

Application Optimization Using Cisco WAAS

Technology Design Guide

December 2013



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency	2
Introduction	3
Technology Use Cases	
Use Case: Optimization of Traffic Traversing the WAN	
Design Overview	3
Cisco WAAS Central Manager	
WAAS Nodes	
AppNav	
WAN Aggregation Design Models	
Remote Sites	10
Deployment Details	14
Configuring the Cisco WAAS Central Manager	14
Configuring the Cisco WAVE Appliance as a WAAS Node	21
Configuring the Cisco WAVE Appliance as an AppNav Controller	
Configuring AppNav-XE on a WAN-Aggregation Router	
Preparing the Cisco UCS E-Series module for vWAAS	
Install VMware ESXi on the Cisco UCS E-Series module	
Configuring Cisco vWAAS on the UCS E-Series module	
Configuring Cisco WAAS on the Cisco Services-Ready Engine module	
Configuring Cisco WAAS Express	128
Appendix A: Product List	135
Appendix B: Changes	

Appendix C: Configuration Examples	
Central Manager	140
WAAS Central Manager (vWAAS)	140
WCCP Design Model	
Primary Site WAAS Node	
Primary Site WAAS Node (vWAAS)	
WAN-Aggregation Router	
WAN-Aggregation Router (DMVPN hub)	
AppNav Off Path Design Model	
AppNav Controller and WAAS Node	
Primary Site WAAS Node	153
WAN-Aggregation Router	155
WAN-Aggregation Router (DMVPN hub)	
AppNav-XE Design Model	158
AppNav-XE Controller	158
Primary Site WAAS Node	
Remote Sites	163
RS202 WAAS Node	163
RS202 WAN Router	166
RS213 WAAS Node (vWAAS)	
RS213 WAN Router (UCS E-Series)	169
RS201 WAAS Node (SRE)	
RS201 WAN Router (SRE)	
RS204 WAASx WAN Router	

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. 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 at a CLI or script prompt appear as follows:

Router# enable

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

police rate 10000 pps burst 10000 packets conform-action set-discard-classtransmit 48 exceed-action transmit

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 feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd/wan

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

• Optimization of Traffic Traversing the WAN–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.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Deployment of Cisco Wide Area Application Services (WAAS) Central Manager and Cisco Wide Area Virtualization Engine (WAVE) appliances
- Deployment of Virtual WAAS (vWAAS) for primary site and remote-site
- Deployment of Application Navigator (AppNav) for intelligent load distribution
- · Integration of WAAS at the WAN aggregation router
- · Integration of WAAS at the WAN remote-site router and switch

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- CCNA Routing and Switching–1 to 3 years installing, configuring, and maintaining routed and switched networks
- VCP VMware–At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

Related CVD Guides MPLS WAN Technology cisco. **Design Guide** VALIDATED DESIGN VPN WAN Technology cisco. ALIDATED **Design Guide Application Optimization** cisco. Using Cisco ISR-WAAS ALIDATED **Technology Design Guide**

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd/wan

Introduction

Application Optimization using Cisco Wide Area Application Services (WAAS) is an essential component of the Cisco Intelligent WAN (IWAN). Cisco IWAN delivers an uncompromised user experience over any connection, allowing an organization to right-size their network with operational simplicity and lower costs.

Technology Use Cases

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.

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.

Use Case: Optimization of Traffic Traversing the WAN

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.

This design guide enables the following capabilities:

- Enhanced end-user experience increasing effective bandwidth and reducing latency
- · Integration into the existing Cisco WAN routers, providing a flexible deployment
- · Centralized operation and management of all the organization's application optimization devices

Design 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 device hosts the WAAS Central Manager GUI, a web-based interface that allows you to configure, manage, and monitor the WAAS devices in your network. WAAS Central Manager resides on a dedicated Cisco Wide Area Virtualization Engine (WAVE) device or as a vWAAS instance (a WAAS running as a virtual machine).

The following table provides details about the Cisco WAVE sizing for Cisco WAAS Central Manager.

Device	Number of managed devices (Cisco WAAS only)	Number of managed devices (Cisco WAAS and Cisco WAAS Express)
WAVE-294-4GB	250	200
WAVE-594-8GB	1000	800
WAVE-694-16GB	2000	2000
vCM-100N	100	80
vCM-2000N	2000	2000

Table 1 -	Cisco V	IAAS	Central	Manager	sizina	options
TUDIC I	01000 11	1110	oonna	manager	JIZII IG	options

WAAS Nodes

A Cisco WAAS node (WN) is a WAAS application accelerator (for instance, a Cisco WAVE appliance, Service Module-Services Ready Engine [SM-SRE] network module, or vWAAS instance, but not a WAAS Express device) that optimizes and accelerates traffic according to the optimization policies configured on the device. The Table 2 provides details about the Cisco WN sizing for the WAN-aggregation site. The fan-out numbers correspond to the total number of remote-peer WNs.

A Cisco WAAS node group (WNG) is a group of WAAS nodes that services a particular set of traffic flows identified by AppNav policies.

	Reader Tip
	Some Cisco product documentation may use different terminology. This guide references the most common terminology in use for consistency.
\	Examples: WAAS Node (WN) = Service Node (SN) WAAS Node group (WNG) = Service Node group (SNG)

Table 2 -	WAN-aggregation	Cisco	WAVE appliances
-----------	-----------------	-------	-----------------

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	100
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

Table 3 - WAN-aggregation for Cisco vWAAS on Cisco UCS B-Series and Cisco UCS C-Series

Device	Max. optimized TCP connections	Max. recommended WAN link [Mbps]	Max. optimized throughput [Mbps]	Max. core fan-out [Peers]
vWAAS-750	750	50	250	100
vWAAS-1300	1300	80	300	200
vWAAS-2500	2500	200	400	300
vWAAS-6000	6000	200	400	300
vWAAS-12000	12000	310	425	1400
vWAAS-50000	50000	700	1000	2800

For comprehensive sizing and planning, please work with your Cisco account team or Cisco partner.

AppNav

Cisco Application Navigator (AppNav) technology enables customers to virtualize WAN optimization resources by pooling them into one elastic resource in a manner that is policy based and on demand with the best available scalability and performance. It integrates transparently with Cisco WAAS physical and virtual network infrastructure and supports the capability to expand the WAN optimization service to meet future demands.

The Cisco AppNav solution is comprised of one or more Cisco AppNav Controllers, which intelligently load share network traffic for optimization to a set of resource pools built with Cisco WAAS nodes. The Cisco AppNav Controllers make intelligent flow distribution decisions based on the state of the WAAS Nodes currently providing services.





A Cisco AppNav Controller (ANC) is a WAVE appliance with a Cisco AppNav Controller I/O Module (IOM) that intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more WAAS nodes for optimization. The ANC function is also available as a component of Cisco IOS-XE software running on the Cisco ASR 1000 Series routers and the Cisco ISR 4451-X router. When the AppNav Controller is running as a router software component, it is referred to as AppNav-XE.

CO Reader Tip

Some Cisco product documentation may use different terminology. This guide references the most common terminology in use for consistency.

Examples:

AppNav Controller (ANC) = AppNav Controller (AC)

AppNav Controller group (ANCG) = AppNav Controller group (ACG)

Appliance	WAVE-APNV-GE-12T WAVE-APNV-GE-12SFP	WAVE-APNV-10GE
WAVE-594	-	AppNav Controller
WAVE-694	WAAS Node AppNav Controller	-
WAVE-7541	WAAS Node AppNav Controller	-
WAVE-7571	WAAS Node AppNav Controller	-
WAVE-8541	WAAS Node AppNav Controller	_

Table 4 - Supported roles for Cisco WAVE appliances with a Cisco AppNav IOM

Tech Tip

The WAVE-APNV-10GE is only available bundled with the WAVE-594 and redundant power supply unit.

A Cisco AppNav Controller group (ANCG) is a group of AppNav Controllers that share a common policy and together provide the necessary intelligence for handling asymmetric flows and providing high availability. The group of all ANC and WN devices configured together as a system is referred to as an AppNav Cluster.

Tech Tip

A Cisco AppNav-XE controller group must contain only members of the same router product family (Example: only Cisco ASR 1000 routers, or only Cisco ISR 4451-X routers). The ANCG may contain up to four AppNav-XE routers.

WAN Aggregation Design Models

There are three different design models for the WAN-aggregation site. The following table provides a brief summary with more detail available in the specific sections for each design model.

Requirement	WAAS with WCCP design model	AppNav Off Path design model	AppNav-XE design model
AppNav IOM	Not needed	Required	Not needed
Mix of different router families	Supported	Supported	All routers must be same product family
Maximum number of ANCs in an ANCG	Not applicable	8	4
Intelligent load sharing	Basic load sharing only	Full AppNav policies	Full AppNav policies

Table 5 - How to choose a WAN Aggregation design model

WAAS node group with WCCP

The Cisco WAAS node group with WCCP design model has been the Cisco recommended design for many years prior to the introduction of AppNav. This design is widely adopted and is still currently supported by Cisco. The AppNav IOMs are not required and because the router redirection method is WCCP, this design allows for a mix of router product families. This design model is the recommended design model for remote-site deployments.

The Cisco WAAS node group with WCCP deployment model uses a single group of two or more WAAS Nodes to provide WAN optimization. The total number of devices required is a minimum of two (for N+1 resiliency).

The Cisco WAVE appliances or Cisco vWAAS instances connect to the distribution-layer switch. The connections to WAVE appliances 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. A vWAAS instance uses network interface card (NIC) teaming in order to provide resiliency. In both cases, the WAAS Nodes connect to the WAN services network that is configured on the distribution switch.

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.

In this design model, 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 WN to router. When a design uses a GRE-negotiated return, it is not required that the WN and the WAN aggregation routers are Layer 2 adjacent.



AppNav Off Path

The Cisco AppNav Off Path design model is the preferred model for new deployments.

The Cisco AppNav Off Path design model logically inserts the ANCs between the redirecting routers and the Cisco WAAS node group(s). WCCP is still used between the routers and the AppNav controllers, but the WCCP function is strictly limited to redirection and performs no load distribution. AppNav performs the intelligent load distribution.

In this design model, 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, as discussed in the previous section:

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

Tech Tip

1

When using a Cisco AppNav Off Path deployment, it is possible to use just a single WCCP service group (Example: service group 61) in order to provide WCCP redirection for both source and destination traffic. However, this design model continues to use a pair of service groups for consistency and ease of migration.

The connections from the distribution switch to the WAN aggregation routers are routed point-to-point links. This design mandates the use of a generic GRE tunnel between the ANCs and the routers. When a design uses a generic GRE tunnel, it is not required that the ANCs and the WAN aggregation routers are Layer 2 adjacent.

You may enable both the ANC and WN capability concurrently on a Cisco WAVE appliance when using the 1-Gbps IOMs. This allows the device to perform dual roles.





AppNav-XE

The Cisco AppNav-XE design model allows you to deploy AppNav with an existing group of Cisco WAAS nodes without requiring the installation of IOMs. You are limited to up to four AppNav-XE Controllers, which must all be members of the same router product family. Also, the ANCG may not include IOM-based ANCs.

The Cisco AppNav-XE deployment model uses an AppNav Controller running natively on the WAN-aggregation routers. Traffic interception is accomplished by using service insertion on the routers' WAN interfaces. WCCP is not required for this deployment model, and the ANCs and the WAN aggregation routers are not required to be Layer 2 adjacent.

Figure 4 - AppNav-XE design model



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 or Cisco vWAAS instance. Similarly, all dual-router sites use dual WAVE appliances or vWAAS instances. The specifics of the WAAS 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 and Cisco vWAAS sizing is provided in the following tables. The optimized throughput numbers correspond to the apparent bandwidth available after successful optimization by Cisco WAAS.

Table 6 -	WAN remote-site	Cisco WAVE appl	iances and WAAS Express
10010 0		0.000 10 10 2 4000	1011000 0110 VV V 10 Exp1000

Device	Max. optimized TCP connections	Max. recommended WAN link [Mbps]	Max. optimized throughput [Mbps]
Cisco1941/WAASx1	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

¹ Single-link design only

Table 7 - WAN remote-site Cisco vWAAS on Cisco UCS E-Series

Device	Max. optimized TCP connections	Max. recommended WAN link [Mbps]	Max. optimized throughput [Mbps]
vWAAS-200	200	10	100
vWAAS-750	750	50	250
vWAAS-1300	1300	80	300
vWAAS-2500	2500	200	400

For comprehensive sizing and planning, please work with your Cisco account team or Cisco partner.

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.





The Cisco WAAS form factors for a WAN remote site include a Cisco UCS E-Series router module, 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:

- Appliance-Two interfaces (both external)
- SRE module–One internal interface (router-connected only), one external interface
- · UCS E-Series module-One or two interfaces (both external)

The approach for connecting the Cisco WAVE or Cisco vWAAS devices to the LAN is to be consistent regardless of the chosen hardware form-factor. All 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 WAAS devices, and the Cisco UCS E-Series module, 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. The internal interface of the UCS E-Series module is not used for this design, except for the initial bootstrapping and management of the device configurations.

You must connect an external Ethernet cable from each Cisco SRE module for this solution. You must also connect one or two external Ethernet cables from each Cisco UCS E-Series module for this solution.

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

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



WCCP 62 (from WAN)

Negotiated GRE Tunnel

Figure 6 - Cisco WAAS topology--remote-site access-layer design



Figure 7 - Cisco WAAS topology--remote-site distribution-layer design



Where possible, connect the Cisco WAVE appliances through both interfaces by using EtherChannel for performance and resiliency. A Cisco vWAAS instance uses NIC teaming to provide resiliency.

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

The WCCP redirect uses service groups 61 and 62 in order 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 negotiatedreturn GRE tunnel from the Cisco 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 design 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 8 -	Universal	design	parameters
-----------	-----------	--------	------------

Network service	CVD 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	

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

PROCESS

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 9 -	Cisco WAAS	S Central Manage	er network parameters

Parameter	CVD values	Site-specific values
Switch interface number	1/0/10	
VLAN number	148	
Time zone	PST8PDT - 8 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 the applicable guide: Data Center Technology Design Guide or Server Room Technology Design 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

1

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 dualhomed 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.



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 the appropriate Cisco WAVE device or Cisco vWAAS from Table 1 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**.

OO Reader Tip

This example shows the configuration of a Cisco WAVE device. When using a vWAAS as the WAAS Central Manager, the setup options may be slightly different.

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
Pres	ss y' to select above def	aults, 'n' to configure all, <1-6> to change
spec	cific default [y]: n	

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

- Application Accelerator
 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 -8 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

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 -8 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]: \mathbf{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] \mathbf{y}
Are you sure? <y/n> [n]: \mathbf{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 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
exit
!
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.

(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 Device Management Using ACS Technology Design 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. Click **Submit**.

Cisco Wide Area Application Services		Home Device Groups Devices AppNav Clusters Locations admi	in Logout
		Dashboard Configure 🔻 Monitor 🔻 Admin 🔻	
Home > Admin > AAA > User Groups			
Creating New User Group	S Print		
		User Group Information	
Name:*	Network Admins		
		Comments	
Note: * - Required Field			
		Submit	Cancel

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

alialia			Home Dev	ice Groups Dev	ices AppNav Clu	sters Locations	admin	Logout
CISCO Cisco Wide Area Application Services		Dashboard	Configure 🔻	Monitor 🔻 🖉	Admin 🔻			
ome > Admin > AAA > User xternal User Group Manac		ement: Domain Managem	ent					
🕑 Refresh Table 🛛 🖪		Remove all Roles						
Roles	<u>.</u>					Items 1-1 of 1 F	tows per page: 25	Go
Filter: Name	✓ Match if: like	•		Go	Clear Filter]		
	Role				Com	iments		
🗙 🔂 admin			Admin role					
						Page 1 of	1 🗐 🖣 🕨	
							Submit Cancel	

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

alada	Home Device Groups Devices AppNav Clusters Locations admin Logout
CISCO Cisco Wide Area Application Services	Dashboard Configure 🔻 Monitor 💌 Admin 💌
Home > Admin > AAA > User Groups	
External User Group Management Role Management Domain Management	
🔞 Refresh Table 🛛 🛤 Assign all Roles 🛛 🧔 Remove all Roles	
Roles	Items 1-1 of 1 Rows per page: 25 👻 Go
Filter: Name Match if: like	Go Clear Filter
Role	Comments
🛇 6Ə admin	Admin role
	Page 1 of 1 14 4 1
Change submitted.	Submit

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.



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



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

Configuration Checklist

1

PROCESS

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.

Tech Tip

This process should also be used for a Cisco vWAAS instance when that instance is already deployed on a VMware ESX server at the WAN-aggregation site. Specific differences are noted throughout the configuration details. Table 10 - Cisco WAAS using Cisco WAVE Appliance network parameters

Parameter	CVD values primary WAVE	CVD values secondary WAVE	Site-specific values
Switch interface numbers	1/0/2	1/0/2	
	2/0/2	2/0/2	
VLAN number	350	350	
VLAN name (optional)	WAN_Service_Net	WAN_Service_Net	
Time zone	PST8PDT -8 0	PST8PDT -8 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.
- Distribution-layer switch for Cisco vWAAS—This device type requires a resilient connection but does not require a routing protocol. This type of connection uses an active/standby port pair.
- 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 Campus Wired LAN Technology Design Guide.

If you are connecting a Cisco Catalyst distribution-layer switch, complete Option 1. If you are connecting a vWAAS instance to a Cisco Catalyst distribution-layer switch, complete Option 2. If you are connecting to a remote-site Cisco Catalyst access-layer switch stack or modular switch, complete Option 3. If you are connecting to a Cisco Catalyst remote-site access-layer switch, complete Option 4.

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

i

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 distribution-layer switch for vWAAS

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 ESXi server ports 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 same VLAN. It is recommended that you use N+1 physical interfaces where N is the number of Cisco vWAAS instances. Also, apply the egress QoS macro. This ensures traffic is prioritized appropriately.

```
interface GigabitEthernet 1/0/12
description Link to ESXi vmnic1
interface GigabitEthernet 2/0/12
description Link to ESXi vmnic2
!
interface range GigabitEthernet 1/0/12, GigabitEthernet 2/0/12
switchport
switchport host
switchport node access
switchport access vlan 350
macro apply EgressQoS
logging event link-status
no shutdown
```

Option 3: 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 4: 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

Tech Tip

This procedure assumes that you are using the WAAS with WCCP design model. If you are using the AppNav off path design model or the AppNav-XE design model, WCCP is not used on the WNs. For Step 7 enter a single unused IP address (any value) and skip Step 12 and Step 13.

You can deploy a group 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 group.

You can also deploy Cisco WAVE appliances at WAN remote sites, either individually or as part of a WNG. You should use this procedure to configure WAN remote-site Cisco 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 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 —————
Pre	ss 'y' to select above def	aults, `n' to configure all, <1-6> to change
spe	cific 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.

```
    WCCP
    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 -8 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 -8 0
4.	Management Interface	GigabitEthernet 1/0

```
5.
                                Enabled
     Autosense
 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, \langle F2 \rangle 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
1
primary-interface PortChannel 1
1
interface PortChannel 1
 ip address 10.4.32.161 255.255.255.192
exit
1
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 settings 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. Skip this step when using the AppNav Off Path design model or the AppNav-XE design model.

```
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. Skip this step when using the AppNav Off Path design model or the AppNav-XE design model.

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 clscol23
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 clsco123
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 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
    exit
!
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 group of Cisco WAVE appliances, repeat Step 1 through Step 19 for the resilient appliance.

This procedure assumes that you are using the WAAS with WCCP design model. If you are using a AppNav off path design model or the AppNav-XE design model, skip this procedure.

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 MPLS WAN Technology Design Guide or VPN WAN Technology Design 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 Cisco WAAS node group.

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 and other protocols which cannot be optimized from WCCP redirect by using a redirect list.

Service	TCP port number
Secure shell (SSH)	22
Telnet	23
TACACS+	49
Border Gateway Protocol (BGP)	179
Network Time Protocol (NTP)	123

Table 11 - Critical traffic types to exempt from WCCP

Table 12 - Additional traffic types to exempt from WCCP

Service	TCP port number(s)
SNMP, SNMP trap	161, 162
SCCP, secure SCCP	2000, 2443
SIP, secure SIP	5060, 5061
H.323 gatekeeper discovery	1718
H.323 (H.225 signalling)	1720
MGCP backhaul	2428
HTTPS	443, 8443
HTTP firmware	6970
NMAP	689

Add a pair of deny statements for each TCP port listed in Table 11 and Table 12.

```
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clscol23
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clscol23
```

```
!
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
deny tcp any any eq 161
deny tcp any eq 161 any
deny tcp any any eq 162
deny tcp any eq 162 any
deny tcp any any eq 2000
deny tcp any eq 2000 any
deny tcp any any eq 2443
deny tcp any eq 2443 any
deny tcp any any eq 5060
deny tcp any eq 5060 any
deny tcp any any eq 5061
deny tcp any eq 5061 any
deny tcp any any eq 1718
deny tcp any eq 1718 any
deny tcp any any eq 1720
deny tcp any eq 1720 any
deny tcp any any eq 2428
deny tcp any eq 2428 any
deny tcp any any eq 443
deny tcp any eq 443 any
deny tcp any any eq 8443
deny tcp any eq 8443 any
deny tcp any any eq 6970
deny tcp any eq 6970 any
deny tcp any any eq 689
deny tcp any eq 689 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.


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.

Parameter	CVD values first ANC	CVD values second ANC	Site-specific values
Switch interface numbers	1/0/19	1/0/20	
	2/0/19	2/0/20	
Switch port-channel number	9	10	
VLAN number	350	350	
VLAN name (optional)	WAN_Service_Net	WAN_Service_Net	
AppNav controller interface numbers	1/0 1/1	1/0 1/1	
AppNav controller port-channel number (for intra-cluster traffic and management)	1	1	
Time zone	PST8PDT -8 0	PST8PDT -8 0	
IP address	10.4.32.163/26	10.4.32.164/26	
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-APPNAV-1	WAVE-APPNAV-2	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS shared key (optional)	SecretKey	SecretKey	

Table 13 - C	Cisco AppNav	controller WAN	service network	parameters
--------------	--------------	----------------	-----------------	------------

Table 14 - Cisco AppNav controller intercept network parameters

Parameter	CVD values primary ANC	CVD values secondary ANC	Site-specific values
AppNav interception network switch interface numbers	1/0/21 2/0/21	1/0/22 2/0/22	
Switch port-channel number	11	12	
VLAN number	349	349	
VLAN name (optional)	AppNav_Intercept_Network	AppNav_Intercept_Network	
AppNav controller interface numbers	1/2 1/3	1/2 1/3	
AppNav controller port- channel number	2	2	
IP address	10.4.32.71/26	10.4.32.72/26	
Intercept network router	10.4.32.65	10.4.32.65	
WCCP routers	10.4.32.2 10.4.32.6 10.4.32.18	10.4.32.2 10.4.32.6 10.4.32.18	
WCCP password	c1sco123	c1sco123	

Procedure 1 Configure switch for WAVE appliances

The distribution switch is the appropriate location to physically connect the Cisco AppNav controller WAVE appliances at the WAN-aggregation site. This guide does not include details for deploying AppNav controllers at 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.

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 Campus Wired LAN Technology Design Guide.

Step 1: If the VLANs do not already exist on the distribution-layer switch, configure them now.

vlan 350
name WAN_Service_Net
vlan 349
name AppNav_Intercept_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
interface Vlan349
ip address 10.4.32.65 255.255.192
no shutdown

Next, you will configure EtherChannel member interfaces.

Tech Tip

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

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 1/0/19
description Link to AppNav-WAVE port 1/0
interface GigabitEthernet 2/0/19
description Link to AppNav-WAVE port 1/1
T
interface GigabitEthernet 1/0/21
description Link to AppNav-WAVE port 1/2 (Intercept Network)
interface GigabitEthernet 2/0/21
description Link to AppNav-WAVE port 1/3 (Intercept Network)
!
interface range GigabitEthernet 1/0/19, GigabitEthernet 2/0/19
switchport
macro apply EgressQoS
channel-group 9 mode on
logging event link-status
logging event bundle-status
I.
interface range GigabitEthernet 1/0/21, GigabitEthernet 2/0/21
 switchport
macro apply EgressQoS
 channel-group 11 mode on
logging event link-status
 logging event bundle-status
```

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

December 2013

Step 4: Assign the VLANs created at the beginning of this procedure to the interface. When using EtherChannel, the port channel numbers must match the channel groups configured in Step 3.

