Active Discovery

Active Discovery

Active Discovery is a feature to enforce data enrichment on the network. As opposed to passive traffic capture principles on which Cisco Cyber Vision is relying on and was originally built around, Active Discovery is an optional feature that explores traffic in an active way. The reason is, some components are sometimes not found by Cisco Cyber Vision because those devices haven't been communicating from the moment the solution started to run on the network. Moreover, some information like firmware version can be difficult to obtain because they are not exchanged often between components.

With Active Discovery enabled broadcast and/or unicast messages will be sent to the targeted subnetworks or devices through sensors to speed up network discovery. Then, returned responses will be analyzed and tagged as Active Discovery. Thus, components and activities will be clarified with additional and more reliable information than what is usually found through passive DPI.

The following protocols are supported:

Broadcast	Unicast
EtherNet/IP	EtherNet/IP
Profinet	SiemensS7
SiemensS7	SNMPv2c
ICMPv6	SNMPv3
	WMI

• Active Discovery is available on the following devices:

• Cisco Catalyst IE3300 10G Rugged Series Switch

• Cisco Catalyst IE3400 Rugged Series Switch

• Cisco Catalyst IE9300 Rugged Series Switch

• Cisco Catalyst 9300 Series Switch

- Cisco Catalyst 9400 Series Switch

- Cisco IC3000 Industrial Compute Gateway

- Cisco IR8340 Integrated Services Router Rugged

Active Discovery jobs can be launched at fixed time intervals or just once.

For more information and instructions on how to configure Active Discovery in Cisco Cyber Vision, refer to the Cisco Cyber Vision Active Discovery Configuration Guide.