SolarWinds LANsurveyor
Administrator Guide

Table of Contents

Introduction

Welcome

Thank you for purchasing SolarWinds LANsurveyor. LANsurveyor is network management software any network manager, administrator, engineer, or designer can use to automatically diagram networks of any size. The LANsurveyor map provides a graphical interface so you can manage your network from anywhere on the network.

With LANsurveyor, you can:

- draw a map showing the logical connectivity of your entire network
- make queries of network objects for such information as Simple Network Management Protocol (SNMP) data, Responder client data, and data from EMC Dantz's Retrospect Client
- add icons to your map to represent network objects
- be alerted when a new devices is added to your network
- launch other applications using the map as an interface
- create reports about any items on the map
- scan your network for intruders using one or more maps as the baseline and automatically disable network access for rogue nodes

With LANsurveyor's Responder client add-on, you can:

- manage remote Windows, Linux, and Mac OS nodes from the LANsurveyor map, including starting and stopping applications, distributing files and folders, restarting and shutting down, and synchronizing clocks
- help you plan your backup and disaster recovery strategy

Package Contents

- LANsurveyor CD-ROM (optional)
- User's Manual

Please register your software electronically. Registered users receive information on free updates and upgrade availability, and only registered users can receive technical support.

Compatibility

To use LANsurveyor, you must have the following:

- A Pentium-class computer with 256MB memory
- Windows 2000, XP, 2003, or Vista (professional, workstation, or server editions)
- A connection to an IP-based network

Additionally, some LANsurveyor features require the following:

- Responder client software add-on installed on nodes for reports and client management.
- nodes that understand SNMP (called "SNMP Agents") and the community string (or password) for SNMP devices you wish to report on. Some of the SNMP Agents used by LANsurveyor are:
  - MIB-II SNMP agents that exist on nearly all IP routers and many IP devices.
  - Printer MIB SNMP agents that exist on some IP printers.
  - Bridge MIB SNMP agents to determine switch port connectivity.
  - Repeater MIB SNMP agents to determine hub port connectivity.
- Microsoft SQL Server or Microsoft SQL Server Express to store SNMP configuration and Responder client information in LANsurveyor's Repository.

Install LANsurveyor

Software Download

Download the software from your SolarWinds account and double-click on the LANsurveyor .msi installer to begin installation.

CD-ROM

Insert the LANsurveyor CD-ROM into your computer. The installation application should automatically start. If not, open the file "setup.exe" to begin the installation process. Check the "Please Read Me.doc" file for the most recent information and last minute documentation updates.

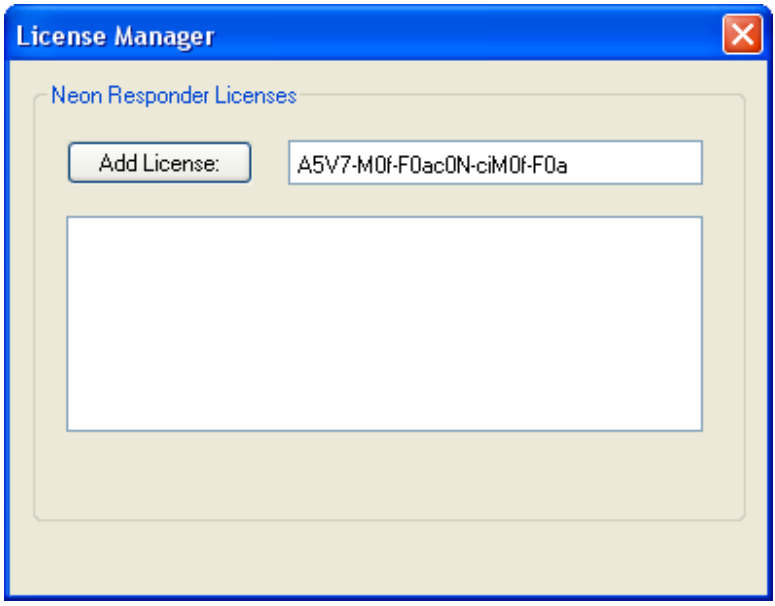
Install Responder Clients

Your LANsurveyor Installation includes the Responder client add-on installers for Windows, Linux, and Mac OS computers. Some of LANsurveyor's most advanced reporting and management features require the Responder client add-on to be installed on network computers, and systems with a Responder client can have their hardware and software asset data automatically stored in LANsurveyor's Repository.

Contact SolarWinds or your reseller to obtain add-on licenses.

Install Responder Client License

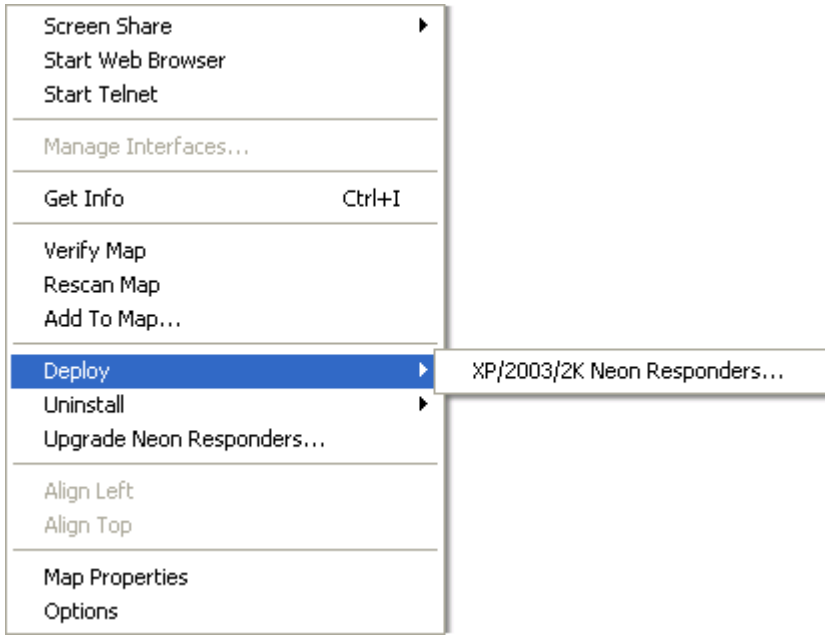
Use LANsurveyor's License Manager to install the Responder client add-on licenses. Select **License Manager** from the **Window** menu then enter your Responder client license code.



Deploy via Directory Services

You can deploy Responder clients to 2000, XP, 2003 and Vista-based Windows computers through Remote Procedure Call and Remote Registry services using a directory service such as Active Directory. To deploy using Active Directory, log into the LANsurveyor computer using an account in an Active Directory administrative group (Domain Admins or Enterprise Admins). When you create your map, LANsurveyor will prompt you to deploy your Responder clients.

If you have already created a map (or declined to deploy when first prompted), select **XP/2003/2K/Vista Neon Responders...** from the **Tools>Deploy** menu. The Deploy Responder client wizard is displayed, allowing you to select the appropriate computers and the schedule for deployment.



Tip: If you're having difficulty deploying via Directory Services, configure your Windows workstations as follows:

- Ensure that the Remote Registry service is running
- Ensure that the RPC service is running
- Turn on file and print sharing service and configure your workstation firewall to allow connections to UDP 137, UDP 138, UDP 445, and TCP 139, and TCP 445 ports

Deploy Manually

You can copy the client installation software to any system (or to a central server) for local installation. All supported Responder client installers are included in folders in the LANsurveyor installation directory (e.g., "Linux Neon Responders").

There are two Linux installers: rpm for RedHat based systems and deb for Debian based systems. Refer to the "nrlinux-readme.doc" file in the folder for up-to-date information on installing Responder clients on Linux systems as well as supported systems.

If you deploy the Responder client manually, you will need to password protect your Responder client using the Manage wizard.

Upgrade Responder Clients

Other than manually using the installation software on each computer, LANsurveyor provides two methods for automatically upgrading Responder client software on your workstations and servers.

Upgrade Responder Clients Wizard

The easiest method is to use the Upgrade Wizard. Select **Upgrade Neon Responder...** from the **Tools>Options** menu, and the wizard will upgrade all Responder clients on any open LANsurveyor map to the latest revision.

There are five steps in the wizard:

- Select the name and location for a Microsoft Excel-format file that will contain the current status of each node during the upgrade process (optional)
- Determine whether systems that require restart should be automatically restarted to complete the upgrade
- Compose an instant message that will be sent if a restart is necessary so users can be prepared for the restart
- Specify retry frequency and number of days to try to upgrade nodes that are offline and cannot be upgraded when the upgrade is executed
- Schedule the upgrade either immediately or at a specified time in the future

The upgrade process will automatically select the proper Responder client version to send to each workstation, only upgrade nodes that are running an older version of the Responder client, and save the status of the upgrade in a file (if you chose one in the wizard).

Send File Wizard

If you would rather upgrade only selected Responder clients, use LANsurveyor's Send File feature.

Select **Send File** from the **Manage** menu to start the three step wizard:

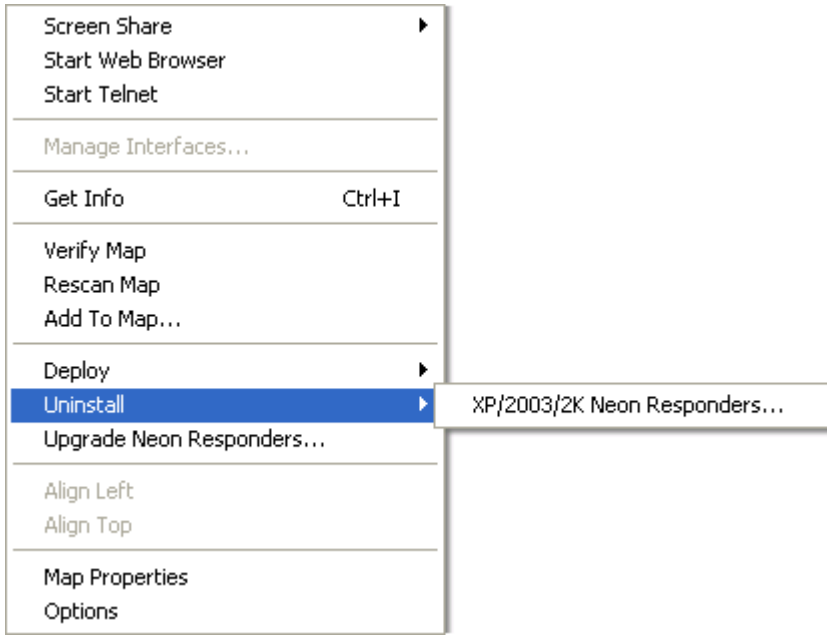
- Select the computers you want to upgrade from each map
- Use the browse button to select the Responder client upgrade file and select Responder client from the Destination pull-down
- Schedule the upgrade either immediately or at a specified time in the future

The Responder client upgrade files are located in the "Neon Responder Updaters" folder in the LANsurveyor application folder. There are different files for the different OSes supported.

Once the wizard completes, you need to either restart the Responder client service (Windows NT/2K/XP/Vista), restart the computer (Windows 95/98/ME and Mac OS), or log off the current user and log back in (Mac OS X) to load the upgraded software.

Remove Responder Clients

You can uninstall Responder clients from 2000, XP, 2003, and Vista-based Windows computers through a directory service such as Active Directory. Log into the LANsurveyor computer using an account in an administrative group (Domain Admins or Enterprise Admins for Active Directory) and open a map with the computers that have the Responder clients installed.



Select **XP/2003/2K Responder clients...** from the **Tools>Uninstall** menu. The Uninstall Responder client wizard is displayed, allowing you to select the appropriate computers and the schedule for the removal.

Manually Remove Responder client

Windows Systems

You can also remove Responder clients manually. For all Windows systems, you can use **Add or Remove Programs** in **Control Panels**. The Responder client software will be uninstalled.

Since the Responder client runs as a service on Windows XP/2003/2000 systems, you can also launch **Computer Management** from the **Administrative Tools** Control Panel. Then pick **Services** from **Services and Applications**. The Responder client service should be displayed among the other running services in the right window. Get **Properties** for the Responder client service and from there you can **Stop** the service and change **Startup type** to disabled. Finally, you can see where the executable is on your disk in the **Path to executable field**.

Linux

Use either rpm or deb to uninstall the Linux Responder client. The uninstall process will also stop the Responder client if it is currently running.

For rpm based installations, use: rpm -e neonresponder

For deb based installations, use: deb -P neonresponder

Mac OS X

Run the Responder client installer software and choose the **Uninstall** option.

Mac OS 9 and earlier

Drag the Responder client extension to the trash can and restart the system.

Notes:

Draw a Map

Start LANsurveyor

LANsurveyor launches exactly like any other application: just double-click on the LANsurveyor icon or on the icon of any LANsurveyor document.

The first time you use LANsurveyor, personalize your copy of the program. Enter your name and serial number in the appropriate text boxes. The serial number is case sensitive and must be typed exactly as you received it.

Once you personalize your copy of LANsurveyor, LANsurveyor prompts you to set your default authentication preferences. At a minimum, we recommend you set your SNMP community string(s). Otherwise, your LANsurveyor map will show neither connectivity outside LANsurveyor's subnet nor managed switch and hub connectivity.

Note: Make sure ICMP Ping requests and responses are allowed in your firewall and the network policy configuration for the user logged into the system running LANsurveyor.

Create a New Map

Once you personalize your copy of LANsurveyor, the Create A New Network Map dialog is displayed. LANsurveyor automatically builds a map of your network by searching for network objects, such as routers, networks and end nodes.

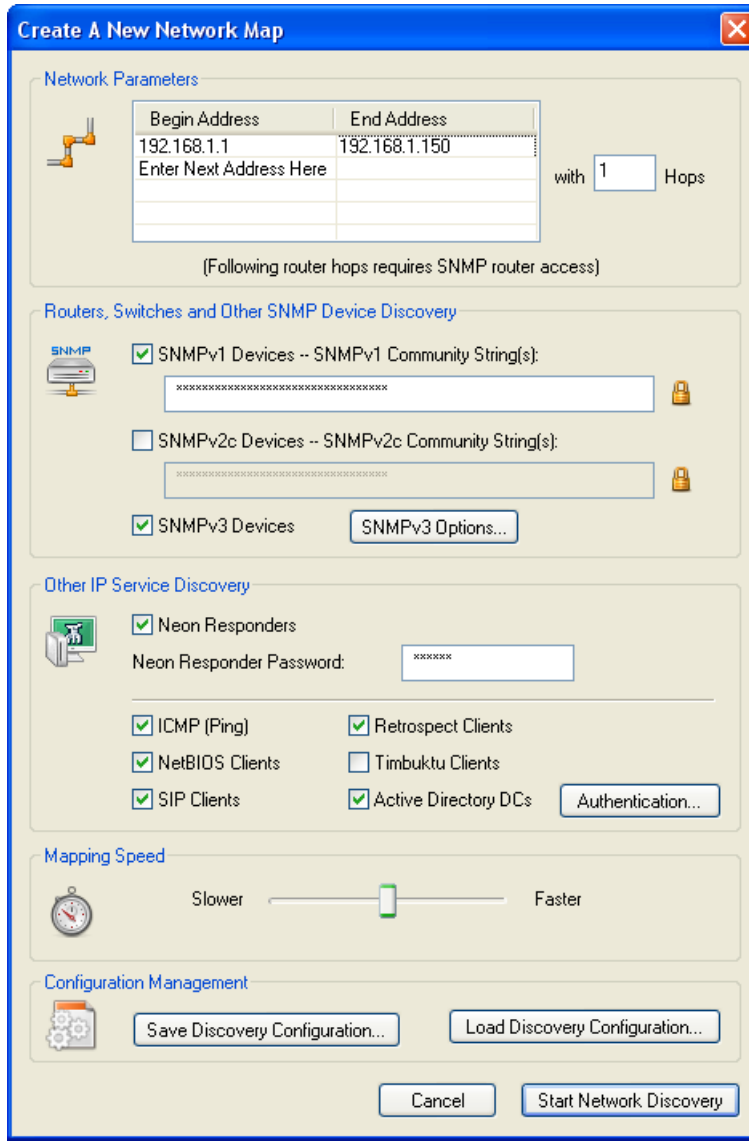
LANsurveyor incorporates a number of different discovery and query methods in order to provide you with the most complete and accurate map possible, including ICMP (ping), SNMP, NetBIOS, SIP, CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol), and installed client software, including our own Responder client software.

Note: Make sure you license and install the Responder client add-on if you want to use LANsurveyor's remote management features or the Windows, Macintosh, and Linux asset management. If you are in an Active Directory environment, you may deploy Windows Responder clients automatically after the map is created.

Select which items you would like to include on your map:

- IP Address Range
- Hops
- SNMP Devices
- Responder clients
- ICMP (Ping)
- NetBIOS
- SIP Clients
- Retrospect and Timbuktu Clients
- Active Directory Domain Controllers

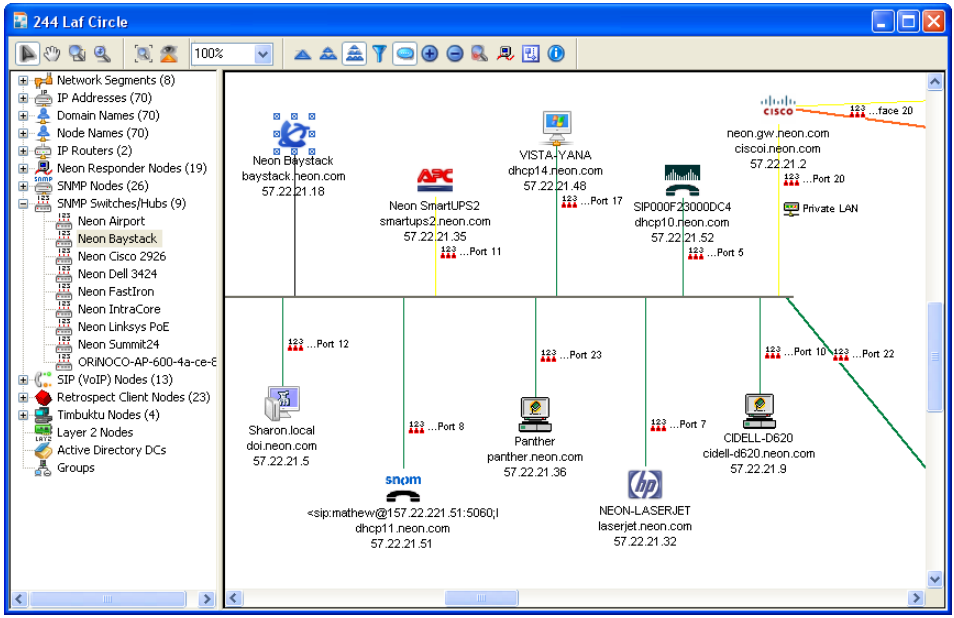
and the mapping speed in this dialog box:



After you have chosen your options, click Start Network Discovery to automatically build your network map.

You may build maps in parallel, and you can open any number of maps, even while a new map is being created.

LANsurveyor automatically builds the map:



- network requests are sent to discover nodes
- items that respond to more than one type of query (e.g., SNMP and ICMP) are merged
- IP addresses are assigned to each network object
- icons are assigned to each network object
- managed switch and hub ports are mapped
- SNMP interfaces are mapped
- networks and nodes are arranged

The map building and layout process may take a long time on large networks. Allow at least four seconds per ten IP addresses with all search options enabled.

LANsurveyor supports different map levels. Level 1 maps show routers, Level 2 maps show routers and switches. Configure your display preferences using LANsurveyor Level Options.

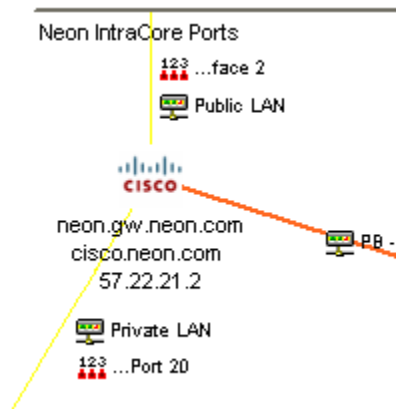
Add another IP address range to an existing map with Add to Map from the **Tools** menu, and keep your map up-to-date (and your network secure) with Continuous Scan.

IP Address Range

Enter the IP address range(s) of your network. This defines the scope of the search for the map. The default IP address range comes from the network settings of the computer running LANsurveyor.

Hops

LANsurveyor can also show connectivity between different networks (i.e., network segments separated by routers or "hops"). Enter the number of hops LANsurveyor should scan. You must have an SNMP-capable router and the SNMP community string to automatically discover connectivity between networks. LANsurveyor can also display each interface and the connected network segment.



SNMP Devices

You may include routers, printers, network attached storage (NAS), UPS systems, and other managed network devices on your map. Simply select SNMP and enter one or more SNMP community strings (or passwords) for the devices, separated by spaces or commas. Enter up to ten community strings and use the lock icon to hide the strings. If you do not know the community string, try "public", a common default access string.

Maps drawn without access to SNMP-based routers will not show connectivity between network segments.

Responder Clients

LANsurveyor's most advanced client reporting and management features are available using the Responder client add-on. Select the Responder client check box and enter your password to map and manage Windows, Linux, and Macintosh computers with the Responder client installed.

To change the Responder client password on remote nodes (or to add a password), select **Update Responder Passwords** from the **Tools** menu and follow the wizard.

The default Responder client password is stored with LANsurveyor's Network Options. Each map can also have its own Responder client password so you can have different passwords for different sites. Set the map-specific password in the Map Properties dialog box or when first creating the map in the Create a New Network Map dialog box.

There are several methods you can use to upgrade your Responder client software, as detailed in the Upgrade Responder clients section.

ICMP (Ping)

Some devices are not supported by Responder clients, do not support SNMP, and do not have supported third party client software. To increase your chances of including those nodes on your map, click the ICMP check box.

NetBIOS

Use NetBIOS to find network nodes running Microsoft Networking and include NetBIOS node names on your network diagram.

SIP Clients

LANsurveyor discovers and diagrams SIP-based Voice-over-IP (VoIP) devices, including telephones, video conferencing systems, and other SIP devices. Reports can include SIP devices and SIP-specific information, and the switch port report identifies exactly where SIP devices are connected to switches.

If your site uses a non-default SIP UDP socket, set your UDP socket number in the Network Options dialog box by selecting **Options** from the **Tools** menu and then selecting the **Network** tab.

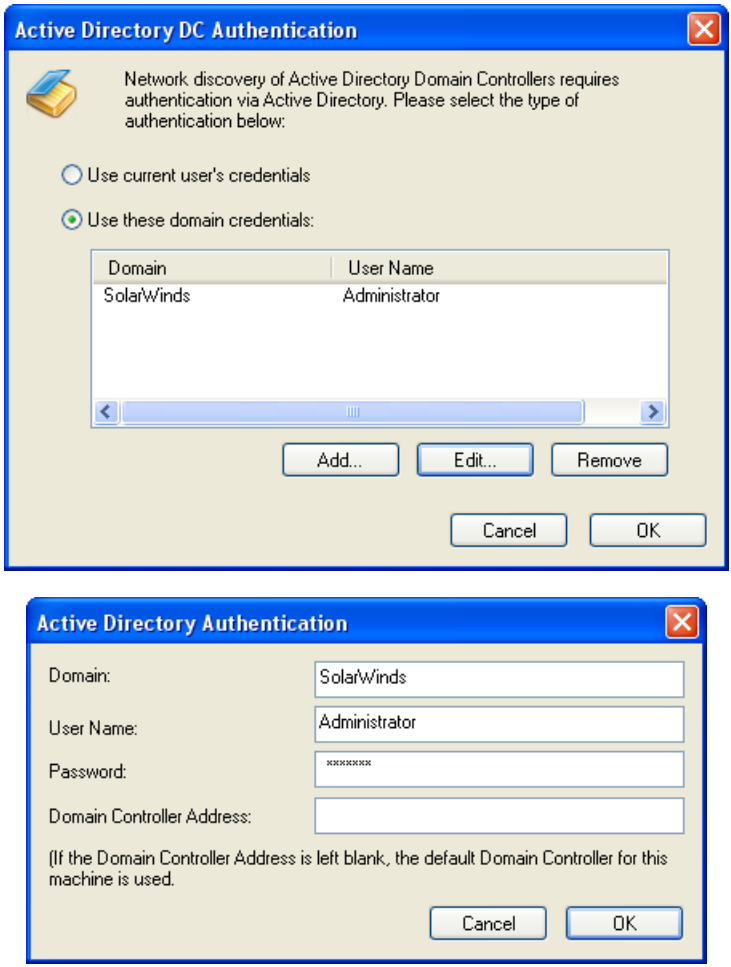
Retrospect and Timbuktu Clients

If you would like to include Retrospect or Timbuktu information on your map and in your reports, click the appropriate check box.

Active Directory Domain Controllers

LANsurveyor can map your Active Directory infrastructure onto the physical infrastructure of your network. If you want to view just your Domain Controllers and your infrastructure, use Filters.

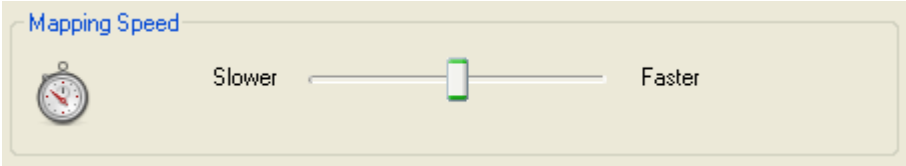
Click the Active Directory DCs option to discover the domain controllers on your network. By default, LANsurveyor uses the credentials of the person running LANsurveyor. If you want to use different credentials, click on the Authentication button then Add... to enter the credentials you would like to use.



Note: Active Directory only allows one user to be logged into a domain at a time from any given system. Therefore, if you are already logged into a domain as the LANsurveyor user and you would like to discover that domain, make sure that user has administrator access.

Mapping Speed

The mapping speed slider modifies the Network Timeouts, set in the Network Tab of the program options dialog box.



Slower devices and devices separated by several hops require more time to discover than faster, closer devices. Setting the slider to "slower" gives greater accuracy.

Mapping switch and hub ports also takes time. You can significantly speed mapping on large networks by if you uncheck the **Map switch/hub ports** option on the **Miscellaneous** tab of LANsurveyor's application preferences.

Troubleshooting Your Map

LANsurveyor maps include icons to represent your end-nodes and SNMP-enabled devices. If the map icons are generic "IP" computer icons, one or more of the following could be true:

- your devices do not support SNMP
- SNMP is not enabled on your devices
- you do not have the correct SNMP community string (password) for your SNMP devices
- your SNMP devices' access control lists haven't been configured to accept requests from the LANsurveyor computer
- a firewall is preventing access to your devices (SNMP, ICMP, SIP, etc. requests are blocked)

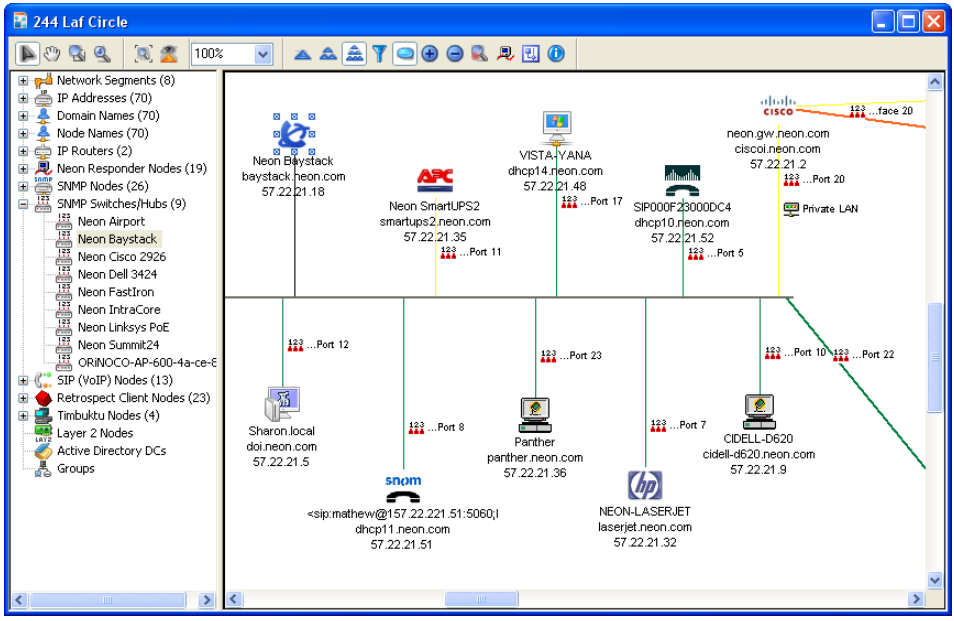
Refer to Appendix C, SNMP Checklist, for troubleshooting details. Also, consider including more autodiscovery options in the Create a New Network Map dialog box, adding Responder clients, and checking to make sure you have the correct SIP UDP port specified in the Network Options dialog box.

Finally, try building your map using a slower, more accurate mapping speed.

Read a Map

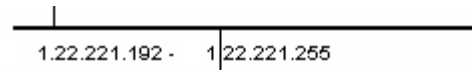
When LANsurveyor finishes searching the network, a Map Window displays your new map. Maps contain four types of network objects: networks, routers, managed switches/hubs, and end nodes. If you have managed hubs or switches and you have entered the community string for those devices, the LANsurveyor map will also display port connectivity for those devices. LANsurveyor will also display interface information for any SNMP device with more than one interface (e.g., routers and servers with more than one network connection).

