



IWAN Application Optimization Using Cisco WAAS and Akamai Connect

Technology Design Guide (IOS XE)

March 2015



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency.....	2
Introduction	3
Technology Use Cases	3
Use Case: Optimization of Traffic Traversing the WAN	3
Design Overview.....	4
Cisco WAAS Central Manager.....	4
WAAS Nodes	4
AppNav	5
ISR-WAAS.....	8
WAN Aggregation Design Models	8
ISR-WAAS Remote-Site Design Models.....	9
Deployment Details	11
Configuring the Cisco WAAS Central Manager	12
Configuring AppNav-XE on a WAN-Aggregation Router.....	19
Deploying ISR WAAS	27
Preparing to Deploy ISR-WAAS.....	28
Deploying ISR-WAAS at a Single-Router Remote Site.....	30
Changing Your Single-Router Remote Site to a Dual-Router Remote Site	35
Deploying ISR-WAAS at a Dual-Router Remote Site	37
Deploying Akamai Connect with Cisco WAAS.....	47
Appendix A: Product List	50
Appendix B: Caveats	54

Appendix C: Changes.....55

Appendix D: Configuration Examples56

 Central Manager 56

 WAAS Central Manager (vWAAS) 56

 Aggregation Router Configuration 58

 Remote-Site Router Configuration 68

Appendix E: Glossary82

Preface

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

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

CVD Foundation Series

This CVD Foundation guide is a part of the *January 2015 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

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:

- **Use Case: Optimization of Traffic Traversing the WAN**—Application optimization can boost network performance along with enhancing security and improving application delivery.

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

Scope

This guide covers the following areas of technology and products:

- Cisco WAAS
- Akamai Connect

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:

- CCNP Routing and Switching
- CCNP Security
- CCNP Wireless

Related CVD Guides



Intelligent WAN
Technology Design Guide



MPLS WAN Technology
Design Guide



VPN WAN Technology
Design Guide

To view the related CVD guides, click the titles or visit [the CVD Foundation web site](#).

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.

This design models in this guide are based on both single-router and dual-router remote sites as defined for use with the Cisco IWAN solution. A prerequisite for this guide is the [Cisco Intelligent WAN Technology Design Guide](#). All design and validation discussed in this document have been verified with that baseline.

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 local-area network (LAN) based business applications across comparatively slow wide-area networks (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 of the organization's application optimization devices

Design Overview

Cisco WAAS Central Manager

Every 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 and vWAAS sizing for Cisco WAAS Central Manager.

Table 1 - Cisco WAAS Central Manager sizing options

Device	Number of managed devices (Cisco WAAS only)
WAVE-294-4GB	250
WAVE-594-8GB	1000
WAVE-694-16GB	2000
vCM-100N	100
vCM-500	500
vCM-1000	1000
vCM-2000N	2000

WAAS Nodes

A Cisco WAAS node (WN) is a WAAS application accelerator (for instance, a Cisco WAVE appliance, Service Module-Services Ready Engine network module, or vWAAS instance, but not a WAAS Express device). A WN optimizes and accelerates traffic according to the optimization policies configured on the device. Table 2 provides details about 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 Cisco Application Navigator (AppNav) policies.



Reader Tip

Some Cisco product documentation may use different terminology. For consistency, this guide uses references to the most common terminology.

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]	Akamai Connect Cache Capacity [GB]
WAVE-594-8GB	750	50	250	172
WAVE-594-12GB	1300	100	300	152
WAVE-694-16GB	2500	200	450	194
WAVE-694-24GB	6000	200	500	176
WAVE-7541	18000	500	1000	N/A
WAVE-7571	60000	1000	2000	N/A
WAVE-8541	150000	2000	4000	N/A

Table 3 - WAN-aggregation for Cisco vWAAS

Device	Max. optimized TCP connections	Max. recommended WAN link [Mbps]	Max. optimized throughput [Mbps]	Akamai Connect Cache Capacity [GB]
vWAAS-200	200	20	100	100
vWAAS-750	750	50	250	250
vWAAS-1300	1300	80	300	300
vWAAS-2500	2500	150	400	350
vWAAS-6000	6000	200	400	400
vWAAS-12000	12000	310	500	N/A
vWAAS-50000	50000	700	1000	N/A

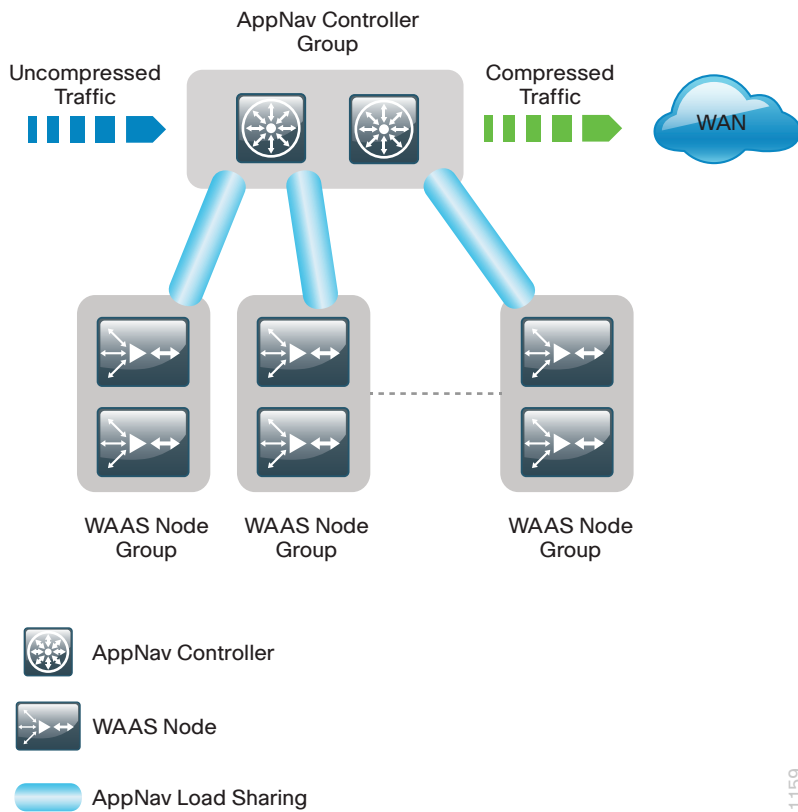
For comprehensive sizing and planning, work with your Cisco account team or Cisco partner.

AppNav

Cisco 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. AppNav 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 composed 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.

Figure 1 - WAAS AppNav components



1159

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.

 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)

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

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	–

i 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.

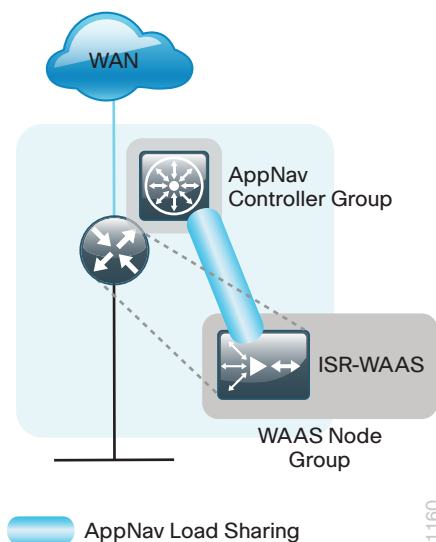
i Tech Tip

A Cisco AppNav-XE controller group must contain only members of the same router product family and model (example: only Cisco ASR 1002-X routers, or only Cisco ISR 4451-X routers). The ANCG may contain up to four AppNav-XE routers.

The AppNav IOM cannot be used within an AppNav-XE Controller group.

The combination of AppNav-XE and ISR-WAAS on the Cisco ISR 4K router delivers the entire application optimization solution on a single hardware platform using resources shared between the router and the vWAAS instance.

Figure 2 - AppNav-XE and ISR-WAAS on the Cisco ISR 4451-X router



ISR-WAAS

Although ISR-WAAS is supported on all the Cisco ISR-4K platforms, the Cisco ISR4451-X router was the first ISR router to run Cisco IOS-XE software and was the only platform validated with this guide. The multi-core CPU architecture of the Cisco ISR4451-X supports a built-in services-virtualization framework that enables on-demand deployment of services such as a vWAAS instance. ISR-WAAS is the specific implementation of vWAAS running in a Cisco IOS-XE software container on the Cisco ISR4451-X router. The term *container* refers to the kernel-based virtual machine hypervisor that runs virtualized applications on the Cisco ISR4451-X router.

In this virtualization framework, the router is the host machine and the virtual service is a guest OS. The virtual service shares CPU and memory resources with the host router but is allocated dedicated CPU cores to isolate itself from router data plane operations. Additionally, to deploy a virtual service, the router requires additional storage beyond the standard bootflash. The Cisco ISR4451-X router supports a network interface module carrier card that can hold one or two 200-GB solid-state drives (SSDs) in order to provide local storage for virtual services. The router requires the **universalk9** package license in order to run ISR-WAAS.

Table 5 - Cisco ISR-4451X requirements for ISR-WAAS

Profile	Max. optimized TCP connections	Router DRAM (GB)	Number of SSDs (200GB)	Compact flash (GB)
ISR-WAAS-750	750	8	1	16
ISR-WAAS-1300	1300	16	1	32
ISR-WAAS-2500	2500	16	2	32

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.

Table 6 - How to choose a WAN Aggregation design model

Requirement	AppNav-XE design model
AppNav IOM	Not needed
Mix of different router families	All routers in a controller group must be the same product model
Maximum number of ANCs in an ANCG	4
Intelligent load sharing	Full AppNav policies

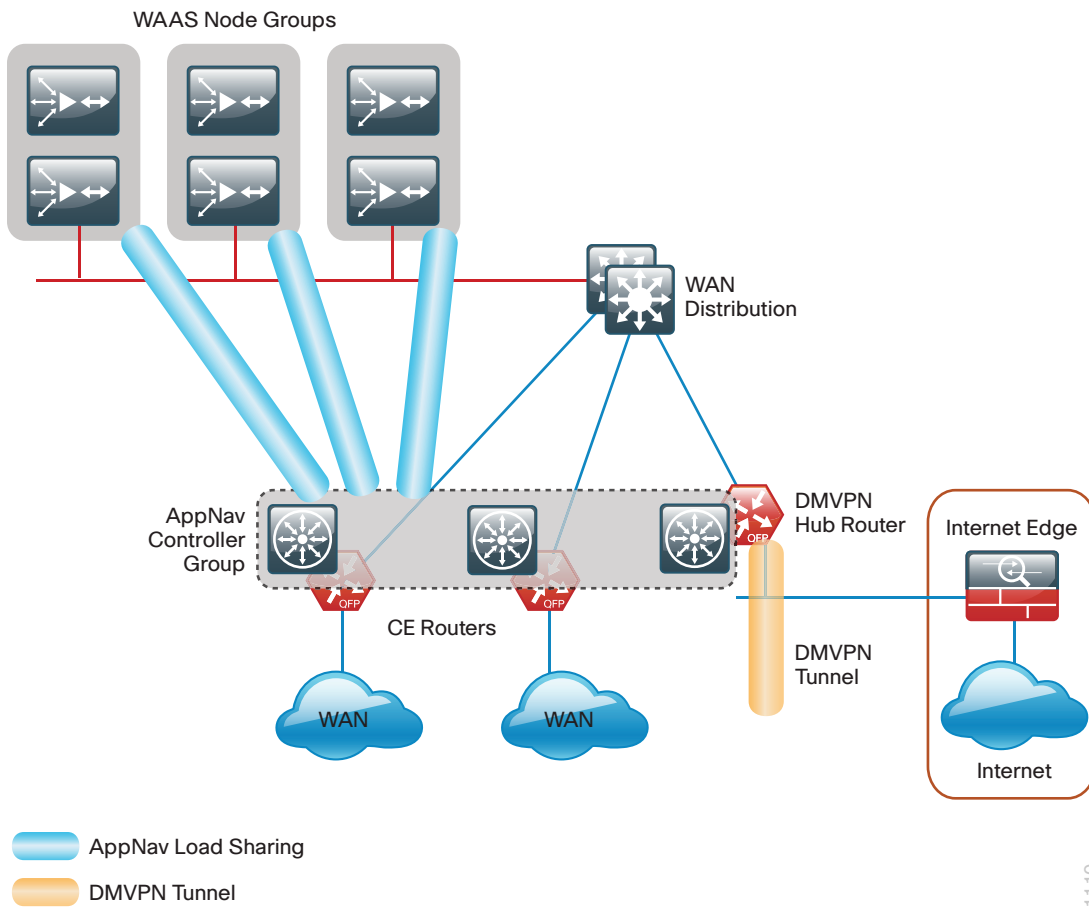
AppNav-XE

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 model. 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.

Cisco AppNav performs the intelligent load-sharing across the different Cisco WAAS node groups.

Figure 3 - AppNav-XE design model

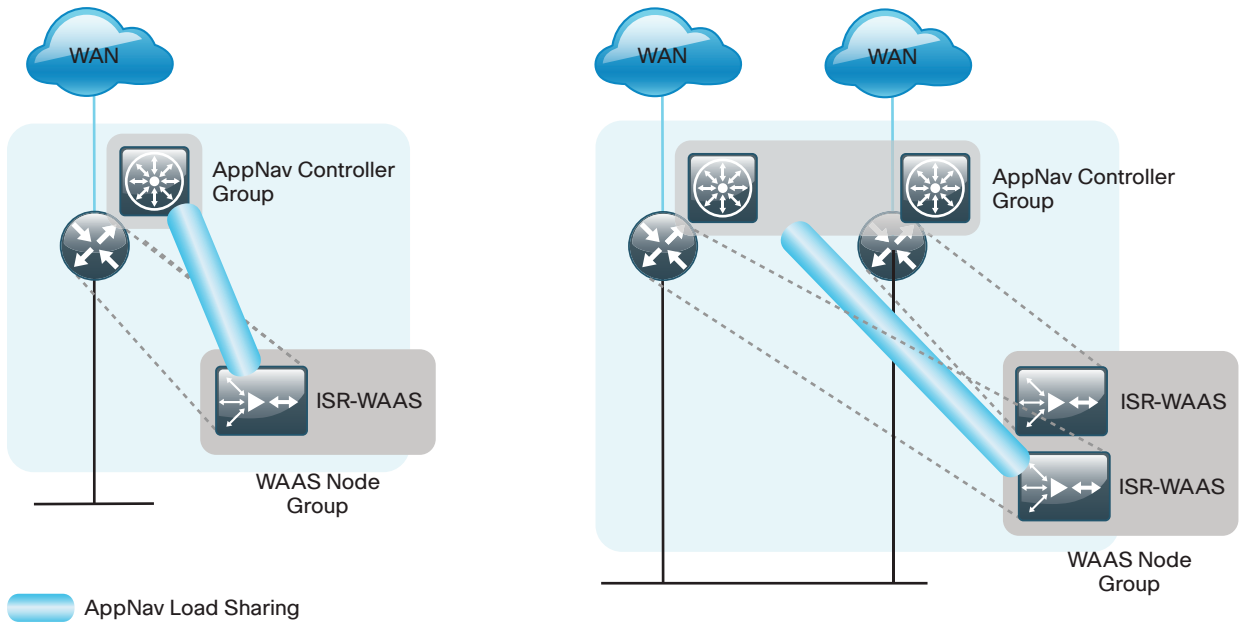


ISR-WAAS Remote-Site Design Models

The combination of AppNav-XE and ISR-WAAS on the Cisco ISR4451-X router is entirely self-contained when deployed at a single-router remote site. Logically, AppNav-XE runs separately on the host OS and ISR-WAAS runs as a guest OS. You configure service insertion on the router and traffic is redirected to ISR-WAAS, but in this case traffic never leaves the router.

