SOLARWINDS TECH TIPS

How to Simplify Network Discovery using SolarWinds® Engineer's Toolset

Share:

solarwinds Unexpected Simplicity™

Creating an effective network monitoring framework is highly reliant on the tools you use to do the job. One common denominator while monitoring your devices is that you should have a robust network discovery mechanism. By discovering all the devices in a network, as well as the resources connected to them, network administrators can gather useful information like status of each device, machine type, location, and more. It gives them a glimpse of what devices they will monitor and the resources connected to it

Attempting network discovery manually can be very cumbersome and time consuming—especially in environments that are growing and changing. Manually adding each device is impractical. There are, however, third-party tools that make this process much easier. Many of these tools provide scheduled periodic network scanning that sends notifications whenever new devices are added to the network. One such tool that provides this type of automatic device discovery is SolarWinds Engineer's Toolset.

How to Make Network Discovery Easy with SolarWinds Engineer's Toolset

Every day administrator performs different network discovery tasks based on their IT needs and requirements. These can vary from simple tasks like discovering just a list of MAC addresses to very detailed tasks like conducting network inventory for generating reports. Network managers repeatedly think about automating essential network discovery tasks, which is difficult for administrators to perform manually including:

Below, we'll show you how to use Engineer's Toolset to accomplish network discovery tasks such as:

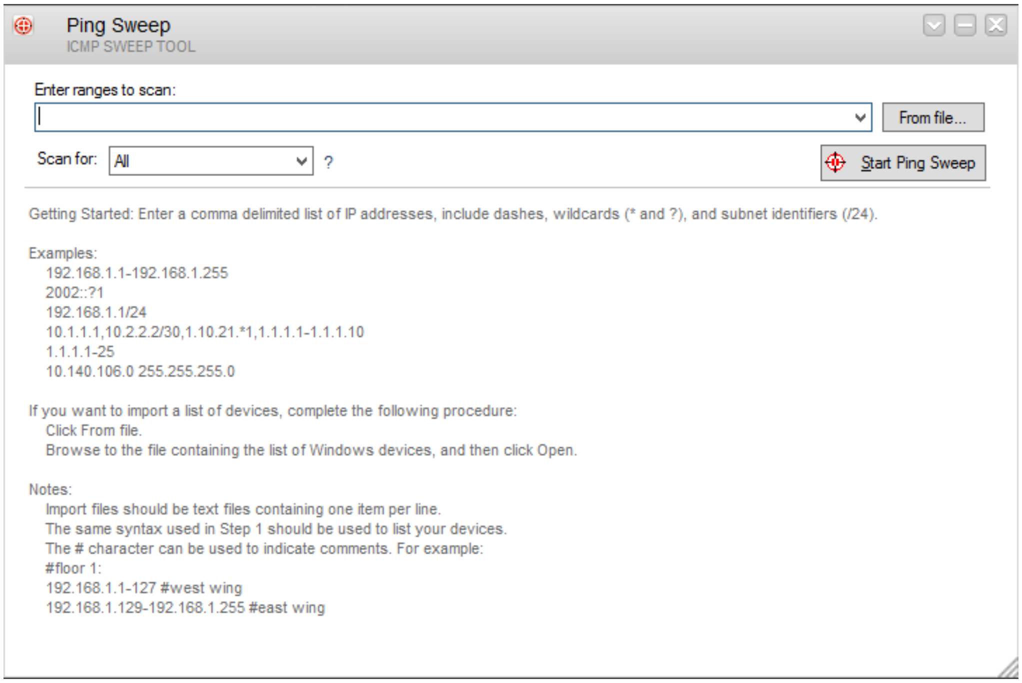
- How to scan IP addresses to identify which IP addresses are used and free
- How to discover a single subnet or a range of subnets using ICMP and SNMP in real time
- How to scan subnets and build information correlating IP addresses to MAC addresses
- How to discover all subnets and masks on a network by scanning route tables on a router
- How to scan open ports on the network
- How to discover devices connected to each port on a switch or hub
- How to discover and build a detailed network inventory

#1 How to Scan IP Addresses to Identify Which IP Addresses are Used/Un-Used

The **Ping Sweep Tool** in Engineer's Toolset can be used to scan a range of IP addresses using ICMP pings. It shows which IP addresses are in use and which are currently free. Also, administrators can look up the DNS name for each IP address using your configured DNS and WINS servers.

To use the Ping Sweep tool

Step 1: From the Launch Pad, click **Network Discovery**, select the **Ping Sweep tool,** and click **Launch**.



Enter ranges to scan:

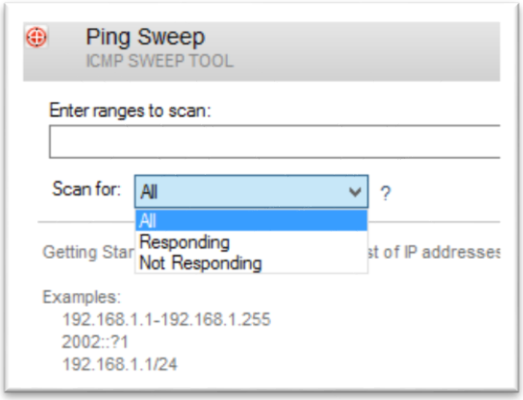
Scan for: All ?

```
Getting Started: Enter a comma delimited list of IP addresses, include dashes, wildcards (* and ?), and subnet identifiers (/24).

Examples:
   192.168.1.1-192.168.1.255
   2002::?1
   192.168.1.1/24
   10.1.1.1,10.2.2.2/30,1.10.21.*1,1.1.1.1-1.1.1.10
   1.1.1.1-25
   10.140.106.0 255.255.255.0

If you want to import a list of devices, complete the following procedure:
   Click From file.
   Browse to the file containing the list of Windows devices, and then click Open.

Notes:
   Import files should be text files containing one item per line.
   The same syntax used in Step 1 should be used to list your devices.
   The # character can be used to indicate comments. For example:
   #floor 1:
   192.168.1.1-127 #west wing
   192.168.1.129-192.168.1.255 #east wing
```

