



Deploying Cisco IOx Applications, Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches

First Published: 2024-03-08

Last Modified: 2024-04-05

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE 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 THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit [Cisco DevNet](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CONTENTS

Full Cisco Trademarks with Software License iii

Communications, services, and additional information iv

Cisco Bug Search Tool iv

Documentation feedback iv

CHAPTER 1

Cisco IOx and Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches 1

Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches 1

Prerequisites 2

CHAPTER 2

Configuring the Network and IOx 3

Configuring the Network for IOx 3

Configure the VLAN ID for the IOx Interface 4

Enable IOx on the Switch 5

CHAPTER 3

Deploying IOx Applications 7

Prerequisites 7

Guidelines for IOx Applications 7

Limitations for IOx Applications 8

Methods of Deploying IOx Applications 8

Deploying IOx Applications Using the IOS-XE CLI 8

Configure an Application Using the CLI 9

Configure Docker Run-Time Options 11

Configure Application Resources 12

IOx Application Installation, Activation and Startup 13

Install, Activate, and Start the Application	13
IOX Application Sign Verification	15
IOx Application Command Examples	16
Deploy an Application using Cisco IOx Local Manager	18

CHAPTER 4	L3NAT for IOx Applications	21
	Overview	21
	L3NAT-IOx	21
	Guidelines and Restrictions	22
	Configuring L3NAT-IOx	22
	Displaying L3NAT-IOx information	24
	Feature History for L3NAT-IOx	24



CHAPTER 1

Cisco IOx and Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches

- [Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches](#), on page 1
- [Prerequisites](#), on page 2

Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches

Cisco IOx (IOS + Linux) is an end-to-end application framework that provides application-hosting capabilities for different application types on Cisco network platforms.

Cisco IOx combines Cisco IOS-XE with Linux OS for secure application hosting. IOx enables you to host applications in the networking infrastructure, and securely manage them using cisco app hosting tools.

IOx allows consistent deployment of applications that are independent of your network infrastructure and Docker tooling for development. It enables you to back up and restore application data, perform upgrades, and view troubleshooting logs.



Note See the [Cisco IOx page](#) on cisco.com for more information.

You can use Cisco IOx with a graphical UI on-premises or cloud-based management, or you can use an on-device CLI.

Since Cisco IOS XE Amsterdam 17.2.1, Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches support IOx application hosting. This allows you to run your own custom code, applications, and containers on the Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches.

This document describes how to deploy, activate and start an IOx application on Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches.

Prerequisites

We recommend that you have knowledge of the following subjects:

- Cisco IOx and Cisco IOS XE Amsterdam 17.2.1 or later
- Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches see [Limitations for IOx Applications](#) for the exact models.



CHAPTER 2

Configuring the Network and IOx

- [Configuring the Network for IOx, on page 3](#)
- [Enable IOx on the Switch, on page 5](#)

Configuring the Network for IOx

Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches have an additional interface for connectivity to the IOx applications, called Ap1/1. You can configure the Ap1/1 interface as a regular, physical, interface in trunk mode.

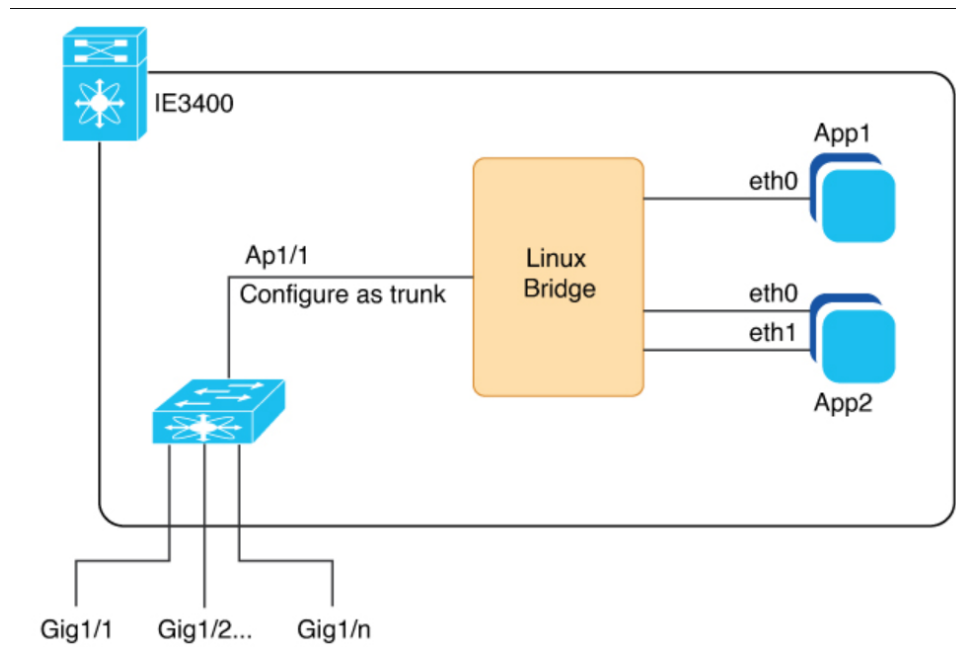
Prerequisites for Establishing a Connection Between Switch and Cisco IOx Applications

