SolarWinds

Network Topology Mapper Administrator Guide

SolarWinds Network Topology Mapper 01.20.15, version 2.2.0

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	www.solarwinds.com/support
User Forums	http://thwack.solarwinds.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

Contents

Chapter 4

Appendix A

Chapter 1

Introduction

The most powerful view of your network is the one that shows how particular nodes are connected to each other. A set of alerts tell you what the team needs to triage; those same alerts distributed as signals on a topology map show how the pattern of alerts indicate—for example—that a particular switch sits in the path of all the nodes currently sending alerts. Triage becomes much more finely focused when you can see how impacted nodes are interconnected.

Fully supporting IPv4 and IPv6 addresses, NTM powerfully enhances node management, creating a visual analogue for all nodes being monitored in you primary network monitoring system (such as SolarWinds Performance Monitorfor example).

Benefits of Network Topology Mapper

Consider the following benefits of SolarWinds Network Topology Mapper (NTM):

Defining and Reusing Credentials

Scheduling Device and Topology Discovery

Mapping Virtual Device Connectivity

Strategically Managing Maps

Sharing and Printing Maps

Encrypting Maps

Reporting

Defining and Reusing Credentials

NTM allows you to define and store credentials for re-use and allows you to order an active set of credentials according to how you want NTM to use them during discovery.

For detailed information, see “Specifying Discovery Credentials”.

Scheduling Device and Topology Discovery

NTM uses multiple discovery methods (SNMP, ICMP, WMI, CDP, VMWare) to map all types of devices and their interconnections—switches, routers, servers, VMs, unmanaged nodes, desktop computers, peripheral devices. In scanning a network, you can exclude devices and network segments from discovery scans and also track changes in network topology through scheduled updates.

Since NTM discovers multiple links for devices and maps Layer 2 (port level) and Layer 3 (logical) connectivity, as well as Etherchannel relationships, you can see and more easily understand physical and logical relationships between devices. NTM lets you view each layer separately or combined them in one map.

With a single discovery scan NTM allows you to create multiple maps and shows detailed system information for discovered devices, including load statistics, with rollover graphics down to the interface level.

For detailed information, see “Discovering Devices and Topologies”.

Mapping Virtual Device Connectivity

By providing both switch and VLAN details (in connection rollovers for HP/3Com and Juniper Switches, and mapping virtual servers to host machines, NTM provides a clear picture of the connectivity of virtual devices to your physical network.

Strategically Managing Maps

In working with the maps based on a discovery scan, you can choose to display or hide various details about the mapped nodes and the connections between them. You can arrange nodes according to predefined layouts or by manually dragging them. As needed, you can select an area of the larger map and copy it into a separate map.

For detailed information, see “Working with Maps”.

Sharing and Printing Maps

NTM facilitates IT monitoring, planning, trouble-shooting workflows by being able to export maps to multiple formats (Visio, PNG, Orion Network Atlas, PDF & NTM Map format).

Encrypting Maps

Enables stored and exported maps to be encryption protected with a password. This secures detailed network information contained in maps from being used by unauthorized persons. NTM uses FIPS-compliant encryption to secure map data in native NTM map files.

Notes:

- You can use maps from earlier versions of NTM but you will be prompted to change all SNMP v3 credentials which are not using FIPS compliant algorithms.
- "Proxy maps" created in previous versions of NTM and Network Atlas are not compatible with new version of NTM running in FIPS mode. If you need to use such older maps, you must disable the FIPS requirement on the operating system.
- If you change the FIPS requirement in your operating system, either by disabling or enabling FIPS, you must restart NTM if it is running at the time.

Reporting

NTM can generate reports on switch ports, VLANs, subnets, and device inventory.

How NTM Works

Using the standard protocols listed below, NTM discovers network nodes and the connectivity between them:

- Simple Network Management Protocol (SNMP)
- Windows Management Instrumentation (WMI)
- Link Layer Discovery Protocol (LLDP)
- Cisco Discovery Protocol
- VMware Management
- Internetwork Control Message Protocol (ICMP ping)

SNMP interrogates several device MIBs, including:

- MIB2:sysInfo
- IF MIB
- Cisco MIB

Note: NTM cannot poll the ipRouteTable MIB for Cisco devices running on IOS release 12.4(13b) and later releases.

After node detail and connectivity data is retrieved from nodes, NTM uses bridge table information if you chose that option in Discovery Settings.

Chapter 2

Installing NTM

NTM provides a simple, wizard-driven installation. Licensing, hardware and software requirements are nominal. Typically, it takes less than 30 minutes to install NTM and discover your network devices and connections.

The following are detailed in this chapter:

- NTM Installation Requirements
- Network Device Requirements
- Installing NTM

NTM Installation Requirements

The following tables provide the minimum requirements for SolarWinds NTM.

Software	Requirements
Operating System	• Microsoft Windows 8.1, 8, 7, Vista SP1, and XP x86 SP3 • Microsoft Windows Server 2003 SP2 and R2 (32/64-bit) • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2012 and R2 **(Note**: NTM supports FIPS on this OS only) Languages: • English • German • Japanese • Chinese
Application Framework	• .NET 3.5 AP1 & .NET 4.0 **Note**: If .NET is missing, NTM installs .Net FW 3.5 or 4.0

Hardware	
CPU Speed	2.66 GHz or faster
Hard Drive Space	10 GB
Memory	500 MB

Note: Device discovery and map rendering are CPU intensive. We recommend installing NTM on the fastest CPU PC available.

Network Device Requirements

The following table describes the requirements for optimal device discovery:

Node Type	
Network Device	SNMPv2c or SNMPv3 enabled
Windows Device	WMI enabled
ICMP Only Devices	Must not block ICMP requests.

Installing NTM

NTM uses a simple wizard driven interface during the installation process.

Note: The you must run the NTM installer from an account on the operating system that has Administrator privileges.

To install Network Topology Mapper:

1. ***If you are installing on Windows Server 2008 or later***, right-click **SolarWinds Network Topology Mapper.exe** and select **Run as Administrator**.
2. ***If you are installing on any of the other approved operating systems***, double-click **Solar Winds Network Topology Mapper.exe**.
3. Enter the e-mail address used to register the product download.
4. Review the End User License Agreement, select **I agree to the terms and conditions**, and then click **Install**.
5. Click **Enter Licensing Information**.
    a. Enter your Activation Key, and then click Next.
    b. Enter the appropriate name and contact information, and then click Next.
    c. Click Finish.
6. Select whether or not to participate in sending anonymous program data to SolarWinds, and then click **OK**.
7. When the installation completes, click **Close**.

Chapter 3

Discovering Devices and Topologies

SolarWinds Network Topology Manager provides a Network Discovery Scan Wizard to facilitate specifying the scope of a network you want to map. Discovery scans include SNMP, WMI, and VMware queries to interrogate devices for their node details and connectivity to other devices.

Each session of the Discovery Wizard creates a scan file, and from a single scan file you can create multiple maps, all of which are saved as part of the specific scan file.

A common strategy for discovering your network is to perform a single scan of each set of subnets and IP ranges for which you intend to create related maps with which to strategically visualize the parts of the overall network. In some cases, depending on the size of your overall network, you may want to scan the entire network and then work with the results to define specific maps.

See the chapter on “Working with Maps” for details on using NTM features to create the views of your network that you want.

Using the Network Discovery Scan Wizard involves entering information in four stages:

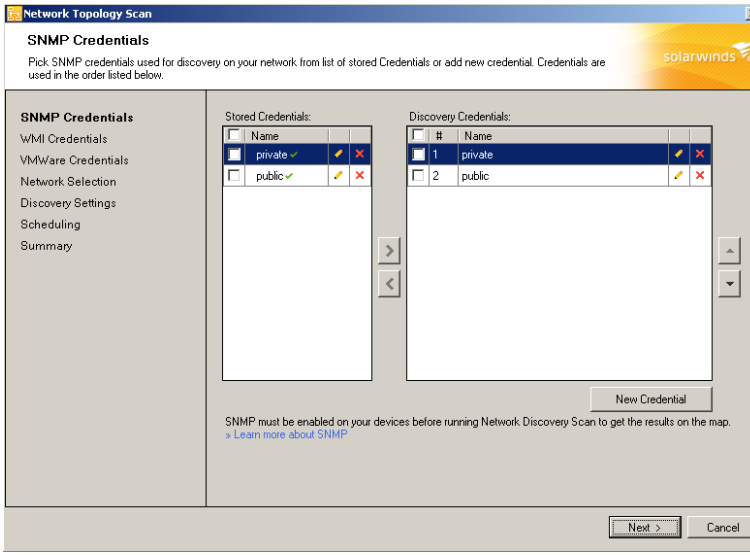
- Specifying Discovery Credentials
- Defining IP Addresses for Discovery
- Naming the Scan and Adjusting Scope
- Scheduling a Discovery
- Rescanning a Network

Specifying Discovery Credentials

Network Topology Manager is FIPS compliant, supporting both AES 192 and 256. Any SNMPv3 credentials you specify use FIPS-compliant algorithms to encrypt credentials.

To specify discovery credentials:

1. Either from the Getting Started with Network Topology Mapper screen—that displays by default when you open NTM—or the main Network Topology Mapper screen, click **New Scan**.



Automatically stored Private and Public credentials are listed under the Discovery Credentials currently available to use.

Note: For any credentials in Stored Credentials that you want to activate, select the credential and click the right arrow to move it into Discovery Credentials. If an active credential by the same name already exists, NTM prompts you either to save the credential you are activating under another name or to overwrite the currently active credential. For any active credentials in Discovery Credentials that you need to deactivate, select the credential and click the left arrow.

2. ***If you are not using the default public and private community strings,*** select **public** and click **Remove Credential**. Repeat this process for the **private** string.

   These credentials remain in Stored Credentials repository but cannot be used. To use them again, you would need to select them in the repository and use the arrow to move them into Discovery Credentials.

3. ***If you use SNMP v1 or v2c***, complete the following steps:
   a. Click **New Credential** and select SNMPv1/2.
   b. Enter a unique **Name**.
   c. Enter the **Community String** the devices use for SNMP read-only access.
   d. Enter a valid device IP address or hostname within your intended scan range, and then click **Test Credential**.
   e. If you want to store the credential, click **Store Credential**.
   f. If you want to make the credential available during future discoveries, click **Automatically use for future discoveries**.

