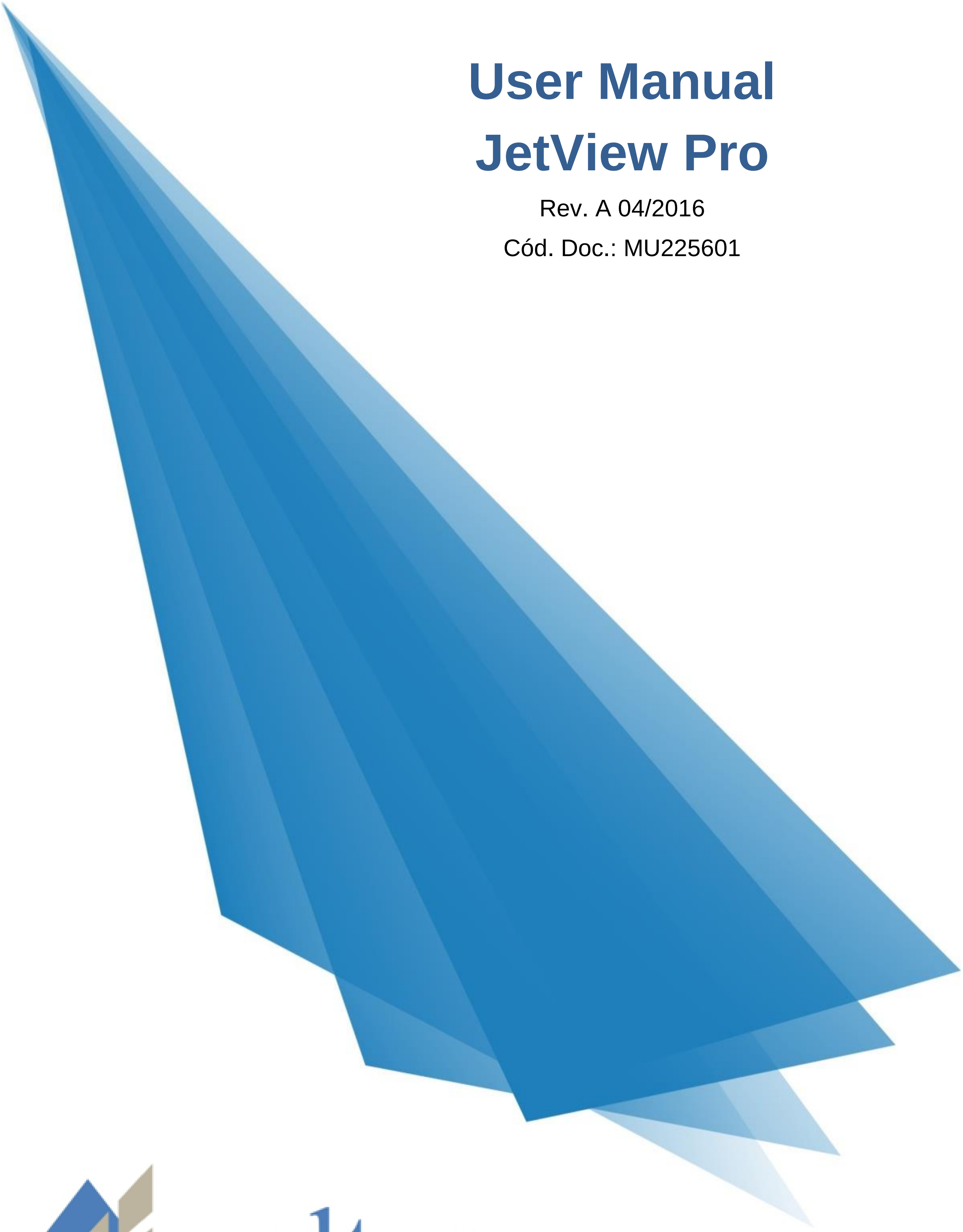
User Manual
JetView Pro

Rev. A 04/2016

Cód. Doc.: MU225601



www.altus.com.br

No part of this document may be copied or reproduced in any form without the prior written consent of Altus Sistemas de Automação S.A. who reserves the right to carry out alterations without prior advice.

According to current legislation in Brazil, the Consumer Defense Code, we are giving the following information to clients who use our products, regarding personal safety and premises.

The industrial automation equipment, manufactured by Altus, is strong and reliable due to the stringent quality control it is subjected to. However, any electronic industrial control equipment (programmable controllers, numerical commands, etc.) can damage machines or processes controlled by them when there are defective components and/or when a programming or installation error occurs. This can even put human lives at risk.

The user should consider the possible consequences of the defects and should provide additional external installations for safety reasons. This concern is higher when in initial commissioning and testing.

The equipment manufactured by Altus does not directly expose the environment to hazards, since they do not issue any kind of pollutant during their use. However, concerning the disposal of equipment, it is important to point out that built-in electronics may contain materials which are harmful to nature when improperly discarded. Therefore, it is recommended that whenever discarding this type of product, it should be forwarded to recycling plants, which guarantee proper waste management.

It is essential to read and understand the product documentation, such as manuals and technical characteristics before its installation or use.

The examples and figures presented in this document are solely for illustrative purposes. Due to possible upgrades and improvements that the products may present, Altus assumes no responsibility for the use of these examples and figures in real applications. They should only be used to assist user trainings and improve experience with the products and their features.

Altus warrants its equipment as described in General Conditions of Supply, attached to the commercial proposals.

Altus guarantees that their equipment works in accordance with the clear instructions contained in their manuals and/or technical characteristics, not guaranteeing the success of any particular type of application of the equipment.

Altus does not acknowledge any other guarantee, directly or implied, mainly when end customers are dealing with third-party suppliers.

The requests for additional information about the supply, equipment features and/or any other Altus services must be made in writing form. Altus is not responsible for supplying information about its equipment without formal request.

COPYRIGHTS

Nexto, MasterTool, Grano and WebPLC are the registered trademarks of Altus Sistemas de Automação S.A.

Windows, *Windows NT* and *Windows Vista* are registered trademarks of Microsoft Corporation.

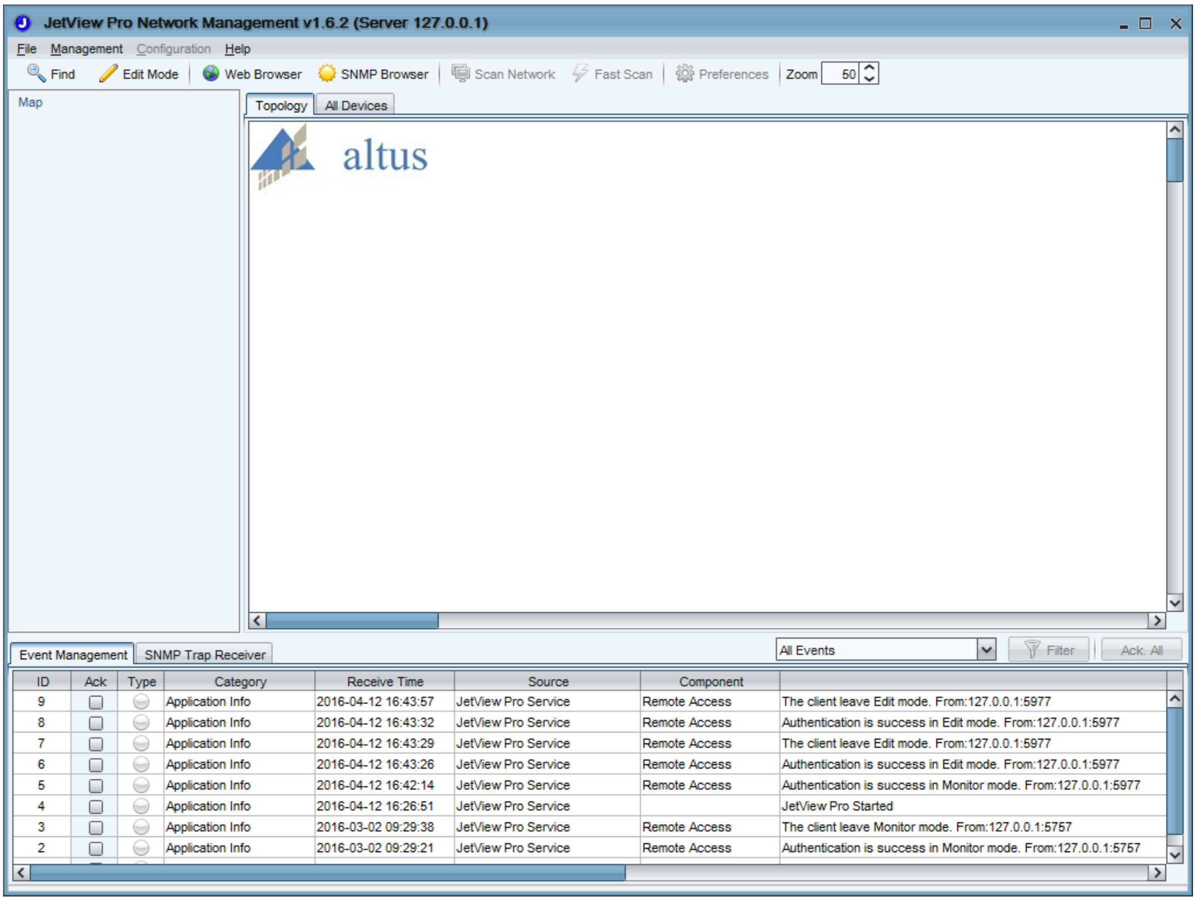
OPEN SOURCE SOFTWARE NOTICE

To obtain the source code under GPL, LGPL, MPL and other open source licenses, that is contained in this product, please contact opensource@altus.com.br. In addition to the source code, all referred license terms, warranty disclaimers and copyright notices may be disclosed under request.

Table of Contents

1. Introduction

The JetView Pro is a Network Management System – NMS and was designed specifically for critical applications on industrial environments. The JetView Pro provides a comprehensive platform for monitoring, configuring, and maintaining mission-critical IP-based communication networks, such as IP surveillance, factory automation, mining, substation, maritime and military applications.



ID	Ack	Type	Category	Receive Time	Source	Component	
9	□	○	Application Info	2016-04-12 16:43:57	JetView Pro Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5977
8	□	○	Application Info	2016-04-12 16:43:32	JetView Pro Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5977
7	□	○	Application Info	2016-04-12 16:43:29	JetView Pro Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5977
6	□	○	Application Info	2016-04-12 16:43:26	JetView Pro Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5977
5	□	○	Application Info	2016-04-12 16:42:14	JetView Pro Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5977
4	□	○	Application Info	2016-04-12 16:26:51	JetView Pro Service		JetView Pro Started
3	□	○	Application Info	2016-03-02 09:29:38	JetView Pro Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5757
2	□	○	Application Info	2016-03-02 09:29:21	JetView Pro Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5757

Figure 1–1. JetView Pro

Innovative Features

JetView Pro has the following features:

- Manage IP-based devices from both central office and remote sites
- Automated network discovery and topology visualization
- Event handling via polling, syslog, email, and SNMP trap. Notifications can be sent via email, application programs, SNMP trap, SMS, and MSN Messenger
- Device configurations via SNMP, Web, Telnet, and SSH
- Provide SNMPv1/v2c/v3 Browser and SNMP MIB compiler
- MSR group management
- Provide performance management
- Provide accounting management
- Centralized management to reduce network traffic

Supported Devices

Supported Devices by Functions:

Auto Topology (LLDP), device management, and device discovery features Auto Topology, device management, and device discovery features can be applied in the IP-enabled devices which support LLDP and SNMP features. For instances, Connect series and 3rd party devices that support LLDP and SNMP features.

- Connect series: JN4508f-m

Device Management and Device Discovery Features

Device management and device discovery features can be applied in the IP-enabled devices which support SNMP feature. For instances, Connect series and 3rd party devices that support SNMP.

- Connect series: JN4508f-m

Device Discovery Feature

Device discovery feature can be widely applied in all the IP-enabled devices. For example, Connect series and 3rd party devices that support WEB or telnet features and general windows PCs.

- Connect series: JN4508f-m

Support MIBs

JetView Pro supports the following standard MIBs in addition to the private MIBs.

- RFC1213-MIB-II.mib RFC1215-MIB-II.mib
- RFC1398-ETHER.mib
- RFC1493-BRIDGE.mib
- RFC1724-RIP.mib
- RFC1757-RMON.mib
- RFC1850-OSPF.mib
- RFC3621-PSE.mib

Ordering Information

A trial version that supports monitoring of 16 IP-enabled devices is available for authorized distributors.

Request licenses as follows:

- 32 – manage 32 devices
- 64 – manage 64 devices
- 128 – manage 128 devices
- 256 – manage 256 devices
- 1024 – manage 1024 devices
- Unlimited – unlimited devices

For more detailed information, please contact your local sales representative.

Documents Related to this Manual

For additional information about JetView Pro, you can examine other specific documents in addition to this one. These documents are available in its last review on www.altus.com.br.

General Regards on Altus Documentation

Each product has a document called Technical Characteristics (CT), where there are the characteristics for the product in question. Additionally, the product may have User Manuals (manual's codes, if applicable, are always mentioned at CTs from the respective modules).

Support and Documentation

It is advisable to consult the following documents as a source of additional information:

Code	Description	Language
CE125000	Connect Series – Technical Characteristics	English
CT125000	Série Connect – Características Técnicas	Portuguese
CS125000	Serie Connect – Características Técnicas s	Spanish

Visual Inspection

Prior to installation, we recommend performing a careful visual inspection of equipment, by checking if there is damage caused by shipping. Make sure all components of your order are in perfect condition. In case of defects, inform the transportation company and the nearest Altus representative or distributor.

CAUTION:
Before removing modules from the package, it is important to discharge eventual static potentials accrued in the body. For this, touch (with nude hands) in a metallic surface grounded before modules handling. Such procedure ensures that the levels of static electricity supported by the module will not be overcome.

It is important to record the serial number of each item received, as well as software revisions, if any. This information will be necessary if you need to contact Altus Technical Support.

Technical Support

To contact Altus Technical Support in São Leopoldo, RS, call +55 51 3589-9500. To find the existent centers of Altus Technical Support in other locations, see our site (www.altus.com.br) or send an email to altus@altus.com.br.

If the equipment is already installed, please have the following information when requesting assistance:

- Models of equipment used and the configuration of installed system
- Equipment review and software version used

Warning Messages Used in this Manual

In this manual, warning messages will present the following formats and meanings:

DANGER:
Relates potential causes that if not noted, generate damages to physical integrity and health, property, environment and production loss.

CAUTION:
Relates configuration details, application and installation that shall be followed to avoid condition that could lead to system fail, and its related consequences.

ATTENTION:
Indicate important details to configuration, application or installation to obtain the maximum operation performance from the system.

2.Installation

This section includes software installation. Following topics are covered in this section.

System Requirements

Processor:

- Minimum Intel Core 2 Duo CPU 2.5 GHz or higher

RAM

- 1GB RAM

Disk

- 1GB hard disk

Software, Operation system

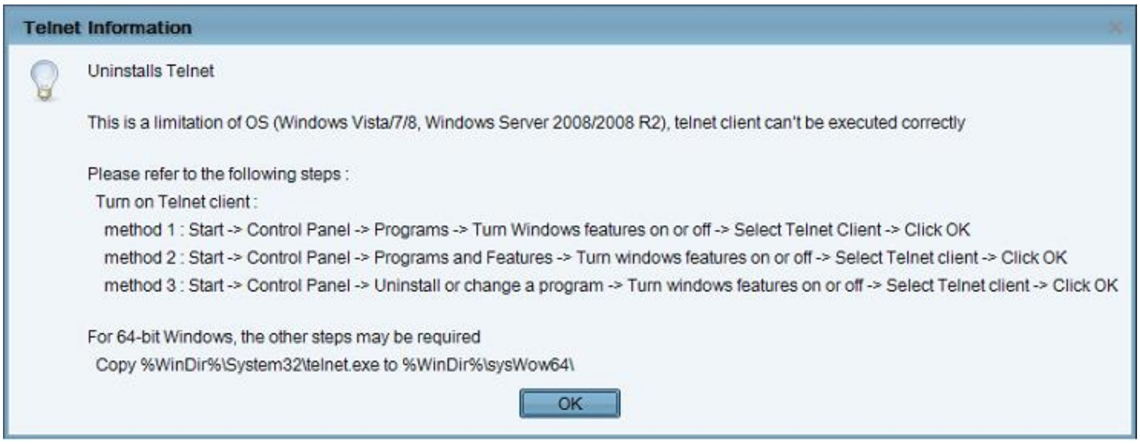
- Windows XP/2000/2003 platforms
- Windows Vista/7 platforms

Windows Vista/7 notice

- Execution JetView Pro using the system administrator

Turn on Telnet and TFTP System Commands:

Turn on Telnet client:



Telnet Information

Uninstalls Telnet

This is a limitation of OS (Windows Vista/7/8, Windows Server 2008/2008 R2), telnet client can't be executed correctly

Please refer to the following steps :
Turn on Telnet client :
method 1 : Start -> Control Panel -> Programs -> Turn Windows features on or off -> Select Telnet Client -> Click OK
method 2 : Start -> Control Panel -> Programs and Features -> Turn windows features on or off -> Select Telnet client -> Click OK
method 3 : Start -> Control Panel -> Uninstall or change a program -> Turn windows features on or off -> Select Telnet client -> Click OK

For 64-bit Windows, the other steps may be required
Copy %WinDir%\System32\telnet.exe to %WinDir%\sysWow64\

Figure 2–1. Turning ON Telnet Client on Windows

Method 1:

Start -> *Control Panel* -> *Programs* -> *Turn Windows features on or off* -> Select *Telnet Client* -> Click *OK*.

Method 2:

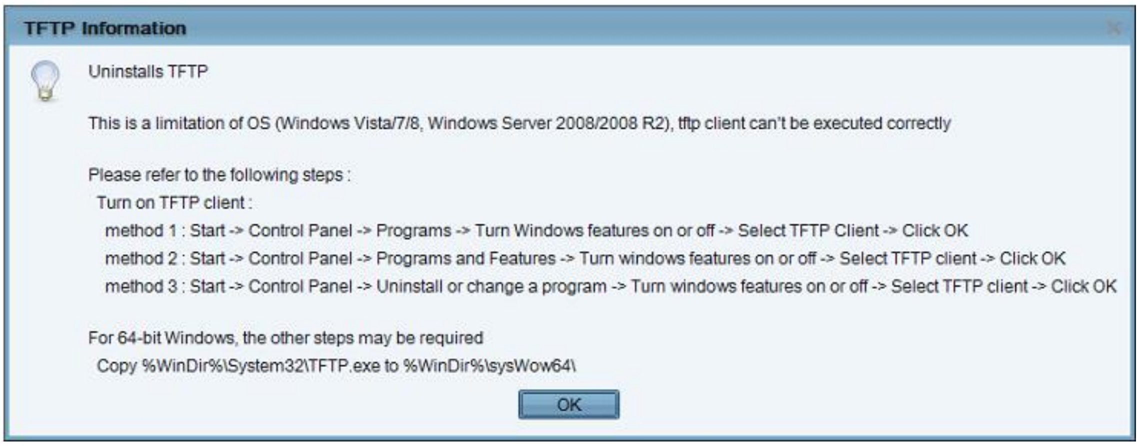
Start -> *Control Panel* -> *Programs and Features* -> *Turn windows features on or off* -> Select *Telnet client* -> Click *OK*.

Method 3:

Start -> *Control Panel* -> *Uninstall or change a program* -> *Turn windows features on or off* -> Select *Telnet client* -> Click *OK*.

For 64-bits Windows, the other steps may be required. Copy %WinDir%\\System32\\telnet.exe to %WinDir%\\sysWow64\\

Turn on TFTP client:



TFTP Information

Uninstalls TFTP

This is a limitation of OS (Windows Vista/7/8, Windows Server 2008/2008 R2), tftp client can't be executed correctly

Please refer to the following steps :
Turn on TFTP client :
method 1 : Start -> Control Panel -> Programs -> Turn Windows features on or off -> Select TFTP Client -> Click OK
method 2 : Start -> Control Panel -> Programs and Features -> Turn windows features on or off -> Select TFTP client -> Click OK
method 3 : Start -> Control Panel -> Uninstall or change a program -> Turn windows features on or off -> Select TFTP client -> Click OK

For 64-bit Windows, the other steps may be required
Copy %WinDir%\System32\TFTP.exe to %WinDir%\sysWow64\

Figure 2–2. Turning ON TFTP on Windows

Method 1:

Start -> *Control Panel* -> *Programs* -> *Turn Windows features on or off* -> Select *TFTP Client* -> Click *OK*.

Method 2:

Start -> *Control Panel* -> *Programs and Features* -> *Turn windows features on or off* -> Select *TFTP client* -> Click *OK*.

Method 3:

Start -> *Control Panel* -> *Uninstall or change a program* -> *Turn windows features on or off* -> Select *TFTP client* -> Click *OK*.

For 64-bit Windows, the other steps may be required:

Copy %WinDir%\\System32\\TFTP.exe to %WinDir%\\sysWow64\\

Windows Firewall

The Windows Firewall may affect the function of backing up Connect device's configuration. Therefore, it is suggested to turn off Windows Firewall or enable TFTP port on Windows Firewall.

Antivirus Software

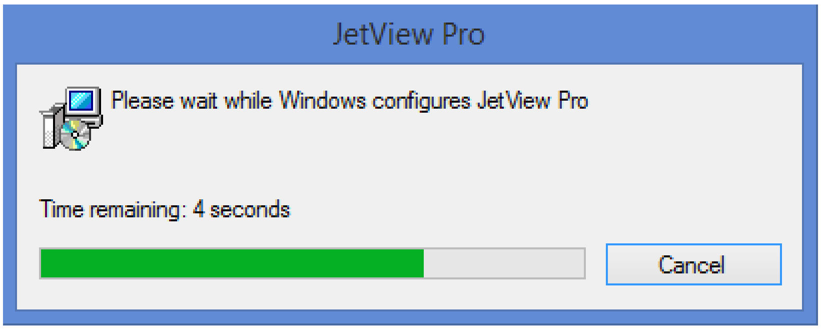
Some of the antivirus software may affect the JetView Pro function, it is suggested to turn off the Antivirus Software, if possible.

Screen Resolution

It is optimized for a screen resolution of 1024x768.

Installation

Run the file JetView Pro.MSI and wait for the installation to complete:


JetView Pro

Please wait while Windows configures JetView Pro

Time remaining: 4 seconds

Figure 2–3. JetView Pro Installation

At the end of the installation process, two shortcuts will be created on desktop:

Figure 2–4. Shortcut for Local Host Connection

Figure 2–5. Shortcut to Connect to Remote Server

Uninstallation

Remember to quit the JetView Pro program before you get starting the uninstall process.

Follow the steps below to uninstall:

1. To uninstall JetView Pro, select Start / Control Panel / Add or Remove Program
2. Select the program *JetView Pro*
3. Click on Remove and follow the instructions of the uninstallation process

Another option is to go directly on Start Menu / All Programs / Altus / Uninstall JetViewPro.

3. Getting Started

JetView Pro Applications

JetView Pro is a client/server based network system. One JetView Pro server can serve many remote access JetView Pro clients (maximum is 5) see Figure 3–1 figure below.

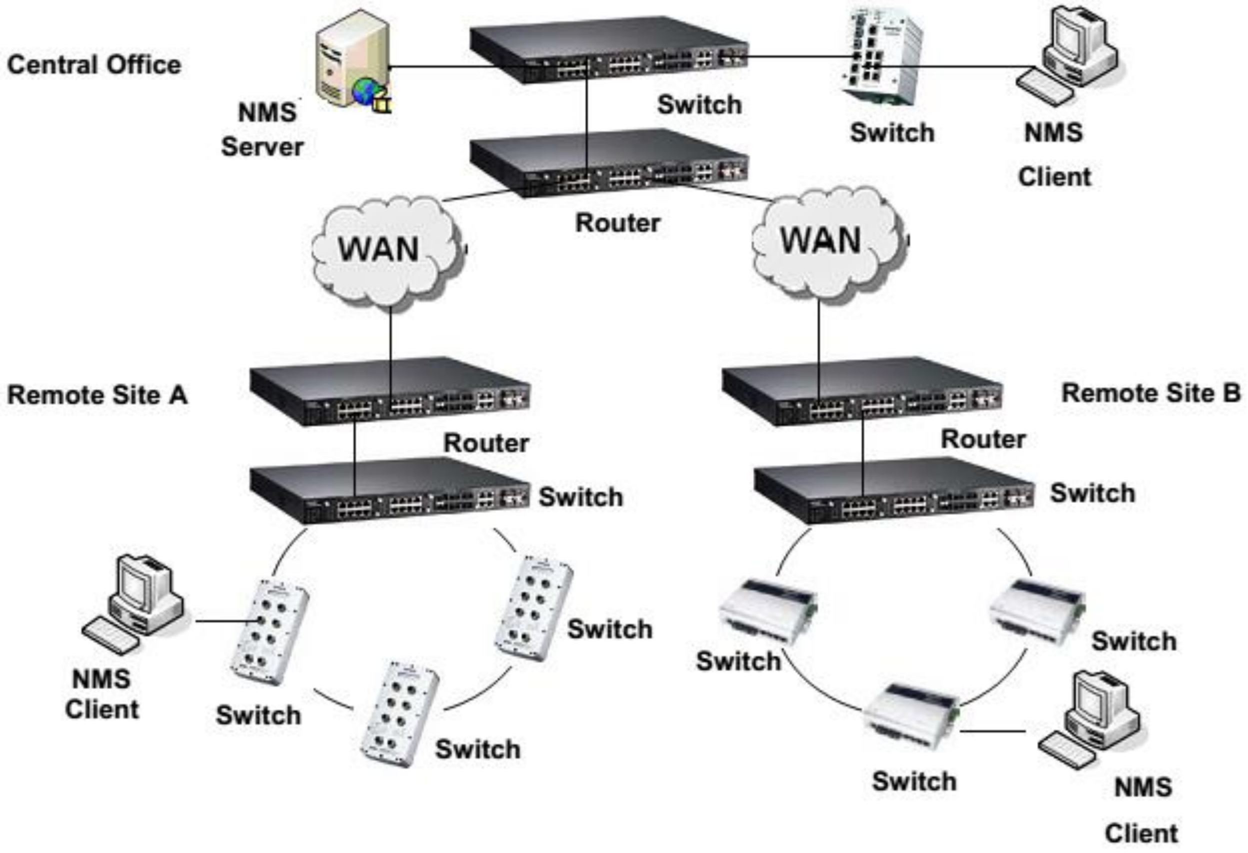


Figure 3–1. Example of Network Using JetView Pro

Due to the accounting management, only one client can enter the Edit mode at the same time and other clients are in the Monitor mode. The default password to enter the two modes is *korenix*. The Monitor mode can only allow viewers to browse the topology. The Edit mode can use all functions.

Note:

Only one remote client connection per computer is possible. The server will refuse the new connection if already one session exists

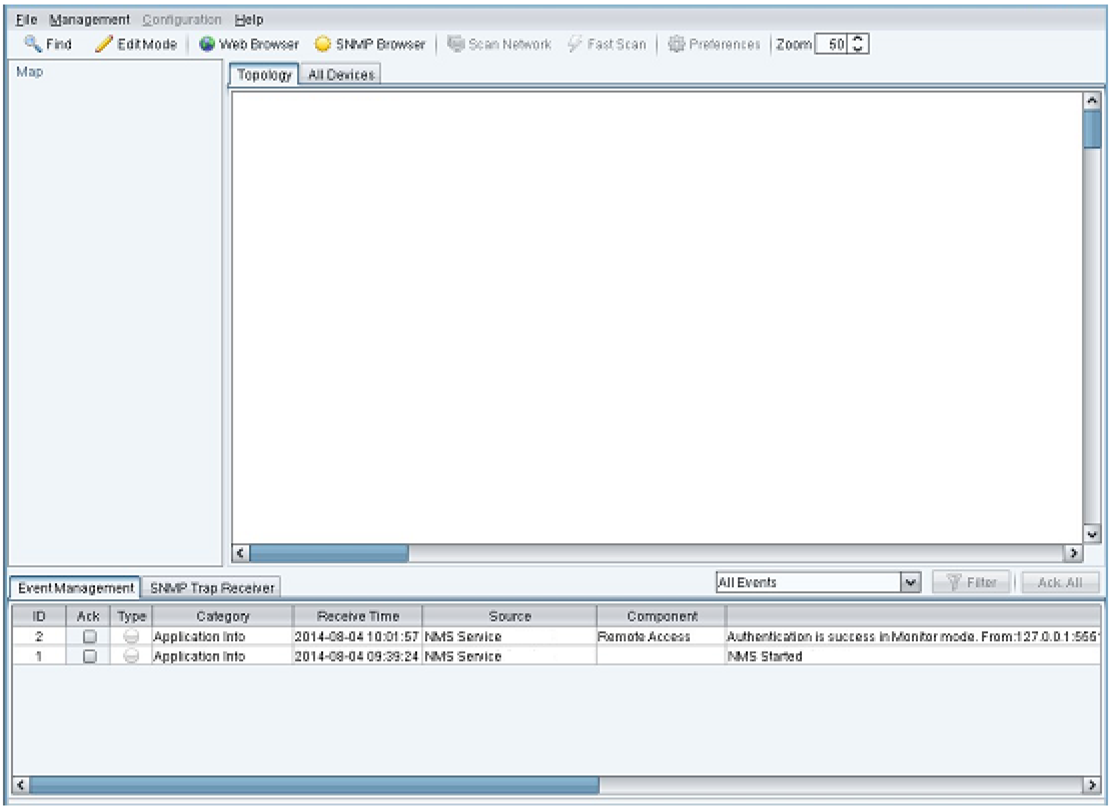
Run JetView Pro Server and Remote Access Clients

JetView Pro Service starts automatically when Windows XP starts. You can get the status of the service in Windows XP under *Start / Control Panel / Administration / Services*. This service has a connection to a database containing all the relevant data for the settings of JetView Pro. Note that when the service is stopped, the relevant monitored data cannot be recorded into the database.

