Set Up the Prime Infrastructure Server

This section contains the following topics:

Server Setup Tasks

Task	See
Verify the backup settings	Set Up Automatic Application Backups
Install any required product licenses and software updates	
Modify the stored Cisco.com credentials (user name and password) used to log on to Cisco.com and: • Check for product updates • Check for device software image updates • Open or review Cisco support cases	Configure Stored Cisco.com Credentials
For software updates: • Enable notifications for product software updates (critical fixes, device support, add-ons) • Specify whether you want credentials stored on Cisco.com when checks for software updates, and if yes, whether you want the user to be prompted for credentials when checking for updates	Enable or Disable Notifications About Software Updates
Set up HTTPS on the server for secure interactions between the server and browser-based GUI client (you can use HTTP but HTTPS is recommended)	Secure the Connectivity of the Server

Task	See
Configure high availability	
Adjust data retention and purging	
For server-related traps that signal system problems, customize the threshold settings and severities, and forward the traps as SNMP trap notifications to configured receivers	Customize Server Internal SNMP Traps and Forward the Traps
Set up NTP (Network Time Protocol) so that time is synchronized between the server and network devices	Set Up NTP on the Server
Configure FTP/TFTP on the server for file transfers between the server and network devices	Enable FTP/TFTP/SFTP Service on the Server
Configure a proxy for the server	Set Up the Proxy Server
Configure the email server	Set Up the SMTP E-Mail Server
Set global SNMP polling parameters for managed network elements	Configure Global SNMP Settings for Communication with Network Elements
Enable the Compliance feature if you plan to use it to identify device configuration deviations	
Configure product feedback to help Cisco improve its products	Set Up Defaults for Cisco Support Requests
Configure product feedback to help Cisco improve its products	Configure Cisco Product Feedback Settings

User Management Setup Tasks

Task	See
Create web GUI users that have administration privileges, and disable the web GUI root account	Create Web GUI Users with Administrator Privileges Disable and Enable the Web GUI root User
Set up user audits	Audit Configuration Archive and Software Management Changes ()
Set up user authentication and authorization	Configure External Authentication Configure Local Authentication
Create user accounts and user groups	Control the Tasks Users Can Perform (User Groups)
Adjust user security settings (password rules for local authentication, idle time logout setting)	Configure Global Password Policies for Local Authentication Configure the Global Timeout for Idle Users

Task	See
Specify which users can approve jobs	Configure Job Approvers and Approve Jobs
Create virtual domains to control device access	Create Virtual Domains to Control User Access to Devices
Create a message that is displayed when users log in to the GUI client	Create a Login Banner (Login Disclaimer)

Fault Management Setup Tasks

Task	See
Forward alarms and events to other receivers in e-mail format	
Forward alarms and events to other receivers in SNMP trap format	
Configure global settings for alarm and event displays and searches: • Hide acknowledged, assigned, and cleared alarms in the Alarms and Events tables • Include acknowledged and assigned alarms in search results • Include device names in alarm messages	Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms
Customize the severity for specific events	Change Severity Levels
Customize the troubleshooting text that is associated with an alarm	Customize the Troubleshooting Text for an Alarm
Customize the auto-clear interval for specific alarms	Change Alarm Auto-Clear Intervals
Make the text in the alarm **Failure Source** field more user-friendly	Change Severity Levels
Control generic event handling	Disable and Enable Generic Trap Processing
Control if and how users can create Cisco Support Requests	Set Up Defaults for Cisco Support Requests

Administrator Setup Tasks

Set Up Operations Center

Operations Center is a licensed feature that allows you to manage multiple instances of from a single instance. Before you can use Operations Center, you must first:

1. Activate your Operations Center license on the server that will host Operations Center. Applying the license will automatically enable Operations Center as the SSO server for the cluster of instances it manages.

Note You can also activate your operation center license on the Prime Infrastructure server that will host Operations Center using smart licensing feature. Applying the smart license will also automatically enableOperations Center as the SSO server for the cluster of Prime Infrastructure instances it manages. To know more on Smart Licensing, see Smart Licensing.

