WoMaster

COVER

User Manual

NetMaster

Industrial Network Management System

May.15.2019 V.1.2

www.womaster.eu

WoMaster

NetMaster Industrial Network Management System

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and to configure the NetMaster. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with the installation, inspection, and utilization of this software.

Disclaimer

WoMaster reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to WoMaster. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. WoMaster assumes no responsibility for its use by the third parties.

WoMaster Online Technical Services

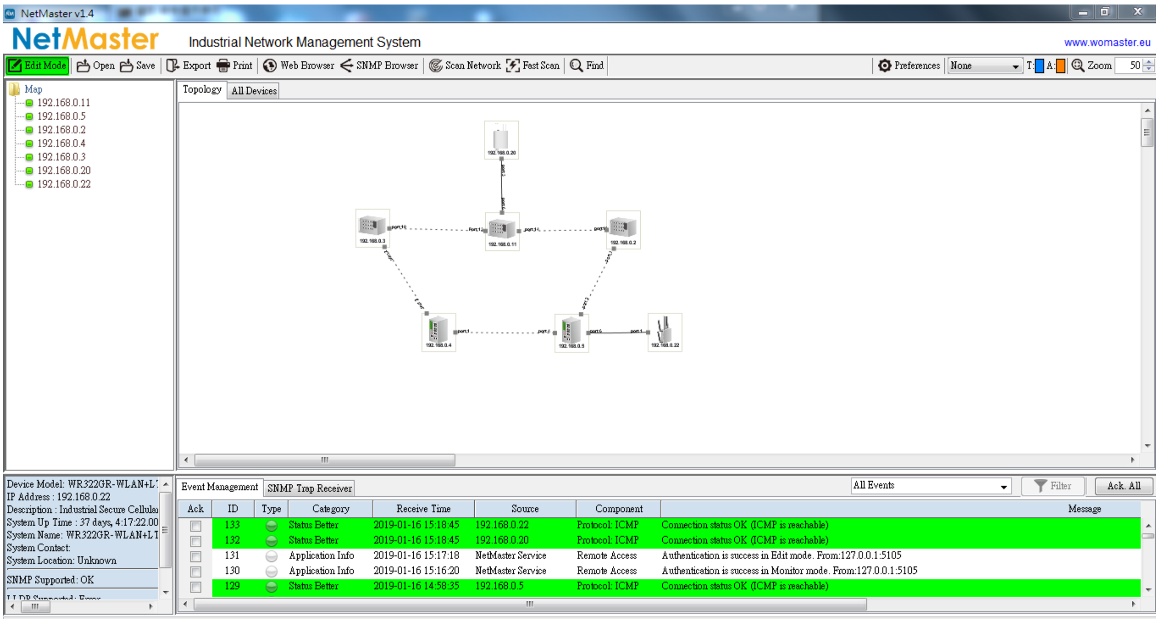
At WoMaster, you can use the online service forms to request the support. The submitted forms are stored in server for WoMaster team member to assign tasks and monitor the status of your service. Please feel free to write to help@womaster.eu if you encounter any problems.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The NetMaster Industrial Network Management System software is designed for network device discovery, configuration, auto topology, real time monitor, and diagnostic. It secures network devices, physical links and resilient network in mission critical industrial networks. The NetMaster manages device configurations, firmware versions and upgrades, fault alert and event logs. A server client operation is designed to ensure network reliability in large scale network up to 2000 nodes including wireless and 3rd party compliant devices. It can be freely download for 20 nodes trial.



Device Model: WR322GR-WLAN+L1
IP Address : 192.168.0.22
Description : Industrial Secure Cellula
System Up Time : 37 days, 4:17:22.00
System Name: WR322GR-WLAN+L1
System Contact:
System Location: Unknown
SNMP Supported: OK
LLDP Supported: Error

Ack	ID	Type	Category	Receive Time	Source	Component	Message
□	133	●	Status Better	2019-01-16 15:18:45	192.168.0.22	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	132	●	Status Better	2019-01-16 15:18:45	192.168.0.20	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	131	○	Application Info	2019-01-16 15:17:18	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5105
□	130	○	Application Info	2019-01-16 15:16:20	NetMaster Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5105
□	129	●	Status Better	2019-01-16 14:58:35	192.168.0.5	Protocol: ICMP	Connection status OK (ICMP is reachable)

Model Name	Description
NetMaster-20	Industrial Network Management System software with a free license for 20 nodes
NetMaster-50	Industrial Network Management System software with a license for 50 nodes
NetMaster-100	Industrial Network Management System software with a license for 100 nodes
NetMaster-250	Industrial Network Management System software with a license for 250 nodes license
NetMaster-500	Industrial Network Management System software with a license for 500 nodes license
NetMaster-1000	Industrial Network Management System software with a license for 1000 nodes license
NetMaster-2000	Industrial Network Management System software with a license for 2000 nodes license

1.2 KNOWN RESTRICTIONS OR LIMITATION

1. The ERPS main screen indicates that the "dotted line" of the detected connection between the DUTs is incorrect.
2. Open NetMaster then insert LAN port, the LAN interface hasn't updated.
3. When Firmware writing, the status will show error display.
4. Event log show error display when user changes the language.
5. Can't do multi-device refresh, ping & telnet if don't login edit mode.
6. More than 500 sets, can't sweep all machines at once.
7. There is no way to change/add MIB value if the type is table view.

1.3 MAJOR FEATURES

Below are the major features of NetMaster:

- Automatic discovery and intuitive visualization of network devices, wireless devices, physical link and network topology
- Real-time status of device availability and traffic performance for physical links
- Server-client operation to ensure network system reliability especially in large scale networks
- High scalability for up to 2000 network nodes
- MIB compiler and MIB browser for private MIBs and MIBs of 3rd party device
- Fault Alert and event logs including source IP filter, network error, login record and warning
- SNMP Trap receiver for all or specific IP addresses
- Multi-language support including English, Chinese & Russian

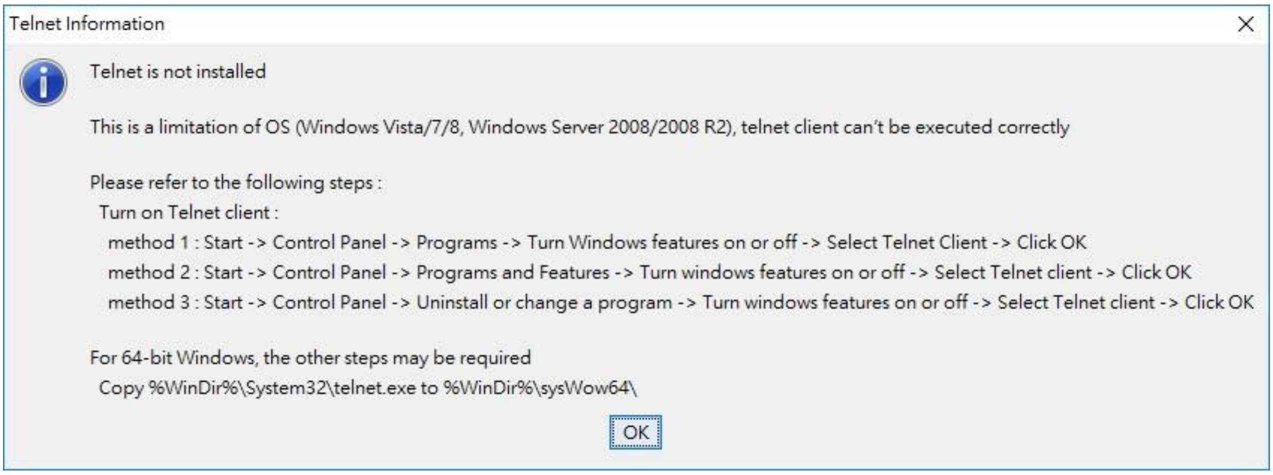
2. NETMASTER INSTALLATION

2.1 SYSTEM REQUIREMENTS

- CPU: Intel Core i5
- RAM: 8GB
- HD space: 1GB
- OS: Windows 7 or Windows 10
- LAN: 100MB or 1000MB Ethernet LAN card

Windows Vista/7/8, Windows Server 2008/ 2008 R2 notice:

Turn on telnet system commands



Telnet Information

Telnet is not installed

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\

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\

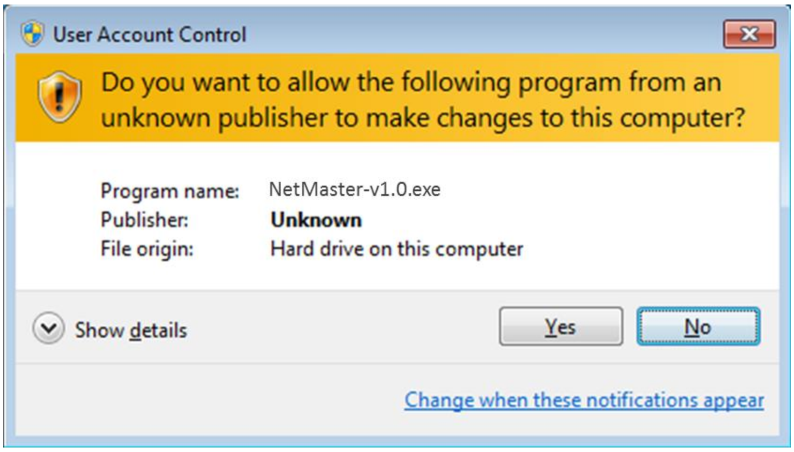
NOTE: When user upgrades the software from V1.0~V1.3 to V1.4, please use the uninstall procedure. Then install the V1.4 from the beginning.

2.2 INSTALLATION

This chapter contains information on NetMaster installation procedures.

STEP 1: Download the NetMaster installation file to computer (https://www.womaster.eu/ download.php). Extract the file and to run the setup program by double clicking the NetMaster-vX.X.exe icon.

STEP 2: Click the installer file, and a warning message from Windows about User Account Control will appear then click **Yes**.

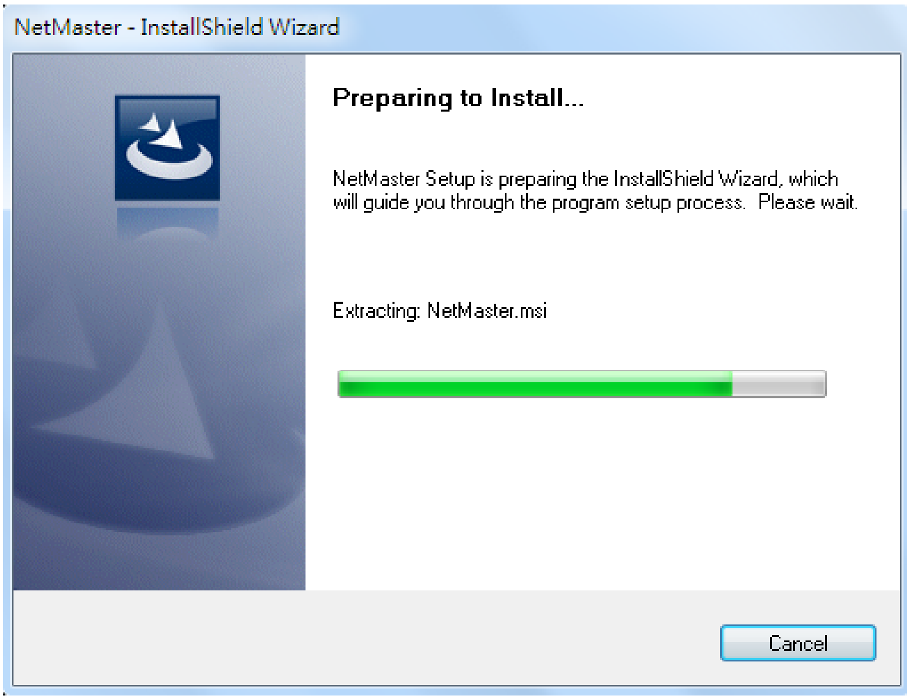


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: NetMaster-v1.0.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

STEP 3: A preparing to install form will appear and wait till extracting the NetMaster.msi file is complete



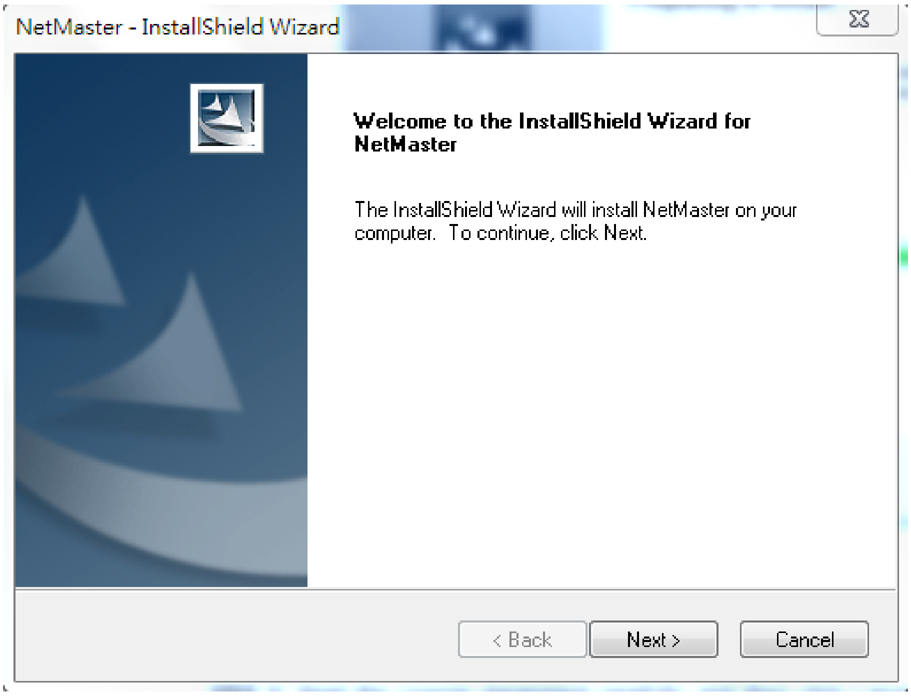
NetMaster - InstallShield Wizard

Preparing to Install...

NetMaster Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Extracting: NetMaster.msi

STEP 4: Click **Next** to install NetMaster installer.

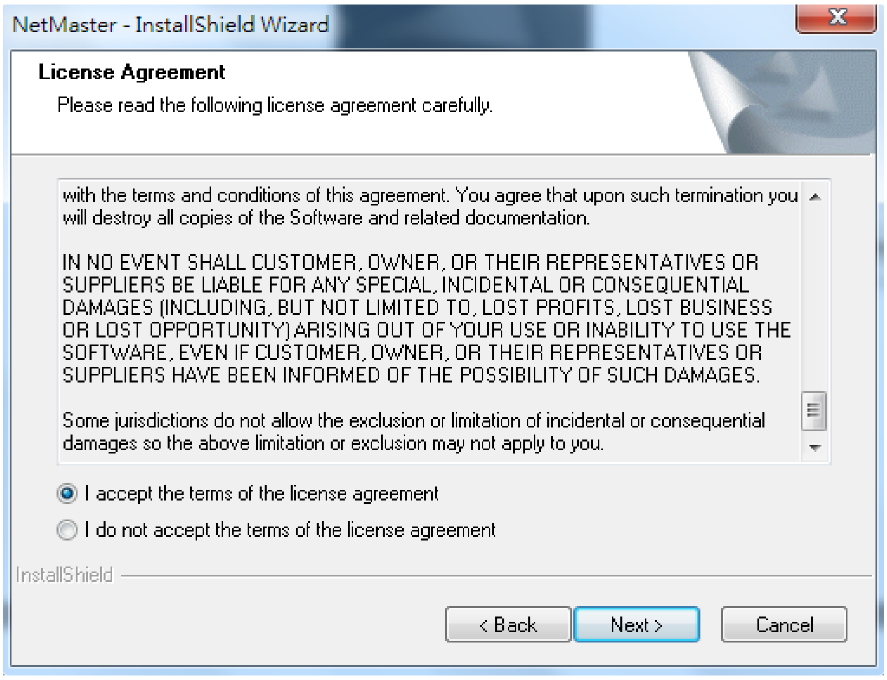


NetMaster - InstallShield Wizard

Welcome to the InstallShield Wizard for NetMaster

The InstallShield Wizard will install NetMaster on your computer. To continue, click Next.

STEP 5: Read the License Agreement carefully, and then click I accept the terms of the license agreement. Click Next to continue.



NetMaster - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

with the terms and conditions of this agreement. You agree that upon such termination you will destroy all copies of the Software and related documentation.

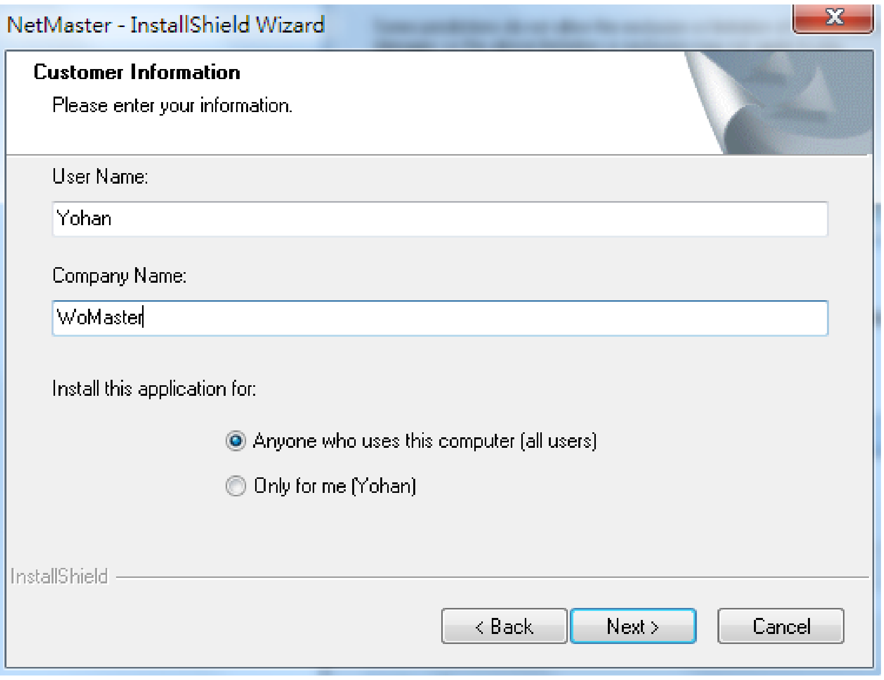
IN NO EVENT SHALL CUSTOMER, OWNER, OR THEIR REPRESENTATIVES OR SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOST BUSINESS OR LOST OPPORTUNITY) ARISING OUT OF YOUR USE OR INABILITY TO USE THE SOFTWARE, EVEN IF CUSTOMER, OWNER, OR THEIR REPRESENTATIVES OR SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages so the above limitation or exclusion may not apply to you.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

STEP 6: Fill the Customer Information form User Name and Company Name, and also choose for who user install the application for. After that click Next to continue.



NetMaster - InstallShield Wizard

Customer Information

Please enter your information.

User Name:

Yohan

Company Name:

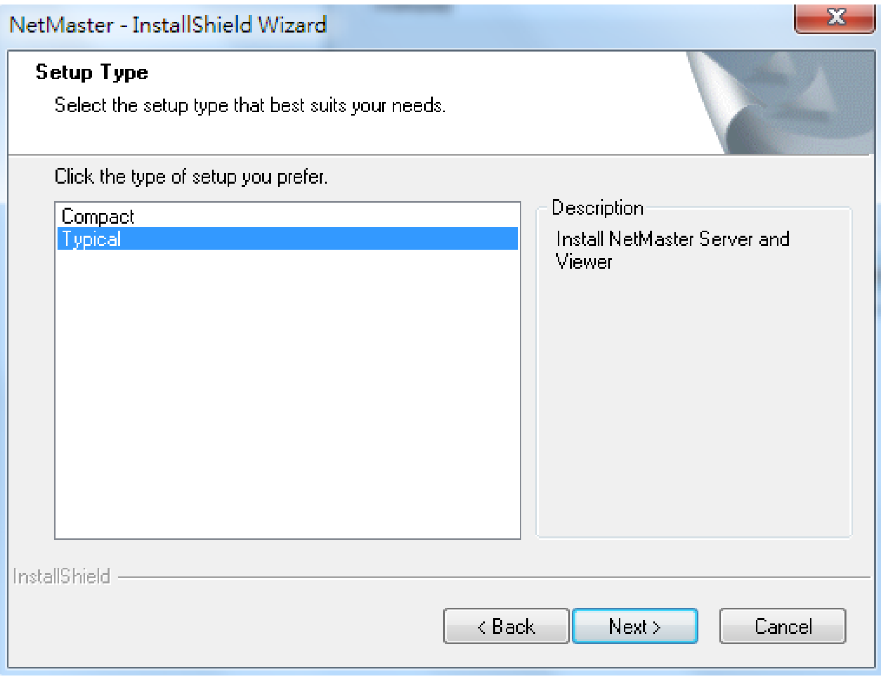
WoMaster

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Yohan)

STEP 7: Select the type of setup, **Compact** for installing the NetMaster Viewer only as a client or **Typical** for installing both NetMaster Server and Viewer, then click Next to continue.



NetMaster - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Click the type of setup you prefer.

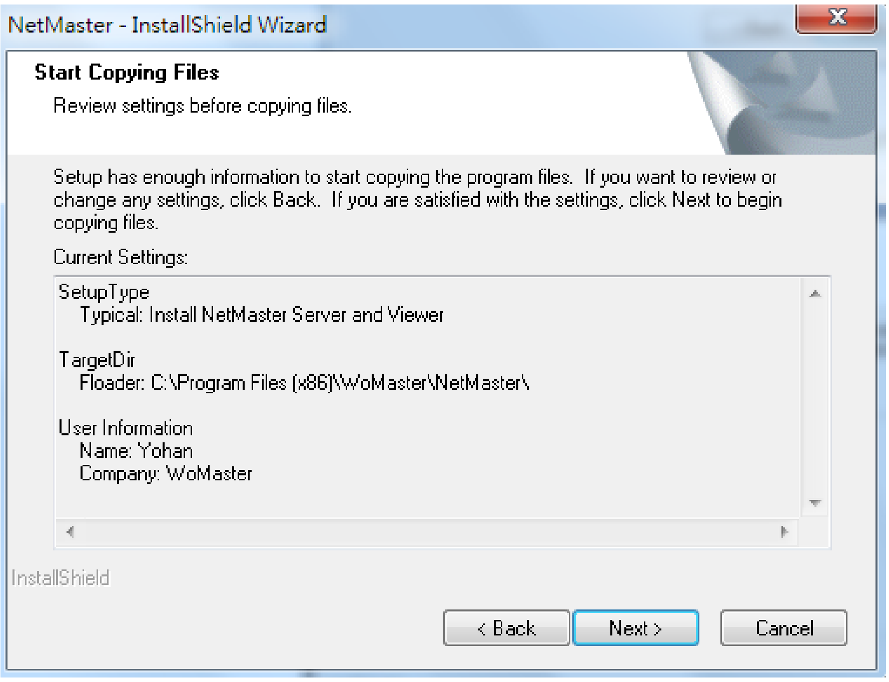
Compact

Typical

Description

Install NetMaster Server and Viewer

STEP 8: Verify that all of the information are correct, and then click Next to continue.



NetMaster - InstallShield Wizard

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

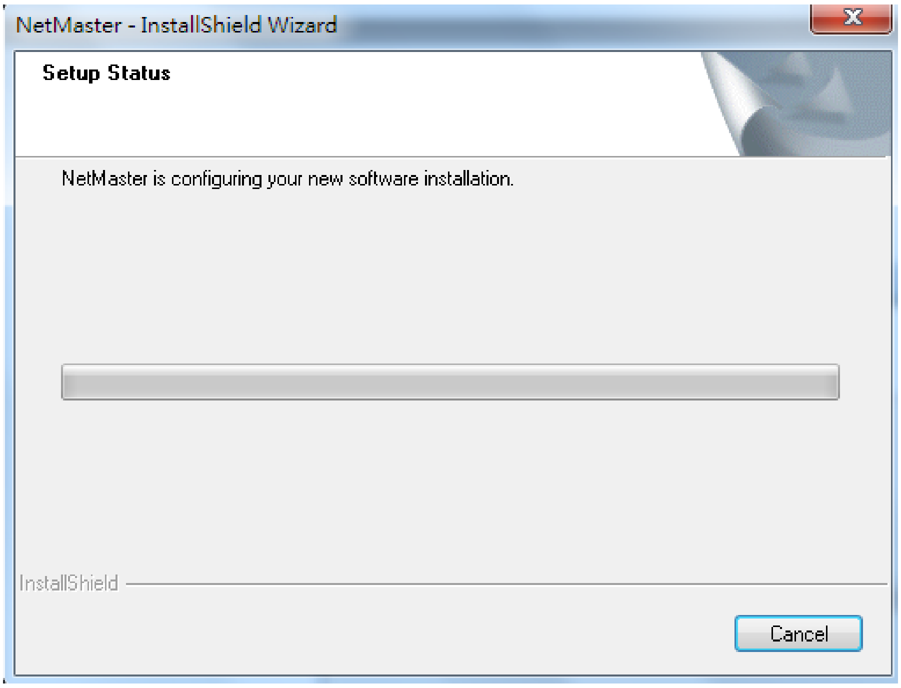
Current Settings:

SetupType
    Typical: Install NetMaster Server and Viewer

TargetDir
    Floader: C:\Program Files (x86)\WoMaster\NetMaster\

User Information
    Name: Yohan
    Company: WoMaster

STEP 9: Wait while the program is installed.

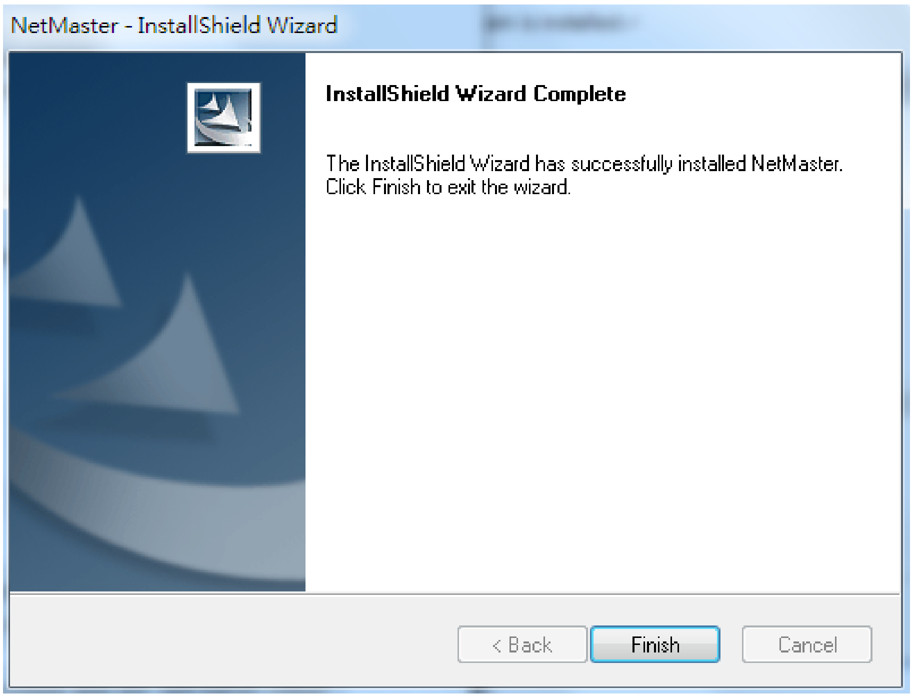


NetMaster - InstallShield Wizard

Setup Status

NetMaster is configuring your new software installation.

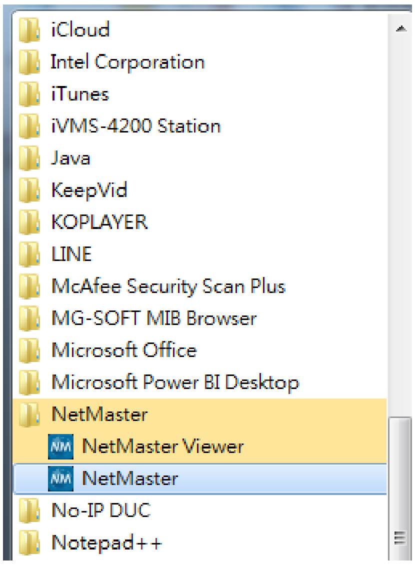
STEP 10: Click **Finish** to complete the installation.


NetMaster - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed NetMaster.
Click Finish to exit the wizard.

STEP 11: To open the user interface of the NetMaster, click Start > Programs > NetMaster



After that the NetMaster interface will appear. When the software is ready, user may click the Edit Mode and enter the default password "admin" then the list will show up some devices that detected by the interface.

2.3 UNINSTALLATION

Remember to quit the NetMaster program before user gets starting the uninstallation procedure. Follow below steps to uninstall the software:

1. To uninstall NetMaster, select **Start** / **Control Panel** / **Add or Remove.**

2. Select the program NetMaster.

3. Click on **Remove** and follow the instructions of the uninstallation procedure.

3. GETTING STARTED WITH NETMASTER

This chapter is included the NetMaster Featured Configuration, user will see all of NetMaster various configuration menus inside the NetMaster interface. Through this web management interface user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the switch on the network.

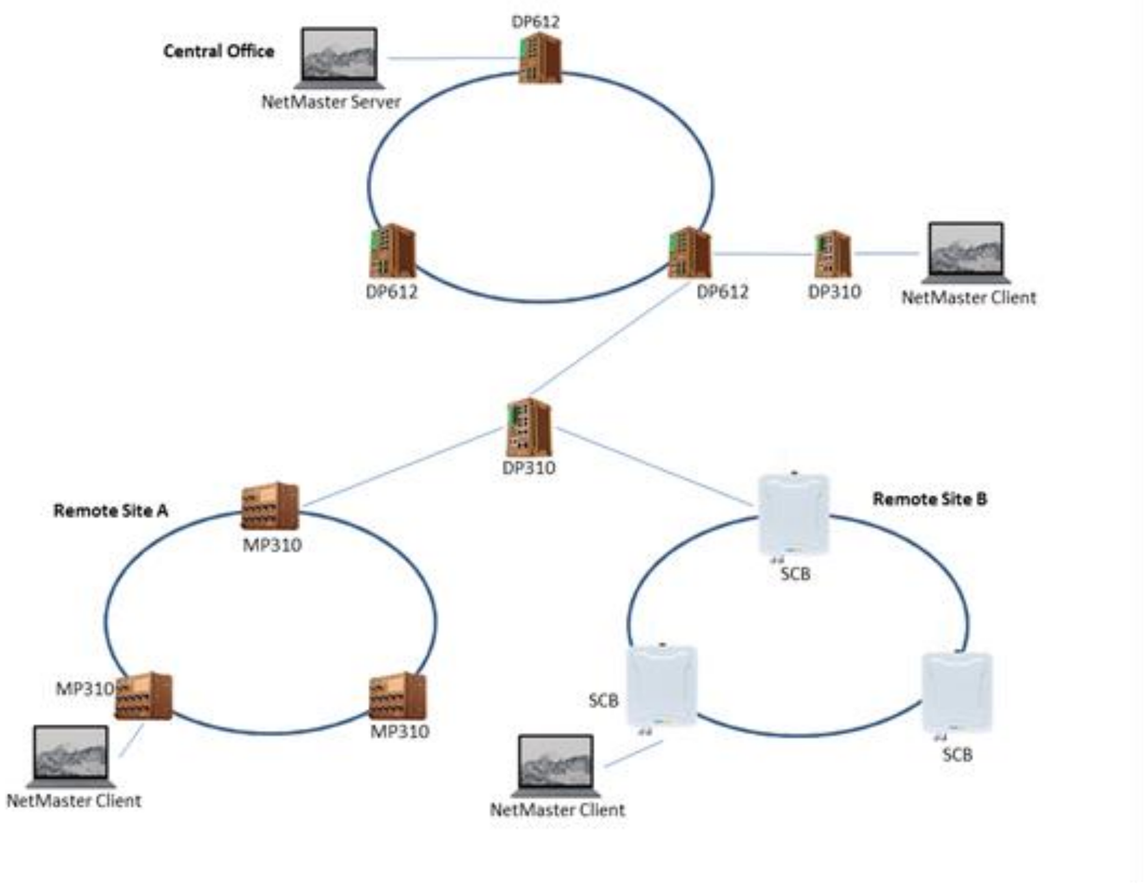
Following topics are covered in this chapter:

3.1 NetMaster Application

3.2 NetMaster Server & Client

3.1 NETMASTER APPLICATION

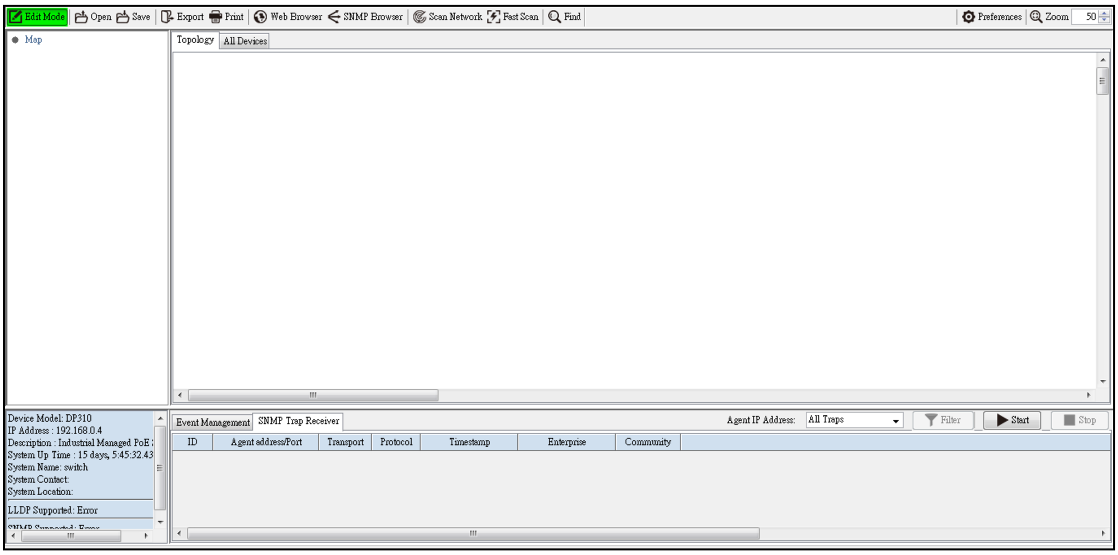
NetMaster is a client/server based network system. One NetMaster server can serve maximum 5 remote access NetMaster clients.



