ManageEngine
DDI Central

How DDI solutions optimize retail network infrastructures

Contents

Introduction

Digital transformation has significantly changed the way many business sectors operate, including retail. Companies like Amazon and eBay have set a new standard for modern consumers, who often now expect a seamless blend of physical and digital shopping experiences. This demand has pushed many retail businesses to adopt digital solutions to make shopping easier and more efficient.

To meet these expectations, retail businesses have expanded their network infrastructures by creating mobile apps and e-commerce websites, and by offering in-store Wi-Fi and connected point-of-sale systems. However, this also makes their networks more vulnerable to cyberattacks.

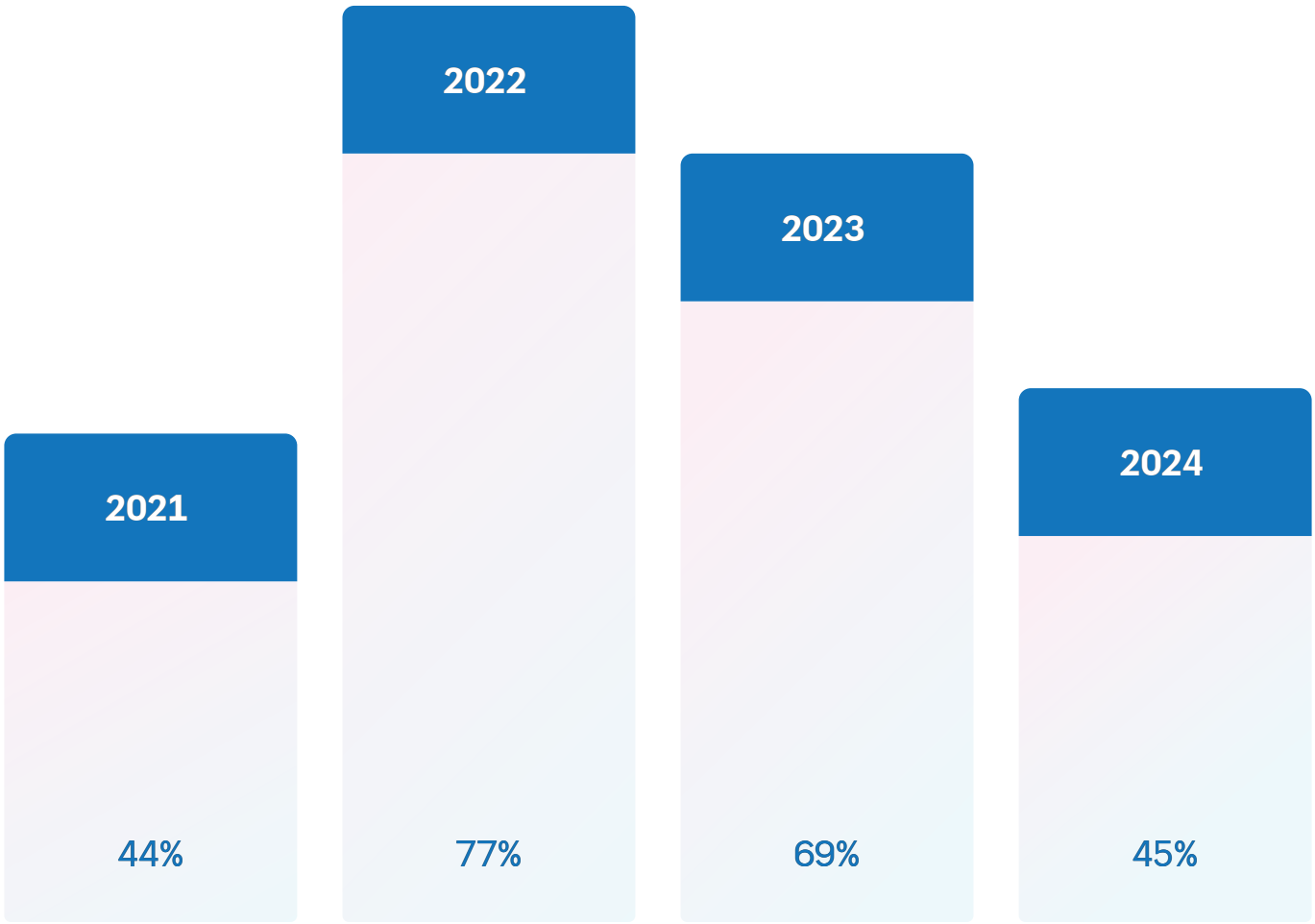
To meet these expectations, retail businesses have expanded their network infrastructures by creating mobile apps and e-commerce websites, and by offering in-store Wi-Fi and connected point-of-sale systems. However, this also makes their networks more vulnerable to cyberattacks.

This whitepaper explains how DDI solutions simplify network management, helping administrators improve network efficiency and security.

Understanding major cyberattacks in the retail sector

The retail sector has been impacted by cyberattacks and threats recently as organizations are implementing digital transformation and adopting IT solutions to enhance their productivity and efficiency. In 2024, 80% of the retailers have experienced at least one cyberattack, and only half of them reported their attacks, according to VikingCloud's retail cyber threat survey.

A survey on ransomware attacks of more than 5,000 IT cybersecurity professionals by Sophos isolated the findings of more than 577 in retail organizations across 14 different countries over the past four years.

