NEC

MasterScope

Network Flow Analyzer 2.0

Release Notes

Copyrights

Export Precautions

While exporting this product, make sure that the rules and regulations of foreign exchange as well as foreign trade and rules and regulations of export management of America are confirmed and necessary procedures are followed.

Further, in case of any doubt please contact our nearest sales office.

Trademarks

Preface

Thank you for choosing MasterScope Network Flow Analyzer 2.0 (hereafter referred to as "NFA"). NFA provides the functions to analyze flow information of the communication on the network and visualize the communication status.

This manual describes the functional items released in this version of NFA and the contents of the NFA installation media. Before using NFA, please read this manual carefully.

Notations and Text Conventions

In this manual, the following notations are used to indicate items that require special attention and supplementary information.

Notations of Items Requiring Attention and Supplementary Information

Notation	Description
Caution	Indicates important points that the user should observe to configure and use the product properly.
Tip	Indicates useful information.

In this manual, the following text conventions are used.

Text Conventions

Notation	Description	Example
	Indicates graphical user interfaces such as dialog boxes, tabs, menus, items, and buttons.	**Dashboard** tab, **OK** button
<userinput>	Indicates items that change depending on the user environment or items that the user must specify.	*<%installation directory%>*, *<filepath>*
`configuration file`	Indicates the contents of the configuration file.	Set the following value: `port = 27120`
`command line`	Indicates command line operations.	Run the following command: `$ rpm -q nec-nfa-controller`

In this manual, the following abbreviations are used.

Abbreviations

Formal Name	Abbreviation
MasterScope Network Flow Analyzer	NFA
MasterScope Integrated Management Server	IMS
MasterScope Network Manager	Network Manager

The default installation directory of this product is as follows:

Default installation directory:

```
/opt/nec/nfa
```

In this manual, the above installation directory is referred to as <*%installation directory%*>. If you installed this product in another directory, please replace this directory name with the appropriate directory name.

In addition, when you install this product, you can specify a different directory to store the data that will be managed by this product. In this manual, the data storage directory is referred to as <*%data directory%*>. If you install this product and store the data in the same directory, <*%data directory %*> and <*%installation directory%*> indicate the same directory.

Contents

Chapter 1. Product Overview

This chapter describes an overview of NFA.

Contents

1.1 Product features

NFA provides the functions required to intuitively analyze the flow information of communications on a network using simple operations, and visualize the communication status from a variety of perspectives.

NFA performs fine-grained analysis of the source and destination of communications, the communication type, and the communication traffic, and displays the communication status, thereby enabling the network to operate stably.

Fine-grained analysis of communication status based on flow information (NetFlow and sFlow)

SNMP is widely used to check the communication status of the network. SNMP can check the communication traffic passing through interfaces such as switches and routers. However, SNMP cannot be easily used to check the details of the communication traffic.

NFA uses flow information (NetFlow and sFlow) instead of SNMP to analyze the communication status. Analysis using flow information allows fine-grained checking of communication traffic details that cannot be checked by using SNMP, such as the source and destination of the communication, the communication type, and the communication traffic. By understanding the communication status in detail, you can efficiently investigate causes of network failures and effectively manage network capacity.

Simple drill-down analysis

NFA allows you to narrow down the information on charts and lists with a single click.

For example, by performing the following intuitive and simple operation on the information displayed on the page, you can check the detailed communication status immediately.

Operation example:

1. Select an interface (for example, Ethernet1/1) from the display showing the communication traffic passing through each interface.

   (The display is narrowed down to the communication traffic on the selected Ethernet1/1.)
2. Select an application (for example, http) from the display showing the communication traffic for each application.
3. The results of analyzing the http communication traffic on Ethernet1/1 are displayed.

Free customization of display contents

NFA allows you to customize the display contents freely to improve visibility.

For example, by customizing the display and analysis contents according to your operating environment as follows, you can gain an accurate understanding of the network status.

Customization examples:

- The contents of charts and lists displayed in the Dashboard (main page) can be defined for each user who logs in to NFA.
- The analysis results can be visualized clearly by uniquely defining job application communications or specifying the target department by using an IP address range.

1.2 Functional overview

The following describes the functions that are provided by NFA.

Dashboard

- This displays the current communication status and event occurrence status of the network managed by the user who is currently logged in to NFA.
- All displayed analysis results can be exported to a CSV file.
- A **widget**, which is an element used to display a chart or list, can be freely located on the dashboard page by a drag-and-drop operation, allowing each user to define the dashboard according to their needs.