3.2 NETMASTER SERVER & CLIENT

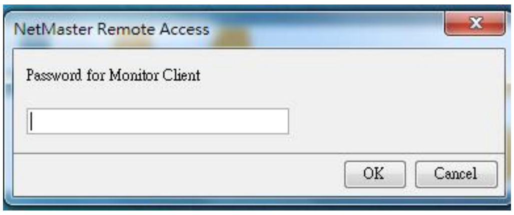
NetMaster Server

The NetMaster Server is limited for 5 clients only. When user clicks the icon, it will ask user to enter the password for monitor client. (Default password: admin). And a white blank screen will appear.

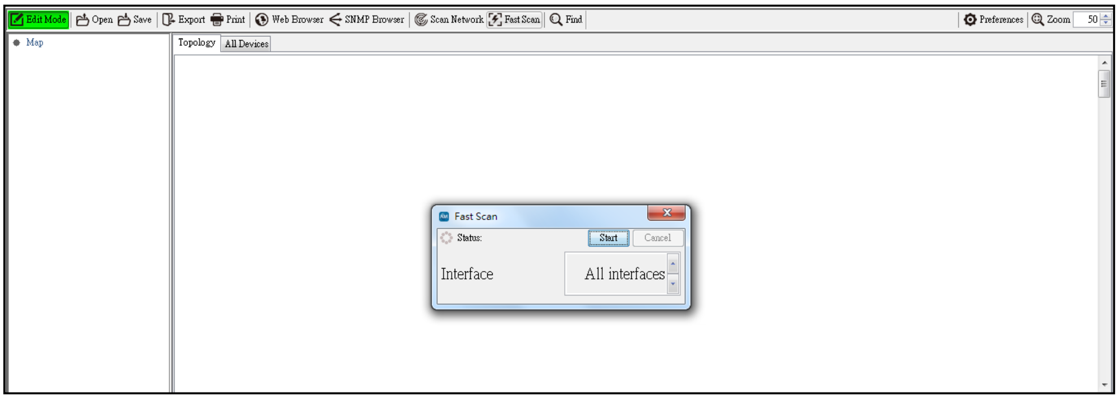


Device Model: DP310
IP Address : 192.168.0.4
Description : Industrial Managed PoE :
System Up Time : 15 days, 5:45:32.43
System Name: switch
System Contact:
System Location:
LLDP Supported: Error
SNMP Supported: Error

Click the Edit mode and once again enter the password, so user can enter the edit mode.

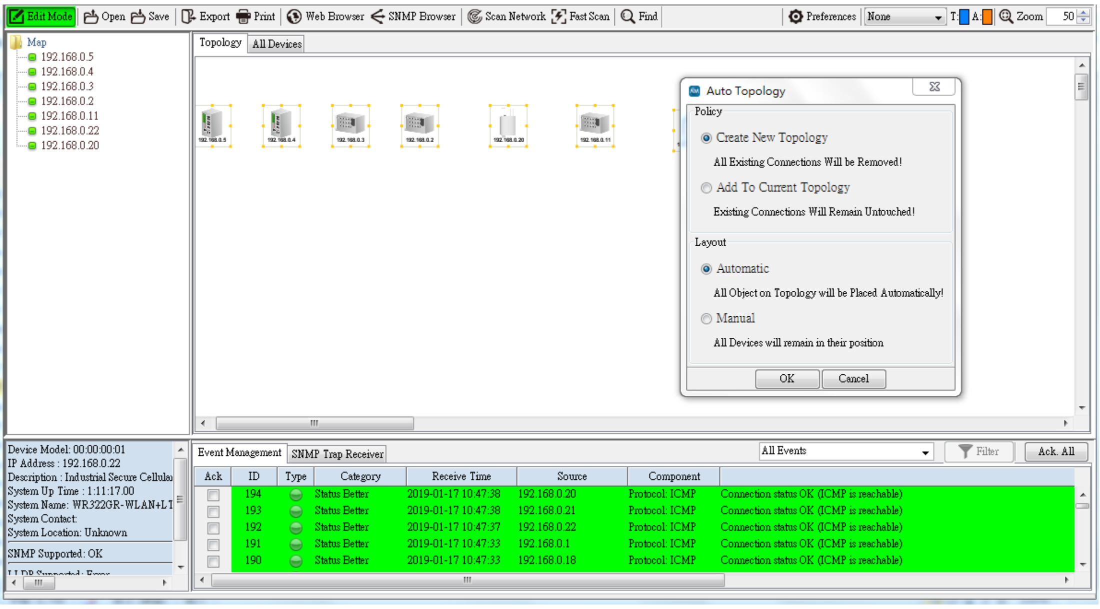


Click Fast Scan, to discover the device through the interface. User may choose the interface.



Interface: All interfaces

After all of the devices are discovered (wireless and switch devices), they will appear on the dashboard. Then user needs to create the topology by do the right click on the dashboard, and choose **Auto Topology**. And another menu will appear then click **OK** and click **Start** to let the NMS draw the topology.



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

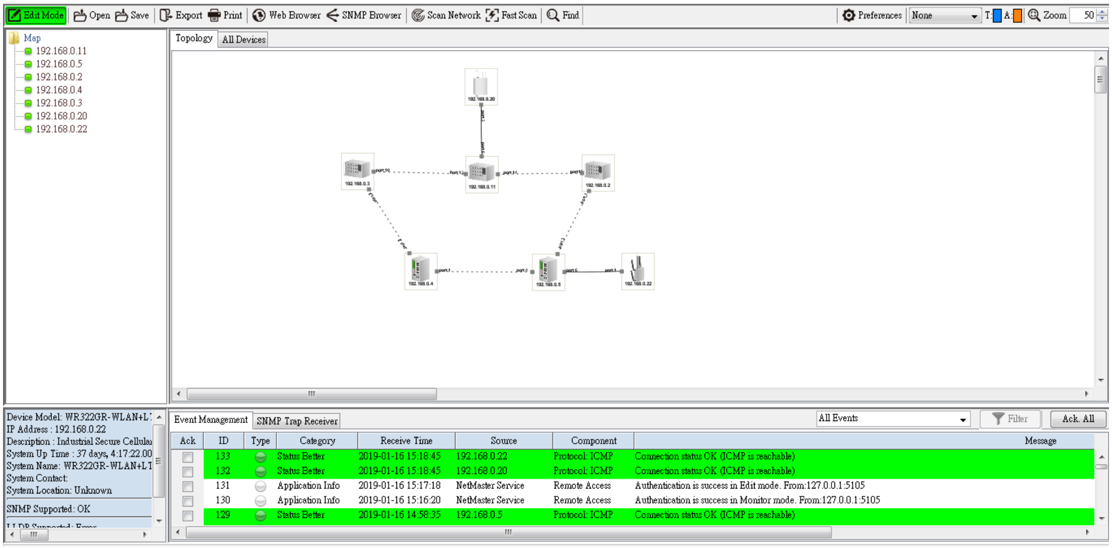
OK Cancel

Device Model: 00:00:00:01
IP Address : 192.168.0.22
Description : Industrial Secure Cellula
System Up Time : 1:11:17.00
System Name: WR322GR-WLAN+LT
System Contact:
System Location: Unknown
SNMP Supported: OK

Event Management | SNMP Trap Receiver | All Events | Filter | Ack. All

Ack	ID	Type	Category	Receive Time	Source	Component	
□	194	●	Status Better	2019-01-17 10:47:38	192.168.0.20	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	193	●	Status Better	2019-01-17 10:47:38	192.168.0.21	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	192	●	Status Better	2019-01-17 10:47:37	192.168.0.22	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	191	●	Status Better	2019-01-17 10:47:33	192.168.0.1	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	190	●	Status Better	2019-01-17 10:47:33	192.168.0.18	Protocol: ICMP	Connection status OK (ICMP is reachable)

After the NetMaster gets the topology, the port line will be established based on the real topology that has been discovered. And user just needs to arrange the position of the device.



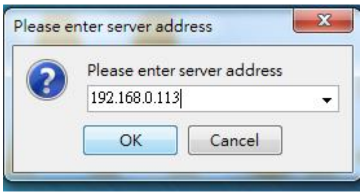
Device Model: WR322GR-WLAN+L
IP Address : 192.168.0.22
Description : Industrial Secure Cellula
System Up Time : 37 days, 4:17:22.00
System Name: WR322GR-WLAN+LT
System Contact:
System Location: Unknown
SNMP Supported: OK

Event Management | SNMP Trap Receiver | All Events | Filter | Ack. All

Ack	ID	Type	Category	Receive Time	Source	Component	Message
□	133	●	Status Better	2019-01-16 15:18:45	192.168.0.22	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	132	●	Status Better	2019-01-16 15:18:45	192.168.0.20	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	131	○	Application Info	2019-01-16 15:17:18	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5105
□	130	○	Application Info	2019-01-16 15:16:20	NetMaster Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5105
□	129	●	Status Better	2019-01-16 14:58:35	192.168.0.5	Protocol: ICMP	Connection status OK (ICMP is reachable)

NetMaster Viewer (Client)

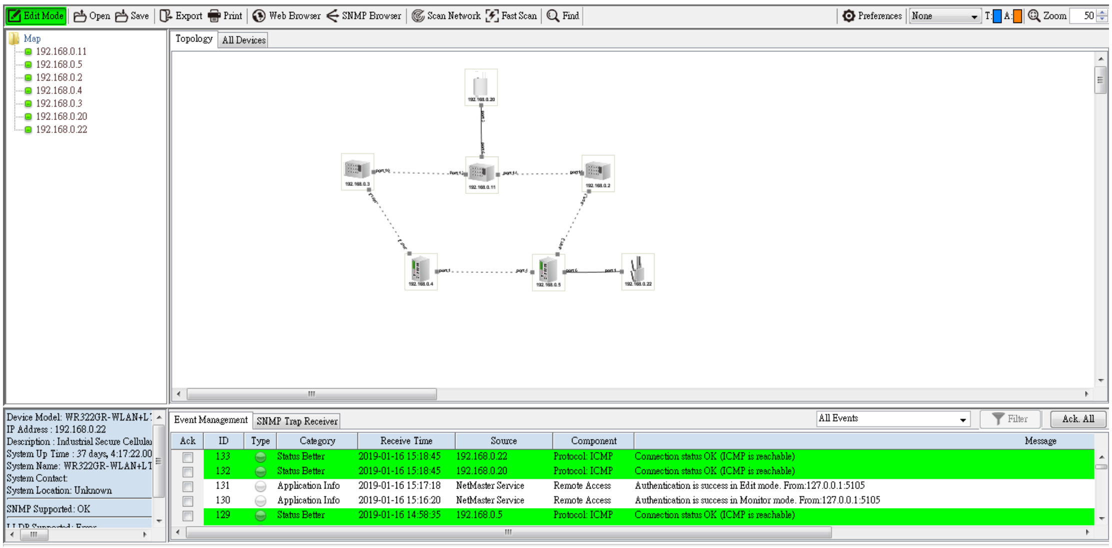
The NetMaster Viewer is the client mode, this software need to access the NetMaster server to get the current topology. When user clicks the icon, it will ask user to enter the server IP Address. And enter the password (Default password: admin).



Please enter server address

192.168.0.113

The similar interface as the NetMaster server will appear.

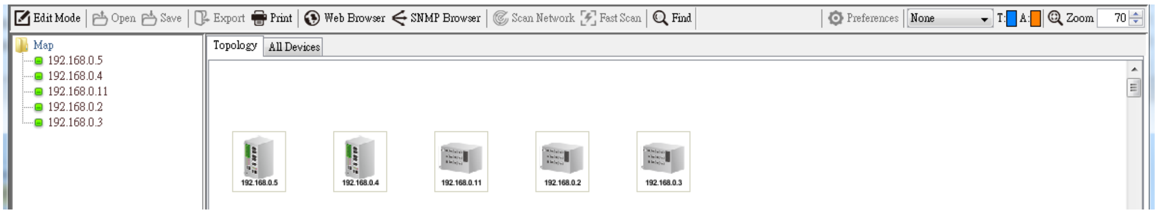


Device Model: WR322GR-WLAN+L
IP Address : 192.168.0.22
Description : Industrial Secure Cellula
System Up Time : 37 days, 4:17:22.00
System Name: WR322GR-WLAN+LT
System Contact:
System Location: Unknown
SNMP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	Message
□	133	●	Status Better	2019-01-16 15:18:45	192.168.0.22	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	132	●	Status Better	2019-01-16 15:18:45	192.168.0.20	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	131	○	Application Info	2019-01-16 15:17:18	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5105
□	130	○	Application Info	2019-01-16 15:16:20	NetMaster Service	Remote Access	Authentication is success in Monitor mode. From:127.0.0.1:5105
□	129	●	Status Better	2019-01-16 14:58:35	192.168.0.5	Protocol: ICMP	Connection status OK (ICMP is reachable)

For Edit Mode section, both server and client cannot be on the same mode or it is not for multiple users. If one user is in the Edit mode, the other user need to wait till the first user leave the Edit Mode section then he can enter the Edit Mode.

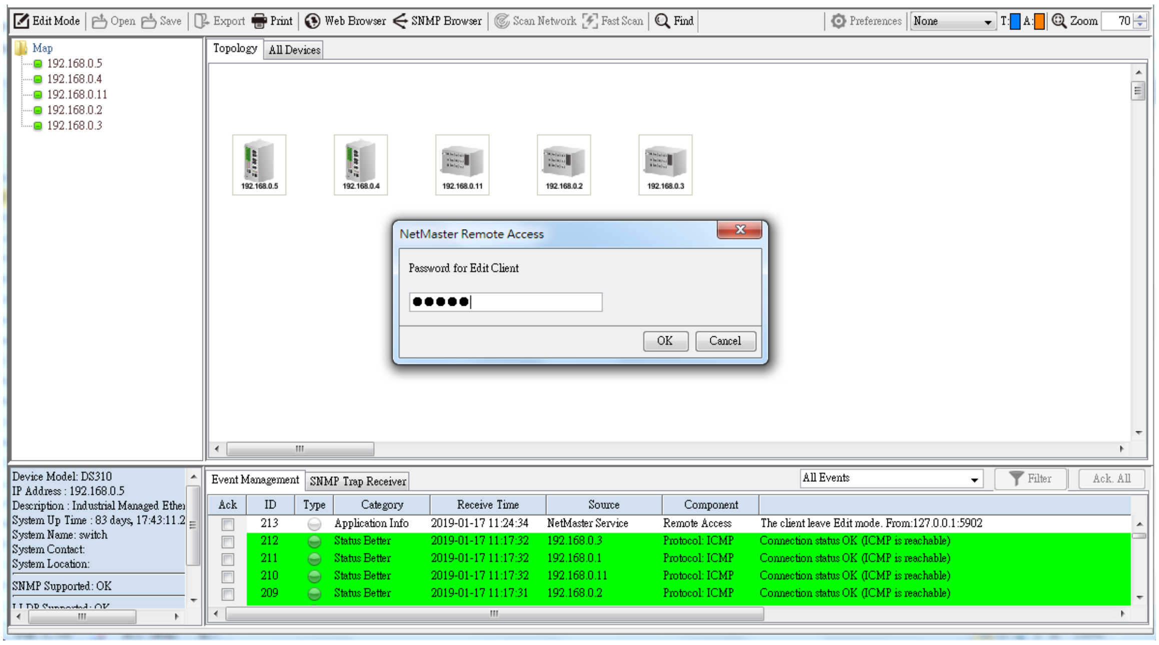
4. NETMASTER MAIN INTERFACE



4.1 EDIT MODE

At the top of the NetMaster dashboard, user will see several toolbar menus. Basically, not all of the toolbar menus are active on the Monitor Mode, until user enters the Edit Mode.

To enter the Edit Mode, click the Edit Mode button and an authentication password is required to get the permission.



NetMaster Remote Access

Password for Edit Client

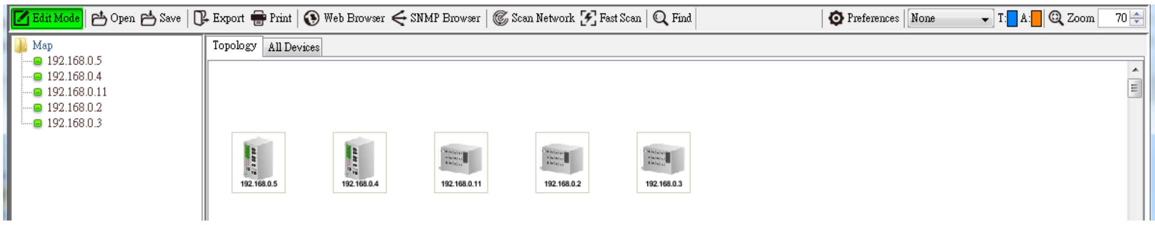
●●●●●

OK Cancel

Device Model: DS310
IP Address : 192.168.0.5
Description : Industrial Managed Ether
System Up Time : 83 days, 17:43:11.2
System Name: switch
System Contact:
System Location:
SNMP Supported: OK
LLDP Supported: OK

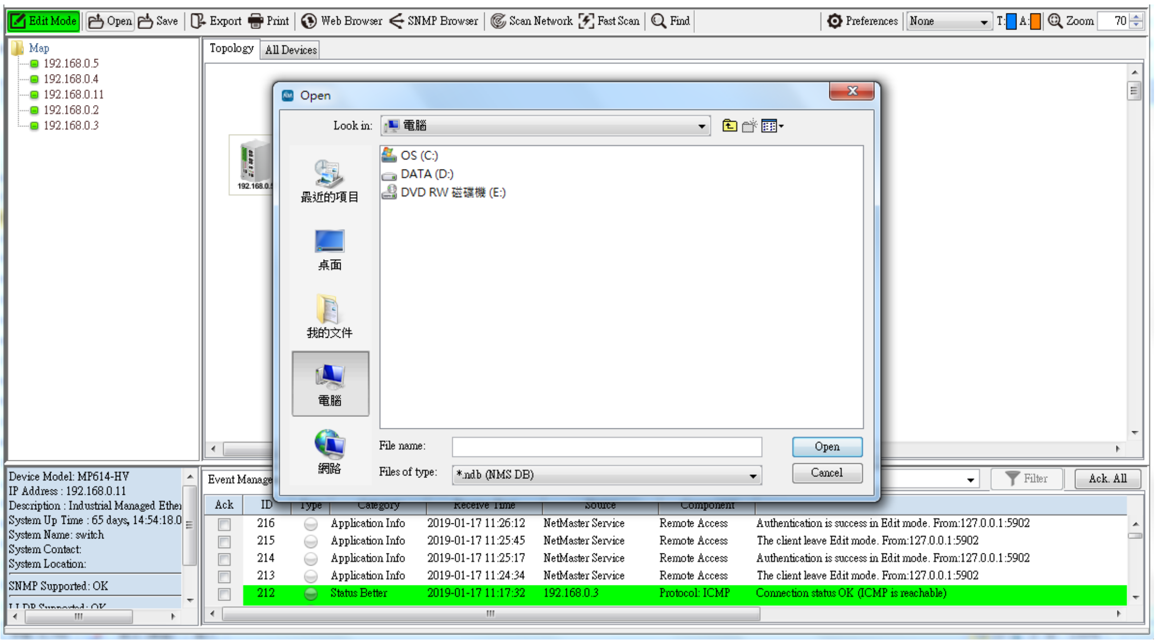
Ack	ID	Type	Category	Receive Time	Source	Component	
□	213	○	Application Info	2019-01-17 11:24:34	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	212	●	Status Better	2019-01-17 11:17:32	192.168.0.3	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	211	●	Status Better	2019-01-17 11:17:32	192.168.0.1	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	210	●	Status Better	2019-01-17 11:17:32	192.168.0.11	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	209	●	Status Better	2019-01-17 11:17:31	192.168.0.2	Protocol: ICMP	Connection status OK (ICMP is reachable)

After the authentication is success, then the Edit Mode button will turn directly to green color. And all of the toolbar menus are activated.



4.2 OPEN

Click Open to open the previous saved NetMaster database file. The default file type is *.ndb. The database will restore all of the configuration and also the topology.

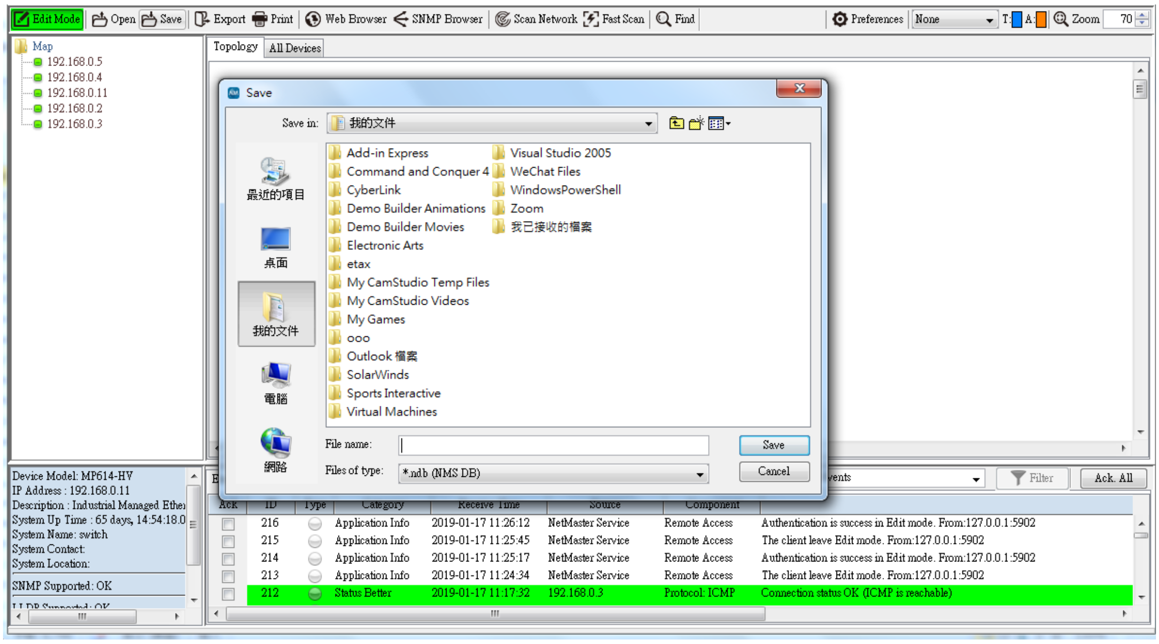


Device Model: MP614-HV
IP Address : 192.168.0.11
Description : Industrial Managed Ether
System Up Time : 65 days, 14:54:18.0
System Name: switch
System Contact:
System Location:
SNMP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	
□	216	○	Application Info	2019-01-17 11:26:12	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5902
□	215	○	Application Info	2019-01-17 11:25:45	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	214	○	Application Info	2019-01-17 11:25:17	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5902
□	213	○	Application Info	2019-01-17 11:24:34	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	212	○	Status Better	2019-01-17 11:17:32	192.168.0.3	Protocol: ICMP	Connection status OK (ICMP is reachable)

4.3 SAVE

Click Save to save the current database into file. The database file should be in "*.ndb" format.

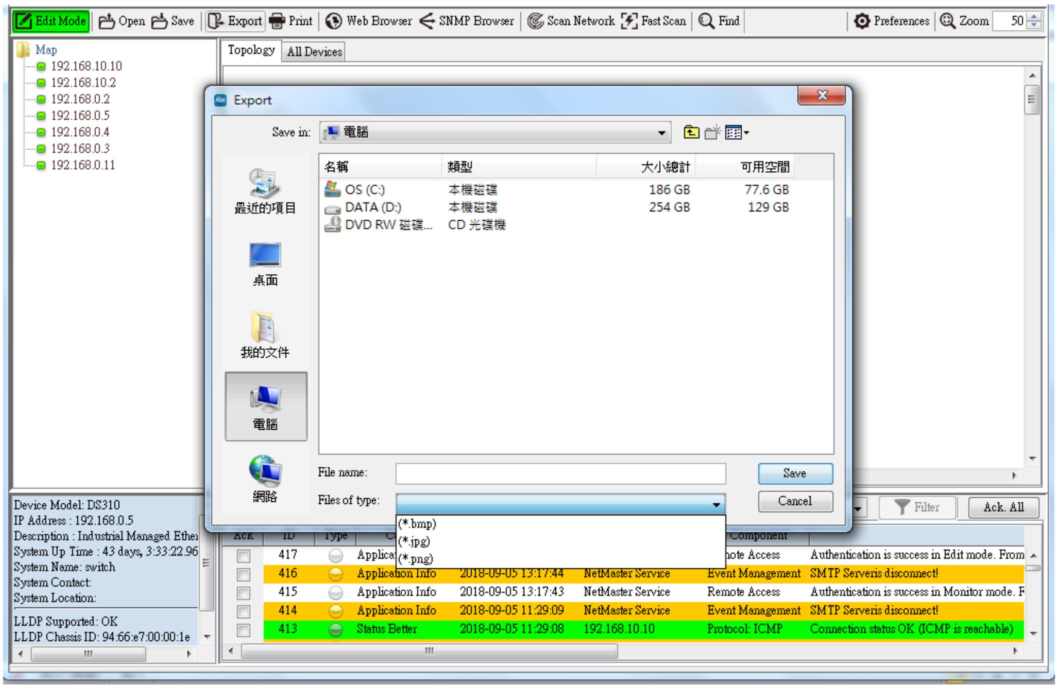


Device Model: MP614-HV
IP Address : 192.168.0.11
Description : Industrial Managed Ether
System Up Time : 65 days, 14:54:18.0
System Name: switch
System Contact:
System Location:
SNMP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	
□	216	○	Application Info	2019-01-17 11:26:12	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5902
□	215	○	Application Info	2019-01-17 11:25:45	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	214	○	Application Info	2019-01-17 11:25:17	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5902
□	213	○	Application Info	2019-01-17 11:24:34	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	212	○	Status Better	2019-01-17 11:17:32	192.168.0.3	Protocol: ICMP	Connection status OK (ICMP is reachable)

4.4 EXPORT

Click Export to export the displayed map in the Topology Map as Image files such BMP, JPG and PNG format.

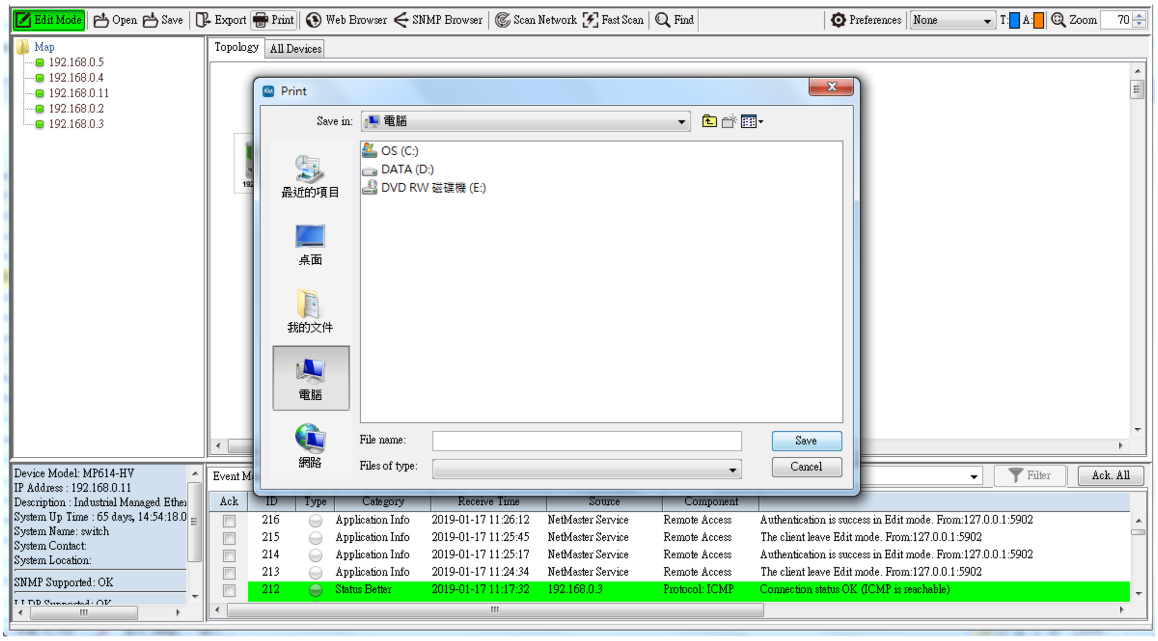


Device Model: DS310
IP Address : 192.168.0.5
Description : Industrial Managed Ether
System Up Time : 43 days, 3:33:22.96
System Name: switch
System Contact:
System Location:
LLDP Supported: OK
LLDP Chassis ID: 94:66:e7:00:00:1e

Ack	ID	Type	C			Component	
□	417	○	Applica			ote Access	Authentication is success in Edit mode. From
□	416	●	Application Info	2018-09-05 13:17:44	NetMaster Service	Event Management	SMTP Serveris disconnect!
□	415	○	Application Info	2018-09-05 13:17:43	NetMaster Service	Remote Access	Authentication is success in Monitor mode. F
□	414	●	Application Info	2018-09-05 11:29:09	NetMaster Service	Event Management	SMTP Serveris disconnect!
□	413	●	Status Better	2018-09-05 11:29:08	192.168.10.10	Protocol: ICMP	Connection status OK (ICMP is reachable)

4.5 PRINT

Click Print to export the displayed map in the Topology Map as PDF file.

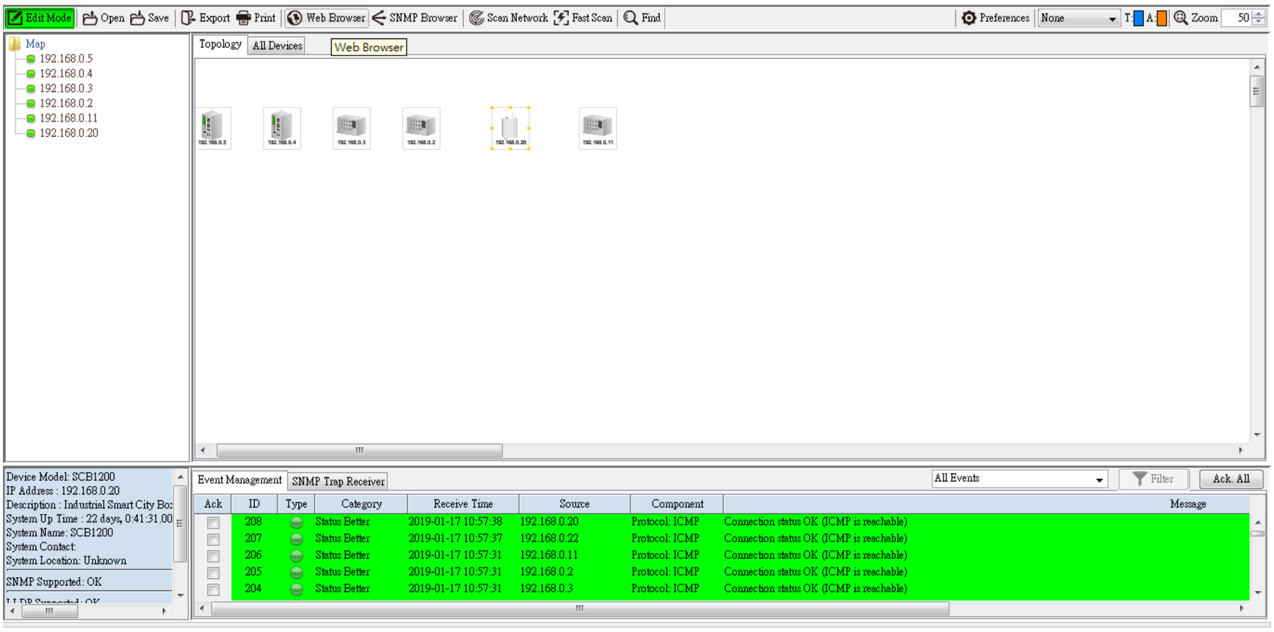


Device Model: MP614-HV
IP Address : 192.168.0.11
Description : Industrial Managed Ether
System Up Time : 65 days, 14:54:18.0
System Name: switch
System Contact:
System Location:
SNMP Supported: OK
LLDP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	
□	216	○	Application Info	2019-01-17 11:26:12	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5902
□	215	○	Application Info	2019-01-17 11:25:45	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	214	○	Application Info	2019-01-17 11:25:17	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5902
□	213	○	Application Info	2019-01-17 11:24:34	NetMaster Service	Remote Access	The client leave Edit mode. From:127.0.0.1:5902
□	212	●	Status Better	2019-01-17 11:17:32	192.168.0.3	Protocol: ICMP	Connection status OK (ICMP is reachable)

4.6 WEB BROWSER

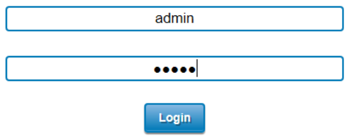
Choose the monitored device on the topology tab then click Web Browser button and it will directly open the Web Management page of the device.