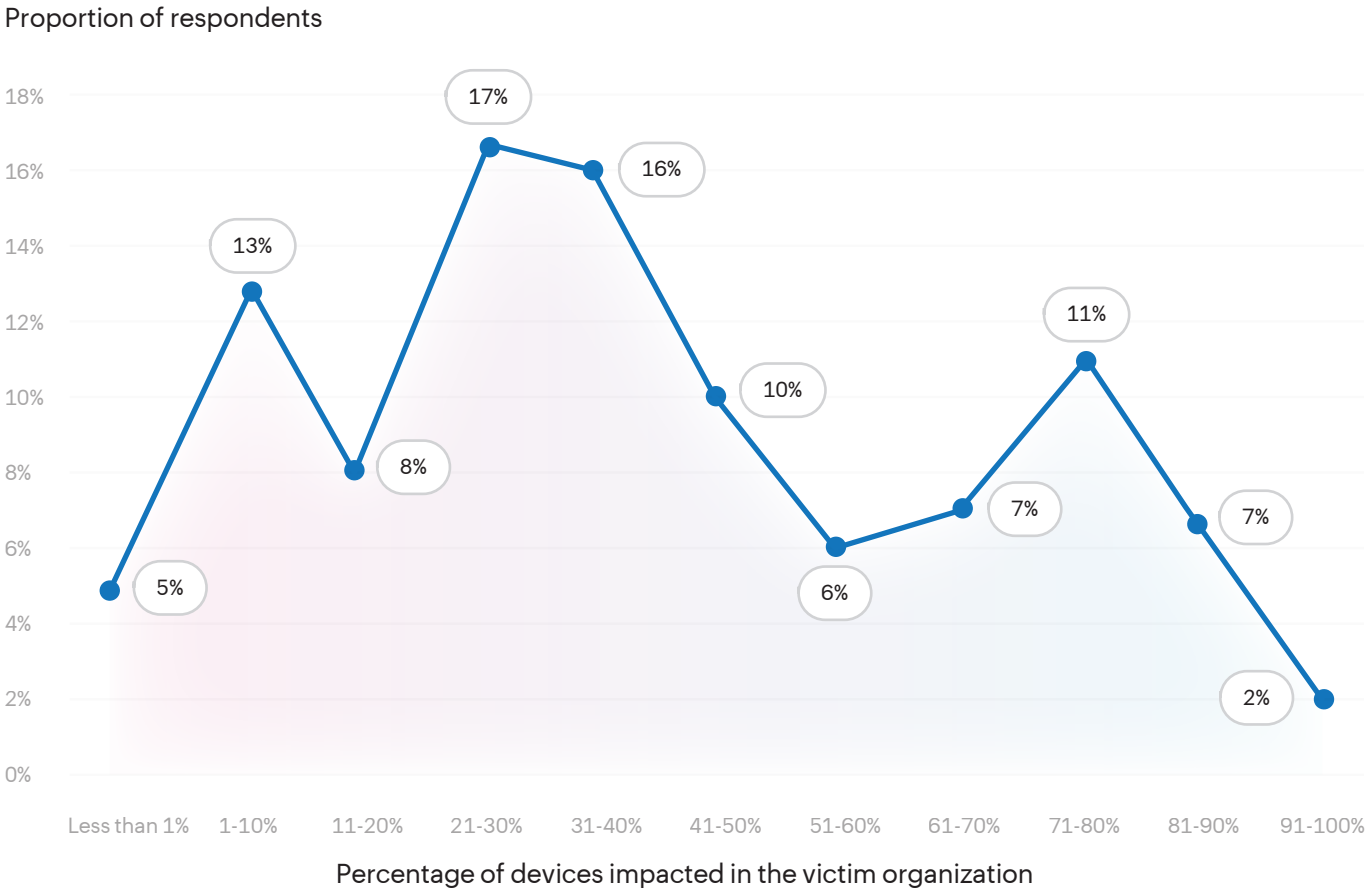


Year-by-year organizations hit by ransomware

The report concluded that there was a gradual increase and decrease of the ransomware attack rate from 2021 to 2024. The starting point for the increase of ransomware was 2021, when 44% of these attacks succeeded. Then, many retailers decided to implement digital solutions to adapt their digital shopping environments to combat ransomware attacks.

Threat actors accelerated their efforts and the attack percentage increased to 77% the next year which prompted many retailers to lose confidential data to cyberattackers. Retailers fought back by implementing different strategies and solutions to mitigate the attacks. As a result, a decrease in the percentage to 69% the next year was achieved, and a more significant drop, to 45%, was achieved by 2024.

The percentage of attacks reported by retail companies in 2024 was decreasing to 59%, comparative lower than the 66% percentage reported in 2022 and 2023. Also, the number of organizations who reported that all their devices got impacted by the attack was found to be minimal.



Only 2% of the retail companies reported that 91% or more of their devices were affected by the ransomware attacks. On the other hand, 5% of the organizations reported that fewer than 1% of their devices were impacted.

One important way they reduced the rate of cyberattacks is by using the right solution to streamline network services. DDI solutions help secure the network infrastructure of the retail sector with a centralized view of the core network services, security policies, custom options, network segmentation, network automation, and more.

Networking demands of the modern retail sector

Retail companies facing growing cyberthreats and security challenges require a robust network solution that addresses their unique operational demands. Here are some of the key requirements:

A unified platform to manage services

Retail sector requires a unified network management platform that provides admins with a single interface to configure, monitor, and manage all network devices and settings across multiple store locations. This streamlines operations by simplifying tasks like troubleshooting, firmware updates, and policy enforcement, reducing the need for manual on-site IT support.

In-store network with connectivity across branches

Establishing reliable and secure communication channels between different retail locations is crucial for seamless collaboration, real-time analytics, and consistent customer experiences. This enables centralized control over retail operations and allows stores to access point-of-sale systems and cloud-based applications.

Robust network security

Implementing robust security measures and adhering to regulatory standards in the retail sector is essential for protecting sensitive customer data, such as payment information and personal details, while ensuring compliance with industry regulations like PCI DSS and others. Strong security and compliance help foster trust among customers, partners, and vendors.

Monitor and manage network traffic

Continuous monitoring of data flows across the retail network helps identify potential cyberthreats, unauthorized access, and optimize traffic routing between stores and headquarters. In a retail environment where sensitive customer data and transaction information are constantly exchanged, real-time network visibility helps detect security breaches, system anomalies, or connectivity issues early.

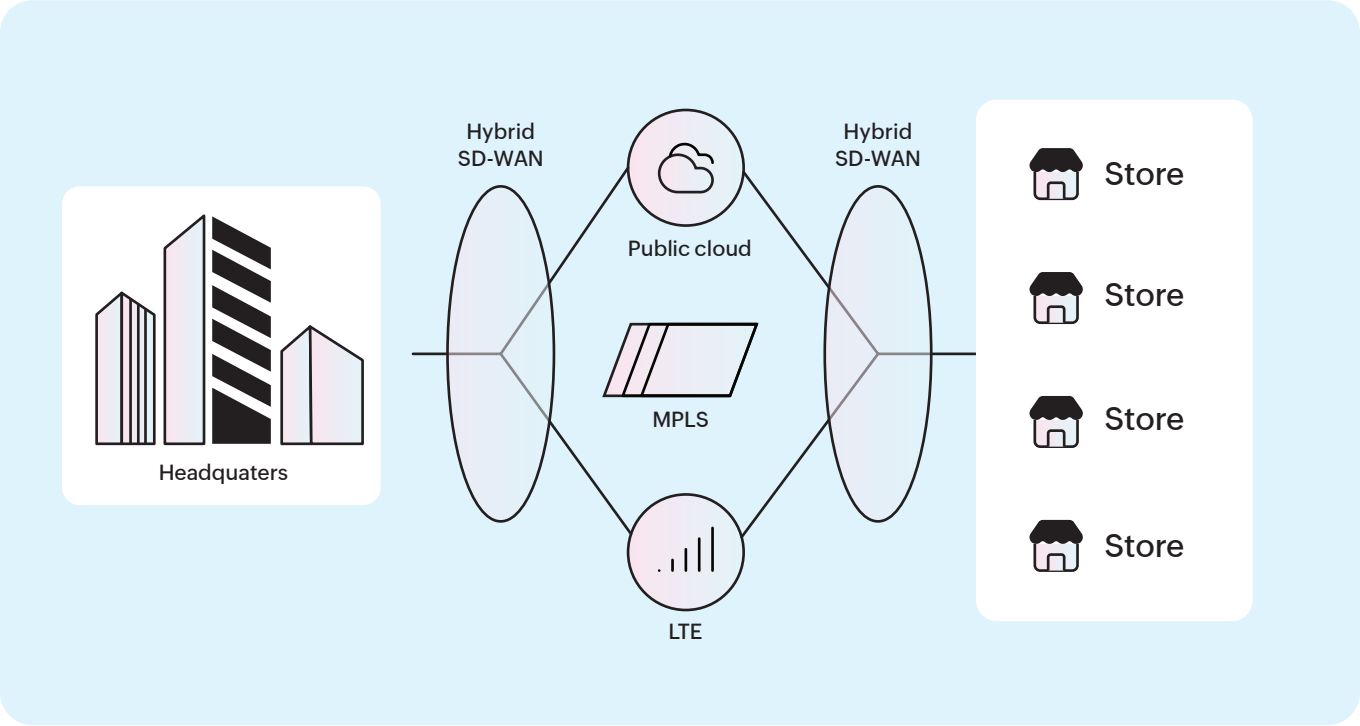
Visibility over network resources

Having a clear visual breakdown of each store's IP addresses, client devices, subnets, DNS queries, and related network metrics helps network admins in the retail sector maintain smooth operations. This level of visibility enables IT teams to identify and troubleshoot network issues, detect potential data breaches, and resolve connectivity problems quickly.

