SolarWinds

Network Topology Mapper Administrator Guide

solarwinds

NETWORK TOPOLOGY MAPPER

SolarWinds Network Topology Mapper 6.10.14, version 2.1.1

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 1

Chapter 2

Chapter 3

Chapter 4

Appendix A

Appendix B

Chapter 1

Introduction

SolarWinds Network Topology Mapper (NTM) delivers detailed, scalable mapping that allows you to see and understand physical and logical connections between your network devices. Through scheduled mapping updates, NTM reflects near real-time changes in connections in intuitive map displays. You can also view device connections for an at-a-glance understanding of the complex connections involved.

NTM offers the following mapping and topology features:

- Layer 2 (port level) connectivity mapping
- Layer 3 (logical) connectivity mapping
- Multi-link mapping
- Switch and VLAN details
- VLAN details in connection rollover (HP/3Com and Juniper Switches)
- Detailed system information for discovered devices
- Customization of device and connection displays
- Mapping virtual servers to the host machine
- Subnet groupings
- Various types of reports

Benefits Of Network Topology Mapper

Consider the following benefits of SolarWinds Network Topology Mapper:

Scheduled Topology Discovery

Virtual Device Connectivity

Shareable and Printable Maps

View Switched and Routed Connectivity

Map Encryption

IPv6 Support

Scheduled Topology Discovery

NTM runs scheduled discoveries to detect new devices on your network and explains how they are connected to your other devices.

Virtual Device Connectivity

Without a visual representation, it is often difficult to understand how virtual devices interact with the network. NTM provides a clear picture of the connectivity of virtual devices to your physical network.

Shareable and Printable Maps

Exports maps in PDF, PNG, Visio, Orion Network Atlas, and native NTM formats. These maps can be imported into a variety of systems, including all SolarWinds products that use Network Atlas maps.

View Switched and Routed Connectivity

Discovers and views layer 2, switched connectivity and layer 3, routed connections in NTM. NTM allows the option to view each layer separately or combined in one map.

Map Encryption

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.

IPv6 Support

NTM fully supports IPv4 and IPv6 addresses.

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.

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 more information on Network Segment nodes, see “Understanding Network Segment Nodes”.

- 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 the "SolarWinds.NTM.BusinessLayer.dll.config" file (by default: \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 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, 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 NTM installer must be run using an account with 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 **SolarWindsNetworkTopologyMapper.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. Select whether or not to participate in sending anonymous program data to SolarWinds, and then click **OK**.
6. When the installation completes, click **Close**. NTM launches the Getting Started with Network Topology Mapper page.

Chapter 3

Discovering Devices and Topologies

The Network Discovery Scan Wizard allows you to quickly specify 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. The discovery wizard consists of four stages:

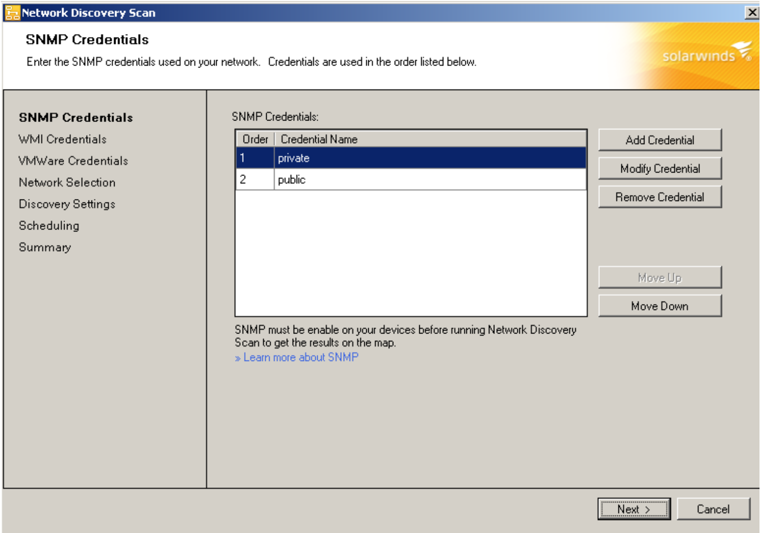
- Discovery Credentials
- Network Selection
- Discovery Settings
- Discovery Scheduling

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. From either the Getting Started with Network Topology Mapper screen or the main Network Topology Mapper screen, click **New Network Scan**.



SNMP Credentials

Enter the SNMP credentials used on your network. Credentials are used in the order listed below.

Order	Credential Name
1	private
2	public

SNMP must be enable on your devices before running Network Discovery Scan to get the results on the map.

