Integrating Microsoft Windows Server 2008 Terminal Services into a Cisco Data Center

Last Update: June 16, 2009

Contents

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

Introduction

Microsoft Terminal Services has been a cornerstone presentation virtualization product for enterprise customers for many years. Microsoft Windows Server 2008 Terminal Services enables an IT organization to more safely support a mobile/remote workforce by allowing remote access to applications and data that hold sensitive information while not allowing leakage of that data to the local device. Terminal Services also allows for the deployment of rugged or purpose-built, thin-client devices that run a remote session into the Terminal Services environment. These rugged or purpose-built endpoints exist in environments that are not traditionally PC friendly due to the physical environment—such as a factory floor, a clean room, or in conditions where extreme temperatures are experienced.

Microsoft Windows Server 2008 Terminal Services offers many new capabilities over the previous version. These new capabilities offer greater functionality, performance and reliability for a wide range of usage models—such as mobile workers, task workers, and workers in extreme environmental conditions. Some of the enhancements include:

- Integrated application delivery
- Built-in support for secure Internet access
- Simplified printing
- Presentation of applications and desktop access through a web page or online application
- Support for additional device redirection
- Enhanced license tracking and reporting
- New application program interfaces (API) to support extensibility

Note Microsoft recently announced that Terminal Services will be renamed *Remote Desktop Services*. This document uses the existing Terminal Services terminology, but for any updates to the document (especially when Windows Server 2008 R2 is used), the name Remote Desktop Services will be used. More information can be found at the following URL: http://download.microsoft.com/download/6/9/3/6933B3E1-A550-4584-91E5-AF58727E670B/WindowsServer2008TerminalServicesRenamed.docx

The solution documented in this publication enables customers to deploy Microsoft Server 2008 Terminal Services in a way that delivers a more robust and streamlined end-user experience. This can be achieved through offloading CPU-intensive operations, such as Secure Socket Layer (SSL) from the servers, performing Layer-4 through Layer-7 server load balancing (SLB), optimizing bandwidth for branch and mobile workers, and reducing the transaction times experienced by terminal server users.

Audience

This document is intended for network engineers and architects who must understand the basics of a Microsoft Windows Server 2008 Terminal Services (known in this paper as *TS2008*) environment and the design and configuration options for providing advanced network services for Terminal Services.

Document Objectives

This document provides design and configuration guidance for SLB, SSL offload, and WAN/network optimization in a TS2008 environment. An overview of the various Terminal Services components and operations are given to provide the reader some context about how the application environment is affected by a Cisco data center design.

The following prerequisites are required to deploy the Cisco solution for Windows Server 2008 Terminal Services:

- Working knowledge of Microsoft Active Directory and Windows 2008 Server installation
- Experience with basic networking and troubleshooting
- Experience installing the Cisco products covered by this network design, including the Cisco Application Control Engine (Cisco ACE) and Cisco Wide Area Application Services (Cisco WAAS) product families

- Working knowledge of the Cisco Internetworking Operating System (IOS)

Additional information that might be useful in understanding and deploying this solution, as well as other applications, can be found at the following links:

- Cisco Connection Online-Data Center—http://www.cisco.com/go/dc
- Cisco Solution Reference Network Designs (SRND)—http://www.cisco.com/go/designzone
- Microsoft Windows Server 2008 Terminal Services—http://www.microsoft.com/windowsserver2008/en/us/ts-product-home.aspx

Solution Overview

The Cisco solution for TS2008 offers increased application availability, performance and security by leveraging the following technologies and services:

- *Application availability*

  The Cisco ACE product family offers Terminal Services application high availability by providing the following:

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

- *Application performance*

  The Cisco ACE and Cisco WAAS product families offer Terminal Services application performance improvement by providing the following:

  - WAN optimization—Provides intelligent caching, compression, and protocol optimization of the remote desktop protocol
  - Server offloading—Specialized hardware that offers greater processing efficiency for application optimization services listed below, which frees up server processing and memory for additional remote desktop sessions
  - Server load balancing—Substitutes for Microsoft Network Load Balancing
  - Secure Socket Layer (SSL) termination—Terminates 15,000 connections per second.
  - Transmission Control Protocol (TCP) connection management—Reduces the number of TCP connections to server
  - Server health monitoring—Ensures that connecting clients reach the most optimal terminal server

- *Application security*

  The Cisco ACE and Cisco Adaptive Security Appliance (ASA) product families offer Terminal Services application security by providing the following:

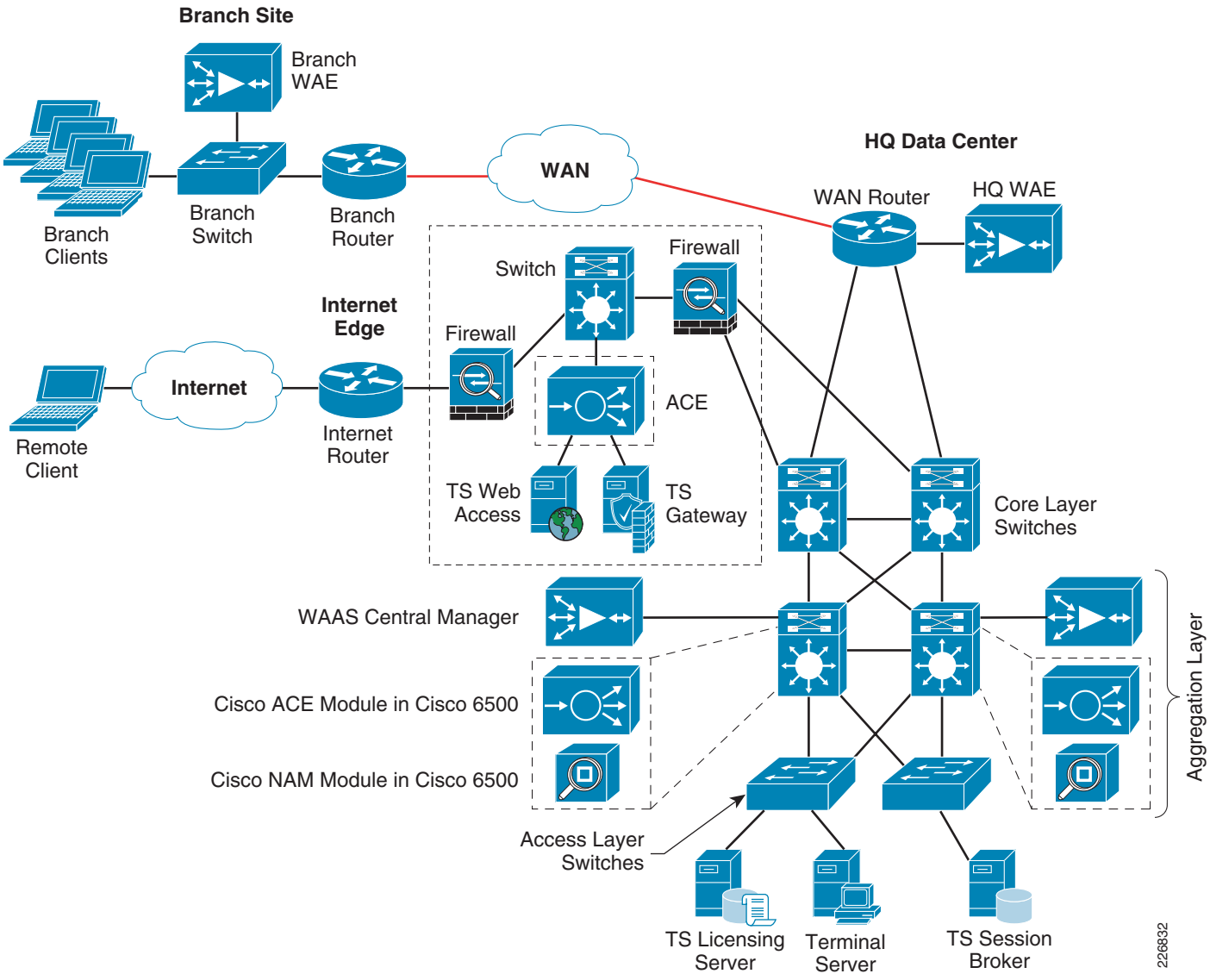
  - SSL termination—Efficiently encrypts and decrypts SSL enabled traffic, which facilitates security services such as firewalls and the use of intrusion detection and prevention before traffic reaches the servers
  - End user access control—Provides Access Control Lists (ACL) to protect client-to-server traffic from worms and intruders that attack vulnerable open server ports not used by the application

Solution Components and Topology

TS2008 can be deployed in a variety of ways that range from a highly consolidated approach focused on small- and medium-sized implementations to highly complex, redundant and scalable implementations used by large enterprise accounts. There are a large number of variables and implementation options available with a Terminal Services implementation. It is important to break down the various Terminal Services roles to their basic elements. In this document a focus will be placed on each Terminal Services role and how the various Cisco solutions fit into those roles.

Figure 1 illustrates the high-level view of the design presented in this publication. Although not shown in this high-level diagram, the TS2008 environment is deployed with multiple servers for each TS2008 role to provide better scale and redundancy.

Figure 1 Cisco Solution for Windows Server 2008 Terminal Services - High Level Overview



The sections that follow briefly describe the components in each area of the diagram

Data Center Access Layer

At the data center access layer, Microsoft Windows Server 2008 Terminal Servers are deployed along with a Terminal Services (TS) Licensing server and also a TS Session Broker. Other servers responsible for required roles such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Active Directory, and so on were also located in the access layer (not shown in this diagram).

Data Center Aggregation Layer

Cisco ACE modules and the Cisco WAAS Central Manager are deployed at the data center aggregation layer Cisco Catalyst 6500s with Network Analysis Modules (Cisco NAM). The Cisco NAM is used to monitor and report network and application traffic statistics going into and out of the server farms in the data center access layer. The Cisco NAM is used in conjunction with the Cisco WAAS Central Manager, Cisco Wide Area Application Engine (WAE), and routers running NetFlow to determine the Remote Desktop Protocol (RDP) traffic profile and the impact WAN optimization has on RDP sessions. The Cisco ACE module is used to perform load balancing of the terminal servers in the access layer.

Note The test bed in this solution did not have Nexus 7000 products in it. The Cisco Catalyst 6500 can easily be substituted with the Nexus 7000 with either a services chassis deployment (to provide access to service modules) or by using appliances attached to the Nexus (Cisco NAM and Cisco ACE come in an appliance form factor as well as a module). More information can be found on the deployment of Nexus 7000 with services at the following link:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/nx_7000_dc.html

WAN Edge

Attached to the WAN router is the headquarters (HQ) Cisco WAE. The HQ Cisco WAE works in conjunction with the branch Cisco WAE and the Cisco WAAS Central Manager to auto-discover RDP flows and to provide WAN optimization services for those flows. In the simulated WAN environment, a network delay and loss generator is used to test a variety of WAN speeds, latency, and loss combinations.

Branch

The branch WAN has a Cisco Integrated Services Router (ISR), Cisco Catalyst switch, and the branch Cisco WAE. In addition, the branch leverages multiple Microsoft Windows XP SP3 and Vista SP1 clients used as Remote Desktop Connection (RDC) clients.

Internet Edge

At the Internet Edge, Cisco ASAs are deployed to perform firewall services for incoming traffic to the TS Web Access and TS Gateway servers. In addition to the Cisco ASA, the Cisco ACE is deployed to provide SSL offload and server load balancing for the TS Web Access and TS Gateway servers.

Cisco Solution Overview for Terminal Services Integration

This section presents the following solution component descriptions:

Cisco Application Control Engine

The Cisco Application Control Engine (Cisco ACE) provides a highly available and scalable data center solution from which the Microsoft Windows Server 2008 Terminal Services environment can benefit. Currently, the Cisco ACE is available as an appliance or integrated services module in the Cisco Catalyst 6500 platform. The Cisco ACE features and benefits include the following:

- Device partitioning (up to 250 virtual Cisco ACE contexts)
- Load-balancing services (up to 16 Gbps of throughput capacity and 345,000 Layer-4 connections per second)
- Security services through deep-packet inspection, access control lists (ACL), unicast reverse path forwarding (uRPF), Network Address Translation (NAT)/Port Address Translation (PAT) with fix-ups, Syslog, and so on
- Centralized, role-based management via Application Network Manager (ANM) GUI or CLI
- SSL offload (up to 15,000 SSL sessions through licensing)
- Support for redundant configurations (intra-chassis, inter-chassis, and inter-context)

Cisco ACE Virtualization

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

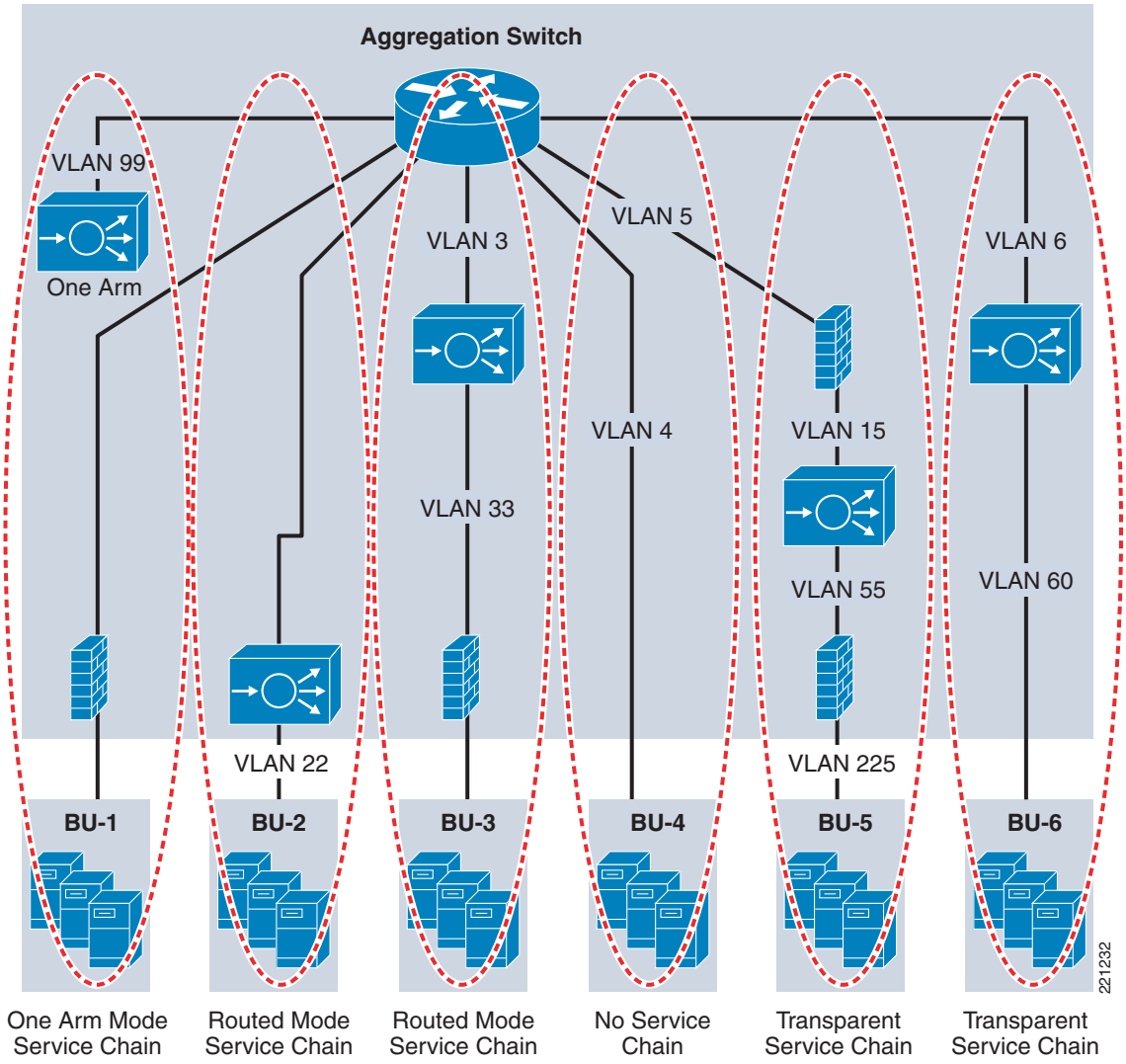
The Cisco ACE supports device partitioning where a single physical device might provide multiple logical devices. This virtualization functionality allows system administrators to assign a single virtual Cisco ACE device to a business unit or application to achieve application performance goals or service-level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

Figure 2 shows the use of virtualized network services afforded through the Cisco ACE and Cisco Firewall Services Module (FWSM). In Service Chaining via Virtualized Network Services, a Cisco Catalyst 6500 housing a single Cisco ACE and Cisco FWSM supports the business processes of five independent business units. The system administrator determines the application requirements and assigns the appropriate network services as virtual contexts. Each context contains its own set of policies, interfaces, resources, and administrators. The Cisco ACE and Cisco FWSMs allow routed, one-arm, and transparent contexts to coexist on a single physical platform. Alternatively the Cisco ACE appliance and Cisco ASA can be used to achieve a similar level of virtualization as their module counterparts can.

The Cisco ACE can be used to apply a different context and associated policies, interfaces and resources for the TS Web Access role and a completely different context for the TS Gateways. Each context can be assigned a different administrator allowing for Role-Based Access Control (RBAC) of the services.

Note In this document the TS Web Access and TS Gateway roles share the same context.

Figure 2 Service Chaining via Virtualized Network Services



SSL Offload

The Cisco ACE is capable of providing secure transport services to a Windows Server 2008 Terminal Services deployment. The Cisco ACE can offload Transport Layer Security (TLS)/SSL processing from the TS Web Access and TS Gateway roles thereby saving processor cycles. The Cisco ACE implements its own SSL stack and does not rely on any version of Open SSL. The Cisco ACE supports TLS 1.0, SSLv3, and SSLv2/3 hybrid protocols. There are three SSL relevant deployment models available to each Cisco ACE virtual context:

- *SSL termination*—Allows for the secure transport of data between the client and Cisco ACE virtual context. The Cisco ACE operates as an SSL proxy. As such, it negotiates and terminates secure connections with a client—and a non-secure or clear-text connection to an application server in the

data center. The advantage of this design is the offloading of application server resource requirements from the CPU and memory demands associated with SSL processing—while continuing to provide intelligent load balancing.

- *SSL initiation*—Provides secure transport between the Cisco ACE and the application server. The client initiates an non-secure HTTP connection with the Cisco ACE virtual context, while the Cisco ACE acts as a client proxy that negotiates an SSL session to an SSL server.
- *SSL end-to-end*—Provides a secure transport path for all communications between a client and the SSL application server residing in the data center. The Cisco ACE uses SSL termination and SSL initiation techniques to support the encryption of data between client and server. Two completely separate SSL sessions are negotiated, one between the Cisco ACE context and the client, the other between the Cisco ACE context and the application server. In addition to the intelligent load balancing services the Cisco ACE provides in an end-to-end SSL model. The system administrator may choose to alter the intensity of data encryption in order to reduce the load on either the frontend client connection or backend application server connection (allowing for the reduction of SSL resource requirements on either entity).

SSL URL Rewrite Offload

The Cisco ACE is capable of inserting or deleting HTTP header information for connections it is sustaining. This capability is highly useful when an application server responds with a HTTP 302 or Moved Temporarily response to a client's HTTP GET or HEAD request. The HTTP 302 response usually indicates a new HTTP LOCATION URL for the client to access. Modifying the HTTP LOCATION value for a secure connection is known as *SSL URL Rewrite*. The SSL URL Rewrite feature allows the system administrator to alter the HTTP LOCATION value returned to the client—resulting in granular control of the application's session flow and persistence in the data center.

SSL Session ID Reuse

SSL session ID reuse allows the client and server to reuse the secret key negotiated during a previous SSL session. This feature generally improves the volume of SSL sessions that an SSL server or SSL proxy can effectively maintain. Clients residing with remote connectivity, for instance across a WAN, generally benefit from this feature. The SSL negotiation load is effectively reduced on the SSL proxy server while simultaneously improving the user experience because key negotiation is a rather lengthy process. The Cisco ACE may maintain the SSL session ID indefinitely or up to 20 hours with a timeout configuration.

SSL ID reuse does not compromise the security of the data center. The ID reuse feature only acknowledges that a secret key already exists between the client and server. Nonetheless, the client must use this key for the application server to receive data from the client. The security resides in the secret key, not the SSL session ID.

Session Persistence

Session persistence is the ability to forward client requests to the same server for the duration of a session. Two common approaches to maintaining session persistence with TS is to use Source IP sticky or TS Session Broker routing tokens. The Cisco ACE supports each of these methods.