Facilitate a hybrid work environment for remote and in-office employees

Retail sector needs technologies that enable seamless collaboration and access to resources for employees across diverse environments, whether at headquarters, in- store, or working remotely. Ensuring remote access to the organization's applications and data allows staff to stay productive and aligned with business goals from anywhere.

Private WAN network distributed across multiple retail stores

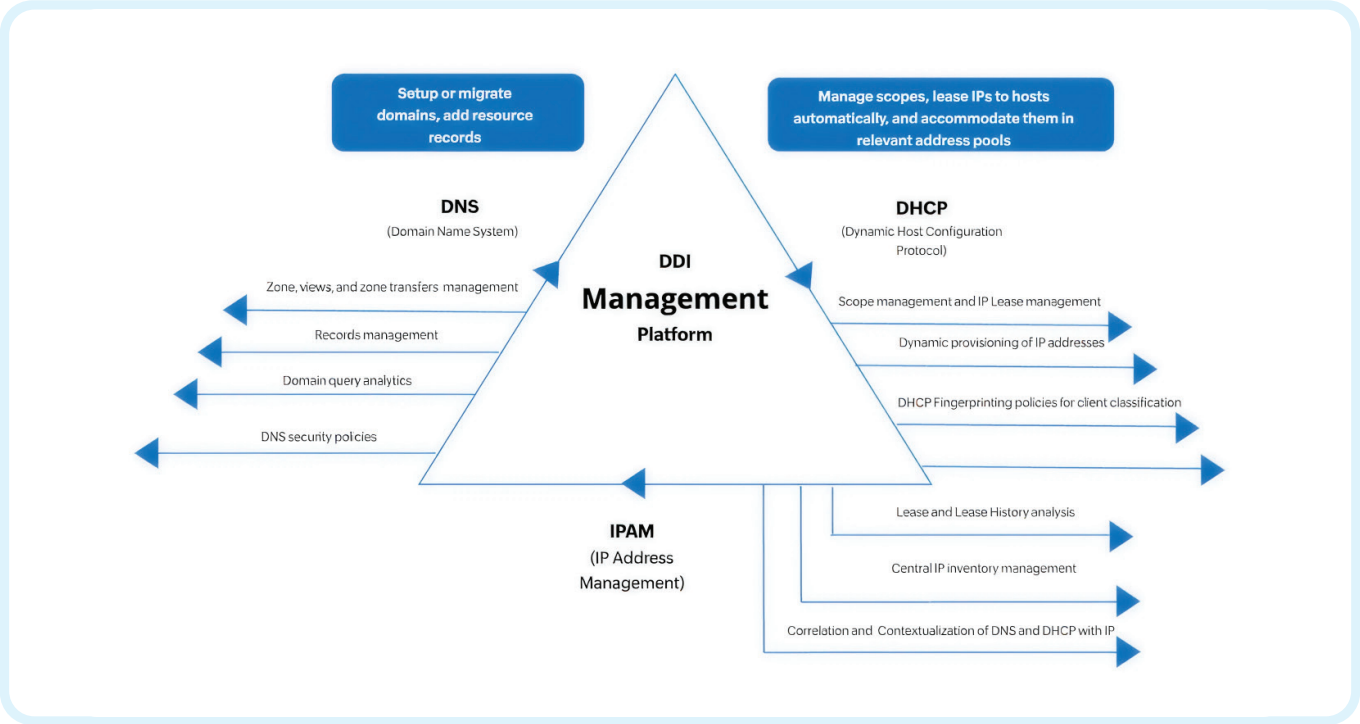


This schematic diagram illustrates a retail sector's private WAN network architecture that connects the central headquarters with multiple remote store locations. At the core of the setup is a software-defined wide area network (Hybrid SD-WAN), which enables dynamic and efficient routing of the network traffic.

The headquarters and stores are connected through this hybrid SD-WAN, leveraging a multi-protocol label switching (MPLS), LTE cellular networks, and public cloud connectivity.

The hybrid SD-WAN enables employees to connect with the stores' network from their remote location. This involves a high performance private WAN serving as the backbone. Now, the main challenge for this network infrastructure is bringing all the stores together under a common IP framework. This is where a DDI solution plays a crucial role.