For Windows XP, it starts automatically *JetView Pro Service* after installation. You can change Startup type of this service to Manual if you don't want the service to run after your pc boot up.

Start JetView Pro Server on Server Site

1. *Start / Programs / Altus / JetViewPro* (local host)
2. Display JetView Pro main window

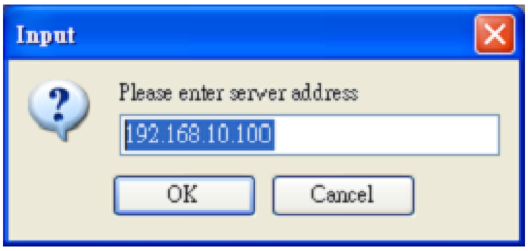


ID	Ack	Type	Category	Receive Time	Source	Component	
2	□		Application Info	2014-08-04 10:01:57	NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:566
1	□		Application Info	2014-08-04 09:39:24	NMS Service		NMS Started

Figure 3–2. JetView Pro Interface

Start JetView Pro Client (Connect to Server)

- *Start / Programs / Altus / JetViewPro*
- Enter server address to connect. (ex. Server IP: 192.168.10.100)



Please enter server address

192.168.10.100

Figure 3–3. Connecting to a Server IP

- Enter password into monitor mode and press *OK*

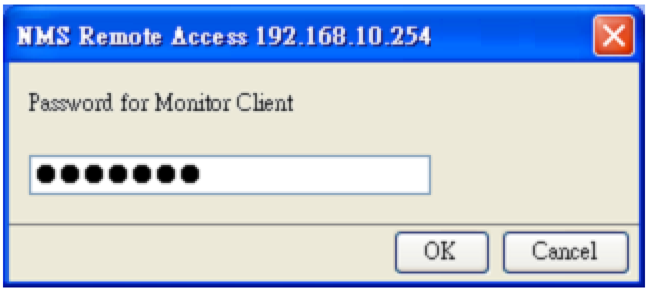
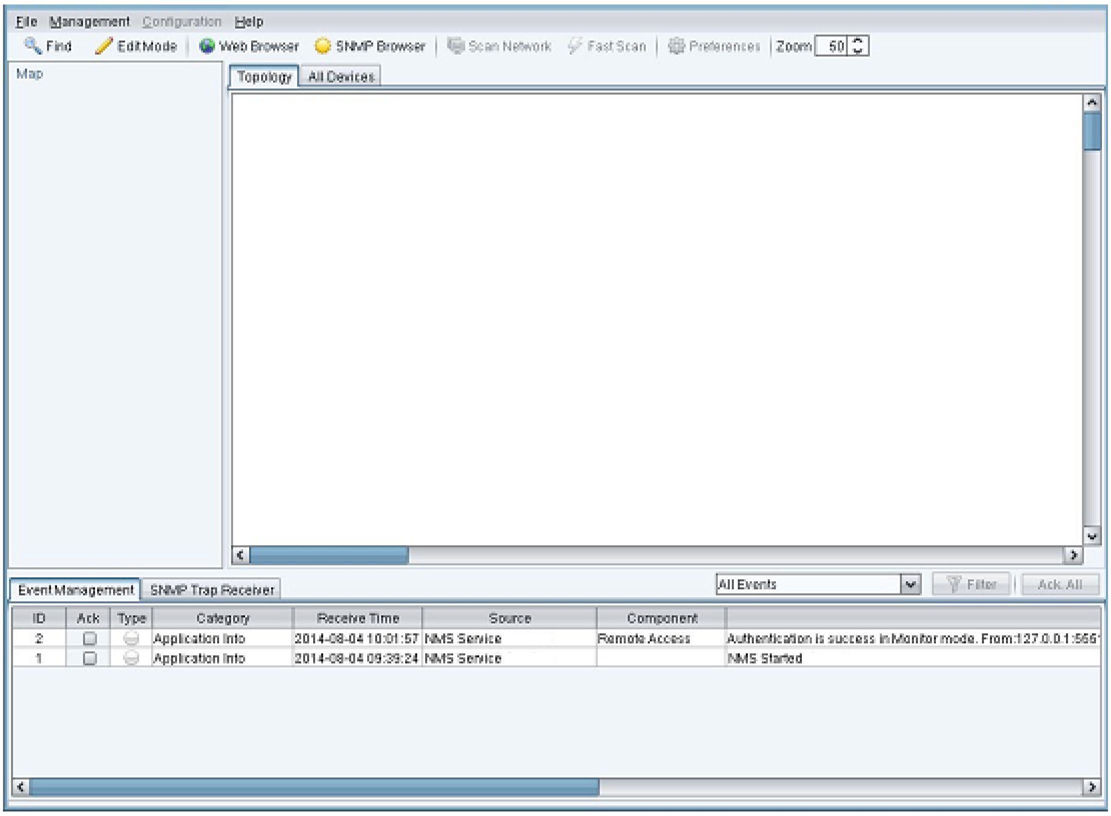


Figure 3–4. Inserting Password for Monitor Client

- Display JetView Pro main window



ID	Ack	Type	Category	Receive Time	Source	Component	
2	□		Application Info	2014-08-04 10:01:57	NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:566
1	□		Application Info	2014-08-04 09:39:24	NMS Service		NMS Started

Figure 3–5. JetView Pro Main Window

4. Interface of JetView Pro

Main Window

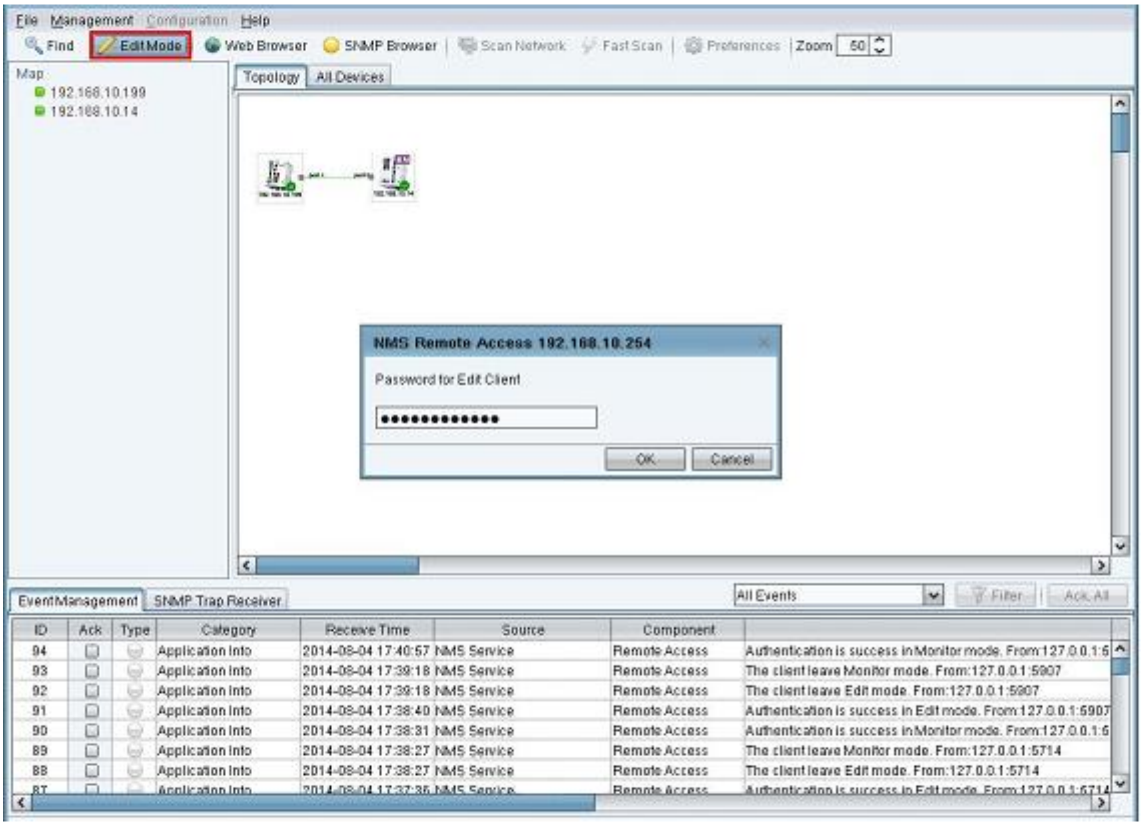
When you start JetView Pro, the main window appears on the screen. It consists of the following parts:

- Menu Function
- Toolbar Function
- Map Tree
- Topology Tab
- All Devices Tab
- Event Management Tab
- SNMP Trap Receiver Tab

Enter the Edit Mode

The Monitor mode is only able to view the topology when starting JetView Pro into main window. To change the settings, need to enter Edit mode.

1. Click on *Edit Mode* on the toolbar, it displays Password dialog.



NMS Remote Access 192.168.10.254

Password for Edit Client

●●●●●●●●●●●●●

OK Cancel

ID	Ack	Type	Category	Receive Time	Source	Component	
94	□		Application Info	2014-08-04 17:40:57	NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
93	□		Application Info	2014-08-04 17:39:18	NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5907
92	□		Application Info	2014-08-04 17:39:18	NMS Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5907
91	□		Application Info	2014-08-04 17:38:40	NMS Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5907
90	□		Application Info	2014-08-04 17:38:31	NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
89	□		Application Info	2014-08-04 17:38:27	NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5714
88	□		Application Info	2014-08-04 17:38:27	NMS Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5714
87	□		Application Info	2014-08-04 17:37:36	NMS Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5714

Figure 4–1. Inserting Password for Editing Mode

2. Input password (default password) and press *OK*
3. After entering Edit Mode, the button will become green.

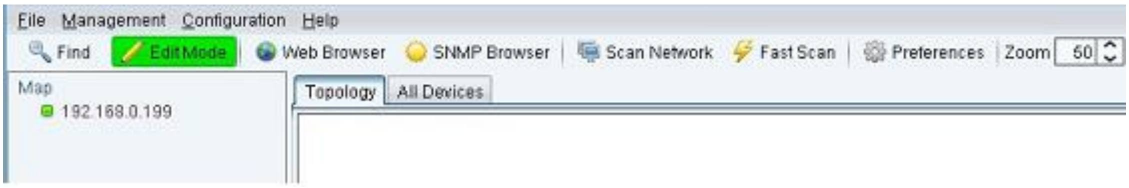


Figure 4–2. Edit Mode Enabled

In the Edit mode, all functions are available. If return to Monitor mode, click on *Edit Mode* again.

Menu Function

The menu function contains the following selection items:

- File
- Management
- Configuration
- Help

Figure 4–3. Function Menu

File Submenu

File – Open: opens the previous saved database file.

File – Save: saves the current database into file.

File – Export: exports the displayed map in the Topology Map as Image file (BMP, JPEG, PNG format)

File – Print: exports the displayed map in the Topology Map as PDF file.

File – Exit: closes the JetView Pro Main Window.

File – Exit and Stop Service: closes JetView Pro Main Window and stops JetView Pro Service

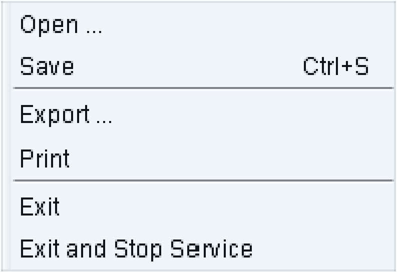


Figure 4–4. Expanded File Menu

Management Submenu

For more information see the chapter Configure File Operation.

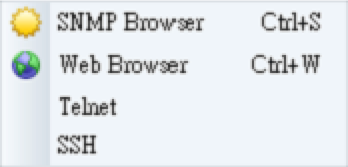


Figure 4–5. Management Submenu

Configuration Submenu

For more information see the chapter Performance Management.

Figure 4–6. Submenu Preferences

Help Submenu

It shows the version and release date of JetView Pro.

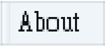
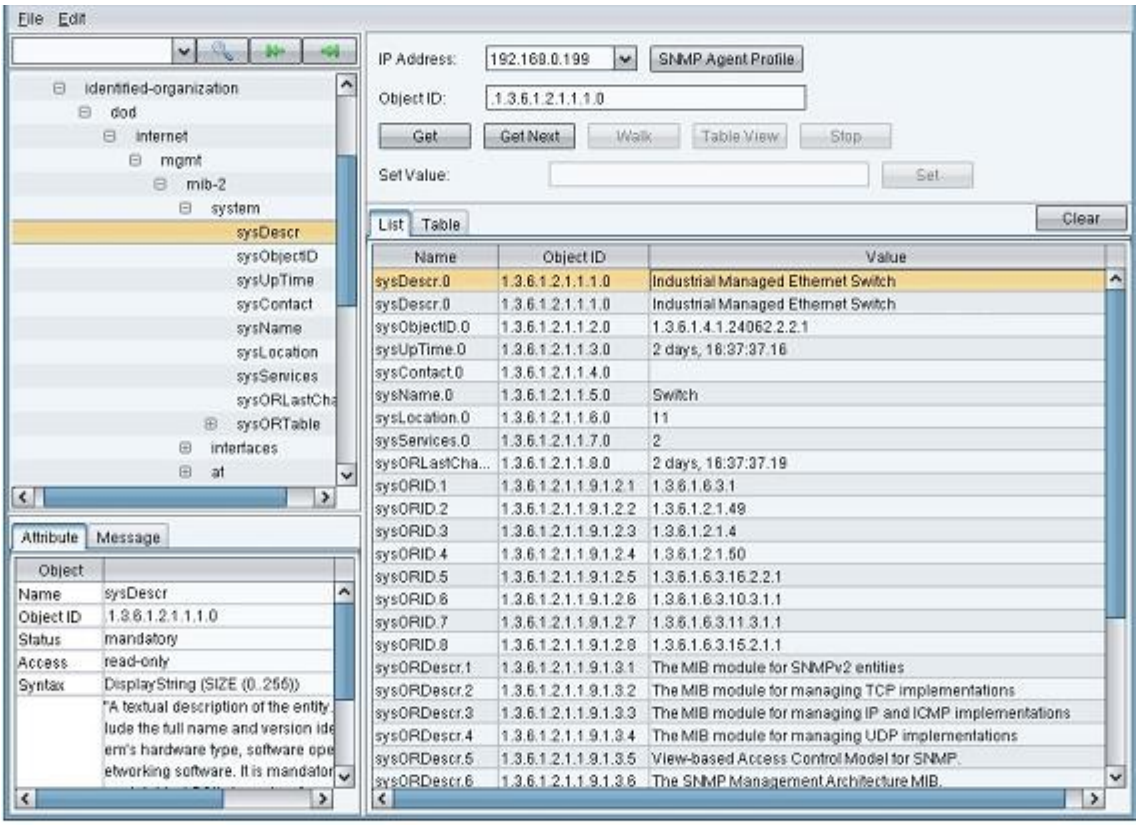


Figure 4–7. About Submenu

Toolbar Function

- **Find**, quickly find out the selected device by IP address
- **Edit Mode**, click on *Edit Mode* to enter into Edit mode by input password
- **Web Browser**, run Web browser to configure by Java Applet on switch device
- **SNMP** Browser, the SNMP Browser tool lets you read and write the MIB of the IP-Address device

For more information see the chapter Restore.



IP Address: 192.168.0.199

Object ID: .1.3.6.1.2.1.1.1.0

Set Value:

Object	
Name	sysDescr
Object ID	.1.3.6.1.2.1.1.1.0
Status	mandatory
Access	read-only
Syntax	DisplayString (SIZE (0..255))
	"A textual description of the entity. lude the full name and version ide em's hardware type, software ope etworking software. It is mandator

Name	Object ID	Value
sysDescr.0	1.3.6.1.2.1.1.1.0	Industrial Managed Ethernet Switch
sysDescr.0	1.3.6.1.2.1.1.1.0	Industrial Managed Ethernet Switch
sysObjectID.0	1.3.6.1.2.1.1.2.0	1.3.6.1.4.1.24062.2.2.1
sysUpTime.0	1.3.6.1.2.1.1.3.0	2 days, 16:37:37.16
sysContact.0	1.3.6.1.2.1.1.4.0	
sysName.0	1.3.6.1.2.1.1.5.0	Switch
sysLocation.0	1.3.6.1.2.1.1.6.0	11
sysServices.0	1.3.6.1.2.1.1.7.0	2
sysORLastCha...	1.3.6.1.2.1.1.8.0	2 days, 16:37:37.19
sysORID.1	1.3.6.1.2.1.1.9.1.2.1	1.3.6.1.6.3.1
sysORID.2	1.3.6.1.2.1.1.9.1.2.2	1.3.6.1.2.1.49
sysORID.3	1.3.6.1.2.1.1.9.1.2.3	1.3.6.1.2.1.4
sysORID.4	1.3.6.1.2.1.1.9.1.2.4	1.3.6.1.2.1.50
sysORID.5	1.3.6.1.2.1.1.9.1.2.5	1.3.6.1.6.3.16.2.2.1
sysORID.6	1.3.6.1.2.1.1.9.1.2.6	1.3.6.1.6.3.10.3.1.1
sysORID.7	1.3.6.1.2.1.1.9.1.2.7	1.3.6.1.6.3.11.3.1.1
sysORID.8	1.3.6.1.2.1.1.9.1.2.8	1.3.6.1.6.3.15.2.1.1
sysORDescr.1	1.3.6.1.2.1.1.9.1.3.1	The MIB module for SNMPv2 entities
sysORDescr.2	1.3.6.1.2.1.1.9.1.3.2	The MIB module for managing TCP implementations
sysORDescr.3	1.3.6.1.2.1.1.9.1.3.3	The MIB module for managing IP and ICMP implementations
sysORDescr.4	1.3.6.1.2.1.1.9.1.3.4	The MIB module for managing UDP implementations
sysORDescr.5	1.3.6.1.2.1.1.9.1.3.5	View-based Access Control Model for SNMP.
sysORDescr.6	1.3.6.1.2.1.1.9.1.3.6	The SNMP Management Architecture MIB.

Figure 4–8. Example of Reading a MIB

- **Scan Network**, find out specified IP range assigned
- **Fast Scan**, find out all switch devices by the View protocol
- **Preferences** please refer to section 9 for more information
- **Zoom**, zoom in and out the device icons, texts and others only on the Topology tab

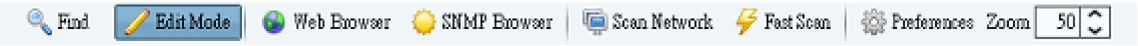
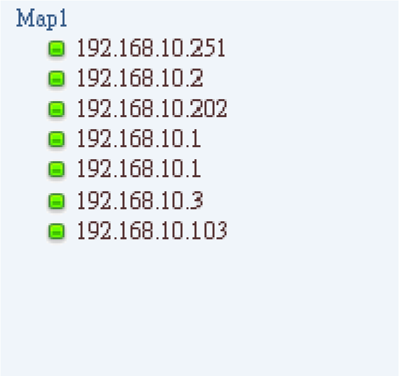


Figure 4–9. Toolbar Function

Map Tree

Click on the tree node to select the device on the *Topology* tab.



Map1
- 192.168.10.251
- 192.168.10.2
- 192.168.10.202
- 192.168.10.1
- 192.168.10.1
- 192.168.10.3
- 192.168.10.103

Figure 4–10. Map Tree

Topology Tab

This page displays the icons for monitored devices.

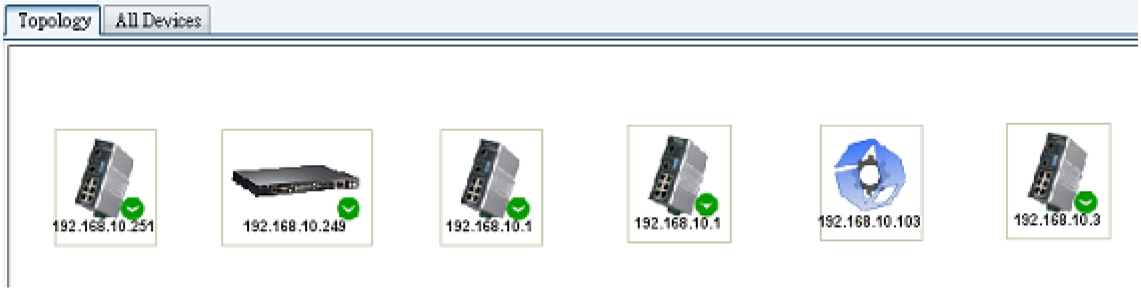
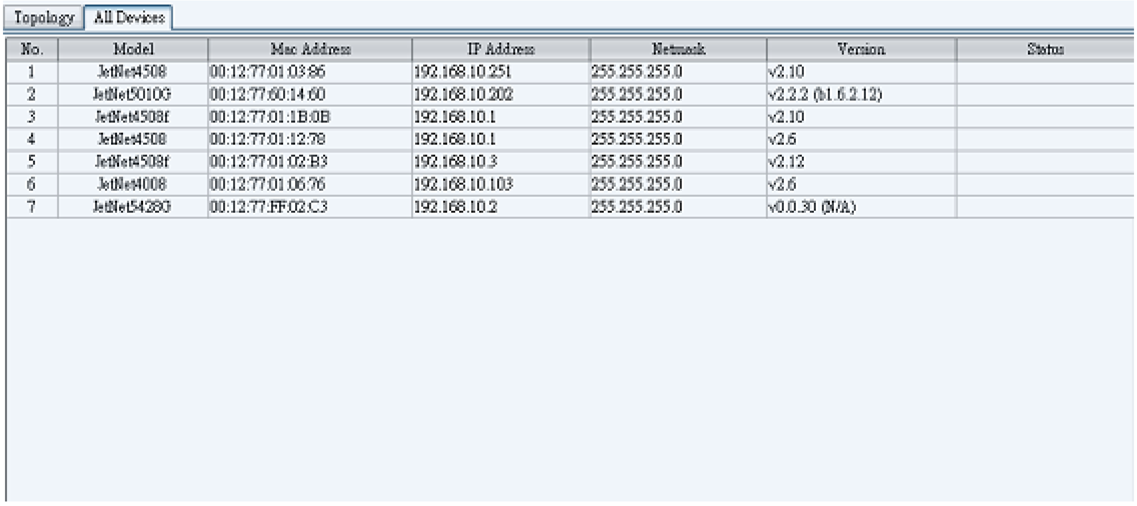


Figure 4–11. Topology in JetView Pro

All Devices Tab

This page displays the icons for monitored devices (as *Topology* tab)

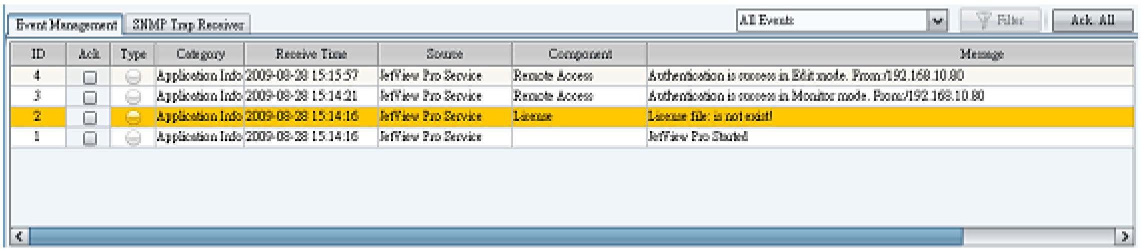


No.	Model	Mac Address	IP Address	Netmask	Version	Status
1	JetNet4508	00:12:77:01:03:86	192.168.10.251	255.255.255.0	v2.10	
2	JetNet5010G	00:12:77:60:14:60	192.168.10.202	255.255.255.0	v2.2.2 (b1.6.2.12)	
3	JetNet4508f	00:12:77:01:1B:0B	192.168.10.1	255.255.255.0	v2.10	
4	JetNet4508	00:12:77:01:12:78	192.168.10.1	255.255.255.0	v2.6	
5	JetNet4508f	00:12:77:01:02:B3	192.168.10.3	255.255.255.0	v2.12	
6	JetNet4008	00:12:77:01:06:76	192.168.10.103	255.255.255.0	v2.6	
7	JetNet5428G	00:12:77:FF:02:C3	192.168.10.2	255.255.255.0	v0.0.30 (N/A)	

Figure 4–12. All Devices Tab in JetView Pro

Event Management Tab

The event displays on the Event Management tab page while the event happens.

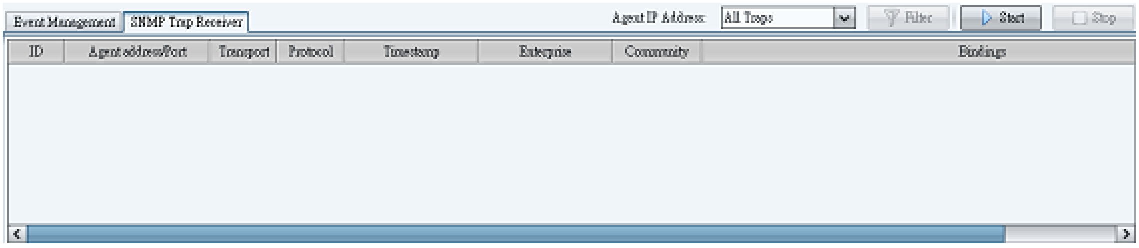


ID	Ack	Type	Category	Receive Time	Source	Component	Message
4	□	○	Application Info	2009-08-28 15:15:57	JetView Pro Service	Remote Access	Authentication is success in Edit mode. From:/192.168.10.80
3	□	○	Application Info	2009-08-28 15:14:21	JetView Pro Service	Remote Access	Authentication is success in Monitor mode. From:/192.168.10.80
2	□	●	Application Info	2009-08-28 15:14:16	JetView Pro Service	License	License file: is not exist!
1	□	○	Application Info	2009-08-28 15:14:16	JetView Pro Service		JetView Pro Started

Figure 4–13. Event Management

SNMP Trap Receiver Tab

The SNMP trap displays on the SNMP Trap Receiver tab page while the trap happens. The SNMP Trap Receiver support SNMP v1/v2c traps receiving.



ID	Agent address/Port	Transport	Protocol	Timestamp	Enterprise	Community	Bindings

Figure 4–14. SNMP Trap Receiver Tab

5. Device Discovery

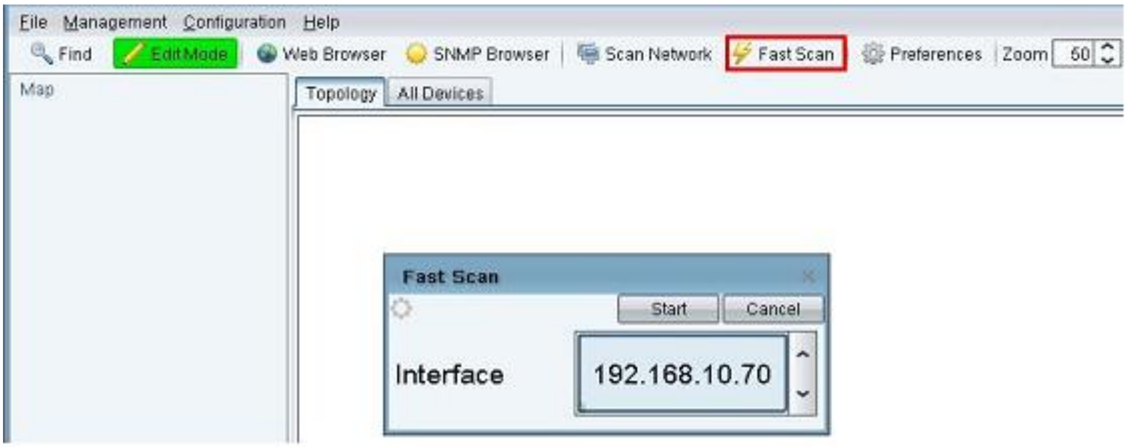
To see the installed devices on the Topology tab or the All Devices tab, you have to add devices. How to do add devices and delete devices? How to quickly update the installed devices? This section gives answers to all the above questions.

