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

Cisco Catalyst IE3300 Rugged Series
Updated April 5, 2024

Topics included

1 Cisco IOx Network Infrastructure Products....4
Cisco IOx network infrastructure....5

2 IOx Applications....6
IOx applications....7
Guidelines for IOx application....7
How to provide connections to IOx applications....7
Configure VLAN ID for IOx interface....8
Enable IOx....10

3 Deploy IOx Applications....12
Prerequisites....13
Guidelines and limitations for IOx applications....13
Deploy IOx applications....13
Deploy an application using Cisco IOx Local Manager....14
Deploying IOx applications using the IOS-XE CLI....14

4 L3NAT for IOx Applications....26
L3NAT in industrial networking....27
L3NAT-IOx....27
Guidelines and restrictions....27
Configure L3NAT-IOx....28
Feature history for L3NAT-IOx....29

1 Cisco IOx Network Infrastructure Products

Topics:

- Cisco IOx network infrastructure

Cisco IOx network infrastructure

Learn how Cisco IOx combines Cisco IOS XE and Linux to securely host and manage applications and containers on supported industrial Ethernet 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. Refer to 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. For each Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches, models and information, refer to Guidelines and limitations for IOx applications on page 13

2 IOx Applications

Topics:

- IOx applications
- Guidelines for IOx application
- How to provide connections to IOx applications
- Configure VLAN ID for IOx interface
- Enable IOx

IOx applications

This topic explains the Ap1/1 interface on Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches, which provides connectivity to IOx applications and can be configured as a regular trunk interface.

IOx applications is an end-to-end application hosting framework that combines Cisco IOS and Linux to provide secure, consistent application deployment and lifecycle management on Cisco network platforms. It has a dedicated connectivity interface Ap1/1 on Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches. It

- provides an additional interface specifically for IOx application connectivity, and
- can be configured as a regular, physical interface in trunk mode, and

Guidelines for IOx application

Review supported application architectures, package storage requirements, and interface, VLAN, and gateway guidelines for deploying 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.

How to provide connections to IOx applications

This process describes how VLANs and trunk interfaces are configured to enable connections to IOx applications on a Cisco Catalyst IE3400 Rugged Series Switch, including network requirements and interface setup.

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.

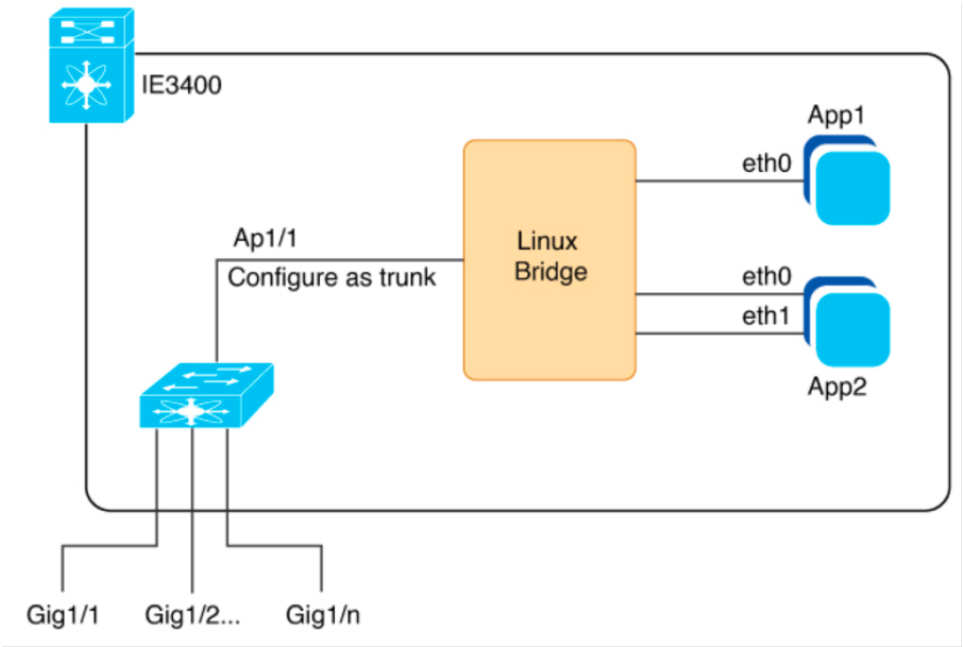
After you configure the network, you must enable IOx on the switch.

Summary

You can configure the allowed VLANs on the Ap1/1 trunk interface to match the VLANs carrying data and management traffic for IOx applications, ensuring proper communication.