How DDI Central improves the retail network experience

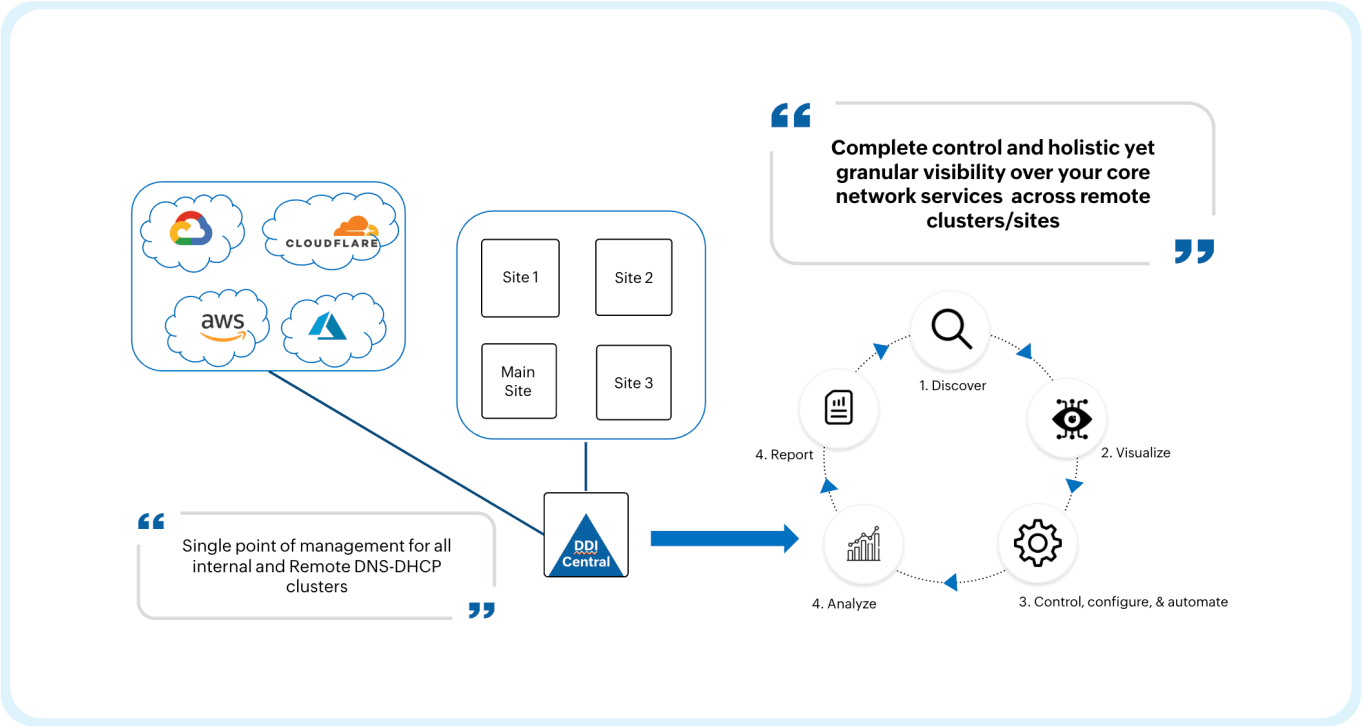


ManageEngine DDI Central is a user-friendly, specialized platform that unifies DNS, DHCP , and IPAM into a single interface, enhancing operational efficiency and network stability. It supports the management of Microsoft Windows DNS and DHCP clusters, as well as existing Linux-based ISC-Bind9 and ISC-DHCP installations, and also allows for the setup of new clusters.

In retail environments, DDI Central acts as a centralized point of administration for networks across multiple store locations and regional branches. With DDI, the three essential network services, DNS, DHCP , and IPAM, can be centrally managed and configured across remote retail stores connected to the corporate network through SD-WAN, IP/MPLS core via VPN, or point-to-point (P2P) links.

When a retail store onboards its DNS and DHCP servers into a dedicated DDI Central, discovering, consolidating, and organizing all of the core network configuration.

With all configurations neatly presented in the UI, DDI Central empowers network administrators to efficiently control core network services and take necessary actions. The built-in visual analytics within each module provide quick insights and actionable data to help with rapid troubleshooting and informed decision-making.



This centralized approach enables IT teams at the main corporate office to gain a holistic view and unified control over the network services deployed across various store locations, all from a single console.

Importance of network segmentation in the retail sector

Network segmentation enhances security by dividing a larger network into smaller, manageable sections and layering multiple protections across the infrastructure. This approach ensures IT administrators can isolate servers and endpoint devices according to their respective roles or functions.

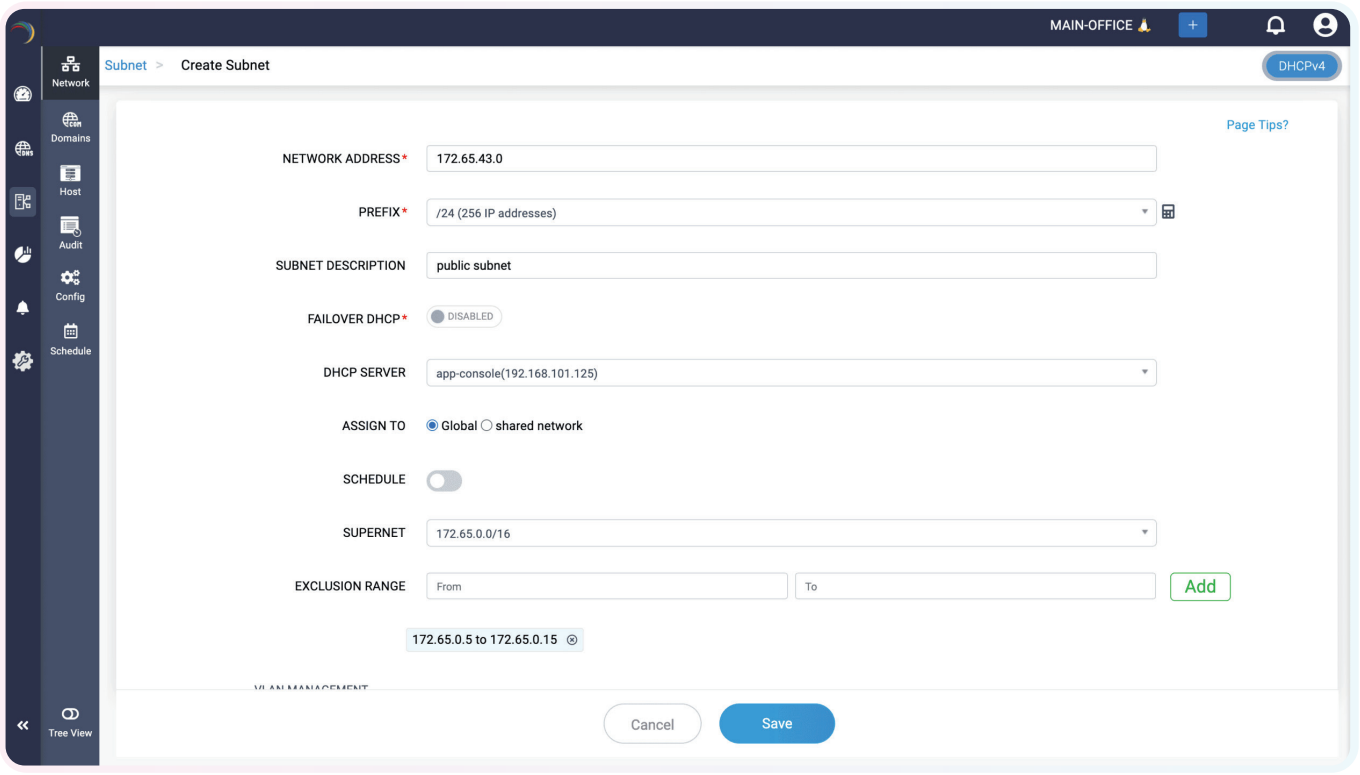
With a DDI solution, segmentation provides deep visibility into each network segment, including associated devices, policies, and DHCP configurations. This enables network admins to monitor activity more effectively and quickly detect signs of malicious behavior or resource strain.

In the event of a security breach, segmentation plays a crucial role by containing the threat within a defined zone, thereby minimizing its impact and preventing it from spreading to other parts of the network.