Device Model: SCB1200
IP Address : 192.168.0.20
Description : Industrial Smart City Bo:
System Up Time : 22 days, 0:41:31.00
System Name: SCB1200
System Contact:
System Location: Unknown
SNMP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	Message
□	208	●	Status Better	2019-01-17 10:57:38	192.168.0.20	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	207	●	Status Better	2019-01-17 10:57:37	192.168.0.22	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	206	●	Status Better	2019-01-17 10:57:31	192.168.0.11	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	205	●	Status Better	2019-01-17 10:57:31	192.168.0.2	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	204	●	Status Better	2019-01-17 10:57:31	192.168.0.3	Protocol: ICMP	Connection status OK (ICMP is reachable)

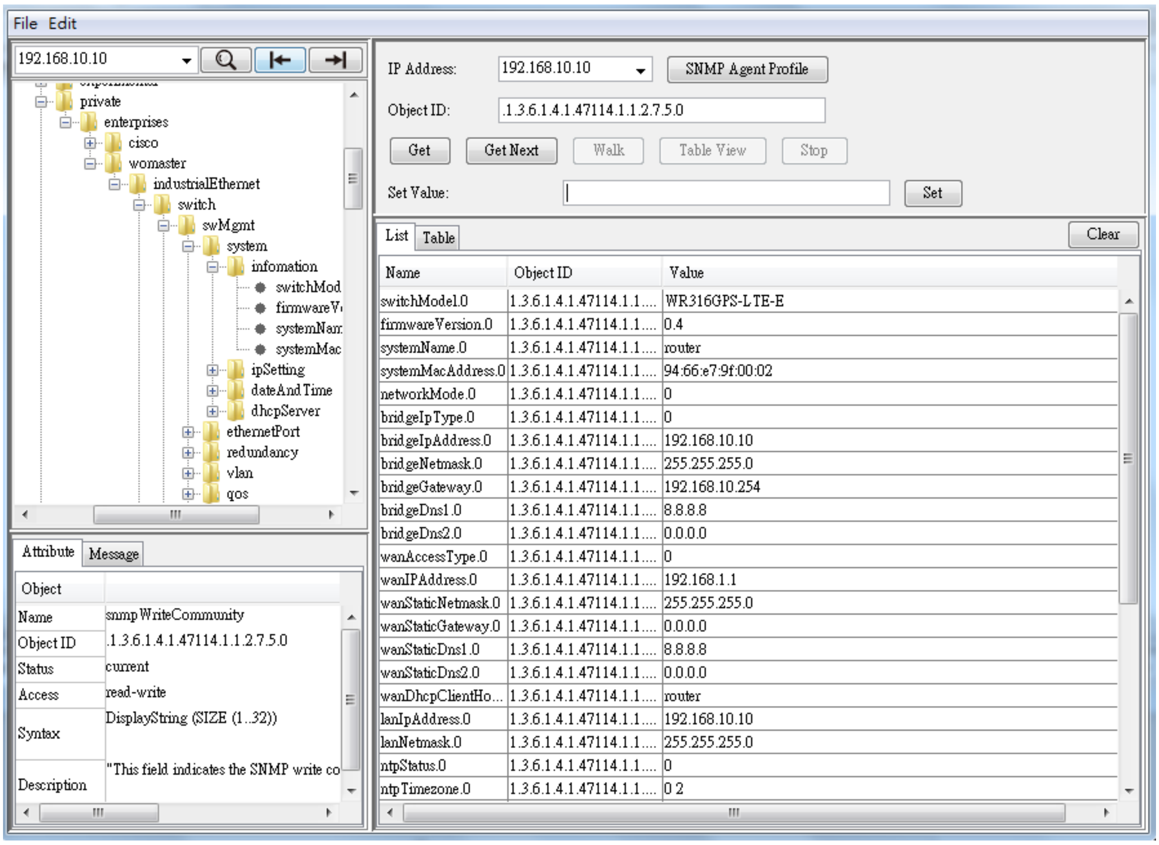
The default web browser would be **Internet Explorer**.


admin

•••••

4.7 SNMP BROWSER

The SNMP Browser tool lets user to read and write the MIB of the selected device. On the SNMP Browser configuration page, user can change the IP Address to get the MIB file from other device.



Object	
Name	snmpWriteCommunity
Object ID	.1.3.6.1.4.1.47114.1.1.2.7.5.0
Status	current
Access	read-write
Syntax	DisplayString (SIZE (1..32))
Description	"This field indicates the SNMP write co

IP Address: 192.168.10.10

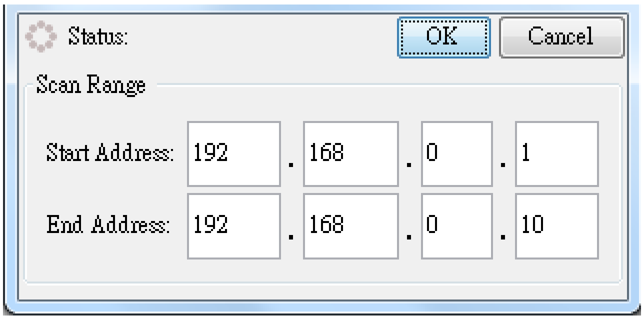
Object ID: .1.3.6.1.4.1.47114.1.1.2.7.5.0

Set Value:

Name	Object ID	Value
switchModel.0	1.3.6.1.4.1.47114.1.1....	WR316GPS-LTE-E
firmwareVersion.0	1.3.6.1.4.1.47114.1.1....	0.4
systemName.0	1.3.6.1.4.1.47114.1.1....	router
systemMacAddress.0	1.3.6.1.4.1.47114.1.1....	94:66:e7:9f:00:02
networkMode.0	1.3.6.1.4.1.47114.1.1....	0
bridgeIpType.0	1.3.6.1.4.1.47114.1.1....	0
bridgeIpAddress.0	1.3.6.1.4.1.47114.1.1....	192.168.10.10
bridgeNetmask.0	1.3.6.1.4.1.47114.1.1....	255.255.255.0
bridgeGateway.0	1.3.6.1.4.1.47114.1.1....	192.168.10.254
bridgeDns1.0	1.3.6.1.4.1.47114.1.1....	8.8.8.8
bridgeDns2.0	1.3.6.1.4.1.47114.1.1....	0.0.0.0
wanAccessType.0	1.3.6.1.4.1.47114.1.1....	0
wanIPAddress.0	1.3.6.1.4.1.47114.1.1....	192.168.1.1
wanStaticNetmask.0	1.3.6.1.4.1.47114.1.1....	255.255.255.0
wanStaticGateway.0	1.3.6.1.4.1.47114.1.1....	0.0.0.0
wanStaticDns1.0	1.3.6.1.4.1.47114.1.1....	8.8.8.8
wanStaticDns2.0	1.3.6.1.4.1.47114.1.1....	0.0.0.0
wanDhcpClientHo...	1.3.6.1.4.1.47114.1.1....	router
lanIpAddress.0	1.3.6.1.4.1.47114.1.1....	192.168.10.10
lanNetmask.0	1.3.6.1.4.1.47114.1.1....	255.255.255.0
ntpStatus.0	1.3.6.1.4.1.47114.1.1....	0
ntpTimezone.0	1.3.6.1.4.1.47114.1.1....	0 2

4.8 SCAN NETWORK

Find out specified IP range assigned.

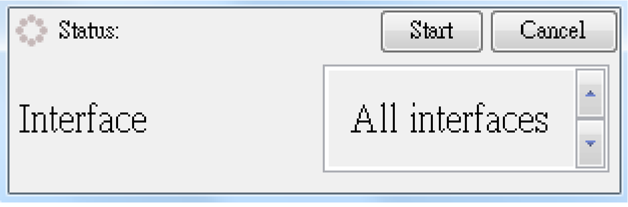


Start Address: 192 . 168 . 0 . 1

End Address: 192 . 168 . 0 . 10

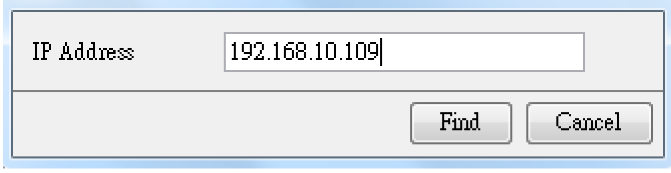
4.9 FAST SCAN

Find out all switch devices by the interface.



4.10 FIND

Find the device by entering the specific IP Address.


IP Address 192.168.10.109

4.11 PREFERENCES

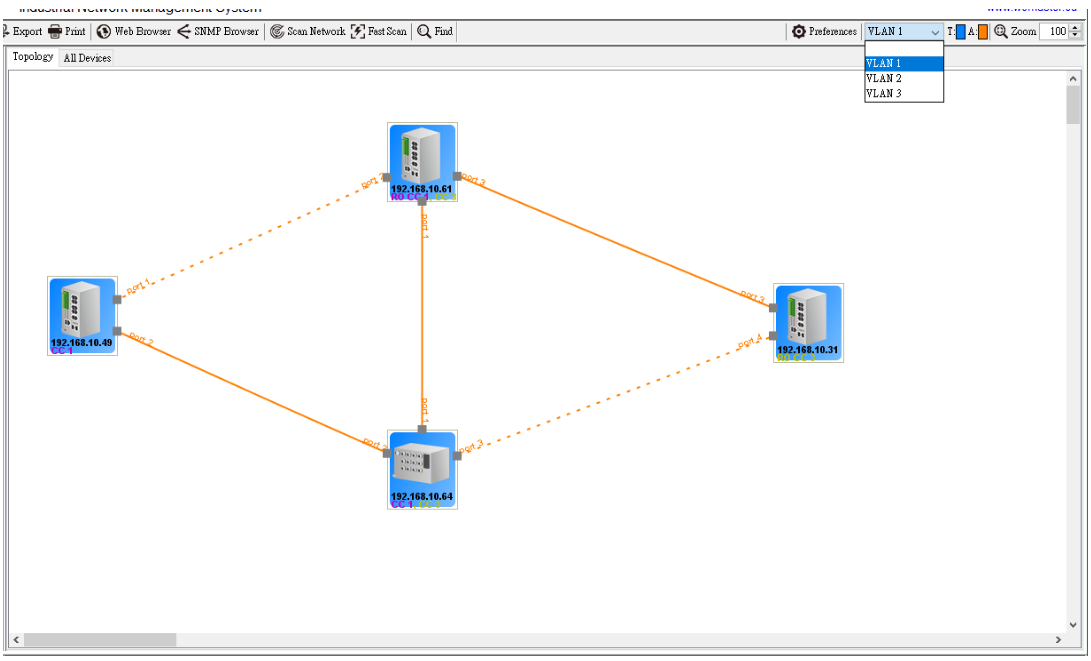
Please refer to Chapter 10 for more information.

4.12 VLAN

If user added any VLAN to the network, by using this feature user can check which device belongs to which VLAN. And user can check the port type as well (Blue: Trunk port and Orange: Access port).

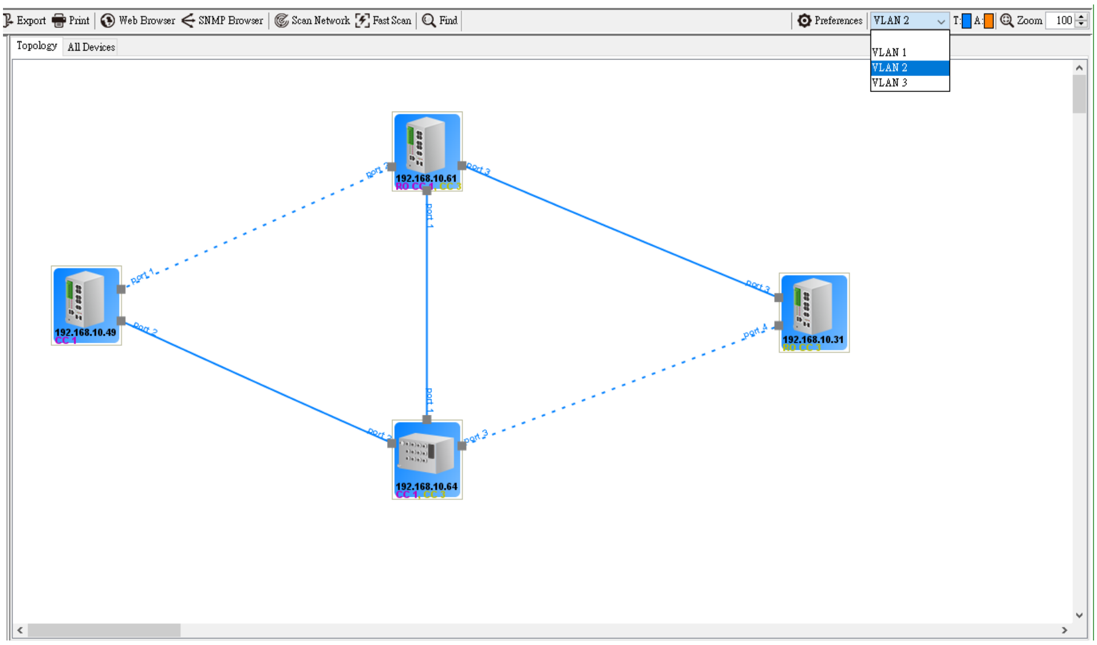
Access Port

The picture below shows if all of the devices are in VLAN1 and the port is Access Port.



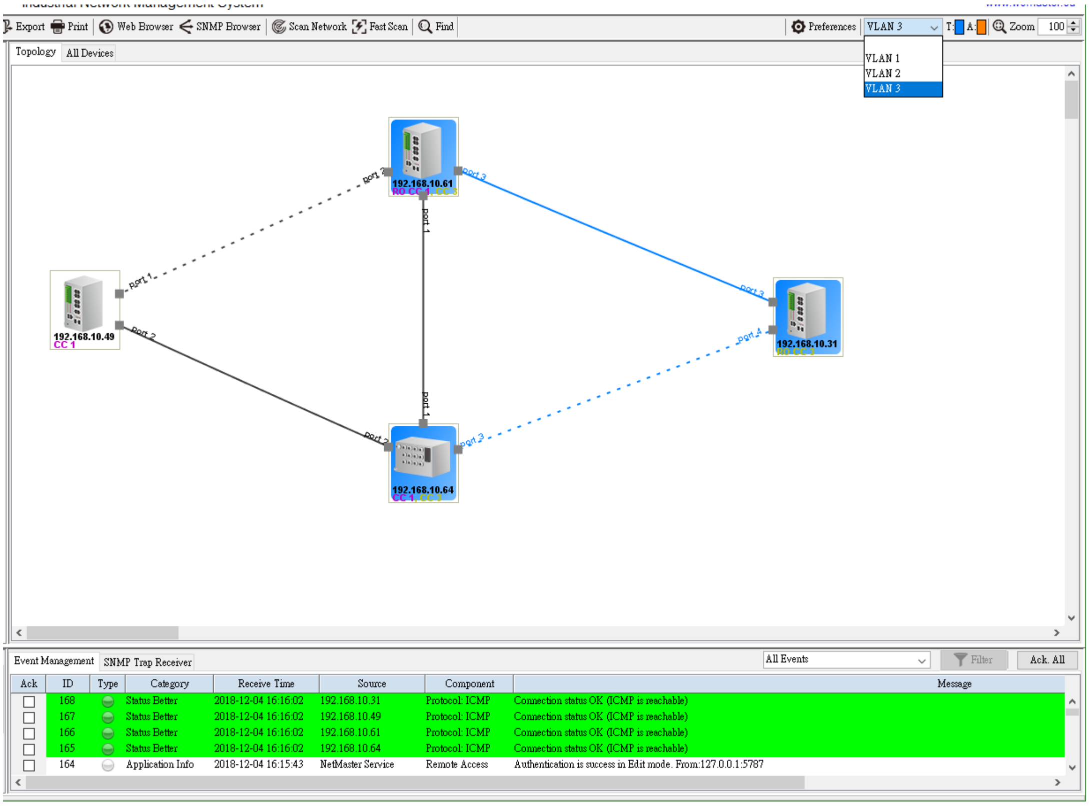
Trunk Port

The picture below shows if all of the devices are in VLAN2 and the port is Trunk Port.



Mix Port

The picture below shows if all of the devices on the right side are in VLAN3 and the port is Trunk Port, then three devices on the left side are not assigned to any VLAN..



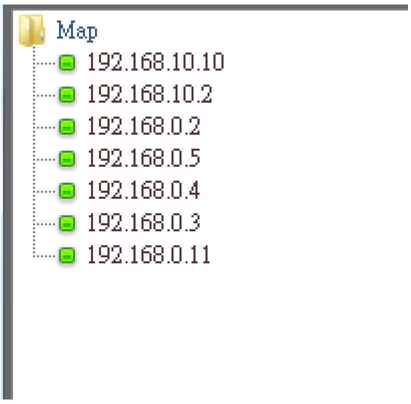
Ack	ID	Type	Category	Receive Time	Source	Component	Message
□	168	●	Status Better	2018-12-04 16:16:02	192.168.10.31	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	167	●	Status Better	2018-12-04 16:16:02	192.168.10.49	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	166	●	Status Better	2018-12-04 16:16:02	192.168.10.61	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	165	●	Status Better	2018-12-04 16:16:02	192.168.10.64	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	164	○	Application Info	2018-12-04 16:15:43	NetMaster Service	Remote Access	Authentication is success in Edit mode. From:127.0.0.1:5787

4.13 ZOOM

Zoom in and out the device icons, texts and others only on the **Topology** tab.

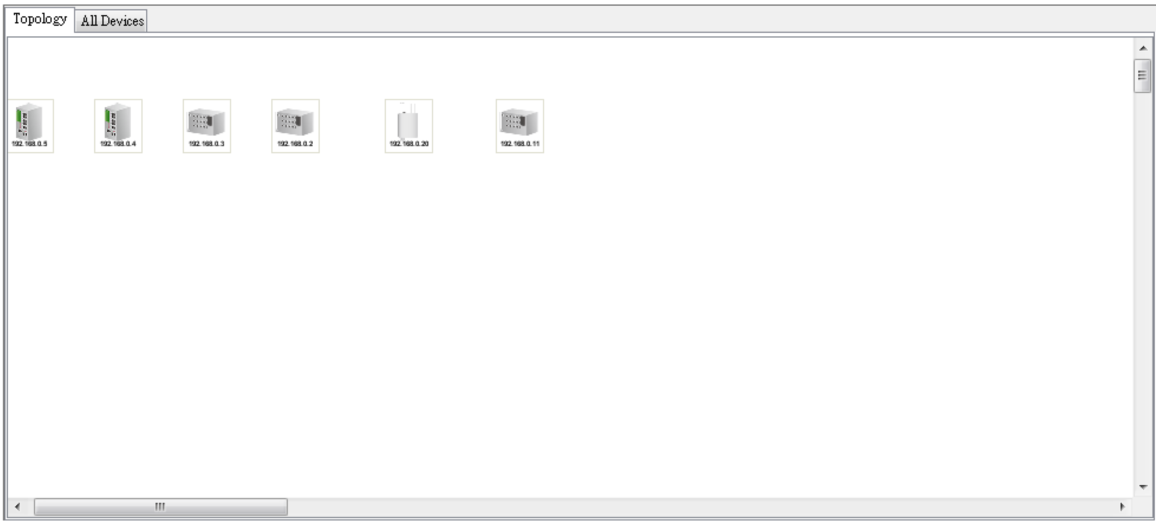
4.14 MAP TREE

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



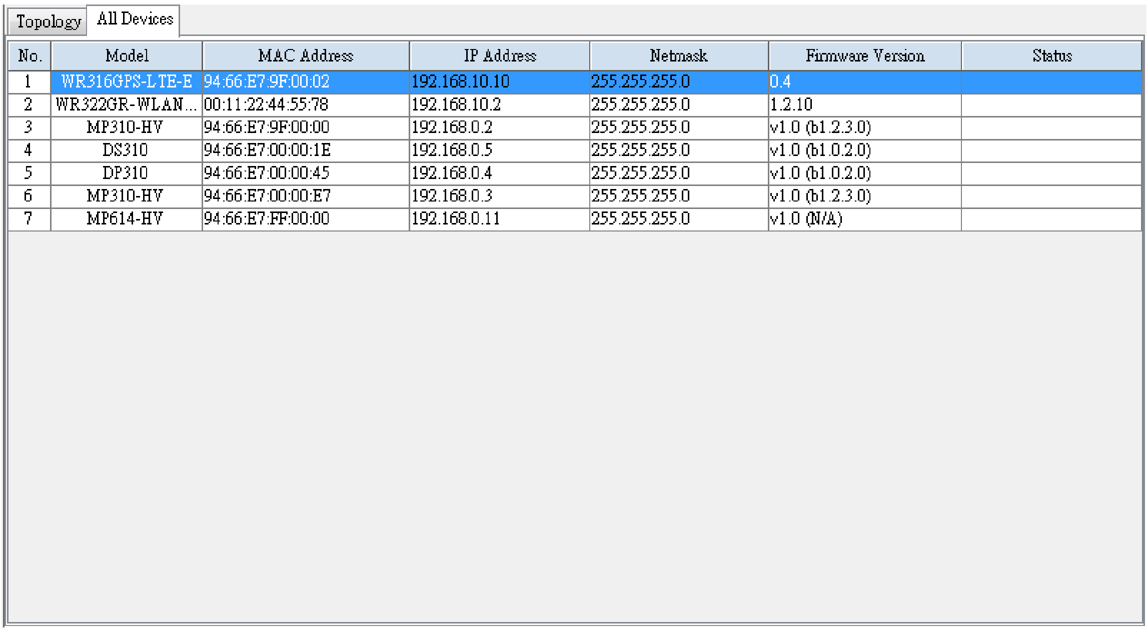
4.15 TOPOLOGY TAB

This page displays the icons from monitored devices.



4.16 ALL DEVICES TAB

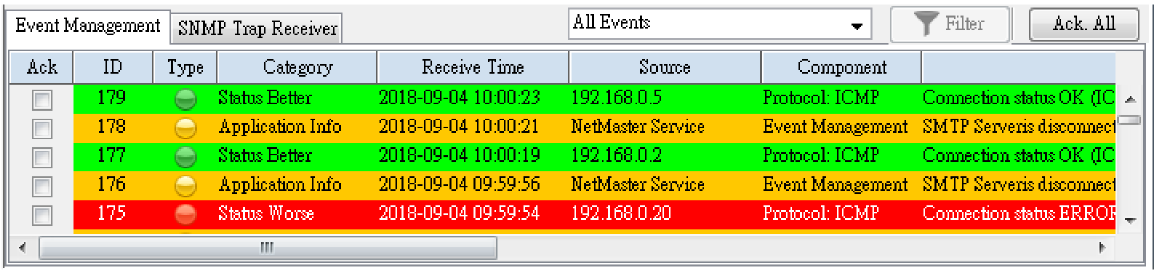
This page displays the list of monitored devices at the **Topology** tab. In this tab, user can do some configuration action by do the right click on the selected device from the list and a sub menu will appear.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR316GPS-LTE-E	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.4	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.2	255.255.255.0	1.2.10	
3	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
4	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
5	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0	v1.0 (b1.2.3.0)	
7	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	

4.17 EVENT MANAGEMENT TAB

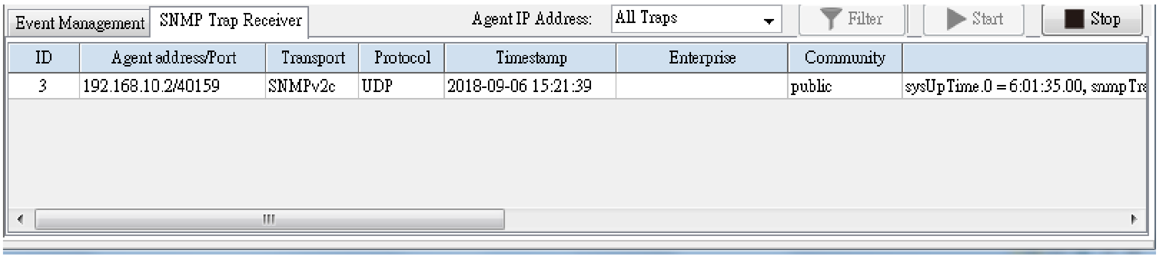
The event displays on the **Event Management** tab page while the real time event happens.



Ack	ID	Type	Category	Receive Time	Source	Component	
□	179	●	Status Better	2018-09-04 10:00:23	192.168.0.5	Protocol: ICMP	Connection status OK (IC
□	178	●	Application Info	2018-09-04 10:00:21	NetMaster Service	Event Management	SMTP Serveris disconnect
□	177	●	Status Better	2018-09-04 10:00:19	192.168.0.2	Protocol: ICMP	Connection status OK (IC
□	176	●	Application Info	2018-09-04 09:59:56	NetMaster Service	Event Management	SMTP Serveris disconnect
□	175	●	Status Worse	2018-09-04 09:59:54	192.168.0.20	Protocol: ICMP	Connection status ERROR

4.18 SNMP TRAP RECEIVER TAB

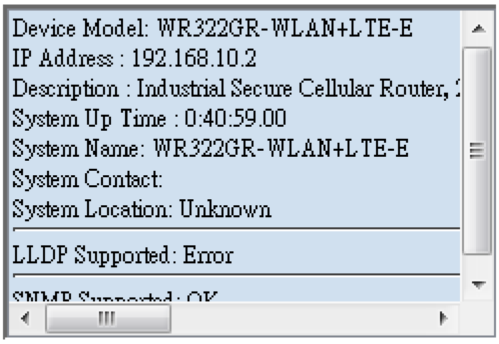
The SNMP Trap Receiver listens for SNMP traps generated by network devices. When an event occurs, the trap details are logged along with the time, IP address, hostname, and trap type and can be used for analysis and correlation. User can enter the specific IP Address for the SNMP Trap and click Filter to get SNMP Trap information from specific device or choose All Traps to get all of the SNMP Traps. Click Start to enable the function.



ID	Agent address/Port	Transport	Protocol	Timestamp	Enterprise	Community	
3	192.168.10.2/40159	SNMPv2c	UDP	2018-09-06 15:21:39		public	sysUpTime.0 = 6:01:35.00, snmpTr

4.19 DEVICE INFORMATION

At the bottom left of the NetMaster interface, it has the device information click the different device to see its information.



Device Model: WR322GR-WLAN+LTE-E
IP Address : 192.168.10.2
Description : Industrial Secure Cellular Router,
System Up Time : 0:40:59.00
System Name: WR322GR-WLAN+LTE-E
System Contact:
System Location: Unknown

LLDP Supported: Error

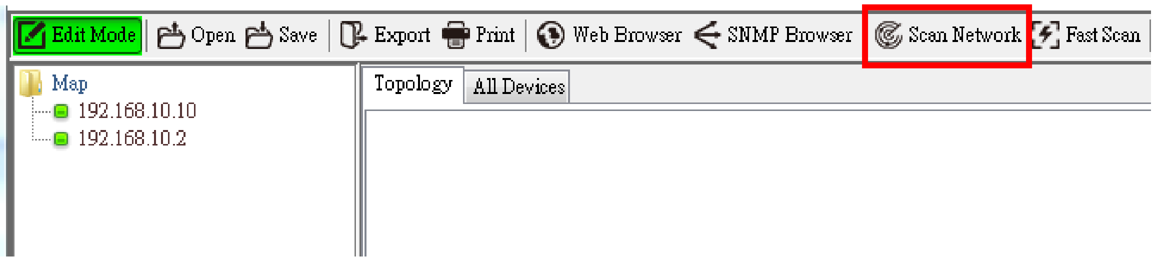
SNMP Supported : OK

5. DEVICE DISCOVERY

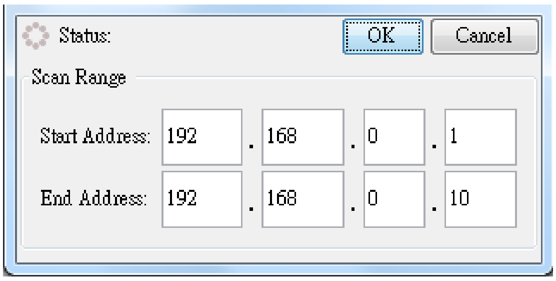
To see the installed devices on the **Topology** tab or the **All Devices** tab, user must discover all of the devices. How to add the device and delete device?

5.1 ADD DEVICES

5.1.1 SCAN NETWORK



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



Scan Range

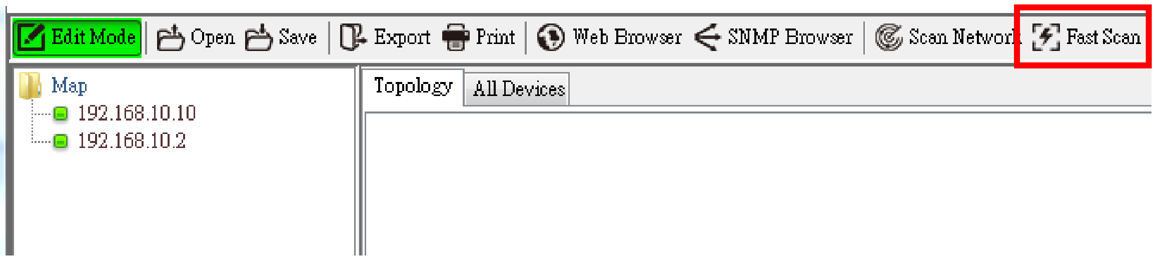
Start Address: 192 . 168 . 0 . 1

End Address: 192 . 168 . 0 . 10

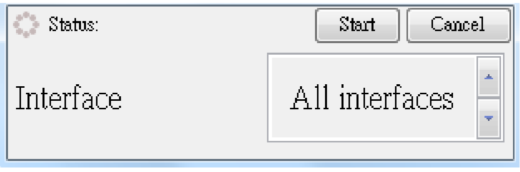
***The End Address should great or equal then Start Address.**

5.1.2 FAST SCAN

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

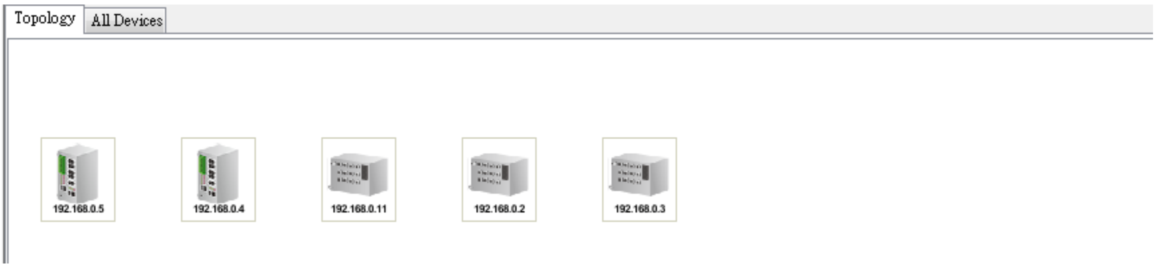


This function is to discovery devices using the **NetMaster** protocol in the local network. It discovers all network devices on the subnet network via the selected interface on the PC.



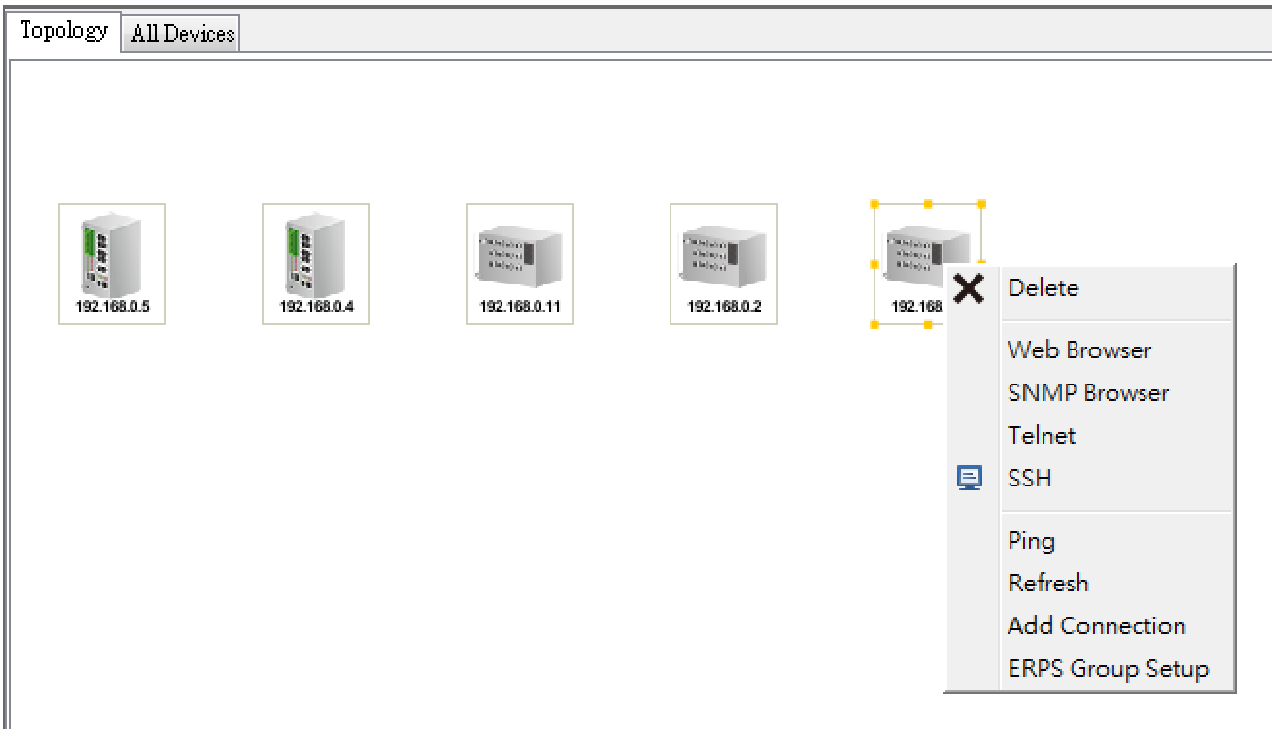
Interface: All interfaces

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



5.2 DELETE DEVICES

User 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. Remember to enter the Edit Mode to execute this function.



6. TOPOLOGY TAB

Following topics are covered in this section:

6.1 Device Information

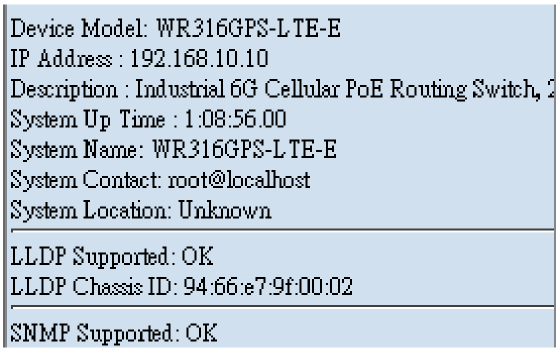
6.2 Auto Topology

6.3 Add and Delete Connection

6.1 DEVICE INFORMATION

6.1.1 DEVICE STATUS

The device status is located on the bottom left side of the NetMaster main interface. User can move the mouse cursor over the monitored device icon on **Topology** tab. It will show the status for the device.