If you have a large network, your map may show just Level 1 objects (routers) or Level 2 objects (routers and switches), depending on the settings in the Levels section in LANsurveyor Options dialog box. Select **Options** from the **Tools** menu and then select the **Levels** tab to view the settings.



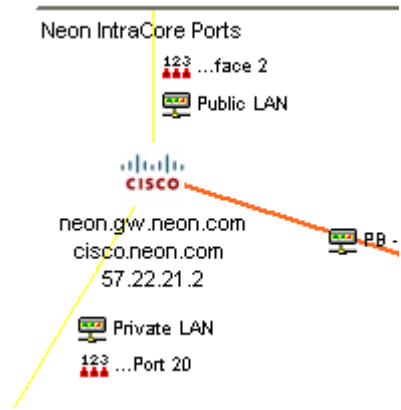
Networks

LANsurveyor represents both wired and wireless networks as lines and displays IP address ranges below and to the left of network lines.



Routers

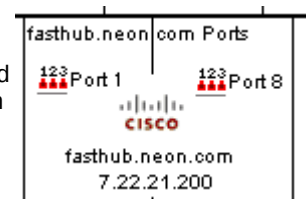
Routers allow the transfer of data between networks. To properly display a network's connectivity, the router must support SNMP. LANsurveyor represents a router by displaying a custom icon with lines drawn to the networks to which the router is directly connected.



If a router's type cannot be determined or no icon is available, a generic router icon is used. You can manually assign a more meaningful icon and name to the router by using the **Node Properties** item in the **Edit** menu.

Managed Switches/Hubs

Most end nodes connect to the network through hubs and switches. If you have SNMP-enabled (or "managed") hubs or switches, LANsurveyor draws those nodes on the map connected to the appropriate hub or switch and displays the port information on the map.

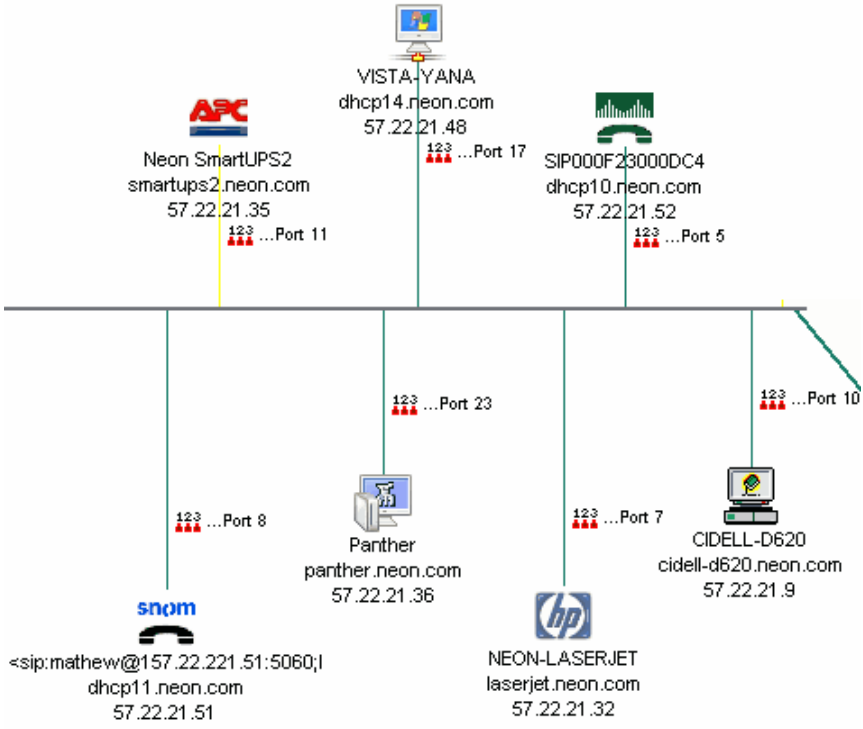


If a hub or switch type cannot be determined or no icon is available, a generic icon is used. You can manually assign a more meaningful icon and name by using the **Node Properties** item in the **Edit** menu.

End Nodes

An end node is any device that does not behave like a router or a managed hub or switch. Examples of end node objects are computers, printers, SIP phones, and unmanaged hubs and switches.

LANsurveyor uses icons to represent end nodes. LANsurveyor includes hundreds of icons to provide the most accurate representation of your network possible.



Computers with Responder clients installed use an icon with the LANsurveyor compass in the center of the screen:

 Green: Windows NT, 2000, XP, 2003, and Vista

 Blue: Windows 95, 98, and ME

 Orange: Linux

 Purple: Mac OS X

 Grey: Classic Mac OS

View Map Levels

Map levels make your maps easier to view. LANsurveyor maps can have thousands of nodes, so LANsurveyor automatically groups map objects into three levels:

- Level 1 includes network segments and routers (SNMP support is required to identify routers)
- Level 2 includes network segments, routers and switches (SNMP support is required to identify switches)
- Level 3 includes network segments, routers, switches, and all other end nodes

Your default map view is determined by the Levels settings in the Options dialog.

Change Map Levels

To change your map level, click on one of the map level icons. Click on the Level 1 icon  to view just your routers and network segments. Click on the Level 2 icon  to view Level 1 plus your switches. The Level 3 icon  displays all map nodes. To limit the nodes displayed in Level 3 to certain classes of objects (e.g., just nodes that responded to SNMP queries), use Level 3 object filtering in the Options dialog.

When you change your map view level, the map is redrawn and any changes you've made to your map will be lost unless you undo the map level change. Therefore, if you have arranged your map objects manually, make sure you save a copy of your initial map to preserve your changes.

Show/Hide Nodes

You can display nodes connected to a specific device using the show/hide icons. For example, if you want to see nodes connected to a switch in a Level 2 view, click on the switch icon on the map then click the show toolbar icon  . If you want to hide nodes connected to a router, click on the router icon on the map then click the hide toolbar icon  .

You can combine map levels and show/hide nodes to display a specific area of interest on your network.

Focus in New Window

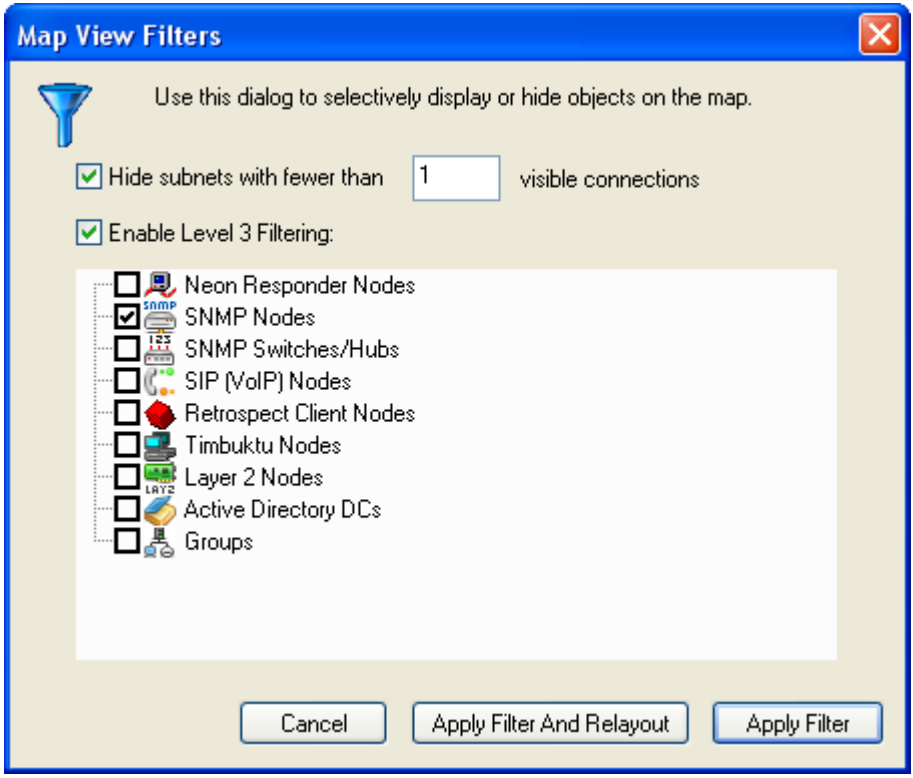
Click the Focus in New Window icon  to create a new map with the selected object and all connected sub-level objects. If you select a router and use Focus in New Window, the router, attached switches, and connected end nodes will be displayed in a new map. If you select a switch, just the nodes connected to the switch will be displayed.

Customized Visio Output

At any point, you can click on the Save to Visio icon or select **Save as Visio** from the **File** menu to generate a copy of what you see on your screen in Visio format. Refer to the Save as Visio section for more information.

Filter Map Objects

Map View Filters allow you to automatically obtain a more focused version of your network. For example, you can display your map with only those nodes with SNMP enabled or just your Active Directory infrastructure.



Combined with the Groups capability, you can filter your map so only those nodes which belong to a specific group or 'system' are included.

Add To Map

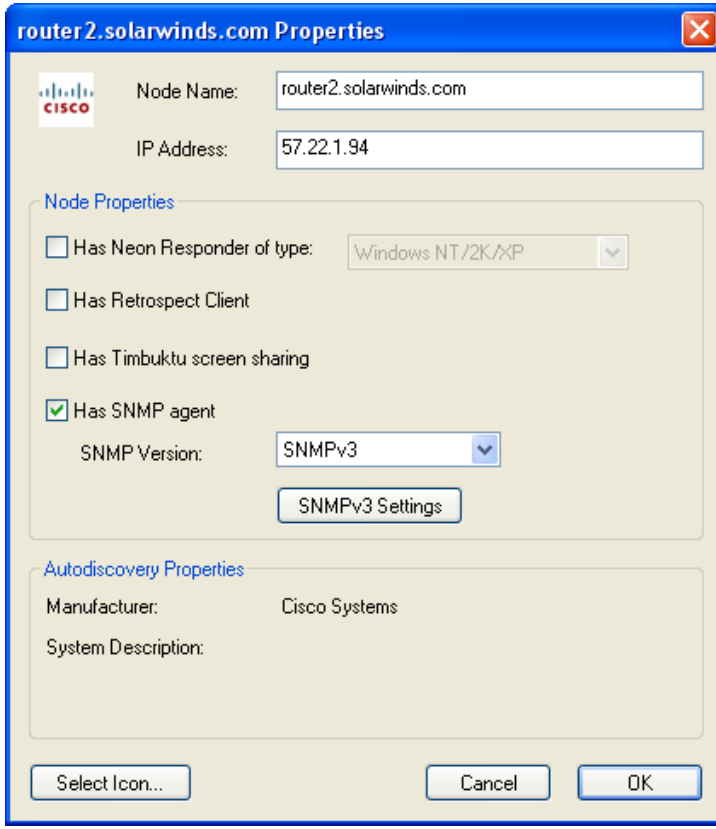
You can include non-contiguous or disconnected network segments on the same map by specifying the ranges on the Create A New Network Map dialog or by selecting **Add To Map** from the **Tools** menu. You can add as many different segments as you would like on the same map.

You can add a single node to your map or connect two different network segments using the **Create Node** option from the **Edit** menu.

Use Continuous Scan if you want LANsurveyor to keep your map up-to-date.

Node Properties

You can change the appearance and underlying properties of any selected map item. Select **Node Properties** from the **Edit** menu to bring up the Node Properties dialog box.



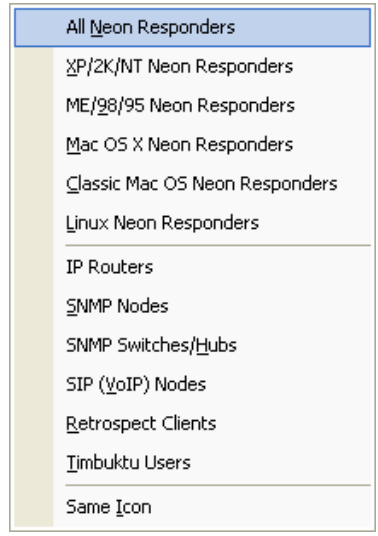
The Node Properties dialog box allows you to change the name, IP address, and icon for the node as well as the underlying technologies supported: Responder client, Retrospect Client, Timbuktu, SNMP, and the SNMP access information. If the device supports CDP or LLDP, information is automatically stored in the Autodiscovery Properties.

If you are using Continuous Scan and wish to automatically disable network access for rogue nodes, you may need to store a read/write SNMP access string for each of your managed switches.

Move Map Objects

Objects on the map can be moved using standard click and drag techniques. To move an object to a new location, simply click and hold the mouse button over the object to highlight it and use the mouse to reposition the object in a new location. All relationships between objects on the map will be maintained when an object is moved. Similarly, you can highlight several objects at the same time and move them to a new location. Multiple objects can be selected using a variety of methods including:

- Click on several objects while holding down the shift key.
- Click on a blank section of the Map Window and hold down while dragging the mouse.
- Use the **Select** option from the **Edit** menu to select the appropriate type of nodes.
- Select a single map object then use the **Select**>**Same Icon** menu item from the **Edit** menu to highlight all network objects with the same icon as the selected object.



Once multiple objects are selected, they can be moved by clicking again on any of the highlighted objects in the group and moving them with the mouse to a new location. Use Undo and Redo to revert node positions.

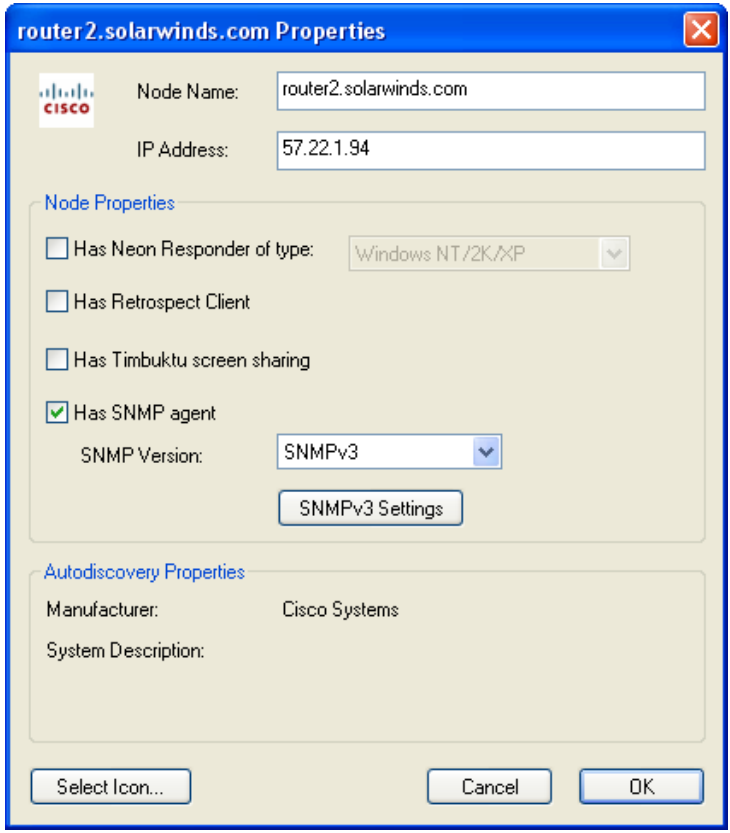
LANsurveyor also has features to align map objects in relation to one another. Select two or more map objects, then select **Align Left** or **Align Top** from the **Tools** menu. Selecting **Align Left** will cause LANsurveyor to move all selected map objects horizontally so that their left edges line up with the left edge of the leftmost object. Selecting **Align Top** will cause LANsurveyor to move all selected map objects vertically so that their top edges line up with the top edge of the topmost object.

If you would like to reset the location of all the nodes on the map back to their original location, use the Map Properties dialog box, pick a different map type, and LANsurveyor will reset the icon locations or simply click between map levels.

Create Map Objects

After you create your map, you may add new map objects to reflect changes on your network, add nodes not discovered during map creation, or connect network segments.

Add new map objects to your map with the **Create Node** command. Click on one or more map objects (any node or network segment). The new node you create will be connected to all selected map objects. Then select **Create Node** from the **Edit** menu. The New Node Properties dialog is displayed.



Enter the Node Name, IP Address, and Node Properties then click on Select Icon to pick a custom icon. Refer to Appendix B, LANsurveyor Icons, for information on creating your own custom icons.

Connect different network segments by selecting two or more segments or nodes on the map and then selecting **Create Node** from the **Edit** menu. LANsurveyor automatically adds a node and connects the networks.

Groups

Groups provide an easy way to generate reports and network diagrams for only those systems which belong to a specific region, function, or system.

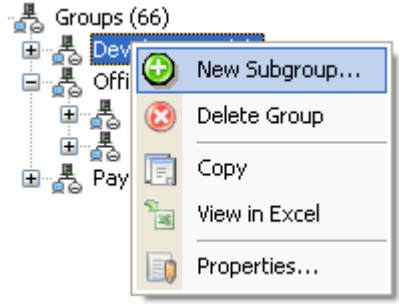
Group information is stored both with the maps used to create the groups and with the application in the Repository. Therefore, the Repository must be active for group information to persist, and any groups you create must be saved in the map before the group information is updated in the database. If you close a map after creating a group and without saving changes, the group changes will be discarded similar to changes made in any document or spreadsheet are discarded if the file is closed without saving changes.

To create a group, right-click on the Groups heading in the left-hand navigation tree:

Name the group and provide additional details, if desired.

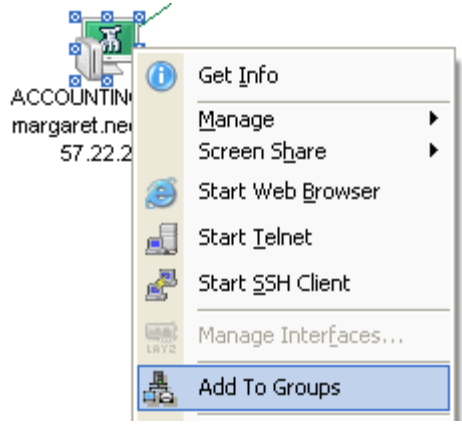
Subgroups

Right-click on any group to add a subgroup.



Add Nodes to Groups

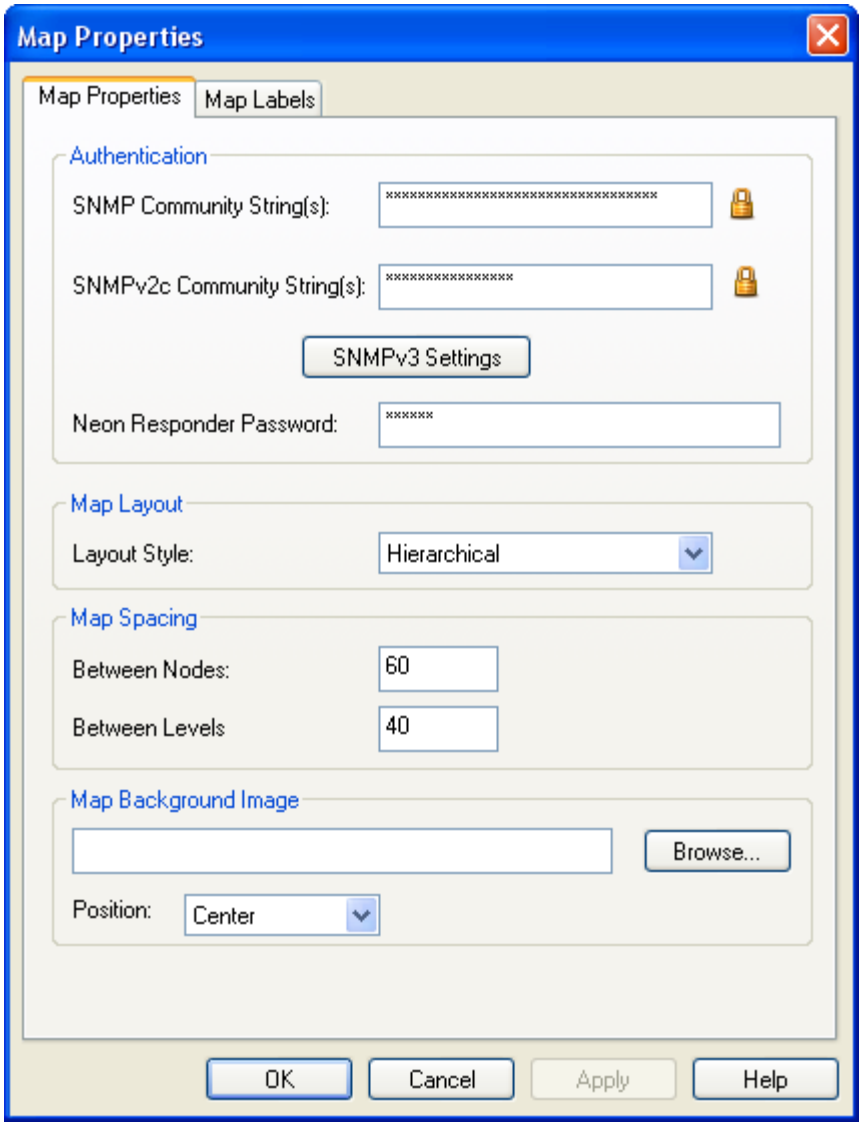
Add nodes to a group by selecting the node(s) on the map or in the left-hand navigation then right-click and select **Add To Groups**. The Add Nodes to Group wizard is displayed.



Map Properties

Customize your map using **Map Properties** from the **Tools** menu. Store updated SNMP community string and Responder client Password information as well as the drawing properties for the map.

Some drawing options cause the map to be redrawn, so use these options immediately after you build a new map and prior to customizations you wish to preserve. When drawing options are altered, the positions of map objects may change.



Adjusting the values contained in the box affects the map layout style, the amount of "padding" space placed between network objects, and the amount of space between levels of the map. LANsurveyor remembers the drawing settings with each saved map and between sessions.

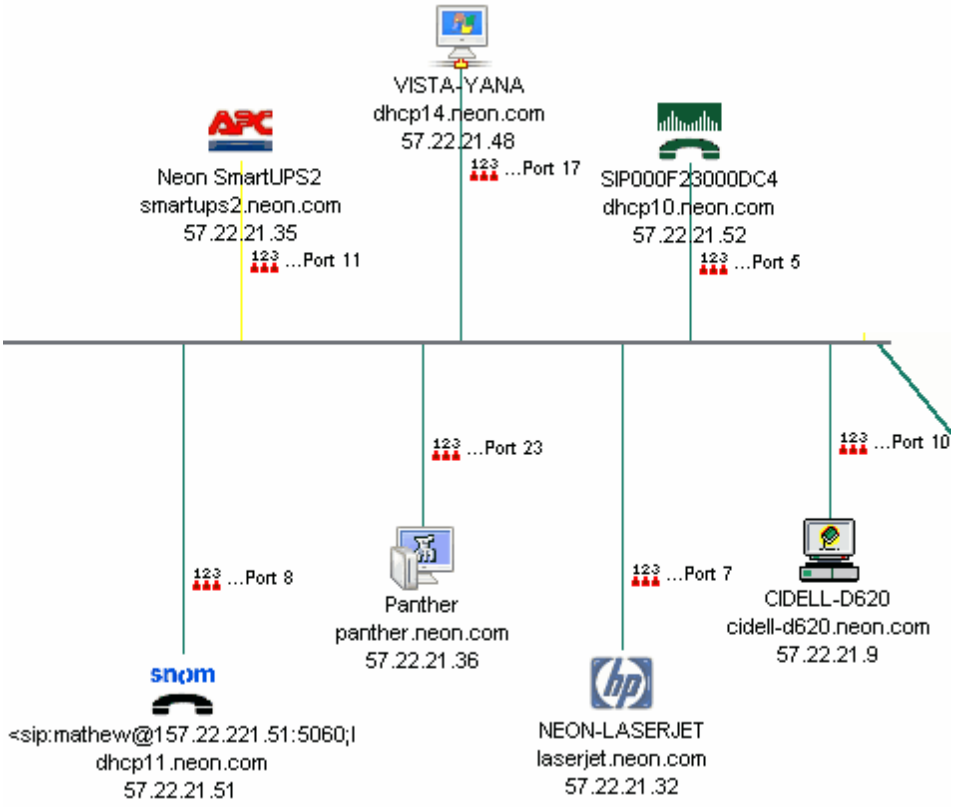
Customize your map using these options:

- Map Layout
- Map Spacing
- Map Background Image
- Map Labels

If you don't like the result of your changes, use **Edit>Undo** to revert (or **Edit>Redo** to revert back).

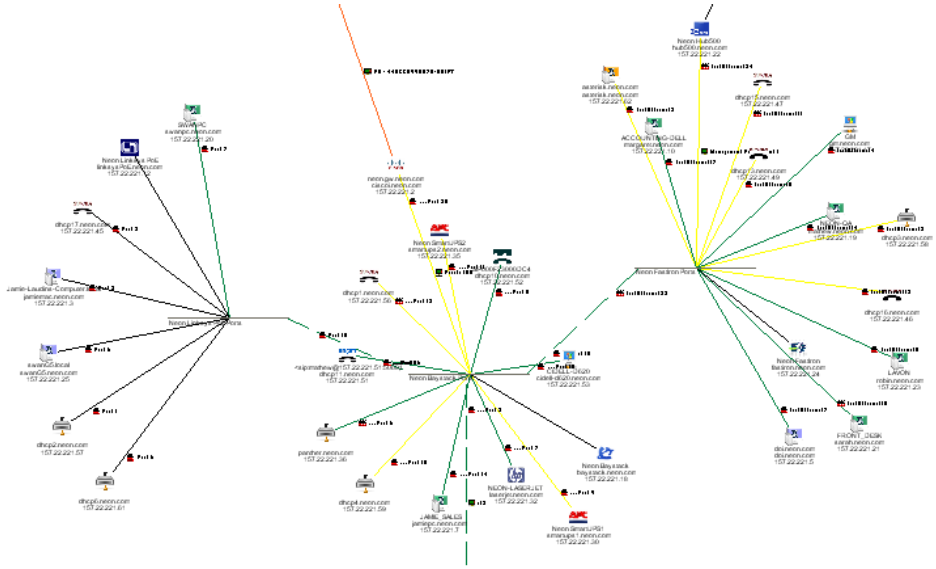
Map Layout

By default, LANsurveyor automatically draws network maps and displays network objects in a map layout style known as Hierarchical. Hierarchical layout draws nodes and network segments along a linear axis and is the most common layout style for representing network hierarchies.

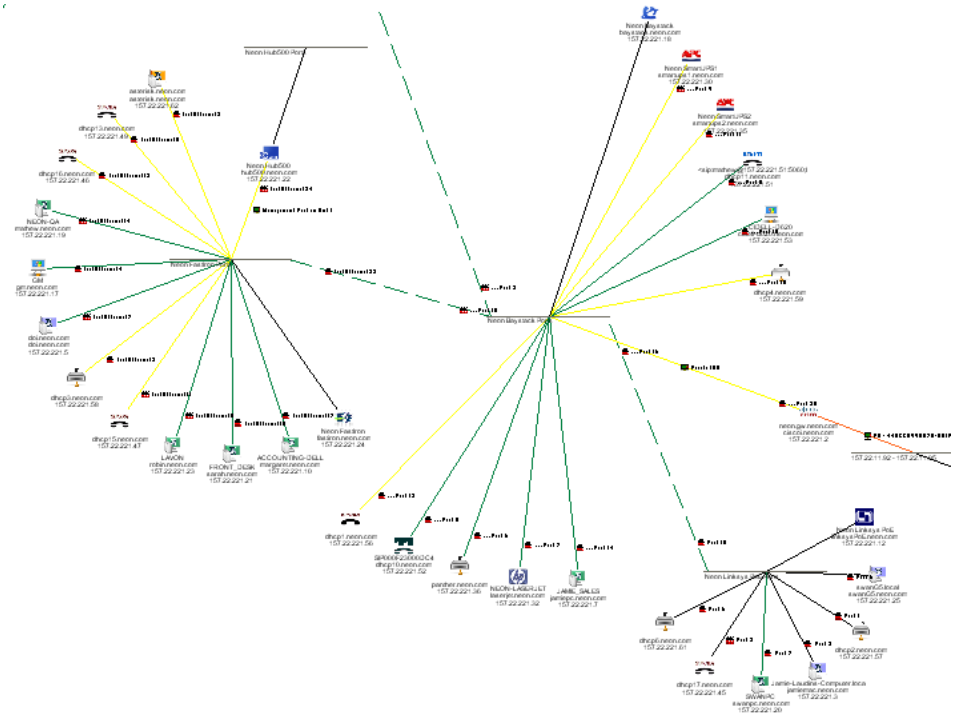


The Layout Style pull-down menu allows the selection of two other layout styles: Symmetrical and Circular.

Symmetrical maps draw nodes and network segments using geometric patterns that match top to bottom and left to right.



Circular maps draw nodes and network segments using circular patterns, grouping nodes around their connected network segments.



The layout style you use depends on personal preference and also on how nodes are distributed on your particular network. Most users will prefer either Hierarchical or Symmetrical layout styles.

Switching between layout styles for an existing network map will cause LANsurveyor to reorganize the map contents radically so any changes in node positions you have made will be lost.

