CHAPTER 2

# Installing and Setting Up the Analyzer

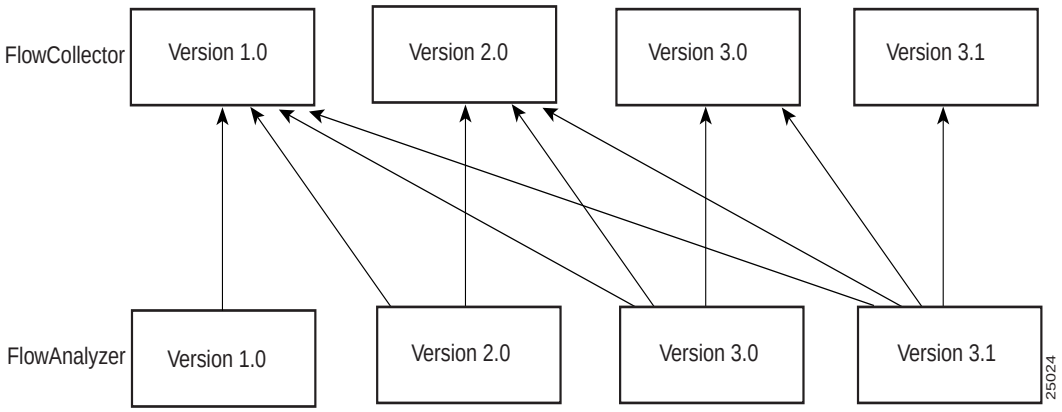
This chapter contains information for installing and setting up the Analyzer and its associated modules. The following topics are covered in this chapter:

# Compatibility with Earlier FlowCollector Releases

Analyzer Version 3.0 is designed to operate with FlowCollector Version 3.0. Figure 2-1 shows the currently supported combinations of releases for the FlowCollector and the Analyzer.

Note that the Analyzer can display traffic data that was collected by the latest or any previous version of the FlowCollector.

**Figure 2-1 Supported Combinations of FlowCollector and Analyzer Releases**




# Equipment Requirements

This section outlines the requirements for the NetFlow-enabled devices configured into your network and for each instance of the Analyzer that you intend to run in the network. It also presents the setup procedures for bringing the Analyzer to its initial operating state.

## Cisco IOS Software Requirements

The NetFlow-enabled devices in your network must be running Cisco IOS Release 12.0(3)T or Release 12.0(6)S to process Version 8 export data for the new on-router aggregation schemes (see the “New in This Release” section on page 1-1 of Chapter 1.

The TMS-enabled devices in your network must be running Cisco IOS Release 12.0(5)S, or higher.

## Analyzer Software Requirements

The software requirements for using the Analyzer are listed below:

- Solaris Version 2.5.1 or 2.6—For the Analyzer running on a UNIX-based workstation
- Windows NT 4.0—For the Display module only running on a workstation or a PC
- Web browser executable (optional)—For viewing Analyzer Help files (requires Internet Explorer Version 5.0 or Netscape Navigator Version 4.5)
- 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 host Analyzer platform:
  - awk
  - basename
  - cat
  - cd
  - chmod
  - echo
  - expr
  - kill
  - ls
  - mkdir
  - nohup
  - ps
  - pwd
  - rm
  - sed
  - touch
  - unalias
  - wc
  - whoami

  Alternatively, you can set these utility programs to be accessible to the Analyzer by means of appropriate entries in the $PATH environment variable for each host Analyzer platform.

## Analyzer Hardware Requirements

If you elect to run the Display module separately on a PC (apart from the host Analyzer workstation), the PC must be an Intel Pentium class machine with at least a 166 Mhz CPU and contain 64 MB or more of RAM.

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

- Sun Microsystems Ultra 5 workstation or above.
- Contain 256 MB of physical memory (RAM) and 400 MB of free logical memory.

  The free logical memory requirement applies only to the host machine on which the DisplayServer module runs.

  If you are not sure how much free logical memory is available on your host Analyzer platform, see the “Calculating Available Memory and Adjusting the MaxMB Value” section on page 4-4 in Chapter 4.
- Contain 70 MB of free disk space for the Analyzer tar and uncompressed installation files; you can delete these files after installation.
- Contain 50 MB of free disk space for the installed Analyzer executable.

A workstation or PC on which the Display module only is installed requires 25 MB of free disk space.

**Caution** To eliminate potential data loss and prevent performance degradation during NetFlow data collection and processing, it is recommended (but not mandatory) that you install the FlowCollector and the Analyzer on different workstations.

# Installing and Running the Analyzer

This section presents the setup procedures for bringing the Analyzer to its initial operating state.

