

***MasterScope***

# Network Flow Analyzer

NEC Corporation  
Cloud Platform Division  
March 2019



# **Orchestrating** a brighter world

NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow.

We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.

# Contents

- Product Overview
- Functions and Features
- Sales Information

# What is MasterScope?

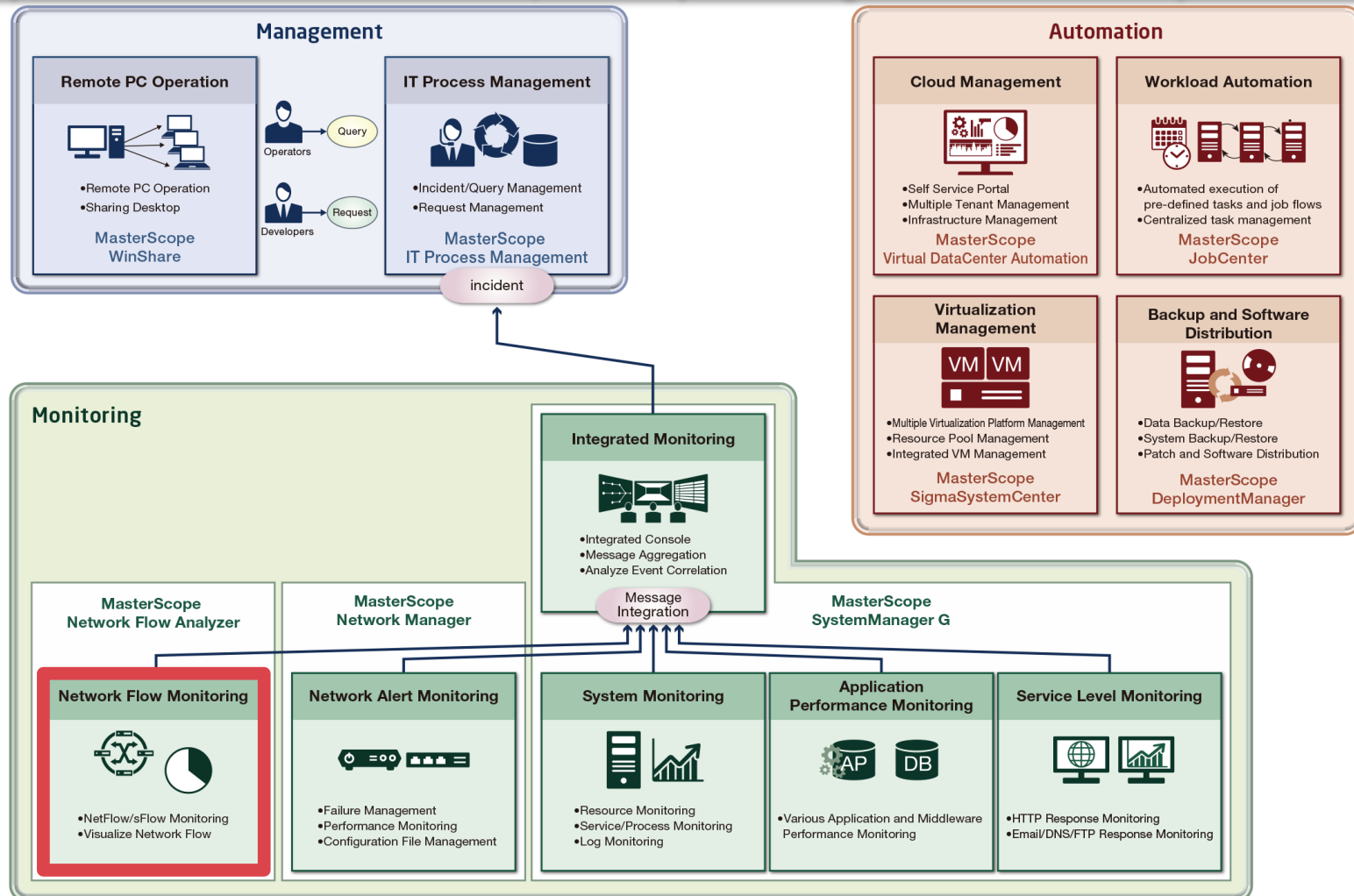
MasterScope is NEC's integrated operations management software brand that leverages the expertise and advanced technologies cultivated by NEC over many years. NEC delivers more than 3,000 MasterScope systems to customers annually.

MasterScope provides end-to-end support for systems encompassing ICT infrastructure to applications, and meets our customers' needs for easy-to-operate products.



# Positioning of Network Flow Analyzer in the MasterScope Series

Network Flow Analyzer 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.



# Network Traffic Monitoring Challenges

NetFlow/sFlow solves challenges of network traffic monitoring via SNMP!

## Increasing traffic, complicated networks

- Advance of interoffice network
- Rapid growth of Cloud Computing

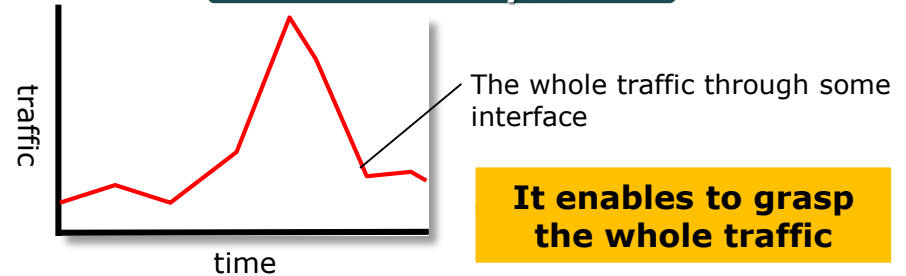
## Request for more detailed traffic analysis than SNMP can provide

- What kind of application traffic is there ?
- Who is accessing WAN ? How much traffic on WAN?
- What kind and how much traffic is being generated by Whom?



