SolarWinds® LANsurveyor

Evaluation Guide

solarwinds

LANSURVEYOR

LANsurveyor Evaluation Guide, Version 10.4, 3.8.2011

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	**Contact Information**
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	http://www.solarwinds.com/support
User Forums	http://www.thwack.com/

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	**Specifying**
Bold	Window items, including buttons and fields.
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified

SolarWinds LANsurveyor Documentation Library

The following documents are included in the SolarWinds LANsurveyor documentation library:

Document	**Purpose**
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Online Help	Provides help for the main windows in the LANsurveyor user interface.
Evaluation Guide	Provides an introduction to LANsurveyor features and instructions for installing, configuring, and using LANsurveyor.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

About SolarWinds iii

Contacting SolarWinds iii

Conventions iii

SolarWinds LANsurveyor Documentation Library iv

Chapter 1

Introduction to LANsurveyor **1**

LANsurveyor Ease of Use 1

LANsurveyor Features 1

Chapter 2

Installing LANsurveyor **1**

Requirements 1

Installing LANsurveyor 2

Configuring LANsurveyor for Windows Vista/7/2008 6

Chapter 3

Using LANsurveyor **9**

Drawing Your Network Map 10

- *Troubleshooting Your Network Map* 13

Saving Your Network Map 14

Viewing and Navigating Your Network Map 14

- *Using the Browser Pane to Navigate the Map* 14
- *Using Map Levels to Navigate the Map* 15
- *Using Overview to Navigate the Map* 16

Creating a Managed Switch/Hub Report 17

- *Drawing a Map with Managed Switches and Hubs* 17
- *Creating the Managed Switches and Hubs Report* 18

Switching Between Report and Map Views 19

Monitoring Your Network Services 19

- *Creating Alerts* 19
- *Monitoring Services using TCP Port Monitoring* 21

Detecting Intrusion with Continuous Scan 24
Investigating LANsurveyor Further 25
    LANsurveyor Responder Clients 25

Chapter 1

Introduction to LANsurveyor

SolarWinds LANsurveyor automatically discovers your network and produces a comprehensive network diagram that can be easily exported to Microsoft Office® Visio®.

LANsurveyor Ease of Use

Discover how simple network mapping can be. Using a unique multi-level discovery technique, LANsurveyor automatically discovers your network and produces comprehensive, easy-to-view network maps that integrate OSI Layer 2 and Layer 3 topology data. Then, with just two mouse clicks, this data can be exported into Microsoft Office® Visio® and easily shared with your colleagues.

LANsurveyor Features

The LANsurveyor solution is characterized by the following distinguishing features:

- Automatically discovers and diagrams network topology
- Supports generation of network maps in Microsoft Office Visio
- Automatically detects new devices and changes to network topology
- Simplifies inventory management for hardware and software assets
- Addresses reporting needs for PCI compliance and other regulatory requirements

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

Note: LANsurveyor Responder clients are beyond the scope of this guide.

Chapter 2

Installing LANsurveyor

LANsurveyor provides a simple, wizard-driven installation.

Requirements

To use LANsurveyor, you must have the following:

- A Pentium-class computer with 256MB memory
- Windows 2003, Vista (professional, workstation, or server editions), 7, 2008, or 2008 R2
- A connection to an IP-based network

Additionally, some LANsurveyor features require the following:

Visio

- 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 2005 or Microsoft SQL Server 2005 Express to store SNMP configuration and Responder client information in LANsurveyor's Repository.

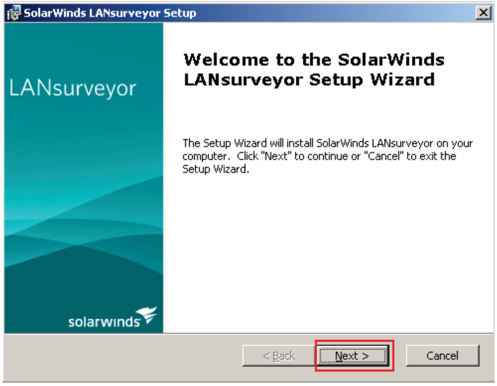
  Note: Microsoft SQL Server 2005 or Microsoft SQL Server 2005 Express is not required for completing this guide, since it does not describe using LANsurveyor Responder clients.

Installing LANsurveyor

This section describes how to install LANsurveyor.

To install LANsurveyor:

1. Navigate to the location of your downloaded `LANsurveyor-v<`*version*`>-Eval.zip` file, where *version* is the version number of your LANsurveyor software. For example `LANsurveyor-v10.4-Eval.zip` is the zip package for the LANsurveyor evaluation version 10.4.
2. Extract the evaluation package to an appropriate location.
3. Double-click the `LANsurveyor<`*version*`>Demo.exe` installer file to run it, where *version* is the version number of your LANsurveyor software. For example `LANsurveyor104Demo.exe` is the installer for LANsurveyor evaluation version 10.4.
4. ***If you are prompted “Do you want to run this file?”,*** click **Run**.
5. Review the Welcome text in the SolarWinds LANsurveyor Setup Wizard, and then click **Next**.

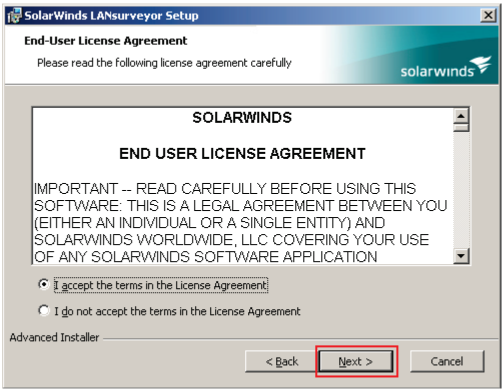


SolarWinds LANsurveyor Setup

Welcome to the SolarWinds LANsurveyor Setup Wizard

The Setup Wizard will install SolarWinds LANsurveyor on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

6. Accept the terms of the license agreement, and then click **Next**.



SolarWinds LANsurveyor Setup

End-User License Agreement

Please read the following license agreement carefully

SOLARWINDS

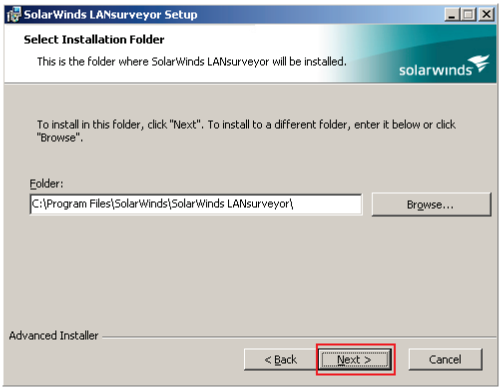
END USER LICENSE AGREEMENT

IMPORTANT -- READ CAREFULLY BEFORE USING THIS SOFTWARE: THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND SOLARWINDS WORLDWIDE, LLC COVERING YOUR USE OF ANY SOLARWINDS SOFTWARE APPLICATION