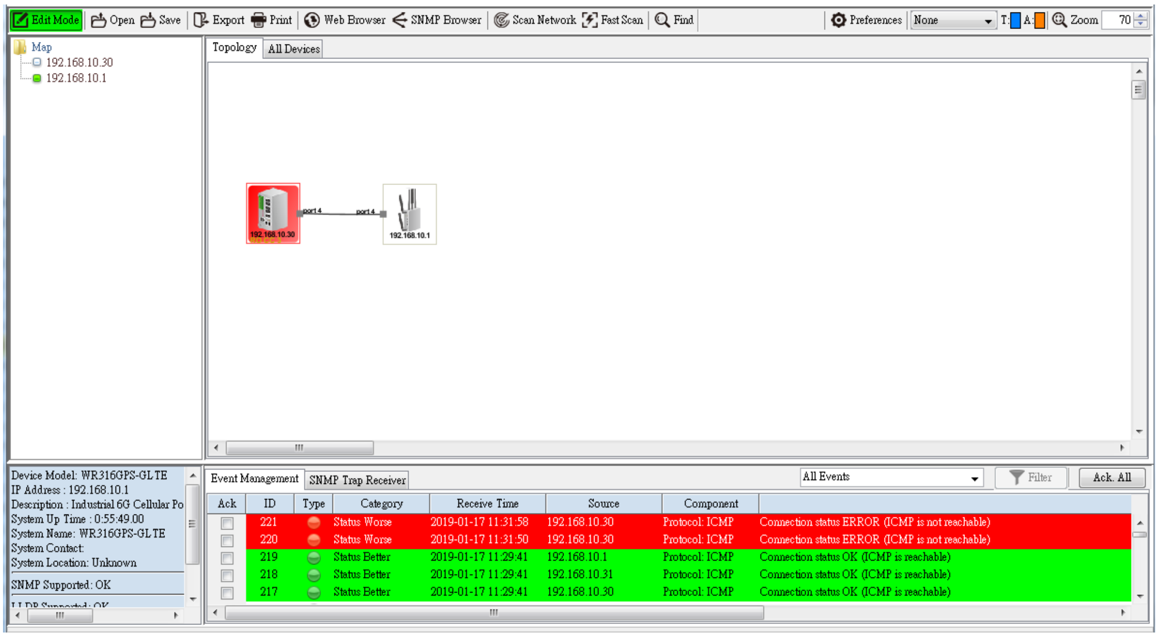


Device Model: WR316GPS-LTE-E
IP Address : 192.168.10.10
Description : Industrial 6G Cellular PoE Routing Switch, 2
System Up Time : 1:08:56.00
System Name: WR316GPS-LTE-E
System Contact: root@localhost
System Location: Unknown

LLDP Supported: OK
LLDP Chassis ID: 94:66:e7:9f:00:02

SNMP Supported: OK

The device lists in map 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 the device status. If the color is red, which indicates an error status (The detail error information is appeared in the Event management tab). In other words, NetMaster sends ICMP Ping request and then receives incorrect response (unreachable).



Device Model: WR316GPS-GLTE
IP Address : 192.168.10.1
Description : Industrial 6G Cellular Po
System Up Time : 0:55:49.00
System Name: WR316GPS-GLTE
System Contact:
System Location: Unknown

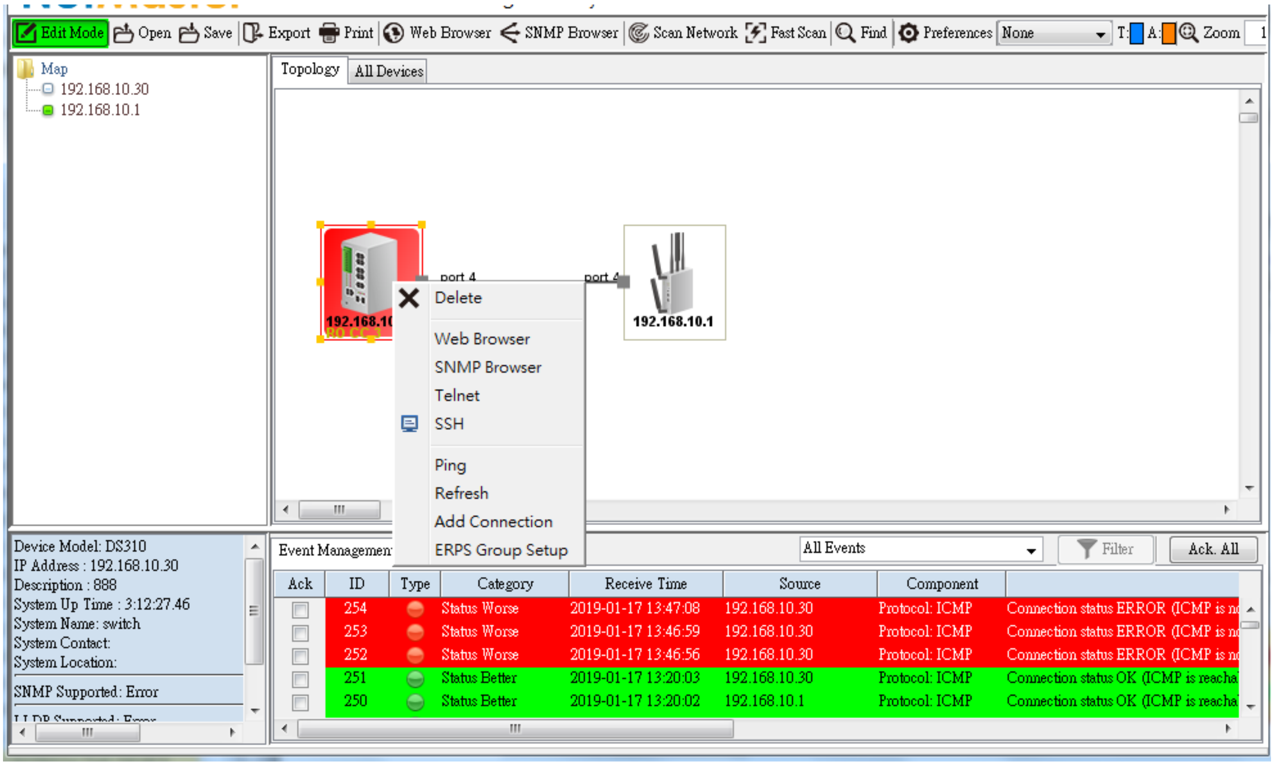
SNMP Supported: OK

LLDP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	
□	221	🟥	Status Worse	2019-01-17 11:31:58	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is not reachable)
□	220	🟥	Status Worse	2019-01-17 11:31:50	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is not reachable)
□	219	🟩	Status Better	2019-01-17 11:29:41	192.168.10.1	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	218	🟩	Status Better	2019-01-17 11:29:41	192.168.10.31	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	217	🟩	Status Better	2019-01-17 11:29:41	192.168.10.30	Protocol: ICMP	Connection status OK (ICMP is reachable)

6.1.2 REFRESH THE DEVICE

To update or refresh the device status, select a device especially on error status and right-click on the selected device. Then pop up a menu as follows:



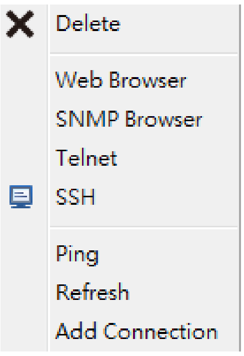
Device Model: DS310
IP Address : 192.168.10.30
Description : 888
System Up Time : 3:12:27.46
System Name: switch
System Contact:
System Location:

SNMP Supported: Error

Ack	ID	Type	Category	Receive Time	Source	Component	
□	254	🔴	Status Worse	2019-01-17 13:47:08	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is nc
□	253	🔴	Status Worse	2019-01-17 13:46:59	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is nc
□	252	🔴	Status Worse	2019-01-17 13:46:56	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is nc
□	251	🟢	Status Better	2019-01-17 13:20:03	192.168.10.30	Protocol: ICMP	Connection status OK (ICMP is reacha
□	250	🟢	Status Better	2019-01-17 13:20:02	192.168.10.1	Protocol: ICMP	Connection status OK (ICMP is reacha

6.1.3 DEVICE MANAGEMENT

If user wants to manage the device, select one device and right-click on the selected device. It will pop up a menu as follows. Choose to use Web Browser, SNMP Browser, Telnet, SSH, or Ping to manage the device. Also refer to section 7.4 for more details.



6.2 AUTO TOPOLOGY

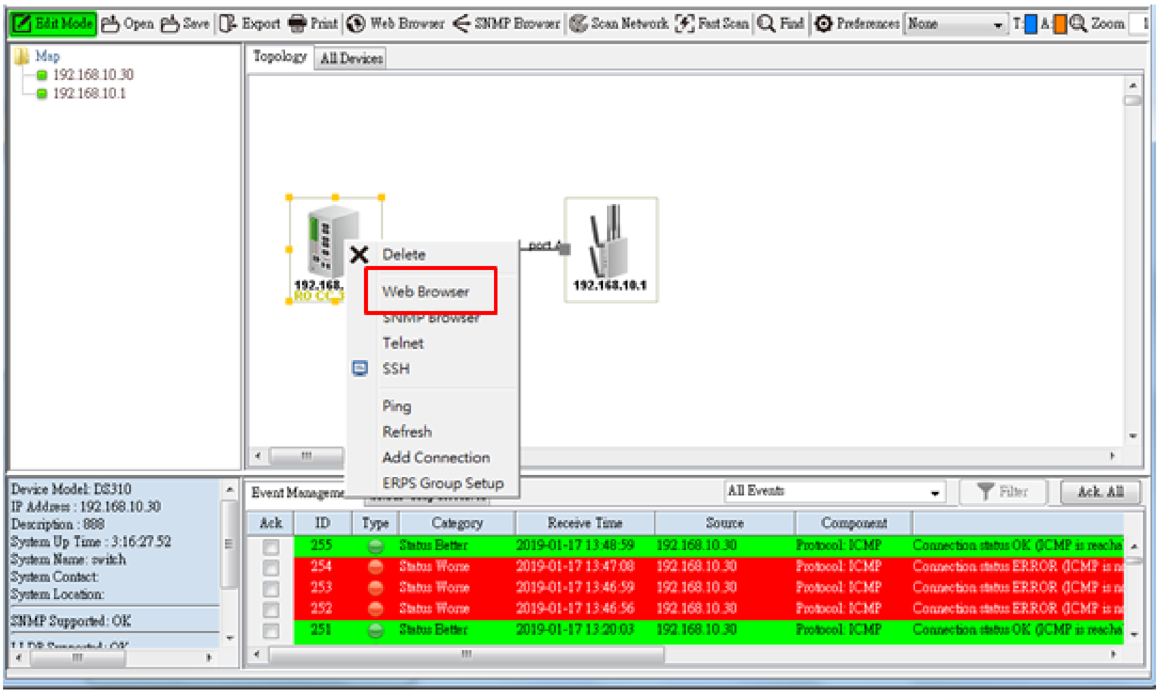
The Auto Topology function allows user to automatically create the connections between the devices (nodes). To support this function, the devices must support with LLDP and SNMP. LLDP enables the user to have automatic topology recognition for his LAN. Therefore the devices support for LLDP and SNMP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

6.2.1 ENABLE LLDP

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

1. Use mouse to select one device on the Topology tab which user wants to enable as LLDP.

2. Mouse right-click on the selected device and click on the **Web Browser** menu-item of pop-up menu.



Device Model: DS310
IP Address : 192.168.10.30
Description : 888
System Up Time : 3:16:27.52
System Name: switch
System Contact:
System Location:
SNMP Supported: OK

Ack	ID	Type	Category	Receive Time	Source	Component	
□	255	●	Status Better	2019-01-17 13:48:59	192.168.10.30	Protocol: ICMP	Connection status OK (ICMP is reacha
□	254	●	Status Worse	2019-01-17 13:47:08	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is n
□	253	●	Status Worse	2019-01-17 13:46:59	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is n
□	252	●	Status Worse	2019-01-17 13:46:56	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is n
□	251	●	Status Better	2019-01-17 13:20:03	192.168.10.30	Protocol: ICMP	Connection status OK (ICMP is reacha

3. When the login page appears, login with the user name and password.

4. Go to **Diagnostics -> LLDP**.

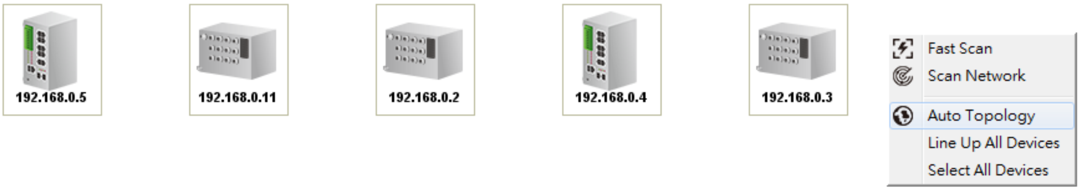
5. Confirm whether LLDP is enabled. If it is Disable, please set Enable and press **Submit**.

6.2.2 GENERATE CONNECTIONS

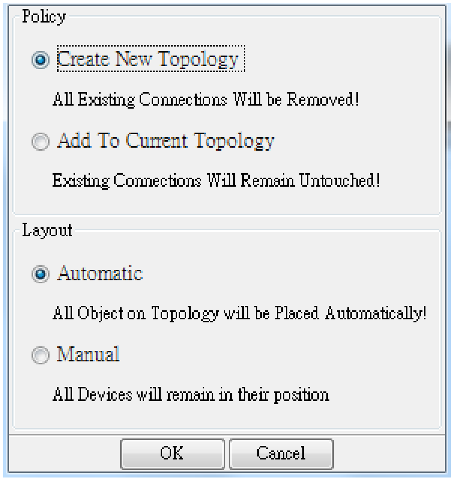
Generate connections between the devices

1. Check if every device has a green LED at the map tree and check the topology tab if S symbol also appear in every device. The device icon with S symbol means the device is supported with the SNMP. If the device doesn't have any S symbol on it then user needs to add the connection manually.

2. Mouse right-click on the Topology tab and click on Auto Topology on pop-up menu. It will display as follows:



3. Click OK to display the following of screen.



Policy

● Create New Topology

All Existing Connections Will be Removed!

○ Add To Current Topology

Existing Connections Will Remain Untouched!

Layout

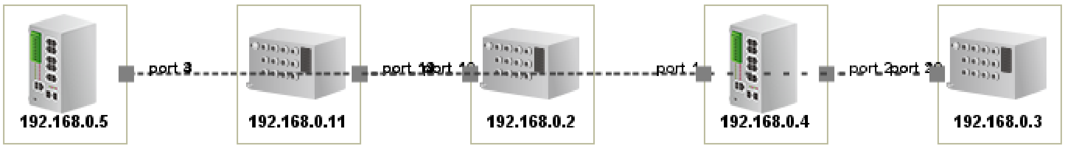
● Automatic

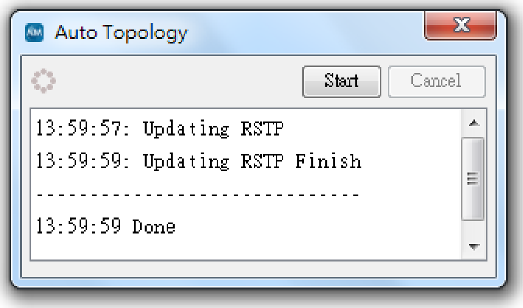
All Object on Topology will be Placed Automatically!

○ Manual

All Devices will remain in their position

Click Start to update the RSTP. After the RSTP has been updated then a line up devices with its connection will appear.





```
13:59:57: Updating RSTP
13:59:59: Updating RSTP Finish
------------------------------
13:59:59 Done
```

User can do the check list to make sure the Auto topology function works well.

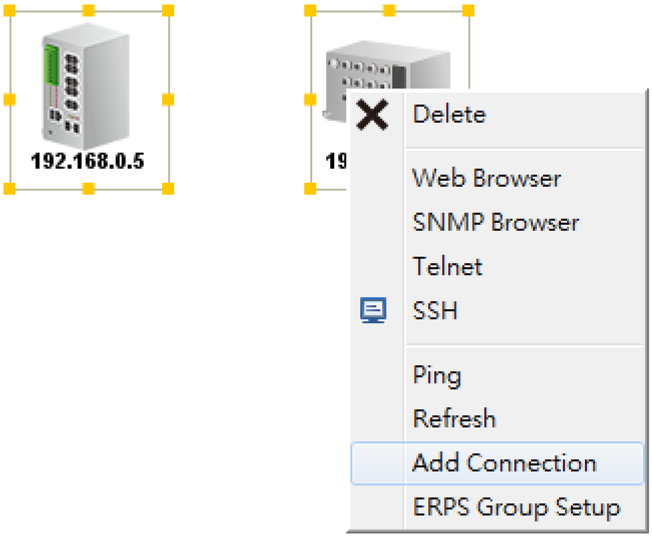
Yes/No	Requirement
	Does every device enable SNMP?
	Does any device not using default SNMP community? (public, private)
	Does every device LED on the Map Tree shows green color?
	Does every device enable LLDP?
	After user fixes the problem, did user refresh the device? (The Icon shows red color)

Note: The Third Party devices may not be displayed in the correctly icon in the NetMaster.

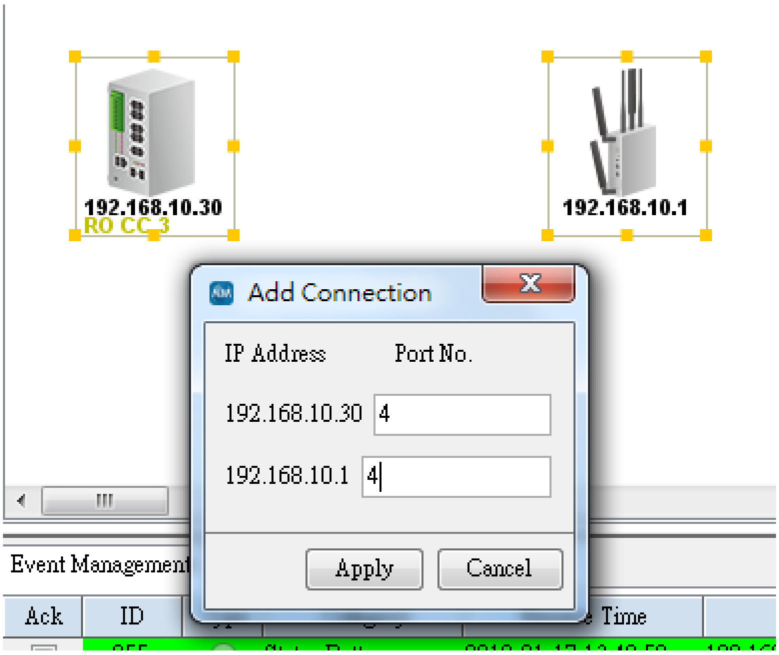
6.3 ADD AND DELETE CONNECTION

6.3.1 MANUAL ADD CONNECTION

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



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.

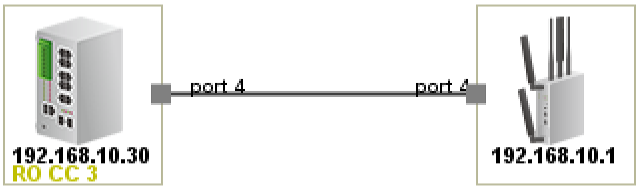


IP Address Port No.

192.168.10.30 4

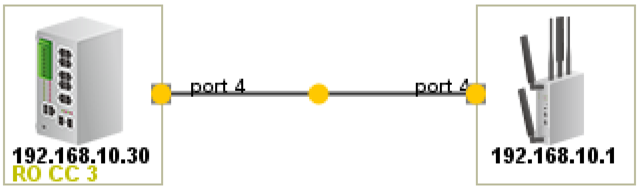
192.168.10.1 4

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

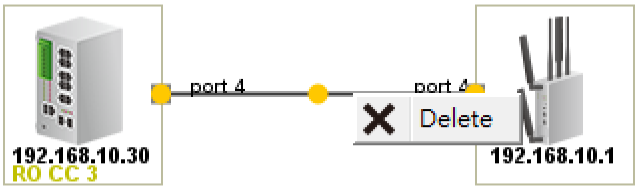


6.3.2 MANUAL DELETE CONNECTION

Select the connection between 192.168.10.10 and 192.168.10.2 by Mouse-Click.



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



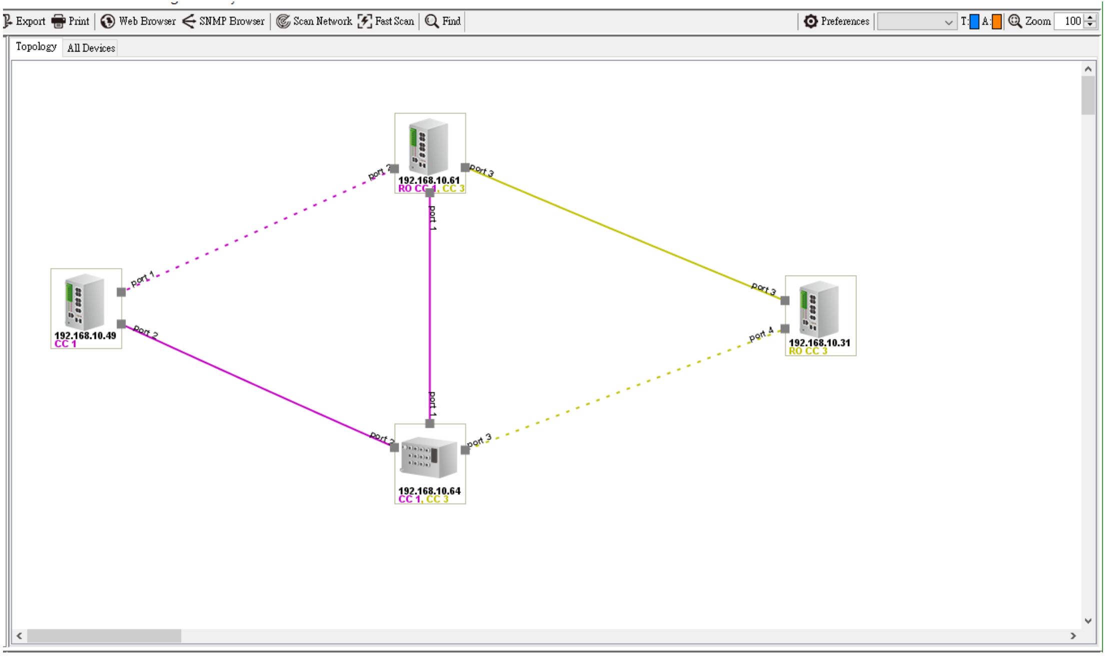
Click **Delete** to delete the connection.

192.168.10.30
RO CC 3
192.168.10.1

6.4 ERPS GROUP SETUP

6.4.1 ERPS VISUALIZATION

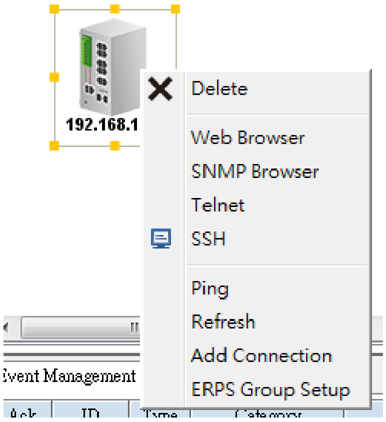
The NetMaster is supported with the ERPS configuration. Through the NetMaster user can set up the ERPS Ring.



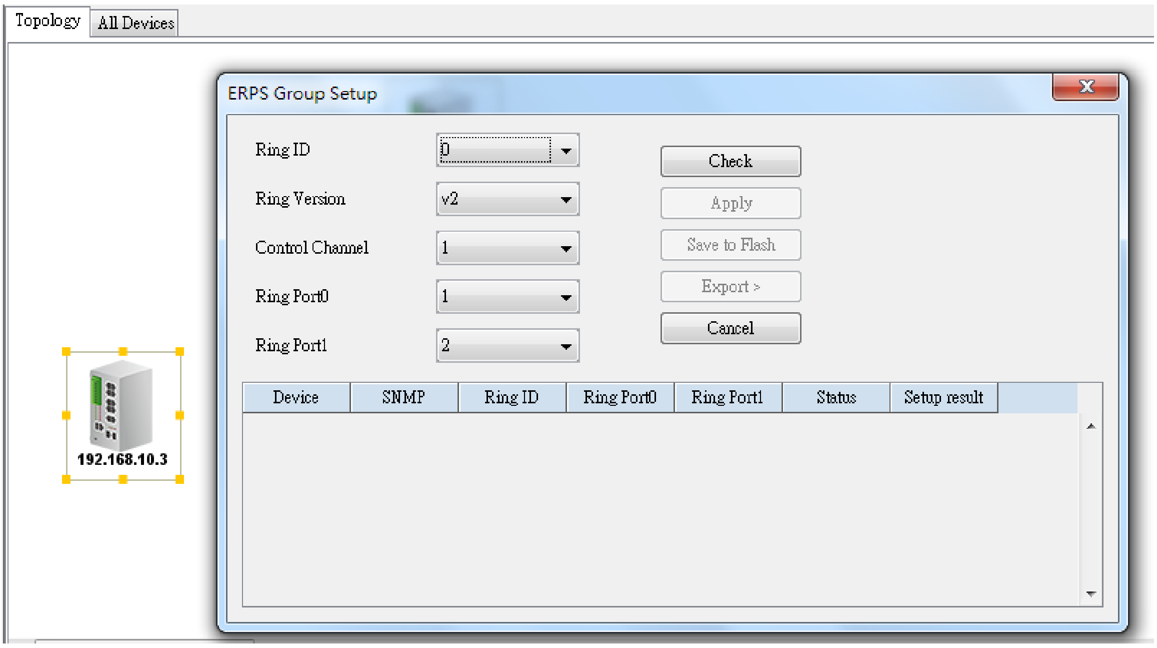
The picture above shows ERPS ring visualization that consists of a Major Ring and a Sub Ring. The device that included in the Major ring is represented with the purple connection color. The device that included in the Sub ring is represented with the dark yellow connection color. This display will be automatic updated every 30 seconds device polling. To assign the device to major or sub ring, user can configure it from the Web Management.

6.4.2 CREATE AN ERPS CONFIGURATION TO A DEVICE.

Click the device and right click on it, then click the ERPS Group Setup.



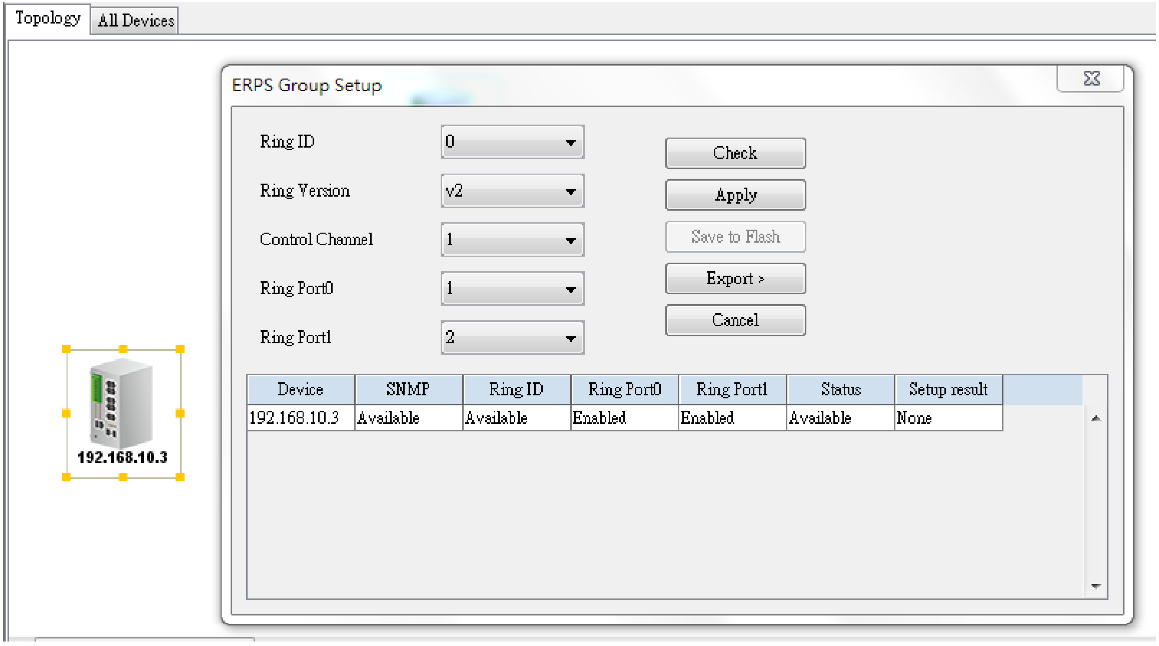
After that ERPS Group Setup interface will appear and user can click Check to make sure if the setting is available and can be used. In the ERPS group setup window, user can do the group setup for the ring ID, version, control channel ring port0 and ring port1.



Ring ID: 0
Ring Version: v2
Control Channel: 1
Ring Port0: 1
Ring Port1: 2

Device	SNMP	Ring ID	Ring Port0	Ring Port1	Status	Setup result

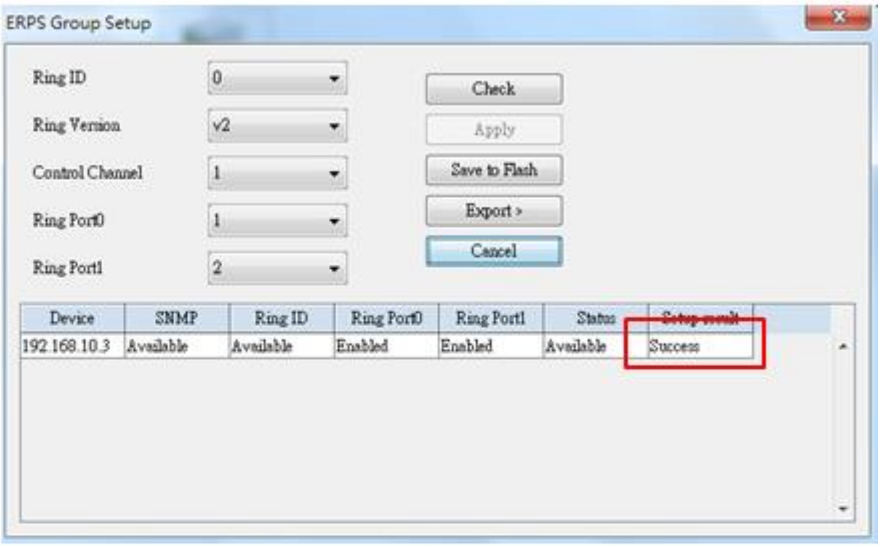
After user click **Check** some informations will appear on the table as below.



Ring ID: 0
Ring Version: v2
Control Channel: 1
Ring Port0: 1
Ring Port1: 2

Device	SNMP	Ring ID	Ring Port0	Ring Port1	Status	Setup result
192.168.10.3	Available	Available	Enabled	Enabled	Available	None

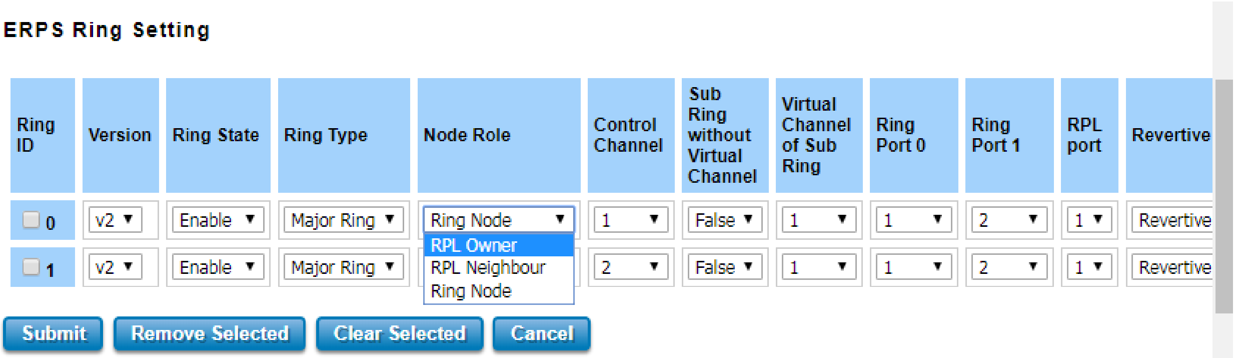
Click **Apply** to apply the ERPS configuration to the device. If the configuration is success, the information will be updated to Success Status. This means user can start create the connection.