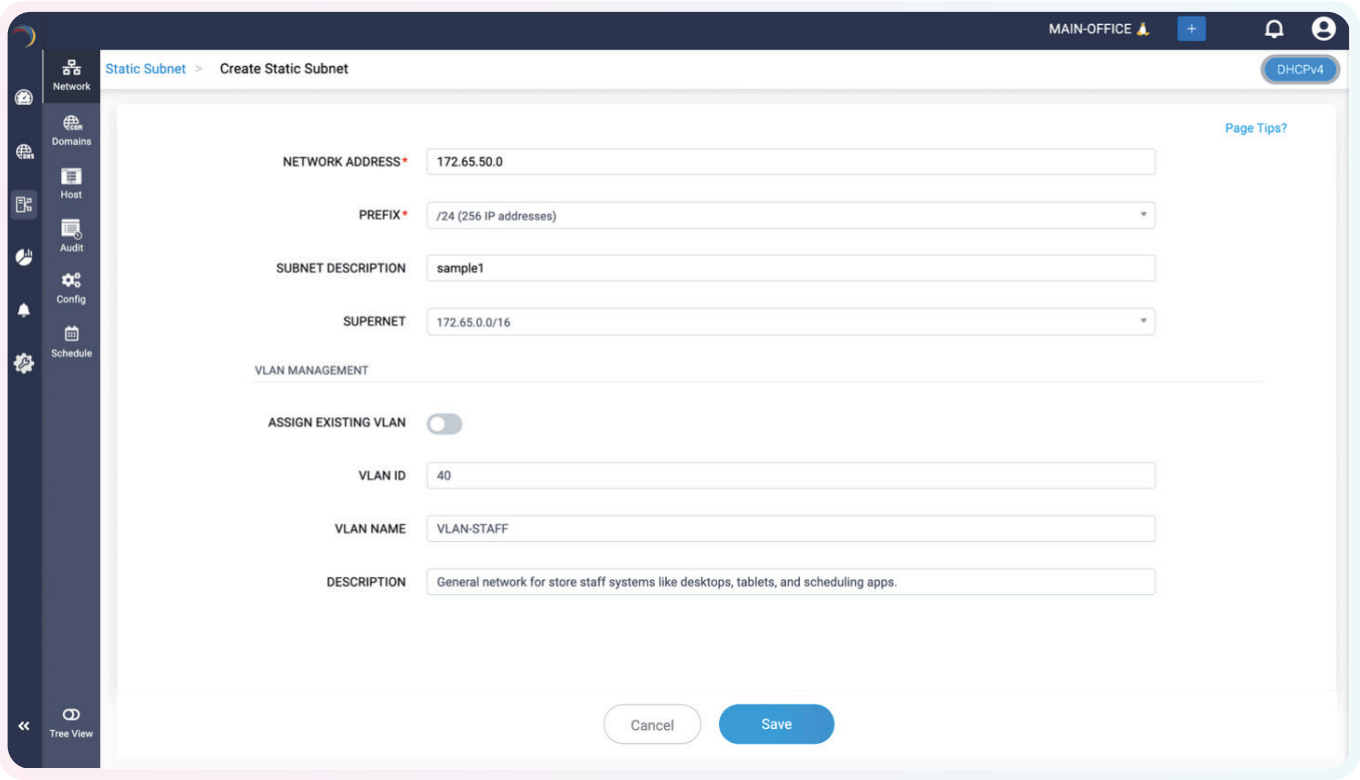
Let's understand the importance of network segmentation in the retail sector for structured network infrastructure with a scenario.

Scenario : A retail chain with multiple store locations and diverse in-store devices—such as POS systems, barcode scanners, digital signage, CCTV cameras, and staff terminals—requires a well-structured network to ensure seamless connectivity. To avoid IP conflicts and overlapping address spaces, devices need to be logically categorized based on their function and priority, enabling effective IP address leasing and network management.

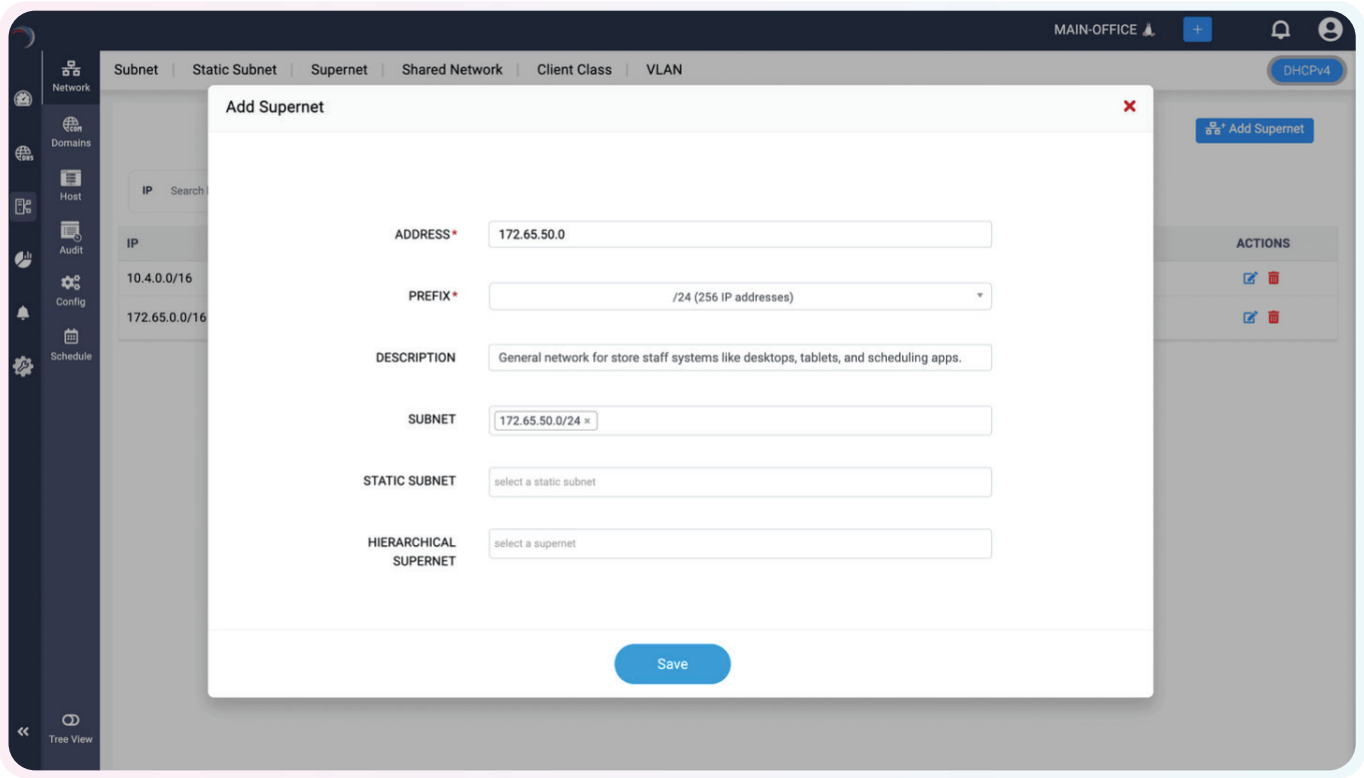
To simplify administration and enhance control, the network should implement policies that segment devices with similar roles into designated network groups. Critical systems like payment servers, inventory databases, and security systems require manual IP management to ensure stability and high availability, rather than relying on dynamic IP assignments. Additionally, certain device types, such as VoIP phones or guest Wi-Fi users, need to be isolated on separate segments so that their DHCP traffic is not affected by unrelated services.