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

Allowed Server Connections

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

Route Health Injection

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

Health Monitoring

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

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

- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Echo (TCP/UDP)
- Finger
- Hypertext Transfer Protocol (HTTP)
- Secure HTTP (HTTPS) SSL Probes
- File Transfer Protocol (FTP)
- Telnet
- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP)
- Post Office Protocol version 3 (POP3)
- Remote Authentication Dial In User Service (RADIUS)
- Real Time Streaming Protocol (RTSP)
- Simple Network Management Protocol (SNMP)
- Scripted—Cisco Tool Command Language (TCL) support

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

For more information on these services, see the Cisco ACE Module documentation at the following URL: http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

Cisco Wide Area Application Services

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

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

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

Advanced Compression Using DRE and LZ Compression

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

Transport File Optimizations

The Cisco WAAS Transport File Optimizations (TFO) uses a robust TCP proxy to safely optimize TCP at the Cisco WAE device by applying TCP-compliant optimizations to shield the clients and servers from poor TCP behavior due to WAN conditions. The Cisco WAAS TFO improves throughput and reliability for clients and servers in WAN environments through increases in the TCP window sizing and scaling enhancements—as well as through the implementation of congestion management and recovery techniques—to ensure that the maximum throughput is restored in the event of packet loss. By default, Cisco WAAS provides only TFO for RDP. If RDP compression and encryption are disabled, then full optimization (TFO+ DRE/LZ) can be enabled for RDP flows.

Common Internet File System Caching Services

The Common Internet File System (CIFS) used by Microsoft applications is an inherently chatty transactional application protocol; it is not uncommon to find several CIFS hundred transaction messages traversing the WAN just to open a remote file. The Cisco WAAS provides a CIFS adapter that

can inspect and predict to a certain degree which follow-up CIFS messages are expected. By doing this, the local Cisco WAE caches these messages and sends them locally, significantly reducing the number of CIFS messages traversing the WAN.

Print Services

The Cisco WAAS provides native small- and medium-sized business (SMB)-based Microsoft print services locally on the Cisco WAE device. Along with CIFS optimizations, this allows for branch server consolidation at the data center. Having full-featured local print services reduces the amount of traffic transiting the WAN. Without the Cisco WAAS print services, print jobs are sent from a branch client to the centralized server(s) across the WAN, and then back to the branch printer(s), thus transiting the WAN twice for a single job. The Cisco WAAS eliminates the need for either WAN trip. In a TS implementation, the Cisco WAAS can offer optimization of the RDP traffic for printer redirection to locally attached printers (such as USB-connected printers) at the branch client device.

Note For more information on these enhanced services, see the Cisco Wide Area Application Services (Cisco WAAS) v4.1 Technical Overview at the following URL: http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml

Cisco WAAS Mobile

In addition to Cisco WAAS for branch optimization, Cisco offers Cisco WAAS Mobile for telecommuters, mobile users, small-branch and home-office users who access corporate networks and need accelerated application performance. Cisco WAAS Mobile is purpose-built for Microsoft Windows PCs and laptops.

Advanced Data Transfer Compression

Cisco WAAS Mobile maintains a persistent and bi-directional history of data on both the mobile PC and the Cisco WAAS Mobile server. This history can be used in current and future transfers, across different VPN sessions, or after a reboot, to minimize bandwidth consumption and to improve performance. In addition, instead of using a single algorithm for all file types, Cisco WAAS Mobile uses a file-format specific compression to provide higher-density compression than generic compression for Microsoft Word, Excel, and PowerPoint files, Adobe Shockwave Flash (SWF) files, ZIP files, and JPEG, GIF, and PNG files.

Application-Specific Acceleration

Cisco WAAS Mobile reduces application-specific latency for a broad range of applications, including Microsoft Outlook Messing API (MAPI), Windows file servers or network attached storage using CIFS, HTTP, HTTPS and other TCP-based applications, such as RDP.

Transport Optimization

Cisco WAAS Mobile extends Cisco WAAS technologies to handle the timing variations found in packet switched wireless networks, the significant bandwidth latency problems of broadband satellite links, and noisy Wi-Fi and digital subscriber line (DSL) connections. The result is significantly higher link resiliency.

Note For more information on Cisco WAAS Mobile, see the Cisco Wide Area Application Services (Cisco WAAS) Mobile Configuration Guides at the following URL: http://www.cisco.com/en/US/products/ps9523/products_installation_and_configuration_guides_list.html

Cisco Network Analysis Module

The Cisco Catalyst 6500 and Cisco 7600 Series Cisco NAM, Cisco NAM 2200 appliance and branch router series Cisco NAM provide performance monitoring, traffic analysis and advanced troubleshooting capabilities. Cisco NAM offers real-time visibility into applications such as Microsoft Window Server 2008 Terminal Services. The Cisco NAM can monitor, analyze and report on traffic via Switched Port Analyzer (SPAN) ports, NetFlow, and Cisco WAAS appliances.

Intelligent Application Performance Analytics

The Cisco NAM provides intelligent application performance (IAP) measurements to accurately characterize end-user experience. It analyzes the TCP-based client/server message to provide transaction and session-based statistics. Intelligence derived from integrated application and network visibility helps to isolate application problems to the network, application, or server. It also helps to quickly analyze the root cause and resolve problems to minimize any impact to end users.

Visibility into WAN-Optimized Networks

Cisco NAM 4.0 uses the built-in instrumentation on the Cisco WAE as additional data sources to gather flow data for optimized traffic and provide end-to-end application performance visibility in a Cisco WAAS environment. It measures and reports on application response time, transaction time, bandwidth usage and LAN/WAN data throughput, and other metrics. As a result, it can accurately quantify the impact of Cisco WAAS optimization.

Network and Application Usage Analysis

One of the foundations of Cisco NAM is its ability to look inside the live packet to gather information on applications, hosts, and conversations. Application monitoring identifies every application that has consumed bandwidth, reports how much bandwidth has been consumed, and detects which hosts are using which applications. Host-and-conversation pair monitoring provides bandwidth consumption per host and shows which hosts are talking to each other along with the amount of traffic each host is generating. Monitoring applications, hosts, and conversations can help to proactively spot bottlenecks before the network suffers impact to performance and availability. It can also help improve the consistency and quality of both individual and overall network services since these metrics reveal usage patterns for users and for router and switch, interface, server, and application resources. Besides delivering a real-time snapshot of bandwidth usage and consumption, Cisco NAM also delivers a continuous historical view of how the bandwidth was used so the network administrator can quickly decide when and where to make changes in network resources.

Advanced Troubleshooting for Cisco NAM

On detecting degradation in performance, Cisco NAM can automatically trigger packet capture to help investigate and analyze the root cause. Captures can be performed using a web browser from any desktop and packet decodes can be viewed through the web-based Traffic Analyzer GUI.

Note For more information on the Cisco NAM family of products, see the following URL: http://www.cisco.com/go/nam

Solution Components—Software Versions

Table 1 lists the software component and releases used in the solution.

Table 1 Solution Software Components and Releases

Location	Device	Version
Branch Router	Cisco ISR 2851	12.4.22T
Branch Switch	Cisco Catalyst 3560	12.2.46-SE
Branch WAE	Cisco WAE-512	4.1.1c
WAN Router	Cisco 7206VXR – NPE-G2	12.4.22T
HQ WAE	Cisco WAE-512	4.1.1c
Core Layer Switches	Cisco Catalyst 6500 Supervisor 720	12.2.33-SXI1
Aggregation Layer Switches	Cisco Catalyst 6500 Supervisor 720	12.2.33-SXI1
Access Layer Switches	Cisco Catalyst 6500 Supervisor 720	12.2.33-SXI1
WAAS Central Manager	Cisco WAE-512	4.1.1c
WAAS Mobile Server	Cisco WAAS Mobile	3.4.2
Cisco ACE Module	Cisco ACE20 Module	A2(1.4)
Cisco NAM Module	Cisco NAM-2	4.0(1)
DMZ Firewall	ASA 5520	8.04
DMZ Switch	Cisco Catalyst 6500 Supervisor 720	12.2.33-SXI1
DMZ ACE Module	Cisco ACE20 Module	A2(1.4)
Internet Router	Cisco 7206VXR – NPE-G2	12.4.22T
All Windows Servers	Microsoft Windows Server 2008	Data Center Edition
Client OS	Microsoft Windows Vista Microsoft Windows XP	Enterprise Edition – SP1 Professional – SP3

Microsoft Windows 2008 Terminal Services Solution Overview

The TS2008 solution offers many advantages to customers to include remote access to applications and desktops, integrated application delivery, simplified printing, and more. The following new or updated features of TS2008, along with a well-designed Cisco solution, help to achieve the best possible customer experience while also providing availability, security, and ease of deployment and management:

- Expanded support for client-side device redirection such as media players and digital cameras.
- Updated support for large monitors or multiple monitors via custom display resolutions and the new multi-monitor support.
- Single sign-on allows for a user to be able to use one set of credentials to access resources on the domain.
- Easy Print allows for the client's local printer to be mapped to the remote session and provides for the elimination of print drivers having to be loaded on the terminal server.
- RemoteApp allows for a user to access one or many different applications that are located on a terminal server as though they were located directly on the client—without having to run a full remote desktop session.
- Terminal Services Web Access (TSWA) allows administrators to publish remote applications and desktops that can be accessed via a web page.
- Terminal Services Gateway (TSGW) allows for remote users to access remote desktops or applications (using RemoteApp) from outside the firewall using RDP over HTTPS (port 443).
- Terminal Services Session Broker (TSSB), along with the Cisco ACE, allows for the high availability and load balancing of RDP sessions to the most optimal terminal server in a Terminal Server (TS) farm.

Information on features, advantages, and comparisons between TS2008 and TS2003 can be found at the following URL:

http://technet.microsoft.com/en-us/library/cc733093.aspx

TS2008 requires an existing Microsoft Active Directory (AD) deployment and leverages AD as a means to authenticate, store, and share information within the terminal services environment. More information regarding the planning and deployment of Microsoft AD can be found here:
http://technet.microsoft.com/en-us/library/cc268216.aspx

Microsoft Windows Server 2008 Terminal Services Roles

There are five *roles* in TS2008. Each role serves a unique purpose within the Terminal Services architecture and is flexible enough to be deployed in various sized organizations with varying requirements.

Most roles, except those exposed directly to the Internet, can be installed together on a single platform or can be deployed completely independent of one another. SMB customers can leverage the diverse number of TS2008 features while limiting the amount of hardware required for deployment by deploying the roles on the same server. Large organizations can leverage having multiple roles deployed in a redundant fashion on independent hardware platforms in geographically dispersed locations.

The five roles in Windows Server 2008 Terminal Services are:

- Terminal Server (TS)
- Terminal Services Licensing (TS Licensing)

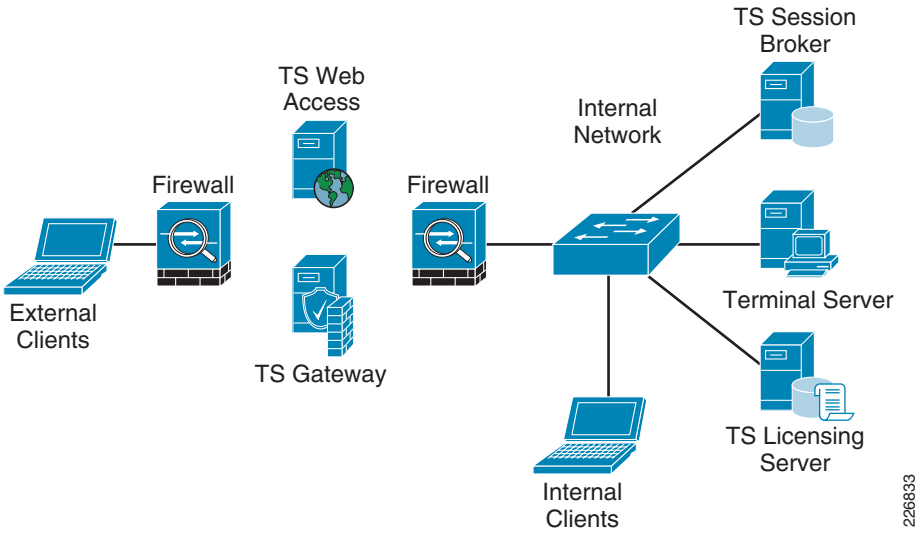
- Terminal Services Gateway (TSGW)
- Terminal Services Session Broker (TSSB)
- Terminal Services Web Access (TSWA)

The sections that follow summarize these five roles and are not meant to provide a tutorial on the architecture, design, and operation of each role.

Detailed information on the Microsoft Windows Server 2008 Terminal Services product, architecture, and design can be found at the following:
http://technet.microsoft.com/en-us/windowsserver/terminal-services/default.aspx

Figure 3 presents an overview of the five TS2008 roles and their general locations in the network.

Figure 3 TS2008 High-Level Diagram]



Terminal Server

The TS role is the core role in the overall TS2008 architecture. The TS allows for users to connect to either a full remote desktop session or to specific applications (using RemoteApp) installed on the TS. Users connect from thin or thick clients to the TS using the RDP.

Unlike many traditional server roles that provide services for only one or a few applications, such as a web server or database server, the TS acts much like a desktop client, but for a large number of users. Due to this unique role, it is recommended that the TS role be installed as a dedicated installation and that it does not run other roles (see "TS Licensing" section on page 17).

TS Licensing

The TS Licensing role maintains a database that is used to track the status of those that have licenses to access the TS. TS Client Access Licenses (TS CAL) are purchased from Microsoft and are available per-user and per-device. Per-device TS CALs are assigned to computers and per-user TS CALs are used as a way to track the total usage of user sessions to the TS and to ensure enough TS CALs are purchased and available for the total number of user sessions.

The TS Licensing role is a very low CPU/memory/network intensive role and only communicates to the TS when the TS is requesting a TS CAL. It is appropriate for the TS Licensing role be installed on a TS due to its low impact.

TS Gateway

The TSGW role is new for Windows Server 2008 and provides users access to a full remote desktop or RemoteApp-deployed applications from essentially anywhere on the Internet. The TSGW sits at the perimeter of a customer's network behind a firewall and provides encrypted access from external clients to the internal TS by running RDP over HTTPS.

Prior to the TSGW role being available, an administrator relied on traditional client VPN connections to provide secured access to the internal TS deployment. While this is still applicable and even preferred if the client must access resources in addition to their RDP sessions, it was often overkill if a thin-client located at a kiosk or a mobile user merely needed quick access to their TS connection. TSGW allows for quick and encrypted access to the TS role.

TS Session Broker

The TSSB role is an update to the function provided by the old Session Directory that provides simple session-based load balancing for terminal servers. The TSSB can identify to which TS or TS farm (grouping of terminal servers) an RDP request is intended, whether the user has an existing session open on the TS, and the TS that has the lowest number of sessions. When matched with a hardware load balancer, such as the Cisco ACE, the TSSB can combine its session information with the Cisco ACE's advanced Layer-4 through Layer-7 server load balancing policies to provide the best distribution in load, high availability, and security to the TS or TS farm.

TS Web Access

The TSWA role is also new for Windows Server 2008 Terminal Services. TSWA is tightly integrated with IIS 7.0 and is used to allow remote HTTP/HTTPS users access to published applications (via RemoteApp) and/or a full remote desktop all from one easy-to-use web page.

Note Throughout the rest of this publication, there will be several illustrations and explanations on how these TS2008 roles are deployed and how the Cisco solution applies to each.

Design and Implementation Details

The following sections describe the design and implementation of TS2008 when used with Cisco ACE, Cisco NAM, and Cisco WAAS/Cisco WAAS Mobile products.

Table 2 provides a brief overview of which methods of server load-balancing (SLB), network optimization, and SSL offload are supported by the TS2008 roles.

Table 2 Microsoft Windows Server 2008 Roles and LB/Optimization/Offload Methods Supported

Terminal Services Role	Server Load-Balancing	SSL Offload	Network Optimization
Terminal Server	Cisco ACE	N/A	Cisco WAAS or Cisco WAAS Mobile
TS License	N/A	N/A	N/A

Table 2 Microsoft Windows Server 2008 Roles and LB/Optimization/Offload Methods Supported

Terminal Services Role	Server Load-Balancing	SSL Offload	Network Optimization
TS Gateway	Cisco ACE	Cisco ACE	Cisco WAAS or Cisco WAAS Mobile
TS Session Broker	Works in conjunction with Cisco ACE	N/A	N/A
TS Web Access	Cisco ACE	Cisco ACE	Cisco WAAS or Cisco WAAS Mobile

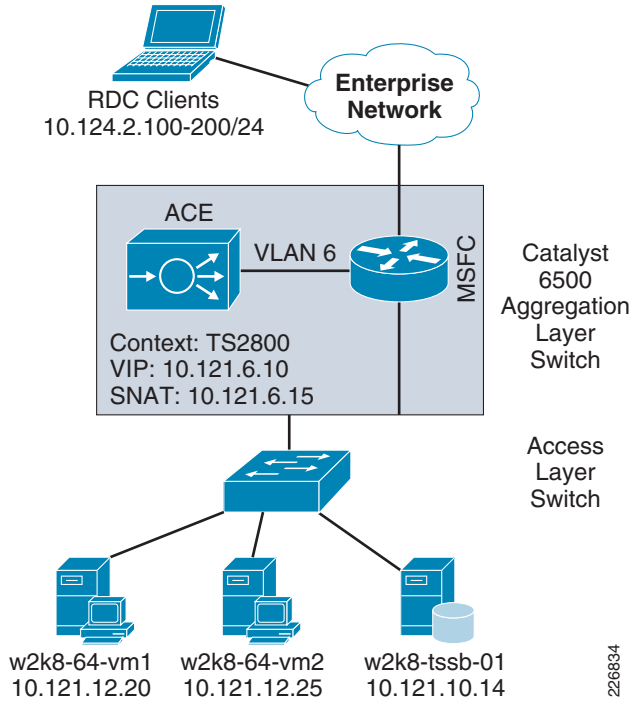
Using the information in Table 2, the remainder of this publication focuses on applying server load-balancing, SSL offload, and network optimization to the appropriate TS2008 roles.

Deploying Cisco ACE for the Terminal Server and TS Session Broker Roles

The terminal server farm members and TS Session Broker servers are located inside the data center access layer. The Cisco ACE is deployed at the data center aggregation layer as either a module or an appliance. In the design used for this paper, the Cisco ACE module is deployed using one-arm mode.

Figure 4 illustrates the various components, names, and IP addressing used in the deployment of Cisco ACE for the TS and TSSB roles.

Figure 4 Detailed Diagram for Cisco ACE and TS/TSSB Roles



The following sections describe the basics of load balancing terminal servers and how the Cisco ACE participates with the TS Session Broker to provide additional intelligence for reestablishing connections.

Load Balancing/Redirection Overview

There are two forms of load balancing that can be used between the client and the TS farm when a TSSB is used: IP address redirection and routing tokens. IP address redirection can be used when the RDC client has direct access, via both routing and security access, to the TS server farm. The following steps illustrate the basic flow of IP address redirection:

1. The client uses RDC to connect to the Cisco ACE and is routed to the most-appropriate terminal server (based on the Cisco ACE SLB policy). The Cisco ACE virtual IP address (VIP) is in DNS and is used as the name/IP address in the RDC.
2. The TS that received the RDP connection from the Cisco ACE contacts the TSSB to determine whether the client connection must be redirected. This is done to determine whether this is a new connection or the client is reconnecting to an already established RDP session that might be on another TS in the farm.
3. The TSSB replies back with the IP address of the final TS to which the client must connect. The redirecting TS sends the IP address of the final TS back to the client.
4. The client uses the information sent from the first TS to establish a new connection directly to the final TS for the session and bypasses the Cisco ACE for this flow.

In essence, the Cisco ACE is only providing SLB for the first stage of the connection. This is fine if the routing and security policies allow for direct connections between the client and the TS farm members. This is also somewhat common in smaller networks where sophisticated Layer-4 through Layer-7 SLB is not required. Most often, administrators want more control over connections to servers located in the data center access layer and want to leverage the security features of the Cisco ACE, such as ACLs, TCP normalization, and so on.

The second load balancing method available with the TSSB is the use of routing tokens. Routing tokens are used when direct IP connectivity between the client and the TS farm is not allowed. The load balancer must support the use of routing tokens because the load balancer must look into the flow to find the routing token information (an Layer-7 operation). The following steps illustrate the basic flow of the routing token redirection method:

1. The client uses RDC to connect to the Cisco ACE (Cisco ACE VIP is in DNS and is used as the name/IP address in the RDC) and is routed to the most appropriate terminal server (based on the Cisco ACE SLB policy).
2. The TS that received the RDP connection from the Cisco ACE contacts the TSSB to determine whether the client connection must be redirected.
3. The TSSB replies back with the final TS to which the client must connect. The TS sends the client a routing token (embedded in the token is the IP address of the final TS) and instructs the client to reconnect to the Cisco ACE VIP.
4. The Cisco ACE inspects the routing token information and connects the RDP session to the TS that is identified in the routing token.

When no routing token is present (no TS IP address present due to this being the initial RDP session for the client) or if the TS is down due to it being out-of-service or having failed the health probes, the Cisco ACE will resort to its standard Layer-4 SLB policy to find the next available TS to which to forward the RDP connection.

Routing Token Overview

This section is not meant to educate the reader on the RDP mechanics or packet layout, but presents a brief overview of routing token operation.