To install Analyzer Version 3.0 from the distribution CD-ROM, perform the following steps:

**Step 1** Log in as root:

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

**Step 2** Copy the tar file from the distribution CD-ROM to the temporary directory and untar the file, as shown below:

```
# cp NDA3_0.SOL.tar .
# tar -xvf NDA3_0.SOL.tar
```

**Step 3** Run the Analyzer installation script, as shown below, and answer all questions in the script.

```
$ chmod +x NDA3_0.setup.sh
$ .NDA3_0.setup.sh NDA3_0.<platform>.Z
```

where: *platform* is **SOL**.

**Step 4** Enter the following command:

```
$ ./NDA3_0.setup.sh ./NDA3_0.SOL.Z
```

You have completed all of the required initial installation and setup procedures for using the Analyzer. If you want to skip the procedures in the "Optional Setup Procedures" section on page 2-4 and the "Setting Time Zones for the FlowCollector" section on page 2-9, you can go directly to the "Starting the Analyzer" section on page 2-10.

# Optional Setup Procedures

After completing the initial installation and setup procedures presented above, you can:

- Start the Analyzer and begin using it immediately. In this case, go to the "Starting the Analyzer" section on page 2-10.
- Perform the following optional setup procedures to customize constituent Analyzer modules.

## Customizing the Display Module

This section describes how to customize the Display module, which provides the user interface for the Analyzer.

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

You can configure the Display module to run independently on a workstation or a PC apart from other the Analyzer modules.

After completing the installation script (as described earlier in the "Installing and Running the Analyzer" section on page 2-4), you can customize the Display module to run in your particular networking environment by editing the start.Display file. The start.Display file is located in the directory /opt/CSCOnfa/NFADisplay/bin/.

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

**Table 2-1 Display Module Customization Parameters**

| Switch Name | Description of Editable Argument |
|---|---|
| -utilityserver | IP address or name of the workstation on which the UtilityServer will be running. You must change the placeholder value UTILITYSERVERHOST to the host name or IP address where the UtilityServer will be running. |
| -utilityserverport | Port on which the UtilityServer listens for network commands. The default port number is 7545. |
| -displayserver | IP address or name of the workstation on which the DisplayServer will be running. You must change the placeholder value DISPLAYSERVERHOST to the host name or IP address where the DisplayServer will be running. |
| -displayserverport | Port on which the DisplayServer listens for network commands. The default port number is 7544. |
| -width | Width (in pixels) of the Display window. The default is 800 pixels. |
| -height | Height (in pixels) of the Display 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 the name of this directory. |
| -defaulttreefile | Use the argument to this switch to identify a user-created file that contains a working tree structure appropriate to your Analyzer operating domain. After you create this file and reference it 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. This working tree structure can refer to a single network device or a defined group of devices (routers or switches). The latter case enables you to issue Display module commands that act on group members as a whole for data retrieval and analysis purposes. By defining a default tree file that is automatically loaded on Display module startup, you 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 "Loading a Tree File" section on page 3-15 in Chapter 3. |
| -browser | The argument to this switch is the name of the browser executable that you intend to use to view the Analyzer's Help system. If the name of the browser is not referenced in your $PATH environment variable, this switch argument must reference the full path name of the browser executable. |
| -helppath | The argument to this switch is the name of the directory containing the Analyzer's Help files. On the Solaris platform, this parameter defaults to: /opt/CSCOnfa/NFADisplay/help. |

# Customizing the UtilityServer Module

After you install the Analyzer (see the "Installing and Running the Analyzer" section on page 2-4), you can perform the following steps to customize the UtilityServer module:

**Step 1** Log in as root (superuser):

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

**Step 2** Use the TCP default port number (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 number of the port you want to use in place of the default value 7545.

**Step 3** Create the configuration files described in the "Managing UtilityServer Configuration Files" section below.

---

**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, refer to the "Maintaining UtilityServer Output Directories" section on page 4-2 of Chapter 4.

---

## Managing UtilityServer Configuration Files

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

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

You create these files and enter appropriate configuration information, as described below.

### HostPreferences.txt File

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

When the Analyzer needs to convert IP addresses to the aliases of host devices, it checks the contents of the HostPreferences.txt file first. Aliases for hosts not listed in this file are determined by means of Domain Name System (DNS) lookup.

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

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

Examples include:

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

### RouterAliases.txt File

Create this file only if you used the RouterAliases.txt file in Version 2.0 of the Analyzer. You can copy the Version 2.0 RouterAliases.txt file into the /opt/CSCOnfa/NFAUtility/config directory.

The UtilityServer module reads 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) and 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.

Use the following format in creating each line of the RouterConfig.txt file:

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

Examples include:

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

In all cases, enter "`netflow`" following the <SNMP community> parameter of each line in the RouterConfig.txt file.

