Network Management System

EnGenius NMS Tools

User Manual

Revision History

Version	Date	Notes
1.0.0	11/2/2009	Initial Version

Table of Content

Table of Content 2
1 System Requirement 4
2 Installation and Un-installation of EnGenius Mesh NMS Tools 5
2.1 Installation for Window (XP, ME, etc) 5
2.1.1 Introduction 5
2.1.2 Step 2: Choose Install Folder 6
2.1.3 Step 3: Choose Shortcut Folder 6
2.1.4 Step 4: Pre-Installation Summary 7
2.1.5 Step 5: Installing 7
2.1.6 Step 6: Install Complete 8
3 Un-installation For Windows (XP, Me, etc) 9
3.1 Step 1: Introduction 9
3.2 Step 2: Uninstalling 10
3.3 Step 3: Uninstall Complete 10
4 How to Use EnGenius Mesh Network Management Tools 11
4.1 Quick Start 11
4.2 Software Overview & Features 12
4.2.1 Software Layout 12
4.2.2 Map Container 12
4.2.3 MIB Reader 13
4.2.4 Alarm Viewer 14
4.2.5 Toolbar Reference 15
4.3 Features 17
4.3.1 Create Map 17
4.3.2 Open Map 18
4.3.3 Save Map 19
4.3.4 Topology Map 20
4.3.5 Set up New Scan 23
4.3.6 Map View 23
4.3.7 Status Pane 25
4.3.8 Scan IP Address 26
4.3.9 SNMP Community / Passwords (for Scan-IP) 27
4.3.10 Socket Port 28
4.3.11 SNMP Community / Passwords (for AP Unit) 29

4.3.12 Scan Interval....30
4.3.13 Import Background Image....31
4.3.14 Map Print....31
4.3.15 Map Zoom....32
4.3.16 Node Label....34
4.3.17 Customize Map....35
4.3.18 Background Image Transparency....38
4.3.19 Block List....39
4.3.20 Lock / Unlock....40
4.3.21 Node details....41
4.3.22 Client Properties....43
4.3.23 EZ Map Settings....45
4.3.24 Show Live Stat (EZ Map)....49
4.3.25 Get/Set using MIB Reader....50
4.3.26 Load/Unload MIB....51
4.3.27 Alarm Table....52
4.3.28 Add Trap Agent....54
4.3.29 View Log Files....56
4.3.30 Show Route....57
4.3.31 Create VPN Connection (Layer-3 Map)....59
4.3.32 Configure Mesh Aps....64
4.3.33 Discovery Tool....65
4.3.34 View Interface and Client Live Statistic....65
4.3.35 Logout Client....67
4.3.36 Performance Analysis....69
4.3.37 Setting NMS Addresses....72
4.3.38 Synchronized-Configuration....74

1 System Requirement

EnGenius Mesh Network Management Tools is written in JAVA, hence it has the feature of cross platform, capable to run in most of the platform. The following are the recommended system requirement.

- 256 MB (recommended minimum)
- > 512 MB (recommended)
- 10 MB hard disk space (without-JVM version)
- 80 MB hard disk space (with-JVM version)
- Microsoft Windows 2000, XP (recommended) or Linux RedHat 3

Besides, in order to enable the NMS to work properly, the following ports must be allowed through any firewall between the NMS and the agent:

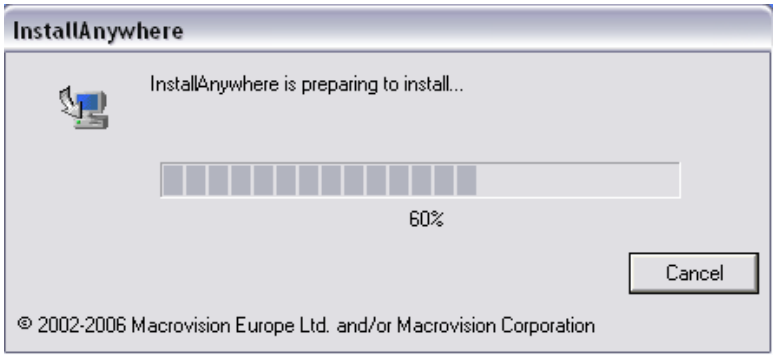
- Port 161 (by default) – Use for standard SNMP Get and Set
- Port 162 (by default) – Use for listen to SNMP Trap
- Port 4608 (by default) – Used by the Discovery Tool
- Port 8188 (by default) – Use to listen for the Layer-2 node's notification

For Linux terminal users, the Java Virtual Machine (JVM) is not included in the installer. Therefore you may need to download a Java Runtime Environment (JRE) or JVM before you install and run the NMS on your system. The minimum version of the Java is 1.6.

2 Installation and Un-installation of EnGenius Mesh NMS Tools

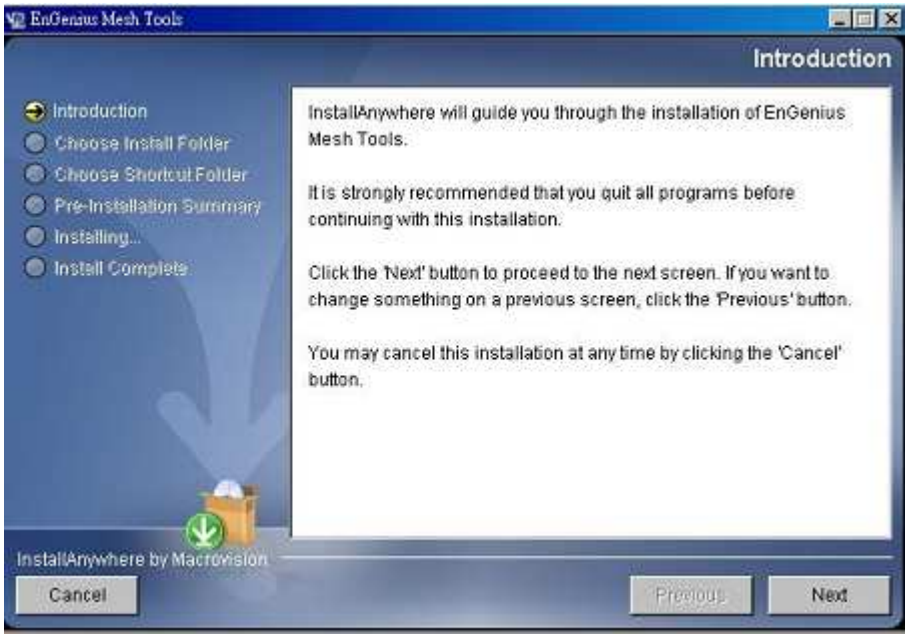
2.1 Installation for Window (XP, ME, etc)

Obtain the executable installation file, *EnGenius Mesh Tools v2.8.11e*, from the companion CD or any other resources, and copy it to the terminal's desktop. Launch the installation wizard by double-click the file



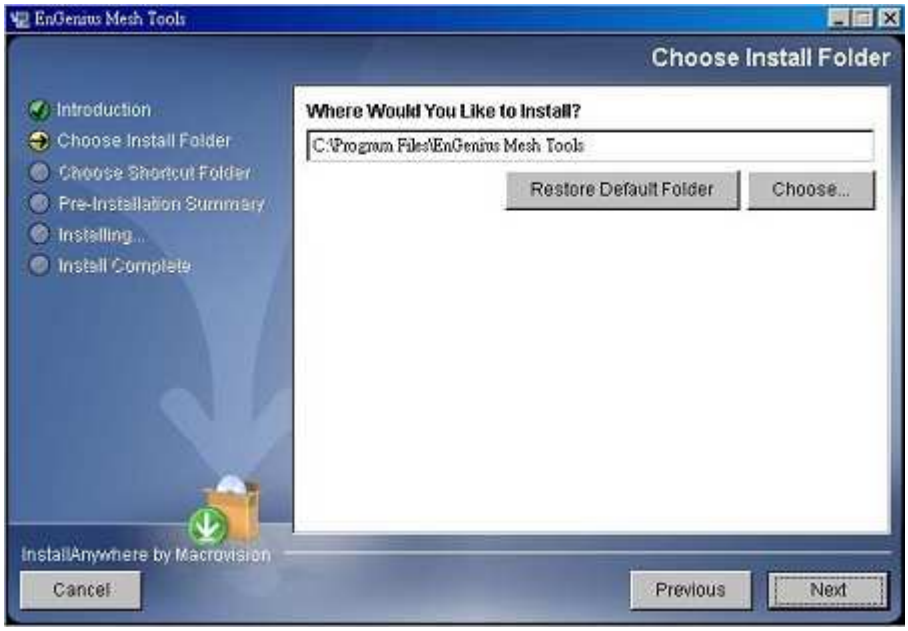
After the wizard is setup completely, follow the 6 easy steps directed by the wizard to perform the installation.

2.1.1 Introduction



Simply explain what this software is about. Press **Next** to proceed.

2.1.2 Step 2: Choose Install Folder

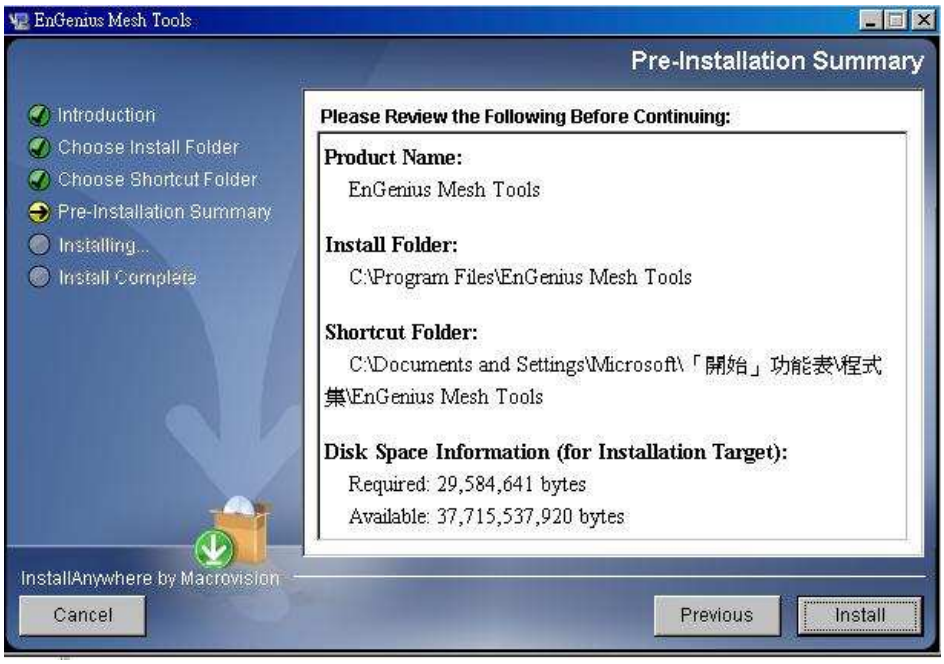


Prompt user to choose the install path (directory) and name the install folder. Press **Next** to proceed.

2.1.3 Step 3: Choose Shortcut Folder

Specify where the software shortcut will be created at. Press **Next** to proceed.

2.1.4 Step 4: Pre-Installation Summary



Let user have a quick review about the installation settings before start installing.

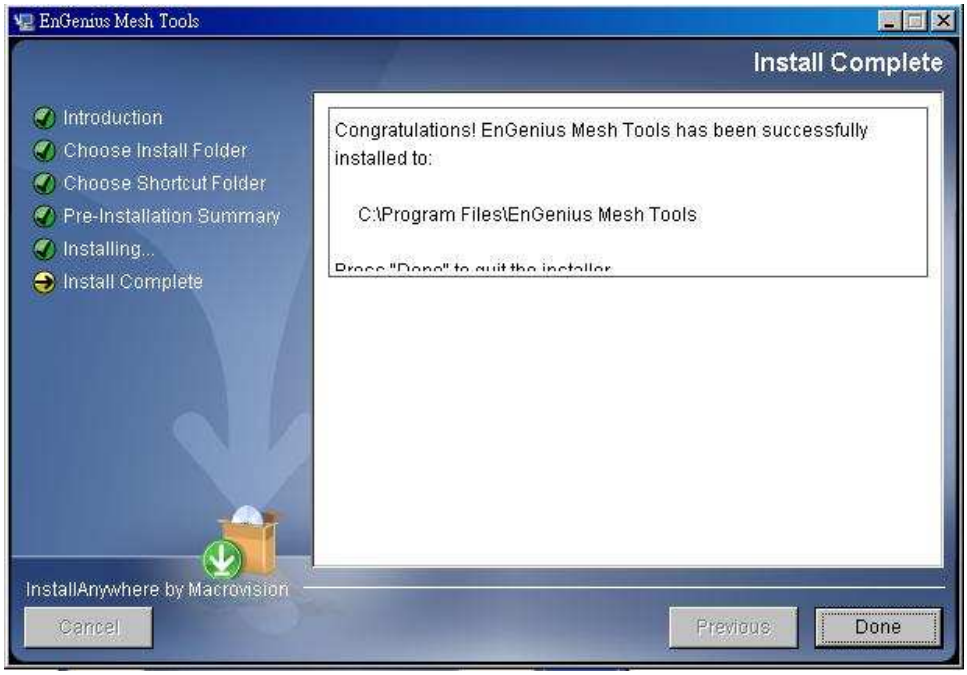
Press **Install** button to start the installation.

2.1.5 Step 5: Installing

Installation is in progress. Once the installation is completed it will direct the user

to the next step.

2.1.6 Step 6: Install Complete

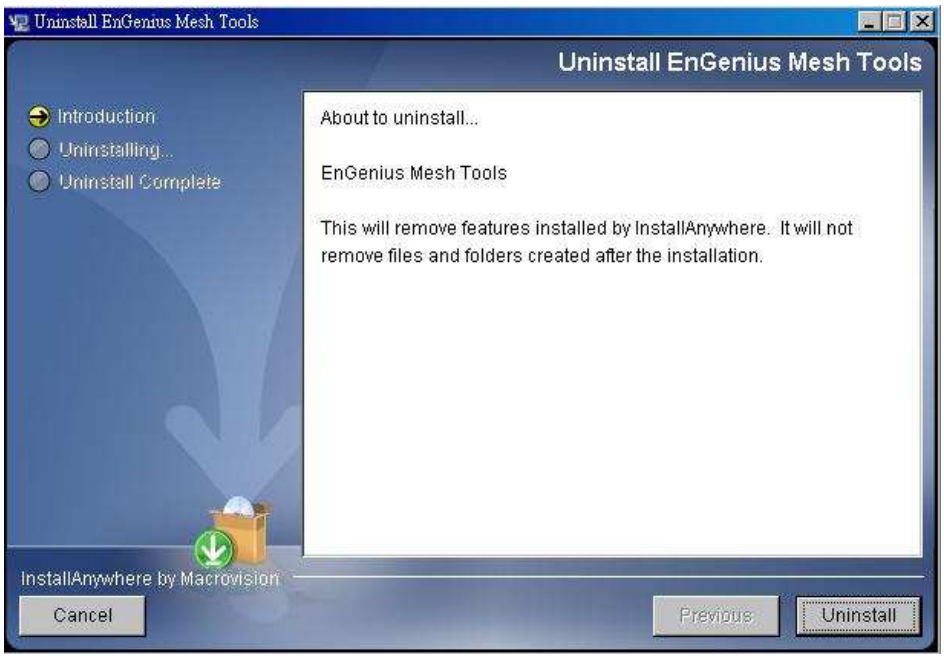


Indicating the installation is completed, and user can select to restart the system instantly or afterward, in order to complete the installation. Press **Done** to conclude the installation. After that, you may launch the NMS through the shortcut you created previously.

3 Un-installation For Windows (XP, Me, etc)

In order to uninstall the *EnGenius Mesh Network Management Tools* from your terminal, you can get the uninstaller wizard from the software directory. The uninstaller, namely *Uninstall EnGenius Mesh Tools*, is located at the *Uninstall EnGenius Mesh Tools* folder. Launch the uninstaller wizard by double-click the executable file. Follows the following steps:

3.1 Step 1: Introduction



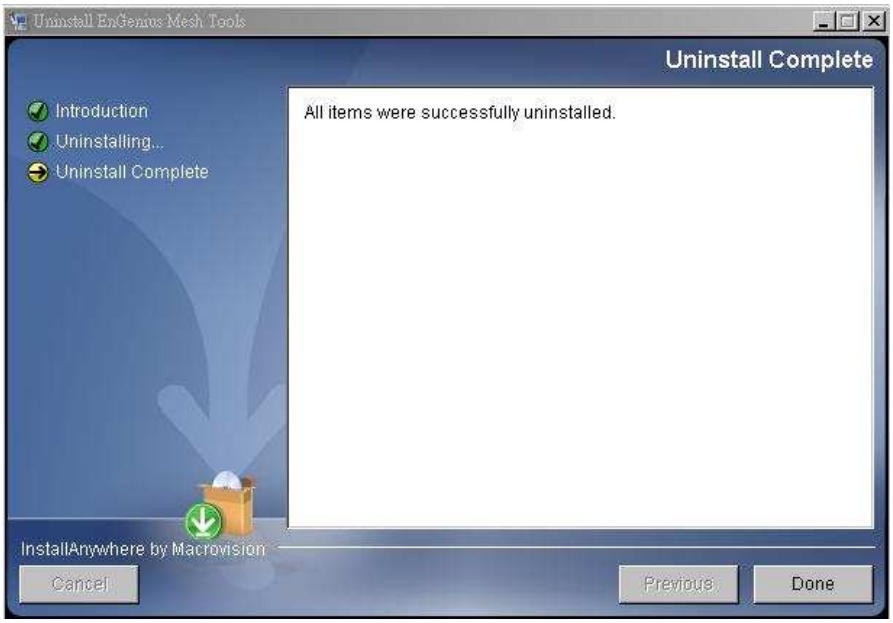
An introduction regarding the uninstallation of the *EnGenius Mesh Management Tool.*

Click **Uninstall** to start the process.

3.2 Step 2: Uninstalling

Uninstallation is in the progress. Once the progress is completed, it will automatically direct you to the next step.

3.3 Step 3: Uninstall Complete



The software is uninstalled. You may choose to restart the terminal instantly or afterward in order to complete the process.

4 How to Use EnGenius Mesh Network Management Tools

4.1 Quick Start

First of all, make sure the terminal where you installed your *EnGenius Mesh Network Management Tools* is connected to the network, via Wireless or Wired LAN. Then, launch the NMS at the location where you install it.

Click the **Create Map** button on the toolbar to generate a new map profile. A dialog box would appear to prompt user to enter the name of the new profile. After that, hit the **OK** button to complete the set up. A new map will be inserted into the NMS.

Then, click on the drop-down list on the toolbar of the new profile, where it prompts users to insert the Scan IP Address, the destination IP Address to be scanned. Enter the desired IP and click the button next to the list to save the IP. Finally, select the **Start Scan** button on the map's toolbar, the scan will be initiated and run. The result of the scan will be plotted on the map area. User is free to adjust the position of the found-unit on the map.

Before shutting down the NMS, user can save the profile settings, including the coordinate of the found Mesh AP units on the map, by click on the **Save Map** button on the map toolbar. The saved profile can be loaded directly to the NMS next time using the **Open Map** button on the toolbar.

For further description regarding the functions and features of the *EnGenius Mesh*

Network Management Tools, user may refer to the following section.

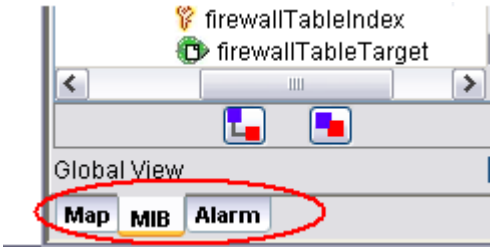
4.2 Software Overview & Features

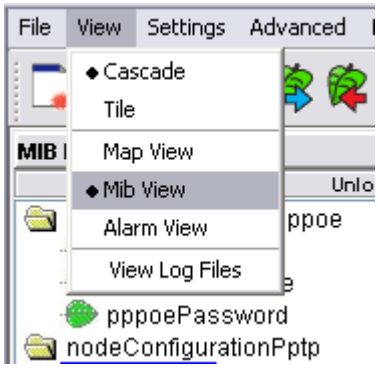
4.2.1 Software Layout

Before we proceed further, let us have an overview at the layout of the NMS. Basically, the *EnGenius Mesh Network Management Tools* is consists of three major sections:

- Map Container
- MIB Reader
- Alarm Viewer

User can switch the view of the NMS by select the tabs at the left bottom corner, or through the menu bar, as illustrated:





4.2.2 Map Container

The *Map Container* is the section where user can monitor and manage the mesh network. The network will be displayed in the form of graphical topology map, and the status will be updated periodically.