The dual-router remote site provides additional resiliency from both a hardware and software perspective. Each router runs both AppNav-XE and ISR-WAAS. You configure a single AppNav controller group (ANCG) to distribute traffic for optimization to a single WNG that includes both ISR-WAAS instances. The application traffic load is shared across both ISR-WAAS instances in the WNG depending on the traffic flows and utilization of each ISR-WAAS instance. Traffic may be sent between the two routers in order to support this resiliency and load sharing.

Figure 4 - Cisco ISR-WAAS remote-site design models



1161

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 ISR-WAAS sizing is provided in the following table. The optimized throughput numbers correspond to the apparent bandwidth available after successful optimization by Cisco WAAS.

Table 7 - WAN remote-site Cisco ISR-WAAS on ISR 4451-X

Profile	Max. optimized TCP connections	Max. recommended WAN link [Mbps]	Max. optimized throughput [Mbps]	Akamai Connect Cache Capacity [GB]
ISR-WAAS-750	750	75	200	30
ISR-WAAS-1300	1300	100	300	30
ISR-WAAS-2500	2500	150	400	50

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

Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined.

Enter them as one command:

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

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

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 Central Manager network parameters

Parameter	CVD values	Site-specific values
Switch interface number	1/0/10	
VLAN number	148	
Time zone	PST8PDT - 8 0	
IP address	10.4.48.102/24	
Default gateway	10.4.48.1	
Host name	iw-iw-waas-cm-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

Because the appliance is dual-homed (because it is on a dual-homed Cisco FEX), you must assign the Ethernet interface configuration on both data center core Cisco Nexus 5500UP switches.

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**.

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

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

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

Step 3: Configure the time zone.

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)> [UTC 0 0]: PST8PDT -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]: 10.4.48.102/24
Enter Default Gateway IP Address [Not configured]: 10.4.48.1
```

Step 5: Configure the domain name system (DNS), host, and network time protocol (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): IW-WAAS-CM-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	10.4.48.102
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	IW-WAAS-CM-1
12. NTP Server Address	10.4.48.17
13. License	Enterprise

```
ESC Quit ? Help ! CLI ----- WAAS Final Configuration -----
```

```
Press 'y' to select configuration, 'd' to toggle defaults display, <1-13> to
change specific parameter [y]: y
```

```
Apply WAAS Configuration: Device Mode changed in SETUP; New configuration takes
effect after a reload. If applicable, registration with CM, CM IP address, WAAS
WCCP configuration etc, are applied after the reboot. Initiate system reload?
```

```
<y/n> [n] y
```

```
Are you sure? <y/n> [n]: y
```

Next, you will configure the device management protocols.

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

Step 9: Generate the RSA key, and then enable the sshd service. This enables secure shell protocol (SSH).

```
ssh-key-generate key-length 2048
sshd 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.

Procedure 4 Enable centralized AAA

(Optional)

This guide assumes that Cisco Secure Access Control System (Cisco Secure ACS) has already been configured. Only the procedures required to support the integration of Cisco WAAS into the deployment are included. For details on how to configure Cisco Secure ACS, see the [Device Management Using ACS Technology Design Guide](#).

Step 1: Log in to the Cisco WAAS Central Manager through the web interface (for example, <https://iw-waas-cm-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. You must complete this step before enabling AAA, and you can only perform it by using the web interface.

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

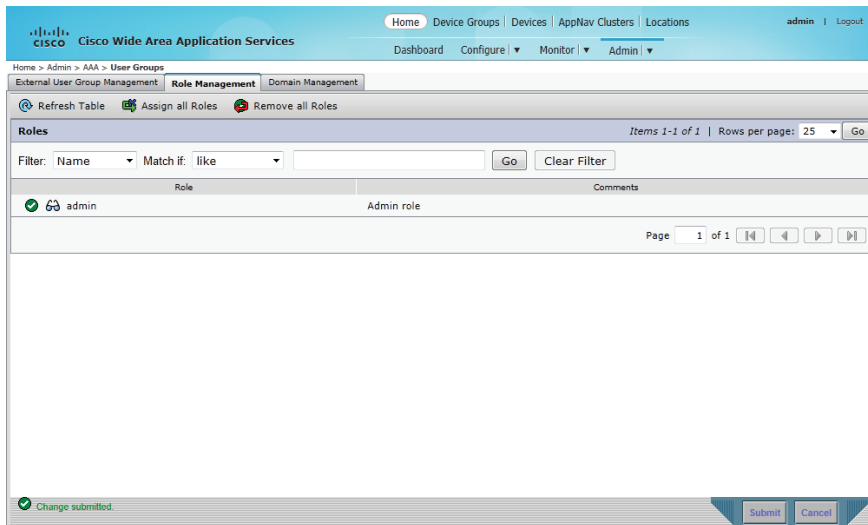
Step 3: In the **Name** box, enter a name. This name must match exactly (case sensitive) the group name used on the AAA server. For example, “Network Admins” in this implementation. Click **Submit**.

The screenshot shows the 'Creating New User Group' form in the Cisco Wide Area Application Services interface. The form has a 'Name' field containing 'Network Admins' and an empty 'Comments' text area. A note at the bottom left states 'Note: * Required Field'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

The screenshot shows the 'Role Management' tab in the Cisco Wide Area Application Services interface. The 'Roles' table has one entry: 'admin' with the role 'Admin role'. The 'Filter' section shows 'Name' and 'Match if: like'. The 'Page' indicator shows 'Page 1 of 1'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

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



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

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

Tech Tip

The AAA configuration details shown are for the Cisco WAAS devices only. Additional configuration is required on the AAA server for successful user authorization. Do not proceed with configuring secure user authentication until you have completed the relevant steps in the [Device Management Using ACS Technology Design Guide](#).

