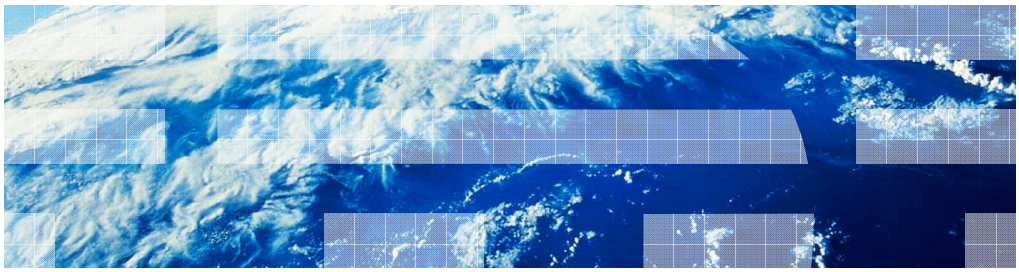
IBM Tivoli Network Manager 3.8

Configuring initial discovery



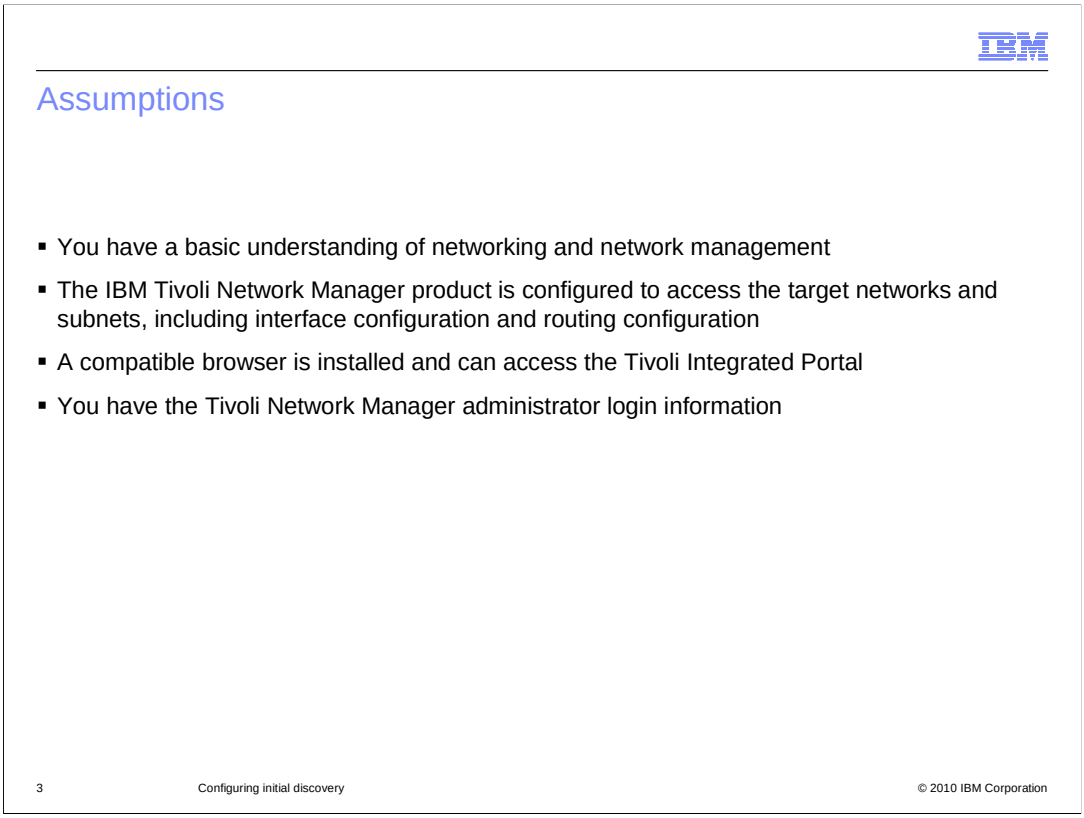
Tivoli software

Welcome to this module for IBM Tivoli® Network Manager 3.8 *Configuring initial discovery.*

Upon completion of this module you will be able to:

Customize the discovery by manually configuring the Ping and File finders, using specific discovery configuration GUI tabs.

Search for discovered devices and display them in the Hop View.



