

nChronos

Network Performance Analysis System



Copyright © 2024 Colasoft. All rights reserved. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying, for any purpose, without the express written permission of Colasoft.

Colasoft reserves the right to make changes in the product design without reservation and without notification to its users.

Contact Us

Sales

sales@colasoft.com

Technical Support

support@colasoft.com

Website

<http://www.colasoft.com/>

Contents

Preface	1
Introduction	3
About nChronos	3
Architecture	3
Deployment	3
Installation, Activation and Uninstall	7
Installing nChronos Console	7
Activating nChronos Console	8
Having trouble upon activating nChronos	8
Uninstalling nChronos Console	8
Server Configurations	10
Logging Server from a browser	10
Storage Settings	10
Agent Configuration	12
Interface Settings	14
Setting a Capture interface	15
Setting a Management interface	16
Link Configuration	17
Predefined Library	21
Analysis Center	22
SMTP Settings	23
Alarm Notification	24
Report Notification	25
User Management	26
Authentication Settings	29
Certificate	30
Security Policy	31
Audit Log	32
Time Synchronization	34
Server Status	35
Server Information	36
Server Management	37

Console User Interface.....	39
Menu bar	39
Start Page	40
Server Explorer	41
System Alert	43
Adding and connecting nChronos Server	44
Adding nChronos Server	44
Connecting nChronos Server	45
Configuring Network Link	46
Capture Filters	46
Creating a Simple filter	48
Creating an advanced filter	51
Storage Filters	54
Name Tables	55
Packet Truncating	58
Network Segments	59
Sublink Configuration	61
References	64
Field Definition	65
Transaction Settings	66
Adding a TCP transaction	67
Adding a database transaction	75
Adding an HTTP transaction	78
Adding an SSL/TSL transaction	82
Adding an SDL sync transaction	83
Analysis Settings	86
Adding a standard application	88
Adding a web application	89
Adding a signature application	90
Application Groups	92
Application Alarms	93
Transaction Alarms	96
Millisecond Traffic Alarms	98
Traffic Alarms	101
Email Alarms	103

Domain Alarms.....	105
Signature Alarms	108
Baseline Alarms.....	111
Burst Alarms.....	113
Abnormal Access Alarms.....	115
VoIP Alarms	119
View Management	122
Exporting Network Link Properties	122
Importing Network Link Properties	123
Link Analysis.....	124
Retrospectively Analyzing a Network Link	124
The Link Analysis window	124
Time Window	125
Trend charts for link analysis	127
Link Analysis views	129
Toolbar and pop-up menus	129
The Summary view	131
The MAC Address view	131
The MAC Conversation view	132
The Network Segment view	133
The Application view	134
The Application Group view	135
The IP Address view.....	136
The IP Conversation view	138
The TCP Conversation view	139
The UDP Conversation view	140
The Segment-Segment view.....	140
The Service Access view	142
The Port view.....	143
The Service Port view	144
The Link Alarm view.....	146
The Virtual Network view	147
The DSCP view	148
The Devices Statistics view	149
The Interface Summary view.....	150
Multi-segment analysis	151

Configuring Multi-Segment analysis.....	151
Detail analysis.....	152
Exporting statistics.....	153
Downloading packets.....	154
Analyzing with Expert Analyzer.....	156
Link Monitor	156
Monitoring a network link in real-time.....	157
The link monitor window	157
The Real-Time Data pane.....	158
The Trend Charts pane.....	158
The Top Segments pane.....	161
The Top Internal Hosts pane.....	162
The Top Applications pane.....	163
The Alarms pane	164
The Matrix pane	165
Custom Analysis in New Window.....	166
Trend charts	166
Analysis views.....	166
Millisecond Analysis.....	167
Time Window	167
The Summary view.....	167
The Millisecond Traffic Alarm view.....	168
Reports	169
Instant reports.....	169
System Reports	171
User-Defined Reports.....	171
Creating a report	171
Duplicating a report.....	173
Managing schedules.....	175
Scheduling a report	176
Report modules.....	177
Alarms	178
Application Monitor.....	179
Monitoring an application.....	179

The Trend Charts pane	180
The Real-Time Data pane	180
The Top Segments pane	181
The Top Clients pane	182
The Alarms pane	183
The Matrix pane	184
Analyzing Applications	185
Analyzing the performance of an application	185
Trend charts for application performance analysis	185
Performance analysis views	186
The Client view	186
The Server view	187
The Network Segment view	188
The IP Conversation view	189
The TCP Conversation view	190
The Packet Size Distribution view	190
The Application Alarms view	191
Analyzing Transactions.....	193
The Transaction view	193
The Client view	195
The Server view	195
The Network Segment view	196
The Transaction Log view	197
The Transaction Alarms view	199
Common Information Query	200
Query server information	200
Query server running status	201
Query link status	202
Query network link configuration information	203
Query user information	204
Query interface information	205
Query storage configuration information	206
Query SMTP settings	207
Query Alarm Sending Configuration Information	208
Query report sending notification	208

Query audit log information	209
Query Information about multiple Processes.....	210

Preface

Summary

This guide is provided to guide the usage of nChronos. It is recommended to read this guide chapter by chapter, which are arranged according to usage and difficulty.

Who should read this paper

This guide is written for all users of nChronos.

Glossary

The commonly used terms in this guide are described in Table 1.

Table 1 Glossary

Term	Description
nChronos Server	The core of nChronos, for capturing, analyzing and storing the traffic data of target network which is also called as network link. Communicates with nChronos Console via the communication port. Also called as Server.
nChronos Console	A data presentation platform. Connects to nChronos Server, provides various statistics for users to view and analyze the network traffic status, and provides retrospective analysis, new analysis and data drilldown. Also called as Console.
Analysis object	The network elements, including protocols, addresses, ports, conversations, applications, hosts, network segments, target network, and other elements.
Capture interface	A network interface/port on nChronos Server, generally connected with the mirror port, for capturing the traffic of the target network.
Management interface	A network interface/port on nChronos Server, generally for accessing the Internet such that nChronos Consoles and third-party apps can access the nChronos Server to obtain statistics and analysis data.
Network link	A network object for nChronos to collect captured network traffic and to make statistics and analysis.
Back-in-time analysis	Also called as retrospective analysis. Provides detailed analysis presentation, data drilldown, new analysis and various statistics for historical network data.
Time Window	A time range with specific span which could be 4 minutes, 20 minutes, 1 hour, 4 hour and other time spans. Smaller time span provides less data volume and finer data granularity.

Term	Description
	With the Time Window, network data of historical time can be retrieved easily.
Filter	A group of user-defined data screening conditions or rules to accept the required data.
IP pair	A pair of IP addresses, without the identification of source address and destination address.
Drilldown	Level-by-level progressive analysis on selected network objects which include applications, network segments, addresses and conversations.
Expert Analyzer	A packet-level analysis system. Provides lots of statistics about selected network objects and original decoding information of the packets.
Web application	URL-based applications and defined by host name, IP address, port number and URL parameters.
Signature application	Applications defined by the feature codes of original data flow, in ASCII, Hex, UTF-8 or UTF-16.
Performance analysis	The analysis on the service performance of an application.

Introduction

This chapter introduces nChronos, and describes the architecture and deployment of nChronos.

About nChronos

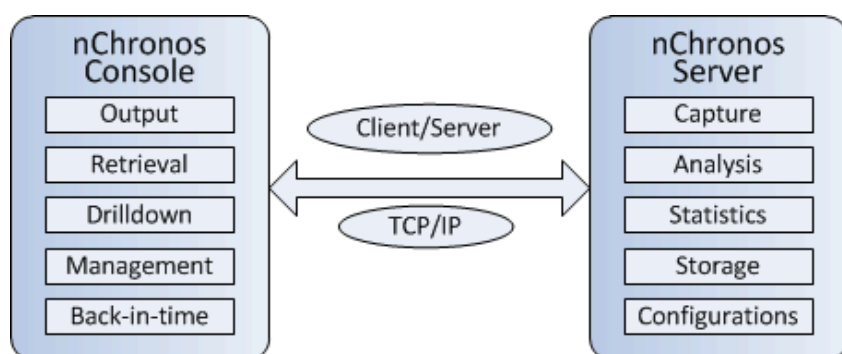
Colasoft nChronos consists of nChronos Server and nChronos Console. nChronos Server is the core of nChronos, for capturing, analyzing and storing the packets of target network. nChronos Console is just like a data presentation platform, for accessing nChronos Server to obtain statistics and other analysis data for presentation. Users should first deploy nChronos Server, and then connect the nChronos Server to a Console to view data.

Architecture

Colasoft nChronos Server contains at least two network interfaces, one called as capture interface and the other as management interface. With the capture interface, nChronos Server captures all packets on the target network via the mirror ports on switches or taps, and then deliveries the packets to analysis and statistical modules to analyze and store. With the management interface, nChronos Server communicates with nChronos Consoles over the LAN or Internet.

Colasoft nChronos Consoles communicate with nChronos Servers using C/S (Client/Server) technology. When nChronos Console monitors the network link in real-time, displays the statistics on the analysis views, exports statistics, downloads packets, drills down network objects, makes refine analysis, and performs other communication operations, it sends request commands to the Server; then the Server responds the commands and returns related data. Furthermore, nChronos Console and nChronos Server communicate over the Internet using TCP/IP protocols with specified port number.

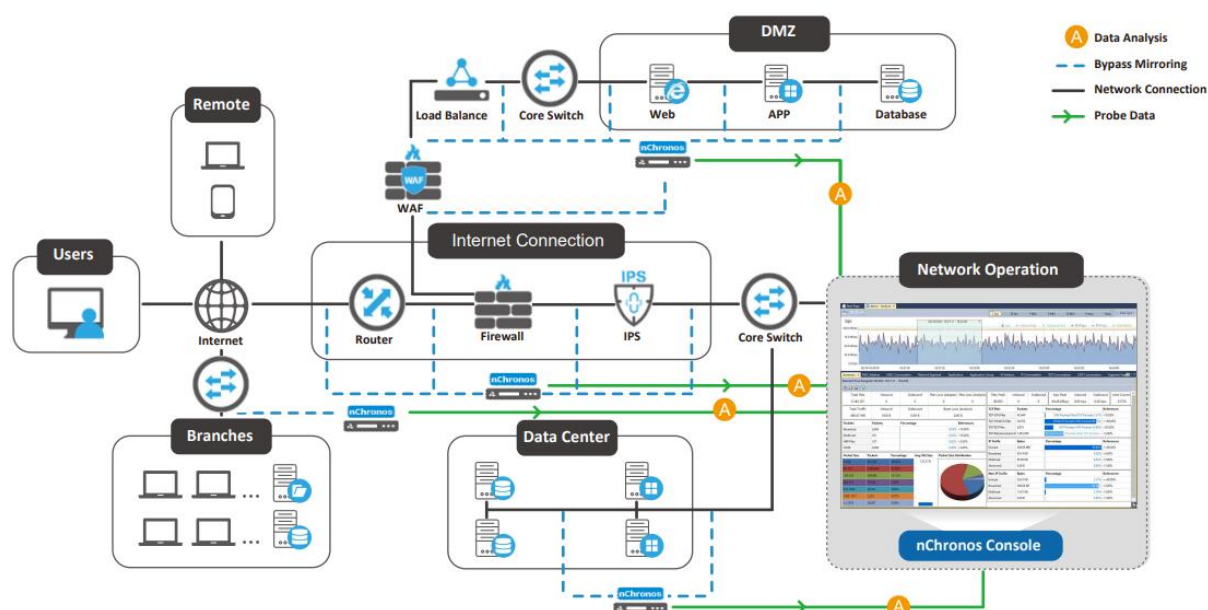
The functional architecture of nChronos Consoles and nChronos Servers is described as the following figure:



Deployment

For the networks of different scales and with multiple network links, nChronos can not only capture and store the network data of local networks but support distributive deployment and remote monitor. For the critical network links, multiple nChronos Servers can be deployed and users can connect to remote nChronos Servers at any place any time for data analysis and network management. Furthermore, using nChronos Consoles, the traffic of critical network links can be

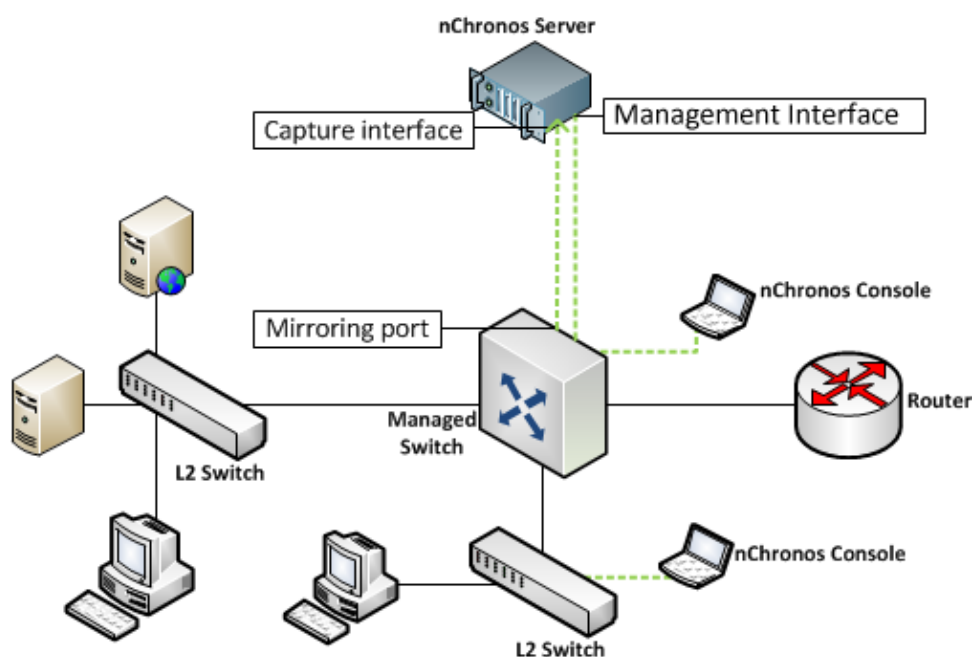
monitored in real-time and can be reported once there are anomalies. The deployment of nChronos is visualized as the following figure:



To capture traffic effectively, the traffic sources are must from appropriate network devices which include managed switches, hubs and taps. Managed switches are the perfect choice because you can use their port mirroring/SPAN function to copy the packets to a monitor port. This function is called as *Port Mirroring* (Cisco calls it *SPAN*). For more details about port mirroring, read Switch Management on our website.

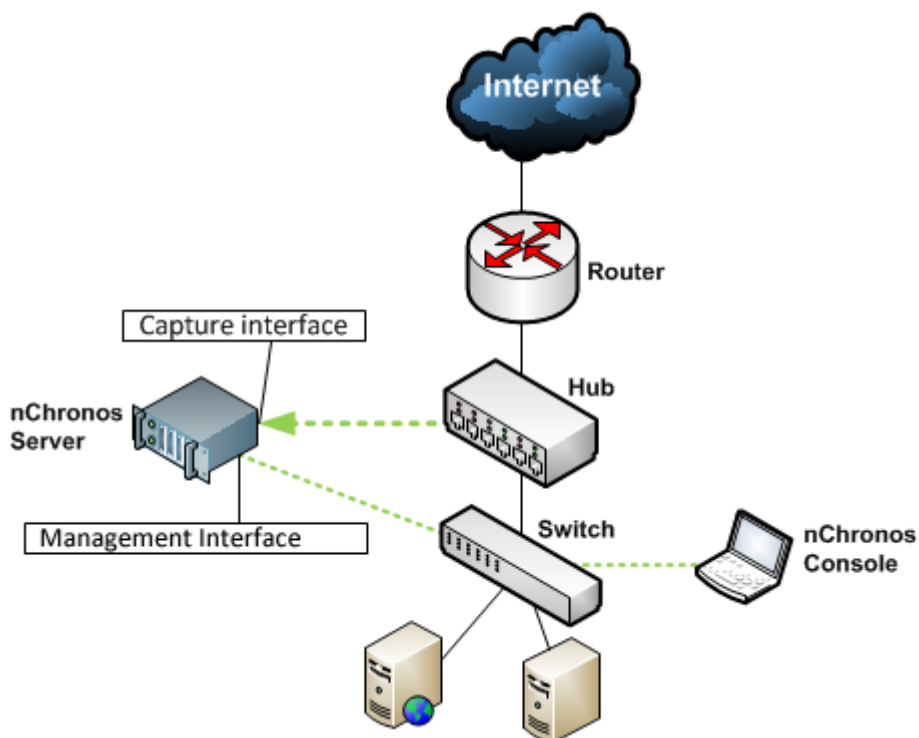
Managed switches

The following figure shows simplified nChronos deployment in a network with managed switches.



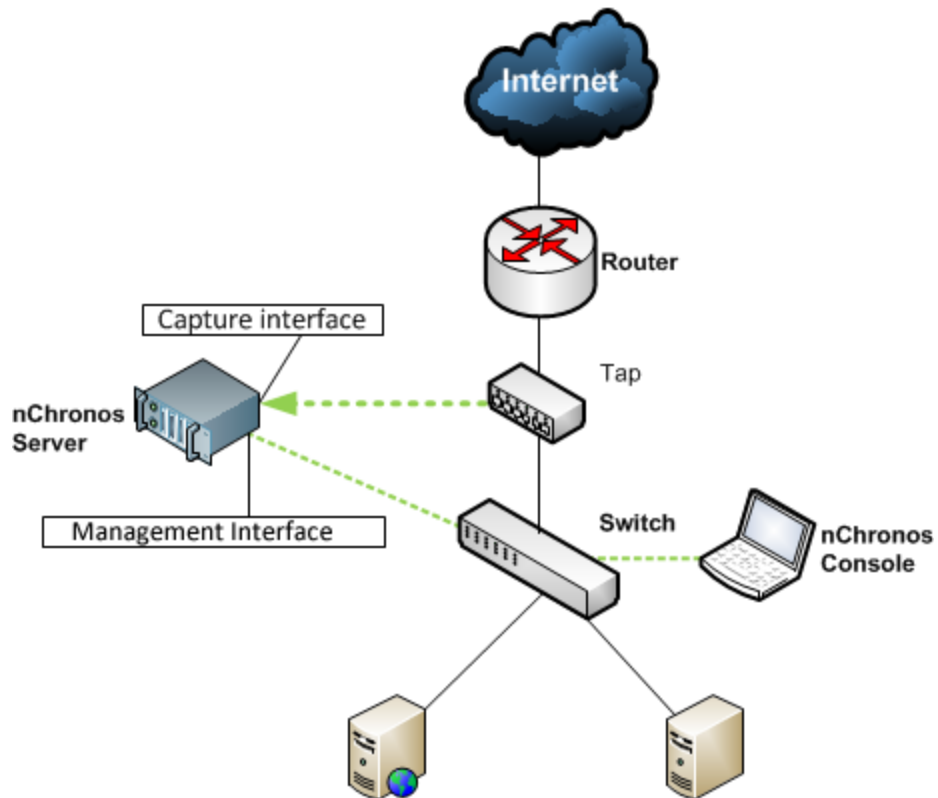
Hub

If a managed switch is unavailable on the network, you may use a hub as the traffic source. In such a network, the capture interfaces are connected to the hub. Note that a hub can only process 100 Mbps of traffic, and it's not a good choice for modern networks. But if the network traffic is small, a hub is also an economical choice. The following figure shows simplified nChronos deployment in a network of hubs.



Tap

Besides using a hub to capture traffic from a small network, a network tap is a more wise choice to be used to capture traffic from a heavily utilized cable. A network tap is acting the port mirroring function of a managed switch, which is able to make a copy of all packets and send it to your server. The figure below shows simplified nChronos deployment in a tap network.



Installation, Activation and Uninstall

This chapter introduces nChronos Console installation, activation, and uninstall.

Installing nChronos Console

System requirements

The recommended system requirements for nChronos Console are:

4-core processor

4GB RAM or more

Independent network adapter

Internet Explorer 11 or higher

Installing nChronos Console

Before installing nChronos Console, you should:

Make sure your machine meets the minimum system requirements.

Close all running applications on your machine.

Uninstall any earlier or trial version of nChronos Console.

To install nChronos Console:

Double-click the installation file of nChronos Console, and then the Setup wizard appears. Click Next.

On the License Agreement page, review the License Agreement and, if you agree, select the I accept the agreement check box, and then click Next.

Review the product updates, and then click Next.

Specify an installation directory. By default, the installation directory is C:\Program Files\Colasoft nChronos Console x.x. To specify another directory, use the field provided or click Browse to locate an installation folder. Then click Next.

Specify the folder name on the Start, and then click Next.

Specify whether to create a desktop icon and a quick start icon, and then click Next.

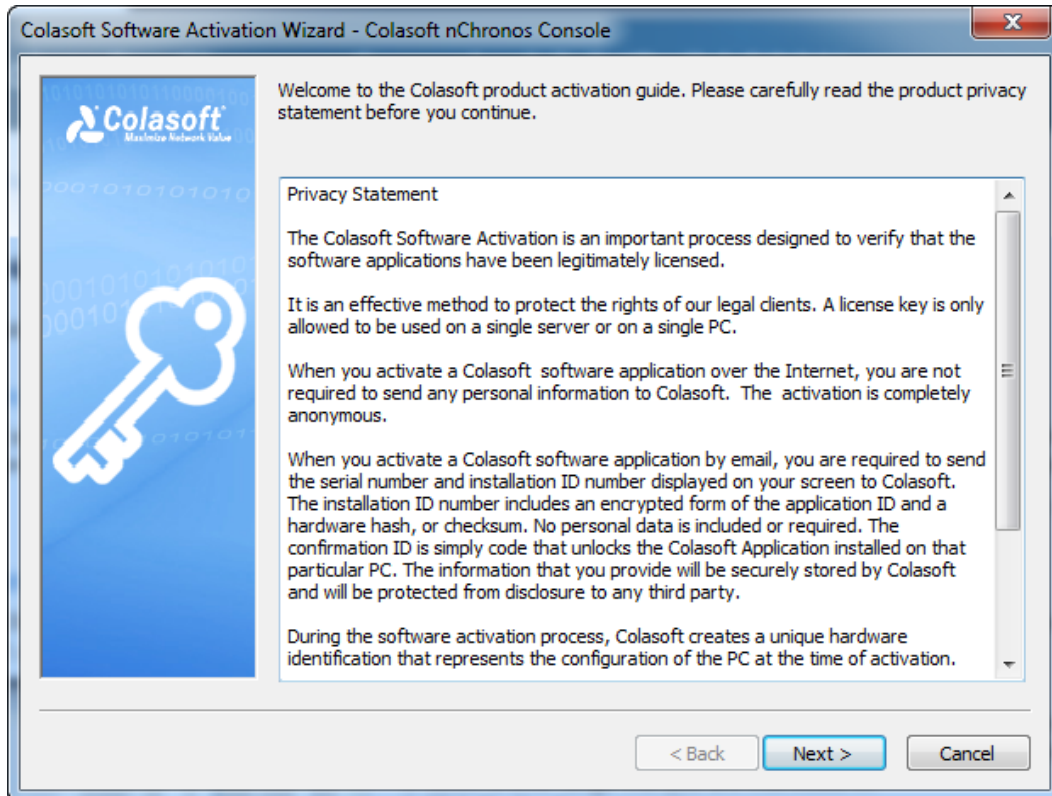
On the Ready to Install page, review the installation information and, if all information are correct, click Install to install nChronos Console to the computer.

Review the Readme, and then click Next.

Click Finish to complete the installation. By default, the Launch Program check box is selected to launch the program after the installation.

Activating nChronos Console

After the installation, the Activation Wizard appears to guide you step by step through the activation process.



Read the Privacy Statement and then click **Next**.

Enter the serial number, and follow the Activation Wizard to complete the activation.

Having trouble upon activating nChronos

Follow steps below to check:

Make sure the SN you are using is typed correctly. nChronos Server and nChronos Console use different Serial Numbers, and cannot share the same Serial Number.

If you are using the right SN, please check if you can connect to Colasoft license server by using command: ping secure.colasoft.com

If there is no response when you ping to secure.colasoft.com, please make sure that your server is connecting to the network and please make sure your DNS is working fine as well.

If you can get response from the ping, but still not able to activate the nChronos Server, please contact our support team by emailing your SN, machine code, and version number to: support@colasoft.com.

Uninstalling nChronos Console

To uninstall nChronos Console,

Do one of the following:

On the **Start** menu, locate the folder of nChronos Console, which, by default, is *Colasoft nChronos Console x.x*, and then click **Uninstall Colasoft nChronos Console x.x**.

On the **Start** menu, click **Control Panel**. In Control Panel, click **Uninstall a program**. Locate Colasoft nChronos Console x.x and then click **Uninstall**.

The Uninstall dialog box pops up as the following figure. Click Yes to continue the uninstallation.

A box pops up to ask whether to keep configurations. Click Yes if you want to keep the configurations, or else click No.



The configurations are the server list information on the Server Explorer.

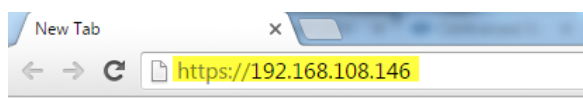
Server Configurations

To capture useful traffic and analyze efficiently, you need to configure nChronos Server. This chapter describes the configurations for nChronos Server, and all these configurations are done on webpages. So, you should first login nChronos Server from a browser.

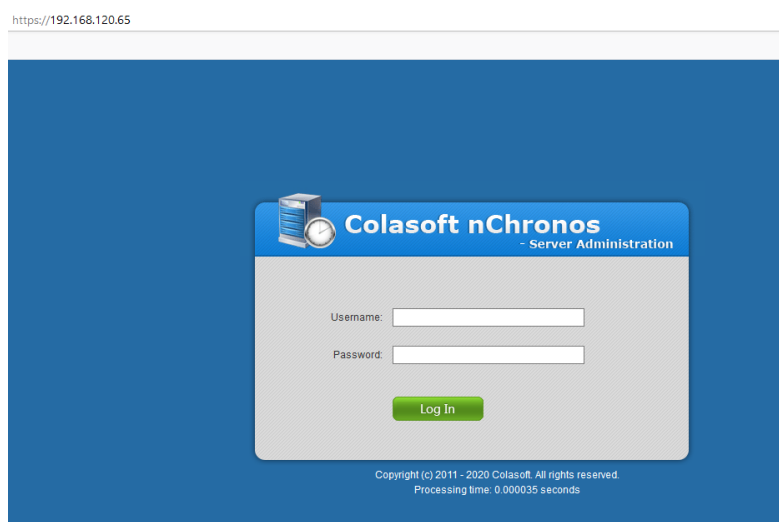
Logging Server from a browser

You can log nChronos Server from the browsers at both the Server side and the Console side. To log in a Server from a browser, follow the steps below:

1. Launch a browser, in the address bar input https:IP and then press ENTER. The IP is the IP address of the management interface of nChronos Server.



On nChronos Server login portal, input the user name admin and the password D&^4Vs.



Click **Log In** to log in the Server.

Storage Settings

This page is provided to configure storage settings:

Storage Settings

Disk Space

Device	Mount Point	Total Space	Available Space	Storage Space Used	Storage Space Configured	Export Data Space
/dev/sda2	/	90GB	73GB	0GB	<input type="text" value="0"/> GB	<input type="radio"/> <input type="text" value="0"/> GB
/dev/sdb1	/data	3206GB	3196GB	3193GB	<input type="text" value="3196"/> GB	<input type="radio"/> <input type="text" value="0"/> GB
/dev/sdb2	/data2	3142GB	3132GB	2484GB	<input type="text" value="3131"/> GB	<input checked="" type="radio"/> <input type="text" value="1"/> GB

Analysis Space

Storage Area	Statistics Space	Packet Space	Transaction Logs Space	Alarm Logs Space
Default storage area	500GB	5027GB	300GB	300GB

[New Storage Area](#)

OK

Disk Space

Disk Space is provided to configure server's storage space. The following list describes the parameters in the list.

Device: The disk in the server machine.

Mount Point: The path of disk in the server machine.

Total Space: The total size of the disk.

Available Space: The free size of the disk.

Storage Space Used: The space that is already used for storing nChronos data.

Storage Space Configured: The size which you specify for storing nChronos data, including captured traffic and analysis data.

Export Data Space: The space for storing link statistics data, application monitoring data and transaction processing data in server machine.

Analysis Space

Analysis Space is provided to configure the size of server's storage space and that of exported data. The following list describes the parameters in the list.

Storage Area: The name of the storage area, which is set by users when adding a new storage area.

Statistics Space: The size of the storage space for storing statistics data.

Packet Space: The size of the storage space for storing packets.

Transaction Logs Space: The size of the storage space for storing transaction logs.

Alarm Logs Space: The size of the storage space for storing alarm logs.

Click the "New Storage Area" link, the New Storage Area dialog box pops up as shown below:

New Storage Area

×

Name:

Storage Type:

▼

Statistics space:

0

GB
▼

Settings

Packets space:

0

GB
▼

Transaction logs space:

0

GB

Alarm logs space:

0

GB

OK

Cancel

You can click the button **Settings** to configure the percentage for each type of statistical data.

Agent Configuration

The traffic forwarding Agent is installed on a third-party server for forwarding the traffic from the server to the capture interface on the nChronos Server. This page is for configuring Agent settings and shows as the following figure:

Agent Configuration

Settings

Agent Name	Agent Version	Status	bps	Duration	Login Time	Operation
183agent	1.0.0.0	Online	3.448 Mbps	24:06:18	08/27/2017 07:18:51	<div style="display: flex; justify-content: center; gap: 10px;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Edit</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">Delete</div> </div>

All the Agents connected to nChronos Server are listed on the Agent Configuration Page. The detail information of Agent is listed below:

Agent Name: The name of Agent, which is set in the Agent configuration file.

Agent Version: The version information of Agent.

Status: The connection status between nChronos server and Agent.

bps: The real-time traffic information of the interfaces selected by Agent.

Duration: The duration of the Agent.

Login Time: The latest login time of Agent.

Operation: The User is able to edit or delete an Agent.

Agent connecting to nChronos Server

When connecting to nChronos server, Agent is the one who initiates the connection. You have to put nChronos server's IP and port within the Agent configuration file. Please follow the steps below:

Agent Name: Set the name for Agent. And Agent will appear in the list with this name.

Agent Interface: Set the network interface to forward the traffic of the Agent.

nChronos Sever IP: Set the nChronos server's IP address for Agent to connect to.

nChronos Sever Port: Set the port for the communication between nChronos and Agent. Port 5111 is the default port.

nChronos Server Interface: The network interface of nChronos server to receive the traffic from the Agent.

Edit

You could edit the Agent which is already connected to the nChronos server. Click the "Edit" button to edit the Agent, as the screenshot below:

Agent Configuration/183agentConfiguration

<input type="checkbox"/>	Name	IP Address	bps	Connection speed
<input type="checkbox"/>	eno1	0.0.0.0	0.000 bps	1000
<input type="checkbox"/>	eno2	0.0.0.0	0.000 bps	1000
<input checked="" type="checkbox"/>	eno3	172.16.0.183	452.288 Kbps	1000
<input checked="" type="checkbox"/>	eno4	192.168.226.88	585.776 Kbps	1000
<input type="checkbox"/>	enp130s0f0	0.0.0.0	0.000 bps	Unknown
<input type="checkbox"/>	enp5s0f0	0.0.0.0	0.000 bps	Unknown
<input type="checkbox"/>	enp130s0f1	0.0.0.0	0.000 bps	Unknown
<input type="checkbox"/>	enp5s0f1	0.0.0.0	0.000 bps	Unknown

Truncate Packets

☐ Limit packet size to bytes

Packet Filter

And Or Invert Edit Delete

Start

End

OK

Cancel

Interface List: Choose the network interfaces whose network traffic is going to be forwarded.

Truncate Packets: When this option is enabled, the Agent will only forward specified bytes of each packet. It can be set between 64-65535 bytes.

Packet Filter: This option is for setting packet filter rule. Packet filter supports IP address and port rules. Logical "and" and "or" relationship are supported.

Settings

The settings can be configured in batch. Click the "Settings" button to batch edit the settings, as the screenshot below:

Agent Configuration/Agent

☐ 183agent

Limit the packet size to:

☐ Limit the packet size to Byte


Packet Filter

And Or Invert Edit Delete

Start

End

OK Cancel

 **Note** When batch settings conflict with single Agent settings, single Agent settings have priority over batch settings.

Interface Settings

This page lists all network interfaces on nChronos Server. The capture interface is for capturing traffic and usually connected to the mirror port of a switch or a tap, and the management interface is for the Server to communicate with nChronos Consoles. The Interface page shows as following:

Interface Settings

Interface ID	Name	bps	Speed (Mbps)	Type	Transmission Medium	Identify IP Layer	Operation
1	eth0(172.16.0.188)	601.696 Kbps	1000	Capture inter ▼	Ethernet ▼	First layer ▼	Edit
2	eth1(0.0.0.0)	0.000 bps	1000	Capture inter ▼	Ethernet ▼	First layer ▼	Edit
3	eth2(0.0.0.0)	0.000 bps	1000	Capture inter ▼	Ethernet ▼	First layer ▼	Edit
4	eth3(0.0.0.0)	0.000 bps	Unknown	Management ▼			Edit
5	eth5(192.168.226.60)	0.000 bps	Unknown	Capture inter ▼	Ethernet ▼	First layer ▼	Edit
6	dpgk port 0(0.0.0.0)	975.140 Mbps	Unknown	Capture inter ▼	Ethernet ▼	First layer ▼	Edit

Name: The name as well as the IP address of the network interface/port.

bps: The output of the network interface/port.

Speed: The bandwidth of the network interface/port.

Type: To specify it is a capture interface or a management interface. When a network interface/port is defined as Capture interface and is allocated to a network link, you cannot modify the interface type of it any more. If you want to modify it, you have to delete the network link first.

Transmission Medium: The transmission protocol of that interface. It could be Ethernet or PPP protocol.

Identify IP Layer: Specify which IP layer to identify. By default, it is the first layer, and users can choose the fourth layer at most. When actual IP layer is less than the set layer, identify it based on the most inner layer.

Setting a Capture interface

To set a capture interface, just click the Edit button following the capture interface to go to the Virtual Interface page, as the following figure:

Interface Configuration / Edit Interface

☐ Customized VXLAN Signature

Port:

Apply

☐ Customized CAPWAP Signature

Port:

Apply

Virtual Interface

Virtual Interface Type: VLAN ▼

New

VLAN ID	Segment Rule	Alias	Operation
---------	--------------	-------	-----------

To add a virtual interface,

1. Select the virtual interface type to be added. You can choose VLAN, ISL VLAN, MPLS VPN, VXLAN, NETFLOW, GRE, Network Segment and MAC address.
2. Click the button New to pop up the add box:

Virtual Interface

VLAN ID:

Segment Rule:

MAC:

Alias:

And then click **OK** to save the settings.

Setting a Management interface

- To set a management interface, follow the steps below:
- Click **Edit** following the Management interface to get into the setup page, like the following figure:

enp1s0 (192.168.5.162)

☒ IPv4

IP address:

IP mask:

Gateway address:

DNS server:

☐ IPv6

IP address:

Prefix length:

Gateway address:

DNS server:

Enter IP address, IP mask, gateway address, and DNS server, and then click **OK**.

Link Configuration

On the **Link Configuration** page, you can view basic information of the network, change the link status, delete and add a network link. This page shows as following:

Link Configuration

Network Link ID	Name	Type	Capture Interface Count	bps	Status	Operation
0	test	Switch (bidirectional traffic mirroring)	1	27.632 Kbps	Stopped	Run Edit Delete
1	replay	Replay packets	0	0.000 bps	Stopped	Run Edit Delete

New Link

The following list describes the columns on this page:

Network Link ID: The number of the network link. It starts from 1.

Name: The name of the network link. It is defined when adding a network link and displays under the Server on the Server Explorer at the Console side.

Type: The type of the network link. It shows the way to capture the traffic.

Capturing Interface Count: The quantity of the Capture Interfaces for this network link.

bps: The traffic speed of the network link.

Status: The status of the network link. It shows whether the network link is running or not. It could be *Running* which means starting to capture and analyze the traffic of the network link, and *Stopped* which means nChronos Server has stopped capturing traffic.

Operation: The operations on the network link. The following list describes the actions:

Edit: Modifies the settings of the network link. The settings are just the same as those when adding a network link.

Delete: Deletes the network link. This action is only available when the link status is *Stopped*.

Stop: Stops the monitor on the network link.

Run: Starts to capture and analyze the traffic of the network link.

Adding a network link

To add a network link, follow the steps below:

1. Click **New Link** on the **Link Configuration** page to show the following page:

Network Link Settings / Edit Link

Basic Information

Link Name: Network link name cannot contain the following characters \ : ? * < > |

Network Link Type:

Storage Area:

Inbound/Outbound Traffic Capturing Interface

Network Interface	Transmission Medium	IP Address	bps	Speed (Mbps)
<input checked="" type="checkbox"/> enp4s0	Ethernet	0.0.0.0	0.000 bps	1000

Internal IP Rule

Note:

The configuration of the inbound / outbound network segments is convenient for you to distinguish the transmission direction of the packets in the network, to help you identify the internal and external network IP addresses, and to more accurately count the inbound and outbound traffic.

Configuration of the inbound / outbound network segments. Support IP address and MAC address. If the IP identification result and the MAC identification result conflict, take the MAC result.

The reference format is as below:

IP address/netmask Eg: 192.168.0.0/24 or 192.168.0.0/255.255.255.0 or 2001:3ef0::/80

IP address range Eg: 192.168.0.0-192.168.1.255 or 2001:3ef0::0001-2001:3ef0::0005

Single IP address 如: 192.168.0.100 or 2001:3ef0::0001

Single MAC address 如: 00:16:EA:AE:3C:40 or 00-16-EA-AE-3C-40

One segment or MAC address per line.

Duplicated segment or MAC address.

Analysis Operation

☐ Enable switch timestamp analysis

☒ ARISTA ☐ VSS monitoring ☐ Gigamon

☐ Export data in CSV format

☐ Enable millisecond traffic statistics

☐ Specify IP statistics layer

☐ Specify virtual network ID statistics layer

☒ Innermost Layer ☐ Outermost Layer ☐ Innermost Layer and Outermost Layer

Inbound/Outbound Bandwidth Utilization

Inbound Bandwidth: Mbps (Range: 1-1,000,000 Mbps)

Outbound Bandwidth: Mbps (Range: 1-1,000,000 Mbps)

Total Bandwidth: Mbps

The total bandwidth cannot be less than the greater one of the inbound bandwidth and outbound bandwidth and cannot be greater than the sum of the inbound bandwidth and outbound bandwidth.

Enter the link name and select a link type. The following list describes the link types.

Switch (bidirectional traffic mirroring): nChronos captures traffic from the switch which has mirrored traffic, including inbound and outbound.

Switch (one-way traffic mirroring): nChronos captures traffic from the switch which has mirrored one-way traffic, inbound or outbound.

Standard tap: A network tap which only mirrors one-way traffic, inbound or outbound.

Aggregation tap: A network tap which mirrors bidirectional traffic, including inbound and outbound.

Select a storage area for the network link. The data of multiple network links can be stored on one storage area.

Set capture interface and network segments:

If you select *Switch (bidirectional traffic mirroring)* or *Aggregation tap*, follow the steps below:
Select the capture interfaces which are connected with the mirror port of the switch or the tap.

Set the network segment, which is for identifying the transmission direction of the packets to further get accurate inbound and outbound traffic statistics. You should enter the IP addresses and the segments that should be recognized as internal addresses.

If you select *Switch (one-way traffic mirroring)* or *Standard tap*, follow the steps below:

- 1) Select the capture interfaces that are connected with the outbound mirror port of the switch or the tap for capturing outbound traffic.

Select the capture interfaces that are connected with the inbound mirror port of the switch or the tap for capturing inbound traffic.

Set up whether to use switch timestamp. At present only three types of switches are supported: ARISTA, VSS Monitoring and Gigamon.

Set up whether to export data automatically. You can export network link statistics data, application performance data and application transaction data in CSV format.

Set up whether to enable millisecond statistics. Millisecond statistics is for the environment that cares about burst traffic. Millisecond traffic alarm can be configured only when millisecond statistics is enabled.

Specify IP statistics layer.

Specify virtual network ID statistics layer.

Set bandwidth. Enter the inbound bandwidth, outbound bandwidth, and the total bandwidth to get accurate bandwidth utilization.

You should enter the actual bandwidth to get accurate bandwidth utilization.

Specify link privileges for normal users.

Click **OK** to save the settings.

Adding a replay link

To add a replay link, follow the steps below:

Click **New Link** on the **Link Configuration** page to show the following page:

Network Link Settings / New Link

Basic Information

Link name: Network link name cannot contain the following characters \ / : ? * < > |

Network link type:

Storage area:

Packet files

File from: ☒ nChronos Server ☐ Local

Path	Date Modified	Size
Add packet files to replay...		

Add Remove Clear

Inbound/Outbound Network Segment

Instructions:

Enter network segment rules to identify internal IP addresses, with one entry per line.

Examples for network segment rules:

IP/subnet: 192.168.0.0/24 or 192.168.0.0/255.255.255.0 or 2001:3ef0::/80

IP address range: 192.168.0.0-192.168.1.255 or 2001:3ef0::0001-2001:3ef0::0005

Single IP address: 192.168.0.100 or 2001:3ef0::0001

One segment per line.

Segment cannot be duplicated.

Analysis Operation

☐ Enable switch timestamp analysis

1. Enter the link name and select link type as "Replay packets".

Select "Create a storage area" from the Storage area drop-down to create a new storage area. Each replay link needs an independent storage area. Multiple replay links cannot share one storage area.

Set where to get the packet files, from nChronos Server or uploading from local.

Set the network segment, which is for identifying the transmission direction of the packets to further get accurate inbound and outbound traffic statistics. You should enter the IP addresses and the segments that should be recognized as internal addresses.

Set up whether to use switch timestamp. At present only three types of switches are supported: ARISTA, VSS Monitoring and Gigamon.

Set up whether to export data automatically. You can export network link statistics data, application performance data and application transaction data in CSV format.

Set up whether to enable millisecond statistics. Millisecond statistics is for the environment that cares about burst traffic. Millisecond traffic alarm can be configured only when millisecond statistics is enabled.

Specify IP statistics layer.

Set bandwidth. Enter the inbound bandwidth, outbound bandwidth, and the total bandwidth to get accurate bandwidth utilization.

Specify link privileges for normal users.

Click **OK** to save the settings.

Running a network link

To view real-time, dynamic, up-to-the-second network data at the Console side, to get the analysis statistics of the network traffic, or to download packets from the Server, you must monitor the network link to make the link running.

To run a network link, just click the button **Run** on the **Network Link** page.

Stopping a network link

When you want to stop the network link, just click the button **Stop** on the **Network Link** page, and then nChronos will stop capturing traffic.

Predefined Library

The **Predefined Library** page lists all uploaded library files, like the following figure:

Predefined Library

Name	Type	Version	Import Date	Count	Operation
System Application	Application	1.5.9	10/08/2016 13:24:06	1846	<input type="button" value="Edit"/>

The following list describes all the columns on this page:

Name: The name of the library, not the name of the file.

Type: The type of the library.

Version: The version of the library.

Import Date: The time when the library file is uploaded.

Count: The quantity of applications if the library is an application library, or the quantity of signature alarms if the library is a signature library.

Operation: The following list describes the actions.

Edit: You can click this button to view the detailed library information. When viewing an application library, you can enable/disable the interested items.

You can update library files by clicking **Library files update**.

Analysis Center

Analysis Center

nChronos Server name:

Center address:

Center port:

Username:

Password:

SSL: ☐

⚙ Please wait while connecting to the Analysis Center...

Connect

This page is for configuring the connection settings to Analysis Center.

nChronos Server name: The name for this nChronos Server.

Center address: The IP address of Analysis Center

Center port: The port number for connecting to Analysis Center. It is 22000 by default.

Username: The user name for connecting to Analysis Center. The user name should be set up in Analysis Center

Password: The password for the user name to connect to Analysis Center. The user name and password should be set up in Analysis Center.

SSL: Applies SSL encryption when transmitting data. If SSL is enabled, the center port is 22100 by default.

SMTP Settings

This page is for setting the connection parameters to an SMTP email server:

SMTP Settings

User Information

User name:

Email address:

Server Information

Email server:

SSL encryption:

Port number:

Login Information

User name:

Password:

User name: The name of the sender.

Email address: The email address of the sender.

Email server: The address of the email server.


SSL encryption: The encryption connection type of email server.

Port number: The port number for the encryption connection.

User name: The user name of the sender to logon the email server.

Password: The password for the sender address.

After the setting, you can click **Test** to check if the settings are correct.

 **Note** At present, nChronos only supports following authentication types: AUTH LOGIN, AUTH PLAIN, AUTH NTLM, ANONYMOUS login.

Alarm Notification

This page is provided to set alarm notification parameters when alarms are triggered, and shows as the following figure:

Alarm Notification

☒ Email notification

Email subject:

Recipient address:

Notification interval:

Range: 1-999 (minutes)

Test

☒ Syslog notification

Syslog server address:

☒ Send every second

☐ Send every:

Range: 1-999 (minutes)

OK

Email notification

To notify with email when alarms are triggered, follow the steps below:

1. Enable the checkbox **Email notification** on this page.

Enter the subject and the recipient address. You can enter multiple recipient addresses.

Set the notification interval.

Click **OK** to save the settings.

You can click **Test** to verify if the settings are correct. If the recipient address receives the test email, you can be sure that the settings are correct.

SYSLOG notification

To notify with syslog when alarms are triggered, follow the steps below:

1. Enable the checkbox **SYSLOG notification** on this page.

Enter the address and the port number of the syslog server.

Set the notification interval. You can send the syslog every second or every specified minutes.

Click **OK** to save the settings.

Report Notification


This page is for setting report options and report recipient addresses.


Report Notification

Report Template

Company name:

Author:

Company logo: 



☒ Prefix:

☒ Show create time

Report format:

☒ Report recipient

E-mail address:

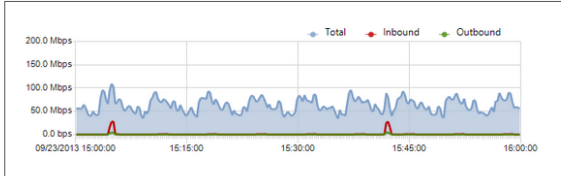
Colasoft

ReportGlobal report

Start time: 09/23/2013 14:00 Author: Administrator
End time: 09/23/2013 15:00 Create time: 09/23/2013 15:05:07
Report object: Global

Bandwidth: 1,000Mbps

Trend Chart



Report options

All the report options will be displayed on reports once users set them up.

Company name: This will be displayed on the top left of reports.

Author: The name of the reports creator.

Company logo: The logo of the company, which will be displayed on the top right of reports.

Prefix: This will be added in the front of all report title as a prefix.

Show create time: Shows the time when reports are created.

Report format: This option is for specifying the format of scheduled reports.

After the settings, users can click Preview to check the display.

Recipient address

The addresses of report recipients. Users can enter multiple addresses with one entry per line.

User Management

This page lists all user accounts. And, on this page, you can add, delete, and kick out users. This page shows as following:

User Management

No.	Username	Type	Status	Date Created	Date Logged in	Notes	Operation
1	admin	Administrator	Online (browser)	10/19/2015 09:34:40	10/27/2015 13:08:14	Administrator	Edit Delete Kick Out
2	hh	Administrator	Offline	10/19/2015 09:40:13	10/27/2015 11:34:23		Edit Delete Kick Out
3	yyy	Administrator	Offline	10/19/2015 09:45:03	10/27/2015 11:34:22		Edit Delete Kick Out
4	test	Administrator	Offline	10/19/2015 09:59:24	10/27/2015 11:34:22		Edit Delete Kick Out
5	hgz	Administrator	Online (Console)	10/19/2015 13:32:45	10/27/2015 12:09:28		Edit Delete Kick Out
6	colasoft	Administrator	Offline	10/20/2015 10:16:06	-		Edit Delete Kick Out
7	wyj	Administrator	Offline	10/20/2015 13:35:49	-		Edit Delete Kick Out
8	wangyong	Administrator	Offline	10/20/2015 14:52:05	10/27/2015 11:49:00		Edit Delete Kick Out
9	test1	Administrator	Offline	10/23/2015 14:30:05	-		Edit Delete Kick Out
10	test2	Administrator	Offline	10/26/2015 15:33:52	10/27/2015 11:34:23		Edit Delete Kick Out
11	jason	Administrator	Online (browser)	10/26/2015 15:39:47	10/27/2015 13:08:30		Edit Delete Kick Out

[New Account](#)

No.: The number of the account, which starts from 1 and increases by 1 every time when a new user account is created. When a user account is deleted, the number of it will be used by the user account following it. Therefore, from the number of the bottom user account, you can know how many user accounts are created for this nChronos Server.

Username: The user name of the account, which is defined when creating a user account.

Type: The type of the account, which could be an administrator, a user, or an auditor. You can change the type of an account by click **Edit** following the account.

Status: The status of the account. The following list describes the status in detail:

Online: The status *Online (Console)* indicates the account logs in the Server from a Console and does not log out yet; the status *Online (Browser)* indicates the account logs in the Server from a browser and does not log out yet; and the status *Online (Console, Browser)* indicates the account logs in the Server both from a Console and a browser and does not log out yet. You can view the audit logs to know the details of the login.

Offline: The account does not log in the Server at present.

Disabled: The account is disabled by an administrator and cannot log in the Server either from the Console or from browsers.

Date Created: The time when the account is added.

Date Logged in: The time when the account logs in, from a Console or a browser.

Notes: The comments for the account.

Operation: The following list describes the operations:

Edit: Modifies the settings of the account. The settings are just the same as those when creating a new account.

Delete: Deletes the account. An account can be deleted only when the status is *Offline*.

Kick Out: Kicks the account out of the connection from the Console. This button is available only when the status is *Online (Console)*.

Adding an account

To add an account, follow the steps below:

1. Click **New Account** on the **User Management** page.

User Management / New User

Authentication type:

Username: Your account can contain only numbers, letters, and the following characters: _ , @ , . , and - ; 20-character maximum.

Password: 6-20 characters in length

Re-enter password:

Notes (optional): At most 256 characters in length

Type:

☐ Disabled account

OK Cancel

Choose an authentication type, which could be Local, Radius, LDAP. For local authentication, it is required to enter the password. For Radius and LDAP authentication, it is required to configure authentication settings on the Authentication Settings page.

Enter the user name, the password for the account, and the notes.

Select the account type:

Administrator: An administrator has the administrator authority, can login the Server from both the Console and browsers, and can configure the Server and the link properties.

User: A user can login the Server from the Console, but cannot configure the link settings.

Auditor: An auditor can only login the Server from browsers, but can only view the audit logs.

Click **OK** to completely add an account.

User privilege

If the account type is User, you can allocate privileges to it, as the screenshot below:

Type:

Privilege type:

Privileges

Link Monitor	Link Analysis	View Alarm Logs	View Reports	Download Packets
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Limit length to <input type="text" value="65535"/> bytes

☐ Disabled account

The privilege can be based on nChronos Server or based on network link. If the privilege is based on nChronos Server, the user has same privileges on all network links on that server, including the network links created later. If the privilege is based on network link, it is required to allocate privileges for each network link.

The privileges include Link Monitor, Link Analysis, View Alarm Logs, View Reports, and Download Packets. The following list describes the details for each privilege:

Link Monitor: Link real-time monitor, and application real-time monitor on that link.

Link Analysis: Link retrospective analysis, millisecond analysis, as well as application performance analysis and application transaction analysis on that link.

View Alarm Logs: View the alarm logs on link/application real-time monitor, on the alarm view on link/application/transaction analysis, and on the Alarm window.

View Reports: All features on the Report window.

Download Packets: Packet download feature and the feature to use Expert Analyzer. To download packets, it is required to set up the packet length. If the stored packet length is greater than download packet length, then take the download packet length as the standard; if the stored packet length is less than download packet length, then take the stored packet length as the standard.

Modifying an account

When you want to modify the type of an account or disable an account, click **Edit** on the **User Management** page, and then select the appropriate type to modify the account type or select **Disable** to disable it.

Authentication Settings

This page is for configuring authentication settings and shows as the following figure:

Authentication Settings

☒ Enable third-party authentication

☐ Radius authentication

Authentication address: 192.168.9.143 Authentication port: 1812
Billing port: 1813 Key: 213
Encryption type: CHAP Time-out: 5 second(s)
Retry count: 3

☒ LDAP authentication

Server type: Microsoft AD Protocol version: 2
Authentication address: 192.168.9.143 Authentication port: 389
Username: administrator Password:
Domain: test.colasoft.com Time-out: 30000 second(s)
Chase referrals: Enable Base DN: DC=test,DC=colasoft,DC= Obtain DN

Test

OK

Users can enable Radius authentication or LDAP authentication.

Radius authentication

The following list describes the options for Radius authentication.

Authentication address: IP address of Radius server.

Authentication port: The port number is 1812 by default, and can be modified.

Billing port: The port number is 1813 by default, and can be modified.

Key: The share key between nChronos Server and Radius server.

Encryption type: The encryption type for passing the share key between nChronos Server and Radius server.

Time-out: The time of user authentication for nChronos Server and Radius server.

Retry count: The connection number that nChronos Server tries when the connection to Radius server fails.

LDAP authentication

The following list describes the options for LDAP authentication.

Server type: LDAP server type.

Protocol version: LDAP protocol version.

Authentication address: IP address of LDAP server.

Authentication port: User authentication port number provided by LDAP server.

Username: The user account with the permission to access LDAP server user privilege. Generally speaking, it is an administrator account.

Password: Password for the user account.

Domain: Domain address of the authentication user.

Time-out: The timeout time for connecting to LDAP server.

Chase referrals: The status of the parameter Chase referrals on LDAP server.

Base DN: The user group of the user to be authenticated on domain server. You can click Obtain DN to quickly configure all user group root directory on domain server, and then set up the user OU to be authenticated.

Certificate

This page is provided to update digital certificate, and shows as the following figure:

Certificate

Issuer	Subject	Valid (From)	Valid (To)	Version
CN= Colasoft-CA	C= US S= OK L= Tulsa O= Colasoft LLC CN= nChronos.colasoft.com	01/28/2013 02:28:50	01/28/2018 02:38:50	V3

Update

By default, there is a certificate file provided by Colasoft. You can also update the certificate.

To update the certificate, click **Update** on the **Certificate** page and upload the certificate file and the corresponding key file.

Update Certificate

Certificate File:

Select(.crt)

Key File:

Select(.key)

Update

Cancel

Security Policy

This page is provided to set the security policies, as the following figure:

Security Policy

Lockout policy

IP lockout threshold:

3

(counts)

IP lockout duration:

10

(minutes)

Reset IP lockout counter after:

10

(minutes)

This policy setting determines the number of failed logon attempts that causes an IP address to be locked out.

When an IP reached failed logon attempts, the IP address will be locked out.

A user cannot log on the Server with a locked-out IP address until the IP address is unlocked by an administrator or until the lockout duration has expired.

You can set a value between 1 and 999.

This policy setting determines the number of minutes a locked-out IP address remains locked out before automatically becoming unlocked. This policy setting only has meaning when the IP lockout threshold is specified.

The available range is from 0 to 9,999 minutes.

If you set the IP lockout duration to 0, the IP address will be locked out until the Server restarts.

This policy setting determines the number of minutes that must elapse after a failed login attempt before the failed logon attempt counter is reset to 0 login attempts.

This policy setting only has meaning when an IP lockout threshold is specified.

The available range is 1 minute to 9,999 minutes. This reset time must be less than or equal to the IP lockout duration.

☒ Client access control

Access control list:

192.168.9.0/24
192.168.5.0/24

Example for whitelist IP Address format:

IP address/mask: 192.168.0.0/24 or 192.168.0.0/255.255.0 or 2001:3e0::/80

IP address range: 192.168.0.0-192.168.1.255 or 2001:3e0::0001-2001:3e0::0005

Single IP address: 192.168.0.100 or 2001:3e0::0001

One IP or IP range per line. Use "Enter" to separate multiple IPs or IP ranges.

Segment can not be the same.

OK

Unlock

By default, IP lockout threshold is 3 times, IP lockout duration is 10 minutes, and lockout counter is 10 minutes. You can modify the default settings.

Following list describes the three parameters:

Copyright © 2024 Colasoft. All rights reserved.

31

IP lockout threshold: This option determines the number of failed login attempts that causes the IP of the computer where a user attempts to login the Server to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 1 and 999 failed login attempts.

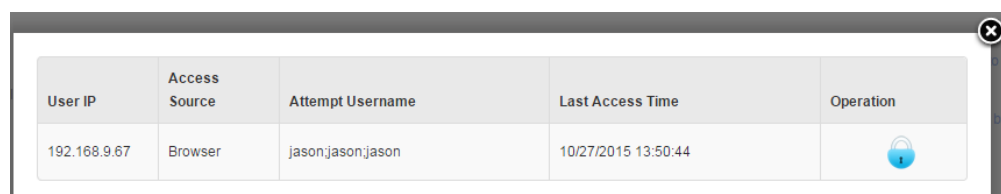
IP lockout duration: This option determines the number of minutes a locked-out IP remains locked out before automatically becoming unlocked. The available range is from 0 minute through 9,999 minutes. If you set the IP lockout duration to 0, the IP will be locked out until the Server restarts.


Reset IP lockout counter after: This option determines the number of minutes that must elapse after a failed login attempt before the failed login attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 9,999 minutes.

Viewing locked IP addresses

When an IP is locked, an administrator can view the lock information.

To view the lock information, click **Unlock** on the **Security Policy** page; and the unlock page pops up, which appears as below:



User IP	Access Source	Attempt Username	Last Access Time	Operation
192.168.9.67	Browser	jason;jason;jason	10/27/2015 13:50:44	

User IP: The IP address where the user attempts to login.

Access Source: Shows the user attempts to login the Server from a Console or a browser.


Attempt Username: Shows which accounts with which the user attempts to login the Server.

Latest Access Time: Shows the latest access time.

Operation: Unlock the IP.

Except the locked IP addresses, but the unlock page also lists the IP addresses that are not locked but failed to login the Server in the IP lockout threshold.

Unlocking an IP

To unlock a locked IP, click **Unlock** to open the unlock page and click .

Client access control

When the option Client access control is enabled, the connections to nChronos Server are only available for the IPs on the control list. Both IPv4 and IPv6 are supported.

Audit Log

This page lists all event logs, for example, which user logs in or logs out the Server, from the Console or from browsers, and other events, as the following figure:

Audit Log

Type Time - Content

No.	Type	Time	User	Event
5748		08/27/2017 10:29:41	qc	Logged out from console(172.16.12.16).
5747		08/27/2017 10:29:41	N/A	System Alarm[3241]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5746		08/27/2017 10:29:41	N/A	System Alarm[3240]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5745		08/27/2017 10:29:41	N/A	System Alarm[3239]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5744		08/27/2017 10:29:41	N/A	System Alarm[3238]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5743		08/27/2017 10:29:41	N/A	System Alarm[3237]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5742		08/27/2017 10:29:41	N/A	System Alarm[3236]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5741		08/27/2017 10:29:41	N/A	System Alarm[3235]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5740		08/27/2017 10:29:41	N/A	System Alarm[3234]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5739		08/27/2017 10:29:41	N/A	System Alarm[3233]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5738		08/27/2017 10:29:41	N/A	System Alarm[3232]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5737		08/27/2017 10:29:41	N/A	System Alarm[3231]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5736		08/27/2017 10:29:41	N/A	System Alarm[3230]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5735		08/27/2017 10:29:41	N/A	System Alarm[3229]: Capture Interface dpdk port 0 has packet-loss. Please modify you capturing strategy.
5734		08/27/2017 10:29:41	admin	Logged in from browser(172.16.17.2).

Total 384 page(s), 5748 record(s), current page 1

You can view the event logs by page turning via the buttons , , , , and .

The following list describes the columns on this page.

No.: The number of the event. It starts from 1.

Type: The type of the event.

: Error.

: Warning.

: Information.

Time: The time when the event occurs.

User: The user who makes the event happen as well as the IP address of the computer which the user is using when happening the event.

Event: The details of the event.

Downloading the logs

You can download the logs for further use or reference. To download the log, click the button **Download**, and the logs will be saved automatically.

Filtering the logs

You can view the logs according to a specific type or according to time.

To view the logs according to types, follow the steps below:

1. Select an appropriate type from the **Type** drop-down list.

Click Filter.