      Selecting this puts the new credential into the repository of active Discovery Credentials.
   g. Click **Save**.
4. If you need to activate or deactivate a credential, select it in the
5. ***If you use SNMP v3***, complete the following steps:
   a. Click **New Credential** and select SNMPv3.
   b. Enter a unique **Name**.
   c. Enter a **User Name**.

      For Cisco devices, this is defined in the `snmp-server users` configuration command.

      Note: NTM cannot poll the ipRouteTable MIB for Cisco devices running on IOS release 12.4(13b) and later releases.
   d. Enter the **Context**. For Cisco devices, this is defined in the `snmp-server group` configuration command.
   e. Select the **Authentication Method**. For Cisco devices, this is defined in the `snmp-server user` configuration command.
   f. Enter the password or key in the **Password/Key** field.
   g. ***If you have entered a key***, select **Password is a key**.
   h. Select the **Privacy/Encryption Method.** For Cisco devices, this is also defined in the `snmp-server user` configuration command.
   i. Enter the password or key in the **Password/Key** field.
   j. ***If you have entered a key***, select **Password is a key**.
   k. Enter a valid device IP address or hostname within your intended scan range, and then click **Test Credential**.

l. ***If the test fails,*** review the device SNMP v3 configurations and ensure you are using the proper fields.

m. If you want to store the credential, click **Store Credential**.

n. If you want to make the credential available during future discoveries, click **Automatically use for future discoveries**.

Selecting this puts the new credential into the repository of active Discovery Credentials.

o. Click **Save**.

6. Click **New Credential** to add WMI credentials.

Notes: NTM uses WMI credentials to gather details about Windows nodes as stand-alone devices and as VMware guests. NTM also uses WMI credentials to discover Hyper-V devices, including roles and guests. By default, no WMI are stored or available.

For any credentials in Stored Credentials that you want to activate, select the credential and click the right arrow to move it into Discovery Credentials. If an active credential by the same name already exists, NTM prompts you either to save the credential you are activating under another name or to overwrite the currently active credential. For any active credentials in Discovery Credentials that you need to deactivate, select the credential and click the left arrow.

a. Enter a unique **Name**.

b. Enter the **WMI User Name**, enter a password and then re-enter the password in the **Confirm Password** field.

c. Enter a valid device IP address or hostname within your intended scan range, and then click **Test Credential**.

d. If you want to store the credential, click **Store Credential**.

e. If you want to make the credential available during future discoveries, click **Automatically use for future discoveries**.

Selecting this puts the new credential into the repository of active Discovery Credentials.

f. Click **Save**.

7. Click **Add Credentials** to add VMware credentials.

Notes: NTM uses VMware credentials to gather details about VMware hosts and guests. VMware discovery displays the host and associated guests by IP address only. To retrieve details about guests, include the use WMI credentials, and ensure that the discovery IP range, including the IP addresses of the guests in your network IP range.

For any credentials in Stored Credentials that you want to activate, select the credential and click the right arrow to move it into Discovery Credentials. If an active credential by the same name already exists, NTM prompts you either to save the credential you are activating under another name or to overwrite the currently active credential. For any active credentials in Discovery Credentials that you need to deactivate, select the credential and click the left arrow.

a. Enter a unique **Name** for the vCenter or ESX.

b. Enter the **VMWare User Name**, enter a password and then re-enter the password in the **Confirm Password** field.

c. Enter a valid device IP address or hostname within your intended scan range, and then click **Test Credential**.

d. If you want to store the credential, click **Store Credential**.

e. If you want to make the credential available during future discoveries, click **Automatically use for future discoveries**.

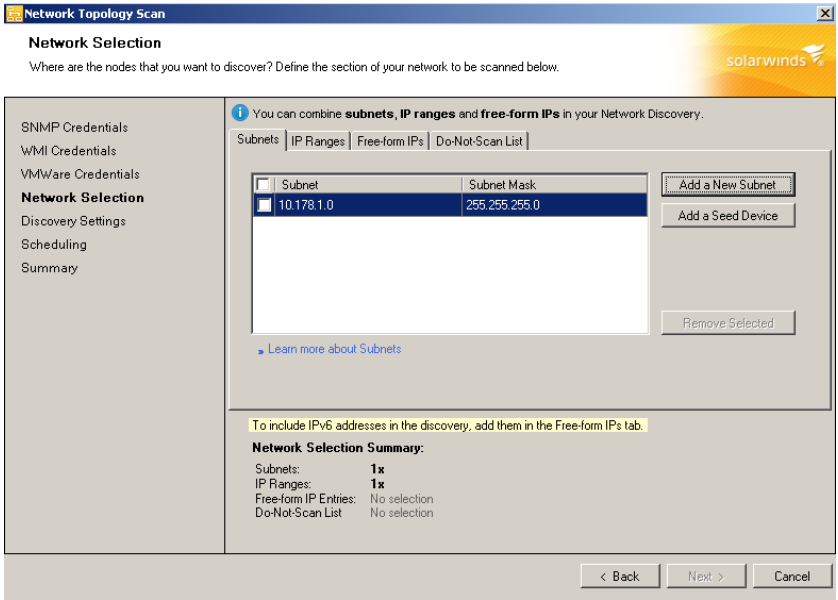
Selecting this puts the new credential into the repository of active Discovery Credentials.

f. Click **Save**.

Defining IP Addresses for Discovery

When all of the credentials for your discovery scan have been added, the discovery wizard advances to the Network Selection section. You can choose from several options to specify the IP addresses you want to discover. You can combine any of the options to better define your discovery range.

Sections are organized in order that the discovery wizard presents you with discovery options.



For information on IP address range options see Appendix A: Network Discovery Options.

Specifying Subnets

Use these steps to discover nodes by the subnet to which they belong.

Caveat: An address range that include more than 2000 nodes takes much longer (one to two days, for example) to discover than the same number of nodes split up into multiple smaller ranges. Additionally, with so many nodes on a map, the user interface and NTM operations may run with noticeable lag.

For example, if you are subnetting with the mask of 255.255.248.0, then the maximum number of nodes within the subnet will be 8 X 255 = 2040. In discovery nodes, the software engine creates a lookup table in memory that includes as many rows as nodes in the defined IP range or subnet. The more rows the more time the engine must spend in finding its point of reference in the table as it iterates through the table. Walking a larger lookup table takes significantly more time than walking smaller tables the cumulatively contain the same number of arrayed items. So the time it takes the engine to complete its discovery task directly depends on the number of possible nodes in the specified range or subnet.

To discover devices by subnets:

1. Click the **Subnets** tab.
2. ***If you want to add discovery subnets,*** click **Add a New Subnet**.
3. Enter a **Subnet Address** and a **Subnet Mask**.
4. To add additional subnets repeat steps 2 and 3.
5. ***If you have finished specifying your discovery nodes, ranges and subnets,*** click **Next**.

To discover devices by seed device:

1. Click the **Subnets** tab.
2. Click **Add a Seed Device**.
3. Enter the **IP Address** of the seed device, and then click **Add**.
4. When the discovery engine populates the **Subnet** dialog, select the subnets to be removed from discovery, and then click **Remove Selected**.
5. ***If you only want to discover these subnets,*** click **Next**.
6. ***If you want to specify other devices by IP address range, or as a free-form set of hostnames and addresses (in either IPv4 or IPv6 networks),*** click the **IP Ranges** or **Free-form IPs** tab.

7. ***If you want to create a Do Not Scan list of devices within the subnets you have defined,*** click **Do-Not-Scan List**.

Specifying an IP Address Range (IPv4)

Use these steps to discover nodes within an IP address range.

To discover a specific range of IP addresses:

1. Click the **IP Ranges** tab.
2. Enter the **Start Address** and **End Address** for a contiguous range of IP addresses.
3. ***If you want to add additional ranges***, click **Add**, and then specify the range.
4. ***If you only want to discover these IP ranges,*** click **Next**.
5. ***If you want to specify other devices by subnets or a seed device, or as a free-form set of hostnames and addresses (in either IPv4 or IPv6 networks),*** click the **Subnets** or **Free-form IPs** tab.
6. ***If you want to create a Do Not Scan list of devices within the ranges you have defined,*** click **Do-Not-Scan List**.

Specifying Freeform Device Information (IPv4/IPv6)

Use these steps to define hostnames and IP addresses (IPv4/IPv6). In specifying a range of devices within a subnet, you can use format that delimits addresses with a hyphen (for example, 10.0.0.10-10.0.0.42) or CIDR notation (for example, 10.0.0.0/24).

To discover hostnames or IP addresses:

1. Click the **Free-form IPs** tab and do one of the following:
   a. ***If you are adding individual hostnames or IP addresses***, type the each one on its own line.
   b. ***If you are defining a range within a subnet***, type each range on its own line.

      In specifying a range of devices within a subnet, you can use format that delimits addresses with a hyphen (for example, 10.0.0.10-10.0.0.42 or 2001:db8:0:0:0:0:0:0-2001:db8:0:ffff:ffff:ffff:ffff:ffff) or CIDR notation (for example, 10.0.0.0/24 or 2001:db8::/48).
2. ***If you only want to discover these nodes,*** click **Next**.
3. ***If you want to specify other devices by IP address ranges or subnets,*** click **IP Ranges** or **Subnets**.

4. ***If you want to create a Do Not Scan list of devices within the ranges you have defined,*** click **Do-Not-Scan List**.

Creating a Do Not Scan List

After you have defined subnets, IP address ranges, and other hostnames and IP addresses in which to discovery devices, use these steps to exclude any devices (if any) from the ranges and subnets.

To exclude devices from discovery:

1. Click the **Do-Not-Scan List** tab and do one of the following:

   a. ***If you are excluding individual hostnames or IP addresses***, type the each one on its own line.

   b. ***If you are excluding a range within a subnet***, type each range on its own line.

      In specifying a range of devices within a subnet, you can use format that delimits addresses with a hyphen (for example, 10.0.0.10-10.0.0.42 or 2001:db8:0:0:0:0:0:0-2001:db8:0:ffff:ffff:ffff:ffff:ffff) or CIDR notation (for example, 10.0.0.0/24 or 2001:db8::/48).

2. ***When you are finished defining exclusions,*** click **Next**.

Naming the Scan and Adjusting Scope

1. Enter a **Scan name**.
2. Select the number of hops you want the discovery to transverse.

   Notes: Hops are only used for subnet and seed device discoveries. Other discovery options will ignore the hops setting. We recommend using zero hops. Using one or more hops may significantly extend the time required to complete discovery.