```
interface Port-channel 9
description EtherChannel link to AppNav-WAVE
switchport access vlan 350
logging event link-status
no shutdown
!
interface Port-channel 11
description EtherChannel link to AppNav-WAVE (Intercept Network)
switchport access vlan 349
logging event link-status
no shutdown
```

Procedure 2 Configure the Cisco AppNav Controller

You can deploy a cluster of Cisco ANCs 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 and use generic GRE tunnels in order to communicate with the WCCP routers. If you don't want resiliency for AppNav at the WAN-aggregation site, you can deploy a single ANC, instead of a cluster. A detailed example topology is shown in the following figure.



You use the same setup utility that you used in the initial configuration of the Cisco WAAS Central Manager to set up ANCs. 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 ANC requires terminal access to the console port for basic configuration options and IP address assignment.

The setup utility configuration steps for the ANCs are similar to the setup of the Cisco WAAS Central Manager, but the steps begin to differ after you choose Cisco AppNav Controller as the device mode. After you choose this mode, the setup script changes in order to allow you to complete the configuration as an ANC.

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 0/0
5.	Autosense	Enabled
6.	DHCP	Enabled
ESC	Quit ? Help ———	WAAS Default Configuration
Pre	ss y' to select above def	aults, `n' to configure all, <1-6> to change
spe	cific default [y]: n	

Step 2: Configure the appliance as a Cisco AppNav controller.

```
1. Application Accelerator
2. AppNav Controller
3. Central Manager
Select device mode [1]: 2
Device Mode AppNav Controller selected in SETUP; New configuration takes effect
after a reload. If applicable, AppNav Controller I/O Module is recognized after
the reboot. Re-run Setup CLI to perform AppNav Controller related configuration
post reboot. Initiate system reload? <y/n> [n] y
Are you sure? <y/n> [n]:y
```

Step 3: After the system reloads, log in to the device again and then, from the command line, enter **setup**. The Cisco AppNav Controller setup utility starts.

Parameter	Default Value
1. Device Mode	AppNav Controller
2. Interception Method	Inline
3. Time Zone	UTC 0 0
4. Management Interface	GigabitEthernet 0/0
5. Autosense	Enabled
6. DHCP	Enabled
ESC Quit ? Help	WAAS Default Configuration
Press 'y' to select above def	aults, 'n' to configure all, <1-6> to change
specific default [y]: n	

Step 4: Configure the appliance as a Cisco AppNav Controller.

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

Step 5: Configure the interception method.

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

Step 6: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)> [UTC 0 0]:
PST8PDT -8 0
```

Step 7: Configure the management interface, IP address, and default gateway.

No.	Interface Name	IP	Address	Network	Mask
1.	GigabitEthernet 0/0		dhcp		
2.	GigabitEthernet 0/1		unassi	gned	
3.	GigabitEthernet 1/0	unassigned			
4.	GigabitEthernet 1/1	unassigned			
5.	GigabitEthernet 1/2		unassi	gned	
6.	GigabitEthernet 1/3		unassi	gned	
7.	GigabitEthernet 1/4		unassi	gned	
8.	GigabitEthernet 1/5		unassi	gned	
9.	GigabitEthernet 1/6		unassi	gned	
10.	GigabitEthernet 1/7		unassi	gned	
11.	GigabitEthernet 1/8		unassi	gned	
12.	GigabitEthernet 1/9		unassi	gned	
13.GigabitEthernet 1/10			unassi	gned	
14.GigabitEthernet 1/11			unassi	gned	
Pres	s <any key=""> to close</any>				

```
Select Management Interface [14]: 3
Enable Autosense for Management Interface? (y/n)[y]: y
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]: 10.4.32.163/26
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 8: 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): AppNav-WAVE-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

Step 9: 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 10: Verify the configuration settings.

```
Parameter
                             Configured Value
 1. Device Mode
                              AppNav Controller
 2. Interception Method
                              WCCP
 3. Time Zone
                              PST8PDT -8 0
 4. Management Interface
                              GigabitEthernet 1/0
 5.
       Autosense
                                 Enabled
 6.
       DHCP
                                 Disabled
 7.
                                 10.4.32.163
      IP Address
      IP Network Mask
                                 255.255.255.192
 8.
 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
                              AppNav-WAVE-1
14. NTP Server Address
                              10.4.48.17
15. License
                              Enterprise
ESC Quit ? Help ! CLI ------ WAAS Final Configuration -----
Press 'y' to select configuration, \langle F2 \rangle to see all configuration, 'd' to toggle
defaults display, <1-16> to change specific parameter [y]: y
Service Context configuration, including interception settings, must be performed
using central manager .....
Please press ENTER to continue ...
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
WAAS configuration applied successfully !!
Saved configuration to memory.
Press ENTER to continue ...
```

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 10.4.32.163 255.255.255.192
exit
!
primary-interface PortChannel 1
!
interface PortChannel 1
ip address 10.4.32.163 255.255.255.192
exit
```

```
!
interface GigabitEthernet 1/0
channel-group 1
exit
interface GigabitEthernet 1/1
channel-group 1
no shutdown
exit
```

Step 12: Configure the port-channel connection for the AppNav intercept network.

```
interface PortChannel 2
ip address 10.4.32.71 255.255.255.192
exit
!
interface GigabitEthernet 1/2
channel-group 2
no shutdown
exit
interface GigabitEthernet 1/3
channel-group 2
no shutdown
exit
```

Step 13: Configure static routes for the WAN-aggregation routers.

ip route 10.4.32.2 255.255.255.255 10.4.32.65 ip route 10.4.32.6 255.255.255.255 10.4.32.65 ip route 10.4.32.18 255.255.255.255 10.4.32.65

Next, you configure device management protocols.

Step 14: Generate the RSA key and enable the sshd service. This enables SSH.

ssh-key-generate key-length 2048
sshd enable
no telnet enable

Step 15: 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 16: 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
exit
!
interface PortChannel 2
ip access-group 155 in
exit
!
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
snmp-server access-list 55
```

Step 17: 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

1

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

copy running-config startup-config

Step 19: If your Cisco AppNav cluster includes more than one Cisco AppNav controller WAVE, repeat Step 1 through Step 19 for the resilient appliance.

Procedure 3 Configure the AppNav cluster

This procedure is used to create the cluster and assign Cisco WAAS nodes.

i	Tech Tip
configu	ocedure assumes that one or more Cisco WAAS nodes have already been ired and are registered to the WAAS Central Manager. Any existing WCCP iration on the WAAS nodes is overwritten by this procedure.

Step 1: Log in to the Cisco WAAS Central Manager through the web interface (for example, https://waas-wcm-1. cisco.local:8443).

Step 2: Navigate to AppNav Clusters > All AppNav Clusters.

Cluster Wizard - Deployment model	×
Choose one of the four platform types.	
AppNav platform: WAVE Appliance Choose one of the four pre-defined deployment models or Custom model. Deployment model: Single AppNav Controller WCCP interception Network topology diagram for selected deployment model: WAN	Cluster Creation Progress Deployment model Cluster settings Device Selection
Controller UNAAS Nodes	Current Step Summary
	Back Next Finish Cancel

Step 3: Start the configuration by starting the AppNav Cluster Wizard.

Step 4: Set the AppNav platform to WAVE Appliance, the Deployment model to Custom, and the Interception method to WCCP, and then click Next.

Cluster Wizard - Deployment model	×
Choose one of the four platform types.	
AppNav platform: WAVE Applance Choose are of the four pre-defined deployment models or Custom model. Deployment model: Custom Interception method: WCCP	Cluster Creation Progress Peployment model Cluster settings Clevice Selection
	Current Step Summary
	Complete AppNav platform: WAVE Appliance Deployment model: Custom Interception method: WCCP
	Back Next Frish Cancel

Step 5: Assign the Cluster Name to AppNav-IOM, add a description, and then click Next.

Cluster Wizard - Cluster settings	х
Configure AppNav Cluster settings.	
Cluster Name: * AppNav-IOM Description: AppNav I/O Module Cluster By default newly created cluster will be operational immediately,disabiling distribution will put cluster in monitoring mode (intercepted traffic is not optimized but is passed through) Disable distribution	Cluster Creation Progress ✓ Deployment model ✓ Cluster settings xr Device Selection
	Current Step Summary Complete Name: AppNav-IDM Active: Yes
	Back Next Finish Cancel

Step 6: Select the Cisco AppNav controllers to assign to the AppNav cluster under configuration. If you would like to use the AppNav controllers in a dual role of AppNav Controller and Application Accelerator, then also select **Enable WAN optimization on selected AppNav Controller(s)**.

If necessary, add additional dedicated Application accelerator Cisco WAAS nodes by selecting the WAAS nodes (Example: WAE-7341-1), and then clicking **Next**.

ect up to 8 AppNav Contro	ollers		Show All	- 7	Cluster Creation Progress
Name	Device Model	IP Address	Location		🔆 AppNav-IOM
AppNav-WAVE-1	OE7571	10.4.32.163	Primary Site		✓ Deployment model
AppNav-WAVE-2	OE7541	10.4.32.164	Primary Site		 Cluster settings
Enable WAN optimization	on selected AppNav C	ontroller(s)			
Enable WAN optimization of ect up to 32 WAAS Nodes			Show All	• 8	
			Show All		Current Step Summary
ect up to 32 WAAS Nodes Name	that are in this location	n or datacenter	Location	- S	
ect up to 32 WAAS Nodes Name KSZ31-WAE-SKE	Device Model	IP Address	Location KS231		Complete AppNav Controller(s): AppNav-WAVE-1
ect up to 32 WAAS Nodes Name R5231-WAE-5RE R5232-WAVE294-1	that are in this locatic Device Model SM-WAE OE294	IP Address 10.3.204.8 Unconfigured	Location K5231 RS232		Complete AppNav Controller(s): AppNav-WAVE-1 AppNav-WAVE-2
ect up to 32 WAAS Nodes Name KSZ51-WAE-SKE RS232-WAVE294-1 RS232-WAVE294-2	Device Model SM-WAE OE294 OE294	IP Address IV.5.204.8 Unconfigured 10.5.215.9	Location r5231 R5232 R5232		Complete AppNav Controller(s): AppNav-WAVE-1 AppNav-WAVE-2 WAAS Node(s): WAE-7341-1
ect up to 32 WAAS Nodes Name RS251-WAE-SRE RS232-WAVE294-1 RS232-WAVE294-2 WAE-7341-1	that are in this location Device Model Sm-wAE OE294 OE294 OE7341	IP Address 10.5.204.8 Unconfigured 10.5.215.9 10.4.32.161	Location N5231 RS232 RS232 Primary Site		Complete AppNav Controller(s): AppNav-WAVE-1 AppNav-WAVE-2 WAAS Node(s): WAE-7341-1

Step 7: Select **Enable WCCP Service**, clear **Enable Single Service Mode**, verify that Service ID1: is set to 61, set the Redirect Method to **WCCP GRE**, and then enter the IP addresses for the WCCP Routers (Example from Table 14: 10.4.32.2 10.4.32.6 10.4.32.18).

Step 8: Expand **Advanced WCCP settings** by clicking it, set the Password and the Confirm Password (Example from Table 14: c1sco123), and then click **Next**.

Cluster Wizard - WCCP se	ttings		x
Configure WCCP settings for App	Nav Controller AppNav-WAVE-1.		
Enable WCCP Service Enable Single Service Mod Service ID1: Service ID2: Redirect Method: Use default gateway as W	61 (1-99) 62 WCCP GRE ▼	*	Cluster Creation Progress AppNav-IDM Depiopment model Custer settings Device Selection WCCP settings for AppNav-WAVE-2
WCCP Routers: * Advanced WCCP settings	10.4.32.2 10.4.32.6 10.4.32.18 (Router List Index = 1)	E	 Cluster Interface for AppNav-WA Cluster Interface for AppNav-WA Cluster Interface for WAE-7341-1
	CP password and other settings		Current Step Summary
Password: Confirm Password:	••••••		Complete
Configure WCCP Assignment S	Settings for Load Balancing		
Source IP Mask:	f (Hex String)		
Destination IP Mask:	0 (Hex String)		
Failure Detection Timeout:	30		
Weinht:	0 (0-10000)	*	
			Back Next Finish Cancel

Step 9: If necessary, repeat Step 7 and Step 8 for additional AppNav controllers.



Step 10: Set the Cluster Interface (Example: PortChannel 1), and then click Next.

Step 11: Repeat Step 9 for all remaining cluster members (Cisco AppNav controllers and Cisco WAAS nodes), and then click **Finish**.

Next, configure authentication within the cluster.

Step 12: Navigate to AppNav Clusters > AppNav-IOM, enter a value for the Authentication key: and Confirm authentication key: (Example c1sco123), and then click Submit.

🔆 Cluster Settings	AppNav Controllers	MAAS Nodes	🟹 WAAS Node Groups
Name: *	AppNav-IOM		
Description:	AppNav I/O Module Clus	ter	
Authentication key:	•••••		
Confirm authentication key:	•••••		
Shutdown Wait Time: *	120	(0-86400) s	econds
Submit Reset			

Procedure 4 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 MPLS WAN Technology Design Guide or VPN WAN Technology Design Guide.

In this design, WCCP diverts network traffic destined for the WAN to the Cisco AppNav controller group for optimization. This method provides for a clean deployment with minimal additional cabling, and it requires both the WAN-aggregation 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 Cisco AppNav Controllers in the group list in order to prevent the use of unauthorized controllers.

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 and other protocols which can not be optimized from WCCP redirect by using a redirect list. A detailed listing is included in Table 11 and Table 12.

```
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list APPNAV password clsco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list APPNAV password clscol23
ip access-list standard APPNAV
permit 10.4.32.71
permit 10.4.32.72
1
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 any eq telnet
deny tcp any eq telnet any
deny tcp any any eq tacacs
deny tcp any eq tacacs any
deny tcp any any eq bgp
deny tcp any eq bgp any
```

deny	tcp	any	any eq 123
deny	tcp	any	eq 123 any
deny	tcp	any	any eq 161
deny	tcp	any	eq 161 any
deny	tcp	any	any eq 162
deny	tcp	any	eq 162 any
deny	tcp	any	any eq 2000
deny	tcp	any	eq 2000 any
deny	tcp	any	any eq 2443
deny	tcp	any	eq 2443 any
deny	tcp	any	any eq 5060
deny	tcp	any	eq 5060 any
deny	tcp	any	any eq 5061
deny	tcp	any	eq 5061 any
deny	tcp	any	any eq 1718
deny	tcp	any	eq 1718 any
deny	tcp	any	any eq 1720
deny	tcp	any	eq 1720 any
deny	tcp	any	any eq 2428
deny	tcp	any	eq 2428 any
deny	tcp	any	any eq 443
deny	tcp	any	eq 443 any
deny	tcp	any	any eq 8443
deny	tcp	any	eq 8443 any
deny	tcp	any	any eq 6970
deny	tcp	any	eq 6970 any
deny	tcp	any	any eq 689
deny	tcp	any	eq 689 any
perm	it t	сра	ny any

Step 2: Configure the generic GRE tunnel for return traffic from the Cisco AppNav controller group. You must use the LAN facing interface as the tunnel source.

Tech Tip

i

The IP address assigned to the tunnel interface is arbitrary. Cisco recommends that you use addresses assigned from the 192.0.2.0/24 network. Choose a tunnel number that is not already in use on your router.

```
interface Tunnel5
description GRE tunnel for AppNav OffPath devices
ip address 192.0.2.1 255.255.255.0
no ip redirects
ip wccp redirect exclude in
tunnel source Port-Channel1
tunnel mode gre multipoint
end
```

Step 3: 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.

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

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

Step 4: 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 5: 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 6: After you make configuration changes, save the configuration.

copy running-config startup-config

Step 7: 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.

Step 8: Log in to the Cisco WAAS Central Manager through the web interface (for example, https://waas-wcm-1. cisco.local:8443).

Step 9: Navigate to AppNav Clusters > AppNav-IOM and verify that the AppNav cluster is operational.



Configuring AppNav-XE on a WAN-Aggregation Router

- 1. Create a WAAS Central Manager user
- 2. Register the router to the WAAS Central Manager
- 3. Configure the AppNav-XE Cluster

Procedure 1 Create a WAAS Central Manager user

There are two options when you are creating the Cisco WAAS Central Manager account. If you want to create the account locally on each Cisco AppNav controller 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 Cisco WAAS Central Manager user.

PROCESS

December 2013

Option 1: Create a local user account

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

username waascm privilege 15 password clscol23

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 waascm and password c1sco123)

Users and Identity Stor	es > Internal	Identity Stores > Use	ers ≻ Creat	e				
General								
o Name:	waascm		Status:	Enabled 👻	0			
Description:	WAAS Cer	ntral Manager user						
🗢 Identity Group:	All Groups			Sele	ect			
Password Info Password must:		cters				Enable Password In Password must • Contain 4 - 32		
Password Typ	e:	Internal Users		S	elect	Enable Password:		
Password:		•••••				Confirm Password:	:	
Confirm Pass	word:	•••••						
🗖 Change p	assword or	n next login						
User Informatio There are no a		entity attributes def	ined for us	ser records				
Required field	ds							
 ≺ Cance 	1							
Cance								

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

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

dentity Groups	
Filter: 📃 Mato	th if: Go 🔻
Name 🔺	
C 🔻 All Groups	Identity Group Root
C Helpdesk	Users who are allowed to login to a device but not make changes
 Network Admins 	Users who are allowed to login to a device and make changes
Create Duplicate [File Operations Export
OK Cancel	Hel

Step 7: Click Submit.

Procedure 2 Register the router to the WAAS Central Manager

Step 1: Verify SSH and HTTPS servers are enabled on the router. If not already configured, configure these services now.

00	Reader Tip
and Te	HATTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP Inet protocols. They use Secure Sockets Layer (SSL) and Transport Layer ty (TLS) to provide device authentication and data encryption.
and HT	e management of the network device is enabled through the use of the SSH TTPS protocols. Both protocols are encrypted for privacy and the nonsecure ols, Telnet and HTTP, are turned off.

Specify the transport preferred none on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
no ip http server
ip http secure-server
line vty 0 15
transport input ssh
transport preferred none
```

Step 2: If you are using AAA authentication, configure the HTTP server to use AAA.

ip http authentication aaa

Step 3: Log in to the Cisco WAAS Central Manager through the web interface (for example, https://waas-wcm-1. cisco.local:8443).

սիսիս				Home Device Groups Devices AppNav Clusters Locations	admin Logout Help About
cisco Cisco W	/ide Area Appli	cation Services		Dashboard Configure 💌 Monitor 💌 Admin 💌	
Home > Admin > Registratio		ers			
Cisco IOS Router Registr	ration				
Router IP address entr	y method: 💿	Manual 🔿 Import	CSV file		
IP Address(es):				Comma separated list up to 50 entries	
Username:					
Password:					
Enable Password:					
HTTP Authentication	Type: Loc	al	-		
Central Manager IP Ad	dress: * 10	.4.48.100		$\ensuremath{}$ Update the Central Manager IP Address if NATed environment is used.	
(i) SSH v1 or SSH v2 m					
		-		in should have the same credentials. ral Manager and the routers after registration finishes.	
	re not used for tu	uninunication betw	een trie cent	rai Manager and the routers after registration inishes.	
Register Retry	Reset				
Registration Status					Total 0
IP Address	Hostname	Router type	Status		
				No data available	

Step 4: Navigate to Admin>Registration>Cisco IOS Routers.

Step 5: Enter the management information of the WAN-aggregation routers running Cisco AppNav-XE, and then click **Register**. You may enter the IP addresses of multiple routers (separated by a comma) if they share the same authentication credentials.

- Router IP address entry method-Manual
- IP Address(es)-10.4.32.245
- Username-waascm
- · Password-c1sco123
- Enable Password-c1sco123
- HTTP Authentication Type-AAA
- Central Manager IP Address-10.4.48.100

altalta cisco Cisco	Wide Area Ap	plication Services		Groups Devices AppNav Clusters onfigure∣▼ Monitor∣▼ Admin		admin Logout Help About
Home > Admin > Registra		touters				
Cisco IOS Router Regi	stration					
Router IP address er	itry method:	⊙ Manual () Impor	t CSV file			
IP Address(es):		10.4.32.245		① Comma separated list up t 	o 50 entries	
Username:	[waascm				
Password:	[•••••				
Enable Password:	[•••••				
HTTP Authentication	n Type: [AAA	•			
Central Manager IP A	ddress: * [10.4.48.100	① Update the Cen	ral Manager IP Address if NATed envi	ronment is used.	
③ SSH v1 or SSH v2	must be enable	d on routers.				
		-	d routers, which should have the sar			
 These credentials 	are not used fo	r communication betw	ween the Central Manager and the r	uters after registration finishes.		
Register Retry	Reset					
Registration Status	Hostname	Router type	Status			
IP Address	mustriame	Router type	Status		No data available	

Step 6: Verify successful registration.

Registration Status			
IP Address	Hostname	Router type	Status
10.4.32.245	METRO-ASR1001-1	AppNav-XE Controller	\checkmark Successfully processed the registration request

Step 7: If necessary, repeat Step 5 and Step 6 for additional routers.

Procedure 3	Configure	the Appl	Vav-XE	Cluster
-------------	-----------	----------	--------	---------

This procedure is used to create the cluster and assign Cisco WAAS nodes.



Step 1: Log in to the Cisco WAAS Central Manager through the web interface (for example, https://waas-wcm-1. cisco.local:8443).

Step 2: Navigate to AppNav Clusters > All AppNav Clusters.

Cluster Wizard - Deployment model × Choose one of the four platform types AppNav platform: * WAVE Appliance **Cluster Creation Progress** Choose one of the four pre-defined deployment models or Custom model. Deployment model
 Cluster settings
 Device Selection Deployment model: * Single AppNav Controller WCCP interception 💌 Network topology diagram for selected deployment model: WAN \geq Current Step Summary AppNav LAN 📀 Complete AppNav platform: WAVE Appliance Deployment model: Single AppNav Controller WCCP interception Cluster interface Back Next Finish Cancel

Step 3: Start the configuration by clicking on the AppNav Cluster Wizard.

Step 4: Set the Cisco AppNav platform to ASR 1000 Series, and then click Next.

i	Tech Tip
You m	AppNav-XE clusters may include routers only within the same product family. hay not mix Cisco ASR 1000 Series routers with Cisco ISR 4451-X routers within ame cluster.

Cluster Wizard - Deployment model	×
Choose one of the four platform types.	
AppNav platform: * ASR 1000 Series Typical network: topology diagram for selected AppNav-XE platform:	Cluster Creation Progress Cluster Setings 2 Cluster settings 2 Cluster Selection Current Step Summary Current Step Summary Complete AppNav platform: ASR 1000 Series Bad Nett Pridh Cancel

Step 5: Assign the Cluster Name to AppNav-XE, and then add a description.

Step 6: Select the default setting of waas/1 for the WAAS Cluster ID, and then click Next.

Cluster Wizard - Cluster settings	×
Configure AppNav Cluster settings.	
Cluster Name: * AppNav-XE Description: AppNav on IOS-XE Cluster WAAS Cluster Id: * waas/1	Cluster Creation Progress
	Current Step Summary Complete Name: AppNav-XE WAAS Cluster Id: waas/1 Active: Yes
	Back Next Finish Cancel

Step 7: Select Cisco AppNav-XE controllers (maximum of 4) to assign to the AppNav cluster under configuration.