The center frame of the *Map Container* is the space to plot the topology map. More

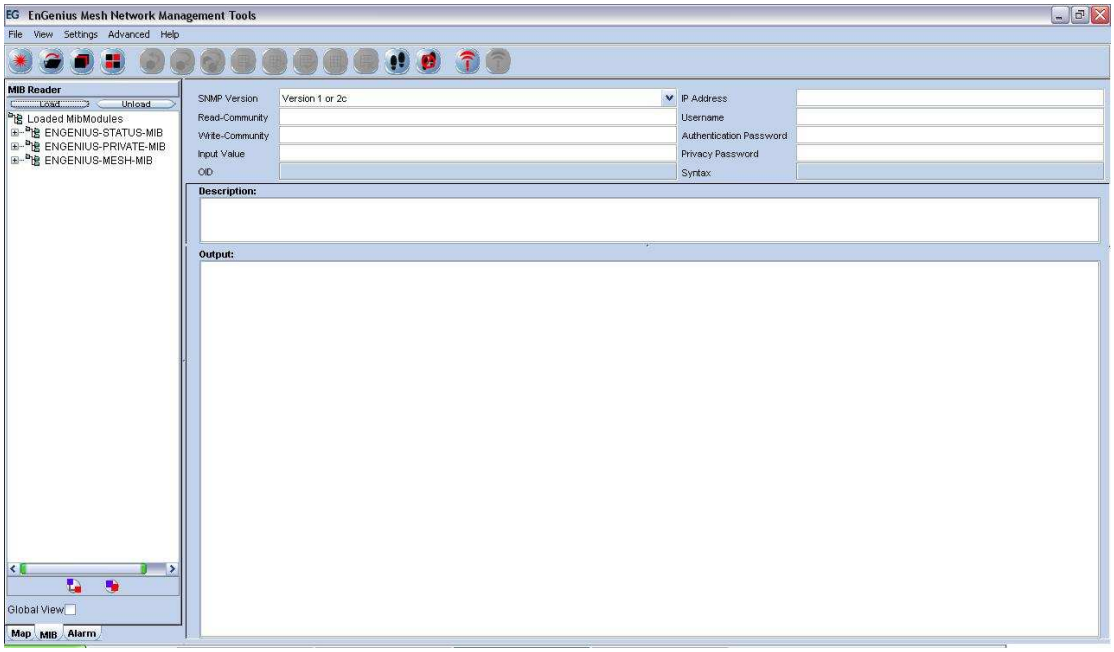
than one map can be created and run simultaneously. The status of the map will be logged to the status pane at the bottom of the map. Each topology map has its own status pane.

The panel at the west of the map space is the *Node Details* panel. It is used to display the properties of the selected Mesh AP unit on the topology map. The information of the AP will be loaded into the table, and the graph below the table shows the signal strength between the selected AP with its neighbor APs. The column at the bottom of this panel is used to invoke the live stat monitoring feature.

The east panel, meanwhile, is to display the details of the clients associated to the Mesh AP unit. The panel is divided into two parts, the *Client Properties* and *Client Signal Strength* portion. Each portion will be automatically updated every minute, to provide the admin user the live result regarding the clients.

4.2.3 MIB Reader

The *MIB Reader* provides user a simple user-interface to retrieve as well as configure the settings of the Mesh AP unit through the standard or vendor proprietary MIB files. With the correct community and password, user can perform the SNMP actions such as SNMPGet, SNMPSet and SNMPTable.



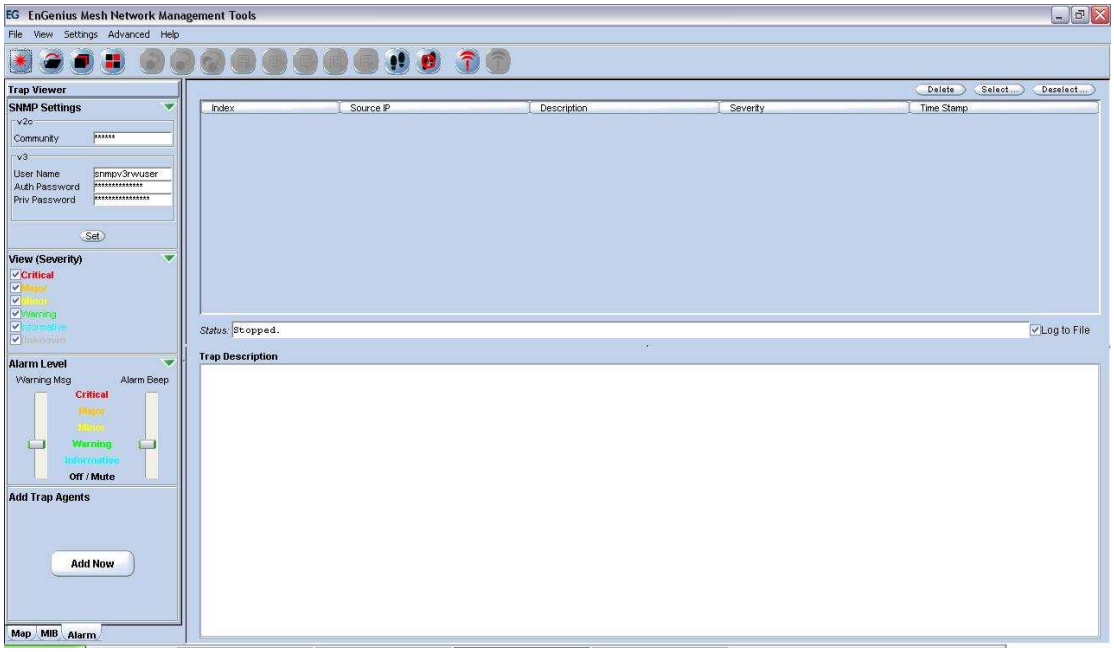
The west pane displays the list of MIB and its tree. User can load and unload MIB file from the desired location. More than one file can be loaded into the *MIB Reader*. In order to read or set an item, expand the MIB tree, select the desired node. Select the SNMP version; fill in the IP Address and other necessary keyword. Then click on the command button (**SnmpGet, SnmpSet, SnmpWalk, Load Table,** etc..) on the toolbar. The output will be shown on the *Output* column.

4.2.4 Alarm Viewer

The *Alarm Viewer* is a SNMP trap server. It received the SNMP alarms and notifications directed by the Mesh AP units and display in the table at the center frame. Select the table entry in order to view the description of the trap.

Note that the table is a read-only table, which displays the trap's source IP Address, description, severity and the time when the trap or alarm was caught. These alarms should be deleted once they were reviewed and resolved, by clicking the **Delete**

button.



4.2.5 Toolbar Reference

This section provides a quick reference for the buttons in the toolbar of the NMS. The description of the toolbar of the NMS is illustrated at the table below:

Button	*Name*	*Function*
	Create Map	Create a new topology map profile
	Open Map	Open a pre-saved topology map profile
	View Tile	View the topology map in grid layout
	View Cascade	View the topology map in cascade layout
	SnmpGet	SnmpGet the data from MIB tree
	SnmpSet	SnmpSet the data from MIB tree

	Synchronized-Configuration	Invoke Synchronized-Configuration window
	Load Table	Load the SNMP table from MIB tree
	Refresh Table	Refresh the SNMP table from MIB tree
	Add Table Row	Add a row to SNMP Table
	Commit Table Change	Commit the selected table row with the edited data
	Del Table Row	Delete a row from SNMP Table
	SnmpWalk	Walk the selected item from the MIB tree
	Start Trap	Initiate the Alarm Host system
	Stop Trap	Stop the Alarm Host system

On the other hand, the following table shows the description of the toolbar of the map container:

Button	*Name*	*Function*
	Import Background	Import an image file to use as the background image of the topology map
	Save Profile	Save the current topology map
	Scan Start	Start the network scanning (Layer-3 & EZ Map only)
	Scan Stop	Stop the network scanning (Layer-3 & EZ Map only)
	Initiate Port	Open port to listen to Layer-2 notification (Layer-2 Map only)
	Close Port	Close Layer-2 notification port (Layer-2 Map only)

	Zoom In	Zoom in the topology map by 25%
	Zoom Out	Zoom out the topology map by 25%
	Zoom Fit	Zoom the topology map to a size that fit the screen
	Lock	Lock the AP units on the map
	Unlock	Unlock the AP units on the map
	Block List	Open the block list window
	Live Stat	Run the live statistic window to monitor the updated statistic of the desired node. (EZ Map only)

4.3 Features

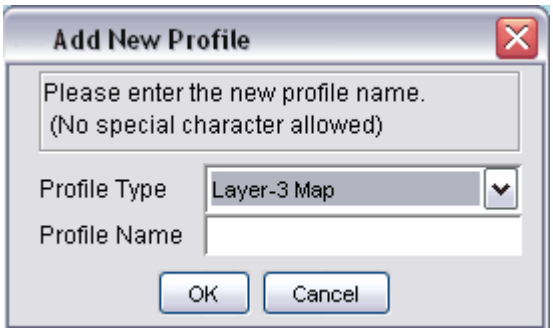
4.3.1 Create Map

In the latest version of NMS, three topology maps are available: Layer-3 Map, Layer-2 Map and EZ Map. These types of map look similar. The main difference between them is the method to read the topology information.

- The **Layer-3 Map** is the ordinary type, where it uses the provided target IP Address and SNMP protocol to collect the topology from the nodes discovered, and then plot the map using the collaborate data.
- Whereas the **Layer-2 Map** opens a specific port to listen for the notification from the nodes, in order to plot the map. Prior to this, user is required to add the information of the NMS (IP Address) to the node. Thus in fact, the Layer-2 Map can receive the notification not only from the layer-2 mode AP, but any other mode as well, as long as the NMS Address table is set.
- The **EZ Map**, on the other hand, broadcast the SNMP packet over the network to search for the SNMP-enabled devices. In the latest release, the discovery

tool scanning mode has been added into EZ Map as an alternative method to perform the node discovering.

In order to create a new Topology map profile, user can click on the **Create New** button on the main toolbar, or select *File > Create New* from the menu bar. A window would turn out to prompt user for the type and name of the new map. User may select the type of the profile from the drop down list, and enter the name in the provided column.



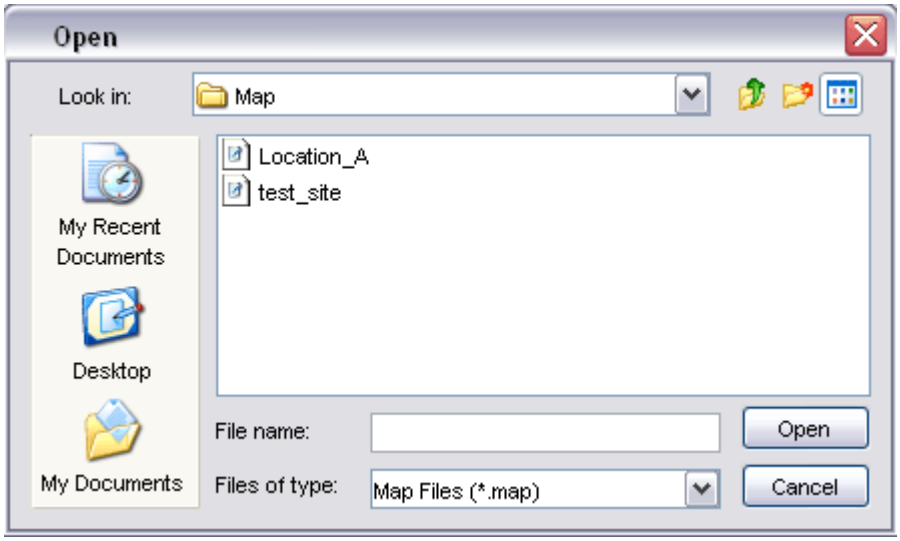
Please be aware that special character such as #, $, % (except _), are not allowed to use as the name of the topology map name to avoid data corruption, since the name of the map will be used as the header of their data file. On the other hand, the system also not allow user to create a new profile with the name of the existing map in the NMS.

Hit the **OK** button to proceed, or **Cancel** to close the window.

4.3.2 Open Map

In stead of create a brand new topology map, user can re-open the map profile that has been saved previously. Click the **Open Map** button, or select *File > Open Map* from menu bar, a file chooser window would appear on the screen, to prompt user to choose a map. Select the desired one, and hit the **Open** button. The profile will be

loaded to the NMS with all its settings.



4.3.3 Save Map

As mentioned previously, the settings of the map profile can be saved to be loaded in the future. Details of the map, for instance, the coordinate and SNMP passwords of the Mesh AP units on the map, background image and block list, will be saved as a setting file.

In order to save a profile, select the **Save Map** button or *File > Save Map* from the map container toolbar of that particular map profile you wish to save. Note that if user is trying to save a map profile that has a same name as one of the existing profile, a warning message would appear to get confirmation from the user to overwrite the file. To proceed with the action, click the **OK** button.

By default, the profile will be saved to the *Map* folder in the program's directory, with the name of the map profile and extension *.map* or *.l2map*, or *.ezmap*.

4.3.4 Topology Map

The topology map is actually the graphical representation of the actual Mesh network topology which is being scanned. When a new scan is initiated, the result of the scan will be processed by the NMS, and output to the map.

The AP unit would appear in different colors and shapes:-

Icon	*Indication*
	Inactive AP
	Accessible Gateway AP
	Inaccessible Gateway AP
	Accessible Relay AP
	Inaccessible Relay AP
	Accessible Client-Relay AP
	Inaccessible Client-Relay AP
	Layer-2 Gateway AP
	Layer-2 AP, which notified the NMS
	Accessible Dual-Radio Gateway AP
	Inaccessible Dual-Radio Gateway AP
	Accessible Dual-Radio Relay AP
	Inaccessible Dual-Radio Relay AP
	Accessible Dual-Radio Client Relay AP
	Inaccessible Dual-Radio Client Relay AP
	AP Bridge

AP Router

MLRD

Repeater

Slave Bridge

Master Bridge

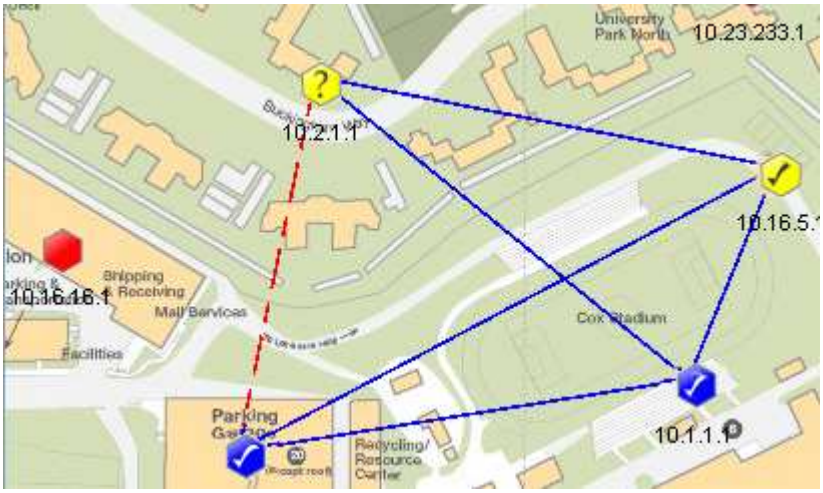
WDS Bridge

WDS Router

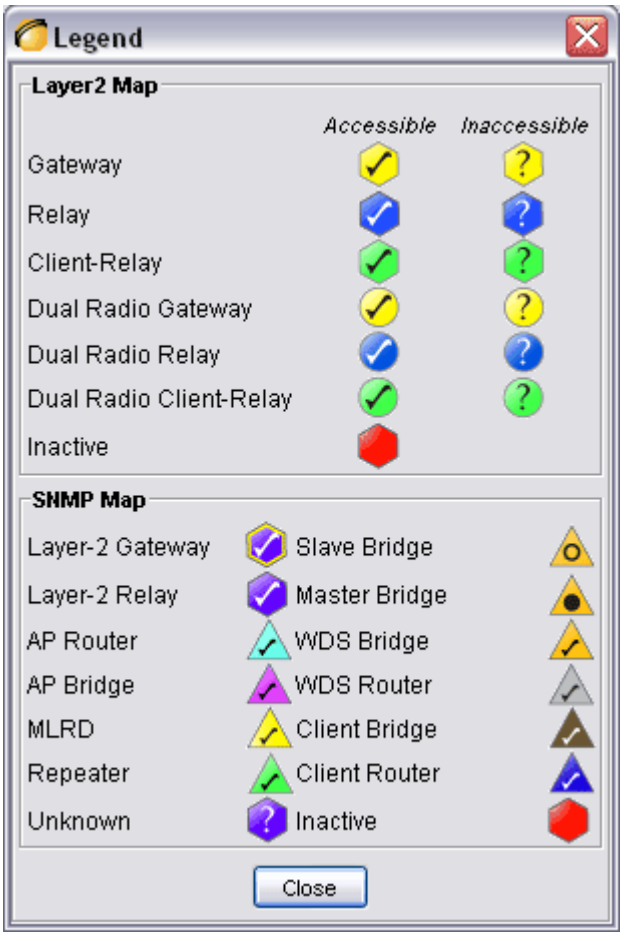
Client Bridge

Client Router

Unknown Node, which the NMS failed to detect its mode



The blue line in between the APs designates the solid link; whereas the red, dashed line shows the indirect link. On the other hand, user may hit the *Help > Legend* option from the menu bar to view the legend regarding the topology.



All the icon, as well as the type of the link describes above are default item. They can be customized through the customization tool according to the administrator preference. .

Occasionally, user may observe some inaccessible node (indicated by “?” sign) from the map. These nodes are actually discovered by its neighbour node. The NMS, however, failed to read the node’s content through SNMP. Normally, this is caused by the SNMP community or password used by the NMS is not matched with the node. It could also happen if the SNMP feature is disabled by the user at the firmware, or the physical signal strength between the NMS host and the node is weak enough that results the data packet is dropped.

4.3.5 Set up New Scan

Layer-3 Map & EZ Map

In order to set up a new scan for a SNMP topology map, click on the **Start Scan** button, or select *Map > Start Scan* from the menu bar. Conversely, hit the **Stop Scan** button or select *Map > Stop Scan* to halt the scanning process. The status of the map will be updated periodically, hence whenever there is a change in the network, user might be able to monitor via the NMS. The status bar at the bottom of the map displays the status of the scan.

Layer-2 Map

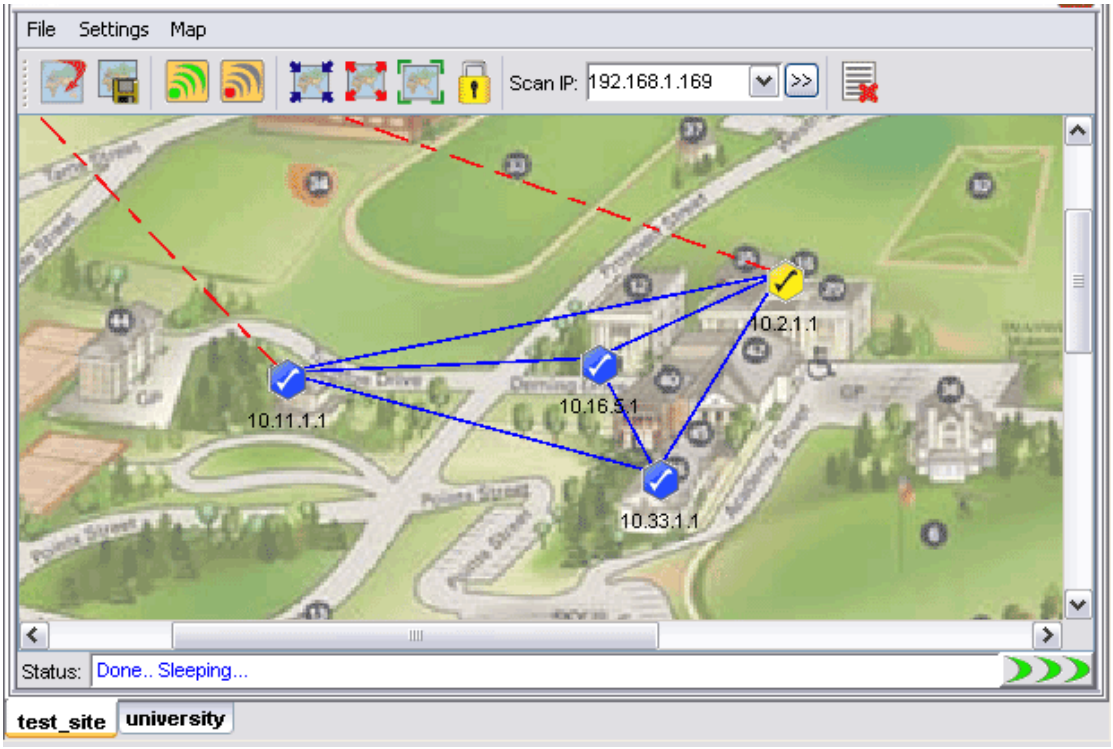
On the other hand, in order to set up a new scan for the Layer-2 topology map, click on the **Initiate Port** button, or select *Map > Initiate Port* from the menu bar. The map will receive the notification sent by the AP and plot the topology on the map. Conversely, hit the **Close Port** button or select *Map > Close Port* from the menu bar to stop listen to the notification.