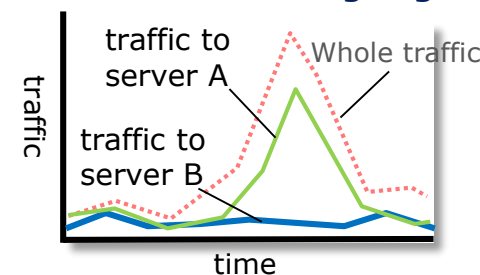
**Visualization of application traffic (based TCP/IP) by NetFlow/sFlow**

### SNMP analysis

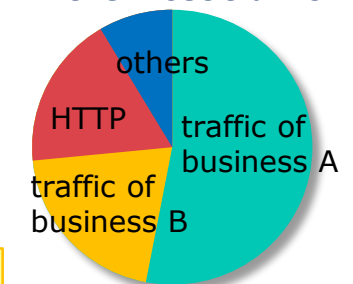


### NetFlow/sFlow analysis

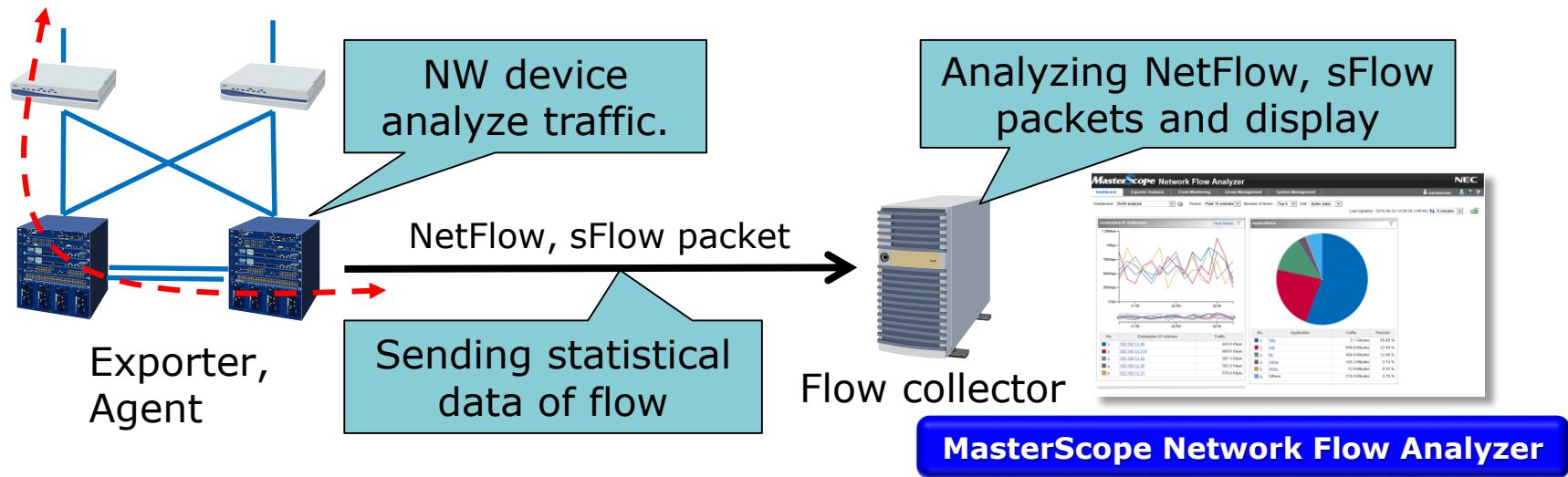
#### Where is the traffic going?



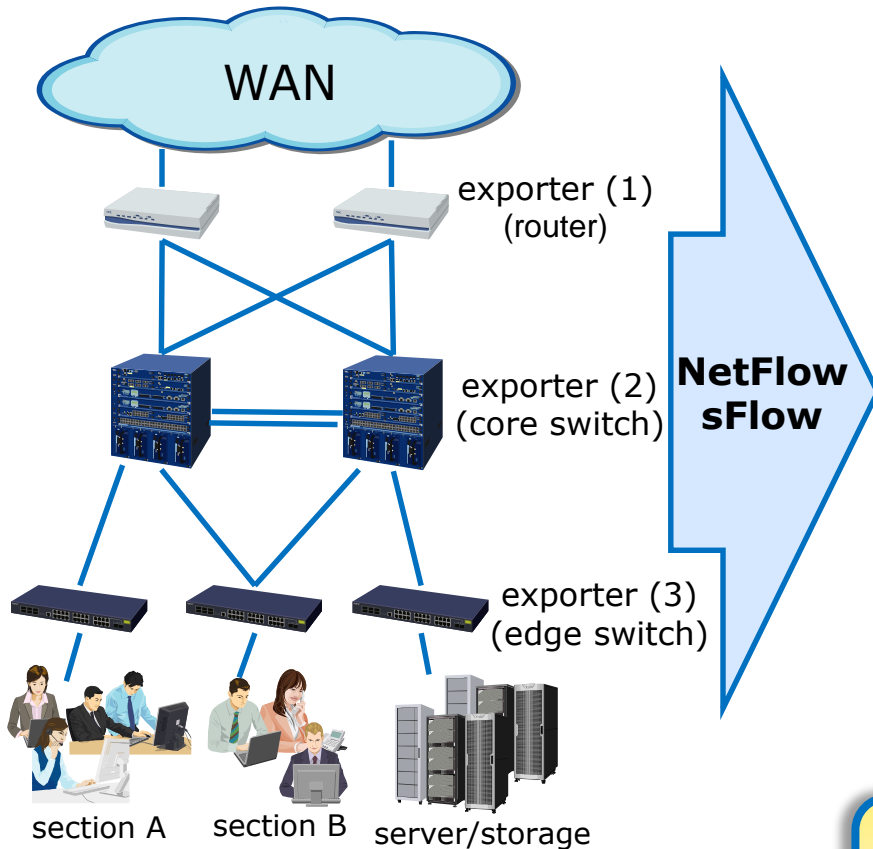
#### Which application has the most traffic?



**The protocol to visualize details of traffic.  
(Destination/Source, Protocol/Application, etc.)**



**The details of the traffic which couldn't be seen by SNMP are visualized by NetFlow/sFlow.**



exporter :  
The device or the software which sends flow data of the NetFlow/sFlow.

## Examples of analysis

- (1) - Analyze factors affecting WAN performance.  
- Check internet usage.
- (2) - Investigate the effect on new system deployment and network configuration change.  
- Manage the traffic between departments.  
(Trend analysis)
- (3) - Analyze the traffic for optimal placement of virtual machines.  
- Investigate the cause of delayed response of the transaction processing system.