Workflow

Figure 1: Connections with IE3400 IOx network with applications



TheConnections with IE3400 IOx network with applications 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 14 in this guide.

These stages describe how to configure VLANs and interfaces for IOx application connectivity.

1. Configure the allowed VLANs on the Ap1/1 trunk interface to match the VLANs required for IOx application data and management traffic. Ensure the same VLAN ID is used for managing applications and avoid using VLAN 1 as the native VLAN if it is used for network communication.
   - Identify the VLANs needed for application and management traffic (for example, VLAN 10).
   - Configure the Ap1/1 interface as a trunk and allow the identified VLANs.
   - Enable IOx on the switch after network configuration is complete.

   The dedicated AppGigabitEthernet1/1 interface for IOx is internally connected to a Linux bridge and must be configured as a trunk. Multiple applications can be supported, each with multiple Ethernet connections in any VLAN.

Configure VLAN ID for IOx interface

Learn how to configure the VLAN ID for the IOx interface and assign an SVI address to enable connectivity and management of the VLAN on your network.

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.

Procedure

1. Configure a VLAN ID for an IOx interface.

a) Use the **configure terminal** command to enter global configuration mode.

Example

```
Switch# configure terminal
```

b) Use the **interface** *interface_id* command to specify an interface.

Example

```
Switch(config)# interface Ap1/1
```

c) Use the **switchport trunk allowed vlan** *vlan_id* command to specify VLAN 10 as allowed on the trunk link for the IOx interface.

Example

```
Switch(config-if)# switchport trunk allowed vlan 10
```

d) Use the **switchport mode trunk** command to set the IOx interface to operate as a trunk port, carrying multiple VLANs.

Example

```
Switch(config-if)# switchport mode trunk
```

e) Use the **end** command to exit configuration mode and return to privileged EXEC mode.

Example

```
Switch(config-if)# end
```

2. Configure a SVI address for the VLAN.

a) Use the **configure terminal** command to enter global configuration mode.

Example

```
Switch# configure terminal
```

b) Use the **interface vlan** *vlan_id* command to specify an interface.

Example

```
Switch(config)# interface vlan 10
```

c) Use the **ip address** *ip_address subnet mask* command to assign the IP address and subnet mask to VLAN 10, enabling layer 3 connectivity for that VLAN.

Example

```
Switch(config-if)# ip address 192.168.0.1 255.255.255.0
```

d) Use the **end** command to exit configuration mode and return to privileged EXEC mode.

Example

```
Switch(config-if)# end
```

Enable IOx

Learn how to enable IOx on the switch by ensuring that the SD card IOx partition is correctly formatted, entering the required CLI commands, and enabling the web server and user access.

Enable IOx on the switch to support IOx applications and services. This procedure ensures the SD card is properly partitioned and the necessary services are configured.

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 is 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.

Procedure

1. Use the **partition sdflash: iox** command to format the SD card IOx partition with the EXT4 filesystem.

   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.

2. Use the **configure terminal** command to enter global configuration mode.

Example

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

3. Use the **iox** command to enable iox.

Example

```
Switch(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.
```

4. Use the **ip http secure-server** command to enable web server.

Example

```
Switch(config)# ip http secure-server
```

This step ensures access to the IOx functionality through the Local Manager UI.

5. Use the **username admin privilege 15 password 0 secret** command to enable user access:

Example

```
Switch(config)# username admin privilege 15 password 0 secret
```

6. Use the **end** command to exit configuration mode.

Example

```
Switch# end
```

7. Use the **show iox-service** command to monitor Iox infrastructure usage.

Example

```
Switch# show iox-service
IOx Infrastructure Summary:
---------------------------
IOx service (CAF) : Running
IOx service (HA) : Running
IOx service (IOxman) : Running
IOx service (Sec storage) : Running
Libvirtd 5.5.0 : Running
Dockerd v19.03.13-ce : Running
```

3 Deploy IOx Applications

Topics:

- Prerequisites
- Guidelines and limitations for IOx applications
- Deploy IOx applications

Prerequisites

Configure network connectivity and enable IOx on the switch before deploying applications.

Ensure that you have completed the tasks in the chapter IOx Applications on page 6 in this guide.

Guidelines and limitations for IOx applications

Use these guidelines when deploying IOx applications on Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches to ensure proper configuration and compatibility.

The application is Cisco Cyber Vision. For more details, refer to Cisco Cyber Vision .

