NEC

MasterScope

Network Flow Analyzer 2.0

Reference Manual

Copyrights

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 functions of NFA and provides details of its operations. To take full advantage of the functions of NFA and efficiently use it, please carefully read and use this manual.

Configuration of This Manual

This manual consists of the following chapters. Read the chapters relevant to you according to your "Target reader" classification in the table below.

: NFA administrator. 

: all NFA users.

Configuration of This Manual

Title	Content	Target reader
"Chapter 1. Product Overview and Basic Operations (page 1)"	Provides an overview of NFA and describes the basic operations of the web console.	User
"Chapter 2. Environment Settings Before Operations (page 21)"	Describes how to configure the environment before using and operating NFA.	Admin
"Chapter 3. Environment Settings During Operations (page 40)"	Describes how to configure the environment as needed while using and operating NFA.	Admin
"Chapter 4. Operations (page 61)"	Describes how to use NFA during operation.	User
"Chapter 5. System Maintenance (page 83)"	Describes how to maintain NFA.	Admin
"Appendix B. Troubleshooting (page 115)"	Describes how to troubleshoot NFA.	Admin
"C.1 Port numbers used in this product (page 119)"	Describes the default port numbers used by NFA.	Admin
Glossary ("A - Z (page 122)")	Describes the functions of NFA and the terms and abbreviations that are used in this manual.	User

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 and Basic Operations

This chapter provides an overview of NFA and describes the basic operations of the web console.

Contents

1.1 Product Overview

This chapter describes an overview of NFA.

1.1.1 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.

1.1.2 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.

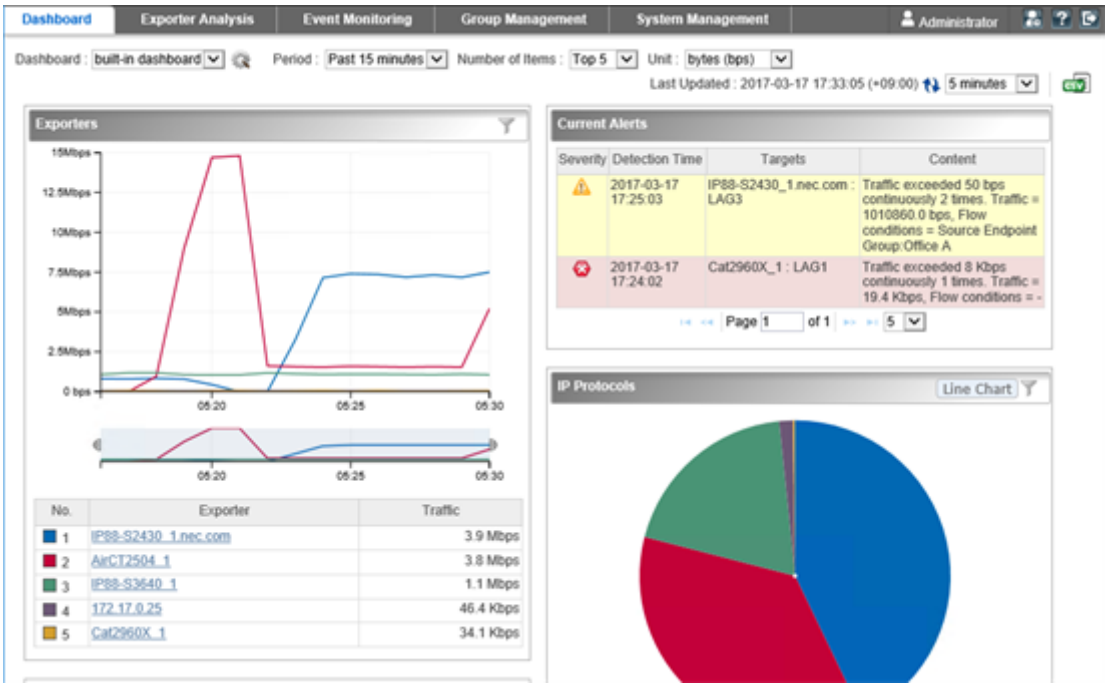

Figure 1-1 Dashboard

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.

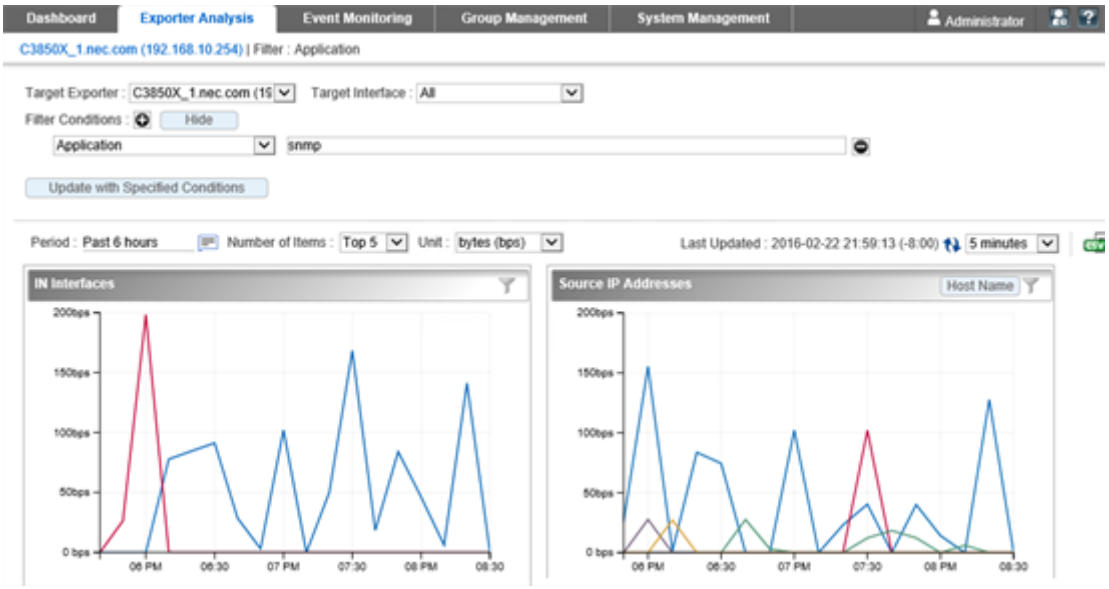

Figure 1-2 Exporter analysis

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.

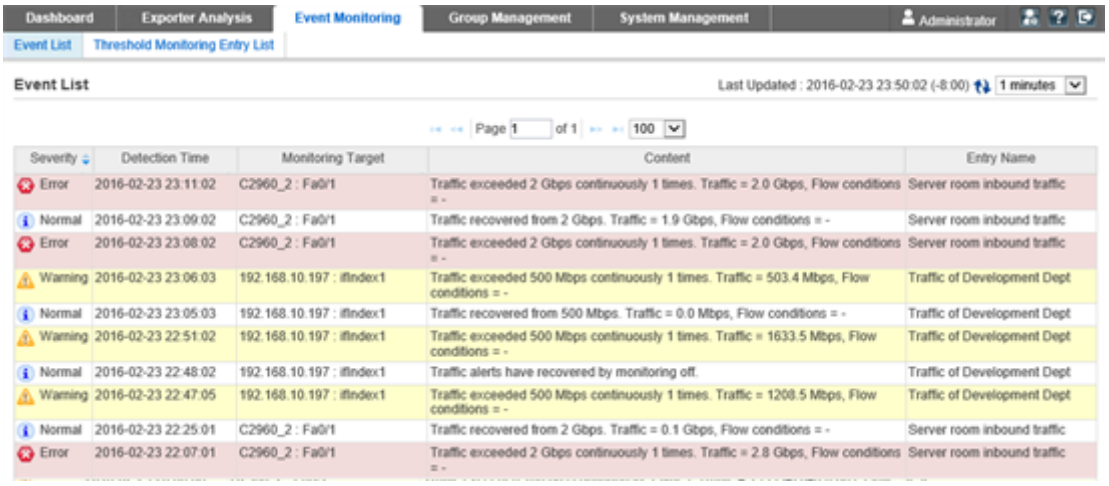

Figure 1-3 Event list

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.

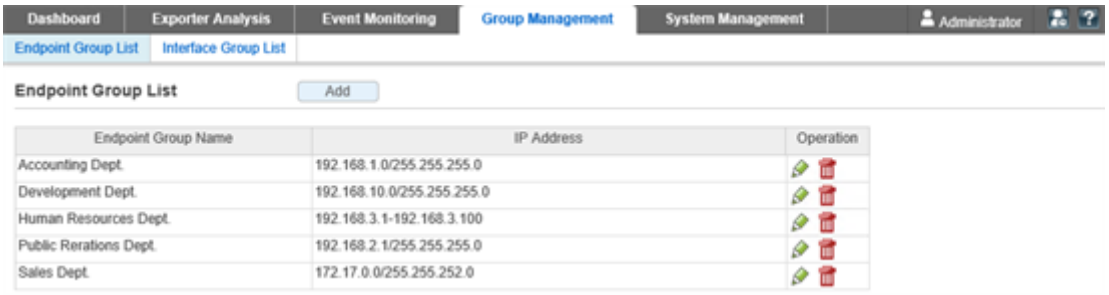

Figure 1-4 Endpoint group list

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.

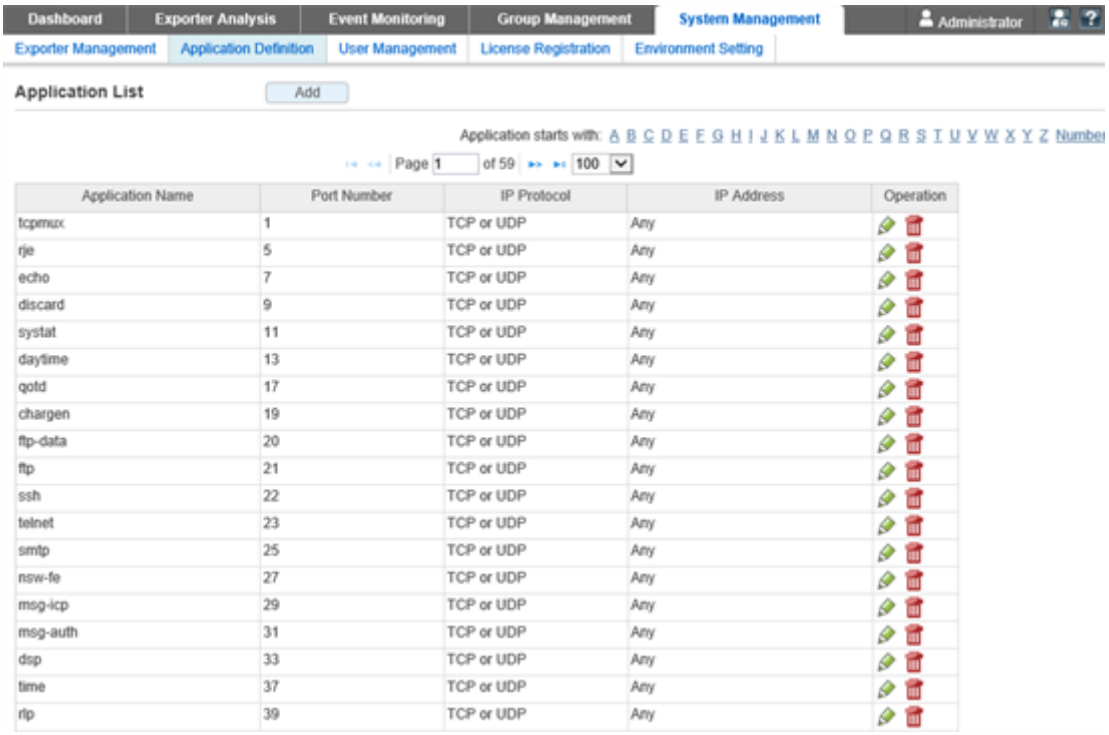

Figure 1-5 Application definitions

1.1.3 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 1-6 System configuration diagram (page 6)".

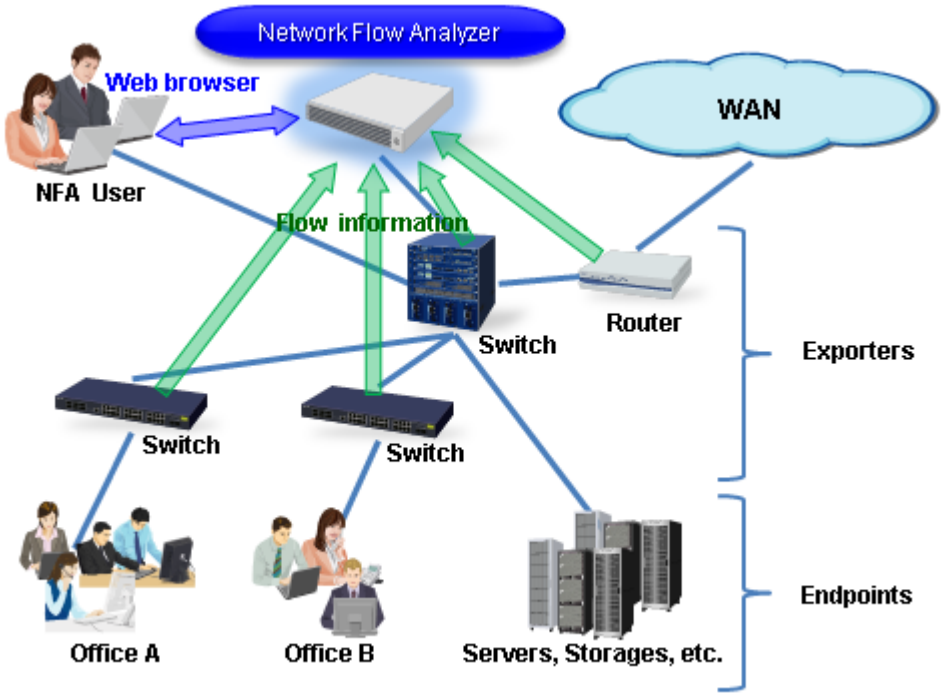

Figure 1-6 System configuration diagram

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 1-7 System configuration example at integrated operation (page 7)".

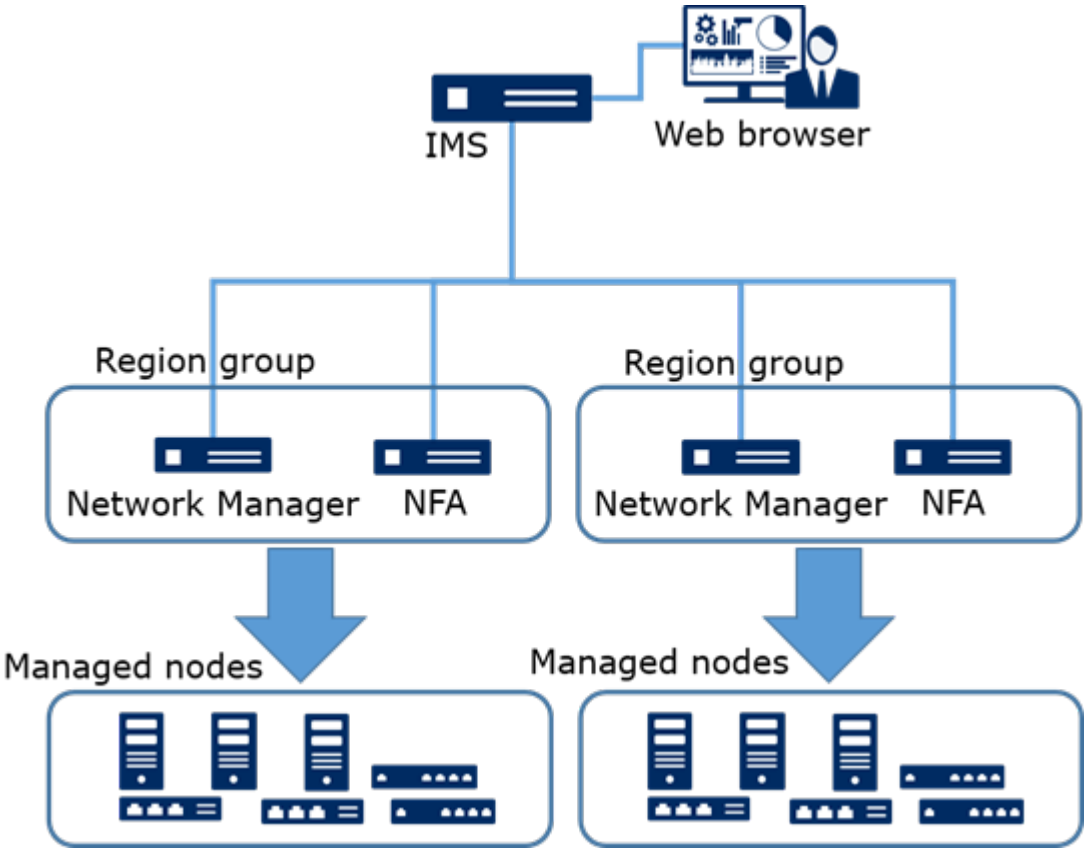

Figure 1-7 System configuration example at integrated operation

NFA and Network Manager which manage the same node (exporter) are grouped by Region group as shown in "Figure 1-7 System configuration example at integrated operation (page 7)". 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.

1.2 Basic operations of web console

To use and operate NFA, connect a terminal to the NFA web console by using a web browser. The following describes how to connect to the NFA web console and the basic operations of the web console.

1.2.1 Preparing to use web console

The following describes the preparations required to use the NFA web console from a web browser.

Configure your web browser before accessing the web console. The following web browser settings only need to be configured once.

1.2.1.1 Synchronizing the time with the NFA server

The time of the computer on which to run the web console must be synchronized with the NFA server clock.

If the time of the web console is not identical to the NFA server clock, the displayed time may appear fast or slow.

Therefore, before using and operating the web console, configure its time to be identical to that of the NFA server clock.

Tip

It is recommended to use an NTP service so that a time lag does not occur.

1.2.1.2 Checking the web browser security settings

The following describes the web browser security settings required to use the NFA web console.

JavaScript and Cookies must be enabled for the web browser to access the web console.

JavaScript and Cookies are enabled by default for supported browsers. Therefore, it is not necessary to specify a particular setting to use the web console. If you have changed the Internet Explorer settings, check whether the settings are appropriate to use NFA.

For Windows Server, if **Enhanced Security Configuration** is set to *"Enable"*, the setting described in "Configuring settings on a Windows Server OS (page 9)" is required.

Checking the Internet Explorer settings

Check the Internet Explorer settings from the Internet Options dialog box. Press ALT+T on the Internet Explorer window and select **Internet Options** from the displayed menu. For details about the settings on each tab, see the help of Internet Explorer.

- **Security** tab
  - Registration to *"Trusted sites"*

    Register the URL of the NFA server to *"Trusted sites"*.

    Tip

    If you do not want to register the NFA server to *"Trusted sites"*, configure the security settings so that the server is assumed to be other than a site on *"Restricted sites"*.

  - Enabling JavaScript

    Confirm that **Active scripting** is set to *"Enable"* on **Custom Level** of *"Trusted sites"*.
- **Privacy** tab

  If the zone to which the NFA server belongs is *"Internet"*, make sure that Cookies are allowed.

  Tip

  - If the zone to which the NFA server belongs is *"Trusted sites"* or *"Local Intranet"*, cookies are not blocked.
  - If the zone to which the NFA server belongs is *"Restricted sites"*, cookies are always blocked and the web console cannot be used.

Checking the Mozilla Firefox settings

Check the Mozilla Firefox settings from the Options page. For details about the settings, see the help of Mozilla Firefox.

- **Privacy** panel

  In the **History** setting, make sure that Cookies from sites are acceptable.

Checking the Google Chrome settings

Check the Google Chrome settings from Settings page. In this page, click **Show advanced settings** at the bottom of the page and then click **Content settings** button under the **Privacy** section. You can check the settings in the Content settings dialog box. For details about the settings, see the help of Google Chrome.

- **Cookie**

  Make sure that Cookies can be stored.

- **JavaScript**

  Make sure that JavaScript is permitted.

Configuring settings on a Windows Server OS

If **Enhanced Security Configuration** is set to *"Enable"*, add *"about:blank"* to *"Trusted sites"* in the Internet Options dialog box.

1.2.1.3 Importing an SSL server certificate to the web browser

The SSL server certificate required to access NFA must be imported to the web browser.

If you select a self-signed type SSL server certificate, you can access NFA safely by importing the certificate to the web browser.

Tip

Even for a certificate issued by a certificate authority, some certificate authorities may instruct you to import a root certificate to the web browser. In this case, follow the instructions of the certificate authority.

⚠ Caution

If you use Internet Explorer without importing the certificate and if the warning continues to be displayed, aberrant behavior might occur such as a page being unable to be displayed or operations being unable to be performed on the web browser. It is therefore strongly recommended to import a certificate when using a web browser.

- Perform the following procedure for Internet Explorer and Google Chrome.

  1. Create a certificate (.cer file) that can be imported by using `exportcert` command of "A.1 nfa_ssl_keytool (page 98)".
  2. Double-click the certificate file created by using `nfa_ssl_keytool exportcert` on the computer on which to run the web browser.
  3. On the displayed Certificate dialog box, click the **Install Certificate** button.

     Certificate Import Wizard is displayed. Click the **Next** button.
  4. Select **Place all certificates in the following store** and click the **Browse** button.
  5. On the Select Certificate Store dialog box, select *"Trusted Root Certification Authorities"* and click the **OK** button.
  6. Click the **Next** button.
  7. Click the **Finish** button.
  8. A security warning is displayed for self-signed certificates. Click the **Yes** button.

The certificate is successfully imported when a dialog message `The import was successful.` is displayed.

- Perform the following procedure for Mozilla Firefox.
  1. Access the following URL by using the web browser.

     https://<NFA server domain name (FQDN)>/nfa/

     Tip

     Name resolution needs to be available for the NFA server domain name specified in the URL.

     A security warning is displayed for self-signed certificates.
  2. Click the **Advanced** button, and then click the **Add Exception** button.
  3. In the Add Security Exception dialog box, confirm that **Permanently store this exception** is checked, and then click the **Confirm Security Exception** button.

     Caution

     Before confirming the security exception, make sure that the adding certificate is collect.

The certificate is successfully imported if the login page is displayed.

1.2.2 Accessing the web console

The following describes how to access the NFA web console from a web browser.

Execute the following to access the web console.

1. Specify the following URL on the address bar of the web browser to open the login page of the web console.

   https://<NFA server domain name (FQDN)>/nfa/

   The host name (FQDN) must be the same as the name specified when creating an SSL server certificate. Otherwise, a warning indicating an invalid certificate is displayed.

   Tip

   To access the web console, name resolution needs to be available for the NFA server domain name specified in the URL.

2. Enter a user name and password to log in to the web console.

When the login to the web console is successful, the Dashboard page set for the login user is displayed.

Caution

- The following are cautions on logging in to the web console and operation.
  - After the first login, change the password of the admin user.

    To change the password, click the **(Personal Settings)** button at the upper right of the page to display the Personal Settings page.
  - The NFA settings cannot be handled (added, changed, or deleted) on multiple web consoles at the same time.
  - If no operation is performed for 30 minutes after logging in to the web console, automatic logout is executed and the login page is displayed again when the next operation is performed.

    However, automatic logout is not executed if 1 minute, 5 minutes, or 15 minutes is set as the update interval on the Dashboard, Exporter Analysis, and Event List pages.

- The following are cautions when enabling single sign-on behavior with the Web Console of the IMS component.
  - In the IMS component, register users with the same name as the NFA. Single sign-on is valid only for users with the same name.
  - Even if you specify the URL for the web console of the NFA when logging in, login page for the web console of the IMS component is displayed. When login is successful, it will automatically transition to the web console page of the NFA.
  - If the IMS component is stopped, access to the web console of the NFA may fail. In this case, specify the following URL, display the login page for the web console of NFA and login.

    https://<NFA server domain name (FQDN)>/nfa/login

1.2.3 Structure of web console

The following describes the configuration of the web console of NFA.

The NFA web console consists of the areas as shown in "Figure 1-8 Configuration of web console (page 11)".

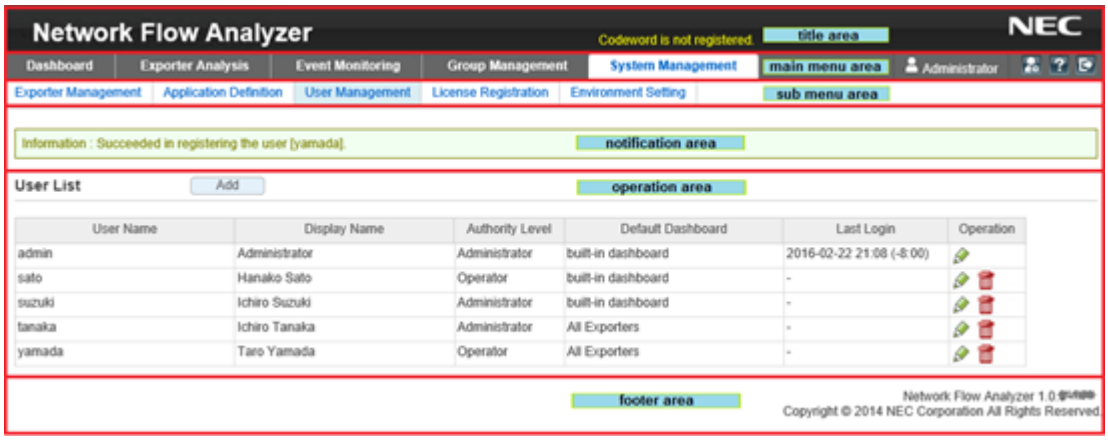

Figure 1-8 Configuration of web console

Title area

Displays the product name, and a message indicating the registration status of the product license and codeword.

Main menu area

Displays menus and operation buttons.

- Main menu (functional category of NFA)
  - **Dashboard** tab

    The operation page for displaying and setting the Dashboard page.
  - **Exporter Analysis** tab

    Displays the Exporter Analysis page where you can narrow down the exporters to be analyzed and analyze the communication traffic in detail.
  - **Event Monitoring** tab

    Displays a page to specify monitoring the communication traffic by using thresholds and to check the history of threshold violation and recovery event occurrence.

- **Group Management** tab

  Displays a setting page to group endpoints that are used in analysis or for display on the Dashboard and Exporter Analysis tab and also to group exporter interfaces. In addition, a list page is displayed to show the current group setting status.

- **System Management** tab

  Displays a page to configure and manage the settings related to the entire system, for example, to manage the exporters and their interfaces and to manage the users who can log in to NFA.

