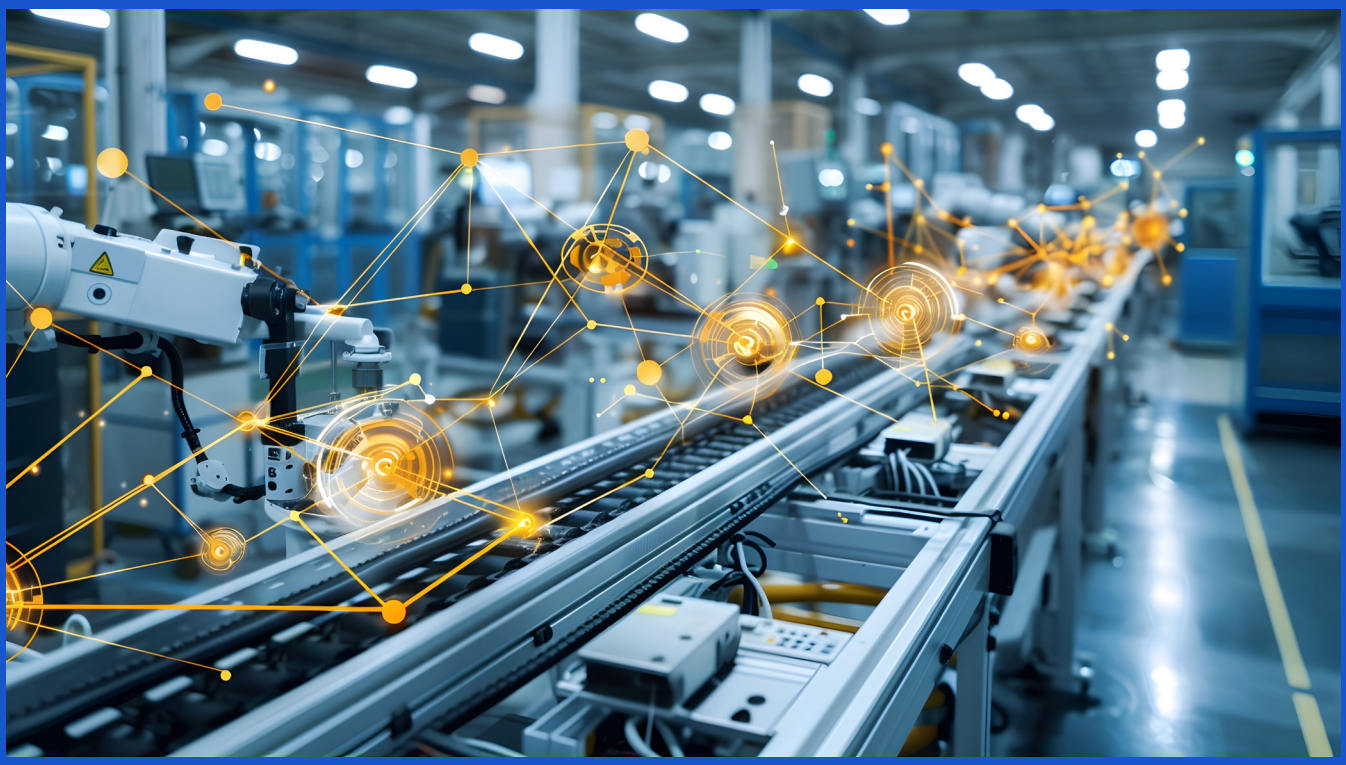
ManageEngine
DDI Central

How DDI solutions benefit the manufacturing sector

Introduction



The manufacturing industry has been growing rapidly through the digitalization of business processes with tools that increase productivity and profit. The Fourth Industrial Revolution (Industry 4.0) encouraged manufacturers to implement automation to their operations and move their software to cloud for simplified management, alongside providing the benefit for employees to connect remotely from anywhere.

Many production tasks are now monitored, managed, and configured through modern networking tools, which means securing the connectivity of the organization and data passing through the network is vital.

Traditional Multi-protocol Label Switching (MPLS) route-based network architecture can be challenging for admins to secure the network, as they are complex to manage and configure. So, manufacturing industry require a DDI network solution comprised of DNS, DHCP and IPAM services.

This white paper shares how DDI solutions solves the manufacturing sectors' network demands, by showcasing key benefits through a product overview, visual insights, and real life use-cases.

Understanding major cyberattacks in the modern manufacturing sector

Cyberattacks are a crucial threat to any industry's network infrastructure, including the manufacturing industry. Manufacturing companies invest in technologies to integrate their information technology (IT) and operation technology (OT) for elevating their operational efficiency.

A survey by TrapX Security in 2020 of 150 cyber and IT professionals directly involved in security strategy, control, and operations, stated that nearly 49% of the organizations have their IT and OT infrastructure tightly integrated.

However, only 41% of organizations employ a robust IT team to protect their OT assets and handle OT related cyberattacks, while the others rely on network technologies or tactics or common network for IT and OT communications.

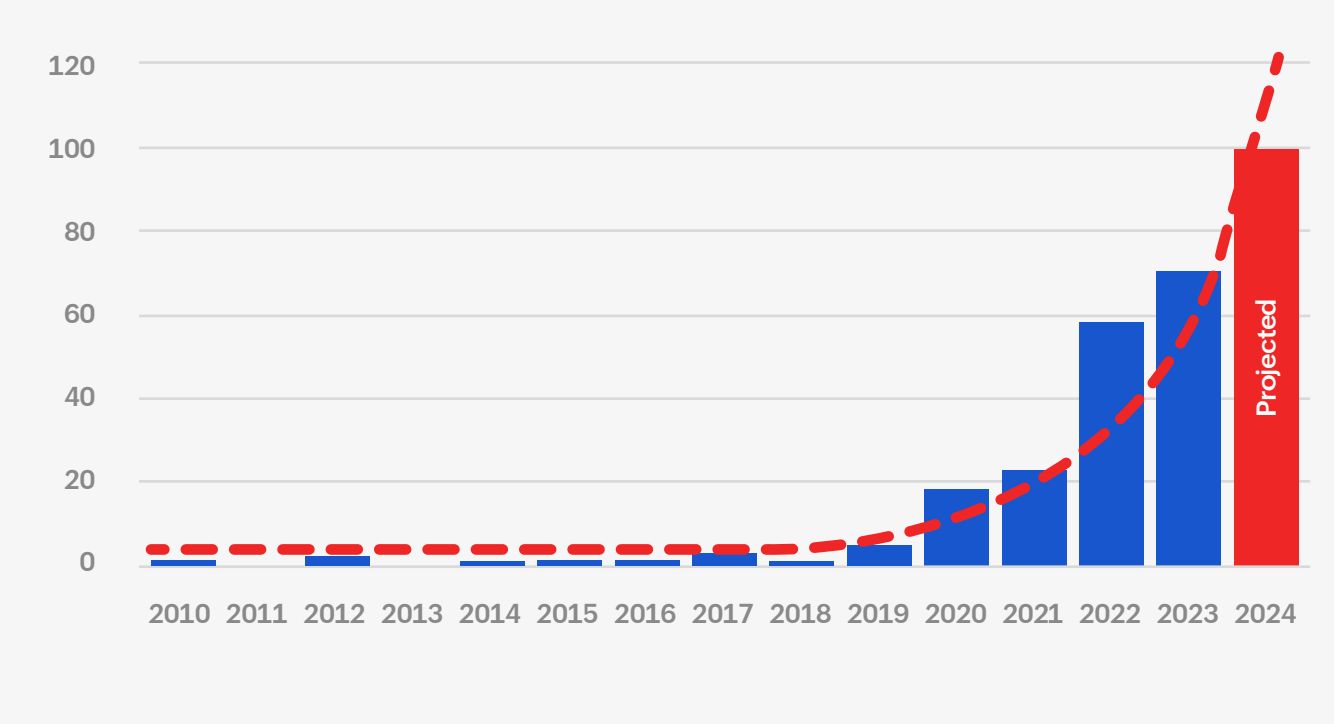
This situation prompted the rapid growth of IT/OT attacks, with 53% of organizations agreeing that their network infrastructure is vulnerable to attacks and many acknowledging that they have suffered some type of cyberattack. IT teams are struggling to manage the increasing number of technologies implemented, leaving them seeking more advanced and adaptive network security solutions.

This situation prompted the rapid growth of IT/OT attacks, with 53% of organizations agreeing that their network infrastructure is vulnerable to attacks and many acknowledging that they have suffered some type of cyberattack. IT teams are struggling to manage the increasing number of technologies implemented, leaving them seeking more advanced and adaptive network security solutions.

Of the organizations surveyed, the need to improve visibility to view malicious OT activities was agreed by 37%, and the need to improve OT focused threat intelligence was agreed by 36%. This survey concludes that manufacturing companies lack visibility to identify threats and resolve them.

When it comes to OT/IT related threats, ransomware remains the most common form of cyberattack in the manufacturing industry.

According to Waterfall's Threat Report published in 2024, more than 68 cyberattacks impacted around 500 sites of manufacturing, and half of these led to production shutdowns, work stoppages, and logistic delays. The report notes that between 2019-2023, cyberattacks have doubled annually—with a growth rate of about 90% each year.



This graph shows that from 2010-2019, we witnessed the doubling of the number of attacks. In 2024, a 19% increase in attacks over the previous year was projected.

In 2024, a 19% increase in attacks over the previous year was projected.

Ransomware accounted for 80%

of cyberattacks in 2023, where the threat actor is known. Most of the attackers tend to hold the confidential data for ransom rather than encrypt systems to hold decryption keys.

Norsk Hydro, a Norwegian aluminum manufacturing company, was hit by the LockerGoga ransomware attack on 2019 that compromised its IT systems across multiple sites, including smelting plants in Norway, Qatar, and Brazil. Norsk Hydro paid a ransom of $71 million to recover its data.

Applied Materials, a multibillion-dollar company that provides technologies to the semiconductor industry, was hit by the supply-chain ransomware attack, while its supplier and partner, MKS instruments, is reported to be the main victim of this attack. This led to a loss of $250 million because of lost sales in the second quarter of 2023.

Networking demands of the modern manufacturing sector

Manufacturing companies facing these cyberthreats and security challenges, require a network solution that can resolve their major networking demands. Key issues that should be addressed include:

Security, regulatory compliance, return on investment, and corporate trust

Manufacturing organizations should enforce cybersecurity protocols to protect their operational data and connected devices on the factory floor. Regulatory compliance, such as adherence to ISO, NIST, or industry-specific standards like ITAR or FDA, is essential to avoid legal liabilities. Investing in solutions benefits manufacturers by ensuring reduced downtime, faster resolving, and robust security. Earning and maintaining corporate trust involves transparency, consistent performance, and secure handling of customer and partner data across all operations.

Business connectivity with multiple branches and offices

Seamless connectivity across multiple branch offices and sites is critical to ensure synchronized operations and real-time analytics for data driven decision-making. Modern manufacturers often implement SD-WAN, VPNs, and cloud-based communication platforms to unify geographically dispersed teams and systems. They need to implement a solution that supports connectivity for centralized monitoring across different sites.

Structured IP address plan with complete network visibility

A structured IP address scheme is crucial for network efficiency, scalability, and security. It enables better segmentation for different departments comprised of different IoT devices and machines to reduce network risks. IT teams need complete insights over device behaviors, traffic flows, and potential vulnerabilities for instant identification of malicious activities.

Monitor real-time network traffic for prioritizing and routing

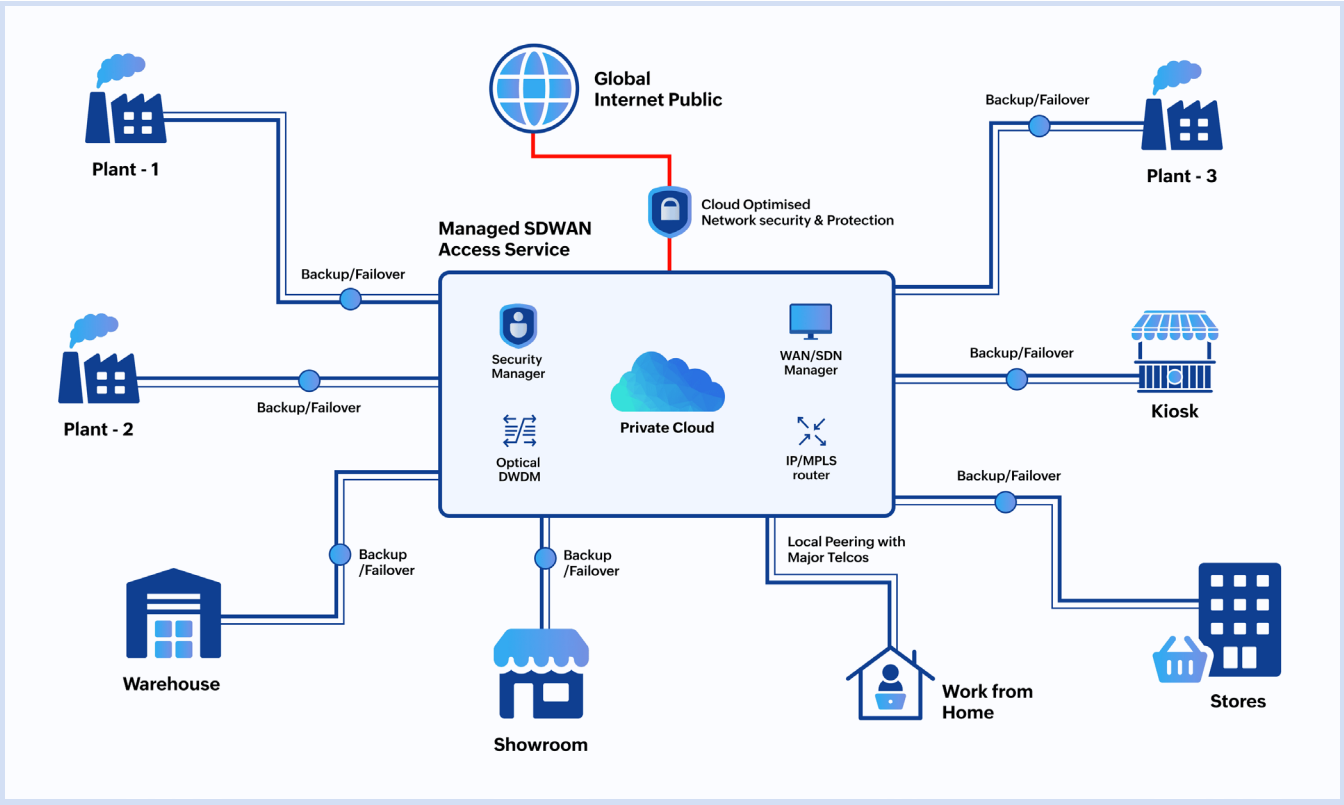
Real-time traffic monitoring allows manufacturers to prioritize critical applications, such as SCADA systems or ERP platforms. Intelligent routing ensures low-latency performance for time-sensitive operations while maintaining bandwidth efficiency. This visibility empowers IT teams to identify bottlenecks, manage capacity proactively, and enforce QoS policies that align network performance with business goals.

Managing a hybrid workforce for remote and in-office employees

Manufacturers are increasingly adopting a hybrid workforce model that blends on-site roles with a remote connection facility for employees to connect from anywhere. This requires securing the organization's network while expanding to bridge the gap between remote and in-office employees. A solution that can enforce security policies to allow only legitimate employees and restrict external unauthorized individuals is vital.

These challenges need to be addressed with the right IT solution, which builds a secure and effective network infrastructure and streamlines the network service for every organization to support its development.

Private WAN network for the manufacturing sector



This image illustrates the Private WAN network connected across different manufacturing plant sites, branch offices, stores, warehouses, and employees' remote locations. Private WAN serves as the backbone of an organization's network infrastructure, consisting of VLANs, LANs, private and public cloud infrastructures, and data centers to link the private WAN.

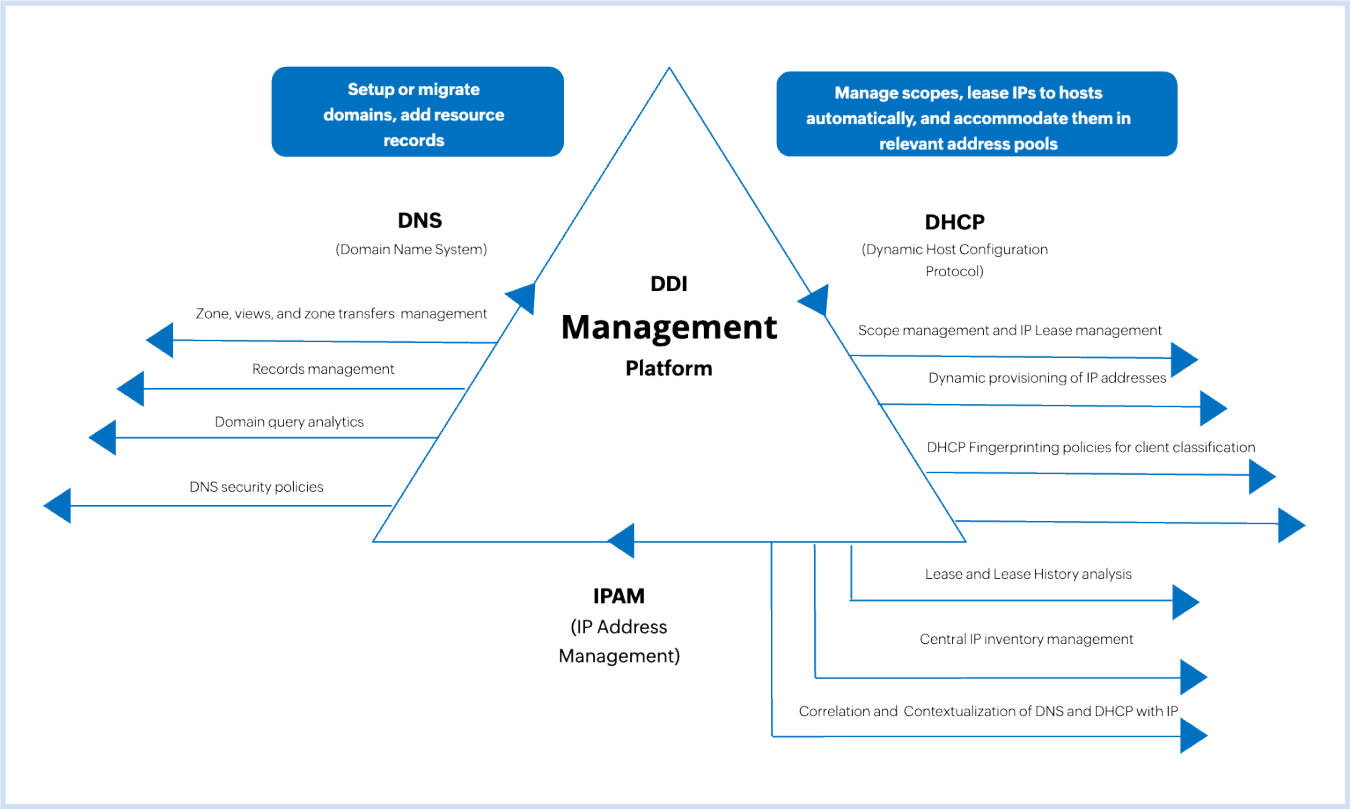
The network centralizes and links multiple manufacturing sites, allowing employees to securely access the sites' network from remote locations. At the core of this setup is a high-performance private WAN that acts as the backbone.

