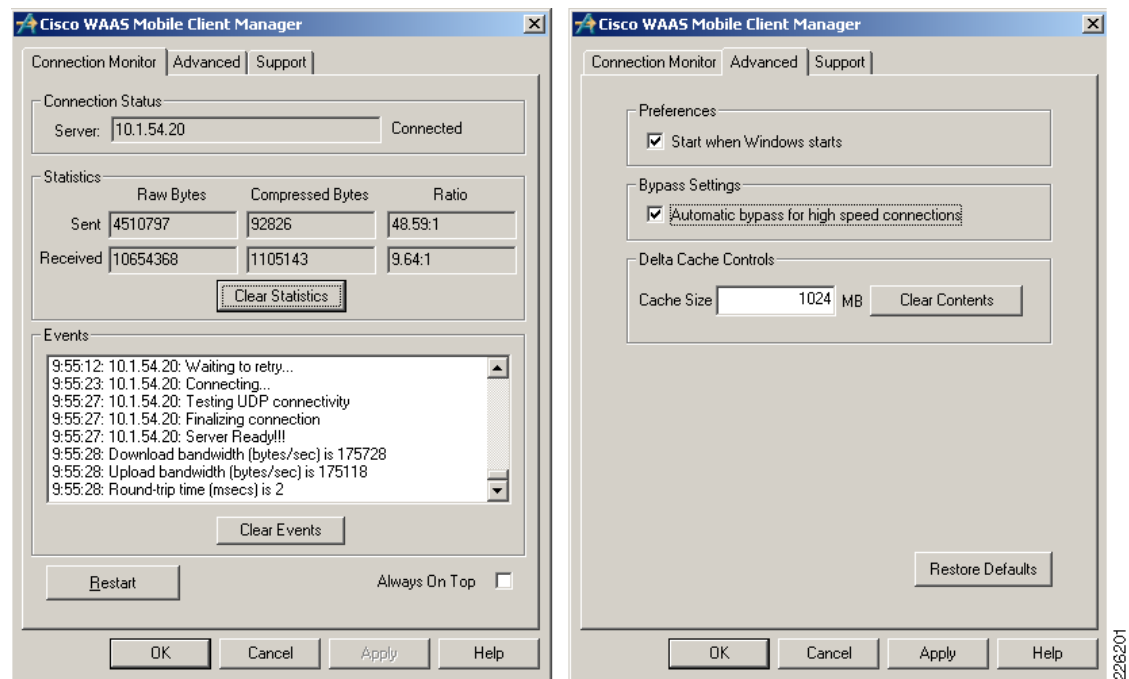


Not Connected —The client lost connection to the WAAS Mobile server and is not accelerating applications. This is also displayed when the client is connected to a high-speed network

## Client Software Configuration

The client configuration can be easily managed from the central WAAS Mobile server, while the client has limited configuration options. [Figure 27](#) shows the WAAS Client Manager displaying connection statistics and the optional Advanced tab allowing the client to change delta cache and startup settings.

**Figure 27** WAAS Mobile Client Manager



## Cisco ASA Configuration

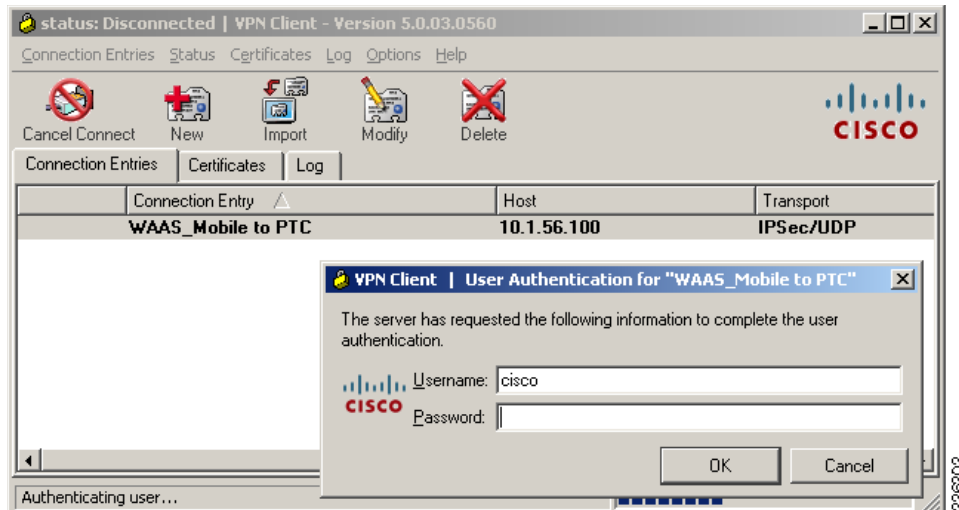
The ASA was configured to support remote VPN user connections. “[Appendix C—Device Configurations](#)” section on [page 78](#) shows the ASA detailed configuration.

## Cisco VPN Client

In order to connect securely to the data center ASA, a VPN connection is established using the Cisco VPN client. For the test environment, local authentication was used to authenticate the user.

[Figure 28](#) shows a client connection to the outside interface of the ASA on IP address 10.1.56.100.

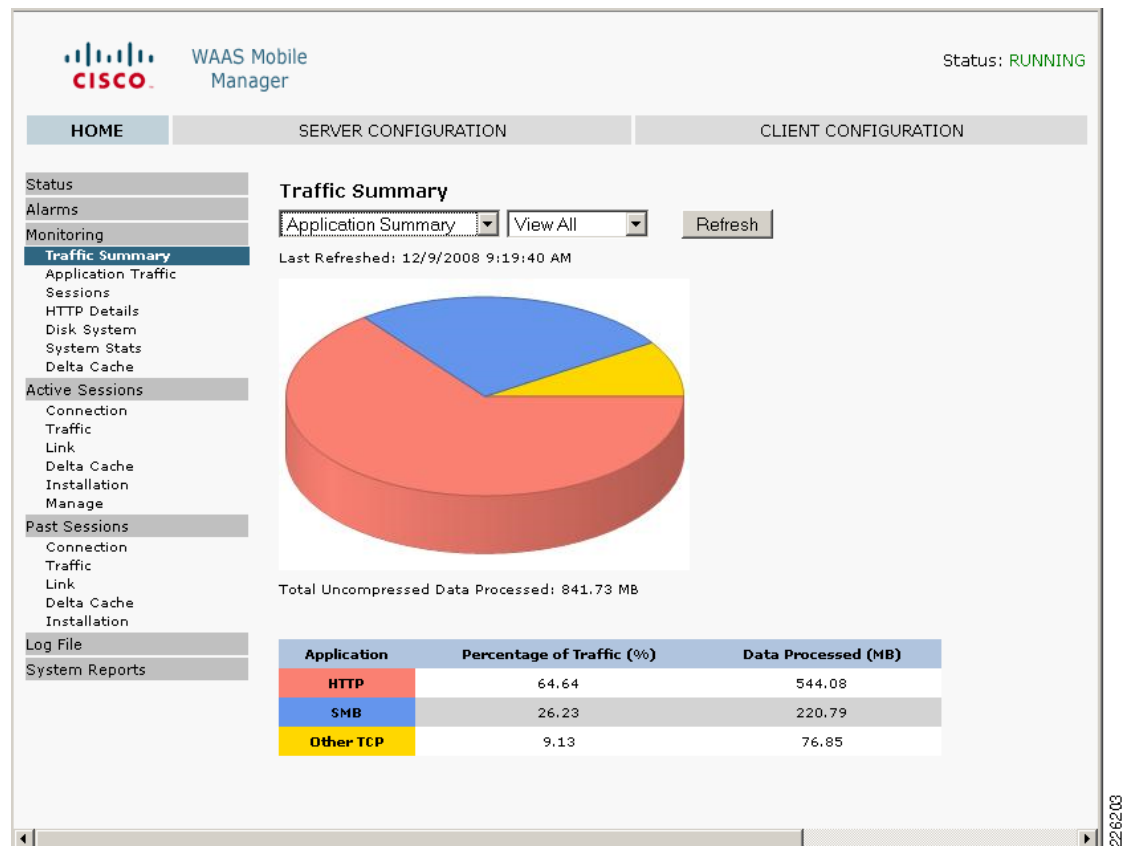
**Figure 28** *Cisco VPN Client*



## System Reports

The WAAS Mobile Manager provides valuable reports to determine the acceleration benefits for an application. [Figure 29](#) shows a sample report describing the traffic summary for different applications and details on how much traffic was processed.

Figure 29 WAAS Mobile Manager



## ACE Implementation and Configuration

The Cisco ACE 4710 appliance was configured in bridged mode, with both the client-side and server-side VLANs on the same subnet. Two ACE 4710 appliances were configured in fault-tolerant mode to ensure that network services and applications are always available. The following features were implemented:

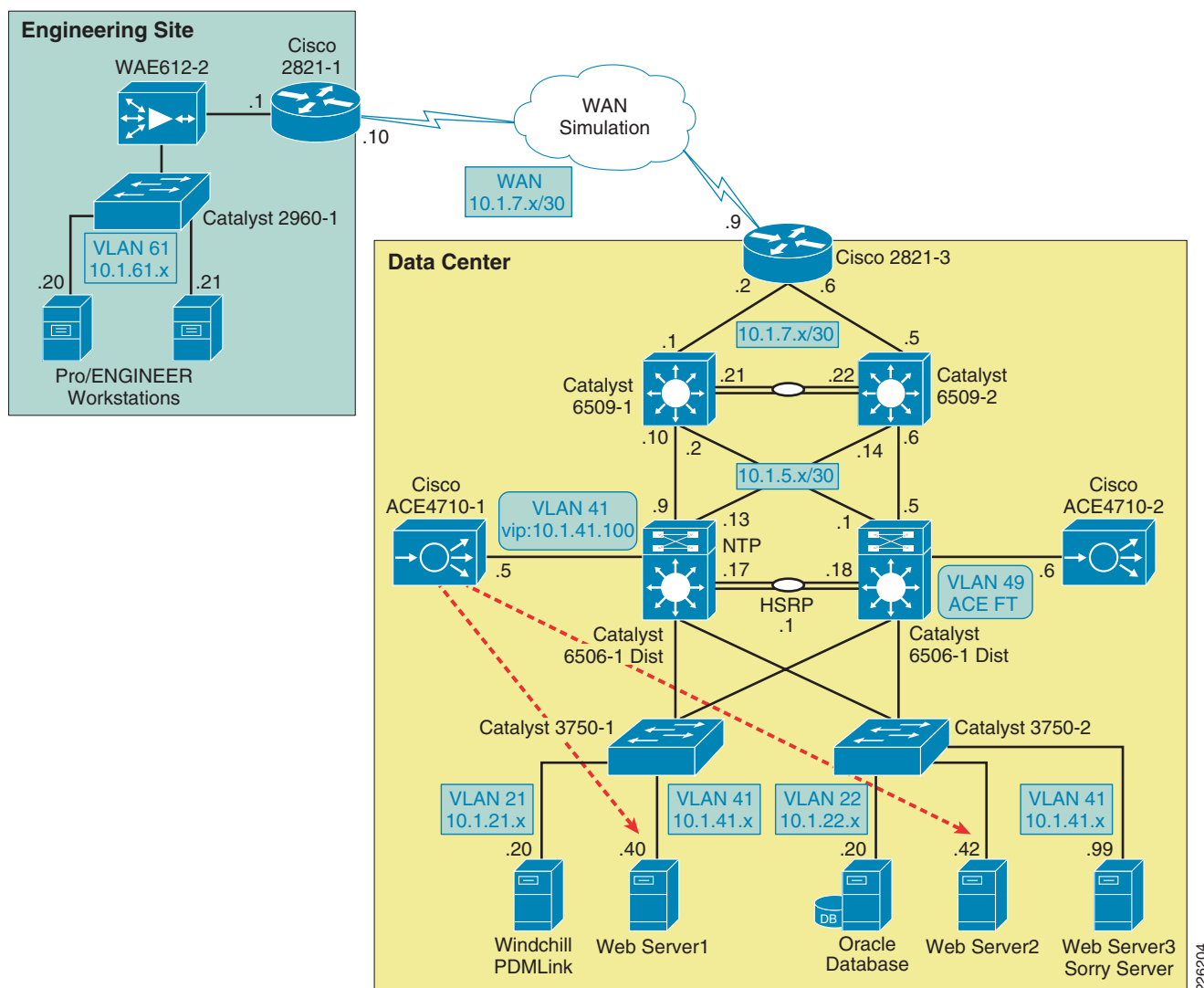
- Serverfarms
- Virtualization
- Server health monitoring
- Layer 7 load balancing
- Persistence-based server cookie
- Connection replication for stateful failover
- Compression
- FlashForward
- Redundancy

A web serverfarm was configured with two servers responding to user requests. The Cisco ACE was configured to provide load balancing between the servers and the remote PTC users. In case the servers were offline or unable to respond to users requests, a third server (sorry server) was configured to make users aware of the service disruption.

## Network Topology

The Cisco ACE appliance uses a range of Cisco application switching technologies, such as Layer 4 load balancing, Layer 7 content switching, caching and TCP processing. The Cisco ACE is deployed in the distribution layer, in front of a web serverfarm supporting the PTC application and Oracle database. As shown in [Figure 30](#), PTC clients reach the ACE through a single virtual IP (VIP) address (at 10.1.41.100) before reaching a server selected by the ACE. In turn, the ACE selects the best web server to service the request.

**Figure 30** ACE Network Topology



## Features and Design Considerations

PTC offers a flexible environment supporting a large number of application servers. The web servers provide clients with access to the PTC applications without directing access to a PTC application server or database directly. A web serverfarm allows the PTC to support a large number of users while providing redundancy and high availability. The web serverfarm allows for the application to be operational while servers are shutdown for maintenance or updates. The configuration used for the testing only employed a load balanced web-tier for simplicity. The Windchill architecture also allows for clustered application servers and database tiers.

## High Availability and Load Balancing Features

For meeting high availability requirements, the Cisco ACE supports the configuration of two ACE appliances in redundant or fault tolerant mode. These appliances are connected to different Cisco Catalyst switches to provide services even if one of the appliances becomes unresponsive. Redundancy is only supported between ACE devices of the same type running the same software release.

By load balancing multiple servers in the serverfarm, the system is able to offer higher availability and scalability. This functionality can be extended to multiple serverfarms, such as PTC Windchill servers, web servers or database servers.

The Cisco ACE provides the following key functions:

- Provides server load balancing to multiple clients. Clients reach the serverfarm with a single virtual IP address and corresponding virtual hostname.
- Incoming requests are distributed according to configurable rules or predictors. The load-balancing method in use determines how the ACE selects a real server in a serverfarm to service a client request. Typical predictors include: round-robin, least-connections, least-loaded, etc.
- The Cisco ACE is able to monitor the health of the servers. Health monitoring probes run periodically to detect server scalability or failures. The Cisco ACE provides a large number of probes, such as ICMP, HTTP, SNMP, etc.
- Stickiness allows a client to maintain simultaneous or subsequent connections with the same server. Depending on the server load balancing policy, the ACE “sticks” a client to an appropriate server and sends all requests to that server, regardless of the load-balancing criteria. If the ACE determines that the client is not stuck to a particular server, it applies the normal load-balancing rules to the request. PTC’s Windchill solution does require session stickiness for proper application functionality.



**Note**

The *Cisco ACE 4700 Series Application Server Load-Balancing Configuration Guide* (see [Appendix B—Reference Documents, page 78](#)) provides more details on high availability features.

## Configuration Task Lists

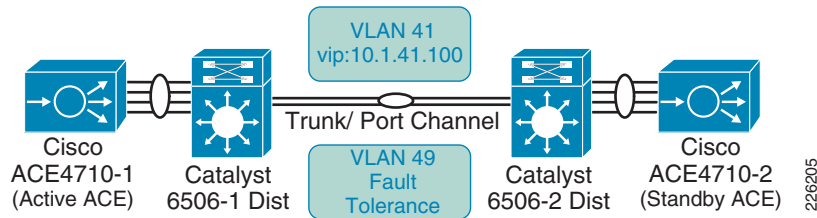
### Catalyst 6500

The ACE 4710 appliances are connected to the Cisco Catalyst 6500 switches in the distribution layer, which provide two main VLANs for connectivity. VLAN 41 is dedicated to the ACE virtual IP address (10.1.41.100) and VLAN 49 is dedicated for redundancy with the backup ACE 4710 appliance. The Catalyst 6500 provides HSRP first-hop redundancy, with the 6506-1 being the active HSRP.

```
!
vlan 41
 name ACE_Server_Side
!
vlan 49
 name ACE__FT
```

As shown in [Figure 31](#), the connection between the Catalyst 6500 and the ACE 4710 is configured as a trunk and as an EtherChannel, allowing up to four 1Gbps interfaces to be active at the same time.

**Figure 31** *ACE Connections to Catalyst 6500*



```
interface Port-channel1
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
!
interface GigabitEthernet1/4
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
!
interface GigabitEthernet1/5
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
!
interface GigabitEthernet1/6
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
```



## Remote Management Access

By default, the ACE blocks all types of network management access. In order to allow protocols such as Telnet, HTTP, HTTPS or ICMP, a policy that allows network management protocols must be configured and applied to the proper interface.

