Cisco NetFlow Collector Installation and Configuration Guide

Release 6.0

Americas 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: 408 527-0883

Customer Order Number:
Text Part Number: OL-11398-01

Cisco NetFlow Collector Installation and Configuration Guide

CONTENTS

About This Guide

Objective

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

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. Cisco NetFlow Collector provides fast, scalable, and economical data collection from multiple export devices exporting NetFlow data records.

Cisco NetFlow Collector, Release 6.0 introduces a tiered netflow collection architecture that provides increased scalability and performance. The role of the first tier (Tier 1) maps to the NFC functionality of Cisco NetFlow Collector 5.0.3 with the addition of new features described in *Release Notes for Cisco NetFlow Collector, Release 6.0*.

Cisco NetFlow Collector, Release 6.0 supports new Cisco NetFlow Collector Tier 2 functionality, also referred to as Multi NetFlow Collector. The Multi NetFlow Collector runs on separate server hardware and provides an aggregation layer that correlates data from several Tier 1 instances.

Prior to reading this manual, you should read the *Release Notes for Cisco NetFlow Collector, Release 6.0* document. These release notes provide information about known software and documentation problems and any last minute information about the NetFlow Collector software not available when this guide was produced.

In previous releases, this product was referred to as Cisco NetFlow Collection Engine (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, Red Hat Enterprise Linux, or Sun Microsystem's Solaris Operating System.

How This Guide Is Organized

This guide is organized as follows:

Chapter 1, "Overview," describes the Cisco NetFlow Collector application.

Chapter 2, "Installing the Cisco NetFlow Collector," describes how to install the Cisco NetFlow Collector application.

Chapter 3, "Configuring the Cisco NetFlow Collector," describes how to configure Cisco NetFlow Collector and then validate that it s operating properly.

Appendix A, "Troubleshooting the Cisco NetFlow Collector,"contains troubleshooting information in case you encounter problems while using the Cisco NetFlow Collector.

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Overview

This chapter describes the Cisco NetFlow Collector (NFC) application, which is used with the NetFlow services data export feature on Cisco routers and Catalyst switches.

This chapter includes the following sections:

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 NetFlow Collector 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 expire after a specified period of time, for example 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 NetFlow Collector, 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 *Cisco NetFlow Collector 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). NetFlow Collector 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 NetFlow Collector. For more information on the distinctions among the NetFlow data export formats, see Appendix B, "NetFlow Export Datagram Formats," in the *Cisco NetFlow Collector 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)

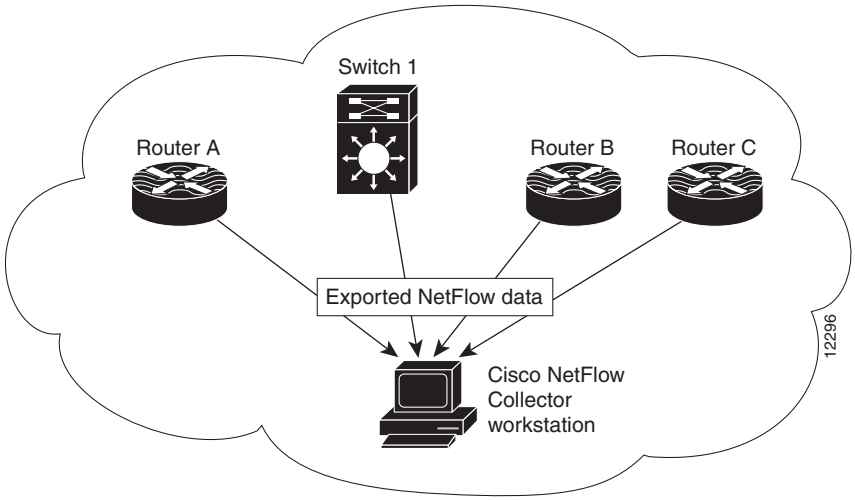
- Shortcut router IP address (present in V7 on Cisco Catalyst 5000 series switches only).

Caution Throughout this publication there are numerous examples of NetFlow Collector 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 Cisco NetFlow Collector?

The Cisco NetFlow Collector application 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 NetFlow Collector UDP and SCTP ports.

