Cisco CNS NetFlow Collection Engine Installation and Configuration Guide, 5.0.2

February, 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: N/A
Text Part Number: OL-6900-01

Cisco CNS NetFlow Collection Engine Installation and Configuration Guide, 5.0.2

CONTENTS

Supplemental License Agreement

Supplemental License Agreement For Cisco Systems Network Management Software: Cisco NetFlow Collection Engine

IMPORTANT–READ CAREFULLY: This Supplemental License Agreement (“SLA”) contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download, or otherwise use the Software. When used below, the term “server” refers to central processor unit.

Additional License Restrictions

Installation and Use

The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Some license terms such as device count and proof of preexisting licenses may be electronically enforced. Customer may install and use following Software components:

Cisco NetFlow Collection Engine Software: May be installed on one (1) server in Customer's network management environment.

Reproduction and Distribution

Customer may not reproduce nor distribute software.

Description Of Other Rights and Limitations

Please refer to the Cisco Systems, Inc. Software License Agreement.

About This Guide

Objective

The *Cisco CNS NetFlow Collection Engine Installation and Configuration Guide, Release 5.0.2* describes the CNS NetFlow Collection Engine application, which is used with the NetFlow services data export feature on Cisco routers and Catalyst 5000 and 6000 series switches. This document also describes the system requirements that must be met to install the CNS NetFlow Collection Engine product, as well as, how to install, start, and configure CNS NetFlow Collection Engine.

NetFlow services consist of high-performance IP switching features that capture a rich set of traffic statistics exported from routers and switches while they perform their switching function. CNS NetFlow Collection Engine provides fast, scalable, and economical data collection from multiple export devices exporting NetFlow data records.

Prior to reading this manual, you should read the *Release Notes for Cisco CNS NetFlow Collection Engine Release 5.0.2* document. These release notes provide information about known software and documentation problems and any last minute information about the CNS NetFlow Collection Engine software not available when this guide was produced.

In previous releases, this product was referred to as Cisco NetFlow FlowCollector (NFC).

Audience

This guide is intended primarily for individuals with network and system administration skills. You should have a basic understanding of network design, operation, and terminology, as well as familiarity with your own network configurations. You also must have a basic familiarity with Web browsers, Hewlett Packard's HP-UX, or Sun Microsystem's Solaris Operating System.

How This Guide Is Organized

This guide is organized as follows:

Chapter 1, “Overview,” describes the CNS NetFlow Collection Engine application.

Chapter 2, “Installing CNS NetFlow Collection Engine,” describes how to install the CNS NetFlow Collection Engine.

Chapter 3, “Configuring CNS NetFlow Collection Engine,” describes how to configure CNS NetFlow Collection Engine and then validate that it s operating properly.

An Index is also provided.

Command Syntax Conventions

Table 1 describes the syntax used with the commands in this document.

Table 1 Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen font`	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco Technical Support Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco Technical Support Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco Technical Support Web Site

The Cisco Technical Support Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco Technical Support Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco Technical Support Web Site. The Cisco Technical Support Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco Technical Support Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco Technical Support Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Overview

This chapter describes the CNS NetFlow Collection Engine application, which is used with the NetFlow services data export feature on Cisco routers and Catalyst 5000 and 6000 series switches.

This chapter includes the following sections:

- What Are NetFlow Services?
- What Is CNS NetFlow Collection Engine?
- CNS NetFlow Collection Engine Architectural Overview

What Are NetFlow Services?

NetFlow services consist of high-performance IP switching features that capture a rich set of traffic statistics exported from routers and switches while they perform their switching functions. The exported NetFlow data consists of traffic flows, which are unidirectional sequences of packets between a particular source device and destination device that share the same protocol and transport-layer information. The captured traffic statistics can be used for a wide variety of purposes, such as network analysis and planning, network management, accounting, billing, and data mining.

Because of their unidirectional nature, flows from a client to a server are differentiated from flows from the server to the client. Flows are also differentiated on the basis of protocol. For example, Hypertext Transfer Protocol (HTTP) Web packets from a particular source host to a particular destination host constitute a separate flow from File Transfer Protocol (FTP) file transfer packets between the same pair of hosts.

Routers and switches identify flows by looking for the following fields within IP packets:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol type
- Type of service (ToS)
- Input interface

Catalyst 5000 series switches can identify flows by looking at a subset of these fields. For example, they can identify flows by source and destination address only.

Note For Catalyst 5000 series switches, the analog to NetFlow services is integrated Multilayer Switching (MLS) management. Included are products, utilities, and partner applications designed to gather flow statistics, export the statistics, and collect and perform data reduction on the exported statistics. MLS management then forwards them to consumer applications for traffic monitoring, planning, and accounting.

NetFlow Services Device and IOS Release Support

You can find the most up-to-date information available to help you determine the compatibility among different Cisco hardware platforms, Cisco IOS software releases, and supported NetFlow data export versions at the following URL:

http://tools.cisco.com/ITDIT/CFN/Dispatch?SearchText=Netflow&act=featSelect&rnFeatId=null&featStartsWith=&task=TextSearch&altrole=

Note Except for descriptions requiring references to specific router or switch platforms, the remainder of this chapter and the remaining chapters of this guide use the term export device instead of the terms router and switch.

NetFlow Data Export

NetFlow data export makes NetFlow traffic statistics available for purposes of network planning, billing, and so on. An export device configured for NetFlow data export maintains a flow cache used to capture flow-based traffic statistics. Traffic statistics for each active flow are maintained in the cache and are updated when packets within each flow are switched. Periodically, summary traffic statistics for all expired flows are exported from the export device by means of User Datagram Protocol (UDP) datagrams, which CNS NetFlow Collection Engine receives and processes.