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

7. Use the default installation folder, or select a different folder, and then click **Next**.



SolarWinds LANsurveyor Setup

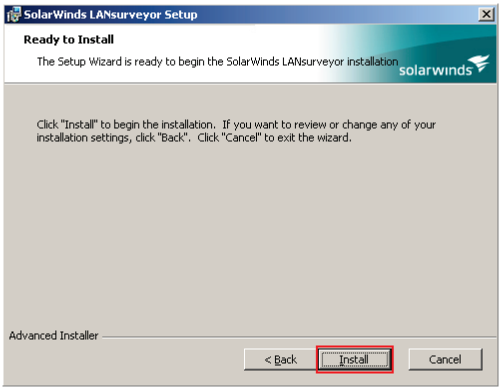
Select Installation Folder

This is the folder where SolarWinds LANsurveyor will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\SolarWinds\SolarWinds LANsurveyor\

8. Confirm the installation, and then click **Install**.



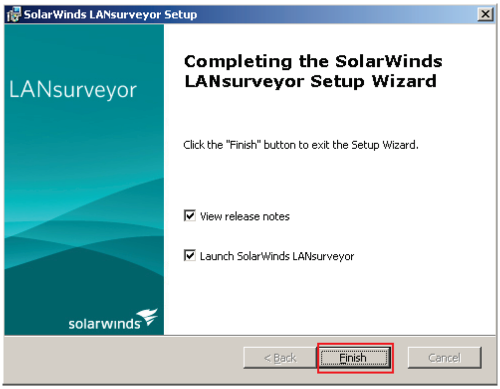
SolarWinds LANsurveyor Setup

Ready to Install

The Setup Wizard is ready to begin the SolarWinds LANsurveyor installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

9. Click **Finish** to exit the Setup Wizard.



Completing the SolarWinds LANsurveyor Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

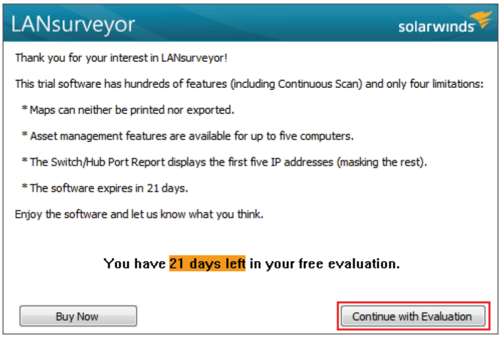
☑ View release notes

☑ Launch SolarWinds LANsurveyor

Note: if you do not choose the option to **Launch SolarWinds LANsurveyor** now, you can launch LANsurveyor at any time by clicking **Start>All Programs>SolarWinds LANsurveyor>LANsurveyor**.

10. Review the *Release Notes*.

11. Review the limitations of the evaluation software and then click **Continue with Evaluation** to continue the evaluation.



Thank you for your interest in LANsurveyor!

This trial software has hundreds of features (including Continuous Scan) and only four limitations:

* Maps can neither be printed nor exported.

* Asset management features are available for up to five computers.

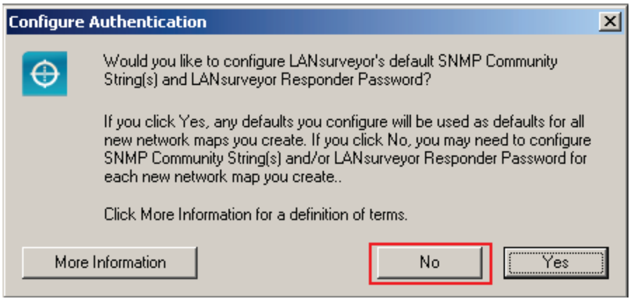
* The Switch/Hub Port Report displays the first five IP addresses (masking the rest).

* The software expires in 21 days.

Enjoy the software and let us know what you think.

You have 21 days left in your free evaluation.

12. The Configure Authentication dialog may be displayed. This dialog allows you to configure the default SNMP Community String(s) and LANsurveyor Responder password. We will do this later, so click **No** to close this dialog.

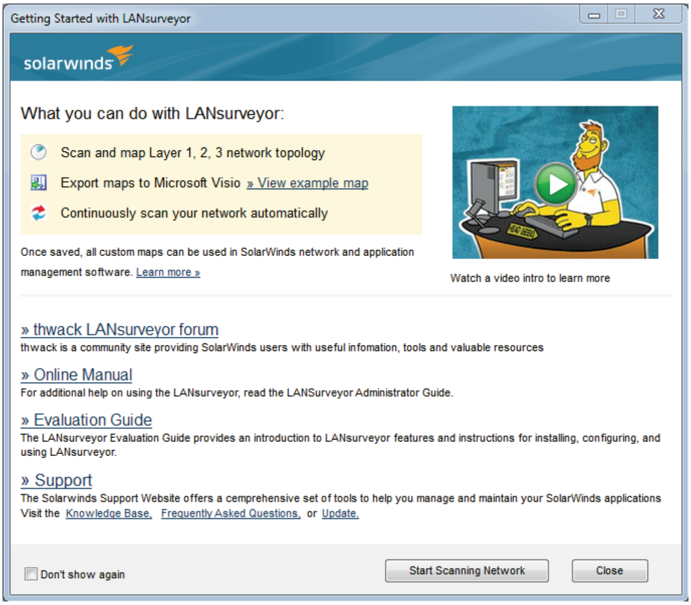


Would you like to configure LANsurveyor's default SNMP Community String(s) and LANsurveyor Responder Password?

If you click Yes, any defaults you configure will be used as defaults for all new network maps you create. If you click No, you may need to configure SNMP Community String(s) and/or LANsurveyor Responder Password for each new network map you create..

Click More Information for a definition of terms.

13. The Getting Started with LANsurveyor dialog is displayed.


Getting Started with LANsurveyor
solarwinds
Watch a video intro to learn more
☐ Don't show again
Start Scanning Network
Close

What you can do with LANsurveyor:

- Scan and map Layer 1, 2, 3 network topology
- Export maps to Microsoft Visio » View example map
- Continuously scan your network automatically

Once saved, all custom maps can be used in SolarWinds network and application management software. Learn more »

» thwack LANsurveyor forum
thwack is a community site providing SolarWinds users with useful infomation, tools and valuable resources

» Online Manual
For additional help on using the LANsurveyor, read the LANSurveyor Administrator Guide.

» Evaluation Guide
The LANsurveyor Evaluation Guide provides an introduction to LANsurveyor features and instructions for installing, configuring, and using LANsurveyor.

» Support
The Solarwinds Support Website offers a comprehensive set of tools to help you manage and maintain your SolarWinds applications
Visit the Knowledge Base, Frequently Asked Questions, or Update.