  Tip

  The **System Management** tab can be used only by a logged in user who has administrator rights.

- Display of user name
  - The logged in user name is displayed. Here, **Display Name** value of the user is displayed. If **Display Name** is not specified, the value of **User Name** is displayed.
- Buttons
  - **(Personal Settings)** button

    Clicking this button displays the page to change the personal settings of the logged in user, such as **Display Name** and **Password**.

    Tip

    We recommend changing the password after the first login.

  - **(Help)** button

    Clicking this button displays the help of NFA.

  - **(Logout)** button

    Clicking this button logs you off from the web console.

Sub menu area

If the selected main menu has sub menus, these are displayed here.

Notification area

Displays information related to the current operation or error information indicating, for example, that the input value is invalid.

Operation area

Displays the operation contents according the selected main menu or sub menu.

Footer

Displays the version and copyright of the NFA.

1.2.4 Widget types

On the Dashboard and Exporter Analysis pages, individual analysis results of the communication status are displayed as widgets. The following describes the widget types that NFA supports.

The supported widgets are roughly classified into the following three types depending on the contents to display.

Line chart widgets

These widgets display the results of analyzing transitions in the communication traffic for each item within the specified period on a line chart. The amount of communication traffic for each item within the specified period is also ranked in a list. The communication traffic unit can be selected from bps or pps.

The following widgets belong to this type.

- Communication traffic analysis widget

Table 1-1 Communication traffic analysis widget

Widget type	Description
Exporters	Displays exporters with a high volume of communication traffic. The communication traffic of an exporter is the total communication traffic passing through the interfaces of the exporter.
IN Interfaces	Displays input interfaces with a high volume of communication traffic.
OUT Interfaces	Displays output interfaces with a high volume of communication traffic.

- Communication source and destination analysis widget

Table 1-2 Communication source and destination analysis widget

Widget type	Description
Source IP addresses	Displays source IP addresses with a high volume of communication traffic. In the widget display, the source IP address can be changed to the host name.
Destination IP addresses	Displays destination IP addresses with a high volume of communication traffic. In the widget display, the destination IP address can be changed to the host name.
Conversations	Displays conversations (communication between two endpoints) with a high volume of communication traffic. In the widget display, the IP addresses of the communicating endpoints can be changed to the host names.
Source Endpoint Groups	Displays source endpoint groups with a high volume of communication traffic.
Destination Endpoint Groups	Displays destination endpoint groups with a high volume of communication traffic.
Source AS	Displays source autonomous systems (AS) with a high volume of communication traffic. The AS is displayed as a number.

Widget type	Description
Destination AS	Displays destination autonomous systems (AS) with a high volume of communication traffic. The AS is displayed as a number.

"Figure 1-9 Line chart widget (page 14)" shows a sample line chart widget.

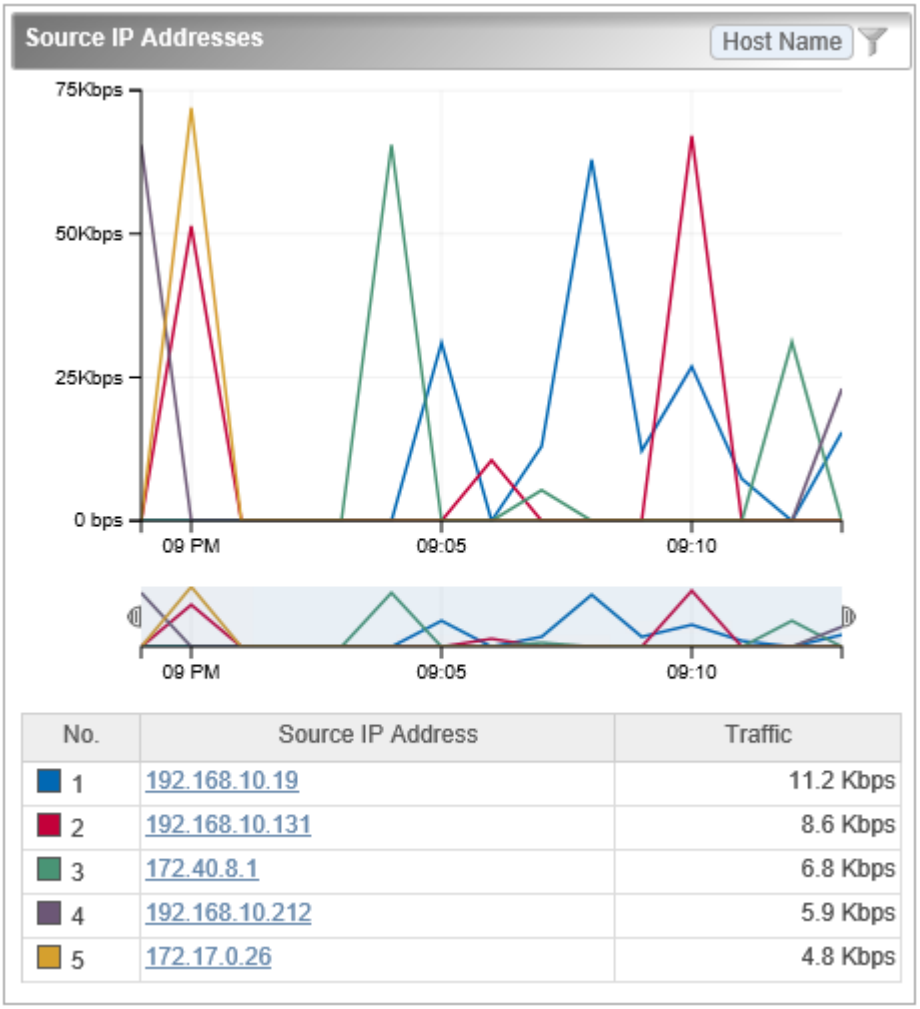

Figure 1-9 Line chart widget

Pie chart/line chart widgets

The analysis result can be displayed as a pie chart or line chart.

- Pie chart

  A pie chart displays the proportion of communication traffic for each item to the total communication traffic within the specified period. The amount of communication traffic for each item within the specified period is also ranked in a list. The communication traffic unit can be selected from bytes or packets.

- Line chart

  These widgets display the results of analyzing transitions in the communication traffic for each item within the specified period on a line chart. The amount of communication traffic for each item within the specified period is also ranked in a list. The communication traffic unit can be selected from bps or pps.

The following widgets belong to this type.

Table 1-3 Pie chart/line chart widgets

Widget type	Description
Applications	Displays applications with a high volume of communication traffic.
IP Protocols	Displays IP protocols with a high volume of communication traffic.
DSCP	Displays DSCP with a high volume of communication traffic.

"Figure 1-10 Pie chart/line chart widget (page 15)" shows a sample pie chart widget.

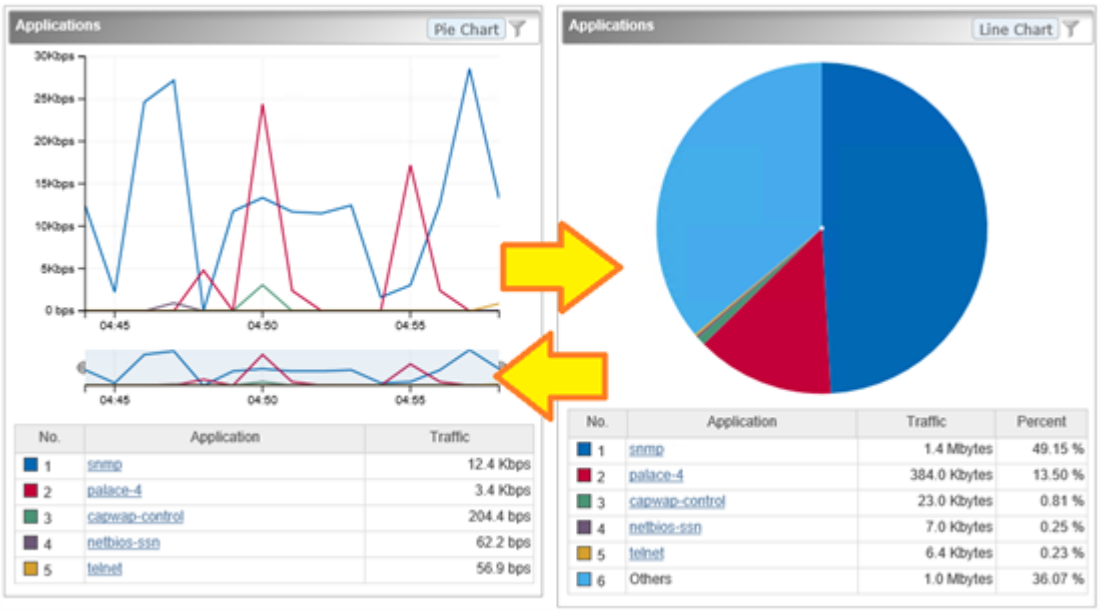

Figure 1-10 Pie chart/line chart widget

List display type

These widgets display information about the communication status in a list.

The following widgets belong to this type.

Table 1-4 List display widget

Widget type	Description
Current Alerts	Displays current alert events.

"Figure 1-11 List display widget (page 16)" shows a sample list display widget.

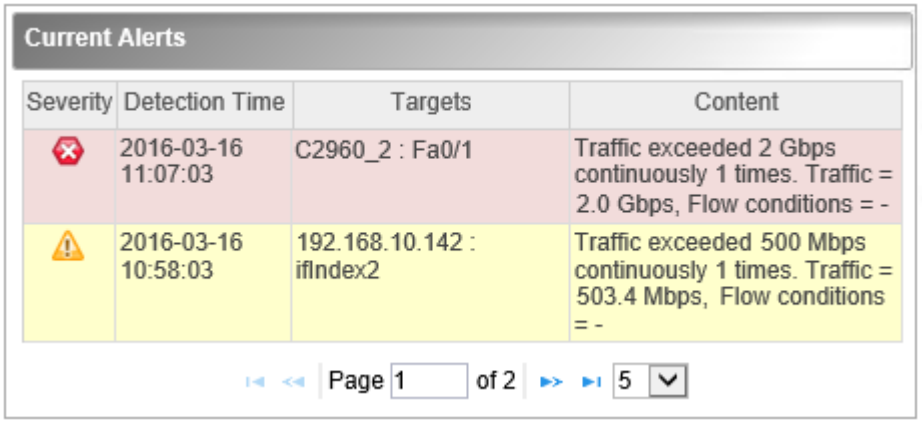

Figure 1-11 List display widget

1.2.5 Performing operations on widgets

For line chart and pie chart widgets, drill-down analysis can be performed and the items displayed by the widget can be filtered. Furthermore, for line chart widgets, the user can zoom in on the chart and the displayed IP address can be changed to the corresponding host name.

For a line chart widget and a pie chart/line chart widget on which a line chart is displayed, the user can zoom in on the chart.

Furthermore, for a widget that displays endpoint information by using an IP address, the displayed IP address can be changed to the corresponding host name.

For a pie chart/line chart widget, a pie chart or line chart can be displayed.

Tip

Click the **Line Chart** button to display a line chart. Click the **Pie Chart** button to change the displayed line chart to a pie chart.

1.2.5.1 Performing drill-down analysis

For line chart and pie chart widgets, the analysis conditions can be narrowed down by clicking the link of the item you want to analyze on the list. The procedure is shown below.

Drill-down analysis is useful if you want to perform detailed analysis from a widget displayed on the Dashboard page or intuitively add a filtering condition to the analysis results on the Exporter Analysis page.

1. Click the link of the item you want to analyze on the list of the target widget.

   #### Tip

   If this is performed for a widget related to multiple exporters on the Dashboard page, a page to select an exporter and the interfaces to be analyzed is displayed. In this case, select the exporter or interface you want to analyze.

2. The selected item is added to **Filter Conditions** on the Exporter Analysis page.

Confirm that the analysis results have been updated.

Operation example:

The following operation example shows how to perform drill-down analysis on the Dashboard page of the communication of the source IP address *"192.168.1.100"* that passes through interface *"0/1"* of the *"base connection router"*.

1. Click the link of the source IP address *"192.168.1.100"* of the *"Source IP Address"* widget on the Dashboard page.
2. The page transitions to the Exporter Analysis page, and **List of Analysis Candidates** is displayed.

   At this time, the source IP address *"192.168.1.100"* is set to **Filter Conditions**. In **List of Analysis Candidates**, the names and communication traffic of the exporter and interfaces that are monitoring the flow corresponding to this condition are displayed.
3. In **List of Analysis Candidates**, click interface *"0/1"* that is the *"base connection router"*.
4. Widgets that analyze the flow corresponding to the following conditions are displayed in the Exporter Analysis page.

   Target Exporter

   Base connection router

   Target Interfaces

   0/1

   Filter Conditions

   Source IP Address ="192.168.1.100"

1.2.5.2 Filtering the items displayed on a chart

For line chart and pie chart widgets, the filtering function allows you to exclude some of the items currently being displayed from the display targets. The procedure is shown below.

Filtering is useful if you want to make a chart more visible by temporarily hiding some of the Top N display items so that you can focus on the desired items.

For example, if you want to compare the 10th to 20th items of the Top 20, you can make a chart more visible by excluding the 1st to 9th items.

1. Click the **(Filter Settings)** button of the target widget.
2. On the Filter Analysis Targets dialog box, clear the check box of an analysis target item to exclude it from the targets.
3. Click the **OK** button to apply the filter settings.

The contents displayed in the widget will change.

- For line chart widgets

  Only the items specified for analysis will be displayed.
- For pie chart widgets

  The proportion of the items specified for analysis to the total communication traffic will be displayed.

1.2.5.3 Zooming in on a line chart

For line chart widgets, a chart can be zoomed in on by reducing the the time scale of the line chart that shows the entire specified period. The procedure is shown below.

You can zoom in on a line chart by specifying the time scale, within the chart display period that is specified in the display settings. This is useful if you want to check the communication status in detail by zooming in on the chart.

1. Select the lower line chart that shows the overall period. This line chart is called the range selector.
2. Adjust the time scale by dragging and dropping the right and left cursors of the range selector.

   If you want to adjust the display position, execute the following:

   - Adjust the the time scale by dragging and dropping the right and left cursors of the range selector.
   - Move the time scale by dragging and dropping the specification area of the range selector.
   - Click outside the specification area of the range selector to release the time specification and specify a new time scale by dragging and dropping.

     Tip

     - The right and left cursors of the range selector are hidden by releasing the time specification. The cursors can be displayed again by specifying the time scale in the range selector.
     - The time scale can also be specified by dragging the area outside the time axis without releasing the time specification.

The upper line chart is zoomed in on within the specified range. The amount and rank of communication traffic for each item within the specified period are also displayed in a list.

1.2.5.4 Changing the IP address display to the host name

For widgets that display endpoint information by using IP addresses, the displayed IP addresses can be changed to the corresponding host names. The procedure is shown below.

To change the IP address that indicates an endpoint to the corresponding host name, NFA must be able to inquire about the host name to the Domain Name System (DNS) that manages host names and IP addresses of endpoints via the network.

Tip

- For an endpoint that is not registered to the DNS, the IP address will be displayed as is because inquiries about host names will fail.
- The host name to be displayed instead of an P address by executing the following procedure is the host name that is obtained from the DNS when the analysis target flow information is received, not the host name obtained by executing this procedure. Therefore, when analyzing the past communication status, if the previous host name at reception of the analysis target flow information differs from the current host name, the previous host name is displayed.

By seeing the displayed the host name, you can easily understand the status of communication endpoints.

1. Click the **Host Name** button of the target widget.
2. The IP addresses indicating the endpoints are changed to the corresponding host names.

   Check the list display of the target widget.

Caution

When the display is changed from an IP address to a host name, the link to the Exporter Analysis page will be disabled.

To return to the original IP address display, click the **IP Address** button.

1.2.5.5 Changing the chart type

For a pie chart/line chart widget, it is possible to change the display from a pie chart to a line chart and vice versa. The procedure is shown below.

This procedure makes it possible to analyze a flow in chronological order in terms of a specific protocol or to analyze the flow percentage for the specified period.

Tip

The chart type can be changed on the following three widgets.

- **Applications** widget
- **IP Protocols** widget
- **DSCP** widget

1. Click the **Line Chart** or **Pie Chart** button of the target widget.
2. The chart on the target widget changes to **Pie Chart** or **Line Chart**.

Caution

To reset the changed chart display to the default chart, move to another page or press the F5 key to refresh the page.

For the procedure to change the default chart type, see "4.1.3.2 Updating a dashboard definition (page 67)".

1.2.6 Updating the personal settings

The following describes the procedure for the user who logged in to the NFA web console to change the own user information including the login password.

Tip

The **User Name** and **Authority Level** settings cannot be changed.

1. Open the Personal Settings page.

   Click the **(Personal Settings)** button of the main menu area.
2. Change the settings on the displayed Personal Settings page.
   - **Display Name**

     Specify a user name to be displayed on the web console. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

     If this is omitted, the name specified for **User Name** is used as a display name.
   - **Default Dashboard**

     Select the name of the dashboard definition that is initially displayed after the login.
   - **Change Password**

Select the check box and enter the current password in the **Old Password** text box.

Enter a new password in the **New Password** text box, and then in the **Confirmation** text box.

Specify the password consisting of 8 to 32 single-byte alphanumeric characters.

3. Check the changes and click the **Save** button.

Chapter 2. Environment Settings Before Operations

This chapter describes how to configure the environment before using and operating NFA.

Contents

2.1 Managing the license

The following describes the licenses of NFA.

2.1.1 Product license and interface license

The following describes the concept of the product license and interface license of NFA.

Product license

A product license is a license that is necessary to validate the NFA product.

After installation, NFA initially behaves as a trial version with limited available functions. For the trial version, only two interfaces for an exporter can be registered as a managed object. The function restrictions can be canceled by registering the product license, allowing the user to use the product functions according to the registered product license.

Interface license

An interface license is a license that is assigned to the interfaces of the managed exporter in order to judge whether to receive flow information. The maximum number of interfaces to which a license can be assigned depends on the registered product license.

2.1.2 Managing the product licenses

The following describes the License Registration page that is used to manage the product licenses.

License Registration page

On this page, you can check the registered license keys and also register a license.

To display the License Registration page, click **System Management**>**License Registration**.

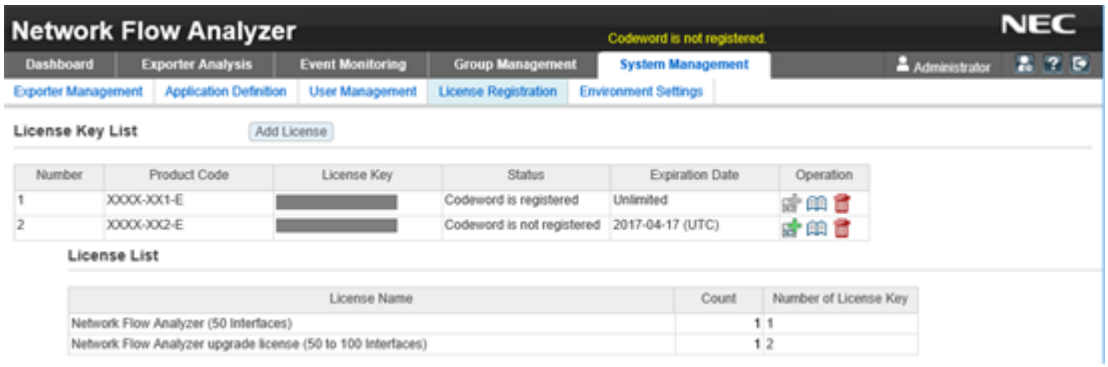

Figure 2-1 License Registration page

Operation area

- **Add License** button

  Use this button to register a license key. The Add License page is displayed by clicking this button.

License Key List

- **Number**

Indicates the number to be used to manage the registered license key.

- **Product Code**

  Displays the product code of the license key that was entered when registering a license key.

- **License Key**

  Displays the value of the registered license key.

- **Status**

  Displays the license registration status.

  If **Codeword is not registered** is displayed, register the codeword before the date specified for **Expiration Date**. If the specified expiration date has passed, the license key becomes invalid and the product cannot be used.

- **Expiration Date**

  Displays the expiration date of the registered license key.

- **Operation**

  Displays the operation buttons that are available for the registered license key.

  - **(Register Codeword)** button

    Click this button to display the Register Codeword page. The codeword of the license key can be registered on the displayed page.

    Caution

    When **Codeword is registered** is displayed in the **Status** column, this button is disabled.

  - **(Show Details)** button

    Click this button to display the Details of License Key page. Detailed information about the license key can be checked on the displayed page.

  - **(Delete)** button

    Use this button to delete the registered license information.

License List

This list displays the following information for the registered license keys in License Key List.

- **License Name**

  Displays the name of the valid product license.

- **Count**

  Displays the number of valid product licenses.

- **Number of License Key**

  Displays the license key number corresponding to **Number** of License Key List.

2.1.2.1 Registering a product license

The following describes the procedure to validate a product license.

Prepare the Codeword Request Form on which the license key to register is described.

Execute the following three steps to register the product license.

1. Register the license key.
2. Request the codeword issuing center to issue the codeword.
3. Register the issued codeword.

These steps are described in detail below.

1. Register the license key.
   a. Open the License Registration page.

      Click **System Management**>**License Registration**.

   b. Click the **Add License** button.

      The Add License page is displayed.

   c. Enter the product code and license key described in the Codeword Request Form.

   d. Click the **Register** button.

      If registration is successful, the codeword request code is displayed in the **Request Code** text box of the Add License page.

2. Request the codeword.

   To get the codeword, send the codeword request code that was displayed. For how to send the codeword request code, see the Codeword Request Form.

   Tip

   To display the codeword request code, click the **(Show Details)** button of the target license key in the License Registration page.

   The codeword will be sent in a few days.

3. Register the codeword.
   a. In the License Registration page, click the **(Register Codeword)** button of the target license key.

      The Register Codeword page is displayed.

   b. Enter the obtained codeword in the **Codeword** text box.

   c. Check the settings and click the **Register** button.

      If registration is successful, the License Registration page is displayed again. Confirm that **Codeword is registered** is displayed in **Status** of the relevant license key in License Key List.

2.1.2.2 Deleting a product license

The following describes the procedure to delete a registered product license.

If you have mistakenly registered a license key, or you want to transfer a registered license key to another system, delete the relevant product license.

1. Open the License Registration page.

   Click **System Management**>**License Registration**.

2. In License Key List, click the **(Delete)** button of the target license key.
3. Check the contents displayed in the Delete Confirmation dialog box.

4. Click the **OK** button to delete the license key.

2.2 Configuring the system environment

The following describes the system environment settings that must be configured before registering the information of the managed exporter (information of the exporter and its interfaces) to NFA.

Before using and operating NFA, configure the following environment settings required to register the managed exporter information.

- Setting the registration policy of the exporter information

  There are the following two policies for registering the information of the exporter to be managed to NFA:

  - Automatic registration at reception of the flow information

    Information of the exporter and interfaces is obtained from the received flow information and automatically registered to NFA as a managed object. At this time, the interface license is also assigned automatically.

  - Manual registration

    The user should manually register the information of the exporter to be managed and its interfaces and also assign an interface license.

  You can register any exporter anytime even if the auto registration policy is selected.

  Tip

  By default, automatic registration at reception of the flow information is enabled.

- Setting the default values of the SNMP information acquisition parameters

  NFA uses SNMP to obtain the host name and interface information of the managed exporter from the exporter's MIB.

  By setting the default values of the SNMP information acquisition parameters, you no longer need to set the parameters for each exporter. Furthermore, SNMP information can be obtained automatically during automatic registration at reception of the flow information.

2.2.1 Setting the registration policy of the exporter information

The following describes the procedure to set the registration policy of the information the managed exporter (information of the exporter and its interfaces).

This procedure is used to specify the registration policy of whether to automatically register the exporter information when receiving the flow information.

Tip

- By default, the exporter information is automatically registered.
- If automatic registration of exporter information has been set up, an interface license is also assigned automatically in that processing.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Select either of the following:

- **Register exporters, interfaces and licenses automatically when receiving flow information.**
- **Do not register exporters, interfaces and licenses automatically.**

3. Check the settings and click the **Save** button.

2.2.2 Setting the default values of the SNMP information acquisition parameters

The following describes the procedure to set the default values of the SNMP parameters that are necessary to obtain the SNMP information of the exporter and its interfaces.

When registering the exporter information, NFA obtains exporter information such as the host name (sysName) and interface name (ifName) from the exporter's MIB by using SNMP.

By setting the default values in advance, you no longer need to set the SNMP parameters for each exporter. Furthermore, SNMP information can be obtained automatically during automatic registration of exporter information at reception of the flow information.

Before executing the following procedure, check the values of the SNMP parameters that have been set to the exporters in your operating environment.

Tip

We recommend setting the same SNMP parameter values (SNMP version, port number, and SNMP community name) for all exporters to be deployed in your operating environment.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Enter the same values as the values of the exporter settings in the following fields of **Parameters for Getting Exporter Information (SNMP)**.

   - **SNMP Version**

     Select the version from the pull-down menu (**1** or **2c**). The default is **2c**.

   - **Port Number**

     Specify a value from 0 to 65535 in single-byte numbers. The default is *"161"*. Generally, *"161"* is used for the SNMP port number.

   - **SNMP Community Name**

     Specify a character string consisting of up to 255 single-byte alphanumeric characters. The default is *"public"*.

3. Check the settings and click the **Save** button.

2.3 Managing the exporter

The following describes the procedure to manage the information of the exporter to be managed (information of the exporter and its interfaces).

Exporter Management page

There are the following two methods to register the exporter to be managed to NFA.

- "2.3.1 Registering exporter information automatically (page 28)"

- "2.3.2 Registering exporter information manually (page 30)"

The following describes the Exporter Management page that is used to manage the exporter information registered by using either of the above methods.

To display the Exporter Management page, click **System Management**>**Exporter Management**.