» Learn more about SNMP

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.
3. ***If you use SNMP v1 or v2c***, complete the following steps:
   a. Click **Add Credential**.

   b. Enter a unique **Credential Name** or select an existing credential from the list. If you select a credential from the list, then the values for that credential are automatically filled in for the Community String; and you should go to step 4.

   c. ***If you are adding a new credential,*** enter the **Community String** the devices use for SNMP read-only access, and then click **Add**.

   d. ***If you use other read-only community strings***, add those strings by repeating steps a through c.

   e. When all of the community strings have been added, click **Next**.
4. ***If you use SNMP v3***, complete the following steps:
   a. Click **Add Credential**.

   b. Enter a unique **Credential Name** or select an existing credential from the list. If you select a credential from the list, then the values for that credential are automatically filled in User Name, Context, and Authentication Method, Password/Key; and you should go to step 5.

   c. Select **SNMPv3**.

- **d.** Enter the **SNMP v3 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.
- **e.** Enter the **Context**. For Cisco devices, this is defined in the `snmp-server group` configuration command.
- **f.** Select the **Authentication Method**. For Cisco devices, this is defined in the `snmp-server user` configuration command.
- **g.** Enter the password or key in the **Password/Key** field.
- **h.** ***If you have entered a key***, select **Password is a key**.
- **i.** Select the **Privacy/Encryption Method.** For Cisco devices, this is also defined in the `snmp-server user` configuration command.
- **j.** Enter the password or key in the **Password/Key** field.
- **k.** ***If you have entered a key***, select **Password is a key**.
- **l.** Click **Test** to test these credentials.
- **m.** ***If the test fails,*** review the device SNMP v3 configurations and ensure you are using the proper fields in NTM.
- **n.** When you have successfully tested your credentials, click **Add**.

5. Click **Add Credentials** to add WMI credentials.

   Note: 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.

   - **a.** Enter a unique **Credential Name** or select an existing credential from the list. If you select a credential from the list, then the values for that credential are automatically filled in for WMI User Name and Password; and you should go to step 6.
   - **b.** Enter the **WMI User Name**, re-enter the password in the **Confirm Password** field, and then click **Test**.
   - **c.** Once the test is successful, click **Add**.
   - **d.** ***If you use other WMI credentials***, add those by repeating steps a through c.
   - **e.** When all of the WMI credentials have been added, click **Next**.
6. Click **Add Credentials** to add VMware credentials.

Note: 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.

a. Enter a unique **Credential Name** or select an existing credential from the list. If you select a credential from the list, then the values for that credential are automatically filled in for the Vmware User Name and Password; and you should click **Next**.

b. Enter the **VMware User Name**, re-enter the password in the **Confirm Password** field, and then click **Test**.

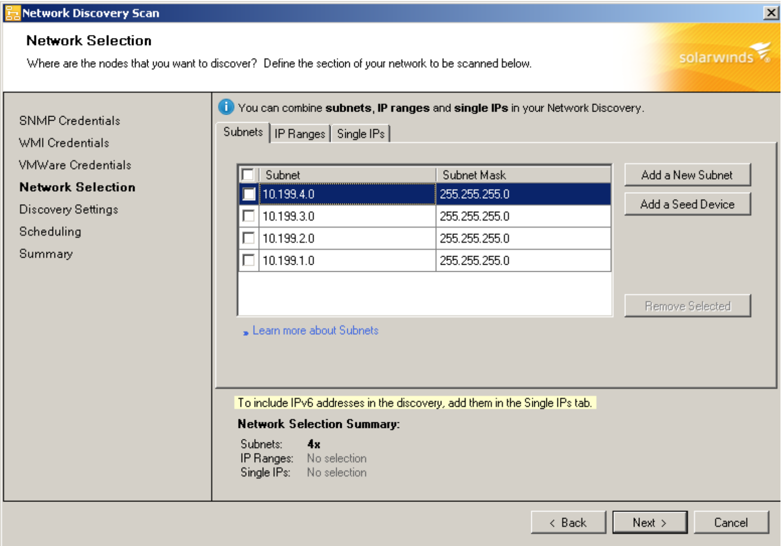
c. Once the test is successful, click **Add**.

d. ***If you use other VMware credentials***, add those by repeating steps **a** through **c**.

e. When all of the VMware credentials have been added, click **Next.**

Network Selection

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 range of IP addresses you want to discover. You can combine any of the options to better define your discovery range.



Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

You can combine **subnets**, **IP ranges** and **single IPs** in your Network Discovery.

☐	Subnet	Subnet Mask
☐	10.199.4.0	255.255.255.0
☐	10.199.3.0	255.255.255.0
☐	10.199.2.0	255.255.255.0
☐	10.199.1.0	255.255.255.0

To include IPv6 addresses in the discovery, add them in the Single IPs tab.

Network Selection Summary:

Subnets: **4x**
IP Ranges: No selection
Single IPs: No selection

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

Specific IP Addresses

Use these steps to discover specific IP addresses.

To discover specific IP addresses:

1. Click the **Specific Nodes** tab.
2. Enter IPv4 or IPv6 addresses, one per line.
3. ***If you only want to discover these nodes,*** click **Next**.
4. ***If you want to specify other devices by IP address ranges or subnets,*** click **IP Ranges** or **Subnets**.