ERPS Group Setup

Ring ID: 0
Ring Version: v2
Control Channel: 1
Ring Port0: 1
Ring Port1: 2

Device	SNMP	Ring ID	Ring Port0	Ring Port1	Status	Setup result
192.168.10.3	Available	Available	Enabled	Enabled	Available	Success

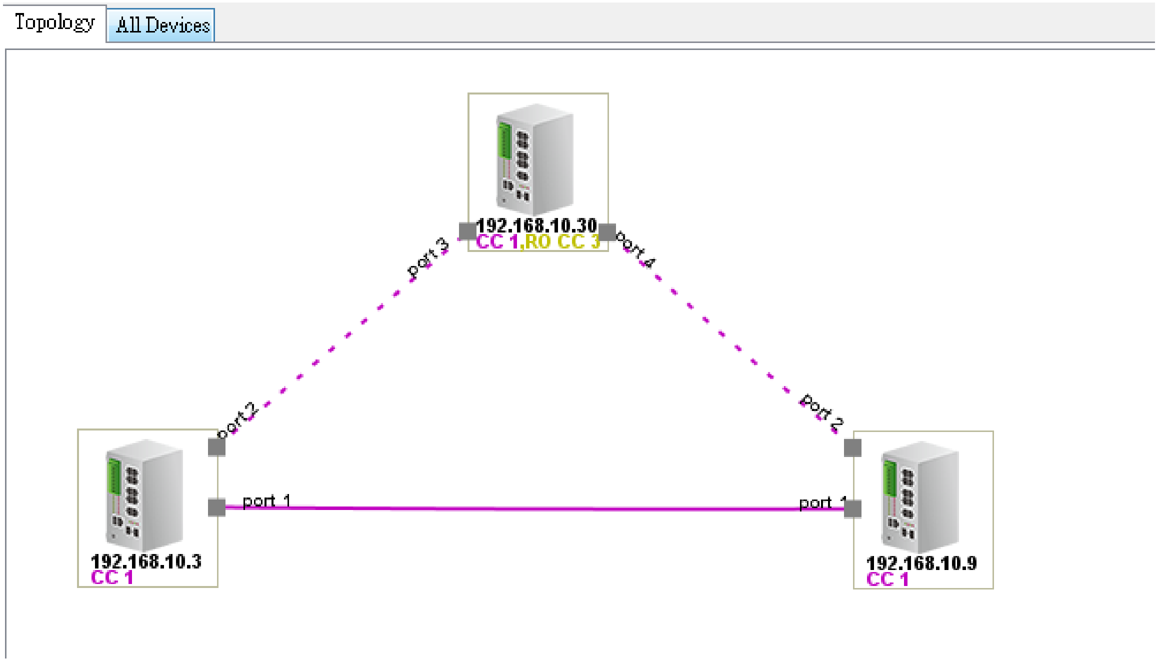


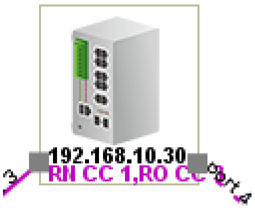
ERPS Ring Setting

Ring ID	Version	Ring State	Ring Type	Node Role	Control Channel	Sub Ring without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 0	Ring Port 1	RPL port	Revertive
□ 0	v2	Enable	Major Ring	Ring Node	1	False	1	1	2	1	Revertive
□ 1	v2	Enable	Major Ring		2	False	1	1	2	1	Revertive

Note: After setup the ERPS environment, don't forget to assign one device as the RPL Owner. User can use the web management to do the configuration.

When the connection is established, it will show the success connection as below.



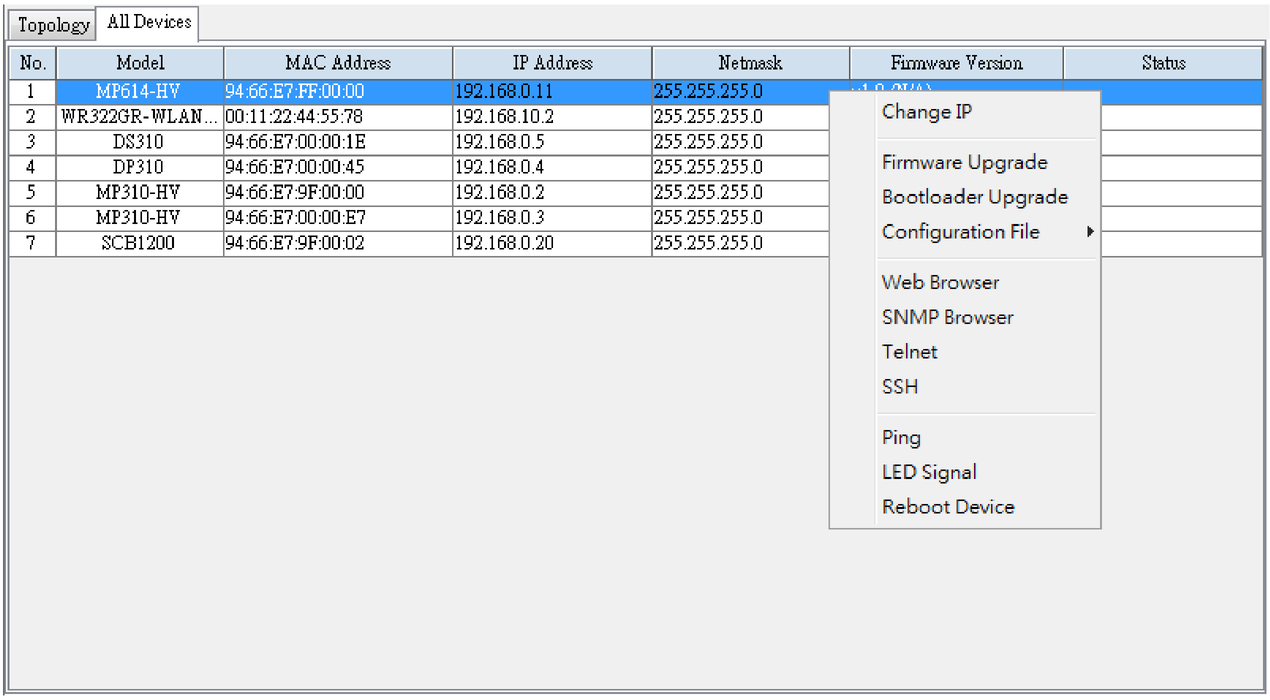


Under the device icon, user will see several label that appear after the ERPS configuration is established. Below is the information.

CC: Control Channel
RO: RPL Owner
RN: RPL Neighbor

7. DEVICE MANAGEMENT

This section explains the device configuration on the **All Devices** Tab. One or group of devices can be configured at a time. The methods of mouse selection can be single selected at any rows by **Ctrl** + mouse click or multiple selected by click one device and then press **Shift** + click to the next device. After having one or more devices selected, use the right click to show pop-up menu.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0		
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.2	255.255.255.0		
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0		
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0		
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0		
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0		
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0		

Following topics are covered in this section describing the pop-up menu functions:

7.1 Global Settings

7.2 Firmware Upgrade

7.3 Configure File

7.4 Manage Device

Note: Remember to stay in Edit Mode and select the device that need to be configured.

7.1 GLOBAL SETTINGS

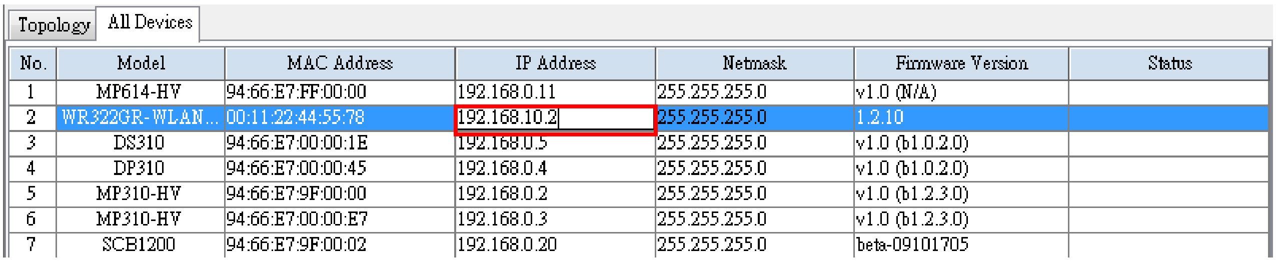
7.1.1 CHANGE IP

User can use this mechanism to assign the new IP address to the devices.

For this mechanism, user just needs to change the IP directly from the list on the IP Address Column.

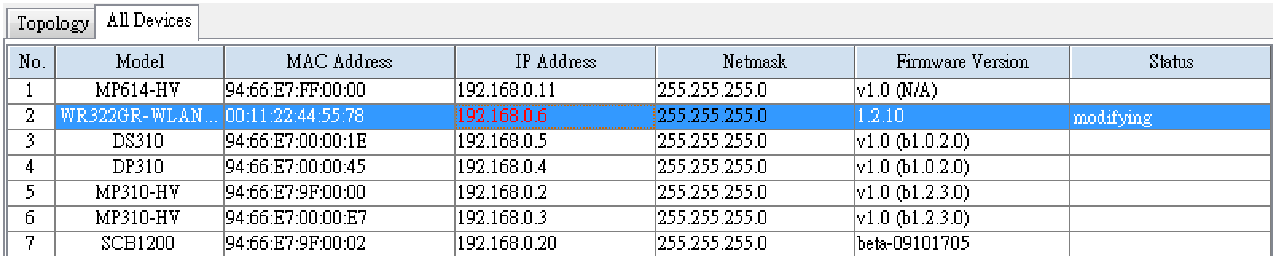
Change IP Mechanism steps:

- Double click at the specific IP Address that user wants to change.



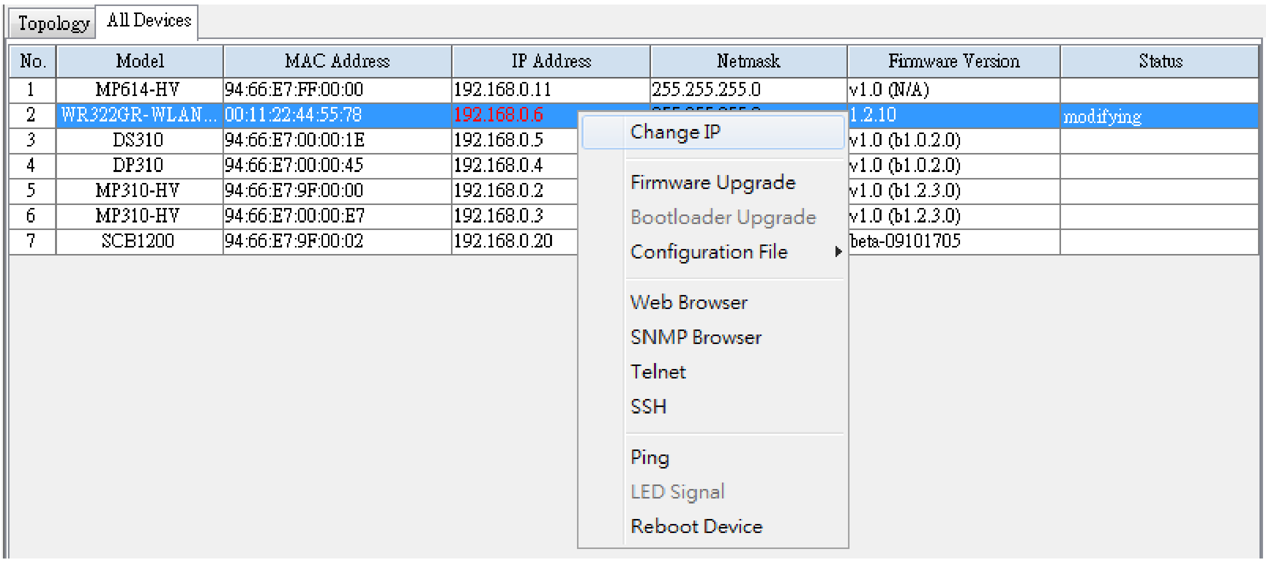
No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.2	255.255.255.0	1.2.10	
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0	v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0	beta-09101705	

- Enter the new IP Address, and then press Enter.



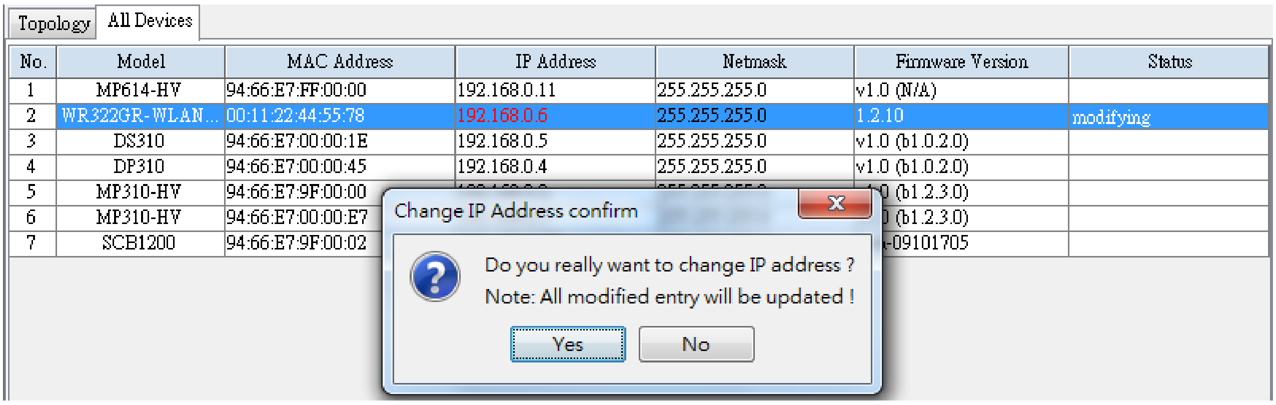
No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	modifying
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0	v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0	beta-09101705	

- Right click at the selected list, and click Change IP



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6		1.2.10	modifying
3	DS310	94:66:E7:00:00:1E	192.168.0.5		v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4		v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2		v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3		v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20		beta-09101705	

- A confirmation pop-up message will appear, and click yes to execute the process.

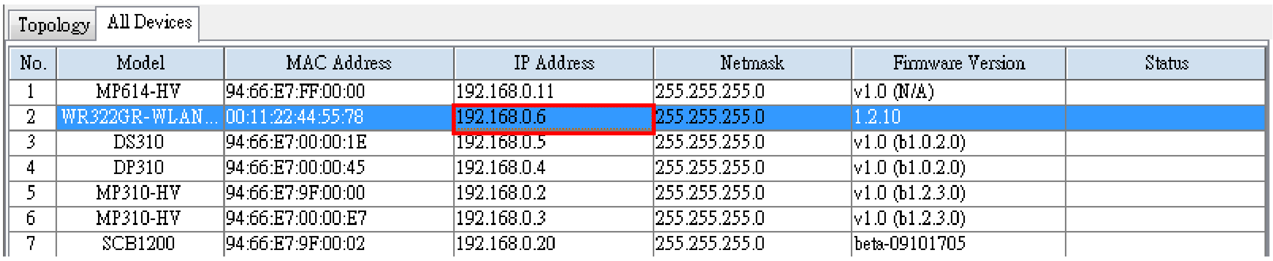


No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	modifying
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00			0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7			0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02			-09101705	

Change IP Address confirm

Do you really want to change IP address ?
Note: All modified entry will be updated !

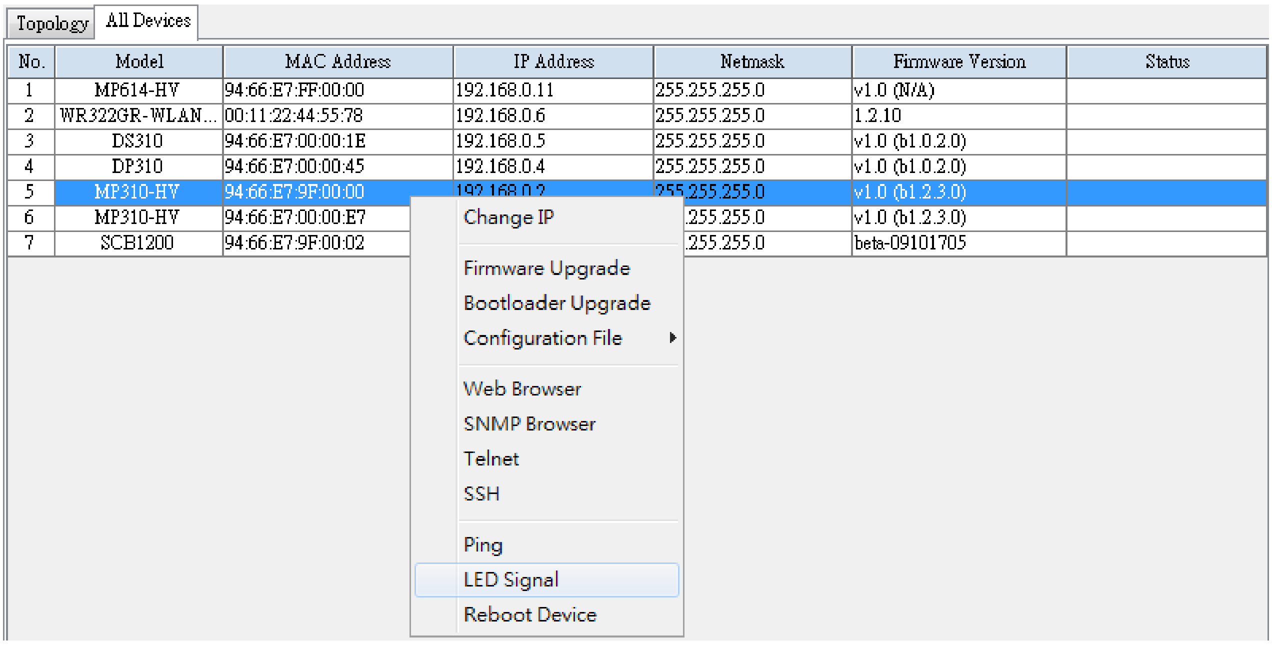
- The IP has been changed.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0	v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0	beta-09101705	

7.1.2 LED SIGNAL

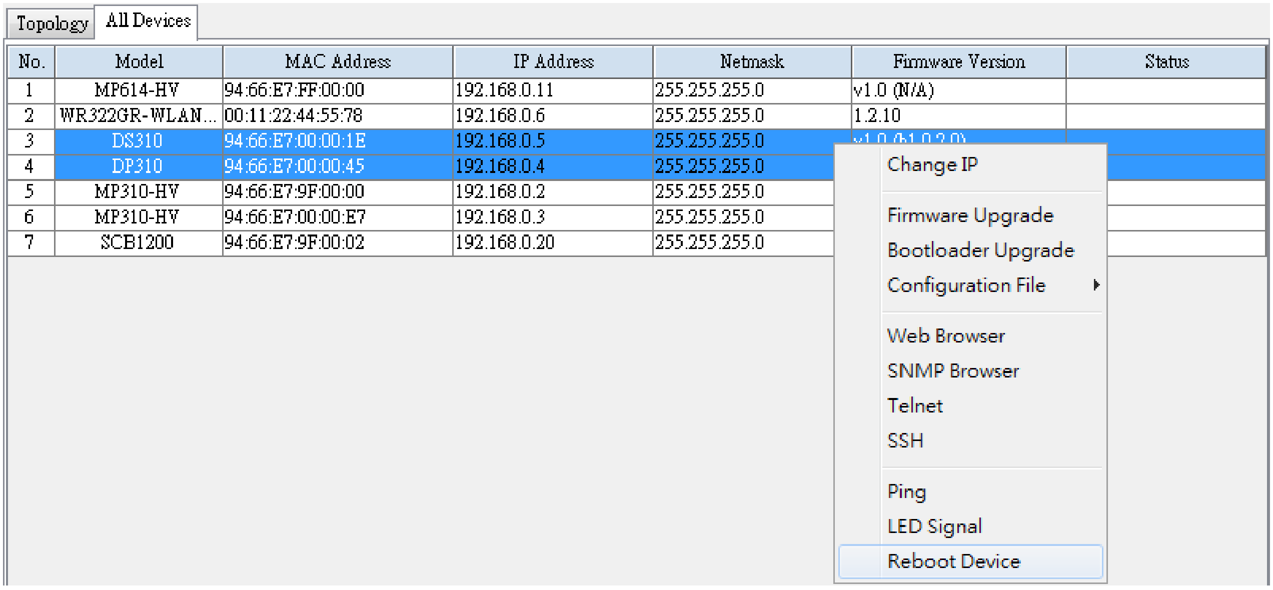
This function is convenient for searching the specific device. While this function is enabled, the light of the System LED from the device will continuously blinking.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7		.255.255.0	v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02		.255.255.0	beta-09101705	

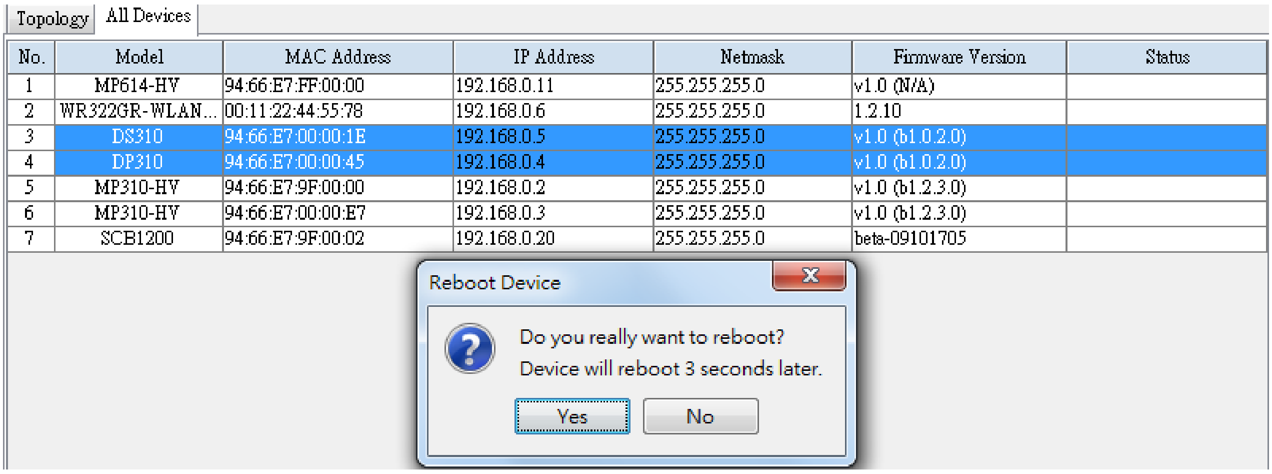
7.1.3 REBOOT DEVICE

Some of the feature change to require user to reboot the system. Click on the selected device then Click **Reboot Device** on pop-menu to reboot the selected device. User can select more than one device.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0		
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0		
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0		
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0		

A pop-up confirmation page will appear and then click yes to reboot the device. The device will be rebooted after 3 seconds.

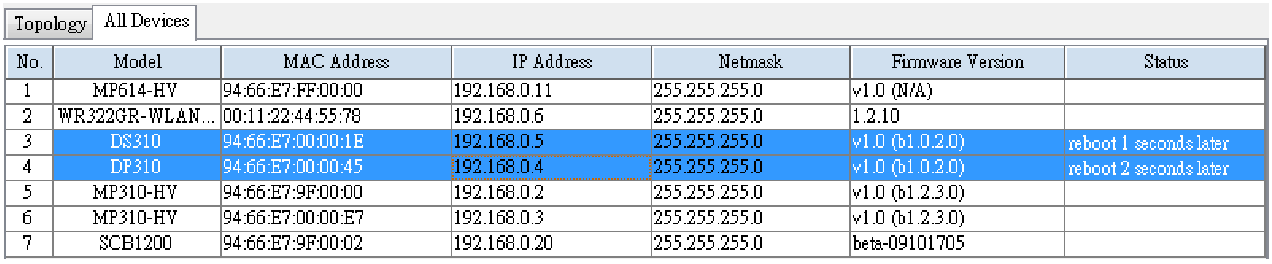


No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0	v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0	beta-09101705	

Reboot Device

Do you really want to reboot?
Device will reboot 3 seconds later.

And user will see the reboot status from the table.

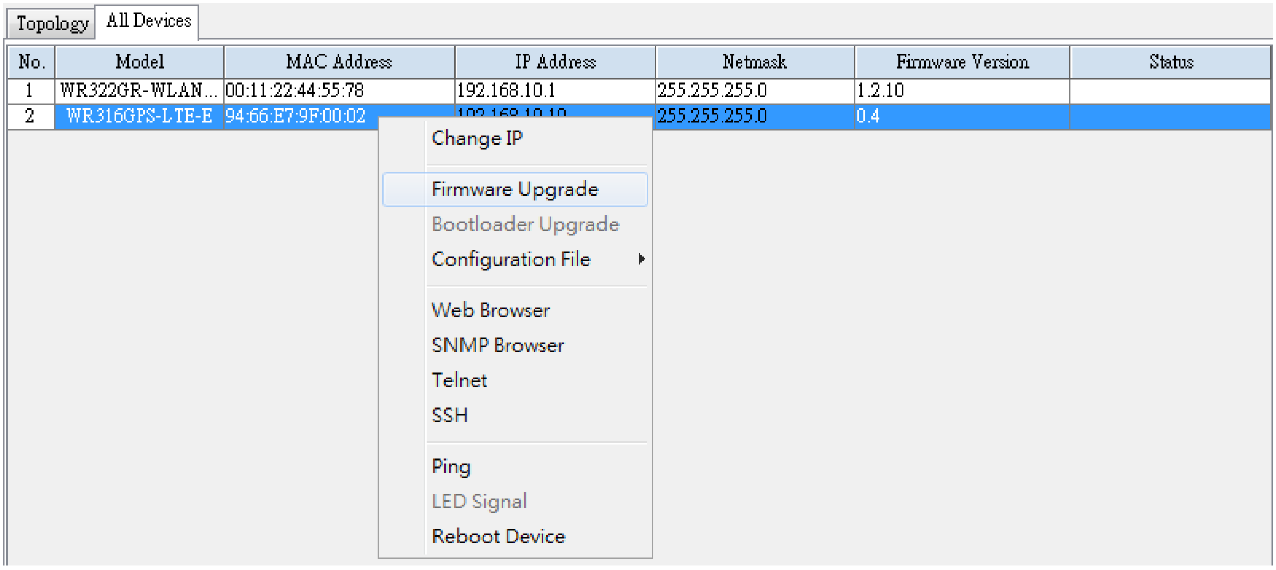


No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	MP614-HV	94:66:E7:FF:00:00	192.168.0.11	255.255.255.0	v1.0 (N/A)	
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.0.6	255.255.255.0	1.2.10	
3	DS310	94:66:E7:00:00:1E	192.168.0.5	255.255.255.0	v1.0 (b1.0.2.0)	reboot 1 seconds later
4	DP310	94:66:E7:00:00:45	192.168.0.4	255.255.255.0	v1.0 (b1.0.2.0)	reboot 2 seconds later
5	MP310-HV	94:66:E7:9F:00:00	192.168.0.2	255.255.255.0	v1.0 (b1.2.3.0)	
6	MP310-HV	94:66:E7:00:00:E7	192.168.0.3	255.255.255.0	v1.0 (b1.2.3.0)	
7	SCB1200	94:66:E7:9F:00:02	192.168.0.20	255.255.255.0	beta-09101705	

7.2 FIRMWARE & BOOTLOADER UPGRADE

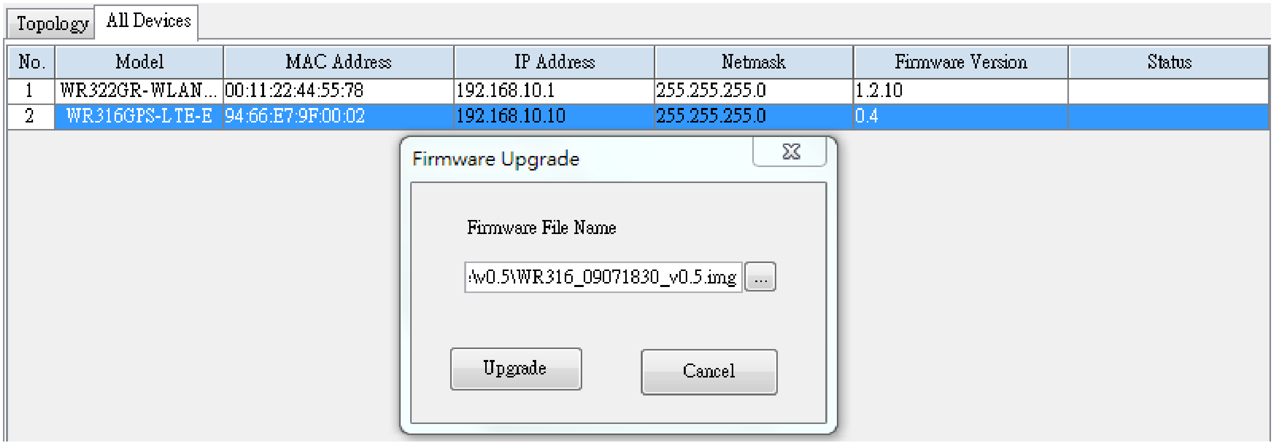
In this section, user can upgrade the latest firmware or bootloader for the device. The latest version can be downloaded from WoMaster website. The new version firmware and bootloader may include new features, bug fixes or other software changes. WoMaster also provides the release notes for the new version as well. Please check the version number after the switch is rebooted. Below is the example of Firmware Upgrade.

- Select the device that needs to be upgraded. Then right click on it, click Firmware Upgrade.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.1	255.255.255.0	1.2.10	
2	WR316GPS-LTE-E	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.4	

- After that, a pop-up window will appear. User can start to find the related firmware file. The file should be image file .img for wireless device or .bin for switch.

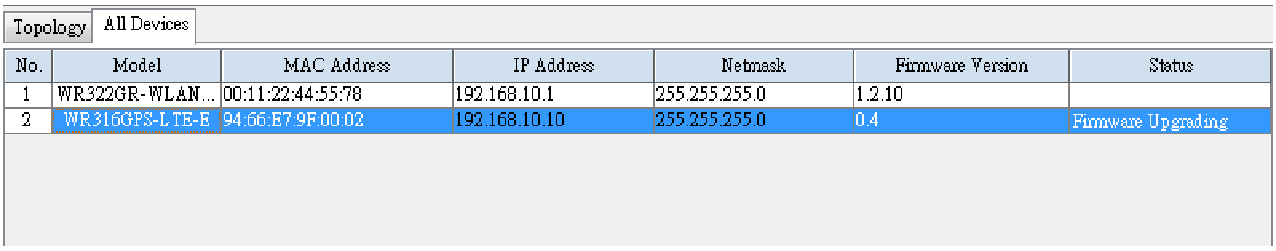


No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.1	255.255.255.0	1.2.10	
2	WR316GPS-LTE-E	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.4	

Firmware File Name

:\v0.5\WR316_09071830_v0.5.img

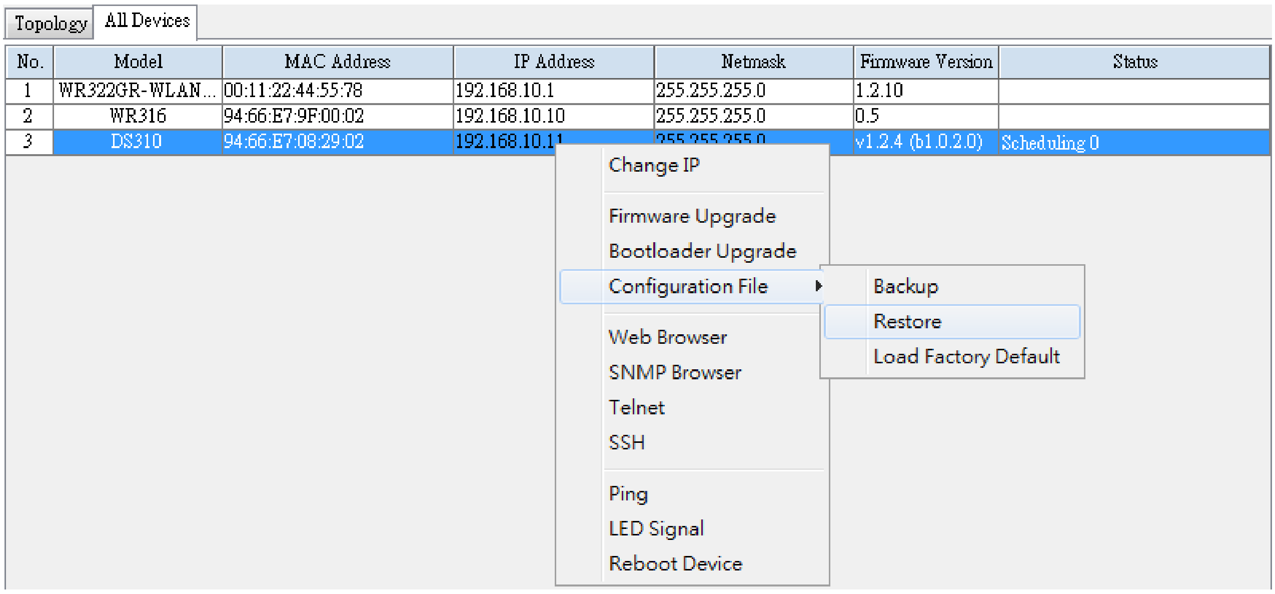
- Then click upgrade button and the status will show Firmware Upgrading. After the firmware or bootloader upgrade process is done, the device will be automatically rebooted.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.1	255.255.255.0	1.2.10	
2	WR316GPS-LTE-E	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.4	Firmware Upgrading

7.3 CONFIGURATION FILE

The configuration file is about back up the configuration, restore the configuration and reset the configuration to the factory default.

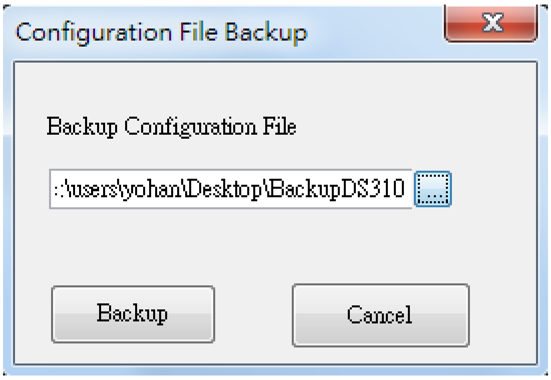


No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.1	255.255.255.0	1.2.10	
2	WR316	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.5	
3	DS310	94:66:E7:08:29:02	192.168.10.11	255.255.255.0	v1.2.4 (b1.0.2.0)	Scheduling 0

7.3.1 BACKUP

With Backup function, the current configuration file can be saved in the device flash.

Find the specific directory to keep the Backup file and enter a name for the backup file. Click Backup to execute then it will automatically give the file name including the IP Address of the device. (Ex: Backup.192.168.10.11.bin)

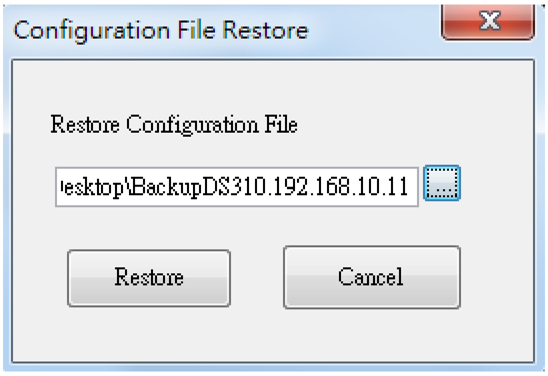


Backup Configuration File

:\users\yohan\Desktop\BackupDS310

7.3.2 RESTORE

This will allow user to go to restore the configuration file back to the device. Find the specific configuration file that should be restored.

