Enterprise Branch Wide Area Application Services Design Guide (Version 1.1)

This document discusses design and deployment considerations in deploying wide area application services (WAAS) over branch architectures. It serves as a supplement to the Cisco enterprise branch architecture documents, which can be found at http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html.

Contents

Introduction

As enterprise businesses extend their size and reach to remote locations, guaranteeing application delivery to end users becomes increasingly important. In the past, remote locations contained their own application file servers and could provide LAN access to data and applications within the remote location or branch. Although this solution guarantees application performance and availability, it also means more devices to manage, increased total cost of ownership, regulatory compliance for data archival, and lack of anywhere, anytime application access. Placing application networking servers within a centralized data center where remote branches access applications across a WAN solves the management of devices and total cost of ownership issues. The benefits for consolidating application networking services in the data center include but are not limited to the following:

- Cost savings through branch services consolidation of application and printer services to a centralized data center

- Ease of manageability because less devices are employed in a consolidated data center

- Centralized storage and archival of data to meet regulatory compliance

- More efficient use of WAN link utilization through transport optimization, compression, and file caching mechanisms to improve overall user experience of application response

The trade-off with the consolidation of resources in the data center is the increase in delay for remote users to achieve the same performance of accessing applications at LAN-like speeds as when these servers resided at the local branches. Applications commonly built for LAN speeds are now traversing a WAN with less bandwidth and increased latency over the network. Potential bottlenecks that affect this type of performance include the following:

- Users at one branch now contend for the same centralized resources as other remote branches.

- Insufficient bandwidth or speed to service the additional centralized applications now contend for the same WAN resources.

- Network outage from remote branch to centralized data center resources cause "disconnected" events, severely impacting remote business operations.

The Cisco WAAS portfolio of technologies and products give enterprise branches LAN-like access to centrally-hosted applications, servers, storage, and multimedia with LAN-like performance. WAAS provides application delivery, acceleration, WAN optimization, and local service solutions for an enterprise branch to optimize performance of any TCP-based application in a WAN or MAN environment.

This document provides guidelines and best practices when implementing WAAS in enterprise architectures. This document gives an overview of WAAS technology and then explores how WAAS operates in branch architectures. Design considerations and complete tested topologies and configurations are provided.

Intended Audience

This design guide is targeted for network design engineers to aid their architecture, design, and deployment of WAAS in enterprise data center architectures.

Updates to Version 1.1

Version 1.1 of this document provides the following updates:

- Interoperability between WAAS and the Cisco IOS firewall
- Cisco IOS IPS signatures supporting the latest Cisco IOS Software version 12.4(11)T2
- Test bed configurations for the branch security/WAAS validation using IOS version 12.4(11)T2 at the branch and WAAS software version 4.0.9

Caveats and Limitations

The technical considerations in this document refer to WAAS version 4.0(9). The following features have not been tested in this initial phase and will be considered in future phases:

- Policy-based routing (PBR)
- Wireless LAN
- Voice services—SIP, CME, IP phone services
- NAC

Although these features are not tested, their expected behavior may be discussed in this document.

Assumptions

This design guide has the following starting assumptions:

- System engineers and network engineers possess networking skills in data center architectures.
- Customers have already deployed Cisco-powered equipment in data center architectures. Interoperability of the WAE and non-Cisco equipment is not evaluated.
- Although the designs provide flexibility to accommodate various network scenarios, Cisco recommends following best design practices for the enterprise data center. This design guide is an overlay of WAAS into the existing network design. For detailed design recommendations, see the data center design guides at the following URL: http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html.

Best Practices and Known Limitations

The following is a summary of best practices that are described in either the *Enterprise Branch WAAS Design Guide* or the *Enterprise Data Center Design Guide*:

- Install the WAE at the WAN edge to increase optimization coverage to all hosts in the network.
- Use Redirect ACL to limit campus traffic going through the WAEs for installation in the aggregation layer; optimization applies to selected subnets.
- Use Web Cache Communications Protocol version 2 (WCCPv2) instead of PBR; WCCPv2 provides more high availability and scalability features, and is also easier to configure.
- PBR is recommended where WCCP or inline interception cannot be used.
- Inbound redirection is preferred over outbound redirection because inbound redirection is less CPU-intensive on the router.

- Two Central Managers are recommended for redundancy.

- Use a standby interface to protect against network link and switch failure. Standby interface failover takes around five seconds.

- For Catalyst 6000/76xx deployments, use only inbound redirection to avoid using "redirection exclude in", which is not understood by the switch hardware and must be processed in software.

- For Catalyst 6000/76xx deployments, use L2 redirection for near line-rate redirection.

- Use Multigroup Hot Standby Routing Protocol (mHSRP) to load balance outbound traffic.

- Install additional WAEs for capacity, availability, and increased system throughput; WAE can scale in near linear fashion in an N+1 design.

WAAS Known Limitations

- A separate WAAS subnet and tertiary/sub-interface are required for transparent operation because of preservation of the L3 headers. Traffic coming out of the WAE must not redirect back to the WAE. Inline interception does not need a separate WAAS subnet.

- IPv6 is not supported by WAAS 4.0; all IP addressing must be based on IPv4.

- WAE overloading such as the exhaustion of TCP connections results in pass-through traffic (non-optimized); WCCP does not know when a WAE is overloaded. WCCP continues to send traffic to the WAE based on the hashing/masking algorithm even if the WAE is at capacity. Install additional WAEs to increase capacity.

WAAS Technology Overview

To appreciate how WAAS provides WAN and application optimization benefits to the enterprise, first consider the basic types of centralized application messages that would be transmitted to and from remote branches. For simplicity, two basic types are identified:

- Bulk transfer applications—Focused more on the transfer of files and objects. Examples include FTP, HTTP, and IMAP. In these applications, the number of roundtrip messages may be few and may have large payloads with each packet. Some examples include WEB portal or lite client versions of Oracle, SAP, Microsoft (SharePoint, OWA) applications, e-mail applications (Microsoft Exchange, Lotus Notes), and other popular business applications.

- Transactional applications—High number of messages transmitted between endpoints. Chatty applications with many roundtrips of application protocol messages that may or may not have small payloads. Examples include Microsoft Office applications (Word, Excel, Powerpoint, and Project).

WAAS uses the following technologies to provide a number of application acceleration as well as remote file caching, print service, and DHCP features to benefit both types of applications:

- Advanced compression using DRE and Lempel-Ziv (LZ) compression

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

- Transport file optimizations (TFO)

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

- Common Internet File System (CIFS) caching services

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

- Print services

    WAAS can cache print drivers at the branch, so an extra file or print server is not required. By using WAAS for caching these services, client requests for downloading network printer drivers do not have to traverse the WAN.

For more information on these enhanced services, see the *WAAS 4.0 Technical Overview* at the following URL: http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml.

Figure 1 shows the logical mechanisms that are used to achieve WAN and application optimization, particularly using WAAS.

Figure 1   *Wide Area Application Services (WAAS) Mechanisms*
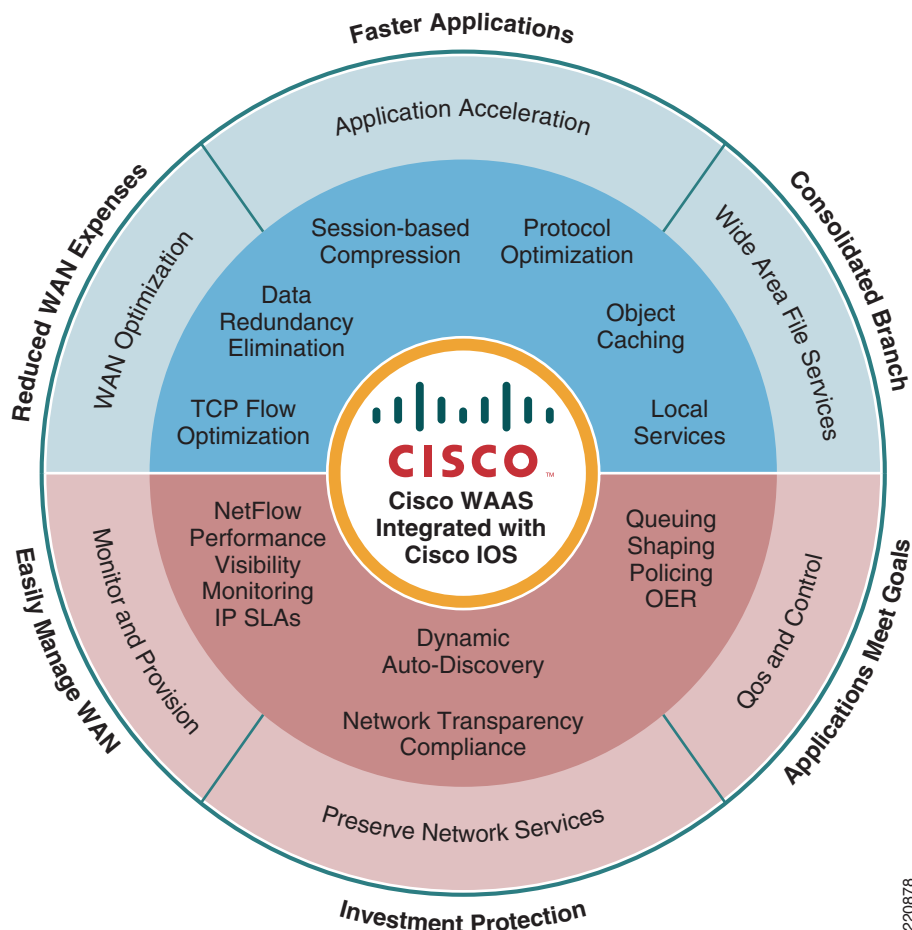
The WAAS features are not described in detail in this guide; the WAAS data sheets and software configuration guide explain them in more detail. This literature provides excellent feature and configuration information on a product level. Nevertheless, for contextual purposes, some of the WAAS basic components and features are reviewed in this document.

WAAS consists mainly of the following main hardware components:

- Application Accelerator Wide Area Engines (WAE) —The application accelerator resides within the campus/data center or the branch. If placed within the data center, the WAE is the TCP optimization and caching proxy for the origin servers. If placed at the branch, the WAE is the main TCP optimization and caching proxy for branch clients.

- WAAS Central Manager (CM)—Provides a unified management control over all the WAEs. The WAAS CM usually resides within the data center, although it can be physically placed anywhere provided that there is a communications path to all the managed WAEs.

For more details on each of these components, see the *WAAS 4.0.7 Software Configuration Guide* at the following URL:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v407/configuration/guide/cfgd.html.

The quantity and WAE hardware model selection varies with a number of factors (see Table 1). For the branch, variables include the number of estimated simultaneous TCP/CIFS connections, the estimated disk size for files to be cached, and the estimated WAN bandwidth. Cisco provides a WAAS sizing tool for guidance, which is available internally for Cisco sales representatives and partners. The NME-WAE is the WAE network module and deployed inside the branch integrated services router (ISR).

Table 1   WAE Hardware Sizing

Device	Max Optimized TCP Connections	Max CIFS Sessions	Single Drive Capacity [GB]	Max Drives	RAM [GB]	Max Recommended WAN Link [Mbps]	Max Optimized Throughput [Mbps]
NME-WAE-302	250	N/A	80	1	0.5	4	90
NME-WAE-502	500	500	120	1	1	4	150
WAE-512-1	750	750	250	2	1	8	100
WAE-512-2	1500	1500	250	2	2	20	150
WAE-612-2	2000	2000	300	2	2	45	250
WAE-612-4	6000	2500	300	2	4	90	350
WAE-7326	7500	2500	300	6	4	155	450

WAAS Optimization Path

Optimizations are performed between the core and edge WAE. The WAEs act as a TCP proxy for both clients and their origin servers within the data center. This is not to be confused with other WAN optimization solutions that create optimization tunnels. In those solutions, the TCP header is modified between the caching appliances. With WAAS, the TCP headers are fully preserved. Figure 2 shows three TCP connections.

Figure 2   WAAS Optimization Path
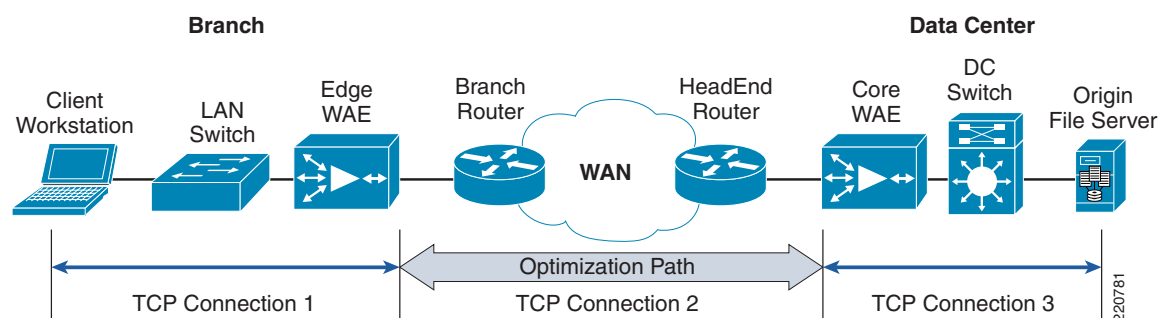
TCP connection #2 is the WAAS optimization path between two points over a WAN connection. Within this path, Cisco WAAS optimizes the transfer of data between these two points over the WAN connection, minimizing the data it sends or requests. Traffic in this path includes any of the WAAS optimization mechanisms such as the TFO, DRE, and LZ compression.

Identifying where the optimization paths are created among TFO peers is important because there are limitations on what IOS operations can be performed. Although WAAS preserves basic TCP header information, it modifies the TCP sequence number as part of its TCP proxy session. As a result, some

features dependent on inspecting the TCP sequence numbering, such as IOS firewall packet inspection or features that perform deep packet inspection on payload data, may not be interoperable within the application optimization path.

The core WAE and thus the optimization path can extend to various points within the campus/data center. Various topologies for core WAE placement are possible, each with its advantages and disadvantages.

WAAS is part of a greater application and WAN optimization solution. It is complementary to all the other IOS features within the ISR and branch switches. Both WAAS and the IOS feature sets synergistically provide a more scalable, highly available, and secure application for remote branch office users.

As noted in the last section, because certain IOS interoperability features are limited based on where they are applied, it is important to be aware of the following two concepts:

- Direction of network interfaces
- IOS order of operations

For identification of network interfaces, a naming convention is used throughout this document (see Figure 3 and Table 2).

Figure 3 **Network Interfaces Naming Convention for Edge WAEs**
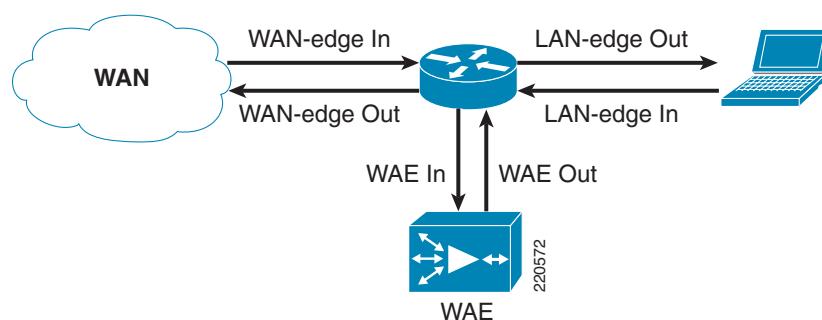
Table 2 **Naming Conventions[1]**

Interface	Description
LAN-edge in	Packets initiated by the data client sent into the switch or router
LAN-edge out	Packets processed by the router and sent outbound toward the clients
WAN-edge out	Packets processed by the router and sent directly to the WAN
WAN-edge in	Packets received directly from the WAN entering the router
WAE-in	• From LAN-edge in—Packets redirected by WCCP or PBR from the client subnet to the WAE; unoptimized data • From WAN-edge in—Packets received from the core WAE; application optimizations are in effect
WAE- out	Packets already processed/optimized by the WAE and sent back towards the router: • To WAN-edge out—WAE optimizations in effect here • To LAN-edge out—no WAE optimizations

1. Source: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080133ddd.shtml

The order of IOS operations varies based on the IOS versions; however, Table 3 generally applies for the versions supported by WAAS. The bullet points in **bold** indicate that they are located inside the WAAS optimization path.

Table 3   Life of a Packet—IOS Basic Order of Operations[1]

Inside-to-Outside (LAN to WAN)	Outside-to-Inside (WAN to LAN)
• If IPsec, then check input access list	• MPLS tunneling (if MPLS WAN deployed)
• Decryption (if applicable) for IPsec	• Decryption (if applicable) for IPsec
• Check input access list	• Check input access list
• Check input rate limits	• Check input rate limits
• Input accounting	• Input accounting
• Policy routing	• NAT outside to inside (global to local translation)
• Routing	• Policy routing
• Redirect via WCCP or L2 redirect	• Routing
• **WAAS application optimization** *(start/end of WAAS optimization path)*	• Redirect via WCCP or L2 redirect
• NAT inside to outside (local to global translation)	• **WAAS application optimization** *(start/end of WAAS optimization path)*
• Crypto (check map and mark for encryption)	• Crypto (check map and mark for encryption)
• Check output access list	• Check output access list
• Stateful Packet Inspection (SPI)	• Stateful Packet Inspection (SPI)
• TCP intercept	• TCP intercept
• Encryption	• Encryption
• Queueing	• Queueing
• MPLS VRF tunneling (if MPLS WAN deployed)	

1. Source: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080133ddd.shtml

The order of operations here may be important because these application and WAN optimizations, as well as certain IOS behaviors, may not behave as expected, depending on where they are applied.

