Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-125

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

SBA

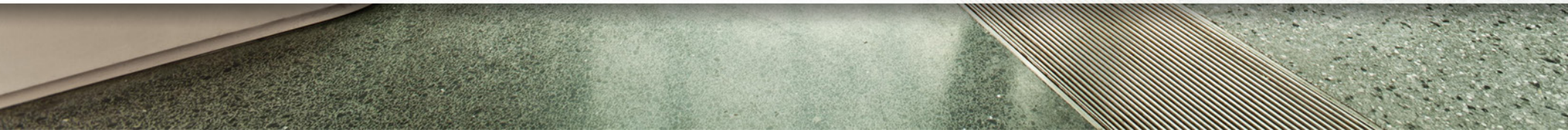
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Application Optimization Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series



Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

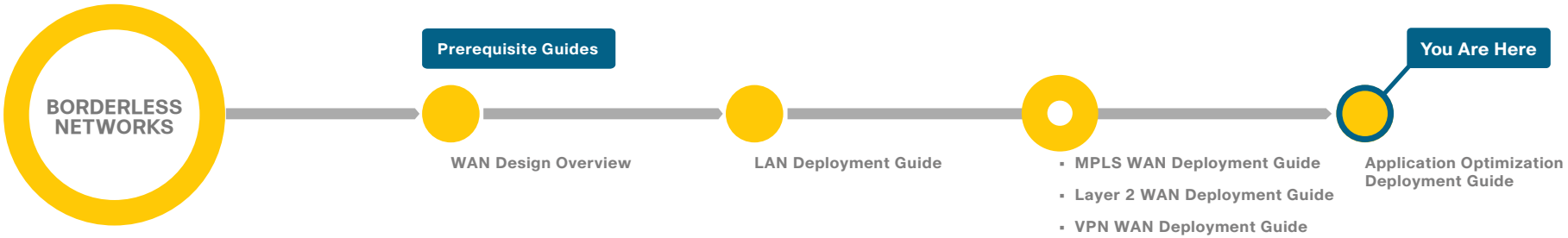
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

Business Overview

The number of remote work sites is increasing, so network administrators need tools to help them ensure solid application performance in remote locations. Recent trends show that a majority of new hires are located at remote sites. These trends are tied to global expansion, employee attraction and retention, mergers and acquisitions, cost savings, and environmental concerns.

In the meantime, remote-site communications requirements are evolving to embrace collaborative applications, video, and Web 2.0 technologies. These developments are also placing greater performance demands on the remote sites and the WAN.

The enterprise trend toward data-center consolidation also continues. The consolidation efforts move most remote-site assets into data centers, largely to comply with regulatory mandates for centralized security and stronger control over corporate data assets.

Consolidating data centers while growing the remote-site population means that increasing numbers of remote employees access LAN-based business applications across comparatively slow WANs. With these applications growing increasingly multimedia-centric and latency-sensitive, IT and networking staffs are further challenged to keep remote-application response times on par with the experiences of users situated locally to the company's application servers in the data center. These local users enjoy multimegabit LAN speeds and are not affected by any distance-induced delay, unlike their counterparts at the other end of a WAN connection.

Application optimization can boost network performance along with enhancing security and improving application delivery. Cisco WAN Optimization is an architectural solution comprising a set of tools and techniques that work together in a strategic systems approach to provide best-in-class WAN optimization performance while minimizing its total cost of ownership.

Technology Overview

Cisco WAAS Central Manager

Every Cisco Wide Area Application Services (Cisco WAAS) network must have one primary Cisco WAAS Central Manager device that is responsible for managing the other WAAS devices in the network. The WAAS Central Manager devices host the WAAS Central Manager GUI, a web-based interface that allows you to configure, manage, and monitor the WAAS devices in your network. The WAAS Central Manager resides on a dedicated Cisco Wide Area Virtualization Engine (Cisco WAVE) device.

Details on the Cisco WAVE sizing is provided in the following table.

Table 1 - Cisco WAAS Central Manager sizing options

Device	Number of managed devices (Cisco WAAS and Cisco WAAS Express)
WAVE-294-4GB	250
WAVE-594-8GB	1000
WAVE-694-16GB	2000
vCM-100N	100
vCM-2000N	2000

WAN Aggregation

The WAN-aggregation site uses a cluster of two or more Cisco WAVE devices to provide Cisco WAAS capabilities. The WAVE appliances connect to the distribution-layer switch. The connections use EtherChannel both for increased throughput and for resiliency. *EtherChannel* is a logical interface that bundles multiple physical LAN links into a single logical link. The WAVE appliances connect to the WAN services network that is configured on the distribution switch.

The total number of devices required is a minimum of two (for N+1 redundancy). The following table provides details on the Cisco WAVE sizing. The fan-out numbers correspond to the total number of remote-peer WAVE devices.

Table 2 - WAN-aggregation Cisco WAVE options

Device	Max optimized TCP connections	Max recommended WAN link [Mbps]	Max optimized throughput [Mbps]	Max core fan-out [Peers]
WAVE-594-8GB	750	50	250	50
WAVE-594-12GB	1300	100	300	100
WAVE-694-16GB	2500	200	450	150
WAVE-694-24GB	6000	200	500	300
WAVE-7541	18000	500	1000	700
WAVE-7571	60000	1000	2000	1400
WAVE-8541	150000	2000	4000	2800

A more comprehensive, interactive Cisco WAAS sizing tool is available for registered users of cisco.com:

http://tools.cisco.com/WAAS/sizing

The Web Cache Communication Protocol (WCCP) is a protocol developed by Cisco. Its purpose is to transparently intercept and redirect traffic from a network device to a WCCP appliance such as a Cisco WAVE appliance running Cisco WAAS.

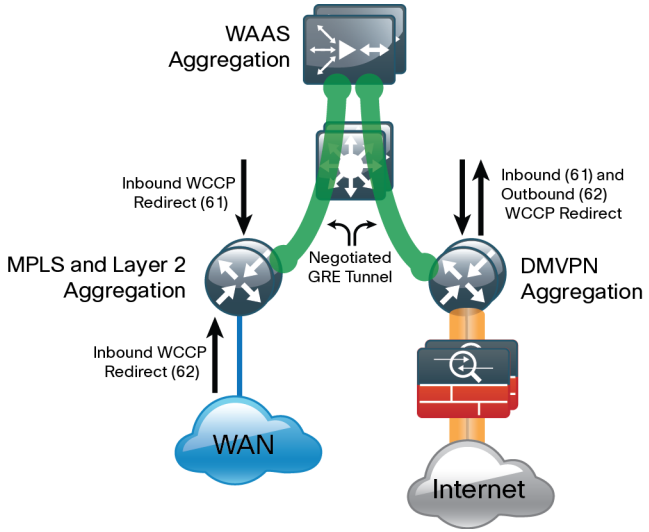
WCCP is enabled on the Multiprotocol Label Switching (MPLS) CE and Dynamic Multipoint VPN (DMVPN) routers. The WCCP redirect uses service groups 61 and 62 in order to match traffic for redirection. These service groups must be used in pairs:

- Service group 61 uses the source address to redirect traffic
- Service group 62 uses the destination address to redirect traffic

This design uses WCCP 61 inbound on LAN-facing interfaces in order to match unoptimized data sourced from the data center that is destined for clients at the WAN remote sites. WCCP 62 is used inbound on WAN-facing interfaces, matching optimized data sourced from the WAN remote sites. WCCP 62 is used outbound on LAN interfaces for DMVPN hub routers.

The connections from the distribution switch to the WAN aggregation routers are routed point-to-point links. This design mandates the use of a negotiated-return generic routing encapsulation (GRE) tunnel from Cisco WAVE to router. When a design uses a GRE negotiated return, it is not required that the Cisco WAVE appliances and the WAN aggregation routers are Layer 2 adjacent.

Figure 1 - WAN aggregation—Cisco WAAS topology



Remote Sites

The WAN optimization design for the remote sites can vary somewhat based on site-specific characteristics. Single router sites use a single (nonredundant) Cisco WAVE appliance. Similarly, all dual-router sites use dual WAVE appliances. The specifics of the WAVE sizing and form factor primarily depend on the number of end users and bandwidth of the WAN links. Low bandwidth (< 2 Mbps) single-router, single-link sites can also use the embedded Cisco WAAS Express (WAASx) capability of the router.

There are many factors to consider in the selection of the WAN remote-site WAN optimization platform. The primary parameter of interest is the bandwidth of the WAN link. After the bandwidth requirement has been met, the next item under consideration is the maximum number of concurrent, optimized TCP connections. Additional detail on the Cisco WAVE sizing is provided in the following table. The optimized throughput numbers correspond to the apparent bandwidth available after successful optimization by Cisco WAAS.

