Supported Discovery Methods

When you perform a discovery, you can choose any or all of the following discovery methods:

- SNMPv1/v2c device polling as described in [SNMP](#).
- SNMPv3 device polling as described in [SNMP](#).
- CLI device querying as described in [CLI](#).
- ICMP Ping Sweep and Smart Subnet Ping Sweep as described in [ICMP](#).
- TCP as described in [TCP](#).
- NetBIOS as described in [NetBIOS](#).

These methods actively scan predefined networks and probe IP addresses. The appliance listens for responses from the IP addresses as proof of activity. The IP discovery scans through the specified network ranges and probes IP addresses (except for the network, broadcast, and multicast address types) in each network, including the /31 and /32 subnets. Note that addresses in the /31 and /32 subnets can be used only as source addresses for point-to-point links and loopbacks. In these cases, no broadcast or network addresses exist in the /31 and /32 subnets, and the appliance can discover source addresses in these subnets.

### SNMP

**Note:** Infoblox does not recommend using vendor default SNMP credentials on network devices. Should you need to use vendor defaults for a given device type, you enter those values in the list of SNMP credentials on the Grid Master.

Network Insight supports discovery of devices and networks through SNMPv1/v2c and through SNMPv3 protocols. Discovery acquires information from standard SNMP MIB object IDs (OIDs) to correctly identify and catalogue devices. You enter or import lists of SNMP credentials with which the appliances query devices on the network to perform discovery.

SNMPv1 and SNMPv2c protocols are combined into a set termed SNIPv1/v2 for discovery. SNIPv1/v2 discovery requires standard read community strings to be stored on the Grid Master. Accounts using SNMPv3 use a standard suite of authentication and security protocols. If Network Insight uses SNMPv3 to collect data from devices supporting the protocol, you can define specific user credentials with combinations of authentication and protocol support, and the unique keys for each protocol. Network Insight also supports multiple entries for the same username string, enabling checking of similar SNMPv3 credentials that use different authentication and security protocols.

Some devices found by discovery may not have known SNMP credentials or credentials that are entered into the sets of SNMP credentials defined for discovery.

**Note:** SNMP Credentials from the Grid or from the Member credential list are always tried in the specified order unless a credential is associated with a host, fixed address or reservation being discovered.

### CLI

**Note:** CLI is optional for discovery but is required for all Port Control operations. Discovery can perform CLI data collection to collect information for specific device types. SNMP is required for all device discovery.

Network Insight enables the use of dynamically created and closed Telnet and SSH command-line sessions to log in, query, and configure ports using each device's command-line syntax. Network Insight does so without requiring extensive configuration from the user. You need to provide known admin account login information and any Enable passwords for devices in the networks to be discovered. CLI credentials are required for port reservation and port configuration operations under Grid Manager. You enter CLI credentials under Grid Discovery Properties (Grid → Grid Manager → click Edit → Grid Discovery Properties) to be inherited by discovery Probe members, and as necessary for each discovery Probe member. You can also override them for individual IPAM objects (fixed addresses, hosts and IPv4 reservations) and test the CLI credentials against devices for correctness. For more information, see [Testing SNMP and CLI Credentials](#).

### ICMP

Discovery uses different variations of Ping traces to perform higher-performance, brute-force device discovery. ICMP is the last resort when devices do not support SNMP management protocols or an SNMP credential is lacking.

The ICMP Smart Ping Sweep option enables brute-force subnet Ping sweeps on IPv4 networks. Subnet ping sweeps are used as a last resort in the discovery process. A subnet ping sweep is performed if Network Insight is unable to identify any network devices in a given subnet. Subnet ping sweeps are performed no more that once per day, and will end the ping sweep on a given subnet once Network Insight discovers a network device and is able to collect data from it. You can configure the timeout value (Ping Sweep Timeout) and the number of attempts (Ping Sweep Attempts).

**Note:** Smart subnet ping sweeps are not performed on subnets larger than /22. Ping sweeps of any kind do not apply on IPv6 networks because of the greater scale of network addresses in the IPv6 realm.

Complete Ping Sweep differs from the Smart Subnet ping sweep in the following ways:

- The discovery ping sweep runs only against the specified range.
The sweep runs regardless of the range size.
The sweep runs regardless of the number of discovered devices within the specified range.

Discovery also performs automatic Ping traceroutes when needed for path collection. Path collections run without user intervention or configuration.

TCP

TCP scanning probes each active host on a list of TCP ports using TCP SYN packets. This method detects all active hosts that generate SYN ACK responses to at least one TCP SYN. The discovery can determine the OS on a host by analyzing how the host reacts to the requests on opened and closed ports. It then uses the TCP fingerprints to guess the OS. To obtain a TCP fingerprint, IP discovery provides two scanning techniques, SYN and CONNECT.

When you use the SYN technique, the discovery sends a TCP SYN packet to establish a connection on a TCP port. If the port is open, the host replies with a SYN ACK response. The discovery does not close the port connection.