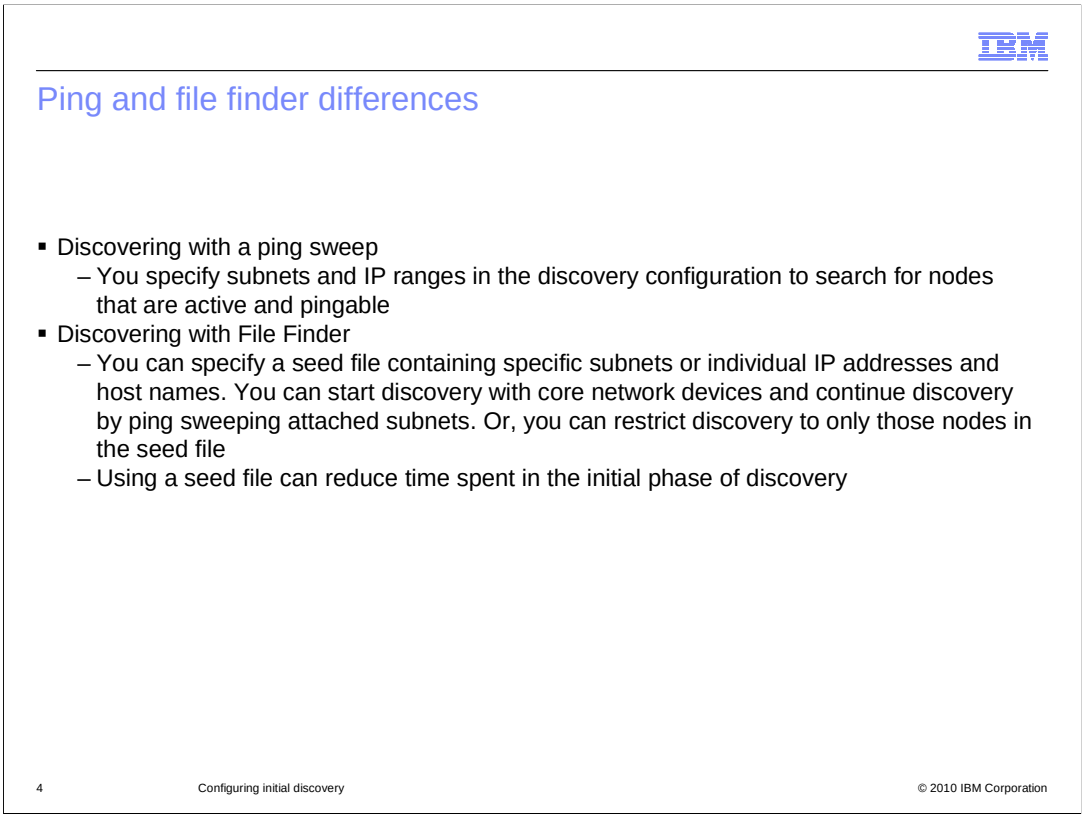
The major assumptions for this module are:

You have a basic understanding of networking and network management.

The IBM Tivoli Network Manager product is configured to access the target networks and subnets, including interface configuration and routing configuration.

A compatible browser is installed and can access the Tivoli Integrated Portal.

You have the Tivoli Network Manager administrator login information.



This slide describes the major differences between discovery using Ping and File Finder.

When discovering the network using Ping, you specify subnets and IP ranges in the discovery configuration tool to search for nodes that are active and pingable. This ping sweep covers a larger network and is useful for an initial discovery because it records all responding nodes.

When discovering with File Finder, you specify a seed file containing specific subnets or individual IP addresses and host names. You can start discovery with core network devices and continue discovery by ping sweeping attached subnets. Or, you can restrict discovery to only those nodes in the seed file. If you build a seed file of discovered hosts after your initial discovery, you can reduce the time spent in subsequent discoveries.

Log into the Tivoli Integrated Portal

- Open a Web browser and enter the secure URL for Tivoli Integrated Portal. This URL includes the port on which Tivoli Integrated Portal is running
  - Example: **https://*myhost*:16316/ibm/console/**
- Log in to Tivoli Integrated Portal with the Tivoli Network Manager administrator user name and password

5 Configuring initial discovery

All the Tivoli Network Manager GUI functions are performed and displayed in the Tivoli Integrated Portal.

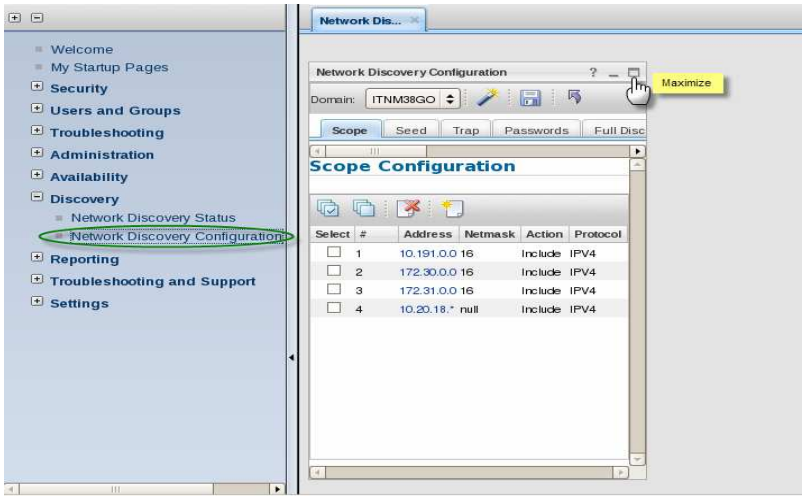
To log in to the Tivoli Integrated Portal, open a Web browser and enter the secure URL for Tivoli Integrated Portal. This URL includes the port on which Tivoli Integrated Portal is running.

An example of the URL is shown on this slide.

Log in to Tivoli Integrated Portal with the Tivoli Network Manager administrator user name and password.

This section shows you how to configure a simple discovery.

Network discovery configuration



Select **Network Discovery Configuration** from the tree menu on the left side of the browser window. Maximize the window for better viewing, if necessary

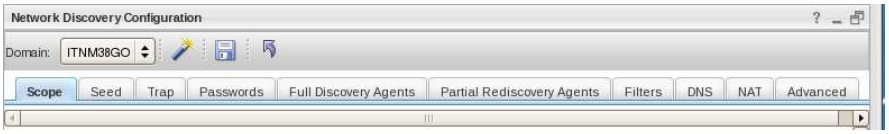
7 Configuring initial discovery

After you log in to the Tivoli Integrated Portal, the Welcome window is displayed.

To begin the Tivoli Network Manager network discovery configuration, select **Network Discovery Configuration** from the tree menu on the left side of the browser window.

When the Network Discovery Configuration window opens in the right pane, some browsers display it in a small window. If your browser does this, you can click the **Maximize** icon in the upper right corner of the frame after the tabs are displayed.