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

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

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

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

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

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 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 you use AAA for router administration, you must also use centralized AAA for the Cisco 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 c1sco123
```

Option 2: Create a centralized AAA account

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

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

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

Step 3: Click **Create**.

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

The screenshot shows the 'Create User' form in the 'Users and Identity Stores' interface. The form is divided into several sections:

- General:** Name: waascm, Status: Enabled, Description: WAAS Central Manager user, Identity Group: All Groups (with a 'Select' button).
- Password Information:** Password must: Contain 4 - 32 characters. Password Type: Internal Users (with a 'Select' button). Password: [masked], Confirm Password: [masked]. There is a checkbox for 'Change password on next login'.
- Enable Password Information:** Password must: Contain 4 - 32 characters. Enable Password: [checkbox], Confirm Password: [input field].
- User Information:** There are no additional identity attributes defined for user records.

At the bottom, there are 'Submit' and 'Cancel' buttons.

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

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

The screenshot shows the 'Identity Groups' selection dialog. It features a search filter and a table of groups:

Name	Description
All Groups	Identity Group Root
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

At the bottom, there are buttons for 'Create', 'Duplicate', 'File Operations', 'Export', 'OK', 'Cancel', and 'Help'.

Step 7: Click **Submit**.

Procedure 2 Register the router to the WAAS Central Manager

Step 1: Verify that SSH and secure HTTP (HTTPS) servers are enabled on the router. If they are not already configured, configure these services now.

Reader Tip

HTTPS and 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 **transport preferred none** on vty lines. This prevents 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://iw-waas-cm-1.cisco.local:8443>).

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)—**10.6.32.243, 10.6.32.244**
- Username—**waascm**
- Password—**c1sco123**
- Enable Password—**c1sco123**
- HTTP Authentication Type—**AAA**
- Central Manager IP Address—**10.4.48.102**

Step 6: Verify successful registration.

The screenshot shows the Cisco Wide Area Application Services (WAAS) Central Manager web interface. The page title is "Cisco IOS Router Registration". The "Router IP address entry method" is set to "Manual". The "IP Address(es)" field is empty. The "Username" is "waascm", the "Password" and "Enable Password" are masked with dots, and the "HTTP Authentication Type" is "AAA". The "Central Manager IP Address" is "10.4.48.102". Below the form, there are three informational messages: "SSH v1 or SSH v2 must be enabled on routers.", "These credentials are used once to register all the listed routers, which should have the same credentials.", and "These credentials are not used for communication between the Central Manager and the routers after registration finishes." The "Register" button is highlighted. Below the form is a "Registration Status" table with the following data:

IP Address	Hostname	Router type	Status
10.6.32.244	VPN-INET-AS...	AppNav-XE Co...	✔ Successfully processed the registration request
10.6.32.243	VPN-INET-AS...	AppNav-XE Co...	✔ Successfully processed the registration request

The bottom right corner of the interface shows "Alarms 3 0 0".

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

Procedure 3 Configure the AppNav-XE Cluster

In this procedure, you create the cluster and assign Cisco WAAS nodes.

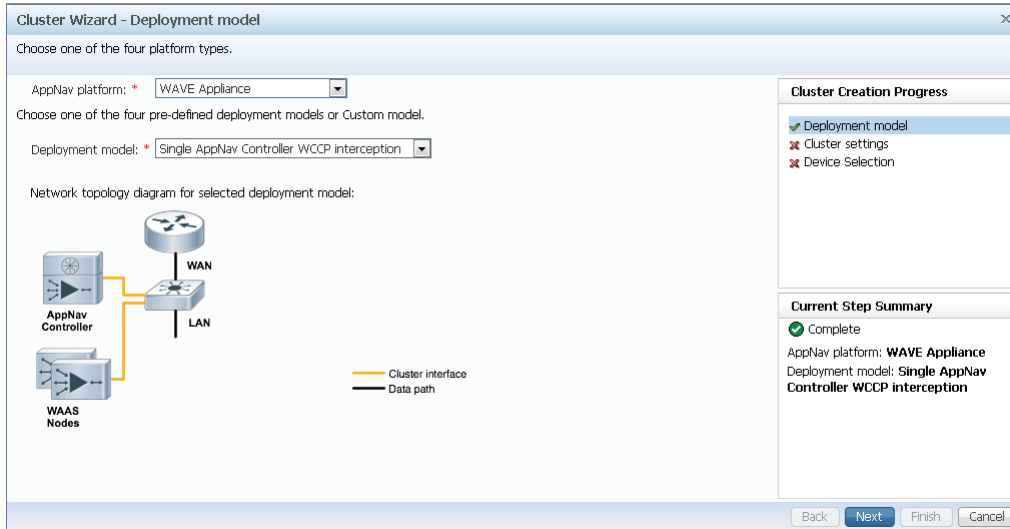
Tech Tip

This procedure assumes that one or more Cisco WAAS nodes have already been configured and are registered to the WAAS Central Manager. Any existing WCCP configuration 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://iw-waas-cm-1.cisco.local:8443>).

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

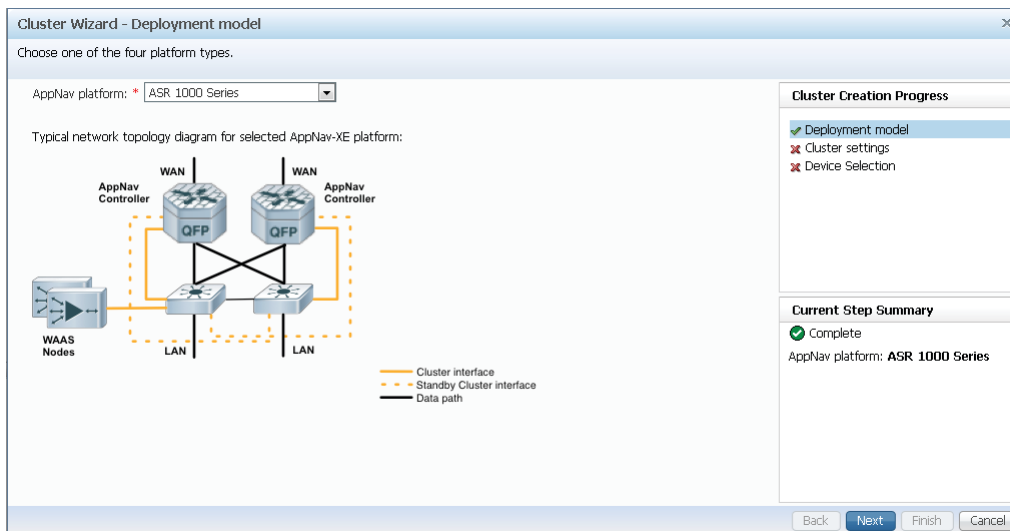
Step 3: Start the configuration by clicking on the AppNav Cluster Wizard.



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

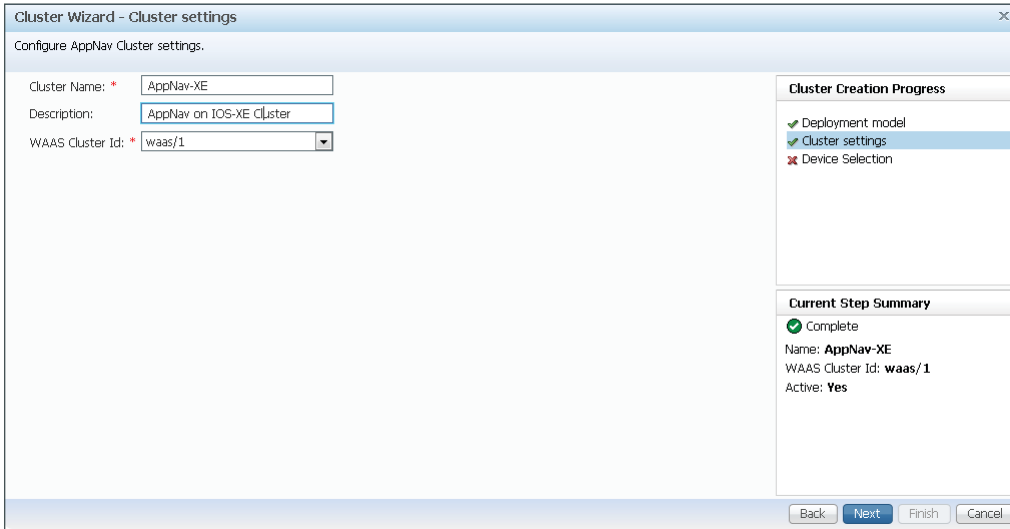
i Tech Tip

Cisco AppNav-XE clusters should include only routers with the same hardware model. ASR 1004 ESP 40 should not be in a cluster with ASR 1001. Likewise, within the ISR 4K family of routers, choose the same hardware model in order to avoid capacity mismatches.



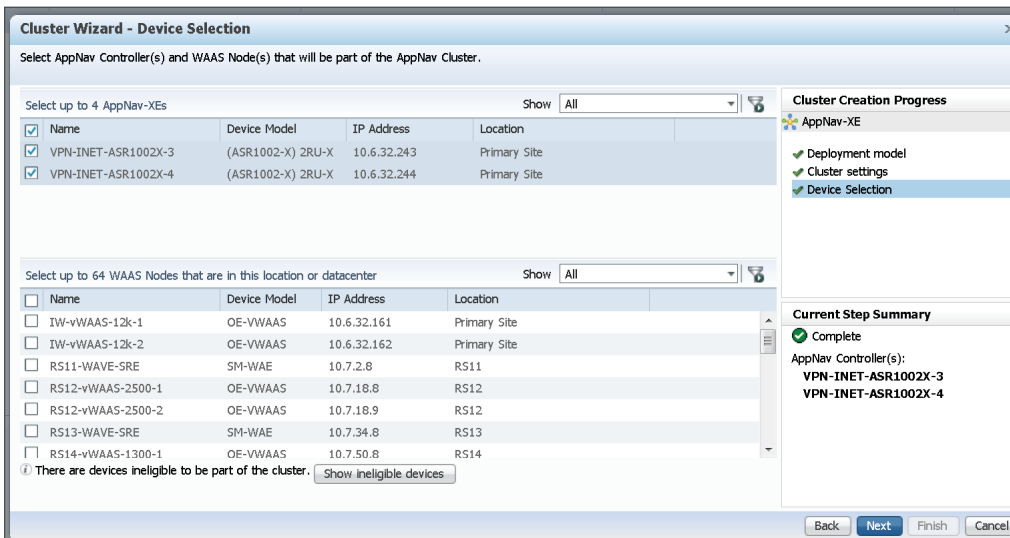
Step 5: Assign the Cluster Name to AppNav-XE, and then add a description.

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

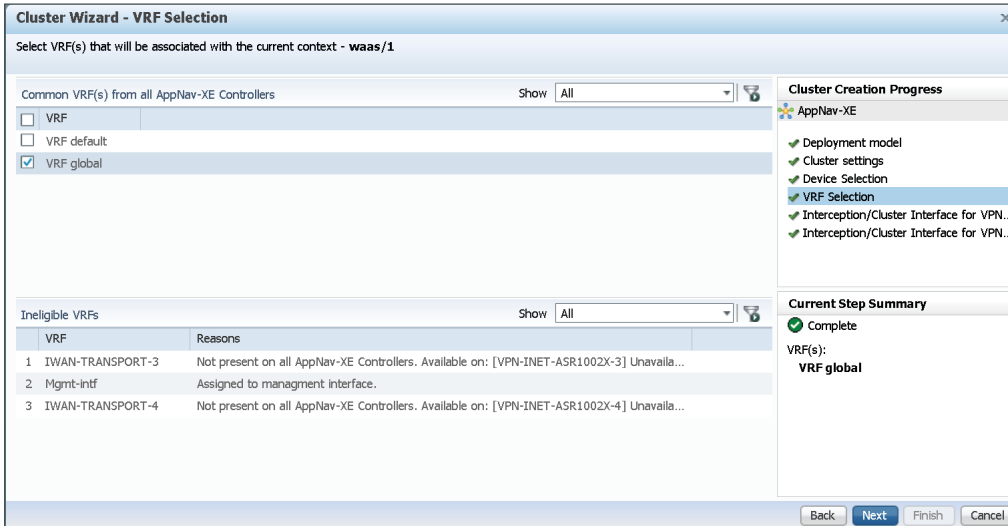


Step 7: Select Cisco AppNav-XE controllers (maximum of 4) to assign to the AppNav cluster under configuration.

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



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



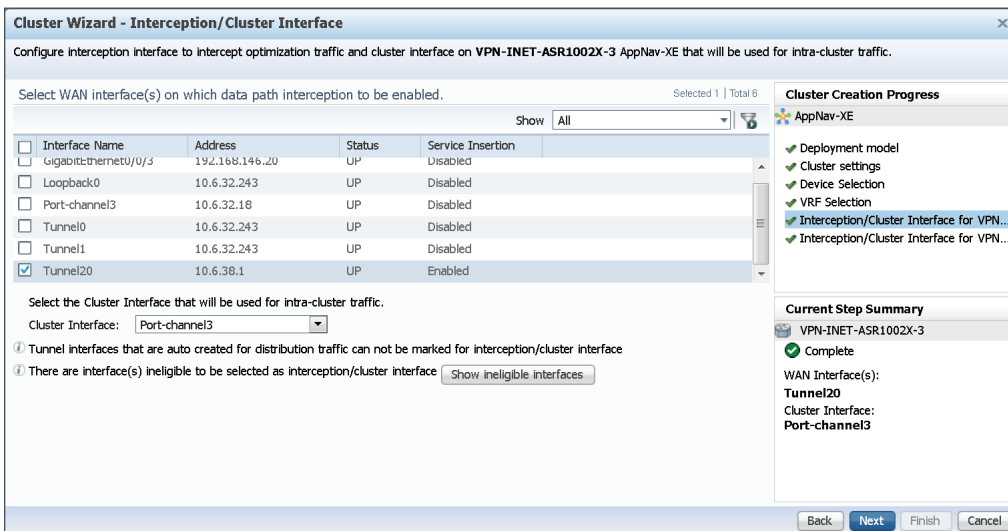
Step 10: Select all WAN-facing interfaces for interception, select the LAN-facing interface as the Cluster Interface for intra-cluster traffic, and then click **Next**. Example settings are shown in the following table.

i
Tech Tip

An AppNav-XE cluster may contain a maximum of four AppNav controllers.

Table 10 - Example Settings for Interception and Cluster Interfaces

Router	WAN transport	Interception interface(s)	Cluster Interface
VPN-ASR1002X-3	DMVPN-3	Tunnel20	Port-Channel3
VPN-ASR1001-4	DMVPN-4	Tunnel20	Port-Channel4

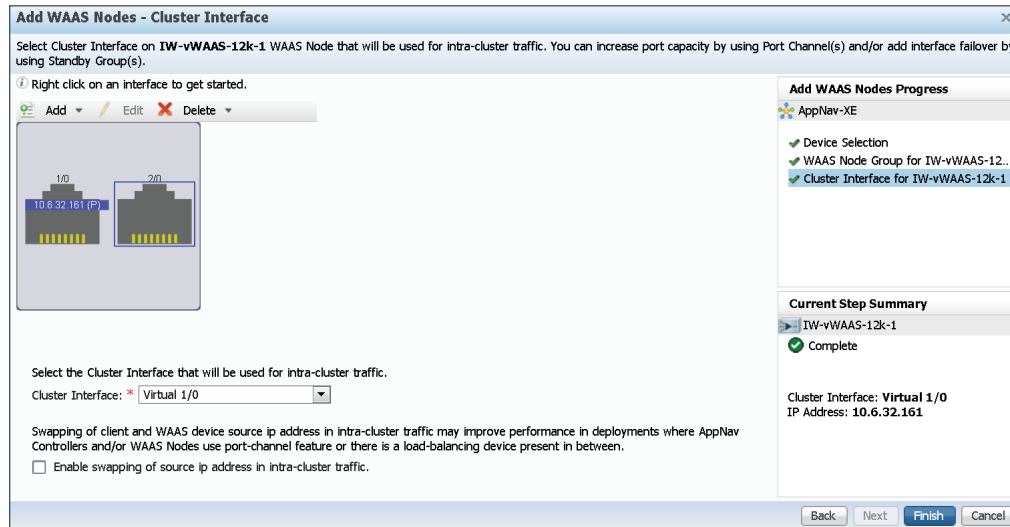


Step 11: Repeat Step 10 for any additional Cisco AppNav-XE controller routers.

Step 12: From the AppNav Cluster Home, select the Add WAAS Node.

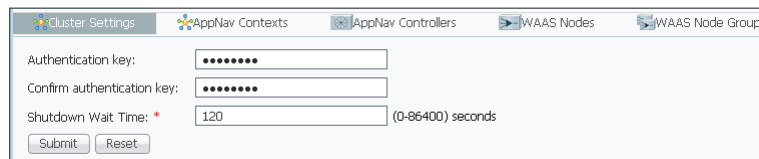
Step 13: Select a local WAAS device, and then click **Next**.

Step 14: Select the interface for the Cisco WAAS node to use for intra-cluster traffic (Example: Virtual 1/0). If this is the last WAAS node, click **Finish**. Otherwise, click **Next**.

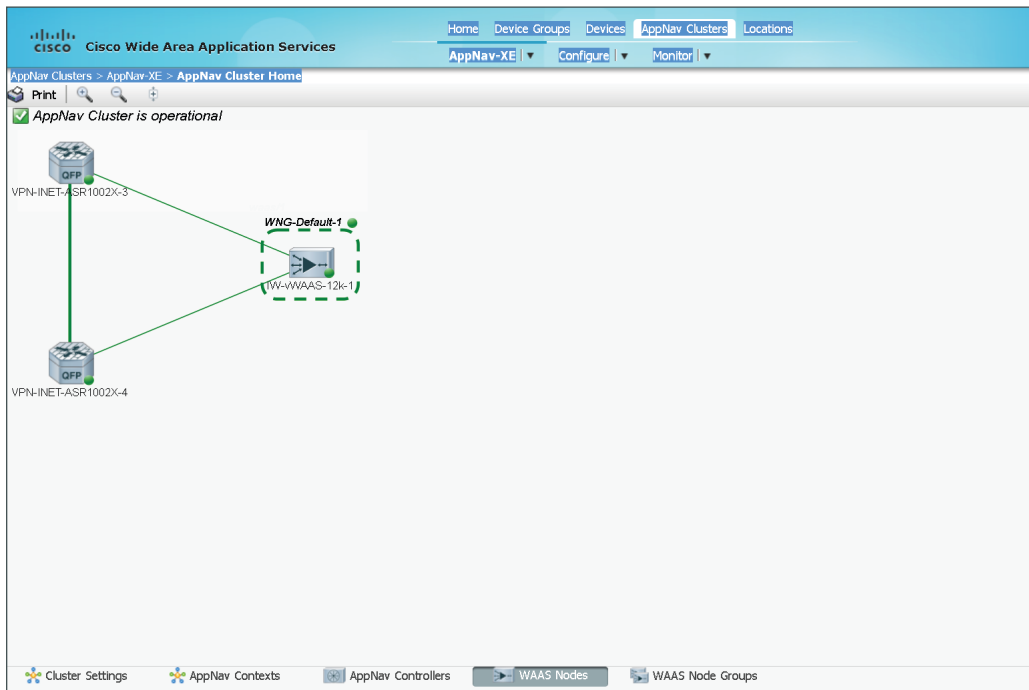


Step 15: Repeat Step 12 thru Step 14 for any additional WAAS nodes.

Step 16: 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.



Step 17: Navigate to **AppNav Clusters > AppNav-XE** and verify that the Cisco AppNav cluster is operational.



Deploying ISR WAAS

In each of the three installation methods, you may use Cisco WAAS Central Manager (WCM) to monitor ISR-WAAS performance.

You should use the method that meets your requirements:

- **Deploying ISR-WAAS at a Single-Router Remote Site**—This is the simplest installation method. The EZConfig setup script installs Cisco ISR-WAAS and configures AppNav-XE. This method is specific to a single-router deployment and requires manual modification if you need to adapt it to a dual-router deployment.
- **Changing Your Single-Router Remote Site to a Dual-Router Remote Site (Optional)**—After you have already completed a single-router, remote-site deployment using EZConfig, you can optionally add a second router. Rather than restart from the beginning, it is most straightforward to use EZConfig to deploy the new router. After completing EZConfig, you merge the two standalone configurations to use a single common ANCG and single common WNG.
- **Deploying ISR-WAAS at a Dual-Router Remote Site**—This is the most flexible method and separates the tasks for installing Cisco ISR-WAAS and configuring AppNav-XE. You add the Cisco ISR4451-X routers to Cisco WCM and then use the AppNav cluster wizard to configure the ANCG and WNG. In this method, you may use WCM to monitor AppNav-XE as well as ISR-WAAS. EZConfig is not used for this method.



Reader Tip

You may use the dual-router, remote-site procedure for a single-router site if you want to have central management and monitoring of AppNav-XE for these sites. Note that separate monitoring of both Cisco ISR4451-X and Cisco ISR-WAAS consumes additional resources on Cisco WCM.

This design guide uses certain standard design parameters and references various network infrastructure services that are not located within this solution. The below table lists these parameters. For your convenience, you can enter your values in the table and refer to it when configuring devices.

Table 11 - Universal design parameters

Network service	CVD values	Site-specific values
Domain name	cisco.local	
Active Directory, DNS server, DHCP server	10.4.48.10	
FTP server	10.4.48.11	
Cisco Secure ACS (Optional)	10.4.48.15	
NTP server	10.4.48.17	
SNMP read-only community	cisco	
SNMP read-write community	cisco123	

PROCESS

Preparing to Deploy ISR-WAAS

1. Verify resources on the ISR-WAAS host router

Procedure 1

Verify resources on the ISR-WAAS host router

The host router shares storage, memory, and CPU resources with the guest Cisco ISR-WAAS instance. There are three profiles available that correspond to the maximum number of concurrent TCP connections that are supported. Choose the required profile based on the expected number of TCP connections and compare the system requirements with the actual available before starting the installation and configuration.

Table 12 - ISR-WAAS profile resource requirements

Profile	ISR-WAAS-750	ISR-WAAS-1300	ISR-WAAS-2500	Site-specific values
Maximum TCP connections	750	1300	2500	
Disk space (MB)	170271	170288	360879	
Memory (MB)	4096	6144	8192	
CPU	25% system CPU	50% system CPU	75% system CPU	
VCPUs	2	4	6	

Step 1: Verify support for the chosen Cisco ISR-WAAS profile by checking the resources on the router. Compare the available resources with the minimum values listed in Table 12.