This backbone is typically built using dedicated IP/MPLS routes or an optical transmission core that interconnects the entire network through high-speed transmission equipment.

Branch locations are then connected to this backbone using technologies like SD-WAN, SDN, or IP/MPLS, often enhanced with VPNs to ensure secure and reliable communication.

Now, the main challenge faced by this network infrastructure is converging the sites under a common IP infrastructure. That's where DDI solution comes into play.

How ManageEngine DDI Central can enhance the network infrastructure



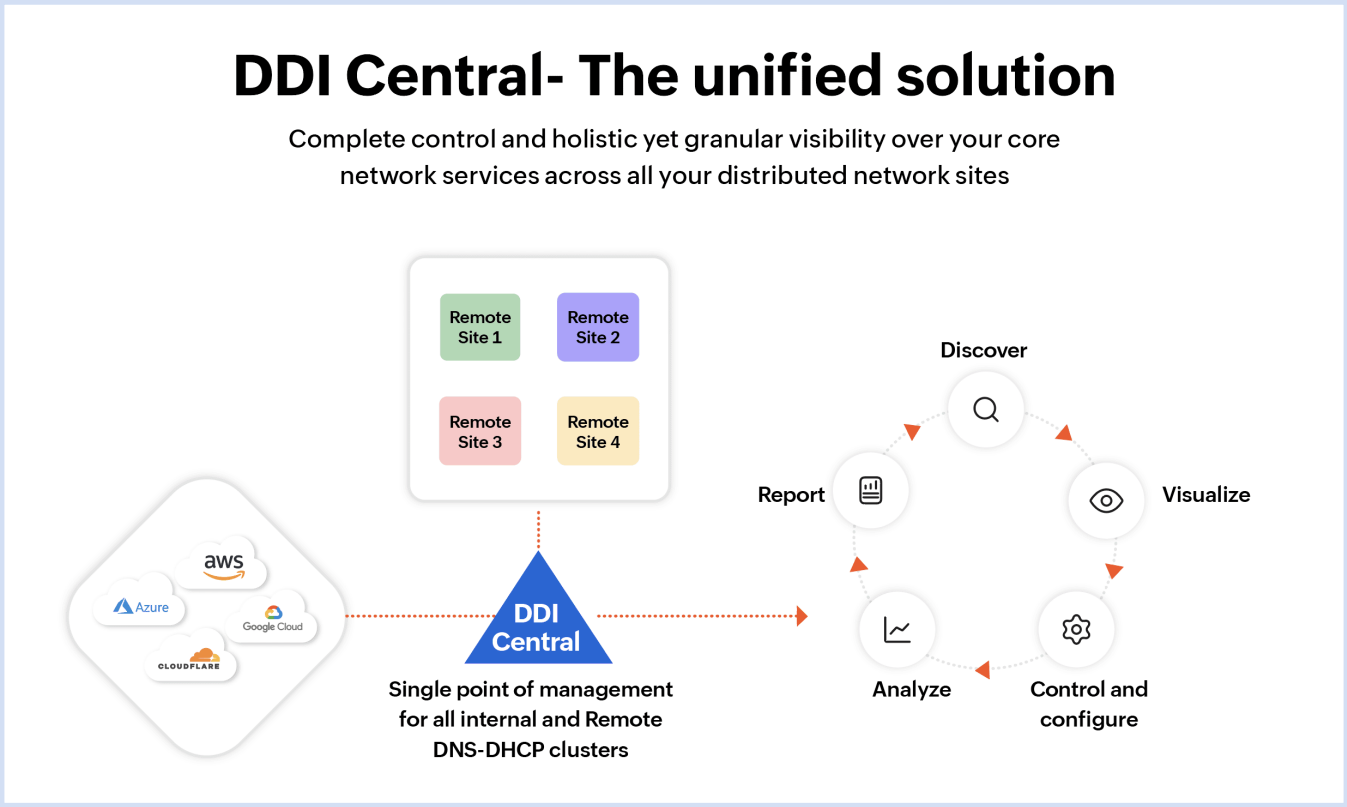
ManageEngine DDI Central is a user-friendly, specialized solution that unifies DNS, DHCP, and IPAM into a single platform for improving operational efficiency and network stability. It can manage Microsoft Windows DNS and DHCP clusters, as well as manage existing Linux-based ISC-Bind9 and ISC-DHCP installations and set up new clusters.

DDI Central serves as a single point of administration for different manufacturing site and plant networks. With DDI, the three core network services (DNS, DHCP, and IPAM) can be managed and their configurations to the remote sites connected with the main manufacturing network.

This is accomplished with technologies like SD-WAN, IP/MPLS core via VPN, or dark fiber cables.

When a manufacturing site onboards all its DNS and DHCP servers as clusters into DDI Central, it starts discovering all the configurations in smaller divisions, and categorizes them to provide clear visibility.

With all the configurations organized in its UI, network administrators can easily control the core network services and taking necessary actions. They are enabled to analyze the visual analytics that accompany each module to gain quick visual snapshots and determine valuable actionable-insights that ensure effective troubleshooting.



This way, the main manufacturing network admins can holistically view and centrally manage the core network services of different remote sites associated with the main plant—all from a single window.

Importance of implementing network segmentation

Network segmentation involves adding multiple layers of protection to the network infrastructure and dissecting the larger network into smaller sub sections, making it easier to manage and monitor. This way, IT admins can compartmentalize servers and endpoint devices based on the line of manufacturing they belong to.

A DDI solution's segmentation provides network admins detailed visibility over the segments, devices associated, objectives and policies through DHCP options, guiding them on identifying and responding to malicious activity or network resource exhaustion.

Also, during a security breach event, segmentation contains the impact of the attack in the limited area, protecting other sections of the network from harmful effects.

Let's review a scenario to understand how a DDI solution's network segmentation features can be utilized to build a secure and effective network infrastructure.

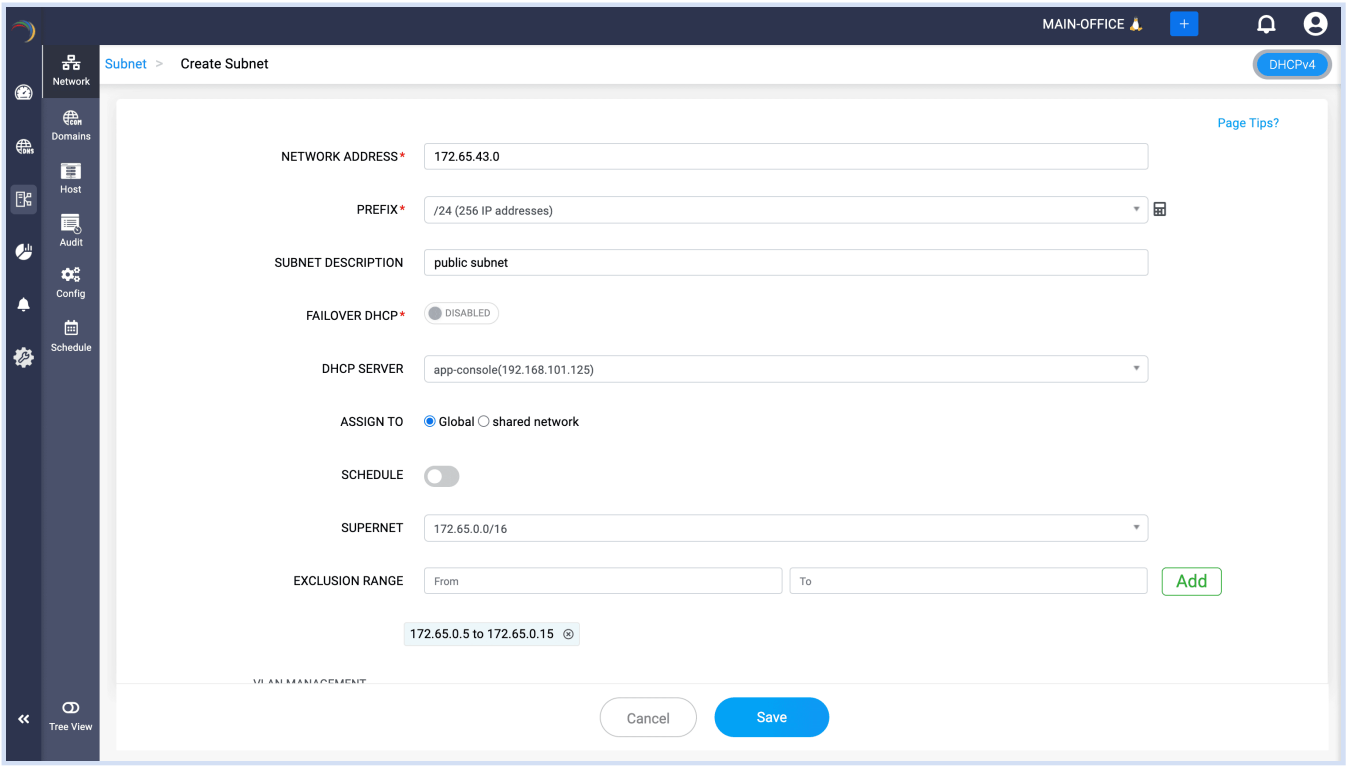
Scenario:

A manufacturing plant, consisting of multiple devices for different operations, needs them to be connected to its network. The devices should not face any IP address conflicts or network overlapping, so their network needs to be categorized based on their purpose and priority for effective IP leasing.

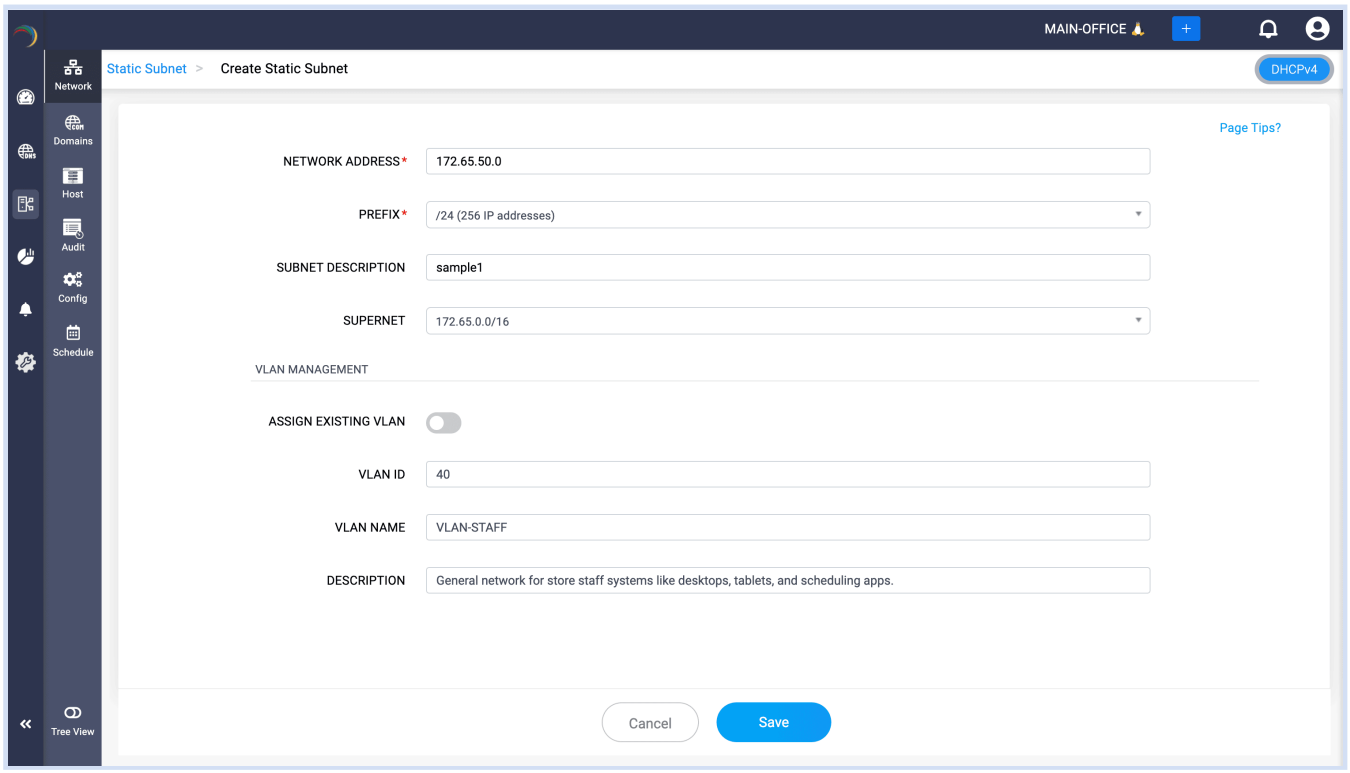
The networks need to implement policies for the network segments sharing the same functionality for simplified management. They need to have manual control over their critical devices, servers, and data centers without relying on dynamic IP allocation.

They also need to isolate specific segments of the network for selected devices, like VoIP phones, where the IP allocation requests shouldn't be interrupted by other departments.

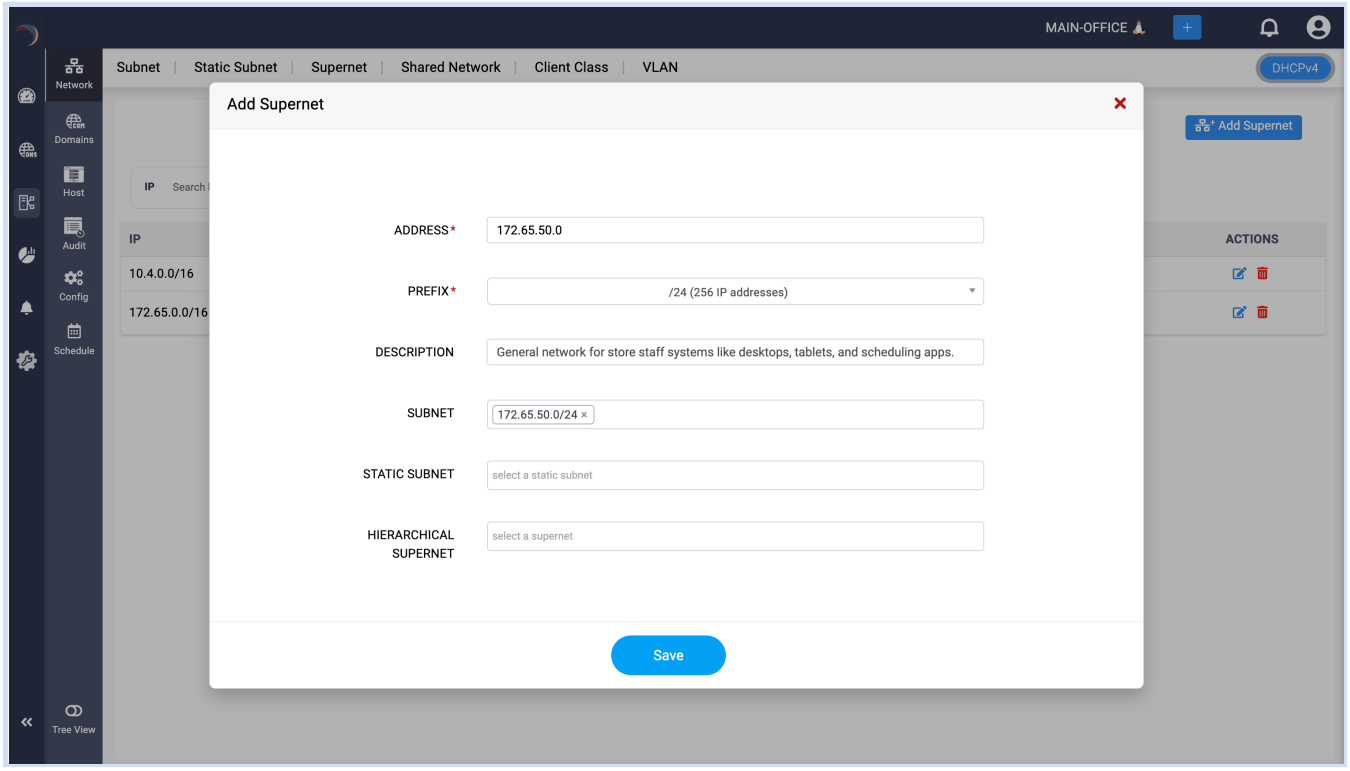
Solution:



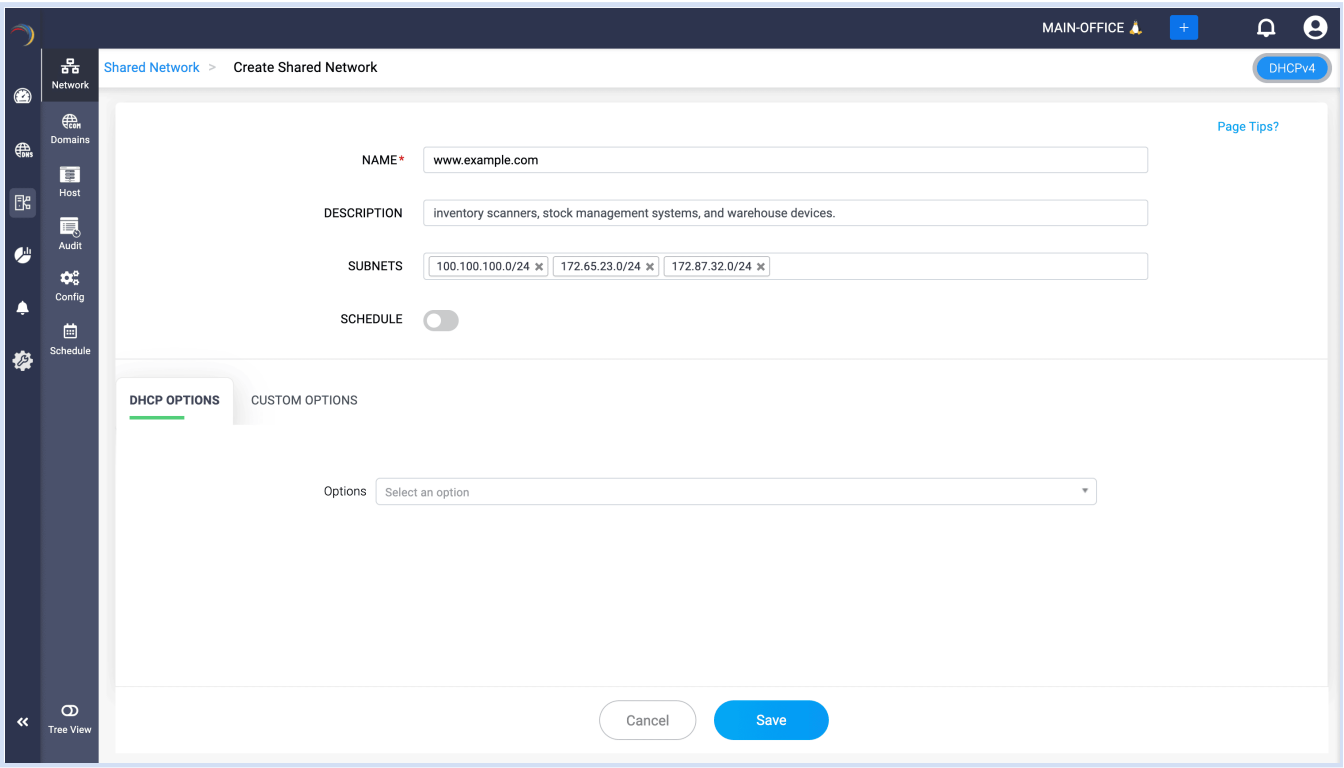
Network admins can create subnets with different pool ranges for different device groups, for example, industrial robots, conveyor belts, and testing machines. This enables the subnets to get IPs leased when they join the network.



