

Chapter 5

Network & Topology Discovery

5.1 Overview

Today, enterprise networks are large, complex, and constantly changing. To help you keep track of the components of your infrastructure, NetVigil provides both network and topology discovery.

Network discovery, included in all NetVigil installations, enables you to automatically discover and provision new devices into NetVigil.

Layer 2 and 3 **topology discovery**, available when you purchase a NetVigil Topology license, discovers devices and maps the relationships between them. (You can also map relationships between devices manually by creating device dependencies as described under “Device Dependency” in the “Web User Guide”.

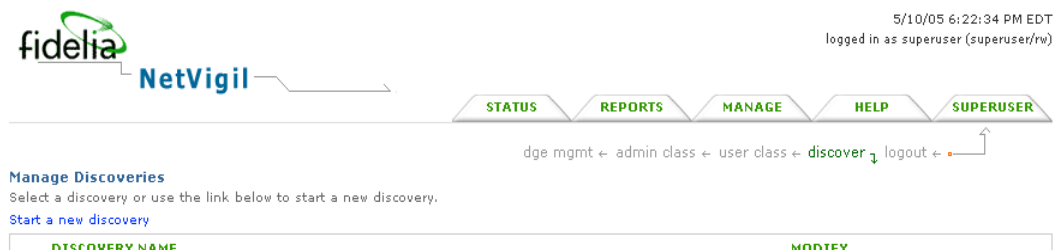


Figure 5.1 Menu item for network discovery

Topology discovery is run for one DGE Location at a time, by the least-loaded DGE in that location. This ensures that discovery is not blocked by firewalls, access lists, etc., since the DGE must have access to the devices that it is to monitor.

NOTE: You must log in as Superuser to run network or topology discovery.

5.1.1 Configuring Scope of Discovery

Discovery scope is the range of devices that are discovered by a single discovery operation. There are two ways to configure discovery scope:

- Specify one or more IP address/subnet mask pairs, and discover devices on those subnets
- Specify a seed router and a number of hops, and discover devices within the specified number of hops from the seed router (Topology license only). (A hop is the trip a data packet takes from one router or intermediate device to another within a network. If a packet travels from a source computer to a router to a second router to a destination computer, it has taken one hop.)

In addition, the final list of discovered devices is affected by the following:

- Discovery location, the DGE location from which the discovery is run

The least-loaded DGE in the selected DGE Location performs discovery. Devices that are inaccessible to this DGE (due to ACLs, firewalls, etc.) are not discovered.

- Discovery filter (Topology license only), which determines what kinds of devices appear in the final list

You can choose to include or exclude specific device types from the final list of discovered devices.

Example: Configuring Discovery Scope

.....
Figure 5.2 shows a sample network that includes three subnets, each of which is connected to a router. All three subnets are part of the same DGE location, which contains only one DGE, in Subnet A.

Here are two sample discovery configurations and their results:

- The Superuser configures discovery by specifying two IP Address/subnet pairs:

```
198.168.2.0/255.255.255.0  
198.168.3.0/255.255.255.0
```

Discovery finds all of the devices on Subnet B and Subnet C.

- Superuser configures discovery by specifying the IP address of Router A, 192.168.1.14, and a maximum of two hops. The result is that devices in all three subnets are discovered, because Router B and Router C are both within two hops of Router A, and devices within the subnets that are connected to the routers fall within the discovery scope.

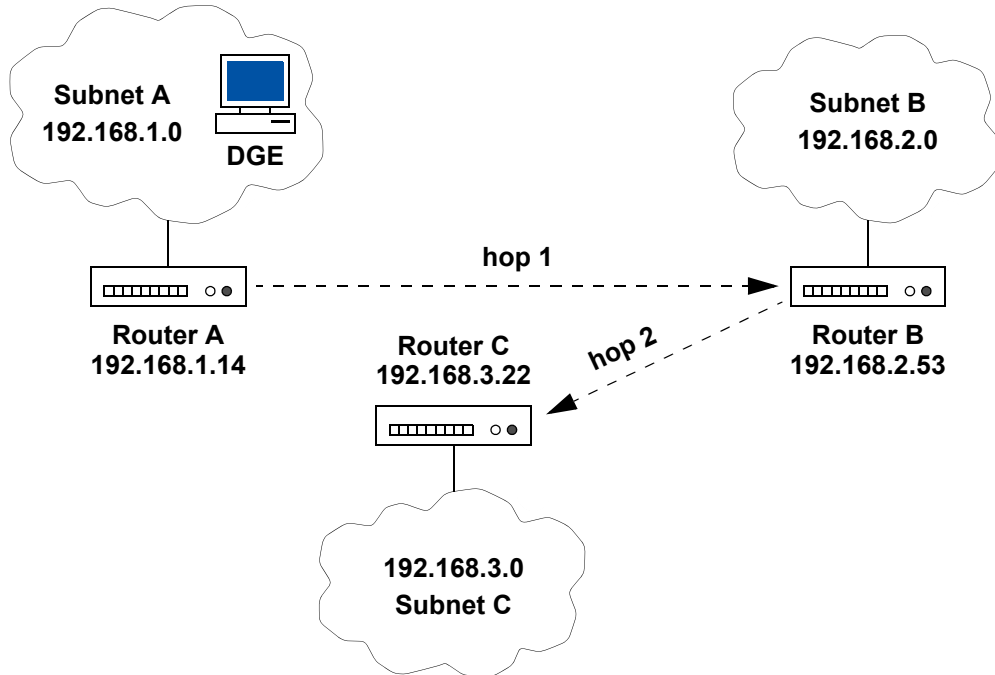


Figure 5.2 Sample network configuration for NetVigil discovery

SUPERUSER

To run Network or Topology Discovery:

1. Click SUPERUSER | discover.

5/10/05 6:22:57 PM EDT
logged in as superuser (superuser/rw)

STATUS REPORTS MANAGE HELP SUPERUSER

dge mgmt ← admin class ← user class ← discover ↓ logout ←

Network Discovery

Select or complete the required fields below. Click 'Run Discovery' to start discovery.

1. Please name your discovery : **discovery (May 10 2005, 6:2)**
2. Network Scope :
Discover devices with ip addresses in the following IP subnets. Specify one IP subnet/netmask per line(e.g., 192.168.1.0/255.255.255.0). You must specify at least one network.
3. Discovery Location :
Network discovery is performed by a DGE at each DGE Location to ensure optimal network efficiency and to avoid access restrictions (e.g., firewall, ACL, private IP space). Please select the location where discovery should be performed. If the location has multiple DGEs, the one with the fewest configured tests is used for discovery.
4. Discovery Filter :
 Include Exclude the following device types
5. SNMP Community Strings :
 Only add devices that support SNMP. If selected, at least one SNMP community string must be specified here. Specify the SNMP community strings that are used in your network. Enter multiple SNMP strings one on each line
6. Advanced Options :
 Discover physical connectivity (topology) between devices :
 Update topology information for provisioned devices only
 Discover new devices and new/updated topology
 Start discovery from following "seed" router. The specified IP address must be the address of a router. If this option is selected, the IP subnet list (above) will be ignored.
Seed router IP address :
Maximum number of hops :

Figure 5.3 Network Discovery screen

2. If no discovery data exists, the Network Discovery page appears.
Configure the following discovery options:

Table 5.1 Network Discovery Configuration Parameters

Field	Purpose
Network Discovery Scope	Specify the subnet(s) on which you want to discover devices. For each subnet, enter an IP address and a subnet mask in dotted quad notation. To enter multiple IP address/subnet mask pairs, list each one on a separate line. You must specify at least one subnet/subnet mask pair. For additional information see Section 5.1.1, "Configuring Scope of Discovery" on page 62.
Discovery Location	Select the DGE Location for which you want to perform discovery. Discovery is performed by the DGE in this location that has the fewest configured tests.
Discovery Filter (Topology license only)	Optionally, to filter discovery results, select include or exclude , and the device types to be included or excluded.
SNMP Community Strings	<p>To automatically discover SNMP tests that are supported by discovered devices, specify the SNMP community strings that are used in your network(s). Enter one community string per line. If no community string is entered, discovered devices are not tested for SNMP capabilities.</p> <p>To discover SNMP devices only, select Exclude devices that do not support SNMP. If this option is selected you must enter at least one SNMP Community string.</p>

Advanced Options (Topology license only)

Table 5.1 Network Discovery Configuration Parameters

Field	Purpose
discover physical connectivity (topology) between devices	<p>Select this to discover relationships between devices. If this option is selected, choose one of the following:</p> <p>update topology information for existing devices only</p> <p>If selected, NetVigil updates information about the relationships between provisioned devices, but does not discover new devices</p> <p>discover new devices and new/updated topology</p> <p>If selected, NetVigil discovers both devices and relationships between devices</p>
start discovery from following "seed" router	<p>Select this option to limit the scope of discovery to devices within a certain number of hops from the specified router. If selected, you must specify the seed router IP address and maximum number of hops. For additional information see Section 5.1.1, "Configuring Scope of Discovery" on page 62.</p>

3. Click **Run Discovery**. While discovery is in progress, the Network Discovery Status page periodically refreshes the status display. Discovery may take several minutes to complete, up to several hours in large networks with tens of thousands of devices.
4. If devices are discovered, the Network Discovery Results page displays them, sorted by device type. (Devices with an unrecognized type are listed as **Type: Unknown/Other**.) To provision discovered devices, select the **Department** to which you want to assign the devices and the devices that you want to provision, and then click **Continue**.
5. The Discovery Topology page displays discovered devices in a hierarchy of expandable folders. If a device has multiple parents, it is listed under all of its parents.
Review your selections. If you are satisfied with them, click **Provision Devices**. After the operation is complete, the Network Discovery Status window displays a message indicating that the devices were successfully provisioned. For each provisioned device, NetVigil creates ICMP ping tests (packet loss and RTT).