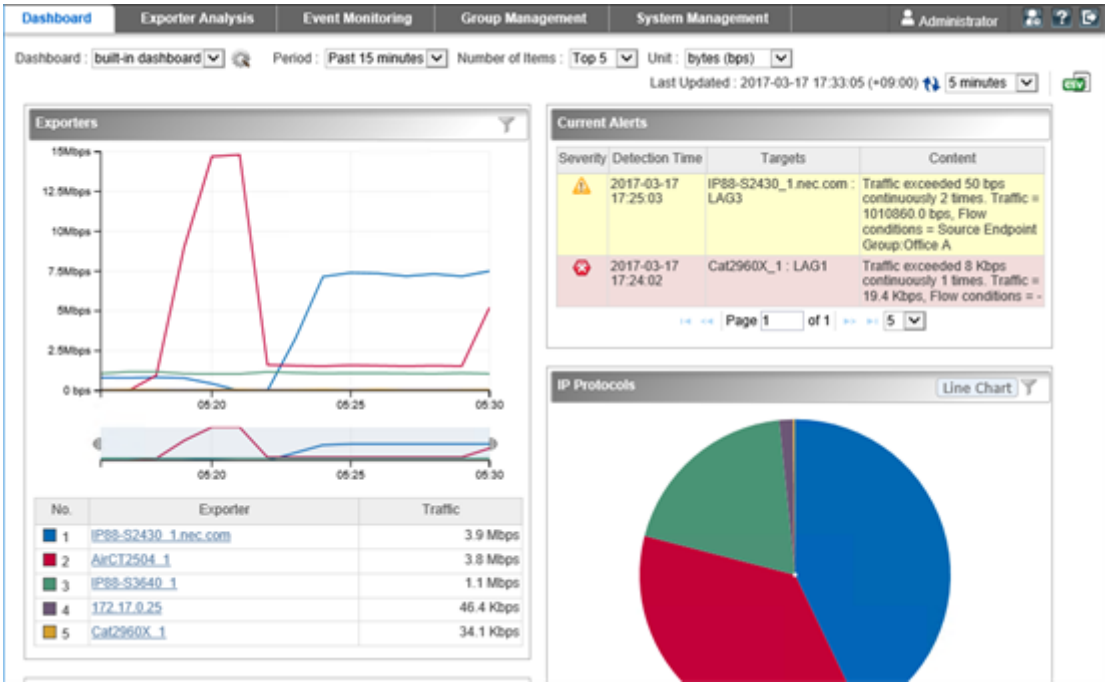

Figure 1-1 Dashboard

Exporter analysis

- Fine-grained analysis of the communication status can be performed by narrowing down the exporters that send flow information and their interfaces.
- Not only the current communication status but also previous communication status can be analyzed, allowing you to check mid-and-long-term changes in the communication status.
- All displayed analysis results can be exported to a CSV file as well as on the Dashboard page.

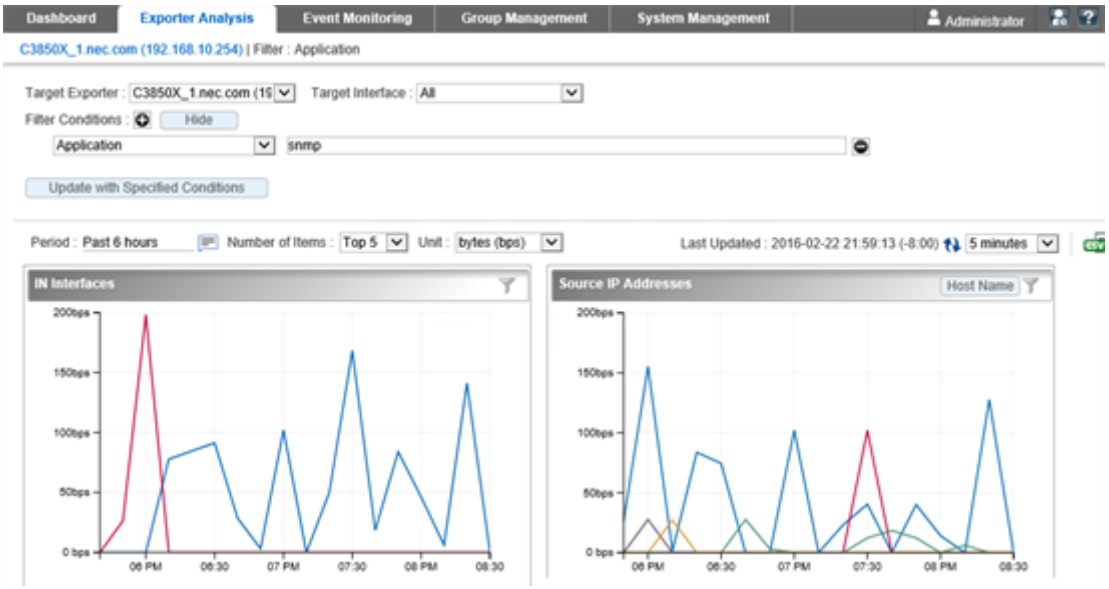

Figure 1-2 Exporter analysis

Event monitoring

- The communication traffic narrowed by conditions such as source and destination IP address or application can be monitored by specifying a threshold.
- The history of threshold violation and recovery event occurrence is displayed in a list. If a current alert widget is set up on the Dashboard page, the current event occurrence status is displayed on the Dashboard page.
- Threshold violation and recovery events can be sent to another management system by using the SNMP trap format.

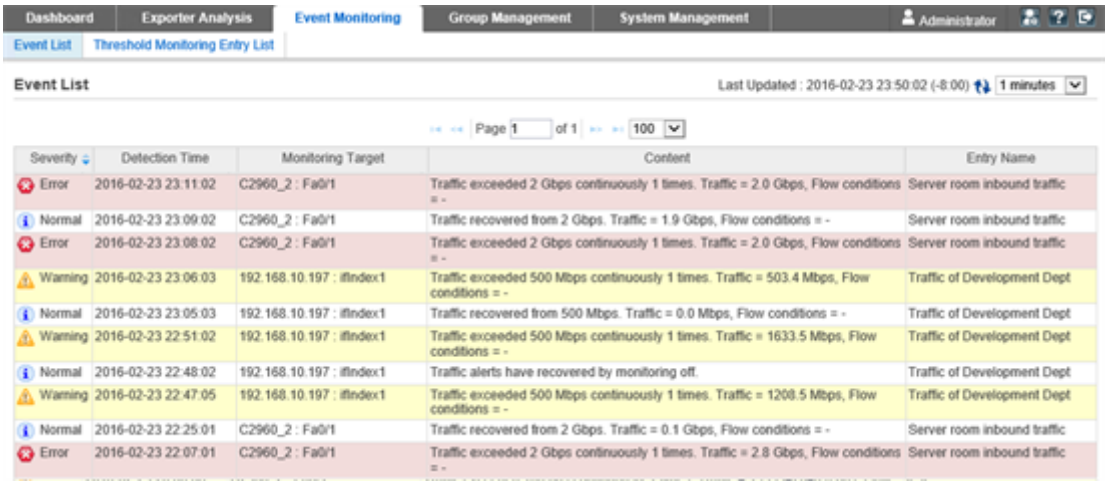

Figure 1-3 Event list

Group management

- The communication traffic can be analyzed in units of groups by grouping multiple IP addresses or network addresses that are endpoints (source or destination) of communication.
- By grouping multiple interfaces that configure a Link Aggregation (LAG), the communication traffic passing through those interfaces can be analyzed as one LAG interface.