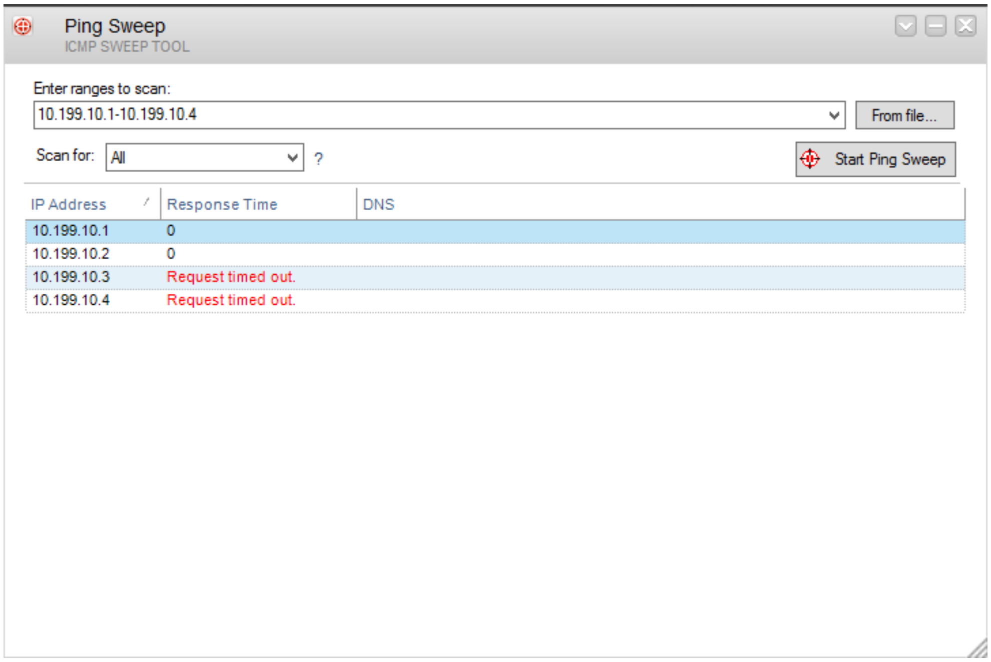
Step 2: Enter **IP ranges** to scan: Type a comma-delimited list of IP addresses to scan. You can type a range using dashes, you can use wildcards (* and ?), as well as subnet identifiers.

Step 3: If you want to use a file containing a large IP range, click **From File**, and then select the file. The file is parsed and each line specifies a multiple range of IPs.

Step 4: Select *Responding*, *Not Responding*, or *All* in the Scan for list.



Step 5: Click **Start Ping Sweep**.

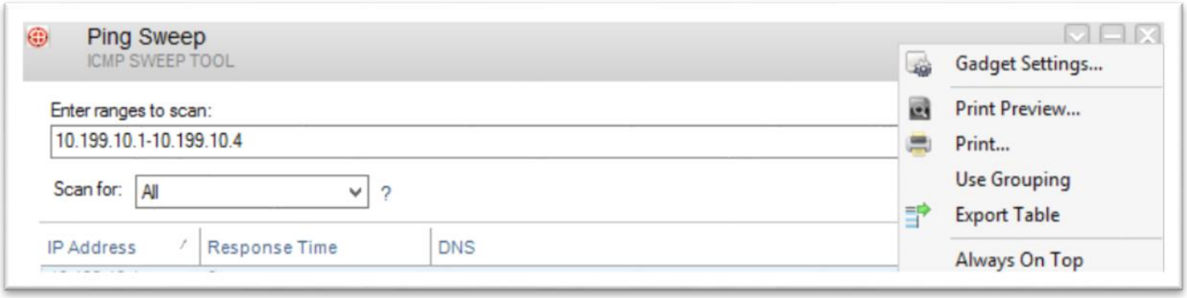


Enter ranges to scan: 10.199.10.1-10.199.10.4

Scan for: All

IP Address	Response Time	DNS
10.199.10.1	0	
10.199.10.2	0	
10.199.10.3	Request timed out.	
10.199.10.4	Request timed out.	

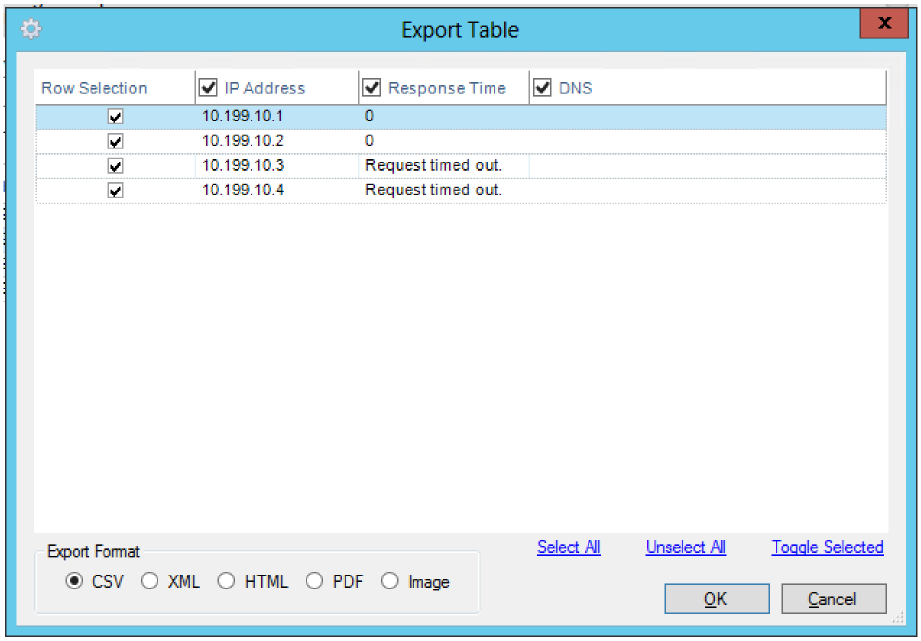
Step 6: If you want to export the results, click the drop-down box in top right corner, and then **click Export Table**.