Map Spacing

You can adjust the amount of space or "padding" around map objects and between networks ("levels") on Hierarchical maps to create a visually pleasing cushion of space.

Map Spacing Between Nodes adjusts the space between the map objects: the higher the number, the greater the space.

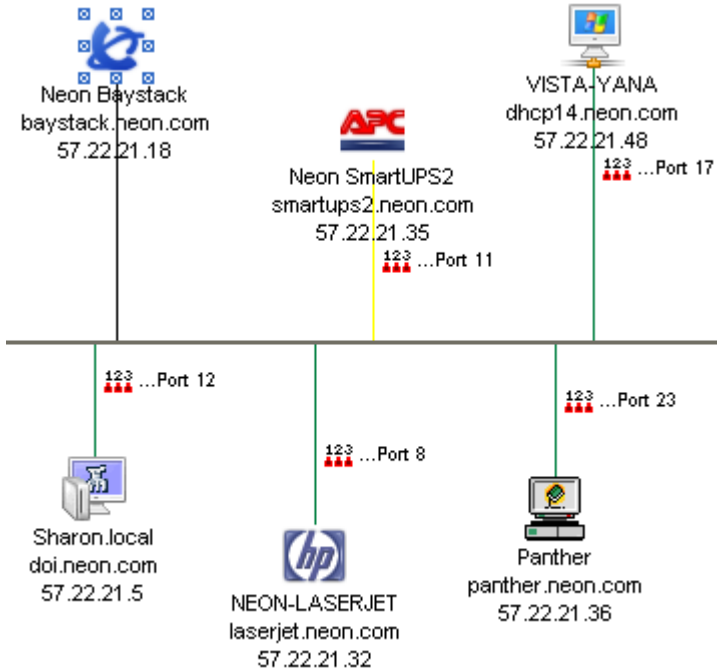
Map Spacing Between Levels adjusts the space between network segments: the higher the number, the greater the space.

Map Background Image

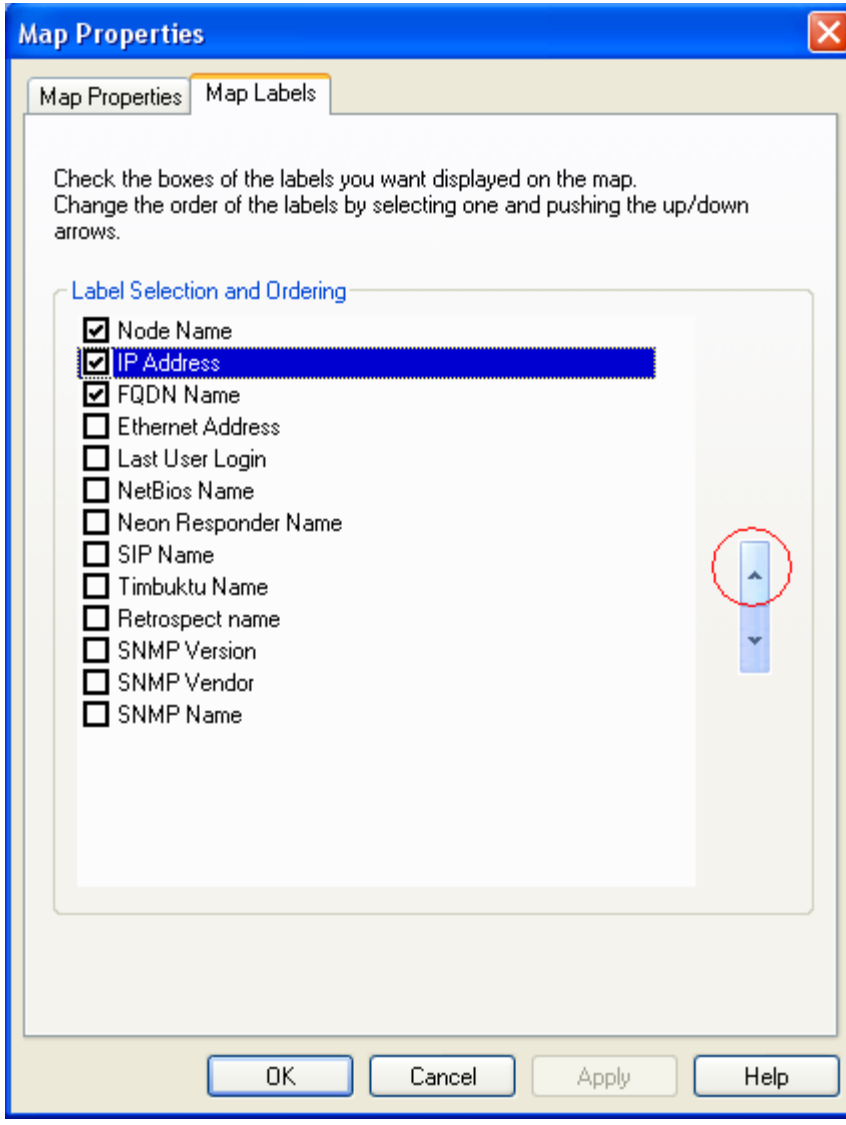
You can include a floor plan, logo, or other image on your map using the **Map Background Image** option. Click the **Browse** button to select the file you would like to include then choose center, stretch, or tile for the image background.

Map Labels

LANsurveyor maps can include node labels to help you understand which node you are viewing. By default, LANsurveyor displays the node name, fully qualified domain name, and IP address on the map.



The Map Labels tab allows you to change the data fields as well as the order for display. Check the box for the fields you would like to display and use the up/down arrows to change the display position.


Map Properties
Map Properties
Map Labels
Check the boxes of the labels you want displayed on the map.
Change the order of the labels by selecting one and pushing the up/down arrows.
Label Selection and Ordering
Node Name
IP Address
FQDN Name
Ethernet Address
Last User Login
NetBios Name
Neon Responder Name
SIP Name
Timbuktu Name
Retrospect name
SNMP Version
SNMP Vendor
SNMP Name
OK
Cancel
Apply
Help

Toolbars and Navigation

Application Buttons

Toolbars contain shortcuts to LANsurveyor's most important features. Buttons on the application toolbars work on either the front-most window or across multiple windows (e.g., multiple open maps).

New Map: a shortcut for the **New Map** from the **File** menu. The New Map button displays the Create New Network Map dialog to begin autodiscovery of a new network map.

Open: a shortcut for **Open** from the **File** menu. Open a saved map, report, or poll list.

Save: a shortcut for **Save** from the **File** menu. Saves a map, report, or poll list.

Print: a shortcut for **Print** from the **File** menu. Print a map or report.

Manage: a shortcut for the **Manage** menu. Brings up the Manage Wizard. The Manage Wizard gives you access to all of LANsurveyor's management options. Refer to the chapter titled "Remote Client Management" for more information on LANsurveyor's management features.

Alerts: a shortcut for **Alerts** from the **Edit** menu. Opens the Alerts dialog box. Refer to the "Alerts" chapter for more information on alerts.

Backup Profiler: a shortcut for **New>Backup Profiler** from the **Report** menu. Starts the Backup Profiler Wizard to help you plan, implement, and monitor your disaster recovery strategy for all selected Responder client nodes.

Software Inventory: a shortcut for **New>Software Inventory** from the **Report** menu. Inventory software applications on all selected Responder client nodes.

Software Meter: a shortcut for **New>Software Meter** from the **Report** menu. Determine which applications are active on all selected Responder client nodes.

Missing Software: a shortcut for **New>Missing Software** from the **Report** menu. Determine which of the selected Responder client nodes do not have the specified software installed.

Hardware Inventory: a shortcut for **New>Hardware Inventory** from the **Report** menu. Hardware Inventory for all selected Responder client nodes.

Switch/Hub Ports: a shortcut for **New>Switch/Hub Ports** from the **Report** menu. Provide a list of managed switches and hubs, their ports, and the devices connected to the ports.

Custom Report: a shortcut for **New>Custom Report** from the **Report** menu. Launches the Custom Report Wizard which allows you to select which information you would like to include in your report.

Contextual Help: toggles cursor to Help arrow. Click on any item or icon to display help for that item.

Map Window Buttons

Map window toolbar buttons affect the map or selected nodes within the map window.

Select: toggles cursor to select arrow to allow selection of items from a map.

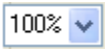
Pan: toggles cursor to pan hand to allow easy navigation around a map.

Zoom with Marquee: toggles cursor to zoom. Zooms into selected region on map.

Zoom Interactively: toggles cursor to allow zoom in or out of selected region on map. Click and drag arrow down to zoom in or click and drag arrow up to zoom out.

Fit in Window: click icon to automatically zoom entire map to fit in map window.

Map Overview: a shortcut for **Overview** from the **Window** menu. Displays a thumbnail of the entire map in a smaller window.



Zoom Percentage: displays current zoom percentage for map window. Change the zoom percentage by selecting from the pull-down menu or enter a number directly in the field. When a LANsurveyor map zoom level is changed, all the relationships between objects are maintained. In addition, when you save, print, or export a map, the zoom level selected will apply to the output.

Display Level 1: redraws map to display only routers and network segments.

Display Levels 1 and 2: redraws map to display only routers, network segments, and switches.

Display Levels 1, 2 and 3: redraws map to display all network nodes. Selected button shows current state of the display level.

Edit Map View Filter: controls which categories of end nodes are displayed plus sets threshold for displaying subnets.

Show/Hide Tool Tips: controls display of tool tips on map (used to display interface speed and switch-to-switch port connectivity.

Show Sub-level: shows Level 3 nodes connected to selected Level 2 node or Level 2 nodes connected to selected Level 1 node.

Hide Sub-level: hides Level 3 nodes connected to selected Level 2 node or Level 2 and Level 3 nodes connected to selected Level 1 node.

Focus in New Window: displays the selected node and all lower-level, connected nodes in a new map window.

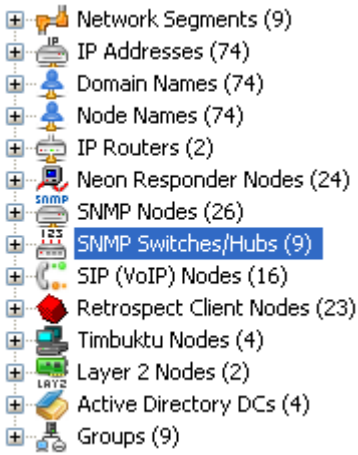
Select Responder clients: a shortcut for **Select>All Responder clients** from the **Edit** menu. Selects all Responder client nodes on all open maps. Selected nodes can then be reported on or managed.

Save As Visio: a shortcut for **Save As Visio** from the **File** menu. Saves the LANsurveyor map in Visio format.

Get Info: a shortcut for **Get Info** from the **Tools** menu. Click icon to get more information about one or more selected map objects. All data available through reporting is available through **Get Info**.

Map Navigation

You can quickly and easily find any map item using the left Navigation Pane. All map items are represented in one or more of twelve different categories. Simply click on any item to select that item and scroll the map to display the item in the center of the map window.

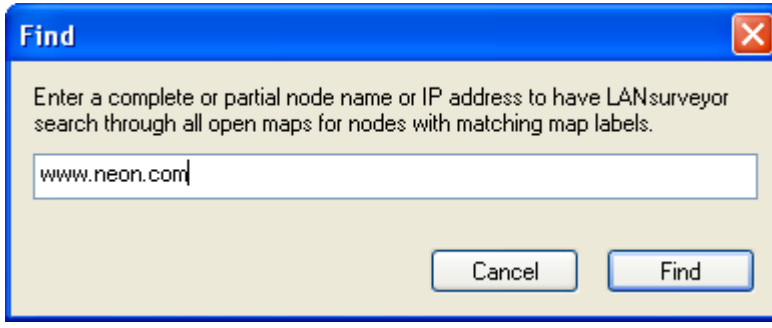


- Network Segments: list of all network segments mapped.
- IP Addresses: list of all network nodes sorted by IP address.
- Node Names: alphabetical list of all nodes on the map.
- IP Routers: alphabetical list of all IP routers on the map.
- Responder Nodes: alphabetical list of all nodes with the Responder client installed and displayed on the map.
- SNMP Nodes: alphabetical list of all nodes on the map that responded to the SNMP query when the map was created.
- SNMP Switches/Hubs: alphabetical list of all managed switches and hubs that responded to a switch/hub-specific SNMP query when the map was created.
- SIP (VoIP) Nodes: alphabetical list of all SIP-based VoIP devices on the map.
- Retrospect Client Nodes: alphabetical list of all nodes on the map with Dantz's Retrospect client installed.
- Timbuktu Nodes: alphabetical list of all nodes on the map with Netopia's Timbuktu client installed.
- Layer 2 Nodes: alphabetical list of Ethernet addresses discovered with Continuous Scan's Layer 2 detection.
- Active Directory DCs: alphabetical list of all Active Directory Domain Controllers on the map.
- Groups: user-defined collections of nodes.

Right click on any category header (e.g., SNMP Nodes) to get information about the nodes in that category. See the Get Info section in the Reports chapter for more information.

Find and Find Again

Search all open maps for any label or IP address using any alphanumeric string. Select **Find** from the **Edit** menu and enter the string. LANsurveyor will find the first occurrence and highlight the map object. Use **Find Again** from the **Edit** menu to find the next object that matches the alphanumeric string you entered.



Select Map Objects

Select map objects to get more information, report, or delete. You can select map objects in a number of different ways.

Responder client Toolbar Icon

Select all Responder clients by clicking on the toolbar icon. 

Computers with Responder clients installed use an icon with the LANsurveyor compass in the center of the screen.

 Green: Windows NT, 2000, XP, 2003, and Vista

 Blue: Windows 95, 98, and ME

 Orange: Linux

 Purple: Mac OS X

 Grey: Classic Mac OS

Select from the Edit Menu

Select map nodes using the **Select** option on the **Edit** menu. You can select:

- All Responder clients
- XP/2K/NT Responders
- Linux Responders
- ME/98/95 Responders
- Mac OS X Responders
- Classic Mac OS Responders
- IP Routers
- SNMP Switches/Hubs
- SIP (VoIP) Nodes
- Retrospect Clients
- Timbuktu Users
- SNMP Nodes
- Nodes with the Same Icon

Select from the Map

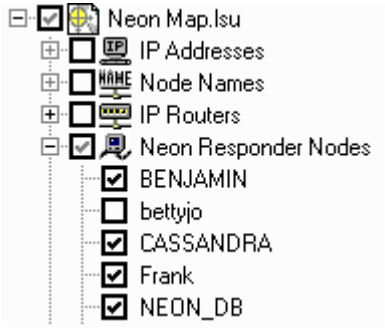
Click directly on any map object to select it. To select more than one object, either hold down the shift key and click or click and drag over several objects to select all objects within the selected rectangle.

Select from Left Navigation Pane

Click directly on any item in the left-hand navigation to select it. To select more than one object, either hold down the shift key and click or ctrl-click to select more nodes.

Select Nodes in Wizards

Check the box next to any map object to select that item. Once an item is selected, a grey check-mark is also placed in the category of that item to indicate something within the category is selected. If you click on a category check-box, all items in that category are selected.



Hint: Any items selected on open maps are automatically selected.

Zoom the Map

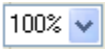
When a LANsurveyor map zoom level is changed, all the relationships between objects are maintained. In addition, when you save, print, or export a map, the zoom level selected will apply to the output.

Zoom from Toolbar

Zoom with Marquee: toggles cursor to zoom. Zooms into selected region on map.

Zoom Interactively: toggles cursor to allow zoom in or out of selected region on map. Click and drag arrow down to zoom in or click and drag arrow up to zoom out.

Fit in Window: click icon to automatically zoom entire map to fit in map window.



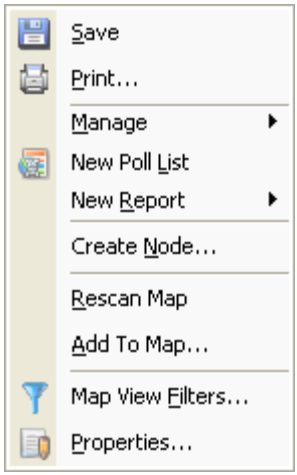
Zoom Percentage: displays current zoom percentage for map window. Change the zoom percentage by selecting from the pull-down menu or enter a number directly in the field. When a LANsurveyor map zoom level is changed, all the relationships between objects are maintained. In addition, when you save, print, or export a map, the zoom level selected will apply to the output.

Context Menus

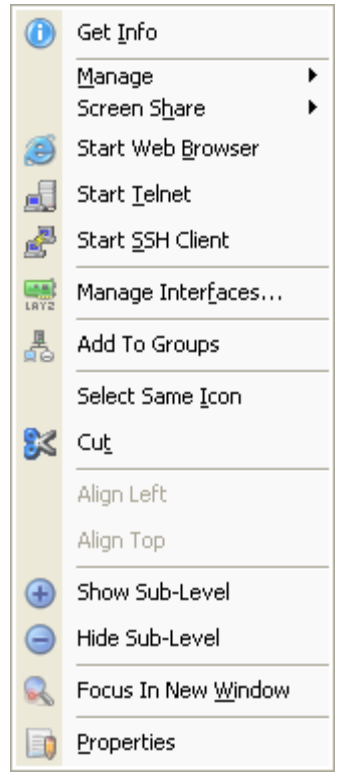
Use the right mouse button to access the context menus. LANsurveyor supports three different context menus: map, node, and left-hand navigation.

The map context menu provides direct access to the most common map functions. All of the options are also available from the LANsurveyor application menu.

The node context menu provides direct access to the most common node functions. All of the options are also available from the LANsurveyor application menu.

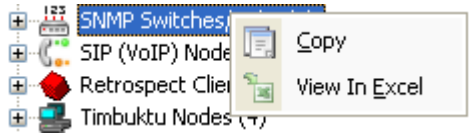


Map Context Menu



Node Context Menu

The left-hand navigation context menu provides direct access to the information contained in the left-hand navigation list, including network segments. Right-click on the section header and select either **Copy** to copy the information to the clipboard or **View in Excel** to open a new worksheet in Excel with the information.



Your Maps

Save and Open Maps

Save Your Map

Once you create a map, you can click on the Save toolbar icon or select **Save** from the **File** menu to save your map to a file.

You can also:

- Export Your Map
- Print Your Map
- Open a Saved Map
- Rescan a Map

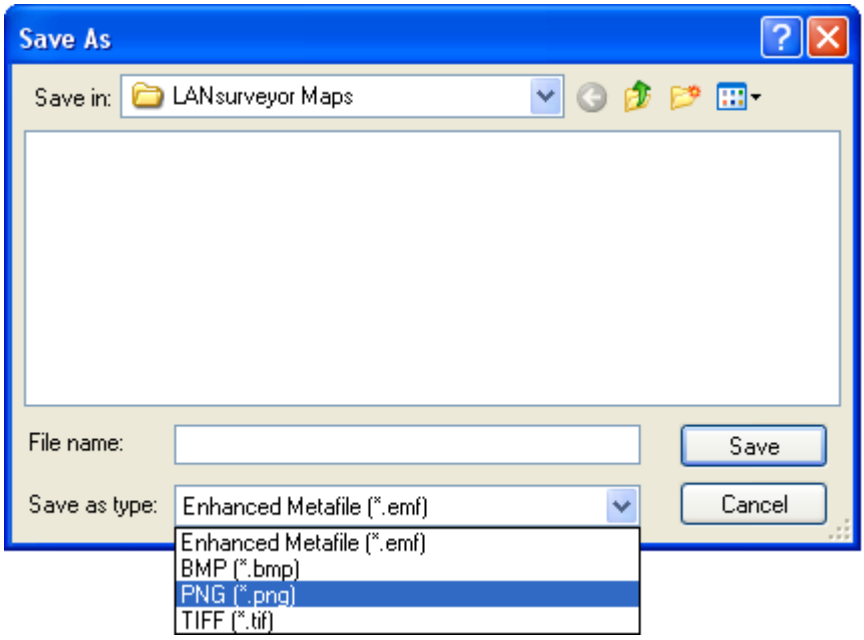
AutoSave Maps

Continuous Scan options include the ability to automatically save time-stamped maps on a schedule. Refer to the AutoSave section of the Continuous Scan documentation for more information.

Save As Image

In addition to saving maps to Visio format, you can save maps to EMF, BMP, PNG, and TIF formats.

To export your map, select **Save As Image** from the **File** menu. Once the dialog is displayed, you can name the exported file.

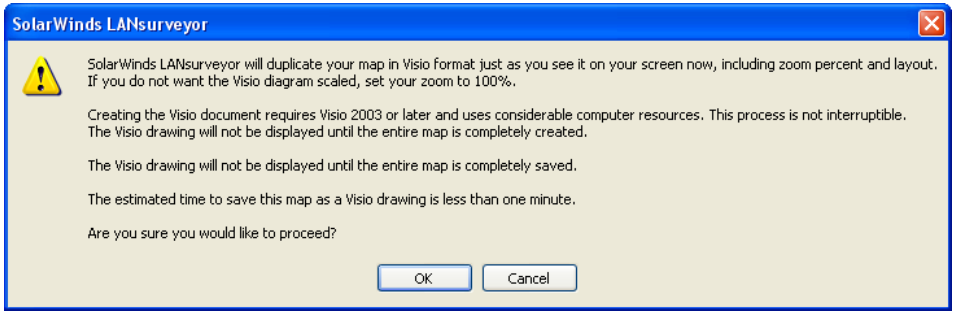


Save As Visio

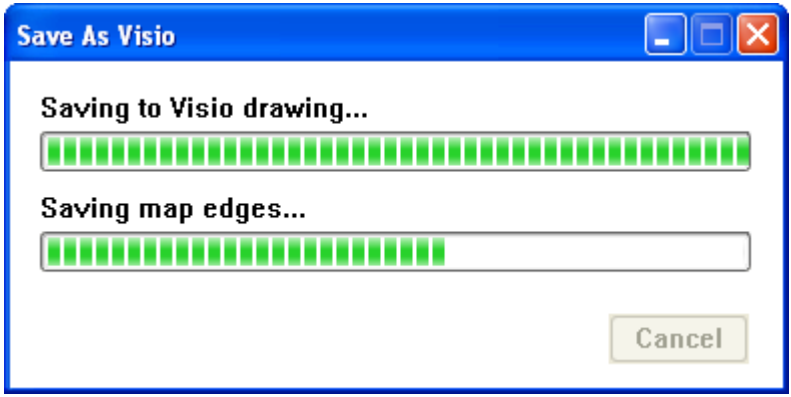
LANsurveyor can create an exact copy of your map in Microsoft Visio format. This feature requires Visio 2003 or newer.

Prior to saving your map in Visio format, lay out the map as you would like it reproduced in Visio, including Map Levels, Show/Hide Nodes, and Zoom percent.

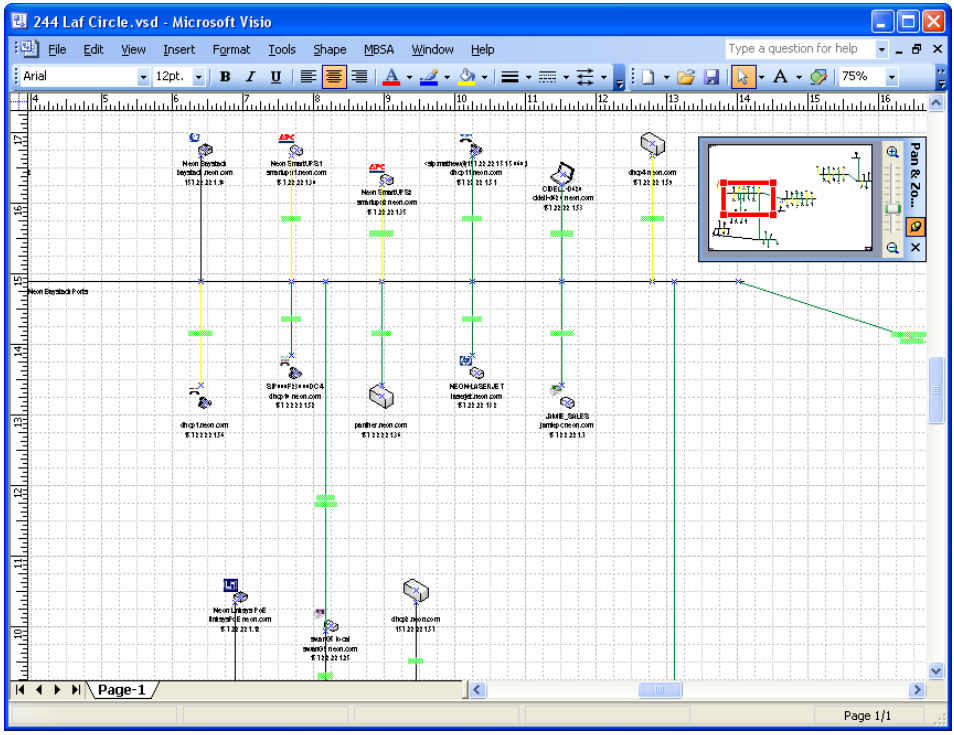
When you select **Save As Visio** from the **File** menu or click on the Save As Visio icon , LANsurveyor displays a notification dialog box:



LANsurveyor must use Microsoft's Visio development tools to create the map nodes and connectors, so the process is not interruptible. Click OK to proceed.



Once completed, your LANsurveyor map is re-created in Visio.



Your new Visio diagram includes your personalized information and a logo in the upper-left hand corner of the diagram. LANsurveyor uses the logo contained in the "YourLogo.bmp" file in the installation directory (typically C:\Program Files\SolarWinds\SolarWinds LANsurveyor). In addition, the line color legend is displayed in the lower-right corner of the diagram.

AutoSave in Visio Format

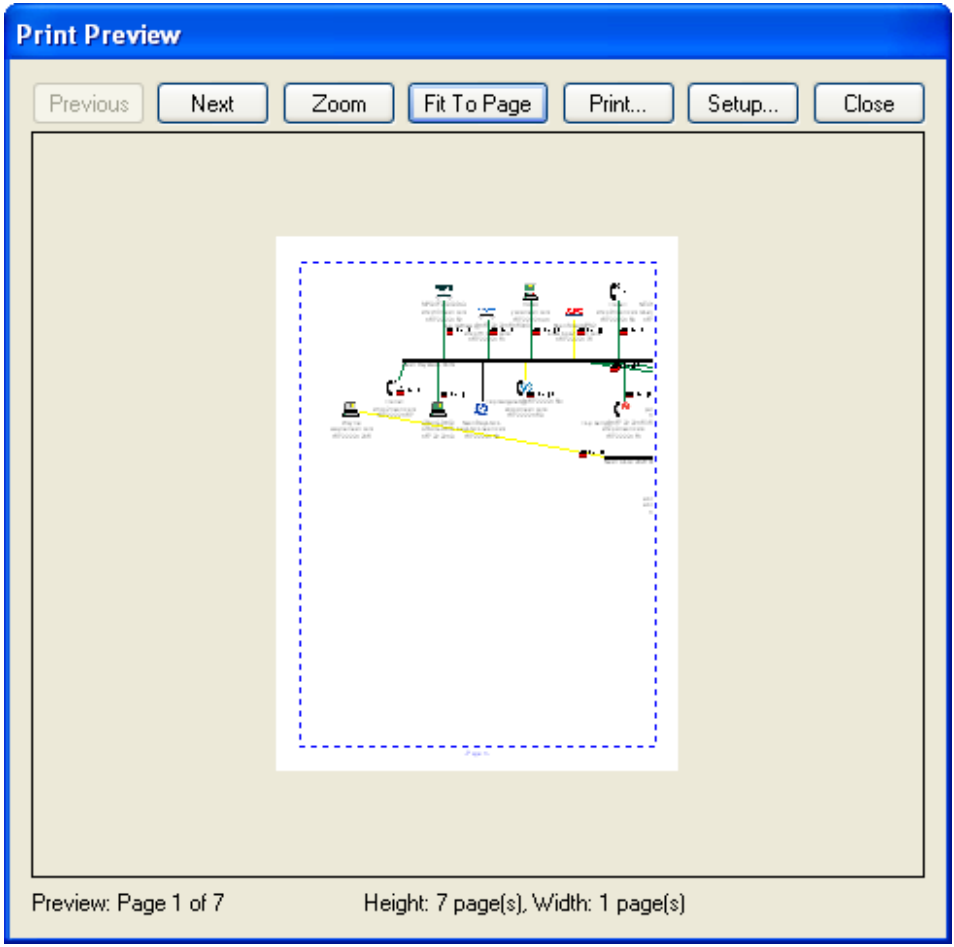
You can also use Continuous Scan's AutoSave feature to save time-stamped Visio-format LANsurveyor maps.

Print Your Map

Click on the Print toolbar icon or select **Print** from the **File** menu to print your map.

LANsurveyor will print your map on any output device, including plotters. Maps too large to print on a single sheet of paper will print across multiple sheets that, when combined, will represent the entire map. Alternatively, you may choose to print your entire diagram on a single sheet using the Fit to Page option from Print Preview.

Select **Print Preview** from the **File** menu to access preview and Fit to Page.



Select Setup to enter header and footer text for your map printout.

Open a Saved Map

Once you've saved a map, the map file functions just as any other file.

Double-click on the file icon  to launch LANsurveyor and open the map.

Or, from within LANsurveyor, click on the Open toolbar icon  or select **Open** from the **File** menu.