The RDP protocol component uses X.224—an approved International Telecommunication Union-Telecommunication (ITU-T) standardization section recommendation—during the connection establishment phase. X 224 is used by RDP to set various connection parameters, such as supported security protocols and routing tokens.

Routing tokens use a *cookie* to set the value of either a DOMAIN\USERID or the ASCII formatted representation of the TS IP address and port number. During the initial request, there is no routing token information present from the TS (as explained in the preceding section). What can be seen in the packet bytes section of the capture is the line `Cookie: mstshash=BLD\ts1`. When no cookie is set by the TS for the client (only happens after a session has been established and then disconnected), a default cookie is set which is the *UserName* of the authenticating client as in this instance.

The following packet capture shows the client (10.124.2.122) RDP connection request to the Cisco ACE VIP (10.121.6.10) using X.224:

```
No.     Time        Source                Destination           Protocol Info
     56 59.237014   10.124.2.122          10.121.6.10           X.224    Connection
Request (0xe0)

Frame 56 (99 bytes on wire, 99 bytes captured)
Ethernet II, Src: Vmware_8e:27:71 (00:50:56:8e:27:71), Dst: Cisco_a5:50:43
(00:12:d9:a5:50:43)
Internet Protocol, Src: 10.124.2.122 (10.124.2.122), Dst: 10.121.6.10 (10.121.6.10)
Transmission Control Protocol, Src Port: 49285 (49285), Dst Port: ms-wbt-server (3389),
Seq: 1, Ack: 1, Len: 45
TPKT, Version: 3, Length: 45
ITU-T Rec X.224
    Length: 40
    1110 .... = Code: Connection Request (0x0e)
    SRC-REF: 0x0000
    0000 .... = Class: Class 0 (0x00)

0000  00 12 d9 a5 50 43 00 50 56 8e 27 71 08 00 45 00   ....PC.PV.'q..E.
0010  00 55 58 3b 40 00 80 06 00 00 0a 7c 02 7a 0a 79   .UX;@......|.z.y
0020  06 0a c0 85 0d 3d ae c5 8c 96 69 ee 0a 78 50 18   .....=....i..xP.
0030  fa f0 1d c0 00 00 03 00 00 2d 28 e0 00 00 00 00   .........-(.....
0040  00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73   .Cookie: mstshas
0050  68 3d 42 4c 44 5c 74 73 31 0d 0a 01 00 08 00 03   h=BLD\ts1.......
0060  00 00 00
```

Once the client has a running RDP session on a TS, disconnects (disconnect is closing the session without logging off), and then later reconnects, the TS sends the client the routing token in its reply (see process steps in the preceding section to understand the flow). When reconnecting, the client again uses the X.224 connection request, but this time a routing token is present with the IP address and TCP port number for the TS that has maintained the client's session.

The following packet capture shows the client RDP connection request using X.224 with a populated routing token for the TS:

```
No.     Time        Source                Destination           Protocol Info
298 68. 488395      10.124.2.122          10.121.6.10           X.224    Connection
Request (0xe0)

Frame 298 (108 bytes on wire, 108 bytes captured)
Ethernet II, Src: Vmware_8e:27:71 (00:50:56:8e:27:71), Dst: Cisco_a5:50:43
(00:12:d9:a5:50:43)
Internet Protocol, Src: 10.124.2.122 (10.124.2.122), Dst: 10.121.6.10 (10.121.6.10)
Transmission Control Protocol, Src Port: 49287 (49287), Dst Port: ms-wbt-server (3389),
Seq: 1, Ack: 1, Len: 54
TPKT, Version: 3, Length: 54
ITU-T Rec X.224
    Length: 49
```

```
    1110 .... = Code: Connection Request (0x0e)
    SRC-REF: 0x0000
    0000 .... = Class: Class 0 (0x00)

0000  00 12 d9 a5 50 43 00 50 56 8e 27 71 08 00 45 00   ....PC.PV.'q..E.
0010  00 5e 58 a7 40 00 80 06 00 00 0a 7c 02 7a 0a 79   .^X.@......|.z.y
0020  06 0a c0 87 0d 3d 62 de c6 4f d7 16 c2 25 50 18   .....=b..O...%P.
0030  fa f0 1d c9 00 00 03 00 00 36 31 e0 00 00 00 00   .........61.....
0040  00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 3d 34 32   .Cookie: msts=42
0050  30 32 34 37 38 31 38 2e 31 35 36 32 39 2e 30 30   0247818.15629.00
0060  30 30 0d 0a 01 00 08 00 03 00 00 00               00........
```

The cookie set by the TS is **`Cookie: msts=420247818.15629.0000`**, which seems to be an arbitrary number. However, there is a method to understanding this cookie value. consider these values:

- **420247818** = the IP address of the TS
- **15629** = the TCP port

You can dissect these values as follows:

1. Take **420247818** and convert it to HEX which is = **0x190C790A**
2. Reverse the HEX value: **0A 79 0C 19**
3. Convert from HEX: **0A=10, 79=121, 0C=12, 19=25**
4. IP address= **10.121.12.25**
5. Perform the same steps on **15629** and you end up with a TCP port number of **3389**.
6. The cookie tells the Cisco ACE to connect the RDP session to host **10.121.12.25:3389**.

Additional information on RDP X.224 connections can be found at the following URLs: http://msdn.microsoft.com/en-us/library/cc240470(PROT.10).aspx and http://msdn.microsoft.com/en-us/library/aa381177(VS.85).aspx

TS Session Broker Logging

The session information can be logged on the TSSB by configuring the registry to enable the output to a file. Instructions on how to enable TSSB logging can be found at the following URL: http://support.microsoft.com/kb/327508.

The following log output from the TSSB shows an initial connection by a client **BLD\ts1** which connects to **TS 10.121.12.25** (**w2k8-64-vm2.bld.ese.com**):

Initial connection:

```
3588: 11:34:37 AM In ServOnline, the Server Address from RPC is 10.121.12.25  NumOfIPaddr:
1
3588: 11:34:37 AM In ServOnline:AddServerToSD
3588: 11:34:37 AM In ServOnline:AddServerToSD, ClusterName=ESE_FARM_1, SrvOnlineFlags=1
InDrain:10000 LB_ServerWeight:100
3588: 11:34:37 AM In ServOnline:AddServerToSD, the Server Name is w2k8-64-vm2.bld.ese.com
3588: 11:34:37 AM In ServOnline:AddServerToSD, the Server NB Name is W2K8-64-VM2
3588: 11:34:37 AM In ServOnline:AddServerToSD, the Server Address from RPC is 10.121.12.25
NumOfIPaddr: 1
3588: 11:34:37 AM In ServOnline:AddServerToSD, ServerID is 1
3588: 11:34:37 AM RepopAllSess: ServID = 1, NumSessions = 2, ...
. . .
3588: 11:34:37 AM RepopAllSess: ServID = 1, SessionId = 3, ts1 BLD...
3588: 11:34:37 AM RepopAllSess: ServID = 1, NumSessions = 0, ...
3588: 11:34:37 AM In SetSessRec, ServID=1, SessID=3, TSProt=2, ResWid=1024, ResHt=768,
ColDepth=4
```

The client disconnects:

```
3588: 11:36:46 AM In GetUserDiscSessEx: ServID = 1, User: ts1, Domain: BLD AppType:
3588: 11:36:46 AM GetUserDiscSess:ServerAddress:10.121.12.25 NumOfServerAddresses: 1
3588: 11:36:46 AM GetUserDiscSess:SessionID 3
3588: 11:36:46 AM GetUserDiscSess:AppType
3588: 11:36:46 AM GetUserDiscSess returns 1 sessions
3588: 11:36:47 AM In SetSessRec, ServID=1, SessID=3, TSProt=2, ResWid=1024, ResHt=768,
ColDepth=4
```

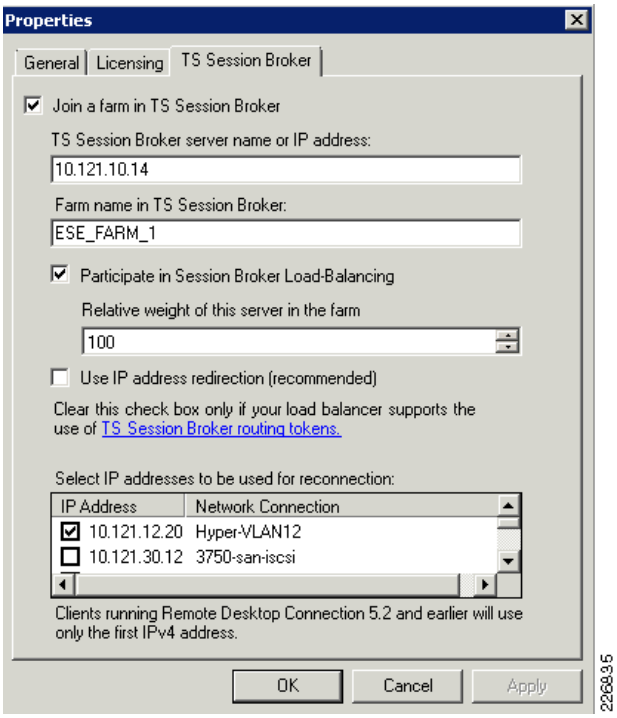
The client performs a logoff action for the session:

```
3588: 11:38:26 AM In DelSession, ServID=1, SessID=3
```

Terminal Servers and TS Session Broker Configuration Summary

Figure 5 shows the TSSB configuration window from one of the two TSes. Notice that the *Use IP address redirection* checkbox is not selected. This enables the use of routing tokens.

Figure 5 TSSB (10.121.10.14) config for w2k8-64-vm1.bld.ese.com (10.121.12.20)



Detailed instructions for installing the terminal server and TS Session Broker can be found at the following URLs:

- *Session Broker Step-by-Step Guide*
  http://technet.microsoft.com/en-us/library/cc772418.aspx
- *Session Broker TechNet Documentation*
  http://technet.microsoft.com/en-us/library/cc771419.aspx

Cisco ACE Configuration for TS and TSSB Roles—Installing Cisco ACE and MSFC Configuration

A Cisco ACE module interacts with clients and servers via virtual LANs (VLAN) that are set up in the Sup720. These VLANs must be configured on the Sup720 to be allowed to be sent to the Cisco ACE module. Without this configuration, the Cisco ACE does not receive any traffic from any VLAN.

The following configuration steps are performed on the MSFC.

Step 1 Add one-arm, management, and failover VLANs:

```
vlan 6
  name Cisco ACE-TS2008
!
vlan 15
  name Cisco ACE-MGMT
!
vlan 100
  name Cisco ACE-FT-VLAN
!
```

Step 2 Add the service line card (SVCLC) configuration.

For this deployment, Cisco ACE is installed in slot 6 in the Cisco Catalyst 6500 chassis. VLAN 6 is for the one-arm connection, VLAN 15 is for management, and VLAN 100 is for the fault-tolerant link. The following configuration must be added to allow Cisco ACE-specific VLAN traffic to be directed towards Cisco ACE:

```
svclc multiple-vlan-interfaces
svclc module 6 vlan-group 1
svclc vlan-group 1 6,15,100
```

Step 3 Add the switched virtual interface (SVI) interface VLAN configuration.

The SVI (interface VLAN) configuration defines the Layer-3 instance on the router via the Multilayer Switch Feature Card (MSFC). The Cisco ACE one-arm configuration for the TS2008 VLAN SVI is as follows:

```
interface Vlan6
  description Cisco ACE-VLAN-ONE-ARM-TS2008
  ip address 10.121.6.2 255.255.255.0
  standby 1 ip 10.121.6.1
  standby 1 priority 110
  standby 1 preempt delay minimum 180
  standby 1 authentication ese
```

Define the Cisco ACE Context

You must define the context and associate the appropriate one-arm VLAN with that context. The following configuration is applied in the Admin Cisco ACE context:

```
context TS2008
  description Context for TS2008 Services
  allocate-interface vlan 6
```

Remote Management Access

To access the Cisco ACE module remotely using Telnet, secure shell (SSH), SNMP, HTTP, or HTTPS or to allow ICMP access to the Cisco ACE module, a policy must be defined and applied to the interface(s) through which access is to be permitted. The following configuration steps are required.

Step 1 Configure a **class-map** of type management:

```
class-map type management match-any REMOTE-MGMT
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
  50 match protocol https any
```

Step 2 Configure a **policy-map** of type management:

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

Step 3 Apply a **policy-map** to the VLAN interfaces:

```
interface vlan 6
  service-policy input REMOTE-ACCESS
```

Configuring Interface(s) and Default Gateway

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

Basic interface configuration includes the following:

- An ACL to permit/deny traffic through Cisco ACE. For example:

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

- IP address and network mask of the interface(s); also apply the ACL from previous step:

```
interface vlan 6
  ip address 10.121.6.5 255.255.255.0
  peer ip address 10.121.6.6 255.255.255.0
  alias 10.121.6.4 255.255.255.0
  access-group input EVERYONE
  access-group output EVERYONE
```

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

```
interface vlan 6
  access-group input EVERYONE
  access-group output EVERYONE
  no shutdown
```

- Default gateway can be configured as:

```
ip route 0.0.0.0 0.0.0.0 10.121.6.1
```

Probes

Cisco ACE uses probes to verify the availability of a real server. Probes are configured by defining their type and name.

There are different types of probes that can be configured on Cisco ACE. The following output example lists these probes:

```
ACE1/Admin(config)# probe ?
  dns       Configure dns probe
  echo      Configure echo probe
  finger    Configure finger probe
  ftp       Configure ftp probe
  http      Configure http probe
  https     Configure https probe
  icmp      Configure icmp probe
  imap      Configure imap probe
  ldap      Configure ldap probe
  pop       Configure pop probe
  radius    Configure radius probe
  scripted  Configure script probe
  smtp      Configure smtp probe
  tcp       Configure tcp probe
  telnet    Configure telnet probe
  udp       Configure udp probe
```

Some key timers and parameters must be tuned when probes are configured. These parameters influence how rapidly Cisco ACE (or any load balancer) takes a server out of rotation and brings it back into service.

The following parameters can be tuned for probes of any type (ICMP, UDP, TCP, HTTP,HTTPS, or scripted):

- *faildetect*—Refers to the number of consecutive failed probes that qualify a server to be declared failed. The faildetect parameter is configured as a counter value. The default value is 3.
- *interval*—Refers to the frequency with which the Cisco ACE sends probes to a server. The interval is configured in seconds. The default value is 120 seconds.
- *passdetect*—Determines how the Cisco ACE re-probes the server after the server has been declared failed. The passdetect variable has two attributes:
  - *passdetect count*—Refers to the number of consecutive successful responses that a Cisco ACE must see before declaring a server as operational. The default value is 3. This value can be tuned according to the requirements.
  - *passdetect interval*—Refers to the number of seconds that a Cisco ACE waits to probe a server after the server has been declared failed. The default value is 300 seconds.

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

- *Open*—Refers to the duration (in seconds) that Cisco ACE waits to keep a TCP connection open. The default value is 10 seconds. Generally, this value is configured close to the interval value.
- *Receive*—Once a TCP SYN (for a probe) is sent to a server, the value for the receive parameter determines the amount of time that a Cisco ACE waits to receive a reply from the server. This value is configured in seconds and the default value is 10 seconds. Generally, it is configured as equal-to-or-less-than the value interval.
- *Connection*—This parameter determines how the Cisco ACE closes the connection after it has successfully sent a probe. By default, the Cisco ACE closes the connection by sending a TCP FIN to close the connection (referred to as a *graceful* connection termination). Optionally, the Cisco ACE can be configured to close the connection with a TCP RESET by configuring connection parameter as *forced*.
- *Port*—TCP/UDP port number on which this probe is sent. The default values for various probes are:
  - *TCP*—Port 80
  - *UDP*—Port 53
  - *HTTP*—Port 80

  - *HTTPS*—Port 443

- *Request*—Used to configure the HTTP Request method (HEAD or GET) and URL for the probe. The default method is GET and default URL is /. Generally, method and URL are configured according to specific applications.

  This parameter is only applicable to HTTP/HTTPS probes.

- *Expect*—Allows Cisco ACE to detect two values from the server:
  - *expect status*—The HTTP status code (or range) to expect from the server. There is no default HTTP return code expected; it must be explicitly configured.
  - *expect regex*—A regex can be configured to parse a specific field in the response data.

  This parameter is only applicable to HTTP/HTTPS probes.

- *SSL*—Configured to define the cipher and SSL version that the Cisco ACE should use when sending an HTTPS probe. Ciphers and SSL versions supported on Cisco ACE are:

```
ssl cipher:
  RSA_EXPORT1024_WITH_DES_CBC_SHA  EXP1024-DES-CBC-SHA Cipher
  RSA_EXPORT1024_WITH_RC4_56_MD5   EXP1024-RC4-MD5 Cipher
  RSA_EXPORT1024_WITH_RC4_56_SHA   EXP1024-RC4-SHA Cipher
  RSA_EXPORT_WITH_DES40_CBC_SHA    EXP-DES-CBC-SHA Cipher
  RSA_EXPORT_WITH_RC4_40_MD5       EXP-RC4-MD5 Cipher
  RSA_WITH_3DES_EDE_CBC_SHA        3DES-EDE-CBC-SHA Cipher
  RSA_WITH_AES_128_CBC_SHA         AES-128-CBC-SHA Cipher
  RSA_WITH_AES_256_CBC_SHA         AES-256-CBC-SHA Cipher
  RSA_WITH_DES_CBC_SHA             DES-CBC-SHA Cipher
  RSA_WITH_RC4_128_MD5             RC4-MD5 Cipher
  RSA_WITH_RC4_128_SHA             RC4-SHA Cipher

ssl versions:
  SSLv2  SSL Version 2.0
  SSLv3  SSL Version 3.0
  TLSv1  TLS Version 1.0
```

  This parameter is only applicable to HTTPS probes.

To ensure that the terminal servers are online and ready to accept connections, the Cisco ACE is configured to perform a health check to determine whether or not the server is up and running and available on port TCP 3389 (RDP). This is done by creating a TCP probe to be sent to the server on port 3389. Note, that more elaborate probes can be configured via the scripting capability on the Cisco ACE.

The following is a configuration example for RDP:

- TCP RDP probe:

```
probe tcp RDP
  port 3389
  interval 2
  faildetect 2
  passdetect interval 10
  passdetect count 2

ACE1/TS2008# show probe

probe       : RDP
type        : TCP
state       : ACTIVE
----------------------------------------------
  port      : 3389    address     : 0.0.0.0         addr type  : -
  interval  : 2       pass intvl  : 10              pass count : 2
  fail count: 2       recv timeout: 10
                      --------------------- probe results ---------------------
```

```
probe association    probed-address  probes      failed      passed      health
-------------------- ---------------+----------+----------+----------+-------
serverfarm  : TS2008
  real      : w2k8-64-vm1[0]
                       10.121.12.20    114          0            114        SUCCESS
  real      : w2k8-64-vm2[0]
                       10.121.12.25    114          0            114        SUCCESS
```

Real Server

The load balancer selects the real servers (called *rserver* in the Cisco ACE) to send the intended traffic based on a certain set of criteria. When configuring a rserver, be aware that rserver name is case sensitive. The minimum configuration needed for rserver configuration is the IP address and configuring the rserver as inservice. The name of the rserver is locally significant and need not match the real name or DNS name of the server.

To take a server out of rotation on a per-serverfarm basis, rserver should be specified as **no inservice** at the serverfarm level.

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

```
rserver host w2k8-64-vm1
  ip address 10.121.12.20
  inservice
rserver host w2k8-64-vm2
  ip address 10.121.12.25
  inservice
```

Serverfarm

A *serverfarm* is a logical collection of rservers that the load balancer selects based on a certain set of criteria. As with the rserver, the serverfarm name is also case sensitive.

Basic serverfarm configuration includes adding rservers and probes to the serverfarm.

Key configuration options within serverfarm sub-configuration mode are as follows:

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

  A configurable option is *failaction purge*, which forces Cisco ACE to remove the connections established to that rserver and send TCP RST(s) towards the client(s) and rserver(s).

- *predictor*—Refers to the load-balancing algorithm for the serverfarm. Options are:
  - *hash*—Based on source/destination IP address, URL, cookie, and header.
  - *leastconns*—Based on least number of connections. By default slow start is enabled for leastconns and its timing can be tuned using predictor leastconns slow start.

    <1-65535> Specify slow start duration in seconds
  - *roundrobin*—Load balance in a roundrobin fashion (default).
- *probe*—Allows a probe to be applied to the serverfarm. Multiple probes can be applied to the same serverfarm.
- *retcode*—Used to configure server health-checks based on the HTTP return code. The configuration allows you to define a range of HTTP return codes and take an action once a threshold is reached. Syntax is as follows:

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

- *rserver*—Used to associate real servers with a serverfarm. Port address translation, maximum and minimum connections, and weight are some common configurations that can be done in rserver sub-configuration mode.
- *transparent*—Equivalent to **no nat server** on the Content Switching Module (CSM) and **type transparent-cache** on Content Services Switch (CSS). When configured, Cisco ACE does not perform NAT on a Layer-3 IP address from the VIP to rserver's IP address.