- Configure a VLAN ID for the Ap1/1 interface, regardless of trunk mode.
 - Ensure that the configured VLAN is not the default VLAN. By default, VLAN 1 serves as the native VLAN and carries untagged packets.
- Assign an IP address to a VLAN interface that is also a member of the Ap1/1 trunk interface.

The allowed VLANs on the Ap1/1 trunk interface should match the VLANs that need to carry data traffic to or from applications on IOx. These VLANs include ones carrying management traffic. The example used in this guide is 10. VLAN 10 is the VLAN carrying traffic for the application to communicate with the network. This traffic can include the IP traffic to the management VLAN. You should configure the same VLAN ID when managing the applications so the VLANs match. If you intend to use vlan 1 to communicate with the network, then choose a different native VLAN on Ap1/1.

After you configure the network, you must enable IOx on the switch.

Figure 1: Connections with IE3400 IOx Network with Applications



The preceding illustration shows Ethernet and Layer 2 connections possible in an IOx network on a Cisco Catalyst IE3400 Rugged Series Switch. The dedicated interface AppGigabitEthernet1/1 for IOx support is internally connected to a Linux bridge. The interface needs to be configured as a trunk. You can have multiple applications in an IOx network, each of which can have multiple Ethernet connections and can be placed in any VLAN.

For a similar illustration showing a sample network configuration, see the section [Deploying IOx Applications Using the IOS-XE CLI, on page 8](#) in this guide.

Configure the VLAN ID for the IOx Interface

You must configure the VLAN ID for the IOx interface and then configure the SVI address for the VLAN. You do so to connect to and manage the VLAN. You must make sure that the VLAN is routable throughout the network.

SUMMARY STEPS

1. Configure a VLAN ID for the IOx interface.
2. Configure the SVI address for the vlan.

DETAILED STEPS

Procedure

Step 1 Configure a VLAN ID for the IOx interface.

Enter the following command:

Example:

```
ie3400#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ie3400(config)#interface Ap1/1
ie3400(config-if)#switchport trunk allowed vlan 10
ie3400(config-if)#switchport mode trunk
ie3400(config-if)#end
```

Step 2 Configure the SVI address for the vlan.

Example:

```
ie3400#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ie3400(config)#interface vlan 10
ie3400(config-if)#ip address 192.168.0.1 255.255.255.0
ie3400(config-if)#end
```

Enable IOx on the Switch

After you configure the VLAN for the IOx interface, you must enable IOx on the switch.



Note Cisco IOS requires at least 1 GB on the SD card. If you have a 4 GB SD card partition for IOx, the default partition size for IOx 70 percent.

Before you begin

Before enabling IOx on the switch, ensure that you have an SD card for IOx with at least 4GB. An SD card is required by IOx for storage.

SUMMARY STEPS

1. Ensure that the SD card IOx partition are formatted with the EXT4 filesystem using CLI using the following command: **partition sdflash: iox**
2. Enable IOx:
3. Ensure that the web server is enabled and that a user is configured for access:
4. Leave configuration mode and enter enable mode:

DETAILED STEPS**Procedure**

Step 1 Ensure that the SD card IOx partition are formatted with the EXT4 filesystem using CLI using the following command:
partition sdflash: iox

The SD card is required to store the IOx applications and data.

Example:

```
Switch# partition sdflash: iox
Partitioning IOS:IOX(30%:70%) Default
Please make sure to back-up "sdflash:" contents
Partition operation will destroy all data in "sdflash:". Continue?[confirm]
```

Note

The default behavior of the partition command is to allocate 70 percent of the 4 GB on the SD Card to IOx.

Step 2 Enable IOx:**Example:**

```
ie3400#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ie3400(config)#iox
Warning: Do not remove SD flash card when IOx is enabled or errors on SD device could occur.
*Feb 21 12:49:18.310: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been notified
to start
*Feb 21 12:49:48.165: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
```

Step 3 Ensure that the web server is enabled and that a user is configured for access:**Example:**

```
ie3400#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ie3400(config)#ip http secure-server
ie3400(config)#username admin privilege 15 password 0 secret
```

This step is required to get access to the IOx functionality through the Local Manager UI.