- Step 1** Create a class map using the **class-map type management** command. The following class-map example allows Telnet, SSH, ICMP, HTTP and HTTPS:

```
class-map type management match-any REMOTE_ACCESS
 description Remote access traffic match
 2 match protocol telnet any
 3 match protocol ssh any
 4 match protocol icmp any
 5 match protocol http any
 6 match protocol https any
```

- Step 2** Create a policy map for traffic destined to an ACE interface. For example, to create a policy-map named **REMOTE\_MGMT\_ALLOW\_POLICY**, enter the following commands:

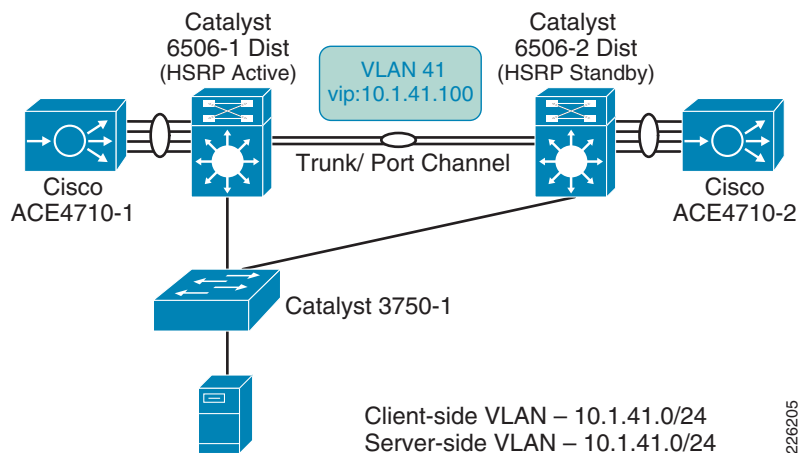
```
policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
 class REMOTE_ACCESS
 permit
```

- Step 3** Apply the policy map to the ACE interfaces:

```
interface vlan 41
 description Server-Side interface
 service-policy input REMOTE_MGMT_ALLOW_POLICY
interface vlan 411
 description Client-Side interface
 service-policy input REMOTE_MGMT_ALLOW_POLICY
```

## Interfaces and Default Gateway

As shown in [Figure 32](#), the ACE appliances are connected to different Catalyst 6500 for redundancy. A trunk is configured between the Catalyst switches and the ACE allowing all VLANs, while a port channel is used to aggregate four ACE 1Gbps interfaces into the Catalyst 6500.

**Figure 32**      **Interfaces and Default Gateway**

The ACE was deployed in Layer 2 (bridged) mode, bridging VLAN 41 and VLAN 411. VLAN 411 acts as the client -side VLAN and VLAN 41 as the server-side VLAN.

An access list named **ALL** is used to permit or deny traffic through the interfaces as shown in the following example:

```
access-list ALL line 8 extended permit ip any any
access-list ALL line 20 extended permit icmp any any

interface vlan 41
 description Server-Side interface
 bridge-group 10
 access-group input ALL
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 no shutdown
interface vlan 411
 description Client-Side interface
 bridge-group 10
 access-group input ALL
 access-group output ALL
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 no shutdown
```

In bridged mode, an interface BVI is required to merge both client- and server-side VLANs as shown below:

```
interface bvi 10
 ip address 10.1.41.5 255.255.255.0
 no shutdown
```

The Catalyst 6500 has interfaces defined for these VLANs and acts as the HSRP group for VLAN 411. All servers point to 10.1.41.1, the HSRP address for their default gateway. In this case, 6506-1 acts as the primary router:

|                                    |                                    |
|------------------------------------|------------------------------------|
| On 6506-1                          | On 6501-2                          |
| interface Vlan411                  | interface Vlan411                  |
| ip address 10.1.41.2 255.255.255.0 | ip address 10.1.41.3 255.255.255.0 |
| standby 41 ip <b>10.1.41.1</b>     | standby 41 ip <b>10.1.41.1</b>     |
| standby 41 priority 110            | standby 41 priority 90             |
| standby 41 preempt                 | standby 41 preempt                 |

Flows initiated from the servers require an inbound access list to allow the flow on the interface where the request is received.

- No routing is needed on the ACE since traffic is bridged through
- Established flows are not disconnected when ACLs are removed, but new flows are not allowed
- Servers are not allowed to access their default gateway without proper access on the server-side VLAN

At a minimum, an ACL is required on the server-side VLAN to allow for server-initiated flows:

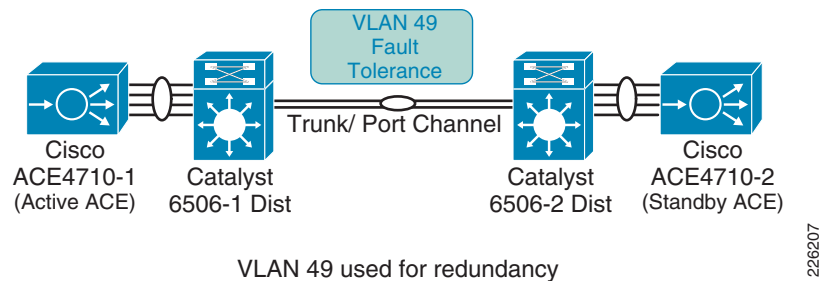
```
!
access-list ALL line 8 extended permit ip any any
!
interface vlan 41
 description Server-Side interface
 bridge-group 10
 access-group input ALL
```

## Redundant ACE Appliances

Redundancy is configured with a maximum of two ACE appliances; the appliances must be of the same ACE type and software release. Redundancy provides a seamless switchover of flows in case an ACE becomes unresponsive or a critical host, interface or HSRP group fails.

Each appliance contains one or more fault-tolerant (FT) groups and each group consists of two members: one active and one in standby. A dedicated FT VLAN is used between the ACEs to transmit flow-state information and the redundancy heartbeat. This VLAN should not be used for normal network traffic. As shown in [Figure 33](#), VLAN 49 is configured as the FT VLAN.

**Figure 33** Redundant ACE Appliances



The following commands are required to enable redundancy at the ACE appliances:

```
!
ft interface vlan 49
 ip address 10.1.49.1 255.255.255.0
 peer ip address 10.1.49.2 255.255.255.0
!
ft peer 1
 heartbeat interval 300
 heartbeat count 10
 ft-interface vlan 49
!
ft group 2
 peer 1
 priority 110
 peer priority 105
```

```
associate-context Admin
inservice
```

The **show ft groups status** command is used to verify that redundancy is enabled:

```
ACE4710-1/Admin# show ft group status

FT Group : 2
Configured Status : in-service
Maintenance mode : MAINT_MODE_OFF
My State : FSM_FT_STATE_ACTIVE
Peer State : FSM_FT_STATE_STANDBY_HOT
Peer Id : 1
No. of Contexts : 1
```

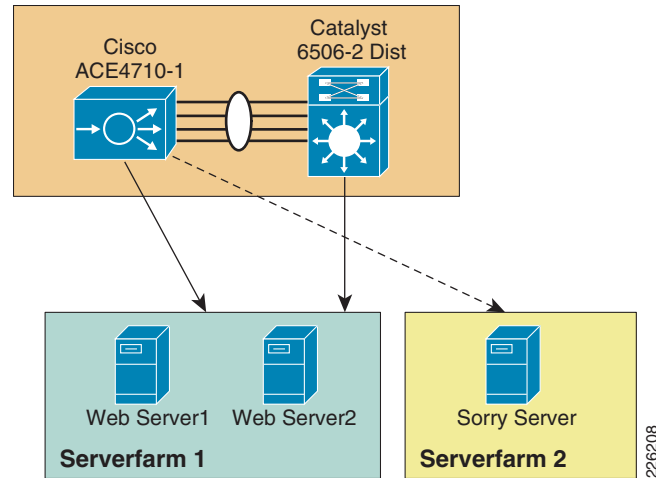
## Real Server and Serverfarm

Real servers are dedicated physical servers configured in groups called serverfarms. Three web servers were configured to provide PTC services. These real servers are used by the ACE to send intended traffic based on certain criteria, while a *sorry* server was configured to alert users of any service disruptions.

The following configurations show the three real servers with their respective IP addresses.

```
server host SERVER1
 description Web_Server_1
 ip address 10.1.41.40
 inservice
rserver host SERVER2
 description Web_Server_2
 ip address 10.1.41.42
 inservice
rserver redirect SORRY_SERVER
 webhost-redirection http://10.1.41.99/
 inservice
```

A serverfarm is a logical collection of real servers that the ACE selects based on certain sets of criteria. Serverfarms contain the same content and typically reside in the same physical location in a data center. The two web servers in Serverfarm 1 (see [Figure 34](#)) serve requests from PTC clients, while the sorry server is accessed only when the servers in Serverfarm 1 are not available.

**Figure 34 Serverfarms**

The following configuration shows the configuration for the two servers in SFARM1 and a sorry server in SFARM2:

```
serverfarm host SFARM1
 rserver SERVER1
 inservice
 rserver SERVER2
 inservice
serverfarm redirect SFARM2
 rserver SORRY_SERVER
 inservice
```

## Session Persistence (Stickiness)

Session Persistence allows multiple connections from the same client to be directed to the same real server for the duration of a session. Persistence is required by Windchill and PTC recommends the use of the HTTP cookie method as the primary type of persistence, but other forms of persistence are also expected to work. The ACE supports several sticky methods, including source and/or destination IP address, HTTP cookie, HTTP header, etc.

- With IP Address Stickiness, the source IP address, the destination IP address, or both may be used to identify individual clients. A possible drawback of using a source IP address is that client connections may be established through a proxy, making it an unreliable indicator of the true source of the request.
- HTTP Cookie Stickiness allows the ace to uniquely identify clients by inserting a small data structure within the HTTP header and storing it at the client. The ACE uses the information in the cookie to direct the content request to the appropriate server. Cookie stickiness is active only during the browser session.
- With HTTP Header Stickiness, a unique portion of the HTTP header may be used to provide stickiness and direct request to the appropriate servers.

With cookie insert, the ACE inserts a cookie on behalf of the server upon the return request, even when the servers are not configured to set cookies. The cookie contains information used by the ACE to ensure persistence to a specific real server.

The following commands define the cookie insert and how they are applied to the proper policy map:

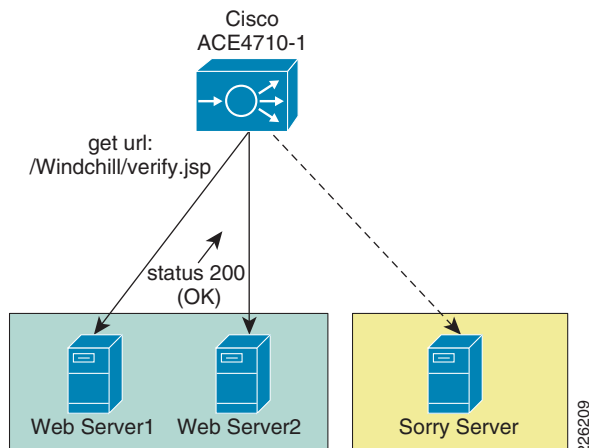
```
sticky http-cookie ACE_COOKIE C-STICKY
 cookie insert browser-expire
 serverfarm SFARM1 backup SFARM2
policy-map type loadbalance first-match L7_VIP_POLICY
 class class-default
 sticky-serverfarm C-STICKY
```

## Health Monitoring

The ACE is able to monitor the state of a server by sending out probes. The ACE verifies the server response and checks for any network problems that can prevent a client to reach a server. Based on the server response, the ACE can place the server in or out of service, and can make reliable load-balancing decisions. The ACE supports 1,000 unique probe configurations, including ICMP, HTTP and other predefined health probes.

The HTTP probe issues an HTTP request to the server for an expected string and status code. The ACE then compares the received response, looking for a string in the received page. If the request fails, the server is marked as failed. [Figure 35](#) shows the probe interaction between the ACE and the web servers.

**Figure 35** Health Monitoring



For the test environment, an HTTP probe was used. The probe is configured to access the **/Windchill/verify.jsp** page and expects a status 200 (OK). The probe is then applied to the serverfarm. The default installation of Windchill does not include the verify.jsp page used in the testing, but can be obtained by contacting PTC Technical Support. The page that is accessed by the probe must be in an anonymously accessible location on the web server.

In the following example, using the *interval* parameter, a probe is sent every 30 seconds to the server. Before the ACE marks a server as failed, it must detect that probes have failed a consecutive number of times. By default when three consecutive probes have failed the ace marks the server as failed. In the lab configuration the *faildetect* parameter was set to two retries.

After the ACE marks a server as failed, it waits a period of time and then sends the probe to the failed server. When a number of consecutive successful probes are received the server is marked as passed. In the lab configuration, failed servers were probed every 30 seconds using the **passdetect interval** command, and three successful probe responses were required before the server was brought back into the serverfarm.

```

http HTTPPROBE
 interval 30
 faildetect 2
 passdetect interval 30
 passdetect count 3
 request method get url /Windchill/verify.jsp
 expect status 200 200
 open 1
!
serverfarm host SFARM1
 probe HTTPPROBE
 rserver SERVER1
 inservice
 rserver SERVER2
 inservice

```

## Layer 7 Load Balancing

Cisco ACE supports both Layer 4 and Layer 7 load balancing. Layer 7 load balancing is deployed in this environment since features such as cookie sticky are enabled. Cisco ACE uses class-map, policy-map, and service-policies to classify and take action on incoming user requests.

For the test environment, the following steps were used to configure load balancing:

- Step 1** Configure the 10.1.41.100 virtual IP (VIP) address using the **class-map** command:

```

class-map match-all L4_VIP_ADDRESS_CLASS
 2 match virtual-address 10.1.41.100 tcp eq www

```

- Step 2** Configure an HTTP class-map for the different objects and server requests. This class-map may be used by some policy-maps that match on specific url contents:

```

class-map type http loadbalance match-any OBJECTS
 3 match http url .*css
 5 match http url .*class
 6 match http url .*jar
 7 match http url .*cab
 8 match http url .*txt
 9 match http url .*ps
 10 match http url .*vbs
 11 match http url .*xsl
 12 match http url .*xml
 13 match http url .*pdfb
 14 match http url .*swf
 22 match http url .*jpg
 23 match http url .*jpeg
 24 match http url .*jpe
 25 match http url .*png
 26 match http url .*gif

```

- Step 3** Configure connection parameters to set for how long objects in the client's browser remain fresh for idle sessions:

```

parameter-map type optimization http EXPIRES
 expires-setting time-to-live 3600
Define a policy-map of type loadbalance to associate the server farm:
policy-map type loadbalance first-match L7_VIP_POLICY
 class class-default
 sticky-serverfarm C-STICKY

```

- Step 4** The following policy-map associates the first-match (L7\_VIP\_POLICY) defined in the previous step.

```

policy-map multi-match L4_VIP_POLICY
 class L4_VIP_ADDRESS_CLASS
 loadbalance vip inservice
 loadbalance policy L7_VIP_POLICY
 loadbalance vip icmp-reply

```

**Step 5** Associate the policy-map to the interface VLAN:

```

interface vlan 411
 description Client-Side interface
 bridge-group 10
 access-group input ALL
 access-group output ALL
 service-policy input L4_VIP_POLICY

```

## ACE Compression

The ACE supports compressing packets to improve site performance and to offload the compression work from the web servers or clients. By performing compression on the ACE, the servers can provide other services to clients and provide faster response times. By default, ACE compression is disabled. When compression is enabled, the appliance compresses data in the HTTP GET or POST responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.

PTC's default configuration for the Apache web server enables web server compression for HTML/TXT content only. Other mime types are not included by default. Web server compression can be completely disabled and offloaded to the ACE. To enable compression on the ACE follow these steps:

**Step 1** Create a policy-map and specify the compression method. In the test environment, gzip compression was enabled.

```

policy-map type loadbalance first-match L7_VIP_POLICY
 class class-default
 compress default-method gzip

```

**Step 2** Specify the parameter map to be used for compression and specify the MIME type. The default is text/\* which includes all text MIME types, such as text/html and text/plain.

```

parameter-map type http HTTP_COMPRESSION
 persistence-rebalance
 compress minimum-size 1024
 compress mimetype "text/*"
 compress mimetype "application/pdf"
 compress mimetype "application/javascript"
 compress mimetype "application/msword"

```

**Step 3** Apply the policy map to the L4\_VIP\_POLICY:

```

policy-map multi-match L4_VIP_POLICY
 class L4_VIP_ADDRESS_CLASS
 appl-parameter http advanced-options HTTP_COMPRESSION

```



## FlashForward Acceleration

The goal of FlashForward is to eliminate the network delays associated with embedded web objects, such as images, style sheets, etc. FlashForward combines the local object storage with dynamic renaming of embedded objects to enforce object freshness within the parent HTML page.

Without FlashForward, the user experiences delays when pages with graphic images load because each object requires validation to ensure that the user has the latest version. Each validation involves an HTTP request from the client to the server, but FlashForward guarantees that clients request only the latest objects and never issue validation requests for objects in the browser cache that the ACE has determined to be valid.

FlashForward places the responsibility for validating object freshness on the ACE rather than on the client, making the process more efficient.