```
RS42-4451X-1#sh virtual-service tech-support | begin Resource
Resource virtualization limits:
Name                               Quota      Committed   Available
-----
system CPU (%)                     75
memory (MB)                        10240
bootflash (MB)                     1000
harddisk (MB)                      20000
volume-group (MB)                  190768
```

Step 2: Configure the FTP client on the host router.

```
ip ftp source-interface Loopback0
ip ftp username cvd
ip ftp password cisco123
```

Step 3: Transfer the Cisco ISR-WAAS OVA file to the host router.

i Tech Tip

Multiple filesystems are available on the Cisco ISR-4451X platform. During installation, the filesystem for the guest virtual service is created on harddisk, but you can store the OVA file on either bootflash or harddisk in order to prepare for the installation.

```
RS42-4451X-1#copy ftp://10.4.48.11/ISR4451X-WAAS-5.4.1.34.ova bootflash:
Destination filename [ISR4451X-WAAS-5.3.1.20.ova]?
Accessing ftp://10.4.48.11/ISR4451X-WAAS-5.3.1.20.ova...
Loading ISR4451X-WAAS-5.3.1.20.ova !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<content intentionally deleted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 939888640/4096 bytes]

939888640 bytes copied in 2836.528 secs (331352 bytes/sec)
```


Deploying ISR-WAAS at a Single-Router Remote Site

1. Use EZConfig to install ISR-WAAS and configure AppNav-XE

The easiest method for installing and configuring Cisco ISR-WAAS is to use the EZConfig program. This method is well-suited to single router-designs and completes most necessary steps. If you have a dual-router design, Cisco recommends that you use the process “Deploying ISR-WAAS at a Dual-Router Remote Site,” later in this guide.

Procedure 1 Use EZConfig to install ISR-WAAS and configure AppNav-XE

This process is for a single-router remote site. The host router does not need to be registered with Cisco WCM for this design because you do the entire configuration by using EZConfig.



Reader Tip

Although you don't use Cisco WCM to configure either the host router or the Cisco ISR-WAAS, you can use it to monitor the status and performance of the ISR-WAAS.

EZConfig:

- Installs the Cisco ISR-WAAS OVA as a guest virtual-service on the host router.
- Creates a WAAS Service Node group and adds Cisco ISR-WAAS as a single member of the group.
- Creates an AppNav Controller group and adds the host router running AppNav-XE as a single member of the group.
- Configures WAAS service insertion on the WAN interfaces.

Table 13 - Cisco ISR-WAAS network parameters

Parameter	CVD values ISR-WAAS	Site Specific Values
Router	RS42-4451X-1	
Virtual service name	AUTOWAAS	
Service node group	AUTOWAAS-SNG	
AppNav Controller group	AUTOWAAS-SCG	
Interception-method	appnav-controller	
Profile	ISR-WAAS-1300	
Data VLAN interface	Port-channel1.50	
Data VLAN IP address (AppNav controller IP)	10.7.208.1	
WAAS service IP	10.7.208.17	
WAN interface	GigabitEthernet0/0/0	
WAN interface 2	Tunnel10	
WAAS Central Manager	10.4.48.102	



Tech Tip

This example shows autodiscovery of the Cisco WCM IP address using DNS.

Step 1: Start Cisco ISR-WAAS EZConfig.

```
RS31-4451X#service waas enable
```

```
*****
****  Entering WAAS service interactive mode.          ****
****  You will be asked a series of questions, and your answers    ****
****  will be used to modify this device's configuration to        ****
****  enable a WAAS Service on this router.                ****
*****
```

```
Continue? [y]: y
```

```
At any time: ? for help, CTRL-C to exit.
```

```
Only one WAAS image found locally (harddisk:/ISR-WAAS-5.4.1.34.ova) - using as default
```

```
Extracting profiles from harddisk:/ISR-WAAS-5.4.1.34.ova, this may take a couple of
minutes ...
```

```
These are the available profiles
```

1. ISR-WAAS-2500
2. ISR-WAAS-1300
3. ISR-WAAS-750

```
Select option [1]: 1
```

```
An internal IP interface and subnet is required to deploy a WAAS service on this router.
This internal subnet must contain two usable IP addresses that can route and communicate
with the WAAS Central Manager (WCM).
```

```
The following ip address type supported for ISR-WAAS
```

- 1) ipv4
- 2) ipv6

```
Select ip address type (1 or 2):1
```

```
Enter the IPV4 address to be configured on the WAAS service: 10.7.130.8
```

```
The following ip address type supported for Host on Router
```

- 1) ipv4
- 2) ipv6

```
Select ip address type (1 or 2):1
```

The following ip address type for WCM

- 1) ipv4
- 2) ipv6

Select ip address type (1 or 2):1

Enter the IP address of the WAAS Central Manager (WCM): 10.4.48.102

The following IP interfaces are currently available on the router:

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	192.168.6.21	YES	NVRAM	up	up
GigabitEthernet0/0/1	172.18.98.202	YES	DHCP	up	up
GigabitEthernet0/0/2	unassigned	YES	NVRAM	up	up
Gi0/0/2.64	10.7.130.1	YES	NVRAM	up	up
Gi0/0/2.65	10.7.132.1	YES	NVRAM	up	up
Gi0/0/2.69	10.7.131.1	YES	NVRAM	up	up
Gi0/0/2.70	10.7.133.1	YES	NVRAM	up	up
Gi0/0/2.80	192.168.192.1	YES	manual	up	up
GigabitEthernet0/0/3	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet0	unassigned	YES	NVRAM	administratively down	down
Loopback0	10.255.241.31	YES	NVRAM	up	up
Loopback192	192.168.255.13	YES	manual	up	up
Tunnel0	10.255.241.31	YES	unset	up	up
Tunnel10	10.6.34.31	YES	NVRAM	up	up
Tunnel11	10.6.36.31	YES	NVRAM	up	up

Enter a WAN interface to enable WAAS interception (blank to skip) []: loop0

Enter additional WAN interface (blank to finish) []:

```
*****  
** Configuration Summary: **  
*****
```

a) WAAS Image and Profile Size:

harddisk:/ISR-WAAS-5.4.1.34.ova (982200320) bytes
ISR-WAAS-1300

b) Router IP/mask:

Using ip unnumbered from interface GigabitEthernet0/0/2.64

WAAS Service IP:

10.7.130.8

c) WAAS Central Manager:

10.4.48.102

d) Router WAN Interfaces:

Loopback0

Choose one of the letter from 'a-d' to edit, 'v' to view config script, 's' to apply config [s]:

The configuration will be applied and the status of the WAAS service will be displayed after deployment

Installing harddisk:/ISR-WAAS-5.4.1.34.ova

installing!!

The Cisco ISR-WAAS OVA is installed and activated. This takes several minutes.

Step 2: Save the configuration on the host router.

```
RS31-4451X# copy running-config startup-config
```

Step 3: Connect to the virtual service console in order to configure the device management protocols. You can exit from the console by typing `^c^c^c`. It may take a few minutes to receive a login prompt after activation, because ISR-WAAS operating system must boot completely. For all Cisco ISR-WAAS devices, the factory default username is **admin** and the factory default password is **default**.

```
RS31-4451X# virtual-service connect name AUTOWAAS console  
Connected to appliance. Exit using ^c^c^c
```

.....

Cisco Wide Area Application Engine Console

Username:

Step 4: In the EXEC mode, enable the propagation of local configuration changes to the WCM.

```
cms lcm enable
```

Step 5: Change the default password for the admin account (Example: c1sco123).

```
username admin passwd  
Warning: User configuration performed via CLI may be overwritten  
by the central manager. Please use the central manager to configure  
user accounts.  
New WAAS password: c1sco123  
Retype new WAAS password: c1sco123
```

Step 6: Generate the RSA key and enable the sshd service. This enables SSH.

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

Step 7: Enable SNMP. This allows the network infrastructure devices to be managed by an NMS. Configure SNMPv2c for both a read-only and a read-write community string.

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

Step 8: 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 9: 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 10: After you make configuration changes, in the EXEC mode, save the configuration.

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

Step 11: Disconnect from the virtual service console by typing **^c^c^c**.

Changing Your Single-Router Remote Site to a Dual-Router Remote Site

1. Install ISR-WAAS and configure AppNav-XE
2. Convert a standalone ISR-WAAS configuration to a group configuration

This optional process assumes you have already completed the previous process, “Deploying ISR-WAAS at a Single-Router Remote Site.”

Because you configure the first router of your dual-router remote site by using EZConfig, you can optionally configure a second router by using EZConfig.

Table 14 - Cisco ISR-WAAS network parameters

Parameter	CVD values ISR-WAAS (Router 1)	CVD Values ISR-WAAS (Router 2)	Site Specific Values
Router	RS42-4451X-1	RS42-4451X-2	
Virtual service name	AUTOWAAS	AUTOWAAS	
Service node group	AUTOWAAS-SNG	AUTOWAAS-SNG	
AppNav Controller group	AUTOWAAS-SCG	AUTOWAAS-SCG	
Interception-method	appnav-controller	appnav-controller	
Profile	ISR-WAAS-1300	ISR-WAAS-1300	
Data VLAN interface	Port-channel1.50	Port-channel2.54	
Data VLAN IP address (AppNav controller IP)	10.7.208.1	10.7.208.9	
WAAS service IP	10.7.208.17	10.7.130.18	
WAN interface	GigabitEthernet0/0/0	GigabitEthernet0/0/0	
WAN interface 2	Tunnel10	Tunnel11	
WAAS Central Manager	10.4.48.102	10.4.48.102	



Tech Tip

Each of the two standalone Cisco ISR4451-X routers includes a static route to the guest OS. It is not necessary to redistribute this static route into the LAN EIGRP process.

```
ip route 10.7.130.8 255.255.255.255 VirtualPortGroup31
```

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, and 2) the destination IP address is contained within an IP range that is referenced by an EIGRP network statement.

```
router eigrp 100
network 10.7.0.0 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.

Procedure 1 Install ISR-WAAS and configure AppNav-XE

Step 1: On the on the second remote site router, use EZConfig in order to install ISR-WAAS and configure AppNav-XE. Use the values in Table 14 column 3 with the configuration steps found in Procedure 1, “Use EZConfig to install ISR-WAAS and configure AppNav-XE.”

Procedure 2 Convert a standalone ISR-WAAS configuration to a group configuration

All AppNav-XE controllers should be in a single ANCG and all WNs should be in a single WNG at a dual-router remote site. The conversion from a pair of standalone ISR-WAAS deployments each created using EZConfig to a single combined deployment requires manual configuration.

Perform this procedure in parallel on both routers.

Step 1: On the first router, add the WAAS service IP address from the Cisco ISR-WAAS instance on the second router to the Service Node group.

```
service-insertion service-node-group AUTOWAAS-SNG
service-node 10.7.130.9
```

Step 2: On the second router, add the WAAS service IP address from the Cisco ISR-WAAS instance on the first router to the Service Node group.

```
service-insertion service-node-group AUTOWAAS-SNG
service-node 10.7.130.8
```

Step 3: On the first router, add the AppNav Controller IP address from the second router to the AppNav Controller group.

```
service-insertion appnav-controller-group AUTOWAAS-SCG
  appnav-controller 10.7.130.3
```

Step 4: On the second router, add the AppNav controller IP address from the first router to the AppNav Controller group.

```
service-insertion appnav-controller-group AUTOWAAS-SCG
  appnav-controller 10.7.130.2
```

Example: RS44-4451X-1

```
service-insertion service-node-group AUTOWAAS-SNG
  service-node 10.7.130.8
  service-node 10.7.130.9
service-insertion appnav-controller-group AUTOWAAS-SCG
  appnav-controller 10.7.130.2
  appnav-controller 10.7.130.3
```

Example: RS44-4451X-2

```
service-insertion service-node-group AUTOWAAS-SNG
  service-node 10.7.130.8
  service-node 10.7.130.9
service-insertion appnav-controller-group AUTOWAAS-SCG
  appnav-controller 10.7.130.2
  appnav-controller 10.7.130.3
```

PROCESS

Deploying ISR-WAAS at a Dual-Router Remote Site

1. Create a WAAS Central Manager user
2. Register the router to the WAAS Central Manager
3. Install the ISR-WAAS OVA as a guest virtual service on the host router
4. Configure the AppNav-XE cluster

In this process, you deploy a dual-router remote site. You register both routers with Cisco WCM. You install the Cisco ISR-WAAS virtual service manually and configure the AppNav-XE cluster by using the WCM AppNav Cluster Wizard. You do not use EZConfig for this process.

i Tech Tip

This process may be used for a single-router remote site. The configuration requires more steps than using EZConfig, but it also allows for centralized management and monitoring of the AppNav-XE controllers.

Procedure 1

Create a WAAS Central Manager user

You have two options for creating the Cisco WCM 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 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 WCM user.

Option 1: Create a local user account

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

```
username waascm privilege 15 password c1sco123
```

Option 2: Create a centralized AAA account

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

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

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

Step 3: Click **Create**.

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

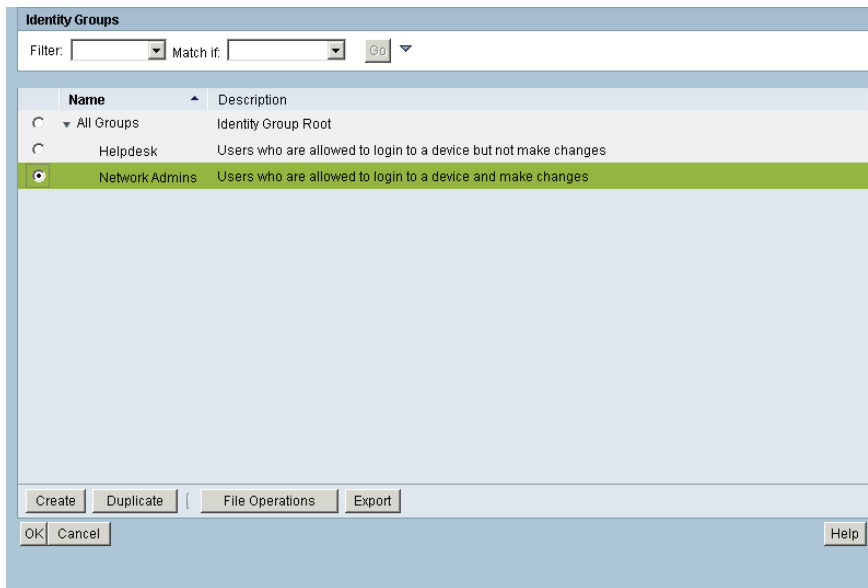
The screenshot displays the 'Create' form for a new user account in the Cisco Secure ACS Administration interface. The breadcrumb navigation at the top reads 'Users and Identity Stores > Internal Identity Stores > Users > Create'. The form is divided into several sections:

- General:** Includes fields for 'Name' (waascm), 'Status' (Enabled), 'Description' (WAAS Central Manager user), and 'Identity Group' (All Groups).
- Password Information:** Includes 'Password must' (Contain 4 - 32 characters), 'Password Type' (Internal Users), 'Password', and 'Confirm Password' fields.
- Enable Password Information:** Includes 'Enable Password' and 'Confirm Password' fields.
- User Information:** Includes a checkbox for 'Change password on next login' and a note: 'There are no additional Identity attributes defined for user records'.