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.

- 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 the 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

- Cisco IOx applications support Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300-8U2X, and IE3300-8T2X Rugged Series Switches.
- 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.

Deploy IOx applications

This topic explains the methods for deploying IOx applications on Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches, including CLI and Local Manager options.

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

- Deploy an application using Cisco IOx Local Manager on page 14 (GUI): Accessed through the web-based user interface, provides resource profiles such as tiny, exclusive, default, and custom. Custom profiles allow modification of CPU, memory, and disk values. A platform-specific application installed as part of the Cisco IOx framework.
- Deploying IOx applications using the IOS-XE CLI on page 14 : Used to manage the device and deploy applications without enabling the web server. The CLI that is part of the switch software for connecting to the switch on the device.

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.*

Deploying IOx applications using the IOS-XE CLI

This process describes how to deploy IOx applications using the IOS-XE CLI, including configuration, installation, activation, and startup steps on Cisco Catalyst IE3400 Rugged Series Switches.

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

Summary

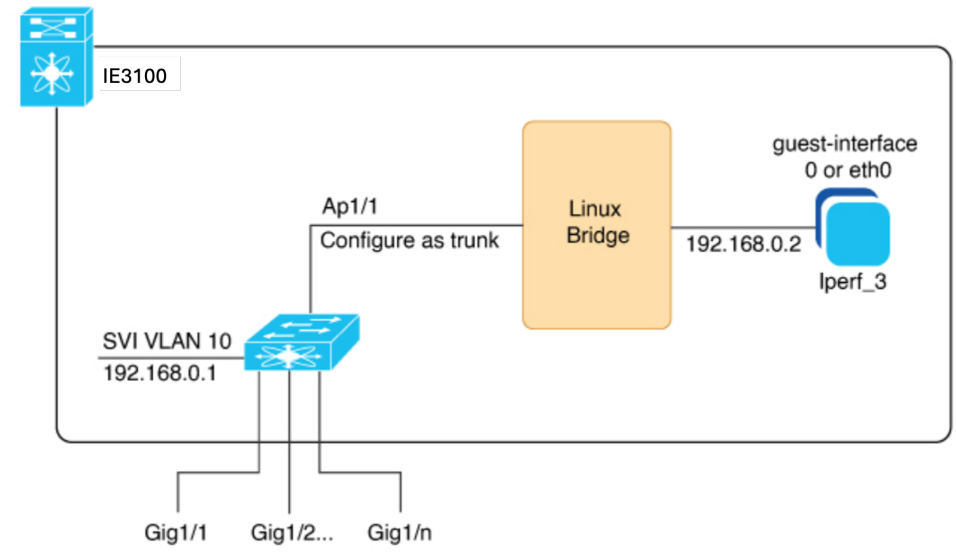
The deployment process involves these actors and components:

- IOx application: The software to be deployed and managed.
- Cisco Catalyst IE3400 Rugged Series Switch: The hardware platform hosting the IOx application.
- AppGigabitEthernet1/1 interface: Dedicated for IOx support, configured as a trunk and internally connected to a Linux bridge.
- SVI LAN 10: Provides the default gateway for the application.

The process consists of configuring the network interfaces, assigning IP addresses, and deploying the IOx application using the IOS-XE CLI.

Workflow

Figure 2: Example of IOx Deployment with Application



These stages describe the deployment of IOx applications using the IOS-XE CLI on Cisco Catalyst IE3400 Rugged Series Switches.

1. Configure the dedicated interface and assign IP addresses for the IOx application.
   - Configure AppGigabitEthernet1/1 as a trunk and connect it internally to a Linux bridge.
   - Assign IP address 192.168.0.2 to the guest interface for the application (e.g., Iperf_3).
   - Assign the default gateway on SVI LAN 10 with IP address 192.168.0.1.

   The preceding illustration shows an example configuration of an IOx network on a Cisco Catalyst IE3400 Rugged Series Switch.

   For an illustration without interface examples, refer to the IOx Applications on page 6.

Configure an application using the CLI

Learn how to configure an application using the IOS-XE CLI. This procedure guides you through the required commands and steps to set up an application on the Cisco IE3400 switch.

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

Before you begin

- You must have configured the network for IOx. See the section IOx applications on page 7.