Step 4 Leave configuration mode and enter enable mode:**Example:**

```
ie3400#end
```

What to do next

Check whether the IOx infrastructure is ready to use, as shown in the following example:

```
IE3400-2-2006#show iox-service

IOx Infrastructure Summary:
-----
IOx service (CAF) : Running
IOx service (HA) : Running
IOx service (IOxman) : Running
IOx service (Sec storage) : Running
Libvirttd 5.5.0 : Running
Dockerd v19.03.13-ce : Running
```



CHAPTER 3

Deploying IOx Applications

- [Prerequisites, on page 7](#)
- [Guidelines for IOx Applications, on page 7](#)
- [Limitations for IOx Applications, on page 8](#)
- [Methods of Deploying IOx Applications, on page 8](#)
- [Deploying IOx Applications Using the IOS-XE CLI, on page 8](#)
- [Deploy an Application using Cisco IOx Local Manager, on page 18](#)

Prerequisites

Ensure that you have completed the tasks in the chapter [Configuring the Network and IOx, on page 3](#) in this guide.

Guidelines for IOx Applications

This section provides guidelines for deploying IOx applications.

One of the most commonly used applications is Cisco Cyber Vision. See the [Cisco Cyber Vision](#) support page for more information.

Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches support both LXC and Docker based applications with ARM64 architecture.

Both IPv4 and Ipv6 configurations are supported.

Place the application package or tar file in the flash or SD card in the IOS partition for configuring with the CLI.

Use the application Gigabit Ethernet interface (AppGig1/1) on the switch for forwarding the Layer 2 application traffic. Ensure that the interface is up on the switch and configured for a trunk port.

When configuring applications:

- Configure Layer 2 interfaces with Ap1/1 and VLAN with an IP address in same VLAN network.
- Configure gateway interfaces for IOx applications to an SVI or IP address in same network.

You can configure multiple guest or Layer 2 interfaces [0-63] for an application, and each interface can be placed in a different VLAN.

You can configure up to three gateway interfaces.

IOx infra supports configuring multiple gateways; you can configure one default gateway to support all the interfaces.

The application configuration allows options to configure Docker runtime options.

Limitations for IOx Applications

This section provides limitations for IOx applications:

- Cisco IOx applications support IE3400/H, IE3300-8U2X, and IE3300-8T2X platforms.
- The CCV sensor support on IE3300-8T2S and IE3300-8P2S is limited to hardware version 6 or later. Check the output of the `show version` command to see the hardware version.

Methods of Deploying IOx Applications

There are two methods of deploying IOx applications to a Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches:

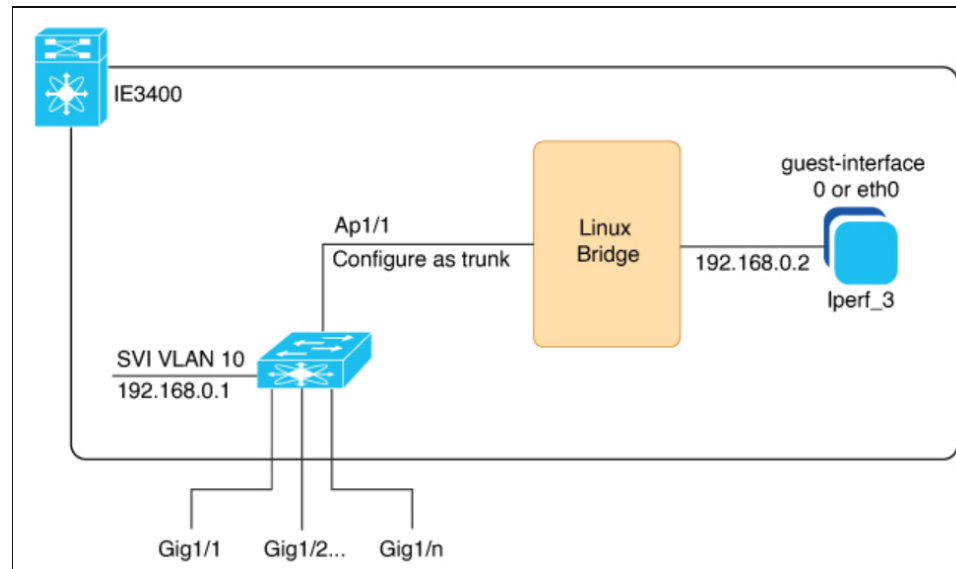
- **IOS-XE CLI:** The CLI that is part of the switch software for connecting to the switch on the device.
You can use the CLI on an IOx-enabled device to manage the device and deploy applications. You do not need to enable the web server on the IOS-XE device.
For more information, see [Deploying IOx Applications Using the IOS-XE CLI, on page 8](#).
- **Cisco IOx Local Manager (GUI):** A platform-specific application that is installed on a host system as part of the installation of the Cisco IOx framework on that device.
You can access Cisco IOx Local Manager from the Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches web-based user interface.
For more information, see [Deploy an Application using Cisco IOx Local Manager, on page 18](#).
- Cisco IOx Local Manager provides resource profiles, such as tiny, exclusive, default and custom. If you choose a custom profile, you can modify CPU, memory and disk values. See [Methods of Deploying IOx Applications, on page 8](#) and [Deploy an Application using Cisco IOx Local Manager, on page 18](#).

