Supported IP Discovery Methods

When you perform an IP discovery, you can choose one of the following discovery methods:

- **ICMP** as described in [ICMP](#).
- **NetBIOS** as described in [NetBIOS](#).
- **TCP** as described in [TCP](#).
- **Full** as described in [Full](#).

These methods actively scan predefined networks and probe IP addresses. The Grid member listens for responses from the IP addresses as proof of activities. 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 the possible addresses in the /31 and /32 subnets can be used only as source addresses for point-to-point links. In these cases, there are no broadcast or network addresses in the /31 and /32 subnets, and the appliance can discover source addresses in these subnets.

**ICMP**

This method detects active hosts on a network by sending ICMP echo request packets (also referred to as pings) and listening for ICMP echo responses. The ICMP discovery is a simple and fast discovery that detects whether an IP address exists or not. It returns only the IP address and MAC address (only if the Grid member running the discovery is on the same discovered network) of a detected host. The ICMP discovery might miss some active hosts on the network due to security measures that are put in place to block ICMP attacks.

You configure the timeout value and the number of attempts in the Discovery Manager wizard. The ICMP discovery 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 Grid member running the discovery is on the same discovered network.

To use the ICMP discovery method, the ICMP protocol between the Grid member performing the discovery and the target networks must be unfiltered.

**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.

You configure the timeout value and the number of attempts in the Discovery Manager wizard. This method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: Only if the discovered host is running Microsoft.
- **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.

**TCP**

The TCP discovery 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. If the host replies with a SYN ACK response, the discovery then sends a RST packet to close the connection. If the response contains a RST flag, it indicates that the port is closed. If there is no reply, the port is considered as filtered. The TCP discovery is a deliberate and accurate discovery method. It can basically detect all active hosts on a network provided that there are no firewalls implemented on the network.

You can select the TCP ports, the TCP scanning technique, and configure the timeout value and the number of attempts in the Discovery Manager wizard. 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 Grid 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 Grid member and the discovered networks must be unfiltered. The default set of ports is defined by the factory settings.

**Full**

The full discovery method is a combination of an ICMP discovery, a NetBIOS discovery, a TCP discovery, and a UDP scan. This method starts by sending an ICMP echo request. If no IP address on the network responds to the ICMP request, the discovery ends. If there is at least one response to the ICMP echo request, a NetBIOS discovery starts. A TCP discovery then follows by skipping through the active hosts that the NetBIOS discovery detects. The TCP discovery also handles the NetBIOS-detected hosts that have no MAC addresses. This method also performs a UDP scan to determine which UDP ports are open.

You configure the timeout value and the number of attempts in the *Discovery Manager* wizard. The full discovery method returns the following information for each detected host:

- IP address
- MAC address
- OS
- NetBIOS name

To use the full discovery, all the filter and firewall requirements in the ICMP, NetBIOS, and TCP discovery methods apply.

The following is a summary of the supported IP discovery methods:

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Returned Data</th>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>• IP address</td>
<td>Use ICMP for a rough and fast discovery</td>
<td>ICMP echo request and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS</td>
<td>• IP address</td>
<td>Use NetBIOS for discovering Microsoft networks or non-Microsoft networks that run some NetBIOS services</td>
<td>NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>• IP address</td>
<td>Use TCP for an accurate but slow discovery</td>
<td>TCP SYN packet and SYN ACK packet</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full</td>
<td>• IP address</td>
<td>Use Full for a general and comprehensive discovery</td>
<td>1. ICMP echo request and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td>2. NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td>3. TCP SYN packet and SYN ACK packet</td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The method you select to run an IP discovery determines the kind of information the discovery returns and the time it takes to complete an IP discovery. If time is a concern, the following are factors you may consider when configuring an IP discovery:

- The timeout value
- The number of attempts
- The number of ports the discovery scans
- The size of network you want to discover