The following is an example of basic serverfarm configuration:

```
serverfarm host TS2008
  probe RDP
  rserver w2k8-64-vm1
    inservice
  rserver w2k8-64-vm2
    inservice
```

Load Balancing

The Cisco ACE can load balance RDP sessions based on IP addresses and ports (Layer-3 and Layer-4 SLB) or can persistently load balanced via routing tokens (Layer-7 SLB). In order for the Cisco ACE to parse and act on the routing token information, the Cisco ACE must see inside the packet. The Layer-7 policy is used to accomplish this. If the routing token is not present (usually due to it being a new session) the Cisco ACE will use the Layer-3 and Layer-4 SLB configuration to determine the target TS for the session. The configuration shown in the following procedure applies to the Cisco ACE using routing tokens in participation with the TSSB:

The following example shows the configuration steps needed.

Step 1 Configure the VIP using **class-map** of type **match-all** for RDP (Layer 3 and Layer 4).

```
class-map match-all TS2008-SLB-VIP
2 match virtual-address 10.121.6.10 tcp eq rdp
```

Step 2 Configure the Layer-7 **policy-map** of type **loadbalance** to include the serverfarm.

```
policy-map type loadbalance rdp first-match TS2008-SLB-POL
  class class-default
    serverfarm TS2008
```

Step 3 Configure **policy-map** of type **multi-match** to associate **class-map** configured in Step 1 (associating Layer-3 and Layer-4 policies with Layer7 policy). Other options listed allow the VIP to reply to ICMP echoes and for the VIP to participate in Route Health Injection (RHI) which advertises the VIP as a host (/32) route:

```
policy-map multi-match TS2008-SLB-MULTI
  class TS2008-SLB-VIP
    loadbalance vip inservice
    loadbalance policy TS2008-SLB-POL
    loadbalance vip icmp-reply
    loadbalance vip advertise active
    nat dynamic 1 vlan 6
```

Step 4 Apply **policy-map** to the interface VLAN.

```
interface vlan 6
  nat-pool 1 10.121.6.15 10.121.6.15 netmask 255.255.255.0 pat
```

```
service-policy input TS2008-SLB-MULTI
```

Note The **nat dynamic 1 vlan6** and **nat-pool 1** configurations are required in one-arm mode to force return traffic from the TS back to the Cisco ACE. Without this configuration the source IP address the TS would see is the IP address of the client. The return packets from the TS would bypass the Cisco ACE and go directly to the client and would break the design. In this configuration the source IP the TS will see is 10.121.6.15 and will reply to that address for all return packets.

Redundancy/High Availability

To provide high availability and redundancy, Cisco ACE modules can be set up and configured in a redundant mode. A Cisco ACE can be configured in a typical active/backup redundancy mode or active/active (per context) redundancy mode. The following is an example configuration for the Admin context.

```
! Configure FT interface
!
ft interface vlan 100
ip address 10.121.100.1 255.255.255.248
peer ip address 10.121.10.2 255.255.255.248
no shutdown
!
! Configure FT peer
!
ft peer 1
ft-interface vlan 100
heartbeat count 3
heartbeat interval 1000
!
! Configure interface tracking
!
ft track interface VLAN6
priority 200
!
!  Create a fault tolerant group
!
ft group 1
peer 1
priority 200
preempt
associate-context admin
inservice
!
```

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

Validation

The following **show** command output illustrates that a client (**10.124.2.122**) has connected to the Cisco ACE VIP (**10.121.6.10**) on port 3389. The Cisco ACE has connected from the source NAT address (**10.121.6.15**) to the rserver (**10.121.12.25**):

```
ACE1/TS2008# show conn
```

```
total current connections : 2

conn-id    np dir proto vlan source                destination           state

----------+--+---+-----+----+---------------------+---------------------+------+

2          2  in  TCP   6    10.124.2.122:49306    10.121.6.10:3389      ESTAB

6          2  out TCP   6    10.121.12.25:3389     10.121.6.15:1084      ESTAB
```

The following statistics show the number of load-balanced packets for RDP and the number of packets containing the routing tokens:

```
ACE1/TS2008# show stats loadbalance rdp

+-------------------------------------------------------+

+------------- Rdp Loadbalance statistics -------------+

+-------------------------------------------------------+

 Total parse results received                 : 15

 Total packets load balanced                  : 60

 Total packets with routing token             : 5

 Total packets with token matching no rserver  : 0
```

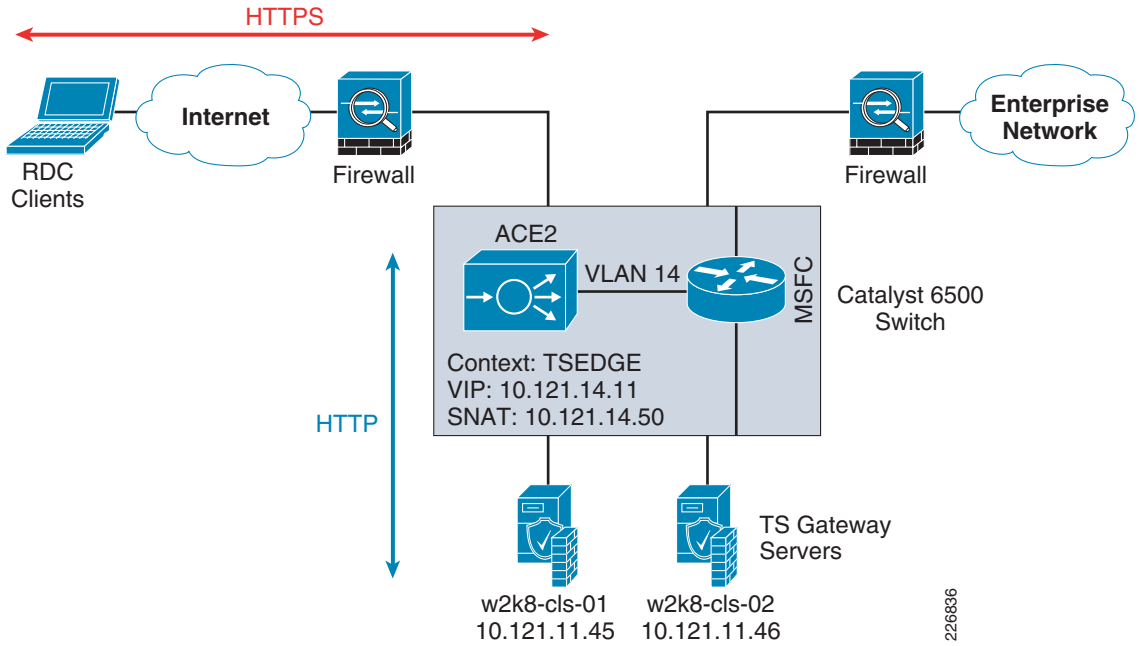
Deploying Cisco ACE for the TS Gateway Role

The TSGW allows for clients to connect to TSes by using TCP port 443 (HTTP over TLS/SSL). The TSGW acts as a proxy for the terminal servers and provides access to clients over TCP port 443 by connecting those client sessions to the TSes over port 3389.

In the design described in this publication, the Cisco ACE is used to perform load balancing for multiple TSGWs and also perform SSL offload for those gateways.

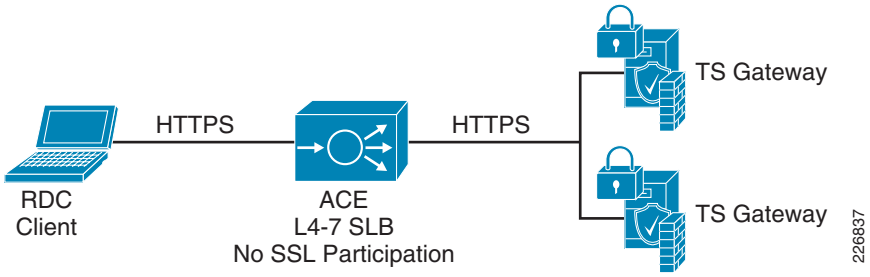
Figure 6 illustrates the various components, names, and IP addressing used in the deployment of Cisco ACE for the TS and TSSB roles.

Figure 6 Diagram for Cisco ACE and TSGW Roles



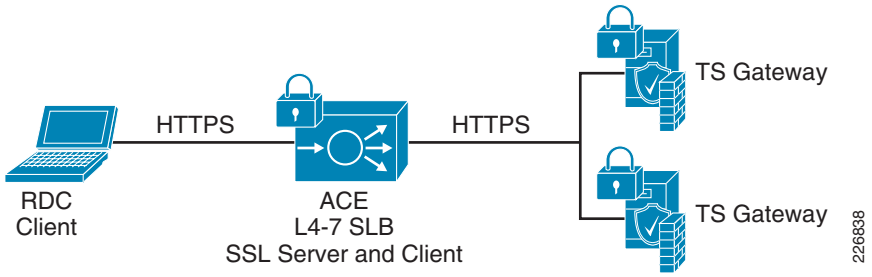
There are a few options available for using the Cisco ACE in conjunction with the TSGW role. The first option (Figure 7) shows the Cisco ACE performing basic load balancing for two TSGWs. The Cisco ACE uses its Layer-4 SLB policy to monitor the health (via a probe) of both TSGWs and pass SSL connections to the most appropriate TSGW based on the SLB policy. The subsequent sections describe the basics of load balancing terminal servers and show how the Cisco ACE participates with the TSSB to provide additional intelligence for reestablishing connections.

Figure 7 Cisco ACE + TSGW—Basic Layer 4 SLB



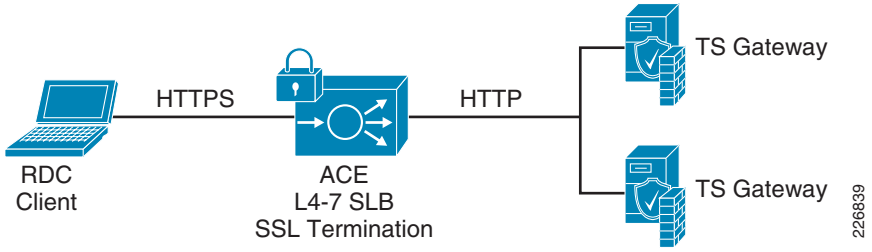
The second option (Figure 8) shows the Cisco ACE performing load balancing along with SSL offload between the client and the Cisco ACE with SSL reestablishment from the Cisco ACE to the TSGW. This combined SSL termination and SSL initiation is called *SSL End-to-End*. One advantage of SSL End-to-End is that it offers the capability of maintaining a level of encryption between the Cisco ACE and server, but allows for the use of a lower cipher than the client-to-Cisco ACE connection which can lessen the SSL load on the TSGW. Figure 8 shows the Cisco ACE serving the role of SSL server (to the client) and also SSL client (to the TSGW).

Figure 8 Cisco ACE + TSGW—SSL End-to-End



The third option (Figure 9) incorporates the Cisco ACE performing load balancing and SSL termination, the SSL connection terminating on the Cisco ACE, and the Cisco ACE communicating with the TSGW over HTTP. This approach allows for the access and resource control of the TS connection access policies (CAP) and TS resource authorization policies (RAP) to be applied from the TSGW—while offloading the resource-intensive SSL operations to the Cisco ACE, which provides hardware-based SSL offload. This publication focuses on the third option.

Figure 9 Cisco ACE + TSGW—SSL Termination



TS Gateway Configuration Summary

Figure 10 shows that two TSGWs are defined.

Figure 10 TS Gateway Server Farm Status

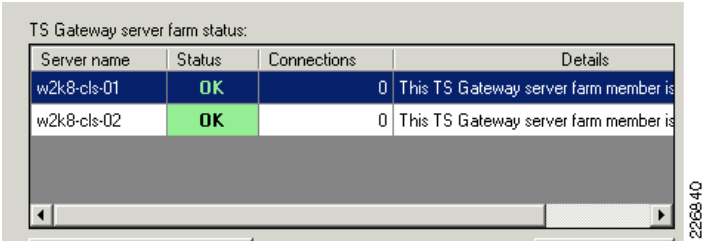
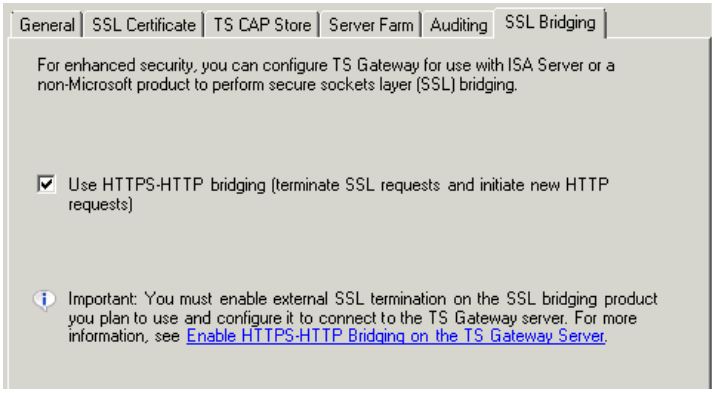


Figure 11 shows the required configuration on the TSGW if SSL offload (*HTTPS-HTTP bridging* is what Microsoft calls it) is to be used. In option 3 summarized in the preceding section, the Cisco ACE performs SSL front-end termination and passes traffic to the TSGW over port 80.

Figure 11 TS Gateway HTTPS-HTTP Bridging



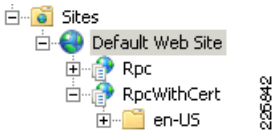
Cisco ACE Configuration for TS Gateway—SLB and SSL Termination

The previous section notated much of the Cisco ACE configuration. For clarity, the following configurations illustrate the TSGW deployment with limited notation and will not include configuration details, such as Cisco Catalyst 6500 VLAN definitions, context, and remote management. The preceding section describes how these configurations are deployed.

Health Probe

One common mistake that users make is to configure a health probe to monitor port 80 or port 443 on the TSGW. The thinking is that if the IIS service is disabled (the TSGW is dependent on that service), then the TSGW is unavailable for accepting connections. While this is true to a certain degree, it does not offer the best view on the availability of the TSGW service. The TSGW uses two applications (as shown in Figure 12) under the default web site in IIS: RPC and RPCWithCert.

Figure 12 TSGW IIS Applications

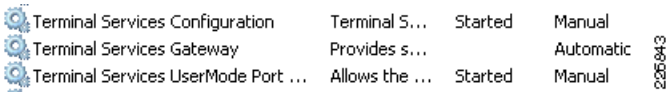


Both require Windows Authentication to allow access. If a probe were setup to monitor these applications, then the load balancer must support NTLM authentication which is not optimal. The alternative is to monitor the root IIS port/directory. The following shows a basic Cisco ACE configuration for an HTTP probe to monitor IIS:

```
probe http TSGW
  interval 2
  passdetect interval 5
  expect status 200 200
```

This is easy enough to do with the Cisco ACE, but it is not optimal either. It is possible for IIS to be running and available, but the TS Gateway service to be down. In this case, a health probe monitoring port 80 or 443 on IIS would still pass and forward connections to the TSGW, but the connection would fail due to the TSGW service being down. Figure 13 illustrates an example in which the health probe for port 80 passes, but the TSGW service is disabled.

Figure 13 Terminal Services Gateway Service Failed on w2k8-tsgw-01




```
ACE2/TSEDGE# show probe TSGW
 probe       : TSGW
 type        : HTTP
 state       : ACTIVE
----------------------------------------------
   port      : 80      address     : 0.0.0.0         addr type  : -
   interval  : 2       pass intvl  : 5               pass count : 3
   fail count: 3       recv timeout: 10
                       -------------------- probe results --------------------
   probe association   probed-address  probes     failed     passed     health
   ------------------ ---------------+----------+----------+----------+-------
   serverfarm  : TSGW
     real      : w2k8-tsgw-01[80]
                       10.121.11.45    49         0          49         SUCCESS
     real      : w2k8-tsgw-02[80]
                       10.121.11.46    49         0          49         SUCCESS
```

A better health probe approach for the TSGW is to monitor a well-known port used by TSGW for RPC proxy services: TCP port 3388. The following process summarizes how you can do this. Note that you can verify that this port is running while the TSGW service is on and that the port is not running with the TSGW services is off.

Step 1 Run the following command from the command prompt on the TSGW with the TSGW service running. The output shows that TCP port 3388 for both IPv4 and IPv6 is listening:

```
C:\> netstat -an |find /i "listening" |find /i "3388"
  TCP    0.0.0.0:3388           0.0.0.0:0              LISTENING
  TCP    [::]:3388              [::]:0                 LISTENING

C:\>
```

Step 2 Stop the TSGW service and re-run the command. There will be no listening port for 3388:

```
C:\> netstat -an |find /i "listening" |find /i "3388"
```

Step 3 With this information, a TCP health probe on the Cisco ACE can be configured to monitor TCP 3388 on the TSGW rservers and bring the server out of rotation if the TSGW or the IIS service fails (remember that the TSGW service is dependent upon IIS, so if the IIS service is stopped or fails, then the TSGW service will also be stopped, but the reverse is not true). The following is an applicable example configuration.

```
probe tcp RPCPROXY
  port 3388
  interval 2
  faildetect 2
  passdetect interval 10
  passdetect count 2
```

Load Balancing

Define the rservers:

```
rserver host w2k8-tsgw-01
  ip address 10.121.11.45
  inservice
rserver host w2k8-tsgw-02
```

```
  ip address 10.121.11.46
  inservice
```

Step 4 Define the serverfarm, add the TCP probe, join the rservers to the serverfarm, and bring the rservers inservice. An example of an applicable configuration follows. Note that there is a port 80 identifier at the end of each **rserver** statement. In this configuration, the Cisco ACE is performing SSL on the client side, but performing HTTP on the TSGW side. The port 80 identifier instructs the Cisco ACE to communicate with the TSGW over port 80 instead of the default port 443 (client side connection).

```
serverfarm host TSGW
  probe RPCPROXY
  rserver w2k8-tsgw-01 80
    inservice
  rserver w2k8-tsgw-02 80
    inservice
```

Step 5 Define the **class-map** and VIP. The VIP 10.121.14.11 is the address that matches the DNS entry for the TSGW address for RDC configuration. The VIP matches on HTTPS (443) which is used by RDC to perform RDP over HTTPS:

```
class-map match-all TSGW-SLB-VIP
  2 match virtual-address 10.121.14.11 tcp eq https
```

Step 6 Associate the serverfarm TSGW with the Layer-7 (HTTP) load balance **policy-map**:

```
policy-map type loadbalance http first-match TSGW-SLB-POL
  class class-default
    serverfarm TSGW
```

Step 7 Tie the Layer-7 and Layer-4 policies together. The VIP replies to ICMP echoes and activates RHI for the VIP address. Note that the policy will be applied to the interface after the SSL configuration is completed:

```
policy-map multi-match TSGW-SLB-MULTI
  class TSGW-SLB-VIP
    loadbalance vip inservice
    loadbalance policy TSGW-SLB-POL
    loadbalance vip icmp-reply
    loadbalance vip advertise active
    nat dynamic 1 vlan 14
```

SSL Termination

Disclaimer*—The discussion of certificates, other than the server certificate on the Cisco ACE, is outside the scope of this document. A thorough understanding of certificates and server authentication is required for anyone deploying the TS2008 solution with or without the Cisco ACE.*

With front-end SSL termination, client-to-Cisco ACE traffic is HTTPS, but the Cisco ACE-to-TSGW traffic is HTTP. It is important to understand that the certificate being configured on the Cisco ACE is known as a *server certificate* because the Cisco ACE is acting as a server to the client. Any client connecting to the Cisco ACE for the purpose of accessing the TSGW must trust the Cisco ACE server certificate by having the certification authority (CA) certificate (from the CA that issued the Cisco ACE certificate) in the client's certificate store.

The following configuration steps illustrate implementing front-end SSL termination.