To view the logs according to time, follow the steps below:

1. Click the first box of **Time** and specify a time.
2. Click the second box of **Time** and specify a time.
3. Click **Filter**.

You can also view the logs both according to types and time simultaneously.



The filter function is a display filter function.

Time Synchronization

This page is provided to synchronize date and time and shows as the following figure:

Time Synchronization

☐ Manual setup

Time zone: (UTC-05:00) Eastern Time (US & Canada) ▼

Time: 09/30/2016 13:43:56

☒ NTP Internet time server

Server: 192.168.9.171 ▼

The system will be reset upon changing time synchronization settings. For the synchronization via Internet time server, the clock will be synchronized with the time server every minute.

OK

To get precise analysis and statistics, you can set the reference time. There are two methods to synchronize the clock.

Manual synchronization

To manually set the time, follow the steps below:

1. Select **Manual settings**.

Select a time zone and enter the appropriate time.

Click **OK**.

NTP synchronization

To synchronize with an Internet time server, follow the steps below:

1. Select NTP Internet time server.
2. Select an Internet time server.
3. Click **OK**.



The data will be reset and the services will be restarted upon changing time synchronization settings. For NTP synchronization, the clock will be synchronized with the time server every minute.

Server Status

This page is for displaying the usage of CPU, memory, and storage as screenshot below:

Server Status



Status Configuration

You could click button "Settings" to configure the figures for normal, high, severe for CPU, memory, and storage usage. The system default is set as below:

Status Configuration

CPU Usage:

Normal <	50	%	≤ High	70	%	Severe
----------	----	---	--------	----	---	--------

Memory Usage:

Normal <	50	%	≤ High	70	%	Severe
----------	----	---	--------	----	---	--------

Storage Usage:

Normal <	50	%	≤ High	70	%	Severe
----------	----	---	--------	----	---	--------

OK Cancel

Server Information

This page provides the basic information of nChronos Server:

Server Information

Product information	
Name:	Colasoft nChronos Server
Version:	1.0.0.0
Edition:	Standard

License information	
Activation status:	Activated
Serial number:	0000-0000-0000-0000-0000-0000-0000-0000 Reactivate
Licensed to:	
Storage capacity:	163840GB
Maximum analysis throughput:	15000Mbps
Maximum capture interfaces:	8
Maximum network links:	4
Concurrent connections to Server:	
Maximum monitored applications:	
Maximum analyzed transactions:	

Product information

The Product information section provides information about the software product:

Name: The name of the software.

Version: The version of the software.

Edition: The edition of the software.

License information

The License information section displays the license information of the software product, including the storage capacity, the maximum analysis throughput, the maximum network interfaces, the

maximum network links, the concurrent connections to a Server, the maximum user accounts, and so on. All those specifications are determined by the license.

Server Management

This page is for managing the Server and displays the running information:

Server Management

Status Information	
Start time:	08/03/2017 18:44:34
Running time:	04:35:08
SSH remote access:	<input checked="" type="checkbox"/> ON
System status monitor log:	<input type="checkbox"/> OFF <small>Colasoft nChronos will send System Status Log every minute.</small>
Analyze original packet length:	<input type="checkbox"/> OFF

Refresh

Export Config

Import Config

Reset

Restart Service

Restart Server

Shut Down

Start time: The time when the service starts.

Running time: The service running time.

SSH remote access: The status of SSH remote access. This function is enabled by default, users can turn it on or off. When it is on, the default port number is 22.

System status monitor log: Whether to send system status monitor log as syslog. Users can turn it on or off. By default, it is off. If users want to send the system status monitor log, users should first go to the **Alarm Notification** page to configure Syslog parameters.

Analyze original packet length: When this option is ON, the system will do the statistics based on the packet length that is not truncated; when this option is OFF, the system will do the statistics based on the truncated packet length.

Buttons

The following list describes the buttons at the bottom of this page:

Refresh: Refreshes the current page.

Export Config: Exports all current configurations of the Server to be a *.dat file, including all Server configurations on the web side and all network link properties on the Console side. You are recommended to export configurations after completing the configuring so as to back up the Server configurations for further use.

Import Config: Imports the configuration file saved before to replace current configurations. Upon the successful import of the configuration file, the service will be restarted.

Reset: Empties all data except configurations, which means the captured packets, statistics, and logs are all deleted. After resetting the server, the service will be restarted.

Restart System: Restarts nChronos service. No data will be deleted.

Restart Server: Restarts the machine where nChronos Server is installed.

Shut Down: Powers off the machine where nChronos Server is installed. Therefore, the connection between nChronos Server and nChronos Console will be cut down certainly.

Console User Interface

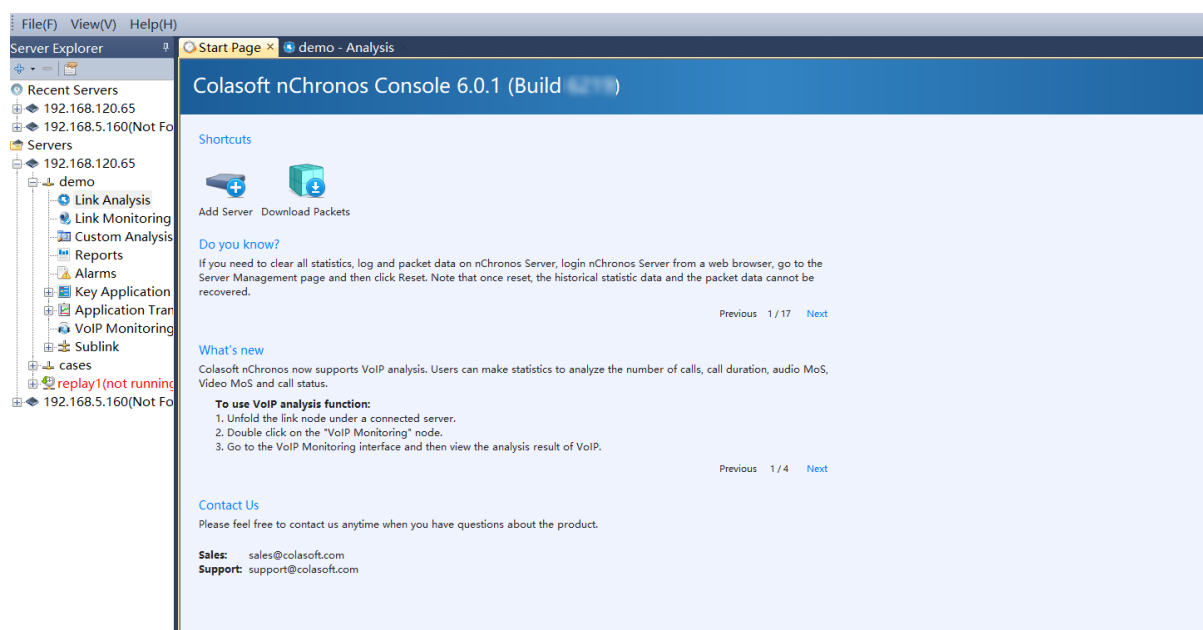
As the data presentation platform, nChronos Console contains three parts: the menu bar, the server explorer, and the start page, and appears as the following figure.

Menu bar

Server explorer

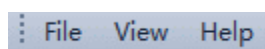
Start Page

System Alert



Menu bar

The Menu bar generally includes four menus, as the following figure:



The File menu

Download Packets: Opens the Download Packets dialog box to download packets from nChronos Servers. For information on how to download packets, see Downloading packets.

Options: System options.

Exit: Exits the program.

The View menu

Start Page: Shows or hides the Start Page.

Explorer: Shows or hides the Explorer pane.

Close Current Window: Closes currently active window.

Close All Windows: Closes all open analysis windows and leaves the Start Page open.

Display Statistics as:

Number: Displays statistics as number.

Auto Format: Displays statistics as auto format.

Show MAC Address as:

Address: Shows MAC address as hexadecimal digits, e.g. *AA:BB:CC:33:44:55*.

Name: Shows MAC address as name, e.g. *localhost*.

Address and Name: Shows MAC address as hexadecimal digits and name, e.g. *AA:BB:CC:33:44:55[localhost]*.

Show IP Address as:

Address: Shows IP address as decimal digits, e.g. *192.168.1.1*.

Name: Shows IP address as name, e.g. *localhost*.

Address and Name: Shows IP address as decimal digits and name, e.g. *192.168.1.1[localhost]*.

Show Adapter Manufacturer: Shows or hides the manufacture of network adapters, e.g. *Intel-AA:BB:CC*.

Manage Downloads and Expert Analysis: Shows the Manage Downloads and Expert Analysis dialog box to display the download and expert analysis history.

View Style: Choose the display style for the analysis views. The background can be black or white.

The Help menu

Content: Launches Help file of .chm format and show the Content page.

Search: Launches Help file of .chm format and show the Search page.

Index: Launches Help file of .chm format and show the Index page.

Activate: Follow the Activation Wizard to activate nChronos Console.

Colasoft Home Page: Goes to the home page of Colasoft website.

Forum: Goes to the technical forum.

About: To view the production information and license file

Start Page

The Start Page is the main interface you see when launching nChronos Console, providing tips, features and other information about the program.

The Start Page shows as following screenshot.

Colasoft nChronos Console 6. (Build)

Shortcuts



Add Server Download Packets

Do you know?

If you need to clear all statistics, log and packet data on nChronos Server, login nChronos Server from a web browser, go to the Server Management page and then click Reset. Note that once reset, the historical statistic data and the packet data cannot be recovered.

Previous 1 / 17 Next

What's new

Colasoft nChronos now supports VoIP analysis. Users can make statistics to analyze the number of calls, call duration, audio MoS, Video MoS and call status.

To use VoIP analysis function:

1. Unfold the link node under a connected server.
2. Double click on the "VoIP Monitoring" node.
3. Go to the VoIP Monitoring interface and then view the analysis result of VoIP.

Previous 1 / 4 Next

Contact Us

Please feel free to contact us anytime when you have questions about the product.

Sales: sales@colasoft.com

Support: support@colasoft.com

Shortcuts: This part provides two default shortcuts, and you can also add a shortcut onto the shortcuts part. You can click the shortcut icons to quickly add a server, or to download packets. To add a shortcut here, right-click the appropriate items on the left explorer pane and click Create Shortcut.



Do you know: This part provides some tips when you use the program.

What's new: This part provides some features of the program and guides you to experience these features step by step.

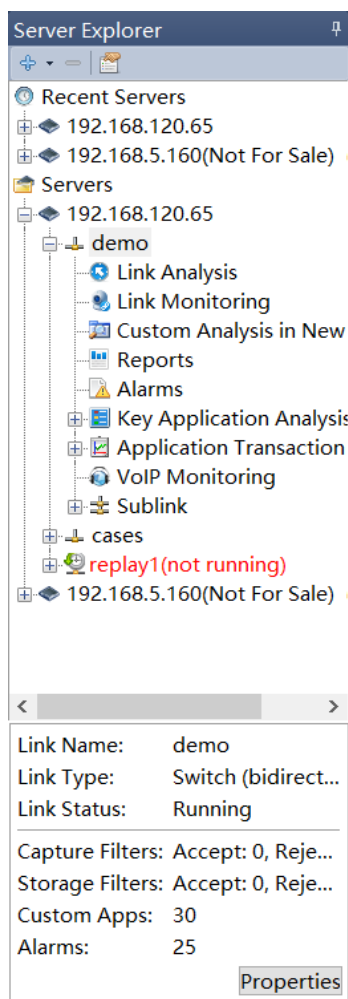
Contact Us: This part provides some contact information. Please feel free to contact us when there are problems.

Server Explorer


The server explorer is at the left side of the program. You can hide it when you want to get a bigger view of the analysis view.

To hide the server explorer, just click  at the top-right corner, and it will shrink into a thin bar to dock at the left side of the program. If you want to show it, just click **Server Explorer** on the thin bar, and click  at the top-right corner to fix it.

The server explorer is for managing nChronos Servers. Once an nChronos Server is added to a Console, it will be displayed:




The list below describes the icon buttons on the Server Explorer.

: Adds a Server or a server group to the Console. For information about operations on a Server, see Managing Servers.

: Removes the selected Server from the Explorer pane.

: Views the properties of the selected item.


 


The icon  indicates server groups for containing Servers.

The icon  indicates nChronos Server.

The icon  indicates network links.

Hiding and showing server explorer


To hide server explorer, just click  at the top-right corner of the server explorer pane, and the server explorer pane will shrink into a thin bar to dock at the left side of the program.


If you want to show the server explorer pane, click  to fix it.

System Alert

nChronos provides system alerts. When the system alerts are triggered, the alert logs will pop up from the lower right corner of the Console user interface, as the screenshot below:



Users can double click the button  to hide this window. You can click the button to toggle the window.

Users can click the button  in front of the alert log to acknowledge the alert log, and then the alert log will be removed from the window.

The Audit Log page from server's webpage displays all triggered system alert logs.

There are six types of system alerts:

Unauthorized IP address access. Unauthorized IP address tries to access nChronos Server. Users can specify which IP addresses have the permission to access the server on the Security Policy page on server's webpage.

User access failure. Users fail to access the server due to invalid username or password and the IP address are locked. Users can configure the lock policy on the Security Policy page on server's webpage.

nChronos Server accident disconnection from the Analysis Center.

Server reboot by accident.

Poor capture performance.

Poor analysis performance.


Adding and connecting nChronos Server

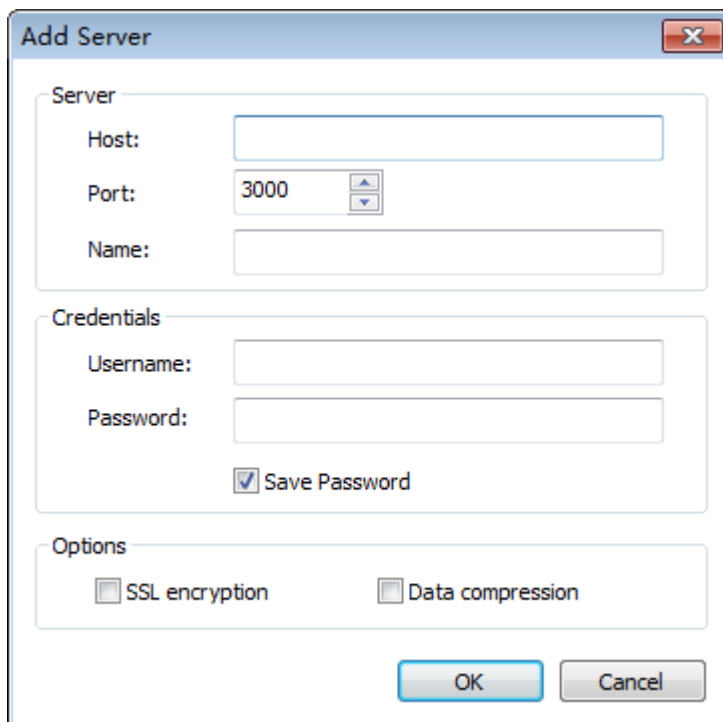
To view the statistics and analysis data through the Console, we must add nChronos Server.

Adding nChronos Server

To add nChronos Server, follow the steps below:

1. On the Server Explorer, click the server group which the server to be added belongs to.

Click  and click **Add Server**; the **Add Server** dialog box appears.



The **Add Server** dialog box is shown with the following fields and options:

- Server**
 - Host: Text input field
 - Port: Spin box with 3000 selected
 - Name: Text input field
- Credentials**
 - Username: Text input field
 - Password: Text input field
 - ☒ Save Password
- Options**
 - ☐ SSL encryption
 - ☐ Data compression

Buttons: **OK** and **Cancel**

Complete the dialog box. See the following list of each label for more information.

Host: The IP address of the management interface on nChronos Server.

Port: The port number for connecting to Server. It is 3000 by default.

Name: A readable name for identifying the Server, for example, Marketing Dept. It will be the same as the IP address if you don't enter one.

Username: The account for logging the Server.

Password: The password for the account.

SSL encryption: Applies SSL encryption when transmitting data from the Server to the Console.


Data compression: Compresses the data in the transmission from the Server to the Console.

Click **OK** after completing the **Add Server** dialog box. Then the added server will display under the Server Group on the Server Explorer.

Connecting nChronos Server

To connect to nChronos Server, do one of the following:

Double-click the server name of the Server that you want to connect.

Click the server name of the Server that you want to connect, and then click  in front of it.

Click the server name of the Server that you want to connect, and then click the button **Connect** at the bottom of the Server Explorer.

Right-click the server name of the Server that you want to connect and click **Connect**.


Configuring Network Link

Network links are created to capture the traffic over the network, define inbound network segments to thereby define internal IP addresses, and set the bandwidth of the network. Therefore, to capture useful packets and obtain effective analysis and statistics, you may need to set the network links before monitoring or analyzing them.

After connecting nChronos Server, the network links belonging to the Server automatically displays under the Server.

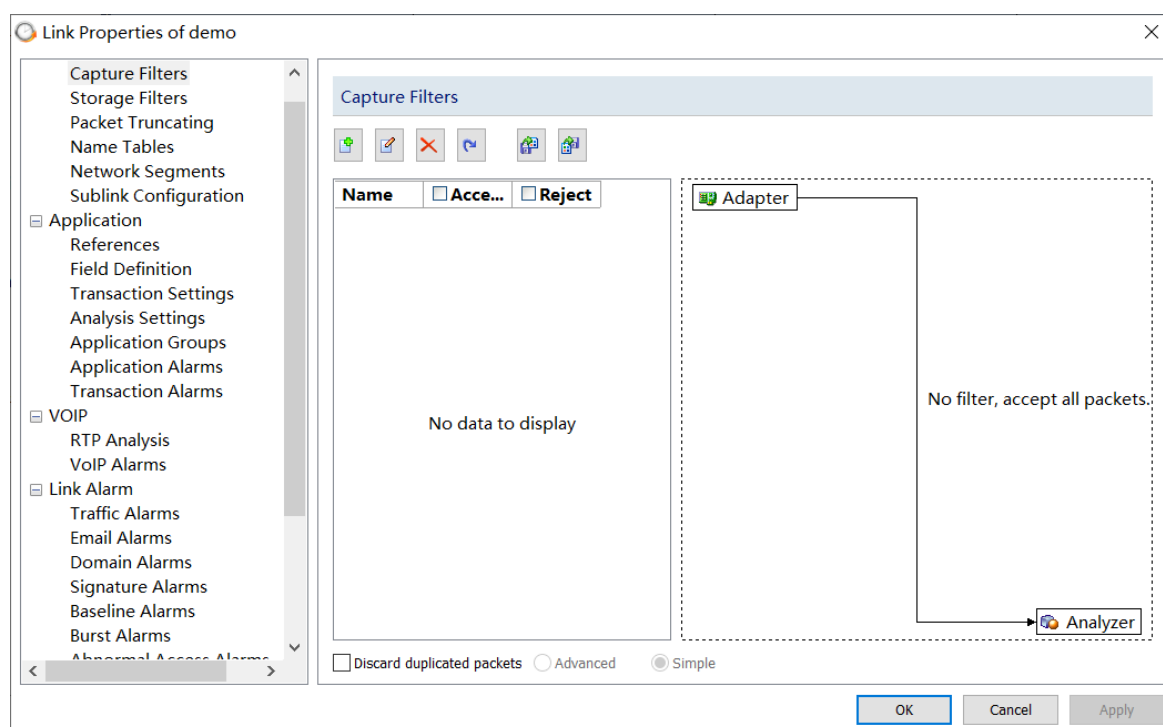
To configure a network link, do one of the following:

Right-click the network link and select **Properties** to open the **Link Properties** dialog box.

Click the network link, and then click  on the top of the Server Explorer to open the **Link Properties** dialog box.

Click the network link, and then click the button **Properties** at the bottom of the Server Explorer to open the **Link Properties** dialog box.

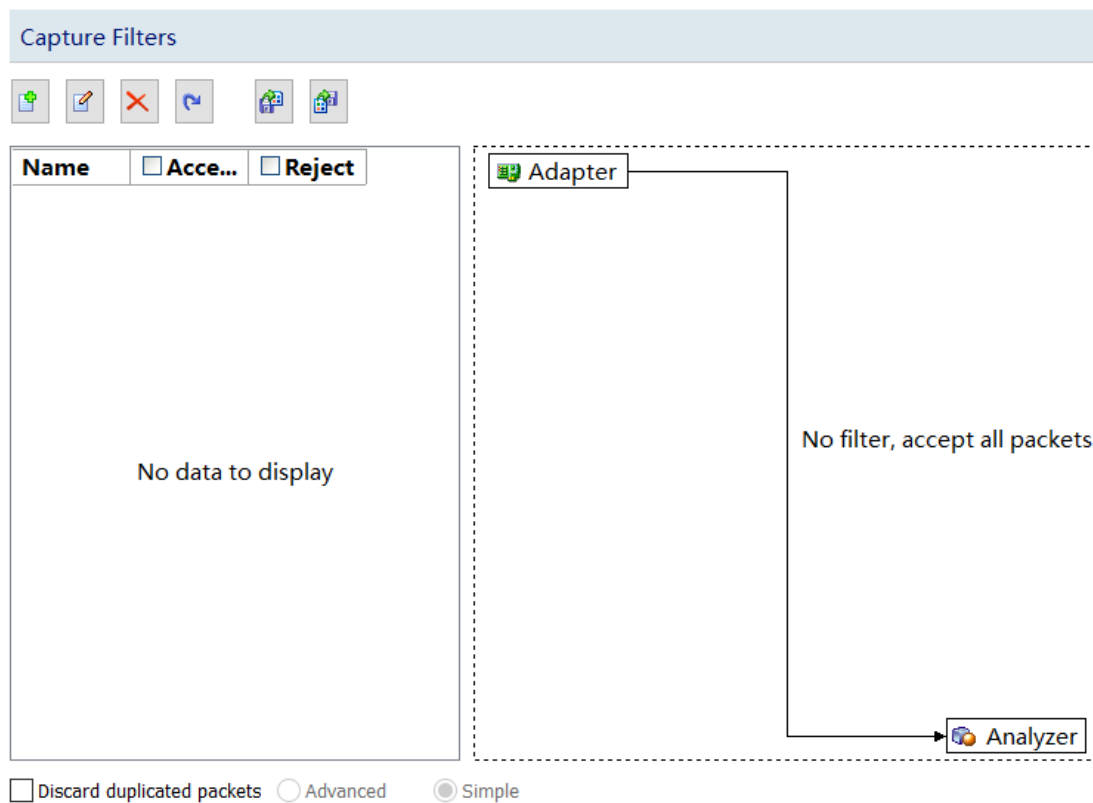
The **Link Properties** dialog box shows as the following figure:



Note Link properties are specific to a network link, regardless of the Console on which the settings are made. Furthermore, the network properties under one nChronos Server could have different settings.

Capture Filters

Capture filters are used to filter out the packets that do not meet the requirements. There are two panes on the **Capture Filter** tab, the left pane and the right pane, as the following figure:



The left pane lists all filters, including default filters and custom filters. For each filter, there are two options, *Accept* and *Reject*. *Accept* means only packets matching the filter will be saved and analyzed, while *Reject* means only packets unmatched will be saved and analyzed. All selected filters are in OR relationship.

The right pane is filter flow chart which shows all selected filter items on the filter list, including *Accept* ones and *Reject* ones. It refreshes upon any changes on the filters. You can double-click a filter on the flow chart to edit it.

Buttons

There are six buttons for setting capture filters.



: Creates a new filter.



: Edits the selected filter.



: Deletes the selected filter.



: Resets the filter to default.




: Imports saved filter files to current filter list. When a filter file was imported, all the filters in current list will be removed.



: Saves all filters in current filter list to disk.

Adding a filter

To add a filter, just click  and then complete the **Capture Filter** dialog box.

For more information about adding simple filters, see [Creating a simple filter](#).

For more information about adding advanced filters, see [Creating an advanced filter](#).

Applying a filter

To apply a filter, just select the **Accept** or **Reject** checkbox, and then click **OK** on the dialog box. Accept means only packets matching the filter will be captured, while Reject means only packets unmatched will be captured.


Discard duplicate packets

Capture Filter allows you to discard duplicate packets. When there are two or more copies of the same packets, only one copy of them will be analyzed and other copies will be discarded. There will be lots of duplicate packets in a misconfigured port mirroring (SPAN) environment, which has bad influence on normal network analysis. Discarding duplicate packets can improve analysis accuracy and save storage space.

There are two methods to discard duplicate packets: **Simple** and **Advanced**:


Simple: This rule identifies the duplicate packets based on source IP address, destination IP address, and IP ID. If two packets have identical source IP, destination IP, and IP ID, then only one packet will be analyzed, and the other one will be discarded.

Advanced: This rule identifies the duplicate packets based on source IP address, destination IP address, source MAC address, destination MAC address, IP ID, and checksum. If two packets have identical source IP, destination IP, source MAC address, destination MAC address, IP ID, and checksum, then only one packet will be analyzed, and the other one will be discarded.

-  **Note** It is recommended to enable the Discard duplicate packets function only when it is very necessary because it has big impact on the storage performance.

Creating a Simple filter

To create a simple filter,

1. Click  on the Capture Filter tab to open the **Packet Filter** dialog box.

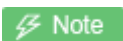
On the Simple **Filter** tab of the **Packet Filter** dialog box, enter the name and the description for the filter, and specify the color for the filter, just like the following figure:

Select the **Address rule** checkbox to define an address rule for the filter.

Select the **Port rule** checkbox to define a port rule for the filter.

Select the **Protocol rule** checkbox to define a protocol rule for the filter.

At last, click **OK** on the Packet Filter dialog box.

-  **Note** When a filter is defined with an address rule, a port rule and a protocol rule, they are connected by logical AND statements. That is, packets must match all of the rules to match the filter.

Defining address rules

To define an address rule, follow the steps below:

1. Select the Address rule checkbox.

Select an address type from **Endpoint1** and enter the address in the textbox below the address type.




Click the direction drop-down list box to select packet transmission direction between the two addresses.

- Endpoint 1 -> 2:** This option indicates the packets transmitted from the address 1 to the address 2.

Endpoint 2 -> 1: This option indicates the packets transmitted from the address 2 to the address 1.

Endpoint 1 <-> 2: This option indicates the packets transmitted from the address 1 to the address 2 or from the address 2 to the address 1.

Select an address type from Endpoint2 and enter the address in the textbox below the address type. Click OK on the Packet Filter dialog box.

 **Tips** Click the icon  to get references if you are not familiar with address format. Click the icon  to delete all items entered before.

Defining port rule

To define a port rule, follow the steps below:

Select the **Port rule** checkbox.

Select a port type from **Port1** and enter the port number in the textbox below the port type.

Click the direction drop-down list box and select packet transmission direction between the two ports.

Port 1 -> 2: This option indicates the packets transmitted from the port 1 to the port 2.

Port 2 -> 1: This option indicates the packets transmitted from the port 2 to the port 1.

Port 1 <-> 2: This option indicates the packets transmitted from the port 1 to the port 2 or from the port 2 to the port 1.

Select a port type from **Port2** and enter the port number in the textbox below the port type.

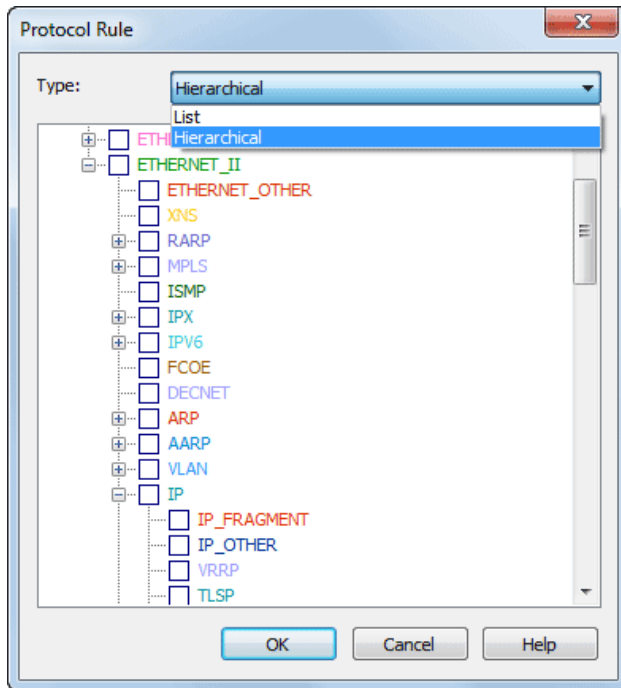
Click **OK** on the **Packet Filter** dialog box.

Defining protocol rule

To define a protocol rule, follow the steps below:

1. Select the Protocol rule checkbox.

Click Select to open the Protocol Rule dialog box which appears as below.




Choose the appropriate protocols and click OK.

Click OK on the Packet Filter dialog box.

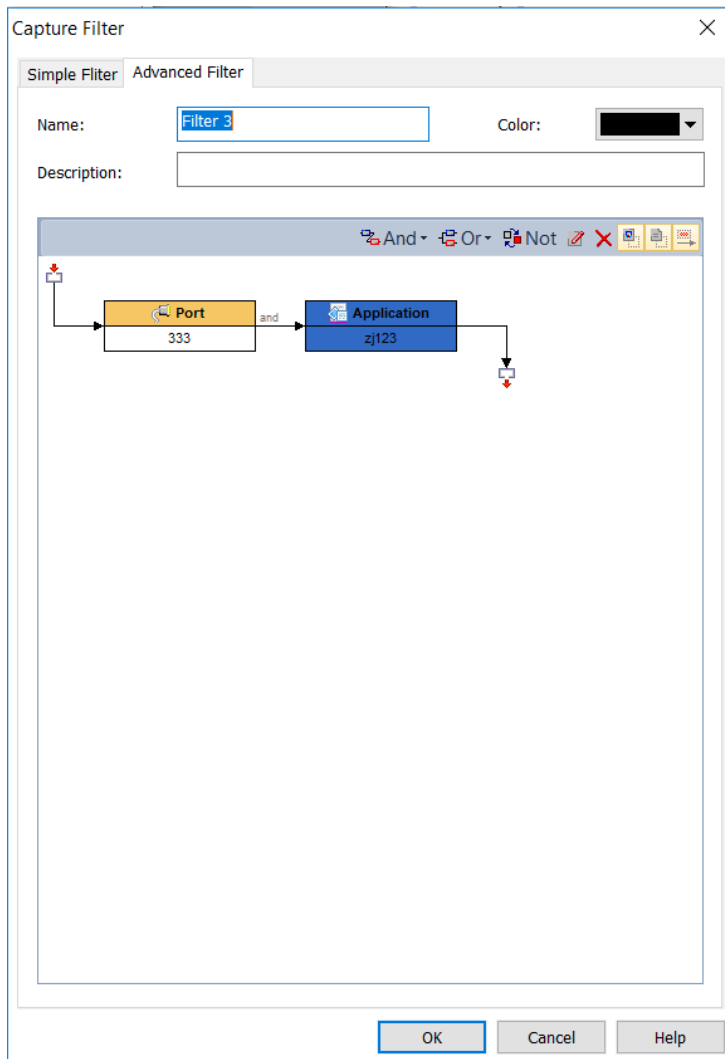
The chosen protocols are listed in Protocol Rule section. You can delete a protocol item from the list with the Remove button.

Creating an advanced filter

To create an advanced filter,

Click  on the Packet Filter tab to open the **Packet Filter** dialog box.

On the **Advanced Filter** tab of the **Packet Filter** dialog box, enter the name and the description for the filter, and specify the color for the filter, just like the following figure:





The toolbar contains the following items:

And: The rules connected by "and" are in logical AND relationship.

Or: The rules connected by "or" are in logical OR relationship.


Not: Only packets unmatched the condition will be captured. The Not rules are marked as red ones.

: Edits the selected rule.

: Deletes the selected rule.

: Shows the icon for each rule.

: Shows the details of the rules.

: Shows the logical relationships of the rules.

The filter rules are arranged in a filter relation map. The map shows the logical relations among the rules from adapter to an analysis project. You can double-click the rule to edit it.

Click **And** to define a rule, which could be address rule, port rule, protocol rule, size rule, value rule and pattern rule.

Click **And** and **Or** to define other rules.

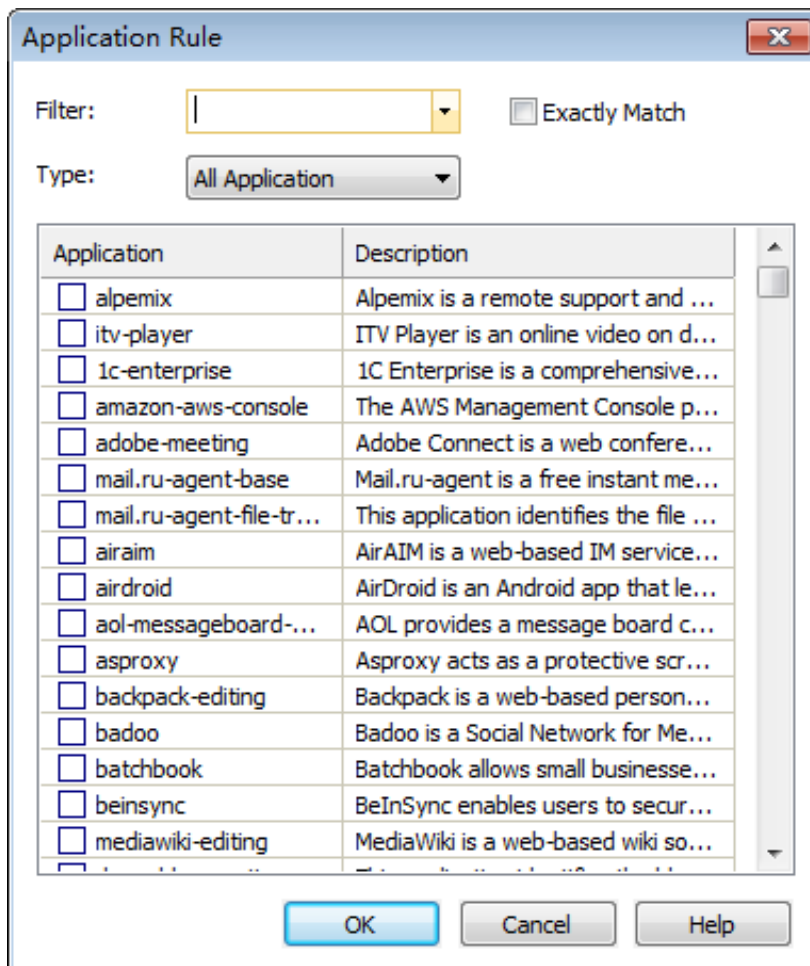
At last, click **OK** on the Capture Filter dialog box.

The Address, Port and Protocol rules are the same to those in simple filters (for more information about how to define these rules, see Simple filter).

Defining application rules

Application rule is for defining filter rules based on applications, which could be system applications and customized applications.

To define an application rule, click **And** or **Or** on the toolbar and select **Application** to open the **Application Rule** dialog box which appears as below.



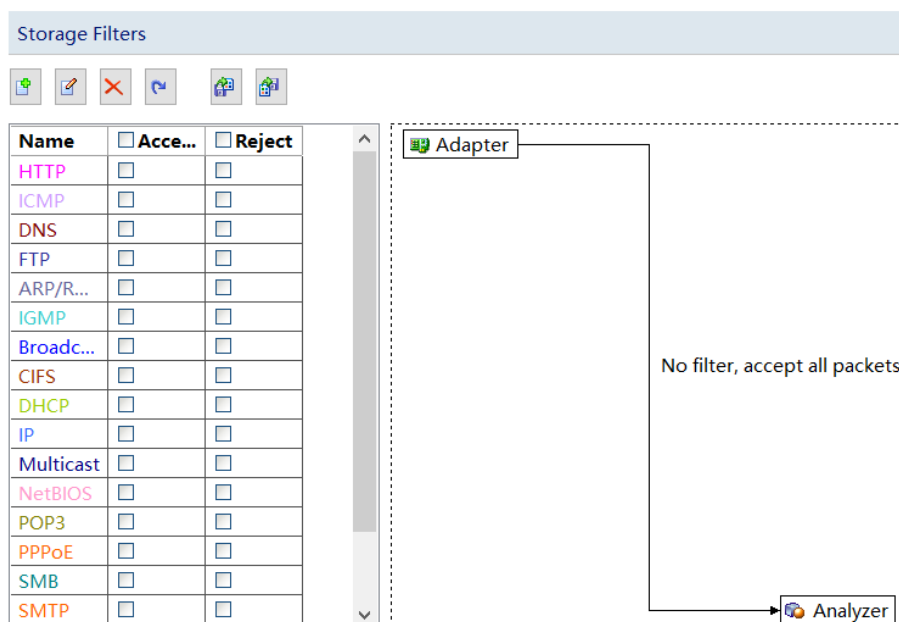
Check the desired applications and click **OK**. You can use the **Filter** box to make a search.

- **Note** Advanced filters can also be converted into simple filters, but some filter rules will be lost because advanced filters have more filter conditions than simple filters.

Storage Filters

The Storage Filter is provided to for users to store the packets that match the filters. For example, if you want to only store HTTP packets, you can enable a HTTP storage filter.

The Storage Filter tab is very much similar to the Capture Filter tab, as the following figure:

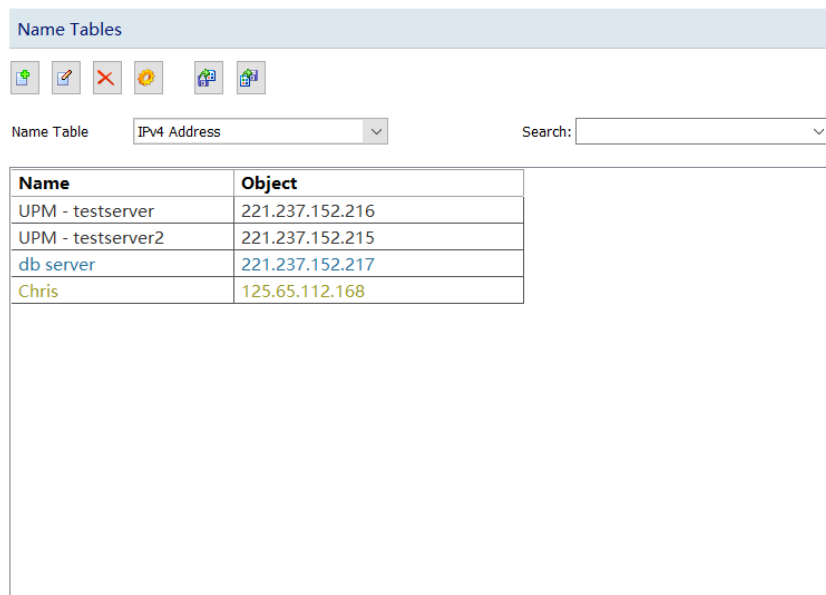


In addition to the similar interface, Storage Filter has the identical settings to the Capture Filter. For how to create a filter, please refer to Capture Filter.

Besides the filters, Storage Filter provides a functionality to truncate the stored packets to a specified size. Enable the Truncate checkbox on the bottom of this tab, and enter a number to specify the packet size.

Name Tables

The **Name Table** tab manages symbolic names for all MAC addresses and IP addresses. There are five types of name table: MAC Name Table, IPv4 Name Table which is only available for IPv4 analysis, IPv6 Name Table which is only available for IPv6 analysis, VLAN ID, MPLS VPN Tag. This tab shows as the following figure:



Buttons

The buttons on this tab are described as below:



: Adds a name for an address.



: Edits the selected item.



: Deletes the selected item.




: Sets name table options.

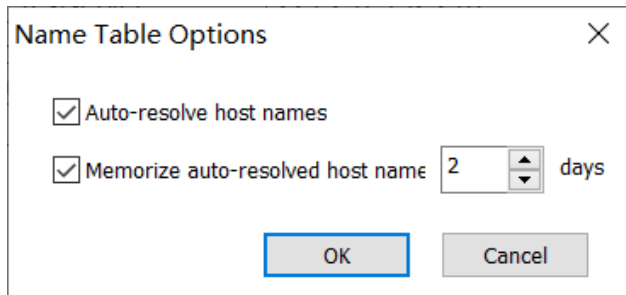


: Imports a name table file to current name list.



: Saves current name list to a .csta file.

Click , the Name Table Options dialog box appears.



Name Table Options [X]

☒ Auto-resolve host names

☒ Memorize auto-resolved host name 2 days

OK Cancel


Auto-resolve host names: Set whether to automatically resolve the names for the hosts.

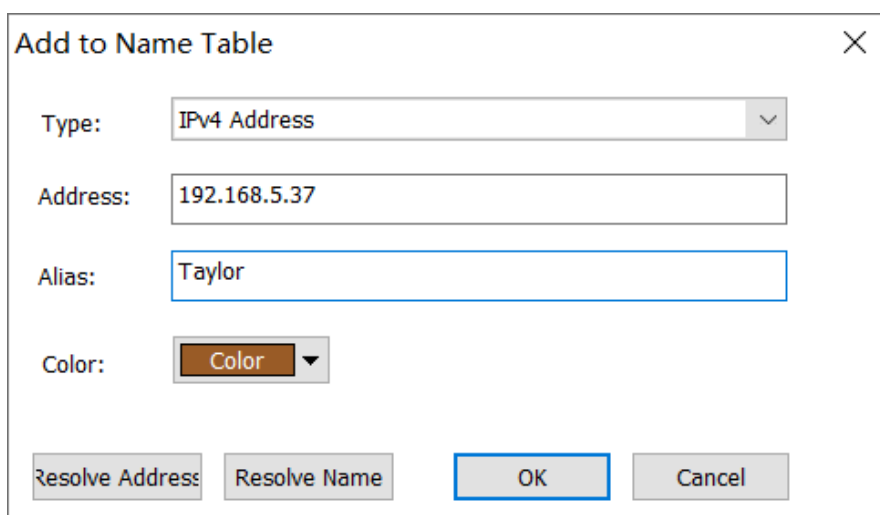
Memorize auto-resolved host names: Set the days to save auto-resolved host names.

Adding a name for an address

To add a name for an address, follow the steps below:

1, Choose the name type from the Name table type drop-down list. For example, if you want to add a name for an IPv4 address, you should choose IPv4 Name Table.

2, Click  to open the Add Name dialog box which appears below.



Add to Name Table [X]

Type: IPv4 Address

Address: 192.168.5.37

Alias: Taylor

Color: Color

Resolve Address Resolve Name OK Cancel

Enter the address, and the name for the address.

Click **OK** on the dialog box, and click **OK** on the Name Table tab.

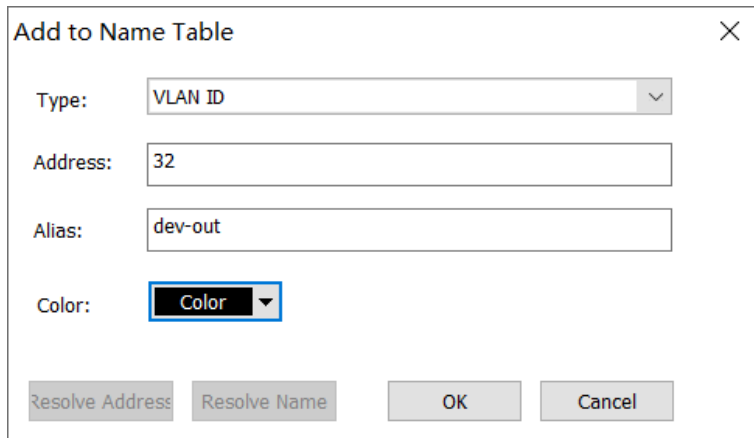
When you do not know the name for the address, you can use **Resolve Address** button to automatically resolve the address; or, when you do not know the address for a name, you can use **Resolve Name** button to automatically resolve the name.

Adding a name for VLAN ID

To add a name for a VLAN ID, follow the steps below:

Choose VLAN ID from the Name table type drop-down list.

Click  to open the **Add Name** dialog box which appears below.



The dialog box titled "Add to Name Table" contains the following fields and buttons:

- Type:** A dropdown menu with "VLAN ID" selected.
- Address:** A text input field containing "32".
- Alias:** A text input field containing "dev-out".
- Color:** A dropdown menu with "Color" selected.
- Buttons:** "Resolve Address", "Resolve Name", "OK", and "Cancel".

Enter the VLAN ID, and the name for the VLAN ID.

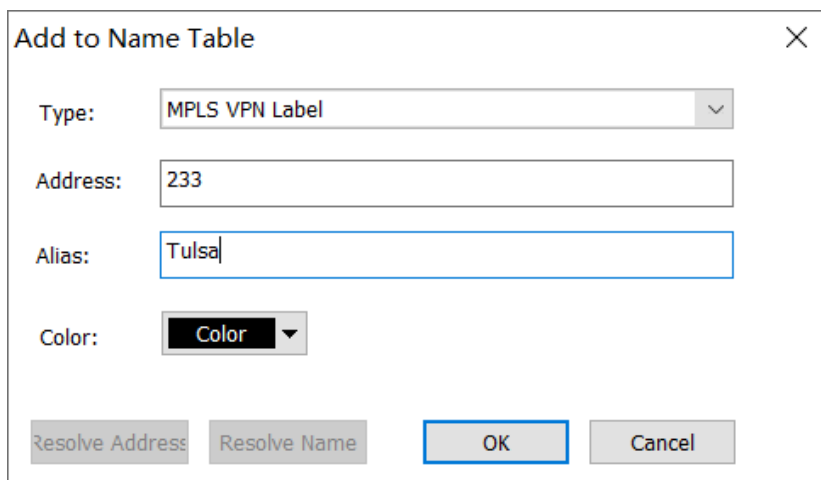
Click **OK** on the dialog box, and click **OK** on the **Name Table** tab.

Adding a name for VPN label

To add a name for a VPN label, follow the steps below:

1, Choose **MPLS VPN** Label from the Name table type drop-down list.

Click  to open the **Add Name** dialog box which appears below.



The dialog box titled "Add to Name Table" contains the following fields and buttons:

- Type:** A dropdown menu with "MPLS VPN Label" selected.
- Address:** A text input field containing "233".
- Alias:** A text input field containing "Tulsa".
- Color:** A dropdown menu with "Color" selected.
- Buttons:** "Resolve Address", "Resolve Name", "OK", and "Cancel".

Enter the VPN label, and the name for the VPN label.

Click **OK** on the dialog box, and click **OK** on the **Name Table** tab.

Adding a name for VXLAN ID

To add a name for a VXLAN ID, follow the steps below:

1. Choose VXLAN ID from the Name table type drop-down list.

Click  to open the **Add Name** dialog box which appears below.

Add to Name Table
✕

Type:

Address:

Alias:

Color:






Enter the VXLAN ID, and the name for the VXLAN ID.

Click **OK** on the dialog box, and click **OK** on the **Name Table** tab.

Packet Truncating

Packet Truncating configuration can truncate packets and store them to improve storage performance and save storage. The configuration interface shows as the screenshot below:

Packet Truncating

Type:
Search:

Ena...	Object	Type	Rule
No data to display			

☐ Truncate all packets to bytes

Buttons

The following list describes the buttons on this tab.



: Adds a new packet truncating setting.



: Edits the selected item.



: Deletes the selected item.



: Import packet truncating configuration from a file.

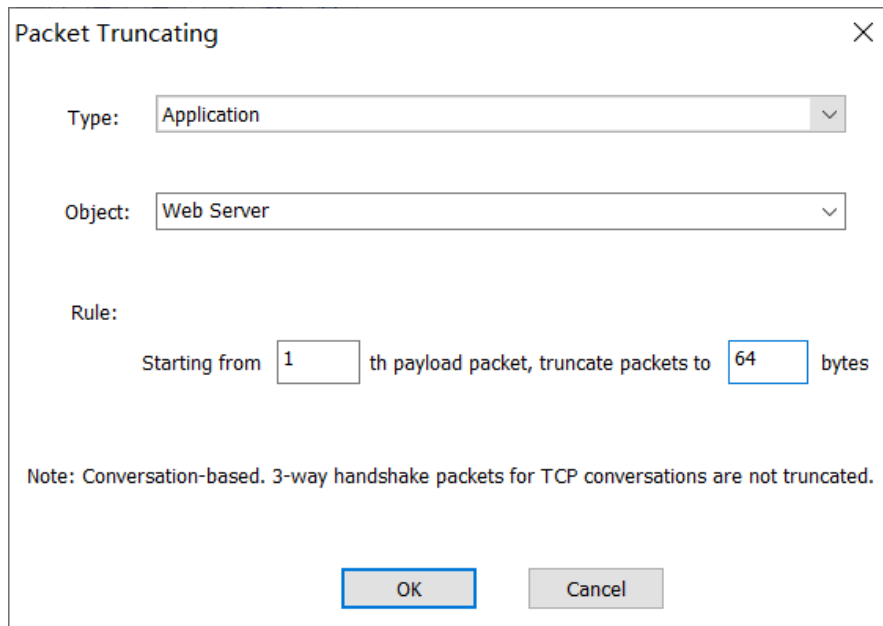


: Saves current configuration to a file.

Add Packet Truncating Configuration

To add a Packet Truncating configuration, follow the steps below:

1. Click  to open the **Packet Truncating** dialog box.



On the **Packet Truncating** dialog box, specify the type and object, and then enter the values for the rule.

Type: The object type of the packet truncating configuration.

Object: The object of the packet truncating configuration. For application and protocol types, objects are all selected from the drop-down list. For virtual interface type, directly input the virtual interface ID.

Rule: Starting from the first N payload packet, the packet is truncated to the specified length. The length range is 64 – 65535.

Click **OK** on the **Packet Truncating** dialog box, and then click **OK** on the **Packet Truncating** tab.

Network Segments

This tab lists all network segments and the rules of the segments, showing as the following figure:

Network Segments



☐ Enable System Segment

Type: Custom Network Segme

Search:

Na...	Geoloc...	T...	Rule	Segment Total Ba...	Segment Inbound Ba...	Segment Ou
UP...	Segme...	1	10.0.0.0/8	100	100	100
UP...	Segme...	1	221.237.152...	100	100	100
UP...	Segme...	1	192.168.0.0/...	100	100	100
UP...	CD	S...	192.168.1.0/...	200	100	100
UP...	Beijing	S...	171.0.0.0/8	200	100	100
UP...	Chengdu	S...	222.0.0.0/8;...	200	100	100
UP...	Shangh...	S...	125.0.0.0/8;...	200	100	100
UP...	HK Offi...	S...	118.0.0.0/8	200	100	100
UP...		vl...	100.0.0.4-10...	200	100	100
we...			192.168.8.0/...	100	100	100
sjl			192.0.0.0/8	100	100	100

Buttons

The following list describes the buttons on this tab.



: Adds a network segment.



: Edits the selected network segment.



: Deletes the selected network segment.



: Imports network segment customizations from a file.

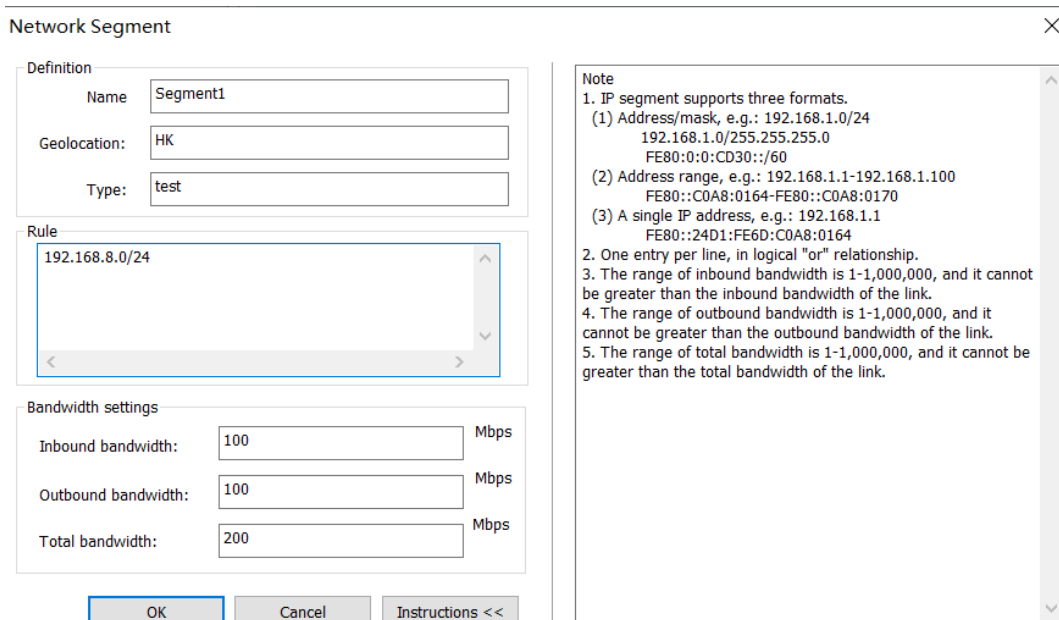


: Exports current network segment customizations to a file.

Adding a network segment

To add a network segment, follow the steps below:

1. Click  to open **New Segment** dialog box:



Network Segment

Definition

Name: Segment1

Geolocation: HK

Type: test

Rule

192.168.8.0/24

Bandwidth settings

Inbound bandwidth: 100 Mbps

Outbound bandwidth: 100 Mbps

Total bandwidth: 200 Mbps

OK Cancel Instructions <<

Note

1. IP segment supports three formats.
 - (1) Address/mask, e.g.: 192.168.1.0/24
192.168.1.0/255.255.255.0
FE80::0:CD30::/60
 - (2) Address range, e.g.: 192.168.1.1-192.168.1.100
FE80::C0A8:0164-FE80::C0A8:0170
 - (3) A single IP address, e.g.: 192.168.1.1
FE80::24D1:FE6D:C0A8:0164
2. One entry per line, in logical "or" relationship.
3. The range of inbound bandwidth is 1-1,000,000, and it cannot be greater than the inbound bandwidth of the link.
4. The range of outbound bandwidth is 1-1,000,000, and it cannot be greater than the outbound bandwidth of the link.
5. The range of total bandwidth is 1-1,000,000, and it cannot be greater than the total bandwidth of the link.

On the **New Segment** dialog box, enter an appropriate name for the new segment, specify the geographical location, and then enter the segment rules and segment bandwidth.

Name: The name for the network segment, which will show in the Network Segment view if the segment is available.


Geo location: The geographical location of the network segment, which will show in the Geo Location columns of the IP Address view and the IP Conversation view if the IP address belonging to the segment is available.

Type: The type of the network segment.

Rule: You can define a single IP address, a range of IP addresses or IP address subnet as a network segment. Note that the rules in different network segments can be identical or crossed.

Bandwidth settings: This option is for setting the bandwidth for the network segment, which is for calculating the bandwidth utilization for the network segment. The inbound bandwidth and outbound bandwidth shall not be greater than the inbound bandwidth and outbound bandwidth of the network link that the network segment belongs to, respectively. The total bandwidth shall not be less than the greater one of the inbound and outbound bandwidth and be greater than the sum of the inbound and outbound bandwidth.






3. Click **OK** on the **New Segment** dialog box, and then click **OK** on the **Network Segment** tab.

-  **Tips** The geographical location will display in the analysis views if available.

Sublink Configuration

In the sublink configuration, you can customize the sublinks of VLAN, ISL VLAN, VXLAN, MPLS VPN, MAC address, NetFlow ID and network segment, which is helpful for users to more conveniently manage and monitor virtual network statistics data and network segment data in the network environment. This tab shows as the following figure:

Sublink Configuration

Type: VLAN Search

Na...	ID	Total Bandwidth	Inbound Bandwidth	Outbound Bandwidth
vla...	32	1000	1000	1000

< >

Buttons

The following list describes the buttons on this tab.



: Adds a network segment.



: Edits the selected network segment.



: Deletes the selected network segment.




: Imports network segment customizations from a file.

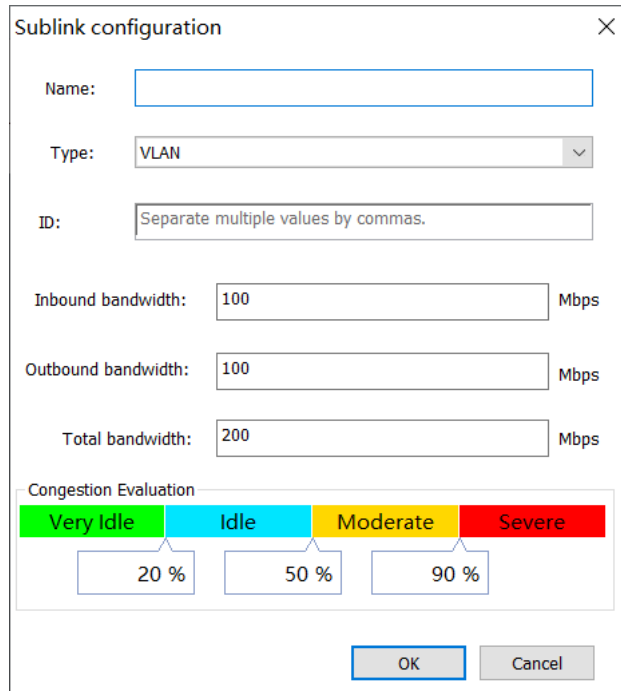


: Exports current network segment customizations to a file.

Adding a sublink

To add a sublink, follow the steps below:

1. Click  to open the Sublink Configuration dialog box.



The Sublink configuration dialog box contains the following fields and sections:

- Name:** A text input field.
- Type:** A dropdown menu currently showing "VLAN".
- ID:** A text input field with a placeholder "Separate multiple values by commas."
- Inbound bandwidth:** A text input field with "100" and a unit "Mbps" label.
- Outbound bandwidth:** A text input field with "100" and a unit "Mbps" label.
- Total bandwidth:** A text input field with "200" and a unit "Mbps" label.
- Congestion Evaluation:** A horizontal bar with four colored segments: "Very Idle" (green), "Idle" (blue), "Moderate" (yellow), and "Severe" (red). Below the bar are three input fields for percentages: "20 %", "50 %", and "90 %".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

2. On the Sublink Configuration dialog box, enter an appropriate name for the new sublink and enter the segments.

Name: The name for the sublink.

Type: The type of the sublink.

Tag: Identification information for the sublink.

Inbound bandwidth: It is used to count the inbound utilization of sunblinks. The range is 1Mbps~1000000Mbps, and it should be \leq the inbound bandwidth of the link to which the network segment belongs.





Outbound bandwidth: It is used to count the outbound utilization of sunblinks. The range is 1Mbps~1000000Mbps, and it should be \leq the outbound bandwidth of the link to which the network segment belongs.

Total bandwidth: It is used to count the total utilization of sunblinks. The maximum of the inbound and outbound bandwidth \leq the total bandwidth \leq the sum of inbound and outbound bandwidth.

3. Click **OK** on the **Sublink Configuration** dialog box.

References

This tab is provided to set the reference values for the items on the Summary view. This tab shows as the following figure:

References	
	
	
Reference Item	Reference Range
Unicast Bytes/Total ...	>=90.00%
Broadcast Bytes/To...	<5.00%
Multicast Bytes/Tot...	<5.00%
Abnormal Address ...	<1.00%
Unicast Bytes/Total ...	>=90.00%
Broadcast Bytes/To...	<5.00%
Multicast Bytes/Tot...	<5.00%
Abnormal Address ...	<1.00%
Broadcast Packets/...	<10.00%
Multicast Packets/T...	<10.00%
ARP Packets/Total P...	<3.00%
ICMP Packets/Total ...	<3.00%
<=64B Packets/Tot...	<45.00%
<=128B Packets/To...	<60.00%
SYN Packets/Total T...	<10.00%
SYNACK Packets/To...	<10.00%

Buttons

The following list describes the icon buttons on this tab:



: Edits the selected item.



: Resets all the reference values to default.



: Imports reference settings from a file.



: Exports reference settings to a file.

Editing a reference value

To edit a reference value, just double-click the item and enter the value on the Reference Value box as below.

Reference Value

×

Item

Unicast Bytes/Total IP Bytes

Scope:

>=

90

%


OK

Cancel

Field Definition

This tab is provided to define fields for custom applications, showing as the following figure:

Name	Description
Importance	The importance of the applications for the system.

-  **Note** When a field is defined successfully, it will display when adding custom applications, and you must enter a value for the field.

Buttons

The following list describes the icon buttons on this tab:



: Adds a new field.



: Edits the selected field.



: Deletes the selected field.



: Imports saved field setting files to current tab.