Rescan a Map

Rescanning performs the same type of search as when the map was originally built. After the **Rescan Map** command completes, any map objects that did not respond will be listed in the session log. (Click on the Session Log icon or select **Session Log** from the **Window** menu to view the session log.)

Any new map objects that are discovered are added to the map. If a map object has moved from one part of the network to another, that map object may appear twice: once in its old network location and once in its new network location.

Use **Rescan Map** to discover new map objects and detect map objects that have either disappeared or moved on the network. The **Rescan Map** feature allows you to continue to use a LANsurveyor map over a period of time. It is a good alternative to building a new map from scratch because any new objects you have defined with the **Create Object** menu item are kept in saved map files.

LANsurveyor can optionally rebuild the map layout in order to show any new objects that have appeared. If you have moved objects to new locations, these node locations may be modified. To prevent re-layout, uncheck **Redraw map** option in the application preferences.

Rescan Map searches only the IP address range(s) already discovered on the map; to add IP address ranges, use **Add To Map** from the **Tools** menu and then use **Rescan Map**.

The Continuous Scan feature continuously rescans your map to keep it up-to-date.

Monitor Your Network

Network Monitoring

LANsurveyor makes it easy to monitor your network and includes a number of different monitoring methods and options.

- Continuous Scan Intrusion Detection uses your network maps as a baseline for identifying network changes, including intruders
- TCP Port Monitoring checks the availability of applications or services running on networked systems
- Alerts can notify you of network problems through a variety of methods

Continuous Scan Intrusion Detection

Continuous Scan is an intrusion detection feature that uses one or more LANsurveyor maps as the baseline network environment. When Continuous Scan is active, LANsurveyor scans the appropriate network ranges and looks for nodes that appear on the network. In a managed switch environment, you can disable network access for rogue nodes directly from the Threat List or automatically disable network access for all rogue nodes.

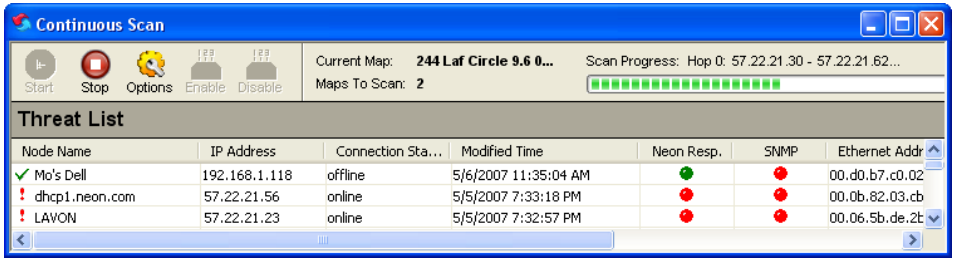
Continuous Scan can be set to either scan all open maps or just maps you specify. Use the AutoOpen option under **Tools>Options** to specify which maps to use.

Continuous Scan is a great way to meet regulatory requirements: Continuous Scan monitors your network for new nodes, checks new nodes for compliance as they connect to the network, and keeps a log of all nodes as they connect to and disconnect from the network.

Select **Continuous Scan** from the **Window** menu to view the Continuous Scan window. Click on the Start button to start scanning and click on the Stop button to stop scanning.

Note: We recommend you run Continuous Scan for at least several days before automatically disabling network ports. As Continuous Scan runs, LANsurveyor is able to aggregate more information, provide more comprehensive network diagrams, and significantly reduce the number of false positives.

When a new node is detected on the network, LANsurveyor adds the node to the Threat List.



The Threat List includes information about when the node was detected, the node name, IP address, Ethernet (MAC) address, the hub or switch the node is connected to, the port number used for the connection if connected to an SNMP-enabled device, and the status of any authentication methods you have configured.

LANsurveyor attempts to authenticate the node using either an SNMP community string or the Responder client password or a third party product such as Microsoft Baseline Security Analyzer (MBSA). If the node is authenticated, the Threat List is updated to reflect the type of authentication. LANsurveyor Alerts can be set based on whether a node is authenticated or unauthenticated. To configure authentication methods, select **Options** from the **Monitor>Continuous Scan** menu and select the **IP Node Response Options** tab.

Disable or Enable Switch Port

If you detect a rogue node, you can disable network access for the node by clicking on the node in the Threat List and clicking the Disable button If you determine a disabled node should be enabled, click on the Enable button. You can automatically disable network access for all rogue nodes from the Response Options tab on the Continuous Scan Options dialog. Only nodes connected to a switch port can be disabled or enabled.

You can also disable or enable ports directly from the map.

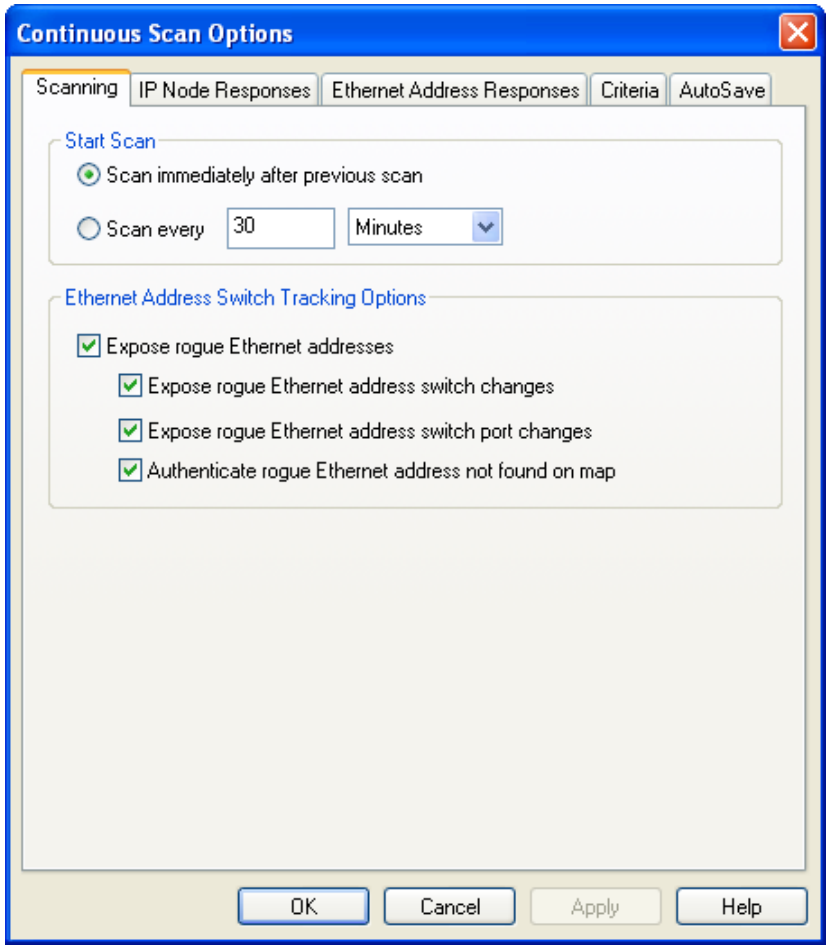
Note: Port enable/disable requires a "managed" or SNMP-enabled switch with the correct read/write community string.

Continuous Scan Options

Click on the Options button on the Continuous Scan window or select **Continuous Scan>Options** from the **Monitor** menu to set the Continuous Scan options.

Scanning Options

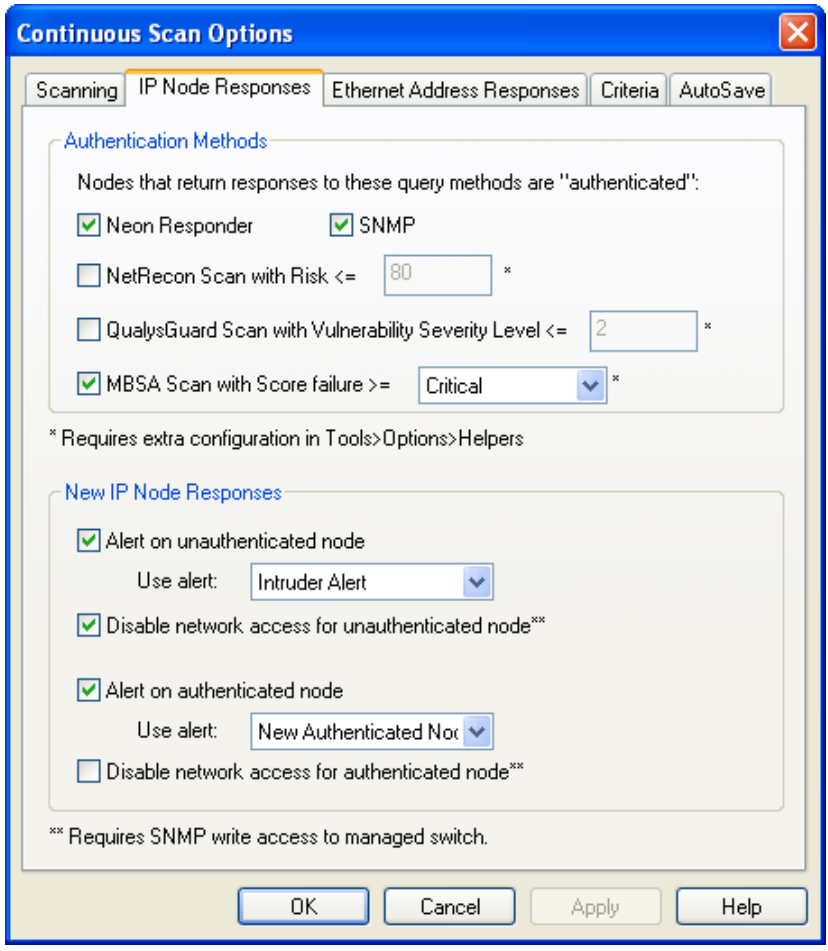
Use Scanning options to set the scanning interval. **Scan every** sets the amount of time between scanning the specified or open maps. If the interval is less than the time it takes to scan the maps, LANsurveyor will scan immediately after the previous scan.



You can also discover rogue nodes that mask their IP addresses and show up only when their network activity can be detected through their Ethernet address. Select **Expose rogue Ethernet addresses** to discover masked nodes and report on those nodes if they change the switch or the switch port they connect through. You can also attempt to authenticate rogue Ethernet addresses using the methods you select in the **Ethernet Address Responses** tab.

IP Node Responses Options

The Responses options allow you to establish authentication criteria and alert settings.



When a new node is encountered, LANsurveyor can authenticate the node through a variety of methods.

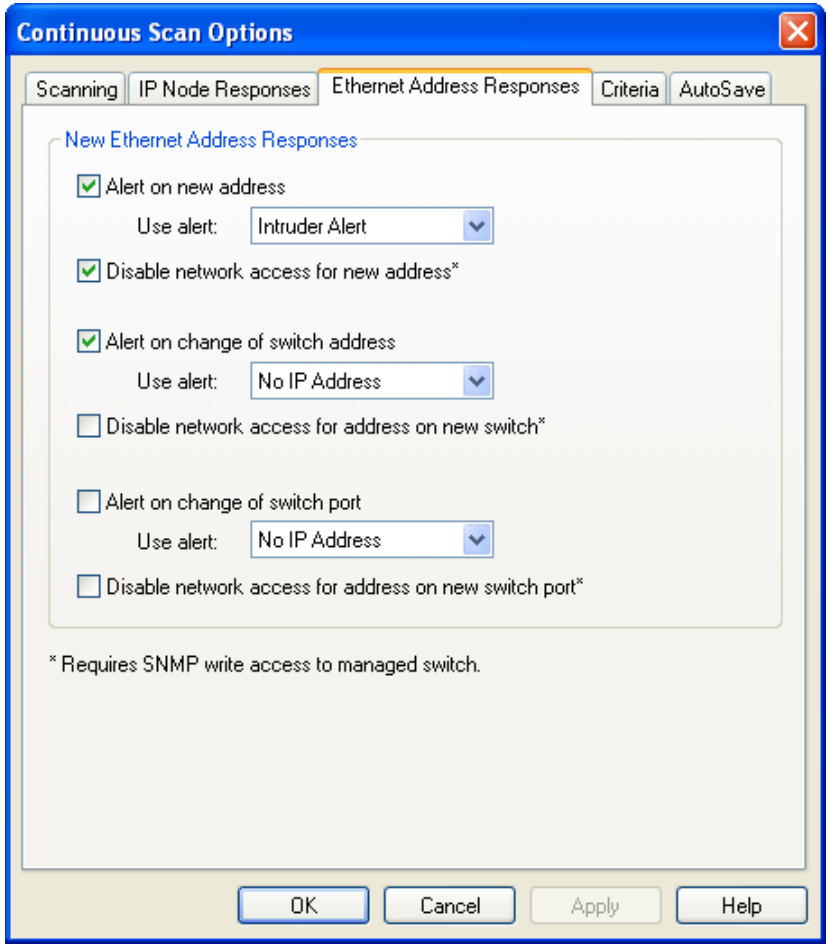
If you have deployed Responder clients, you can ensure the discovered node is part of your network with a check of the Responder client password. Nodes with the correct password are authenticated, and nodes without the correct password are unauthenticated. Similarly, you can use SNMP community strings to authenticate new network hardware.

Continuous Scan is also integrated with a variety of third party solutions, including Symantec's NetRecon, Qualys' QualysGuard, and Microsoft's Baseline Security Analyzer (MBSA). These options are covered more completely under the Application Integration section of the manual.

You can receive different alerts when LANsurveyor encounters either an authenticated or unauthenticated node. You can also automatically disable network access for nodes that appear on the Threat List if the node is directly connected to a managed switch and LANsurveyor knows your read/write SNMP community string.

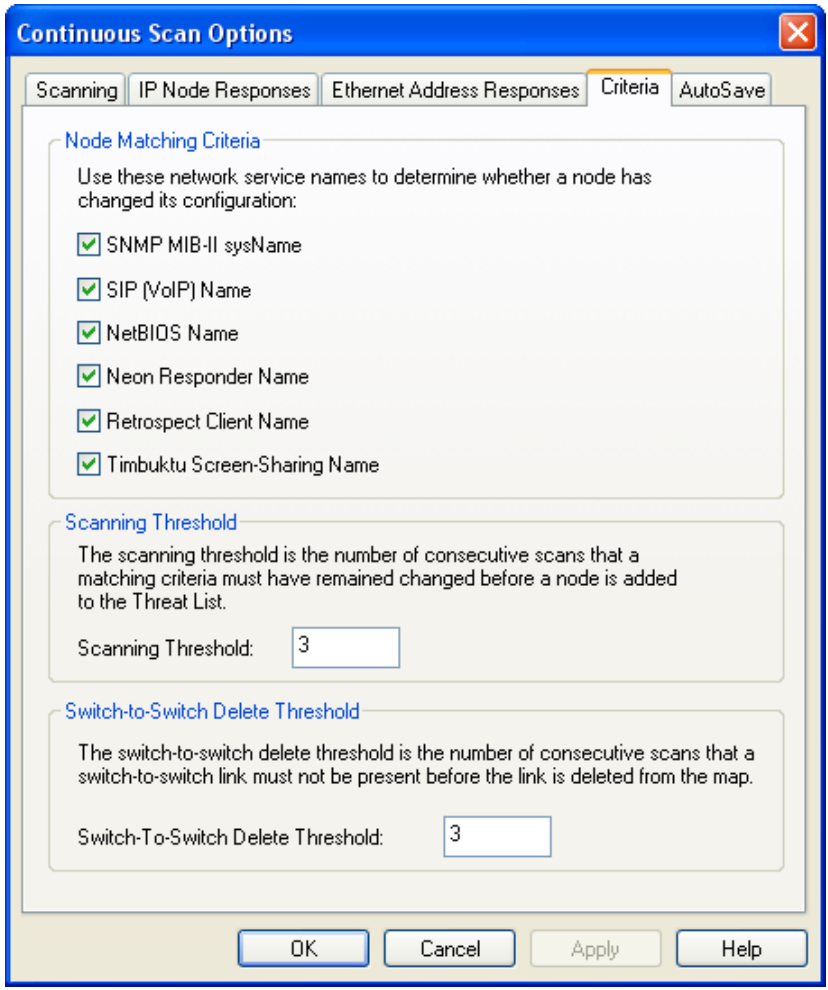
Ethernet Address Responses

If you have selected **Expose rogue Ethernet addresses** to discover masked nodes on the **Scanning** tab, select the response for newly discovered nodes on the **Ethernet Address Responses** tab. You can receive alerts when new addresses are discovered, the Ethernet address uses a different switch, or the switch port changes. You can optionally disable network access if the node is directly connected to a managed switch and LANsurveyor knows your read/write SNMP community string.



Criteria Options

If your network uses DHCP, it is possible for a node to obtain a different IP address after your baseline map was created. Rather than report numerous false positives, LANsurveyor can use several different naming criteria to determine if it is the same node or a new node.

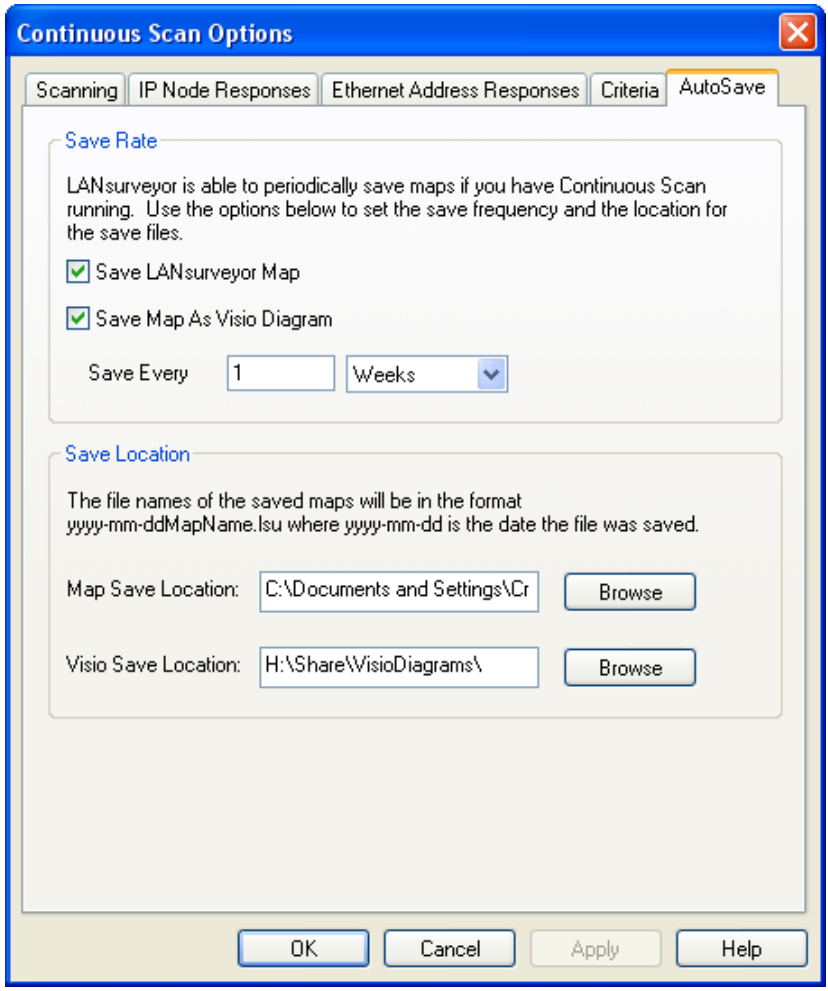


Since switch re-configuration is relatively rare, LANsurveyor allows you to specify the number of scans a switch-to-switch connection is maintained on the map given the connection has not been re-discovered.

AutoSave Options

You can automatically save LANsurveyor maps in either LANsurveyor or Visio format to create archival reference views of your network. The archival diagrams are useful for troubleshooting and before/after scenarios. In addition, some auditors require documentation of network modifications, and archival diagrams make the process easier.

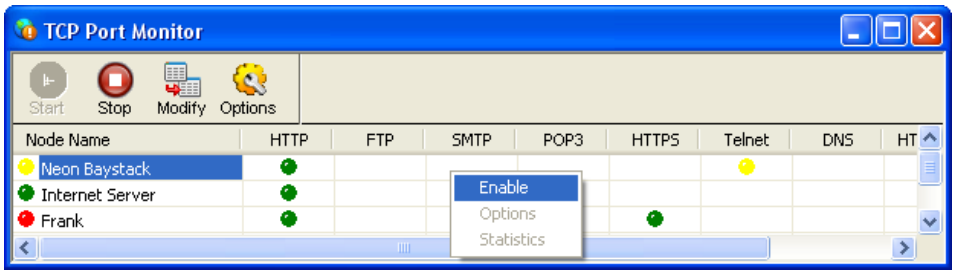
Specify the rate for saving the maps in hours, days, or weeks in addition to the target directories for your map archives.



TCP Port Monitoring

LANsurveyor allows you to monitor availability of applications and services on your network through TCP Port Monitoring. Select **Window>TCP Port Monitor** to view the TCP Port Monitoring window. You can monitor up to 20 different nodes.

Click on the Modify button to select the nodes to monitor in the wizard, then right-click in the appropriate cell to enable monitoring of the node in that row and the port in that column.



Click on the Start button or select **Start Monitoring** from the **Monitor>TCP Port** menu to start monitoring.

Click on the Stop button or select **Stop Monitoring** from the **Monitor>TCP Port** menu to stop monitoring.

While waiting for the status of the TCP Port, LANsurveyor displays an empty circle ○. If the port responds and the ASCII text received from the port matches the expected result for the TCP server in question, a green dot is displayed; if there is no response, a red dot is displayed. A warning dot is displayed when the TCP port is responding, but the ASCII text received does not match the expected result for the TCP server in question. An alert is triggered when the number of retries set in Options has been reached.

To view the exact ASCII text received by the TCP server being monitored, right-click the warning dot and select Statistics. The Last Script Receipt section of the TCP Port Statistics dialog box contains the last ASCII text received as well as the ASCII text that was expected by LANsurveyor.

TCP Port Monitor Options

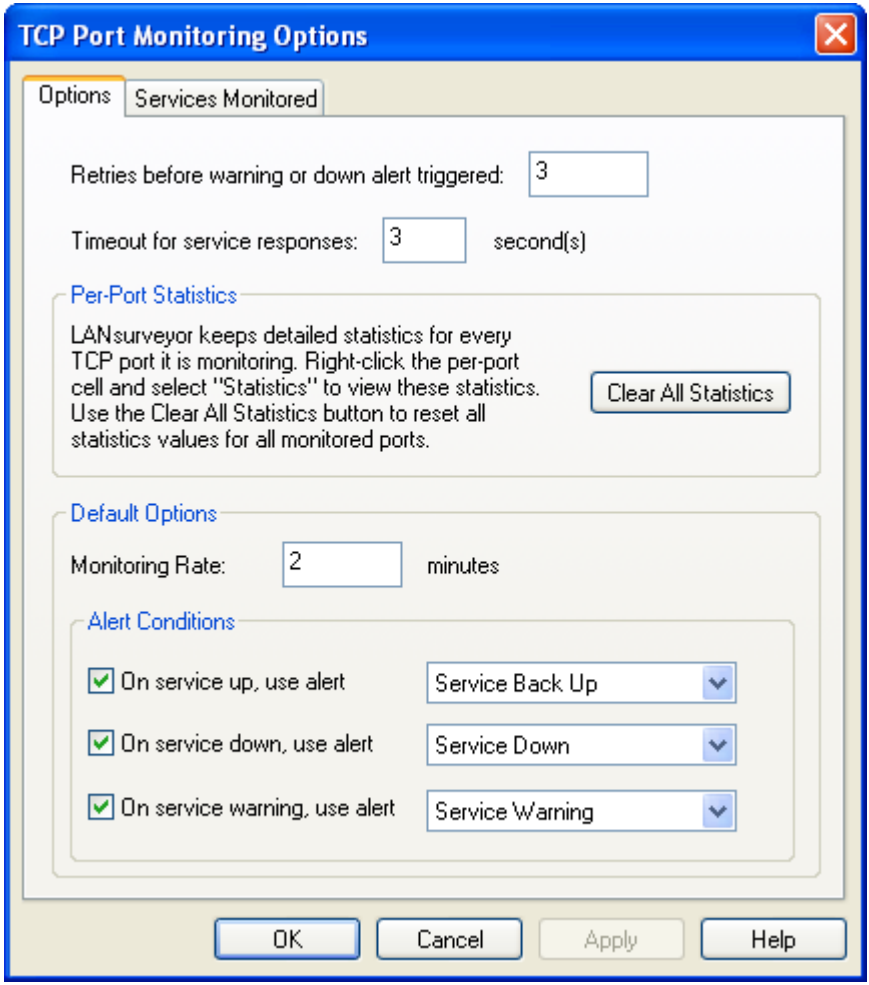
Click on the Options button on the TCP Port Monitor window or select **TCP Port>Options** from the **Monitor** menu to set the TCP Port Monitor options.

Specify the number of retries LANsurveyor should use before warning or declaring the TCP port "down" as well as the number of seconds LANsurveyor should wait for a response from the TCP port.

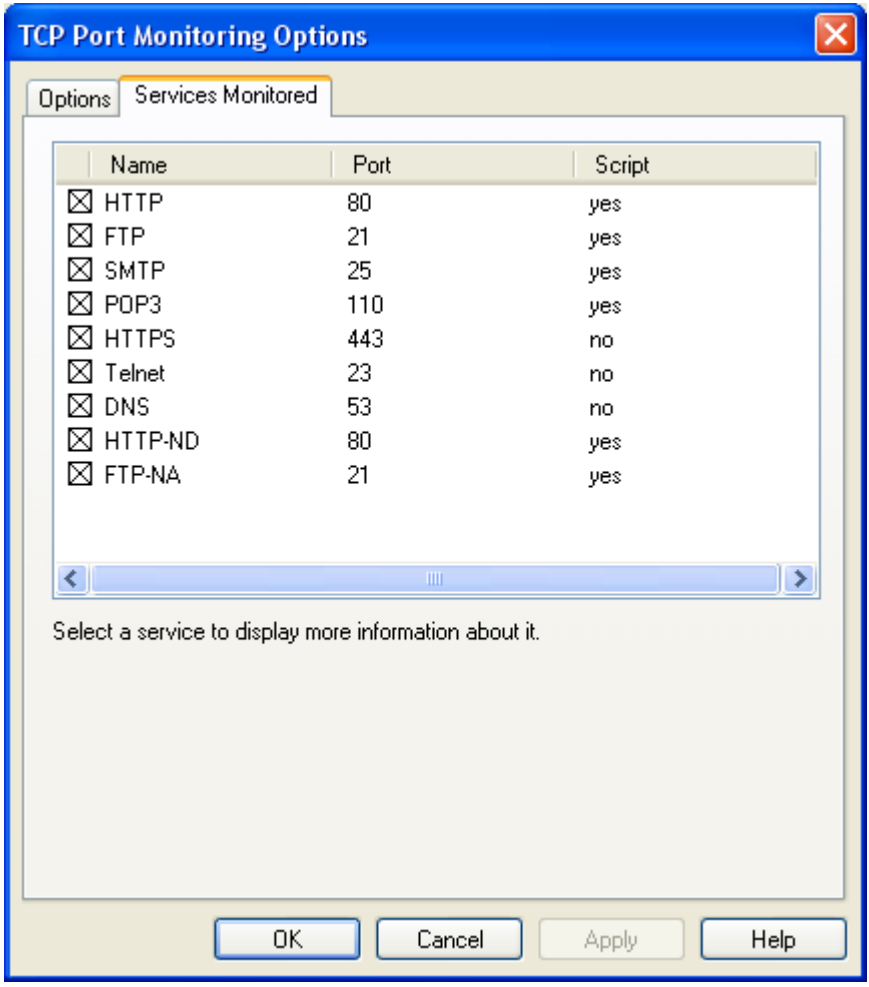
LANsurveyor keeps detailed statistics for every TCP port monitored. Right-click on the cell and select **Statistics** to view the statistics. Click on the **Clear All Statistics** button to reset all statistics for all monitored ports.

The **Default Options** section includes the monitoring rate (in minutes) as well as the alert actions to take when port up, down, or warning conditions are triggered. Alerts are edge-triggered. For example, if a TCP port is not responding after the specified number of retries, LANsurveyor will send the selected alert. No further "down" alert will be sent unless the port becomes available and then fails again.

If you want different monitoring rates and/or alerts for different nodes and ports, use the custom **TCP Ports Options** dialog.