Every new found Mesh AP unit will be place on the right top angle on the map, with zero coordinate. Then user is free to move the AP unit around the map. Once user completes the positioning, save the map, and the system will remember the new coordinates in the future scan.

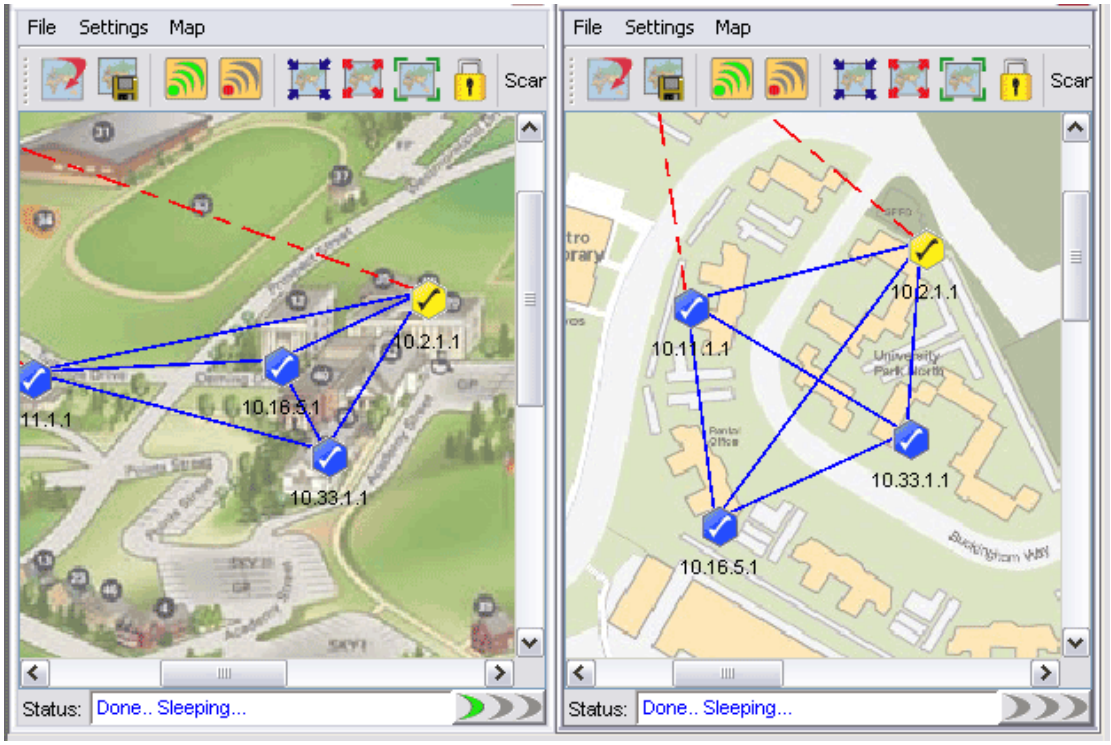
4.3.6 Map View

More than one topology map can be loaded to the NMS at the same time. By default, the maps are viewed in cascade mode, where user needs to click on the tab at the bottom to switch the map to view.

In order to change the view type, click the **Tile** button on the main toolbar, or select *View* > *Tile* from the menu bar. The tile mode arranges the topology maps in a grid layout. To convert the view mode to cascade, hit the **Cascade** button, or *View* > *Cascade*. The following figures illustrate the difference between the two modes.



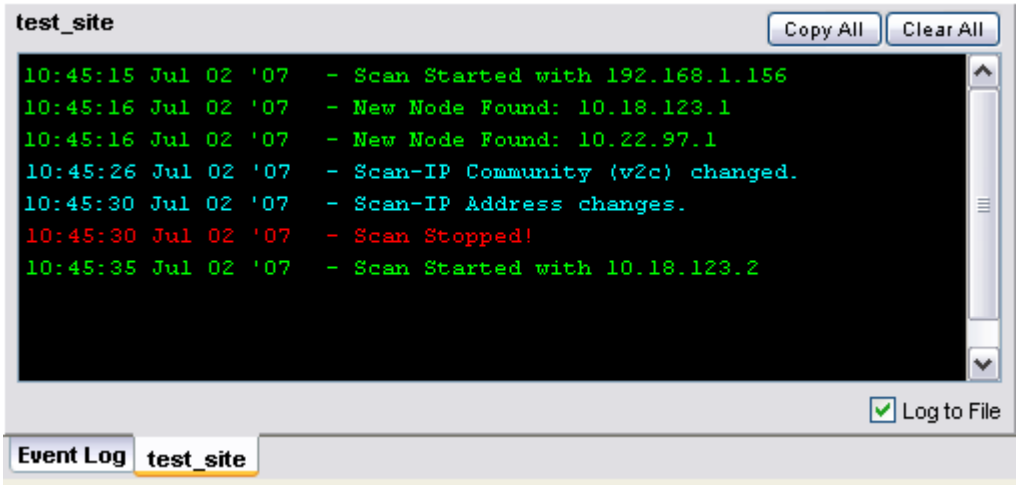
(Cascade mode)



(Tile Mode)

4.3.7 Status Pane

The status pane is located at the bottom of the map container. It displays the nodes' status with the time and date; enable users to keep track of the changes in the topology.



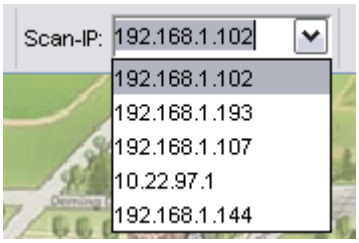
The type of message can be varied by the color of the text. Green text indicating positive message such as scan started or nodes found; red text shows the negative message such as nodes down or timeout; whereas cyan text displaying system message, for instance, system settings changed.

The **Copy All** and **Clear All** buttons on the top of the pane performs the copy and delete text action in the status pane. Tick the checkbox at the bottom to log the status message to the alarm log file, which will be saved to the folder *Alarm_Log* at the install directory.

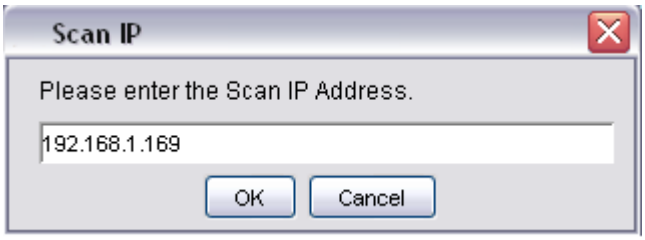
4.3.8 Scan IP Address

The *Scan IP Address* is the IP Address that the scanning process uses when initiate a scan for a Layer-3 Map.

User might enter the IP Address at the drop down list, or choose from the list. In order to apply the new *Scan IP*, user is required to restart the network scanning. (A running scan will be stopped when a new IP Address is selected.)



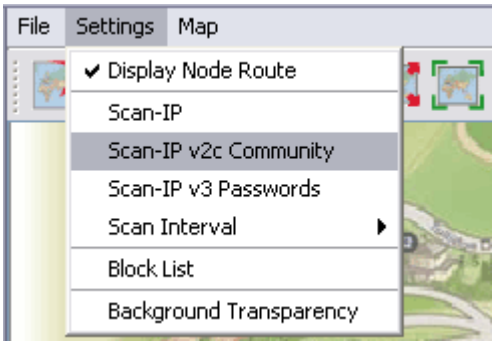
On the other hand, the *Scan IP* can also be set by selecting *Settings > Scan IP* from the map container's toolbar. A window would appear to prompt user for the new IP Address. Hit the **OK** button to apply the change.



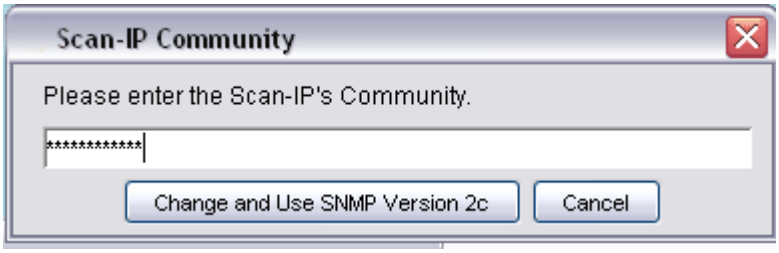
4.3.9 SNMP Community / Passwords (for Scan-IP)

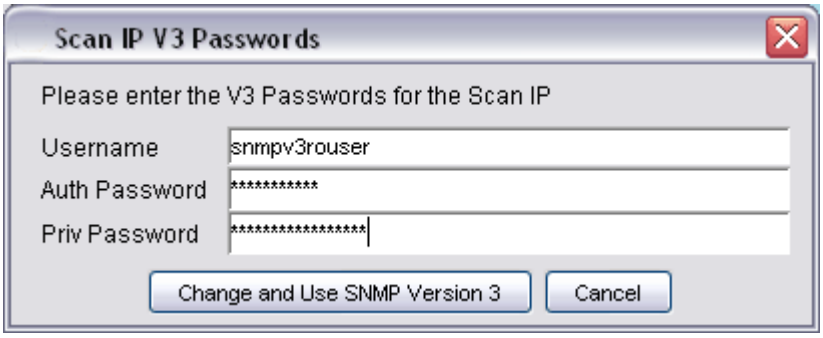
The *EnGenius Mesh Network Management Tools* use the SNMP method to read the topology of the network. There are two types of SNMP key used for the topology scan, which are the Scan-IP key and the AP Unit key. More details about the latter please click here.

Commonly, the use of SNMP varies by its version. If a user select version 2c, the SNMP key to use is a community; on the other hand, if version 3 is used, the SNMP key will be a SNMPv3 username, with its corresponding authentication password and privacy pass phrase. As you can see throughout this document, every feature that implements SNMP will have both options

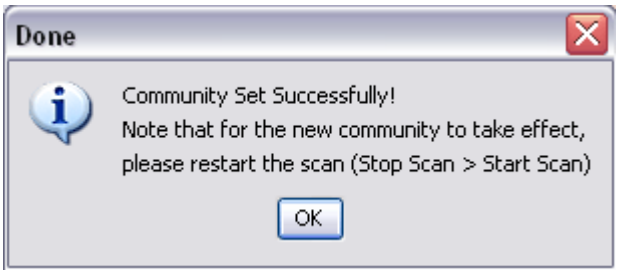


Basically, the Scan-IP key is the SNMP key that used for the Scan-IP which initiates the scan. In order to configure the community of the Scan-IP, select *Settings > Scan-IP v2c Community* from the map container menu. On the other hand, select *Settings > Scan-IP v3 Passwords* to change the SNMP version 3 Passwords. A window would turn up to prompt user for the new key(s).





Press **Change and Use SNMP Version X** button to proceed. If the change is successfully, the following dialog box would appear, to remind user to reset the scan in order to let the new community or passwords to take effect.



The default value for Scan-IP:

Community: *public*

Username: *snmpv3rouser*

Password: *snmpv3password*

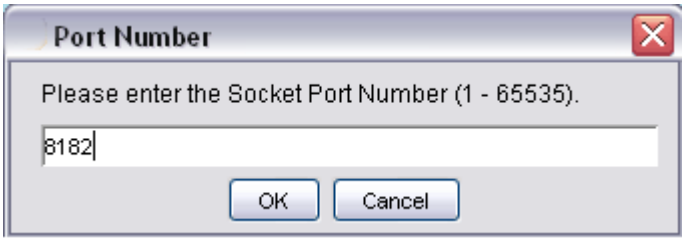
Passphrase: *snmpv3passphrase*

4.3.10 Socket Port

The notification of an AP node is sent according to its NMS Address Table. The table defines the IP Address and port number of the destination (NMS). For instance, if the

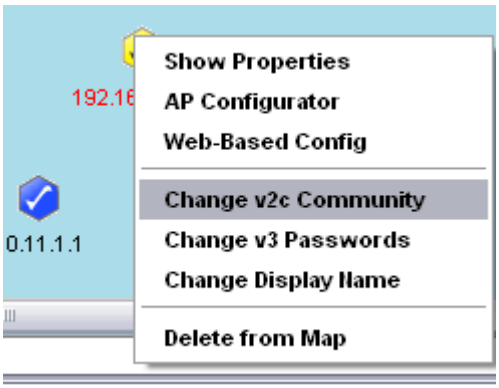
admin has added a table entry with port number 8000 at the AP, the NMS user can change the socket port number to 8000 in order to receive the notification.

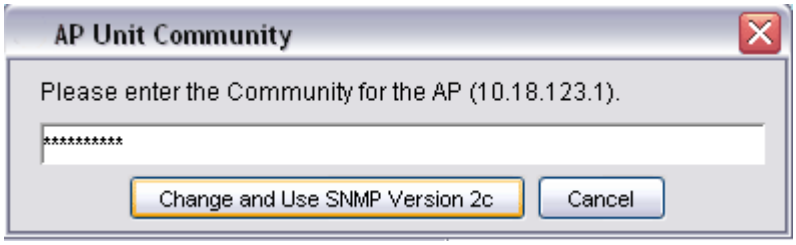
In order to update the socket port, select *Settings* > *Socket Port* from the menu bar. A dialog box would appear on the screen to prompt for the port number, which range from 1 to 65535. Hit **OK** to confirm the change.

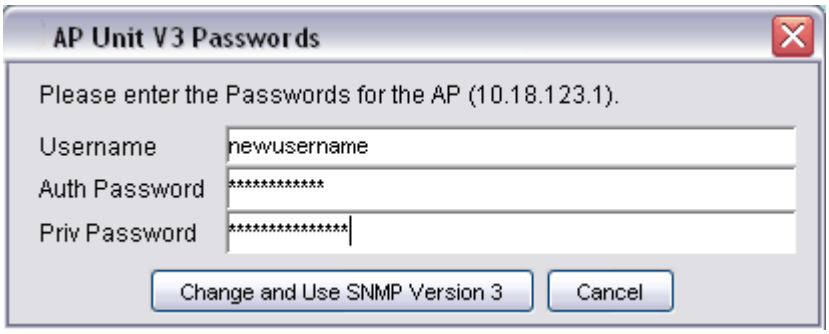


4.3.11 SNMP Community / Passwords (for AP Unit)

In case if a Mesh AP utilizes a different community or passwords from the others, the NMS might fail to read the topology from it. Hence, user might need to edit the individual AP unit SNMP keys, by right-click the desired active node. Select *Change v2c Community* from the popup menu to change the community; or click *Change v3 Passwords* to change the v3 keys; enter the correct value in the dialog box and click **Change and Use SNMP Version X**.







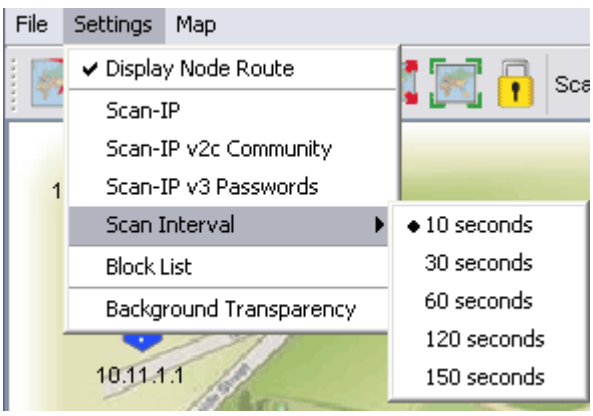
Note that the AP Unit Keys is also used for read the Node Details and Client Properties. The default SNMP version and keys of the Mesh AP is inherited from the Scan-IP that found them.

4.3.12 Scan Interval

The scan interval defines the time interval between every round of scanning. By default, the NMS will sleep for 10 seconds once a network scan is completed. User may change the time interval by select *Settings* > *Scan Interval*, and choose the desired time interval. The available options:

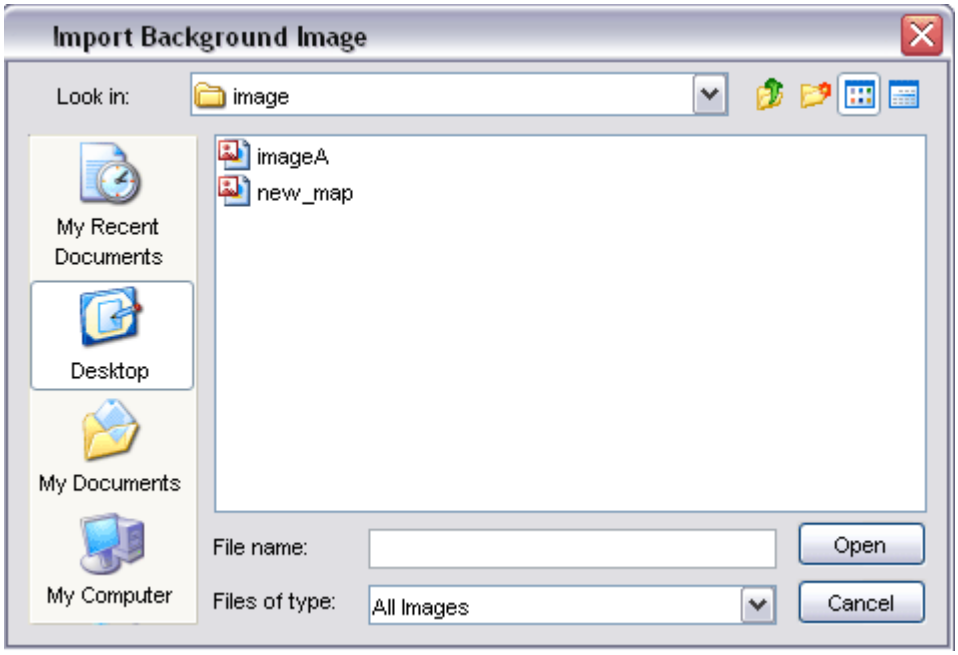
- 10 seconds
- 30 seconds
- 60 seconds
- 120 seconds
- 150 seconds

The changes will take effect immediately.



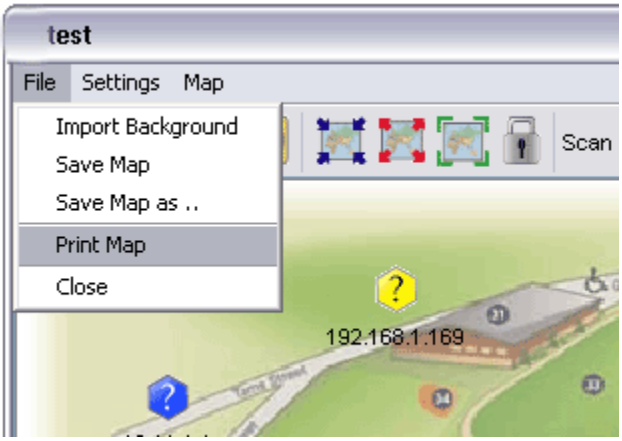
4.3.13 Import Background Image

User can change the background of the topology map by import any desired image file from other resource. Click on the **Import Background Image** button, or select *File > Import Background* from the map container's menu bar. A file chooser window would appear, to prompt user for the image file that wished to import.



After select a image file (.jpg, .gif, .png ..etc), click the **Open** button. The new image will be loaded into the topology map.

4.3.14 Map Print

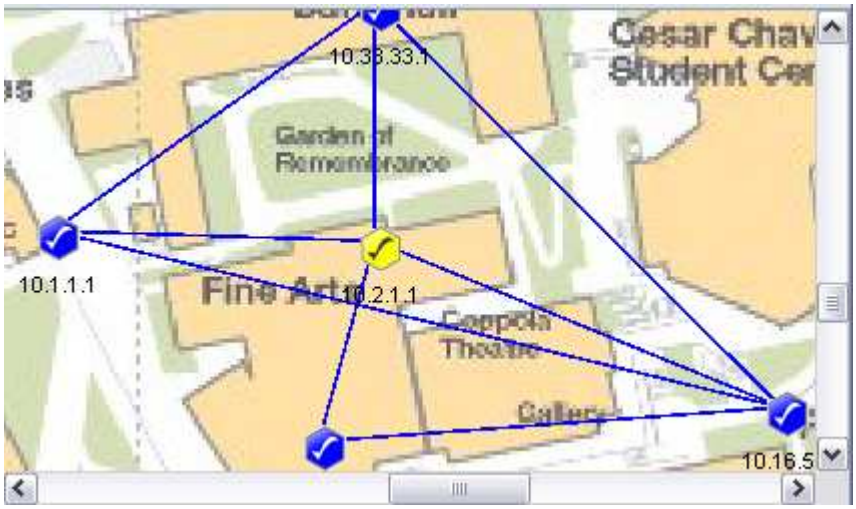


The NMS also provide the printing feature, where user is able to print the whole map by just select the *File > Print Map* option from the Map Container menu bar. Then it will redirect the map to the printer connected to the terminal where you run the NMS.