From this dialog, you have several options for beginning to learn about LANsurveyor (which you can investigate as you continue using LANsurveyor):

- **>> View example map** – view a sample map using Visio (requires a supported version of Visio).
- **Watch a video intro** – watch a video introduction to using LANsurveyor.
- **Learn more >>** – read about creating maps for Orion with LANsurveyor.

- **>> thwack LANsurveyor forum** – browse questions and answers from LANsurveyor users.
- **>> Online Manual** – display a page where you can click the link to view the *LANsurveyor Online Manual*.
- **>> Evaluation Guide** – display a page where you can click the link to view the *LANsurveyor Evaluation Guide*.
- **>> Support** – view the SolarWinds Customer Support portal, where you can find support resources.

Note: This dialog is displayed for your reference each time you run LANsurveyor unless you check the option **Don't show again** at the bottom of the dialog.

14. Click **Start Scanning Network**. The Create a New Network Map dialog is displayed.

    Leave this dialog open. You will be filling out the information requested here in Chapter 2, "Using LANsurveyor".

If you are using Windows Vista, Windows 7, or Windows 2008, you must *first* configure LANsurveyor, as described in the following section "Configuring LANsurveyor for Windows Vista/7/2008", before creating the new network map.

If you are using Windows 2003, you should skip the next section and go directly to Chapter 2, "Using LANsurveyor" on page 9.

Configuring LANsurveyor for Windows Vista/7/2008

The Windows Vista/7/2008 firewall blocks ICMP ping replies by default, preventing LANsurveyor from performing network discovery using **ping**. To correct the situation, either administratively turn off the Vista firewall or add a rule permitting ping replies through the firewall, as shown in the following procedure.

To add a rule enabling ICMP ping for LANsurveyor on Windows Vista/7/2008:

1. Login to Windows as an Administrator.
2. Click **Start>Control Panel>Administrative Tools>Windows Firewall with Advanced Security**.

   Note: This option is not available if you are not an Administrator.
3. Click **Inbound Rules** in the left pane.
4. Click **New Rule** in the right pane.
5. Select **Custom**, and then click **Next**.
6. Select **All programs**, and then click **Next**.

7. Select **ICMPv4** as the Protocol type, and then click **Next**.
8. Confirm that **Any IP address** is selected for both **Which local IP addresses does this rule match?** and **Which remote IP addresses does this rule match?**, and then click **Next**.
9. Select **Allow the connection** on the Action page, and then click **Next**.
10. Confirm that all options are checked on the Profile page, and then click **Next**.
11. Provide an appropriate **Name** for your new rule, and then click **Finish**.
12. Repeat the preceding steps, clicking **Outbound Rules** instead of **Inbound Rules**.

Chapter 3

Using LANsurveyor

This chapter provides a step-by-step guide for configuring and using LANsurveyor to map and manage your entire network.

Using LANsurveyor, you will learn how to:

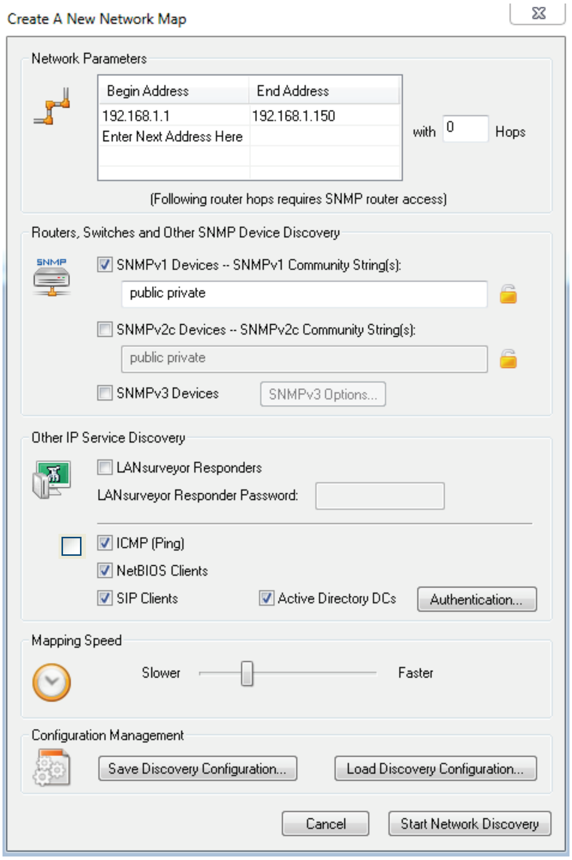
- Draw a map showing the logical connectivity of your network and navigate around the map
- Create a report that includes all your managed switches and hubs
- Be alerted when nodes become unresponsive (or become responsive again) via a variety of notification methods
- Monitor your network applications
- Scan your network for intruders using one or more maps as the baseline and automatically disable network access for rogue nodes

If you are continuing with the guide from the previous chapter, your LANsurveyor is already running and is displaying the Create A New Network Map dialog.

If your LANsurveyor is not running, click **Start>All Programs>SolarWinds LANsurveyor>LANsurveyor** to launch LANsurveyor.

   - Click **Continue with Evaluation** and click **Close** to close the Getting Started dialog.

- Then click **File>New** to display the Create A New Network Map dialog.



Create A New Network Map

Network Parameters

Begin Address	End Address
192.168.1.1	192.168.1.150
Enter Next Address Here	

with 0 Hops

(Following router hops requires SNMP router access)

Routers, Switches and Other SNMP Device Discovery

☑ SNMPv1 Devices -- SNMPv1 Community String(s): public private

☐ SNMPv2c Devices -- SNMPv2c Community String(s): public private

☐ SNMPv3 Devices

Other IP Service Discovery

☐ LANsurveyor Responders

LANsurveyor Responder Password:

☑ ICMP (Ping)

☑ NetBIOS Clients

☑ SIP Clients

☑ Active Directory DCs

Mapping Speed

Configuration Management

Drawing Your Network Map

LANsurveyor's map allows you to see a visual representation of your network setup including the devices attached to your network.

To create your first network map:

1. 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. Use this IP address range or enter another range. LANsurveyor can map and manage both local and remote networks.

   Note: LANsurveyor is capable of discovering and mapping multiple VLANs on Layer 2. For example, to map a switch connecting multiple, non-consecutive VLANs (for example, 10.110.1.0, 10.111.1.0, 10.112, 1.0), simply enter your VLAN ranges as the IP address ranges to search.

2. Enter the number of Hops.

   LANsurveyor can also show connectivity between different networks (that is, 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.

3. Select the SNMP version and enter one or more SNMP community strings (or passwords) for your devices.

   Be sure to separate SNMP community strings by spaces or commas. Use the lock icon 🔓 to hide the strings. If you do not know the community string, try "public", a common default access string.