How and When Flow Statistics Are Exported

NetFlow data exported from the export device contains NetFlow statistics for the flow cache entries that have expired since the last export. Flow cache entries expire and are flushed from the cache when one of the following conditions occurs:

- The transport protocol indicates that the connection is completed (TCP FIN) plus a small delay to allow for the completion of the FIN acknowledgment handshaking.
- Traffic inactivity exceeds 15 seconds.

For flows that remain continuously active, flow cache entries currently expire every 30 minutes to ensure periodic reporting of active flows.

NetFlow data export packets are sent to a user-specified destination, such as the workstation running CNS NetFlow Collection Engine, either when the number of recently expired flows reaches a predetermined maximum, or every second-whichever occurs first. For:

- Version 1 datagrams, up to 24 flows can be sent in a single UDP datagram of approximately 1200 bytes.

- Version 5 datagrams, up to 30 flows can be sent in a single UDP datagram of approximately 1500 bytes.
- Version 7 datagrams, up to 27 flows can be sent in a single UDP datagram of approximately 1500 bytes.
- Version 8 datagrams, the number of flows sent in a single UDP datagram varies by aggregation scheme.
- Version 9 datagrams, the number of flows is variable, and depends on the number and size of fields defined in one or more templates.

See Appendix B, "NetFlow Export Datagram Formats," in the *CNS NetFlow Collection Engine User Guide* for details on all versions of the NetFlow data export format.

NetFlow Data Export Formats

NetFlow exports flow information in UDP datagrams in one of five formats: Version 1 (V1), Version 5 (V5), Version 7 (V7), Version 8 (V8), or Version 9 (V9).

Version 1 is the original format supported in the initial NetFlow releases. Version 5 is an enhancement that adds Border Gateway Protocol (BGP) autonomous system information and flow sequence numbers. Version 7 is an enhancement that exclusively supports Cisco Catalyst 5000 series switches equipped with a NetFlow feature card (NFFC). V7 is not compatible with Cisco routers. Version 8 is an enhancement that adds router-based aggregation schemes. Version 9 is an enhancement to support different technologies such as Multicast, Internet Protocol Security (IPSec), and Multi Protocol Label Switching (MPLS). CNS NetFlow Collection Engine Release 5.0 can collect, filter, and aggregate Version 9 data in the same way it does for NetFlow Data Export Versions 1 through 8.

Versions 2, 3, 4, and 6 are not supported by CNS NetFlow Collection Engine. For more information on the distinctions among the NetFlow data export formats, see Appendix B, "NetFlow Export Datagram Formats," in the *CNS NetFlow Collection Engine User Guide.*

The following types of information are part of the detailed traffic statistics:

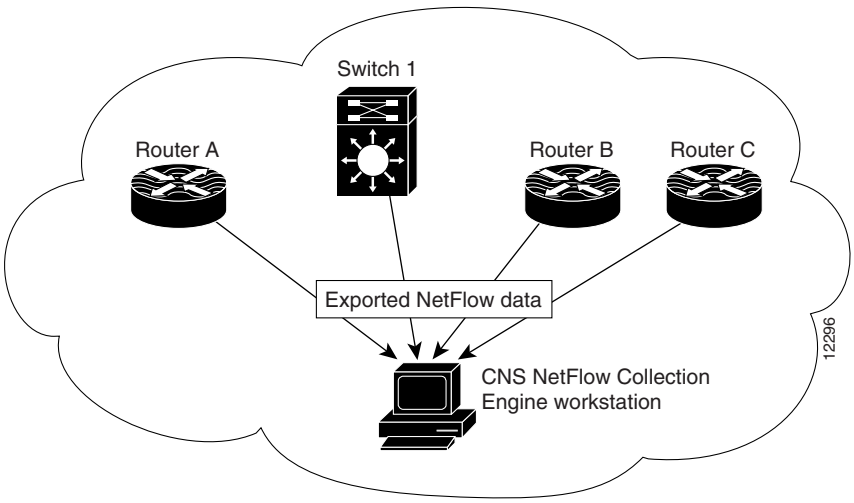
- Source and destination IP addresses
- Next hop address
- Input and output interface numbers
- Number of packets in the flow
- Total bytes (octets) in the flow
- First and last time stamps of packets that were switched as part of this flow
- Source and destination port numbers
- Protocol
- Type of service (ToS)
- Source and destination autonomous system (AS) numbers, either origin or peer (present in V5 and select V8 datagrams)
- Source and destination prefix mask bits (present in V5, V7, and V8 datagrams)
- Shortcut router IP address (present in V7 on Cisco Catalyst 5000 series switches only).

Caution Throughout this publication there are numerous examples of CNS NetFlow Collection Engine input commands and output results. Included are examples of IP addresses. Be aware that IP address examples are not usable IP addresses. The examples do not represent real-life configurations.

What Is CNS NetFlow Collection Engine?

CNS NetFlow Collection Engine provides fast, scalable, and economical data collection from multiple export devices exporting NetFlow data records. Figure 1-1 shows an example of a typical NetFlow data export scheme. In it, various export devices send export data to user-specified CNS NetFlow Collection Engine UDP ports.