Step 8: Add application accelerator Cisco WAAS nodes by selecting the WAAS nodes (Example: WAE-7341-2). After selecting all devices, click **Next**.

elect up to 4 AppNav-XEs			Show All	- 8	Cluster Creation Progress
Name	Device Model	IP Address	Location		🔆 AppNav-XE
METRO-ASR1001-1	ASR1001	10.4.32.245	Primary Site		Deployment model
VPN-ASR1001-2	ASR1001	10.4.32.244	Primary Site		🖌 Cluster settings
					Device Selection
Select up to 32 WAAS Nodes			Show All	• 8	
Select up to 32 WAAS Nodes	Device Model	IP Address	Location		Current Sten Summary
Name				v 5	Current Step Summary
Name K5212-WAVE574	Device Model UE574	IP Address 10.5.1/5.8	Location R5212		Current Step Summary Complete AppNav Controller(s);
Name R5212-WAVE574 R5213-WAVE574	Device Model UE5/4 OE574	IP Address 10.5.175.8 10.5.180.8	Location K5212 R5213		Complete
Name R5212-WAVE574 R5213-WAVE574 R5231-WAVE574	Device Model UE374 OE574 SM-WAE	IP Address 10.5.175.8 10.5.180.8 10.5.204.8	Location K5212 RS213 RS231		Complete AppNav Controller(s):
Name K5212-WAVE574 RS213-WAVE574 RS231-WAE-SRE RS232-WAVE294-1	Device Model UE374 OE574 SM-WAE OE294	IP Address 10.5.1/5.8 10.5.180.8 10.5.204.8 10.5.215.8	KS212 RS213 RS231 RS232		Complete AppNav Controller(s): METRO-ASR1001-1

Step 9: Clear VRF default, select VRF global, and then click Next.

Cluster Wizard - VRF Selection			×
Select $VRF(s)$ that will be associated with	the current context - waas/1		
Common VRF(s) from all AppNav-XE Cont	rollers Show A	- 7	Cluster Creation Progress
VRF		,	🔆 AppNav-XE
VRF default VRF global Ineligible VRFs	show A		Deployment model Oluster settings Device Selection VRF Selection Interception/Cluster Interface for M Interception/Cluster Interface for VP Ouster Interface for WAE-7341-2 Current Step Summary
			Complete
VRF Reasons	to managment interface.		VRF(s):
VRF Reasons 1 Mgmt-intf Assigned	I to managment interface. ent on all AppNav-XE Controllers. Available on: [VPN-ASR16	,	
VRF Reasons 1 Mgmt-intf Assigned		,	VRF(s):

Step 10: Select all WAN-facing interfaces for interception, select the LAN-facing interface as the Cluster Interface for intra-cluster traffic, and then click **Next**. Example settings are shown in the following table.



Table 15 - Example Settings for Interception and Cluster Interfaces

Router	WAN transport	Interception interface(s)	Cluster Interface
CE-ASR1002X-1	MPLS-A	Gig0/0/3	Port-Channel1
CE-ASR1001-2	MPLS-B	Gig0/0/3	Port-Channel2
VPN-ASR1002X-1	DMVPN-1	Tunnel10	Port-Channel3
VPN-ASR1001-2	DMVPN-2	Tunnel10	Port-Channel4
METRO-ASR1001-1	Layer 2 WAN	Gig0/0/3.38	Port-Channel5
		Gig0/0/3.39	

nfigure interception inter	face to intercept optimiza	ition traffic and clu	ster interface on METRO	-ASR1001-1 AppN	av-XE that will be us	ed for intra-cluster traffic.
elect WAN interface(s) (on which data path interc	eption to be enab	led.		Selected 2 Total 4	Cluster Creation Progress
			Show	All	- 5	🔆 AppNav-XE
Interface Name Gi0/0/3.38 Gi0/0/3.39 Loopback0 Port-channel5	Address 10.4.38.1 10.4.39.1 10.4.32.245 10.4.32.34	Status UP UP UP UP	Service Insertion Enabled Disabled Disabled			Deployment model Cluster settings Device Selection VRF Selection Interception/Cluster Interface for Interception/Cluster Interface for Cluster Interface for WAE-7341-2
Cluster Interface: Por	ace that will be used for ir t-channe!5 eligible to be selected as i	•	r interface Show ineligib	ole interfaces		Current Step Summary
						WAN Interface(s): Gi0/0/3.38 Gi0/0/3.39 Cluster Interface: Port-channel5
						< •

Step 11: If necessary, repeat Step 10 for any additional Cisco AppNav-XE controller routers.

Step 12: Select the Cluster Interface for the Cisco WAAS node to use for intra-cluster traffic (Example: PortChannel 1). If this is the last WAAS node, click **Finish**, otherwise click **Next**.

Cluster Wizard - Cluster Interface	×
Select Cluster Interface on WAE-7341-2 WAAS Node that will be used for intra-cluster traffic. You can increase port capacity by using F by using Standby Group(s).	Port Channel(s) and/or add interface failover
Right click on an interface to get started.	Cluster Creation Progress
😢 Add 👻 🥖 Edit 🗙 Delete 👻	🔆 AppNav-XE
	Deployment model Custer settings Device Selection VRF Selection VRF Selection Interception/Custer Interface for M Interception/Custer Interface for VP Custer Interface for WAE-7341.2
	Current Step Summary
PortChannel 1	3 WAE-7341-2
Select the Ouster Interface that will be used for intra-cluster traffic. Ouster Interface: * PortChannel 1	Curplete Cluster Interface: PortChannel 1 IP Address: 10.4.32.162
	Back Next Finish Cancel

Step 13: Repeat Step 12 for any additional WAAS nodes if necessary.

Step 14: Navigate to **AppNav Clusters > AppNav-XE**, enter a value for the **Authentication key** and **Confirm authentication key** (Example c1sco123), and then click **Submit**. Authentication with the cluster is configured.

🔅 Cluster Settings	AppNav Contexts	AppNa	av Controllers	► WAAS Nodes	WAAS Node Groups
Authentication key:	•••••]		
Confirm authentication key:	•••••]		
Shutdown Wait Time: *	120		(0-86400) second	ls	
Submit Reset					

Step 15: Navigate to AppNav Clusters > AppNav-XE and verify that the Cisco AppNav cluster is operational.

The default Cisco AppNav policy includes video acceleration and the Cisco WAAS Central Manager indicates that the AppNav cluster is degraded if any of the WAAS nodes do not have a video license.



Next, if the Cisco WAAS nodes do not have a video license, disable video acceleration for the Cisco AppNav-XE cluster by following Step 16 through Step 19.

Step 16: If the cluster is not already selected, navigate to AppNav Cluster > AppNav-XE, select the cluster, and then navigate to Configure>AppNav Policies.

App!	-		devices in a context will I	be same							Selected 1 Tot.	tal
		/ Edit 🗙 Delete	Unassign Policy						Show	Al		7
	Name		Description	AppNay Contex	ts	AppNav Con	trollers			L		
1 (V-1-PMAP		waas/1		VPN-ASR100	1-2, METRO-ASR100)1-1				
		· · ·	idit 🗙 Delete 📑 Move						Show	L	•	9
		e ee Insert / E Class-Map	dit X Delete SS Move Source IP	to 🔹 🤟 🌴 🛗 Destination IP	Save Moved Rows Destination P	Protocol	Remote Devices	Distribute		All	•	4
	Position	· · ·				Protocol mapi	Remote Devices	Distribute WNG-Def	То	L	•	ę
9 A	Position 1	Class-Map	Source IP any	Destination IP any	Destination P		Remote Devices		To ault-1	Monitor	T	4
	Position 1 2	Class-Map MAPI	Source IP	Destination IP	Destination P		Remote Devices	WNG-Def	To ault-1 ault-1	Monitor MAPI Accelerator	•	4
	Position 1 2 3	Class-Map MAPI HTTPS	Source IP any any any any any any	Destination IP any any any any any any	Destination P 443 www 3128 8000 8080		Remote Devices	WNG-Def- WNG-Def-	To ault-1 ault-1	Monitor MAPI Accelerator SSL Accelerator		
	Position 1 2 3 4	Gass-Map MAPI HTTPS HTTP	Source IP any any any any any any any any	Destination IP any any any any any any any any	443 www 3128 8000 8080 8080 8088 139		Remote Devices	WNG-Def	To ault-1 ault-1 ault-1	Monitor MAPI Accelerator SSL Accelerator HTTP Accelerator		
	Position 1 2 3 4 5	Class-Map MAPI HTTPS HTTP CLIFS	Source IP any any any any any any any any any any	Destination IP any any any any any any any any any any	443 WWW 3128 8000 8080 8088 139 445		Remote Devices	WNG-Def- WNG-Def- WNG-Def-	To ault-1 ault-1 ault-1 ault-1	Monitor MAPI Accelerator SSL Accelerator HTTP Accelerator		
	Position 1 2 3 4 5 6	Class-Map MAPI HTTPS HTTP CIFS Citris-ICA	Source IP any any any any any any any any any any	Destination IP any any any any any any any any any any	Destination P 443 www 3128 8080 8080 8088 139 445 1494		Remote Devices	WNG-Def	To To ault-1	Monitor MAPI Accelerator SSL Accelerator HTTP Accelerator CIFS Accelerator ICA Accelerator	•]	q
	Position 1 2 3 4 5 6 6 7	Class-Map MAPI HTTPS HTTP CIFS Cltric-ICA Cltric-ICA Cltric-CGP	Source IP any any any any any any any any any any	Destination IP any any any any any any any any any any	Destination P 443 www 3128 8000 8088 139 445 1494 2598 2049 2049		Remote Devices	WNG-Defa WNG-Defa WNG-Defa WNG-Defa WNG-Defa	To To ault-1	Monitor MAPI Accelerator SSL Accelerator HTTP Accelerator CIFS Accelerator ICA Accelerator ICA Accelerator	•]	
	Position 1 2 3 4 4 5 6 6 7 7 8	Class-Map MAPI HTTPS HTTP CIFS Cltric-ICA Cltric-ICA Cltric-CGP epmap	Source IP any any any any any any any any any any	Destination IP any any any any any any any any any any	Destination P 443 www 3128 8000 8080 8088 139 445 1494 2598 msrpc		Remote Devices	WNG-Def	To T	Monitor MAPI Accelerator SSL Accelerator HTTP Accelerator CIFS Accelerator ICA Accelerator ICA Accelerator ICA Accelerator MS PortMapper	• • •	~

Step 17: In the lower pane, select the policy rule with the Monitor assigned to Video Accelerator (Example: Position 9 – RTSP), then click **Edit**.

Step 18: Change the setting for Monitor to None, click OK, and then accept the warning message by clicking OK again.

AppNav Policy Rule		×
AppNav Class-Map: *	RTSP 💌	Edit Create New
AppNav Action		
Distribute To:	WNG-Default-1	Create New
Monitor: *	None	
		OK Cancel

Step 19: Navigate to **AppNav Clusters > AppNav-XE** and verify that the Cisco AppNav cluster is now operational. Expect a short delay for the new status to be reflected.

alialia	Home Device G	roups Devices	AppNav Clusters	Locations
CISCO Cisco Wide Area Application Services	AppNav-XE 🔻	Configure 🔻	Monitor 🔻	
AppNav Clusters > AppNav-XE > AppNav Cluster Home				
🗳 Print 🔍 🔍				
AppNav Cluster is operational				
METRO-ASK1001-1 WMG-Default-1 WAE-7341-2 VPN-ASK1001-2				

PROCESS

Preparing the Cisco UCS E-Series module for vWAAS

- 1. Configure remote switch for Cisco UCS E-Series
- 2. Configure the Cisco Integrated Management Controller
- 3. Configure UCS E-Series using CIMC
- 4. Configure RAID Using CIMC GUI

CO Reader Tip

This process must be combined with the Install VMware ESXi on the Cisco UCS E-Series module process and the Configuring Cisco vWAAS on the UCS E-Series module process to complete the full installation and configuration of Cisco vWAAS on the UCS E-Series.

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 vWAAS running on the Cisco UCS E-Series module. For your convenience, you can enter your values in the table and refer to it when configuring the UCS E-Series module. The values you enter will differ from those in this example, which are provided for demonstration purposes only.

Parameter	CVD values for an access-layer connection	CVD values for a distribution-layer connection	Site-specific values
In-band management network	10.5.180.0/24 (existing data subnet)	10.5.168.16/29 (new subnet for UCS E management)	
UCS E-Series interface address	unnumbered gig0/2.64	10.5.168.17/29	
Cisco IMC interface address	10.5.180.10/24	10.5.168.18/29	
VMware ESXi interface address	10.5.180.11/24	10.5.168.19/29	
Switch interface number	0/22	1/0/7	
VLAN number	64	106	
Time zone	PST8PDT -8 0	PST8PDT -8 0	
IP address	10.5.180.8/24	10.5.175.8/24	
Default gateway	10.5.180.1/24	10.5.175.1/24	
WAAS Central Manager	10.4.48.100	10.4.48.100	
Hostname	RS213-vWAAS	RS212-vWAAS	
IP addresses of routers intercepting traffic with WCCP	10.255.255.213	10.255.255.212	
WCCP password	c1sco123	c1sco123	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS shared key (optional)	SecretKey	SecretKey	

Table 16 - Cisco vWAAS on the Cisco UCS E-Series module network parameters

Procedure 1 Configure remote switch for Cisco UCS E-Series

The access switch is the appropriate location to physically connect Cisco UCS E-Series 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. At distribution layer sites, the Cisco UCS E-Series module is physically connected to the distribution layer switch.

This guide assumes that the Cisco UCS E-Series module has been installed into the remote-site router and that the LAN switch has already been configured. Only the procedures required to complete the connection of the switch to the UCS E-Series module are included. For details on how to configure switches, see the Campus Wired LAN Technology Design Guide.

Step 1: Connect the Cisco UCS E-Series module's external Ethernet port to an Ethernet port on the remote site's access or distribution layer switch, and then return the switchport configuration to the default.

default interface GigabitEthernet1/0/7

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

```
interface GigabitEthernet1/0/7
description UCS E-Series external port (vWAAS)
switchport access vlan 64
switchport host
ip arp inspection trust
logging event link-status
macro apply EgressQoS
no shutdown
```

Procedure 2 Configure the Cisco Integrated Management Controller

Tech Tip

The UCS E-Series procedures in this guide assume that you are using an ISR G2 2900 series router or ISR G2 3900 series router. The ISR 4451-X router procedure, while similar, is not included in this guide.

The Cisco UCS E-Series module has two internal interfaces on the router. These interfaces are numbered depending on which slot the UCS E-Series module is installed. Interface ucse_/0 represents a routed PCIe interface and interface ucse_/1 represents the multi-gigabit fabric (MGF) interface. This procedure configures the PCIe interface, which is also referred to as the Console interface.

Option 1: Layer 2 access switch

This is the recommended configuration for remote sites with an access layer only.

Perform these steps to set up the Cisco Integrated Management Controller (CIMC) interface.

Step 1: Determine the UCS-E interfaces.

RS213-2911# show	ip interface	brief	includ	e ucse				
ucse1/0	unassigned	YES	unset	administr	atively	down	down	
ucsel/1	unassigned	YES	unset	up	up			



Step 2: Assign an IP address to the router's UCS E-series interface. In this configuration you use **IP unnumbered** to share the IP address assigned to the internal data VLAN. This will be the gateway IP address for the Cisco UCS E-Series CIMC and hypervisor.

```
interface ucse1/0
  ip unnumbered interface GigabitEthernet0/2.64
```

Step 3: Assign an IP address and gateway to the CIMC.

```
interface ucse1/0
imc ip address 10.5.180.10 255.255.255.0 default-gateway 10.5.180.1
```

Tech Tip

Ĩ

If HSRP is configured, do not use the HSRP virtual IP address. Use the real IP address assigned to the interface or subinterface.

Step 4: Configure the CIMC LAN on Motherboard (LOM) for shared access.

```
interface ucse1/0
imc access-port shared-lom console
no shutdown
```

Tech Tip

Shared console access allows this interface to be used for CIMC access and network traffic. Dedicated mode allows only CIMC access.

Step 5: Configure a static host route for the CIMC host via the internal UCS-E interface. ip route 10.5.180.10 255.255.255 ucse1/0 **Step 6:** Configure an additional static host route for the VMware ESXi host that will reside on the same subnet and share the UCS-E console for access.

```
ip route 10.5.180.11 255.255.255.255 ucse1/0
```

Step 7: If this is a dual router remote site, you may need to redistribute the static routes created in Step 5 and Step 6 into the LAN EIGRP process (Example: EIGRP-100).

```
1
        Tech Tip
Each of the two routers includes static routes to the UCS E-Series module. It is not
necessary to redistribute these static routes into the LAN EIGRP process.
    ip route 10.5.180.10 255.255.255.255 ucsel/0
    ip route 10.5.180.11 255.255.255.255 ucse1/0
This type of static route is known as a pseudo-static or pseudo-connected route
because it meets two conditions:
1) The static route points directly to an interface.
2) The destination IP address is contained within an IP range that is referenced by an
EIGRP network statement.
    router eigrp 100
     network 10.5.0.0 0.0.255.255
A pseudo-connected route is treated like a connected route and is automatically
advertised within the EIGRP autonomous system as an EIGRP internal route so no
redistribution is required.
Although the pseudo-connected routes will be automatically brought into the EIGRP
topology and treated similarly to a connected route, EIGRP does not reclassify
the route as a connected. Redistribution of static routes, and then applying
configuration commands (such as route maps) to the redistributed routes will affect
these routes.
```

As a best practice, a route-map with an access-list is used to explicitly list which static routes are redistributed. If static route redistribution is already configured, then redistribution of the pseudo-connected routes is also required. In this case, add a new access-list and the additional clause for the route-map.

If static route redistribution is not already configured, then you may skip this step.

```
ip access-list standard STATIC-ROUTE-LIST
remark UCS-E CIMC & ESXi host routes
permit 10.5.180.10
permit 10.5.180.11
!
route-map STATIC-IN permit 20
match ip address STATIC-ROUTE-LIST
!
router eigrp 100
redistribute static route-map STATIC-IN
```

Next, verify the CIMC configuration.

Step 8: Open a browser window to the CIMC address (example: https://10.5.180.10), enter the factory default username admin and factory default password password, and then click Log In.

	uluili. cisco	Cisco Integrated Management Controller R8240-3045-UC51405 Wenner 14(CarD8022730001)	Usename. Pasaword Log in Cancel
/			

Step 9: If this is the first login to this device, you will be prompted to change the password. Enter a new password (Example: c1sco123), and then click **Save Changes**.

First Login	0
Please change your pase	sword
New Password:	
Confirm New Password:	
	Save Changes Reset Values

Option 2: Layer 3 distribution switch-dedicated UCS-E subnet

This is the recommended configuration for remote sites with a distribution layer.

When connecting to the distribution layer you must assign a dedicated subnet range for Cisco UCS E-Series management. The CIMC and ESXi interfaces are both assigned addresses in this range. The external UCS E-series interface(s) are connected to the LAN for communication between the Cisco vWAAS and the redirecting router.

Perform these steps to set up the CIMC interface.

Step 1: Determine the UCS-E interfaces.

	RS212-2911# show	ip interface	brief	include	e ucse		
	ucse1/0	unassigned	YES	unset	administrat	ively down	down
	ucsel/1	unassigned	YES	unset	up	up	
•	Tech Tip						

This example shows the Cisco UCS E-Series module installed in slot 1 of the router.

Step 2: Assign an IP address to the router's UCS E-series interface. In this configuration you explicitly assign an IP address on the newly assigned subnet range. This will be the gateway IP address for the Cisco UCS E-Series CIMC and hypervisor.

interface ucse1/0 ip address 10.5.168.17 255.255.258.248

Step 3: Assign an IP address and gateway to the CIMC.

interface ucsel/0
imc ip address 10.5.168.18 255.255.255.248 default-gateway 10.5.168.17

Step 4: Configure the CIMC LOM for shared access.

```
interface ucse1/0
imc access-port shared-lom console
no shutdown
```



Next, verify the CIMC configuration.

Step 5: Open a browser window to the CIMC address (example: https://10.5.168.18), enter the factory default username **admin** and factory default password **password**, and then click **Log In**.

	Cisco Integrated Management Controller RozMa3045-VCS1406 Www.ec.tk.481302213009)	Usemanne Password Log in Cancel
1		

Step 6: If this is the first login to this device, you will be prompted to change the password. Enter a new password (Example: c1sco123), and then click **Save Changes**.

First Login	0
Please change your pass	word
New Password:	
Confirm New Password:	
(Save Changes Reset Values

Procedure 3 Configure UCS E-Series using CIMC

Step 1: Verify the server status. From the Server Summary screen you can verify the installed CPU, if the memory and disk are correctly reported, that the correct versions of CIMC and BIOS are installed.



Step 2: Enter a description for this device (Example: RS213 UCS E-Series), and click then Save Changes.

Next, configure Network Settings.

Step 3: Click the **Admin** tab, select **Network**, and then click the **Network Settings** tab. Configure a hostname (Example: RS213-UCSE140S) and the primary DNS server if necessary (Example: 10.4.48.10), and then click **Save Changes**. On the warning window, click **OK**.

cisco Cisco Integ	grated Management Controller	CIMC Hostname: Logged in as:	Unknown admin@10.4.48.145 Log Out
Overall Server Status	0 0 🗏 🗮 0 0		
Good	Network		
Server Admin	Network Settings Network Security		
User Management Network	NIC Properties-		
Communications Services	NIC Redundancy: None		
Certificate Management CIMC Log	NIC Interface:		
Event Management	MAC Address: E0:2F:6D:E0:8E:0F		
Firmware Management	Common Properties		
Utilities	Hostname: RS213-UCSE140S		
	/IPv4 Properties		
	Enable IPv4: 🗹		
	Use DHCP:		
	IP Address: 10.5.180.10		
	Subnet Mask: 255.255.255.0		
	Gateway: 10.5.180.1		
	Obtain DNS Server Addresses From DHCP:		
	Preferred DNS Server: 10,4,48.10		
	Alternate DNS Server: 0.0.0.0		
	(YLAN Properties		
	Enable VLAN:		
	VLAN ID: 1		
	Priority: 0		
		Save Char	iges Reset Values

Step 1: Click on the Server tab, select Inventory, and then click the Storage tab.

cisco Cisco Integ	CIMC Hostname: #\$213-UC\$E1.485 grated Management Controller Logged in as: admin#10.4.0.143 Logged in as: admin#10.4.0.143								
Overall Server Status	C 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1								
Storage Cards									
Server Admin	CPUs Memory Power Supplies Storage PCI Adapters								
Summary	{Storage Adapters								
Inventory	Controller Product Name Firmware Package Build Product ID Cache Memory Size								
Sensors	SLOT-5 LSI MegaRAID SAS 2004 RC 20.10.1-0092 LSI Logic 0 MB								
System Event Log									
Remote Presence BIOS	Storage Card: SLOT-5								
Power Policies	ControllerInfo Physical Drive Info Virtual Drive Info								
Fault Summary	(Firmware Versions								
Host Image Mapping	Product Name: LSI MegaRAID SAS 2004 ROMB Predictive Fail Poll Interval: 300 sec								
	Firmware Package Build: 20.10.1-0092 Rebuild Rate: 30 MB/s								

Step 2: Click the Physical Drive Info tab.

cisco Cisco Integ	rated Management Controller	CIMC Hostname: Logged in as:	R5213-UCSE1405 admin@10.4.48.145 Log Out				
Overall Server Status	c I I I I I 0 0 Storage Cards						
Server Admin Summary	CPUs Memory Power Supplies Storage PCI Adapters Storage Adapters						
Inventory Sensors System Event Log	Controller Product Name Firmware Package Build Product ID Cache Memory Size SLOT-5 LSI MegaRAID SAS 2004 RC 2010.1-0092 LSI Legic 0 MB						
Remote Presence BIOS	Storage Card: SLOT-5						
Power Policies Fault Summary Host Image Mapping	ControllerInfo Physical Drive Info Physical Drives						
nost mage mapping	Slot Number State Mode Type Coerced Size Actions 1 system JBOD HDD, SATA 475883 MB - Actions - 2		<u> </u>				
	2 system 3BOD HDD, SATA 475983 MB - Actions - 5		Ŧ				

Step 3: For the drive in Slot Number 1, choose Change State from the Actions list.

cisco Cisco Integ	jrated Manage	ment Con	troller				CIMC Hostname: Logged in as:	RS213-UCSE1405 admin@10.4.48.145 Log Out
Overall Server Status 💦 🐮 🐮 🧱 🔞 🙃								
Good	Storage Cards							
Server Admin	CPUs Memory	Power Supplies	Storage	PCI Adapters				
Summary	Storage Adapters							
Inventory	Controller Pri	oduct Name	Firmware	Package Build	Product ID	Cache Memory Size	1	
Sensors	SLOT-5 LSI Megal				LSI Logic			A V
System Event Log								T
Remote Presence BIOS Power Policies	Storage Card: SLOT-5							
Fault Summary		tysical brite into	Virtual Dri	ve into				
Host Image Mapping	Physical Drives -		II	1		r 11		
	Slot Number	State	Mode	Туре	Coerced Size	Actions		
	1	system	JBOD	HDD, SATA	475883 MB	- Actions - 💈		Ê
	2	system	JBOD	HDD, SATA	475883 MB	- Actions -		
	Change State Rebuild							
	General Arrow Arr							

Step 4: If necessary, for the Physical Drive State, choose UnconfiguredGood, and then click Confirm.