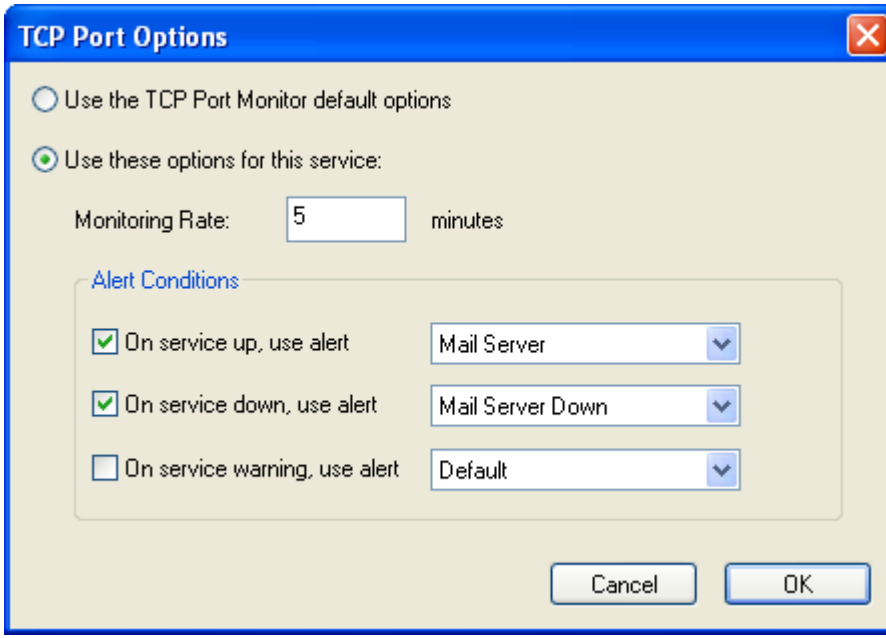


The **Services Monitored** tab of the **TCP Port Monitoring Options** dialog provides a list of applications or servers available for monitoring and allows you to select which are displayed in the columns of the TCP Port Monitoring window. Only checked items will appear on the monitoring window.


TCP Port Monitoring Options
Options
Services Monitored
Name
Port
Script
HTTP 80 yes
FTP 21 yes
SMTP 25 yes
POP3 110 yes
HTTPS 443 no
Telnet 23 no
DNS 53 no
HTTP-ND 80 yes
FTP-NA 21 yes
Select a service to display more information about it.
OK
Cancel
Apply
Help

Custom TCP Port Options

Some nodes and/or services may be more important than others or may be monitored by different people. LANsurveyor allows you to override the **Default Options** for any cell on the TCP Port Monitor window. Once monitoring is enabled in the cell, right-click in the cell, select **Options**, click **Use these options for this service** and specify the cell-specific monitoring rate and alerts.



Alerts

LANsurveyor has the ability to alert you to potential problems on your network on a real-time basis. LANsurveyor's alert options can notify you of network problems either locally or remotely, so you can be alerted to signs of network trouble before network users begin complaining. LANsurveyor's extensive alert capabilities are used in conjunction with TCP Port Monitor and Continuous Scan intrusion detection.

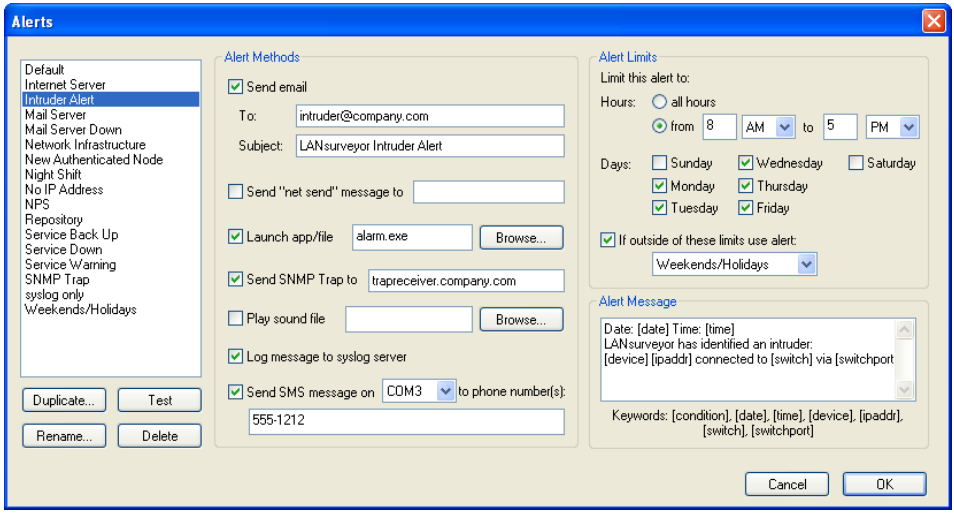
LANsurveyor's alerts are what is known as "edge-triggered." This means that when an alert condition occurs, any configured alerts are sent and the alerts will not be sent again until:

- the alert condition no longer exists and
- the alert condition then occurs again

Click on the Alerts toolbar icon or select **Alerts** from the **Edit** menu to Set Up Alerts.

The Alerts dialog box is made up of three types of alerts. Any combination of these alerts can be formed into a named alert.

To create a new alert, select one of the existing alert names and click the **Duplicate** button. After naming the new alert, enable one or more of the alert options and, if desired, the alert message. The "Default" alert configuration will always be present. Click the **Rename** button to rename an alert configuration. Click the **Delete** button to delete an alert configuration.



Email

Check this option to receive LANsurveyor alerts via SMTP (Simple Mail Transfer Protocol). After enabling this alert, enter the email address or addresses and subject in the **To** and **Subject** edit fields. If you would like to send email to multiple email addresses, separate each email address by a comma. Please make sure to configure the **Primary Email Server**, the **Backup Email Server** and **Email From Address** in the Options dialog box (select **Options** from the **Tools** menu).

net send

Use the "net send" command to send text messages across a network to another Windows computer.

Launch app/file

When the alert is triggered, launch the specified application or open the specified file. This allows you to integrate LANsurveyor alerts into other applications or begin trouble-shooting automatically.

SNMP Trap

Send SNMP traps to communicate with another SNMP-based network monitoring system. The trap sent is the contents of the Alert Message.

Play sound file

Plays the specified sound file for an audio alert.

Log message to syslog server

Logs the error message to the syslog server you specify in LANsurveyor's Network Options.

Send SMS message

Send an SMS alert using an attached phone. The phone must be capable of sending SMS messages as a modem through a COM port on the computer running LANsurveyor. For more information on capable phones, visit http://www.solarwinds.com/lansurveyor/SMS.html.

Alert Message

Use the **Alert Message** edit field to modify the contents of the alert message sent. LANsurveyor recognizes seven keywords within the contents of the alert message: condition, date, time, node name, IP address, switch name, and switch port. Whenever LANsurveyor encounters one of these key words enclosed by square brackets ([ ]), LANsurveyor replaces the appropriate text for the keyword. For example, the time keyword will be replaced by the time that the alert condition is detected.

Alert Limits

You can configure alerts to only function within certain timeframes. This feature lets you monitor conditions within specific hours (e.g., only notify if a system is unavailable during the work day) and allows you to have different alerts for nights and weekends.

It's easy to set up: simply configure your primary alert with the correct time frame and days of the week. Then, specify which alert to use if the problem occurs outside the alert limit (or leave un-checked if you want no alert outside the timeframe specified). If an alert is specified, that alert's timeframe is then checked. If the alert occurs outside the second alert's timeframe, the next alert specified is used and so on.

This allows you to have a workday alert, a weekday evening alert, and a weekend alert all configured for the same alert condition.

Test Your Alert Settings

After you have set the desired alert options, use the **Test Alert** button to have LANsurveyor simulate an alert condition. For example, if you have checked the **Send email** option, clicking **Test Alert** will cause LANsurveyor to send an SMTP message to the designated recipients.

Note: if your alert email fails, make sure you have the proper settings established under Network Options in the LANsurveyor application preferences.

Session Log

Alerts are logged in LANsurveyor's Session Log. Select **Session Log** from the **Window** menu to view the session log.

Notes:

Reports

Create Reports

LANsurveyor features several different types of reports:

- Get Info
- Standard Reports
  - Backup Profiler
  - Software Inventory
  - Software Meter
  - Missing Software
  - Hardware Inventory
  - Switch/Hub Ports
- Custom Reports

To take full advantage of LANsurveyor's reporting features, make sure you have drawn your map after installing the optional Responder clients on every Windows, Linux, and Macintosh computer. In addition, use SNMP with the correct SNMP community string (or password) when drawing the map.

LANsurveyor also includes support for a database Repository that allows for ongoing information collection from workstations and servers running the Responder client software. This feature allows you to create most asset reports whether or not the system is available on the network at the time the report is created.

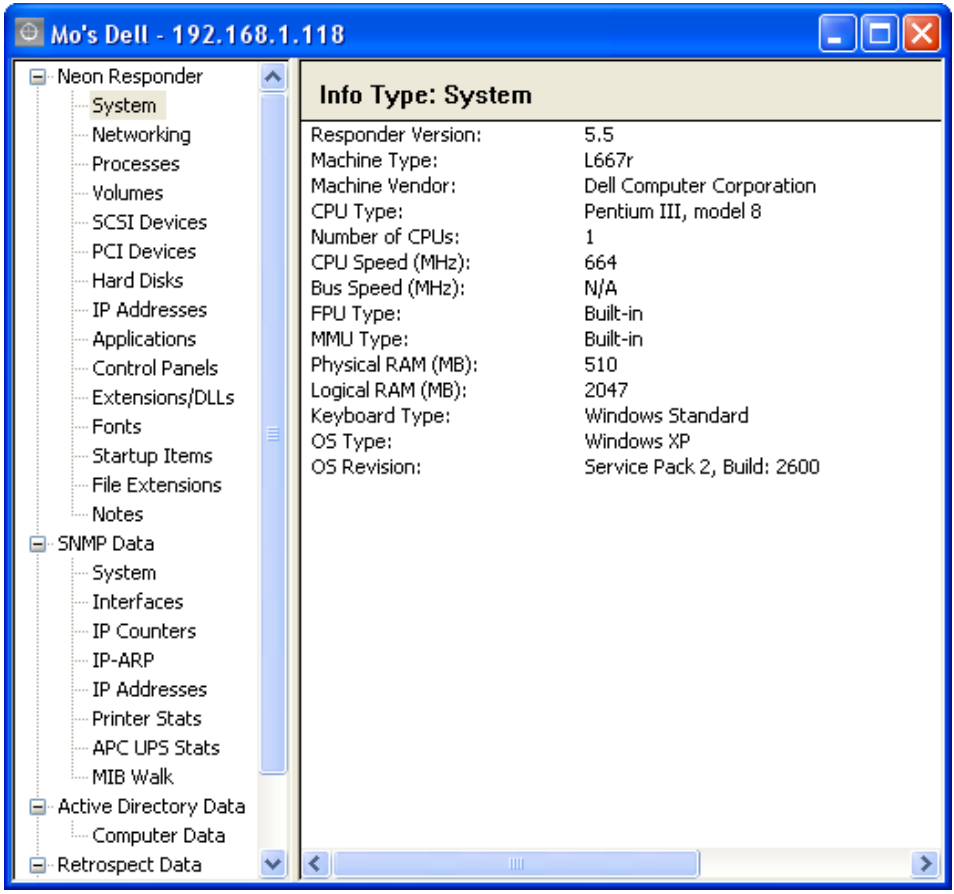
For a complete list of all the information fields available and their definitions, refer to LANsurveyor Report Fields.

Once you have created a report, you can:

- Save and Open Reports
- Rerun and Modify Reports
- Export Reports to Excel

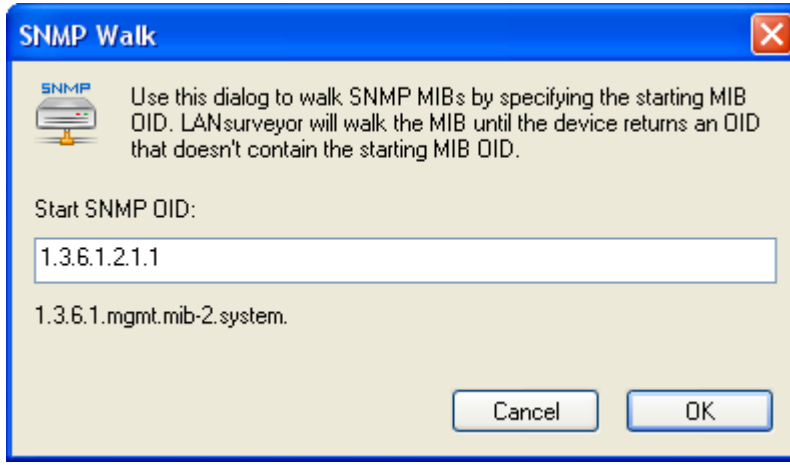
Instant Information

Get instant, live information about any map item by clicking on the map item and selecting **Get Info** from the **Tools** menu or double-clicking on the map icon. Get information about more than one item by selecting them and clicking on the Get Info icon.



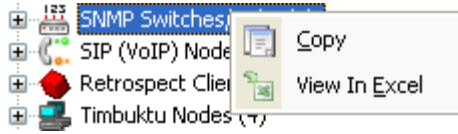
Most of the data available in both standard and custom reports is available through Get Info. Use the Get Info window's left navigation pane to choose which information is displayed. If you want to copy or save information from one or more nodes, use either a Standard Report or a Custom Report.

You can also use **Get Info** to SNMP MIB Walk. Click on **MIB Walk** and enter the starting SNMP OID (object identifier definition) then OK.



Lists from Left-Hand Navigation

Obtain node or network information from the map using the left-hand navigation tree. Click on any category to select that category (e.g., Network Segments) then right-click on the same category to either copy the information to the clipboard or open the information in Excel.



Repository

LANsurveyor's Repository collects asset data from SNMP-enabled network equipment in addition to workstations and servers running the Responder client software and stores the data on a regular basis in a database. LANsurveyor uses either Microsoft SQL Server Express or Microsoft SQL Server (either locally or across the network).

This chapter covers pre-installation considerations as well as Repository setup.

Responder clients

Asset data stored in the Repository is gathered from systems running the optional Responder client software. In order to store data in the Repository, Responder clients must be version 5.4 or later. Refer to the Install Responder clients or Upgrade Responder client sections of this manual for more information.

Responder clients are assigned their primary database key based on the millisecond the LANsurveyor system installs the key.

SNMP-enabled Network Equipment

SNMP asset data can also be stored in the Repository including basic configuration information, printer statistics, and APC-specific UPS data.

Architecture Considerations

If you plan to use just one copy of LANsurveyor at your site, you can skip this section. You can also skip this section if you plan to implement multiple copies of LANsurveyor with independent Repository databases.

If your organization plans to implement more than one copy of LANsurveyor with a shared database, you need to consider which copy of LANsurveyor will be responsible for gathering data from which clients. The responsibility for gathering client data lies with the LANsurveyor applications and is based on the maps either opened or specified at each copy of LANsurveyor under AutoOpen options.

Computers included on maps opened by multiple copies of LANsurveyor will be subject to multiple Repository requests within the same data collection period. There will not be multiple primary records for the computers; rather, there will be duplicate entries for individual pieces of information, such as memory, CPU speed, etc. For example, if there are two copies of LANsurveyor, a central SQL Server Repository, and the Repository is set to gather information once a week from each system, each system included on the active or specified LANsurveyor diagrams of both LANsurveyor systems will have information gathered twice per week rather than once per week.

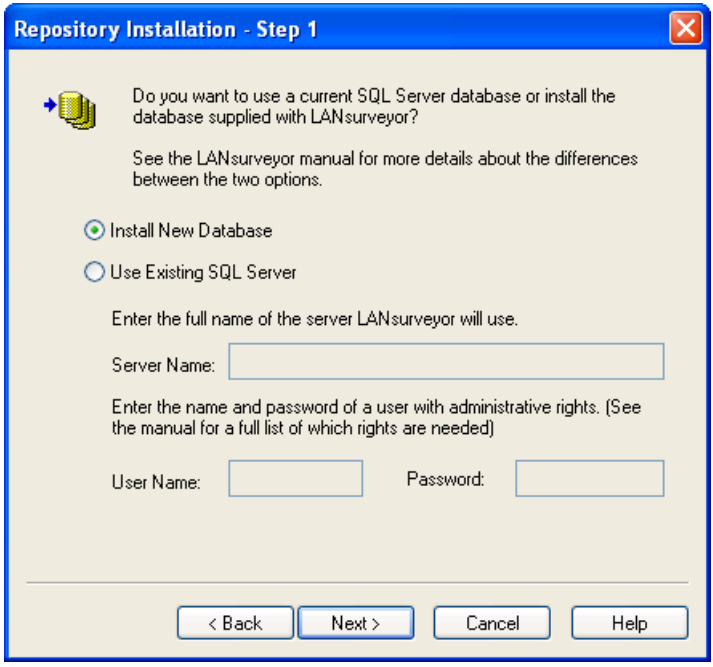
Sites with multiple copies of LANsurveyor may share maps between systems so each copy has access to a superset of network data. In order to prevent inadvertent duplication of Repository resources, each copy of LANsurveyor can specify which maps should be used for Repository tasks using the AutoOpen option.

Repository Installation

To install, configure and run the Repository, select **Tools>Options** and click on the **Repository** tab. Click the "Install Repository" button to begin the process.

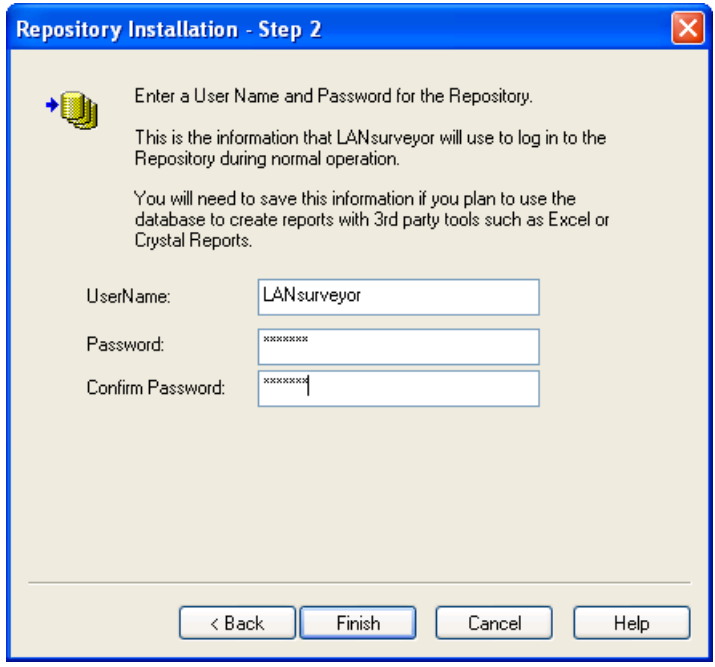
You can either connect to an existing SQL Server or have LANsurveyor install a new SQL Server Express database.

If you choose to use an existing SQL Server installation, you must provide an administrator's login name and password (or a login with enough permissions to create a database and run the *sp_addlogin* stored procedure).

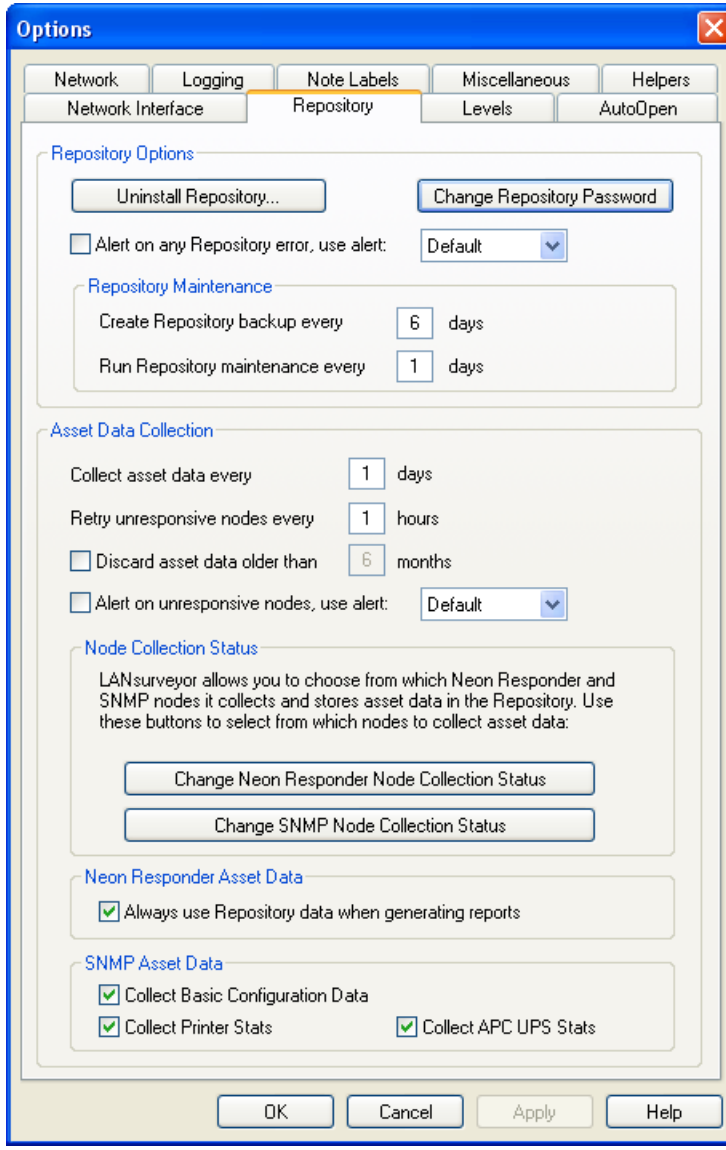


The most current installation instructions and links to supported SQL Server Express software are available on the SolarWinds website at http://www.solarwinds.com/lansurveyor/RepositoryInstructions.htm.

If you choose to install a new database, the next step in the wizard allows you to select your user name and password for this installation.



Once the Repository is successfully installed, the other options become available.



If you have maps created with prior versions of LANsurveyor or older Responder client software installed, you will need to upgrade your Responder client software and draw a new map to begin data capture.

Repository Options

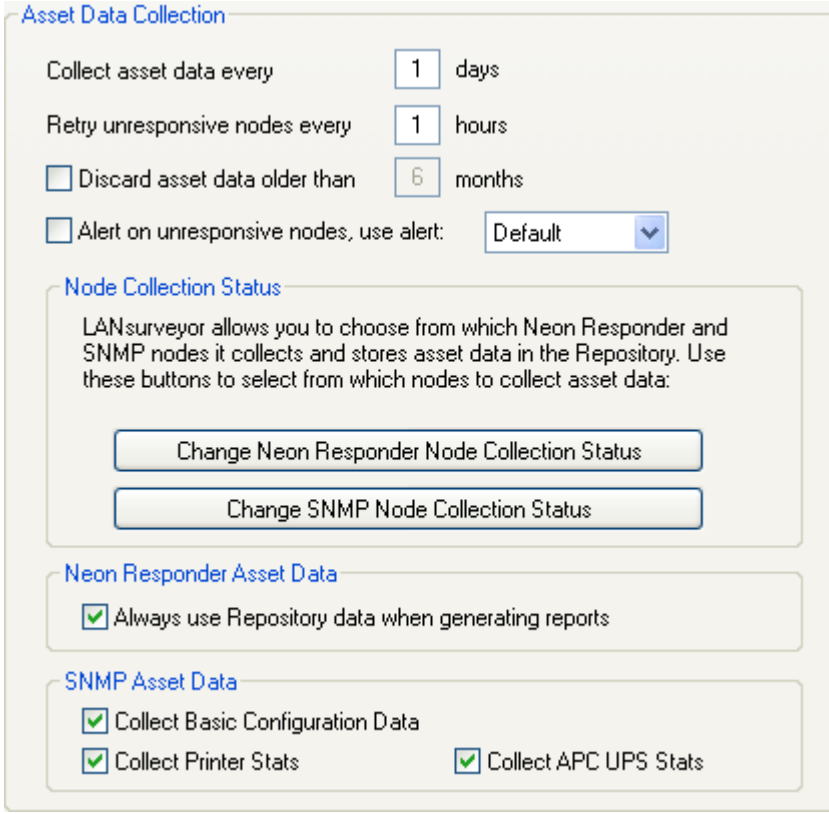
LANsurveyor includes built-in database maintenance utilities to optimize and protect your Repository. You can set the frequency of backup and internal maintenance routines as well as specify an alert should LANsurveyor encounter a Repository error.

Click Change Repository Password to change the database login name and/or access password using this dialog box:

Asset Data Collection

The Asset Data Collection section of the Repository tab allows you to specify Repository settings for this specific copy of LANsurveyor. LANsurveyor will attempt to collect asset data during the period you specify trying every "n" hours to connect if the a system is not available at the collection time.

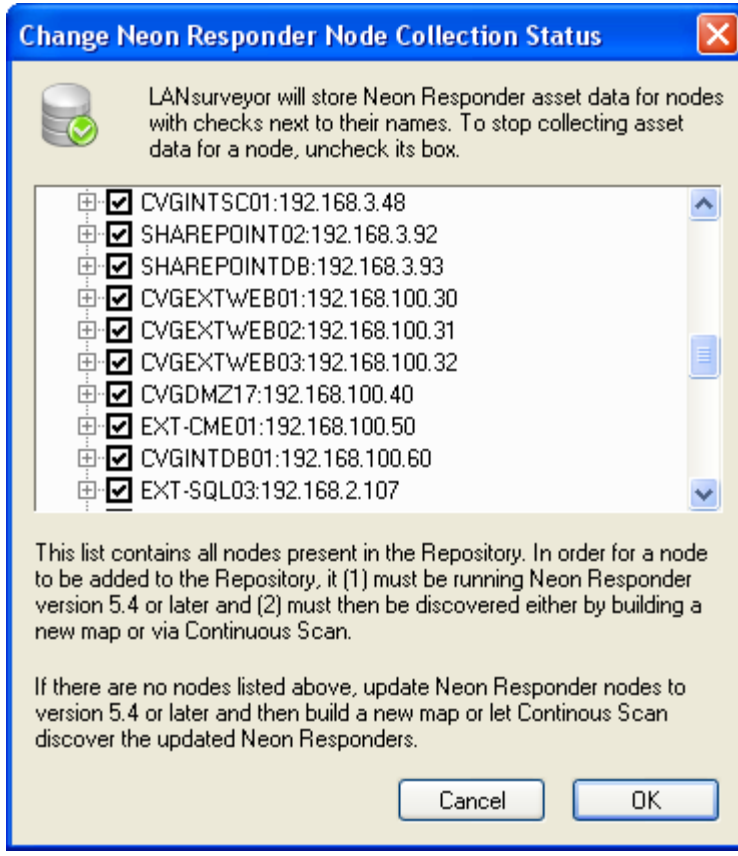
This section also includes a **Discard asset data older than** grooming capability to help minimize the database resources used to maintain asset information.



If **Always use Repository data when generating reports** is selected, LANsurveyor will use Repository for all custom reports with Responder client data fields as well as the Software Inventory, Missing Software, and Hardware Inventory standard reports. LANsurveyor will never use the Repository for Backup Profiler, Software Meter, or Get Info reports as these are real-time in nature.

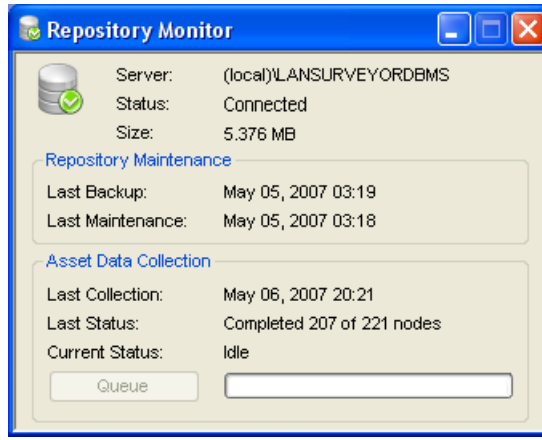
If LANsurveyor fails to gather asset data within the given number of days, selecting **Alert on unresponsive nodes** will cause an alert to be sent for each missing node.

After the Repository is created and a new LANsurveyor map is generated, Responder clients and SNMP systems are automatically tracked in the Repository. You can specify which SNMP and Responder nodes are included in the Repository using the Change Collection Status buttons.


Change Neon Responder Node Collection Status
LANsurveyor will store Neon Responder asset data for nodes with checks next to their names. To stop collecting asset data for a node, uncheck its box.
CVGINTSC01:192.168.3.48
SHAREPOINT02:192.168.3.92
SHAREPOINTDB:192.168.3.93
CVGEXTWEB01:192.168.100.30
CVGEXTWEB02:192.168.100.31
CVGEXTWEB03:192.168.100.32
CVGDMZ17:192.168.100.40
EXT-CME01:192.168.100.50
CVGINTDB01:192.168.100.60
EXT-SQL03:192.168.2.107
This list contains all nodes present in the Repository. In order for a node to be added to the Repository, it (1) must be running Neon Responder version 5.4 or later and (2) must then be discovered either by building a new map or via Continuous Scan.
If there are no nodes listed above, update Neon Responder nodes to version 5.4 or later and then build a new map or let Continous Scan discover the updated Neon Responders.
Cancel
OK

Repository Monitor

The Repository Monitor shows the current status of the Repository database, including the last maintenance operations and any current actions. Select **Repository Monitor** from the **Window** menu to view the Repository Monitor.



If LANsurveyor is unable to collect data from every node within the time specified in the Asset Data Collection section of the Repository options tab, the nodes are listed in the Repository Asset Data List. Press the Queue button to view the list. If the Queue button is unavailable, every node is up to date.