3. ***If you want to ignore nodes that do not respond to WMI or SNMP***, select **Ignore node that only respond to ICMP (ping)**.

   Note: For more information on this option, see General Discovery Options.

4. ***If you want to eliminate bridge tables from topology calculations,*** select **Don't use Bridge Table information to calculate network topology**.

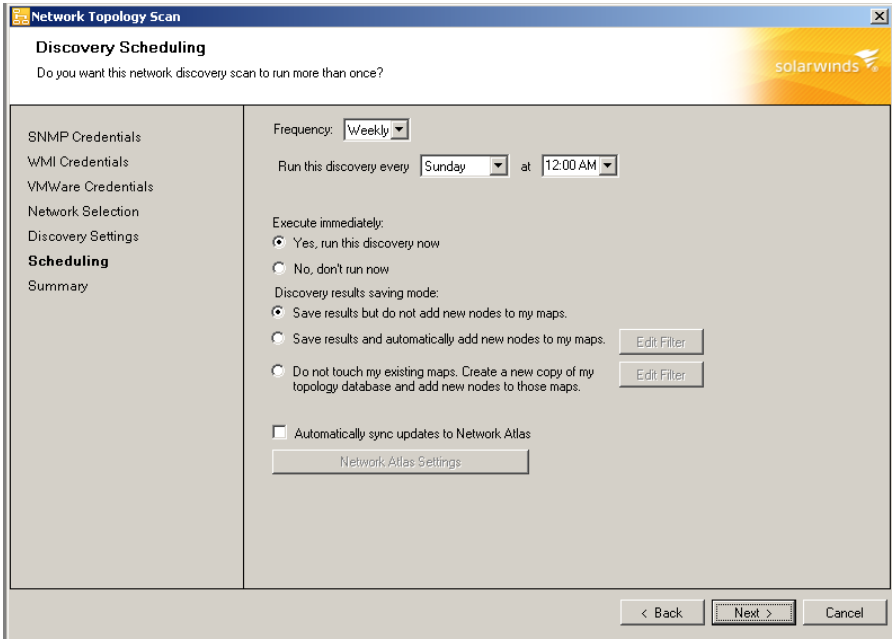
   Note: For more information on this option, see General Discovery Options.

5. Click **Next**.

Scheduling a Discovery

NTM provides controls for scheduling a discovery either once or recurrently. For scheduled discoveries, NTM must be running in order to apply latest results to the relevant map(s).

Discovery may take several minutes depending on the discovery IP range and complexity of device connectivity.



Use the follow steps to schedule a discovery.

1. ***If you want to run a manual discovery***, then do the following:
   - **a.** Select **Once** under Frequency.
   - **b.** ***If you want to run the discovery now*****,** select **Yes, run this discovery now** and then click **Next**.
   - c. ***If you want to run the discovery later***, select **No, don't run now**, and then click **Next**.
   - **d.** Review your selections and click **Discover** (if you selected to scan now) or **Save** (if you selected to scan later).
2. ***If you want to run a scheduled discovery***, select a schedule interval under Frequency.

a. ***If you select Daily***, then select a time for executing the scan each day.

b. ***If you select Weekly***, then select a day and time for executing the scan each week.

c. ***If you select Monthly***, then select a day and time for executing the scan each month.

d. ***If you select Custom***, then define the pattern for recurrently executing the scan.

3. Select an option under execute immediately.

   a. ***If you want to activate the scheduled discovery now*****,** select **Yes, run this discovery now** and then click **Next**.

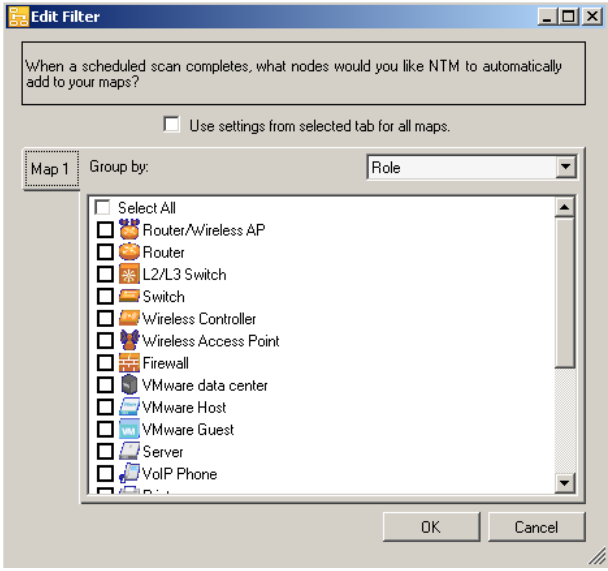
   b. ***If you want to activate the scheduled discovery later***, select **No, don't run now**, and then click **Next**.

4. Select an option for saving the results of your scan.

   a. ***If you want NTM not to add newly discovered nodes but to remove nodes from maps that are not found in any scheduled rescans***, select the option: **Save results but do not add new nodes to my maps**.

   b. ***If you want NTM to add new nodes to maps based on your filter settings***, select the option: **Save results and automatically add new nodes to my maps**.

      Clicking **Edit Filter** lets you select the types of new nodes NTM will add to your maps.

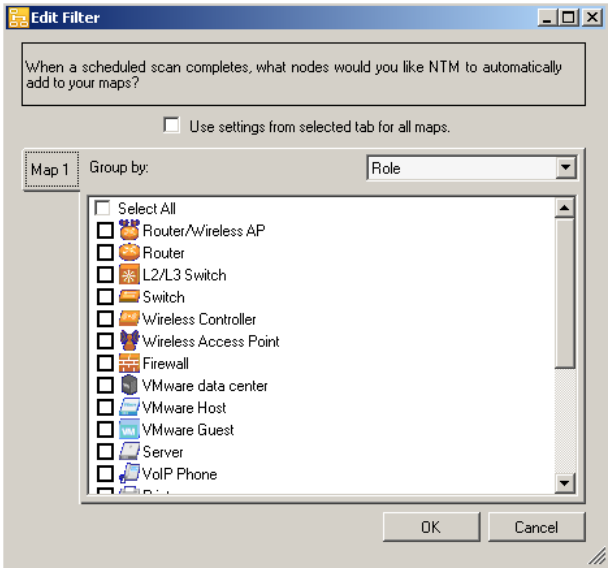


Note:

Do not use this option if you intend to manually edit a map whose scan file is setup for automatic updates. Instead, to preserve your manual edits, use the option: **Do not touch my existing maps. Create a new copy of my topology database and add new nodes to those maps.**

c. ***If you want NTM to copy your existing topology database and add new nodes to those maps*****,** select the option: **Do not touch my existing maps. Create a new copy of my topology database and add new nodes to those maps.**

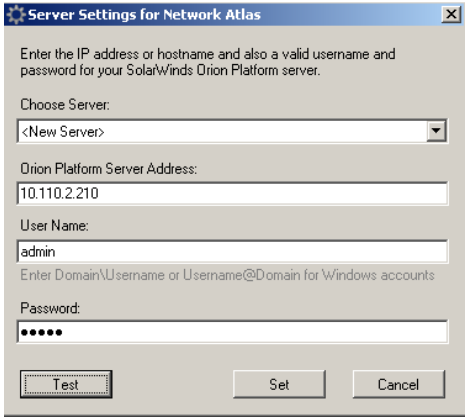
Clicking **Edit Filter** lets you select the types of new nodes NTM will add to your maps in the copy of the scan.



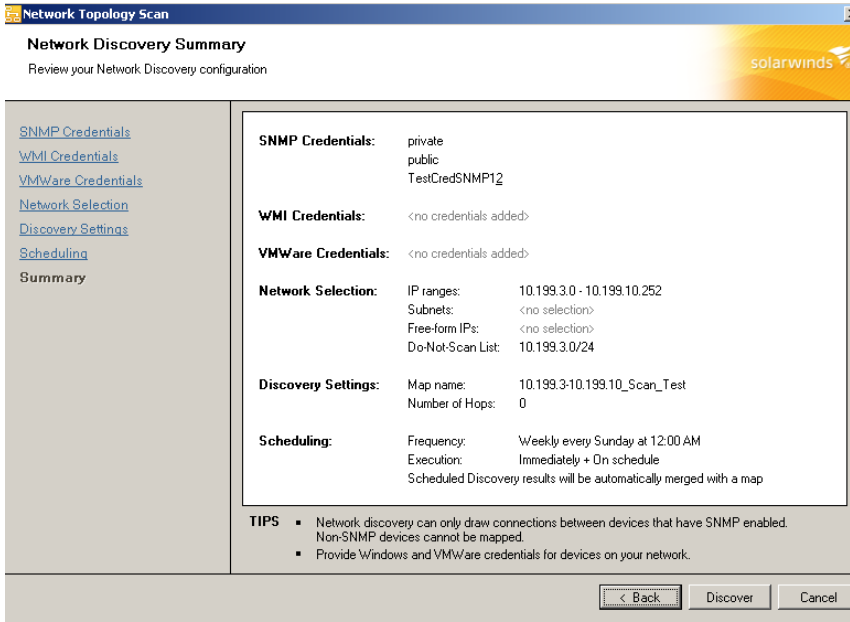
Note:

Use this option especially if you intend to manually edit a map whose scan file is setup for automatic updates**.**

5. If you have Network Performance Manager and you intend to export your map data to Network Atlas, then select **Automatically sync updates to Network Atlas**.



6. Enter the information on your Network Atlas server.
7. Click **Next**.



8. Review your selections and click **Discover** (if you selected to activate the scheduled discovery) or **Save** (if you selected to activate the scheduled discovery later).

Reviewing Discovery Results

When discovery completes, SolarWinds NTM presents the results in a default map called **Map1**, on NTM automatically displays all discovered switches and routers.

By default, if NTM discovers fewer than 100 switches and routers, then it also shows the Network Segments and other nodes to which switches and routers are connected. For detailed information about Network Segments, see “Opening Maps from Earlier Versions of NTM”.

If NTM discovers 100 or more switches or routers, it omits Network Segment and other nodes from the default map. In this case, you can always reveal these other nodes by using the Neighbors feature. See the section on “Showing and Hiding Neighbors” for details.