Add Devices

Fast Scan

This function is to discovery devices using the View protocol in the local network. JetView Pro discovers all network devices on the subnet network via the selected interface on the PC. This function adapts to setup a newly installed network.

To update installed network components (or devices), click on *Fast Scan* on the toolbar and select one of your NIC which connect to network devices.



Interface 192.168.10.70

Figure 5–1. Fast Scan Option

It displays all Connect devices in the network on the Topology tab.

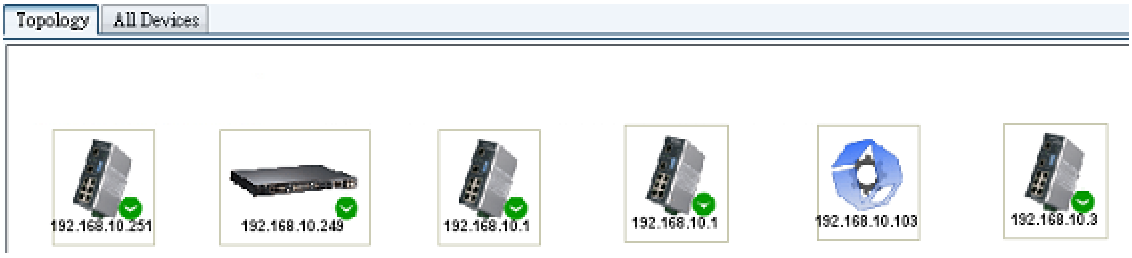


Figure 5–2. Topology Tab

Scan Network

This function is to discovery devices via the assigned IP address range. While you want to add the specified IP-enabled device, this function is suitable.

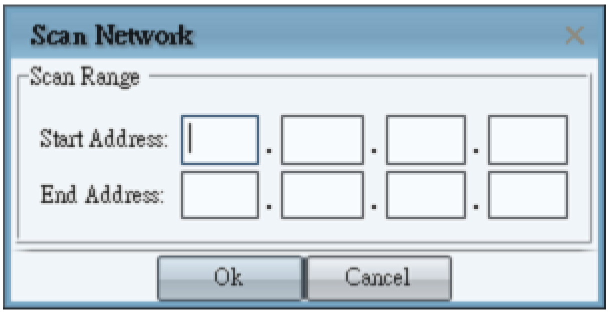


Figure 5–3. Scan Address Range

Note:

The *End Address* should great or equal then *Start Address*.

Delete Devices

You can delete any device on Topology tab. Use the mouse to select multiple devices by CTRL key and right-click the selected device. Then display a pop-up menu and click on *Delete* menu item.

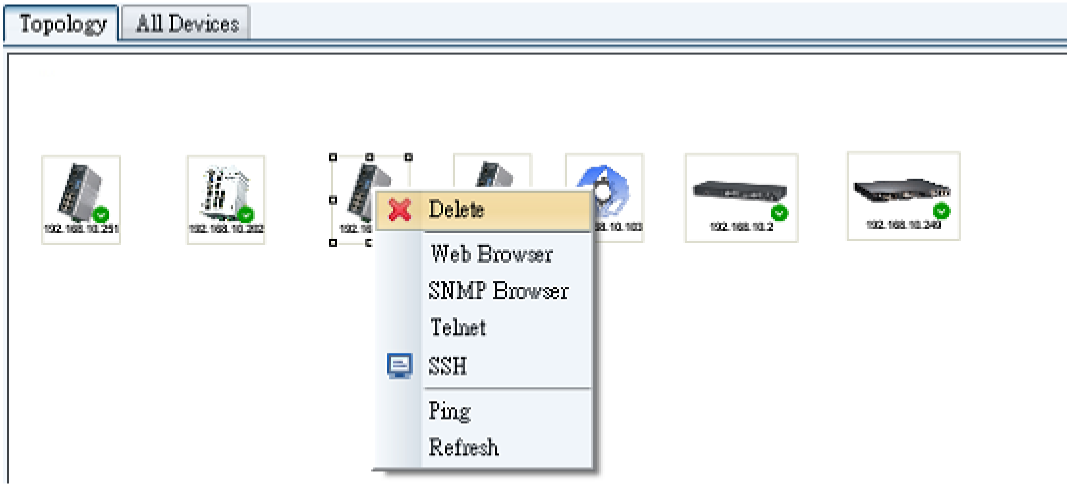


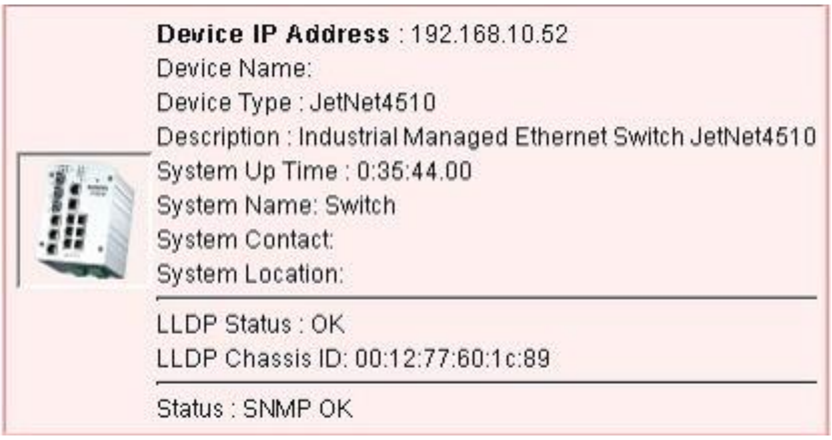
Figure 5–4. Deleting a Device from Topology Tab

6. Topology Map

Device Information

Device Status

Move mouse cursor over the switch device icon on Topology tab. It will show the following status for the device.



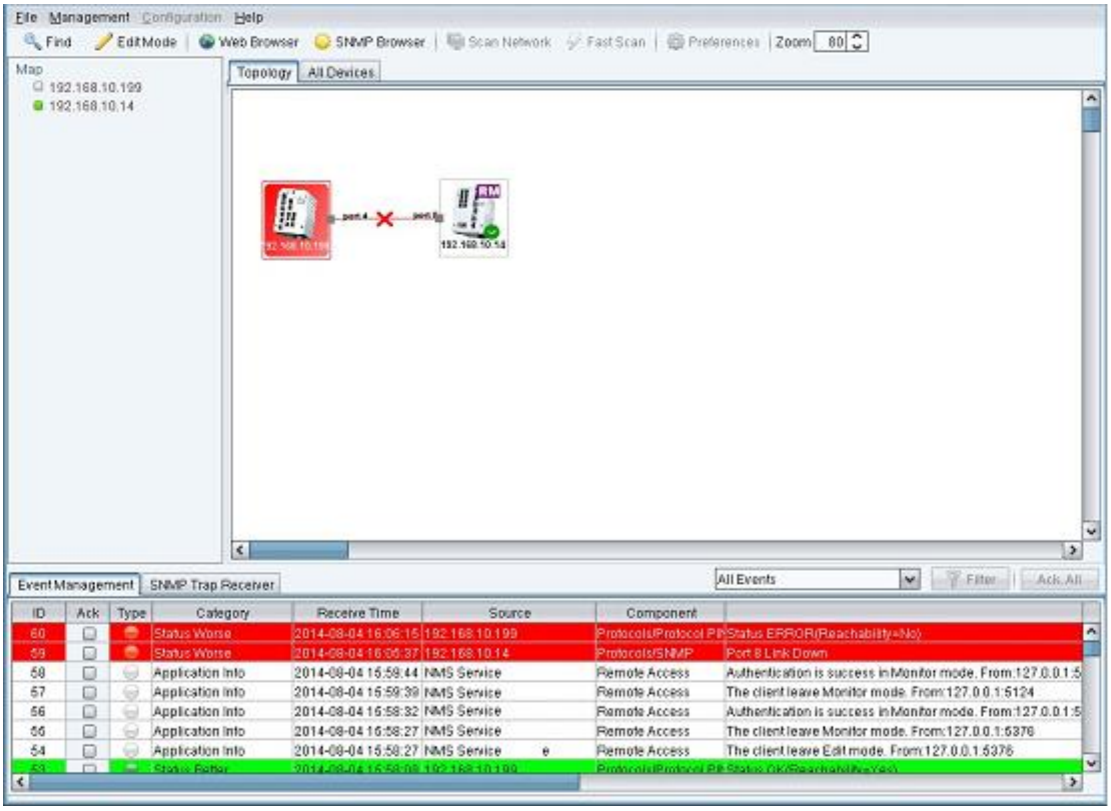
Device IP Address : 192.168.10.52
Device Name:
Device Type : JetNet4510
Description : Industrial Managed Ethernet Switch JetNet4510
System Up Time : 0:35:44.00
System Name: Switch
System Contact:
System Location:

LLDP Status : OK
LLDP Chassis ID: 00:12:77:60:1c:89

Status : SNMP OK

Figure 6–1. Device Status

The device (IP address: 192.168.10.1) lists in left tree panel with a status icon use to show its online/offline status. Green means online, while white means offline. The device icon on Topology tab also shows its status in the background. If the color is red, which indicates an error status (hint: the detail is in Event management tab). In other words, JetView Pro sends ICMP Ping request and then receives incorrect response (unreachable).



ID	Ack	Type	Category	Receive Time	Source	Component	
60	□	●	Status Worse	2014-08-04 16:06:15	192.168.10.199	Protocols/Protocol PI	Status ERROR(Reachability=No)
59	□	●	Status Worse	2014-08-04 16:05:37	192.168.10.14	Protocols/SNMP	Port 8 Link Down
58	□	○	Application Info	2014-08-04 15:59:44	NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
57	□	○	Application Info	2014-08-04 15:59:39	NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5124
56	□	○	Application Info	2014-08-04 15:58:32	NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
55	□	○	Application Info	2014-08-04 15:58:27	NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5376
54	□	○	Application Info	2014-08-04 15:58:27	NMS Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5376
53	□	●	Status Better	2014-08-04 15:58:08	192.168.10.199	Protocols/Protocol PI	Status OK(Reachability=Yes)

Figure 6–2. Connecting to Device

There is a green check indicates the normal status for SNMP.

Device Refresh

To update the device status, select one more device (especially on error status) and right-click mouse on the selected device. Then pop up as follows:

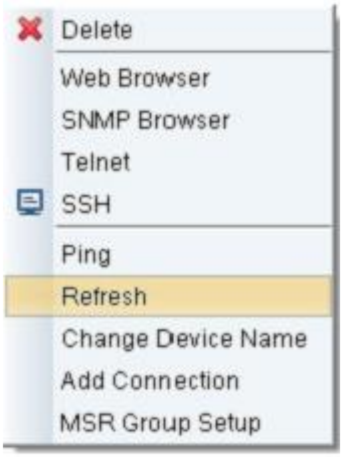


Figure 6–3. Device Refreshing List

Deleting Devices

To remove the device nodes, select one or one more devices and right-click mouse on the selected device. Then pop up as follows:

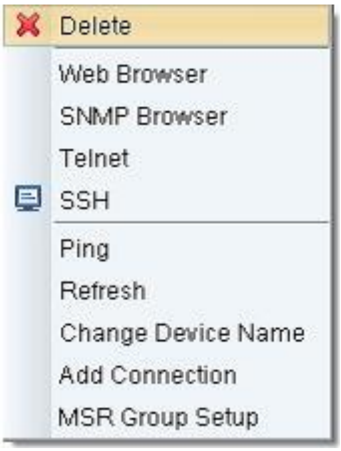


Figure 6–4. Deleting Selected Device

Managing Devices

To manage the devices, select one device and right-click mouse on the selected device. It will pop up a dialog as follows. Choose to use Web Browser, SNMP Browser, Telnet, SSH, or Ping to manage the device.

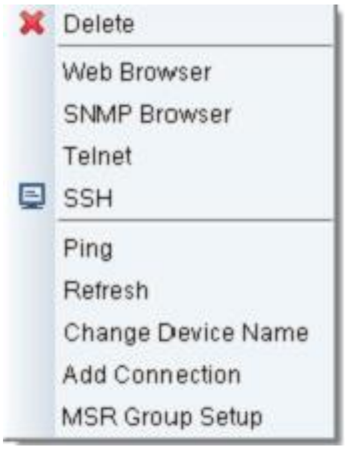


Figure 6–5. Options for Device Management

Auto Topology

The *Auto Topology* function allows you to automatically create the links (connections) between the devices (nodes). To support this function, the devices must support with LLDP and SNMP. LLDP enables the user to have automatic topology recognition for his LAN. Therefore the devices support for LLDP and SNMP and have to be configured to ready state.

Enable LLDP

To let *Auto Topology* working, each device MUST enable LLDP function on installed network devices. You can use Web browser to confirm whether LLDP is enabled.

1. Use mouse to select one device on the *Topology* tab which you want to enable as LLDP
2. Mouse right-click on the selected device and click on the Web Browser menu-item of pop-up menu

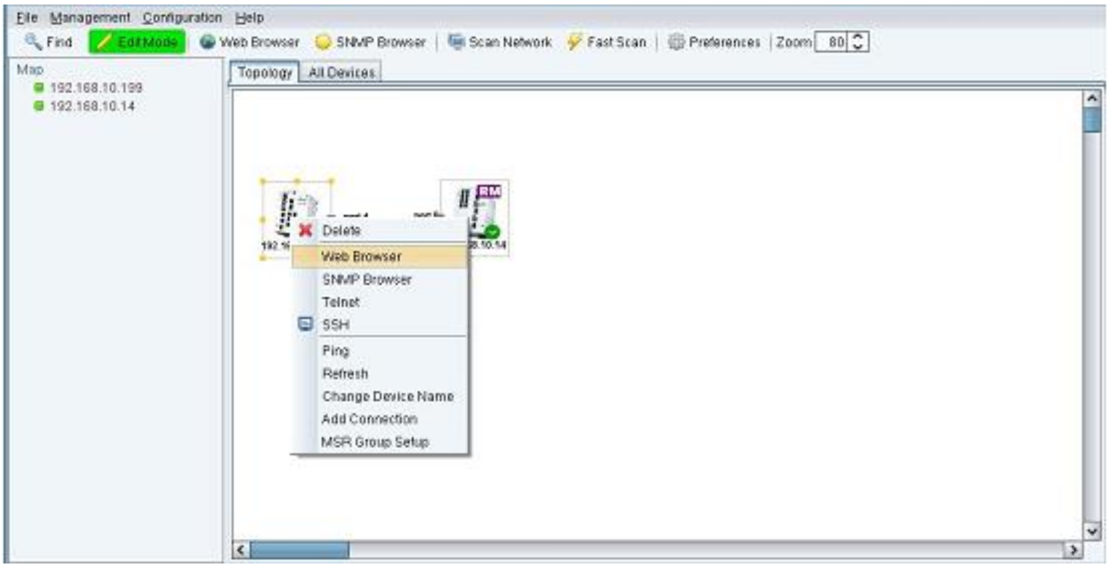
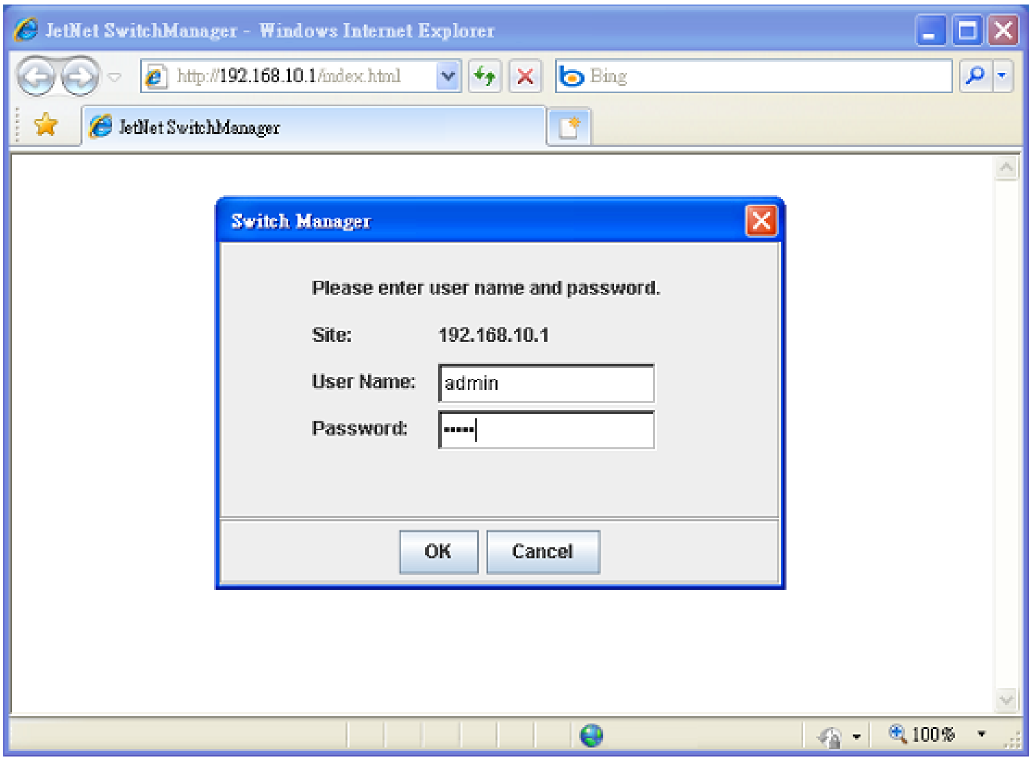


Figure 6–6. Step 2 to Enable LLDP

3. When the login screen appears, login with the user name and password (default Username and Password is admin/admin).


JetNet SwitchManager - Windows Internet Explorer
http://192.168.10.1/index.html
Bing
JetNet SwitchManager
Switch Manager
OK
Cancel
100%

Please enter user name and password.

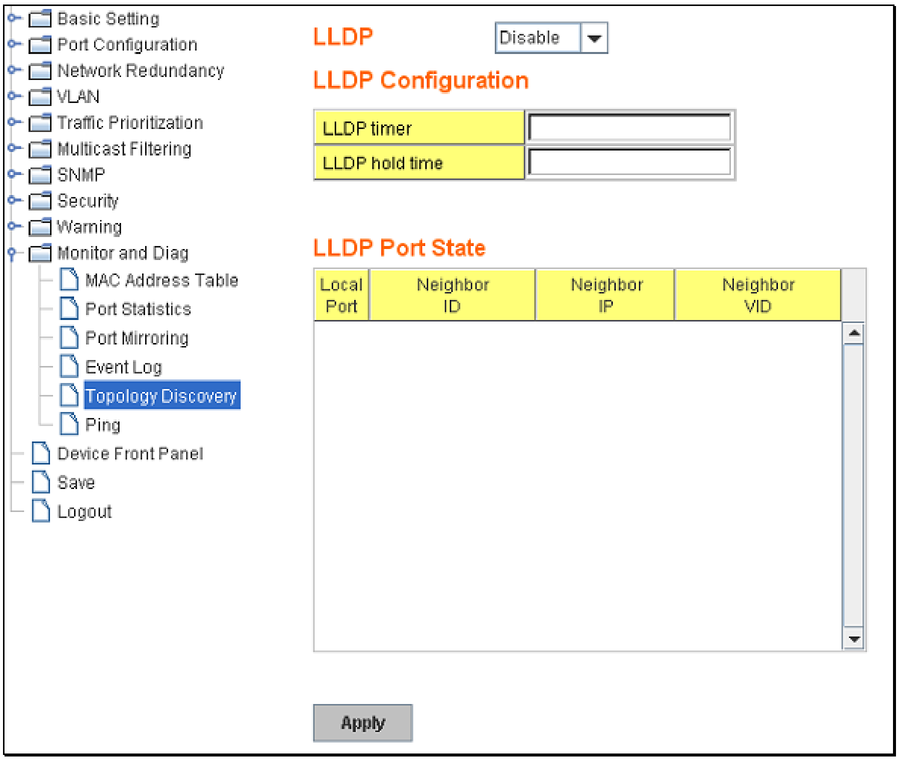
Site: 192.168.10.1

User Name: admin

Password: •••••

Figure 6–7. Step 3 to Enable LLDP

4. Click on the tree node *Topology Discovery*.



LLDP: Disable

LLDP Configuration

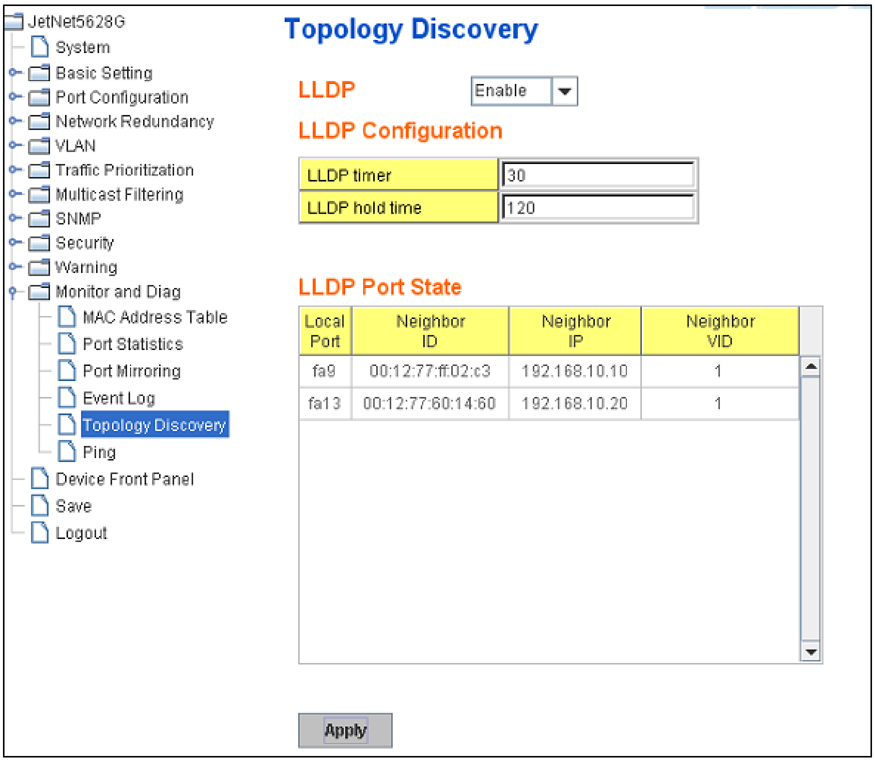
LLDP timer	
LLDP hold time	

LLDP Port State

Local Port	Neighbor ID	Neighbor IP	Neighbor VID

Figure 6–8. Step 4 to Enable LLDP

5. Confirm whether LLDP is enabled. If it is disabled, please set Enable and press *Apply*. You can manual set the timers of LLDP. The range of LLDP timer is 5~254 and LLDP hold time is 10~255.



Topology Discovery

LLDP: Enable

LLDP Configuration

LLDP timer	30
LLDP hold time	120

LLDP Port State

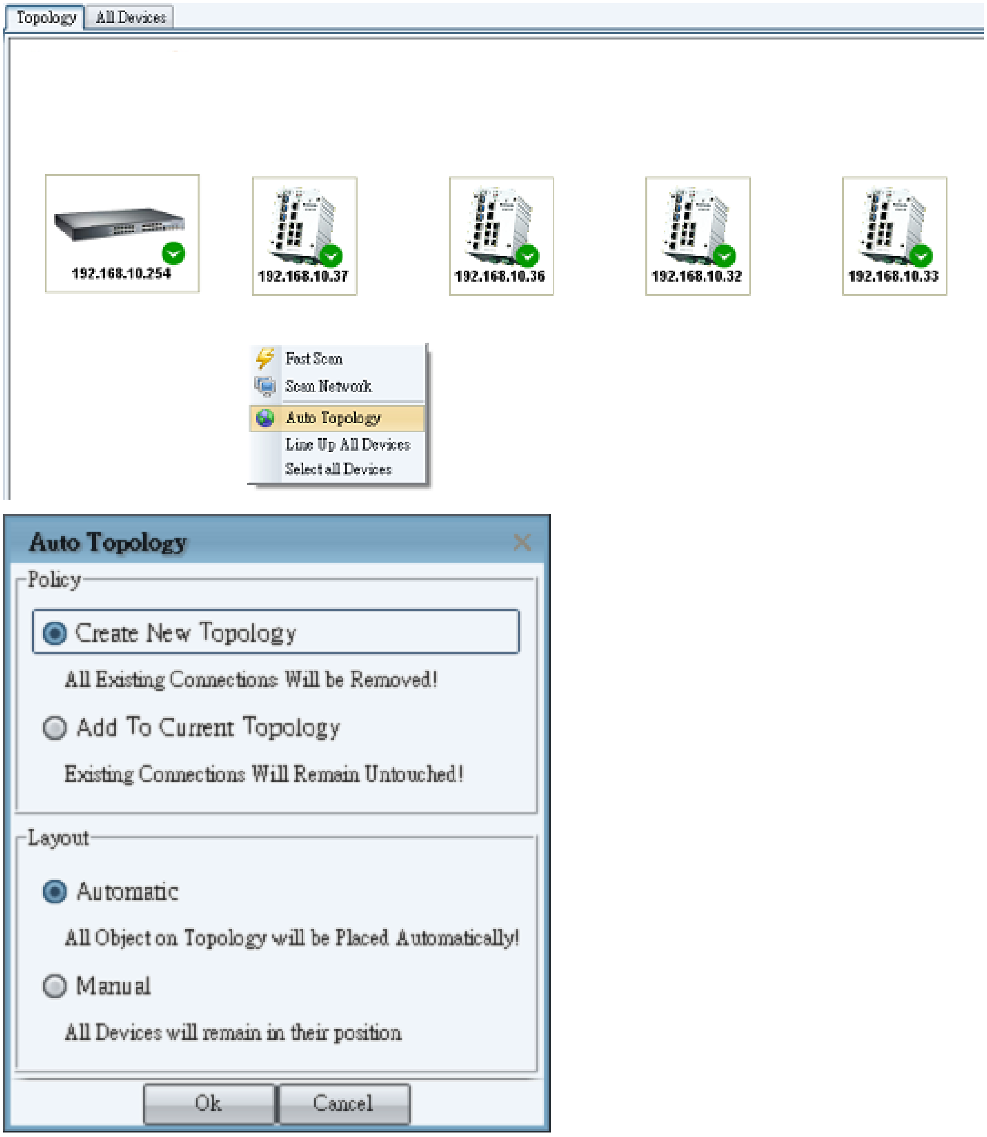
Local Port	Neighbor ID	Neighbor IP	Neighbor VID
fa9	00:12:77:ff:02:c3	192.168.10.10	1
fa13	00:12:77:60:14:60	192.168.10.20	1

Figure 6–9. Step 5 to Enable LLDP

Generate Connections

Generate connections between the devices.

1. Check every device’s icon that each one has a green check ✓ on it. Device icon without check icon can’t access by SNMP.
2. Mouse right-click on the *Topology* tab and click on *Auto Topology* on pop-up menu. It will display as follows:



Auto Topology

Policy

● Create New Topology

All Existing Connections Will be Removed!

○ Add To Current Topology

Existing Connections Will Remain Untouched!

Layout

● Automatic

All Object on Topology will be Placed Automatically!

○ Manual

All Devices will remain in their position

Figure 6–10. Auto Topology Configuration

3. Press *OK* to display the following of screen.

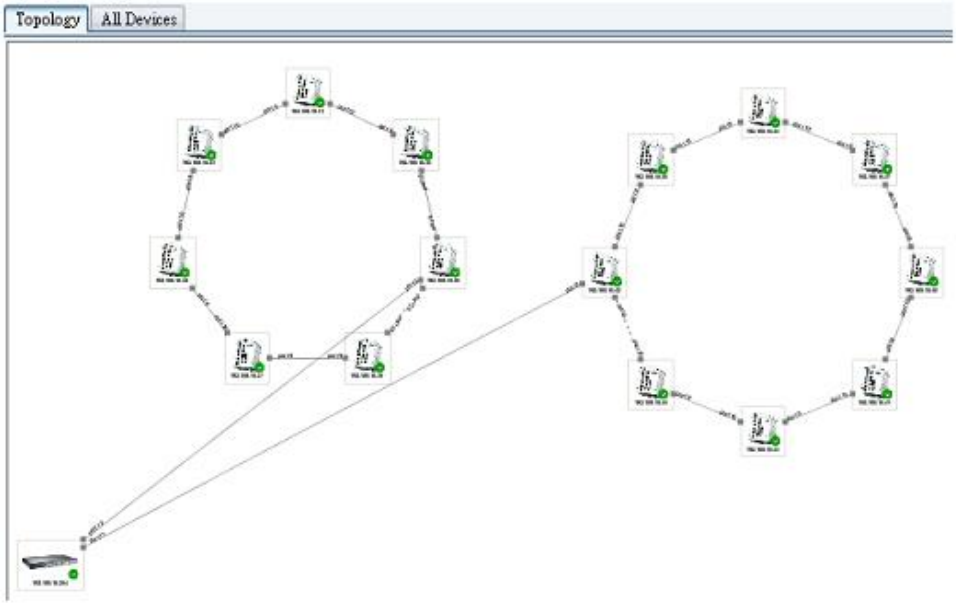


Figure 6–11. Auto Topology Map

Auto Topology Check List:

Yes / No	Requirement
?	Does every device enable SNMP?
?	Does any device not using default SNMP community? (Public, private)
?	Does every device's icon show green?
?	Does every device enable LLDP?
?	If the device show red (not reachable), after you fix the problem, did you refresh the device?