Network discovery configuration tabs

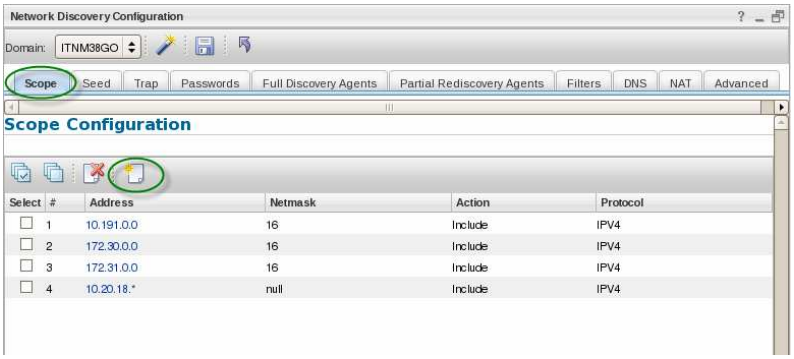


The network discovery configuration consists of ten configuration tabs:

- Scope
- Seed
- Trap
- Passwords
- Full discovery agents
- Partial rediscovery agents
- Filters
- DNS
- NAT
- Advanced

The Network Discovery Configuration consists of ten configuration tabs: Scope, Seed, Trap, Passwords, Full Discovery Agents, Partial Rediscovery Agents, Filters, DNS, NAT and Advanced.

Ping sweep discovery configuration

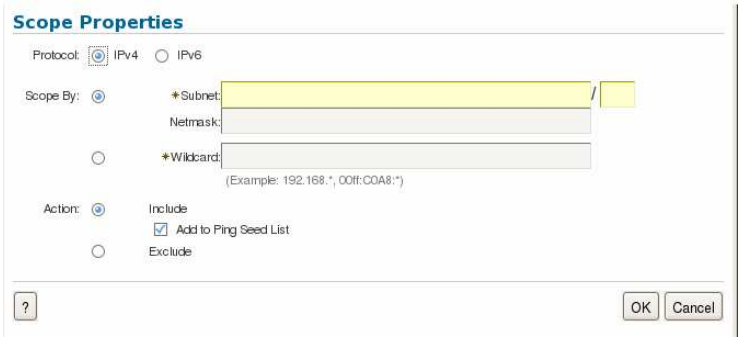


- Click the **Scope** tab in the Network Discovery Configuration window to display the Scope Configuration
- Click the **New** icon to open the Scope Properties window

A discovery using a ping sweep is good for new networks and subnetworks because it discovers all IP devices that are up and pingable.

To begin configuring a ping sweep discovery, click the **Scope** tab (if not already open). Then, click the **New** icon to open the Scope Properties window.

Scope properties



- Specify **IPv4** or **IPv6** network addressing
- You can specify subnets to include or exclude from the discovery scope. Use an explicit subnetwork in Classless Inter-Domain Routing (CIDR) notation, such as 192.168.1.0/24. Or, use a wildcard, such as 192.168.* in an IPV4 network or 00ff:COA8:* in an IPv6 network
- Select the appropriate **Action** radio buttons: Include or exclude. If needed, add the subnet to the ping seed list

IBM Tivoli Network Manager works with IPv4 or IPv6 network addressing.

There are two ways to define the subnet to discover with Ping. You can use an explicit subnetwork in Classless Inter-Domain Routing (CIDR) notation. Or, you can use a wildcard.

Select the appropriate radio button and enter the required information.

Select the appropriate Action radio buttons to include or exclude the subnet in the discovery. If needed, add the subnet to the Ping Seed List.

SNMP version

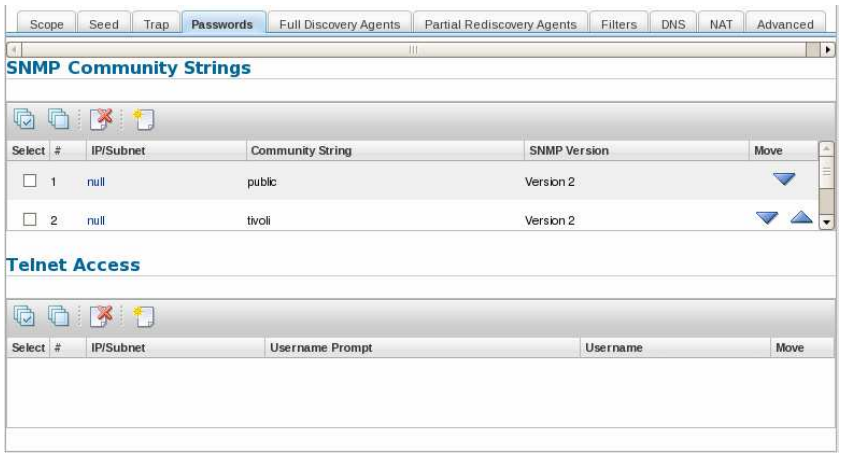
- Specify the SNMP community strings that Tivoli Network Manager will use during discovery
- Click the Password tab in the Network Discovery Configuration window. If some of your network devices use SNMP version 1 community strings, specify each community string twice. Specify a version 2 or 3 string before specifying the version 1 string. Tivoli Network Manager tries using the version 2 or 3 method first, which results in a more efficient use of network bandwidth during discovery than a version 1 string.

The next window displays the SNMP community strings that Tivoli Network Manager uses to communicate with target systems. Specify the SNMP community strings that Tivoli Network Manager will use during discovery.