4. This guide does not discuss LANsurveyor Responders, so do *not* check **LANsurveyor Responders.**

   > For the latest information about LANsurveyor Responders, refer to the Online Manual at: http://www.solarwinds.com/support/lansurveyor/docs/LS10_online_manual/index.html.

5. Check **ICMP**.

   Some devices are not supported by Responder clients and do not support SNMP. Use ICMP to increase your chances of including these nodes on your map.

6. Check **NetBIOS**.

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

7. Check **SIP Clients**.

   Use SIP Clients to discover SIP-based Voice-over-IP (VoIP) devices, including telephones, video conferencing systems, and other SIP devices.

8. Check **Active Directory DCs**.

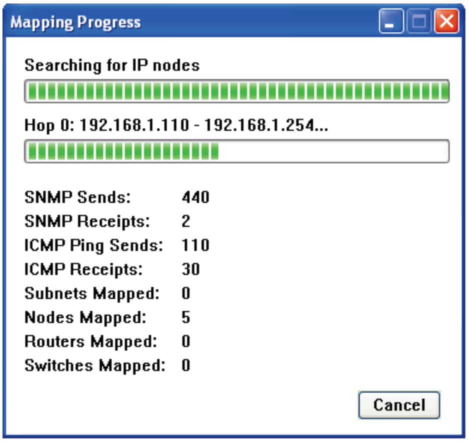
   Use the Active Directory DCs option to discover the domain controllers on your network. By default, LANsurveyor uses the credentials of the person running LANsurveyor. If you want to use different credentials, click **Authentication**, then click **Use these domain credentials**, **and** then click **Add...**. In the dialog that is displayed, enter the credentials you would like to use.

9. Adjust the **Mapping Speed** slider.

   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.

10. Click **Start Network Discovery**.

    LANsurveyor displays a progress dialog as it maps your network.



Searching for IP nodes

Hop 0: 192.168.1.110 - 192.168.1.254...

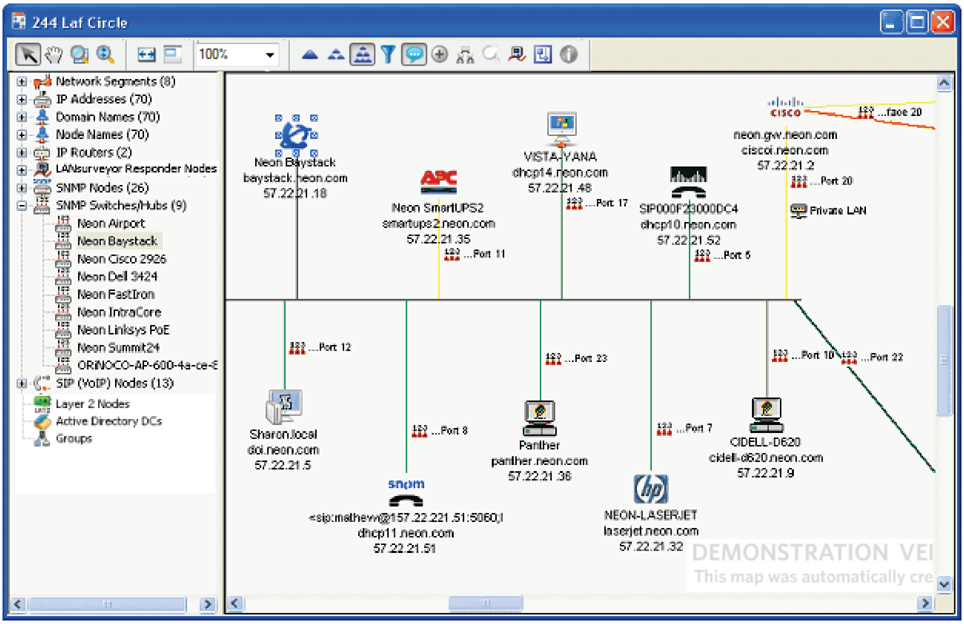
SNMP Sends:	440
SNMP Receipts:	2
ICMP Ping Sends:	110
ICMP Receipts:	30
Subnets Mapped:	0
Nodes Mapped:	5
Routers Mapped:	0
Switches Mapped:	0

11. LANsurveyor performs the following to map your network:

    - Network requests are sent to discover nodes
    - Items that respond to more than one type of query (for example 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.

12. LANsurveyor displays the map of your network:

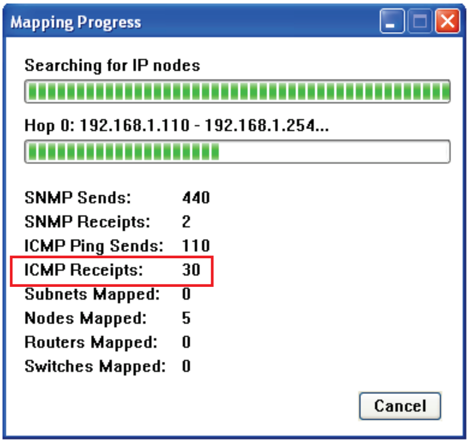


Troubleshooting Your Network Map

If you are having trouble creating your network map, and you are using Windows Vista, Windows 7, or Windows 2008, perform the following to troubleshoot your network map:

1. Test the new rules you created permitting ping replies through the firewall in the section “Configuring LANsurveyor for Windows Vista/7/2008” on page 6, by opening LANsurveyor and then creating a new map with only **ICMP (Ping)** checked in the Other IP Service Discovery area of the Create a New Network Map window.
2. The Mapping Progress window will show ICMP receipts, and the resulting map should show one or more workstations with generic IP icons.

3. Adjust the new rules if needed until the ICMP receipts are shown in the Mapping Progress window.



Searching for IP nodes

Hop 0: 192.168.1.110 - 192.168.1.254...

SNMP Sends: 440
SNMP Receipts: 2
ICMP Ping Sends: 110
ICMP Receipts: 30
Subnets Mapped: 0
Nodes Mapped: 5
Routers Mapped: 0
Switches Mapped: 0

Saving Your Network Map

You can save your network map by clicking **File>Save As**. A dialog is displayed where you can specify the name and location of the file.

After you have saved your map file, you can open it at any time by clicking **File>Open**. As an alternative, you can click the numbered map file name that is displayed near the bottom of the **File** menu.