IP Address Range

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 as described in step 2.
4. ***If you have finished specifying discovery nodes and ranges,*** click **Next**.
5. ***If you want to specify other devices by subnets or by a seed device,*** click the **Subnets** tab.

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.

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 have finished specifying your discovery nodes, ranges, subnets, and seed devices,*** click **Next**.

Discovery Settings

1. Enter a **Map 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**.

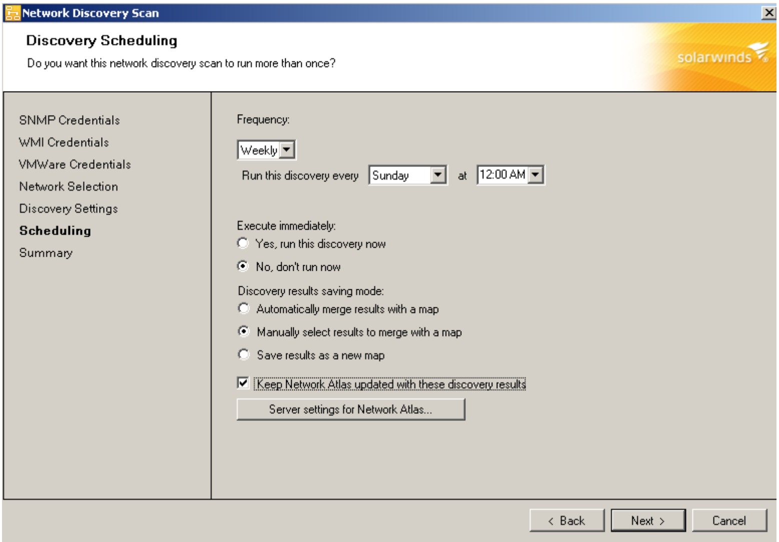
   Note: For more information on this option, see General Discovery Options.

5. Click **Next**.

Discovery Scheduling

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.



Discovery Scheduling

Do you want this network discovery scan to run more than once?

Frequency: Weekly

Run this discovery every Sunday at 12:00 AM

Execute immediately:

○ Yes, run this discovery now

● No, don't run now

Discovery results saving mode:

○ Automatically merge results with a map

● Manually select results to merge with a map

○ Save results as a new map

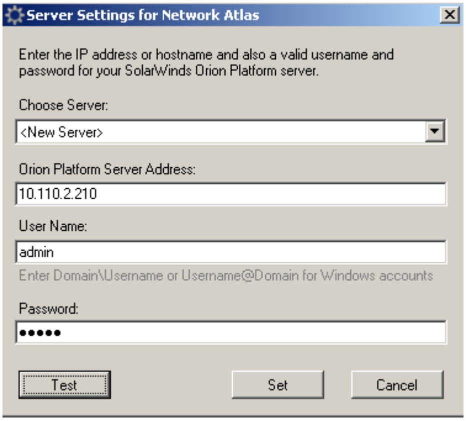
☑ Keep Network Atlas updated with these discovery results

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. Select **automatically merge results with map** if you want the results to appear on the map created with the first iteration of the scheduled scan.
   b. Select **manually select results to merge with map** if you want to review scan results and opt to include in the existing map or exclude from it particular results.
   c. Select **save results on a new map** if you want to leave the previous iteration of your map untouched.
5. If you have Network Performance Manager and you intend to export your map data to Network Atlas, then select **Keep Network Atlas updated with these discovery results**.


Server Settings for Network Atlas

Enter the IP address or hostname and also a valid username and password for your SolarWinds Orion Platform server.

Choose Server: <New Server>

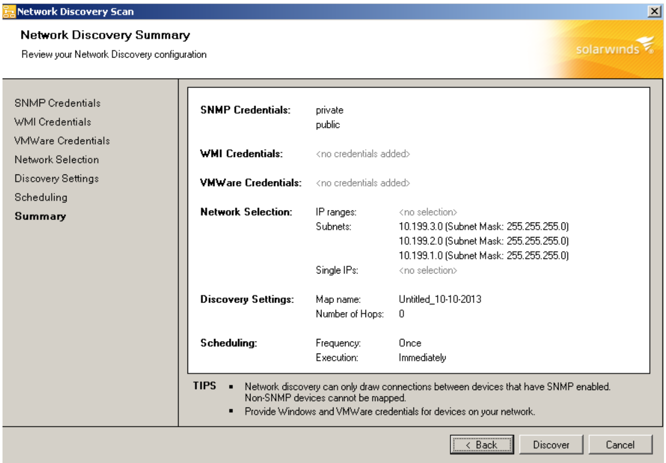
Orion Platform Server Address: 10.110.2.210

User Name: admin

Enter Domain\Username or Username@Domain for Windows accounts

Password: ●●●●●

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


Network Discovery Scan

Network Discovery Summary

Review your Network Discovery configuration

SNMP Credentials: private
public

WMI Credentials: <no credentials added>

VMWare Credentials: <no credentials added>

Network Selection:
IP ranges: <no selection>
Subnets: 10.199.3.0 (Subnet Mask: 255.255.255.0)
10.199.2.0 (Subnet Mask: 255.255.255.0)
10.199.1.0 (Subnet Mask: 255.255.255.0)
Single IPs: <no selection>