Figure 1-1 CNS NetFlow Collection Engine Overview



Each of the export devices in this example is configured for NetFlow data export. Part of the configuration information for each export device includes the IP address and the UDP port number (a logical port designator) that identify CNS NetFlow Collection Engine as the receiver of flows from this export device. The UDP port number is a user-configurable designator: you can configure CNS NetFlow Collection Engine to listen for flows on a number of different UDP ports, and then configure your export devices so that each device exports flows to a dedicated UDP port, or have a number of devices export flows to the same, shared UDP port.

After you configure and start CNS NetFlow Collection Engine, it listens to the user-specified UDP ports for exported flows from the export devices you have configured for NetFlow data export.

CNS NetFlow Collection Engine performs the following functions:

- NetFlow data collection from multiple export devices
- Reduction in data volume through filtering and aggregation
- Hierarchical data storage (helps client applications retrieve data)
- File system space management

CNS NetFlow Collection Engine collects and summarizes (aggregates) data into data files based on user-defined criteria specified in a CNS NetFlow Collection Engine *aggregator*. An *aggregator* is an aggregation task defined by a set of user-configurable attributes that specify how CNS NetFlow Collection Engine summarizes the traffic flows that are received. Two important aggregator attributes are:

- Aggregation schemes – defines the subset of data of interest in a traffic flow, as well as which statistics are kept
- Filter – criteria for accepting or rejecting flows that are aggregated or summarized

CNS NetFlow Collection Engine provides a set of predefined aggregation schemes to help you collect NetFlow export data and summarize the data (that is, aggregate the flows). You can choose one or more of these aggregation schemes to customize CNS NetFlow Collection Engine for your operating context. Moreover, in Release 5.0 you can modify any of the predefined aggregation schemes or define your own aggregation schemes based on them. You can also use filters with aggregation schemes to include or exclude certain types of NetFlow data.

For more information about threads, aggregation schemes, and filters, see Chapter 4, "Customizing the CNS NetFlow Collection Engine," in the *CNS NetFlow Collection Engine User Guide*.

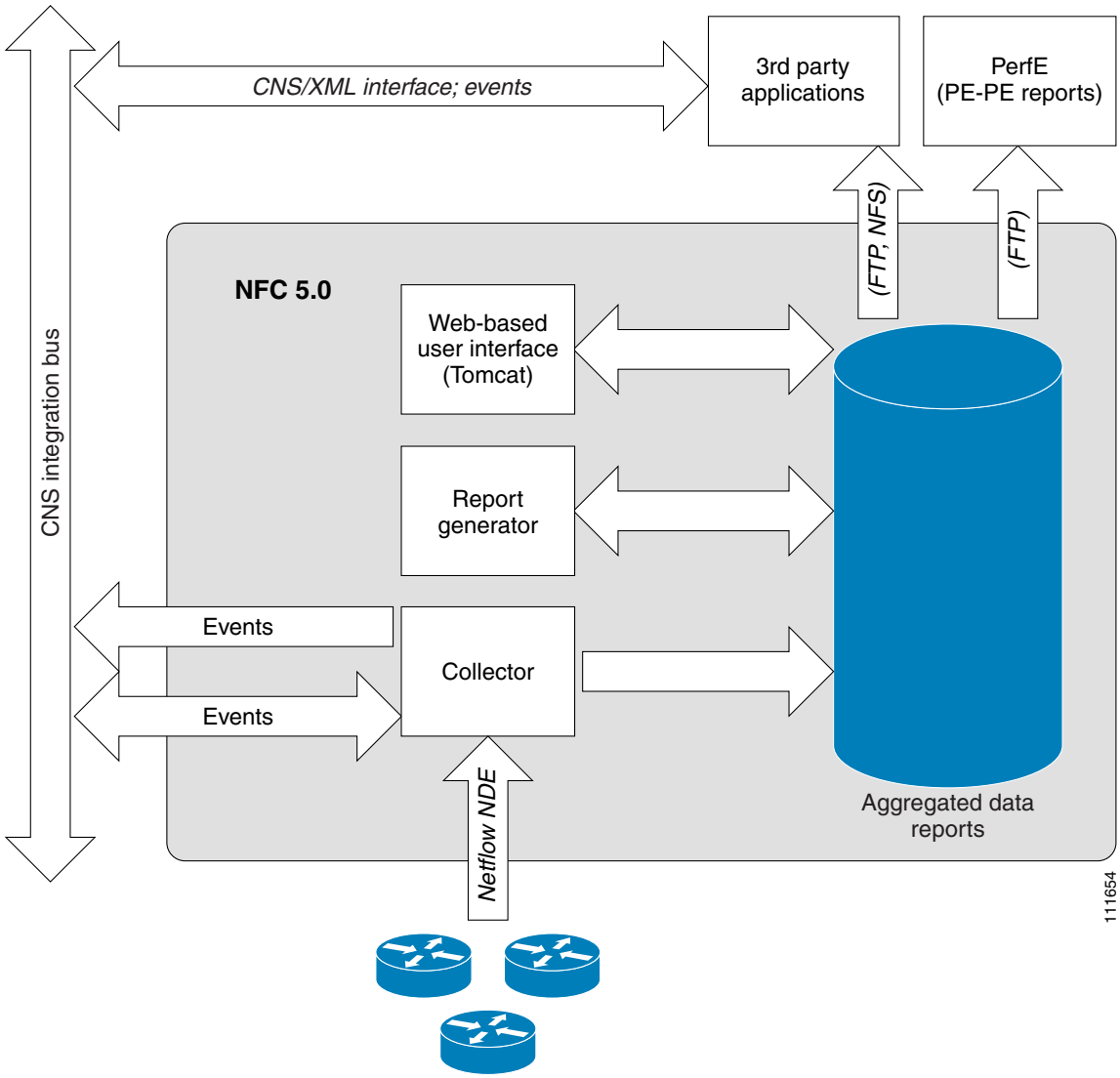
CNS NetFlow Collection Engine Architectural Overview