Viewing and Navigating Your Network Map

There are several ways to view and navigate around your map:

- Browser Pane
- Map Levels
- Map Overview

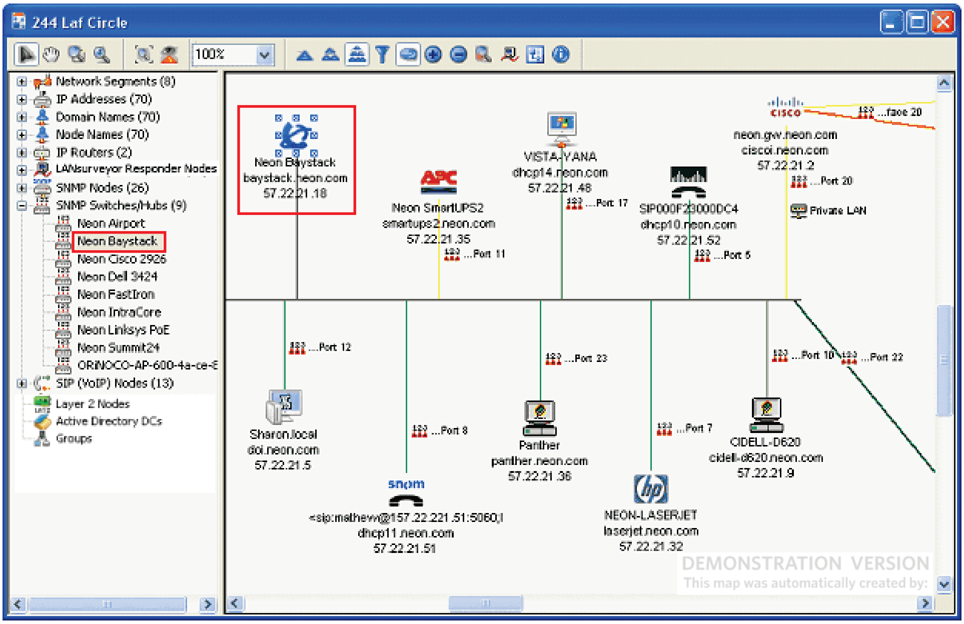
Using the Browser Pane to Navigate the Map

You can quickly and easily find any map item using the browser (left) pane. All map items are represented in one or more of twelve different categories.

To view and navigate around your map using the browser pane:

1. Click the expand icon ⊞ to expand a category in the browser (left) pane.

2. Click on any item in the category to select that item and scroll the map to display the item in the map window.



Using Map Levels to Navigate the Map

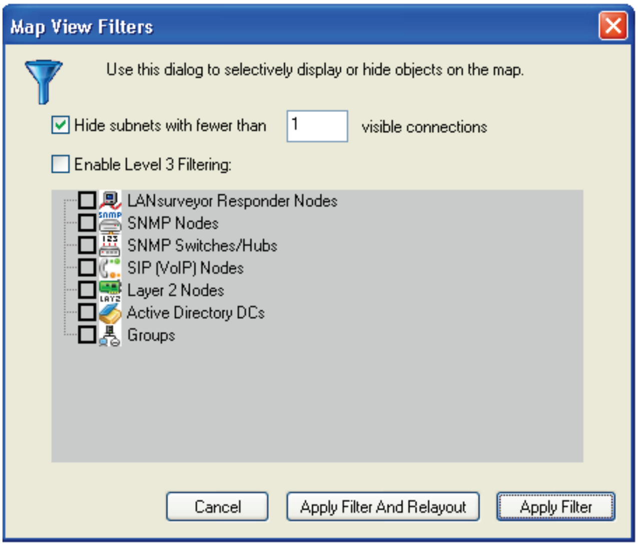
Map levels make your maps easier to view. Your map can have thousands of nodes, so LANsurveyor automatically groups map objects into three levels:

- 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

To view and navigate around your map using map levels and map view filters:

1. Click the Level 1 icon ▲ in the toolbar to view just your routers and network segments.
2. Click the Level 2 icon ▲ in the toolbar to view Level 1 plus your switches.
3. Click the Level 3 icon ▲ in the toolbar to display all map nodes.

4. Click the Map View Filters icon in the toolbar to selectively display or hide objects on the map:



Map View Filters

Use this dialog to selectively display or hide objects on the map.

☑ Hide subnets with fewer than 1 visible connections

☐ Enable Level 3 Filtering:

- ☐ LANsurveyor Responder Nodes
- ☐ SNMP Nodes
- ☐ SNMP Switches/Hubs
- ☐ SIP (VoIP) Nodes
- ☐ Layer 2 Nodes
- ☐ Active Directory DCs
- ☐ Groups

a. Check **Hide subnets with fewer than *n* visible connections** to hide the subnets and enter the number of visible connections desired.

b. Check **Enable Level 3 Filtering** and then check the boxes for the categories of objects to display.

For example, to display just nodes that responded to SNMP queries, check **SNMP Nodes**.

c. Then click **Apply Filter** to display / hide the specified items.

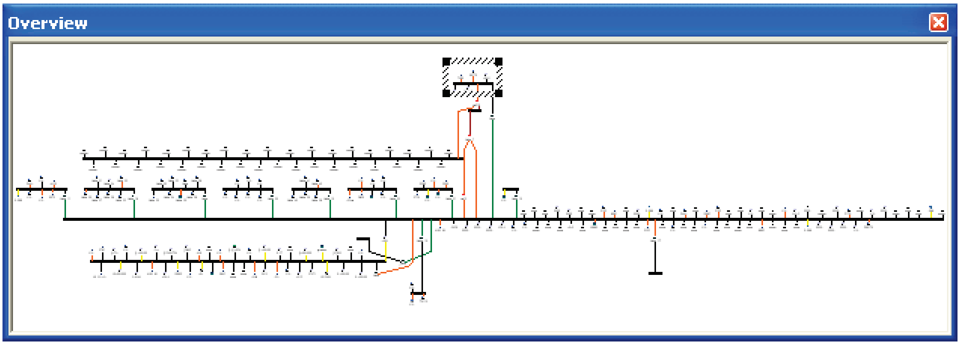
d. ***If you want to remove the filter,*** click the Map View Filters icon in the toolbar, uncheck the checkbox for **Enable Level 3 Filtering**, and click **Apply Filter** to display / hide the specified items.

Using Overview to Navigate the Map

The map Overview makes it easy to move around large maps.

To view and navigate around your map using the map Overview:

1. Click the Overview icon in the toolbar to display the map Overview.



2. Scroll the map window by dragging the rectangle displayed over the area you would like to view in the map window.
3. When you are finished using the Overview, click its close button .

Creating a Managed Switch/Hub Report

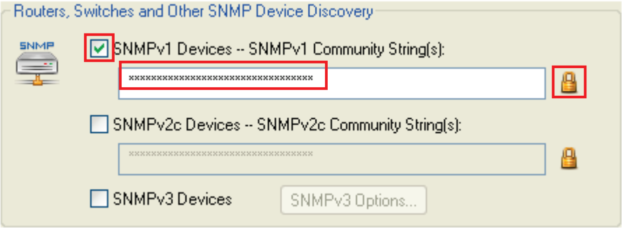
LANsurveyor makes it easy to identify where nodes on the map are physically connected if they are connected to a managed switch or hub. To use the managed switch/hub features in LANsurveyor, your hardware must support SNMP and you must have the correct SNMP community string (or password).

Drawing a Map with Managed Switches and Hubs

This section describes creating a new map that includes all your managed switches and hubs.