Table 3 - WAN remote-site Cisco WAVE options

Device	Max optimized TCP connections	Max recommended WAN link [Mbps]	Max optimized throughput [Mbps]
Cisco1941/WAASx[1]	150	4	8
SRE-710-S	200	20	200
SRE-710-M	500	20	500
SRE-910-S	200	50	200
SRE-910-M	500	50	500
SRE-910-L	1000	50	1000
WAVE-294-4GB	200	10	100
WAVE-294-8GB	400	20	150
WAVE-594-8GB	750	50	250
WAVE-594-12GB	1300	100	300
WAVE-694-16GB	2500	200	450
WAVE-694-24GB	6000	200	500

Notes:

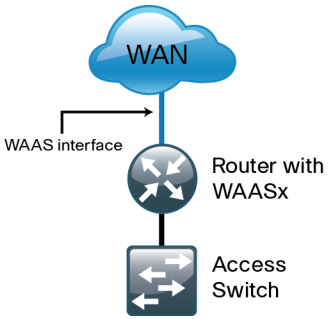
1. Single-link design only

A more comprehensive, interactive WAAS sizing tool is available for registered users of cisco.com:

http://tools.cisco.com/WAAS/sizing

The embedded Cisco WAASx provides a subset of the full set of WAAS capabilities available on the Cisco WAVE platforms. The current WAASx software release is compatible with single-link WAN designs, cost-effective, and easy to deploy. No design or architecture changes are required to enable this functionality on the router.

Figure 2 - WAN remote-site—Cisco WAASx topology



The Cisco WAVE form factors previously discussed include a Cisco Services-Ready Engine (SRE) router module and an external appliance. These variants all run the same WAAS software and are functionally equivalent. The primary difference is the method of LAN attachment for these devices:

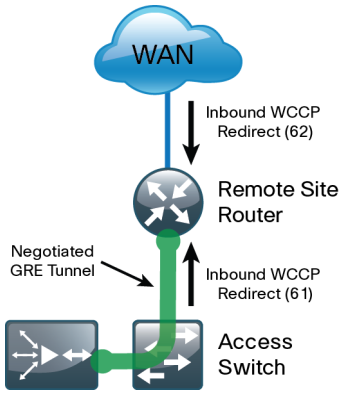
- **SRE module**—One internal interface (router-connected only), one external interface
- **Appliance**—Two interfaces (both external)

The approach for connecting the Cisco WAVE devices to the LAN is to be consistent regardless of the chosen hardware form-factor. All WAVE connections are made using the external interfaces. The benefit of this method is that it is not necessary to create a dedicated network specifically to attach the WAVE devices, and the Cisco SRE module and appliance devices can use an identical design. The internal interface of the SRE module is not used for this design, except for the initial bootstrapping of the device configurations.

You must connect an external Ethernet cable from each Cisco SRE module for this solution.

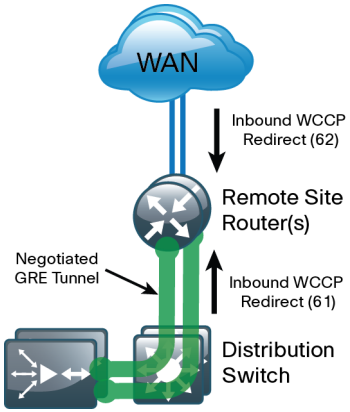
You should connect the Cisco WAVE devices to the data VLAN of the access switch in all flat Layer 2 designs.

Figure 3 - WAN remote-site—Cisco WAAS topology (access-layer connection)



When the deployment uses a distribution-layer design, the Cisco WAVE devices should connect to the primary data VLAN on the distribution switch.

Figure 4 - WAN remote-site—Cisco WAAS topology (distribution-layer connection)



Where possible, connect the Cisco WAVE appliances through both interfaces by using EtherChannel for performance and resiliency.

WCCP Version 2 is enabled on the WAN routers to redirect traffic to the WAAS appliances.

The WCCP redirect uses service groups 61 and 62 to match traffic for redirection. These services groups must be used in pairs:

- Service group 61 uses the source address to redirect traffic
- Service group 62 uses the destination address to redirect traffic

This design uses WCCP 61 inbound on LAN-facing VLAN subinterfaces in order to match unoptimized data sourced from the clients and destined for the data center (or other remote sites). In all cases, WCCP 62 is used inbound on WAN-facing interfaces in order to match optimized data sourced from the data center (or other remote sites).

Because the Cisco WAVE appliance is connected to the data VLAN, this design requires the use of a negotiated-return GRE tunnel from the WAVE appliances to the router. When using a GRE-negotiated return, you are not required to create a new network on the routers specifically to attach the WAVE appliances.

Deployment Details

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within this solution. These parameters are listed in the following table. For your convenience, you can enter your values in the table and refer to it when configuring the appliance.

Table 4 - Universal design parameters

Network service	Cisco SBA values	Site-specific values
Domain name	cisco.local	
Active Directory, DNS server, DHCP server	10.4.48.10	
Cisco Secure ACS (Optional)	10.4.48.15	
Network Time Protocol (NTP) server	10.4.48.17	
SNMP read-only community	cisco	
SNMP read-write community	cisco123	

Process

Configuring the Cisco WAAS Central Manager

1. Configure switch for Central Manager
2. Install the vWAAS virtual machine
3. Configure the WAAS Central Manager
4. Enable centralized AAA

Configuration Checklist

The following table specifies the parameters and data, in addition to the universal design parameters that you need in order to set up and configure the Cisco WAAS Central Manager. For your convenience, you can enter your values in the table and refer to it when configuring the appliance. The values you enter will differ from those in this example, which are provided for demonstration purposes only.

Table 5 - Cisco WAAS Central Manager network parameters

Parameter	Cisco SBA values	Site-specific values
Switch interface number	1/0/10	
VLAN number	148	
Time zone	PST8PDT -7 0	
IP address	10.4.48.100/24	
Default gateway	10.4.48.1	
Host name	waas-wcm-1	
Management network (optional)	10.4.48.0/24	
TACACS shared key (optional)	SecretKey	

Procedure 1 Configure switch for Central Manager

This guide assumes that the switches have already been configured. The following steps contain only the information required to complete the connection of the switch to the Cisco WAVE appliances. For full details on switch configuration, see *Cisco SBA —Server Room Deployment Guide* or *Cisco SBA —Data Center Deployment Guide*.

If you are configuring a Cisco Catalyst server room switch, complete Option 1. If you are configuring a Cisco Nexus data center switch, complete Option 2.

Option 1. Configure the server room switch

Step 1: Connect the Cisco WAVE appliance's external Ethernet port to an Ethernet port on the switch, and then return the switchport configuration to the default.

```
default interface GigabitEthernet1/0/10
```

Step 2: Define the switchport as an access port, and then apply quality-of-service (QoS) configuration.

```
interface GigabitEthernet1/0/10
 description Link to WAAS-CM
 switchport access vlan 148
 switchport host
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

Option 2. Configure the data center switch

Step 1: Connect the single-homed appliance to a dual-homed Cisco Fabric Extender (FEX), Define the switchport as an access port, and then apply quality-of-service (QoS) configuration.

```
interface Ethernet102/1/1
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Tech Tip

You must assign the Ethernet interface configuration on both data center core Cisco Nexus 5500UP switches as the appliance is dual-homed because it is on a dual-homed Cisco FEX.

Procedure 2 Install the vWAAS virtual machine

This procedure is only required if you are using a Cisco Virtual WAAS (Cisco vWAAS) virtual machine.

Cisco vWAAS is provided as an open virtual appliance (OVA). The OVA is prepackaged with disk, memory, CPU, network interface cards (NICs), and other virtual-machine-related configuration parameters. This is an industry standard, and many virtual appliances are available in this format. Cisco provides a different OVA file for each vWAAS model.

Tech Tip

The OVA files are available only in DVD media format and are not available for download on www.cisco.com at this time.

Step 1: Deploy the OVF template with the VMware vSphere client.

Step 2: Before you configure Cisco vWAAS, using VMware vSphere, install the vWAAS OVA on the VMware ESX/ESXi server.

Step 3: In the VMware console, configure the Cisco vWAAS.

The procedures and steps for configuring the Cisco vWAAS Central Manager and vWAAS Application Accelerator devices are identical to those for the Cisco WAVE appliance and Cisco SRE form factors. Apply the following procedure to complete the vWAAS configuration.

Procedure 3 Configure the WAAS Central Manager

Use a Cisco WAVE-594 or WAVE-294 device for the Cisco WAAS Central Manager function at the primary location in order to provide graphical management, configuration, and reporting for the Cisco WAAS network. This device resides in the server farm because it is not directly in the forwarding path of the WAN optimization, but it provides management and monitoring services. In order to initially configure the WAAS Central Manager, you must have terminal access to the console port for basic configuration options and IP address assignment. For all Cisco WAVE devices, the factory default

username is admin and the factory default password is default.