Enter ranges to scan: 10.199.10.1-10.199.10.4

Scan for: All

Step 7: To check the items you want to export, select the format you want to export to from the Export Format options and click **OK.**



Row Selection	☑ IP Address	☑ Response Time	☑ DNS
☑	10.199.10.1	0	
☑	10.199.10.2	0	
☑	10.199.10.3	Request timed out.	
☑	10.199.10.4	Request timed out.	

Export Format

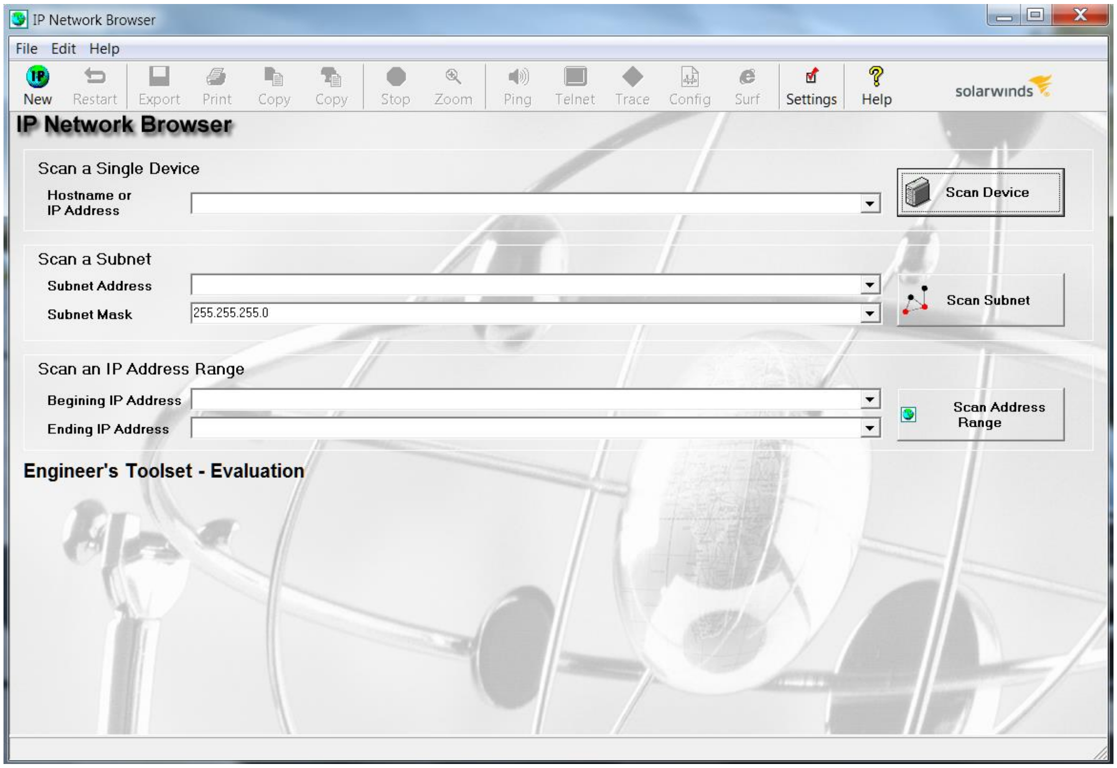
● CSV ○ XML ○ HTML ○ PDF ○ Image

Ping Sweep has the ability to export or print results to any of the following:

- Comma Delimited file (CSV)
- Plain Text file (TXT)
- HTML
- Excel® spreadsheet
- Copy to the clipboard

#2 How to Discover a Single Subnet or a Range Of Subnets using ICMP and SNMP in Real Time

The IP Network Browser tool in Engineer's Toolset can scan a subnet and show the details about the devices on the subnet. Each IP address is sent a PING. For each responding address, IP Network Browser attempts to gather more information using SNMP. IP Network Browser can discover any device with an IP address. If the device has an SNMP agent and the correct SNMP community string is included in the IP Network Browser Settings, IP Network Browser can discover more about the device.



Subnet Mask: 255.255.255.0

To scan a single device

Step 1: Type a **hostname or IP address** in the Hostname or IP Address field.

Step 2: Click **Scan Device.**

To scan a subnet

Step 1: Type an **IP address** in the Subnet Address field.

Step 2: Type the **subnet mask in the Subnet Mask field**, and then click Scan Subnet.

To scan an IP range

Step 1: **Type the beginning IP address** in the Beginning IP Address field.

Step 2: Type the final IP address of the range in the Ending IP Address field, and then click Scan Address Range.

To Export the data

Step 1: Click **File > Export Wizard,** check the nodes you want to include, and then **click Next**.

Step 2: **Select** the discovery groups you would like included in the report, and then **click Next**.

Step 3: Specify SNMP community strings, and then **click Export**.

Note: Network Sonar can discover your network and create a Microsoft® Access database.