Note:

The L3 interface (IP interface) may not be displayed correctly in the version of JetView Pro v1.6.x.

Manual Add Connection and Delete

Manual Add Connection

Select two switch icons and mouse right-click to show popup menu.

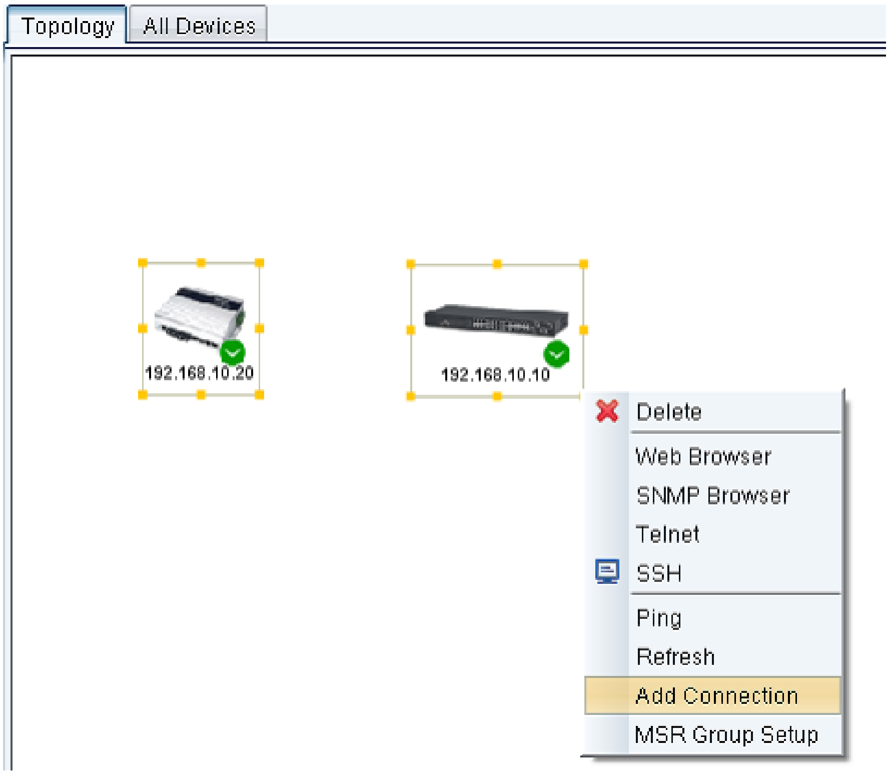
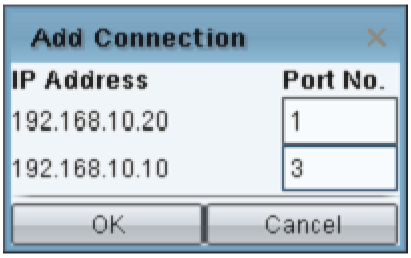


Figure 6–12. Adding a Connection Manually

Click on *Add Connection* menu item of the pop menu. It will show this Add Connection dialog. Enter two port number connected between two switches and press *OK*.


Add Connection

IP Address	Port No.
192.168.10.20	1
192.168.10.10	3

Figure 6–13. Add Connection Parameters

The screen will display that there is a connection between two switches.

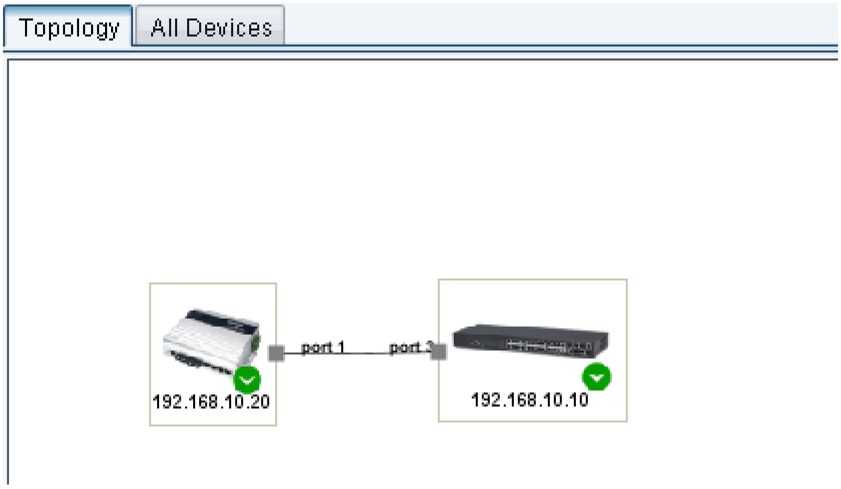


Figure 6–14. Connection Established Manually

Manual Delete Connection

Select the connection between 192.168.10.20 and 192.168.10.10 by Mouse-Click.

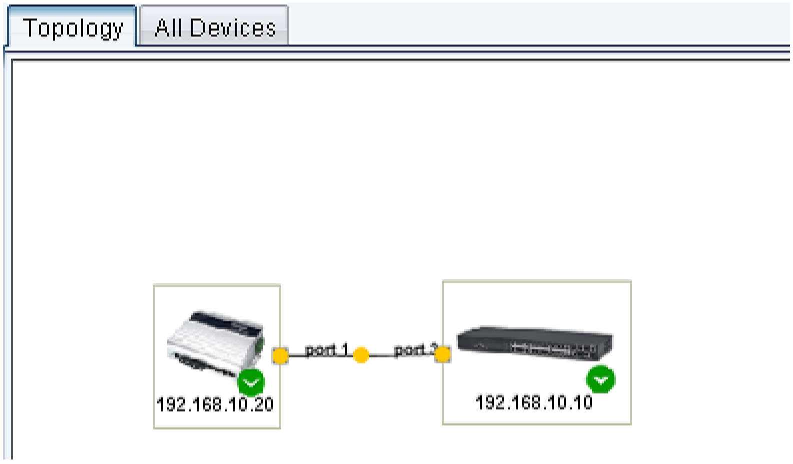


Figure 6–15. Deleting Connection Manually Step 1

Mouse Right-Click the connection and pop up *Delete* menu-item of pop-up menu.

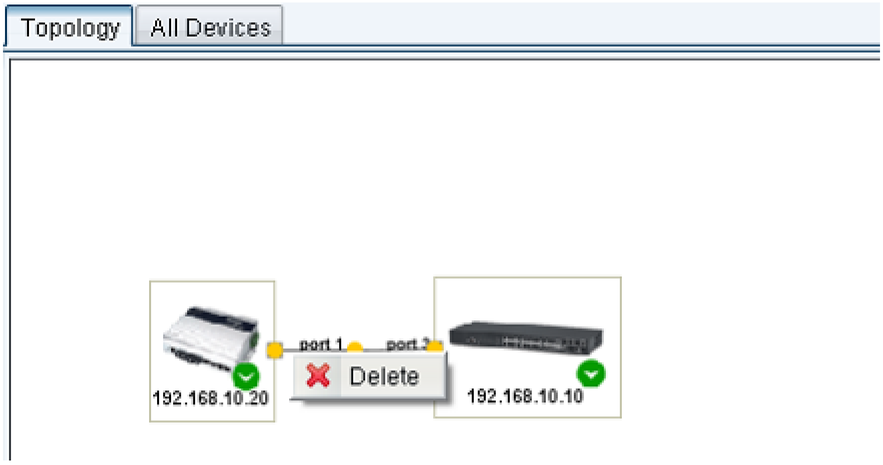


Figure 6–16. Deleting Connection Manually Step 2

Click *Delete* to delete the connection.

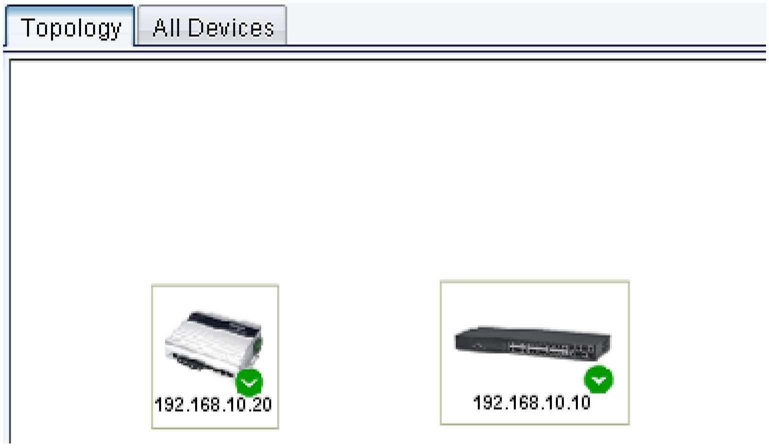


Figure 6–17. Deleting Connection Manually Step 3

Save Topology Map

To present to *Topology Map*, you could need to get topology map.

Save Topology Map as File

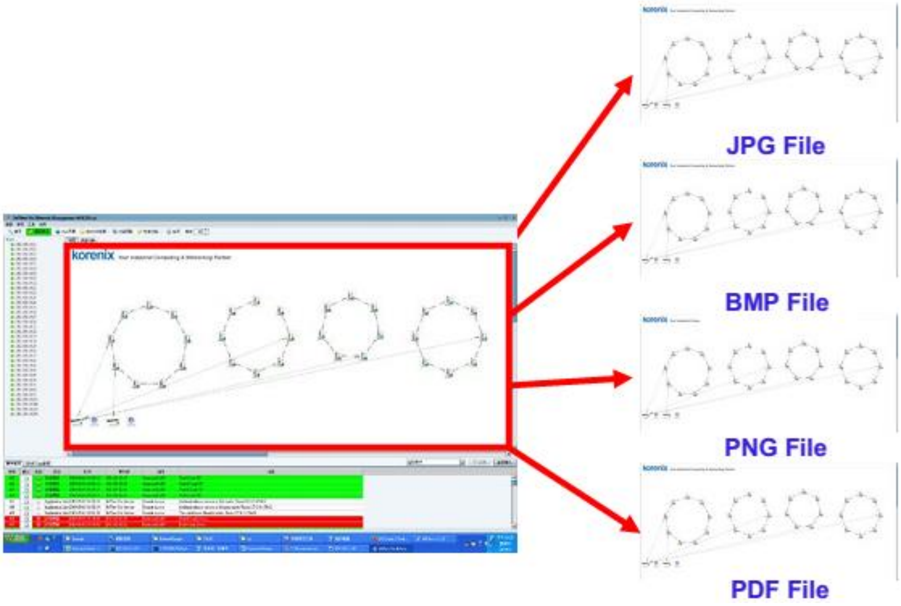
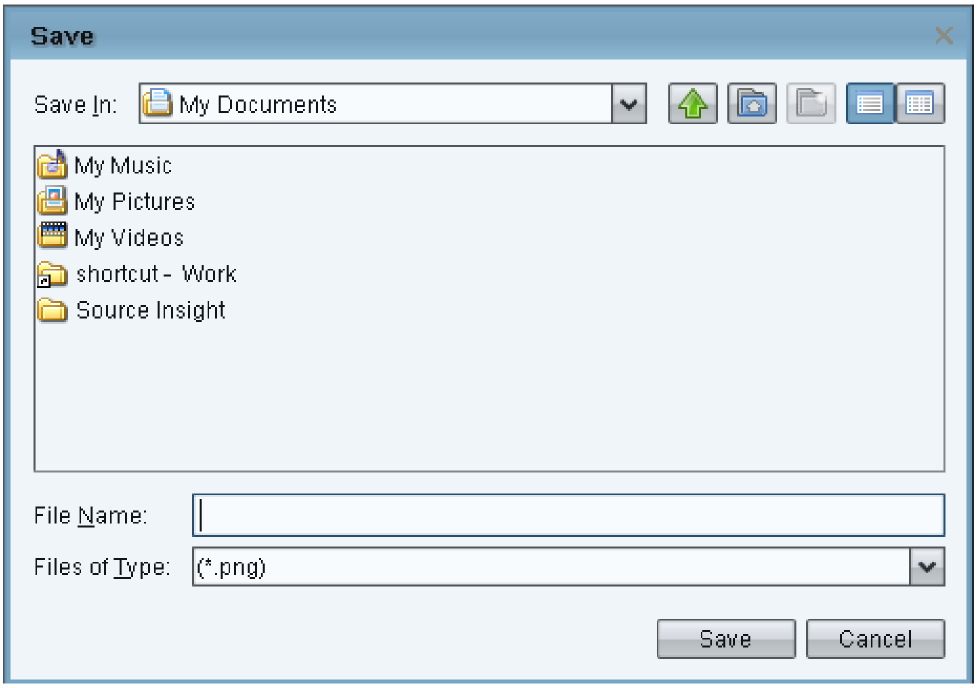


Figure 6–18. Saving Topology Map as File

These two methods can help you save currently displayed map in the Topology Map to file.

1. Image format file (BMP, JPEG, PNG). Click on *File / Export*, choose *File of Type* to use BMP, JPEG, PNG image format, Input File Name and press *Save* to save the file.



Save

Save In: My Documents

My Music
My Pictures
My Videos
shortcut - Work
Source Insight

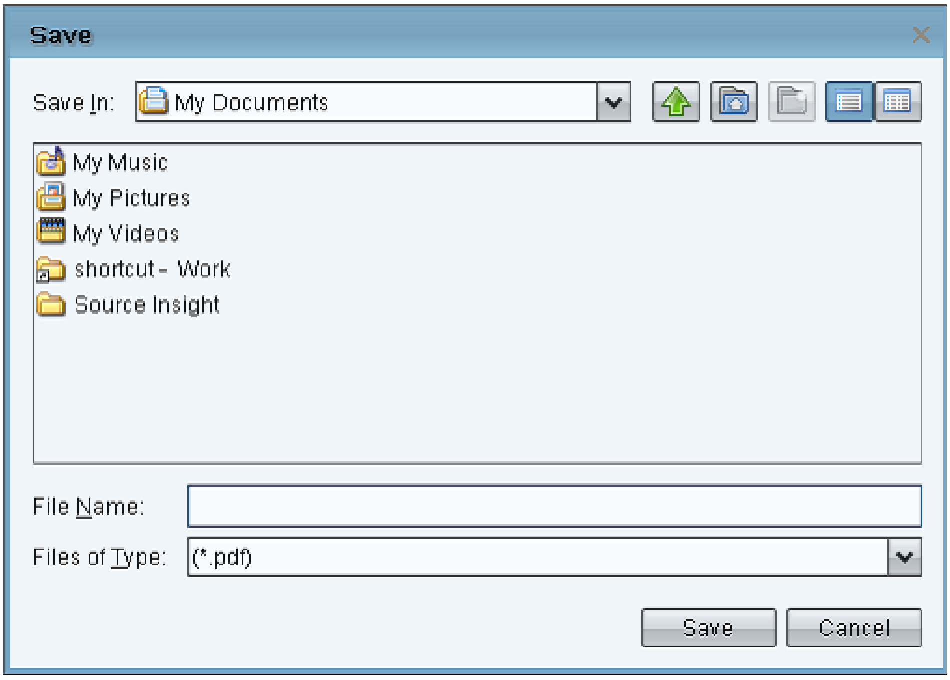
File Name:

Files of Type: (*.png)

Save Cancel

Figure 6–19. Save Topology as File Options

2. PDF file. Click on *File / Print*. Input File Name and press *Save* to save the file.



Save In: My Documents

File Name:

Files of Type: (*.pdf)

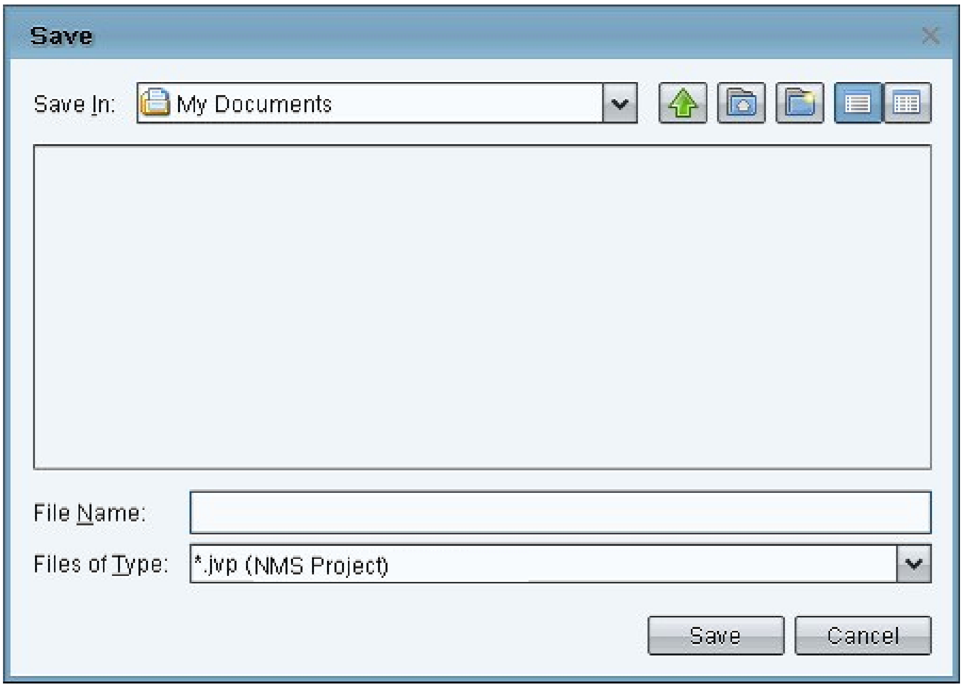
Figure 6–20. Save Topology as PDF

A PDF file will be generated. You can print it with the print function of your PDF viewer.

Save Topology Map as Database File (*.JVP)

To record current displayed map in the *Topology Map*, use this map again. First, you need to save Topology Map as database file.

Click on *File / Save*. Input *File Name* and press *Save* to save the file. (ex. demo.JVP)



Save In: My Documents

File Name:

Files of Type: *.jvp (NMS Project)

Figure 6–21. Save Topology as JVP

To restore previous saved Topology Map, you click on *File / Open*.

Set File Name (ex. demo.JVP) and press *Open* to restore previous saved Topology Map.

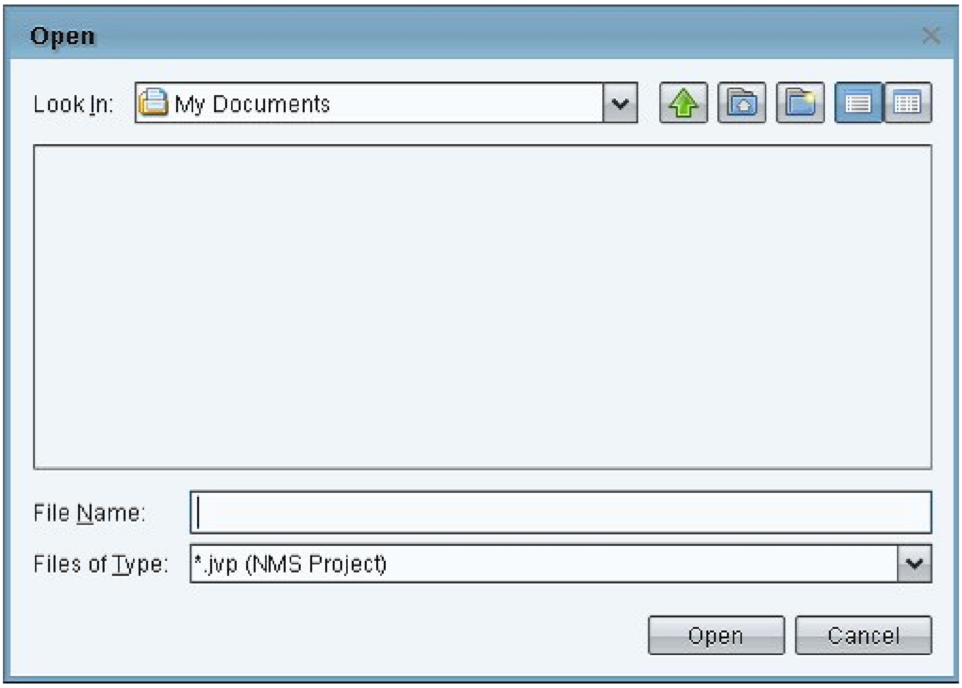


Figure 6–22. Opening Previous Saved File

Note:

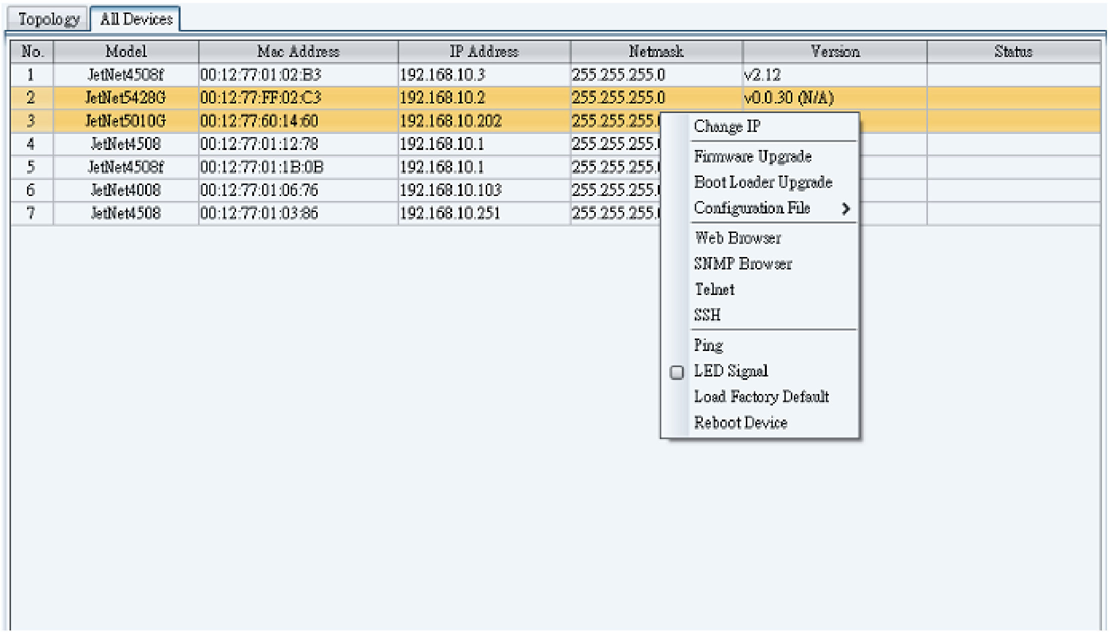
This function only available on server. Remote client can’t backup/restore database due to security precautions.

7. Device Configuration

This section explains the device configuration on the *All Devices* Tab. One switch device can be configured by one mouse selection. Group devices can also be configured by many selections at a time.

The methods of mouse selection can be single selected any rows by CTRL + mouse click or continuously selected by first mouse click and then SHIFT + mouse click. Remember that first mouse select the switch devices to configure before the following of device configurations.

After having one more devices selections, show pop-up menu by mouse right-click.



No.	Model	Mac Address	IP Address	Netmask	Version	Status
1	JetNet4508f	00:12:77:01:02:B3	192.168.10.3	255.255.255.0	v2.12	
2	JetNet5428G	00:12:77:FF:02:C3	192.168.10.2	255.255.255.0	v0.0.30 (N/A)	
3	JetNet5010G	00:12:77:60:14:60	192.168.10.202	255.255.255.		
4	JetNet4508	00:12:77:01:12:78	192.168.10.1	255.255.255.		
5	JetNet4508f	00:12:77:01:1B:0B	192.168.10.1	255.255.255.		
6	JetNet4008	00:12:77:01:06:76	192.168.10.103	255.255.255.		
7	JetNet4508	00:12:77:01:03:86	192.168.10.251	255.255.255.		

Figure 7–1. Device Options

Note:

Before using pop-up menu functions, remember to select the target device (mouse selection) that should be configured.

Global Settings

Change IP

You can assign the new IP address to the switch devices.

LED Signal

This function is convenient for searching the switch device. While this function is enabled, the light of the LED on the switch device constantly twinkles.

Load Factory Default

You can reset all the configurations of the switch to default setting.

Reboot Device

Some of the feature change to require you rebooting the system. Click on *Reboot Device* on pop-menu to reboot your device.

MSR Group Setup

To let *Auto Topology* to generate Ring Topology, devices in the install ring network have to setup Multiple Super Ring (MSR) function.

1. Use mouse right click to select multiple devices on the Topology tab by CTRL key which you want to setup MSR function.
2. Mouse right-click on the selected device and click on the MSR Group Setup menu-item of pop-up menu.