Figure 1-1 NetFlow Collector 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 or SCTP port number (a logical port designator) that identify NetFlow Collector as the receiver of flows from this export device. The port number is a user-configurable designator: you can configure NetFlow Collector to listen for flows on a number of different ports, and then configure your export devices so that each device exports flows to a dedicated port, or have a number of devices export flows to the same, shared port.

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

Cisco NetFlow Collector 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

Cisco NetFlow Collector collects and summarizes (aggregates) data into data files based on user-defined criteria specified in a NetFlow Collector *aggregator*. An *aggregator* is an aggregation task defined by a set of user-configurable attributes that specify how NetFlow Collector 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

Cisco NetFlow Collector 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 NetFlow Collector for your operating context. Moreover, starting 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 *Cisco NetFlow Collector User Guide*.

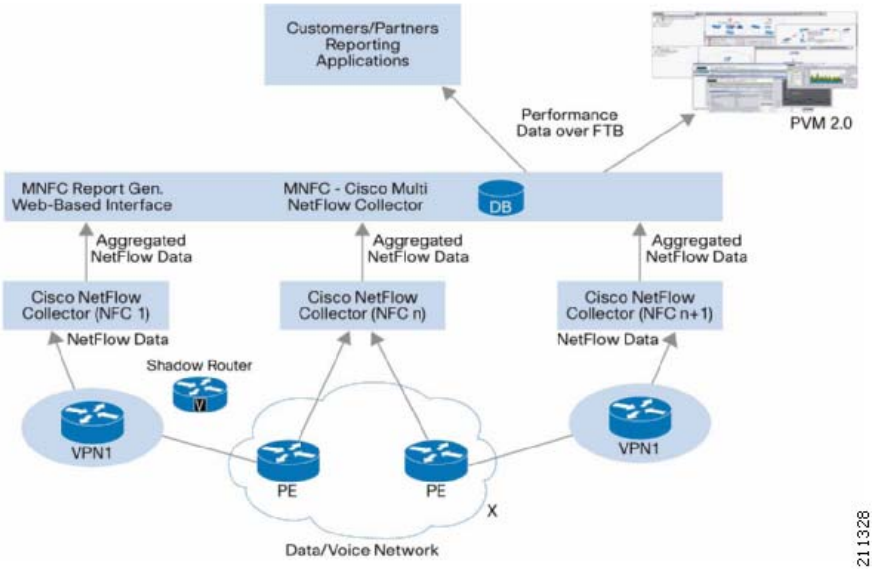
Cisco NetFlow Collector Architectural Overview

Cisco NetFlow Collector consists of the following components:

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

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

Figure 1-2 NetFlow Collector System Architecture



Collector

The Collector subsystem collects NetFlow data, aggregates or summarizes 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.

Report Generator

The Report Generator produces on-demand, 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 Cisco NetFlow Collector output with BGP attributes.

CHAPTER 2

Installing the Cisco NetFlow Collector

This chapter describes how to install the Cisco NetFlow Collector (NFC) application.

This chapter includes the following sections:

NFC Requirements

The following sections describe the Cisco NetFlow Collector, Release 6.0 requirements.

System Requirements

The following requirements are new for Cisco NetFlow Collector, Release 6.0:

- The amount of system swap space must be greater than the amount of memory specified for the collection process in the file **/opt/CSCOnfc/config/nfcmem**. The configured amount of memory is now allocated at startup; sufficient swap space must now be available for creating child processes when the collection process starts.
- NFC is licensed per host. Refer to the "Licensing" section on page 2-7 for information on obtaining a license.

Note For licensing to function properly, the **/etc/hosts** file must contain separate entries for the loopback and host name address (by default, Red Hat Enterprise Linux configures only a loopback entry in **/etc/hosts** that is also associated with the hostname).

Hardware Requirements

Cisco NetFlow Collector, Release 6.0 has the following hardware requirements:

- Minimum: 2 GB RAM, 73 GB disk, dual processor on an entry-level server.
- Recommended: 4 to 8 GB RAM, two or more 15K SAS 146 GB or greater disks, dual 3 GHz dual-core (5160) processor entry-level server.