Change Physical Drive State 🛛 🥹
Change State to: UnconfiguredGood 🛟
Confirm

Step 5: If necessary, repeat Step 3 and Step 4 for the remaining drives.

Step 6: Click the Virtual Drive Info tab. In the Actions pane, click Create.

If you are select RA	Tech Tip If you are configuring a Cisco UCS E-Series module with a single hard drive you can select RAID 0 and add the single drive to the list. Using two drives is recommended when possible.					
cisco .	grated Management Controller CMC Hotshame: R\$213.80561.406 Logged in sci admini910.4.481.45 Log Oct					
Geod Server Admin Summary Inventory Sensors System Event Log Remote Presence Bio Power Policias Fault Summary Host Image Mapping	Controller Work Supplies Storage Stora					

Step 7: In the **Configure Virtual Drive** window, select RAID Level **RAID 1** from the drop down menu. If your system only has a single drive, select RAID Level **RAID 0** (this will be the only available option).

c 3 3 🔳	00		Log Ou
Storage Car CPUs Memor Storage Adapts Controller SLOT-5 LSI ControllerInfo	Configure Virtual Drive	Selected Drives:	roduct ID Cache Memory Size
Virtual Drive		Next Cancel	Actions Actions
Step 8: Select the drives to be included in the RAID configuration, and then move them from the Unconfigured Drives column to the Selected Drives column by clicking **Add**. After selecting all the drives, click **Next**.

Configure Virtual Drive		
RAID Level: RAID 1	\$	
Unconfigured Drives:		Selected Drives:
		1
	Add >	2
	< Remove	
		Next Cancel

Step 9: In the Configure Raid Parameters window, select Set Bootable, and then click Next.

Configure	RAID Parameters 🤫
Strip Size:	64KB
Access Policy:	Read-Write 🗘
Drive Cache:	Unchanged 🗘
Initialization:	Quick 🗘
HSP:	
Set Bootable:	
	Back Next Cancel

Step 10: In the Confirm RAID Configuration window, verify the proper drives are listed, and then click Submit.

Confirm R	AID Confi	guration 🤨
RAID Level:	RAID 1	Drives:
Strip Size:	64KB	1
Access Policy:	Read-Write	2
Drive Cache:	Unchanged	
Initialization:	Quick	
HSP:	Disabled	
Set Bootable:	Enabled	
	Back	Submit Cancel

Step 11: Verify the virtual and physical drives are properly assigned by navigating to the **Server** tab, selecting **Inventory**, clicking the **Storage** tab, and then clicking the **Virtual Drive Info** tab.

liulu Cisco Inte	rated Management Controller	CIMC Hostname: Logged in as:	
Overall Server Status	C 🕹 🛃 📓 0 0		
Good	Storage Cards		
Server Admin	CPUs Memory Power Supplies Storage PCI Adapters		
Summary	/Storage Adapters		
Inventory	Controller Product Name Firmware Package Build Product ID Cache Memory Size		
Sensors	SLOT-5 LSI MegaRAID SAS 2004 RC 20.10.1-0092 LSI Logic 0 MB		0
System Event Log			Ŧ
lemote Presence	Storage Card: SLOT-5		
SIOS Iower Policies			
ault Summary			
lost Image Mapping	Virtual Drives		
	Virtual Drive Name State Size RAID Level Actions		Actions
	0 Optimal 475883 ME RAID 1 - Actions -		E Create
			Edit
			Delete
	General Physical Drives)
	Name: Virtual Drive Physical Drive Span Starting Block	Number Of Blocks	State
		74608384	online
		74608384	online
	Span Depth: 1		
	Access Policy: Read-Write		
	Cache Policy: Direct Read Ahead Policy: None		
	Write Cache Policy: Write Through		
	Disk Cache Policy: Unchanged		
	Allow Background Init: true		
	Auto Snapshot: false		
	Auto Delete Oldest: true		

cisco Cisco Integ	rated Management Controller Controller Loged in 85: admin@10.448.178 Loged in 85: admin@10.448.178
Overall Server Status	C 🕹 🕹 🧱 0 0
Good	Storage Cards
Server Admin	CPUs Memory Power Supplies Storage PCI Adapters
Summary	(Storage Adapters
Inventory	Controller Product Name Firmware Package Build Product ID Cache Memory Size
Sensors	SLOT-5 LSI MegaRAID SAS 2004 RC 20.10.1-0092 LSI Logic 0 MB
System Event Log Remote Presence	
BIOS	Storage Card: SLOT-5
Power Policies	ControllerInfo Physical Drive Info Virtual Drive Info
Fault Summary	(Virtual Drives
Host Image Mapping	Virtual Drive Name State Size RAID Level Actions
	0 Optimal 571250 ME RAID 1 - Actions -
	tot t t t
	General Physical Drives
	Name: Virtual Drive Physical Drive Span Starting Block Number Of Blocks
	Stripe Size: 64 KB 0 1 0 0 1169920000 Drives Per Span: 2 0
	Drives per Span: 2 0 3 0 0 1169920000 Span Depth: 1
	Access Policy: Read-Write
	Cache Policy: Direct
	Read Ahead Policy: None Write Cache Policy: Write Through
	Disk Cache Policy: Unchanged
	Allow Background Init: true
	Auda Canadadi. Estea
	Save Changes Reset Values



If possible install ESXi on the Cisco UCS-E server modules before shipping them to remote locations. This will avoid WAN utilization and possible congestion problems on your network.

Tech Tip

i

If you are using VMware FL-SRE-V-HOST license (equivalent to VMware vSphere Hypervisor™ 5.X), make sure that the installed Cisco UCS-E RAM is 32 GB or less. If the installed UCS-E RAM is more than 32 GB, you will get an error message, and you will not be able to apply the license.

If you want to use 48-GB RAM on the UCS-E server, upgrade your license to FL-SRE-V-HOSTVC. You can verify the memory configuration prior to installing VMware ESXi by navigating to the **Server** tab, selecting **Inventory**, and then clicking the **Memory** tab.

Procedure 1 Download UCS E-Series VMware ESXi image

A custom version of VMware ESXi has been developed specifically for use on Cisco UCS Servers. Use the following steps to download the custom ISO image.

Step 1: Open a browser and navigate to the VMware login page, https://my.vmware.com/web/vmware/login.

Step 2: Enter your VMware credentials, and then click Log In. If you do not have an account with VMware, create an account by clicking Register.

Step 3: Click on All Downloads.

Step 4: Select the All Products tab and then click on View Download Components for VMware vSphere.

All Downloads	
Search All Downloads	0
My Products All Products A-Z	
	All Products 🔹
Datacenter & Cloud Infrastructure	
VMware vCloud Suite	View Download Components I Drivers & Tools I Buy
VMware vSphere with Operations Management	View Download Components I Drivers & Tools I Try
VMware vSphere Data Protection Advanced	View Download Components I Drivers & Tools I Try
VMware vSphere	View Download Components I Drivers & Tools I Try

Step 5: Select version 5.1 in the Select Version dropdown box.

Download VMware vSphere		
Select Version: 5.1 5.5 5.1 5.0 4.1 4.0	Customers who have purchased VMware vSphere 5.1 can download their relevant installation package from the product download tab below. Looking to upgrade from vSphere 4 or Infrastructure 3? Visit the VMware vSphere Upgrade Center.	

Step 6: Select the Custom ISOs tab, and expand the OEM Customized Installer CDs by clicking the right arrow.

Product Downloads	Drivers & Tools	Open Source	Custom ISOs	
Custom ISOs Release Date		Release Date		
> OEM Customized Installer CDs				

Step 7: Click on Go to Downloads for the Cisco Custom Image for ESXi 5.1.0 U1 GA Install CD.

Product Downloads Drivers	& Tools Open Source Custom ISO	s	
Custom ISOs		Release Date	
 OEM Customized Inst 	aller CDs		
HP Custom Image for	ESXi 5.1.0 Update 1 Install CD	2013-09-30	Go to Downloads
Hitachi Custom Image	e for ESXi 5.1.0 Update 1 Install CD	2013-05-31	Go to Downloads
Cisco Custom Image	for ESXi 5.1.0 U1 GA Install CD	2013-05-30	Go to Downloads

Step 8: In the Product Downloads Tab, click the Download Now for the File type: iso version.



Step 9: The customized VMware vSphere Hypervisor image is downloaded.

Procedure 2 Install VMware ESXi on UCS-E Server

This procedure details several important tasks, including mounting the VMware ESXi ISO, setting the UCS-E Boot settings, and installing VMware ESXi onto the SD card of the UCS-E server. It is important to keep both the CIMC and KVM console windows open throughout these steps.



Step 1: Using your web browser, navigate to the CIMC address of the UCS E-Series module and login. [ex: https://10.5.180.10] [admin/c1sco123]. Accept any browser warnings due to untrusted certificates.

Step 2: On the Server tab, select Remote Presence, click the Virtual Media tab, and then ensure the Enabled check box is selected.

cisco Integrated Management Controller		
Overall Server Status	C 达 🕹 🧱 0 0	
Good	Remote Presence	
Server Admin	Virtual KVM Virtual Media Serial over LAN	
Summary	Virtual Media Properties	
Inventory	Enabled: 🗹	
Sensors	Active Sessions: 0	
System Event Log	Enable Virtual Media Encryption: 🔲	
Remote Presence		
BIOS		
Power Policies		
Fault Summary		
Host Image Mapping		

Step 3: Click the Virtual KVM tab, and then ensure the enabled check box is selected.

cisco Integrated Management Controller		
Good	C 3 3 3 10 10 10 10 10 10 10 10 10 10 10 10 10	
Summary Inventory Sensors System Event Log Remote Presence BIOS Power Policies Fault Summary Host Image Mapping	Actions Launch KVM Console vKVM Properties Enabled: Max Sessions: 4 Active Sessions: 0 Remote Port: 2068 Enable Video Encryption: Enable Local Server Video: M	

Step 4: In the Actions pane, on the Virtual KVM tab, click Launch KVM Console. Accept any security warnings. The virtual KVM window opens.

cisco Cisco Integrated Management Controller			
Overall Server Status Good Server Admin Summary Inventory Sensors System Event Log Remote Presence BIOS Power Policies Fault Summary Host Image Mapping	C C C C C C C C C C C C C C C C C C C		

Step 5: In the KVM Console window, click the Virtual Media tab.



Step 6: In the KVM Console window, click Add Image.

10.5.180.10 -	KVM Console	6				
Help						
VM Virtual	Media					
Client View						
Mapped	Read Only	Drive				Exit
		🖃 I: - Remova	ble Disk			
		🖃 H: - Remov	able Disk			Create Image
		🖃 G: - Remov	able Disk			Add Image
		F: - Remov	able Disk			Remove Image
		🙆 E: - CD/DVE)			Details ±
4	1	1				•
Details						
Target Drive	Mapp	ed To	Read Bytes	Write Bytes	Duration	
Virtual CD/DV	D Not m	apped				USB Reset
Removable Di	isk Not m	apped				
Floppy	Not m	apped				

Step 7: Browse for the VMware ESXi ISO image, and then click Open.

Open .ook <u>I</u> n:	CVD			•	a a	
		custom-Cis	sco-5.1.1.1.is			
ile <u>N</u> ame:						

Step 8: For the newly added image, select Mapped. This maps the ISO file and completes the mount.

10.5.180.10 -	KVM Console						
e Help							
VM Virtual	Media						
Client View							
Mapped	Read Only	Drive					Exit
		🖃 I: - Removable D	isk				
		🖃 H: - Removable I	Disk				Create Image
		G: - Removable I	Disk				Add Image
		E F: - Removable D	Disk				Remove Image
		🛃 E: - CD/DVD					
		C:ICVDIESXI-5.1	0-1065491-0	custom-Cisco-	5.1.1.1.iso - ISO Image	File	Details ±
Details							
Target Drive	Марр	ed To	Read Bytes	Write Bytes	Duration		
Virtual CD/DV	/D 🙆 C:	CVD\ESXi-5.1.0-10	0	0	00:00:08		USB Reset
Removable D	lisk Not m	apped					
Floppy	Not m	apped					

Step 9: Return to the **KVM Console** window by clicking the **KVM** tab. You can monitor the status of the server by using this console window. Keep this window open and visible.



Step 10: From the CIMC, navigate to the server summary screen, and then reboot the server by clicking **Power** Cycle Server. In the warning window, click OK. The console screen turns blank and green for a moment during this process.

cisco Cisco Integ	rated Management Controller	CIMC Hostname: RS240-3945-UCS140S Lagged in as: admin@10.4.48.178 Log Out
Urerall Server Status Construction Server Admin Server Admin Server Admin Server Status Server Admin Server Status Server Admin Server Status Server Status Server Palaias Power Palaias Power Palaias Power Palaias Power Palaias	Attoas Server Summary Deveryde the server? D	Logged in as: admin@10.4.48.178
		Save Changes Reset Values

Step 11: Monitor the KVM Console window as the server boots, and, when prompted, enter the BIOS setup by pressing F2.

Step 12: When prompted, enter the password (Example: c1sco123). If this is the first time entering the BIOS, you are prompted to set a BIOS password (Example: c1sco123).



Step 13: Using the arrows on your keyboard, navigate to the Boot tab, highlight Boot Option #1, and then press Enter.



Step 14: In the window, select Cypress, and then press Enter.



Step 15: Press **F10**. In the save and exit dialog box, select **Yes,** and then press **Enter**. This saves the BIOS settings and exits BIOS. The system will now reboot.



Step 16: In the virtual KVM window, click the **KVM** tab, and then monitor the **KVM Console** window as the server boots. The server loads the ESXi Installer from the mapped ISO image.

Step 17: When the Vmware Vmisor Boot Menu appears, select the ESXi custom installer.



Step 18: On the welcome screen, press Enter. The installation of ESXi begins.



Step 19: Accept the license by pressing F11.

End User License Agreement (EULA)			
VMWARE END USER LICENSE AGREEMENT			
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.			
EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period			
Use the arrow keys to scroll the EULA text			
(ESC) Do not Accept (F11) Accept and Continue			

Step 20: Using the down arrow, select the SD card as the local storage device, and then press **Enter**. (example: Cypress Astoria SD Card). When prompted to confirm disk selection, press **Enter**.

* Contains a VMFS		Install or Upgra	ade	
Storage Device				Capacity
Local: * LSI MRSASRoMB-4 Cupress Astoria Remote: (none)	i (naa.6d867d9c7 SD Card (mpx.vm		e3cd571)	557.86 GiB 7.44 GiB
(Esc) Cancel	(F1) Details	(F5) Refresh	(Enter)	Cont inue

Select a Disk to Install or Upgrade									
* Cont	* Contains a VMFS partition								
Stora	a Confirm Disk Selection								
LS Cy	$ ilde{{f t}}$ If you continue the selected disk will be overwritten.								
	(Esc) Cancel (Enter) OK								
(Es	c)Cancel (F1)Details (F5)Refresh (Enter)Contin	nue							

Step 21: For the keyboard layout, select the US Default, and then press Enter.

Please select a keyboard layout					
Swiss French Swiss German Turkish US Default US Dvorak Ukrainian United Kingdom					
Use the arrow keys to scroll.					
(Esc) Cancel (F9) Back (Enter) Continue					

Step 22: Set the root password, and then press Enter (example: c1sco123).



Step 23: The system scans for resources, which may take a few moments. Press **F11**. A status bar shows the progress of the ESXi installation.

(Confirm Install	L. C.						
	The installer is configured to install ESXi 5.1.0 on: mpx.vmhba33:CO:TO:LO.							
Warning: This	Warning: This disk will be repartitioned.							
(Esc) Cancel	(F9) Back	(F11) Install						

Step 24: After a successful installation of ESXi, select the Virtual Media tab on the KVM Console window, click Remove Image, and agree to the warning. This unmounts the image.

0.5.180.10 - K	VM Console	0							-
Help									
M Virtual I	Media								
lient View									
Mapped	Read Only	Drive							Exit
		🖃 I: - Removable Di	sk						Caracter Immerse
		🖃 H: - Removable D	isk						Create Image
		🖃 G: - Removable D	isk						Add Image
		F: - Removable Di	sk					[Remove Image
	V	🚔 E: - CD/DVD							Details ±
		2 C:\CVD\ESXi-5.1.0	-1065491-c	ustom-Cisco-f	5.1.1.1.iso - ISO Im	age File			Details ±
1			11.)	
etails									
arget Drive	Mappe	ed To F	Read Bytes		Duration				
	-	CVD/ESXI-5.1.0-10 3	16.981M	0	00:43:14				USB Reset
irtual CD/DVE emovable Dis	-		16.981M	0	00:43:14				USB Reset

Step 25: On the KVM tab, press Enter. The system restarts, loading the ESXi image installed on the SD drive.



Procedure 3

Configure VMware ESXi Host Settings

Step 1: In the KVM Console window, press F2. This enables you to customize the system after ESXi is finished booting.



Step 2: Log in using the credentials you set during installation. [example: root/c1sco123]



Step 3: Using the down arrow key, highlight to the Configure Management Network option, and then press Enter.

File View Macros Tools Help KVM Virtual Media	
System Customization	Configure Managenent Network
Configure Passuord Configure Lockdown Mode	Hostname: localhost
Configure Management Network Restart Management Network Test Management Network	IP Address: 169.254.140.114
Network Restore Options	IPv6 Addresses: fe80::e22f:6dff:fee0:708c/64
Configure Keyboard Troubleshooting Options	
View System Logs	detail, press 〈Enter〉.
View Support Information	
Reset System Configuration	

Step 4: Select IP Configuration, and then press Enter.

File View Macros Tools Help KVM Virtual Media							
Configure Management Network	IP Configuration						
Network Adapters VLAN (optional) IP Configuration IPOS Configuration DMS Configuration Custon DMS Suffixes	Autonatic IP Address: 169.254.140.114 Subnet Mask: 255.255.0.0 Default Gateway: Not set This host can obtain an IP address and other networking parameters autonatically if your network includes a DHCP server. If not, ask your network administrator for the appropriate settings.						

Step 5: Highlight Set static IP address and network configuration, and select it by pressing the space bar.

Step 6: Using the down arrow, enter the assigned values from Table 16 (example:10.5.180.11, 255.255.255.0, 10.5.180.1) for **IP address**, **subnet mask** and **default gateway**, and then press **Enter**.

IP Configuration	
This host can obtain network settings autor includes a DHCP server. If it does not, the specified:	
() Use dynamic IP address and network cont	figuration
(o) Set static IP address and network conf	
	iguration: [10.5.180.11]
(o) Set static IP address and network conf IP Address Subnet Mask	iguration: [10.5.180.11] [255.255.255.0]
(o) Set static IP address and network conf IP Address	iguration: [10.5.180.11]

Step 7: Using the down arrow, select DNS Configuration, and then press Enter.

File View Macros Tools Help KVIM Virtual Media				
Configure Management Network	DNS Configuration			
Network Adapters VLAN (optional) IP Configuration DNS Configuration DNS Configuration Custow DNS Suffixes	Manual Primary DNS Server: Not set Alternate DNS Server: Not set Hostname localhost If this host is configured using DHCP, DMS server addresses and other DNS parameters can be obtained automatically. If not, ask your network administrator for the appropriate settings.			

Step 8: Configure the primary DNS server and hostname (Example: 10.4.48.10 and RS213-ESXi), and then press **Enter**.

DNS Configuration				
This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.				
() Obtain DNS server addresses and a hostname automatically (o) Use the following DNS server addresses and hostname:				
Primary DNS Server [10.4.48.10] Alternate DNS Server []				
Hostname [RS213-ESXi.cisco.local_]				
KUp/Down> Select KSpace> Mark Selected Kenter> OK KEsc> Cancel				

Step 9: On the Configure Management Network screen, exit by pressing ESC.

File View Macros Tools Help KVM Virtual Media				
Configure Management Network	DNS Configuration			
Network Adapters VLAN (optional) IP Configuration DPu6 Configuration DNS Configuration Custom DNS Suffixes	Manual Primary DMS Server: 10.4.40.10 Alternate DMS Server: Not set Hostnane RS213-ESX1.cisco.local If this host is configured using DHCP, DNS server addresses and other DMS parameters can be obtained automatically. If not, ask your network administrator for the appropriate settings.			

Step 10: On the confirmation dialog box, confirm that you want to apply changes and restart by pressing Y.

Configure Management Network: Confirm	
You have made changes to the host's management netwo Applying these changes may result in a brief network disconnect remote management software and affect run machines. In case IPv6 has been enabled or disabled restart your host.	k outage, nning virtual
Apply changes and restart management network?	
<y> Yes <n> No</n></y>	<pre>KEsc> Cancel</pre>

Procedure 4 Add VMware ESXi host to vCenter

Step 1: From the VMware vSphere client, select the folder location where you want to add the ESXi host (Example: Remote Sites).

Step 2: On the Getting Started tab, under basic tasks, click Add a host.

Tech Tip

i

You must have the ESXi hostname and IP address configured in your DNS database if you want to be able to reference it by name in the vCenter. Add a new DNS entry if required.



Step 3: In the Connection Settings window, enter the hostname of the ESXi host and the username and password [root / c1sco123], and then click **Next**. If necessary, accept the Security Alert by clicking **Yes**.

Add Host Wizard Specify Connection Settings Type in the information used to a	connect to this host.
Connection Settings Host Summary Virtual Machine Location Ready to Complete	Connection Enter the name or IP address of the host to add to vCenter. Host: rs213-esxi.cisco.local Authorization Enter the administrative account information for the host. vSphere Client will use this information to connect to the host and establish a permanent account for its operations. Username: root Password: *******
Help	< Back Cancel

Step 4: In the Host Summary window, verify the details of the ESXi host you wish to add, and then click Next.

Add Host Wizard			_ 0
Host Information Review the product information	for the specified host.		
Connection Settings	You have chose	n to add the following host to vCenter:	
Host Summary Assign License Lockdown Mode Virtual Machine Location	Name: Vendor: Model:	rs213-esxi.cisco.local Cisco Systems, Inc.	
Ready to Complete	Version: Virtual Machine	VMware ESXI 5.1.0 build-1065491 es:	
]
Help		< Back Next >	Cancel

Step 5: In the **Assign License** window, click in the circle to assign the appropriate VMware license key or add a new license key and then click **Next**.

🛃 Add Host Wizard		_ 🗆 ×
Assign License Assign an existing or a new	/ license key to this host.	
Connection Settings Host Summary	🔂 Add License Key	X
Assign License Lockdown Mode Virtual Machine Location Ready to Complete	New license key:	Cancel
	Assign a new license key to this host Enter Key Product: - Capacity: - Available: - Expires: - Label: -	
Help	< Back	Next > Cancel

Step 6: In the Lockdown Mode window, verify that Enable Lockdown Mode is cleared, and then click Next.

|--|

Step 7: In the Virtual Machine Location window, select the proper location for the new ESXi host, and then click Next.

Add Host Wizard					_ 0
Virtual Machine Location Select a location in the vCenter Se	rver inventory for the h	ost's virtual machine	s.		
Connection Settings Host Summary Assign License Lockdown Mode Virtual Machine Location Ready to Complete		for this host's virtua			
Help			< Back	Next >	Cancel

In the Ready to Complete summary window, verify the information, and then click Finish.

Add Host Wizard			
Ready to Complete Review the options you have sele	cted and click Finish to add t	he host.	
Connection Settings Host Summary	Review this summa	ry and click Finish.	
Assign License Lockdown Mode Virtual Machine Location Ready to Complete	Version:	rs213-esxi.cisco.local VMware ESXi 5.1.0 build-1065491 VM Network Disabled	

Step 8: Select the new ESXi host, click the Summary tab, and then verify the information is correct.

