



Set Up Network Monitoring

- [Set Up Port and Interface Monitoring, on page 1](#)
- [Set Up Enhanced Wireless Client Monitoring Using Cisco ISE, on page 2](#)
- [Set Up NAM and NetFlow Data Collection for Performance Monitoring, on page 3](#)

Set Up Port and Interface Monitoring

To monitor your device ports, you can create a port group and then display monitoring information on dashboards. Port groups are logical groupings of interfaces that allow you to monitor device ports by the function they serve. For example, you can create a port group for the WAN ports and create another port group for the internal distribution ports on the same router.

After you create groups, you can create an interface health monitoring policy on those ports as explained in the following steps:

-
- Step 1** Choose Monitor > Monitoring Tools > Monitoring Policies.
 - Step 2** Click My Policies.
 - Step 3** Click Add.
 - Step 4** Choose Interface Health under Policy Types.
 - Step 5** From the Device Selection drop-down list, choose Port Group.
 - Step 6** Choose the User Defined group and click OK.
 - Step 7** Enter the policy name.
 - Step 8** Select required the Parameters and Threshold and complete the required fields.
 - Step 9** Click OK.
 - Step 10** Click Save and Activate.
 - Step 11** To display the results, choose Dashboards > Overview > Network Interface, and view the Top N Interface Utilization dashlet.
 - Step 12** Edit the Top N Interface Utilization dashlet and add the port group that you previously created.
-

Set Up WAN Interface Monitoring

Creating a WAN interface port group allows you to efficiently monitor all WAN interfaces in a specific port group. For example, if you have many small branch offices that have low bandwidth issues, you can create a port group that includes all WAN interfaces from each branch office, and then monitor this port group for issues.

By default, provides a static WAN Interfaces port group on which health monitoring is automatically deployed. The following procedure shows you how to:

1. Add interfaces to the WAN Interfaces port group.
2. Verify the utilization and availability of the WAN interfaces from the Site dashboard.

Step 1 To add interfaces to the WAN Interfaces port group:

- a) Choose Inventory > Group Management > Port Groups.
- b) From the menu on the left, choose System Defined > WAN Interfaces.
- c) Select the device, then click Add to Group.

Step 2 To display the results:

- a) Choose Dashboard Overview Add Dashlets.
 - b) Click either of the following:
 - Top N WAN Interfaces by Utilization
 - Top N WAN Interfaces with Issues
-

Set Up Enhanced Wireless Client Monitoring Using Cisco ISE

manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, collects additional information about these clients from Cisco ISE and provides all client relevant information to to be visible in a single console.

When posture profiling is enforced in the network, communicates with Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

You can get enhanced information about managed clients using the Cisco ISE server.

If is integrated with an ISE server (to access endpoint information), you can:

- Check an End User's Network Session Status.
- Using the User 360° View, you can identify possible problems with the end user's authentication and authorization for network access.
- Troubleshoot the User Application and Site Bandwidth Utilization.

displays ISE Profiling attributes only for authenticated endpoints.

Add Cisco Identity Service Engines

A maximum of two ISEs can be added to . If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add a second node.

To add an Identity Services Engine, follow these steps:

Step 1 Choose Administration > Servers > ISE Servers.

Step 2 From the Select a command drop-down list, choose Add ISE Server, then click Go.

Step 3 Complete the required fields, then click Save.

The credentials should be superuser credentials local to ISE. Otherwise, ISE integration does not work.

Set Up NAM and NetFlow Data Collection for Performance Monitoring

If your implementation includes Assurance licenses, you must enable data collection via NAMs and NetFlow configurations. This is necessary to populate the additional dashlets, reports, and other features supplied with Assurance.

Enable NAM Data Collection

To ensure that you can collect data from your Network Analysis Modules (NAMs), you must enable NAM data collection. You can do this for each discovered or added NAM, or for all NAMs at the same time.