Note: To change the maximum number of nodes—besides all the discovered switches and routers—that NTM should add to the default map, you can edit the value of the parameter NewScanNodeCountThreshold in SolarWinds.NTM.Client.exe.config (Program Files\SolarWinds\Network Topology Mapper). For example, if you set the value of NewScanNodeCountThreshold to 1000, NTM will display all switches and routers and, assuming there are fewer than 1000 of those devices, NTM will also display some number of their neighbors until the display count in the default map equals 1000.

In the left pane, based on the results displayed in Map1, use a pattern from Map Layouts to reorganize the distribution of nodes, Group By options under Discovered Nodes to highlight nodes in the map, Node Display Options and Connection Display Options to control what details regarding nodes and connections display in the map.

See Chapter 4 for detailed information on “Working with Maps”.

Rescanning a Network

NTM enables you to rescan (rediscover) the network based on the existing settings. You can also adjust settings and rescan based on the modified settings; in this case, NTM overwrites the data in the existing scan file.

Notes:

- If you are rediscovery your network based on an NTM 1.0 map, then as part of the results you will see Network Segment nodes added to the existing map. For more information about Network Segment nodes, see “Opening Maps from Earlier Versions of NTM”.
- If you are rediscovering your network based on a map created in any previous version of NTM, then link aggregations automatically display only after rescanning. For more information, see “Opening Maps from Earlier Versions of NTM”.

To rescan a network:

1. ***If the scan file is not already open*****,** open it (**File > Open)**.
2. ***If you do not need to adjust any settings***, simply click **Rescan** on the toolbar.
3. ***If you need to adjust settings***, click **Discovery Settings** at the lower left and make your changes, as needed, and then click Discover in the Summary screen.

   Note: NTM will overwrite the data in the existing scan file based on the modified settings. If you do not want to change the data in the existing scan file, use the Discovery Wizard to create a new scan.

Missing Connections

NTM may be unable to generate connections among discovered nodes for the following reasons:

- Invalid credentials

  Use “Test” at the bottom of the Add Credential resource to verify before adding or modifying credential.

- Device does not support SNMP

  NTM uses SNMP polling to retrieve CDP and LLDP data. Without that Layer 2 and Layer 3 data, NTM cannot map direct connections among discovered nodes.

  So in such a case, assuming a device doesn not support SNMP but supports and can respond to ICMP, NTM would the node as indirectly connected only to other relevant ICMP devices, through a Network Segment node.

  For detailed information about Network Segments, see “Opening Maps from Earlier Versions of NTM”.

- Device is configured not to return CDP/LLDP data by SNPM requests

  The result is the same as in the case that the device does not support SNMP.

- Timeouts are triggered due to slow response from a devices

  If NTM is configured not to retry, or the specified number of retries fail, then the device is treated as an ICMP node.

  You can modify timeout settings in "SolarWinds.NTM.BusinessLayer.dll.config" (\Program Files\SolarWinds\Network Topology Mapper).

  ```
  <appSettings>
  ```

```
...
<add key="NtmICMPTimeout" value="5000"/>
<add key="NtmMaxSnmpReplies" value="5"/>
<add key="NtmSnmpTimeout" value="3000"/>
<add key="NtmSnmpRetries" value="0"/>
...
<add key="NtmWmiRetryInterval" value="1000"/>
<add key="NtmWmiRetries" value="3"/>
...
<add key="NTMVIMTimeout" value="3000"/>
...
</appSettings>
```

Chapter 4

Working with Maps

NTM offers several options for viewing, customizing, importing, exporting and saving maps. This chapter details each of these options.

This section describes the use of the following features:

- Opening Maps from Earlier Versions of NTM
- Showing and Hiding Neighbors
- Using Map Navigator
- Navigating Nodes in a Map
- Filtering Nodes and Searching Maps
- Using Discovered Nodes

Finding More Nodes

If a node you need to track does not fall within the IP ranges or subnets you have already discovered, and so appears neither in your existing maps nor the list under Discovered Nodes, you can use **Find More Nodes** to extend your discovery.

To find more nodes:

1. Click **Find More Nodes** under Discovered Nodes.
2. Read the message and click OK to acknowledge it.
3. Add additional IP ranges or subnets to the Network Selection tabs of the discovery wizard.
4. Click through the other wizard screens, making changes as needed.
5. Click Discover.

For more information on node discovery, see “Discovering Devices and Topologies”.

- Viewing Connection Information
- Viewing and Editing Nodes and Node Details
- Using Map Layouts

Opening Maps from Earlier Versions of NTM

In opening a map from SolarWinds NTM version 2.1 or earlier, NTM first converts the map into a scan file, retaining the existing name.

In preparing to display the map for the new scan file, NTM consults the value of the parameter **ForceAddOnlyNetworkDevices** (Program Files\SolarWinds\Network Topology Mapper) to determine which and how many nodes to display. If the value is **true**, NTM behaves as it would in creating the default map for a new scan, displaying all switches and routers and only as many neighbor devices as can fit within the threshold set for **NewScanNodeCountThreshold** in SolarWinds.NTM.Client.exe.config (Program Files\SolarWinds\Network Topology Mapper).

Like other maps in NTM 2.2, a converted map is connected to its scan file, and you can create additional maps based on that same file.

Showing Aggregated Links (EtherChannel)

During network discovery, by default, SolarWinds NTM version 2.2 obtains information about links that are aggregated through supported protocols (LACP, PAgp).

For any map created with an earlier version of NTM, to see link aggregation information, you must perform a rescan following the map's conversion into a scan file. Aggregated links are indicated by a loop around link lines:

To show aggregated links in converted maps:

1. Open Calculation.cfg (\Program Files\SolarWinds\Orion) in a text editor.
2. Find the ResultProcessors group at the bottom of the file.

```
<ResultProcessors>
    <string>CalculationNodesResultProcessor</string>
    <string>L2LinksResultProcessor</string>
    <string>L3LinksResultProcessor</string>
    ...
  </ResultProcessors>
```

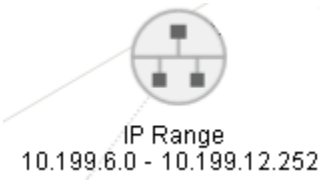
3. Add EtherchannelLinksProcessor as a string element.

```
<ResultProcessors>
 <string>CalculationNodesResultProcessor</string>
 <string>L2LinksResultProcessor</string>
 <string>L3LinksResultProcessor</string>
 <string>EtherchannelLinksProcessor</string>
 ...
</ResultProcessors>
```

4. Save the file.
5. With the appropriate scan file open, click **Rescan** and follow the prompts.

Understanding Network Segment Nodes

In generating a map based on a discovery scan, if NTM did not detect specific connection information for a node, NTM generates a Network Segment node that indicates the subnet or IP range to which the node is related. For example, this Network Segment node represents an IP Range:



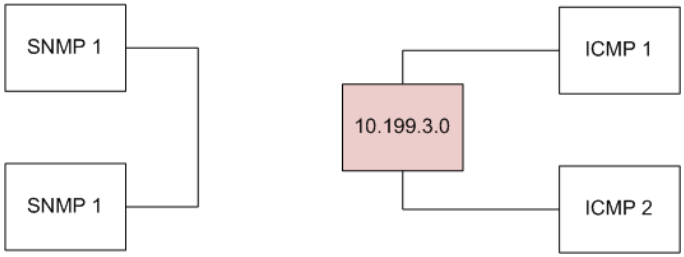
NTM generates Network Segment nodes based on the three types of connection information that it collects and builds:

- Layer 2 connections - based on LLDP or CDP advertisements and MAC addresses in Bridge tables.
- Layer 3 connections - based on subnet membership and next hop information retrieved from devices.
- Virtualization connections – based on host/guest hierarchy.

Based on connections that it discovers for these three connection types, NTM creates a virtual node that points the way to figuring out how an ambiguously connected device is positioned on the network.

Example

Let's assume we discover 4 nodes—2 via SNMP and 2 via ICMP. The SNMP nodes are directly connected; the ICMP nodes are indrectly connected as part of the same subnet. Here is how the map objects appear:



Node 10.199.3.0 is a Network Segment node that indicates the subnet in which the two discovered ICMP nodes are connected.

Though it generates network segment nodes as part of the scan file for a discovery, NTM automatically displays network segments on a default map—the one created after the Discovery Wizard completes its scan—if the total number of switches and routers the wizard discovers is less than 100. If 100 or more switches or routers are discovered, NTM omits network segments from the default map. However, you can always reveal a network segment to which one or more of your nodes is connected by using the Neighbors feature.

For more information, see “Showing and Hiding Neighbors”.

Showing and Hiding Neighbors

All maps relate to a specific discovery scan file. For nodes on a specific map, based on all the discovered nodes in the scan file, NTM indicates that there are unseen neighbors that connect to a given node.

Clicking the Neighbors icon inset at the top right on a node, or right-clicking the node and selecting **Add Neighbors**, shows all nodes to which the selected node is connected. In many cases, the neighboring node is a network segment node. For detailed information about Network Segments, see “Opening Maps from Earlier Versions of NTM”.

In discovering your network, based on your selections in the Discovery Wizard, NTM automatically shows all switches and routers on a default map (“Map1”). You can use the Neighbors icon on these network devices to reveal more connections on the default map, as needed. Before revealing neighbors of device, if you want to know how many neighbors are currently hidden, hold the mouse over the device to see a summary that includes **Hidden Neighbors**.

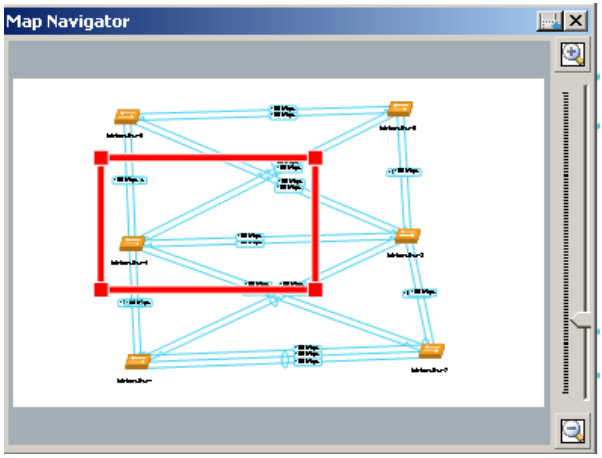
As you increase the detail on the default map, consider selecting and copying sections of the map to a new map (**File > New Map**). This new map, along with any others you make based on the single scan file, will always appear in its own tab when you open the relevant scan file.