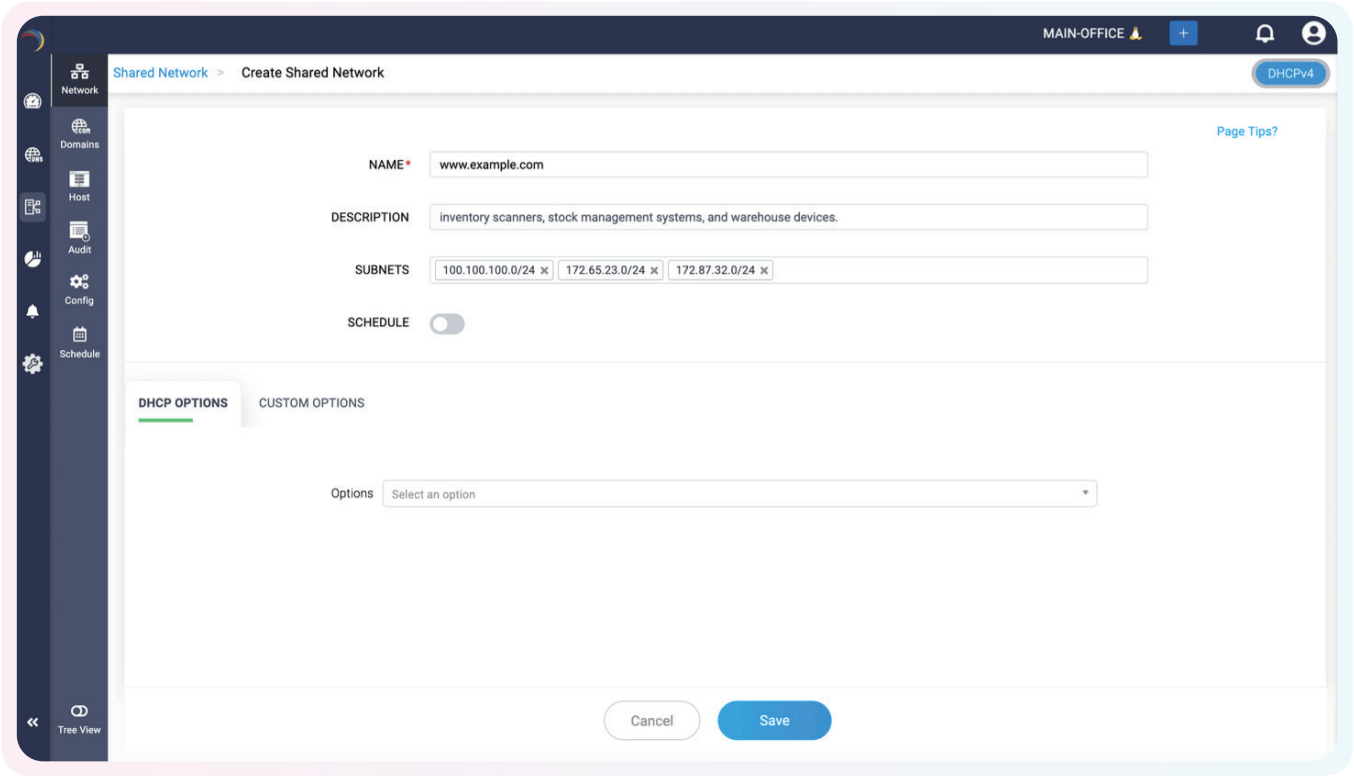
Network administrators can create dedicated subnets with separate IP pool ranges for different device categories—for instance, POS terminals, customer-facing kiosks, surveillance systems, and back-office desktops. This ensures each device group receives IPs from its own pool, eliminating conflicts and enabling consistent performance across the store network.



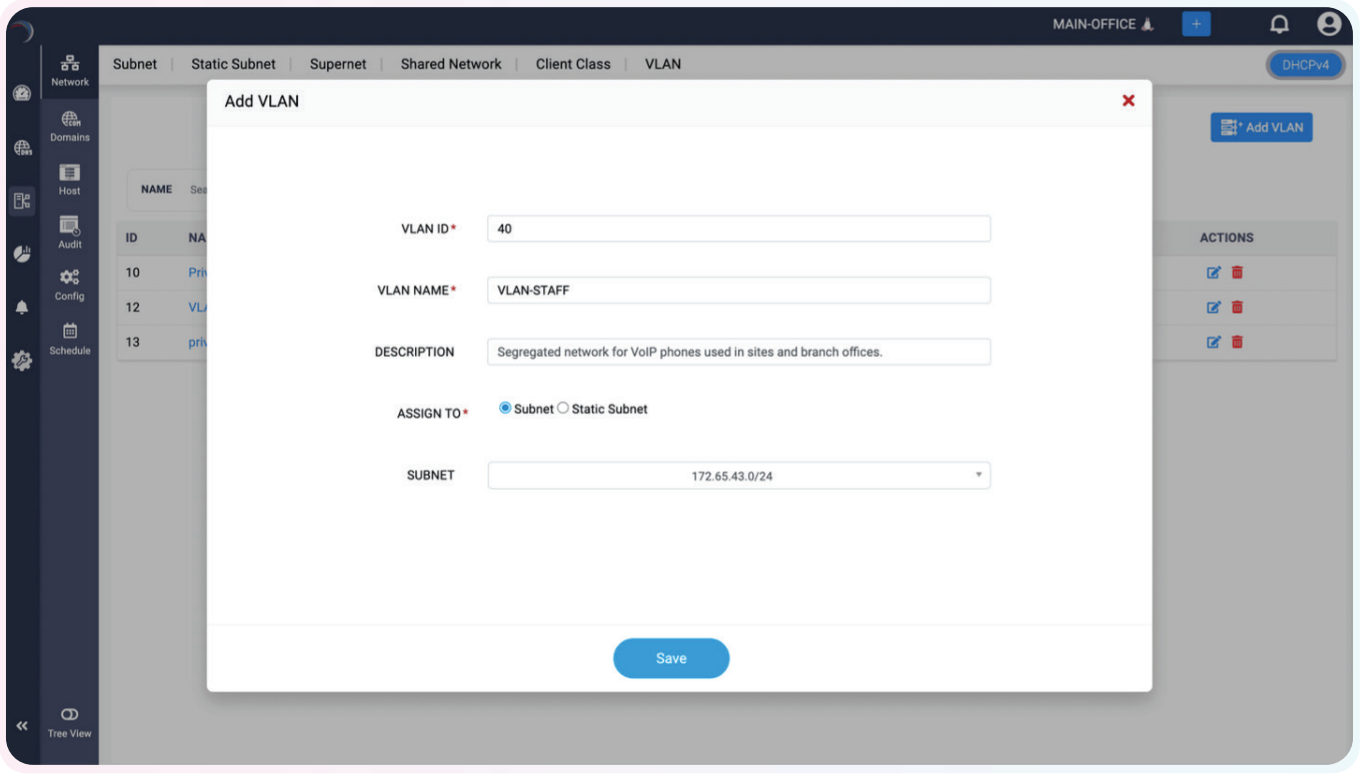
For mission-critical systems such as payment processing servers, in-store data hubs, and remote access gateways, static subnets can be defined with specific pool ranges. This gives administrators full manual control over IP assignment, ensuring these vital systems operate with uninterrupted connectivity and are not impacted by dynamic address changes.



To improve routing and manageability, multiple subnets across store locations can be combined into a single supernet and organized hierarchically. This enables network admins to visualize and manage the infrastructure more effectively, while supporting scalability across growing retail operations.