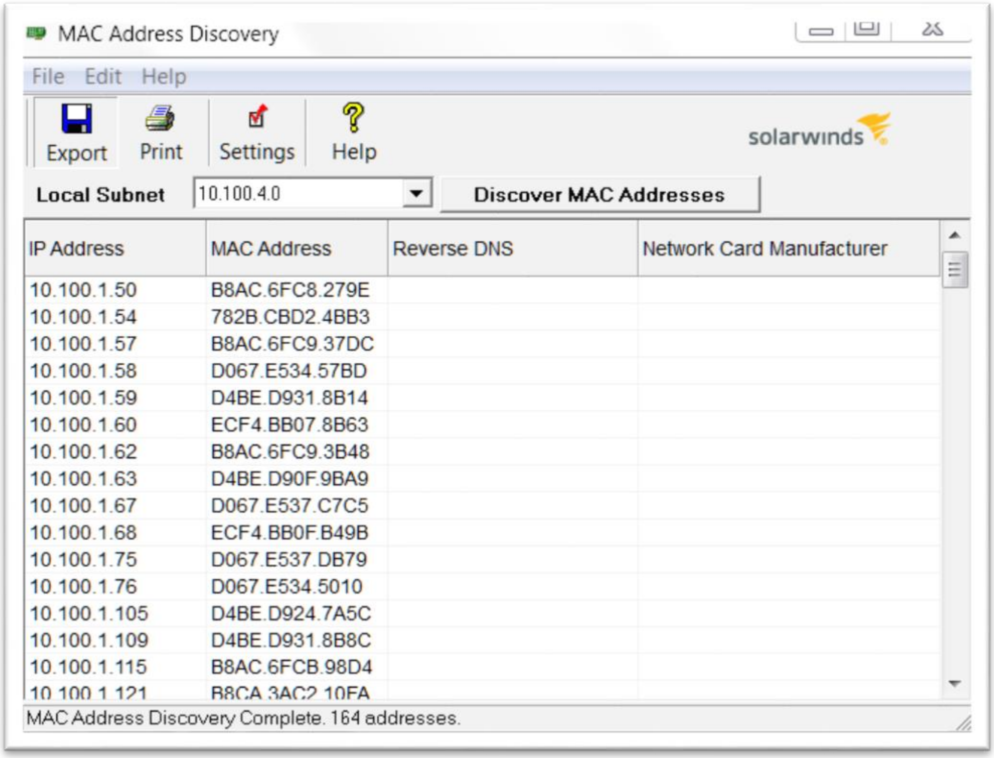
#3 How to Scan Subnets and Build Information Relating IP Addresses To MAC Addresses

The MAC Address Discovery tool for Engineer's Toolset can discover the MAC addresses, hardware manufacturer, IP address, and hostnames of the devices connected to your local network. If you want to discover the MAC addresses of devices connected to remote subnets, run the tool on a laptop that you can plug into the remote subnets.

To start your discovery

Step 1: Select the local subnet from the Local Subnet list. If your computer is attached to one subnet, only one choice is provided in the list.

Step 2: Click **Discover MAC Addresses**.



Local Subnet: 10.100.4.0

IP Address	MAC Address	Reverse DNS	Network Card Manufacturer
10.100.1.50	B8AC.6FC8.279E		
10.100.1.54	782B.CBD2.4BB3		
10.100.1.57	B8AC.6FC9.37DC		
10.100.1.58	D067.E534.57BD		
10.100.1.59	D4BE.D931.8B14		
10.100.1.60	ECF4.BB07.8B63		
10.100.1.62	B8AC.6FC9.3B48		
10.100.1.63	D4BE.D90F.9BA9		
10.100.1.67	D067.E537.C7C5		
10.100.1.68	ECF4.BB0F.B49B		
10.100.1.75	D067.E537.DB79		
10.100.1.76	D067.E534.5010		
10.100.1.105	D4BE.D924.7A5C		
10.100.1.109	D4BE.D931.8B8C		
10.100.1.115	B8AC.6FCB.98D4		
10.100.1.121	B8CA.3AC2.10FA		

MAC Address Discovery Complete. 164 addresses.

To export discovered results

Step 1: Click **File > Export**, and then select the type of export.

Step 2: Check the information you want to export.

Step 3: Specify the name and path for the exported information.

#4 How to Discover all Subnets and Masks on a Network by Scanning Route Tables on a Router

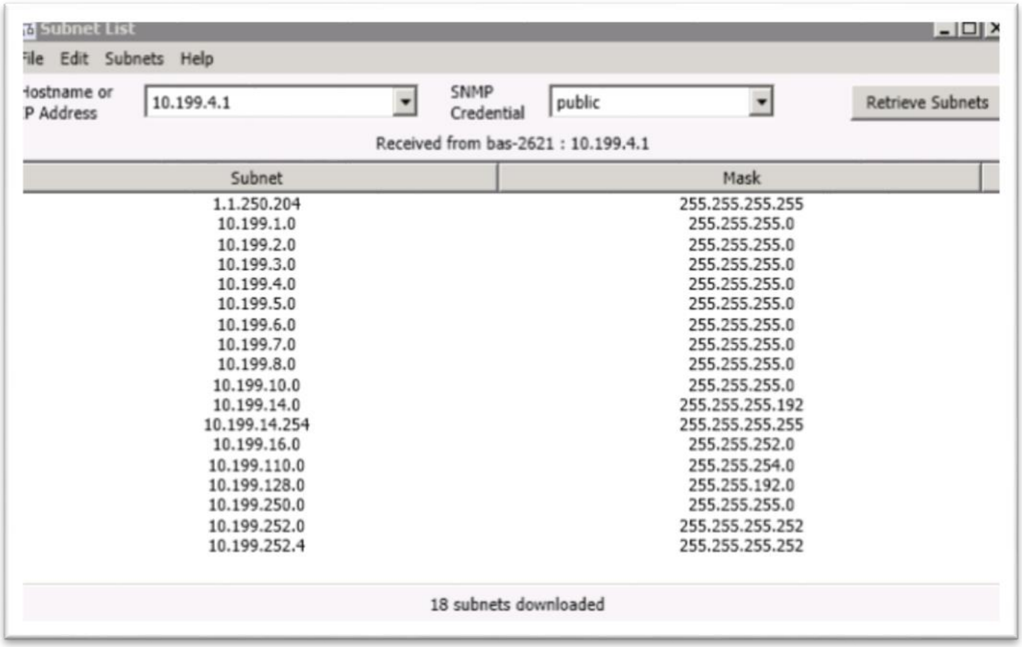
The Subnet List tool from Engineer's Toolset builds a list of network subnets by scanning route tables on a seed router. The target router must have SNMP enabled, and administrators must know the SNMP community string.