Step 1: From the command line, enter **setup**. The initial setup utility starts.

```
    Parameter                 Default Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 1/0
 5. Autosense                 Enabled
 6. DHCP                      Enabled
ESC Quit ? Help ———————— WAAS Default Configuration
————————————

Press 'y' to select above defaults, 'n' to configure all, <1-
6> to change specific default [y]: n
```

Step 2: Enter option **2** to configure as **Central Manager**.

```
1. Application Accelerator
2. Central Manager
Select device mode [1]: 2
```

Step 3: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST8PDT -7 0
```

Step 4: Configure the management interface, IP address, and default gateway.

```
No.      Interface Name      IP Address    Network Mask
1.       GigabitEthernet         1/0            dhcp
2.       GigabitEthernet         2/0            dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.4.48.100/24
Enter Default Gateway IP Address [Not configured]: 10.4.48.1
```

Step 5: Configure the Domain Name System (DNS), host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAAS-WCM-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

Step 6: Select the appropriate license.

```
The product supports the following licenses:
1. Enterprise
Enter the license(s) you purchased [1]: 1
```

Step 7: Verify the configuration settings, and then initiate reload.

```
   Parameter                 Configured Value
 1. Device Mode               Central Manager
 2. Time Zone                 PST8PDT -7 0
 3. Management Interface      GigabitEthernet 1/0
 4. Autosense                 Enabled
 5. DHCP                      Disabled
 6. IP Address                10.4.48.100
 7. IP Network Mask           255.255.255.0
 8. IP Default Gateway        10.4.48.1
 9. DNS IP Address            10.4.48.10
10. Domain Name(s)            cisco.local
11. Host Name                 WAAS-WCM-1
12. NTP Server Address        10.4.48.17
13. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration
————————————
```

```
Press 'y' to select configuration, 'd' to toggle defaults
display, <1-13> to change specific parameter [y]: y
Apply WAAS Configuration: Device Mode changed in SETUP; New
configuration takes effect after a reload. If applicable,
registration with CM, CM IP address, WAAS WCCP configuration
etc, are applied after the reboot. Initiate system reload?
<y/n> [n] y
Are you sure? <y/n> [n]: y
```

Next, you will configure the device management protocols.

Step 8: Reboot, and then log in to the Cisco WAAS Central Manager.

Step 9: Generate the RSA key, and then enable the sshd service. This enables Secure Shell Protocol (SSH).

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
no telnet enable
```

Step 10: Enable Simple Network Management Protocol (SNMP), which allows the network infrastructure devices to be managed by a Network Management System (NMS), and then configure SNMPv2c for a read-only and a read-write community string.

```
snmp-server community cisco
snmp-server community cisco123 RW
```

Step 11: If you want to limit access to the appliance, configure management access control lists (ACLs).

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
interface GigabitEthernet 1/0
 ip access-group 155 in
 !
ip access-list standard  55
 permit 10.4.48.0 0.0.0.255
 exit
snmp-server access-list 55
```

Step 12: After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Step 13: Reboot. The Cisco WAAS Central Manager device should be up and running after the reload completes, and it should be accessible to a web browser at the IP address assigned during setup or at the associated host name if it has been configured in DNS.

Procedure 4 Enable centralized AAA

(Optional)

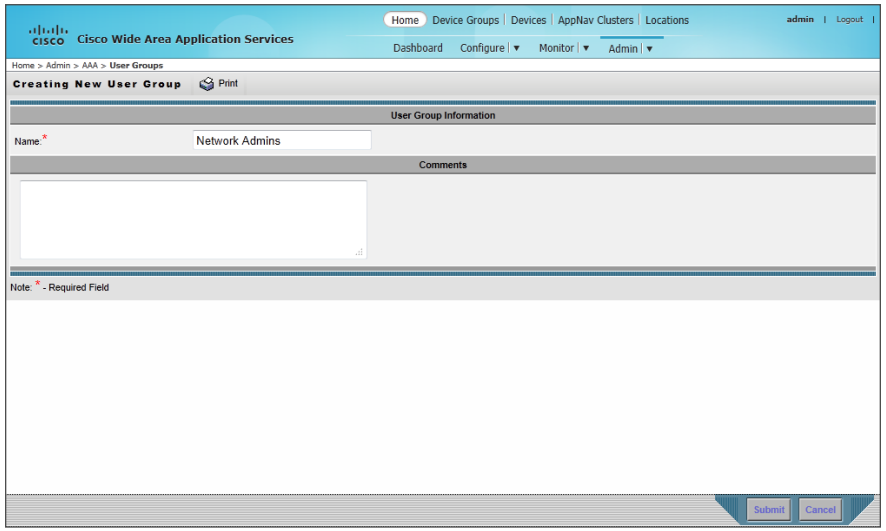
This guide assumes that Cisco Secure Access Control System (Cisco Secure ACS) has already been configured. Only the procedures required to support the integration of Cisco WAAS into the deployment are included. For details on how to configure Cisco Secure ACS, see the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

Step 1: Log in to the Cisco WAAS Central Manager through the web interface (for example, https://waas-wcm-1.cisco.local:8443) by using the default user name of **admin** and password of **default**.

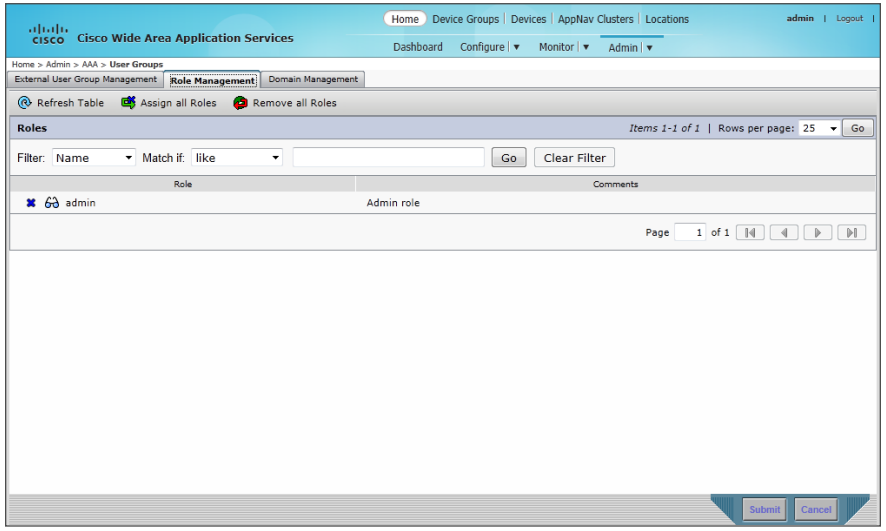
Next, you will configure the Network-Admins user group. The web interface for the Cisco WAAS Central Manager requires a user group with the proper role assigned in order to authorize users from an external authentication, authorization, and accounting (AAA) database. This step must be completed before enabling AAA and can only be performed by using the web interface.

Step 2: In **Admin > AAA > User Groups,** click **Create**.

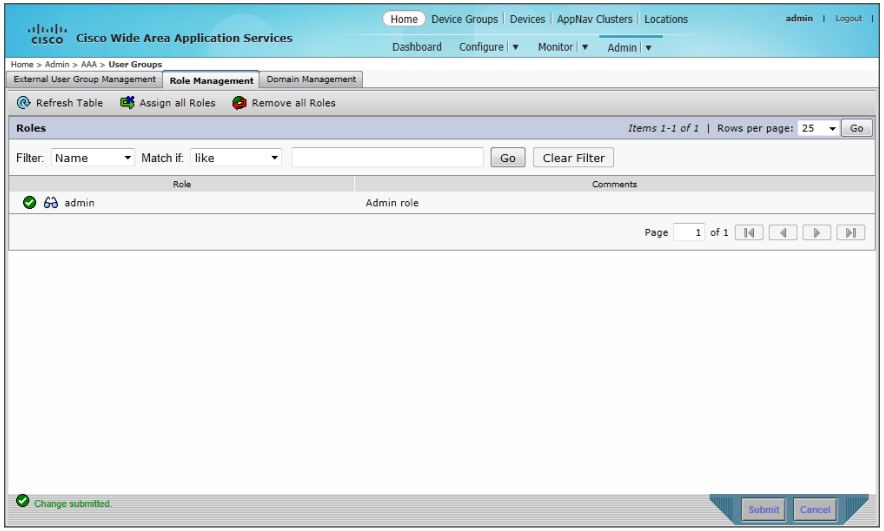
Step 3: In the **Name** box, enter a name. This name must match exactly (case sensitive) the group name used on the AAA server. For example, "Network Admins" in this implementation.



Step 4: After you create the group, click the **Role Management** tab, click the **X** to assign the role, and then click **Submit**.



After you properly assign the role, a large, green check mark appears next to the icon.



Next, you will configure secure user authentication. AAA controls all management access to the Cisco WAAS and Cisco WAVE devices (SSH and HTTPS).

A local admin user was created on the Cisco WAAS and Cisco WAVE appliances during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or in case you do not have a TACACS+ server in your organization.

Tech Tip

The AAA configuration details shown are for the Cisco WAAS devices only. Additional configuration is required on the AAA server for successful user authorization. Do not proceed with configuring secure user authentication until you have completed the relevant steps in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

Step 5: From the command-line interface, using SSH, log in to the Cisco WAAS Central Manager by using the default user name of **admin** and password of **default**.

Step 6: Enable AAA authentication for access control. The following configures TACACS+ as the primary method for user authentication (login) and user authorization (configuration).

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 7: After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Process

Configuring the Cisco WAVE Appliance

1. Configure switch for WAVE appliances
2. Configure the Cisco WAVE appliance
3. Configure WCCPv2 on routers

Configuration Checklist

The following table specifies the parameters and data, in addition to the universal design parameters, that you need in order to set up and configure the Cisco WAAS network. For your convenience, you can enter your values in the table and refer to it when configuring the WAAS network. The values you enter will differ from those in this example, which are provided for demonstration purposes only.

Table 6 - Cisco WAAS using Cisco WAVE Appliance network parameters

Parameter	Cisco SBA values primary WAVE	Cisco SBA values secondary WAVE	Site-specific values
Switch interface Numbers	1/0/2 2/0/2	1/0/2 2/0/2	
VLAN number	350	350	
VLAN name (optional)	WAN_Service_Net	WAN_Service_Net	
Time zone	PST8PDT -7 0	PST8PDT -7 0	
IP address	10.4.32.161/26	10.4.32.162/26	
Default gateway	10.4.32.129/26	10.4.32.129/26	
WAAS Central Manager	10.4.48.100	10.4.48.100	
Hostname	WAVE-1	WAVE-2	
IP addresses of routers intercepting traffic with WCCP	10.4.32.241 10.4.32.242 10.4.32.243	10.4.32.241 10.4.32.242 10.4.32.243	
WCCP password	c1sco123	c1sco123	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS shared key (optional)	SecretKey	SecretKey	

Procedure 1 Configure switch for WAVE appliances

There are three options for where to connect Cisco WAVE appliances. The distribution switch is the appropriate location to physically connect WAVE appliances at the WAN-aggregation site and two-tier remote sites. The access switch is the appropriate location to physically connect WAVE appliances at single-tier remote sites.

- Distribution-layer switch—This device type requires a resilient connection but does not require a routing protocol. This type of connection can use a Layer 2 EtherChannel link.
- Remote-site access-layer switch stack or modular switch—This type of connection can use a Layer 2 EtherChannel link.
- Remote-site access-layer switch—This type of connection can use a Layer 2 access interface.

This guide assumes that the switches have already been configured, so it includes only the procedures required to complete the connection of the switch to the Cisco WAVE appliances. For details on how to configure a distribution-layer switch, see *Cisco SBA—Borderless Networks LAN Deployment Guide*.

If you are connecting a Cisco Catalyst distribution-layer switch, complete Option 1. If you are connecting to a remote-site Cisco Catalyst access-layer switch stack or modular switch, complete Option 2. If you are connecting to a Cisco Catalyst remote-site access-layer switch, complete Option 3.

Option 1. Connect a distribution-layer switch

Step 1: If a VLAN does not already exist on the distribution-layer switch, configure it now.