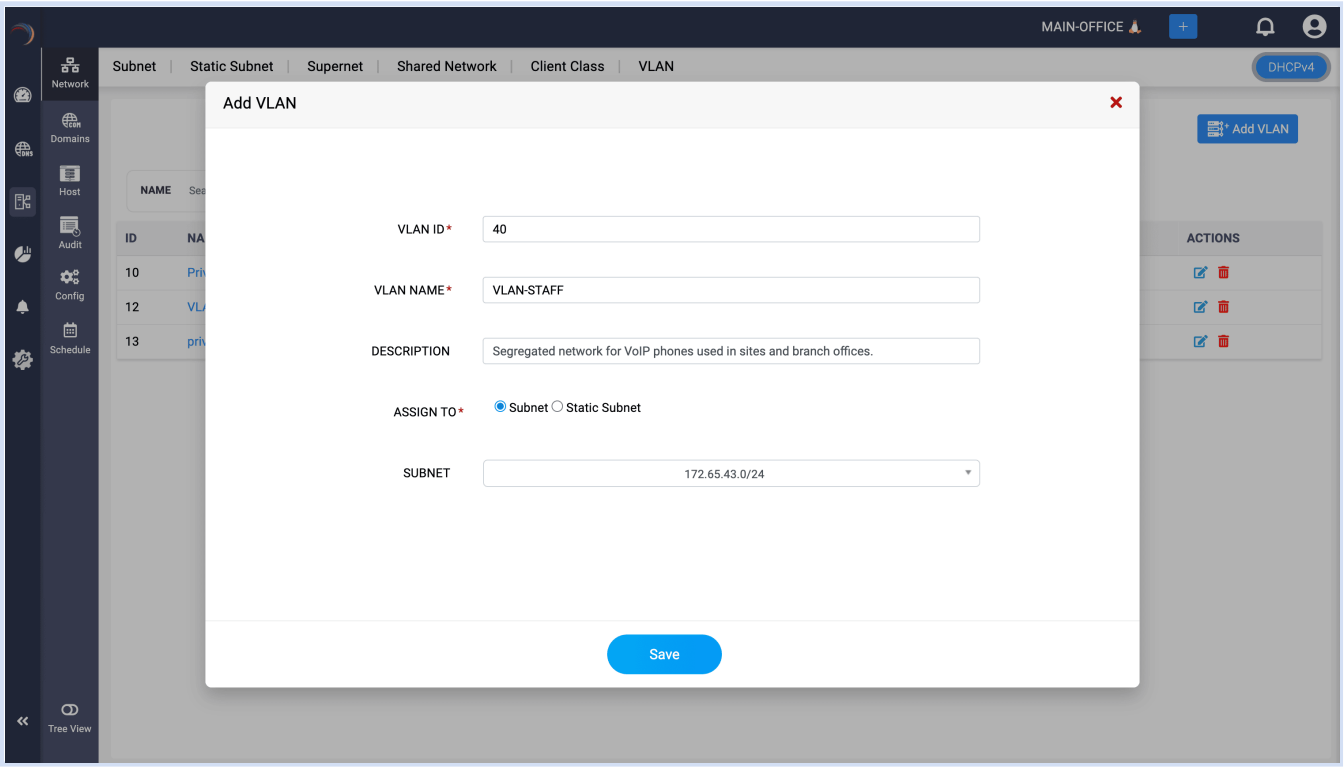
Static subnets can be created with specific pool ranges, which provides manual control to network admins to configure and manage IP allocation for critical application servers, data centers, security devices, and systems. These devices are highly reliant on manual control and not on automated IP allocation, as they need to provide continuous non-stop services and data management.



Two or more subnets can be combined into a single supernet and organized on a hierarchical way. This way, network admins can structure and manage their network segments for better visualization and routing purposes.



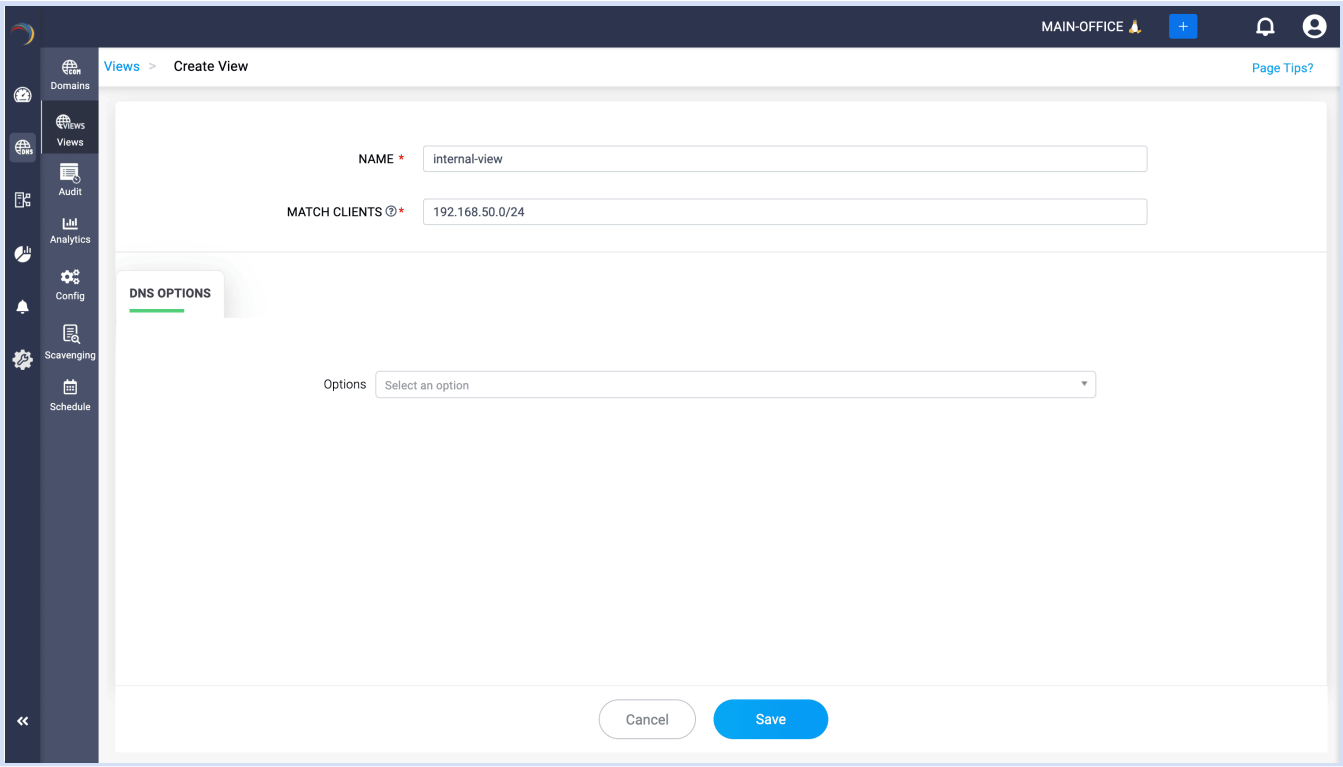
When different subnets have the same functionality for a specific category of devices, they can be combined into a single SharedNetwork and apply DHCP options or custom options.



VLAN plays a crucial role in separating IP allocation for devices like VoIP phones. Admins can create a VLAN for the VoIP phones by providing VLAN ID, VLAN name, and description, so it can easily be associated with the subnet created specifically for VoIP phones.

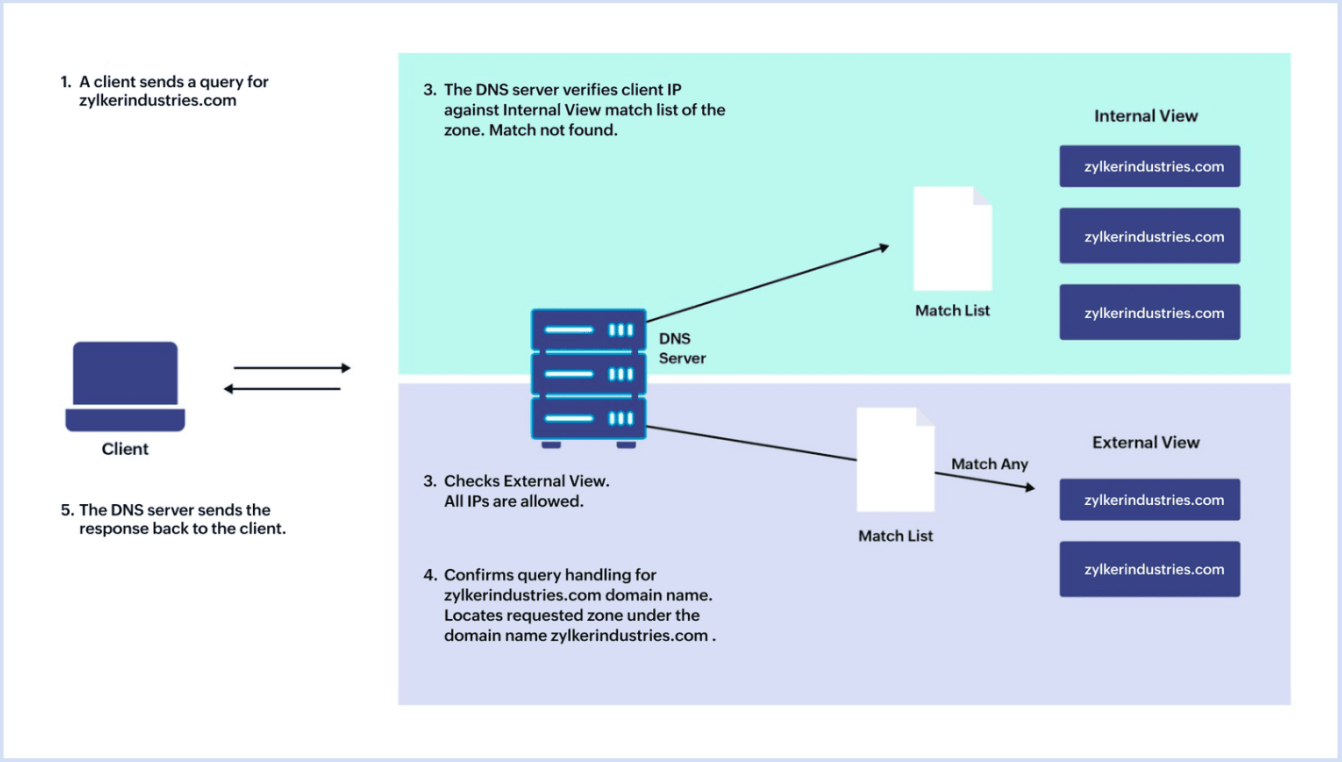
VLAN helps isolate the broadcast message sent by the VoIP phones to the DHCP server for IP allocation, and prevents it from getting interrupted by other network traffic.

DNS Views



DNS views or Domain views help network admins implement a selective query response based on the user's profile and background. A specific resolution is required to provide the organization's data separately for internal and external view. This way, only legitimate employees of the organization can view the confidential data, while external visitors can view the published generic data, or they are redirected to a safe webpage that won't let their system be exposed to malware, cyberattacks, or access malicious domains.

Along with several DNS options, DNS or domain views can be configured for the organization's needs, based on clients, destined response, recursive response, forwarders response, and etc. Let's look at a scenario to understand DNS view and its functionality better.



Scenario:

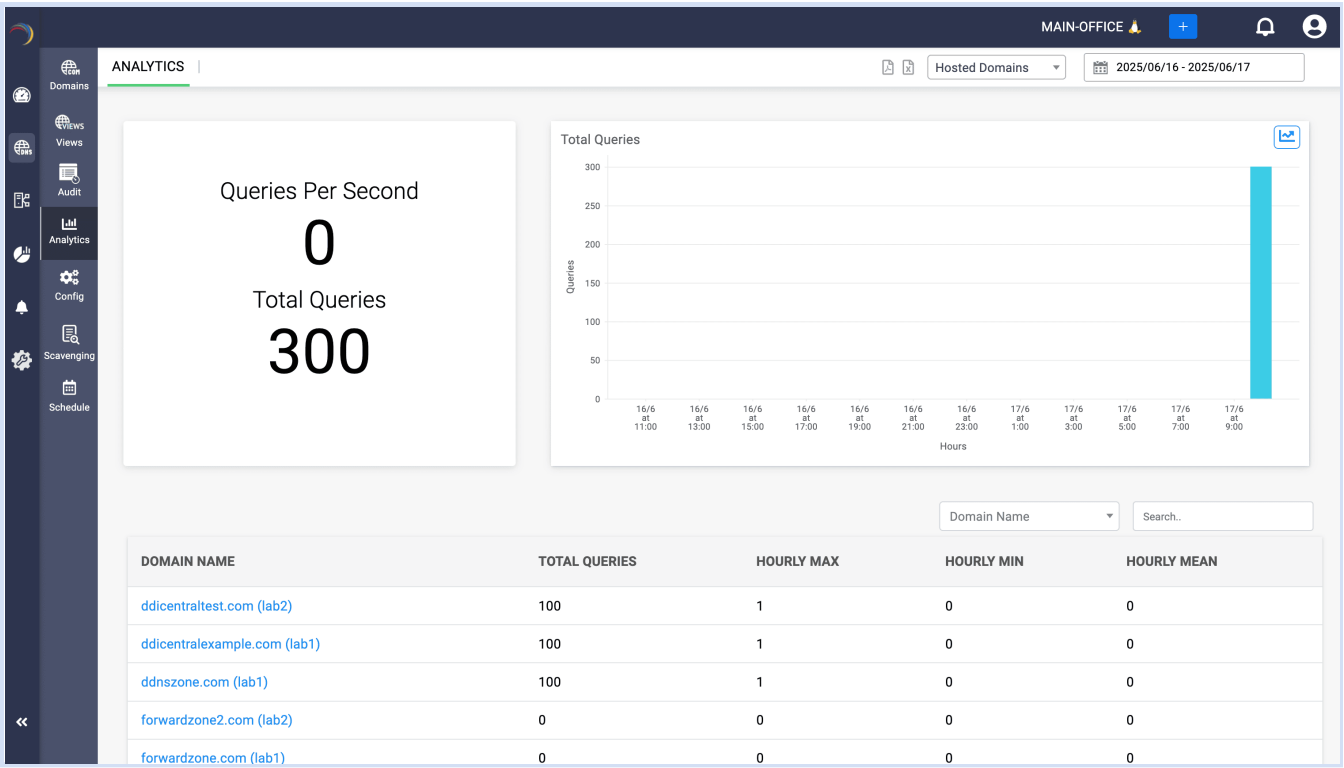
Two different users are sending query for the domain name **zylkerindustries.com** to the DNS server. One is the organization's employee, and the other is an external visitor.

Upon receiving the query, the DNS server first checks both the user's IP with the internal and external view match list. The internal view match list contains the IPs of the organization's registered employees, while the external view match lists those that match any public IPs that are not in the internal range.

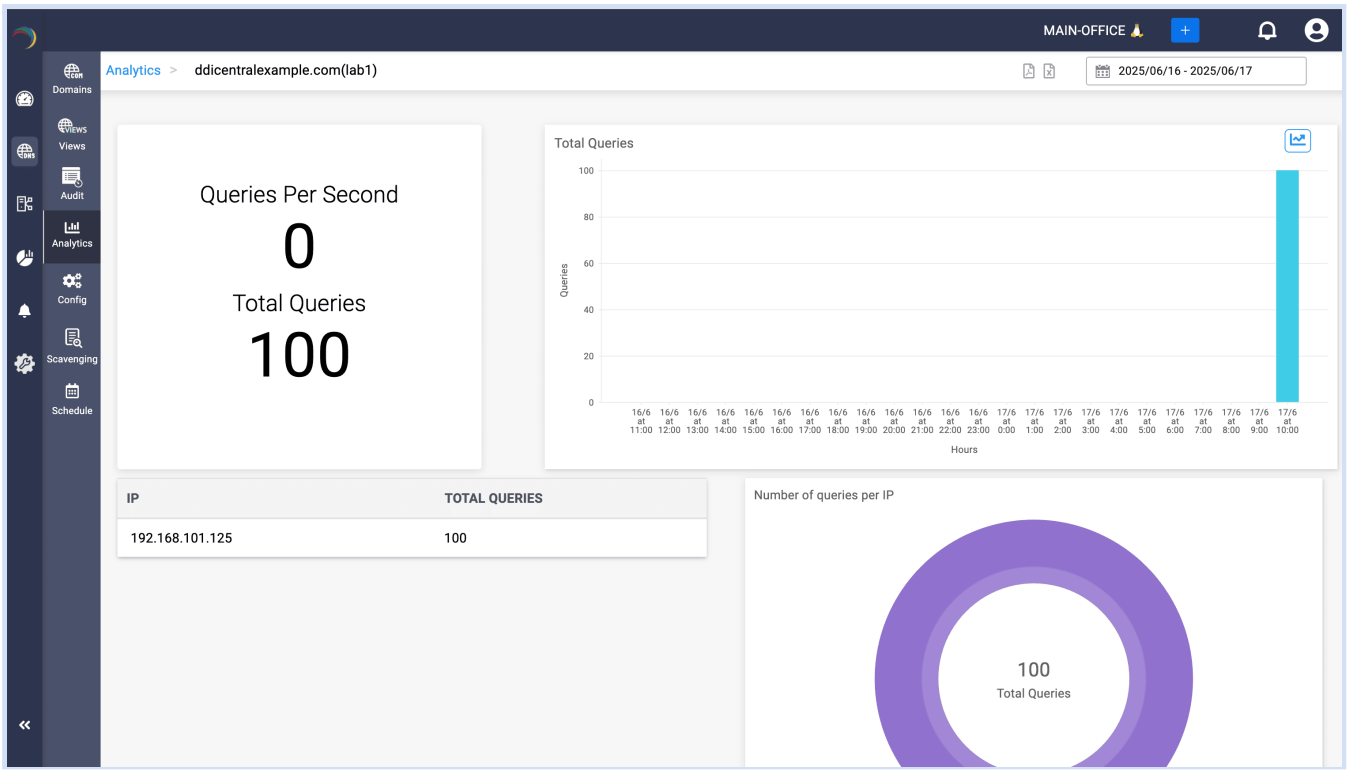
The employee's IP gets matched with the internal view match list, while the external visitor's IP gets matched with the external view match list.