To retrieve subnet lists for your network

Step 1: Enter the **hostname or IP address** of the router or server.

Step 2: Enter or **select SNMP Credential** for a core router.

Step 3: Click **Retrieve Subnets**.



Hostname or IP Address: 10.199.4.1

SNMP Credential: public

Received from bas-2621 : 10.199.4.1

Subnet	Mask
1.1.250.204	255.255.255.255
10.199.1.0	255.255.255.0
10.199.2.0	255.255.255.0
10.199.3.0	255.255.255.0
10.199.4.0	255.255.255.0
10.199.5.0	255.255.255.0
10.199.6.0	255.255.255.0
10.199.7.0	255.255.255.0
10.199.8.0	255.255.255.0
10.199.10.0	255.255.255.0
10.199.14.0	255.255.255.192
10.199.14.254	255.255.255.255
10.199.16.0	255.255.252.0
10.199.110.0	255.255.254.0
10.199.128.0	255.255.192.0
10.199.250.0	255.255.255.0
10.199.252.0	255.255.255.252
10.199.252.4	255.255.255.252

18 subnets downloaded

Note: Subnet List Tool creates subnet lists by scanning route tables. If subnets have been summarized into a summary route on the router you are scanning, Subnet List cannot discover all your subnets. Direct the tool to a different router, one that does not have routes summarized.

To export, copy or print discovered results

Step 1: Click **File > Export**, select the export format and **click OK**.

Step 2: Click **Edit** and select either **Copy or Copy All**.

Step 3: Click **File > Print**, and then select the information you want to print.

#5 How to Scan Open Ports on the Network

The Port Scanner tool from Engineer's Toolset remotely discovers the status of TCP ports on devices. You can specify a range of IP addresses to include in the scan, and then scan a Quick List of port numbers or manually select the ports from a list that includes their common purposes.

To begin scanning ports

Step 1: Type the **beginning and ending IP addresses** of the computers whose ports you want to scan.

Step 2: If you want to use a Quick List for your scan, check Use Quick List, and then type a list of ports or **select a predefined Quick List**.

Step 3: If you want to select ports from a list which includes common port definitions, complete the following procedure:

a. **Click Settings**.

b. Check the ports you want to scan in the Available Ports list.

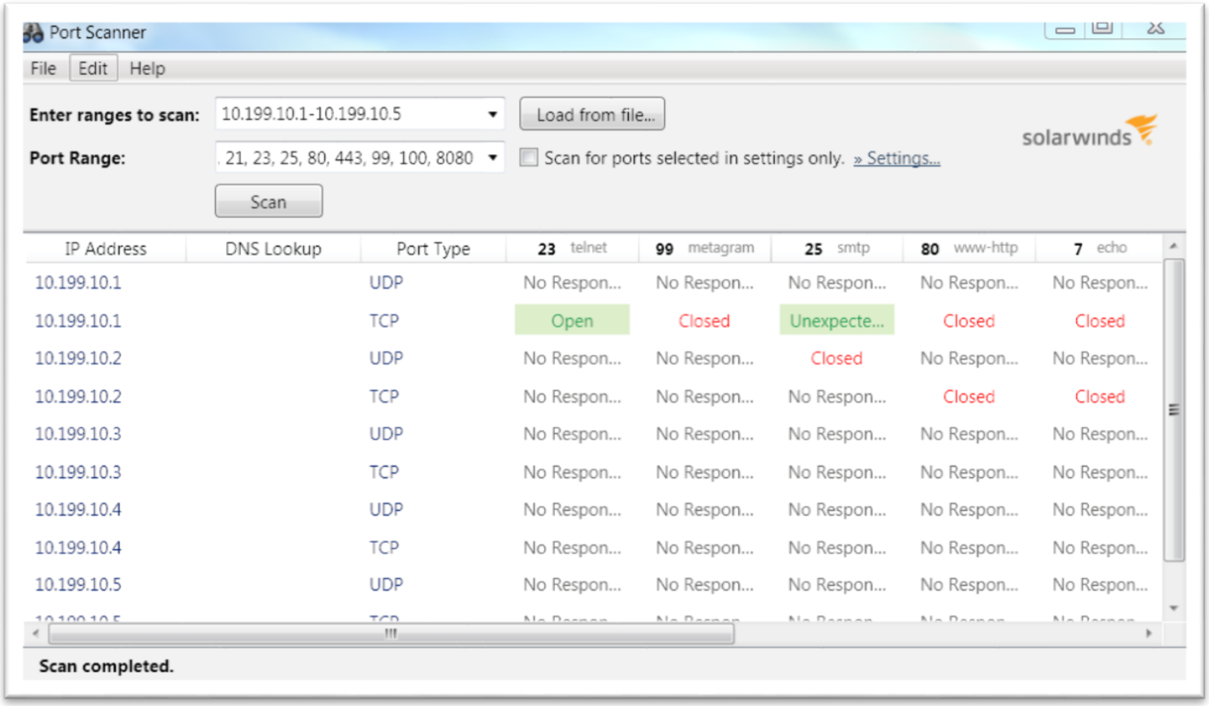
c. If you want to add a new port, type the port and a description in the Add New Port window grouping, and then **click Add New**.

d. If you want to delete a port, select the port, and then click Delete.

e. If you want to change the sort or filter the window to show only those ports already selected, check the appropriate field.

f. **Click OK**.

Step 4: Click **Scan**.



Enter ranges to scan: 10.199.10.1-10.199.10.5

Port Range: 21, 23, 25, 80, 443, 99, 100, 8080

□ Scan for ports selected in settings only. » Settings...