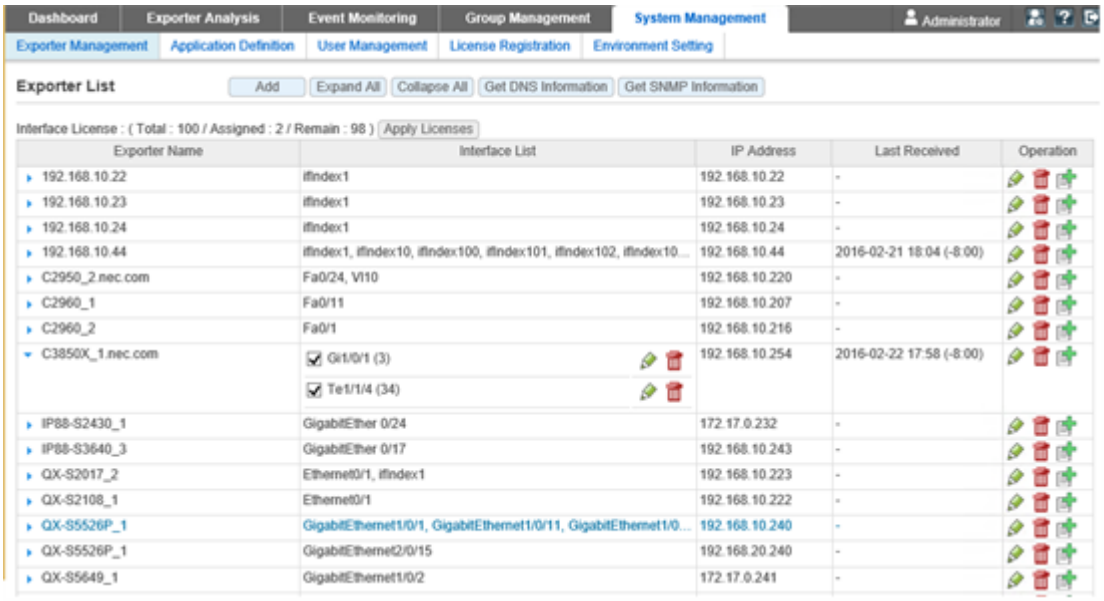

Figure 2-2 Exporter Management page

Operation area

- **Add** button

  Use this button to register a new exporter. The Add Exporter page is displayed by clicking this button.

- **Expand All** button

  Use this button to expand the **Interface List** of all exporters.

- **Collapse All** button

  Use this button to collapse the **Interface List** of all exporters.

- **Get DNS Information** button

  Use this button to obtain the host names (domain names) of all exporters by making an inquiry to the DNS.

- **Get SNMP Information** button

  Use this button to obtain the host name (sysName) and managed interface name (ifName) of all exporters by using SNMP.

- **Apply Licenses** button

  Use this button to apply the changed interface license assignment.

Exporter List

- **Exporter Name**

  Displays the name of the managed exporter.

Click the ▸ or ▾ button to expand or collapse the **Interface List** of the relevant exporter.

- **Interface List**

  Displays the managed interfaces.

  - **Interface name** check box

    Displays the interface license assignment status.

    * Check box: Selected

      The license is assigned.

    * Check box: Not selected

      The license is not assigned.

  - **(Edit)** button

    Use this button to change the registered contents of the interface. The Edit Interface page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete the interface information.

- **IP Address**

  Displays the IP address of the managed exporter.

- **Last Received**

  Displays the last time the flow data was received from the exporter.

- **Operation**

  Displays the operation buttons that are available for the registered exporter.

  - **(Edit)** button

    Use this button to change the registered contents of the exporter. The Edit Exporter page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete the exporter information.

  - **(Add Interface)** button

    Use this button to register a new interface. The Add Interface page is displayed by clicking this button.

2.3.1 Registering exporter information automatically

NFA provides a function to automatically register the managed exporter information when flow information is received.

To enable automatic registration of the exporter information, it is necessary that the automatic registration policy is selected in the **Automatic Registration Policy of Exporter** setting. For details, see "2.2.1 Setting the registration policy of the exporter information (page 25)".

The automatic registration processing registers the following information automatically according to the received flow information.

- Identification information of the exporter
- Information of the interface to be analyzed

- Assigning the interface license

Registering the identification information of the exporter

- The destination IP address of the flow information is registered as the IP address of the exporter.

  If another exporter that uses the same IP address is already registered to NFA, the exporter is not be registered, assuming that it has already been registered.

- For registration of a new exporter, an inquiry will be made to the DNS and the found host name is registered as a fully-qualified domain name (FQDN).
- If SNMP is enabled for the exporter, the host name (sysName) is obtained from the exporter's MIB by using SNMP, and the obtained host name is registered. When performing this SNMP information acquisition, the SNMP parameters that are specified in "2.2.2 Setting the default values of the SNMP information acquisition parameters (page 26)" are used.

Tip

Names of exporters that are automatically registered are displayed in the following order.

1. Host name (DNS)
2. Host name (SNMP sysName)
3. IP address

Registering the information of the interface to be analyzed

- Among the flow information, NFA assumes that communication on the input side (IN) of the interface is set as the analysis target in the flow information output setting of the exporter. Therefore, NFA registers the identifier (ifIndex) of the interface indicating the input side (IN) of the received flow information as the interface to be analyzed to NFA.

  If another exporter that has the same ifIndex value is already registered to NFA, the interface is not registered, assuming that it has already been registered.

- If SNMP is enabled for the exporter, the interface name (ifName) is obtained from the exporter's MIB by using SNMP, and the obtained host name is registered. When performing this SNMP information acquisition, the SNMP parameters that are specified in "2.2.2 Setting the default values of the SNMP information acquisition parameters (page 26)" are used.

  If the ifName value could be obtained, the obtained name is displayed as the interface name of each page. If the ifName value could not be obtained, the interface name is displayed in the ifIndex<ifIndex-value> format.

Caution

Among the flow information, if communication on the output side (OUT) of the interface is set as an analysis target in the flow information output setting of the exporter, automatic registration of the exporter information does not work properly. In this case, update the registration information manually.

Assigning the interface license

- The interface license is assigned to the input side (IN) interface that NFA assumes as the analysis target at the same time as the interface information is registered.
- If there is no assignable interface license, assignment processing is not performed.

Tip

Once the registration processing up to interface license assignment is completed successfully, the relevant flow information is accumulated and managed in NFA. If interface license assignment fails due to an excess number of licenses, the received flow information is discarded.

2.3.2 Registering exporter information manually

You can register exporter information to NFA anytime manually.

In the case of manual registration, register the following information on the Exporter Management page.

- Identification information of the exporter

  Click the **Add** button of Exporter List to register the identification information. For details, see "2.3.2.1 Adding an exporter (page 30)".

- Information of the exporter to be analyzed

  Click the **(Add Interface)** button of Exporter List to register the identification information. For details, see "2.3.2.2 Adding a managed interface (page 31)".

  Tip

  For manually registered interfaces, an interface license must be assigned so that the flow information can be received and analyzed.

2.3.2.1 Adding an exporter

The following describes the procedure to add identification information of an exporter to NFA.

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. Click the **Add** button.

3. Specify an appropriate value for each item on the displayed Exporter Settings page.

   - **Display Name**

     Specify the display name of the exporter by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

     The display name specified here is displayed for the exporter on the pages of NFA. If this item is omitted, the following are displayed in this order as the exporter name.

     a. Host name (DNS)

     b. Host name (SNMP sysName)

     c. IP address

   - **IP Address**

     Specify the IPv4 address that is the source of the flow information. An IP address that is already being used by another exporter cannot be specified.

   - **SNMP Settings**

     Specify the following three parameters according the SNMP settings of the exporter.

     - **SNMP Version**

Select the version from the pull-down menu (**blank (omitted)**, **1**, or **2c**).

- **Port Number**

  Specify a value from 0 to 65535 in single-byte numbers. Generally, 161 is used for the SNMP port number.

- **SNMP Community Name**

  Specify a character string consisting of up to 255 single-byte alphanumeric characters.

These three parameters can be omitted. The default values for these parameters are those specified on the Environment Settings page. For details, see "2.2.2 Setting the default values of the SNMP information acquisition parameters (page 26)".

4. Specify the sampling rate, if necessary.

   - **Sampling Rate Manual Settings**

     This option is available only for an exporter that sends NetFlow or IPFIX packets. Use this option for an exporter that cannot report a sampling rate even if sampling is being performed or to manually specify a sampling rate.

     When **Sampling Rate** is specified, the result of multiplying the flow information received from the exporter by the specified sampling rate is regarded as the actual communication traffic.

     - **Sampling Rate**

       * Blank (No sampling rate is specified.)

         This is the default value.

         The sampling rate notified by the exporter is used.

       * Integer of 1 or more

         The specified sampling rate is used.

     - **Use Notice of Exporter**

       * Check box: Selected

         The sampling rate notified from the exporter is used.

         This check box is selected by default.

       * Check box: Cleared

         By clearing this check box, the **Sampling Rate** box is enabled.

         Clear this check box to manually specify the sampling rate.

   Tip

   - An sFlow packet always includes a sampling rate. Therefore, if the exporter sending sFlow packets is automatically registered, **Sampling Rate** cannot be specified manually.
   - When NFA is upgraded from version 1.0, **Use Notice of Exporter** is selected for all exporters that were registered before upgrading.

5. Check the settings and click the **OK** button.

2.3.2.2 Adding a managed interface

The following describes the procedure to register interface information to be analyzed to NFA.

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. In Exporter List, click the **(Add Interface)** button of the target exporter.
3. Specify an appropriate value for each item on the displayed Interface Settings page.
   - **Index (SNMP ifIndex)**

     Specify the ifIndex value indicating the interface to be analyzed. Specify a value from 1 to 2147483647 in single-byte numbers.

   - **Display Name**

     Specify the display name of the interface by using any characters. The available number of characters is 32. The display name specified here is displayed for the interface on the pages of NFA.

     If this item is omitted, the following are displayed as the interface name. "ifName" takes precedence over "ifIndex<ifIndex-value>".

     a. ifName

     b. ifIndex<ifIndex-value>

4. Check the settings and click the **OK** button.

2.3.3 Updating or deleting exporter information

Exporter information registered to NFA can be updated or deleted on the Exporter Management page.

2.3.3.1 Updating exporter information

The following describes the procedure to update the exporter information registered to NFA.

Tip

IP Address cannot be changed.

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. In Exporter List, click the **(Edit)** button of the target exporter.

   The Edit Exporter page is displayed.

3. Change the value of the item to be updated on the Edit Exporter page.
   - **Display Name**

     Specify the display name of the exporter by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

     The display name specified here is displayed for the exporter on the pages of NFA. If this item is omitted, the following are displayed in this order as the exporter name.

     a. Host name (DNS)

     b. Host name (SNMP sysName)

     c. IP address

   - **Host name (DNS)**

Click the **Get DNS Information** button to update the information. If information could not be obtained, nothing is displayed.

- **Host name (SNMP sysName)**

  Click the **Get SNMP Information** button to update the information. If information could not be obtained, nothing is displayed.

- **SNMP Settings**

  Specify the following three parameters according the SNMP settings of the exporter.

  - **SNMP Version**

    Select the version from the pull-down menu (**blank (omitted)**, **1**, or **2c**).

  - **Port Number**

    Specify a value from 0 to 65535 in single-byte numbers. Generally, 161 is used for the SNMP port number.

  - **SNMP Community Name**

    Specify a character string consisting of up to 255 single-byte alphanumeric characters.

  These three parameters can be omitted. The default values for these parameters are those specified on the Environment Settings page. For details, see "2.2.2 Setting the default values of the SNMP information acquisition parameters (page 26)".

4. Specify the sampling rate, if necessary.

   - **Sampling Rate Manual Settings**

     This option is available only for an exporter that sends NetFlow or IPFIX packets. Use this option for an exporter that cannot report a sampling rate even if sampling is being performed or to manually specify a sampling rate.

     When **Sampling Rate** is specified, the result of multiplying the flow information received from the exporter by the specified sampling rate is regarded as the actual communication traffic.

     - **Sampling Rate**

       * Blank (No sampling rate is specified.)

         This is the default value.

         The sampling rate notified by the exporter is used.

       * Integer of 1 or more

         The specified sampling rate is used.

     - **Use Notice of Exporter**

       * Check box: Selected

         The sampling rate notified from the exporter is used.

         This check box is selected by default.

       * Check box: Cleared

         By clearing this check box, the **Sampling Rate** box is enabled.

         Clear this check box to manually specify the sampling rate.

Tip

- An sFlow packet always includes a sampling rate. Therefore, if the exporter sending sFlow packets is automatically registered, **Sampling Rate** cannot be specified manually.
- When NFA is upgraded from version 1.0, **Use Notice of Exporter** is selected for all exporters that were registered before upgrading.

5. Check the settings and click the **OK** button.

2.3.3.2 Updating managed interface information

The following describes the procedure to update the interface information registered to NFA.

The following items can be updated.

- **Display Name**

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. In Exporter List, click the **(Edit)** button of the target interface.

   The Edit Interface page is displayed.

3. Change the value in the **Display Name** text box on the Edit Interface page.

   - **Display Name**

     Specify the display name of the interface by using any characters. The available number of characters is 32. The display name specified here is displayed for the interface on the pages of NFA.

     If this item is omitted, the following are displayed as the interface name. "ifName" takes precedence over "ifIndex<ifIndex-value>".

     a. ifName

     b. ifIndex:<ifIndex-value>

   Click the **Get SNMP Information** button to update the interface name (SNMP ifName).

4. Check the changes and click the **OK** button.

2.3.3.3 Deleting exporter information

The following describes the procedure to delete the exporter information registered to NFA.

Caution

The following information is also deleted by deleting the exporter information.

- All interface information
- Accumulated flow information of all interfaces

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. In Exporter List, click the **(Delete)** button of the target exporter.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the information.

2.3.3.4 Deleting managed interface information

The following describes the procedure to delete the interface information registered to NFA.

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. In Exporter List, click the **(Delete)** button of the target interface.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the information.

2.3.4 Updating license assignment status of all interfaces at once

The license assignment status of all the interfaces registered to NFA can be updated at once.

Before updating the license assignment status, make sure that the number of assigned licenses after updating will not exceed the number of assignable licenses.

- NFA receives and accumulates the flow information of only the interfaces for which an interface license has been assigned.
- If updating the status causes all interface licenses to become unassigned, licenses will no longer be assigned to interfaces automatically even if automatic registration of exporter information is enabled.

1. Open the Exporter Management page.

   Click **System Management**>**Exporter Management**.

2. In Exporter List, click the **Expand All** button.

   All the interface information is displayed.

3. Change the interface license assignment status.

   Select or clear the check boxes in **Interface List**.

   - Check box: Selected

     Interface licenses will be assigned.

   - Check box: Cleared

     Interface licenses will not be assigned.

   If the interface license assignment status is changed, the cell color of the relevant interface will be changed.

4. Check the changes and click the **Apply Licenses** button.

2.4 Managing users

The following describes how to manage the login users of the NFA web console.

2.4.1 User types

The operations available for NFA users can be controlled by setting authority levels

There are two user authority levels: Administrator and Operator.

Administrator

An Administrator user can use and operate all pages and functions of NFA.

Operator

An Operator user can only execute reference operations. In terms of NFA settings, Operator users can only perform some flow analysis operations.

The specific restrictions are as follows:

Table 2-1 Operations that can be performed by Operator users

Main menu	Operation	Remarks
Dashboard tab	○	All operations are available. However, for dashboard definitions, Operator users can edit and delete the definitions that they have created.
Exporter Analysis tab	○	-
Event Monitoring tab	△	The operation to set monitoring by using a threshold is not available.
Group Management tab	△	The operations to set an endpoint group and interface group are not available.
System Management tab	×	This tab is not displayed for Operator users.
(Personal Settings) button	○	-
(Help) button	○	-
(Logout) button	○	-

2.4.2 Performing operations on user information

The following describes the User Management page on which to manage NFA user information.

User Management page

You can check the information of registered users and also register a new user in User List.

To display the User Management page, click **System Management**>**User Management**.

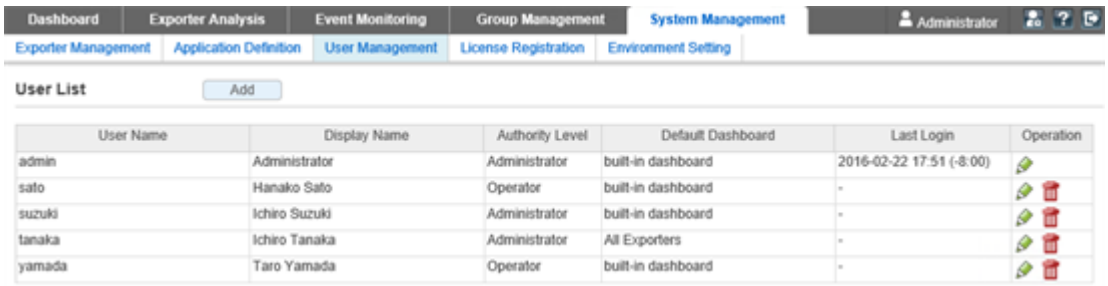

Figure 2-3 User Management page

Operation area

- **Add** button

Use this button to register a new user. The Add User page is displayed by clicking this button.

User List

- **User Name**

  Displays the name of the registered user.

- **Display Name**

  Displays the user display name that is displayed at login.

- **Authority Level**

  Displays the authority level of the user (Administrator or Operator).

- **Default Dashboard**

  Displays the name of the default dashboard definition that is initially displayed after login.

- **Last Login**

  Displays the date and time when the user last logged in.

- **Operation**

  Displays the operation buttons that are available for the registered user.

  - **(Edit)** button

    Use this button to change the user's registered contents. The Edit User page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete a registered user.

    Caution

    * The initial user *"admin"* cannot be deleted. This button is not displayed for the "admin" user.
    * This button is disabled for the currently logged-in user.

2.4.2.1 Adding an user

The following describes the procedure to add a new user.

1. Open the User Management page.

   Click **System Management**>**User Management**.

2. Click the **Add** button in the User List.

3. Specify an appropriate value for each item on the displayed Add User page.

   - **User Name**

     Specify a user name that is unique in NFA. The available number of characters is 32. The available characters are single-byte alphanumeric characters, hyphens(-), underscores (_), dots (.), and apostrophes (').

   - **Display Name**

     Specify the user name to be displayed on the console page. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

If this is omitted, the name specified for **User Name** is used as the display name.

- **Initial Password**

  Specify the initial password of the user to be registered. Specify a character string consisting of 8 to 32 single-byte alphanumeric characters.

- **Confirmation**

  Enter the password specified in **Initial Password**.

- **Authority Level**

  Select **Administrator** or **Operator**.

- **Default Dashboard**

  Select the name of the dashboard definition that is initially displayed after the user logs in.

4. Check the settings and click the **OK** button.

2.4.2.2 Updating user information

The following describes the procedure to update user information.

Tip

User Name cannot be changed.

1. Open the User Management page.

   Click **System Management**>**User Management**.

2. In User List, click the **(Edit)** button of the target user.
3. Change the settings on the displayed Edit User page.

   - **Display Name**

     Specify the user name to be displayed on the console page. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

     If this is omitted, the name specified for **User Name** is used as the display name.

   - **Authority Level**

     Select **Administrator** or **Operator**.

   - **Default Dashboard**

     Select the name of the dashboard definition that is initially displayed after the user logs in.

   - **Change Password**

     Select the check box of the target user, enter a new password in the **New Password** text box, and then enter the same password again in the **Confirmation** text box. Specify a character string consisting of eight to 32 single-byte alphanumeric characters.

4. Check the changes and click the **OK** button.

2.4.2.3 Deleting user information

The following describes the procedure to delete a registered user.

1. Open the User Management page.
   Click **System Management**>**User Management**.
2. In User List, click the **(Delete)** button of the target user.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the information.

Chapter 3. Environment Settings During Operations

This chapter describes how to configure the environment as needed while using and operating NFA.

Contents

3.1 Aggregating and analyzing the flow information of multiple interfaces

NFA provides an interface group function to group multiple physical interfaces to be analyzed into a single logical interface according to the exporter settings.

3.1.1 interface groups

The following describes how to use an interface group.

Purpose of an interface group

Some exporter specifications allow multiple physical interfaces to be grouped into a single logical interface by using link aggregation (LAG). However, because an exporter cannot send flow information to a logical interface, the flow information usually needs to be analyzed for each physical interface.

An interface group enables NFA to analyze the flow information of a logical interface consisting of physical interfaces, in accordance with the interface settings of the exporter.

Operations that can be performed on interfaces grouped into an interface group

NFA handles interfaces grouped into an interface group in the same way as a general interface. Therefore, the following operations can be performed on interfaces grouped into an interface group.

- You can check the amount of communication traffic by referring to the **IN interfaces** widget and **OUT Interfaces** widget on the Dashboard page and Exporter Analysis page.
- By specifying the interfaces in the interface groups for **Target Interfaces** on the Dashboard page and Exporter Analysis page, you can check the results of analyzing the communication traffic of the specified interfaces by referring to the widgets.
- The communication traffic of the interfaces in the interface group can be monitored by using a threshold.

Tip

- Interfaces in the same exporter can be grouped into an interface group. However, interfaces in different exporters cannot be grouped.
- An interface cannot belong to multiple interface groups.
- If an interface in an interface group is deleted, it is also deleted from the interface group.

3.1.2 Performing operations on interface groups

The following describes the Interface Group List page.

Interface Group List page

On this page, you can check the registered interface groups and also register an interface group.

To display the Interface Group List page, click **Group Management**>**Interface Group List**.

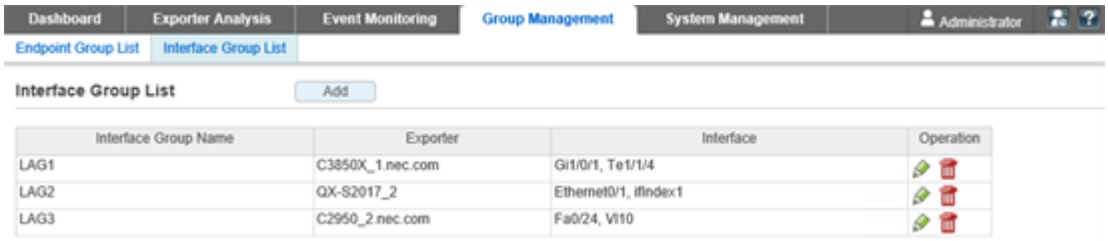

Figure 3-1 Interface Group List page

Operation area

- **Add** button

  Use this button to register a new interface group. The Add Interface Group page is displayed by clicking this button.

Caution

If the authority level of the user is Operator, this button is not displayed.

Interface Group List

- **Interface Group Name**

  Displays the interface group name.

- **Exporter**

  Displays the name of the exporter that has the interfaces grouped into the interface group.

- **Interface**

  Displays the name of the interfaces belonging to the interface group.

- **Operation**

  Displays the operation buttons that are available for the registered interface group.

  - **(Edit)** button

    Use this button to change the registered contents of the interface group. The Edit Interface Group page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete a registered interface group.

Caution

If the authority level of the user is Operator, the **Operation** column is not displayed.

3.1.2.1 Adding an interface group

The following describes the procedure to add a new interface group.

1. Open the Interface Group List page.

   Click **Group Management**>**Interface Group List**.

2. Click the **Add** button.

3. Specify an appropriate value for each item on the displayed Add Interface Group page.

- **Interface Group Name**

  Specify an interface group name by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

- **Target Exporter**

  Select the exporter registered to NFA from the pull-down menu.

- **Target Interfaces**

  This is displayed by specifying **Target Exporter**. Select the check boxes of the interfaces to be added to the group.

  Check box: Selected

  Adds the interface to the group.

  Check box: Not selected

  Removes the interface from the group.

Tip

Interfaces that already belong to other interface groups are not displayed in **Target Interfaces**.

4. Check the settings and click the **OK** button.

3.1.2.2 Updating an interface group

The following describes the procedure to update the registered information of an interface group.

Tip

Target Exporter cannot be changed.

1. Open the Interface Group List page.

   Click **Group Management**>**Interface Group List**.

2. In Interface Group List, click the **(Edit)** button of the target interface group.
3. Change the settings on the displayed Edit Interface Group page.

   - **Interface Group Name**

     Specify an interface group name by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

   - **Target Interfaces**

     Select the check boxes of the interfaces to be added to the group.

     Check box: Selected

     Adds to the interface to the group.

     Check box: Not selected

     Removes the interface from the group.

4. Check the changes and click the **OK** button.

3.1.2.3 Deleting an interface group

The following describes the procedure to delete a registered interface group.

1. Open the Interface Group List page.

   Click **Group Management**>**Interface Group List**.

2. In Interface Group List, click the **(Delete)** button of the target interface group.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the interface group.

3.2 Aggregating and analyzing the flow information of multiple destination and source IP addresses

NFA provides an endpoint grouping function to analyze the communication traffic on a group basis by grouping multiple source and destination IP addresses that are the endpoint of a communication.

3.2.1 Endpoint groups

The following describes how to use an endpoint group.

Purpose of an endpoint group

When investigating the communication load on the network between departments or sites, it is time-consuming to investigate the communication traffic of individual endpoints, making it difficult to examine the overall situation of the communication contents.

To avoid this, NFA provides an endpoint grouping function to group multiple endpoints and aggregate the communication traffic of each endpoint group, and analyze a breakdown of the aggregated communication traffic in detail.

This endpoint grouping function makes it possible to grasp the communication situation in units of organization such as a department or site that uses the network. The grasped contents are useful for managing the capacity of the network between departments or sites.

Operations that can be performed on an endpoint group

The NFA endpoint grouping function enables the following operations:

- You can check the amount of communication traffic of individual endpoint groups by referring to the **Source Endpoint Group** widget and **Destination Endpoint Group** widget on the Dashboard page and Exporter page.
- By specifying **Source Endpoint Group** or **Destination Endpoint Group** in **Filter Conditions** on the Exporter Analysis page, you can check the results of analyzing the communication traffic of the specified endpoint group by referring to the widgets.
- The communication traffic of an endpoint group can be monitored by using a threshold.

3.2.2 Performing operations on endpoint groups

The following describes the Endpoint Group List page.

Endpoint Group List page

On this page, you can check the registered endpoint groups and also register an endpoint group.

To display the Endpoint Group List page, click **Group Management**>**Endpoint Group List**.

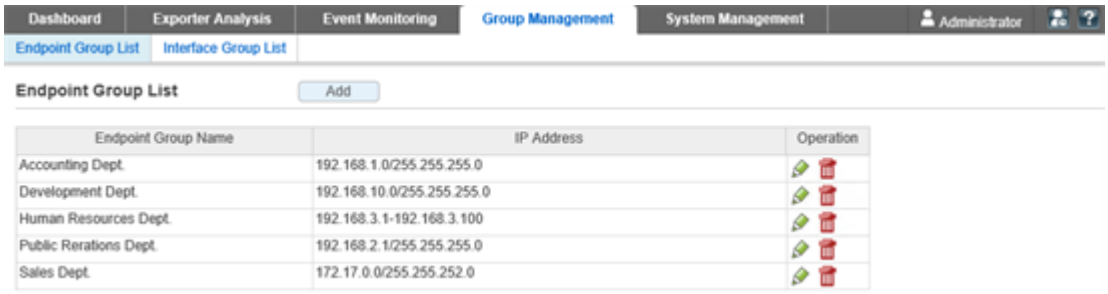

Figure 3-2 Endpoint Group List page

Operation area

- **Add** button

  Use this button to add a new endpoint group. The Add Endpoint Group page is displayed by clicking this button.