Click the Password tab in the Network Discovery Configuration window. If some of your network devices use SNMP V1 community strings, specify each community string twice. Make sure that you specify a version 3 or version 2 string before specifying the V1 string. In the screen shown here, notice that the **tivoli** and **public** strings are specified first as a version 2 string, then as a version 1 string. Tivoli Network Manager tries using the version 2 SNMP protocol first. This method is more efficient and generates less network traffic than the data gathering method associated with SNMP version 1. If an older device cannot respond to the version 2 protocol, Tivoli Network Manager tries the version 1 protocol, if it is specified here.

When interrogating devices, Tivoli Network Manager first looks for strings specific to the device's IP address. Then, it tries strings that are specific to the device subnet, and finally global community strings. Within any level of specificity, it will process strings in the order that they are entered in the GUI. For example, in the screen shown here, if Tivoli Network Manager were interrogating 192.168.1.1, it would first attempt to use the **ilovit** community string. If that did not work, it would move to the subnet community string of **tivoli** and try SNMP version 2 first, then version 1. If those did not work, it would attempt the community string **nilhor** because that is the next most specific match. Finally, it would attempt the global community strings in the order in which they were entered into the GUI.

Telnet access



You can use the **Telnet Access** panel, which is below the SNMP panel, to set telnet or SSH parameters. You can use this panel to gather information that is not available from SNMP

You can use the **Telnet Access** panel below the SNMP panel to set telnet parameters. These parameters are used by the discovery process to gather information that cannot be gathered with SNMP. For example, some older Cisco catalyst switches use CATOS instead of IOS. Information about Mac addresses connected to switched ports is only available through telnet. Also, most devices using Multiprotocol Label Switching (or MPLS) only expose information about virtual routing and forwarding tables through telnet or SSH. When configuring the telnet password, you can specify SSH instead.

Discovery agents

- Click the Full Discovery Agents tab to choose specific discovery agents or groups of agents. By clicking **Full Layer 2 and Layer 3 Discovery,** you enable all agents in that agent group
- A Layer 3 discovery is recommended for your first discovery. This discovery completes quickly and lets you know if you have any problems accessing devices. It does not include data for network fault isolation or root cause analysis (RCA)
- A Layer 2 discovery collects data link information that can be used for RCA. It is a more thorough discovery, but it takes more time

13 Configuring initial discovery

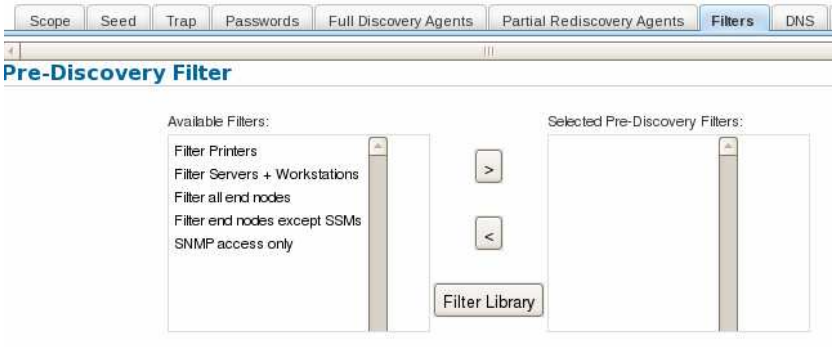
You can select the agents or agent groups that you want to use during discovery. For example, if you select Full Layer 2 and Layer 3 Discovery from the agent menu, all agents in that group are enabled. These agents can then interrogate your devices during discovery. If you click the name of any agent, you can display a description of that agent in a frame to the right of the agent names.

For a first discovery, it is typically a good idea to select a layer 3 discovery. This discovery complete quickly, and you can find out if you have any problems accessing network devices. However, to enable Tivoli Network Manager to perform network fault isolation, you need to run a layer to discover which will gather pertinent data link information.

To perform a discovery on both Layer 2 and Layer 3 devices, select the **Full Layer 2 and Layer 2 Discovery** check box.

To perform discovery on Layer 3 devices only, clear any selected boxes under the **Full Layer 2 and Layer 2 Discovery** heading and select the **Layer 3** check box.

Filtering discovery



- Click the Filters tab to select what type of node is displayed in Tivoli Network Manager after discovery. Typically, you filter end nodes from the discovery that you do not want in the network map
- By selecting a prediscovery filter, you prevent Tivoli Network Manager from interrogating the filtered devices. This selection reduces discovery time
- Use the provided filters or create a custom filter by selecting the **Filter Library** button

14 Configuring initial discovery

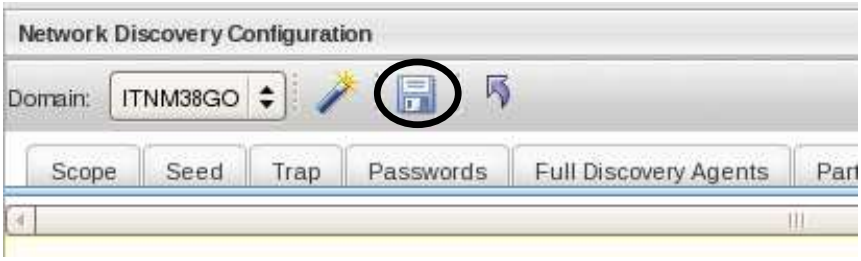
You can use the **Filters** tab to select what type of node is displayed in Tivoli Network Manager after discovery. Typically, you use this option to filter nodes from the discovery that you do not want in the network map.

By selecting a prediscovery filter, you prevent Tivoli Network Manager from interrogating the filtered devices and reduce discovery time.