A legend at the bottom left indicates that orange asterisks denote required fields. The form includes 'Submit' and 'Cancel' buttons at the bottom.

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

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



Step 7: Click **Submit**.

Procedure 2 Register the router to the WAAS Central Manager

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

Reader Tip

HTTPS and SSH are secure replacements for the HTTP and Telnet protocols. They use SSL and 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.

Step 2: Specify **transport preferred none** on vty lines. This prevents 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
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

Step 3: If you are using AAA authentication, configure the HTTP server to use AAA.

```
ip http authentication aaa
```

Step 4: Log in to Cisco WCM through the web interface (for example, https://waas-cm.cisco.local:8443).

Step 5: Navigate to **Admin > Registration > Cisco IOS Routers**.

The screenshot shows the 'Cisco IOS Router Registration' configuration page in the Cisco Wide Area Application Services (WAAS) web interface. The 'Router IP address entry method' is set to 'Manual'. The 'IP Address(es)' field is empty. The 'Username' field is empty, 'Password' and 'Enable Password' fields are masked with asterisks. The 'HTTP Authentication Type' is set to 'Local'. The 'Central Manager IP Address' is set to '10.4.48.102'. Below the form, there is a 'Register' button and a 'Registration Status' table which currently shows 'No data available'.

Step 6: Enter the management information of the WAN remote-site 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)—**10.255.241.215, 10.255.241.215**
- Username—**waascm**
- Password—**c1sco123**
- Enable Password—**c1sco123**
- HTTP Authentication Type—**AAA**
- Central Manager IP Address—**10.4.48.102**

The screenshot shows the 'Cisco IOS Router Registration' configuration page after successful registration. The 'Registration Status' table now displays two entries:

IP Address	Hostname	Router type	Status
10.255.241.42	RS42-4451X-1	AppNav-XE Co...	✔ Successfully processed the registration request.
10.255.242.42	RS42-4451X-2	AppNav-XE Co...	✔ Successfully processed the registration request.

Step 7: Verify successful registration.

Registration Status			
IP Address	Hostname	Router type	Status
10.255.241.42	RS42-4451X-1	AppNav-XE Co...	✔ Successfully processed the registration request
10.255.242.42	RS42-4451X-2	AppNav-XE Co...	✔ Successfully processed the registration request

Procedure 3 Install the ISR-WAAS OVA as a guest virtual service on the host router

Table 15 - Cisco ISR-WAAS network parameters

Parameter	CVD values ISR-WAAS (Router 1)	CVD values ISR-WAAS (Router 2)	Site-specific values
Router	RS42-4451X-1	RS42-4451X-2	
Virtual Service Name	RS42_4451X_1_WAAS	RS42_4451X_2_WAAS	
Profile	ISR-WAAS-1300	ISR-WAAS-1300	
Data VLAN Interface	Port-channel1.50	Port-channel2.54	
WAAS service IP	10.7.208.8	10.7.208.9	
WAAS Central Manager	10.4.48.102	10.4.48.102	

Step 1: Install the Cisco ISR-WAAS virtual service. Run this command from router exec mode.

i Tech Tip

The virtual service name may not include a dash "-".

```
RS42-4451X-1#virtual-service install name RS42_4451X_1_WAAS package harddisk:ISR-WAAS-5.4.1.34.ova
```

Step 2: Verify installation of the virtual service.

```
RS42-4451X-1#sh virtual-service list
Virtual Service List:
```

```

Name                               Status          Package Name
-----
RS42_4451X_1_WAAS                 Installed       ISR-WAAS-5.4.1.34.ova
```

Step 3: Configure the virtual port group interface and static route to the WAAS service IP.

```
interface VirtualPortGroup0
 ip unnumbered Port-channel1.50
!
ip route 10.7.208.8 255.255.255.255 VirtualPortGroup0
```



Tech Tip

It is not necessary to redistribute the following static route into the LAN EIGRP process.

```
ip route 10.7.208.8 255.255.255.255 VirtualPortGroup0
```

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, and 2) the destination IP address is contained within an IP range that is referenced by an EIGRP network statement.

```
router eigrp 100
network 10.7.0.0 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.

Step 4: Assign a profile to the virtual service, and then activate it.



Tech Tip

The virtual service name used below must match the virtual service name used in the installation above in Step 1.

```
virtual-service RS42_4451X_1_WAAS
profile ISR-WAAS-1300
vnic gateway VirtualPortGroup0
guest ip address 10.7.208.9
activate
```

Step 5: Verify activation of the virtual service.

```
RS42-4451X-1#sh virtual-service list
Virtual Service List:
```

Name	Status	Package Name
RS42_4451X_1_WAAS	Activated	ISR-WAAS-5.4.1.34.ova

Step 6: Connect to the virtual service console to configure the device management protocols. You can exit from the console by typing `^c^c^c`. It may take a few minutes to receive a login prompt after activation, because Cisco ISR-WAAS operating system must boot completely. For all Cisco ISR-WAAS devices, the factory default username is **admin** and the factory default password is **default**.

```
RS42-4451X-1# virtual-service connect name RS42_4451X_1_WAAS console
Connected to appliance. Exit using ^c^c^c
```

```
.....
```

```
Cisco Wide Area Application Engine Console
```

```
Username:
```

Step 7: Enter configuration mode.

```
RS43-4451X-1-ISR-WAAS# config t
```

Step 8: Change the default password for the admin account (Example: c1sco123).

```
username admin passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New WAAS password: c1sco123
Retype new WAAS password: c1sco123
```

Step 9: Generate the RSA key and enable the sshd service. This enables SSH.

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

Step 10: Enable SNMP. This allows the network infrastructure devices to be managed by an NMS. Configure SNMPv2c for both 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 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 12: 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 13: After you make configuration changes, in the EXEC mode, save the configuration.

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

Step 14: Disconnect from the virtual service console by typing `^c^c^c`.

Step 15: Register Cisco ISR-WAAS to Cisco WCM.