Standard Reports

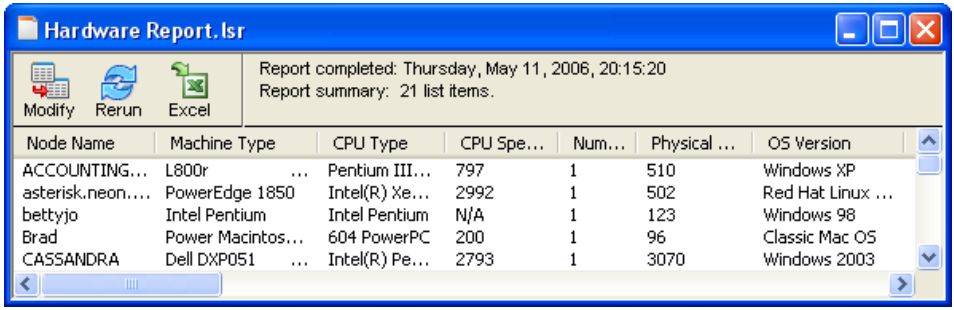
LANsurveyor includes six pre-built standard reports for the most common network documentation requirements. Once a report is created, the report can be modified, rerun, or exported into Microsoft Excel by clicking on the icon or selecting the option from the **Report** menu.

Standard reports include:

- Backup Profiler
- Software Inventory
- Software Meter
- Missing Software
- Hardware Inventory
- Switch/Hub Ports

If you have enabled the LANsurveyor Repository, the Software Inventory, Missing Software, and Hardware Inventory standard reports will use data from the Repository unless **Always use Repository data when generating reports** is unchecked in the Repository options. LANsurveyor will never use the Repository for Backup Profiler or Software Meter reports as these are real-time in nature.

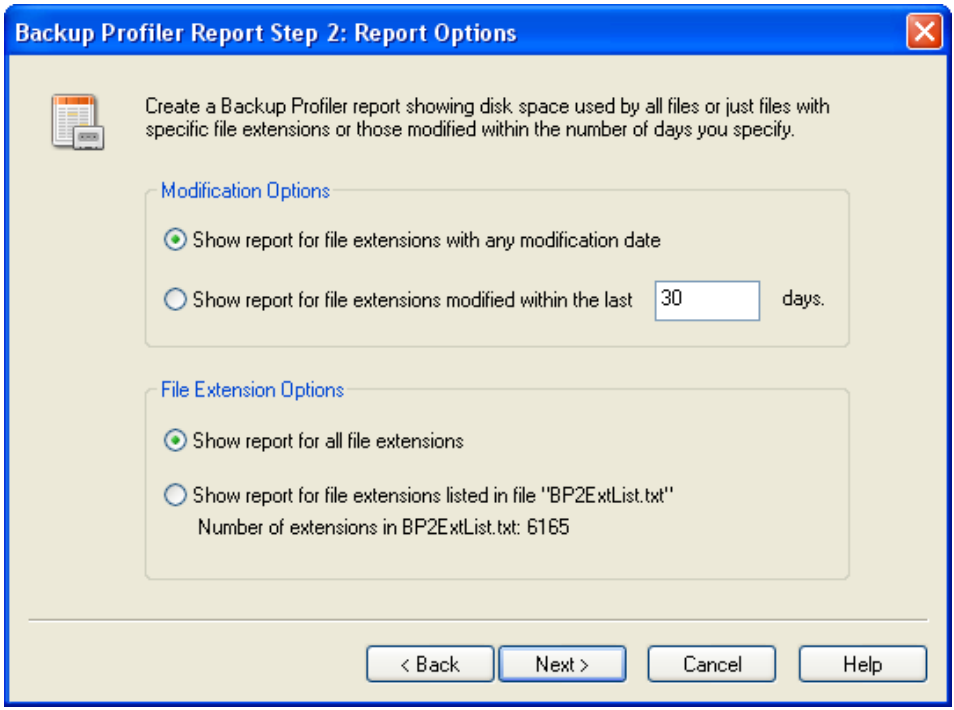
Any report generated using any Repository data lists an **Oldest Repository Data** timestamp in the report header.


Hardware Report.lsr
Modify
Rerun
Excel
Report completed: Thursday, May 11, 2006, 20:15:20
Report summary: 21 list items.
Node Name
Machine Type
CPU Type
CPU Spe...
Num...
Physical ...
OS Version
ACCOUNTING...
L800r ...
Pentium III...
797
1
510
Windows XP
asterisk.neon....
PowerEdge 1850
Intel(R) Xe...
2992
1
502
Red Hat Linux ...
bettyjo
Intel Pentium
Intel Pentium
N/A
1
123
Windows 98
Brad
Power Macintos...
604 PowerPC
200
1
96
Classic Mac OS
CASSANDRA
Dell DXP051 ...
Intel(R) Pe...
2793
1
3070
Windows 2003

Backup Profiler

Backup Profiler provides valuable information for backup and disaster recovery planning. Use Backup Profiler to plan for data security on all your Windows and Mac OS servers and computers with a Responder client installed.

Backup Profiler provides summary information for each volume connected to each computer included in the profile. You may select data that has changed within "n" days, providing an accurate method for determining how much backup storage space would be required for daily, weekly, or bimonthly incremental and differential backups.



The report can include all files on the volumes or just file extensions listed in the "BP2ExtList.txt" file, located in the "SolarWinds/SolarWinds LANsurveyor" subdirectory in the All Users documents folder. The included file includes over 6,000 file extensions and the applications used to create the files, but you may replace or edit the file to include only those files you define as critical to your organization. For example, you could choose to only report on files with .doc, .xls, and .dbf extensions.

The report output includes node name, volume name, volume capacity, volume free space, volume used space, volume throughput (GB/hr), number of files changed, space used by changed files, average file size, number of extensions found, minimum backup time, and all Responder client Note Fields.

Create a Backup Profiler Report by clicking on the Backup Profiler toolbar icon or selecting **New>Backup Profiler** from the **Report** menu. Once selected, the Backup Profiler Wizard is displayed, allowing you to select the nodes with Responder clients, the number of days to include, and the schedule to run the report.

All selected map objects are automatically selected in the first screen of the wizard. Once you have selected the map objects to include in the report, click **Next**. Then choose whether you want to profile all files or just files modified within "n" days. Click **Next**, determine the schedule for running the report, and then click **Finish**. LANsurveyor will then gather the information from the selected nodes.

Software Inventory

Use the Software Inventory Reports to measure software license compliance or to determine software upgrade needs. The Software Inventory Report creates a list of applications, Control Panels, Extensions, Fonts or Startup Items and their versions according to a search pattern you define.

Click on the Software Inventory toolbar icon or select **New>Software Inventory** in the **Report** menu to create a Software Inventory Report. Once selected, the Software Inventory Wizard is displayed, allowing you to select the nodes with Responder clients, the search pattern, and the schedule to run the report.

All selected map objects are automatically selected in the first screen of the wizard. Once you have selected the map objects to include in the report, click **Next**. Then choose which types of files you want to inventory and optionally any text string you would like to use to narrow the search. Click **Next**, determine the schedule for running the report, and then click **Finish**. Depending on your Repository settings, LANsurveyor will either gather the information live or from the Repository.

Software Meter

Use Software Meter Reports to measure software license compliance or to determine software upgrade needs. The Software Meter Report creates a list of running applications and processes according to a search pattern you define.

Click on the Software Meter toolbar icon or select **New>Software Meter** in the **Report** menu to create a Software Meter Report. Once selected, the Software Meter Wizard is displayed, allowing you to select the nodes with Responder clients, the search pattern, and the schedule to run the report.

All selected map objects are automatically selected in the first screen of the wizard. Select the map objects to include in the report then click **Next**. Then optionally choose a text string you would like to use to narrow the search. Click **Next**, determine the schedule for running the report, and then click **Finish**. LANsurveyor will then gather the information from the selected nodes.

Missing Software

Use Missing Software Reports to measure software license compliance or to determine software upgrade needs. The Missing Software Report creates a list of applications, Control Panels, Extensions, Fonts or Startup Items and their versions according to a search pattern you define.

Click on the Missing Software toolbar icon or select **New>Missing Software** in the **Report** menu to create a Missing Software Report. Once selected, the Missing Software Wizard is displayed, allowing you to select the nodes with Responder clients, the search pattern, and the schedule to run the report.

All selected map objects are automatically selected in the first screen of the wizard. Select the map objects to include in the report then click **Next**. Then choose a text string you would like to use to define the search. Click **Next**, determine the schedule for running the report, and then click **Finish**. Depending on your Repository settings, LANsurveyor will either gather the information live or from the Repository.

Hardware Inventory

Use Hardware Inventory Reports to get an overview of the hardware installed on any client computers with a Responder client installed.

The Hardware Inventory Report includes the node name, machine type, CPU type, CPU speed, number of CPUs, RAM, OS version, IP address, router address, net mask, Ethernet Address, number of disks, number of volumes, number of PCI cards, and all Responder client Note Fields.

Click on the Hardware Inventory toolbar icon or select **New>Hardware Inventory** in the **Report** menu to create a Hardware Inventory Report. Once selected, the Hardware Inventory Wizard is displayed, allowing you to select the nodes with Responder clients and the schedule to run the report. Depending on your Repository settings, LANsurveyor will either gather the information live or from the Repository.

Switch/Hub Ports

Use Switch/Hub Ports Reports to obtain a list of managed switches and hubs and the port number, Ethernet address, and IP addresses for each connected device.

Click on the Switch/Hub Ports Report toolbar icon or select **New>Switch/Hub Ports** in the **Report** menu to create a Switch/Hub Ports Report. Once selected, the Switch/Hub Ports Wizard is displayed, allowing you to select the switches, hubs and the schedule to run the report.

Some switches are set by default to flush their Ethernet data relatively frequently. If your Switch/Hub Port reports are not as complete as they should be, consider running the report immediately after creating a new map that includes those end nodes or turn on the Continuous Scan option.

The Switch/Hub Ports report includes the following information:

Switch/Hub Name: name of the switch or hub node, usually the domain name but may be the SNMP machine name (repeats for each port of the device).

IP Address: the IP address of the switch or hub (repeats for each port of the device).

Port Index: the device's internal number for indexing each port. For hubs, these will be unique across the hub. For switches, these may be repeated depending on how many Ethernet addresses have been routed through this port.

Port Description: an optional, usually more descriptive name for the port, as provided by the switch or hub.

Physical Address: the Ethernet address of the device(s) connected to this port. For hubs, there will be only one Ethernet address, which is the last Ethernet address that transmitted data on the port. For switches, there may be multiple rows, each with a different Ethernet address. If a switch port is duplicated this could mean several things:

- this is an uplink or downlink port connecting switches together and the port will list some or all of the up or downstream Ethernet addresses.
- two or more devices with different Ethernet addresses have been connected to this port.
- there is an unmanaged switch or hub uplinked to the port and several nodes with different Ethernet addresses are connected to that unmanaged switch or hub.

Mapped IP Address: LANsurveyor attempts to find the IP address associated with the Ethernet address present in the Physical Address column. This column may be empty if the associated node is down or hasn't communicated via Ethernet for a long period (switch/hub configuration-dependent).

Mapped Node Name: a name associated with the IP address of the previous column, usually the domain name.

Custom Reports

The Custom Report feature allows you to create reports using almost 200 pieces of information. Custom Reports can be saved, rerun, and exported into Microsoft Excel with a single click on the appropriate toolbar icon or selection from the **Report** menu.

Click on the Custom Report toolbar icon or select **New>Custom Report** in the **Report** menu to create a Custom Report. Once selected, the Custom Report Wizard is displayed, allowing you to select nodes, report fields, and the schedule to run the report.

All selected map objects are automatically selected in the first screen of the wizard. Once you have selected the map objects to include in the report, click **Next**. Choose which fields you would like to use in your report. (Refer to Appendix A, "Report Fields" for a complete list of fields and their descriptions.) Click **Next**, determine the schedule for running the report, and then click **Finish**. Depending on your Repository settings, LANsurveyor will either gather the information live or from the Repository.

Save and Open Reports

Any report can be saved to a file and opened later for future reference. To save a report, click on the Save toolbar icon or select **Save** from the **File** menu. Once saved, it can be opened. Click on the Open toolbar icon or select **Open** from the **File** menu.

Rerun and Modify Reports

You can update a report with current information using the parameters you set when you created the report. Click on the Rerun Report button or select **Rerun Report** from the **Report** menu. If you are using LANsurveyor's Repository, any Responder client data will be pulled from the Repository, depending on your Repository settings.

If you would like to make changes in your report options or would like to create a new report based on a template you already created, use Modify Report. To modify a report, open the report you would like to modify and click on the Modify Report button or select **Modify Report** from the **Report** menu. Once selected, the appropriate report wizard is displayed, allowing you to easily make changes to your report.

Export Reports to Excel

Once you have run a report, LANsurveyor displays the report data in a report window. The report data can easily be manipulated and summarized using Microsoft Excel. Simply click on the View in Excel button or select **View in Excel** from the **Report** menu. LANsurveyor creates a temporary, tab-delimited text file with an Excel extension and opens that file in Excel.

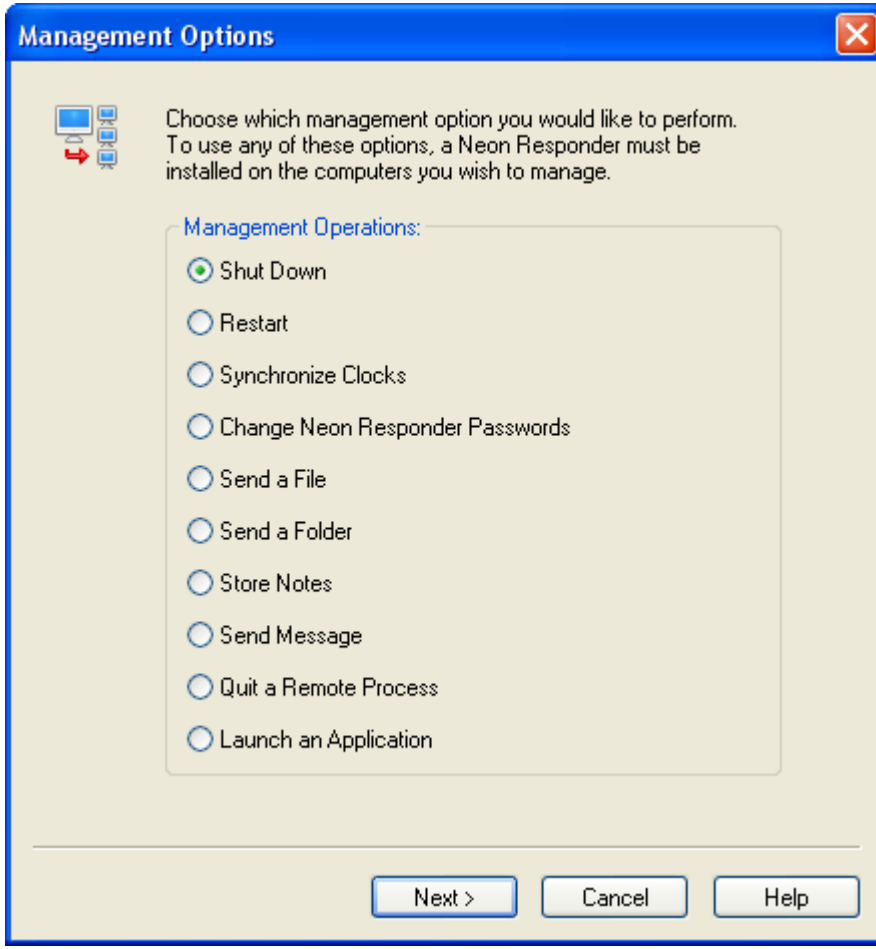
Manage Clients

Remote Client Management

You can use LANsurveyor to remotely manage computers running the Responder client. You gain considerable control over client computers with Responder clients.

Management operations can be performed on a computer-by-computer basis or by selecting a group of computers and applying the operation on these nodes as a group.

There are ten management options. Access any of these options through the Manage Wizard, available from either the **Manage** menu or toolbar icon. There are three or four panes on the wizard: select task, select Responder clients (or verify if already selected on the map), select options specific to that task (if any), and schedule the management task.



If any errors occur during any management operation, LANsurveyor will record details of the error in the Session Log.

Management options include:

- shut down remote computers
- restart remote computers
- synchronize the remote computers' clock with that of the LANsurveyor machine's clock
- change the remote computers' Responder client password
- send a file to the remote computers
- send a folder to the remote computers
- send an instant message to the remote computers
- store notes on the remote computers
- quit a running process (application, INIT, etc.) on a remote computer
- launch an application on a remote computer

The first task for any network manager using LANsurveyor should be to protect the Responder client by installing a password.

Protect Responder Clients

Responder clients installed via Active Directory are password protected using the Deploy Responder client wizard (available from the **Tools** menu). Manually installed Responder clients are installed without a password. Once a password is set, LANsurveyor sends an encrypted password for authentication purposes before making any request of a computer with a Responder client installed.

After installing Responder clients manually, use LANsurveyor to remotely set the password for those Responder clients on open maps. Here are instructions for adding or changing the Responder client password for all Responder clients:

1. Click on the Select Responder clients toolbar icon  or choose **Select>All Neon Responders** from the **Edit** menu.
2. Select **Change Password** from the **Manage** menu or click on the Manage toolbar icon and select Change Password in the Management Wizard and click **Next**.
3. Type in your old password (it doesn't have to match the current password for the map) then enter and confirm the new password and click **Next**.
4. Make the change immediately or at the time you designate and click **Finish**.

If you would like to change the password on specific Responder clients, simply select those nodes in step 1.

Now configure the same password you just entered for the Responder clients into the LANsurveyor application:

5. Choose **Map Properties** from the **Tools** menu.
6. Enter the same password as you typed above into the Responder client Password edit field and click **OK**.

You can have different Responder client passwords for different maps using Map Properties.

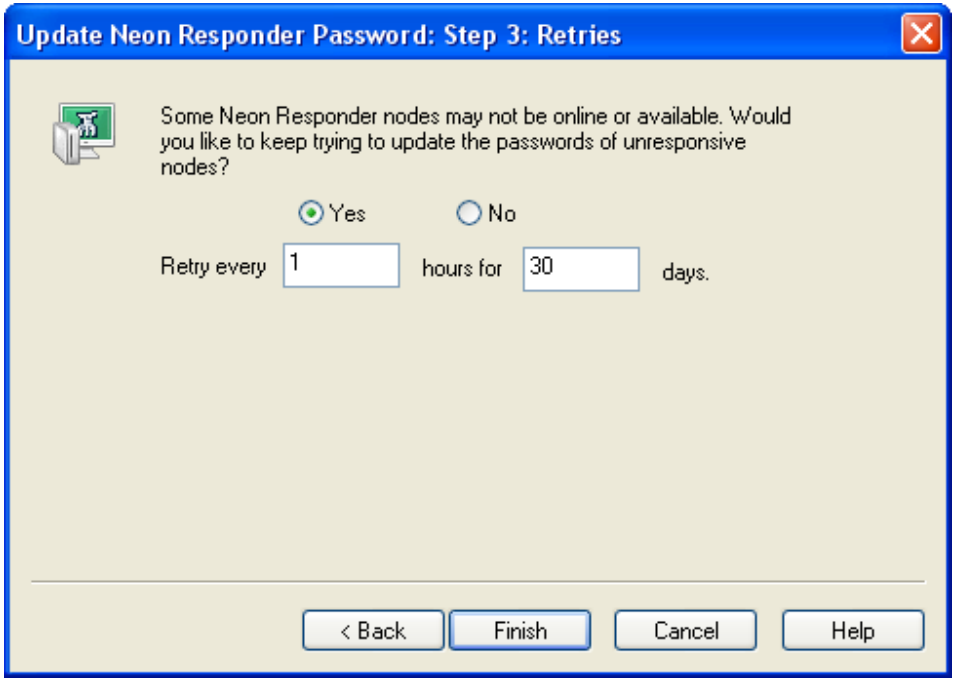
If you would like to change your application preferences to reflect the new password, follow these steps:

7. Choose **Options** from the **Tools** menu. Make sure the **Network** tab is selected.
8. Enter the same password as you typed above into the Responder client Password edit field and click **OK**.

Do not forget your Responder client password. If you do, you will have to uninstall and then re-install all your Responder clients.

Update Responder Password

Some organizations require passwords to be changed on a regular basis. LANsurveyor makes changing Responder client passwords easy. Select **Update Neon Responder Passwords** from the **Tools** menu to launch the password update wizard. Offline nodes are updated when they are discovered again on the network.



Find Responder Clients

The easiest way to find all computers running the Responder client is to click on the Select Responder clients toolbar icon  or choose **Select>All Neon Responders** from the **Edit** menu. LANsurveyor then highlights any nodes running the Responder client on all open maps.

Some management operations might apply to only certain types of computers (e.g., file and folder distribution). Move your mouse over **Select** on the **Edit** menu to choose Responder clients by platform: Windows XP/NT/2000, Windows ME/95/98, Linux, Mac OS X, or Classic Mac OS.

Shut Down

Causes the remote computer to quit all applications and shut down as if a user had selected **Shut Down**.

Note: Some applications running on remote computers may display dialog boxes that require direct user input before a successful shut down. Consequently, while LANsurveyor will report that a remote computer has been successfully shut down, the remote computer may still be waiting for the dialog boxes to be dismissed.

Restart

Quits all applications and restarts the computer as if a user had selected **Restart**. **Restart** is an excellent way to have newly-installed software become active on a remote machine. It is particularly useful in conjunction with the LANsurveyor **Send a File** management operation.

Note: Some applications running on remote computers may display dialog boxes that require direct user input before a successful restart. Consequently, while LANsurveyor will report that a remote computer has been successfully restarted, the remote computer may still be waiting for the dialog boxes to be dismissed.

Synchronize Clocks

Synchronizes the remote computers' clocks with the clock on the LANsurveyor machine. The **Sync Clock** operation is useful to ensure backup dates are correct, database updates are synchronized, and adjustments are made for daylight savings time.

Note: Sync Clock does not take into account time zone settings. This means that the remote computers' clocks will be set to match that of the LANsurveyor machine, independent of the time zone set on any of the machines.

Send a File

The **Send File** operation is an excellent way to install new versions of software on remote machines. For example, if Neon Software produces a new version of the Responder client, you can use **Send File** to distribute the new client software without having to physically visit the remote computer.

Select the file you would like to send and click **Open**. After the file has been selected, specify the destination to which to send the file you have selected. If a file with the same name already exists in that destination on the remote computer, the old file will be moved to the remote computer's Trash or Recycle Bin before the new file is sent from the LANsurveyor machine.

Select the **Launch file after sending** option to automatically launch or open the file on the remote computer.

If you send a file with a ".sit" extension to a Mac OS or Mac OS X system, LANsurveyor will automatically extract the files from the StuffIt® archive.

Software Distribution

Use **Send File** in conjunction with the **Send a Message**, **Quit a Process**, and **Launch an Application** operations to install a new version of a running application.

1. send the new version
2. notify the user of the impending change
3. quit the old version
4. launch the new version

Or, simply **Launch file after sending** for silent installs.

Send a Folder

The **Send Folder** operation is an excellent way to install a new folder of software from the LANsurveyor computer to remote computers. Select the folder you would like to send, then click the **Select** button. After the folder has been selected, LANsurveyor will display the destination selection dialog box.

Software Distribution

Use **Send Folder** in conjunction with the **Send a Message**, **Quit a Process**, and **Launch an Application** operations to install a new version of a running application.

1. send the new version
2. notify the user of the impending change
3. quit the old version
4. launch the new version

Send a Message

The **Send Message** operation is an excellent way to inform users of important information that might otherwise be delayed by such communications methods as voice mail or email. Messages are instantly displayed on the remote machine. After typing the message you'd like to send to the remote user(s), click **OK**. The Responder client will display the message on the remote computer.

Store Notes

Store up to 10 user-defined notes on the remote computer. Notes can be used to record information such as: asset tag numbers, device location, telephone numbers, names of persons responsible for the computer, and purchase and installation date. By default, the note labels will be Note #1 through Note #10. You can change these labels by selecting **Options** from the **Tools** menu and then clicking on the **Note Labels** tab.

Quit a Process

Terminates a running process (application, INIT, etc.) on the remote computer. **Quit Process** will cause LANsurveyor to query the remote Responder client for all running processes then display a list of the running processes. Select the process you would like to quit and click **OK**.

Launch an Application

Starts an application that resides on the remote computer, including silent software installations (no prompts) for remote software distribution. LANsurveyor queries the remote computer for all applications. Select one of the applications from the list and click **OK**. LANsurveyor will then instruct the remote computer to launch the application.

Schedule a Management Operation

The last pane of the Manage Wizard allows you to schedule the management operation. Perform the task immediately or schedule it to occur at some time in the future. Deferred operation is extremely useful for software distribution at off-peak network hours.

For a list of all scheduled operations, select **Scheduled Events** from the **Edit** menu. Use the Scheduled Events dialog box to delete events that you no longer want to occur.

Application Integration

LANsurveyor helps you reduce costs and manage your network more effectively by integrating with a variety of third party applications and tools. This allows you to manage your network by using the map as a console through which other management applications can be used to remotely monitor or control network nodes. You can:

- open a browser to directly manage the device
- launch telnet or an SSH session directly to a device
- use Microsoft's Baseline Security Analyzer (MBSA) to authenticate newly discovered nodes using Continuous Scan
- use Qualys' QualysGuard to authenticate newly discovered nodes using Continuous Scan
- use Symantec's NetRecon to authenticate newly discovered nodes using Continuous Scan
- screen-share using Microsoft's Remote Desktop, VNC, and Netopia's Timbuktu from the LANsurveyor map
- manage switch interfaces directly from the LANsurveyor map

Open Browser

Open a browser directly into any device on the map that supports remote management via http.

To launch a browser from the LANsurveyor map, right-click on the map object or select **Start Web Browser** from the **Tools** menu. LANsurveyor will launch your default browser and open a connection with the selected map object.

Launch Telnet

Telnet is a non-graphical terminal interface used to access devices such as routers.

To launch telnet from the LANsurveyor map, right-click on the map object or select **Start Telnet** from the **Tools** menu. LANsurveyor will launch telnet and will open a telnet session with the selected map object. If a telnet session can be established, a telnet window will open.

Note: you may have to press the Return key in order to receive a telnet prompt.

SSH Client

Use PuTTY or your favorite SSH client to connect to any supported device on your map.

Right-click on the map object or select **Start SSH Client** from the **Tools** menu. LANsurveyor will launch the SSH client software you specify on the Helpers tab.

Microsoft Baseline Security Analyzer

Continuous Scan intrusion detection uses one or more LANsurveyor maps as the baseline network environment. When Continuous Scan is active, LANsurveyor scans the appropriate network ranges and looks for nodes that appear on the network.

Continuous Scan gives you the option of authenticating newly found network nodes. One of the methods Continuous Scan uses to authenticate is Microsoft's Baseline Security Analyzer (MBSA). If the new node fails authentication, Continuous Scan identifies the node as Unauthenticated and takes the actions you specify in Continuous Scan Options.

MBSA is a free, best practices vulnerability assessment tool for the Microsoft platform. It is a tool designed for the IT Professional that helps with the assessment phase of an overall security management strategy. MBSA includes a graphical and command line interface that can perform local or remote scans of Windows systems.

LANsurveyor supports MBSA versions 1.2 or 2.0. You can download MBSA directly from Microsoft's web site. Go to http://www.solarwinds.com/lansurveyor/MBSA.html for up-to-date links and information about MBSA.

Qualys QualysGuard

Continuous Scan intrusion detection uses one or more LANsurveyor maps as the baseline network environment. When Continuous Scan is active, LANsurveyor scans the appropriate network ranges and looks for nodes that appear on the network.

Continuous Scan can authenticate newly found network nodes. One of the methods Continuous Scan uses to authenticate is Qualys' QualysGuard vulnerability management software. QualysGuard can be used to discover vulnerabilities and ensure compliance of the newly found nodes. If the new node fails authentication, Continuous Scan identifies the node as Unauthenticated and takes the actions you specify in Continuous Scan Options.

You can get more information about QualysGuard directly from Qualys' web site. Go to http://www.solarwinds.com/lansurveyor/Qualys.html for up-to-date links and information about QualysGuard.

Symantec NetRecon

Continuous Scan intrusion detection uses one or more LANsurveyor maps as the baseline network environment. When Continuous Scan is active, LANsurveyor scans the appropriate network ranges and looks for nodes that appear on the network.

Continuous Scan gives you the option of authenticating newly found network nodes. One of the methods Continuous Scan uses to authenticate is Symantec's NetRecon vulnerability assessment software. NetRecon can be use to discover vulnerabilities and ensure compliance of the newly found nodes. If the new node fails authentication, Continuous Scan identifies the node as Unauthenticated and takes the actions you specify in Continuous Scan Options.

You can get more information about NetRecon directly from Symantec's web site. Go to http://www.solarwinds.com/lansurveyor/NetRecon.html for up-to-date links and information about NetRecon.

Launch Remote Desktop

Remote Desktop is Microsoft's screen-sharing and control application. Remote Desktop allows users to screen-share and control machines remotely. In order to use LANsurveyor's integrated Remote Desktop features, Remote Desktop must be installed on both the computer running LANsurveyor and the remote computer you would like to control or observe.

To launch Remote Desktop from the LANsurveyor map, right-click on the map object or select **Share Screen>Start Remote Desktop Connection** from the **Tools** menu.

Launch VNC

VNC is an open-source, cross-platform screen-sharing and control application. VNC (Virtual Network Computing) allows users to screen-share and control machines remotely across a wide variety of platforms including Mac OS, Windows and UNIX. In order to use LANsurveyor's integrated VNC features, the VNC client application must be installed on the computer running LANsurveyor, and the VNC server application must be installed on the remote computer you would like to control or observe.