**The traffic is analyzed from the various angles and stable network operation is supported.**



## Visualize application and traffic, and solve network administrator's problems!

### Main function

#### 1. Visualize application and traffic

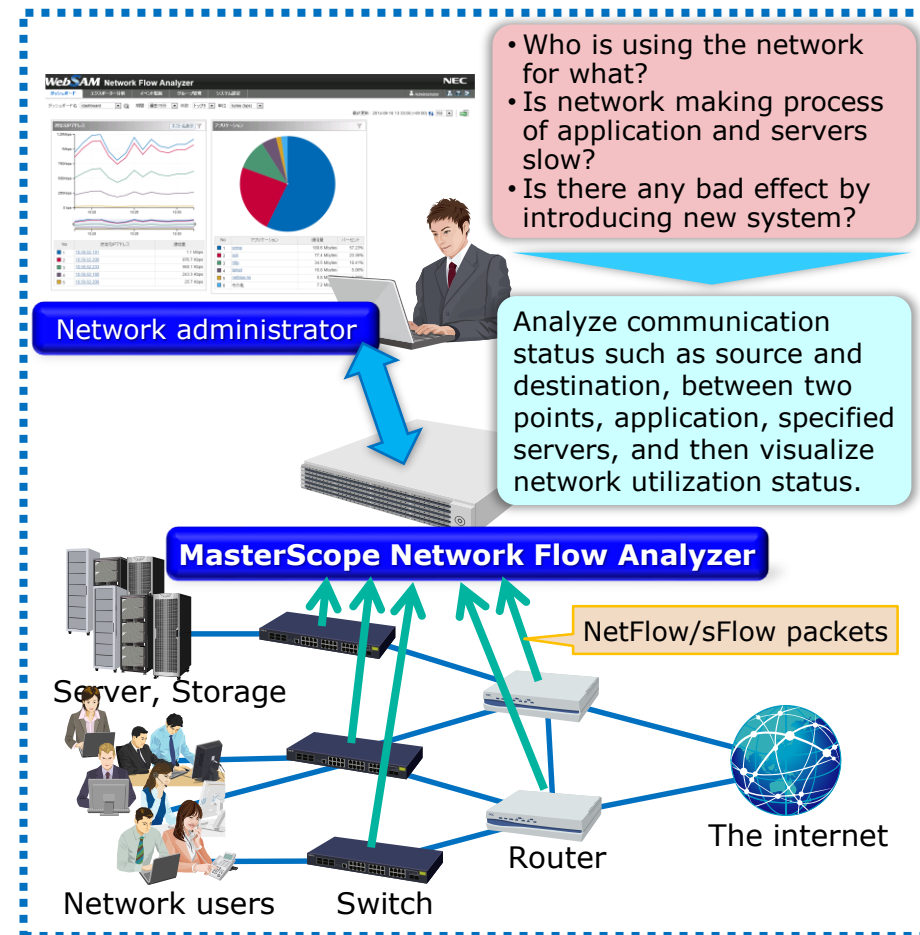
- Realize capacity planning and make failure investigation efficient by visualizing traffic of application or traffic between servers and clients using NetFlow/sFlow analysis.

#### 2. Provide flexible dashboards

- Enable to confirm required information by locating graphs, etc. freely and drill down for detail information from dashboard.

#### 3. Realize user-friendly visibility

- Display by division unit, service, or application name such as YouTube, etc.



# Features of MasterScope Network Flow Analyzer

## Various Analysis

Analyzing traffic by various conditions is enabled.  
(IP address, Application, etc.)

## Easy Operation

GUI is web-based and easy to operate.  
Monitoring can be started quickly because default monitoring setting is included.

## High Performance

20,000 flow data/sec can be analyzed. It can be used in heavy traffic environment.

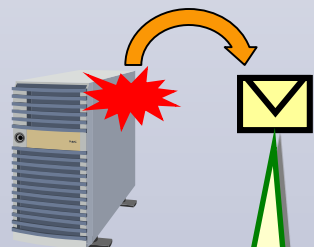
## Starting Small Environment

Minimum monitoring target is 20 interfaces.  
It can be expanded to 1,000 interfaces with upgrade license.

# Operations with MasterScope Network Flow Analyzer

## Detecting a failure

Traffic is slow...



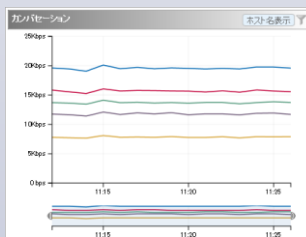
MasterScope  
Network Manager

Traffic has  
exceeded the  
threshold.

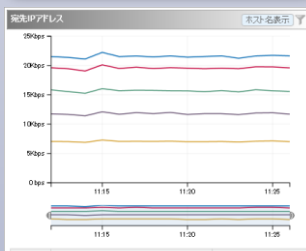
## Confirming status (Dashboard)



WAN traffic

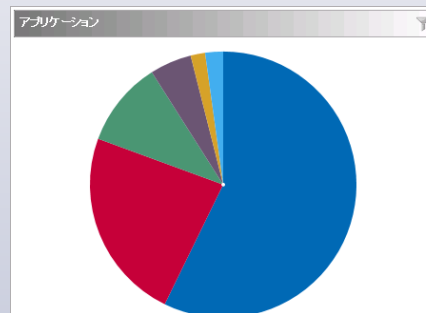


Traffic between  
departments



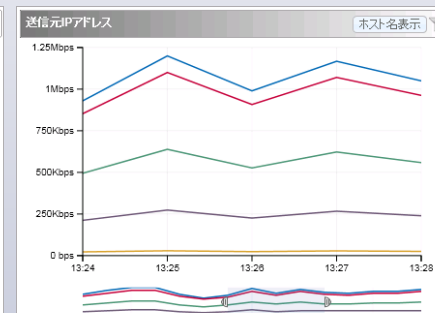
Traffic of  
specified servers

## Analyzing communication content (Analyzing exporter)



No	アプリケーション	通信量	パーセント
1	snmp	189.6 Mbytes	57.23%
2	ssh	77.4 Mbytes	23.36%
3	http	34.5 Mbytes	10.41%
4	telnet	16.8 Mbytes	5.06%
5	netbios-ns	5.8 Mbytes	1.76%
6	その他	7.2 Mbytes	2.17%

Application traffic



No	送信元IPアドレス	通信量
1	10.58.82.191	1.1 Mbps
2	10.58.82.200	978.4 Kbps
3	10.58.82.233	568.1 Kbps
4	10.58.82.180	243.3 Kbps
5	10.58.82.208	25.9 Kbps

Source IP traffic

If abnormality is found while checking traffic of each viewpoint on dashboard, administrator can analyze its root cause from detail information of source IP, application, etc. by exporter unit.