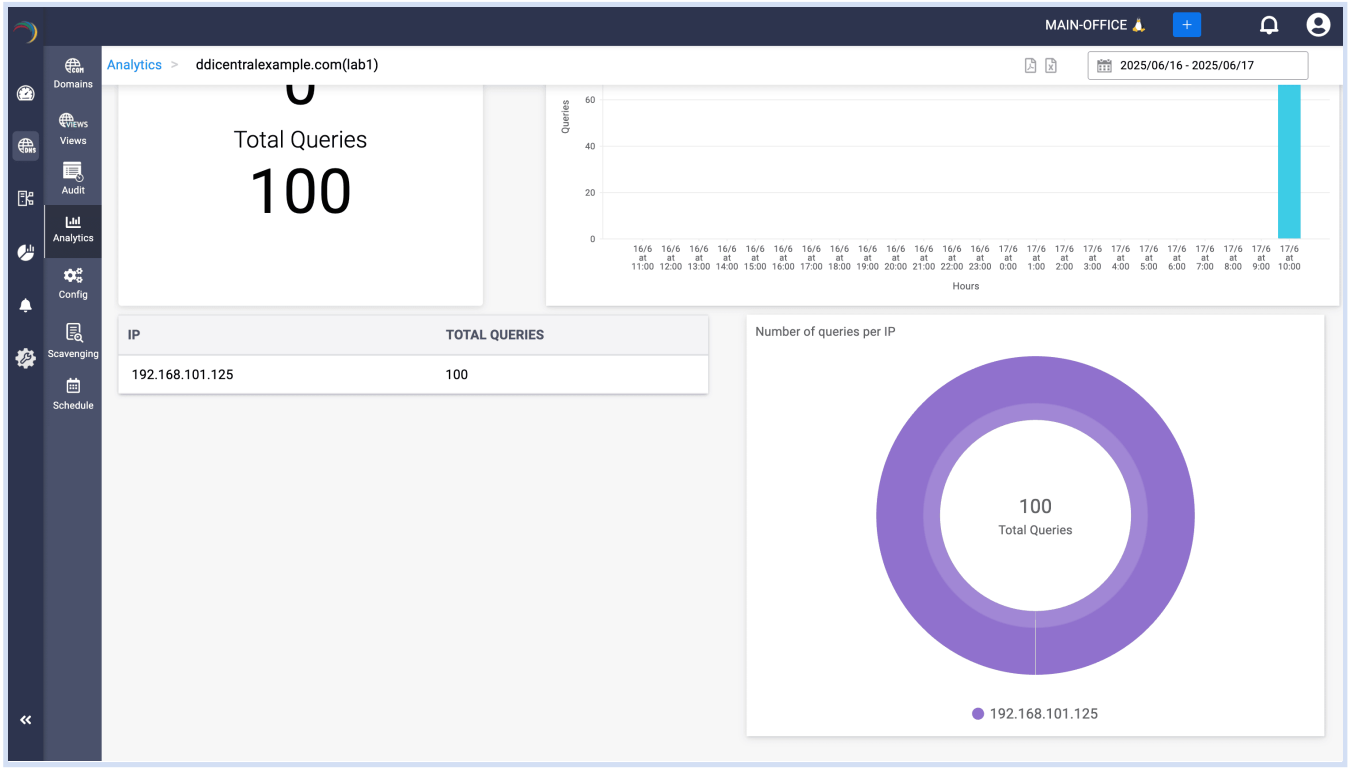
Now, the organization can resolve two different IP address for the domain name **zylkerindustries.com**. One contains the confidential data of the organization used for internal purposes, resolved for the employee, and the other one will be a redirection to the safer page, resolved for the external visitor as they are restricted from visiting that domain.

Domain Query Analytics

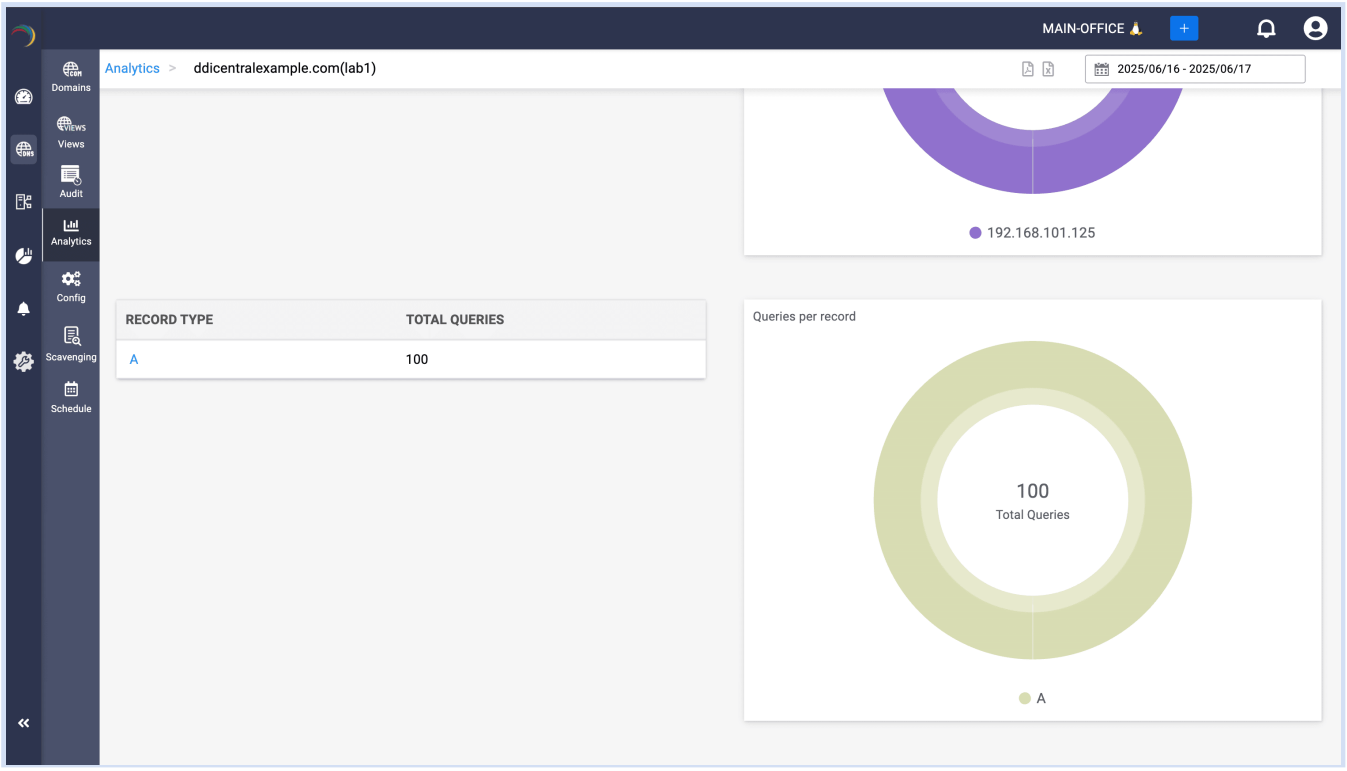


DDI Central's Domain Query Analytics enables admins to have clear visibility about the number of queries to the views and domains per session, and the number of queries received per IP. Admins can analyze the queries made to the configured views, including those for both hosted and non-hosted domains.





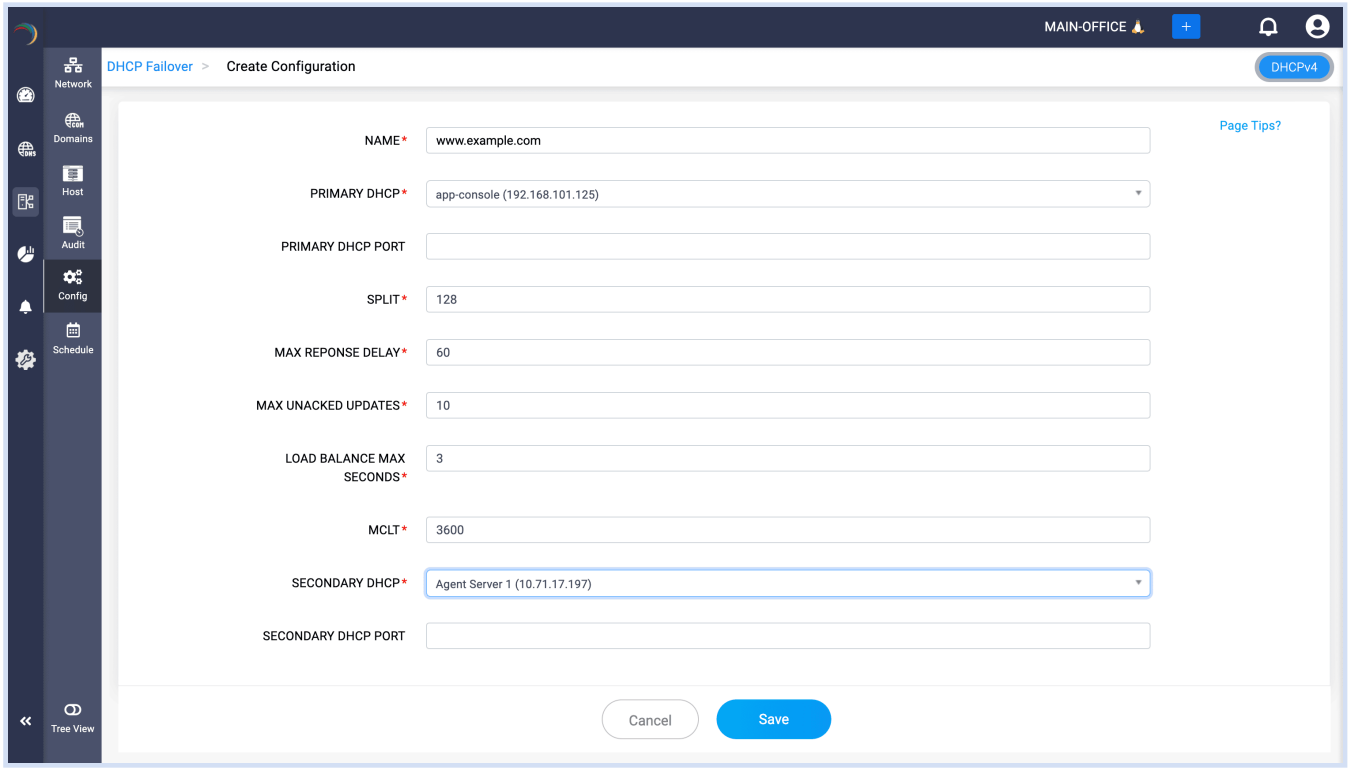
Clicking on a specific domain or view displays the domain's performance metrics, with the hourly query load over a specific time frame. Along with that, it showcases details of the IP address leased for a domain, such as lease duration, the host's MAC address, and vendors of the host machines.

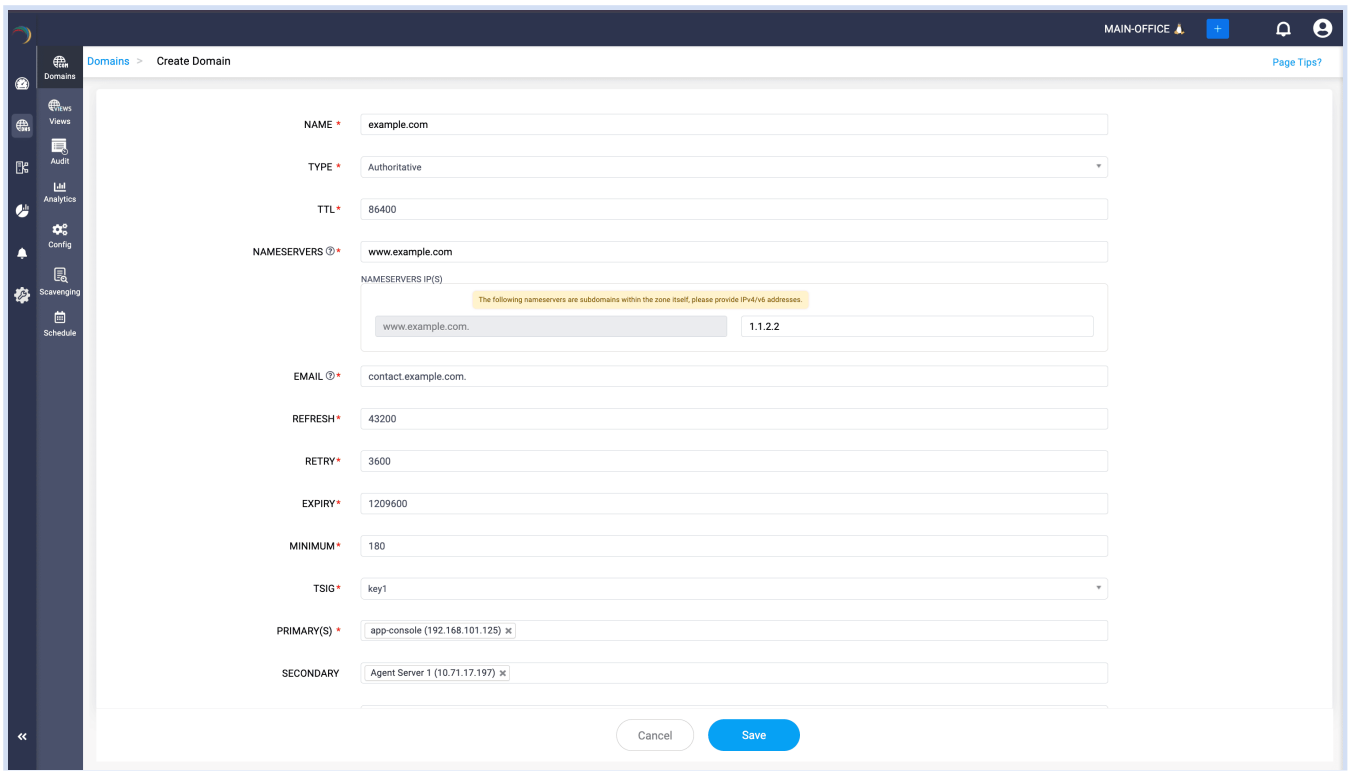


Also, the total query load across all IPs, and the individual query loads are visually presented in a donut chart for a specific IP address. Plus, a separate donut chart breaking down the query volume is generated for the given DNS records.

Clicking on the record type displays a comprehensive list of all zones queried for that record, with key performance indicators for hourly query load, queries per second, and the total number of queries covering that particular zone.
Selecting a specific zone within the record type helps display a visual summary of the query analytics about that zone's records.

High availability of DNS and DHCP



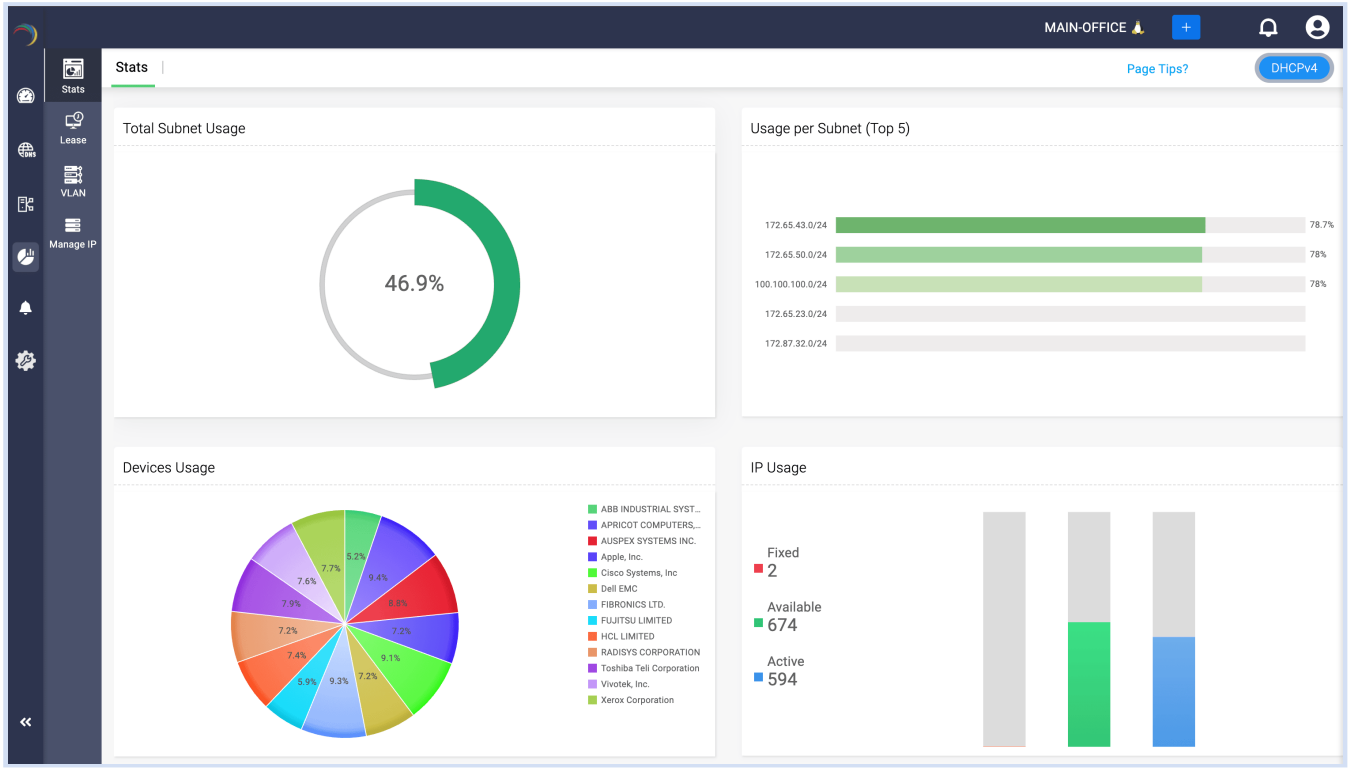


DDI Central's auto failover setups for DNS and DHCP services help manufacturing sites during critical situations where servers handling network traffic goes down. Network admins can add primary and secondary servers for both DNS and DHCP services, where they can have more than one secondary servers.