To launch VNC from the LANsurveyor map, right-click on the map object or select **Share Screen>Start VNC** from the **Tools** menu.

VNC is included on the LANsurveyor CD. Please refer to the VNC website (www.realvnc.com) for more information about VNC, to download the latest client and server software, and to monitor for updates to this product.

For more information on configuring Windows 2000 and XP to launch VNC from the map, view our application note: http://www.solarwinds.com/lansurveyor/LS_appnote1.html.

Launch Timbuktu

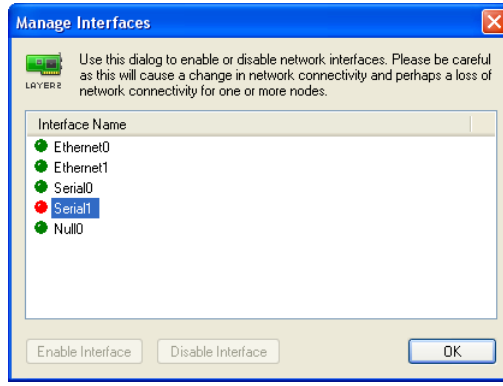
Timbuktu is Netopia's screen-sharing, chat and file-transfer application. In order to use LANsurveyor's integrated Timbuktu features, Timbuktu must be installed on the computer running LANsurveyor and on the remote computer you would like to control or observe via screen-sharing.

To launch Timbuktu from the LANsurveyor map, right-click on the map object or select **Share Screen>Start Timbuktu** from the **Tools** menu. LANsurveyor will launch Timbuktu and automatically start up a screen-sharing Control Session with the map object you have chosen.

Manage SNMP Interfaces

LANsurveyor allows you to directly enable or disable network interfaces for any SNMP device, including managed switch ports. In order to manage interfaces, make sure you have configured the node to include your read/write SNMP community string by clicking on the device and then selecting **Node Properties** from the **Edit** menu.

To enable or disable interfaces, select the SNMP node on your map and then select **Manage Interfaces...** from the **Tools** menu or select **Manage Interfaces...** from the right-click context menu. Interfaces listed with green dots are enabled; red dots indicate the interface is disabled. Select the interface name and press either the Enable Interface or Disable Interface button in the dialog box.

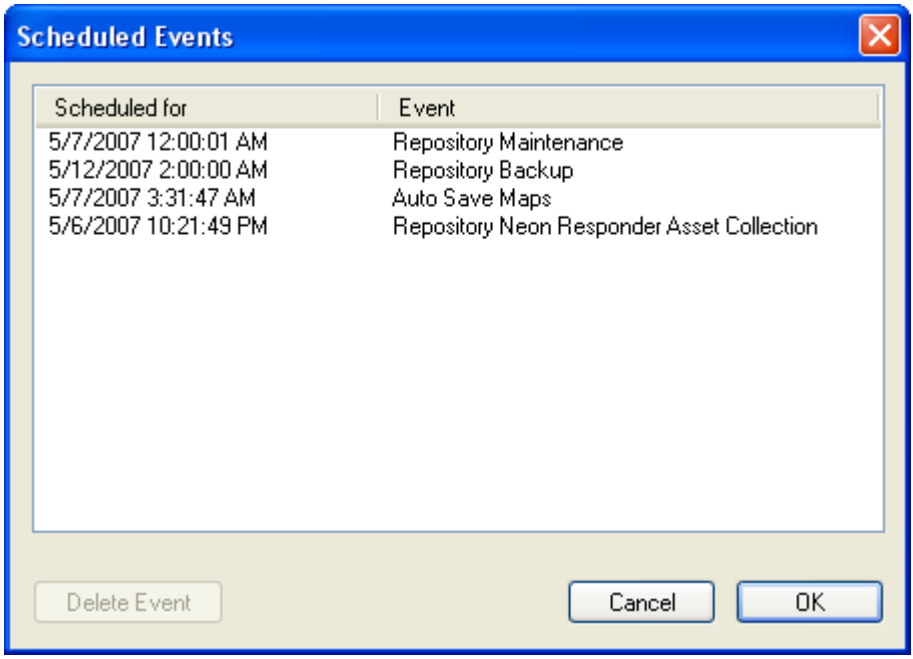


Scheduled Events

Scheduled Events Window

Reports and management operations can be run immediately or scheduled for future execution. Once an operation has been scheduled for future execution, it is added to the Scheduled Events list.

You can view and delete Scheduled Events by selecting **Scheduled Events** from the **Edit** menu. To delete an event, click on it and press "Delete Event."



Event Logging

Session Log Window

LANsurveyor's Session Log keeps an ongoing record of all the significant activities and events LANsurveyor monitors.

Examples of information included in the Session Log include:

- new map creation information, including IP address range and map drawing options
- missing map nodes on Continuous Scan and Rescan
- remote client management operations and the status of those operations
- Repository status and operations and the status of those operations
- report execution
- alerts
- logging nodes on and off the network during Continuous Scan

View the Session Log

Select **Session Log** from the **Window** menu to view the session log. LANsurveyor keeps a record of activity, including network problems, in the Session Log. Use Ctrl-A to select the entire session log for copying/pasting into another application for additional sorting options.

Clear Session Log

Clear the Session Log by selecting all the text in the log and pressing the **Delete** key.

Syslog

LANsurveyor also works with syslog servers, allowing you to log LANsurveyor's node discovery, alerts, and monitoring events. Set your syslog information in the LANsurveyor Options dialog and include syslog entries in your alerts to create syslog entries.

LANsurveyor Preferences

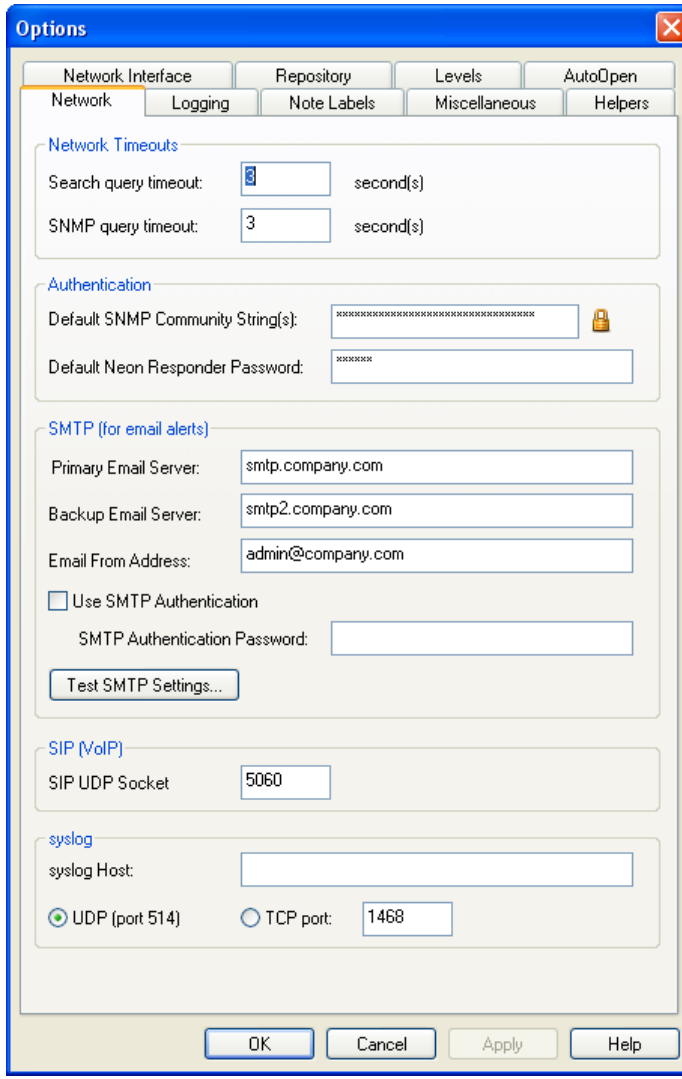
Set Options

Set the LANsurveyor application options by selecting **Options** from the **Tools** menu. All options set in the Options Dialog box are saved with the application and used for alerts, reports, map node access, authentication, logging, and other general application preferences.

Network Options

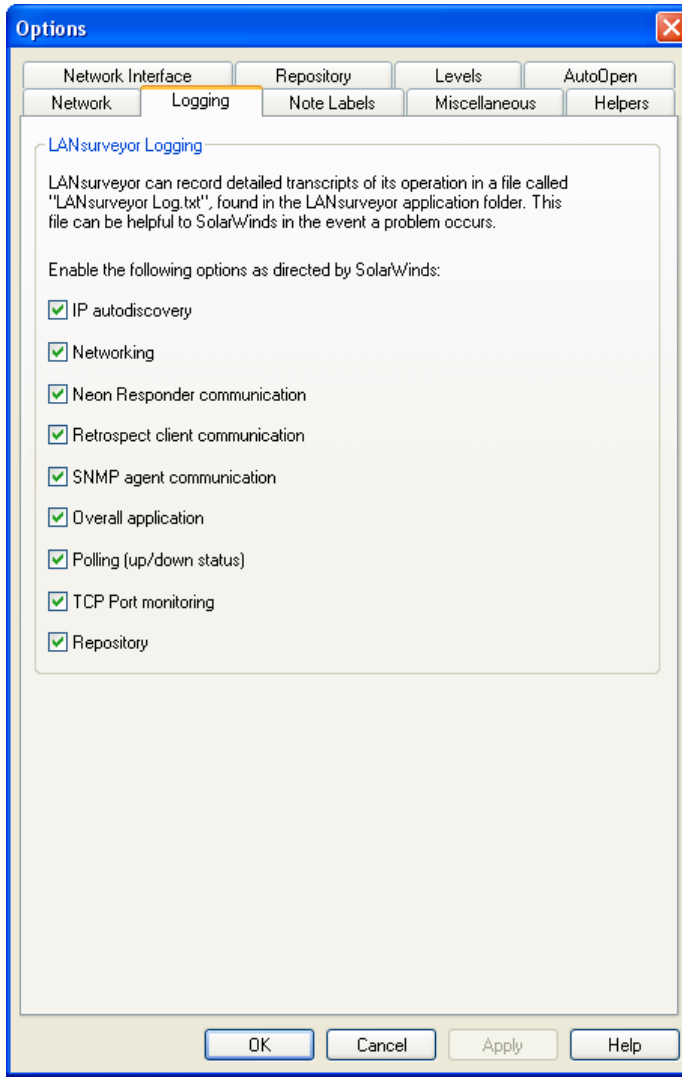
Enter network timeouts, authentication, SMTP email settings, and SIP UDP socket settings via the Network tab. Timeouts are used when querying map objects or creating new maps. Network Timeouts can be changed on a map-by-map basis using the Mapping Speed slider. Authentication is required for accessing node information and reporting. Click the lock icon to show or hide your SNMP community string.

SMTP options are required for email alerts and include SMTP Authentication. The Voice-over-IP SIP UDP Socket number can also be set to match your VoIP environment, and you can specify a syslog host to receive LANsurveyor logging information.


Options
Network Interface
Repository
Levels
AutoOpen
Network
Logging
Note Labels
Miscellaneous
Helpers
Network Timeouts
Search query timeout:
3
second(s)
SNMP query timeout:
3
second(s)
Authentication
Default SNMP Community String(s):
Default Neon Responder Password:
SMTP (for email alerts)
Primary Email Server:
smtp.company.com
Backup Email Server:
smtp2.company.com
Email From Address:
admin@company.com
Use SMTP Authentication
SMTP Authentication Password:
Test SMTP Settings...
SIP (VoIP)
SIP UDP Socket
5060
syslog
syslog Host:
UDP (port 514)
TCP port:
1468
OK
Cancel
Apply
Help

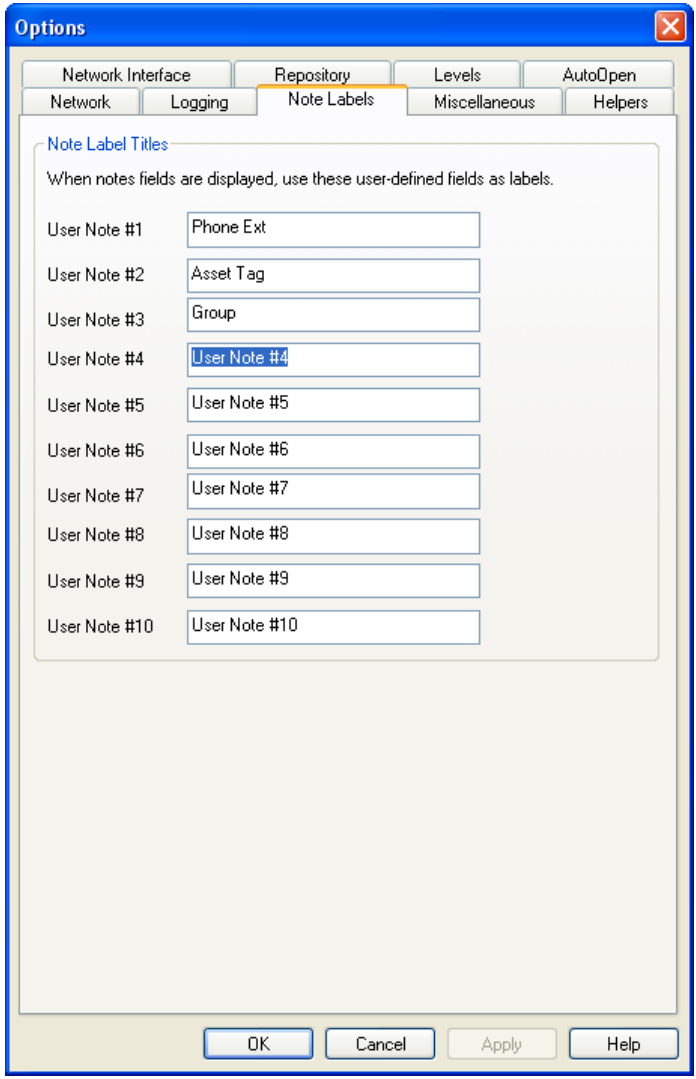
Logging

In addition to the LANsurveyor Session Log, LANsurveyor can maintain a more detailed log in an external text file. The Logging options set which events are recorded and can help pinpoint application errors when working with Neon Software technical support.



Note Labels

Note labels are useful for adding descriptive text for reports. If you customize node labels, the text you enter here replaces "User Note #" in your reports that include Responder client data.



Miscellaneous

Don't show Neon Responder authentication alerts

Responder clients without passwords are automatically detected, and you are presented with the option to update the Responder with the password stored in the Network tab of the Options Dialog box. If you do not want to see this alert, select this option.

Don't show scheduling wizards

Reports and management operations give you the option to schedule those operations at a later time and date. If you would rather not encounter the scheduling portion of the report and management wizards, select this option.

Search private IP address ranges

Some organizations do not route private IP address ranges (e.g., 192.168.x and 10.x). However, many organizations assign these IP address ranges with DHCP servers and wish to map those nodes. If you would like to ignore private IP address ranges, uncheck this option.

Use switch port index rather than network interface name

Some switches have more descriptive switch port index names than network interface names. If you primarily use Cisco equipment, keep this item checked.

Use synchronous reverse-DNS lookups

Due to an anomaly in Windows networking, asynchronous reverse-DNS lookups can cause LANsurveyor to abort. Unchecking this option is not recommended.

Map switch/hub ports

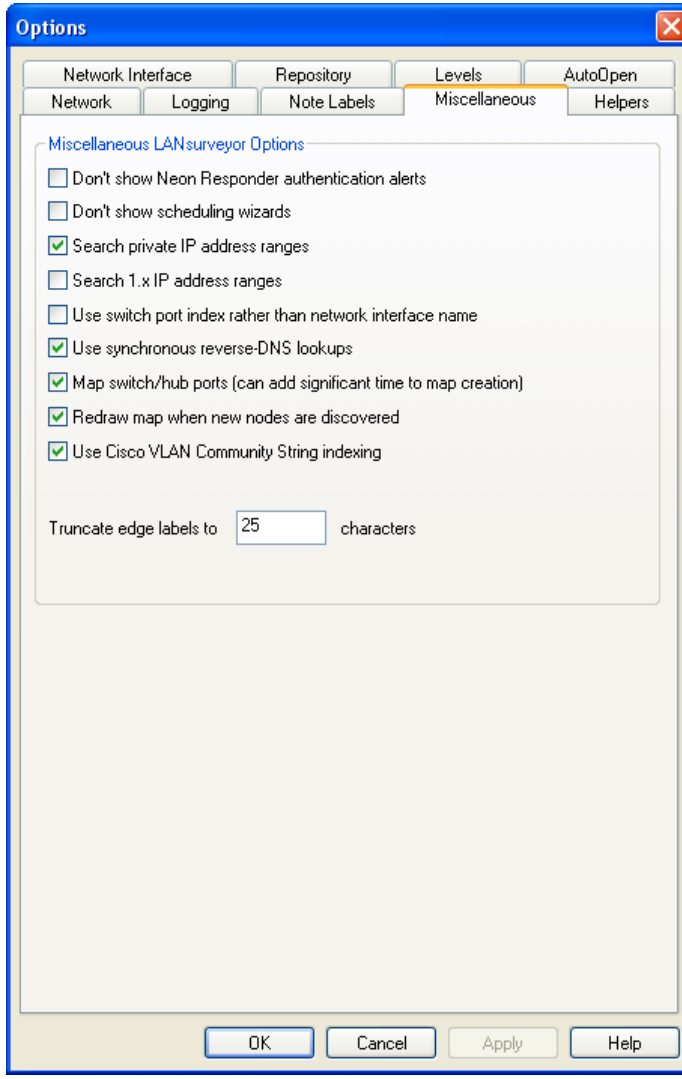
Mapping switch/hub ports can show important information about how your network is physically connected. However, discovering those connections takes more time when drawing maps. You can set LANsurveyor to ignore switch/hub port connections by unchecking this option.

Redraw map when new nodes are discovered

When new nodes are discovered either using Rescan Map or Continuous Scan, LANsurveyor will automatically redraw your map, optimizing the network diagram layout. If you customize your map by moving nodes around and would like to preserve your customizations, uncheck this option.

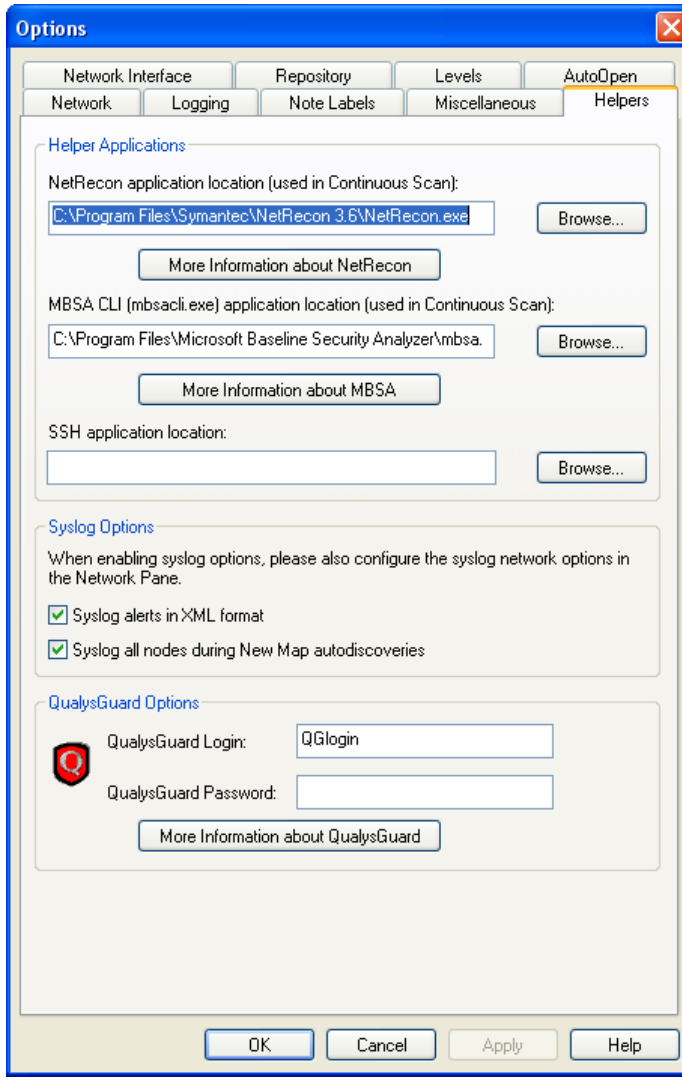
Use Cisco VLAN Community String indexing

If your network equipment uses long port or interface names, you can truncate the map labels automatically to the number of characters you specify.


Options
Network Interface
Repository
Levels
AutoOpen
Network
Logging
Note Labels
Miscellaneous
Helpers
Miscellaneous LANsurveyor Options
Don't show Neon Responder authentication alerts
Don't show scheduling wizards
Search private IP address ranges
Search 1.x IP address ranges
Use switch port index rather than network interface name
Use synchronous reverse-DNS lookups
Map switch/hub ports (can add significant time to map creation)
Redraw map when new nodes are discovered
Use Cisco VLAN Community String indexing
Truncate edge labels to
25
characters
OK
Cancel
Apply
Help

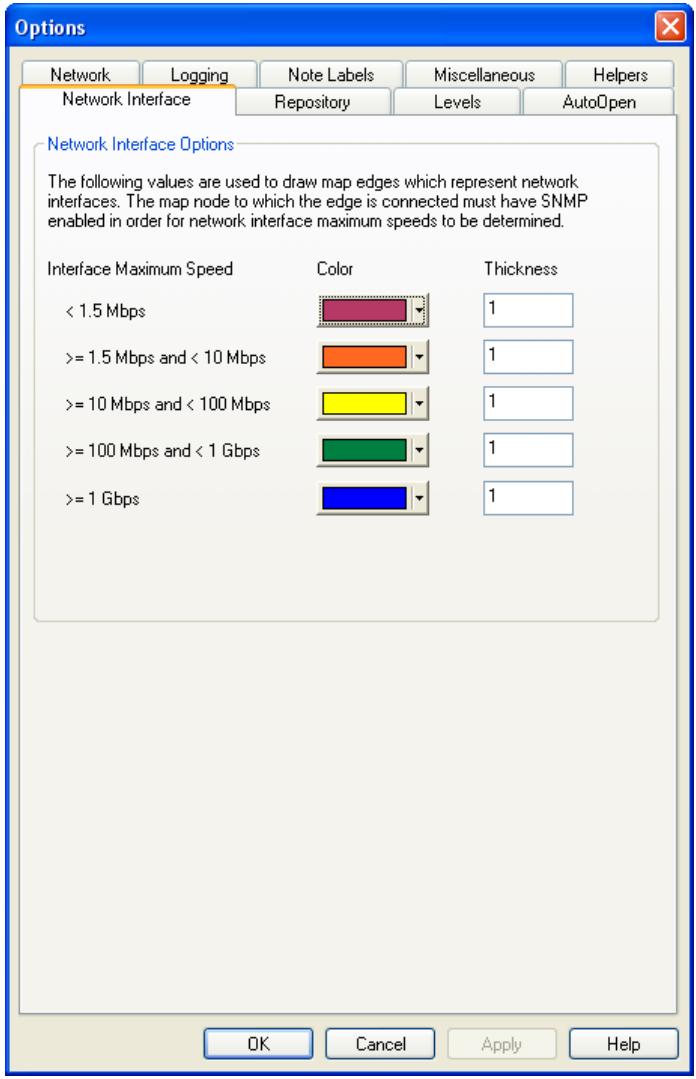
Helpers

LANsurveyor works with third-party applications including Symantec's NetRecon, Microsoft's Baseline Security Analyzer, SSH clients, Qualys' QualysGuard, and syslog servers to increase your network security. Set options for those applications in this dialog box.



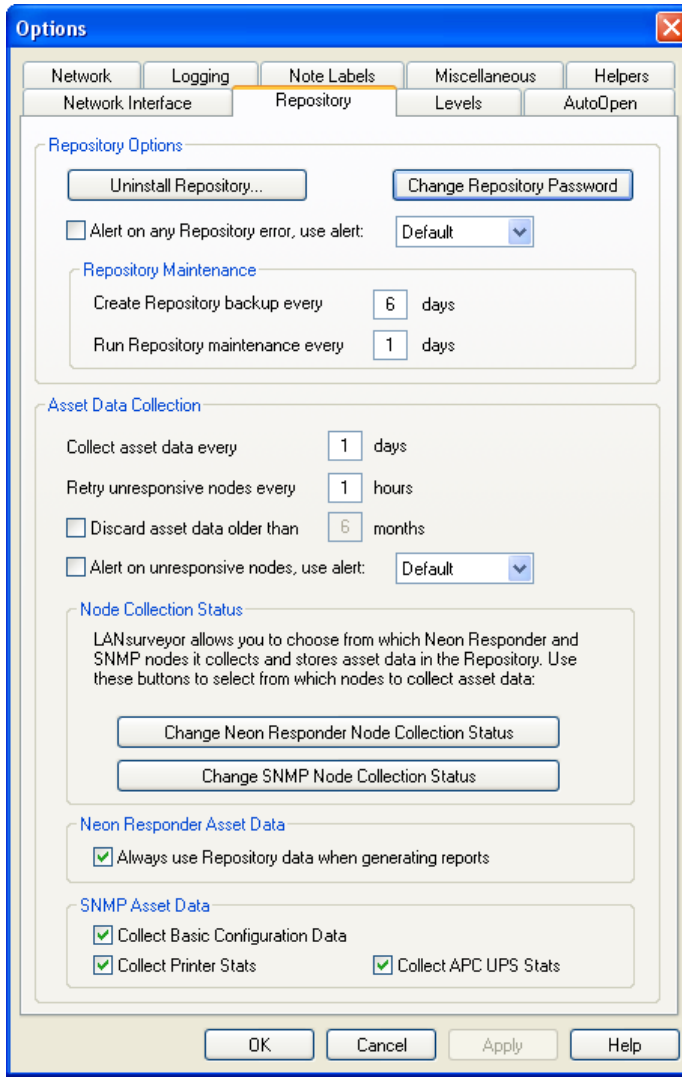
Network Interface

LANsurveyor uses lines (or edges) to connect nodes. If a node has SNMP enabled and the interface speed can be determined, you can specify the color and line thickness of those edges based on the maximum interface speed.



Repository

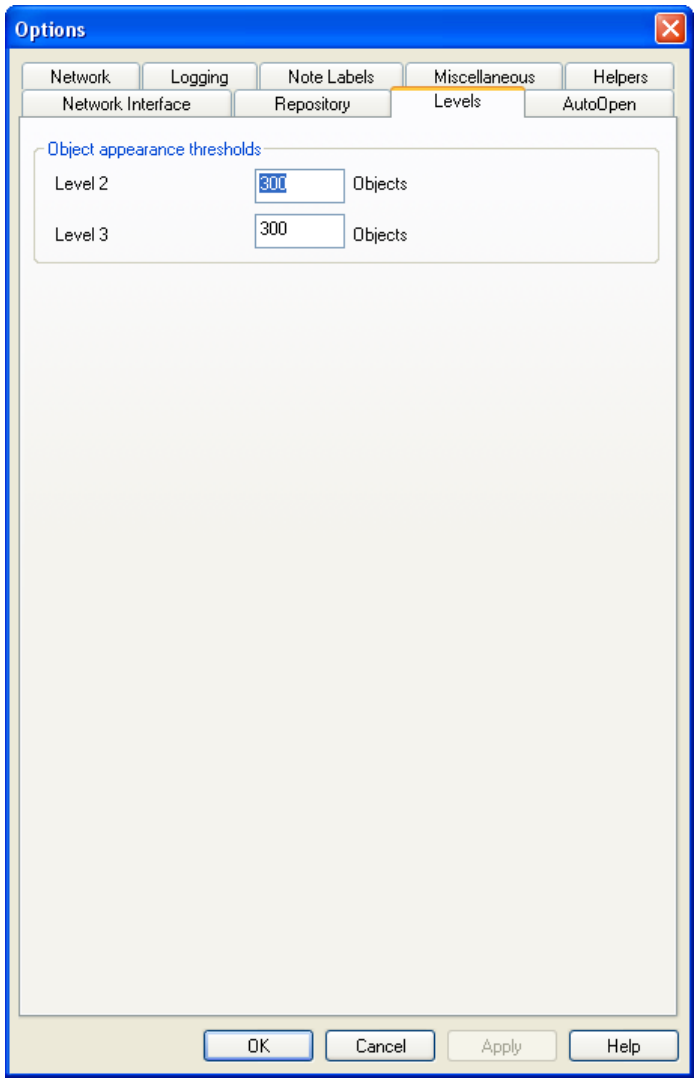
These Repository options are covered in the Reports section of this manual in the Repository chapter.



Levels

Your maps might have thousands of nodes, so LANsurveyor makes it easy to view your maps at different levels. Routers and network segments are Level 1 objects. Switches are Level 2 objects. Everything else is Level 3. If there are more than the specified number of Level 2 objects, routers and network segments (Level 1) will be displayed by default. Likewise, if there are more than the specified number of Level 3 objects, only Level 1 and Level 2 objects will be displayed.