Step 1 Generate key.

```
ACE2/TSEDGE# crypto generate key 2048 ts2008.key
ACE2/TSEDGE# show crypto key all
```

```
Filename                                 Bit Size Type
--------                                 -------- ----
ts2008.key                               2048     RSA
```

Step 2 Define CSR parameters set.

```
crypto csr-params ts2008-params
  country US
  state Colorado
  locality Boulder
  organization-name ESE
  organization-unit DC
  common-name ts2008.bld.ese.com
```

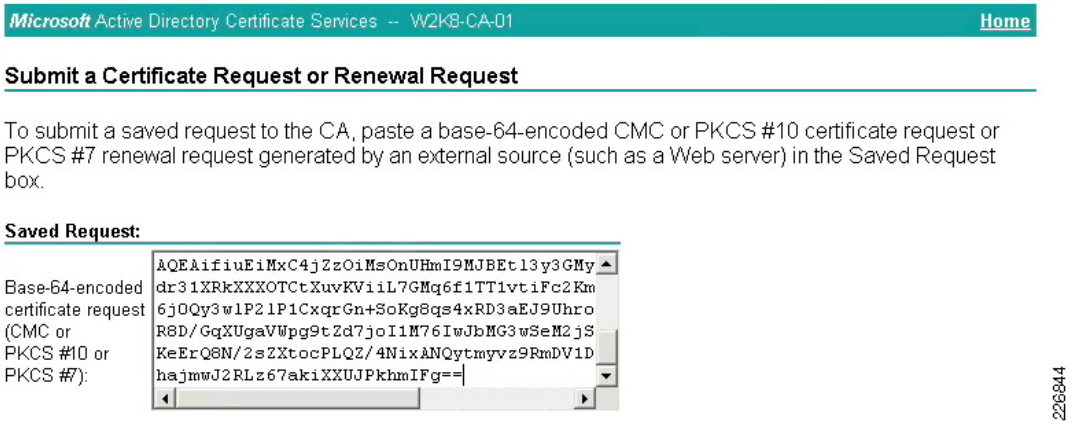
Step 3 Generate the Certificate Signing Request (CSR).

```
ACE2/TSEDGE# crypto generate csr ts2008-params ts2008.key
-----BEGIN CERTIFICATE REQUEST-----
MIICrzCCAZcCAQAwajELMAkGA1UEBhMCVVMxETAPBgNVBAgTCENvbG9yYWRvMRAw
DgYDVQQHEwdCb3VsZGVyMQwwCgYDVQQKEwNFU0UxCzAJBgNVBAsTAkRDMRswGQYD
VQQDExJ0czIwMDguYmxkLmVzZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDf1vHvEqNAz+bzSBBm/FsQ36voDtur7fu6p9yemExgi2rNNPr/FmNR
/aFZDTLmDIszqzaFtD33C/drT7UlhVnBOUbaVzfwIjmpP3atnpY56zWVroS8Pj+J
8PWmfLDrOO8xmdk01JHtwFiwsSM3hX3UukmqL0UWZYm3D366Figw5+7BwoDMUhYj
XB/zA6W6aRgZf5bbNsi+gOUVmdOUm6fri2X5AU44MY2O5IShy6DvvA5yPlRb17k3
YnQS9Y/nQDnQzh1GL8qEL70ToLCgSZubFvMcF/lAJuBmJ02nuCAvldClFWutU32x
AupaZ5yRuTbflCc3q7bI7HRQXkpNR+BdAgMBAAGgADANBgkqhkiG9w0BAQQFAAOC
AQEAifiuEiMxC4jZzOiMsOnUHmI9MJBEtl3y3GMyAR0HZ1xjN5mje8yEga+3ty04
dr31XRkXXXOTCtXuvKViiL7GMq6f1TT1vtiFc2Km8EpZOKWe9ToyTIX/MH1jTDNz
6j0Qy3wlP2lP1CxqrGn+SoKg8qs4xRD3aEJ9Uhrogp+Pl2c5TB2XMCu3W6LCgMlU
R8D/GqXUgaVWpg9tZd7joI1M76IwJbMG3wSeM2jS7UsICPoZhzl8uPzZhbOmCAcj
KeErQ8N/2sZXtocPLQZ/4NixANQytmyvz9RmDV1Dqvi+FY7O5Gu6y8crLw44OXfT
hajmwJ2RLz67akiXXUJPkhmIFg==
-----END CERTIFICATE REQUEST-----
```

Step 4 Obtain certificate.

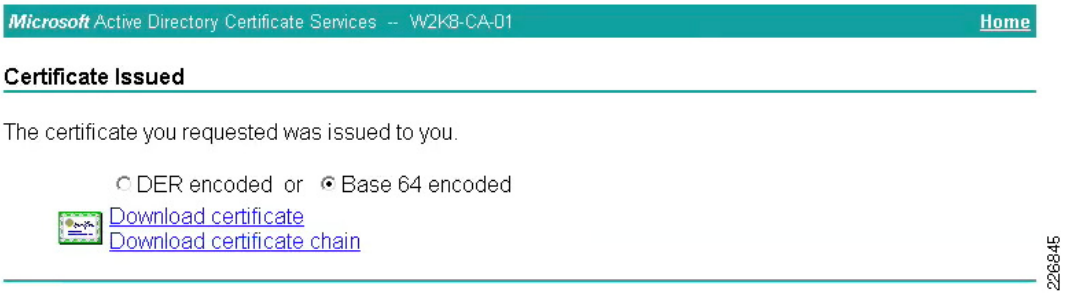
The SSL certificate can be obtained from various CA companies. Figure 14 shows the submission of the above generated CSR on a local Microsoft CA.

Figure 14 Submit Cisco ACE Certificate Request on Microsoft CA Server



A certificate is issued after the request has been submitted and approved by the CA administrator. Figure 15 shows the *Certificate Issued* screen from the Microsoft CA. The certificate file is downloaded and then imported to the Cisco ACE (see Step 5).

Figure 15 Cisco ACE Certificate Issued by Microsoft CA Server



Step 5 Import certificate on Cisco ACE.

```
ACE2/TSEDGE# crypto import ftp 10.121.10.254 administrator ts2008.cer ts2008-cert.cer
Password:
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
##
Successfully imported file from remote server.
```

Note Optionally, the certificate can be imported from the terminal without copying the file over. See the Cisco ACE documentation on using the terminal method.

Step 6 Validate the certificate using the key.

```
ACE2/TSEDGE# crypto verify ts2008.key ts2008-cert.cer

Keypair in ts2008.key matches certificate in ts2008-cert.cer.
```

Step 7 Configure SSL parameters and SSL proxy service as follows:

a. SSL parameter configuration

```
parameter-map type ssl SSLPARAMS
  version TLS1
```

b. SSL proxy service configuration

```
ssl-proxy service SSL-Proxy-TS2008
  key ts2008.key
  cert ts2008-cert.cer
  ssl advanced-options SSLPARAMS
```

Step 8 Apply the SSL proxy server policy:

```
policy-map multi-match TSGW-SLB-MULTI
  class TSGW-SLB-VIP
    ssl-proxy server SSL-Proxy-TS2008
```

Step 9 Apply the policy-map as a **service policy** on the one-arm VLAN. As a reminder, because this is a one-arm configuration, it is necessary to perform source NAT (SNAT) so that the TSGW understands that the source address is that of the Cisco ACE and not the client. The source address (TSGW sees it as the client) will be 10.121.14.50.

```
interface vlan 14
  description VLAN-ONEARM-TSEDGE
  ip address 10.121.14.5 255.255.255.0
  nat-pool 1 10.121.14.50 10.121.14.50 netmask 255.255.255.0 pat
  service-policy input TSGW-SLB-MULTI
```

```
no shutdown
```

Validation

When establishing an RDC connection to a terminal server via the TSGW, the RDC profile (Figure 16) must be configured for the TS which, in this design, is the data center Cisco ACE VIP for the TS farm—**ts-vip.bld.ese.com**. The TSGW settings in the RDC profile (Figure 17) must also have the DNS name for the Cisco ACE VIP for the TSGW configuration—**ts2008.bld.ese.com**.

Note **ts2008.bld.ese.com** in the RDC profile must match the **common-name** found in the Cisco ACE **csr-params** section of the configuration. In most production environments, these settings are deployed via Group Policy to ease the deployment burden and to reduce support issues with users not being able to connect due to common configuration errors.

Figure 16 RDC Profile With Terminal Server Name

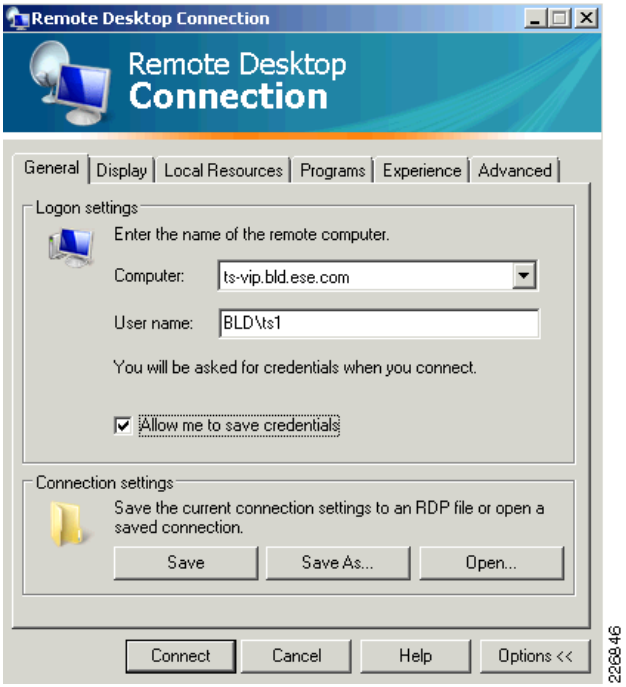
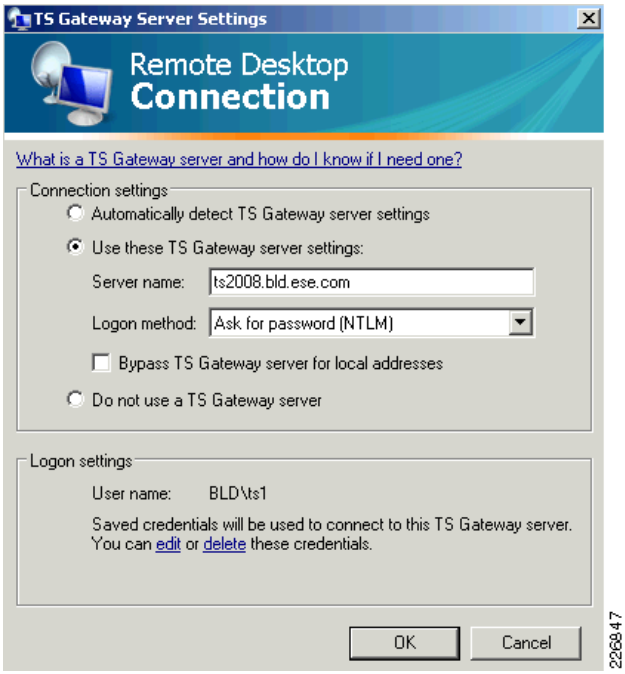


Figure 17 RDC Profile with TS Gateway Settings



The following **show** command output illustrates that the client 10.124.2.122 is connected to the Cisco ACE VIP (10.121.14.11) on port 443 and the Cisco ACE has a connection from its source NAT (10.121.14.50) address to the TSGW (10.121.11.45) on port 80:

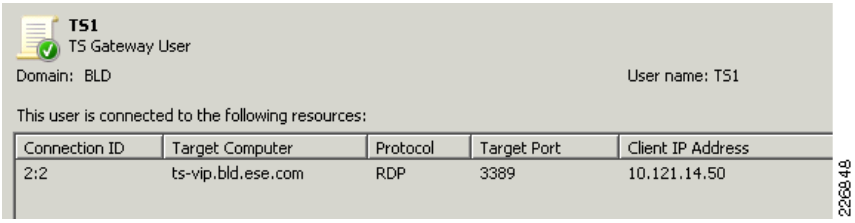
```
ACE2/TSEDGE# show conn

total current connections : 2
conn-id    np dir proto vlan source                 destination            state
----------+--+---+-----+----+---------------------+----------------------+------+
15          1  in  TCP   14    10.124.2.122:49234    10.121.14.11:443       ESTAB
10          1  out TCP   14    10.121.11.45:80       10.121.14.50:1065      ESTAB
```

The combination of the connection status from the Cisco ACE (above) and the TSGW output in Figure 18, yields the following:

- There is a client connection through the perimeter Cisco ACE (represented by the SNAT address of **10.121.14.50**)—see **conn-id 15** in the preceding output.
- The Cisco ACE has a connection to the TSGW—see **conn-id 10** in the preceding output.
- The TSGW has a connection to the downstream Cisco ACE—**ts-vip.bld.ese.com** (data center Cisco ACE that was discussed for load balancing the TS with the TSSB) on port **3389**.
- The Cisco ACE in the data center has a connection to a load balanced TS on port **3389**.

Figure 18 Active Client Connection Using TS Gateway



The previous sections illustrated the configuration of Cisco ACE load balancing for the TS role in conjunction with the TSSB, the Cisco ACE load balancing, and SSL offload of the TSGW. The next section shows the same Cisco ACE that was used to service the TSGW and provides load balancing and SSL offload for the TSWA role.

Deploying Cisco ACE for the TS Web Access Role

The TSWA role provides client access to TS RemoteApps, terminal server farms, and standard remote desktops (such as an individual PC desktop) from a web site.

In this design, the TSWA is deployed in the perimeter of the network in the same area as the TSGW. This allows the same security products, such as the Cisco Adaptive Security Appliance (ASA), and the same Cisco ACE module/appliance to service both the TSWA and TSGW roles.

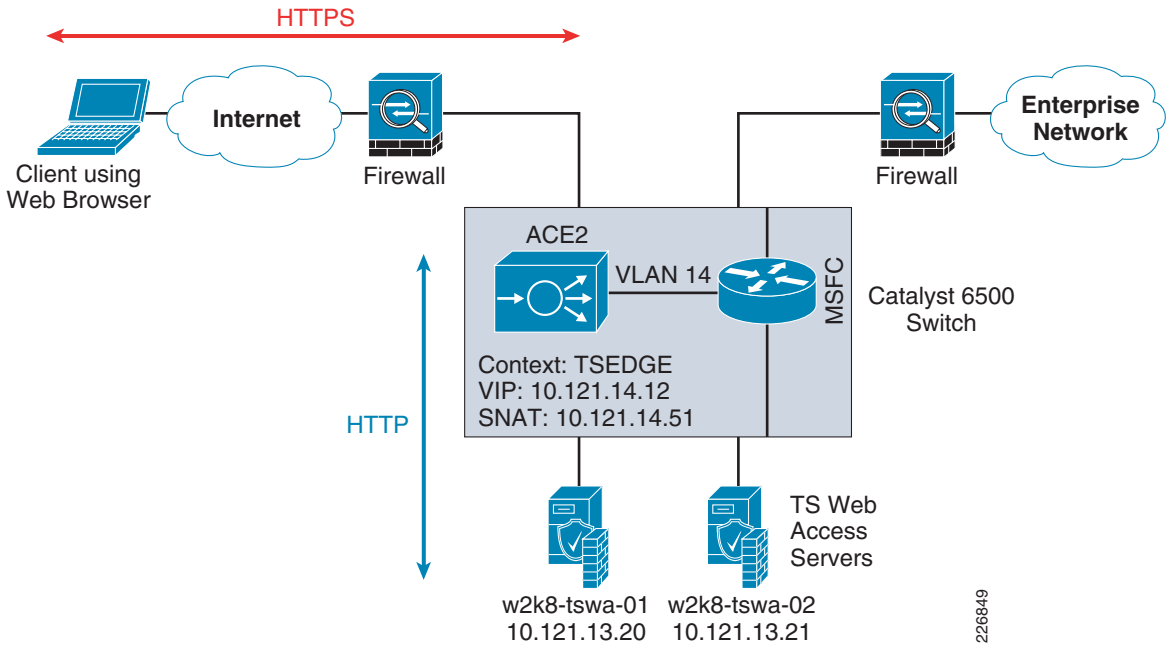
There are three deployment options for the TSWA when used with the Cisco ACE. These options are the same as was discussed in the"Deploying Cisco ACE for the TS Gateway Role" section on page 31. In summary, the three options are:

- Cisco ACE + TSWA with basic Layer -4 SLB (no SSL offload)
- Cisco ACE + TSWA with SSL end-to-end
- Cisco ACE + TSWA with SSL termination (SSL offload)

This paper focuses on the Cisco ACE providing load balancing and SSL termination for the TSWA role.

Figure 19 illustrates the various components, names, and IP addressing used in the deployment of Cisco ACE for the TS and TSWA roles.

Figure 19 Diagram for Cisco ACE and TSWA Roles

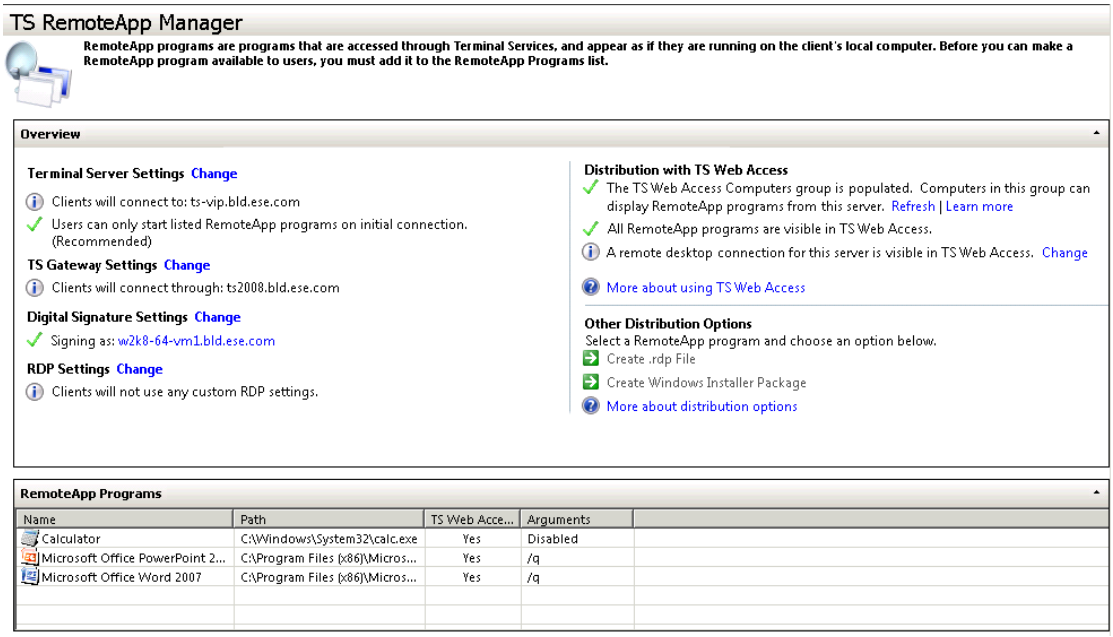


TS Web Access Configuration Summary

The TSWA is a web server running IIS 7, so the installation and configuration are very basic. The purpose of the TSWA is to provide browser-based clients access to TS RemoteApps and RDP sessions. The configuration is mostly done on the TSes themselves. Without the TS RemoteApp configuration from the TS, the only thing the TSWA could offer is a browser front-end that the client can use to RDP into the PC-based remote desktops.

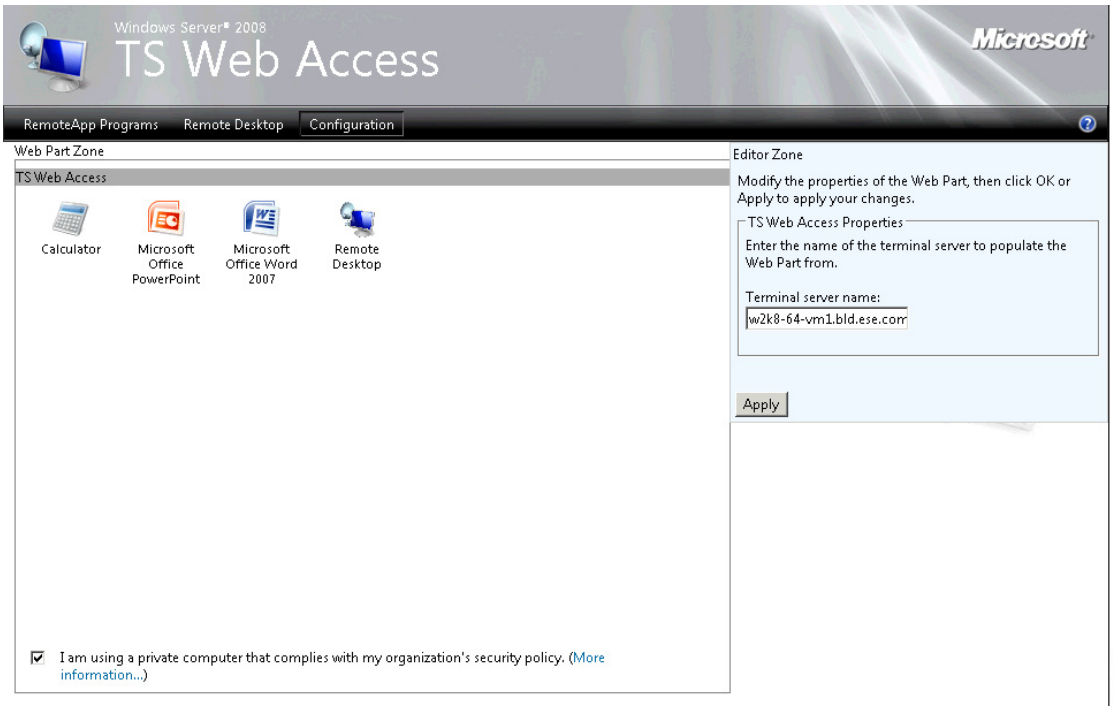
Figure 20 shows the TS RemoteApp manager screen from one of the TSes. Information such as TS settings, TSGW, digital signature, and published RemoteApp programs are all used by the two RemoteApp distribution methods: RDP/MSI files or TSWA.