You have several predefined filters for removing end nodes. You can filter printers, servers, and workstations, or any combination of these items. You can also filter all end nodes except for those using Tivoli system agents. You can discover servers that had an installed Tivoli system agent and eliminate Windows® workstations on which no agent was installed. You also have a filter for eliminating devices to which you had no SNMP access. Typically, when Tivoli Network Manager discovers a device to which it does not have SNMP access, it instantiates that device in the network map with a generic system icon. Using the **SNMP access only** filter prevents the display of these devices in the network map. However, it is best not to use this filter on your first discovery because it can be helpful to know which devices you do not have access to.

Use one or more of the provided filters or create a custom filter by selecting the **Filter Library** button. Most discovery filters are based on the object ID (or OID) number of the device. However, you can also use the IP address or system description as a part of the prediscovery filter.

Save the discovery configuration

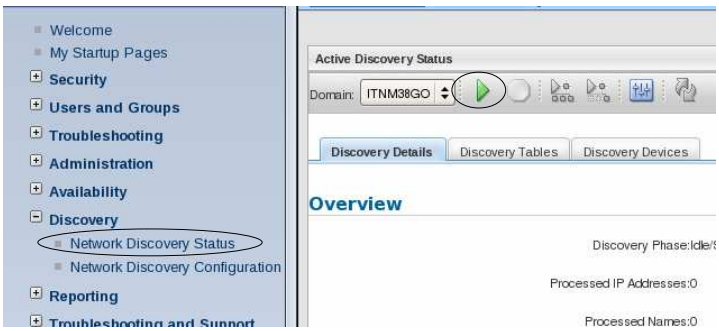


- Save the discovery configuration by clicking the diskette icon above the tabs

After you complete the discovery configuration, you must save it before it can be used for discovery.

Save the discovery configuration by clicking the diskette icon above the tabs.

Start the discovery process



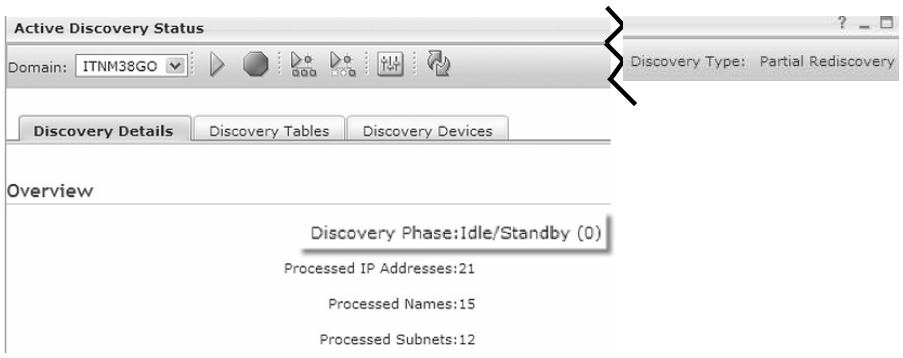
- To start the discovery process, click the Network Discovery Status menu item in the left navigation menu
- After the Active Discovery Status window displays in the right pane, click the green arrow at the top of the pane to start the discovery

To start the discovery process, click the Network Discovery Status menu item in the left navigation menu.

After the Active Discovery Status window opens in the right pane, click the green arrow at the top of the pane to start the discovery.

If you have run a discovery previously, the green arrow might not be available. In that case, click the red stop sign icon to stop the current discovery process. Then, click the green arrow to start a new discovery after reading the modified discovery configuration information.

Discovery status



- As the discovery runs, the status is displayed in the Overview section
- The discovery is complete when the Discovery Phase displays **Idle/Standby** and the Discovery Type changes to **Partial Discovery**
- An event is sent to the ObjectServer, indicating that discovery is complete

As the discovery runs, the status is displayed in the Overview section.

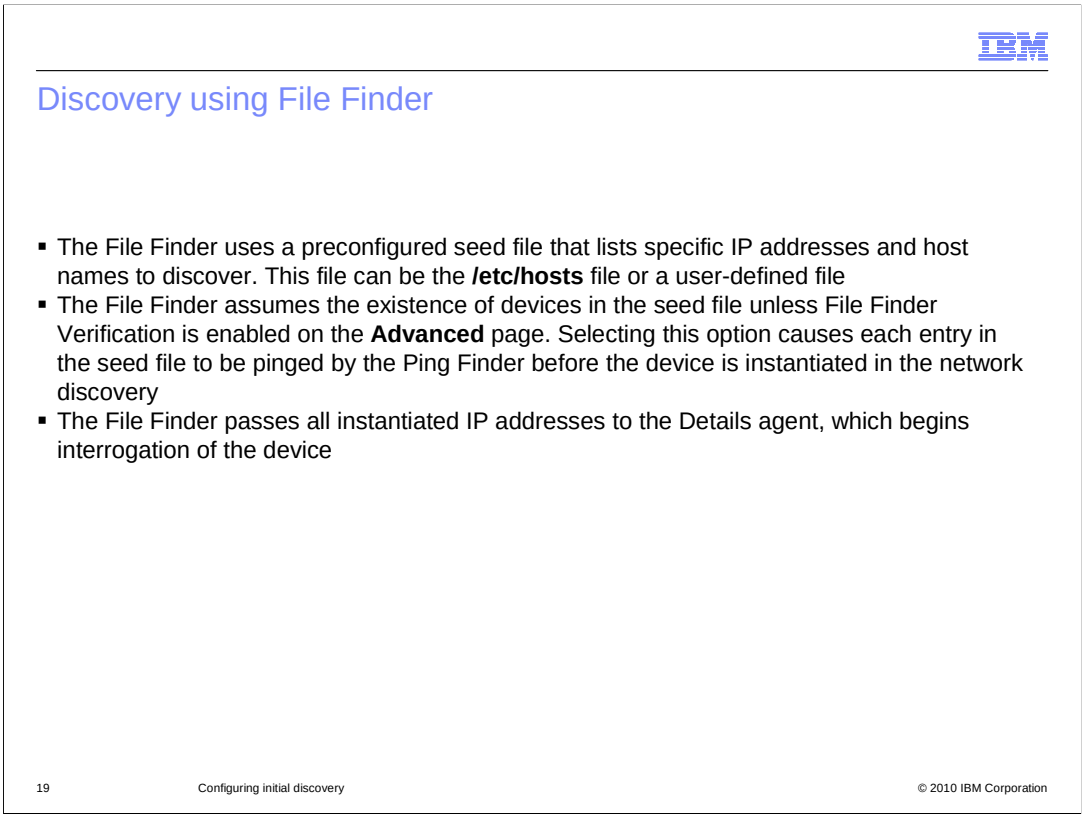
The discovery is complete when the Discovery Phase displays Idle/Standby and the Discovery Type in the upper right part of the window changes to Partial Discovery. Also, Tivoli Network Manager sends an event to the ObjectServer, indicating that discovery has completed.