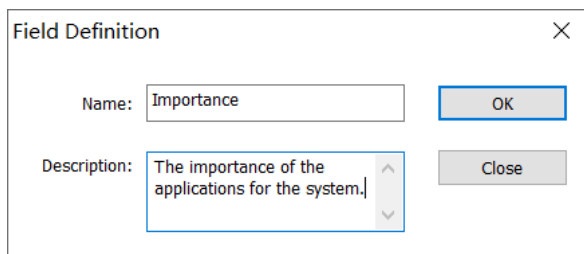


: Saves all field settings on this tab as *.csta file.

Adding a field

To add a field, follow the steps below:

1. Click  to open the **Field Definition** dialog box, which appears as the following figure:



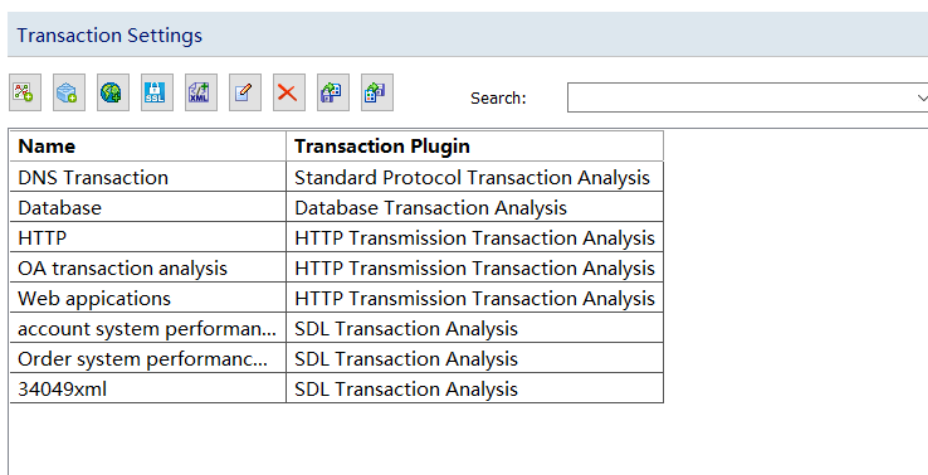
The dialog box titled "Field Definition" has a close button (X) in the top right corner. It contains two text input fields: "Name:" with the value "Importance" and "Description:" with the value "The importance of the applications for the system.". There are two buttons: "OK" and "Close".

Enter the field name and the description if necessary.

Click **OK**.

Transaction Settings

The Transaction Settings tab is provided to configure application layer protocols and transaction identification condition. When a transaction is defined, it can be correlated to standard application for transaction analysis. The Transaction Settings tab shows as the screenshot below:



The screenshot shows the "Transaction Settings" tab with a toolbar containing icons for adding transactions (TCP, Database, HTTP, SSL, etc.) and a search bar. Below the toolbar is a table with two columns: "Name" and "Transaction Plugin".

Name	Transaction Plugin
DNS Transaction	Standard Protocol Transaction Analysis
Database	Database Transaction Analysis
HTTP	HTTP Transmission Transaction Analysis
OA transaction analysis	HTTP Transmission Transaction Analysis
Web applications	HTTP Transmission Transaction Analysis
account system performan...	SDL Transaction Analysis
Order system performanc...	SDL Transaction Analysis
34049xml	SDL Transaction Analysis

Buttons

The following list describes the icon buttons on this tab:



: Add TCP Transaction. For more information on how to add a TCP transaction, please refer to Adding a TCP transaction.



: Add Database Transaction. For more information on how to add a database transaction, please refer to Adding a database transaction.



: Add HTTP Transaction. For more information on how to add an HTTP transaction, please refer to Adding an HTTP transaction.



: Add SSL/TLS Transaction. For more information on how to add an SSL/TLS transaction, please refer to Adding an SSL/TLS transaction.



: Add SDL Sync Transaction. For more information on how to add an SDL sync transaction, please refer to Adding an SDL sync transaction.



: Edit the selected transaction group.



: Delete the selected transaction group.




: Import transaction settings from a file.



: Export current transaction settings to a file.

One transaction setting item may include more than one transaction, therefore one transaction setting item is called as one transaction group.

Adding a TCP transaction

To add a TCP transaction, on the Transaction Settings tab, click the button  to open the Transaction Settings box, as the screenshot below:

Transaction Settings

Basic Information

Transaction Group Name: Transaction Plugin:

Cross Flow: Communication Type:

Protocol Information

Request Protocol **Response Protocol**

Request Protocol

Request Protocol

Name: Field type:

Value type: Extract value via:

Beginning offset: Offset:

Match length:

Constraint:

☒ Print to log

Transaction Information

Setp one: General configuration

If the transactions comply with same rule, you can click to configure them.

Setp two: Detail configuration

Transact...	Transaction Identification Con...	Transaction Match Co...	Transaction End...	Transaction Suc...
e3e311	request.New Protocol.cmd=0xe...			
e3e31k				

Transaction identification follows the listed sequence. After one transaction is identified successfully, the identification session ends.

The Transaction Settings box includes three parts:

Basic Information

The Basic Information part includes four options described as below:

Transaction Name: The name of the transaction. It should be unique.

Transaction Plugin: Transaction identification plugin. Only TCP transaction analysis plugin is available for now.

Cross Flow: To configure whether the transaction group is identified by crossing flows. Yes means to cross flows.


Communication Type: The communication type of transaction group. It could be Asynchronous or Synchronous. If the transaction group is identified by crossing flows, then the communication type should be asynchronous.

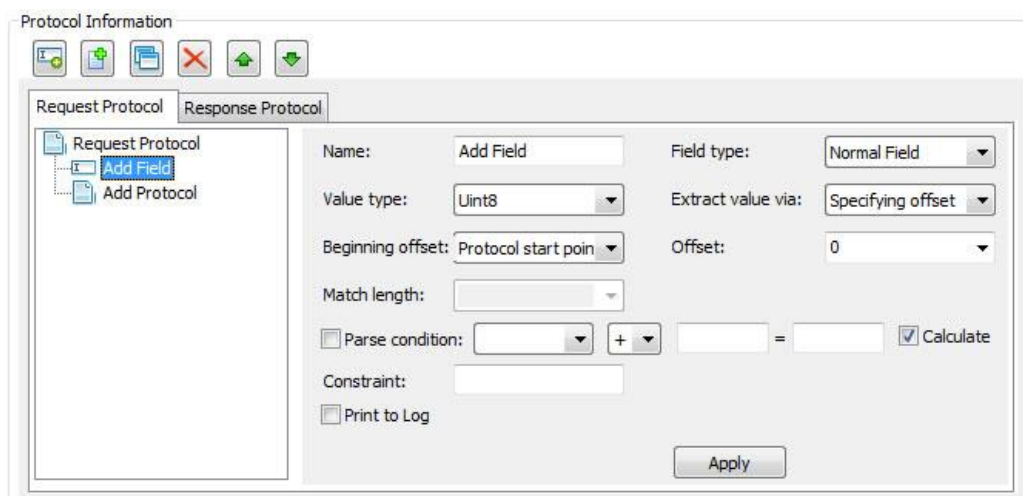
Protocol Information

The Protocol Information part is for describing application layer protocols. When configuring protocols, it is required to configure related fields and sub-protocols based on protocol sequence. The protocols added under a protocol are called as sub-protocols.

To accurately describe protocols, it is required to configure request protocols and response protocols separately. The methods for configuring request protocols are exactly same to those for configuring response protocols. Here, take configuring request protocols as an example.

Adding field

Click the Add Field button  to add a protocol field, as the screenshot below:



The following list describes the options for adding a field:

Name: The name of the field. Field names of same level should be unique.

Field type: Field type could be Normal Field or Protocol Length. Protocol Length means that the field is for flagging the total data length on the protocol layer. One protocol only contains one protocol length field.

Value type: Value type could be Uint8, Unit16, Uint32, Uint64, or String. If the Field type is Protocol Length, then Value type cannot be String.

Extract value via: There are three methods to extract the value. Different extract methods bring different options.

Specifying offset: Extract the value after offsetting some bytes.

- **Beginning offset:** Select a configured field or offset from protocol start point.
- **Offset:** Select a configured field or enter a positive integer to be the offset.
- **Match length:** Enter a positive integer to be the match length. Match length must be specified when Value type is String.

Matching pattern: Extract the value based on pattern.

- **Beginning offset:** Select a configured field or offset from protocol start point.
- **Offset:** Select a configured field or enter a positive integer to be the offset.

- **Search length:** Enter a positive integer to be the search length.
- **Pattern type:** Pattern type can only be Regular Expression for now.
- **Match pattern:** Enter the match pattern based on regular expression, or click the drop-down list to choose a match pattern to set up quickly.

Calculating: Extract the value by logical operation.

- **Calculation rule:** Supported calculation rules include adding, subtracting, multiplying, dividing, logical AND, and logical OR. For dividing, only the integer part of the result is returned.
- **Constraint:** Constraint is for checking field extracting result.


Only when the constraint is matched, the protocol is parsed correctly. If the constraint is not matched, then protocol parsing failed. If no constraint is set up, then the result will not be checked.

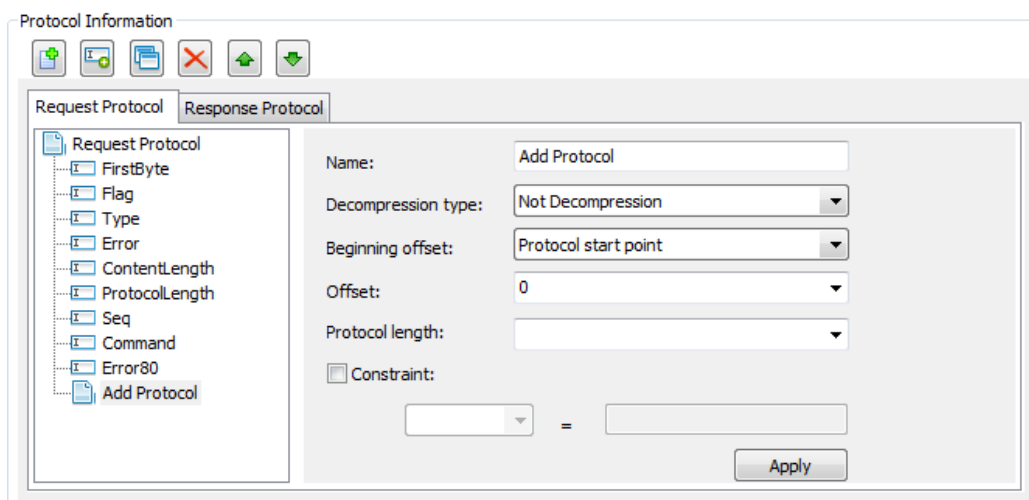
Constraint can be a single value, a value range, or a set of multiple values. Value range is defined with "-", while a set of multiple values is defined with ",". The value can be decimal figures, hexadecimal figures, or string.

For example, "0-99" indicates an integer value not less than 0 and not greater than 99. "2,5,7" indicates a set of 2, 5, and 7. "abc, def, xyz" indicates a set of three strings.

Print to log: If this option is checked, field parse results will be displayed when do transaction analysis on the Transaction Log view.

Adding sub-protocol

Click the Add Protocol button  to add a sub-protocol, as the screenshot below:



The following list describes the options for adding a sub-protocol:

Name: The name of the sub-protocol. Protocol names of same level should be unique.

Decompression type: This option could be Not Decompression or FTD Decompression. If the protocol data is encrypted with FTD method, then this option should be FTD Decompression; or else the protocol cannot be identified correctly.


Beginning offset: The point to start the sub-protocol identification. Choose a configured field to be the beginning offset.


Offset: Select a configured field or enter a non-negative integer to be the offset.

Protocol length: Select a configured field or enter a positive integer to be the protocol length.



Constraint: This option can be enabled when the protocol is identified with specific condition. Select a field and enter the condition. The condition can be a single value, a value range, or a set of multiple values. Value range is defined with "-", while a set of multiple values is defined with ",". The value can be decimal figures, hexadecimal figures, or string.

Node operation

Select a node and click the button  to copy the selected protocol/field as a new protocol/field.

Select the root node Request Protocol/Response Protocol and click the button , then all sub-protocols and fields will be copied to Response Protocol/Request Protocol.

You can click the button  to delete a selected node.

You can click the button  to move up the selected node, and click the button  to move down the selected node.

You can further right-click a node to move up/down a node by one level.

Transaction Information

The Transaction Information part is provided to configure transactions, and includes two steps: General configuration and Detail configuration.

General configuration

General configuration is an optional step. If the transactions to be configured have same transaction match conditions, transaction end flags or transaction success flags, then you can use General configuration to configure them all, to avoid duplicate configuration steps. The General Configuration box shows as the figure below:

The following list describes the options on the General Configuration box:

Name: Define the field name.

Transaction Match Condition: One or more match conditions can be defined. Multiple match conditions are in logical AND relationship. The match condition can be configured as: a field in request protocol = a field on response protocol.

Transaction Request End Flag: This option can be configured as a field in request protocol = a constraint. The constraint has rules same to those for adding a field.

Transaction Response End Flag: This option can be configured as a field in response protocol = a constraint. The constraint has rules same to those for adding a field.

Transaction Success Flag: This option can be configured as a field in response protocol equal to or not equal to a constraint. The constraint has rules same to those for adding a field.

Return Code: Add a response field as transaction return code.

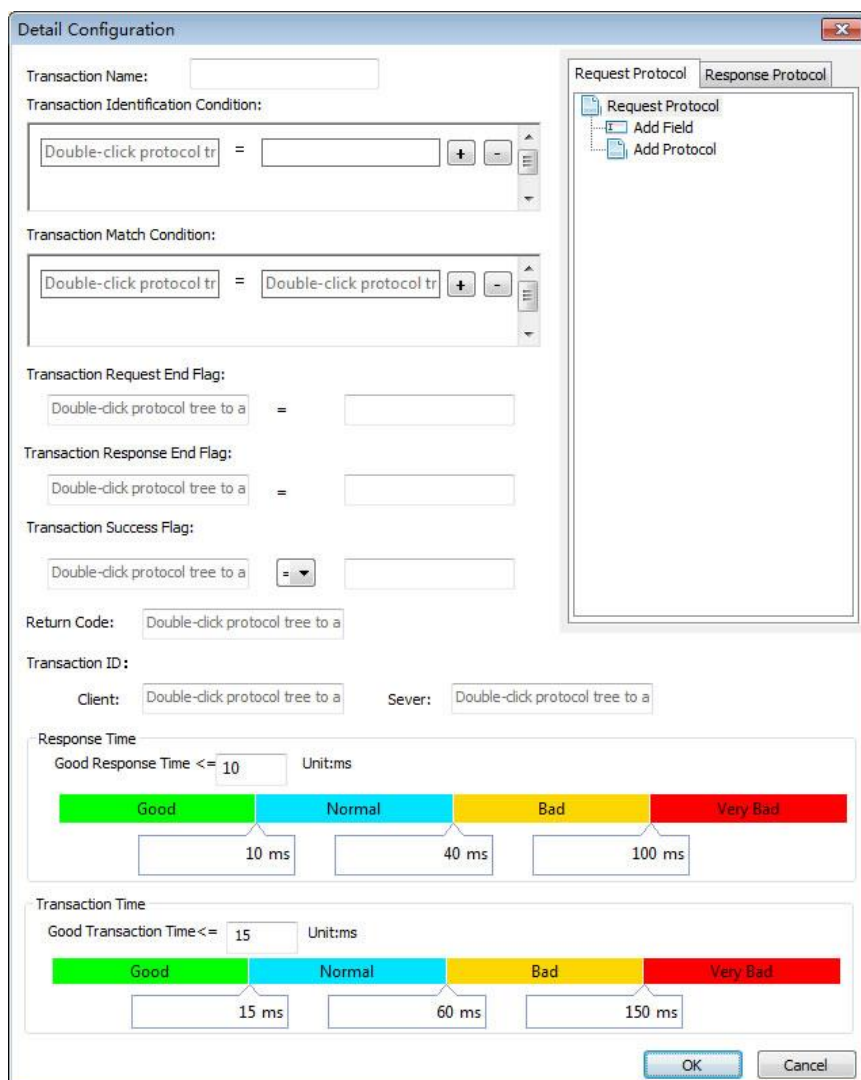
Transaction ID: This option is to identify a transaction, add a request field as the client and add a response field as the server.

After configuring general match rules, you can further configure them for a specific transaction. When general configuration and specific transaction set up conditions for a same rule, the conditions are in logical AND relationship.

Taking Transaction Success Flag as an example, for general configuration, the condition is set up as request protocol.transaction status field = response protocol.transaction status field; for transaction A, the condition is request protocol.other field = response protocol.other field. Then, transaction A will be successfully identified only when both the conditions are met with; or else, transaction A will be marked as transaction failure.

Detail configuration

Detail configuration is for configuring a specific transaction. Click the Add Transaction button to open the Detail Configuration box, as the screenshot below:



The screenshot shows the 'Detail Configuration' dialog box. It has a 'Transaction Name' field. Below it is the 'Transaction Identification Condition' section with a text box containing 'Double-click protocol tr' followed by an equals sign and a dropdown menu. To the right of this is a tree view with 'Request Protocol' and 'Response Protocol' tabs. Under 'Request Protocol', there are 'Add Field' and 'Add Protocol' buttons. Below the identification condition is the 'Transaction Match Condition' section, which has a similar text box and dropdown. Further down are sections for 'Transaction Request End Flag', 'Transaction Response End Flag', and 'Transaction Success Flag', each with a text box and a dropdown. Below these is the 'Return Code' section with a text box and a dropdown. The 'Transaction ID' section has 'Client' and 'Server' fields, each with a text box and a dropdown. The 'Response Time' section has a 'Good Response Time <= ' field with a value of 10 and a 'Unit:ms' label. Below this is a horizontal bar with four colored segments: 'Good' (green), 'Normal' (blue), 'Bad' (yellow), and 'Very Bad' (red). Below the bar are three text boxes with values 10 ms, 40 ms, and 100 ms. The 'Transaction Time' section has a 'Good Transaction Time <= ' field with a value of 15 and a 'Unit:ms' label. Below this is a similar horizontal bar with four colored segments: 'Good' (green), 'Normal' (blue), 'Bad' (yellow), and 'Very Bad' (red). Below the bar are three text boxes with values 15 ms, 60 ms, and 150 ms. At the bottom right are 'OK' and 'Cancel' buttons.

The following list describes the options on the Detail Configuration box:

Transaction Name: Transaction names should be unique within a transaction group.

Transaction Identification Condition: One or more identification conditions can be defined. Multiple identification conditions are in logical AND relationship. The identification condition can be

configured as: a field in request protocol = a constraint. The constraint has rules same to those for adding a field.

Transaction Match Condition: No need to configure if general configuration is already set up. The configuration method is same to set up general configuration.

Transaction Request End Flag: No need to configure if general configuration is already set up. The configuration method is same to set up general configuration.

Transaction Response End Flag: No need to configure if general configuration is already set up. The configuration method is same to set up general configuration.

Transaction Success Flag: No need to configure if general configuration is already set up. The configuration method is same to set up general configuration.

Return Code: No need to configure if general configuration is already set up. The configuration method is same to set up general configuration.


Transaction ID: No need to configure if general configuration is already set up. The configuration method is same to set up general configuration.


Response Time: The standard response time for a transaction. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time:good response time:bad response time = 1:4:10. You can modify the response time manually. Good response time must be less than normal response time which must be less than bad response time.



Transaction Time: The standard transaction time for a transaction. When the good transaction time is set, normal transaction time and bad transaction time will be calculated automatically. By default, normal transaction time:good transaction time:bad transaction time = 1:4:10. You can modify the transaction time manually. Good transaction time must be less than normal transaction time which must be less than bad transaction time.

Transaction operation


You can select a transaction and click the button  to copy the selected transaction as a new transaction for further modification.

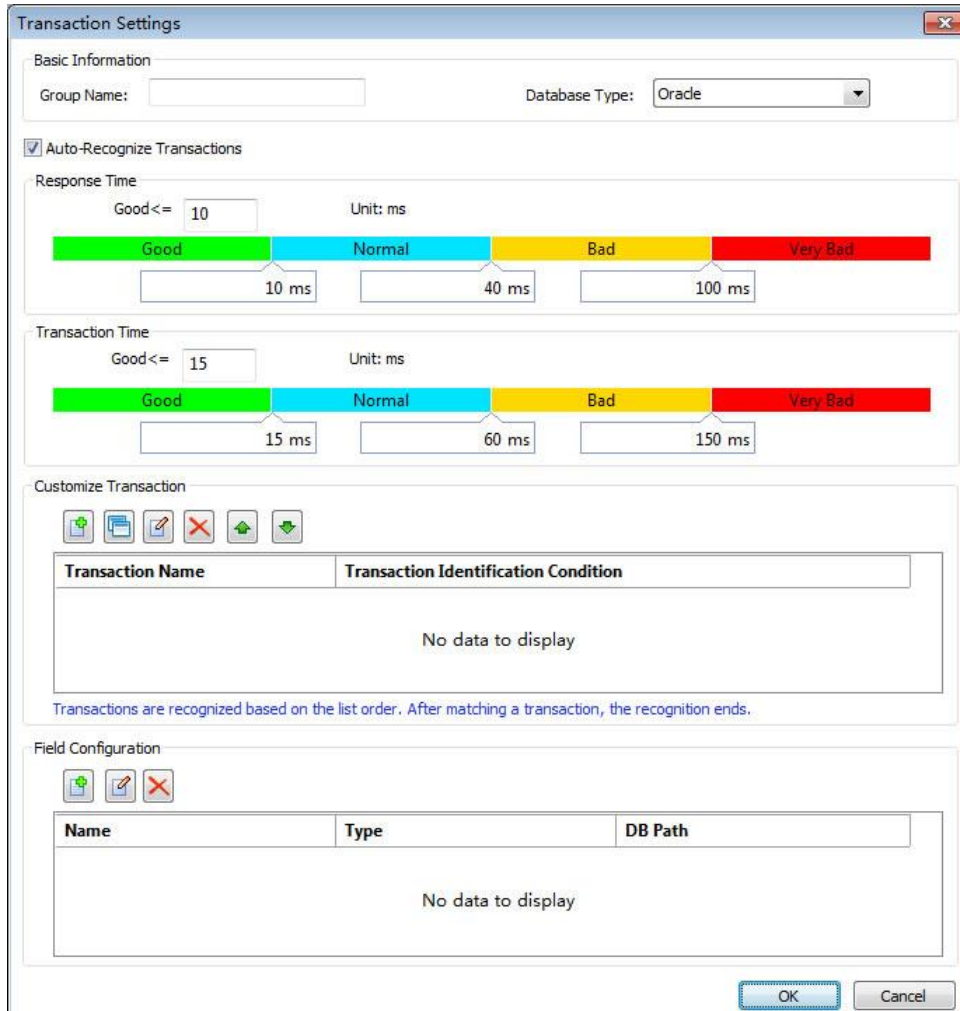
You can click the button  to delete the selected transaction.

You can click the button  to modify the selected transaction.

You can click the button  to move up the selected transaction, and click the button  to move down the selected transaction. Upper transactions have priority over the lower transactions.

Adding a database transaction

To add a database transaction, on the Transaction settings tab, click the button  to open the settings box, as the screenshot below:



The screenshot shows the 'Transaction Settings' dialog box with the following sections:

- Basic Information:**
 - Group Name:
 - Database Type:
- Auto-Recognize Transactions:**
 - ☒ Auto-Recognize Transactions
 - Response Time:**
 - Good <= Unit: ms
 - Timeline: Good (0-10 ms), Normal (10-40 ms), Bad (40-100 ms), Very Bad (100-150 ms)
 - Transaction Time:**
 - Good <= Unit: ms
 - Timeline: Good (0-15 ms), Normal (15-60 ms), Bad (60-150 ms), Very Bad (150-150 ms)
- Customize Transaction:**
 - Buttons: Add, Edit, Delete, Up, Down
 - Table:

Transaction Name	Transaction Identification Condition
No data to display	
 - Note: Transactions are recognized based on the list order. After matching a transaction, the recognition ends.
- Field Configuration:**
 - Buttons: Add, Edit, Delete
 - Table:

Name	Type	DB Path
No data to display		

Buttons: OK, Cancel

The Transaction Settings box includes four parts:

Basic Information

Auto-Match

Customize Transaction

Field Configuration

Basic Information

The Basic Information part includes options described as below:

Transaction Group Name: The name of the transaction group. It should be unique.

Database: Select the database type you are using.

Auto-Match

The option Auto-Match is enabled by default, users can choose enable or disable this option. System will automatically recognize transactions according to the SQL statement. And system will take the keyword and table name as transaction name to recognize it.

Response Time: This option is provided for users to customize the reference time for transaction response quality. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time : good response time : bad response time = 1 : 4 : 10. Users can modify the response time manually. Good response time must be less than normal response time which must be less than bad response time.

Transaction Time: This option is provided for users to customize the reference time for transaction quality. When the good transaction time is set, normal transaction time and bad transaction time will be calculated automatically. By default, normal transaction time : good transaction time : bad transaction time = 1 : 4 : 10. You can modify the transaction time manually. Good transaction time must be less than normal transaction time which must be less than bad transaction time.

Customize Transaction

nChronos provides customize transaction function for database transactions, as the screenshot below:

Transaction Configuration

Transaction Name:

Transaction Identification Condition:

Response Time

Good <= Unit: ms

Good Normal Bad Very Bad

Good <= Unit: ms

Good Normal Bad Very Bad

Identification ID:

OK Cancel


Transaction Name: The name of the transaction. It should be unique.

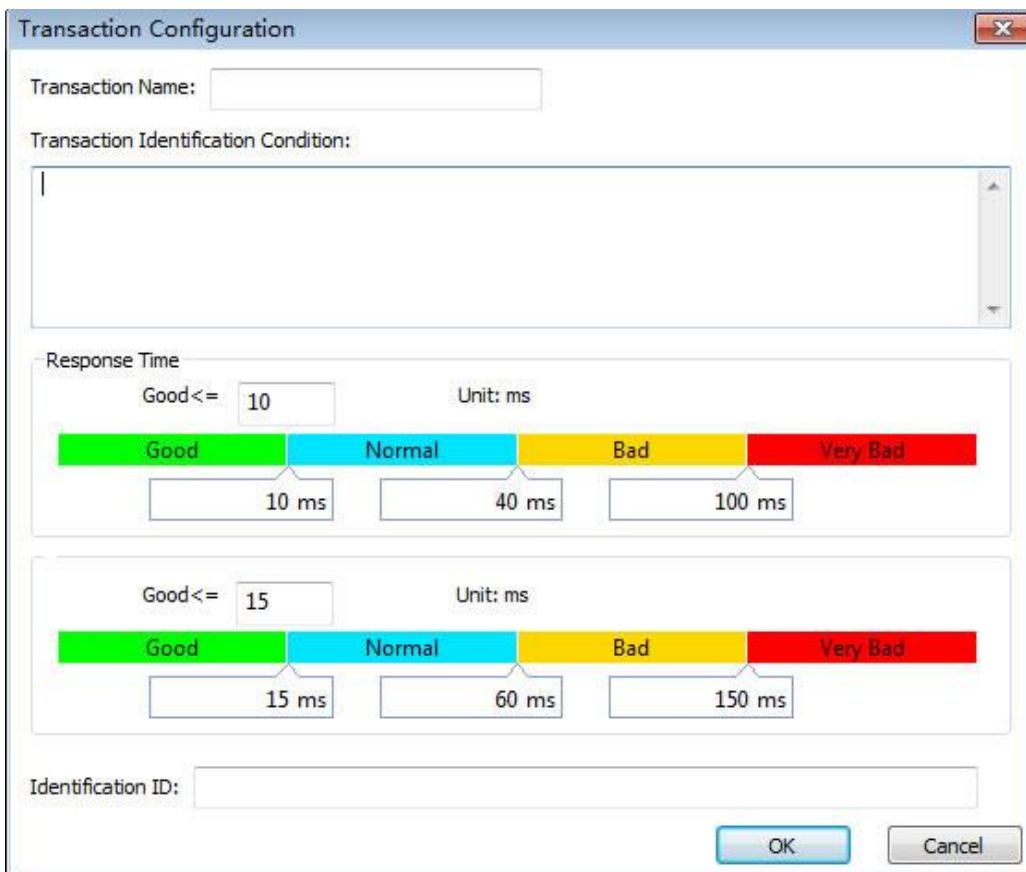
Transaction Identification Condition: One SQL statement is the one identification condition of database transaction, SQL statement supports the wildcard character "?" , "?" represents zero or multiple characters.

Response Time: The standard response time for a transaction. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time:good response time:bad response time = 1:4:10. You can modify the response time manually. Good response time must be less than normal response time which must be less than bad response time.

Transaction Identification Number: Use the identification number to set the transaction. As to database transaction, usually, the transaction identification number is a field of the information chart.

Field Configuration

Click the button , options description of the field configuration and the screenshot showed as below:



Transaction Configuration

Transaction Name:

Transaction Identification Condition:

Response Time

Good <= Unit: ms

Good Normal Bad Very Bad

Good <= Unit: ms

Good Normal Bad Very Bad

Identification ID:


OK Cancel

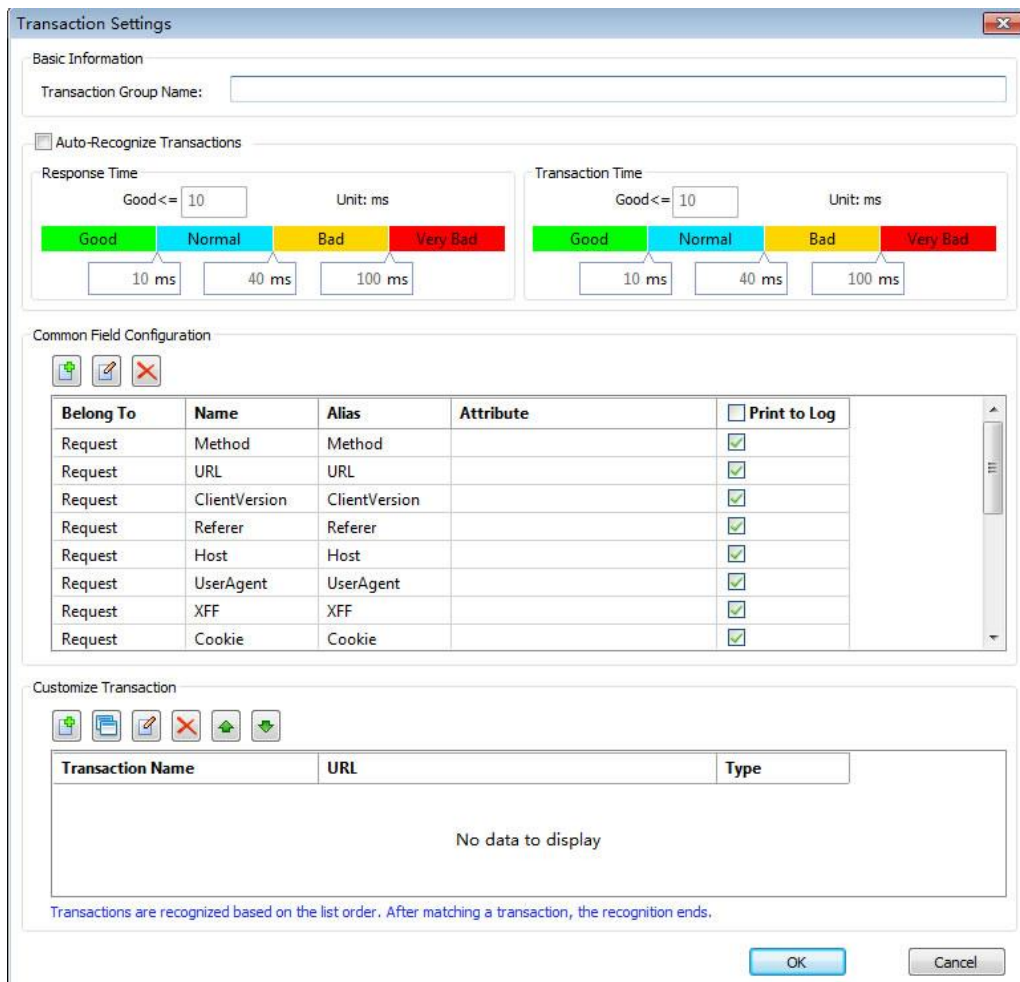
Users can add custom statistics field and transaction identification ID in field configuration.

When you add custom statistics field, you need to set field name and the location of the database where the field is located.

When you add identification ID, you don't need set the field name, just set the location of the database where the field is located. When you have added multiple transaction identification ID, transactions match the sequence according to the identification ID, when matched the identification ID which can meet the conditions, stop matching other identification ID.

Adding an HTTP transaction

To add an HTTP transaction, on the Transaction Settings tab, click the button  to open the settings box, as the screenshot below:



The Transaction Settings dialog box is divided into four main sections:

- Basic Information:** Contains a text field for "Transaction Group Name".
- Auto-Recognize Transactions:** Includes a checkbox to enable auto-recognition. Below it are two performance scale visualizations:
 - Response Time:** A scale from 0 to 100 ms, divided into Good (0-10 ms), Normal (10-40 ms), Bad (40-100 ms), and Very Bad (100-1000 ms).
 - Transaction Time:** A similar scale from 0 to 100 ms.
- Common Field Configuration:** A table with columns: Belong To, Name, Alias, Attribute, and Print to Log. It lists various HTTP request attributes like Method, URL, ClientVersion, Referer, Host, UserAgent, XFF, and Cookie.
- Customize Transaction:** A section with icons for adding, editing, deleting, and saving transactions. Below is a table with columns: Transaction Name, URL, and Type. The table is currently empty, showing "No data to display".

At the bottom, there are "OK" and "Cancel" buttons.

The Transaction Settings box includes four parts:

Basic Information

Auto-Recognize Transactions

Common Field Configuration

Customize Transaction

Basic Information

Transaction Group Name: The name of the transaction group. It should be unique.

Auto-Recognize Transactions

When the option Auto-Recognize Transactions is enabled, nChronos will automatically recognize HTTP requests as transactions. The URL will be taken as the name of the transaction. Custom

transactions have priority over auto-recognized transactions. When custom transactions cannot be identified, nChronos will take URL as transaction name to recognize it.

Transaction request content and response content will not be saved for auto-recognized transactions.

Users can set response time and transaction time for auto-recognized transactions.

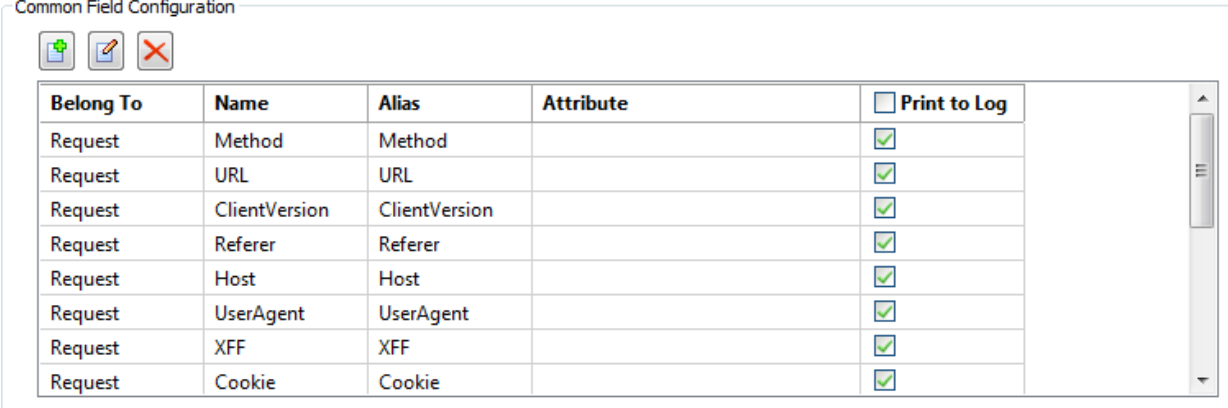
Response Time: This option is provided for users to customize the reference time for transaction response quality. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time : good response time : bad response time = 1 : 4 : 10. Users can modify the response time manually. Good response time must be less than normal response time which must be less than bad response time.

Transaction Time: This option is provided for users to customize the reference time for transaction quality. When the good transaction time is set, normal transaction time and bad transaction time will be calculated automatically. By default, normal transaction time : good transaction time : bad transaction time = 1 : 4 : 10. You can modify the transaction time manually. Good transaction time must be less than normal transaction time which must be less than bad transaction time.


Common Field Configuration

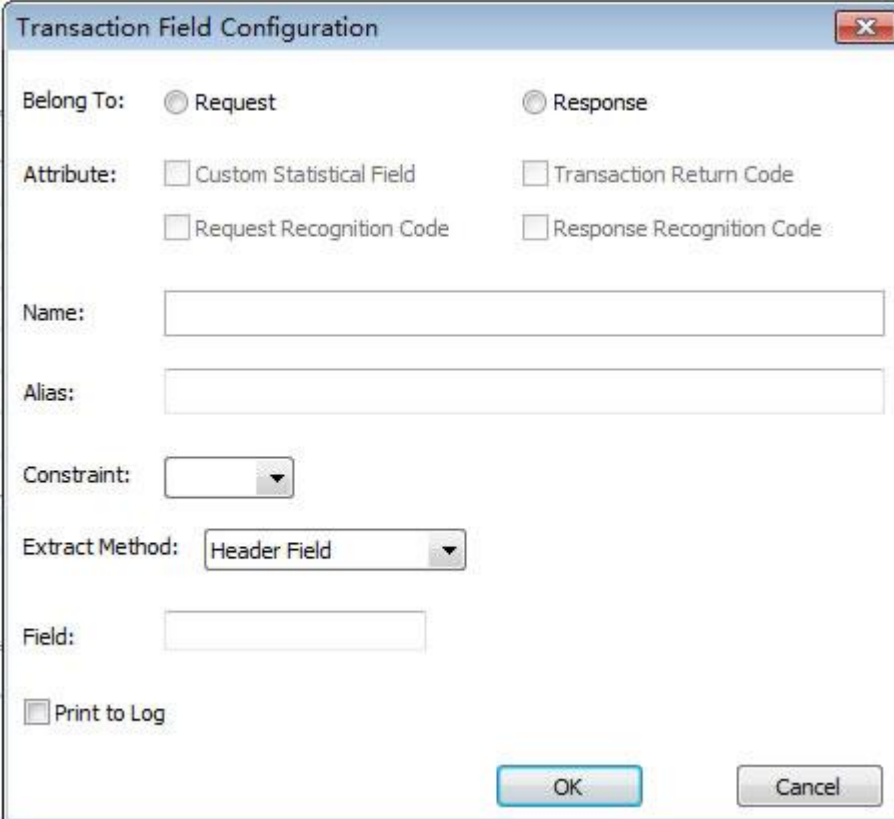
nChronos provides some common fields for HTTP transactions, as the screenshot below:

Common Field Configuration



Belong To	Name	Alias	Attribute	<input type="checkbox"/> Print to Log
Request	Method	Method		<input checked="" type="checkbox"/>
Request	URL	URL		<input checked="" type="checkbox"/>
Request	ClientVersion	ClientVersion		<input checked="" type="checkbox"/>
Request	Referer	Referer		<input checked="" type="checkbox"/>
Request	Host	Host		<input checked="" type="checkbox"/>
Request	UserAgent	UserAgent		<input checked="" type="checkbox"/>
Request	XFF	XFF		<input checked="" type="checkbox"/>
Request	Cookie	Cookie		<input checked="" type="checkbox"/>

Users can add new common fields. To add a new common field, click the button  to open the Transaction Field Configuration box, as screenshot below:



The screenshot shows a 'Transaction Field Configuration' dialog box. It has a title bar with a close button. Inside, there are two radio buttons for 'Belong To': 'Request' and 'Response'. Below these are four checkboxes under the 'Attribute' label: 'Custom Statistical Field', 'Transaction Return Code', 'Request Recognition Code', and 'Response Recognition Code'. There are two text input fields for 'Name' and 'Alias'. A 'Constraint' dropdown menu is shown with a downward arrow. The 'Extract Method' dropdown menu is set to 'Header Field'. There is a 'Field' text input field. At the bottom left is a 'Print to Log' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

Belong To: Specify the field belongs to a request or a response.

Attribute: The type of the field.

One transaction group can contain 3 custom statistical fields at most. Only common fields can be defined as custom statistical fields.

Every transaction can be defined with a transaction return code, which will be taken as the default statistical field.

Every transaction can be defined with a request recognition code.

Every transaction can be defined with a response recognition code.

Name: The name of the transaction field.

Alias: The alias of the transaction field.

Constraint: Constraint condition.

Extract Method: Choose the extract method.

Print to Log: This option is provided to print the transaction field to transaction log.

Customize Transaction

The Custom HTTP Transaction configuration user interface shows as screenshot below:

Custom HTTP Transaction

Basic Information
Name: Description:

Rule
Host:
URL: ☐ Auto-match subpath

Parameters

Parameter	Value
Click to input parameter...	Click to input parameter...

Parameter is optional. The logical relationship between multiple parameters is 'and'.
If the value of parameter is not certain, you could set the parameter's name only.

Response Time
Good <= Unit: ms
Good
Normal
Bad
Very Bad

Transaction Time
Good <= Unit: ms
Good
Normal
Bad
Very Bad

Custom Field Configuration

Belong To	Name	Alias	Attribute	<input type="checkbox"/> Print to Log
Request	Method	Method		<input checked="" type="checkbox"/>
Request	URL	URL		<input checked="" type="checkbox"/>
Request	ClientVersion	ClientVersion		<input checked="" type="checkbox"/>
Request	Referer	Referer		<input checked="" type="checkbox"/>

Save
☐ Save request content ☐ Save response content

The Custom HTTP Transaction box includes five parts:

Basic Information: Define transaction name and description.

Rule: Define transaction rule.

Host: The host for HTTP request. This option could be null.

URL: The URL path for HTTP request. This option must be defined.

Auto-match subpath: This option is enabled to apply fuzzy match onto the subpath. If this option is not enabled, the transaction will be identified only when the URL subpath is identical to what is defined.


Parameters: The parameters of the URL. You can enter the parameters in a form of key=value, for example, para1=value1. You can enter multiple parameters with one per line.

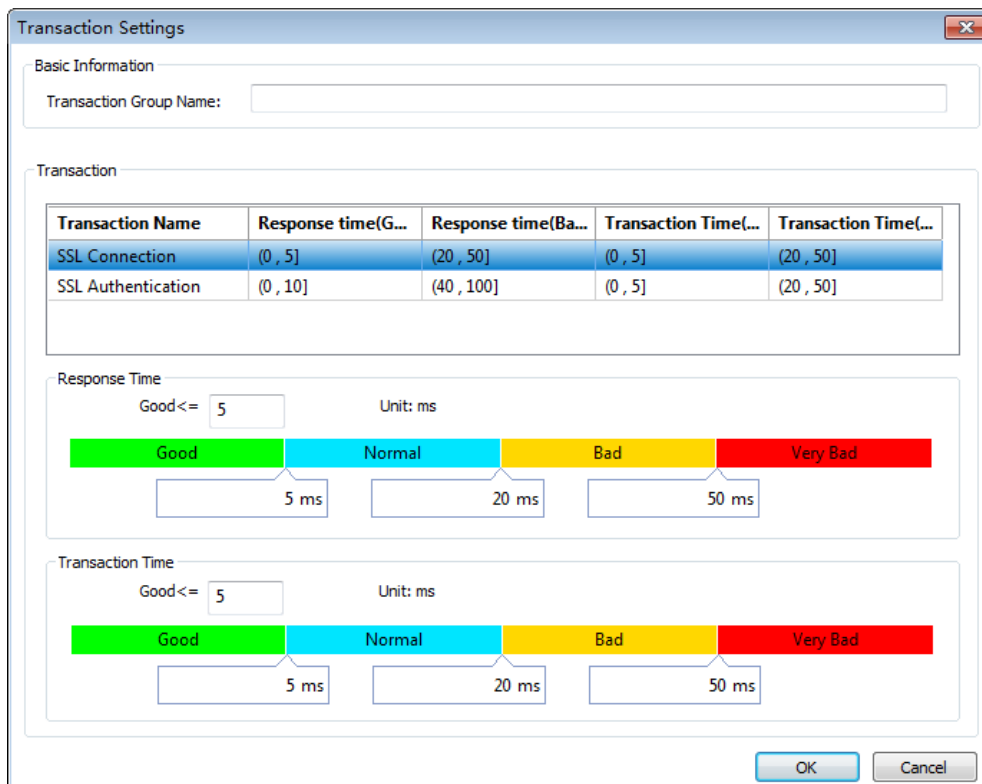
Response Time and Transaction Time: Define response time and transaction time, which are same as those for auto-recognized transaction on this page.

Custom Field Configuration: The definition method for custom field configuration is same as it for common field configuration.

Save request content and response content: Save transaction request content and transaction response content.

Adding an SSL/TSL transaction

To add an SSL/TSL transaction, on the Transaction settings tab, click the button  to open the settings box, as the screenshot below:



The screenshot shows the 'Transaction Settings' dialog box. It has two main sections: 'Basic Information' and 'Transaction'. The 'Basic Information' section contains a 'Transaction Group Name' text field. The 'Transaction' section contains a table with transaction details and two configuration sections for 'Response Time' and 'Transaction Time'.

Transaction Name	Response time(G...	Response time(Ba...	Transaction Time(...	Transaction Time(...
SSL Connection	(0 , 5]	(20 , 50]	(0 , 5]	(20 , 50]
SSL Authentication	(0 , 10]	(40 , 100]	(0 , 5]	(20 , 50]

Below the table, there are two identical configuration sections for 'Response Time' and 'Transaction Time'. Each section has a 'Good <= ' input field (set to 5) and a 'Unit: ms' label. Below this is a horizontal bar divided into four colored segments: Good (green), Normal (blue), Bad (yellow), and Very Bad (red). Below each segment is a time value: 5 ms for Good, 20 ms for Normal, and 50 ms for Bad. The Very Bad segment does not have a value.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

The Transaction Settings box includes two parts:

Basic Information

Transaction

Basic Information

Transaction Group Name: The name of the transaction group. It should be unique.

Transaction


SSL transaction provides two built-in transactions: SSL Connection and SSL Authentication. Users are able to configure the response time and transaction time for the two transactions.

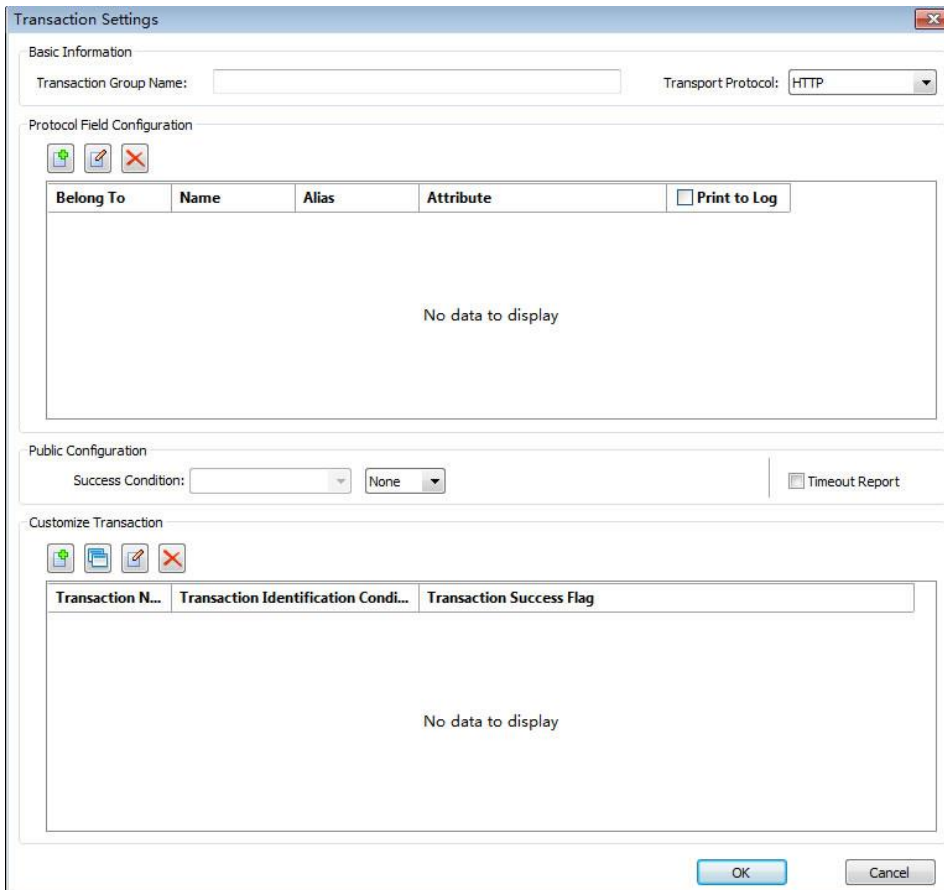
Response Time: This option is provided for users to customize the reference time for transaction response quality. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time : good response time : bad

response time = 1 : 4 : 10. Users can modify the response time manually. Good response time must be less than normal response time which must be less than bad response time.

Transaction Time: This option is provided for users to customize the reference time for transaction quality. When the good transaction time is set, normal transaction time and bad transaction time will be calculated automatically. By default, normal transaction time: good transaction time : bad transaction time = 1 : 4 : 10. You can modify the transaction time manually. Good transaction time must be less than normal transaction time which must be less than bad transaction time.

Adding an SDL sync transaction

To add an SDL sync transaction, on the Transaction settings tab, click the button  to open the settings box, as the screenshot below:



Transaction Settings

Basic Information

Transaction Group Name: Transport Protocol: HTTP

Protocol Field Configuration

Belong To	Name	Alias	Attribute	<input type="checkbox"/> Print to Log
No data to display				

Public Configuration

Success Condition: None ☐ Timeout Report

Customize Transaction

Transaction N...	Transaction Identification Condi...	Transaction Success Flag
No data to display		

OK Cancel

The Transaction Settings box includes four parts:

Basic Information

Protocol Field Configuration

Public Configuration

Customize Transaction

Basic Information


The Basic Information part includes two options described as below:

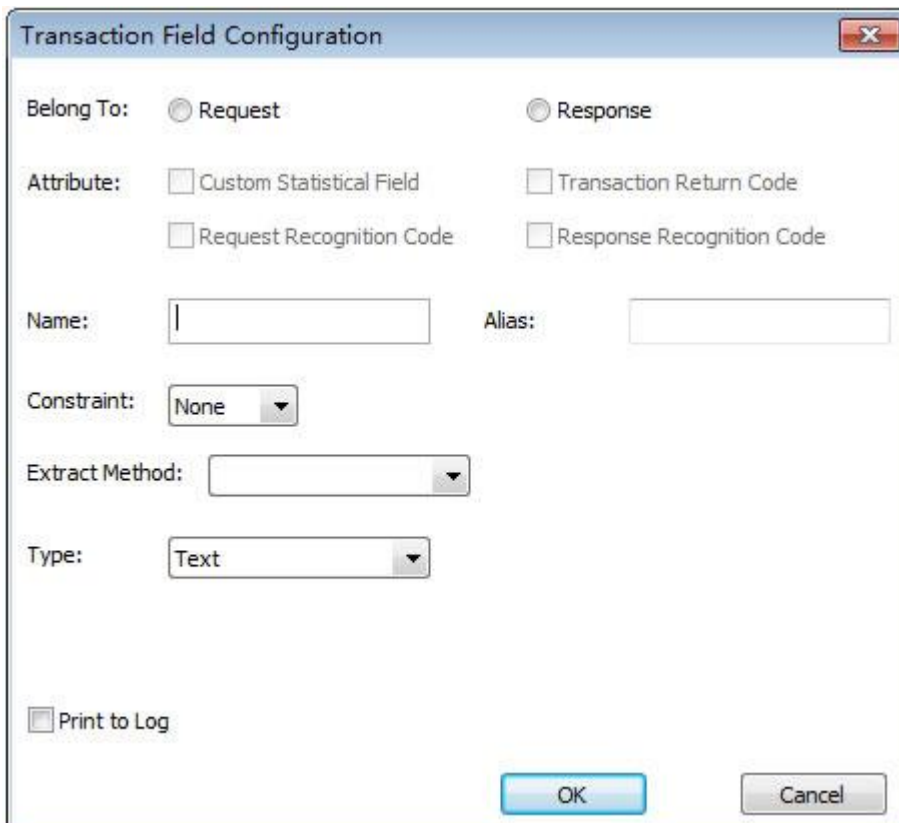
Transaction Group Name: The name of the transaction group. It should be unique.

Transport Protocol: Only HTTP protocol is supported for now.

Protocol Field Configuration

Protocol Field Configuration is for defining request and response protocol fields.

To add a new common field, click the button  to open the Transaction Field Configuration box, as screenshot below:



The configuration method is very similar with that for configuring the common fields for HTTP transactions. You can refer to Common Field Configuration for details.

Public Configuration

Success Condition: The success condition for the transaction group. Users are able to input multiple values, with blank to separate them, in logical OR relationship. For example, Equal to CD001 CD002 means equal to CD001 or equal to CD002.

Timeout Report: This option is provided to specify whether to report the transaction record when the transaction times out. The timeout value is defined by transport layer protocol. There is no need to configure it.

Customize transaction

The configuration box for SDL sync transaction shows as the screenshot below:

SDL Transaction

Basic Information

Name:

Identification: =

Success Flag:

Response Time

Good <= Unit:ms

Good Normal Bad Very Bad

Transaction Time

Good <= Unit:ms

Good Normal Bad Very Bad

Custom Field Configuration

Belong To	Name	Alias	Attribute	<input type="checkbox"/> Print to Log
No data to display				

☐ Timeout Report

The configuration details in configuration dialog box are as follows:

Basic Information

Response Time

Transaction Time

Custom Field Configuration

Basic Information

Name: The name of the transaction. It should be unique.

Identification: The condition for identifying transactions. Identification field must be described in Protocol Field Configuration. Only support "Equal". You can input multiple values, with blank to separate.

Success Flag: The condition to judge it's a successful transaction or a failed transaction.

Response Time

This option is provided for users to customize the reference time for transaction response quality. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time: good response time: bad response time = 1 : 4 : 10. Users can modify the response time manually. Good response time must be less than normal response time which must be less than bad response time.

Transaction Time

This option is provided for users to customize the reference time for transaction quality. When the good transaction time is set, normal transaction time and bad transaction time will be calculated automatically. By default, normal transaction time: good transaction time: bad transaction time = 1 : 4 : 10. You can modify the transaction time manually. Good transaction time must be less than normal transaction time which must be less than bad transaction time.






Custom Field Configuration



The Custom Field Configuration is as same as the Protocol Field Configuration. The difference is that the fields for custom transactions cannot be taken as custom statistical field.

Analysis Settings




This tab is provided to customize applications, which could be standard application, web application, signature application, encryption applications and protocol applications, and enable Performance Analysis as well as Transaction Analysis. This tab shows as the following figure:

Analysis Settings

Enable	Name	Application Type	<input type="checkbox"/> Performance Analysis	<input type="checkbox"/> Transaction Analysis
<input type="checkbox"/>	163	Web Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Web Application2	Web Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Signature Applic...	Signature Applic...	<input checked="" type="checkbox"/>	

Buttons

The following list describes the icon buttons on this tab:



: Adds a new standard application. See Adding a standard application for more information.



: Adds a new web application. See Adding a web application for more information.



: Adds a new signature application. See Adding a signature application for more information.



: Add an encryption application. An encryption application is an application with a corresponding key



: A protocol application is used to add a protocol application that defines rules based on network protocols.



: Edits the selected application.



: Deletes the selected application.



: Imports custom applications from a file.



: Exports current custom applications to a file.



: Enable all custom applications.



: Disable all custom applications.



: After you click, the enabled user-defined applications become disabled. The disabled custom applications will be enabled.

Columns

The following list describes the table columns on this tab:

Enable: Shows which applications are enabled.

Name: The name of the application.


Application Type: The type of the application.

Performance Analysis: To enable the monitor and the performance analysis of the application. The application could be any of the three types of custom application. This column is only available when the column **Enable** is selected.

Transaction Analysis: To analyze the transactions of the application which can only be web application. This column is only available when the column **Enable** is selected and the application is defined with transactions.


When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.

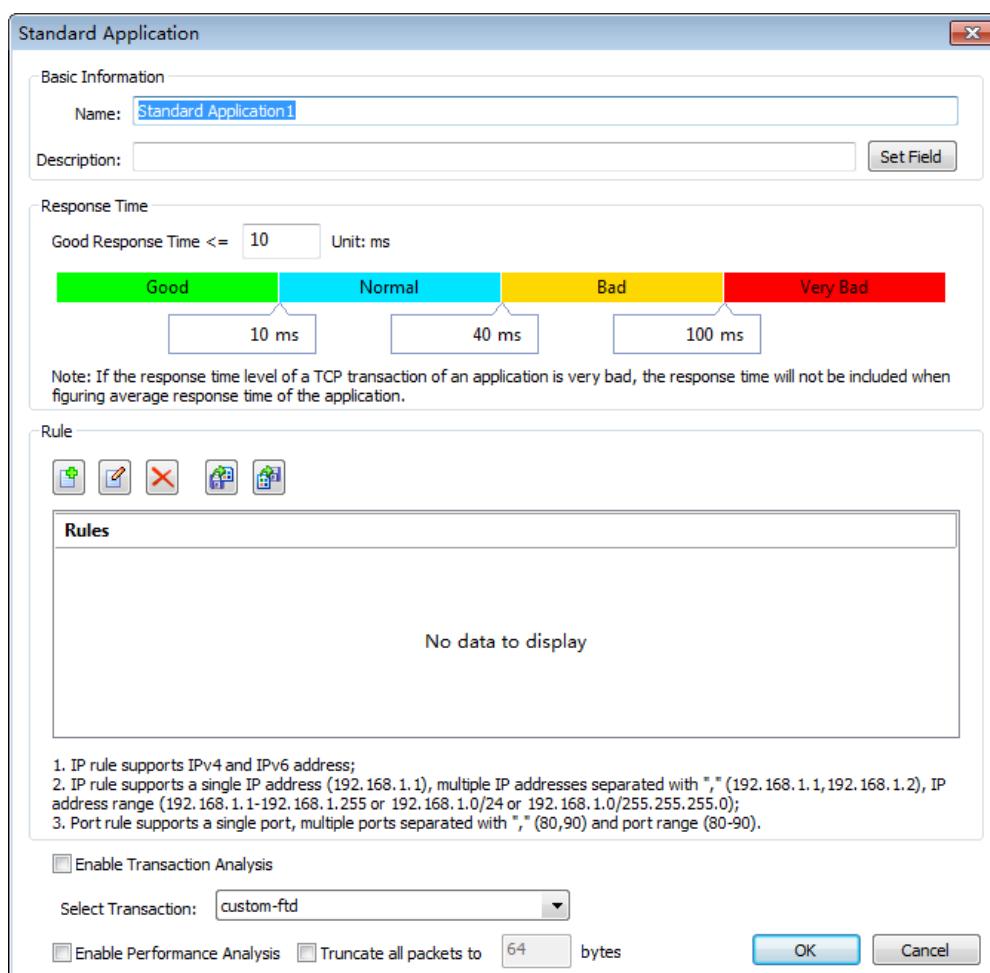
To enable a custom application, you must select the **Enable** checkbox in front of the applications.

-  The custom applications have priority over the system applications when conflicting or overlapping.

Adding a standard application

To add a standard application, follow the steps below:

1. Click  on the **Analysis Settings** tab to open the Standard Application dialog box as the following figure:




The dialog box is titled "Standard Application" and contains the following sections:

- Basic Information:**
 - Name:
 - Description:
 - Set Field button
- Response Time:**
 - Good Response Time <= Unit: ms
 - Visual scale: Good (0-10 ms), Normal (10-40 ms), Bad (40-100 ms), Very Bad (100+ ms)
 - Note: If the response time level of a TCP transaction of an application is very bad, the response time will not be included when figuring average response time of the application.
- Rule:**
 - Icons: Add, Edit, Delete, Import, Export
 - Rules list: No data to display
 - Help text:
 - 1. IP rule supports IPv4 and IPv6 address;
 - 2. IP rule supports a single IP address (192.168.1.1), multiple IP addresses separated with "," (192.168.1.1,192.168.1.2), IP address range (192.168.1.1-192.168.1.255 or 192.168.1.0/24 or 192.168.1.0/255.255.255.0);
 - 3. Port rule supports a single port, multiple ports separated with "," (80,90) and port range (80-90).
- Enable Transaction Analysis:**
 - ☐ Enable Transaction Analysis
 - Select Transaction:
- Enable Performance Analysis:**
 - ☐ Enable Performance Analysis
 - ☐ Truncate all packets to bytes
- Buttons: OK, Cancel

On the **Standard Application** dialog box, enter the application name as well as the description, enter the field value if available.