Discovery Settings:
Map name: Untitled_10-10-2013
Number of Hops: 0

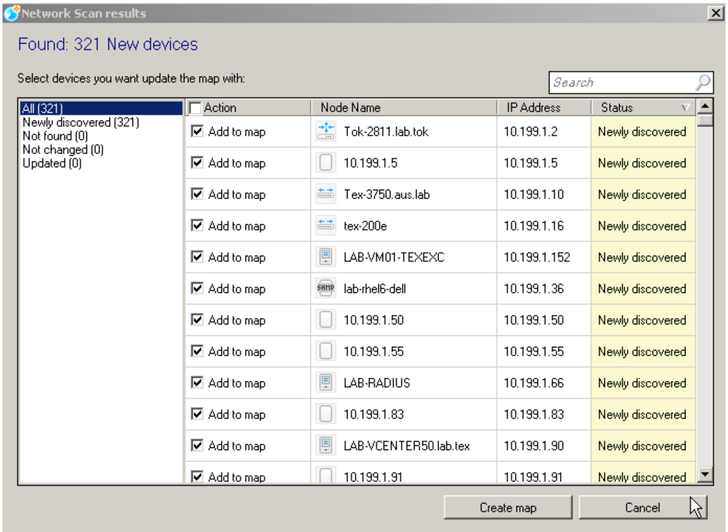
Scheduling:
Frequency: Once
Execution: Immediately

TIPS
- Network discovery can only draw connections between devices that have SNMP enabled. Non-SNMP devices cannot be mapped.
- Provide Windows and VMWare credentials for devices on your network.

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).

Discovery Results

When discovery completes, NTM presents the results.



Found: 321 New devices

Select devices you want update the map with:

- All (321)
- Newly discovered (321)
- Not found (0)
- Not changed (0)
- Updated (0)

☐ Action	Node Name	IP Address	Status
☑ Add to map	Tok-2811.lab.tok	10.199.1.2	Newly discovered
☑ Add to map	10.199.1.5	10.199.1.5	Newly discovered
☑ Add to map	Tex-3750.aus.lab	10.199.1.10	Newly discovered
☑ Add to map	tex-200e	10.199.1.16	Newly discovered
☑ Add to map	LAB-VM01-TEXEXC	10.199.1.152	Newly discovered
☑ Add to map	lab-rhel6-dell	10.199.1.36	Newly discovered
☑ Add to map	10.199.1.50	10.199.1.50	Newly discovered
☑ Add to map	10.199.1.55	10.199.1.55	Newly discovered
☑ Add to map	LAB-RADIUS	10.199.1.66	Newly discovered
☑ Add to map	10.199.1.83	10.199.1.83	Newly discovered
☑ Add to map	LAB-VCENTER50.lab.tex	10.199.1.90	Newly discovered
☑ Add to map	10.199.1.91	10.199.1.91	Newly discovered

When the scan finishes the **Network Scan results** window displays. All discovered devices are listed with one of three possible status indicators:

Newly Discovered. These devices were not discovered in the previous scan. To eliminate any of these nodes from being mapped, clear the **Add to map** check box.

Not found. These are devices that were detected in a previous scan that do not respond to this scan. To retain any of these nodes on the new map, clear the **Remove from map** check box.

Unchanged. These devices have not changed status from the previous scan.

Updated. The devices include new information.

By default, NTM selects all discovered devices to add into the map.

Click **Create map** to add all discovered devices. Otherwise, deselect any devices you do not want added to the map, and then click **Create map**.

NTM creates a map using the option selected. Depending on the number of devices and connectivity complexity, rendering the map may take several minutes.

Rescanning an Existing Map

NTM allows you to rescan (rediscover) an existing map on demand or by using a scheduled discovery update.

Note: 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 "Understanding Network Segment Nodes".

To rescan an existing map:

1. Open the map from the **File** menu.
2. Click **Rescan this Network** on the toolbar.
3. Click **Edit Map Properties.**
4. Enter any changes in the credentials and network selection.
5. Click **Scan**.

   When the scan finishes the **Network Scan results** window displays. All discovered devices are listed with one of three possible status indicators:

Newly Discovered. These devices were not discovered in the previous scan. To eliminate any of these nodes from being mapped, clear the **Add to map** check box.

Not found. These are devices that were detected in a previous scan that do not respond to this scan. To retain any of these nodes on the new map, clear the **Remove from map** check box.

Unchanged. These devices have not changed status from the previous scan.

Updated. The devices include new information.

6. ***If you want to add discovered devices to the map***, select All, verify that Add to map is selected, and **Create map**.