Caution

If the authority level of the user is Operator, this button is not displayed.

Endpoint Group List

- **Endpoint Group Name**

  Displays the endpoint group name.

- **IP Address**

  Displays the information of the IP addresses, IP address range, and network addresses that belong to the endpoint group.

- **Operation**

  Displays the operation buttons that are available for the registered endpoint group.

  - **(Edit)** button

    Use this button to change the registered contents of the endpoint group. The Edit Endpoint Group page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete a registered endpoint group.

Caution

If the authority level of the user is Operator, the Operations column is not displayed.

3.2.2.1 Adding an endpoint group

The following describes the procedure to add a new endpoint group.

1. Open the Endpoint Group List page.

Click **Group Management**>**Endpoint Group List**.

2. Click the **Add** button.
3. Specify an appropriate value for each item on the displayed Add Endpoint page.
   - **Endpoint Group Name**

     Specify an endpoint group name. The available number of characters is 32. A comma (,) cannot be used. In addition, a single-byte space cannot be used at the beginning and end of the name.
   - **Target IP Addresses**

     Specify the IP address conditions of the endpoints to be grouped. Specify at least one of the following conditions:
     - Buttons
       * **(Add)** button

         Use this button to add an input text box for specifying the target IP addresses.
       * **(Delete)**

         Use this button to delete an input text box for specifying the target IP addresses.
     - **IP Address**

       Specify one IPv4 address for the target endpoint.
     - **IP Address Range**

       Specify a range of IPv4 addresses for the target endpoint.
     - **Network Address**

       Specify the network address and netmask to which the target endpoint belongs.
4. Check the changes and click the **OK** button.

3.2.2.2 Updating an endpoint group

The following describes the procedure to update the registered information of an endpoint group.

1. Open the Endpoint Group List page.

   Click **Group Management**>**Endpoint Group List**.
2. In Endpoint Group List, click the **(Edit)** button of the target endpoint group name.
3. Change the settings on the displayed Edit Endpoint page.
   - **Endpoint Group Name**

     Specify an endpoint group name. The available number of characters is 32. A comma (,) cannot be used. In addition, a single-byte space cannot be used at the beginning and end of the name.
   - **Target IP Addresses**

     Specify the IP address conditions of the endpoints to be grouped. Specify at least one of the following conditions:
     - Buttons
       * **(Add)** button

Use this button to add an input text box for specifying the target IP addresses.

* **(Delete)**

  Use this button to delete an input text box for specifying the target IP addresses.

- **IP Address**

  Specify one IPv4 address for the target endpoint.

- **IP Address Range**

  Specify a range of IPv4 addresses for the target endpoint.

- **Network Address**

  Specify the network address and netmask to which the target endpoint belongs.

4. Check the changes and click the **OK** button.

3.2.2.3 Deleting an endpoint group

The following describes the procedure to delete an endpoint group.

1. Open the Endpoint Group List page.

   Click **Group Management**>**Endpoint Group List**.

2. In Endpoint Group List, click the **(Delete)** button of the target endpoint group name.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the endpoint group.

3.3 Identifying system-specific application communications

NFA provides an application definition function to identify individual application communications.

This function makes it possible to set the source and destination IP addresses as identification conditions for identifying a system-specific application communication in addition to the port number and IP protocol of the communication, which are generally used as identification conditions.

3.3.1 Application definitions

The following describes the usage of application definitions.

Purpose of application definitions

To analyze the communication traffic of an application, the conditions for identifying the communication of the application must be specified. A general method used to identify an application communication is to check the port number and IP protocol used by the communication. For example, an htttp communication is identified by confirming that the communication is a TCP or UDP communication using port number 80. However, depending on the specifications, an application may use the same port number or IP protocol as that of an http communication, or may provide services through http communications. Because it is difficult to accurately identify a communication of such an application, it is not possible to analyze the communication traffic with a high degree of precision.

To avoid this, NFA provides a function to set the source and destination IP addresses as identification conditions to identify a system-specific application communication in addition to the port number and IP protocol of the communication, which are generally used as identification conditions.

For example, if an application server provides a business service using an http communication, the communication with this business service is treated as an application communication that is different from a general http communication, making it possible to individually analyze the communication traffic.

Operations that can be performed on application definitions

NFA can perform the following analysis operations by adding an application definition.

- You can check the amount of communication traffic of individual applications, including defined applications, by referring to the **Application** widget on the Dashboard page and Exporter Analysis page.
- By specifying the application name that is specified for **Application** in **Filter Conditions** on the Exporter Analysis page, you can check the results of analyzing the communication traffic of the specified application by referring to the widgets.
- The communication traffic of the defined application can be monitored by using a threshold.

3.3.2 Performing operations on application definitions

The following describes the usage of the Application Definitions page.

Application Definitions page

On this page, you can check the registered application definitions and also register an application definition.

To display the Application Definitions page, click **System Management**>**Application Definition**.

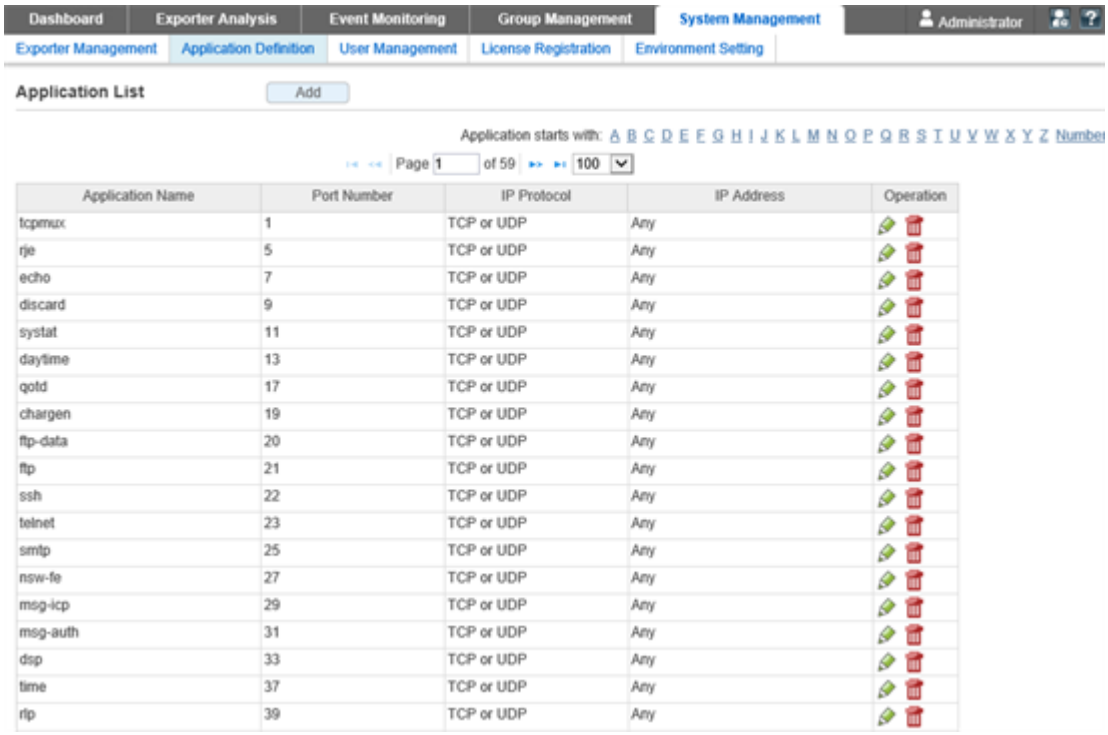

Figure 3-3 Application Definitions page.

Tip

As an application definition, the NFA incorporates definitions that can uniquely identify applications using a combination of port numbers and IP protocols, among applications managed by IANA as of October 2014.

Operation area

- **Add** button

  Use this button to add a new application definition. The Add Application page is displayed by clicking this button.

- **Application start with:**

  Use these links to display application names that start with a certain letter. If you select *"All"*, all application names are displayed.

Application Definition List

- **Application Name**

  Displays the application name.

- **Port Number**

  Displays the port number that is used in the communication of the relevant application.

- **IP Protocol**

  Displays the IP protocol that is used in the communication of the relevant application.

- **IP Address**

  Displays the IP address condition (specific IP address, IP address range, or network address) used to identify the communication of the relevant application.

- **Operation**

Displays the operation buttons that are available for the registered application.

- **(Edit)** button

  Use this button to change the registered contents of the application definition. The Edit Application page is displayed by clicking this button.

- **(Delete)** button

  Use this button to delete a registered application definition.

3.3.2.1 Adding an application definition

The following describes the procedure to add a new application definition.

1. Open the Application Definition page.

   Click **System Management**>**Application Definition**.

2. Click the **Add** button.

3. Specify an appropriate value for each item on the displayed Add Application page.

   - **Application Name**

     Specify the name of the application. The available number of characters is 32. A comma (,) cannot be used. In addition, a single-byte space cannot be used at the beginning and end of the name.

   - **Port Number**

     Specify the source or destination port number that the application uses. Specify a value from 0 to 65535 in single-byte numbers.

     When specifying multiple port numbers, separate them by commas (,).

     When specifying the range of port numbers, use the following format:

     <starting port number>-<ending port number>

     This item can be omitted when a value other than **TCP**, **UDP**, and **TCP or UDP** is specified for **IP Protocol**.

   - **IP Protocol**

     Select the IP protocol that the relevant application uses from the pull-down menu.

     Tip

     If **TCP or UDP** is selected for an application that uses both TCP and UDP, the result of analysis that is performed by aggregating the communication traffic of TCP and UDP can be obtained.

   - **IP Address**

     Specify the condition of the source or destination IP address used to identify the application.

     Select either of the following:

     - **Any IP Address**

       Select this option when no IP condition is set to identify the application.

     - **Specific IP Addresses**

       Specify one or more conditions to identify the application.

* Buttons
  + **(Add)** button

    Use this button to add an input text box for specifying the condition.
  + **(Delete)**

    Use this button to delete an input text box for specifying the condition.
* **IP Address**

  Specify one IPv4 address.
* **IP Address Range**

  Specify a range of IPv4 addresses.

4. Check the settings and click the **OK** button.

3.3.2.2 Updating an application definition

The following describes the procedure to update an application definition.

1. Open the Application Definition page.

   Click **System Management**>**Application Definition**.
2. In Application List, click the **(Edit)** button of the target application name.
3. Change the settings on the displayed Edit Application page.
   - **Application Name**

     Specify the name of the application. The available number of characters is 32. A comma (,) cannot be used. In addition, a single-byte space cannot be used at the beginning and end of the name.
   - **Port Number**

     Specify the source or destination port number that the application uses. Specify a value from 0 to 65535 in single-byte numbers.

     When specifying multiple port numbers, separate them by commas (,).

     When specifying the range of port numbers, use the following format:

     <starting port number>-<ending port number>

     This item can be omitted when a value other than **TCP**, **UDP**, and **TCP or UDP** is specified for **IP Protocol**.
   - **IP Protocol**

     Select the IP protocol that the relevant application uses from the pull-down menu.

     Tip

     If **TCP or UDP** is selected for an application that uses both TCP and UDP, the result of analysis that is performed by aggregating the communication traffic of TCP and UDP can be obtained.
   - **IP Address**

     Specify the condition of the source or destination IP address used to identify the application.

     Select either of the following:

- **Any IP Address**

  Select this option when no IP condition is set to identify the application.

- **Specific IP Addresses**

  Specify one or more conditions to identify the application.

  * Buttons

    + **(Add)** button

      Use this button to add an input text box for specifying the condition.

    + **(Delete)**

      Use this button to delete an input text box for specifying the condition.

  * **IP Address**

    Specify one IPv4 address.

  * **IP Address Range**

    Specify a range of IPv4 addresses.

4. Check the changes and click the **OK** button.

3.3.2.3 Deleting an application definition

The following describes the procedure to delete an application definition.

1. Open the Application Definition page.

   Click **System Management**>**Application Definition**.

2. In Application List, click the **(Delete)** button of the target application name.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the application definition.

3.4 Monitoring a flow by using a threshold

NFA can monitor the flow of communication between endpoints by using a threshold.

3.4.1 Threshold monitoring

The following describes how to perform threshold monitoring.

Purpose of threshold monitoring

It is difficult to visually detect an unexpected increase in communication traffic for communication between endpoints. Visually monitoring the communication situation at all times is unrealistic if there are a lot of flows to be analyzed.

To avoid this, NFA provides a function to monitor communication between endpoints by setting thresholds from various perspectives. For example, it is possible to monitor the communication of a specific application or destination IP address.

Functional overview of threshold monitoring

The NFA threshold monitoring function enables the following operations:

- Threshold monitoring of the communication traffic of a flow by specifying the following flow conditions:
  - Source or destination IP address
  - Source or destination endpoint group
  - Source or destination AS number
  - Application
  - IP protocol
  - DSCP
- The interval to judge the occurrence of a threshold violation is one minute. The average communication traffic per minute of a flow that has met the specified conditions is monitored.
- The occurrence of a threshold violation can be checked by referring to the Event List page on the **Event Monitoring** tab. The current occurrence status of threshold violations can be checked on the **Current Alerts** widget of the Dashboard page.
- Threshold violation and recovery events can be sent to another management system (SNMP manager) by using the SNMP trap.

3.4.2 Performing operations on threshold monitoring entries

The following describes the Threshold Monitoring Entry List page.

Threshold Monitoring Entry List page

On this page, you can check the registered threshold monitoring entries and also register a threshold monitoring entry.

To display the Threshold Monitoring Entry List page, click **Event Monitoring**>**Threshold Monitoring Entry List**.

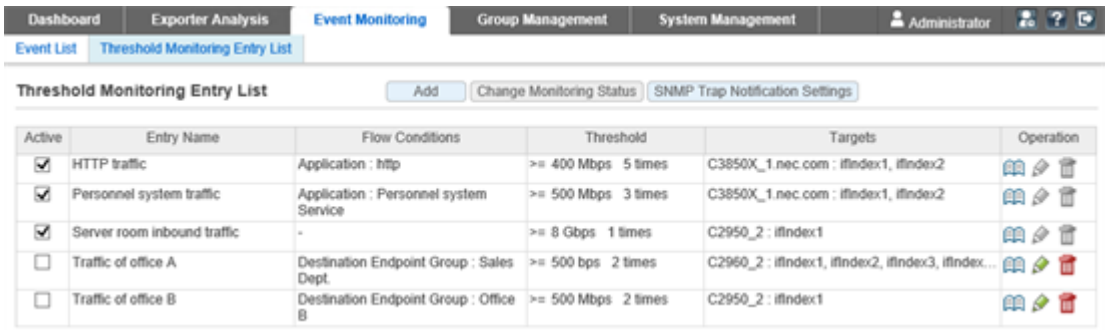

Figure 3-4 Threshold Monitoring Entry List page

Operation area

- **Add** button

  Use this button to add a new threshold monitoring entry. The Add Threshold Monitoring Entry page is displayed by clicking this button.
- **Change Monitoring Status** button

  Use this button to apply changes made to the execution status of the threshold monitoring entry.
- **SNMP Trap Notification Settings** button

Use this button to specify the contents of the threshold violation and recovery event to be sent by using the SNMP trap. The SNMP Trap Notification Settings page is displayed by clicking this button.

Caution

If the authority level of the user is Operator, the buttons of the operation area are not displayed.

Threshold Monitoring Entry List

- **Active**

  Displays the monitoring status of the threshold monitoring entry.

  Check box: Selected

  The threshold monitoring entry is active (running).

  Check box: Not selected

  The threshold monitoring entry is not active (not running).

- **Entry Name**

  Displays the threshold monitoring entry name.

- **Flow Conditions**

  Displays the flow conditions to be monitored.

- **Threshold**

  Displays the conditions to judge whether a threshold violation has occurred (threshold, number of consecutive occurrences).

- **Targets**

  Displays the names of the monitored exporters and its interfaces.

- **Operation**

  Displays the operation buttons that are available for the registered threshold entry.

  - **(Show Details)** button

    Use this button to display detailed information of the threshold monitoring entry. The Details of Threshold Monitoring Entry page is displayed by clicking this button.

  - **(Edit)** button

    Use this button to change the registered contents of the threshold monitoring entry. The Edit Threshold Monitoring Entry page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete a registered threshold monitoring entry.

  Caution

  The displayed operation buttons differ depending on the user authority level.

  - Administrator

    For the threshold monitoring entry that is active (the **Active** check box is selected), only the **(Show Details)** button is available. Other buttons are displayed in a disabled state.

  - Operator

Only the **(Show Details)** button is available. Other buttons are not displayed.

3.4.2.1 Adding a threshold monitoring entry

The following describes the procedure to add a new threshold monitoring entry.

1. Open the Threshold Monitoring Entry List page.

   Click **Event Monitoring**>**Threshold Monitoring Entry List**.

2. Click the **Add** button.

3. Specify an appropriate value for each item on the displayed Add Threshold Monitoring Entry page.

   - **Entry Name**

     Specify a threshold monitoring entry name by using any characters. The available number of characters is 64. A single-byte space cannot be used at the beginning and end of the name.

   - **Specify Flow Conditions**

     Select this check box to specify the conditions.

     Select the condition for identifying the flow to be monitored from the pull-down menu (**Application** / **Source IP Address** / **Destination IP Address** / **Source Endpoint Group** / **Destination Endpoint Group** / **Source AS Number** / **Destination AS Number** / **IP Protocol** / **DSCP**) and specify a value.

   - **Target Interfaces**

     Specify the exporter and interfaces to be monitored.

     - **Expand All** button

       Use this button to expand and display all tree items of the **Selected** or **Not Selected** column.

     - **Collapse All** button

       Use this button to collapse all tree items of the **Selected** or **Not Selected** box.

     - **<<Add** button

       Add the interfaces selected in the **Not Selected** box to the **Selected** box as a monitoring target.

     - **Delete>>** button

       Delete the interfaces selected in the **Selected** box from the monitoring targets.

   - **Threshold Settings**

     Specify the conditions for judging whether a threshold violation has occurred.

     - **Measured Value**

       * **Inequality Sign**

         >: Judges that a threshold violation has occurred when the measured value exceeds the threshold.

         >=: Judges that a threshold violation has occurred when the measured value is equal to or exceeds the threshold.

       * **Threshold**

Specify the threshold. Specify a value from 1 to 99999 in single-byte numbers.

* **Unit**

  Select the unit for the value specified as the threshold from the pull-down menu (**bps** / **Kbps** / **Mbps** / **Gbps** / **Tbps**).

- **Consecutive Occurrences *N* times**

  Specify the number of consecutive occurrences of threshold violations at which an event will be sent. Specify a value from 1 to 1000 in single-byte numbers.

• **Notification Settings**

  Specify the contents of the event to be reported when the system judges that a threshold violation has occurred.

  - **Event Severity**

    Select the event severity of the threshold violation from the pull-down menu (**Warning** / **Error**).

  - **Notify events via SNMP traps**

    Select this check box to send the event issued by the relevant threshold monitoring entry by using the SNMP trap.

    Tip

    To send the SNMP trap, the settings of the destination must have been specified on the SNMP Trap Notification Settings page. For details, see "3.4.2.4 Reporting event occurrence by using the SNMP trap (page 58)".

4. Check the settings and click the **OK** button.

⚠ Caution

NFA performs the threshold violation judgment processing for the average communication traffic per minute of a flow that has met the specified conditions at one-minute intervals.

If a lot of monitoring items are specified, there is a risk that the judgment processing of all thresholds cannot be performed within one minute, resulting in the inability to perform proper threshold monitoring.

The appropriate number of monitoring items varies depending on the number of managed exporters, number of received flows, and machine specifications. The number of monitoring items here is the total number of interfaces specified in each threshold monitoring entry. For example, when the following monitoring entry is specified, the number of monitoring items is *"7"*.

• Entry Name: Entry 01

  Target Interfaces:

  - Interfaces 0/1 and 0/2 of Router A
  - Interfaces 0/1 and 0/2 of Router B

  Number of monitoring items of Entry 01 = *"4"*

• Entry Name: Entry 02

  Target Interfaces:

  - Interface 0/2 of Router A
  - Interfaces 0/1 and 0/2 of Router C

  Number of monitoring items of Entry 02 = *"3"*

A log dedicated to threshold monitoring is output to the following file. Confirm that the following log has not been output to this file. A *"skipped"* log indicates that the processing has not finished in one minute and monitoring items may be too much.

File:

```
<%installation directory%>/controller/log/com.nec.nfa.threshold.information.log
```

Log:

```
2016-12-13 14:51:32.755 INFO   15974 15  threshold monitoring time:
1481608292, 120 entries will be skipped.
```

3.4.2.2 Updating a threshold monitoring entry

The following describes the procedure to update a threshold monitoring entry.

Tip

Entry Name cannot be changed.

1. Open the Threshold Monitoring Entry List page.

   Click **Event Monitoring**>**Threshold Monitoring Entry List**.

2. Click the **(Edit)** button of the threshold monitoring entry whose registered information is to be updated on Threshold Monitoring Entry List.

3. Change the settings on the displayed Edit Threshold Monitoring Entry page.

   - **Specify Flow Conditions**

     Select this check box to specify the conditions.

     Select the condition for identifying the flow to be monitored from the pull-down menu (**Application** / **Source IP Address** / **Destination IP Address** / **Source Endpoint Group** / **Destination Endpoint Group** / **Source AS Number** / **Destination AS Number** / **IP Protocol** / **DSCP**) and specify a value.

   - **Target Interfaces**

     Specify the exporter and interfaces to be monitored.

     - **Expand All** button

       Use this button to expand and display all tree items of the **Selected** or **Not Selected** column.

     - **Collapse All** button

       Use this button to collapse all tree items of the **Selected** or **Not Selected** box.

     - **<<Add** button

       Add the interfaces selected in the **Not Selected** box to the **Selected** box as a monitoring target.

     - **Delete>>** button

       Delete the interfaces selected in the **Selected** box from the monitoring targets.

   - **Threshold Settings**

     Specify the conditions for judging whether a threshold violation has occurred.

     - **Measured Value**

       * **Inequality Sign**

>: Judges that a threshold violation has occurred when the measured value exceeds the threshold.

>=: Judges that a threshold violation has occurred when the measured value is equal to or exceeds the threshold.

* **Threshold**

  Specify the threshold. Specify a value from 1 to 99999 in single-byte numbers.

* **Unit**

  Select the unit for the value specified as the threshold from the pull-down menu (**bps** / **Kbps** / **Mbps** / **Gbps** / **Tbps**).

- **Consecutive Occurrences *N* times**

  Specify the number of consecutive occurrences of threshold violations at which an event will be sent. Specify a value from 1 to 1000 in single-byte numbers.

• **Notification Settings**

Specify the contents of the event to be reported when the system judges that a threshold violation has occurred.

- **Event Severity**

  Select the event severity of the threshold violation from the pull-down menu (**Warning** / **Error**).

- **Notify events via SNMP traps**

  Select this check box to send the event issued by the relevant threshold monitoring entry by using the SNMP trap.

Tip

To send the SNMP trap, the settings of the destination must have been specified on the SNMP Trap Notification Settings page. For details, see "3.4.2.4 Reporting event occurrence by using the SNMP trap (page 58)".

4. Check the changes and click the **OK** button.

3.4.2.3 Deleting a threshold monitoring entry

The following describes the procedure to delete a threshold monitoring entry.

1. Open the Threshold Monitoring Entry List page.

   Click **Event Monitoring**>**Threshold Monitoring Entry List**.

2. Click the **(Delete)** button of the threshold monitoring entry to be deleted on Threshold Monitoring Entry List.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the monitoring entry.

3.4.2.4 Reporting event occurrence by using the SNMP trap

An event that has occurred can be sent to another management system (SNMP manager) by using the SNMP trap. The following describes the procedure to set the destination information of the SNMP trap transmission on the SNMP Trap Notification Settings page.

Event information will be sent to the specified destination by using the SNMP trap. This function is enabled by selecting the **Notify events via SNMP traps** check box of **Notification Settings** when adding or editing a threshold monitoring entry.

For details about the operations that can be performed on threshold monitoring entries, see "3.4.2.1 Adding a threshold monitoring entry (page 55)" and "3.4.2.2 Updating a threshold monitoring entry (page 57)".

1. Open the Threshold Monitoring Entry List page.

   Click **Event Monitoring**>**Threshold Monitoring Entry List**.

2. Click the **SNMP Trap Notification Settings** button.

3. Specify an appropriate value for each item on the displayed SNMP Trap Notification Settings page.

   A trap will be sent to the destination specified here.

   - **SNMP Version**

     Select the SNMP version of the SNMP trap to be sent from the pull-down menu (**1** / **2c**). The default is **2c**.

   - **SNMP Community Name**

     Specify an SNMP trap community name consisting of up to 255 single-byte alphanumeric characters. The default is *"public"*.

   - **Destination Port Number**

     Specify the destination port number. Specify a value from 0 to 65535 in single-byte numbers. The default is *"162"*.

   - **Destination IP Address**

     Specify the IPv4 address of the destination to which to send the SNMP trap.

4. Check the settings and click the **OK** button.

The contents of the SNMP trap that NFA sends are as follows. Specify the reception settings of the SNMP manager according to the specifications of the SNMP manager that receives the SNMP trap sent by NFA.

- nfaTrafficThreshExceeded

  Indicates that a communication traffic threshold violation has occurred.

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	1	
Variable Bindings :	nfaEventOccurTime :	Event occurrence date
	nfaEventOccurExpAddr :	IP address of the exporter
	nfaEventOccurExpIfIndex :	ifIndex of the exporter
	nfaEventOccurExpName :	Name of the exporter
	nfaEventOccurExpIfName :	Name of the interface of the exporter
	nfaEventOccurEntryName :	Name of the monitoring entry
	nfaEventLevel :	Severity
	nfaThreshFlowConditions :	Flow conditions to be monitored
	nfaThreshConfData :	Threshold

	nfaThreshConfTimes :	Specified number of consecutive occurrences
	nfaThreshConfUnit :	Unit of the threshold and measured value
	nfaThreshMeasuredData :	Measured value

- nfaTrafficThreshCleared

  Indicates that the communication traffic threshold violation has been resolved.

