Installing and Setting Up the FlowAnalyzer

This chapter provides information for installing and setting up the NetFlow FlowAnalyzer application. It contains the following sections:

- Required Installation and Setup Procedures
  - Before You Begin
  - Installing and Running FlowAnalyzer Version 2.0
- Optional Setup Procedures
  - Optional Setup Procedures
  - Customizing the UtilityServer Module
  - Customizing the DisplayServer Module
  - Setting Time Zones for the FlowCollector Application
  - Starting the FlowAnalyzer

Required Installation and Setup Procedures

This section presents the required installation and setup procedures for the NetFlow FlowAnalyzer application.

Before You Begin

Before installing and setting up the FlowAnalyzer, note the system requirements in the following sections.

IOS Software Requirements

For the FlowAnalyzer application to operate properly, the NetFlow-enabled devices in your network (from which you plan to collect NetFlow data) must be running Cisco IOS Release 11.1CC or 11.1(11)CA, or later.

System Software Requirements

The UNIX and PC platform requirements for the FlowAnalyzer application are listed below:

- Solaris software—Version 2.5.1 or 2.6 running on an ULTRA-1 workstation
- Windows NT 4.0—For the FlowAnalyzer Display module only
- HP-UX 10.20 systems must be running at least the April, 1998 version of Hewlett Packard's General Release Recommended patches, which includes the Extension Software patch bundle XSW700GR1020/CR1020 B-10.20.37.
- See the additional software requirements noted in the section entitled "Important Information Regarding This Product" in Chapter 1.
- The Bourne shell "sh" (/bin/shell) must be available for execution
- The following standard UNIX utility programs must be in the /usr/bin or /bin directory of your FlowAnalyzer workstation:
  - awk
  - basename
  - cat
  - cd
  - chmod
  - echo
  - expr
  - kill
  - ls
  - mkdir
  - nohup
  - ps
  - pwd
  - rm
  - sed
  - touch
  - unalias
  - wc
  - whoami

  Alternatively, these utility programs can be made accessible to the FlowAnalyzer by means of appropriate entries in the $PATH environment variable of each FlowAnalyzer workstation user.

Hardware Requirements

The PC on which you run the Display module must meet the following requirements:

- Pentium machine containing at least a 166 Mhz processor and 64 MB or more of RAM.

The workstation on which you run the FlowAnalyzer must meet the following requirements:

- Contain 256 MB of physical memory (RAM) and 400 MB of free logical memory (this is a requirement only for the host on which the DisplayServer module runs).

  If you are not sure how much free logical memory is available on your FlowAnalyzer workstation, see the section entitled "Calculating Available Memory and Adjusting the MaxMB Value" in Chapter 4.

- Contain 70 MB of free disk space for the tar and uncompressed installation files (these files can be deleted after installation).
- Contain 50 MB of free disk space for the installed executable (25 MB is required for the NFADisplay executables running on the PC).

Caution To eliminate potential data loss and to prevent workstation performance degradation during NetFlow data collection and processing, it is recommended (but not mandatory) that you install the NetFlow FlowCollector and the NetFlow FlowAnalyzer applications on different workstations, as depicted in Figure 1-1.

Installing and Running FlowAnalyzer Version 2.0

To install FlowAnalyzer Version 2.0 from the distribution CD-ROM, perform the following steps:

Step 1 Log in as root:

```
$ su root
password: <enter the password>
```

Step 2 Depending on your installation platform, do either of the following:

For Solaris, copy the tar file from the distribution CD-ROM to the temporary directory and untar the file, as shown below:

```
# cp NFA2_0.SOL.tar .
# tar -xvf NFA2_0.SOL.tar
```

For HP-UX, copy the tar file from the distribution CD-ROM to the temporary directory and untar the file, as shown below:

```
$ cp NFA2_0.hP_10.tar
$ tar -xvf NFA2_0.HP_10.tar
```

Step 3 Run the FlowAnalyzer installation script, as shown below, and answer all questions.

```
$ chmod +x NFC2_0.setup.sh
$ .NFA2_0.setup.sh NFA2_0.<platform>.Z
```

where: *platform* can be either **SOL** or **HPUX**, as appropriate.

For Solaris, enter the following command:

```
$ ./NFA2_0.setup.sh ./NFA2_0.SOL.Z
```

For HP-UX, enter the following command:

```
$ .nFA2_0.setup.sh .NFA2_0.HP_10.Z
```

Optional Setup Procedures

After completing the required installation and setup procedures presented earlier in this chapter, you can:

- Start the FlowAnalyzer application and begin using it immediately.