Set the reference response time. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time is three times of good response time, and bad response time is ten times of normal response time. You can also modify normal response time and bad response time manually.


Click  to add an application rule, which could be the combination of a single port, multiple ports, port range, an IP address, multiple IP addresses, and IP address range.

Set whether to enable transaction analysis. When transaction analysis is enabled, choose a transaction group, and then the related transaction analysis will be done for the application.

Set whether to enable performance analysis. Only when the performance analysis is enabled, the application will be monitored and analyzed.


Set whether to truncate the packets of that application to a specified length. Please note that this setting will be invalid when it is greater than the setting on storage filter.

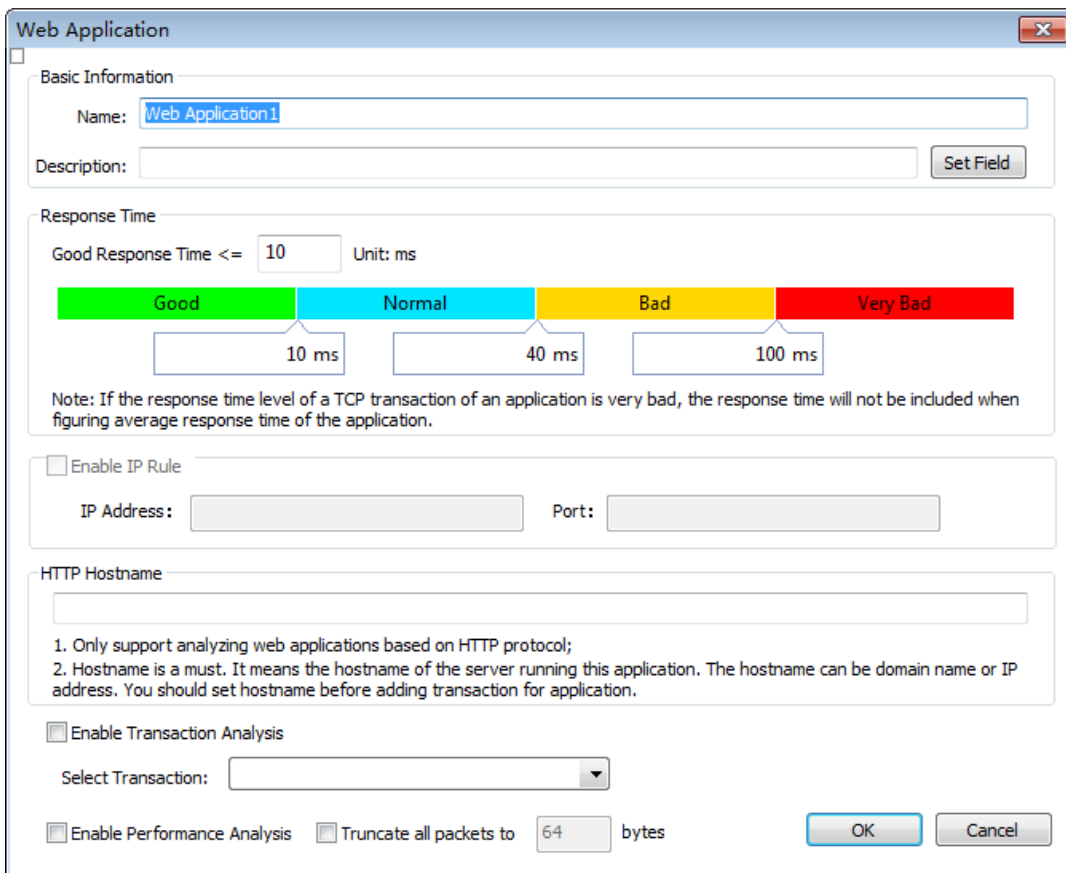
Click **OK** on the **Analysis Settings** tab to completely add a standard application.

-  **Tips** If you want to add specific fields for an application, you should first define fields on the Field Definition tab of the Link Properties dialog box, and then enter the value for the fields.

Adding a web application

To add a web application, follow the steps below:

- 1, Click  on the **Analysis Settings** tab to open the Web Application dialog box as the following figure:



The **Web Application** dialog box is shown with the following fields and options:

- Basic Information**
 - Name:
 - Description: Set Field
- Response Time**
 - Good Response Time <= Unit: ms
 - Response time scale: **Good** (0-10 ms), **Normal** (10-40 ms), **Bad** (40-100 ms), **Very Bad** (100+ ms)
 - Note: If the response time level of a TCP transaction of an application is very bad, the response time will not be included when figuring average response time of the application.
- Enable IP Rule**
 - ☐ Enable IP Rule
 - IP Address: Port:
- HTTP Hostname**
 -
 - 1. Only support analyzing web applications based on HTTP protocol;
 - 2. Hostname is a must. It means the hostname of the server running this application. The hostname can be domain name or IP address. You should set hostname before adding transaction for application.
- Enable Transaction Analysis**
 - ☒ Enable Transaction Analysis
 - Select Transaction:
- Enable Performance Analysis**
 - ☐ Enable Performance Analysis
 - ☐ Truncate all packets to bytes
- Buttons**: OK Cancel

On the **Web Application** dialog box, enter the application name as well as the description, and enter the field value if available.

Name: The name of the application.

Description: The description of the application, for reference use.

Set Field: This section is only available when there are fields predefined on the **Field Definition** tab of the **Link Properties** dialog box.

Set the reference response time. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time is three times of good response time, and bad response time is ten times of normal response time. You can also modify normal response time and bad response time manually.

Enter the hostname, for example, www.colasoft.com. The web applications only identify HTTP protocol.

If necessary, enable Transaction Analysis and choose a transaction.


Set whether to enable performance analysis. Only when the performance analysis is enabled, the application will be monitored and analyzed.

Set whether to truncate the packets of that application to a specified length. Please note that this setting will be invalid when it is greater than the setting on storage filter.

Click **OK**, and then click **OK** on the **Analysis Settings** tab to successfully add a web application.

Adding a signature application

To add a signature application, follow the steps below:

- 1, Click  on the **Analysis Settings** tab to open the Signature Application dialog box as the following figure:

Signature Application

Basic Information

Name:

Description:

Response time

Good response time <= Unit:ms

Good
Normal
Bad
Very Bad

Note: If the response time level of a TCP transaction of an application is very bad, the response time will not be included when figuring average response time of the application.

☐ Enable IP Rule

IP Address:

Signature rule

Signature	Type
No data to display	

☐ Enable Performance Analysis
 ☐ Truncate all packets to bytes

On the **Signature Application** dialog box, enter the application name as well as the description, and enter the field value if available.

Name: The name of the application.

Description: The description of the application, for reference use.

Response time: Used to set the response quality baseline time to apply a TCP transaction. After the user modify "good response time", the system will automatically calculate the average response time "and" poor response time, "default" general response time "for four times" good response time ", "poor response time" for 10 times "good response time", the user can also select the "general response time" or the value of the response time of the "poor", modify the corresponding values. Enabling Key Applications

IP rules: This parameter is used to configure IP rules for protocol application.


Select agreement: Protocol rules used to configure applications.

Enable transaction analysis: After this function is enabled, you can select a set trading group in The Trading Settings section. After the protocol is configured, the system can analyze

transactions for the protocol application.

Enabling Key Applications: After this function is enabled, the system can monitor and analyze the protocol application.


Set the reference response time. When the good response time is set, normal response time and bad response time will be calculated automatically. By default, normal response time is three times of good response time, and bad response time is ten times of normal response time. You can also modify normal response time and bad response time manually.

Click  to define a signature rule.

Set whether to enable performance analysis. Only when the performance analysis is enabled, the application will be monitored and analyzed.

Set whether to truncate the packets of that application to a specified length. Please note that this setting will be invalid when it is greater than the setting on storage filter.






Click **OK** on the **Signature Application** dialog box, and then click **OK** on the **Analysis Settings** tab to successfully add a signature application.

-  **Tips** The option Application Performance Analysis on the Signature Application dialog box is for enabling the performance analysis of the application. It has the same function with the column Performance Analysis on the Analysis Settings tab.

Application Groups

The Application Groups tab is provided to group applications. Once application groups are defined, the Application Group view will do traffic statistics based on the groups.

The Application Groups tab shows as the screenshot below:

Application Groups		
<div>      </div> <div>Search: <input type="text"/></div>		
Name	Applications Included	Type
165	10.141.165.2:80,10.141.165.58:12063,10.141.165.251,10.141.165.209:80,10.141.165.61:88	Test

Buttons

The following list describes the buttons on this tab:



: Adds an application group.



: Edits the selected application group.



: Deletes the selected application group.




: Imports application group configurations from a file.



: Exports current application group configurations to a file.

Adding an application group

To add an application group, follow the steps below:

1. Click the button  to open the **Application Group** dialog box.







The screenshot shows the 'Application Group' dialog box. It has a title bar with a close button. Inside, there are two text input fields: 'Name:' with the value '165' and 'Type:' with the value 'Test'. Below these is a section 'Applications Included:' with a dropdown menu set to 'All Applications' and a search box. A list of applications follows, each with a checkbox: 'C... Application' (unchecked), 'UPM - Web Server' (checked), 'UPM - App Server' (checked), 'UPM - DB Server' (checked), 'Amazon' (unchecked), 'Amazon Web Services' (unchecked), 'Google Analytics' (unchecked), 'Google Play' (unchecked), 'KapaoTalk' (unchecked), and 'Adobe' (unchecked). At the bottom are 'OK' and 'Cancel' buttons.



On the **Application Group** dialog box, enter an appropriate name for the application group, specify the type, and check the applications included. You can use the drop-down list and search box to display desired applications. The applications could be system applications and user-defined applications.

Click **OK** on the **Application Group** dialog box, and then click **OK** on the **Application Group** tab.

Application Alarms

This tab is provided to define application alarms on the monitored applications, and the statistical object can be the traffic of a specific custom application, a specific client, a network segment, or a server using monitored applications. This tab shows as the following figure:

Application Alarms						
     						
Ena...	Name	Categ...	Type	Seve...	Creation Time	Description
<input type="checkbox"/>	UPM - Co...	Abno...	Applicatio...	Severe	05/26/2020 17:...	The host s...
<input type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Select the ...
<input checked="" type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	High	05/26/2020 17:...	Adjust the ...
<input checked="" type="checkbox"/>	UPM - Ser...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Apply to fi...
<input checked="" type="checkbox"/>	UPM - Ba...	Abno...	Applicatio...	Severe	05/26/2020 17:...	It shouldn'...
<input checked="" type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Apply to a...
<input type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Assess the ...
<input type="checkbox"/>	UPM - Ap...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Adjust thr...
<input type="checkbox"/>	UPM - Int...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Bad netwo...
<input type="checkbox"/>	UPM - Ne...	Abno...	Applicatio...	Severe	05/26/2020 17:...	This alarm ...
<input checked="" type="checkbox"/>	UPM - Co...	Abno...	Applicatio...	Severe	05/26/2020 17:...	The host s...
<input checked="" type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Select the ...
<input checked="" type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	High	05/26/2020 17:...	Adjust the ...
<input checked="" type="checkbox"/>	UPM - Ser...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Apply to fi...
<input checked="" type="checkbox"/>	UPM - Ba...	Abno...	Applicatio...	Severe	05/26/2020 17:...	It shouldn'...
<input type="checkbox"/>	UPM - Hi...	Abno...	Applicatio...	Severe	05/26/2020 17:...	Apply to a...

-  **Note** You should first configure custom applications before defining application alarms, or else the application alarms will be unavailable.
- This tab lists all application alarms according to name, severity, category, object, application, address/segment, description, and so on.
-  **Tips** When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.
- To enable an alarm, just select the **Enable** checkbox.

Buttons

The following list describes the icon buttons on this tab:



: Adds a new application alarm. You can create simple application alarms or advanced application alarms.



: Copies the selected alarm.



: Edits the selected alarm.



: Deletes the selected alarm.




: Imports application alarms from a backup file.

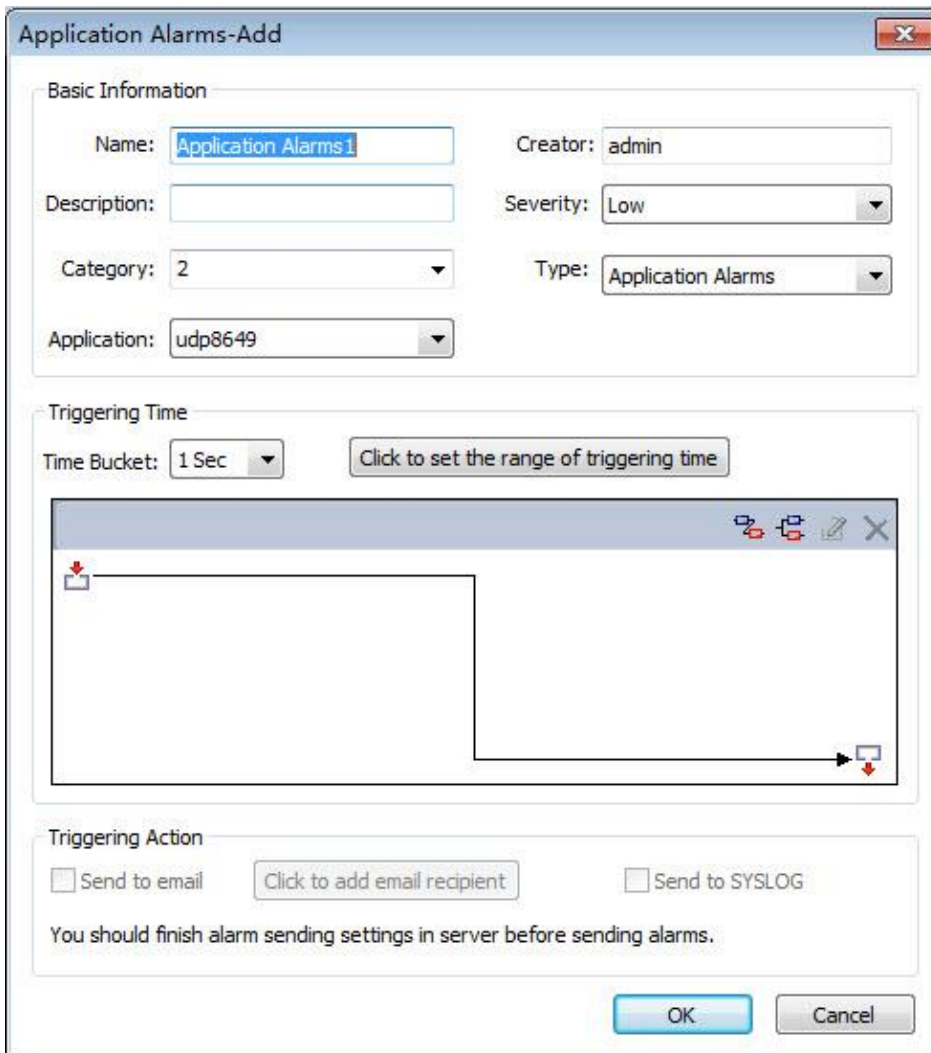


: Exports current application alarms to a file.

Adding an application alarm

To add an application alarm, follow the steps below:

1. Click  on the **Application Alarms** tab to open the **Application Alarms-Add** dialog box as the following figure:



On the **Application Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Severity: The severity of the new alarm. It could be Minor, Major, and Severe.

Description: The description of the alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of the application alarm.

Application: The application that the alarm is made for.

Set the trigger condition. The Time Bucket parameter is the statistical duration of the trigger value.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

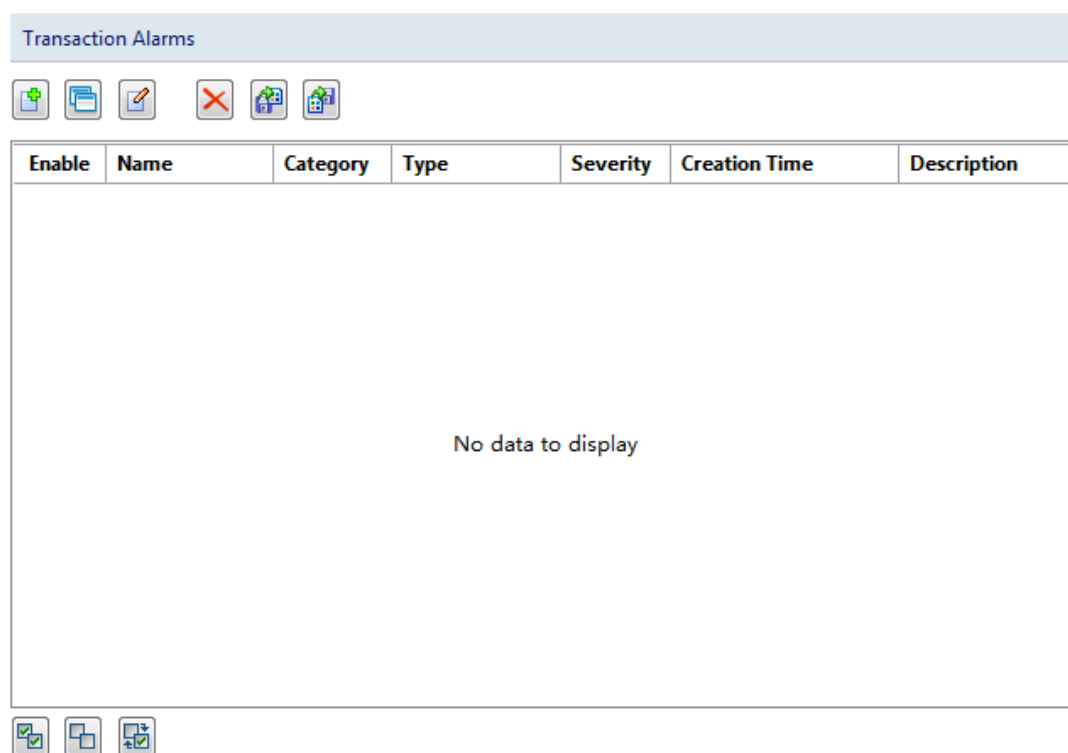
Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the CSNRAS Server.

Click **OK** to save the settings.

Transaction Alarms

This tab is provided to define transaction alarms on the applications that enable their transaction analysis. This tab shows as the following figure:



Note Before defining transaction alarms, you should first configure web applications and enable the transaction analysis for the applications.

This tab lists all transaction alarms according to name, severity, category, object, application, transaction, description, create time, and creator.

Tips When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.

To enable an alarm, just select the **Enable** checkbox.

Buttons

The following list describes the icon buttons on this tab:



: Adds a new transaction alarm.



: Copies the selected alarm.



: Edits the selected alarm.



: Deletes the selected alarm.



: Imports alarms from a backup file.



: Exports current alarms to a file.

Adding a transaction alarm

To add a transaction alarm, follow the steps below:

1. Click to open the Transaction Alarms-Add dialog box as the following figure:

The screenshot shows the 'Transaction Alarms-Add' dialog box with the following sections:

- Basic Information:**
 - Name: Transaction Alarms1
 - Creator: admin
 - Description: (empty)
 - Severity: Low
 - Category: Worm
 - Application: Transaction statistics
 - Type: Standard Application1
 - Transaction: Collection
 - All Transactions (checkbox)
 - Set trigger dimension button
- Triggering Condition:**
 - Time Bucket: 1 Sec
 - Duration: 0
 - Set the range of triggering time button
 - Diagram area showing a sequence of events with a red arrow pointing to a red square.
- Triggering Action:**
 - ☐ Send to email
 - Click to add email recipient button
 - ☐ Send to SYSLOG
 - You should finish alarm sending settings in server before sending alarms.

Buttons: OK, Cancel

On the **Transaction Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the alarm.

Severity: The severity of the new alarm. It could be Minor, Major, and Severe.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of alarm.

Application: This option is for specifying an application.

Transaction: This option is for specifying a transaction.

Set the trigger condition. The Time Bucket parameter is the statistical duration of the trigger value.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the nChronos Server.










Click **OK** to save the settings.

Drilling down a transaction alarm

You can drill down a transaction alarm for more detailed information. To drill a transaction alarm, right-click the item, then click Drill Down and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click Drill Down to drill down more information.

Millisecond Traffic Alarms

This tab is provided to define millisecond traffic alarms. Traffic Alarm has the statistics calculated based on seconds, while Millisecond Traffic Alarm has the statistics calculated based on milliseconds.

Millisecond Traffic Alarms						
     						
Enable	Name	Category	Type	Severity	Creation Time	Description
No data to display						
  						

This tab lists all millisecond traffic alarms according to alarm name, severity, category, description, create time, and creator.



Tips

When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.

To enable an alarm, just select the **Enable** checkbox.

Buttons

The following list describes the icon buttons on this tab:



: Adds a new millisecond traffic alarm.



: Copies the selected alarm.



: Edits the selected alarm.



: Deletes the selected alarm.



: Imports alarms from a backup file.

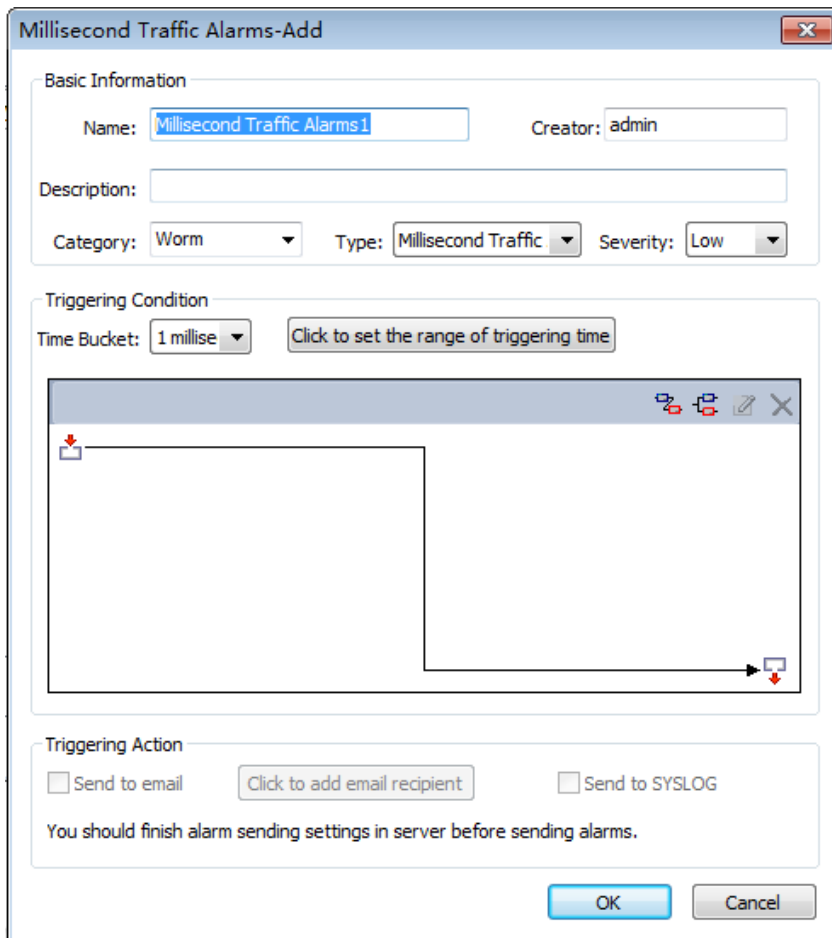


: Exports current alarms to a file.

Adding a millisecond traffic alarm

To add a transaction alarm, follow the steps below:

1. Click  to open the Millisecond Traffic Alarms-Add dialog box as the following figure:



Millisecond Traffic Alarms-Add

Basic Information

Name: Creator:

Description:

Category: Type: Severity:

Triggering Condition

Time Bucket:

Triggering Action

☐ Send to email ☐ Send to SYSLOG

You should finish alarm sending settings in server before sending alarms.

On the **Millisecond Traffic Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of alarm.

Severity: The severity of the new alarm. It could be Minor, Major, and Severe.

Set the trigger condition. The Time Bucket parameter is the statistical duration of the trigger value.


Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.







Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the nChronos Server.

Click **OK** to save the settings.

 **Note** Millisecond traffic alarm is available for configuration only when the millisecond statistics feature is enabled for the network link.

Traffic Alarms

This tab is provided to configure traffic alarms on the traffic of the network, including, packets, bytes, and average packet size. When capturing eligible traffic, the traffic alarms will be triggered. This tab shows as the following figure:

Traffic Alarms						
						
Ena...	Name	Categ...	Type	Seve...	Creation Time	Description
<input checked="" type="checkbox"/>	UPM - slo...	333	Network ...	High	05/18/2020 14:...	
<input checked="" type="checkbox"/>	UPM - IC...	333	IP Conver...	Low	05/20/2020 17:...	
<input checked="" type="checkbox"/>	UPM - IC...	333	IP Conver...	Severe	05/28/2020 14:...	
<input type="checkbox"/>	test77	333	Global	Low	05/26/2020 15:...	
<input checked="" type="checkbox"/>	Host Scan	Attack	Network ...	Severe	09/06/2015 09:...	
<input checked="" type="checkbox"/>	SYN Floo...	Attack	Internal IP...	Low	09/06/2015 09:...	
<input checked="" type="checkbox"/>	CIFS Wor...	Worm	Network ...	Low	09/06/2015 09:...	
<input checked="" type="checkbox"/>	Abnormal...	Abno...	Internal IP...	Low	09/06/2015 09:...	Two many ...

Buttons

The following list describes the icon buttons on this tab:



: Adds a new traffic alarm.



: Copies the selected alarm.



: Edits the selected alarm.



: Deletes the selected alarm.




: Imports traffic alarms from a file.

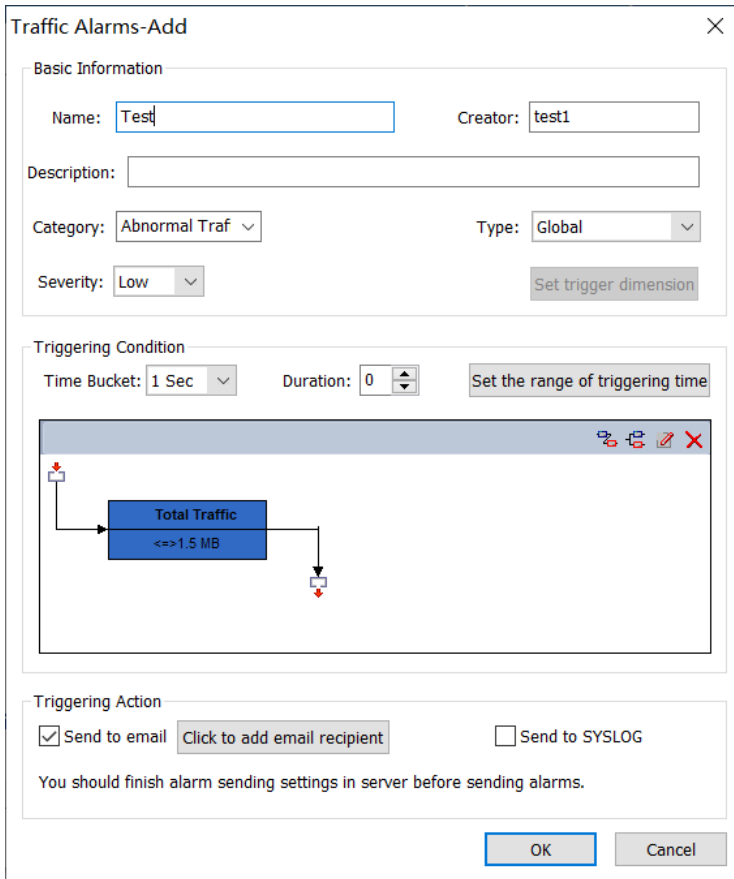


: Exports current traffic alarms to a file.

Adding a traffic alarm

To add a traffic alarm, follow the steps below:

1. Click  to open the Traffic Alarms-Add dialog box as the following figure:



The dialog box is titled "Traffic Alarms-Add" and contains three main sections:

- Basic Information:**
 - Name:
 - Creator:
 - Description:
 - Category:
 - Type:
 - Severity:
 - Set trigger dimension
- Triggering Condition:**
 - Time Bucket:
 - Duration:
 - Set the range of triggering time
 - Diagram: A flowchart showing a box labeled "Total Traffic" with a condition "<=>1.5 MB" below it. An arrow points from the box to a small square icon with a red cross.
- Triggering Action:**
 - ☒ Send to email
 - ☐ Send to SYSLOG
 - You should finish alarm sending settings in server before sending alarms.

Buttons: OK, Cancel

On the Traffic Alarms-Add dialog box, complete the **Basic Information** section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of alarm.

Severity: The severity of the new alarm. It could be Minor, Major, and Severe.

Set the trigger condition. The Time Bucket parameter is the statistical duration of the trigger value.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

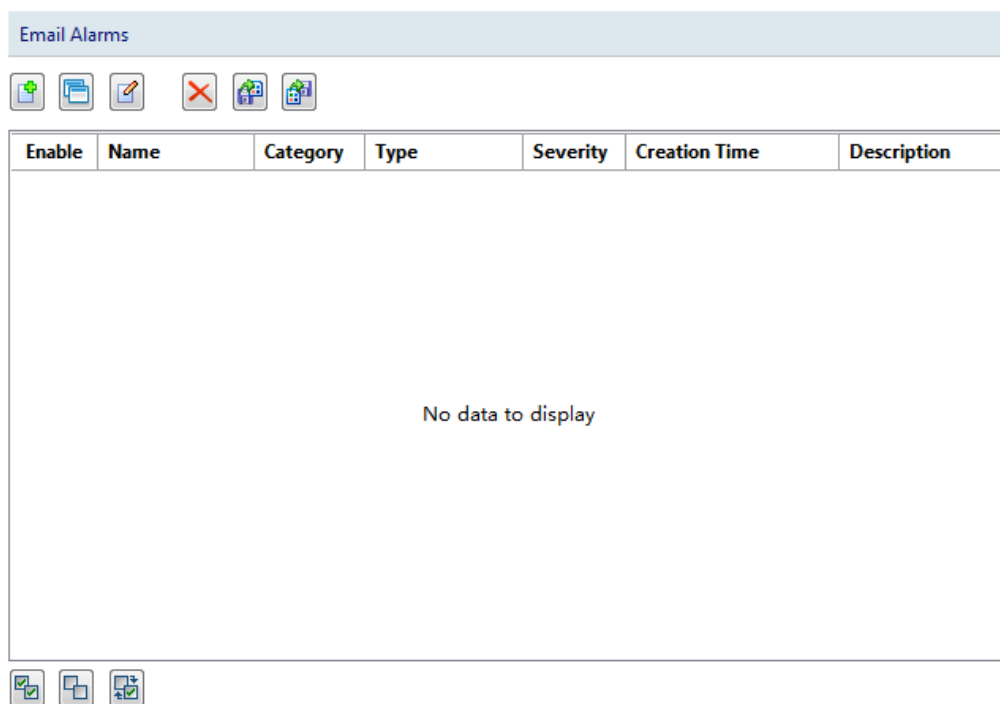
Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the nChronos Server.

Click to **OK** save the settings.

Email Alarms

This tab shows as the following figure:



Email alarms can be created for the emails over the network. When the emails contain the defined keywords, the email alarms will be triggered.

Buttons

The following list describes the icon buttons on this tab:



: Adds a new email alarm.



: Copies the selected alarm.



: Edits the selected alarm.



: Deletes the selected alarm.



: Imports email alarms from a file.



: Exports current email alarms to a file.

Columns

The following list describes the table columns on this tab:

Enable: Shows which alarms are enabled.

Name: The name of the alarms.


Category: The category of the alarms.

Type: The type of the alarms.

Severity: The severity of the alarms.


Creation Time: The time when the alarms are created.

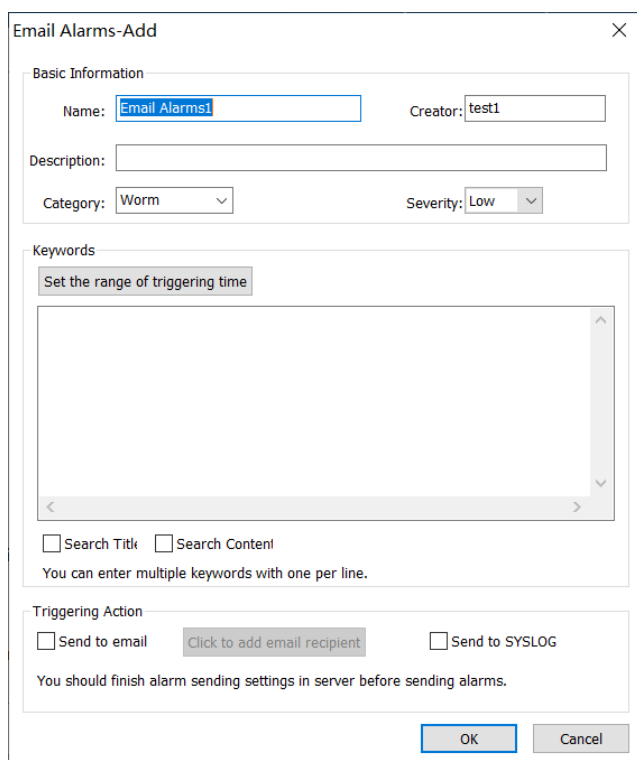
Description: The description of the alarms.

-  **Tips** When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.

Creating an email alarm

To create an email alarm, follow the steps below:

1. Click  on the **Email Alarms** tab to open the **Email Alarms-Add** dialog box as the following figure:



The dialog box titled "Email Alarms-Add" contains the following sections:

- Basic Information:**
 - Name:
 - Creator:
 - Description:
 - Category:
 - Severity:
- Keywords:**
 - Set the range of triggering time
 - ☐ Search Title ☐ Search Content
 - You can enter multiple keywords with one per line.
- Triggering Action:**
 - ☐ Send to email
 - ☐ Send to SYSLOG
 - You should finish alarm sending settings in server before sending alarms.

Buttons:

On the **Email Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the options:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the new alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Severity: The severity of the new alarm. It could be *Minor*, *Major*, and *Severe*.

Enter the keywords. The keywords are the trigger condition of the email alarm. You can enter multiple keywords in one email alarm, with one per line.

Specify where to search the keywords.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are specified in **Alarm Notification**.

Click **OK** to save the settings.

Domain Alarms

This tab shows as the following figure:

Domain Alarms						
Ena...	Name	Categ...	Type	Seve...	Creation Time	Description
<input checked="" type="checkbox"/>	Dynamic ...	Worm	Domain Al...	Low	09/06/2015 10:...	Trojan or ...
<input checked="" type="checkbox"/>	Botnet	Worm	Domain Al...	Low	09/06/2015 10:...	
<input checked="" type="checkbox"/>	zeus botnet	Worm	Domain Al...	Low	09/06/2015 10:...	
<input checked="" type="checkbox"/>	WannaCry	Worm	Domain Al...	Low	08/29/2018 17:...	

Domain alarms can be created for the domain names visited over the network. When visiting the defined domains, the domain alarms will be triggered.

Buttons

The following list describes the icon buttons on this tab:



: Adds a new domain alarm.



: Copies the selected alarm.



: Edits the selected alarm.



: Deletes the selected alarm.



: Imports domain alarms from a file.



: Exports current domain alarms to a file.

Columns

The following list describes the table columns on this tab:

Enable: Shows which alarms are enabled.

Name: The name of the alarms.


Category: The category of the alarms.

Type: The type of the alarms.

Severity: The severity of the alarms.


Creation Time: The time when the alarms are created.

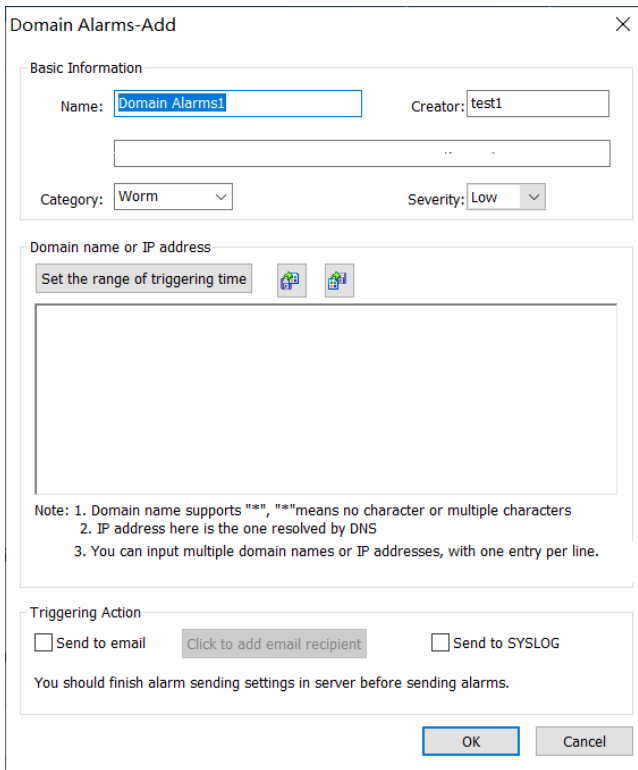
Description: The description of the alarms.

-  **Tips** When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.

Creating a domain alarm

To create a domain alarm, follow the steps below:

1. Click  on the **Domain Alarms** tab to open the **Domain Alarms-Add** dialog box as the following figure:





Domain Alarms-Add

Basic Information

Name: Creator:

Category: Severity:

Domain name or IP address

Set the range of triggering time  

Note: 1. Domain name supports "*", "*" means no character or multiple characters
2. IP address here is the one resolved by DNS
3. You can input multiple domain names or IP addresses, with one entry per line.

Triggering Action

☐ Send to email ☐ Send to SYSLOG

You should finish alarm sending settings in server before sending alarms.

On the **Domain Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the options:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the new alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Severity: The severity of the new alarm. It could be Minor, Major, and Severe.

Enter the domain names and/or addresses. The domain names and the addresses are the trigger condition of the domain alarm. You can enter multiple domain names and addresses in one domain alarm, with one per line.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can enter multiple keywords in one email alarm, with one per line.

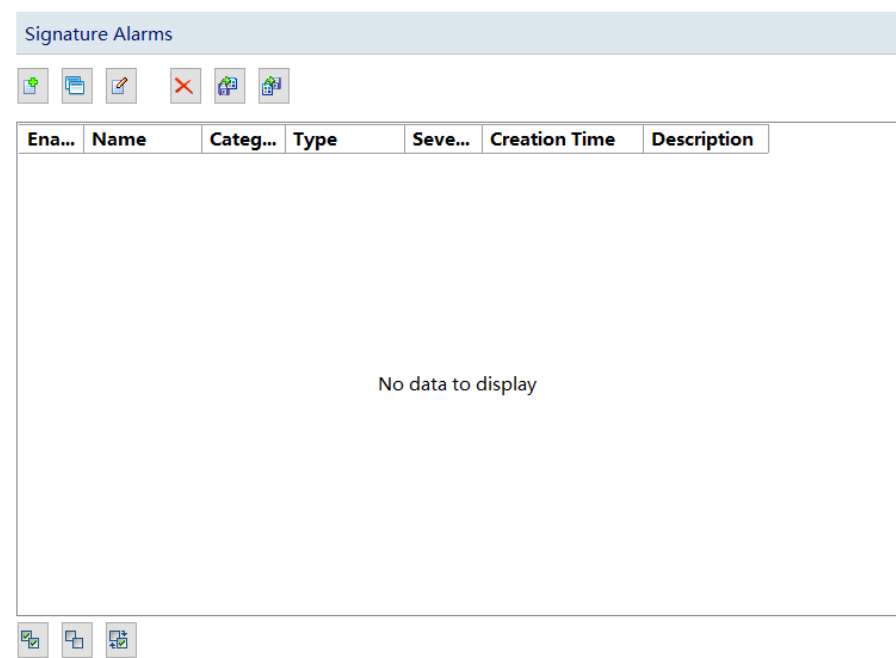
Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are specified in **Alarm Notification**.

Click **OK** to save the settings.

Signature Alarms


This tab shows as the following figure:





Signature alarms can be created for the flows over the network. When capturing the defined signature flow, the signature alarms will be triggered.


Buttons

The following list describes the icon buttons on this tab:


: Adds a new signature alarm.

: Copies the selected alarm.

: Edits the selected alarm.

: Deletes the selected alarm.

: Imports signature alarms from a file.

: Exports current signature alarms to a file.

Columns

The following list describes the table columns on this tab:

Enable: Shows which alarms are enabled.

Name: The name of the alarms.


Category: The category of the alarms.

Type: The type of the alarms.

Severity: The severity of the alarms.


Creation Time: The time when the alarms are created.

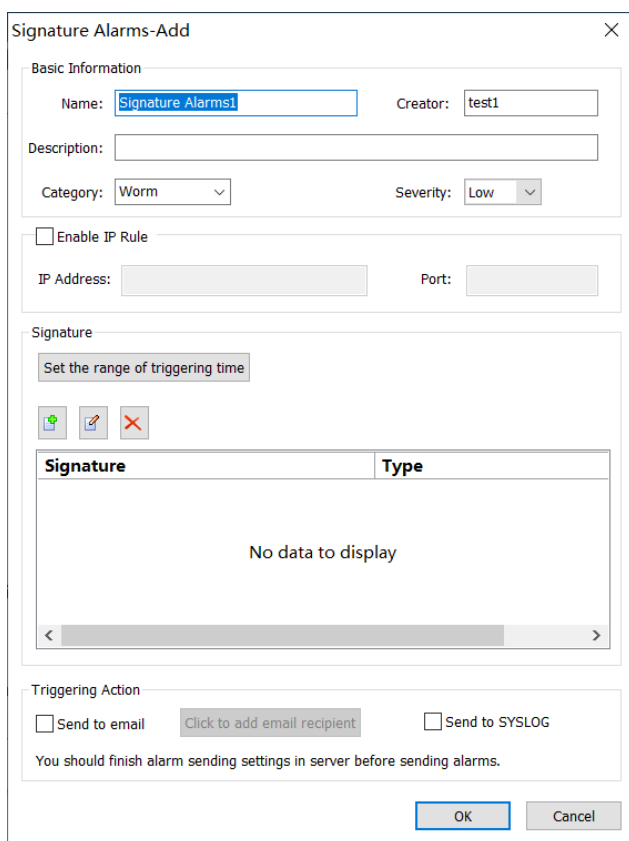
Description: The description of the alarms.

-  **Tips** When the column does not have enough space for displaying the texts, you can just move your mouse on the line between columns and drag to enlarge the space.




Creating a signature alarm

To create a signature alarm, follow the steps below:

1. Click  on the **Signature Alarms** tab to open the Signature Alarms-Add dialog box:



The dialog box is titled "Signature Alarms-Add" and contains the following sections:

- Basic Information:**
 - Name:
 - Creator:
 - Description:
 - Category:
 - Severity:
- Enable IP Rule:**
 - ☐ Enable IP Rule
 - IP Address:
 - Port:
- Signature:**
 - Set the range of triggering time:
 - Buttons:   
 - Table:

Signature	Type
No data to display	
- Triggering Action:**
 - ☐ Send to email
 - ☐ Send to SYSLOG
 - You should finish alarm sending settings in server before sending alarms.

Buttons:

On the **Signature Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the options:

Name: The name of the new alarm.


Creator: The person who defines this alarm.

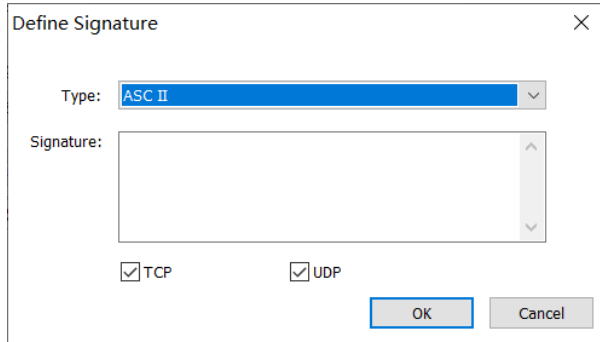
Description: The description of the new alarm.

Category: The category of the new alarm. You can just enter the category or click the little

triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Severity: The severity of the new alarm. It could be Minor, Major, and Severe.

Click  at the bottom section of this tab to add a triggering condition, which appears as below:



The dialog box titled "Define Signature" contains the following elements:

- Type:** A dropdown menu currently showing "ASC II".
- Signature:** A large text input area for defining the signature value.
- Protocol Checkboxes:** Two checkboxes labeled "TCP" and "UDP", both of which are checked.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

The following list describes the options on this dialog box.

Type: The type of the packet decoding information.

Signature: The signature value of the alarm.

Set the sending parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

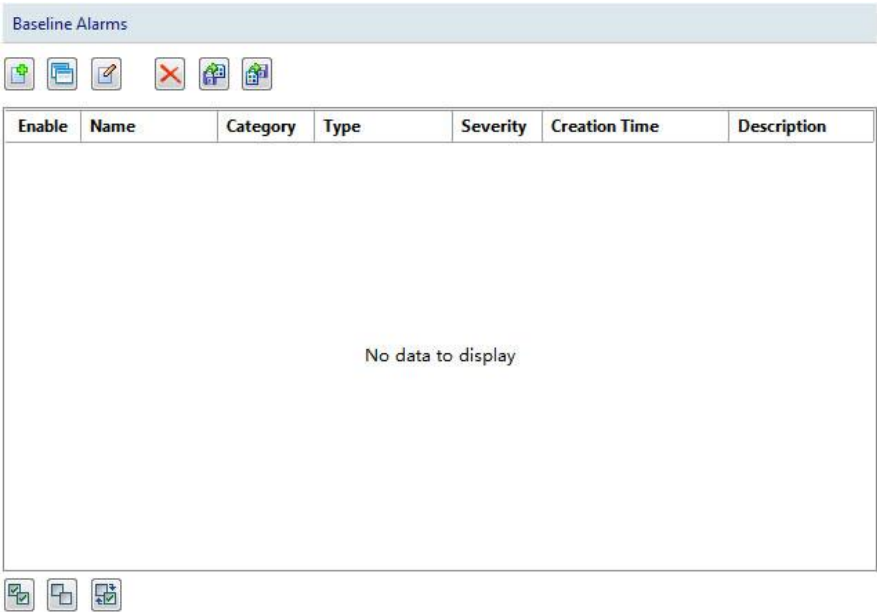
Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are specified in **Alarm Notification**.

Click **OK** to save the settings.







Baseline Alarms

The Baseline Alarms tab is provided to configure baseline alarms. When the deviation of the actual data from the baseline data reaches the defined condition, the alarm will be triggered. The tab shows as the following figure:



Buttons

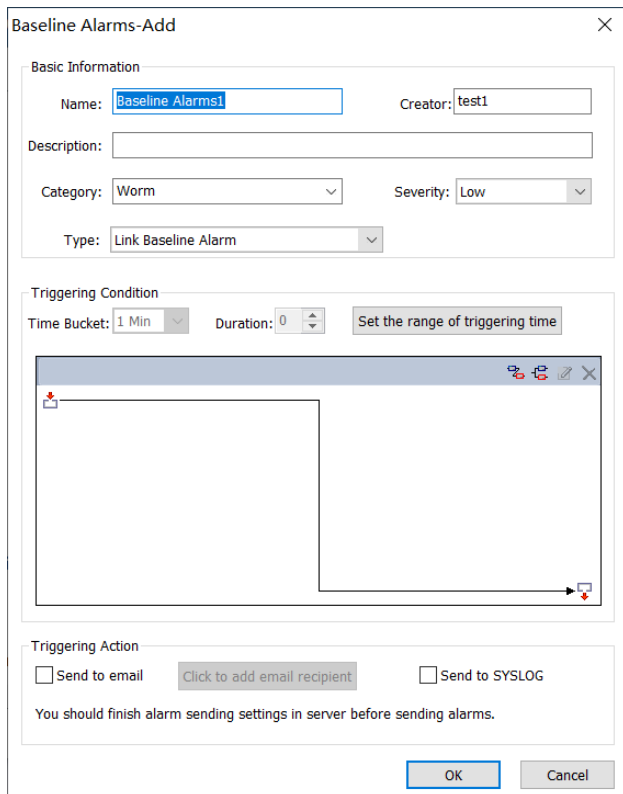
The following list describes the icon buttons on this tab:

- : Adds a new baseline alarm.
- : Copies the selected alarm.
- : Edits the selected baseline alarm.
- : Deletes the selected baseline alarm.
- : Imports baseline alarm configurations from a file.
- : Exports current baseline alarm configurations to a file.

Adding a baseline alarm

To add a baseline alarm, follow the steps below:

1. Click the button  to open the Baseline Alarms-Add dialog box as the following figure:



On the **Baseline Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of alarm.

Severity: The severity of the new alarm. It could be *Minor*, *Major*, and *Severe*.

Set the trigger condition.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

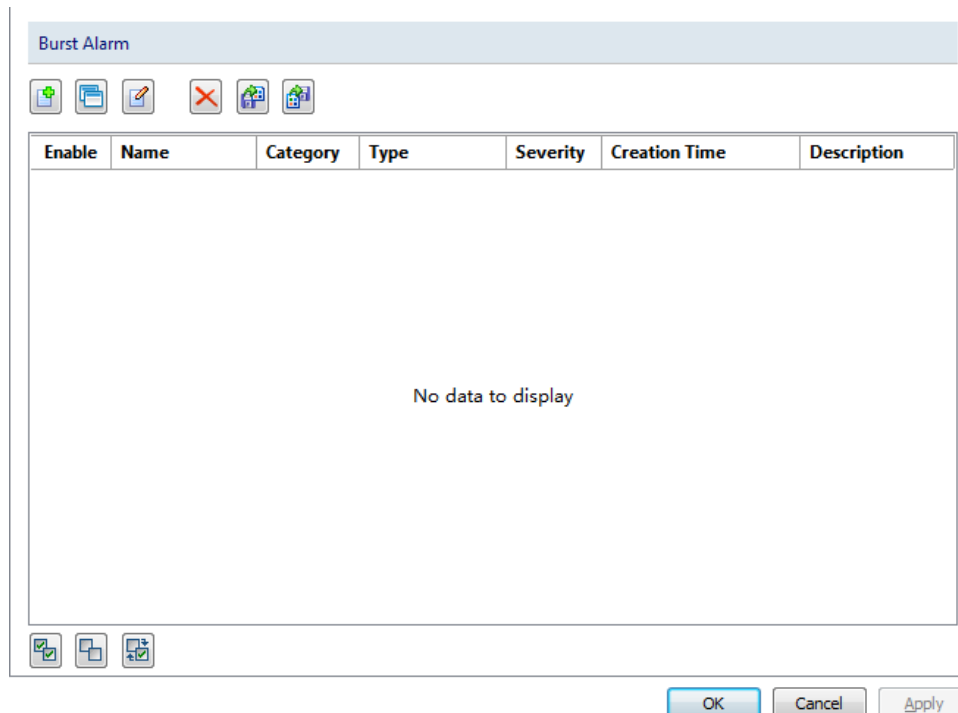
Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the nChronos Server.

Click **OK** to save the settings.

Burst Alarms

The Burst Alarm tab is provided to configure a burst alarm. Burst alarm is used to warn of abnormal burst. In order to improve the accuracy of alarm, the system will compare the captured data with those of the previous N cycles. At the same time, the captured data can be also compared with the baseline data and index threshold data. The Burst Alarm tab shows as the screenshot below:



Buttons

The following list describes the icon buttons on this tab:



: Adds a new baseline alarm.



: Copies the selected alarm.



: Edits the selected baseline alarm.



: Deletes the selected baseline alarm.



: Imports baseline alarm configurations from a file.

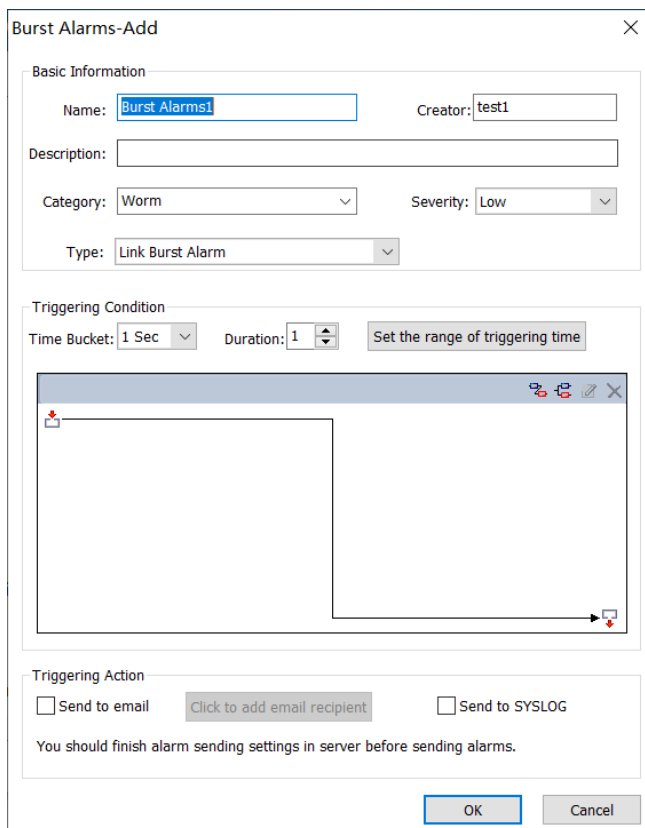


: Exports current baseline alarm configurations to a file.

Adding a burst alarm

To add a burst alarm, follow the steps below:

1. Click the button  to open the Burst Alarms-Add dialog box as the following figure:



The dialog box is titled "Burst Alarms-Add" and contains three main sections:

- Basic Information:**
 - Name:
 - Creator:
 - Description:
 - Category:
 - Severity:
 - Type:
- Triggering Condition:**
 - Time Bucket:
 - Duration:
 - Set the range of triggering time
- Triggering Action:**
 - ☐ Send to email
 - ☐ Send to SYSLOG
 - You should finish alarm sending settings in server before sending alarms.

Buttons: OK, Cancel

2. On the Burst Alarms-Add dialog box, complete the **Basic Information** section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of alarm.

Severity: The severity of the new alarm. It could be *Minor*, *Major*, and *Severe*.

3. Set the trigger condition.

4. Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the CSNRAS Server.

- Click OK to save the settings.

Abnormal Access Alarms

The Abnormal Access Alarms tab is provided to configure abnormal access alarms. Each link is configured with two abnormal access alarms by default, **IP access abnormal alarm** and **MAC access abnormal alarm**. The Abnormal Access Alarms tab shows as the screenshot below:

Abnormal Access Alarms						
Ena...	Name	Categ...	Type	Seve...	Creation Time	Description
<input type="checkbox"/>	IP Abnor...	Sensit...	IP Access ...	Severe		
<input checked="" type="checkbox"/>	MAC Abn...	Abno...	MAC Acc...	Severe		

IP Access Abnormal Alarm

Set accessing rules in IP Access Abnormal Alarm. When nChronos detects a conflict between a rule and the set access rule, the abnormal access alarm will be triggered. The dialog box is shown below.

Abnormal Access Alarms-IP Abnormal Access Alarm

Basic Information

Name: IP Abnormal Access Alarm

Creator: ellen

Category: Abnormal Traffic

Severity: Severe

Description:

Triggering Condition

Time: 1 Min

☒ Enable Trigger Inhibition

The range of triggering time

Search:

Group Name

☐ Ena...

Rules

Acc...

Rej...

No data to display

Triggering Action

☐ Send to email

Click to add email recipient

☐ Send to SYSLOG

You should finish alarm sending settings in server before sending alarms.

OK

Cancel

Options

The following list describes the options on this tab:

- **Name:** The name of the IP abnormal access alarm.
- **Creator:** The person who defines the alarm.
- **Description:** The description of the alarm.
- **Category:** The category of the alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.
- **Severity:** The severity of the alarm. It could be Minor, Major, and Severe.
- **Time Bucket:** The time bucket of alarm setting. The time bucket in the baseline alarm is "1 minute" and cannot be modified. If the trigger condition is reached, the baseline alarm will be triggered.
- **The range of triggering time:** The triggering time range of alarm setting. The alarm will only trigger within the specified time range.
- **Triggering Condition:** Set the triggering time and triggering rules.
- **Triggering Action:** Set alarm log sending action when the alarm is triggered.

Access Rule Setting

- Access rules need to be grouped in a certain rule group, usually a rule group represents an access control strategy for an application and a domain.
- Access rules can be set to Accept and Reject. If it is set to Accept, it means that this type of traffic is allowed to be accessed, and the alarm will not be triggered when this type of traffic is detected; if it is set to Reject, then it will be prohibited from being accessed, and when this type of traffic is detected, it will trigger the alarm.
- In the access rule, the destination address and source address support the reverse setting.
- The identification of access rules is related to the order of rules. The rules and the order of rule grouping can be moved with up and down arrows.

To add an IP abnormal access, click the button  to open the Add box and set up the elements.

The screenshot shows a dialog box titled "Add IP Access Abnormally Alarm". It contains the following fields and options:

- Group Name:** A text input field.
- Description:** A text input field.
- Dest. Address:** A dropdown menu with "IP" selected, followed by a text input field and a checkbox labeled "Not".
- Dest. Port:** A dropdown menu with "Port" selected, followed by a text input field.
- Source Address:** A dropdown menu with "IP" selected, followed by a text input field and a checkbox labeled "Not".
- Application:** A dropdown menu with "Any applicati" selected, followed by a text input field.
- Protocol:** A dropdown menu with "Specified pro" selected, followed by a dropdown menu with "RMI" selected.
- Access Strategy:** Two radio buttons: "Accept" and "Reject" (selected).
- Priority:** Two radio buttons: "Set-top" and "Set-bottom" (selected).
- Buttons:** "OK" and "Cancel" buttons at the bottom.

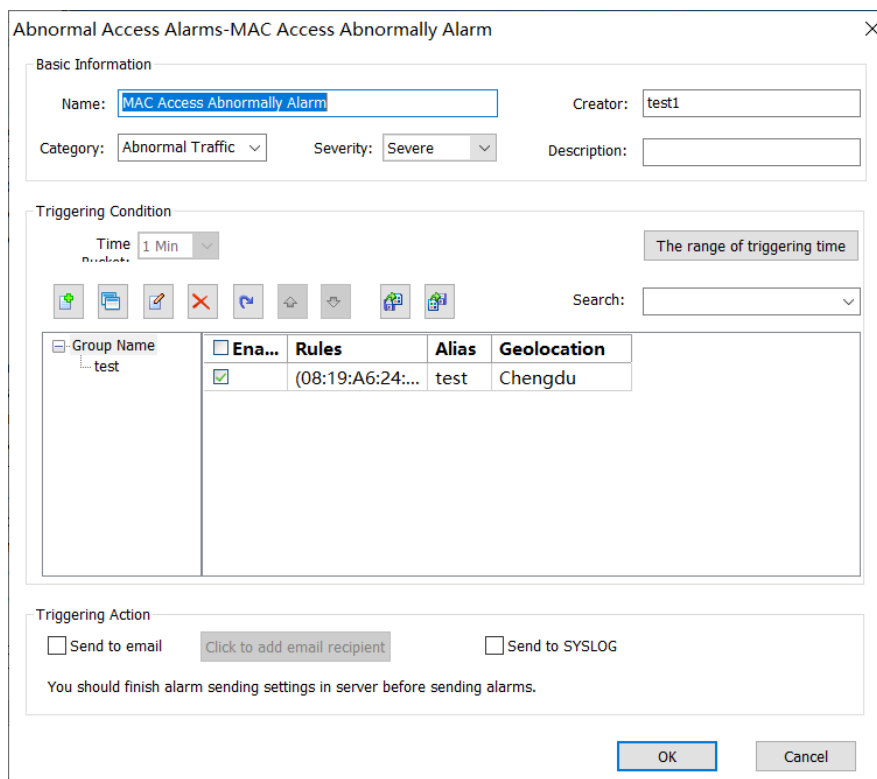
The following list describes the options:

- **Group Name:** The name of the new alarm.
- **Description:** Describe the detailed information of the rule, such as restricting access to an application or server.
- **Dest. Address:** Support IP, network segment and any IP. Support inversion setting.
- **Dest. Port:** Support any port.
- **Source Address:** Support IP, network segment and any IP. Support inversion setting.
- **Application:** Custom application or any application. Support inversion setting.
- **Protocol:** System protocol or any protocol.
- **Access Strategy:** Includes Accept and Reject.
- **Priority:** Includes Set-top and Set-bottom

IP access abnormal alarm provides a trigger inhibition function. After the trigger inhibition function is enabled, the system will merge the alarms according to the access rules every minute. For the same access rule, the trigger sources that meet the access rule will be merged, and only one alarm will be triggered. In the alarm condition of the alarm log, the number of triggers of the access rule will be displayed, and the trigger source will be displayed at the same time.