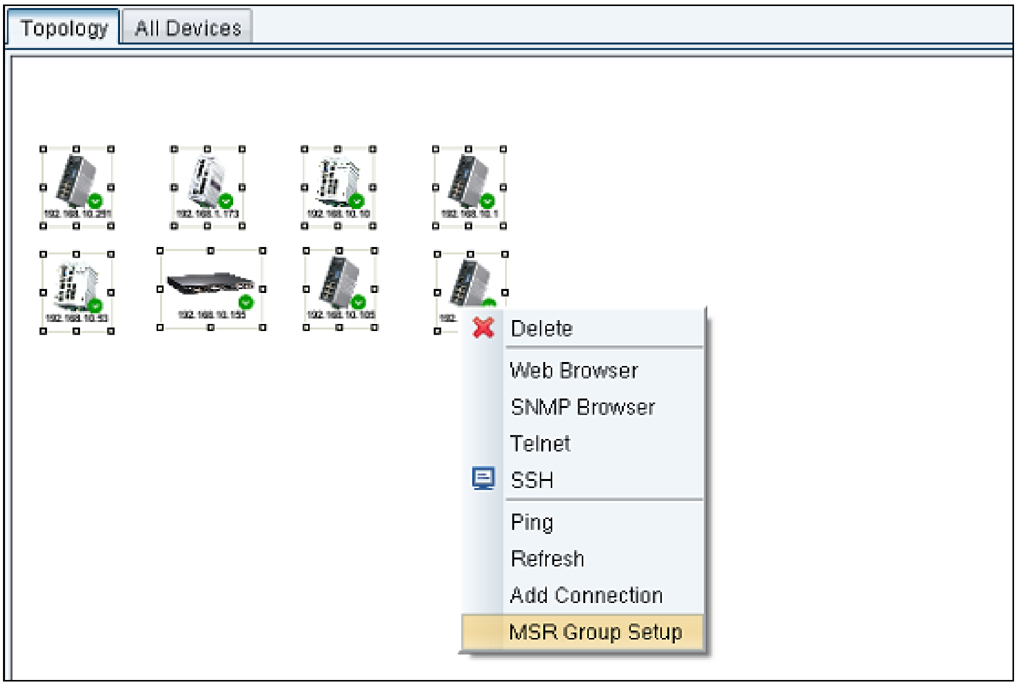
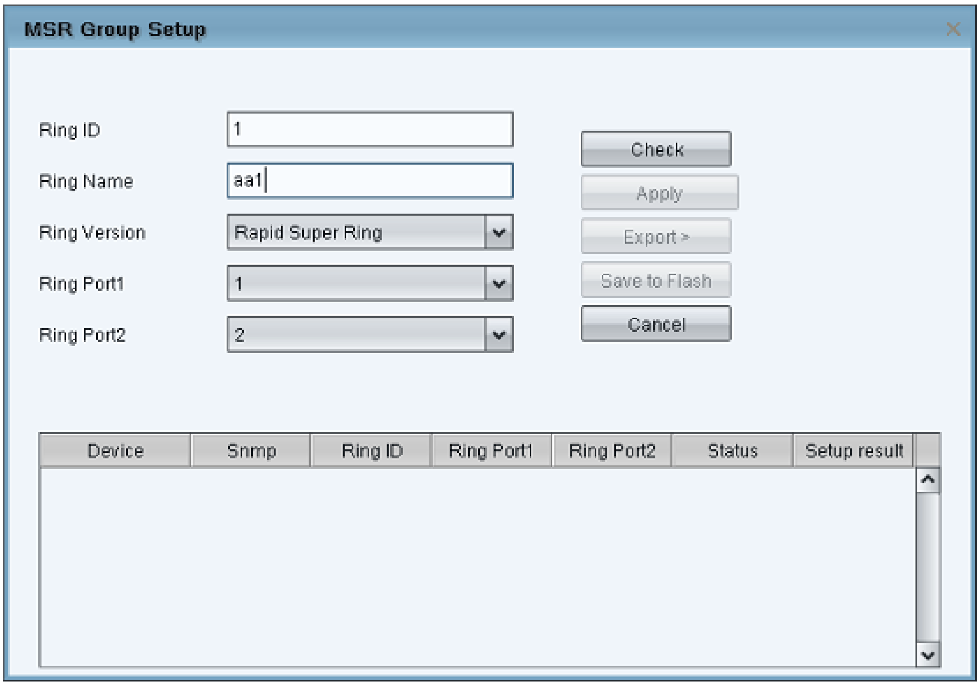


Figure 7–2. MSR Group Setup

3. It will show MSR Group Setup window. Set Ring ID (0~31), Ring Name, Ring Version, Ring Port1 and Ring Port2 for MSR setup. Then press *Check* button



MSR Group Setup

Ring ID: 1

Ring Name: aa1

Ring Version: Rapid Super Ring

Ring Port1: 1

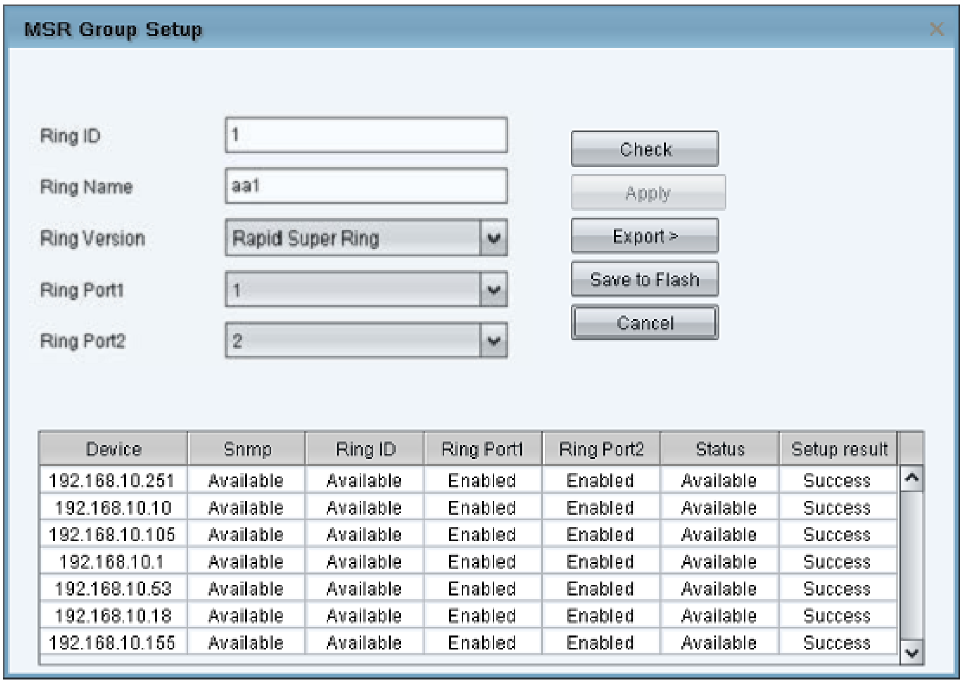
Ring Port2: 2

Device	Snmp	Ring ID	Ring Port1	Ring Port2	Status	Setup result

Figure 7–3. Options for MSR Groups Setup

4. It will show check status of selected device in the bottom of MSR Group Setup window. The columns in the table explain as follow:

   - Device: IP address
   - SNMP: Connect via SNMP is available
   - Ring ID: whether Ring ID is used or exceeds the ring number limit
   - Ring Port1: whether Ring Port1 is enabled or exceed the port number limit for device
   - Ring Port2: whether Ring Port2 is enabled or exceed the port number limit for device
   - Status: the device status based on the status of SNMP, RingID, Ring Port1, Ring Port2
   - Setup result: response this column after pressing Apply button



Ring ID: 1

Ring Name: aa1

Ring Version: Rapid Super Ring

Ring Port1: 1

Ring Port2: 2

Device	Snmp	Ring ID	Ring Port1	Ring Port2	Status	Setup result
192.168.10.251	Available	Available	Enabled	Enabled	Available	Success
192.168.10.10	Available	Available	Enabled	Enabled	Available	Success
192.168.10.105	Available	Available	Enabled	Enabled	Available	Success
192.168.10.1	Available	Available	Enabled	Enabled	Available	Success
192.168.10.53	Available	Available	Enabled	Enabled	Available	Success
192.168.10.18	Available	Available	Enabled	Enabled	Available	Success
192.168.10.155	Available	Available	Enabled	Enabled	Available	Success

Figure 7–4. Options for MSR Groups Setup for Selected Devices

5. To indicate that there is at least one of device in the unavailable status if the *Apply* is disabled. Press Check button again after solving the problem for unavailable devices. If all the selected devices are in the available status, the Apply button will enable. Then press Apply button to setup MSR setting for all selected devices. Final, the setup result will show the last column in the table.
6. If you want to use these settings for rebooted devices, you MUST press *Save to Flash* button to save these settings into flash for each devices.

Firmware Upgrade

In this section, you can update the latest firmware for your switch.. The new firmware may include new features, bug fixes or other software changes. We'll also provide the release notes for the update as well. For technical viewpoint, we suggest you use the latest firmware before installing the switch to the customer site.

The UI also shows you the version and built date of current firmware. Please check the version number after the switch is rebooted.

Note:

The system will be automatically rebooted after you finished upgrading new firmware/bootloader. Please remind the attached users before you do this.

Configure File Operation

The configuration file of the switch is a pure text file. You can open it by word/txt read file. You can also modify the file, add/remove the configuration settings, and then restore back to the switch.

Backup

With Backup function, you can save current configuration file saved in the switch's flash

Restore

This will allow you to go to Restore function later to restore the configuration file back to the switch.

Load default

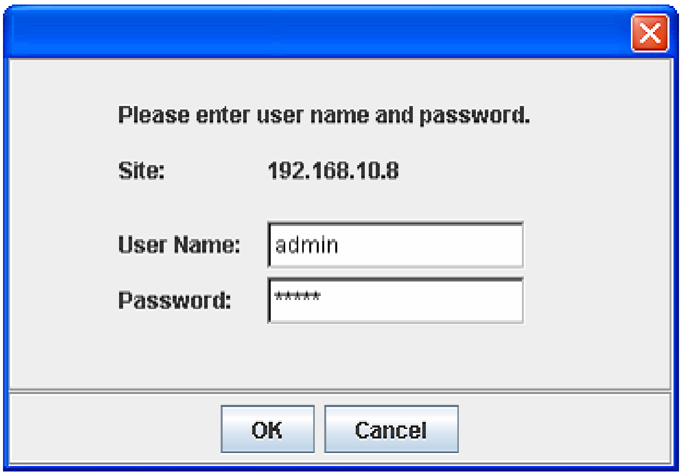
All of the configurations will be rollback to the factory default settings, except the device IP address.

Manage by Application

Web browser

For managing Ethernet switch devices, you need to consider that they have Web management function. Web management page is developed by JAVA. It allows you to use a standard Web-browser such as Microsoft Internet Explorer, or Mozilla, to configure and interrogate the switch from anywhere on the network.

1. Use mouse to select one device on the Topology tab which you want to configure
2. Mouse right-click the selected device and click on the *Web Browser* menu-item of pop-up menu
3. The login screen will appear next
4. Key in *user name* and the *password*. Default user name and password are both admin.



Please enter user name and password.

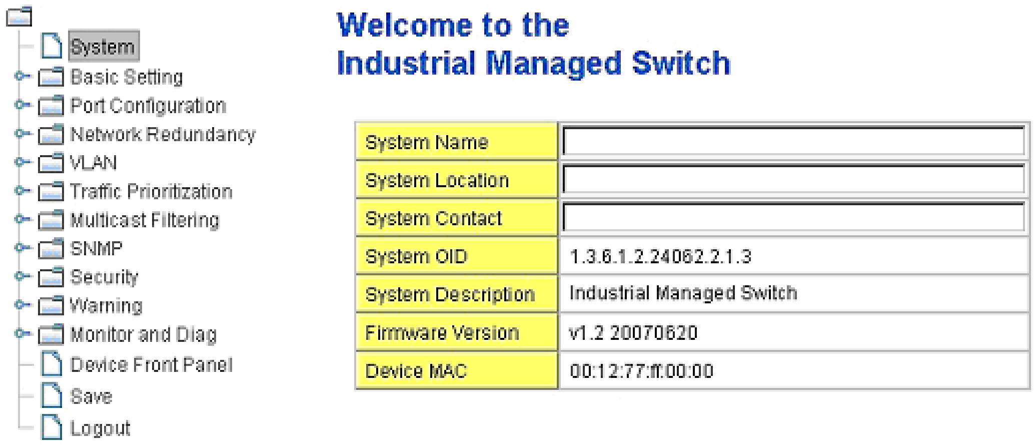
Site: 192.168.10.8

User Name: admin

Password: *****

Figure 7–5. Welcome Page of the Web-Based Management Interface

5. Press ENTER or click on *OK*. Welcome page of the Web-based management interface will then appear.



Welcome to the
Industrial Managed Switch

System Name	
System Location	
System Contact	
System OID	1.3.6.1.2.24062.2.1.3
System Description	Industrial Managed Switch
Firmware Version	v1.2 20070620
Device MAC	00:12:77:ff:00:00

Figure 7–6. Configurations of Industrial Managed Switch

6. Once you enter the Web-based management interface, you can freely change the IP address to fit your network environment.

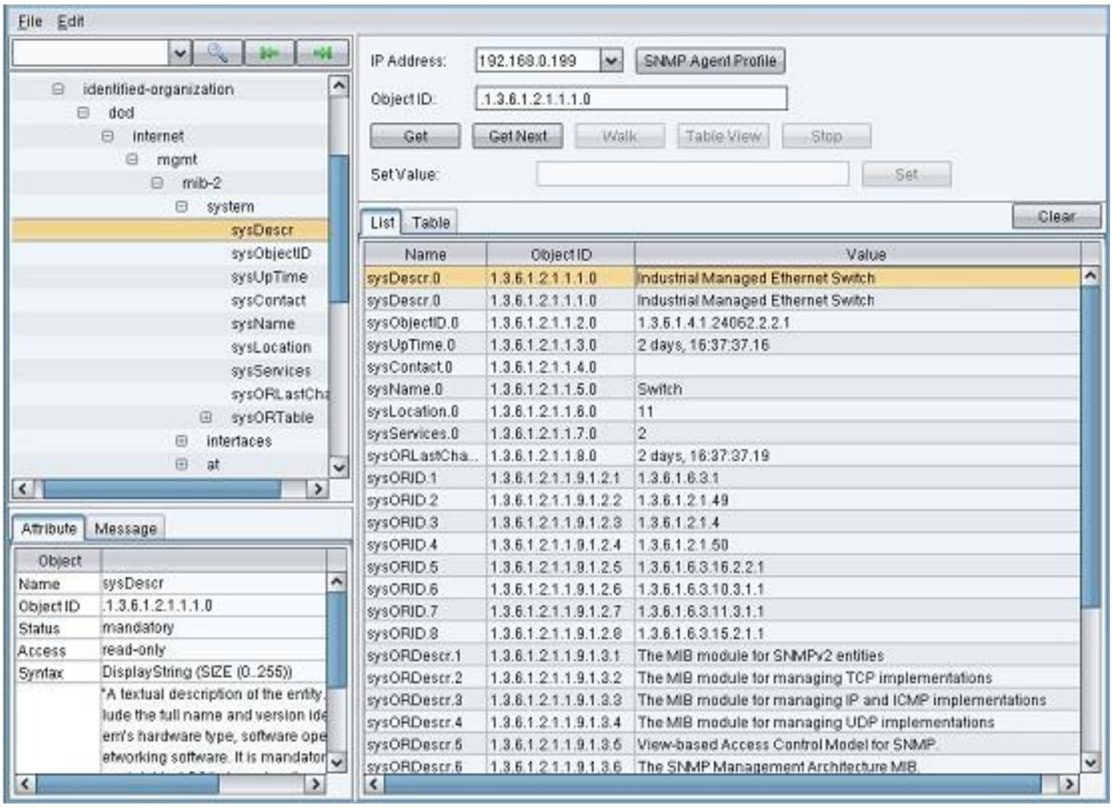
SNMP Browser

JetView Pro provides a SNMP browser for user to management SNMP devices. The SNMP Browser supports SNMP v1/v2c/v3 get, get next, walk, table view and set functions. And the SNMP Browser provides MIB file compiler tool *MIB File Manager* that can load public standard MIBs and private MIBs and build a MIB tree.

Provides many standard MIBs for users to configure or monitor the switch’s configuration by SNMP. But, since some commands can’t be found in standard MIB, JetView Pro provides Private MIB to meet up the need. Compile the private MIB file by you

Private MIB tree is the same as the Web tree. This is easier to understand and use. If you are not familiar with standard MIB, you can directly use private MIB to manage /monitor the switch, no need to learn or find where the OIDs of the commands are.

The SNMP Browser tool lets you read and write the MIB of the selected device.



IP Address: 192.168.0.199

Object ID: .1.3.6.1.2.1.1.1.0

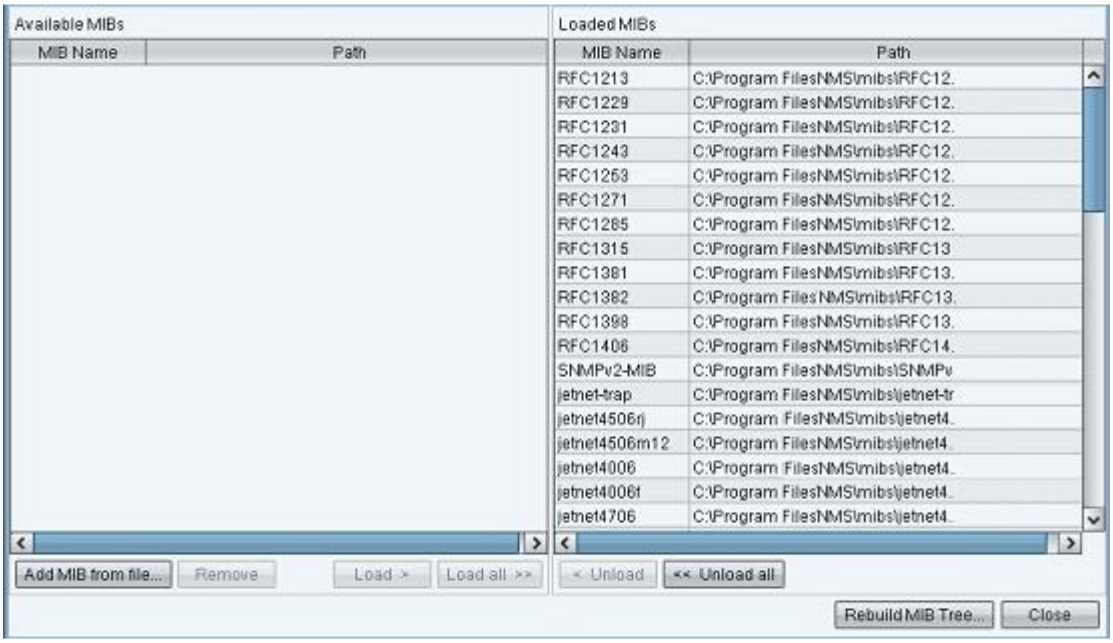
Set Value:

Object	
Name	sysDescr
Object ID	.1.3.6.1.2.1.1.1.0
Status	mandatory
Access	read-only
Syntax	DisplayString (SIZE (0..255))
	"A textual description of the entity. lude the full name and version ide em's hardware type, software ope etworking software. It is mandator

Name	Object ID	Value
sysDescr.0	1.3.6.1.2.1.1.1.0	Industrial Managed Ethernet Switch
sysDescr.0	1.3.6.1.2.1.1.1.0	Industrial Managed Ethernet Switch
sysObjectID.0	1.3.6.1.2.1.1.2.0	1.3.6.1.4.1.24062.2.2.1
sysUpTime.0	1.3.6.1.2.1.1.3.0	2 days, 16:37:37.16
sysContact.0	1.3.6.1.2.1.1.4.0	
sysName.0	1.3.6.1.2.1.1.5.0	Switch
sysLocation.0	1.3.6.1.2.1.1.6.0	11
sysServices.0	1.3.6.1.2.1.1.7.0	2
sysORLastCha...	1.3.6.1.2.1.1.8.0	2 days, 16:37:37.19
sysORID.1	1.3.6.1.2.1.1.9.1.2.1	1.3.6.1.6.3.1
sysORID.2	1.3.6.1.2.1.1.9.1.2.2	1.3.6.1.2.1.49
sysORID.3	1.3.6.1.2.1.1.9.1.2.3	1.3.6.1.2.1.4
sysORID.4	1.3.6.1.2.1.1.9.1.2.4	1.3.6.1.2.1.50
sysORID.5	1.3.6.1.2.1.1.9.1.2.5	1.3.6.1.6.3.16.2.2.1
sysORID.6	1.3.6.1.2.1.1.9.1.2.6	1.3.6.1.6.3.10.3.1.1
sysORID.7	1.3.6.1.2.1.1.9.1.2.7	1.3.6.1.6.3.11.3.1.1
sysORID.8	1.3.6.1.2.1.1.9.1.2.8	1.3.6.1.6.3.15.2.1.1
sysORDescr.1	1.3.6.1.2.1.1.9.1.3.1	The MIB module for SNMPv2 entities
sysORDescr.2	1.3.6.1.2.1.1.9.1.3.2	The MIB module for managing TCP implementations
sysORDescr.3	1.3.6.1.2.1.1.9.1.3.3	The MIB module for managing IP and ICMP implementations
sysORDescr.4	1.3.6.1.2.1.1.9.1.3.4	The MIB module for managing UDP implementations
sysORDescr.5	1.3.6.1.2.1.1.9.1.3.5	View-based Access Control Model for SNMP.
sysORDescr.6	1.3.6.1.2.1.1.9.1.3.6	The SNMP Management Architecture MIB.

Figure 7–7. MIB Example Compiler

The MIB Compiler assists user in building MIB tree. While MIB files have been changed, user uses the MIB Compiler to rebuild MIB tree. To add new MIB into MIB Tree, *go File > MIB Manager*. It will show the following window.



Available MIBs

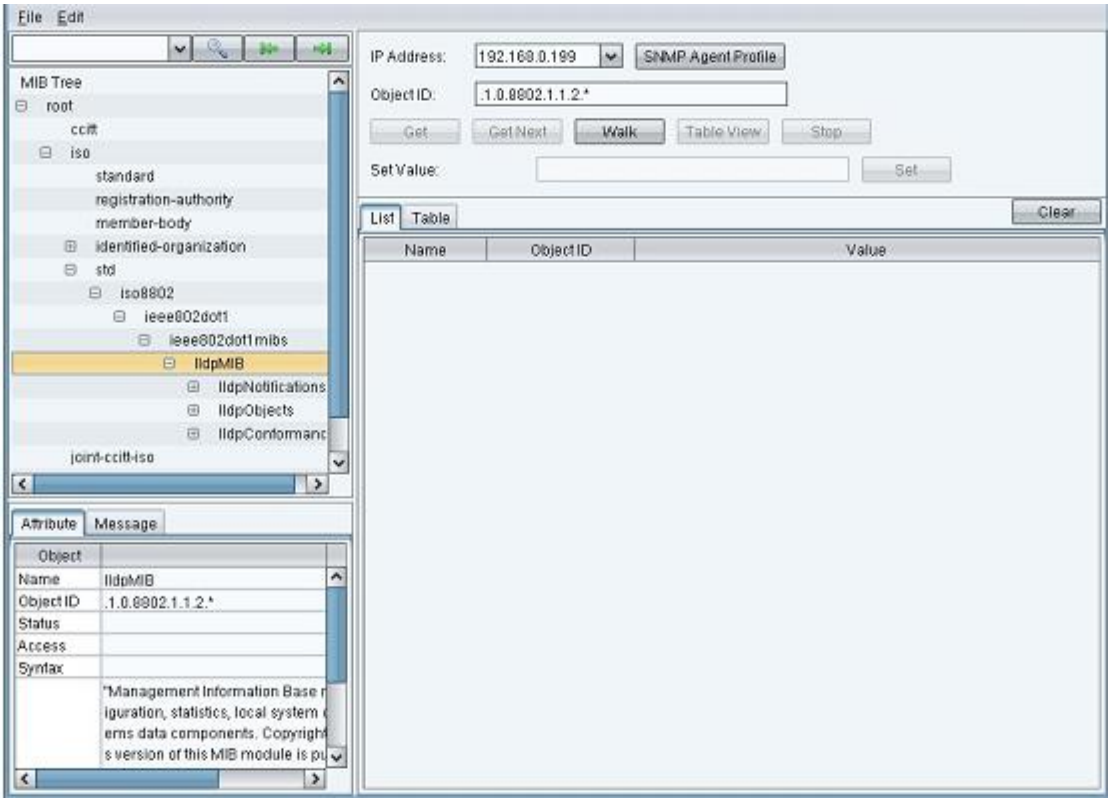
MIB Name	Path

Loaded MIBs

MIB Name	Path
RFC1213	C:\Program FilesNMS\mibs\RFC12.
RFC1229	C:\Program FilesNMS\mibs\RFC12.
RFC1231	C:\Program FilesNMS\mibs\RFC12.
RFC1243	C:\Program FilesNMS\mibs\RFC12.
RFC1253	C:\Program FilesNMS\mibs\RFC12.
RFC1271	C:\Program FilesNMS\mibs\RFC12.
RFC1285	C:\Program FilesNMS\mibs\RFC12.
RFC1315	C:\Program FilesNMS\mibs\RFC13
RFC1381	C:\Program FilesNMS\mibs\RFC13.
RFC1382	C:\Program Files NMS\mibs\RFC13.
RFC1398	C:\Program FilesNMS\mibs\RFC13.
RFC1406	C:\Program FilesNMS\mibs\RFC14.
SNMPv2-MIB	C:\Program FilesNMS\mibs\SNMPv
jetnet-trap	C:\Program FilesNMS\mibs\jetnet-tr
jetnet4506rj	C:\Program FilesNMS\mibs\jetnet4..
jetnet4506m12	C:\Program FilesNMS\mibs\jetnet4..
jetnet4006	C:\Program FilesNMS\mibs\jetnet4..
jetnet4006f	C:\Program FilesNMS\mibs\jetnet4..
jetnet4706	C:\Program FilesNMS\mibs\jetnet4..

Figure 7-8. Adding a MIB

Press *Add MIB from file* to add new MIB file. Load this new MIB file and then press *Rebuild MIB Tree* to update MIB Tree.



IP Address: 192.168.0.199

Object ID: .1.0.8802.1.1.2.*

Set Value:

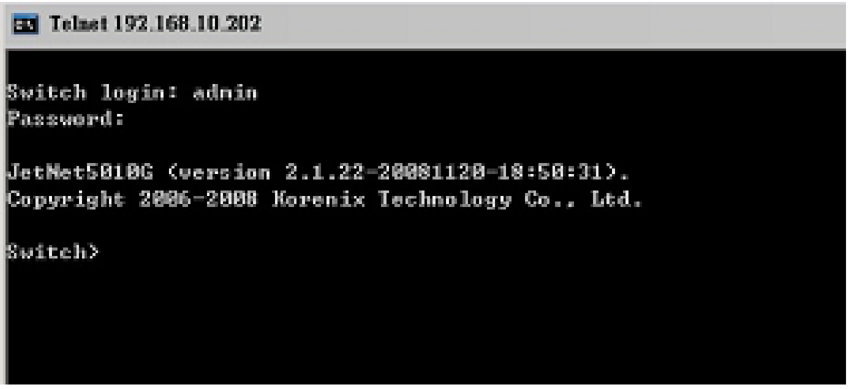
Object	
Name	lldpMIB
Object ID	.1.0.8802.1.1.2.*
Status	
Access	
Syntax	
	"Management Information Base f iguration, statistics, local system ems data components. Copyright s version of this MIB module is pu

Figure 7–9. Loaded MIB

Telnet

Connect's network devices support Telnet console. You can connect to the switch by

Telnet, the command lines are the same as what you see by RS232 console port. You can use CLI command to configure your device.



```
Switch login: admin
Password:

JetNet5010G (version 2.1.22-20081120-18:50:31).
Copyright 2006-2008 Korenix Technology Co., Ltd.

Switch>
```

Figure 7–10. Telnet Command Line

SSH (Secure Shell)

Connect's network devices also support SSH console. You can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you sent to the switch.

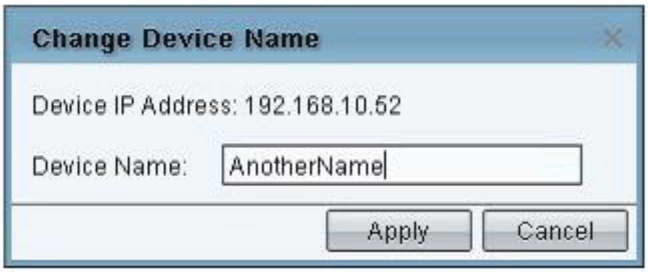
SSH is a client/server architecture where network devices are considered as the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

Ping

This ping function can confirm your host access to Connect’s network devices via network. Ping the selected device to verify a normal response time.

Change Device Name

You can give device an alias for a device by *Change Device Name* function.

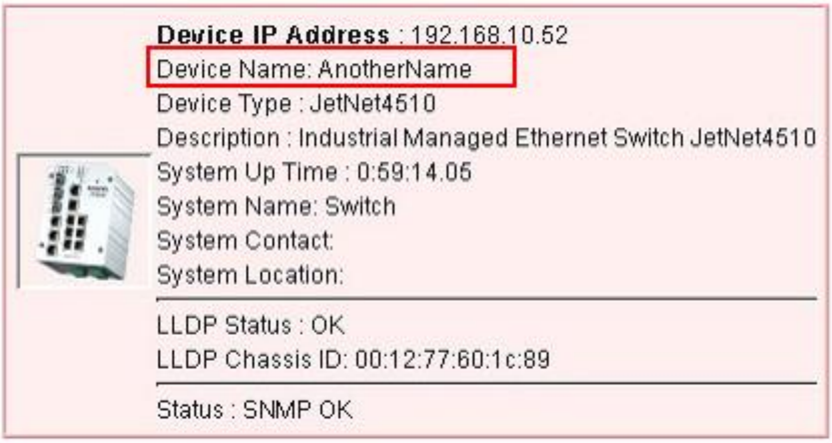


Change Device Name

Device IP Address: 192.168.10.52

Device Name: AnotherName

Figure 7–11. Changing Device Name



Device IP Address : 192.168.10.52
Device Name: AnotherName
Device Type : JetNet4510
Description : Industrial Managed Ethernet Switch JetNet4510
System Up Time : 0:59:14.05
System Name: Switch
System Contact:
System Location:

LLDP Status : OK
LLDP Chassis ID: 00:12:77:60:1c:89

Status : SNMP OK

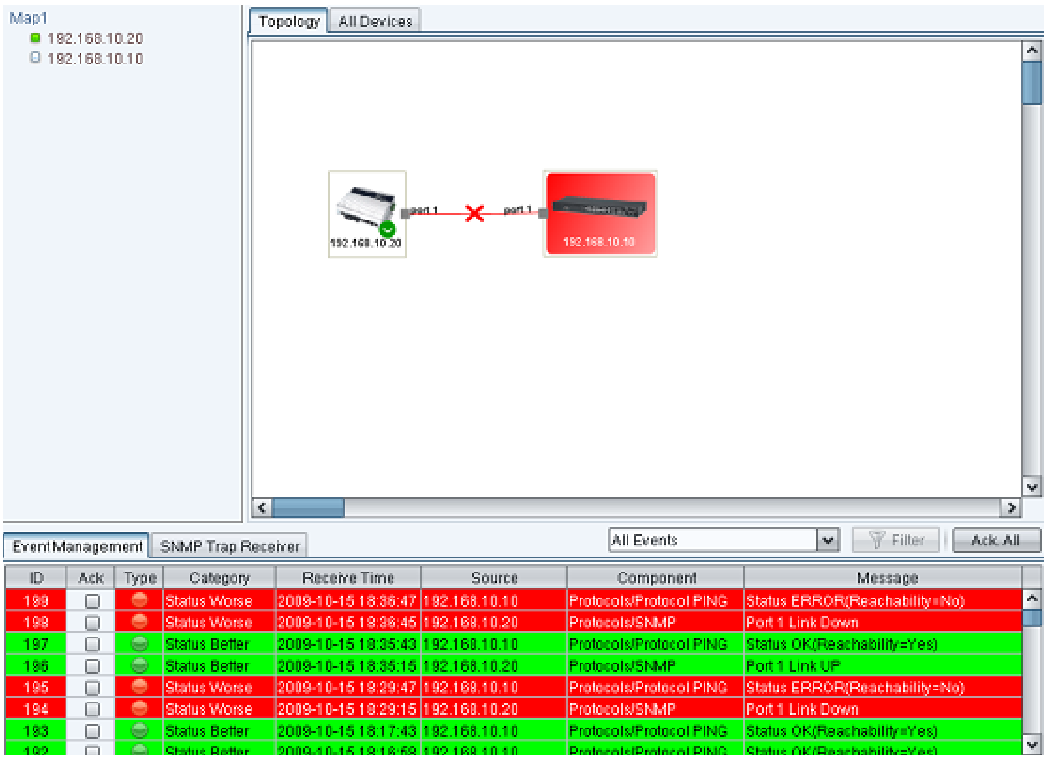
Figure 7–12. Applied Device Name Change

8. Event and Alarm Management

Event Management

Administers can identify the event threshold (OK, Warning, Error, No Status) by the color. Notifications based on any event (Node up, Node down, Link up, Link down, Remote Access Client mode, etc.) can be generated. Besides, notifications can be sent via email, SNMP trap and this JetView Pro program. For the event settings refer to section 9.1.