# MasterScope Network Flow Analyzer

## Functions and Features

# Function List

Function	Summary
Dashboard	<ul style="list-style-type: none"><li>- The current state of the responsible area is indicated by a chart and an alert list.</li><li>- Outputs result of the analysis in CSV.</li><li>- The analysis contents and arrangement of a chart and a current alert list can be customized freely.</li></ul>
Analyzing exporter	<ul style="list-style-type: none"><li>- The traffic flow which goes through exporter and the specific interface is analyzed.</li><li>- Specifying destination/source IP addresses and application/protocol names narrows down target data and Top N is displayed.</li><li>- The traffic status during the specified period is displayed.</li><li>- Outputs result of the analysis in CSV.</li></ul>
Setting application definition	<ul style="list-style-type: none"><li>- Enable an application definition by combination of destination/source IP addresses and service port number. Example: 80 TCP port for 10.10.10.1 is "business application" and for other addresses is "http."</li></ul>
Grouping	<ul style="list-style-type: none"><li>- Grouping endpoints enables analyzing for the organization/sections.</li><li>- Grouping interfaces enables analyzing for LAG interfaces.</li></ul>
Threshold monitoring	<ul style="list-style-type: none"><li>- Enables threshold monitoring with application/protocol, destination/source IP addresses, and AS.</li><li>- Enables SNMP trap notification of threshold value excess events.</li></ul>
Exporting flow data	<ul style="list-style-type: none"><li>- Enables long-term storage of accumulated flow data as external files (CSV) without deteriorating data granularity.</li></ul>

## Easy installation and analysis .

Install MasterScope  
Network Flow Analyzer

Setting NetFlow/sFlow  
to a flow exporter

Monitoring starts by  
the default setting

- Top 10 of the traffic in each exporter
  - Application, IP protocol, Conversation, Source IP, Destination IP
- Current Alert



## Selectable widget type and customizable arrangement

Selecting indicate widget

**Add Widgets**

Select widgets added to the dashboard.

**Exporter Analysis :**

- ☐ Top N Exporters
- ☐ Top N IN Interfaces
- ☐ Top N OUT Interfaces

**Communication Content Analysis :**

- ☐ Top N Applications
- ☐ Top N IP Protocols

**Endpoint Analysis :**

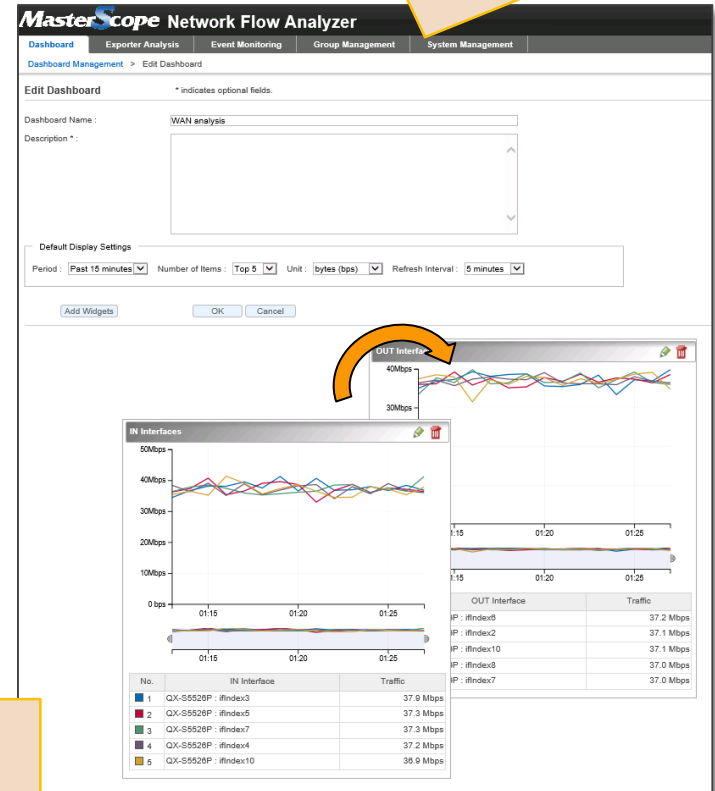
- ☐ Top N Source IP Addresses
- ☐ Top N Destination IP Addresses
- ☐ Top N Conversations
- ☐ Top N Source Endpoint Groups
- ☐ Top N Destination Endpoint Groups
- ☐ Top N Source AS
- ☐ Top N Destination AS

**Others :**

- ☐ Current Alerts

OK Cancel

Widgets are arranged by free order.