```
vlan 350
 name WAN_Service_Net
```

Step 2: Configure Layer 3. Be sure to configure a VLAN interface (SVI) for every new VLAN added so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan350
 ip address 10.4.32.129 255.255.255.192
 no shutdown
```

Next, you will configure EtherChannel member interfaces.

Step 3: Connect the Cisco WAVE appliance EtherChannel uplinks in order to separate switches in the distribution-layer switches or stack (for the Cisco Catalyst 4507R+E distribution layer, this separates redundant modules for additional resiliency), and then configure two or more physical interfaces to be members of the EtherChannel. It is recommended that the physical interfaces are added in multiples of two. Also, apply the egress QoS macro. This ensures traffic is prioritized appropriately.

Tech Tip

Configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

```
interface GigabitEthernet 1/0/2
 description Link to WAVE port 1
interface GigabitEthernet 2/0/2
 description Link to WAVE port 2
!
interface range GigabitEthernet 1/0/2, GigabitEthernet 2/0/2
 switchport
 macro apply EgressQoS
 channel-group 7 mode on
 logging event link-status
 logging event bundle-status
```

Next, you will configure the EtherChannel. An access-mode interface is used for the connection to the Cisco WAVE appliance.

Step 4: Assign the VLAN created at the beginning of the procedure to the interface. When using EtherChannel, the port channel number must match the channel group configured in Step 3.

```
interface Port-channel 7
 description EtherChannel link to WAVE
 switchport access vlan 350
 logging event link-status
 no shutdown
```

Option 2. Connect a remote-site access-layer switch stack or modular switch

Next, you will configure EtherChannel member interfaces. The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Tech Tip

EtherChannel is a logical interface which bundles multiple physical LAN links into a single logical link.

Step 1: Connect the Cisco WAVE appliance EtherChannel uplinks to separate switches in the stack, and in the case of the Cisco Catalyst 4507R+E access layer, to separate redundant modules for additional resiliency, and then configure two or more physical interfaces to be members of the EtherChannel and return their switchport configuration to the default. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro. This ensures traffic is prioritized.

```
default interface GigabitEthernet 1/0/2
default interface GigabitEthernet 2/0/2
!
interface GigabitEthernet 1/0/2
 description Link to WAVE port 1
interface GigabitEthernet 2/0/2
 description Link to WAVE port 2
!
interface range GigabitEthernet 1/0/2, GigabitEthernet 2/0/2
 switchport
 macro apply EgressQoS
 channel-group 7 mode on
 logging event link-status
 logging event bundle-status
```

Next, you will configure the EtherChannel. You use an access-mode interface for the connection to the Cisco WAVE appliance.

Step 2: Assign the data VLAN to the interface. When using EtherChannel, the port channel number must match the channel group configured in the previous step.

```
interface Port-channel 7
 description EtherChannel link to WAVE
 switchport access vlan 64
 ip arp inspection trust
 logging event link-status
 no shutdown
```

Option 3. Connect a remote-site access-layer switch

Step 1: Connect the Cisco WAVE appliance's external Ethernet port to an Ethernet port on the remote site's access switch, and then return the switchport configuration to the default.

```
default interface GigabitEthernet1/0/3
```

Step 2: Define the switchport in the remote-site access switch as an access port for the data VLAN, and then apply port-security and QoS configuration.

```
interface GigabitEthernet1/0/3
 description Link to WAVE
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

Procedure 2 Configure the Cisco WAVE appliance

You can deploy a cluster of Cisco WAVE appliances at the WAN-aggregation site in order to provide the headend termination for Cisco WAAS traffic to and from the remote sites across the WAN. You then connect these devices directly to the distribution-layer switch, using GRE-negotiated return in order to communicate with the WCCP routers. If you don't want resiliency for application acceleration at the WAN-aggregation site, you can deploy an appliance individually, instead of in a cluster.

You can also deploy Cisco WAVE appliances at WAN remote sites, either individually or as part of a WAVE cluster. You should use this procedure to configure WAN remote-site WAVE appliances. You use the same setup utility that you used in the initial configuration of the Cisco WAAS Central Manager to set up WAVE appliances. These devices require only basic setup through their console port in order to assign initial settings. After you complete this setup, you can perform all management of the WAAS network through the WAAS Central Manager console. Initial configuration of the Cisco WAVE application accelerators requires terminal access to the console port for basic configuration options and IP address assignment.

The setup utility configuration steps for the application accelerator Cisco WAVE appliances are similar to the setup of the Cisco WAAS Central Manager, but the steps begin to differ after you choose application-accelerator as the device mode. After you choose this mode, the setup script changes in order to allow you to register the WAVE appliance with the existing WAAS Central Manager and to define the traffic interception method as WCCP.

For all Cisco WAVE devices, the factory default username is admin and the factory default password is default.

Step 1: From the command line, enter **setup**. The initial setup utility starts.

```
    Parameter                 Default Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 1/0
 5. Autosense                 Enabled
 6.     DHCP                     Enabled
ESC Quit ? Help ———————— WAAS Default Configuration
————————————

Press 'y' to select above defaults, 'n' to configure all, <1-
6> to change specific default [y]: n
```

Step 2: Configure the appliance as an application accelerator.

```
1. Application Accelerator
2. AppNav Controller
3. Central Manager
Select device mode [1]: 1
```

Step 3: Configure the interception method.

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

Step 4: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST8PDT -7 0
```

Step 5: Configure the management interface, IP address, and default gateway.

```
No.      Interface Name      IP Address    Network Mask
1.       GigabitEthernet     1/0            dhcp
2.       GigabitEthernet     2/0            dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.4.32.161/26
Enter Default Gateway IP Address [Not configured]: 10.4.32.129
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.48.100
```

Step 6: Configure the DNS, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAVE-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

Step 7: Configure the WCCP router list.

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.4.32.241 10.4.32.242 10.4.32.243
```

Step 8: Select the appropriate license.