CNS NetFlow Collection Engine consists of the following components:

- Collector
- Web-based User Interface (UI)
- CNS/XML Interface
- Reporting engine
- Border Gateway Protocol (BGP) Peer

These subsystems work together to provide CNS NetFlow Collection Engine functionality, including data collection, the user interface, configuration and control, and reporting. They also allow custom client applications to interface with CNS NetFlow Collection Engine. See Figure 1-2 for a graphical representation of the CNS NetFlow Collection Engine system architecture.

Figure 1-2 CNS NetFlow Collection Engine System Architecture



Collector

The Collector subsystem collects NetFlow data, aggregates (or summarizes) that data, and filters specified data from supported Cisco routers and switches. Output is stored in files that are organized in an easy-to-use directory structure.

Web-Based User Interface

The Web-Based User Interface is provided for configuration, control, status, and reporting.

CNS/XML Interface

The CNS/XML Interface is used to send and receive configuration/control requests and responses, and unsolicited event notifications. The CNS/XML interface uses the CNS Integration Bus to communicate with clients.

Report Generator

The Report Generator produces hourly and daily reports based on Collector output files by performing further aggregation of the records in these files based on criteria selected by the user.

BGP Peer

A passive BGP peer is provided for supplementing CNS NetFlow Collection Engine output with BGP attributes.

Installing CNS NetFlow Collection Engine

This chapter describes how to install Cisco CNS NetFlow Collection Engine.

This chapter includes the following sections:

Verifying System Requirements

CNS NetFlow Collection Engine, Release 5.0 has the following hardware requirements:

- Minimum of 1 GB RAM, 10K SCSI, 30 GB disk, single processor on an entry-level server.
- Recommended: 4 GB RAM, 15K Ultra 320 SCSI, dual 70 GB disks, dual processors on an entry-level server.

The following operating systems and platforms are supported:

- Solaris 8 and Solaris 9 on an entry-level server, such as the Sun Fire 280R with 1 GHz or greater UltraSPARC III or IIIi processors.
- HP-UX Version 11i for PA-RISC on an entry-level server, such as the rp2400 series.
- Red Hat Enterprise Linux 2.1 or 3 ES on an entry-level server, such as an IBM x336 with 2.8 GHz or greater Intel Xeon processors.

Note that the CPU, RAM, and disk space recommendations above are minimum requirements, and that actual requirements are determined by your configuration and by the volume and *uniqueness* of NetFlow data that is received. Actual resource usage can vary greatly depending on these factors.

Note To prevent NetFlow data export packet loss, the workstation should be dedicated to the CNS NetFlow Collection Engine and should not be running other applications.

The CNS NetFlow Collection Engine generates output files containing aggregated data. The exact amount of disk space the output files require depends on the flow arrival rate, collection interval, number of aggregation schemes specified, use of compression or not, and data file retention policies.

For more information on planning and managing memory usage, see the"Tuning Memory Usage"section of the *Cisco CNS NetFlow Collection Engine User Guide*. For more information on planning and managing disk space usage, see the "Managing Disk Space" section of the *Cisco CNS NetFlow Collection Engine User Guide*.

Using the CNS NetFlow Collection Engine Installation Script

The CNS NetFlow Collection Engine is distributed on CD-ROM. Updates are made available at http://www.cisco.com. When installing from the CD-ROM:

- Run the install script **setup.sh** in the root directory of the CD-ROM.

When downloading an update:

- Identify a partition such as **/tmp** that you can use to hold the CNS NetFlow Collection Engine download and image files.

Note You should verify that the partition you plan to use contains at least 200 MB of free disk space. This partition must be large enough to hold the gzipped download file, distribution files, and the temporary work files created by the installation script while it is installing the CNS NetFlow Collection Engine.

- Unzip and untar the download file.
- Run the installation script **NFC_setup.sh**.

The CNS NetFlow Collection Engine installation script makes the installation process as easy as possible by automatically handling new and upgrade installation issues. The installation script searches for files from a previously installed version of CNS NetFlow Collection Engine. If it detects a previously installed version, it preserves existing data and configuration files. Preserving the configuration files retains any additions or changes to the CNS NetFlow Collection Engine resource definitions or parameter settings that you might have made while using the previously installed version of CNS NetFlow Collection Engine.

Later in the installation process, the installation script allows you to specify whether you want to use the existing configuration files, or use the new configuration files. Depending on your choice, the unused files are saved in case you need them later.

The installation script also saves existing log files before clearing the logs directory during an upgrade.

Note If the installation script does not find files from a previously installed version of CNS NetFlow Collection Engine, the installation is a first-time installation and is basically the same as for an upgrade installation, but with fewer prompts from the installation script. The installation script prompts you for responses to any required steps.

Installing on a Solaris or HP-UX Platform

The procedure for installing CNS NetFlow Collection Engine on Solaris and HP-UX are nearly identical. The primary difference is in the output written by the platform installation programs (**pkgadd** on Solaris and **swinstall** on HP-UX.

If you are installing CNS NetFlow Collection Engine for the first time, the installation is basically the same, but with fewer prompts from the installation script.