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	2	
Variable Bindings :	nfaEventOccurTime :	Event occurrence date
	nfaEventOccurExpAddr :	IP address of the exporter
	nfaEventOccurExpIfIndex :	ifIndex of the exporter
	nfaEventOccurExpName :	Name of the exporter
	nfaEventOccurExpIfName :	Name of the interface of the exporter
	nfaEventOccurEntryName :	Name of the monitoring entry
	nfaEventLevel :	Severity (Reports information(1).)
	nfaThreshFlowConditions :	Flow conditions to be monitored
	nfaThreshConfData :	Threshold
	nfaThreshConfUnit :	Unit of the threshold and measured value
	nfaThreshMeasuredData :	Measured value

- nfaThreshStopped

  Indicates that the threshold violation has been resolved by stopping monitoring of the threshold monitoring entry.

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	5	
Variable Bindings :	nfaEventOccurTime :	Event occurrence date
	nfaEventOccurExpAddr :	IP address of the exporter
	nfaEventOccurExpIfIndex :	ifIndex of the exporter
	nfaEventOccurExpName :	Name of the exporter
	nfaEventOccurExpIfName :	Name of the interface of the exporter
	nfaEventOccurEntryName :	Name of the monitoring entry
	nfaEventLevel :	Severity (Reports information(1).)
	nfaThreshFlowConditions :	Flow conditions to be monitored
	nfaThreshConfData :	Threshold
	nfaThreshConfUnit :	Unit of the threshold and measured value

Chapter 4. Operations

This chapter describes how to use NFA during operation.

Contents

4.1 Checking the current network status

NFA provides a dashboard function for the login user to immediately grasp the current status of the network range that is managed by the login user.

4.1.1 Dashboard

The following describes how to use the dashboard.

Purpose of the dashboard

The dashboard is provided as a home page on which the user can immediately grasp the current communication status of the network range that they manage.

The dashboard is designed to enable an overview of the entire status of the managed network range. Therefore, it is possible to compare and analyze the communication status of each interface of multiple exporters and to check for threshold violation occurrences in the managed network range. Furthermore, the dashboard page can be used as an initial page on which to narrow down flow conditions according to overall communication trends and drill down a status for detailed analysis.

Operations that can be performed on the dashboard

The following analysis operations can be performed on the NFA dashboard.

- Compare and analyze the communication traffic of each interface of multiple exporters on the widget.
- Freely define the contents of the initial dashboard for each NFA login user.
- Switch to another registered dashboard definition according to the network status during operation and check the flow status.
- Move to (drill-down analyze) the Exporter Analysis page with the analysis conditions narrowed down by clicking a link in the list on the widget.
- Export the analysis results of the widget to a CSV file.

4.1.2 Performing operations on the dashboard display page

The following describes the Dashboard page.

Dashboard page

The current communication status of the analysis target exporter and interfaces can be grasped by checking widgets.

The Dashboard pages is displayed immediately after logging in to NFA. This page can also be displayed by clicking the **Dashboard** tab.

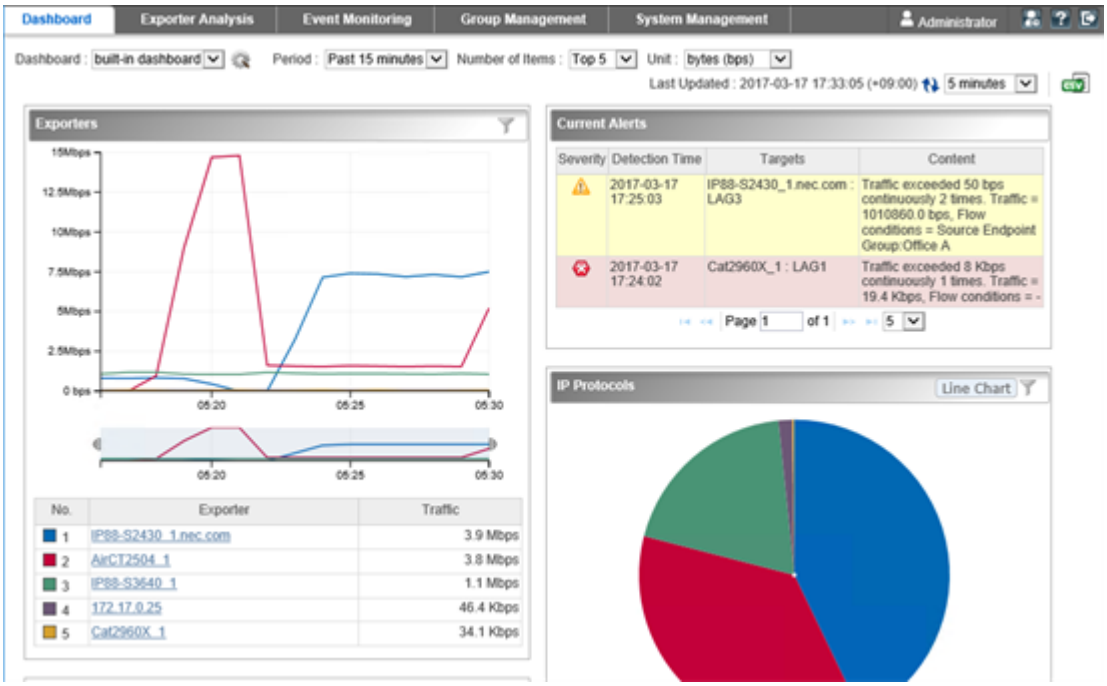

Figure 4-1 Dashboard display page

Operation area

- **Dashboard Name**

  Select the registered dashboard definition from the pull-down menu. The analysis contents to be displayed on the dashboard can be switched.

- **(Dashboard Management)** button

  Use this button to check the contents of the registered dashboard definition, and add, update, or delete a dashboard definition. The Dashboard Management page is displayed by clicking this button.

- **Period**

  Select the analysis period for the target flow from the pull-down menu (**Past 15 minutes** / **Past 30 minutes** / **Past 1 hour** / **Past 6 hours** / **Past 24 hours** / **Past 48 hours** / **Past 72 hours**). The default is **Past 15 minutes**.

- **Number of Items**

  Select the number of top data items to be displayed on widgets of the dashboard from the pull-down menu (**Top 5** / **Top 10** / **Top 20**). The default is **Top 5**.

  Note that, however, for a pie chart widget, items below the specified number of items to be displayed are displayed as one item in *"Other"*. Therefore, the number of items displayed on a chart is *"specified number of items to be displayed + 1"*.

- **Unit**

  Select the unit of the communication traffic to be displayed on the widgets of the dashboard from the pull-down menu (**bytes (bps)** / **packets (pps)**). The default is **bytes (bps)**.

- **Last Updated**

  Displays the date when the widget was last updated.

- **(Update)** button

Updates the analysis results of all widgets on the dashboard to the latest information.

- **Refresh Interval**

  Select the interval to refresh the analysis results of the widgets on the dashboard from the pull-down menu (**1 minutes** / **5 minutes** / **15 minutes** / **None**). The default is **5 minutes**.

- **(CSV Export)**

  Exports the analysis results of all widgets on the dashboard to a CSV file. For details, see "4.3.2 Exporting analysis results to a CSV file from the Web console (page 77)".

Widget display area

Displays widgets. For details about the operations that can be performed on widgets displayed on the dashboard, see "1.2.5 Performing operations on widgets (page 16)".

4.1.3 Performing operations on the dashboard

The following describes the Dashboard Management page.

Dashboard Management page.

On this page, you can check the registered dashboard definitions and also register a dashboard definition.

To display the Dashboard Management page, click the **(Dashboard Management)** button on the Dashboard page.

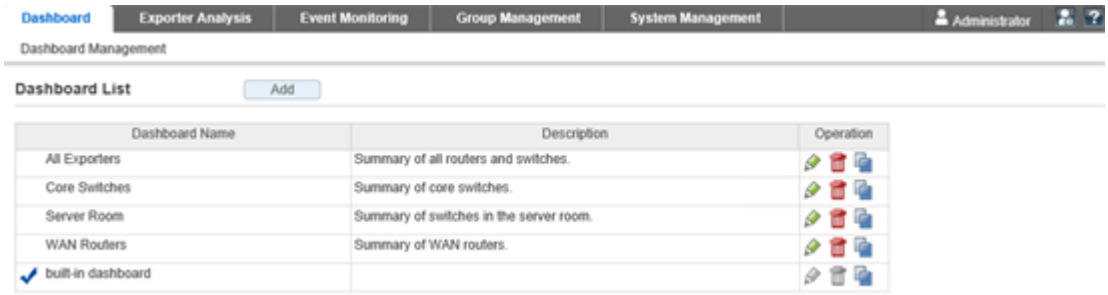

Figure 4-2 Dashboard Management page

Operation area

- **Add** button

  Use this button to add a new dashboard definition. The Add Dashboard page is displayed by clicking this button.

Dashboard List

- **Dashboard Name**

  Displays the name of the dashboard definition.

  ### Tip

  indicates that the marked dashboard has been set as **Default Dashboard** of the logged in user.

- **Description**

Displays a description of the dashboard definition.

- **Operation**

  Displays the operation buttons that are available for the registered dashboard.

  - **(Edit)** button

    Use this button to change the registered contents of the dashboard definition. The Edit Dashboard page is displayed by clicking this button.

  - **(Delete)** button

    Use this button to delete a registered dashboard definition.

  - **(Copy)** button

    Use this button to create a new dashboard definition by copying an existing dashboard definition. The Add Dashboard page is displayed by clicking this button.

Caution

The displayed operation buttons differ depending on the user authority level.

- Administrator

  Only the **(Copy)** button is available for *"built-in dashboard"*, which is registered by default. Other buttons are displayed in a disabled state.

- Operator

  All operation buttons are available for a dashboard definition that the logged in user has created.

  For a dashboard definition created by another user, only the **(Copy)** button is available. Other buttons are not displayed.

4.1.3.1 Adding a dashboard definition

The following describes the procedure to add a new dashboard definition.

1. Open the Dashboard Management page.

   Click the **(Dashboard Management)** button on the Dashboard page.

2. Click the **Add** button.

   Tip

   When creating a new dashboard definition based on an existing dashboard definition, click the **(Copy)** button of the source dashboard definition in Dashboard List. The Add Dashboard page is displayed.

3. Specify an appropriate value for each item on the displayed Add Dashboard page.

   - **Dashboard Name**

     Specify a dashboard definition name by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

   - **Description**

     Describe the purpose and contents of the dashboard definition by using any characters. The available number of characters is 1024.

   - **Default Display Settings**

Specify the default settings of the dashboard display.

- **Period**

  Select the analysis period for the target flow from the pull-down menu (**Past 15 minutes** / **Past 30 minutes** / **Past 1 hour** / **Past 6 hours** / **Past 24 hours** / **Past 48 hours** / **Past 72 hours**). The default is **Past 15 minutes**.

- **Number of Items**

  Select the number of top data items to be displayed on a widget from the pull-down menu (**Top 5** / **Top 10** / **Top 20**). The default is **Top 5**.

- **Unit**

  Select the unit of the communication traffic to be displayed on a widget from the pull-down menu (**bytes (bps)** / **packets (pps)**). The default is **bytes (bps)**.

- **Refresh Interval**

  Select the interval to refresh the analysis results of widgets from the pull-down menu (**1 minutes** / **5 minutes** / **15 minutes** / **None**). The default is **5 minutes**.

4. Add a widget.

   a. Click the **Add Widgets** button to display the Add Widgets dialog box.

   b. Select the check box of the widget to be added to the dashboard.

   For details of the selectable widgets, see "1.2.4 Widget types (page 13)".

   c. Check the settings and click the **OK** button.

   The selected widget is added to the Add Dashboard page.

Tip

Up to 20 widgets can be added on one dashboard.

5. Specify the widget title or analysis target in detail.

   a. Click the **(Edit)** button of the widget to display the Widget Settings page.

   - **Display Title**

     Specify a widget title by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

     The default is a widget type name.

   - **Number of Items**

     Select **Number of Items** from the pull-down menu (**Use default setting** / **Top 5** / **Top 10** / **Top 20**). The default is **Top 5**.

     Specify this item if you want to display the data items of a widget that differ from the number of display items specified for **Default Display Settings** on the Add Dashboard page.

   - **Target**

     Select from the following:

     - **All Exporters**

       Select this to analyze all interfaces of all exporters that are registered to NFA.

     - **Specific Exporters**

Select this to select the exporter to be analyzed from the exporters that are registered to NFA.

Select the desired exporter from the **Not Selected** box and click the **Add** button.

- **Specific Interfaces**

  Select this to select the interface to be analyzed from the interfaces that are registered to NFA.

  Select the interface of the desired exporter from the **Not Selected** box and click the **Add** button.

  Tip

  This will not be displayed on the *"Exporter"* widget.

b. Check the settings and click the **OK** button.

6. Set the chart type to be displayed on the widget.

   Click the **Line Chart** or **Pie Chart** button of the target widget.

   Tip

   The **Line Chart** and **Pie Chart** buttons may not be displayed depending on the widget type.

   Click the **Line Chart** button to display a line chart. Click the **Pie Chart** button to change the displayed line chart to a pie chart.

7. Adjust the display of the widget.
   - To change the widget position:

     Place the cursor on the widget, and drag and drop it to the desired position on the page.
   - To delete an unnecessary widget:

     Click the **(Delete)** button of the widget.
8. Check the settings and click the **OK** button.

4.1.3.2 Updating a dashboard definition

The following describes the procedure to update a dashboard definition.

1. Open the Dashboard Management page.

   Click the **(Dashboard Management)** button on the Dashboard page.
2. In Dashboard List, click the **(Edit)** button of the target dashboard.
3. Change the settings on the displayed Edit Dashboard page.

   The following settings can be changed.
   - **Dashboard Name**

     Specify a dashboard definition name by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.
   - **Description**

     Describe the purpose and contents of the dashboard definition by using any characters. The available number of characters is 1024.

- **Default Display Settings**

  Specify the default settings of the dashboard display.

  - **Period**

    Select the analysis period for the target flow from the pull-down menu (**Past 15 minutes** / **Past 30 minutes** / **Past 1 hour** / **Past 6 hours** / **Past 24 hours** / **Past 48 hours** / **Past 72 hours**). The default is **Past 15 minutes**.

  - **Number of Items**

    Select the number of top data items to be displayed on a widget from the pull-down menu (**Top 5** / **Top 10** / **Top 20**). The default is **Top 5**.

  - **Unit**

    Select the unit of the communication traffic to be displayed on a widget from the pull-down menu (**bytes (bps)** / **packets (pps)**). The default is **bytes (bps)**.

  - **Refresh Interval**

    Select the interval to refresh the analysis results of widgets from the pull-down menu (**1 minutes** / **5 minutes** / **15 minutes** / **None**). The default is **5 minutes**.

4. Add a widget.

   a. Click the **Add Widgets** button to display the Add Widgets dialog box.

   b. Select the check box of the widget to be added to the dashboard.

      For details of the selectable widgets, see "1.2.4 Widget types (page 13)".

   c. Check the settings and click the **OK** button.

      The selected widget is added to the Add Dashboard page.

5. Change the displayed widget title or the analysis target.

   a. Click the **(Edit)** button of the widget to display the Widget Settings page.

      - **Display Title**

        Specify a widget title by using any characters. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

        The default is a widget type name.

      - **Number of Items**

        Select **Number of Items** from the pull-down menu (**Use default setting** / **Top 5** / **Top 10** / **Top 20**). The default is **Top 5**.

        Specify this item if you want to display the data items of a widget that differ from the number of display items specified for **Default Display Settings** on the Add Dashboard page.

      - **Target**

        Select from the following:

        - **All Exporters**

          Select this to analyze all interfaces of all exporters that are registered to NFA.

        - **Specific Exporters**

          Select this to select the exporter to be analyzed from the exporters that are registered to NFA.

Select the desired exporter from the **Not Selected** box and click the **Add** button.

- **Specific Interfaces**

  Select this to select the interface to be analyzed from the interfaces that are registered to NFA.

  Select the interface of the desired exporter from the **Not Selected** box and click the **Add** button.

  Tip

  This will not be displayed on the *"Exporter"* widget.

b. Check the settings and click the **OK** button.

6. Change the chart type to be displayed on the widget.

   Click the **Line Chart** or **Pie Chart** button of the target widget.

   Tip

   The **Line Chart** and **Pie Chart** buttons may not be displayed depending on the widget type.

   Click the **Line Chart** button to display a line chart. Click the **Pie Chart** button to change the displayed line chart to a pie chart.

7. Adjust the display of the widget.

   - To change the widget position:

     Place the cursor on the widget, and drag and drop it to the desired position on the page.

   - To delete an unnecessary widget:

     Click the **(Delete)** button of the widget.

8. Check the changes and click the **OK** button.

4.1.3.3 Deleting a dashboard definition

The following describes the procedure to delete a dashboard definition.

1. Open the Dashboard Management page.

   Click the **(Dashboard Management)** button on the Dashboard page.

2. In Dashboard List, click the **(Delete)** button of the target dashboard.
3. Check the contents displayed in the Delete Confirmation dialog box.
4. Click the **OK** button to delete the dashboard definition.

4.2 Analyzing the flow in detail for each exporter

NFA can analyze the flow in detail by specifying the exporter and its interfaces and identifying the part of flow to be monitored. The following describes the exporter analysis function used to analyze the current and past flow status in detail.

4.2.1 Exporter analysis

The following describes the purpose of exporter analysis.

Purpose of exporter analysis

Exporter analysis is used to focus on a specific exporter or interface and analyze the communications that pass through that exporter or interface in detail. This function can also be used to check past flow status in addiction to current flow status, unlike analysis using the dashboard.

Exporter analysis is useful for detecting errors while observing the entire status on the dashboard, and for drilling down and investigating error causes. It is also useful for checking what the status of communication was when an error occurred on the network.

Operations that can be performed with exporter analysis

NFA exporter analysis can be used to perform the following analysis operations.

- Specify a past date and analyze the flow of a certain period in detail.
- Specify multiple filtering conditions (such as a source IP address and application) to narrow down flows and analyze them in detail. Filtering conditions can also be specified by clicking the links in the list of the widget.
- Export the analysis results of the widget to a CSV file.

4.2.2 Performing operations on the Exporter Analysis page

The following describes the Exporter Analysis page.

Exporter Analysis page

Flow status can be analyzed in detail by specifying various conditions to identify the flow.

To display the Exporter Analysis page, click the **Exporter Analysis** tab.

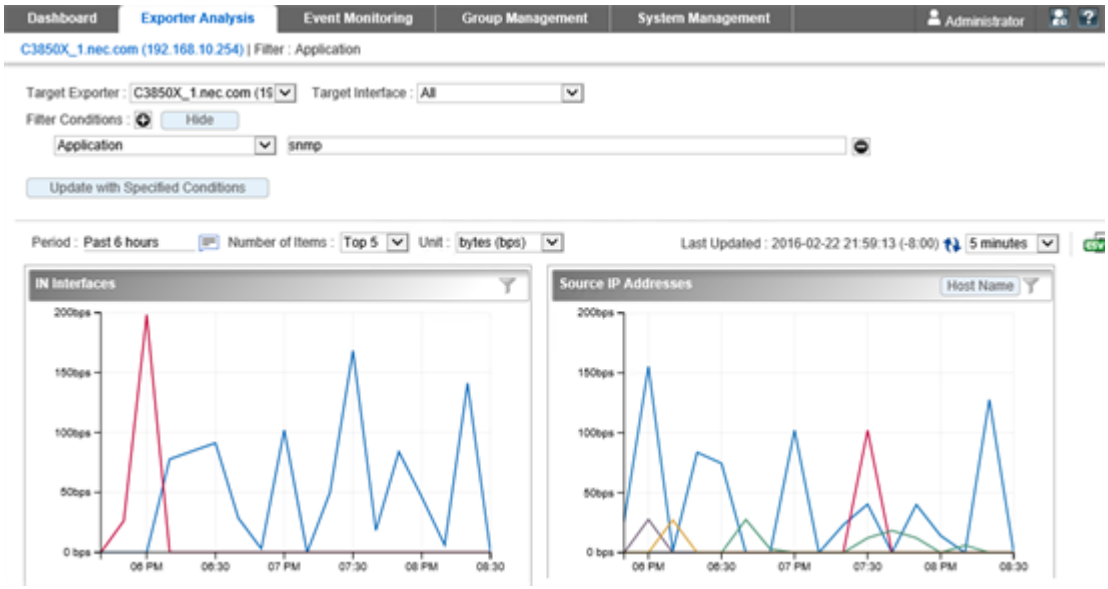

Figure 4-3 Exporter Analysis page

Operation area

- Analysis Target
  - **Target Exporter**

    Select the exporter to be analyzed.

- **Target Interfaces**

  Select the interface to be analyzed for the exporter selected in **Target Exporter** from the pull-down menu.

Tip

Exporters and interfaces for which an interface license has been assigned can be selected.

- **Filter Conditions**

Specify filtering conditions if you want to narrow down the target flow.

- Buttons
  * **(Add)** button

    Use this button to add a text box in the **Filter Conditions**. The flow that meets all the added conditions (AND condition) becomes the target of analysis.

  * **(Delete)**

    Use this button to delete a text box in the **Filter Conditions**.

  * **Show**/ **Hide** button

    Use this button to show or hide the **Filter Conditions**.

    This button is useful if you want to display the analysis results in as wide an area as possible in the widget.

- Condition specification

  The following conditions can be specified.

  * **Source IP Address**

    Focuses on the communication from the specified IP address and analyzes it considering the following:

    + Which IP address receives a lot of communication traffic?
    + Which application performs a lot of communications?
    + Which IP protocol is frequently used for communication?
    + Which DSCP value (PHB) is frequently used for communication?

  * **Destination IP Address**

    Focuses on the communication to the specified IP address and analyzes it considering the following:

    + Which IP address sends a lot of communication traffic?
    + Which application performs a lot of communications?
    + Which IP protocol is frequently used for communication?
    + Which DSCP value (PHB) is frequently used for communication?

  * **Source Endpoint Group**

    Focuses on the communication from the IP address belonging to the specified endpoint group and analyzes it considering the following:

    + Which IP address of the specified endpoint group sends a lot of communication traffic?

- Which IP address receives a lot of communication traffic?
- Which application performs a lot of communications?
- Which IP protocol is frequently used for communication?
- Which DSCP value (PHB) is frequently used for communication?

* **Destination Endpoint Group**

  Focuses on the communication to the IP address belonging to the specified endpoint group and analyzes it considering the following:

  - Which IP address of the specified endpoint group receives a lot of communication traffic?
  - Which IP address sends a lot of communication traffic?
  - Which application performs a lot of communications?
  - Which IP protocol is frequently used for communication?
  - Which DSCP value (PHB) is frequently used for communication?

* **Application**

  Focuses on the communication of the specified application and analyzes it considering the following:

  - Which IP address sends a lot of communication traffic?
  - Which IP address receives a lot of communication traffic?
  - Which DSCP value (PHB) is frequently used for communication?

* **IP Protocol**

  Focuses on the communication using the specified IP protocol and analyzes it considering the following:

  - Which IP address sends a lot of communication traffic?
  - Which IP address receives a lot of communication traffic?
  - Which application performs a lot of communication?
  - Which DSCP value (PHB) is frequently used for communication?

* **DSCP**

  Focuses on the communication using the specified DSCP value (PHB) and analyzes it considering the following:

  - Which IP address sends a lot of communication traffic?
  - Which IP address receives a lot of communication traffic?
  - Which application performs a lot of communication?
  - Which IP protocol is frequently used for communication?

* **Source AS Number**

  Focuses on the communication from the network of the specified AS number and analyzes it considering the following:

  - Which AS number's network receives a lot of communication traffic?
  - Which IP address sends a lot of communication traffic?
  - Which IP address receives a lot of communication traffic?

+ Which application performs a lot of communications?
+ Which IP protocol is frequently used for communication?
+ Which DSCP value (PHB) is frequently used for communication?

* **Destination AS Number**

  Focuses on the communication to the network of the specified AS number and analyzes it considering the following:

  + Which AS number's network sends a lot of communication traffic?
  + Which IP address sends a lot of communication traffic?
  + Which IP address receives a lot of communication traffic?
  + Which application performs a lot of communications?
  + Which IP protocol is frequently used for communication?
  + Which DSCP value (PHB) is frequently used for communication?

Tip

* When specifying multiple values in one text box, separate them by commas (,). The flow that meets any of the specified conditions (OR condition) becomes the target of analysis.
* The available number of characters for each condition text box is 255.

- **Update with Specified Conditons** button

  Use this button to display the analysis results of the flow that meets the specified conditions.

  The widget type to be displayed as the analysis results differs depending on the specified filtering conditions. For details, see "4.2.3 Flow filtering conditions and widgets to be displayed (page 74)".

Display settings area

Specify the conditions to be applied to the display such as the analysis period and the number of display items.

The analysis results will be updated by changing any of the following items:

- Analysis period
  - **Period**

    Click the  button, and then specify the analysis period on the displayed page.

    * **Select from Default Periods** (default)

      Select the analysis period from the pull-down menu (**Past 15 minutes** / **Past 30 minutes** / **Past 1 hour** / **Past 6 hours** / **Past 24 hours** / **Past 48 hours** / **Past 72 hours**). The default is **Past 15 minutes**.

    * **Specify Starting Time and Period**

      Specify the date and time to start analysis and the analysis period. The default is from *"1 hour ago"* to *"current time"*.

      1. Specify the start date of the analysis period. Enter a value in the text box or select by clicking the  button.
      2. Select the start time from the pull-down menu. The selectable start time differs as follows depending on the specified date.

Table 4-1 Times that can be specified for each start date

Specified date	Time that can be specified
Today or yesterday	The time can be specified in 1-hour units starting from 0:00.
Two or three days ago	The time can be specified in 6-hour units starting from 0:00.
Four or more days ago	A time cannot be specified.

3. Select the analysis period from the pull-down menu. NFA offers appropriate choices according to the granularity of the flow data that NFA stores.

- **Number of Items**

  Select the number of top data items to be displayed on widgets from the pull-down menu (**Top 5** / **Top 10** / **Top 20**). The default is **Top 5**.

- **Unit**

  Select the unit of the communication traffic to be displayed on a widget from the pull-down menu (**bytes (bps)** / **packets (pps)**). The default is **bytes (bps)**.