```
The product supports the following licenses:
1. Transport
2. Enterprise
3. Enterprise & Video
4. Enterprise & Virtual-Blade
5. Enterprise, Video & Virtual-Blade
Enter the license(s) you purchased [2]: 2
```

Step 9: Verify the configuration settings.

```
    Parameter                 Configured Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 PST8PDT -7 0
 4. Management Interface      GigabitEthernet 1/0
 5. Autosense                 Enabled
 6. DHCP                      Disabled
 7. IP Address                10.4.32.161
 8. IP Network Mask           255.255.255.192
 9. IP Default Gateway        10.4.32.129
10. CM IP Address             10.4.48.100
11. DNS IP Address            10.4.48.10
12. Domain Name(s)            cisco.local
13. Host Name                 WAVE-1
14. NTP Server Address        10.4.48.17
15. WCCP Router List          10.4.32.241 10.4.32.242
10.4.32.243
16. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration
————————

Press 'y' to select configuration, <F2> to see all
configuration, 'd' to toggle defaults display, <1-16> to
change specific parameter [y]: y
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
```

Step 10: In the EXEC mode, enable the propagation of local configuration changes to the Cisco WAAS Central Manager.

```
cms lcm enable
```

Step 11: If you are connecting the Cisco WAAS appliance to a distribution switch or switch stack, configure the port-channel connection and register it to the Cisco WAAS Central Manager.

```
interface GigabitEthernet 1/0
 no ip address 10.4.32.161 255.255.255.192
 exit
!
primary-interface PortChannel 1
!
interface PortChannel 1
 ip address 10.4.32.161 255.255.255.192
 exit
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 no shutdown
 exit
```

There are several additional, non-default settings that you must enable on the Cisco WAVE devices in order to complete the configuration. These setting are configured in the next steps.

Step 12: Configure the GRE-negotiated return. All Cisco WAVE devices use GRE-negotiated return with their respective WCCP routers.

```
no wccp tcp-promiscuous service-pair 1 2
wccp tcp-promiscuous service-pair 61 62 redirect-method gre
wccp tcp-promiscuous service-pair 61 62 egress-method wccp-gre
```

Step 13: Configure the WCCP router list. This design uses authentication between the routers and Cisco WAVE appliances.

If any of the WCCP routers are Cisco ASR1000 Series routers, then change the default setting of **hash-source-ip** to **mask-assign**. This change must be made for WCCP to operate properly and is made on the Cisco WAVE appliances, not on the routers.

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 7
wccp tcp-promiscuous service-pair 61 62 assignment-method mask
wccp tcp-promiscuous service-pair 61 62 password c1sco123
wccp tcp-promiscuous service-pair 61 62 enable
```

All other router platforms can use the default setting:

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 7
wccp tcp-promiscuous service-pair 61 62 password c1sco123
wccp tcp-promiscuous service-pair 61 62 enable
```

Next, you will configure device management protocols.

Step 14: Log in to the Cisco WAVE appliance.

Step 15: Generate the RSA key and enable the sshd service. This enables SSH.

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
no telnet enable
```

Step 16: Enable Simple Network Management Protocol (SNMP). This allows the network infrastructure devices to be managed by a Network Management System (NMS). Configure SNMPv2c for both a read-only and a read-write community string.

```
snmp-server community cisco
snmp-server community cisco123 RW
```

Step 17: If you want to limit access to the appliance, configure management ACLs.

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
interface PortChannel 1
 ip access-group 155 in
!
ip access-list standard  55
 permit 10.4.48.0 0.0.0.255
 exit
snmp-server access-list 55
```

Step 18: If you have a centralized TACACS+ server, enable AAA authentication for access control. This configures secure user authentication as the primary method for user authentication (login) and user authorization (configuration). AAA controls all management access to the Cisco WAAS and Cisco WAVE devices (SSH and HTTPS).

Tech Tip

A factory default local admin user was created on the Cisco WAAS and Cisco WAVE appliances during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or if you do not have a TACACS+ server in your organization.

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 19: After you make configuration changes, in the EXEC mode, save the configuration.

```
copy running-config startup-config
```

Step 20: If you are deploying a cluster of Cisco WAVE appliances, repeat Procedure 1 through Step 19 for the resilient appliance.

Procedure 3 Configure WCCPv2 on routers

This guide assumes that the router has already been configured. Only the procedures required to support the integration of Cisco WAAS into the deployment are included. For details on how to configure a WAN router, see the *Cisco SBA—Borderless Networks MPLS WAN Deployment Guide*, *VPN WAN Deployment Guide* or *Layer 2 WAN Deployment Guide*.

In this design, WCCP diverts network traffic destined for the WAN to the Cisco WAAS system for optimization. This method provides for a clean deployment with minimal additional cabling, and it requires both the WAN-aggregation and remote-site routers to be configured for WCCP.

Step 1: Configure global WCCP parameters, enable services 61 and 62, and then configure a group list and password. Permit only the on-site Cisco WAVE appliances in the group list in order to prevent unauthorized Cisco WAVE devices from joining the WAAS cluster.

You must enable services 61 and 62 for WCCP redirect for Cisco WAAS. As a best practice, exempt certain critical traffic types from WCCP redirect by using a redirect list.

```
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password c1sco123
!
ip access-list standard WAVE
 permit 10.4.32.161
 permit 10.4.32.162
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
```

Step 2: Configure WCCP redirection for traffic from the LAN. Be sure to identify specific interfaces where traffic to and from the WAN are intercepted.

Traffic from the LAN is intercepted with service 61 inbound on LAN interfaces. It is not necessary to configure WCCP interception on voice interfaces and voice VLANs.

If the LAN interface is a Layer 3 interface, define WCCP redirection on the interface directly.

```
interface Port-Channel 1
 ip wccp 61 redirect in
```

If the LAN interface is a VLAN trunk, define WCCP redirection on the data VLAN subinterface.

```
interface GigabitEthernet0/2.64
 ip wccp 61 redirect in
```

Next, you will configure WCCP redirection for traffic from the WAN.

Step 3: If you are configuring any Cisco WAN router, except a DMVPN hub router, intercept traffic from the WAN by using service 62 inbound on all WAN interfaces, including DMVPN tunnel interfaces (but not their underlying physical interfaces).

Example - MPLS WAN Interface

```
interface GigabitEthernet 0/3
 ip wccp 62 redirect in
```

Example - DMVPN WAN Interface

```
interface Tunnel 10
 ip wccp 62 redirect in
```

Step 4: If you want to configure DMVPN hub routers, configure WCCP 62 outbound on the LAN interface. This supports dynamic creation of spoke-to-spoke tunnels. Traffic from the WAN is intercepted with service 62 outbound on the LAN interfaces.

```
interface PortChannel 1
 ip wccp 62 redirect out
```

Step 5: After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Step 6: If you have multiple WAN routers at the site or multiple WAN interfaces on a single router, repeat the steps in this procedure for each WAN-facing interface.

Process

Configuring Cisco WAAS on the Cisco Services-Ready Engine module

1. Configure remote switch for Cisco SRE
2. Configure the Cisco SRE module
3. Configure WCCPv2 on routers

Configuration Checklist

The following table specifies the parameters and data, in addition to the universal design parameters, that you need in order to set up and configure the Cisco SRE module. For your convenience, you can enter your values in the table and refer to it when configuring the SRE module. The values you enter will differ from those in this example, which are provided for demonstration purposes only.

Table 7 - Cisco WAAS on the Cisco SRE module network parameters

Parameter	Cisco SBA values primary WAVE	Cisco SBA values secondary WAVE	Site-specific values
Switch interface number	1/0/3	1/0/4	
VLAN number	64	64	
Time zone	PST8PDT -7 0	PST8PDT -7 0	
IP address	10.5.52.8/24	10.5.52.9/24	
Default gateway	10.5.52.1/24	10.5.52.1/24	
WAAS Central Manager	10.4.48.100	10.4.48.100	
Hostname	WAVE-sre-1	WAVE-sre-2	
IP addresses of routers intercepting traffic with WCCP	10.255.251.203 (r1) 10.255.253.203 (r2)	10.255.251.203 (r1) 10.255.253.203 (r2)	
WCCP password	c1sco123	c1sco123	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS shared key (optional)	SecretKey	SecretKey	

Procedure 1 Configure remote switch for Cisco SRE

The access switch is the appropriate location to physically connect Cisco SRE modules at single-tier remote sites. Regardless of the switch type—single switch, switch stack, or modular—this type of connection must use a Layer 2 access interface.

This guide assumes that the LAN switch has already been configured. Only the procedures required to complete the connection of the switch to the Cisco WAVE appliances are included. For details on how to configure switches, see *Cisco SBA—Borderless Networks LAN Deployment Guide*.

Step 1: Connect the Cisco WAVE appliance's external Ethernet port to an Ethernet port on the remote site's access switch, and then return the switchport configuration to the default.