The steps to view the discovered network are described later in this module.

Section

IBM Tivoli Network Manager IP Edition: Enhancing discovery with pattern matching

This section shows you how to configure a discovery using the File Finder.



The File Finder uses a preconfigured seed file that lists specific IP addresses and host names to discover. This can be the **/etc/hosts** file or a user-defined file.

The File Finder assumes the existence of devices in the seed file unless File Finder Verification is enabled in the **Advanced** tab. Selecting this option causes each entry in the seed file to be pinged by the Ping Finder before the device is instantiated in the network discovery.

The File Finder passes all instantiated IP addresses to the Details agent, which begins interrogation of the device.

Create a seed file

- You can use the **/etc/hosts** file, another seed file, or several different seed files
- To edit a seed file, use an editing program such as **vi** and list the hosts that you want to discover. Use the *ipaddress<tab>hostname* notation, similar to that used in the **/etc/hosts** file
  - Example: **vi $NCHOME/etc/precision/10.20.hosts**

    10.20.18.193 kepler
    10.20.18.196 galileo
    10.20.18.197 messier
  - You can also use a space or comma as the delimiter character. Always be consistent in your use of a delimiter character within an individual seed file
  - Save the seed file and exit the editor

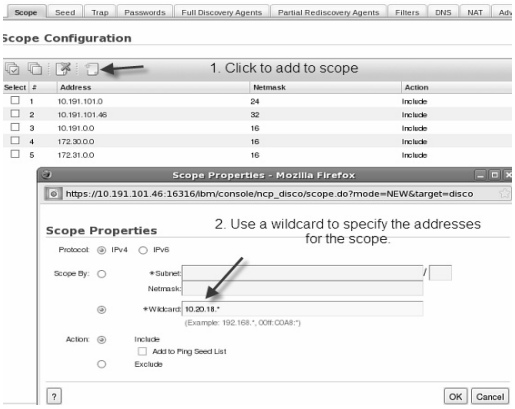
You can use the **/etc/hosts** file, another seed file, or several different seed files.

To edit a seed file, use an editing program such as **vi** and list the hosts to discover, using the *ipaddress<tab>hostname* notation, similar to that used in the **/etc/hosts** file.

You can also use a space or comma as the delimiter character. Always be consistent in your use of a delimiter character within an individual seed file.

On this slide is an example of the vi command using a complete relative path to the seed file and three end nodes contained in that file.

Update the scope information



- Add the network to the scope of the discovery using the **Scope** tab. Use CIDR notation in the Subnet field or use part of an IP address with a wildcard
- When you select the **Add to Ping Seed List** check box, you ping the nodes that are in the seed file. If you do not want the nodes to be pinged, ensure this check box is not selected

Addresses of devices that you are adding in the seed list might not be contained within the scope of the discovery. Those individual IP addresses or the subnets that contain them must be added to the discovery scope.

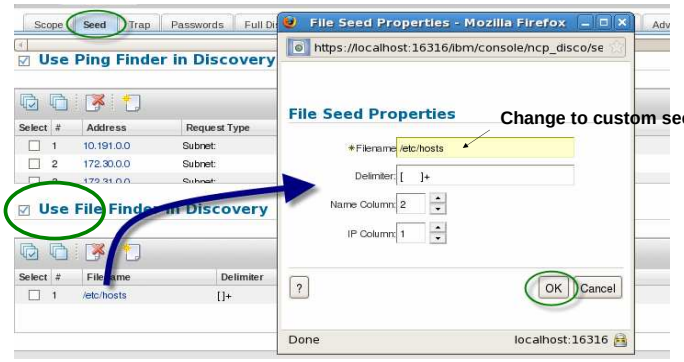
Remember that any chassis that is not in the discovery scope cannot be pinged, polled, or instantiated into the network discovery. Out-of-scope interfaces that are contained with in an in-scope chassis are instantiated in the discovery, but the discovery does not continue outward through that interface.

Add the network to the scope of the discovery using the **Scope** tab in CIDR notation in the Subnet field. Or, use part of an IP address with a wildcard in the Wildcard field.

The **Add to Ping Seed List** box, when selected, pings the nodes that are contained in the seed file. This option is helpful if new nodes have been added to the network but are not fully operational at the time of the discovery.

If you do not want the nodes to be pinged, ensure this check box is not selected.