- Updating and exporting the analysis results

  The analysis results can be updated and exported to a file.

  - **Last Updated**

    Displays the date when the widget was last updated.

  - **(Update)** button

    Updates the analysis results of all widgets to the latest information.

  - **Refresh Interval**

    Select the interval to refresh the analysis results of widgets from the pull-down menu (**1 minutes** / **5 minutes** / **15 minutes** / **None**). The default is **5 minutes**.

  - **(CSV Export)**

    The analysis results of all widgets can be exported to a CSV file. For details, see "4.3.2 Exporting analysis results to a CSV file from the Web console (page 77)".

Widget display area

Displays the analysis result of the flow that meets the specified conditions. The following operations can be performed on the widgets that shows the analysis results.

- "1.2.5.1 Performing drill-down analysis (page 16)"
- "1.2.5.2 Filtering the items displayed on a chart (page 17)"
- "1.2.5.3 Zooming in on a line chart (page 18)"
- "1.2.5.4 Changing the IP address display to the host name (page 18)"

4.2.3 Flow filtering conditions and widgets to be displayed

The following describes the widgets that are displayed by specifying **Filter Conditions** on the Exporter Analysis page.

The Exporter Analysis page shows the analysis results according to the following five viewpoints. The display contents of the analysis results differ depending on the specified **Filter Conditions**.

Analyzing the communication traffic for each interface

The communication traffic of the flow that meets the **Filter Conditions** value is displayed for each interface in the following widgets:

- **IN Interface** widget
- **OUT Interfaces** widget

Analyzing the communication traffic from the aspect of the endpoint

The flow that meets the **Filter Conditions** value is analyzed from the aspect of the endpoint in the following widgets:

- **Source IP Address** widget
- **Destination IP Address** widget
- **Conversation** widget

Tip

- If either **Source IP Address** or **Destination IP Address**, but not both, is specified for **Filter Conditions**,

  the communication traffic of the endpoint opposite to the specified condition is analyzed. For example, if **Source IP Address** is specified, the analysis results of the **Destination IP address** widget are displayed.
- If both **Source IP Address** and **Destination IP Address** are specified for **Filter Conditions**,

  the conversation of the flow is identified, so communication traffic analysis from the aspect of the endpoint is not executed.

Analyzing the communication traffic from the aspect of the communication type

The flow that meets the **Filter Conditions** value is analyzed from the aspect of the communication type (application, IP protocol and DSCP) in the following widgets:

- **Application** widget
- **IP Protocol** widget
- **DSCP** widget

Tip

- If **IP Protocol** is specified for **Filter Conditions**,

  the communication traffic of the application that uses the specified IP protocol is analyzed.
- If **Application** is specified for **Filter Conditions**,

  the communication type of the flow is identified, so communication traffic analysis from the aspect of the communication type is not executed.

Analyzing the communication traffic from the aspect of the endpoint group

If either **Source Endpoint Group** or **Destination Endpoint Group** is specified for **Filter Conditions**, the communication traffic of the endpoint group opposite to the specified condition is analyzed in the following widgets:

- **Source Endpoint Group** widget
- **Destination Endpoint Group** widget

Tip

- If both **Source Endpoint Group** and **Destination Endpoint Group** are specified for **Filter Conditions**,

  the source and destination endpoint groups of the flow are identified, so communication traffic analysis from the aspect of the endpoint group is not executed.

Analyzing the communication traffic from the aspect of the AS

If either **Source AS Number** or **Destination AS Number** is specified for **Filter Conditions**, the communication traffic for the AS opposite to the specified condition is analyzed in the following widgets:

- **Source AS** widget
- **Destination AS** widget

Tip

- If both **Source AS Number** and **Destination AS Number** are specified for **Filter Conditions**,

  the source and destination ASs of the flow are identified, so communication traffic analysis from the aspect of the AS is not executed.

4.3 Exporting accumulated data and analysis results

NFA provides a command to output flow data accumulated in a database to CSV files and a function to output the flow information displayed on widgets to CSV files from the Web console.

nfa_flow_export command

The `nfa_flow_export` command is used to output the detailed flow data accumulated in a database to external CSV files.

CSV output from the Web console

This function is used to output flow information that has been analyzed and displayed on widgets of the Dashboard and Exporter Analysis pages to external CSV files.

4.3.1 Exporting accumulated data to CSV files by using a command

Flow data stored in a database can be output to external CSV files by using the `nfa_flow_export` command.

To output CSV file by this command, specify a target flow data type, data granularity, and period. There are the two main data types: detailed flow data focusing on one exporter, and flow data of the entire network integrating information of all exporters.

Registering this command to a program such as cron makes it possible to export flow data to CSV files periodically.

For details, see "A.2 nfa_flow_export (page 101)" and "A.2.3 Usage examples (page 112)".

4.3.2 Exporting analysis results to a CSV file from the Web console

The following describes the procedure to export the analysis results displayed on a widget of the Dashboard and Exporter Analysis pages.

1. Open the flow information analysis page.
   - To display the Dashboard page, click the **Dashboard** tab.
   - To display the Exporter Analysis page, click the **Exporter Analysis** tab.
2. Specify the flow analysis conditions.

   The analysis results of each widget are displayed.
3. Click **(CSV Export)** in the right corner of the widget display area.

   Downloading a zip file that includes the analysis results of the widgets displayed on the page starts.

   Tip

   Files to be downloaded are named as follows:
   - For the Dashboard page:

     `DashboardCSV_<yyyymmdd-hhmmss>.zip`
   - For the Exporter Analysis page:

     `ExporterAnalysisCSV_<yyyymmdd-hhmmss>.zip`

   <*yyyymmdd-hhmmss*> indicates the NFA server date and time when the relevant files were exported.
4. Check the contents of the downloaded zip file.

   Unzip the zip file and check that CSV files corresponding to the analysis results of all widgets on the page exist.

   The correspondence between a widget and CSV file can be judged by the CSV file name. CSV files are named as follows:

   <ID>_<widget number>_<widget name>_<chart type>.csv
   - ID

     Shows a unique ID that is internally assigned to a widget by NFA.
   - Widget number and widget name

Shows the number and name corresponding to the widget type. The following table shows their correspondence.

Table 4-2 Widget number and widget name corresponding to widget type

Widget type	Widget number	Widget name
Exporter	1	Exporters
IN Interface	2	InInterfaces
OUT Interface	3	OutInterfaces
Source IP Address	20	SourceIPAddresses
Destination IP Address	21	DestinationIPAddresses
Conversation	23	Conversations
Source Endpoint Group	40	SourceEndpointGroups
Destination Endpoint Group	41	DestinationEndpointGroups
Source AS	30	SourceAS
Destination AS	31	DestinationAS
Application	13	Applications
IP Protocol	14	IPProtocols
Current Alerts	50	CurrentAlerts
DSCP	81	DSCP

- Chart type

  Shows how the data in the CSV file is displayed. The following table describes the display types.

Table 4-3 Chart types

Chart type	Description
line	Indicates data of a line chart.
pie	Indicates data of a pie chart.
table	Indicates data of a list.

5. Check the contents of the CSV file.

   The following table describes the CSV file contents.

Table 4-4 CSV file contents

Line No.	Item	Description
1	Date	Indicates the date and time when the data was exported to the CSV file.
2	CsvType	Indicates the page from which the CSV file was exported. • Dashboard The CSV file was exported from the Dashboard page. The name of the dashboard definition of the relevant page is also exported. • ExporterAnalysis The CSV file was exported from the Exporter Analysis page.

Line No.	Item	Description
3	Widget	Displays the information of the widget that was analyzed. The format is as follows: <widget number>,<widget name>,<chart type>
4	StartingTime	Indicates the starting time of the analysis period of the exported data. *"-"* is always displayed for the **Current Alerts** widget.
5	EndingTime	Indicates the ending time of the analysis period of the exported data. *"-"* is always displayed for the **Current Alerts** widget.
6	Interval(minutes)	Indicates the interval at which line chart data is plotted in minutes *"-"* is always displayed for a pie chart and list data.
7	Unit	Indicates the unit of the exported data. The available units are as follows: bytes, bps, packets, pps, -
8	StartingPosition	Indicates the line number in the CSV file from which the actual data was exported.
9	TargetType	Indicates the type of the analysis target. • Exporters The analysis target is an exporter. • Interfaces The analysis target is an interface.
10	Exporters or Interfaces	Indicates the name of the analysis target exporter or interface. Multiple names are displayed separated by commas. An interface name is displayed in the following format: <exporter name> : <interface name> When interfaces of all exporters are the analysis targets, the following is displayed. (All)
11	FilterCount	Indicates the number of filtering conditions specified on the Exporter Analysis page. The content of this line was not exported if the data was exported from the Dashboard page.
~N	<Filter Conditions>	If the value of *"FilterCount"* is other than *"0"*, the filtering conditions are displayed on the 12th and subsequent lines one by one in the following format: <filtering condition>,<set value> The filtering conditions are described as follows: • SourceIPAddress Indicates that the filtering condition is **Source IP Address**. • DestinationIPAddress Indicates that the filtering condition is **Destination IP Address**. • SourceEndpointGroup Indicates that the filtering condition is **Source Endpoint Group**. • DestinationEndpointGroup Indicates that the filtering condition is **Destination Endpoint Group**. • SourceAS

Line No.	Item	Description
		Indicates that the filtering condition is **Source AS Number**. • DestinationAS Indicates that the filtering condition is **Destination AS Number**. • Application Indicates that the filtering condition is **Application**. • IPProtocol Indicates that the filtering condition is **IP Protocol**. • DSCP Indicates that the filtering condition is **DSCP**.
N+1	Blank line	A blank line is inserted in order to separate the above information and the actual exported data.
N+2	WidgetTitle	Indicates the title of the widget that was analyzed. For data exported from the Dashboard page, this item is displayed on the 12th line and the title of the widget that the user specified in the dashboard definition is exported.
N+3	<data label>	The label describing the content of the exported file is displayed in the following format: Time,<item>,...
N+4	<data>	Data corresponding to the data label is exported separated by commas (,).

Tip

Time information in the file is displayed as a UNIX time format.

Caution

In principle, data in the same time range as the analysis result chart displayed on the web console is exported to a CSV file. For the Current Alerts widgets, a new alert that has occurred internally might not be displayed on the page if it occurred at the same time that the web console display was refreshed. Therefore, the current alerts exported to the CSV file might differ from those displayed on the web console because the exported current alerts were current at the time the data was exported to the CSV file.

4.4 Checking event information

Event occurrence detected by NFA can be checked on the Event List page.

4.4.1 Checking the history of threshold violation and recovery event occurrence

The following describes the contents displayed on the Event List page.

Event List page

This page displays the history of threshold violations and recovery events that NFA has detected.

NFA stores up to 10,000 of the latest events.

To display the Event List page, click **Event Monitoring**>**Event List**.

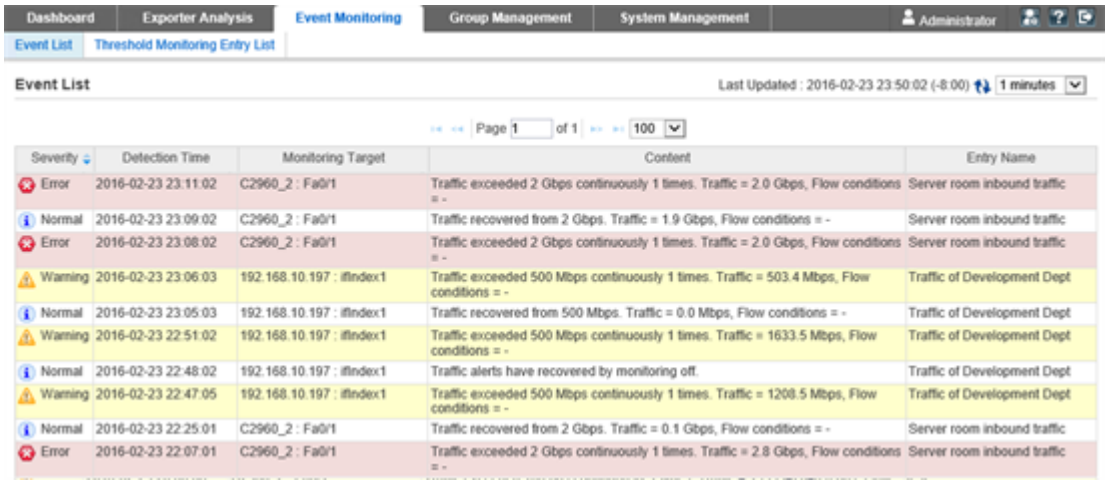

Figure 4-4 Event List page

Display settings area

The following items can be updated and displayed in this area.

- **Last Updated**

  Displays the date when the history was last updated.

- **(Update)** button

  Updates the analysis results of all widgets on the dashboard to the latest information.

- **Refresh Interval**

  Select the interval to refresh the **Event List** from the pull-down menu (**1 minutes** / **5 minutes** / **15 minutes** / **None**). The default is **1 minutes**.

Event list

- Page navigation buttons

  Displays the stored event information over multiple pages. The following operations can be performed on the displayed pages.

  - Page transition buttons

    * button

      Use this button to display the first page (latest information).

    * button

      Use this button to display the previous page of the currently displayed page.

    * button

      Use this button to display the next page of the currently displayed page.

    * button

      Use this button to display the last page.

  - **Page** text box

    Enter the page number to be displayed.

- **Number of Items**

  Select the number of events to be displayed per page from the pull-down menu (**50** / **100** / **250** / **500** / **1000**). The default is **100**.

- Event list
  - **Severity**

    Displays the severity of the event as follows:

    *  Error
    *  Warning
    *  Normal

  - **Detection Time**

    Displays the date and time when NFA detected the event.

  - **Monitoring Target**

    Displays the names of the monitored exporter and interfaces where the event was detected.

  - **Content**

    Displays the content of the event.

  - **Entry Name**

    Displays the name of the monitoring entry in which the event was detected.

Tip

The displayed data can be sorted by clicking the column headers: **Severity** and **Detection Time**.

Chapter 5. System Maintenance

This chapter describes how to maintain NFA.

Contents

5.1 Maintaining the system environment

The following describes the procedure to maintain the system environment.

5.1.1 Checking the product version

The following describes the procedure to check the product version.

Before contacting the NEC Customer Support Center about NFA operations, or applying an update program obtained from the NEC Customer Support Center, confirm the correct version of NFA being used.

There are two methods to check the version. One is checking from the web console, and the other is checking by using a command. In an environment or state in which the web console cannot be opened, use a command to check the version.

- Checking from the web console
  1. Connect to the NFA web console.
  2. Check the version displayed in the footer area. You can check the version on any page.

     The version is displayed in the following format:

     MasterScope Network Flow Analyzer <version number>-<release number>

     Example: When the version is *"1.0.0"* and the release number is *"16"*

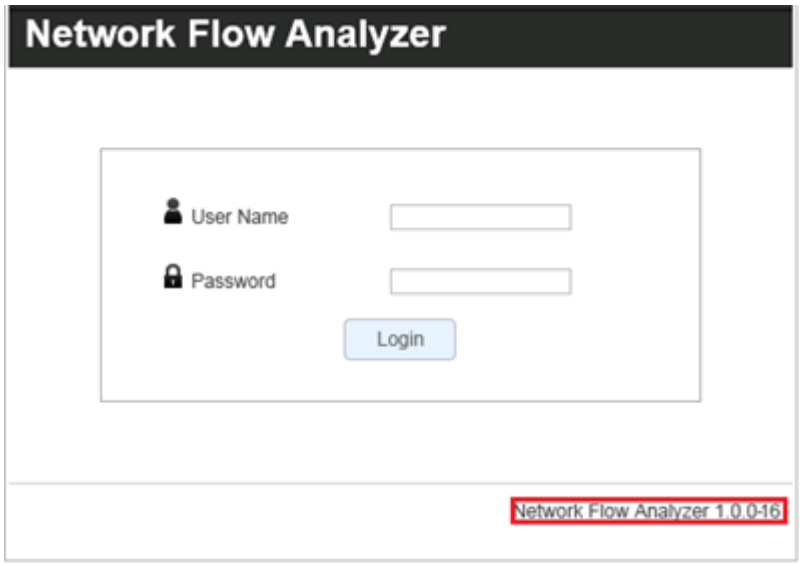

Figure 5-1 Version information display

- Checking by using a command
  1. Log in to the NFA server. (You can also log in as a user other than a root user.)
  2. Run the following command:

```
$ rpm -q nec-nfa-controller
```

  1. Check the displayed version.

     The version is displayed in the following format:

     nec-nfa-controller-<version number>-<release number>.x86_64

     Example: When the version is *"1.0.0"* and the release number is *"16"*

```
$ rpm -q nec-nfa-controller
nec-nfa-controller-1.0.0-16.x86_64
```

5.1.2 Starting or stopping the service

The following describes the procedure to manually start or stop the NFA service on the server on which NFA is running.

The NFA service automatically starts or stops in conjunction with the start or shutdown of the OS.

To stop and restart only the NFA service for maintenance of NFA while the OS is running, run the following command provided by NFA.

`/etc/init.d/nec-nfa-service`

To run this command, you need to log in to the NFA server as a root user.

- To start the service, run the command with the argument `start` specified.

  ```
  # /etc/init.d/nec-nfa-service start
  ```

  If all service processes of NFA started successfully, the command returns 0.

  - In Red Hat Enterprise Linux 6

    ```
    Starting systemdb:                [  OK  ]
    Starting eventdb:                 [  OK  ]
    Starting controller:              [  OK  ]
    Starting web server:              [  OK  ]
    Starting flowdb:                  [  OK  ]
    Starting logserver:               [  OK  ]
    Starting collector:               [  OK  ]
    ```

  - In Red Hat Enterprise Linux 7

    ```
    Starting nec-nfa-service (via systemctl):  [  OK  ]
    ```

- To stop the service, run the command with the argument `stop` specified.

  ```
  # /etc/init.d/nec-nfa-service stop
  ```

  If all service processes of NFA stopped successfully, the command returns 0.

  - In Red Hat Enterprise Linux 6

    ```
    Stopping collector:               [  OK  ]
    Stopping logserver:               [  OK  ]
    Stopping flowdb:                  [  OK  ]
    Stopping web server:              [  OK  ]
    Stopping controller:              [  OK  ]
    Stopping eventdb:                 [  OK  ]
    Stopping systemdb:                [  OK  ]
    ```

  - In Red Hat Enterprise Linux 7

    ```
    Stopping nec-nfa-service (via systemctl):  [  OK  ]
    ```

- The service status can be checked by running the command with the argument `status` specified.

  ```
  # /etc/init.d/nec-nfa-service status
  ```

  When the service is running, the following message is displayed. In addition, the command returns 0.

```
systemdb (pid 12340) is running...
eventdb (pid 12341) is running...
controller (pid 12342) is running...
web server (pid 12343) is running...
flowdb (pid 12344) is running...
logserver (pid 12345) is running...
collector (pid 12346) is running...
```

When the service has stopped, the following message is displayed. In addition, the command returns 3.

```
systemdb is stopped
eventdb is stopped
controller is stopped
web server is stopped
flowdb is stopped
logserver is stopped
collector is stopped
```

5.1.3 Changing the port number used in this product

The following describes the procedure to change the port number that NFA uses.

For the port numbers that NFA uses, see "C.1 Port numbers used in this product (page 119)".

Execute the following procedure to change the port numbers used by NFA.

1. Log in to the server as a root user.
2. Stop the NFA service.

   ```
   # /etc/init.d/nec-nfa-service stop
   ```

3. Change the content of the configuration file corresponding to the port number to be changed and save the file.

   For details about the configuration files, see "Table 5-1 Configurations for communication port numbers (external communication) (page 86)" and "Table 5-2 Configurations for communication port numbers (internal communication) (page 87)". If no configuration file exists, create a configuration file.

   The configuration files are stored in *<%data directory%>*.

Table 5-1 Configurations for communication port numbers (external communication)

Purpose	Setting items

HTTP communication	• Configuration file
	`controller/conf/tomcat.properties`
	• Specification format
	`nfa.tomcat.https.port = 443`

Reception of sFlow packets	• Configuration file
	`collector/conf/collector.conf`
	• Specification format
	`sflow.port = 6343`

Reception of NetFlow packets	• Configuration file `collector/conf/collector.conf`

Purpose	Setting items
	• Specification format `netflow.port = 9995`

The configuration files are stored in *<%data directory%>*.

Table 5-2 Configurations for communication port numbers (internal communication)

Purpose	Setting items

Flow database communication	• Configuration file
	`collector/conf/flowdb.conf`
	• Specification format
	`flowdb.port = 27100`

	• Configuration file
	`collector/conf/flowdb-extra.conf`
	• Specification format
	`port = 27100`

System database communication	• Configuration file
	`controller/conf/controller.properties`
	• Specification format
	`systemdb.port = 27110`

	• Configuration file
	`controller/conf/systemdb-extra.conf`
	• Specification format
	`port = 27110`

Event database communication	• Configuration file
	`controller/conf/event.properties`
	• Specification format
	`eventdb.port = 27120`

	• Configuration file
	`controller/conf/eventdb-extra.conf`
	• Specification format
	`port = 27120`

Controller control communication	• Configuration file
	`controller/conf/controller.properties`
	• Specification format
	`message.server.port = 27200`

	• Configuration file `collector/conf/collector.conf` • Specification format

Purpose	Setting items
	`controller.port = 27200`

Collector log service communication	• Configuration file
	`collector/conf/nfalog.conf`
	• Specification format
	`Port = 27210`

Caution

For a communication port for which one item is described in multiple configuration files, edit all the files at the same time to specify the same port number. If the specified port number differs among the relevant configuration files, this product does not work properly.

4. Review the firewall settings as required.

   The port number for external communication is often blocked by a firewall. Therefore, after changing the port number, check that the firewall settings are appropriate.

5. Start the NFA service.

```
# /etc/init.d/nec-nfa-service start
```

After the service is restarted, the changed port number is applied to the NFA.

5.1.4 Changing the web server URL

The following describes the procedure to change the URL to access NFA.

The domain name (FQDN) of the URL to access NFA can be changed. After changing the domain name, change the domain name (CN of the identification name) on the SSL server certificate.

To perform operations on the SSL server certificate, use `nfa_ssl_keytool` command provided by this product. For details, see "A.1 nfa_ssl_keytool (page 98)".

1. Log in to the NFA server as a root user.
2. Run the following command and check the Owner information in the output message.

```
# <%installation directory%>/controller/bin/nfa_ssl_keytool list -v
```

Execution example:

```
# cd /opt/nec/nfa/controller/bin
# ./nfa_ssl_keytool list -v | grep '^Owner'
Owner:  CN=nfa.nec.com, OU=IT Operation Division, O=NEC Corporation,
 L=Minato-ku, ST=Tokyo, C=JP
```

3. Run `nfa_ssl_keytool selfcert` command with the `-dname` option specified to update the identification name.

```
# <%installation directory%>/controller/bin/nfa_ssl_keytool selfcert
 -dname <dname>
```

In the checked Owner information, change the value of CN related to the domain name, and run the command.

Execution example:

```
# ./nfa_ssl_keytool selfcert -dname "CN=new-nfa.nec.com,
 OU=IT Operation Division, O=NEC Corporation, L=Minato-ku,
 ST=Tokyo, C=JP"
```

4. If the certificate was issued by a public certificate authority, ask the certificate authority to issue the certificate again.

   a. Run the following command to output the certificate signing request (CSR) to be sent to the certificate authority to a file.

   ```
   # <%installation directory%>/controller/bin/nfa_ssl_keytool
    certreq -dns <FQDN> <filename>
   ```

   The contents of the CSR are output to the specified file.

   b. Submit the certificate signing request (CSR) to the certificate authority.

   Submit the CSR file contents output by `nfa_ssl_keytool certreq` command to the certificate authority.

   The certificate authority will sign the certificate according to the contents of the CSR and return to the signed certificate to you. It might take several days until you receive the signed certificate.

   c. Import the signed certificate returned from the certificate authority.

   Run `nfa_ssl_keytool importcert` command without the `-alias` option specified.

   ```
   # <%installation directory%>/controller/bin/nfa_ssl_keytool
    importcert <filename>
   ```

   If `Failed to establish chain from reply` is displayed, the certificate chain could not be built. The root and/or intermediate certificates might not have been imported. Ask the certificate authority about the root and/or intermediate certificates that must be imported.

5. Restart the NFA service.

```
# /etc/init.d/nec-nfa-service stop
# /etc/init.d/nec-nfa-service start
```

6. If you use a self-signed certificate, run `nfa_ssl_keytool exportcert` command to export the certificate to a file in order to import it to a web browser.

```
# <%installation directory%>/controller/bin/nfa_ssl_keytool exportcert
 <filename>
```

Any name can be specified for <*filename*>. However, we strongly recommend specifying `.cer` as the file extension to enable the created file to be easily imported to a web browser.

Distribute and import the certificate file exported by using `nfa_ssl_keytool exportcert` command to all web browsers that access NFA. This prevents security problems such as a phishing attack whereby an unauthorized server acts as a NFA web server.

For how to import the certificate to a web browser, see "1.2.1.3 Importing an SSL server certificate to the web browser (page 9)".

Updating the certificate of the NFA server is now complete.

Even for a certificate issued by a public certificate authority, it might be necessary to install the certificate to the web browser depending on the certificate authority. For details, follow the instructions of the certificate authority.

5.1.5 Backing up and restoring the environment settings

The following describes the procedure to back up and restore the NFA environment settings.

Information set by NFA can be backed up by backing up the environment settings. You can restore the environment at the time of backup by restoring this backup data.

Note that the following information in the environment settings is not backed up.

- Accumulated flow data
- Occurred event data
- Registered license information

Because this data is not restored, the relevant information of the restoration destination will remain as is.

Tip

You can also back up the environment settings as well as the accumulated flow data and event data. For details, see "5.1.6 Backing up and restoring all data (page 91)".

The environment settings can be backed up while the NFA service is running, unlike backing up all data.

Notes on restoration

- The backup data does not include license information. Therefore, if the registered licenses differ between the environment whose settings were backed up and the restoration destination, register as many licenses as the licenses of the backup source environment to the restoration destination before restoring the backup data.

  For details about the license management, see "2.1 Managing the license (page 22)".
- If the domain name of NFA (URL to access to the web server) differs between the backup source environment and the restoration destination, modify the SSL server certificate.
- Specify the same value for the kernel parameter kernel.shmmax of both the backup source environment and the restoration destination, or specify a larger value for the restoration destination.