The following sections in this document contain instructions for deploying IOx using each method.

Deploying IOx Applications Using the IOS-XE CLI

To deploy IOx applications using the IOS-XE CLI, you need to configure the application and then install, activate, and start it.

Figure 2: Example of IOx Deployment with Application



The preceding illustration shows an example configuration of an IOx network on a Cisco Catalyst IE3400 Rugged Series Switch. The dedicated interface AppGigabitEthernet1/1 for IOx support is configured as a trunk and is internally connected to a Linux bridge. In the example, a single application, Iperf_3, is assigned the IP address 192.168.0.2 to the guest interface. The default gateway is assigned on SVI LAN 10 with the IP address of 192.168.0.1. For an illustration without interface examples, see the section [Configuring the Network and IOx, on page 3](#) in this guide.

Configure an Application Using the CLI

Enter the commands in the following procedure to configure an application using the IOS-XE CLI.



Note The following procedure describes how to install and run the iPerf application.

Before you begin

- You must have configured the network for IOx. See the section [Configuring the Network for IOx, on page 3](#).

SUMMARY STEPS

- enable**
- configure terminal**
- app-hosting appid iperf_3**
- app-vnic AppGigabitEthernet trunk**
- vlan 10 guest-interface 0**
- guest-ipaddress *guest_ip_address* netmask|prefix *number***
- exit**

8. **exit**
9. **app-default-gateway** *default_gateway_address* **guest-interface** *guest_interface number*
10. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: switch#enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: switch#configure terminal	Enters global configuration mode.
Step 3	app-hosting appid iperf_3 Example: switch(config)#app-hosting appid iperf_3	Configures an application name and enters application-hosting configuration mode.
Step 4	app-vnic AppGigabitEthernet trunk Example: switch(config-app-hosting)#app-vnic AppGigabitEthernet trunk	Configures AppGigabitEthernet trunk and enters application-hosting trunk-configuration mode.
Step 5	vlan 10 guest-interface 0 Example: switch(config-config-app-hosting-trunk)#vlan 10 guest-interface 0	Configures a VLAN guest interface and enters application-hosting VLAN-access IP configuration mode. The configuration places Eth0 into vlan 10.
Step 6	guest-ipaddress <i>guest_ip_address</i> netmask prefix number Example: <ul style="list-style-type: none"> • IPv4 (config-config-app-hosting-vlan-access-ip)# guest-ipaddress 192.168.0.2 netmask 255.255.255.0 • IPv6 (config-config-app-hosting-vlan-access-ip)# guest-ipv6address 2001::1 prefix 64 	Configures a static IP address. The subnet for this IP address on the VLAN (in this example <code>vlan 10</code>) must match the subnet configured for the IP address assigned to <code>vlan 10</code> interface. See the preceding examples.
Step 7	exit Example: switch(config-config-app-hosting-vlan-access-ip)#exit	Exits submode.

	Command or Action	Purpose
Step 8	exit Example: <code>switch(config-config-app-hosting-trunk)#exit</code>	You must enter exit again because of the nested submodes.
Step 9	app-default-gateway <i>default_gateway_address</i> guest-interface <i>guest_interface number</i> Example: <code>switch(config-app-hosting)#app-default-gateway 192.168.0.1 guest-interface 0</code>	Configures the default gateway for the application. The VLAN ID interface of the switch is used as the gateway. Note No more than three gateways are supported.
Step 10	end Example: <code>switch(config-app-hosting)#end</code>	Ends the session.

Configure Docker Run-Time Options

You can add a maximum of 30 lines of run time options. The system generates a concatenated string from line 1 through line 30. A string can have more than one Docker run time option.

When a run time option changes, do the following: Stop, deactivate, activate, and then start the application for the new run time options to take effect.

Before you begin

SUMMARY STEPS

1. **app-hosting appid iperf_3**
2. **app-resource docker**
3. **run-opts 1 "--entrypoint '/bin/sleep 10000'"**
4. **exit**
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	app-hosting appid iperf_3 Example: <code>switch(config)#app-hosting appid iperf_3</code>	Configures an application name and enters application-hosting configuration mode.
Step 2	app-resource docker Example: <code>switch(config-app-hosting)#app-resource docker</code>	Enters application-hosting docker-configuration mode.