In the case of red background icon on Topology tab, relevant fields in the event line of Event Management tab are colored as red (see Figure 8–1). According to the event message, users can identify what occurs to the devices with red background.

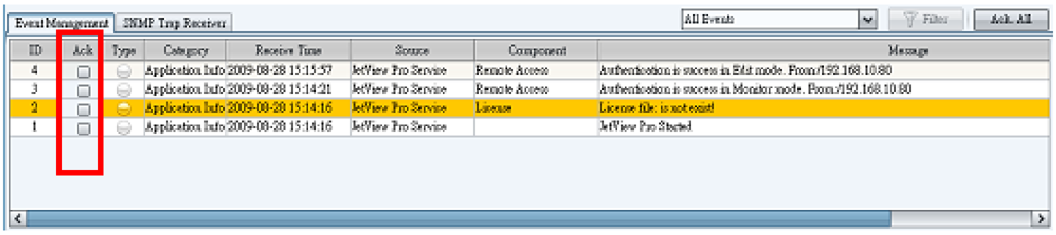


ID	Ack	Type	Category	Receive Time	Source	Component	Message
199	□	●	Status Worse	2009-10-15 18:36:47	192.168.10.10	Protocols/Protocol PING	Status ERROR(Reachability=No)
198	□	●	Status Worse	2009-10-15 18:36:45	192.168.10.20	Protocols/SNMP	Port 1 Link Down
197	□	●	Status Better	2009-10-15 18:35:43	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)
196	□	●	Status Better	2009-10-15 18:35:15	192.168.10.20	Protocols/SNMP	Port 1 Link UP
195	□	●	Status Worse	2009-10-15 18:29:47	192.168.10.10	Protocols/Protocol PING	Status ERROR(Reachability=No)
194	□	●	Status Worse	2009-10-15 18:29:15	192.168.10.20	Protocols/SNMP	Port 1 Link Down
193	□	●	Status Better	2009-10-15 18:17:43	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)
192	□	●	Status Better	2009-10-15 18:18:58	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)

Figure 8–1. Event Management Example

Ack This column is to check the status of each event and confirm these events for network manager. After checking Ack, the corresponding links or device icons in the topology are restored to the normal color. This is also to recognize updated status in the topology.

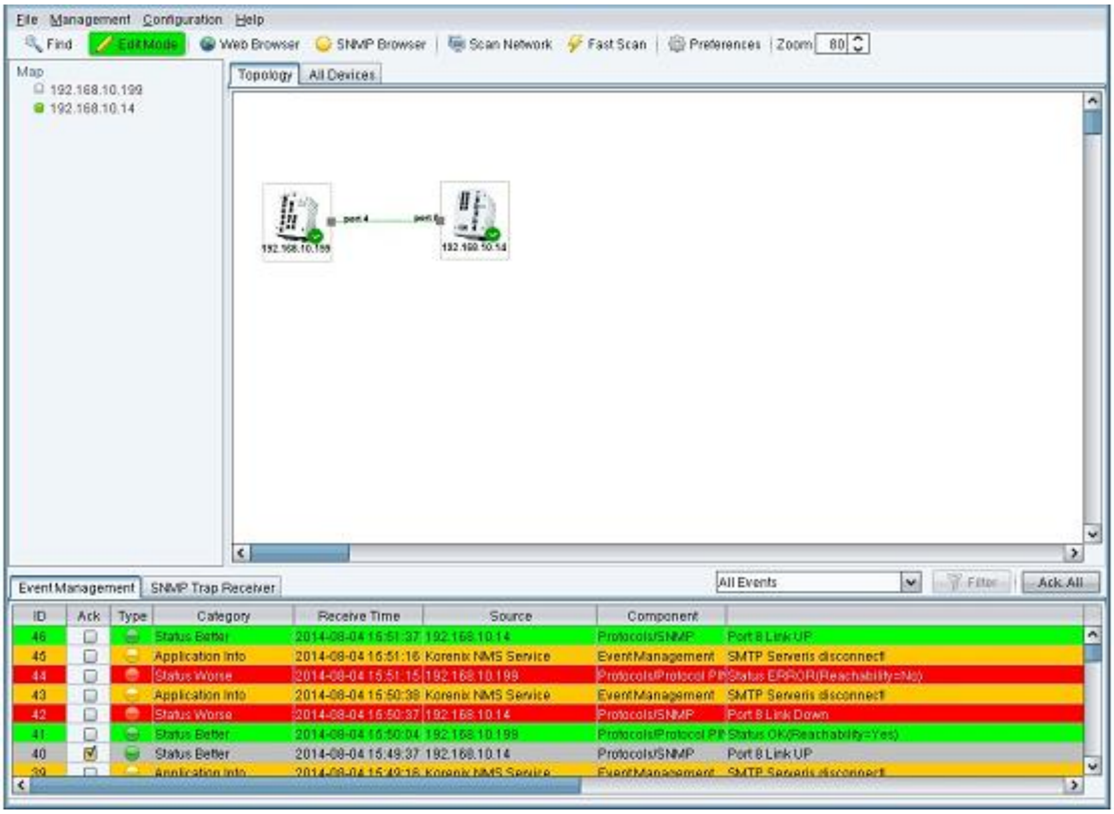
Use mouse to click checkbox to check.



ID	Ack	Type	Category	Receive Time	Source	Component	Message
4	□	○	Application Info	2009-08-28 15:15:57	JetView Pro Service	Remote Access	Authentication is success in Edit mode. From:/192.168.10.80
3	□	○	Application Info	2009-08-28 15:14:21	JetView Pro Service	Remote Access	Authentication is success in Monitor mode. From:/192.168.10.80
2	□	●	Application Info	2009-08-28 15:14:16	JetView Pro Service	License	License file: is not exist!
1	□	○	Application Info	2009-08-28 15:14:16	JetView Pro Service		JetView Pro Started

Figure 8–2. Selecting Devices to Ack

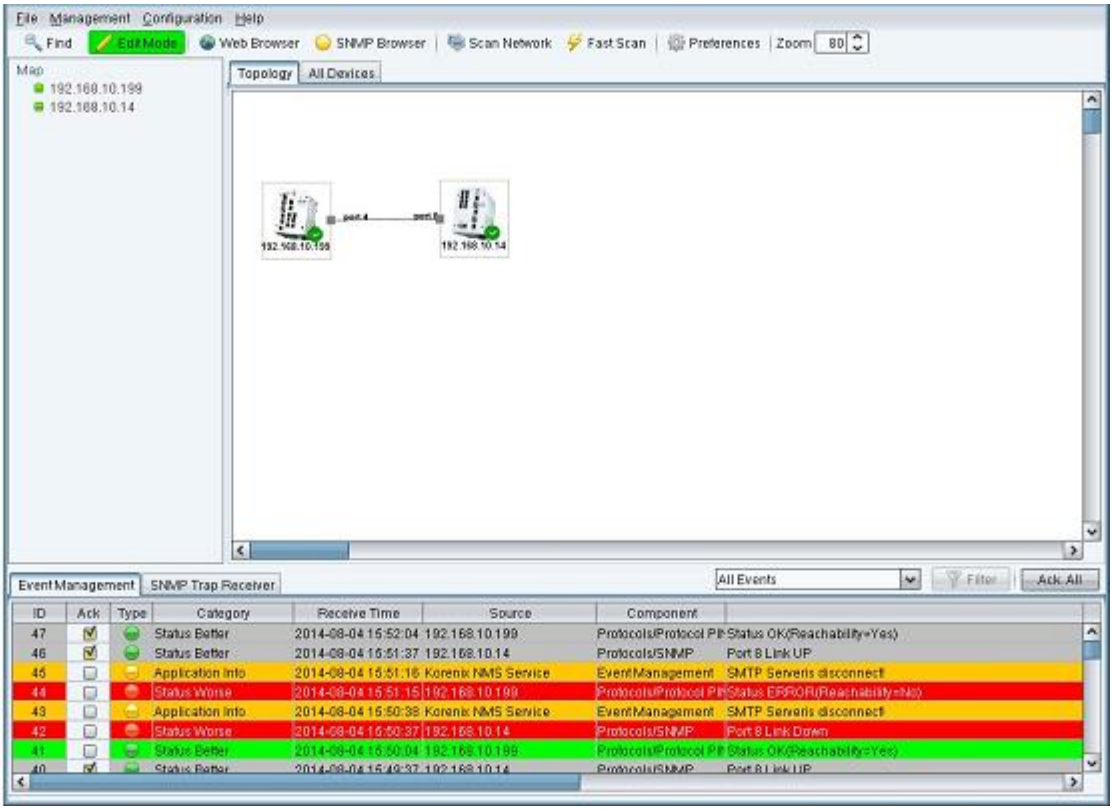
Ack for the green link, for example.



ID	Ack	Type	Category	Receive Time	Source	Component	
46	□	●	Status Better	2014-08-04 15:51:37	192.168.10.14	Protocols/SNMP	Port 8 Link UP
45	□	●	Application Info	2014-08-04 15:51:16	Korenix NMS Service	EventManagement	SMTP Serveris disconnect!
44	□	●	Status Worse	2014-08-04 15:51:15	192.168.10.199	Protocols/Protocol PI	Status ERROR(Reachability=No)
43	□	●	Application Info	2014-08-04 15:50:38	Korenix NMS Service	EventManagement	SMTP Serveris disconnect!
42	□	●	Status Worse	2014-08-04 15:50:37	192.168.10.14	Protocols/SNMP	Port 8 Link Down
41	□	●	Status Better	2014-08-04 15:50:04	192.168.10.199	Protocols/Protocol PI	Status OK(Reachability=Yes)
40	☑	●	Status Better	2014-08-04 15:49:37	192.168.10.14	Protocols/SNMP	Port 8 Link UP
39	□	●	Application Info	2014-08-04 15:49:16	Korenix NMS Service	EventManagement	SMTP Serveris disconnect!

Figure 8–3. Event Management, Ack

While you check this Ack of ID 46 and 47, the link color will restore from green to gray.



ID	Ack	Type	Category	Receive Time	Source	Component	
47	☑	●	Status Better	2014-08-04 15:52:04	192.168.10.199	Protocols/Protocol Pi	Status OK(Reachability=Yes)
46	☑	●	Status Better	2014-08-04 15:51:37	192.168.10.14	Protocols/SNMP	Port 8 Link UP
45	□	●	Application Info	2014-08-04 15:51:16	Korenix NMS Service	EventManagement	SMTP Serveris disconnect
44	□	●	Status Worse	2014-08-04 15:51:15	192.168.10.199	Protocols/Protocol Pi	Status ERROR(Reachability=No)
43	□	●	Application Info	2014-08-04 15:50:38	Korenix NMS Service	EventManagement	SMTP Serveris disconnect
42	□	●	Status Worse	2014-08-04 15:50:37	192.168.10.14	Protocols/SNMP	Port 8 Link Down
41	□	●	Status Better	2014-08-04 15:50:04	192.168.10.199	Protocols/Protocol Pi	Status OK(Reachability=Yes)
40	☑	●	Status Better	2014-08-04 15:49:37	192.168.10.14	Protocols/SNMP	Port 8 Link UP

Figure 8–4. Event Filter for Ack

Event Filter You can choose to use *All Events*, *Unacknowledged Events*, *Warnings & Errors*, *Warnings*, *Errors*, *Unacknowledged Warnings & Errors and Source*=, so that show the event status you want to see. While choosing *Source* =, you must append the IP address (ex, 192.168.10.1) behind the *Source* = string and press Filter button to filter the events matched by Source column,

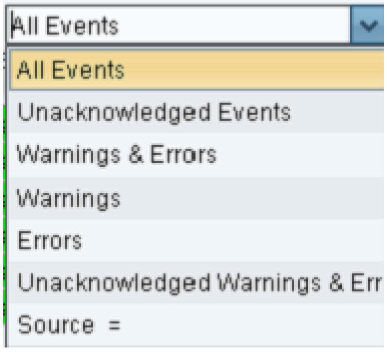
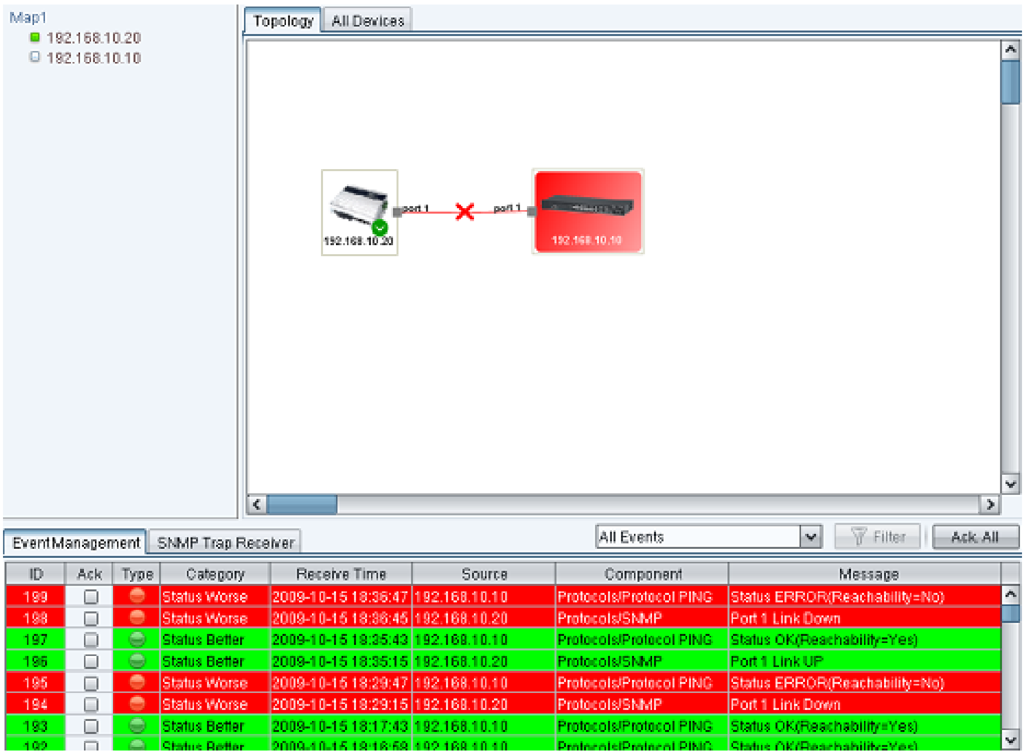


Figure 8–5. Filters

Link up/down Events

While the link failure happens, JetView Pro will issue a Link Down event in Event

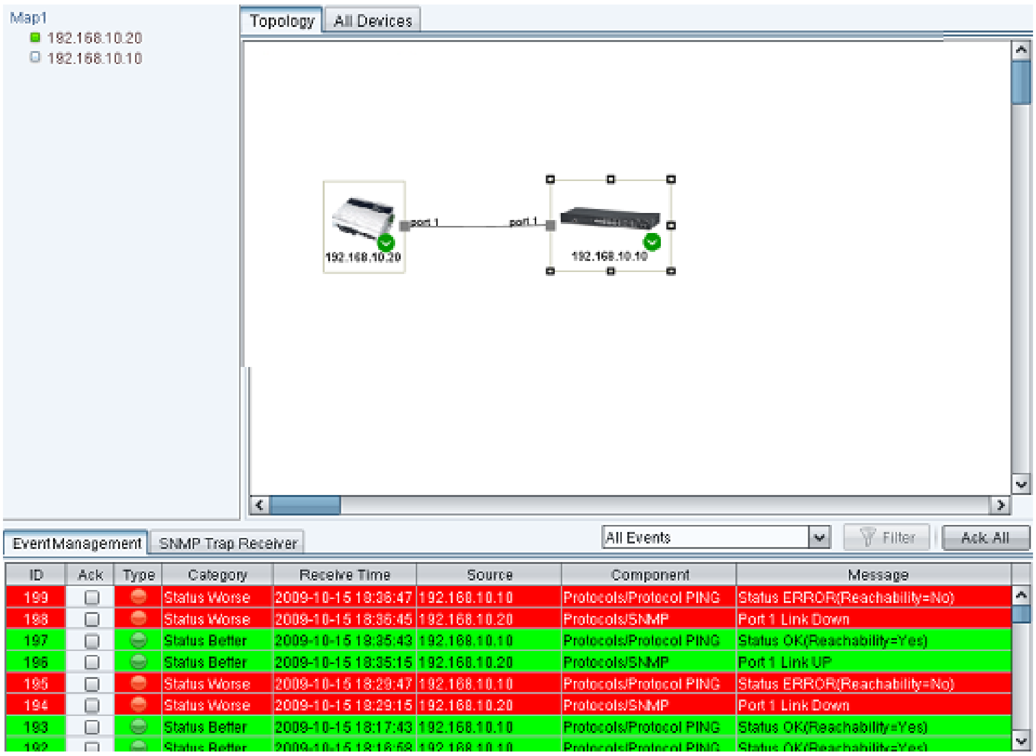
Management tab page and update the Topology Map Figure 8–6. This event will show *Port1 Link Down* Message.



ID	Ack	Type	Category	Receive Time	Source	Component	Message
199	□	●	Status Worse	2009-10-15 18:36:47	192.168.10.10	Protocols/Protocol PING	Status ERROR(Reachability=No)
198	□	●	Status Worse	2009-10-15 18:36:45	192.168.10.20	Protocols/SNMP	Port 1 Link Down
197	□	●	Status Better	2009-10-15 18:35:43	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)
196	□	●	Status Better	2009-10-15 18:35:15	192.168.10.20	Protocols/SNMP	Port 1 Link UP
195	□	●	Status Worse	2009-10-15 18:29:47	192.168.10.10	Protocols/Protocol PING	Status ERROR(Reachability=No)
194	□	●	Status Worse	2009-10-15 18:29:15	192.168.10.20	Protocols/SNMP	Port 1 Link Down
193	□	●	Status Better	2009-10-15 18:17:43	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)
192	□	●	Status Better	2009-10-15 18:16:59	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)

Figure 8–6. Link Down Event

While the link restores, JetView Pro will issue a Link Up event in Event Management tab page and update the Topology Map Figure 8–7. This event will show *Port1 Link UP* Message.

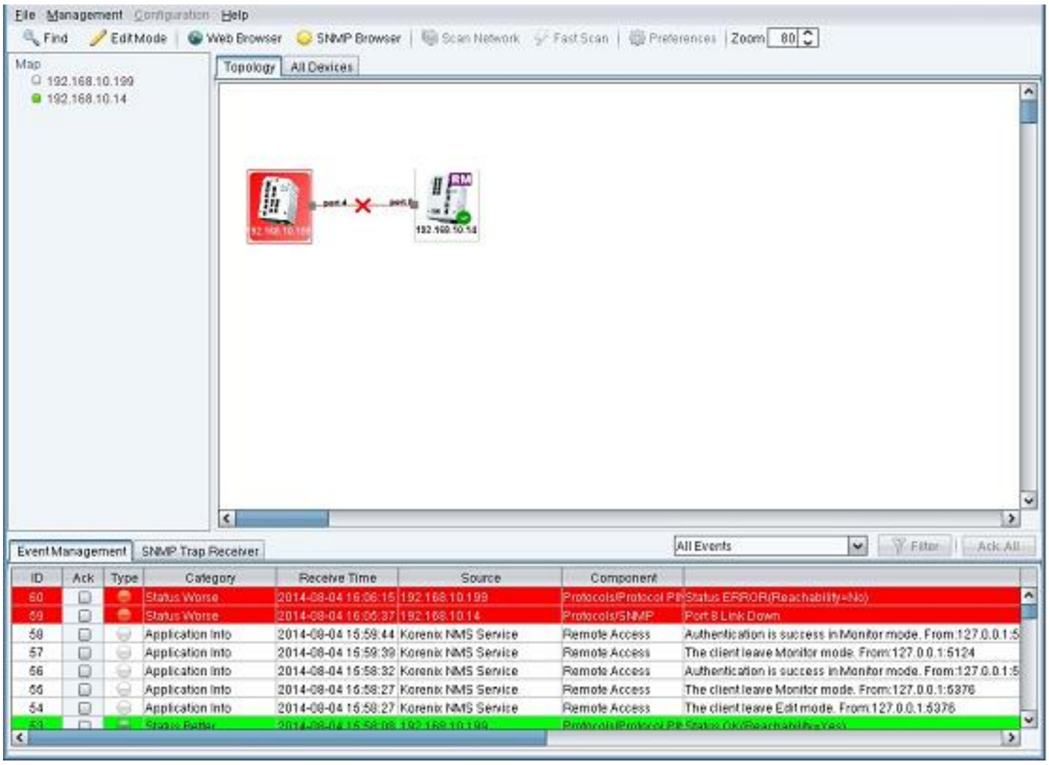


ID	Ack	Type	Category	Receive Time	Source	Component	Message
199	□	●	Status Worse	2009-10-15 18:36:47	192.168.10.10	Protocols/Protocol PING	Status ERROR(Reachability=No)
198	□	●	Status Worse	2009-10-15 18:36:45	192.168.10.20	Protocols/SNMP	Port 1 Link Down
197	□	●	Status Better	2009-10-15 18:35:43	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)
196	□	●	Status Better	2009-10-15 18:35:15	192.168.10.20	Protocols/SNMP	Port 1 Link UP
195	□	●	Status Worse	2009-10-15 18:29:47	192.168.10.10	Protocols/Protocol PING	Status ERROR(Reachability=No)
194	□	●	Status Worse	2009-10-15 18:29:15	192.168.10.20	Protocols/SNMP	Port 1 Link Down
193	□	●	Status Better	2009-10-15 18:17:43	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)
192	□	●	Status Better	2009-10-15 18:16:59	192.168.10.10	Protocols/Protocol PING	Status OK(Reachability=Yes)

Figure 8–7. Link Up Event

Node up/down Events

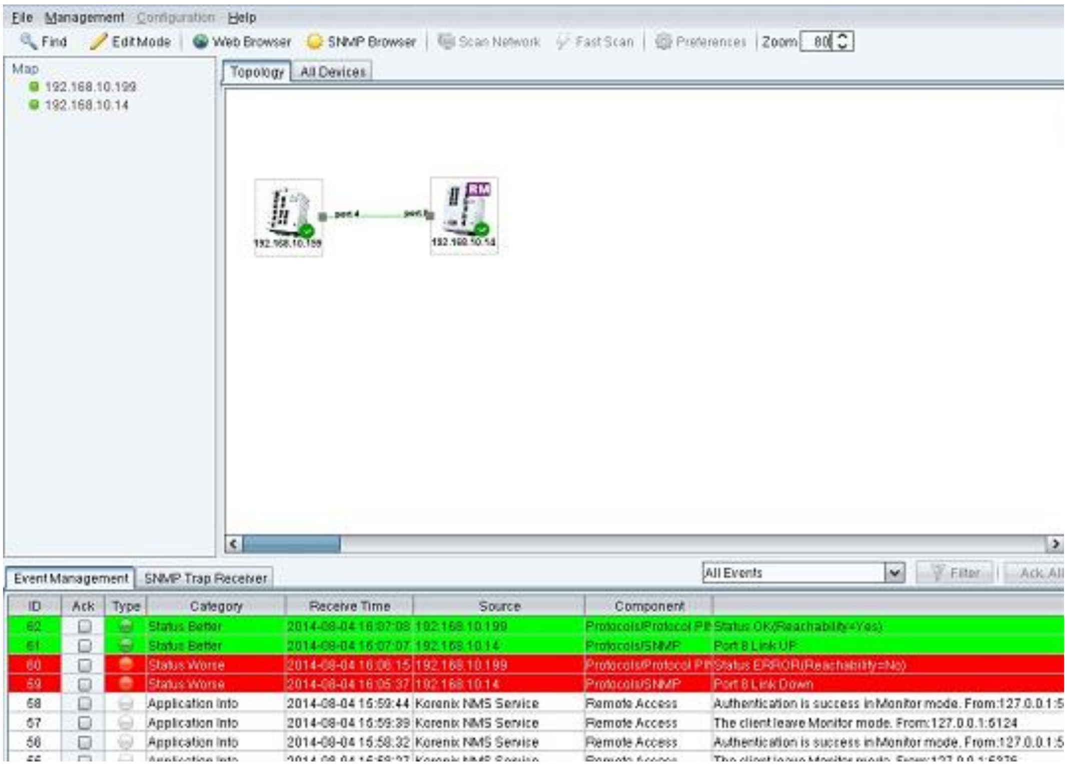
While the node failure happens, JetView Pro will issue a Node down event in Event Management tab page and update the Topology Map Figure 8–8. This event will show *Status ERROR(Reachability=No)* Message.



ID	Ack	Type	Category	Receive Time	Source	Component	
60	□	●	Status Worse	2014-08-04 16:06:15	192.168.10.199	Protocols/Protocol PI	Status ERROR(Reachability=No)
59	□	●	Status Worse	2014-08-04 16:05:37	192.168.10.14	Protocols/SNMP	Port 8 Link Down
58	□	○	Application Info	2014-08-04 15:59:44	Korenix NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
57	□	○	Application Info	2014-08-04 15:59:39	Korenix NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5124
56	□	○	Application Info	2014-08-04 15:58:32	Korenix NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
55	□	○	Application Info	2014-08-04 15:58:27	Korenix NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5376
54	□	○	Application Info	2014-08-04 15:58:27	Korenix NMS Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5376
53	□	●	Status Better	2014-08-04 15:58:08	192.168.10.199	Protocols/Protocol PI	Status OK(Reachability=Yes)

Figure 8–8. Node Down Event

While the node restores, JetView Pro will issue a Node up event in Event Management tab page and update the Topology Map Figure 8–9. This event will show *Status OK(Reachability=Yes)* Message.



ID	Ack	Type	Category	Receive Time	Source	Component	
62	□	🟩	Status Better	2014-08-04 16:07:08	192.168.10.199	Protocols/Protocol PI	Status OK(Reachability=Yes)
61	□	🟩	Status Better	2014-08-04 16:07:07	192.168.10.14	Protocols/SNMP	Port 8 Link UP
60	□	🟥	Status Worse	2014-08-04 16:06:15	192.168.10.199	Protocols/Protocol PI	Status ERROR(Reachability=No)
59	□	🟥	Status Worse	2014-08-04 16:05:37	192.168.10.14	Protocols/SNMP	Port 8 Link Down
58	□	○	Application Info	2014-08-04 15:59:44	Korenix NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
57	□	○	Application Info	2014-08-04 15:59:39	Korenix NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:6124
56	□	○	Application Info	2014-08-04 15:58:32	Korenix NMS Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5
55	□	○	Application Info	2014-08-04 15:58:27	Korenix NMS Service	Remote Access	The client leave Monitor mode. From:127.0.0.1:5376

Figure 8–9. Node Up Event

SNMP Trap

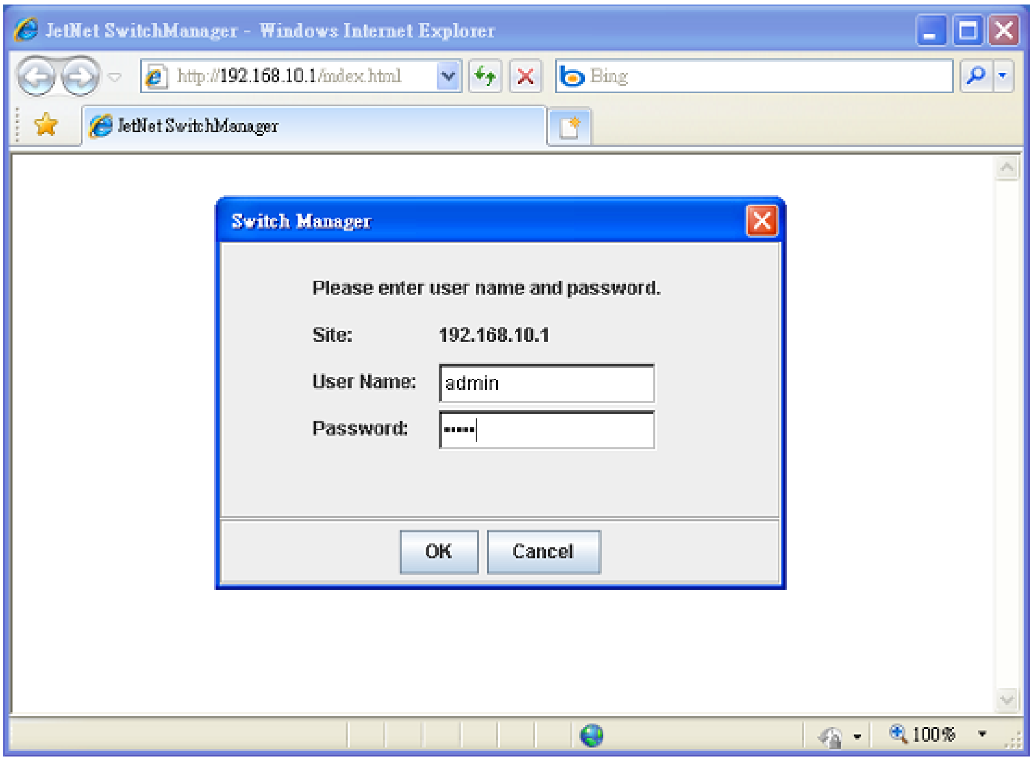
SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you don't need to install new application to read the notification information. The SNMP Trap Receiver of JetView Pro supports SNMP v1/v2c traps receiving.

