Cyber Vision Distributed Edge Active Discovery

Understanding the real implications of using active discovery for identifying industrial assets

Over the last few years the market has come to accept that **Passive Discovery** of industrial assets through deep pack inspection (DPI) of industrial control system (ICS) protocol traffic is not enough to get full visibility to the control system. Gaps have to be filled through **Active Discovery**. As a result, today almost every ICS detection vendor augments their Passive Detection solution with some sort of bolt-on Active Discovery capability.

As ICS detection solutions are seeing increased adoption in industrial networks, one aspect has proved challenging for current offerings in the market: Gaining *100% visibility* of assets by using Active Discovery mechanisms that are *non-disruptive*.

Issues and Misconceptions

While many industrial customers are now opening up to deploying Active Discovery as a means to get better visibility into their networks, there are two main issues that plague most solutions.

Centralized active discovery solutions are still disruptive and can result in unexpected crashes

The argument made by most vendors is that their solutions only use valid protocol commands supported by the industrial assets. These commands are similar to what the ICS vendor products use for asset management and are hence non-disruptive.

In reality, the reason why old ICS devices are susceptible to crashes during active scanning is because they have limited processing power for network functions and get overwhelmed when repeated connection attempts are made for communication. So, the reason for the crashes has less to do with valid or invalid commands being used but rather a factor of how many connection attempts are being made by the active discovery solution.

From a network hygiene standpoint, it is not uncommon to see industrial networks badly designed with all devices being addressed from a flat /16 IP subnet. Most ICS detection solution available in the market today are based on a centralized architecture where traffic mirroring (SPANing) is used to feed an appliance (or a software VM) located at Level-3 of the Purdue model that does the Passive Discovery.

© 2020 Cisco and/or its affiliates. All rights reserved.

When the bolt-on Active Discovery capability of these solutions initiate a scan from this central location, they need to **cycle through a range of IP address** within the scan range. Now, one of the first things that needs to happen to establish communication for Active Discovery is to resolve ARP. These ARP requests are seen by all devices within the flat network and it is the processing of the barrage of ARP requests that can overwhelm the networking stack on legacy ICS devices causing them to crash. While this is not the only reason for legacy devices crashing, it is quite often the primary cause.

In addition, in most multi-vendor ICS environments, centralized discovery solutions sitting at Level-3 of the Purdue model are not aware of the specific protocol being used at the Level 0-2 edge. This requires the scanning process to **cycle through a range of ICS protocols** (CIP, PROFINET, Modbus, etc.) until the device responds based on the protocol it supports. This results in unnecessary communication attempts that can also overwhelm the processing power of legacy devices causing disruption.

Centralized active discovery solutions cannot penetrate NAT boundaries

Industrial networks are usually built up of units like cells, zones, bays, etc. that are comprised of machines or control systems supplied by machine builders and system integrators. It is common practice for these machines especially in discrete manufacturing to be built in a standardized manner with ICS devices across machines configured in a cookie-cutter approach with repeating IP addresses. Consequently, industrial networks are rife with network address translation (NAT) being used to allow the operations and control systems located in the Level-3 to communicate with ICS devices sitting in the lower levers with duplicate IP addresses.

When it comes to address translation only a small fraction of ICS devices (like PLC, HMI, RTU, etc.) actually communicate with the site operations layer, and only those devices IP address are translated at the NAT device. The implication of this is that centralized Active Discovery solutions cannot communicate with the vast majority of ICS devices (like IO, drives, safety controllers, relays, IED) sitting below the NAT boundary whose IP addresses are not translated. In the auto manufacturing industry as an example it is typical for less than 17% of devices in level 0-2 to be visible to a centralized Active Discovery solution. This results in a 83% gap in visibility!