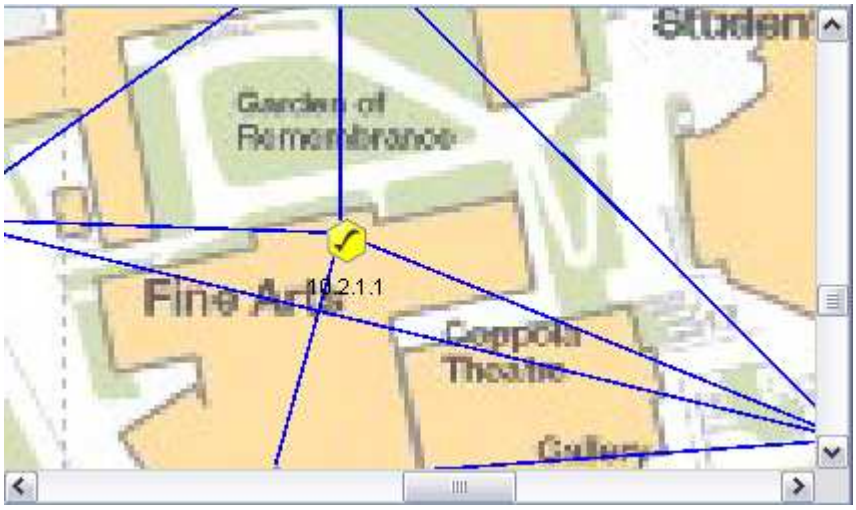
4.3.15 Map Zoom

As a graphical solution for a network system, the *EnGenius Mesh Network Management Tools* provides the zooming feature for the user to manage the topology map more efficiency. Three options are available: *Zoom In, Zoom out* and *Zoom Fit*.

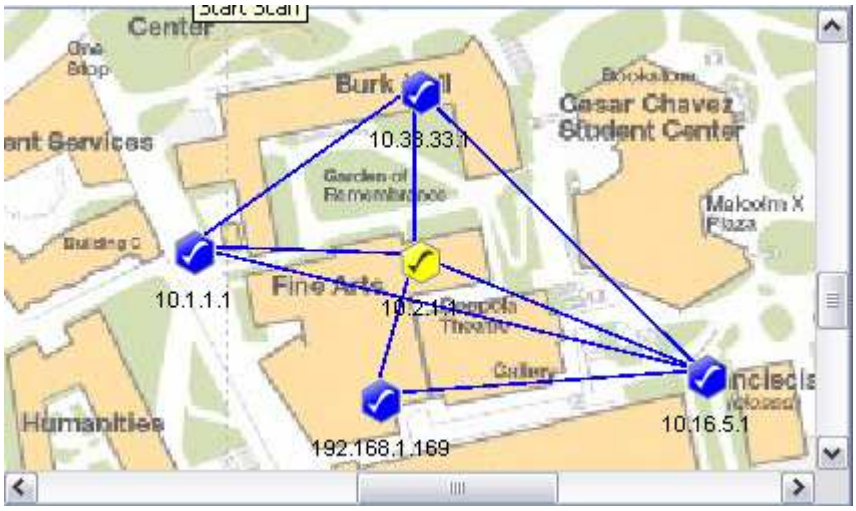
The *Zoom In* and *Zoom Out* feature enable user to enlarge and minimize, respectively, at the scale of 25%. Whereas the *Zoom Fit* feature will resize the topology map to the most suitable size to fit in the screen. The following figures illustrate the effect of the zoom features.



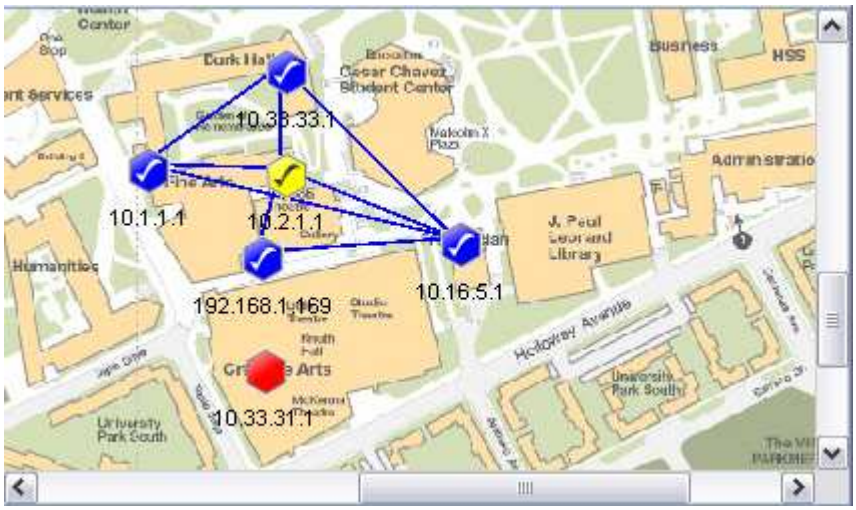
(Original size)



(Zoom In)



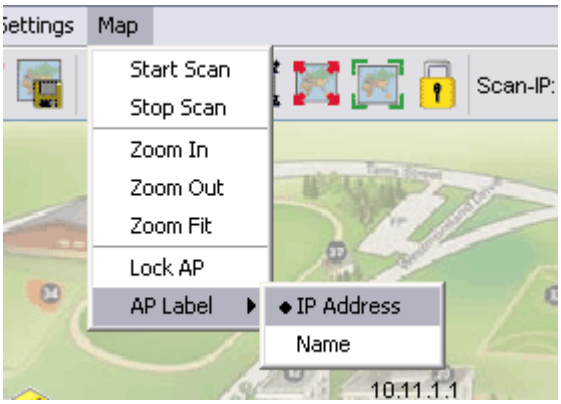
(Zoom Out)

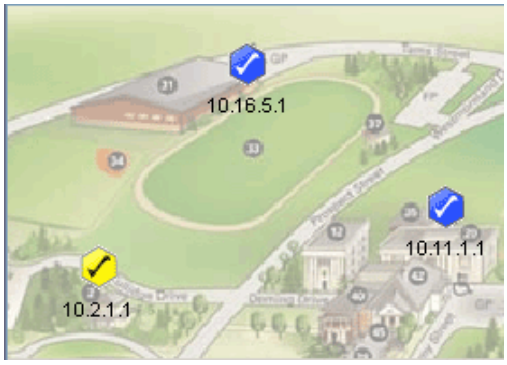


(Zoom Fit)

4.3.16 Node Label

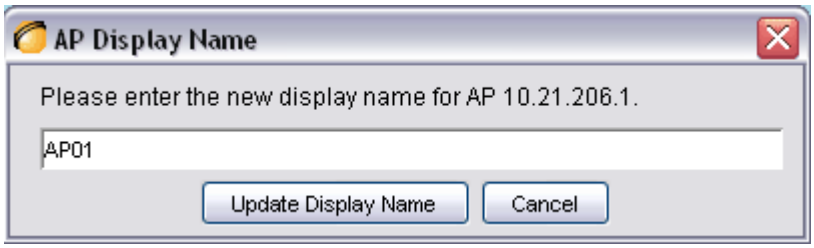
When a topology is plotted on the NMS map, user might wish to display the nodes label with something else instead of the IP Address (or MAC Address for Layer-2 map). In order to change the label view of the topology, select *Map > AP Label* from the topology map menu bar. Two options are available: *IP Address* and *Name.*





By default, when a new node is found and added into the map, its initial name is "Undefined". Therefore, if user is wish to update the name of the specific node, right-click on the node, and select *Change Display Name* from the popup menu.

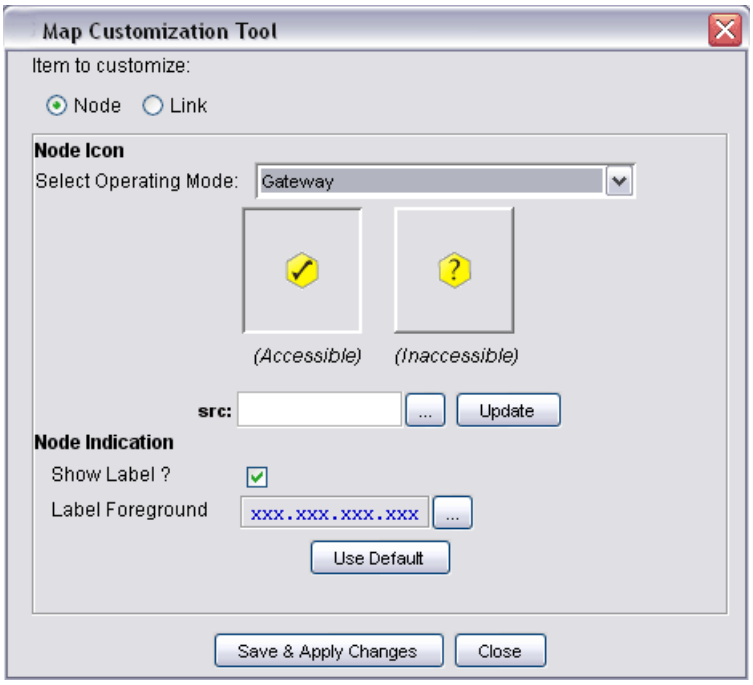
Following the step, a dialog box would popup to prompt user to enter the desired name for the specific node. Click **Update Display Name** button to complete the step.

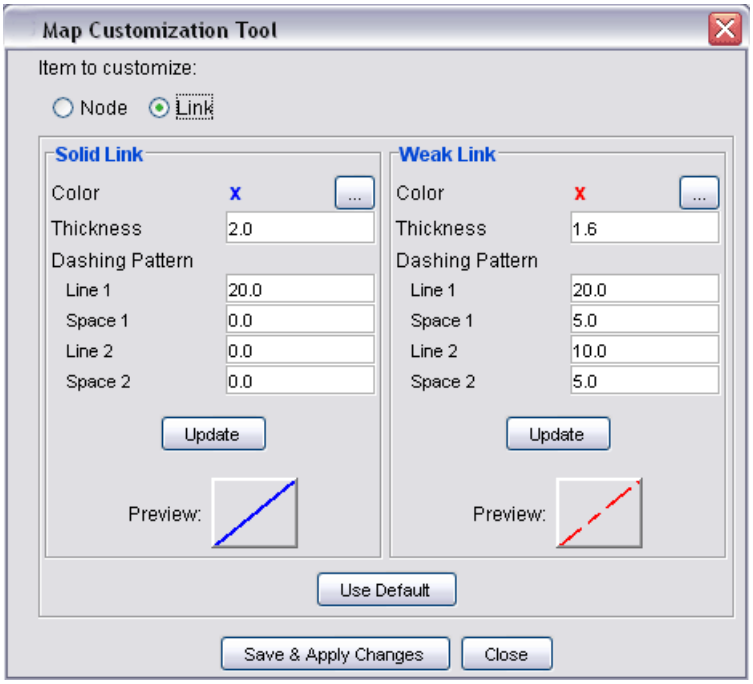


4.3.17 Customize Map

This feature provides user the flexibility to change the look and feel of the topology map, by replacing the existing AP unit icon and the links between AP in the map. User can import their custom-made icon, or adjust the color to fit their visual requirement.

The customization can be divided to three parts, the *Node*, *Link (Radio 1)* and *Link (Radio 2)*. The method is straight forward. Select *Settings > Customized Map* from the NMS menu bar, to invoke the Map Customization Tool window, as illustrated.





At the *Node* part, user may select the icon that need to be updated from the drop down list. The item in the list includes every operating mode that recognized by the NMS. After that, fill in the path of the new image at the **src** column (or click the "…" button to choose from the file chooser window). Hit the **Update** button to update the new image icon. Besides, user can also decide whether to show the indication of the AP-unit, which could be IP Address or MAC Address, by using the available checkbox; and alter the foreground color of the IP Address using the "**…**" button to select a desired color from the popup window. Hit the **Save & Apply Changes** button to commit the changes. The **Use Default** button enables the user to restore the default settings of the AP unit look and feel.

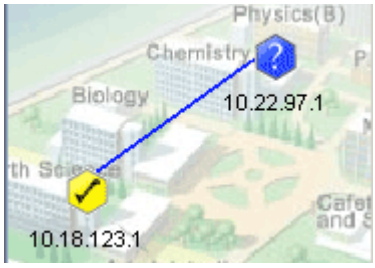
Meanwhile, in order to change the style of the link, switch the *Map Customization Tool* to the *Link* page. User can change the color by hitting the "**…**" button to select a desired color from the popup window. Then key in the thickness of the link and its dashing pattern. The dashing pattern defines the way the dashed link look like. The following table explains how to use the dashing pattern. After fill in the data, user

may click the **Update** button to update the image at the preview. Once confirm the changes, select the **Save & Apply Changes** button to commit the change.

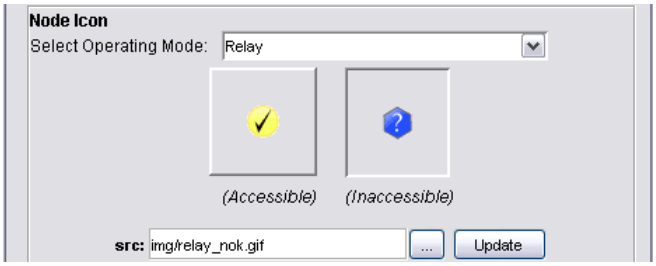
Pattern (line1, space1, line2, space2)	**Preview**
20, 0, 0, 0	
20, 10, 20, 10	
5, 10, 5, 10	
20, 3, 10, 3	
20, 10, 30, 5	

Here is an example to show the effect of the map customization.

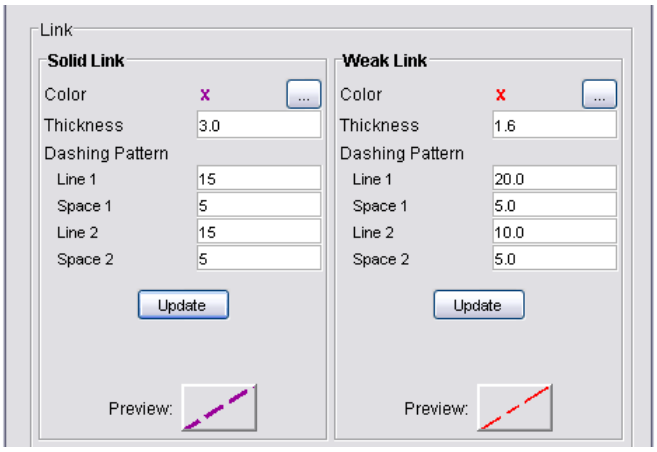
a) The original map



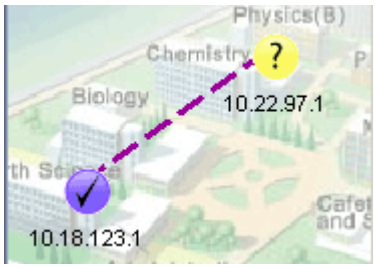
b) Select Map Customization Tool and change the gateway & relay icon



c) Switch to Link page and edit the attributes



d) The customized map will look like this now.

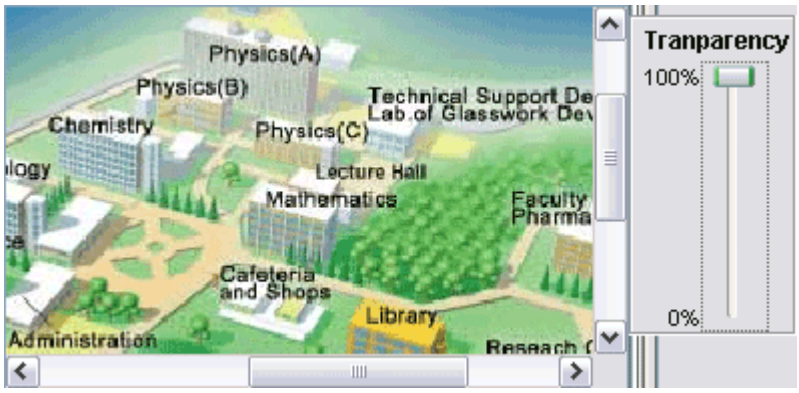


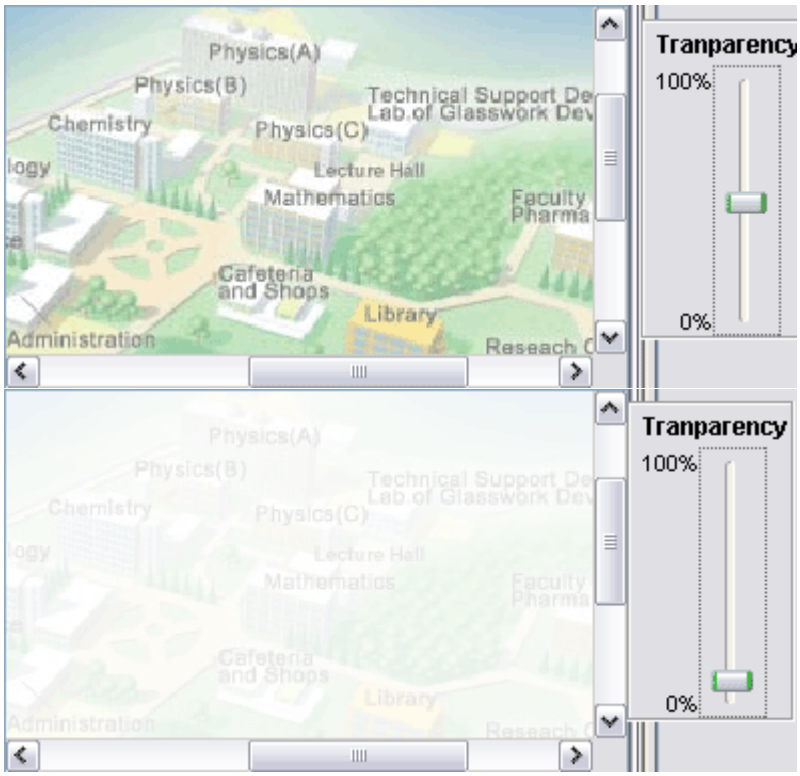
Note that, the changes of the AP unit node and link applies to every map created or opened on the NMS.

4.3.18 Background Image Transparency

This is a special tool used to adjust the opacity of the background image of the topology map. Select *Settings* > *Background Transparency* from the map container menu bar to allow users to alter the transparency of the background to a level that the APs and links are clear to view.

View the following figures to see the effect of the transparency tool.





The tool will be closed automatically when it loses focus (mouse click anywhere out from the tool).

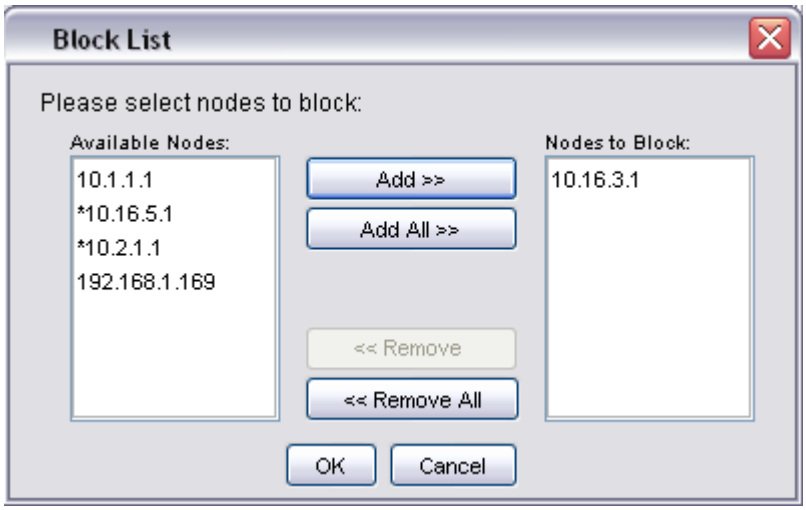
4.3.19 Block List

The *Block List* offers the NMS users a filtering tool in the topology map. User can define the IP Address to block, once the AP is blocked, it will be removed from the topology map, and will not be added to the map even if it is detected by the NMS.

To move an IP to the block list, click the **Block List** button on the toolbar, or select *Settings* > *Block List* from the menu bar. A window will emerge, as shown by the figure above. Then user can choose the node to block from the *Available Nodes* column. Select the IP, and hit the **Add** button. The IP will be move over to the *Nodes to Block* column. On the other hand, if user wishes to undo the step, use the **Remove** button to move the IP back to the available list.

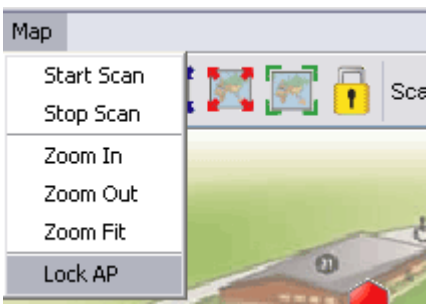
The **Add All** and **Remove All** button perform the same operation by moving every IPs in the list. Finally, hit the **OK** button to commit the change. (*Note: asterisk in the list shows the IP is a gateway node*).

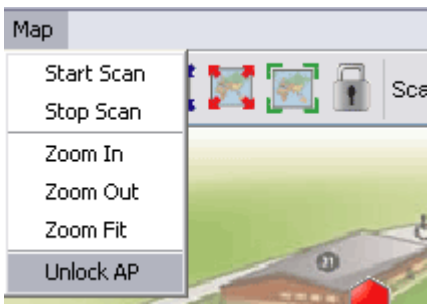
The blocked IP Address will be saved into the map setting file when the user saves the topology map. Hence the IP will still be blocked when the current map profile reload in the future.