To configure FlashForward on the test environment, the following commands were configured:

---

**Step 1** Configure class-maps to define the objects that will benefit from FlashForward:

```
class-map type http loadbalance match-any OBJECTS
 3 match http url .*css
 5 match http url .*class
 6 match http url .*jar
 7 match http url .*cab
 8 match http url .*txt
 9 match http url .*ps
 10 match http url .*vbs
 11 match http url .*xsl
 12 match http url .*xml
 13 match http url .*pdfb
 14 match http url .*swf
 22 match http url .*jpg
 23 match http url .*jpeg
 24 match http url .*jpe
 25 match http url .*png
 26 match http url .*gif
class-map type http loadbalance match-all PAGE
 2 match http url .*
```

**Step 2** Define a policy-map with the previously defined class-maps:

```
policy-map type optimization http first-match OPTIMIZER
 class OBJECTS
 action OBJECTS parameter EXPIRES
 class PAGE
 action PAGE
```

**Step 3** Create the action-lists for FlashForward optimization:

```
action-list type optimization http OBJECTS
 flashforward-object
action-list type optimization http PAGE
 flashforward
```

**Step 4** Apply the OPTIMIZER policy-map to the L4\_VIP\_POLICY policy-map:

```
policy-map multi-match L4_VIP_POLICY
 class L4_VIP_ADDRESS_CLASS
 optimize http policy OPTIMIZER
```

Packet capture tools such as HTTPWatch or FireBug can be used to verify FlashForward optimization. On a first visit to the web servers, all objects are served from the server, with at response of 200 OK. Once the ACE cache has been populated, the PTC client browser will also download the FlashForward embedded objects referenced in the HTML container page. The HTTPWatch capture in [Figure 36](#) shows that the HTML source of the container page has been modified by changing the embedded object URL:

**Figure 36** FlashForward Capture

|     | Time  | Sent  | Re...  | Method | Result  | Type                  | URL                                                                                                 |
|-----|-------|-------|--------|--------|---------|-----------------------|-----------------------------------------------------------------------------------------------------|
|     | 0.382 | 12528 | 467    | POST   | 200     | text/html;charset...  | http://plm.cisco.com/Windchill/servlet/UIValidationAJAXServlet                                      |
|     | 0.543 | 12529 | 467    | POST   | 200     | text/html;charset...  | http://plm.cisco.com/Windchill/servlet/UIValidationAJAXServlet                                      |
|     | 0.286 | 12916 | 692    | POST   | 200     | text/html;charset...  | http://plm.cisco.com/Windchill/servlet/WizardServlet?ContainerOid=OR%3Awt.inf.library.WTLibrary...  |
| les | 0.969 | 3329  | 180... | POST   | 200     | text/html;charset...  | http://plm.cisco.com/Windchill/netmarkets/jsp/library/listFiles.jsp?wt.reqGrp=fl69czer%3B2726%3B... |
|     | 0.001 | 0     | 0      | GET    | (Cache) | text/css              | http://plm.cisco.com/Windchill/netmarkets/css/nmstyles_CISCO_ACC_FLASHFORWARD_n1.jyq3yfy...         |
|     | 0.006 | 0     | 0      | GET    | (Cache) | text/css              | http://plm.cisco.com/Windchill/WTDefault_CISCO_ACC_FLASHFORWARD_Sesvjp4lo3qnyhmc5ed60...            |
|     | 0.007 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/prototype.js                                   |
|     | 0.001 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/scriptaculous.js                           |
|     | 0.001 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/builder.js                                 |
|     | 0.000 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/effects.js                                 |
|     | 0.000 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/dragdrop.js                                |
|     | 0.001 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/controls.js                                |
|     | 0.001 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/slider.js                                  |
|     | 0.001 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/templates/cadx/common/triUtils.js                                    |
|     | 0.000 | 0     | 0      | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/templates/HTML/templateutl/submitFunctions.js                        |

On a repeat visit, the browser should not validate objects in its cache, therefore response time is improved and the number of requests to build a page is reduced. FlashForward objects are served from the local browser's cache, as opposed to the web server. A new capture should show that only a few client requests are made to the web server and that most content is served from the browser's cache. The number of 304 responses (Not Modified) should also be reduced. [Figure 37](#) shows a capture with all requests being served from the local browser's cache.

**Figure 37** FlashForward Optimization

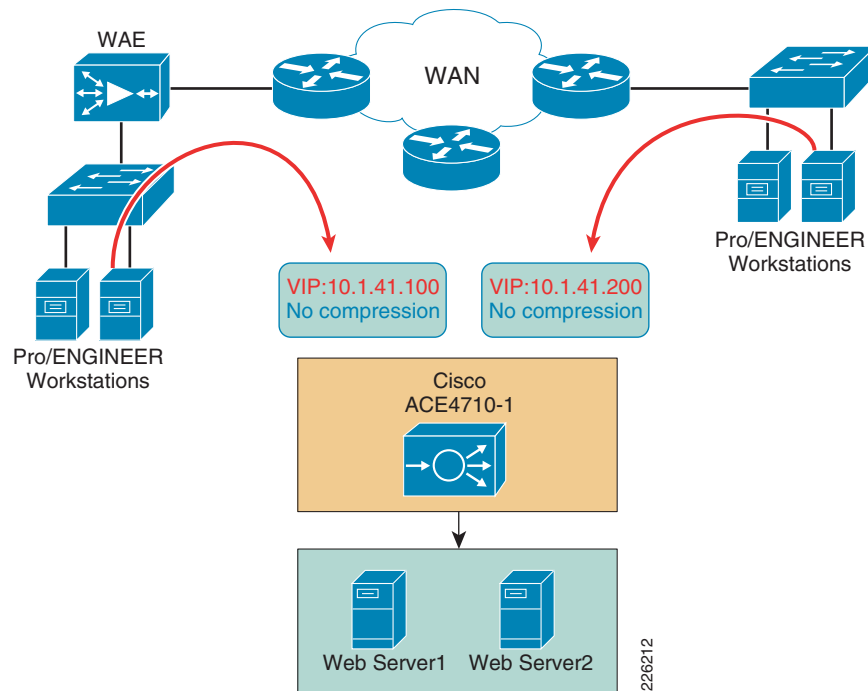
|  | Time  | Sent | Re... | Method | Result  | Type                  | URL                                                                                      |
|--|-------|------|-------|--------|---------|-----------------------|------------------------------------------------------------------------------------------|
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/main.js                         |
|  | 0.001 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/calendar.js                     |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/vtcore/js/com/ptc/core/ca/web/misc/content.js             |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/feedback.js                     |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/cad.js                          |
|  | 0.001 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/components/wizard.js                |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/vtcore/js/com/ptc/core/components/menu.js                 |
|  | 0.001 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/attachments/attachments.js          |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/ui/CommonResources/javascript/statusMessage.js            |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/templates/uwgm/cadx/openincadtool/openincadtool.js        |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/templates/uwgm/cadx/caddoc/contentcompare.js              |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/templates/htmlcomp/location/browseFoldersUtils.js         |
|  | 0.001 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/utl/validate.js                     |
|  | 0.000 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/netmarkets/javascript/components/driverAttributesSetup.js |
|  | 0.001 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/vtcore/js/com/ptc/core/cancel/cancel.js                   |
|  | 0.001 | 0    | 0     | GET    | (Cache) | application/javasc... | http://plm.cisco.com/Windchill/templates/cadx/common/triUtils.js                         |

## ACE Implementation Caveats or Limitations

### WAAS and ACE Compression

During testing, it was determined that compression should not be enabled at both WAAS and ACE when both are part of the traffic flow. When both WAAS and ACE are part of the traffic flow compression, should be enabled on the WAAS and disabled on the ACE. In a future release, the ACE will be able to determine what packets have already been compressed by the WAAS and disable compression for those flows. With the tested software releases, a manual configuration must take place for specific flows.

ACE Compression still provides valuable performance improvements for remote sites that do not have WAAS deployed. A simple way to do this is to create a separate VIP address for sites that want to benefit from ACE compression but have not deployed WAAS, as shown in [Figure 38](#).

**Figure 38** ACE and WAAS Compression

## FlashForward

The benefits of FlashForward are more apparent on applications that contain objects embedded within HTML pages or pages with graphic objects that can be served from a local browser. PTC Windchill provides a very dynamic environment and many pages are created dynamically.

While FlashForward is able to accelerate applications and reduce requests to the server, the results did not show an overall improvement for PTC Windchill within the lab testing environment. PTC has customers that have implemented a similar equivalent to FlashForward within their web server configuration to address these performance concerns and have seen significant improvements in cached object verifications. It is anticipated that the use of FlashForward will provide benefits for users that may experience these issues and be transparent for users that would not notice under their working conditions, but the lab testing did not provide the opportunity to calculate the benefits of using FlashForward, since a full regression test was not performed to identify other areas that may impact PTC applications.

During testing, an issue with FlashForward was found and bug CSCsu90166 was filed. The bug showed the ACE leaving client connections open and, therefore, blocking subsequent file uploads until a timeout occurred. This bug only has an impact when WAAS and ACE are enabled.

Until the bug is fixed, the following workarounds should be considered:

- Increase the server connection idle timeout to something higher than 15 seconds, the ACE's default. This would prevent the server from sending a FIN and getting connections in a frozen state.
- Add a NAT-pool with PAT. This causes the ACE to generate a new IP and source port, as opposed to reusing established connections. The following configuration defines a NAT-pool with IP address 10.1.41.60 and how it is applied to the policy-map.

```
interface vlan 41
 description Server-Side interface
```

```

bridge-group 10
access-group input ALL
nat-pool 1 10.1.41.60 10.1.41.60 netmask 255.255.255.255 pat
!
policy-map multi-match L4_VIP_POLICY
class L4_VIP_ADDRESS_CLASS
loadbalance vip inservice
loadbalance policy L7_VIP_POLICY
nat dynamic 1 vlan 41

```

## Troubleshooting Commands

The following commands may be useful when troubleshooting the ACE configuration:

- **show stats**—Displays the statistical information relating to the operation of the Cisco ACE.
- **show service-policy *policy\_name***—Displays the statistics for service policies enabled globally within a context or on a specific interface.
- **show serverfarm *name* detail**—Displays the summary or detailed server-farm statistics.
- **show rserver *rserver\_name* detail**—Displays the summary or detailed statistics for a named real server or for all real servers.
- **show probe**—Displays the probe information including script probes.
- **show arp**—Displays the current active IP address-to-MAC address mapping in the ARP table, statistics, or inspection or timeout configuration.
- **show context**—Verifies the auto-sync configuration of all contexts.
- **show ft group status**—Verifies FT status of all configured context in the Cisco ACE.
- **show ft peer detail**—Verifies the state of FT peering.
- **show resource usage**—Displays the resource usage for each context.

## Testing Results and Conclusions

The optimization tests were performed on a full working copy of PTC Windchill, Oracle database and web servers operating on virtual machines. A full data center implementation and remote engineering site were configured to provide the proper connectivity. Cisco ACE, WAAS, and WAAS Mobile devices were also tested in different configurations to validate the optimization of PTC applications.

WAAS and WAAS Mobile optimizations are noted in the WAN as well as the end-user experience of applications. Application performance is measured depending on who is the consumer of the data. To the end user, the application response time is important, since performance is evaluated by the user experience while to the network administrator low bandwidth utilization and network performance are important.

One of the most compelling reasons to use the Cisco WAAS is to provide the user with as close to LAN-like response as possible, with the PTC application residing over the WAN in the data center. This implies that the user and application response time become critical metrics. End-to-end latency times (application client/server latency plus network latency) from the client perspective can be measured easily by capturing download times and perceived download rates.

## Test Methodology

A series of test were performed to stimulate PTC Windchill and Pro/ENGINEER users during a typical working day. The following three main categories were tested:

- HTTP operations
- HTTP content operations
- Folder browsing operations

## Pro/ENGINEER Testing

- Adding an assembly to a workspace
- Uploading a new assembly

The following three types of tests were conducted for each category:

- **Native WAN Tests:** These tests show the native performance between the client and server over the WAN. Native WAN testing can be achieved by disabling the WAEs or by configuring them in pass-through mode (for WAAS) and by exiting the client application (for WAAS Mobile). For the inline WAE at the engineering site, execute the following commands:

```
(config)#interface inlinegroup 1/0
(config-if)#shutdown
```

For the data center WAE, disable WWCP at the core switches:

```
(config)#no ip wccp 61
(config)#no ip wccp 62
```

- **Cold Test:** Cold tests capture the performance over the first transfer through the WAAS and WAAS Mobile. The performance of transport optimization, data compression and caching, and corresponding application optimizers for the application are captured. The first transfer will show some performance improvement and a reduction in bandwidth utilization.
- **Warm Test:** Warm tests show full WAAS and WAAS Mobile performance of transport optimization, data compression and caching. This is done by repeating the same PTC operation. The second transfer will show dramatic improvement in performance as it makes use of a ‘hot’ cache.

Additional tests were performed to focus on compression, window sizing, and acceleration features. Optimization with SSL traffic is planned for a future release of this deployment guide.

## Application Test Results

The PTC Windchill PDMLink tests were performed using Internet Explorer and HTTPWatch for data collection. The purpose of the test was to stimulate a typical PTC environment, with remote users dispersed throughout the world and the PTC application deployed in a centralized data center.



### Note

The following results are comparative in nature and were obtained under controlled lab conditions; therefore, a customer should not expect to obtain the same exact results in their environment.

[Table 3](#) represents a summary of the results obtained for each group of PTC operations. The summary was collected from WAAS and WAAS Mobile over a T-1, 100ms delay. Each result represents numerous combinations of tests. Detailed charts are presented in the next few sections.

**Table 3**      **Summary Test Results**

| <b>WAAS</b>             |                          |                       |
|-------------------------|--------------------------|-----------------------|
|                         | <b>Improvement Range</b> | <b>x Times Faster</b> |
| HTTP Operations         | 8% to 92%                | 6                     |
| HTTP Content Operations | 69% to 99%               | 41                    |
| Folder Browsing Testing | 33 to 90%                | 5                     |
| Pro/ENGINEER Operations | 90 to 92%                | 11                    |
|                         |                          |                       |
| <b>WAAS Mobile</b>      |                          |                       |
|                         | <b>Improvement Range</b> | <b>x Times Faster</b> |
| HTTP Operations         | 20% to 90%               | 4                     |
| HTTP Content Operations | 64% to 100%              | 95                    |
| Folder Browsing Testing | 47% to 90%               | 5                     |
| Pro/ENGINEER Operations | 91% to 97%               | 25                    |

## WAN Simulation

For WAAS testing, two different bandwidth speeds were used during testing, each one with different latency and drop capabilities (see [Table 4](#)). The purpose was to stimulate a typical intra-continental circuit and a slower intercontinental circuit.

**Table 4**      **WAN Simulation Speeds**

| <b>Location</b>   | <b>Bandwidth</b> | <b>Latency</b> | <b>Drop</b> |
|-------------------|------------------|----------------|-------------|
| Intra-continental | T1               | 100ms          | 1%          |
| Inter-continental | T1               | 400ms          | 1%          |

For WAAS Mobile testing, a T-1 connection with 100ms latency and 1 percent packet loss was used to simulate a typical Internet connection. It should be noted that remote access network characteristics vary widely depending on the type of internet connection (Wi-Fi, 3G, DSL, cable, and satellite), creating dramatic performance differences for remote users. The results in this test are indicative of a best-case Internet connection; the improvement for other connections would be even greater, as the unaccelerated test times would increase as network conditions degrade.

## HTTP Operations—WAAS

This group of tests focused on typical user operations performed with a web browser. The optimization benefits become apparent when WAAS is part of the traffic flow. [Figure 39](#) shows the Home Overview page for PTC Windchill.