WAAS Branch Design Considerations

WAAS Placement over Branch Topologies

The branch architecture identifies three profiled topologies, generally based on the size and resiliency of infrastructure services, that a branch may require. These profiles serve more as a general suggestion for customers deploying branches and are not intended to be statically defined. Most branches deployed today have aspects from each of the profiles. The scope of this document is simply to explain how WAAS fits within each of the branch profile topologies and interoperates with the identified branch services. Further technical details about each branch profile can be found in the *Enterprise Branch Architecture Design Overview* document at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/EnBrOver.html.

Figure 4 shows the placement of the WAE in each of the branch topologies.

Figure 4   *WAAS Placement in the Current Branch Topologies*
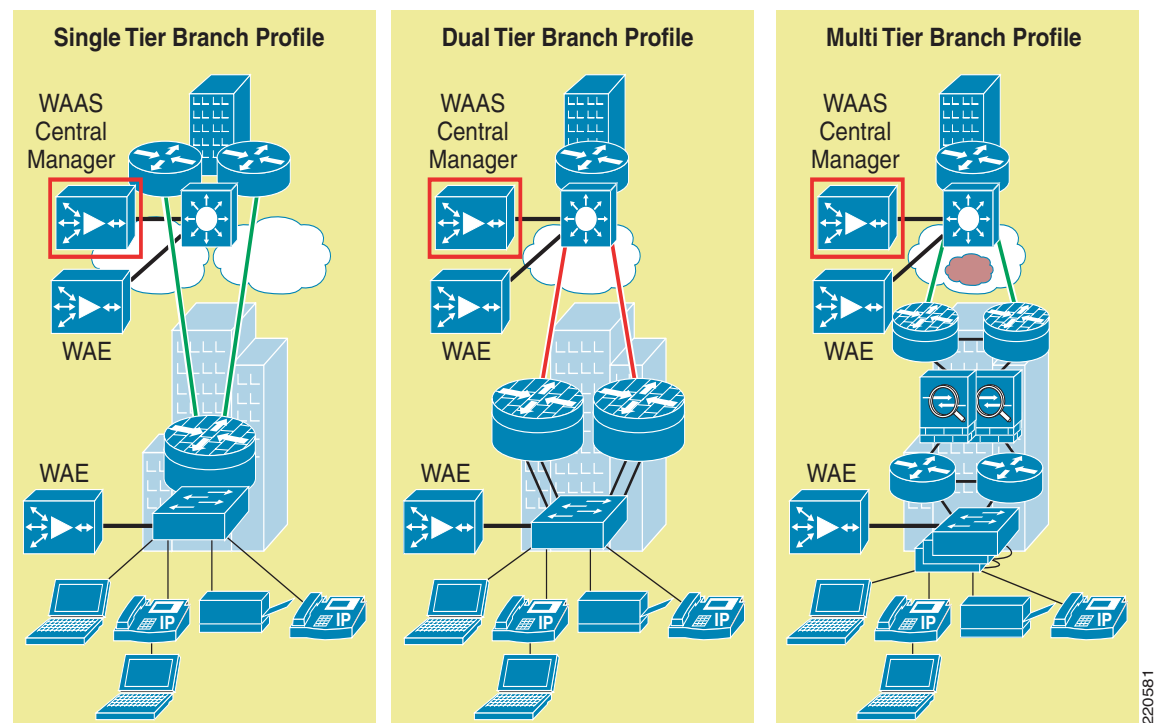
Figure 4 shows that the placement of the acceleration WAEs, namely at the branch, and WAAS Central Manager is similar in all three topologies. Within the full service branch (discussed in the next section), the WAAS network module, NME-WAE, is located within the integrated services router (ISR). Further discussions on LAN and WAN services design and configuration for the WAEs are provided later in this document.

WAAS is available as a hardware appliance or a network module. The WAAS network module, NME-WAE, can be either an edge WAE or a core WAE. Within each of the branch topologies, there are the following two branch topologies related to WAAS (see Figure 5).

- Extended Services Branch

- Consolidated Branch

Figure 5   ***Edge WAE Topologies***

Branch 1
Extended Services Branch
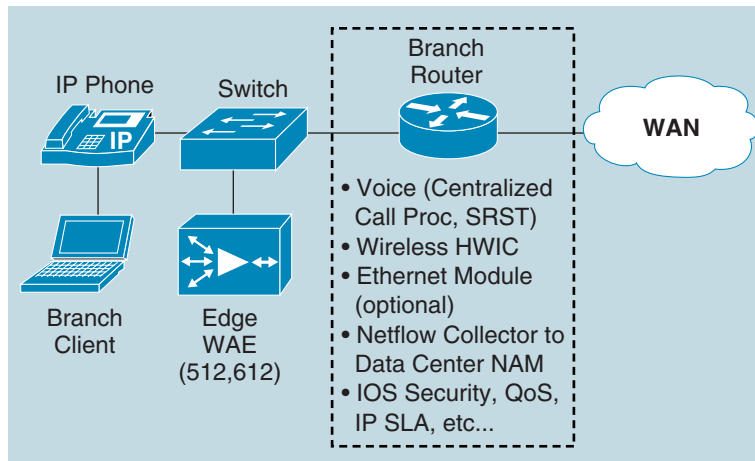
Branch 2
Consolidated Branch
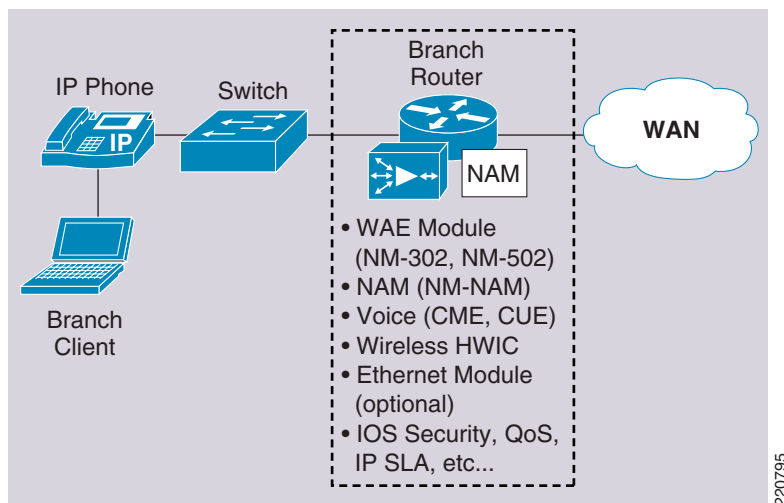
Branch 1—Extended Services Branch

The extended services branch is designed as an extension to an enterprise campus. It offloads as many of its infrastructure services to the headquarters campus as possible, including the following services:

- Voice services—Call processing agents located at the data center with voice endpoints at the branch. Call processing occurs over the WAN with high availability using Survivable Remote Site Telephony (SRST).

- Application networking services—WAAS appliances (WAE-512, WAE-612) provide scalable performance.

Branch 2—Consolidated Branch

A full-service consolidated branch provides a complete suite of LAN, WAN, wireless, voice, security services, network management, and WAN/application optimization services for the small and independent branch office. These services, similar to other branch profile solutions, use IOS routing and switching, QoS, security, and voice features to empower the branch. It differs from the other branch topologies in that aims to deliver all these services, including the hardware, within the single integrated services router (ISR) platform. The consolidated branch fits best into the smallest single-tier topology in the branch architecture profiles. Failover provisions for most services are not considered because the goal for this branch is to provide consolidated services in a manageable form factor at lower costs.

In addition to the generic services also offered in the extended services branch, consolidated branch includes the following services:

- Voice services—Call processing agents located at the data center with voice endpoints at the branch. Call processing occurs over the WAN with high availability using Survivable Remote Site Telephony (SRST).

- Application networking services—WAE network module (NME-WAE-302, NME-WAE-502).

- Network management services—The Network Access Module (NM-NAM) offers network monitoring services for branch LAN and WAN traffic. Cisco NetFlow data instead of being transported over the WAN to a NetFlow collector in the data center, is now offered in an ISR network module form factor.

- Security services—VPN AIM module for IPsec and SSL encryption services.

- LAN services—Ethernet switch network modules with or without Power over Ethernet (PoE) are available and vary between 16 and 36 ports in a single or dual NM form factor. The aim is to provide LAN services for a small amount of wired branch clients.

- Wireless LAN services—An AP supporting 802.11b and 802.11g is available in an HWIC form factor within the ISR for WLAN services to a small number of wireless branch clients.

Table 4 shows the some common ISR network and HWIC hardware for these services.

Table 4   Consolidated Branch Service and Hardware

Service	Consolidated Branch Hardware	Hardware Form Factor	Remarks
LAN	16 port	Network Module	The full-service branch may or may not have the client switchports within the ISR. This depends on the ISR hardware model, memory, and services enabled.
WAN	T1/E1 Frame Relay ATM MPLS	HWIC	MPLS and MetroEthernet may use the additional GE interface on the ISR to the service provider router.
Security	IP IPS	Network module	

Table 4   Consolidated Branch Service and Hardware

WAN optimization	NME-WAE-302 NME-WAE-502	Network module	WAAS network modules cannot be configured as a WAAS CM. Supported on the 2800 and 3800 ISR routers.
Network management	NM-NAM	Network module	

The Cisco 3825 or 3845 ISR is recommended for these services, although the 3825 router does not have enough network module slots to accommodate the EtherSwitch network module in addition to the WAAS NME-WAE and the NM-NAM.

For a comprehensive list of supported modules, see the *Cisco 3800 Series Integrated Services Router Data Sheet* at the following URL:
http://www.cisco.com/en/US/products/ps5855/products_data_sheet0900aecd8016a8e8.html.

Branch LAN Services

This section describes only basic types of configurations as they relate to the branch architecture. The *WAAS Deployment Cookbook* offers a number of possible configurations available with various switch and router configurations for both the data center and the branch.

LAN Services—Generic Considerations

LAN services with WAAS include the following areas of design considerations:

- LAN application traffic redirection and flow
- LAN segmentation

LAN Application Traffic Redirection and Flow

You can control whether client application traffic requests are redirected and processed by the WAE. Generally, this can be done in two modes: transparent (using WCCP), and policy-based routing (PBR). WCCPv2, deployed in most branches, is the preferred mechanism for interception and redirection in networks that use WAAS for acceleration. PBR is usually recommended in branch deployments that cannot deploy WCCP for any reasons, which may include hardware or IOS versions deployed that do not support WCCPv2. As a result, the focus is on WCCP deployment considerations at the branch.

There are several methods of deployment for the edge WAE as it relates to traffic redirection with WCCP. However, a brief review and better understanding of WCCP is necessary before describing these methods.

WCCP is a Cisco IOS feature that enables routing platforms to transparently redirect content requests. With the current version, WCCP v2, one router can support up to 32 routers redirecting to 32 different caching engines in an NxN configuration. WCCP has certain characteristics regarding how traffic is handled and distributed to various cache engines. They involve traffic flow assignments, traffic forwarding mechanisms, traffic re-direction, and intelligent filtering of traffic.

The WCCP traffic is forwarded to the WAE using one of two mechanisms:

- GRE encapsulation

Configuration with GRE encapsulation allows the router to be located multiple levels away from the WAE. For example, within the data center, it is possible to have the core WAE on a subnet within the data center access layer with the WCCP-configured router located at the WAN edge. Although rather minimal, the additional traffic and latency generated over the aggregation and core layers make this configuration suboptimal. For small- and medium-sized branches, the simplest and most direct configuration is with a WCCP GRE-encapsulated router.

- Layer 2 (L2) redirection

  L2 redirection applies only to branches that have a Catalyst switch configured. Furthermore, the WCCP router must be adjacent to the switch. ISRs do not support L2 redirection.

WCCP uses service groups to determine to which WAE to redirect traffic for further processing. These service groups are determined by the web cache and configured for identification by WCCP. The WAAS TCP promiscuous mode uses WCCP service groups 61 and 62 for traffic redirection. With WAAS configurations, within each location, service group 61 should be in the path of packet flow for one direction, and service group 62 should be in the path of packet flow for the opposite direction. For example, in the branch office, service group 61 should be in the path for traffic going from the client and the server. In the branch office, service group 62 should be in the path for traffic coming from the server back to the client.

Using WCCP ACL redirection may be beneficial for conserving WAAS processing. By default, all traffic is redirected to the WAE for inspection and optimization if configured in the application traffic policies (ATP). For the WAAS appliance, this may reduce the LAN traffic redirected to the WAE. It also offloads the WAAS network module for inspecting traffic that it would consider pass-through (for example, UDP-based packets). However, this is at the cost of router CPU utilization.

LAN Segmentation over Branch Topologies

The branch architecture identifies different types of LAN configurations at the branch, as shown in Figure 6.

Figure 6   *Branch Architecture WAN Topologies with WAAS*
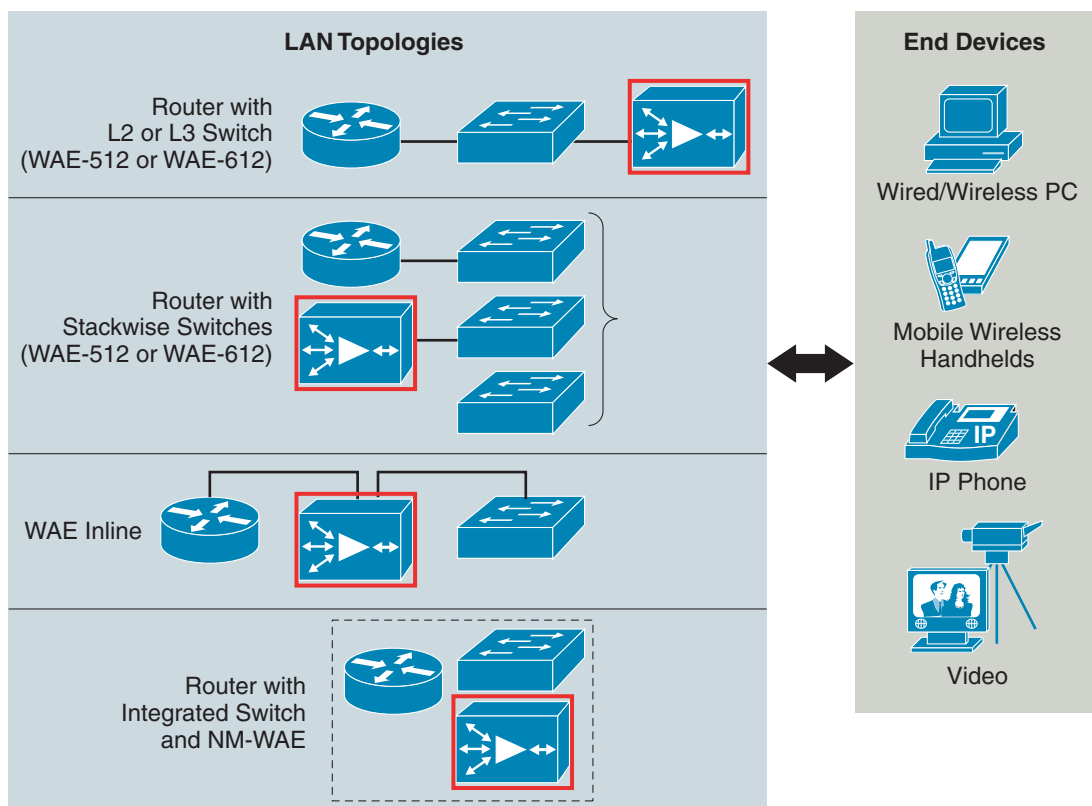
In each configuration, the branch WAE resides in its own VLAN, separate from either the data or voice clients. The WAE requires a tertiary interface, either on a separate interface or subinterface directly from the router. Doing this prevents a WCCP redirection loop where optimized or pass-through traffic from the WAE is intercepted and redirected back to itself by the WCCP-enabled router in the single subnet branch deployment model. Even in the second profile for the fully-empowered branch with the integrated switch, the WAAS network module appears as a client on an isolated VLAN.

The third topology contains the WAE inline network adapter. Because the configuration is inline, all TCP traffic is redirected through the WAE, bypassing any WCCP configuration and dependencies or IOS version dependencies for WCCP. Although its scalability is not as high as WCCP for redirection, the WAE inline network adapter has important benefits because of its simplicity and ease of configuration. For this reason, the inline network adapter is very appropriate for quick demo setups, initial rollouts of a solution to new branches, and even for smaller branch offices. More information on configuring the WAE inline network adapter can be found at the following URL:
http://www.cisco.com/en/US/products/ps6474/prod_module_installation_guide09186a00807bb70b.html.

Although the possibility of the last profile with an integrated switch is proposed, the option of a router with the integrated switch is somewhat impractical for scalability and shortsighted in capacity planning, limited to the number of wired branch clients. Such a configuration with NAM and NME-WAE can accommodate only a 16-port Ethernet slot and only within a 3845 ISR. Integrating the wireless module within the ISR does not accommodate any switchports. Therefore, unless the branch office is smaller than 16 clients, or perhaps configured so that all the clients are wireless, it is not very practical to have switchports integrated.

The following sample configuration shows the branch WAE tertiary interface on a router configured as a subinterface Gig 0/1.33 while the PC LAN interface configured on a separate subinterface, Gig 0/1.30.

```
interface GigabitEthernet0/1.30
 description ** BRANCH DATA VLAN **
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group LANout in
 ip wccp 61 redirect in   -- WCCP service 61 redirect to WAE
 ip wccp 62 redirect out  -- WCCP service 62 redirect from WAE to PC LAN
 ip flow ingress
 ...etc...
!
 interface GigabitEthernet0/1.33
 description ** BRANCH WAE VLAN **
 encapsulation dot1Q 33
 ip address 192.168.33.1 255.255.255.0
 ip wccp redirect exclude in - Block WCCP redirection back to the WAE
 ip flow ingress
 ip flow egress
 no cdp enable
...etc...
```

> **Note** IPv6 is not supported for WAAS 4.0 at this time. All IP addressing designs must be based on IPv4.

