L3NAT for IOx Applications

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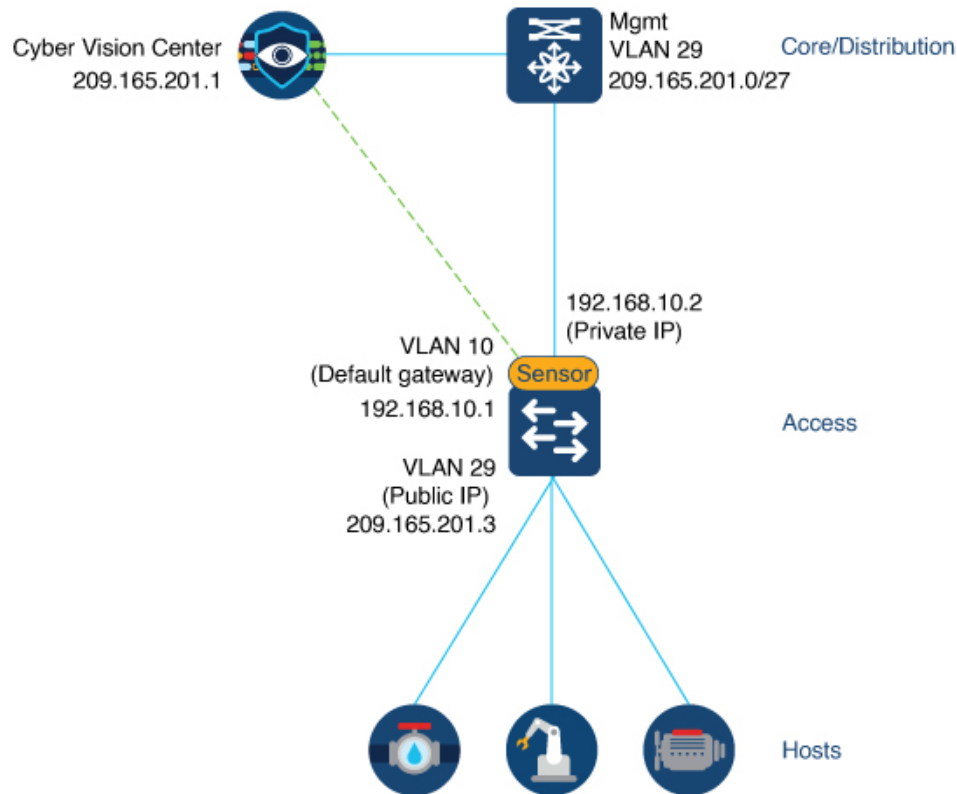
The above figure shows application hosting on the switch using a Private IP address. The CCV sensor application is installed on the access devices to which hosts are connected. The management public IP address is given to the devices located in the 209.165.201.0/27 network. CCV sensor is installed using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

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

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