Note During an upgrade installation, existing configuration files and log files are detected and moved to the directories **NFC_DIR/config/old** and **NFC_DIR/logs/old**, respectively.

To install the CNS NetFlow Collection Engine, perform the following steps:

Step 1 Log into the host as root.

Step 2 Perform one of the following:

a. When installing from CD-ROM, run **setup.sh** in the CD-ROM base directory.

b. When downloading the image over the web:

- Download the zipped distribution file to a directory with at least 200 MB of available space.
- Unzip and untar the distribution with gzcat and tar:

```
gzcat <download-file> | tar xf -
```

The following files are created:

NFC_setup.sh – Install script

CSCOnfc-<platform>-<version>-<build>.<type> – Install image. For example **CSCOnfc-solaris- 5.0-2.standard**

- Run the install script specifying the install image as the argument, for example:

```
./NFC_setup.sh CSCOnfc-solaris-5.0-2.standard
```

Note On Solaris, the install image **CSCOnfc-<platform>-<version>- <build>.<type>** is a software package file in the format recognized by the Solaris install program **pkgadd**. On HP-UX, it is a directory containing files for the HP-UX install program **swinstall**.

Note Software can only be installed in the directory **/opt/CSCOnfc**. If some other directory is desired, create a symbolic link to **/opt/CSCOnfc** before installing the software.

The following example illustrates these steps. The installation script is invoked while logged in as root.

Example

```
# ./NFC_setup.sh CSCOnfc-solaris-5.0-2.standard
Fri Jan  2 14:00:01 EST 2004

Using software package /var/tmp/./CSCOnfc-solaris-5.0-2.standard.

*********************************************************************

CNS Netflow Collection Engine 5.0.2 [standard image, build 2]
Copyright (c) 2003-2005 by Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute
or use encryption. Importers, exporters, distributors and users
are responsible for compliance with U.S. and local country laws.

By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local
laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to export@cisco.com.

*********************************************************************

Press Return to continue...
```

Step 3 Press return when prompted after the banner page is displayed.

Step 4 Unlike earlier releases of the CNS Netflow Collection Engine, programs are not installed with setuid-to-bin permission. Therefore, you must select an existing user ID as the owner of installed files and NFC processes:

```
An existing userid must be selected as the owner of NFC files and
processes.

Enter userid: bin
```

In this example, the bin account was specified. Note that the account must already exist on the system. If it does not, an error is indicated and the install is terminated.

File ownership is set to the specified user. Also, if the autostart option is selected later during the installation, the CNS Netflow Collection Engine processes are owned by this user when started at system initialization. Otherwise, the CNS Netflow Collection Engine must be started manually by this user; if not, the CNS Netflow Collection Engine will not have write permission for its files and directories.

Step 5 Next, the install script checks whether the CNS Netflow Collection Engine is already installed and verifies that the CNS Netflow Collection Engine is not running on the system:

```
Found existing installation: 4.0 in /opt/CSCOnfc.

Verifying that NFC is not running...
```

If the CNS Netflow Collection Engine is running, an error is indicated and the install is terminated. You must first stop all NFC processes.

Next, if the CNS Netflow Collection Engine was already installed, all files under **NFC_DIR/logs** are automatically moved to the directory **NFC_DIR/logs/old**, and all files under **NFC_DIR/config** are moved to N**FC_DIR/config/old**. The previous installation is then removed using **pkgrm** on Solaris or **swremove** on HP-UX:

```
Saving old config, logs, and data files...

Removing previous NFC package...
```

Note that all output files under **NFC_DIR/Data** and all **filesready** files in the logs directory are preserved.

The new package is then installed. If you are installing CNS NetFlow Collection Engine on a Solaris platform, proceed to Step 6. Otherwise, proceed to step 9.

Step 6 If CNS NetFlow Collection Engine is already installed on the system, the **pkgrm** program prompts whether to remove the previously installed package. Enter **y**:

```
The following package is currently installed:

   CSCOnfc         Cisco CNS NetFlow Collection Engine
                   (Solaris2.8) 5.0 [standard image, build 23]

Do you want to remove this package? y
```

Step 7 The **pkgadd** program prompts whether to install the new package, to which you should press return (or specify **all**):

```
The following packages are available:
  1  CSCOnfc     Cisco CNS NetFlow Collection Engine
                 (Solaris2.8) 5.0 [standard image, build 2]

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Step 8 The **pkgadd** program also detects that certain files and directories remaining from the previous installation are no longer owned by a package and prompts whether to install the new files at that location. You should respond **y**:

```
The following files are already installed on the system and are being
used by another package:
* /opt/CSCOnfc/Data <attribute change only>
* /opt/CSCOnfc/config <attribute change only>
* /opt/CSCOnfc/logs <attribute change only>
* /opt/CSCOnfc/tomcat <attribute change only>
* /opt/CSCOnfc/tomcat/conf <attribute change only>

* - conflict with a file which does not belong to any package.

Do you want to install these conflicting files [y,n,?,q] y
```

Step 9 If a previous installation was detected, you are prompted whether to use old configuration files or to install new configuration files:

```
Please choose one of the following..