NOTE: Devices that are already provisioned (with the same name) are not created again.

If you just want to update the topology (dependencies) for provisioned devices, then remember to set the option 'Update topology for provisioned devices only' in the scope configuration as described above.

The screenshot shows the 'Network Discovery Results' page. At the top, there is a navigation bar with 'discover' highlighted. Below the navigation bar, the text reads: 'The following devices were discovered at the specified location. Please choose the department to which you want to provision devices. To prevent specific devices from being provisioned, deselect individual device names or device types.'

The main content area is titled 'Provision Devices In This Department: ITdept_NY' and 'Enable Smart Notification: [checked]'. It displays five categories of devices, each with a list of discovered items and checkboxes for 'Ping', 'Snmp', 'WMI', and 'Port':

- Type: Windows:** ip_192.168.1.154, ip_192.168.1.160, ip_192.168.1.202, ip_192.168.1.203, lab3. Checkboxes: Ping [checked], Snmp [checked], WMI [checked], Port [unchecked].
- Type: Linux/Other Unix:** ecos, ip_192.168.1.156. Checkboxes: Ping [checked], Snmp [checked], Port [checked].
- Type: Printer:** ip_192.168.1.10, ip_192.168.1.11. Checkboxes: Ping [checked], Snmp [unchecked], Port [unchecked].
- Type: Switch/Hub:** sw00.corp.fidelia.com. Checkboxes: Ping [checked], Snmp [checked], Port [unchecked].
- Type: Other/Unknown:** ip_192.168.1.1, ip_192.168.1.150, ip_192.168.1.151, ip_192.168.1.155, ip_192.168.1.206. Checkboxes: Ping [checked], Snmp [unchecked], Port [unchecked].

At the bottom of the interface are three buttons: 'Continue', 'Delete', and 'New Discovery'.

5.1.2 Manual Batch Creation of Devices and Tests

You can add devices and tests using the web interface. However, for bulk additions or changes, NetVigil includes tools to provision large numbers of devices into the provisioning database via the BVE API. The tool will also automatically discover available network interfaces, system resources, various application services, etc. on the devices, and using the default test threshold values, automatically create the tests in the system so that you can be up and running in a very short period of time.

Before using the bulk import tool (`provisionDevices.pl`), make sure that all necessary Departments and admin/end-user logins have been created. The import tool is meant to be used for importing devices for

one Department at a time. For each such Department create a text file (e.g. `network_devices.txt`) and add device information (one device per line) in the following format:

```
device_name device_address device_type snmp_community
```

Where

- `device_name` is either the FQDN or a descriptive name of the device.
- `device_address` is the ip address of the device. This should be in dotted-quad (`n.n.n.n`) notation
- `device_type` is one of
 - ▶ UNIX
 - ▶ NT
 - ▶ ROUTER
 - ▶ SWITCH
 - ▶ UNKNOWN (determine automatically)
- `snmp_community` is the snmp community string of the device, if the device supports snmp. This information is used to automatically discover network and system resources.

Devices are imported for one logical location at a time also. So make sure to include devices in an import file that are meant to belong to the same Department and monitored from the same location. Once this import file is ready, use the `provisionDevices.pl` tool to proceed with the import. General syntax of the tool is:

```
NETVIGIL_HOME/utils/provisionDevices.pl --host=prov_host \  
--user=login_id --password=login_password --file=import_file \  
--location=location_name
```

Where

- `prov_host` is the fqdn/ip address of host where the BVE socket server is running. Usually you would provision devices from the same host, so this would be `localhost`.
- `login_id` and `login_password` are the userid and corresponding password for an end-user, who is a member of the specific Department you want the newly provisioned devices to belong to.
- `import_file` is the text file containing the device information as outlined above.

- `location_name` is the name of the location as defined in the database. The default NetVigil installation is pre-configured with location name **Default Location**.

As the device is created and tests are discovered and added to the provisioning database, information will be printed.

Example: Batch Creation of Tests

```
.....
reading contents of import file '/tmp/import.txt' ...
connecting to provisioning host ...
succesfully logged in as user test with supplied password
creating new device 'my_test_host' (192.168.100.100)
attempting to perform auto-provisioning for 'port' tests ...
  created 'port' test for 'HTTP'
  created 'port' test for 'POP3'
  created 'port' test for 'HTTPS'
  created 'port' test for 'IMAP'
attempting to perform auto-provisioning for 'snmp' tests ...
  created 'snmp' test for 'hme0 Status'
  created 'snmp' test for 'hme0 Util In'
  created 'snmp' test for 'hme0 Util Out'
  created 'snmp' test for 'hme0 Err In'
  created 'snmp' test for 'hme0 Err Out'
  created 'ping' test for 'Packet Loss'
  created 'ping' test for 'Round Trip Time'
data import complete in 0 days, 0:00:31
```

.....
NOTE: Tests are created based on thresholds and intervals defined in `TestTypes.xml`, so if you want to make changes to the defaults, make sure to edit this file **before** starting the import task.