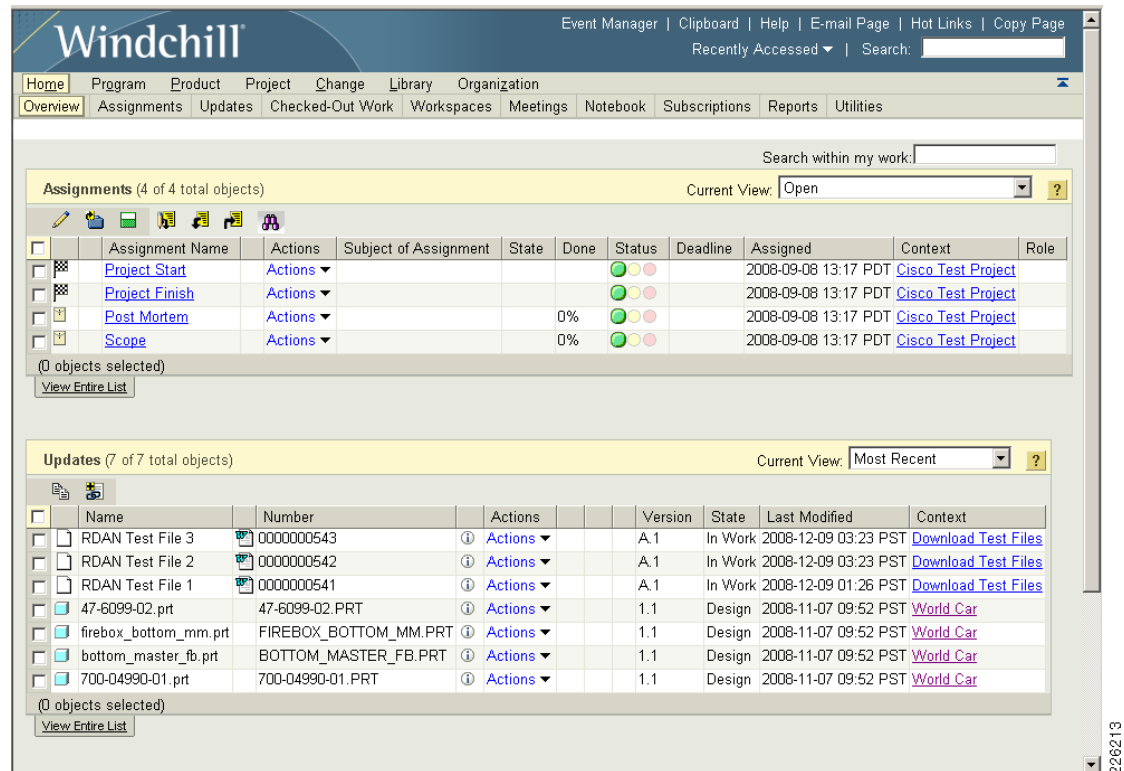
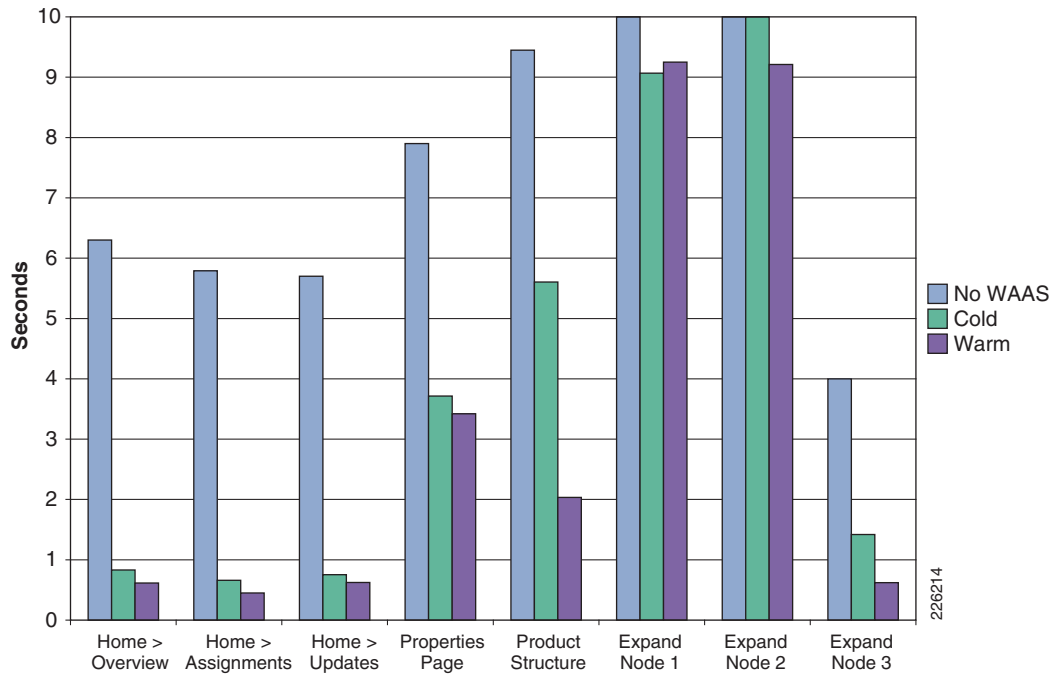
**Figure 39** PTC Windchill HTTP Operations

Table 5 shows the number of objects used for some of the HTTP operations.

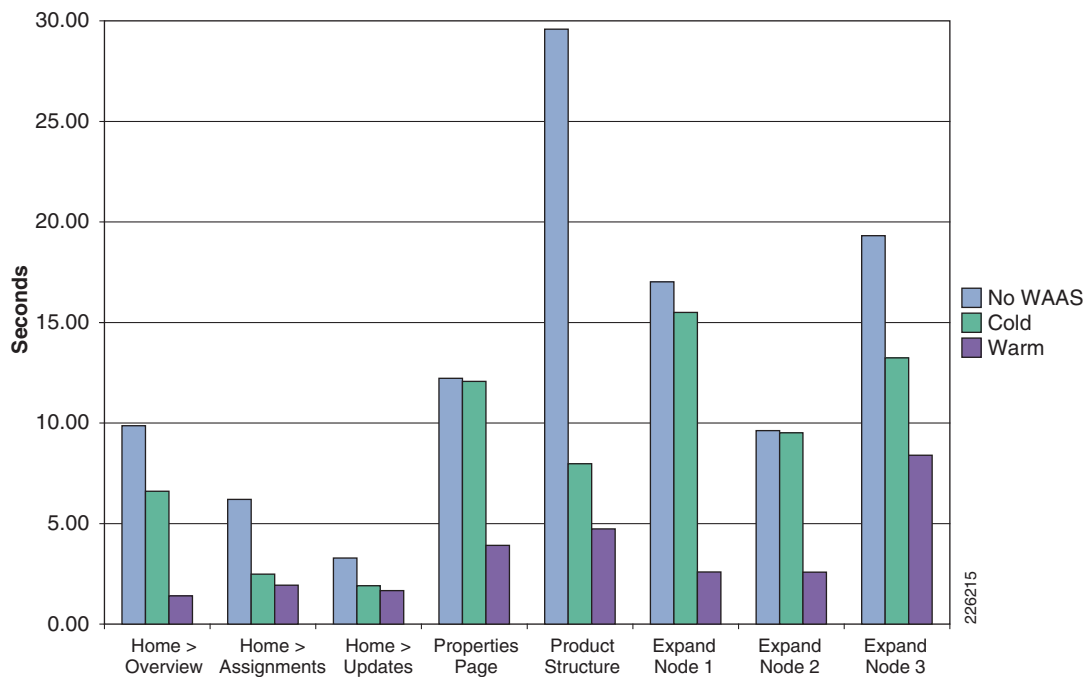
**Table 5** Number of Objects

| Windchill Test    | Total Objects |
|-------------------|---------------|
| Product Structure | 5,218         |
| Expand Node 1     | 357           |
| Expand Node 2     | 544           |
| Expand Node 3     | 92            |

Figure 40 shows the performance over a T-1, 100ms delay while Figure 41 shows the performance over a T-1, 400ms delay.

**Figure 40** HTTP Operations – T1 100ms 1% Drop

The results in [Figure 41](#) show the impact that WAAS has on a T1 400ms, and shows that the warm results are very similar to a T-1 100ms delay.

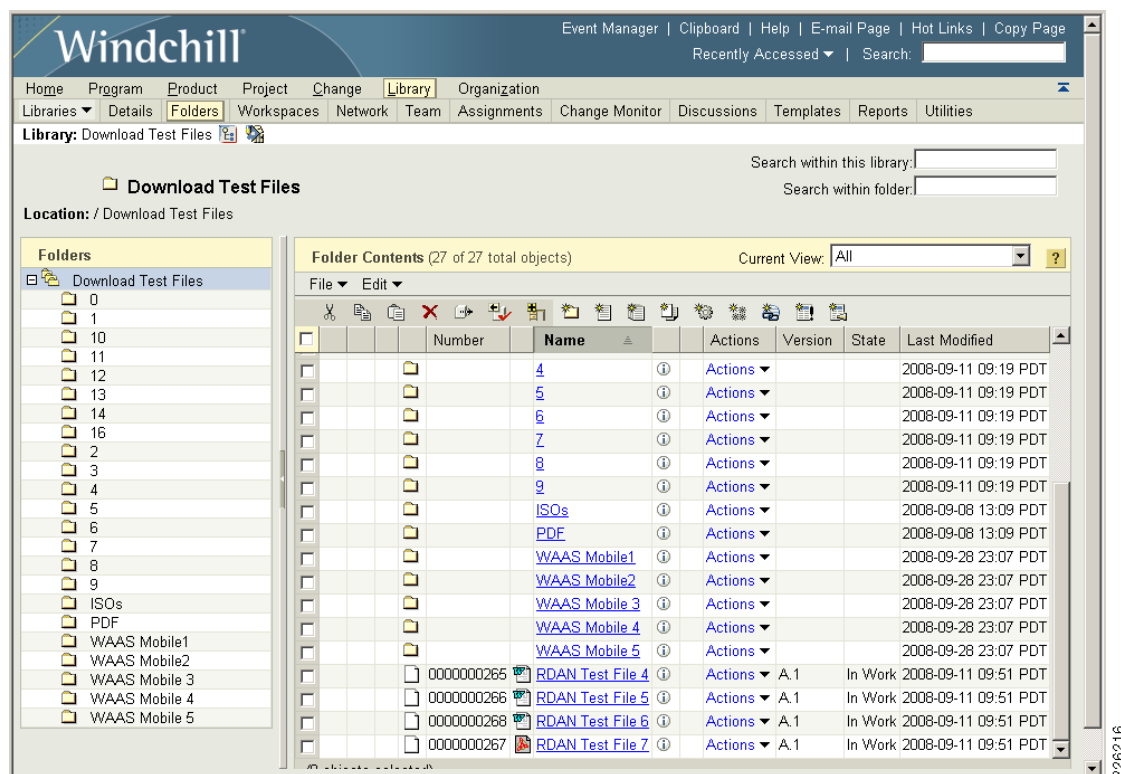
**Figure 41** HTTP Operations - T1 400ms 1% Drop



## HTTP Content Operations—WAAS

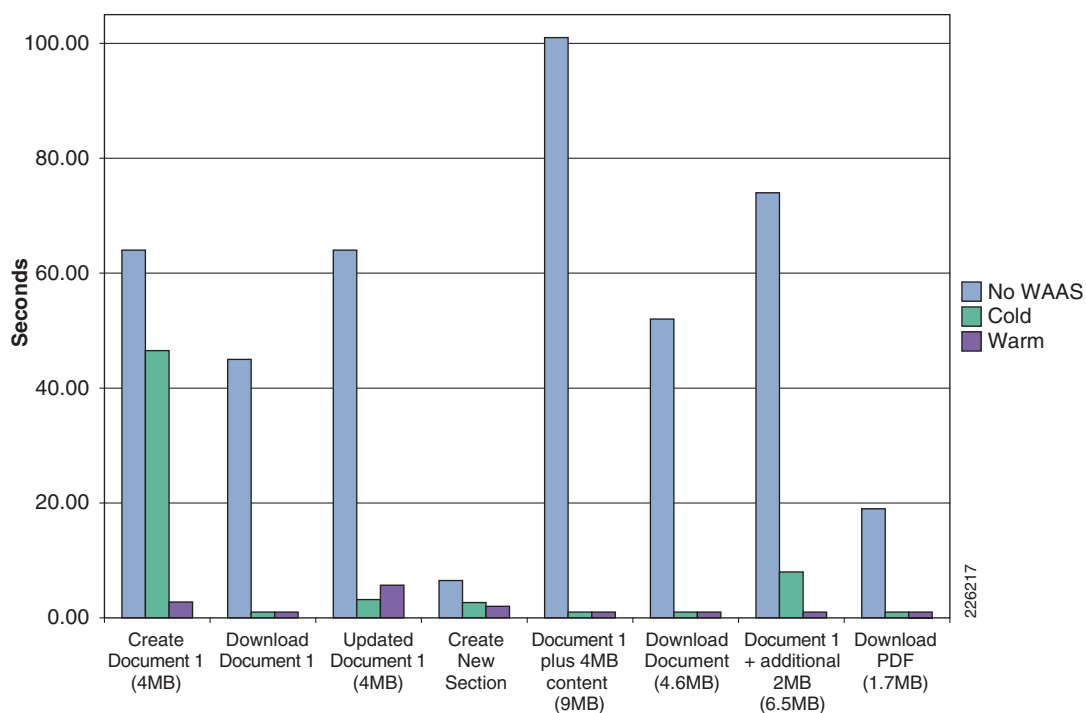
Typical file upload/download operations can benefit from application acceleration, particularly large CAD files. Once a file has been transferred once, WAAS is able to identify any portion of the document and only transfer the portions of the document that have been updated or modified. [Figure 42](#) shows the **Library > Folders** screen used in the test environment.

**Figure 42** PTC Windchill Content Operations

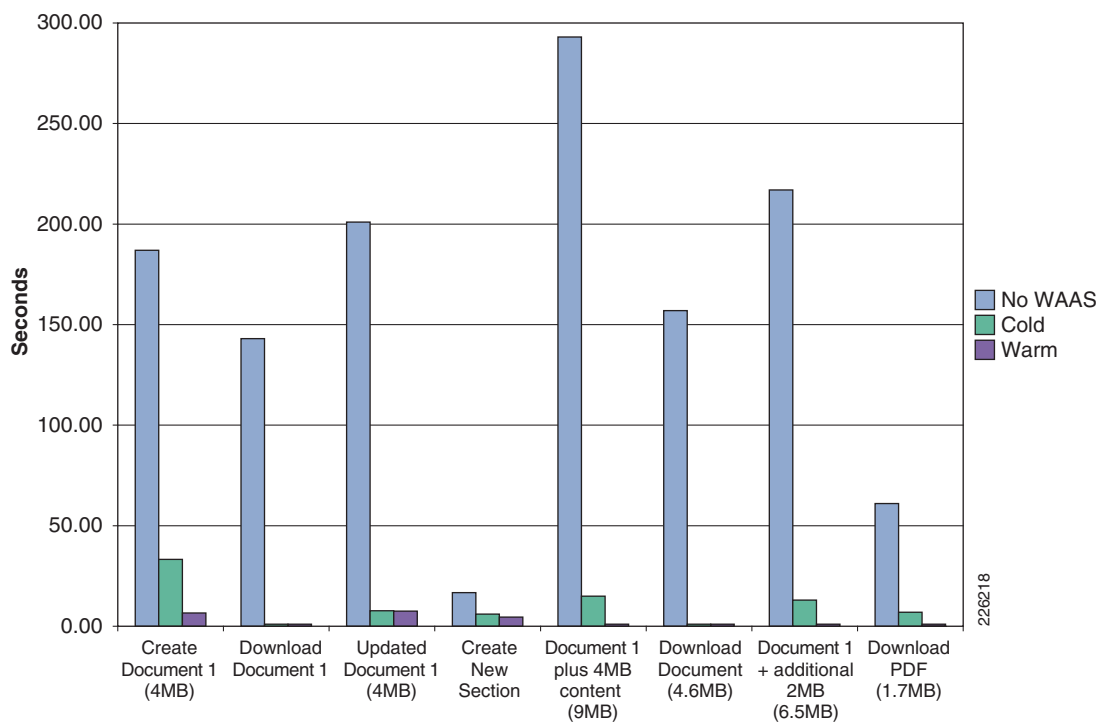


The following test results include creating a document and making updates to the different sections of the document. [Figure 43](#) and [Figure 44](#) show details for different T-1 configurations.

**Figure 43** HTTP Operations - T1 100ms 1% Drop



**Figure 44** HTTP Operations - T1 400ms 1% Drop

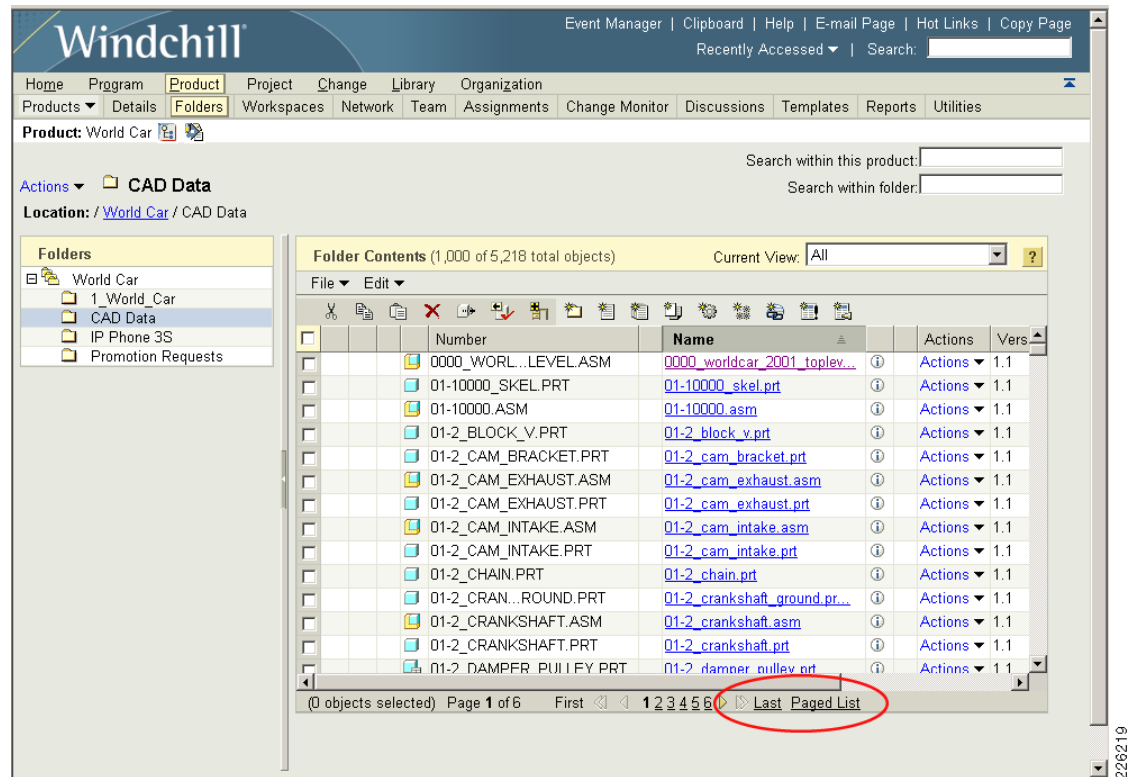


## Folder Browsing Operations —WAAS

The following tests focus on capturing the time that it takes to retrieve folder lists from the server. This function can be slow since all data is retrieved from the origin server. By default, only 200 items are displayed on a page, but selecting “Full List” retrieves the complete list of items from the server (5,218 total objects).

