Copyright © 2016 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 ................................................................. 6
   Installing nChronos Server ................................................................................ 6
   Installing nChronos Console ............................................................................. 7
   Activating nChronos Console ......................................................................... 8
   Uninstalling nChronos Console ...................................................................... 8
Server Configurations ......................................................................................... 9
   Logging Server from a browser ......................................................................... 9
   Storage Settings ................................................................................................. 10
   Interface Settings ............................................................................................. 11
      Defining interface type ................................................................................... 12
      Setting a Capture interface .......................................................................... 12
      Setting a Management interface .................................................................. 13
   Link Configuration ............................................................................................. 14
   Predefined Library ............................................................................................ 17
   Analysis Center ................................................................................................. 18
   SMTP Settings .................................................................................................. 19
   Alarm Notification ............................................................................................. 20
   Report Notification ........................................................................................... 21
   User Management ............................................................................................. 22
   Certificate .......................................................................................................... 23
   Security Policy .................................................................................................. 24
   Audit Log ........................................................................................................... 26
   Time Synchronization ....................................................................................... 27
   Server Information ............................................................................................ 28
   Server Management .......................................................................................... 29
Console User Interface ......................................................................................... 30
   Menu bar ............................................................................................................ 30
   Start Page .......................................................................................................... 32
Adding and Connecting nChronos Server..........................33
  Adding an nChronos Server ......................................33
  Connecting nChronos Server ...................................34
Configuring Network Link ............................................35
  Capture Filters .......................................................35
  Simple filter .......................................................37
  Advanced filter ....................................................40
  Storage Filters ......................................................42
  Name Tables ........................................................43
  Network Segments ..................................................45
  References ..........................................................47
  Field Definitions ...................................................48
  Analysis Settings ...................................................50
    Adding a standard application ...................................51
    Adding a web application .......................................52
    Adding a signature application ................................54
  Application Alarms ................................................55
    Adding an application alarm .....................................56
  Transaction Alarms ................................................57
  Traffic Alarms .......................................................59
    Adding a traffic alarm ..........................................60
  Millisecond Traffic Alarms .......................................61
  Email Alarms ........................................................63
  Domain Alarms .......................................................65
  Signature Alarms ...................................................67
  View Management ..................................................69
  Exporting network link properties .............................70
  Importing network link properties .............................70
Link Analysis ........................................................71
  Retrospectively analyzing a network link ......................71
  The Link Analysis window .......................................71
  Time Window .......................................................72
  Trend charts for link analysis ..................................74
  Analysis views .....................................................74
    Toolbar and pop-up menus ......................................75
    The Summary view ..............................................76
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>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nChronos Server</td>
<td>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.</td>
</tr>
<tr>
<td>nChronos Console</td>
<td>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.</td>
</tr>
<tr>
<td>Analysis object</td>
<td>The network elements, including protocols, addresses, ports, conversations, applications, hosts, network segments, target network, and other elements.</td>
</tr>
<tr>
<td>Capture interface</td>
<td>A network interface/port on nChronos Server, generally connected with the mirror port, for capturing the traffic of the target network.</td>
</tr>
<tr>
<td>Management interface</td>
<td>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.</td>
</tr>
<tr>
<td>Network link</td>
<td>A network object for nChronos to collect captured network traffic and to make statistics and analysis.</td>
</tr>
<tr>
<td>Back-in-time analysis</td>
<td>Also called as retrospective analysis. Provides detailed analysis presentation, data drilldown, new analysis and various statistics for historical network data.</td>
</tr>
<tr>
<td>Time Window</td>
<td>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. With the Time Window, network data of</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Filter</td>
<td>A group of user-defined data screening conditions or rules to accept the required data.</td>
</tr>
<tr>
<td>IP pair</td>
<td>A pair of IP addresses, without the identification of source address and destination address.</td>
</tr>
<tr>
<td>Drilldown</td>
<td>Level-by-level progressive analysis on selected network objects which include applications, network segments, addresses and conversations.</td>
</tr>
<tr>
<td>Expert Analyzer</td>
<td>A packet-level analysis system. Provides lots of statistics about selected network objects and original decoding information of the packets.</td>
</tr>
<tr>
<td>Web application</td>
<td>URL-based applications and defined by host name, IP address, port number and URL parameters.</td>
</tr>
<tr>
<td>Signature application</td>
<td>Applications defined by the feature codes of original data flow, in ASCII, Hex, UTF-8 or UTF-16.</td>
</tr>
<tr>
<td>Performance analysis</td>
<td>The analysis on the service performance of an application.</td>
</tr>
</tbody>
</table>
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 delivers 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:

![Architecture Diagram]

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:

![Diagram of nChronos deployment](image)

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.

![Diagram of simplified nChronos deployment](image)

**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 the installation of nChronos Server and installation, activation and uninstall of nChronos Console.

Installing nChronos Server

Follow the steps below to install CentOS 6.6 first, and then install nChronos Server.

Note: The installation of the OS will overwrite previous OS.

Prerequisites
1. ColaOS 6.6 installation file;
2. nChronos Server installation file: nchronoss-xxxx.rpm;
3. There should be two RAID partitions and mount data partition onto /data.

RAID Partitions
1. Start the machine, and press corresponding shortcut key according to the model of RAID card to go to the RAID card configuration interface.
   Taking PERC H710P for example, press CTRL+R to go to the RAID card configuration interface.
2. Press F2, choose Clear Config to delete the default configuration information.
3. Choose Create New VD, choose RAID-5, select all physical disks, use Tab key to switch, set VD Size of VD1 as recommended 60 G and VD Name as system, and then choose OK all the way.
4. Add VD2 on Disk Group, no need to choose physical disk again here, choose RAID-5 for RAID Level, choose the rest storage space, set VD Name as data, choose Advanced Settings, set Element Size as 1 MB, and choose OK.

5. Initialize the two partitions, select the partition, press F2, select Fast Init.

6. Restart the server after finishing the settings.

**Installing Operating System**
Install the operating system CentOS 6.6.

**Installing nChronos Server**

1. Use SSH tool to remotely connect to the server, put the installation file in the file folder “root”, as shown below:

```
-rw-r--r-- 1 root root 58477252 Nov 12 10:24 nchronos-5.0.2.2802.x86_64.rpm
```

2. Modify the privilege with the command: chmod +x nchronoss-xxxx.rpm

3. Add a new file folder named data with the command: mkdir /data

4. Execute the installation command: rpm -ivh nchronoss-xxxx.rpm

The default username for connecting to nChronos Server is admin and the password is D&^4Vs.