Before you begin

You must specify the HTTP/HTTPS credentials for each NAM. See “Adding NAM HTTP/HTTPS Credentials.”

Step 1 Choose Services > Application Visibility & Control > Data Sources.

Step 2 In the NAM Data Collector section, select the required NAM datasources for which you want to enable data collection.

Step 3 Click Enable.

Note After enabling the NAM Polling, you can verify the NAM data Top N Application dashlet from Application dashboard.

To disable NAM Data collection, select the required(enabled) NAM or NAM datasources from the NAM Data Collector section and click Disable.

Define NAM Polling Parameters

You can specify data that is collected from NAMs.

-
- Step 1** Choose Monitor > Monitoring Policies.
- Step 2** Click Add, then select NAM Health under the Policy Types list from the left sidebar menu.
- Step 3** Select the NAM devices from which you want to collect data, then complete the required fields.
- Step 4** Under Parameters and Thresholds, specify the parameters you want to poll from the NAM devices and threshold conditions.
- Step 5** Click Save and Activate.
-

Enable NetFlow Data Collection

To start collecting NetFlow and Flexible NetFlow data, you must configure your NetFlow-enabled switches, routers, and other devices (ISR/ASR) to export this data to . The following table shows the various device types that support NetFlow and the ways to configure devices to export NetFlow data to .

The following table gives the detailed information of NetFlow support summary.

Table 1: NetFlow Support Summary

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco ASR	IOS XE 3.11 to 15.4(1) S, and later Easy PerfMon based configuration (EzPM)	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility Application Traffic Stats	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-URL- Netflow-Aggregated-Traffic-Stats-
	IOS XE 3.9, 3.10	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility AVC Troubleshooting	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Host- Netflow-App-Traffic- Netflow-Voice-Video- Netflow-URL- Netflow-AVC-Troubleshooting-

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco ISR	15.1(3) T	TCP/UDP conversation traffic Voice & Video	TCP/UDP: Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics Voice Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
	IOS XE 3.11 to 15.4(1) S, and later Easy PerfMon based config (EzPM)	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility Application Traffic Stats	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-URL- Netflow-Aggregated-Traffic-Stats-
	IOS XE 3.9, 3.10	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility AVC Troubleshooting	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Host- Netflow-App-Traffic- Netflow-Voice-Video- Netflow-URL- Netflow-AVC-Troubleshooting-

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco ISR G2	15.1(4) M and 15.2(1) T	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video	TCP/UDP, ART: Create a CLI template. See “Configure NetFlow on ISR Devices” Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Voice-Video-
	15.2(4) M and 15.3(1) T	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video	Choose: Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Voice-Video-
	15.4(1) T and later Easy PerfMon based configuration (EzPM)	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-App-Traffic-URL-
Cisco Catalyst 2000	15.0(2) UCP and later	TCP/UDP conversation traffic	Create a custom CLI template. See “Configuring NetFlow Export on Catalyst 2000 Switches” . Format: V5, V9	Netflow-Traffic-Conv-
Cisco Catalyst 3750-X, 3560-X	15.0(1) SE IP base or IP services feature set and equipped with the network services module.	TCP/UDP conversation traffic	Create a custom CLI template. See “Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches.” Format: V9	Netflow-Traffic-Conv-

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco Catalyst 3850 (wired)	15.0(1)EX and later	TCP/UDP conversation traffic Voice & Video	TCP/UDP: Create a custom CLI template. Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches.” Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
Cisco Catalyst 3850 (wireless)	Cisco IOS XE Release 3SE (Edison)	TCP/UDP conversation traffic	See “Configuring Flexible NetFlow.” Format: V9	Netflow-Traffic-Conv-
Cisco CT5760 Controller (Wireless)	Katana 5760	TCP/UDP conversation traffic	See “Application Visibility and Flexible Netflow.” Format: V9	Netflow-Traffic-Conv-
Cisco Catalyst 4500	15.0(1)XO and 15.0(2)SG onwards	TCP/UDP conversation traffic Voice & Video	TCP/UDP: Create a custom CLI template. See” Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches.” Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
Cisco Catalyst 6500	15.1(1)SY and later	TCP /UDP conversation traffic Voice & Video	TCP/UDP: Create a custom CLI template. See” Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches.” Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-

Configure NetFlow Export on Catalyst 2000 Switches

To manually configure NetFlow export on Catalyst 2000 devices, create a user-defined CLI template as shown in the following steps.