  If the kernel.shmmax value of the restoration destination is smaller than that of the backup source environment, the service will not be able to start after restoration.
- Information such as registered exporters is managed by assigning a different internal ID per system. Flow data is also managed by using this internal ID. If the backup of the environment settings is restored to an environment whose configuration differs from the backup source environment, the flow data accumulated in the restoration destination might be displayed as different content from the original information.

  Therefore, we recommend setting the restoration destination in the same system or in an environment in which this product has just been installed and no flow data has accumulated.

5.1.5.1 Backing up the environment settings

The following describes the procedure to back up the NFA environment settings.

The environment settings can be backed up while the NFA service is running.

1. Log in to the NFA server as a root user.
2. Run the following command:

```
# <%installation directory%>/controller/bin/nfa_backup <path>
```

For the argument <*path*>, specify the directory to which to export the backup.

If the command ends normally with no error message output, a backup file has been created in the specified output directory.

Save the created backup directory to an external storage media and store it in a safe place.

5.1.5.2 Restoring the environment settings

The following describes the procedure to restore the backup of the NFA environment settings.

Before restoring the backup environment settings, stop the NFA service.

There are some notes that pertain to restoring the backup environment settings. Before restoring the backup environment settings, see "Notes on restoration (page 90)".

Before starting restoration, deploy the backup directory stored in "5.1.5.1 Backing up the environment settings (page 90)" to the NFA server.

Tip

The backup directory stored in "5.1.6.1 Backing up all data (page 92)" can also be used. In this case, the flow data and event data are not restored. Only the environment settings are restored.

1. Log in to the NFA server as a root user.
2. Stop the NFA service.

   ```
   # /etc/init.d/nec-nfa-service stop
   ```

3. Run the following command to restore the NFA environment settings.

   ```
   # <%installation directory%>/controller/bin/nfa_restore <path>
   ```

   For the argument <*path*>, specify the directory in which the backup is stored.

   If the command ends normally with no error message output, the restoration is complete.

4. If the domain name of NFA (URL to access the web server) differs between the backup source environment and the restoration destination, update the SSL server certificate.

   For details about the update procedure, see "5.1.4 Changing the web server URL (page 88)".

5. Start the NFA service.

   ```
   # /etc/init.d/nec-nfa-service start
   ```

5.1.6 Backing up and restoring all data

The following describes the procedure to back up and restore the environment settings and the accumulated data all at once.

Information set by NFA and all of the accumulated flow data and event data can be backed up by backing up the environment settings and accumulated data all at once. You can restore the environment at the time of backup by restoring this backup.

Note that the registered license information is not backed up. The license information of the restoration destination will remain as is instead of being restored to the information at the time of backup.

Tip

You can back up the environment settings only and not include the accumulated flow data and event data. For details, see "5.1.5 Backing up and restoring the environment settings (page 90)".

The accumulated data cannot be backed up while the NFA service is running, unlike backing up the environment settings.

Notes on backup

- For an environment that has a lot of exporters or flows, the size of the data to be backed up might be several hundred GB to several TB. Back up the data by allocating the enough free space in the backup data output or storage destination.
- If the size of data to be backed up is several hundred GB to several TB, the backup processing might take several hours to a day or more.

Notes on restoration

- If the size of data to be restored is several hundred GB to several TB, the restore processing might take several hours to a day or more.
- The backup data does not include license information. Therefore, if the registered licenses differ between the environment whose settings were backed up and the restoration destination, register as many licenses as the licenses of the backup source environment to the restoration destination before restoring the backup data.

  For details about the license management, see "2.1 Managing the license (page 22)".
- If the domain name of NFA (URL to access to the web server) differs between the backup source environment and the restoration destination, modify the SSL server certificate.
- Specify the same value for the kernel parameter kernel.shmmax of both the backup source environment and the restoration destination, or specify a larger value for the restoration destination.

  If the kernel.shmmax value of the restoration destination is smaller than that of the backup source environment, the service will not be able to start after restoration.

5.1.6.1 Backing up all data

The following describes the procedure to back up the environment settings and accumulated data all at once.

To back up data all at once, the NFA service must be stopped.

There are some notes that pertain to backing up data all at once. Before backing up data all at once, see "Notes on backup (page 92)".

1. Log in to the NFA server as a root user.
2. Check the current size of the data to be backed up.

   Run the following command to check the size.

   ```
   # du -sm <%data directory%>/{controller,collector}/{conf,db}
   ```

   The result is displayed in MB units for each directory. Total the displayed sizes.

   Execution example:

```
# du -sm /opt/nec/nfa/{controller,collector}/{conf,db}
1       /opt/nec/nfa/controller/conf
92      /opt/nec/nfa/controller/db
1       /opt/nec/nfa/collector/conf
1016208 /opt/nec/nfa/collector/db
```

In the above example, the size of the data to be backed up is approximately 993 GB.

3. Stop the NFA service.

```
# /etc/init.d/nec-nfa-service stop
```

4. Run the following command:

```
# <%installation directory%>/controller/bin/nfa_backup -full <path>
```

For the argument <*path*>, specify the directory to which to export the backup. Specify a disk that has enough free space for the estimated backup size.

If the command ends normally with no error message output, a backup file has been created in the specified output directory.

Caution

It might take several hours to a day or more until the command completes, depending on the size of the data to be backed up.

5. Start the NFA service.

```
# /etc/init.d/nec-nfa-service start
```

Save the created backup directory to an external storage media and store it in a safe place.

5.1.6.2 Restoring a backup of all data

The following describes the procedure to restore the backed up environment settings and accumulated data all at once.

Before restoring the backup data, stop the NFA service.

There are some notes that pertain to restoring the backup data. Before restoring data all at once, see "Notes on restoration (page 92)".

Before starting restoration, deploy the backup directory backed up in "5.1.6.1 Backing up all data (page 92)" to the NFA server.

1. Log in to the NFA server as a root user.
2. Stop the NFA service.

```
# /etc/init.d/nec-nfa-service stop
```

3. Run the following command to restore the NFA environment settings.

```
# <%installation directory%>/controller/bin/nfa_restore -full <path>
```

For the argument <*path*>, specify the directory in which the backup is stored.

If the command ends normally with no error message output, the restoration is complete.

Caution

It might take several hours to a day or more until the command completes, depending on the size of the data to be backed up.

4. If the domain name of NFA (URL to access the web server) differs between the backup source environment and the restoration destination, update the SSL server certificate.

   For details about the update procedure, see "5.1.4 Changing the web server URL (page 88)".

5. Start the NFA service.

```
# /etc/init.d/nec-nfa-service start
```

5.2 Flow data management

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

5.2.1 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 5-3 Data unit times and retention periods (page 94)" 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 5-3 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
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.

5.2.2 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 "5.2.1 Flow data retention periods and data aggregation (page 94)", 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 "5.2.1 Flow data retention periods and data aggregation (page 94)".

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] = $(N + 5) \times P \times L \times 0.000415 + A \times 0.15 + 10{,}000$ [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.

  Tip

  If the maximum number of flows has been changed, specify an appropriate value according to that number.For how to change the maximum number of flows, see "5.2.3 Changing the maximum number of flows that can be stored (page 96)".

- 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

5.2.3 Changing the maximum number of flows that can be stored

The following describes the procedure to change the maximum number of flows that can be stored.

NFA stores the top 1,000 flows for each exporter per unit time by default.

This number can be changed.

⚠ Caution

Note that the larger the maximum number of flows to be stored, the larger the load on the NFA server. Therefore, the load on the server may become increasingly heavy, depending on the number of managed exporters, the number of received flows, and the machine specifications, with the result that NFA may not work properly.

After executing operations for one or more days in the actual operating environment, check the following to confirm that this product can work properly.

- No delay occurred in **Last Received** of all exporters on the Exporter Management page.
- Flow data can be viewed on the Dashboard and Exporter Analysis pages.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Specify the maximum number of flow data items that can be saved in the **Maximum Number of Flows** box.

Specify a value from 1,000 to 10,000 for the maximum number of flows. Use the following as a guide when considering the number of exporters as an index.

1 to 10

Top 10,000 flows

11 to 20

Top 6,000 flows

21 to 30

Top 3,000 flows

31 or more

It is not recommended to increase the maximum number of flows.

Tip

- You can change the maximum number by editing the following configuration file. If no configuration file exists, create a configuration file. If you change the maximum number of data flow items from **System Management**>**Environment Settings**, this file will be overwritten.
- After editing the configuration file, restart the NFA service to enable the change.
- *<%data directory%>*/controller/conf/flowdb.properties
- Specify the same value for the following six parameters:

```
flowdb.table.record.limit.1 = 1000
flowdb.table.record.limit.2 = 1000
flowdb.table.record.limit.3 = 1000
flowdb.table.record.limit.4 = 1000
flowdb.table.record.limit.5 = 1000
flowdb.table.record.limit.6 = 1000
```

5.2.4 Changing the flow retention periods

The following describes the procedure to change the maximum number of flows that can be stored.

NFA defines the retention periods to store flow data in a database according to "5.2.1 Flow data retention periods and data aggregation (page 94)".

Tip

It takes from several to 40 minutes after the maximum number of flows or the maximum retention period is decreased until the data will be actually deleted.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Specify the retention periods of flow data items to be saved in each input field of **Maintenance Settings of Flow Data**.

   Specify a longer retention period in order from the top of the above table. For example, if the retention period of **Flow Data of 1 Minute Unit** is set to 36 hours, the retention period of **Flow Data of 10 Minutes Unit** must be longer than 36 hours.

Appendix A. Command Reference

The following describes the commands that are provided by NFA.

A.1 nfa_ssl_keytool

This command is used to create and manage SSL server certificates that are used in HTTPS communication.

This command is a wrapper command that provides the functions of the Java keytool command in an easy-to-use format for this product. The Java keytool command functions that this command can use are limited. The names and meanings of the arguments are the same as those of the Java keytool command.

For details about the Java keytool command, see the following URL.

- https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html *1

The differences between this command and the Java keytool command are described below.

- For the first argument, specify a subcommand name such as `genkeypair`. `-` is not needed at the beginning of the argument name of the subcommand.
- For this command, the path of the keystore is fixed to *<%data directory%>*`/controller/conf/server.keystore`.
- `genkeypair` subcommand records the keystore passwords, the aliases of the entries in the keystore, and key passwords in the following file:

  <%data directory%>`/controller/conf/tomcat.properties`

  The information recorded in this file is automatically used when the `-storepass`, `-alias`, and `-keypass` options are omitted in subcommands. This permits users to run the command with the minimum number of arguments specified.
- The default values of the `-keyalg` and `-validity` options differ.
- An original subcommand `initstore` is implemented.

Path

<%installation directory%>`/controller/bin/nfa_ssl_keytool`

Synopsis

```
nfa_ssl_keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
nfa_ssl_keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-sigalg SIGALG] [-validity DAYS] [-dname DNAME]
```

```
nfa_ssl_keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-dns DNS] FILE
```

*1 This URL is current as of January 2019.

```
nfa_ssl_keytool importcert [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] FILE

nfa_ssl_keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE

nfa_ssl_keytool storepasswd [-help] [-storepass PASS] [-new NEWPASS]

nfa_ssl_keytool keypasswd [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-new NEWPASS]

nfa_ssl_keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]

nfa_ssl_keytool delete [-help] [-storepass PASS] [-alias ALIAS]

nfa_ssl_keytool initstore [-help]

nfa_ssl_keytool -help
```

Description

The following describes the subcommands.

- `genkeypair`

  Generates a key pair (public key and associated private key) and stores it in the keystore. This subcommand also writes the information required to used the key generated by the web server to the following file:

  <%data directory%>`/controller/conf/tomcat.properties`

- `selfcert`

  Creates a self-signed certificate for the key of the keystore entry.

- `certreq`

  Generates a certificate signing request (CSR) in the PKCS#10 format.

- `importcert`

  Reads the certificate or certificate chain from a file and stores it in the keystore.

- `exportcert`

  Reads the certificate from the keystore and stores it in a file as a binary encoded certificate.

- `storepasswd`

  Changes the password of the keystore.

- `keypasswd`

  Changes the key password of the keystore entry.

- `list`

  Displays a specific keystore entry or the entire contents of the keystore.

- `delete`

  Deletes an entry from the keystore.

- `initstore`

  Deletes a keystore file.

Arguments

-storepass *PASS*

Specifies a password for the keystore.

If this argument is omitted when running `genkeypair` subcommand, you will be prompted to enter a password while the command is running. If this argument is omitted when running other subcommands, the value read from the tomcat.properties file will be used.

-alias *ALIAS*

Specifies an alias for an entry in the keystore.

If this argument is omitted when running `genkeypair` subcommand, *"tomcat"* will be used by default. If this argument is omitted when running `list` subcommand, all entries will be displayed. If this argument is omitted when running other subcommands, the value read from the tomcat.properties file will be used.

-keypass *KEYPASS*

Specifies a password for the key.

If this argument is omitted when running `genkeypair` subcommand, you will be prompted to enter a password while the command is running. If this argument is omitted when running other subcommands, the value read from the tomcat.properties file will be used.

-keyalg *KEYALG*

Specifies an encryption algorithm for the password. For example, *"RSA"*, *"DSA"*, *"EC"* can be specified. The default is *"RSA"*.

For the algorithms that can be specified for `-keyalg` and `-sigalg`, see Java Cryptography Architecture (JCA) Reference Guide. *2

-keysize *KEYSIZE*

Specifies the size of the key to be generated.

The specifiable value range and default value comply with the Java keytool specifications.

-sigalg *SIGALG*

Specifies the algorithm used to sign a self-signed certificate.

An algorithm that is compatible with `-keyalg` must be specified. The specifiable value range and default value comply with the Java keytool specifications.

-validity *DAYS*

Specifies the number of days a self-signed certificate is valid. A value from 0 to 365000 can be specified. The default is 3650 (10 years).

-dname *DNAME*

Specifies the X.500 identification name to be used as the issuer and the subject fields of a self-signed certificate.

If this argument is omitted, you will be prompted to enter an identification name while the command is running.

-dns *DNS*

Specifies the FQDN for Subject Alternative Name (SAN) extension.

*2 This URL is current as of March 2016.

In `genkeypair` subcommand, if this argument is omitted, Common Name of a certificate is used as SAN.

-new *NEWPASS*

Specifies a new password if you want to change the kestore or key password.

If this argument is omitted, you will be prompted to enter a new password while the command is running.

-rfc

Specifies the output format of `list` subcommand. The content of a certificate will be output in a printable encoding format.

This option cannot be specified together with the `-v` option.

-v

Specifies the output format of `list` subcommand. The detailed content of the certificate will be output in a human readable format.

This option cannot e specified together with the `-rfc` option.

-help

Displays how to use commands in general or a specific command.

Return values

Success: 0 is returned. Failure: A value other than 0 is returned.

A.2 nfa_flow_export

This command is used to output flow data stored in a database to external CSV files.

To output CSV files by this command, specify a flow data type, data granularity, and target period.

- Target data types

  There are the following two main data types:

  - There are the following two main data types:
  - Flow data of the entire network integrating information of all exporters

    For the flow data of the entire network, select any of the following six data types: communication traffic of the exporters and its interfaces, source and destination IP addresses, applications, IP protocols, ToS (DSCP) and source and destination AS numbers.

- Target data granularity

  NFA manages received data by aggregating it every unit time and changing the data granularity. Specify the unit of data to be output as a parameter. For details about the data unit and aggregation, see "5.2.1 Flow data retention periods and data aggregation (page 94)".

- Target period

  Specify the start and end times of data to be output.

  It is possible to specify to output data after the end time of the previous output so as to output data periodically.

In addition to the data type, unit, and period, conditions to narrow down flow data to be output (filtering) and the CSV files output destination can be specified.

There are two methods of specifying the command parameters. One is to directly specify them as command arguments. The other is to describe the parameters in a configuration file. If the parameters are directly specified as command arguments, flow data of one type can be output by one command execution. If the parameter configuration file is used, flow data of multiple types can be output to CSV files by one command execution.

For detail of the output CSV file format, see "A.2.2 Output CSV file format (page 109)".

Path

<%installation directory%>/collector/bin/nfa_flow_export

Synopsis

```
nfa_flow_export -type DATATYPE -level { 1 | 2 | 3 | 4 | 5 | 6 }
    {-period START END | -continue} -out OUTDIR [OPTIONS...]
```

```
nfa_flow_export -file FILEPATH
```

```
nfa_flow_export -help
```

Arguments (when using command arguments)

-type *DATATYPE*

Specify a data type to be output. This cannot be omitted. The following data types can be specified:

- exporter *EXPORTER*[:*INTERFACE*]

  Outputs flow data of the specified exporter and its interfaces. Specify an exporter after `exporter` keyword. You can specify *":"* and interface after the exporter specification in order to output flow data for a specified interface only.

  Only one exporter and one interface can be specified. For specifying an exporter and interface, you can use an IP address, ifIndex value, and interface group name in addition to a display name. For details, see "Supplements for the value specification format (page 106)".

- traffic

  Outputs flow data of communication traffic of all exporters and their interfaces.

- ipaddr

  Outputs flow data from the aspect of IP addresses (communication endpoints) over the entire network.

- app

  Outputs flow data from the aspect of applications over the entire network.

- tos

  Outputs flow data from the aspect of ToS (DSCP) values over the entire network.

- ipprot

  Outputs flow data from the aspect of IP protocols over the entire network.

- as

  Outputs flow data from the aspect of AS numbers over the entire network.

-level { 1 | 2 | 3 | 4 | 5 | 6 }

Specify a level from 1 to 6 as the unit of data to be exported. This cannot be omitted.

For details about the correspondence between levels and data units, see "Relationship between the unit time of flow data and period (page 104)".

-period *START END*

Specify a period of flow data to be output. One of `-period` or `-continue` must be specified. Both cannot be specified at the same time.

Specify a start and end dates of the desired output period in the form of yyyymmdd or yyyymmddhhmm[ss].

Depending on the level specified by `-level`, a period between a start and end dates is limited. For details, see "Relationship between the unit time of flow data and period (page 104)".

-continue

Specify this option to output flow data from the last execution time of this command to the current time. One of `-continue` or `-period` must be specified. Both cannot be specified at the same time.

At the first execution on the output directory specified by `-out`, this command records only the execution time and does not output any flow data. Flow data will be output from the next time execution.

Depending on the level specified by `-level`, a period that one `-continue` execution can output is limited. For details, see "Relationship between the unit time of flow data and period (page 104)".

-out

Specify an output directory of CSV files. This cannot be omitted.

You can specify a directory as a relative or absolute path. You must create the specified directory before execution.

-filter *CONDITIONS*

Specify conditions for filtering flow data to be output. When conditions are set, only flow data that matches those conditions is output.

For details about how to specify filters, see "How to specify filter conditions (page 105)".

-full

Outputs detailed flow data. For details about the additional output information, see "A. 2.2 Output CSV file format (page 109)".

This option can be used when `exporter` is specified for `-type`.

-limit *N*

Specify the maximum number of flow data items to be output in one command execution. Flow data items are output in descending order of communication traffic volume in byte unit, and flow data items exceeding the specified limit are not output.

If this option is not specified, there is no limitation in the number of flow data items to be output.

-limit-by-packet

Changes the reference unit limited by `-limit` from byte to packet.

-line *N*

Specify the maximum number of lines to be output in one CSV file. If this option is not specified, the default value of 65,535 lines is used. You can specify it up to 1,048,575 lines.

When the number of flow data items exceeds the specified lines, output data is split in multiple CSV files. The file names of split CSV files end with a sequential number, such as _001.csv, _002.csv, etc.

-no-header

Prevents outputting the header field line in the first line of CSV files.

Arguments (when using a configuration file)

-file *FILE*

Specify a configuration file (parameter configuration file) in which the parameters of this command are described to run this command.

By using a parameter configuration file, you can output flow data of multiple targets by one command execution. If there are many targets, it is recommended to use a parameter configuration file.

For details of the parameter configuration file format, see "A.2.1 Parameter configuration file format (page 107)".

Arguments (others)

-help

Displays how to use this command.

Return values

Success: 0 is returned. Failure: A value other than 0 is returned.

Relationship between the unit time of flow data and period

Flow data is managed by splitting levels for each unit time. The ranges of a period that can be specified in `-period` are defined for each level. Similarly, the maximum output ranges at one `-continue` execution are defined for each level.

"Table A-1 Relationship between the unit time of flow data and period (page 104)" describes the range of period that can be specified for each level.

Table A-1 Relationship between the unit time of flow data and period

Level	Data unit time	Minimum period	Maximum period
1	1 minute	1 minute	60 minutes
2	10 minutes	10 minutes	12 hours
3	60 minutes	60 minutes	3 days
4	6 hours	6 hours	14 days
5	24 hours	24 hours	60 days
6	7 days	7 days	365 days

You must specify a period in `-period` within above ranges. For example, to get flow data with 60 minutes period (maximum for level 1) from 2017/4/1 10:00 in the level 1 data unit, you need to specify `-period 201704011000 201704011059`.

When using `-continue` to output flow data periodically, it is recommended to repeat this command at an interval of about half of the maximum period. In addition, if a long time that exceeds the maximum period has passed since the last execution, you can narrow an interval of the `-continue` execution in order to catch up the current time quickly.

Tip

When executing the command with `-continue` for a period in which flow data does not exist, no CSV file is output and the record of the last output time is only updated. Consider a situation in which the flow data retention period is the default and 30 hours have passed since the last execution for the level 1 data, for example. In this situation, when executing the command with `-continue`, no CSV file is output and the last output time is updated with the time indicating 29 hours ago (60 minutes after since 30 hours ago) because of exceeding the retention period. In this case, you can run the command with `-continue` repeatedly in order to catch up the current time quickly.

For details about the flow data retention period, see "5.2.1 Flow data retention periods and data aggregation (page 94)".

How to specify filter conditions

A filter condition is specified by a filter name and value joined with *"="*. No white space character is needed around *"="*.

The following filter conditions can be specified:

- exporter=*EXPORTER*[:*INTERFACE*][,*EXPORTER*[:*INTERFACE*]...]

  Filtering by the exporter. You can specify *":"* and interface after the exporter specification in order to filter the specific interface.

  For specifying an exporter and interface, you can use an IP address, ifIndex value, and interface group name in addition to a display name. For details, see "Supplements for the value specification format (page 106)".

  This can be used when `-type` is `traffic`, `ipaddr`, `app`, `ipprot`, `tos` or `as`.

- srcip=*IPADDR*[,*IPADDR*...]

  Filtering by the source IP address.

  This can be used when `-type` is `exporter` or `ipaddr`.

- dstip=*IPADDR*[,*IPADDR*...]

  Filtering by the destination IP address.

  This can be used when `-type` is `exporter` or `ipaddr`.

- srcendpt=*GROUP*[,*GROUP*...]

  Filtering by the source endpoint group name.

  This can be used when `-type` is `exporter` or `ipaddr`.

- dstendpt=*GROUP*[,*GROUP*...]

  Filtering by the destination endpoint group name.

  This can be used when `-type` is `exporter` or `ipaddr`.

- app=*APPLICATION*[,*APPLICATION*...]

  Filtering by the application name.

  This can be used when `-type` is `exporter` or `app`.

- ipprot=*PROTOCOL*[,*PROTOCOL*...]

  Filtering by the IP protocol. You can use IP protocol names or IP protocol numbers.

  This can be used when `-type` is `exporter` or `ipprot`.

- dscp=*DSCP*[,*DSCP*...]

  Filtering by the DSCP value (PHB). You can use DSCP value (6 digit binary number) or PHB.

  This can be used when `-type` is `exporter` or `tos`.

- srcas=*AS*[,*AS*...]

  Filtering by the source AS number.

  This can be used when `-type` is `exporter` or `as`.

- dstas=*AS*[,*AS*...]

  Filtering by the destination AS number.

  This can be used when `-type` is `exporter` or `as`.

For each filter condition, when specifying multiple values to filter by OR condition, specify them on the right of an equals sign, delimited by a comma. White space characters before and after the commands are not needed.

In addition, multiple filter conditions can be specified, in order to filter by AND condition, by delimiting with white spaces.

Supplements for the value specification format

- Exporter

  In this command, an exporter can be specified by a display name or IP address.

  A colon (:) is used as a delimiter between an exporter and interface, so if an exporter name contains a colon, you need to insert *"\"* before the colon as an escape character.

  ### Tip

  In shells such as bash, *"\"* on the command line may be treated as an escape character and may not recognize as a normal character. In this case, you can specify it correctly by enclosing the specified name with quote characters (' ' or " ").

  Example: The exporter name is Asystem:exporter1.

  ```
  # ./nfa_flow_export -type exporter 'Asystem\:exporter1:GBE0/1' ...
  ```

- Interface

  In this command, an interface can be specified by a display name, ifIndex, or interface group name.

  Like an exporter name, a colon (:) has a special meaning in an interface name, so if an interface name contains a colon, you need to insert *"\"* before the colon as an escape character.

- IP protocol

  IP protocol names and numbers that can be specified in this command are compliant with Protocol Numbers published by IANA. Uppercase and lowercase letters are distinguished in the specification of IP protocol names.

  http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml [*3]

- Filter condition value

  A comma is used as a delimiter when specifying multiple values on the right of an equals sign of a filter condition. If a value contains a comma, insert *"\"* before the comma as an escape character.

- Specifying values with white space characters from the command line

  When specifying a value that contains a white space character, such as an exporter name, interface name, and filter condition value, from the command line, the while space character is recognized as a delimiter of arguments and specified value is not recognized correctly.

  If a value contains a white space character, you need to enclose the entire value by quote characters (' ' or " ").

Notes

- To run this command, NFA service must be running. And, only root user can run this command.
- When specifying an exporter name, an error occurs in identifying an exporter if multiple exporters have this specified name. In this case, run this command by specifying an IP address of the exporter, or change the exporter display name.

  Similarly, when specifying an interface name, an error may occur in identifying an interface or interface group if multiple interfaces or interface groups on the same exporter have this specified name. In this case, run this command by specifying an ifIndex value or the interface, or change the interface or interface group display name.
- When specifying an interface group name that consists of only digits, an unexpected interface may be selected because the specified value cannot be distinguished from an interface ifIndex. Change the interface group name into one that contains non-digit characters beforehand.
- After running this command, nfa_flow_export.dat file is created in the directory specified by `-out`. This file has execution records such as an output target, last execution time, etc. If this file is deleted, periodically execution by `-continue` does not run correctly.