Configure the File Finder



- Click the **Seed** tab
- Select the **Use File Finder in Discovery** check box
- Click the icon to add a new file, or click an existing entry to modify it. The **File Seed Properties** dialog box opens. Specify the correct path and file name of your seed file in the **Filename** field
- Specify the correct delimiter for your seed file and specify which column contains the address and which column contains the name

The next step is to specify the custom seed file in the Seed window.

To begin, click the **Seed** tab.

Then, select the **Use File Finder in Discovery** check box.

Click the icon to add a new file, or click **/etc/hosts** and edit that entry to match the parameters of your new seed file. The File Seed Properties dialog box opens.

Specify the correct path and file name of your seed file in the **Filename** field.

Specify the correct delimiter for your seed file. If you use a tab or space as the delimiter, enclose this delimiter in square brackets followed by a plus sign. The plus sign allows for one or more of the characters within brackets to work.

If someone else provides you with a seed file, the format of that seed file might not be consistent. Very often, people insert spaces in some lines of the seed file. These lines make the numbers or names line up with other lines that can only have tabs in them. Put both a tab and space within square brackets and then put a plus sign (+) after the brackets. The file finder can correctly parse the delimiter as consisting of one or more tabs or spaces. Then, the file finder is more tolerant of inconsistent formatting in seed files that have been provided to you.

Make sure that you specify which column contains the address and which column contains the name.

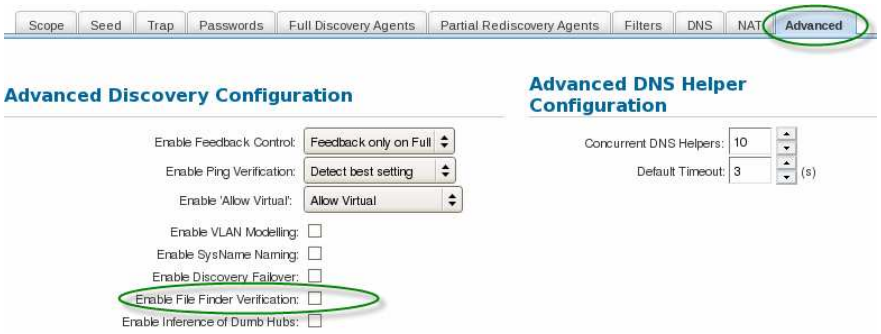
Select the appropriate agents

- Click the **Full Discovery Agents** tab
- Select the check box for each agent or agent group that you want to run
- Click the **Filters** tab and select any filters that you want to use, if you have not already done so

Next, define the full discovery agent to use during discovery.

Click the **Full Discovery Agents** tab and select the check box for **Full Layer 2 and Layer 3 Discovery** to enable this option.

Configure optional parameters



- Click the **Advanced** tab
- Scroll down to the **Advanced Discovery Configuration** section
- Select or clear the **Enable File Finder Verification** option

Set the Advanced Discovery Configuration options.

Click the **Advanced** tab.

Scroll down to the **Advanced Discovery Configuration** section.

Select or clear the **Enable File Finder Verification** option**.**

With **File Finder Verification** selected or enabled, Tivoli Network Manager pings all file finder entries to verify that those devices are active in the network.

Those that do not respond are not instantiated in the network map.

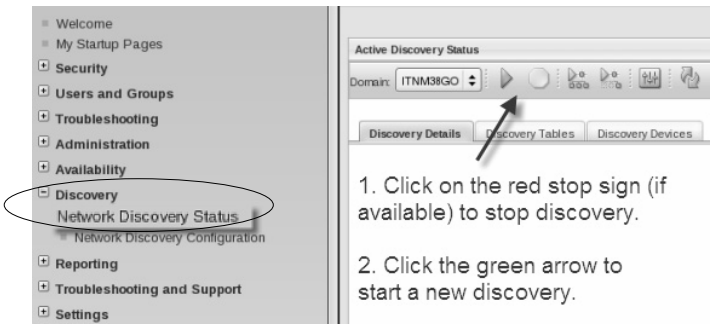
With **File Finder Verification** cleared or disabled, Tivoli Network Manager does not verify the existence of the hosts. All entries found by the file finder are assumed to exist.

Save the discovery configuration

- Save the discovery configuration by clicking the diskette icon

Save the discovery configuration by clicking the diskette icon.

Start or restart the network discovery



- Click **Discovery Status** on the Discovery tab
- Click the red stop sign to stop the discovery process if it is already running
- Click the green arrow to start a new discovery

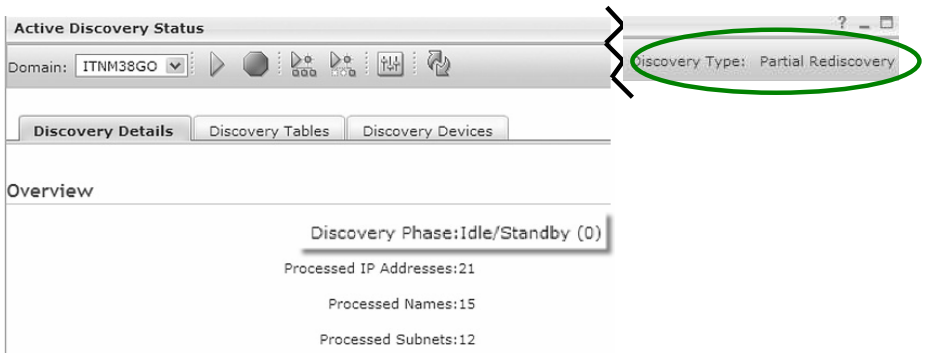
Run discovery using the newly defined custom seed file with the other options that were set in the previous slides.