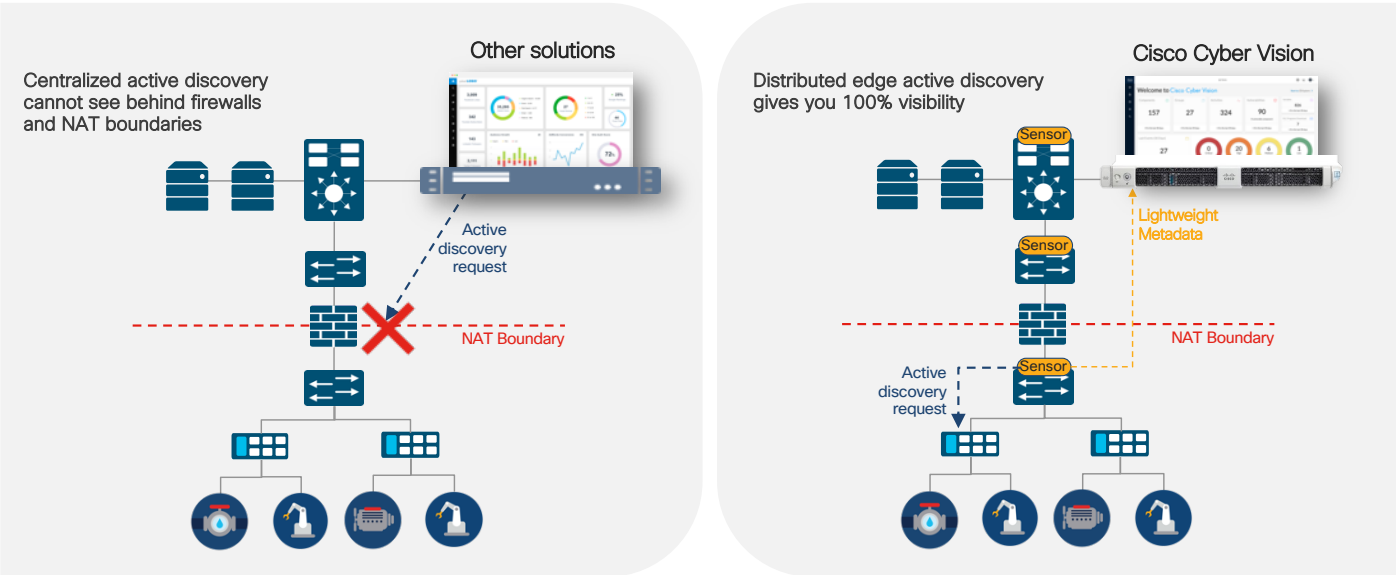

Figure 1. Cyber Vision sensors embedded in industrial network equipment at the edge are responsible for sending active discovery messages, hence capable of reaching 100% of industrial devices.

© 2020 Cisco and/or its affiliates. All rights reserved.

Centralized discovery solutions involve huge networking costs

While the discussion here is on drawbacks of centralized Active Discovery solutions, it also exposes a key point that many customers fail to recognize when choosing Passive Detection solutions as well. That is the fact that control loops are highly localized to machines and processes, and to get full visibility to the ICS one must inspect traffic at the edge of the network where the devices connect.

In a centralized Passive Discovery solution, the cost of standing up a out-of-band SPAN collection network involving cabling, collection switches, power etc. to get visibility to this access layer far outweighs the cost of the centralized Passive Discovery solution itself. Many Infosec departments discover this only after choosing a Passive Detection solution and the projects often stall at deployment phase as neither the IT nor the line of business is willing to foot the bill for the SPAN collection infrastructure.