-
- Step 1** Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.
- Step 2** Hover your mouse cursor over the information icon and click New to create a new CLI template.
- Step 3** Enter a name for the new CLI template (for example, “Prime_NF_CFG_CAT2K”).
- Step 4** From the Device Type list, choose Switches and Hubs.
- Step 5** In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example):

```
flow record PrimeNFRec

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match interface input

match transport source-port

match transport destination-port

collect counter bytes long

collect counter packets long

!

!

flow exporter PrimeNFExp

destination 172.18.54.93

transport udp 9991

option exporter-stats timeout 20

!

!

flow monitor PrimeNFMon
```



```
record PrimeNFRec

exporter PrimeNFExp

interface GigabitEthernet3/0/1

ip flow monitor PrimeNFMon input
```

- Step 6** Click Save as New Template. After you save the template, deploy it to your devices. See “[Ways to Create Configuration Templates Using Prime Infrastructure](#).”

Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches

To manually configure NetFlow to export TCP and UDP traffic on Catalyst 3000, 4000, or 6000 devices, create a user-defined CLI template as shown in the following steps.

-
- Step 1** Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.
- Step 2** Hover your mouse cursor over the information icon and click New to create a new CLI template.
- Step 3** Enter a name for the new CLI template (for example, “Prime_NF_CFG_CAT3K_4K”).
- Step 4** From the Device Type list, choose Switches and Hubs.
- Step 5** In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example):

```
flow record PrimeNFRec

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match interface input

match transport source-port

match transport destination-port

collect counter bytes long

collect counter packets long

flow exporter PrimeNFExp
```

```

destination 172.18.54.93

transport udp 9991

option exporter-stats timeout 20

flow monitor PrimeNFMon

record PrimeNFRec

exporter PrimeNFExp

interface GigabitEthernet3/0/1

ip flow monitor PrimeNFMon input

```

- Step 6** Click Save as New Template. After you save the template, deploy it to your devices See “ [Ways to Create Configuration Templates Using Prime Infrastructure](#).”

Configure NetFlow on ISR Devices

To manually configure NetFlow to export ART traffic on an ISR device, use the following steps to create a user-defined CLI template:

- Step 1** Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.
- Step 2** Hover your mouse cursor over the information icon and click New to create a new CLI template.
- Step 3** Enter a name for the new CLI template (for example, “Prime_NF_CFG_TEMPLATE”).
- Step 4** From the Device Type list, choose Routers.
- Step 5** In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example).

```

flow record NFARecord
match ipv4 source address
match ipv4 destination address
match ipv4 protocol
match transport source-port
match transport destination-port
match application name
match interface input
collect interface output
collect ipv4 source mask
collect ipv4 destination prefix
collect ipv4 destination mask
collect counter bytes long

```

```
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!

flow exporter NFAExporter
destination <Prime server ip address>
source <Any L3 interface or the device>
transport udp 9991
template data timeout 60
option application-table timeout 60
option application-attributes timeout 300
!

flow monitor NFAMonitor
exporter NFAExporter
cache timeout active 60
record NFARecord
!

interface <L3 interface provided in exporter:source section>
ip flow monitor NFAMonitor input
!
```

Step 6 Click Save as New Template. After you save the template, deploy it to your devices. See “[Ways to Create Configuration Templates Using Prime Infrastructure](#).”