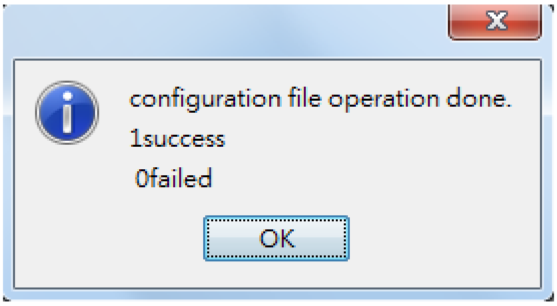


Configuration File Restore

Restore Configuration File

'esktop\BackupDS310.192.168.10.11

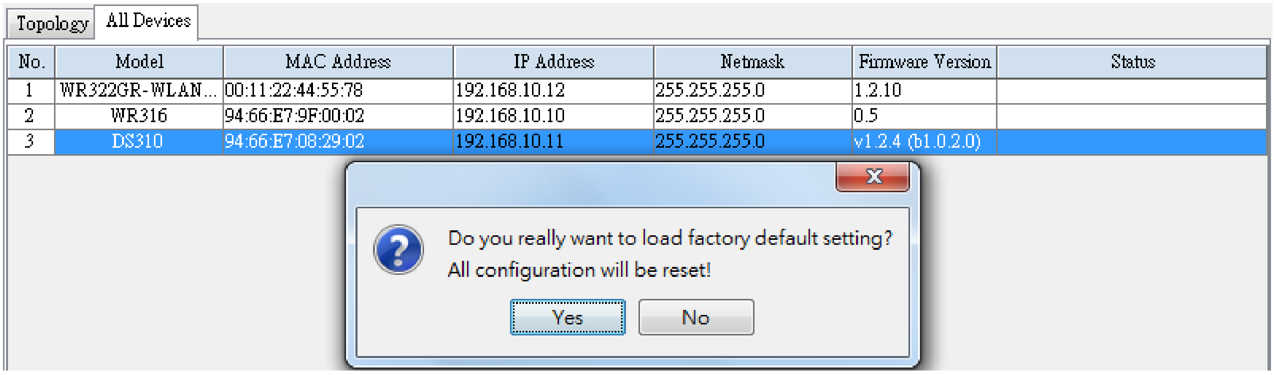
Click Restore to execute, after the restoration process is done a pop-up window will appear to inform whether the process is success or failed.



configuration file operation done.
1success
0failed

7.3.3 LOAD FACTORY DEFAULT

User can reset all the configurations of the device to the factory default setting include the IP Address will be reset to the default IP Address (192.168.10.1). When user executes the Load Factory Default feature, a pop-up window will appear for confirmation. Click Yes to execute.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.12	255.255.255.0	1.2.10	
2	WR316	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.5	
3	DS310	94:66:E7:08:29:02	192.168.10.11	255.255.255.0	v1.2.4 (b1.0.2.0)	

Do you really want to load factory default setting?
All configuration will be reset!

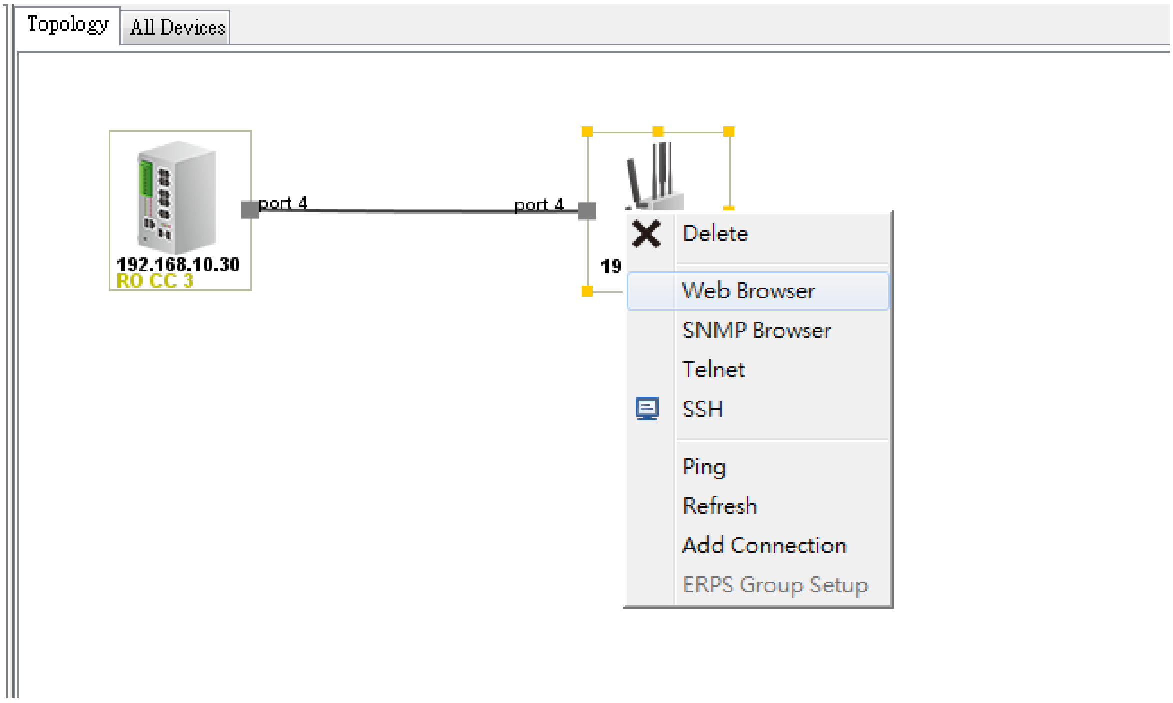
7.4 MANAGE DEVICE

WoMaster devices are supported with both in-band and out-of-band network management. The user can either configure the device through the user friendly Web/HTTPS management or remotely manage the device through the network by console management or Telnet/SSH.

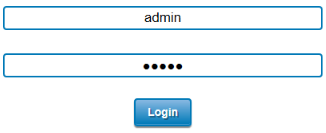
7.4.1 WEB BROWSER

WoMaster devices are supported with user friendly web management. It allows user to use a standard web-browser such as Internet Explorer, Google Chrome or Mozilla, to configure and monitor the device from anywhere on the network.

1. Select a device on the Topology tab or All Device tab which user wants to configure.



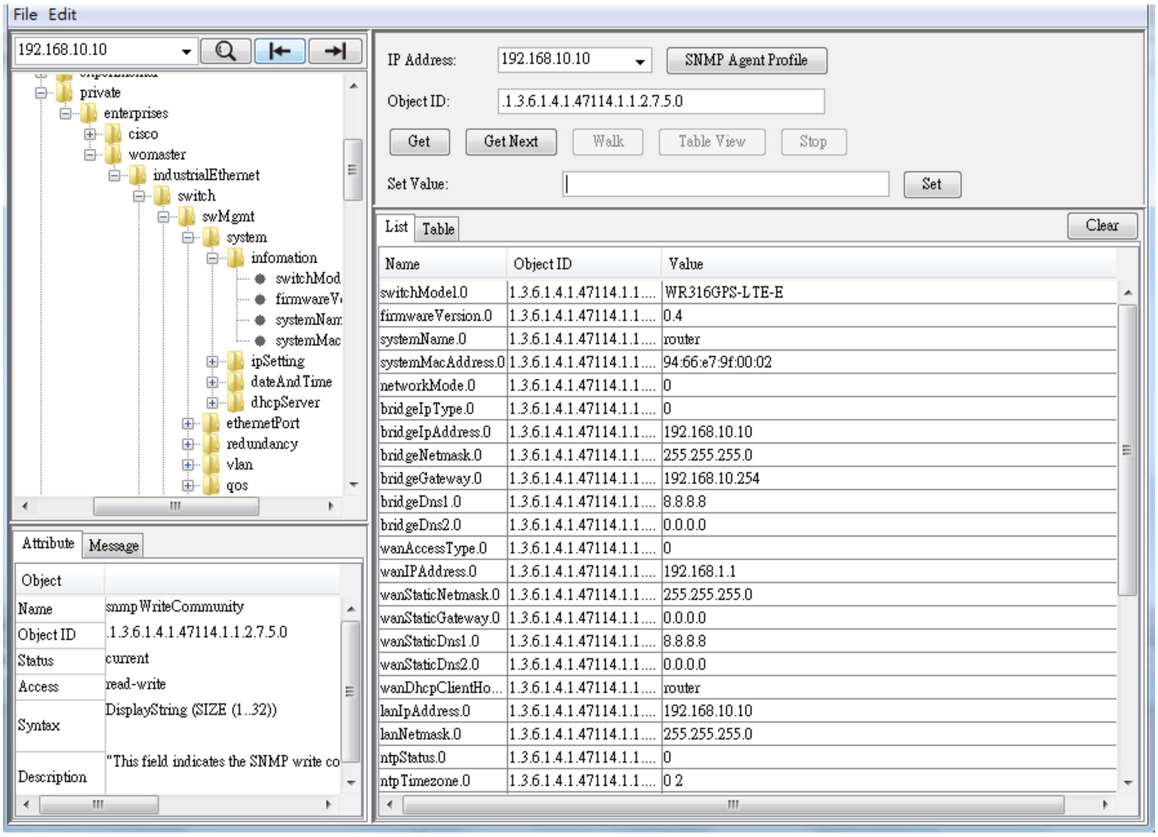
2. Do the right-click after selected the device and click on the **Web Browser** menu-item of pop-up menu.
3. The login screen in Internet Explorer will appear.
4. Key in user name and the password. Default user name and password are both **admin**.



5. Once user enters the web-based management interface, user can freely change the configuration to fit the network environment.

7.4.2 SNMP BROWSER

NetMaster provides a SNMP browser tool 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. WoMaster provides many standard MIBs for users to configure or monitor the device configuration by SNMP. WoMaster supports Public MIB and also provides Private MIBs for users to configure or monitor the device’s configuration by SNMP. WoMaster provides Private MIB to meet up the need. The Private MIB can be found in or downloaded from WoMaster Web site (www.womaster.eu). The SNMP Browser tool allows user to read and write the MIB of the selected device.



IP Address: 192.168.10.10

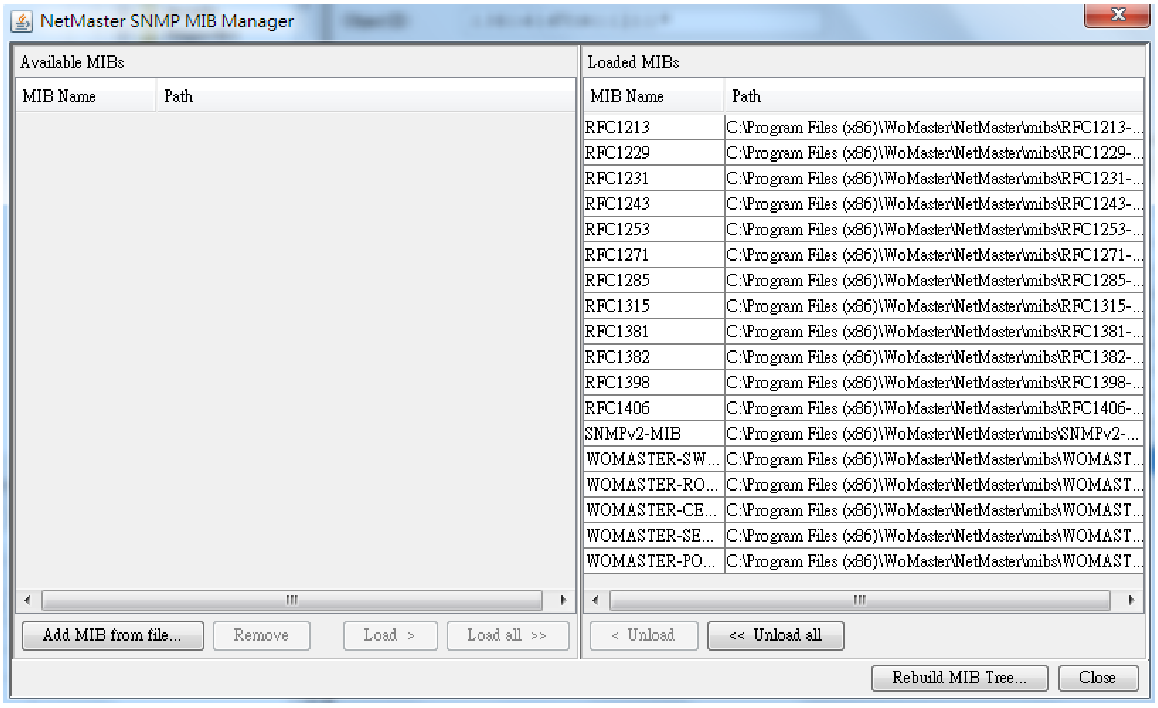
Object ID: .1.3.6.1.4.1.47114.1.1.2.7.5.0

Set Value:

Object	
Name	snmpWriteCommunity
Object ID	.1.3.6.1.4.1.47114.1.1.2.7.5.0
Status	current
Access	read-write
Syntax	DisplayString (SIZE (1..32))
Description	"This field indicates the SNMP write co

Name	Object ID	Value
switchModel.0	1.3.6.1.4.1.47114.1.1....	WR316GPS-LTE-E
firmwareVersion.0	1.3.6.1.4.1.47114.1.1....	0.4
systemName.0	1.3.6.1.4.1.47114.1.1....	router
systemMacAddress.0	1.3.6.1.4.1.47114.1.1....	94:66:e7:9f:00:02
networkMode.0	1.3.6.1.4.1.47114.1.1....	0
bridgeIpType.0	1.3.6.1.4.1.47114.1.1....	0
bridgeIpAddress.0	1.3.6.1.4.1.47114.1.1....	192.168.10.10
bridgeNetmask.0	1.3.6.1.4.1.47114.1.1....	255.255.255.0
bridgeGateway.0	1.3.6.1.4.1.47114.1.1....	192.168.10.254
bridgeDns1.0	1.3.6.1.4.1.47114.1.1....	8.8.8.8
bridgeDns2.0	1.3.6.1.4.1.47114.1.1....	0.0.0.0
wanAccessType.0	1.3.6.1.4.1.47114.1.1....	0
wanIPAddress.0	1.3.6.1.4.1.47114.1.1....	192.168.1.1
wanStaticNetmask.0	1.3.6.1.4.1.47114.1.1....	255.255.255.0
wanStaticGateway.0	1.3.6.1.4.1.47114.1.1....	0.0.0.0
wanStaticDns1.0	1.3.6.1.4.1.47114.1.1....	8.8.8.8
wanStaticDns2.0	1.3.6.1.4.1.47114.1.1....	0.0.0.0
wanDhcpClientHo...	1.3.6.1.4.1.47114.1.1....	router
lanIpAddress.0	1.3.6.1.4.1.47114.1.1....	192.168.10.10
lanNetmask.0	1.3.6.1.4.1.47114.1.1....	255.255.255.0
ntpStatus.0	1.3.6.1.4.1.47114.1.1....	0
ntpTimezone.0	1.3.6.1.4.1.47114.1.1....	0 2

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.

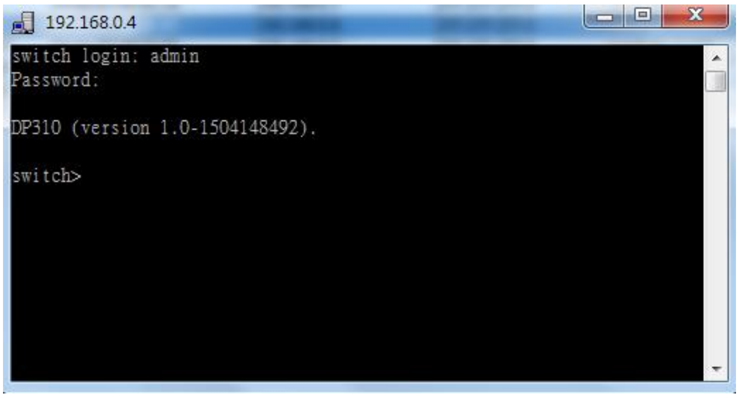


MIB Name	Path
RFC1213	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1213-...
RFC1229	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1229-...
RFC1231	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1231-...
RFC1243	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1243-...
RFC1253	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1253-...
RFC1271	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1271-...
RFC1285	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1285-...
RFC1315	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1315-...
RFC1381	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1381-...
RFC1382	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1382-...
RFC1398	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1398-...
RFC1406	C:\Program Files (x86)\WoMaster\NetMaster\mibs\RFC1406-...
SNMPv2-MIB	C:\Program Files (x86)\WoMaster\NetMaster\mibs\SNMPv2-...
WOMASTER-SW...	C:\Program Files (x86)\WoMaster\NetMaster\mibs\WOMAST...
WOMASTER-RO...	C:\Program Files (x86)\WoMaster\NetMaster\mibs\WOMAST...
WOMASTER-CE...	C:\Program Files (x86)\WoMaster\NetMaster\mibs\WOMAST...
WOMASTER-SE...	C:\Program Files (x86)\WoMaster\NetMaster\mibs\WOMAST...
WOMASTER-PO...	C:\Program Files (x86)\WoMaster\NetMaster\mibs\WOMAST...

Click **Add MIB from file…** to add new MIB file. Load this new MIB file and then click **Rebuild MIB Tree…** to update **MIB Tree**. In this page user can **load or unload** the MIB file based on the needs.

7.4.3 TELNET

WoMaster devices are supported with Telnet console. User can connect to the device by Telnet. Here user can use CLI command to configure the device.



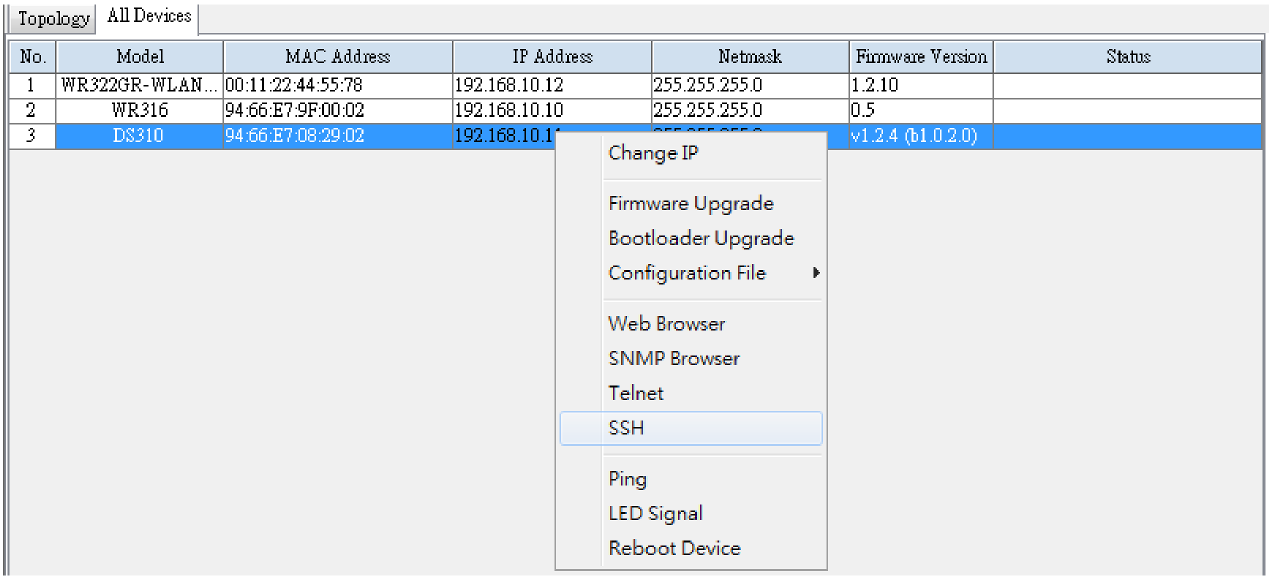
```
switch login: admin
Password:

DP310 (version 1.0-1504148492).

switch>
```

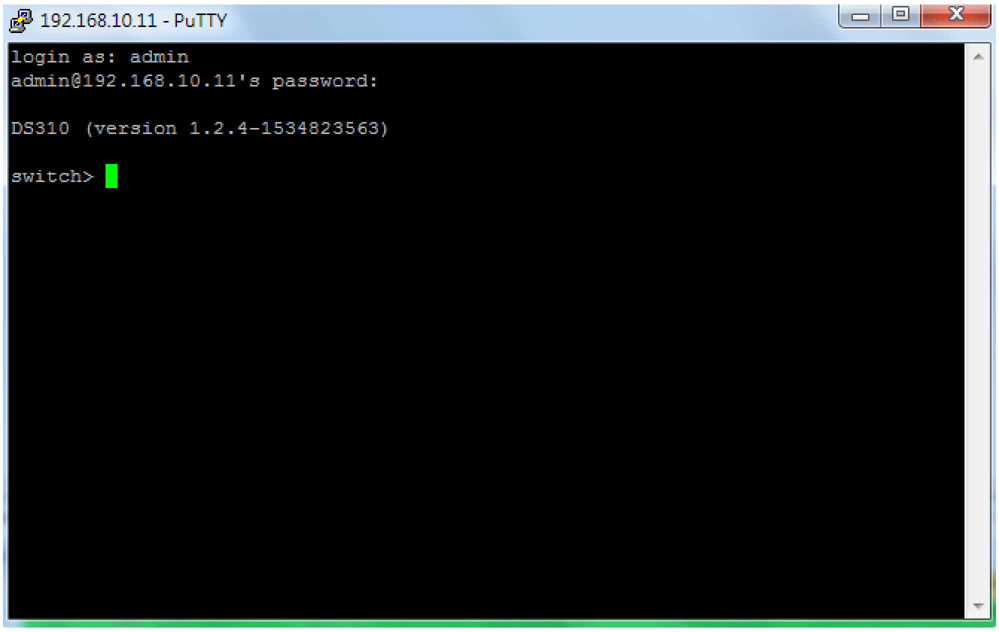
7.4.4 SSH (SECURE SHELL)

WoMaster devices also supported with SSH console. User can remotely connect to the device by command line interface. The SSH connection can secure all the configuration commands that sent to the device. SSH is a client/server architecture where network devices are considered as the SSH server. When user wants to make SSH connection with the switch, please download the SSH client tool first. The example below is using PuTTY software.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.12	255.255.255.0	1.2.10	
2	WR316	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0	0.5	
3	DS310	94:66:E7:08:29:02	192.168.10.1		v1.2.4 (b1.0.2.0)	

After user click the SSH from the menu then a SSH application will open directly. For the SSH application please refers to 10.4 External Application. In the External Application page user can use any kind of external application.



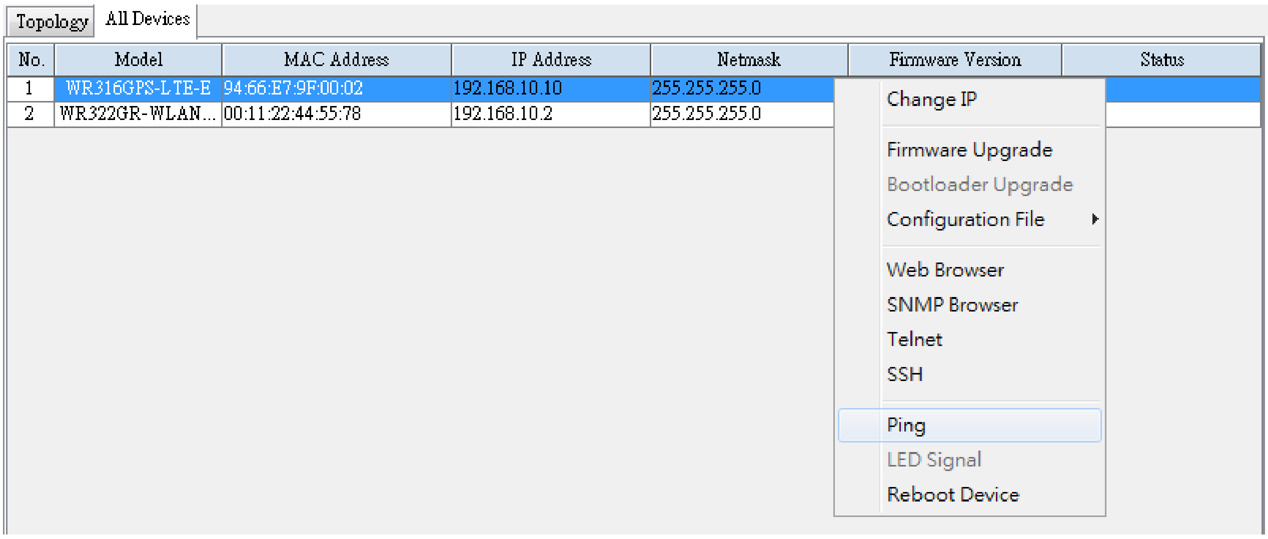
```
login as: admin
admin@192.168.10.11's password:

DS310 (version 1.2.4-1534823563)

switch>
```

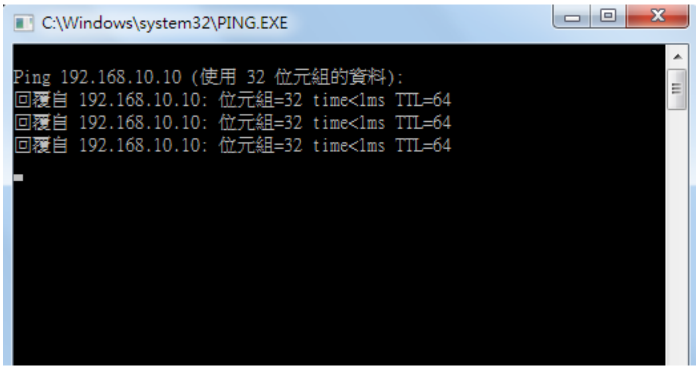
7.4.5 PING

This ping function can confirm the access to WoMaster devices via network. Ping the selected device to verify a normal response time.



No.	Model	MAC Address	IP Address	Netmask	Firmware Version	Status
1	WR316GPS-LTE-E	94:66:E7:9F:00:02	192.168.10.10	255.255.255.0		
2	WR322GR-WLAN...	00:11:22:44:55:78	192.168.10.2	255.255.255.0		

After user click the Ping feature, then a Ping window will directly appear and execute the Ping function to the selected device.

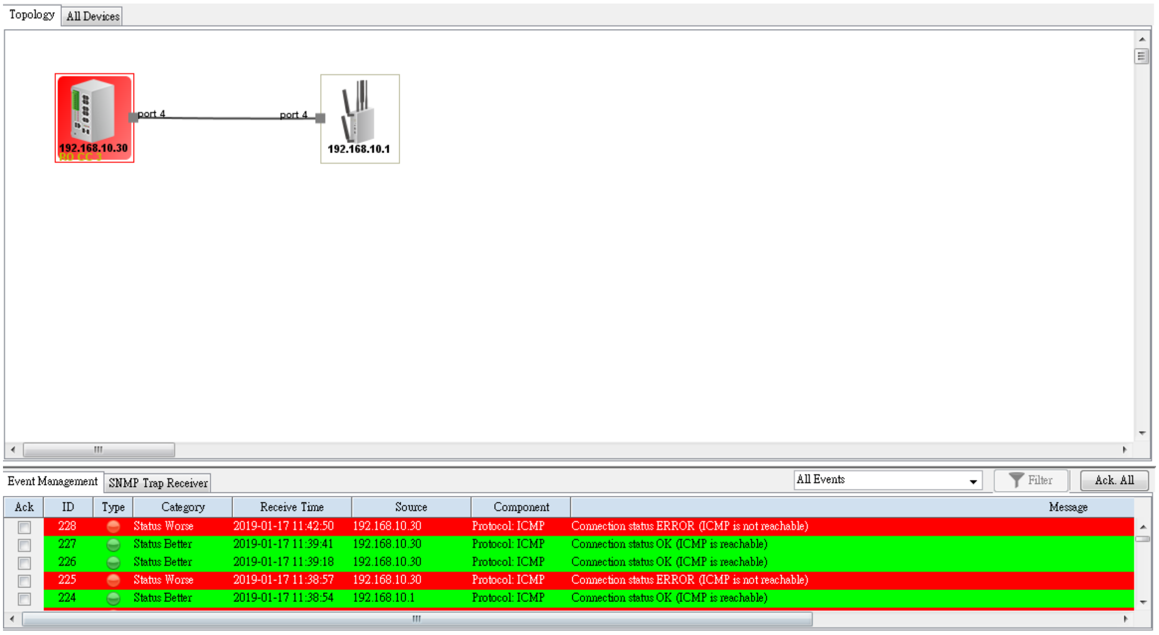


```
Ping 192.168.10.10 (使用 32 位元組的資料):
回覆自 192.168.10.10: 位元組=32 time<1ms TTL=64
回覆自 192.168.10.10: 位元組=32 time<1ms TTL=64
回覆自 192.168.10.10: 位元組=32 time<1ms TTL=64
```

8. EVENT AND ALARM MANAGEMENT

8.1 EVENT MANAGEMENT

User can identify the event type from the event management list (OK - Green, Warning - Yellow, Error - Red, and Normal Status - White) by the color. The notification can be generated based on any appear events. All of the notifications can be notify via email, SNMP trap, Pop up Message and NetMaster.

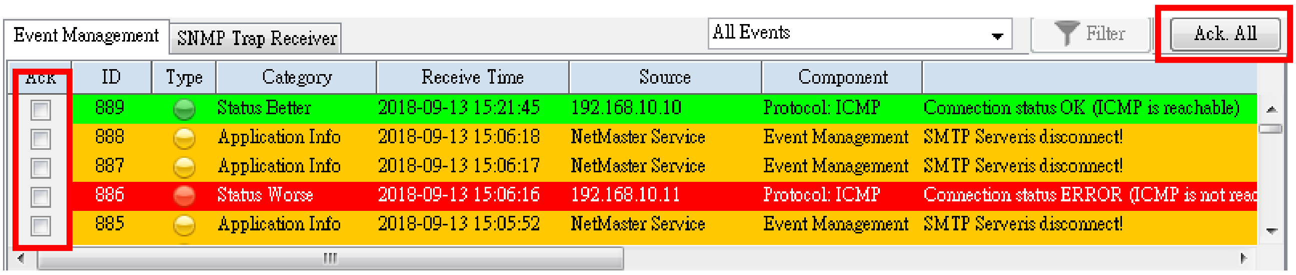


Ack	ID	Type	Category	Receive Time	Source	Component	Message
□	228	●	Status Worse	2019-01-17 11:42:50	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is not reachable)
□	227	●	Status Better	2019-01-17 11:39:41	192.168.10.30	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	226	●	Status Better	2019-01-17 11:39:18	192.168.10.30	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	225	●	Status Worse	2019-01-17 11:38:57	192.168.10.30	Protocol: ICMP	Connection status ERROR (ICMP is not reachable)
□	224	●	Status Better	2019-01-17 11:38:54	192.168.10.1	Protocol: ICMP	Connection status OK (ICMP is reachable)

Every real time event that happened on the Topology tab will be explained clearly in the event Management line. See the red icon and the red list on the event management tab. According to the event message, user can identify what is the detail of the event that occurs to the devices with red background.

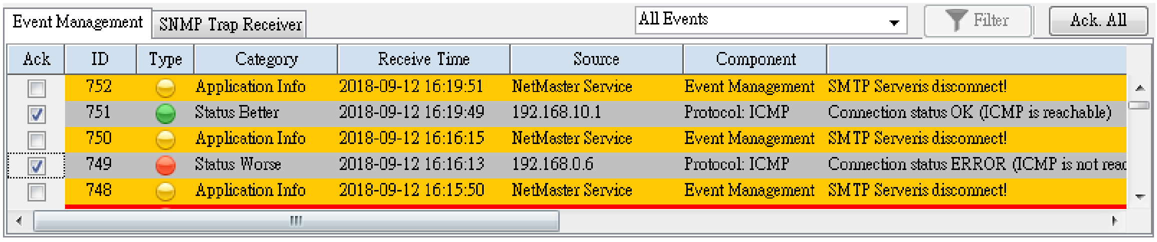
8.1.1 ACK/ACK ALL

Ack/Ack All - This column is to check the status of each event and confirm these events for the 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. Click checkbox to check or Ack All to check all of the lines on the event management.



Ack	ID	Type	Category	Receive Time	Source	Component	
□	889	●	Status Better	2018-09-13 15:21:45	192.168.10.10	Protocol: ICMP	Connection status OK (ICMP is reachable)
□	888	●	Application Info	2018-09-13 15:06:18	NetMaster Service	Event Management	SMTP Serveris disconnect!
□	887	●	Application Info	2018-09-13 15:06:17	NetMaster Service	Event Management	SMTP Serveris disconnect!
□	886	●	Status Worse	2018-09-13 15:06:16	192.168.10.11	Protocol: ICMP	Connection status ERROR (ICMP is not reac
□	885	●	Application Info	2018-09-13 15:05:52	NetMaster Service	Event Management	SMTP Serveris disconnect!

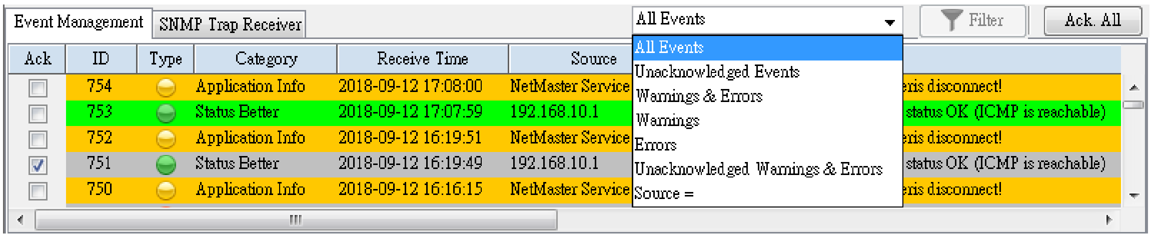
For example, while user checks this Ack checkbox of ID 749 and 751, the link color will change to grey.