```
default interface GigabitEthernet1/0/3
```

Step 2: Define the switchport in the remote-site access switch as an access port for the data VLAN, and then apply port-security and QoS configuration.

```
interface GigabitEthernet1/0/3
 description Link to WAVE
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

Procedure 2 Configure the Cisco SRE module

This guide assumes that the router has already been configured. Only the procedures required to support the integration of Cisco WAAS into the deployment are included. For details on how to configure the WAN router, see the *Cisco SBA—Borderless Networks MPLS WAN Deployment Guide*, *VPN WAN Deployment Guide*, or *Layer 2 WAN Deployment Guide*.

You can use a variety of Cisco WAVE appliances or Cisco SRE form-factors for the remote-site Cisco WAAS equipment in this design, depending on the performance requirements.

You can insert the Cisco SRE modules directly into a corresponding module slot in the remote-site router and configure them somewhat differently from the appliances. If you are using an appliance, you can follow the Configuring the Cisco WAVE Appliance process with remote-site addressing parameters.

Although the remote-site router can potentially communicate directly with the Cisco SRE module by using the router backplane, this design uses the external interfaces on the modules, which allows for a consistent design implementation regardless of the chosen Cisco WAVE device. You must enable the service module (SM) interface and assign an arbitrary (locally significant only) IP address in order for the SM interface to be accessed through a console session from the host router.

You must connect the external interface to the data network on the access or distribution switch for this configuration to work properly.

If AAA is enabled on the router, configuring an exemption on the router is required. If you do not configure an exemption, you will be prompted for both a router login and a Cisco WAAS login, which can be confusing. Disabling the initial router authentication requires that you create an AAA method, which you then apply to the specific line configuration on the router associated with the Cisco SRE module.

Step 1: On the host router, configure console access and Cisco SRE module IP addresses. This permits console access to the SRE modules.

```
interface SM1/0
 ip address 192.0.2.2 255.255.255.252
 service-module external ip address 10.5.52.8 255.255.255.0
 service-module ip default-gateway 10.5.52.1
 no shutdown
```

Tech Tip

The IP address assigned 192.0.2.2 to SM/0 is arbitrary in this design and only locally significant to the host router.

Next, if AAA has been enabled on the router, you will configure an AAA exemption for Cisco SRE devices.

If you are not using AAA services, skip to Step 6.

Step 2: If you are using AAA services, create the AAA login method.

```
aaa authentication login MODULE none
```

Step 3: Determine which line number is assigned to Cisco SRE module. The example output below shows line 67.

```
RS203-2921-1# show run | begin line con 0
line con 0
 logging synchronous
line aux 0
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
 flowcontrol software
line vty 0 4
 transport preferred none
 transport input ssh
```

Step 4: Restrict access to the Cisco SRE console by creating an access list. The access-list number is arbitrary, but the IP address must match the address assigned to the SM interface in Step 1.

```
access-list 67 permit 192.0.2.2
```

Step 5: Assign the method to the appropriate line.

```
line 67
 login authentication MODULE
 access-class 67 in
 transport output none
```

Step 6: Connect to the Cisco WAVE console by using a session from the host router.

After the IP address is assigned, and the interface is enabled, it is possible to open a session on the Cisco WAVE appliance and run the setup script. For all WAVE devices, the factory default username is admin, and the factory default password is default.

If you are using secure user authentication on the router and have not created an AAA exemption, you must first authenticate with a valid router login credential before logging into the Cisco WAVE console session.

```
RS203-2921-1# service-module sm 1/0 session
```

Step 7: In the command line interface, enter **setup**. The initial setup utility starts.

```
    Parameter                 Default Value
    Device Mode               Application Accelerator
 1. Interception Method       WCCP
 2. Time Zone                 UTC 0 0
 3. Management Interface      GigabitEthernet 1/0    (internal)
    Autosense                 Disabled
    DHCP                      Disabled
ESC Quit ? Help ————————————— WAAS Default Configuration
————————————

Press 'y' to select above defaults, 'n' to configure all, <1-
3> to changespecific default [y]: n
```

Step 8: Configure the interception method.

```
1. WCCP
2. AppNav Controller
3. Other
Select Interception Method [1]: 1
```

Step 9: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST8PDT -7 0
```

Step 10: Configure the management interface, IP address, and default gateway.

This design uses the external interface as the management interface.

```
No.      Interface Name      IP Address     Network Mask
1.   GigabitEthernet 1/0     unassigned     unassigned
(internal)
2.   GigabitEthernet 2/0     dhcp           (external)
Select Management Interface [1]: 2
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
```

Tech Tip

If you receive the following warning, you may disregard it because the IP address configuration was provided previously.

```
*** You have chosen to disable DHCP! Any network
configuration learnt from DHCP server will be
unlearnt! SETUP will indicate failure as the
management interface cannot be brought up - Please
make sure WAVE Management Interface IP address and
Default Gateway are configured from the Router;
Press ENTER to continue:
```

Step 11: Configure the Cisco WAAS Central Manager address.

```
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.48.100
```

Step 12: Configure DNS, host, and NTP settings.

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAVE-SRE-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

Step 13: Configure the WCCP router list.

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.255.251.203 10.255.253.203
```

Step 14: Select the appropriate license.

```
The product supports the following licenses:
1. Transport
2. Enterprise
3. Enterprise & Video
Enter the license(s) you purchased [2]: 2
```

Step 15: Verify the configuration settings.

```
    Parameter                 Configured Value
 1. Interception Method       WCCP
 2. Time Zone                 PST8PDT -7 0
 3. Management Interface      GigabitEthernet 2/0      (external)
 4. Autosense                 Enabled
 5. DHCP                      Disabled
    IP Address                10.5.52.8
    IP Network Mask           255.255.255.0
    IP Default Gateway        10.5.52.1
 6. CM IP Address             10.4.48.100
 7. DNS IP Address            10.4.48.10
 8. Domain Name(s)            cisco.local
 9. Host Name                 WAVE-SRE-1
10. NTP Server Address        10.4.48.17
11. WCCP Router List          10.255.251.203 10.255.253.203
12. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration
————————————

Press 'y' to select configuration, <F2> to see all
configuration, 'd' to toggle defaults display, <1-12> to
change specific parameter [y]: y
                Router WCCP configuration
First WCCP router IP in the WCCP router list seems to be an
external address; WCCP configuration on external routers is
not allowed through SETUP. Please press ENTER to apply WAAS
configuration on WAVE ...
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
WAAS configuration applied successfully!!
Saved configuration to memory.
Press ENTER to continue ...
```

When you are prompted with a recommended router WCCP configuration template, you don't have to retain the information. This router configuration is covered in depth in a following procedure.

Step 16: In the EXEC mode, enable the propagation of local configuration changes to the Cisco WAAS Central Manager.

```
cms lcm enable
```

Step 17: Configure the GRE-negotiated return. All Cisco WAVE devices use GRE-negotiated return with their respective WCCP routers.

```
no wccp tcp-promiscuous service-pair 1 2
wccp tcp-promiscuous service-pair 61 62 redirect-method gre
wccp tcp-promiscuous service-pair 61 62 egress-method wccp-gre
```

Step 18: Configure the WCCP router list. This design uses authentication between the routers and Cisco WAVE appliances.

If any of the WCCP routers are Cisco ASR1000 Series routers, then change the default setting of **hash-source-ip** to **mask-assign**. This change must be made for WCCP to operate properly and is made on the Cisco WAVE appliances, not on the routers.

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 7
wccp tcp-promiscuous service-pair 61 62 assignment-method mask
wccp tcp-promiscuous service-pair 61 62 password c1sco123
wccp tcp-promiscuous service-pair 61 62 enable
```

All other router platforms can use the default setting:

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 7
wccp tcp-promiscuous service-pair 61 62 password c1sco123
wccp tcp-promiscuous service-pair 61 62 enable
```

Next, you will configure device management protocols.

Step 19: Log in to the Cisco WAVE appliance.

Step 20: Generate the RSA key and enable the sshd service. This enables SSH.

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
no telnet enable
```

Step 21: Enable Simple Network Management Protocol (SNMP) in order to allow the network infrastructure devices to be managed by a Network Management System (NMS), and then configure SNMPv2c both for a read-only and a read-write community string.

```
snmp-server community cisco
snmp-server community cisco123 RW
```

Step 22: If you want to limit access to the appliance, configure management ACLs.

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
interface GigabitEthernet 1/0
 ip access-group 155 in
!
ip access-list standard  55
 permit 10.4.48.0 0.0.0.255
 exit
snmp-server access-list 55
```

Step 23: If you have a centralized TACACS+ server, enable AAA authentication for access control. This configures secure user authentication as the primary method for user authentication (login) and user authorization (configuration). AAA controls all management access to the Cisco WAAS and Cisco WAVE devices (SSH and HTTPS).

Tech Tip

A factory default local admin user was created on the Cisco WAAS and Cisco WAVE appliances during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable or if you do not have a TACACS+ server in your organization.