2. Add to Operations Center the instances you want to manage. You can configure each instance as an SSO client as it is added to Operations Center
3. (Optional) Disable the personal and global idle-user timeouts for Operations Center and all of its managed instances.
4. (Optional) Configure remote AAA using TACACS+ or RADIUS servers for Operations Center and all of its managed instances,

The Related Topics explain how to complete each of these tasks.

Related Topics

Add Instances to Operations Center, on page 6
Disable Idle User Timeouts for Operations Center, on page 6

Activate Your Operations Center License

Before setting up Operations Center:

- Verify that the DNS entry for the server that will host the Operations Center matches the host name configured on that server. For example: Running the commands **nslookup** *ipaddress* and **hostname** on the server that will host the Operations Center should yield the same output.
- Ensure that all users who will access network information using Operations Center have both NBI Read and NBI Write access privileges. You can do this by editing these users' profiles to make them members of the "NBI Read" and "NBI Write" User Groups (see " Change User Group Memberships " in Related Topics).
- By default, five is the maximum SSO login sessions for one Operations Center user. This is also applicable for instances. Hence, ensure that the number of Active SSO Sessions does not exceed five, or else the managed instances will go into an "unreachable" state.
- If you plan to use remote AAA with Operations Center: Set up a RADIUS or TACACS+ AAA server before you begin (see "Enable AAA for Operations Center" in Related Topics)

Operations Center does not require a separate installation. Instead, you can select or install the server that you want to use to manage other instances, and then activate an Operations Center license on that server.

When activating the license, Operations Center automatically configures itself as the SSO server .

The number of instances you can manage using Operations Center depends on the license you have purchased. For details, see the Cisco Prime Infrastructure Ordering and Licensing Guide.

Step 1 Select **Administration > Licenses and Software Updates > Licenses** > **Files > License Files**. The License Files page displays.

Step 2 Click **Add**. The **Add a License File** dialog box displays.

Step 3 Click **Choose File**.

Step 4 Navigate to your license file, select it, then click **Open**.

Step 5 Click **OK**. will confirm that the Operations Center license has been added.

Step 6 If you are notified that SSO is not set up:

- Click **Yes**, to configure this new Operations Center as an SSO server automatically.
- Click **No** to configure SSO with DNS Name. Seamless SSO will Add SSO server with DNS Name.

Step 7 When prompted to log out: Click **OK**. The newly active license should now be listed in the **Licenses > License Files** page.

Step 8 Log out of and then log back in. The login page that appears should display “Cisco Prime Infrastructure Operations Center [SSO]”, which indicates the license has been applied.

Related Topics

Set Up Operations Center, on page 4
Enable AAA for Operations Center, on page 7
Change User Group Memberships

Enable Smart Software Licenses for Operations Center

Step 1 If this is the first time you are choosing Smart licenses:

a) Choose **Administration > Licenses and Software Updates > Licenses**.

After a few moments, Prime Infrastructure displays a dialog box informing you that you cannot access the page because you are not using traditional licensing. This is normal.

b) In the dialog box, click **Smart License Settings**.

c) Click the **Licensing Settings** tab.

Step 2 If you are already using Smart Licensing:

a) Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.

b) Click the **Licensing Settings** tab.

Step 3 Click **Smart Software Licensing** radio button.

Step 4 Choose Prime Infrastructure Operation Center from the **Product Name** drop-down list and click **Enable Smart Software Licensing**.

Note To enable Operation Center SSO, click **Yes** in the **If you want to add SSO for the same server with IP/DNS** dialog box.

Step 5 Select the licenses in the Available Licenses dialog box, then click **Save**.

Add Instances to Operations Center

Once you have activated your Operations Center license, you must add to Operations Center each of the server instances you want to manage using Operations Center.

Note that each server instance you plan to manage using Operations Center must be enabled as an SSO client of the Operations Center server. You can do this in advance, by adding Operations Center as the SSO server for the managed instance (see "Add SSO Servers" in Related Topics). You can also have Operations Center do this for you when you add the server to Operations Center (you must know the password for the "root" user on the server instance).

Step 1 Log in to **Prime Infrastructure Operations Center**.

Step 2 Select **Monitor > Manage and Monitor Servers**.

Step 3 Click **Add**.