2 vCenter51 - vSphere Client				
File Edit View Inventory Administration Plug-In-	; Help			
🖸 🔝 🏠 Home 🕨 🛃 Inventory 🕨 🖱	I Hosts and Clusters			Search Inventory
8° 88				
- 🚱 vCenter51	rs213-esxi.cisco.local VMware E			
🗄 📂 Remote Sites	Getting Started Summary Virt	ual Machines 🔧 Resource Allocatio	Performance Configuration Tasks & Events Alarms Permissions	Maps Storage Views Hardware Status
rs213-es:d.disco.local □ rs240-es:d-1.disco.local MWS-Storage-Gateway	Configuration Issues No datastores have been configu	red		Ī
Gisco WAAS: vWAAS-750 RS240-WIN2008-1	System logs on host rs213-esxi.cl	isco-local are stored on non-persiste	nt storage.	
B RS240-WIN701	General		Resources	
⊟ rs242-es:d-1.dsco.local AWS-Storage-Gateway-2 Rs242-UBUNTU01	Manufacturer: Model:	Cisco Systems, Inc.	CPU usage: 0 MHz Capacity 4 × 0.999 GHz	
R5242-WIN701	CPU Cores: Processor Type:	4 CPUs × 0.999 GHz Intel(R) Xeon(R) CPU @ 1.00GHz	Memory usage: 0.00 MB Capacity 16330.93 MB	
	License:	Evaluation Mode -	Storage × Status Drive Type	
	Processor Sockets:	1	· · ·	
	Cores per Socket:	4	Network Type Sta	
	Logical Processors: Hyperthreading:	8 Active	🙎 VM Network Standard port group 🥏	
	Number of NICs:	3	<u> </u>	
	State:	Connected	Fault Tolerance	
	Virtual Machines and Templates: vMotion Enabled:	0 No	Fault Tolerance Version: 4.0.0-4.0.0-4.0.0	
	Whiware EVC Mode:	Disabled 💭	Refresh Virtual Machine Counts	
	vSphere HA State Host Configured for FT:	③ N/A No	Total Primary VMs: Powered On Primary VMs: Total Secondary VMs:	-
	Active Tasks: Host Profile:		Powered On Secondary WMs:	
	Image Profile:	ES/4-5.1.0-1065491-custom		
	Profile Compliance:	🕝 N/A		
	DirectPath I/O:	Not supported 📮		

Procedure 5 Add a datastore to ESXi hosts

In this procedure, you will add storage for the virtual machines and other system files to use. The storage will be a disk drive physically located on the server.



Step 1: Using vSphere Client, log in to the ESXi host.

Step 2: On the Configuration tab, in the Hardware pane, click Storage.

Step 3: If your ESXi host does not have a provisioned virtual machine file system (VMFS), in main window, in the "The VMware ESX Server does not have persistent storage" message, click **Click here to create a datastore**.

	Ki, 5.1.0, 1065491 Evaluation (60 days rema al Machines Resource Allocation Performance	
The ESXi host does not h	ave persistent storage. st one datastore for maintaining virtual machines and	l other system files.
I CARL INTER ON CALL INCOMENTS	an andar weight weight weight weight and the first and the	lapters and network connections are properly configured before continuing.
To add storage now, dick here to cre	ate a datastore	
Hardware	Processors	
Processors	General	
Memory	Model	Intel(R) Xeon(R) CPU @ 1.00GHz
Storage	Processor Speed	1 GHz
Networking	Processor Sockets	1
Storage Adapters	Processor Cores per Socket	4
Network Adapters	Logical Processors	8
Network Adapters Advanced Settings	Logical Processors Hyperthreading	8 Enabled

Step 4: In the Add Storage wizard, select Disk/LUN, and then click Next.

🛃 Add Storage	
Select Storage Type Specify if you want to for	rmat a new volume or use a shared folder over the network.
Disk/LUN Select Disk/LUN File System Version Current Disk Layout Properties Formatting Ready to Complete	Storage Type Note: Storage Type Note:
Help	<back next=""> Cancel</back>

Step 5: On the Select Disk/LUN page, select the local disk and then click Next.

lect Disk/LUN Select a LUN to create a	datastore or expand the current	one		
<u>(LUN</u> Select Disk/LUN	Name, Identifier, Path ID,	LUN, Capacity, Expandable or VI	MFS Label c 👻	c
File System Version Current Disk Layout	Name	Path ID	LUN 🔨 Drive Typ	
Properties	Local LSI Disk (naa.6e02f6	de08e0a vmhba0:C2:T0:L0	0 Non-SSD	929.46
Formatting dy to Complete				
ay to complete				
	Lon Los			

Step 6: On the File System Version page, select **VMFS-5** or **VMFS-3**. Hosts running ESXi 4.x will not be able to access VMFS-5 datastores. Unlike VMFS-3, VMFS-5 uses standard 1 MB file system block size with support of 2 TB+ virtual disks.

🛃 Add Storage	
File System Version Specify the version of the	VMFS for the datastore
Disk/LUN Select Disk/LUN File System Version Current Disk Layout Properties Formatting Ready to Complete	File System Version • VMFS-5 Select this option to enable additional capabilities, such as 2TB+ support. WMFS-5 is not supported by hosts with an ESX version older than 5.0. • VMFS-3 Select this option if the datastore will be accessed by legacy hosts. Select this option if the datastore will be accessed by legacy hosts.
Help	< Back Next > Cancel

Step 7: Review the disk capacity and partition information, and then click Next.

Current Disk Layout You can partition and form	at the entire device, all free space, or a si Review the current disk layout:	ngle block of free	e space.		
Priesc Descroti File System Version Current Disk Layout Properties Formatting Ready to Complete	Device Local LSI Disk (naa.6e02f6de0 Location /vmfs/devices/disks/naa.6e02f6de Partition Format Unknown	Drive Type Non-SSD e08e0a0001a27b	Capacity 929.46 GB 065e0c2d1342	Available 929.46 GB	LUN O
	There is only one layout configuration pages.	The hard disk is available. Use ti		proceed with the ot	her wizard
	A partition will be created ar	nd used			
Help			< Back	Next >	Cancel

Step	8:	Enter	а	datastore	name,	and	then	click I	Next.
------	----	-------	---	-----------	-------	-----	------	---------	-------

🛃 Add Storage		
Properties Specify the properties fo	r the datatore	
Disk/LUM Select Disk/LUN File System Version Current Disk Lavout Properties Formatting Ready to Complete	Enter a datastore name	
Help		< Back Next > Cancel

Step 9: On the Disk/LUN Formatting page, accept the defaults by clicking **Next**. This formats the maximum available space in the disk.

🛃 Add Storage				_ 🗆 ×
Disk/LUN - Formatting Specify the maximum file	size and capacity of the datastore			
Disk/LUN Select Disk/LUN Ele System Version Current Disk Layout Properties Formatting Ready to Complete	Capacity Maximum available space Custom space setting 929.46 A GB of 929.46 GB available space			
Help		< Back	Next >	Cancel

Step 10: Click Finish. The Add Storage wizard is completed.

Disk/LUN Ready to Complete	Disk layout:	
Keady to Lomplete	Device Drive Type Capacity Local LSI Disk (naa.6e02f6de08e0 Non-SSD 929.46 GB Location /vmfs/devices/disks/naa.6e02f6de08e0a0001a27b65e0c2d1342 Partition Format GPT Primary Partitions Capacity VMFS (Local LSI Disk (naa.6e02f6d 929.46 GB	UUN O
	File system: Properties Datastore name: R5213-ESXi-LocalDisk Formatting File system: vmfs-5 Block size: 1 MB Maximum file size: 2.00 TB	

Procedure 6 Configure networking for ESXi host

The following table is used during this procedure to map the correct network interfaces to the vSwitch.

Interface usage	UCS-E140S (single wide)	UCS-E140D (double wide)
console/internal	vmnic0	vmnic0
internal MGF	vmnic1	vmnic1
external (1)	vmnic2	vmnic2
external (2)		vmnic3
vSwitch Port Group Network Label	ESXi-external	ESXi-external-dual

Step 1: Click the Configuration tab, and then click Networking.

🛃 vCenter51 - vSphere Client				
File Edit View Inventory Administration Plug-ine	s Help			
🖸 🔝 🛕 Home 🕨 🛃 Inventory 👂 🖱	Hosts and Clusters		Search Inventory	Q
त द स				
Control 1 Control 1	a and a second	1.0. (USS-01 Evolution (C) devices remainered) New "Research Standards (C) devices Configuration" (Evolution Configuration") Ver: "General Standard Standard Standard Standard Standard Standard Standard Versional Played Advance Played Advance Played Advance Play	Vennisiona, Magio (Borga Veen, Mardener Baka), Rafrash Additeteoring	Properties

Step 2: Click Add Networking, on the Connection Type dialog box, select Virtual Machine, and then click Next.

ionnection Type letwork Access ionnection Settings ummary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXI services: vSphere vMotion, iSCSI, NFS, and host management.

Next, configure a standard vSwitch for ESXi.

Step 3: Select the external NIC card, **vmnic2**, to be used for this vSwitch , and then click **Next**. This example uses a single interface. For dual NIC configurations, select both **vmnic2** and **vmnic3**.

Virtual Machines - Nel Virtual machines rea	twork Access ch networks through uplink adapters attached to vSphere standard switches.				
Connection Type Network Access	Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.				
Connection Settings Summary	Create a vSphere standard switch Speed Networks Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet				
	🔽 📟 vmnic1 1000 Full None				
	🗌 📟 vmnic2 1000 Full 0.0.0.1-255.255.255				
	C Use vSwitch0 Speed Networks				
	Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet				
	🔲 📟 vmnic0 1000 Full None				
	ı Preview:				
	Virtual Machine Port Group Physical Adapters				
	1				

Step 4: In the Port Group Properties pane, edit the Network Label (Example from Table 17: ESXi-external), set the VLAN ID to None (0), and then click Next.

🛃 Add Network Wizard				_ 🗆 🗙
Virtual Machines - Connec Use network labels to ide		ions common to two or more hosts.		
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VLAN ID (Optional):	ESXi-external None (0)	Y	
	Preview: Virual Machine Port Group - ESX-external	Physical Adapters		
Help			< Back Ne	xt > Cancel

Step 5: Review the final host networking configuration, and then click Finish.
--

Add Network Wizard Ready to Complete	
	d modified vSphere standard switches are configured appropriately.
Connection Type Network Access Connection Settings	Host networking will include the following new and modified standard switches: Preview:
Summary	- Virtual Machine Port Group ESXI-external
Help	< Back Finish Cancel

Procedure 7 Configure ESXi NIC teaming for resiliency

Optional

This procedure is only required if you have two external NICs connecting to external switches for resiliency. This example uses the default ESXi NIC teaming configurations for redundancy.

This procedure uses the values in Table 17 to map the correct network interfaces to the vSwitch.

Step 1: View properties by clicking properties for the newly created vSwitch (Example: vSwitch1).

andard Switch: vSwitch1	Remove Properties
Virtual Machine Port Group	Physical Adapters Physical Adapters wmnic3 1000 Full wmnic2 1000 Full

Step 2: In the vSwitch Properties window, select the Port Group (Example: ESXi-external-dual), and click Edit.

Tech Tip

i

This NIC redundancy configuration using the default VMware settings provides failover for link or switch failure for applications installed on a Cisco UCS E-Series double-wide module such as the UCSE140D.

orts	Network Adapters				
			-Port Group Properties		
	guration vSwitch	Summary 120 Ports	Network Label:	ESXi-external-dual	
	ESXi-external-dual	Virtual Machine	VLAN ID:	None (0)	
			Effective Policies		
			Security		
			Promiscuous Mode:	Reject	
			MAC Address Changes:	Accept	
			Forged Transmits:	Accept	
			Traffic Shaping		
			Average Bandwidth:		
			Peak Bandwidth:		
			Burst Size:		
			Failover and Load Balanci	ing	
			Load Balancing:	Port ID	
			Network Failure Detection:	Link status only	
			Notify Switches:	Yes	
			Failback:	Yes	
			Active Adapters:	vmnic2, vmnic3	
			Standby Adapters:	None	
Add	d	Edit Remove	Unused Adapters:	None	

Step 3: In the Port Group Properties window, view the Failover and Load Balancing details by selecting the **NIC Teaming** tab. The configuration options display.

Load Balancing:			be originating viri	ual port ID 🛛 💌
Vetwork Failow	ar Detection :		he originating viri	- dai port ib
Network Failover Detection: Notify Switches:		Link status only Yes		
Failover Order:				
	vitch failover orde	er:		
		ers for this port group. In a fa	ailover situation.	standby
adapters activa	ate in the order s	pecified below.	allover sicadion,	standby
Name	Speed	Networks		Move Up
Active Adapt	1 1			nove op
wnnic2	1000 Full	None		Move Down
wmic3	1000 Full	None		
Standby Ada	pters			
Standby Ada Unused Adap	-			
-	-			
-	-			
Unused Adar	oters			
-	oters			
Unused Adap	oters			
Unused Adap -Adapter Deta Name:	oters			
Unused Adap	oters			
Unused Adap -Adapter Deta Name:	oters			



To avoid WAN congestion and possible installation issues, download or copy the installation Open Virtual Appliance (OVA) files to a local host at the remote location and perform the installation from a remote host at that location.

Cisco vWAAS is available as OVA and is designed to be installed into a virtual environment. The OVA is an industry standard format with prepackaged disk, memory, CPU, NICs, and other virtual-machine-related configuration parameters.

Procedure 1 Deploy the OVA

Step 1: From vCenter, click the ESXi host that you will use to run your virtual machine (Example: rs213-esxi. cisco.local).

Step 2: From the File menu, choose Deploy OVF template.

File	Edit	View	Inventory	Administ	
	New			•	
	Depl	oy OVI	Template		
	Expo	ort 🗟		•	
	Repo	ort		•	
	Browse VA Marketplace				
	Print	t Maps		Þ	
	Exit				

Step 3: Browse for the local OVA file to install, and then click Next.


Step 4: Review the template details, and then click Next.



Step 5: Enter a name for the OVA (Example: RS213-vWAAS-1300), select the proper location, and then click Next.

Deploy O¥F Template		_ 🔲 :
Name and Location		
Specify a name and loca	tion for the deployed template	
Source	Name:	
OVF Template Details	R5213-vWAA5-1300	_
Name and Location Disk Format	The name can contain up to 80 characters and it must be unique within the inventory folder.	
Network Mapping		
Ready to Complete	Inventory Location:	
	10k	
	1	
Help	< Back Next > Ca	
Holp	<back next=""> Ca</back>	ncel

Step 6: Accept the recommended Disk Format settings by clicking Next.

Deploy OVF Template				
Disk Format In which format do you	want to store the virtual disks?			
Source OVF Template Details Name and Location	Datastore: Available space (GB):	local-disk-esxi		
Disk Format Network Mapping Ready to Complete	Fridiable space (ab)	1 10010		
	Thick Provision Lazy	Zeroed		
	C Thick Provision Eager	Zeroed		
	C Thin Provision			
Help			< Back Next :	> Cancel

Step 7: Click the current setting for Destination Networks. All destination network choices are displayed.

Step 8: Select the destination network by choosing the ESXi networking profile created in Procedure 5, Step 4 (Example: ESXi-external), and then click **Next**.

PDeploy OVF Template		-	
Network Mapping What networks should th	he deployed template use?		
Source OVF Template Details Name and Location Disk Format Network Mapping	Source Networks	template to networks in your inventory Destination Networks	
Ready to Complete	VM Network	ESXI-external ESXI-external VM Network	
	, Description: The VM Network network		×
ud. 1			
Help		< Back Next > Cano	tel

Step 9: Review the OVA summary information, select Power on after deployment, and then click Finish.

🛃 Deploy OVF Template		
Ready to Complete Are these the options yo	u want to use?	
Source OVF Template Details Name and Location Disk Format Network Mapping Ready to Complete	When you click Finish, the deplo Deployment settings: OVF file: Download size: Size on disk: Name: Folder: Host/Cluster: Datastore: Disk provisioning: Network Mapping: Network Mapping:	yment task will be started. 2:\Shared\Cisco\WAAS\Cisco-WAAS-vWAAS-1300.ova 1.6 GB 304.0 GB R\$213-vWAAS-1300 10k r\$213-esxi.cisco.local local-disk-esxi Thick Provision Lazy Zeroed "VM Network" to "ESXi-external"
Help		< Back Finish Cancel

Step 10: Monitor the deployment.

🛃 4% Deploying R5213-vWAAS-1300	_ 🗆 🗵
Deploying RS213-vWAAS-1300	
Deploying disk 2 of 2	
11 minutes remaining	
Close this dialog when completed	Cancel

🛃 Deployment Completed Successfully	
Deploying R5213-vWAAS-1300	
Completed Successfully	
	Close

Step 11: After the OVA is installed, highlight the installed OVA, and then, on the Summary tab, verify its status.

🚱 vCenterS i - vSphere Client					
File Edit View Inventory Administration Plug-ins Help					
🖸 🔝 🏠 Home 🕨 👸 Inventory 🕨 🎁	Hosts and Clusters		Search Inventory		
	* • *				
	Ceneral Persurce Alocatori Performance Concol Concol Product: Caso: WAAS-1300 Version: 5.2.1 (6.2.1) Version: Caso: WAAS-1300	Telds & Events' Alarmic Console Permissions' Maps' Storage Verv Resources Consume Host CPU: 0 MHz Consume Host Remony: 31.00 MB			
FS240-WIX2005-1 FS240-WIX2005-1 FS240-WIX201 T2242-essi1-Licison.hcal AW-5-50-age-Gataway-2 FS242-WIX701 T2242-essi-2.cisco.hcal	Textury Could systems Guett OS: Other 26.cv Linux (64-bit) W1 Version: 8 CPU: 2 v/2FU Memory: 644 MB Memory: 59.80 MB VPMour Tools: (2) VPMours Tools: (2)	Active Guest Memory: 4608.00 MB Provisioned Storage: 304.09 GB Not-shard Storage: 304.09 GB Usd Storage: 304.09 GB Usd Storage: 304.09 GB Storage 304.09 GB With Storage: 304.09 GB Usd Storage: 304.09 GB Storage Status Provertype R5213-ES04.0cal Ø Normal			
	IP FAULTESES: DNS Name: EVC Mode: N/A State: Powered On Hoot: rs213-ess1.cisco.local	Network Type Standard port group			
	vSphere HA Protection: ③ N/A 모 Commands	VM Storage Profiles: Profiles Compliance:			
	Power Off Suspend Constant Suspend Constant Suspend Den Console Mayate Console Mayate Console Console Console Console Console Console				

Procedure 2

Configure the WAAS Node

This procedure uses the recommended network parameters from Table 16, repeated below.

Parameter	CVD values for an access-layer connection	CVD values for a distribution-layer connection	Site-specific values
In-band management network	10.5.180.0/24 (existing data subnet)	10.5.168.16/29 (new subnet for UCS E management)	
UCS E-Series interface address	unnumbered gig0/2.64	10.5.168.17/29	
Cisco IMC interface address	10.5.180.10/24	10.5.168.18/29	
VMware ESXi interface address	10.5.180.11/24	10.5.168.19/29	
Switch interface number	0/22	1/0/7	
VLAN number	64	106	
Time zone	PST8PDT -8 0	PST8PDT -8 0	
IP address	10.5.180.8/24	10.5.175.8/24	
Default gateway	10.5.180.1/24	10.5.175.1/24	
WAAS Central Manager	10.4.48.100	10.4.48.100	
Hostname	RS213-vWAAS	RS212-vWAAS	
IP addresses of routers intercepting traffic with WCCP	10.255.255.213	10.255.255.212	
WCCP password	c1sco123	c1sco123	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS shared key (optional)	SecretKey	SecretKey	

December 2013



Step 1: From vCenter, click the Cisco vWAAS that you will want to configure (Example: RS213-vWAAS-1300), and then click the **Summary** tab.

🔛 🏠 Home 👂 🛃 Inventory 👂 🎁 H	osts and Clusters				Search Inventory
I III 🕟 🧐 🖾 🕼 🗊 🛃 😡	> 📀 🛃				
10k	5213-vWAA5-1300 ietting Started Summary Resource Alloc	tion Performance Tasks & Events Alarms Co	ionsole Permissions	Maps Storage Views	
B R5213-VWAAS-1300	Seneral	Resources			
AWS Storage Galeway AWS Storage Galeway Based With200+1 Based With200+1 Based With200+1 Based With201 If242 easi-1.cso.bcol Add Storage Galeway 2 Based With201 If242 easi-1.cso.bcol Storage Galeway 2 Based With201 If242 easi-1.cso.bcol	Product: Case: WARS: WWAR Version: 5.2.1 (5.2.1) Version: Case: Systems Gaset OS: Offer 2.6.x. Unut. (141 Version: 2 VGRU Sectors Memory: 61 44 MB Memory: 61 44 MB Werker Tools: 50 Mot Mores DIS Name: DVS Name: DIS Name: NA	Consumed Host CPO: Consumed Host Memory: Active Guest Memory:	R Status		
	State: Powered On Host: rs213-essi.cisco.loc Active Tasks: vSphere HA Protection: ② N/A 모	VM Storage Profiles		Refresh	
	Commands	VM Storage Profiles: Profiles Compliance:			
	Power Off Suspend Suspend Edit Settings Edit Settings Migrate Migrate Conc to New Virtual Machine	L			

Step 2: In the Commands pane, click Open Console, and then log in. The factory default username is admin and the factory default password is default.

Step 3: In the console window, 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	Virtual 1/0
	Autosense	Disabled
4.	DHCP	Enabled
ESC	Quit ? Help ———	WAAS Default Configuration
Pres	ss y' to select above defa	aults, `n' to configure all, <1-4> to change
spec	cific default [y]: 4	

Step 4: Disable DHCP.

Enable DHCP for Mana	gement Interface? (y/n)[y]: n
Parameter	Configured Value
Device Mode	Application Accelerator
1. Interception Method	WCCP
2. Time Zone	UTC 0 0
3. Management Interface	Virtual 1/0
Autosense	Disabled
4. DHCP	Disabled
ESC Quit ? Help ———	- WAAS Default Configuration
Press 'y' to select above de	faults, 'n' to configure all, <1-4> to change
specific default [y]: n	

Step 5: Configure the interception method.

```
    WCCP
    AppNav Controller
    VPATH
    Other
    Select Interception Method [1]: 1
```

Step 6: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)> [UTC 0 0]:
PST8PDT -8 0
```

Step 7: 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. Virtual 1/0 dhcp 2. Virtual 2/0 dhcp Select Management Interface [1]: 1 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]: 10.5.180.8/24 Enter Default Gateway: 10.5.180.1

Step 8: 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 9: 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): RS213-vWAAS Enter NTP Server IP Address [None]: 10.4.48.17

Step 10: Configure the WCCP router list.

Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []: 10.255.255.213

Step 11: 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 12: Verify the configuration settings.

Parameter	Configured Value
2. Time Zone	PST8PDT -8 0
3. Management Interface	Virtual 1/0
Autosense	Disabled
4. DHCP	Disabled
Speed	1000 (full-duplex)
5. IP Address	10.5.180.8
6. IP Network Mask	255.255.255.0
7. IP Default Gateway	10.5.180.1
8. CM IP Address	10.4.48.100
9. DNS IP Address	10.4.48.10
10. Domain Name(s)	cisco.local
11. Host Name	RS213-vWAAS
12. NTP Server Address	10.4.48.17
13. WCCP Router List	10.255.255.213
13. License	Enterprise
ESC Quit ? Help ! CLI —	WAAS Final Configuration
Press 'y' to select configur	ation, <f2> to see all configuration, 'd' to toggle</f2>
defaults display, <1-12> to	change specific parameter [y]: y
Router WCCP c	onfiguration
First WCCP router IP in the	WCCP router list seems to be an external address;
WCCP configuration on extern	al routers is not allowed through SETUP. Please press
ENTER to apply WAAS configur	ation on WAVE
Applying WAAS configuration	on WAE
May take a few seconds to co	mplete
WAAS configuration applied s	uccessfully!!
Saved configuration to memor	У.
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 13: In the EXEC mode, enable the propagation of local configuration changes to the Cisco WAAS Central Manager.

cms lcm enable

Step 14: 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 15:** 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 clscol23
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 **clsco123** wccp tcp-promiscuous service-pair 61 62 enable

Next, you will configure device management protocols.

Step 16: Log in to the Cisco vWAAS.

Step 17: Generate the RSA key and enable the sshd service. This enables SSH.

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

Step 18: 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 19: 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 Virtual 1/0
ip access-group 155 in
exit
!
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
snmp-server access-list 55
```

Step 20: 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 21: After you make configuration changes, in the EXEC mode, save the configuration.

copy running-config startup-config

Each Cisco vWAAS instance registers with the Cisco WAAS Central Manager as it becomes active on the network.