4.3.20 Lock / Unlock

This feature is intended to prevent the user from dragging the node away from its current position accidentally. User can select *Map > Lock AP* from the menu bar or use the **Lock AP** button on the toolbar to lock up the nodes on the map.

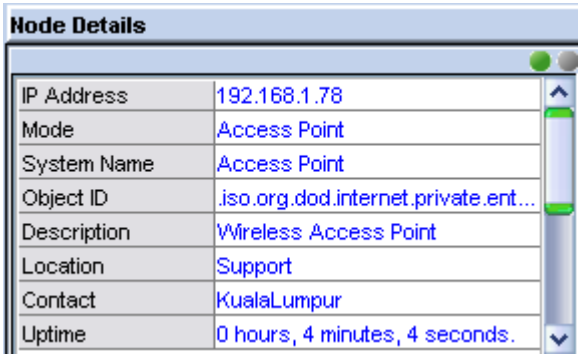




Conversely, click the *Map > Unlock AP* or **Unlock AP** button on the toolbar to release the lock. Hence, once user has complete positions the nodes, turn on the lock.

4.3.21 Node details

The table next to the map container is the node details table. The table displays the properties of the selected Mesh AP unit. In order to load the data, user can double-click on an active unit (gateway or relay or client-relay), or right click then choose the *Show Properties* item from the popup menu.



The node details table displays the following items:

1. IP Address
2. Operation Mode
3. System Name
4. Object ID
5. Description
6. Location
7. Contact
8. Uptime

The lower part of the table is a dynamic table, which would displays parameters based on the selected node's operation mode. The following figures show the parameters that displayed by each mode:

Profile 1	XXX/WPA/AES/ Enable
Profile 2	EEE/Shared Key/WEP/ Enable
Profile 3	EYY/Open System/No Encrypti...
Profile 4	EEE/Open System/No Encryptio...
Wireless MAC	00:02:6F:57:22:C5
Wireless Mode	802.11b (2GHz/11Mbps)
Channel	2.462GHz (channel 11)
TX Power	20 dBm

(Access Point mode)

SSID	EnGenius
Wireless MAC	00:02:6F:57:22:C5
Connection Status	Associated
Wireless Mode	802.11b (2GHz/11Mbps)
Channel	2.432 MHz(Channel 5)
Security	WPAPSK-TKIP
Tx Data Rate	Bit Rate=1
TX Power	20 dBm

(Client Bridge mode)

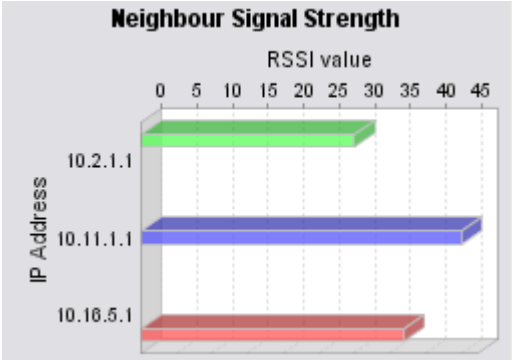
SSID	EnGenius
Wireless MAC	00:02:6F:57:22:C5
Connection Status	Associated
Wireless Mode	802.11b (2GHz/11Mbps)
Channel	2.462 MHz(Channel 11)
Security	WPAPSK-TKIP
Tx Data Rate	Bit Rate=1
TX Power	20 dBm
Connection Type	Static IP
WAN IP	0.0.0.0
WAN Subnet	0.0.0.0
Interface	Down

(Client Router mode)

Profile Mesh	EngeniusMesh/Open-System
Profile AP1	EngeniusAP1/WPA-AES/Enable
Profile AP2	EngeniusAP2/WEP-Shared/Ena...
Mesh Mode	Relay
Wireless MAC	00:02:6F:57:22:C5
Wireless Mode	802.11b (2GHz/11Mbps)
Channel	2.462GHz (channel 11)
TX Power	20 dBm

(Mesh mode)

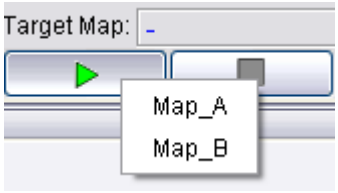
As mentioned previously, the NMS use the SNMP method to read the data. Hence if the data is failed to load, you may check the SNMP Community or Passwords. The two small circles on the top of the table indicate the status of the table. If the green circle is light up, it shows the table is loaded completely; if the orange circle is light up, it means the table is loading the data, else if the circle to turn to red color, it indicates that the data loading is failed.



On the other hand, the bar chart at the bottom of the table displaying the signal strength (in RSSI) between the selected AP and all its neighbour nodes. The scale of the chart can be enlarged by dragging the desired range of x-axis. Drag backward to reset the chart.

4.3.22 Client Properties

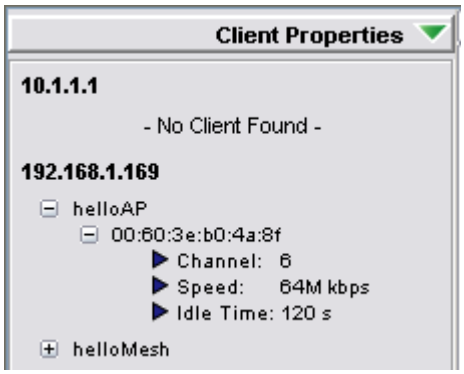
The client properties panel is located at the other side of the map container. In order to initiate the NMS to download the client details, hit on the **Start** button at the bottom of the panel. In case if there is more than one map is running, a menu would popup to prompt user to select which map to be targeted. Once selected, the scanning will be started instantly. (*Please note that this feature is not applicable to EZ Map type*)

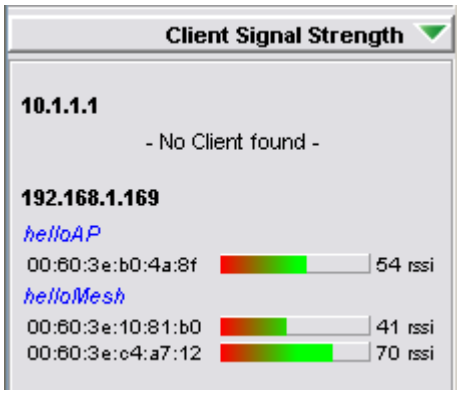


The automatic refresh feature of the client properties panel enable the admin uses the live information regarding the clients associated to the Mesh AP unit discovered by the NMS. The panel will be refreshed once per minute. On the other hand, if user wishes to refresh the panel manually, simply click the **Refresh** button at the bottom of the panel. While the downloading is in progress, the buttons will be replaced by a progress bar, showing the status of the process. The NMS will download the

information from every single node in the target map discovered. To stop the scan, simply hit on the **Stop** button. The *Target Map* column displays the name of the map where the client panel is scanning.

The panel is divided into two portions, the *Client Properties* and *Client Signal Strength.* The *Client Properties* portion display the details regarding the client, for instance the MAC Address, channel number, link speed and the idle time. In the case if there is no client associated to the AP, a message "*No Client Found*" will be displayed instead.



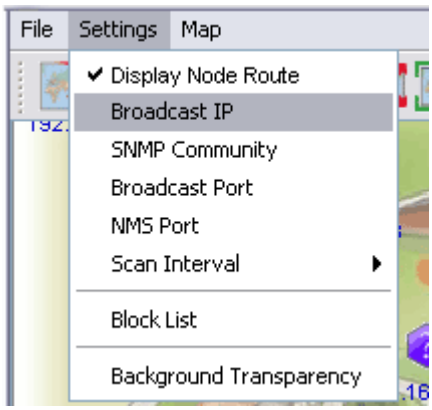


On the other hand, the *Client Signal Strength* panel displays the signal strength of the clients associated to the AP, in the unit of rssi. Similarly, if there is no client associated to the AP, a message "*No Client Found*" will be shown.

4.3.23 EZ Map Settings

The EZ Map broadcasts the SNMP packet over the network to locate the activated SNMP device. The devices that has been discovered, will report themselves at the NMS recursively.

By default, the broadcast packet use SNMP version 2c community '*public*'. That says, any device that has SNMP enabled and the same community with the NMS will be able to be located by the NMS. The settings that affecting the discovery process includes broadcast IP, SNMP Community, and broadcast port, and they can be configured via the menu bar *Settings* option, as shown below:



Broadcast IP

By default, the broadcast IP used is 255.255.255.255. If user would like to filter out certain subnet from the NMS, they can change the IP Address thru *Settings* > *Broadcast IP*.

Enter the desired broadcast IP Address in the column provided, and click the **Update** button. Now as the new setting has been saved, user will be required to restart the scan in order for the new settings to be loaded.

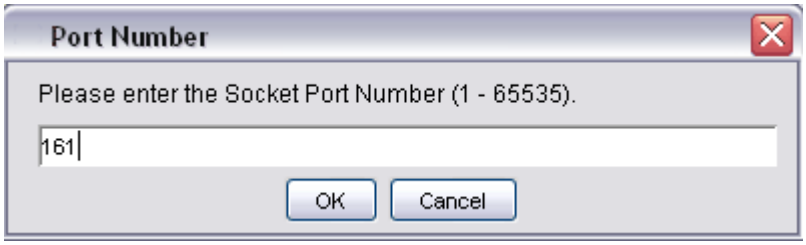
SNMP Community

The EZ Map broadcast the SNMP version 2c packet in order to discover the network. Corresponding to SNMP version 2c, a read-only community key word is required. By default, the community used is '*public*'. Any device that has a different community than this *SNMP Community* will not be discovered at the EZ Map. In order to change the community, select *Settings* > *SNMP Community* at the menu bar.

Enter the new read-only SNMP community to the provided column, and click the **Update** button to save the new setting. Now as the new setting has been saved, user will be required to restart the scan in order for the new settings to be loaded.

Broadcast Port

The broadcast port is the port number of the socket that used to broadcast the SNMP packet. By default, the port that used for SNMP is 161. If user would like to change the port number, select *Settings* > *Broadcast Port* from the menu bar.

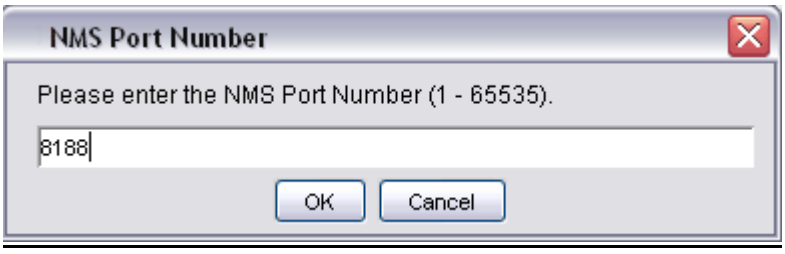


Enter the new port number (in the range of 1 to 65535), and click the **OK** button. Now as the new setting has been saved, user will be required to restart the scan in order for the new settings to be loaded. Please note that if the port has been used, the EZ Map will not be able to start up the scan.

NMS Port

At the EZ Map, the node discovered through the scan process has limited information. However, if the node has the EnGenius mesh module installed within, the NMS is able to grab more details, such as the operation mode and neighbour list from the node. By setting the NMS Address configuration at the web-based configuration page (more), the nodes now are able to report their information back to the EZ Map using the similar method as the Layer-2 Map.

In order to change the NMS Port number, select *Settings* > *NMS Port* from the menu bar. Enter the new NMS port number (in the range of 1 to 65535, default is 8188), and hit the **OK** button.



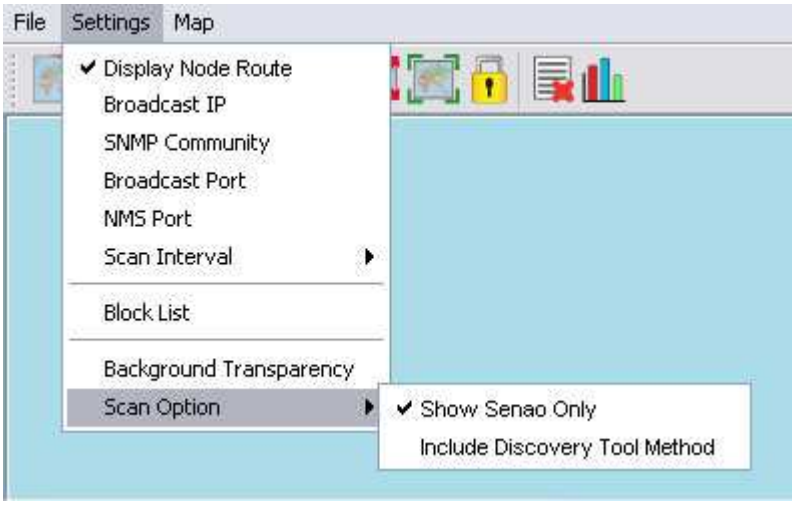
Show Senao Only*

(Feature has been replaced)

Scan Option

User can configure the scan option in order to achieve discovery optimization based on their needs.

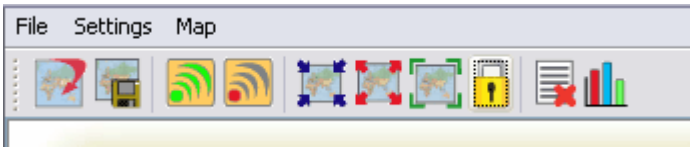
Since the EZ Map is able to scan every SNMP-enabled device at the same network, it is possible that the map is able to detect other devices that are not recognized (eg: network printer, etc). In order to filter those unknown device from the NMS, enable the *Settings > Scan Option > Show Senao Only* option from menu bar, will automatically filter the nodes that are not belongs to Senao Network.



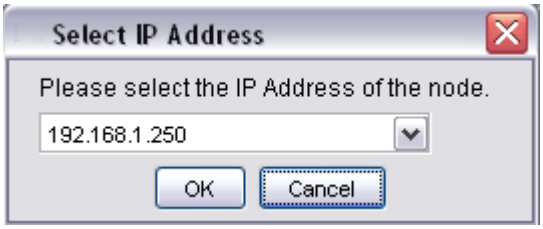
On the other hand, there is another selection at the Scan Option portion – *Include Discovery Tool Method*. This method duplicates the node-scanning technique that is used by the Discovery Tool. This feature is useful to discover the pre-set APs, which does not have SNMP setup yet, or APs that are using different password. Please note that enabling this mode will automatically disable the *Show Senao Only* option.

4.3.24 Show Live Stat (EZ Map)

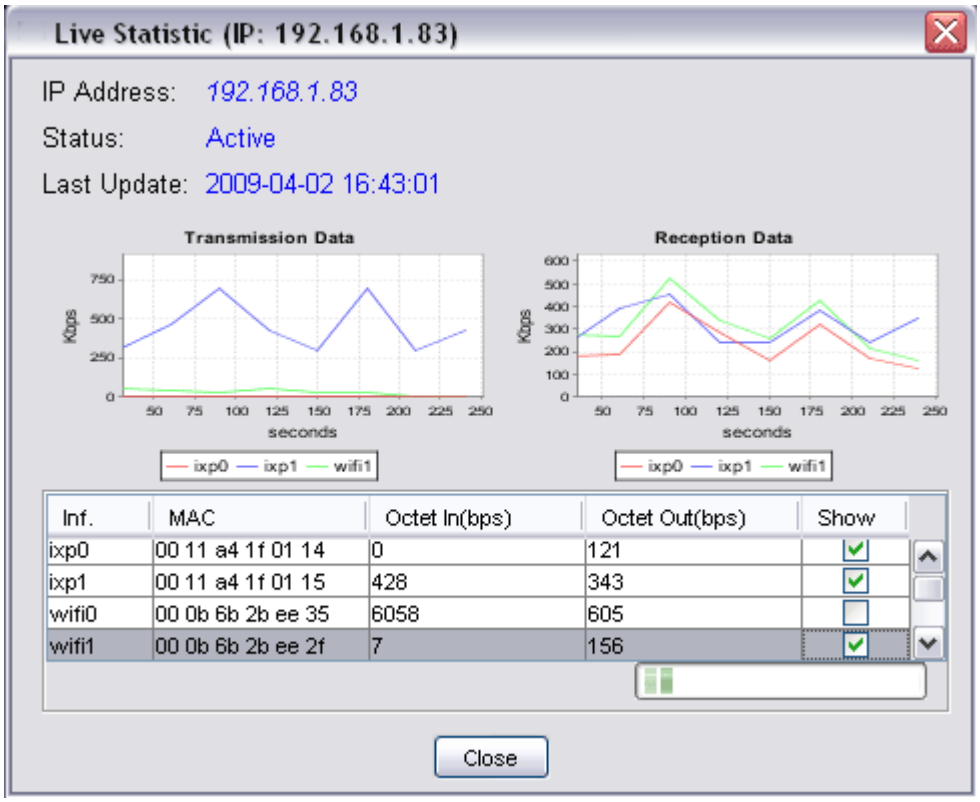
Since some of the nodes discovered by the EZ Map do not have EnGenius mesh module installed, they are not able to view through the Live Stat window at the main window. Therefore, EZ Map provides user a customized live stat window in order for the user to monitor the statistic of the nodes.



Select the **Show Live Stat** button, a window would popup, and required user to select the IP Address of the node that available in the map.

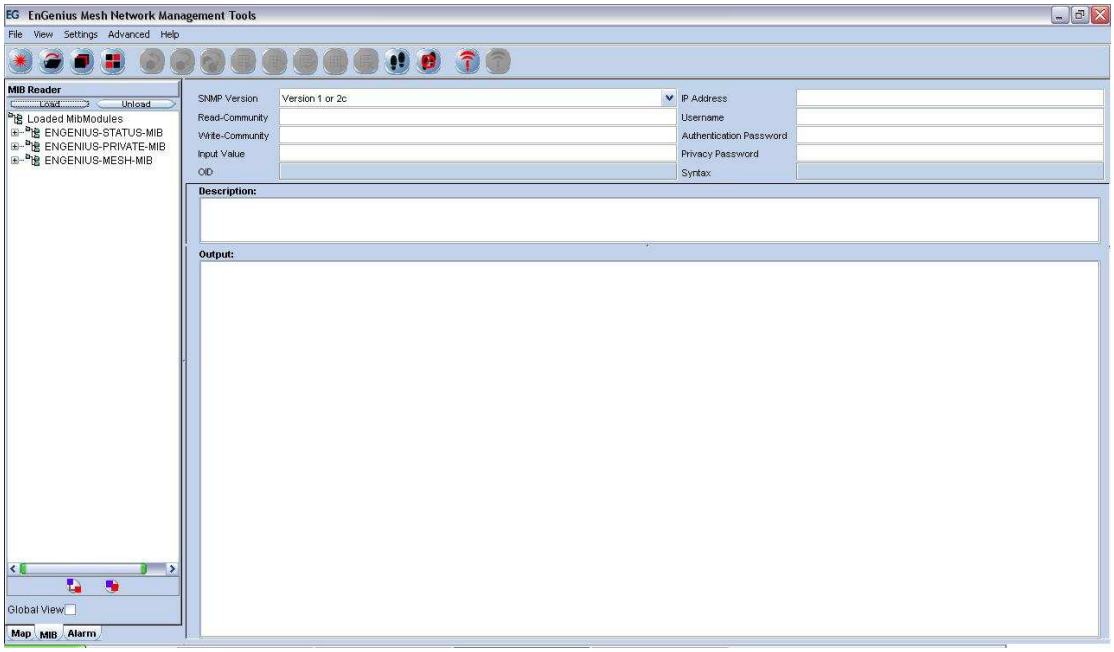


Select the desired IP Address from the drop down list, and hit the **OK** button. Then the EZ Map live stat window would appear. The information will be automatically updated every 30 seconds.

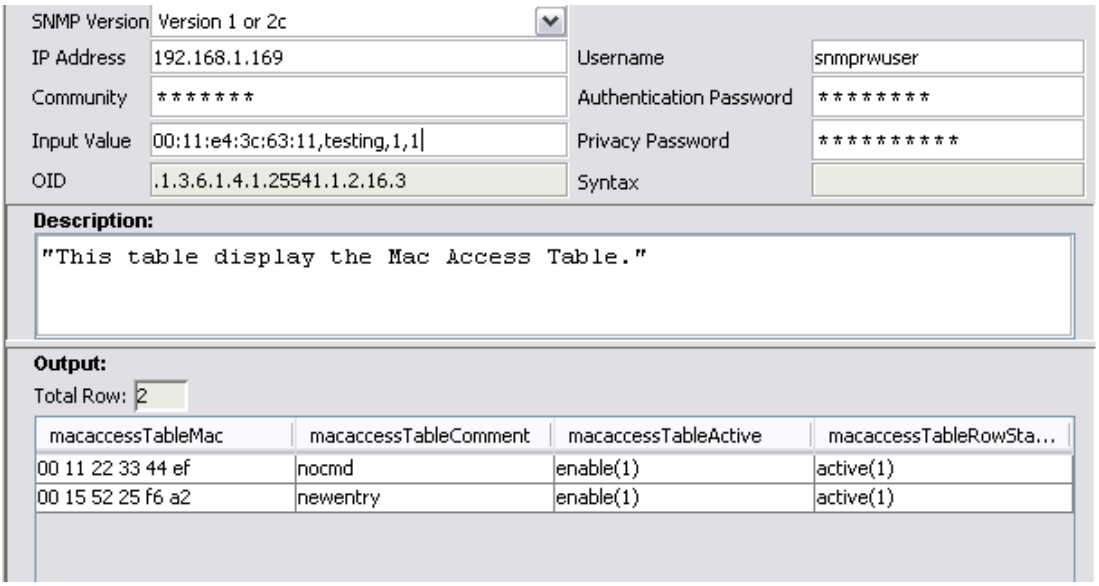


The window would display the throughput of the node in the graph and table. User is able to filter the interface to be displayed at the graph by clicking the checkbox at the table.