Supported Operating Systems and Platforms

Cisco NetFlow Collector, Release 6.0 supports the following operating systems and platforms:

- Solaris 8, Solaris 9, or Solaris 10 on an entry-level server with dual 1 GHz or greater SPARC processors such as a Sun Fire V240.
- Red Hat Enterprise Linux 2.1, 3.0, or 4.0 (ES and AS) on an entry-level server, such as an IBM x3550 or x3650 with dual 2.8 GHz or greater Intel Xeon single-core processor or dual 3 GHz dual-core (5160) processors.

Note that the CPU, RAM, and disk space recommendations above are suggested, 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 NetFlow Collector and should not be running other applications.

Cisco NetFlow Collector 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 disk space usage, see the section “Memory Usage” in the *Cisco NetFlow Collector User Guide*.

Cisco NetFlow Collector, Release 6 supports the Stream Control Transmission Protocol (SCTP) as a message transport service. To use SCTP, you must be running NFC on either the Red Hat Enterprise Linux release 4 (Update3) or Solaris 10 platforms.

Browser Requirements

The NetFlow Collector, Release 6.0 web-based user interface is compatible with Microsoft Internet Explorer 6 and Mozilla Firefox 1.5 or greater on Windows or UNIX. The web-based UI requires that the browser support a Java virtual machine (JVM) to run applets.

Note The Sun JVM must be used; the JVM version must be 1.5 or higher. You can download Sun JVM 1.5 from the website http://java.sun.com/javase/downloads/index.jsp.

Installing NetFlow Collector

The Cisco NetFlow Collector is distributed on CD-ROM. Updates are made available at http://www.cisco.com.

The Cisco NetFlow Collector 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 the NFC. 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 NFC resource definitions or parameter settings that you might have made while using the previously installed version of Cisco NetFlow Collector.

Note Automatic upgrade from Cisco NetFlow Collector Release 5.x or 6 is supported in Release 6. When upgrading from an earlier release, configuration based on earlier configuration files is not applied and must be created with the web-based interface.

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.

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

To install the Cisco NetFlow Collector, perform the following steps:

Step 1 Log into the host as root.

Step 2 The NFC software can only be installed in the directory **/opt/CSCOnfc**. Enter:

df –k /opt

to verify that **/opt** contains at least 1GB (1,000,000KB) of available space. Note that significantly more space may be required to hold output files.

Also verify that at least one gigabyte of swap space is configured on the system by running **swap -s** on the Solaris platform, or **swapon -s** on the Linux platform. Four gigabytes might be required if the memory settings in **/opt/CSCOnfc/nfcmem** are increased at a later time, which is common.

Note If you wish to install NFC in some other directory, create a symbolic link to **/opt/CSCOnfc** before installing the NFC software.

Step 3 If NetFlow Collector is already installed on the system, you must stop all NetFlow Collector processes. Enter:

/opt/CSCOnfc/bin/nfcollector shutdown

Step 4 When downloading the image over the web, download the image to a temporary directory such as **/tm**p with at least 400 MB of available space.

Step 5 To untar the NFC image, enter:

tar xvf CSCOnfc-*version*.tar

Note The image should not be untarred under the install directory **/opt/CSCOnfc**.

The directory CSCOnfc-*version* is created in the current working directory.

Step 6 Perform one of the following:

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

b. When downloading the image over the web, run NFC**setup.sh** in CSCOnfc-*version* subdirectory created when the image was untarred.

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

Example

```
[root@nfc-lnx CSCOnfc-6.0.0-31-standard]# ./NFC_setup.sh
Fri Mar 23 16:10:14 EDT 2007

Using software package /var/tmp/nfc/dist/CSCOnfc-6.0.0-31-standard/./CSCOnfc.zip.

Checking platform version...

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

Cisco NetFlow Collector 6.0.0 [standard image, build 26]
Copyright (c) 2003-2007 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 7 Press return when prompted after the banner page is displayed.

Step 8 As the owner of NFC installed files and processes, you must select an existing user ID. The account must already exist on the system. If it does not, an error is displayed and the install is terminated.

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

Enter userid: nfcuser

This will be installed and run with user id nfcuser; group id is eng.
```

Step 9 The install script checks whether NFC is already installed and verifies that it is not running on the system. If NFC is running, an error is displayed and the install is terminated.