```
RS42-4451X-1# service waas wcm ip address 10.4.48.102
```

Step 16: Repeat Step 1 through Step 15 for the second router at the site.

Procedure 4 Configure the AppNav-XE cluster

In this procedure, you create the cluster and assign Cisco ISR-WAAS instances.

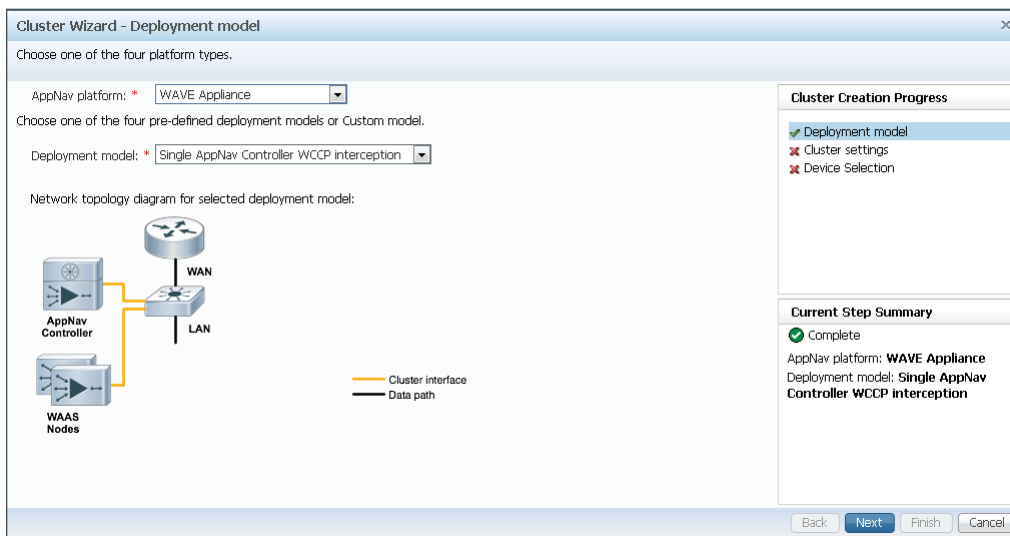
Tech Tip

This procedure assumes that one or more Cisco ISR-WAAS instances have already been configured and are registered to Cisco WCM.

Step 1: Log in to Cisco WCM through the web interface (for example, <https://iw-waas-cm-1.cisco.local:8443>).

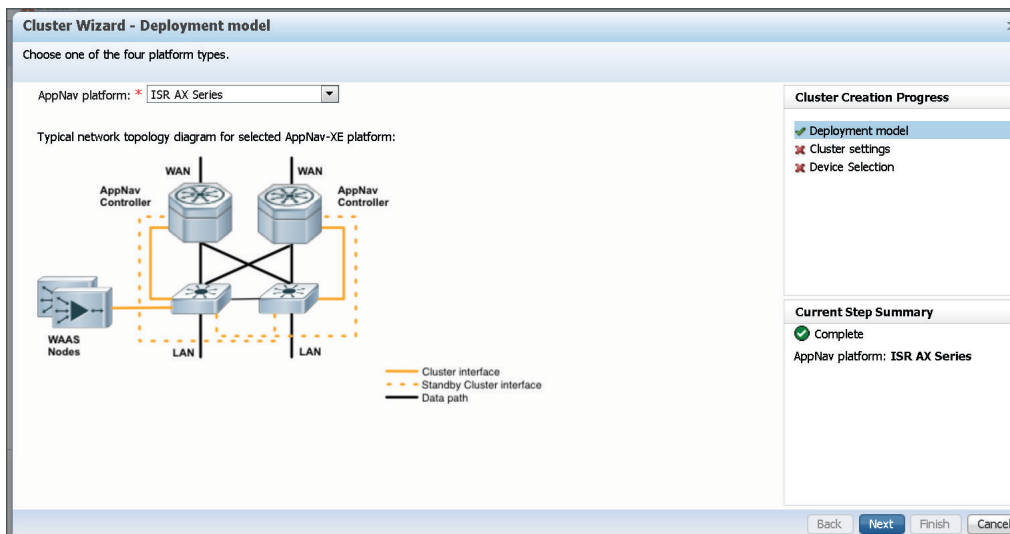
Step 2: Navigate to **AppNav Clusters > All AppNav Clusters**.

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



The screenshot shows the 'Cluster Wizard - Deployment model' window. The 'AppNav platform' is set to 'WAVE Appliance' and the 'Deployment model' is 'Single AppNav Controller WCCP interception'. A network topology diagram shows an AppNav Controller connected to a central switch (WAN/LAN) and WAAS Nodes. The 'Cluster Creation Progress' pane shows 'Deployment model' as complete, while 'Cluster settings' and 'Device Selection' are not. The 'Current Step Summary' pane confirms the configuration: 'AppNav platform: WAVE Appliance' and 'Deployment model: Single AppNav Controller WCCP interception'. Navigation buttons 'Back', 'Next', 'Finish', and 'Cancel' are at the bottom.

Step 4: Set the Cisco AppNav platform to **ISR AX Series**, and then click **Next**.



The screenshot shows the 'Cluster Wizard - Deployment model' window with the 'AppNav platform' set to 'ISR AX Series'. The 'Typical network topology diagram for selected AppNav-XE platform' shows two AppNav Controllers connected to a central switch (WAN/LAN) and WAAS Nodes. The 'Cluster Creation Progress' pane shows 'Deployment model' as complete, while 'Cluster settings' and 'Device Selection' are not. The 'Current Step Summary' pane confirms the configuration: 'AppNav platform: ISR AX Series'. Navigation buttons 'Back', 'Next', 'Finish', and 'Cancel' are at the bottom.



Tech Tip

Cisco AppNav-XE clusters should include only routers with the same hardware model. ASR 1004 ESP 40 should not be in a cluster with ASR 1001. Likewise, within the ISR 4K family of routers, choose the same hardware model in order to avoid capacity mismatches.

Step 5: In the **Cluster Name** box, enter **RS42-AppNav-XE**, and then in the **Description** box, enter a description.

Step 6: In the **WAAS Cluster Id** list, choose the default setting of **waas/1**, and then click **Next**.

Cluster Wizard - Cluster settings

Configure AppNav Cluster settings.

Cluster Name: * RS42-AppNav-XE
Description: RS42-AppNav-XE Cluster
WAAS Cluster Id: * waas/1

Cluster Creation Progress

- ✓ Deployment model
- ✓ Cluster settings
- ✗ Device Selection

Current Step Summary

✓ Complete
Name: RS42-AppNav-XE
WAAS Cluster Id: waas/1
Active: Yes

Back Next Finish Cancel

Step 7: Select Cisco AppNav-XE controllers (maximum of 4) that you want to assign to the AppNav cluster under configuration (Example: RS42-4451X-1, RS42-4451X-2).

Step 8: Select the WAAS nodes that you want to assign to the AppNav cluster under configuration (Example: RS42-4451X-1-ISR-WAAS, RS42-4451X-2-ISR-WAAS). After you have selected all devices you want, click **Next**.

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

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.



Tech Tip

An AppNav-XE cluster may contain a maximum of four AppNav Controllers.

Table 16 - Example settings for interception and cluster interfaces

Router	WAN transport	Interception interface(s)	Cluster Interface
RS42-4451X-1	Layer 2 WAN	Gig0/0/3.39	Port-Channel1.64
RS42-4451X-2	DMVPN-1	Tunnel10	Port-Channel2.64

Step 11: 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: Virtual1/0). If this is the last WAAS node, click **Finish**, otherwise click **Next**.

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

Step 14: Navigate to **AppNav Clusters > RS42-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.

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

PROCESS

Deploying Akamai Connect with Cisco WAAS

1. Enable Akamai Connect within Cisco WAAS Central Manager

Starting with release 5.4 of Cisco WAAS, there is support for enabling Akamai Connect on Cisco WAAS devices from within Cisco WAAS Central Manager. Although the software is available, it requires a Cisco Akamai Connect license to be uploaded before it can be enabled.

Reader Tip

You can find the platforms that support Akamai Connect in the [Cisco IWAN with Akamai Connect Data Sheet](#) . The [Cisco WAAS Configuration Guide](#) details the required steps.

Some of the features and benefits of adding Akamai Connect to your WAAS deployment include:

Features:

- Intelligent transparent object-caching
- Integration with Akamai's Edge Grid Network, which provides low-latency content delivery network transfers (via Akamai Connected Cache)
- Dynamic URL cache to enable caching of sites like YouTube that use unique URLs per request
- Cache prepositioning (warming) for site, video, or software content that you specify
- First- and second-pass acceleration; Akamai Connect works with WAAS middle-mile capabilities (including DRE, LZ, TFO, SSL acceleration)

Benefits:

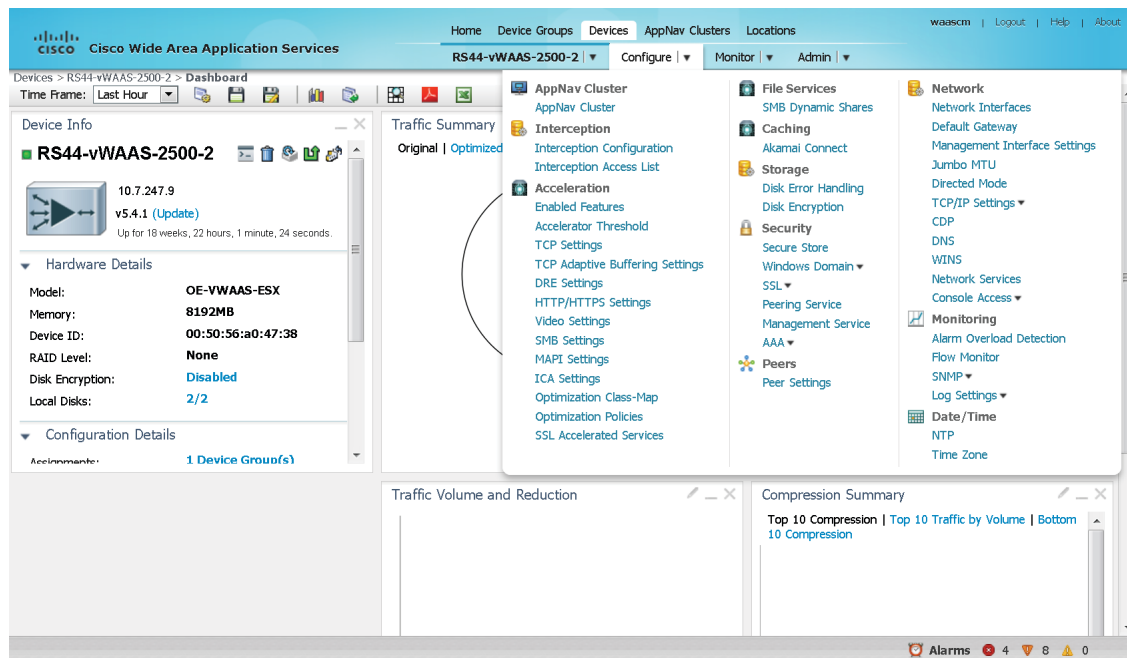
- Significant and measurable WAN and DIA data offload.
- Improved application performance for both intranet and Internet sites/applications
- Scalable solution to support video delivery and software updates at branch locations

There are several options for further improving the Akamai caching. The testing for this design did not change any of these settings; for details regarding deployment requirements and about specifics regarding these option settings, see the [Cisco WAAS Configuration Guide](#).

Procedure 1 Enable Akamai Connect within Cisco WAAS Central Manager

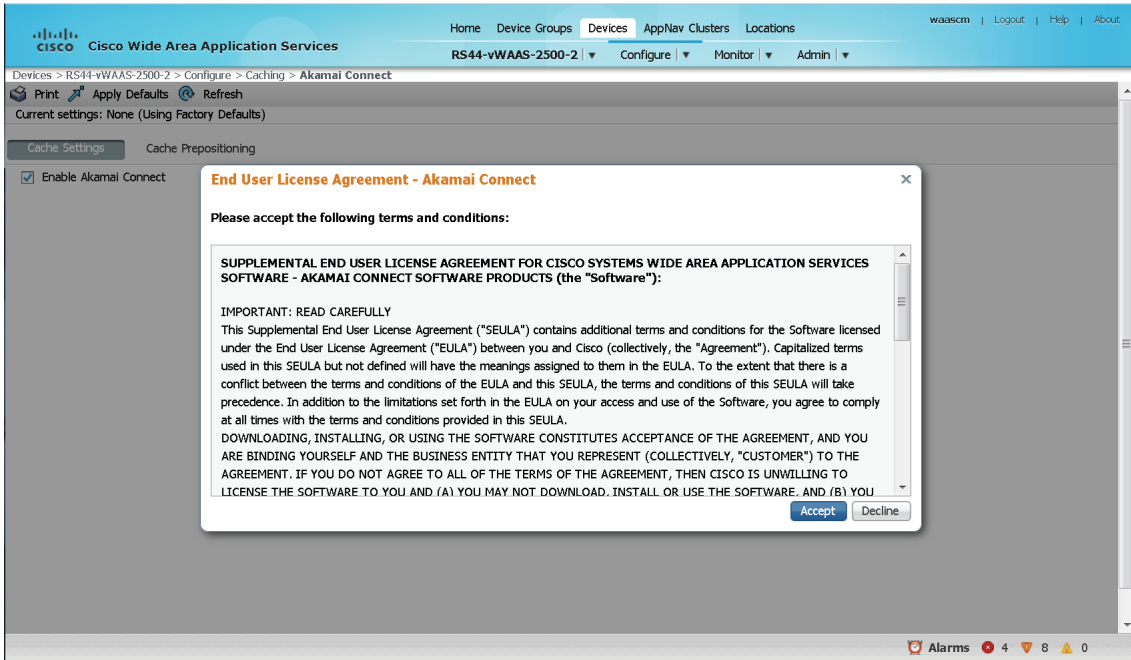
Step 1: From the listing of **All Devices**, select the remote site in order to add Akamai Connect caching.

Step 2: Select **Configure > Caching > Akamai Connect**.

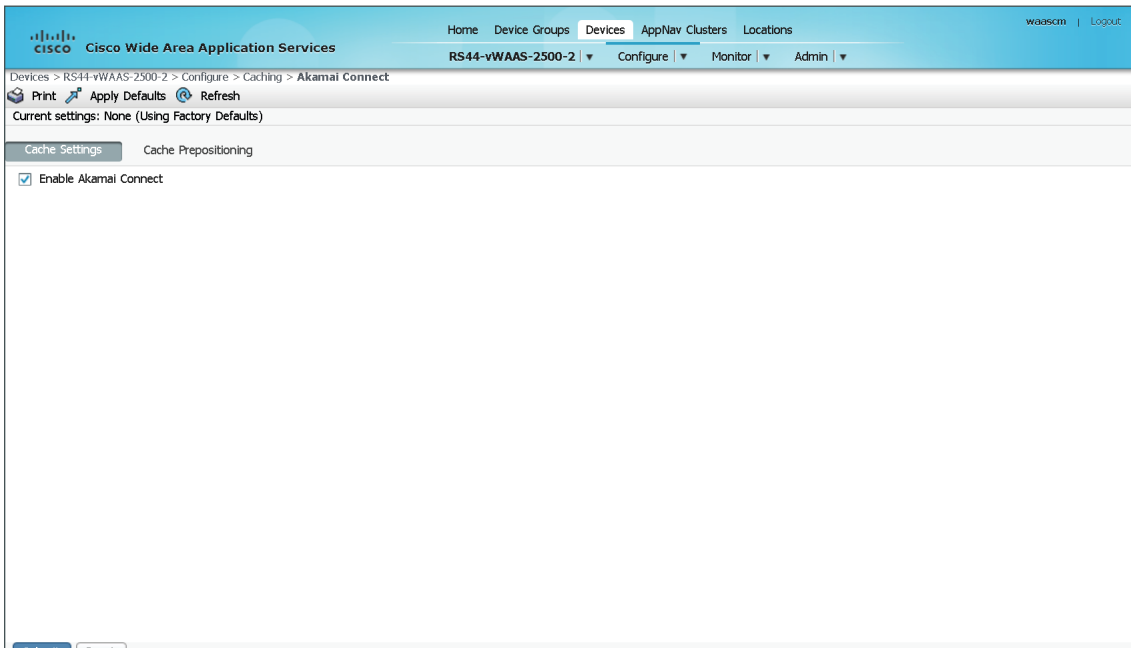


Step 3: Select **Enable Akamai Connect**.

Step 4: In the licensing dialog box, click **Accept**.



Step 5: At the bottom of the page, click **Submit**.



Appendix A: Product List

WAN Aggregation

Place In Network	Product Desc.	Part Number	SW Version	Feature Set
WAN-aggregation Router	Aggregation Services 1002X Router	ASR1002X-5G-VPNK9	IOS-XE 15.5(1)S	Advanced Enterprise
	Cisco ISR 4451-X Security Bundle w/ SEC license PAK	ISR4451-X-SEC/K9	IOS-XE 15.5(1)S	securityk9

WAN Remote Site

Place In Network	Product Desc.	Part Number	SW Version	Feature Set
Modular WAN Remote-site Router	Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU	ISR4451-X-AX/K9	IOS-XE 15.5(1)S	securityk9, appxk9

LAN Access Layer

Place In Network	Product Desc.	Part Number	SW Version	Feature Set
Modular Access Layer Switch	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.1XO(15.1.1XO1)	IP Base
	Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps	WS-X45-SUP8-E	3.3.1XO(15.1.1XO1)	IP Base
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	–	–
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	–	–
	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3)	IP Base
	Cisco Catalyst 4500E Supervisor Engine 7L-E, 520Gbps	WS-X45-SUP7L-E	3.5.3E(15.2.1E3)	IP Base
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	–	–
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	–	–

Place In Network	Product Desc.	Part Number	SW Version	Feature Set
Stackable Access Layer	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.6.0E(15.2.2E)	IP Base
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	3.6.0E(15.2.2E)	IP Base
	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 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink	WS-C3650-24PD	3.6.0E(15.2.2E)	IP Base
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	3.6.0E(15.2.2E)	IP Base
	Cisco Catalyst 3650 Series Stack Module	C3650-STACK	–	–
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.2(1)E3	IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	15.2(1)E3	IP Base
	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	–	–
	Cisco Catalyst 2960-X Series 24 10/100/1000 Ethernet and 2 SFP+ Uplink	WS-C2960X-24PD	15.0(2)EX5	LAN Base
	Standalone Access Layer Switch	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	3.6.0E(15.2.2E)

LAN Distribution Layer

Place In Network	Product Desc.	Part Number	SW Version	Feature Set
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	15.1(2)SY3	IP Services
	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.1(2)SY3	IP Services
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	–	–
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	–	–
	Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	–	–
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	–	–
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	15.1(2)SY3	IP services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	15.1(2)SY3	IP services
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	–	–
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	–	–
	Cisco Catalyst 6500 48-port GigE Mod (SFP)	WS-X6748-SFP	–	–
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	–	–
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	–	–
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	–	–
Extensible Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6880-X Extensible Fixed Aggregation Switch (Standard Tables)	C6880-X-LE	15.1(2)SY3	IP Services
	Cisco Catalyst 6800 Series 6880-X Multi Rate Port Card (Standard Tables)	C6880-X-LE-16P10G	–	–
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3)	Enterprise Services
	Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	3.5.3E(15.2.1E3)	Enterprise Services
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	–	–
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	–	–
Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500-X Series 32 Port 10GbE IP Base Front-to-Back Cooling	WS-C4500X-32SFP+	3.5.3E(15.2.1E3)	Enterprise Services

Place In Network	Product Desc.	Part Number	SW Version	Feature Set
Stackable Distribution Layer Switch	Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet	WS-C3850-12S	3.6.0E(15.2.2E)	IP Services
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	–	–
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	–	–
	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.2(1)E3	IP Services
	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	–	–

Appendix B: Caveats

Since the validation of this system, bug ID CSCur23656 has been opened to evaluate the impacts of the SSLv3 POODLE vulnerability on platforms running IOS and IOS XE. It is highly recommended that you:

- Deploy a version of IOS XE that contains the necessary fixes, or
- Avoid the use of SSLv3 and instead use TLSv1.

Appendix C: Changes

- This guide combines previously published material from the Application Optimization Using Cisco WAAS Design Guide and the Application Optimization Using Cisco ISR-WAAS Design Guide.
- We enabled Akamai Connect from within WAAS Central Manager where applicable.

Appendix D: Configuration Examples

Central Manager

WAAS Central Manager (vWAAS)

```
IW-WAAS-CM#sh run
! waas-universal-k9 version 5.4.1 (build b34 Aug  8 2014)
!
device mode central-manager
!
!
!
hostname IW-WAAS-CM
!
clock timezone PST8PDT -7 0
!
!
ip domain-name cisco.local
!
!
primary-interface Virtual 1/0
!
interface Virtual 1/0
 ip address 10.4.48.102 255.255.255.0
 ip access-group 155 in
 exit
interface Virtual 2/0
 shutdown
 exit
!
ip default-gateway 10.4.48.1
!
!
! ip path-mtu-discovery is disabled in WAAS by default
!
ip name-server 10.4.48.10
!
!
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
!
!
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
!
!
!
!
no telnet enable
!
sshd enable
!
!
!
!
!
!
! End of WAAS configuration

```

Aggregation Router Configuration

```
VPN-MPLS-ASR1002X-1#sh run
Building configuration...

