Overview

This guide provides an overview of the ISR-WAAS and AppNav-XE component on Cisco ISR 4451-X in Cisco IOS-XE Release 3.9, and describes the quick start process to easily configure the features. It also provides details of the CLI commands along with examples and troubleshooting tips.

Overview of the WAAS Solution on Cisco ISR 4451-X

The WAAS solution for Cisco ISR 4451-X includes the following:

- ISR-WAAS: Virtualized WAAS in a Cisco IOS-XE container.
- AppNav Controller: Component that intelligently distributes traffic from a router to services.
- AppNav service node auto discovery feature: Feature that automatically discovers service nodes and adds them to an AppNav cluster. See the "About the AppNav Service Node Auto Discovery Feature" section on page 1-3.
- EZConfig: A CLI-based, simplified deployment of the AppNav-XE component and the ISR-WAAS solution on the Cisco ISR 4451-X.
- WAAS Central Manager (WCM): Used to monitor and configure the vWAAS application.

AppNav-XE Component Overview

The AppNav-XE component is made up of a distribution unit called the AppNav Controller and service nodes. The AppNav Controller distributes flows and the service nodes process the flows. Additionally up to four AppNav Controllers can be grouped together to form an AppNav Controller group to support asymmetric flows and high availability. Note that all the routers in the AppNav Controller group need to be the same platform and also have the same memory capacity.

Advantage of Using the AppNav-XE Component

The advantages of using the AppNav-XE component are:

- It can intelligently redirect new flows based on the load on each service node. This includes loads of individual L7 application accelerators.
- For flows that do not require any optimization, service nodes can inform the AppNav Controller to directly pass-through the packets, thereby minimizing the latency and resource utilization.
- There is no impact to traffic when adding or removing service nodes.
- The AppNav-XE component supports VRF so that VRF information is preserved when traffic returns from a service node.
- For special applications such as MAPI (Exchange) and VDI (Citrix), the AppNav-XE component ensures that flows from the same client and destined to the same server and server port are redirected to the same service node.
- You can use an AppNav Controller group to optimize asymmetric flows. An asymmetric flow is when the traffic in one direction goes through one AppNav Controller and the return traffic goes through a different AppNav Controller, but both AppNav Controllers redirect the traffic to the same service node.
- Inter-router high availability, where if one router goes down, traffic can be rerouted to a different router within the AppNav Controller group, keeping the traffic flows uninterrupted.

Interoperability of the AppNav-XE Component

The AppNav component can interoperate with the following features on the router:

- QoS
- NAT (Note that the video application accelerator is disabled and that asymmetric routing and inter-router high availability handled both by the AppNav-XE component and NAT is not supported.)
- AVC 2.0 (FNF, NBAR) (Note that AVC 2.0 does not support symmetric routing and inter-router high availability.)
- IPSec
- GET-VPN
- EzVPN
- DMVPN
- ACL
- VRF
- MPLS (The supported topology is an MPLS network on the WAN side and an IP network on the LAN side.)

- WCCP-AppNav-XE coexistence (WCCP and AppNav-XE can be configured on the same interface only if they act on different flows. Use ACLs for this. WCCP and AppNav XE can be configured on different interfaces—AppNav-XE on WAN and WCCP on LAN (supported on Cisco IOS-XE Release 3.10 and later.)
- PBR/PFR (supported on Cisco IOS-XE Release 3.10.1 and later)

The AppNav-XE component introduces the concept of a virtual interface, which allows users to configure features specific to compressed or uncompressed traffic. For instance, to monitor the traffic that is being redirected to the service node and the traffic that is returning from the service node, you can configure the FNF feature on the AppNav-UnCompress and AppNav-Compress virtual interfaces. Note that these AppNav-XE virtual interfaces appear to the user just as any other interface. However from the above list, the only features that work on the AppNav-XE virtual interfaces are FNF, ACL, and QoS (except for queueing).