The speed of the switch used for integration is determines how the edge WAE is configured. Both the WAE appliance and network module have 2 Gigabit Ethernet interfaces. If the switch and router connected to the WAE are all Gigabit Ethernet, then the WAE can be left to a default of auto-negotiating the speed. However if any of the interfaces are FastEthernet, then the WAE needs to be manually configured for full-duplex with a speed of 100.

LAN Services—Branch 1

In the branch 1 topology, geared towards extended services and a larger number of users, the WAE hardware appliance is most likely deployed instead of the NME-WAE. The appliances have an external interface that connects to an external switch, or as part of a set of stackable switches.

The WAE has two external Gigabit Ethernet interfaces. Typically, one interface is configured for traffic redirection and optimization, and the other as a management interface. However, it is possible to use this second interface in a multi-homing configuration, provided that both interfaces are on the same subnet. The reason for this is that the WAE can have only one default gateway configured. More information about this is discussed in Branch LAN HA—Generic Considerations, page 22.

LAN Services—Branch 2

The NME-WAE has the following minor variations with the WAE appliance in its LAN configuration:

- The NME-WAE has an internal interface (through the router backplane) as well as an external interface (front-panel facing, connects to a switch). The internal interface is recommended for most common deployments using an ISR with Gigabit interfaces. The external interface is recommended for deployments that:
  - Use routers that have only FastEthernet interfaces and no GigabitEthernet (that is, 2811)
  - Use non-ISR routers including the 3725 and 3745
  - Are installed in routers that are already running at very high levels of CPU utilization
- The NME-WAE supports only WCCP redirection, where the WAE appliance can have either WCCP or Layer 2 redirection configured.

- The NME-WAE also appears within the branch router configuration as a service module, as follows:

```
interface Integrated-Service-Engine2/0
 description ** WAAS BRYCE MODULE **
 ip address 192.168.43.1 255.255.255.0
 ip wccp redirect exclude in
 ip nbar protocol-discovery
 service-module ip address 192.168.43.3 255.255.255.0
 service-module ip default-gateway 192.168.43.1
 no keepalive
 !
```

In this example, the primary IP address of the WAE is identified as 192.168.43.3 as well as its gateway, 192.168.43.1, and as with the WAAS appliance configuration, the NM-WAE that resides on a subinterface additionally excludes IP WCCP redirects from returning into the WAE and causing an endless loop.

For the branch 2 topology, the option of a router with the integrated switch is somewhat impractical for scalability, and is shortsighted in capacity planning, being limited to the number of wired branch clients. Such a configuration with NAM and NME-WAE can accommodate only a 16-port Ethernet slot and only within a 3845 ISR. Integrating the wireless module within the ISR does not accommodate any switchports. Therefore, it is not very practical to have switchports integrated, unless the branch office is smaller than 16 clients or perhaps is configured so that all the clients are wireless.

WAN Services

A number of branch profiles are available, generally based on size and complexity of the branch as well as the campus head end and the number of branches that it must service.

WAN Services—Generic Considerations

Application performance over the WAN can be affected by the following two important factors:

- Bandwidth—Generally, bandwidth is a measure of capacity over a communications channel.

- Delay—Within the context of this section on the WAN, delay is the round-trip latency for a packet across the WAN from the branch edge to the campus WAN edge. Although the true roundtrip-time (RTT) for an application includes latency from the application client and servers as well as the LAN infrastructures, this document scopes the delay to the WAN edges.

Both bandwidth and delay factors can be combined into a quantified value by which to measure the maximum amount of data that can be transferred over a WAN at a point in time. It can be seen as the storage capacity for data in transit over the WAN. This value is called the bandwidth delay product (BDP) and can be calculated with the following formula:

BDP [Kbytes] = (Bandwidth Link [Kbytes/sec] * Round-trip Latency [sec])

For example, the BDP value for a T1 link with a 60 millisecond delay is (1544 kbps/8 * .06 s) = 11.58 KB. This implies that for using the full T1 link with a 60 millisecond delay, the WAN can accommodate approximately 12 KB of data in transit at any point in time.

BDP can be used to determine whether TCP applications are making the most effective use of the WAN. This is related to how TCP does windows scaling. In a typical TCP transaction, the maximum segment size (MSS) is transmitted between both TCP endpoints. MSS determines the maximum amount of data that can be in transit and unacknowledged at any given time. Note the following observations about the MSS-to-BDP relationship:

- If MSS > BDP, the application can fill the available bandwidth pipe.

- If BDP > MSS, the application cannot fully use the network capacity and cannot fill the bandwidth pipe, although there may also be cases where an application has a maximum window size of 1 GB but it cannot fill the bandwidth pipe because of application latency.

In WAN links with very low bandwidth and/or very high latency, the BDP has relevance in maximizing WAAS TFO. The WAEs can be tuned so that its MSS is best suited for the type of WAN link at the branch. Wide area file services are also affected by the BDP and need to be tuned for its established sockets to be used most effectively.

The following guidelines are provided for WAAS TFO transfer and receive buffers:

- When deploying WAAS in hub-and-spoke scenarios, with mixed traffic and many connections, it is recommended to leave the buffers as they are (default, preconfigured values).

- When deploying or testing for high-speed links, and few batch transfer connections for specific use cases (for example, cross-data center replication) or link utilization testing, Cisco recommends to set the buffers to the maximum possible.

- In general production deployment, use the defaults if you have more than ~10 connections to be optimized on the link. In a low connection count scenario, use the defaults or if too low compared to the calculated BDP, use 4xBDP instead (up to the maximum buffer size allowed).

BDP settings for the WAE device can be configured either through CLI or the WAAS Central Manager GUI. For more information, see the *WAAS 4.07 Software Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v407/configuration/guide/cfgd.html.

Multi-Tier Branch WAN Design with MPLS

The multi-tier branch WAN design within the enterprise branch topologies was chosen because an increasing number of enterprises with a large number of branches have been migrating towards a multi-protocol label switching (MPLS) virtual private network (VPN) WAN design. MPLS offers the benefits of service provider management for dynamic any-to-any site tunneling, QoS, and service-level agreements.

Within MPLS, each VPN is associated with one or more VPN routing/forwarding instances (VRFs) that define the VPN membership of a customer site that is attached to a provider edge (PE) router. For more information about MPLS VRFs and its configuration in IOS, see the *Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4* at the following URL: http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/12_4/mp_12_4_book.html.

At the time of this writing, WCCP is not VRF-aware. Subsequently, VRF tunnels should not be configured on any routers with direct interfaces to the WAE. MPLS tunneling should work provided that the WAEs are deployed outside of the network tunnels. VRF support for WCCP is expected for WCCP v3.0, tentatively scheduled for release later this year.

While MPLS tunneling offers some measure of security, the tunnel itself is not encrypted. Some enterprises do not consider MPLS tunneling by itself secure enough for their data, and additionally opt for establishing encrypted tunnels between the branch and data center. Encrypted tunnels include IPsec, Dynamic Multipoint VPN (DMVPN), and Secure Socket Layer (SSL) VPNs. Group Encrypted Transport VPN (GETVPN) is a tunnel-less solution but has not been validated at the time of this writing. More about these tunnels are discussed in Secure Connectivity, page 24.

Figure 7 shows the separation between the types of tunnels established between a branch deployed with WAAS and the campus over an encrypted MPLS WAN.

Figure 7 Network Tunneling with WAAS
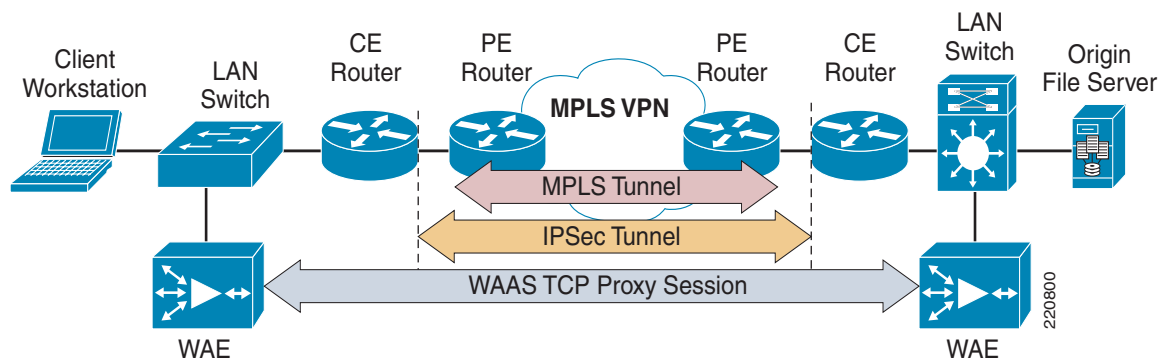
Note in Figure 7 that the MPLS and IPsec tunnels are configured outside the optimization path. Referring back to Table 3, you see that these network tunnels are established within the edge and core WAEs. This configuration was validated and tested with the results in the appendices of this document.

As long as the service provider meets the contracted service levels, the packets received at remote branches reflect the scheduling policies of the hub router (sometimes referred to as a *WAN aggregator*). The WAN aggregator controls not only campus-to-branch traffic, but also branch-to-branch traffic (which is homed through the hub). For a full-mesh design, QoS should equally be configured in all branch routers. For more information, see the *Enterprise QoS SRND v3.3* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html.

WAAS Sizing and Tuning for the WAN

Table 5 provides sizing guidelines for Cisco WAAS, effective FCS of WAAS 4.0.7. For the branch, note that the WAN link is one of the major criterion for choosing which model is appropriate:.

Table 5 Recommended WAN Links for WAAS Hardware Models

Device	Max Recommended WAN Link [Mbps]	Max Optimized Throughput [Mbps]
NME-WAE-302	4	90
NME-WAE-502	4	150
WAE-512-1	8	100
WAE-512-2	20	150
WAE-612-2	45	250
WAE-612-4	90	350
WAE-7326	155	450

The maximum optimized throughput is the throughput going through the WAE. Consider this table as a general rule of thumb in evaluating the WAN with the choice of WAE model. As mentioned before, Cisco recommends using the WAAS sizing tool as an aid to help streamline and automate sizing decisions. The WAAS sizing tool is available to Cisco sales teams and partners.

WAN Services—Branch 1

Branch 1 characteristics also include provisions for high availability at the WAN. More information on WAN high availability is discussed in Branch WAN HA, page 22.

WAN Services—Branch 2

Referring to Table 5, the branch 2 topology deployed with the NME-WAE is limited to 4 Mbps for the WAN.

High Availability

High availability (HA) at the branch can be viewed on several levels. As it relates to the branch, three levels of availability are the focus:

- WAAS-level HA
- Branch LAN HA
- Branch WAN HA

Considerations for each of these HA levels is discussed in the next sections.

WAAS-level HA

WAAS-level HA refers to the availability and error recovery within the WAAS appliance or module itself. WAAS offers several mechanisms to guarantee failover and error recovery capabilities:

- The WAAS DRE cache is persistent and loosely synchronized, enabling quick recovery in case of a reboot or software restart.
- All WAE appliances (51X, 61X, 7326) are configured with RAID 1 (when two or more drives are present) to provide storage redundancy and protection from disk drive failures.
- All WAE devices store vital configuration files (machine identity, network settings, and so on) as well as a recovery image on non-volatile compact flash.
- WAAS Central Manager can be configured as a hot/standby with a second central manager.
- WAAS Device Manager offers the ability to back up individual devices to enable fast restore onto a standby/replacement device.

Both the WAAS appliance and network module hardware include two Ethernet ports reserved for the network and management interfaces respectively. Note here, however, that WAAS allows the configuration of only one gateway address, so static routes are needed for the second network.

Core WAEs in a cluster are fault-tolerant and transparent to the edge WAE. That is, if one of the core WAEs in a single cluster fail, any of the other core WAEs within that cluster seamlessly handle further requests from any of the requesting edge WAEs. Similar behavior also applies to edge WAEs. Edge WAEs are also fault-tolerant and transparent to the client as to which WAE is used for application traffic optimization.

Branch LAN HA

At the branch, LAN high availability refers to transparent failover mechanisms at the LAN and branch client level.

Branch LAN HA—Generic Considerations

At this level, the WAAS failover options are considered. This is also rather straightforward if you configure two edge WAEs. Multiple edge WAEs can be configured in a cluster. By default, load balancing is done by round-robin, although it can be done by source and destination IP address. As an observation, it appears that the last WAE to be configured is the first WAE chosen in the round-robin by WCCP. The load balancing, however, is dependent on the hashing algorithm used by WAAS. Furthermore, each WAE in the branch cluster can be assigned a priority weight that favors preference of one WAE over the other:

- When used with WCCPv2, a service group of up to 32 WAEs and routers can be configured to provide high availability, load balancing, and automatic failover and failback.

- If used with PBR, up to four WAEs can be used as next-hop routes. PBR can be configured to leverage Cisco IOS features such as IP SLAs to monitor and track the availability of these next-hop routes.

Branch LAN HA—Branch 1

There are no unique branch topology considerations apart from those of the generic considerations.

Branch LAN HA—Branch 2

The branch 2 profile is not focused on providing hardware redundancy and failover, especially with network modules configured within the ISR platform. Nevertheless, it is technically possible to configure multiple-edge NME-WAENME-WAEs as part of a cluster at a branch within the same ISR. It is also technically possible to have an edge WAE appliance in the same device group as the NME-WAENME-WAE. Failure of a single WAE should not affect the continued transmission of traffic to its destination. It is instead sent unoptimized.

Branch WAN HA

WAN high availability refers to availability of WAN connectivity between the branch and campus WAN edge. It includes redundancy and seamless failover WAN links if a primary connection goes down.

For WAN high availability, active/passive WAN configuration is the most straightforward approach for WAAS. There are also configurations, based on routing decisions, where an asymmetric routing condition may occur.

Cisco WAAS supports asymmetric routing through the use of sharing network interception and redirection configuration across WAN boundary routers within a location. If all routers that connect a location to the WAN are participating in the same WCCPv2 service groups or have the same list of WAEs configured as next-hop routers (in the same order), the same WAE receives redirected traffic regardless of the WAN link to which the traffic was destined or from which it was coming.

For instance, if a customer has two WAN connections, one going to provider #1 and another going to provider #2, WCCPv2 can be configured such that the routers participate in the same WCCPv2 service groups, and the WAEs can be configured to register with both of the routers. This also requires that the WCCPv2 redirection configuration be applied identically across each of the routers within the same location; that is, use of 61/in on the LAN side on both routers and 62/out on the LAN side on both routers (or any valid combination of 61/62 in/out as long as they are identical among all routers within the location).

As traffic enters a WAN boundary router, it determines to which WAE to redirect the traffic based on a hash of either the source IP (service group 61 in the network path) or destination IP (service group 62 in the network path). The allocated hash buckets are synchronized within the service group, and the hash

value obtained at either router is the same as it would be had the traffic been forwarded through the opposite router. In this way, traffic is always redirected to the same WAE every time, regardless of which WAN link is used, or to which router the traffic was forwarded. As such, Cisco WAAS provides support for environments where asymmetric routing may be encountered.

Asymmetric routing may affect the WAAS Endpoint Mapper (EPM) service. The EPM service allows more a greater degree customization for enterprises applications that use a range of port addresses. It does so by mapping the optimization to the UUID value of the enterprise application rather than static mapping of all TCP ports used by that application.

Note EPM may not operate in deployments that may have asymmetric routing. In this case, EPM should be disabled. EPM is disabled by default in version WAAS 4.0.7 and higher.

Single- and Dual-Tier Profiles

The failover in the profile shown in Figure 8 shows that the backup has a much higher latency than the primary WAN interface. This implies that in a failover situation, WAAS optimizations have much more relevance during the downtime.

WAAS provides the most significant benefits in a high-latency WAN deployment. T1 and E1 at the branch may or may not be enough bandwidth, and for various reasons such as cost or service provider options, upgrading to a WAN with greater bandwidth is not possible.

The branch profile shown in Figure 8 belongs to the smallest type of branch deployment with some degree of high availability, where the primary link is a private T1 WAN and the backup is an ADSL connection over the Internet. For WAAS, the failover link is simply the addition of a second router in the WCCP TCP promiscuous list.

Figure 8   *WAAS Redundancy within the Single-Tier Branch*
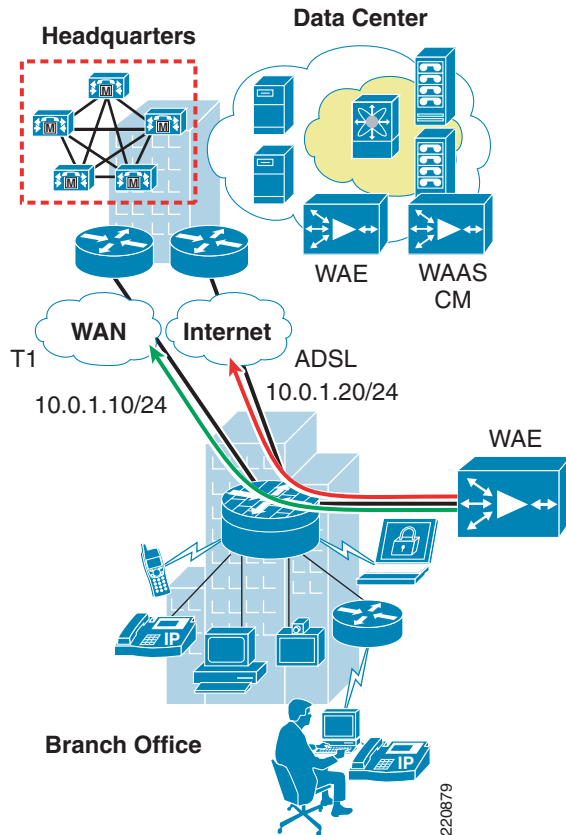
Security Services

Security services encompass a number of characteristics at the branch. The *Enterprise Branch Security Design Guide* identifies these as perimeter security, privacy, and threat mitigation.