A.2.1 Parameter configuration file format

The following describes the parameter configuration file format used in `-file` option of `nfa_flow_export`.

File format

Create a configuration file according to the following rules:

- Create a parameter configuration file in UTF-8 encoding.
- Lines beginning with *"#"* are treated as comment lines.
- Configure settings in units of output data.

  Specify a setting name in square brackets [ ]. After this line, specify parameters that can be specified in the command line. A block of lines between square bracket lines is called as a section. A setting name of a section must be unique in the file.
- In a section, you can write settings that are equivalent to the command line arguments at one per line. A setting format is *`parameter name : value`*. For a parameter name, specify a name without *"-"* from the beginning of the name of command line argument. For a parameter value,

*3 This URL is current as of March 2017.

specify the same value as the command line one. For example, to specify the parameter that corresponding to `-type exporter` *exporter-name* on the command line, you need to write `type : exporter` *exporter-name* in the file.

To specify a parameter without a value in the command line arguments, such as `-continue` and `-full`, you need to write *"on"* as a value of it. The value *"on"* means its parameter is enabled. On the other hand, the value *"off"* means its parameter is disabled (not specified).

- The section named DEFAULT is treated as a special section.

  Settings described in the DEFAULT section are treated as default value in all other sections. For example, if you want to specify the same period on all sections, you can write `period` parameter in the DEFAULT section, and no need to write `period` parameter in any other sections.

  It should be noted that you cannot write `out` parameter in the DEFAULT section. Is must be written in each section.

Supplements for the value specification format

Values of parameters described in the file are basically same as ones of command line arguments. But there are following differences.

- Multiple filter conditions

  In the command line, to specify multiple filter conditions in `-filter` argument, you need to delimit the conditions by white space characters. But in the parameter configuration file, you need to delimit the conditions by line feed characters instead of white space characters. In addition, lines after line feed delimiters must start with white space characters. See "Configuration examples (page 108)" for examples.

- Specifying values with *"%"*

  To specify a value that contains *"%"* character, you must double it like *"%%"*.

- Specifying values with white space characters

  Unlike command line arguments, even if a value contains white space characters, you do not need to enclose it in quote characters.

In addition, as with the command line arguments, escaping is necessary when specifying a value that contains the following characters:

- If an exporter or interface name contains a colon (:), you need to insert *"\"* before the colon as an escape character.
- If a filter condition value contains a comma (,), insert *"\"* before the comma as an escape character.

Configuration examples

The following is an example of outputting flow data of level 1 (1 minute unit) for three exporters at a period of 30 minutes from 2017/4/1 10:00.

```
[DEFAULT]
period : 201704011000 201704011029
level : 1

[Router01]
type : exporter Router01
out : /csvdata/Router01/
```

```
[Router02]
type : exporter Router02
out : /csvdata/Router02/

[Router03]
type : exporter Router03
out : /csvdata/Router03/
```

The following is an example of outputting flow data periodically for one data type with different filter conditions.

```
[DEFAULT]
continue : on
level : 2
type : ipaddr

[src/dst address: Router01 (1)]
# Flows captured on Router01, destination is 192.168.0.10.
out : /csvdata/ipaddr-Router01-1/
filter : exporter=Router01
  dstip=192.168.0.10

[src/dst address: Router01 (2)]
# Flows captured on Router01, destination is 192.168.0.20.
out : /csvdata/ipaddr-Router01-2/
filter : exporter=Router01
  dstip=192.168.0.20

[src/dst address: Router02 GBE0/1]
# Flows captured on Gigabitethernet0/1 of Router02.
out : /csvdata/ipaddr-Router02-if01/
filter : exporter=Router02:Gigabitethernet0/1

[src/dst address: Router02 GBE0/2]
# Flows captured on Gigabitethernet0/2 of Router02.
out : /csvdata/ipaddr-Router02-if02/
filter : exporter=Router02:Gigabitethernet0/2
```

A.2.2 Output CSV file format

`The following describes the output CSV format of nfa_flow_export` command.

Output file name

Files to be output are named as follows:

<yyyymmddhhmmss>_<data type>_<sequential number>.csv

- *yyyymmddhhmmss*

  Indicates the date time when the command has started.

- *data type*

  Indicates the data type that is specified in `-type`.

  If `exporter` is specified as a data type, an exporter name is used as a part of file name instead of a data type name (exporter). If an interface is also specified, it is added after the exporter

name. Characters in an exporter and interface name that cannot be used as a file name are replaced with *"_"*.

- *sequential number*

  3-digit sequential number, starting from 001. When there is too many data in one command execution, it is output into multiple files such as 001, 002, 003.

Example: If the target is the interface "Gigabitethernet1/1" on the exporter "Router".

```
20170401100147_Router_Gigabitethernet1_1_001.csv
```

Output file format

The structure of output CSV files is as follows:

- The file encoding is UTF-8.
- There is a header fields line at the first line.

  When `-no-header` option is specified, the header fields line is omitted and flow data is output from the first line.
- Flow data is output from the second line. It is output in ascending order of date and time.

The all output columns is listed in "Table A-2 Column list in CSV file (page 110)". The output columns vary depending on the data type. The relationship between the data type and output columns is shown in "Table A-3 Output columns for each data type (page 111)".

Table A-2 Column list in CSV file

Column name	Description
DATE	Indicates the date and time when NFA receives the flow. Received time is truncated by the granularity (unit time) of data.
EXPORTER	Indicates the exporter name where the flow was detected. It corresponds to the filter condition *"exporter"*.
BYTES	Indicates communication traffic volume of the flow (number of octets).
PKTS	Indicates the number of communication packets.
PROTOCOL	Indicates the IP protocol name. For unknown protocols, an IP protocol number is output instead of a name. It corresponds to the filter condition *"ipprot"*.
TOS	Indicates the TOS (Type Of Service) field value. It is output in decimal notation.
TCP_FLAGS	Indicates the OR of the control flags in TCP header. The logical OR of flags that are ON is output in hexadecimal notation. The value of flags are: FIN=0x01, SYN=0x02, RST=0x04, PSH=0x08, ACK=0x10, URG=0x20, ECE=0x40, CWR=0x80, NS=0x0100
L4_SRC_PORT	Indicates the source port number.
IPV4_SRC_ADDR	Indicates the source IPv4 address. It corresponds to the filter condition *"srcip"*.
SRC_MASK	Indicates the subnet mask of the source IPv4 address.
INPUT_IF	Indicates the input interface name on the exporter. If it matches the interface group, the interface group name is output instead. It corresponds to the filter condition *"exporter"* with interface.

Column name	Description
L4_DST_PORT	Indicates the destination port number.
IPV4_DST_ADDR	Indicates the destination IPv4 address. It corresponds to the filter condition *"dstip"*.
DST_MASK	Indicates the subnet mask of the destination IPv4 address.
OUTPUT_IF	Indicates the output interface name on the exporter. If it matches the interface group, the interface group name is output instead. It corresponds to the filter condition *"exporter"*with interface.
IPV4_NEXT_HOP	Indicates the IPv4 address of the next hop router.
SRC_AS	Indicates the source AS number. It corresponds to the filter condition *"srcas"*.
DST_AS	Indicates the destination AS number. It corresponds to the filter condition *"dstas"*.
FRAMETYPE	Indicates the name of Ethernet frame type. It is output as one of *"Ethernet 2"*, *"IEEE802.3 SNAP"*, *"IEEE802.3 RAW"*, and *"IEEE802.3 LLC"*.
ETHERTYPE	Indicates the value of Ethernet frame type. It is output in hexadecimal notation.
VLAN_TAG	Indicates the VLAN ID.
APP	Indicates the application name of the flow. It corresponds to the filter condition *"app"*.
SRC_ENDPOINT_GROUP	Indicates the source endpoint group name. It corresponds to the filter condition *"srcendpt"*.
DST_ENDPOINT_GROUP	Indicates the destination endpoint group name. It corresponds to the filter condition *"dstendpt"*.
SRC_HOSTNAME	Indicates the FQDN corresponding to the source IPv4 address.
DST_HOSTNAME	Indicates the FQDN corresponding to the destination IPv4 address.
DSCP	Indicates the DSCP value (PHB) of the flow. If the corresponding PHB does not have a value, output it as a 6 digit binary number.

Tip

NFA aggregates flow data that exceed the maximum number of flows to be stored per unit time as *"other"* flow. In output CSV files, columns of *"other"* flows are all empty except of DATE, BYTES, and PKTS, and these are output at the last in the unit time.

For details of flow data aggregation, see also "5.2.1 Flow data retention periods and data aggregation (page 94)".

Table A-3 Output columns for each data type

Column name	exporter	exporter (-full)	traffic	app	ipaddr	ipprot	as	tos
DATE	Y	Y	Y	Y	Y	Y	Y	Y
EXPORTER			Y	Y	Y	Y	Y	Y
BYTES	Y	Y	Y	Y	Y	Y	Y	Y

Column name	exporter	exporter (-full)	traffic	app	ipaddr	ipprot	as	tos
PKTS	Y	Y	Y	Y	Y	Y	Y	Y
PROTOCOL	Y	Y				Y		
TOS	Y	Y						Y
TCP_FLAGS		Y						
L4_SRC_PORT	Y	Y						
IPV4_SRC_ADDR	Y	Y			Y			
SRC_MASK		Y						
INPUT_IF	Y	Y	Y	Y	Y	Y	Y	Y
L4_DST_PORT	Y	Y						
IPV4_DST_ADDR	Y	Y			Y			
DST_MASK		Y						
OUTPUT_IF	Y	Y	Y	Y	Y	Y	Y	Y
IPV4_NEXT_HOP		Y						
SRC_AS	Y	Y					Y	
DST_AS	Y	Y					Y	
FRAMETYPE		Y						
ETHERTYPE		Y						
VLAN_TAG		Y						
APP	Y	Y		Y				
SRC_ENDPOINT_GROUP	Y	Y			Y			
DST_ENDPOINT_GROUP	Y	Y			Y			
SRC_HOSTNAME		Y			Y			
DST_HOSTNAME		Y			Y			
DSCP	Y	Y						Y

A.2.3 Usage examples

The following describes the usage examples of `nfa_flow_export`.

Output flow data by specifying the exporter and the period

To output the detailed flow data of 60 minutes unit for the exporter "Router01" including all interfaces from 2017/4/1 to 4/2 (2 days), run the following commands.

```
# mkdir -p /nfa-csv
# /opt/nec/nfa/collector/bin/nfa_flow_export -type exporter Router01
    -period 20170401 20170402 -level 3 -full -out /nfa-csv/
```

A CSV file is created in /nfa-csv directory after finishing the command.

Output flow data of the entire network periodically

As the entire network flow data, the following types of data can be output: communication traffic of exporters, source and destination IP address, application, IP protocol, ToS (DSCP), source and destination AS number. To output them as 1 minute unit data periodically, create the following file first.

```
[DEFAULT]
continue : on
level : 1

[Traffic]
type : traffic
out : /nfa-csv/traffic

[Endpoint IP Address]
type : ipaddr
out : /nfa-csv/ipaddr

[Application]
type : app
out : /nfa-csv/app

[IP protocol]
type : ipprot
out : /nfa-csv/ipprot

[DSCP]
type : tos
out : /nfa-csv/dscp

[AS number]
type : as
out : /nfa-csv/as
```

Save the created file as /nfa-csv/flowexport.conf.

Next, create directories that are specified as `out` parameters.

```
# mkdir /nfa-csv
# cd /nfa-csv
# mkdir traffic app ipaddr ipprot dscp as
```

After preparation, configure cron, etc. to run `nfa_flow_export` periodically.

The following is an example of the setting to run the command every 30 minutes using cron.

```
0,30 * * * *    /opt/nec/nfa/collector/bin/nfa_flow_export
    -file /nfa-csv/flowexport.conf
```

CSV files are created in the subdirectories under /nfa-csv at every 30 minutes.

For details about cron, see the manual of the OS in use.

Tip

`nfa_flow_export` command does not manage the output CSV files. It is necessary to manage output CSV files so as not to put pressure on the disk capacity by periodically moving them to an external server or somewhere else.

Output flow data continuously from the past to the current

For the purpose of network delay investigation, for example, you can export flow data continuously from the past to the current time.

The following is an example of outputting flow data of 1 minute unit from 2017/4/1 0:00 to 2017/4/1 10:00 (current).

1. At the first execution, use `-period` to output 60 minutes data.

```
# mkdir /nfa-csv
# /opt/nec/nfa/collector/bin/nfa_flow_export -type exporter Router01
    -period 201704010000 201704010059 -level 1 -full -out /nfa-csv/
```

2. Run the second time without leaving a time from the first run. In the second run, use `-continue` instead of `-period` to output flow data continuously from the last run.

```
# /opt/nec/nfa/collector/bin/nfa_flow_export -type exporter Router01
    -continue -level 1 -full -out /nfa-csv/
```

   After the second run, 60 minutes flow data from 2017/4/1 1:00 was output.

3. Run the command with `-continue` repeatedly until catching up the current time.

   One command run outputs 60 minutes flow data.

Tip

After catching up the current time, you can configure cron, etc. to continue to output flow data periodically.

Appendix B. Troubleshooting

The following describes the problems that might occur while using NFA and the suggested actions to take to resolve those problems.

B.1 Connection to the web console cannot be established.

Event

Attempted to connect to the web console by specifying the given URL, but failed.

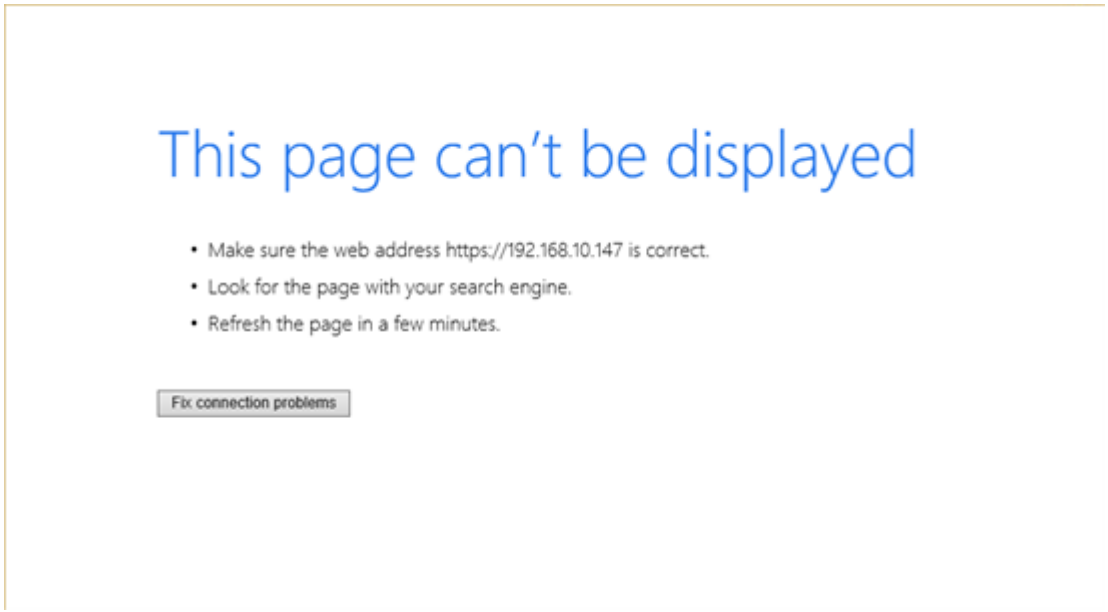

Figure B-1 Screenshot

Cause

The NFA service might not be started on the NFA server.

Action

Restart the NFA service. For the procedure, see "5.1.2 Starting or stopping the service (page 85)".

B.2 No charts are displayed in the widgets on the Dashboard page.

Event

For all widgets that should display charts on the Dashboard page, the messages `Failed to get data` and `There is no data` are displayed and no charts are displayed.

Figure B-2 Screenshot

Cause 1

The flow collector might not be running on the NFA server.

Action 1

Restart the NFA service. For the procedure, see "5.1.2 Starting or stopping the service (page 85)".

Cause 2

The accumulated flow data cannot be referenced correctly because there is a significant discrepancy between the time of the client machine on which the web console is running and the NFA server time.

Action 2

Adjust the time between the client machine on which the web console is running and the NFA server.

B.3 Failed to specify the settings of this product.

Event

Attempted to specify the settings, but failed with the message `Failed` displayed.

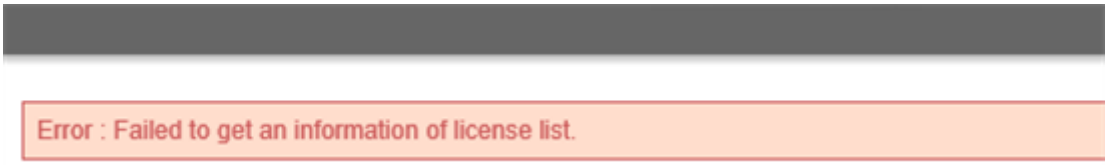

Figure B-3 Screenshot

Cause

A part (some service processes) of the service might not be running on the NFA server.

Action

Restart the NFA service. For the procedure, see "5.1.2 Starting or stopping the service (page 85)".

B.4 An exporter that was deleted is restored for some reason.

Event

Even though an exporter was deleted, the relevant exporter is registered again when a flow is received from that exporter.

Cause

The automatic registration function might be enabled.

In this case, even though an exporter was deleted, the relevant exporter is registered again when a flow is received from that exporter.

Action

Take either of the following actions:

- Disable the flow sending setting of the exporter.
- Disable the automatic exporter registration function of NFA.

  For the procedure, see "2.2.1 Setting the registration policy of the exporter information (page 25)".

B.5 The host name is not displayed in a widget.

Event

The host name is not displayed until at least five minutes after reception of the flow has started.

Cause

It might take five minutes or more to show a host name because name resolution is performed to obtain the host name so that an excessive load is not applied to the DNS server. Therefore, there is no problem because this is a normal operation according to the specifications.

Action

None

If you want to check that the DNS server setting is correct, run `nslookup` or `ping` command, etc. on the flow collector machine to check whether the host name can be obtained.

The following is an example of running `nslookup` command.

```
$ nslookup 192.168.10.100
```

B.6 The layout of the web console does not display correctly.

Event

The layout of the web console does not display correctly.

Cause

The web browser in use might not be supported by this product; for example, Internet Explorer 8.

Action

Use a web browser that is supported by NFA.

- Internet Explorer 11
- Mozilla Firefox 60 or later
- Google Chrome 71 or later

B.7 `"Page has expired, or the request is invalid"` is displayed.

Event

When attempting to change the settings or performing other operations, `"Page has expired, or the request is invalid"` is displayed.

Cause

Other settings might be being specified on another page.

Action

When configuring settings, be sure not to perform multiple operations on NFA at the same time.

Appendix C. System Resources Used in This Product

The following describes the system resources used by this product.

C.1 Port numbers used in this product

The following describes the default port numbers used by this product.

The port numbers that NFA uses for external and internal communications are listed in "Table C-1 Communication port numbers that NFA uses for external communication (page 119)" and "Table C-2 Communication port numbers that NFA uses for internal communication (page 119)".

Table C-1 Communication port numbers that NFA uses for external communication

Name	Port Number	Protocol	Direction	Purpose
HTTPS communication port	443	TCP	IN	This is an HTTPS communication port.
sFlow packet reception port	6343	UDP	IN	This is an sFlow packet reception port.
NetFlow packet reception port	9995	UDP	IN	This is a NetFlow packet reception port.

Table C-2 Communication port numbers that NFA uses for internal communication

Name	Port Number	Protocol	Direction	Purpose
Flow database communication port	27100	TCP	IN	This is a communication port for a flow database.
System database communication port	27110	TCP	IN	This is a communication port for a system configuration management database.
Event database communication port	27120	TCP	IN	This is a communication port for an event database.
Controller control communication port	27200	TCP	IN	This is a communication port for controller process control.
Collector log service communication port	27210	UDP	IN	This is a communication port for a log service of a collector process.

These port numbers can be changed. For the procedure to change the port number to use, see "5.1.3 Changing the port number used in this product (page 86)".

Appendix D. Linking with Other Systems

The following describes the procedure to link NFA with other systems.

D.1 Linking with UNIVERGE PF6800 Web GUI

The following describes the procedure to connect the Web GUI of UNIVERGE PF6800 (hereafter referred to as "PFC") to the NFA web console without login authentication.

This setting permits users to seamlessly operate NFA from the PFC Web GUI.

Tip

- The PFC version that can be linked with NFA is 6.1 or later.
- In addition to the following settings on NFA, you need to make linking settings on PFC.
  For the PFC setting procedure, see the *"Web GUI User's manual"* provided with PFC.

1. Stop the NFA service.

```
# /etc/init.d/nec-nfa-service stop
```

2. Edit the following configuration file. If no configuration file exists, create a configuration file.

   <%data directory%>/controller/conf/sso.properties

   The synopsis of the configuration file is as follows:

```
sso.ipaddr.n = <IPv4 address of PFC>
sso.username.n = <user name>
```

   - *n*

     Specify a serial number starting from 1. You can specify multiple IP addresses and user names by increasing this number.

   - *<IPv4 address of PFC>*

     Specify the IPv4 address set to the PFC operations management NIC (such as eth0).

   - *<user name>*

     Specify the name of the NFA user who logs in to NFA.

     If the user specified for *<user name>* is not registered to NFA, connection to NFA cannot be established. However, connection is established as the admin user in the following cases:

     - No *<user name>* is specified
     - *"sso.username.n = "* is omitted

3. Start the NFA service.

```
# /etc/init.d/nec-nfa-service start
```

Configuration example:

The following is an example of a configuration to log in to NFA as user *"PFC_User"* in a system in which PFC1 (192.168.10.1) and PFC2 (192.168.10.2) have a redundant configuration.

```
sso.ipaddr.1 = 192.168.10.1
sso.username.1 = PFC_User
sso.ipaddr.2 = 192.168.10.2
sso.username.2 = PFC_User
```

Glossary

A - Z

A

AS

AS stands for autonomous system. This is an RFC 1930 compliant autonomous network that is owned and operated by an organization within a large-scale TCP/IP network, such as the Internet.

An AS number is used to identify this autonomous network. AS numbers are managed by the Network Information Center (NIC) of each country.

C

Conversation

For NFA, this means a mutual communication between two specific points.

D

DNS

DNS stands for domain name system. This is a system that manages the mapping between host names or domain names on a network and IP addresses.

DSCP

DSCP stands for Differentiated Services Code Point. This is a method to prioritize packets. DSCP uses 6 bits of the ToS field (8 bits) in the IP header. This makes it possible to prioritize in 64 levels.

E

Endpoint

This is a generic name for network terminals such as personal computers that connect to a network and perform various types of communication. For NFA, not only clients but also servers are referred to as endpoints.

Endpoint Group Name

This is a grouping function that is used to accumulate and analyze the flows of multiple source addresses and destination addresses that are the endpoints of communication.

An endpoint group is considered to be used to analyze the flows of each department by grouping the IP addresses of the relevant department.

Exporter

For NFA, this is a generic name for devices such as switches and routers, and software, that can send packets in a flow (sFlow, NetFlow, IPFIX).

F

Flow

This indicates a communication flow between endpoints, or information (sFlow, NetFlow, IPFIX) generated by monitoring this communication flow by an exporter.

FQDN

FQDN stands for fully qualified domain name. This is a full domain name that includes the domain name, subdomain names, and host name.

I

IANA

IANA stands for Internet Assigned Numbers Authority. This is an organization that manages various numbers related to the Internet, such as IP addresses, protocol numbers, port numbers.

ifIndex

This is one of the most frequently used identifiers in SNMP network management and indicates a unique identification number that is associated with a physical or logical interface.

NFA uses the ifIndex value to identify the interface of flow information.

ifName

This is the name of the MIB object to which the name of the physical or logical interface of a device is recorded.

interface group

This is a grouping function that is used to tally and analyze flows that run across multiple interfaces.

The interface group function is used to group multiple interfaces in a link aggregation (LAG) configuration and analyze the flow viewing them as a single LAG interface.

IP protocol

For NFA, this refers to the protocol that is indicated by the protocol number (IP Protocol Number) in the IP header. In particular, this is a generic name for TCP, UDP, and ICMP.

IPFIX

IPFIX stands for IP Flow Information Export. This is a technology used to monitor the network communication status. This is an expanded IETF standard technology based on NetFlow version 9.

L

LAG

LAG means link aggregation groups. This technology treats multiple physical interfaces as one interface by virtually bundling them. LAG is defined by IEEE P802.3ad.

M

MIB

MIB stands for management information base. This is management information that is issued externally by a network device that can be managed by SNMP to report its own state. The MIB information can be referenced externally by specifying the target object name by using SNMP.

N

NetFlow

This technology has been developed by Cisco Systems, Inc. in the United States to monitor the communication status of a network. The specifications of version 9 have been published as RFC3954.

NetFlow targets only IP-based communication information, and offers two communication packet monitoring methods: full mode and sampling mode.

NFA

This is an abbreviation of MasterScope Network Flow Analyzer.

P

PHB

PHB stands for Per Hop Behavior. This indicates the packet forwarding behavior corresponding to the DSCP value.

Port number

This is a number to identify the communication destination program in TCP/IP communication.

S

sFlow

This technology was developed by InMon Corp. in the United States to monitor the communication status of a network. The specifications of version 4 were published as RFC3176.

sFlow offers a mechanism to sample communication packets in a specific ratio and calculate the total communication traffic by analyzing the sampled information statistically.

NFA samples communication packets on a switch or router, receives the generated information (sFlow packets), and calculates the communication traffic by analyzing the information statistically.

SNMP

This stands for Simple Network Management Protocol. This is a protocol for network management, and is defined by RFC1157.

SNMP enables network devices connected to a TCP/IP network to be monitored and managed via the network.

For NFA, SNMP v1 or v2c is used to obtain exporter names and interface information.

SNMP trap

This is a mechanism provided by SNMP to enable an agent to report its own status by way of an unsolicited message.

For NFA, SNMP traps are used to enable external reporting of events detected by threshold monitoring.

sysName

This is the name of the MIB object in which a device host name is recorded. The sysName value can be set in the device configuration.

T

ToS

ToS stands for Type of Service. It is one of the fields in IP header and is used to tell each packet forwarding device how to forward the packet.

W

Widget

This is a component of the Dashboard and Exporter Analysis page. Charts and lists are displayed as widgets.

MasterScope
Network Flow Analyzer 2.0
Reference Manual

NFA00ME0200-01

February, 2019 01 Edition

NEC Corporation