	Command or Action	Purpose
Step 3	run-opts 1 "--entrypoint '/bin/sleep 10000'" Example: switch(config-app-hosting-docker)#run-opts 1 "--entrypoint '/bin/sleep 10000'"	Specifies the Docker run time options.
Step 4	exit Example: switch(config-app-hosting-docker)#exit	Exits application-hosting docker-configuration mode.
Step 5	end Example: switch(config-app-hosting)#end	Ends session.

Configure Application Resources

Complete the following steps to activate application hosting, which is required before resource changes take effect.

Before you begin

Check memory and storage using the command **show app-hosting resource**.

SUMMARY STEPS

1. **app-hosting appid iperf_3**
2. **app-resource profile custom**
3. **cpu value**
4. **memory value**
5. **persist-disk value**
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	app-hosting appid iperf_3 Example: switch(config)#app-hosting appid iperf_3	Configures an application name and enters application-hosting configuration mode.
Step 2	app-resource profile custom Example: switch(config-app-hosting)#app-resource profile custom	Configures the custom application resource profile, and enters custom application resource profile configuration mode. Note

	Command or Action	Purpose
		Only the custom profile name is supported.
Step 3	cpu value Example: <code>switch(config-app-resource-profile-custom)#cpu 500</code>	Configures CPU units.
Step 4	memory value Example: <code>switch(config-app-resource-profile-custom)#memory 256</code>	Configures memory in megabytes.
Step 5	persist-disk value Example: <code>switch(config-app-resource-profile-custom)#persist-disk 256</code>	Configures disk space in megabytes.
Step 6	end Example: <code>switch(config-app-resource-profile-custom)#end</code>	Ends the session.

IOx Application Installation, Activation and Startup

After you configure an application in the IOS-XE CLI, you activate the application by taking it through three states.

You first install the application using the `app-hosting install` command, which after installation, the application moves to the deployed state. During installation, the sign verification of the application is checked, if the check is enabled. For more information, see the section [IOX Application Sign Verification, on page 15](#).

After installation, you activate the application using the `app-hosting activate` command. During activation, the application is assigned resources on the switch; activation fails if there are not enough resources available.

After activation, you move the application to the running state using the `app-hosting start` command. During start, the application interfaces are created and assigned IP addresses.



Note You can check the state of the application at any point of installation, activation, or start by using the `show app-hosting list` command. You can use the `show app-hosting details` command to see a description of the application with IP allocation, resource allocation, and other details.

Install, Activate, and Start the Application

Complete the following commands to install, activate, and start the IOx application on the switch and to configure the interfaces.

Before you begin

You must have configured the network and the IOx application. See the section [Configuring the Network and IOx, on page 3](#).

SUMMARY STEPS

1. **app-hosting install appid** *application_name* **package** *application_filename*
2. (Optional) Confirm the application's installation and state by entering the `show app-hosting list` command:
3. **app-hosting activate appid** *application_name*
4. **app-hosting start appid** *application_name*

DETAILED STEPS**Procedure****Step 1** **app-hosting install appid** *application_name* **package** *application_filename***Example:**

```
IE3400-2-2006#app-hosting install appid iperf_3 package flash:iperf_3_eft_dockerimage_aarch.tar
```

Installing package 'flash:iperf_3_eft_dockerimage_aarch.tar' for 'iperf_3'. Use 'show app-hosting list' for progress.

```
IE3400-2-2006#show app-hosting list
App id State
-----
```

```
iperf_3 INSTALLING
```

```
IE3400-2-2006#
```

```
Oct 12 21:51:58.285: %IOXCAF-6-INSTALL_MSG: Switch 1 R0/0: ioxman: app-hosting: iperf_3 installed successfully Current state is DEPLOYED
```

```
IE3400-2-2006#show app-hosting list
```

```
App id State
-----
```

```
iperf_3 DEPLOYED
```

Installs the application and moves it into the deployed state.

Step 2 (Optional) Confirm the application's installation and state by entering the `show app-hosting list` command:**Example:**

```
switch #sh app-hosting list
```

```
App id State
-----
```

```
iperf_3 DEPLOYED
```

Step 3 **app-hosting activate appid** *application_name***Example:**

```
switch# app-hosting activate appid iperf_3
```

```
Current state is: ACTIVATED
```

Activates the application and assigns it switch resources.