4.3.25 Get/Set using MIB Reader



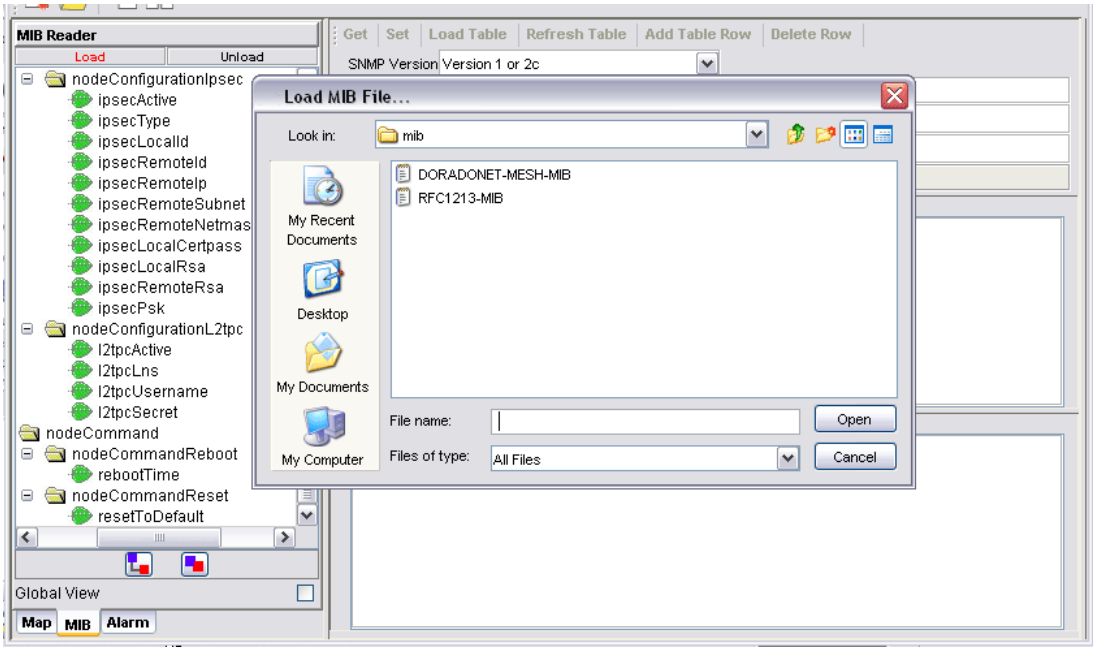
This section describes briefly about the usage of the *MIB Reader* of the *EnGenius Mesh Network Management Tools*. As illustrated, the center frame of the *MIB Reader* consists of three parts, SNMP keywords, description area and output area. The SNMP keywords portion is the area where user fills in the necessary parameter that need to perform any SNMP action. For instance, if the SNMP version to use is version 1 or 2c, then the *Community* is the required field; else if version 3 is selected, then user need to fill in the *username, authentication password,* and *privacy password* fields. The *Input Value* field is used when user wish to execute the SNMP Set command.



The *Description* area displays the description of the selected MIB tree node; whereas the *Output* area prints out the output of the SNMP action.

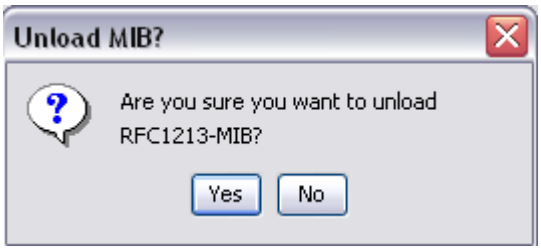
4.3.26 Load/Unload MIB

The *MIB Reader* of the NMS includes the feature to load and unload the MIB file from other resource. Therefore, instead of the customized MIB, user can load other standard MIB into the *MIB Reader* as well to read the parameter of the managed device.



In order to load a MIB, click on the **Load** button on the top of the MIB tree. A file chooser window would popup, to prompt user to enter the desired MIB file. Click **Open** to load the file.

On the other hand, the **Unload** button next to the **Load** button would unload the existing MIB in the tree. Select the unwanted MIB, click on the **Unload** button. A confirmation dialog box would turn up, to get confirmation from the user to remove the selected MIB. Click the **Yes** button to proceed.

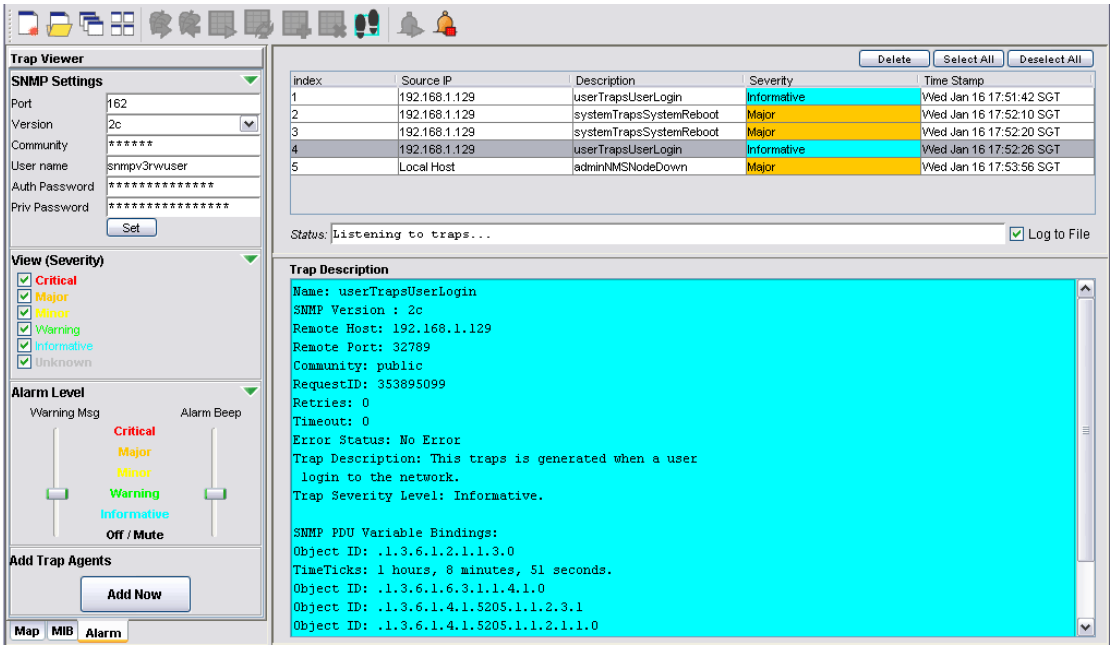


4.3.27 Alarm Table

The *Alarm Table* of the *EnGenius Mesh Network Management Tools* enable user to check on the traps and notifications caught by the trap receiver. The entries are read-only, and shall be deleted once they were resolved or reviewed.

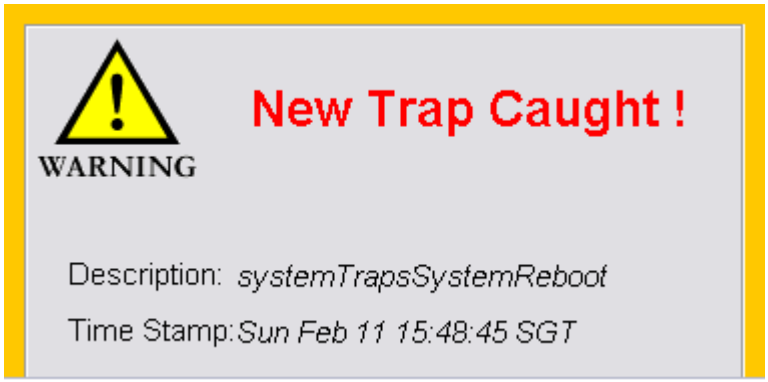
In order to start listen to the traps, hit the **Start** button at the toolbar or select *Settings > Start Trap* from the menu bar. Select the **Stop** button, or *Settings > Stop Trap* to stop the trap listener. User can change the SNMP Trap community or passwords at the available columns and hit the **Set** button. The checkboxes at the bottom of the settings section are the table filtering options. Clear the selection of the checkbox to hide the relative entry in the trap table. Each level of severity is represented by a different color.

Select any entry from the alarm table, its description will be displayed at the *Trap Description* area at the bottom of the table. If you wish to remove the selected entry, click on the **Delete** button.



The Alarm Level area is to enable the user to determine the level of the warning message popup and the alarm beep sound. User may drag the slider to alter the level. For instance, drag the slider of the warning message to *Minor*, the warning message would not popup if the level of the alarm received is *Warning* or *Informational*. The

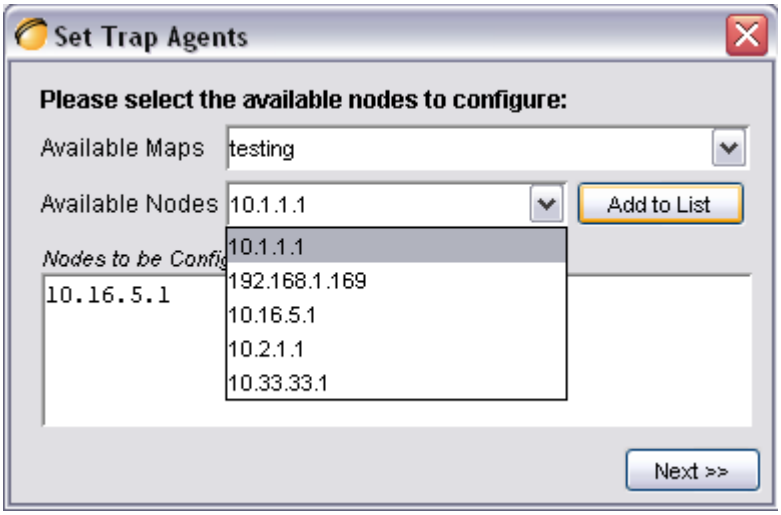
following figures illustrate the example of Warning Message, which will be displayed at the left bottom corner of the screen when the trap is received.



4.3.28 Add Trap Agent

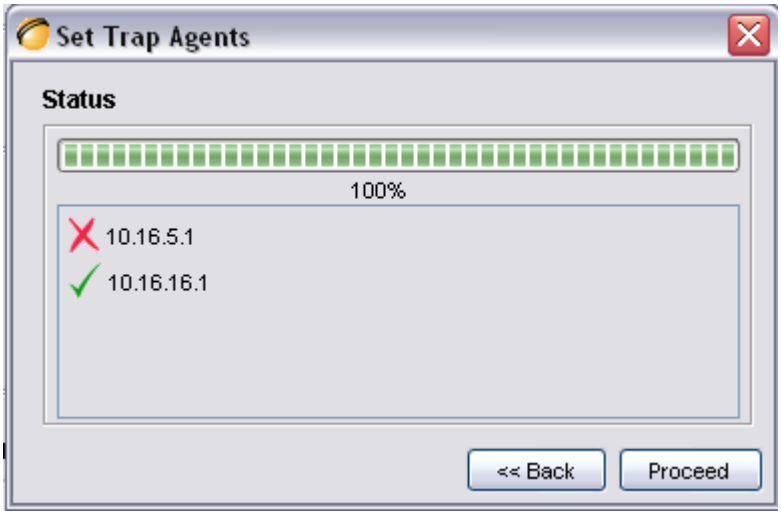
This feature is a wizard window, intended to assist the user to set one, or more than one node to be the trap agent of the host system at the NMS, simultaneously.

Hit the **Add Now** button at the trap viewer mode, to invoke the wizard. At the first page of the wizard, user will be prompt to enter the IP Address of the desired nodes, to be set as alarm agent. User can enter the IP Address manually, or select from the drop down list provided. Click **Next** to proceed.

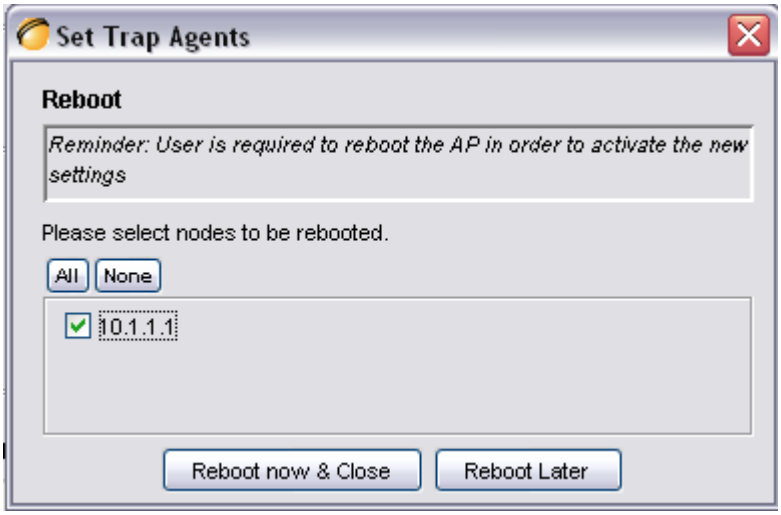


Then, enter the required SNMP keywords, such as version and community. Click **Set** to proceed or **Back** to back to the first step.

Once the configuration is done, click **Proceed** button to proceed to reboot page, or **Back** to the previous page.



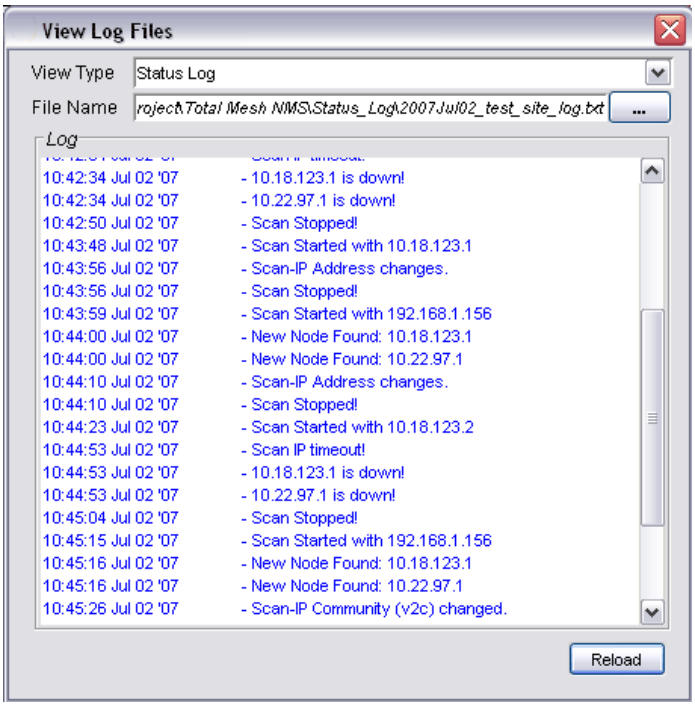
If **Proceed** is pressed, the following page will be displayed. User may select the IP Address of the node configured just now to be rebooted. In case if user is wished to reboot the device manually afterwards, click **Reboot Later**. On the other hand, hit the **Reboot now & Close** button to start reboot the devices.



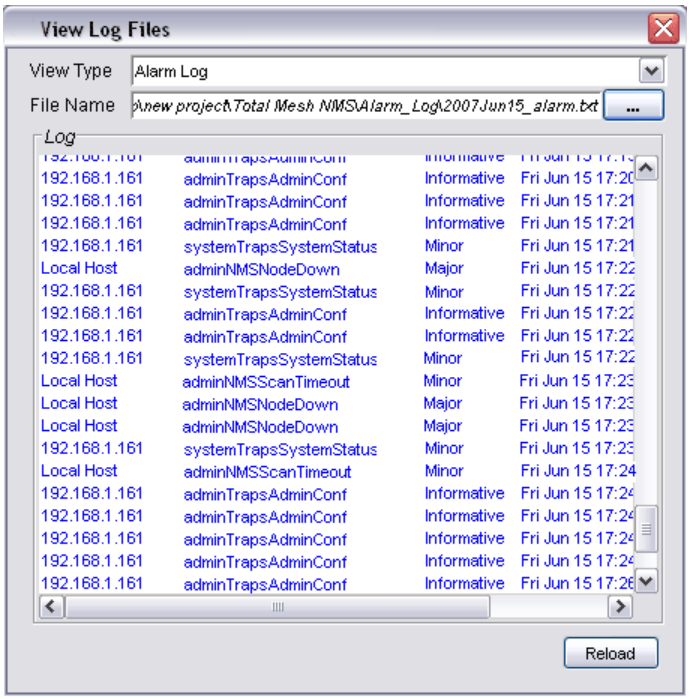
Once the AP unit is rebooted completely, it will contain the information of the Alarm Host System in the NMS. Hence, it will redirect the alarm message and notification to the NMS when there is any.

4.3.29 View Log Files

There is a feature in the NMS allow the user to back-track the log files of the system. Select *View > View Log Files* from the NMS menu bar to invoke a new dialog box, as shown at the following figures.

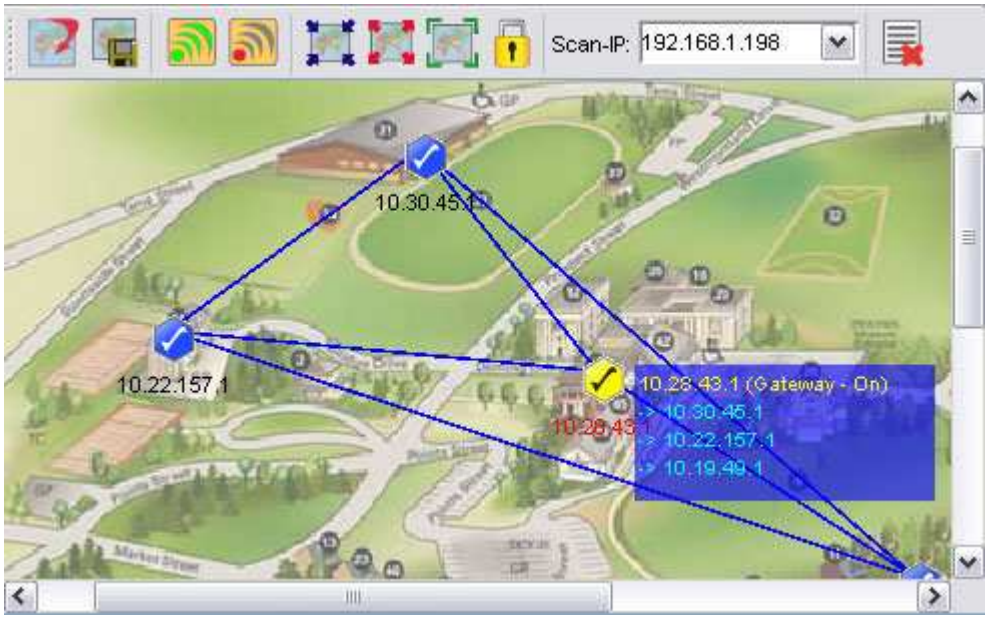


Then user can select the type of log to view, including Status Log and Alarm Log. Key in the desired file name, or hit the button next to the column to select the file, and select the **Reload** button to load the content of the file.

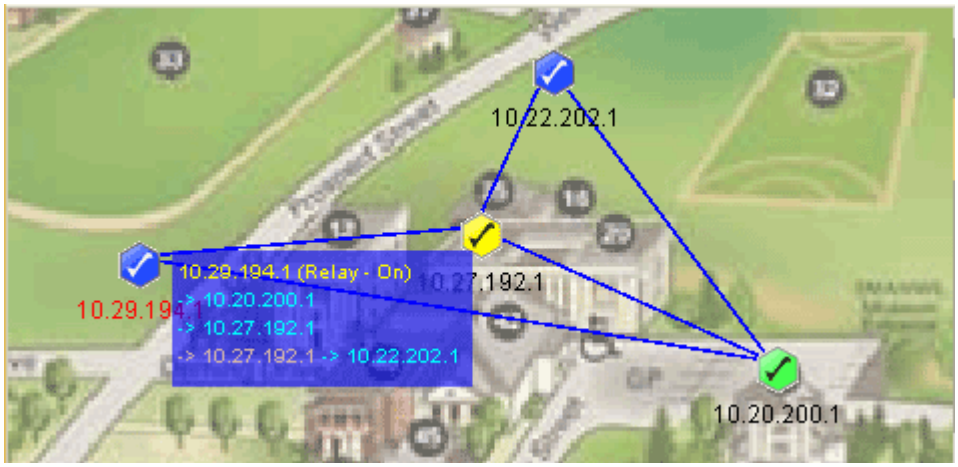


4.3.30 Show Route

When user moves the mouse over the plotted AP unit on the topology map, a small blue dialog would appear on the screen, displaying the routes of the selected unit. The route describes how the AP link to the other nodes in the same mesh network, as illustrated by the figure below.