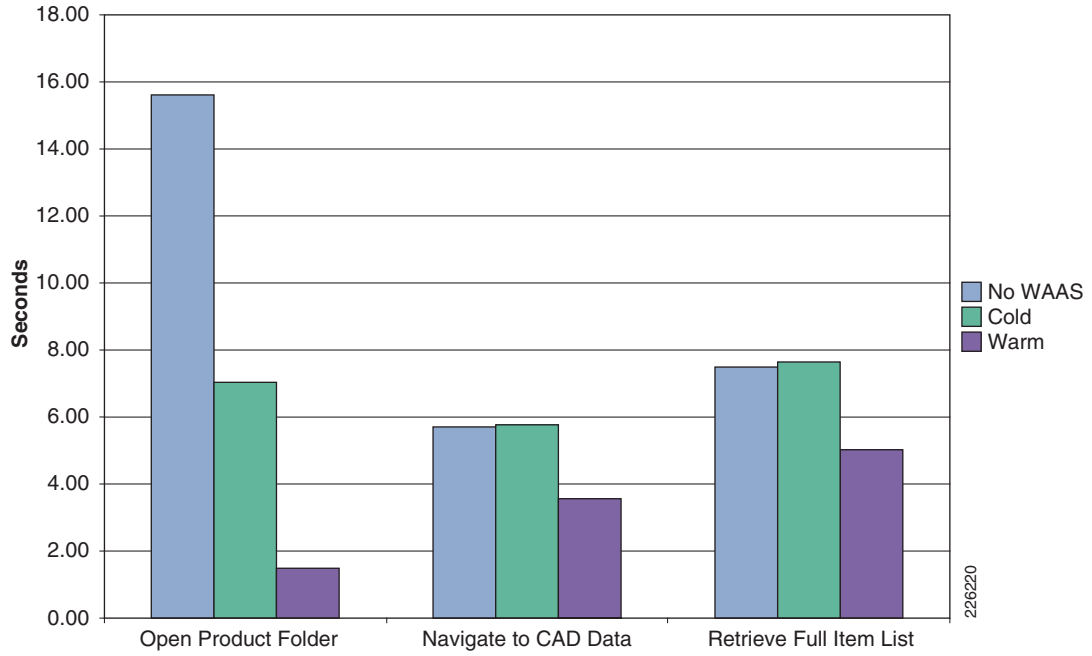
Figure 45 shows the folders used in the test environment and how to select the Paged List or Full List of objects.

**Figure 45** PTC Windchill - Folder Operations

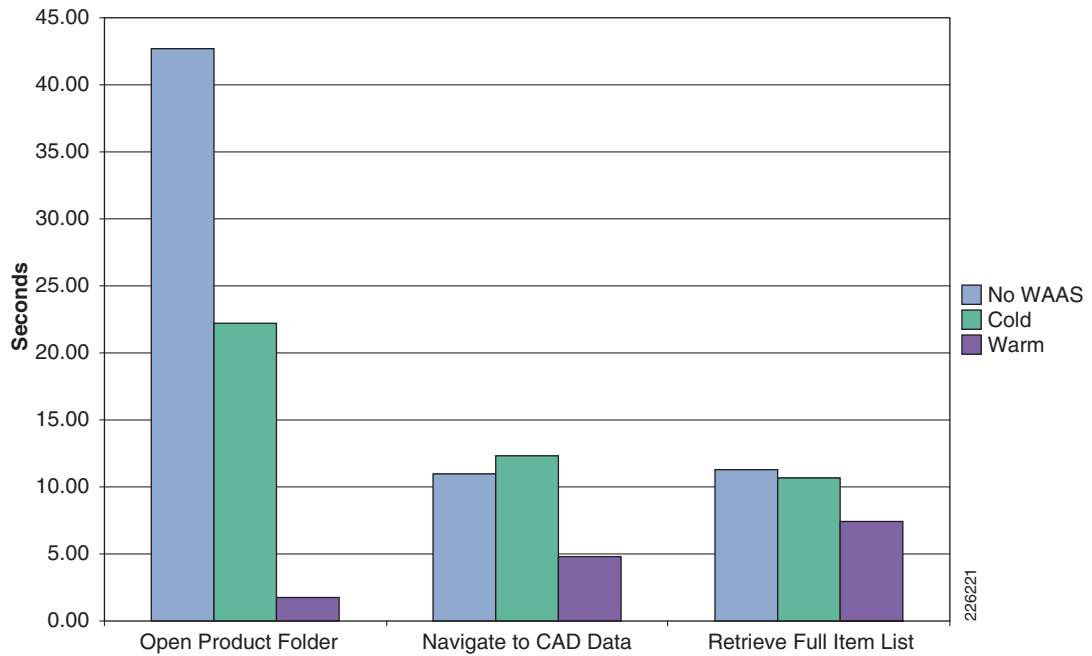


The test results in Figure 46 and Figure 47 show the results from different T-1 configurations.

**Figure 46** Folder Browsing - T1 100ms 1% Drop



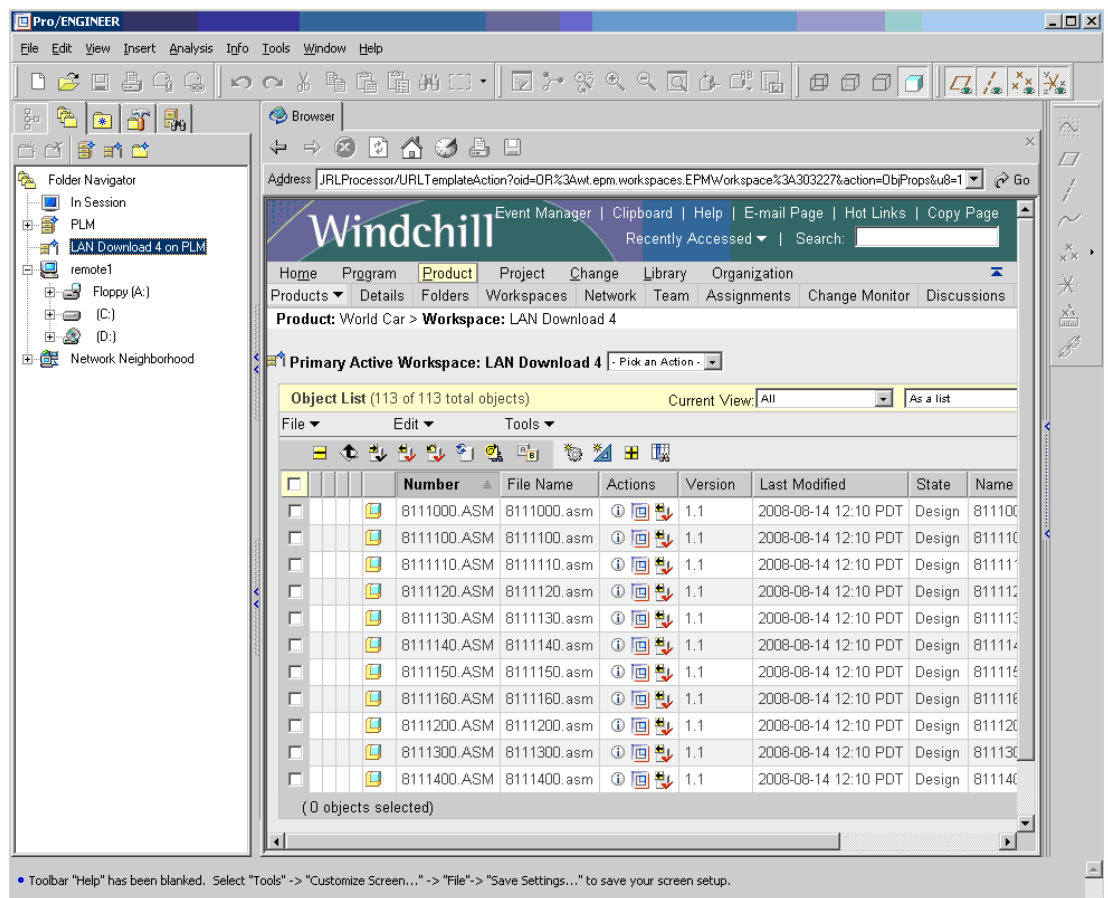
**Figure 47** Folder Browsing - T1 400ms 1% Drop



## Pro/ENGINEER Testing—WAAS

The following tests show typical operations performed by Pro/ENGINEER users working with different assemblies. An **Add to Workspace** operation was performed for a subset of the PTC World Car assembly. A subsequent workspace operation was performed uploading a Cisco provided Pro/ENGINEER assembly for a IP Phone product design. [Figure 48](#) shows the Pro/ENGINEER Wildfire workspace.

**Figure 48** Pro/ENGINEER Workspace



The tests results in [Figure 49](#) show typical operations performed by Pro/ENGINEER users working with different assemblies and adding a subassembly of the world car or uploading the Cisco IP phone. The results were gathered using different T-1 configurations.

**Figure 49** *Pro/ENGINEER Testing - T1 100ms 1% Drop*

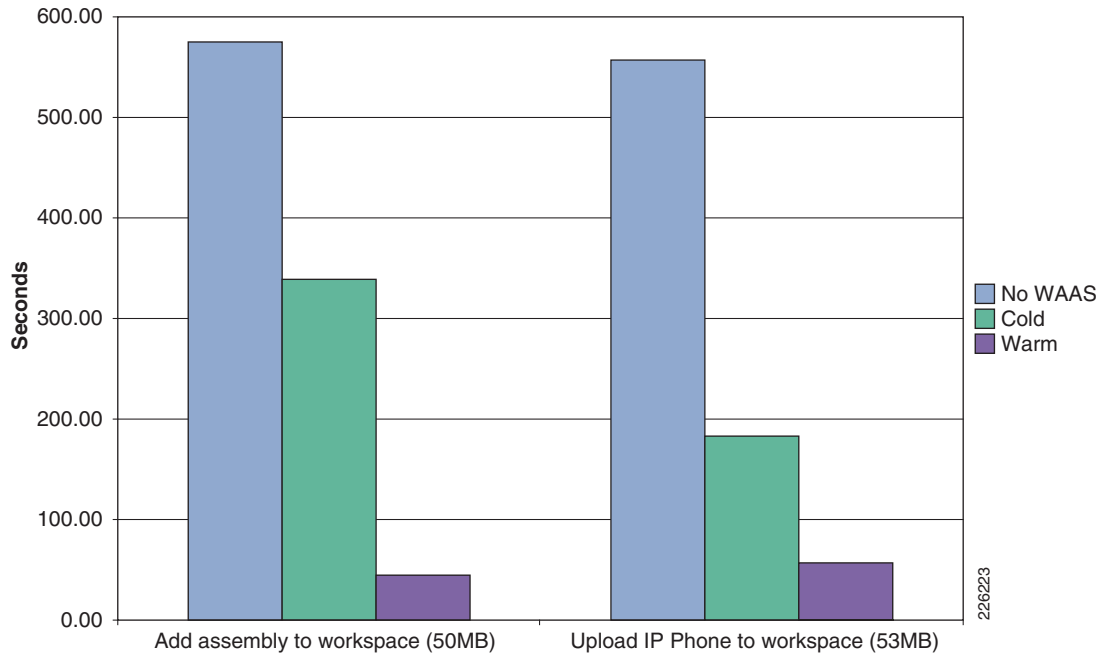
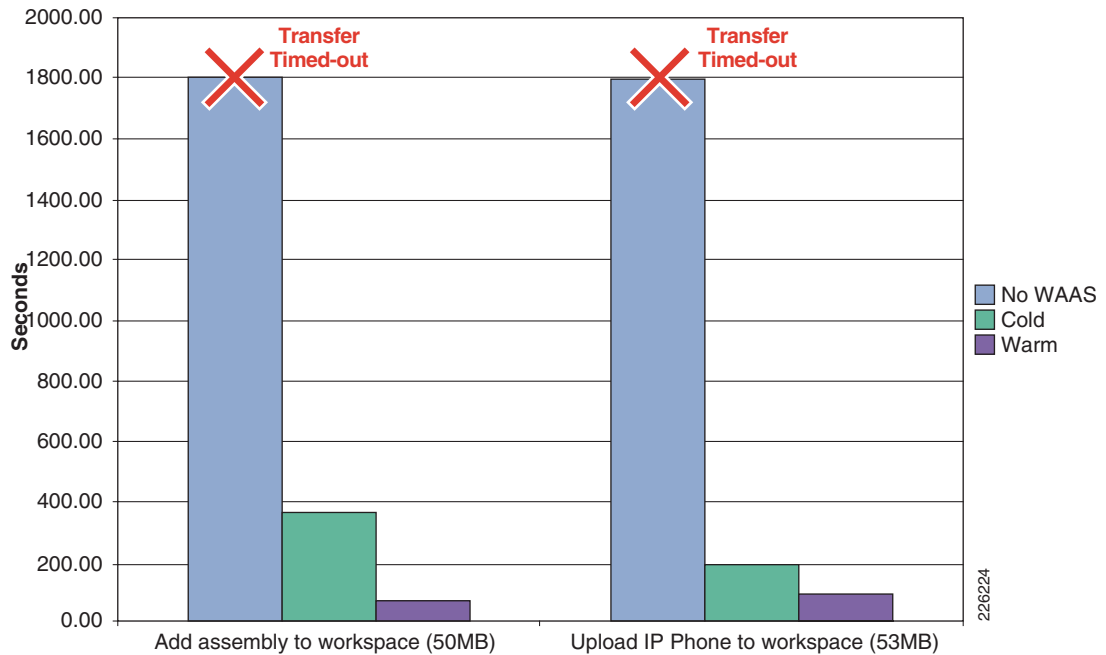


Figure 50 shows the results for a T-1 400 ms delay. For the tests without WAAS, the transactions were unable to complete and the application timed-out after 22 minutes.

**Figure 50** *Pro/ENGINEER Testing - T1 400ms 1% Drop*



## WAAS Mobile Test Results

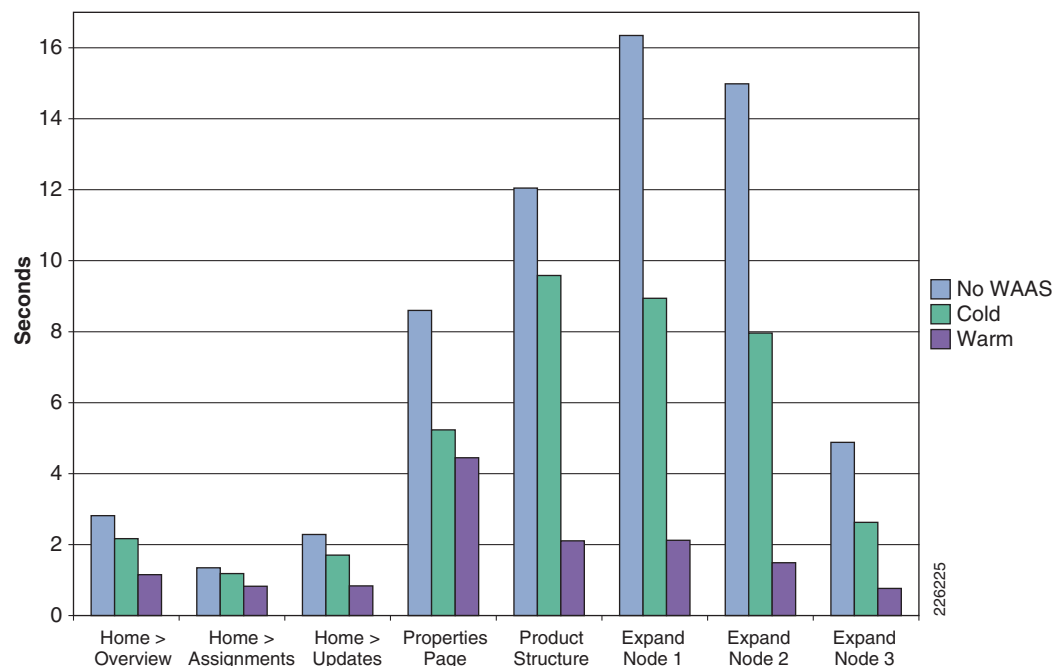
The WAAS Mobile tests were also grouped in typical user operations. The client workstation was configured with 1 GB of local cache, and the WAN simulation consisted of T-1 with 100ms delay and 1 percent packet drop.

The results show that WAAS Mobile also provides similar optimization to WAAS, even when the remote clients connect through the Internet and a VPN tunnel. The results should also demonstrate that users in small offices where WAAS is not deployed could also benefit from the acceleration benefits provided by WAAS Mobile.