Infrastructure Protection

Infrastructure protection involves taking measures that protect infrastructure devices, which include such as actions as turning off unnecessary services, shutting down unused switchports, and so on.

Secure Connectivity

This document considers the following four types of IP VPNs that establish secure connectivity over the WAN between the branch and the campus:

- IPsec
- DMVPNs
- SSL
- GETVPN

All four establish encrypted tunnels over the WAN. Encryption across the WAN should not be a problem as long as the traffic is encrypted after the source WAE optimization and decrypted before the packet reaches the destination WAE.

As noted in Figure 7, the encrypted tunnels should be established between the branch router WAN interface and the campus head-end router so that encryption and decryption are handled within the WAE TCP proxy connections. The test bed for this paper configured DMVPN tunnels between both branch topologies and the campus, and validated that DMVPN tunnels can be set up provided that the WAAS optimizations occur outside the tunnels.

Regardless of the type of tunneling chosen, you need to consider the amount of overhead for the WAN tunneling. The overhead may affect the bandwidth delay product (BDP) and possibly require additional parameter tuning of the WAAS maximum size segment (MSS) and TFO buffer sizes. BDP calculations and MSS adjustments are discussed in WAN Services, page 18.

Threat Defense

Threat defense includes provisions that are able to identify and mitigate against security attacks such as denial-of-service (DoS), Internet worms, and so on. Within the scope of the enterprise branch, threat defense includes such mechanisms as access control lists (ACLs), packet inspection with firewalls, and intrusion protection.

Access Control Lists

ACLs can be successfully deployed for a number of purposes. It can be used by WCCP to determine whether traffic is redirected to a particular web cache (in this case, the WAE) or sent directly through the router. Some applications are not only bandwidth-intensive but undesirable within the enterprise (for example, Kazaa, Bit Torrent). Although WAAS has classifiers for some of these applications, you need to consider whether you even want this packet to be redirected to the branch WAE for unnecessary processing. Note, however, that the more ACLs are added, the greater the processing load on the router. This needs to be balanced with the current hardware and processing load of the branches.

As per the branch architecture, you can apply traffic ACLs on the WAN-edge-in interface of the router (this is likely applied to tunnels as well). The ports shown in Table 6 are relevant to WAAS operations that should be permitted in the access lists.

Table 6   WAAS Relevant Ports

Port	Description
80	HTTP
139 or 445	CIFS file services
443	Secure-HTTP connection to WAAS CM GUI
4050	Communications between the branch WAE and core WAE

More details on the description of each port is available in the *WAAS 4.07 Software Configuration Guide* at the following URL:
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v407/configuration/guide/cfgd.html.

Packet Inspection with Firewalls

Firewalls are an inherent part of a security strategy for threat mitigation and perimeter defense. Its benefits include stateful, application-based filtering and defense against network attacks such as SYN flooding, port scans, and packet injection. For Cisco, firewall solutions include the firewall services module (FWSM), the Application Control Engine (ACE), the Cisco Adaptive Security Appliance (ASA), and IOS firewalls.

At the branch, the IOS firewall is used as the primary means of packet inspection and filtering. At the time of this writing, WAAS and stateful firewalling are interoperable if the packet inspection is applied outside of the WAAS TCP proxy sessions. From the branch perspective, this would be applying the firewall packet inspection to the LAN ingress interface. A future release of IOS will allow the IOS firewall packet inspection to also be applied at the WAN egress interface.

Although its deployment is more common for the campus and data center rather than the branch, the firewall services module, FWSM (v3.2), introduced a feature called "TCP state machine bypass", which allows traffic to bypass all the traditional TCP checks such as sequence number or unknown/invalid TCP flags and options. To implement this feature, you need to define a policy map that applies the "tcp-state-bypass" advanced option. You need to define the policy map for both directions, and apply the policy to inside and outside interfaces.

With Cisco's Adaptive Security Appliance (ASA), WCCP is supported only at the ingress of an interface at this time. See the *Cisco Security Appliance Command Line Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html.

The IOS firewall is one of the core components of branch security. IOS firewall uses Context-Based Access Control (CBAC), also known as IOS firewall stateful packet inspection and filtering.

With IOS version 12.4(11)T2, the IOS firewall allows traffic originating from the WAE to pass through.

The following changes are required for IOS firewall interoperability with WAAS:

- IOS version 12.4(11)T2 and above
- Additional IOS commands for inspecting packets coming from the WAE:
  - **ip inspect WAAS enable**
  - **ip wccp notify** (enabled by default)
- Zone security configuration

> **Note** IOS firewall compatibility with WAAS is supported only with zone-based security configuration.

Zone Security Configuration

Zone-based policy firewall (also known as "zone-policy firewall" or "ZPF") changes the firewall from the older interface-based model to a more flexible, more easily-understood zone-based configuration model. Interfaces are assigned to zones, and an inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface. This makes stateful packet inspection configuration much more simple because network administrators can more easily understand and configure firewall policies on network traffic, simplifying firewall troubleshooting and ensuring greater accuracy for firewall policies. Modular, granular firewall policies improve security by tightly controlling network service access and enforcement.

Zone-based firewalls do not have to replace existing ACLs; they can also be complementary. Also, zone-based firewalls are compatible with WCCP redirect ACLs, which can filter and either redirect traffic to the WAE or bypass the WAE entirely as pass-through.

Using Cisco Policy Language (CPL) configuration, the following tasks can be used to configure a zone-policy firewall:

- Define zones
- Define zone pairs
- Define class maps that describe traffic that must have policy applied as it crosses a zone pair
- Define policy maps to apply action to class map traffic
- Apply policy maps to zone pairs
- Assign interfaces to zones

To explain the concept of zone-based security as it relates to WAAS, consider the sample topology in Figure 9 and the following configuration.

Figure 9   ***WAAS Zone Security Configuration—Branch 1 Example***
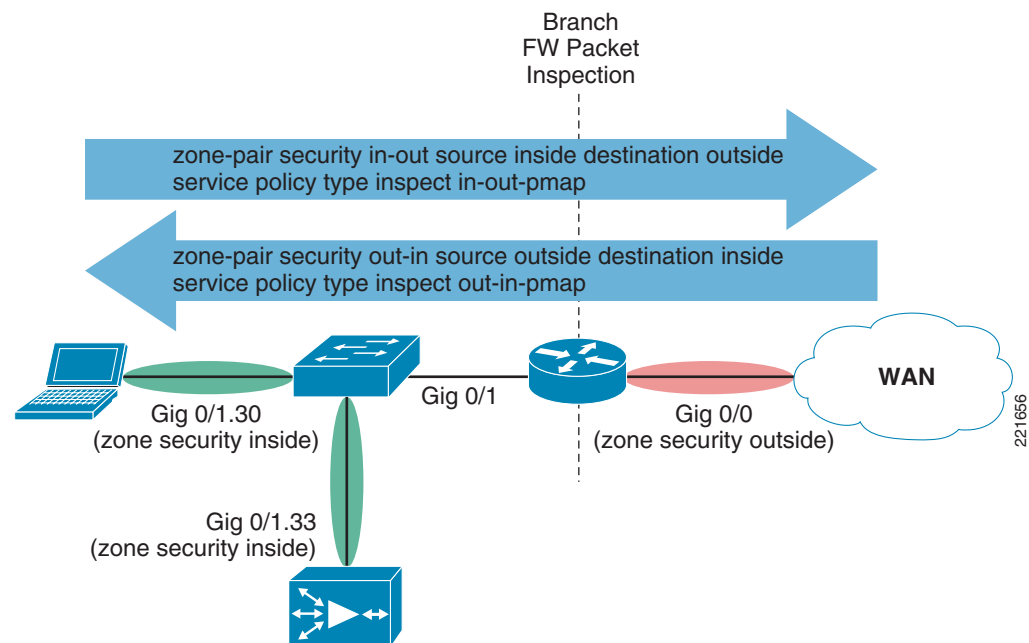
The following is a branch 1 IOS code snippet:

```
hostname FSB4-3825-2
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-11.T2.fc3
boot-end-marker
ip inspect WAAS enable -- allows WAE traffic through the firewall
! ...etc...
class-map type inspect match-any most-traffic--identifies traffic for ZPF packet inspection
 match protocol tcp
 match protocol udp
 match protocol icmp
! ...etc...
policy-map type inspect out-in-pmap-- policy map for zone-pair (traffic out to in)
 class type inspect most-traffic
  inspect
 class class-default
policy-map type inspect in-out-pmap-- policy map for zone-pair (traffic in to out)
```

```
 class type inspect most-traffic
  inspect
 class class-default
! ...etc...
!
!       -- The next section assigns zones to interfaces and policies to zone-pairs
!
zone security inside
zone security outside
zone-pair security out-in source outside destination inside
 service-policy type inspect out-in-pmap
zone-pair security in-out source inside destination outside
 service-policy type inspect in-out-pmap
!
!
interface GigabitEthernet0/0
 description ** WAN interface **$FW_OUTSIDE$
 ip address 192.168.20.1 255.255.255.0
 ip ips myips in
 ip ips myips out
 zone-member security outside
!   ...etc...
!
interface GigabitEthernet0/1
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 max-reserved-bandwidth 100
!   ...etc...
!
interface GigabitEthernet0/1.30
 description ** BRANCH DATA VLAN **$FW_INSIDE$
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 zone-member security inside
!   ...etc...
!
interface GigabitEthernet0/1.33
 description ** BRANCH WAE VLAN **$FW_INSIDE$
 encapsulation dot1Q 33
 ip address 192.168.33.1 255.255.255.0
 ip wccp redirect exclude in
 zone-member security inside
!
!   ...etc...
```

In this simple branch zone security example, two zones are identified and given the arbitrary names *inside* and *outside*. Interfaces residing behind the router at the branch and generally considered trusted endpoints are put in the inside zone. The WAN-facing interface, Gig 0/0, is identified as an outside zone and is generally considered untrusted. A zone pair matches up policies based on the traffic flow between the specified source and destination zones. In this case, two policies are created, *in-out-pmap* and *out-in-pmap*. Thus, in-out-pmap was assigned to traffic whose source was any interface assigned to *inside* and whose destination was any interface designated as *outside*. Similarly, the out-in-pmap policy was assigned to traffic flowing from the outside-to-inside zones. These policies are assigned classes of traffic that are inspected, similarly to the way QoS is configured. In this case, both policies are mapped to a class called **class-map type inspect match-any most-traffic**, which performs stateful packet

inspection on TCP, ICMP, and UDP traffic and sets them to default class. The policy could have easily been configured to permit or deny the traffic specified in the most traffic class. Finally, **ip inspect waas enable** is included for WAE traffic to pass through the firewall, and **ip wccp notify** is enabled by default.

For more details on zone-based policy firewall design and configuration, see the *Zone-Based Policy Firewall Design and Application Guide* at the following URL:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml.

Intrusion Protection

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. For more details, see the *Cisco IOS IPS Signature Deployment Guide* at the following URL:
http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd80327257.shtml.

IOS IPS uses a new XML-based signature format as of IOS versions 12.4(11)T and above. In addition to using XML-based signature definitions, IOS IPS 5.X requires a public crypto key. More details on configuring IOS IPS v5.X signatures can be found at the following URL:
http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd805c4ea8.shtml.

The following IOS IPS code example loads a basic IPS signature set:

```
!                      -- IOS IPS Public Crypto Key (downloaded from CCO)
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
!
ip ips config location flash:/ipsstore/ -- specifies location of XML sigdef file
ip ips notify SDEE
ip ips name myips
!
ip ips signature-category             -- loads basic IDS signatures
  category all
   retired true
  category ios_ips basic
   retired false
```

The example above specifies the location of the IPS signatures to the "flash:/ipsstore" directory, and specifies that the basic signatures "IOS IPS basic" be loaded. Cisco recommends the option of loading only the basic or the advanced signature set. Note that "category all" or all of the signatures have been disabled before loading the basic signatures. This is required to properly parse and load either the basic or advanced IPS signatures. The list of supported signatures for the IOS IPS v5.X format can be found at the following URL:
http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd8062ac75.shtml.

Enterprise branches that have already configured IOS IPS and are upgrading to this IOS version or above may require a migration procedure that converts IPS v4.X format signatures to 5.X. Note that the IOS IPS 5.X signatures are not backwards compatible, so they cannot seamlessly be rolled back to the previous version after you have migrated from 4.X to 5.X. For more details on how to migrate IOS IPS signatures from 4.X to 5.X, see the following URL: http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd8057558a.shtml.

Security Services —Branch 1 Considerations

No unique branch topology considerations from that of the generic considerations.

Security Services—Branch 2 Considerations

IOS firewall zone security should be trusted at both the network interface for the NM-NAM and NME-WAE, as well as at the actual NME-WAE integrated service engine and NM-NAM analysis module interfaces.

Figure 10 illustrates this example topology.

Figure 10   *WAAS Zone Security Configuration—Branch 2 Example*
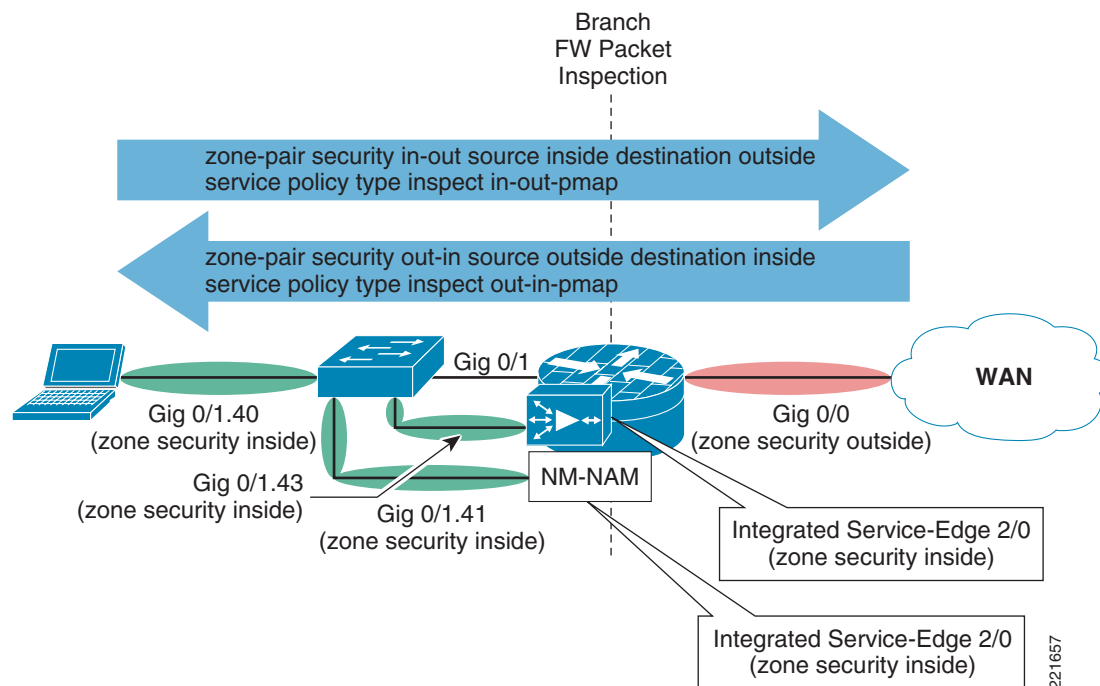
Both the NM-WAE and NM-NAM reside within the ISR and identified as interfaces *Integrated-Service-Engine2/0* and *Analysis-Module1/0,* respectively. However, the NME-WAE logically resides on subinterface Gig 0/1.43 with 192.168.43.1 as its primary gateway. Similarly, the NM-NAM resides on subinterface Gig 0/1.41 with 192.168.43.1 as its primary gateway. The WAN-facing interface is specified as *zone security outside*. Policies can then be applied to determine each zone's level of trust, as per infosec policy. The following is an IOS code snippet for the topology shown in Figure 10:

```
hostname FSB4-3825-2
!
boot-start-marker
```

```
boot system flash c3825-adventerprisek9-mz.124-11.T2.fc3
boot-end-marker
!
! ...etc...
class-map type inspect match-any most-traffic-- class map for zone fw policy
 match protocol tcp
 match protocol udp
 match protocol icmp
! ...etc...
policy-map type inspect out-in-pmap-- policy map for zone fw (traffic out to in)
 class type inspect most-traffic
  inspect
 class class-default
policy-map type inspect in-out-pmap-- policy map for zone fw (traffic in to out)
 class type inspect most-traffic
  inspect
 class class-default
! ...etc...
!
!   -- The next section sets the firewall zones and policies to enforce
!
zone security inside
zone security outside
zone-pair security out-in source outside destination inside
 service-policy type inspect out-in-pmap
zone-pair security in-out source inside destination outside
 service-policy type inspect in-out-pmap
!
!
interface GigabitEthernet0/0
 description ** WAN interface **$FW_OUTSIDE$
 ip address 192.168.21.1 255.255.255.0
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nbar protocol-discovery
 ip flow ingress
 ip flow egress
 ip ips myips in
 zone-member security outside
 ip route-cache flow
 duplex auto
 speed auto
 media-type rj45
 analysis-module monitoring
 no keepalive
 no mop enabled
 max-reserved-bandwidth 100
 service-policy output branch-wan-edge
!
interface GigabitEthernet0/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 zone-member security inside
! ...etc...
!
interface GigabitEthernet0/1.40
 description ** BRANCH2 DATA CLIENTS **$FW_INSIDE$
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip wccp 61 redirect in
```

```
 ip wccp 62 redirect out
 ip flow ingress
 zone-member security inside
 analysis-module monitoring
 service-policy input branch-lan-edge-in
! ...etc...
!
interface GigabitEthernet0/1.41
 description ** NAM MODULE **
 encapsulation dot1Q 41
 zone-member security inside
! ...etc...
!
interface GigabitEthernet0/1.43
 description ** WAAS MODULE **
 encapsulation dot1Q 43
 ip wccp redirect exclude in
 ip flow ingress
 ip flow egress
 zone-member security inside
! ...etc...
!
interface Analysis-Module1/0
 description ** NAM MODULE **
 ip address 192.168.41.2 255.255.255.0
zone-member security inside
! ...etc...
!
interface Integrated-Service-Engine2/0
 description ** WAAS BRYCE MODULE **
 ip address 192.168.43.1 255.255.255.0
 ip wccp redirect exclude in
zone-member security inside
service-module ip address 192.168.43.3 255.255.255.0
 service-module ip default-gateway 192.168.43.1
! ...etc...
!
```

Quality of Service

From an application perspective, quality of service (QoS) provides the most IOS-related control over how application messages are transmitted over the network. The QoS toolset consists of many IOS features available within the branch switch and router, selectively used based on how application traffic is handled.

