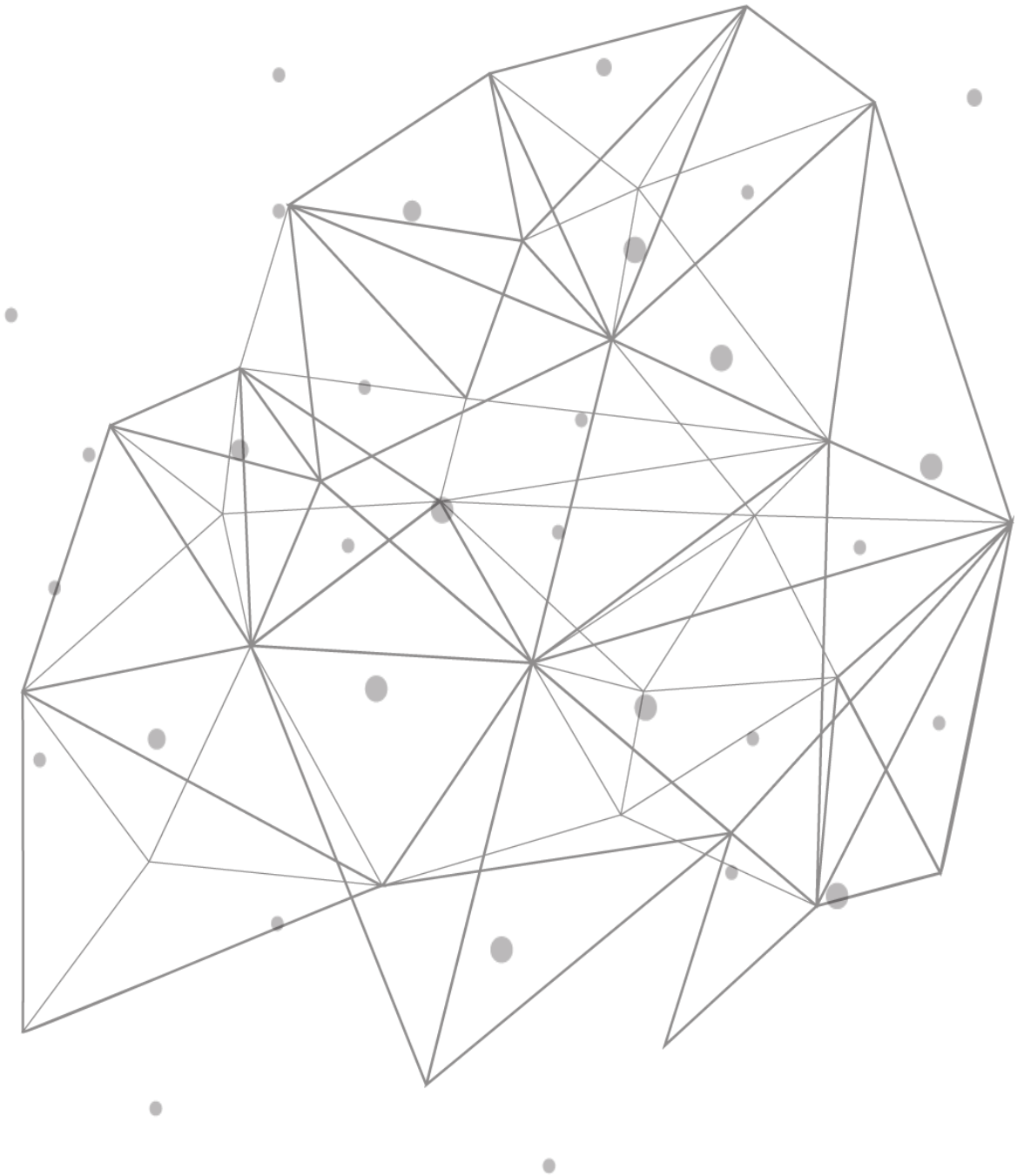
# TCPWave DDI

## Distributed Discovery

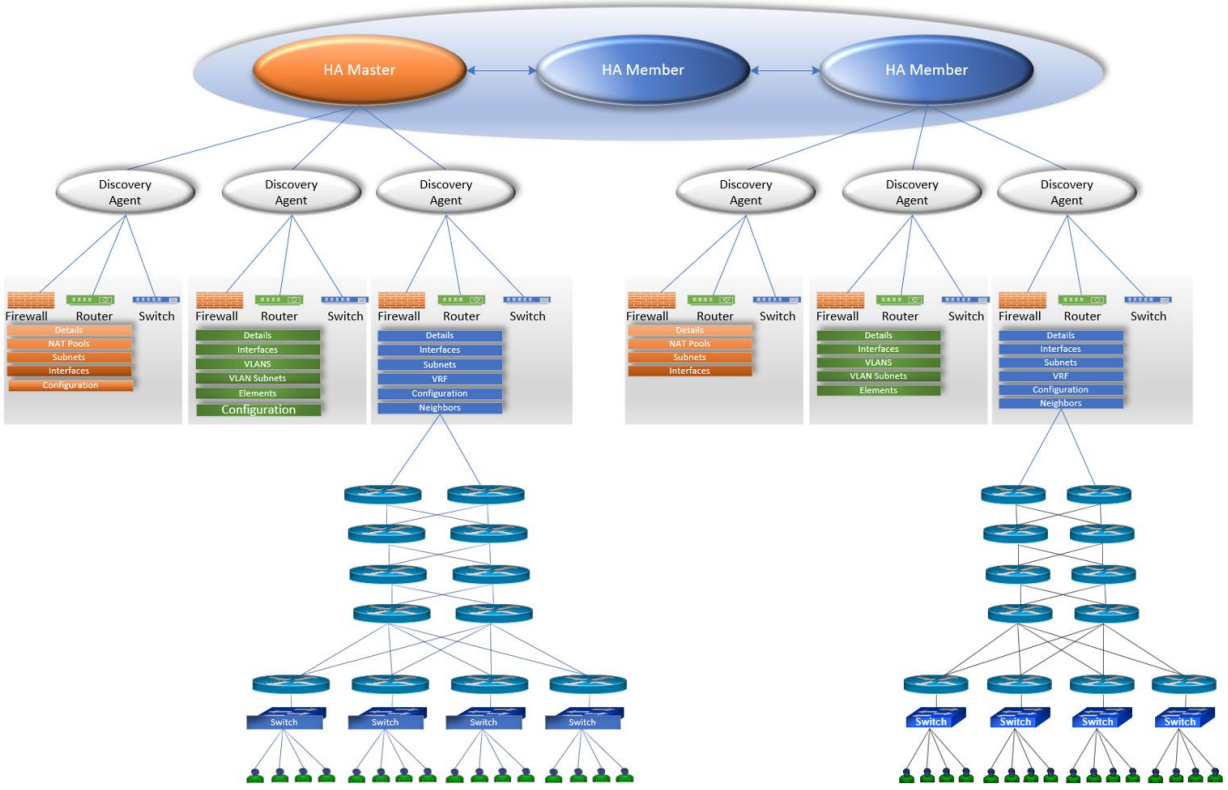


# Introduction

In the digital era, many organizations rely on networks more than ever before, and additionally, with the influx of many digital transformation initiatives, the networks have become more dynamic. It has made it difficult for the organizations to gain visibility into the network topology – which includes devices connected to the network, those devices have access to, and how those devices interact. Manually monitoring your organization's network can lead to inaccuracies due to undetected devices, outdated data, and other common visibility issues. Hence organizations look forward to having a tool that automatically discovers the entire IoT infrastructure, provides a deep insight into one's network's performance, and aids troubleshooting. This white paper provides an insight into TCPWave's Distributed Discovery.

# TCPWave's Distributed Discovery Architecture

Discovery Crawler Engine (DCE) runs on the IPAM/remote appliance or VM instance. DCE makes periodic REST API calls to fetch the configuration instructions from the IPAM master. Once the DCE receives the configuration from the IPAM master and after validating the configurations, DCE checks for the available router or switch to start the discovery process. The configurations are stored in the DB for the systematic discovery process.



DCE uses SNMP, SSH, PING, NMAP, etc., discovery methods to fetch the router or switch configurations and derive appropriate seed routers and connected devices. While crawling the seed router and if DCE identifies any other seed routers connected, the new routers' information is posted to IPAM. IPAM generates the configuration with new routers and decides the next available remote appliance to perform the discovery. DCE identifies connected leaf routers or switches. These details are sent to IPAM to determine the available remotes agent. DCE uses multithreading for crawling multiple routers, switches, and objects. The discovery engine supports detecting hardware of multi-vendors such as Cisco, Juniper, Huawei, Extreme, Arista, FortiGate, etc., The ability to perform the discovery process is controlled by the permissions of the TCPWave Identity Administration module.