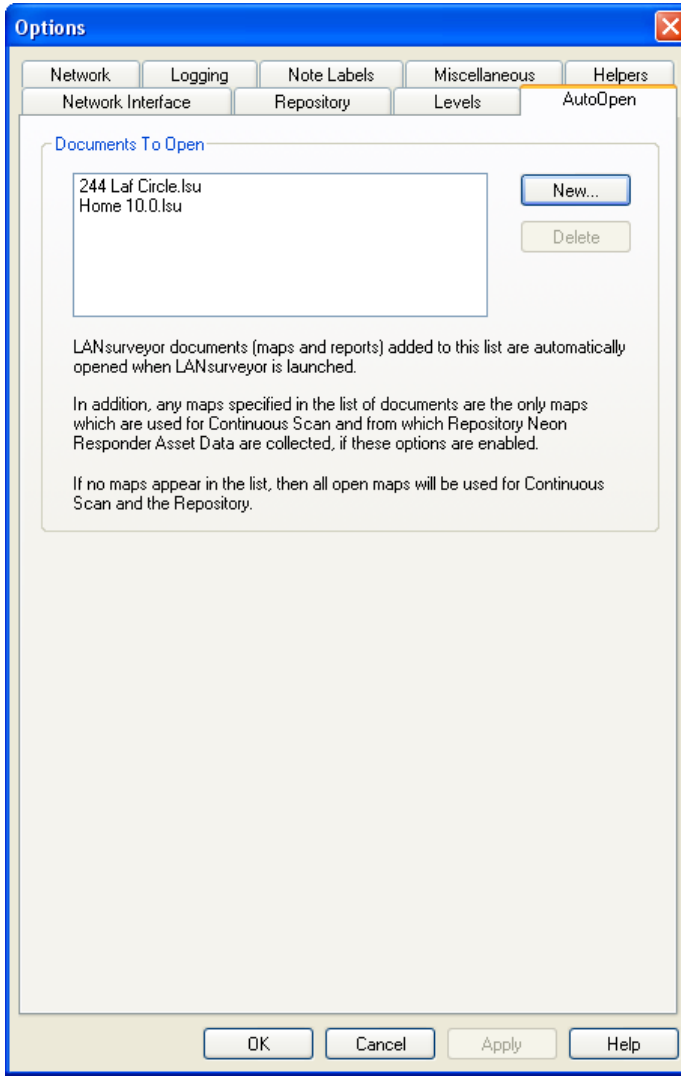
You may also Filter which Level 3 objects are displayed.



AutoOpen

Any LANsurveyor documents selected for AutoOpen are automatically opened when LANsurveyor is launched either manually or when LANsurveyor is run as a service.

If maps are specified, only those maps are used for Continuous Scan and Repository collection.

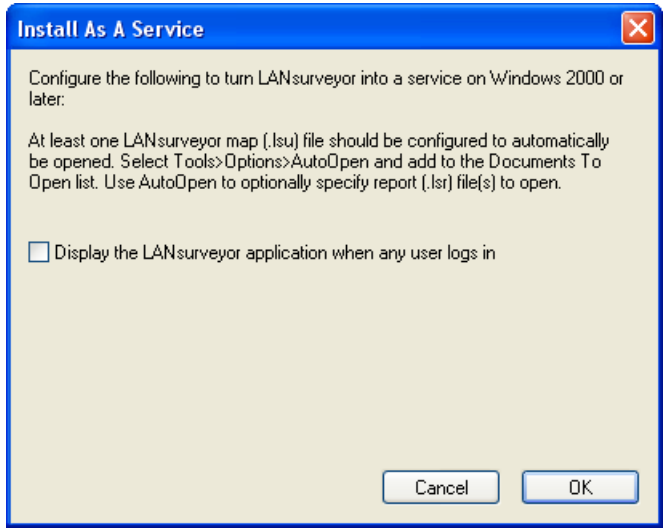


Run as a Service

You may want to run LANsurveyor as a Windows service to ensure network monitoring continues after a power outage or restart.

LANsurveyor can run as a service on your Windows 2000 or later computer. If you run LANsurveyor as a service, LANsurveyor can monitor your network without requiring a user to be logged into the computer. In addition, if your computer restarts, monitoring automatically restarts.

When preparing to run LANsurveyor as a service, log into your computer as the administrator of the computer. This allows LANsurveyor to install properly and assures the options function properly. Then select **Run As A Service...** from the **File** menu to set the service options.



If you want the user interface displayed when any user logs in, click the check box next to **Display the LANsurveyor application**. Click **OK** and LANsurveyor will install the service components.

Once LANsurveyor is running as a service, the manually launched instance of LANsurveyor will exit and the LANsurveyor service will relaunch LANsurveyor. Once the service is started, LANsurveyor will keep relaunching itself to monitor and create reports, even if the logged in user tries to exit the application.

AutoOpen Documents

Any LANsurveyor documents specified in the AutoOpen setting are automatically opened by LANsurveyor when launched as a service. Any specified maps are then available for Continuous Scan and Repository data gathering.

Stop LANsurveyor Service

To stop the service, access the Windows **Start** menu, select **Settings>Control Panel> Administrative Tools>Services**, click on the **LANsurveyor Service**, and select **Stop**.

Uninstall LANsurveyor Service

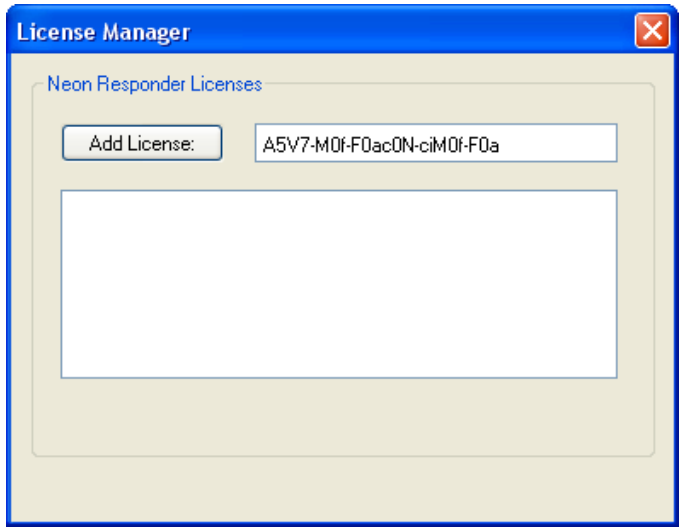
To uninstall the LANsurveyor service, go to the SolarWinds LANsurveyor documents folder (in the Documents folder for All Users) and double-click on the "FireDaemon OEM" folder. Launch the "FireDaemonUI.exe" application, click on the LANsurveyor Service, and select **Uninstall** from the **Service** menu.

Licensed Options

Select **License Manager** from the **Window** menu to access the License Manager Window.

The License Manager Window displays the current status of your Responder client licenses.

To add a license, enter your serial number exactly as you received it from SolarWinds or your supplier. To obtain more licenses, contact your local dealer or visit the SolarWinds web site.



Notes:

Appendix A - Report Fields

This section includes a complete list of fields available from the Get Info window and custom reports, including:

Responder Client Data

Responder client data is available from workstations and servers with the optional Responder client installed. This information is automatically stored in the LANsurveyor Repository if enabled.

System Information

Responder Version: the version of the Responder client currently running.

Machine Type: the model of a computer. LANsurveyor may not be able to differentiate certain types of models and may not be able to identify machines released after the LANsurveyor application.

Machine Vendor: the brand of the computer.

CPU Type: the type of CPU (processor).

Number of CPUs: the number of CPUs installed.

CPU Speed: the clock speed of the CPU. Only available for Windows machines running Windows NT/2K/XP, Linux, and some Mac OS machines.

Bus Speed: the clock speed of the system bus. Not available for Windows machines and may not be available for all Mac OS machines, especially 68k-based machines.

FPU Type: the type of Floating Point Unit.

MMU Type: the type of Memory Management Unit.

Physical RAM: the amount of physical RAM installed.

Logical RAM: the amount of logical RAM available. This value is the same as the Physical RAM when virtual memory is not enabled. On some machines, this value might be less that the Physical RAM because some RAM may be used by the video display and the operating system.

Keyboard Type: the type of keyboard attached.

OS Type: the operating system name.

OS Version: the version number of the operating system.

Networking

TCP/IP version: Windows machines display WinSock. Linux machines display BSD Sockets. Mac OS machines display either Open Transport and its version or MacTCP and its version.

IP Address: an IP address assigned to this machine.

Router Address: an IP address of the machine's router.

Net Mask: an IP net mask assigned to this machine.

IP Ethernet Address: Ethernet hardware (MAC) address assigned to the default TCP/IP interface.

AppleTalk Version: Open Transport or Classic (pre-Open Transport) and the version number for each, if Open Transport is running. Not available for Linux or Windows machines.

AppleTalk Address: the AppleTalk address assigned to this machine, in the form of "net.node". Not available for Linux or Windows machines.

AppleTalk Ethernet Address: the Ethernet hardware (MAC) address assigned to the AppleTalk interface. If AppleTalk is not running on an Ethernet interface, "N/A" will appear. Not available for Linux or Windows machines.

Processes

Process Name: the name of the process.

Process Type: the type of process. For Windows machines, the type will always be Application. For Mac OS, process types include Application, INIT, Background, and Finder.

Process Size: the amount of memory allocated by the process. For computers running Windows 95/98/ME or Mac OS X, this value will always be zero, as it is not available.

Process Active Time: the accumulated time during which the process has used the CPU, including both foreground and background processing time. For Mac OS X and Windows machines running Windows 95/98/ME, this value will always be zero, as it is not available.

Volumes

Volume Name: the name of the volume.

Volume Kind: "Local" indicates that this is a volume directly connected to the machine. "Remote" indicates a shared volume that is mounted over the network.

Volume Capacity: the amount of space available for use on the volume (expressed in megabytes). Windows 98 nodes do not return accurate information for this value.

Volume Free Space: the amount of free space on the volume (expressed in megabytes). Windows 98 nodes do not return accurate information for this value.

SCSI Devices

For Windows machines, SCSI devices can only be discovered and listed if the machine is running Windows NT/2K/XP.

SCSI Bus: the SCSI Bus value. Usually the bus value will be zero, unless an external or expansion SCSI bus is in use on the map object.

SCSI ID: the SCSI I.D. value. This can range from 0 to 7 for each SCSI bus.

SCSI Type: is vendor-specified but usually has a name such as Disk, Tape or CD-ROM.

SCSI Vendor: is usually an abbreviated version of a company name.

SCSI Product: is usually an abbreviated version of a device name.

SCSI Version: is defined by the vendor and may contain unprintable characters.

PCI Devices

PCI Name: the name of the PCI card or device.

PCI Type: the type of PCI card.

PCI Location: the bus the PCI card uses to connect to the system.

PCI Vendor ID: the manufacturer of the card or driver.

Hard Disks

Disk Name/Type: the type or system name for the drive.

Disk Capacity: the capacity of the drive.

IP Addresses

IP Address: the IP address(es) of the node.

Router Address: the router address for this IP address.

Net Mask: the Net Mask for this IP address.

Ethernet Address: Ethernet hardware (MAC) address assigned to this specific TCP/IP interface.

Applications

Application Name: name of the application.

Version: application version number.

Control Panels

Control Panel Name: name of the control panel. Not available for Linux.

Version: control panel version number.

Extensions/DLLs

Extension/DLL Name: all enabled DLLs (Windows) or Extensions (Mac OS) or .so Libraries (Linux) on the startup disk.

Version: Extension or DLL version number.

Fonts

Font Name: name of the font.

Version: font version number.

Startup Items

Startup Item Name: For Windows machines running Windows 95/98/ME, displays a list of all items found in the RunServices Registry entry. Entries in RunServices Registry key are applications that are run automatically when Windows 95/98/ME starts up. The Responder client for Windows is an example of such an application. For Windows machines running Windows NT, 2000 and XP, displays a list of all NT Services and their status. For Linux, the list of daemons run at system startup. For Mac OS, displays a list of all items found in the Startup Folder.

Startup Version/Status: version or status of the startup item.

File Extensions

File Extension: up to four letters or numbers found after the period at the end of a file name. If a file has no extension, it is placed in the list under the "[No Extension Present]". Not available for Linux.

File Extension Size (KB): the amount of space used by the files with that extension.

Volume Throughput

Vol Name: the name of the volume tested for throughput.

Vol Throughput (GB/hr): the number of gigabytes per hour that could be transferred from the volume to the computer running LANsurveyor.

Notes

User Note #1 through **User Note #10**

SNMP Data

System

Description: a description of the device.

SNMP ID: the object ID of the agent software.

Time Running: how long ago the agent started running.

Contact Person: the name of the contact person for the device.

Machine Name: the device name.

Location: the device's physical location.

Interfaces

Description: usually an abbreviated name and version of the interface.

Type: a description of what kind of network connection the interface is running. Examples of interface types might be Ethernet-csmacd (which is 10 Megabit Ethernet), PPP or Frame Relay.

Address: the network's physical address for the interface.

Max Speed (Kbps): the maximum speed reported for the interface.

Status: indicates whether the interface can actually transmit and receive network data. If the status is down, this usually indicates the interface has not been configured, or, for a Mac OS computer, indicates that network services such as AppleTalk or TCP/IP are not using the interface.

Bytes In: a counter of how many bytes of network data have been received by the interface.

Bytes Out: a counter of how many bytes of network data have been transmitted by the interface.

Errs In: a counter of how many errors occurred when network data was being received by the interface.

Errs Out: a counter of how many errors occurred when network data was being transmitted by the interface.

IP Counters

Forwarding?: has two values: Gateway, which indicates that this device routes IP data between one or more network interfaces, and Host, which indicates that this device is an IP end-node and does not route IP data.

Default TTL: the Time-To-Live value configured for IP, in seconds. This indicates how long IP data can be routed through an IP network before it is considered too old to route anymore.

Receives: how many IP data packets this device has received.

Input Header Errors: how many received IP packets discarded because of errors in the IP header, such as TTL exceeded or checksum errors.

Input Address Errors: how many received IP packets discarded because of errors in the IP addresses found in the packet.

Forwarded Datagrams: how many IP packets received that needed to be routed to other IP addresses, that is, packets that were not addressed to this IP device and needed to be forwarded to another IP device.

Input Unknown Protocols: how many received IP packets discarded because the device didn't support a particular protocol. This might be the case if a device receives an SNMP request but SNMP is not enabled.

Input Discards: how many received IP packets discarded because problems encountered when trying to process them. Reasons for these discards might be because of lack of input receive memory or because the device is too busy to process the data.

Input Delivers: how many received IP packets that were actually received without error.

Output Requests: how many IP packets that were attempted to be sent via IP.

Output Discards: how many IP packets that could not be sent because of problems such as lack of transmit memory.

Output No Routes: how many IP packets that could not be sent because no IP route could be found. This might indicate an unavailable remote network or a misconfigured local IP router.

Reassembly Timeout: the maximum number of seconds which received IP fragments of data are held waiting for the rest of their fragments.

Reassembly Requireds: how many IP packet fragments of data received which need to be reassembled when all fragments are received.

Reassembly OKs: how many IP packets received that were reassembled correctly after all fragments are received.

Reassembly Failures: how many IP packets received that could not be reassembled, usually because of timeouts waiting for all fragments.

Fragment OKs: how many IP packets that need to be fragmented before they can be sent by this device.

Fragment Failures: how many IP packets that need to be fragmented but could not be, usually because of protocol errors.

Fragments Created: how many IP packets sent that were generated as the result of fragmentation.

IP-ARP

Displays information contained in the IP Address Resolution Protocol (ARP) table. ARP is used to translate between IP addresses and physical (hardware) addresses. For example, in order to send IP data to an Ethernet device, the device's Ethernet address must be obtained. ARP is the protocol by which an IP node requests an Ethernet address for a given IP address. The IP-ARP table is useful for mapping IP address assignments to their corresponding Ethernet addresses. The IP-ARP table contains several columns:

If Index: a number assigned to a device's network interface. This interface is used to send IP data for the particular IP address contained in the third column.

Physical Address: the hardware address, usually a six-byte Ethernet address, corresponding to the IP address contained in the third column.

Network Address: the IP address that is assigned to the hardware (Ethernet) address contained in the second column.

Media Type: one of four values indicating the type of IP-to-Hardware address mapping. "Invalid" indicates that the particular mapping is invalid, usually because of a manual configuration option a user has set. "Dynamic" indicates that ARP has been used to generate a mapping, that is, the device has asked other devices on the network if they can supply a hardware (Ethernet) address for a particular IP address. "Static" indicates that a user has manually configured an address mapping for a particular Ethernet address. "Other" indicates some other type of unspecified mapping.

Printer Stats

Description: a description of the device, usually containing a model number and type of printer.

Printer Status: the current running status of the printer. This can include: Running, the printer is in operation with no error conditions; Warning, the printer has detected an error (low paper, low toner) but is still operational; Testing: the printer is not available because it is in a test state; or Down, the printer is not available for any use.

Impressions Count: the total number of pages printed by this printer. This value may be reset by the printer administrator but generally is the total number of pages printed since the printer was manufactured.

Toner/Ink Sources: the total number of toner or ink sources. If this is a monochrome printer, there will usually be only one source. If this is a color printer, there will likely be more than one source. For each source, a three line description will be present under the Toner/Ink Sources number: Description (A description of the toner or ink source, usually containing a model number if the source is a cartridge); Type (The type of the source, which can include Toner, Ink, Ribbon, Wax or many others); and Current / Capacity (The current Toner or Ink capacity and maximum capacity. Many printers cannot sense this data so the Current and/or Capacity values may read zero or unknown.)

Printer Toner Type: a description of the device, usually containing a model number and type of printer.

Printer Toner Cur/Cap: a description of the device, usually containing a model number and type of printer.

Paper Sources: the total number of sources of paper available to the printer. For each source, a three line description will be present under the Paper Sources number: Description (usually the name of the paper tray.); Type (includes such information as whether a tray is removable or non-removable, and the type of paper); and Current / Capacity (current paper source capacity and maximum capacity, which may be zero or unknown if the printer cannot report these data.)

Printer Paper Descr: a description of the device, usually containing a model number and type of printer.

Printer Paper Type: a description of the device, usually containing a model number and type of printer.

Printer Paper Cur/Cap: a description of the device, usually containing a model number and type of printer.

APC UPS Stats

Battery Health: indicates whether the UPS batteries need replacing.

Runtime (Minutes): the UPS battery run time remaining before battery exhaustion.

Low Battery Condition: the status of the UPS batteries. A Battery Low value indicates the UPS will be unable to sustain the current load, and its services will be lost if power is not restored.

% Capacity: the remaining battery capacity expressed in percent of full capacity.

% Load: the current UPS load expressed in percent of rated capacity.

Last Self-Test Status: the results of the last UPS diagnostics test performed.

Utility Power Status: the current state of the UPS.

Model Number: the UPS model name (e.g. 'APC Smart-UPS 600').

Manufacture Date: the date when the UPS was manufactured in mm/dd/yy format.

Battery Replaced Date: the date when the UPS system's batteries were last replaced in mm/dd/yy format.

Serial Number: an 8-character string identifying the serial number of the UPS internal microprocessor.

Active Directory Data

Computer Data

OS Type: the OS installed.

OS Version: the version of the OS installed.

OS Service Pack: the OS Service Pack installed.

When Created: the date and time the user account was initially created.

When Changed: the date and time the user account was last modified.

Last Logon: the last date and time a user logged onto the system.

Last Logoff: the last date and time a user logged off. A value of zero indicated 'unknown.'

Password Last Set: the date and time the password was last changed.

Bad Password Count: number of times the user attempted to log on using a bad password.

Bad Password Time: the last date and time the user attempted a login with an incorrect password.

Retrospect Client Data

The information in these fields depends on the EMC Retrospect client version installed. Some information is only available with the most recent version of the Retrospect client.

Client Name: the name assigned to the Retrospect client, which is usually the File Sharing name.

Status: the status of the Retrospect client, which can include Ready, Busy, Locked, or Off.

Client Version: the version of the Client.

Priority: the priority assigned to backup operations. A priority of 100% favors backup operations, whereas 20% favors user operations. This value is user-selectable in the Retrospect Client Control Panel.

Security: indicates whether this Retrospect client is password protected or not.

Machine: the type of machine on which the Client is running. For Mac OS nodes, this will be the model number. For Windows systems, this will be the processor type.

Processor: the type of processor running in the Client machine.

Memory (MB): the amount of memory installed on the Client machine.

Virtual Memory: for Mac OS machines, indicates whether virtual memory is running or not. This field is not applicable for Windows systems.

System: for Mac OS machines, the version of Mac OS. For Windows systems, the version of Windows.

Up Time: how long the Client machine has been running.

Idle Time: how long the Client machine has been idle. For Windows systems, this number always appears to be zero.

Echo Time (MS): the time delay, in milliseconds, recorded when communicating with this Client.

Backup Status: the time this Client was last backed up by Retrospect.

Application: for Mac OS machines, the front most application the user is running. This value is not available for Windows systems.

For more information about data returned by Retrospect Data queries, please refer to Retrospect User's Guide or visit www.emcinsignia.com.

SIP Client Data

SIP client data is available for SIP-based VoIP clients. The data in these fields is based on the Request for Comments (RFC) for SIP: Session Initiation Protocol.

SIP: the version of SIP implemented and the current status of the connection.

Via: the IP address of the LANsurveyor computer (which receives the response to the SIP request) and a branch parameter that identifies this request (transaction).

From: the display name ("LANsurveyor") and a SIP or SIPS URI that indicate the originator of the request (sip:LANsurveyor). There is also a tag parameter containing an identification string.

To: the display name and a SIP or SIPS URI that indicate the request destination (the map node).

Call-ID: a globally unique identifier for the current request.

CSeq: the Command Sequence contains a request ID and the name of the request LANsurveyor made to populate these data fields.

Contact: contains a SIP or SIPS URI that represents a direct route to the node, usually composed of a username at a fully qualified domain name (FQDN). While an FQDN is preferred, many end systems do not have registered domain names, so IP addresses are permitted. While the Via header field tells other elements where to send the response, the Contact header field tells other elements where to send future requests.

User-Agent: the type of SIP device (which may also include the specific software version).

Accept-Language: the preferred language for the transaction.

Accept: the type of message body acceptable in the response.

Allow: a list of commands supported by the node.

Allow-Events: a list of events supported by the node.

Supported: the list of SIP option tags supported.

Content-Length: a byte count of the message body.

Autodiscovery Data

Create reports based on the data collected by LANsurveyor during the mapping/autodiscovery process.

IP Address: the IP address of the node.

Domain Name: the name of the system as determined during the autodiscovery process.

Ethernet Address: the MAC address for the device as determined by SNMP queries.

Last Login: the name of the last user logged into the computer (obtained from Responder client discovery).

Login Last Updated: the date and time the last login information was updated.

Has Responder client?: is the Responder client installed? Yes or no.

Has Retrospect Client?: is there a Retrospect Client installed? Yes or no.

Has Timbuktu?: is Timbuktu installed? Yes or no.

Has SNMP?: was LANsurveyor able to get a response to an SNMP query? Yes or no.

Has NetBIOS?: is node responding to a NetBIOS query? Yes or no.

Appendix B - LANsurveyor Icons

LANsurveyor produces network maps using icons to represent network objects. This appendix shows you how to create your own icons for use in LANsurveyor.

Icon Files

LANsurveyor icons are stored as Windows Bitmap (.bmp) files in the NodeImages folder inside LANsurveyor's application folder. Files are named "#.bmp" where # represents either the SNMP ID byte or a LANsurveyor identification number. For example, APC uninterruptible power supplies use the icon in file 193.bmp since 193 is the SNMP ID for APC equipment. Numbers above 50000 are LANsurveyor identification numbers.

Icon images are loaded each time a map is built. Any images you replace, add, or edit are used the next time you create a map.

Icons should be 32-by-32 pixel images, and files stored in the NodeImages folder must named with numerals.

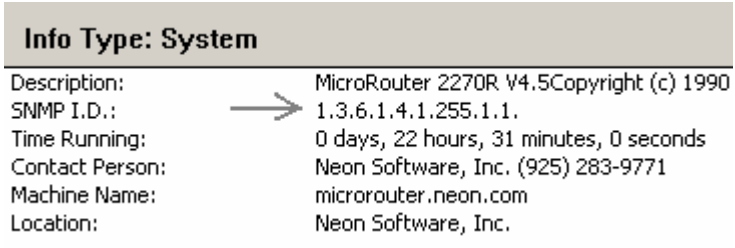
Change Icons

You can change the icon used for a device LANsurveyor knows about by simply replacing the .bmp file with one you create or just modifying the existing file.

Add Icons

LANsurveyor is extensible: you can add icons for any SNMP-based device not already supported by LANsurveyor. Simply create a .bmp file using the SNMP ID of the device.

To find the SNMP ID of your device, locate the device on your network and double-click on it to view the Get Info window. Then, view the System information under SNMP Data. The SNMP ID is the seventh number in the line of period-delimited numbers. If the string is 1.3.6.1.4.1.255.1.1, the actual SNMP ID is 255.



Save as Visio

Visio documents created by LANsurveyor can also use new icons you create.

LANsurveyor uses a Visio stencil file named "LANsurveyor.vss" in the LANsurveyor installation folder. Launch Visio then open the stencil. The icons in the stencil are named the same as the icons in the NodeImages folder.

Notes:

Appendix C - SNMP Checklist

LANsurveyor queries network equipment that supports SNMP (or "managed devices") to gather important connectivity information for network maps. SNMP data allows LANsurveyor to identify routers, switches, and connectivity between networking hardware and other systems.

If LANsurveyor has access to a device's SNMP MIB-II agent, the device will be listed under SNMP Nodes in the left-hand map navigation. LANsurveyor requires read-only access to SNMP for map drawing; read-write access is not required.

LANsurveyor identifies switches using the SNMP Bridge MIB (RFC 1493) and hubs using the SNMP Repeater MIB (RFC 2108). If LANsurveyor has access to these MIBs, LANsurveyor can map port connectivity. If your routers and switches are not displayed in the left-hand navigation, use this checklist to troubleshoot your SNMP access.

1. Does your device support SNMP?
SNMP-capable devices are sometimes called "smart" or "managed." You may need to check with the device's manufacturer to make sure.

2. Is SNMP enabled?
Some devices require you to specifically enable SNMP.

3. Are you using the correct SNMP community string?
Community strings, like passwords, are case sensitive. Make sure the correct community string is entered into the Create a New Network Map dialog.

4. Is the computer running LANsurveyor on the access control list for your device?

Many devices limit SNMP access to a specific IP address or address range. This is configured using the switch management interface, generally via a web browser.

5. Is the device too busy to respond to SNMP queries?
If a device is at or near 100% utilization, it may not have the resources available to respond to SNMP queries.

6. Is there something between you and the target device that's preventing access?
Some sites have firewalls around their routers that prevent access. LANsurveyor uses UDP port 161 for SNMP queries.

7. Is the timeout sufficiently long?
Increase the SNMP Query Timeout in LANsurveyor Options dialog box if queries are sent across particularly slow or busy links.

Notes:

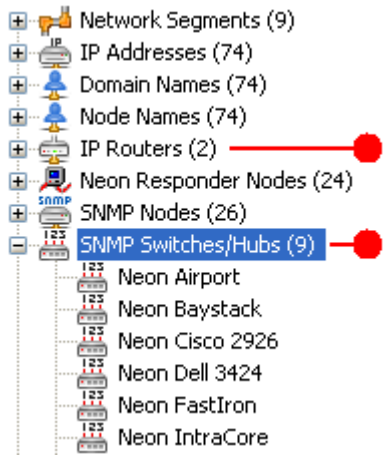
Appendix D - Large Diagram Tips

LANsurveyor can diagram both small and large networks. Customers have shared success stories about maps with more than 2000 routers and 4000 switches.

If you are mapping a large network, you may have some challenges visualizing your network completely on your computer. This Appendix provides tips for adjusting the LANsurveyor diagram to best match your requirements.

Full Discovery

Check to make sure your routers and switches were discovered and mapped. Use the left-hand navigation to see the list of routers and switches/hubs LANsurveyor discovered.



Map Levels

Use the Map Level 1 icon to redraw the map and display just your routers and network segments.

If LANsurveyor discovers over 300 routers, by default the map will display in Level 1. You can change the default in the LANsurveyor Preferences. You can also use the LANsurveyor preferences to display only selected nodes by type, for example just Responder clients.

Click the Level 2 icon to show network segments, routers, and switches.

Show/Hide Nodes

Display nodes connected to a router using with the Show icon. Click on a router (or managed switch) then click the Show icon to display the attached nodes.

If your map still has too many nodes, you can right-click on a router and select "Focus in New Window." This allows you to "drill down" on any specific router and see its

connections in a completely separate map window. You can still do Level 1, 2, and 3 displays of that new map, print it, and export it to Visio.

Map Overview

The Map Overview icon  opens a new window with a very small zoom percentage and a rectangular selection that allows you to move to different areas of the map quickly. Use the Map Overview in conjunction with the zoom percentage and the left-hand navigation to quickly move to specific routers or switches--just click on the node you want to center on the map.

Continuous Scan

LANsurveyor map generation creates very little network overhead. To get the most accurate maps possible, turn on Continuous Scan and let LANsurveyor make a few passes at creating the map during periods of normal network activity.

A lot of information is gathered from routers and switches. If there's no network activity, it will be impossible to determine the exact connectivity for your network.

Index

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- X -

- Z -