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

Step 24: After you make configuration changes, in the EXEC mode, save the configuration.

```
copy running-config startup-config
```

Each Cisco WAVE appliance registers with the Cisco WAAS Central Manager as it becomes active on the network.

Step 25: If you want to verify the Cisco WAVE registration, on the respective WAVE appliance or via the web interface to the Cisco WAAS Central Manager, enter **show cms info**.

Step 26: When this configuration is complete, press the *escape sequence* **Ctrl+Shift+6** and then enter **x**. The command line of the host router returns.

Tech Tip

If you are using a terminal server the escape sequence is slightly different. Press and hold the escape sequence Ctrl+Shift, enter 6, enter 6 again, release the key combination, and then enter x. Entering 6 once returns you to the terminal server; entering 6 twice returns you to the host router.

Step 27: If you are deploying a cluster of Cisco WAVE appliances, repeat Procedure 1 through Procedure 2 for the resilient appliance.

Procedure 3 Configure WCCPv2 on routers

In this design, WCCP diverts network traffic destined for the WAN to the Cisco WAAS system for optimization. This method provides for a clean deployment with minimal additional cabling, and it requires both the WAN-aggregation and remote-site routers to be configured for WCCP.

This guide assumes that the router has already been configured. Only the procedures required to support the integration of Cisco WAAS into the deployment are included. Full details on WAN router configuration are included in the *Cisco SBA—Borderless Networks MPLS WAN Deployment Guide*, *VPN WAN Deployment Guide*, or *Layer 2 WAN Deployment Guide*.

Step 1: Configure global WCCP parameters, enable services 61 and 62, and then configure a group list and password. Permit only the on-site Cisco WAVE appliances in the group list in order to prevent unauthorized Cisco WAVE devices from joining the WAAS cluster.

You must enable services 61 and 62 for WCCP redirect for Cisco WAAS. These services should be using WCCP Version 2. As a best practice, exempt certain critical traffic types from WCCP redirect by using a redirect list.

```
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password c1sco123
!
```

```
ip access-list standard WAVE
 permit 10.5.52.8
 permit 10.5.52.9
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
```

Step 2: Configure WCCP redirection for traffic from the LAN.

Specific interfaces must be identified where traffic to and from the WAN are intercepted.

Traffic from the LAN is intercepted with service 61 inbound on all LAN interfaces. It is not necessary to configure WCCP interception on voice interfaces and voice VLANs.

If the LAN interface is a Layer 3 interface, define WCCP redirection on the interface directly.

```
interface Port-Channel 1
 ip wccp 61 redirect in
```

If the LAN interface is a VLAN trunk, define WCCP redirection on the data VLAN subinterface.

```
interface GigabitEthernet0/2.64
 ip wccp 61 redirect in
```

Step 3: Configure WCCP redirection for traffic from the WAN.

Traffic from the WAN is intercepted with service 62 inbound on all WAN interfaces, including DMVPN tunnel interfaces (but not their underlying physical interfaces).

Example - MPLS WAN Interface

```
interface GigabitEthernet 0/3
 ip wccp 62 redirect in
```

Example - DMVPN WAN Interface

```
interface Tunnel 10
 ip wccp 62 redirect in
```

Step 4: After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Step 5: If you have multiple WAN routers at the site, repeat Step 1 through Step 4 for each WAN router.

Process

Configuring Cisco WAAS Express

1. Configure the Central Manager for WAASx
2. Create WAAS Express user
3. Configure WAAS Express routers

Configuration Checklist

The following table specifies the parameters and data, in addition to the universal design parameters, that you need in order to set up and configure Cisco WAAS Express. For your convenience, you can enter your values in the table and refer to it when configuring the router. The values you enter will differ from those in this example, which are provided for demonstration purposes only

Table 8 - Cisco WAAS Express network system parameters checklist

Parameter	Cisco SBA values primary WAVE	Site-specific values
WAAS Central Manager	10.4.48.100	
WAASx username	waasx	
WAASx password	c1sco123	

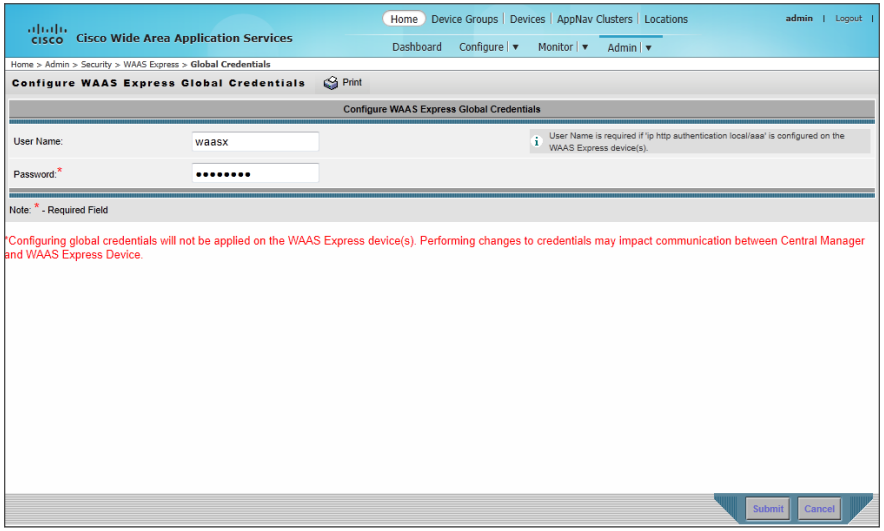
Procedure 1 Configure the Central Manager for WAASx

You can use the Cisco WAAS Central Manager to centrally manage WAASx routers, similar to a Cisco WAVE appliance. You must define a user name and password for the WAAS Central Manager to use to access the WAASx routers for monitoring and management. You secure these communications by using HTTPS, which requires the use of digital certificates.

To enable secure communications between the Cisco WAAS Central Manager and the router requires that you install the digital certificate from the WAAS Central Manager on each of the WAASx routers. The certificate can be exported in privacy enhanced mail (PEM) base64 format. This command is available through the device command line interface.

In this procedure, you will configure login and password credentials for the Cisco WAASx router by using the Cisco WAAS Central Manager web interface (https://waas-wcm-1.cisco.local:8443) and you will export the Cisco WAAS Central Manager certificate necessary to ensure secure communication between the Cisco WAAS Central Manager and the WAASx routers in your deployment.

Step 1: In Cisco WAAS Central Manager, navigate to **Admin > Security > WAAS Express > Global Credentials**.



Step 2: Enter the appropriate user name and password that you also plan to configure on the Cisco WAASx router or on the central AAA server. (Example: user name waasx and password c1sco123)

Step 3: Export the trusted digital certificate from Cisco WAAS Central Manager.

```
WAAS-WCM-1#show crypto certificate-detail admin | begin BEGIN
...skipping
-----BEGIN CERTIFICATE-----
<certificate data deleted>
-----END CERTIFICATE-----
```

Step 4: Because this information is required for all Cisco WAASx routers, copy and paste this certificate, and then save it to a secure file.

Procedure 2 Create WAAS Express user

There are two options when you are creating the Cisco WAAS Express account. If you want to create the account locally on each WAAS Express router, complete Option 1. If you want to create it once on the central AAA server, complete Option 2.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized authentication, authorization and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis.

Be aware that if AAA is used for router administration, centralized AAA must also be used for the WAAS Express user.

Option 1. Create a local user account

Step 1: Create a local user on the remote-site router.

```
username waasx privilege 15 password c1sco123
```

Option 2. Create a centralized AAA account

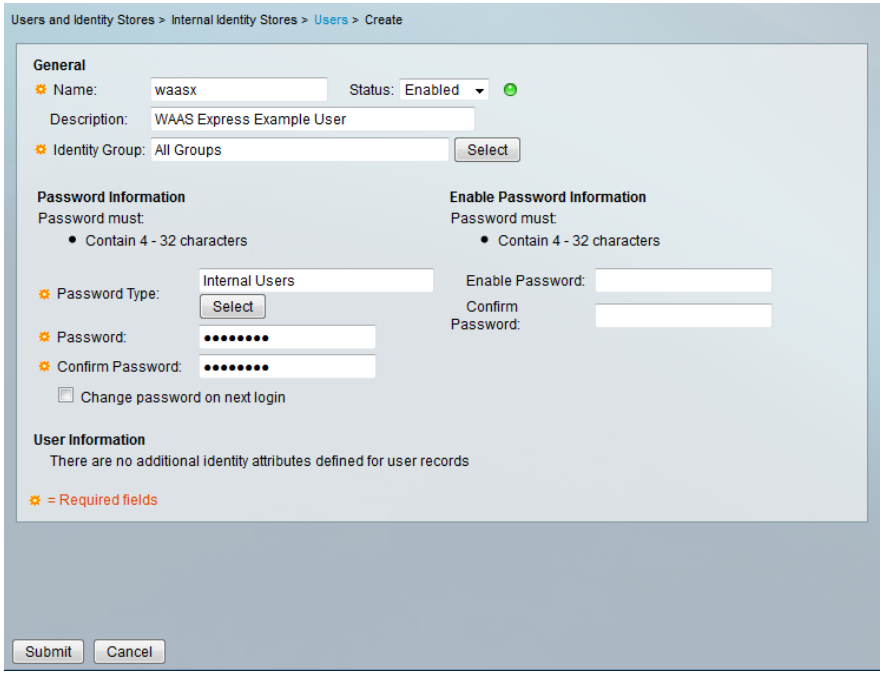
The Cisco Secure ACS internal identity store can contain all the network administrator accounts or just accounts that require a policy exception if an external identity store (such as Microsoft Active Directory) is available. A common example of an account that would require an exception is one associated with a network management system that allows the account to perform automated configuration and monitoring.