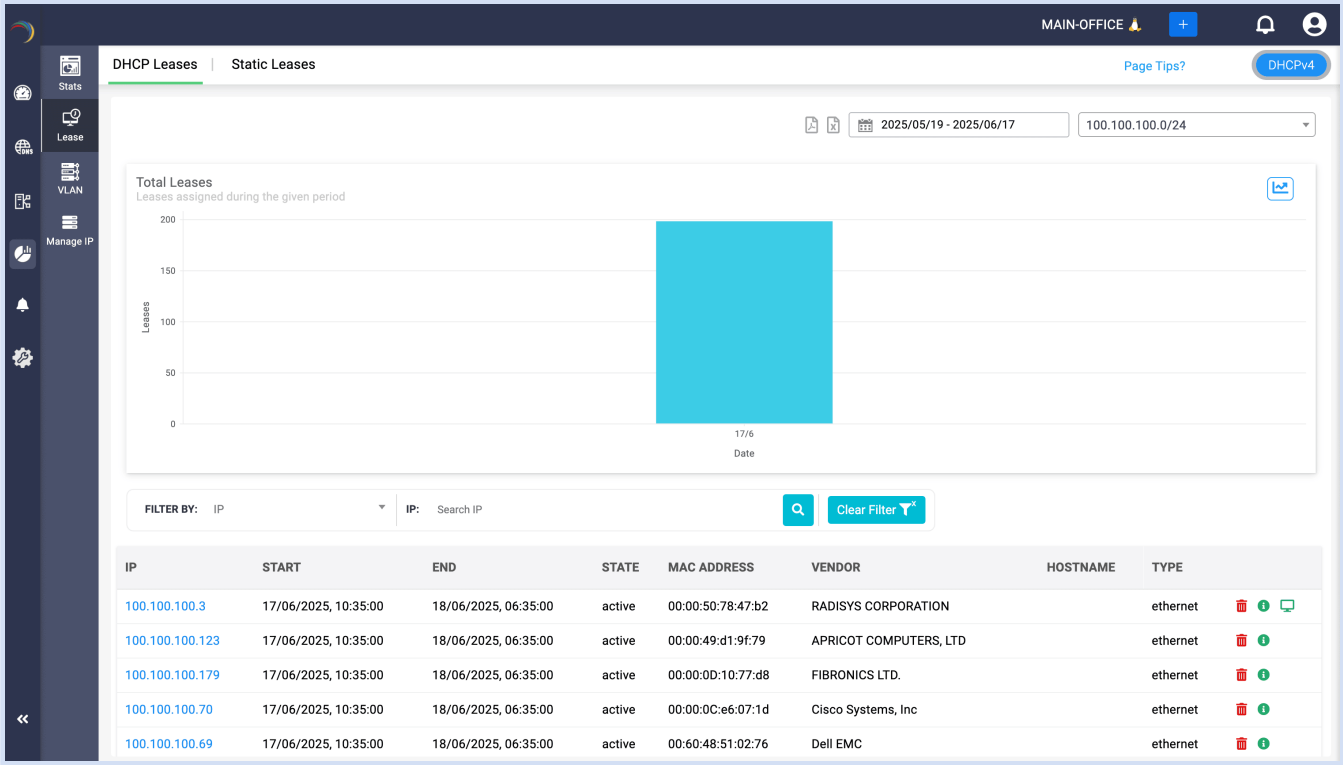
During the primary server going down, secondary servers can step in and take full responsibility for handling the network traffic and maintaining consistent network flow for the organization. Both primary and secondary servers can be configured to split the query load for better load balancing to handle the network traffic effectively.

For scenarios where network service or application service need to be provided constantly to clients without interruptions, auto failover setups are crucial for efficient, reliable, and non-stop service and support without compromises.

IPAM as NSoT

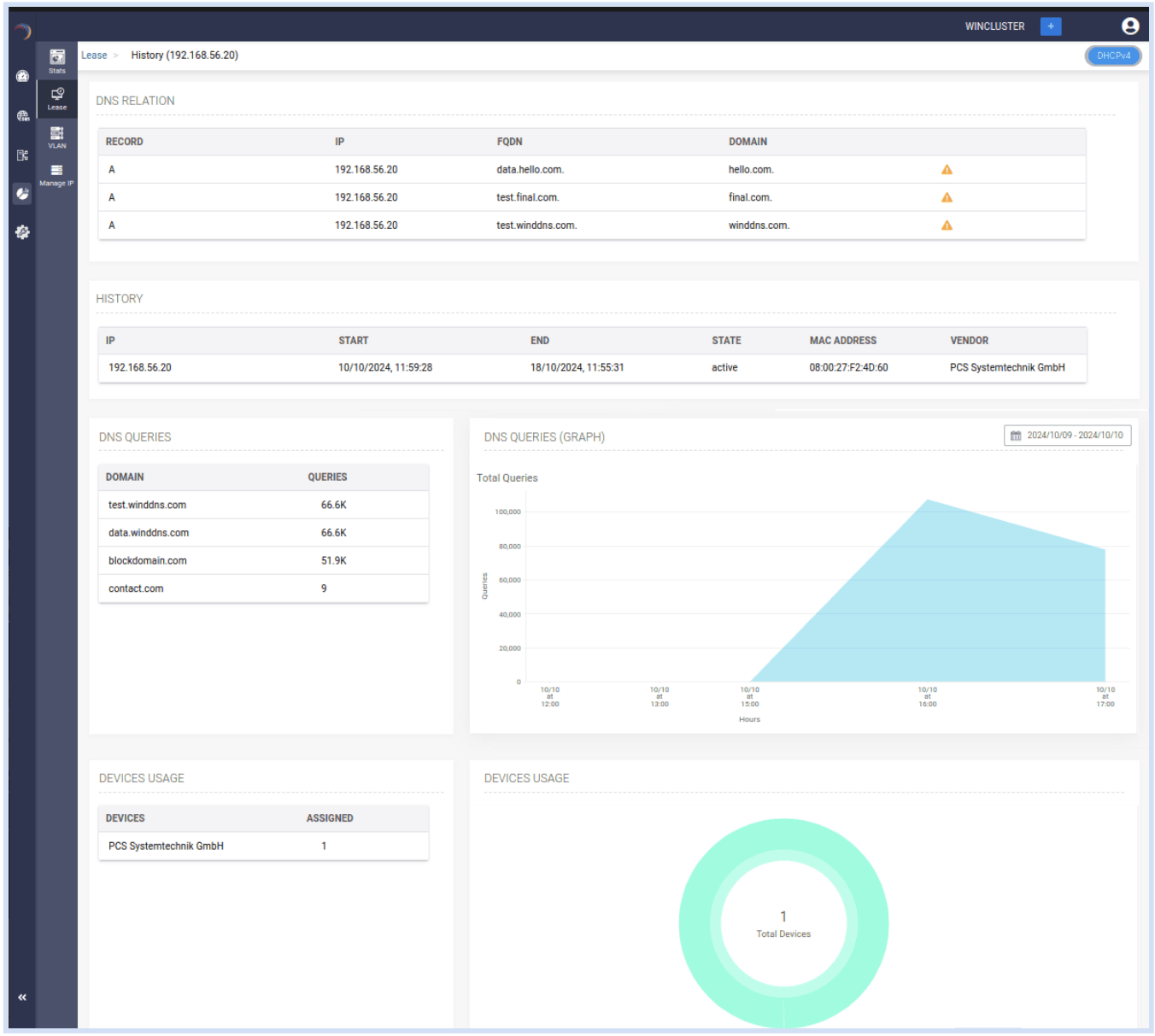


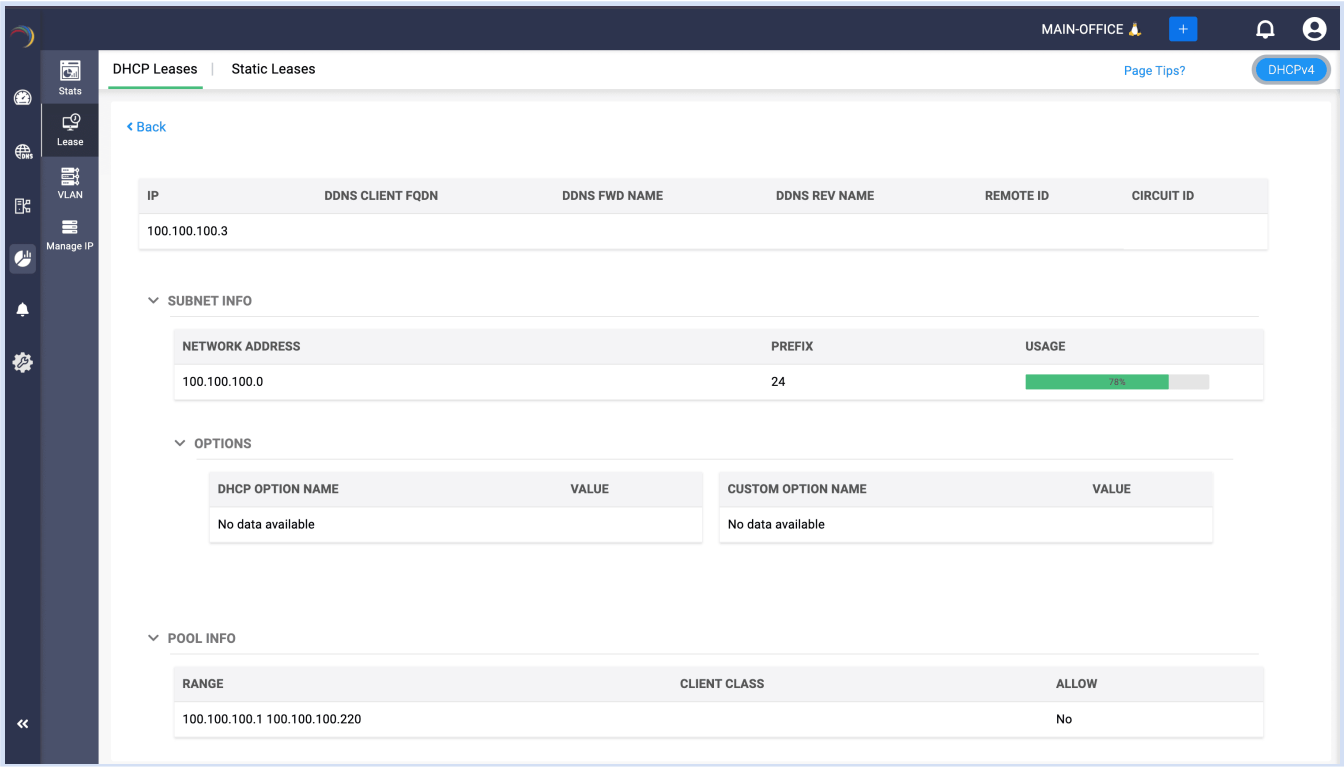
IPAM in DDI Central collects and correlates DNS and DHCP data in all the clusters, providing a contextualized view and deeper insights over the network services and issues service as an Network Source of Truth (NSoT). Meta data like DNS records, DHCP leases, and IP address allocations can be visualized in charts view, simplifying data drive decisions for network admins and also troubleshoot issues.



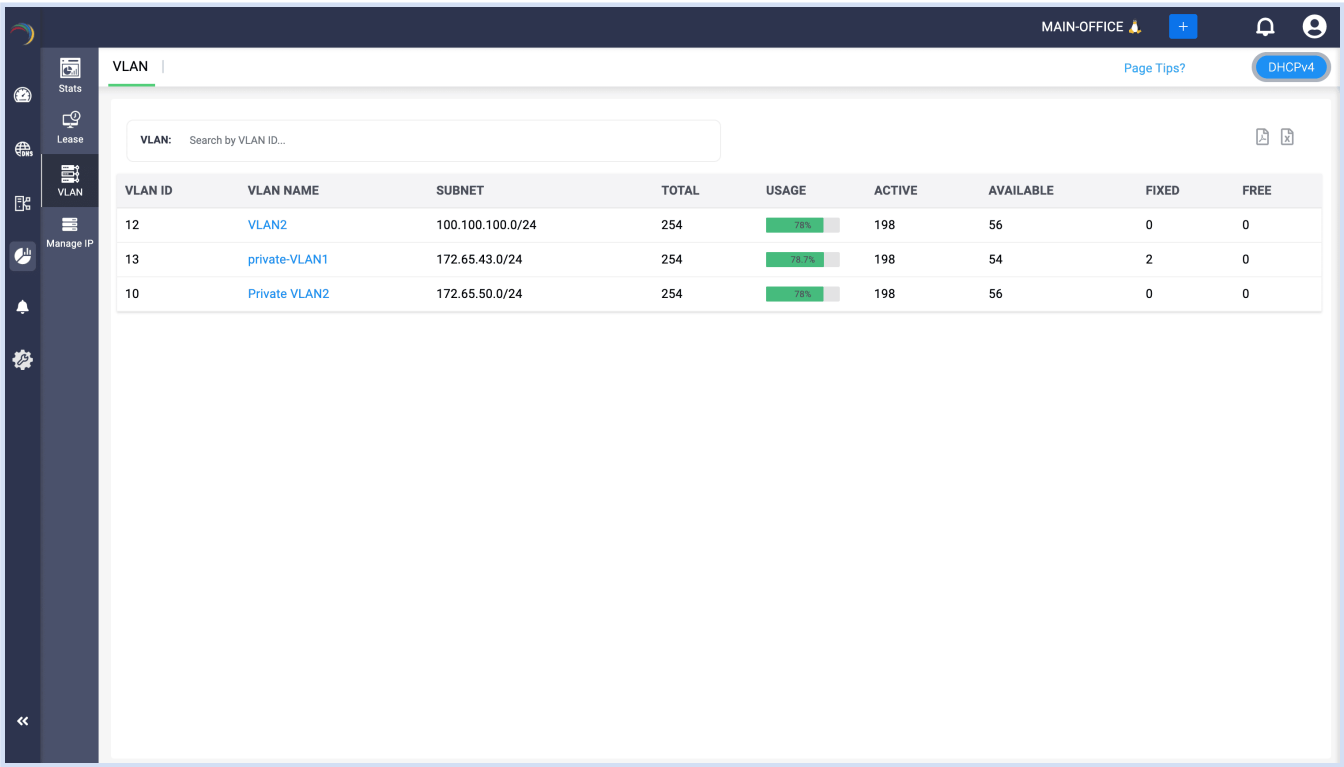
In the DHCP Leases section, admins can view the total leases assigned within an hour in graph view. A tabular view displays the IP address, its lease period, status, the device's MAC address it is assigned to, hostname, vendor, and type of connection. Also, with the integration with Endpoint Central, a Monitor icon near the Info and Delete icon is displayed, indicating that the device details are in the Endpoint Central database.

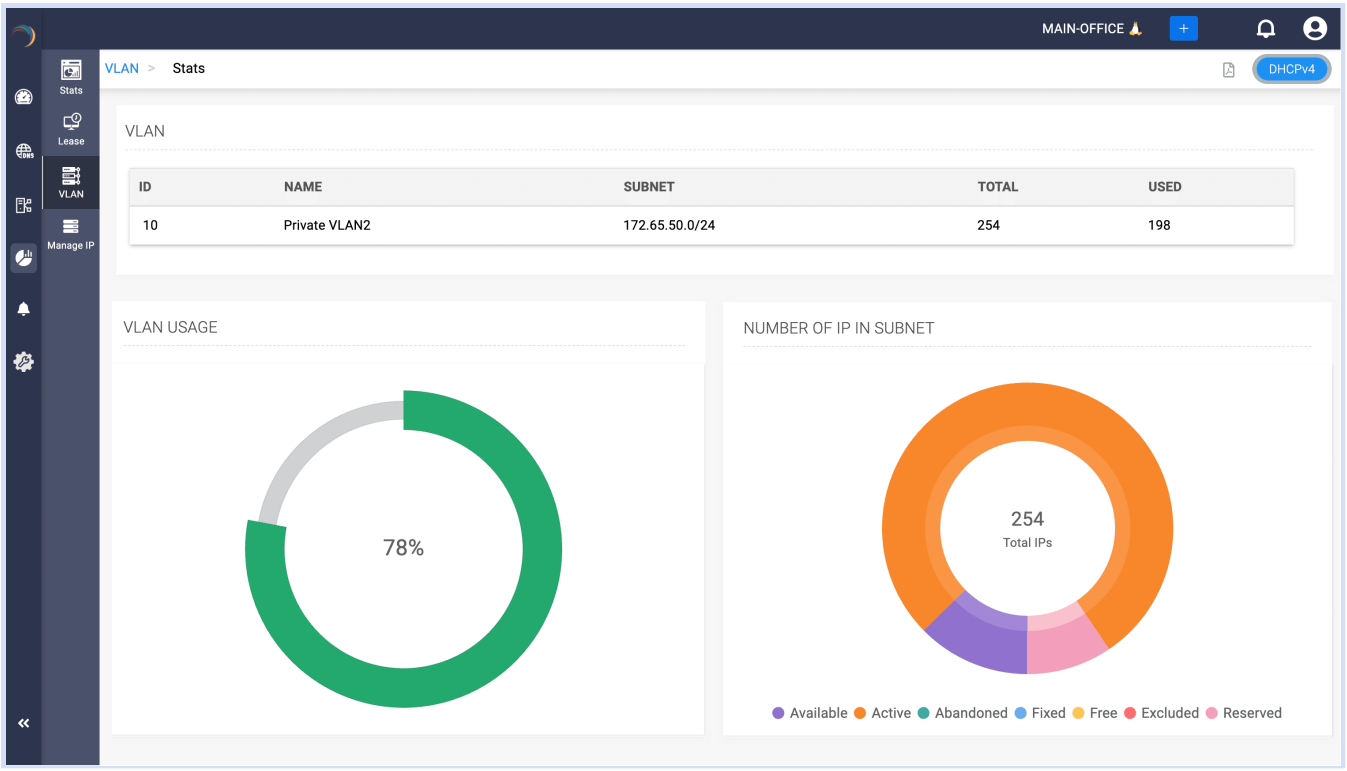
Clicking on the Monitor icon provides a contextualized view on the device details, along with patch and vulnerability details, that includes device/OS details, disk usage, patch summary, missing patches based on severity, and vulnerability based on severity and CVSS score.