Figure 20 TS RemoteApp Manager



Once the RemoteApp settings have been made on the TS, the TSWA administration page can be opened and the TSWA properties can be populated by the TS as shown in Figure 21. Once populated, the applications (Calculator, Microsoft PowerPoint 2007, Microsoft Word 2007) that were configured in the RemoteApp manager are now available on the TSWA site in addition to the Remote Desktop program.

Figure 21 TS Web Access Administration



Cisco ACE Configuration for TS Web Access—SLB and SSL Termination

Health Probe

The TSWA has the same challenge for health probes as does the TSGW. The IIS directory uses Windows Authentication (NTLM) for the web pages for TSWA. Although the TSWA web pages/directories are protected by Windows Authentication, it does, by default, serve the contents of *\inetpub\wwwroot* which can be used to configure a health probe. If the World Wide Web Publishing Service (IIS) is disabled then all functionality of the TSWA is also disabled. Alternatively, a basic TCP probe for port 80 or 443 can be used.

The following is a simple HTTP probe used for the TSWA. The probe checks the status of IIS by performing a *GET* for the default *iisstart.htm*. You can modify the path or directory as requires. The following is an example configuration.

```
probe http TSWA
  interval 2
  passdetect interval 5
  request method get url /iisstart.htm
  expect status 200 200
```

Load Balancing

Define the rservers.

```
rserver host w2k8-tswa-01
  ip address 10.121.13.20
  inservice
rserver host w2k8-tswa-02
  ip address 10.121.13.21
  inservice

serverfarm host TSWA
  probe TSWA
  rserver w2k8-tswa-01 80
    inservice
  rserver w2k8-tswa-02 80
    inservice

class-map match-all TSWA-SLB-VIP
  2 match virtual-address 10.121.14.12 tcp eq https

policy-map type loadbalance http first-match TSWA-SLB-POL
  class class-default
    serverfarm TSWA

policy-map multi-match TSWA-SLB-MULTI
  class TSWA-SLB-VIP
    loadbalance vip inservice
    loadbalance policy TSWA-SLB-POL
    loadbalance vip icmp-reply
    loadbalance vip advertise active
    nat dynamic 2 vlan 14
```

SSL Termination

Disclaimer*—The discussion of certificates, other than the server certificate on the Cisco ACE, is outside the scope of this document. A thorough understanding of certificates and server authentication is required for anyone deploying the TS2008 solution with or without the Cisco ACE.*

The connection between the client and the Cisco ACE is HTTPS, but the Cisco ACE to TSWA traffic is HTTP. Refer to the "Deploying Cisco ACE for the TS Gateway Role" section on page 31 section for an explanation of the SSL configuration.

```
crypto csr-params tswa-params
  country US
  state Colorado
  locality Boulder
  organization-name ESE
  organization-unit DC
  common-name tswa.bld.ese.com

parameter-map type ssl SSLPARAMS
 version TLS1

ssl-proxy service SSL-Proxy-TSWA
  key tswa.key
  cert tswa.cer
  ssl advanced-options SSLPARAMS

policy-map multi-match TSWA-SLB-MULTI
  class TSWA-SLB-VIP
    ssl-proxy server SSL-Proxy-TSWA

interface vlan 14
  nat-pool 2 10.121.14.51 10.121.14.51 netmask 255.255.255.0 pat
  service-policy input TSWA-SLB-MULTI
```

Validation

The client will use a web browser to establish an HTTPS connection to the TSWA by first connecting to the Cisco ACE. The client must trust the CA certificate that issued the Cisco ACE server certificate. In most deployments, Group Policy is used to add the trusted CA to the client's local certificate store. The Cisco ACE will load balance the connection using its Layer-7 SLB policy and then create a new HTTP connection to the TSWA for further processing.

Note HTTP can be used by the client if it is located internally or at a trusted remote site

Figure 22 shows the client browser with an HTTPS connection to the DNS name (**tswa.bld.ese.com**) of the Cisco ACE VIP (10.121.14.12). Remember, the DNS name used in the connection must match the **common-name** in the *csr-params* profile on the Cisco ACE.

Figure 22 Client Internet Explorer 7 Browser Connection to TSWA

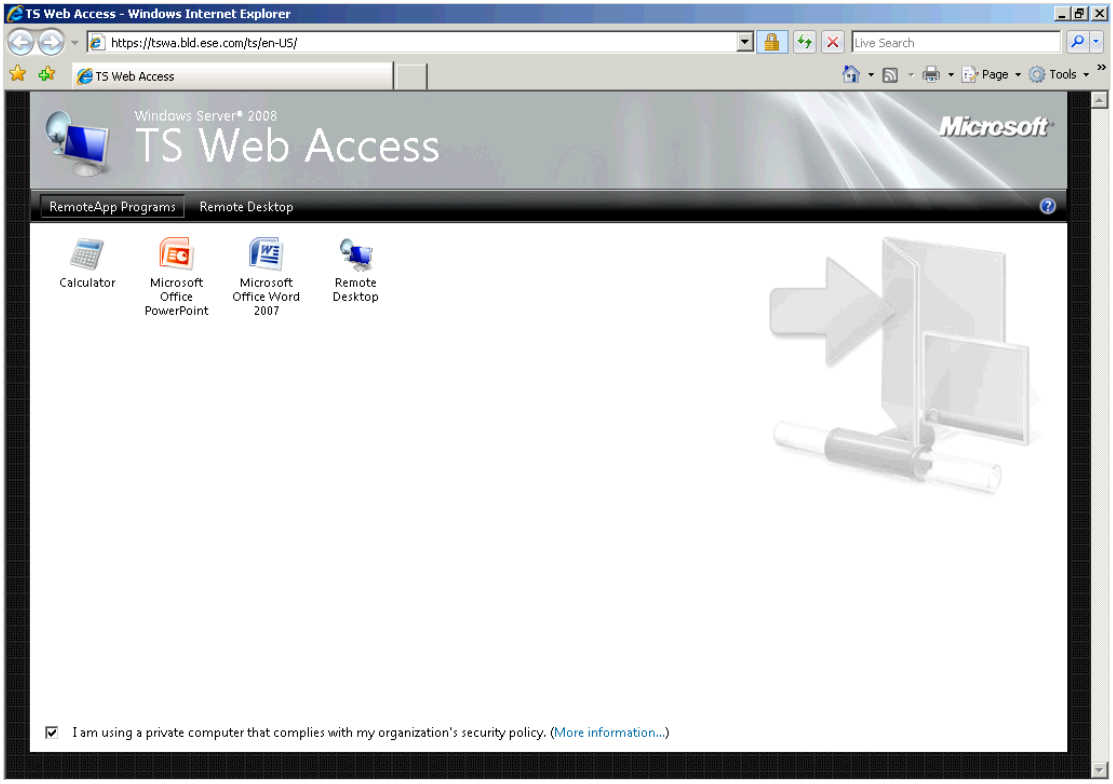
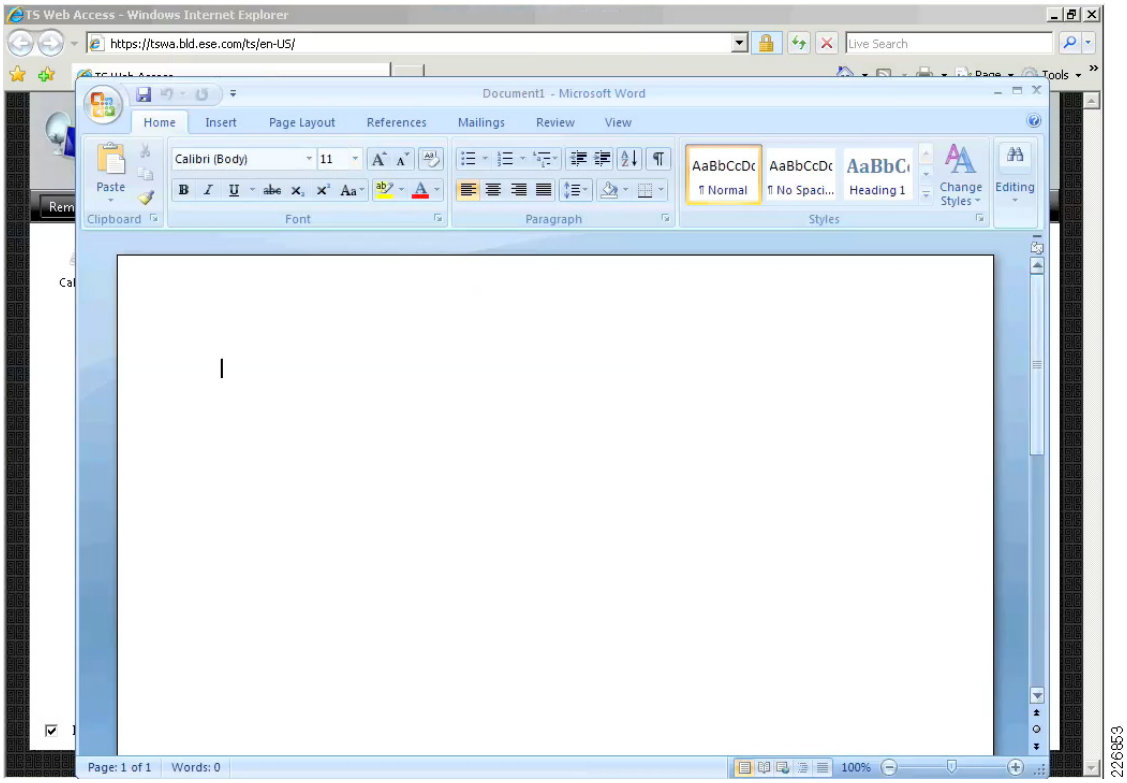


Figure 23 shows the client with a RemoteApp session for Microsoft Office 2007 Word open using the TSWA gateway:

Figure 23 RemoteApp Session for MS Word 2007 Launched from TSWA



The following output from the Cisco ACE shows the connections from the client to the Cisco ACE and the Cisco ACE to the TSWA (the number or connections is dependent on the number of objects shown on the TSWA web page:

```
ACE2/TSEDGE# show conn

total current connections : 16

conn-id    np dir proto vlan source                destination           state
----------+--+---+-----+----+--------------------+---------------------+------+
18          1  in   TCP    14    10.124.2.122:49567    10.121.14.12:443        ESTAB
3           1  out  TCP    14    10.121.13.20:80       10.121.14.51:1030       ESTAB
15          1  in   TCP    14    10.124.2.122:49568    10.121.14.12:443        ESTAB
8           1  out  TCP    14    10.121.13.20:80       10.121.14.51:1033       ESTAB
11          1  in   TCP    14    10.124.2.122:49565    10.121.14.12:443        ESTAB
23          1  out  TCP    14    10.121.13.20:80       10.121.14.51:1028       ESTAB
17          1  in   TCP    14    10.124.2.122:49563    10.121.14.12:443        ESTAB
16          1  out  TCP    14    10.121.13.20:80       10.121.14.51:1026       ESTAB
6           2  in   TCP    14    10.124.2.122:49569    10.121.14.12:443        ESTAB
1           2  out  TCP    14    10.121.13.20:80       10.121.14.51:1031       ESTAB
4           2  in   TCP    14    10.124.2.122:49566    10.121.14.12:443        ESTAB
3           2  out  TCP    14    10.121.13.20:80       10.121.14.51:1029       ESTAB
11          2  in   TCP    14    10.124.2.122:49564    10.121.14.12:443        ESTAB
5           2  out  TCP    14    10.121.13.20:80       10.121.14.51:1027       ESTAB
7           2  in   TCP    14    10.124.2.122:49562    10.121.14.12:443        ESTAB
12          2  out  TCP    14    10.121.13.20:80       10.121.14.51:1025       ESTAB
```

Resource Virtualization—All TS2008 Roles on Cisco ACE

Virtualization is a method to allocate available resources into two or more contexts for security and management purposes. Up to 250 (5 with no additional license requirements) contexts can be configured on Cisco ACE. Resources can be allocated to each context to avoid a single context consuming the entire pool of resources. This document only covers the basic virtualization configuration. Within each context, Domains and Role Base Access Controls (RBACs) can be further configured to provide additional security and access control to the resources.

Context Configuration

Sample context configuration steps are as described in the following process list.

Step 1 Configure resource-class(es). In this example the class *Gold* is being defined.

```
ACE1/Admin(config)# resource-class Gold
  <cr>  Carriage return.
```

The different resources that can be segmented are as follows:

```
ACE1/Admin(config-resource)# limit-resource ?
  acl-memory         Limit ACL memory
  all                Limit all resource parameters
  buffer             Set resource-limit for buffers
  conc-connections   Limit concurrent connections (thru-the-box traffic)
  mgmt-connections   Limit management connections (to-the-box traffic)
  proxy-connections  Limit proxy connections
  rate               Set resource-limit as a rate (number per second)
  regexp             Limit amount of regular expression memory
  sticky             Limit number of sticky entries
  xlates             Limit number of Xlate entries
```

Step 2 Configure context(s).

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

```
context TS2008
  description Context for TS2008 Services
  allocate-interface vlan 6
  member Gold
```

Cisco ACE SSL Offload Results

Disclaimer*—The following results are for reference only and are not to be taken as a baseline comparison for what can be expected in a production deployment. Session load, number of simultaneous sessions, levels of encryption, network configuration and server Hardware (CPU/Memory/IO) will cause performance numbers to vary wildly from deployment to deployment. The reader might experience radically (positive or negative) different results than the ones shown here. The reader should deploy a Proof of Concept (PoC) in his or her own network to validate the true impact of L4-7 SLB and SSL Offload. The sole purpose of these results is to provide a reference validation for the TS2008 roles when combined with Cisco ACE.*

The previous sections have shown the configurations and deployment considerations for Cisco ACE SSL offload for the TSGW and TSWA roles. The following section shows some example results that were reported during the pre-post SSL offload of the TSGW role.

The summary findings for the testing are:

- TSGW CPU—SSL terminated on TSGW; average 91 percent
- TSGW CPU—SSL terminated on Cisco ACE; average 52 percent
- Total Transactions Completed—SSL terminated on TSGW; 75,594
- Total Transactions Completed—SSL terminated on Cisco ACE; 31,015
- Average Transaction Response Time—SSL terminated on TSGW; 1.195 seconds
- Average Transaction Response Time—SSL terminated on Cisco ACE; 0.704

Figure 24 shows the statistics from Reliability and Performance Monitor on the TSGW. This test has HTTPS connections terminating directly on the TSGW. Figure 25 shows the statistics when the HTTPS connections are being terminated on the Cisco ACE module (HTTP is used between the Cisco ACE and TSGW). The CPU reports illustrate that, all things being equal (disk I/O, Network, memory), SSL offload/termination has a positive impact on the servers CPU.

Figure 24 SSL Terminated on Server

Figure 25 SSL Terminated on Cisco ACE Module

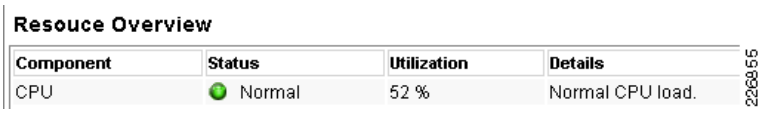


Figure 26 shows the comparison of the total number of completed transactions with SSL sessions terminating directly on the TSGW and the Cisco ACE. With the CPU-intensive SSL operations being offloaded by the Cisco ACE, the TSGW has more processing power available to complete more transactions.

Figure 26 Total Transactions Completed Comparison

Figure 27 shows the transaction response time chart for the SSL connections to the TSGW.

Figure 27 Transaction Response Time for TSGW

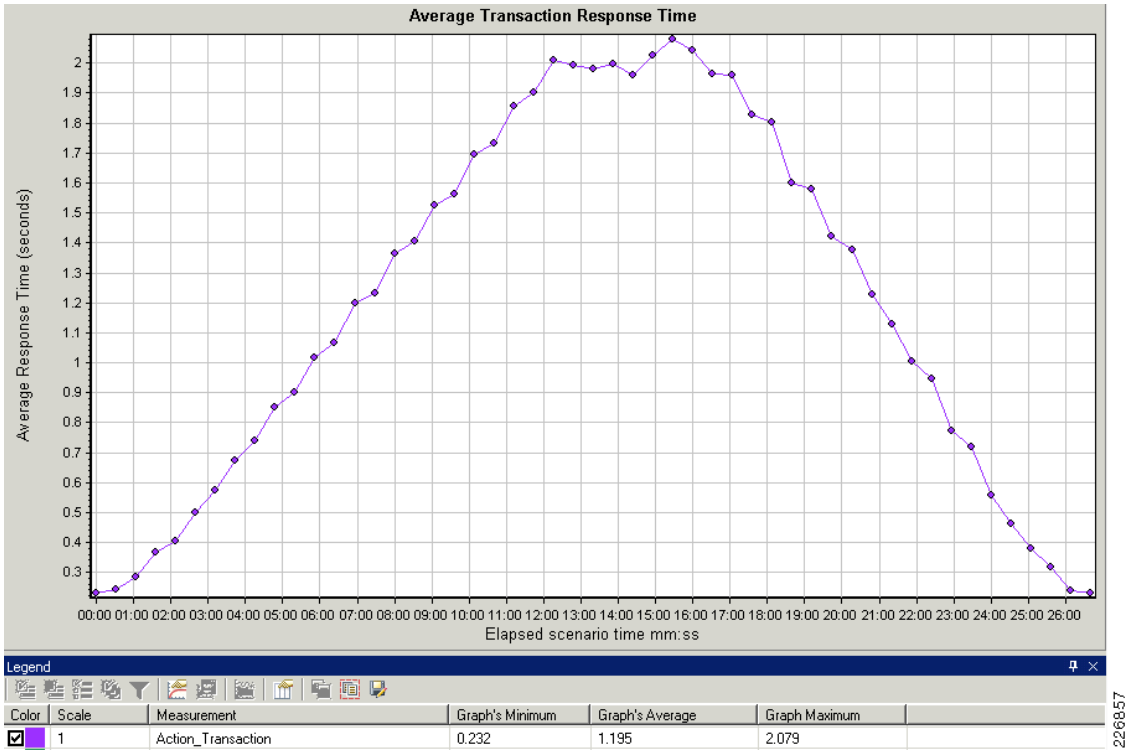
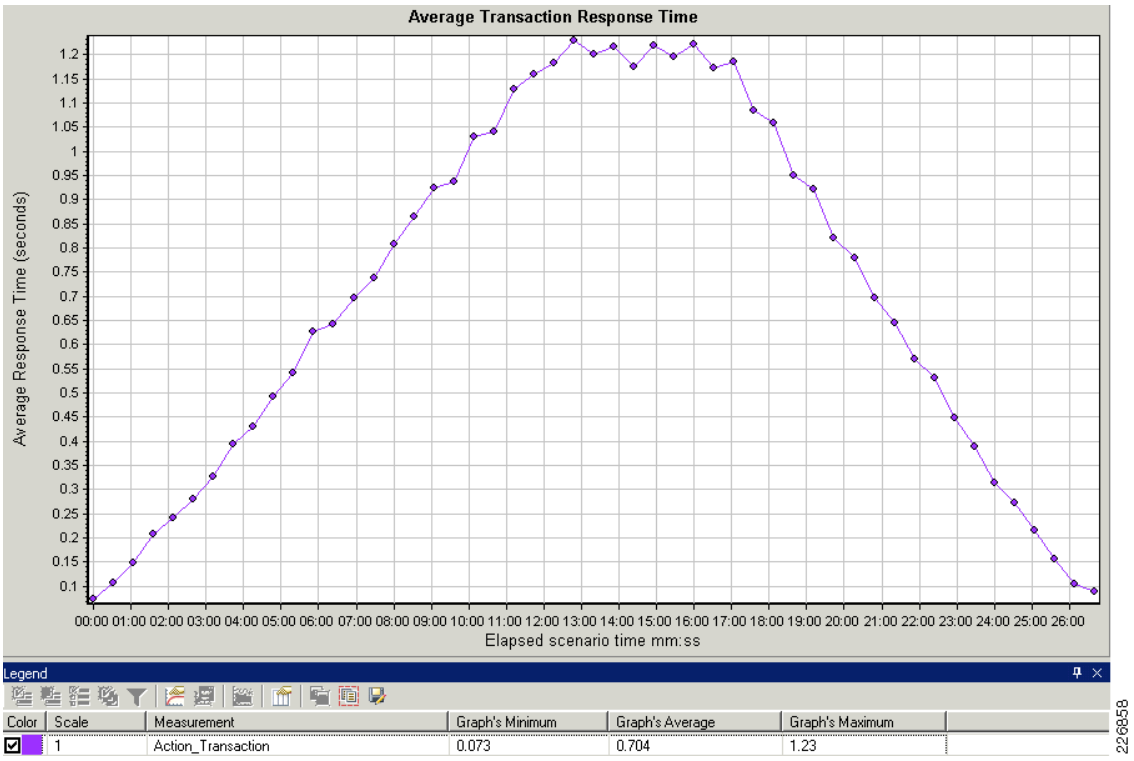


Figure 28 shows the transaction response time for the SSL connections being offloaded by the Cisco ACE. A lower transaction response time allows for a larger number of transactions that can be completed. This yields higher productivity by users because they can complete tasks more quickly within a given session.