Procedure

1. Use the **enable** command to enable privileged EXEC mode.

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

2. Use the **configure terminal** command to enter global configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

3. Use the **app-hosting appid iperf_3** command to configure an application name.

   Example

   ```
   Switch(config)# app-hosting appid iperf_3
   ```

4. Use the **app-vnic AppGigabitEthernet trunk** command to configure AppGigabitEthernet trunk.

   Example

   ```
   Switch(config-app-hosting)# app-vnic AppGigabitEthernet trunk
   ```

5. Use the **vlan 10 guest-interface** *0* command to configure a VLAN guest interface and enter application-hosting VLAN-access IP configuration mode.

Example

```
switch(config-config-app-hosting-trunk)#vlan 10 guest-interface 0
```

The configuration places Eth0 into vlan 10.

6. Use the **guest-ipaddress** *guest_ip_address* **netmask|prefix** *number* command to configure a static IP address.

   Example

   - IPv4

     ```
     Switch(config-config-app-hosting-vlan-access-ip)# guest-ipaddress
     192.168.0.2 netmask 255.255.255.0
     ```

   - IPv6

     ```
     Switch(config-config-app-hosting-vlan-access-ip)# guest-ipv6address 2001::1
      prefix 64
     ```

   The subnet for this IP address on the VLAN (in this example `vlan 10`) must match the subnet configured for the IP address assigned to `vlan 10` interface. See the preceding examples.

7. Use the **exit** command to exit submode.

   Example

   ```
   Switch(config-config-app-hosting-vlan-access-ip)# exit
   ```

8. Use the **exit** command to exit submode.

   Example

   ```
   Switch(config-config-app-hosting-trunk)# exit
   ```

9. Use the **app-default-gateway** *default_gateway_address* **guest-interface** *guest_interface number* command to configure the default gateway for the application.

   Example

   ```
   Switch(config-app-hosting)# app-default-gateway 192.168.0.1 guest-interface
   0
   ```

   The VLAN ID interface of the switch is used as the gateway.

   > **Note**
   >
   > Only three gateways are supported.

Configure Docker run-time options

Learn how to configure Docker run-time options for an application on Cisco IE3400. Use this procedure to specify and apply run-time options for Docker containers.

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.

Procedure

1. Use the **enable** command to enable privileged EXEC mode.

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

2. Use the **configure terminal** command to enter global configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

3. Use the **app-hosting appid iperf_3** command to configure an application name.

   Example

   ```
   Switch(config)# app-hosting appid iperf_3
   ```

4. Use the **app-resource docker** command to enter application-hosting docker-configuration mode.

   Example

   ```
   Switch(config-app-hosting)# app-resource docker
   ```

5. Use the **run-opts 1 "--entrypoint '/bin/sleep 10000'"** command to specify the Docker run time options.

   Example

   ```
   Switch(config-app-hosting-docker)# run-opts 1 "--entrypoint '/bin/sleep 10000'"
   ```

6. Use the **exit** command to exit the application-hosting docker-configuration mode.

   Example

   ```
   Switch(config-app-hosting-docker)# exit
   ```

Configure application resources

Learn how to configure application resources on the Cisco IE3400 switch by setting up application hosting and customizing resource profiles.

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** .

Procedure

1. Use the **enable** command to enable privileged EXEC mode.

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

2. Use the **configure terminal** command to enter global configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

3. Use the **app-hosting appid iperf_3** command to configure an application name.

   Example

   ```
   Switch(config)# app-hosting appid iperf_3
   ```

4. Use the **app-resource profile custom** command to configure the custom application resource profile.

   Example

   ```
   Switch(config-app-hosting)# app-resource profile custom
   ```

   Note

   Only the custom profile name is supported.

5. Use the **cpu** *value* command to configure CPU units.

   Example

   ```
   Switch(config-app-resource-profile-custom)# cpu 500
   ```

6. Use the **memory** *value* command to configure memory in megabytes.

Example

```
Switch(config-app-resource-profile-custom)# memory 256
```

7. Use the **persist-disk** *value* command to configure disk space in megabytes.

Example

```
Switch(config-app-resource-profile-custom)# persist-disk 256
```

IOx application installation, activation and startup

This topic explains how to install, activate, and start an IOx application on the IE3400 switch using IOS-XE CLI commands, including sign verification and resource allocation steps.

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

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 Verify IOx application signature on page 20 .

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

Learn how to install, activate, and start the IOx application on the Cisco IE3400 switch, including configuring the required interfaces for application communication.

Install, activate, and start the IOx application on the switch, and configure the interfaces to enable communication with 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 IOx Applications on page 6 .

Procedure

1. Use the **app-hosting install appid** *application_name* **package** *application_filename* command to install the application and move it to the deployed state.