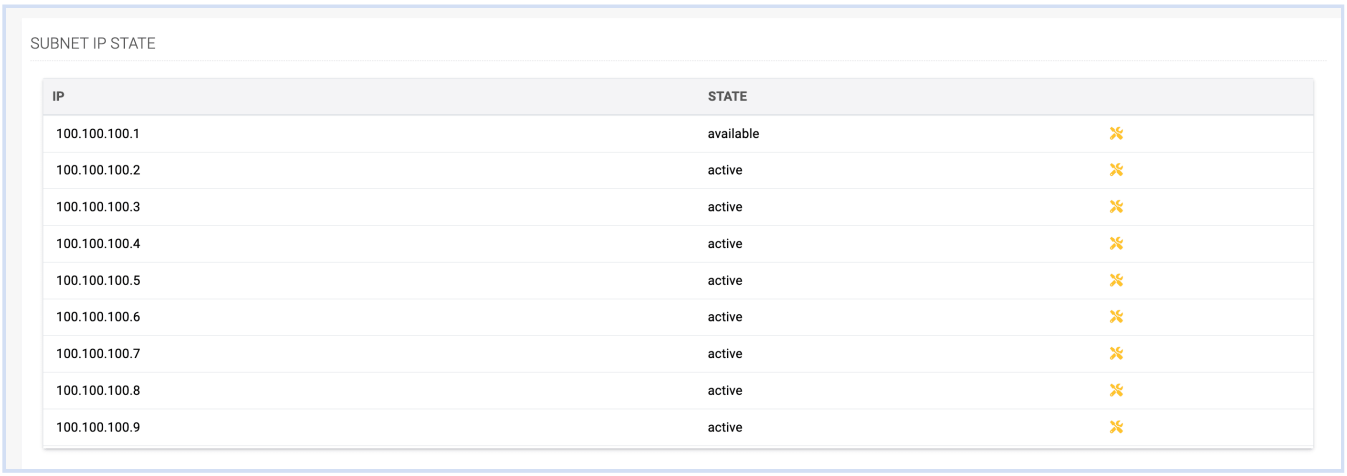

WINCLUSTER
Stats
Lease
VLAN
Manage IP
Lease > History (192.168.56.20)
DHCPv4
DNS RELATION
RECORD IP FQDN DOMAIN
A 192.168.56.20 data.hello.com. hello.com.
A 192.168.56.20 test.final.com. final.com.
A 192.168.56.20 test.winddns.com. winddns.com.
HISTORY
IP START END STATE MAC ADDRESS VENDOR
192.168.56.20 10/10/2024, 11:59:28 18/10/2024, 11:55:31 active 08:00:27:F2:4D:60 PCS Systemtechnik GmbH
DNS QUERIES
DOMAIN QUERIES
test.winddns.com 66.6K
data.winddns.com 66.6K
blockdomain.com 51.9K
contact.com 9
DNS QUERIES (GRAPH)
2024/10/09 - 2024/10/10
Total Queries
100,000
80,000
60,000
40,000
20,000
0
Queries
10/10 at 12:00
10/10 at 13:00
10/10 at 15:00
10/10 at 16:00
10/10 at 17:00
Hours
DEVICES USAGE
DEVICES ASSIGNED
PCS Systemtechnik GmbH 1
DEVICES USAGE
1
Total Devices



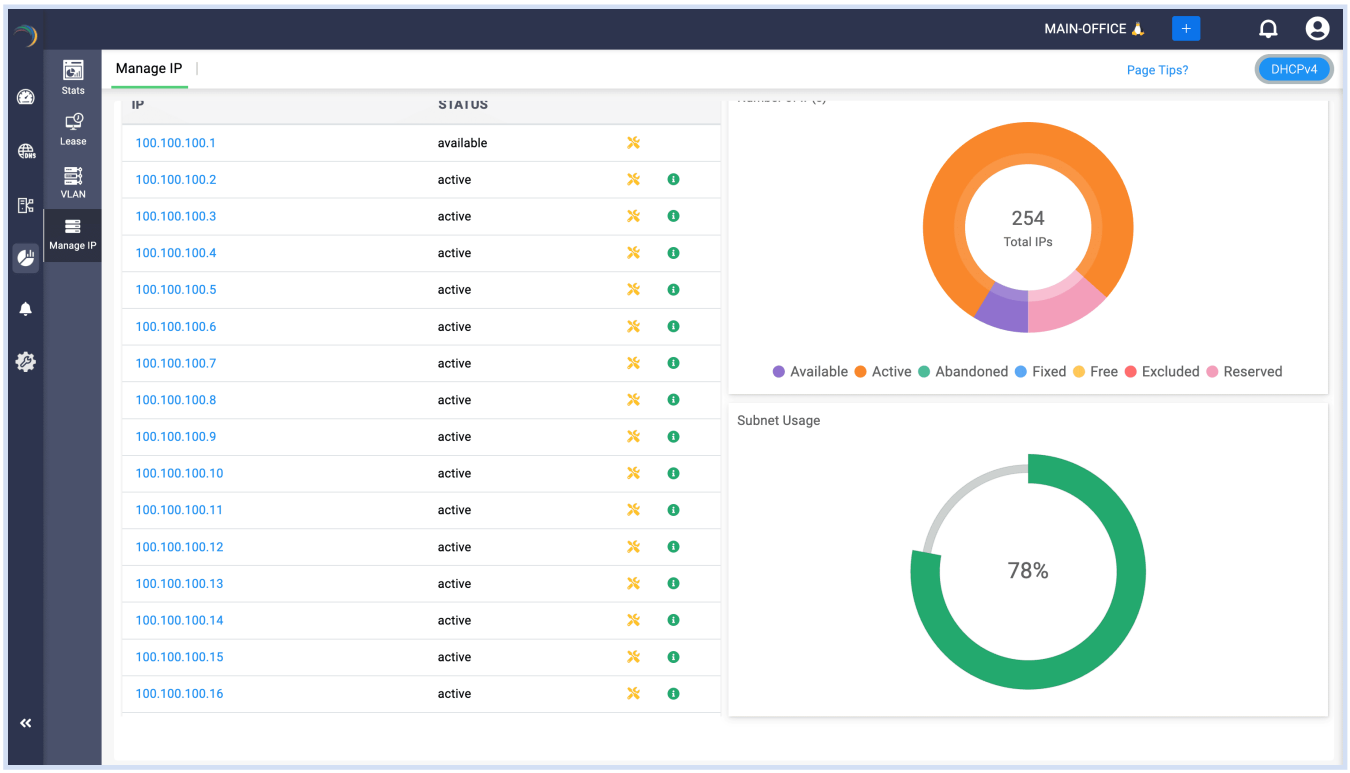
Clicking on a specific IP address in the DHCP Leases section provides a great visibility on the lease history, DNS queries received for the IP address, and devices assigned with no of times assigned, in both tabular and chart view.







The VLAN details created by network admins, including VLAN ID, name, subnet associated, total subnets, usage, status, and their usage, are visually represented to give deeper insights.



The same details are displayed in the Manage IP section, and clicking on the Tools icon next to the Info icon, will provide Ping, Telnet, and DNS Relation options.

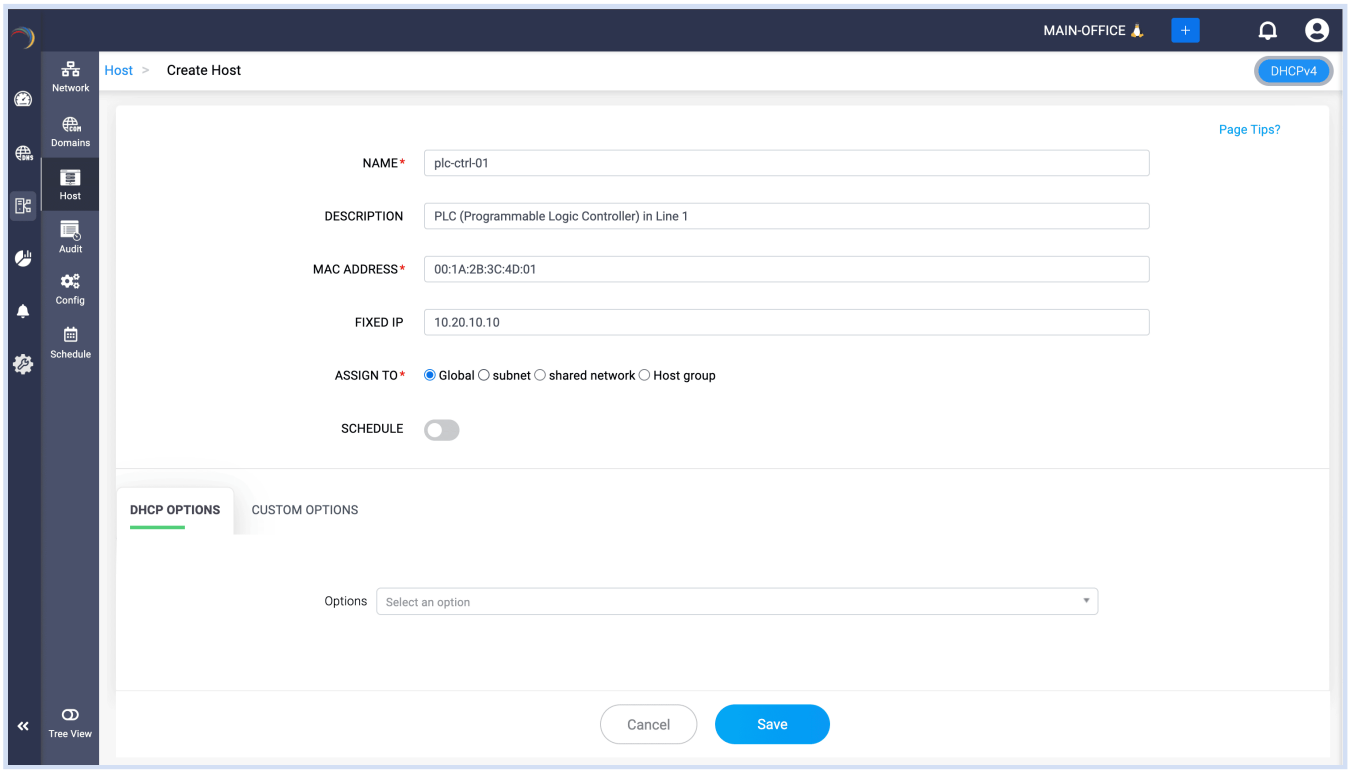
Clicking on the DNS relation will display the the status of the IP/host, the domain associated with, the record it has been mapped, and the zone associated with the IP through the DNS relation table, helping users to have a clear visibility.

DDI as an automation hub

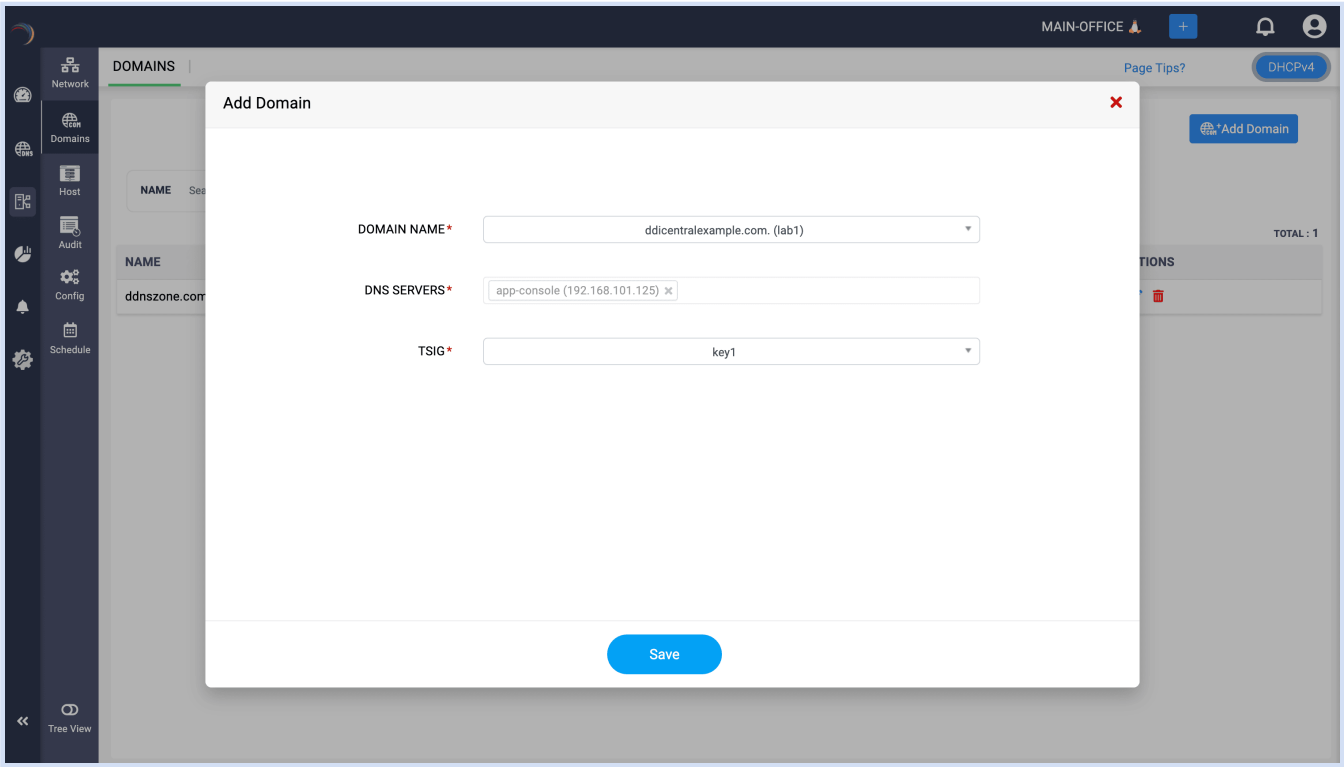
Let's say an organization has a need to automate some of its major DNS and DHCP tasks, such as IP assigning to critical devices, updating DNS records when IP address changes dynamically, updating the IP address inventory, scheduling DNS and DHCP resources and reports, and setting up failover.

These tasks can't be controlled and configured manually by IT admins as it would be time consuming and slow progressing. Therefore, the organization would require a network solution that can automate and manage these network tasks to reduce manual work.

DDI Central helps network admins by setting up end-to-end automation easily with its unified platform. Here are the following ways they can be automated:

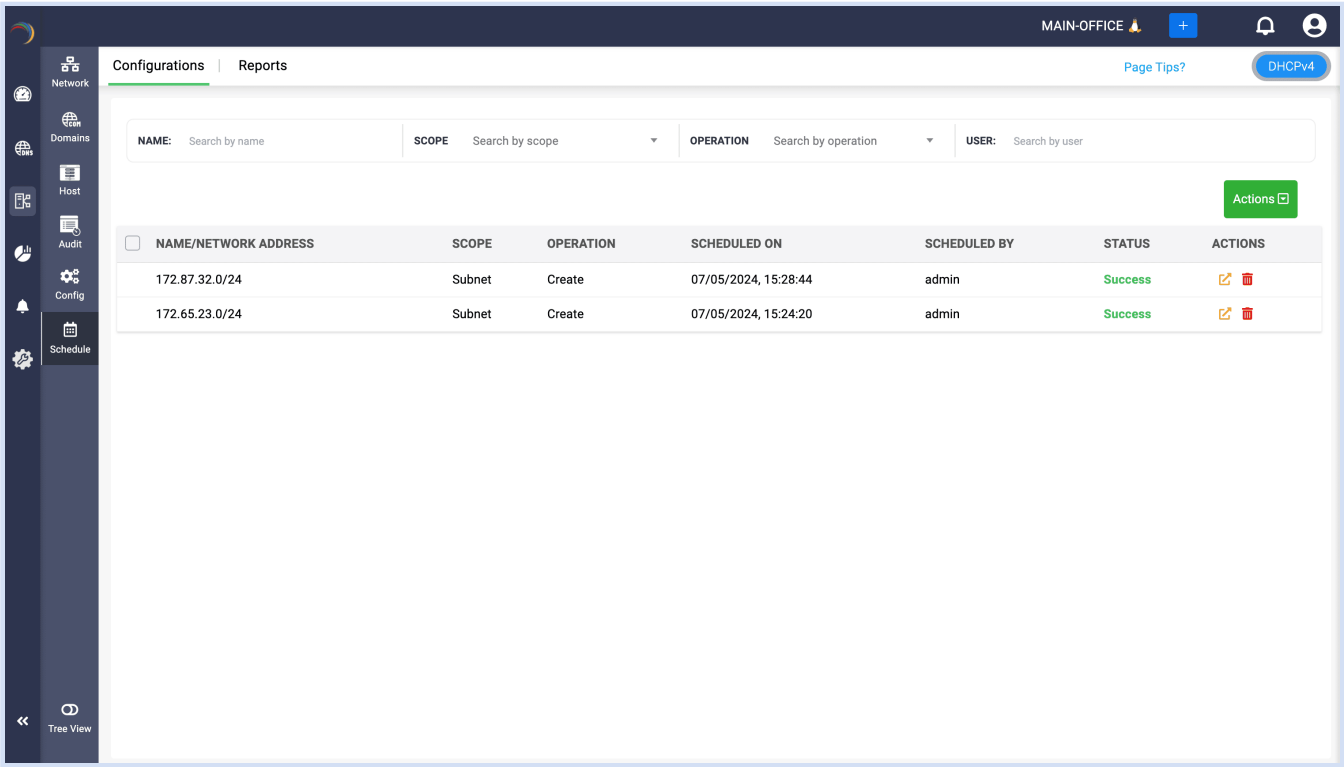


IP addresses can be configured to be fixed and automated for assigning to critical devices joining the network, such as surveillance cameras, printers, and sensors with the help of DHCP Host reservations. This helps reduce outages and IP exhaustion for critical devices that are needed to be connected within the network.

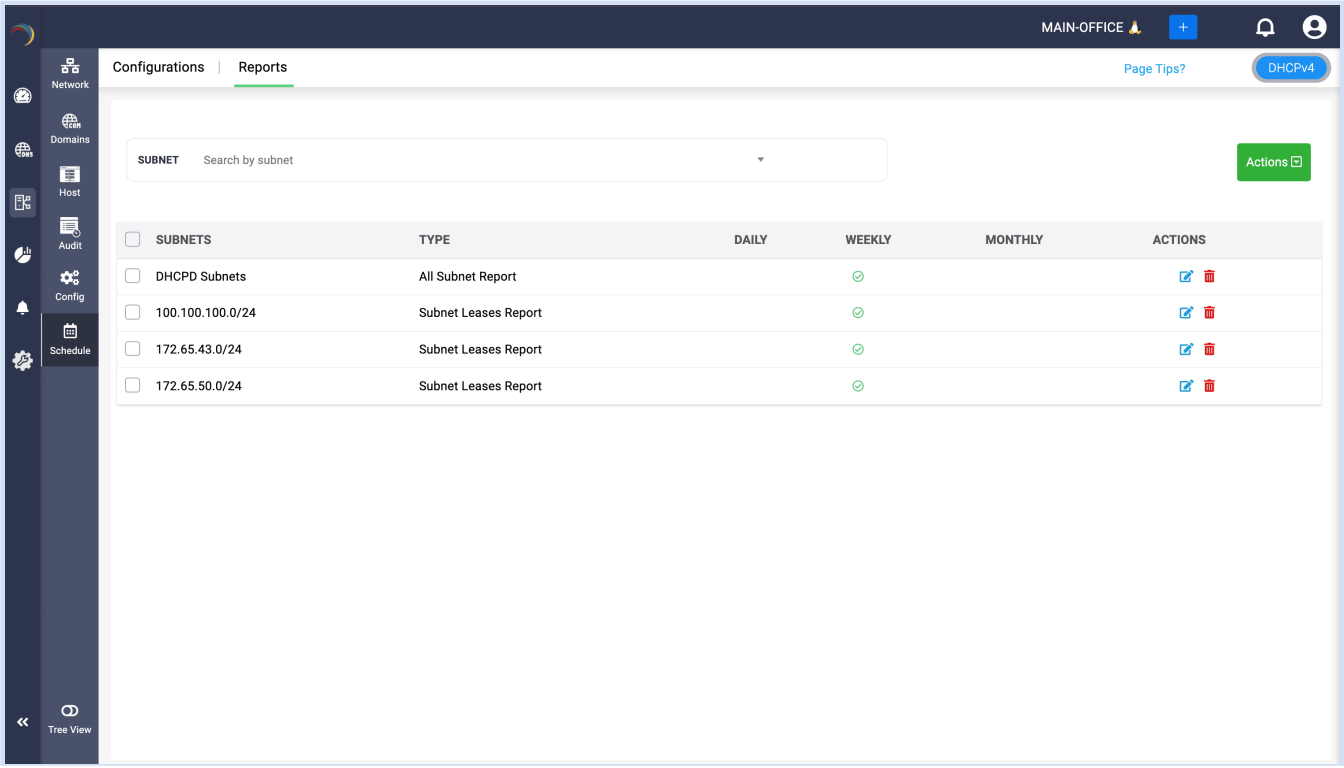


DNS records can be updated whenever the IP address configured to those records change dynamically using Dynamic DNS (DDNS). This ensures that the network is always accessible through hostnames, as they are crucial for dynamic environments and site settings, where frequent configuration changes occur, and real-time updates are needed.