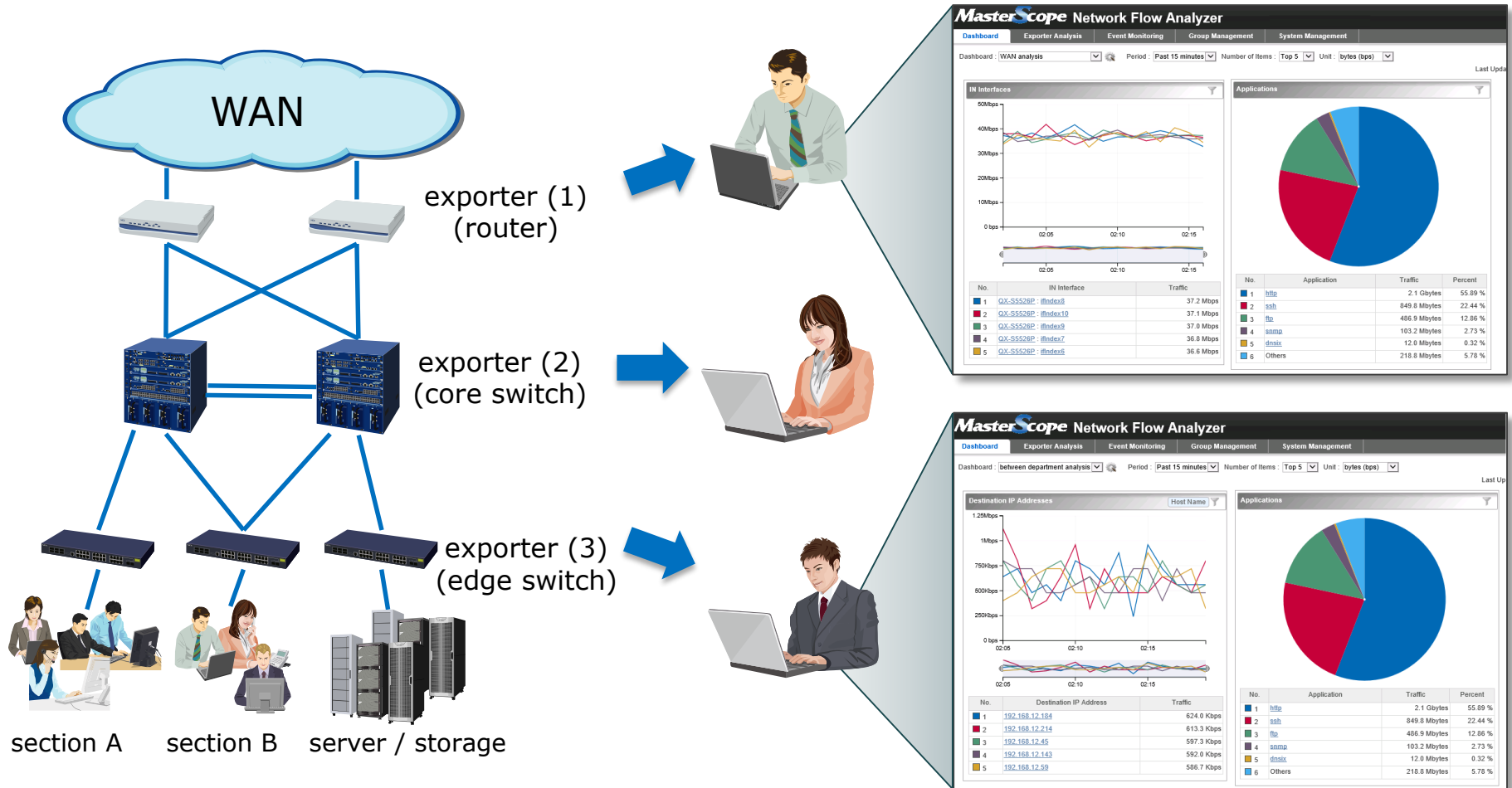


Dashboard : WAN analysis between department analysis built-in dashboard

Dashboard definitions can be created and selected.

# Dashboard for Each User

Each user can customize a dashboard according to their needs.





# In-Depth Analysis for Each Exporter

**Traffic flow can be analyzed for each exporter from various point of views.**

**Traffic**  
(in/out interface)

Which is a high load interface ?



**in-depth analysis**

**IP protocol**

Which protocol is having high traffic ?

**Application**

Which application is having high traffic ?

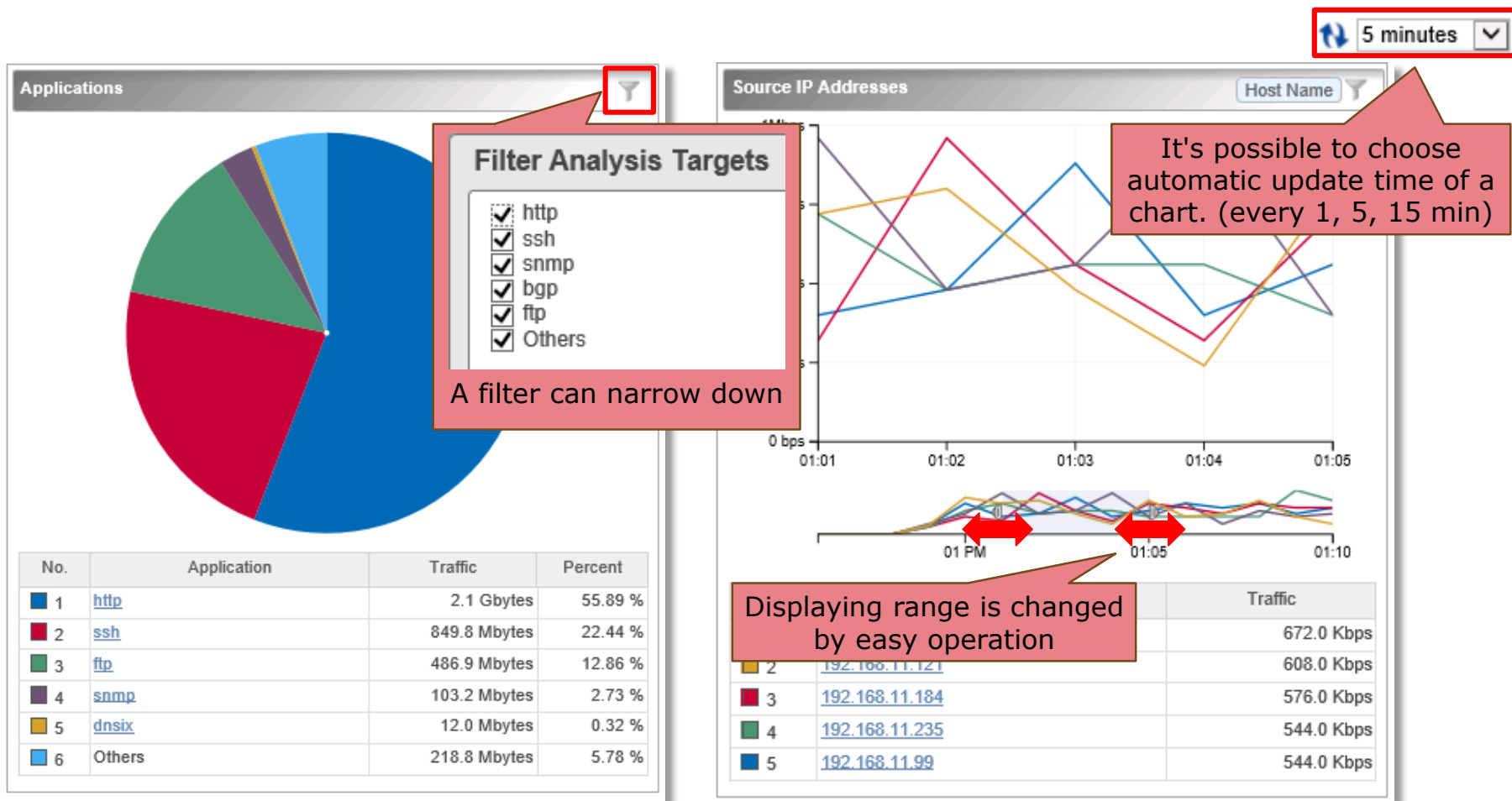
**Destination IP/  
Source IP**

Where data is being sent to?  
Where data is being received from ?