If NFC is already installed on the system all log, configuration, and output files are first moved under **/opt/CSCOnfc.sav**e. When the installation is almost complete, log files are automatically moved to the directory **/opt/CSCOnfc/logs/old**, and configuration files are moved to the directory **/opt/CSCOnfc/config/old**. Output files under **/opt/CSCOnfc/Data** and filesready files in the logs directory are preserved.

```
Checking for installed copy of NFC...

Found existing installation: 5.0.3 in /opt/CSCOnfc.

Verifying that existing NFC is not running...

Saving files from existing installation...
```

Step 10 Solaris platform only—If a previous version of NFC prior to Release 6.0 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) 5.0.3 [standard image, build 2]

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

Step 11 The Java Runtime Environment (JRE) is installed. On Red Hat Enterprise Linux, the 32-bit or 64-bit JRE is automatically selected depending on which operating system is running, x86 or EM64T. On Solaris, you are prompted to select the 32-bit or 64-bit JRE. Because for NetFlow Collector the 32-bit JRE stores data significantly more efficiently, it is recommended that you select 32-bit JRE.

```
Installing Java from jdk-1_5_0_10-linux-i586.bin...
```

Step 12 If a previous installation is detected, you are prompted whether to use old configuration files or to install new configuration files:

```
Please choose one of the following..

(1) Clean install
    (Existing configuration and log files will be saved
    in */old should you want to refer to them later)

(2) Retain existing files
    (New default configuration will be saved in */new)
```

If you select option 1, previous files are stored in the **/opt/CSCOnfc/config/old** subdirectory as indicated. If you select option 2, new configuration files are saved with the new directory, and the previous installation's configuration files are retained.

When upgrading to Release 6 from Release 5, configuration differences are automatically migrated. When upgrading from Release 4 or earlier, the previous configuration is not migrated; in this case the user must create configuration with the web-based user interface.

```
Please choose: 2

Existing files will be retained.
Migrating /opt/CSCOnfc/config/nfc-config.xml from NFC 5.0.x to 6.0 ...
Migrating /opt/CSCOnfc/config/nfcmem from 5.0.x to 6.0
```

Step 13 Specify the default login name and password for accessing the web-based user interface. This is not a system account and password; the login name and password are stored in the NetFlow Collector configuration. The login name **nfcuser** is used by default if you press return without specifying a name. However you must enter and confirm the password.

```
Web UI login name: [nfcuser]
Web UI password for nfcuser:
Enter value again to confirm:

Setting file ownership...

Updating platform config...
```

Step 14 Indicate whether NFC should be started automatically when the system initializes:

```
Would you like to start this when the system initializes? (y/n) y

CSCOnfc will be started automatically when the system initializes.
```

If you respond **y**, the following rc scripts are created for autostarting NetFlow Collector when the system initializes:

Solaris:

- /etc/init.d/csco_nfcd
- /etc/rc2.d/K99csco_nfcd
- /etc/rc3.d/S99csco_nfcd

Linux:

- /etc/init.d/csco_nfcd
- /etc/rc[01246].d/K01csco_nfcd
- /etc/rc[35].d/S99csco_nfcd

Step 15 The NFC installation is completed and the following message displays:

```
Installation of Cisco NetFlow Collector 6.0.0 [standard image, build 22]
is complete.
```

Step 16 For NetFlow Collector to run, a host-specific license must be obtained from Cisco.com. Copy the license file or license file contents with no alterations to **/opt/CSCOnfc/config/nfc.lic**. If you are upgrading from a previous version of Release 6 and retain the existing configuration, the existing license file is preserved. See the "Licensing" section on page 2-7 for additional details about licensing.

```
Note: In order to use this product, you must first obtain a license
from Cisco at http://www.cisco.com/go/license and copy
it to /opt/CSCOnfc/config/nfc.lic

[root@nfc-lnx CSCOnfc-6.0.0-31-standard]#
```

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

Step 17 Update time zone data in the Java Runtime Environment (JRE) packaged with NFC with the latest time zone data available. See the "Updating JRE Time Zone Data" section on page 3-5 for details.