You can hide neighbors from a map either by undoing the action of revealing them (**Edit > Undo**) or simply by deleting them (**right-click > Delete node**). Nodes deleted from a map remain in the scan file and can be re-added to the same map or to any other map at any time.

Using Map Navigator

The Map Navigator allows you to quickly navigate large, complicated maps. The navigator launches when NTM renders a new map. The Map navigator consists of these components:

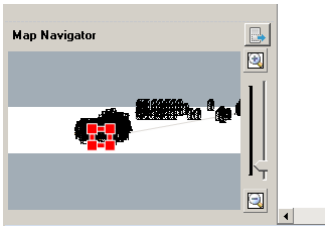
- Map Navigator widget screen
- Selection window (red box)
- Zoom bar
- Snap In



To move the navigator selection window, click and hold inside the red selection window and drag the box to a new location. You can change the area of the map selection window by clicking the edges or corners of the selection and dragging to a new location within the navigator.

To zoom in or out, use the zoom bar controls or the zoom slider. You can also zoom using the zoom option on the top map menu bar. The map navigator automatically adjusts to display the selected zoom area.

Use the Snap In button to dock the Map Navigator in the left pane.



Use the Snap Out button to free the Map Navigator from the left pane.

To close Map Navigator, click in the navigator window. To reopen the navigator select **View > Map Navigator**.

Navigating Nodes in a Map

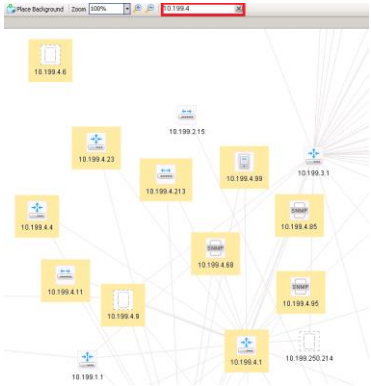
Besides using Map Navigator to control the area of a map in view, you can navigate the map using Move Map, Zoom, and windows controls. Move Map and Zoom are on the map top menu bar. To zoom using windows controls, press and hold the control key and use the mouse scroll wheel.

Filtering Nodes and Searching Maps

You can filter the nodes on your map using the search option on the top menu bar. The filter applies only to properties of nodes as they are currently displayed. To alter the displayed node properties, click **Node Display Option** on the left options bar and select the display option to match your search.

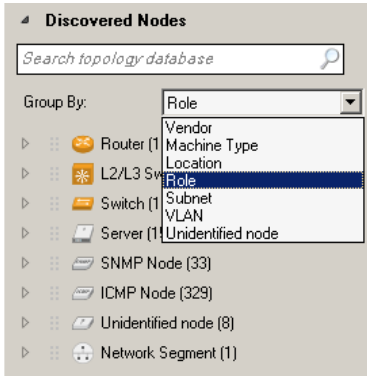
For example, to filter using IP addresses:

1. Click **Node Display Options**.
2. Select **IP Address**.
3. Enter the IP Address filter in the search window. The graphic displays a search for relevant IP addresses where the found items are highlighted in yellow.



Using Discovered Nodes

To access this view, click **Discovered Nodes** in the left options menu.

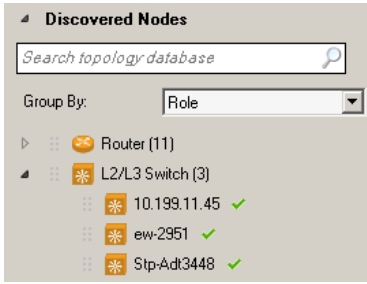


To select the grouping, click **Group by:** and select a grouping option from the list. The display options are described below:

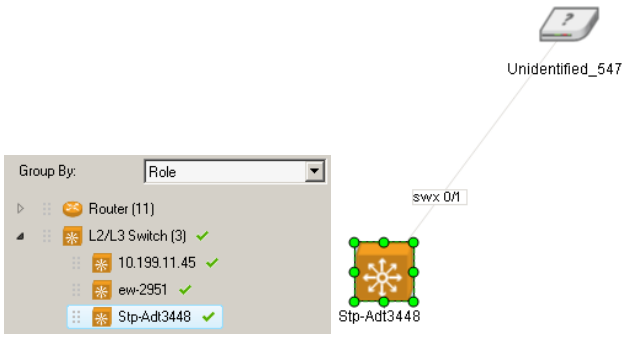
- **Vendor**: The vendor information listed in SNMP MIB2:sysDiscr.
- **Machine Type**: Make and model listed in SNMP MIB2:sysInfo.
- **Location**: Location listed in SNMP MIB2:sysLocation.
- **Role**: The network service provided, such as router, switch, server, or wireless controller.
- **Subnet**: The configured subnet from the IF MIB.
- **VLAN**: The configured VLAN from the IF MIB. The view displays the ID with VLAN Name; if a VLAN Name is not defined the VLAN shows as Unknown.
- **Unidentified node**: Nodes which respond to ICMP only.

- **Custom Property**: A user assigned property.

To view node within a group (except Unknown nodes) click the expand triangle next to the group.



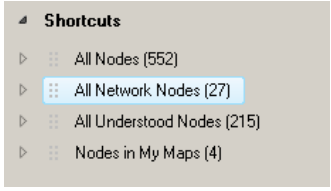
To select a node and highlight it on the map, click the node name.



Double-click the node name to center the map around a node.

Using Shortcuts

To access this view, click **Shortcuts** in the left options menu.



Click one of the shortcuts to highlight all the relevant nodes in the currently displayed map. To locate and highlight a specific node in a shortcut category, click the triangle next to the shortcut to reveal a list of all nodes in the category, and then click a specific node.

Finding More Nodes

If a node you need to track does not fall within the IP ranges or subnets you have already discovered, and so appears neither in your existing maps nor the list under Discovered Nodes, you can use **Find More Nodes** to extend your discovery.

To find more nodes:

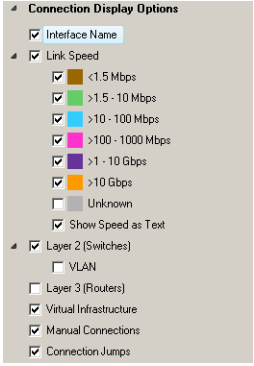
1. Click **Find More Nodes** under Discovered Nodes.
2. Read the message and click OK to acknowledge it.
3. Add additional IP ranges or subnets to the Network Selection tabs of the discovery wizard.
4. Click through the other wizard screens, making changes as needed.
5. Click Discover.

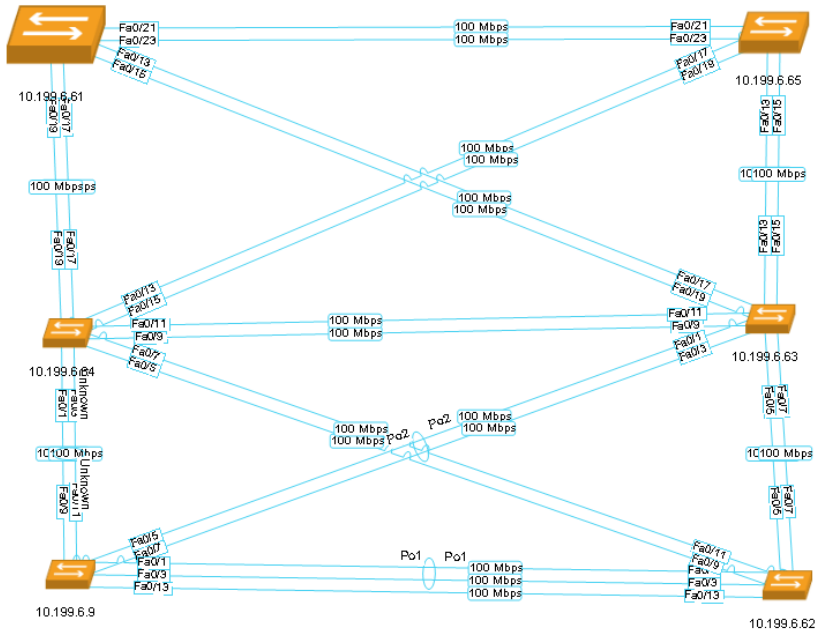
For more information on node discovery, see “Discovering Devices and Topologies”.

Viewing Connection Information

Hover the mouse over a node connection line to view connection information. The link speed indicated is the speed range defined in **Connection Display Options**.

To see the configured speed of interfaces, click **Connection Display Options** on the left options bar and select **Show speed by text**.





The **Link Speed** options only affect the displayed coloring of layer 2 links by speed range, and the display of **Speed by text**. When link speed is cleared, all connections show as grey lines.

The **Connection Display Options** allow you to view layer 2 (Link layer), layer 3 (IP layer) information, virtual infrastructure and custom/manual connections.

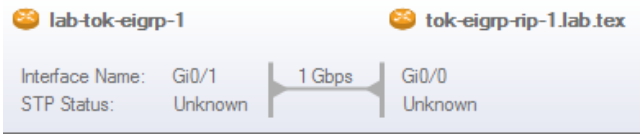
When a connection has information from both layers 2 and 3, the connection only displays layer 2 information. To switch to layer 3 information, clear the **Layer 2 (Switches)** check box in **Connection Display Options** and select **Layer 3**.

Select **Virtual Infrastructure** to see the virtual machines running on discovered nodes

A custom connection is one that you manually add to the map with the Connect Devices tool.

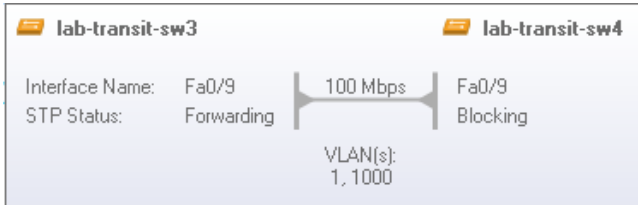
To display custom connections in your map select **Manual Connections** in **Connection Display Options**.

You can rollover any link on your map to see for each device in the link the Interface Name, Port Number, and any STP details; and the link speed by which data passes between the devices.



If you select **Layer 3** for your Connection Display, you see the IP Address and Subnet for the devices.

If you select **Layer 2 VLAN** then you see any VLANS running through a connection; rolling-over the VLAN indications shows you the VLAN IDs associated with the connection along with the other connection information related to the devices.