**Installing nChronos Console**

**System requirements**
The recommended system requirements for nChronos Console are:

- 4-core processor
- 4GB RAM
- Independent network adapter
- Internet Explorer 9.0 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:

1. Double-click the installation file of nChronos Console, and then the Setup wizard appears. Click Next.
2. 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.
3. Review the product updates, and then click Next.
4. Specify an installation directory. By default, the installation directory is C:\Program Files\Colasoft nChronos Console 5.0. To specify another directory, use the field provided or click Browse to locate an installation folder. Then click Next.
5. Specify the folder name on the Start, and then click Next.
6. Specify whether to create a desktop icon and a quick start icon, and then click Next.
7. 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.
8. Review the Readme, and then click Next.
9. 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.

Follow the Activation Wizard to complete the activation.

Uninstalling nChronos Console

To uninstall nChronos Console 5.0,

1. Do one of the following:
   - On the Start menu, locate the folder of nChronos Console, which, by default, is Colasoft nChronos Console 5.0, and then click Uninstall Colasoft nChronos Console 5.0.
   - On the Start menu, click Control Panel. In Control Panel, click Uninstall a program. Locate Colasoft nChronos Console 5.0 and then click Uninstall.
2. The Uninstall dialog box pops up as the following figure. Click Yes to continue the uninstallation.
3. A box pops up to ask whether to keep configurations. Click Yes if you want to keep the configurations, or else click No.

Tips 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, enter the IP address and port number in the Address bar, and then press ENTER.
2. Enter the user name and the password both of which are defined when you initialize nChronos Server.
3. Click Log In to log in the Server.
Storage Settings

This page is provided to configure storage settings:

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.

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:
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:

- **Name**: The name as well as the IP address of the network interface/port.
- **Status**: The connection status of the network interface/port.
- **Speed**: The connection speed of the network interface/port.
- **Type**: To specify it is a capture interface or a management interface.
- **Action**: Only available for Management interface.
Defining interface type
To define an interface type for a network interface/port, just select the appropriate type from the drop-down list under the **Type** column.

<table>
<thead>
<tr>
<th>Tips</th>
<th>You can define multiple Capture interfaces.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

![Virtual Interface Page](image)

To add a virtual interface,

1. Select the type of the virtual interface to be added. You can choose one of VLAN and MPLS VPN.
2. Click the button Add Virtual Interface to pop up the add box:
3. Type the ID or label, and the name for the virtual interface, and then click **OK** to save the settings.

### Setting a Management interface

To set a management interface, follow the steps below:

1. Click **Edit** following the Management interface to get into the setup page, like the following figure:

```
Management Interface / Edit Interface
```

```
eht5()
```