Step 4 Enter the IP address/FQDN of the server instance that you want to manage using Operations Center. You may also enter an alias or host name for the server.

The port number 443 is preset for HTTPS communications between Operations Center and its managed instances. Do not change this value unless you have configured HTTPS for a different port.

Step 5 Click OK.

If the server instance you are adding is already configured to use Operations Center as its SSO server, it is added as a managed server instance.

If the server instance is not configured as an SSO client:

a) Select **Enable Single-Sign-On Automatically**. Operations Center prompts you for a **Username** and **Password**.
b) Enter the user name and password for the "root" user on the server instance you want to add.

Note When you login as an SSO authenticated user and want to run an API query, make sure that you login as a local user in that particular instance, because SSO does not support basic authentication required by the API.

c) Click **OK** again.

Step 6 Repeat these steps to add more servers, up to the license limit.

Related Topics

Set Up Operations Center, on page 4
Add SSO Servers

Disable Idle User Timeouts for Operations Center

By default, automatically signs out all users whose sessions stay idle for too long. This feature is enabled by default to preserve network bandwidth and processing cycles for active use.

This feature can be annoying for Operations Center users, who will typically have sessions opened not only with Operations Center, but with one or more of the instances of that Operations Center is managing. Idleness in one of these sessions can force a global idle-user timeout for all the sessions, resulting in a sudden logout without warning.

To avoid this inconvenience, administrators must:

1. Disable the global idle user timeout feature, as explained in *Adjust Your GUI Idle Timeout and Other Settings* section in Cisco Prime Infrastructure User Guide. Note that the administrator must disable this feature *separately* , on *each* of the managed instances that Operations Center manages.
2. Instruct Operations Center users to disable the user-specific idle-user timeout feature for the managed instances they access, as explained in *Change Your Idle User Timeout* section in Cisco Prime Infrastructure User Guide. Note that each user must disable this feature *separately* , on *each* of the managed instances they access.

Related Topics

Set Up Operations Center, on page 4

Enable AAA for Operations Center

Operations Center supports local authentication as well as remote AAA using TACACS+ and RADIUS servers. Using remote AAA is optional, but if you want to use it, follow this workflow:

1. Complete the setup for TACACS+ or RADIUS in the remote server. See Use Cisco ACS With RADIUS or TACACS+ for External Authentication or Use Cisco ISE With RADIUS or TACACS+ for External Authentication
2. Login to Operations Center server and navigate to **Administration** > **Users** > **Users, Roles & AAA**
3. Add a TACACS+ or RADIUS server to Operations Center.
4. Click on **SSO Server Settings**. Depending on the remote server authentication, select TACACS+ or RADIUS under **SSO Server AAA** mode.
5. Click on Enable Fall-back to Local check box and select "On Authentication Failure or No Response from Server" from the drop-down list. Remember that the shared secret configured on the AAA server must match the shared secret.

Note Make sure you do not change the AAA setting under **Administration** > **Users** > **Users, Roles & AAA** > **AAA Mode Setting**. It should be in SSO mode only.

6. Perform steps to manage instance in Prime Infrastructure servers.

Note Prime Infrastructure Manage Instance will only fall back to TACACS+ or RADIUS if SSO server is unreachable or not responding.

What to do Next

When you have completed the setup tasks, you are ready to use Operations Center.

You can enable the Operations Center instance for High Availability (HA). HA uses a pair of linked, synchronized Prime Infrastructure servers, to minimize or eliminate the impact of application or hardware failures that may take place on either server. For details, see “Enable HA for Operations Center” in Related Topics

Related Topics

Set Up Operations Center, on page 4
Enable HA for Operations Center

Required Software Versions and Configurations

To work with , your devices must run at least the minimum required software versions shown in the list of supported devices. You can access this list using the user interface: Choose **Help > Supported Devices**.

You must also configure your devices to support SNMP traps and syslogs, and the Network Time Protocol (NTP), as explained in the related topics.

Related Topics

Configure SNMP, on page 8
Configure NTP, on page 9

Configure SNMP

To ensure that can query SNMP devices and receive traps and notifications from them, you must:

- Set SNMP credentials (community strings) on each device you want to manage using.
- Configure these same devices to send SNMP notifications to the server.