IP Address	DNS Lookup	Port Type	23 telnet	99 metagram	25 smtp	80 www-http	7 echo
10.199.10.1		UDP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...
10.199.10.1		TCP	Open	Closed	Unexpecte...	Closed	Closed
10.199.10.2		UDP	No Respon...	No Respon...	Closed	No Respon...	No Respon...
10.199.10.2		TCP	No Respon...	No Respon...	No Respon...	Closed	Closed
10.199.10.3		UDP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...
10.199.10.3		TCP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...
10.199.10.4		UDP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...
10.199.10.4		TCP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...
10.199.10.5		UDP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...
10.199.10.5		TCP	No Respon...	No Respon...	No Respon...	No Respon...	No Respon...

Scan completed.

To export, copy, or print results

Step 1: Click **File > Export**, select the export format and **click OK**.

Step 2: Click **Edit** and select either **Copy or Copy All**.

Step 3: Click **File > Print**, and then select the information you want to print.

#6 How to Discover Devices Connected to Each Port on a Switch or Hub

The Switch Port Mapper tool remotely discovers the devices connected to each port on a switch or hub. It also discovers the MAC address, IP address, and hostname of connected devices, as well as details about each port. Port mapping is done by discovering and correlating port information to MAC address and IP address information. The MAC and IP address information is discovered through a layer 3 device such as a router or server directly connected to the same subnet as the switch or hub.

To map your switch or hub

Step 1: Start **Switch Port Mapper**.

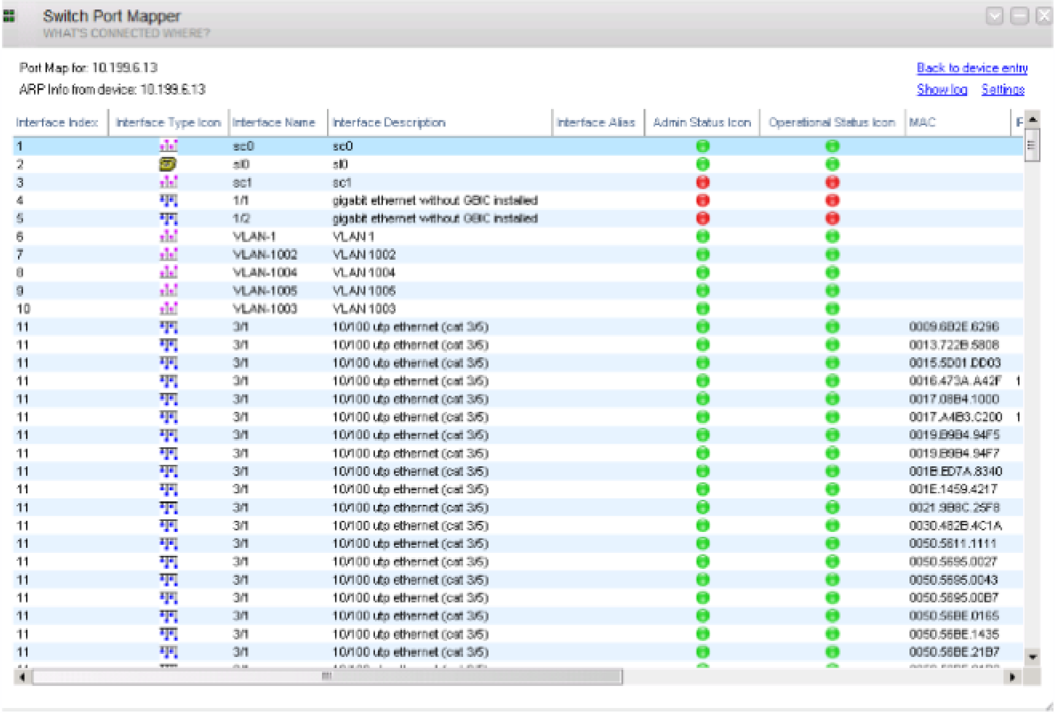
Step 2: Type the **IP address or host name** of the switch you want to map, and then select or type in the credentials or community string used to communicate with the switch.

Step 3: If your **switch is a Layer 3 switch**, check Get Layer 3 info from switch.

Step 4: If your **switch is not a Layer 3 switch**, type the IP address or host name of the router the switch is connected to in the Layer 3 Device field. Then, select or type in the credentials or community string used to communicate with the router.

Step 5: Click **Map Ports**.

Step 6: If you want to enable or disable an interface, right-click the interface in the results table, and then **click Enable/Disable Interface**.



Port Map for: 10.199.6.13
ARP Info from device: 10.199.6.13

Interface Index	Interface Type Icon	Interface Name	Interface Description	Interface Alias	Admin Status Icon	Operational Status Icon	MAC	F
1		sc0	sc0		🟢	🟢		
2		sl0	sl0		🟢	🟢		
3		sc1	sc1		🔴	🔴		
4		1/1	gigabit ethernet without GBIC installed		🔴	🔴		
5		1/2	gigabit ethernet without GBIC installed		🔴	🔴		
6		VLAN-1	VLAN 1		🟢	🟢		
7		VLAN-1002	VLAN 1002		🟢	🟢		
8		VLAN-1004	VLAN 1004		🟢	🟢		
9		VLAN-1005	VLAN 1005		🟢	🟢		
10		VLAN-1003	VLAN 1003		🟢	🟢		
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0009.6B2E.6296	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0013.722B.5808	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0015.5D01.DD03	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0016.473A.A42F	1
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0017.08B4.1000	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0017.A4B3.C200	1
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0019.B9B4.94F5	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0019.B9B4.94F7	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	001B.ED7A.8340	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	001E.1459.4217	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0021.9B8C.25F8	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0030.482B.4C1A	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.5811.1111	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.5695.0027	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.5695.0043	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.5695.00B7	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.56BE.0165	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.56BE.1435	
11		3/1	10/100 utp ethernet (cat 3/5)		🟢	🟢	0050.56BE.21B7	

To export results

Step 1: Click the drop-down arrow at top right corner, click **Export**, select the export format, and then **click OK**.