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>IP mask</td>
<td></td>
</tr>
<tr>
<td>Gateway address</td>
<td></td>
</tr>
<tr>
<td>DNS server</td>
<td></td>
</tr>
</tbody>
</table>
```

2. Enter the IP address, subnet mask, gateway, and DNS server address, 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:

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.
- **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:
2. Enter the link name and select a link type. The following list describes the link types.
   - **Switch (bidirectional mirroring):** nChronos captures traffic from the switch which has mirrored traffic, including inbound and outbound.
   - **Switch (unidirectional 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.

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

4. Set capture interface and network segments:
   - If you select Switch (mirrored bidirectional traffic) or Aggregation tap, follow the steps below:
     1) Select the capture interfaces which are connected with the mirror port of the switch or the tap.
     2) 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 (mirrored unidirectional traffic) 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.
     2) Select the capture interfaces that are connected with the inbound mirror port of the switch or the tap for capturing inbound traffic.
5. Set up whether to use switch timestamp. At present only three types of switches are supported: ARISTA, VSS Monitoring and Gigamon.

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

7. 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.

8. Set bandwidth. Enter the inbound bandwidth, outbound bandwidth, and the total bandwidth.
   You should enter the actual bandwidth to get accurate bandwidth utilization.

9. Click OK to save the settings.

Adding a replay link

To add a replay link, follow the steps below:

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

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

3. 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.

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

5. 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.
6. Set up whether to use switch timestamp. At present only three types of switches are supported: ARISTA, VSS Monitoring and Gigamon.

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

8. 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.

9. Set bandwidth. Enter the inbound bandwidth, outbound bandwidth, and the total bandwidth.
   You should enter the actual bandwidth to get accurate bandwidth utilization.

10. 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**

This page lists all uploaded library files, like the following figure:

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.

**Analysis Center**

**Analysis Center**

- **nChronos Server name**: R&D
- **Center address**: 192.168.5.161
- **Center port**: 22100
- **Username**: csadmin
- **Password**: ************
- **SSL**: 

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

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 22100 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.
SMTP Settings

This page is for setting the connection parameters to an SMTP email server, which is for sending email notifications for alarms and scheduled reports.

**User Information**

- **Your name**: The name of the sender.
- **Email address**: The email address of the sender.

**Server Information**

- **Email server**: The address of the email server.
- **SSL encryption**: Non
- **Port number**: 25

**Login Information**

- **User name**:
- **Password**:

[Test] [OK]
- **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.

### Alarm Notification

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

#### Alarm Notification

<table>
<thead>
<tr>
<th>Email notification</th>
<th>Email subject</th>
<th>Recipient address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notification interval:</th>
<th>1</th>
<th>Range: 1-999 (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syslog notification</th>
<th>Syslog server address:</th>
<th>192.168.9.50:514</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Send every second:</th>
<th>1</th>
<th>Range: 1-999 (minutes)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Send every:</th>
<th>1</th>
<th>Range: 1-999 (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Email notification

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

1. Enable the checkbox **Email notification** on this page.
2. Enter the subject and the recipient address. You can enter multiple recipient addresses.
3. Set the notification interval.
4. 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.
2. Enter the address and the port number of the syslog server.
3. Set the notification interval. You can send the syslog every second or every specified minutes.
4. Click OK to save the settings.

**Report Notification**

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

**Report Notification**

**Report options**

- **Company name**: Colasoft LLC
- **Author**: Administrator
- **Company logo**: ![Colasoft logo]
- **Fretic**: [on/off]
- **Show create time**: [on]
- **Recipient address**: [on]
- **Addresses**:
  - [Email address]
  - [Email address]

[Preview] [Change] [Test] [Save]
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 titles as a prefix.
- **Show create time**: Shows the time when reports are created.

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:

<table>
<thead>
<tr>
<th>No.</th>
<th>Username</th>
<th>Type</th>
<th>Status</th>
<th>Date Created</th>
<th>Date Logged</th>
<th>Notes</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>admin</td>
<td>Administrator</td>
<td>Online (Console, Browser)</td>
<td>2013/08/15 17:32:12</td>
<td>2013/08/21 15:12:47</td>
<td>Default administrator</td>
<td>Edit Delete Kick Out</td>
</tr>
<tr>
<td>2</td>
<td>test</td>
<td>Administrator</td>
<td>Offline</td>
<td>2015/08/23 16:24:47</td>
<td></td>
<td>for test users</td>
<td>Edit Delete Kick Out</td>
</tr>
</tbody>
</table>

- **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 nChromos 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.
- **Create Time**: The time when the account is added.
- **Login Time**: The time when the account logs in, from a Console or a browser.
- **Notes**: The comments or notes for the account.
- **Actions**: The following list describes the actions:
- **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. **New Account** on the **User Account** page to show the following page.

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

3. 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 settings.
   - **User**: A user can login the Server from the Console, but cannot configure the link settings.
   - **Auditor**: An audit can only login the Server from browsers, but can only view the audit logs.

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

### Certificate

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

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.

Security Policy

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

To set the security policy, follow the steps below:

1. Select Lockout policy.
2. Enter the times in the **IP lockout threshold** box.
   This setting 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.

3. Enter the lockout duration in the **IP lockout duration** box.
   This setting 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.
4. Type a number in the **Reset IP lockout counter** after box. This setting 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.

5. Click **OK** to save the settings. Once the Lock policy is enabled, if someone login the Server incorrectly for the times of IP lockout threshold, the IP will be locked. However, if the Lock policy is disabled, the locked IP will be unlocked automatically.

**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:

- **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 Account**: Shows which accounts with which the user attempts to login the Server.
- **Latest Access Time**: Shows the latest access time.
- **Action**: Unlock the IP.

Except the locked IP addresses, 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 **Unlock**.
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:

You can view the event logs by page turning via the buttons ←, →, ↓, ↑, and Go.

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 and the IP address of the computer which the user is using when the event happens.
- **Event**: The details of the event.

**Downloading the logs**

You can download the logs for further use or reference. To download the log, follow the steps below:

1. Click the button **Download** above the log list.
2. Click **OK** to save the log as a .txt file.
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.
2. Click Filter.

To view the logs according to time, follow the steps below:
3. Click the first box of Time and specify a time.
4. Click the second box of Time and specify a time.
5. Click Filter.

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

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

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:
2. Select a time zone and enter the appropriate time, and then 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, and then click OK.

Note: 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 ten minutes.
Server Information

This page provides the basic information of nChronos Server:

### Product Information

<table>
<thead>
<tr>
<th>Product information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Colasoft nChronos Server</td>
</tr>
<tr>
<td>Version:</td>
<td>4.3.0.5021</td>
</tr>
<tr>
<td>Edition:</td>
<td>Standard</td>
</tr>
</tbody>
</table>

### License Information

<table>
<thead>
<tr>
<th>License information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation status:</td>
<td>Activated</td>
</tr>
<tr>
<td>Serial number:</td>
<td></td>
</tr>
<tr>
<td>Licensed to:</td>
<td></td>
</tr>
<tr>
<td>Storage capacity:</td>
<td>163840GB</td>
</tr>
<tr>
<td>Max analysis throughput:</td>
<td>2000Mbps</td>
</tr>
<tr>
<td>Max network interfaces:</td>
<td>8</td>
</tr>
<tr>
<td>Max network links:</td>
<td>4</td>
</tr>
<tr>
<td>Concurrent connections to Server:</td>
<td>2</td>
</tr>
<tr>
<td>Max user accounts:</td>
<td>100</td>
</tr>
<tr>
<td>Maximum monitored applications:</td>