It is important to remember that WAAS and QoS are completely complementary and to be considered as tools in the overall goal of application and WAN optimization. Traffic differentiation and prioritization relies on both technologies to achieve maximum performance benefits.

QoS—Generic Considerations

A revised picture of the QoS Strategy from the *Enterprise Branch Security Architecture* document with WAAS is shown in Figure 11.

Figure 11   QoS Branch Strategy (revised with WAAS)
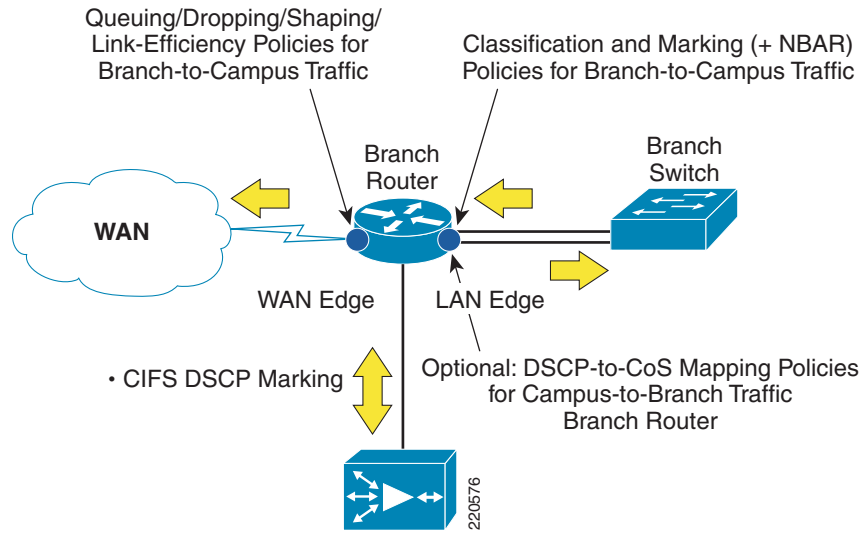
A good approach to applying traffic differentiation is explained in the Networkers 2006 presentation, "Introduction to Application Acceleration Technologies":

- Use NetFlow to determine what types of applications are residing on the network and where they are communicating

- Apply QoS traffic differentiation techniques as identified in the IOS QoS behavioral model

- Use monitoring tools such as IP SLA to evaluate the effectiveness of the applied QoS techniques on application performance

NetFlow and IP SLA interoperability with WAAS are discussed later in this document.

Traffic Differentiation at the Branch

The ten-class baseline QoS model for the branch edge was used for consistency with the existing branch architecture. The QoS configuration in Appendix C—Test Bed Configuration, page 50 is applied at the branch router. It is not applied at the core router because different QoS tools may be applied based on the actual location of the route on the campus. See the QoS SRND for more information on deploying QoS within the campus.

Traffic Classification

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. This classification can be done within the client itself, at the switch, or in the router.

The client application may provide DSCP markings for traffic before sending the packet over the network. However, the marked traffic may or may not be processed depending on whether the application is coming from a trusted client. Unless traffic is DSCP-marked by a trusted client, at the switch, or by WAAS, all traffic optimized by the edge WAE is classified as *class-default*.

Note   DSCP markings are not preserved for CIFS transport connections at this time. All TCP-promiscuous transport connects do preserve DSCP markings.

Network-Based Application Recognition (NBAR) is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that use dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by classifying packets and then applying QoS to the classified traffic. More details on the NBAR overview and configuration can be found in *Cisco IOS Quality of Services Solutions Configuration Guide 12.4* at the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/12_4t/qos_12_4t_book.html.

Because the WAE does not change any TCP header information, the operations performed by NBAR are transparent. Therefore, NBAR is able to inspect traffic and apply additional policies to it without affecting any of the WAAS optimizations, and vice versa.

Congestion Management

Congestion management features allow you to control congestion by determining the order in which packets are sent out an interface based on priorities assigned to those packets. Congestion management entails the creation of queues, assignment of packets to those queues based on the classification of the packet, and scheduling of the packets in a queue for transmission. The congestion management QoS feature offers four types of queueing protocols. All four allow you to specify the creation of a different number of queues, which affords greater or lesser degrees of differentiation of traffic, and also to specify the order in which that traffic is sent.

Real-time applications such as voice and video that need to be forwarded with the least latency and jitter use Low Latency Queueing (LLQ). This traffic should be passed unaltered by WAAS as pass-through and not affect queueing policies applied between the core and edge WAEs. Class-based Weighted Fair Queueing (CBWFQ) can be applied to all other non-critical applications.

Consistent with the QoS SRND, the branch should balance real-time priority applications with best effort. The recommendations to reserve at least 25 percent for best effort and to limit priority queuing to no greater than 33 percent link capacity. For more information on congestion management recommendations, see the *Enterprise Branch Security Design Guide* at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html.

In addition to queueing techniques applied within IOS, WAAS offers its own form of congestion management through its TCP windowing mechanisms. For example, selective dropping of packets causes WAAS TCP windowing mechanisms to throttle back window sizes.

Traffic Shaping and Policing

Policers and shapers usually identify traffic descriptor violations in an identical manner; however, they differ in how they respond to violations. For example, a policer typically drops traffic. On the other hand, a shaper typically delays excess traffic using a buffer, or queueing mechanism, to hold packets and to shape the flow when the data rate of the source is higher than expected.

Traffic shaping may be useful for the branch in cases where WAN traffic may need to be downscaled, such as an implementation where the committed rate is lower than the physical port speed. The LAN obviously has much more bandwidth and lower latency than traffic over the WAN. WAAS provides mechanisms such as DRE caching to reduce the amount of data that is needed to traverse the WAN between branch clients and origin servers.

Policing tools determine whether packets are conforming to administratively-defined traffic rates and to take action accordingly. Actions for this traffic may include marking, remarking, or dropping a packet. Revisiting the case of the bandwidth-intensive non-critical user applications such as Kazaa or Bit Torrent, you would perhaps want to either mark it as best effort or to even drop the packet entirely.

QoS parameters for traffic shaping and rate limiting can be used, provided that each individual application being shaped is well understood. For example, some applications may be sensitive to the buffer filling that may occur when the traffic rate is configured with a set average rate and burst.

For more information, see the *Cisco IOS QoS Configuration Guide, Release 12.4,* "Policing and Shaping Overview" at the following URL:
http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/12_4t/qos_12_4t_book.html.

IP Communication Services

The *Cisco Unified Communications SRND based on Cisco CallManager 5.x* (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a0080637440.html) identifies three IP telephony deployment models:

- Single-site—No VoIP calls traverse the WAN to remote branches. All phone calls going outside the campus go through a PSTN gateway to remote sites.
- Centralized WAN, Centralized Call Processing
- Centralized WAN, Distributed Call Processing—Consists of multiple independent sites, each with its own call processing agent connected to an IP WAN that carries voice traffic between the distributed sites. The IP WAN in this model does not carry call control signaling between the sites because each site has its own call processing agent.

Voice application messages can be categorized into two sets of protocols:

- Call control protocols—These protocols are responsible for call control services such as setup, tear down, and supplementary services such as call transfer and forwarding. They tend to be TCP-based. Examples of these include SCCP, Media Gateway Control Protocol (MGCP), and SIP.
- Streaming protocols—These protocols handle voice streams that occur between voice endpoints. These protocols tend to be UDP-based. Streaming protocols are delay and jitter sensitive and subsequently assigned high priority classification and priority queueing over typical enterprise non-mission-critical applications; examples include RTP.

By default, all traffic is directed (either by WCCP or PBR) to the WAE. Based on the application traffic policies, the WAE determines whether to apply optimizations or consider it pass-through. Given our descriptions of these voice messages, the WAE may improve performance for the TCP-based call control protocols because there is a TCP classifier for voice management; however, all the UDP-based streaming protocols are considered pass-through. WAAS, in the latter case, becomes only one extra stop and additional latency for the mission-critical voice streams, potentially affecting voice quality. Therefore, as a precaution, such traffic should be configured in WCCP so that this traffic is *not* redirected to the WAE at the branch. This can be done using a WCCP ACL.

Consider the following sample configuration snippet:

```
ip wccp 61 redirect-list WCCP-WAE
 ip wccp 62 redirect-list WCCP-WAE

    ...config etc...

 ip access-list extended WCCP-WAE
 permit ip 192.168.30.0 0.0.0.255 any
 permit ip 192.168.33.0 0.0.0.255 any
 permit ip 192.168.1.0 0.0.0.255 any
 permit ip 192.168.12.0 0.0.0.255 any
 permit ip 10.50.0.0 0.0.255.255 any
 permit ip 10.20.0.0 0.0.255.255 any
 deny   ip any any
```

In this example, the access list *WCCP-WAE* is applied to WCCP services 61 and 62. The data clients are on VLAN 30, the WAE is on VLAN 33, and the voice VLAN is on VLAN 32. The ACL is configured to permit traffic from the clients on VLAN 30 and VLAN 33. VLAN 32, on network 192.168.32.0, not listed on the access list, goes through the **deny ip any any** criteria, and is therefore not redirected to the WAE.

Cisco IP Phone Services

In addition to call control and voice streams, Cisco IP telephony also has IP phone services that provide some degree of web browser application control on the IP phone itself. IP phones such as the 7960s, 7970s, 7920, and 7921 models have basic HTTP client capabilities. Pressing the "Services" button generates an HTTP GET to the primary CallManager subscriber over port 80 on the phone client. There may be some optimization that varies based on the type of phone services application that has been developed and what types of HTTP calls it makes to the HTTP server. For example, the 7970 IP phone has the ability to download and display PNG files. Although not quantified, there may be some significant savings if many phones from different branches need to download and acquire PNG files at the same time.

Voice Services—Remote Branch 1

In the branch 1 profile, VoIP call processing and voicemail storage are centralized within the data center. In this hub-and-spoke model, calls originating from the branch first traverse the WAN to the CallManager server in the data center. After the call is established, the CallManager removes itself from the call until the call requires further call processing services (for example, transfer, call forwarding, and so on).

The other unique aspect with branch 1 in this situation is that of high availability with SRST. If the WAN fails and the connection between branch IP phones and the CallManager is not available, call control is then handled by the branch router. The connection re-establishes to the CallManager server after the WAN is up again.

Because both SCCP and SIP are TCP-based, it is technically possible to apply WAAS policies at the branch for both protocols. There are in fact default policies for VoIP and call management that include TCP port 2000, the default TCP port for SCCP. Preliminary tests show a modest improvement of approximately 1.7:1.

RTP voice streams are UDP-based and are not redirected to the WAE. Although more testing is needed to better quantify the effect of WAAS on voice applications that rely on enterprise data applications, the most latency-sensitive component of voice, being UDP-based, should not be affected by WAAS. Regardless, you can apply WCCP ACLs such that all TCP-based call control traffic is not redirected to the WAE.

Voice Services—Remote Branch 2

Unlike branch 1, branch 2 has the call processing agent as well as the voicemail storage located within the branch router using Cisco CallManager Express (CCME) and Cisco Unity Express (CUE).

CCME and CUE can technically co-exist with the WAE. Because CCME is IOS-version independent, if you already have a branch with CCME deployed and want to deploy WAAS, you must ensure that the IOS versions are compatible with both CCME and the NME-WAE. IOS version 12.4(9)T and 12.4(11)T are compatible versions for both. More details on compatible IOS versions can be found in the Unified CallManager Express Interoperability Matrix at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_installation_guide09186a00805acf50.html

Branch 2 has not fully been tested with CCME and CUE co-located at this time. As with the voice services general considerations, it is not clear what the impact of co-located voice services is with a branch router running application networking services. To be safe, Cisco recommends that any voice traffic be redirected to the branch WAE until there is a better understanding of the impact on voice packet latency for both call control (TCP traffic optimized by WAAS) and voice streams (UDP traffic is not routed to WAAS by default, but is considered pass-through and not optimized).

Measuring Optimizations and Performance Improvements

WAAS is essentially a branch solution where the optimizations are noted in the WAN as well as the end-user experience of applications.

Application performance is measured depending on who is the consumer of the data. To the end user, it is the application response time because performance is evaluated by the user experience. To the network administrator facing a low bandwidth, high latency WAN, the metrics include the following:

- Link utilization

- Effective capacity

- Client/server response time

- TCP and application protocol latency

- Dropped packets

There are performance metrics that are unique to the particular application that is being deployed on the enterprise. Cisco provides various tools for measuring performance. IOS-based tools include NetFlow and IP SLA. The Network Access Module (NAM) is also available as a network module within the ISR. These are discussed further in the following sections.

User-Centric Metrics

One of the most compelling reasons to use WAAS is to provide the user with as close to LAN-like response as possible, with an application now residing over the WAN. This implies that the user and application response time become critical metrics. End-to-end latency times (application client/server latency + network latency) from the client perspective can be measured easily for bulk-data applications such as HTTP and FTP. In these applications, you can capture download times and perceived download rates.

NetFlow

Cisco IOS NetFlow services provide network administrators with access to information concerning IP flows within their data networks. Exported NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting, and departmental chargebacks, Internet service provider (ISP) billing, data warehousing, combating DoS attacks, and data mining for marketing purposes.

NetFlow is UDP-based, and although there are classifiers within the WAAS CM, they are considered pass-through. Nevertheless, NetFlow is interoperable with WAAS, and IP route cache flows can be applied on the interface performing WCCP redirects.

NetFlow statistics can be viewed using the IOS CLI with the command **show ip cache flow**. An example NetFlow output using the CLI (shown below) lists the top ten TCP- or UDP-based applications as well as the number of packets and flows from the source interface to the destination interface. In this case, the traffic flows are from the edge WAE (192.168.33.3) to the branch router (192.168.33.1), and from the edge WAE to the WAAS Central Manager (192.168.33.1) located in the data center:

```
FSB4-3825-1#sh ip cache flow
IP packet size distribution (33553957 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002 .471 .364 .071 .005 .013 .001 .001 .000 .000 .000 .000 .000 .003 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .000 .002 .056 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  8 active, 4088 inactive, 10863748 added
  184947568 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  9 active, 1015 inactive, 10864829 added, 10863748 added to flow
  0 alloc failures, 31963 force free
  1 chunk, 5148 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows    /Sec    /Flow   /Pkt    /Sec    /Flow      /Flow
TCP-Telnet         307      0.0      20     58      0.0     11.0       10.9
TCP-FTP            398      0.0       5     55      0.0      6.7        8.4
TCP-FTPD           561      0.0    3037    952      0.8     21.1        8.3
TCP-WWW          79716      0.0       7    578      0.3      0.5        6.3
TCP-SMTP           104      0.0       1     44      0.0      0.0        5.6
TCP-X              104      0.0       1     44      0.0      0.0        7.0
TCP-BGP            104      0.0       1     44      0.0      0.0        6.7
TCP-NNTP           104      0.0       1     44      0.0      0.0        6.3
TCP-other     10596579      5.4       1     82     10.5      0.1       15.2
UDP-DNS            229      0.0      68     69      0.0    191.0       14.8
UDP-NTP          22170      0.0       1     76      0.0      0.0       15.4
UDP-TFTP          1890      0.0       1     56      0.0      0.0       15.4
UDP-other        59775      0.0       9    189      0.2     32.8       15.3
ICMP             51730      0.0       1     73      0.0      0.0       14.4
GRE              48888      0.0     201    130      5.0     14.6       15.4
IP-other          1086      0.0     384     60      0.2   1774.1        2.4
Total:        10863745      5.6       3    150     17.3      0.6       15.2

SrcIf        SrcIPaddress    DstIf       DstIPaddress    Pr SrcP DstP  Pkts
Gi0/1.33     192.168.33.3    Local       192.168.33.1    11 0800 0800   158
Gi0/1.33     192.168.33.3    Gi0/0       192.168.1.33    11 2711 07D0     1
FSB4-3825-1#
```
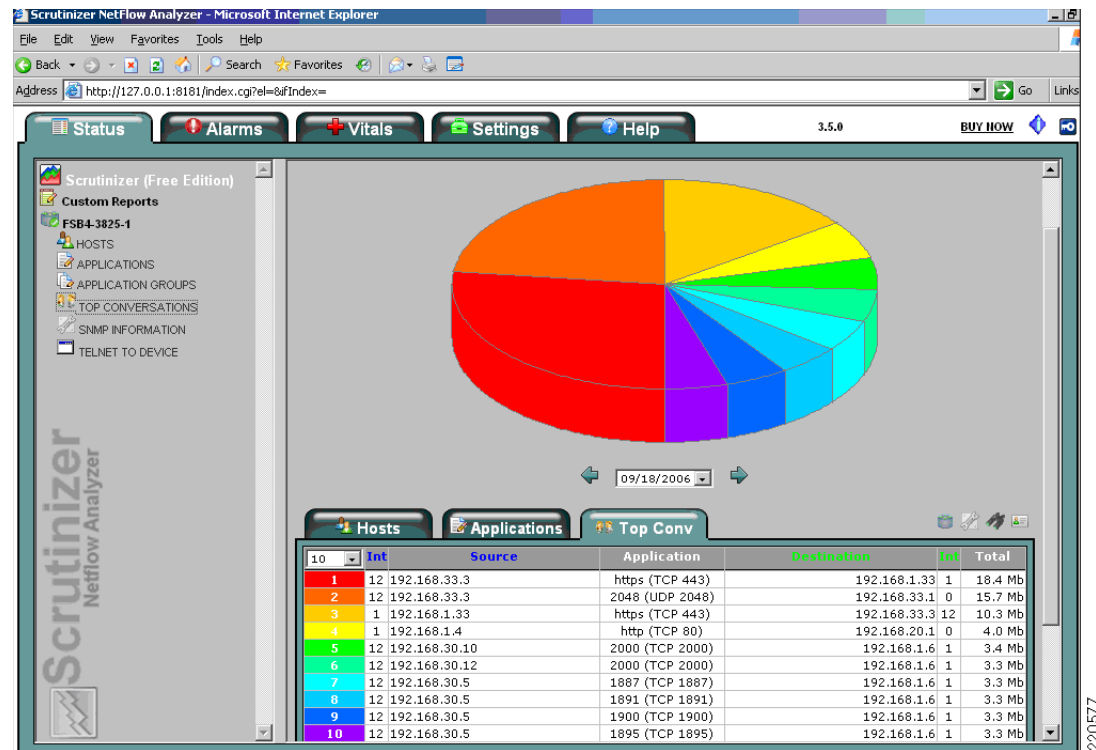
NetFlow Collector applications are available commercially, providing a user-friendly GUI to process and view NetFlow statistics.