Figure 28 Transaction Completion Time for SSL Offload on Cisco ACE



Configuring the Cisco WAAS Solution

This section describes Cisco WAAS solution considerations in the context of TS2008 integration. The following topics are presented:

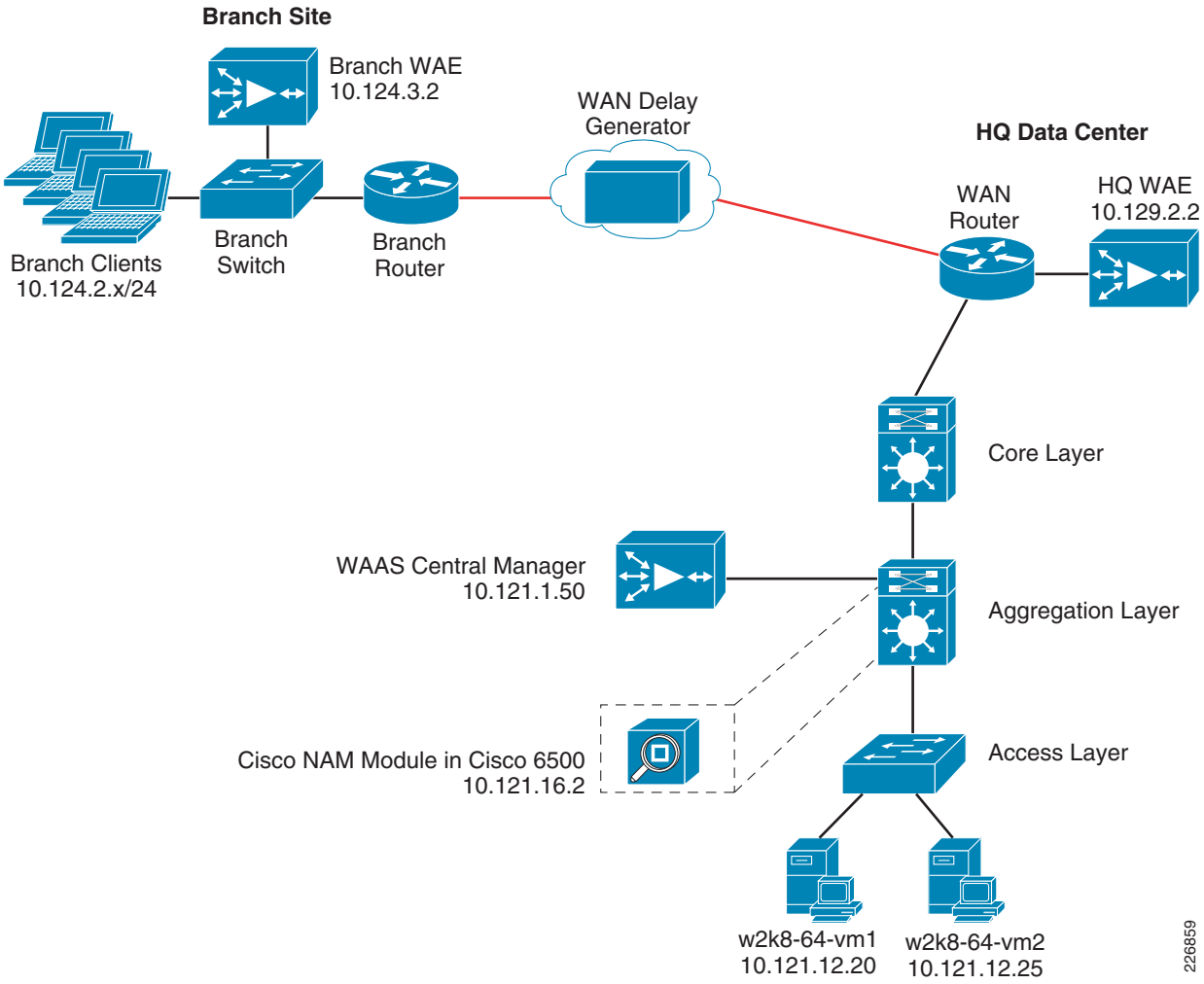
Cisco WAAS Implementation Overview

The Cisco WAAS solution requires a minimum of three Cisco WAE devices to auto-discover and deliver applicable application optimizations. One Cisco WAE is placed in the enterprise data center and the other at the branch site. The enterprise data center Cisco WAE is placed at the WAN edge connected to the WAN router. The branch topology for the Cisco WAE uses the extended branch model. The third Cisco WAE is used for the Central Manager (CM). The extended services branch offloads the Cisco WAE device from the local branch router and leverages the available ports on a local switch.

Cisco WAAS Network Topology

Figure 29 provides a summary of topology for the Cisco WAAS networking environment as described in this solution.

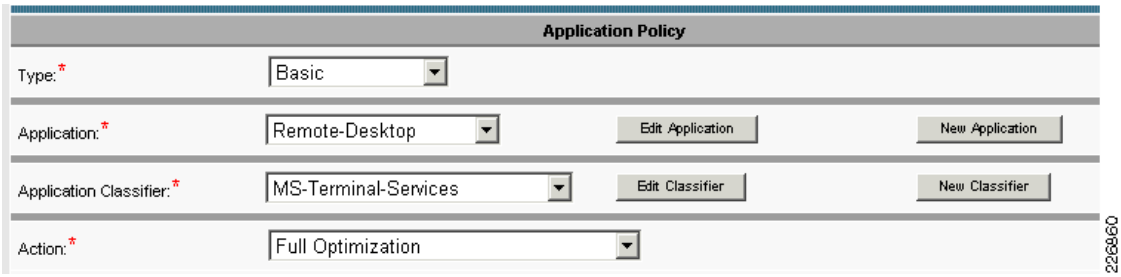
Figure 29 Cisco WAAS Network Topology



Enabling Full Optimization for TS2008

TFO, DRE, and LZ-compression are enabled by default on many application policies on the Cisco WAE; however, only TFO is enabled by default for the Remote Desktop policy. In this solution, a change must be made to alter the default optimization support for Remote Desktop to include full optimization. Figure 30 shows the Cisco WAAS CM screen and the application policy for Remote Desktop has been changed to full optimization.

Figure 30 Cisco WAAS Remote Desktop Application Policy



Cisco WAAS High Availability

Cisco WAAS deployments are transparent to the application. The application client and server do not know Cisco WAAS is optimizing traffic flows. High availability is built into the Web Cache Communications Protocol (WCCP) interception. When WCCP is not active, or if Cisco WAAS devices are not functioning, WCCP does not forward traffic to the Cisco WAEs which results in non-optimal traffic flow. This is the worse case scenario; traffic flow continues, but is not optimized.

Device High Availability

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

N+1 Availability

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

Cisco WAAS Configuration Task Lists

The following subsections describe the configurations used in this design:

Central Manager

CM is the management component of Cisco WAAS. CM provides a GUI for configuring, monitoring, and managing multiple branch and data center Cisco WAEs. CM can scale to support thousands of Cisco WAE devices for large-scale deployments. The CM is necessary for making any configuration changes via the web interface.

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

Centralized reporting can be obtained from the CM. Detailed reports—such as total traffic reduction, application mix, and pass-through traffic—can be obtained from CM GUI.

The following example configuration process summarizes the steps needed to configure CM.

Note At least one Cisco WAE must be the CM. Adding backup CMs increases availability. CMs should be installed in the data center with other critical servers—not near the branch- or WAN-facing segments.

Step 1 Configure the device to be CM. It is set to application-accelerator mode by default.

```
device mode central-manager
```

Step 2 Configure the CM IP address.

```
interface GigabitEthernet 1/0
 ip address 10.121.1.50 255.255.255.0
```

Step 3 Set up the default gateway.

```
ip default-gateway 10.121.1.1
```

Step 4 Set the primary interface. Cisco WAAS supports multiple network interface types, port channels, and standby interfaces. Cisco WAAS uses the primary interface for traffic interception and delivery. The primary interface must be defined.

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

Step 5 Define the Network Time Protocol (NTP) server. Traffic statistics are captured and forwarded to the CM. The time stamp on each packet must be accurate. All Cisco WAEs and routers should synchronize to the same NTP server.

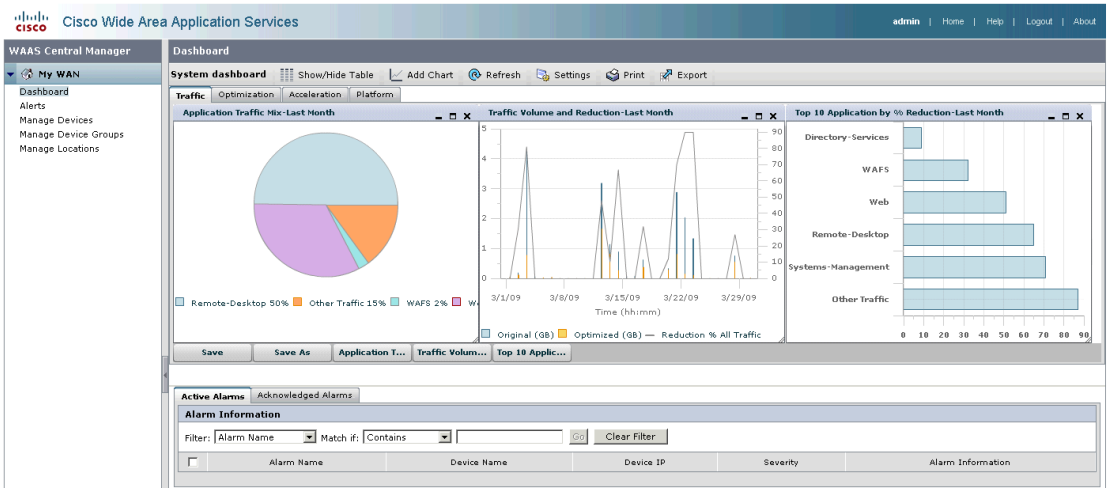
```
ntp server 10.121.99.1
```

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

```
cms enable
```

Step 7 Log in to the CM web GUI (Figure 31) on port 8443 after the CM is up and running. The initial CM window provides an overview of the health of the system. It contains information on number of devices, status, application traffic, and optimization rate.

Figure 31 Cisco WAAS Central Manager



Branch and HQ Cisco WAE

Table 3 compares the configurations in the branch and HQ Cisco WAEs. The configuration is very similar to the CM detailed in the preceding section.

Table 3 Comparison of Branch and HQ Cisco WAE Configuations

HQ Cisco WAE	Branch Cisco WAE
device mode application-accelerator ! hostname wae-core ! clock timezone US/Mountain -6 0 ! ip domain-name bld.ese.com ! primary-interface GigabitEthernet 1/0 ! interface GigabitEthernet 1/0 ip address 10.129.2.2 255.255.255.0 exit ! ip default-gateway 10.129.2.1 ! ip name-server 10.121.10.16 ! ntp server 10.121.99.1 ! wccp router-list 1 10.129.254.1 wccp tcp-promiscuous router-list-num 1 password **** wccp version 2 ! egress-method negotiated-return intercept-method wccp ! flow monitor tcpstat-v1 host 10.121.16.2 flow monitor tcpstat-v1 enable ! tfo tcp optimized-send-buffer 512 tfo tcp optimized-receive-buffer 512	device mode application-accelerator ! hostname wae-branch ! clock timezone US/Mountain -6 0 ! ip domain-name bld.ese.com ! primary-interface GigabitEthernet 1/0 ! interface GigabitEthernet 1/0 ip address 10.124.3.2 255.255.255.0 exit ! ip default-gateway 10.124.3.1 ! ip name-server 10.121.10.16 ! ntp server 10.121.99.1 ! wccp router-list 1 10.124.2.1 wccp tcp-promiscuous router-list-num 1 password **** l2-redirect mask-assign wccp version 2 ! egress-method negotiated-return intercept-method wccp ! flow monitor tcpstat-v1 host 10.121.16.2 flow monitor tcpstat-v1 enable ! tfo tcp optimized-send-buffer 512 tfo tcp optimized-receive-buffer 512

Cisco WAE Deployment with Cisco NAM

The following configuration is used for sending flow information to the Cisco NAM (10.121.16.2) located in the data center aggregation layer:

```
flow monitor tcpstat-v1 host 10.121.16.2
flow monitor tcpstat-v1 enable
```

Figure 32 shows the Cisco WAAS Device configuration in the Cisco NAM. **10.129.2.2** is the HQ Cisco WAE and **10.124.3.2** is the Branch Cisco WAE.

Figure 32 Cisco WAAS Devices Configured on Cisco NAM

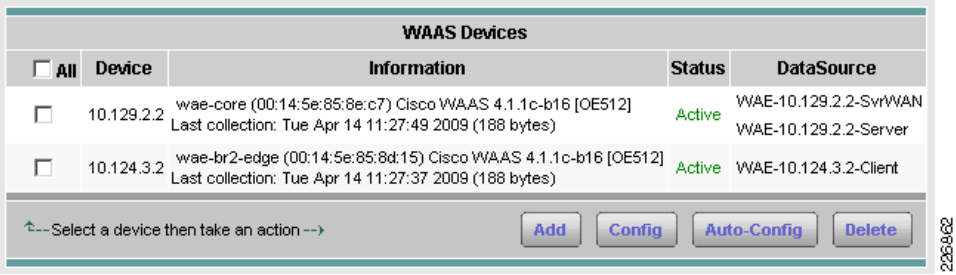
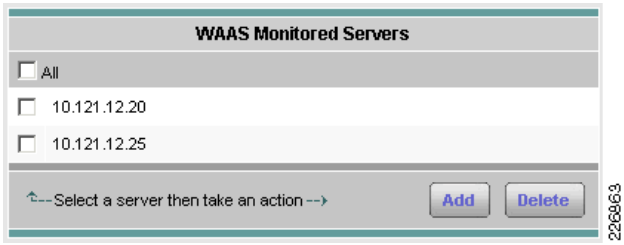


Figure 33 shows the Cisco WAAS Monitored Server configuration in the Cisco NAM. **10.121.12.20** is w2k8-64-vm1 and **10.121.12.21** is w2k8-64-vm2—both are terminal servers. The Cisco NAM will collect flow information from the Cisco WAEs so that application, network and server statistics can be analyzed for RDP flows terminating on both terminal servers.

Figure 33 Cisco WAAS Monitored Server Configuration on Cisco NAM



Branch Switch

The extended branch design used in this solution has the branch Cisco WAE attached to a Cisco Catalyst switch. This is one of several deployment options that the customer can use to connect the branch Cisco WAE to the network. The Cisco Catalyst switch in the branch provides WCCP interception points for Cisco WAAS. Without WCCP interception, Cisco WAAS does not know where to obtain and optimize traffic flow. Different methods of interception and redirection are supported by routers and switches. Redirection methods depend on the speed requirements and router/switch platforms. In this Cisco Catalyst deployment example, Layer-2 return is used.

The loopback interface on the branch switch is essential for identifying the router ID. While any IP address can be used to identify the router ID, the loopback interface is preferred over the physical interfaces. Loopback interfaces are always available as they are logical and not tied to any physical interface. Other routing protocols also use loopback interfaces as a preferred method for naming the router ID.

The following procedure summarizes the process of using the loopback interface to attach the branch Cisco WAE to a Cisco Catalyst.

Step 1 Configure the loopback interface.

```
interface Loopback0
  ip address 10.124.254.2 255.255.255.255
```

WCCP service 61 and 62 direct the switch to re-route traffic from the interface to the WCCP group. Service 61 redirects ingress traffic from the clients and service 62 redirects traffic from the WAN. Both service 61 and 62 are needed to complete redirect bi-directional traffic flow.

Step 2 Configure WCCP service 61 and 62 with a password.

```
ip wccp 61 password ESE
ip wccp 62 password ESE
```

Step 3 Configure the switch-to-Cisco WAE interface. The Cisco WAE must reside in its own subnet for WCCP interception.

```
interface FastEthernet0/13
  description WAE-Branch2
  ip address 10.124.3.1 255.255.255.0
```

Step 4 Configure the client VLAN. This is the VLAN or interface for WCCP interception. Also configure WCCP interception service 61 on the client VLAN. Ingress packets from the client VLAN are forwarded to the Cisco WAE for optimization.

```
interface Vlan2
  description VLAN for Branch2
  ip address 10.124.2.1 255.255.255.0
  ip wccp 61 redirect in
```

Step 5 Configure the interface connecting to the branch router. Also configure WCCP interception service 62 on the router interface. Return packets from WAN are forwarded back to the Cisco WAE.

```
interface FastEthernet0/1
  description To Branch Router
  ip address 10.124.1.2 255.255.255.252
  ip wccp 62 redirect in
```

Step 6 Configure NTP to synchronize to a master clock. Traffic statistics are captured and forwarded to the CM. The time stamp on each packet must be accurate. All Cisco WAEs and switches/routers should synchronize to the same NTP server.

```
ntp server 10.121.99.1
```

Data Center WAN Router

The following configuration example applies to the data center WAN router that is connected to the data center Cisco WAE.

Step 1 Configure the loopback interface.

```
interface Loopback0
  ip address 10.129.254.1 255.255.255.255
```

Step 2 Configure WCCP service 61 and 62 with a password.

```
ip wccp 61 password ESE
ip wccp 62 password ESE
```

Step 3 Configure the connection to the Cisco WAE. The Cisco WAE must reside in its own subnet for WCCP interception.

```
interface GigabitEthernet0/0.4
  description To WAE VLAN
  encapsulation dot1q 4
  ip address 10.129.2.1 255.255.255.0
```

Step 4 The interception exclusion is required because the router does not discriminate between traffic from the Cisco WAE for client or server. A forwarding loop would occur without this command.

```
ip wccp redirect exclude in
```

Step 5 Enable the NetFlow collection for outgoing traffic from the Cisco WAEs.

```
ip flow egress
```

Step 6 Configure the connection to the data center core.

```
interface GigabitEthernet0/0.5
  description To DC Core
  encapsulation dot1q 5
  ip address 10.129.1.1 255.255.255.0
  ip flow egress
```

Step 7 Configure WCCP interception service 61 and 62 on the client VLAN. All ingress/egress packets from this VLAN/interface are forwarded to the Cisco WAE for optimization.

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

Step 8 Configure the connection to the WAN.

```
interface GigabitEthernet0/1
  description To WAN Cloud
  ip address 10.128.1.1 255.255.255.0
  ip flow egress
```

Step 9 Configure NTP to synchronize to a master clock.

```
ntp server 10.121.99.1
```

Step 10 Configure NetFlow to send information to the Cisco NAM. NetFlow also uses the loopback interface as the source address. NetFlow statistics can be overwhelming for smaller connections. It is recommended that Cisco WAAS optimize NetFlow transfers.

```
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.121.16.2 3000
```

Testing the TS2008 and Cisco WAAS Solution

This section briefly describes testing for the TS2008-to-Cisco WAAS integration solution.

WAN Simulation

During this testing a WAN delay generator was deployed to simulate common WAN latency and loss. The results shown in this publication are based on a WAN configuration of a single T1 link (1.5 Mbps) and a WAN delay of 80 msec.

Test Procedure

A combination of scripts was used to launch RDC 6.1 sessions into the TS farm. Once logged in, each user session would launch one of several AutoIT scripts inside the terminal session to perform various application tasks. When testing TS2008, it is important to configure a test that utilizes a suite of applications that mimics the common applications used by mainstream terminal services clients. The following applications were used:

- *Microsoft Outlook 2007*—Compose, read, and delete E-mails. Create, read, change and, delete calendar appointments.
- *Microsoft Word 2007*—Create, edit, print and save documents.
- *Microsoft PowerPoint 2007*—Create, edit, and view slideshow; print and save presentations.
- *Microsoft Excel 2007*—Create, edit, view, print, and save spreadsheets.
- *Internet Explorer 7*—Browse several websites that have varying amount of animation. Scroll, refresh, resize, and print each page.
- *Adobe Acrobat 8*—Open, read, and print PDF files.