<td>5</td>
</tr>
<tr>
<td>Maximum analyzed transactions:</td>
<td>15</td>
</tr>
</tbody>
</table>

**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, and the maximum user accounts. All those specifications are determined by the license.
Server Management

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

- **Start time**: The time when the service starts.
- **Running time**: The service running time.
- **CPU utilization**: The CPU utilization of the Server.
- **Memory information**: The total memory, used memory, and available memory information.
- **Storage disks**: The space utilization information.
- **SSH remote access**: The status of SSH remote access. 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.

**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 settings 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

The Console user interface includes three parts: menu bar, server explorer, and start page.

Menu bar
The Menu bar includes four menus.

The File menu
- **Download Packets**: Opens the Download Packets dialog box to download packets from nChronics Servers.
- **Options**: System options.
- **Exit**: Exits the program nChronics Console.

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.

### 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.
- **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

### Server Explorer

The Server Explorer lists all added Servers and server groups and, if you select a Server or a network link, shows the basic information of the Server or the network link at the bottom of the Server Explorer.

After adding nChronos Servers, the Server Explorer shows as the following figure:

![Server Explorer](image)

The list below describes the icon buttons on the Server Explorer.
- ![Add](image): Adds a Server or a server group to the Console.
.: Removes the selected Server from the Explorer pane.

.: Views the properties of the selected item.

**Tips**

- 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.

**Start Page**

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

The Start Page mainly includes five sections.

- **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, to replay packet files, 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 section provides some tips when you use the program.
- **What's new**: This section provides some features of the program and guides you to experience these features step by step.
- **Documents**: This section provides some documents about the program. You can get them from our website.
- **Contact Us**: This section provides some contact information. Please feel free to contact us when there are any problems about the program.
Adding and Connecting nChronos Server

As a result of the architecture of nChronos, all captured packets, statistics and other analysis data are stored on nChronos Server. Therefore, to obtain the data and display it on nChronos Console, you must add and connect the nChronos Server to the Console.

Adding an nChronos Server

To add an nChronos Server, follow the steps below:

1. On the Server Explorer, click \( \text{Add Server} \) and click \textbf{Add Server}; the \textbf{Add Server} dialog box appears.

2. Complete the dialog box. See the following list of each label for more information.
   - \textbf{Host}: The IP address of the management interface on nChronos Server.
   - \textbf{Port}: The port number for connecting to Server. It is 3000 by default.
   - \textbf{Name}: A readable name for identifying the Server, for example, \textit{Marketing Dept}. It will be the same as the IP address if you don’t enter one.
   - \textbf{Username}: The account for logging the Server.
   - \textbf{Password}: The password for the account.
   - \textbf{SSL encryption}: Applies SSL encryption when transmitting data from the Server to the Console.
   - \textbf{Data compression}: Compresses the data in the transmission from the Server to the Console.
   - \textbf{Local Authentication/RADIUS Authentication}: Set the authentication method for the connection between nChronos Server and nChronos Console.

3. Click \textbf{OK} after completing the \textbf{Add Server} dialog box. Then the added Server will display on the Server Explorer.
Connecting nChronos Server

Generally speaking, the Console automatically connects the Server upon clicking **OK** in the adding of the Server. If the Console does not connect the Server, you can connect it by the following steps:

- 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:

The Link Properties dialog box includes a variety of settings: Capture Filter, Name Table, Network Segment, Field Definition, Analysis Settings, Application Alarm, Traffic Alarm, Email Alarm, Domain Alarm, and Signature Alarm.

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, like 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.

- ![Create](image) Creates a new filter.
- ![Edit](image) Edits the selected filter.
- ![Delete](image) Deletes the selected filter.
- ![Import](image) Imports saved filter files to current filter list. When a filter file was imported, all the filters in current list will be removed.
- ![Save](image) Saves all filters in current filter list to disk.
- ![Reset](image) Resets the filter to default.

**Adding a filter**

To add a filter, just click ![Create](image) and then complete the Capture Filter dialog box. You can add simple filters or advanced filters.
Applying a filter
To apply a filter, just select the Accept or Reject checkbox, and then click OK on the Link Properties dialog box.

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.

Simple filter
The Simple Filter tab allows you to create simple filters by address, port and protocol. When two or three rules are set, they are connected by logical AND statements. That is, packets must match all of the conditions to match the filter. The Simple Filter tab appears as the following figure:
For distinction and readability, you can define filters by specifying the name, the color, and the description about them.

In order to get packets precisely, you can specify the packet transmission direction in IP address rule, MAC address rule and port rule.

**Defining address rules**

To define an address rule, follow the steps below:

1. Select the **Address rule** checkbox.
2. Select an address type from **Endpoint1** and enter the address in the textbox below the address type.
3. Click the direction drop-down list box to select packet transmission direction between the two addresses.
4. Select an address type from **Endpoint2** and enter the address in the textbox below the address type.

5. 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 rules**

To define a port rule, follow the steps below:

1. Select the **Port rule** checkbox.
2. Select a port type from **Port1** and enter the port number in the textbox below the port type.
3. Click the direction drop-down list box to select packet transmission direction between the two ports.
4. Select a port type from **Port2** and enter the port number in the textbox below the port type.
5. Click **OK** on the **Packet Filter** dialog box.

**Defining protocol rules**

To define a protocol rule, follow the steps below:

1. Select the **Protocol Rule** checkbox.
2. Click **Select** to open the Protocol Rule dialog box which appears as below.

![Protocol Rule Dialog Box]

3. Choose the appropriate protocols and click **OK**.
4. 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.
Advanced filter

The Advanced Filter tab appears as below.

![Advanced Filter Diagram]

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.

Toolbar

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.

For advanced filters, there are six kinds of rules, including Address, Port, Protocol, Size, Value and Pattern. The Address, Port and Protocol rules are the same to those in simple filters.

Defining size rules

Size rule is for defining the rule on packet size. Only packets of the size satisfying the rule will be captured.
To define a size rule, click And or Or on the toolbar and select Size to open the Size Rule dialog box which appears as below.

You can choose < (less than), <= (less than or equal to), > (greater than), => (greater than or equal to), = (equal to), != (not equal to), Between (size range) to define the size rule.

**Defining value rules**

Value rule is for defining the rule on the value of decoded field of a packet.

To define a value rule, click And or Or on the toolbar and select Value to open the Value Rule dialog box which appears as below.

- **Length**: Specifies the length of the mask, and the length of the value for the rule. It could be 1 byte, 2 bytes and 4 bytes.
- **From**: Specifies where to offset in a packet. It could be Raw data, IP Header, ARP Header, TCP Header, and UDP Header.
- **Offset**: Specifies the bytes to be offset. The unit is byte.
- **Mask**: The hexadecimal mask of the value.
- **Byte order**: The order of the bytes. It could be network byte order and host byte order.
- **Operator**: It could be = (equal to), != (not equal to), < (less than), <= (less than or equal to), > (greater than), >= (greater than or equal to).
- **Type**: The type of the value. It could be binary, octal, unsigned decimal and hex.
- **Value**: The value for the rule.
When a value rule is enabled, do logical AND operation between the specified bytes in a packet and the mask, and compare the operation result with the value for the rule. If the compare result is consonant, the packet will be captured; or else, the packet will be filtered out.

**Defining pattern rules**

Content rule is for defining the rule on the content of a packet.

To define a content rule, click **And** or **Or** on the toolbar, select Pattern to open the Pattern Rule dialog box which appears as below, select the type for the content, enter the content, set the offset options, and click **OK**.

![Pattern Rule dialog box](image)

The unit for offset is byte.

**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 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 information on 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, like the following figure:

![Name Table](image)

**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](image)

- **Auto-resolve host names**: Enabled by default 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 Name dialog box](image)

3. Enter the address, and the name for the address.