About Configuring the AppNav-XE Component

Note the following points regarding configuring the AppNav-XE component:

- You must identify the WAN interfaces for the router that is running the AppNav Controller. The AppNav Controller intercepts packets on both ingress and egress of WAN interface. Only configure the AppNav Controller on WAN interfaces, including all WAN interfaces that will be load balancing.
- Do not use the VRF to access the service node from the AppNav Controller. Neither the service node nor the AppNav Controller IP address should have VRF on the AppNav Controller.
- You can use port channel between the AppNav Controller and the service nodes to increase AppNav Controller-service node bandwidth.
- The **config replace** command cannot be used with AppNav-XE configuration.
- If you use an AppNav Controller group with two or more AppNav Controllers, the AppNav-XE configuration on all the AppNav Controllers must be the same. This also means that the names of the AppNav policy maps and class maps on the AppNav Controllers need to match. Also the VRF names for the traffic seen by the AppNav-XE component need to be the same on all the AppNav Controllers.
- If AppNav-XE is managed by WCM, the authentication key in the service-context configuration cannot be modified using the command line interface (CLI).

For additional information and caveats about configuring the AppNav-XE component, see Chapter 3, “Detailed Configuration”.

About the AppNav Service Node Auto Discovery Feature

The AppNav service node auto discovery feature is targeted for small branch installations. With this feature, the system automatically discovers the service nodes within the same L2 connectivity of the AppNav router and adds them to the service node cluster.

Restriction

The AppNav service node auto discovery feature can only be enabled on one interface on a service node.

To enable the AppNav service node auto discovery feature, do the following:

Procedure

Step 1 Initiate a discovery request on the AppNav-XE component on the router by doing the following:

a. Determine the service node group for which you want to enable the auto discovery.

b. Issue the following commands:

```
router(config)# service-insertion service-node-group sng
router(config-service-insertion-sng)# node-discovery enable
```

Step 2 Initiate a service respond on the service nodes by doing the following:

a. On the WAAS appliance, determine the interface for which you want to enable node discovery. This interface must be in the same subnet as the AppNav Controller.

b. Enable node discovery by issuing the following commands:

```
auto-sn(config)# service-insertion service-node
auto-sn(config-sn)# node-discovery enable GigabitEthernet 0/1
auto-sn(config-sn)# enable
```

Container Overview

The term “container” refers to the KVM hypervisor that runs virtualized applications on the Cisco ISR 4451-X. The term “host” refers to the primary operating system running on a system. For ISR-WAAS on Cisco ISR 4451-X, the host is defined as a Cisco ISR 4451-X running on Cisco IOS XE Release 3.9.

The Virtualization Manager tasks vary depending on the phase of the virtual service deployment. Table 1-1 summarizes this information.

Table 1-1 Virtualization Manager Tasks

Phase	Trigger	Actions	Virtual Service Instance State
Pre-Installation		1. Gather and prepare system resources. 2. Establish internal communication infrastructures.	Host is ready to accept new virtual service.
Installation	Virtualization Manager received a request to install a virtual service package.	1. Unzip and unpack the virtual service definition from its OVA package. 2. Perform SHA2 code signing check using the artifacts in the OVA (.cert, .mf) and a hidden Cisco public key. 3. Validate the machine definition specified in the OVA and perform preliminary resource check (for warnings). 4. Parse the machine definition and create internal objects for manageability. 5. Process tiered resource profiles requests.	• Validated that package is Cisco signed. • Validated integrity of OVA content. • Validated and parsed machine definition and binds it to a virtual service “instance name”.
Configuration	Virtualization infrastructure received a request to configure an instance of the virtual service.	1. Perform validation and necessary network provisioning for configured guest IP address (if applicable). 2. Perform resource check and reservation for selected profile.	Virtual service is configured.
Activation	Virtualization infrastructure received a request to activate the virtual service.	1. Carve out storage resource from host system as needed. 2. Commit CPU, memory, storage, and networking resources as needed. 3. Update the machine definition XML and start the virtual machine. 4. Service to console, aux, logging and tracing ports as needed.	Virtual service is activated.
Post Activation		1. Perform monitoring services. 2. Process lifecycle control services.	

ISR-WAAS Overview

ISR-WAAS is a virtualized WAAS instance running on a Cisco IOS-XE container on a Cisco ISR 4451-X platform. ISR-WAAS provides WAN optimization functionality to the Cisco ISR 4451-X.