Click the **Network Discovery Status** submenu item in the **Discovery** menu on the left.

Then, click the red stop sign to stop the discovery processes.

Finally, click the green arrow to start a new discovery.

Discovery completion



- Discovery is finished when the discovery phase returns to **Idle/Standby (0)** and the discovery type returns to **Partial Rediscovery**
- Tivoli Network Manager also sends an event to the ObjectServer, indicating that discovery is complete

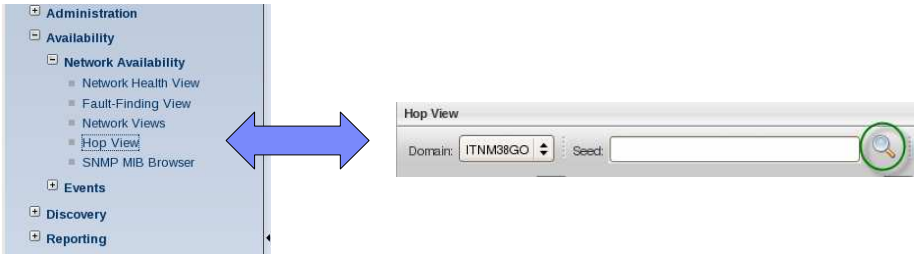
Discovery is finished when the discovery phase returns to **Idle/Standby (0)** in the Discovery Details window and the discovery type returns to **Partial Rediscovery.** Tivoli Network Manager also sends an event to the ObjectServer, indicating that discovery is complete.

Section

Verifying discovery results

This section shows you how to verify your discovery results.

Discovery verification



- After discovery is finished, verify that hosts specified in the seed file are in the discovery results
- Select the **Hop View** from the tree menu at the left side of the screen
- Enter an IP address you want to view and click the green play arrow at the right side of the window
- You can also click the **Search for Seed** icon to the right of the **Seed** field in the Hop View window to search for devices that meet a certain criteria

After discovery is finished, verify that the hosts specified in the seed file are in the discovery results.

Select the **Hop View** from the tree menu at the left side of the screen.

Enter an IP address you want to view and then click the green play arrow at the right side of the window.

You can also click the **Search for Seed** icon to the right of the **Seed** field in the Hop View window to search for devices that meet a certain criteria.

Searching for a network entity

- In the **Entity Search** window, select the **mainNodeDetails** table
- Specify the field name you want to use to search for applicable entities
- Enter the comparator in the Value field
- If using regular expression matching, the percent sign (**%**) is a wildcard character
- Click **Find** to display a list of devices in the results window
- Double-click an entry in the results window to populate the **Seed** field in the Hop View window
- Click the **Close** button to dismiss the search window

In the Entity Search window, select the **mainNodeDetails** table.

Specify the field name you want to use to search for applicable entities. In the example shown here, the **ipAddress** field is selected.

Enter the comparator in the Value field.

If using regular expression matching, the percent sign (%) is a wildcard character.

Click **Find** to display a list of devices in the results window.

Double-click an entry in the results window to populate the **Seed** field in the Hop View window.

Click the **Close** button to dismiss the search window.

Viewing the device in the Hop view

- The device is displayed in the **Hop View** window
- More component details about the device are displayed in the **Structure Browser** information at the bottom of the **Hop View**
- Increase the number of hops and click the green player arrow to see more devices surrounding the specified device. No other devices are displayed when increasing the hops, if the specified device did not provide connectivity information to Tivoli Network Manager

The device opens in the Hop View window.

Further component details about the device are displayed in the **Structure Browser** information at the bottom of the **Hop View**.

Increase the number of hops and click the green player to see more devices surrounding the specified device. No other devices are displayed when increasing the hops if the specified device did not provide connectivity information to Tivoli Network Manager.

Combinations of ping and file finder

- Ping finder only: Discovery ping sweeps specified IP addresses, subnets, and any discovered subnets that are within the scope of discovery
- File finder only:
  - With ping verification disabled: Discovery instantiates all devices specified in the seed file
  - With ping verification enabled: Discovery only instantiates those devices in the seed file that respond to the verification ping
  - This method is often used by managed service providers (MSPs) to find only those devices they are paid to manage
- Ping and file finder:
  - With feedback enabled, discovery begins with the seeded devices. When it detects that there is a subnet attached to a device, it ping sweeps that subnet if it is within scope
  - With feedback disabled, this behavior does not occur. The Ping Finder only pings those addresses for which it was previously configured

There are several ways to use combinations of the Ping Finder and File Finder. When you use only the Ping finder, the discovery engine attempts to ping all specified IP addresses and subnets. These addresses and subnets are either configured or discovered if they are within scope.

If you use the file finder only, discovery only finds those devices that are listed in the file finder seed list. This method is often used by many service providers. They only find the devices on the customer networks that they are being paid to manage. Enabling file finder verification ensures that a device responds to a ping before it is instantiated in the network map.

When using both the ping and file finders, you can use an option on the Advanced tab to enable or disable feedback. With feedback enabled, discovery begins with the seeded devices. When it detects that there is a subnet attached to a device, it ping sweeps that subnet if it is within scope. With feedback disabled, this behavior does not occur. The Ping Finder only pings those addresses for which it was previously configured.

With the completion of this IBM Education Assistant module you should now be able to:

Customize the discovery by manually configuring the Ping and File finders using specific discovery configuration GUI tabs.

Search for discovered devices and make them display the Hop View.

This concludes the IBM Education Assistant module for IBM Tivoli Network Manager 3.8 *Configuring initial discovery.*

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_configuring_discovery.ppt

This module is also available in PDF format at: ../configuring_discovery.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information