Setting Up Network Monitoring

After you add devices to the Cisco Prime Infrastructure inventory and set up device and port groups, you need to set up your devices to allow Prime Infrastructure to monitor the devices.

- Specifying Which Interfaces and Ports to Monitor, page 5-1

You can also configure Prime Infrastructure to monitor more advanced information:

- Getting Enhanced Client Information by Integrating with ISE, page 5-3
- Setting Up Assurance for Performance Monitoring, page 5-4

Specifying Which Interfaces and Ports to Monitor

You create monitoring templates to monitor device features, usage, health, and other factors. After you create and deploy monitoring templates, Prime Infrastructure collects and processes data from specified devices and displays the information in dashboards, dashlets (see Dashboards and Dashlets, page A-2), and reports.

To monitor your device ports, you can create a port group and then display monitoring information on the Prime Infrastructure dashboard. 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.

When you create a port group, you must determine which types of ports you want to monitor. The following port groups are typical of most networks:

- Port Type
- User Defined
- WAN Interfaces

After you create port groups, you can more efficiently configure all of the devices belonging to a port group.

Setting Up WAN Interface Monitoring

Creating a WAN interface port group allows you to efficiently configure settings on all WAN interfaces in a specific port group. For example, a small branch office might have a problem where the WAN bandwidth is as low as 1.544 Mb/s, and a round trip latency of 300 ms. To watch the WAN bandwidth used by this branch, you set up the interface from the router that connects to the ISP as a WAN interface.

The following procedure shows you how to:

1. Create a port group for the WAN interfaces.
2. Create and deploy a WAN interface health monitoring template on those ports.
3. Verify the utilization and availability of the WAN interfaces from the Site dashboard.

Step 1 To create the port group:

a. Choose **Design > Management Tools > Port Grouping**.

b. Choose the device IP addresses that you know are WAN interfaces and that you want to add to the port group, then choose **Add to Group > Select Group > WAN Interfaces**.

Step 2 To create and deploy a WAN interface health monitoring template:

a. Choose **Design > Configuration > Monitor Configuration.**

b. In the Templates menu on the left, click **Features > Metrics > Interface Health**.

c. Complete the basic template fields, select the attributes that you want to monitor (for example, Interface Availability, ifInErrors, ifOutErrors, inputUtilization, and outputUtilization), then click **Save as New Template**.

d. Choose **Deploy > Configuration Deployment > Monitoring Deployment**.

e. From the Templates menu on the left, click **My Templates**.

f. Select the new template, choose **Deploy > Port Groups > WAN Interfaces,** and click **Submit.**

Step 3 Display the results:

a. Choose **Home > Detail Dashboards > Sites >**  **> Add Dashlets**.

b. Select either of the following:

- **Top N WAN Interfaces by Utilization**
- **Top N WAN Interfaces with Issues**

Getting Enhanced Client Information by Integrating with ISE

You can get enhanced information about managed clients using the Cisco Identify Services Engine (ISE) or ACS View servers.

Adding an Identity Services Engine

A maximum of two ISEs can be added toPrime Infrastructure. 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 **Design > Management Tools > External Management Servers > ISE Servers**.

Step 2 From the Select a command drop-down list, choose **Add Identity Services Engine**.

Step 3 Complete the required fields, then click **Save**.

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

Configuring ACS View Servers

If you do not have ISE, you can integrate your Cisco Secure Access Control ACS View server with Prime Infrastructure. To access the ACS View Server tab, you must add a view server with credentials.

Note Prime Infrastructure supports only ACS View Server 5.1 or later.

To configure an ACS View Server, follow these steps:

Step 1 Choose **Design > External Management > ACS View Servers**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the time, in seconds, after which the authentication request times out and a retransmission is attempted by the Cisco WLC controller.

Step 5 Specify the number of retries to be attempted.

Step 6 Click **Save**.

Setting Up Assurance for Performance Monitoring

If your Prime Infrastructure 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.

Enabling 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, page 3-10).

Step 1 Choose **Administration > System Settings > Data Sources.**

Step 2 In the **NAM Data Collector** section, select all of the NAMs for which you want to enable data collection.

Step 3 Click **Enable**.

Enabling 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 Prime Infrastructure. The following table shows the various device types that support NetFlow and the ways to configure devices to export NetFlow data to Prime Infrastructure.

Table 5-1 NetFlow Support Summary

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
Catalyst 3750-X / 3560-X	15.0(1)SE IP base or IP services feature set and equipped with the network services module.	TCP and UDP traffic	See Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6.
Catalyst 3850	15.0(1)EX	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
Catalyst 4500	15.0(1)XO and 15.0(2)	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
Catalyst 6500	SG15.1(1)SY	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
ISR	15.1(3) T	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI > Collecting Traffic Statistics** To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**

Table 5-1 NetFlow Support Summary (continued)

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
ISR G2	15.2(1) T and 15.1(4)M	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see Configuring NetFlow on ISR Devices, page 5-8. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
ISR G2	15.2(4) M2 or later, 15.3(1)T or later	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see Configuring Application Visibility, page 13-2.
ASR	15.3(1)S1 or later	TCP and UDP traffic, application response time, Voice & Video, HTTP URL visibility	
ISR G3	15.3(2)S or later		

Configuring 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, use the following steps to create a user-defined CLI template:

Step 1 Choose **Design > Feature Design > CLI Templates > CLI**, hover your mouse cursor over the information icon and click **New**.

Step 2 Provide a name for the template (for example, Prime_NF_CFG_CAT3K_4K).

Step 3 From the Device Type list, choose **Switches and Hubs**.

Step 4 In the **Template Detail > CLI Content** text box, enter the following commands, modifying them for your network:

Figure 5-1 Catalyst 3000, 4000, and 6000 CLI Commands

```
flow record PrimeNFRec
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 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 5 Choose **Deploy > Configuration Tasks** to save and deploy the template to the relevant devices**.**

Configuring NetFlow on ISR Devices

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

Step 1 Choose **Design > Feature Design > CLI Templates > CLI**, hover your mouse cursor over the information icon and click **New**.

Step 2 Provide a name for the template (for example, Prime_NF_CFG_MACE).

Step 3 From the Device Type list, choose **Routers**.

Step 4 In the **Template Detail > CLI Content** text box, enter the following commands, modifying them for your network:

Figure 5-2 ISR MACE CLI Commands

```
flow record type mace mace-record
collect application name
collect art all
!
flow exporter mace-export
destination <PI_SERVER_IP_ADDRESS>
source GigabitEthernet0/1
transport udp 9991
!

flow monitor type mace mace-monitor
record mace-record
exporter mace-export
cache timeout update  600

class-map match-all PrimeNFClass
    match protocol ip
    exit

policy-map type mace mace_global
                class PrimeNFClass
                flow monitor mace-monitor
                exit
exit

interface GigabitEthernet 0/1
                mace enable
```

Step 5 Choose **Deploy > Configuration Tasks** to save and deploy the template to the relevant devices.