**Conversation**

Who is having heavy traffic/communication with whom?

# Graphs

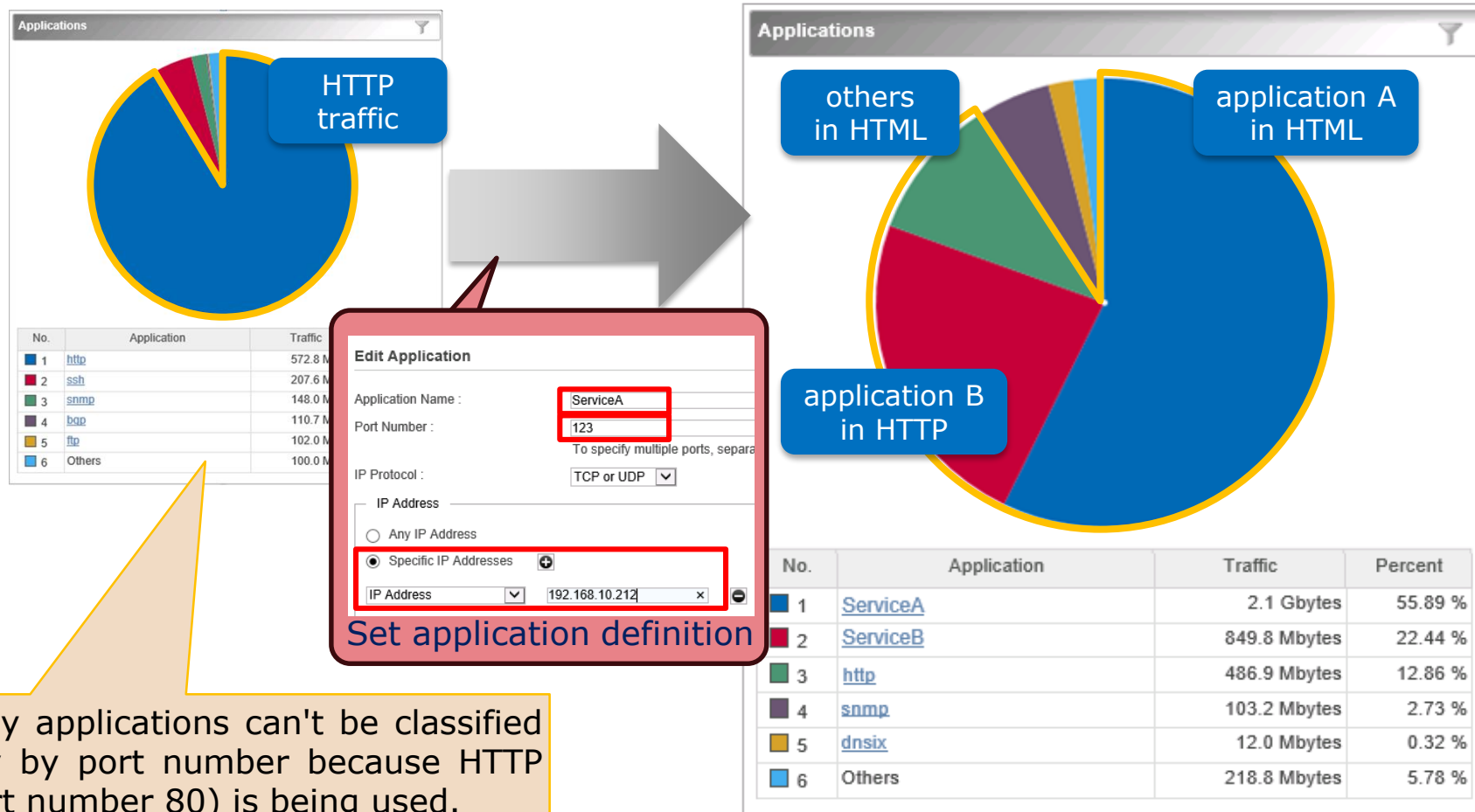


**pie graph**  
(IP protocol, Application)

**line graph**  
(Traffic, Destination/Source IP, Conversation)

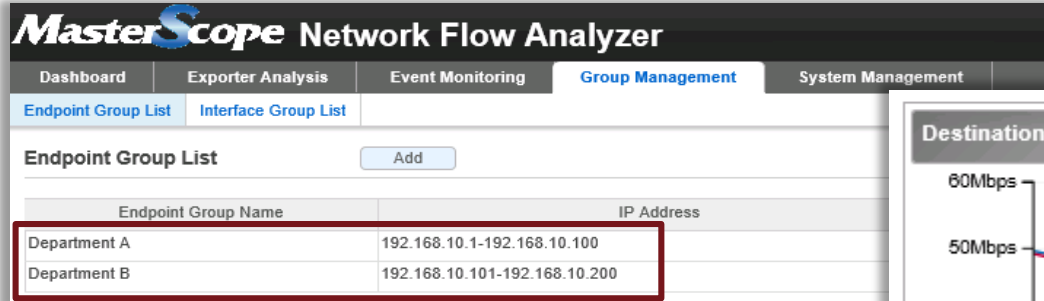
# Analyzing Traffic of Internal Business Application