MAC Access Abnormal Alarm

Set MAC address whitelist in MAC Address Abnormal Alarm. When nChronos detects that there is traffic from a MAC address other than the whitelist, the abnormal access alarm will be triggered. The dialog box is shown below.



The dialog box is titled "Abnormal Access Alarms-MAC Access Abnormally Alarm". It contains three main sections: Basic Information, Triggering Condition, and Triggering Action.

Basic Information:

- Name: MAC Access Abnormally Alarm
- Creator: test1
- Category: Abnormal Traffic
- Severity: Severe
- Description: (empty)

Triggering Condition:

- Time: 1 Min
- The range of triggering time: (empty)
- Search: (empty)
- Group Name: test
- Ena...: (checked)
- Rules: (08:19:A6:24:...
- Alias: test
- Geolocation: Chengdu

Triggering Action:

- Send to email: (unchecked)
- Click to add email recipient: (button)
- Send to SYSLOG: (unchecked)
- You should finish alarm sending settings in server before sending alarms.

Buttons: OK, Cancel


Options

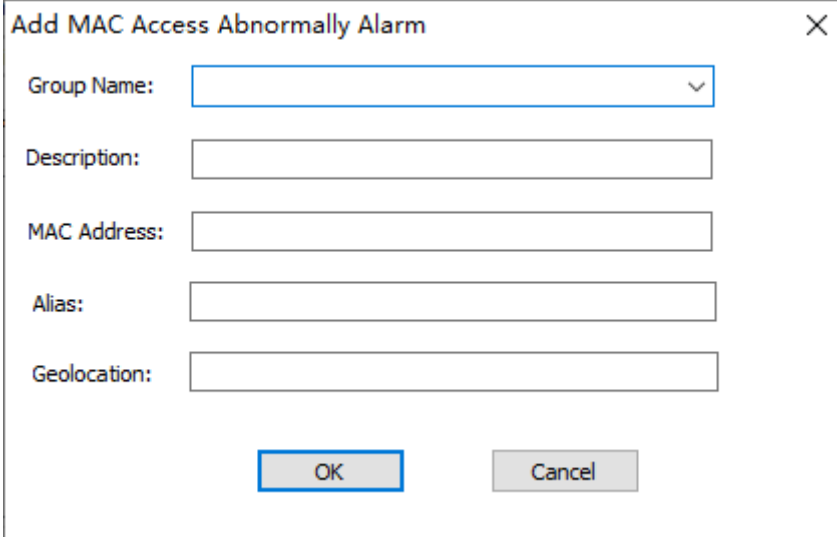
The following list describes the options on this tab:

- **Name:** The name of the MAC abnormal access alarm.
- **Creator:** The person who defines the alarm.
- **Description:** The description of the alarm.
- **Category:** The category of the alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.
- **Severity:** The severity of the alarm. It could be Minor, Major, and Severe.
- **Time Bucket:** The time bucket of alarm setting. The time bucket in the baseline alarm is "1 minute" and cannot be modified. If the trigger condition is reached, the baseline alarm will be triggered.
- **The range of triggering time:** The triggering time range of alarm setting. The alarm will only trigger within the specified time range.
- **Triggering Condition:** Set the triggering time and add blacklist.
- **Triggering Action:** Set alarm log sending action when the alarm is triggered.

Access Rule Setting

- Access rules need to be grouped in a certain rule group, usually a rule group represents an access control strategy for an application and a domain.

To add a single MAC abnormal access, click the button  to open the Add box and set up the elements.

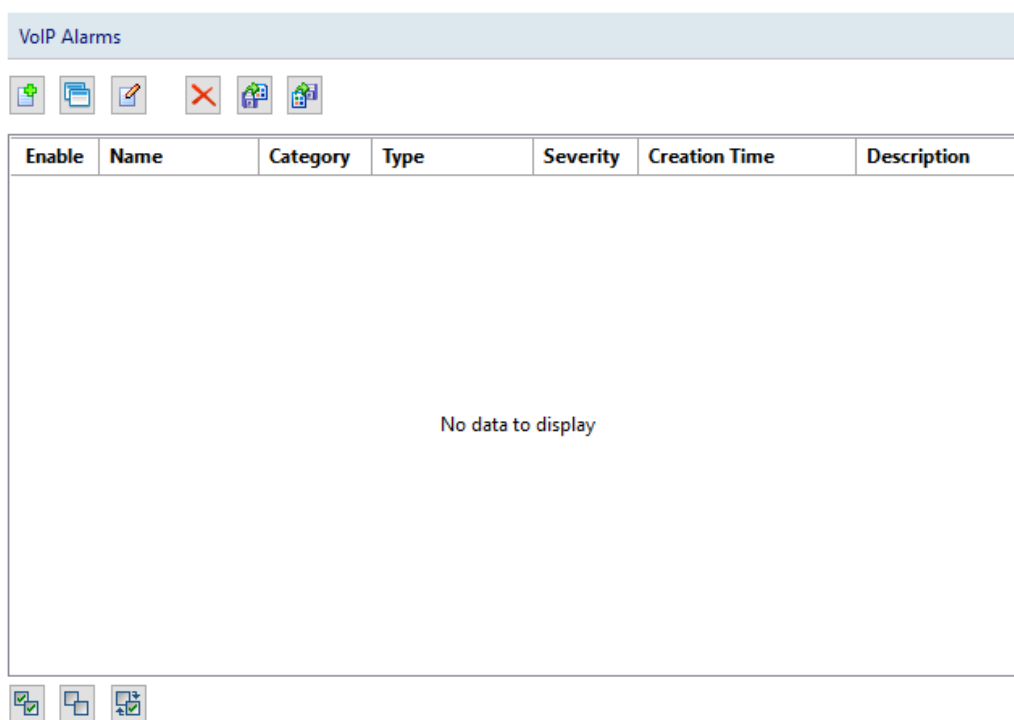


The following list describes the options:

- Group Name: Describe the detailed information of the rule, such as related information of the MAC address.
- Description: The description of the new alarm.
- MAC Address: The MAC address of the new alarm. Only support a single MAC address.
- Alias: The alias of the MAC address, used for checking the MAC address.
- Geolocation: The geolocation of the MAC address, used for checking the MAC address.

VoIP Alarms

In VoIP alarms configuration interface, users can configure and manage VoIP alarms. There are 6 types, including VoIP summary statistics alarms, VoIP conversation alarms, VoIP endpoint alarms, VoIP endpoint conversation alarms, VoIP network segment statistics alarms and VoIP segment-segment statistics alarms. The VoIP Alarm tab shows as the screenshot below:



Buttons

The following list describes the icon buttons on this tab:



: Adds a new baseline alarm.



: Copies the selected alarm.



: Edits the selected baseline alarm.



: Deletes the selected baseline alarm.



: Imports baseline alarm configurations from a file.

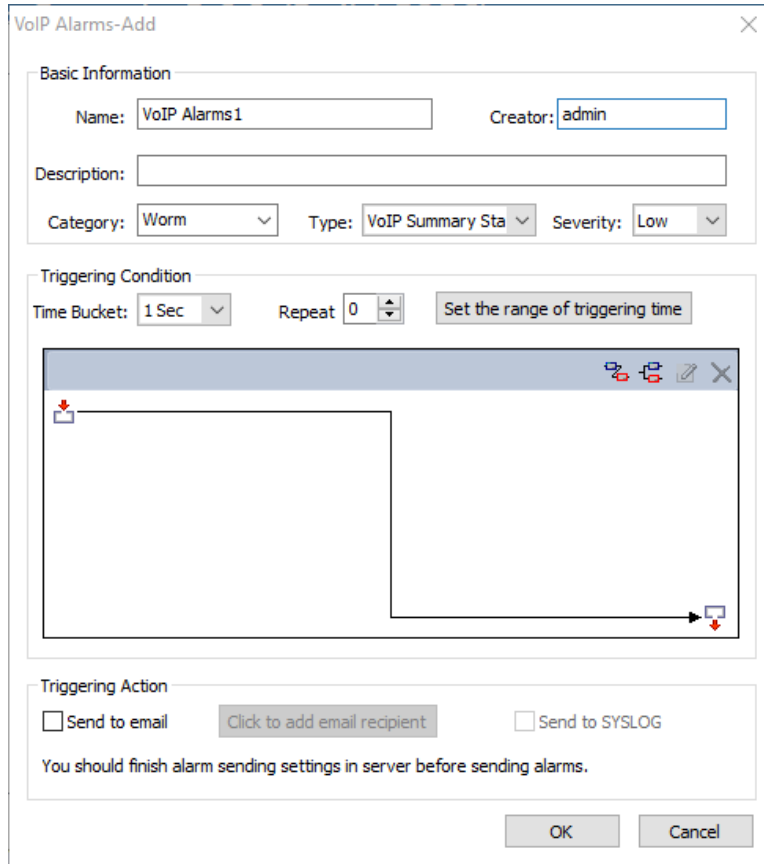


: Exports current baseline alarm configurations to a file.

Adding a VoIP alarm

To add a VoIP alarm, follow the steps below:

1. Click the button  to open the VoIP Alarms-Add dialog box as the following figure:



The dialog box is titled "VoIP Alarms-Add" and contains the following sections:

- Basic Information:**
 - Name: VoIP Alarms1
 - Creator: admin
 - Description: (empty text box)
 - Category: Worm (dropdown menu)
 - Type: VoIP Summary Sta (dropdown menu)
 - Severity: Low (dropdown menu)
- Triggering Condition:**
 - Time Bucket: 1 Sec (dropdown menu)
 - Repeat: 0 (spin box)
 - Set the range of triggering time (button)
 - Diagram area: A large rectangle with a small red square at the top-left corner and a small red square at the bottom-right corner, connected by a line.
- Triggering Action:**
 - ☐ Send to email (button: Click to add email recipient)
 - ☐ Send to SYSLOG
 - You should finish alarm sending settings in server before sending alarms.

Buttons: OK, Cancel

On the VoIP Alarms-Add dialog box, complete the Basic Information section. The following list describes the settings:

Name: The name of the new alarm.

Creator: The person who defines this alarm.

Description: The description of the alarm.

Category: The category of the new alarm. You can just enter the category or click the little triangle to select a category. The category you entered will be memorized for next use and can be used by other alarm types.

Type: The type of alarm.

Severity: The severity of the new alarm. It could be *Minor*, *Major*, and *Severe*.

Set the trigger condition.

Set the send parameters:

Send to email: Sends the alarm log as an email when the alarm is triggered. You can select existing recipients or enter new recipient addresses.

Send to SYSLOG: Sends the alarm log to SYSLOG when the alarm is triggered.

Both the email and the SYSLOG parameters are defined in Alarm Notification when configuring the nChronos Server.

Click **OK** to save the settings.

View Management

There are four tabs under View Management: The Link Retrospective Analysis tab, the Alarms tab, the Application Performance Analysis tab, and the Application Transaction Analysis tab, which are provided to manage the statistical views. You can check a view name to show/hide the view, and you can also click the button to move down/up a view.

The following list describes the icon buttons on this tab:



: Deletes the selected view. Default views cannot be deleted. Only user-defined views can be deleted.



: Edits the selected view. Default views cannot be edited. Only user-defined views can be edited.



: Imports view settings from a file.



: Exports view settings to a file.



: Moves the selected view up.



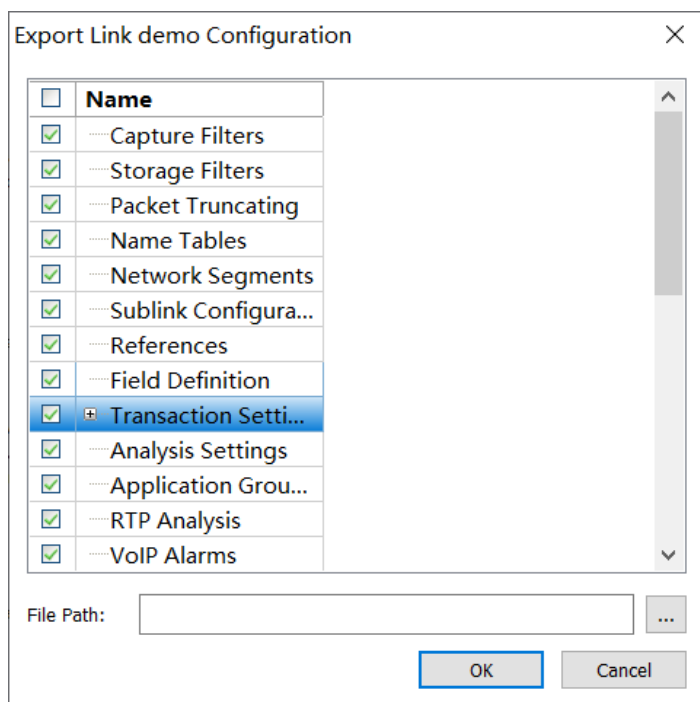
: Moves the selected view down.

Exporting Network Link Properties

All items of network link properties can be exported for further use in other network links.

To export the properties of a network link, follow the steps below:

Right-click the network link and click **Export Link Properties** to open the **Export Link Properties** dialog box:



On the **Export Link Properties** dialog box, select the items that you want to export.
Enter the file path and file name, and then click **OK**.

Importing Network Link Properties

To import the properties of a network link, follow the steps below:

1. On the Server Explorer, right-click the link and click **Import Link Properties**.

On the popup dialog box, select the file to be imported, and click **OK**.

Link Analysis

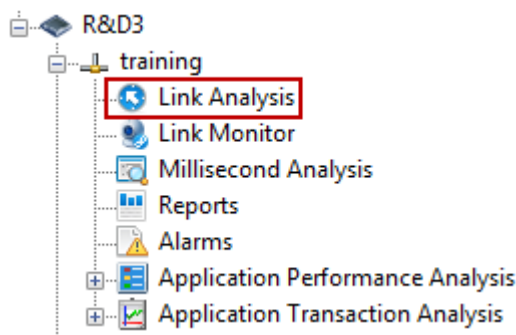
With retrospective analysis, the network status of past time can be displayed. This chapter describes how to retrospectively analyze a network link, the elements on the Link Analysis window, and how to use Expert Analyzer.

Retrospectively Analyzing a Network Link

To retrospectively analyze a network link:

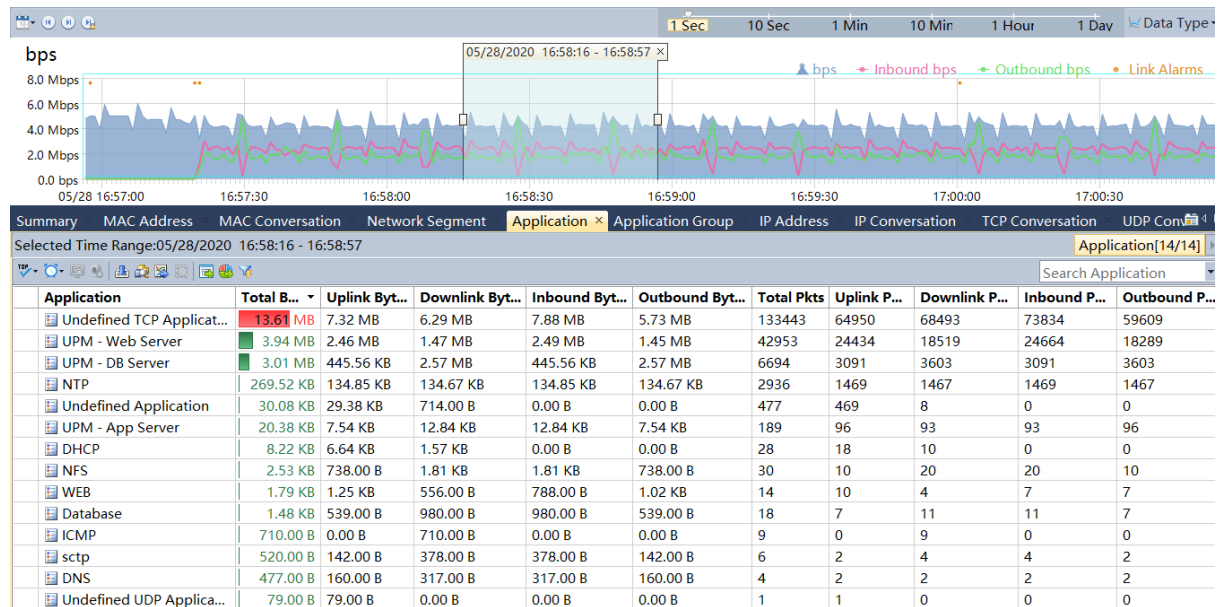
1. Connect a Server, and then network links created for the Server displays under the Server on the Server Explorer.

Double-click the node Link Analysis under the network link to open the Link Analysis window.



The Link Analysis window

The Link Analysis window is the main workbench of retrospective analysis, showing as below:



It generally includes a Time Window pane, and an analysis views pane.

To resize the Time Window pane and the analysis views pane, move the mouse pointer on the border between panes, and when the pointer becomes a double-headed arrow, drag the pointer to move the split line.

Time Window

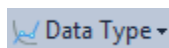
The following list describes the items on the Time Window.



: These icon buttons are for setting the time range of the Time Window.



: You can move this slide bar to select a time window type. You can also select a window type by right-clicking the Time Window, pointing to **Window Type** and clicking the appropriate window type.



: Click this icon to select a data type to display. You can also display a data type by right-clicking the Time Window, pointing to **Data Type** and clicking the appropriate data type.

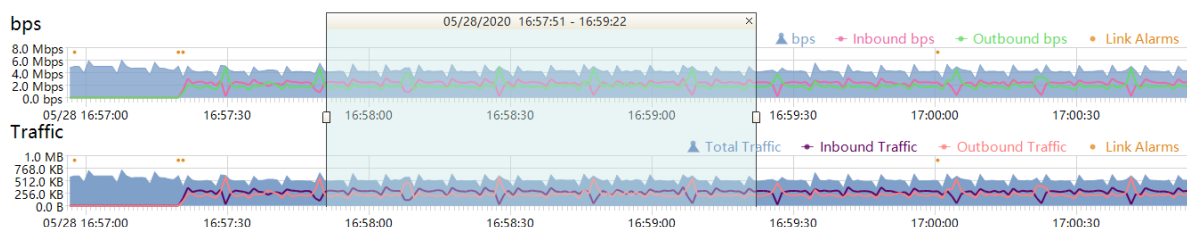
The Time Window provides charts with draggable time line. You can view the traffic, alarms, utilization, and packet loss of past time of the whole network, or even a specific network object. For more information about Time Window, see Time Window.

Analysis views


The analysis views provide various statistics and analysis data during the time range selected on the Time Window. You can export the statistics, drill down the network object, and analyze the traffic with Expert Analyzer. For more information about analysis views, see Link analysis views.

Time Window

With the Time Window, you can get graphical view of several types of network data, including traffic, alarms, packets, packet loss, TCP packets, utilization, etc. The Time Window appears as following figure:



Draggable Time Window


You can drag the Time Window to view network data of past time range. To drag the Time Window, move your mouse on the time scales of the charts, and drag when the mouse becomes .

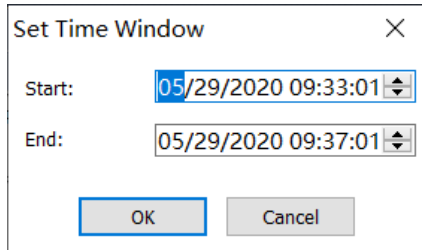
Setting the Time Window

You can choose to set the Time Window or to set the selected time range.

To set the Time Window, follow the steps below:




Click  and select **Set Time Window**. The **Set Time Window** dialog box appears.



Set the start time in the Start field and set the end time in the End field. Note that the start time must be later than the analysis start time.

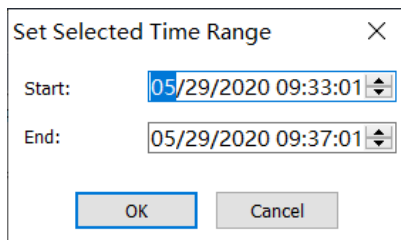
To set the start time and the end time, just click the time, and then enter the appropriate time or click the spin button.

Click **OK**.

 **Note** If the duration between Start and End is not one of 4 minutes, 20 minutes, 1 hour, 4 hours, 8 hours, 12 hours, 24 hours, 2 days, 10 days, and 40 days, the Time Window will automatically take the Start as the start time and extend the end time to match current Time Window with a proximate type of Time Window.

To set a time range to be selected, follow the steps below:

1. Click  and select **Set Selected Time Range**. The **Set Selected Time Range** dialog box appears.



Set the start time in the Start field and set the end time in the End field. Note that the start time must be later than the analysis start time.

To set the start time and the end time, just click the time, and then enter the appropriate time or click the spin button.

Click **OK**.

Once setting a selected time range, the time range will be automatically selected on the Time Window.

Locating the Time Window

Besides setting Time Window, you can use following buttons to locate the Time Window.



: Locates the start time of current Time Window to the moment when the network link is monitored.

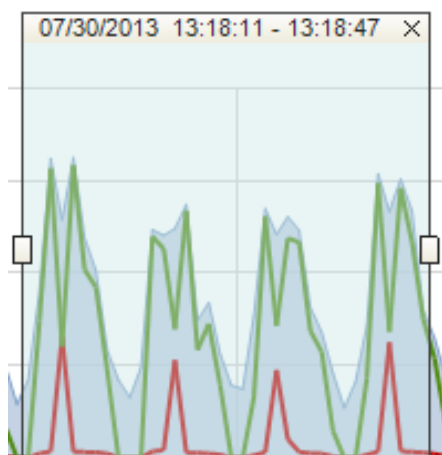


: Locates the end time of current Time Window to the latest moment that the network link is monitored.



Selecting a time range

The analysis views below the Time Window display the data of selected time range on the Time Window.

To select a time range, just drag your mouse on the Time Window, and then the range will be framed with two handles and a time bar, just like the following figure:

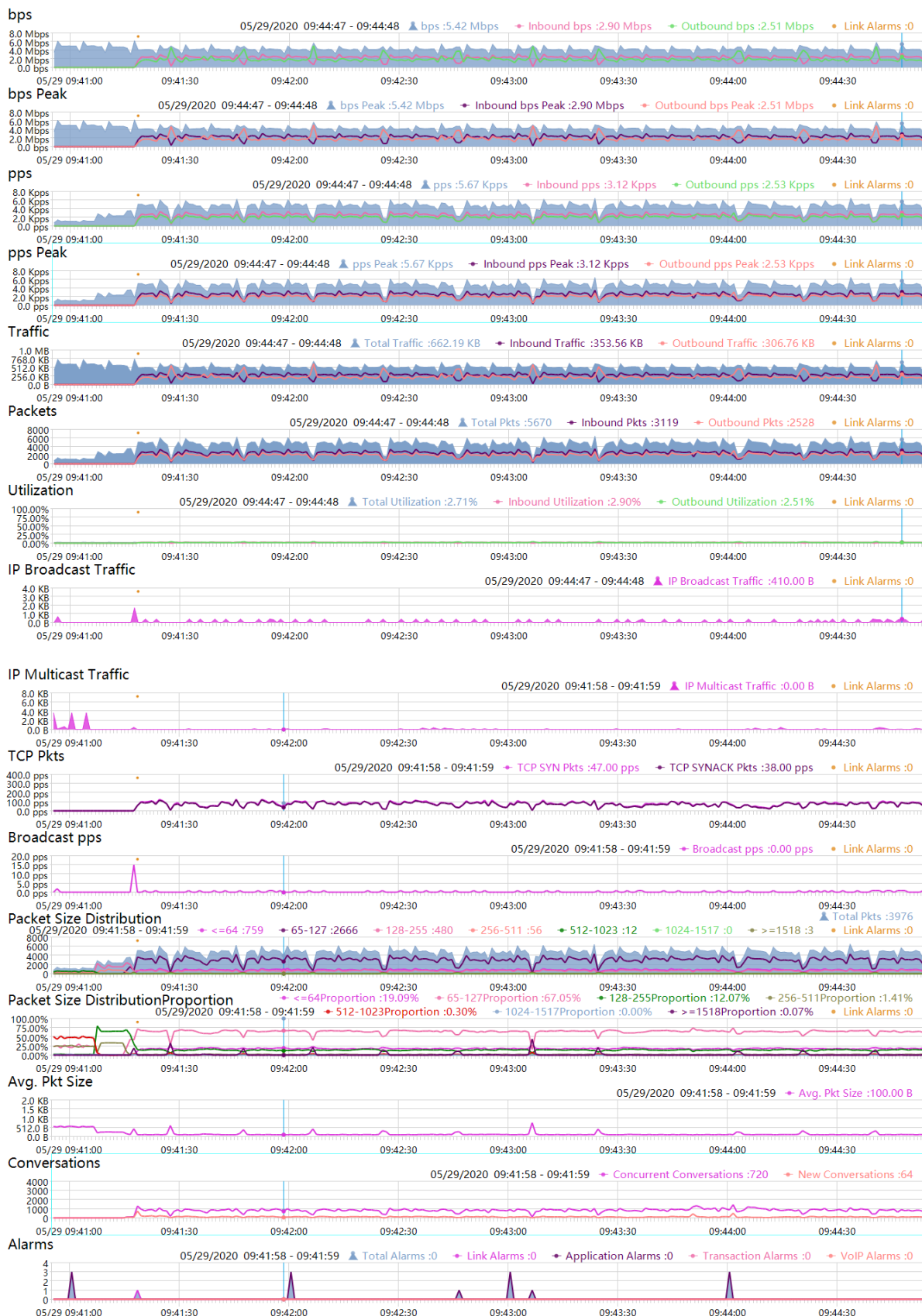


You can drag the handles to widen or narrow the time range.

The time bar shows the duration in the framed range, and you can move the framed range to select different time range with the same range value. To move the framed range, put your mouse on the time bar and drag it when the mouse becomes . To close the framed range, just click the close button .

Trend charts for link analysis

There are several types of trend charts in the Time Window, including bps, bps peak, valley, bps95p peak, pps, pps peak, traffic, packets, utilization, IP broadcast traffic, IP multicast traffic, TCP packet, broadcast pps, packet size distribution, packet size distribution proportion, avg. packets size, conversations and alarms, which are the same to those on the link monitoring window, as the following figure:



By default, it only displays the bps trend chart. To display other trend charts, just right-click the trend chart and select the appropriate one.

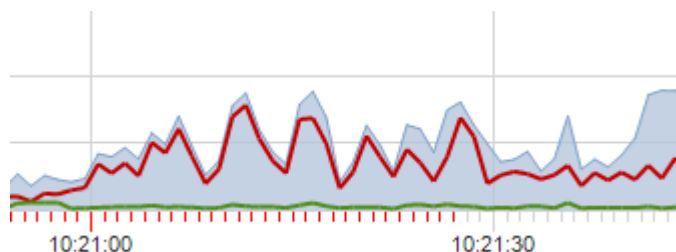


Tips

You should set up the network bandwidth with a reasonable value, if the utilization on the Utilization trend chart is greater than 100%.

The small yellow dots on the trend charts indicate that there are alarms triggered.

The red scales on the horizontal axis indicate that the packets captured in that time period have been cleared. As the following figure, the packets before 10:21:27 have been cleared:



Baseline analysis

When the time scale for trend charts is 1-minute and the trend chart is Traffic, Packets, Utilization, or Broadcast Packets, nChronos can calculate the baseline based on historical data.

To do baseline analysis, click the button  to choose the interested parameter.

Baseline can be generated for following parameters:

- Traffic: Total Traffic, Inbound Traffic, Outbound Traffic
- Utilization: Total Utilization, Inbound Utilization, Outbound Utilization
- Packets: Total Packets, Inbound Packets, Outbound Packets
- Broadcast Packets

Link Analysis views

There are several analysis views to display the statistics in different types. They work together with trend charts and time range selection on it to reduce statistic data volumes and let you focus on analyzing and drilldown to look into network issues. Note that the views, except the Summary view, will have records displayed only when you select a time range on the trend chart. And when you change the selection of the time range, the statistics on the views will refresh automatically.


Toolbar and pop-up menus

Buttons on the toolbar

There is a toolbar on the top of each analysis view and the same buttons on different toolbars have the same functions.

The following list describes all the buttons on the toolbar.



: Downloads packets of current time range. For more information about downloading packet, see *Download Packets dialog box* in this section.



: Launches the Expert Analyzer to analyze the packets of selected time range.



: Saves the current statistical list as a .csv file. For more information about exporting statistics, see *Export Statistics dialog box* in this section.



: Shows the top number of statistics on the view.



: Opens the new analysis window to make new analysis on the selected objects.



: Opens the network segment pane at the left of the view to view the statistics according to segment.



: Opens the Multi-Segment Analysis window to perform multi-segment analysis.



: Click to reconstruct the HTTP packets of selected objects as HTTP conversation.



: Click to quickly launch Expert Analyzer to decode packets of selected objects.



: Click to generate a temporary report based on the statistics on the current view.



: Click to generate a graph based on the statistics on the current view. Click the icon again to close the graph back to list data. After generating a graph, you can right-click to show it as pie chart or column chart, to change the top numbers and the sample fields.



: Click to generate an advanced filter view based on current view.

Pop-up menus

When you right-click the analysis views, there is a pop-up menu. The pop-up menus from different analysis views may include different command items. The following list describes all of the items.

Advanced Filter: Click to generate an advanced filter view based on current view.

Analyze in new window: Opens a new window to dedicatedly analyze the network object selected on the analysis view.

Drill Down: Drills down the specific elements based on the selected objects.

Exit Drilldown: Closes drilldown windows.

Reconstruct HTTP Packets: Reconstructs the HTTP packets of selected objects as HTTP conversation

Copy: Copies currently selected rows as well as the header row to the clipboard.

Copy Column: Copies the column of currently selected objects to the clipboard.

Show Column: Shows the columns on the view. Click **Default** to only show default columns. You can also show the columns by right-clicking the header of the columns.

Export Statistics: Saves the current statistical list as a .csv file.

Download Packets: Downloads packets of current time range.

Multi-Segment Analysis: Opens the Multi-Segment Analysis window to perform multi-segment analysis.

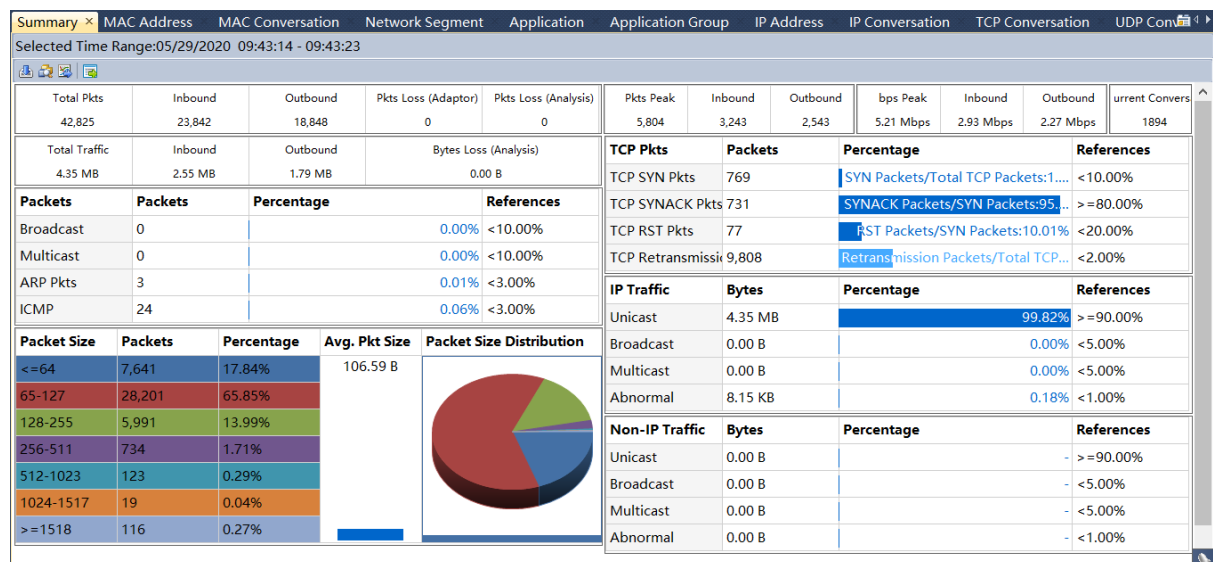
Analyze Packets: Launches the Expert Analyzer to analyze the packets of selected time range.

Decode Packets: Click to quickly launch Expert Analyzer to decode packets of selected objects.

Generate Report: Click to generate a temporary report based on the statistics on the current view.

The Summary view

The **Summary** view provides traffic statistics of currently selected time range and shows as the following figure:



There will be data on this view if no time range is selected on the Time Window.

The MAC Address view



The **MAC Address** view provides the statistics and analysis of the traffic according to MAC addresses, and shows as the following figure:

Summary MAC Address MAC Conversation Network Segment Application Application Group IP Address IP Conversation TCP Conversation UDP Conversation													
Selected Time Range:05/29/2020 09:43:14 - 09:43:23													
MAC Address[10/10]													
Search MAC Address													
Endpoint	Total B...	Tx Bytes	Rx Bytes	Bps	bps	Tx bps	Rx bps	Total Pkts	Tx Pkts	Rx Pkts	Tx pps	Rx pps	pps
08:19:7...	4.35 MB	2.55 MB	1.79 MB	494.39 KBps	4.05 Mbps	2.38 Mbps	1.67 Mbps	42695	23845	18850	2.65 Kpps	2.09 Kpps	4.74
34:40:f...	1.78 MB	721.07 ...	1.08 MB	202.98 KBps	1.66 Mbps	656.33 Kbps	1.01 Mbps	18210	7969	10241	885.44 pps	1.14 Kpps	2.02
5C:F3:f...	1.20 MB	455.38 ...	771.00 KB	136.26 KBps	1.12 Mbps	414.50 Kbps	701.78 Kbps	13075	5928	7147	658.67 pps	794.11 pps	1.45
20:37:c...	998.73 KB	365.38 ...	633.35 KB	110.97 KBps	909.06 Kbps	332.58 Kbps	576.49 Kbps	10112	4326	5786	480.67 pps	642.89 pps	1.12
5C:F3:f...	394.24 KB	291.15 ...	103.09 KB	43.80 KBps	358.84 Kbps	265.01 Kbps	93.83 Kbps	1256	606	650	67.33 pps	72.22 pps	139.5
FF:FF:F...	8.15 KB	0.00 B	8.15 KB	927.11 Bps	7.42 Kbps	0.00 bps	7.42 Kbps	130	0	130	0.00 pps	14.44 pps	14.44
10:1B:b...	7.94 KB	7.94 KB	0.00 B	903.11 Bps	7.22 Kbps	7.22 Kbps	0.00 bps	127	127	0	14.11 pps	0.00 pps	14.11
5C:F3:f...	3.38 KB	1.67 KB	1.71 KB	384.56 Bps	3.08 Kbps	1.52 Kbps	1.56 Kbps	42	21	21	2.33 pps	2.33 pps	4.67
34:40:f...	128.00 B	128.00 B	0.00 B	14.22 Bps	113.78 bps	113.78 bps	0.00 bps	2	2	0	0.22 pps	0.00 pps	0.22
28:6E:f...	88.00 B	88.00 B	0.00 B	9.78 Bps	78.22 bps	78.22 bps	0.00 bps	1	1	0	0.11 pps	0.00 pps	0.11

Viewing MAC address statistics

The **MAC Address** view displays the traffic of the network according to MAC addresses, as well as bytes, and packets. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of MAC addresses on the MAC Address view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a MAC address

You can drill down a MAC address for more detailed information. To drill a MAC address, right-click the IP address, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back.

To close a drilldown window, just deselect the drilled objects.

Analyzing MAC addresses in a new window



















On the MAC Address view, you can make analysis on one or more MAC addresses independently. To analyze MAC addresses in new window, just right-click a MAC address and click **Analyze in New Window**.

Searching the MAC Address view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the IP Address view will only display the items having the keyword.

The MAC Conversation view



The **MAC Conversation** view provides the statistics and analysis of the traffic according to MAC conversations, and shows as the following figure:

Summary	MAC Address	MAC Conversation	Network Segment	Application	Application Group	IP Address	IP Conversation	TCP Conversation	UDP Conversation			
Selected Time Range:05/29/2020 09:43:14 - 09:43:23												
Search MAC Conversation												
Endpoint 1	Endpoint 2	Total B...	Bps	Endpoint ...	Endpoint 2 Tx Byt...	bps	Endpoint ...	Endpoint 2 Tx b...	Total Pkts	pps	Endpoint...	Endpoi...
 34:40:B5:AA:3E:36	 08:19:A6:24:08:EF	 1.78 MB	2....	721.07 KB	1.08 MB	1....	656.33 Kbps	1.01 Mbps	18210	2....	7969	10241
 5C:F3:FC:DB:9A:4C	 08:19:A6:24:08:EF	 1.20 MB	1....	455.38 KB	771.00 KB	1....	414.50 Kbps	701.78 Kbps	13075	1....	5928	7147
 20:37:06:C5:E8:9E	 08:19:A6:24:08:EF	 998.73 KB	1....	365.38 KB	633.35 KB	1....	332.58 Kbps	576.49 Kbps	10112	1....	4326	5786
 5C:F3:FC:BA:B0:FE	 08:19:A6:24:08:EF	 394.24 KB	4....	291.15 KB	103.09 KB	3....	265.01 Kbps	93.83 Kbps	1256	1....	606	650
 FF:FF:FF:FF:FF:FF	 10:1B:54:5B:07:28	 7.94 KB	9....	0.00 B	7.94 KB	7....	0.00 bps	7.22 Kbps	127	1....	0	127
 5C:F3:FC:DB:C9:EC	 08:19:A6:24:08:EF	 3.32 KB	3....	1.61 KB	1.71 KB	3....	1.46 Kbps	1.56 Kbps	41	4....	20	21
FF:FF:FF:FF:FF:FF	28:6E:D4:19:43:FA	88.00 B	9....	0.00 B	88.00 B	7....	0.00 bps	78.22 bps	1	0....	0	1
FF:FF:FF:FF:FF:FF	5C:F3:FC:DB:C9:EC	64.00 B	7....	0.00 B	64.00 B	5....	0.00 bps	56.89 bps	1	0....	0	1
FF:FF:FF:FF:FF:FF	34:40:B5:AA:3D:96	64.00 B	7....	0.00 B	64.00 B	5....	0.00 bps	56.89 bps	1	0....	0	1
34:40:B5:AA:3D:96	08:19:A6:24:08:EF	64.00 B	7....	64.00 B	0.00 B	5....	56.89 bps	0.00 bps	1	0....	1	0

Viewing MAC conversation statistics

The MAC Conversation view displays the traffic of the network according to communication nodes, as well as node bytes, and packets. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of MAC conversations on the Physical Conversation view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Searching the MAC Conversation view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the MAC Conversation view will only display the items having the keyword.

The Network Segment view

The **Network Segment** view shows as the following figure:



Summary	MAC Address	MAC Conversation	Network Segment	Application	Application Group	IP Address	IP Conversation	TCP Conversation	UDP Conversation
Selected Time Range: 05/29/2020 09:43:14 - 09:43:23									
Network Segment [7/7]									
Search Network Segment									
Segment	Geolocation	Type	Total Bandwidth	Inbound Bandwidth	Outbound Bandwidth	Total Bytes	Tx Bytes	Rx Bytes	Bps
UPM - Chengdu	Chengdu	Subnet Mask	200	100	100	4.35 MB	1.43 MB	2.29 MB	494.39 KBps
UPM - segment 2	Segment 2	1	100	100	100	4.35 MB	1.79 MB	2.55 MB	494.39 KBps
Undefined Segment	-		200	100	100	1.14 MB	736.43 KB	426.92 KB	129.26 KBps
UPM - Shanghai Branch	Shanghai Branch	Subnet Mask	200	100	100	1015.78 KB	612.44 KB	403.34 KB	112.86 KBps
UPM - Beijing	Beijing	Subnet Mask	200	100	100	973.72 KB	685.99 KB	287.73 KB	108.19 KBps
UPM - HK Office	HK Office	Subnet Mask	200	100	100	654.02 KB	305.31 KB	348.71 KB	72.67 KBps
UPM - segment 1	Segment 1	1	100	100	100	330.00 B	0.00 B	330.00 B	36.67 Bps

The **Network Segment** view provides the statistics and analysis of the traffic according to network segments which are defined when configuring the network link.

Viewing segment statistics

The **Network Segment** view displays the traffic of the segment, as well as bytes, packets, internal bytes, and internal packets. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are too many statistical items on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a segment

You can drill down a segment for more detailed information. To drill a segment, right-click the segment, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:

Network Segment[1/1] ▶ Application[16/16] ▶ IP Conversation[10/10] ▶ TCP Conversation[3/3]

To close a drilldown window, just deselect the drilled objects.

Analyzing segments in a new window

On the **Network Segment** view, you can make analysis on one or more segments independently. To analyze segments in new window, just right-click a segment and click **Analyze in New Window**.

Searching the Network Segment view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Network Segment view will only display the items having the keyword.

The Application view

The **Application** view shows as the following figure:



Application	Total B...	Uplink Byt...	Downlink Byt...	Inbound Byt...	Outbound Byt...	Total Pkts	Uplink P...	Downlink P...	Inbound P...	Outbound P...
Undefined TCP Applicat...	2.90 MB	1.67 MB	1.23 MB	1.79 MB	1.11 MB	30433	15060	15373	16968	13465
UPM - Web Server	97.16 KB	629.87 KB	367.29 KB	632.48 KB	364.68 KB	10088	5753	4335	5773	4315
UPM - DB Server	388.31 KB	98.84 KB	289.47 KB	98.84 KB	289.47 KB	1210	625	585	625	585
NTP	81.52 KB	39.66 KB	41.86 KB	39.66 KB	41.86 KB	888	432	456	432	456
Undefined Application	8.21 KB	8.21 KB	0.00 B	0.00 B	0.00 B	131	131	0	0	0
UPM - App Server	7.13 KB	1.88 KB	5.25 KB	5.25 KB	1.88 KB	60	24	36	36	24
Database	502.00 B	154.00 B	348.00 B	348.00 B	154.00 B	6	2	4	4	2
NFS	379.00 B	77.00 B	302.00 B	302.00 B	77.00 B	5	1	4	4	1
ICMP	312.00 B	156.00 B	156.00 B	0.00 B	0.00 B	4	2	2	0	0

The **Application** view provides statistics of applications, including system applications and custom applications. The system applications are the applications imported when you configure the Server settings at the Server side, while the custom applications are the applications defined when you configure the network link properties at the Console side. The custom applications have priority over the system applications in display on the Application view when both of them include the same applications.

Viewing application statistics

The **Application** view displays the traffic of the network according to applications name, as well as bytes, packets, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of applications on the Application view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down an application

You can drill down an application for more detailed information. To drill an application, right-click the application, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:

Application[13/13] ▶ Network Segment[2/2] ▶ Internal IP[20/20] ▶ IP Conversation[50/50] ▶ UDP Conversation[1/1]

To close a drilldown window, just deselect the drilled objects.

Analyzing applications in new window








On the **Application** view, you can make analysis on one or more applications independently. To analyze applications in new window, just right-click an application and click **Analyze in New Window**.

Searching the Application view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Application view will only display the items having the keyword.

The Application Group view

The **Application Group** view shows as the following figure:



Summary	MAC Address	MAC Conversation	Network Segment	Network Segment Group	Application	Application Group			
Selected time range:09/27/2016 22:00:17 - 22:01:04									
Application Group[3/3]									
<div>TOP       </div> <div>Search Application Group</div>									
	Application Group	Total Bytes	Uplink Bytes	Downlink Bytes	Total Packets	Uplink Pkts	Downlink Pkts	Avg. Pkt Size	Bps
	Group152	184.97 MB	86.50 MB	98.47 MB	1393351	704938	688413	139.20 B	3.94
	Group5	62.44 MB	27.87 MB	34.57 MB	303090	81177	221913	216.01 B	1.33
	Group0	49.62 MB	10.87 MB	38.74 MB	216024	118453	97571	240.83 B	1.06

The **Application Group** view provides statistics of application groups, which are defined when configuring the network link.

Viewing application group statistics

The **Application Group** view displays the traffic of the network according to application group name, as well as bytes, packets, average packet size, etc. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

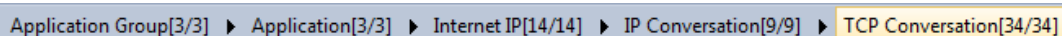
When there are a lot of application groups on the Application Group view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

The columns on the Application Group view are same to those on the Application view.

Drilling down an application group

You can drill down an application group for more detailed information. To drill an application group, right-click the application group, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Analyzing application groups in new window

On the **Application Group** view, you can make analysis on one or more application groups independently. To analyze application groups in new window, just right-click an application group and click **Analyze in New Window**.

Searching the Application Group view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Application Group view will only display the items having the keyword.

The IP Address view

The **IP Address** view provides the statistics and analysis of the traffic according to IP addresses, and shows as the following figure:


Summary	MAC Address	MAC Conversation	Network Segment	Application	Application Group	IP Address ×	IP Conversation	TCP Conversation	UDP Conversation			
Selected Time Range:05/29/2020 09:42:16 - 09:44:34												
Internal IP Addresses[10/10]												
Internal IP Addresses External IP Addresses All IP Addresses												
Search Internal IP Address												
Endpoint	Geolocation	TCP/U...	Total B...	Tx Bytes	Rx Bytes	Inbound Byt...	Outbound Byt...	Total Pkts	Tx Pkts	Rx Pkts	Inbound P...	Outbound P...
testserver2	Segment 2	UDP	27.33 MB	11.41 ...	15.92 MB	15.92 MB	11.41 MB	269878	1184...	151416	151416	118461
221.237.152.213	Segment 2	TCP	8.72 MB	7.03 MB	11.69 MB	11.69 MB	7.03 MB	199422	91187	108235	108235	91187
testserver	Segment 2	TCP	13.61 MB	5.36 MB	8.26 MB	8.26 MB	5.36 MB	145066	66302	78764	78764	66302
db server	Segment 2	TCP	10.09 MB	8.58 MB	1.52 MB	1.52 MB	8.58 MB	22905	12187	10718	10718	12187
221.237.152.212	Segment 2	TCP	70.80 KB	34.51 KB	36.29 KB	22.04 KB	20.48 KB	797	372	425	238	190
221.237.152.54	Segment 2	ICMP	28.03 KB	14.24 KB	13.79 KB	0.00 B	0.00 B	368	187	181	0	0
221.237.152.214	Segment 2	TCP	7.05 KB	3.64 KB	3.41 KB	3.41 KB	2.55 KB	71	40	31	31	26
221.237.152.255	Segment 2	UDP	741.00 B	0.00 B	741.00 B	0.00 B	0.00 B	3	0	3	0	0
224.0.0.22	-	IGMP	640.00 B	0.00 B	640.00 B	0.00 B	0.00 B	10	0	10	0	0
224.0.0.252	-	UDP	237.00 B	0.00 B	237.00 B	0.00 B	0.00 B	3	0	3	0	0


Viewing IP address statistics

By default, this view displays the statistics of internal IP. You can click **External IP** to view the statistics of external network.

The **IP Address** view displays the traffic of the network according to IP addresses, as well as bytes, packets, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of IP addresses on the IP Address view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

In addition, you can click  to open the network segment pane at the left of the view to view the statistics according to segment. The network segment pane will automatically list all available class C segments, and you can click the segment to view only the statistics of that segment.

Drilling down an IP address

You can drill down an IP conversation for more detailed information. To drill an IP conversation, right-click the IP conversation, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:

Internal IP[57/57] ▶ Application[4/4] ▶ IP Conversation[119/119] ▶ UDP Conversation[4/4]

To close a drilldown window, just deselect the drilled objects.

Analyzing IP addresses in new window

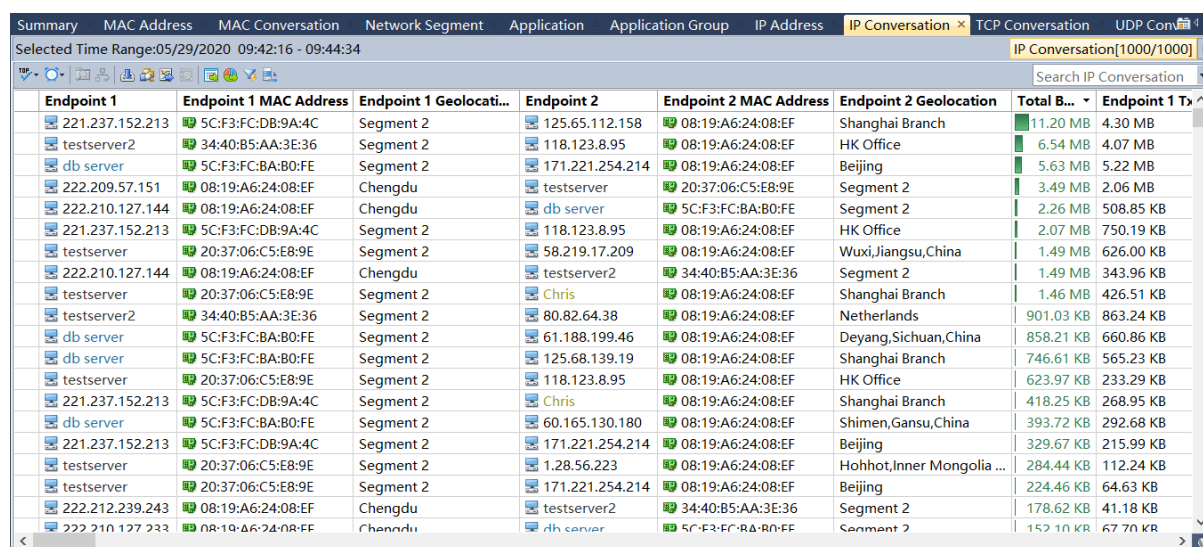
In the **IP Conversation** view, you can make analysis on one or more IP conversations independently. To analyze IP conversations in new window, just right-click an IP conversation and click **Analyze in New Window**.

Searching the IP Address view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the IP Address view will only display the items having the keyword.

The IP Conversation view

The **IP Conversation** view provides the statistics and analysis of the traffic according to IP conversations, and shows as the following figure:




Endpoint 1	Endpoint 1 MAC Address	Endpoint 1 Geoloca...	Endpoint 2	Endpoint 2 MAC Address	Endpoint 2 Geolocation	Total B...	Endpoint 1 Tx
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	11.20 MB	4.30 MB
testserver2	34:40:B5:AA:3E:36	Segment 2	118.123.8.95	08:19:A6:24:08:EF	HK Office	6.54 MB	4.07 MB
db server	5C:F3:FC:BA:B0:FE	Segment 2	171.221.254.214	08:19:A6:24:08:EF	Beijing	5.63 MB	5.22 MB
222.209.57.151	08:19:A6:24:08:EF	Chengdu	testserver	20:37:06:C5:E8:9E	Segment 2	3.49 MB	2.06 MB
222.210.127.144	08:19:A6:24:08:EF	Chengdu	db server	5C:F3:FC:BA:B0:FE	Segment 2	2.26 MB	508.85 KB
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	118.123.8.95	08:19:A6:24:08:EF	HK Office	2.07 MB	750.19 KB
testserver	20:37:06:C5:E8:9E	Segment 2	58.219.17.209	08:19:A6:24:08:EF	Wuxi, Jiangsu, China	1.49 MB	626.00 KB
222.210.127.144	08:19:A6:24:08:EF	Chengdu	testserver2	34:40:B5:AA:3E:36	Segment 2	1.49 MB	343.96 KB
testserver	20:37:06:C5:E8:9E	Segment 2	Chris	08:19:A6:24:08:EF	Shanghai Branch	1.46 MB	426.51 KB
testserver2	34:40:B5:AA:3E:36	Segment 2	80.82.64.38	08:19:A6:24:08:EF	Netherlands	901.03 KB	863.24 KB
db server	5C:F3:FC:BA:B0:FE	Segment 2	61.188.199.46	08:19:A6:24:08:EF	Deyang, Sichuan, China	858.21 KB	660.86 KB
db server	5C:F3:FC:BA:B0:FE	Segment 2	125.68.139.19	08:19:A6:24:08:EF	Shanghai Branch	746.61 KB	565.23 KB
testserver	20:37:06:C5:E8:9E	Segment 2	118.123.8.95	08:19:A6:24:08:EF	HK Office	623.97 KB	233.29 KB
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	Chris	08:19:A6:24:08:EF	Shanghai Branch	418.25 KB	268.95 KB
db server	5C:F3:FC:BA:B0:FE	Segment 2	60.165.130.180	08:19:A6:24:08:EF	Shimen, Gansu, China	393.72 KB	292.68 KB
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	171.221.254.214	08:19:A6:24:08:EF	Beijing	329.67 KB	215.99 KB
testserver	20:37:06:C5:E8:9E	Segment 2	1.28.56.223	08:19:A6:24:08:EF	Hohhot, Inner Mongolia ...	284.44 KB	112.24 KB
testserver	20:37:06:C5:E8:9E	Segment 2	171.221.254.214	08:19:A6:24:08:EF	Beijing	224.46 KB	64.63 KB
222.212.239.243	08:19:A6:24:08:EF	Chengdu	testserver2	34:40:B5:AA:3E:36	Segment 2	178.62 KB	41.18 KB
222.210.127.233	08:19:A6:24:08:EF	Chengdu	db server	5C:F3:FC:BA:B0:FE	Segment 2	152.10 KB	67.70 KB

Viewing IP conversation statistics

The **IP Conversation** view displays the traffic of the network according to communication nodes, as well as node geographic location, bytes, and packets. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of IP conversations on the IP Conversation view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Drilling down an IP conversation

You can drill down an IP conversation for more detailed information. To drill an IP conversation, right-click the IP conversation, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:

IP Conversation[299/299] ▶ TCP Conversation[3/3]

To close a drilldown window, just deselect the drilled objects

Analyzing IP conversations in new window

In the **IP Conversation** view, you can make analysis on one or more IP conversations independently. To analyze IP conversations in new window, just right-click an IP conversation and click **Analyze in New Window**.

Searching the Application view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the IP Conversation view will only display the items having the keyword.

The TCP Conversation view


The **TCP Conversation** view provides the statistics and analysis of the traffic according to TCP conversations, and shows as the following figure:

Summary	MAC Address	MAC Conversation	Network Segment	Application	Application Group	IP Address	IP Conversation	TCP Conversation	UDP Conversation
Selected Time Range: 05/29/2020 09:42:16 - 09:44:34									
TCP Conversation[1000/1000]									
Search TCP Conversation									
Client	Client MAC Address	Client Geolocation	Client Port	Server	Server MAC Address	Server Geolocation	Server Port	Protocol	App
171.221.254.214	08:19:A6:24:08:EF	Beijing	50560	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	
testserver2	34:40:B5:AA:3E:36	Segment 2	63392	118.123.8.95	08:19:A6:24:08:EF	HK Office	13000	TCP	
125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	61960	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13000	TCP	
125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	61961	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13002	TCP	
testserver2	34:40:B5:AA:3E:36	Segment 2	63391	118.123.8.95	08:19:A6:24:08:EF	HK Office	13000	TCP	
125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	61959	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13002	TCP	
125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	61958	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13000	TCP	
222.210.127.144	08:19:A6:24:08:EF	Chengdu	37669	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	
61.188.199.46	08:19:A6:24:08:EF	Deyang, Sichuan, China	35447	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	
125.68.139.19	08:19:A6:24:08:EF	Shanghai Branch	13616	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	
Chris	08:19:A6:24:08:EF	Shanghai Branch	10926	testserver	20:37:06:C5:E8:9E	Segment 2	3306	MYSQL	
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13000	118.123.8.95	08:19:A6:24:08:EF	HK Office	2667	TCP	
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13002	118.123.8.95	08:19:A6:24:08:EF	HK Office	2666	TCP	
Chris	08:19:A6:24:08:EF	Shanghai Branch	51879	testserver	20:37:06:C5:E8:9E	Segment 2	8030	TCP	
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13000	118.123.8.95	08:19:A6:24:08:EF	HK Office	2668	TCP	
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13002	118.123.8.95	08:19:A6:24:08:EF	HK Office	2669	TCP	
60.165.130.180	08:19:A6:24:08:EF	Shimen, Gansu, China	2360	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	
Chris	08:19:A6:24:08:EF	Shanghai Branch	51876	testserver	20:37:06:C5:E8:9E	Segment 2	8030	TCP	
171.221.254.214	08:19:A6:24:08:EF	Beijing	50907	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	
171.221.254.214	08:19:A6:24:08:EF	Beijing	50465	db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	TCP	

Viewing TCP conversation statistics

The **TCP Conversation** view displays the traffic of the network according to communication nodes, as well as node geographic location, port number, application, round-trip time, bytes, packets, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of TCP conversations on the TCP Conversation view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Analyzing TCP Conversation in new window

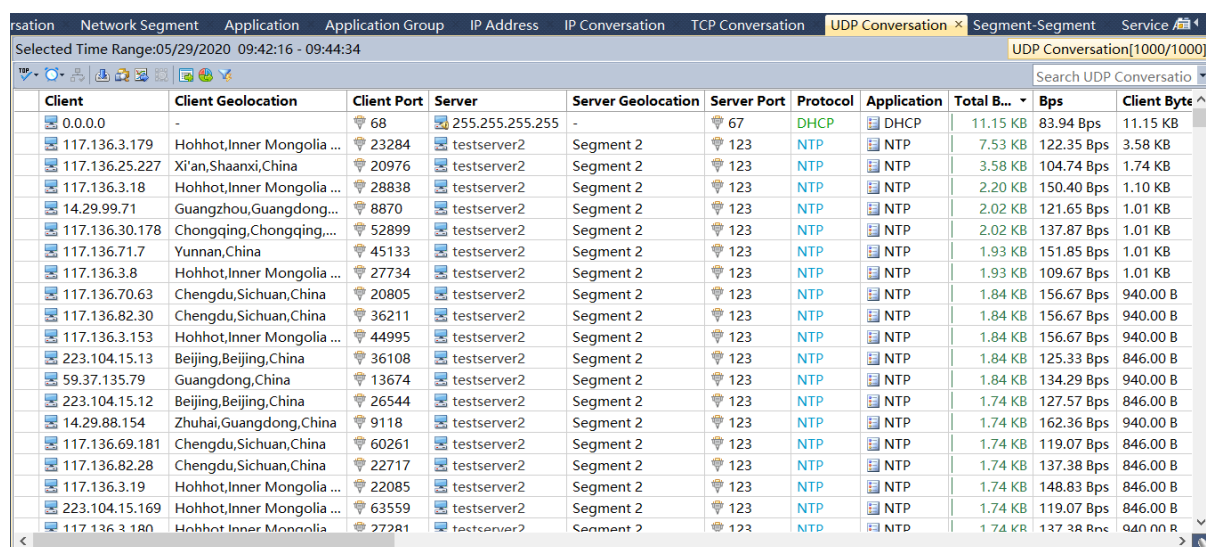
In the **TCP Conversation** view, you can make analysis on one or more TCP conversations independently. To analyze TCP conversations in new window, just right-click a TCP conversation and click **Analyze in New Window**.

Searching the TCP Conversation view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the TCP Conversation view will only display the items having the keyword.