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:

- Understanding
- Using Map Navigator
- Additional Navigation Options
- Filtering Nodes and Searching Maps
- Using the Network Tree View
- Viewing Connection Information
- Viewing and Editing Nodes and Node Details
- Using Map Layouts

Understanding Network Segment Nodes

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

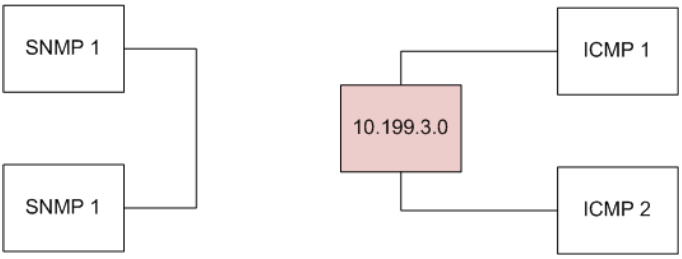
NTM generates Network Segment nodes based on the three types of connection information that it collects and builds:

- 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:

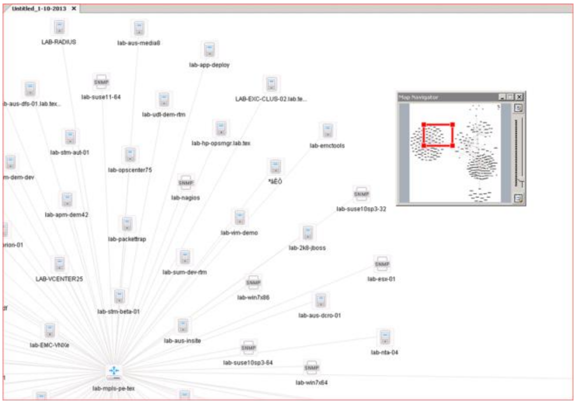


Node 10.199.3.0 is a Network Segment node that indicates the subnet in which the two discoved ICMP nodes are connected.

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



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.

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

Additional Navigation Options

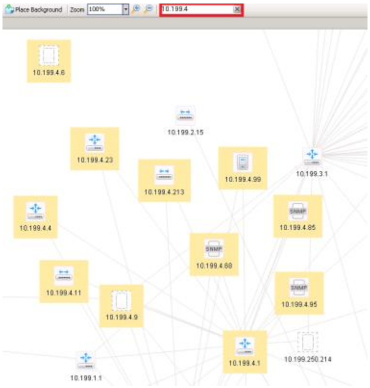
You can navigate the map using Move Map, Zoom list, and windows controls. Move Map and Zoom are on the map top menu bar. To zoom using windows controls, press and hold the control key and use the mouse scroll wheel.

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.

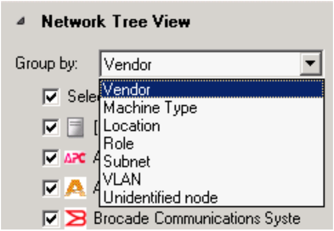
For example, to filter using IP addresses:

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 a specific subnet where the found items are highlighted in yellow.



Using the Network Tree View

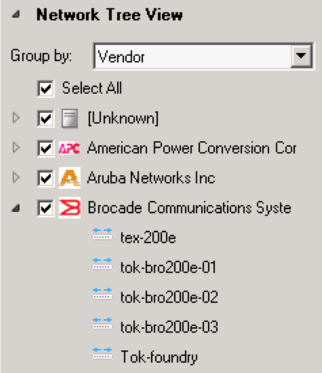
To access this view, click Network Tree View in the left options menu.



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

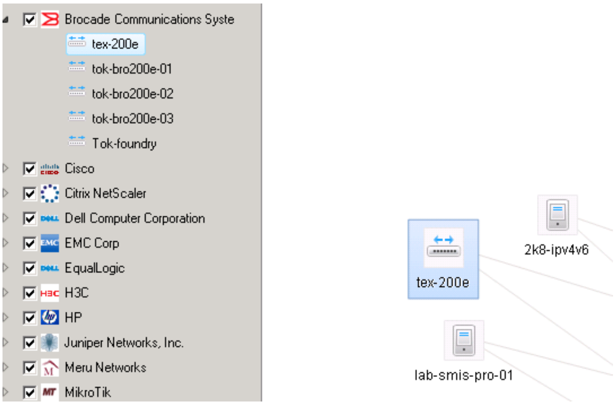
- **Vendor**: The vendor information listed in SNMP MIB2:sysDiscr.
- **Machine Type**: Make and model listed in SNMP MIB2:sysInfo.
- **Location**: Location listed in SNMP MIB2:sysLocation.
- **Role**: The network service provided, such as router, switch, server, or wireless controller.
- **Subnet**: 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.