**Setting destination/source IP address and port number can classify more detailed application.**



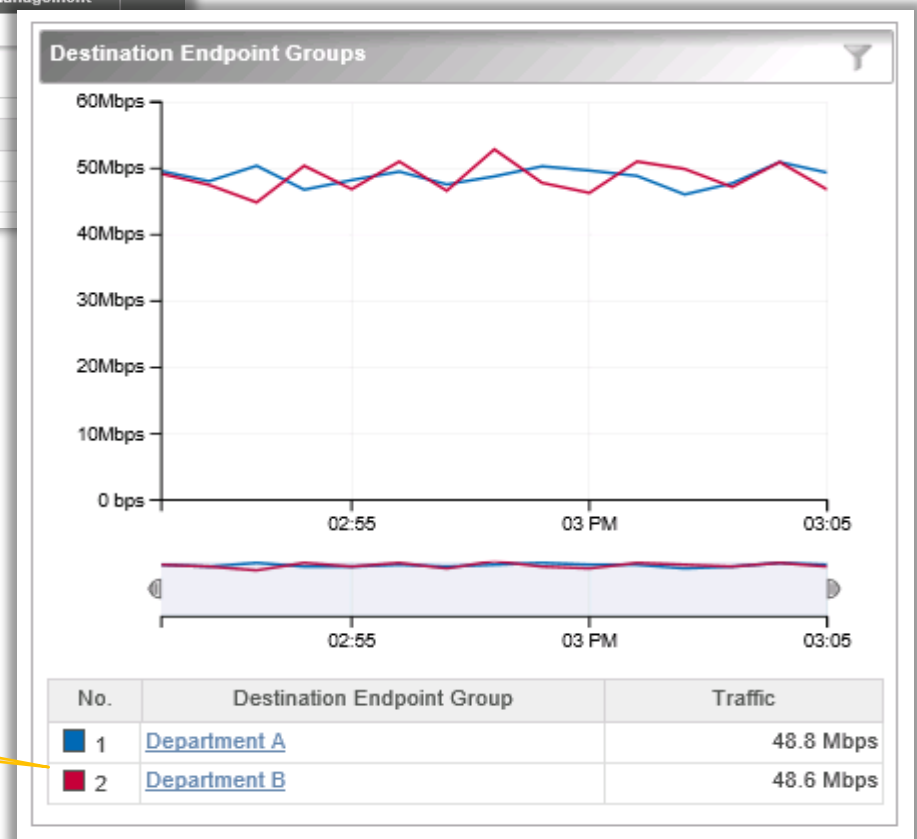
# Traffic Analysis for Each Section

**For a capacity planning the feature of the traffic of each section is captured.**



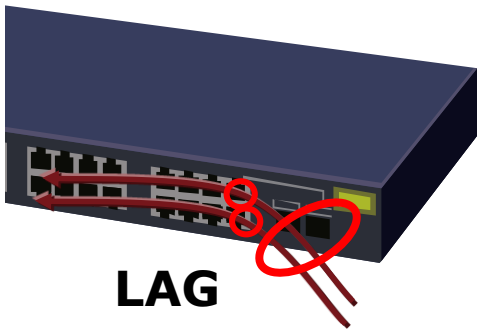
The respective IP address range of the section A and the section B is set as a group.

It's able to display the traffic for the section A and B by a section unit.



# Analyzing Flows That Go through LAG Interfaces

**It enables to set interfaces of exporter as a group.**

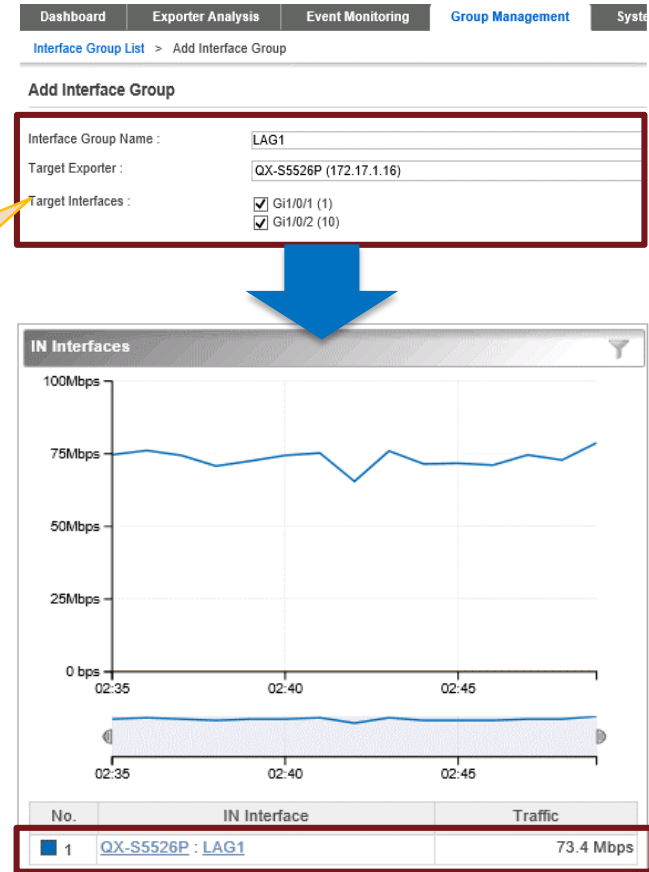


The interfaces of which LAG is composed are set as a group

User wants to analyze the traffic which goes through LAG interfaces.

Flow information can be usually shown by only each interface unit.

The traffic of LAG can be analyzed by setting interfaces as a group.




Graph of LAG can be displayed

# Threshold Monitoring of Flow Data

**Before any failure occurs, threshold monitoring (\*) can detect performance degradation.**

Alerts can be confirmed with the current alert widget on dashboard and event list screen.

Severity	Detection Time	Targets	Content
	2016-06-24 14:57:03	QX-S5526P : ifIndex2	Traffic exceeded 400 Kbps continuously 1 times. Traffic = 16560.0 Kbps, Flow conditions = -

Page 1 of 1

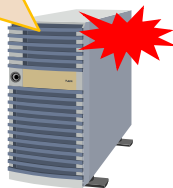
MasterScope Network Flow Analyzer

Dashboard | Exporter Analysis | **Event Monitoring** | Group Management | System Management

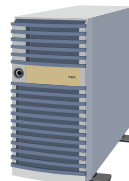
Event List

Severity	Detection Time	Monitoring Target	Content	Entry Name
Warning	2016-06-24 14:57:03	QX-S5526P : ifIndex2	Traffic exceeded 400 Kbps continuously 1 times. Traffic = 16560.0 Kbps, Flow conditions = -	Warning