Example

```
Switch# show app-hosting list
App id State
------------------------------------------------------------
iperf_3 INSTALLING
Switch#
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
Switch# show app-hosting list
App id State
------------------------------------------------------------
iperf_3 DEPLOYED
```

Installs the application and moves it into the deployed state.

2. (Optional) Use the **show app-hosting list** command to confirm the application's installation and state.

Example

```
Switch# show app-hosting list
App id                                   State
---------------------------------------------------------
iperf_3                                  DEPLOYED
```

3. Use the **app-hosting activate appid** *application_name* command to activate the application and assigns it switch resources.

Example

```
Switch# app-hosting activate appid iperf_3
Current state is: ACTIVATED
```

4. Use the **app-hosting start appid** *application_name* command to start an application on the switch.

Example

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

Verify IOx application signature

Learn how to verify the signature of a Cisco IOx application during installation to ensure the package is valid and from a trusted source.

Application package signature ensures that an application package is valid and the one installed on the device comes from a trusted source.

You can check signature verification of a Cisco IOx application during its installation. The configuration keyword `start` is available under application-hosting application configurations. If you use this keyword, IOx infra automatically activates and starts the application after installation. Otherwise, you must explicitly use the **activate** and **start** CLI commands to start the application.

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

Before you begin

- Ensure you have access to the device and application-hosting configuration mode.

Procedure

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

- IOx infra checks for a signature in these 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.
- You cannot run non-Cisco applications if signature verification is enabled. 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.

Example

```
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)
```

IOx application command examples

This topic explains examples of IOS-XE CLI commands for IOx applications, including resource viewing, application information, and management operations on Cisco switches.

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

View resources on the switch

Use the **show app-hosting resource** command to view 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)
        VCPU:
        Count: 2
        Memory:
        Quota: 1248(MB)
        Available: 0(MB)
        Storage space:
        Total: 2548(MB)
        Available: 268(MB)
```

Use the **show app-hosting infra** command to view the CPU quota in units and 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

Use the **show app-hosting list** command to view the application-related information on the switch.

```
Switch# show app-hosting list
        App id                                   State
        ---------------------------------------------------------
        iperf_3                                  RUNNING
```

Use the **show app-hosting detail appid** *app_id* command to view the detailed application-related information on the switch.

```
Switch# show 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#
```

Stop, deactivate, and uninstall the application

Use the **app-hosting stop appid** *app_id* command to stop the IOx application on the switch.

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

Use the **app-hosting deactivate appid** *app_id* command to deactivate the IOx application on the switch.

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

Use the **app-hosting uninstall appid** *app_id* command to uninstall the IOx application on the switch.

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

This list shows the `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
```

4 L3NAT for IOx Applications

Topics:

- L3NAT in industrial networking
- L3NAT-IOx
- Guidelines and restrictions
- Configure L3NAT-IOx
- Feature history for L3NAT-IOx

L3NAT in industrial networking

This topic explains how Layer3 Network Address Translation (L3NAT) for IOx applications simplifies industrial networking by reducing the need for multiple public IP addresses and streamlining application hosting on IE devices.

Layer3 Network Address Translation (L3NAT) for IOx applications is a feature that enables the use of the switch management IP as a proxy for all applications within the routed network, reducing the need for multiple public routable IP addresses.

- Reduces the overhead and complexity of managing multiple public IP addresses for Industrial Ethernet (IE) devices.
- Supported on the IE3x00 platform with the Cisco Cyber Vision (CCV) IOx application.
- Cannot be used to NAT other Ethernet traffic from hosts connected to the switch's physical Ethernet ports.

L3NAT in industrial networking environment

In industrial networking environments, efficient communication between internal applications and external servers is essential for seamless operations. 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.

L3NAT-IOx

This topic explains the L3NAT-IOx feature, which enables translation of private IP addresses to public IP addresses at the network layer, facilitating secure communication between internal applications and external servers.

L3NAT-IOx is a networking feature that translates private IP addresses in an internal network to a public IP address at the network layer, using hardware components such as ASIC and FPGA.

- Translates private IP addresses to public IP addresses before packets are sent to an external network.
- Utilizes hardware components such as Application-Specific Integrated Circuit (ASIC) and Field-Programmable Gate Array (FPGA) for implementation.
- Ensures seamless communication between internal applications and external servers by managing address translation in both directions.

How L3NAT-IOx enables secure communication

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

Use these guidelines when configuring L3NAT-IOx to ensure proper feature support, licensing, and application compatibility.