The UDP Conversation view

The **UDP Conversation** view provides the statistics and analysis of the traffic according to UDP conversations, and shows as the following figure:




Client	Client Geolocation	Client Port	Server	Server Geolocation	Server Port	Protocol	Application	Total Bps	Bps	Client Bytes
0.0.0.0	-	68	255.255.255.255	-	67	DHCP	DHCP	11.15 KB	83.94 Bps	11.15 KB
117.136.3.179	Hohhot, Inner Mongolia ...	23284	testserver2	Segment 2	123	NTP	NTP	7.53 KB	122.35 Bps	3.58 KB
117.136.25.227	Xi'an, Shaanxi, China	20976	testserver2	Segment 2	123	NTP	NTP	3.58 KB	104.74 Bps	1.74 KB
117.136.3.18	Hohhot, Inner Mongolia ...	28838	testserver2	Segment 2	123	NTP	NTP	2.20 KB	150.40 Bps	1.10 KB
14.29.99.71	Guangzhou, Guangdong...	8870	testserver2	Segment 2	123	NTP	NTP	2.02 KB	121.65 Bps	1.01 KB
117.136.30.178	Chongqing, Chongqing...	52899	testserver2	Segment 2	123	NTP	NTP	2.02 KB	137.87 Bps	1.01 KB
117.136.71.7	Yunnan, China	45133	testserver2	Segment 2	123	NTP	NTP	1.93 KB	151.85 Bps	1.01 KB
117.136.3.8	Hohhot, Inner Mongolia ...	27734	testserver2	Segment 2	123	NTP	NTP	1.93 KB	109.67 Bps	1.01 KB
117.136.70.63	Chengdu, Sichuan, China	20805	testserver2	Segment 2	123	NTP	NTP	1.84 KB	156.67 Bps	940.00 B
117.136.82.30	Chengdu, Sichuan, China	36211	testserver2	Segment 2	123	NTP	NTP	1.84 KB	156.67 Bps	940.00 B
117.136.3.153	Hohhot, Inner Mongolia ...	44995	testserver2	Segment 2	123	NTP	NTP	1.84 KB	156.67 Bps	940.00 B
223.104.15.13	Beijing, Beijing, China	36108	testserver2	Segment 2	123	NTP	NTP	1.84 KB	125.33 Bps	846.00 B
59.37.135.79	Guangdong, China	13674	testserver2	Segment 2	123	NTP	NTP	1.84 KB	134.29 Bps	940.00 B
223.104.15.12	Beijing, Beijing, China	26544	testserver2	Segment 2	123	NTP	NTP	1.74 KB	127.57 Bps	846.00 B
14.29.88.154	Zhuhai, Guangdong, China	9118	testserver2	Segment 2	123	NTP	NTP	1.74 KB	162.36 Bps	940.00 B
117.136.69.181	Chengdu, Sichuan, China	60261	testserver2	Segment 2	123	NTP	NTP	1.74 KB	119.07 Bps	846.00 B
117.136.82.28	Chengdu, Sichuan, China	22717	testserver2	Segment 2	123	NTP	NTP	1.74 KB	137.38 Bps	846.00 B
117.136.3.19	Hohhot, Inner Mongolia ...	22085	testserver2	Segment 2	123	NTP	NTP	1.74 KB	148.83 Bps	846.00 B
223.104.15.169	Hohhot, Inner Mongolia ...	63559	testserver2	Segment 2	123	NTP	NTP	1.74 KB	119.07 Bps	846.00 B
117.136.3.180	Hohhot, Inner Mongolia ...	27281	testserver2	Segment 2	123	NTP	NTP	1.74 KB	137.38 Bps	846.00 B

Viewing UDP conversation statistics

The **UDP Conversation** view displays the traffic of the network according to communication nodes, as well as node geographic location, port number, application, bytes, packets, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of **UDP conversations** on the UDP Conversation view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Searching the UDP Conversation view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the UDP Conversation view will only display the items having the keyword.

The Segment-Segment view

The **Segment-Segment** view shows as the following figure:

IP Address

IP Conversation

TCP Conversation

UDP Conversation

Segment-Segment

Service Access

Port

Link Alarms

VLAN

MPLS VPN

Selected time range:09/27/2016 16:55:35 - 16:56:07

TCP

Search Segment-Segment

Endpoint 1	Endpoint 2	Protocol	Application	Total Bytes	Bps	Bytes Sent by Endpoint...	Bytes Sent by Endpoint...	bps
Segment9	Unknown Segment	TCP	hao123	565.96 MB	17.69 MBps	57.32 MB	508.65 MB	148.36 M
Segment0	Unknown Segment	UDP	DNS	349.00 MB	10.91 MBps	13.72 MB	335.28 MB	91.49 Mb
Segment9	Segment0	ICMP	ICMP	12.06 MB	385.83 KBps	3.29 MB	8.77 MB	3.16 Mbp
Segment5	Segment9	TCP	WEB	7.34 MB	235.03 KBps	6.58 MB	785.47 KB	1.93 Mbp
Segment9	Segment6	TCP	Unknown TCP Application	5.21 MB	166.59 KBps	322.57 KB	4.89 MB	1.36 Mbp
Segment5	Unknown Segment	UDP	DNS	1.01 MB	32.18 KBps	223.19 KB	806.64 KB	263.64 Kb
Segment5	Segment0	TCP	Unknown TCP Application	11.92 KB	381.53 Bps	4.60 KB	7.32 KB	3.05 Kbp



111

The **Segment-Segment** view provides the statistics and analysis of the traffic according to network segments which are defined when configuring the network link.

Viewing statistics

The **Segment-Segment** view displays the traffic between segments, as well as bytes, packets, internal bytes, etc. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are too many statistical items on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a segment

You can drill down a segment for more detailed information. To drill a segment, right-click the segment, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back.

To close a drilldown window, just deselect the drilled objects.

Analyzing Segment-Segment in new window

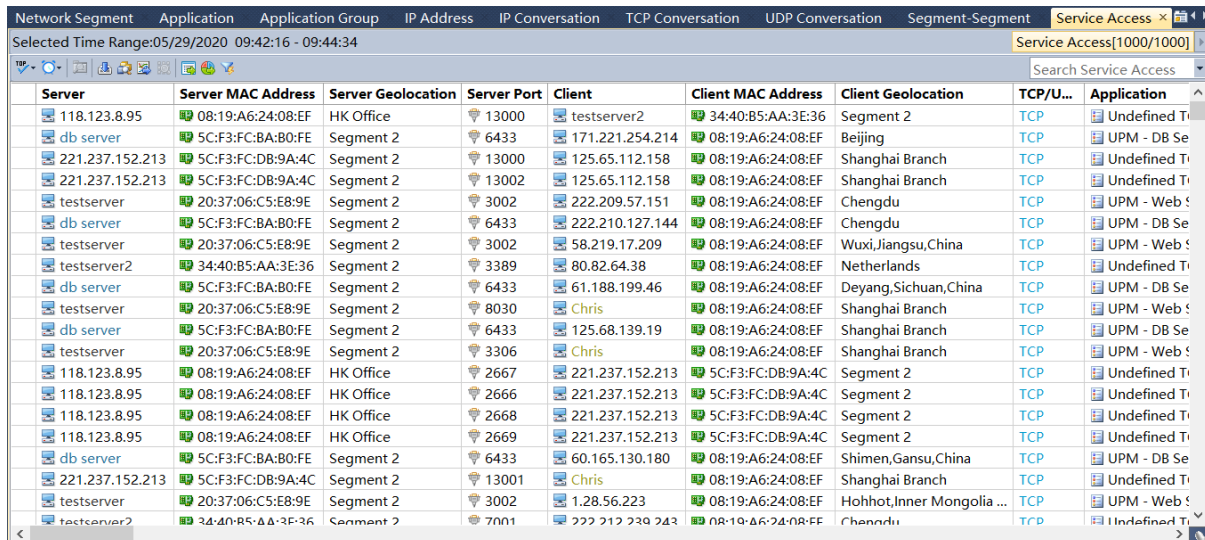
On the **Segment-Segment** view, you can make analysis on one or more items independently. To analyze segment-segment items in new window, just right-click a segment-segment item and click **Analyze in New Window**.

Searching the Segment-Segment view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Segment-Segment view will only display the items having the keyword.

The Service Access view

The **Service Access** view shows as the following figure:




Server	Server MAC Address	Server Geolocation	Server Port	Client	Client MAC Address	Client Geolocation	TCP/U...	Application
118.123.8.95	08:19:A6:24:08:EF	HK Office	13000	testserver2	34:40:B5:AA:3E:36	Segment 2	TCP	Undefined T...
db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	171.221.254.214	08:19:A6:24:08:EF	Beijing	TCP	UPM - DB Se
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13000	125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	TCP	Undefined T...
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13002	125.65.112.158	08:19:A6:24:08:EF	Shanghai Branch	TCP	Undefined T...
testserver	20:37:06:C5:E8:9E	Segment 2	3002	222.209.57.151	08:19:A6:24:08:EF	Chengdu	TCP	UPM - Web S
db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	222.210.127.144	08:19:A6:24:08:EF	Chengdu	TCP	UPM - DB Se
testserver	20:37:06:C5:E8:9E	Segment 2	3002	58.219.17.209	08:19:A6:24:08:EF	Wuxi,Jiangsu,China	TCP	UPM - Web S
testserver2	34:40:B5:AA:3E:36	Segment 2	3389	80.82.64.38	08:19:A6:24:08:EF	Netherlands	TCP	Undefined T...
db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	61.188.199.46	08:19:A6:24:08:EF	Deyang,Sichuan,China	TCP	UPM - DB Se
testserver	20:37:06:C5:E8:9E	Segment 2	8030	Chris	08:19:A6:24:08:EF	Shanghai Branch	TCP	UPM - Web S
db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	125.68.139.19	08:19:A6:24:08:EF	Shanghai Branch	TCP	UPM - DB Se
testserver	20:37:06:C5:E8:9E	Segment 2	3306	Chris	08:19:A6:24:08:EF	Shanghai Branch	TCP	UPM - Web S
118.123.8.95	08:19:A6:24:08:EF	HK Office	2667	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	TCP	Undefined T...
118.123.8.95	08:19:A6:24:08:EF	HK Office	2666	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	TCP	Undefined T...
118.123.8.95	08:19:A6:24:08:EF	HK Office	2668	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	TCP	Undefined T...
118.123.8.95	08:19:A6:24:08:EF	HK Office	2669	221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	TCP	Undefined T...
db server	5C:F3:FC:BA:B0:FE	Segment 2	6433	60.165.130.180	08:19:A6:24:08:EF	Shimen,Gansu,China	TCP	UPM - DB Se
221.237.152.213	5C:F3:FC:DB:9A:4C	Segment 2	13001	Chris	08:19:A6:24:08:EF	Shanghai Branch	TCP	Undefined T...
testserver	20:37:06:C5:E8:9E	Segment 2	3002	1.28.56.223	08:19:A6:24:08:EF	Hohhot,Inner Mongolia ...	TCP	UPM - Web S
testserver2	34:40:B5:AA:3E:36	Segment 2	7001	222.212.239.243	08:19:A6:24:08:EF	Chengdu	TCP	Undefined T...

Viewing service access statistics

The **Service Access** view displays application access statistics of the monitored network link. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

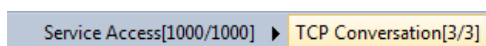
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of items on the Service Access view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a service access item

You can drill down a service access item for more detailed information. To drill a service access item, right-click the item, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Analyzing service accesses in new window

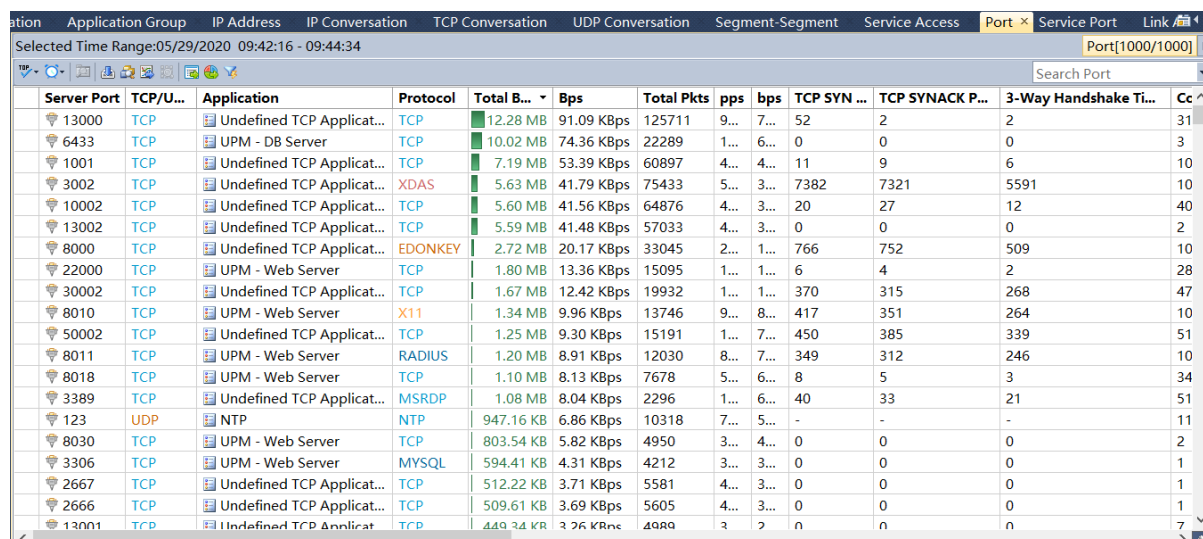
On the **Service Access** view, you can make analysis on one or more items independently. To analyze service access items in new window, just right-click a service access item and click **Analyze in New Window**.

Searching the Service Access view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Service Access view will only display the items having the keyword.

The Port view

The **Port** View statistics and displays the port information in the selected time period. The Port view shows as the following figure:





Server Port	TCP/U...	Application	Protocol	Total B...	Bps	Total Pkts	pps	bps	TCP SYN ...	TCP SYNACK P...	3-Way Handshake Ti...	Cc
13000	TCP	Undefined TCP Applicat...	TCP	12.28 MB	91.09 KBps	125711	9...	7...	52	2	2	31
6433	TCP	UPM - DB Server	TCP	10.02 MB	74.36 KBps	22289	1...	6...	0	0	0	3
1001	TCP	Undefined TCP Applicat...	TCP	7.19 MB	53.39 KBps	60897	4...	4...	11	9	6	10
3002	TCP	Undefined TCP Applicat...	XDAS	5.63 MB	41.79 KBps	75433	5...	3...	7382	7321	5591	10
10002	TCP	Undefined TCP Applicat...	TCP	5.60 MB	41.56 KBps	64876	4...	3...	20	27	12	40
13002	TCP	Undefined TCP Applicat...	TCP	5.59 MB	41.48 KBps	57033	4...	3...	0	0	0	2
8000	TCP	Undefined TCP Applicat...	EDONKEY	2.72 MB	20.17 KBps	33045	2...	1...	766	752	509	10
22000	TCP	UPM - Web Server	TCP	1.80 MB	13.36 KBps	15095	1...	1...	6	4	2	28
30002	TCP	Undefined TCP Applicat...	TCP	1.67 MB	12.42 KBps	19932	1...	1...	370	315	268	47
8010	TCP	UPM - Web Server	X11	1.34 MB	9.96 KBps	13746	9...	8...	417	351	264	10
50002	TCP	Undefined TCP Applicat...	TCP	1.25 MB	9.30 KBps	15191	1...	7...	450	385	339	51
8011	TCP	UPM - Web Server	RADIUS	1.20 MB	8.91 KBps	12030	8...	7...	349	312	246	10
8018	TCP	UPM - Web Server	TCP	1.10 MB	8.13 KBps	7678	5...	6...	8	5	3	34
3389	TCP	Undefined TCP Applicat...	MSRDP	1.08 MB	8.04 KBps	2296	1...	6...	40	33	21	51
123	UDP	NTP	NTP	947.16 KB	6.86 KBps	10318	7...	5...	-	-	-	11
8030	TCP	UPM - Web Server	TCP	803.54 KB	5.82 KBps	4950	3...	4...	0	0	0	2
3306	TCP	UPM - Web Server	MYSQL	594.41 KB	4.31 KBps	4212	3...	3...	0	0	0	1
2667	TCP	Undefined TCP Applicat...	TCP	512.22 KB	3.71 KBps	5581	4...	3...	0	0	0	1
2666	TCP	Undefined TCP Applicat...	TCP	509.61 KB	3.69 KBps	5605	4...	3...	0	0	0	1
13001	TCP	Undefined TCP Applicat...	TCP	449.34 KB	3.26 KBps	4989	3	2	0	0	0	7

Viewing port statistics

The **Port** view statistics and displays the port information in the selected time period. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

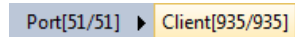
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of items on the Service Port view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a port item

You can drill down a port item for more detailed information. To drill a port item, right-click the item, then click Drill Down and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click Drill Down to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Analyzing ports in new window

On the **Port** view, you can make analysis on one or more items independently. To analyze port items in new window, just right-click a port item and click Analyze in New Window.

Searching the Port view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box

on the top-right corner, and then the Port view will only display the items having the keyword.

The Service Port view



The **Service** Port view includes two tabs: TCP Service Port and UDP Service Port, showing as the following figure:

Application Group	IP Address	IP Conversation	TCP Conversation	UDP Conversation	Segment-Segment	Service Access	Port	Service Port	Link
Selected Time Range: 05/29/2020 09:42:16 - 09:44:34									
TCP Service Port [1000/1000]									
Server	Server Geolocation	Server Port	Application	Protocol	Total Bytes	Bps	Total Pkts	pps	bps
db server	Segment 2	6433	UPM - DB Server	TCP	10.02 MB	74.36 KBps	22289	161.51 pps	609.14 Kbps
118.123.8.95	HK Office	13000	Undefined TCP Applicat...	TCP	6.54 MB	48.53 KBps	66778	483.90 pps	397.56 Kbps
testserver	Segment 2	3002	UPM - Web Server	XDAS	5.40 MB	40.04 KBps	72638	526.36 pps	328.04 Kbps
221.237.152.213	Segment 2	13000	Undefined TCP Applicat...	TCP	5.73 MB	42.53 KBps	58884	426.70 pps	348.44 Kbps
221.237.152.213	Segment 2	13002	Undefined TCP Applicat...	TCP	5.59 MB	41.48 KBps	57033	413.28 pps	339.82 Kbps
testserver2	Segment 2	1001	Undefined TCP Applicat...	TCP	7.19 MB	53.39 KBps	60897	441.28 pps	437.35 Kbps
221.237.152.213	Segment 2	8000	Undefined TCP Applicat...	EDONKEY	2.71 MB	20.13 KBps	32978	238.97 pps	164.90 Kbps
testserver2	Segment 2	3389	Undefined TCP Applicat...	SSL	912.65 KB	6.61 KBps	1214	8.80 pps	54.18 Kbps
testserver	Segment 2	8011	UPM - Web Server	KISMET	1.20 MB	8.91 KBps	12030	87.17 pps	73.00 Kbps
testserver	Segment 2	8010	UPM - Web Server	X11	1.16 MB	8.58 KBps	11687	84.69 pps	70.28 Kbps
testserver2	Segment 2	30002	Undefined TCP Applicat...	TCP	1.67 MB	12.42 KBps	19932	144.43 pps	101.77 Kbps
testserver	Segment 2	22000	UPM - Web Server	TCP	1.80 MB	13.36 KBps	15095	109.38 pps	109.42 Kbps
testserver2	Segment 2	50002	Undefined TCP Applicat...	TCP	1.25 MB	9.30 KBps	15191	110.08 pps	76.18 Kbps
118.123.8.95	HK Office	2667	Undefined TCP Applicat...	TCP	512.22 KB	3.71 KBps	5581	40.44 pps	30.41 Kbps
118.123.8.95	HK Office	2666	Undefined TCP Applicat...	TCP	509.61 KB	3.69 KBps	5605	40.62 pps	30.25 Kbps
testserver2	Segment 2	7001	Undefined TCP Applicat...	IRC	381.77 KB	2.77 KBps	3027	21.93 pps	22.66 Kbps
118.123.8.95	HK Office	2669	Undefined TCP Applicat...	TCP	429.50 KB	3.11 KBps	4571	33.12 pps	25.50 Kbps
118.123.8.95	HK Office	2668	Undefined TCP Applicat...	TCP	430.63 KB	3.12 KBps	4597	33.31 pps	25.56 Kbps
testserver	Segment 2	8018	UPM - Web Server	TCP	1.10 MB	8.13 KBps	7678	55.64 pps	66.61 Kbps
221.237.152.213	Segment 2	13001	Undefined TCP Applicat...	TCP	342.05 KB	2.48 KBps	3703	26.83 pps	20.30 Kbps

Viewing service port statistics

The **Service** Port view displays port access statistics based on IP address + port number. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

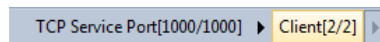
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of items on the Service Port view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a service port

You can drill down a service port for more detailed information. To drill a service port, right-click the port, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Analyzing service ports in new window

On the **Service Port** view, you can make analysis on one or more items independently. To analyze service port items in new window, just right-click a service port item and click **Analyze in New Window**.

Searching the Service Port view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Service Port view will only display the items having the keyword.

The Link Alarm view

The **Link Alarm** view provides the logs of all triggered link alarms, and shows as the following figure:

Selected Time Range: 05/29/2020 09:29:00 - 09:51:00										
All Alarms[11/11]										
Name	Statistics Time	Start Time	Durati...	Severity	Type	Category	Trigger Condition	IP Address	MAC Address	
upm-slo...	05/29/2020 09:30:00	05/29/2020 09:20:00	-	High	Network Application ...	333	Avg. Response Time : 2...	-	-	
upm-slo...	05/29/2020 09:30:00	05/29/2020 09:20:00	-	High	Network Application ...	333	Avg. Response Time : 6...	-	-	
upm-slo...	05/29/2020 09:30:00	05/29/2020 09:20:00	-	High	Network Application ...	333	Avg. Response Time : 1...	-	-	
upm-IC...	05/29/2020 09:32:50	05/29/2020 09:32:49	-	Severe	IP Conversation Alarm	333	pps : 205.00 pps > 60.0...	-	-	
upm-slo...	05/29/2020 09:40:00	05/29/2020 09:30:00	-	High	Network Application ...	333	Avg. Response Time : 2...	-	-	
upm-slo...	05/29/2020 09:40:00	05/29/2020 09:30:00	-	High	Network Application ...	333	Avg. Response Time : 1...	-	-	
upm-slo...	05/29/2020 09:40:00	05/29/2020 09:30:00	-	High	Network Application ...	333	Avg. Response Time : 5...	-	-	
upm-slo...	05/29/2020 09:40:00	05/29/2020 09:30:00	-	High	Network Application ...	333	Avg. Response Time : 3...	-	-	
upm-IC...	05/29/2020 09:41:18	05/29/2020 09:41:17	-	Severe	IP Conversation Alarm	333	pps : 205.00 pps > 60.0...	-	-	
upm-IC...	05/29/2020 09:49:45	05/29/2020 09:49:44	-	Severe	IP Conversation Alarm	333	pps : 205.00 pps > 60.0...	-	-	
upm-slo...	05/29/2020 09:50:00	05/29/2020 09:40:00	-	High	Network Application ...	333	Avg. Response Time : 2...	-	-	

Traffic alarms, millisecond traffic alarms, email alarms, domain alarms, and signature alarms are defined when configuring the link properties. For information about how to define an alarm, see Link Properties. Note that this view lists the logs of all triggered alarms except application alarms.


Viewing alarm logs

The **Link Alarm** view displays the link alarm logs according to alarm types. You can click **All Alarms** tab on the toolbar to view the logs of all network alarms, click **Traffic Alarm** to view the logs of traffic

alarms, click **Email Alarm** to view the logs of email alarms, click **Domain Alarm** to view the logs of domain alarms, and click **Signature Alarm** to view the logs of signature alarms.

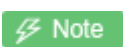
All link alarm logs are listed with trigger time, alarm category, alarm name, severity, and trigger condition. Furthermore, click the column name on the column header, and you can sort the alarm logs according to the column.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of alarm logs on the Link Alarm view, you can click  to display only the top number of items, which are displayed according to trigger time.

Analyzing alarm logs in new window

On the **Link Alarm** view, you can make analysis on one or more alarm logs. To analyze alarm logs in new window, just right-click an item and then click **Analyze in New Window**.

-  You can only make further analysis on the alarm logs on the Traffic Alarm tab, the Email Alarm tab, the Domain Alarm tab, and the Signature Alarm tab.

Searching the Service Access view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Link Alarm view will only display the items having the keyword.

The Virtual Network view

The **Virtual Network** view consists of four tabs, VLAN, MPLS VPN, VXLAN and all Virtual Network, as the figure below:

dress IP Conversation TCP Conversation UDP Conversation Segment-Segment Service Access Port Service Port Link Alarm Virtual Network x DSCP

Selected Time Range:05/29/2020 09:29:00 - 09:51:00



VLAN[11/11]

tab

Viewing Virtual Network statistics

The **Virtual Network** view displays virtual network statistics based on ID. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of items on the **Virtual Network** view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a Virtual Network

You can drill down a virtual network for more detailed information. To drill a virtual network, right-click the virtual network, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:

VLAN[11/11] ▶ IP Conversation[5/5] ▶ TCP Conversation[2/2]

To close a drilldown window, just deselect the drilled objects.

Analyzing Virtual Networks in new window

On the **Virtual Network** view, you can make analysis on one or more items independently. To analyze virtual network items in new window, just right-click a virtual network item and click **Analyze in New Window**.

Searching the Virtual Network view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. For example, enter the appropriate keyword in the search box

on the top-right corner, and then the VLAN view will only display the items having the keyword.

The DSCP view



The **DSCP** view displays DSCP traffic statistics for the monitored network link, showing as the following figure:

ess		IP Conversation	TCP Conversation	UDP Conversation	Segment-Segment	Service Access	Port	Service Port	Link Alarm	Virtual Network	DSCP	DSCP[5/5]	
Selected Time Range:05/29/2020 09:29:00 - 09:51:00													
<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>													

Viewing DSCP statistics

The **DSCP** view displays DSCP statistics based on DSCP Marking. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of items on the DSCP view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All**.

Analyzing DSCPs in new window

On the **DSCP** view, you can make analysis on one or more items independently. To analyze DSCP items in new window, just right-click a DSCP item and click **Analyze in New Window**.

Searching the DSCP view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the DSCP view will only display the items having the keyword.

The Devices Statistics view



The **Devices Statistics** view counts and displays the Devices Statistics information of selected time periods, showing as the following figure:

IP Conversation	TCP Conversation	UDP Conversation	Segment-Segment	Service Access	Port	Service Port	Link Alarm	Interface Summary	DSCP	Device Statistics		
Select a time range in the Time Window.										Device Statistics		
<div>TPP </div>										<div> Search Device Statistics</div>		
Devi...	Broadcast P...	Multicast Pk...	ICMP Pkts	New Conversatio...	Concurrent Conversatio...	Inbound Traf...	Outbound Traf...	Total Traf...	bps	Inbound bps	Outbound bps	Inbound Pkts

Viewing Devices statistics

The **Devices Statistics** view counts and displays the Devices Statistics information of selected time periods. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

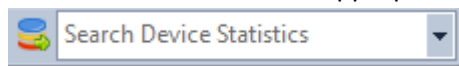
When there are a lot of items on the Devices Statistics view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All**.

Analyzing Devices in new window

On the **Devices Statistics** view, you can make analysis on one or more items independently. To analyze device items in new window, just right-click an item and click **Analyze in New Window**.

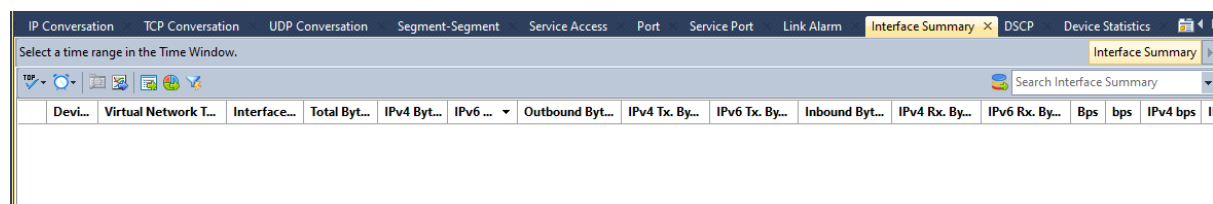
Searching the Devices Statistics view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box

 on the top-right corner, and then the Devices Statistics view will only display the items having the keyword.

The Interface Summary view



The **Interface Summary** view counts and displays the interface information of selected time periods, showing as the following figure:



Viewing Interface statistics

The **Interface Summary** view counts and displays the interface information of selected time periods. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

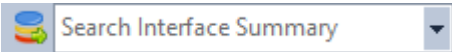
When there are a lot of items on the Interface view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column. If you want to display all the statistical items on this view, just click  and click **Show All**.

Analyzing Interfaces in new window

On the **Interface Summary** view, you can make analysis on one or more items independently. To analyze interface items in new window, just right-click an item and click **Analyze in New Window**.

Searching the Interface Summary view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box

 on the top-right corner, and then the Interface view will only display the items having the keyword.


Multi-segment analysis

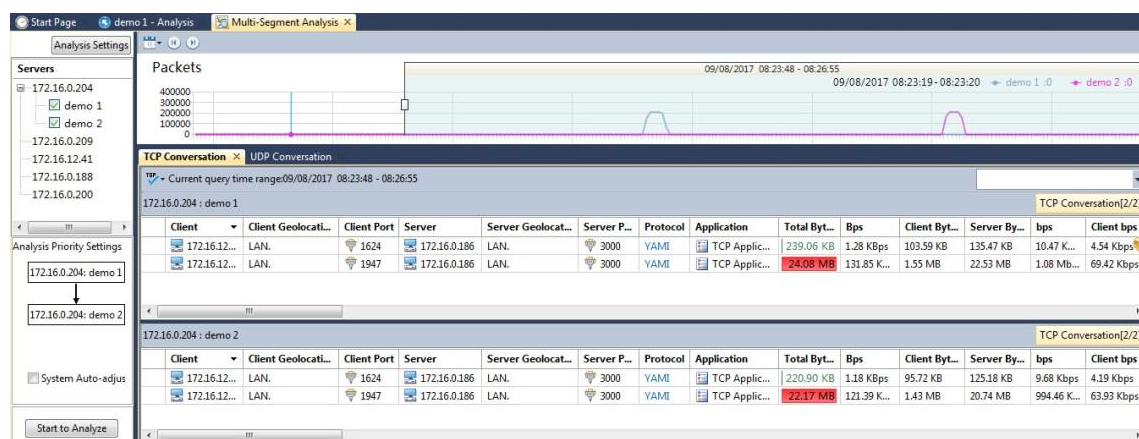
Multi-segment analysis provides collaborative analysis for the conversations across multiple segments, to provide packet loss, network delay, retransmission and other related information.

Multi-segment analysis can provide summary analysis and detail analysis for the conversations across multiple segments.

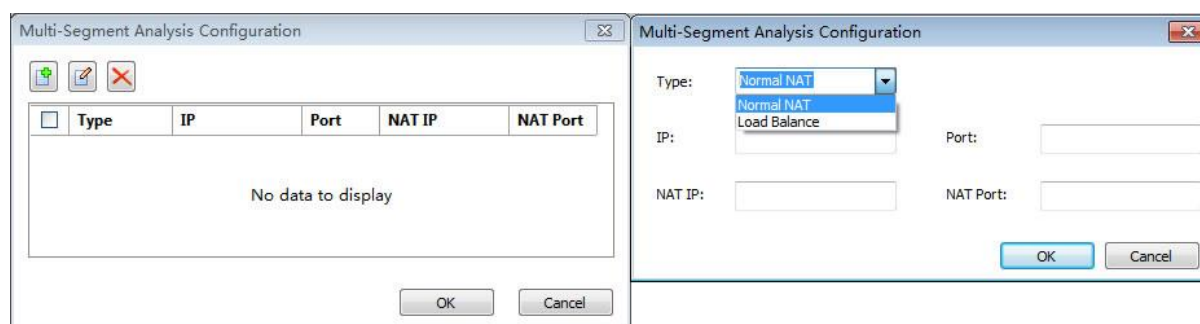
Configuring Multi-Segment analysis

The steps of Multi-Segment Analysis configuration are as follows:

On the TCP Conversation view, the UDP Conversation view or the IP Conversation view, select an interested conversation, right-click and then click **Multi-Segment Analysis**, or click the button  on the toolbar. The Multi-Segment Analysis window shows as follows:



If it is required, by clicking the button Analysis Settings, users can configure NAT collaborative analysis and Load Balance collaborative analysis.



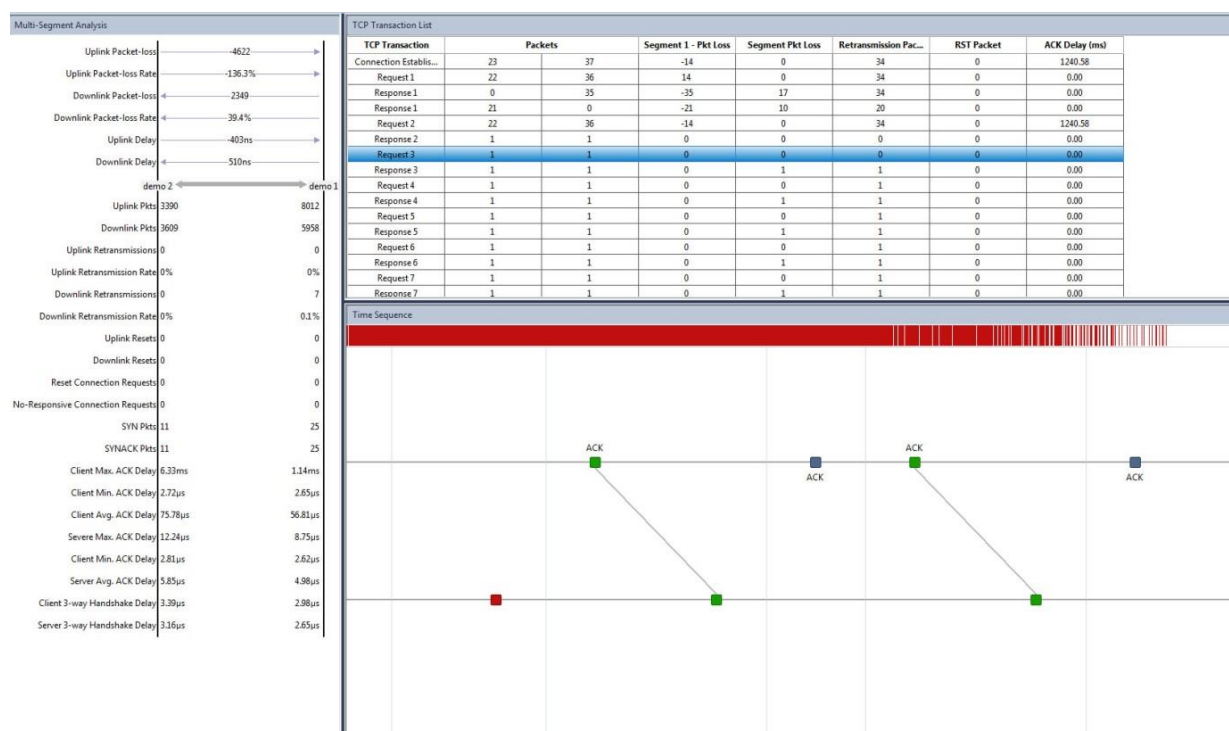
Choose network links (at most 3 network links) for concurrent analysis. If the server is not connected, just double-click to connect it and choose the appropriate network link.

Users can drag to adjust the sequence of network links in Analysis Priority Settings. Users can also select System Auto-adjust option.

Click the button Start to Analyze, to start the Multi-Segment Analysis.

Detail analysis

On the Multi-Segment Analysis window, click an interested conversation, and then click Start to Analyze. The Multi-Segment Detail Analysis window opens, as the figure below:



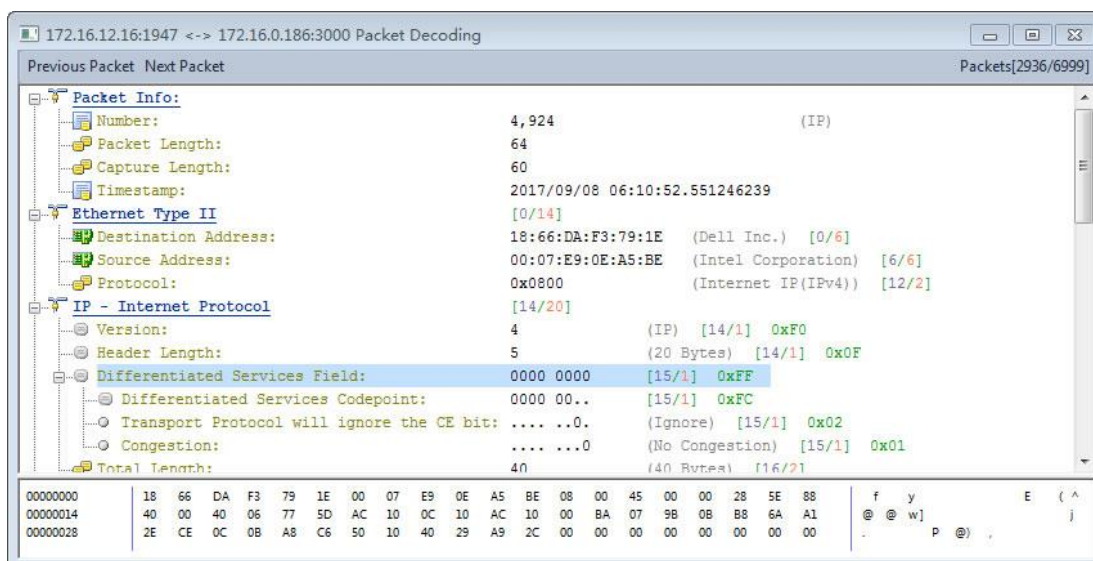
Multi-Segment Detail Analysis window consists of a left pane which lists parameter statistics, a time sequence chart, and a TCP Transaction List.

The left pane provides statistics on uplink and downlink packet loss, uplink and downlink network delay, uplink and downlink retransmission, uplink and downlink TCP flags, and so on.

The time sequence chart graphically displays the packet transmission among the network links, taking the conversation time as the horizontal axis.

The TCP Transaction List displays the count of packets, segment packet loss, RST packet, ACK delay and so on.

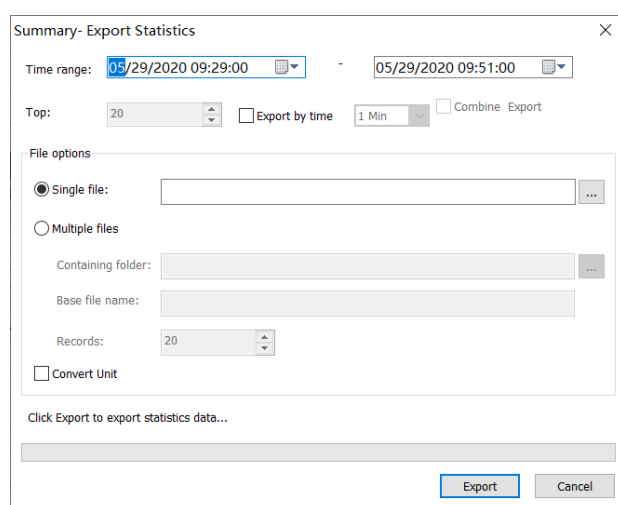
When you click a packet on the time sequence chart, the packet decoding pane will display the detailed decoding information for that packet.



Exporting statistics

To export statistics, follow the steps below:

Click  on the toolbar to open the Export Statistics dialog box which shows as the following figure:




The Export Statistics dialog box

The following list describes the items on the Export Statistics dialog box.

Time range: This option is for specifying the statistics of which time range will be exported. You can just click the numbers to specify the time or click the little triangle to specify the time. By default, the time range is just the one that you select on the Time Window.

Top: This option is for specifying which statistical items to be exported. The statistical items are sorted according to the value of **Bytes** for all analysis views. This option is not available for the Summary view.

Export by time: This option indicates to export the statistics of the selected time range according to specified time interval. For example, taking the time range as 8 hours and the time interval as 1 hour, **Export by time** indicates to export 8 parts of statistics with one recording the statistics of one hour.

Single file: This option is for exporting the statistics of selected time range as one file. You can click  to specify the file path and the file name.

Multiple files: This option is for exporting the statistics of selected time range as multiple files. Once you select this option, you should set the following options:

Containing folder: This option is for specifying the folder for storing the multiple files.

Base file name: This option is for specifying the prefix of the file name.

Records: This option is for setting how many records one file contains. When one file contains records of this setting, a new file will generate to save the other records.

Convert Unit: This option is to enable the unit conversion of the statistics. For example, the statistic is 1024 bytes and, if you enable this option, it will be 1KB.

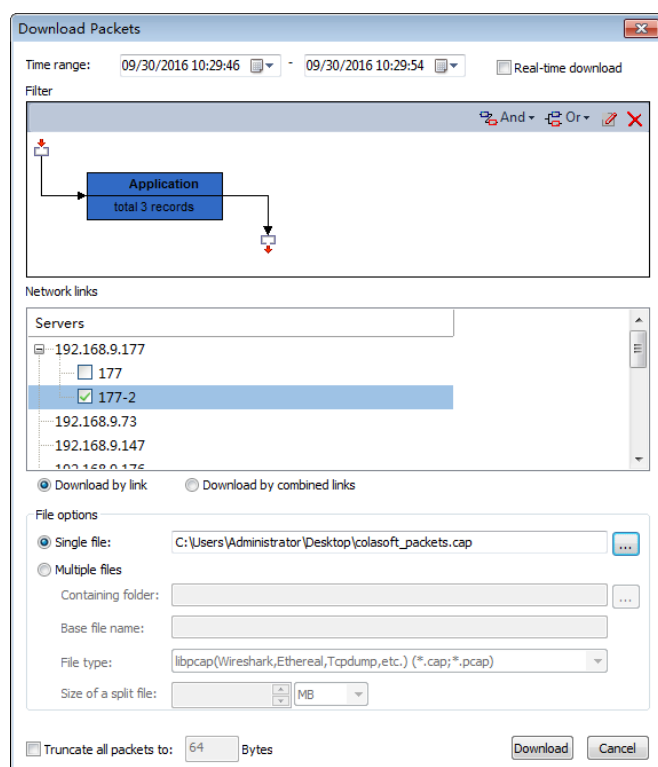
Progress: This option is for displaying the export progress, as well as the sum of exported records.

Downloading packets

To download packets, follow the steps below:

For packets downloading, in nChronos system, both **time-specific download** mode and **real-time download** mode are supported.

Click  on the toolbar to open the Download Packet dialog box which shows as the following figure:



Time-Specific Download: Users need to set the time range, filter condition, file option, file type and other information according to their needs. After settings, click the button Download to start downloading.

Real-time download: When this option is enabled, nChronos starts to download packets from the latest moment until the download is stopped manually.

☒ Real-time download

What's more convenient, in both the two modes, the system supports downloading packets from different links at the same time.

In the list of servers, select the links that packets need be downloaded from. Users can set up separate download (downloaded data of each link is saved as a separate packet) or combined download (all the download data of multiple links are saved as one packet) according needs.

The Download Packets dialog box

The following list describes the items on the Download Packets dialog box.


Time range: This option is for specifying the packets of which time range will be downloaded. You can just click the numbers to specify the time or click the little triangle to specify the time. By default, the time range is just the one that you select on the Time Window.

Real-time download: When this option is enabled, nChronos starts to download packets from the latest moment until the download is stopped manually.

Filter: This option is for filtering out unnecessary packets. You can set the filter according to application, conversation, address, port, and network segment with logical AND rule and logical OR rule.

Download by link: When this option is enabled, the packets will be downloaded separately according to network links.

Download combined: When this option is enabled, the packets from multiple network links will be downloaded together.

Single file: This option is for downloading the packets of selected time range as one file. You can click  to specify the file path and the file name.

Multiple files: This option is for downloading the packets of selected time range as multiple files. Once you select this option, you should set the following options:

Containing folder: This option is for specifying the folder for storing the multiple packet files.

Base file name: This option is for specifying the prefix of the packet file name.

File type: This option is for specifying the packet file format to store the packets. You can store the packets in .rawpkt format and in .cap format.


Split size: This option is for specifying the file size of downloaded packets. The downloaded packets will be automatically split into multiple files according to the split size.

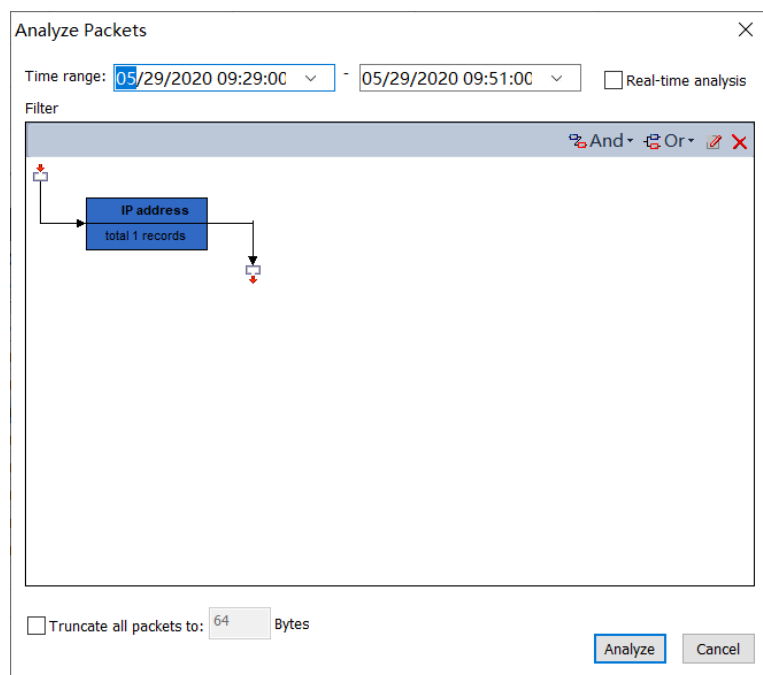
Truncate all packets to: When this option is enabled, all packets will be truncated to the specified size.

Analyzing with Expert Analyzer

The Expert Analyzer provides expert analysis and diagnosis on and decodes the downloaded packets.

To analyze packets with Expert Analyzer, follow the steps below:

Click  on the toolbar of the analysis views to open the **Analyze Packets** dialog box, which shows as the following figure:



Time range: Shows the packets of which time period will be analyzed. You can set the range by typing directly or by pressing the appropriate arrow keys. By default, if a range is selected on the *Time Window*, the range will be the selected range; and if no range is selected on the *Time Window*, the range will be just the same as that of the *Time Window*.

Real-time analysis: When this option is enabled, nChronos starts to analyze packets from the latest moment until the analysis project is stopped manually.

Filter: Shows the filters to separate particular packets. You can click **And/Or** to define filter conditions.

Truncate all packets to: When this option is enabled, all packets will be truncated to the specified size.

Complete the Analyze Packets dialog box, and then click Analyze to open the Expert Analyzer user interface.

For more information about Expert Analyzer, you can press **F1** when loading Expert Analyzer to get the Help document about Expert Analyzer.

Link Monitor

Once an nChronos Server is connected, the Server Explorer displays the network links under the Server, and then you can choose to monitor the network link in real-time or retrospectively analyze

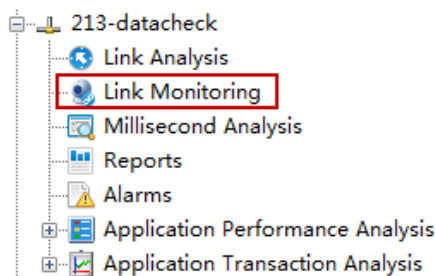
the network link. This chapter describes how to monitor a network link and the elements on the link monitor window.

Monitoring a network link in real-time

To monitor the network link in real-time:

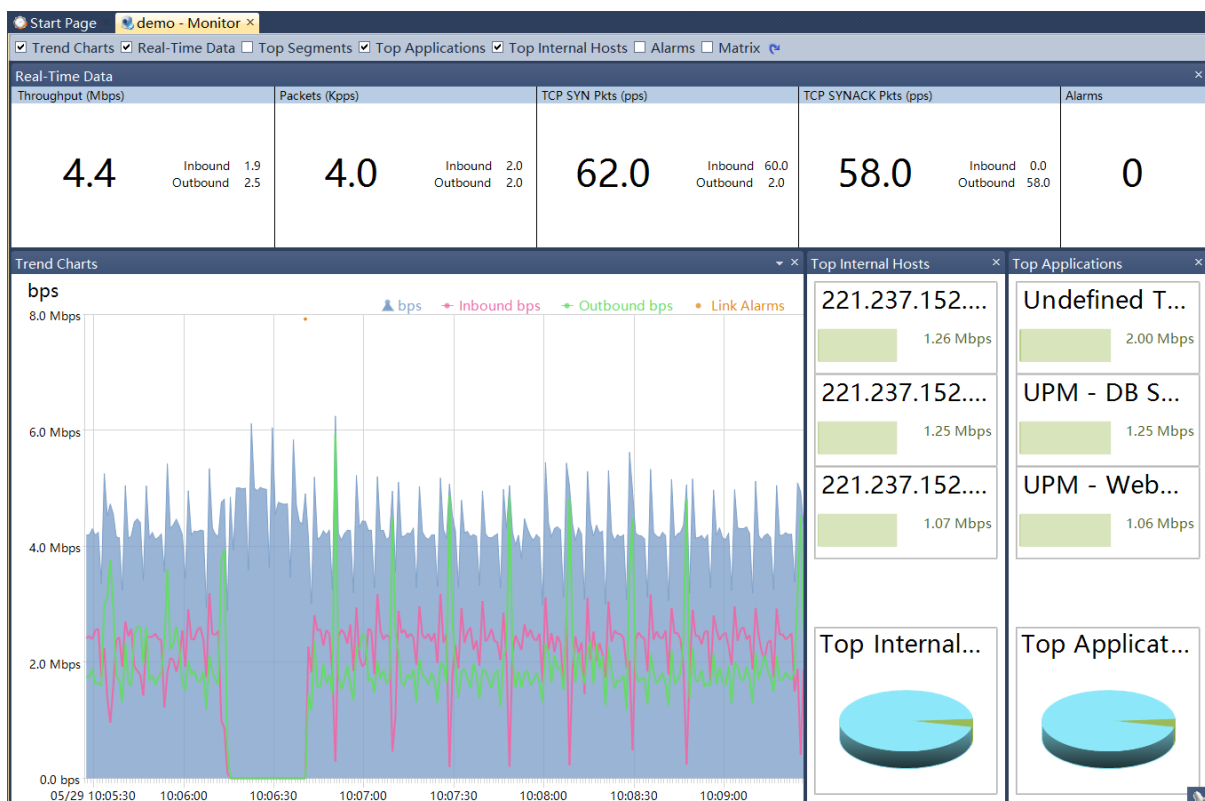
1. Connect a Server, and then network links created for the Server displays under the Server on the Server Explorer.

Double-click the node **Link Monitor** under the network link to open the Monitor window.




The link monitor window

Once a network link is monitored, a link monitor window appears to show the real-time status of the network link, like the following figure:



The link monitor window includes a top bar and several panes: the Real-Time Data pane, the Trend Charts pane, the Top Segments pane, the Top Internal Hosts pane, the Top Applications pane, the Alarms pane, and the Matrix pane.

The top bar includes checkboxes to show or hide the seven panes, and a Default Layout button.

Select the checkbox in front of a pane to show the pane. Click  to display the link monitor window in the default layout.

To close a pane, just click the close button on the top right corner on each pane or cancel the selection on the check box in front of the pane name on the top bar of the link monitor window.

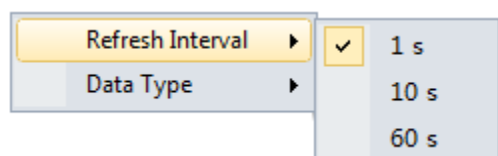
To change the size of the panes, move the mouse pointer on the border between panes, and when the pointer becomes a double-headed arrow, drag the pointer to move the split line.

The Real-Time Data pane

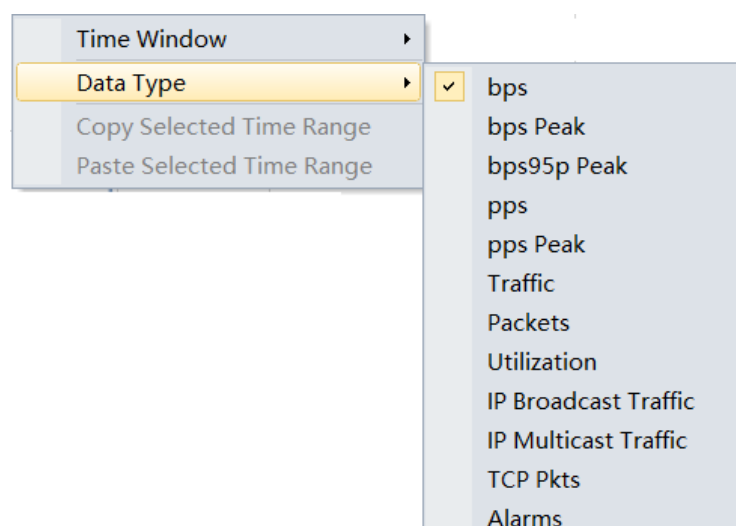
The **Real-Time Data** pane displays the real-time data of the network, including throughput, packets, bandwidth utilization, TCP SYN packets, TCP SYNACK packets, and alarm quantity, just like the following figure:

Real-Time Data											
Throughput(Mbps)			Packets(pps)			TCP SYN Pkts(pps)			TCP SYNACK Pkts(pps)		Alarms
1.1			338.0			5.0			6.0		1
Inbound 0.3			Inbound 94.0			Inbound 0.0			Inbound 3.0		
Outbound 0.1			Outbound 88.0			Outbound 2.0			Outbound 0.0		

You can set the refresh interval for the Real-Time Data pane by right-clicking in it.

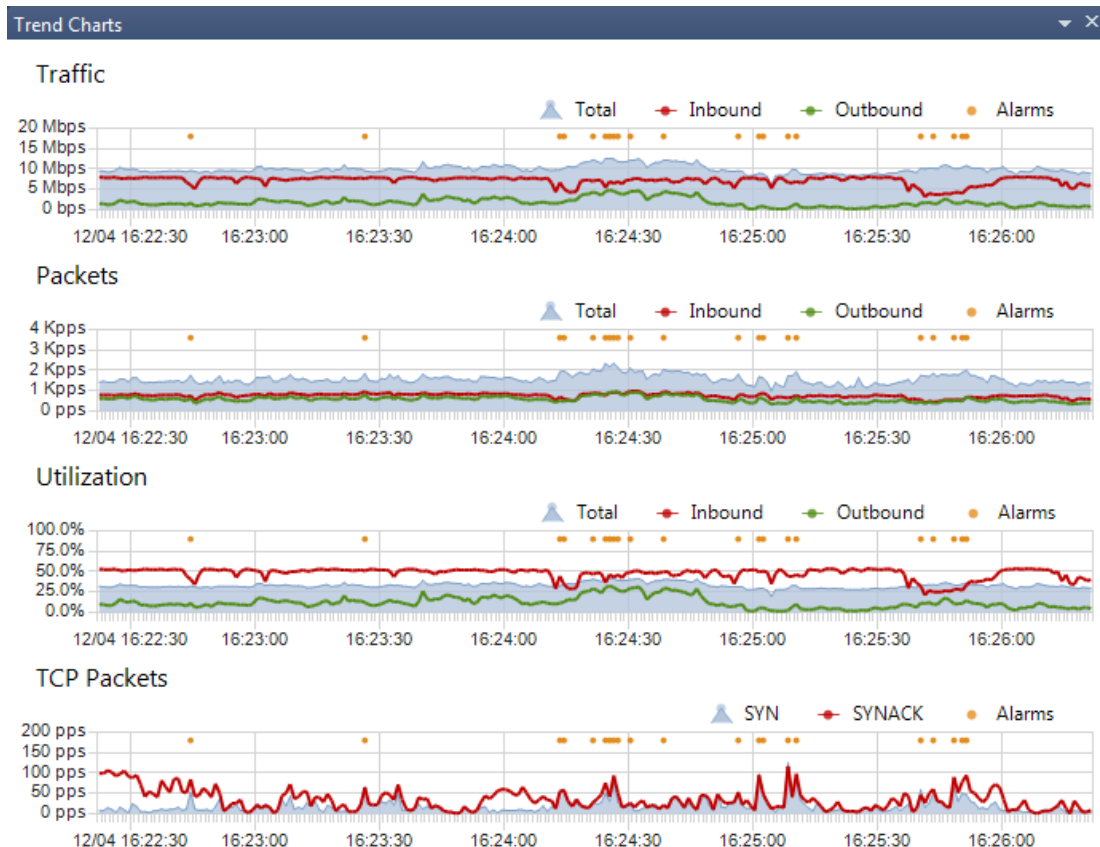


Furthermore, you can hide or show a type of real-time data by right-clicking the Real-Time Data pane and then deselecting or selecting the data type.



The Trend Charts pane

The **Trend Charts** pane on the link monitoring window is provided to display the real-time status of the network, with a horizontal axis marked with time scales and a vertical axis marked with value scales. The trend charts update automatically from right to left, displaying the latest data. By trend charts, you can get a direct view of the network status. The **Trend Charts** pane shows as the following figure:

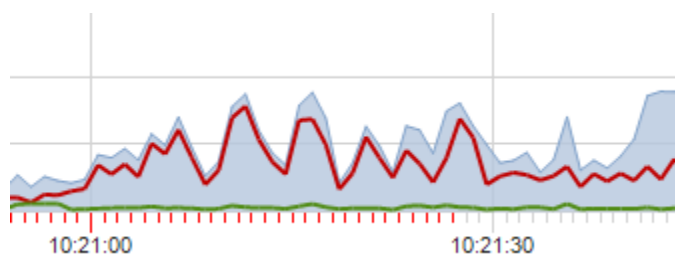


To close the trend charts pane, just deselect **Trend Charts** on the top bar.

○ [Tips](#)

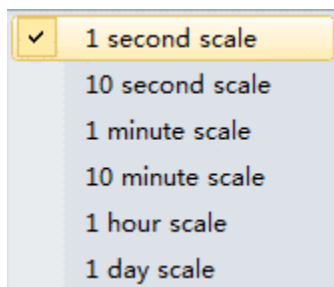
The small yellow dots on the trend charts indicate that there are alarms triggered.

The red scales on the horizontal axis indicate that the packets captured in that time period have been cleared. As the following figure, the packets before 10:21:27 have been cleared:



Time window type

All trend charts are displayed in a time window, which has a time axis marked with time scales. The time scales change according to time window types. You can select the appropriate time window by right-clicking any trend charts and selecting the appropriate one. In front of the first time scale, the date of that time displays.



The following list describes the time window types:

1 second scale: The trend charts display the network status of the latest 4 minutes with the smallest time scale as 1 second.


10 second scale: The trend charts display the network status of the latest 40 minutes with the smallest time scale as 10 seconds.

1 minute scale: The trend charts display the network status of the latest 4 hours with the smallest time scale as 1 minute.

10 minute scale: The trend charts display the network status of the latest 40 hours with the smallest time scale as 10 minutes.

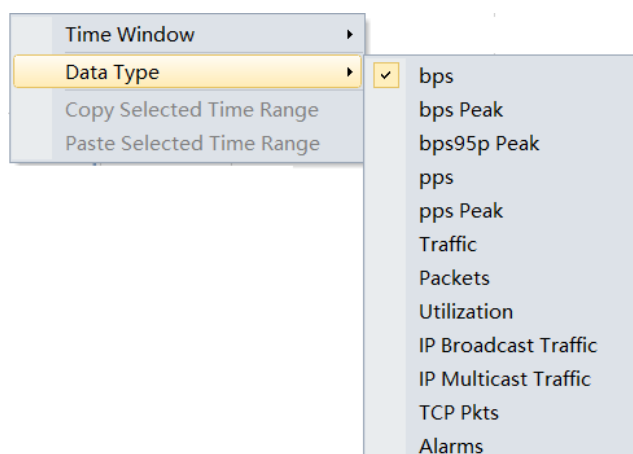
1 hour scale: The trend charts display the network status of the latest 10 days with the smallest time scale as 1 hour.

1 day scale: The trend charts display the network status of the latest 240 days with the smallest time scale as 1 day.

 **Note** All trend charts have the same time window.

Trend chart type

There are several types of trend charts on the link monitoring window, each displaying the data of that type of the network.