Detecting a threshold excess



SNMP trap



Turn on flasher

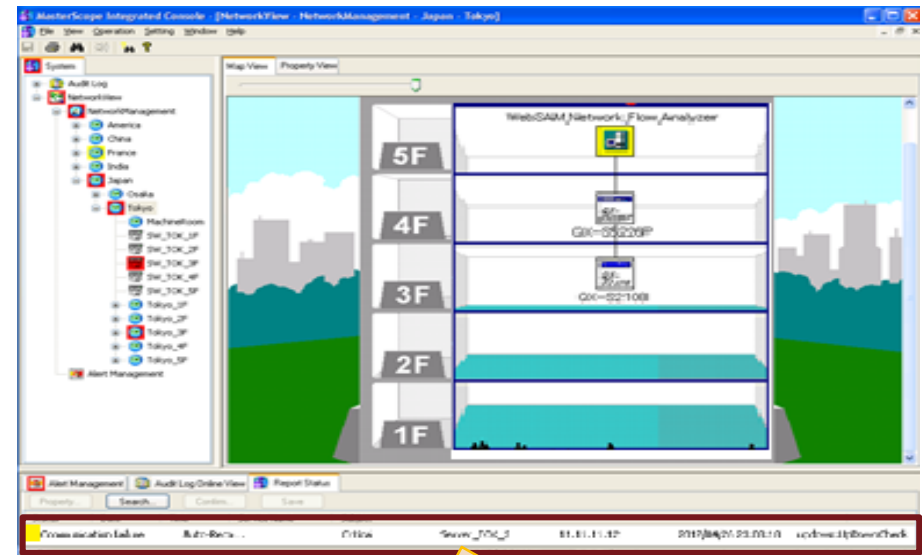


Sending E-mail

MasterScope  
Network Flow Analyzer

MasterScope  
Network Manager

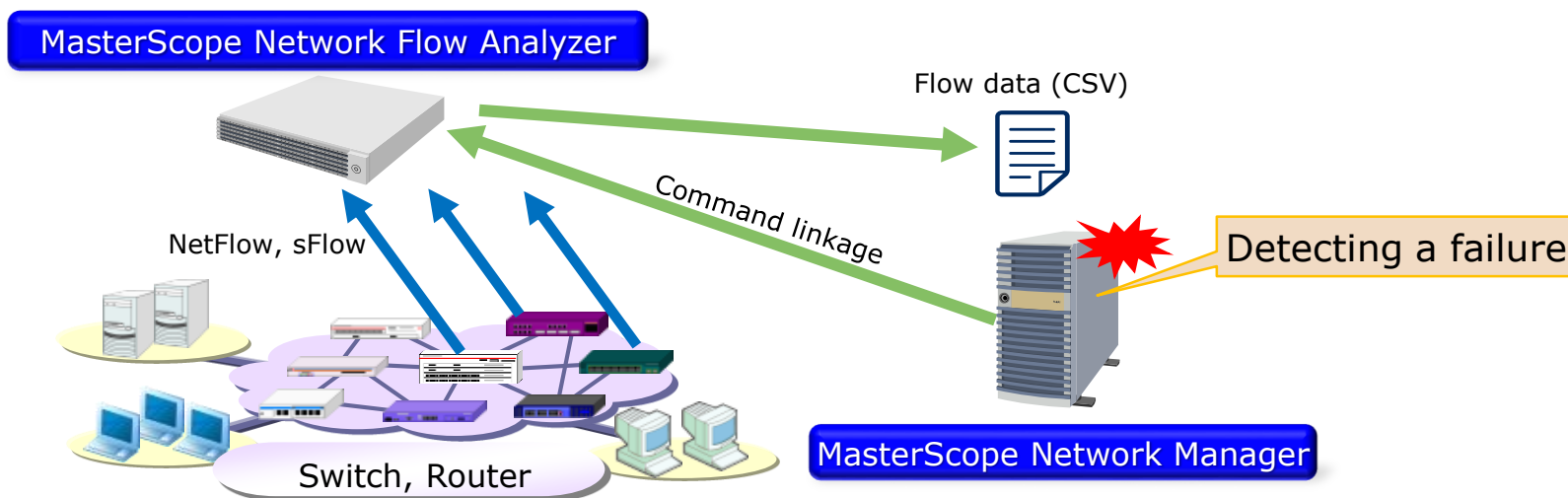
\* The following flow data can be monitored: "Application", "IP protocol", "Destination/Source IP address", "Destination/Source AS"



MasterScope Network Manager can receive a SNMP trap of threshold excess, and report by E-mail and flasher, etc..

# Exporting Flow Data

**Details of communication status at the time of failure can be automatically stored by collaboration with external operation management software.**



In addition, Administrator can store detailed past data for long-term as external files, or periodically generate original data to make analysis reports by calling commands to export flow data with cron, etc.

# MasterScope Network Flow Analyzer

Sales Information



# System Requirements of MasterScope Network Flow Analyzer

## ■ Hardware environment

CPU	Intel Quad Core Xeon or more, or equal compatible CPU
System memory	8GB or more
Disk (free space)	5GB or more (100GB or more is recommended)

## ■ Software environment

OS	Red Hat Enterprise Linux 6 (x86_64) Red Hat Enterprise Linux 7 (x86_64)
Browser	Windows Internet Explorer 11 Mozilla Firefox 60 or later Google Chrome 71 or later
Supported Flow protocol	NetFlow v5, v9 IPFIX sFlow v4, v5 *“Sampling” feature of NetFlow, IPFIX is supported.
Supported Clustering software	ExpressCluster X

## Main product license

Product name
MasterScope Network Flow Analyzer 2.0 for Linux (20 interfaces)
MasterScope Network Flow Analyzer 2.0 for Linux (50 interfaces)
MasterScope Network Flow Analyzer 2.0 for Linux (100 interfaces)
MasterScope Network Flow Analyzer 2.0 for Linux (250 interfaces)
MasterScope Network Flow Analyzer 2.0 for Linux (500 interfaces)
MasterScope Network Flow Analyzer 2.0 for Linux (1000 interfaces)

\* A license for the number of target interface which analyzed flow information is needed.  
Without restriction to the number of exporter

## Upgrade license

Product name
MasterScope Network Flow Analyzer upgrade license for Linux (20 to 50 interfaces)
MasterScope Network Flow Analyzer upgrade license for Linux (50 to 100 interfaces)
MasterScope Network Flow Analyzer upgrade license for Linux (100 to 250 interfaces)
MasterScope Network Flow Analyzer upgrade license for Linux (250 to 500 interfaces)
MasterScope Network Flow Analyzer upgrade license for Linux (500 to 1000 interfaces)

# Thank You

---

## **MasterScope**

Realize simple and integrated system operation

For more product information,  
visit >> <http://www.nec.com/masterscope/>

For more information, please contact your local NEC  
representative or contact us at [global@soft.jp.nec.com](mailto:global@soft.jp.nec.com)

---

 **Orchestrating** a brighter world

**NEC**