Multiple clients were deployed to run the RDP sessions. The Operating Systems (OS) included Window XP SP3 and Windows Vista, both using RDC 6.1. The RDP settings used in a customer environment can vary widely and are generally based on a balance between user experience (desktop/application look and feel) and performance. The RDP settings for the pre and post-Cisco WAAS testing were as follows:

- Display
  - Remote desktop size: 1024 by 768
  - Colors: 32 bit
- Local Resources
  - Remote computer sound: Bring to this computer.
  - Local devices and resources: Printers and Clipboard
- Experience:
  - Performance setting: Broadband (128 Kbps to 1.5 Mbps)

    Disabled—Desktop background

    Disabled—Font smoothing (also known as ClearType which can significantly increase bandwidth utilization)

    Enabled—Desktop composition

    Enabled—Show contents of window while dragging

    Enabled—Menu and window animation

    Enabled—Themes

    Enabled—Bitmap caching

Note Microsoft recently published an RDP performance guide that is an excellent resource for understanding the performance impact of each RDC feature and the comparison of RDP versions. The performance guide can be found at the following URL: http://download.microsoft.com/download/4/d/9/4d9ae285-3431-4335-a86e-969e7a146d1b/RDP_Performance_WhitePaper.docx

Pre-Cisco WAAS testing utilized the preceding settings on the RDC configuration which, by default, include compression and negotiated encryption. In order to gain the most out of what Cisco WAAS can offer, it is important to disable RDP compression and encryption. Compression can be disabled by either altering the RDP connection file or via Active Directory Group Policy. To disable compression in the RDP connection file, perform the following steps.

Step 1 Using a text editor, edit the RDP connection file (has an *.rdp* extension).

Step 2 Change the line compression:i:1 to be compression:i:0

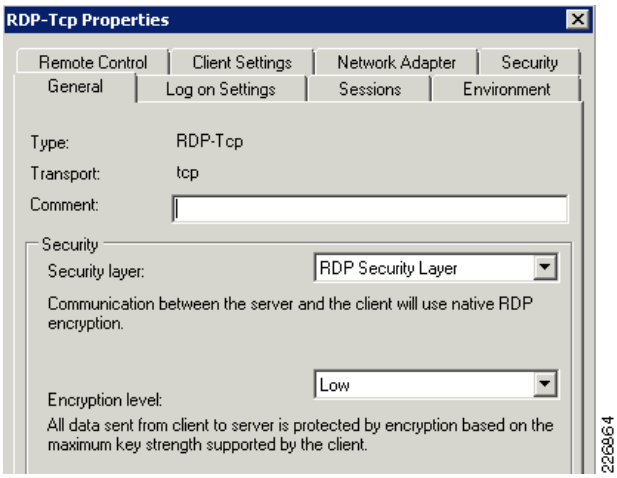
Step 3 Save the file and exit the text editor.

Encryption can be disabled from the Terminal Services Configuration application as shown in Figure 34. The settings should be as follows:

- Security Layer = RDP Security Layer
- Encryption Level=Low

A message will appear stating that the registry has changed. Restart the *Terminal Services* service for the changes to take effect.

Figure 34 Terminal Services Encryption Settings



Alternatively, the required changes to encryption can be made by editing the following registry keys on the TS:

- Set HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\MinEncryptionLevel to 1.
- Set HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer as a DWORD value and set it to 0.

Results and Conclusions

Disclaimer*—The following results are for reference only and are not to be taken as a baseline comparison for what can be expected in a production deployment. RDP sessions and the bandwidth, response times and transaction times vary significantly from session to session based on a number of factors that include bandwidth, network and application delay, length of session, applications and activity in the session, features enabled in the RDP session (Font smoothing, audio redirection, and so on), and the levels of compression and encryption used. The reader might experience substantively (positive or negative) different results those shown here. The reader should deploy a PoC in his or her own network to validate the true impact that any WAN optimization solution might provide. The sole purpose of these results is to provide a reference validation for the TS2008 roles when combined with the Cisco WAAS product in the test environment shown.*

Figure 35 shows a pre- and post-view of an RDP test that lasted approximately 20 minutes. Using the testing criteria defined above, an RDP test was initiated at 9:00 and was run until 9:20. The RDP session had both compression and encryption enabled as would a default RDP configuration. The traffic shown is reported by the data center WAN router (Orange) using NetFlow. Cisco WAAS was enabled, RDP compression and encryption were disabled, and a new test was initiated at 9:30 and was run until 9:50. The Cisco NAM reported both the data center WAN router NetFlow information (Orange) as well as the branch Cisco WAE traffic for the RDP Client (Aqua blue). What this shows is that a significant drop off in branch WAN traffic occurred due to the Cisco WAAS solution providing TFO, DRE caching and LZ compression on the RDP flow. There is a large increase in traffic to the client as indicated by the *RDP-WAE-Branch* bar due to the branch client hitting the local branch Cisco WAE's cache instead of retrieving data all the way across the WAN from the data center terminal server. This local cache hit for the client, along with the TFO and LZ compression, yielded a significantly better user experience due to faster application response time.

Figure 35 Pre- and Post-Cisco WAAS as Reported by the Cisco NAM

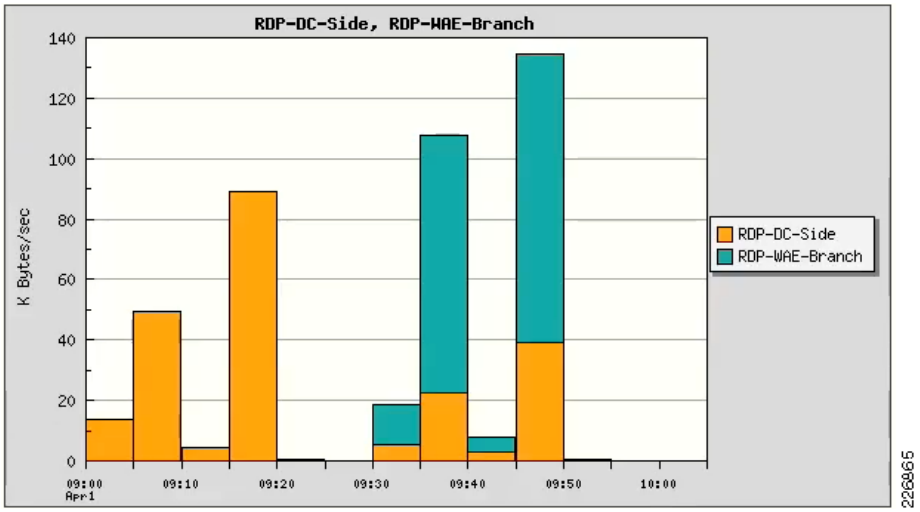


Figure 36 illustrates the connection status from the Cisco WAAS CM. The client (**10.124.2.122**) is connected to a terminal server (**10.121.12.20**) and has a full optimization (TFO, DRE, and LZ compression) policy applied and currently the Cisco WAEs are compressing 71 percent of the data in the RDP flow.

Figure 36 Cisco WAAS Connection Statistics for RDP Session

	Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open Duration	Org Bytes	Opt Bytes	% Comp	Classifier Name
	10.124.2.122:49453	10.121.12.20:3389	wae-br2-edge		0:9:54	28.0003 MB	8.172 MB	71%	MS-Terminal-Services

226866

As more RDP sessions come online from the branch, more objects can be cached and compressed even if every user is running different applications inside their respective RDP sessions. This happens due to the fact that there are many objects that exist inside of RDP sessions that are redundant such as desktop backgrounds, Microsoft PowerPoint toolbars, themes, color schemes, and so on. The more similar the applications are that are used from the branch and the more concurrent sessions that are active the better Cisco WAAS can optimize the connections. Figure 37 illustrates active connections for multiple RDP sessions. The open duration (time the connection has been active) is shown with the newest at the bottom. The longer these sessions are open the higher their compression percentages will go. High compression percentages indicate that there are many similarities in the RDP session that can be handled by DRE and LZ compression. The more similar the data, the higher the compression percentage. Other testing

conducted during this project revealed that the more similar the TS administrator can make each desktop session (themes, colors, desktop icon layout, and so on) the better the optimization results. Even when the majority of objects and applications are intentionally configured to be different, optimization was still ranging from 15 to 52 percent.

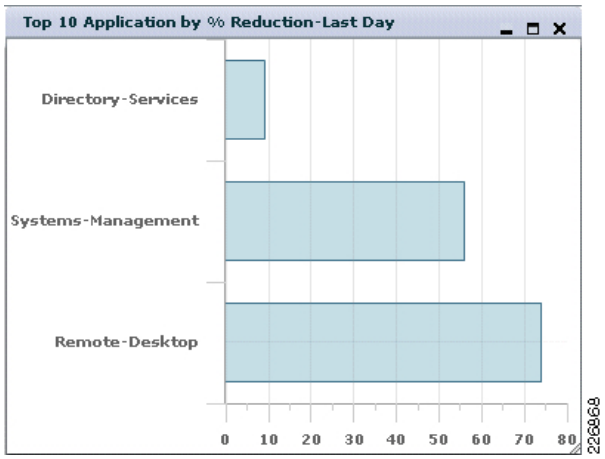
Figure 37 Cisco WAAS Connection Statistics for Multiple RDP Sessions

	Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open Duration	Org Bytes	Opt Bytes	% Comp	Classifier Name
	10.124.2.123:49174	10.121.12.20:3389	wae-br2-edge		0:4:30	16.8647 MB	4.6575 MB	72%	MS-Terminal-Services
	10.124.3.2:14695	10.121.16.2:7878	wae-br2-edge		0:3:51	973.0391 KB	220.1191 KB	77%	WAAS-FlowMonitor
	10.124.2.123:49176	10.121.12.20:3389	wae-br2-edge		0:2:58	6.8938 MB	1.9382 MB	72%	MS-Terminal-Services
	10.124.2.122:50308	10.121.12.20:3389	wae-br2-edge		0:1:1	921.0684 KB	832.9932 KB	10%	MS-Terminal-Services
	10.124.2.122:50310	10.121.12.20:3389	wae-br2-edge		0:0:27	171.9287 KB	146.7832 KB	15%	MS-Terminal-Services

226867

Figure 38 illustrates the percentage of reduction by the Cisco WAAS after a day of RDP sessions from 10 users.

Figure 38 Cisco WAAS Sample Results for Percentage Reduced for Past Day



TS2008 + Cisco WAAS Mobile

In addition to the Cisco WAAS solution using Cisco WAE appliances, the Cisco WAAS Mobile solution was used to validate remote workers using TS2008. Figure 39 shows the high-level topology used during the testing of the Cisco WAAS Mobile solution with TS2008.

Figure 39 Cisco WAAS Mobile with Windows Server 2008 Terminal Services

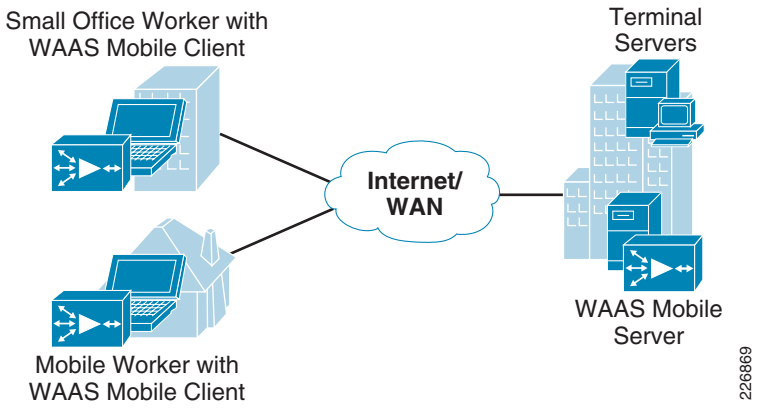


Figure 40 illustrates the amount of data transferred to the remote client running an RDP session. This graph shows the amount of data transferred from the terminal server located in the data center to the remote client located on the Internet. The *Native RDP* bar shows the amount of data transferred without the Cisco WAAS Mobile Client being used. The *Cisco WAAS Mobile 1st Session* shows the RDP session being optimized by the Cisco WAAS Mobile solution. There is a significant drop off in data transferred over the network due to the optimization of the RDP data by the Cisco WAAS Mobile Client. The session was disconnected and then re-established to the same RDP session. *Cisco WAAS Mobile Reconnect to Session* illustrates that the client can leverage data that is still in the local Delta Cache located on the client.

Figure 40 Cisco WAAS Mobile Comparison Chart - Data Transferred

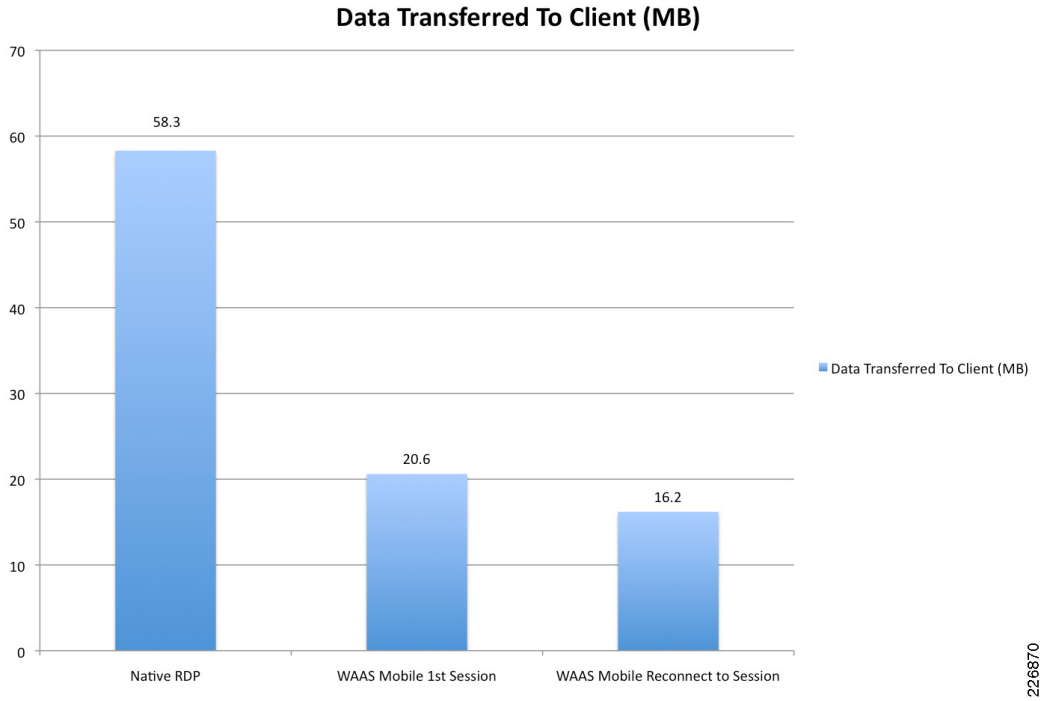


Figure 41 illustrates the network transfer rate (in Kbps) between the terminal server and the remote client during the RDP session. For the same reasons mentioned above, there is a significant drop off in the transfer rate between the *Native RDP* test and the subsequent *Cisco WAAS Mobile* tests. This yields a

better user experience for the client as a large percentage of the RDP data is optimized and available local to the client instead of transiting across a potentially high latency connection to the data center. This bandwidth savings allows the client to utilize the Internet connection for other purposes while reducing the load on the enterprise VPN system through which the client might be using to connect.

Figure 41 Cisco WAAS Mobile Comparison Chart - Transfer Rate

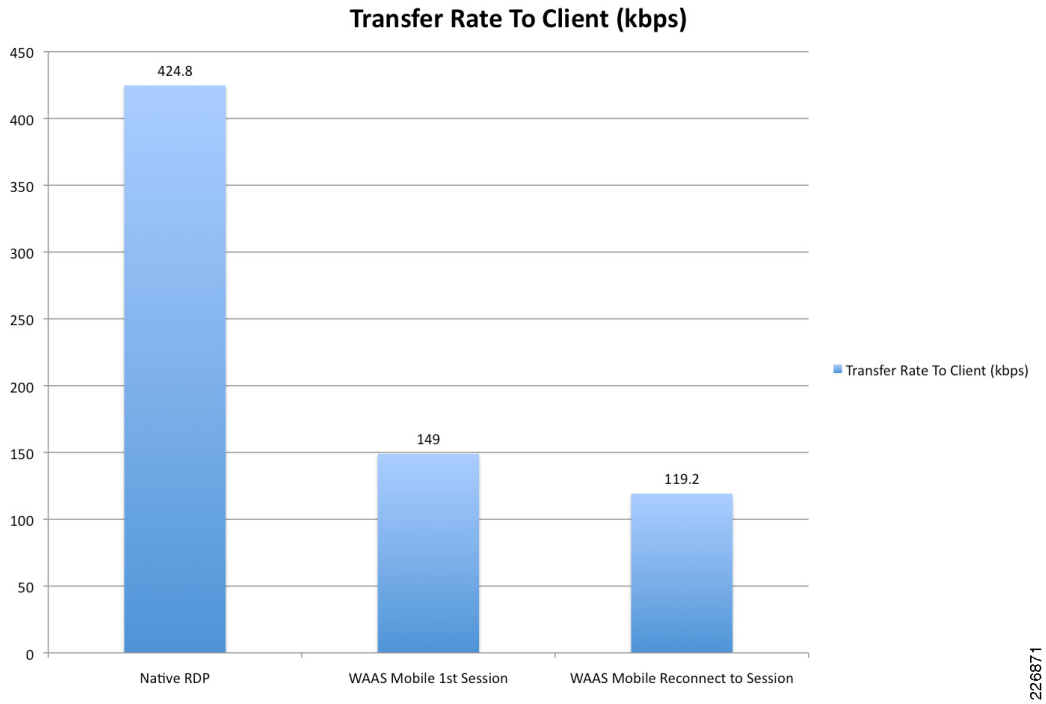
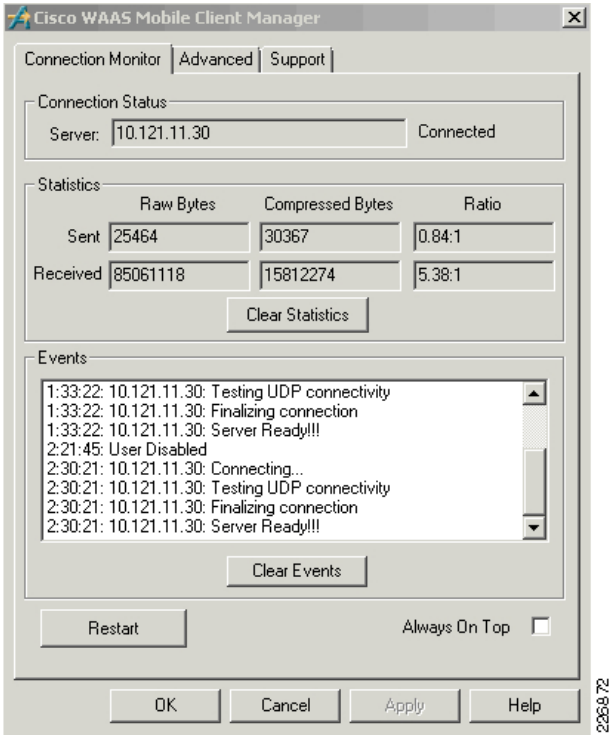


Figure 42 illustrates the Cisco WAAS Mobile Client. The *Ratio* shows 5.38:1 for the received data during the *Cisco WAAS Mobile Reconnect to Session* test run.

Figure 42 Cisco WAAS Mobile Client Statistics



Conclusion

Microsoft Windows Server 2008 Terminal Services, along with the Cisco solution discussed in this publication, provides a scalable, available and feature-rich user-experience for presentation virtualization. Cisco provides server load balancing and SSL offload via the Cisco ACE for TS2008 roles such as the TS/TSSB, TSGW, and TSWA. WAN optimization for RDP flows is provided by Cisco WAAS and Cisco WAAS Mobile. Combining the Cisco ACE, Cisco WAAS, and Cisco WAAS Mobile products with the Cisco NAM allows for the monitoring, reporting, and troubleshooting of a TS2008 environment. The capabilities presented in this document demonstrate that the Cisco solution for TS2008 offers improved transaction times, lower bandwidth utilization, optimal server utilization, and increased availability—all of which combine to yield a more streamlined user-experience and increased productivity.

Related Documents

Cisco Connection Online—Data Center
http://www.cisco.com/go/dc

Cisco Solution Reference Network Designs (SRND)
http://www.cisco.com/go/designzone

Microsoft Windows Server 2008 Terminal Services
http://www.microsoft.com/windowsserver2008/en/us/ts-product-home.aspx
http://technet.microsoft.com/en-us/windowsserver/terminal-services/default.aspx
http://technet.microsoft.com/en-us/library/cc733093.aspx

Microsoft RDP Performance Guide
http://download.microsoft.com/download/4/d/9/4d9ae285-3431-4335-a86e-969e7a146d1b/RDP_Performance_WhitePaper.docx

Microsoft Active Directory Planning and Deployment|
http://technet.microsoft.com/en-us/library/cc268216.aspx

Cisco Nexus 7000 with Services Design Guide
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/nx_7000_dc.html

Cisco ACE Module Documentation
http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

Cisco WAAS Documentation
http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml

Cisco WAAS Data Center Design Guide
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c649/ccmigration_09186a008081c7da.pdf

Cisco WAAS Branch Design Guide
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c649/ccmigration_09186a008081c7d5.pdf

Cisco WAAS Mobile Documentation
http://www.cisco.com/en/US/products/ps9523/products_installation_and_configuration_guides_list.html

Cisco NAM Website
http://www.cisco.com/go/nam