Step 22: If you want to verify the Cisco vWAAS registration, on the respective vWAAS instance or via the web interface to the Cisco WAAS Central Manager, enter **show cms info**.

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 MPLS WAN Technology Design Guide or VPN WAN Technology Design 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 and other protocols which can not be optimized from WCCP redirect by using a redirect list. A detailed listing is included in Table 11 and Table 12.

December 2013



```
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clscol23
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clscol23
1
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
deny tcp any any eq 161
deny tcp any eq 161 any
deny tcp any any eq 162
deny tcp any eq 162 any
deny tcp any any eq 2000
deny tcp any eq 2000 any
deny tcp any any eq 2443
deny tcp any eq 2443 any
deny tcp any any eq 5060
deny tcp any eq 5060 any
deny tcp any any eq 5061
deny tcp any eq 5061 any
deny tcp any any eq 1718
deny tcp any eq 1718 any
deny tcp any any eq 1720
deny tcp any eq 1720 any
deny tcp any any eq 2428
deny tcp any eq 2428 any
deny tcp any any eq 443
deny tcp any eq 443 any
deny tcp any any eq 8443
deny tcp any eq 8443 any
deny tcp any any eq 6970
deny tcp any eq 6970 any
deny tcp any any eq 689
deny tcp any eq 689 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-Channel1

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 GigabitEthernet0/3
ip wccp 62 redirect in

Example: DMVPN WAN Interface

interface Tunnel10
 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.



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.

Parameter	CVD values primary WAVE	CVD values secondary WAVE	Site-specific values
Switch interface number	1/0/3	1/0/4	
VLAN number	64	64	
Time zone	PST8PDT -8 0	PST8PDT -8 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	RS203-WAVE-SRE-1	RS203-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	

Table 19 - Cisco WAAS on the Cisco SRE module network parameters

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 Campus Wired LAN Technology Design 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 MPLS WAN Technology Design Guide or VPN WAN Technology Design 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 192.0.2.2 255.255.252
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.

December 2013



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: Login to the Cisco WAVE console.

The factory default username is admin and the factory default password is default.

Procedure 3 Configure the WAAS Node

Step 1: 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 Configurat:	ion ———
Press 'y' to select above d	efaults, `n' to configure a	all, <1-3> to changespecific
default [y]: n		

Step 2: Configure the interception method.

WCCP
 AppNav Controller
 Other
 Select Interception Method [1]: 1

Step 3: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)> [UTC 0 0]:
PST8PDT -8 0
```

Step 4: 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** 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 5: 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 6: 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): RS203-WAVE-SRE-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 ...) []: 10.255.251.203 10.255.253.203

Step 8: 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 9: Verify the configuration settings.

Parameter	Configured Value	
1. Interception Method	WCCP	
2. Time Zone	PST8PDT -8 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 RS203-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, $\langle F2 \rangle$ 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 10: In the EXEC mode, enable the propagation of local configuration changes to the Cisco WAAS Central Manager.

cms lcm enable

Step 11: 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 12: 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 clscol23
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 **clsco123** wccp tcp-promiscuous service-pair 61 62 enable

Next, you will configure device management protocols.

Step 13: Log in to the Cisco WAVE appliance.

Step 14: Generate the RSA key and enable the sshd service. This enables SSH.

ssh-key-generate key-length 2048
sshd enable
no telnet enable

Step 15: 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 16: 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
exit
!
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
snmp-server access-list 55
```

Step 17: 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

1

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 18: 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 19: 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 20: When this configuration is complete, press the *escape sequence* **Ctrl+Shift+6** and then enter **x**. The command line of the host router returns.



Step 21: If you are deploying a cluster of Cisco WAAS nodes, repeat Procedure 1 through Procedure 3 for the remaining nodes.

Procedure 4 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 MPLS WAN Technology Design Guide or VPN WAN Technology Design 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 and other protocols which can not be optimized from WCCP redirect by using a redirect list. A detailed listing is included in Table 11 and Table 12.

```
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clscol23
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clscol23
!
ip access-list standard WAVE
permit 10.5.52.8
```

permit	10.5	.52.9
ip acce	ess-li	st extended WAAS-REDIRECT-LIST
remar	WAAS	WCCP Redirect List
deny t	tcp an	y any eq 22
deny t	tcp an	y eq 22 any
deny t	tcp an	y eq telnet any
deny t	tcp an	y any eq telnet
deny t	tcp an	y eq tacacs any
deny t	tcp an	y any eq tacacs
deny t	tcp an	y eq bgp any
deny t	tcp an	y any eq bgp
deny f	tcp an	y any eq 123
deny t	tcp an	y eq 123 any
deny t	tcp an	y any eq 161
deny t	tcp an	y eq 161 any
deny t	tcp an	y any eq 162
deny t	tcp an	y eq 162 any
deny t	tcp an	y any eq 2000
deny t	tcp an	y eq 2000 any
deny t	tcp an	y any eq 2443
deny t	tcp an	y eq 2443 any
deny t	tcp an	y any eq 5060
deny t	tcp an	y eq 5060 any
deny t	tcp an	y any eq 5061
deny t	tcp an	y eq 5061 any
deny t	tcp an	y any eq 1718
deny t	tcp an	y eq 1718 any
deny t	tcp an	y any eq 1720
deny t	tcp an	y eq 1720 any
		y any eq 2428
		y eq 2428 any
		y any eq 443
deny t	tcp an	y eq 443 any
		y any eq 8443
		y eq 8443 any
		y any eq 6970
		y eq 6970 any
		y any eq 689
		y eq 689 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.

Configuring Cisco WAAS Express

- 1. Configure the Central Manager for WAASx
- 2. Create WAAS Central Manager user
- 3. Enable WAAS Express on the remote-site router
- 4. Register the router to the WAAS Central Manager

Configuration Checklist

PROCESS

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.

Parameter	CVD values primary WAVE	Site-specific values
WAAS Central Manager	10.4.48.100	
WAASx username	waascm	
WAASx password	c1sco123	

Table 20 - Cisco WAAS Express network system parameters checklist

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 > Cisco IOS Router Global Credentials**. 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 waascm and password c1sco123)

 cisco	Cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Locations Dashboard Configure I v Monitor I v Admin I v	admin
	🕽 Remove Settings 🔞 Refresh		
User Name:	: waascm 🛈 User Na	ne is required if 'ip http authentication local/aaa' is configured on Cisco IOS router(s).	
Password:	*		
① Configuring	ng global credentials will not be applied on the Cisco IOS ro	uter(s). Performing changes to credentials may impact communication between Central Manager	and Cisco IOS router.
Submit	Reset		

Procedure 2 Create WAAS Central Manager user

There are two options when you are creating the Cisco WAAS Central Manager 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 Central Manager user.

Option 1: Create a local user account

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

username waascm privilege 15 password clscol23

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 waascm and password c1sco123)

Users and Identity Stor	es > Internal	Identity Stores > Use	ers > Crea	ate			
General							
🌣 Name:	waascm		Status:	Enabled	•	0	
Description:	WAAS Cer	ntral Manager user					
C Identity Group:	All Groups				Sele	ect	
Password Info Password must: • Contain 4		cters					Enable Password Information Password must • Contain 4 - 32 characters
C Password Typ	e:	Internal Users			S	elect	Enable Password:
Password:		•••••					Confirm Password:
Confirm Pass	word:						
🗖 Change p	assword or	n next login					
User Informatio There are no a		entity attributes def	ined for (user record	ls		
© = Required field	ls						
•	_						m
Submit Cance	H						

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

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

dentity Groups		
Filter: 📃 Matcl	nit. Go 🔻	
Name 🔺	Description	
C v All Groups	Identity Group Root	
C Helpdesk	Users who are allowed to login to a device but not make changes	
 Network Admins 	Users who are allowed to login to a device and make changes	
Create Duplicate (File Operations Export	
OK Cancel	н	elp
		-

Step 7: Click Submit.

Procedure 3 Enable WAAS Express on the remote-site router

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 MPLS WAN Technology Design Guide or VPN WAN Technology Design 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 1: Verify SSH and HTTPS servers are enabled on the router. If not already configured, configure these services now.

Tech Tip

1

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

Specify the transport preferred none on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
no ip http server
ip http secure-server
line vty 0 15
transport input ssh
transport preferred none
```

Step 2: If you are using AAA authentication, configure the HTTP server to use AAA.

ip http authentication aaa

Step 3: Log in to the Cisco WAAS Central Manager through the web interface (for example, https://waas-wcm-1. cisco.local:8443).

Step 4: Navigate to Admin>Registration>Cisco IOS Routers.

				ups Devices AppNa ure∣▼ Monitor∣▼			admin Logout Help About
Cisco IOS Router Registration	Kouters						
Router IP address entry method:	Manual Import	CSV file					
IP Address(es):				① Comma separate	ed list up to	o 50 entries	
Username:							
Password:							
Enable Password:							
HTTP Authentication Type:	Local	•					
Central Manager IP Address: *	10.4.48.100 ① Update the Central Manager IP Address if NATed environment is used.						
③ SSH v1 or SSH v2 must be enabled	led on routers.						
 These credentials are used once 	-						
 These credentials are not used to 	for communication betw	een the Central Mana	iger and the router	s after registration finis	hes.		
Register Retry Reset							
Registration Status							Total O
IP Address Hostname	Router type	Status					
			No data	available			

Step 5: Enter the management information of the Cisco WAAS Express remote-site routers, then click **Register**. You may enter the IP addresses of multiple routers (separated by a comma) if they share the same authentication credentials.

- Router IP address entry method-Manual
- IP Address(es)-10.255.251.204
- Username-waascm
- Password-c1sco123
- Enable Password-c1sco123
- HTTP Authentication Type-AAA
- Central Manager IP Address-10.4.48.100

	Application Services	Home Device Groups Devices AppNav Clusters Locations Dashboard Configure I Monitor I Admin I
Home > Admin > Registration > Cisco IOS Cisco IOS Router Registration	Routers	
CISCO 105 NOULER Negistration		
Router IP address entry method:	● Manual ○ Import CSV file	
IP Address(es):	10.255.251.204	① Comma separated list up to 50 entries
Username:	waascm	
Password:	******	
Enable Password:	••••••	
HTTP Authentication Type:	AAA	
Central Manager IP Address: *	10.4.48.100	(i) Update the Central Manager IP Address if NATed environment is used.
(i) SSH v1 or SSH v2 must be enab	led on routers.	
(i) These credentials are used once	e to register all the listed routers, whi	ch should have the same credentials.
(i) These credentials are not used t	for communication between the Cen	tral Manager and the routers after registration finishes.
Register Retry Reset		
Registration Status		Total O
IP Address Hostname	Router type Status	
	No data availa	ble
•	m	,

Step 6: Verify successful registration.

Registration Status			Total 1
IP Address	Hostname	Router type	Status
10.255.251.204	RS204-1941	WAAS Express	\checkmark Successfully processed the registration request

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	5.3.1
	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	5.3.1
	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
AppNav Controller Appliance	WAVE-594 bundled with 4port 10 GigE AppNav IOM	WAVE-APNV-10GE	5.3.1
	Cisco Wide Area Virtualization Engine 8541	WAVE-8541-K9	
	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	
	AppNav IOM for WAVE - 12 port GigE copper	WAVE-APNV-GE-12T	
	AppNav IOM for WAVE - 12 port GigE SFP	WAVE-APNV-GE12SFP	
AppNav-XE Controller	Aggregation Services 1002X Router	ASR1002X-5G-VPNK9	IOS-XE 15.3(3)S
	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	Advanced Enterprise license
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
Application Accelerator Appliance	Cisco Wide Area Virtualization Engine 8541	WAVE-8541-K9	5.3.1
	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	
Application Accelerator Virtual	Virtual WAAS	WAAS-ENT-VIRT-K9	5.3.1
Appliance	License for 50000 optimized connections	LIC-50K-VWAAS	
	License for 12000 optimized connections	LIC-12K-VWAAS	
	License for 6000 optimized connections	LIC-6K-VWAAS	
	License for 2500 optimized connections	LIC-2500-VWAAS	
	License for 1300 optimized connections	LIC-1300-VWAAS	
	License for 750 optimized connections	LIC-750-VWAAS	

WAAS Remote Site

Functional Area	Product Description	Part Numbers	Software
Application Accelerator Appliance	Cisco Wide Area Virtualization Engine 694	WAVE-694-K9	5.3.1
	Cisco Wide Area Virtualization Engine 594	WAVE-594-K9	
	Cisco Wide Area Virtualization Engine 294	WAVE-294-K9	
Application Accelerator Virtual Appliance	Virtual WAAS 5.3 SW image. (C2911-AX/K9, C2921-AX/K9 and C2951-AX/K9 include 1300 connection RTU license for vWAAS. C3925-AX/K9 and C3945-AX/K9 include 2500 connection RTU license for vWAAS.)	SF-VWAAS-5.3-K9	5.3.1
	Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Six Core processor, 8GB RAM, 2 SD cards, PCIe card	UCS-E160DP-M1/K9	
	Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Six Core processor, 8GB RAM, 2 SD cards	UCS-E160D-M1/K9	
	Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Quad Core processor, 8GB RAM, 2 SD cards, PCIe card	UCS-E140DP-M1/K9	
	Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Quad Core processor, 8GB RAM, 2 SD cards	UCS-E140D-M1/K9	
	Cisco UCS E-Series Single-Wide Server Blades, Intel Xeon E3 Quad Core processor, 8GB RAM, 2 SD cards	UCS-E140S-M1/K9	
Remote-Site WAVE SRE	Cisco WAAS 5.3 SRE SW image. (C2911-AX/K9, C2921-AX/K9 and C2951-AX/K9 include 1300 connection RTU license for WAAS. C3925-AX/K9 and C3945-AX/K9 include 2500 connection RTU license for WAAS.)	SF-WAAS-5.3-SM-K9	5.3.1
	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	
	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	
Remote-Site WAAS Express	Cisco ISR 1941 Router w/ 2 GE, 2 EHWIC slots, 256MB CF, 2.5GB DRAM, IP Base, DATA, SEC, AX license with; AVC and WAAS-Express	C1941-AX/K9	15.2(4)M4 securityk9 license datak9 license

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002X Router	ASR1002X-5G-VPNK9	IOS-XE 15.3(3)S Advanced Enterprise license
	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.2(4)M4 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 ISR 3945 w/ SPE150, 3GE, 4EHWIC, 4DSP, 4SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, and WAAS/vWAAS with 2500 connection RTU	C3945-AX/K9	15.2(4)M4 securityk9 license datak9 license
	Cisco ISR 3925 w/ SPE100 (3GE, 4EHWIC, 4DSP, 2SM, 256MBCF, 1GBDRAM, IP Base, SEC, AXlicenses with; DATA, AVC, WAAS/vWAAS with 2500 connection RTU	C3925-AX/K9	
	Cisco ISR 2951 w/ 3 GE, 4 EHWIC, 3 DSP, 2 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2951-AX/K9	
	Cisco ISR 2921 w/ 3 GE, 4 EHWIC, 3 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2921-AX/K9	
	Cisco ISR 2911 w/ 3 GE,4 EHWIC, 2 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC and WAAS/vWAAS with 1300 connection RTU	C2911-AX/K9	
	Cisco ISR 1941 Router w/ 2 GE, 2 EHWIC slots, 256MB CF, 2.5GB DRAM, IP Base, DATA, SEC, AX license with; AVC and WAAS-Express	C1941-AX/K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.2(4)M4 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	3.4.0.SG(15.1-2SG) 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 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	_
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 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	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 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)SE2 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	

Appendix B: Changes

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

- We added functional summary of AppNav and its components to the design overview.
- We updated the Cisco WAAS software version to 5.3.1.
- We updated the Cisco ASR1000 Series router software to 15.3(3)S0.
- We update the Cisco ISR G2 Series router software to 15.2(4)M4.
- We added two new WAN aggregation design models:
 - AppNav Off Path
 - AppNav-XE
- We added the AppNav controller I/O module to support the AppNav Off Path design model.
- We added support for Cisco vWAAS at the primary site.
- We added support for Cisco vWAAS at remote sites using the UCS E-Series module on the Cisco ISR-G2 2900 Series and 3900 Series routers.
- We simplified the configuration procedures for Cisco WAAS Express.

Appendix C: Configuration Examples

Central Manager

WAAS Central Manager (vWAAS)

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
1
device mode central-manager
!
1
!
hostname WAAS-WCM-1
!
clock timezone PST8PDT -8 0
!
1
ip domain-name cisco.local
!
1
primary-interface Virtual 1/0
!
interface Virtual 1/0
ip address 10.4.48.100 255.255.255.0
ip access-group 155 in
exit
interface Virtual 2/0
 shutdown
exit
!
ip default-gateway 10.4.48.1
1
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
1
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
!
```

```
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
!
!
ntp server 10.4.48.17
!
l
Į.
1
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco
snmp-server community cisco123 rw
snmp-server access-list 55
!
!
1
tacacs key ****
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
!
!
no telnet enable
!
sshd enable
!
!
cms enable
!
!
! End of WAAS configuration
```
WCCP Design Model

Primary Site WAAS Node

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode application-accelerator
!
interception-method wccp
!
!
hostname WAE-7341-1
!
clock timezone PST8PDT -8 0
!
1
ip domain-name cisco.local
!
!
primary-interface PortChannel 1
!
interface PortChannel 1
ip address 10.4.32.161 255.255.255.192
ip access-group 155 in
exit
!
interface GigabitEthernet 1/0
channel-group 1
exit
interface GigabitEthernet 2/0
channel-group 1
exit
!
ip default-gateway 10.4.32.129
!
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
Ţ.
ip name-server 10.4.48.10
!
1
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
 exit
!
```

```
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
!
!
ntp server 10.4.48.17
!
!
wccp router-list 7 10.4.32.241 10.4.32.242 10.4.32.243
wccp tcp-promiscuous service-pair 61 62
router-list-num 7
password ****
redirect-method gre
egress-method wccp-gre
enable
exit
!
!
1
L
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco
snmp-server community cisco123 rw
snmp-server access-list 55
1
!
!
tacacs key ****
tacacs password ascii
tacacs host 10.4.48.15 primary
1
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
!
Ţ.
no telnet enable
!
sshd enable
!
!
```

```
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
1
!
accelerator mapi wansecure-mode auto
!
!
central-manager address 10.4.48.100
cms enable
1
!
stats-collector logging enable
stats-collector logging rate 30
!
1
! End of WAAS configuration
```

Primary Site WAAS Node (vWAAS)

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode application-accelerator
!
interception-method wccp
!
!
hostname vWAAS-12000-1
!
clock timezone PST8PDT -8 0
1
!
ip domain-name cisco.local
!
1
primary-interface Virtual 1/0
1
interface Virtual 1/0
ip address 10.4.32.162 255.255.255.192
ip access-group 155 in
exit
interface Virtual 2/0
shutdown
exit
!
ip default-gateway 10.4.32.129
!
!
no auto-register enable
```

```
ļ
! ip path-mtu-discovery is disabled in WAAS by default
1
ip name-server 10.4.48.10
1
!
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
1
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
!
!
ntp server 10.4.48.17
!
!
wccp router-list 7 10.4.32.241 10.4.32.242 10.4.32.243
wccp tcp-promiscuous service-pair 61 62
router-list-num 7
password ****
redirect-method gre
egress-method wccp-gre
enable
exit
1
!
!
!
username admin password 1 ****
username admin privilege 15
1
snmp-server community cisco
snmp-server community cisco123 rw
snmp-server access-list 55
!
!
1
tacacs key ****
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
!
1
no telnet enable
1
sshd enable
1
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
accelerator mapi wansecure-mode auto
!
!
central-manager address 10.4.48.100
cms enable
!
1
stats-collector logging enable
stats-collector logging rate 30
!
!
! End of WAAS configuration
```

WAN-Aggregation Router

```
version 15.3
1
hostname CE-ASR1001-2
!
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE password clsco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE password c1sco123
!
interface Loopback0
ip address 10.4.32.242 255.255.255.255
1
interface Port-channel2
ip address 10.4.32.6 255.255.255.252
ip wccp 61 redirect in
I.
interface GigabitEthernet0/0/3
ip address 192.168.4.1 255.255.255.252
ip wccp 62 redirect in
1
```

```
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
        tcp any eq bgp any
deny
deny
        tcp any any eq bgp
        tcp any any eq 123
deny
deny
        tcp any eq 123 any
        tcp any any eq 161
deny
deny
        tcp any eq 161 any
        tcp any any eq 162
deny
        tcp any eq 162 any
deny
        tcp any any eq 2000
deny
        tcp any eq 2000 any
deny
        tcp any any eq 2443
deny
        tcp any eq 2443 any
deny
deny
        tcp any any eq 5060
        tcp any eq 5060 any
deny
        tcp any any eq 5061
deny
        tcp any eq 5061 any
deny
deny
        tcp any any eq 1718
        tcp any eq 1718 any
deny
        tcp any any eq 1720
deny
        tcp any eq 1720 any
deny
deny
        tcp any any eq 2428
        tcp any eq 2428 any
deny
        tcp any any eq 443
deny
        tcp any eq 443 any
deny
        tcp any any eq 8443
deny
        tcp any eq 8443 any
deny
        tcp any any eq 6970
deny
deny
        tcp any eq 6970 any
deny
        tcp any any eq 689
        tcp any eq 689 any
deny
permit tcp any any
```

WAN-Aggregation Router (DMVPN hub)

```
version 15.3
!
hostname VPN-ASR1002X-1
!
ip wccp source-interface Loopback0
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 clsco123
!
interface Loopback0
ip address 10.4.32.243 255.255.255.255
1
interface Port-channel3
 ip address 10.4.32.18 255.255.255.252
ip wccp 61 redirect in
ip wccp 62 redirect out
!
interface Tunnel10
bandwidth 100000
ip address 10.4.34.1 255.255.254.0
1
ip access-list standard WAVE
permit 10.4.32.161
permit 10.4.32.162
1
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 bqp
 deny tcp any any eq 123
 deny tcp any eq 123 any
 deny tcp any any eq 161
 deny tcp any eq 161 any
 deny tcp any any eq 162
 deny tcp any eq 162 any
 deny tcp any any eq 2000
 deny tcp any eq 2000 any
       tcp any any eq 2443
 deny
      tcp any eq 2443 any
 deny
 deny
       tcp any any eq 5060
```

deny	tcp	any	eq 5060 any
deny	tcp	any	any eq 5061
deny	tcp	any	eq 5061 any
deny	tcp	any	any eq 1718
deny	tcp	any	eq 1718 any
deny	tcp	any	any eq 1720
deny	tcp	any	eq 1720 any
deny	tcp	any	any eq 2428
deny	tcp	any	eq 2428 any
deny	tcp	any	any eq 443
deny	tcp	any	eq 443 any
deny	tcp	any	any eq 8443
deny	tcp	any	eq 8443 any
deny	tcp	any	any eq 6970
deny	tcp	any	eq 6970 any
deny	tcp	any	any eq 689
deny	tcp	any	eq 689 any
permit	tcp	any	any

AppNav Off Path Design Model

AppNav Controller and WAAS Node

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode appnav-controller
!
interception-method wccp
!
!
hostname AppNav-WAVE-2
!
clock timezone PST8PDT -8 0
1
!
ip domain-name cisco.local
!
!
primary-interface PortChannel 1
1
interface PortChannel 1
ip address 10.4.32.164 255.255.255.192
ip access-group 155 in
exit
interface PortChannel 2
 ip address 10.4.32.72 255.255.255.192
ip access-group 155 in
```

```
exit
!
interface GigabitEthernet 0/0
shutdown
exit
interface GigabitEthernet 0/1
shutdown
exit
interface GigabitEthernet 1/0
channel-group 1
exit
interface GigabitEthernet 1/1
channel-group 1
exit
interface GigabitEthernet 1/2
channel-group 2
exit
interface GigabitEthernet 1/3
channel-group 2
exit
interface GigabitEthernet 1/4
shutdown
exit
interface GigabitEthernet 1/5
shutdown
exit
interface GigabitEthernet 1/6
shutdown
exit
interface GigabitEthernet 1/7
shutdown
exit
interface GigabitEthernet 1/8
shutdown
exit
interface GigabitEthernet 1/9
shutdown
exit
interface GigabitEthernet 1/10
shutdown
exit
interface GigabitEthernet 1/11
shutdown
exit
!
ip default-gateway 10.4.32.129
!
```

```
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
1
ip name-server 10.4.48.10
!
ip route 10.4.32.2 255.255.255.255 10.4.32.65
ip route 10.4.32.6 255.255.255.255 10.4.32.65
ip route 10.4.32.18 255.255.255.255 10.4.32.65
Ţ.
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
1
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
1
!
ntp server 10.4.48.17
!
!
wccp router-list 1 10.4.32.2 10.4.32.6 10.4.32.18
wccp tcp-promiscuous service-pair 61 62
router-list-num 1
password ****
redirect-method gre
enable
exit
1
!
1
!
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco123 rw
snmp-server community cisco
snmp-server access-list 55
!
!
!
tacacs key ****
tacacs password ascii
```

```
tacacs host 10.4.48.15 primary
1
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
1
Į.
!
I.
no telnet enable
1
sshd enable
1
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
service-insertion service-node-group WNG-Default
 service-node 10.4.32.161
 service-node 10.4.32.162
 service-node 10.4.32.163
 service-node 10.4.32.164
 service-node 10.4.32.165
 service-node 10.4.32.166
 exit
1
!
accelerator mapi wansecure-mode auto
!
1
!
central-manager address 10.4.48.100
cms enable
!
!
stats-collector logging enable
stats-collector logging rate 30
!
service-insertion appnav-controller-group scg
 appnav-controller 10.4.32.163
 appnav-controller 10.4.32.164
 exit
!
!
```

```
service-insertion service-context AppNav-IOM
 description AppNav IOM CLuster
 authentication shal key ****
 appnav-controller-group scg
  service-node-group WNG-Default
  service-policy appnav default
 enable
 exit
1
service-insertion service-node
 description WN of AppNav-IOM
 authentication shal key ****
 enable
 exit
1
!
! End of WAAS configuration
```