Use the following Cisco IOS configuration commands to set read/write and read-only community strings on an SNMP device:

- admin(config)# **snmp-server community** *private* **RW**
- admin(config)# **snmp-server community** *public* **RW**

where:

- *private* and *public* are the community strings you want to set.

After you set the community strings, you can specify that device notifications be sent as traps to the server using the following Cisco IOS global configuration command on each SNMP device:

admin(config)# **snmp-server host** *Host* **traps** *version community notification-type*

where:

- *Host* is the IP address of the server.
- *version* is the version of SNMP that is used to send the traps.
- *community* is the community string sent to the server with the notification operation.
- *notification-type* is the type of trap to send.

You may need to control bandwidth usage and the amount of trap information being sent to the server using additional commands.

For more information on configuring SNMP, see:

- The snmp-server community and snmp-server host commands in the Cisco IOS Network Management Command Reference.
- The Configuring SNMP Support section and the list of notification-type values in the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2.

If you are planning on implementing IPSec tunneling between your devices and the server, be advised that you will not receive syslogs transmitted from those devices to the server after implementing IPSec tunneling because IPSec does not support free-form syslogs. However, IPSec does support SNMP traps. To continue getting SNMP notifications of any kind from these devices, you need to configure your devices to send SNMP traps to the server.

Configure NTP

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the server. This includes all -related servers: any remote FTP servers that you use for backups, secondary high-availability servers, the Plug and Play Gateway, VMware vCenter and the ESX virtual machine, and so on.

You specify the default and secondary NTP servers during server installation. You can also use **ntp server** command to add to or change the list of NTP servers after installation. For details, see How to Connect Via CLI and the section on the **ntp server** command in the Command Reference Guide . Note that cannot be configured as an NTP server; it acts as an NTP client only.

Failure to manage NTP synchronization across your network can result in anomalous results in . Management of network time accuracy is an extensive subject that involves the organization's network architecture, and is outside the scope of this Guide. For more information on this topic, see (for example) the Cisco White Paper Network Time Protocol: Best Practices .

Configure Data Sources for With Assurance

If you are licensing the Assurance features, you must complete pre-installation tasks so that Assurance can monitor your network interfaces and services. See Supported Assurance Data Sources for information about these tasks.

Supported Assurance Data Sources

with Assurance needs to collect data from your network devices using the exported data sources shown in Table 1: Assurance: Supported Data Sources, Devices and Software Versions . For each source, the table shows the devices that support this form of export, and the minimum version of Cisco IOS or other software that must be running on the device to export the data.

Use Table 1: Assurance: Supported Data Sources, Devices and Software Versions to verify that your network devices and their software are compatible with the type of data sources uses. If needed, upgrade your hardware or software. Note that each software version given is a *minimum* . Your devices can run any later version of the same software or Cisco IOS release train.

You may also need to make changes to ensure that can collect data using SNMP, as explained in Configure SNMP.

Configure Assurance Data Sources

Before installing e, you should enable the supported devices shown in the below table to provide with fault, application, and performance data, and ensure that time and date information are consistent across your network. The following table provide guidelines on how to do this.

Table 1: Assurance: Supported Data Sources, Devices and Software Versions

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 the *Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches* section in the Cisco Prime Infrastructure User Guide.
' Catalyst 3850	15.0(1)EX	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, See the *Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches* section in the Cisco Prime Infrastructure User Guide. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > 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 the *Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches* section in the Cisco Prime Infrastructure User Guide. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > 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 the *Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches* section in the Cisco Prime Infrastructure User Guide. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
ISR	15.1(3) T	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics** To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**
ISR G2	15.2(1) T and 15.1(4)M	TCP and UDP traffic, application response time, Voice & Video	To configure TCP, UDP, and ART, see the *Configure NetFlow on ISR Devices* section in Cisco Prime Infrastructure User Guide. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > 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 the *Improve Application Performance With Application Visibility and Control* chapter in the Cisco Prime Infrastructure User Guide.
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		

Enable Medianet NetFlow

To ensure that Cisco can make use of Medianet data, your network devices must:

- Enable Medianet NetFlow data export for the basic set of statistics supported in .
- Export the Medianet NetfFlow data to the server and port.