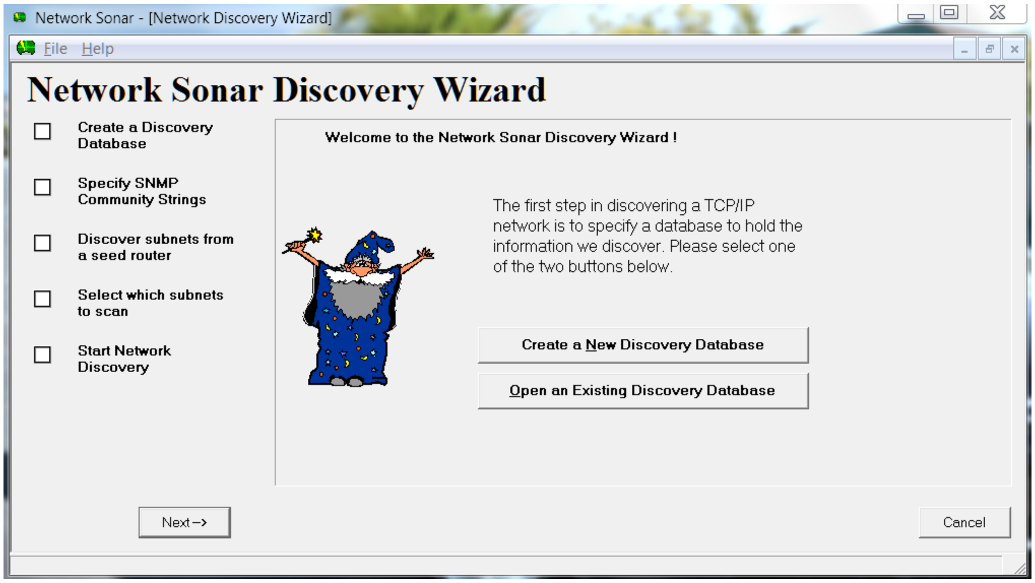
#7 How to Discover and Build a Detailed Network Inventory

Network Sonar is a high-performance network discovery tool that allows you to build a database of the structure and devices on a TCP/IP network. It enables you to produce a detailed network inventory in just minutes and generate reports using built-in templates. With Network Sonar, there's no need for special agents or data collectors. Network Sonar uses standard SNMP to collect detailed information about your network and produce a network inventory.

To start the wizard

Step 1: Open Network Sonar, check **Discovery Wizard,** and then click **OK**.

Step 2: If you are creating a new database, click **Create a New Discovery Database**, and then complete the following steps.



Network Sonar - [Network Discovery Wizard]

Network Sonar Discovery Wizard

Welcome to the Network Sonar Discovery Wizard !

The first step in discovering a TCP/IP network is to specify a database to hold the information we discover. Please select one of the two buttons below.

File Help
☐ Create a Discovery Database
☐ Specify SNMP Community Strings
☐ Discover subnets from a seed router
☐ Select which subnets to scan
☐ Start Network Discovery
Create a New Discovery Database
Open an Existing Discovery Database
Next-->
Cancel

a. Type a name and then select the type of database you want to create in the Save as type field:

- Sonar Database
- Access Database

b. Click **Save**.

Step 3: If you want to use a previously created database, click **Open an Existing Discovery Database**, select your database, click **OK**, and then click **Next**.

Step 4: Type your **SNMP community strings** into the Add field, click **Add,** and then click **Next**.

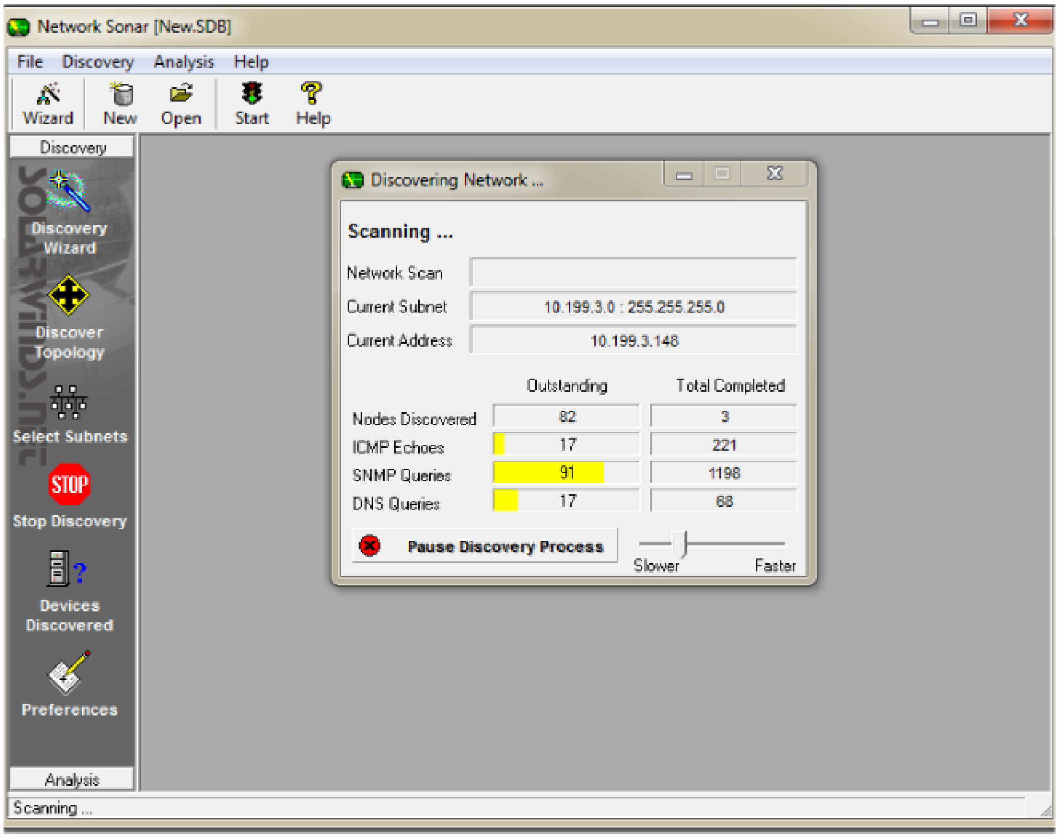
Step 5: Click Specify a **Seed Router and Discover Network Topology**. (A seed router is any router in your network. A server, switch, or workstation that supports SNMP can also be used. However, for best results use a core router.)