Uninstalling NetFlow Collector

To uninstall and remove all files for all files for NetFlow Collector Release 6, do the following:

Step 1 Enter the following to stop the NFC server :

/nfcollector shutdown

Step 2 Log in as root and run the following:

/opt/CSCOnfc/bin/uninstall.sh

Licensing

A license file is required for each host running NetFlow Collector Release 6. The license is specific to the IP address of the host. You can obtain a limited-time demo license at the NetFlow Collector product page on Cisco.com, or a permanent license at http://www.cisco.com/go/license.

In both cases you must have the IP address of the host on which NetFlow Collector will run. To obtain a permanent license, you must also have the PAK you received after purchasing NetFlow Collector. After you enter the information, a license file is emailed to you. Copy the license file or its contents with no alterations to **/opt/CSCOnfc/config/nfc.lic**.

The first line of the license file contains either the demo expiration date or the word **permanent** for a permanent license, and the IP address of the host to which NetFlow Collector is licensed.

If the host running NetFlow Collector has more than one network card and IP address, specify the IP address associated with the hostname when licensing the product.

Note By default, Red Hat Enterprise Linux associates the system hostname with the loopback address **127.0.0.1** in **/etc/hosts**. However, for licensing to work, the hostname must be associated with the host's IP address. Edit **/etc/hosts**, remove the hostname from the loopback address entry, and add an entry for the licensed IP address.

The file **/etc/nsswitch.conf** is normally configured so that hostname lookups are first obtained from files (**/etc/hosts**).

Note If a clean install is performed, the previous license file is not retained. The previous license file is saved at **/opt/CSCOnfc/config/old/nfc.lic**.

CHAPTER 3

Configuring the Cisco NetFlow Collector

This chapter describes how to configure the Cisco NetFlow Collector application and then validate that it is operating properly.

This chapter includes the following sections:

Required Patches and Software Packages

Solaris Platform

Prior to running Cisco NetFlow Collector on the Solaris platform, the latest Recommended Patch Cluster for the release should be installed.

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

Red Hat Enterprise Linux Platform

Prior to running Cisco NetFlow Collector on Red Hat Enterprise Linux platform, you must install the the following packages :

- 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 and 4, you must ensure that the compat-libstdc++ RPM is installed on the system. This RPM is included in the Red Hat Enterprise distribution CDs.

UNIX Environment Variables

In releases prior to version 5.0, the Cisco NetFlow Collector 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 Cisco NetFlow Collector. The environment is automatically determined by startup scripts in the 6.0 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 or SCTP port number used to identify Cisco NetFlow Collector as the receiver of exported NetFlow data. For information on configuring the UDP ports that Cisco NetFlow Collector uses to receive NetFlow exported data, refer to the "**Creating an Aggregator**" section in the *Cisco NetFlow Collector User Guide*.
- 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 the Cisco NetFlow Collector

To start Cisco NetFlow Collector, perform the following steps:

Step 1 Log in as the user specified during installation. Refer to the "Installing NetFlow Collector" section on page 2-3.

Step 2 Enter the following command:

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

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

In most cases, NFC is configured during installation to be started automatically by the system when the host reboots. When this is the case, startup scripts are placed in the file **/etc/rc*d**.

Verifying That Cisco NetFlow Collector Is Running

To verify that Cisco NetFlow Collector is running properly, perform the following steps.

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

Step 2 Verify that the UDP and/or SCTP 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 **/opt/CSCOnfc/logs/nfc.logs** for error messages.

If you are receiving data and there are no error messages in the log files, Cisco NetFlow Collector is running properly.

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

NetFlow Collector Configuration Files

Table 3-1 displays all of the configuration files used by Cisco NetFlow Collector.

Table 3-1 Cisco NetFlow Collector 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-specified 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.
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 (scheduled reports).
nfcrd-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the report daemon (custom reports).