DDI Central can automatically detect and resolve IP address conflicts between users and helps maintain an updated IP address inventory of the site, ensuring reliable connectivity and preventing downtime in sites operations.

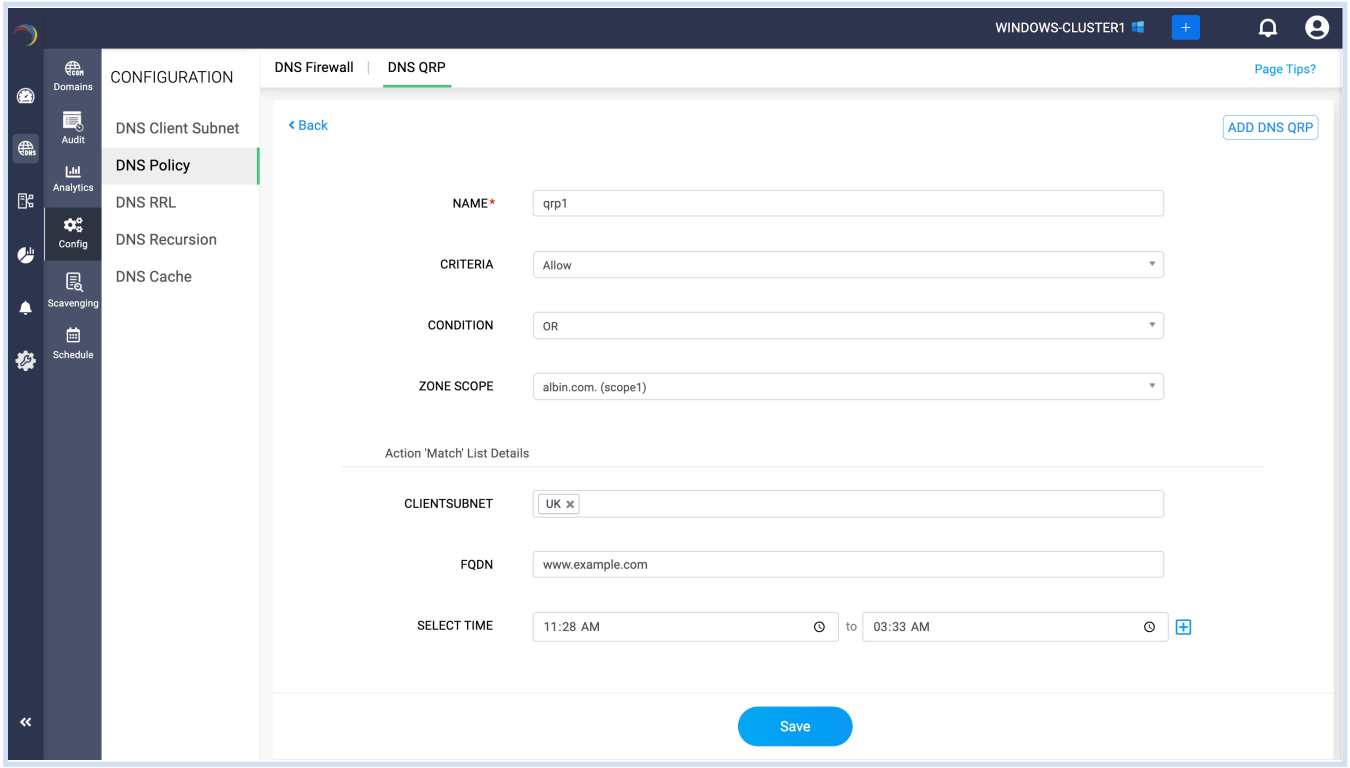


Network admins can set a schedule-and-forget-it mode by enrolling DHCP scopes and DNS records with DDI Central. This enables the admins to implement network expansions or updates at predetermined time periods to maintain the network services' flow.



Scheduled DNS and DHCP reports at consistent time periods help admins to obtain real-time insights over the current subnet capacities and zone query analytics for network planning. Admins can implement automated failover setups for DNS and DHCP services, guarantee business continuity in the event of infrastructure failure in manufacturing networks.

DNS Query Resolution Policies



DDI Central's DNS Query Resolution Policies (QRP) for Windows Microsoft servers can benefit network admins in easily configuring query responses and redirecting clients queries based on criteria like time, internet protocol, transfer protocol and more.

DNS-based attacks occur through servers resolving queries for unauthorized individuals and unauthorized domains, letting attackers breach the network and infect the servers to gain control over the confidential data.

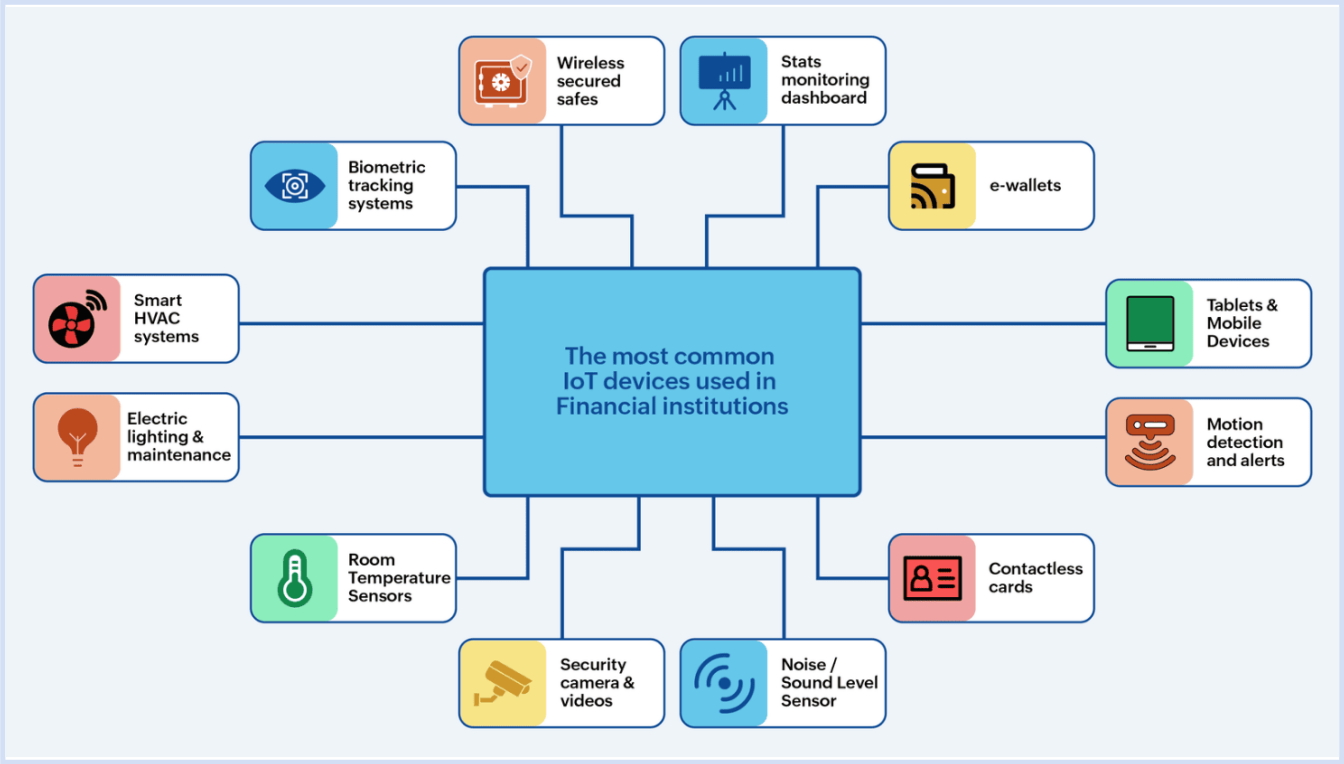
Let's say a manufacturing site, holding onto confidential data of its organization, needs its network admins to have granular control over its DNS resolution. It wants to categorize its responses for different departments and restrict resolving for unauthorized users. It also needs to protect its DNS network from DNS base attacks like DNS amplification attack, DNS cache poisoning, etc.

DDI Central for Windows Microsoft enables organizations to configure DNS responses for different applications or services by defining the zone scopes. They can configure the Actions match list and Actions exemptions list.

These lists help DNS servers to function and allow certain queries to resolve based on the conditions given by the admin. The network admin can configure these lists so that the clients' queries that match these conditions can be resolved, while redirecting the queries that don't match to a safer page.

This helps implement split-brain configuration in Windows Microsoft DNS servers for both internal and external view, so that admins can manage the network traffic and segment the responses for different departments of the organization.

IoT Auto provisioning



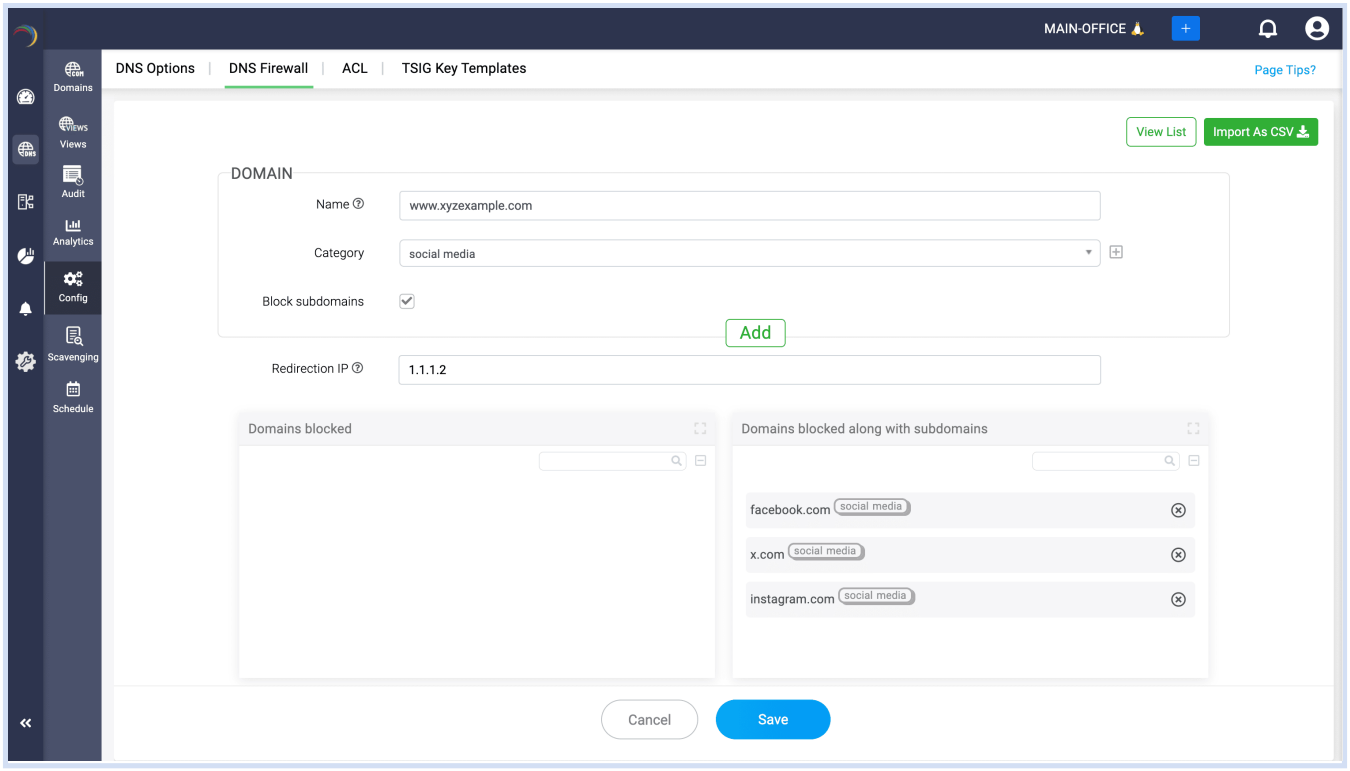
Manufacturing sites are often comprised of multiple different devices for different operations, and each device needs to be connected to distinct network departments for better segmentation. While the subnets are sliced and segmented into different components, the devices joining the network need to be connected to specific subnets allocated for those purposes.

DDI Central can help in these scenarios with the implementation of DHCP fingerprinting through Client Class. Network admins create a Client Class, assign IP addresses at global or subnet level, and provide the devices' MAC address match values.

When the MAC addresses of the devices joining the network match the values given in the client class, they will be categorized and allocated with the IP address configured in that class.This helps in proper IP allocation and device configuration with policies by segregated devices based on their type.

Along with that, implementing by toggling, admins can import the values from the Preboot Execution Environment template to a client class to quickly distribute essential boot files based on the device OS type identification. Firmware and OS files can be deployed into the devices in the manufacturing site by identifying the architecture type.

DNS Firewall



DNS firewall is considered the first line of defense in the network, and it is consist of multiple layers of security. It redirects unauthorized queries with response policy zones and actively blocks malicious activity using domain blocking.

DNS Firewall's Response Policy Zones (RPZs) enables network admins to customize DNS responses for recognizable domain names through configuring the security measures. DDI Central analyzes the queries received in the DNS server based on the RPZ policy configured.

When it matches with the policy settings, the query gets resolved to the respective IP address given, and when it doesn't match, it gets blocked, and the user will be redirected to a safer page.

This helps network admins manage the DNS resolution and prevent unauthorized domains from getting resolved for unauthorized users. The RPZ also logs the queries to blocked domains, providing valuable insights into attempted access to harmful sites and helping to identify patterns of malicious activity.

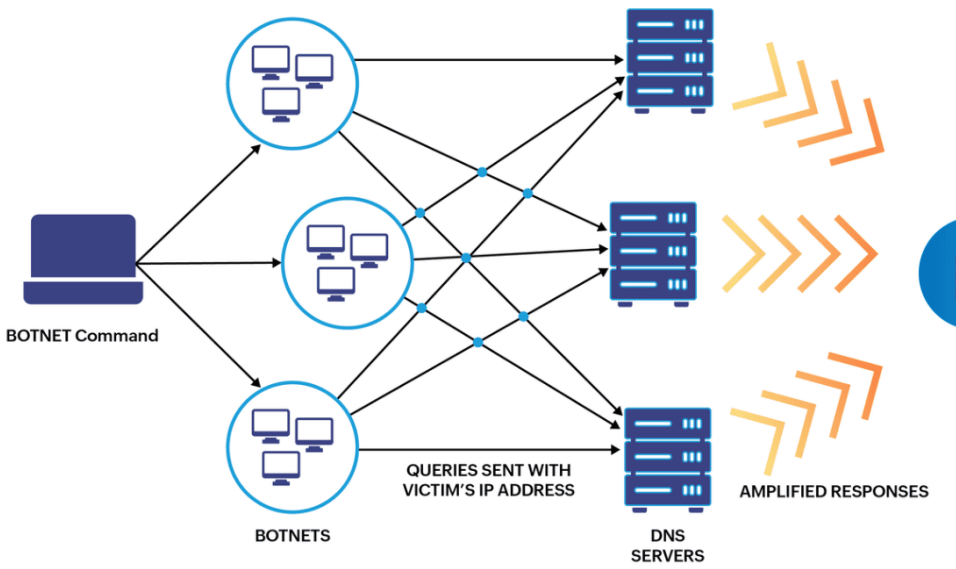
Domain blocking or DNS blocking in DDI Central can help during malware situations. Certain malware, when connected to the sites' network, can covertly try to access malicious domains with the DNS resolver.

DNS firewall maintains a deny-list comprising a recognized collection of undesirable domains for blocking. Before the resolver can provide the actual IP address, it checks the domain against this deny-list.

If there is a match on the deny-list, the resolver does not proceed to fetch the real IP address from the external authoritative DNS server. Instead of connecting to the malicious site, the user is redirected to a safety page.

With the analytics page, you can identify which host is violating policies and accessing malicious sites from your network and at what time. Network admins can be alerted about any form of security breaches.

Response Rate Limiting

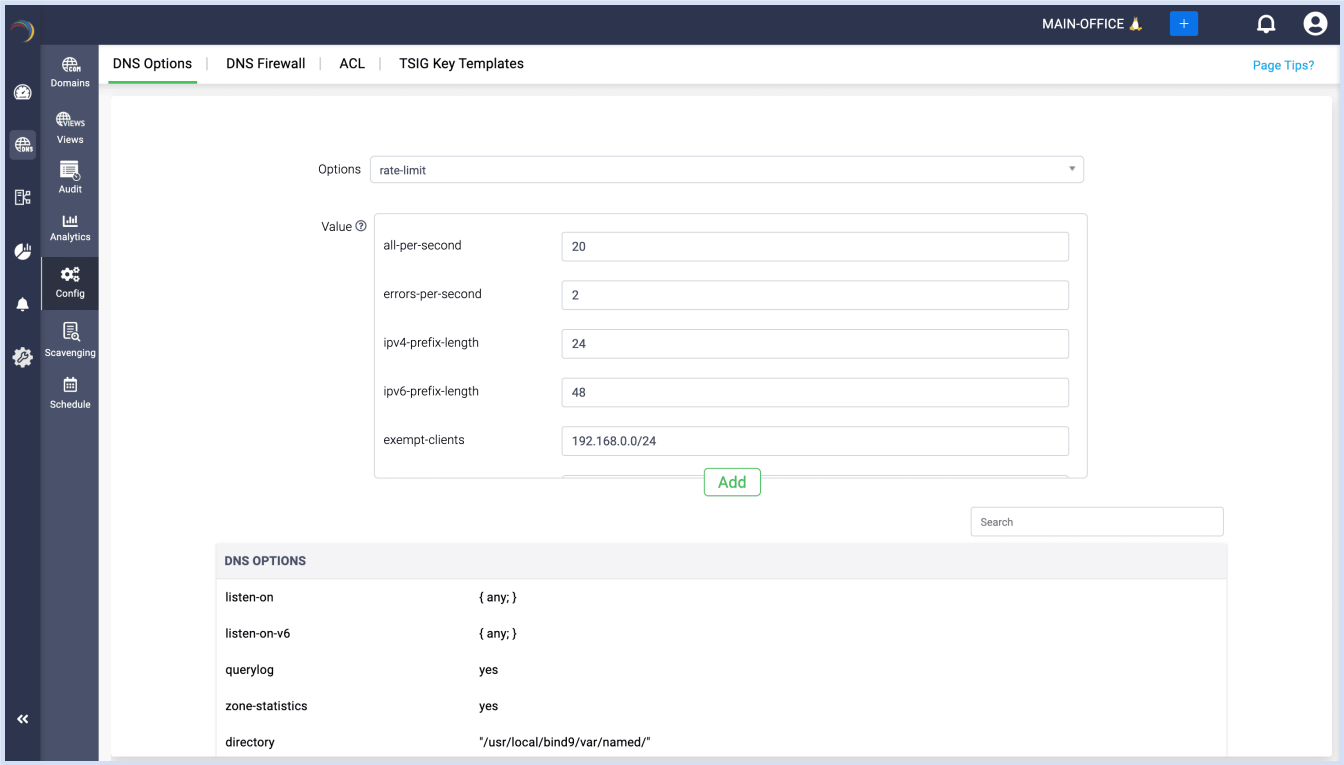


Let us dissect a common cyberattack scenario, DDoS attack, that involved a botnet in the manufacturing site. A Botnet command center targets a particular victim's network in the site and starts sending instructions to the botnets.