4. 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:

1. Choose VLAN ID from the Name table type drop-down list.
2. Click to open the Add Name dialog box which appears below.

![Add Name dialog box](image)

3. Enter the VLAN ID, and the name for the VLAN ID.
4. 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.
2. Click to open the Add Name dialog box which appears below.

![Add Name dialog box]

3. Enter the VPN label, and the name for the VPN label.
4. 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.
2. Click to open the Add Name dialog box which appears below.

![Add to Name Table dialog box]

3. Enter the VXLAN ID, and the name for the VXLAN ID.
4. Click OK on the dialog box, and click OK on the Name Table tab.

**Network Segments**

This tab lists all network segments and the rules of the segments, like the following figure:
Buttons

The following list describes the buttons on this tab.

- ![add button]: Adds a network segment.
- ![edit button]: Edits the selected network segment.
- ![delete button]: Deletes the selected network segment.
- ![import button]: Imports network segment customizations from a file.
- ![export button]: Exports current network segment customizations to a file.

Adding a network segment

To add a network segment, follow the steps below:

1. Click ![add button] to open **New Segment** dialog box:
2. On the **New Segment** dialog box, enter an appropriate name for the new segment, specify the location, and then enter the segment rules.

   - **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.
   - **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 cannot 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.

**References**

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

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

- ![Add](image) Adds a new parameter value.
- ![Edit](image) Edits the selected parameter value.
- ![Delete](image) Deletes the selected parameter value.
- ![Import](image) Imports saved setting files to current tab. When a setting file was imported successfully, all the values in current list will be removed.
- ![Save](image) Saves all settings on this tab as *.csta file.

**Adding a field**

To add a field, follow the steps below:

1. Click ![Add](image) to open the **Field Definition** dialog box, which appears as the following figure:
2. Enter the field name and the description if necessary.
3. Click OK.

**Analysis Settings**

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

### Analysis Settings

<table>
<thead>
<tr>
<th>Enable</th>
<th>Name</th>
<th>Application Type</th>
<th>Performance Analysis</th>
<th>Transaction Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>163</td>
<td>Web Application</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>☐</td>
<td>Web Application2</td>
<td>Web Application</td>
<td>☑</td>
<td>☐</td>
</tr>
<tr>
<td>☑</td>
<td>Signature Application</td>
<td>Signature Application</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

### Buttons

The following list describes the icon buttons on this tab:
- ![Add Standard Application](image1.png): Adds a new standard application.
- ![Add Web Application](image2.png): Adds a new web application.
- ![Add Signature Application](image3.png): Adds a new signature application.
- ![Edit Selected Application](image4.png): Edits the selected application.
- ![Delete Selected Application](image5.png): Deletes the selected application.
- ![Import Custom Applications](image6.png): Imports custom applications from a file.
- ![Export Custom Applications](image7.png): Exports current custom applications to a file.

### 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.

- **Transactions 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.

⚠️ **Note**: 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:

![Standard Application Dialog Box](image)

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

3. 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.

4. 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.
5. Set whether to enable performance analysis. Only when the performance analysis is enabled, the application will be monitored and analyzed.

6. 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.

7. 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:

   ![Web Application dialog box](image)

2. 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.
   - **Custom fields**: This section is only available when there are fields predefined on the Field Definition tab of the Link Properties dialog box.

3. 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.

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

5. If necessary, enable **Transaction Analysis**, and then click ![+] to add application transactions. For information about how to add transactions, see *Adding an application transaction* in this section.

The following list describes the other two buttons on this dialog box.

- ![+] This button is for modify the selected transaction.
- ![−] This button is for delete the selected transaction. Once a transaction is deleted, the transaction procedures under it will be also deleted.

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

7. 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.

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

**Adding an application transaction**

To add an application transaction, follow the steps below:

1. On the **Web Application** dialog box, enable **Application Transaction Analysis**, and then click ![+] to open the **Transaction** dialog box as the following figure:
2. On the **Transaction** dialog box, enter the transaction name, and the description.
3. Enter the URL subpath and the parameters. The following list describes the options.
   - **URL path**: The URL of the transaction. It consists of the host name and a URL subpath, and generates automatically when you enter a URL subpath.
   - **URL subpath**: The sub path of the URL.
   - **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.
4. If necessary, enable **Save request content** and **Save response content** to save the transaction request and response content.
5. At last, click **OK** to complete adding transactions.

### 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 dialog box]

2. 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.
   - **Custom fields**: This section is only available when there are fields predefined on the **Field Definition** tab of the **Link Properties** dialog box.
3. 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.

4. Click to define a signature rule.
5. Set whether to enable performance analysis. Only when the performance analysis is enabled, the application will be monitored and analyzed.
6. 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.
7. Click OK on the Signature Application dialog box, and then click OK on the Analysis Settings tab to successfully add a signature application.

**Application Alarms**

You can 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, like the following figure:

![Application Alarms Table]

<table>
<thead>
<tr>
<th>Enable</th>
<th>Name</th>
<th>Category</th>
<th>Object</th>
<th>Severity</th>
<th>Creation Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>Application...</td>
<td>Worm</td>
<td>Network Application...</td>
<td>Low</td>
<td>2016-04-06 16:25:53</td>
<td></td>
</tr>
</tbody>
</table>

**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:

- ![Icon](image) Adds a new application alarm. You can create simple application alarms or advanced application alarms.
- ![Icon](image) Edits the selected alarm.
- ![Icon](image) Deletes the selected alarm.
- ![Icon](image) Imports application alarms from a backup file.
- ![Icon](image) Exports current application alarms to a file.

Adding an application alarm

To create an application alarm, follow the steps below:

1. Click ![Icon](image) on the Application Alarms tab to open the Application Alarms-Add dialog box.

2. 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 Severity.
- 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.

3. Set the trigger condition. The Duration parameter is the statistical duration of the trigger value.
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.
5. 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:

![Transaction Alarms Table]

**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:

- ![Add](image) Adds a new transaction alarm.
- ![Edit](image) Edits the selected alarm.
- ![Delete](image) Deletes the selected alarm.
- ![Import](image) Imports alarms from a backup file.
- ![Export](image) Exports current alarms to a file.

Adding a transaction alarm

To add a transaction alarm, follow the steps below:

1. Click ![Add](image) to open the Transaction Alarms-Add dialog box as the following figure:

![Traffic Alarms-Add](image)

2. 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 *Severity*.
   - **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.
3. Set the trigger condition. The Duration parameter is the statistical duration of the trigger value.

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 nChronos Server.

5. Click **OK** to save the settings.

**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:

### Buttons

The following list describes the icon buttons on this tab:

- ![Add](image) Adds a new traffic alarm. You can create simple traffic alarms or advanced traffic alarms.
- ![Edit](image) Edits the selected alarm.
- ![Delete](image) Deletes the selected alarm.
- ![Import](image) Imports traffic alarms from a file.
- ![Export](image) Exports current traffic alarms to a file.
Adding a traffic alarm

To create a simple traffic alarm, follow the steps below:

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

2. 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 Severity.

3. Set the trigger condition. The Time Bucket parameter is the statistical duration of the trigger value.
4. Set the send parameters:
   - **Send to email**: Sends the alarm log as an email when the alarm is triggered.
   - **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.

5. Click OK to save the settings.
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.

<table>
<thead>
<tr>
<th>Enable</th>
<th>Name</th>
<th>Category</th>
<th>Type</th>
<th>Severity</th>
<th>Creation Time</th>
<th>Description</th>
</tr>
</thead>
</table>