To draw a map with managed switches and hubs:

1. Click **File>New** to create a new map. The Create a New Network Map dialog is displayed.
2. Make sure to enable the appropriate version(s) of SNMP and enter the correct community string(s) for your switches and hubs when you create the map. Use the lock icon to hide or show the strings.



Routers, Switches and Other SNMP Device Discovery

☑ SNMPv1 Devices -- SNMPv1 Community String(s):

☐ SNMPv2c Devices -- SNMPv2c Community String(s):

☐ SNMPv3 Devices

3. Then click **Start Network Discovery** to create the new map.
4. Click **File>Save As** to save the new map to a filename of your choice.

Creating the Managed Switches and Hubs Report

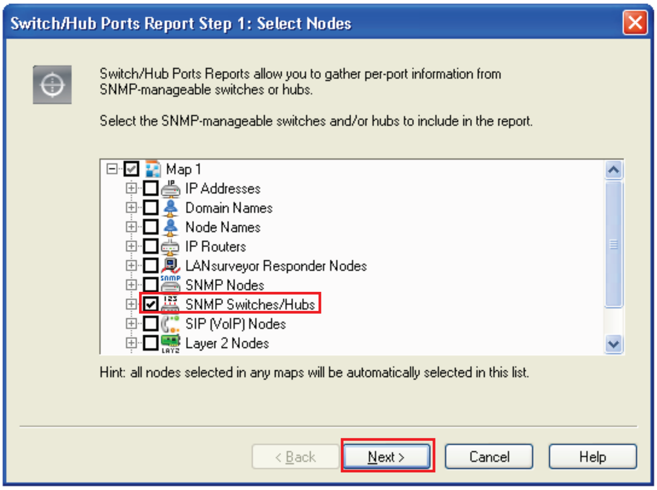
Create the report that includes all your managed switches and hubs.

To create the report with managed switches and hubs:

1. Start the Switch/Hub Ports Report Wizard by clicking the icon in the toolbar or selecting **Report>New>Switch/Hub Ports**.

   The Switch/Hub Ports Wizard is displayed.

2. Click ⊞ to expand the map. Any nodes already selected on the map will be checked. To select all the managed Switches and Hubs, check **SNMP Switches/Hubs** and then click **Next**.



Switch/Hub Ports Reports allow you to gather per-port information from SNMP-manageable switches or hubs.

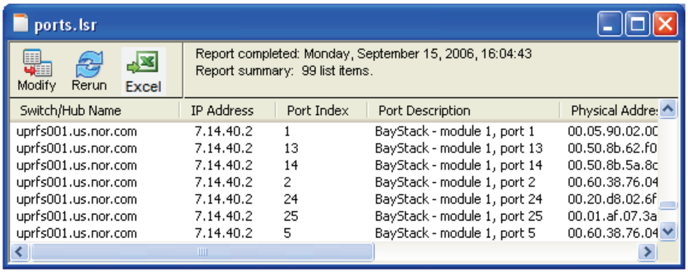
Select the SNMP-manageable switches and/or hubs to include in the report.

- ☑ Map 1
  - ☐ IP Addresses
  - ☐ Domain Names
  - ☐ Node Names
  - ☐ IP Routers
  - ☐ LANsurveyor Responder Nodes
  - ☐ SNMP Nodes
  - ☑ SNMP Switches/Hubs
  - ☐ SIP (VoIP) Nodes
  - ☐ Layer 2 Nodes

Hint: all nodes selected in any maps will be automatically selected in this list.

3. Schedule the time to run the report or check **now** and then click **Finish**.

   The report is generated.



Report completed: Monday, September 15, 2006, 16:04:43
Report summary: 99 list items.

Switch/Hub Name	IP Address	Port Index	Port Description	Physical Addre
uprfs001.us.nor.com	7.14.40.2	1	BayStack - module 1, port 1	00.05.90.02.0C
uprfs001.us.nor.com	7.14.40.2	13	BayStack - module 1, port 13	00.50.8b.62.f0
uprfs001.us.nor.com	7.14.40.2	14	BayStack - module 1, port 14	00.50.8b.5a.8c
uprfs001.us.nor.com	7.14.40.2	2	BayStack - module 1, port 2	00.60.38.76.04
uprfs001.us.nor.com	7.14.40.2	24	BayStack - module 1, port 24	00.20.d8.02.6f
uprfs001.us.nor.com	7.14.40.2	25	BayStack - module 1, port 25	00.01.af.07.3a
uprfs001.us.nor.com	7.14.40.2	5	BayStack - module 1, port 5	00.60.38.76.04

4. Click on any column to sort by that column.

   For a description of the column data, press F1 for help in LANsurveyor.

5. Click on any column to sort by that column.
6. Click **File>Save** to save the report, or click the **View Report with Excel** icon Excel to automatically open the report in Excel.

Switching Between Report and Map Views

You can conveniently switch between the report and map views (and vice-versa) at any time using the **Window** menu.

When you are finished viewing the report and want to redisplay your map, click **Window><*your_map*>**, where *your_map* is the name of the map you created (defaults to **Map 1**).

Similarly to switch between the map and report view, click **Window><*your_report*>**, where *your_report* is the name of the map you created (defaults to **Report 1**).

Monitoring Your Network Services

You can use LANsurveyor’s alerts along with its TCP Port Monitor to be notified of potential problems and to test the availability of services on your network.

Creating 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.

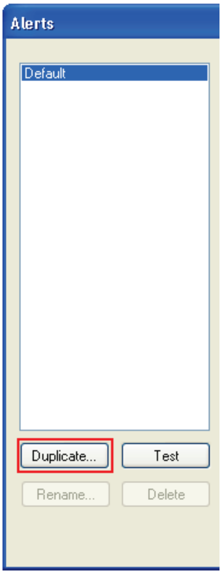
To set up alerts:

1. Use the map you created in the section “Drawing Your Network Map” on page 10, or create a new map that includes the computers and/or devices you would like to monitor.
2. Set up alerts to allow you to receive immediate notification of network problems.
   a. Click **Edit>Alerts** to view your configured alerts.

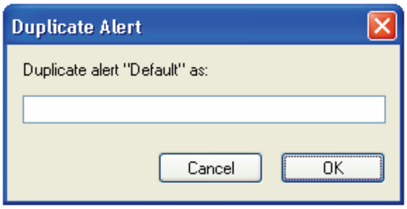
      Initially, only the Default alert is displayed.

   b. Select **Default** and then click **Duplicate**.

You can use **Duplicate** at any time to copy an existing alert and create a new one.