These botnets then attacks the DNS servers by sending malicious queries with the victim's IP address, this is known as IP spoofing.

The DNS servers respond to these queries without identifying whether they are safe or malicious. However, due to the nature of the attack, these responses are not just simple replies. They are massively amplified, meaning a small query triggers a large response.

These responses start to flood the DNS servers, overwhelming it with data, and leading to servers going down and network disruption.

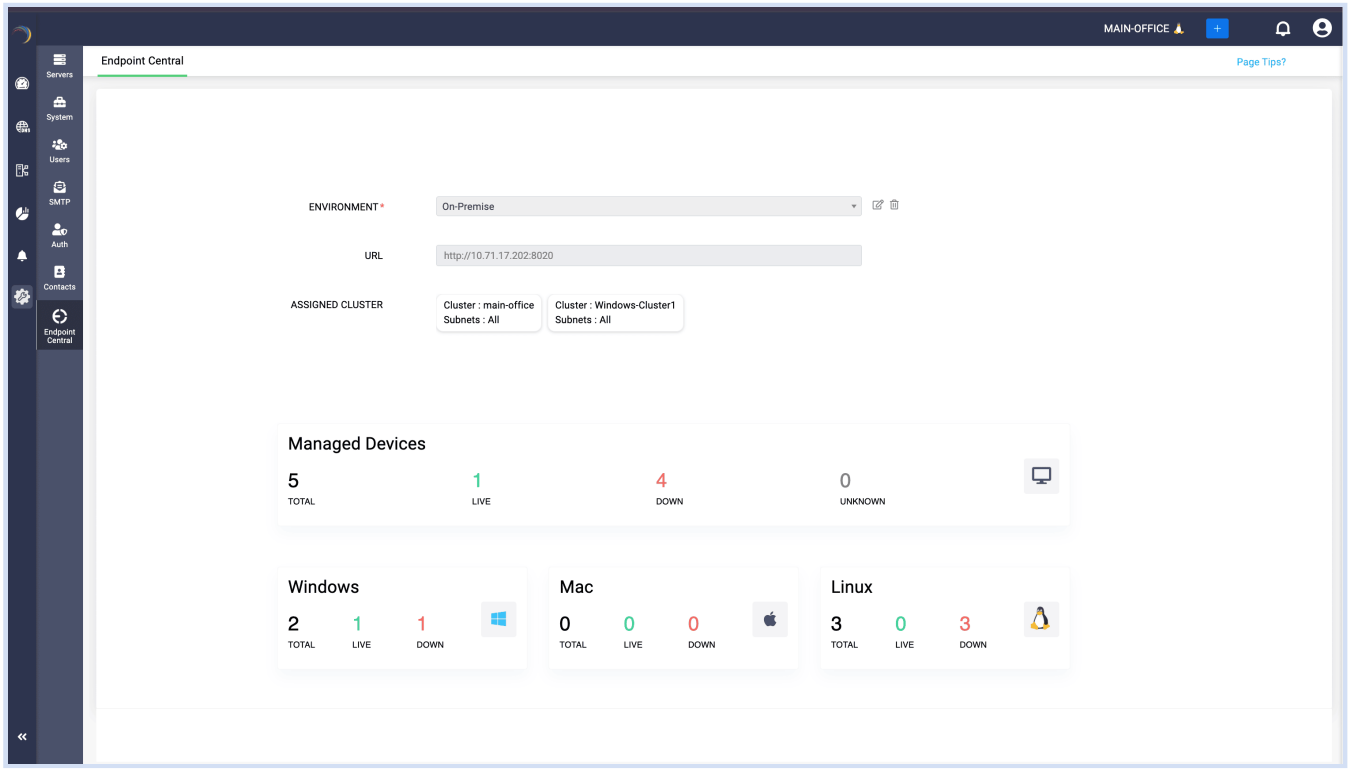


DDI Central's Response Rate Limiting (RRL) helps mitigating the DDoS attacks. Network admins can configure the servers to limit the response rate for a specific query. This helps prevent DNS servers from being used as amplifiers to send multiple responses and prevent malware spreading from compromised end-user systems to more sensitive systems and data center resources.

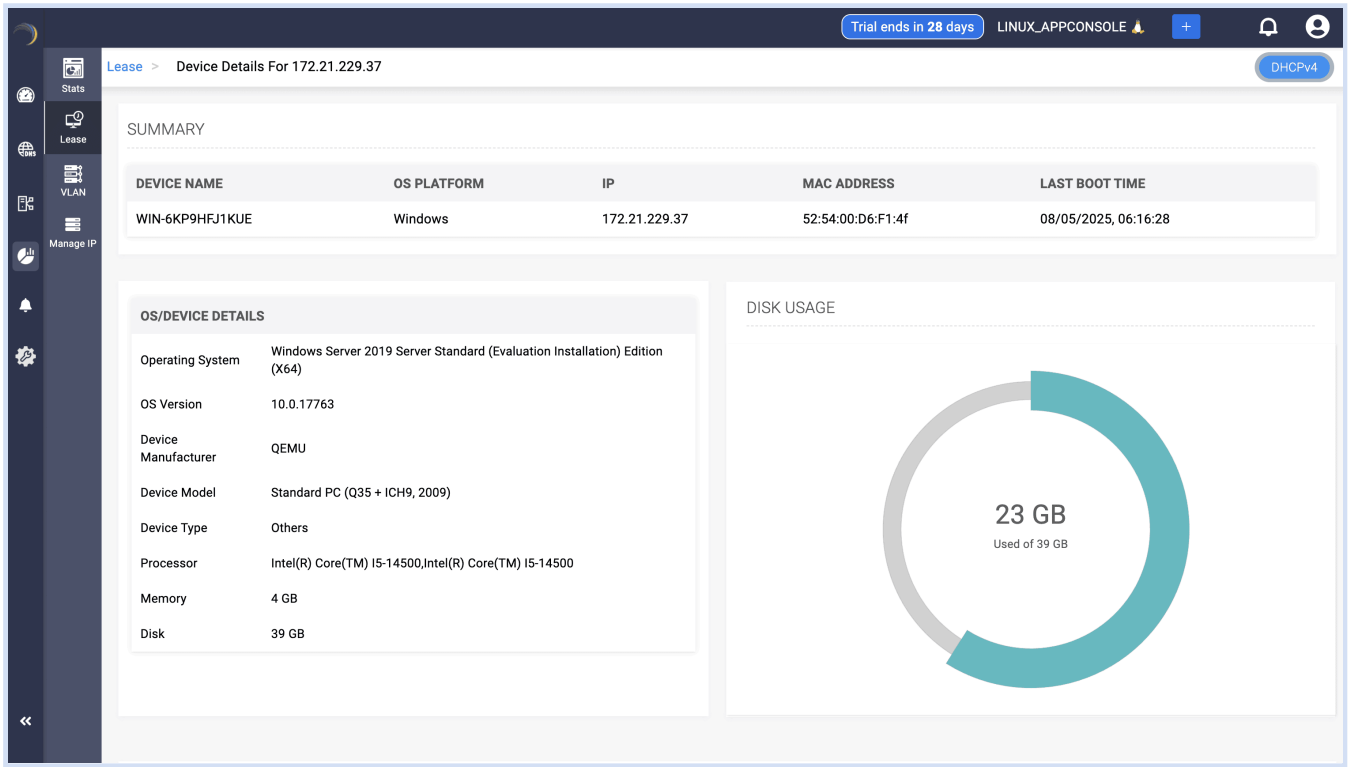
Response rate limiting is a DNS security feature that intelligently regulates response throttling to mitigate the impact of DNS amplification attacks, ensuring uninterrupted access for legitimate clients and upholding a well-balanced approach to security.

It facilitates a selective response mechanism that ensures your network is not only resilient against attacks but also remains efficient and reliable for legitimate users.

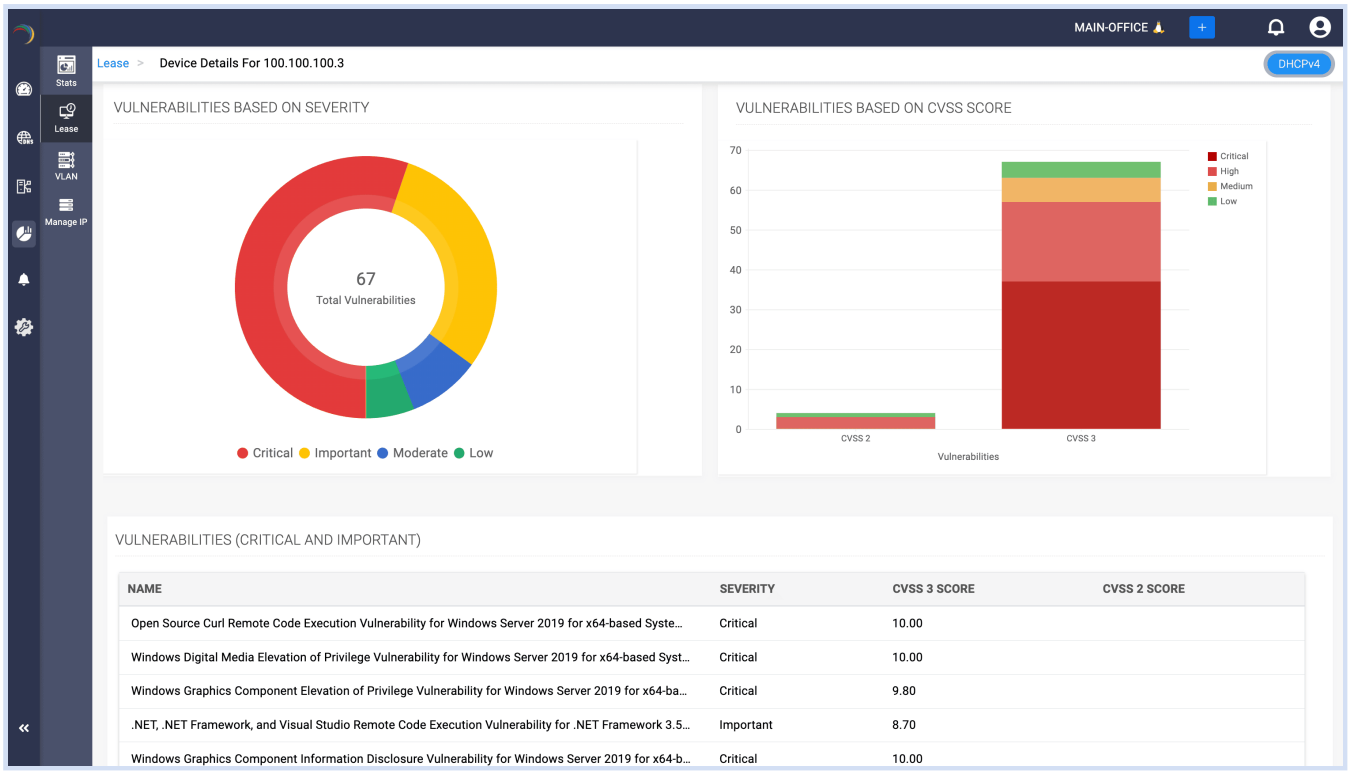
Endpoint Central

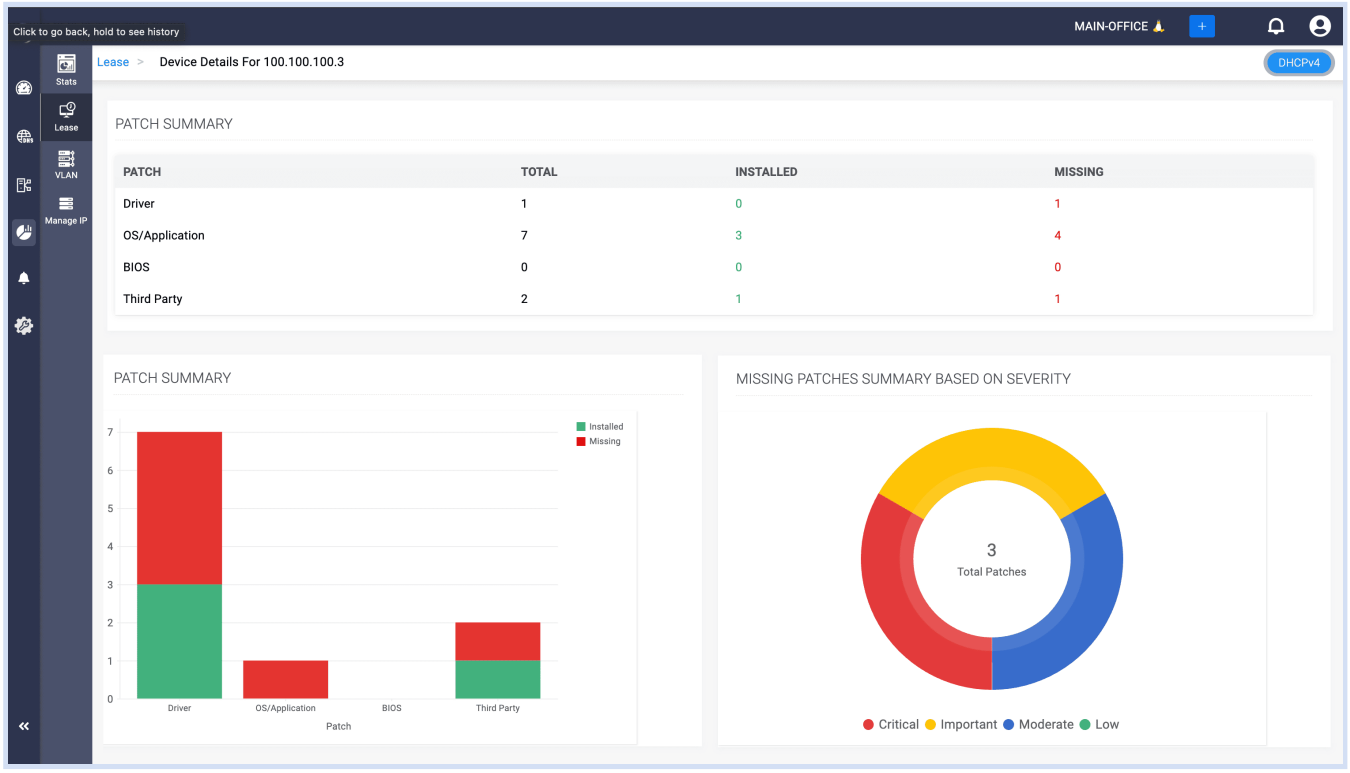


DDI Central facilitates integration with ManageEngine Endpoint Central where network admins can configure their Endpoint Central application database within DDI Central dashboard to receive deeper insights over the details of IP leased devices, and their vulnerabilities and patches.



This requires knowing which endpoint device is using a DHCP lease, and which unpatched or high-risk machines are in the network so they can be isolated by blocking the DNS resolution or reclaiming the lease assigned. This increases the security level in the network.





Vulnerability and patch details of devices are visualized for network admins to resolve the missing patches and vulnerabilities with high priorities before network disruption occurs.

Managing hybrid resources in DDI Central

A manufacturing plant, consisting of multiple devices for different operations, needs them to be connected to its network. The devices should not face any IP address conflicts or network overlapping, so their network needs to be categorized based on their purpose and priority for effective IP leasing.

The networks need to implement policies for the network segments sharing the same functionality for simplified management. They need to have manual control over their critical devices, servers, and data centers without relying on dynamic IP allocation.

They also need to isolate specific segments of the network for selected devices, like VoIP phones, where the IP allocation requests shouldn't be interrupted by other departments.

Use case:
Improving network connectivity for remote manufacturing employees

With the rise in remote work due to the impact of COVID-19, there came demand among many industries, including the manufacturing sector, for employees to work from remote locations. The manufacturing sector now has enabled machines like industrial robots, conveyor belt systems, automated guided vehicles, and supervisory control and data acquisition systems to be operated from remote locations, which is convenient and safer for complicated tasks.

Expanding the network across different remote locations will make the boundaries vulnerable for attackers to breach in and cause damage to the infrastructure. Adopting a hybrid workplace environment makes it even more crucial to secure the network and ensure only workers are allowed to access confidential resources and covert access is prevented.

To resolve this problem, DDI Central provides the Client Class feature, where administrators can configure a client class that programs the DHCP server to recognize the client device, allowing only authorized workers to enter the network.

Let's say there are 10 workers in charge of operating industrial robots from a remote location; the client class will be defined to identify the MAC address of those 10 workers and allow them to get the IP leased.

Say one of them is stuck with a certain operation and they need support from their team; they can invite one of the members in the group of 10 to collaborate with them, which can also be done with the help of the client class.

Conclusion

A full-stack DDI solution consolidates all essential tools into a single interface, streamlining network administration and enhancing efficiency. While some plants use freeware or open-source DNS and DHCP server software, or manage networks with spreadsheets, these approaches often lack the robustness needed for complex configurations.

DDI solution eliminates these costs and frees admins from routine tasks, allowing holistic visibility and centralized management across distributed sites. DDI solutions synchronize security, management, and operational efficiency, safeguarding manufacturing networks from cyber threats. As cyber threats evolve, DDI's importance in site networks will grow, making it a crucial component of digital infrastructure.

In an era of rapid digital transformation in the manufacturing sector, embracing DDI solutions is more than a technological investment. It marks a manufacturing unit's commitment towards delivering high-quality, flexible, and reliable network services that the internal employees expect.


ManageEngine
DDI Central