Ack	ID	Type	Category	Receive Time	Source	Component	
☐	752	●	Application Info	2018-09-12 16:19:51	NetMaster Service	Event Management	SMTP Serveris disconnect!
☑	751	●	Status Better	2018-09-12 16:19:49	192.168.10.1	Protocol: ICMP	Connection status OK (ICMP is reachable)
☐	750	●	Application Info	2018-09-12 16:16:15	NetMaster Service	Event Management	SMTP Serveris disconnect!
☑	749	●	Status Worse	2018-09-12 16:16:13	192.168.0.6	Protocol: ICMP	Connection status ERROR (ICMP is not reac
☐	748	●	Application Info	2018-09-12 16:15:50	NetMaster Service	Event Management	SMTP Serveris disconnect!

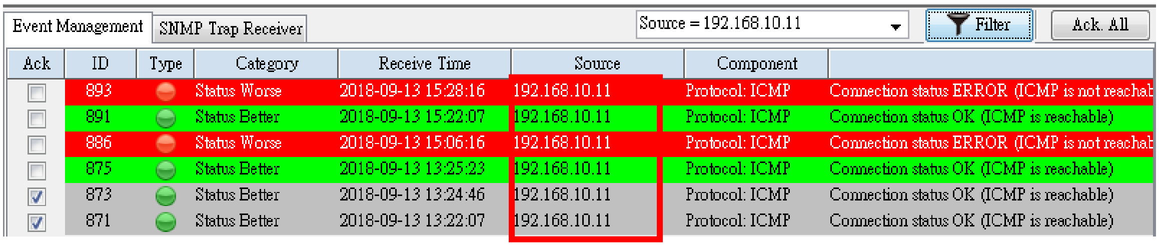
8.1.2 EVENT FILTER

Event Filter - User can choose to use All Events, Unacknowledged Events, Warnings & Errors, Warnings, Errors, Unacknowledged Warnings & Errors and Source = ,so that it can show the event status user wants to see. While choosing "Source =", user should enter the IP address (ex, 192.168.10.1) behind the "Source = "string and click Filter button to filter the events according to the Source column.



Ack	ID	Type	Category	Receive Time	Source	
☐	754	●	Application Info	2018-09-12 17:08:00	NetMaster Service	ris disconnect!
☐	753	●	Status Better	2018-09-12 17:07:59	192.168.10.1	status OK (ICMP is reachable)
☐	752	●	Application Info	2018-09-12 16:19:51	NetMaster Service	ris disconnect!
☑	751	●	Status Better	2018-09-12 16:19:49	192.168.10.1	status OK (ICMP is reachable)
☐	750	●	Application Info	2018-09-12 16:16:15	NetMaster Service	ris disconnect!

For Example: Source = 192.168.10.11, the event list will show all of the events that related with the source.



Ack	ID	Type	Category	Receive Time	Source	Component	
☐	893	●	Status Worse	2018-09-13 15:28:16	192.168.10.11	Protocol: ICMP	Connection status ERROR (ICMP is not reachab
☐	891	●	Status Better	2018-09-13 15:22:07	192.168.10.11	Protocol: ICMP	Connection status OK (ICMP is reachable)
☐	886	●	Status Worse	2018-09-13 15:06:16	192.168.10.11	Protocol: ICMP	Connection status ERROR (ICMP is not reachab
☐	875	●	Status Better	2018-09-13 13:25:23	192.168.10.11	Protocol: ICMP	Connection status OK (ICMP is reachable)
☑	873	●	Status Better	2018-09-13 13:24:46	192.168.10.11	Protocol: ICMP	Connection status OK (ICMP is reachable)
☑	871	●	Status Better	2018-09-13 13:22:07	192.168.10.11	Protocol: ICMP	Connection status OK (ICMP is reachable)

8.1.3 EVENT MANAGEMENT LIST

TYPE	CATEGORY	SOURCE	COMPONENT	MESSAGE
ERROR	STATUS WORSE	Device IP Address	Configuration Backup	Configuration backup failed. Network Error!
ERROR	STATUS WORSE	Device IP Address	Configuration Backup	Configuration file I/O error!
ERROR	STATUS WORSE	Device IP Address	Configuration Restore	Network Error!!
ERROR	STATUS WORSE	Device IP Address	Configuration Restore	Error: connection timeout!!
ERROR	STATUS WORSE	Device IP Address	Configuration Restore	Error: I/O exception occurred while sending file!
ERROR	STATUS WORSE	Device IP Address	Protocol:SNMP	Port XX Link Down

ERROR	STATUS WORSE	Device IP Address	Protocol: ICMP	Connection status ERROR (ICMP is not reachable)
ERROR	STATUS WORSE	NetMaster Service	License	Not Enough License Found!
ERROR	STATUS WORSE	deviceIP	SNMP Trap Receiver	Link down trap OID
NORMAL_STATUS	APPLICATION INFO	NetMaster Service		NetMaster Started
NORMAL_STATUS	APPLICATION INFO	NetMaster Service		Trap Service Ready
NORMAL_STATUS	APPLICATION INFO	NetMaster Service	Remote Access	The client leave Monitor mode. From: Client_IP:Client_port
NORMAL_STATUS	APPLICATION INFO	NetMaster Service	Remote Access	The client leave Edit mode. From: Client_IP:Client_port
NORMAL_STATUS	APPLICATION INFO	NetMaster Service	Remote Access	Authentication is success in Monitor mode. From: Client_IP:Client_port
NORMAL_STATUS	APPLICATION INFO	NetMaster Service	Remote Access	Authentication is success in Edit mode. From: Client_IP:Client_port
NORMAL_STATUS	APPLICATION INFO	NetMaster Service	SNMP Trap Daemon	SNMP Trap Daemon start
NORMAL_STATUS	APPLICATION INFO	NetMaster Service	SNMP Trap Daemon	SNMP Trap Daemon stop
OK	STATUS BETTER	Device IP Address	Configuration Backup	Configuration backup success!
OK	STATUS BETTER	Device IP Address	Configuration Restore	Configuration restore finished.
OK	STATUS BETTER	Device IP Address	Protocol:SNMP	Port XX Link Up
OK	STATUS BETTER	Device IP Address	Protocol: ICMP	Connection status OK (ICMP is reachable)
OK	STATUS BETTER	Device IP Address	SNMP Trap Receiver	Link up trap OID
OK	APPLICATION INFO	Device IP Address	SNMP Trap Receiver	Trap source: source Bindings: binding

WARNING	APPLICATION INFO	Device IP Address	Configuration Restore	Error: No backup configuration file!
WARNING	APPLICATION INFO	Device IP Address	Configuration Restore	MAC address changed
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	The Edit client: Client_IP:Client_port is disconnect!
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	The Monitor client: Client_IP:Client_port is disconnect!
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	Authentication is fail in Monitor mode! From: Client_IP:Client_port
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	It has one client enter Monitor mode! From: Client_IP:Client_port
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	The number of monitor client is exceeded! (Maximum number is 5) From: Client_IP:Client_port
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	Authentication is fail in Edit mode! From: Client_IP:Client_port
WARNING	APPLICATION INFO	NetMaster Service	Remote Access	It has one client enter Edit mode! (Only one client can enter Edit mode)! From: Client_IP:Client_port
WARNING	APPLICATION INFO	NetMaster Service	Event Management	SMTP Server is disconnect!
WARNING	APPLICATION INFO	NetMaster Service	SNMP Trap Daemon	SNMP Trap Daemon Listening port already in used!

****NOTE: Mention in red is the dynamic variable that can change, such as IP Address, port number link and client IP.**

8.2 SNMP TRAP

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

8.2.1 ENABLE THE SNMP TRAP FEATURE

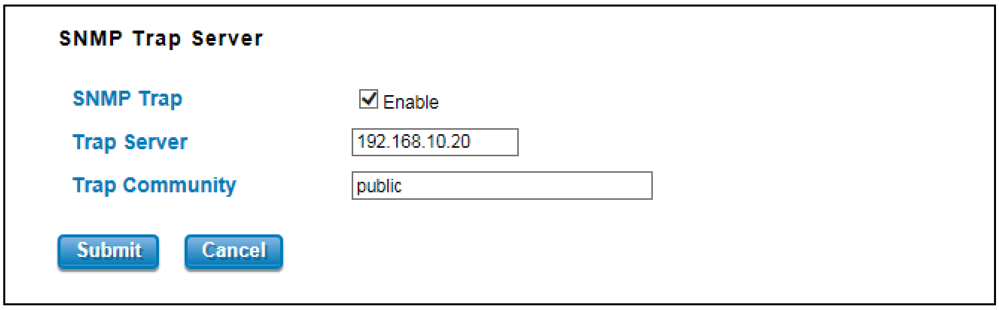
To enable SNMP Trap Server, go to the web management to configure these settings.

1. Select a device on the **Topology** tab or **All Device** tab which user wants 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.

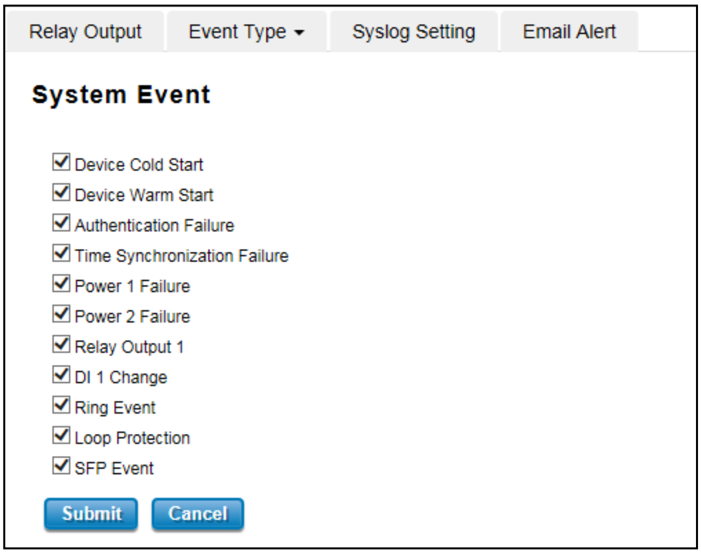
4. Click on SNMP menu. Enable the SNMP feature and SNMP Trap Server, and set SNMP Trap Server IP address (PC IP Address) and set the trap community.



SNMP Trap Server

SNMP Trap	☑ Enable
Trap Server	192.168.10.20
Trap Community	public

5. Don't forget to choose the **Event Type** selection.



System Event

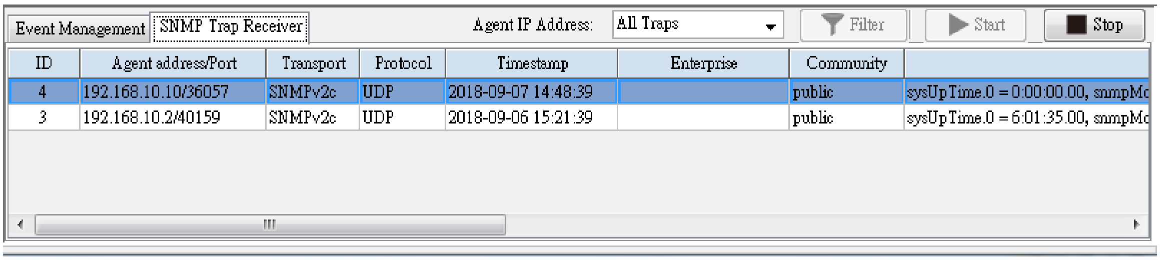
☑ Device Cold Start
☑ Device Warm Start
☑ Authentication Failure
☑ Time Synchronization Failure
☑ Power 1 Failure
☑ Power 2 Failure
☑ Relay Output 1
☑ DI 1 Change
☑ Ring Event
☑ Loop Protection
☑ SFP Event

8.2.2 RECEIVE SNMP TRAP

The SNMP Trap receiver will receive any kind of SNMP traps that generated by the network devices. When an event occurs, the trap details will be directly logged

1. Click on **Start** on the **SNMP Trap Receiver** tab to start receiving the SNMP Trap.

2. For example, when user forgets the password when trying to enter the web management. It will display as follows:



ID	Agent address/Port	Transport	Protocol	Timestamp	Enterprise	Community	
4	192.168.10.10/36057	SNMPv2c	UDP	2018-09-07 14:48:39		public	sysUpTime.0 = 0:00:00.00, snmpMo
3	192.168.10.2/40159	SNMPv2c	UDP	2018-09-06 15:21:39		public	sysUpTime.0 = 6:01:35.00, snmpMo

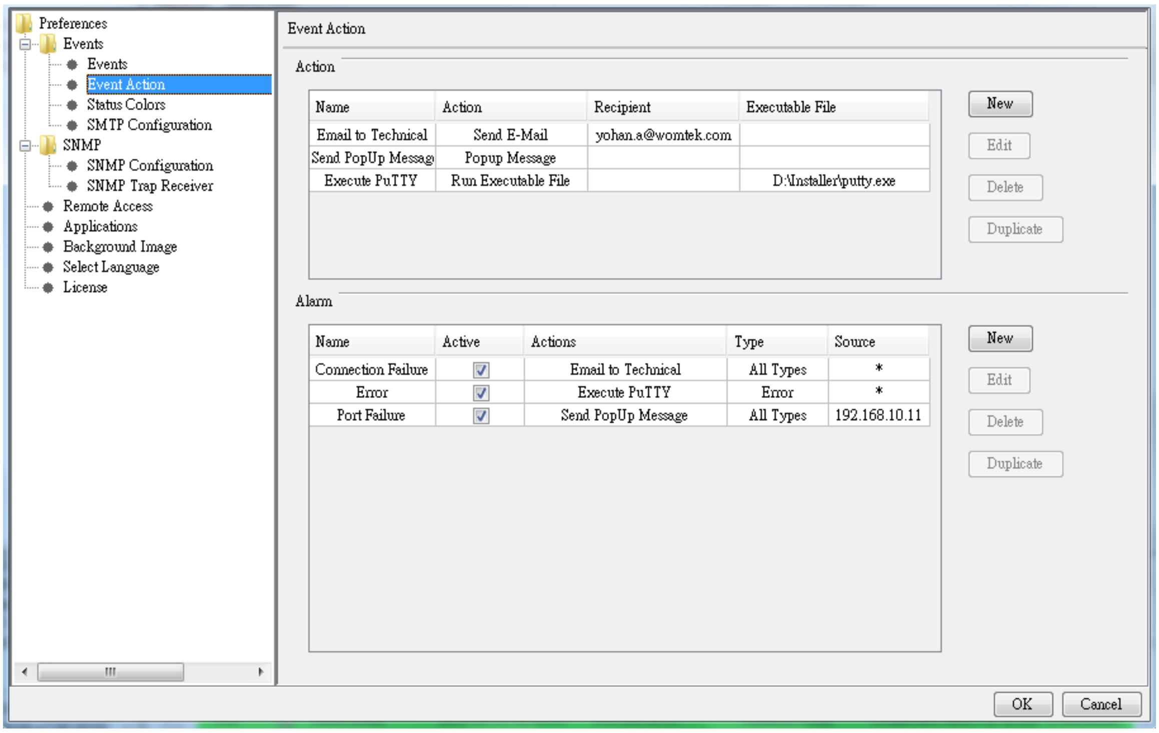
***Note:** If the NetMaster cannot receive any SNMP traps, user needs to check if some other application such as MG-Soft MIB Browser, etc has occupied **the default port: 162**.*

8.3 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 that NetMaster supported are Popup Message, E-mail and Run Executable File.

8.3.1 CREATE AN ACTION

Go to Preference -> Events -> Event Action and new an action.



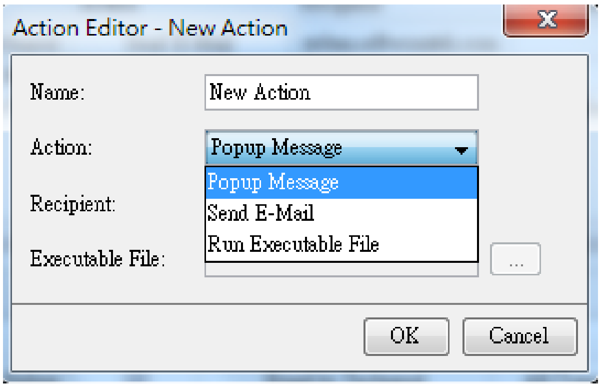
Action

Name	Action	Recipient	Executable File
Email to Technical	Send E-Mail	yohan.a@womtek.com	
Send PopUp Messag	Popup Message		
Execute PuTTY	Run Executable File		D:\Installer\putty.exe

Alarm

Name	Active	Actions	Type	Source
Connection Failure	☑	Email to Technical	All Types	*
Error	☑	Execute PuTTY	Error	*
Port Failure	☑	Send PopUp Message	All Types	192.168.10.11

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



Action Editor - New Action

Name: New Action

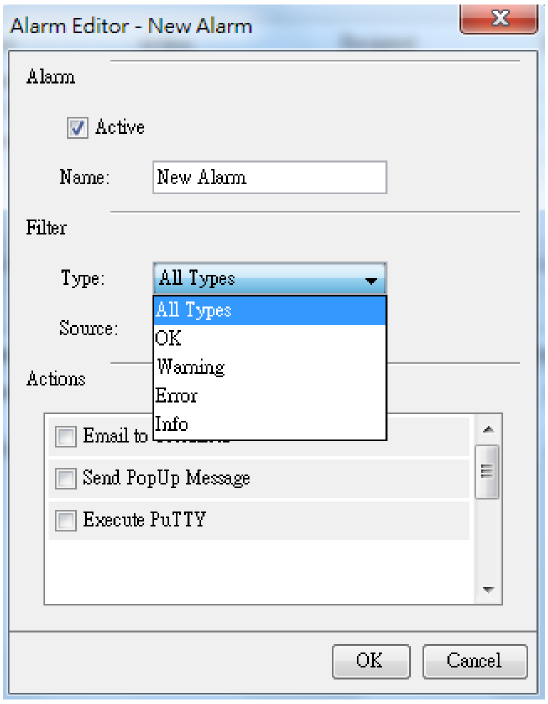
Action: Popup Message

Recipient:

Executable File:

8.3.2 CREATE AN ALARM

Go to Preference -> Event -> Event Action. Click the New button and the Alarm Editor window will be opened. User needs input alarm 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 user wants to trigger. Select action that has been created to decide what action will be executed when this alarm is trigged.



Alarm Editor - New Alarm

Alarm

☑ Active

Name: New Alarm

Filter

Type: All Types

Source:

Actions

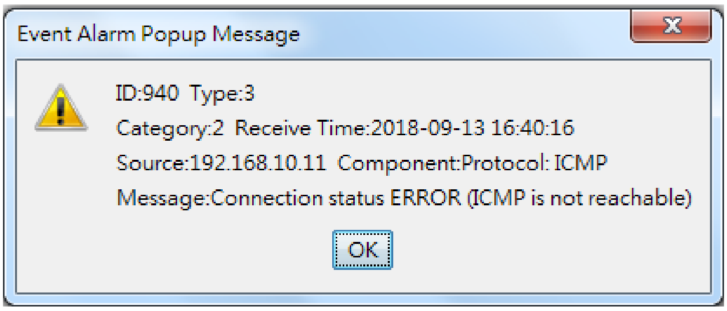
□ Email to

□ Send PopUp Message

□ Execute PuTTY

8.3.3 EVENT ALARM POPUP MESSAGE

When a Popup Message action is executed, the NetMaster server and all of the NetMaster clients will get any popup message as follows:

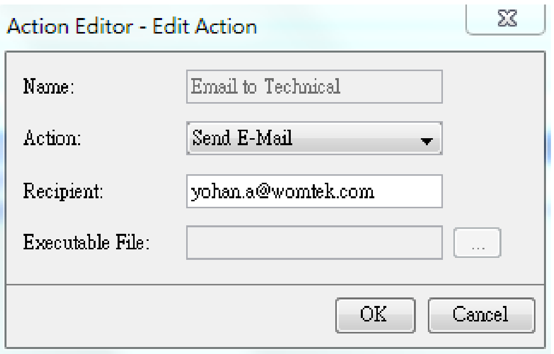


Event Alarm Popup Message

ID:940 Type:3
Category:2 Receive Time:2018-09-13 16:40:16
Source:192.168.10.11 Component:Protocol: ICMP
Message:Connection status ERROR (ICMP is not reachable)

8.3.4 E-MAIL ACTION

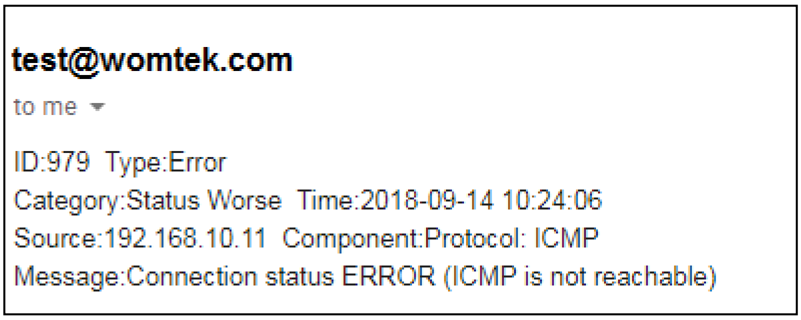
When an E-mail action is executed, the NetMaster will send an alarm e-mail to the registered e-mail account (configured in Preference->SMTP configuration (10.1.4)).



Action Editor - Edit Action

Name: Email to Technical
Action: Send E-Mail
Recipient: yohan.a@womtek.com
Executable File:

The e-mail could show as follows:

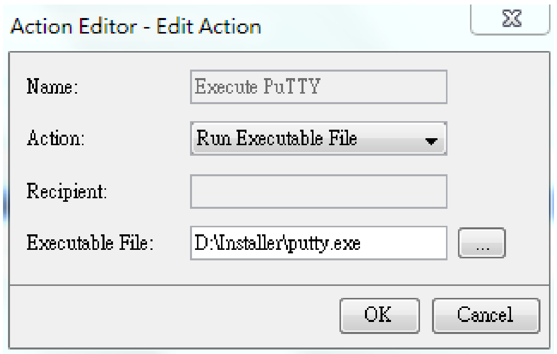


test@womtek.com
to me

ID:979 Type:Error
Category:Status Worse Time:2018-09-14 10:24:06
Source:192.168.10.11 Component:Protocol: ICMP
Message:Connection status ERROR (ICMP is not reachable)

8.3.5 RUN EXECUTABLE FILE ACTION

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



Action Editor - Edit Action

Name: Execute PuTTY

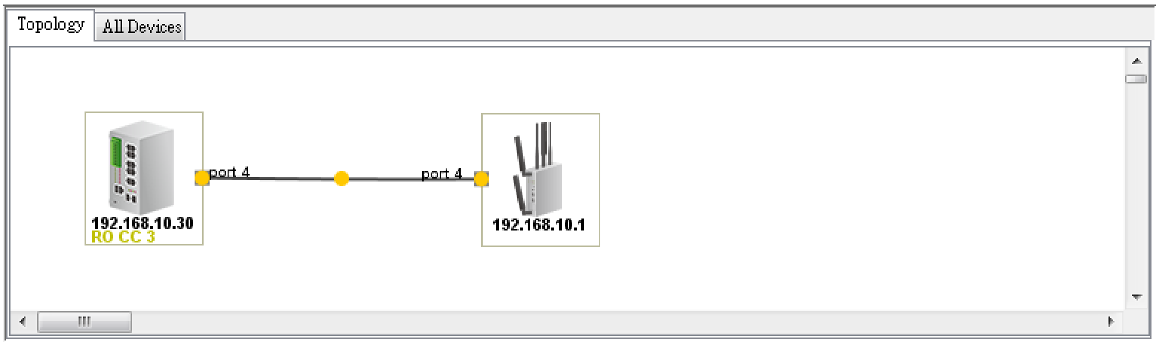
Action: Run Executable File

Recipient:

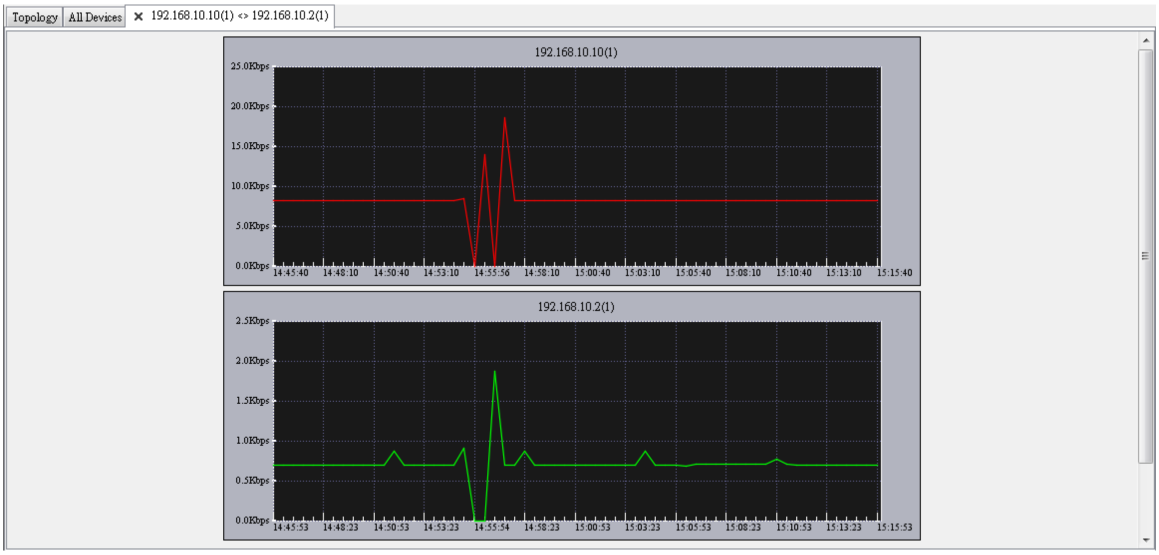
Executable File: D:\Installer\putty.exe

9. NETWORK PERFORMANCE MANAGEMENT

If user wants to monitor the traffic of user local network for a period of time, NetMaster can give user 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. The NetMaster can monitor and report selected connection statistics.



The tab name of the current traffic history will appear and shows two connected devices' IP address and port -- Port 1 on the device (192.168.10.10) connects to port 1 on the other device (192.168.10.2). 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.



To view the traffic report

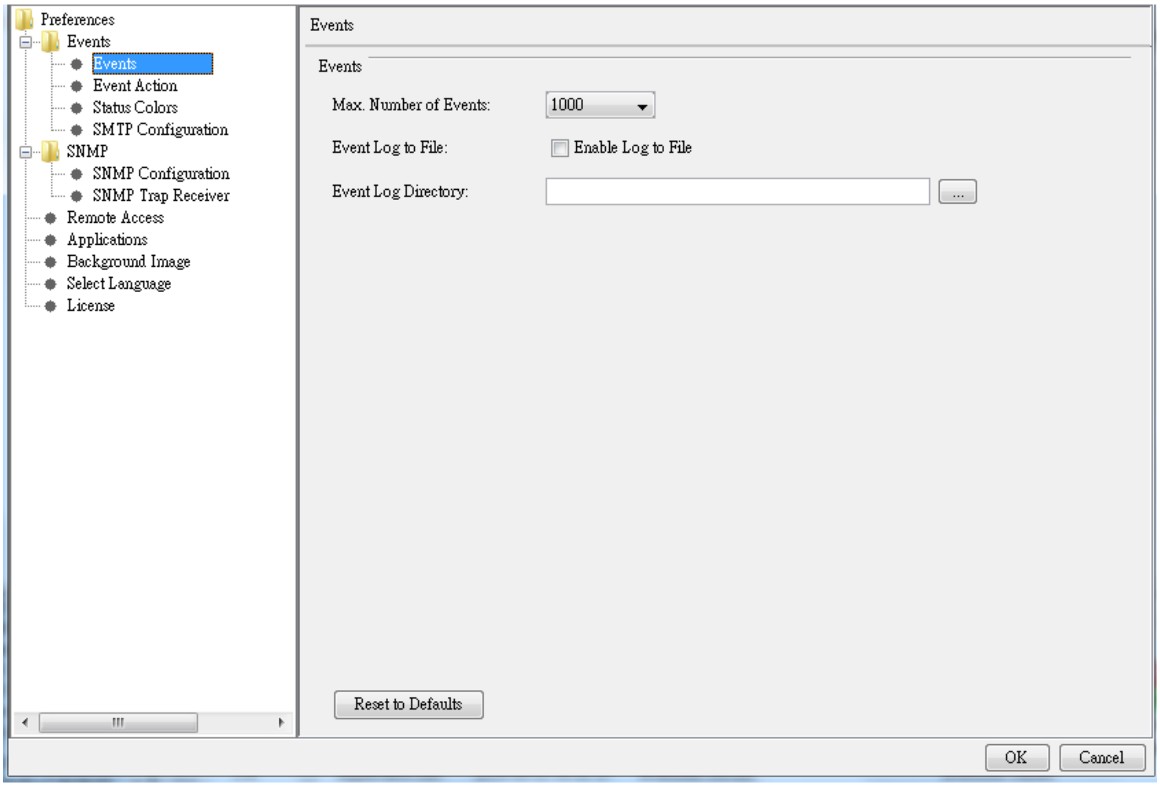
- Mouse **Double-Click** on the line between the two devices.
- The traffic report only available if the network connection is present.
- The traffic tab provides an indication of the network traffic for the connection.

10. PREFERENCES

10.1 EVENTS

10.1.1 EVENTS

This page allows user to record events into the log file. User can change maximum number of events, event log to file and event log directory.



Max. Number of Events: 1000

Event Log to File: □ Enable Log to File

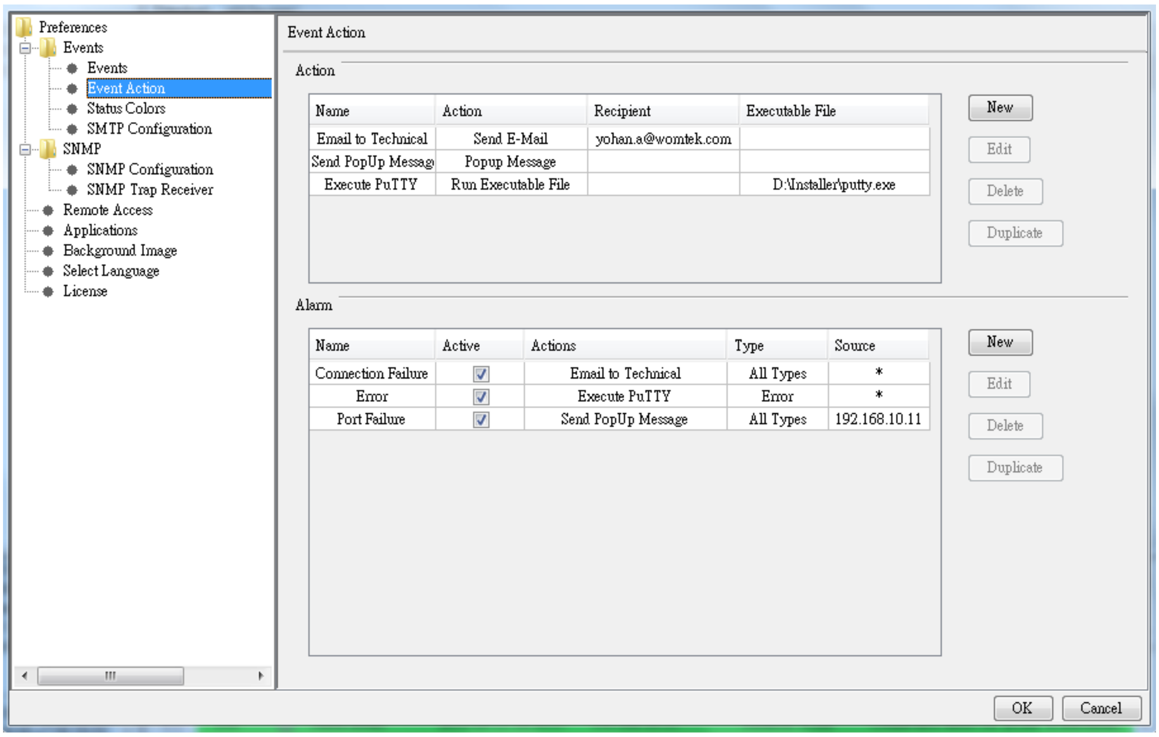
Event Log Directory:

Below is the Event interface description:

TERMS	DESCRIPTION
Max. Number of Events	**Default: 1000.** User can configure the max number of the Event list. The range is from 100 ~ 10000.
Event Log to File	By checking the box, It means the event log will be saved into a file. (.txt)
Event Log Directory	Choose the specific directory to save the event log file.

10.1.2 EVENT ACTION

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



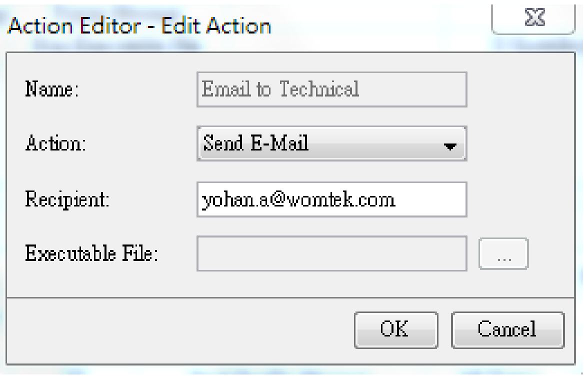
Action

Name	Action	Recipient	Executable File
Email to Technical	Send E-Mail	yohan.a@womtek.com	
Send PopUp Messag	Popup Message		
Execute PuTTY	Run Executable File		D:\Installer\putty.exe

Alarm

Name	Active	Actions	Type	Source
Connection Failure	☑	Email to Technical	All Types	*
Error	☑	Execute PuTTY	Error	*
Port Failure	☑	Send PopUp Message	All Types	192.168.10.11

If user clicks New, Edit, Delete or Duplicate button, the page will pop-up for configuring the Action and Alarm.