## Business Advantages

- It provides end-to-end network visibility that is a proactive solution for the network teams and reduces the mean time to resolution for reactive issues.
- Dive deep into the organization's data by getting a glimpse of the IT infrastructure.
- Monitor faults, availability, and performance of your network devices, ensuring the end-users can always access the applications and services they need.
- It helps to discover various public and private cloud assets.
- It helps track your entire asset landscape that drives business and financial decisions, reduces IT overspending, mitigates potential technology risks, and maintains compliance standards.
- Reduction of repetitive tasks.
- Locate IP addresses and ports.
- It helps to track utilization of ports on each switch and reclaim unused ports using the TCPWave's Switch Port Utilization report.
- Switch port monitoring reduces the risks associated with unused switch ports, that ensures the infrastructure protection that the organizations rely on to facilitate day-to-day workflows.
- It helps to specify exclusion rules to exclude specific IP ranges or routers from the discovery process.
- An alerting mechanism generates when a conflicting network or subnet is detected during the scheduled automatic or on-demand discovery process.
- It helps track ports' utilization on each switch and reclaims unused ports using the TCPWave's Switch Port Utilization report.

- Switch port monitoring reduces the risks associated with unused switch ports, ensuring the infrastructure protection that organizations rely on to facilitate day-to-day workflows.

## Conclusion

TCPWave's Distributed Discovery is a one-stop solution for all organizations. It examines and monitors multi-vendor networks with visually pleasing network insights, the alert mechanism to signal a warning before it is noticed, and sends alerts via messaging platforms email, telegram, slack, etc., based on threshold configuration. Additionally, it improves the organization's security by helping the network teams identify open ports on connected devices that lead to identifying any threats sitting quietly on network infrastructure, poised for a malicious attack. For a quick demo on TCPWave's Distributed Discovery, contact the TCPWave Sales Team.