### HTTP Operations—WAAS Mobile

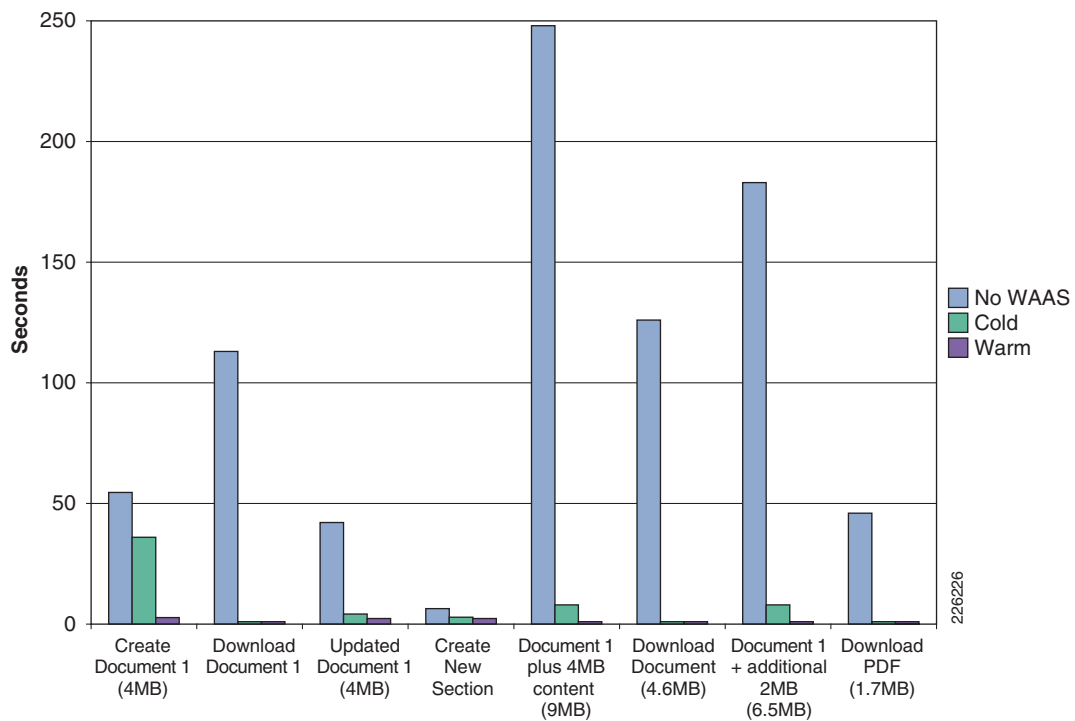
Figure 51 shows the results of typical user operations performed with a web browser using WAAS Mobile.

**Figure 51** WAAS Mobile HTTP Operations



### HTTP Content Operations—WAAS Mobile

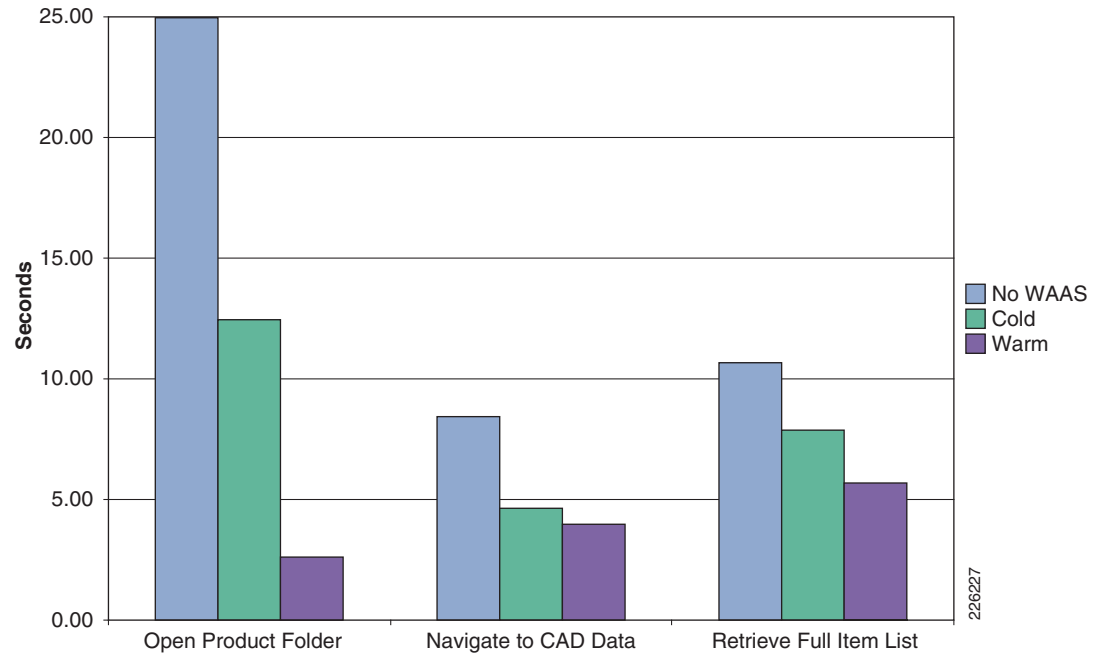
Figure 52 shows the results of creating a document and updating different sections of it using WAAS Mobile.

**Figure 52** *WAAS Mobile Content Operations*

## Folder Operations—WAAS Mobile

Figure 53 shows the results when retrieving folder lists from the server using WAAS Mobile. This function can be slow since all data is retrieved from the origin server. By default, only 200 items are displayed on a page, but selecting **Full List** shows that the complete list of items contains 5,218 objects.



**Figure 53** *WAAS Mobile Folder Operations*

## Pro/ENGINEER—WAAS Mobile

Figure 54 shows typical operations performed by remote Pro/ENGINEER users working with different assemblies and adding them to the workspace.

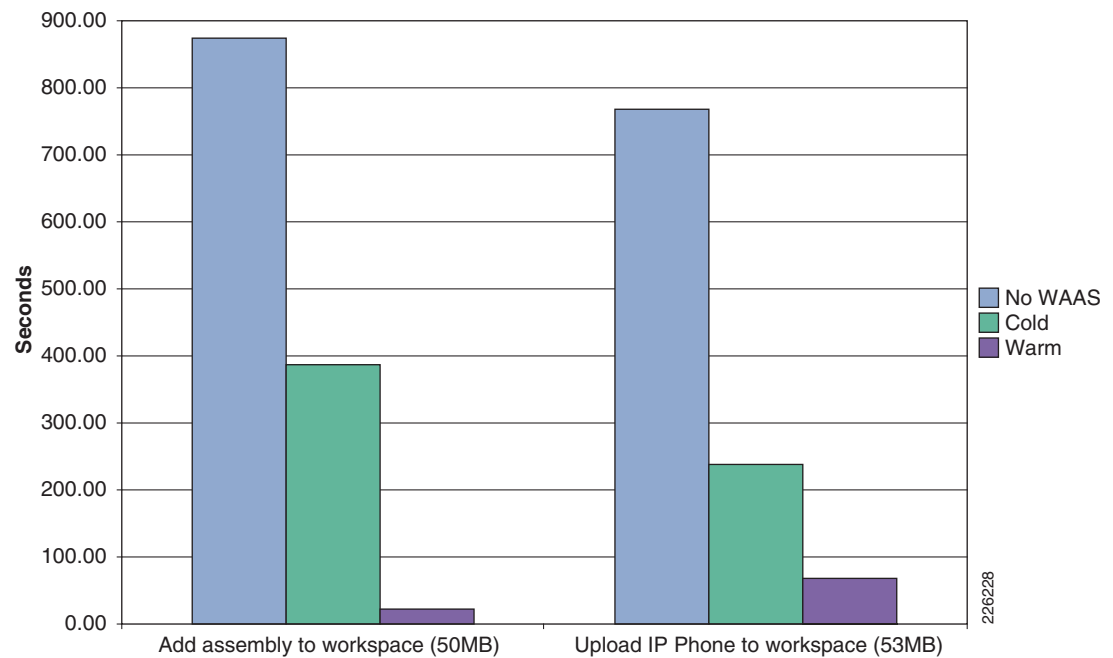
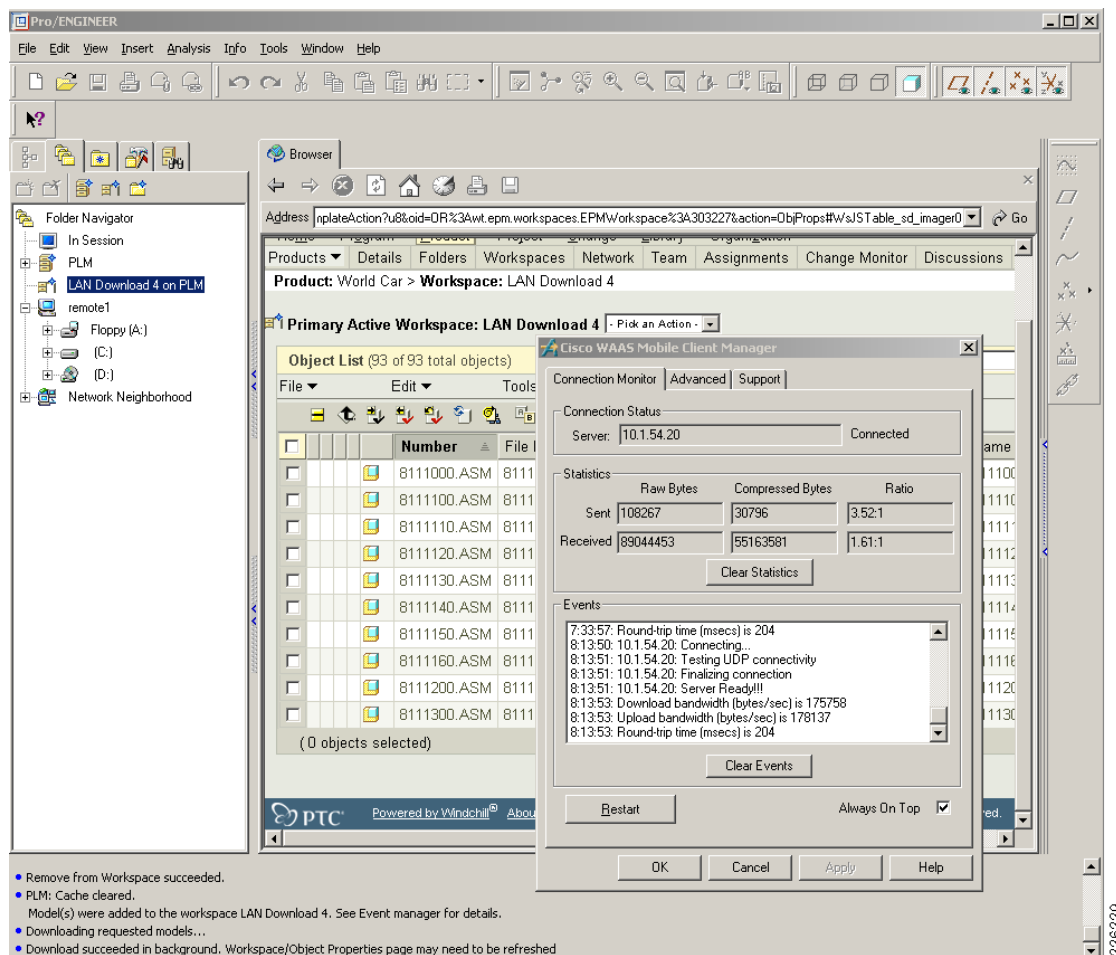
**Figure 54** *WAAS Mobile Pro/ENGINEER Operations*

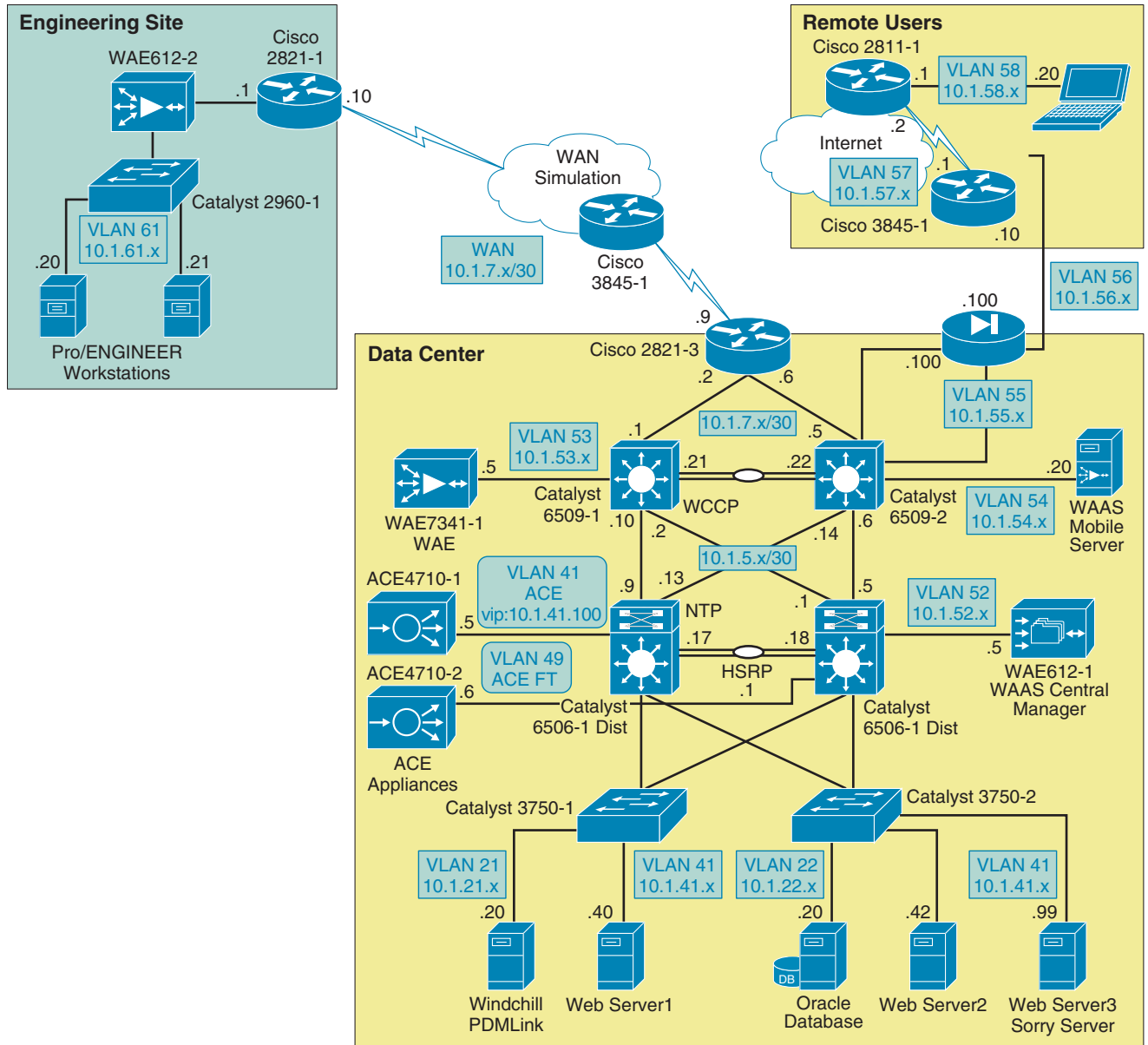
Figure 55 shows the WAAS Mobile statistics while a Pro/ENGINEER operation is taking place. The Figure 55 also shows that the client is connected to the WAAS Mobile at server at 10.1.54.20 and the current compression ratios.

**Figure 55** *Pro/ENGINEER and WAAS Mobile*



# Appendix A—Test Environment

**Figure 56** Full Network Topology



## Hardware and Software Releases

Table 6 lists the PTC software used in this solution.

**Table 6** *PTC Software*

| Software              | Release  |
|-----------------------|----------|
| PTC Windchill PDMLink | 9.0 M040 |
| Pro/ENGINEER Wildfire | 3.0      |

Table 7 lists the Cisco WAAS and ACE software releases used in this solution.

**Table 7** *WAAS/ACE*

| Device          | Location         | Software Release |
|-----------------|------------------|------------------|
| ACE 4710        | Data Center      | A3(1.0)          |
| WAE-612         | Central Manager  | 4.1.1            |
| WAE-612         | Engineering Site | 4.1.1            |
| WAE-7341        | Data Center      | 4.1.1            |
| WAAS-MBL-SVR_SW | Data Center      | 3.4.1.1488       |
| WAAS-MBL-LIC##  | Remote User      | 3.4.1.1588       |

Table 8 lists the Cisco Catalyst switches used in this solution.

**Table 8** *Catalyst Switches*

| Device                     | Location         | Software Release |
|----------------------------|------------------|------------------|
| 6509 Core Switches         | Data Center      | 12.2(33)SHX3     |
| 6509 Distribution Switches | Data Center      | 12.2(33)SHX2a    |
| 3750 Access Switches       | Data Center      | 12.2(25)SEE4     |
| 2960 Access Switch         | Engineering Site | 12.2(37)SE1      |

Table 9 lists the Cisco ISR routers used in this solution.

**Table 9** *Cisco ISR Routers*

| Device                 | Location         | Software Release |
|------------------------|------------------|------------------|
| 2821 WAN ISR Router    | Data Center      | 12.4(12c)        |
| 2821 Remote ISR Router | Engineering Site | 12.4(12c)        |
| 2821 Internet Router   | Internet         | 12.4(12c)        |
| 2811 Internet Router   | Internet         | 12.4(3i)         |

Table 10 lists the Cisco ASA Adaptive Security Appliance used in this solution.