(1) Install new default configuration files
    (Your existing configuration files have been saved in the
    config/old subdirectory should you want to refer to them later)

(2) Retain existing configuration files
    (New default configuration files will be saved with '.default'
    extensions should you want to refer to them later)

Please choose: 1
```

If option **1** is selected, previous files are kept in the **NDC_DIR/config/old** subdirectory as indicated. If option **2** is selected, new configuration files are saved with the **.default** suffix, and the previous installation's configuration files are retained.

a. When upgrading to CNS Netflow Collection Engine, Release 5.0 from version 4 or earlier, the previous configuration is not backwards compatible so this prompt is not displayed. A tool is provided to assist the user with migrating their previous configuration. See Appendix G, "CNS NetFlow Collection Engine Migration Tools."[link] for additional details.

b. When upgrading to CNS Netflow Collection Engine, Release 5.0.2 from version 5.0 or 5.0.1 and option **2** is selected, a migration script is run to automatically migrate minor changes in the XML configuration format for release 5.0.2. Before the migration, the following is displayed:

```
Preparing to migrate 5.0/5.0.1 configuration...

Please carefully note any instructions given during the migration
since some configuration options have changed in this release.
```

After the migration, the following is displayed:

```
Successfully migrated /opt/CSCOnfc/config/nfc-config.xml.
Please carefully note any instructions above regarding additional
configuration updates that might be needed.
```

In certain unusual cases, this can be preceded by additional information about a configuration incompatibility that cannot be resolved automatically. In that case, refer to details about configuration format updates introduced in CNS Netflow Collection Engine, Release 5.0.2 in the Release Notes for Cisco CNS NetFlow Collection Engine, 5.0.2.

Step 10 Ownership of all files under the install directory **/opt/CSCOnfc** is set to the user that was specified earlier; group ownership is set to that user's default group.

```
Setting file ownership...
```

Next, operating system-specific configuration is verified:

```
Checking platform config...
```

This includes verifying that the data segment size limit returned by **ulimit –d** is sufficient. If not, a warning message is displayed, and you should consult the platform system administration guide to determine how this value is updated. This value should be at least the maximum size specified for the collector process as described at [link to memory tuning section of customizing chapter].

Step 11 You are asked whether CNS Netflow Collection Engine should be started automatically when the system initializes:

```
Would you like NFC to be started when the system initializes? (y/n) y
```

If you respond **y**, the following rc scripts are created for autostarting CNS Netflow Collection Engine when the system initializes:

- *rcdir*/init.d/csco_nfcd
- *rcdir*/rc3.d/S999csco_nfcd (symbolic link to **../init.d/csco_nfcd**)
- *rcdir*/rc2.d/K999csco_nfcd (symbolic link to **../init.d/csco_nfcd**)

On Solaris, *rcdir* is **/etc**; on HP-UX it is **/sbin**.

The record of this installation session is saved in **/opt/CSCOnfc/logs/nfc_install.log**.

Note When CNS Netflow Collection Engine is uninstalled from the system, you must remove these files yourself after the uninstall completes.

Installing on a Red Hat Enterprise Linux Platform

Note When reinstalling the same or an earlier version of CNS Netflow Collection Engine than is currently installed on a Red Hat Enterprise Linux platform, you must first remove the currently-installed package by running **rpm -e CSCOnfc**.

To install CNS NetFlow Collection Engine Release 5.0 on a Red Hat Enterprise Linux platform, perform the following steps:

Note During an upgrade installation, existing configuration files and data files are detected and moved to the directories **NFC_DIR/config/old** and **NFC_DIR/logs/old**, respectively.

Step 1 Log into the host as root.

Step 2 Perform one of the following:

a. If installing from CD-ROM, run **setup.sh** in the CD-ROM base directory.

b. If downloading the image over the web:

- Download the distribution file to a directory with as least 200 MB of available space.
- Untar the distribution tar:

  tar xf <download-file>

  The following files are created:

  NFC_setup.sh (the install script)

  CSCOnfc-linux- <version>-<build>.<type>.i386.rpm (the install image)
- Run the install script specifying the install image as the argument, for example:

  ./NFC_setup.sh CSCOnfc-linux-5.0-4.standard.i386.rpm

Note On Linux, the install image **CSCOnfc-linux-<version>- <build>.<type>.i386.rpm** is an RPM package file in the format recognized by the Red Hat RPM program

Note Software can only be installed in the directory **/opt/CSCOnfc**. If some other directory is desired, create a symbolic link to **/opt/CSCOnfc** before installing the software.

The following example illustrates these steps. The installation script is invoked while logged in as root.

```
#./NFC_setup.sh CSCOnfc-5.0-4.standard.i386.rpm

Thu Mar 4 15:58:12 EST 2004
./NFC_setup.sh CSCOnfc-5.0-4.standard.i386.rpm

*********************************************************************

CNS Netflow Collection Engine 5.0.2 [standard image, build 4]
Copyright (c) 2003-2005 by Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute
or use encryption. Importers, exporters, distributors and users
are responsible for compliance with U.S. and local country laws.

By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local
laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to export@cisco.com.