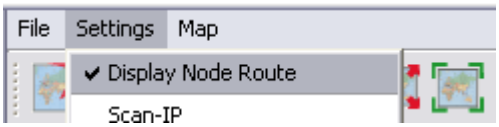


The figure above shows the node 10.28.43.1 is currently connected directly (in blue font) to 10.30.45.1, 10.22.157.1, and 10.19.49.1.



Whereas the figure above illustrates how the routes are displayed when nodes are not directly connected. From the example, node 10.29.194.1 and 10.22.202.1 are not directly connected. Instead, the connection between them is established via node 10.27.192.1 (red color font), according to the route box.

If user would like to disable this feature, please select *Settings > Display Node Route* from the map container menu bar.



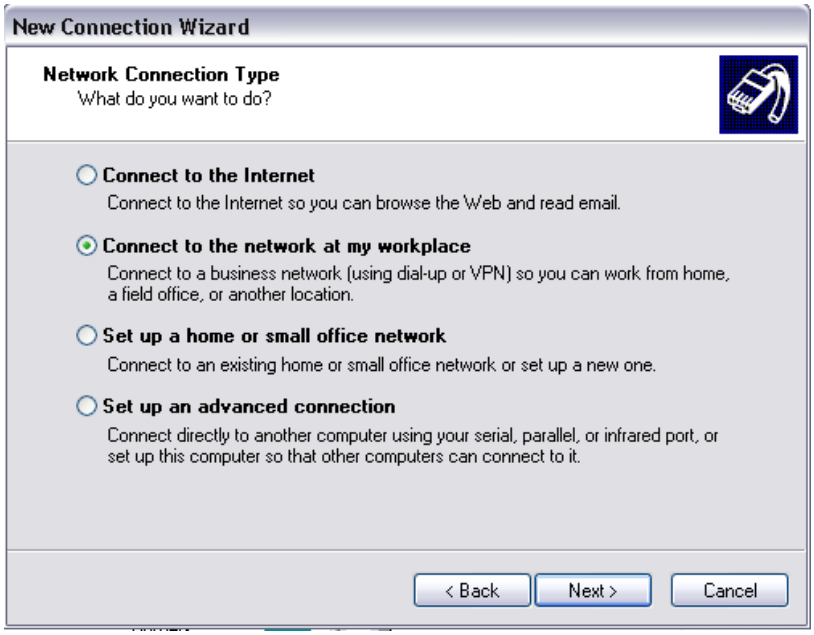
4.3.31 Create VPN Connection (Layer-3 Map)

If user would like to scan a network through the backbone line (WAN), a VPN Connection is required in order to create the communication link between the NMS and the Mesh APs discovered through a VPN Server.

To create a new VPN Connection, use the *New Connection wizard* of Windows. In order to start-up the wizard, open the *Network Connections* Page (*Start Menu > Control Panel > Network Connections),* then select *New Connection Wizard*. When the wizard turn up, follow the following steps to do the set up: (*refer to the following screen shots)

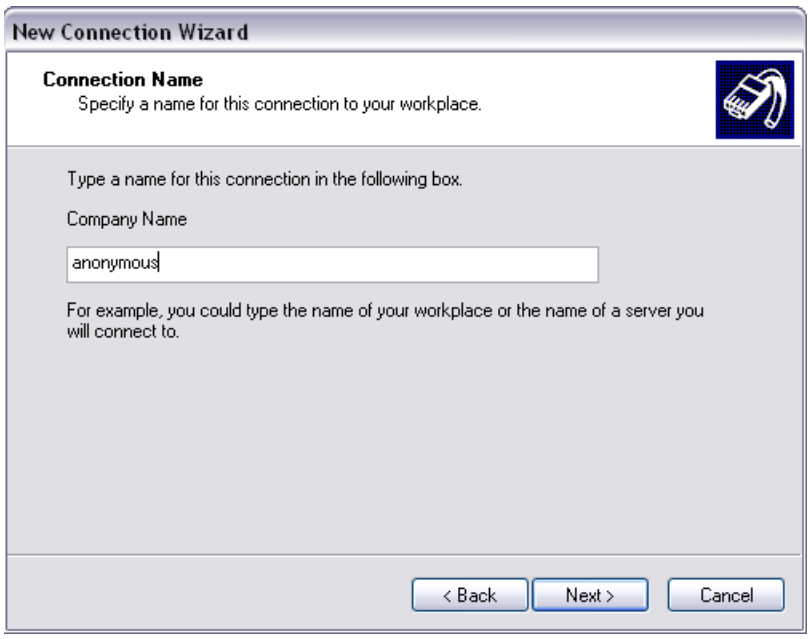
- Introduction – Welcome page of the wizard

- Network Connection Type – Select *Connect to the network at my workplace* and click **Next** button



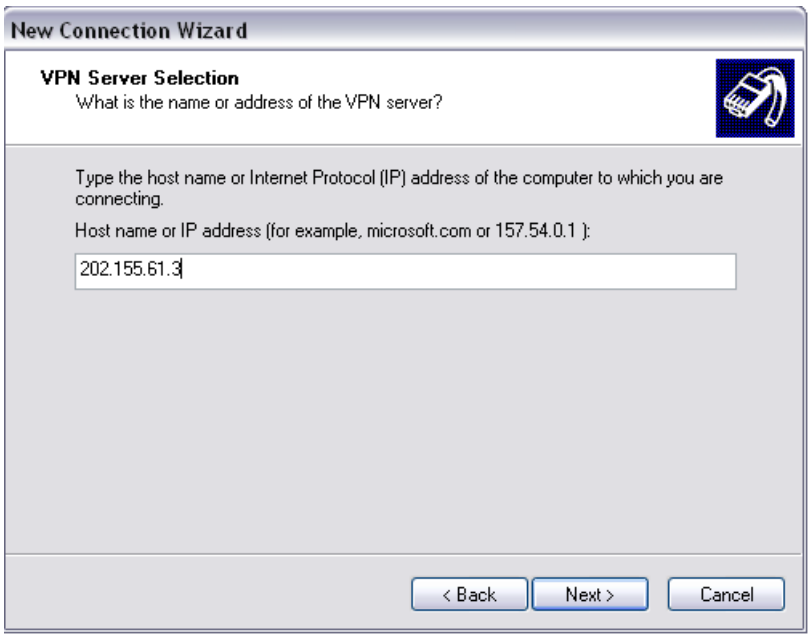
- Network Connection – Select *Virtual Private Network* and click the **Next** button

- Connection Name – Enter a desired Connection Name and hit the **Next** button



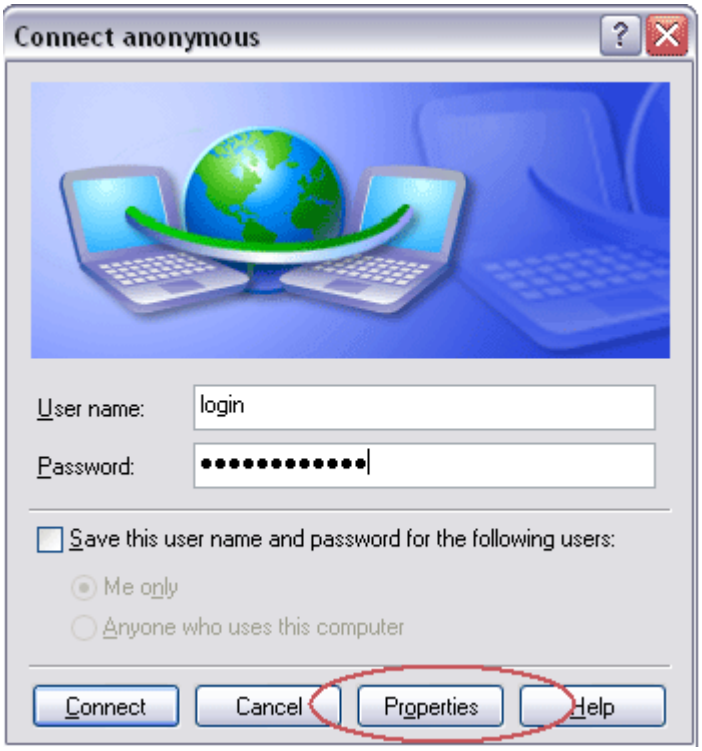
- Public Network – Select *Do not dial initial connection* and press **Next** button

- VPN Server Selection – Enter the host name or the IP Address of the VPN Server that you wish to connect, and click the **Next** button



- Complete – Click **Finish** to complete the set up

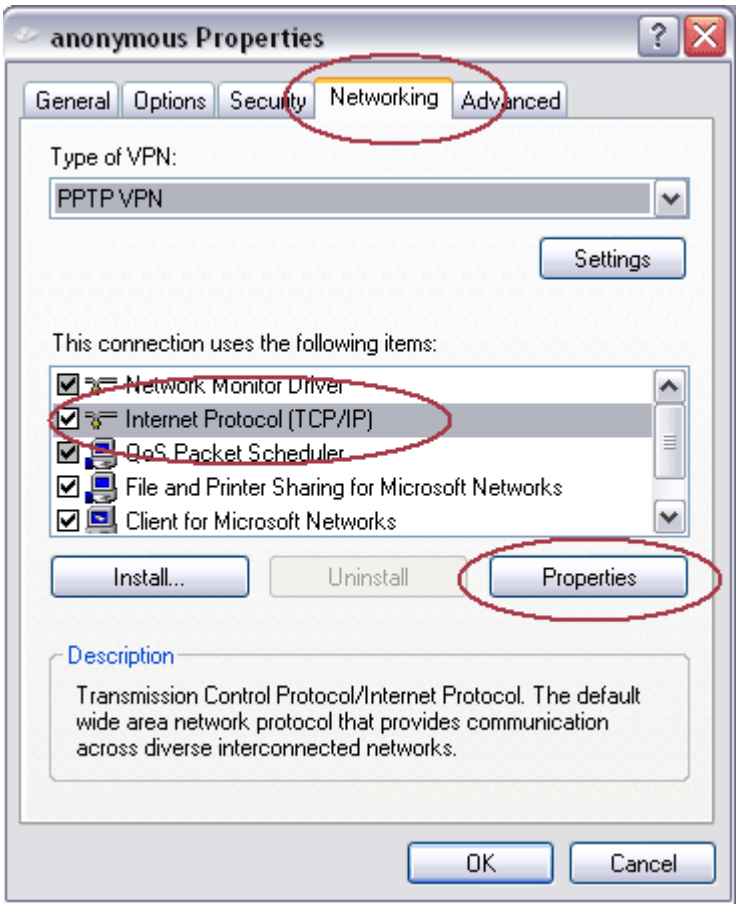
After the shortcut is created, user is required to go to the *Properties* page, by right-click on the shortcut icon, and then choose from the popup menu. Alternatively, it can be opened from the *Connect* page, as shown:

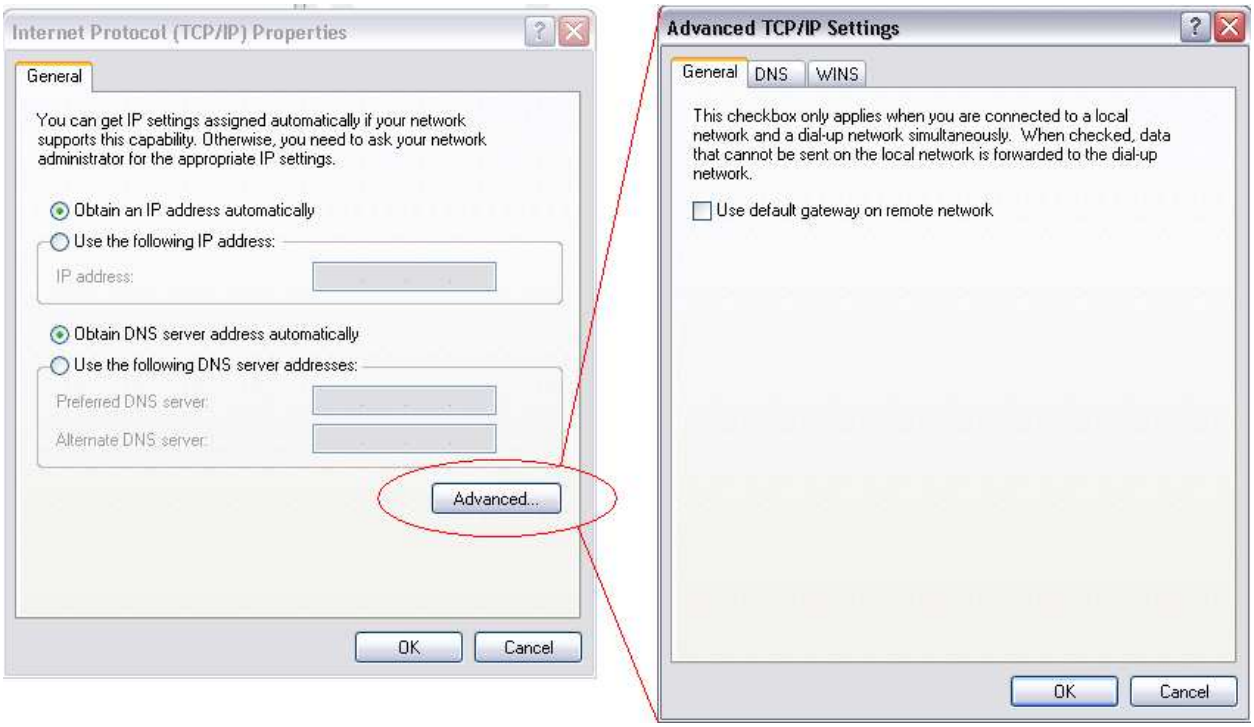


At the *Connection Properties* window, perform the following steps:

- Select the *Networking Tab* at the top of the page

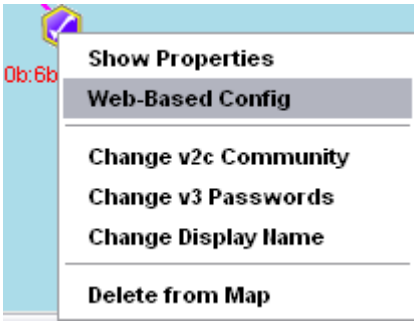
- Select the *Internet Protocol* (*TCP/IP*) from the available list
- Hit the **Properties** button to configure the item's properties
- At the TCP/IP Properties window, select the **Advanced..** button, another window (*Advanced TCP/IP Settings*) would appear.
- At this window, make sure the *Use default gateway on remote network* option is checked and click the **OK** button.





4.3.32 Configure Mesh Aps

User is able to configure the Mesh AP unit remotely with the NMS thru Web-based Configuration Page. In order to invoke the config page, right click on any of the active Mesh AP unit on the topology map (gateway or relay). A popup menu would appear, as shown:



Select the *Web-Based Config* option. The following figure shows the screenshot of the Web-based Configuration page.

4.3.33 Discovery Tool

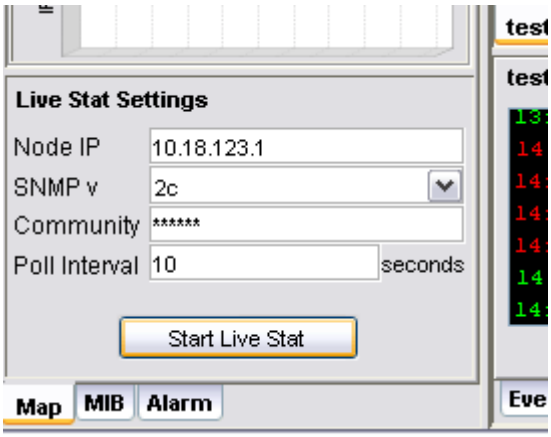
The discovery tool is an advance feature added to the NMS. Its main function is used to discover the recognized AP unit locating in the same subnet. Hit the **Discover** button at the bottom to initiate the scan. The APs found throughout the process will be displayed on the table.

User may click on the entry on the table to view the information regarding the AP, such as system name, MAC address and so forth. Further more, the selected unit can be configured by using the button at the top of the **Discover** button, to open the Web-based configuration page.

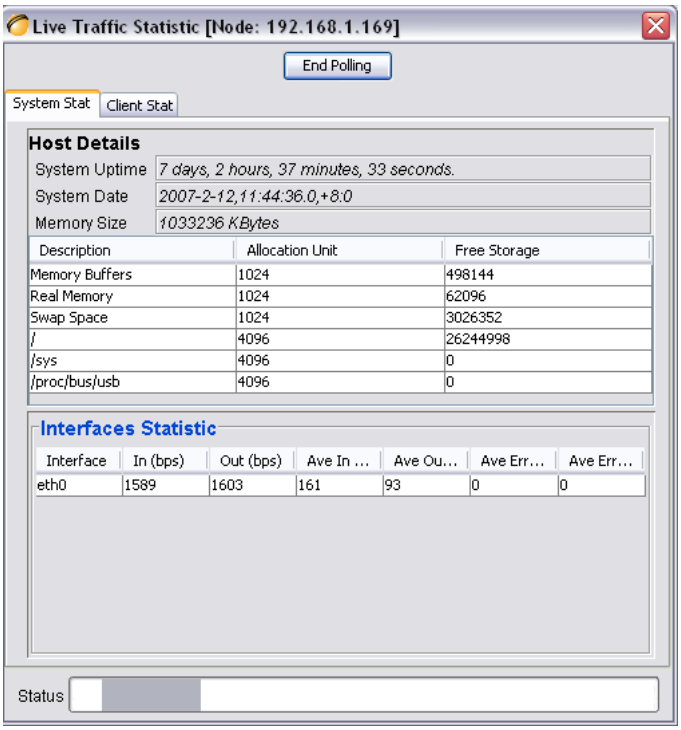
4.3.34 View Interface and Client Live Statistic

This feature provides user a graphical and readable statistic table regarding the target Mesh AP unit. The information that monitored by the live stat portion includes the interfaces throughput, clients' throughput, as well as the memory status.

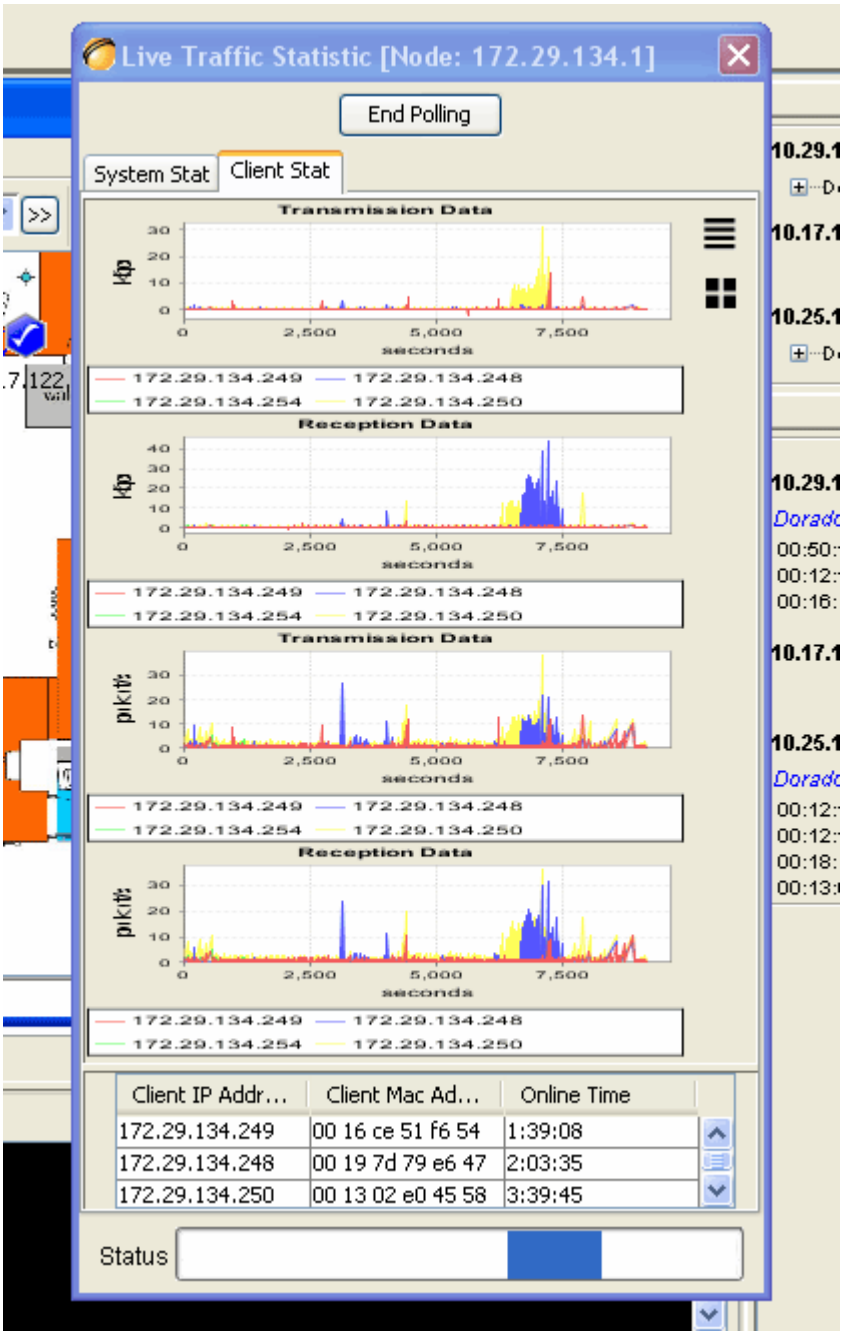
In order to invoke the live stat window, switch the NMS to the Map Container view, and then look for the Live Stat Settings portion at the left bottom corner. User may enter the IP Address of the target node (or just click on the node on the map to load the IP) to be monitored, and its corresponding SNMP Key. Hit the **Start Live Stat** button to initiate the window.