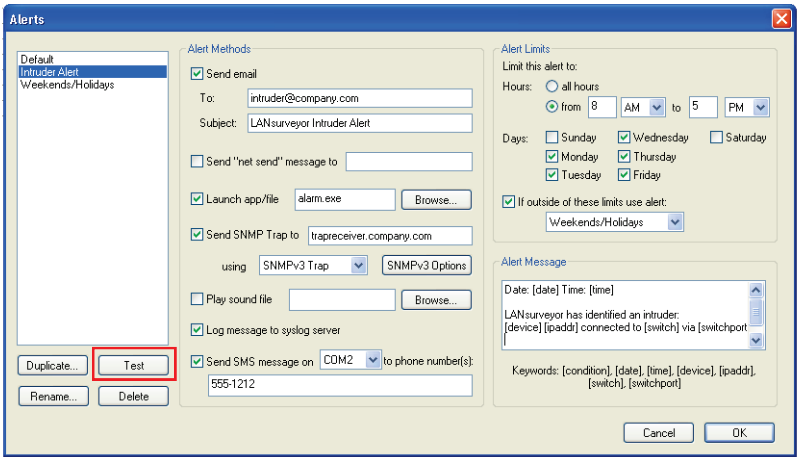


c. A dialog is displayed where you can specify a name for the duplicated alert.



Then click **OK**.

d. Use a name for the alert that has some meaning to you and your organization such as Critical, Mail Server, or www. You may have as many different named alerts as you would like.



Default
Intruder Alert
Weekends/Holidays

Alert Methods
☑ Send email
To: intruder@company.com
Subject: LANsurveyor Intruder Alert
☐ Send "net send" message to
☑ Launch app/file alarm.exe
☑ Send SNMP Trap to trapreceiver.company.com
using SNMPv3 Trap
☐ Play sound file
☑ Log message to syslog server
☑ Send SMS message on COM2 to phone number(s):
555-1212

Alert Limits
Limit this alert to:
Hours: ○ all hours
● from 8 AM to 5 PM
Days: ☐ Sunday ☑ Wednesday ☐ Saturday
☑ Monday ☑ Thursday
☑ Tuesday ☑ Friday
☑ If outside of these limits use alert:
Weekends/Holidays

Alert Message
Date: [date] Time: [time]

LANsurveyor has identified an intruder:
[device] [ipaddr] connected to [switch] via [switchport

Keywords: [condition], [date], [time], [device], [ipaddr], [switch], [switchport]

e. After you create your new alert, change the settings to be appropriate for your organization. Modify the options by clicking directly into the field or clicking the appropriate check box.

f. Click **Test** to make sure your alert settings work.

g. Click **OK** when you have finished setting alerts.

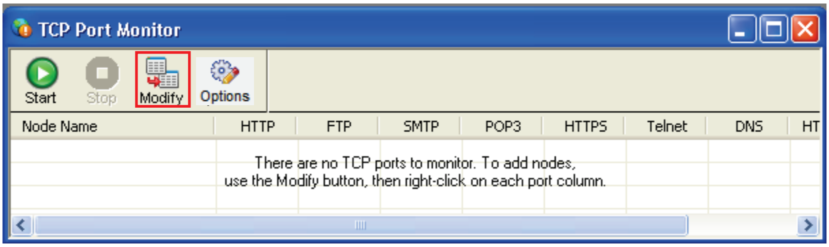
You can always add more alerts later.

Monitoring Services using TCP Port Monitoring

LANsurveyor allows you to monitor availability of services on your network through TCP Port Monitoring.

To set up TCP Port Monitoring:

1. Open the TCP Port Monitor window, select nodes to monitor, and begin monitoring.
   a. Click **Window>TCP Port Monitor** to view the TCP Port Monitoring window.



There are no TCP ports to monitor. To add nodes, use the Modify button, then right-click on each port column.

b. Click **Modify** to select the nodes to monitor in the wizard.

c. Click the expand icon ⊞ to expand the Map and then click the expand icon ⊞ to expand the Node Names category.

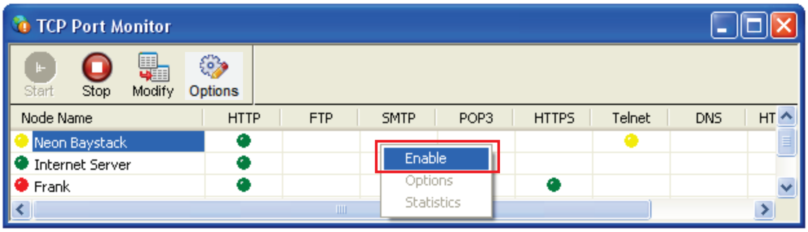
d. Check the nodes to monitor, and then click **Finish**.

You can monitor up to 20 nodes with the basic version of LANsurveyor.

e. Click ▶ Start to begin monitoring.

f. Enable monitoring for each of the desired nodes/ports by right-clicking in the appropriate cell of the node in that row and the port in that column to display the context menu. Then click **Enable**.

For example, to monitor Neon Baystack on SMTP, right-click in the cell for the Neon Baystack row in the SMTP column, and then click **Enable**.



Note: the node status will not be indicated in color until enough time passes for the nodes to be polled.

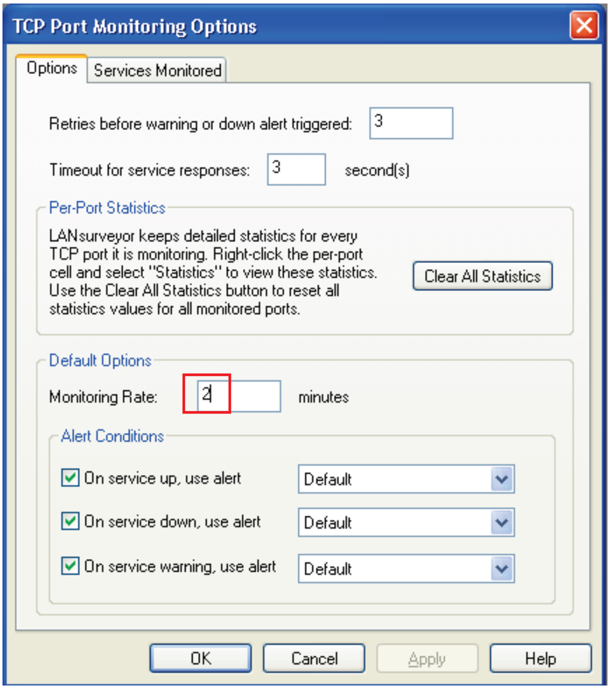
While waiting for the status of the TCP Port, LANsurveyor displays an empty circle ○. If the port responds and the ASCII text received from the port matches the expected result for the TCP server in question, a green dot ● is displayed. If there is no response, a red dot ● is displayed. A warning dot ● 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.

- **g.** To view the exact ASCII text received by the TCP server being monitored, right-click the warning dot and then click **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.

2. Select the TCP Port Monitoring Options.

- **a.** Click Options (or alternatively, click **Monitor>TCP Port>Options**) to view the TCP Port Monitoring Options window.
- **b.** 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.