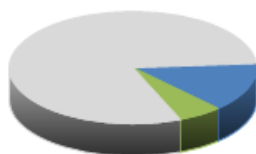
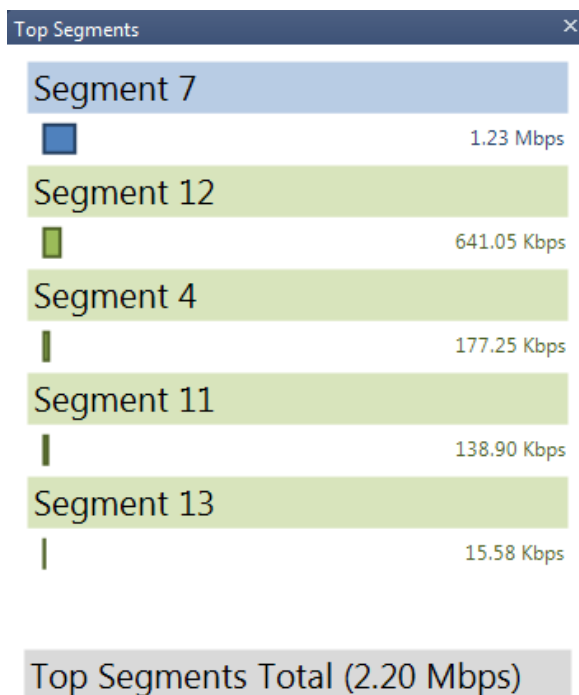
You can hide or show a trend chart by right-clicking any trend charts and then deselecting or selecting the trend chart.

The following list describes the trend chart types:

- **Traffic:** The traffic trend chart displays the real-time traffic of the network link. **Total** indicates the total traffic of the network, **Inbound** indicates inbound traffic, and **Outbound** indicates outbound traffic. Both inbound and outbound are defined when you add a network link.
- **Packets:** The packets trend chart displays the real-time traffic of the network link in a form of packets. **Total** indicates the quantity of total packets per second, **Inbound** indicates the quantity of inbound packets per second, and **Outbound** indicates the quantity of outbound packets per second.
- **TCP Packets:** The TCP packets trend chart displays the TCP packets quantity over the network. **TCP SYN** indicates the quantity of TCP SYN packets per second, and **TCP SYNACK** indicates the quantity of TCP SYNACK packets per second.
- **Utilization:** The utilization trend chart displays the bandwidth utilization.
- **Alarms:** The alarms trend chart displays all the alarm quantity of the network link. All alarms are defined by you when configuring a network link. You can also upload signature alarms to the library of Server configurations.

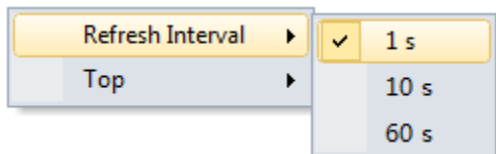
The Top Segments pane

The **Top Segments** pane lists the top network segments according to the traffic of them, and the traffic is displayed by bar charts as well as real-time figures just below the segments. The segments are defined when you configuring the network settings. The **Top Segments** pane shows as the following figure:

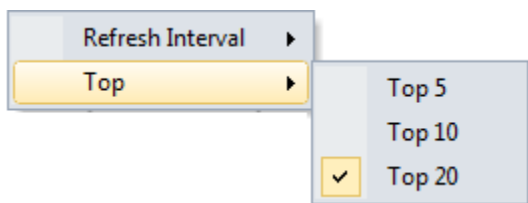


Below the top segment list, there is a pie chart, in which the colors represent corresponding top segments and when two or more segments share one color it means the color in the pie chart represents the sum of corresponded segments.

You can set the refresh interval of the Top Segments pane by right-clicking in it and then selecting the appropriate interval.



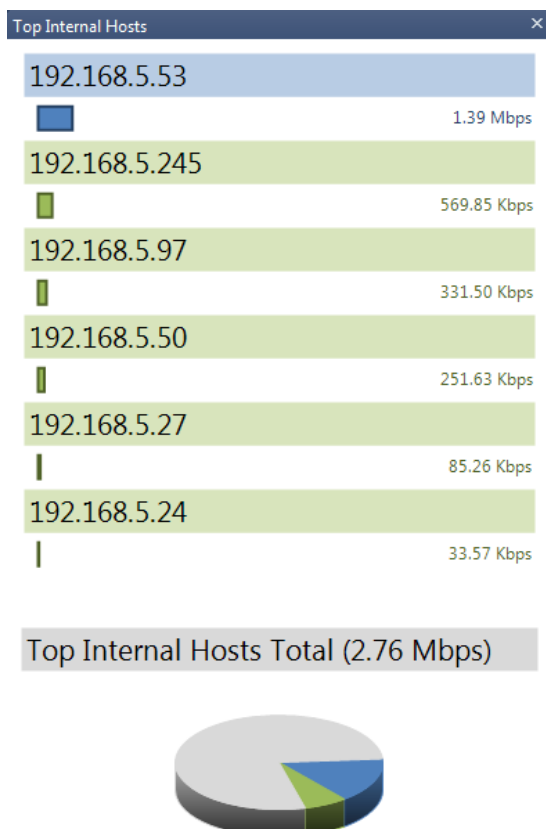
In addition, you can also set the number for the top segments.



The Top Internal Hosts pane

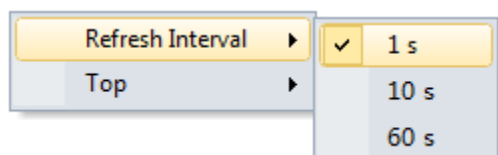
The **Top Internal Hosts** pane lists the top internal hosts according to the traffic of them, and the traffic is displayed by bar charts as well as real-time figures just below the hosts. The hosts are displayed as names or IP addresses, which is determined according to the setting in the View menu.

The **Top Internal Hosts** pane shows as the following figure:

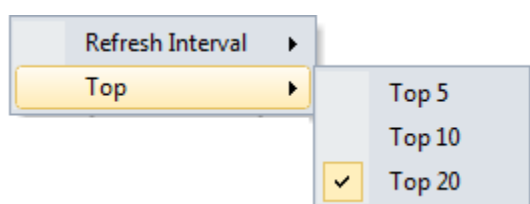


Below the top internal host list, there is a pie chart, in which the colors represent corresponding top internal hosts and when two or more hosts share one color it means the color in the pie chart represents the sum of corresponded hosts.

You can set the refresh interval of the Top Internal Hosts pane by right-clicking in it and then selecting the appropriate interval.

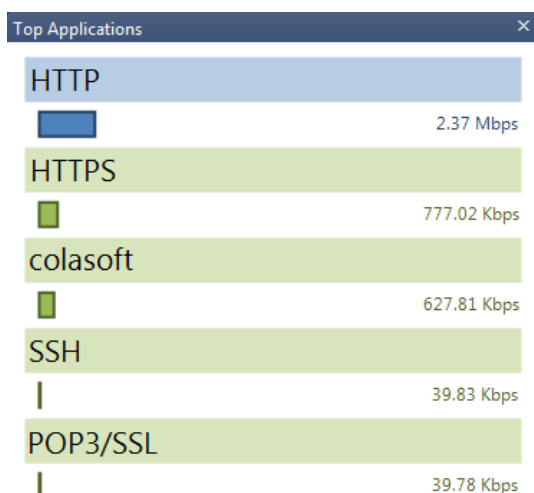


In addition, you can also set the number for the top internal hosts.



The Top Applications pane

The **Top Applications** pane lists the top applications according to the traffic of them, and the traffic is displayed by bar charts as well as real-time figures just below the applications. The **Top Applications** pane shows as the following figure:



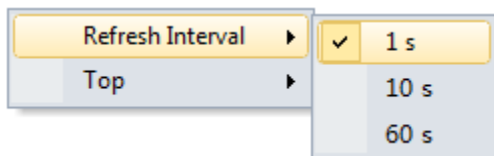
Top Applications Total (3.86 Mbps)



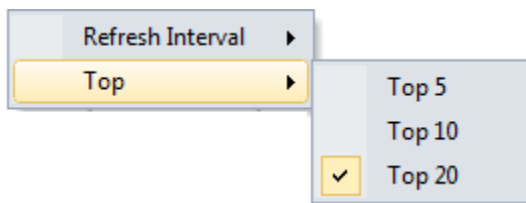
The applications can be system application and custom applications, but the custom applications have priority over the system applications. The system applications are uploaded to the library when configuring the Server and the custom applications can be customized when configuring link properties.

Below the top application list, there is a pie chart, in which the colors represent corresponding top applications and when two or more applications share one color it means the color in the pie chart represents the sum of corresponded applications.

You can set the refresh interval of the Top Applications Hosts pane by right-clicking in it and then selecting the appropriate interval.



In addition, you can also set the number for the top applications.



The Alarms pane

The **Alarms** pane lists all alarms triggered in the current second, including trigger time, alarm category, alarm object, alarm name, alarm severity, and trigger condition, showing as the following figure:

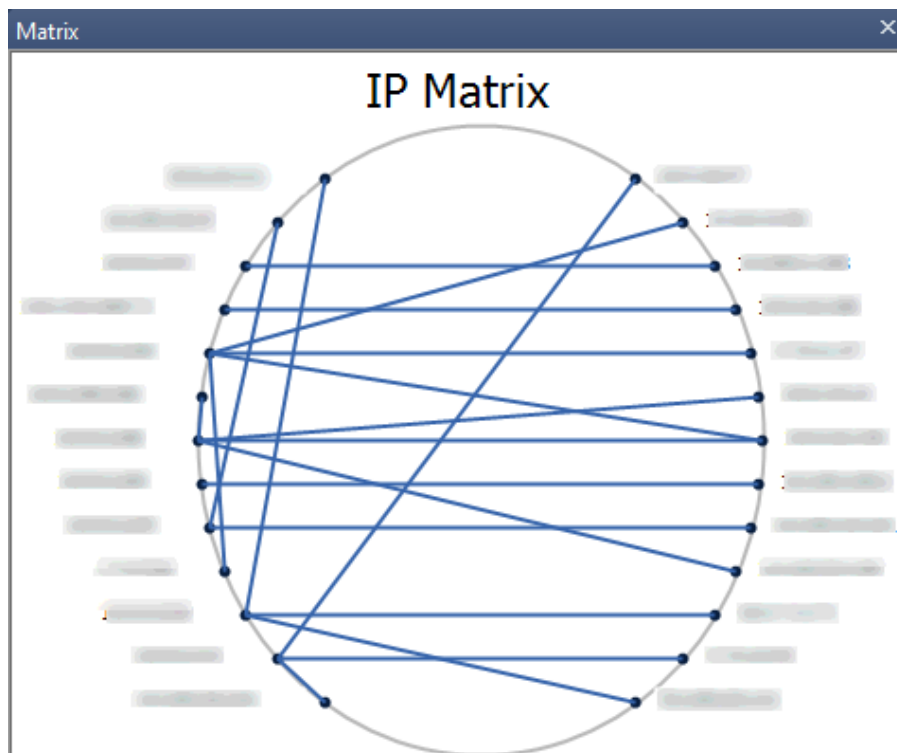
Alarms					
Statistic Time	Trigger Time	Alarm Name	Severity	Summary	
09/28/2014 11:19:58	09/28/2014 11:19:57	Traffic Alarm1	Minor	Bps: 111329933 >= 10000000	
09/28/2014 11:19:57	09/28/2014 11:19:56	Traffic Alarm3	Major	192.168.0.208, pps: 99454 >= 30000	
09/28/2014 11:19:56	09/28/2014 11:19:55	Traffic Alarm2	Severe	Utilization: 34% >= 30%	
09/28/2014 11:19:56	09/28/2014 11:19:55	Traffic Alarm1	Minor	Bps: 87038270 >= 10000000	
09/28/2014 11:19:54	09/28/2014 11:19:53	Traffic Alarm3	Major	192.168.0.208, pps: 73156 >= 30000	
09/28/2014 11:19:52	09/28/2014 11:19:51	Traffic Alarm1	Minor	Bps: 68409963 >= 10000000	
09/28/2014 11:19:51	09/28/2014 11:19:50	Traffic Alarm3	Major	192.168.0.208, pps: 57839 >= 30000	
09/28/2014 11:19:50	09/28/2014 11:19:50	Traffic Alarm1	Minor	Bps: 61635509 >= 10000000	
09/28/2014 11:19:40	09/28/2014 11:19:40	Traffic Alarm1	Minor	Bps: 49755959 >= 10000000	
09/28/2014 11:19:40	09/28/2014 11:19:40	Traffic Alarm1	Minor	Bps: 61219600 >= 10000000	

You can click the drop-down triangle  to view the logs of specific alarm type.

All alarms are defined by you when configuring a network link. You can also upload signature alarms to the library of Server configurations.

The Matrix pane

The **Matrix** pane shows the network communication in peer map. The **Matrix** pane shows as the following figure:



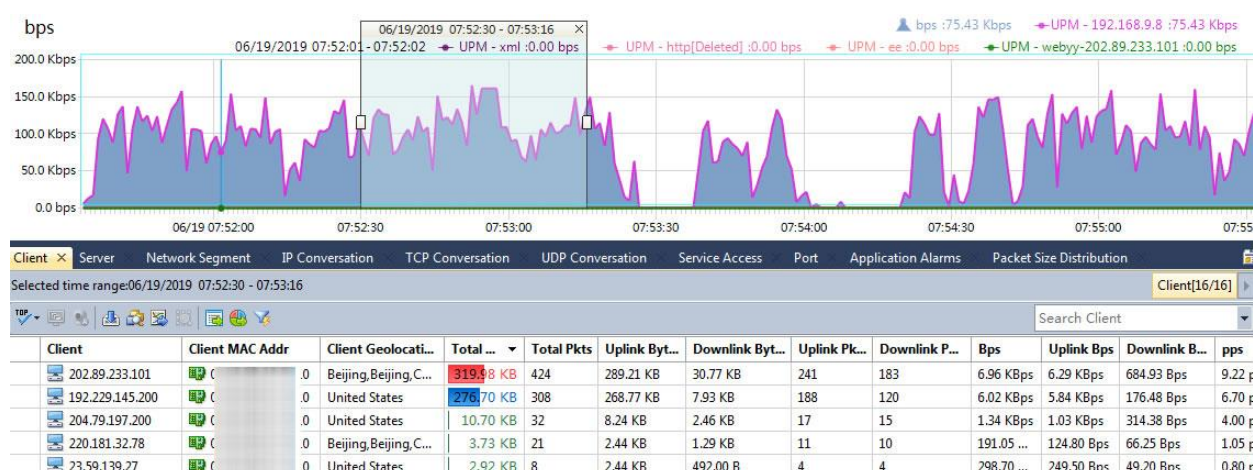
Move your mouse over one node, it will display the transmitted packets and bytes as well as received packets and bytes of the node, and display the peer nodes in highlight.

By default, the matrix pane displays the peer map of the communications between IP addresses. You can right-click the matrix and select **MAC Matrix** to display the peer map of the communications between MAC addresses.

Furthermore, you can select the refresh interval of the matrix by right-clicking the matrix and clicking the appropriate interval.

Custom Analysis in New Window

Custom Analysis in New Window provides retrospective analysis of defined objects. Users can select or input objects for retrospective analysis according to their needs. The interface includes trend charts and the statistics view. This function is similar to **Analysis in New Window**, but it is faster and more convenient. The analysis window for custom objects shows as the screenshot below:



The analysis window for analyzing custom analysis includes a time window on the upper pane and some analysis views on the lower pane, both of which are just the same as those in retrospective analysis. However, the time window in custom analysis only displays charts of the traffic of analyzed custom objects, and the Time Window in the Link Analysis window displays the traffic of the whole network.

Trend charts

The custom analysis time window provides a chart for each analyzed custom object. For example, if you select three objects to analyze, then the custom analysis time window provides three charts, each for one object with different colors to identify. When you move your mouse over the charts, the statistics of that time point will be displayed on the top right of the charts.

By default, the charts are traffic ones. You can click Data Type to display packets charts.

You can area-select any time range on the time window to view the detailed statistics of that time range on the analysis views below.

Analysis views

The analysis views for application group analysis include the Client view, the Server view, the Network Segment view, the IP Conversation view, the TCP Conversation view, the UDP Conversation view, the Service Access view, the Port view, the Application Alarms view and the Packet Size Distribution view.

Millisecond Analysis

Millisecond analysis provides traffic analysis accurate to one millisecond.

The Millisecond Analysis window is only available when the millisecond statistics is enabled for the network link. For example, the network link "training" enables millisecond statistics:

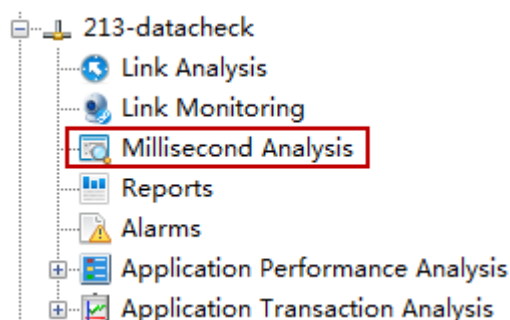
Network Link / Edit Network Link

Link name: training

Link type: Switch (bidirectional mirroring)

☒ Enable millisecond statistics

Then the network link "training" is provided with Millisecond Analysis feature:

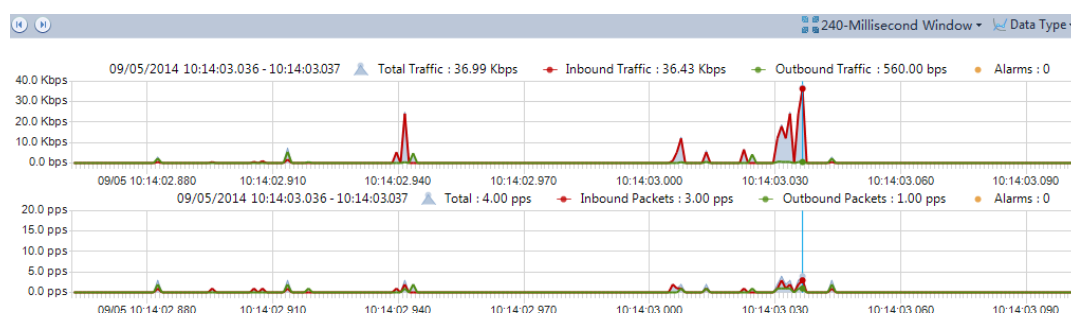


The Millisecond Analysis window includes a Time Window and two analysis views.

Time Window

The Time Window for millisecond analysis is a 240-millisecond one. The minimum scale on the horizontal axis is one millisecond.




The Time Window includes two types of charts: Traffic in bps, and Packets in pps:





The Time Window for millisecond analysis is very same to the Time Window for link analysis. You can drag and move to view historical traffic.


The Summary view

When select a time range on the Time Window, the Summary view displays the summary statistics for that range. The statistics only includes packets information and bytes information.

Summary Millisecond Traffic Alarm					
Selected time range: 09/28/2014 11:26:44.854 - 11:26:44.928					
					
Pkts	Inbound	Outbound	Bytes	Inbound	Outbound
24	12	11	14.25 KB	10.75 KB	3.40 KB










You can click the download button  to download the packets of the second that contains the selected time range.

You can click the Analyze button  to use the Expert Analyzer to analyze the packets of the second that contains the selected time range.



You can click the Export button  to export the statistics of the second that contains the selected time range.

The Millisecond Traffic Alarm view

The Millisecond Traffic Alarm view displays the logs of all triggered millisecond traffic alarms of selected time range.

Summary Millisecond Traffic Alarm							
Selected time range: 09/28/2014 11:37:52.883 - 11:37:52.948							
			 0  5  0			Search Millisecond Traffic Alarm	
Statistic Time	Millisecond Trigger Time	Category	Object	Alarm Name	Severity	Trigger Condition	
09/28/2014 11:37:52	2014/09/28 11:37:51.896	Other	Millisecond traffic	Millisecond Traffic Alarm1	 Major	Bytes per millisecond: 1430 >= 100	
09/28/2014 11:37:52	2014/09/28 11:37:51.897	Other	Millisecond traffic	Millisecond Traffic Alarm1	 Major	Bytes per millisecond: 264 >= 100	
09/28/2014 11:37:52	2014/09/28 11:37:51.915	Other	Millisecond traffic	Millisecond Traffic Alarm1	 Major	Bytes per millisecond: 264 >= 100	
09/28/2014 11:37:52	2014/09/28 11:37:51.916	Other	Millisecond traffic	Millisecond Traffic Alarm1	 Major	Bytes per millisecond: 200 >= 100	
09/28/2014 11:37:52	2014/09/28 11:37:51.928	Other	Millisecond traffic	Millisecond Traffic Alarm1	 Major	Bytes per millisecond: 262 >= 100	

All alarm logs are listed with millisecond traffic statistic time, trigger time, alarm category, alarm name, severity, trigger source and trigger condition. Furthermore, click the column name on the column header, and you can sort the alarm logs according to that column.

When there are a lot of alarm logs on the view, you can click  to display only the top number of items, which are displayed according to trigger time. If you want to display all the statistical items on this view, just click  and click Show All Records.

Reports

nChronos provides System Reports by default, and users can define reports. Both default reports and user-defined reports can be sent by email. In addition, users can schedule a report.

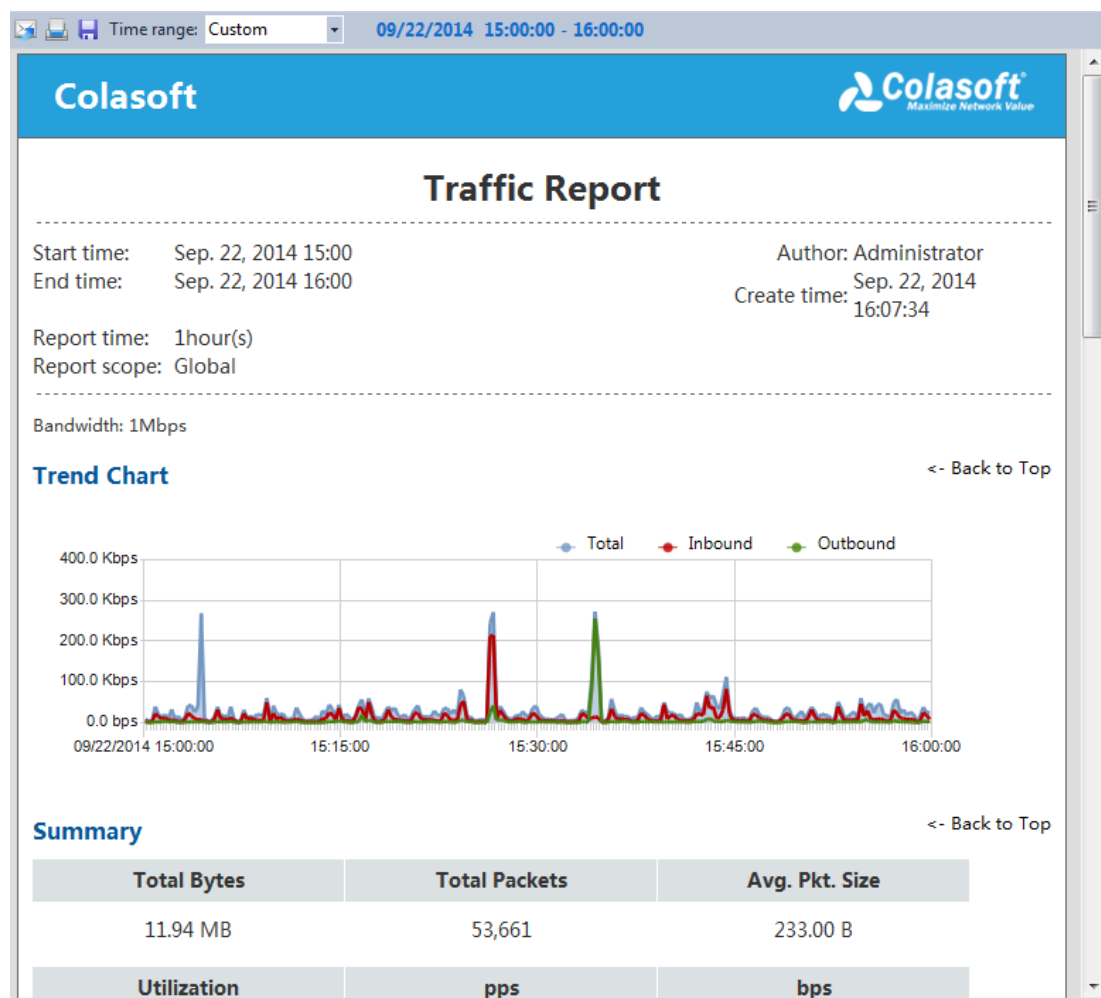
Instant reports

According to report view type, there are instant reports and scheduled reports.

Instant reports are the reports users can directly view on the Reports window of nChronos Console. An instant report could be any one of system reports, customized reports and temporary reports.

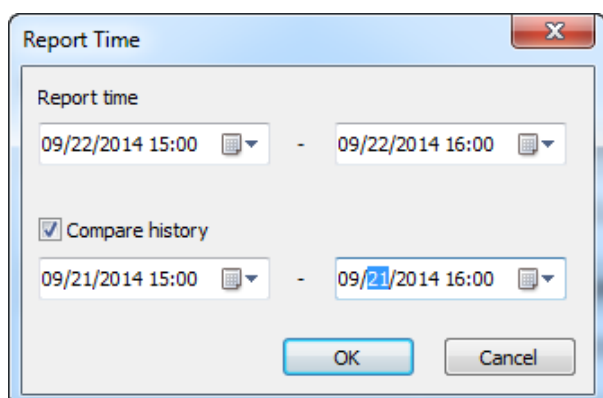
Scheduled reports are the reports scheduled by users and can only be available in the email inbox.

Following is an example of instant reports:



When users want to view the report on the Console, just click the report name on the left pane. By default, the report statistical time is the last hour. Users can click the Report time drop-down list to choose interested time duration, or just click the time to make changes on the report time.

You can compare report data with historical data. To enable comparison, click the report time to open the Report Time dialog box, enable the Compare history checkbox, and then set the compare time.



Instant reports can be printed, saved and sent by email.


Print

Click  to print an instant report.

Tips

When an instant report includes IP Traffic, MAC Address, or Segments report module, users are recommended to print the report in landscape.

Save

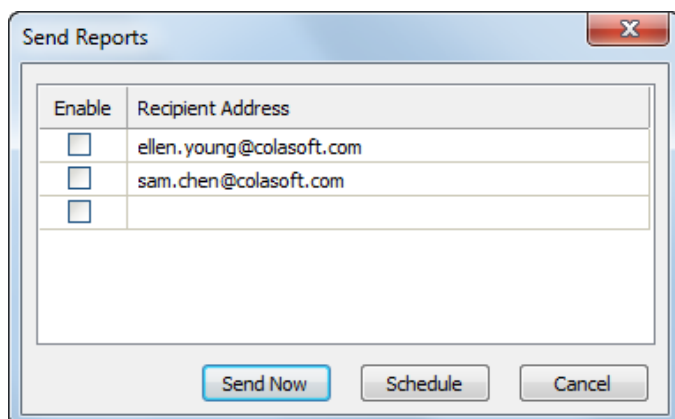
Instant reports can be viewed through nChronos Console, but they are not saved automatically. To save an instant report, click .

Email

Instant reports can be sent to email recipients.

To email an instant report,


1. Click  to open the Send Reports dialog box:



Specify the recipient.

If the recipient address is not on the list, you can click an empty list to enter a new recipient address. Click **Send Now** to send the instant report.

You can also click **Schedule** to schedule a report based on the instant report.

 **Note** Before sending a report, please make sure the SMTP Settings on Server Administration Web are configured correctly.

System Reports

By default, nChronos provides 11 System Reports, which cannot be edited or deleted, but can be duplicated. Users can duplicate a System Report and then make some modifications so as to get a user-defined report efficiently.

The System Reports include: Global Report, Traffic Report, IP Address Application Distribution Report, MAC Address Traffic Report, Alarm Statistics Report, Application Performance Analysis Report, Application Transaction Analysis Report, Top Applications Report, Top Hosts Report, Top Internal Hosts Report, and Top Segments Report.

System reports can be printed, saved to local, and sent as email. You can also schedule a system report.

User-Defined Reports

Users can create reports in two ways:

Creating a report: Creates a totally new report.

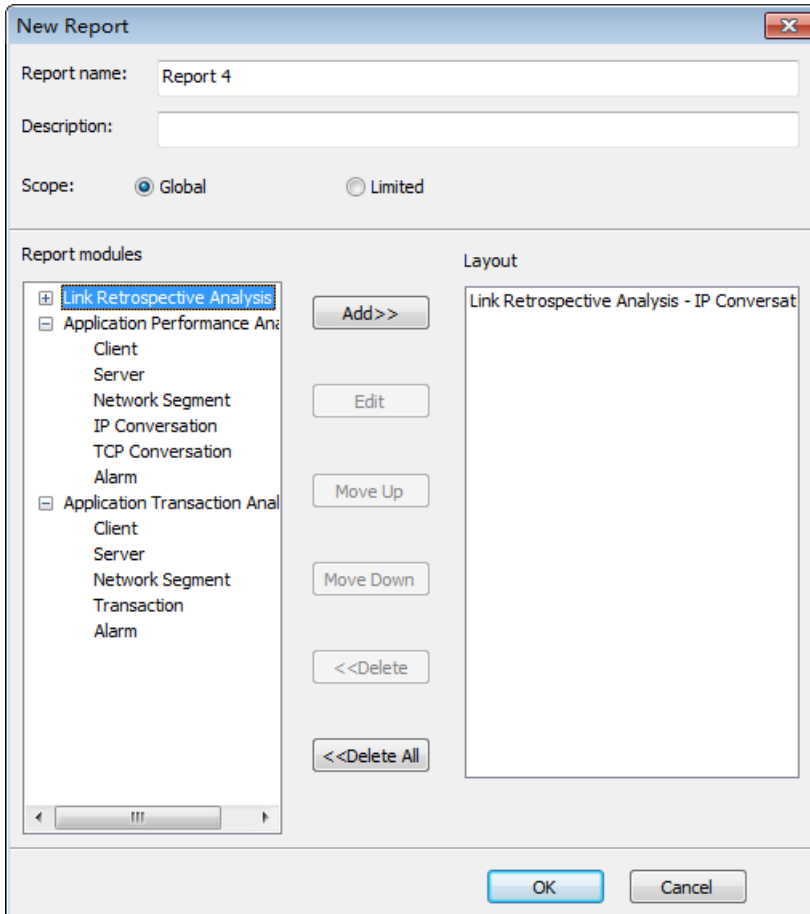
Duplicating a report: Duplicates an existent report to make some modifications to thereby fast add a new report.

Creating a report

Users can create reports based on built-in report modules.

To create a report,

1. On the Report window, locate the node **Customized Reports**, and click  to open the **New Report** dialog box:



Enter the report name and the description. The report name should be a unique one which cannot be the same as an existent report.

Select the report scope.

If you want to create a report for all network objects, click **Global**, which means the report statistics are calculated based on all network objects.

If you want to create a report for a specific network object, click **Limited** to open the **Report Scope** dialog box:

Report Scope

☐ Address

☒ Type: IP address

You can enter multiple entries with one per line.

☐ Segment Segment9

☒ Application

Name: colasoft

OK Cancel

The scope could be IP addresses, MAC addresses, network segment, or a user-defined application, which means the report statistics are calculated based on selected scope.

Click the report modules you are interested and then click **Add** to add the interested report modules to the new report.

Different report scope is provided with different report modules. The Global scope is provided with all report modules. For more information about report modules, please refer to *Report modules*.


For some modules, you can set the number of statistical objects.

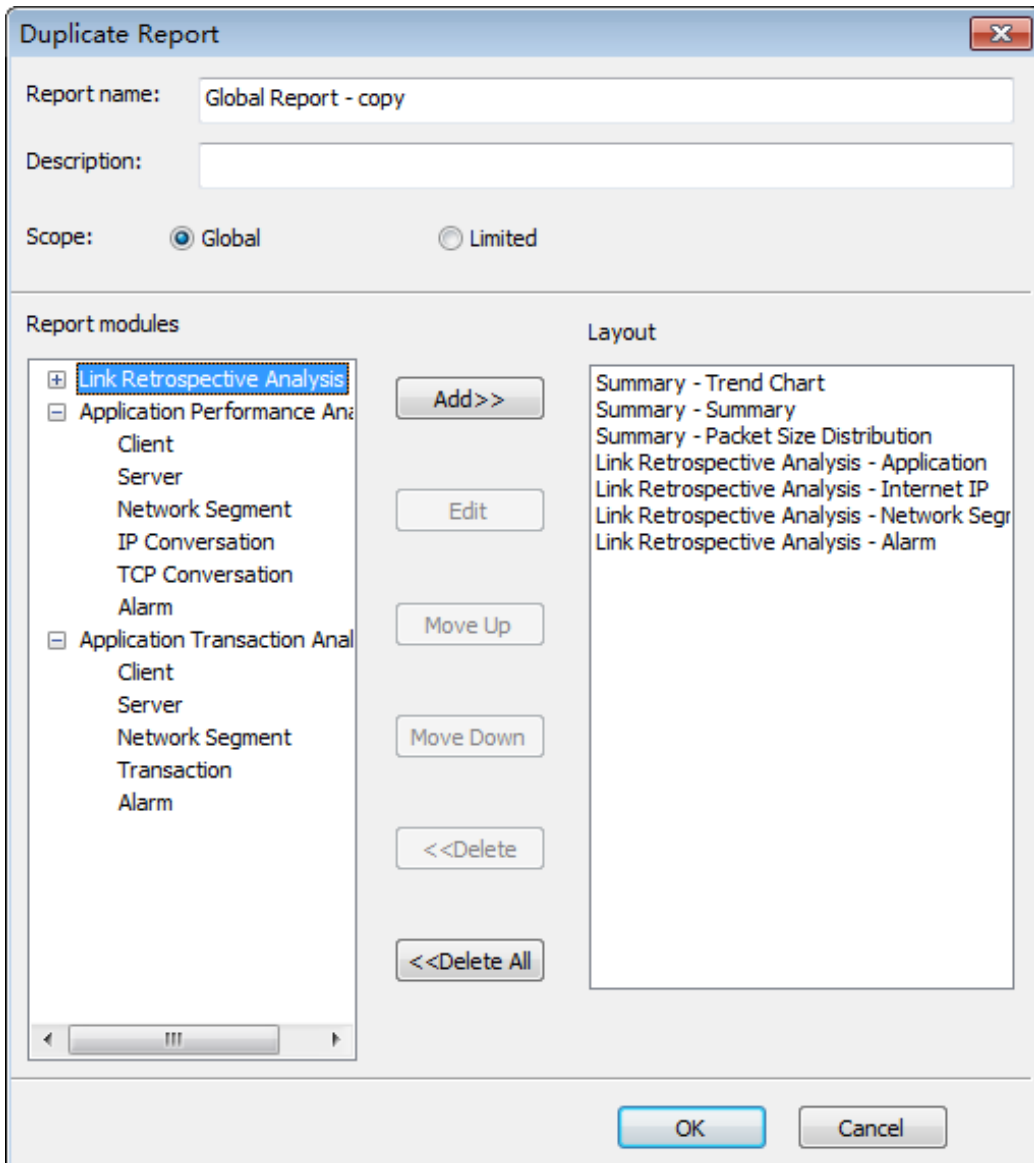
Click **OK** to complete creating a report. You can view the new report under the node **Customized Reports**.

Duplicating a report

Users can duplicate an existent report to fast create a new report. The existent could be a System Report or a User-Defined Report.

To duplicate a report,

1. On the Report window, locate the report you want to duplicate, and then click  to open the **Duplicate Report** dialog box:



Enter the report name and the description. The report name cannot be same to the duplicated one.


Modify the report scope according to the need.

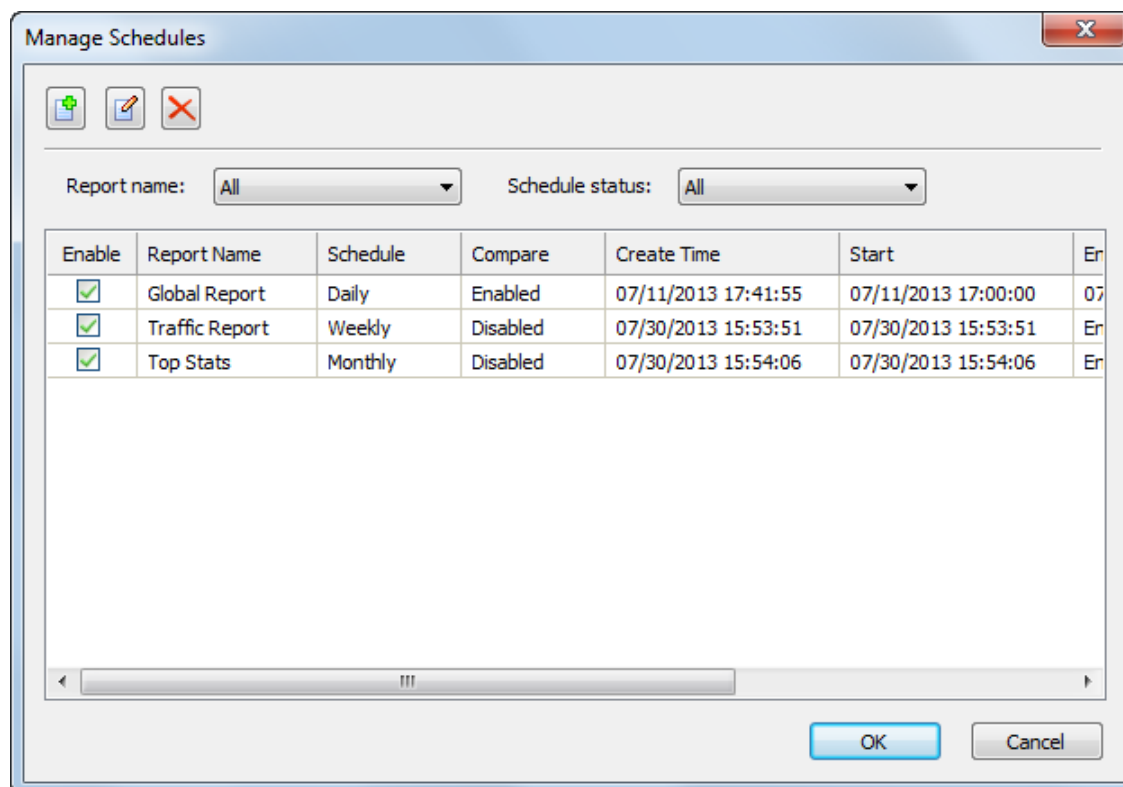
Modify the report modules according to the need.

Different report scope is provided with different report modules. The Global scope is provided with all report modules. For more information about report modules, please refer to *Report modules*.

Click **OK** to complete duplicating a report. You can view the new report under the node **Customized Reports**.

Managing schedules

Besides creating reports, users can schedule reports and send the automatically generated reports to specified email address. To manage these schedules, on the Report window, click  to open the **Manage Schedules** dialog box:



Report Name: The name of the report which the schedule is based on.

Schedule: Shows how frequently the report will be generated automatically.

Compare: Shows if the scheduled report enables the function of comparing current statistics with historical statistics.

Create Time: Shows when the schedule is created.

Start: Shows when the schedule starts.

End: Shows when the schedule will end. If the end time is not specified, it will display *Endless*, which means the schedule is always valid till the network link is removed.

Generated Reports: Shows how many reports have already been generated.

Status: Shows the status of the schedule:

Ready: The schedule is ready to run.

In progress: The schedule is in progress.


Completed: The schedule is finished. No reports will be generated for this schedule anymore.


In the **Manage Schedules** dialog box, users can search interested report schedules according to report name and schedule status.

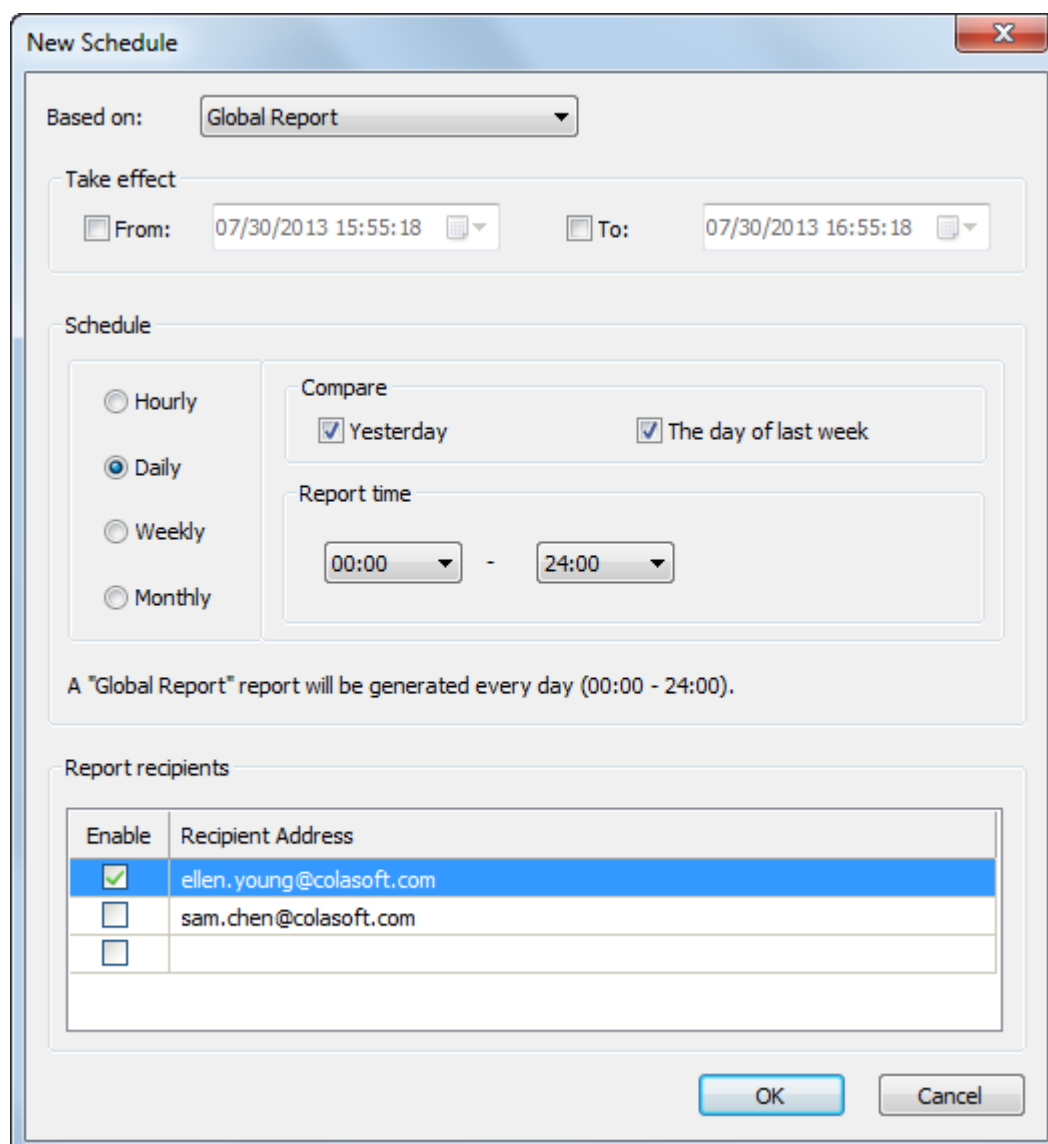
Scheduling a report

Users can schedule a report based on an existent report.

To schedule a report:

1. On the **Report window**, click  to open the **Manage schedules** dialog box.

On the **Manage Schedules** dialog box, click  to open the **New Schedule dialog** box:



The **New Schedule** dialog box is shown with the following settings:

- Based on:** Global Report
- Take effect:**
 - ☐ From: 07/30/2013 15:55:18
 - ☐ To: 07/30/2013 16:55:18
- Schedule:**
 - ☐ Hourly
 - ☒ Daily
 - ☐ Weekly
 - ☐ Monthly
- Compare:**
 - ☒ Yesterday
 - ☒ The day of last week
- Report time:** 00:00 - 24:00
- Summary:** A "Global Report" report will be generated every day (00:00 - 24:00).
- Report recipients:**

Enable	Recipient Address
<input checked="" type="checkbox"/>	ellen.young@colasoft.com
<input type="checkbox"/>	sam.chen@colasoft.com
<input type="checkbox"/>	

Buttons: OK, Cancel

Choose the report which the schedule is based on.

If necessary, specify the effective duration, which means to specify a time when the schedule starts to take effect.

Both the start and the end of the effective duration should be later than current time.


If the start time is not specified, the start time will be the time when the schedule is created.

If the end time is not specified, the end time will be the time when the link is deleted.

Specify the schedule trigger and specify whether to compare with historical statistics.

Specify the recipients for receiving the scheduled report. You can just enable the recipients on the list or you can also enter the email address of the recipient.

You can just enable the recipients on the list or you can also enter the email address of the recipient.

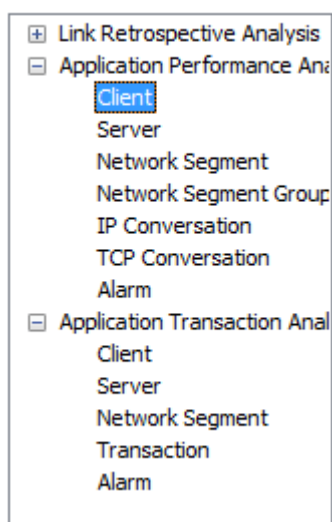
 **Tips** Right-click an existent report and then click New Schedule, in this way you can also schedule a report conveniently.

Report modules

A report consists of one or multiple built-in report modules.

All statistical fields on the default statistical views can be generated as a report. The statistical view is taken as a report module, as the following figure:

Report modules

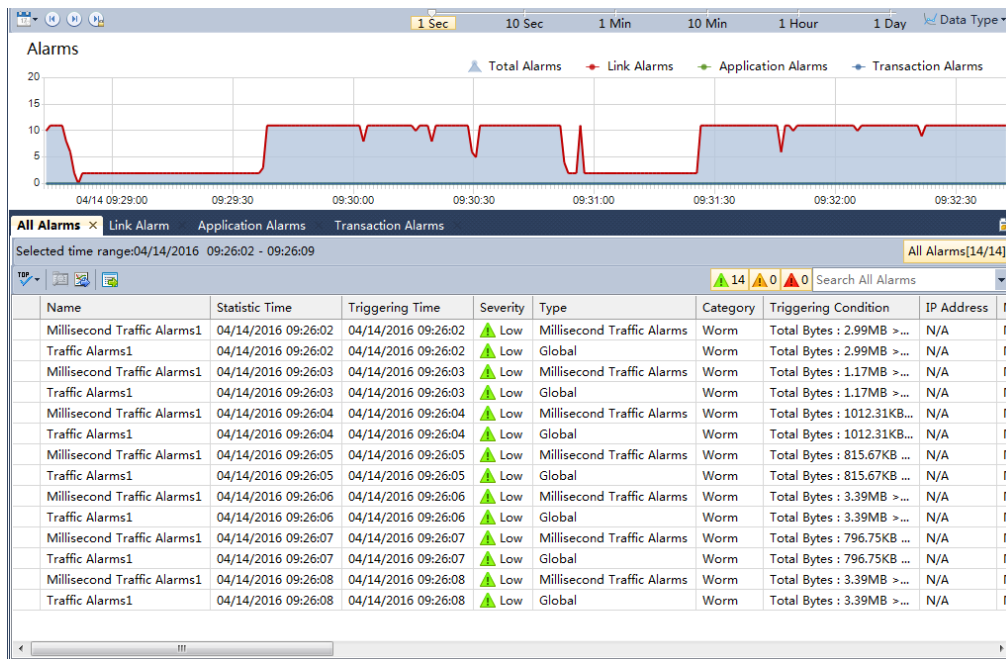


Alarms

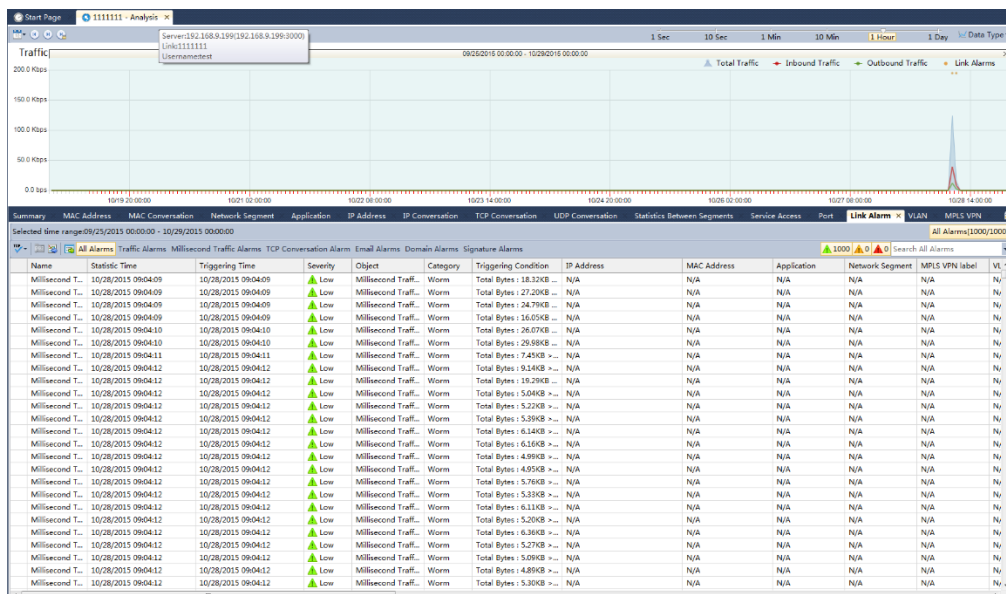
When configuring a network link, you can define alarms as required, and once the alarms are triggered, alarm logs are generated for them.

To view the alarm logs,

1. Double-click the **Alarm** node under the network link.



Then the Alarms window appears to display all alarm logs, including link alarm logs and application alarm logs.



The Alarms window includes an Alarms trend chart on the top pane and several alarm views on the bottom pane. The Alarms trend chart displays all triggered alarms in a trend chart; and the alarm views are sorted according to alarm types.

Application Monitor

Besides monitoring a network link, nChronos can also monitor a single application independently, and the application could be any custom application. This chapter describes how to monitor an application, and the elements on the application monitor window.

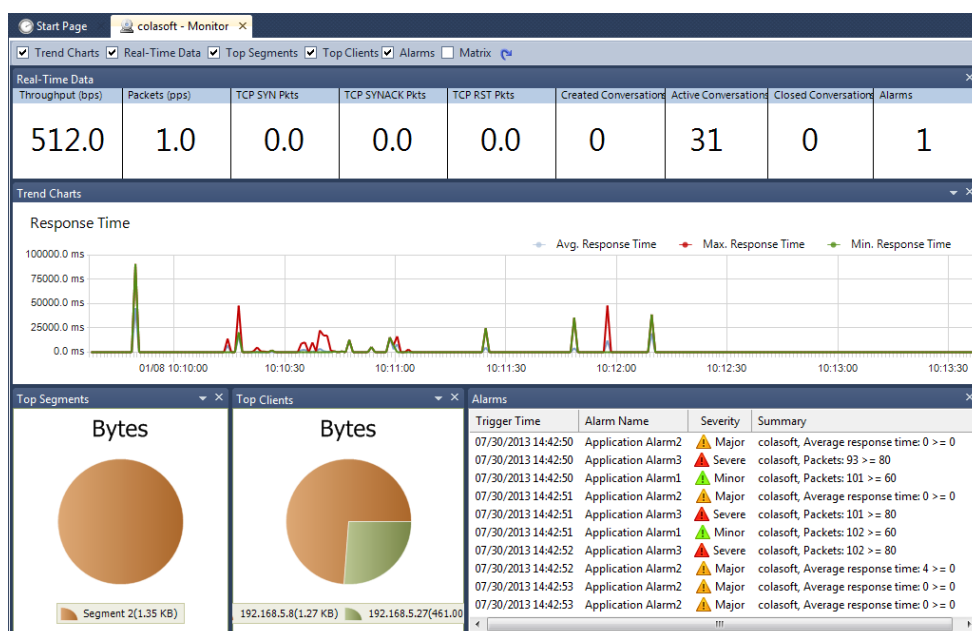
Monitoring an application

To monitor an application,

1. Select the checkboxes **Enable** and **Performance Analysis** on the **Analysis Settings** tab of the **Link Properties** dialog box.

Once an application is monitored, it will display under the network link on the Server Explorer.

Right-click the application under the network link and select Monitor, and then an application monitor window appears to show the real-time status of the application:



The application monitor window looks very like the link monitoring window and includes six panes:

Trend Charts

Real-Time Data

Top Segments

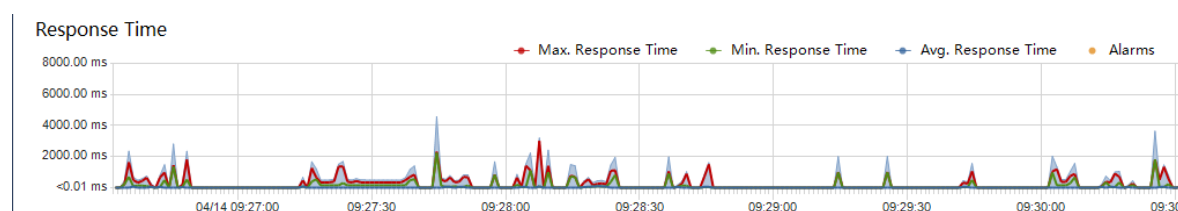
Top Hosts

Alarms

Matrix

The Trend Charts pane

The Trend Charts pane shows as the following figure:



There are several trend charts on the Trend Charts pane:

Traffic: The traffic trend charts for the application, including Total Bytes, Uplink Bytes, Downlink Bytes, and Alarms.

Packets: The packets trend charts for the application, Total Packets, Uplink Pkts, Downlink Pkts, and Alarms.

Response Time: The response time trend charts for the application, including Avg. Response Time, Max. Response Time, Min. Response Time, and Alarms.

Transactions: The TCP transactions trend charts for the application, including Total TCP Transactions, TCP Transaction Requests, TCP Transaction Responses, Good TCP Transactions, Normal TCP Transactions, Bad TCP Transactions, No Response TCP Transactions, and Alarms.

TCP Packets: The TCP packets trend charts for the application, including TCP SYN Pkts, TCP SYNACK Pkts, TCP RST Pkts, and Alarms.

Times When TCP window size is 0: The times when TCP window size is 0, including Server TCP Zero Window Count, Client TCP Zero Window Count and Alarms.

Connection Status: Includes Reset Connection Requests, Unresponsive Connection Requests, and Alarms.

Connection Time: Includes Average Connection Establish Time and Maximum Connection Establish Time.

TCP Conversations: The TCP conversation trend charts for the application, including Created Conversations, Closed Conversations, Active Conversations, and Alarms.

Packet Size Distribution: The packet size distribution for the application, including Total Packets trend chart, and trend charts with packet length in some ranges.

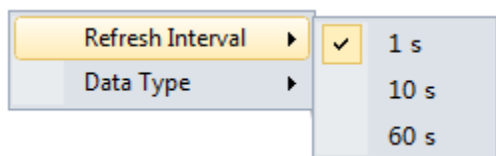
Right-click on the trend charts, you can choose which charts to show and can set the time window of the charts.

The Real-Time Data pane

The Real-Time Data pane displays the real-time data of the application, including throughput, packets, TCP SYN packets, TCP SYNACK packets, TCP RST packets, new conversations, active conversations, closed conversations, and alarm quantity:

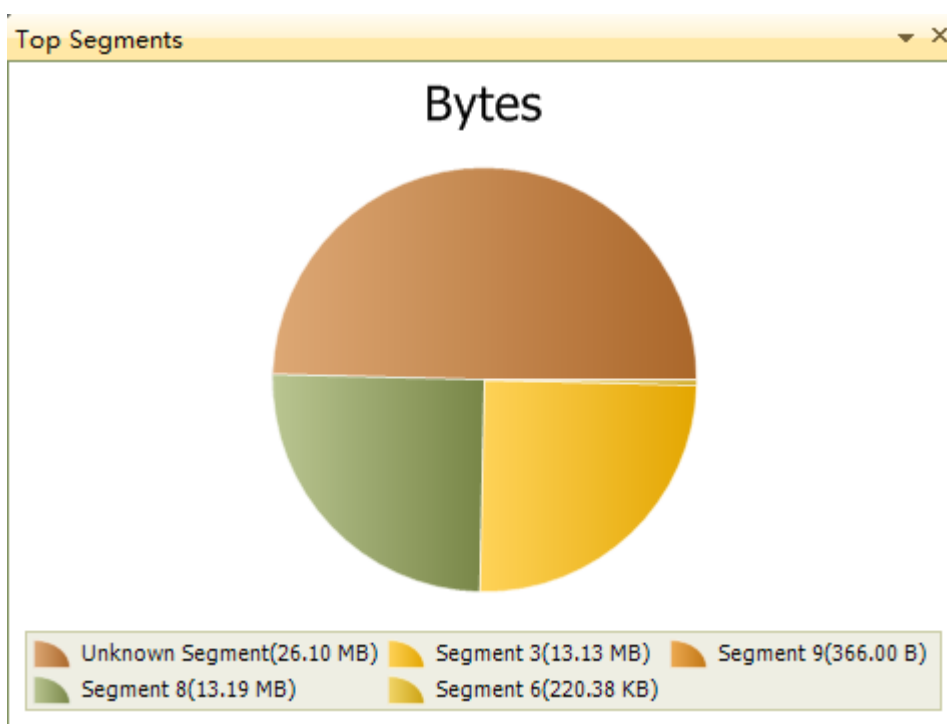
Real-Time Data								
Throughput (Kbps)	Packets (pps)	TCP SYN Pkts	TCP SYNACK Pkts	TCP RST Pkts	Created Conversations	Active Conversations	Closed Conversations	Alarms
73.1	13.0	2.0	2.0	0.0	2	1	1	0

You can set the refresh interval for the Real-Time Data pane by right-clicking in it.

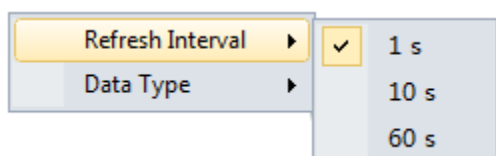


The Top Segments pane

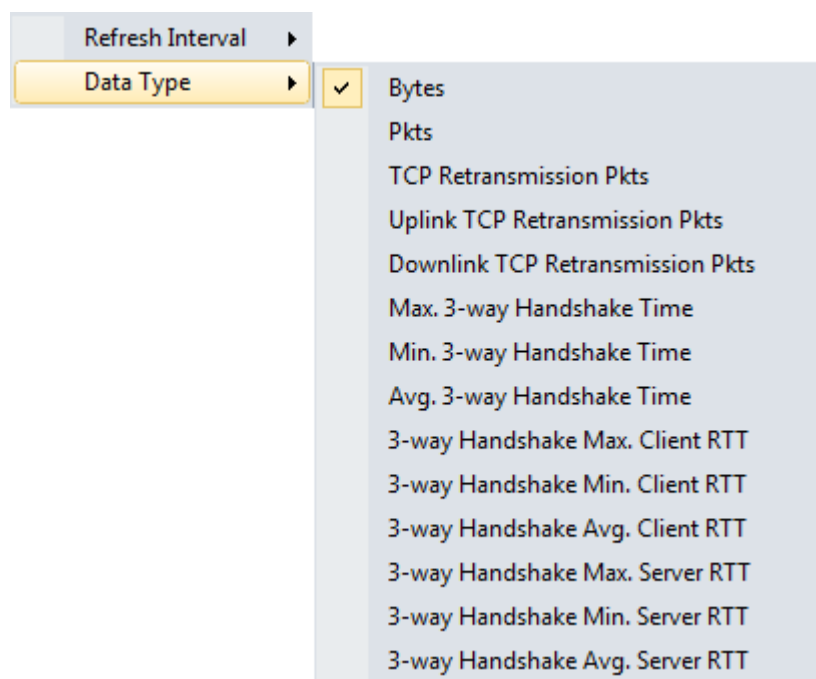
The Top Segments pane displays the top network segments of the application in a pie chart. The segments as well as their real-time figures are displayed just below the pie chart. The segments are defined when you configuring the network settings.



You can set the refresh interval for the Top Segments pane by right-clicking in it.