Table 3-1 Cisco NetFlow Collector Configuration Files (continued)

File	Directory	Description
nfcnmpd-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the SNMP Daemon.
nfcxml-log4j.properties	/opt/CSCOnfc/config	Logging properties file for the Cisco/XML interface.
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.
auth.config	/opt/CSCOnfc/config	Authentication information for web-based UI.
healthmonitor.properties	/opt/CSCOnfc/config	Health monitor configuration.
nfcsnmpd.properties	/opt/CSCOnfc/config	SNMP configuration.
peList.conf	/opt/CSCOnfc/config	PE ID list

Browser Requirements

The Cisco NetFlow Collector, Release 6.0 web-based user interface is compatible with Microsoft Internet Explorer 6.0 and Firefox 1.5 on Windows or UNIX. The web-based UI requires that the browser run the Sun Java virtual machine (JVM) to run applets. For the filter editor , threshold editor, and multi-field map editor applets to be displayed, a Sun JVM version 1.5 or higher must be used.

Starting the Cisco NetFlow Collector User Interface

To start the Cisco NetFlow Collector User Interface, do the following:

Step 1 To run Cisco NetFlow Collector, log in as the user specified during installation.

Step 2 Enter the following command:

/opt/CSCOnfc/bin/nfcollector start all

Step 3 From a web browser enter:

//<*nfc-hostname*>:8080/nfc

Note The web-based UI only works with the collector located on the same machine. To access a different instance of Cisco NetFlow Collector you must start that collector's web server and access it through the corresponding URL.

Stopping Cisco NetFlow Collector

To stop the Cisco NetFlow Collector, you must be logged in as the user specified during installation.

To stop Cisco NetFlow Collector, enter the following command:

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

The **shutdown** option waits for the NFC process to exit. If a process fails to stop after a configurable number of seconds, the nfcollector script returns a non-zero exit status. 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 Cisco NetFlow Collector functions cease immediately. Use this command with caution. The **nfcollector shutdown** command is the preferred way to shut down Cisco NetFlow Collector.

Cisco NetFlow Collector 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
```

Updating JRE Time Zone Data

Cisco NetFlow Collector requires up-to-date time zone data in the Java Runtime Environment (JRE) bundled with NFC so that files and reports that contain the time-of-day accurately reflect current Daylight Saving Time rules that are in effect. Time zone data in NFC's JRE should be updated using the TZupdater tool provided by Sun Microsystems when NFC is installed and whenever local Daylight Saving Time rules change.

Note JRE time zone data that NFC depends on is separate from system time zone data. Although it is recommended that you should also update your operating system time zone data when local Daylight Saving Time rules change, NFC will report times correctly if only the JRE is updated.

Sun Microsystems has provided general information about this topic in the article *Timezone Data and the Java Runtime Environment* at http://java.sun.com/javase/timezones/. To see if a change announced recently for your location is reflected in the latest data provided by Sun, see *Timezone Data Versions in the JRE Software* at http://java.sun.com/javase/timezones/tzdata_versions.html.

To update the JRE timezone information for NFC, do the following:

Step 1 Login as the system user who owns NFC files and processes; this account was specified when NFC was installed.

Step 2 Run **umask** to verify that the current umask is not set to a restrictive value higher than 022. If set to a higher value, set to 022 by running **umask 022**.

Step 3 Download the latest TZupdater tool from Sun Microsystems. If you don't have a Sun Online Account, you will be prompted to create one. Information about the tool including a link to the download location of the most recent version is available at http://java.sun.com/javase/tzupdater_README.html.

Step 4 In a temporary directory, extract the zipped contents of the download file. This creates the subdirectory **tzupdater-*version*** containing the jar file **tzupdater.jar**.

Step 5 Shut down NFC by running **/opt/CSCOnfc/bin/nfcollector shutdown**. Verify that no java processes by running **ps -ef | grep java**.

Step 6 Run the TZupdater tool to update JRE timezone data as follows:

/opt/CSCOnfc/java/bin/java -jar *path-to-tzupdater-files*/tzupdater.jar -u

Note: On the Solaris platform, ignore package-related warning messages such as:

***path-to-java-bin*/java not directly found in contents file, no package resolution performed. (May not be in PKG form, not an absolute path, or is a symlink.)**

Step 7 Restart Cisco NetFlow Collector. See the "Starting the Cisco NetFlow Collector User Interface" section on page 3-4

APPENDIX A

Troubleshooting the Cisco NetFlow Collector

This appendix provides helpful information and procedures in case you encounter problems while using the Cisco NetFlow Collector (NFC).

This appendix includes the following:

Using the nfcollector list Command

The **nfcollector list** command provides an easy way to determine which NFC processes are running (or not running). To invoke the **nfcollector list** command, enter the following command line at the UNIX prompt:

$NFC_DIR/bin/nfcollector list

When invoked, the **nfcollector list** command displays status information about the Cisco NetFlow Collector, as in the following example:

```
rmiregistry: Running (pid: 13415)
nfcxml: Running (pid: 13403)
snmpd: Running (pid: 13425)
collection: Running (pid: 13405)
rd: Running (pid: 13404)
re: Not Running; autostart not configured
web: Running (pid: 7590)
```

Note If the **nfcollector list** command lists that a process is not running but autostart is configured for that process, there may be a problem with the NetFlow Collector. See the "Starting the Cisco NetFlow Collector User Interface" section on page 2-1 for information on how to start NetFlow Collector processes. Keep in mind that the **re** process for running scheduled reports is not autostarted by the process watcher unless you update the default process watcher configuration in **/opt/CSCOnfc/config/nfcpw.xml**.

Using the show-tech Command to Capture Troubleshooting Information

The **show-tech** command provides an easy way to generate all the debugging information necessary for support and troubleshooting purposes. To invoke the **show-tech** command, enter the following command line at the UNIX prompt:

$NFC_DIR/bin/nfcollector show-tech

Note To capture running configuration information, you should invoke the **show-tech** command while NetFlow Collector is running.

When invoked, the **show-tech** command creates a log file named **show-tech.log** in the **$NFC_DIR/logs** directory.

NetFlow Collector Tools and Utilities

The utilities described in this section are typically used to troubleshoot NetFlow Collector operation by providing a way to capture and play back received NetFlow data. The process emulates a Cisco export device generating NetFlow data through the NetFlow data export feature. The utilities are available in the **$NFC_DIR/tools** directory and include the following:

- fdcount Utility
- ndeget Utility
- get_bgp_rib Utility
- fdget Utility
- fdplayback Utility

fdcount Utility

The **fdcount** utility listens to a user-specified UDP port, samples a user-specified number of incoming datagrams, and calculates the average incoming rate. Enter:

```
$NFC_DIR/tools/fdcount [-p UDP-port] [-c count] [-s socket-buffer]
```

where:

-p *UDP-port*	UDP port number on which flows are to be received. The default is 9991.
-c *count*	Number of flows to sample before calculating the incoming rate. The default is 100.
-s *socket-buffer*	Receive socket buffer size, in bytes. The default is 90000 bytes.

ndeget Utility

The **ndeget** utility listens to a user-specified UDP port to receive flow data and prints the contents of the received flow packets to the standard output. This is intended to replace the fdget utility, which is still included for backwards compatibility. Unlike fdget, ndeget can display the contents of NetFlow version 9 packets. Enter:

```
$NFC_DIR/tools/ndeget.sh -port port [-hex] [-maxpacketlen length]
```

where:

-port port	UDP port number on which flows are to be received.
-hex	Optionally display a hex dump of the contents of packets.
-maxpacketlen len	Optionally change the size of the packet buffer.

get_bgp_rib Utility

The **get_bgp_rib** utility displays the contents of the NetFlow Collector BGP Peer's routing information base. Enter:

```
$NFC_DIR/tools/get_bgp_rib.sh [-p port ] [ -x ]
```

where:

-p port	Optionally change the port used for contacting the BGP peer.
-x	Optionally display the result as XML.

fdget Utility

The **fdget** utility is made obsolete by the **ndeget** utility.

The fdget utility listens to a user-specified UDP port to receive flow data and prints some of the fields from the received flow packets to the standard output. One use of this capability is to print flow data sent by the **fdplayback** utility. Enter:

```
$NFC_DIR/tools/fdget [-p UDP-port] [-s socket-buffer] [-a]
```

where:

-**p** *UDP-port*	UDP port number on which flows are to be received. The default is 9991.
-s *socket-buffer*	Receive socket buffer size, in bytes. The default is 90000 bytes. This argument and value determine how many datagrams the kernel stores in this buffer as datagrams come in from the network. The larger the buffer, the more time **fdget** has to consume data from the buffer before the buffer overflows. If the buffer overflows, datagrams are lost.
-a	Print an acknowledgment only. The default is to print the content of flows. Using **-a** means print only an acknowledgment for each datagram received rather than the content of the datagram.

fdplayback Utility

The **fdplayback** utility reads a data file of NetFlow data created by NetFlow Collector or some other tool and sends the flow data to a user-specified destination. Enter:

```
$NFC_DIR/tools/fdplayback [-f datafile] [-d IP-address] [-p UDP-port] [-i delay]
[-b burst] [-s socket-buffer] [-t flows]
```

where:

-f *datafile*	Name of data file to play back to the user-specified destination (defined by IP address and UDP port number).
-d *IP-address*	Destination IP address.
-p *UDP-port*	Destination UDP port number. The default is 9991.
-i *delay*	Delay (in milliseconds) between datagrams. The default is 1000. The longer the delay, the more separation there is between datagrams being sent to the receiving destination.
-b *burst*	Number of flows sent in each burst. The default is 10. This argument is used in conjunction with **-i** to control the speed and "burstiness" of the playback.
-s *socket-buffer*	Receive socket buffer size, in bytes. The default is 90000 bytes.
-t *flows*	Number of flows to play back in this session. The default is all flows in the data file. If the data file contains 1000 datagrams and you set **-t** to 1, **fdplayback** only sends one datagram.

Solving NetFlow Collector Problems

This section discusses some basic problems that you might encounter while attempting to run NetFlow Collector.

Symptom Licensing errors in the **/opt/CSCOnfc/logs/nfc.log file**.

Possible Cause Either the license file is missing or invalid; or the system hostname and address information is not configured properly on the host. This is particularly an issue with Red Hat Linux where the default **/etc/hosts** file must be updated for licensing to work.

Recommended Action

1. Look in the **nfc.log** file and determine the specific error. The error information returned by the FlexLM library can be useful.
2. Verify that the contents of the **/opt/CSCOnfc/config/nfc.lic** file was copied verbatim from the license key sent in email. The files must match exactly. Note that in some cases detaching the file from email can sometimes introduce Windows-style carriage return characters that the FlexLM library does not handle properly.
3. Do the following:
   a. Verify that the IP address matches the **HOSTID=INTERNET=ipaddress** line in the **/opt/CSCOnfc/config/nfc.lic** file. If not, the license file is not valid for this host.
   b. Verify that the hostname is set, using the **hostname** command, and is set to a value other than **localhost**, **localhost.localdomain**, etc.
   c. Verify that **/etc/hosts** contains an entry for this hostname, and that the IP address in the entry matches the IP address in the **nfc.lic** file. Verify that the loopback address **127.0.0.1** in **/etc/hosts** does not contain **localhost**, **localhost.localdomain**, etc. as the hostname. These are defaults for Red Hat Enterprise Linux and must be changed. You must remove the hostname mapping to the loopback address and add an entry for the licensed IP address. On Solaris systems, in **/etc/nsswitch.conf**, the **hosts** entry is normally set to **files dns** so that **/etc/hosts** is searched for the IP address.

Symptom Unable to login to the NetFlow Collector UI with a general error message on the login screen about checking for errors in collector log files.

Possible Cause The collection process is not running. The collection process must be running before you are allowed to login.

Recommended Action Check the **/opt/CSCOnfc/logs/nfc.log** file for specific error information. The most common causes of this are:

- Licensing problem. See the above section Symptom Licensing errors in the /opt/CSCOnfc/logs/nfc.log file.
- XML configuration problem. Identify the log message corresponding to the invalid XML and fix it.

Symptom During installation on a Solaris system, an error is encountered and NetFlow Collector does not finish installing.

Possible Cause The system is running Solaris 7 or lower.

Recommended Action Use a system running Solaris 8, 9, or 10. Solaris 7 or lower is not supported.

Symptom During installation on a Linux system, an error is encountered and NetFlow Collector does not finish installing.

Possible Cause The system is not running Red Hat Enterprise 2.1, 3, or 4 Linux.

Recommended Action Use a system running Red Hat Enterprise 2.1, 3, or 4 Linux.

INDEX

N

P

S

T

U

V