The following sections illustrate SNMP Trap with Link down and up event.

Enable Link-down and Link-up Event

To enable link-down and link-up event, you must enable SNMP Trap Server and Link down and up event. Enter Web screen to configure these settings.

1. Use mouse to select one device on the Topology tab which you want to enable link down and up event.
2. Mouse right-click the selected device and click on the Web Browser menu-item of pop-up menu.
3. When the login screen appears, login with the user name and password. The default login User Name and Password: admin/admin



JetNet SwitchManager - Windows Internet Explorer
http://192.168.10.1/index.html
Bing
JetNet SwitchManager
Switch Manager
100%

Please enter user name and password.

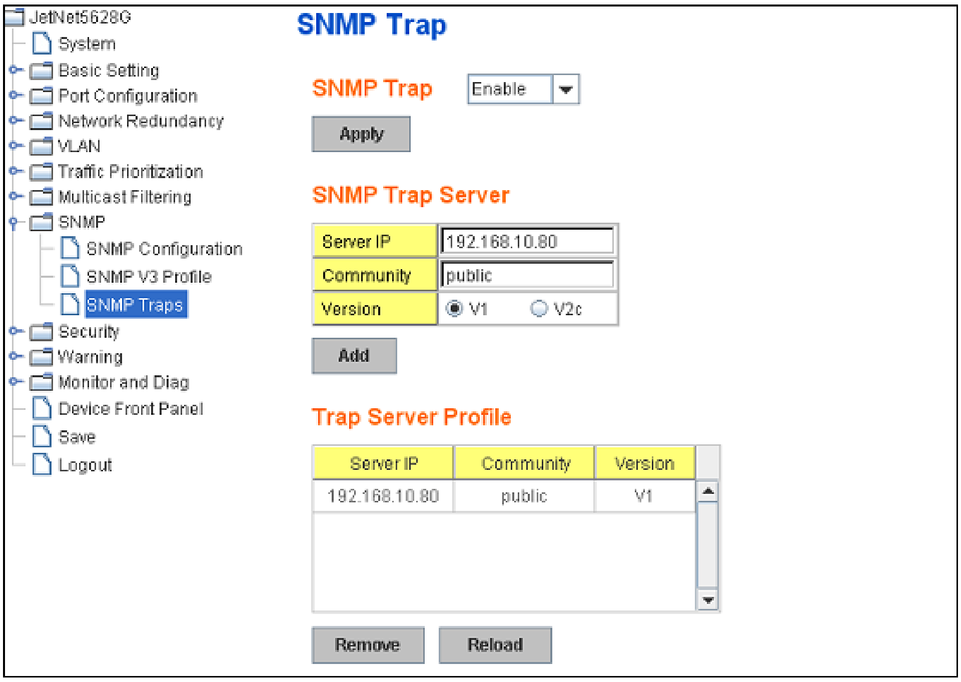
Site: 192.168.10.1

User Name: admin

Password: •••••

Figure 8–10. Connect Switch – Switch Manager Start Page

4. Click on the tree node SNMP Traps. Enable SNMP Trap, and set SNMP Trap Server IP address on the machine where the JetView Pro is installed.



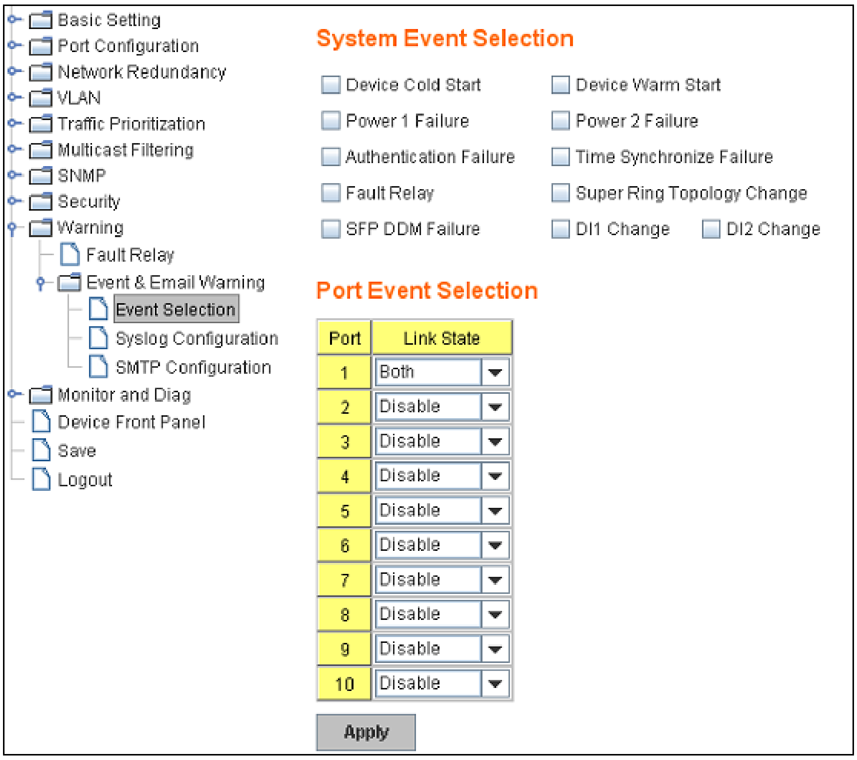
SNMP Trap: Enable

Server IP	192.168.10.80
Community	public
Version	● V1 ○ V2c

Server IP	Community	Version
192.168.10.80	public	V1

Figure 8–11. Connect Switch – SNMP Trap Configuration

5. Click on the tree node Event Selection. Enable the specified port for link-down and link-up event (ex. Set Port 1 as both).



System Event Selection

□ Device Cold Start □ Device Warm Start
□ Power 1 Failure □ Power 2 Failure
□ Authentication Failure □ Time Synchronize Failure
□ Fault Relay □ Super Ring Topology Change
□ SFP DDM Failure □ DI1 Change □ DI2 Change

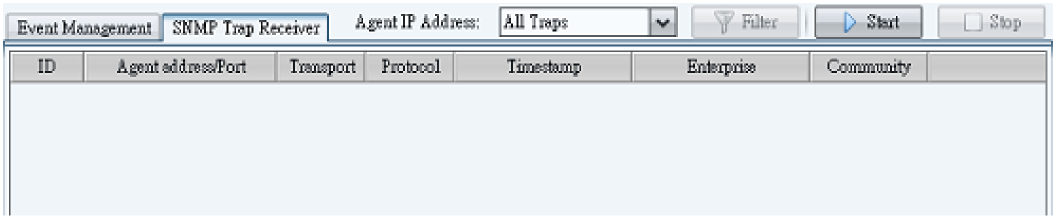
Port Event Selection

Port	Link State
1	Both
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable

Figure 8–12. Management, Event Selection Configuration

Receive SNMP Trap

1. Click on *Start* on the SNMP Trap Receiver tab.

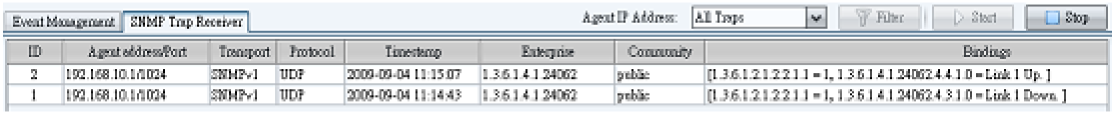


Agent IP Address: All Traps

ID	Agent address/Port	Transport	Protocol	Timestamp	Enterprise	Community

Figure 8–13. SNMP Trap Receiver Tab

2. While plugging in or out the network line (ex. RJ45) on the port 1 of device (ex.192.168.10.1), it will display as follows:



Agent IP Address: All Traps

ID	Agent address/Port	Transport	Protocol	Timestamp	Enterprise	Community	Bindings
2	192.168.10.1/1024	SNMPv1	UDP	2009-09-04 11:15:07	1.3.6.1.4.1.24062	public	[1.3.6.1.2.1.2.2.1.1 = 1, 1.3.6.1.4.1.24062.4.4.1.0 = Link 1 Up.]
1	192.168.10.1/1024	SNMPv1	UDP	2009-09-04 11:14:43	1.3.6.1.4.1.24062	public	[1.3.6.1.2.1.2.2.1.1 = 1, 1.3.6.1.4.1.24062.4.3.1.0 = Link 1 Down.]

Figure 8–14. SNMP Trap Receiver with Values Captured

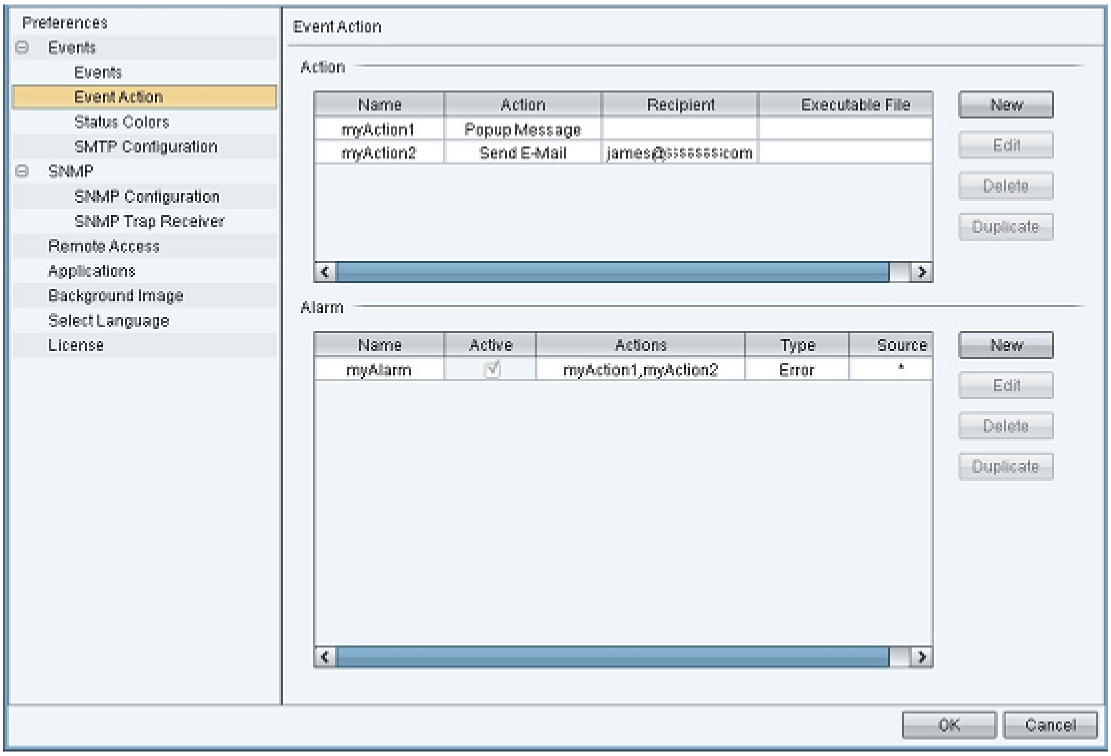
Alarm and Action

When event or SNMP trap are produced. They in addition to display in event management or SNMP Trap Receiver, and they can trigger some alarms and do some actions. The alarm can be triggered by type or other field of event. The actions of JetView Pro supported are Popup Message, E-mail and Run Executable File.

The following sections illustrate how to use alarm and action.

Create an Action

Open JetView Pro Preference, select Event Action and new an action.



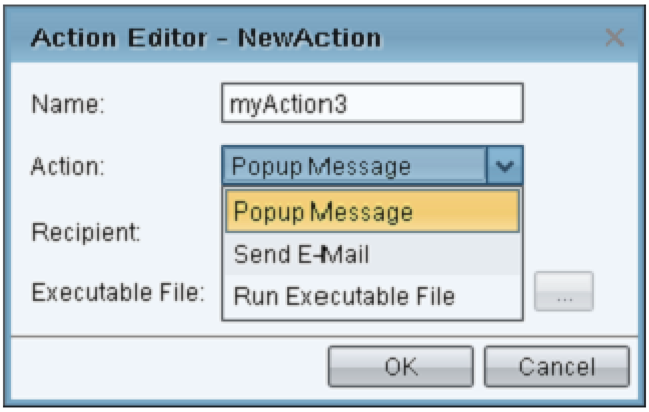
Name	Action	Recipient	Executable File
myAction1	Popup Message		
myAction2	Send E-Mail	james@sssssss.com	

Name	Active	Actions	Type	Source
myAlarm	☑	myAction1,myAction2	Error	*

Figure 8–15. Creating an Action

Press *New* button the Action Editor window will be opened. You need input action name and select an action type (*Popup Message, Send E-Mail or Run Executable File*) to create a new action.

Or you can manage actions via *Edit, Duplicate* or *Delete* functions.



Name: myAction3

Action: Popup Message

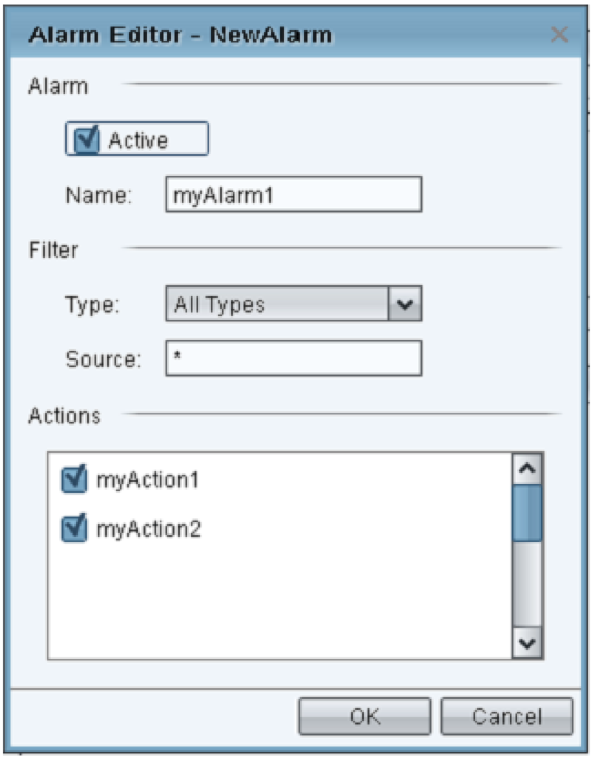
Figure 8–16. Action Editor

Create an Alarm

Open JetView Pro Preference, select Event Action and new an alarm.

Press *New* button the Alarm Editor window will be opened. You need input action name and select actions to create a new alarm. Select Active option to active this alarm. *Change Filter Type* or *Source* to filter what event that you want to trigger. Select actions to decide what action will be executed when this alarm is trigged.

Or you can manage actions via *Edit, Duplicate* or *Delete* functions.



☑ Active

Name: myAlarm1

Type: All Types

Source: *

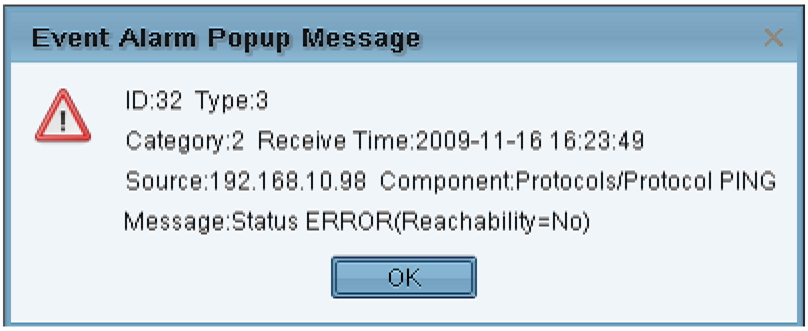
☑ myAction1

☑ myAction2

Figure 8–17. Alarm Editor

Popup Message Action

When a Popup Message action is executed, all JetView Pro clients will pop up a message as follows:

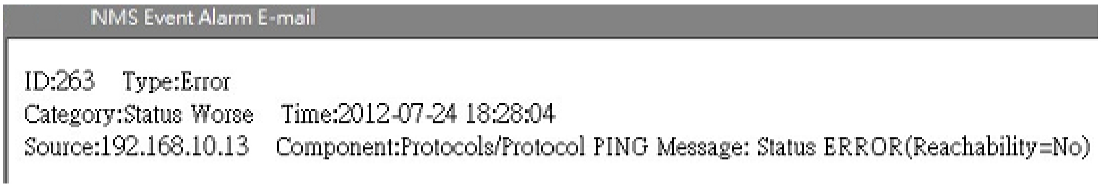


ID:32 Type:3
Category:2 Receive Time:2009-11-16 16:23:49
Source:192.168.10.98 Component:Protocols/Protocol PING
Message:Status ERROR(Reachability=No)

Figure 8–18. Event Alarm Popup Message

E-mail Action

When a Send E-mail action is executed, the JetView Pro will send an alarm e-mail to your e-mail account (configured in Preference->SMTP configuration). The e-mail could show as follows:



ID:263 Type:Error
Category:Status Worse Time:2012-07-24 18:28:04
Source:192.168.10.13 Component:Protocols/Protocol PING Message: Status ERROR(Reachability=No)

Figure 8–19. E-mail Action

Run Executable File Action

When a Run Executable File action is executed, the user specified executable file will be executed.

9. Performance Management

If you want to monitor the traffic of your local network for a period of time, JetView Pro can give you an indication of the network traffic for the connections in a time context. It is useful as a quick reference for determining the amount of network bandwidth being consumed.

Traffic Report

JetView Pro monitor and report selected connection statistics. The tab name of the current traffic history shows two connected devices' IP address and port - Port 13 on the device (192.168.10.10) connects to port 9 on the other device (192.168.10.1). The data was collected by through SNMP's polling. The default sampling rate is set to 30 seconds.

The figure below indicates network load for the specified port. In order to show a visible line on the graph for network traffic on any interface, the view automatically scales to magnify the Y-axle's unit of traffic. The X-axle is time. The Y-axle means the total number of bytes sent on the connection in the polling time interval. The maximum number of entries can be recorded in 30 minutes. When the maximum number of entries is reached, JetView Pro throws out the oldest entry when a new one is recorded.

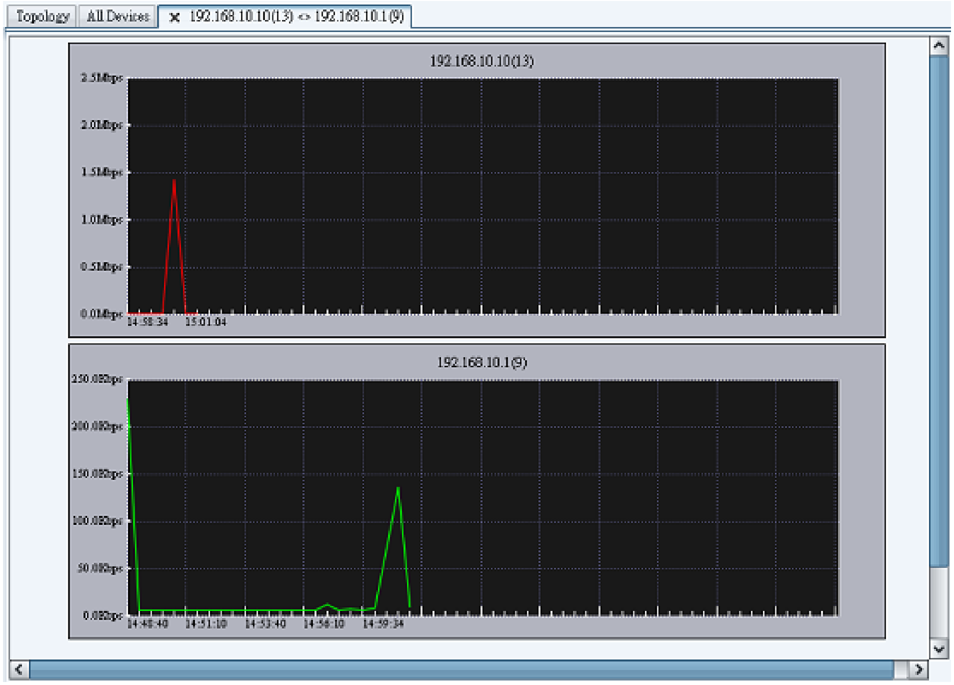


Figure 9–1. Traffic Graphic

To view the traffic report

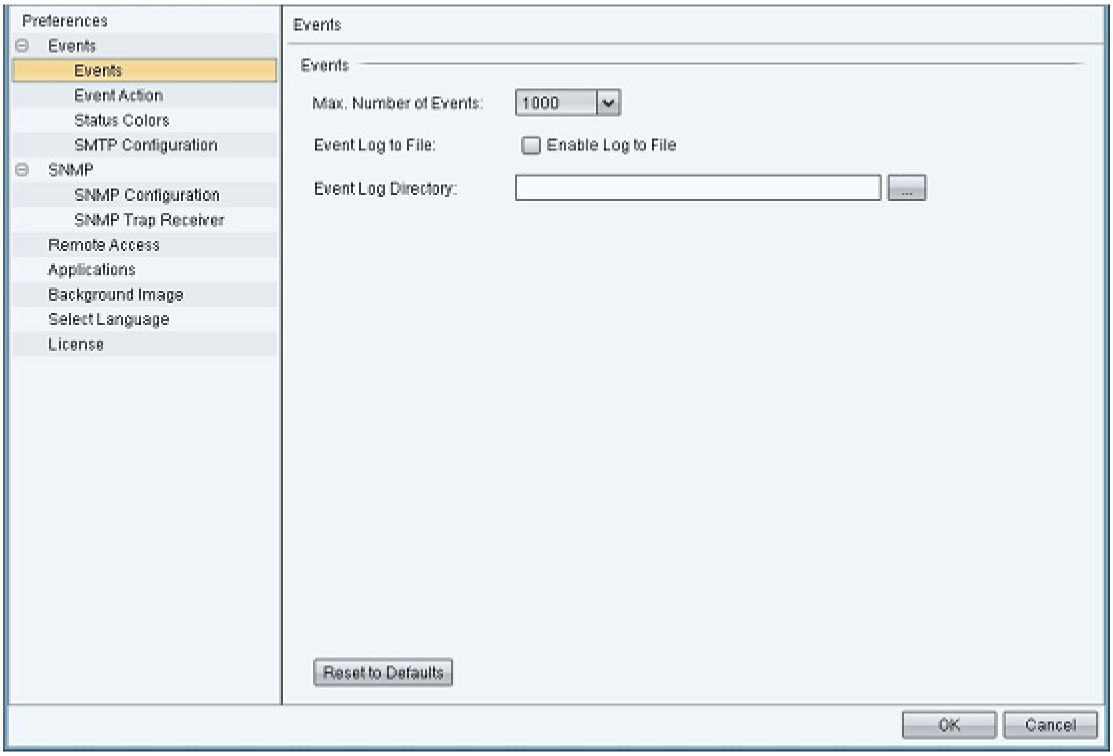
- Mouse Double-Click on the line between the two devices
- The traffic report only available if the network connection is present
- The traffic tab provides an indication of the network traffic for the connection

10. Preferences

Event

Events

This page allows you to record events into the log file. You can change maximum number of traps, trap log to file and trap log directory.



Events

Max. Number of Events: 1000

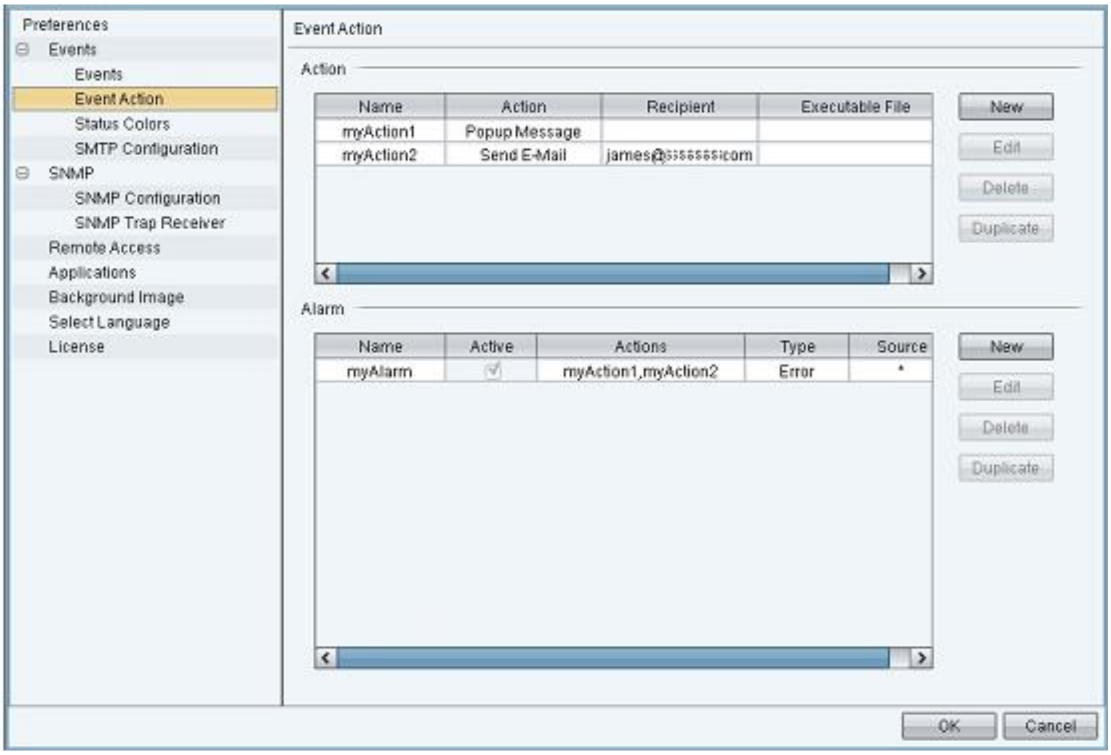
Event Log to File: □ Enable Log to File

Event Log Directory:

Figure 10–1. Events Preferences

Events Action

This page allows you to manage Actions and Alarms; the management functions include *New, Edit, Delete and Duplicate.*



Event Action

Action

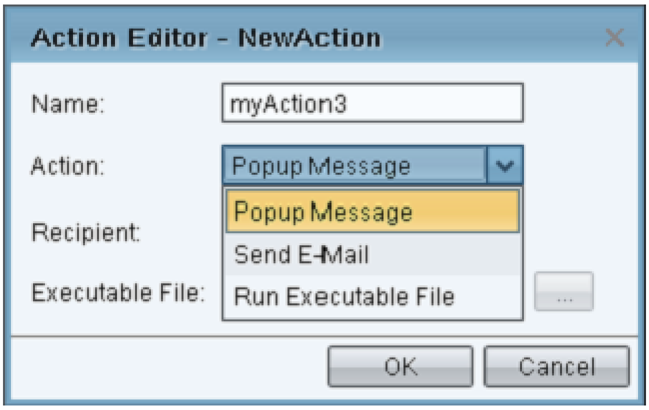
Name	Action	Recipient	Executable File
myAction1	Popup Message		
myAction2	Send E-Mail	james@ssssss.com	

Alarm

Name	Active	Actions	Type	Source
myAlarm	☑	myAction1,myAction2	Error	*

Figure 10–2. Event Action

If you press *New*, *Edit*, *Delete* or *Duplicate of Action*, the Action Editor will pop up for Action configuring.