Current configuration : 10395 bytes
!
! Last configuration change at 07:48:22 PDT Tue Mar 31 2015 by agroudan
! NVRAM config last updated at 13:10:13 PST Tue Jan 20 2015 by kfleshne
!
version 15.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname VPN-MPLS-ASR1002X-1
!
boot-start-marker
boot system bootflash:asr1002x-universalk9.03.13.01.S.154-3.S1-ext.SPA.bin
boot-end-marker
!
aqm-register-fnf
!
vrf definition IWAN-TRANSPORT-1
!
address-family ipv4
exit-address-family
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
enable secret 5 $1$S7wW$LwAu9mADPzeXE.yQjFmIc1
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
```

```

aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
!
!
!
!
!
!
!

ip domain name cisco.local

ip multicast-routing distributed
!
!
!
!
!
!
!
!
!
!
!
subscriber templating
!
!
flow record Record-FNF-IWAN
  description Flexible NetFlow for IWAN Monitoring
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  match flow direction
  collect routing source as

```

```

collect routing destination as
collect routing next-hop address ipv4
collect ipv4 dscp
collect ipv4 id
collect ipv4 source prefix
collect ipv4 source mask
collect ipv4 destination mask
collect transport tcp flags
collect interface output
collect flow sampler
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect application name
!
!
flow exporter Export-FNF-LiveAction
description FNFv9 with LiveAction
destination 10.4.48.178
source Loopback0
transport udp 2055
option interface-table
option application-table
option application-attributes
!
!
flow monitor Monitor-FNF-IWAN
description IWAN Traffic Analysis
exporter Export-FNF-LiveAction
cache timeout inactive 10
cache timeout active 60
record Record-FNF-IWAN
!
multilink bundle-name authenticated
!
domain iwan
vrf default
border
source-interface Loopback0
master 10.6.32.251
password 7 06055E324F41584B56
collector 10.4.48.178 port 2055
!
key chain LAN-KEY
key 1
key-string 7 011057175804575D72

```

```

key chain WAN-KEY
  key 1
    key-string 7 0007421507545A545C
  !
!
!
!
!
!
!
!
!
license udi pid ASR1002-X sn JAE180107T0
license boot level adventerprise
spanning-tree extend system-id
!
username admin secret 5 $1$SnKm$ibEw/1V702JMAMj/C/qzs.
!
redundancy
  mode none
!
!
!
crypto ikev2 keyring DMVPN-KEYRING-1
  peer ANY
    address 0.0.0.0 0.0.0.0
    pre-shared-key c1sco123
  !
!
!
crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-1
  match fvrf IWAN-TRANSPORT-1
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local DMVPN-KEYRING-1
!
!
!
cdp run
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 00071A150754
ip tftp source-interface GigabitEthernet0
!
class-map match-any STREAMING-VIDEO

```



```

    match dscp af31 af32 cs5
class-map match-any INTERACTIVE-VIDEO
    match dscp cs4 af41 af42
class-map match-any CRITICAL-DATA
    match dscp af11 af21
class-map match-any NET-CTRL-MGMT
    match dscp cs2 cs6
class-map match-any VOICE
    match dscp ef
class-map match-any SCAVENGER
    match dscp cs1
class-map match-any CALL-SIGNALING
    match dscp cs3
!
policy-map WAN
    class INTERACTIVE-VIDEO
        bandwidth remaining percent 30
        random-detect dscp-based
        set dscp tunnel af41
    class STREAMING-VIDEO
        bandwidth remaining percent 10
        random-detect dscp-based
        set dscp tunnel af41
    class NET-CTRL-MGMT
        bandwidth remaining percent 5
        set dscp tunnel cs6
    class CALL-SIGNALING
        bandwidth remaining percent 4
        set dscp tunnel af41
    class CRITICAL-DATA
        bandwidth remaining percent 25
        random-detect dscp-based
        set dscp tunnel af21
    class SCAVENGER
        bandwidth remaining percent 1
        set dscp tunnel af11
    class VOICE
        priority level 1
        police cir percent 10
        set dscp tunnel ef
    class class-default
        bandwidth remaining percent 25
        random-detect
        set dscp tunnel default
policy-map RS-GROUP-200MBPS-POLICY
    class class-default
        shape average 200000000

```

```

    bandwidth remaining ratio 200
    service-policy WAN
policy-map RS-GROUP-4G-POLICY
    class class-default
    shape average 8000000
    bandwidth remaining ratio 8
    service-policy WAN
policy-map RS-GROUP-20MBPS-POLICY
    class class-default
    shape average 20000000
    bandwidth remaining ratio 20
    service-policy WAN
policy-map WAN-INTERFACE-G0/0/3-SHAPE-ONLY
    class class-default
    shape average 1000000000
policy-map RS-GROUP-30MBPS-POLICY
    class class-default
    shape average 30000000
    bandwidth remaining ratio 30
    service-policy WAN
policy-map RS-GROUP-300MBPS-POLICY
    class class-default
    shape average 300000000
    bandwidth remaining ratio 300
    service-policy WAN
policy-map RS-GROUP-100MBPS-POLICY
    class class-default
    shape average 100000000
    bandwidth remaining ratio 100
    service-policy WAN
policy-map RS-GROUP-50MBPS-POLICY
    class class-default
    shape average 50000000
    bandwidth remaining ratio 50
    service-policy WAN
policy-map RS-GROUP-10MBPS-POLICY
    class class-default
    shape average 10000000
    bandwidth remaining ratio 10
    service-policy WAN
!
!
!
!
!
!
!
!
!
!

```

```

!
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE-TRANSPORT-1
set transform-set AES256/SHA/TRANSPORT
set ikev2-profile FVRF-IKEv2-IWAN-TRANSPORT-1
!
!
!
!
!
!
!
!
!
interface Loopback0
ip address 10.6.32.241 255.255.255.255
ip pim sparse-mode
!
interface Port-channel1
description IWAN-D3750X
ip address 10.6.32.2 255.255.255.252
ip flow monitor Monitor-FNF-IWAN input
ip flow monitor Monitor-FNF-IWAN output
ip pim sparse-mode
no negotiation auto
!
interface Tunnel10
bandwidth 1000000
ip address 10.6.34.1 255.255.254.0
no ip redirects
ip mtu 1400
ip flow monitor Monitor-FNF-IWAN input
ip flow monitor Monitor-FNF-IWAN output
ip pim nbma-mode
ip pim sparse-mode
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp map group RS-GROUP-50MBPS service-policy output RS-GROUP-50MBPS-POLICY
ip nhrp map group RS-GROUP-10MBPS service-policy output RS-GROUP-10MBPS-POLICY
ip nhrp map group RS-GROUP-300MBPS service-policy output RS-GROUP-300MBPS-POLICY
ip nhrp map group RS-GROUP-200MBPS service-policy output RS-GROUP-200MBPS-POLICY
ip nhrp map group RS-GROUP-100MBPS service-policy output RS-GROUP-100MBPS-POLICY
ip nhrp map group RS-GROUP-30MBPS service-policy output RS-GROUP-30MBPS-POLICY

```

```

ip nhrp map group RS-GROUP-20MBPS service-policy output RS-GROUP-20MBPS-POLICY
ip nhrp map group RS-GROUP-4G service-policy output RS-GROUP-4G-POLICY
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
tunnel source GigabitEthernet0/0/3
tunnel mode gre multipoint
tunnel key 101
tunnel vrf IWAN-TRANSPORT-1
tunnel protection ipsec profile DMVPN-PROFILE-TRANSPORT-1
domain iwan path MPLS
!
interface GigabitEthernet0/0/0
description IWAN-D3750X Gig1/0/1
no ip address
negotiation auto
cdp enable
channel-group 1
!
interface GigabitEthernet0/0/1
description IWAN-D3750X Gig2/0/1
no ip address
negotiation auto
cdp enable
channel-group 1
!
interface GigabitEthernet0/0/2
no ip address
negotiation auto
!
interface GigabitEthernet0/0/3
bandwidth 1000000
vrf forwarding IWAN-TRANSPORT-1
ip address 192.168.6.1 255.255.255.252
negotiation auto
service-policy output WAN-INTERFACE-G0/0/3-SHAPE-ONLY
!
interface GigabitEthernet0/0/4
no ip address
negotiation auto
!
interface GigabitEthernet0/0/5
description IWAN-IOS-CA
vrf forwarding IWAN-TRANSPORT-1
ip address 192.168.6.253 255.255.255.252

```

```

negotiation auto
cdp enable
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp IWAN-EIGRP
!
 address-family ipv4 unicast autonomous-system 400
!
  af-interface default
   passive-interface
  exit-af-interface
!
  af-interface Port-channell
   authentication mode md5
   authentication key-chain LAN-KEY
   no passive-interface
  exit-af-interface
!
  af-interface Tunnel10
   authentication mode md5
   authentication key-chain WAN-KEY
   hello-interval 20
   hold-time 60
   no passive-interface
   no split-horizon
  exit-af-interface
!
 topology base
  distribute-list route-map SET-TAG-DMVPN-1 out Port-channell
  distribute-list route-map SET-TAG-ALL out Tunnel10
  distribute-list route-map BLOCK-DMVPN-2 in Port-channell
 exit-af-topology
 network 10.6.0.0 0.1.255.255
 eigrp router-id 10.6.32.241
 nsf
 exit-address-family
!
 ip forward-protocol nd
!
 no ip http server
 ip http authentication aaa

```

```

no ip http secure-server
ip pim autorp listener
ip pim register-source Loopback0
ip route vrf IWAN-TRANSPORT-1 0.0.0.0 0.0.0.0 192.168.6.2
ip tacacs source-interface Loopback0
!
ip access-list standard DMVPN-1-SPOKES
  permit 10.6.34.0 0.0.1.255
!
no service-routing capabilities-manager
!
route-map BLOCK-DMVPN-2 deny 10
  description Do not advertise routes sourced from DMVPN-2
  match tag 10.6.36.0
!
route-map BLOCK-DMVPN-2 permit 100
!
route-map SET-TAG-DMVPN-1 permit 10
  description Tag routes sourced from DMVPN-1
  match ip route-source DMVPN-1-SPOKES
  set tag 10.6.34.0
!
route-map SET-TAG-DMVPN-1 permit 100
  description Advertise all other routes with no tag
!
route-map SET-TAG-ALL permit 10
  set tag 10.6.34.0
!
route-tag notation dotted-decimal
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp ifmib ifindex persist
!
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 15210E0F162F3F0F2D2A
!
!
!
control-plane
!
!
!
!
!
!

```

```

!
!
!
!
line con 0
  exec-timeout 0 0
  transport preferred none
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  exec-timeout 0 0
  transport preferred none
line vty 5 15
  exec-timeout 0 0
  transport preferred none
!
ntp source Loopback0
ntp server 10.4.48.17
!
!
end

```

VPN-MPLS-ASR1002X-1#

Remote-Site Router Configuration

```

RS42-4451X-1#sh run
Building configuration...

```

Current configuration : 17453 bytes

```

!
! Last configuration change at 13:56:44 PDT Mon Mar 16 2015 by jvogel
! NVRAM config last updated at 13:50:31 PDT Mon Mar 16 2015 by jvogel
!
version 15.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname RS42-4451X-1
!
boot-start-marker

```



```

ip domain name cisco.local
ip name-server 10.4.48.10

ip multicast-routing distributed
!
!
!
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
flow record Record-FNF-IWAN
  description Flexible NetFlow for IWAN Monitoring
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  match flow direction
  collect routing source as
  collect routing destination as
  collect routing next-hop address ipv4
  collect ipv4 dscp
  collect ipv4 id
  collect ipv4 source prefix
  collect ipv4 source mask
  collect ipv4 destination mask
  collect transport tcp flags
  collect interface output
  collect flow sampler
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect application name
!
!
flow exporter Export-FNF-LiveAction

```

```

description FNFv9 with LiveAction
destination 10.4.48.178
source Loopback0
transport udp 2055
option application-attributes
option interface-table
option application-table
!
!
flow monitor Monitor-FNF-IWAN
description IWAN Traffic Analysis
exporter Export-FNF-LiveAction
cache timeout inactive 10
cache timeout active 60
record Record-FNF-IWAN
!
!
domain iwan
vrf default
border
source-interface Loopback0
master local
password 7 0508571C22431F5B4A
collector 10.4.48.178 port 2055
master branch
source-interface Loopback0
password 7 141443180F0B7B7977
hub 10.6.32.251
collector 10.4.48.178 port 2055
!
!
!
!
key chain WAN-KEY
key 1
key-string 7 110A4816141D5A5E57
key chain LAN-KEY
key 1
key-string 7 011057175804575D72
!
!
crypto pki trustpoint TP-self-signed-714959929
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-714959929
revocation-check none
rsa-keypair TP-self-signed-714959929
!

```

```

crypto pki trustpoint IWAN-CA
  enrollment url http://10.6.24.11:80
  serial-number none
  fqdn RS4451X-1.cisco.local
  ip-address 10.255.241.42
  fingerprint 1A070F4338068E1CBE04A8FBCBAA406F
  revocation-check none
  rsakeypair IWAN-CA-KEYS 2048 2048
!
!
crypto pki certificate chain TP-self-signed-714959929
certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 37313439 35393932 39301E17 0D313431 30303730 33303734
  355A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3731 34393539
  39323930 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  998D5D57 D8DB2B08 68A1D6B4 D0AF4626 723CC17C 58C9B85B 3728058D D6ADDCDF
  6A66D612 BAB01C11 E89306F2 DE92B604 DF50C109 6C252FBA E6BAA09F 5376A188
  25829CEC 0D12F24B AB4EDF70 7232DF93 7210D4BD EE5CBF41 20A1053D F5A512B8
  86725D62 362522AB 0BD348D3 8B80D6D3 34386AA9 7D842024 B1912FC9 A00776F1
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 1680143B 32B67B88 1989FC7D CBB097C7 B416D6D1 BE269730 1D060355
  1D0E0416 04143B32 B67B8819 89FC7DCB B097C7B4 16D6D1BE 2697300D 06092A86
  4886F70D 01010505 00038181 008B9BF1 1E808F2A 0830D67C 5DDDE5B8 D2B57845
  0494DC2D DA402F63 DD646F9D AA467BCA 577B0EC2 A211C415 EA17E0EA 8345C823
  12AA5F99 779221ED A285455A F1CF13C6 7C7E996C D77F712D 3119ED75 74B281F8
  97BD599F 13AC152E C341A073 52B42CDE 0003C654 7F879CE2 5761143F BE4C2FC5
  A3D3AAC9 E40C6C0C 9B49F38A 9D
quit
crypto pki certificate chain IWAN-CA
certificate 07
  30820315 3082027E A0030201 02020107 300D0609 2A864886 F70D0101 05050030
  38313630 34060355 0403132D 4957414E 2D43412D 494E4554 2E636973 636F2E6C
  6F63616C 204C3D53 616E4A6F 73652053 743D4341 20433D55 53301E17 0D313431
  31313332 32353632 395A170D 32313131 31313232 35363239 5A304231 40301A06
  092A8648 86F70D01 0908130D 31302E32 35352E32 34312E34 32302206 092A8648
  86F70D01 09021615 52533434 3531582D 312E6369 73636F2E 6C6F6361 6C308201
  22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201 0100B9EB
  AEB9CE6E E5350968 E99538CB DAD2AE21 A8E8A7E8 60109EBB DF63E844 9FD50165
  2C69892E 83250800 06F5092C B80FFF52 35F33EB6 6A6FF9C5 94DA293B D26FEA2D
  BE3488A4 65D939DD 8CFF01FB BD3272AC 38F75224 BCE2D12F 524B4A0E F71129AD
  E3120FC0 D98F73EB CA860D60 9B985F3B 8738A73D CD1DF934 918DC0F2 F0B68A26
  CA31F2D2 7770B5BF D704A0EA A1E37EE7 741249A9 9FC5BB6B 0AEFE880 963B6009
  0DE72A89 0E0CF529 B71E0C49 D576D4FA 8EF80577 172A6507 00CECD14 AE06C21F
  BEC48E4F 00DABB89 1D0EC96A EDB3B9B5 C097F2C6 610DCB0B CB6545E2 96E0301B

```