Use a configuration like the following example to ensure that gets the Medianet data it needs:

- flow record type performance-monitor PerfMonRecord
- match ipv4 protocol
- match ipv4 source address
- match ipv4 destination address
- match transport source-port
- match transport destination-port

- collect application media bytes counter
- collect application media bytes rate
- collect application media packets counter
- collect application media packets rate
- collect application media event
- collect interface input
- collect counter bytes
- collect counter packets
- collect routing forwarding-status
- collect transport packets expected counter
- collect transport packets lost counter
- collect transport packets lost rate
- collect transport round-trip-time
- collect transport event packet-loss counter
- collect transport rtp jitter mean
- collect transport rtp jitter minimum
- collect transport rtp jitter maximum
- collect timestamp interval
- collect ipv4 dscp
- collect ipv4 ttl
- collect ipv4 source mask
- collect ipv4 destination mask
- collect monitor event
- flow monitor type performance-monitor PerfMon
- record PerfMonRecord
- exporter PerfMonExporter
- flow exporter PerfMonExporter
- destination PrInIP
- source Loopback0
- transport udp PiInPort
- transport udp PiInPort
- class class-default

- ! Enter flow monitor configuration mode.
- flow monitor PerfMon
- ! Enter RTP monitor metric configuration mode.
- monitor metric rtp
- !Specifies the minimum number of sequential packets required to identify a stream as being an RTP flow
- min-sequential 2
- ! Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring metrics.
- max-dropout 2
- max-reorder 4
- ! Enter IP-CBR monitor metric configuration mode
- monitor metric ip-cbr
- ! Rate for monitoring the metrics (1 packet per sec)
- rate layer3 packet 1
- interface interfacename
- service-policy type performance-monitor input PerfMonPolicy
- service-policy type performance-monitor output PerfMonPolicy

In this example configuration:

- *PrInIP* is the IP address of the server.
- *PiInPort* is the UDP port on which the server is listening for Medianet data (the default is 9991).
- *interfacename* is the name of the interface (such as GigabitEthernet0/0 or fastethernet 0/1) sending Medianet NetFlow data to the specified *PrInIP* .

For more information on Medianet configuration, see the Medianet Reference Guide.

Enable NetFlow and Flexible NetFlow

To ensure that can make use of NetFlow data, your network devices must:

- Have NetFlow enabled on the interfaces that you want to monitor.
- Export the NetFlow data to the server and port.

As of version 2.1, supports Flexible NetFlow versions 5 and 9. Note that you must enable NetFlow on each *physical* interface for which you want to collect data. These will normally be Ethernet or WAN interfaces. This applies to physical interfaces only. You do not need to enable NetFlow on VLANs and Tunnels, as they are included automatically whenever you enable NetFlow on a physical interface.

Use the following commands to enable NetFlow on Cisco IOS devices:

- Device(config)# interface interfaceName

- Device(config)# ip route-cache flow where *interfaceName* is the name of the interface (such as fastethernet or fastethernet0/1) on which you want to enable NetFlow.

Once NetFlow is enabled on your devices, you must configure exporters to export NetFlow data to . You can configure an exporter using these commands:

- Device(config)# ip flow-export version 5
- Device(config)# ip flow-export destination PrInIP PiInPort
- Device(config)# ip flow-export source interfaceName where:
- *PrInIP* is the IP address of the server.
- *PiInPort* is the UDP port on which the server is listening for NetFlow data. (The default is 9991.)
- *interfaceName* is the name of the interface sending NetFlow data to the specified *PrInIP* . This will cause the source interface's IP address to be sent to as part of NetFlow export datagrams.

If you configure multiple NetFlow exporters on the same router, make sure that only one of them exports to the server. If you have more than one exporter on the same router exporting to the same destination, you risk data corruption.