The Cisco ISR 4451-X does not support RAID.

ISR-WAAS can run on a Cisco ISR 4451-X router with these minimum requirements:

- 8 GB RAM
- 200 GB hard disk

The Cisco ISR 4451-X requires more resources depending on the ISR-WAAS profile that you install. See Table 1-2.

Table 1-2 Profile Specifications

	Profile Specifications				Router Requirements			
Profile Name	**Connections**	**RAM (GB)**	**Disk (GB)**	**vCPUs**	**RAM**	**# of 200 GB SSD disks**	**CF (GB)**	**Target WAN throughput**
ISR-WAAS-750	750	4	170	2	8	1	16	50 Mbps
ISR-WAAS-1300	1300	6	170	4	16	1	32	100 Mbps
ISR-WAAS-2500	2500	8	360	6	16	2	32	150 Mbps

Licensing Requirements

To deploy both the ISR-WAAS and the AppNav-XE component on the Cisco ISR 4451-X, use the appxk9 package license.

Procedure

Step 1 Enter the licensing command as follows:

```
router(config)# license boot level appxk9
router(config)# end
router# write mem
```

Step 2 Reload the router using the following command:

```
router# reload
```

Step 3 Enter the **show license detail** command as follows:

```
router# show license detail
```

Step 4 To verify that the license is enabled, review the output of the command. Verify that the appxk9 package license is active and in use. The output for “Feature: appxk9” should show “License State: Active, In Use”. Here is an example:

```
router# show license detail
Index 1: Feature: appxk9          Version 1.0
License Type: EvalRightToUse
License State: Active, In Use
    Evaluation total period: 8 weeks 4 days
```

```
    Evaluation period left: 7 weeks 6days
    Period used: 4 days 14 hours
    Transition date: Apr 15 2013 10:27:31
Lock type: Non Node locked
```

Recommendations to Upgrade/Downgrade the Cisco ISR 4461 Running WAAS Software

To upgrade/downgrade the Cisco 4461 ISR running WAAS software for different versions of Cisco IOS XE, Cisco recommends the following steps.

Note Cisco 4461 ISR supports ISR-WAAS installation only from WAAS 6.4.1b release.

For the Cisco 4461 running Cisco IOS XE Fujie 16.9.1 release, follow these steps:

Step 1 Install ISR-WAAS version 6.4.1b using the **service waas enable** command. The appropriate OVA file should be on the flash drive of the Cisco 4461 ISR.

Step 2 To upgrade from WAAS 6.4.1b to WAAS 6.4.3, use the bin image (copy ftp/http install) process using the CLI or Central Manager.

Step 3 To downgrade back to WAAS 6.4.1b, uninstall the current version using the **service waas disable** command and install a new image of WAAS using step 1 above.

Recommendations to Upgrade/Downgrade the Cisco ISR 4451-X Running WAAS Software

To upgrade/downgrade an ISR-4451-X running WAAS software for different versions of Cisco IOS XE, Cisco recommends the following steps.

For Cisco IOS-XE 3.9

For the Cisco ISR 4451-X running Cisco IOS-XE 3.9 release, follow these steps:

Step 1 Install ISR-WAAS version 5.2 using the **service waas enable** command. The appropriate OVA file should be on the flash drive of the Cisco ISR 4451-X.

Step 2 To upgrade from WAAS 5.2 to WAAS 5.3, use the bin image (copy ftp/http install) process using the CLI or Central Manager.

Step 3 To downgrade back to WAAS 5.2.1, uninstall the current version using the **service waas disable** command and install a new image of WAAS using step 1 above.

For Cisco IOS-XE 3.10

For the Cisco ISR 4451-X running Cisco IOS-XE 3.10 release, follow these steps:

Step 1 Install ISR-WAAS version 5.3 only. Do not downgrade IOS-XE to earlier versions.

Step 2 If IOS-XE 3.9 version is required, first uninstall WAAS 5.3 using the **service waas disable** command, then downgrade IOS-XE 3.10 to version 3.9.

Step 3 Enable WAAS 5.2 using the appropriate OVA file and the **service waas enable** command.