  In this case, see the section entitled “Starting the FlowAnalyzer” at the end of this chapter.

- Perform the optional setup procedures presented in this section.

Note The TrawhoisServer module requires no setup. Any installation or configuration instructions stored in the TrawhoisServer module subdirectories do not apply to FlowAnalyzer installations. You can ignore all such instructions in these TrawhoisServer subdirectories.

Customizing the Display Module

This section tells you how to customize the Display module to run as desired on your workstation or PC.

You can install the Display module on any workstation or PC in the network, or on several such platforms, provided that each platform meets the installation requirements for the Display module.

The Display module functions as the user interface to the NetFlow system. It can be configured to run on a workstation or a PC apart from other FlowAnalyzer modules.

After completing the installation script (as described in the previous section), you can edit the start.Display file to customize the Display module to run in your particular networking environment. This file is located in the /opt/CSCOnfa/NFADisplay/bin/start.Display directory.

The switches and arguments in the start.Display file are described in Table 2-1. You can modify certain switch arguments to customize the Display module to suit your particular operating requirements. However, you should be fully mindful of the effects of changing any of the default values listed in Table 2-1 for the switches.

Table 2-1 Switches and Arguments in the Start.Display File

Switch Name	Description of Editable Argument
-utilityserver	The IP address or name of the workstation on which the UtilityServer module will be running. You must change the placeholder value UTILITYSERVERHOST to the host name or IP address where the UtilityServer module will be running.
-utilityserverport	The port on which the UtilityServer module listens for network commands. The default port is 7545.
-displayserver	The IP address or name of the workstation on which the DisplayServer module will be running. You must change the placeholder value DISPLAYSERVERHOST to the host name or IP address where the DisplayServer module will be running.
-displayserverport	The port on which the DisplayServer module listens for network commands. The default port is 7544.
-width	The width (in pixels) of the Display module window. The default is 800 pixels.
-height	The height (in pixels) of the Display module window. The default is 600 pixels.
-classpath	This switch refers to the default directory, /opt/CSCOnfa/NFADisplay/bin, in the host workstation or PC where the Display module’s Java classes are stored. Do not change this directory.

-defaulttreefile	The argument to this switch is used to identify a user-created file that contains a working tree structure of particular relevance to your local FlowAnalyzer operating domain. Once this file is created and referenced as an argument to the defaultreefile switch, the working tree structure in this file is loaded by default into the Netflow Data area of the Display module window on startup. Note that this working tree structure can incorporate defined router groups, enabling you to issue Display module commands that act on group members as a whole for data analysis purposes. By defining a default tree file that is automatically loaded on Display module startup, you can avoid the repetitive tasks associated with manually adding data set paths to the Netflow Data area of the Display module window. The procedure for loading a default tree file is presented in the section entitled "Loading a Named Tree File" in Chapter 3.
-browser	The argument to this switch should be the name of the browser executable you are going to use to view the FlowAnalyzer help system. If the name of the browser is not in your $PATH environment variable, this parameter should contain the full path name of the browser executable.
-helppath	The argument to this switch should be the name of the directory containing the FlowAnalyzer system help files. This parameter defaults to /opt/CSCOnfa/NFADisplay/help on the Solaris platform.

Customizing the UtilityServer Module

After installing the FlowAnalyzer application (see the section above entitled "Installing and Running FlowAnalyzer Version 2.0"), perform the following steps to customize the UtilityServer module:

Step 1 Log in as root (superuser):

```
$ su root
 password: <enter the password>
```

Step 2 It is strongly recommended that you use the official TCP default port (7545) for running the UtilityServer module. If you want to use a different port number for the UtilityServer, you must edit the /opt/CSCOnfa/NFAUtility/bin/NFAUS.resources file to add the following line:

```
NFAU_TCP_PORT <portnum>
```

where *portnum* is the port number you wish to use in place of the default value 7545.

Step 3 Create the configuration files described in the section entitled "Configuration Files in the /opt/CSCOnfa/NFAUtility/config Directory."

Note The UtilityServer module writes data to several output subdirectories under the /opt/CSCOnfa/NFAUtility directory. The logs directories must be periodically checked for errors and purged. For more information about these tasks, see the section entitled "Maintaining the UtilityServer Output Directories" in Chapter 4.

Configuration Files in the /opt/CSCOnfa/NFAUtility/config Directory

The directory /opt/CSCOnfa/NFAUtility/config is used to store the following user-defined configuration files:

- HostPreferences.txt
- RouterAliases.txt
- RouterConfig.txt

You create these files and enter appropriate configuration information in each one, as described in the following subsections.