Figure 12 shows a sample NetFlow capture for the branch router using the Plixer International Scrutinizer NetFlow Analyzer.

Figure 12   *Sample NetFlow Capture*

This GUI snapshot of the top ten talkers at the branch router interface, taken with the test bed in IDLE state, shows that the most traffic in IDLE state was basic housekeeping traffic generated between the edge WAE (192.168.33.3) and the WAAS CM (192.168.1.33).

Top applications show on average how many packets belonging to the application passed through the interface. A snapshot of this is shown in Figure 13.

Figure 13   *Traffic Snapshot*
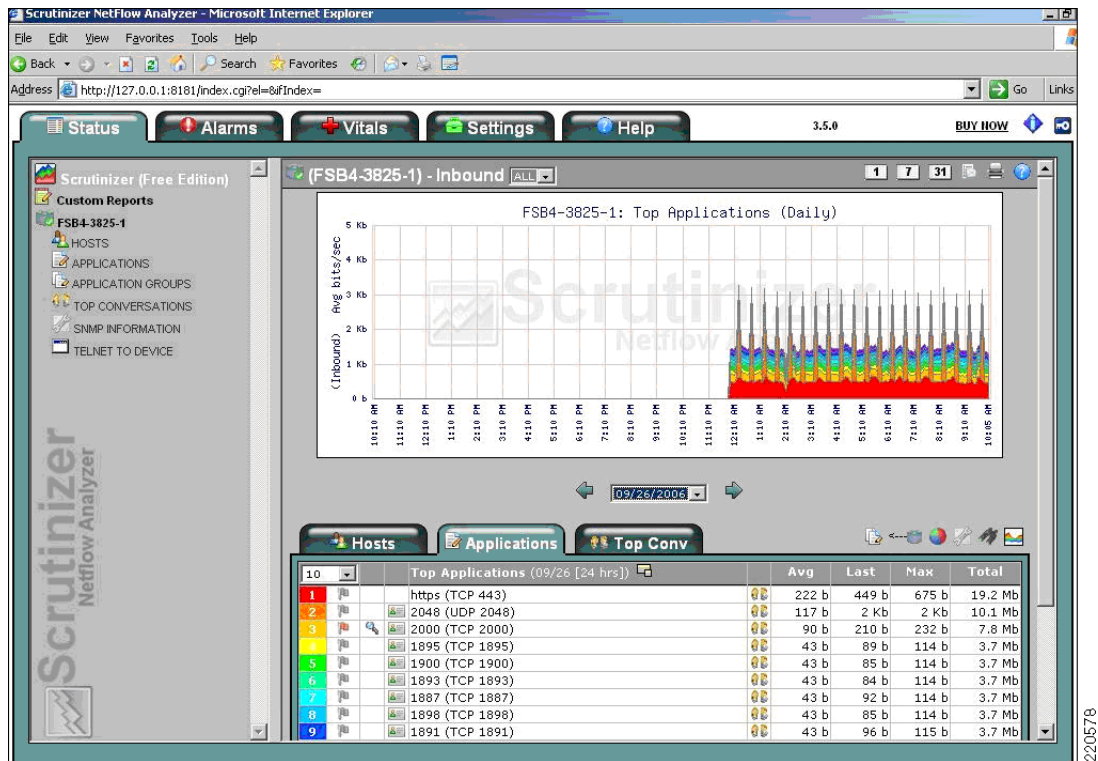
NetFlow—Branch 1 Considerations

To save processing on the edge WAE, you may also want to process LAN-edge-in flows to bypass redirection to the WAE to reduce processing on the WAE. This of course also increases WCCP and overall CPU processing on the branch router.

NetFlow—Branch 2 Considerations

The Network Analysis Module (NM-NAM) feature is a network module that monitors and analyzes network traffic for a system using extended Remote Monitoring (RMON) standards, RMON2, and other Management Information Bases (MIBs). The NM-NAM provides application response visibility for the consolidated branch, removes the need for a local NetFlow collector file server, and offloads processing for the logging of NetFlow information within a syslog file within the router. Figure 14 shows a summary of the top applications that were processed following a small load test of generating HTTP traffic.

Figure 14   *NAM Traffic Analyzer*
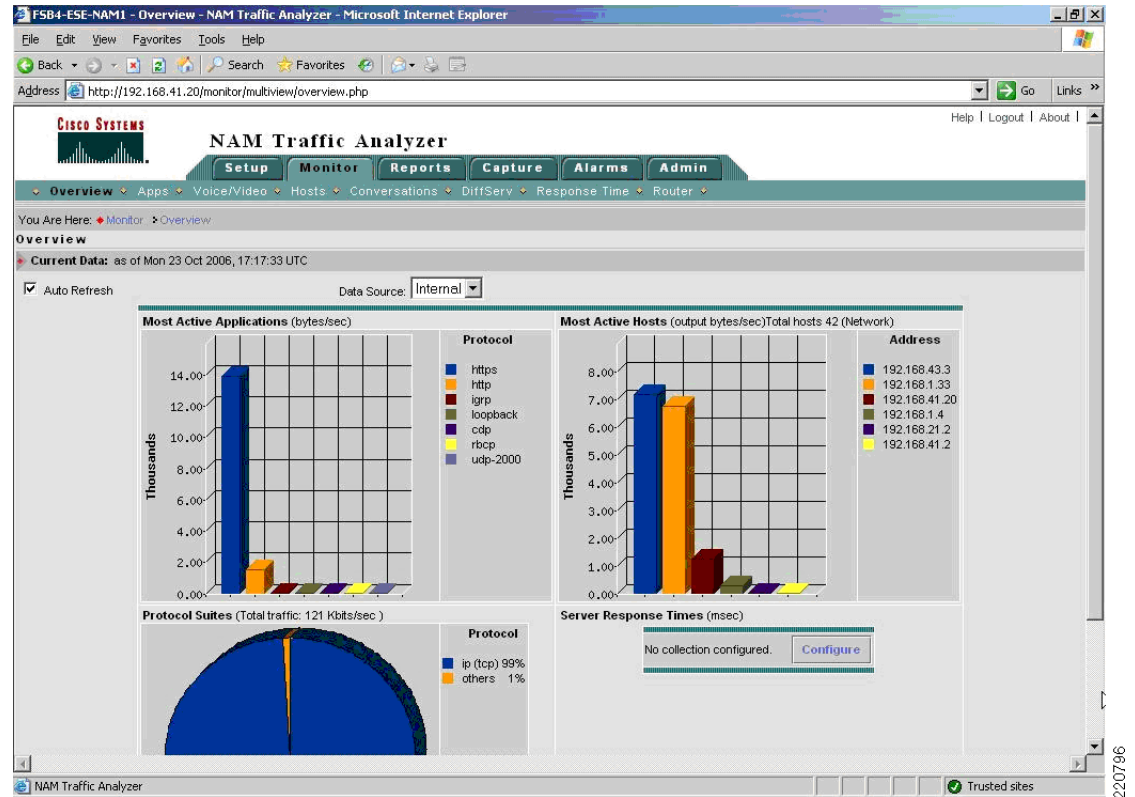
NetFlow collection can be applied at any interface and is interoperable with the WAE. In fact, it is a good tool to measure how much traffic is being passed in between the WAAS components. Consider the NM-NAM traffic statistics shown in Figure 15.

Figure 15   *NM-NAM Traffic Statistics*
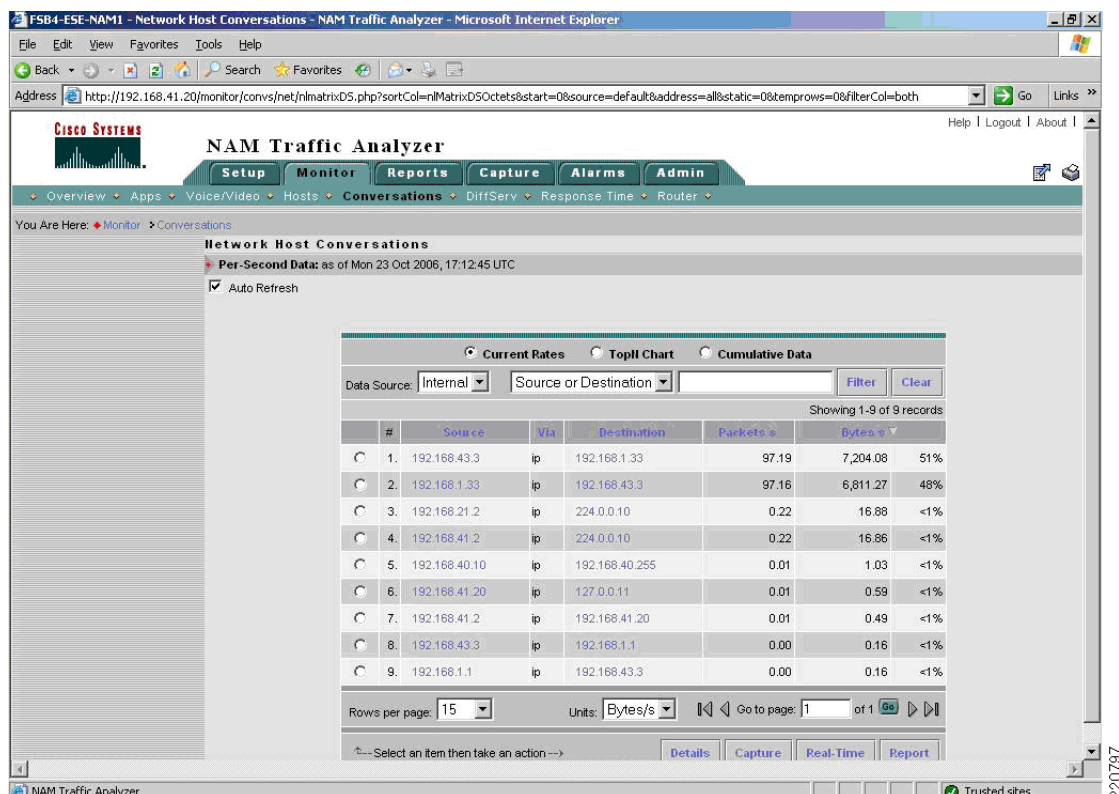
In Figure 15, following a rather small load test of generated HTTP traffic from a branch client to a web server in the data center, you can see the average amount of packets and bytes per second that is generated between the edge WAE (192.168.43.3) and the WAAS central manager (192.168.1.33).

IP Service Level Agreements

IP Service Level Agreements (IP SLAs) provide a means to measure network performance through the simulation of common network data and IP services, collecting this network performance in real-time, and sending alerts if certain configured thresholds are not met. IP SLA supports a number of common TCP protocols that include but are not limited to ICMP, HTTP, FTP, voice protocols such as SIP and H.323. For more information on which protocols are supported, see the *IP SLAs Configuration Guide, Release 12.4* at the following URL:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804441596.html. Metrics such as delay, jitter, packet loss, voice quality, and server or website download time may be captured as part of real-time or post-processing analysis. From the branch router perspective, an IP SLA responder on the head end may be configured depending on the type of protocol monitored.

It is interesting to note that for most WAAS deployments, running some of the IP SLA configurations monitors only the supported TCP protocols from router to router (if there is an IP SLA responder configured), or from the branch router to a server within the data center. The client in each of the IP SLA sources is actually configured within the router. This means that the IP SLA results may not always display the optimizations done between the core and edge WAEs.

The following IOS snippet shows an example of configuring IP SLA for an HTTP operation.

```
ip sla monitor responder
ip sla monitor 10
```

```
 type http operation get url http://10.20.200.200:8081/Kelev/view/home.php
 frequency 300
ip sla monitor schedule 10 life forever start-time now
```

This example is set to send the HTTP get to the configured URL every five minutes indefinitely. Statistics for round-trip time can be seen in the following:

```
FSB4-3825-1#sho ip sla mon stat
Round trip time (RTT)   Index 10
       Latest RTT: 912 ms
Latest operation start time: 12:51:39.009 EST Fri Mar 2 2007
Latest operation return code: OK
Latest DNS RTT: 0 ms
Latest TCP Connection RTT: 86 ms
Latest HTTP Transaction RTT: 826 ms
Number of successes: 1
Number of failures: 0
Operation time to live: Forever
```

Note here that the HTTP get is originating from the router going to the web server URL, and is outside the WAAS optimization path. Subsequently, if you assume that the LAN delay is negligible, you use these IP SLA statistics as a baseline comparison and see the WAAS improvements for calls made to the same URL.

Note There is IP SLA full feature parity with the IOS 12.4 "non-T" train on ISRs, and there are no incompatibility issues. However, as of this writing, the most current IOS version supporting the NME-WAENME-WAE, 12.4(11)T, does not have the full implementation of IP SLA and is not officially supported at this time.

WAAS-Centric Performance Metrics

As previously mentioned, application performance at remote sites is most often measured by the user experience. WAAS, however, also provides its own analysis as to what application traffic was reduced, how link utilization is improved, and what this means in terms of effective capacity of the WAN link.

One of the useful WAAS statistics pages is seen in Figure 16.

Figure 16   WAAS Traffic Statistics Detail Report Example
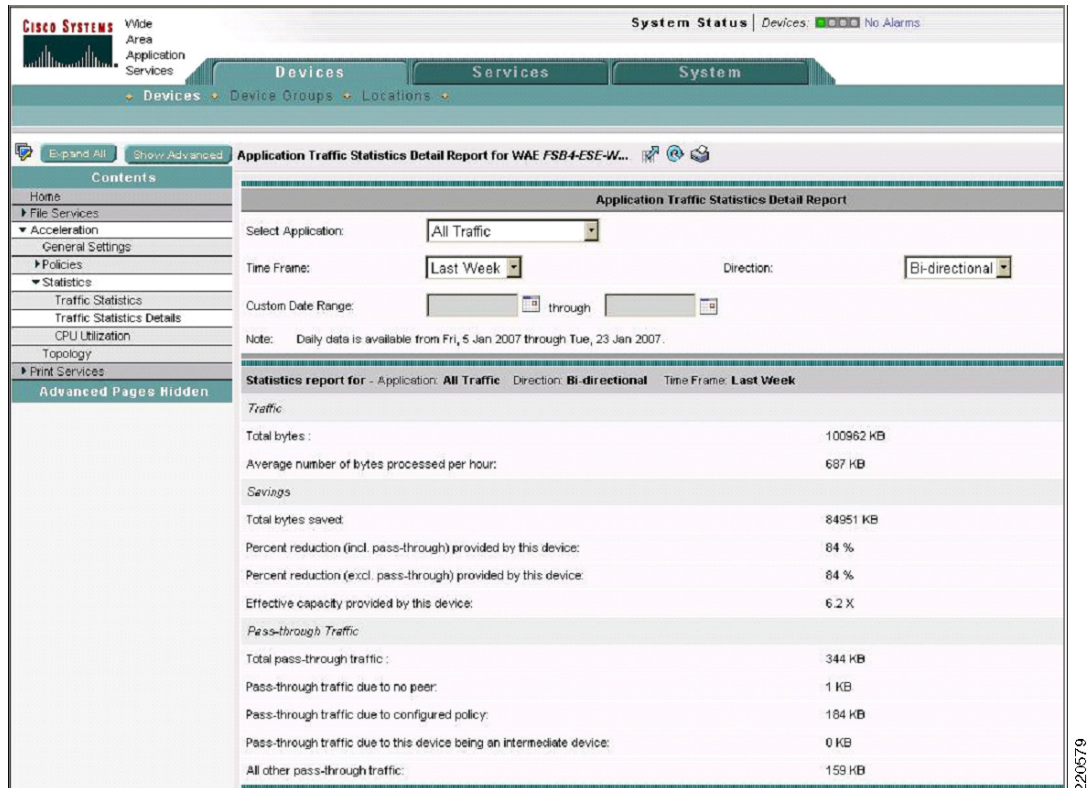
This statistics report reveals how many bytes passed through the WAE, and based on the optimizations for the application traffic policy (ATP) applied (DRE, LZ, TFO), how many bytes were saved overall. Some of the basic statistics are discussed below:

- Percent reduction—The percentage of total bytes saved from the total number of bytes passing through the WAE. For example, in Figure 16, this is easily calculated. The total number of bytes saved, 84951 KB is approximately 84 percent of the total bytes, or 100962 KB.