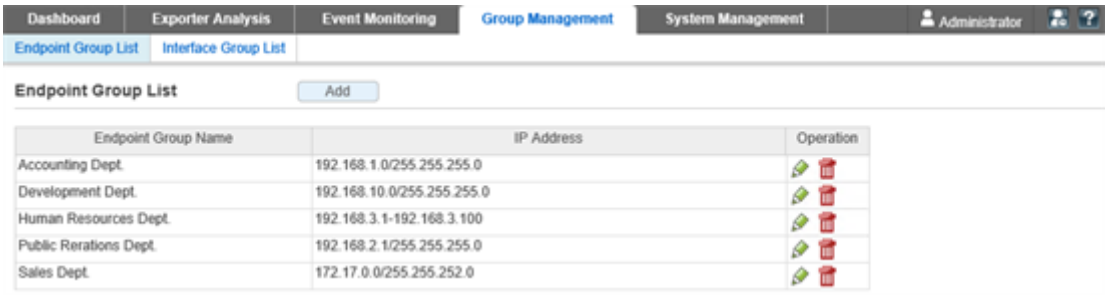

Figure 1-4 Endpoint group list

System Management

- Applications that are used to analyze the communication status can be defined. An application can be defined in detail by combining an IP protocol, port number, and a source or destination IP address.
- The exporters that send flow information, their interfaces, and license assignment status can be managed in a list.
- NFA user information, such as a password or default dashboard definition, can be managed.

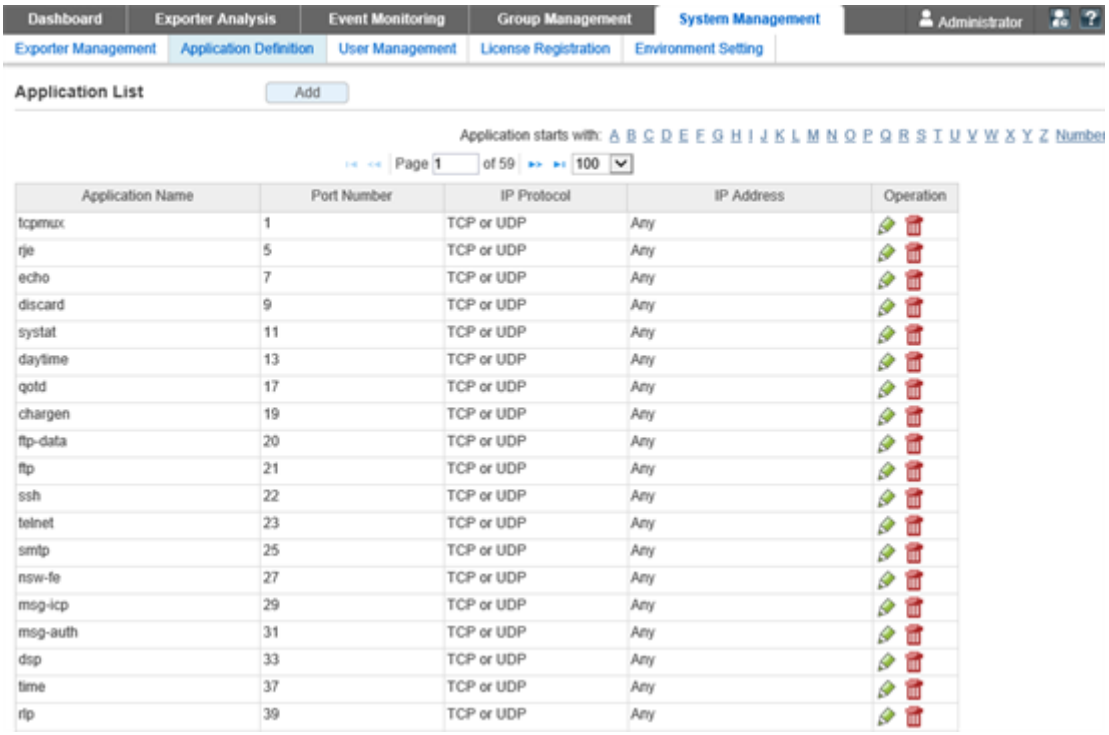

Figure 1-5 Application definitions

Chapter 2. Operating Environment

This chapter describes the operating environment of NFA.

Contents

2.1 System configuration

The following describes the system configuration of NFA.

System configuration of NFA

The NFA operating environment consists of a server to which NFA is installed (NFA server), the terminals of the NFA users, exporters, and endpoints as shown in "Figure 2-1 System configuration diagram (page 7)".