HostPreferences.txt File

This file maps Internet host IP addresses to aliases (that is, the names of individual, manageable network devices).

When the FlowAnalyzer application needs to convert IP addresses to the aliases of host devices, it checks the HostPreferences.txt file first.

Aliases for hosts not listed in this file are determined by means of Domain Name System (DNS) lookup.

You use the following format in creating each line of the HostPreferences.txt file:

```
<IP address> <alias>
```

For example:

```
3.69.204.177    ksharko-sun.cisco.com
1.1.1.1         dummy
171.69.204.177  dummy2.cisco.com
```

RouterAliases.txt File

You create this file only if you used the RouterAliases.txt file in Version 1.0 of the FlowAnalyzer. You can copy the Version 1.0 RouterAliases.txt file into the /opt/CSCOnfa/NFAUtility/config directory.

The UtilityServer module will read the contents of the RouterAliases.txt file to configure router aliases.

RouterConfig.txt File

This file contains a list of routers (arranged by IP addresses), their associated SNMP read community.

The UtilityServer module uses the information in this file to communicate with routers in the network when NetFlow data is being collected.

You use the following format to create each line of the RouterConfig.txt file:

```
<router IP address> <SNMP community> <netflow>
```

For example:

```
193.69.209.4 public netflow
193.69.209.5 public netflow
194.70.210.5 public netflow
```

The entry following the <SNMP community> parameter of each line in the RouterConfig.txt file should be “netflow.”

At this point, you have completed all of the required installation and setup procedures for using the NetFlow FlowAnalyzer. If you want to skip the procedures presented in the subsequent sections entitled “Optional Setup Procedures” and “Setting Time Zones for the FlowCollector Application,” you can proceed directly to the section at the end of this chapter entitled “Starting the FlowAnalyzer.”

Customizing the DisplayServer Module

The DisplayServer module does not require any optional setup procedures.

You can alter the DisplayServer module's behavior to suit your NetFlow data analysis needs by changing some of the parameters in the NFADS.resources file. This section tells you how to make such changes.

You can customize the DisplayServer module if

- You wish to change the number of the protocol port on which the DisplayServer module listens for network commands.
- You wish to fine-tune the amount of memory used by the DisplayServer module or the file size allowances defined for that module.

Note See the section entitled "Calculating Available Memory and Adjusting the MaxMB Value" in Chapter 4 to determine how much logical memory is available on your FlowAnalyzer workstation and how to fine-tune the workstation for efficient memory use.

Customizing the NFADS.resources File

The NFADS.resources file of the DisplayServer module contains configuration parameters that you can customize according to your operational NetFlow data processing requirements (see Table 2-2).

When you redefine the configuration parameters in the NFADS.resources file and change their default values, the following rules apply:

1. You must redefine one parameter per line.
2. Parsing stops at the first blank line encountered in the file.
3. Any line that does not start with a valid parameter key word is treated as a comment and ignored.
4. If a parameter is defined more than once, the last parameter definition encountered in the file takes precedence.

Use the following format to redefine the parameters in the NFADS.resources file:

```
<parameter_keyword> <new_value>
```

Table 2-2 describes the parameters in the NFADS.resources file that you can modify to customize the DisplayServer module.

Table 2-2 Modifiable Parameters in the NFADS.resources File

Parameter Keyword	Default Value	Range of Values	Description
Port	7544	**Min:** 5000 **Max:** 10000	The application port on which the DisplayServer module listens for network commands.
MaxSimultaneousCommands	24	**Min:** 1 **Max:** 64	Defines the maximum number of commands that the DisplayServer module will accept.
MaxMB	224	**Min:** 32 **Max:** The most your system can handle	Determines the size of the dynamic memory pool in megabytes (MB). For best FlowAnalyzer performance, this value should be no greater than the amount of physical RAM, minus 32 MB, and no greater than the amount of free memory, minus 100 MB (approximately). The value of the MaxMB parameter can be set to nearly the full size of the workstation swap space, provided that you are willing to tolerate severe disk thrashing. The operating system kills processes when the swap space of the system is exhausted.
MaxMBperCommand	224	**Min:** 24 **Max:** Value of MaxMB	Defines the maximum amount of memory, in megabytes, that will be used in executing a single network command. The value of the MaxMBperCommand parameter cannot exceed the value of the MaxMB parameter. If it does, the DisplayServer module resets the value of the MaxMBperCommand parameter to equal the value of the MaxMB parameter.
Max_Stored_NoWait_MB	384	**Min:**2 **Max:** $2^{31} - 1$	Defines the maximum aggregate amount of storage, in megabytes, that can be consumed by background NoWait command response files being stored in the /opt/CSCOnfa/NFAServer/Cache directory of the DisplayServer module. The system always tries to store one file, even if it is larger than the value of this parameter. The practical maximum value of this parameter is whatever your DisplayServer workstation can handle.[1] The default value is 384 MB.
MaxWellKnownProtocolPort	1023	**Min:** 0 **Max:** 65535	Defines the maximum “well-known” protocol port number for the DisplayServer module. A well-known protocol port retains its identity for defining traffic flows, even if no text description exists (in the Proto.txt file or the Port.txt file in the AliasDefn directory) to define the port number. The default value of this parameter is 1023.