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:

- ![Add](image) Adds a new millisecond traffic alarm.
- ![Edit](image) Edits the selected alarm.
- ![Delete](image) Deletes the selected alarm.
- ![Import](image) Imports alarms from a backup file.
- ![Export](image) Exports current alarms to a file.

Adding a millisecond traffic alarm

To add a transaction alarm, follow the steps below:

1. Click ![Add](image) to open the Millisecond Traffic Alarms-Add dialog box as the following figure:
2. On the **Millissecond 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 *Severity*.

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

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 nChronos Server.
5. 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.

**Email Alarms**

This tab shows as the following figure:

![Email Alarms Tab](image)

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:

- ![Add](image) Adds a new email alarm.
- ![Edit](image) Edits the selected alarm.
- ![Delete](image) Deletes the selected alarm.
- ![Import](image) Imports email alarms from a file.
- ![Export](image) Exports current email alarms to a file.

**Creating an email alarm**

To create an email alarm, follow the steps below:

1. Click ![Add](image) on the **Email Alarms** tab to open the **Email Alarms-Add** dialog box:
2. On the **Email Alarms-Add** dialog box, complete the **Basic Information** section. The following list describes the settings on this dialog box:
   - **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 *Severity*.

3. 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.

4. Specify where to search the keywords.

5. 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.

6. Click **OK** to save the settings.
Domain Alarms

This tab shows as the following figure:

![Domain Alarms](image)

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:

- ![Add](image): Adds a new domain alarm.
- ![Edit](image): Edits the selected alarm.
- ![Delete](image): Deletes the selected alarm.
- ![Import](image): Imports domain alarms from a file.
- ![Export](image): Exports current domain alarms to a file.

**Creating a domain alarm**

To create a domain alarm, follow the steps below:

1. Click ![Add](image) on the Domain Alarms tab to open the Domain Alarms-Add dialog box:
2. On the Domain Alarms-Add dialog box, complete the Basic Information section. The following list describes the settings on this dialog box:
   - **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 Severity*.

3. 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.

4. Set the send parameters:
   - **Send to email**: Sends the alarm log as an email when the alarm is triggered.
   - **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.

5. Click **OK** to save the settings.
Signature Alarms

This tab shows as the following figure:

You can configure signature alarms 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.
- Edits the selected alarm.
- Deletes the selected alarm.
- Imports signature alarms from a file.
- Exports current signature alarms to a file.

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

- **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 *Severity*.

3. Click at the bottom of this dialog box to add a trigger condition, which appears as below:

The following list describes the options on this dialog box:

- **Type**: The type of the packet decoding information.
- **Signature**: The signature of the application.

4. 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 defined in Alarm Notification when configuring the nChronos Server.

5. Click **OK** to save the settings.

**View Management**

There are five tabs under View Management, which are provided to manage the statistical views, showing much like the following figure:

![Link Retrospective Analysis](image)

**Buttons**

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.
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:

1. Right-click the network link and click Export Link Properties to open the Export Link Properties dialog box:

2. On the Export Link Properties dialog box, select the items that you want to export, and then click OK.
3. On the Save As dialog box, enter the file name, and then click OK.

Importing network link properties

To import the properties of a network link, follow the steps below:

1. Right-click the link and click Import Link Properties.
2. On the Open dialog box, double-click the file that you want to import.
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.
2. 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 the following figure:

The Link Analysis window includes a Time Window pane, and an analysis views pane.

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.
Time Window

The following list describes the icon buttons on the Time Window.

These icon buttons are for setting the time range of the Time Window.

Click this icon 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.

With the Time Window, you can get graphical view of several types of network data, including traffic, alarms, packets, packet loss, TCP packets, and utilization. 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:

1. Click and select Set Time Window. The Set Time Window dialog box appears.

2. 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.

3. 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 hour, 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.

2. 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.

3. 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.
- ᵒ: 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 a variety of trend charts in the Time Widow, which are the same to those on the link monitor window, as the following figure:

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:

**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 statistics of current time window and currently selected time range and shows as the following figure:

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Inbound</th>
<th>Outbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>113.43 KB</td>
<td>137.45 KB</td>
</tr>
</tbody>
</table>

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, just like the following figure:

**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.

**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 cancel the selection on the checkbox in front of the drilled object.

**Analyzing MAC addresses in a new window**

To specifically analyze the MAC addresses on the **MAC Address** view, right-click the MAC addresses and click **Analyze in New Window**.

The analysis window for analyzing MAC addresses 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 MAC addresses analysis only displays charts of the traffic of analyzed MAC addresses, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The MAC address analysis time window provides a chart for each analyzed MAC address. For example, if you select three MAC addresses on the MAC Address view to analyze, then the MAC address analysis time window provides three charts, each for one MAC address with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

![MAC Address Analysis Chart](image)

**The MAC Conversation view**

The **MAC Conversation** view provides the statistics and analysis of the traffic according to MAC conversations, just like the following figure:
Viewing MAC conversation statistics

The Physical 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.

The Network Segment view

The Network Segment view shows as the following figure:

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.

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:


To close a drilldown window, just cancel the selection on the checkbox in front of the drilled object.

**Analyzing segments in a new window**

To specifically analyze the segments on the **Network Segment** view, right-click the segments and click **Analyze in New Window**.

The analysis window for analyzing segments 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 segment analysis only displays charts of the traffic of analyzed segments, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The segment analysis time window provides a chart for each analyzed segment. For example, if you select three segments on the Segment view to analyze, then the segment analysis time window provides three charts, each for one segment with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

![Traffic chart](image)

**The Application view**

The **Application** view shows as the following figure:

![Application view](image)

The **Application** view provides statistics of network applications, including system applications and custom applications. The system applications are uploaded to the library when configuring the Server at the Server side and the custom applications can be customized when configuring network link at the Console side. The custom applications have priority over the system 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 a) to display only the top number of items, which are displayed according to the value of the Bytes column.

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:

![Figure](applicationView.png)

To close a drilldown window, just cancel the selection on the checkbox in front of the drilled object.

Analyzing applications in a new window

To specifically analyze the applications on the Application view, right-click the applications and click Analyze in New Window.

The analysis window for analyzing applications 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 application analysis only displays charts of the traffic of analyzed applications, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The application analysis time window provides a chart for each analyzed application. For example, if you select three applications on the Application view to analyze, then the application analysis time window provides three charts, each for one application with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

![Figure](chartExample.png)
The IP Address view

The IP Address view provides the statistics and analysis of the traffic according to IP addresses, just like the following figure:

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 address for more detailed information. To drill an IP 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, like the figure below:

```
```

To close a drilldown window, just cancel the selection on the checkbox in front of the drilled object.

Analyzing IP addresses in a new window

To specifically analyze the IP addresses on the IP Address view, right-click the IP addresses and click Analyze in New Window.

The analysis window for analyzing IP addresses 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 IP addresses analysis only displays charts of the traffic of analyzed IP
addresses, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The IP address analysis time window provides a chart for each analyzed IP address. For example, if you select three IP addresses on the IP Address view to analyze, then the IP address analysis time window provides three charts, each for one IP address with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

![Link Analysis](image)

**The IP Conversation view**

The IP Conversation view provides the statistics and analysis of the traffic according to IP conversations, just like the following figure:

![IP Conversation View](image)

**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 ![Top](image) 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.
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 cancel the selection on the checkbox in front of the drilled object.

### The TCP Conversation view

The TCP Conversation view provides the statistics and analysis of the traffic according to TCP conversations, just like the following figure:

#### 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.

### The UDP Conversation view

The UDP Conversation view provides the statistics and analysis of the traffic according to UDP conversations, just like the following figure:
**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.

**The Service Access view**

The Service Access view shows as the following figure:

**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 to 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.

To close a drilldown window, just deselect the drilled objects.

**Analyzing service accesses in a new window**

To specifically analyze the service accesses on the Service Access view, right-click the service accesses and click **Analyze in New Window**.

The analysis window for analyzing service accesses 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 service access analysis only displays traffic charts of analyzed service accesses, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The service access analysis time window provides a chart for each analyzed service access. For example, if you select three service accesses on the Service Access view to analyze, then the service access analysis time window provides three charts, each for one service access with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

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.

**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 includes two tabs: TCP Service Port and UDP Service Port, showing as the following figure:
Viewing port statistics
The 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 Port view, you can click \(\text{Top}\) 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 \(\text{Top}\) 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.
To close a drilldown window, just deselect the drilled objects.

Analyzing ports in a new window
To specifically analyze the ports on the Port view, right-click the ports and click Analyze in New Window.

The analysis window for analyzing ports 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 port analysis only displays traffic charts of analyzed ports, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The port analysis time window provides a chart for each analyzed service port. For example, if you select three service ports on the Port view to analyze, then the port analysis time window provides three charts, each for one service port with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

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.
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 Link Alarm view
The Link Alarm view provides the logs of all alarms, just like the following figure:

Viewing alarm logs
The Link Alarm view displays link alarm logs according to alarm types. You can click All Alarms tab on the toolbar to view the logs of all link 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 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 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 a new window
To specifically analyze the alarm logs on the Link Alarm view, right-click the alarm logs and click Analyze in New Window.

The analysis window for analyzing alarm logs 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 alarm log analysis only displays charts of the traffic of analyzed addresses or applications, and the Time Window in the Link Analysis window displays the traffic of the whole network.

Analysis on traffic alarm logs is different from that on email, domain and signature alarm logs.

Analyzing traffic alarm logs in a new window is in fact analyzing trigger sources in a new window, which may be IP addresses, MAC addresses and applications. So, the trend charts and analysis views are different when the trigger source is different. The following list describes the details:
• When the trigger source is an IP address, analyzing traffic alarm logs in a new window is just the analysis on a node on the IP Address view.
• When the trigger source is a MAC address, analyzing traffic alarm logs in a new window is just the analysis on a node on the MAC Address view.
• When the trigger source is an application, analyzing traffic alarm logs in a new window is just the analysis on an application on the Application view.

Analyzing email, domain, and signature alarm logs in a new window is in fact analyzing IP address in a new window, the source IP or the destination IP.

To analyze email, domain, and signature alarm logs in a new window, right-click a log, click Analyze in a new window and click the appropriate IP address to open the analysis window. Therefore, you can analyze on one IP address at a time.

The VLAN view

The VLAN view displays VLAN traffic statistics for the monitored network link, showing as the following figure:

Viewing VLAN statistics

The VLAN view displays VLAN statistics based on VLAN 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 VLAN 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 VLAN

You can drill down a VLAN for more detailed information. To drill a VLAN, right-click the VLAN, 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 VLANS in a new window

To specifically analyze the VLANS on the VLAN view, right-click the VLANS and click Analyze in New Window.
The analysis window for analyzing VLANs 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 VLAN analysis only displays traffic charts of analyzed VLANs, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The VLAN analysis time window provides a chart for each analyzed VLAN. For example, if you select two VLANs on the VLAN view to analyze, then the VLAN analysis time window provides two charts, each for one VLAN 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, like the figure below:

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.

**Searching the VLAN 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 VLAN view will only display the items having the keyword.

**The MPLS VPN view**
The **MPLS VPN** view displays MPLS VPN traffic statistics for the monitored network link, showing as the following figure:

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.

**Searching the VLAN 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 VLAN view will only display the items having the keyword.

**The MPLS VPN view**
The **MPLS VPN** view displays MPLS VPN traffic statistics for the monitored network link, showing as the following figure:

**Viewing MPLS VPN statistics**
The MPLS VPN view displays MPLS VPN statistics based on VPN tag. 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 MPLS VPN view, you can click [TOP] 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 [TOP] and click Show All Records.

**Drilling down an MPLS VPN**
You can drill down an MPLS VPN for more detailed information. To drill an MPLS VPN, right-click the MPLS VPN, 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:

![Drilldown Window](image)

To close a drilldown window, just deselect the drilled objects.

**Analyzing MPLS VPNs in a new window**
To specifically analyze the MPLS VPNs on the MPLS VPN view, right-click the MPLS VPNs and click Analyze in New Window.

The analysis window for analyzing MPLS VPNs 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 MPLS VPN analysis only displays traffic charts of analyzed MPLS VPNs, and the Time Window in the Link Analysis window displays the traffic of the whole network.

The MPLS VPN analysis time window provides a chart for each analyzed MPLS VPN. For example, if you select two MPLS VPNs on the MPLS VPN view to analyze, then the MPLS VPN analysis time window provides two charts, each for one MPLS VPN with different colors to identify. When you move you mouse over the charts, the statistics of that time point will be displayed on the top right of the charts, like the figure below:

![Chart Example](image)

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.
**Searching the MPLS VPN 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 MPLS VPN view will only display the items having the keyword.

**The VXLAN view**
The VXLAN view displays VXLAN traffic statistics for the monitored network link, showing as the following figure:

![VXLAN view](image)

**Viewing VXLAN statistics**
The VXLAN view displays VXLAN statistics based on VXLAN 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 VXLAN view, you can click ![top](image) 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 ![top](image) and click Show All.

**Drilling down a VXLAN**
You can drill down a VXLAN for more detailed information. To drill a VXLAN, right-click the VXLAN, 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 VXLANs in a new window**
On the VXLAN view, you can make analysis on one or more items independently. To analyze service port items in a new window, just right-click a service port item and click Analyze in New Window.

**Searching the VXLAN 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 VXLAN 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.

**Summary analysis**

On the TCP 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:

NAT collaborative analysis is for configuring NAT collaborative analysis. Just enable it and enter the IP address and port number.

Multi-segment analysis supports at most three network links for concurrent analysis. If the server is not connected, just double-click to connect it and choose the appropriate network link.

When choosing a conversation for multi-segment analysis, if other network links have the same conversations, the conversations will be selected and highlighted automatically.

**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 packet decoding pane.

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.

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:

1. Click ![Export] on the toolbar to open the Export Statistics dialog box which shows as the following figure:

![Export Statistics Dialog Box](image)

2. Complete the dialog box and click **Export**.

   **Note** The Export Statistics dialog box from the Summary view is different from that from other analysis views.

**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:

1. Click on the toolbar to open the Download Packet dialog box which shows as the following figure:

2. Complete the dialog box and click Download.
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.
- **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.

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:

1. Click on the toolbar of the analysis views to open the Analyze Packets dialog box, which shows as the following figure:
2. 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.
2. 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 link, including throughput, packets, bandwidth utilization, TCP SYN packets, TCP SYNACK packets, and alarm quantity.

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 on the link monitor window display the real-time status of the network link, 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.

By default, all trend charts are displayed in a four-minute time window which has a four-minute horizontal axis and the trend charts update every one second. Furthermore, the trend charts can be displayed in other types of time window.

**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.

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.
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 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 one second, including trigger time, alarm category, alarm object, alarm name, alarm severity, and trigger condition.

All alarms are defined when configuring a network link. Furthermore, signature alarms can be uploaded to the library when configuring the Server.

**The Matrix pane**

The **Matrix** pane shows the network communication 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.

By default, the matrix pane displays the peer map of the communications between IP addresses. 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.
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 view screenshot](image)

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.

![Millisecond Traffic Alarm view screenshot](image)

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.

According to report view type, there are instant reports and scheduled reports.

Instant reports are the reports users can directly view on the Report window of nChronos Console. Instant report could be any one of System Reports and User-Defined Reports.

Scheduled reports are the reports scheduled by users and can only be available in the email inbox.

Instant reports

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.
When comparing statistics, 0.00% indicates no change, and ∞% indicates no data in the compared time period.

Instant reports can be printed, saved and sent by email.

**Print**

Click ![icon] 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 ![icon].

**Email**

Instant reports can be sent to email recipients.

To email an instant report,

1. Click ![icon] to open the Send Reports dialog box:

2. Specify the recipient.
   If the recipient address is not on the list, you can click an empty list to enter a new recipient address.
3. Click **Send Now** to send the instant report.
   You can also click **Schedule** to schedule a report based on the instant report.

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.


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:
2. Enter the report name and the description. The report name should be a unique one which cannot be the same as an existent report.

3. 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:
The object could be IP addresses, MAC addresses, network segment, or a user-defined application, which means the report statistics are calculated based on selected object.

4. 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.

5. Click OK to complete creating a report. You can view the new report under the node User-Defined 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:
2. Enter the report name and the description. The report name cannot be same to the duplicated one.

3. Modify the report scope according to the need.

4. 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.

5. Click OK to complete duplicating a report. You can view the new report under the node User-Defined 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.
2. On the **Manage Schedules** dialog box, click to open the **New Schedule** dialog box:
3. Choose the report which the schedule is based on.
4. 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.

5. Specify the schedule trigger and specify whether to compare with historical statistics.
6. 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.

   **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:
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 node **Alarms** under the network link.

2. 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.
Monitoring Applications

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 the **Performance Analysis** on the **Analysis Settings** tab of the **Link Properties** dialog box.
2. Once an application is monitored, it will display under the network link on the Server Explorer.
3. 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 monitor window for network link and includes six panes:

- Trend Charts
- Real-Time Data
- Top Segments
- Top Hosts
- Alarms
- Matrix

The above panes for application monitor are much like those for link monitor, only the former for the monitored application and the latter for the whole network link.

The Trend Charts pane

There are several trend charts on the Trend Charts pane: Response Time, TCP Retransmissions, TCP Conversations, Transactions, Traffic, Packets, and etc.
Right-click on the trend charts, you can choose which charts to show and can set the time length 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.

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 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.
2. Once an application is monitored, it will display under the network link on the **Server Explorer**.
3. 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, as the following figure:

![Trend charts for application performance analysis](image)

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.

There are seven performance analysis views in the performance analysis window for the application performance analysis: the Client view, the Server view, the Network Segment view, the IP Conversation view, the TCP Conversation view, and the Application Alarms view.

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

When viewing the statistics on the Client view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that 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.

In addition, 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.

Drilling down a client

You can drill down any objects on the Client view for more detailed information. To drill an object, right-click it, 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:

To close a drilldown window, just deselect the drilled objects.

**The Server view**

The Server view for application analysis provides the statistics and analysis data of the traffic according to the IP addresses of the servers of the application.

**Viewing server statistics**

When viewing the statistics on the Server view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that column.

When there are a lot of servers on the view, you can click ![top](image) to display only the top number of items, which are displayed according to the value of the Bytes column.

In addition, 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.

**Drilling down a server**

You can drill down any objects on the Server view for more detailed information. To drill an object, right-click it, 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.

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

When viewing the statistics on the Network Segment view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that 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.

In addition, 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.

Drilling down a segment

You can drill down any objects on the Network Segment view for more detailed information. To drill an object, right-click it, 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.

**The IP Conversation view**

The **IP Conversation** view for application analysis provides the statistics and analysis data of the traffic according to IP conversations of the application.

When viewing the statistics on the IP Conversation view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that 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.

In addition, 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 according to TCP conversations of the application.

When viewing the statistics on the TCP Conversation view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that 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.

In addition, 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.

The Application Alarms view displays the alarm logs according to alarm types.

- The Application Alarms 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 conversations 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.

In addition, 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 the **Transaction Analysis** on the **Analysis Settings** tab of the **Link Properties** dialog box.
2. Then the application displays under the network link on the Server Explorer.
3. Double-click the application under the network link, 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:

There are five analysis views in the transaction analysis window for the application transaction analysis: the Client view, the Server view, the Network Segment view, the Transaction view, and the Transaction Log view.

**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.

When viewing the statistics on the Client view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that column.

You can drill down any objects on the Client view for more detailed information. To drill an object, right-click it, then click **Drill Down** and select the appropriate drilldown object. Next, you will see that a drilldown window slides out.

**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.

When viewing the statistics on the Server view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns.
Furthermore, click a column on the column header, the statistics will be sorted according to that column.

You can drill down any objects on the Server view for more detailed information. To drill an object, right-click it, 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 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.

When viewing the statistics on the Network Segment view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that column.

You can drill down any objects on the Network Segment view for more detailed information. To drill an object, right-click it, 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 Transaction view**

The Transaction view provides the transaction statistics for the application, like the following figure:

![Transaction View](image)

**Note** All transactions must be defined in Custom App of Network Link Properties; or else, there will be no statistics on this view.

When viewing the statistics on the Transaction view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that column.

You can drill down any objects on the Transaction view for detailed transaction log information. To drill a transaction, just double-click it, then the drill down window slides out.
The Transaction Log view

The Transaction Log view provides the logs of all transactions, with one transaction having one log, like the following figure:

When viewing the statistics on the Transaction Log view, there are some default columns and, you can right-click the column header and then click the appropriate column to display other columns. Furthermore, click a column on the column header, the statistics will be sorted according to that column.

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:

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 Transaction Alarms 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.