- Effective capacity—Effective capacity is an important metric for the network administrator, who is monitoring whether the WAN has sufficient bandwidth to accommodate the increasing traffic demands of data-intensive applications.

- Pass-through traffic—Pass-through traffic consists of data that passes through the WAE, but is not optimized. This is no different from traffic that is passed over a native WAN. Pass-through may be a valuable metric because if the pass-through percentage is high, you need to investigate why this is happening. One possible reason may be that the application TCP port is not included in any of the ATP classifiers and it needs to be added.

In addition to the overall statistics in Figure 16, you can see the reductions by the type of ATP traffic configured or identified as illustrated in Figure 17.

Figure 17   *WAAS Application Traffic Statistics Report*
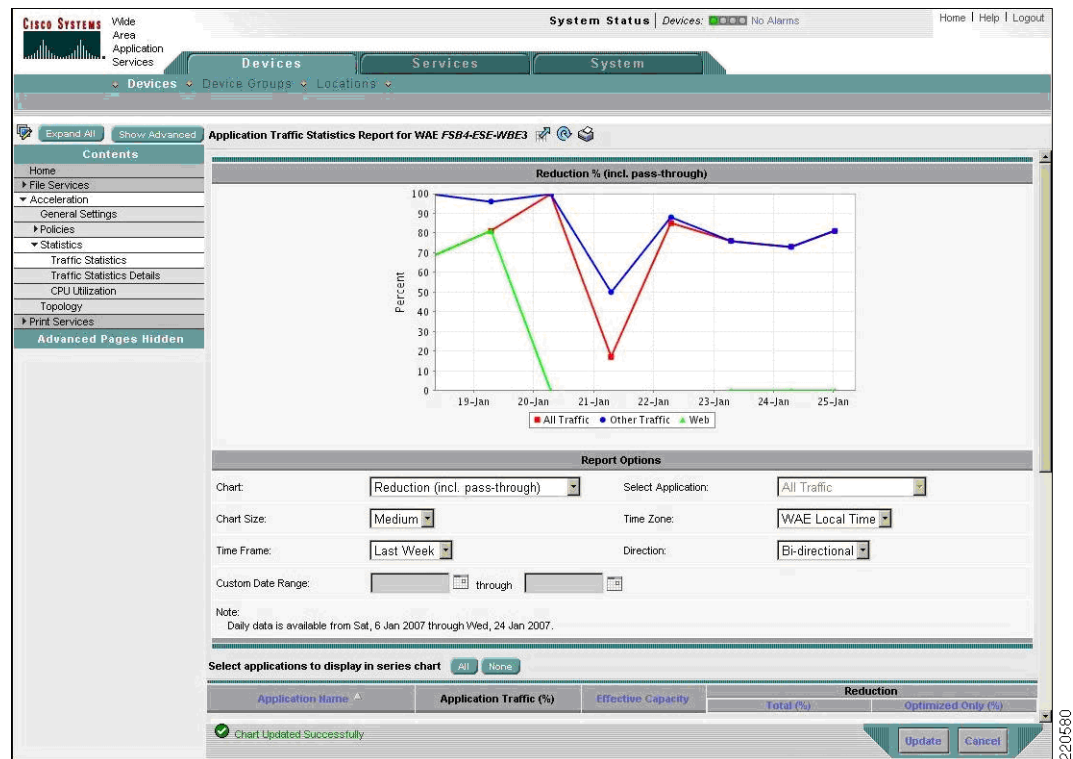
In this example, note the graph for traffic generated on Jan 20. The branch clients have made multiple HTTP requests to a web server within the data center that contains web pages with PHP scripts. These pages had a combination of web objects to download, and which WAAS properly identified as web traffic. However, there were a number of messages that WAAS could not identify that were classified as "Other".

"Other" traffic optimizations can involve traffic that may not have been explicitly configured in the WAAS ATPs. However, WAAS identified them as TCP messages and could have performed optimizations on them anyway such as TFO or DRE. Basically, this shows that WAAS improved packet savings overall, but it is not possible to see with greater granularity exactly what was optimized.

Therefore, this encourages more of the recommendation that the network administrator better understand the behavior of the application that is being traversed over the WAN. The more you understand and are able to classify the application traffic ports, the better the ability to monitor the reduction savings on this traffic.

Several tools can help identify what traffic that may be. One of them is a freeware called TCPView, and is available for download on the Microsoft site: http://www.microsoft.com/technet/sysinternals/utilities/TcpView.mspx. This tool can be run on a Windows client or server to determine what TCP traffic along with their ports are being used. With this information, you can then edit either existing classifiers or create new custom classifiers on either the branch or core WAE for applying its optimization mechanisms.

Branch 1 Considerations

There are no unique branch topology considerations apart from those of the generic considerations.

Branch 2 Considerations

There are no unique branch topology considerations apart from those of the generic considerations.

Miscellaneous Operations

Synchronization and Timing

All the WAEs and the WAAS CM must be properly synchronized to avoid minor alarms and ensure that traffic statistics are properly updated for management in the WAAS CM. For this reason, Cisco recommends having a Network Time Protocol (NTP) server on the campus so that branch WAEs from multiple sites can synchronize to a common centralized source.

Summary

WAAS is one of the key Cisco application networking service components for the improvement of application and WAN optimization solutions. However, as branch offices increase in the size and complexity of their deployment, so do the interdependencies of their infrastructure services. The approach to WAN and application optimization begins with a comprehensive understanding of the behavior of branch applications. A branch infrastructure needs to be designed as a whole to capitalize on network resource features. By doing so, you add a measure of intelligent application inspection and routing for response time and link utilization, which are the two common bottleneck resources at the branch.

Appendix A—WAAS-IOS Branch Interoperability Matrix

Interoperability with certain IOS features found within the branch could be summarized in the matrix in Figure 18. The matrix itself shows the IOS features that were enabled at various switches and routers in the application traffic path, and whether they were interoperable with WAAS.

Figure 18   **WAAS-IOS Interoperability Matrix**

Feature / Router Interface	DC LAN Edge	Core WAE	Campus WAN Edge	WAN	Branch WAN Edge	Branch WAE	Branch LAN Edge
QoS	Y		Y	N/A	Y		Y
NBAR	Y		Y	N/A	Y		Y
IOS FW SPI (ip inspect)	Y		N	N	Y		Y
IOS FW ACLs	Y		Y	N/A	Y		Y
IOS IPS	Y		N	N	Y		Y
Netflow	Y		Y	N/A	Y		Y
IP SLA	N/A		Y	N/A	Y		N/A

More discussion on Cisco IOS interoperability with WAAS is available in the *WAAS 4.07 Software Configuration Guide at the following URL:*
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v407/configuration/guide/cfgd.html.

Appendix B—Example Test Configuration

The test configuration used for the branch test bed is shown in Figure 19.

Figure 19 **WAAS Test Configuration for Branch Services Interoperability**
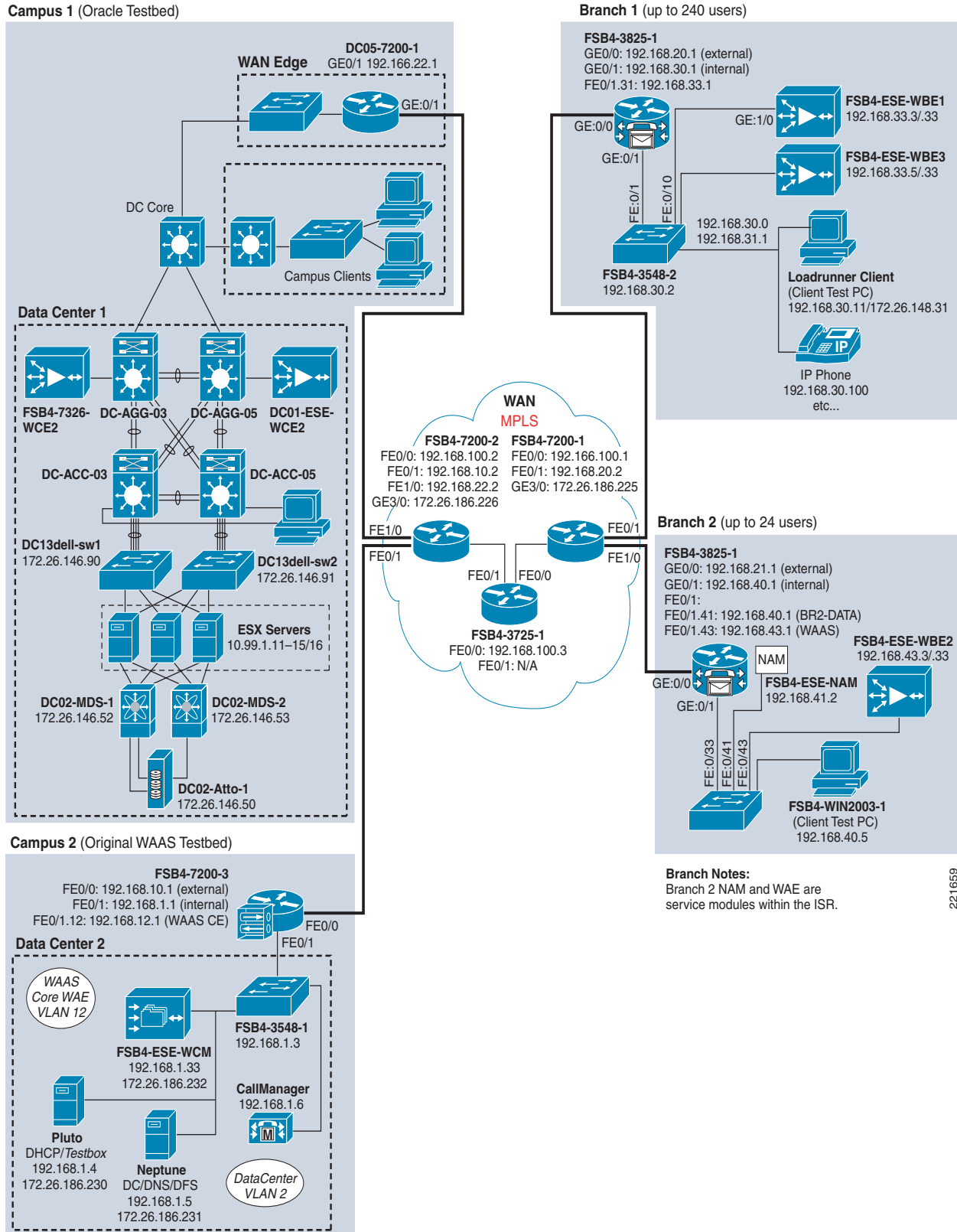
Table 7 shows the test configuration hardware and software versions.

Table 7   Test Configuration Hardware and Software Versions

Network Component	Hardware Model	Software Version
Branch1 router (FSB4-3825-1)	3825 ISR	12.4(11)T2
Branch1 WAE (FSB4-ESE-WBE1)	WAE-511	4.0.9 b10
Branch1 switch (FSB4-3548-1)	WS-3548	12.0(5) WC15
Branch2 router (FSB4-3825-2)	3825 ISR	12.4(11)T2
Branch2 WAE (FSB4-ESE-WBE2)	NME-WAE-502	4.0.9 b10
Branch2 switch (FSB4-3560-1)	WS-3560	12.0(5) WC15

The WAEs and WAAS central manager were all synchronized to a common NTP server, set in this case to a router Campus 1. This could have easily been a separate server residing in the data center.

The WAN edge and branch routers were configured as customer premise equipment (CE) with a direct interface to the MPLS provider equipment (PE). DMVPN tunnels were created from each of the branch routers to the head-end router. The MPLS tunnel was created at the PE within the MPLS cloud.

Pageant (PMOD), a WAN simulator written for IOS, was used to create the WAN delay in this configuration. The WAN simulator was configured with an 60 millisecond delay and a 10 millisecond deviation. Because of background network traffic such as Cisco Discovery Protocol (CDP) and Intra Module Command Protocol (IMCP), as well as application traffic such as intermittent DNS and DHCP broadcasts, realistic delays ranged from 60 milliseconds +/- 10 milliseconds.

Appendix C—Test Bed Configuration

For relevancy to the branch, only the enterprise branch configurations are shown in this section. The IOS configurations for the data center portion of this test bed can be found in the Enterprise Data Center white paper, *Application Networking–Oracle E-Business Suite 11i.*

Branch1 Router (FSB4-3825-1)

```
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname FSB4-3825-1
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-11.T2.fc3
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 warnings
enable secret 5 $1$fMs6$xfGdok//2SiHau8QgcctX0
```

```
enable password 7 13061E010803
!
aaa new-model
!
!
aaa authentication login local_authen local
aaa authorization exec local_author local
!
!
aaa session-id common
clock timezone EST -5
no ip source-route
ip wccp 61
ip wccp 62
ip cef
ip tcp synwait-time 10
!
!
!
ip ftp username cisco
ip ftp password 7 094F471A1A0A
no ip bootp server
ip domain list eselab.com
no ip domain lookup
ip domain name eselab.com
ip name-server 192.168.1.5
ip inspect log drop-pkt
ip inspect WAAS enable
ip inspect dns-timeout 10
ip inspect tcp reassembly queue length 1024
ip inspect name in-out-pmap fragment maximum 1000 timeout 30
ip ips config location flash:/ipsstore/ retries 1
ip ips notify SDEE
ip ips name myips
!
ip ips signature-category
  category all
    retired true
  category ios_ips basic
    retired false
!
!
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
!
!
```

```
username esecisco privilege 15 password 7 070C285F4D06485744
!
!
class-map match-all branch-bulk-data
 match protocol ftp
 match access-group name bulk-data-apps
class-map match-all sql-slammer
 match packet length min 404 max 404
class-map match-all bulk-data
 match ip dscp af11  af12
class-map match-all interactive-video
 match ip dscp af41  af42
class-map match-any sdm_p2p_kazaa
 match protocol fasttrack
 match protocol kazaa2
class-map match-any call-signalling
 match ip dscp cs3
 match ip dscp af31
class-map match-any sdm_p2p_edonkey
 match protocol edonkey
class-map match-any sdm_p2p_gnutella
 match protocol gnutella
class-map match-any branch-scavenger
 match protocol napster
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map type inspect match-any most-traffic
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map match-all net-mgmg
 match ip dscp cs2
class-map match-any sdm_p2p_bittorrent
 match protocol bittorrent
class-map match-all transactional-data
 match ip dscp af21  af22
class-map match-any branch-transactional-data
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match protocol http url "*cisco.com"
 match protocol http url "*10.20.220.220*"
class-map match-all branch-mission-critical
 match access-group name mission-critical-servers
class-map match-any worms
 match protocol http url "*.ida*"
 match protocol http url "*cmd.exe*"
 match protocol http url "*root.exe*"
 match protocol http url "*readme.eml*"
 match class-map sql-slammer
 match protocol exchange
 match protocol netbios
class-map match-all voice
 match ip dscp ef
class-map match-all mission-critical-data
 match ip dscp 25
class-map match-any branch-net-mgmt
 match protocol snmp
 match protocol syslog
 match protocol telnet
 match protocol nfs
 match protocol dns
 match protocol icmp
```

```
 match protocol tftp
class-map match-all routing
 match ip dscp cs6
class-map match-all scavenger
 match ip dscp cs1
!
!
policy-map branch-lan-edge-in
 class sdm_p2p_edonkey
   drop
 class sdm_p2p_gnutella
   drop
 class sdm_p2p_kazaa
   drop
 class sdm_p2p_bittorrent
   drop
 class branch-mission-critical
 class branch-transactional-data
 class branch-net-mgmt
 class branch-bulk-data
  set dscp af31
 class branch-scavenger
 class worms
   drop
 class class-default
  set ip dscp default
policy-map type inspect out-in-pmap
 class type inspect most-traffic
  inspect
 class class-default
policy-map type inspect in-out-pmap
 class type inspect most-traffic
  inspect
 class class-default
policy-map branch-wan-edge
 class sdm_p2p_edonkey
   drop
 class sdm_p2p_gnutella
   drop
 class sdm_p2p_kazaa
   drop
 class sdm_p2p_bittorrent
   drop
 class voice
  priority percent 18
 class interactive-video
  priority percent 15
 class call-signalling
  bandwidth percent 5
 class routing
  bandwidth percent 3
 class net-mgmg
  bandwidth percent 2
 class mission-critical-data
  bandwidth percent 15
 class transactional-data
  bandwidth percent 12
 class bulk-data
  bandwidth percent 4
 class scavenger
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
```

```
!
zone security inside
zone security outside
zone-pair security in-out source inside destination outside
 service-policy type inspect in-out-pmap
zone-pair security out-in source outside destination inside
 service-policy type inspect out-in-pmap
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet0/0
 description ** WAN interface **$FW_OUTSIDE$
 ip address 192.168.20.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nbar protocol-discovery
 ip flow ingress
 ip ips myips in
 ip ips myips out
 zone-member security outside
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no mop enabled
 no clns route-cache
 max-reserved-bandwidth 100
 service-policy output branch-wan-edge
!
interface GigabitEthernet0/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache cef
 no ip route-cache
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no mop enabled
 no clns route-cache
 max-reserved-bandwidth 100
!
interface GigabitEthernet0/1.30
 description ** BRANCH DATA VLAN **$FW_INSIDE$
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip nbar protocol-discovery
 zone-member security inside
 no ip route-cache
 service-policy output branch-lan-edge-in
!
interface GigabitEthernet0/1.32
 description ** VOICE VLAN **$FW_INSIDE$
 encapsulation dot1Q 32
```

```
    ip address 192.168.32.1 255.255.255.0
   no ip redirects
   no ip unreachables
   no ip proxy-arp
   ip flow ingress
   zone-member security inside
   no ip route-cache
   no cdp enable
   service-policy output branch-lan-edge-in
  !
  interface GigabitEthernet0/1.33
   description ** BRANCH WAE VLAN **$FW_INSIDE$
   encapsulation dot1Q 33
   ip address 192.168.33.1 255.255.255.0
   no ip redirects
   no ip unreachables
   no ip proxy-arp
   ip wccp redirect exclude in
   ip flow ingress
   ip flow egress
   zone-member security inside
   no ip route-cache
   no cdp enable
  !
  interface Vlan1
   no ip address
   no ip redirects
   no ip unreachables
   no ip proxy-arp
   ip route-cache flow
  !
  router eigrp 1
   network 10.0.0.0
   network 192.168.0.0 0.0.255.255
   auto-summary
  !
  ip route 192.168.10.1 255.255.255.255 192.168.20.2
  !
  ip flow-export source GigabitEthernet0/1.30
  ip flow-export version 9 peer-as
  ip flow-export destination 192.168.1.4 335
  ip flow-top-talkers
   top 20
   sort-by bytes
  !
  ip http server
  ip http access-class 1
  ip http authentication local
  ip http secure-server
  !
  ip sla responder
  ip sla 10
   http get http://10.20.220.220:8081/Kelev/view/home.php
   frequency 300
  ip sla schedule 10 life forever start-time now
  no cdp run
  !
  control-plane
  !
  banner login ^CESE Branch 1 - FSB4-3825-1^C
  !
  line con 0
   exec-timeout 30 0
   login authentication local_authen
```

```
 transport output telnet
 stopbits 1
line aux 0
 login authentication local_authen
 transport output telnet
 stopbits 1
line vty 0 4
 access-class 100 in
 authorization exec local_author
 login authentication local_authen
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp clock-period 17180041
ntp server 10.99.1.1
!
end
```