Primary Site WAAS Node

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode application-accelerator
!
interception-method appnav-controller
!
!
hostname WAVE7341-1
!
clock timezone PSt8PDT -8 0
!
1
ip domain-name cisco.local
!
I.
primary-interface PortChannel 1
!
interface PortChannel 1
 ip address 10.4.32.161 255.255.255.192
ip access-group 155 in
exit
!
interface GigabitEthernet 1/0
channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 exit
```

```
!
ip default-gateway 10.4.32.129
!
!
no auto-register enable
1
! ip path-mtu-discovery is disabled in WAAS by default
1
ip name-server 10.4.48.10
!
Ţ.
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
1
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
1
!
ntp server 10.4.48.17
!
!
!
!
!
1
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco
snmp-server community cisco123 rw
snmp-server access-list 55
!
!
1
tacacs key ****
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
```

```
ļ
L
Į.
no telnet enable
1
sshd enable
1
1
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
1
!
!
accelerator mapi wansecure-mode auto
1
!
I.
central-manager address 10.4.48.100
cms enable
!
1
stats-collector logging enable
stats-collector logging rate 30
!
service-insertion service-node
 description WN of AppNav-IOM
 authentication shal key ****
 enable
 exit
!
!
! End of WAAS configuration
```

WAN-Aggregation Router

```
version 15.3
!
hostname CE-ASR1001-2
!
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list APPNAV password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list APPNAV password c1sco123
!
interface Loopback0
ip address 10.4.32.242 255.255.255
!
interface Port-channel2
ip address 10.4.32.6 255.255.255.252
```

```
ip wccp 61 redirect in
I.
interface Tunnel5
description GRE tunnel for AppNav OffPath devices
ip address 192.0.2.2 255.255.255.0
no ip redirects
ip wccp redirect exclude in
tunnel source Port-channel2
 tunnel mode gre multipoint
!
interface GigabitEthernet0/0/3
ip address 192.168.4.1 255.255.255.252
ip wccp 62 redirect in
L
ip access-list standard APPNAV
permit 10.4.32.71
permit 10.4.32.72
!
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
       tcp any any eq 22
deny
       tcp any eq 22 any
 denv
       tcp any eq telnet any
 deny
       tcp any any eq telnet
 deny
 deny
       tcp any eq tacacs any
       tcp any any eq tacacs
 deny
       tcp any eq bgp any
 deny
       tcp any any eq bgp
 deny
 deny
       tcp any any eq 123
       tcp any eq 123 any
 deny
       tcp any any eq 161
 deny
       tcp any eq 161 any
 deny
 deny
       tcp any any eq 162
       tcp any eq 162 any
 deny
       tcp any any eq 2000
 deny
       tcp any eq 2000 any
 deny
       tcp any any eq 2443
 deny
       tcp any eq 2443 any
 deny
       tcp any any eq 5060
 deny
 deny
       tcp any eq 5060 any
       tcp any any eq 5061
 deny
       tcp any eq 5061 any
 deny
       tcp any any eq 1718
 deny
       tcp any eq 1718 any
 deny
       tcp any any eq 1720
 deny
       tcp any eq 1720 any
 deny
 deny
       tcp any any eq 2428
```

```
denytcpanyeq2428anydenytcpanyanyeq443denytcpanyeq443anydenytcpanyanyeq8443denytcpanyeq8443anydenytcpanyeq6970denytcpanyeq6970anydenytcpanyeq689denytcpanyeq689denytcpanyeq689denytcpanyanyeqdenytcpanyanyeqdenytcpanyanyeq
```

WAN-Aggregation Router (DMVPN hub)

```
version 15.3
I.
hostname VPN-ASR1002X-1
1
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list APPNAV password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list APPNAV password c1sco123
!
interface Loopback0
ip address 10.4.32.243 255.255.255.255
Ţ.
interface Port-channel3
ip address 10.4.32.18 255.255.255.252
ip wccp 61 redirect in
ip wccp 62 redirect out
1
interface Tunnel10
bandwidth 100000
ip address 10.4.34.1 255.255.254.0
!
ip access-list standard APPNAV
permit 10.4.32.71
permit 10.4.32.72
1
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
```

tcp	any	eq 123 any
tcp	any	any eq 161
tcp	any	eq 161 any
tcp	any	any eq 162
tcp	any	eq 162 any
tcp	any	any eq 2000
tcp	any	eq 2000 any
tcp	any	any eq 2443
tcp	any	eq 2443 any
tcp	any	any eq 5060
tcp	any	eq 5060 any
tcp	any	any eq 5061
tcp	any	eq 5061 any
tcp	any	any eq 1718
tcp	any	eq 1718 any
tcp	any	any eq 1720
tcp	any	eq 1720 any
tcp	any	any eq 2428
tcp	any	eq 2428 any
tcp	any	any eq 443
tcp	any	eq 443 any
tcp	any	any eq 8443
tcp	any	eq 8443 any
tcp	any	any eq 6970
tcp	any	eq 6970 any
tcp	any	any eq 689
tcp	any	eq 689 any
tcp	any	any
	tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp	tcp any tcp any

AppNav-XE Design Model

AppNav-XE Controller

```
version 15.3
!
hostname METRO-ASR1001-1
!
class-map type appnav match-any RTSP
match access-group name APPNAV-ACL-RTSP
class-map type appnav match-any MAPI
match protocol mapi
class-map type appnav match-any HTTP
match access-group name APPNAV-ACL-HTTP
class-map type appnav match-any APPNAV-class-default
match access-group name APPNAV-ACL-class-default
class-map type appnav match-any CIFS
match access-group name APPNAV-ACL-CIFS
```

```
class-map type appnav match-any Citrix-CGP
 match access-group name APPNAV-ACL-Citrix-CGP
class-map type appnav match-any HTTPS
match access-group name APPNAV-ACL-HTTPS
class-map type appnav match-any Citrix-ICA
 match access-group name APPNAV-ACL-Citrix-ICA
class-map type appnav match-any NFS
match access-group name APPNAV-ACL-NFS
class-map type appnav match-any epmap
match access-group name APPNAV-ACL-epmap
I.
policy-map type appnav APPNAV-1-PMAP
 class MAPI
  distribute service-node-group WNG-Default-1
  monitor-load mapi
 class HTTPS
  distribute service-node-group WNG-Default-1
  monitor-load ssl
 class HTTP
  distribute service-node-group WNG-Default-1
  monitor-load http
 class CIFS
  distribute service-node-group WNG-Default-1
  monitor-load cifs
 class Citrix-ICA
  distribute service-node-group WNG-Default-1
  monitor-load ica
 class Citrix-CGP
  distribute service-node-group WNG-Default-1
  monitor-load ica
 class epmap
  distribute service-node-group WNG-Default-1
  monitor-load MS-port-mapper
 class NFS
  distribute service-node-group WNG-Default-1
  monitor-load nfs
 class RTSP
  distribute service-node-group WNG-Default-1
 class APPNAV-class-default
  distribute service-node-group WNG-Default-1
service-insertion service-node-group WNG-Default-1
  service-node 10.4.32.162
1
service-insertion appnav-controller-group scg
  appnav-controller 10.4.32.22
  appnav-controller 10.4.32.34
```

```
!
service-insertion service-context waas/1
 authentication shal key 7 130646010803557878
 appnav-controller-group scg
 service-node-group WNG-Default-1
  service-policy APPNAV-1-PMAP
 vrf global
 enable
L
interface Port-channel5
ip address 10.4.32.34 255.255.255.252
1
interface GigabitEthernet0/0/3
no ip address
1
interface GigabitEthernet0/0/3.38
encapsulation dot1Q 38
ip address 10.4.38.1 255.255.255.0
service-insertion waas
Т
interface GigabitEthernet0/0/3.39
encapsulation dot1Q 39
ip address 10.4.39.1 255.255.255.0
service-insertion waas
L
interface AppNav-Compress1
ip unnumbered Port-channel1
no keepalive
1
interface AppNav-UnCompress1
ip unnumbered Port-channel1
no keepalive
L
ip access-list extended APPNAV-ACL-CIFS
permit tcp any any eq 139
permit tcp any any eq 445
ip access-list extended APPNAV-ACL-Citrix-CGP
permit tcp any any eq 2598
ip access-list extended APPNAV-ACL-Citrix-ICA
permit tcp any any eq 1494
ip access-list extended APPNAV-ACL-HTTP
permit tcp any any eq www
permit tcp any any eq 3128
permit tcp any any eq 8000
permit tcp any any eq 8080
permit tcp any any eq 8088
ip access-list extended APPNAV-ACL-HTTPS
```

```
permit tcp any any eq 443
ip access-list extended APPNAV-ACL-NFS
permit tcp any any eq 2049
ip access-list extended APPNAV-ACL-RTSP
permit tcp any any eq 554
permit tcp any any eq 8554
ip access-list extended APPNAV-ACL-class-default
permit tcp any any
ip access-list extended APPNAV-ACL-epmap
permit tcp any any eq msrpc
```

Primary Site WAAS Node

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode application-accelerator
!
interception-method appnav-controller
!
Ţ.
hostname WAE7341-2
1
clock timezone PST8PDT -8 0
1
!
ip domain-name cisco.local
!
1
primary-interface PortChannel 1
1
interface PortChannel 1
ip address 10.4.32.162 255.255.255.192
ip access-group 155 in
exit
!
interface GigabitEthernet 1/0
channel-group 1
exit
interface GigabitEthernet 2/0
channel-group 1
shutdown
exit
!
ip default-gateway 10.4.32.129
!
!
no auto-register enable
1
```

```
! ip path-mtu-discovery is disabled in WAAS by default
I.
ip name-server 10.4.48.10
!
I.
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
1
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
1
!
ntp server 10.4.48.17
!
!
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco
snmp-server community cisco123 rw
snmp-server access-list 55
1
!
!
tacacs key ****
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
Ţ.
!
!
no telnet enable
1
sshd enable
!
1
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
```

```
ļ
!
!
accelerator mapi wansecure-mode auto
!
!
!
central-manager address 10.4.48.100
cms enable
!
!
!
!
!
stats-collector logging enable
stats-collector logging rate 30
!
service-insertion service-node
 description WN of AppNav-XE
 authentication shal key ****
 enable
 exit
!
!
! End of WAAS configuration
```

Remote Sites

RS202 WAAS Node

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode application-accelerator
!
interception-method wccp
!
!
hostname RS202-WAVE594
!
clock timezone PST8PDT -8 0
!
!
ip domain-name cisco.local
!
!
primary-interface GigabitEthernet 0/0
!
```

```
interface GigabitEthernet 0/0
 ip address 10.5.68.8 255.255.255.0
ip access-group 155 in
exit
interface GigabitEthernet 0/1
 shutdown
exit
!
ip default-gateway 10.5.68.1
!
Ţ.
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
bmc lan ip address set-to-factory-default
no bmc lan enable
no bmc serial-over-lan enable
1
!
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
1
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
!
!
ntp server 10.4.48.17
1
!
wccp router-list 7 10.255.252.202
wccp tcp-promiscuous service-pair 61 62
router-list-num 7
password ****
 redirect-method gre
 egress-method wccp-gre
enable
exit
L
!
username admin password 1 ****
```

```
username admin privilege 15
!
snmp-server community cisco
snmp-server community cisco123 rw
snmp-server access-list 55
!
!
tacacs key ****
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
Į.
1
!
no telnet enable
1
sshd enable
1
1
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
accelerator mapi wansecure-mode auto
!
!
virtual-blade enable
!
central-manager address 10.4.48.100
cms enable
!
!
1
!
!
stats-collector logging enable
stats-collector logging rate 30
!
!
! End of WAAS configuration
```

RS202 WAN Router

```
version 15.2
!
hostname RS202-2911
!
ip wccp source-interface Loopback0
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
interface Loopback0
ip address 10.255.252.202 255.255.255.255
L
interface Tunnel10
ip address 10.4.34.202 255.255.254.0
ip wccp 62 redirect in
interface GigabitEthernet0/0
ip address 192.168.4.5 255.255.255.252
ip wccp 62 redirect in
1
interface GigabitEthernet0/2
no ip address
!
interface GigabitEthernet0/2.64
 encapsulation dot1Q 64
ip address 10.5.68.1 255.255.255.0
ip wccp 61 redirect in
L
ip access-list standard WAVE
permit 10.5.68.8
1
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
       tcp any any eq 161
 deny
       tcp any eq 161 any
 deny
 deny
        tcp any any eq 162
```

tcp any eq 162 any deny deny tcp any any eq 2000 tcp any eq 2000 any deny deny tcp any any eq 2443 tcp any eq 2443 any deny tcp any any eq 5060 deny tcp any eq 5060 any deny tcp any any eq 5061 deny deny tcp any eq 5061 any deny tcp any any eq 1718 tcp any eq 1718 any deny tcp any any eq 1720 deny tcp any eq 1720 any deny tcp any any eq 2428 deny tcp any eq 2428 any deny tcp any any eq 443 deny deny tcp any eq 443 any deny tcp any any eq 8443 tcp any eq 8443 any deny tcp any any eq 6970 deny deny tcp any eq 6970 any tcp any any eq 689 deny deny tcp any eq 689 any permit tcp any any

RS213 WAAS Node (vWAAS)

```
! waas-universal-k9 version 5.2.1 (build b34 Apr 25 2013)
!
device mode application-accelerator
!
interception-method wccp
!
!
hostname RS213-vWAAS
1
clock timezone PST8PDT -8 0
!
!
ip domain-name cisco.local
!
!
primary-interface Virtual 1/0
1
interface Virtual 1/0
ip address 10.5.180.8 255.255.255.0
exit
interface Virtual 2/0
```

```
shutdown
exit
!
ip default-gateway 10.5.180.1
!
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
T.
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
!
!
ntp server 10.4.48.17
!
!
wccp router-list 7 10.255.255.213
wccp tcp-promiscuous service-pair 61 62
router-list-num 7
password ****
redirect-method gre
egress-method wccp-gre
enable
exit
!
!
!
1
username admin password 1 ****
username admin privilege 15
!
snmp-server community cisco
snmp-server community cisco123 rw
!
!
!
tacacs key ****
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
Ţ.
!
no telnet enable
1
sshd enable
1
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
1
!
accelerator mapi wansecure-mode auto
1
!
central-manager address 10.4.48.100
cms enable
!
1
1
stats-collector logging enable
stats-collector logging rate 30
!
!
! End of WAAS configuration
```

RS213 WAN Router (UCS E-Series)

```
version 15.2
!
hostname RS213-2911
1
ip wccp source-interface Loopback0
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
!
interface Loopback0
ip address 10.255.255.213 255.255.255
T
interface Tunnel10
ip address 10.4.34.213 255.255.254.0
ip wccp 62 redirect in
1
interface GigabitEthernet0/0
```

```
no ip address
I.
interface GigabitEthernet0/0.39
encapsulation dot1Q 39
ip address 10.4.39.213 255.255.255.0
ip wccp 62 redirect in
!
interface GigabitEthernet0/2
no ip address
!
interface GigabitEthernet0/2.64
encapsulation dot1Q 64
ip address 10.5.180.1 255.255.255.0
ip wccp 61 redirect in
1
interface ucse1/0
ip unnumbered GigabitEthernet0/2.64
imc ip address 10.5.180.10 255.255.255.0 default-gateway 10.5.180.1
imc access-port shared-lom console
1
ip route 10.5.180.10 255.255.255.255 ucse1/0
ip route 10.5.180.11 255.255.255.255 ucsel/0
1
ip access-list standard WAVE
permit 10.5.180.8
Ţ.
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
deny
       tcp any any eq telnet
       tcp any eq telnet any
 deny
       tcp any any eq 22
 deny
       tcp any eq 22 any
 deny
 deny
       tcp any any eq 161
       tcp any eq 161 any
 deny
       tcp any any eq 162
 deny
       tcp any eq 162 any
 deny
       tcp any any eq 123
 deny
       tcp any eq 123 any
 deny
       tcp any any eq bgp
 deny
 deny
       tcp any eq bgp any
 deny
       tcp any any eq tacacs
       tcp any eq tacacs any
 deny
 deny
       tcp any any eq 2000
       tcp any eq 2000 any
 deny
       tcp any any eq 2443
 deny
       tcp any eq 2443 any
 deny
 deny
       tcp any any eq 5060
```

```
deny
      tcp any eq 5060 any
deny
      tcp any any eq 5061
     tcp any eq 5016 any
deny
deny
      tcp any any eq 1718
      tcp any eq 1718 any
deny
     tcp any any eq 1720
deny
     tcp any eq 1720 any
deny
     tcp any any eq 2428
deny
deny tcp any eq 2428 any
deny
     tcp any any eq 443
     tcp any eq 443 any
deny
     tcp any any eq 8443
deny
     tcp any eq 8443 any
deny
     tcp any any eq 6970
deny
deny tcp any eq 6970 any
     tcp any any eq 689
deny
deny tcp any eq 689 any
permit tcp any any
```

RS201 WAAS Node (SRE)

```
! waas-universal-k9 version 5.3.1 (build b20 Aug 4 2013)
!
device mode application-accelerator
!
interception-method wccp
!
T.
hostname RS201-2911-SRE
1
clock timezone PST8PDT -8 0
Ţ.
!
ip domain-name cisco.local
!
1
primary-interface GigabitEthernet 2/0
!
interface GigabitEthernet 1/0
shutdown
exit
interface GigabitEthernet 2/0
ip address 10.5.44.8 255.255.255.0
ip access-group 155 in
exit
!
ip default-gateway 10.5.44.1
!
```

```
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
1
ip name-server 10.4.48.10
1
1
ip access-list standard 55
permit 10.4.48.0 0.0.0.255
exit
!
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
1
!
ntp server 10.4.48.17
1
!
wccp router-list 7 10.255.251.201
wccp tcp-promiscuous service-pair 61 62
router-list-num 7
password ****
redirect-method gre
egress-method wccp-gre
enable
exit
!
!
username admin password 1 ****
username admin privilege 15
1
snmp-server community cisco123 rw
snmp-server community cisco
snmp-server access-list 55
!
!
tacacs key ****
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
Ţ.
!
no telnet enable
1
sshd enable
!
!
tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048
!
!
accelerator mapi wansecure-mode auto
1
!
central-manager address 10.4.48.100
cms enable
!
1
stats-collector logging enable
stats-collector logging rate 30
1
1
! End of WAAS configuration
```

RS201 WAN Router (SRE)

```
version 15.2
1
hostname RS201-2911
1
aaa authentication login MODULE none
!
ip wccp source-interface Loopback0
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 clsco123
!
interface Loopback0
ip address 10.255.251.201 255.255.255
!
interface Tunnel10
ip address 10.4.34.201 255.255.254.0
ip wccp 62 redirect in
1
interface Port-channel1
no ip address
!
```

```
interface Port-channel1.64
encapsulation dot10 64
ip address 10.5.44.1 255.255.255.0
ip wccp 61 redirect in
L
interface GigabitEthernet0/0
ip address 192.168.3.21 255.255.255.252
ip wccp 62 redirect in
Т
interface SM1/0
ip address 192.0.2.2 255.255.255.252
service-module external ip address 10.5.44.8 255.255.255.0
service-module ip default-gateway 10.5.44.1
!
ip access-list standard WAVE
permit 10.5.44.8
!
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
deny
       tcp any any eq telnet
deny
       tcp any eq telnet any
       tcp any any eq 22
 denv
       tcp any eq 22 any
 deny
       tcp any any eq 161
 deny
 deny
       tcp any eq 161 any
       tcp any any eq 162
 deny
       tcp any eq 162 any
 deny
       tcp any any eq 123
 deny
 deny
       tcp any eq 123 any
        tcp any any eq bgp
 deny
       tcp any eq bgp any
 deny
       tcp any any eq tacacs
 deny
 deny
       tcp any eq tacacs any
       tcp any any eq 2000
 deny
       tcp any eq 2000 any
 deny
       tcp any any eq 2443
 deny
       tcp any eq 2443 any
 deny
        tcp any any eq 5060
 deny
        tcp any eq 5060 any
 deny
 deny
       tcp any any eq 5061
       tcp any eq 5016 any
 deny
        tcp any any eq 1718
 deny
       tcp any eq 1718 any
 deny
        tcp any any eq 1720
 deny
        tcp any eq 1720 any
 deny
        tcp any any eq 2428
 deny
 deny
        tcp any eq 2428 any
```

```
deny
      tcp any any eq 443
 deny
      tcp any eq 443 any
deny tcp any any eq 8443
 deny tcp any eq 8443 any
deny tcp any any eq 6970
deny tcp any eq 6970 any
deny tcp any any eq 689
deny tcp any eq 689 any
permit tcp any any
!
access-list 67 permit 192.0.2.2
!
line 67
 access-class 67 in
login authentication MODULE
```

RS204 WAASx WAN Router