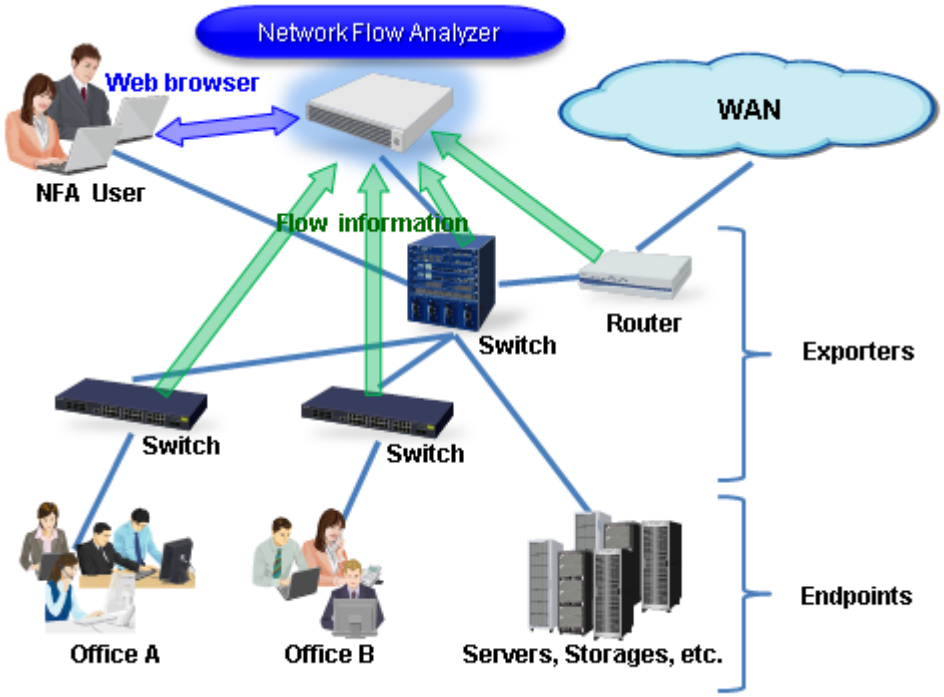

Figure 2-1 System configuration diagram

NFA has two roles: one is a flow collector that receives and accumulates flow information, and the other is a flow analyzer that analyzes the communication status according to the accumulated flow information. A web server function that provides operation pages for NFA users is also included. In NFA, the flow collector function is called *"collector"*, and the flow analyzer and web server functions are collectively called *"controller"*.

NFA users can connect to the NFA web console via a web browser from their terminals.

Tip

- In NFA, terminals and servers that connect to a network and perform communication are collectively called an endpoint.
- Switches and routers that convert communication contents between endpoints to flow information and send the information to NFA are collectively called an exporter.

System configuration when using IMS component

By using the IMS component, it is possible to integrate the operation of multiple NFAs, or NFA and Network Manager. A system configuration example at integrated operation is shown in "Figure 2-2 System configuration example at integrated operation (page 8)".

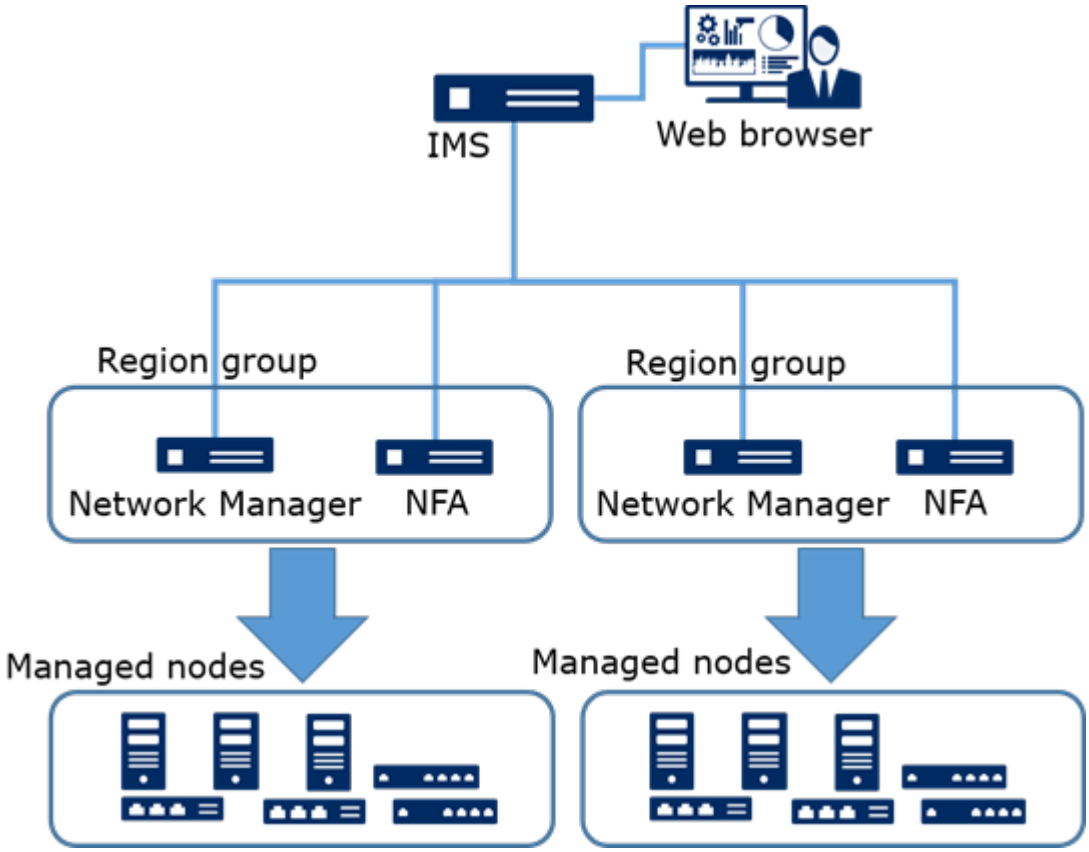

Figure 2-2 System configuration example at integrated operation

NFA and Network Manager which manage the same node (exporter) are grouped by Region group as shown in "Figure 2-2 System configuration example at integrated operation (page 8)". In the Web Console of the IMS component, information of the same node (exporter) managed by each product in the same Region group is integrated and displayed.

Tip

It is possible to install NFA and IMS component on the same server. However, it may cause problems such as slow response to the operation. Therefore, thoroughly assess the system configuration before starting operations. If possible, it is recommended to install them separately on multiple servers.

2.2 System requirements

The following describes the system requirements for properly operating NFA and the supported environment.

Table 2-1 Server system requirements

Item	Description
CPU	Intel Quad-Core Xeon or higher, or equivalent compatible processor recommended
System memory	4 GB or more (8 GB or more recommended)
Disk capacity	Installation directory: 5 GB or more
	Data directory: 100 GB or more [1)]
OS	• Red Hat Enterprise Linux 6 (x86_64) [2)] • Red Hat Enterprise Linux 7 (x86_64)

Item	Description
Flow protocol	• NetFlow (v5, v9) • IPFIX • sFlow (v4, v5) Sampling mode is supported for NetFlow and IPFIX.

Note

1. This product frequently accesses the hard disk on specifications. It is recommended to use hard disk with high access performance such as SAS 15,000 rpm according to usage environment.
2. Operation with version 6.6 or higher OS is supported.