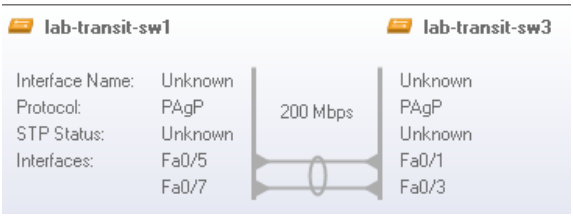


Finally, **Connection Jumps** indicate the separation of links where they seem to intersect in your maps.

Viewing Aggregated Links (EtherChannel)

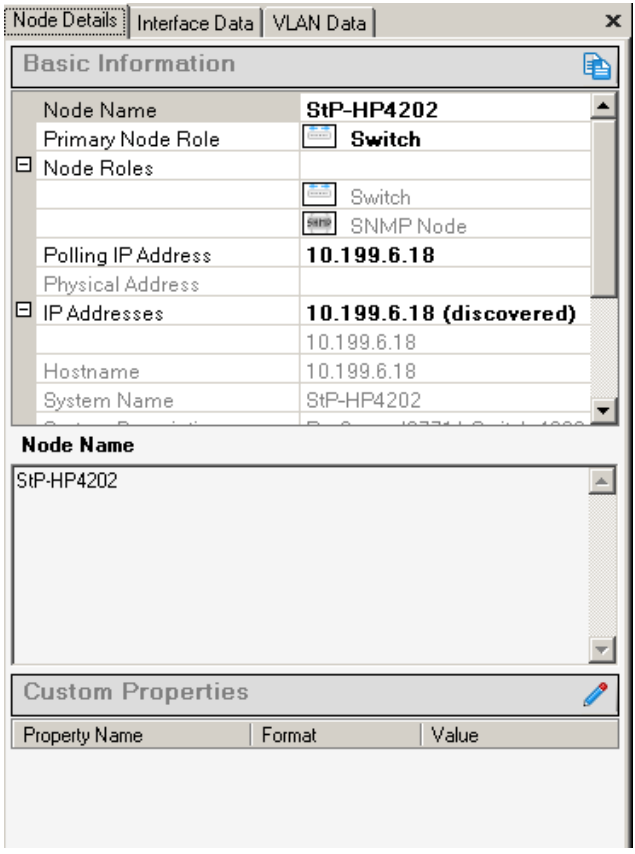
During network discovery, by default, SolarWinds NTM version 2.2 obtains information about links that are aggregated through supported protocols (LACP, PAgp). Aggregated links are indicated by a loop around link lines:

Hovering over an aggregated link icon reveals information about related interfaces, protocols, STP statuses, interfaces, and link speeds:



Viewing and Editing Nodes and Node Details

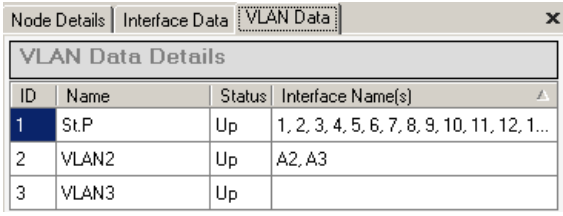
You can view node details by hovering the mouse cursor over a node. To view more detailed node information, right-click a node and select **Node Properties**.



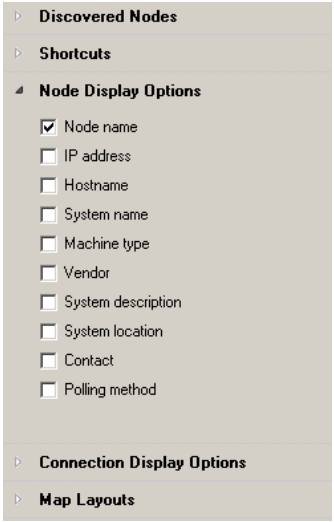
You can edit the node name, change the Node Role or Polling IP Address from dropdown lists; and review information on the discovered IP Address(es), Hostname, System Name, System Description, Machine Type, Vendor, System Location, Contact, and Polling Method.

You can review the node's Interface Data, including the ARP cache related to MAC/IP Address matches.

And you can review the node's VLAN Data: the name, status, and interfaces for each VLAN for which the node is configured.



By default NTM uses node names for map displays. To select the node information displayed on maps, click **Node Display Options** on the left option bar.



To enable any of the **Node Display Options**, select the check box next to the option name. The map updates when the check boxes are selected.

Notes:

- By default, NTM displays up to 22 characters in a node name. If you need to increase the number of available characters, adjust the value of NTMMapNodeNameLength parameter in SolarWinds.NTM.Client.exe.config (Program Files\SolarWinds\Network Topology Mapper).
- Options can only be selected one at a time. Allow the map to update a selected option before selecting an additional option.

Using Map Layouts

To select a map layout, expand Map Layouts from the left options bar and click the option you want to see. The map layout options are described below:

- **Radial**: Nodes are arranged on concentric circles around core devices.
- **Symmetrical**: Nodes are arranged on concentric circles using uniform connection lengths. This option is very similar to the radial layout option.
- **Orthogonal**: Device connections are vertical and horizontal only.
- **Layered**: Nodes are arranged orthogonally and sorted by map object type such as multiple connections (core) or single connection (leaf) devices.

Use the option that best fits your preference or mapping standards.

With **Align** options you can align selected nodes left, right, top, bottom, and center them vertically or horizontally. With **Distribute** options you can arrange selected nodes with respect to each other either horizontally or vertically.

Importing Maps

NTM allows you to import Orion Network Atlas maps. For more information about Orion Network Atlas, see the *SolarWinds Orion Network Atlas Administrator Guide*.

To import a map:

1. Click **File > Import > Network Atlas Maps**.
2. Create a file password as needed.
3. Navigate to a saved Network Atlas map and click **Open**.

Saving Maps
Follow these steps to save a map.

To save a map:

1. Click **File > Save as**.
2. Navigate to the folder you want to save map files in, enter a **File Name**, and then click **Save**.

Opening a Saved Map
Follow these steps to open a map.

To open a saved map:

1. Click **File > Open**.
2. Navigate to the folder containing the map, and then click **Open**.

Using Map Backgrounds
Map backgrounds allow you to arrange nodes in NTM to the fit layout of your network. Backgrounds should show network locations and not include Network nodes or connections. NTM nodes and connections overlay backgrounds. You have two sample map backgrounds available in NTM. These backgrounds are meant to demonstrate how map backgrounds look. They are not specific to any actual network.

Notes:

- Map background files must be gif, jpeg, jpg, or PNG format.
- For best fit and resolution files should be 1600 X 1024 at 72 DPI.
- Background files are stored in \Documents and Settings\{*user_name*}\My Documents\My Pictures\Network Topology Mapper Backgrounds.

To import and apply a new map background file or apply an existing background:

1. Click **Edit > Background picture import…**.
2. Navigate to your background map, and then click **Open**.

To remove a background from a map click **Edit > Remove background**.

Exporting Maps

You can export maps as Visio, PNG, Network Atlas (SolarWinds Orion), PDF, or map (native NTM) files. When exporting to Network Atlas or NTM formats you will be prompted for a map password. Enter any password as an encryption key for that export.

Note:

NTM 2.1.1 exported maps work in NPM 10.6 but not 10.4.2.

In exporting from NTM, keep in mind that:

- NTM exports data on nodes, interfaces, edges, and map styles and general map-making information.
- NTM does not export credentials; accessing the exported data depends on credentials selected in Orion Platform.
- An NTM multiple connection (that hides two or more edge connections) is displayed in Network Atlas as separate edge connections.
- NTM "unidentified" objects are dispaled as "unknown" in Network Atlas.
- Network Atlas maps do not show differences between L2 and L3 connections between nodes.

In exporting maps from Network Atlas, keep in mind that:

- Only Network Atlas "node" objects are exported.
- Only Network Atlas edges are exported; labels and custom objects are not exported.

Integration with Network Performance Manager

When you have NTM integrated with NPM, NTM allows you to export map data into Network Atlas. After you do this, if you update the scan for the NTM map, then NTM automatically updates the data you exported to Network Atlas.

To: Export an NTM Map into Network Atlas:

1. Create a map in Network Topology Mapper.

   See Discovering Devices and Topologies for details on discovery and map creation.

If you intend to keep your Network Atlas version of the NTM map updated, you must enable the setting **Keep Network Atlas updated with these discovery results** as described in Scheduling a Discovery

2. Click **File > Export > Network Atlas**.
3. Choose **Export as a map** or **Open directly in Network Atlas**.
4. In saving the exported file, set a password as needed.
5. Open Network Atlas, and then open the exported map, providing the file password as needed.
6. ***If you want to discover nodes and add them into the Orion platform database***, select 'Yes'.
7. ***If you do not want to discover nodes***, select 'No'.
8. Customize the map as needed. For example, change the default graphics, text formatting, or map layout.
9. Name the imported map and click **OK** to save it.
10. Open Network Performance Monitor.
11. Click **Edit** on the Network Map resource.
12. Select the imported map from the list and click **Submit**.

To export a map from NA to NTM:

1. Create a map in Network Atlas.
2. Click **Atlas > Export > Export to NTM**.
3. Save the map and set a password on the file as needed.

Working with Icons and Labels

SolarWinds NTM version 2.2 represents devices on maps with these icons:

- EnergyWise Device

- Firewall

- Hyper-V Guest

- Hyper-V Host

- ICMP Node

- L3/L2 Switch

- Network Segment Node

- Printer

- Router

- Router Wireless AP

- EnergyWise Device

- Switch

- VMWare Datacenter

- VMWare Guest

- VMWare Host

- VOIP Phone

- Wireless AP

- Wireless Controller

- WMI Node

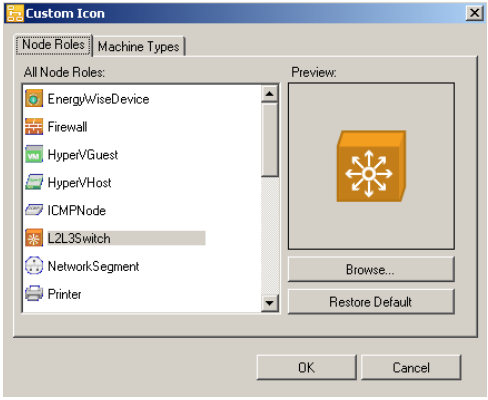
- Shadow Node

- SNMP Node

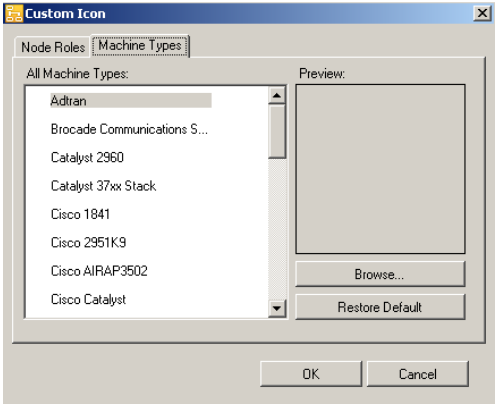
Additionally, you can use custom icons on your computer to represent any node.