```
version 15.2
1
hostname RS204-1941
!
parameter-map type waas waas global
tfo optimize full
 tfo auto-discovery blacklist enable
 lz entropy-check
 dre upload
 accelerator http-express
 no enable
 accelerator cifs-express
  no enable
 accelerator ssl-express
  enable
!
class-map type waas match-any BFTP
match tcp destination port 152
class-map type waas match-any proshare
match tcp destination port 5713 5717
class-map type waas match-any msnp
match tcp destination port 1863
match tcp destination port 6891 6900
class-map type waas match-any Laplink-surfup-HTTPS
 match tcp destination port 1184
class-map type waas match-any msmq
match tcp destination port 1801
match tcp destination port 2101
 match tcp destination port 2103
 match tcp destination port 2105
```

class-map type waas match-any rrac match tcp destination port 5678 class-map type waas match-any nameserver match tcp destination port 42 class-map type waas match-any ms-sql-s match tcp destination port 1433 class-map type waas match-any WINS match tcp destination port 1512 class-map type waas match-any NNTP match tcp destination port 119 class-map type waas match-any PPTP match tcp destination port 1723 class-map type waas match-any hp-pdl-datastr match tcp destination port 9100 class-map type waas match-any RTSP match tcp destination port 554 match tcp destination port 8554 class-map type waas match-any VocalTec match tcp destination port 1490 match tcp destination port 6670 match tcp destination port 25793 match tcp destination port 22555 class-map type waas match-any PostgreSQL match tcp destination port 5432 class-map type waas match-any Danware-NetOp match tcp destination port 6502 class-map type waas match-any TACACS match tcp destination port 49 class-map type waas match-any isns match tcp destination port 3205 class-map type waas match-any klogin match tcp destination port 543 class-map type waas match-any auth match tcp destination port 113 class-map type waas match-any Cisco-CallManager match tcp destination port 2748 match tcp destination port 2443 class-map type waas match-any sunrpc match tcp destination port 111 class-map type waas match-any ccmail match tcp destination port 3264 class-map type waas match-any netrjs-3 match tcp destination port 73 class-map type waas match-any orasrv match tcp destination port 1525 match tcp destination port 1521 class-map type waas match-any ircs

match tcp destination port 994 class-map type waas match-any PDMWorks match tcp destination port 30000 match tcp destination port 40000 class-map type waas match-any eTrust-policy-Compliance match tcp destination port 1267 class-map type waas match-any ircu match tcp destination port 531 match tcp destination port 6660 6665 match tcp destination port 6667 6669 class-map type waas match-any timbuktu match tcp destination port 407 class-map type waas match-any sshell match tcp destination port 614 class-map type waas match-any corba-iiop-ssl match tcp destination port 684 class-map type waas match-any sametime match tcp destination port 1533 class-map type waas match-any Laplink-ShareDirect match tcp destination port 2705 class-map type waas match-any EMC-SRDFA-IP match tcp destination port 1748 class-map type waas match-any FTPS match tcp source port 989 class-map type waas match-any ftps match tcp destination port 990 class-map type waas match-any novadigm match tcp destination port 3460 match tcp destination port 3461 match tcp destination port 3464 class-map type waas match-any tell match tcp destination port 754 class-map type waas match-any sftp match tcp destination port 115 class-map type waas match-any talk match tcp destination port 517 class-map type waas match-any Veritas-NetBackup match tcp destination port 13720 match tcp destination port 13721 match tcp destination port 13782 match tcp destination port 13785 class-map type waas match-any Basic-TCP-services match tcp destination port 1 19 class-map type waas match-any cvspserver match tcp destination port 2401 class-map type waas match-any imap match tcp destination port 143


class-map type waas match-any kshell match tcp destination port 544 class-map type waas match-any ms-olap4 match tcp destination port 2383 class-map type waas match-any TFTP match tcp destination port 69 class-map type waas match-any svrloc match tcp destination port 427 class-map type waas match-any HTTP match tcp destination port 80 match tcp destination port 8080 match tcp destination port 8000 match tcp destination port 8088 match tcp destination port 3128 class-map type waas match-any pcanywheredata match tcp destination port 5631 5632 match tcp destination port 65301 class-map type waas match-any QMTP match tcp destination port 209 class-map type waas match-any LDAP match tcp destination port 389 match tcp destination port 8404 class-map type waas match-any sqlsrv match tcp destination port 156 class-map type waas match-any smtp match tcp destination port 25 class-map type waas match-any BitTorrent match tcp destination port 6881 6889 match tcp destination port 6969 class-map type waas match-any exec match tcp destination port 512 class-map type waas match-any FCIP match tcp destination port 3225 class-map type waas match-any UniSQL match tcp destination port 1978 match tcp destination port 1979 class-map type waas match-any openmail match tcp destination port 5755 match tcp destination port 5757 match tcp destination port 5766 match tcp destination port 5767 match tcp destination port 5768 match tcp destination port 5729 class-map type waas match-any ssgl match tcp destination port 3352 class-map type waas match-any SoulSeek match tcp destination port 2234

match tcp destination port 5534 class-map type waas match-any WBEM match tcp destination port 5987 5990 class-map type waas match-any ms-sql-m match tcp destination port 1434 class-map type waas match-any afpovertcp match tcp destination port 548 class-map type waas match-any CIFS match tcp destination port 139 match tcp destination port 445 class-map type waas match-any IBM-TSM match tcp destination port 1500 1502 class-map type waas match-any xmpp-client match tcp destination port 5222 class-map type waas match-any pcsync-http match tcp destination port 8444 class-map type waas match-any xprint-server match tcp destination port 8100 class-map type waas match-any Telnet match tcp destination port 23 match tcp destination port 107 class-map type waas match-any Remote-Anything match tcp destination port 3999 4000 class-map type waas match-any Double-Take match tcp destination port 1105 match tcp destination port 1100 class-map type waas match-any cisco-q931-backhaul match tcp destination port 2428 class-map type waas match-any msft-gc match tcp destination port 3268 class-map type waas match-any net-assistant match tcp destination port 3283 class-map type waas match-any imap3 match tcp destination port 220 class-map type waas match-any ms-content-repl-srv match tcp destination port 560 match tcp destination port 507 class-map type waas match-any netapp-snapmirror match tcp destination port 10565 10569 class-map type waas match-any Amanda match tcp destination port 10080 class-map type waas match-any gds db match tcp destination port 3050 class-map type waas match-any radmin-port match tcp destination port 4899 class-map type waas match-any PSOM-MTLS match tcp destination port 8057

class-map type waas match-any sybase-sqlany match tcp destination port 1498 match tcp destination port 2638 match tcp destination port 2439 match tcp destination port 3968 class-map type waas match-any print-srv match tcp destination port 170 class-map type waas match-any EMC-Celerra-Replicator match tcp destination port 8888 class-map type waas match-any ftps-data match tcp source port 20 class-map type waas match-any Gnutella match tcp destination port 6346 6349 match tcp destination port 6355 match tcp destination port 5634 class-map type waas match-any HP-OpenView match tcp destination port 7426 7431 match tcp destination port 7501 match tcp destination port 7510 class-map type waas match-any sip-tls match tcp destination port 5061 class-map type waas match-any Yahoo-Messenger match tcp destination port 5000 5001 match tcp destination port 5050 match tcp destination port 5100 class-map type waas match-any pop3s match tcp destination port 995 class-map type waas match-any Apple-iChat match tcp destination port 5297 match tcp destination port 5298 class-map type waas match-any Siebel match tcp destination port 8448 match tcp destination port 2320 match tcp destination port 2321 class-map type waas match-any Kerberos match tcp destination port 88 match tcp destination port 888 match tcp destination port 2053 class-map type waas match-any MS-GROOVE match tcp destination port 2492 class-map type waas match-any MS-NetMeeting match tcp destination port 522 match tcp destination port 1503 match tcp destination port 1731 class-map type waas match-any Oracle match tcp destination port 66 class-map type waas match-any ssc-agent

match tcp destination port 2847 match tcp destination port 2848 match tcp destination port 2967 match tcp destination port 2968 match tcp destination port 38037 match tcp destination port 38292 class-map type waas match-any soap-http match tcp destination port 7627 class-map type waas match-any Pervasive-SQL match tcp destination port 1583 class-map type waas match-any iFCP match tcp destination port 3420 class-map type waas match-any sql-net match tcp destination port 150 class-map type waas match-any xmpp-server match tcp destination port 5269 class-map type waas match-any pcmail-srv match tcp destination port 158 class-map type waas match-any AOL match tcp destination port 5190 5193 class-map type waas match-any SAP match tcp destination port 3200 3204 match tcp destination port 3206 3219 match tcp destination port 3390 3399 match tcp destination port 3284 3305 match tcp destination port 3226 3259 match tcp destination port 3261 3263 match tcp destination port 3265 3267 match tcp destination port 3662 3699 match tcp destination port 3221 3224 match tcp destination port 3270 3282 match tcp destination port 3307 3351 match tcp destination port 3353 3388 match tcp destination port 3600 3658 class-map type waas match-any waas-default match tcp any class-map type waas match-any TFTPS match tcp destination port 3713 class-map type waas match-any WinMX match tcp destination port 6699 class-map type waas match-any ezMeeting match tcp destination port 10101 10103 match tcp destination port 26260 26261 class-map type waas match-any afs3 match tcp destination port 7000 7009 class-map type waas match-any NetIQ match tcp destination port 2220

match tcp destination port 2735 match tcp destination port 10113 10116 class-map type waas match-any Grouper match tcp destination port 8038 class-map type waas match-any apple-sasl match tcp destination port 3659 class-map type waas match-any SSH match tcp destination port 22 class-map type waas match-any h323hostcallsc match tcp destination port 1300 class-map type waas match-any IPP match tcp destination port 631 class-map type waas match-any NTP match tcp destination port 123 class-map type waas match-any VoIP-Control match tcp destination port 1718 1719 match tcp destination port 11000 11999 class-map type waas match-any HTTPS match tcp destination port 443 class-map type waas match-any mgcp-gateway match tcp destination port 2427 class-map type waas match-any Clearcase match tcp destination port 371 class-map type waas match-any novell-zen match tcp destination port 1761 1763 match tcp destination port 2544 match tcp destination port 8039 match tcp destination port 2037 class-map type waas match-any iso-tsap match tcp destination port 102 class-map type waas match-any ms-streaming match tcp destination port 1755 class-map type waas match-any Napster match tcp destination port 8875 match tcp destination port 7777 match tcp destination port 6700 match tcp destination port 6666 match tcp destination port 6677 match tcp destination port 6688 class-map type waas match-any mgcp-callagent match tcp destination port 2727 class-map type waas match-any Kazaa match tcp destination port 1214 class-map type waas match-any kerberos-adm match tcp destination port 749 class-map type waas match-any Telnets match tcp destination port 992

class-map type waas match-any pcsync-https match tcp destination port 8443 class-map type waas match-any WASTE match tcp destination port 1337 class-map type waas match-any BGP match tcp destination port 179 class-map type waas match-any BMC-Patrol match tcp destination port 6161 match tcp destination port 6162 match tcp destination port 8160 match tcp destination port 8161 match tcp destination port 6767 match tcp destination port 6768 match tcp destination port 10128 class-map type waas match-any Rsync match tcp destination port 873 class-map type waas match-any Qnext match tcp destination port 44 match tcp destination port 5555 class-map type waas match-any Liquid-Audio match tcp destination port 18888 class-map type waas match-any timbuktu-srv match tcp destination port 1417 1420 class-map type waas match-any eDonkey match tcp destination port 4661 4662 class-map type waas match-any h323hostcall match tcp destination port 1720 class-map type waas match-any DNS match tcp destination port 53 class-map type waas match-any Filenet match tcp destination port 32768 32774 class-map type waas match-any backup-express match tcp destination port 6123 class-map type waas match-any ControlIT match tcp destination port 799 class-map type waas match-any NFS match tcp destination port 2049 class-map type waas match-any Netopia-netOctopus match tcp destination port 1917 match tcp destination port 1921 class-map type waas match-any VNC match tcp destination port 5800 5809 match tcp destination port 5900 5909 class-map type waas match-any Vmware-VMConsole match tcp destination port 902 class-map type waas match-any cisco-sccp match tcp destination port 2000 2002

class-map type waas match-any intersys-cache match tcp destination port 1972 class-map type waas match-any pop3 match tcp destination port 110 class-map type waas match-any Other-Secure match tcp destination port 261 match tcp destination port 448 match tcp destination port 695 match tcp destination port 2252 match tcp destination port 2478 match tcp destination port 2479 match tcp destination port 2482 match tcp destination port 2484 match tcp destination port 2679 match tcp destination port 2762 match tcp destination port 2998 match tcp destination port 3077 match tcp destination port 3078 match tcp destination port 3183 match tcp destination port 3191 match tcp destination port 3220 match tcp destination port 3410 match tcp destination port 3424 match tcp destination port 3471 match tcp destination port 3496 match tcp destination port 3509 match tcp destination port 3529 match tcp destination port 3539 match tcp destination port 3660 match tcp destination port 3661 match tcp destination port 3747 match tcp destination port 3864 match tcp destination port 3885 match tcp destination port 3896 match tcp destination port 3897 match tcp destination port 3995 match tcp destination port 4031 match tcp destination port 5007 match tcp destination port 7674 match tcp destination port 9802 match tcp destination port 12109 class-map type waas match-any IBM-DB2 match tcp destination port 523 class-map type waas match-any citriximaclient match tcp destination port 2598 class-map type waas match-any Legato-RepliStor match tcp destination port 7144

match tcp destination port 7145 class-map type waas match-any lotusnote match tcp destination port 1352 class-map type waas match-any MDaemon match tcp destination port 3000 match tcp destination port 3001 class-map type waas match-any dmdocbroker match tcp destination port 1489 class-map type waas match-any ftp match tcp destination port 21 class-map type waas match-any Altiris-CarbonCopy match tcp destination port 1680 class-map type waas match-any login match tcp destination port 513 class-map type waas match-any iscsi match tcp destination port 3260 class-map type waas match-any msft-gc-ssl match tcp destination port 3269 class-map type waas match-any objcall match tcp destination port 94 match tcp destination port 627 match tcp destination port 1965 match tcp destination port 1580 match tcp destination port 1581 class-map type waas match-any imaps match tcp destination port 993 class-map type waas match-any printer match tcp destination port 515 class-map type waas match-any netbios match tcp destination port 137 class-map type waas match-any smtps match tcp destination port 465 class-map type waas match-any kpasswd match tcp destination port 464 class-map type waas match-any epmap match tcp destination port 135 class-map type waas match-any ldaps match tcp destination port 636 class-map type waas match-any cmd match tcp destination port 514 class-map type waas match-any sip match tcp destination port 5060 class-map type waas match-any ica match tcp destination port 1494 class-map type waas match-any cuseeme match tcp destination port 7640 match tcp destination port 7642

match tcp destination port 7648 match tcp destination port 7649 class-map type waas match-any Legato-NetWorker match tcp destination port 7937 match tcp destination port 7938 match tcp destination port 7939 class-map type waas match-any citrixadmin match tcp destination port 2513 class-map type waas match-any sqlexec match tcp destination port 9088 9089 class-map type waas match-any CommVault match tcp destination port 8400 8403 class-map type waas match-any Veritas-BackupExec match tcp destination port 6101 match tcp destination port 6102 match tcp destination port 6106 match tcp destination port 3527 match tcp destination port 1125 class-map type waas match-any nntps match tcp destination port 563 class-map type waas match-any groupwise match tcp destination port 1677 match tcp destination port 9850 match tcp destination port 7205 match tcp destination port 3800 match tcp destination port 7100 match tcp destination port 7180 match tcp destination port 7101 match tcp destination port 7181 match tcp destination port 2800 class-map type waas match-any x11 match tcp destination port 6000 6063 class-map type waas match-any citrixima match tcp destination port 2512 class-map type waas match-any L2TP match tcp destination port 1701 class-map type waas match-any LANDesk match tcp destination port 9535 match tcp destination port 9593 9595 class-map type waas match-any ms-wbt-server match tcp destination port 3389 class-map type waas match-any MySQL match tcp destination port 3306 class-map type waas match-any netviewdm match tcp destination port 729 731 class-map type waas match-any OpenVPN match tcp destination port 1194

```
class-map type waas match-any sqlserv
match tcp destination port 118
class-map type waas match-any HotLine
match tcp destination port 5500 5503
class-map type waas match-any laplink
match tcp destination port 1547
class-map type waas match-any ncp
match tcp destination port 524
class-map type waas match-any flowmonitor
match tcp destination port 7878
class-map type waas match-any connected
match tcp destination port 16384
1
L
policy-map type waas waas global
class afs3
 optimize tfo dre lz application File-System
class AOL
 passthrough application Instant-Messaging
 class Altiris-CarbonCopy
 passthrough application Remote-Desktop
class Amanda
 optimize tfo application Backup
 class hp-pdl-datastr
 optimize tfo dre lz application Printing
class afpovertcp
 optimize tfo dre lz application File-System
 class net-assistant
 passthrough application Remote-Desktop
class Apple-iChat
 passthrough application Instant-Messaging
class BFTP
 optimize tfo dre lz application File-Transfer
class BGP
 passthrough application Other
 class BMC-Patrol
 passthrough application Systems-Management
class backup-express
 optimize tfo application Backup
class Basic-TCP-services
 passthrough application Other
 class BitTorrent
 passthrough application P2P
 class gds db
 optimize tfo dre lz application SQL
class CIFS
  optimize tfo dre lz application CIFS accelerate cifs-express
```

class cuseeme passthrough application Conferencing class cvspserver optimize tfo dre lz application Version-Management class Cisco-CallManager passthrough application Call-Management class ica optimize tfo dre lz application Remote-Desktop class citriximaclient optimize tfo dre 1z application Remote-Desktop class Clearcase optimize tfo dre lz application Version-Management class CommVault optimize tfo application Backup class connected optimize tfo application Backup class ControlIT optimize tfo application Remote-Desktop class DNS passthrough application Name-Services class Danware-NetOp optimize tfo application Remote-Desktop class dmdocbroker optimize tfo dre lz application Content-Management class Double-Take optimize tfo dre lz application Replication class EMC-Celerra-Replicator optimize tfo dre lz application Replication class EMC-SRDFA-IP optimize tfo dre lz application Storage class FCIP optimize tfo lz application Storage class ftp passthrough application File-Transfer class ftps-data optimize tfo dre lz application File-Transfer class FTPS passthrough application File-Transfer class ftps optimize tfo application File-Transfer class Filenet optimize tfo dre lz application Content-Management class Gnutella passthrough application P2P class Grouper passthrough application P2P class openmail

optimize tfo dre lz application Email-and-Messaging class HP-OpenView passthrough application Systems-Management class novadigm optimize tfo dre lz application Systems-Management class HTTP optimize tfo dre lz application Web accelerate http-express class HTTPS optimize tfo application SSL class HotLine passthrough application P2P class IBM-DB2 optimize tfo dre lz application SQL class netviewdm passthrough application Systems-Management class IBM-TSM optimize tfo dre lz application Backup class objcall optimize tfo dre lz application Systems-Management class IPP optimize tfo dre lz application Printing class proshare passthrough application Conferencing class intersys-cache optimize tfo dre lz application SQL class imap optimize tfo dre lz application Email-and-Messaging class imap3 optimize tfo dre lz application Email-and-Messaging class pop3 optimize tfo dre lz application Email-and-Messaging class smtp optimize tfo dre lz application Email-and-Messaging class imaps optimize tfo application Email-and-Messaging class pop3s optimize tfo application Email-and-Messaging class smtps optimize tfo application Email-and-Messaging class xmpp-client passthrough application Instant-Messaging class xmpp-server passthrough application Instant-Messaging class Kazaa passthrough application P2P class Kerberos passthrough application Authentication

class kerberos-adm passthrough application Authentication class klogin passthrough application Authentication class kshell passthrough application Authentication class tell passthrough application Authentication class kpasswd passthrough application Authentication class L2TP optimize tfo application VPN class LANDesk optimize tfo dre lz application Systems-Management class LDAP optimize tfo dre lz application Directory-Services class msft-gc optimize tfo dre lz application Directory-Services class msft-qc-ssl passthrough application Directory-Services class ldaps passthrough application Directory-Services class laplink optimize tfo dre lz application Remote-Desktop class pcsync-http optimize tfo dre lz application Replication class pcsync-https optimize tfo application Replication class Laplink-ShareDirect passthrough application P2P class Laplink-surfup-HTTPS optimize tfo application Remote-Desktop class Legato-NetWorker optimize tfo application Backup class Legato-RepliStor optimize tfo application Backup class Liquid-Audio optimize tfo dre lz application Streaming class lotusnote optimize tfo dre 1z application Email-and-Messaging class sametime passthrough application Instant-Messaging class MDaemon optimize tfo dre lz application Email-and-Messaging class ms-content-repl-srv optimize tfo application Replication class epmap

optimize tfo application Other class MS-GROOVE optimize tfo application Enterprise-Applications class msmq optimize tfo dre lz application Other class MS-NetMeeting passthrough application Conferencing class ms-streaming optimize tfo dre lz application Streaming class msnp passthrough application Instant-Messaging class ms-olap4 optimize tfo application SQL class ms-sql-s optimize tfo dre lz application SQL class ms-wbt-server optimize tfo application Remote-Desktop class MySQL optimize tfo dre lz application SQL class NFS optimize tfo dre 1z application File-System class NNTP optimize tfo dre lz application Email-and-Messaging class nntps optimize tfo application Email-and-Messaging class NTP passthrough application Other class Napster passthrough application P2P class netapp-snapmirror optimize tfo dre lz application Replication class NetIQ passthrough application Systems-Management class timbuktu optimize tfo application Remote-Desktop class timbuktu-srv optimize tfo application Remote-Desktop class Netopia-netOctopus passthrough application Systems-Management class groupwise optimize tfo dre lz application Email-and-Messaging class ncp optimize tfo dre 1z application File-System class novell-zen optimize tfo dre lz application Systems-Management class talk passthrough application Instant-Messaging

class OpenVPN optimize tfo application VPN class Oracle optimize tfo dre lz application SQL class orasrv optimize tfo dre lz application SQL class Other-Secure passthrough application Other class corba-iiop-ssl passthrough application Other class ircs passthrough application Other class netrjs-3 optimize tfo application Remote-Desktop class pcanywheredata optimize tfo application Remote-Desktop class pcmail-srv optimize tfo dre lz application Email-and-Messaging class PDMWorks optimize tfo dre lz application CAD class PPTP optimize tfo application VPN class PSOM-MTLS passthrough application Conferencing class Pervasive-SQL optimize tfo dre lz application SQL class PostgreSQL optimize tfo dre lz application SQL class QMTP optimize tfo dre lz application Email-and-Messaging class Qnext passthrough application P2P class radmin-port optimize tfo application Remote-Desktop class RTSP optimize tfo dre lz application Streaming class Remote-Anything optimize tfo application Remote-Desktop class rrac optimize tfo application Replication class Rsync optimize tfo dre lz application Replication class apple-sasl passthrough application Authentication class sip-tls passthrough application Call-Management class soap-http

optimize tfo dre lz application Web class sqlsrv optimize tfo dre lz application SQL class SSH optimize tfo application SSH class sshell passthrough application Console class xprint-server optimize tfo dre lz application Printing class ssql optimize tfo dre lz application SQL class svrloc passthrough application Name-Services class Siebel optimize tfo dre lz application Enterprise-Applications class sftp optimize tfo dre lz application File-Transfer class SoulSeek passthrough application P2P class sunrpc passthrough application File-System class sybase-sqlany optimize tfo dre lz application SQL class ssc-agent optimize tfo dre lz application Other class TACACS passthrough application Authentication class TFTP optimize tfo dre lz application File-Transfer class TFTPS optimize tfo application File-Transfer class Telnet passthrough application Console class login passthrough application Console class Telnets passthrough application Console class UniSQL optimize tfo dre lz application SQL class printer optimize tfo dre lz application Printing class print-srv optimize tfo dre lz application Printing class cmd passthrough application Console class exec passthrough application Console

```
class Veritas-BackupExec
optimize tfo application Backup
class Veritas-NetBackup
optimize tfo application Backup
class Vmware-VMConsole
 optimize tfo application Remote-Desktop
class VoIP-Control
passthrough application Call-Management
class cisco-q931-backhaul
passthrough application Call-Management
class cisco-sccp
passthrough application Call-Management
class h323hostcall
passthrough application Call-Management
class h323hostcallsc
passthrough application Call-Management
class sip
passthrough application Call-Management
class VocalTec
passthrough application Conferencing
class flowmonitor
 optimize tfo lz application Systems-Management
class WASTE
passthrough application P2P
class WBEM
passthrough application Systems-Management
class WINS
passthrough application Name-Services
class nameserver
passthrough application Name-Services
class netbios
passthrough application Name-Services
class WinMX
passthrough application P2P
class iso-tsap
optimize tfo dre lz application Email-and-Messaging
class x11
 optimize tfo application Remote-Desktop
class Yahoo-Messenger
passthrough application Instant-Messaging
class eDonkey
passthrough application P2P
class eTrust-policy-Compliance
optimize tfo application Systems-Management
class ezMeeting
passthrough application Conferencing
class iFCP
```

optimize tfo dre lz application Storage class iscsi optimize tfo dre lz application Storage class isns passthrough application Name-Services class ircu passthrough application Instant-Messaging class SAP optimize tfo dre lz application Enterprise-Applications class VNC optimize tfo application Remote-Desktop class auth passthrough application Authentication class citrixadmin optimize tfo dre lz application Remote-Desktop class citrixima optimize tfo dre lz application Remote-Desktop class mgcp-callagent passthrough application Call-Management class mgcp-gateway passthrough application Call-Management class ms-sql-m optimize tfo dre lz application SQL class sqlexec optimize tfo dre lz application SQL class sql-net optimize tfo dre lz application SQL class sqlserv optimize tfo dre lz application SQL class ccmail optimize tfo dre lz application Email-and-Messaging class waas-default optimize tfo dre lz application waas-default ! interface Loopback0 ip address 10.255.251.204 255.255.255.255 I. interface GigabitEthernet0/0 ip address 192.168.3.29 255.255.255.252 waas enable Ţ. ip http authentication aaa ip http secure-server

Feedback

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

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

B-0000125-1 12/13