Discover new devices by IP address

Published: 2020-02-23

The ExtraHop Discover appliance automatically discovers devices that are communicating on the locally monitored network. This identification process is known as device discovery. After a device is discovered, you can search for the device and analyze device metrics in the Discover or Command appliances.

By default, Discover by IP is enabled, which means that devices are discovered when the ExtraHop system detects a response to an Address Resolution Protocol (ARP) request for an IP address. This method is also known as L3 discovery mode.

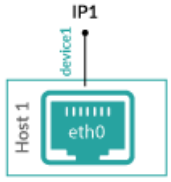
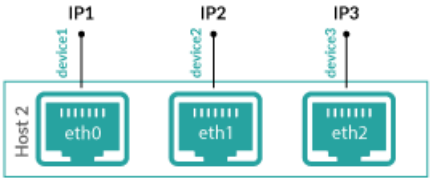
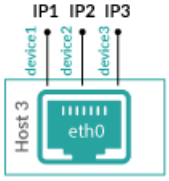
Note: Packet brokers can filter ARP requests. The ExtraHop system relies on ARP requests to associate L3 IP addresses with L2 MAC addresses.

If the ExtraHop system detects an IP address that does not have associated ARP traffic, that device is considered a remote device. Remote devices are not automatically discovered, but you can configure a remote range of IP addresses for discovery.

You can disable Discover by IP and only discover devices by unique MAC address. This method is known as L2 discovery mode. It is important to note that disabling Discover by IP changes the number of devices that are discovered by the ExtraHop system. The following table shows two Discover by IP scenarios, three common server NIC configurations, and the number of L3 devices (by IP address) and L2 devices (by MAC address) that are discovered for each scenario and configuration.

Note: Learn more about finding devices in the ExtraHop system.

Table 1: Discover by IP

Diagram	Enabled	Disabled
 Single NIC with single IP address	2 devices discovered: • eth0 device (L2) • IP1 device (L3)	1 device discovered: • eth0 device (L2)
 Multiple NICs, each with their own IP address	6 devices discovered: • eth0 device (L2) • IP1 device (L3) • eth1 device (L2) • IP2 device (L3) • eth2 device (L2) • IP3 device (L3)	3 devices discovered: • eth0 device (L2) • eth1 device (L2) • eth2 device (L2)
 Single NIC, multihomed with multiple IP addresses	4 devices discovered: • eth0 device (L2) • IP1 device (L3) • IP2 device (L3) • IP3 device (L3)	1 device discovered: • eth0 device (L2)

When Discover by IP is enabled, L2 devices are considered parents of their L3 devices. You can view metrics associated with each IP address by L3 device. When Discover by IP is disabled, only L2 devices are discovered, and metrics associated with those IP addresses are merged into the L2 device.

Remote discovery

The ExtraHop system automatically discovers local L3 devices based on observed ARP traffic that is associated with IP addresses. If the ExtraHop system detects an IP address that does not have ARP traffic, the ExtraHop system considers that IP address to be a remote device. Remote devices are not automatically discovered unless you configure a remote IP address range for remote discovery. When the ExtraHop system sees traffic associated with the range of remote IP addresses, it will discover those devices.

Note: If you have a proxy ARP configured in your network, the ExtraHop system might automatically discover remote devices. For more information, see this ExtraHop forum post.

Remote discovery is useful in the following scenarios:

- Your organization has a remote office without an on-site ExtraHop appliance but users at that site access central data center resources that are directly monitored by an ExtraHop appliance. The IP addresses at the remote site can be discovered as devices.
- A cloud service or other type of off-site service hosts your remote applications and has a known IP address range. The remote servers within this IP address range can be individually tracked.

Important: Devices discovered through remote discovery count towards your licensed device limit.

Add a remote IP address range

You can configure the ExtraHop system to automatically discover devices on remote subnets by adding a range of IP addresses.

Important considerations about remote discovery:

- Only public-facing IP addresses are discovered and visible in the ExtraHop appliance. Private IP addresses, such as those on a private subnet, behind a router, or behind a NAT device, are not visible to the ExtraHop system.
- Additionally, L2 information, such as device MAC address and L2 traffic, is not available if the device is on a different network from the one being monitored by the ExtraHop appliance. This information is not forwarded by routers, and therefore is not visible to the ExtraHop appliance.
- Exercise caution when specifying CIDR notation. A /24 subnet prefix might result in 255 new devices discovered by the ExtraHop system. A wide /16 subnet prefix might result in 65,535 new devices discovered, which might exceed your device limit.

1. Log into the Admin UI on the Discover appliance.
2. In the System Configuration section, click **Capture**.
3. Click **Discover by IP**.
4. The Enable checkbox is selected by default. If the checkbox is deselected, select **Enable**.
5. In the Remote Discovery section, type the IP address in the IP address ranges field. You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.

   Important: Every actively communicating remote IP address that matches the CIDR block will be discovered as a single device in the ExtraHop appliance. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.
6. Click the green plus icon (**+**) to add the IP address. You can add another IP address or range of IP addresses by repeating steps 5-6.

Important: The capture must be restarted when removing IP address ranges before the changes take effect. We recommend deleting all entries before restarting the capture. The capture does not need to be restarted when adding IP address ranges.