Step 4 `app-hosting start appid application_name`

Example:

```
switch# app-hosting start appid iperf_3
iperf_3 started successfully
Current state is: RUNNING
```

IOX Application Sign Verification

You can check sign verification of a Cisco IOx application during its installation. Application package signature ensures that an application package is valid and that the one installed on the device comes from a trusted source.

The configuration keyword `start` is available under application-hosting application configurations. If you use this keyword, then IOx infra automatically activates and starts the application after installation. Otherwise, you must explicitly use `and activate` and `start` CLI commands to start the application.

IOx infra checks for a signature in the following cases:

- When signature verification is enabled.
- When IOx infra uses bootflash as storage; it then checks for a signature regardless of signature verification status.
- If an application is using a restricted resource, such as secure storage.

If signature verification is enabled, and the application is not signed, the application will not be allowed to install, activate or start.

However you cannot run non-Cisco applications if signature verification is enabled. However, you can run unsigned non-Cisco applications if the following criteria are met:

- Signature verification is disabled.
- An SD card is used for storage instead of boot flash.
- The application is not using a restricted resource.

Use the `app-hosting verification enable` command to enable sign verification and the `app-hosting verification disable` command to disable sign verification.

You can see whether signature verification is enabled by entering the command `show app-hosting infra`.

```
switch# show app-hosting infra
IOX version: 2.11.0.0
App signature verification: enabled
CAF Health: Stable
Internal working directory: /flash11/iox

Application Interface Mapping
AppGigabitEthernet Port # Interface Name Port Type Bandwidth
1 VirtEth KR Port - Internal 1G

CPU:
```

```
Quota: 33(Percentage)
Available: 0(Percentage)
Quota: 1400(Units)
Available: 0(Units)
```

```
switch#
```



Note You can enable or disable sign verification at any time regardless of any installed application states.

IOx Application Command Examples

This section provides examples of IOS-XE CLI commands for IOx applications.

View Resources on the Switch

The command in the following example shows the maximum resources and available resources on the switch for all iox applications:

```
switch# show app-hosting resource
CPU:
Quota: 33(Percentage)
Available: 0(Percentage)
VCPUs:
Count: 2
Memory:
Quota: 1248(MB)
Available: 0(MB)
Storage space:
Total: 2548(MB)
Available: 268(MB)
```

The command in the following example shows the CPU quota in units, whether app signature verification is enabled on the switch for IOx:

```
switch# show app-hosting infra
IOX version: 2.11.0.0
App signature verification: enabled
CAF Health: Stable
Internal working directory: /flash11/iox

Application Interface Mapping
AppGigabitEthernet Port # Interface Name Port Type Bandwidth
1 VirtEth KR Port - Internal 1G

CPU:
Quota: 33(Percentage)
Available: 0(Percentage)
Quota: 1400(Units)
Available: 0(Units)
```

View IOx Application Information on the Switch

The command in the following example shows application-related information on the switch:

```
switch #show app-hosting list
App id                               State
```

```
-----
iperf_3                                RUNNING
```

The command in the following example shows detailed application-related information on the switch:

```
switch# sh app-hosting detail appid iperf_3
App id           : iperf_3
Owner            : iox
State            : RUNNING
Application
  Type           : docker
  Name            : networkstatic/iperf_3
  Version        : latest
  Description     :
  Author         : Brent Salisbury <brent.salisbury@gmail.com>
  Path           : bootflash:iperf_3x86.tar
  URL Path       :
Activated profile name : custom

Resource reservation
  Memory         : 500 MB
  Disk           : 500 MB
  CPU            : 173 units
  CPU-percent    : 5 %
  VCPU          : 1

Platform resource profiles
  Profile Name   CPU(unit)  Memory(MB)  Disk(MB)
-----
Attached devices
  Type           Name           Alias
-----
  serial/shell   iox_console_shell  serial0
  serial/aux     iox_console_aux    serial1
  serial/syslog  iox_syslog         serial2
  serial/trace   iox_trace          serial3

Network interfaces
-----
eth0:
  MAC address    : 52:54:dd:67:81:6f
  IPv6 address   : ::
  Network name   : mgmt-bridge300
eth3:
  MAC address    : 52:54:dd:b2:4d:86
  IPv4 address   : 20.1.2.2
  IPv6 address   : ::
  Network name   : VPG0
eth1:
  MAC address    : 52:54:dd:f2:29:67
  IPv4 address   : 10.1.1.2
  IPv6 address   : 2001:1::5054:ddff:fef2:2967
  Network name   : mgmt-bridge-v2340

Docker
-----
Run-time information
  Command       :
  Entry-point    : /bin/sleep 10000
  Run options in use : --entrypoint '/bin/sleep 10000'
  Package run options :
Application health information
  Status        : 0
```

```
Last probe error      :
Last probe output    :
```

```
switch#
```