  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.
- **c.** Set the **Monitoring Rate** to 2 minutes for more frequent monitoring.



Retries before warning or down alert triggered: 3

Timeout for service responses: 3 second(s)

Per-Port Statistics

LANsurveyor keeps detailed statistics for every TCP port it is monitoring. Right-click the per-port cell and select "Statistics" to view these statistics. Use the Clear All Statistics button to reset all statistics values for all monitored ports.

Default Options

Monitoring Rate: 2 minutes

Alert Conditions

☑ On service up, use alert: Default

☑ On service down, use alert: Default

☑ On service warning, use alert: Default

- **d.** Specify the alert actions to take when service up, down, or warning conditions are triggered.

  If you did not create additional alerts in the section “Creating Alerts” on page 19, accept the **Default** alert.

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.

e. Click **OK** to save the TCP port monitoring options.

3. When you are finished monitoring TCP ports, click Stop.

   You can resume TCP port monitoring at any time by clicking Start.

Detecting Intrusion with Continuous Scan

Continuous Scan was designed to help organizations meet security requirements by providing continuously updated network documentation, logging nodes on and off the network, and maintaining an up-to-date network diagram.

The Continuous Scan option is an intrusion detection system that uses one or more LANsurveyor maps as the base line network environment. Once you have identified the systems on the baseline map as acceptable, turn on Continuous Scan.

When Continuous Scan is active, LANsurveyor scans the network and looks for any new nodes. Since they weren't already on the map, the new nodes may not belong on the network. Therefore, they are listed on the Threat List.

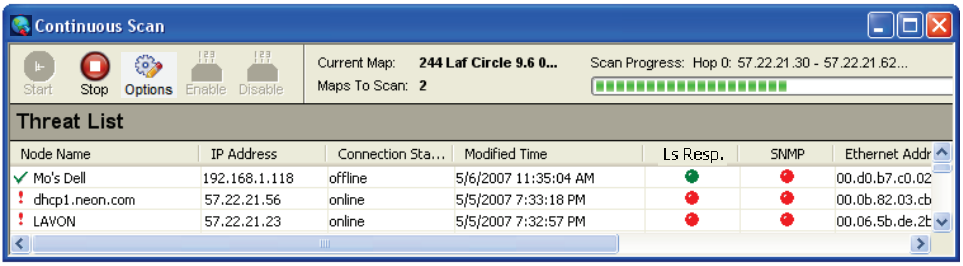
To set up Continuous Scan:

1. Use the map you created in the section “Drawing Your Network Map” on page 10 or create a new map that includes the computers and/or devices you would like to monitor using continuous scan.

   Verify that all the systems connected to the network should be connected. Since this map will be your new baseline, you don’t want to include any intruder systems that should not be connected.

2. Click **Window>Continuous Scan** to display the Continuous Scan window.

3. Click Start to begin scanning your network for intruders and other new nodes.



Current Map: **244 Laf Circle 9.6 0...**
Maps To Scan: 2
Scan Progress: Hop 0: 57.22.21.30 - 57.22.21.62...

Threat List

Node Name	IP Address	Connection Sta...	Modified Time	Ls Resp.	SNMP	Ethernet Addr
✓ Mo's Dell	192.168.1.118	offline	5/6/2007 11:35:04 AM	🟢	🔴	00.d0.b7.c0.02
! dhcp1.neon.com	57.22.21.56	online	5/5/2007 7:33:18 PM	🔴	🔴	00.0b.82.03.cb
! LAVON	57.22.21.23	online	5/5/2007 7:32:57 PM	🔴	🔴	00.06.5b.de.2b

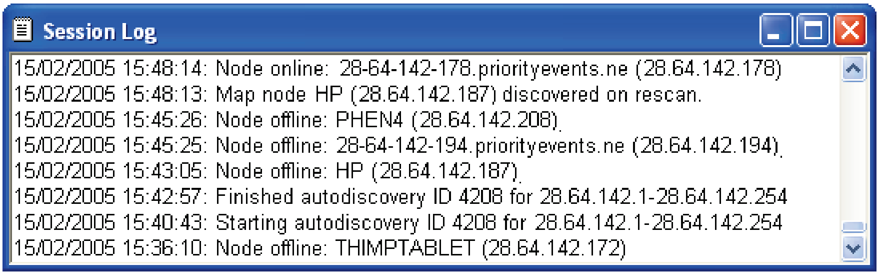
The Threat List includes information about when the node was detected and the node name, IP address, Ethernet address, the hub or switch the node is connected to, and the port number used for the connection if connected to an SNMP-enabled device.

4. ***If you detect a rogue node,*** you can disable network access for the node by clicking the node in the Threat List and then clicking the **Disable** button. If you determine a disabled node should be enabled, click the **Enable** button.

   Note: Only nodes connected to a switch port can be disabled or enabled.

5. Remove a node from the Threat List by selecting it and pressing the **Delete** key.

6. To access the Session Log, click **Window>Session Log**. The log lists the most recent information at the top and the oldest at the bottom of the log window.



```
15/02/2005 15:48:14: Node online:  28-64-142-178.priorityevents.ne (28.64.142.178)
15/02/2005 15:48:13: Map node HP (28.64.142.187) discovered on rescan.
15/02/2005 15:45:26: Node offline: PHEN4 (28.64.142.208)
15/02/2005 15:45:25: Node offline: 28-64-142-194.priorityevents.ne (28.64.142.194)
15/02/2005 15:43:05: Node offline: HP (28.64.142.187)
15/02/2005 15:42:57: Finished autodiscovery ID 4208 for 28.64.142.1-28.64.142.254
15/02/2005 15:40:43: Starting autodiscovery ID 4208 for 28.64.142.1-28.64.142.254
15/02/2005 15:36:10: Node offline: THIMPTABLET (28.64.142.172)
```

   Continuous Scan logs nodes on and off the network during scans, providing information vital for network forensics.

7. There are a large number of options you can configure by clicking **Monitor>Continuous Scan>Options.** Refer to the online help for details.

Investigating LANsurveyor Further

This concludes the guided tour of LANsurveyor.

LANsurveyor Responder Clients

LANsurveyor Responder clients are beyond the scope of this guide. If you want to install LANsurveyor Responder clients for evaluation, refer to the section “Install Responder Clients” in the *LANsurveyor Online Manual* at: http://www.solarwinds.com/support/lansurveyor/docs/LS10_online_manual/installneonresponders.htm.

Note that you will also need to connect to an existing SQL Server or have LANsurveyor install a new SQL Server Express database to use as the Repository for the information gathered by the Responder clients. Refer to the section “Repository” in the *LANsurveyor Online Manual* at: http://www.solarwinds.com/support/lansurveyor/docs/LS10_online_manual/repository.htm.

Explore the full wealth of monitoring features available by reading the SolarWinds LANsurveyor Administrator Guide available on the SolarWinds website.