## Customizing the DisplayServer Module

This section describes how you can alter the behavior of the DisplayServer module to suit your NetFlow data analysis needs by changing some of the parameters in the NFADS.resources file. For example, you can customize the DisplayServer module to:

- Change the number of the protocol port on which the DisplayServer module listens for network commands.
- Change the amount of memory used by the DisplayServer module or the file size allowances defined for the module.

---

**Note** See the "Calculating Available Memory and Adjusting the MaxMB Value" section on page 4-4 in Chapter 4 to determine how much logical memory is available on your Analyzer workstation or PC and how to fine-tune the platform 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 NetFlow data processing requirements (see Table 2-2).

When you change the configuration parameters in the NFADS.resources file from their default values, observe the following rules:

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 (see Table 2-2) is treated as a comment and ignored.

4 If a parameter is defined more than one time, the last such parameter definition encountered in the NFADS.resources file takes precedence.

To change the default parameters in the NFADS.resources file, use the following format in editing the lines in the 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 to meet your particular NetFlow data processing needs.

**Table 2-2 DisplayServer Module Customization Parameters**

| Parameter Keyword | Default Value | Range of Values | Description |
|---|---|---|---|
| Port | 7544 | Min: 5000<br>Max: 10000 | Port number on which the DisplayServer listens for network commands. |
| MaxSimultaneousCommands | 24 | Min: 1<br>Max: 64 | Defines the maximum number of commands that the DisplayServer accepts. |
| MaxMB[1] | 224 | Min: 32<br>Max: The most your system can handle | Defines the size of the dynamic memory pool in megabytes (MB) for the DisplayServer.<br>For optimum performance, ensure that this value is no greater than the amount of physical RAM, minus 32 MB, and no greater than the amount of free memory, minus 100 MB (approximately).<br>You can set the value of the MaxMB parameter 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 system swap space is exhausted. |
| MaxMBperCommand | 224 | Min: 24<br>Max: Value of MaxMB | Defines the maximum amount of memory in megabytes (MB) that will be used in executing a single network command.<br>Ensure that the parameter value of the MaxMBperCommand does not exceed that of the MaxMB command. If it does, the DisplayServer automatically changes the value of the MaxMBperCommand parameter to agree with that of the MaxMB parameter. |
| Max_Stored_NoWait_MB | 384 | Min: 2<br>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 DisplayServer /opt/CSCOnfa/NFAServer/Cache directory. 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 any value that the DisplayServer workstation or PC can handle.[2]<br>The default value is 384 MB. |

**Table 2-2 DisplayServer Module Customization Parameters (continued)**

| Parameter Keyword | Default Value | Range of Values | Description |
|---|---|---|---|
| MaxWellKnownProtocolPort | 1023 | Min: 0<br>Max: 65535 | Defines the maximum “well-known” protocol port number for the DisplayServer. 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. |
| MaxRegisteredProtocolPort | 1023 | Min: 0<br>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<br>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 “Maintaining the DisplayServer Cache Directory” section on page 4-3 in Chapter 4.
2. Memory use by the DisplayServer is limited primarily by the value of the MaxMB parameter, as defined in the NFADS.resources file. Do not configure the DisplayServer to use excessive memory. Doing so may exhaust available system swap space on your Analyzer workstation, resulting in severe disk thrashing.

# Setting Time Zones for the FlowCollector

This section describes how to prevent time zone problems that can affect the operation and use of the Analyzer. This step should be taken during the configuration of the NetFlow FlowCollector application. For more information about this application, refer to the *NetFlow FlowCollector Installation and User Guide*.

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 (GMT) at the time daylight saving time causes the local clock to be shifted backward in the fall. A convenient way to address these problems is to run the FlowCollector using GMT.

To run the FlowCollector using GMT, you must edit the nf.resources file of the FlowCollector 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 follows:

```
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 nfconfig.file of the FlowCollector.

# Starting the Analyzer

To start the Analyzer modules on a UNIX platform, 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 modules of the Analyzer:

```
# start.All
```

To start only the Display module, issue the following command:

```
# cd NFADisplay/bin
# start.Display
```

To start the Display module on a PC platform, perform the following steps:

**Step 1** Issue the following commands to change to the directory in which the Display module files are stored:

```
C:\> cd NFADisplay\bin
C:\NFADisplay\bin>
```

**Step 2** Issue the following command to start the Display module:

```
C:\NFADisplay\bin>startPC_Display
```

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

During normal operations, it is recommended that you leave the UtilityServer module and the DisplayServer module running at all times. If a problem occurs, such as after a power loss or a system crash, you must restart these modules.

For instructions on stopping any one of the Analyzer modules, checking its status, or starting it individually, see the “Controlling Analyzer Modules” section on page 4-5 in Chapter 4.

If the UtilityServer and the DisplayServer are already running on your host Analyzer workstation, see the “Starting the Display Module” section on page 4-7 in Chapter 4 for instructions on starting the Display module by itself.