To adjust the icon for a node:

1. Right-click a node and select **Custom Icon**.



2. Select the relevant Node Role.
3. ***If you want to use a custom icon for the node role***, click Browse and locate the desired image file on your computer.
4. Click the Machine Types tab.



5. ***If you want to use a custom icon for the machine type***, click Browse and locate the desired image file on your computer.
6. Click **OK**.
7. To resize the icon, right-click, select **Icon Size > Small/Medium/Large/Default**.

To adjust the label for a node:

Click the label and drag to relocate. Alternately, right-click the label, select **Place Text** and the desired option.

Running External Diagnostic Tools on Map Nodes

To help you diagnose problems with your network, you can run external tools on any of the nodes visible in your map.

Run Windows Ping, Remote Desktop, Telnet, or TraceRoute

1. Right-click any node.
2. Select **Integration with Windows Tools**.

You can run:

- Remote Desktop
- Traceroute
- Ping
- Telnet

Run SolarWinds Engineer's Toolset Tools

1. Right-click any node.
2. Select **Integration with Engineer's Toolset**.

If you have SolarWinds Engineer's Toolset v10.9 or later installed, you can run:

- Traceroute
- Enhanced Ping
- Lookup IP Address
- Lookup Hostname
- CPU Gauge
- Switchport Mapper

Running Custom Tools

If you want to run some other utility on the node, you can create a Custom Tool. A custom tool can run your utility and pass the node's IP address, hostname, or SNMPv2 community string as parameters.

The available parameters are ${IP}, ${HOSTNAME}, ${COMMUNITY}. Placing any of these strings into your command line passes the appropriate parameter to the utility.

Example: DameWare Mini Remote Control (MRC)

Let us set up a custom tool to establish DameWare remote control of a node on your NTM map. Assuming you already have the DameWare utility installed on your NTM server, here is how we create the appropriate custom tool.

1. Right-click any node and then select **Integration with Custom Tools > Add Custom Tools**.
2. Add a custom tool defined as follows:

   Name: **DameWare MRC**

   Executable Path: **C:\Program Files\SolarWinds\DameWare Mini Remote Control 10.0\DWRCC.exe (**by default)

   Command line arguments:

   dwrcc.exe -c: m:${IP} -u:myUsername -p:"my Password”
3. To use DameWare Mini Remote Control, right-click any node on the map and then select **Integration with Custom Tools > DameWare MRC**

For more information on DameWare command line parameters see http://support.dameware.com/kb/article.aspx?ID=300002

Example: DameWare Remote Control (DRS)

Let us set up a custom tool to establish DameWare remote control of a node on your NTM map. Assuming you already have the DameWare utility installed on your NTM server, here is how we create the appropriate custom tool.

1. Right-click any node and then select **Integration with Custom Tools > Add Custom Tools**.
2. Add a custom tool defined as follows:

   Name: **DameWare DRS**

   Executable Path: **C:\Program Files\SolarWinds\DameWare Remote Support 10.0\ (**by default)

   Command line arguments:

   None
3. To use DameWare Mini Remote Control, right-click any node on the map and then select **Integration with Custom Tools > DameWare DRS**

Example: OpenSSH

Let us set up a custom tool to establish an SSH connection to a node using the third-party utility OpenSSH. The usage of SSH is typically **ssh.exe user@remotehost**. Here is how we create that.

1. Right-click any node and then select **Integration with Custom Tools > Add Custom Tools**.
2. Add a custom tool defined as follows:
   Name: **SSH**
   Executable Path: **C:\Program Files (x86)\OpenSSH\bin\ssh.exe**
   Command line arguments: **Administrator@${IP}**

Now when you want to SSH to a node, you:

- Right-click any node and then select **Integration with Custom Tools > SSH**.

Using Custom Properties

Custom properties allow you to assign custom values to nodes. Once you have assigned these values, they can be displayed on the map and in reports. For example, you may want to indicate if nodes are leased or owned. To accomplish this you can add a Yes/No custom property called Leased, and select which nodes to which you want to apply this property.

Custom Property formats are:

- Text
- Number (Integers)
- Decimal
- Yes/No (true/false)
- Date/Time

To add a new Custom Property:

1. Click **Edit > Custom Property Manager…**.
2. Double -click the **Property Name** field. Enter a descriptive name for you custom property.
3. Select a **Format**.
4. Click the **Edit values** tab.
5. Select the check box to mark **Yes/No** properties as Yes (true).

6. Double-click the custom property field next to the node IP for a node you want to assign text, number, decimal, or date properties.
7. When you have finished assigning the property to nodes, click **OK**.

To display custom properties, click **Node Display Options > Custom Properties**.

To edit custom properties click **Custom Property Manager…** and select the property you want to edit.

Map Reports

NTM offers the following reports:

- Inventory
- Known Connections
- Switch Ports
- VLANs (includes VLAN IP Address)
- STP
- ARP Cache
- Subnets
- Scheduled Discoveries

To run a report click **Reports >New Report**, and then select the report you want to run.

Use the **Search** tool to find specific string patterns among the report data.

To remove columns from a report click **Options >Display Columns**, and click the column you want to remove from the report.

To sort on any column, click the column header.

To apply the node display options used on the map, click **Options > Apply map filters**.

Using NTM for an Ad Hoc Compliance Report

You may need to produce a report for specific compliance audits. In such cases, you could schedule a scan of your network for the audit date, providing you with a current snapshot.

For example, to demonstrate for auditors that your network complies with PCI DSS, you would schedule a scan and then, based on the results, print an inventory report (Reports > New Report > Inventory Report).

Accessing Support Tools

Support tools (**Help > Support Tools**) currently include these utilities:

- **Log Adjuster**

  Log adjuster allows you to change the level of event logging for NTM. This may be required if you are troubleshooting an issue with SolarWinds Technical Support. Do not change the settings in this tool unless you are requested to do so by Technical Support.

- **Create Tech diagnostic file**

  The diagnostics tool creates files for SolarWinds Technical Support. This may be required if you are troubleshooting an issue with SolarWinds Technical Support. Do not use this tool unless you are requested to do so by Technical Support.

- **Grab SNMPWalk**

  The SNMPWalk tool begins with the specified Root OID and queries the device for each OID in sequence, displaying its current value.

- **Discovery Log Utility**

  Discovery Log records devices for which SNMP information could not be retrieved during a discovery.

Appendix A

Network Discovery Options

The following sections detail:

- General Discovery Options
- Network Selection Discovery Options

General Discovery Options

The following topics are detailed in this section:

- About SNMP
- About Subnets
- What are Hops?
- What are VMware Credentials?
- What Permissions are required for VMware queries?
- Ignoring ICMP Only Nodes
- When not to use Bridge Tables
- Map Encryption
- Setting an initial encryption password
- Changing the encryption password

About SNMP

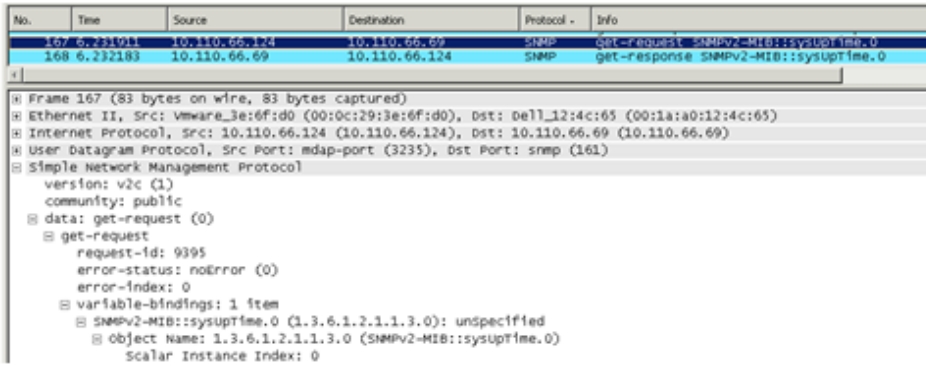
NTM uses Simple Network Management Protocol (SNMP) to retrieve information about device interfaces, ARP cache, CDP data, and a variety of other statistics. SNMP queries (polls) devices for specific information, and NTM acts as an SNMP manager, polling SNMP agents installed on managed devices. The following requirement must be met for NTM to successfully poll devices:

- The device must have SNMP enabled. To enable SNMP on your devices, see the manufacturer's documentation for the device.
- The device and NTM must share the same SNMPv2c community strings or SNMPv3 security access.
- SNMP (UDP port 161) must not be blocked between the device and NTM.

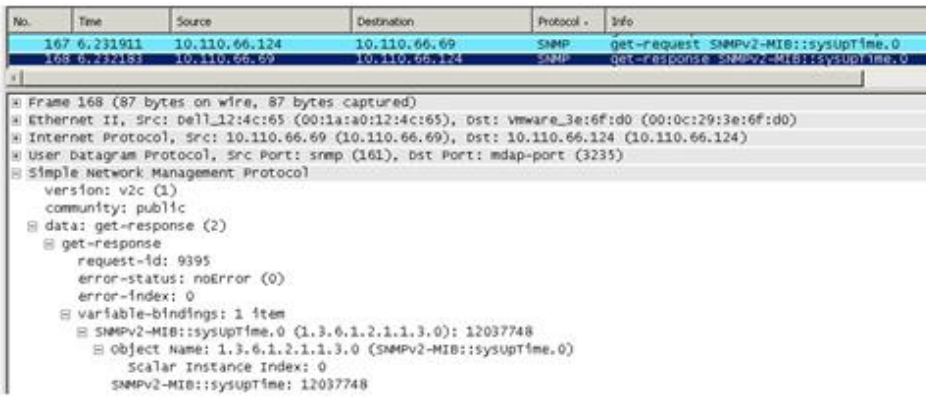
If your device fails to respond to SNMP complete the following troubleshooting steps:

- Check the device NTM credentials (SNMPv2c community string or SNMPv3 credentials) and ensure they are the same as the credentials used in NTM.
- Run a test from the NTM Add Credential interface before running discovery.
- Use a third party protocol analyzer to capture packets between NTM and the node to evaluate the issue.