Use the following commands to verify that NetFlow is working on a device:

- Device# show ip flow export
- Device# show ip flow export
- Device# show ip cache flow
- Device# show ip cache verbose flow

For more information on NetFlow configuration, see:

- Cisco IOS Switching Services Configuration Guide, Release 12.2
- Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T
- Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting

Deploy Network Analysis Modules NAMs

Ensure that your NAMs are placed appropriately in the network. For more information, see:

- Cisco Network Analysis Module Software 5.1 User Guide — Includes deployment scenarios and covers a variety of topics, including deploying NAMs in the branch, and deploying NAMs for WAN optimization.
- Cisco Network Analysis Module Deployment Guide —See the section Places in the Network Where NAMs Are Deployed.

If your NAMs are deployed properly, then no other pre installation work is required. When you conduct discovery using Cisco Prime AM, you will need to enter HTTP access credentials for each of your NAMs.

uses a more efficient REST interface to query NAMs. For this reason, it does not support the direct export of NetFlow data from NAMs. Any device exporting NetFlow data must export that NetFlow data directly to , not via a NAM. Exporting NetFlow data from any NAM to will result in data duplication.

Enable Performance Agent

To ensure that can collect application performance data, use the Cisco IOS **mace** (for Measurement, Aggregation and Correlation Engine) keyword to configure Performance Agent (PA) data flow sources on your branch-office routers.

For example, use the following commands in Cisco IOS global configuration mode to configure a PA flow exporter on a router:

- Router (config)# flow exporter mace-export
- Router (config)# destination 172.30.104.128
- Router (config)# transport udp 9991
- Use commands like the following to configure flow records for applications with flows across the router:
  - Router (config)# flow record type mace mace-record
  - Router (config)# collect application name

Router (config)# collect art all where application name is the name of the application whose flow data you want to collect.To Configure teh PA flow Monitor type:

- Router (config)# flow monitor type mace mace-monitor
- Router (config)# record mace-record
- Router (config)# exporter mace-export

To collect traffic of interest, use commands like the following:

- Router (config)# **access-list 100 permit tcp any host 10.0.0.1 eq 80**
- Router (config)# **class-map match-any mace-traffic**
- Router (config)# **match access-group 100**

To configure a PA policy map and forward the PA traffic to the correct monitor:

- Router (config)# policy-map type mace mace_global
- Router (config)# class mace-traffic
- Router (config)# flow monitor mace-monitor

Finally, enable PA on the WAN interface:

- Router (config)# interface Serial0/0/0
- Router (config)# mace enable

For more information on configuring Performance Agent, see the Cisco Performance Agent Deployment Guide.

Install Patches

You may need to install patches to get your version of to the level at which upgrade is supported. You can check the version and patch version you are running by using the CLI commands **show version** and **show application**.

Different patch files are provided for each version of and its predecessor products. Download and install only the patch files that match the version of your existing system and that are required before you upgrade to a later version. You can find the appropriate patches by pointing your browser to the Cisco Download Software navigator .

Before installing a patch, you will need to copy the patch file to your server's default repository. Many users find it easy to do this by first downloading the patch file to a local FTP server, then copying it to the repository. You can also copy the patch file to the default repository using any of the following methods:

- cdrom—Local CD-ROM drive (read only)
- disk—Local hard disk storage
- ftp—URL using an FTP server
- http—URL using an HTTP server (read only)
- https—URL using an HTTPS server (read only)
- nfs—URL using an NFS server
- sftp—URL using an SFTP server
- tftp—URL using a TFTP server

Step 1 Download the appropriate point patch to a local resource in your environment:

a) With the Cisco Download Software navigator displayed in your browser, choose **Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions >** .
b) Select the version of that most closely matches the one you are currently using.
c) Click **Prime Infrastructure Patches** to see the list of available patches for that version of the product.
d) Next to each patch that is required, click **Download**, then follow the prompts to download the file.

Step 2 Open a command-line interface session with the server (see How to Connect Via CLI).

Step 3 Copy the downloaded patch file to the default local repository. For example:

admin# **copy** *source path*/**defaultRepo**

Where:

- *source* is the downloaded patch file's location and name.
- *path* is the complete path to the default local backup repository, defaultRepo (for example: /localdisk)

Step 4 Install the patch:

admin# **patch install** *patchFile Repositoryname*

Where:

- *patchFile* is the name of the patch file you copied to /localdisk/defaultRepo

- *Repositoryname* is the name of the repository

For example: admin# patch install test.tar.gz defaultRepo