The CONNECT technique is a three-way TCP handshake. The discovery starts with the same process as the SYN technique by sending the TCP SYN packet. A response containing a RST flag indicates that the port is closed. If the host replies with a SYN ACK response, discovery sends a RST packet to close the connection. If there is no reply, the port is considered filtered. TCP scanning is a deliberate and accurate discovery method, enabling detection of all active hosts on a network provided that there are no firewalls blocking TCP packet exchanges.

You can choose the TCP ports and the TCP scanning technique in the Grid Discovery Properties editor. This method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: The discovery returns the MAC address only if the Probe member running the discovery is on the same discovered network.
- **OS**: This is set to the highest probable OS reported in the response.

To use the TCP discovery method, the TCP port and a specific set of ports between the Probe member and the discovered networks must be unfiltered. The default set of ports is defined by the factory settings.

TCP Port Scanning

By enabling port scanning, Network Insight probes the list of TCP ports enabled in the Advanced tab, to determine whether they are open. You can control some settings for port scanning behavior, including the choice of a TCP scanning technique.

- **Profile Device**: If enabled, Network Insight attempts to identify the network device based on the response characteristics of its TCP stack, and uses this information to determine the device type. In the absence of SNMP access, the Profile Device function is usually the only way to identify devices that do not support SNMP. If you disable Profile Device, devices accessible via SNMP are still correctly identified; all other devices are assigned a device type of Unknown. Profile Device is disabled by default for discovery polling.

The Profile Device option uses the editable list of TCP protocol ports from the Grid Discovery Properties –> Polling –> Advanced tab as its profile, and polls each of the ports enabled in that list, using the configured timeout value and the number of polling attempts for each port.

For more information, see Defining Seed Routers for Probe Members.

Should you disable Port Scanning, discovery attempts no port probes other than SNMP on any device.

NetBIOS

The NetBIOS method queries IP addresses for an existing NetBIOS service. This method detects active hosts by sending NetBIOS queries and listening for NetBIOS replies. It is a fast discovery that focuses on Microsoft hosts or non-Microsoft hosts that run NetBIOS services.

NetBIOS discovery returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: Listed only if the discovered host is running Microsoft, otherwise blank.
- **OS**: This value is set to Microsoft for an active host that has a MAC address in the NetBIOS reply.
- **NetBIOS name**: This value is set to the name returned in the NetBIOS reply.

To use the NetBIOS discovery method, ports 137 (UDP/TCP) and 139 (UDP/TCP) between the Grid member performing the discovery and the target networks must be unfiltered.

The following table summarizes the supported discovery methods:

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Returned Data</th>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
</table>
| Smart IPv4 Subnet Ping Sweep | • IP address  
• MAC address | Apply on known subnetworks on which no devices are readily found. Limited to networks of /22 and smaller. | ICMP echo request and reply. |
| Complete Ping Sweep | • IP address  
• MAC address | Last resort for discovery. Use ICMP for a rough and fast discovery. Enables path tracing. | ICMP echo request and reply, ICMP traceroute. |
| NetBIOS | • IP address  
• MAC address  
• OS  
• NetBIOS name | Use NetBIOS for discovering Microsoft networks or non-Microsoft networks that run some NetBIOS services | NetBIOS query and reply. |
<table>
<thead>
<tr>
<th><strong>TCP</strong></th>
<th>IP address</th>
<th>MAC address</th>
<th>OS</th>
<th>Use TCP for an accurate but slow discovery</th>
<th>TCP SYN packet and SYN ACK packet.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Scanning/Profile Device</strong></td>
<td>Open and Closed TCP ports</td>
<td>IP Address</td>
<td></td>
<td>Disabled by default, use for non-SNMP devices.</td>
<td>Scans specified list of TCP ports, using TCP SYN packet.</td>
</tr>
<tr>
<td><strong>SNMPv1/v2</strong></td>
<td>Open and Closed TCP ports</td>
<td>IP Address</td>
<td>System Description</td>
<td>System Up Time</td>
<td>Routing Neighbors</td>
</tr>
<tr>
<td><strong>SNMPv3</strong></td>
<td>Similar data set to SNMP</td>
<td>May be used instead of, or in combination with, SNMP</td>
<td>Requires correctly defined admin login tuples and Enable passwords where needed for device types.</td>
<td>You may test credentials against devices and assign CLI credentials to individual objects, overriding Grid-level and Network-level credential settings.</td>
<td>Uses standard device-language scripts and configured Telnet or SSH connection settings to collect discovery data.</td>
</tr>
</tbody>
</table>
| **CLI (Device Command-Line by Telnet or SSH)** | Add the VMware vSphere servers on which you want to perform the vDiscovery. For information about how execute a vDiscovery, see Configuring vDiscovery Jobs. | | | | | | | | The appliance communicates with the vSphere servers to collect discovery data on virtual machine instances. |}

...