Step 1: Navigate and log in to the Cisco Secure ACS Administration page. (Example: https://acs.cisco.local)

Step 2: Navigate to **Users and Identity Stores** > **Internal Identity Stores** > **Users**.

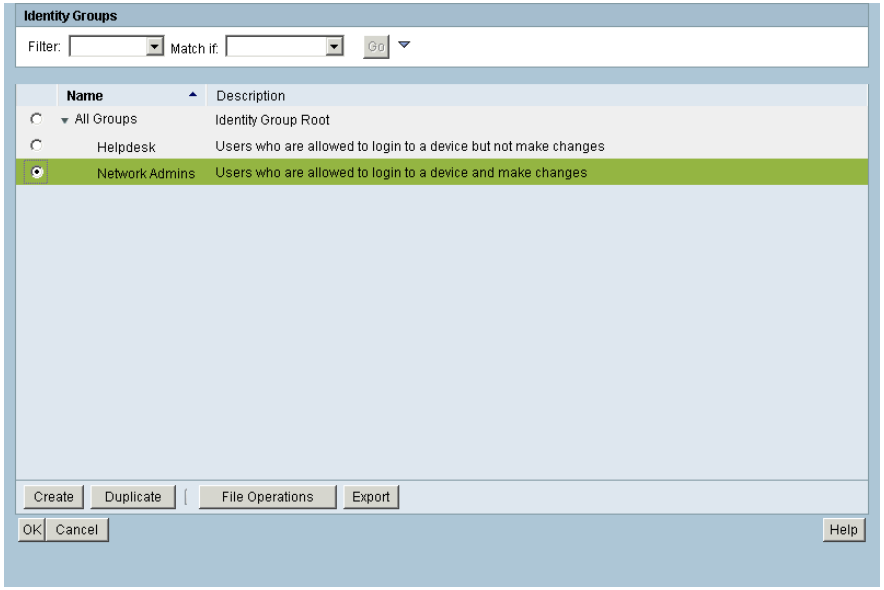
Step 3: Click **Create**.

Step 4: Enter a name, description, and password for the user account. (Example: user name waasx and password c1sco123)



Step 5: To the right of Identity Group, click **Select**.

Step 6: Select **Network Admins**, and then click **OK**.



Step 7: Click **Submit**.

Procedure 3 Configure WAAS Express routers

This guide assumes that the router has already been configured. Only the procedures required to support the integration of Cisco WAAS into the deployment are included. Full details on WAN router configuration are included in the *Cisco SBA—Borderless Networks MPLS WAN Deployment Guide*, *VPN WAN Deployment Guide*, or *Layer 2 WAN Deployment Guide*.

If you want to turn on the embedded WAN optimization, you must enable Cisco WAAS optimization on the router's WAN interface. The same Cisco WAAS Central Manager used with Cisco WAVE devices can also centrally manage WAASx. The router must also be properly configured to communicate securely with the WAAS Central Manager.

Note the following:

- Cisco WAASx is a specially licensed feature. This license must be installed on a router with sufficient DRAM to support the WAASx functionality.
- Cisco WAASx routers must be configured with maximum DRAM.
- WCCP redirection is not used for a Cisco WAASx implementation. There is no need to redirect traffic to an external device, because all traffic optimization is performed on the router.

Step 1: On a remote-site router, enable Cisco WAAS with WAN interface GigabitEthernet0/0.

```
interface GigabitEthernet0/0
 waas enable
```

Step 2: Configure a self-signed trustpoint, and then generate a digital certificate.

This step is necessary even if you already have a self-signed trustpoint that is auto-generated from HTTPS and was enabled previously. For the **subject-alt-name** field, match the host name and domain name that are already configured on the router.

```
crypto pki trustpoint SELF-SIGNED-TRUSTPOINT
 enrollment selfsigned
 subject-alt-name RS204-1941.cisco.local
 revocation-check none
 rsakeypair SELF-SIGNED-RSAKEYPAIR 2048
 exit
crypto pki enroll SELF-SIGNED-TRUSTPOINT
The router has already generated a Self Signed Certificate for
trustpoint TP-self-signed-xxxxxx.
If you continue the existing trustpoint and Self Signed
Certificate will be deleted.
Do you want to continue generating a new Self Signed
Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/
no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

Step 3: Configure the Cisco WAASx router to use a loopback interface as the source for any HTTP client communication.

```
ip http client source-interface Loopback0
```

Step 4: Enable the HTTPS secure server.

```
ip http secure-server
ip http secure-trustpoint SELF-SIGNED-TRUSTPOINT
```

Step 5: Create a trustpoint, and then import the Cisco WAAS Central Manager certificate.

```
crypto pki trustpoint WAAS-WCM
 revocation-check none
 enrollment terminal pem
 exit
crypto pki authenticate WAAS-WCM
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

Step 6: Paste the PEM certificate that was generated in the previous procedure from the Cisco WAAS Central Manager.

```
-----BEGIN CERTIFICATE-----
<certificate data deleted>
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
 Fingerprint MD5: 2EA6FF8F 38ABC32F 25168396 1A587F17
Fingerprint SHA1: 8DAB6185 7B95FC4C 34FDACDC A8F2B1A4 8074709B
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

You have completed generating and installing the digital certificates.

Step 7: In the EXEC mode, register the Cisco WAASx router with the Cisco WAAS Central Manager.

```
waas cm-register https://10.4.48.100:8443/wcm/register
```

The router appears as a managed device on the Cisco WAAS Central Manager.

Step 8: After you make configuration changes, save the configuration.

```
copy running-config startup-config
```

Notes

Appendix A: Product List

WAAS Central Manager

Functional Area	Product Description	Part Numbers	Software
Central Manager Appliance	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	5.0.1
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	
	Cisco Wide Area Virtualization Engine 294	WAVE-294-K9	
Central Manager Virtual Appliance	Virtual WAAS Central Manager	WAAS-CM-VIRT-K9	5.0.1
	License to manage up to 2000 WAAS Nodes	LIC-VCM-2000N	
	License to manage up to 100 WAAS Nodes	LIC-VCM-100N	

WAAS Aggregation

Functional Area	Product Description	Part Numbers	Software
WAVE Aggregation Appliance	Cisco Wide Area Virtualization Engine 8541	WAVE-8541-K9	5.0.1
	Cisco Wide Area Virtualization Engine 7571	WAVE-7571-K9	
	Cisco Wide Area Virtualization Engine 7541	WAVE-7541-K9	
	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	

WAAS Remote Site

Functional Area	Product Description	Part Numbers	Software
Remote Site WAVE Appliance	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	5.0.1
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	
	Cisco Wide Area Virtualization Engine 294	WAVE-294-K9	
Remote-Site WAVE SRE	Cisco SRE 910 with 4-8 GB RAM, 2x 500 GB 7,200 rpm HDD, RAID 0/1, dual-core CPU configured with ISR G2	SM-SRE-910-K9	5.0.1
	WAAS software container for SRE SM 900	SM9-WAAS	
	WAAS Enterprise License for SRE Large deployment	WAAS-ENT-SM-L	
	WAAS Enterprise License for SRE Medium deployment	WAAS-ENT-SM-M	
	WAAS Enterprise License for SRE Small deployment	WAAS-ENT-SM-S	
	Cisco SRE 710 with 4 GB RAM, 500 GB 7,200 rpm HDD, single-core CPU configured with Cisco ISR G2	SM-SRE-710-K9	
	WAAS software container for SRE SM 700	SM7-WAAS	
	WAAS Enterprise License for SRE Medium deployment	WAAS-ENT-SM-M	
	WAAS Enterprise License for SRE Small deployment	WAAS-ENT-SM-S	
Remote-Site WAAS Express	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M5 securityk9 license datak9 license
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S2 Advanced Enterprise License
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M5 securityk9 license datak9 license
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M5 securityk9 license datak9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M5 securityk9 license datak9 license

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Functional Area	Product Description	Part Numbers	Software
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(1b) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We made changes to improve the readability and technical accuracy of this guide.
- We modified the time zone settings in order to match the rest of Cisco SBA documentation.

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000125-1 1/13