- The feature supports only the CCV application. It is not supported for any other IOx application.
- Only static translation is supported.
- Translation is limited to TCP and UDP packets only.

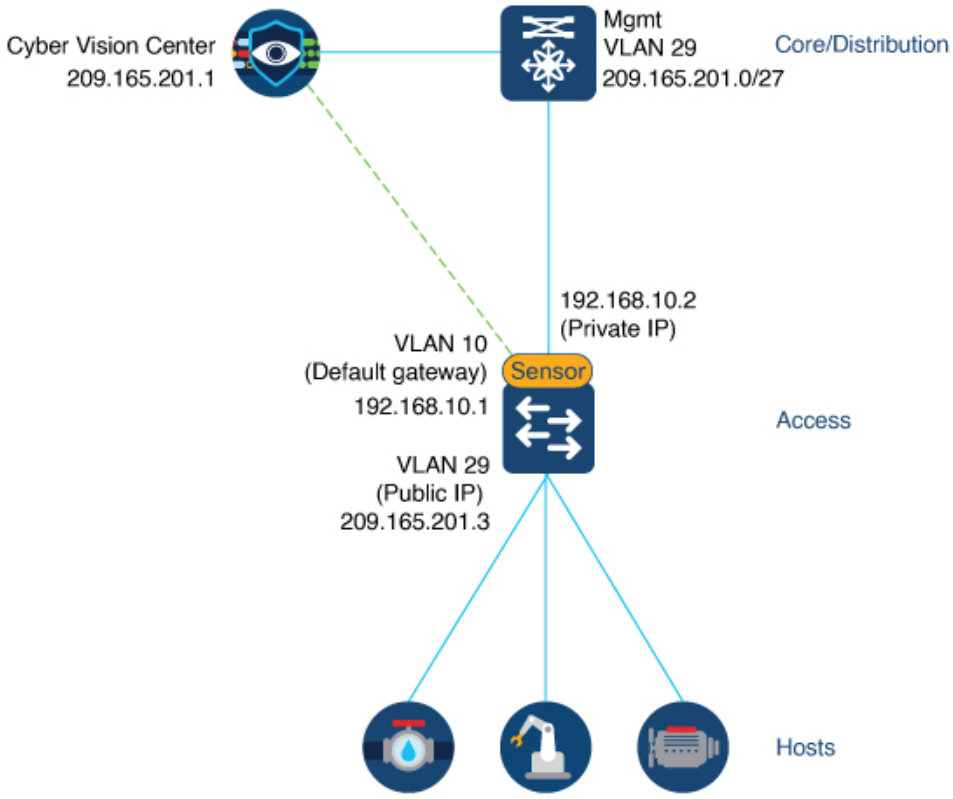
- Users must create an additional SVI on IE for the private network used by the application. The IP assigned to the SVI will serve as the default gateway for the application.
- This feature requires a Network Advantage license.
- The L3NAT-IOx statistics cannot be fetched using YANG with Network Configuration Protocol (NETCONF).

Configure L3NAT-IOx

Learn how to configure L3NAT-IOx for CCV onboarding using SVI interfaces and NAT settings on a switch hosting the CCV sensor application.

The configuration example is based on the CCV onboarding topology:

Figure 3: CCV onboarding



The figure *CCV onboarding* 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. The CCV sensor is installed using the private IP network 192.168.10.x.

Procedure

1. Use the **int vlan** *vlan_id* command to 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
```

2. Use the **int vlan** *vlan_id* command to 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
```

3. Use the **l3nat-iox** command to configure the L3NAT-IOx.

```
Switch(config)# l3nat-iox
```

4. Use the **app-ip** *app_ip* **svi-ip** *svi_ipapp-name* **CCV-ONPREM server-ip** *server_ip* command to map the private application IP to the public SVI IP, associating it with the specified application name and server IP for L3NAT translation.

```
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
```

5. Use the **exit** command to exit IOx NAT configuration mode.

```
Switch(config-iox-nat)# exit
```

6. Use the **exit** command to exit configuration mode.

```
Switch(config)# exit
```

7. Use the **show ioxnat statistics** command to view NAT statistics.

   - The statistics show the translated IP addresses and the count of egress and ingress translations between the private application IP address and the 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, this 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

This topic explains the feature history for L3NAT-IOx, including release information and supported platforms.

This topic provides the feature history for L3NAT for IOx Applications, including release details and supported platforms.

Table 1: 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