Table 2-2 Web browser requirements

Item	Description
Supported browser	The following browsers running on Windows • Internet Explorer 11 • Mozilla Firefox 60 or later • Google Chrome 71 or later
CPU	Intel Core i3 or higher, or equivalent compatible processor recommended
System memory	1 GB or more

Tip

- It is recommended to apply the latest bug fix updates to the browser before using it. If the bug fix updates have not been applied, some functions might not work properly.
- Depending on a browser, a Unicode surrogate pair character is treated as two characters. In this case, an actual number of characters that can be input to each input field will be less.

2.3 Flow data management

NFA manages received data in a database. The following describes how flow data is managed.

2.3.1 Flow data retention periods and data aggregation

To store large amounts of data for a long period with a limited disk capacity, NFA manages received data by aggregating it every unit time shown in "Table 2-3 Data unit times and retention periods (page 9)" and changing the data granularity. In addition, NFA defines the retention periods for each data unit time and discards the data beyond the defined retention periods. You can change the retention period.

Table 2-3 Data unit times and retention periods

Data unit time	Default retention period	Available range for retention period
1 minute	24 hours	2 to 168 hours
10 minutes	72 hours	12 to 336 hours
60 minutes	14 days	4 to 60 days
6 hours	60 days	14 to 365 days
24 hours	365 days	60 to 1095 days

Data unit time	Default retention period	Available range for retention period
7 days	1095 days	365 to 2190 days

The flow data aggregation processing aggregates all flow data whose seven flow keys described below are the same for each unit time.

1. Source IP address
2. Destination IP address
3. Source port number
4. Destination port number
5. IP protocol
6. ToS byte (DSCP)
7. Input Interface

In addition, to minimize the disk capacity required to accumulate flow data, NFA also performs the following operations in the aggregation process.

- Manages data of the top 1,000 flows whose communication traffic is large per unit time as a target of detailed analysis.
- Aggregates and manages data of flows below the top 1,000 as *"other"* flows.

2.3.2 Estimating the required disk capacity

The following describes the procedure to estimate the disk capacity required to accumulate and manage received flows.

The disk capacity required to accumulate and manage flow data depends on the number of exporters managed by NFA and the flow occurrence frequency. As described in "2.3.1 Flow data retention periods and data aggregation (page 9)", NFA defines the retention periods of flow data per unit time and the maximum number of flows to be stored. Therefore, the estimated disk capacity required to accumulate the flow data can be obtained by a formula that takes into account these definitions.

⚠ Caution

The larger the number of exporters, the larger the flow data size. There is therefore a risk that the disk capacity will be exhausted. If the disk capacity is exhausted, new flow data cannot be received, and the system as a whole cannot operate properly. Therefore, we recommend assigning a slightly smaller value for the maximum number of flows.

The specific calculation method is described below.

1. Check the number of exporters managed by NFA.

   If it is possible that the number of exporters will increase in the future, clarify the final number of managed exporters.

2. Check the retention periods of flow data, and calculate the coefficient by using the following formula:

   Coefficient of retention periods: $P = P1 \times 60 + P2 \times 6 + P3 \times 24 + P4 \times 4 + P5 + P6 \div 7$

   - P1: Retention period of 1 minute unit data (unit: hour)
   - P2: Retention period of 10 minutes unit data (unit: hour)
   - P3: Retention period of 60 minutes unit data (unit: day)

- P4: Retention period of 6 hours unit data (unit: day)
- P5: Retention period of 24 hours unit data (unit: day)
- P6: Retention period of 7 days unit data (unit: day)

Round the calculation result up to zero decimal point.

If the retention periods of flow data remain at those default values, the coefficient P is equal to 2,970.

Tip

For details of the flow data retention periods, see "2.3.1 Flow data retention periods and data aggregation (page 9)".

3. Check the flow occurrence frequency (average number of flows per minute) in the operating environment.

   Assume that the average number of communication sessions that have occurred per minute in the operating environment is the approximate flow occurrence frequency.

4. Calculate the estimated disk capacity by using the following formula:

   Estimated disk capacity [MB] = (N + 5) × P × L × 0.000415 + A × 0.15 + 10,000 [MB]

   - N: Number of exporters managed by NFA

     Assign the value that was checked in step 1.

   - P: Coefficient of the flow retention periods in NFA

     Assign the value that was checked in step 2.

   - L: Maximum number of flows to be stored per unit time

     By default, the maximum number of flows to be sored is 1,000.

   - A: Average number of flows per minute that NFA received

     Assign the value that was checked in step 3.

Calculation example:

When the number of exporters is 50, the retention periods and the maximum number of flows to be stored per unit time remain at those default values, and the average number of flows per minute is 600,000, the calculation result is as follows:

- N = 50
- P = 2,970 (24 × 60 + 72 × 6 + 14 × 24 + 60 × 4 + 365 + 1095 ÷ 7)
- L = 1,000
- A = 600,000
- Estimated = (50 + 5) × 2,970 × 1,000 × 0.000415 + 600,000 × 0.15 + 10,000 ≒ 163.9GB

Chapter 3. Documents

The following describes the NFA documents supplied with this version.

Table 3-1 NFA documentation

Title (File name)	Description
MasterScope Network Flow Analyzer 2.0 Release Notes (nfa-release.pdf)	This document. The NFA 2.0 release contents are described.
MasterScope Network Flow Analyzer 2.0 Getting Started Guide (nfa-startup.pdf)	This describes the procedure to set up NFA 2.0. Procedures of the new installation and upgrade (version up) are described in it.
MasterScope Network Flow Analyzer 2.0 Reference Manual (nfa-reference.pdf)	This describes the procedures to use and operate NFA 2.0.
MasterScope Network Flow Analyzer 2.0 Open Source Software License Acknowledgement (nfa-oss-license.pdf)	This describes the license agreements and copyrights of the open source software that NFA 2.0 uses.

Chapter 4.
Added and Enhanced Functions

This chapter describes the released contents.