Group by: Vendor

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

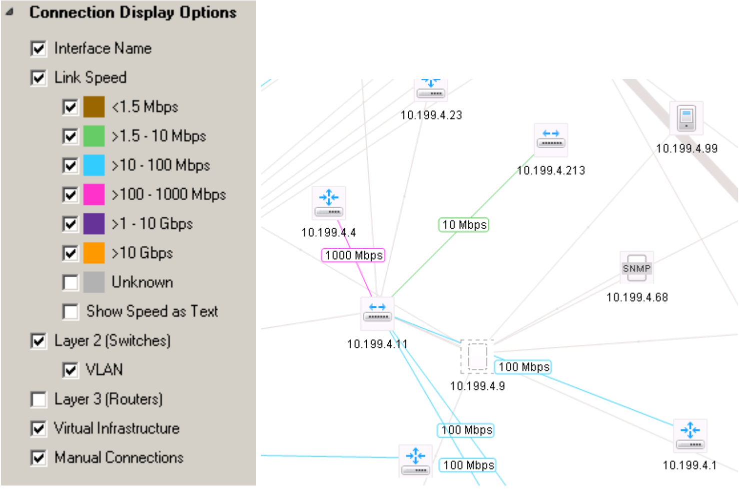


Double-click the node name to center the map around a node.

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**.



Connection Display Options

- ☑ Interface Name
- ☑ Link Speed
  - ☑ 🟫 <1.5 Mbps
  - ☑ 🟩 >1.5 - 10 Mbps
  - ☑ 🟦 >10 - 100 Mbps
  - ☑ 🟥 >100 - 1000 Mbps
  - ☑ 🟪 >1 - 10 Gbps
  - ☑ 🟧 >10 Gbps
  - ☐ ⬜ Unknown
  - ☐ Show Speed as Text
- ☑ Layer 2 (Switches)
  - ☑ VLAN
- ☐ Layer 3 (Routers)
- ☑ Virtual Infrastructure
- ☑ Manual Connections

Note: 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.

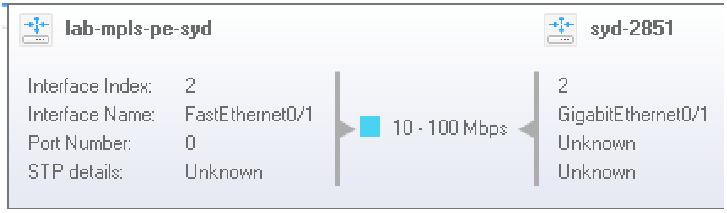
When a connection has information from both layers 2 and 3, the connection only displays layer 2 information. To switch to layer 3 information, clear the **Layer 2 (Switches)** check box in **Connection Display Options** and select **Layer 3**.

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.

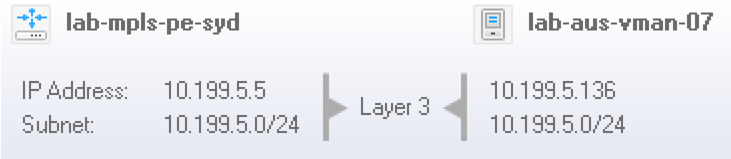
To display custom connections in your map select that option in **Connection Display Options**.

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



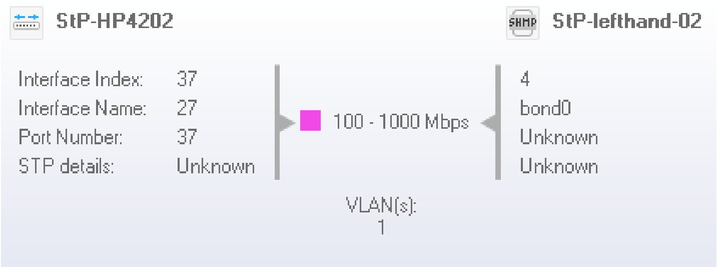
	lab-mpls-pe-syd		syd-2851
Interface Index:	2	🟦 10 - 100 Mbps	2
Interface Name:	FastEthernet0/1		GigabitEthernet0/1
Port Number:	0		Unknown
STP details:	Unknown		Unknown

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



	lab-mpls-pe-syd		lab-aus-vman-07
IP Address:	10.199.5.5	Layer 3	10.199.5.136
Subnet:	10.199.5.0/24		10.199.5.0/24

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.