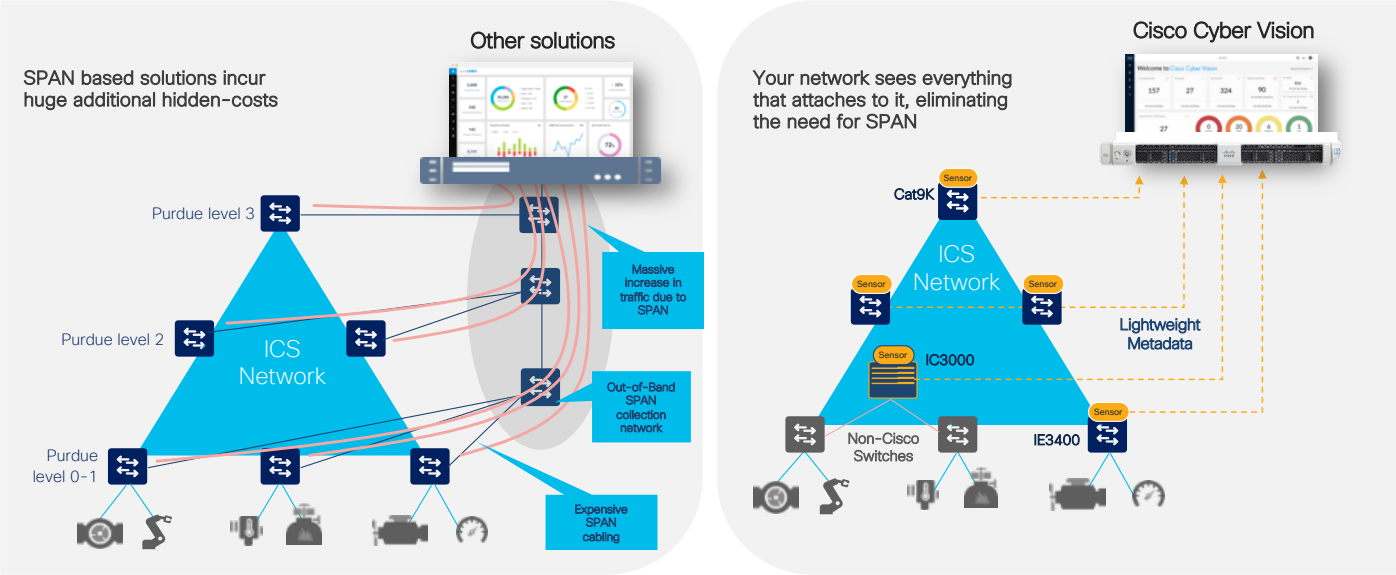

Figure 2. Distributed edge active discovery dramatically reduces network costs and complexity.

Cisco Distributed Edge Active Discovery

Cisco Cyber Vision is the only two-tier ICS detection solution in the market where there is a clean separation between deep packet inspection of ICS traffic and the analytics of data extracted from deep packet inspection. This allows for the **Cyber Vision Sensor** which performs the deep packet inspection to be embedded as a lightweight software component within the Cisco industrial networking (IE) switches and stream metadata to the **Cyber Vision Center** which performs the analytics. This enables a distributed edge detection solution that eliminates the need for unnecessary collection appliances and expensive SPAN collection networks.

The benefits of Cisco's distributed edge architecture goes far beyond the inherently limited complexity and low total cost of ownership (TCO). It also enables a new Active Discovery technology generation. With Cyber Vision, the **active discovery is initiated by the Cyber Vision Sensor embedded in the Cisco IE switches**, that are distributed at the edge of the industrial network.

The solution does much more than just distributing the initiator of the discovery. The Active Discovery is a **closed-loop system between the Passive and the Active Discovery components**. It works by the Passive Discovery first listening to the traffic on the network and then informing the Active Discovery component on which protocols are present on that section of the network. The Active Discovery component then initiates a

© 2020 Cisco and/or its affiliates. All rights reserved.

broadcast hello request in the semantics of specific ICS protocol at play, and the Passive Discovery component decodes the response from the ICS devices. When needed the Active Discovery component may initiate a unicast command to collect further information from the discovered devices.

Cyber Vision Active Discovery is Non-Disruptive

The fact that the Passive and Active components are embedded on the switches at the very point where the ICS devices connect to the network enables Cyber Vision discovery to be **extremely precise and non-disruptive**. There is no longer a need to enter IP scan ranges nor is there a need to guess which protocol is being used on a specific machine or process at the edge of the network. The intelligence built into the closed-loop system automates the Active Discovery. The user simply has to enable Active Discovery and has full control to activate the capability on a per switch basis if needed.

Cyber Vision Active Discovery is not handicapped by the presence of NAT

As the market leader in industrial networking Cisco recognizes the need for NAT in industrial networks and simplifies the process by providing L2 NAT (mapping between inside and outside IPs bound to MAC address) capability at line rate on the Cisco IE switches. This eliminates the need to additional L3 NAT devices. But regardless of whether L2 or L3 NAT is used, by virtue of the Passive and Active components of the Cyber Vision Sensor being embedded in the IE switches, the Active Discovery is distributed and is initiated from below the NAT layer, and results in **100% visibility to the ICS devices** on the industrial network.

References

https://www.linkedin.com/pulse/scanning-wont-work-ics-dale-peterson

https://www.langner.com/2019/07/the-simple-truth-why-ics-detection-passive-scanning-cant-scale/

Document history

New or revised topic	Described in	Date
Document creation		October 25, 2020

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2020 Cisco and/or its affiliates. All rights reserved.