```
C034BFB1 ABD3DA4B A496B412 ED20C30B C5E8DD9F BF6327AD B22B5251 52470203
010001A3 81A03081 9D304E06 03551D1F 04473045 3043A041 A03F863D 68747470
3A2F2F31 39322E31 36382E31 34342E31 32372F63 67692D62 696E2F70 6B69636C
69656E74 2E657865 3F6F7065 72617469 6F6E3D47 65744352 4C300B06 03551D0F
04040302 0520301F 0603551D 23041830 16801416 6769F5AE A467CBAB 43FC776E
F14A2E45 42553630 1D060355 1D0E0416 0414AD45 BD3A2C15 A2130CA7 F82DA3C7
552E9584 5754300D 06092A86 4886F70D 01010505 00038181 0073E83D 3AD96055
E21642DA 9E1F3BE1 71148777 3BE03D8E C571CA7B C86F15F4 40B1EB56 EF676DF9
D792A4B7 2968F800 6C8A5AD7 C345D7BB 3EB7D8B5 FFAB576E 56A80A76 21E9F297
DF6A5EC2 615D765E 0786F0CB F19E6D1B 53639AB1 B19A937C 0DB71A20 57109703
9E82AF9B 6C746790 EAEB5E7A 6CCC9049 27712AE4 86436472 61
```

quit

certificate 06

```
30820315 3082027E A0030201 02020106 300D0609 2A864886 F70D0101 05050030
38313630 34060355 0403132D 4957414E 2D43412D 494E4554 2E636973 636F2E6C
6F63616C 204C3D53 616E4A6F 73652053 743D4341 20433D55 53301E17 0D313431
31313332 32353631 325A170D 32313131 31313232 35363132 5A304231 40301A06
092A8648 86F70D01 0908130D 31302E32 35352E32 34312E34 32302206 092A8648
86F70D01 09021615 52533434 3531582D 312E6369 73636F2E 6C6F6361 6C308201
22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201 01009756
7E55A602 0C5A76EC 7ACD9EE0 B6830F74 48CA4E91 0AD88C05 CD6C37F7 39037F29
AFD5ED00 2E4C7D4A 8B45B6CA D669BD05 74868F9B A8A55609 0E710971 E7FB7EF5
9974A240 DC267E55 883F23DD 88985753 D50D2A18 26334C57 C23C0AC6 8838EF60
A5FBD821 3991C5FB F38C9540 651109FD 945D4170 2DB27559 CB8B9B29 AAAAE33F
3E091C9D EF56653A 76567DED 55986169 A4DF81D4 DBF6A61A 5E0CB7B3 EAACC714
7BAB5451 ED921D45 B7E6E6B3 50810D39 86388FCB 298C4BD9 02A043B1 A2E0762E
5FB40084 530D7F78 8E364E75 A7BA4F96 A0CB1BDA 7E975F7A 9A2CA1D0 28F49D3E
DCFF7273 4E068B32 0468E065 C157BB32 3E33E048 94756775 DEA4CC58 E7F10203
010001A3 81A03081 9D304E06 03551D1F 04473045 3043A041 A03F863D 68747470
3A2F2F31 39322E31 36382E31 34342E31 32372F63 67692D62 696E2F70 6B69636C
69656E74 2E657865 3F6F7065 72617469 6F6E3D47 65744352 4C300B06 03551D0F
04040302 0780301F 0603551D 23041830 16801416 6769F5AE A467CBAB 43FC776E
F14A2E45 42553630 1D060355 1D0E0416 041454BC 17CC63D8 87BF1792 15F935CF
21E2321D 2F18300D 06092A86 4886F70D 01010505 00038181 00241280 B1F19A72
55B32AB0 C4925099 BD8FE477 38035683 CED949E5 B096B00B 4040052E 890D3B9B
7B6A75FE 6131A716 958A3CAA 57256A3F D0508A5B 52CEDC38 22C2918B 7DC21DF4
2F4F0425 E9852B8D 8946F508 F4CA9E8A AA56395C 1161CA10 2CEF86A5 75E99AA1
A909CF34 F2FFA575 AD3D30ED BCAFB5F2 565C0526 5FAEF055 F5
```

quit

certificate ca 01

```
30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
38313630 34060355 0403132D 4957414E 2D43412D 494E4554 2E636973 636F2E6C
6F63616C 204C3D53 616E4A6F 73652053 743D4341 20433D55 53301E17 0D313431
31313131 38323835 375A170D 33343131 31313138 32383537 5A303831 36303406
03550403 132D4957 414E2D43 412D494E 45542E63 6973636F 2E6C6F63 616C204C
3D53616E 4A6F7365 2053743D 43412043 3D555330 819F300D 06092A86 4886F70D
01010105 0003818D 00308189 02818100 B744E800 9ABF4B06 64794FF3 48994B4E
```

```

6D15AFC8 ED2AAC6F DE5BBBD7 46C36EC1 F25992E1 EC36492A E9EBDC0B 519F8FA8
272BBD9B F959EA94 E6FEAF8E A64560A0 5FB664C3 B3332123 AA7D2096 323FD23F
69A27CE9 5C30E086 D99A6F5D 50462241 EAACC434 602FD776 A8578233 9EF93703
55E80203 A6D2198E E9B7D855 C9D6D139 02030100 01A36330 61300F06 03551D13
0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D
23041830 16801416 6769F5AE A467CBAB 43FC776E F14A2E45 42553630 1D060355
1D0E0416 04141667 69F5AEA4 67CBAB43 FC776EF1 4A2E4542 5536300D 06092A86
4886F70D 01010405 00038181 00282322 3EEDE811 D909B4D0 5298AF2B DD51B481
91F6F8B9 6E31E1B4 F3AC4E12 0F21BC1B FA8904C6 CC5A6975 FE6E3A61 CCF6209D
74053507 1478D641 8D944053 A72527F6 ACA7DD40 A76F3B5C D7D5E2A2 EF5E7786
6E2AF9BC 0CC46A99 FD5681C7 09D80B6D 2A0F82D2 9310F4EC F7D68BC8 D35F2B9F
EC98D695 11915941 54B58EA8 D8
quit
!
!
!
!
!
!
!
!
!
voice-card 0/4
no watchdog
!
license udi pid ISR4451-X/K9 sn FOC18293U7P
spanning-tree extend system-id
!
username admin secret 5 $1$SnKm$ibEw/1V702JMAMj/C/qzs.
!
redundancy
mode none
!
!
!
crypto ikev2 keyring DMVPN-KEYRING-1
peer ANY
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123
!
!
!
crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-1
match fvrf IWAN-TRANSPORT-1
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local DMVPN-KEYRING-1

```

```

!
crypto ikev2 dpd 40 5 on-demand
!
!
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 05080F1C2243
ip tftp source-interface GigabitEthernet0
ip ssh source-interface Loopback0
ip ssh version 2
ip scp server enable
!
class-map match-any STREAMING-VIDEO
  match dscp af31 af32 cs5
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41 af42
class-map match-any CRITICAL-DATA
  match dscp af11 af21
class-map match-any NET-CTRL-MGMT
  match dscp cs2 cs6
  match access-group name ISAKMP
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match dscp cs1
class-map match-any JABBER-VIDEO
  match access-group 101
class-map match-any JABBER-VOICE
  match access-group 100
class-map match-any CALL-SIGNALING
  match dscp cs3
class-map match-any JABBER-SIP
  match access-group 102
!
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af41
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af41
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6

```

```

class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af41
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  set dscp af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp af11
class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
class class-default
  bandwidth remaining percent 25
  random-detect
  set dscp default
policy-map WAN-INTERFACE-G0/0/0
  class class-default
    shape average 300000000
    service-policy WAN
policy-map Ingress-LAN-Mark
  class JABBER-VOICE
    set dscp af41
  class JABBER-VIDEO
    set dscp af41
  class JABBER-SIP
    set dscp cs3
!
!
!
!
!
!
!
!
!
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE-TRANSPORT-1
  set transform-set AES256/SHA/TRANSPORT
  set ikev2-profile FVRF-IKEv2-IWAN-TRANSPORT-1
!
!

```

```

!
!
!
!
!
!
!
interface Loopback0
 ip address 10.255.241.42 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 no ip address
 no negotiation auto
!
interface Port-channel1.50
 description Link to distribution layer
 encapsulation dot1Q 50
 ip address 10.7.208.1 255.255.255.252
 ip flow monitor Monitor-FNF-IWAN input
 ip flow monitor Monitor-FNF-IWAN output
 ip pim sparse-mode
 service-policy input Ingress-LAN-Mark
!
interface Port-channel1.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.7.208.9 255.255.255.252
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 300000
 ip address 10.6.34.42 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip flow monitor Monitor-FNF-IWAN input
 ip flow monitor Monitor-FNF-IWAN output
 ip pim dr-priority 0
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp group RS-GROUP-300MBPS
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.6.34.1 nbma 192.168.6.1 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip tcp adjust-mss 1360

```



```

if-state nhrp
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel key 101
tunnel vrf IWAN-TRANSPORT-1
tunnel protection ipsec profile DMVPN-PROFILE-TRANSPORT-1
!
interface VirtualPortGroup0
ip unnumbered Port-channel1.50
no mop enabled
no mop sysid
!
interface GigabitEthernet0/0/0
bandwidth 300000
vrf forwarding IWAN-TRANSPORT-1
ip address 192.168.6.33 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
negotiation auto
no mop enabled
no lldp transmit
no lldp receive
service-policy output WAN-INTERFACE-G0/0/0
!
interface GigabitEthernet0/0/1
no ip address
shutdown
negotiation auto
no cdp enable
!
interface GigabitEthernet0/0/2
no ip address
negotiation auto
channel-group 1
!
interface GigabitEthernet0/0/3
no ip address
negotiation auto
channel-group 1
!
interface Service-Engine0/4/0
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown

```

```

negotiation auto
!
!
router eigrp IWAN-EIGRP
!
address-family ipv4 unicast autonomous-system 400
!
af-interface default
  passive-interface
exit-af-interface
!
af-interface Tunnel10
  summary-address 10.7.208.0 255.255.248.0
  authentication mode md5
  authentication key-chain WAN-KEY
  hello-interval 20
  hold-time 60
  no passive-interface
exit-af-interface
!
af-interface Port-channel1.99
  authentication mode md5
  authentication key-chain WAN-KEY
  no passive-interface
exit-af-interface
!
af-interface Port-channel1.50
  authentication mode md5
  authentication key-chain LAN-KEY
  no passive-interface
exit-af-interface
!
topology base
  distribute-list route-map ROUTE-LIST out Tunnel10
exit-af-topology
network 10.6.34.0 0.0.1.255
network 10.7.0.0 0.0.255.255
network 10.255.0.0 0.0.255.255
eigrp router-id 10.255.241.42
eigrp stub connected summary redistributed leak-map STUB-LEAK-ALL
exit-address-family
!
!
virtual-service RS42_4451X_1_WAAS
  profile ISR-WAAS-1300
  vnic gateway VirtualPortGroup0
  activate

```

```

!
ip forward-protocol nd
no ip http server
ip http authentication local
ip http secure-server
ip http secure-trustpoint TP-self-signed-714959929
ip http client secure-trustpoint TP-self-signed-714959929
ip pim autorp listener
ip pim register-source Loopback0
ip route 10.7.208.13 255.255.255.255 VirtualPortGroup0
ip route vrf IWAN-TRANSPORT-1 0.0.0.0 0.0.0.0 192.168.6.34
ip tacacs source-interface Loopback0
!
!
ip access-list standard DEFAULT-ONLY
  permit 0.0.0.0
!
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
!
no service-routing capabilities-manager
access-list 67 permit 192.0.2.2
access-list 100 permit udp any range 3000 3999 any
access-list 101 permit udp any range 4000 4999 any
access-list 102 permit tcp any range 5060 5061 any
!
route-map STUB-LEAK-ALL permit 100
  description Leak all routes to neighbors
!
route-map ROUTE-LIST deny 10
  description Block readvertisement of learned WAN routes
  match tag 10.6.34.0 10.6.36.0
!
route-map ROUTE-LIST deny 20
  description Block advertisement of Local Internet Default route out to WAN
  match ip address DEFAULT-ONLY
!
route-map ROUTE-LIST permit 100
  description Advertise all other routes
!
route-tag notation dotted-decimal
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp ifmib ifindex persist
!
tacacs server TACACS-SERVER-1

```

```

address ipv4 10.4.48.15
key 7 15210E0F162F3F0F2D2A
!
!
!
control-plane
!
!
!
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
  transport preferred none
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  exec-timeout 0 0
  transport preferred none
  transport input ssh
line vty 5 15
  transport preferred none
  transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end

RS42-4451X-1#

```

Appendix E: Glossary

AAA authentication, authorization, and accounting

ACL access control list

ACS Cisco Secure Access Control System

ANCG Cisco Application Navigator controller group

AppNav Cisco Application Navigator

Cisco AppNav Cisco Application Navigator

Cisco WCM Cisco Wide Area Application Services Central Manager

Cisco FEX Cisco Fabric Extender

Cisco IWAN Cisco Intelligent WAN

Cisco Secure ACS Cisco Secure Access Control System

Cisco SRE Cisco Services-Ready Engine

Cisco WAAS Cisco Wide Area Application Services

Cisco WAASx Cisco Wide Area Application Services Express

Cisco WAVE Cisco Wide Area Virtualization Engine

DNS domain name system

FEX Cisco Fabric Extender

HTTPS secure HTTP

IWAN Cisco Intelligent WAN

LAN local-area network

NIC network interface card

NMS network-management system

NTP network time protocol

OVA open virtual appliance

QoS quality of service

SNMP simple network management protocol

SRE Cisco Services-Ready Engine

SSD solid-state drive

SSH secure shell protocol

SSL secure sockets layer

TLS transport layer security

vWAAS virtual Cisco Wide Area Application Services

WAAS Cisco Wide Area Application Services

WAASx Cisco Wide Area Application Services Express

WAN wide-area network

WAVE Cisco Wide Area Virtualization Engine

WCM Cisco Wide Area Application Services Central Manager

WN Cisco Wide Area Application Services node

WNG Cisco Wide Area Application Services node group

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. USERS 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.

© 2015 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)