Contents

4.1 Contents released in version 2.0

The following describes the additional functions and improvements of NFA 2.0.

4.1.1 Integrated operation using IMS component

By using the MasterScope Integrated Management Server (IMS) component, it has been now possible to integrate the operation of multiple NFAs, or NFA and Network Manager.

By using the Web Console provided by IMS component, the following operations are possible.

- In environments using multiple NFAs, widgets of each NFA can be arranged side by side on one dashboard. This makes it easy to grasp the status of the entire network to be managed.
- You can check the status of SNMP monitoring by the Network Manager and the flow information by the NFA at the same time. This makes it smoothly investigate the cause of network failure.
- You can launch the Web Console provided by the NFA from the Web Console provided by the IMS component with single sign-on. This makes it seamlessly enable the operation the two Web Consoles.

In addition to the above, by using the IMS component, it is possible to notify the threshold monitoring event of the NFA by sending e-mail or executing arbitrary command.

4.1.2 Flow analysis in terms of DSCP

NFA 2.0 can now analyze using the DSCP value in flow information.

By analyzing the flow information using the DSCP value, you can check the following communication status.

- Check whether the intended QoS setting (marking by DSCP) is being performed for packets flowing on the route.
- Check the change in communication status due to QoS setting (DSCP setting).
- Check the communications traffic for each priority of DSCP.

Specifically, the functions to analyze flow information using the DSCP value are as follows:

- Dashboard

  The **DSCP** widget has been added as a pie chart or line chart widgets. You can check the communications traffic for each DSCP value (PHB).

- Exporter analysis

  You can check the flow information analysis result with the **DSCP** widget. And By specifying the DSCP value (PHB) as the filter condition, you can check the communications traffic and the communication contents for a specific DSCP value (PHB).

- Threshold monitoring

  You can specify the DSCP value (PHB) as the condition of the flow subject to threshold monitoring.

- CSV file output

  On the Dashboard page and the Exporter Analysis page, the flow information analyzed and displayed by the **DSCP** widget can be output as a external CSV file like other widgets.

In the `nfa_flow_export` command, the DSCP value (PHB) has been added to the CSV file to be output, in addition to the items previously supported.

4.1.3 Fixed issues in version 2.0

The following describes the issues that have been fixed in version 2.0.

1. The following OSSs have been upgraded to incorporate bug corrections.
   - Java Runtime (upgraded to 8u131)
   - Apache Tomcat (upgraded to 8.5.35)
   - Apache Struts2 (upgraded to 2.3.36)
   - Apache Commons Collections (upgraded to 3.2.2)
   - Apache Commons FileUpload (upgraded to 1.3.3)
   - Apache Commons BeanUtils (upgraded to 1.9.3)
   - Apache Commons Logging (upgraded to 1.2)
2. When setting the exporter's display name or endpoint group name or application name to "*Other*", a link for the "*Other*" was not created in the "**Exporters**" and "**Source Endpoint Groups**" and "**Destination Endpoint Groups**" and "**Applications**" widgets.
3. nfa_collector process might terminate abnormally when stopping the service.
4. When sFlow exporter was configured to monitor outbound traffic, the flow information from the exporter might not be displayed correctly.
5. In the database that stores the received flow information, the data size might bloat.

4.2 Contents released in version 1.1

The following describes the additional functions and improvements of NFA 1.1.

4.2.1 Flow data export function

The `nfa_flow_export` command has been added to output flow data accumulated in a database in CSV files.

This command makes it possible to save the accumulated data in external files for long term storage without reducing data granularity.

Major examples of operations using this command are as follows:

- Detailed past data is saved in external files for long term storage.
- Source data to create an analysis report is generated periodically by calling this command from cron or other programs.
- The communication status when an incident occurs and event details are saved automatically by calling this command from external operation management software.

The CSV file created by this command can be edited or analyzed freely by importing the file into external spreadsheet software. Flow data can be flexibly output in CSV files according to each operation, such as by specifying an analysis period or specifying to continue from the previous command execution.

This function is a command line interface (CLI). Therefore, a web browser is not required.

4.2.2 Dynamic changing of the flow data retention periods

To store large amounts of data for a long period, NFA aggregates data for every period and changes the data granularity. This function has been enhanced in NFA 1.1 so as to change the retention periods.

The following table shows the default retention periods and available ranges for retention periods.

Table 4-1 Data unit times and retention periods

Data unit time	Default retention period	Available range for retention period
1 minute	24 hours	2 to 168 hours
10 minutes	72 hours	12 to 336 hours
60 minutes	14 days	4 to 60 days
6 hours	60 days	14 to 365 days
24 hours	365 days	60 to 1095 days
7 days	1095 days	365 to 2190 days

You can change the retention periods without stopping operations. Therefore, if the number of monitoring exporters increases or the disk space becomes low due to storing large amounts of flow data during an operation, you can take appropriate action by changing the retention periods.

You can also set a different retention period for each data unit time. Retention periods can be changed according to the purpose of operation. For example, the retention period of detailed flow data is increased and the retention period of coarse-grained data is decreased.

4.2.3 Performance improvement of the threshold monitoring function

The processing performance of the threshold monitoring function has been improved. NFA 1.0 recommends specifying no more than 150 monitoring items. In NFA 1.1, more items can be monitored because the processing performance of the threshold monitoring function has been improved.

NEC has verified that this product can monitor 2,000 items in the following environment.

Table 4-2 Environment in which 2,000 items can be monitored

Item	Support
CPU	Intel E5-2630v3(2.40 GHz) * 8 core
System memory	64 GB
Disk	2.5 inch SAS (15000 rpm)
OS	Red Hat Enterprise Linux 7.3 (x86_64)
Number of flows	20,000 flows per second

4.2.4 Supported flow protocol enhancement

NFA 1.1 supports NetFlow sampling. Also, this version supports IPFIX as a flow protocol.

NetFlow sampling

Flow information can now be analyzed even if the exporter sends NetFlow Lite and other sampled information. You can manually set a different sampling rate for each exporter. If the received flow information includes a sampling rate setting, the sampling rate setting can be read automatically.