Stopping, Deactivating, and Uninstalling the Application

The command in the following example stops the IOx application:

```
switch# app-hosting stop appid iperf_3
iperf_3 stopped successfully
Current state is: STOPPED
switch#
```

The command in the following example stops the IOx application:

```
switch# app-hosting deactivate appid iperf_3
iperf_3 deactivated successfully
Current state is: DEPLOYED
switch#
```

The command in the following example stops the IOx application:

```
switch#
ie3400#app-hosting uninstall appid iperf_3
Uninstalling 'iperf_3'. Use 'show app-hosting list' for progress.
switch#
```

The following shows the list of app-hosting commands:

```
switch# app-hosting ?
  activate      Application activate      <== to activate app
  clear         Clear console/aux connection  <== to clear console or aux session if
connected
  connect       Application connect      <== to connect the app console or aux or session
once in run state
  data          Application data          <== to upload files to the apps
  deactivate    Application deactivate    <== to deactivate an app
  debug         debug                   <== for caf related debug commands
  install       Application install      <== to install app
  move          Move File                <== to move trace or core file
  settings      Application settings     <== to configure app specific setting using file
  start         Application start        <== to start an app
  stop          Application stop         <== to stop an app
  uninstall     Application uninstall    <== to uninstall an app`
  upgrade       Application upgrade      <== to upgrade app to new version
  verification  Application signature verification setting (global) <== to enable/disable
the sign verification
```

Deploy an Application using Cisco IOx Local Manager

Cisco IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot applications on a host system, and to perform various related activities. You can access Cisco IOx Local Manager from the Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches web-based user interface and use Cisco IOx Local Manager to deploy applications.

To access Cisco IOx Local Manager, choose **Configuration > IOx (IOx appears under Services)**. In the Cisco IOx Local Manager log in window that appears, enter the user name and password that you use to log in to Cisco IOS, then click **Log In**.

For detailed information about Cisco IOx Local Manager, including how to add, deploy, activate, start, and stop applications, see [Cisco IOx Local Manager Reference Guide](#).



CHAPTER 4

L3NAT for IOx Applications

- [Overview, on page 21](#)
- [L3NAT-IOx, on page 21](#)
- [Guidelines and Restrictions, on page 22](#)
- [Configuring L3NAT-IOx, on page 22](#)
- [Displaying L3NAT-IOx information, on page 24](#)
- [Feature History for L3NAT-IOx, on page 24](#)

Overview

In industrial networking environments, efficient communication between internal applications and external servers is essential for seamless operations. However, the requirement for each application to have a public routable IP address, in addition to the IP address for switch management, poses challenges for network administrators. This additional overhead and the need for multiple routable IP addresses for Industrial Ethernet (IE) devices act as barriers to the widespread adoption of application hosting solutions.

To address these challenges, the Layer3 Network Address Translation (L3NAT) for IOx applications is supported for IOx applications starting with IOS XE release 17.14.1. This feature uses the management IP of the switch as a proxy for all applications within the routed network. The complexity and overhead associated with managing multiple public IP addresses is reduced. The IE3x00 platform supports the L3NAT feature with the Cisco Cyber Vision (CCV) IOx application. It cannot be used to NAT other Ethernet traffic from hosts connected to its physical Ethernet ports.

L3NAT-IOx

L3NAT is a networking technique used to translate private IP addresses in an internal network to a public IP address before packets are sent to an external network at the network layer of the OSI model. The L3NAT-IOx feature utilizes hardware components such as Application-Specific Integrated Circuit (ASIC) and Field-Programmable Gate Array (FPGA) for implementation.

When a Cyber Sensor application communicates with the external CCV server, the NAT protocol translates the source private IP address of the Cyber Sensor application to the public IP address of the Management Switched Virtual Interface (SVI) of the switch. This translation allows the packets to navigate through the external network, giving the impression that they originate from the switch management SVI IP address.

When the external CCV server communicates to the Cyber Sensor application, the NAT protocol reverses the translation. The incoming packets that are addressed to the public IP address of the switch management SVI

are translated to the private IP address of the destination Cyber Sensor application. This ensures seamless communication between the application and external servers.