Branch1 First WAE (FSB4-WBE1)

```
! WAAS version 4.0.9 (build b10 Apr  6 2007)
!
device mode application-accelerator
!
!
hostname FSB4-ESE-WBE1
!
!
clock timezone EST5EDT -4 0
!
!
ip domain-name ese-waas.cisco.com
!
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 description ** EDGE WAE1 INTERFACE **
 ip address 192.168.33.3 255.255.255.0
 exit
interface GigabitEthernet 2/0
 description ** FLASH MGT INTERFACE **
 ip address 172.26.186.236 255.255.255.0
 exit
!
!
!
ip default-gateway 192.168.33.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.1.5
!
!
!
ntp server 10.99.1.1
```

```
!
!
wccp router-list 1 192.168.33.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
! wccp slow-start is disabled in WAAS by default
!
!
!
username admin password 1 ofvZWyQ9EwDYY
username admin privilege 15
!
snmp-server community CLI_TRIGGER_4358 rw
!
!
!
windows-domain netbios-name "FSB4-ESE-WBE1"
!
authentication login local enable primary
authentication configuration local enable primary
!
inetd enable ftp
!
!
!
!
central-manager address 192.168.1.33
cms enable
!
! adapter epm is disabled by default
!
!
policy-engine application
    name Authentication
    name Backup
    name Call-Management
    name Conferencing
    name Console
    name Content-Management
    name Directory-Services
    name Email-and-Messaging
...etc...
```

Branch 1 Second WAE (FSB4-WBE3)

```
! WAAS version 4.0.9 (build b10 Apr  6 2007)
!
device mode application-accelerator
!
!
hostname FSB4-ESE-WBE3
!
!
clock timezone EST5EDT -4 0
!
!
ip domain-name ese-waas.cisco.com
!
!
!
primary-interface GigabitEthernet 1/0
```

```
!
!
!
interface GigabitEthernet 1/0
 description ** BRANCH 1 second WAE **
 ip address 192.168.33.5 255.255.255.0
 exit
interface GigabitEthernet 2/0
 description ** FLASH MGT INTERFACE **
 ip address 172.26.186.233 255.255.255.0
 exit
!
!
!
ip default-gateway 192.168.33.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 192.168.1.5
!
!
!
ntp server 10.99.1.1
ntp server 172.26.186.1
!
!
wccp router-list 1 192.168.33.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
! wccp slow-start is disabled in WAAS by default
!
!
!
username admin password 1 K9vPF0Kd9loVo
username admin privilege 15
username admin print-admin-password 1 A00B9194BEDB81FEAAD3B435B51404EE 5C800F13A
3CE86ED2540DD4E7331E9A2
!
!
!
!
windows-domain netbios-name "FSB4-ESE-WBE3"
!
authentication login local enable primary
authentication configuration local enable primary
!
inetd enable ftp
!
!
!
!
central-manager address 192.168.1.33
cms enable
!
!
! adapter epm is disabled by default
!
!
policy-engine application
   name SQL
   name File-System
   name Systems-Management
```

```
    name Console
    name Remote-Desktop
    name Directory-Services
    name Conferencing
    name Version-Management
    name P2P
    name WAFS
...etc...
```

Branch 1 Switch (FSB4-3548-1)

```
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname FSB4-3548-2
!
enable password cisco
!
!
!
!
!
!
ip subnet-zero
ip domain-name ese-waas.cisco.com
!
!
!
interface FastEthernet0/1
 description ** TO BRANCH ROUTER **
 duplex full
 speed 100
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,30-33,1002-1005
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
!
interface FastEthernet0/3
 switchport access vlan 30
!
interface FastEthernet0/4
 switchport access vlan 30
!
interface FastEthernet0/5
 switchport access vlan 30
!
interface FastEthernet0/6
 switchport access vlan 30
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
```

```
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
!
interface FastEthernet0/11
 description ** BRANCH WAE **
 switchport access vlan 33
!
!
...etc...
!
!
interface FastEthernet0/20
 description ** Voice VLAN **
 switchport access vlan 32
!
interface FastEthernet0/21
 switchport access vlan 32
!
interface FastEthernet0/22
 switchport access vlan 32
!
...etc...
!
!
interface GigabitEthernet0/1
 description ** BRANCH1 INTERNAL NETWORK **
!
interface GigabitEthernet0/2
 description ** TO FLASH NETWORK **
!
interface VLAN1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN30
 description ** BRANCH DATA VLAN **
 ip address 192.168.30.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
interface VLAN32
 description ** BRANCH VOICE VLAN **
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN33
 description ** BRANCH WAE VLAN **
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN41
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN186
 ip address 172.26.186.229 255.255.255.0
 no ip directed-broadcast
```

```
 no ip route-cache
 shutdown
!
ip default-gateway 192.168.30.1
no ip http server
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

Branch 2 Router

```
!
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname FSB4-3825-2
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-11.T2.fc3
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 notifications
logging console critical
enable secret 5 $1$9Ni3$JIT8f6.Ht7ezCzUpb5wi7/
enable password 7 0822455D0A49
!
aaa new-model
!
!
aaa authentication login local_authen local
aaa authorization exec local_author local
!
!
aaa session-id common
clock timezone EST -5
no network-clock-participate wic 0
no ip gratuitous-arps
ip wccp 61
ip wccp 62
ip cef
ip tcp synwait-time 10
!
!
!
!
no ip bootp server
ip domain name ese-waas.cisco.com
```

```
ip name-server 192.168.1.5
ip inspect log drop-pkt
ip inspect WAAS enable
ip ips config location flash:ipsstore/ retries 1
ip ips notify SDEE
ip ips name myips
!
ip ips signature-category
  category all
    retired true
  category ios_ips basic
    retired false
!
!
multilink bundle-name authenticated
!
isdn switch-type primary-5ess
voice-card 0
 no dspfarm
!
!
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
!
!
username esecisco privilege 15 secret 5 $1$k1VO$45bvlKt0.oc7ykoOn7OjG1
!
!
controller T1 0/0/0
 framing esf
 linecode b8zs
!
controller T1 0/0/1
 framing esf
 linecode b8zs
!
class-map match-all branch-bulk-data
 match access-group name bulk-data-apps
class-map match-all sql-slammer
 match packet length min 404 max 404
class-map match-all bulk-data
 match ip dscp af11  af12
class-map match-all interactive-video
 match ip dscp af41  af42
class-map match-any call-signalling
 match ip dscp cs3
 match ip dscp af31
class-map match-any branch-scavenger
 match protocol napster
 match protocol gnutella
 match protocol fasttrack
```

```
 match protocol kazaa2
class-map type inspect match-any most-traffic
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map match-all net-mgmg
 match ip dscp cs2
class-map match-all transactional-data
 match ip dscp af21   af22
class-map match-any branch-transactional-data
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match protocol http url "*cisco.com"
 match protocol http url "*ese-waas.cisco.com"
class-map match-any branch-mission-critical
 match access-group name mission-critical-servers
class-map match-any worms
 match protocol http url "*.ida*"
 match protocol http url "*cmd.exe*"
 match protocol http url "*root.exe*"
 match protocol http url "*readme.eml*"
 match class-map sql-slammer
 match protocol exchange
 match protocol netbios
class-map match-all voice
 match ip dscp ef
class-map match-all mission-critical-data
 match ip dscp 25
class-map match-any branch-net-mgmt
 match protocol snmp
 match protocol syslog
 match protocol telnet
 match protocol nfs
 match protocol dns
 match protocol icmp
 match protocol tftp
class-map match-all routing
 match ip dscp cs6
class-map match-all scavenger
 match ip dscp cs1
!
!
policy-map branch-lan-edge-out
 class class-default
  set cos dscp
policy-map branch-lan-edge-in
 class branch-mission-critical
  set ip dscp 25
 class branch-transactional-data
  set ip dscp af21
 class branch-net-mgmt
  set ip dscp cs2
 class branch-bulk-data
  set ip dscp af11
 class branch-scavenger
  set ip dscp cs1
 class worms
   drop
 class class-default
  set ip dscp default
policy-map type inspect out-in-pmap
 class type inspect most-traffic
  inspect
```

```
        class class-default
       policy-map type inspect in-out-pmap
        class type inspect most-traffic
         inspect
        class class-default
       policy-map branch-wan-edge
        class voice
         priority percent 18
        class interactive-video
         priority percent 15
        class call-signalling
         bandwidth percent 5
        class routing
         bandwidth percent 3
        class net-mgmg
         bandwidth percent 2
        class mission-critical-data
         bandwidth percent 15
        class transactional-data
         bandwidth percent 12
         random-detect dscp-based
        class bulk-data
         bandwidth percent 4
         random-detect dscp-based
        class scavenger
         bandwidth percent 1
        class class-default
         bandwidth percent 25
         random-detect
       !
       zone security inside
       zone security outside
       zone-pair security out-in source outside destination inside
        service-policy type inspect out-in-pmap
       zone-pair security in-out source inside destination outside
        service-policy type inspect in-out-pmap
       !
       !
       interface Null0
        no ip unreachables
       !
       interface GigabitEthernet0/0
        description ** WAN interface **$FW_OUTSIDE$
        ip address 192.168.21.1 255.255.255.0
        ip verify unicast reverse-path
        no ip redirects
        no ip unreachables
        no ip proxy-arp
        ip nbar protocol-discovery
        ip flow ingress
        ip flow egress
        ip ips myips in
        zone-member security outside
        ip route-cache flow
        duplex auto
        speed auto
        media-type rj45
        analysis-module monitoring
        no keepalive
        no mop enabled
        max-reserved-bandwidth 100
        service-policy output branch-wan-edge
       !
       interface GigabitEthernet0/1
```

```
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 zone-member security inside
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no keepalive
 no mop enabled
 no clns route-cache
 max-reserved-bandwidth 100
 service-policy input branch-lan-edge-in
!
interface GigabitEthernet0/1.40
 description ** BRANCH2 DATA CLIENTS **$FW_INSIDE$
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip nbar protocol-discovery
 ip flow ingress
 zone-member security inside
 analysis-module monitoring
 service-policy input branch-lan-edge-in
!
interface GigabitEthernet0/1.41
 description ** NAM MODULE **
 encapsulation dot1Q 41
 no ip redirects
 no ip unreachables
 no ip proxy-arp
zone-member security inside
!
interface GigabitEthernet0/1.43
 description ** WAAS MODULE **
 encapsulation dot1Q 43
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip wccp redirect exclude in
 ip flow ingress
 ip flow egress
 zone-member security inside
!
interface FastEthernet0/1/0
 shutdown
!
interface FastEthernet0/1/1
 shutdown
!
interface FastEthernet0/1/2
 shutdown
!
interface FastEthernet0/1/3
 shutdown
!
interface Analysis-Module1/0
 description ** NAM MODULE **
```

```
       ip address 192.168.41.2 255.255.255.0
       no ip redirects
       no ip unreachables
       no ip proxy-arp
       ip nbar protocol-discovery
       zone-member security inside
       ip route-cache flow
       hold-queue 60 out
      !
      interface Integrated-Service-Engine2/0
       description ** WAAS BRYCE MODULE **
       ip address 192.168.43.1 255.255.255.0
       no ip redirects
       no ip unreachables
       no ip proxy-arp
       ip wccp redirect exclude in
       ip nbar protocol-discovery
       zone-member security inside
       ip route-cache flow
       service-module ip address 192.168.43.3 255.255.255.0
       service-module ip default-gateway 192.168.43.1
       no keepalive
      !
      interface Vlan1
       no ip address
       no ip redirects
       no ip unreachables
       no ip proxy-arp
       ip nbar protocol-discovery
       ip route-cache flow
       no mop enabled
      !
      router eigrp 1
       network 10.0.0.0
       network 192.168.0.0 0.0.255.255
       auto-summary
      !
      ip route 192.168.10.1 255.255.255.255 192.168.21.2
      ip route 192.168.41.20 255.255.255.255 Analysis-Module1/0
      ip route 192.168.43.3 255.255.255.255 Integrated-Service-Engine2/0
      !
      ip flow-cache timeout active 60
      ip flow-top-talkers
       top 10
       sort-by bytes
      !
      ip http server
      ip http authentication local
      ip http secure-server
      ip http timeout-policy idle 600 life 86400 requests 10000
      !
      logging trap debugging
      logging 192.168.40.11
      snmp-server community public RO
      snmp-server community private RW
      !
      !
      !
      control-plane
      !
      !
      !
      banner login ^CCisco Systems Branch 2 ISR FSB4-3825-2^C
      !
```

```
line con 0
 transport output all
 stopbits 1
line aux 0
 transport output none
 stopbits 1
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output all
line 130
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output all
line vty 0 4
 transport input all
 transport output all
!
scheduler allocate 20000 1000
!
end
```

Branch 2 Edge WAE

```
! WAAS version 4.0.2 (build b170 Sep 27 2006)
!
!
hostname FSB4-ESE-WBE2
!
!
clock timezone EST -5 0
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 ip address 192.168.43.3 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
ip default-gateway 192.168.43.1
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
!
ntp server 192.168.1.1
!
!
wccp router-list 1 192.168.43.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
```

```
! wccp slow-start is disabled in WAAS by default
!
!
!
username admin password 1 K9vPF0Kd9loVo
username admin privilege 15
username admin print-admin-password 1 A00B9194BEDB81FEAAD3B435B51404EE
5C800F13A3CE86ED2540DD4E7331E9A2
!
!
!
!
windows-domain netbios-name "FSB4-ESE-WBE2"
!
authentication login local enable primary
authentication configuration local enable primary
!
inetd enable ftp
!
!
!
!
central-manager address 192.168.1.33
cms enable
!
!
!
!
!
policy-engine application
   name Authentication
   name Backup
   name Call-Management
   name Conferencing
   name Console
   name Content-Management
   name Directory-Services
   name Email-and-Messaging
   name Enterprise-Applications
   name File-System
   name File-Transfer
   name Instant-Messaging
   name Name-Services
   name Network-Analysis
   name P2P
   name Printing
   name Remote-Desktop
   name Replication
   name SQL
   name SSH
   name Storage
   name Streaming
...etc...
```

Appendix D—Additional References

- Application Networking–Oracle E-Business Suite 11i—
  http://www.cisco.com/en/US/solutions/ns340/ns629/net_sol_design_guidance_sona_ap_ntwk_opt_oracle_ebiz_suite.html

- Enterprise Data Center Wide Area Application Services—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/WAASDC11.html

- Enterprise Branch Architecture Design Overview—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/EnBrOver.html

- Enterprise Branch Security Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html

- Enterprise QoS Solution Network Reference Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND
-Book.html

- WAAS 4.0 Technical Overview—
http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml

- Cisco 3800 Series Integrated Services Router Data Sheet—
http://www.cisco.com/en/US/products/ps5855/products_data_sheet0900aecd8016a8e8.html

- Cisco Wide Area Application Services Configuration Guide, Software Version 4.01—
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/quick/guide/waasqcg.htm
l

- Cisco white paper, "Accelerating Application Response Times in Branch Offices",
http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051c07f.shtml

- "Deploying Zone-based Firewalls", Ivan Pepelnjak, Cisco Press, 2006.

- IP SLA Configuration Guide:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080
441596.html

- Networker 2006 APP-1101 Presentation, "Introduction to Application Acceleration Technologies"

- Unified Communications SRND using CallManager 5.0—
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide
_chapter09186a0080637440.html.