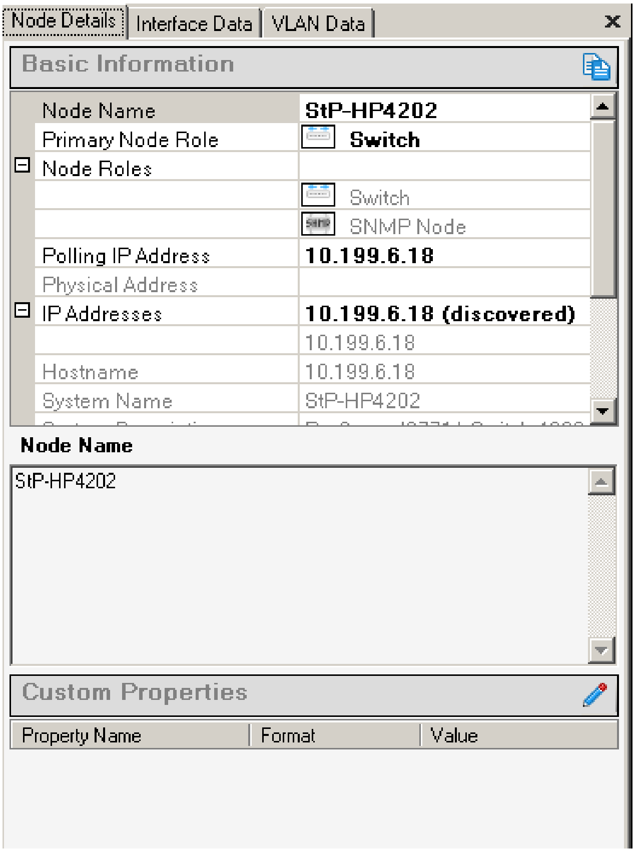


	StP-HP4202		StP-lefthand-02
Interface Index:	37	■ 100 - 1000 Mbps	4
Interface Name:	27		bond0
Port Number:	37		Unknown
STP details:	Unknown		Unknown

VLAN(s):
1

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**.



Basic Information

Node Name	**StP-HP4202**
Primary Node Role	**Switch**
Node Roles	
	Switch
	SNMP Node
Polling IP Address	**10.199.6.18**
Physical Address	
IP Addresses	**10.199.6.18 (discovered)**
	10.199.6.18
Hostname	10.199.6.18
System Name	StP-HP4202

Node Name

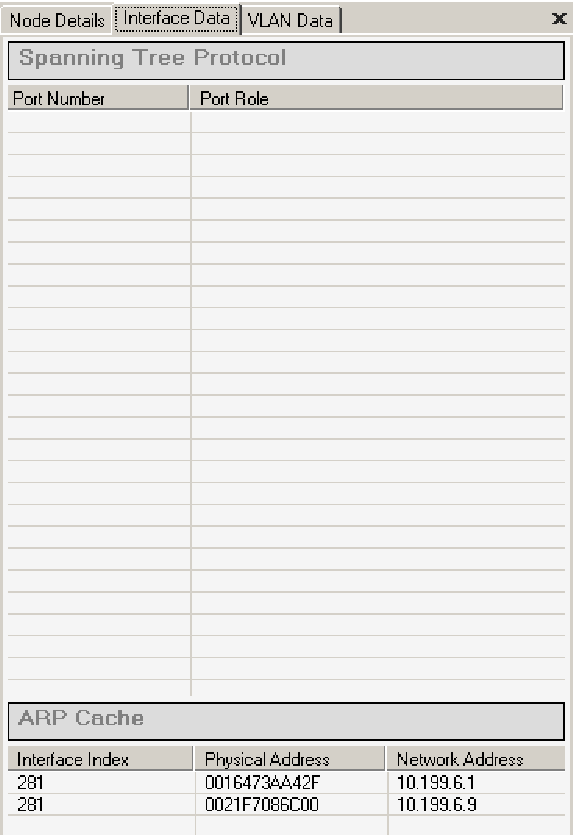
StP-HP4202

Custom Properties

Property Name	Format	Value

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, Location, Contact, and Polling Method.

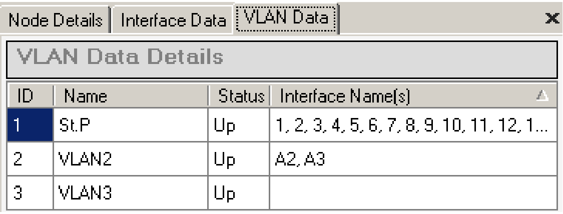
You can review the node’s Interface Data, including the ARP cache related to MAC/IP Address matchings.



Port Number	Port Role

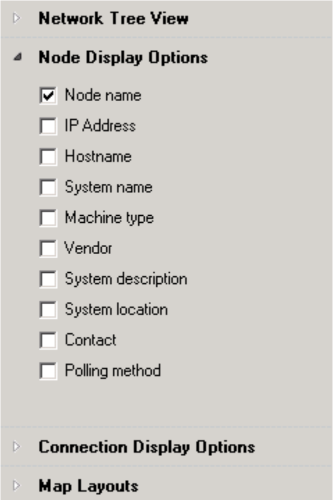
Interface Index	Physical Address	Network Address
281	0016473AA42F	10.199.6.1
281	0021F7086C00	10.199.6.9

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



ID	Name	Status	Interface Name(s)
1	St.P	Up	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 1...
2	VLAN2	Up	A2, A3
3	VLAN3	Up	

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.



Network Tree View

Node Display Options

- ☑ Node name
- ☐ IP Address
- ☐ Hostname
- ☐ System name
- ☐ Machine type
- ☐ Vendor
- ☐ System description
- ☐ System location
- ☐ Contact
- ☐ Polling method

Connection Display Options

Map Layouts

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.

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**.

Export, Import and File Options

The following sections include information on exporting and importing maps and related file options.

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 Discovery Scheduling
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.

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**.