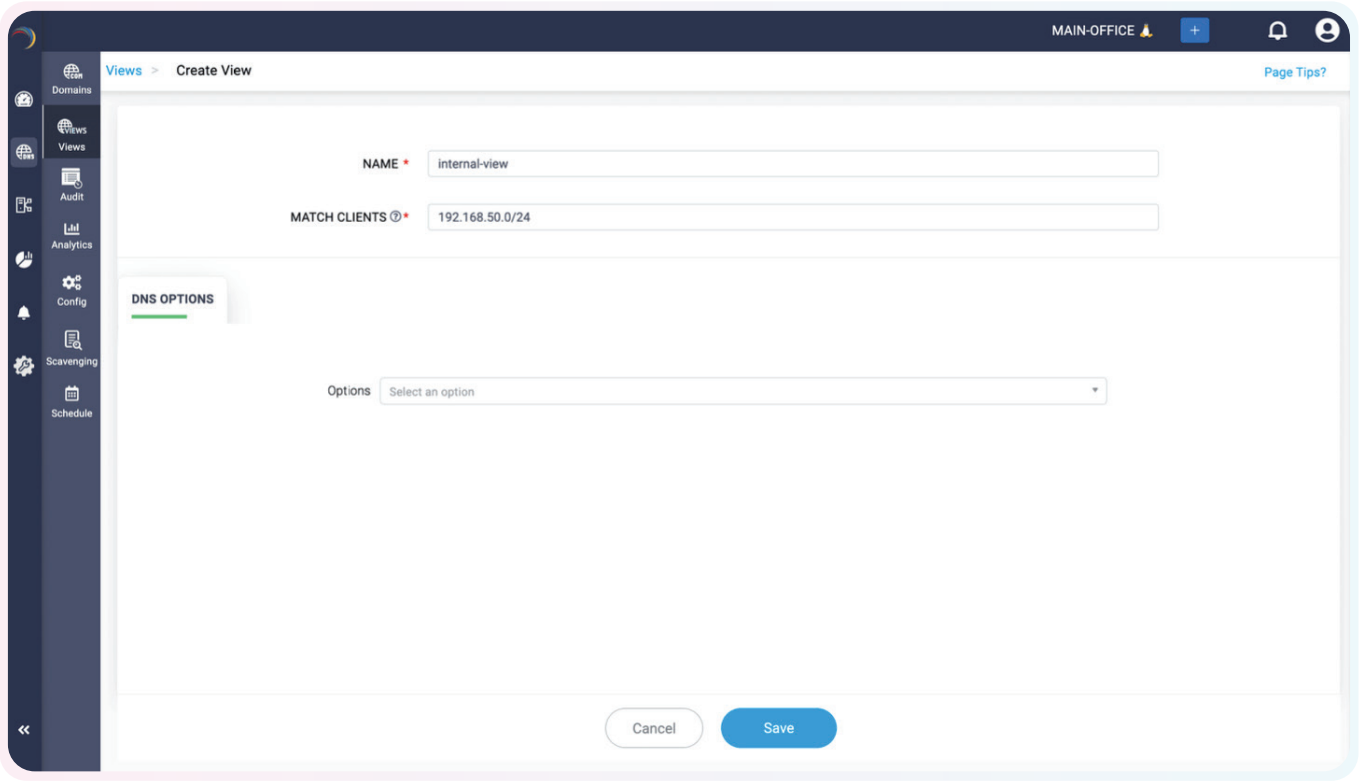
When devices across different subnets share common configurations and policies, they can be grouped into a single Shared Network, simplifying DHCP management for network administrators.



VLANs play a vital role in isolating device broadcast traffic within the network, ensuring efficient communication between specific devices and the DHCP server without external interference. For example, VoIP phones in stores can be assigned a dedicated VLAN by defining a VLAN ID, name, and description. This VLAN can then be mapped to its corresponding subnet, ensuring that IP requests from VoIP devices are handled separately and securely, without interference from POS terminals or staff computers.

By segmenting the retail network in this way, organizations can enhance security, streamline troubleshooting, optimize resource usage, and ensure a consistent and reliable experience for both employees and customers.

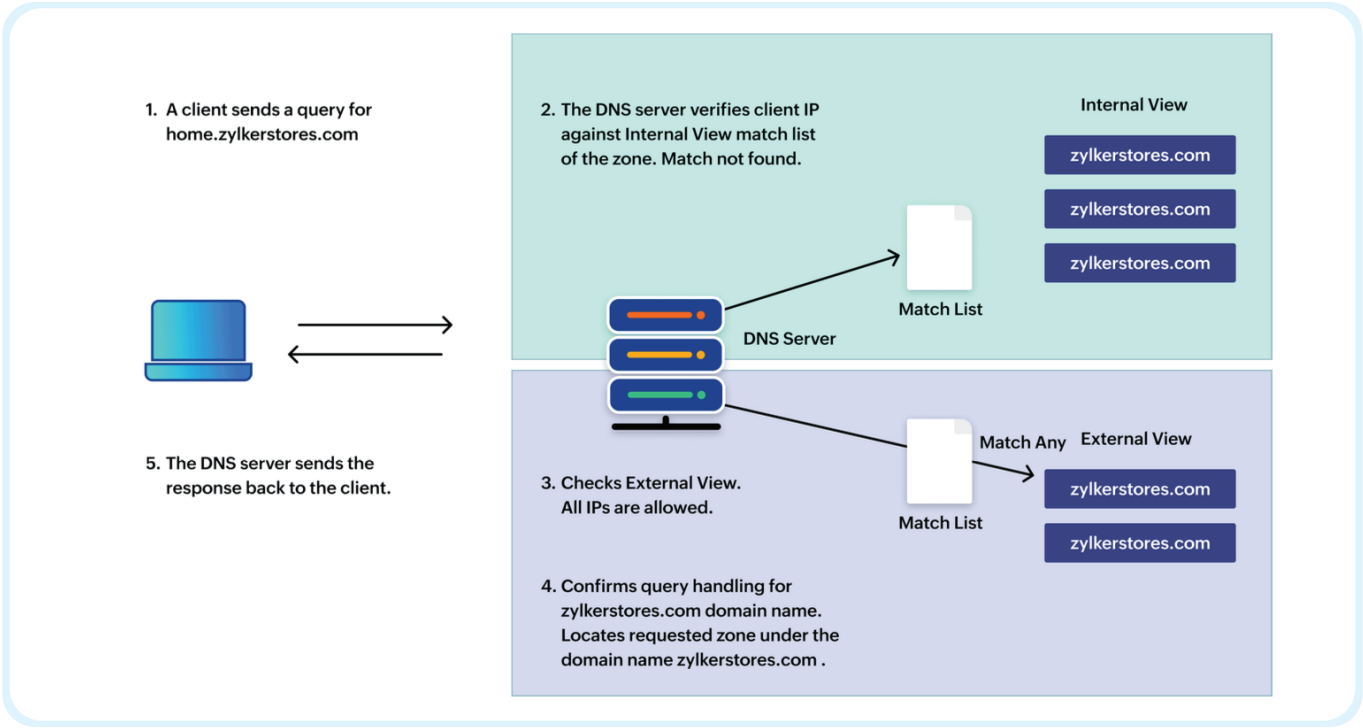
DNS Views



DNS views (also known as domain views) enable network administrators to deliver tailored DNS query responses based on the user's profile or origin. This selective resolution helps organizations present different data sets for internal and external users. For example, internal employees can access confidential information, while external users only see publicly available data or are redirected to a secure, restricted-access page.

DNS views can be configured with various options to suit organizational requirements, such as client-specific responses, destination-based resolution, recursive query handling, and forwarder settings.

To better understand how DNS views work in practice, let's explore a real-world scenario demonstrating their functionality and benefits.