At the popup live stat window, click the Start Polling button at the top to start the live stat. The window consists of two parts: the System Stat and the Client Stat. The System Stat page displays the memory status of the system and the statistic of the interfaces throughput. The table will be updated at a certain interval, which is set by the Poll Interval field at the Live Stat Settings corner.



The second page shows the throughput statistic of every client that associated to target node. The results of the transmission and reception data packet rate are displayed in the form of graph. The table at the bottom of the graphs tabulates the client list with their respective MAC Address and online time. To stop the polling process, click the **End Polling** button at the top.



4.3.35 Logout Client

At the latest version of the NMS, the administrator is able to log out and block the user from accessing the network, by using the **Logout and Block user** button at the Live Stat Window

In order to remove the client, user must run the Live Stat Window. In the Client Stat portion, the table at the bottom lists the client that has log on to the network. Select the client (Mac Address) that to be removed, and hit the **Logout and Block user** button.

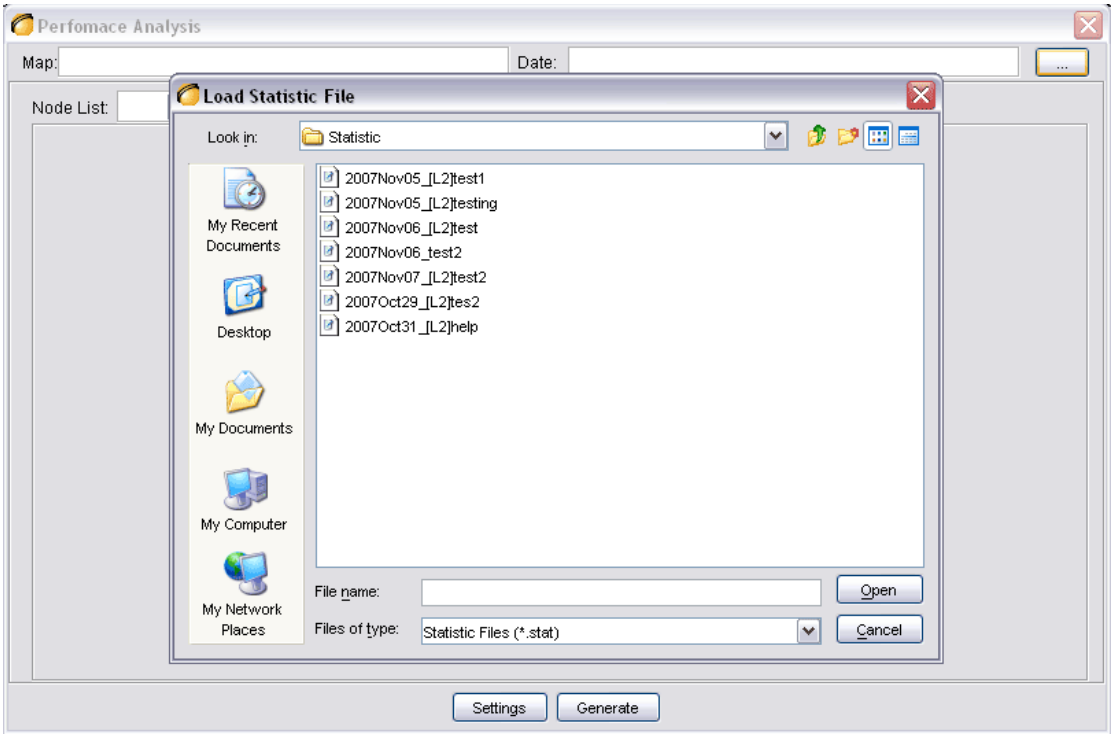
A window would appear on the screen to prompt user for the SNMP version to use and its corresponding community or passwords. Click the **Block User** button once completed the step, and the selected client will be removed from the active client table, and added into the MAC Access Table.

4.3.36 Performance Analysis

Since version 2.3, the feature of generate a performance summary of the network have been added into the NMS. The network analysis is generated automatically once a topology map (SNMP or Layer-2) is initiated. The reading will be refreshed at a certain interval.

In order to open the analysis report of the running topology map, select *File* > *Performance Analysis* from the map menu bar. The figure below illustrates the performance analysis:

On the other hand, if user wishes to view the reports saved previously, select *Advanced > Performance Analysis* from the NMS menu bar. Hit the "**…**" button on the top to explore the desired file from the statistic directory. Choose the desired statistic file, and hit the **Generate** button to update the window.



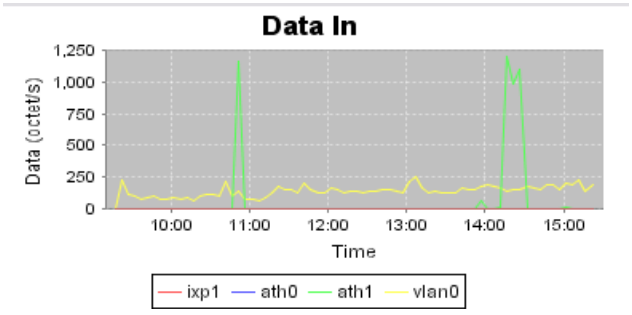
The following information that capture by the report:

1. Neighbour nodes signal strength
2. Client signal strength
3. Data throughput (In & Out)
4. Node Status
5. Memory Status and Uptime

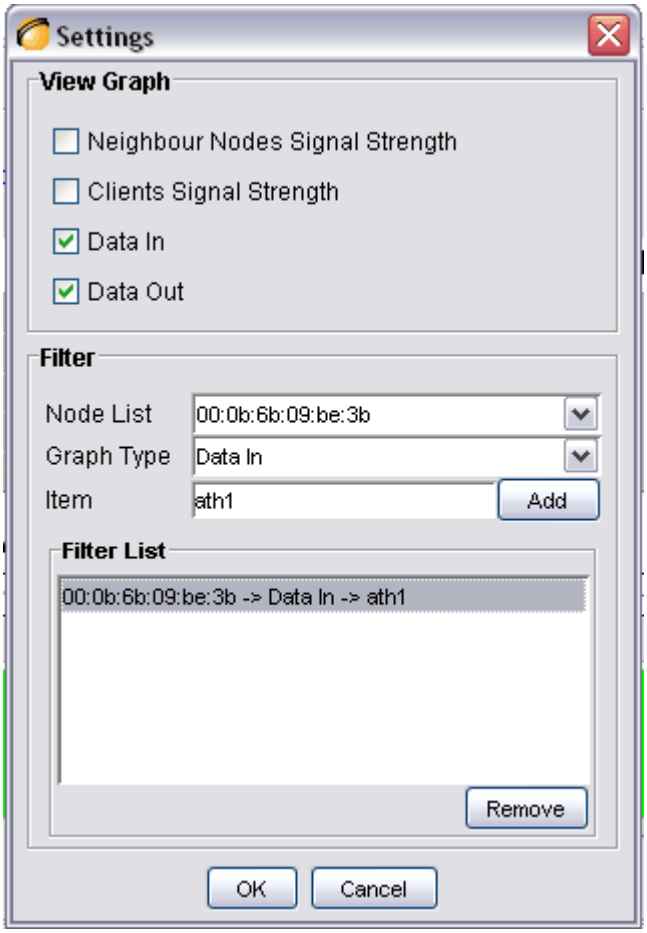
Use the drop down list on the top to view the analysis of another node.

The **Settings** button of the performance analysis enable user to edit the view of the graphs in the window. User can decide to hide or show the information, and use the filter list to filter the unwanted data.

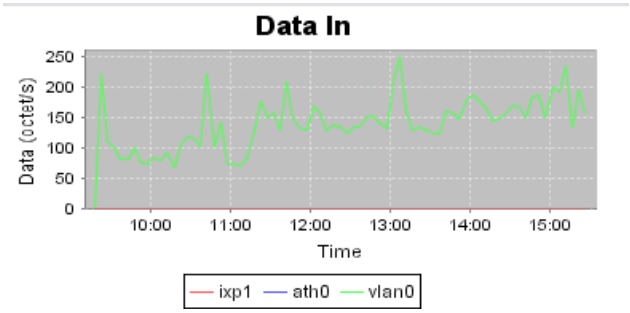
For instance, given the *Data In* graph of node *00:0b:6b:09:be:3b*,



In order to remove the *ath1* line from the graph, open the setting window. At the filter portion, choose the node name (*00:0b:6b:09:be:3b* in this case) from the drop down list. Next, select the graph to filter, which is *Data In*. Then, key in the item to be filtered, which is "*ath1*", in the Item field. Once completed, click the **Add** button, and press **OK** to load the settings.



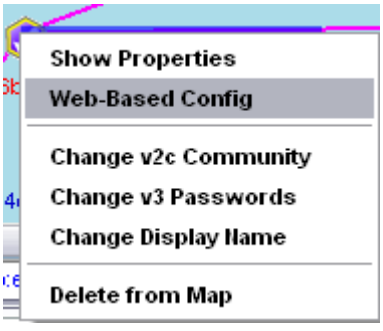
The line of "*ath1*" has been hidden and the graph would look like this now:



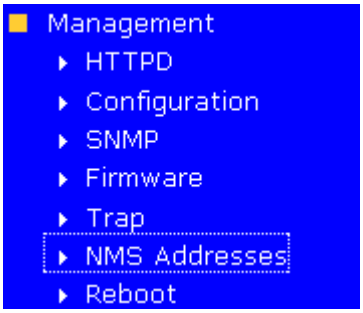
4.3.37 Setting NMS Addresses

In order for the Layer-2 map type to receive notification packet from the node, user is require to configure the *NMS Addresses* table at the configuration page. This table defines the destination of the notification. By adding a new entry, with the IP Address and port number of the NMS, into the table, the AP would redirect a notification to the specific NMS, in the defined interval. This table applies to every operating mode of the AP.

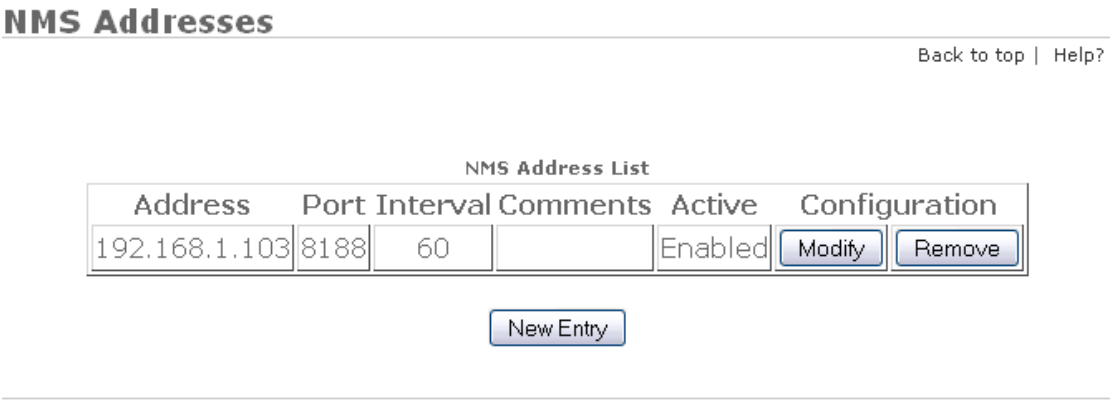
In order to access to the NMS Addresses page, firstly, user would need to open the Web-based configuration page. A method to run the page would be right-click the nodes on the map, and select the *Web-Based Config* option from the menu.



Then your web-browser will be redirected to the configuration page of the selected node. Enter the admin username and password, and then choose *Management* > *NMS Addresses* from the menu.

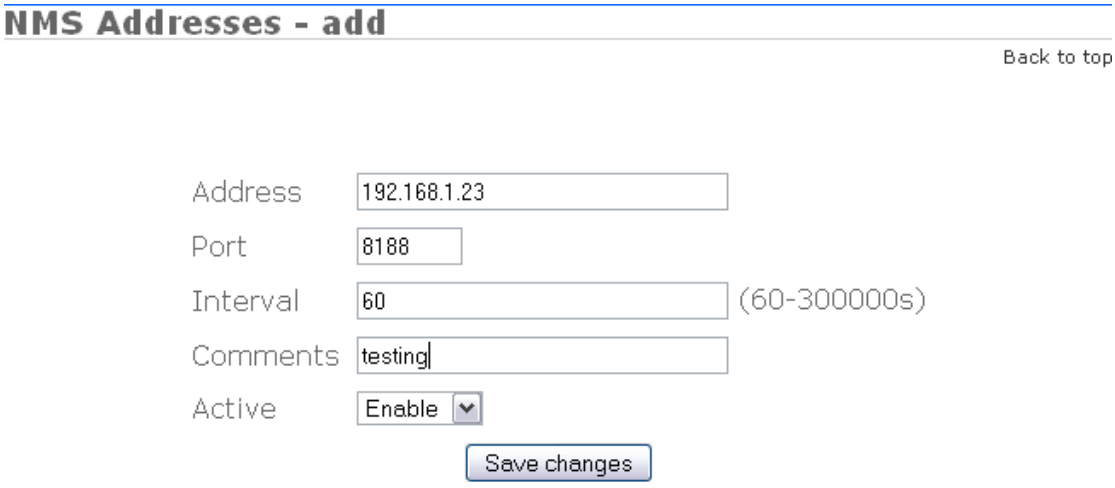


And the *NMS Addresses* page will be loaded into the browser.



Press the **New Entry** button, and key in the following details at the add-entry page:

- Address – The IP Address or Host name of the system which running the NMS.
- Port – The port bind with the Address to receive the notification from the nodes. Default value: 8188
- Interval – The resend interval of the notification, in seconds. Default value: 60
- Comments – An optional comment regarding the table entry.
- Active – The status of the table entry. Select *Active* to activate the table entry.



Click the **Save changes** button, and the NMS should be able to receive the notification from the configured node.

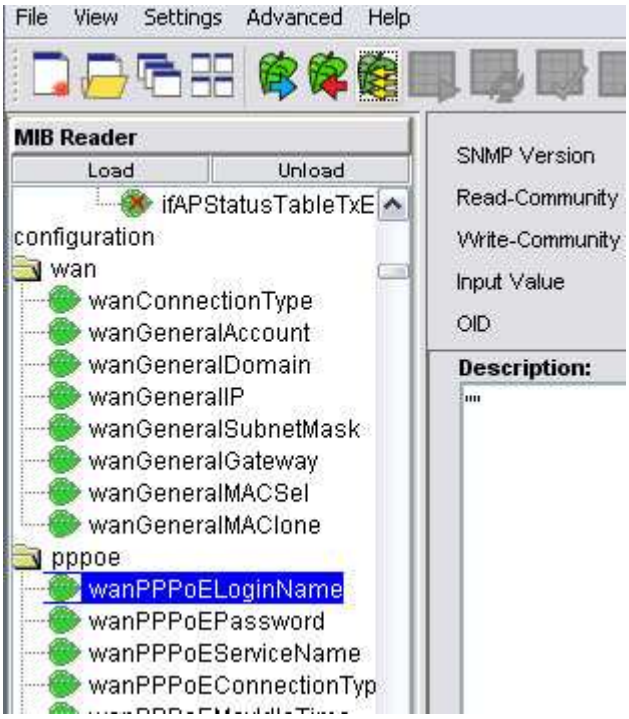
4.3.38 Synchronized-Configuration

The synchronized-configuration is a feature that enables the user to perform SNMP Set on more than one device simultaneously. However, this feature can only be applied to parameters that have **Read-Write** accessibility from the MIB file.

Step-by-Step Guide to Synchronized-Configuration

1. Switch the NMS to MIB-browser mode.

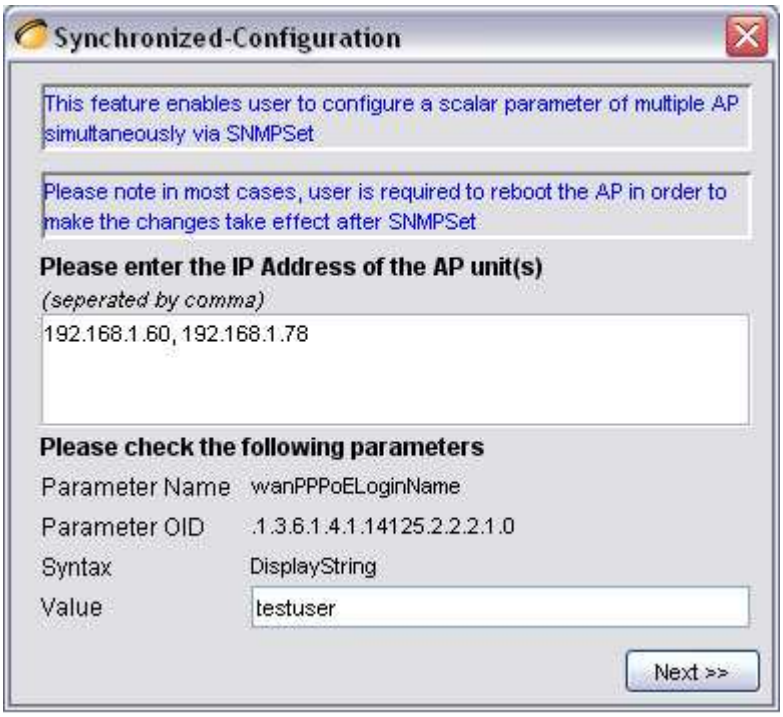
2. Expand the MIB tree and get a desired scalar parameter (Read-Write).



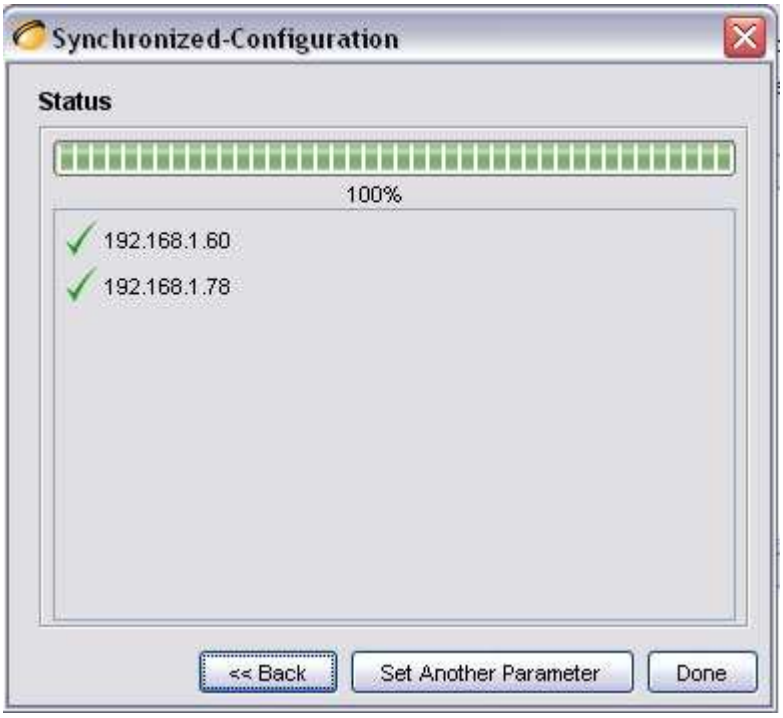
3. Click on the **SNMP Synchronized Configuration** button on the toolbar, to invoke the Synchronized-Configuration Window.

4. At the popup window, enter the list of IP Address of the AP that will be configured. (separated by comma)

5. Enter the desired value in the *Value* text-box, and hit the **Next** button.



6. Enter the appropriate SNMP password / community based on the SNMP Version using. Click the **Set** button.

7. A status page will be shown, displaying the result of the synchronized-configuration. Hit **Done** to close the window, or else, click the **Set Another Parameter** button, to go back to the first page of the configuration, where

user can select another parameter from the MIB-tree at the MIB Browser, and repeat the steps.