**Table 10 Cisco ASA Adaptive Security Appliance**

| Device             | Location    | Software Release |
|--------------------|-------------|------------------|
| ASA 5540 Appliance | Data Center | 8.0(3)           |

The following platforms are recommended for use with Cisco WAAS and the WCCP services:

- Cisco Integrated Services Routers (1800, 2800, 3800)
- Cisco 3700, 7200 (NPE-400, NPE-G1, and NPE-G2 only), 7600, and ASR 1000 Series Routers
- Cisco Catalyst 3560 and 3750 Series Switches
- Cisco Catalyst 4500 and 4948 Series Switches
- Cisco Catalyst 6500 Series Switches

Table 11 lists the key capabilities of each platform.

**Table 11 WCCP Platform Support**

| Platform                     | OS Version   | Forwarding | Return    | Assignment   | Direction | Redirect List |
|------------------------------|--------------|------------|-----------|--------------|-----------|---------------|
| IOS (Software-based)         | < 12.4(20)T  | GRE        | GRE       | Hash         | In or Out | Yes           |
| IOS (Software-based)         | > 12.4(20)T  | GRE or L2  | GRE or L2 | Hash or Mask | In or Out | Yes           |
| ASR 1000 Series              | 2.1 XE       | GRE or L2  | GRE or L2 | Mask         | In        | Yes           |
| Cisco 7600 Series            | 12.2(18)SXD1 | GRE or L2  | GRE       | Hash or Mask | In or Out | Yes 1         |
| Catalyst 3560/3750           | 12.2(37)SE   | L2         | GRE or L2 | Mask         | In        | Yes 2         |
| Catalyst 4500/4948           | 12.2(31)SG   | L2         | L2        | Mask         | In        | No            |
| Catalyst 6500 (Sup2)         | 12.1(13)E    | GRE or L2  | GRE       | Hash or Mask | In or Out | Yes 1         |
| Catalyst 6500 (Sup32/Sup720) | 12.2(18)SXD1 | GRE or L2  | GRE or L2 | Hash or Mask | In or Out | Yes 1         |

1. The following options are supported in the redirect list:
  - Source and destination IP addresses (host or subnet)
  - Individual source and destination port numbers (**eq** operator only)
  - DSCP, ToS and precedence operators (**dscp**, **precedence**, and **tos** keywords)
  - IP options (**options** keyword)
  - Logging
2. Only **permit** entries are supported.

The following platforms support WCCP, but their implementation is not compatible with WAAS:

- Catalyst 6500, Sup1a
- Cisco PIX/ASA Firewalls

- Catalyst 3550 Series Switch

## Appendix B—Reference Documents

- *Enterprise Data Center Wide Area Application Services (WAAS) Design Guide*  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/WAASDC11.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/WAASDC11.html)
- *Enterprise Branch Wide Area Application Services Design Guide (Version 1.1)*  
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/WAASBr11.html>
- *Cisco WAAS Mobile Administration Guide*  
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/waas\\_mobile/v3.4/configuration/administration/guide/CiscoWAASMobile\\_AG3.4.pdf](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas_mobile/v3.4/configuration/administration/guide/CiscoWAASMobile_AG3.4.pdf)
- *Cisco ACE 4700 Series Application Server Load-Balancing Configuration Guide*  
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/data\\_center\\_app\\_services/ace\\_appliances/vA3\\_1\\_0/configuration/slb/guide/slbgd.html](http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA3_1_0/configuration/slb/guide/slbgd.html)
- *Enterprise Class Teleworker (ECT) Solution Reference Network Design (SRND)*  
[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/guide\\_c07\\_458724.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/guide_c07_458724.html)

## Appendix C—Device Configurations

### Cisco ACE Configurations

#### Admin Context

```

Generating configuration....
resource-class R1
 limit-resource all minimum 0.00 maximum unlimited
 limit-resource sticky minimum 10.00 maximum equal-to-min

boot system image:c4710ace-mz.A3_1_0.bin
boot system image:c4710ace-mz.A1_8_0a.bin

login timeout 0

hostname ACE4710-1
interface gigabitEthernet 1/1
 channel-group 1
 no shutdown
interface gigabitEthernet 1/2
 speed 1000M
 duplex FULL
 channel-group 1
 no shutdown
interface gigabitEthernet 1/3
 speed 1000M
 duplex FULL
 channel-group 1
 no shutdown

```

```

interface gigabitEthernet 1/4
 speed 1000M
 duplex FULL
 channel-group 1
 no shutdown
interface port-channel 1
 switchport trunk native vlan 41
 switchport trunk allowed vlan 41-42,49,411
 port-channel load-balance src-dst-port
 no shutdown

access-list ALL line 8 extended permit ip any any
access-list ALL line 20 extended permit icmp any any

optimize
 debug-level 7

class-map type management match-any REMOTE_ACCESS
 description Remote access traffic match
 2 match protocol telnet any
 3 match protocol ssh any
 4 match protocol icmp any
 5 match protocol http any
 6 match protocol https any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
 class REMOTE_ACCESS
 permit

interface vlan 42
 ip address 10.1.42.5 255.255.255.0
 peer ip address 10.1.42.6 255.255.255.0
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 no shutdown

ft interface vlan 49
 ip address 10.1.49.1 255.255.255.0
 peer ip address 10.1.49.2 255.255.255.0
 no shutdown

ft peer 1
 heartbeat interval 300
 heartbeat count 10
 ft-interface vlan 49
ft group 2
 peer 1
 priority 110
 peer priority 105
 associate-context Admin
 inservice

ip route 0.0.0.0 0.0.0.0 10.1.42.1

context PLM
 allocate-interface vlan 41
 allocate-interface vlan 411
 member R1

ft group 3
 peer 1
 priority 110

```

```

peer priority 105
associate-context PLM
inservice
username admin password 5 1YgD5V.U3$2wYtUr71x8SHBCEzWHXB4/ role Admin domain
default-domain
username www password 5 1WZHqs8dd$1BCU1GjeHc15obfo7njVt1 role Admin domain de
fault-domain
ssh key rsa 1024 force

```

## PLM Context

```

ACE4710-1/Admin# changeto PLM
ACE4710-1/PLM#
ACE4710-1/PLM# show running-config
Generating configuration....

logging console 7

access-list ALL line 8 extended permit ip any any
access-list ALL line 20 extended permit icmp any any

probe http HTTPPROBE
interval 30
faildetect 2
passdetect interval 30
passdetect count 3
request method get url /Windchill/verify.jsp
expect status 200 200
open 1
parameter-map type optimization http EXPIRES
expires-setting time-to-live 3600
parameter-map type http HTTP_COMPRESSION
persistence-rebalance
compress minimum-size 1024
compress mimetype "application/msword"
compress mimetype "application/javascript"
compress mimetype "application/pdf"
compress mimetype "text/.*"

rserver host SERVER1
description Web_Server_1
ip address 10.1.41.40
inservice
rserver host SERVER2
description Web_Server_2
ip address 10.1.41.42
inservice
rserver redirect SORRY_SERVER
webhost-redirection http://10.1.41.99/
inservice

action-list type optimization http OBJECTS
flashforward-object
action-list type optimization http PAGE
flashforward

serverfarm host SFARM1
probe HTTPPROBE
predictor leastconns
rserver SERVER1
inservice

```



```

rserver SERVER2
 inservice
serverfarm redirect SFARM2
 rserver SORRY_SERVER
 inservice

sticky http-cookie ACE_COOKIE C-STICKY
 cookie insert browser-expire
 serverfarm SFARM1 backup SFARM2

class-map match-all L4_VIP_ADDRESS_CLASS
 2 match virtual-address 10.1.41.100 tcp eq www
class-map type http loadbalance match-any OBJECTS
 3 match http url .*css
 5 match http url .*class
 6 match http url .*jar
 7 match http url .*cab
 8 match http url .*txt
 9 match http url .*ps
 10 match http url .*vbs
 11 match http url .*xsl
 12 match http url .*xml
 13 match http url .*pdfb
 14 match http url .*swf
 22 match http url .*jpg
 23 match http url .*jpeg
 24 match http url .*jpe
 25 match http url .*png
 26 match http url .*gif
class-map type http loadbalance match-all PAGE
 2 match http url .*
class-map type management match-any REMOTE_ACCESS
 description Remote access traffic match
 2 match protocol telnet any
 3 match protocol ssh any
 4 match protocol icmp any
 5 match protocol http any
 6 match protocol https any
class-map type http loadbalance match-any default-compression-exclusion-mime-typ
 2 match http url .*js
class-map type http loadbalance match-any default-compression-exclusion-mime-typ
e
 2 match http url .*gif
 3 match http url .*css
 4 match http url .*js
 5 match http url .*class
 6 match http url .*jar
 7 match http url .*cab
 9 match http url .*ps
 10 match http url .*vbs
 11 match http url .*xsl
 12 match http url .*xml
 13 match http url .*pdf
 14 match http url .*swf
 15 match http url .*jpg
 16 match http url .*jpeg
 17 match http url .*jpe
 18 match http url .*png

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
 class REMOTE_ACCESS
 permit

policy-map type loadbalance first-match L7_VIP_POLICY

```

```

class class-default
 sticky-serverfarm C-STICKY

policy-map type optimization http first-match OPTIMIZER
 class OBJECTS
 action OBJECTS parameter EXPIRES
 class PAGE
 action PAGE

policy-map multi-match L4_VIP_POLICY
 class L4_VIP_ADDRESS_CLASS
 loadbalance vip inservice
 loadbalance policy L7_VIP_POLICY
 loadbalance vip icmp-reply

interface vlan 41
 description Server-Side interface
 bridge-group 10
 access-group input ALL
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 no shutdown
interface vlan 411
 description Client-Side interface
 bridge-group 10
 access-group input ALL
 access-group output ALL
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 service-policy input L4_VIP_POLICY
 no shutdown

interface bvi 10
 ip address 10.1.41.5 255.255.255.0
 no shutdown

ip route 0.0.0.0 0.0.0.0 10.1.41.1
username plmadmin password 5 1Ig9wi8sh$RR.1.Pb0OyUX.m0dfzCc9/ role Admin doma
in default-domain

```

## Cisco WAAS Configurations

### Engineering Site WAE

```

! WAAS version 4.1.1 (build b23 Aug 28 2008)
!
device mode application-accelerator
!
hostname WAE612-2-EDGE
!
clock timezone PST -8 0
!
primary-interface InlineGroup 1/0
!
!
interface GigabitEthernet 1/0
 no autosense
 bandwidth 100
 full-duplex
 shutdown
 exit
interface GigabitEthernet 2/0

```

```

shutdown
exit
!
interface InlineGroup 1/0
 ip address 10.1.61.5 255.255.255.0
 inline vlan all
 exit
interface InlineGroup 1/1
 inline vlan all
 exit
!
ip default-gateway 10.1.61.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 128.107.241.185
!
ntp server 10.1.6.1
!
username admin password 1 cCTB/7G867nyQ
username admin privilege 15
username admin print-admin-password 1 7DBAC309DB4F1FD425AD3B83FA6627C7 DC1E9A5ED
AEFD48CA8CE9F73F2F76954
!
windows-domain netbios-name "WAE612-2"
!
authentication login local enable primary
authentication configuration local enable primary
!
central-manager address 10.1.52.5
cms enable
!
flow monitor tcpstat-v1 host 10.88.80.155
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 512
tfo tcp optimized-receive-buffer 512
... more...

```

## Data Center WAE

```

! WAAS version 4.1.1 (build b23 Aug 28 2008)
!
device mode application-accelerator
!
hostname WAE7341-1
!
clock timezone PST -8 0
!
ip domain-name cisco.com
!
exec-timeout 45
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.1.53.5 255.255.255.0
 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 10.1.53.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 128.107.241.185
!
ntp server 10.1.6.1
!
wccp router-list 1 10.1.53.1 10.1.6.12
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
username admin password 1 cCTB/7G867nyQ
username admin privilege 15
username admin print-admin-password 1 7DBAC309DB4F1FD425AD3B83FA6627C7
DC1E9A5EDA EFD48CA8CE9F73
F2F76954
!
windows-domain netbios-name "WAE7341-1"
!
authentication login local enable primary
authentication configuration local enable primary
!
central-manager address 10.1.52.5
cms enable
!
flow monitor tcpstat-v1 host 10.88.80.155
flow monitor tcpstat-v1 enable
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
... more...

```

## Central Manager WAE

```

! WAAS version 4.1.1 (build b23 Aug 28 2008)
!
device mode central-manager
!
hostname WAE612-1-CentralMgr
!
clock timezone PST -8 0
!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0

```

```

ip address 10.1.52.5 255.255.255.0
exit
interface GigabitEthernet 2/0
shutdown
exit
!
ip default-gateway 10.1.52.1
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 128.107.241.185
!
ntp server 10.1.6.1
!
!
username admin password 1 cCTB/7G867nyQ
username admin privilege 15
username admin print-admin-password 1 7DBAC309DB4F1FD425AD3B83FA6627C7 DC1E9A5ED
AEFD48CA8CE9F73F2F76954
!
!
authentication login local enable primary
authentication configuration local enable primary
!
!
cms enable
!
!
! End of WAAS configuration

```

## Catalyst Switches

### Data Center Core Switch 1

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname 6509-1
!
boot system flash

sup-bootdisk:s3223-advipservicesk9_wan-mz.122-33.SXH3.bin
boot-end-marker
!
enable password 7 03025A08120033551E
!
no aaa new-model
clock timezone PST -8
!
ip subnet-zero
ip wccp 61
ip wccp 62
!
no ip domain-lookup
vtp domain cisco
vtp mode transparent
!
redundancy

```

```

 keepalive-enable
 mode sso
 main-cpu
 auto-sync running-config
 spanning-tree mode pvst
 spanning-tree extend system-id
 system flowcontrol bus auto
 !
 vlan 53
 name WAE
 !
 vlan 111
 remote-span
 !
 no crypto ipsec nat-transparency udp-encaps
 !
 interface Loopback1
 ip address 10.1.6.11 255.255.255.255
 !
 interface Port-channel1
 ip address 10.1.5.21 255.255.255.252
 !
 interface GigabitEthernet2/1
 description Trunk_To 6509-2
 no ip address
 channel-group 1 mode on
 !
 interface GigabitEthernet2/2
 description Trunk_To 6509-2
 no ip address
 channel-group 1 mode on
 !
 interface GigabitEthernet2/3
 description to 2821-3
 ip address 10.1.7.1 255.255.255.252
 ip wccp 62 redirect in
 !
 interface GigabitEthernet2/4
 description WAE7341-1_Core
 switchport
 switchport access vlan 53
 spanning-tree portfast
 !
 ... more...
 !
 no ip address
 !
 interface GigabitEthernet2/47
 description to 6506-2 Distribution
 ip address 10.1.5.2 255.255.255.252
 ip wccp 61 redirect in
 !
 interface GigabitEthernet2/48
 description to 6506-1 Distribution
 ip address 10.1.5.10 255.255.255.252
 ip wccp 61 redirect in
 !
 interface Vlan1
 no ip address
 !
 interface Vlan53
 ip address 10.1.53.1 255.255.255.0
 ip wccp redirect exclude in
 !

```

```

router eigrp 10
 network 10.0.0.0
 no auto-summary
!
ip classless
snmp-server community public RO
!
line con 0
line vty 0 4
 password 7 130316111F0316337B
 login
 transport input lat pad udptn telnet rlogin ssh acercon
line vty 5 15
 login
 transport input lat pad udptn telnet rlogin ssh acercon
!
ntp master 3
ntp update-calendar
!
end

```

## Data Center Core Switch 2

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service internal
service counters max age 5
!
hostname 6509-2
!
boot system flash sup-bootdisk:s3223-advipservicesk9_wan-mz.122-33.SXH3.bin
!
enable password 7 000212051054191F5F
!
no aaa new-model
clock timezone PST -8
!
ip subnet-zero
ip wccp 61
ip wccp 62
!
no ip domain-lookup
vtp domain cisco
vtp mode transparent
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
 auto-sync running-config
spanning-tree mode pvst
system flowcontrol bus auto
!
vlan 54
 name WAAS_Mobile
!
vlan 55
 name ASA5540-1
!
vlan 111

```

```

remote-span
!
interface Loopback1
 ip address 10.1.6.12 255.255.255.255
!
interface Port-channel1
 no ip address
!
interface GigabitEthernet2/1
 description Trunk_To 6509-1
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet2/2
 description Trunk_To 6509-1
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet2/3
 description to 2821-3
 ip address 10.1.7.5 255.255.255.252
 ip wccp 62 redirect in
!
interface GigabitEthernet2/4
 description WAAS Mobile
 switchport
 switchport access vlan 54
!
interface GigabitEthernet2/5
 description ASA5540-1
 switchport
 switchport access vlan 55
!
interface GigabitEthernet2/47
 description to 6506-1 Distribution
 ip address 10.1.5.14 255.255.255.252
 ip wccp 61 redirect in
!
interface GigabitEthernet2/48
 description to 6506-2 Dist
 ip address 10.1.5.6 255.255.255.252
 ip wccp 61 redirect in
!
... more...
!
interface Vlan21
 ip address 10.1.21.3 255.255.255.0
 standby 21 ip 10.1.21.1
 standby 21 priority 110
 standby 21 preempt
!
interface Vlan22
 ip address 10.1.22.3 255.255.255.0
 standby 22 ip 10.1.22.1
 standby 22 priority 110
 standby 22 preempt
!
interface Vlan52
 description WAE-CM
 ip address 10.1.52.1 255.255.255.0
!
interface Vlan54
 description WAAS Mobile
 ip address 10.1.54.1 255.255.255.0