The screen captures below show a successful NTM query.



SNMP Get Request



SNMP Get Response

About Subnets

An IP subnet is a logical division of a network into one or more smaller networks. This is accomplished by borrowing some of the host IP address space in a network and allocating a portion of that space to a subnet address. For example, the IP network 10.0.0.0 has 2^{24} host IP addresses. By specifying some of the host bits as subnet bits and assigning a subnet address the 10.0.0.0 network can contain a 10.1.1.0 subnet with 2^{8} host addresses. A subnet mask is used to specify which part of the host bits are used to identify a subnet.

The sub-netting of the 10.0.0.0 network to the 10.1.1.0 subnet is accomplished by adding the subnet mask shown below.

Subnet = 10.1.1.0

Subnet mask = 255.255.255.0

This subnet mask indicates that the first three octets of the IP address specify the subnet and only the last octet specifies host addresses. The range of usable hosts is 10.110.1.0 to 10.110.1.254 (with .0 host allowed).

Large Subnets and Discovery

An address range that include more than 2000 nodes takes much longer (one to two hours, for example) to discover than the same number of nodes split up into multiple smaller ranges. Additionally, with so many nodes on a map, the user interface and NTM operations may run with noticeable lag.

For example, if you are subnetting with the mask of 255.255.248.0, then the maximum number of nodes within the subnet will be 8 X 255 = 2040. In discovery nodes, the software engine creates a lookup table in memory that includes as many rows as nodes in the defined IP range or subnet. The more rows the more time the engine must spend in finding its point of reference in the table as it iterates through the array of items. Walking a larger lookup table takes significantly more time than walking smaller tables that cumulatively contain the same number of arrayed items. So the time it takes the engine to complete its discovery task directly depends on the number of possible nodes in the specified range or subnet.

What are Hops?

Hops specify the number of devices that must be transverse to reach a target IP device. A zero hops discovery discovers all devices responding to the discovery protocols on the specified subnet or seed device, as well as any networks and subnets directly connected to devices on the target subnet. We recommend using a zero hop discovery.

A one hop discovery discovers all of the devices specified in the above zero hop discovery and all networks, subnets, and devices directly connected to all devices on the edge of the zero hops discovery.

Depending on the complexity of your network, discovering past zero hops has the potential to discover several times the number of subnets and hundreds of times the number of total devices. Discovering two hops or more has the potential of discovering thousands of subnets and devices.

Any discovery using more than zero hops may have a large impact on discovery performance.

Windows Credentials (WMI)

You must use a Windows administrator account to collect details about Microsoft Windows servers. We use a technology called WMI to retrieve this information and this information is only available if we can provide administrator credentials.

Information we can retrieve for Microsoft Windows servers using WMI includes:

- IP Address
- Node name
- MS Software (Machine Type)
- System Description
- System Location
- Contact

Note: All of the above except Machine Type are discovered in SNMP discovery as well.

What are VMware Credentials?

NTM uses a VMware API to query data from VMware servers. The API requires a VMware account with at least read-only access to VMware. The data from the VMware API allows NTM to associate host VM servers and the guest virtual servers.

To gather complete information about the guest servers, ensure that the guest servers' IP addresses and VMware credentials are included in your discovery.

What Permissions are required for VMware queries?

To query VMs from NTM you must use an account that has Administrator access on the target VMware server.

Ignoring ICMP Only Nodes

If you select Ignore nodes that only respond to ICMP (ping) you will eliminate nodes that do not respond to SNMP or WMI. When ICMP only nodes are discovered NTM can only discover that some device is responding at the IP address. No node details or connectivity can be discovered for ICMP only nodes.

We recommend you select the ignore ICMP only nodes option.

When not to use Bridge Tables

Bridge tables are used by NTM to discover connections and calculate connectivity. Selecting **Don't use Bridge Table information to calculate network topology** eliminates the bridge table information from the connection calculations. Connectivity discovered using bridge table information may be less accurate then with Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP), however, it is still a valuable source of data. Additionally, eliminating bridge tables may decrease the time needed to calculate connectivity.

Bridge table information has a much greater impact on Orion Network Atlas maps; therefore, if you will be importing maps from NTM to Orion Network Atlas we recommend you do not use bridge table information.

Map Encryption

NTM offers encryption for NTM files and Orion Network Atlas files.

Setting an initial encryption password

The first time you start a network scan or open a map NTM prompts for a maps encryption password. This password is used for all your maps by default. Default maps encryption password can be changed at any time. You can change an encryption password for exported maps as well.

Changing the encryption password

To change the default map password:

1. Select **Edit -> Change maps Encryption Password.**
2. Enter the **Old Password**.
3. Enter the **New Password**.
4. Enter the New Password again in the **Confirm Password** field, and then click **Save**.

Network Selection Discovery Options

The NTM Discovery Wizard allows you to specify the range of IP addresses you want to discover. After IP nodes are discovered, you can select which ones you want to include on your map. The time it takes to complete a discovery scan relies heavily on the range of IP addresses you specify. The following provides guidelines and steps to create discovery ranges that will accurately discover the devices you want to map without including large number of other devices.

To better understand the network selection options you should consider the specificity of each option. Network selection discovery options are listed below in order from the most specific option to the most general option.

1. Specific Nodes. This option discovers only the nodes you specify by IP address.

2. IP Ranges. This option discovers only the nodes you specify by IP address range. The range can be any contiguous IP address block. Multiple ranges can be included to allow for discovery of non-contiguous ranges.

3. Subnets. This option discovers the specified subnet and all networks directly connected to devices on the specified subnet.

4. Seed Device. This option discovers all subnets that the specified device is aware of. By adding hop counts this option will discover devices several networks away.

Using Specific Nodes

This option is useful when you have an existing map and you want to add a specific node without having to discover a number of subnets or IP addresses.

Add specific nodes by their IPv4 address or IPv6 address. Add the node one per line.

Using Discovery IP Ranges

Discovery ranges allow you to specify contiguous IP address ranges for discovery. Node outside the specified range will not be discovered and the Hop Count discovery option is ignored for IP ranges.

For example a discovery using the range 10.110.1.1 to 10.110.3.255 defines a contiguous discovery range including all possible IP addresses between .110.1.1 and 10.110.3.255.

In contrast, a discovery including the starting address of 10.110.1.1 and the ending IP address of 10.110.2 255 along with an additional range of 10.110.3.1 to 10.110.3.255 will discover only those ranges and will not include the 10.110.2.0 subnet between them.

IPv6 ranges are supported.

Using Subnets

Subnet discovery scans all specified subnets and subnets directly attached to devices included in the subnet.

For example, consider a discovery for the 10.110.1.0 subnet with a subnet mask of 255.255.255.0. If the discovery finds a router on the 10.110.1.0 subnet that also has interfaces on 10.10.20.0 and 192.168 5 0 subnets, those subnets will also be scanned for devices and connectivity. Additional subnets connected to those devices on the new subnets are not scanned.

After discovering subnets, clear the checkbox next to a subnet to remove that subnet from your map.

IPv6 subnets are supported.

Using Seed Devices

You can use a seed device to discover subnets, connectivity and network devices throughout your network. A seed device must be a layer 3 switch or router. NTM will scan the connection to the indicated device and use that information to scan directly connected devices.

After discovering directly connected devices, NTM will discover devices on connected subnets to the extent you have indicated in the **Number of Hops** option.

IPv6 see device addresses are supported.

Note: Using a hop count greater than zero may greatly impact the time required to complete a scan.

Appendix B

FAQ

What does “Requests made” mean in discovery?

Request made represents the sum of the SNMP, WMI, VMware and ICMP requests sent by the NTM discovery engine to all of the nodes. This number will increment through the discovery process and will be several times larger than the number of nodes discovered.

Why does my map show unidentified devices or unknown device types connected to one of my routers or switches?

NTM can determine that an unknown device is connected to a specific interface on a fully discovered device using the IP address of the discovered device’s interfaces and the IP address of the unknown device.

Why are some unknown devices shown with no connectivity?

Devices that only respond to ICMP and cannot be determined to be directly connected to a known device can only be shown as unknown devices. Use the Ignore nodes that only respond to ICMP (ping) discovery option to discover only connected devices.

What database does NTM use?

NTM uses Microsoft SQL server Compact v3.5 SP2. This database is installed in \Program Files\Microsoft SQL Server during NTM installation. This database is not accessible from outside the system on which NTM is installed.

What does the log adjuster tool do?

Log adjuster allows you to change the level of event logging for NTM. This may be required if you are troubleshooting an issue with SolarWinds Technical Support. Do not change the settings in this tool unless you are requested to do so by Technical Support.

What does the Create Tech diagnostic file tool do?

The diagnostics tool creates files for SolarWinds Technical Support. This may be required if you are troubleshooting an issue with SolarWinds Technical Support. Do not use this tool unless you are requested to do so by Technical Support.

What does the Grab SNMPWalk tool do?

The SNMPWalk tool begins with the specified Root OID and queries the device for each OID in sequence, displaying its current value.

What does the Discovery Log Utility do?

For any node discovery the Discovery Log records devices for which SNMP information could not be retrieved.

How long does it take to complete a discovery?

The length of discovery depends on several factors including:

- The IP range or size of the network specified.
- The number and type of nodes discovered.
- The number of methods used in discovery (SNMP, ICMP, VMware API, WMI).
- The number of discovery hops allowed.
- The number of networks directly connected to discovered devices.

What can I do to speed up discovery?

Some options include:

- Eliminate any discovery methods that do not apply to the network.
- Use a specific IP Address Range rather than a seed device or a subnet.
- Use a zero hop count discovery.

What do the Spanning Tree State numbers mean?

- 1 = disabled
- 2 = listening
- 3 = learning
- 4 = blocking
- 5 = forwarding

Note: NTM supports only Common Spanning Tree (CST) data; IEEE 802.1Q.

Which map layout option should I use?

The layout options are available to make it easier for you to use maps in a format that you prefer. You can use the layout that makes the best fit for your network and any existing maps you have.