IPFIX

IPFIX is now supported as a flow protocol. Even if the sampled flow information is received, flow data can be analyzed adequately by setting a sampling rate manually.

4.2.5 Chart display type switching function

The application and IP protocol widgets have been enhanced so that both a pie chart and line chart are displayed.

In NFA 1.0, only a pie chart can be displayed on the application and IP protocol widgets. NFA 1.1 has been enhanced so that a line chart is displayed in addition to a pie chart.

This makes it possible to analyze a flow in chronological order in terms of application or IP protocol.

The chart display can be switched dynamically between a pie chart and line chart on the Dashboard page and Exporter Analysis page.

On the Dashboard page, the default chart display can be defined as a pie chart or line chart. Additionally, by defining multiple widgets, a pie chart and line chart can be displayed side by side.

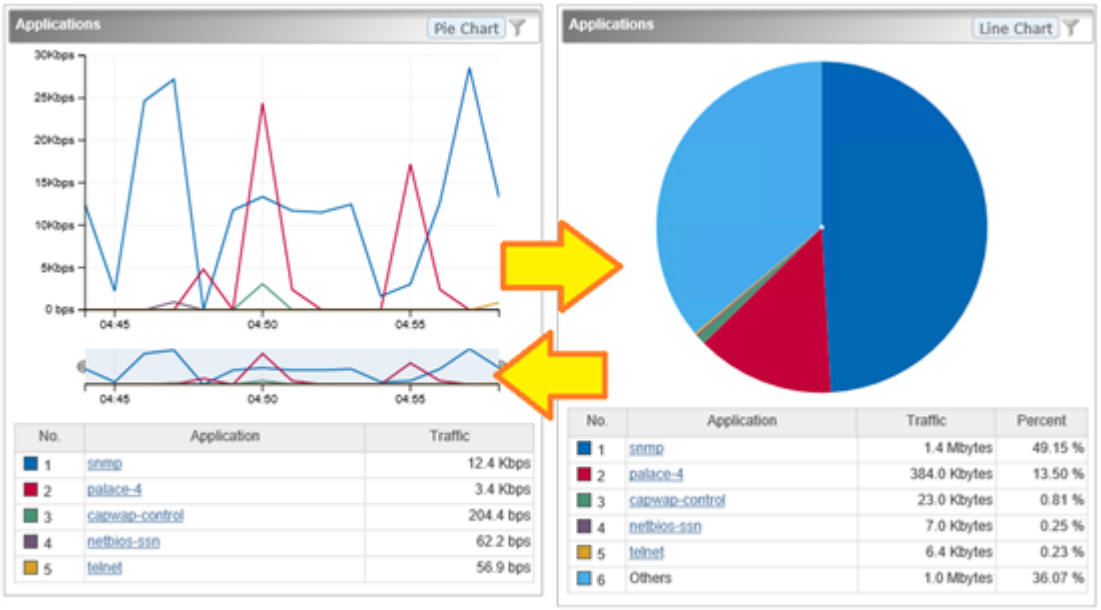

Figure 4-1 Pie chart/line chart widgets

4.2.6 Specification changes in version 1.1

The following describes the specification changes in version 1.1.

4.2.6.1 Changes to the analysis result output to a CSV file

The specifications to output the analysis result from the Dashboard and Exporter Analysis pages to a CSV file have been changed.

Changes to the file names

- Download file name

  The name prefix of the download file to be output in a CSV format on the Exporter Analysis page has been changed.

Before change	After change
ExporterAnalyzeCSV_	ExporterAnalysisCSV_

- CSV file name

  The widget names of a CSV file in the downloaded zip file have been changed.

Before change	After change
ExporterTraffic	Exporters
InterfaceInputTraffic	InInterfaces
InterfaceOutputTraffic	OutInterfaces
srcIPAddress	SourceIPAddresses
dstIPAddress	DestinationIPAddresses
Conversation	Conversations
srcEndPointGroup	SourceEndpointGroups
dstEndPointGroup	DestinationEndpointGroups
srcAS	SourceAS
dstAS	DestinationAS
Application	Applications
IPProtocol	IPProtocols
CurrentAlert	CurrentAlerts

Changes to the CSV file contents

- Some item names have been changed.
  - Common

Before change	After change
StartTime	StartingTime
EndTime	EndingTime
Exporter	Exporters
Interface	Interfaces
FlowFilterCount	FilterCount
WidgetName	WidgetTitle

  - Widget names to be output from the Exporter Analysis page

Before change	After change
ExporterTraffic	Exporters
InterfaceInputTraffic	InInterfaces
InterfaceOutputTraffic	OutInterfaces

Before change	After change
srcIPAddress	SourceIPAddresses
dstIPAddress	DestinationIPAddresses
Conversation	Conversations
srcEndPointGroup	SourceEndpointGroups
dstEndPointGroup	DestinationEndpointGroups
srcAS	SourceAS
dstAS	DestinationAS
Application	Applications
IPProtocol	IPProtocols
CurrentAlert	CurrentAlerts

- Item names when the flow conditions are specified on the Exporter Analysis page

Before change	After change
srcIPAddress	SourceIPAddress
dstIPAddress	DestinationIPAddress
srcEndPointGroup	SourceEndpointGroup
dstEndPointGroup	DestinationEndpointGroup
srcAS	SourceAS
dstAS	DestinationAS

- The output formats of some values have been changed.
  - Time information of the following items is now output in the UNIX time format.
    - Date
    - StartingTime
    - EndingTime
    - <value indicating the time in a data line>
  - For the "Exporters" item, the value indicating "all exporters" has been changed as follows:

Before change	After change
(all)	(All)

  - For the "Exporters" and "Interfaces" items, an IP address is now added to the exporter name.