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:

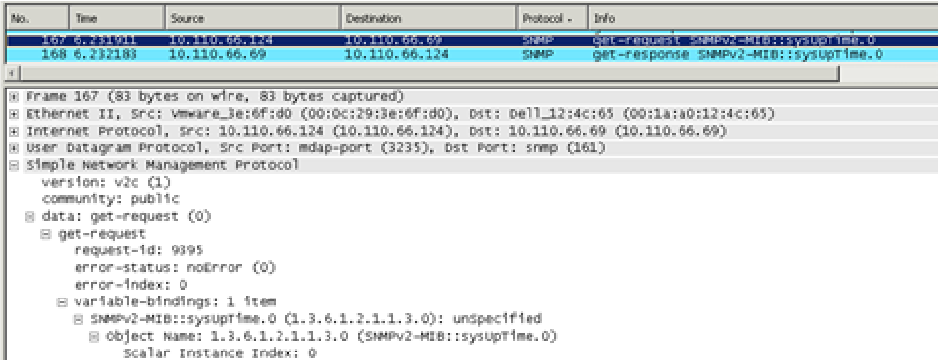
- The device must have SNMP enabled. To enable SNMP on your devices, see the manufacturer's documentation for the device.

- 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.

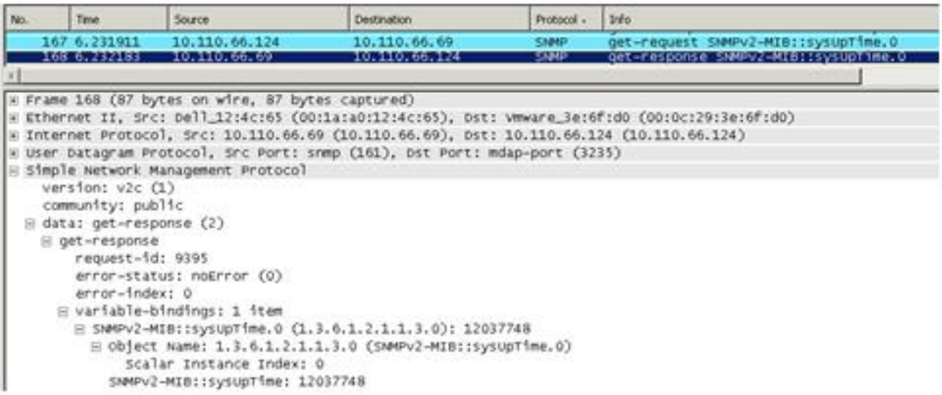
The screen captures below show a successful NTM query.



No.	Time	Source	Destination	Protocol	Info
167	6.231911	10.110.66.124	10.110.66.69	SNMP	get-request SNMPv2-MIB::sysUpTime.0
168	6.232183	10.110.66.69	10.110.66.124	SNMP	get-response SNMPv2-MIB::sysUpTime.0

```
⊞ Frame 167 (83 bytes on wire, 83 bytes captured)
⊞ Ethernet II, Src: Vmware_3e:6f:d0 (00:0c:29:3e:6f:d0), Dst: Dell_12:4c:65 (00:1a:a0:12:4c:65)
⊞ Internet Protocol, Src: 10.110.66.124 (10.110.66.124), Dst: 10.110.66.69 (10.110.66.69)
⊞ User Datagram Protocol, Src Port: mdap-port (3235), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    version: v2c (1)
    community: public
  ⊟ data: get-request (0)
    ⊟ get-request
        request-id: 9395
        error-status: noError (0)
        error-index: 0
      ⊟ variable-bindings: 1 item
        ⊟ SNMPv2-MIB::sysUpTime.0 (1.3.6.1.2.1.1.3.0): unspecified
          ⊟ Object Name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
              Scalar Instance Index: 0
```

SNMP Get Request



```
No.   Time        Source         Destination    Protocol  Info
  167 6.231911    10.110.66.124  10.110.66.69   SNMP      get-request SNMPv2-MIB::sysUpTime.0
  168 6.232183    10.110.66.69   10.110.66.124  SNMP      get-response SNMPv2-MIB::sysUpTime.0

⊞ Frame 168 (87 bytes on wire, 87 bytes captured)
⊞ Ethernet II, Src: Dell_12:4c:65 (00:1a:a0:12:4c:65), Dst: Vmware_3e:6f:d0 (00:0c:29:3e:6f:d0)
⊞ Internet Protocol, Src: 10.110.66.69 (10.110.66.69), Dst: 10.110.66.124 (10.110.66.124)
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: mdap-port (3235)
⊟ Simple Network Management Protocol
    version: v2c (1)
    community: public
  ⊟ data: get-response (2)
    ⊟ get-response
        request-id: 9395
        error-status: noError (0)
        error-index: 0
      ⊟ variable-bindings: 1 item
        ⊟ SNMPv2-MIB::sysUpTime.0 (1.3.6.1.2.1.1.3.0): 12037748
          ⊟ Object Name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
              Scalar Instance Index: 0
            SNMPv2-MIB::sysUpTime: 12037748
```

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.

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.