Guidelines and Restrictions

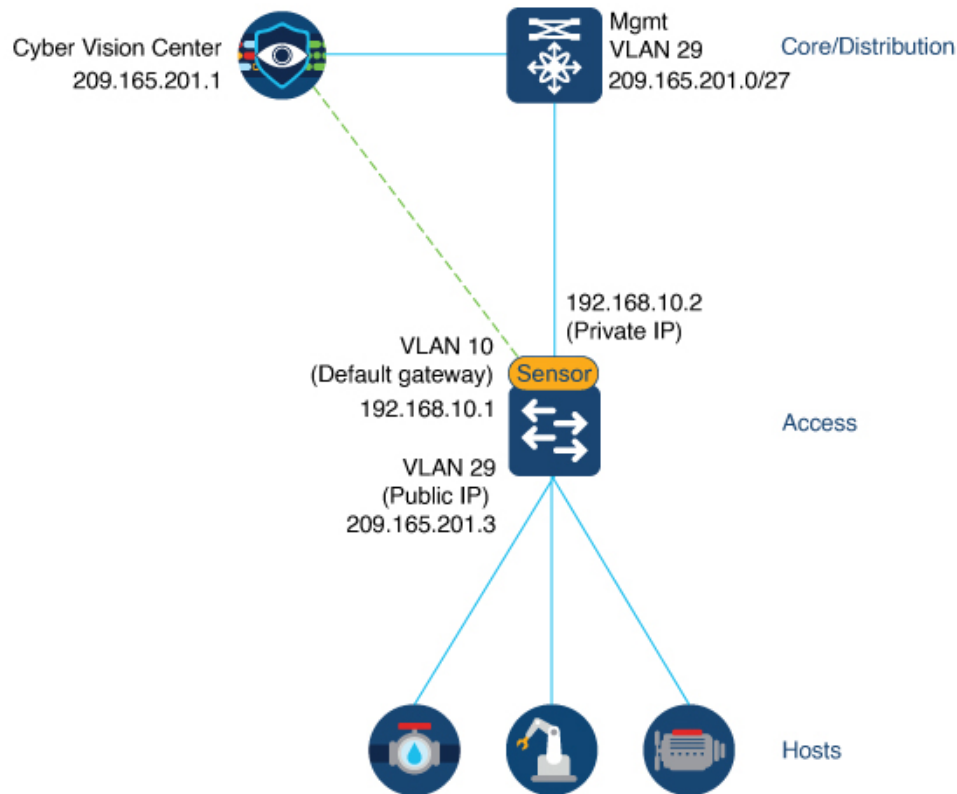
The guidelines and restrictions for L3NAT-IOx are as follows:

- The feature supports only CCV application, not supported for any other IOx application.
- Only static translation is supported.
- Translation is limited to TCP and UDP packets only.
- Users must create an additional SVI on IE for the private network used by the application. The IP assigned to the SVI will serve as the default gateway for the application.
- This feature requires a Network Advantage license.
- The L3NAT-IOx statistics cannot be fetched using YANG with Network Configuration Protocol (NETCONF).

Configuring L3NAT-IOx

The configuration example is based on the following topology:

Figure 3: CCV Onboarding



The above figure shows application hosting on the switch using a Private IP address. The CCV sensor application is installed on the access devices to which hosts are connected. The management public IP address is given to the devices located in the 209.165.201.0/27 network. CCV sensor is installed using the private IP network 192.168.10.x.

Procedure

Step 1 Create the SVI for the 192.168.10.x network with an IP address that serves as the default gateway for the application.

```
Switch(config)# int vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.224
```

Step 2 Create the SVI for the 209.165.201.0/27 network with an IP address that serves as the public IP to reach CCV center.

```
Switch(config)# int vlan 29
Switch(config-if)# ip address 209.165.201.3 255.255.255.224
```

Step 3 Configure the L3NAT-IOx.

```
Switch# configure terminal
Switch(config)# l3nat-iox
Switch(config-iox-nat)# app-ip 192.168.10.2 svi-ip 209.165.201.3 app-name CCV-ONPREM server-ip
209.165.201.1
```

Displaying L3NAT-IOx information

Procedure

To view NAT statistics, use the following command:

- The statistics show the translated IP addresses and the count of egress and ingress translations between the private application IP address and local SVI IP address.

```
Switch#show ioxnat statistics
TRANSLATED STATS for CCV-ONPREM (IN PACKETS)
=====
DIRECTION SA/DA ORIGINAL IP      TRANSLATED IP    COUNT
-----
EGRESS    SA   192.168.10.2    209.165.201.5   107
INGRESS   DA   209.165.201.5  192.168.10.2    91
```

- When the configuration fails, the following show command output is displayed.

```
Switch#show ioxnat statistics
ERROR STATS for (IN PACKETS)
=====
EGRESS OVERFLOW STATS      0
EGRESS CRC ERROR STATS     0
INGRESS OVERFLOW STATS     0
INGRESS CRC ERROR STATS    0
```

Feature History for L3NAT-IOx

Feature Name	Release	Description
L3NAT for IOx Applications	Cisco IOS XE 17.14.1	Initial support on IE3300, and IE3400/IE3400H series switches