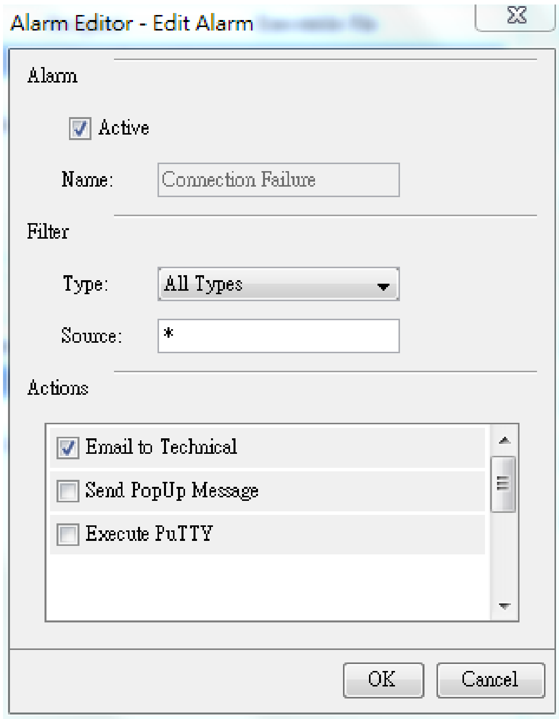
Name: Email to Technical

Action: Send E-Mail

Recipient: yohan.a@womtek.com

Executable File:

User can create any easy name for the action depends on the needs. In this Event action setting page, user can create less action and more alarms. User may assign one action to several alarms.



Alarm Editor - Edit Alarm

Alarm

☑ Active

Name: Connection Failure

Filter

Type: All Types

Source: *

Actions

☑ Email to Technical

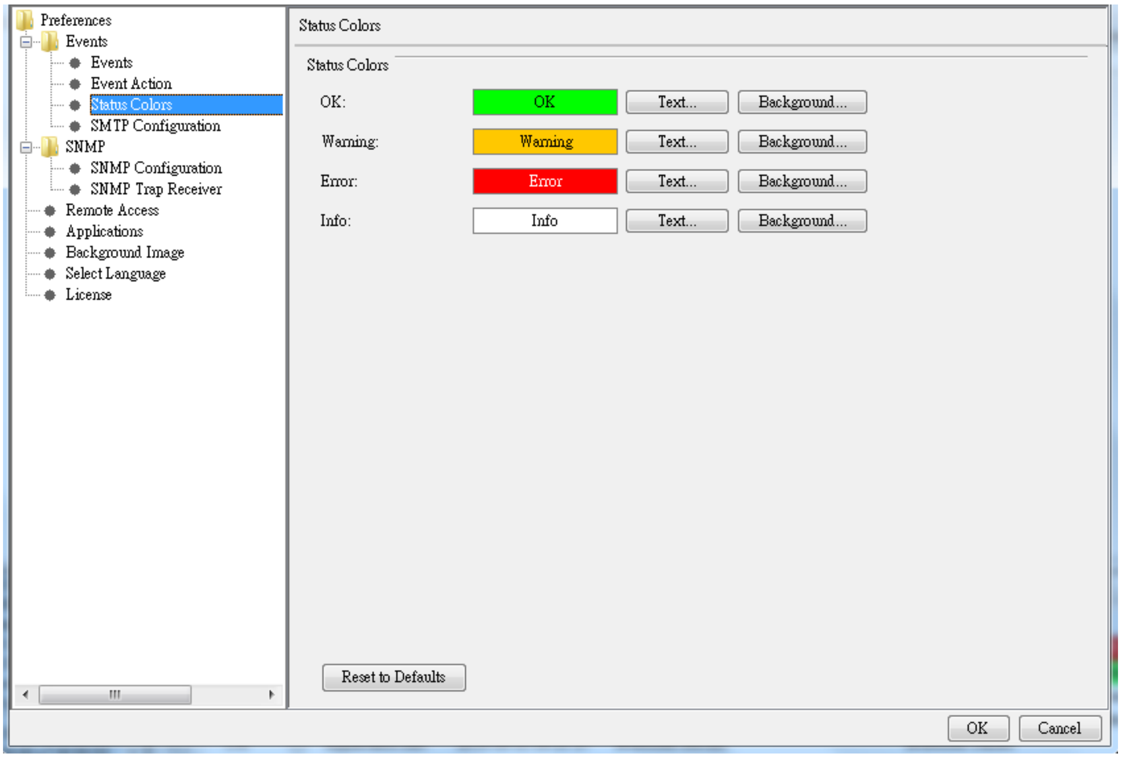
□ Send PopUp Message

□ Execute PuTTY

For this alarm editor page, user can create any kind of alarm and filter the alarm type whether it is about warning, error, OK status and info. And also user can set the source section; just by entering the keyword it can be assign to any kind of actions.

10.1.3 STATUS COLORS

This page allows user to assign a color to each status. User can change the text color and the background color of the 4 type status.



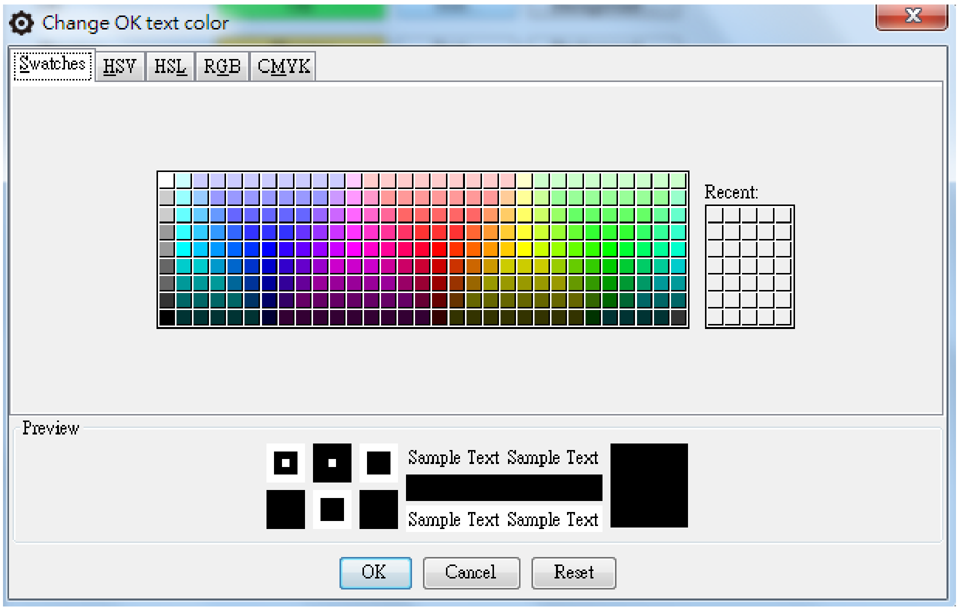
OK: OK Text... Background...

Warning: Warning Text... Background...

Error: Error Text... Background...

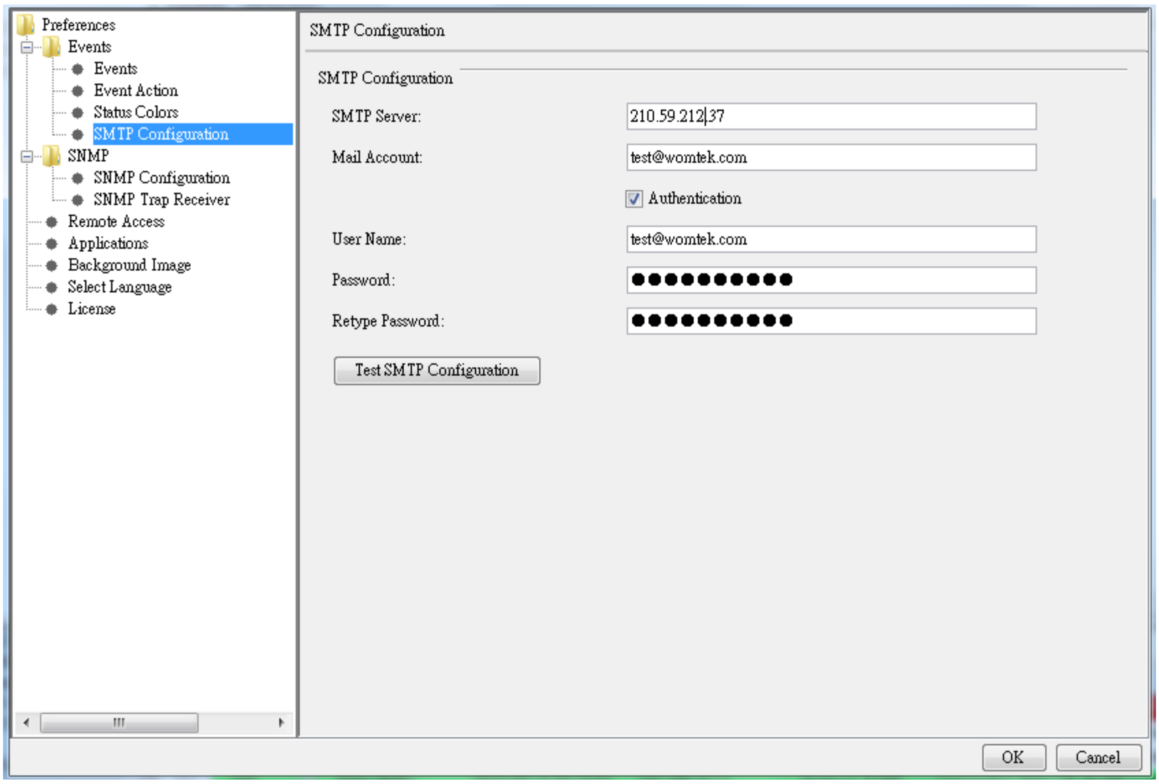
Info: Info Text... Background...

If user click the text or background button, a configuration page will pop-up.



10.1.4 SMTP CONFIGURATION

While user needs to send an Email for Event Action, user must configure SMTP Configuration. If the SMTP server requests to authorize first, user can set up the username and password in this page. And click **Test SMTP Configuration** to test the configuration.



SMTP Configuration

SMTP Server: 210.59.212.37

Mail Account: test@womtek.com

☑ Authentication

User Name: test@womtek.com

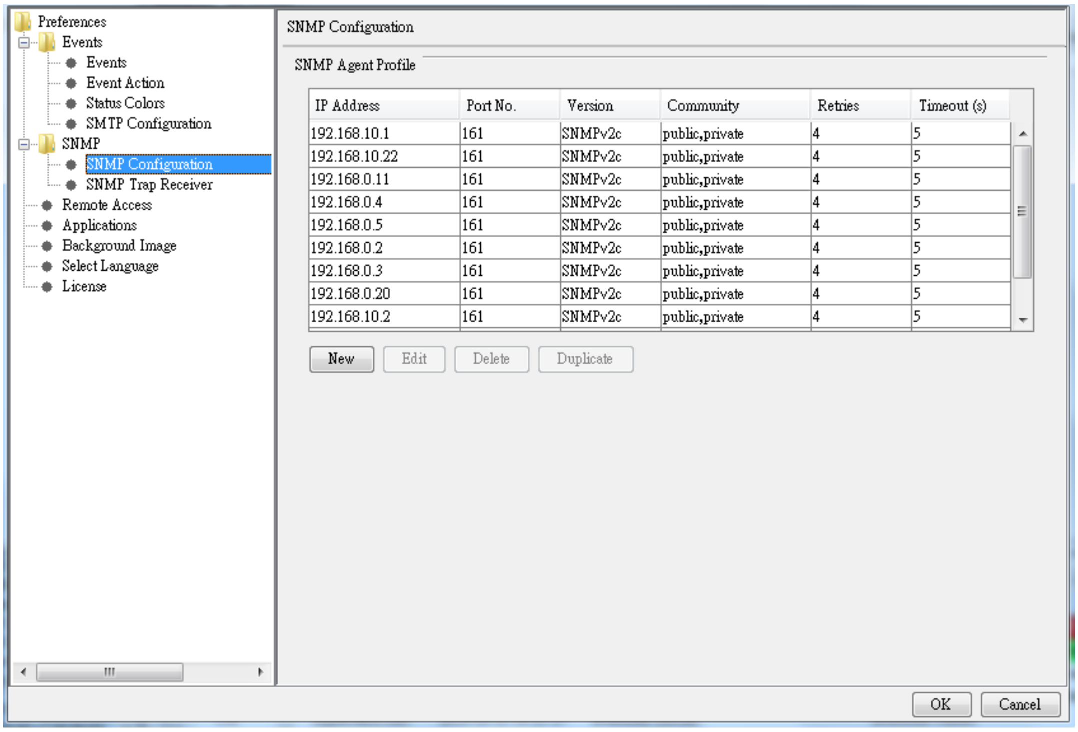
Password: ●●●●●●●●●●●

Retype Password: ●●●●●●●●●●●

10.2 SNMP

10.2.1 SNMP CONFIGURATION

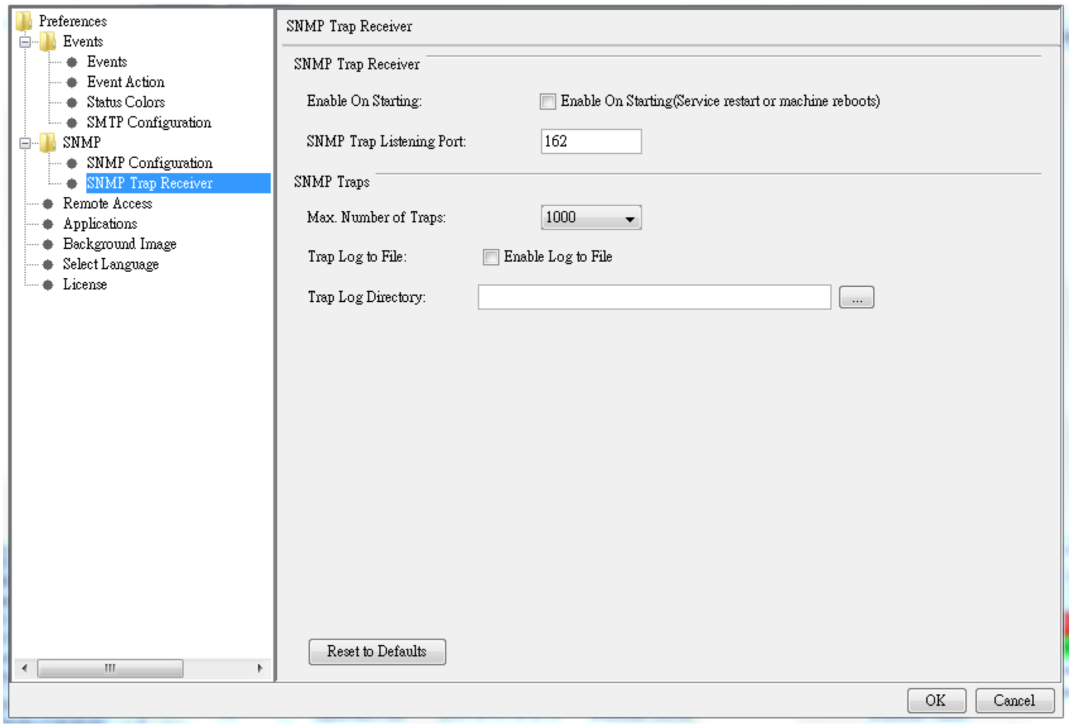
The NetMaster will add a default SNMP agent profile for discovered devices. User can use this page to create a new SNMP Agent Profile, edit, delete or duplicate a profile. The configurations of profile include agent listening port (default is 161), SNMP version (support v1/v2c/v3), read/write community,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



IP Address	Port No.	Version	Community	Retries	Timeout (s)
192.168.10.1	161	SNMPv2c	public,private	4	5
192.168.10.22	161	SNMPv2c	public,private	4	5
192.168.0.11	161	SNMPv2c	public,private	4	5
192.168.0.4	161	SNMPv2c	public,private	4	5
192.168.0.5	161	SNMPv2c	public,private	4	5
192.168.0.2	161	SNMPv2c	public,private	4	5
192.168.0.3	161	SNMPv2c	public,private	4	5
192.168.0.20	161	SNMPv2c	public,private	4	5
192.168.10.2	161	SNMPv2c	public,private	4	5

10.2.2 SNMP TRAP RECEIVER

In this page user can configure the SNMP Trap Receiver and record SNMP Trap into the log file. User can enable the SNMP Trap Receiver when the system starting by checking the box and it will restart the system and reboot the device machine, change listening port (the default value is 162), change maximum number of traps (Range value is between 100 – 10000), trap log to file and trap log directory.



SNMP Trap Receiver

SNMP Trap Receiver

Enable On Starting: □ Enable On Starting(Service restart or machine reboots)

SNMP Trap Listening Port: 162

SNMP Traps

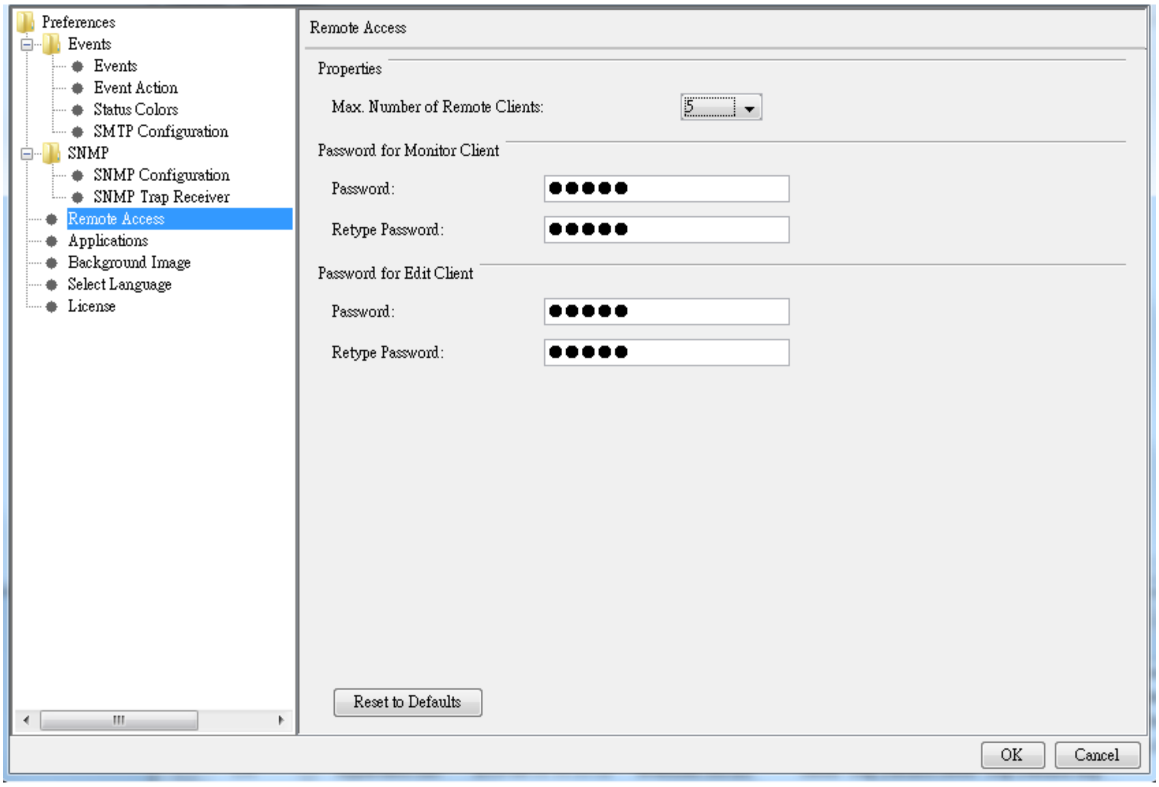
Max. Number of Traps: 1000

Trap Log to File: □ Enable Log to File

Trap Log Directory: ...

10.3 REMOTE ACCESS

Due the access synchronization, only one client can access the Edit Mode and the other clients on the Monitor Mode. On the Edit Mode, client can use all of the functions and on the Monitor Mode client is only allowed to see the topology. The default password to enter the Edit Mode and Monitor Mode is admin. In this Remote Access page, user may change the password for the Edit Mode and the Monitor Mode. The maximum number of remote client is 5 clients.



Remote Access

Properties

Max. Number of Remote Clients: 5

Password for Monitor Client

Password: ●●●●●

Retype Password: ●●●●●

Password for Edit Client

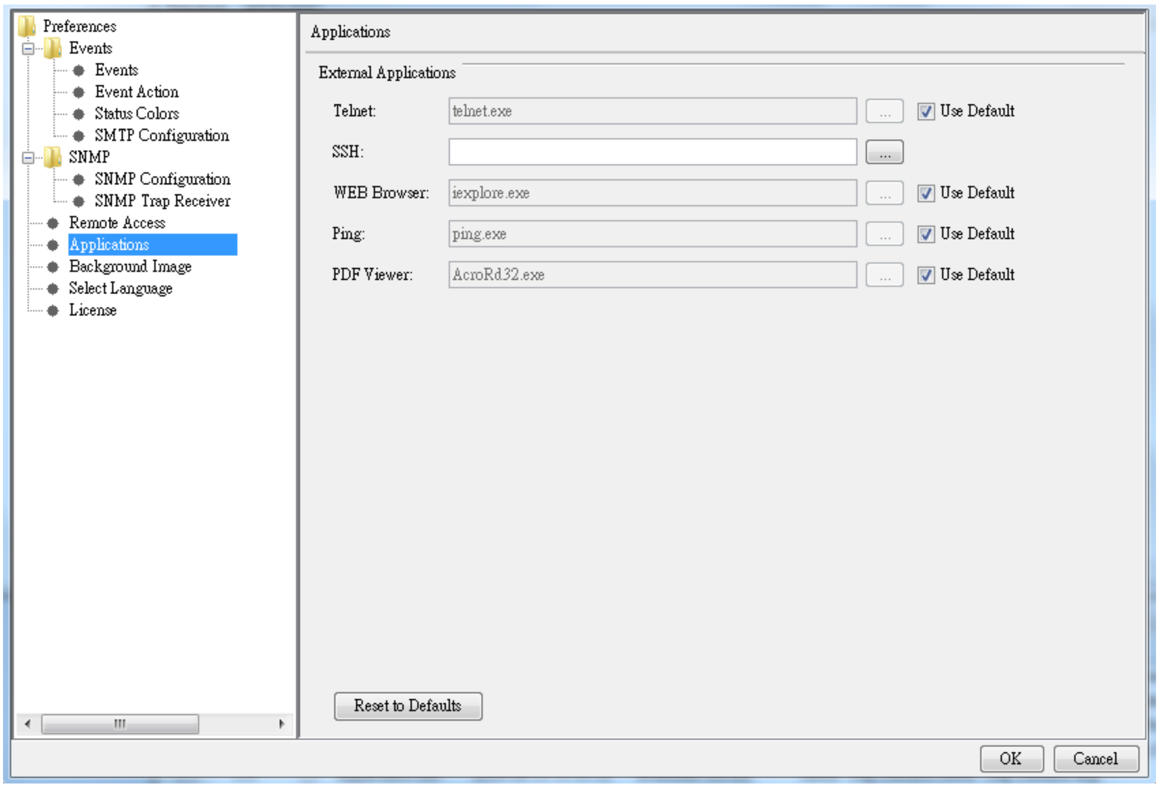
Password: ●●●●●

Retype Password: ●●●●●

***Please change the username and password due to the security consideration.**

10.4 EXTERNAL APPLICATION

NetMaster allows user to use external applications to run the functions. This page allows user to assign specified programs or use default application to run the functions. It supports Telnet, SSH, Web Browser, Ping and PDF Viewer.



Applications

External Applications

Telnet: telnet.exe ... ☑ Use Default

SSH: ...

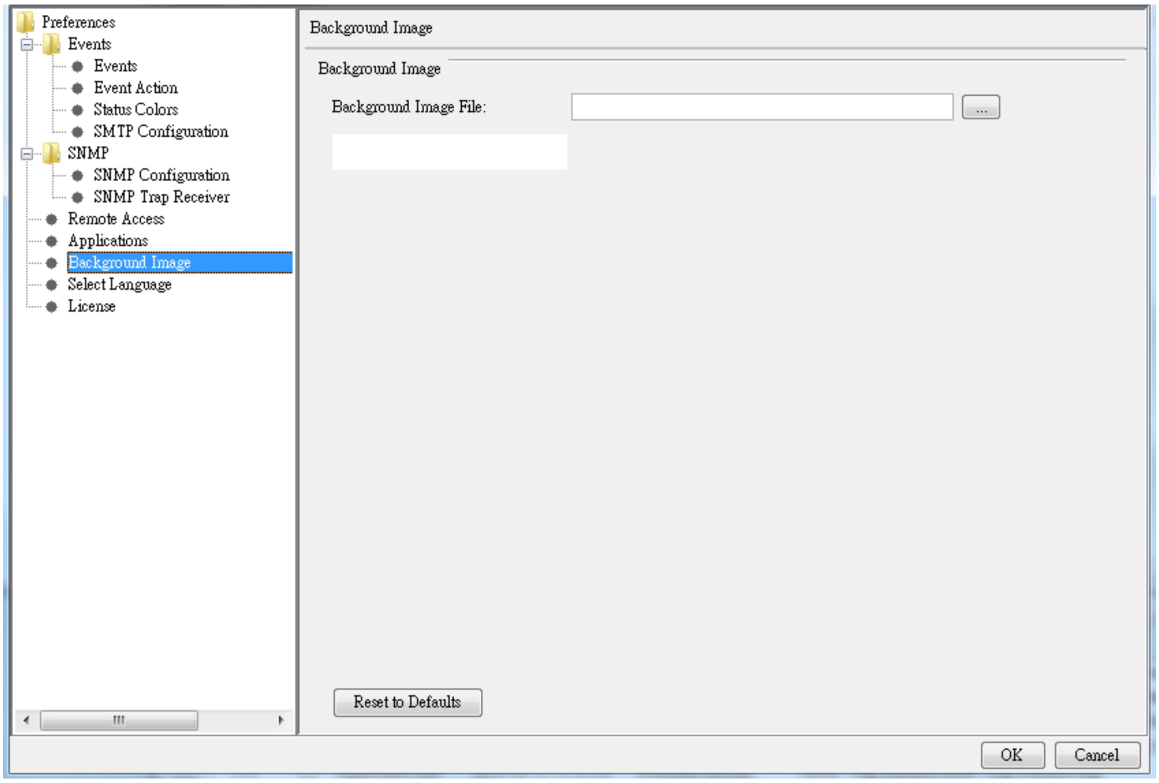
WEB Browser: iexplore.exe ... ☑ Use Default

Ping: ping.exe ... ☑ Use Default

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

10.5 BACKGROUND IMAGE

This page allows user to change the background image of the topology dashboard. User can select an image file to change the default background image.



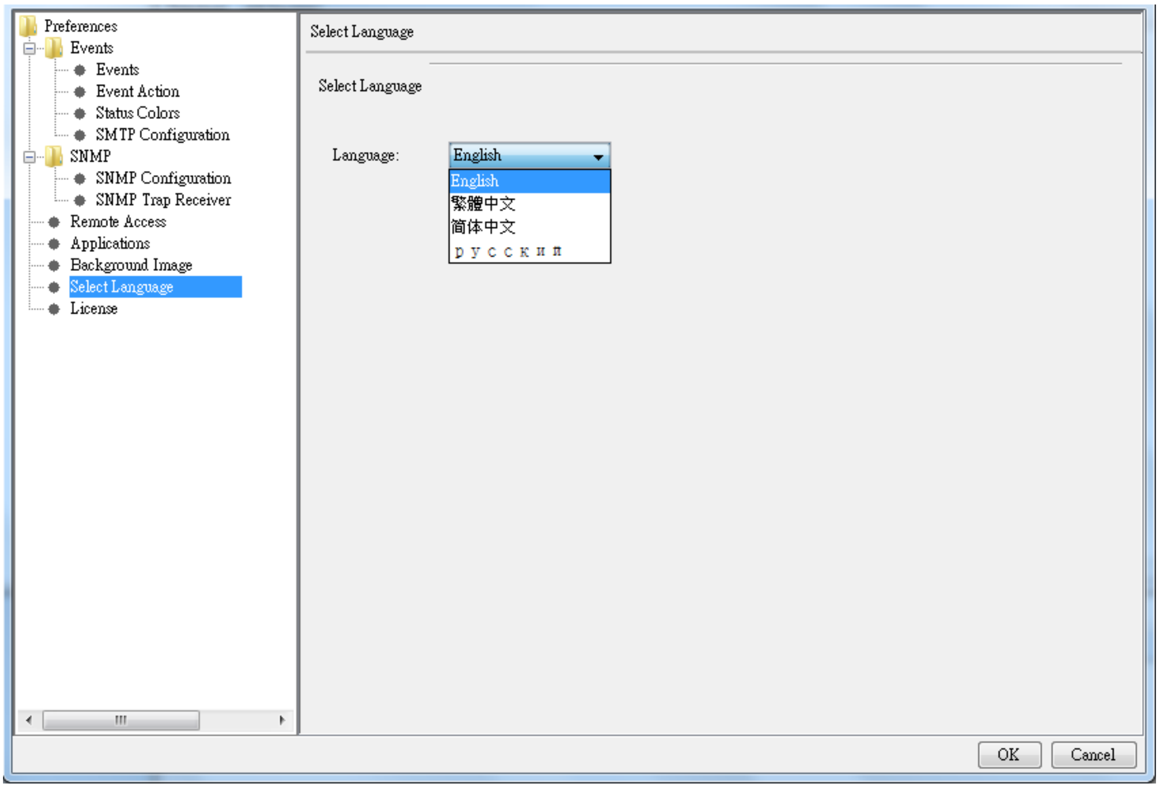
User may change back the background image by clicking **Reset to Defaults** button.

10.6 LANGUAGE

NetMaster is supported with 4 language interfaces English, Traditional Chinese, Simplified Chinese and Russian.

User can change NetMaster display interface by selecting a language option. Click OK then Language will be applied immediately.

Note: If the event log was logged with other language rather than currently selected language, it is possible fail to display the log correctly



Language: English

10.7 LICENSE

Please follow the instruction to enter the NetMaster License.

Basically WoMaster has two kinds of license:

a. License with MAC Address bundle.

For this license, user needs to include the hardware MAC Address when requesting the license to WoMaster. So this license only can be applied to the device with the registered MAC Address, cannot be applied to other device.

b. License without MAC Address bundle.

For this license, user doesn't include the MAC Address when requesting the license to WoMaster. After user receives the license and registers it, the MAC Address will automatically generate **FF:FF:FF:FF:FF:FF** as default.

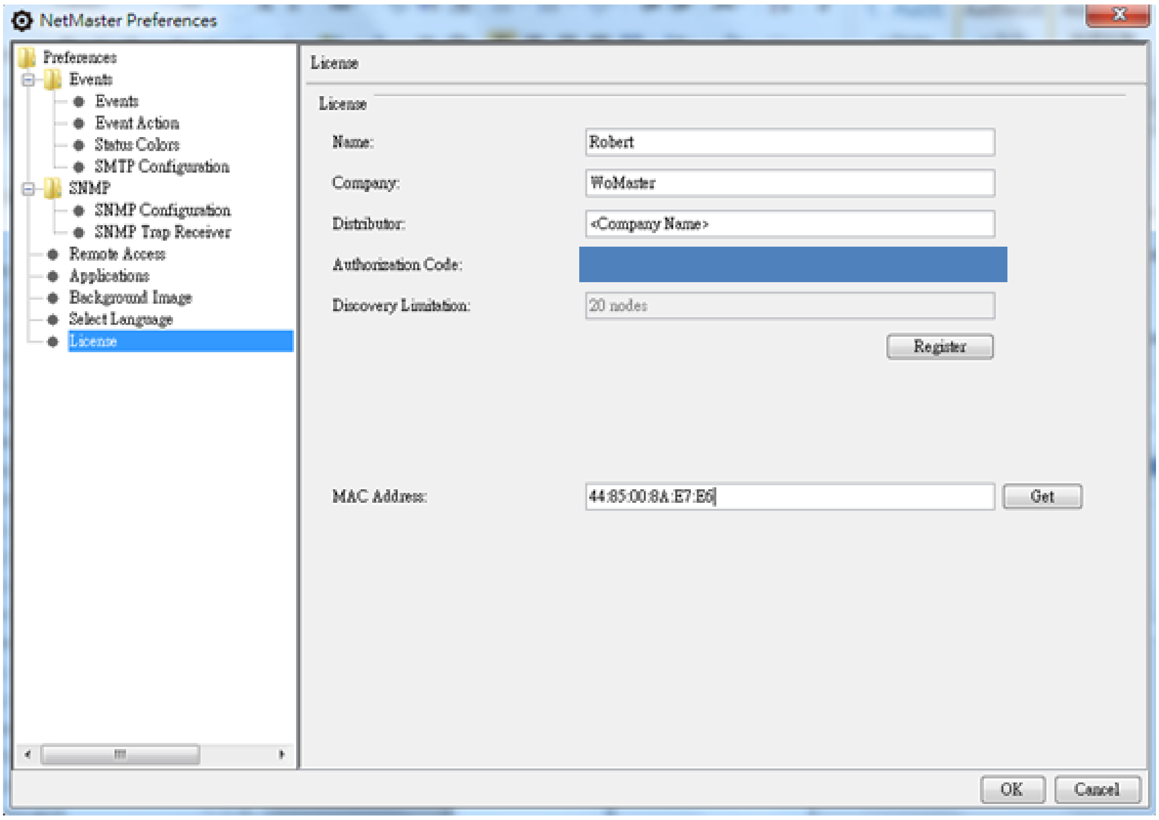
1. Download and install the latest NetMaster from WoMaster website.

   (https://www.womaster.eu/download.php)

2. After receiving the E-mail letter from WoMaster, go to NetMaster -> Preferences -> License.

3. Fill out Name, Company, Distributor, and Authorization Code base on the content of E-mail letter. And then

   click Register button.



License

Name: Robert

Company: WoMaster

Distributor: <Company Name>

Authorization Code: [redacted]

Discovery Limitation: 20 nodes

MAC Address: 44:85:00:8A:E7:E6

4. Click Get to get the PC MAC Address.

5. Finally, click OK to apply the license.

11. REVISION HISTORY

Version	Description	Date	Editor
V1.0	Released	18/09/2018	Yohan
V1.1	Add ERPS Group Setup VLAN License	18/01/2019	Yohan
V1.2	Add limitation for language	15/05/2019	Kylie