Name: myAction3

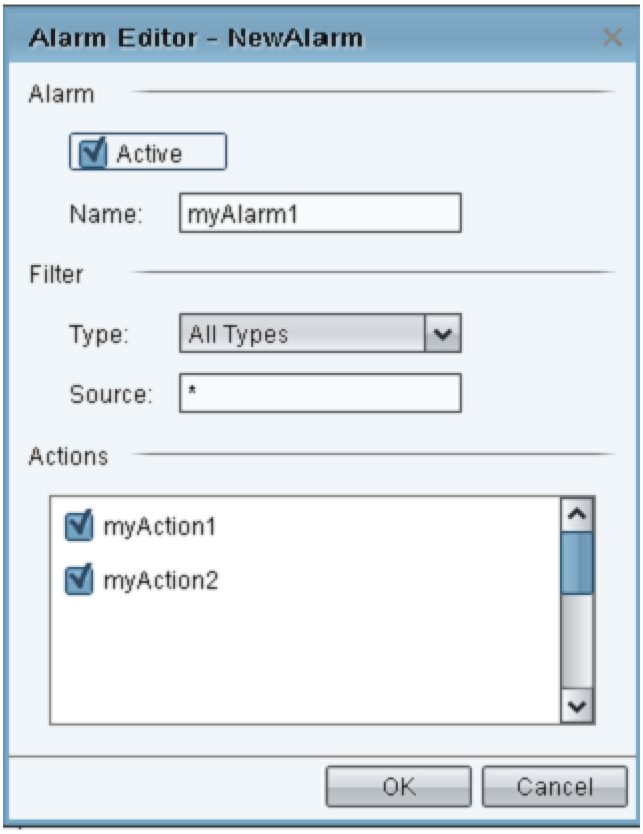
Action: Popup Message

Recipient:

Executable File:

Figure 10–3. Action Editor – New Action

If you press *New, Edit, Delete or Duplicate of Alarm*, the Alarm Editor will pop up for Alarm configuring.



Alarm Editor - NewAlarm

Alarm

☑ Active

Name: myAlarm1

Filter

Type: All Types

Source: *

Actions

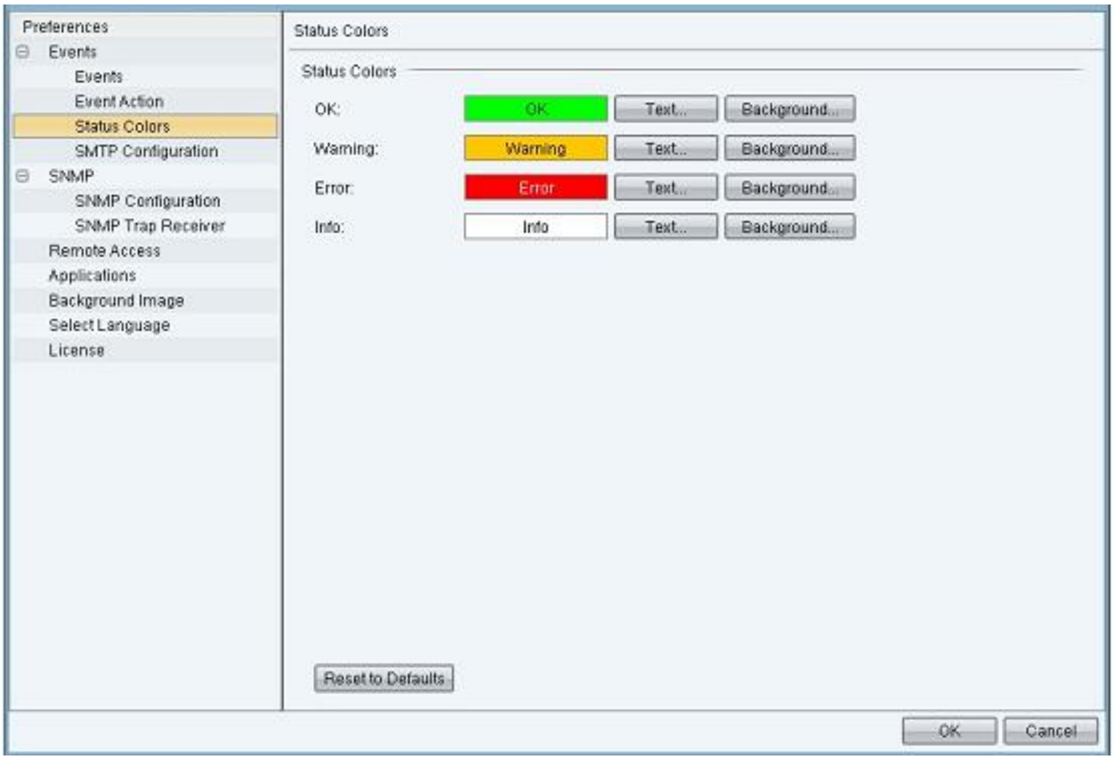
☑ myAction1

☑ myAction2

Figure 10–4. Alarm Editor – New Alarm

Status Colors

This page allows you to assign a color to each status. You can change text and background color of 4 types status.



OK: OK

Warning: Warning

Error: Error

Info: Info

Figure 10–5. Editing Event Status Colors

SMTP Configuration

While you use to send Email function for Event Action, you must set SMTP Configuration. If SMTP server requests you to authorize first, you can also set up the username and password in this page. And you can press *Test SMTP configuration* to test your configuration after you finish this configuration.

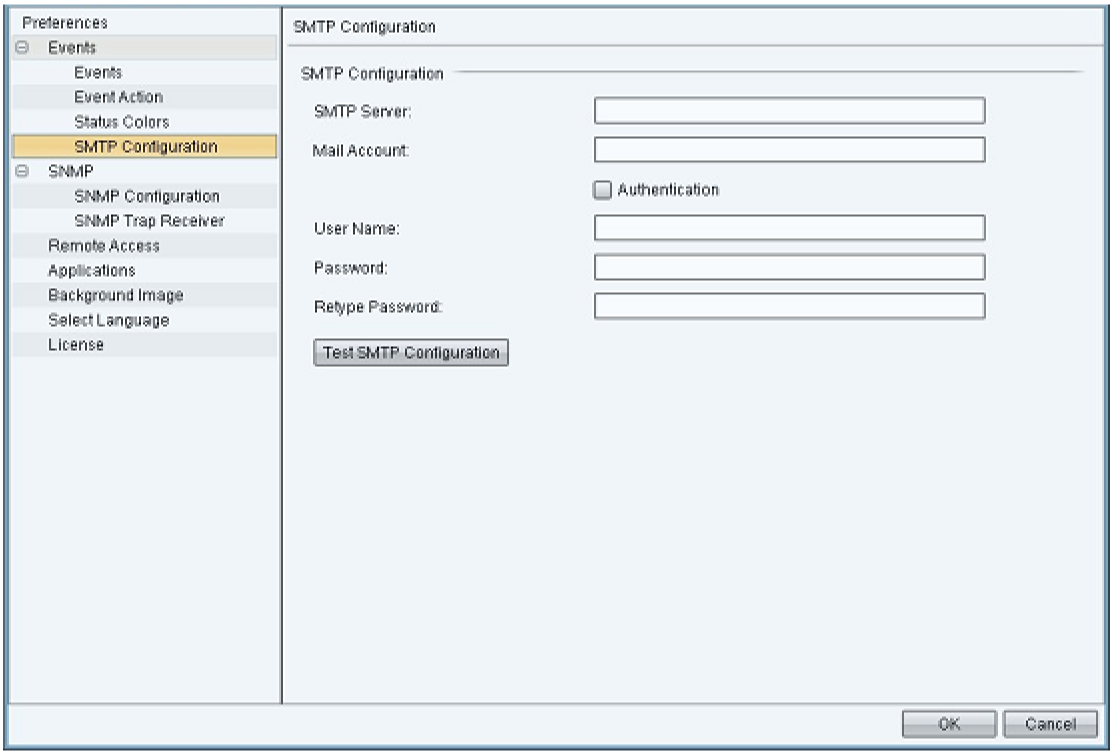
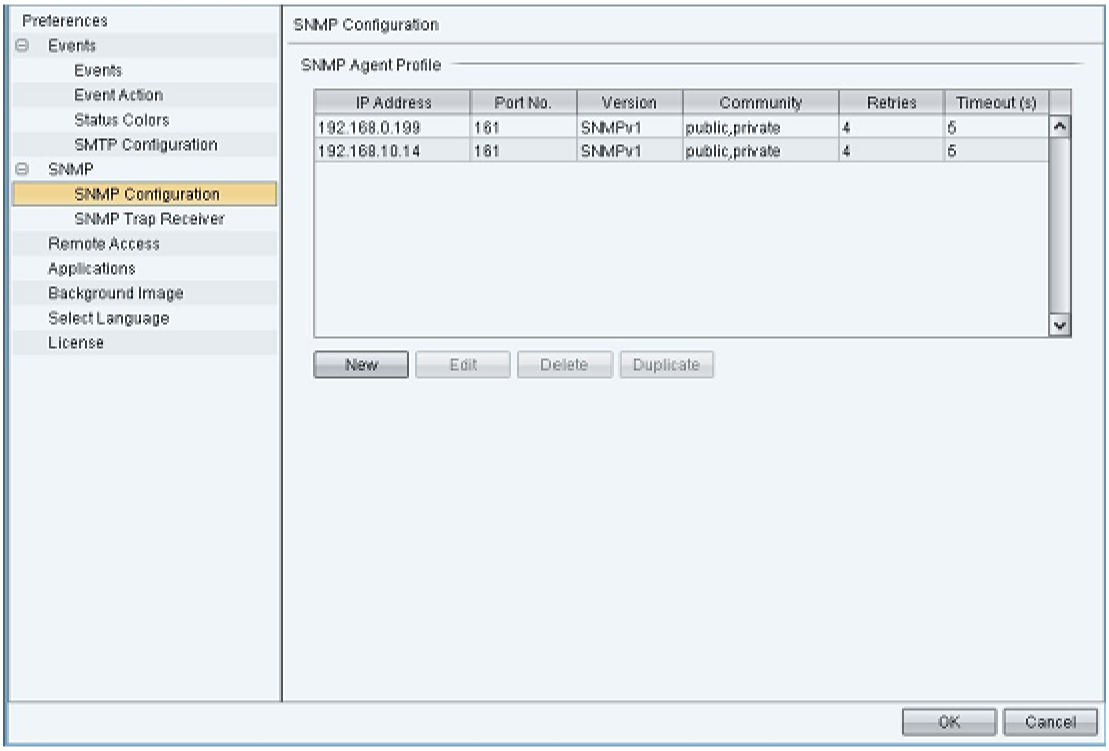


Figure 10–6. SMTP Configuration

SNMP

SNMP Configuration

The JetView Pro will add a default SNMP agent profile for discovered devices. You can use this page to new, edit, delete or duplicate a profile. The configurations of profile include agent listening port (default is 161), SNMP version (support v1/v2c/v3), read/write community, retry numbers and timeout (in second(s)).

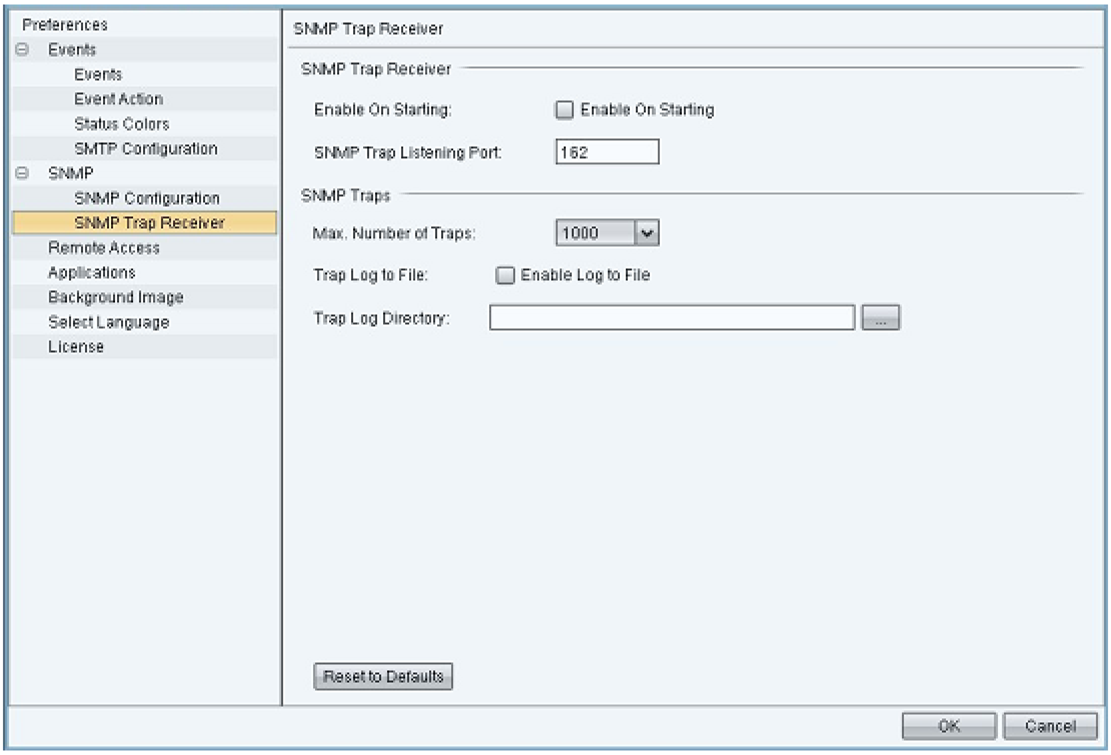


IP Address	Port No.	Version	Community	Retries	Timeout (s)
192.168.0.199	161	SNMPv1	public,private	4	5
192.168.10.14	161	SNMPv1	public,private	4	5

Figure 10–7. SNMP Configurations

SNMP Trap Receiver

This page allows you to configure SNMP Trap Receiver and record SNMP Trap into the log file. You can enable the SNMP Trap Receiver on system starting, change listening port, change maximum number of traps, trap log to file and trap log directory.



SNMP Trap Receiver

SNMP Trap Receiver

Enable On Starting: □ Enable On Starting

SNMP Trap Listening Port: 162

SNMP Traps

Max. Number of Traps: 1000

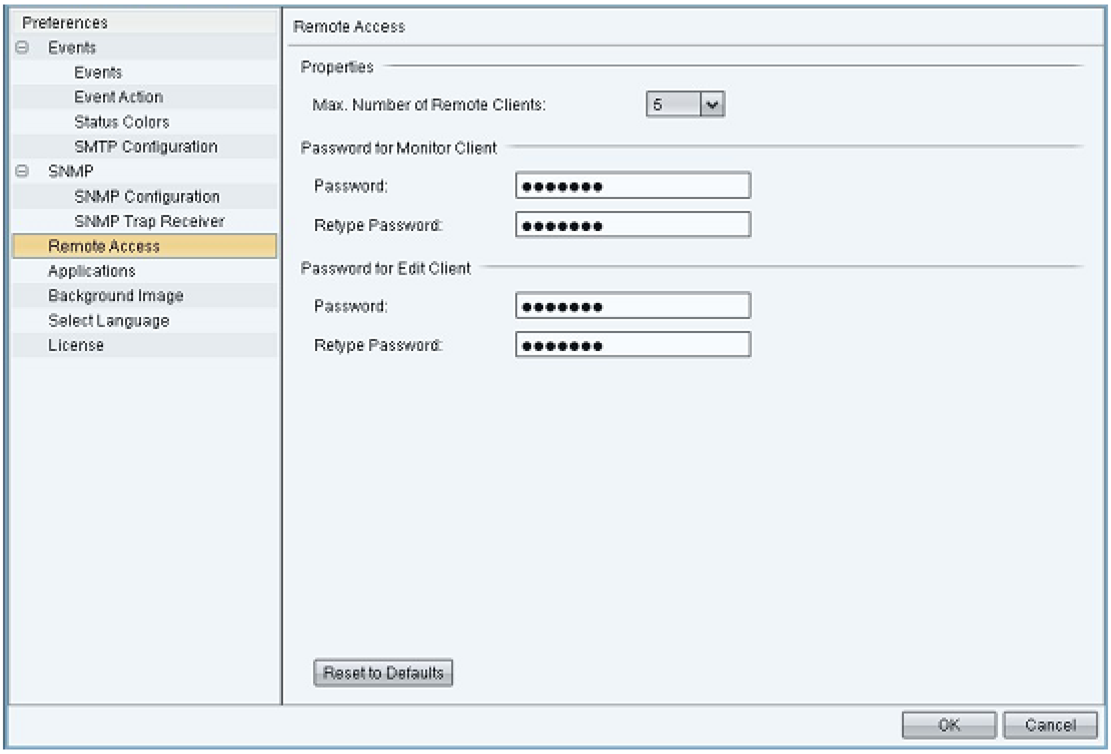
Trap Log to File: □ Enable Log to File

Trap Log Directory:

Figure 10–8. SNMP Trap Receiver Configuration

Remote Access

Due to the access synchronization, we only allow one client to enter the Edit mode at the same time and the other clients on Monitor mode. The Monitor mode can only allow viewer to browse the topology. Edit mode can use all functions. The maximum number of remote client is default 5. You can setup new passwords on Monitor and Edit mode.



Remote Access

Properties

Max. Number of Remote Clients: 5

Password for Monitor Client

Password: ●●●●●●●

Retype Password: ●●●●●●●

Password for Edit Client

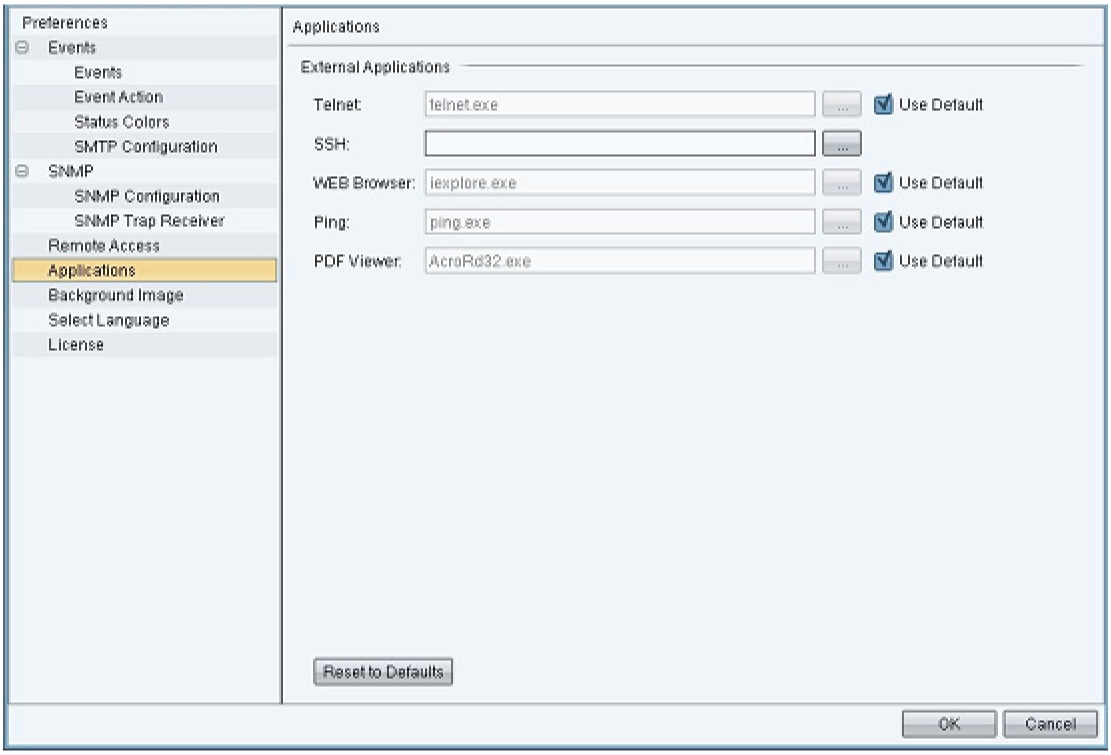
Password: ●●●●●●●

Retype Password: ●●●●●●●

Figure 10–9. SNMP Remote Access Configuration

Applications

The JetView Pro uses external applications for the functions. This page allows you to assign specified programs or use default application to run the functions.



Applications

External Applications

Telnet: telnet.exe ... ☑ Use Default

SSH: ...

WEB Browser: iexplore.exe ... ☑ Use Default

Ping: ping.exe ... ☑ Use Default

PDF Viewer: AcroRd32.exe ... ☑ Use Default

Figure 10–10. SNMP Application Configurations

Background Image

This page allows you to configure background image for topology map. You can select an image file to change the default background image.

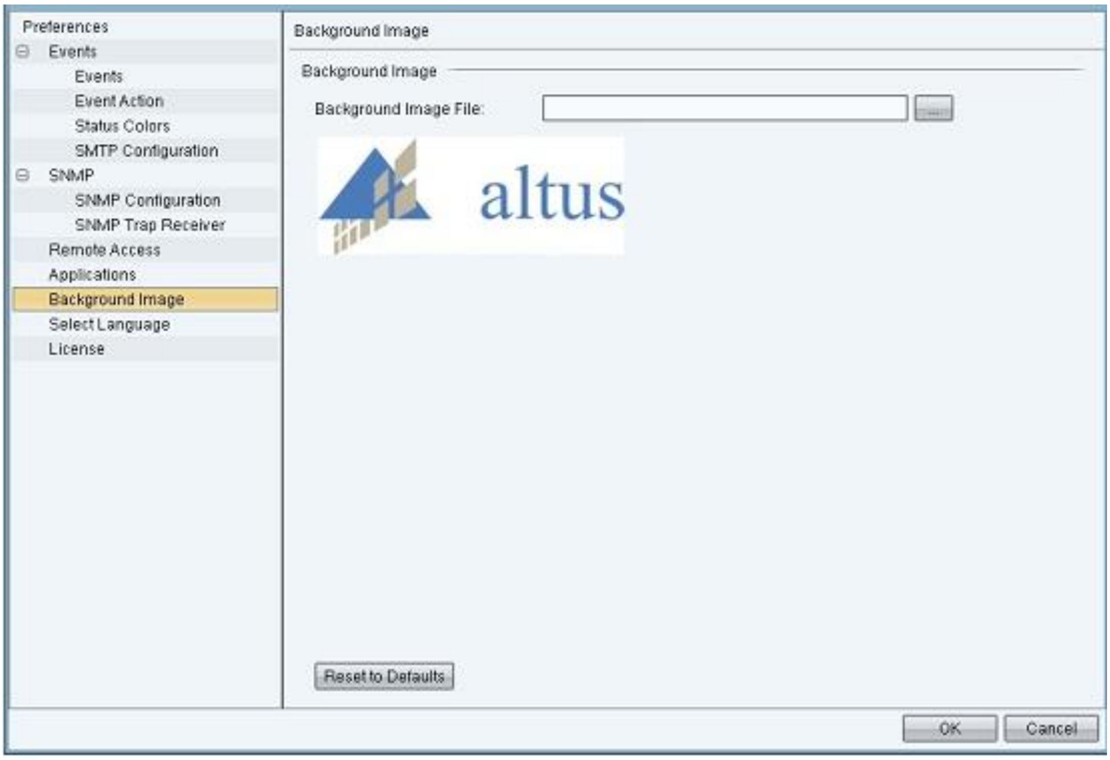
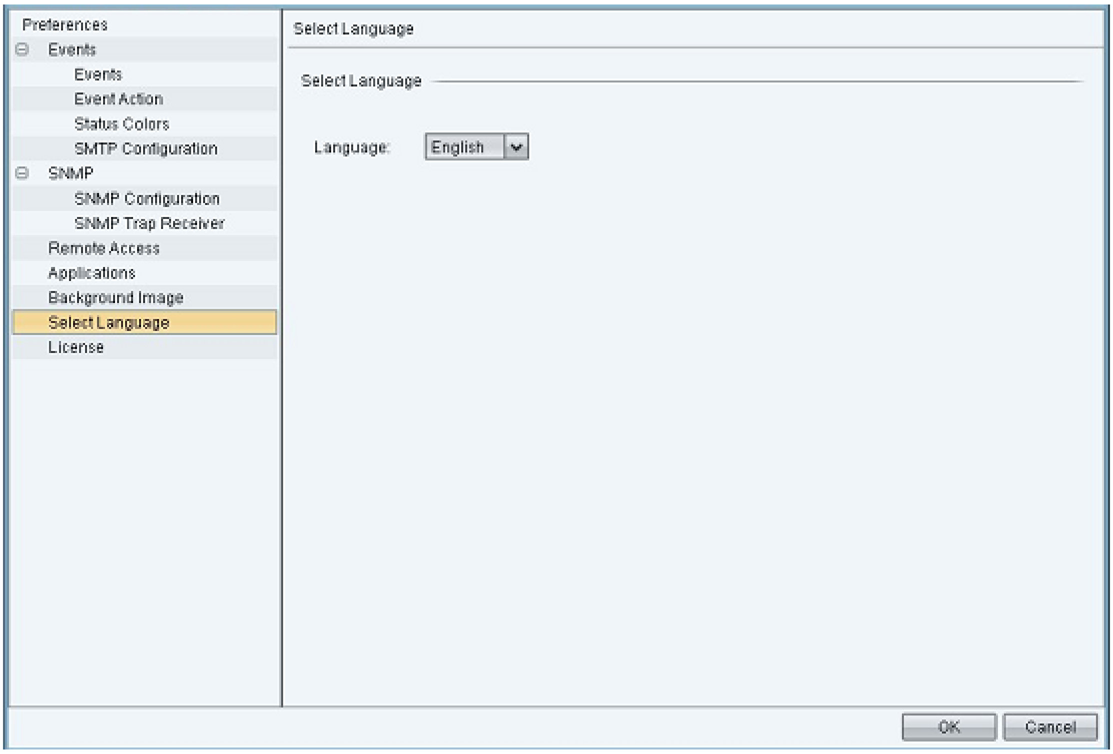


Figure 10–11. SNMP Background Image Configuration

Select Language

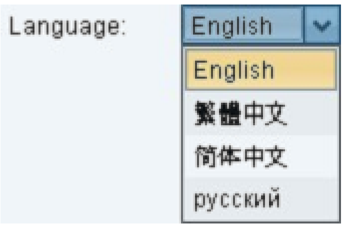
JetView Pro support 4 language interfaces.



Language: English

Figure 10–12. Selecting Language

You can change JetView Pro display interface by selecting a language option. The Language will apply immediately.



Language: English

Figure 10–13. Language Options

11. Glossary

Baud rate Rate in which information bits are transmitted through a serial interface or communication network (measured in Bits/second, bps)

Bit Basic information unit, it may be at 1 or 0 logic level.

Bus Set of electrical signals that are part of a logic group with the function of transferring data and control between different elements of a subsystem

Byte Information unit composed by eight bits.

Communication Network Set of devices (nodes) interconnected by communication channels.

CPU Central Processing Unit. It controls the data flow, interprets and executes the program instructions as well as monitors the system devices.

Database A group of data organized in a table.

Default A value that is commonly used as a standard

Diagnostic Procedures to detect and isolate failures. It also relates to the data set used for such tasks, and serves for analysis and correction or problems.

Download Information that is sent to some device/path.

ESD Electrostatic Discharge.

Firmware The operating system of a PLC. It controls the PLC basic functions and executes the application programs.

Frame Information unit transmitted in the network.

Gateway Device to connect two communication networks with different protocols.

Hardkey Connector normally attached to the parallel port of a microcomputer to avoid the use of illegal software copies

Hardware Physical equipment used to process data where normally programs (software) are executed

I/O See Input/Output.

Input/output Also known as I/O. Data input or output devices in a system. In PLCs these are typically the digital or analog modules that monitor or actuate the devices controlled by the system.

Interface Normally used to refer to a device that adapts electrically or logically the transferring of signals between two equipments.

Kbytes Memory size unit. Represents 1024 bytes.

LED Light Emitting Diode. Type of semiconductor diode that emits light when energized. It’s used for visual feedback.

Master Device connected to a communication network originating all the command requests to other network units.

Master-slave communication network Communication network where the data transfer are initiated only by one node (the network master). The remaining network nodes (slaves) only reply when requested.

Media access Method used by all nodes in a network to synchronize data transmission and solve possible conflicts in simultaneous transmissions.

Menu Set of available options for a program, they may be selected by the user in order to activate or execute a specific task

Module (hardware) Basic element of a system with very specific functionality. It’s normally connected to the system by connectors and may be easily replaced.

Module (software) Part of a program capable of performing a specific task. It may be executed independently or in conjunction with other modules through information sharing by parameters.

Module address: Address used by the CPU in order to access a specific I/O module.

Node Any station in a network with the capacity to communicate using a determined protocol.

Operands Elements on which software instructions work. They may represent constants, variables or set of variables.

PLC See Programmable Controller.

Programming Language Set of rules, conventions and syntaxes utilized when writing a program.

Protocol Procedures and formats rules that allow data transmission and error recovery among devices with the use of control signals

RAM Random Access Memory. Memory where all the addresses may be accessed directly and in random order at the same speed. It is volatile, in other words, its content is erased when powered off, unless there is a battery to keep its contents.

RX Acronym used to indicate serial reception.

Serial Channel Unit interface that transfers data serially.

Software Computer programs, procedures and rules related to the operation of a data processing system

Sub network Segment of a communication network that connects a group of devices (nodes) with the goal of isolating the local data traffic or using different protocols or physical media.

Supervisory Station Equipment connected to a PLC network with the goal of monitoring and controlling the process variables

Tag Name associated to an operand or to logic that identifies its content.

Time-out Maximum preset time to a communication to take place. When exceeded, then retry procedures are started or diagnostics are activated.

Toggle Element with two stable states that are switched at each activation.

TX Acronym used to indicate serial transmission.

Upload Reading a program or configuration from the PLC.

Word Information unit composed by 16 bits.