Before change	After change
Exporter-001	Exporter-001 (192.168.10.1)

  - The expression indicating that an interface, endpoint group, or application was deleted has been changed. The target widgets are as follows:
    - Input Interface
    - Output Interface
    - Source Endpoint Group
    - Destination Endpoint Group

* Application

Before change	After change
deleted	(deleted)

- If no target flow data exists, *"No Data"* is now output. The target widgets are as follows:
  * Application
  * IP protocol
- The CsvType value output from the Exporter Analysis page has been changed.

Before change	After change
ExporterAnalyze	ExporterAnalysis

- The value output formats of some data lines have been changed.
  - The expression indicating *"others"* has been changed. The target widgets are as follows:
    * Application
    * IP protocol

Before change	After change
(Other)	Others

  - The data label name of the current alert widget has been changed.

Before change	After change
OccurredTime,Severity,Target,Detail	Severity,DetectionTime,Targets,Content

4.2.7 Fixed issues in version 1.1

The following describes the issues that have been fixed in version 1.1.

1. The following OSSs have been upgraded to incorporate bug corrections.
   - Java Runtime (upgraded to 8u121)
   - Apache Tomcat (upgraded to 8.0.39)
   - Apache Struts2 (upgraded to 2.3.32)
   - Apache Commons FileUpload (upgraded to 1.3.2)
   - Log4j2 (upgraded to 2.5)
   - ICU (upgraded to 58.2)
2. The windows of Network Flow Analyzer could not be open from the WebGUI of UNIVERGE PF6800 Ver. 6.3.
3. If the start time is set to within one hour from current time and the period is set to *"To Current Time"* in the period specification on the Exporter Analysis page, the analysis result included data one minute before the time specified as the analysis start date.
4. When a choice other than *"To Current Time"* was specified for **Specify Starting Time and Period** on the Exporter Analysis page, the specified period and the period displayed as the analysis result were different (the displayed period of the analysis result was one unit time longer than the specified period).

   For details about the unit time, see *"Flow data retention periods and data aggregation"* in Reference Guide.

5. When *"Until the current time"* was specified for **Specify Starting Time and Period** on the Exporter Analysis page and the analysis result was output to a CSV file on the displayed analysis result page, the unit time of data of the line chart widget might be finer than the unit time on the page.
6. If a date three days before the current time was specified for the analysis start date in the analysis period specification on the Exporter Analysis page, the time might not be able to be specified (the pull-down list might not be able to be selected).
7. If an attempt was made to obtain DNS information or SNMP information from multiple exporters at the same time, information might not be able to be obtained, or the message indicating that the operation failed might be displayed on the page even if the information was obtained successfully.
8. The display processing performance of the Event List page is slow when there are many events.
9. If a flow that does not have a valid (1 or larger) identifier of the input side interface (IN ifIndex) is received, the following problems occurred.
    - If the relevant exporter is an sFlow exporter, values on a chart are displayed as 0.
    - Values displayed on a chart are incorrect because a received flow is aggregated assuming the flow is the same as another flow in flow data aggregation processing.

Chapter 5. Notes and Restrictions

This chapter describes the notes and restrictions for NFA2.0.

Contents

5.1 Notes and restrictions for exporter settings

The following describes the notes and restrictions for exporter settings.

5.1.1 SNMP ifIndex persistence configuration

To analyze flows correctly by using NFA, the exporter must be configured so that the ifIndex value corresponding to the analysis target interface does not change.

After the exporter is restarted, the ifIndex value corresponding to the analysis target interface may change depending on the exporter specifications.If the ifIndex value changes, NFA cannot identify the analysis target interface and the analysis results may not be displayed correctly.

An exporter can be configured so that the ifIndex value does not change, depending on the exporter specifications.Before starting the operation, check the exporter specifications concerning ifIndex value persistence and specify the settings so that the ifIndex value does not change.

The following is an example of exporter settings that ensure the ifIndex value does not change (for the Cisco Catalyst 6500 series).

```
(config)# snmp-server ifindex persist
```

⚠ Caution

The specifications of the command to be used to configure an exporter differ depending on the exporter model. Read the configuration manual of the exporter before configuring the exporter.

5.1.2 Using NetFlow v9

For NetFlow v9, NFA supports a specific format.

To use NetFlow v9, create a flow record definition including the following field types in the exporter settings.

1. Source IP address / destination IP address Note 1
2. Source port number / destination port number Note 1
3. IP protocol Note 1
4. ToS byte (DSCP) Note 1
5. Input interface / output interface Note 2
6. Number of bytes and number of packets in a flow Note 3

Note

1. It is not essential to include this field type. However, as long as there is no special reason not to, include them in the flow record definition of the exporter settings.

   If there is no relevant information in a flow record, this field is assumed to be an arbitrary value (zero). This means that the relevant widget cannot be displayed and the flow might not be analyzed correctly.
2. This field type must be included in the flow record definition of the exporter settings.

   This information is essential to assign licenses correctly.
3. This field type must be included in the flow record definition of the exporter settings.

   This information is essential to conduct a statistical analysis of the communication traffic of a flow.

The following is an example of a flow record definition of the exporter settings (for the Cisco Catalyst 3850 series).

```
(config)# flow record NetFlow-record
(config)# match ipv4 tos
(config)# match ipv4 protocol
(config)# match ipv4 source address
(config)# match ipv4 destination address
(config)# match transport source-port
(config)# match transport destination-port
(config)# collect interface input
(config)# collect interface output
(config)# collect counter bytes long
(config)# collect counter packets long
(config)# collect timestamp sys-uptime first
(config)# collect timestamp sys-uptime last
```

⚠ Caution

The commands to be used to configure an exporter differ depending on the exporter model. Read the configuration manual of the exporter before configuring the exporter.

5.1.3 Analyzing an IPv6 communication flow

NFA2.0 does not have a function to analyze an IPv6 communication flow .

If an IPv6 communication flow is set as a monitoring target in the exporter settings, NFA cannot process the relevant flow data.

To avoid unnecessary traffic, do not set an IPv6 communication flow as a monitoring target in the exporter settings.

MasterScope
Network Flow Analyzer 2.0
Release Notes

NFA00RE0200-01

February, 2019 01 Edition

NEC Corporation