Parameter Keyword	Default Value	Range of Values	Description
MaxRegisteredProtocolPort	1023	**Min:** 0 **Max:** 65535	Defines the maximum “registered” protocol port number. A protocol port number greater than the value of the “well-known” protocol port, but less than the value of the “registered” protocol port, retains its identity for defining flows only if a text description exists for it (in the Proto.txt file or the Port.txt file in the AliasDefn directory). The default value of this parameter is 1023.
UsePortText	false	**true** **false**	Displays the protocol ports in the “Protocol” field (column) of the DisplayServer command response according to their IANA-STD-2-registered keyword identification. The default value of this parameter is false.

1. For more information about this parameter, see the section entitled “Maintaining the DisplayServer Cache Directory” in Chapter 4.

Managing Memory for the DisplayServer Module

By defining the following memory management parameters in the DisplayServer module, you can configure the module to operate efficiently on your FlowAnalyzer workstation:

- MaxMBperCommand (see Table 2-2)
- MaxMB (see Table 2-2)

The value of the MaxMBperCommand parameter cannot exceed the value of the MaxMB command parameter. If it does, the value of the MaxMBperCommand parameter is automatically changed to agree with that of the MaxMB parameter.

The use of memory by the DisplayServer module is limited primarily by the value of the MaxMB parameter, as defined in the NFADS.resources file. You must not configure the DisplayServer module to use excessive memory; doing so may exhaust the available swap space on your FlowAnalyzer workstation, resulting in severe disk thrashing.

Setting Time Zones for the FlowCollector Application

This section presents a step you can take to prevent problems that affect the operation of the NetFlow FlowAnalyzer application. This step can be taken during the configuration of the NetFlow FlowCollector application.

For more information about the NetFlow FlowCollector application, refer to the *NetFlow FlowCollector Installation and User Guide*.

You can run the NetFlow FlowCollector application using Greenwich Mean Time (GMT). To run the application in this mode, you must edit the nf.resources file of the FlowCollector application to uncomment the line containing the GMT_FLAG parameter. By default, the GMT_FLAG parameter in the nf.resources file is set to the on (yes) state.

To uncomment the GMT_FLAG parameter in the nf.resources file, ensure that this parameter appears in the file as shown below:

```
GMT_FLAG  yes
```

The DisplayServer module can accommodate the shift forward to daylight savings time in the spring and will support the locally named file for a single time zone used for each DataSetPath. The DataSetPath for each thread is defined in the FlowCollector's nfconfig.file.

The FlowCollector database may contain anomalies if you collect data from different time zones for the same DataSetPath. The FlowCollector database may also contain anomalies if you are not using Greenwich Mean Time at the time daylight saving time causes the local clock to be shifted backward in the fall.

Starting the FlowAnalyzer

To start the FlowAnalyzer if you chose not to start it during the installation process, perform the following steps:

Step 1 Log in as root:

```
$ su root
password: <enter the password>
```

Step 2 Change to the following directory:

```
# cd /opt/CSCOnfa
```

Step 3 Execute the start.All script to start all the server modules of the FlowAnalyzer application:

```
# start.All
```

Step 4 Issue the following command to start the Display module:

```
# /opt/CSCOnfa/NFADisplay/bin/start.Display
```

On execution of this command, the main Display module window appears on your workstation screen.

When you finish using the Display module, exit from it and restart it later, as needed.

During normal operations, you should leave the three server modules of the FlowAnalyzer running. These modules need to be restarted only if a problem occurs, such as a system crash.

For instructions on stopping the FlowAnalyzer modules, checking their status, or starting them individually, see the section entitled "Controlling FlowAnalyzer Modules" in Chapter 4.