Step 6: Type an **IP address or hostname** in the Hostname or IP address field and then click Add.

Step 7: Click **Discover Network Topology**.

Step 8: Click **OK on the Network Topology** window and then **click Next**.

Step 9: **Check the subnets** you want to include, click **Next**, and then click **Start Discovery**.



Scanning ...

Network Scan

Current Subnet 10.199.3.0 : 255.255.255.0

Current Address 10.199.3.148

	Outstanding	Total Completed
Nodes Discovered	82	3
ICMP Echoes	17	221
SNMP Queries	91	1198
DNS Queries	17	68

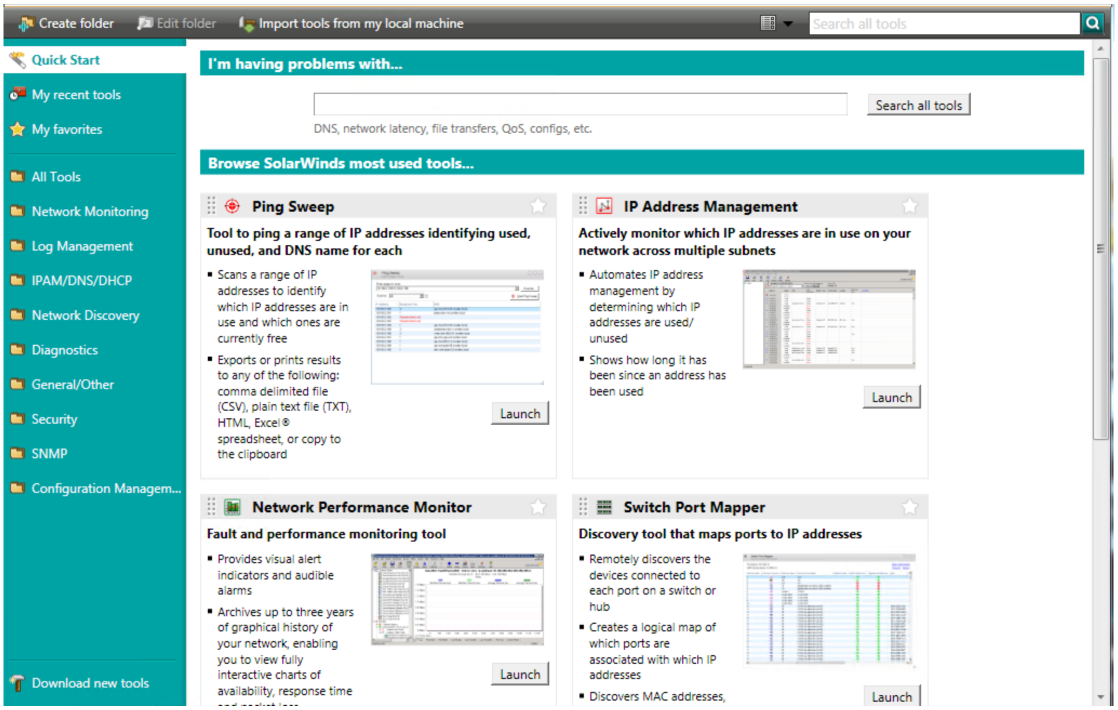
Scanning ...

Using Network Sonar's built-in reports and graphs, you can quickly and easily visually display your network inventory.

Top 5 Reasons to Try SolarWinds Engineer’s Toolset

Engineer’s Toolset delivers an advanced collection of monitoring, discovery, diagnostic, and Cisco® tools. Here are the top 5 reasons to use SolarWinds Engineer’s Toolset:

- Over 50 network tools in one complete package
- Monitoring tools include Real-Time Interface Monitor, SNMP Real-Time Graph, and more
- Diagnostic tools include Ping Sweep, DNS Analyzer, and Trace Route, and more
- Network discovery tools include Port Scanner, Switch Port Mapper, Advanced Subnet Calculator, and more
- Cisco management tools include Real-time NetFlow Analyzer, Config Downloader, and more



DNS, network latency, file transfers, QoS, configs, etc.

Ping Sweep

Tool to ping a range of IP addresses identifying used, unused, and DNS name for each

- Scans a range of IP addresses to identify which IP addresses are in use and which ones are currently free
- Exports or prints results to any of the following: comma delimited file (CSV), plain text file (TXT), HTML, Excel® spreadsheet, or copy to the clipboard

IP Address Management

Actively monitor which IP addresses are in use on your network across multiple subnets

- Automates IP address management by determining which IP addresses are used/ unused
- Shows how long it has been since an address has been used

Network Performance Monitor

Fault and performance monitoring tool

- Provides visual alert indicators and audible alarms
- Archives up to three years of graphical history of your network, enabling you to view fully interactive charts of availability, response time

Switch Port Mapper

Discovery tool that maps ports to IP addresses

- Remotely discovers the devices connected to each port on a switch or hub
- Creates a logical map of which ports are associated with which IP addresses
- Discovers MAC addresses,

LEARN MORE »

DOWNLOAD FREE TRIAL

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack®, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.