```



```

!
interface Vlan55
 ip address 10.1.55.1 255.255.255.0
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
ip classless
snmp-server community public RO
!
line con 0
line vty 0 4
 password 7 121F041406041E1D7A
 login
 transport input lat pad udptn telnet rlogin ssh acercon
line vty 5 15
 login
 transport input lat pad udptn telnet rlogin ssh acercon
!
ntp clock-period 17224056
ntp update-calendar
ntp server 10.1.6.1
!
End

```

## Data Center Distribution Switch 1

```

Current configuration : 7725 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service counters max age 5
!
hostname 6506-1
!
boot-start-marker
boot system sup-bootdisk:s72033-ip services_wan-mz.122-33.SXH2a.bin
boot system flash:sup-bootdisk:s72033-ip services_wan-mz.122-33.SXH2a.bin
boot-end-marker
!
no logging console
enable password 7 094A4F0A0D0A050B5B
!
no aaa new-model
clock timezone PST -8
svcllc multiple-vlan-interfaces
svcllc module 4 vlan-group 1,
analysis module 2 management-port access-vlan 85
ip subnet-zero
!
!
no ip domain-lookup
vtp domain cisco
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
no mls flow ip

```

```

mls cef error action freeze
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
 auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
no power enable module 4
fabric switching-mode allow truncated threshold 1
fabric switching-mode allow truncated
port-channel load-balance src-dst-port
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 21-22
!
vlan 41
 name ACE_Server_Side
!
vlan 42
 name ACE_Management
!
vlan 49
 name ACE__FT
!
vlan 85
 name NAM
!
vlan 111
 remote-span
!
vlan 411
 name ACE_Client__Side
!
!
interface Loopback1
 ip address 10.1.6.1 255.255.255.255
!
interface Port-channel1
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
!
interface GigabitEthernet1/1
 description Trunk_To_6506-2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/2
 description Trunk_To_6506-2
 switchport
 switchport trunk encapsulation dot1q

```

```

 switchport mode trunk
 !
interface GigabitEthernet1/3
 switchport
 switchport access vlan 55
 !
interface GigabitEthernet1/4
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
 !
interface GigabitEthernet1/5
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
 !
interface GigabitEthernet1/6
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
 !
interface GigabitEthernet1/7
 description ACE4710-1
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 speed 1000
 duplex full
 channel-group 1 mode on
 !
interface GigabitEthernet1/8
 no ip address
 !
...more...
 !
interface GigabitEthernet1/45
 description to 3750-1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 21
 switchport trunk allowed vlan 21,41
 switchport mode trunk
 !
interface GigabitEthernet1/46

```

```

description to 3750-2
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 22
switchport trunk allowed vlan 22,41
switchport mode trunk
!
interface GigabitEthernet1/47
description to 6509-2 Core
ip address 10.1.5.13 255.255.255.252
!
interface GigabitEthernet1/48
description to 6509-1 Core
ip address 10.1.5.9 255.255.255.252
!
...more...
!
interface Vlan1
no ip address
shutdown
!
interface Vlan21
description PTC Windchill
ip address 10.1.21.2 255.255.255.0
standby 21 ip 10.1.21.1
standby 21 priority 110
standby 21 preempt
!
interface Vlan22
description Oracle DB
ip address 10.1.22.2 255.255.255.0
standby 22 ip 10.1.22.1
standby 22 priority 110
standby 22 preempt
!
interface Vlan42
description ACE Management
ip address 10.1.42.2 255.255.255.0
standby 42 ip 10.1.42.1
standby 42 priority 110
standby 42 preempt
!
interface Vlan51
description ACE4710
ip address 10.1.51.2 255.255.255.0
standby 51 ip 10.1.51.1
standby 51 priority 110
standby 51 preempt
!
interface Vlan85
description NAM
ip address 10.1.85.2 255.255.255.0
standby 85 ip 10.1.85.1
standby 85 priority 90
standby 85 preempt
!
interface Vlan411
ip address 10.1.41.2 255.255.255.0
standby 41 ip 10.1.41.1
standby 41 priority 110
standby 41 preempt
!
router eigrp 10
network 10.0.0.0

```

```

 no auto-summary
 !
 ip classless
 !
 no ip http server
 !
 ip access-list standard public
 !
 snmp-server community public RO
 !
 control-plane
 !
 line con 0
 line vty 0 4
 exec-timeout 30 0
 password 7 130316111F0316337B
 login
 transport input lat pad udptn telnet rlogin
 line vty 5 15
 login
 transport input lat pad udptn telnet rlogin
 !
 ntp source Loopback1
 ntp master 3
 ntp update-calendar
 !
end

```

## Data Center Distribution Switch 2

```

Current configuration : 7379 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service counters max age 5
!
hostname 6506-2
!
boot-start-marker
boot system flash bootflash:s72033-ip-services_wan-mz.122-33.SXH2a.bin
boot-end-marker
!
no logging console
enable password 7 020005581F091D381C
!
no aaa new-model
clock timezone PST -8
svcllc multiple-vlan-interfaces
svcllc module 4 vlan-group 1,
!
no ip domain-lookup
vtp domain cisco
vtp mode transparent
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
 auto-sync running-config

```

```

!
spanning-tree mode rapid-pvst
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
no power enable module 4
fabric switching-mode allow truncated threshold 1
fabric switching-mode allow truncated
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 21-22
!
vlan 41
 name ACE_Server_Side
!
vlan 49
 name ACE__FT
!
vlan 52
 name WAE-CM
!
vlan 69
!
vlan 85
 name NAM
!
vlan 411
 name ACE_Client__Side
!
interface Loopback1
 ip address 10.1.6.2 255.255.255.255
!
interface Port-channel1
 description ACE4710-2
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/1
 description Trunk_To_6506-1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/2
 description Trunk_To_6506-2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/3
 description to WAE612-1 Central_Manager
 switchport
 switchport access vlan 52
!
interface GigabitEthernet1/4
 description ACE4710-2
 switchport
 switchport access vlan 41
 switchport trunk encapsulation dot1q
 switchport mode trunk

```

```

channel-group 1 mode on
!
interface GigabitEthernet1/5
description ACE4710-2
switchport
switchport access vlan 41
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface GigabitEthernet1/6
description ACE4710-2
switchport
switchport access vlan 41
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface GigabitEthernet1/7
description ACE4710-2
switchport
switchport access vlan 41
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface GigabitEthernet1/8
no ip address
!
...more...
!
interface GigabitEthernet1/45
description to 3750-2
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 22
switchport trunk allowed vlan 1,22,41
switchport mode trunk
!
interface GigabitEthernet1/46
description to 3750-1
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 21
switchport trunk allowed vlan 21,41
!
interface GigabitEthernet1/47
description to 6509-1 Core
ip address 10.1.5.1 255.255.255.252
!
interface GigabitEthernet1/48
description to 6509-2 Core
ip address 10.1.5.5 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
interface Vlan21
description PTC Windchill
ip address 10.1.21.3 255.255.255.0
standby 21 ip 10.1.21.1
standby 21 priority 90
standby 21 preempt

```

```

!
interface Vlan22
 description Oracle DB
 ip address 10.1.22.3 255.255.255.0
 standby 22 ip 10.1.22.1
 standby 22 priority 90
 standby 22 preempt
!
interface Vlan42
 description ACE Management
 ip address 10.1.42.3 255.255.255.0
 standby 42 ip 10.1.42.1
 standby 42 priority 110
 standby 42 preempt
!
interface Vlan51
 description ACE4710
 ip address 10.1.51.3 255.255.255.0
 standby 51 ip 10.1.51.1
 standby 51 priority 90
 standby 51 preempt
!
interface Vlan52
 description WAE-CM
 ip address 10.1.52.1 255.255.255.0
!
interface Vlan85
 description NAM
 ip address 10.1.85.3 255.255.255.0
 standby 85 ip 10.1.85.1
 standby 85 priority 90
 standby 85 preempt
!
interface Vlan411
 ip address 10.1.41.3 255.255.255.0
 standby 41 ip 10.1.41.1
 standby 41 priority 90
 standby 41 preempt
!
router eigrp 10
 passive-interface default
 no passive-interface GigabitEthernet1/1
 no passive-interface GigabitEthernet1/2
 no passive-interface GigabitEthernet1/44
 no passive-interface GigabitEthernet1/47
 no passive-interface GigabitEthernet1/48
 network 10.0.0.0
 no auto-summary
!
ip classless
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 30 0
 password 7 14111308180B383274
 login
 transport input lat pad udptn telnet rlogin
line vty 5 15
 login
 transport input lat pad udptn telnet rlogin
!
end

```



## Data Center Access Switch 1

```

version 12.2
no service pad
!
hostname 3750-1
!
enable password 7 094A4F0A0D0A050B5B
!
no aaa new-model
switch 1 provision ws-c3750g-24ps
ip subnet-zero
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface GigabitEthernet1/0/1
description to 6506-1
switchport access vlan 21
switchport trunk encapsulation dot1q
switchport trunk native vlan 21
switchport mode trunk
!
interface GigabitEthernet1/0/2
description to 6506-2
switchport access vlan 21
switchport trunk encapsulation dot1q
switchport trunk native vlan 21
switchport mode trunk
!
...more...
!
interface GigabitEthernet1/0/13
description VMWARE-2
switchport access vlan 22
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 21,41
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
!
...more...
!
interface Vlan1
no ip address
!
interface Vlan21
ip address 10.1.21.5 255.255.255.0
!
ip default-gateway 10.1.21.1
ip classless
!
line con 0
line vty 0 4
password 7 03025A08120033551E
login
line vty 5 15
no login
!
End

```

## Data Center Access Switch 2

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname 3750-2
!
enable password 7 15140A0F1025393D78
!
no aaa new-model
switch 1 provision ws-c3750g-24ps
ip subnet-zero
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/0/1
description to 6506-2 Distribution
switchport access vlan 22
switchport trunk encapsulation dot1q
switchport trunk native vlan 22
switchport mode trunk
spanning-tree portfast
!
interface GigabitEthernet1/0/2
description to 6506-1 Distribution
switchport access vlan 22
switchport trunk encapsulation dot1q
switchport trunk native vlan 22
switchport mode trunk
spanning-tree portfast
!
...more...
!
interface GigabitEthernet1/0/13
description VMWARE-2
switchport access vlan 22
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 22,41
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
!
...more...
!
interface Vlan1
no ip address
!
interface Vlan22
ip address 10.1.22.5 255.255.255.0
!
ip default-gateway 10.1.22.1
ip classless
ip http server
!

```

```

line con 0
line vty 0 4
 password 7 06000E2258411B0055
 login
line vty 5 15
 no login
!
end

```

## Engineering Site Access Switch

```

version 12.2
!
hostname 2960-1
!
enable password 7 050D070C35435C1049
!
system mtu routing 1500
ip subnet-zero
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 description WAE612-2 Inline
 switchport access vlan 61
 switchport trunk native vlan 61
 switchport trunk allowed vlan 61,65
 switchport mode trunk
!
...more...
!
interface FastEthernet0/13
 description VMWARE-2
 switchport access vlan 65
!
...more...
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan61
 ip address 10.1.61.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.1.61.1
ip http server
ip http secure-server
!
line con 0
line vty 0 4
 password 7 15140A0F1025393D78
 login
line vty 5 15
 login
!
End

```

## Cisco ISR Routers

### Branch Router

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 2821-1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$1BRQ$Dw8Vd1TK2q86BOugYyeqU/
!
no aaa new-model
!
!
no ip domain lookup
!
!
interface Loopback1
 ip address 10.1.6.21 255.255.255.0
!
interface GigabitEthernet0/0
 description to 2960-1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1
!
interface GigabitEthernet0/0.2
!
interface GigabitEthernet0/0.61
 encapsulation dot1Q 61 native
 ip address 10.1.61.1 255.255.255.0
!
interface Serial0/2/0
 description to WAN Simulation
 ip address 10.1.7.10 255.255.255.252
 service-module t1 timeslots 1-24
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password 7 0709204F5A060B1C47
 login
!
End

```

## Data Center WAN Router

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 2821-3
!
boot-start-marker
boot system flash:c2801-tpgen+ipbase-mz.PAGENT.4.5.0
enable secret 5 $1$2ae6$40.1Cz0fSo/aqKYvAVLOm1
!
ip cef
!
interface Loopback1
 ip address 10.1.6.13 255.255.255.0
!
interface GigabitEthernet0/0
 description to 6509-1 Core
 ip address 10.1.7.2 255.255.255.252
 duplex auto
 speed auto
 no keepalive
!
interface GigabitEthernet0/1
 description to 6509-2 Core
 ip address 10.1.7.6 255.255.255.252
 duplex auto
 speed auto
 no keepalive
!
interface Serial0/2/0
 ip address 10.1.7.9 255.255.255.252
 service-module t1 timeslots 1-24
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password 7 011507074F04141671
 login
 transport input telnet
!
End

```

## Internet Router 1

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2811-1
!
logging buffered 51200 warnings

```

```

enable secret 5 1TMso$L5cbowE8uREbV77ZfRT.r1
!
ip subnet-zero
!
ip cef
!
interface FastEthernet0/0
 ip address 10.1.58.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 10.1.57.2 255.255.255.252
 service-module t1 clock source internal
 service-module t1 timeslots 1-24
!
router eigrp 100
 network 10.0.0.0
 no auto-summary
!
ip classless
!
access-list 23 permit 10.10.10.0 0.0.0.7
!
line con 0
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
End

```

## Internet Router 2

```

version 12.4
!
hostname 2821-2
!
ip cef
!
interface GigabitEthernet0/0
 ip address 10.1.56.10 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/3/0
 ip address 10.1.57.1 255.255.255.252
 service-module t1 clock source internal
 service-module t1 timeslots 1-24
!
router eigrp 100
 network 10.0.0.0

```

```

 no auto-summary
 !
 line con 0
 line aux 0
 line 1/0 1/31
 line vty 0 4
 login
 !
 scheduler allocate 20000 1000
 !
 End

```

## Cisco ASA

### ASA for Remote VPN Users

```

ASA Version 8.0(3)
!
hostname ASA5540-1
enable password 7w22FjI5eWall1BPD encrypted
names
!
interface GigabitEthernet0/0
description Connected to inside lab net
nameif inside
security-level 100
ip address 10.1.55.100 255.255.255.0
!
interface GigabitEthernet0/1
description Connected to outside remote users
nameif outside
security-level 0
ip address 10.1.56.100 255.255.255.0
!
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa803-k8.bin
ftp mode passive
access-list inside_in extended permit ip any any
access-list inside_nat0_outbound extended permit ip any 10.1.55.192 255.255.255.192
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu management 1500
ip local pool client_pool 10.1.55.200-10.1.55.250 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-611.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
route inside 0.0.0.0 0.0.0.0 10.1.55.1 1
route outside 10.1.58.0 255.255.255.0 10.1.56.10 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

```

```

dynamic-access-policy-record DfltAccessPolicy
http server enable
http 10.1.55.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
http 10.1.54.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-SHA
ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5
ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet 10.1.55.0 255.255.255.0 inside
telnet 10.1.54.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
management-access inside
dhcpd address 10.1.56.101-10.1.56.105 outside
dhcpd enable outside
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
group-policy ciscovpngroup internal
group-policy ciscovpngroup attributes
 vpn-tunnel-protocol IPSec
username cisco password NepX7TmK00YjhQjA encrypted privilege 0
username cisco attributes
 vpn-group-policy ciscovpngroup
tunnel-group ciscovpngroup type remote-access
tunnel-group ciscovpngroup general-attributes
 address-pool client_pool
 default-group-policy ciscovpngroup
tunnel-group ciscovpngroup ipsec-attributes
 pre-shared-key *
!
prompt hostname context
Cryptochecksum:d6fc31b415e2ef43e01c841e12783c80
: end

```



# 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 <http://www.cisco.com/go/validateddesigns>.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R).

---

Portions of this work are contributed by and used under permission from Parametric Technology Corporation (PTC); ©PTC. Information described herein is furnished for informational use only, is subject to change without notice, and should not be construed as a guarantee, commitment, condition or offer from PTC. Products and services are described by their respective suppliers and all inquires thereon should be directed toward the supplying party. Neither PTC nor Cisco Systems, Inc is authorized to act or make commitments on the other's behalf.

PTC and its logo, The Product Development Company, Pro/ENGINEER, Wildfire, Windchill, Arbortext, Mathcad, CoCreate, CoCreate Modeling, CoCreate Model Manager, CADDs, Windchill ProjectLink, Windchill PDMLink, Windchill PartsLink, Windchill DynamicDesignLink, Windchill MPMLink, ProductView, Optegra, InterComm, IsoDraw, IsoView, FlexPLM, ProductPoint and all PTC product names and logos are trademarks or registered trademarks of PTC and/or its subsidiaries in the United States and in other countries.