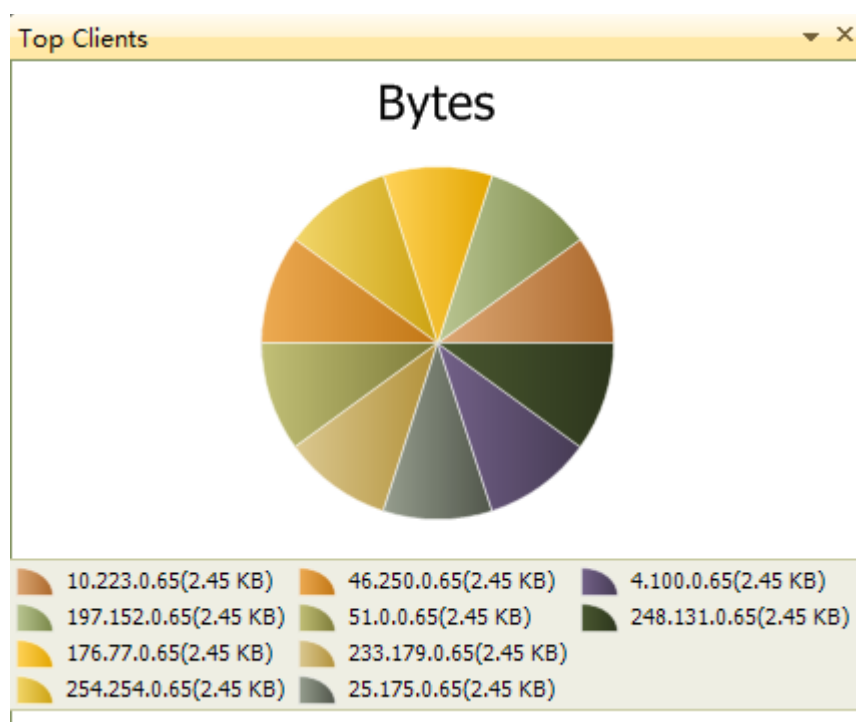


Furthermore, you can display the top segments according to other data type just by right-clicking in it.

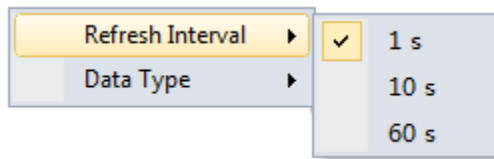


The Top Clients pane

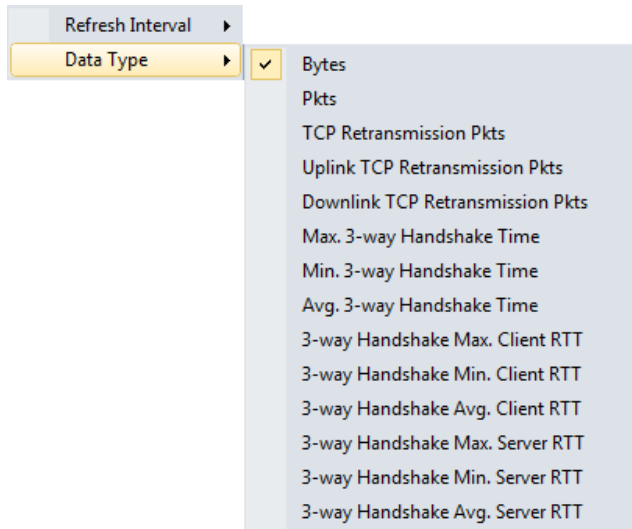
The Top Clients pane displays the top clients of the application in a pie chart. The clients as well as their real-time figures are displayed just below the pie chart.



You can set the refresh interval for the Top Clients pane by right-clicking in it.



Furthermore, you can display the top clients according to other data type just by right-clicking in it.



The Alarms pane

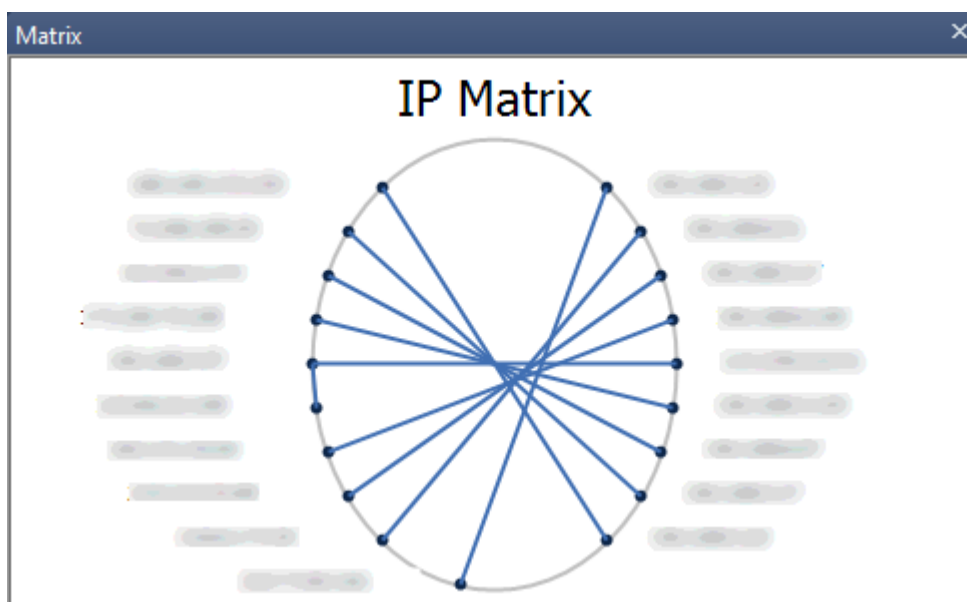
The Alarms pane lists all application alarms triggered in the one second, including trigger time, alarm category, alarm object, alarm name, alarm severity, and trigger condition.

The following figure shows the Alarms pane on the application monitor window.

Alarms					
Trigger Time	Category	Object	Alarm Name	Severity	Summary
07/30/2013 14:41:45	Example	Monitored application	Application Alarm1	Minor	colasoft, Packets: 87 >= 60
07/30/2013 14:41:46	Example	Monitored application	Application Alarm2	Major	colasoft, Average response time: 0 >= 0
07/30/2013 14:41:47	Example	Monitored application	Application Alarm3	Severe	colasoft, Packets: 87 >= 80
07/30/2013 14:41:48	Example	Monitored application	Application Alarm1	Minor	colasoft, Packets: 84 >= 60
07/30/2013 14:41:49	Example	Monitored application	Application Alarm2	Major	colasoft, Average response time: 0 >= 0
07/30/2013 14:41:49	Example	Monitored application	Application Alarm3	Severe	colasoft, Packets: 84 >= 80
07/30/2013 14:41:50	Example	Monitored application	Application Alarm1	Minor	colasoft, Packets: 73 >= 60
07/30/2013 14:41:50	Example	Monitored application	Application Alarm2	Major	colasoft, Average response time: 7 >= 0
07/30/2013 14:41:51	Example	Monitored application	Application Alarm2	Major	colasoft, Average response time: 0 >= 0
07/30/2013 14:41:51	Example	Monitored application	Application Alarm2	Major	colasoft, Average response time: 0 >= 0

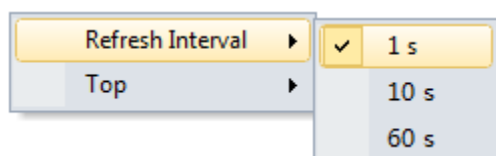
The Matrix pane

The Matrix pane shows the communication of the application in peer map.

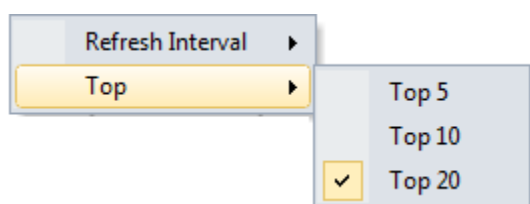


Move your mouse over one node, it will display the transmitted packets and bytes as well as received packets and bytes of the node, and display the peer nodes in highlight.

You can select the refresh interval of the matrix by right-clicking the matrix and then selecting the appropriate interval.



In addition, you can also set the top number for the matrix.



Analyzing Applications

Besides analyzing the whole network link, you can also analyze a specific application independently, which provides a separate window to display the clients, the servers, the segments, the conversations, and the alarms of the applications. Furthermore, you can retrospectively analyze an application to view its history data.

Analyzing the performance of an application

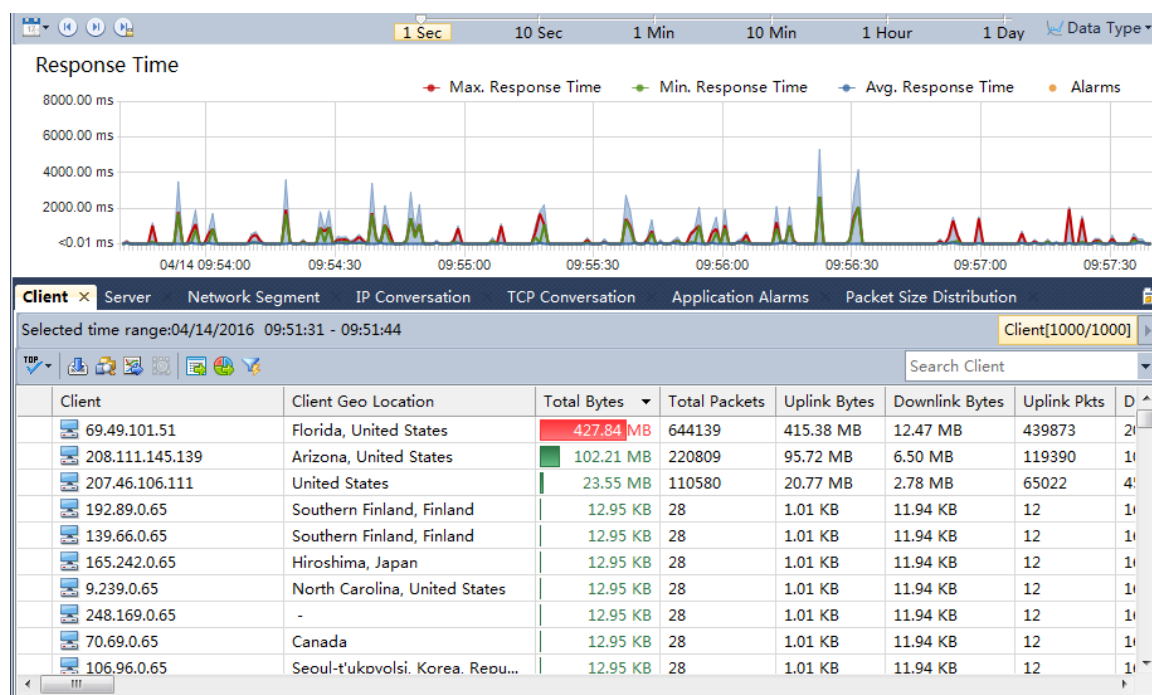
To analyze the performance of an application independently,

1. Select the checkboxes **Enable** and **Performance Analysis** on the **Analysis Settings** tab of the **Link Properties** dialog box.

Once an application is monitored, it will display under the network link on the Server Explorer.

Double-click the application under the network link, and then a performance analysis window appears to show the traffic data of the application.

The performance analysis window looks very like the Link Analysis window and includes a Time Window as well as six analysis views, like the following figure:



The Time Window is just like that in the Link Analysis window.

Trend charts for application performance analysis

The trend charts in the Time Window include:

Traffic: The traffic trend charts for the application, including Total Bytes, Uplink Bytes, Downlink Bytes, and Alarms.

Packets: The packets trend charts for the application, Total Packets, Uplink Pkts, Downlink Pkts, and Alarms.

Response Time: The response time trend charts for the application, including Avg. Response Time, Max. Response Time, Min. Response Time, and Alarms.

Transactions: The TCP transactions trend charts for the application, including Total TCP Transactions, TCP Transaction Requests, TCP Transaction Responses, Good TCP Transactions, Normal TCP Transactions, Bad TCP Transactions, No Response TCP Transactions, and Alarms.

TCP Packets: The TCP packets trend charts for the application, including TCP SYN Pkts, TCP SYNACK Pkts, TCP RST Pkts, and Alarms.

Times When TCP window size is 0: The times when TCP window size is 0, including Server TCP Zero Window Count, Client TCP Zero Window Count and Alarms.

Connection Status: Includes Reset Connection Requests, Unresponsive Connection Requests, and Alarms.

Connection Time: Includes Average Connection Establish Time and Maximum Connection Establish Time.

TCP Conversations: The TCP conversation trend charts for the application, including Created Conversations, Closed Conversations, Active Conversations, and Alarms.

Packet Size Distribution: The packet size distribution for the application, including Total Packets trend chart, and trend charts with packet length in some ranges.

Performance analysis views

When analyzing the performance of a specified application, the program shows an independent window to present the statistics and analysis data for the application. The independent window is very like the Link Analysis window and includes a Time Window containing several trend charts and multiple analysis views.


The Client view

The **Client** view for application analysis provides the statistics and analysis data of the traffic according to the IP addresses of the clients of the application.

Viewing client statistics

By default, the Client view displays the traffic of the application according to the IP address of the client of the application, as well as the geographic location of the client, bytes, packets, sessions, TCP packets and response time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

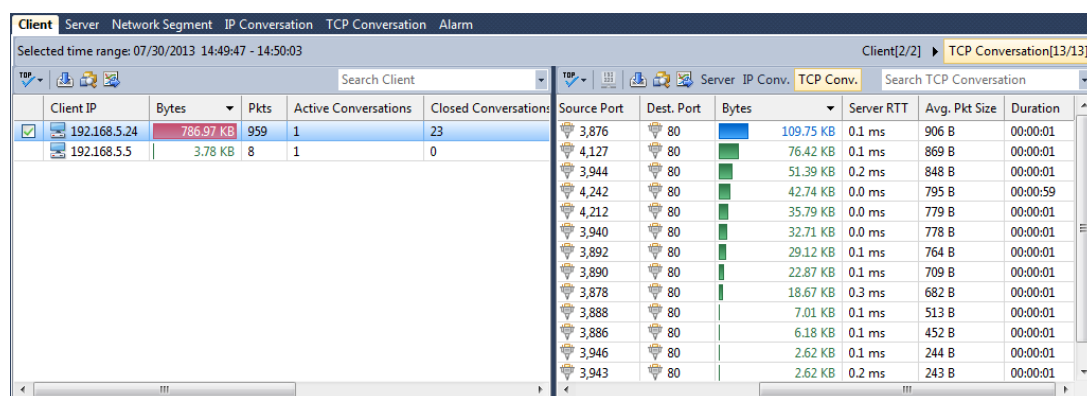
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of clients on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Drilling down a client

You can drill down any objects on the Client view for more detailed information. To drill an object, right-click the client, then click Drill Down and select the appropriate drilldown object. Next, you will see that a drilldown window slides out.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



The screenshot shows the Colasoft network analysis software interface. The main window displays the 'Client' view with a table of client statistics. A drilldown window for 'TCP Conversation' is open on the right, showing a detailed list of TCP connections.

Client IP	Bytes	Pkts	Active Conversations	Closed Conversations
192.168.5.24	786.97 KB	959	1	23
192.168.5.5	3.78 KB	8	1	0

Source Port	Dest. Port	Bytes	Server RTT	Avg. Pkt Size	Duration
3,876	80	109.75 KB	0.1 ms	906 B	00:00:01
4,127	80	76.42 KB	0.1 ms	869 B	00:00:01
3,944	80	51.39 KB	0.2 ms	848 B	00:00:01
4,242	80	42.74 KB	0.0 ms	795 B	00:00:59
4,212	80	35.79 KB	0.0 ms	779 B	00:00:01
3,940	80	32.71 KB	0.0 ms	778 B	00:00:01
3,892	80	29.12 KB	0.1 ms	764 B	00:00:01
3,890	80	22.87 KB	0.1 ms	709 B	00:00:01
3,878	80	18.67 KB	0.3 ms	682 B	00:00:01
3,888	80	7.01 KB	0.1 ms	513 B	00:00:01
3,886	80	6.18 KB	0.1 ms	452 B	00:00:01
3,946	80	2.62 KB	0.1 ms	244 B	00:00:01
3,943	80	2.62 KB	0.2 ms	243 B	00:00:01

To close a drilldown window, just deselect the drilled objects.

Searching the Client view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Client view will only display the items having the keyword.


The Server view

The Server view for application analysis provides the statistics and analysis data of the traffic for the application according to the IP addresses of the servers of the application.

Viewing server statistics

By default, the Server view displays the traffic of the application according to the IP address of the server of the application, as well as bytes, packets, sessions, TCP packets and response time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

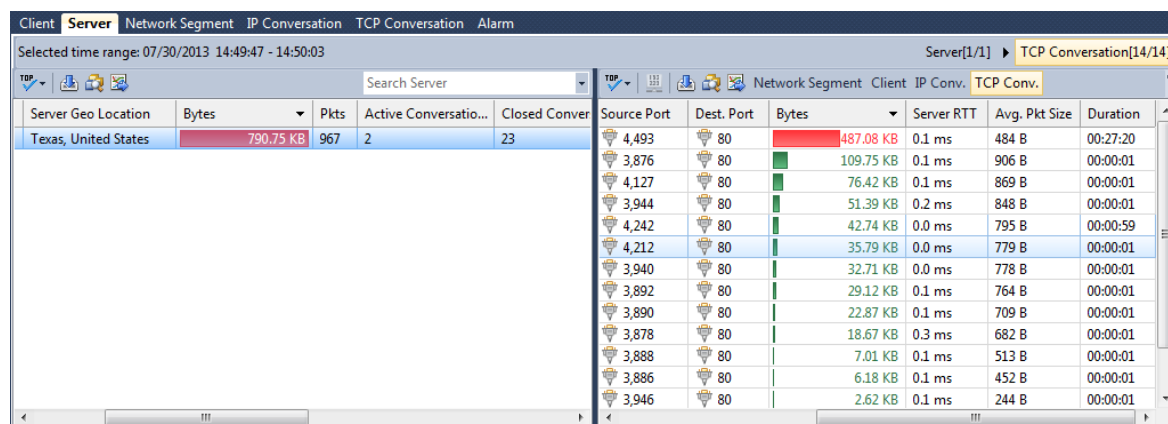
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of servers on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Drilling down a server

You can drill down a server for more detailed information. To drill a server, right-click the client, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



Server Geo Location	Bytes	Pkts	Active Conversation...	Closed Conversation...	Source Port	Dest. Port	Bytes	Server RTT	Avg. Pkt Size	Duration
Texas, United States	790.75 KB	967	2	23	4,493	80	487.08 KB	0.1 ms	484 B	00:27:20
					3,876	80	109.75 KB	0.1 ms	906 B	00:00:01
					4,127	80	76.42 KB	0.1 ms	869 B	00:00:01
					3,944	80	51.39 KB	0.2 ms	848 B	00:00:01
					4,242	80	42.74 KB	0.0 ms	795 B	00:00:59
					4,212	80	35.79 KB	0.0 ms	779 B	00:00:01
					3,940	80	32.71 KB	0.0 ms	778 B	00:00:01
					3,892	80	29.12 KB	0.1 ms	764 B	00:00:01
					3,890	80	22.87 KB	0.1 ms	709 B	00:00:01
					3,878	80	18.67 KB	0.3 ms	682 B	00:00:01
					3,888	80	7.01 KB	0.1 ms	513 B	00:00:01
					3,886	80	6.18 KB	0.1 ms	452 B	00:00:01
					3,946	80	2.62 KB	0.1 ms	244 B	00:00:01

To close a drilldown window, just deselect the drilled objects.

Searching the Server view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Server view will only display the items having the keyword.


The Network Segment view

The **Network Segment** view for application analysis provides the statistics and analysis data of the traffic according to the network segments of the application, which network segments are defined when setting the network link.

Viewing segment statistics

By default, the Network Segment view displays the traffic of the application according to the network segment of the application, as well as bytes, packets, sessions, TCP packets and response time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

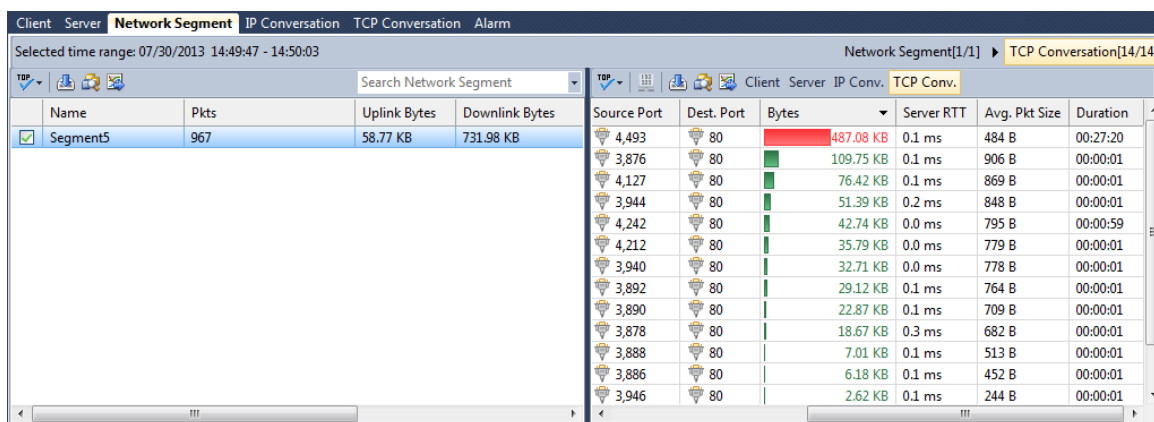
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of network segments on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Drilling down a segment

You can drill down a network segment for more detailed information. To drill a network segment, right-click the client, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Searching the Network Segment view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Network Segment view will only display the items having the keyword.


The IP Conversation view

The **IP Conversation** view for application analysis provides the statistics and analysis data of the traffic for the application according to IP conversations of the application.

Viewing IP conversation statistics

The IP Conversation view displays the traffic of the application according to client IP, server IP, bytes, packets, TCP packets, response time, and three-way handshake time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of segments on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Drilling down an IP conversation

You can drill down an IP conversation for more detailed information. To drill an IP conversation, right-click the IP conversation, then click Drill Down and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click Drill Down to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back.

To close a drilldown window, just deselect the drilled objects.

Searching the IP Conversation view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the IP Conversation view will only display the items having the keyword.


The TCP Conversation view

The TCP Conversation view for application analysis provides the statistics and analysis data of the traffic for the application according to TCP conversations of the application.

Viewing TCP conversation statistics

The TCP Conversation view displays the traffic of the application according to port number, bytes, packets, round-trip time, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

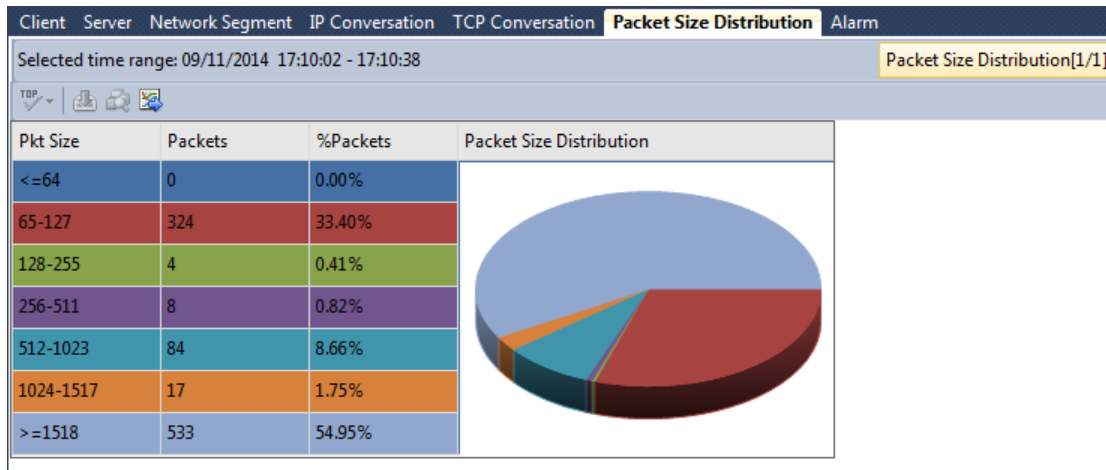
When there are a lot of segments on the view, you can click  to display only the top number of items, which are displayed according to the value of the Bytes column.

Searching the TCP Conversation view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the TCP Conversation view will only display the items having the keyword.

The Packet Size Distribution view

The Packet Size Distribution view calculates the packet size distribution for the application, showing as follows:



The Application Alarms view

The Application Alarms view for application analysis provides the logs of all application alarms. All these application alarms are defined when configuring the link properties.

Viewing alarm logs

The Application Alarms view displays the alarm logs according to alarm types.

The **All Alarms** tab lists the logs of all triggered application alarms.

The **Application Alarm** tab lists the logs of all triggered application alarms which are defined taking monitored applications as the alarm object.

The **Client Alarm** tab lists the logs of all triggered client alarms which are defined taking clients as the alarm object.


The **Server Alarm** tab lists the logs of all server alarms which are defined taking a single server or servers as the alarm object.

The **Segment Alarm** tab lists the logs of all triggered segment alarms which are defined taking network segments as the alarm object.

The **IP Conversation Alarm** tab lists the logs of all triggered IP conversation alarms which are defined taking IP conversation as the alarm object.

The **TCP Conversation Alarm** tab lists the logs of all triggered TCP conversation alarms which are defined taking TCP conversations as the alarm object.

All alarm logs are listed with trigger time, alarm category, alarm name, severity, and trigger condition. Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of alarm logs on the view, you can click  to display only the top number of items, which are displayed according to trigger time.

Searching the Alarm view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then it will only display the items having the keyword.

Analyzing Transactions

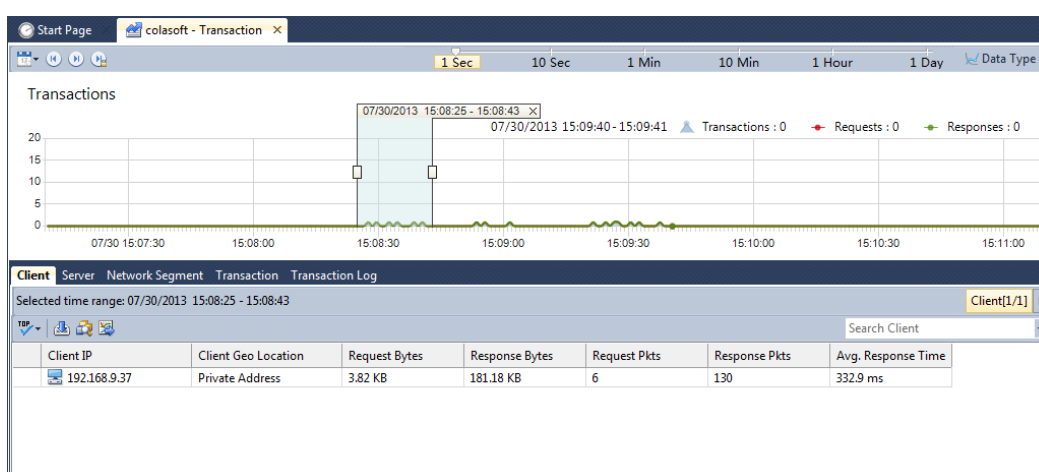
To analyze the transactions of an application,

1. Select the checkboxes **Enable** and **Transaction Analysis** on the **Analysis Settings** tab of the **Link Properties** dialog box.

Click **OK** on the **Link Properties** dialog box. Then the application displays under the node Application **Transaction Analysis** of that network link on the **Server Explorer**.

Under the node **Application Transaction Analysis**, double-click the **application**, and then a transaction analysis window appears to show the transaction data of the application.

The transaction analysis window looks very like the **Link Analysis** window and includes a Time Window as well as five views, as the following figure:



The Time Window is just like that in the Link Analysis window.

The trend charts in the Time Window include:

Transactions: The trend charts of the transactions which are defined by users based on the application. Consists of the Transactions trend chart, the Requests trend chart which indicates the trend chart for transaction requests, the Responses trend chart which indicates the trend chart for transaction response, and the Alarms trend chart. One transaction may be achieved by multiple TCP conversations.

Transaction Response Time: The trend charts of transaction processing time. Consists of the Avg. Response Time trend chart, the Min. Response Time trend chart, the Max. Response Time trend chart, and the Alarms trend chart.

Transaction Status: The trend charts of transaction status. Consists of the Transactions trend chart, the Successes trend chart, the Failures trend chart, and the Alarms trend chart.


The Transaction view

The Transaction view provides the transaction statistics for the application, like the following figure:

Client Server Network Segment Transaction Transaction Log


Selected time range: 07/30/2013 15:08:25 - 15:08:43

Transaction[3/3]

TDP 

Search Transaction



Transaction	Request Bytes	Response Bytes	Request Pkts	Response Pkts	Avg. Response Time	Avg. Request Transfer Time
products	1.22 KB	67.02 KB	2	48	331.9 ms	161.1 ms
purchase	1.30 KB	60.22 KB	2	44	337.5 ms	162.8 ms
support	1.29 KB	53.94 KB	2	38	329.3 ms	161.2 ms

 **Note** All transactions must be defined on the **Analysis Settings** tab of the Link Properties dialog box; or else, there will be no statistics on this view.

Viewing Transaction statistics

The Transaction view displays the transactions over the network in the selected time range according to transaction name, the name of the application that the transaction belongs to, the quantity of the transaction, the packets and the bytes for the transaction. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

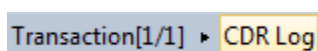
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of transactions on the Transaction view, you can click  to display only the top number of items, which are displayed according to the name of the transactions. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a transaction


When you view the transaction, you can drill down it for detailed transaction log information. To drill a transaction, double-click the transaction, and then you can see that a drilldown window slides out. You can only drill down a transaction for transaction logs of it.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Searching the Transaction view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box  on the top-right corner, and then the Transaction view will only display the items having the keyword.



The Client view

The Client view for transaction analysis provides the statistics and analysis data of the traffic for the transactions of analyzed application according to the IP addresses of the clients of the application.

Viewing client statistics

By default, the Client view displays the traffic of the application according to the IP address of the client of the application, as well as the geographic location of the client, bytes, packets, sessions, TCP packets and response time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

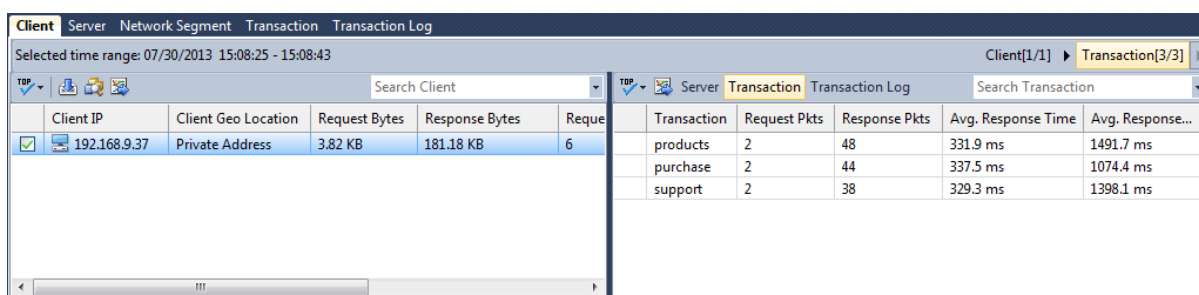
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of transactions on the Transaction view, you can click  to display only the top number of items, which are displayed according to the name of the transactions. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a client

You can drill down a client for more detailed information. To drill a client, right-click the client, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Searching the Client view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Client view will only display the items having the keyword.



The Server view

The Server view for transaction analysis provides the statistics and analysis data of the traffic for the transactions of analyzed application according to the IP addresses of the servers of the application.

Viewing server statistics

By default, the Server view displays the traffic of the application according to the IP address of the server of the application, as well as bytes, packets, sessions, TCP packets and response time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

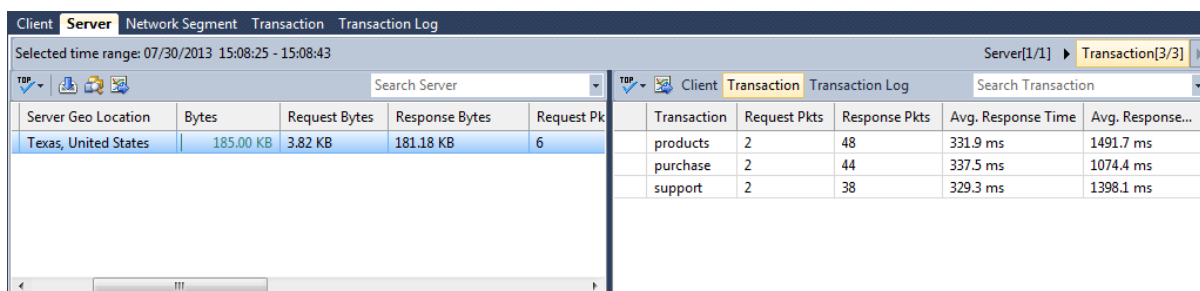
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of transactions on the Transaction view, you can click  to display only the top number of items, which are displayed according to the name of the transactions. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a server

You can drill down a server for more detailed information. To drill a server, right-click the client, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



The screenshot shows the Colasoft NetworkMiner interface with two main panels. The left panel is the 'Server' view, and the right panel is the 'Transaction' view.

Server View:

Server Geo Location	Bytes	Request Bytes	Response Bytes	Request Pk
Texas, United States	185.00 KB	3.82 KB	181.18 KB	6

Transaction View:

Transaction	Request Pkts	Response Pkts	Avg. Response Time	Avg. Response...
products	2	48	331.9 ms	1491.7 ms
purchase	2	44	337.5 ms	1074.4 ms
support	2	38	329.3 ms	1398.1 ms

To close a drilldown window, just deselect the drilled objects.

Searching the Server view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Server view will only display the items having the keyword.



The Network Segment view

The Network Segment view for transaction analysis provides the statistics and analysis data of the traffic for the transactions of analyzed application according to the network segments of the application, which network segments are defined when setting the network link.

Viewing segment statistics

By default, the Network Segment view displays the traffic of the application according to the network segment of the application, as well as bytes, packets, sessions, TCP packets and response time. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

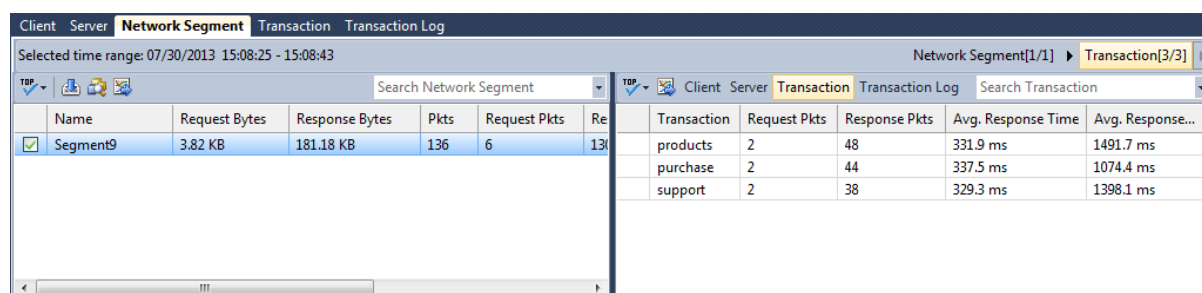
Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

When there are a lot of transactions on the Transaction view, you can click  to display only the top number of items, which are displayed according to the name of the transactions. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Drilling down a segment

You can drill down a network segment for more detailed information. To drill a network segment, right-click the client, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out. You can further right-click an object and click **Drill Down** to drill down more information.

The drilldown window always slides out from right to left. If you want to return back the primary view or other drilldown window, you can click the name of it on the right-top of the analysis view to go back, like the figure below:



To close a drilldown window, just deselect the drilled objects.

Searching the Network Segment view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Network Segment view will only display the items having the keyword.

The Transaction Log view

The Transaction Log view provides the logs of all transactions, with one transaction having one log, like the following figure:



Client	Server	Network Segment	Transaction	Transaction Log					
Selected time range: 07/30/2013 15:33:00 - 15:33:03					Transaction Log[1/1]				
TOP					Search Transaction Log				
Transaction	Server Port	Server Geo Location	Client IP	Client Port	Request At	Response At	Response Time	Req	
support	80	Texas, United States	192.168.9.37	1,289	07/30/2013 15:32:54.950532	07/30/2013 15:32:55.183805	233.3 ms	631.	

Note All transactions must be defined on the **Analysis Settings** tab of the Link Properties dialog box; or else, there will be no statistics on this view.

Viewing transaction logs

The Transaction Log view displays the logs of all transactions over the network in the selected time range according to transaction name, the application that the transaction belongs to, the IP address of the host that initiates the transaction, the IP address of the host that responds the transaction, the packets and the bytes for the transaction. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

Furthermore, click the column name on the column header, and you can sort the statistics according to the column.

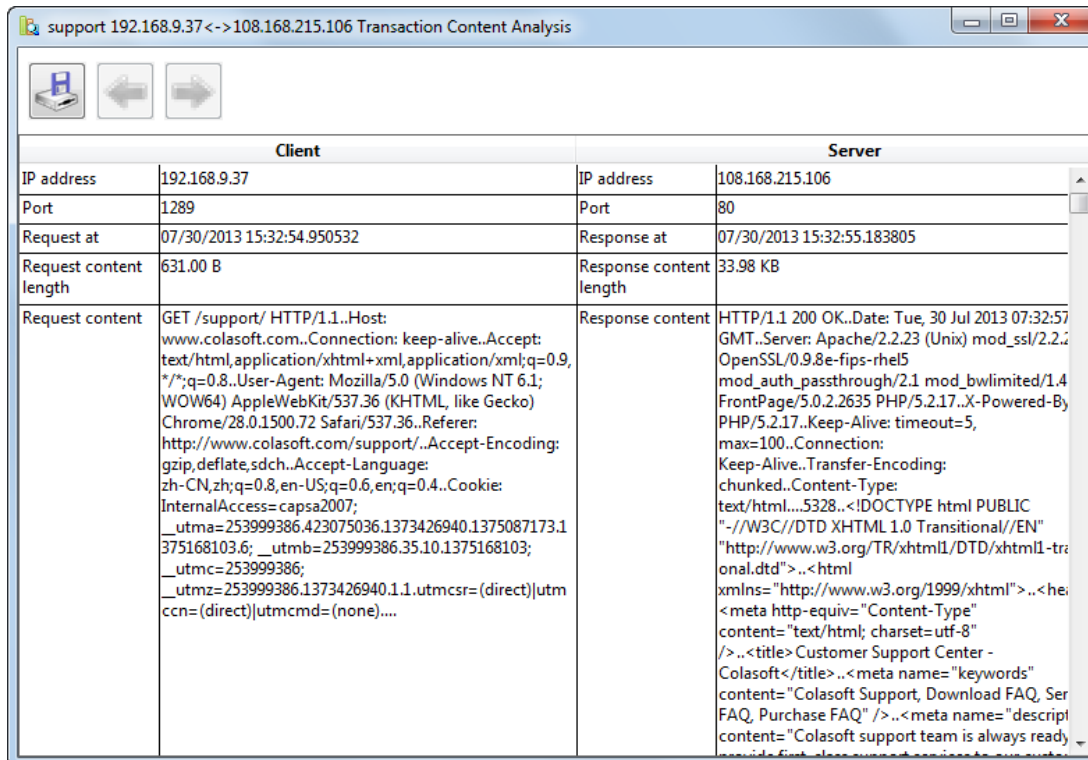
When there are a lot of transactions on the Transaction view, you can click  to display only the top number of items, which are displayed according to the name of the transactions. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Searching the Transaction Log view

When there are lots of statistics on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box on the top-right corner, and then the Alarm view will only display the items having the keyword.

Analyzing transaction content



On the Transaction Log view, select one or more transaction logs, right-click and then click Transaction Analysis, a **Transaction Content Analysis** window shows up to display the details of the transaction:



Client		Server	
IP address	192.168.9.37	IP address	108.168.215.106
Port	1289	Port	80
Request at	07/30/2013 15:32:54.950532	Response at	07/30/2013 15:32:55.183805
Request content length	631.00 B	Response content length	33.98 KB
Request content	GET /support/ HTTP/1.1..Host: www.colasoft.com..Connection: keep-alive..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.72 Safari/537.36..Referer: http://www.colasoft.com/support/..Accept-Encoding: gzip,deflate,sdch..Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.6,en;q=0.4..Cookie: InternalAccess=capsa2007; __utma=253999386.423075036.1373426940.1375087173.1375168103.6; __utmb=253999386.35.10.1375168103; __utmc=253999386; __utmz=253999386.1373426940.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none)...	Response content	HTTP/1.1 200 OK..Date: Tue, 30 Jul 2013 07:32:57 GMT..Server: Apache/2.2.23 (Unix) mod_ssl/2.2.2 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.17..X-Powered-By: PHP/5.2.17..Keep-Alive: timeout=5, max=100..Connection: Keep-Alive..Transfer-Encoding: chunked..Content-Type: text/html...5328..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">...<html xmlns="http://www.w3.org/1999/xhtml">...<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" />...<title>Customer Support Center - Colasoft</title>...<meta name="keywords" content="Colasoft Support, Download FAQ, Ser FAQ, Purchase FAQ" />...<meta name="description" content="Colasoft support team is always ready to provide first-class support services to our customers..."</head>...<body>...</body></html>

The Transaction Content Analysis window displays the IP addresses and port numbers of the client and the server, the request and response time, the length of the request content and the response content, and the details of the request content and the response content.



When there are multiple transaction logs to be analyzed, you can click  or  to conveniently view related transaction content.

The Transaction Alarms view

The Transaction Alarms view for transaction analysis provides the logs of all transaction alarms. All these transaction alarms are defined when configuring the link properties.

Viewing alarm logs



The Alarm view displays the alarm logs according to alarm types.

The **All Transaction Alarms** tab lists the logs of all triggered transaction alarms.

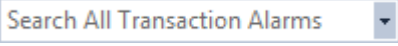
The **Transaction Log Alarm** tab lists the logs of all triggered transaction log alarms which are defined taking transaction log as the alarm object.

The **Transaction Statistics Alarm** tab lists the logs of all triggered transaction statistics alarms which are defined taking transaction statistics as the alarm object.

All alarm logs are listed with statistic time, trigger time, alarm category, alarm name, severity, trigger condition and so on. Furthermore, click the column name on the column header, and you can sort the alarm logs according to the column.

When there are a lot of alarm logs on the Transaction Alarms view, you can click  to display only the top number of items, which are displayed according to trigger time. If you want to display all the statistical items on this view, just click  and click **Show All Records**.

Searching the Transaction Alarms view

When there are lots of alarm logs on this view, you can use the display filter function to view the interested data. Enter the appropriate keyword in the search box  on the top-right corner, and then the Transaction Alarms view will only display the items having the keyword.

Common Information Query

This section describes how to query common information, including server information, network link configuration, user information, interface configuration, port configuration, alarm notification parameters, and audit logs.

Query server information

Server information includes product name, server version, server model, and authorization information. Authorization information includes active status, software & service time limit, and authorized users, service analysis of the maximum storage space, flow rate, the maximum number of network interface, the console of the maximum number of network link, the number of connections, the maximum number of transaction analysis, console, console much analysis free activation, VoIP monitoring.

The steps to query server information:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose Server Information. The Server Information page is displayed.
3. Query server information, as shown in the following figure:

Product Information	
Name:	Colasoft nChronos Server
Version:	
Model:	Standard Evaluation

License Information	
Activation Status:	Activated
Serial Number:	<div></div> <button>Reactivate</button>
Software Period:	Limited
Maintenance Period:	12/16/2021 06:00:00 - 02/03/2023 05:59:59
Licensed to:	
Storage Capacity:	32768GB
Maximum Analysis Throughput:	3000Mbps
Maximum Capture Interfaces:	4
Maximum Network Links:	4
Concurrent Connections to Server:	8
Maximum Analyzed Transactions:	40
Console, Multi-Segment Analysis:	Enabled
Console, Free-activate:	Enabled
VoIP Monitoring:	Enabled

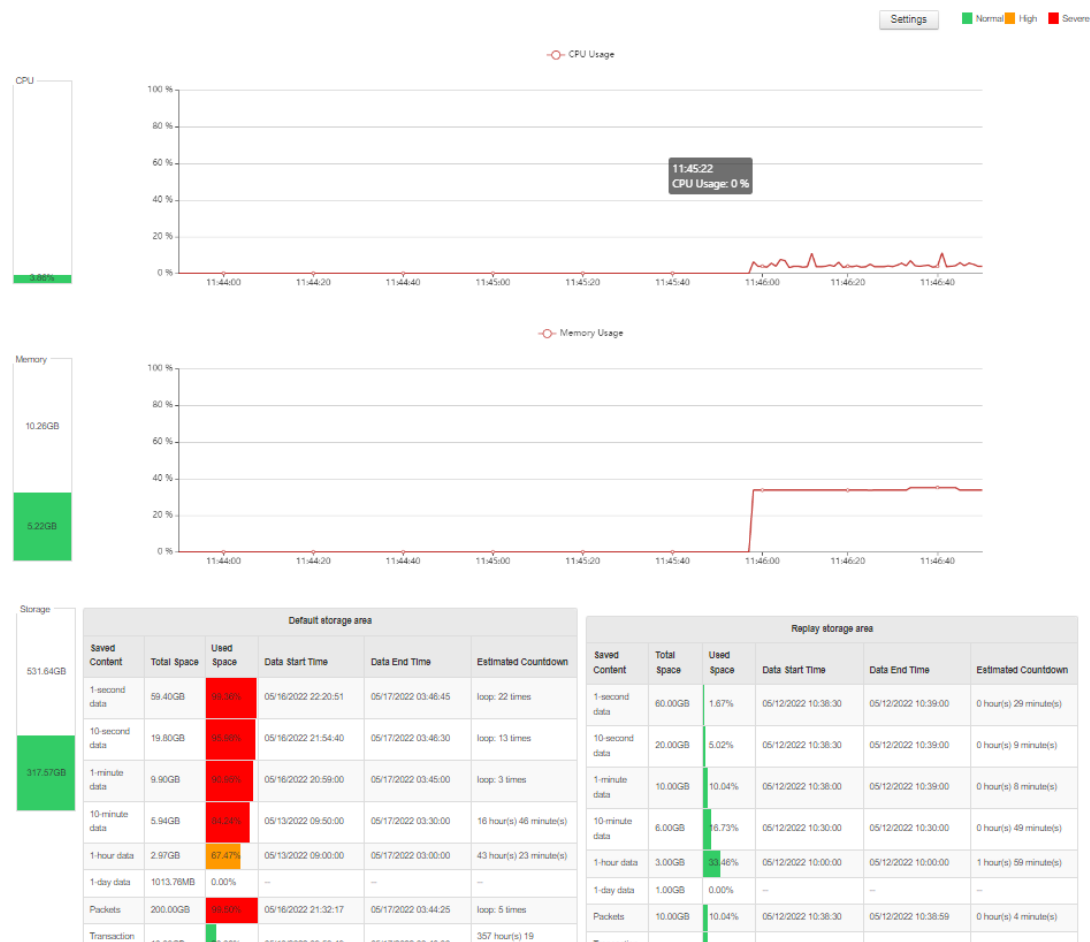
Query server running status

The server running status includes the start time, running time, CPU usage, memory, available memory, memory usage, disk capacity configuration, remaining disk capacity, and disk capacity usage percentage.

To query the running status of a server, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose Server Status. The Server Status page is displayed.
3. Query the running status of the server, as shown in the following figure:

Server Status



Query link status

The network link information includes the link name, link type, number of interfaces, and link status. You can query the network link information on the console or server.

To query network link information on the console, perform the following steps:

1. Connect to the server through the console.

2. Select the network link that you want to view and view the network link information in the server Manager window, as shown in the following figure:

Link Name: demo2
Link Type: Switch (bidirectional mirroring)
Link Status: Running

Capture Filters: Accept: 0, Reject: 0
Storage Filters: Accept: 0, Reject: 0
Custom Apps: 61
Alarms: 81

Properties

To query network link information on the server, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose Link Configuration. The Link Configuration page is displayed.
3. Query network link information, as shown in the following figure:

Link Configuration

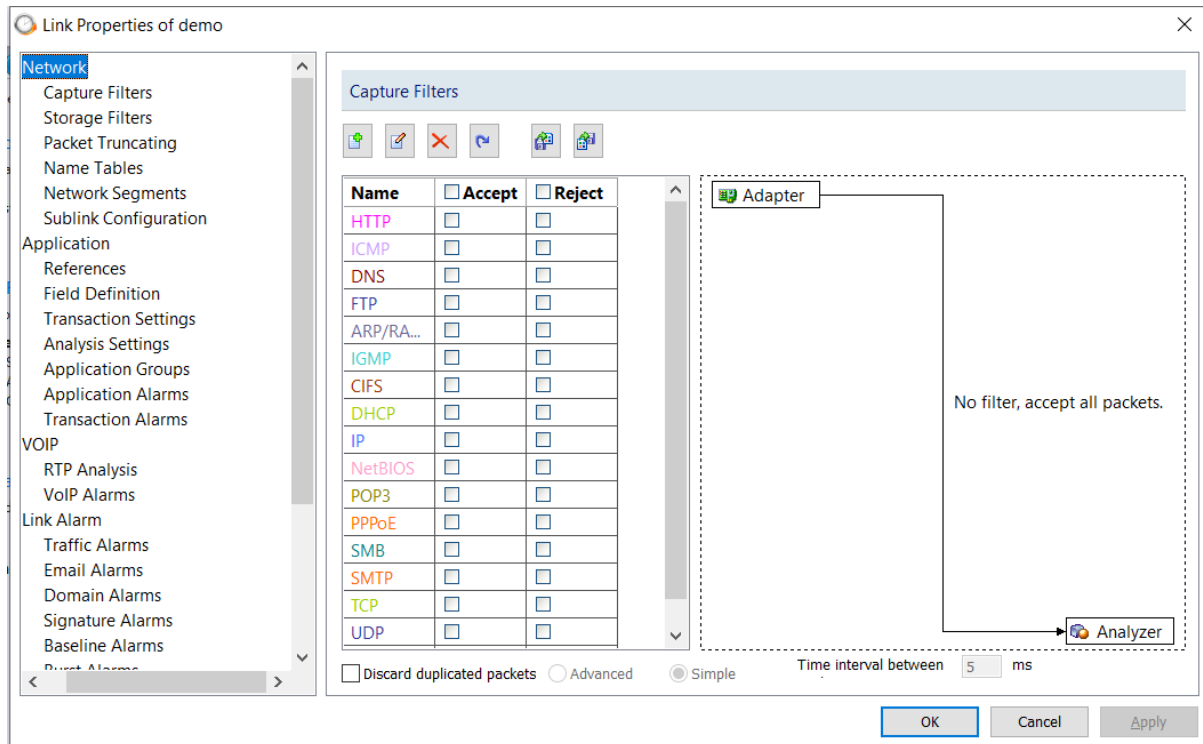
Network Link ID	Name	Type	Capture Interface Count	bps	Status	Operation		
8	demo	Switch (bidirectional traffic mirroring)	1	0.000 bps	Stopped	Run	Edit	Delete
16	Replay	Replay Packets	0	0.000 bps	Stopped	Run	Edit	Delete
17	demo2	Switch (bidirectional traffic mirroring)	1	0.000 bps	Running	Stop	Edit	Delete

Query network link configuration information

Network link configuration information includes filters, custom applications, alerts, inbound and outbound traffic statistics, and inbound and outbound utilization statistics.

To query network link configuration information, perform the following steps:

1. Connect to the server through the console.
2. Select the network link that you want to view and view the configuration of the network link in the browser window, as shown in the following figure:



Query user information

The user information includes the user name, user type, user status, creation time, remarks, and operations that the current user can perform.

To query user information, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose User Management. The User Management page is displayed.
3. Query user information, as shown in the following figure:

User Management

No.	Username	Type	Authentication Type	Status	Date Created	Date Logged	Notes	Operation
1	admin@local	Administrator	Local Authentication	Online (Console, Browser)	07/02/2021 02:11:16	05/17/2022 06:05:03	Administrator	<button>Edit</button> <button>Delete</button> <button>Kick Out</button>
2		Administrator	Local Authentication	Offline	03/03/2022 01:57:40	-		<button>Edit</button> <button>Delete</button> <button>Kick Out</button>
3		Administrator(UPM)	UPM Authentication	Offline	05/17/2022 03:27:08	-		<button>Check</button> <button>Delete</button> <button>Kick Out</button>
4		Administrator(UPM)	UPM Authentication	Offline	11/28/2019 10:31:15	-		<button>Check</button> <button>Delete</button> <button>Kick Out</button>
5		Administrator(UPM)	UPM Authentication	Offline	05/18/2020 09:13:24	-		<button>Check</button> <button>Delete</button> <button>Kick Out</button>
6		User(UPM)	UPM Authentication	Offline	06/01/2020 16:44:42	-		<button>Check</button> <button>Delete</button> <button>Kick Out</button>
7		Administrator(UPM)	UPM Authentication	Offline	12/31/2020 17:46:21	-		<button>Check</button> <button>Delete</button> <button>Kick Out</button>
8		Administrator(UPM)	UPM Authentication	Offline	07/02/2021 11:35:39	-		<button>Check</button> <button>Delete</button> <button>Kick Out</button>

Query interface information

The interface information includes the interface name, interface status, connection speed, and interface type. If the interface type is Config Interface, you can query the name, IP address, mask, gateway address, and DNS server address of the config interface.

To query configuration interface information, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose Interface Settings. The Interface Settings page is displayed.
3. Query information about the interface, as shown in the following figure:

Interface Settings

Interface ID	PCI	Name	bps	Speed (Mbps)	Type	Transmission Medium	Identify IP Layer	Remarks	Operation
0	0000:01:00:0	enp1s0f0(0.0.0.0)	0.000 bps	1000	Capture interf	Ethernet	First Layer		<button>Edit</button>
1	0000:03:00:0	eno1(192.168.120.65)	138.457 Kbps	1000	Management i				<button>Edit</button>
2	0000:01:00:1	enp1s0f1(0.0.0.0)	0.000 bps	1000	Capture interf	Ethernet	First Layer		<button>Edit</button>
3	0000:02:00:0	enp2s0f0(0.0.0.0)	0.000 bps	Unknown	Capture interf	Ethernet	First Layer		<button>Edit</button>
4	0000:02:00:1	enp2s0f1(0.0.0.0)	0.000 bps	Unknown	Undefined				
5	0000:03:00:1	enc2(0.0.0.0)	0.000 bps	Unknown	Undefined				
6	0000:01:00:2	enp1s0f2(0.0.0.0)	0.000 bps	Unknown	Undefined				
7	0000:01:00:3	enp1s0f3(0.0.0.0)	0.000 bps	Unknown	Undefined				

4. If the interface type is Config Interface, click Edit to set the IP address of the management interface, as shown in the following figure:

Interface Configuration / Edit Interface

eno1 (192.168.120.65)

☒ IPv4

IP address: 192.168.120.65

IP mask: 255.255.255.0

Gateway address: 192.168.120.1

DNS server: 114.114.114.114

☐ IPv6

IP address:

Prefix length:

Gateway address:

DNS server:

OK

Cancel

Query storage configuration information


The storage configuration information includes retrospective analysis of the total storage space of the system, as well as the percentage of storage space occupied by statistics, packets, alert logs, and transaction logs.

To query storage Settings, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose Storage Settings, the page is displayed.
3. Query storage configuration information, as shown in the following figure:

Storage Settings

Disk Space

Disk Partition	Device Set	Total Space	Available Space	Storage Space Used	Storage Space Configured	Export Data Space	
default	/dev/mapper/centos-data	806GB	779GB	317GB	770GB	0GB	

[New disk partition](#)

Analysis Space

Storage Area	Storage Type	Disk Partition	Statistics Space	Packet Space	Transaction Logs Space	Alarm Logs Space	
Default storage area	Normal	default	111GB	200GB	10GB	10GB	
Replay storage area	Replay Storage	default	100GB	10GB	10GB	10GB	

[New Storage Area](#)

Query SMTP settings

The SMTP server is a mail sending server that complies with the SMTP protocol and is used to send or forward emails. Only when the SMTP server is correctly configured, the system can send alarms and reports to the email addresses of the specified recipients.

To query SMTP Settings, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose SMTP Settings. The SMTP Settings page is displayed.
3. Query the SMTP server parameter Settings, as shown in the following figure:

SMTP Settings

User Information

User Name:

Email Address:

Server Information

Email Server:

SSL Encryption: Port Number:

Login Information

User Name:

Password:

Query Alarm Sending Configuration Information

Alarm sending Settings include alarm recipient Settings and SYSLOG parameter Settings. When an alarm occurs in the system, the system automatically sends the alarm information to the specified mailbox by email and to the SYSLOG server by log.

To query alarm sending Settings, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.
2. In the navigation tree, choose Alarm Notification. The Alarm Notification page is displayed.
3. Query the settings of alarm sending parameters, as shown below:

Alarm Notification

☐ Email Notification

Email Subject:

Recipient Address:

Notification Interval: Range: 1-999 (minutes)

☒ Syslog Notification

Syslog Server Address:

Encode:

☒ Send every second

☐ Send every: Range: 1-999 (minutes)

Query report sending notification

Report sending Settings include report template Settings and report recipient address Settings.

To query report sending Settings, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator.


2. In the navigation tree, choose Report Notification. The Report Notification page is displayed.
3. Query the Settings of report sending parameters, as shown in the following figure:


Report Notification

Report Template

Company name:

Author:

Company logo: 



☒ Prefix:

☒ Show create time

Report format:

☒ Report recipient

E-mail address:

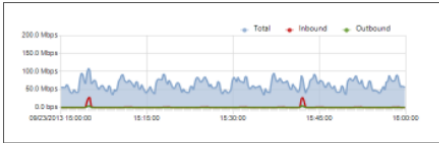
Colasoft

Test_Global report

Start time: 09/23/2013 14:00 Author: Administrator
End time: 09/23/2013 15:00 Create time: 09/23/2013 15:05:07
Report object: Global

Bandwidth: 1,000Mbps

Trend Chart



Query audit log information














Audit log information includes the log type, log time, user, and event. Audit logs help you query the operations performed by users in the retrospective analysis system.

To query audit logs, perform the following steps:

1. Log in to the Web configuration page of the server as an administrator or auditor.
2. In the navigation tree, choose Audit Logs. The Audit Logs page is displayed.
3. You can filter and download logs by log type or time range, as shown in the following figure:

Audit Log

Type Time - Content

No.	Type	Time	User	Initiator IP	Event
53731		05/17/2022 08:42:38	admin@local	192.168.16.23	Logged in from browser(192.168.16.23).
53730		05/17/2022 08:31:43	admin@local	192.168.16.23	The user automatically logged out of the system from browser 192.168.16.23 due to inactivity.
53729		05/17/2022 08:08:37	admin@local	192.168.16.23	Logged in from browser(192.168.16.23).
53728		05/17/2022 08:05:35	admin@local	192.168.16.163	The user automatically logged out of the system from browser 192.168.16.163 due to inactivity.
53727		05/17/2022 07:23:02	admin@local	192.168.16.23	The user automatically logged out of the system from browser 192.168.16.23 due to inactivity.
53726		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Enabled server account 'yexiaolin'.
53725		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Modified the name of the server account " to 'yexiaolin'.
53724		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Modified the type of server account 'yexiaolin' to 'Administrator'.
53723		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Modified the authentication method of server account 'yexiaolin' to 'UPM'.
53722		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Enabled server account 'test234'.
53721		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Modified the name of the server account " to 'test234'.
53720		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Modified the type of server account 'test234' to 'User'.
53719		05/17/2022 07:04:58	Colasoft UPM	192.168.120.66	Modified the authentication method of server account 'test234' to 'UPM'.

Query Information about multiple Processes

Customer can run the appClient command to perform multi-process operations.

Enter the appclient -h to view the help information of the command, as shown in the following figure:

```
[root@localhost ~]# appclient -h
Command usage of a process:
  appclient start xxx
  appclient stop xxx
  appclient restart xxx
Command usage of all processes:
  appclient start all
  appclient stop all
  appclient restart all
Command usage of a process group:
  appclient startgroup xxx
  appclient stopgroup xxx
  appclient restartgroup xxx
Command change user to run subprocess:
  appclient setuser xxx
Command usage of all processes information:
  appclient info
```

Appclient start/stop/restart

Command description: start, stop, or restart a process

appclient start/stop/restart all

Command description: start, stop, and restart all processes except the appinitd process

Appclient start/stop/restart

Command description: start, stop, or restart all processes in a process group

appclient setuser xxx

Command description: Specify the user to run other processes except csrssd and conf. The XXX command must be created in advance. This command is not used in general cases

appclient info

Command description: View the process status