*********************************************************************

Hit Return to continue...
```

Step 3 Press return when prompted after the banner page is displayed.

Step 4 The install script checks whether the CNS Netflow Collection Engine is already installed and verifies that the CNS Netflow Collection Engine is not running on the system:

```
Searching for existing copy of CSCOnfc..
Found previous copy of CSCOnfc, performing upgrade...
```

If the CNS Netflow Collection Engine is running, an error is indicated and the install is terminated. You must stop all NFC processes before attempting to install CNS NetFlow Collection Engine on a Red Hat Enterprise Linux platform.

If the CNS Netflow Collection Engine was already installed, all files under **NFC_DIR/logs** are automatically moved to the directory **NFC_DIR/logs/old**, and all files under **NFC_DIR/config** are moved to **NFC_DIR/config/old**.

Note that all output files under **NFC_DIR/Data** and all **filesready** files in the logs directory are preserved.

See Appendix G, "CNS NetFlow Collection Engine Migration Tools," of the *Cisco CNS NetFlow Collection Engine User Guide* for information on the CNS NetFlow Collection Engine Release 5.0 migration tool.

Note When upgrading to CNS Netflow Collection Engine, Release 5.0.2 from version 5.0 or 5.0.1, a migration script is run to automatically migrate minor changes in the XML configuration format for release 5.0.2. In certain unusual cases, additional information may be displayed in Step 7 below about a configuration incompatibility that cannot be resolved automatically. In that case, refer to details about configuration format updates introduced in CNS Netflow Collection Engine, Release 5.0.2 in the Release Notes for Cisco CNS NetFlow Collection Engine, 5.0.2.

Step 5 Unlike earlier releases of the CNS Netflow Collection Engine, programs are not installed with **setuid-to-bin** permission. As a result, you must select an existing userid as the owner of installed files and NFC processes:

```
Enter the existing user account that will run NetFlow Collector [nfcuser]: nfcuser
```

In this example, the **nfcuser** account was specified. If this account does not already exist on the system then it will be created with a password and group equal to the username.

File ownership is set to the specified user. Also, if the autostart option is selected later during the installation, the CNS Netflow Collection Engine processes are owned by this user when started at system initialization. Otherwise, the CNS Netflow Collection Engine must be started manually by this user; if not, the CNS Netflow Collection Engine will not have write permission for its files and directories.

Step 6 Specify whether the CNS Netflow Collection Engine should be started automatically when the system initializes:

```
Would you like the Flow Collector applications to be
automatically started when the system is initialized?  (y/n)? y
```

If you respond **y**, the following rc scripts are created for autostarting CNS Netflow Collection Engine when the system initializes and autostopping at shutdown:

- *rcdir*/init.d/csco_nfcd
- *rcdir*/rc0.d/K99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)
- *rcdir*/rc1.d/K99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)
- *rcdir*/rc2.d/S99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)
- *rcdir*/rc3.d/S99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)

- *rcdir*/rc4.d/S99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)
- *rcdir*/rc5.d/S99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)
- *rcdir*/rc6.d/K99csco_nfcd (symbolic link to **../init.d/csco_nfcd**)

On Red Hat Enterprise Linux, **rcdir** is **/etc/rc.d**.

Note When CNS Netflow Collection Engine is uninstalled from the system, if you have modified any of these files you must remove them yourself after the uninstall completes.

Step 7 The operating system-specific configuration is verified:

```
Checking system tunable parameters ...
Validation successful
```

This includes verifying that the data segment size limit returned by **ulimit -d** is sufficient. If not, a warning message is displayed, and you should consult the platform system administration guide to determine how this value is updated. This value should be at least the maximum size specified for the collector process as described in the "Tuning Memory Usage" section on page 4-26 in the *Cisco CNS NetFlow Collection Engine User Guide*.

The new package is then installed.

```
...Starting FlowCollector Install ....
FlowCollector installation completed successfully.
```

The record of this installation session is saved in **/opt/CSCOnfc/logs/nfc_install.log**.

Uninstalling CNS NetFlow Collection Engine 5.0

To uninstall and remove all files for CNS NetFlow Collection Engine Release 5.0, log in as **root** and run the following:

- On a Solaris platform: **pkgrm CSCOnfc**
- On an HP-UX platform: **swremove CSCOnfc**
- On a Red Hat Enterprise Linux platform: **rpm -e CSCOnfc**

During installation, if you specified to automatically start CNS Netflow Collection Engine when the system initializes, remove the **rcdir** files described in Step 11 for installing on a Solaris or HP-UX platform, or in Step 6 for installing on a Red Hat Enterprise Linux platform.

Recursively remove the installation directory **/opt/CSCOnfc** and the files it contains.

Configuring CNS NetFlow Collection Engine

This chapter describes how to configure Cisco CNS NetFlow Collection Engine and then validate that it is operating properly.

This chapter includes the following sections:

Required Patches and Software Packages

Solaris Platform

On the Solaris platform, the following patch should be installed on the system prior to running CNS NetFlow Collection Engine:

- "32-Bit Shared library patch for C++" (108434-13 or later for Solaris 8, 111711-06 or later for Solaris 9)

Solaris patches can be downloaded at http://sunsolve.sun.com/.

Red Hat Enterprise Linux Platform

On Red Hat Enterprise Linux platform, the following packages must be installed on the system prior to running CNS NetFlow Collection Engine:

- The X Windows package must be installed for the web-based user interface to function properly. This is part of the default system configuration when Red Hat Enterprise Linux is installed; otherwise refer to Red Hat Enterprise Linux documentation for further instructions.
- For Red Hat Enterprise 3, you must ensure that the compat-libstdc++ RPM is installed on the system. This RPM is included in the Red Hat Enterprise 3 distribution CDs.

UNIX Environment Variables

In releases prior to version 5.0, the CNS NetFlow Collection Engine Installation Guide recommended setting a number of environment variables, such as **NFC_DIR** and **NFC_RESOURCEFILE**. These settings should be removed from the environment for this release prior to installing and running CNS NetFlow Collection Engine. The environment is automatically determined by startup scripts in the 5.0 release.

Enabling NetFlow Data Export

Because of the configuration differences between routers and switches, any detailed configuration description for either type of NetFlow export device is beyond the scope of this guide. At the broadest conceptual level, you must perform the following types of configuration tasks on the export devices:

- Enable NetFlow services on Cisco routers; enable Multilayer Switching (MLS) on Catalyst 5000 series switches equipped with an NFFC.
- Specify the IP address and the UDP port number used to identify CNS NetFlow Collection Engine as the receiver of exported NetFlow data. In a default CNS NetFlow Collection Engine installation, UDP ports 9995 and 9996 are automatically configured as the UDP ports CNS NetFlow Collection Engine uses to receive NetFlow exported data.
- Enable NetFlow data export.

For information on Cisco IOS software features related to NetFlow services on Cisco routers, see the Cisco IOS software configuration guides and command references.

For information on specific configuration commands for Cisco Catalyst 5000 series switches, see the "**NetFlow Switching Enhancements**" feature module in Cisco IOS release notes and feature modules.

For information on software features related to MLS on Catalyst 5000 series switches, see the *Catalyst 5000 Series Multilayer Switching User Guide*.

Starting CNS NetFlow Collection Engine

To start CNS NetFlow Collection Engine, you must be logged in as the user specified during installation. Beginning in version 5.0, CNS NetFlow Collection Engine executables no longer have setuid-to-bin permission.

Step 1 To run CNS NetFlow Collection Engine, log in as the user specified during installation.

Step 2 Enter the following command:

```
/opt/CSCOnfc/bin/nfcollector start all
```

CNS NetFlow Collection Engine runs as several processes. See the "CNS NetFlow Collection Engine Architectural Overview" section on page 1-5 for details about these processes.

Note Typically, CNS NetFlow Collection Engine is started and allowed to run until there is some reason to stop it.

Verifying That CNS NetFlow Collection Engine Is Running

To verify that CNS NetFlow Collection Engine is running properly, perform the following steps.

Step 1 To display a table of CNS NetFlow Collection Engine statistics, use the web-based user interface as described in the "Status" section of the CNS NetFlow Collection Engine User Guide.

Step 2 Verify that the UDP ports that are expected to receive export data are receiving data. The status page of the web UI should indicate that flows are being received.

Step 3 Check log files in **NFC_DIR/logs** for error messages.

If you are receiving data on the CNS NetFlow Collection Engine UDP port and there are no error messages in the log files, CNS NetFlow Collection Engine is running properly.

You should periodically monitor the log files for error and warning messages.

NetFlow Collection Engine Configuration Files

Table 3-1 displays all of the configuration files used by CNS NetFlow Collection Engine.

Table 3-1 CNS NetFlow Collection engine Configuration Files

File	Directory	Description
nfcmem	/opt/CSCOnfc/config	Memory limits for each collector process.
nfc-config.xml	/opt/CSCOnfc/config	Collector configuration file for the user-specific configuration.
nfc-config-predefined.xml	/opt/CSCOnfc/config	Collector configuration file of predefined configuration. You should never modify this file.
nfcbgp.xml	/opt/CSCOnfc/config	BGP peer configuration file.
nfcre.xml	/opt/CSCOnfc/config	Report generator configuration file.
nfcpw.xml	/opt/CSCOnfc/config	Process watcher configuration file.
nfcifname.xml	/opt/CSCOnfc/config	SNMP interface name mapping configuration file.
dnslookup.conf	/opt/CSCOnfc/config	DNS mapping configuration file.
nfc-log4j.properties	/opt/CSCOnfc/config	Logging properties file for collector.
nfcweb-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the web-based UI.
nfcpw-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the process watcher.
nfcre-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the report generator.
nfcxml-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the CNS/XML interface.

Table 3-1 CNS NetFlow Collection engine Configuration Files (continued)

File	Directory	Description
nfcbgp-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the BGP peer.
server.xml	/opt/CSCOnfc/tomcat/conf	Web server configuration file.
web.xml	/opt/CSCOnfc/tomcat/webapps/nfc/WEB-INF	Web application configuration file for web-based UI.

Browser Requirements

The CNS NetFlow Collection Engine, Release 5.0 web-based user interface is compatible with Microsoft Internet Explorer 6.0.28, and Netscape Navigator 7.0.1 on Windows or UNIX. The web-based UI requires that the browser support a Java virtual machine (JVM) to run applets. Either the Microsoft JVM or the Sun JVM can be used. For the filter editor and multi-field map editor applets to be displayed, a Sun JVM (version 1.4.1_02 or higher) must be used.

Stopping CNS NetFlow Collection Engine

To stop the CNS NetFlow Collection Engine, you must be logged in as the user specified during installation. Beginning in version 5.0, CNS NetFlow Collection Engine executables no longer have setuid-to-bin permission.

To stop CNS NetFlow Collection Engine, enter the following command to stop the CNS NetFlow Collection Engine application:

```
# /opt/CSCOnfc/bin/nfcollector shutdown
```

To immediately and ungracefully stop all CNS NetFlow Collection Engine processes, enter the following command:

```
# /opt/CSCOnfc/bin/nfcollector clean
```

Caution The **nfcollector clean** command does not gracefully stop the system. Any and all CNS NetFlow Collection Engine functions cease immediately. Use this command with caution. The **nfcollector shutdown** command is the preferred way to shut down CNS NetFlow Collection Engine.

CNS NetFlow Collection Engine subsystems can also be stopped individually. For example, only the collection subsystem is stopped by entering the following command:

```
# /opt/CSCOnfc/bin/nfcollector stop collection
```

B

C

D

F

H

I

L

N

P

S

T

U

V