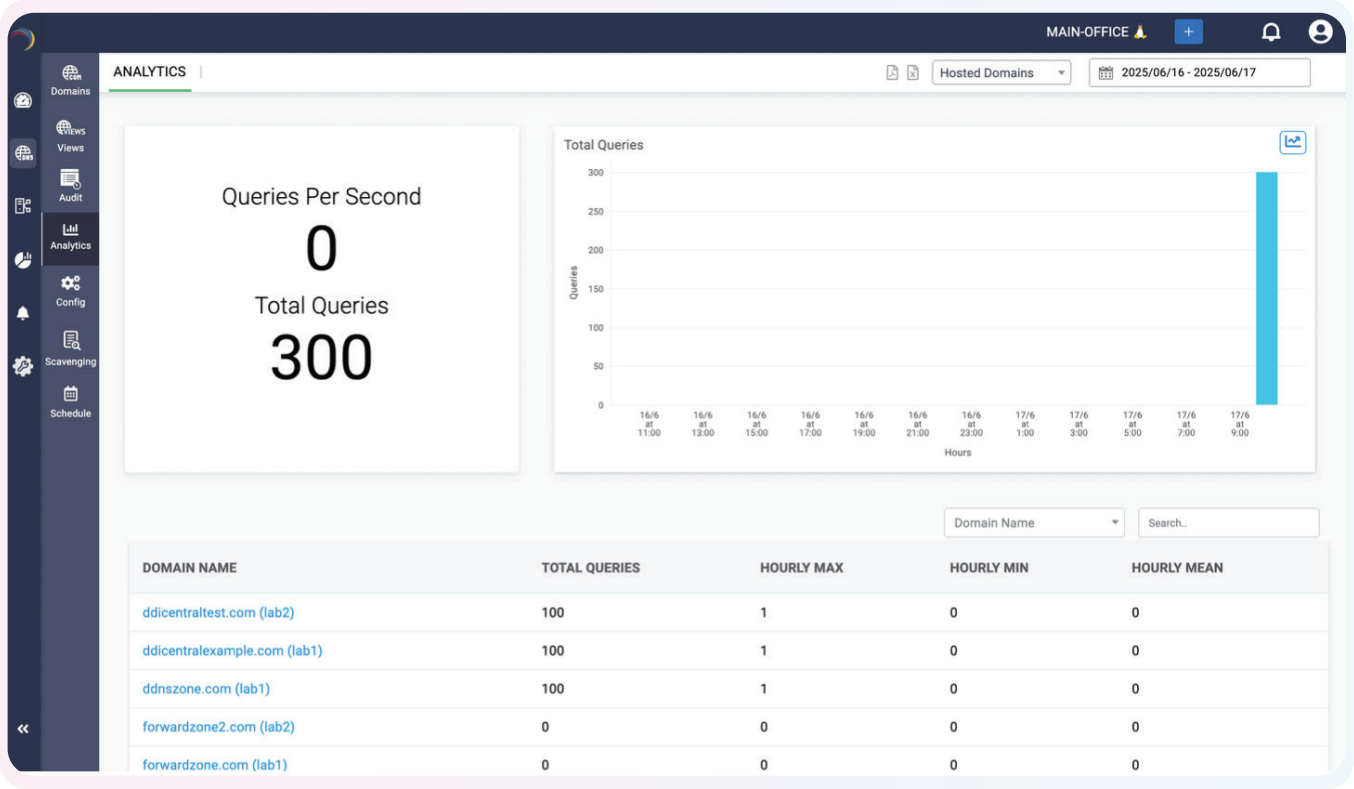
Scenario: Two users send DNS queries for the domain name zylkestores.com, one is an internal employee, and the other is an external customer.

When the DNS server receives these queries, it first checks each user's IP address against predefined match lists for internal and external views. The internal view match list includes IP addresses registered to the retail store's employees, while the external view match list covers public IPs not associated with the internal network.

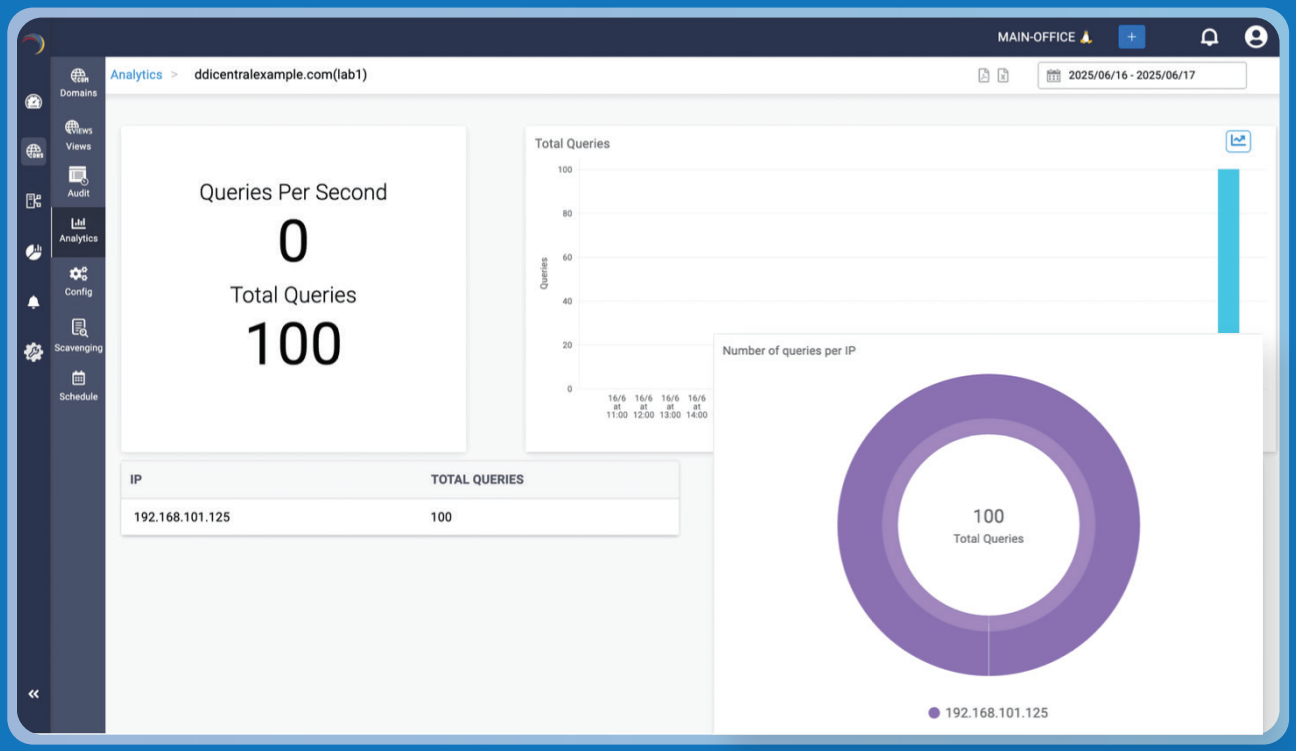
The employee's IP address matches the internal list, so the DNS server responds with the internal IP address for zylkerstores.com, which leads to a version of the site containing confidential, internal-use information. On the other hand, the external customer's IP matches the external list, and the DNS server responds with a different IP , redirecting the user to a public-facing or safer page, as access to the internal content is restricted.

This way, DNS views allow the store to deliver customized, secure responses based on the user's identity and access level.

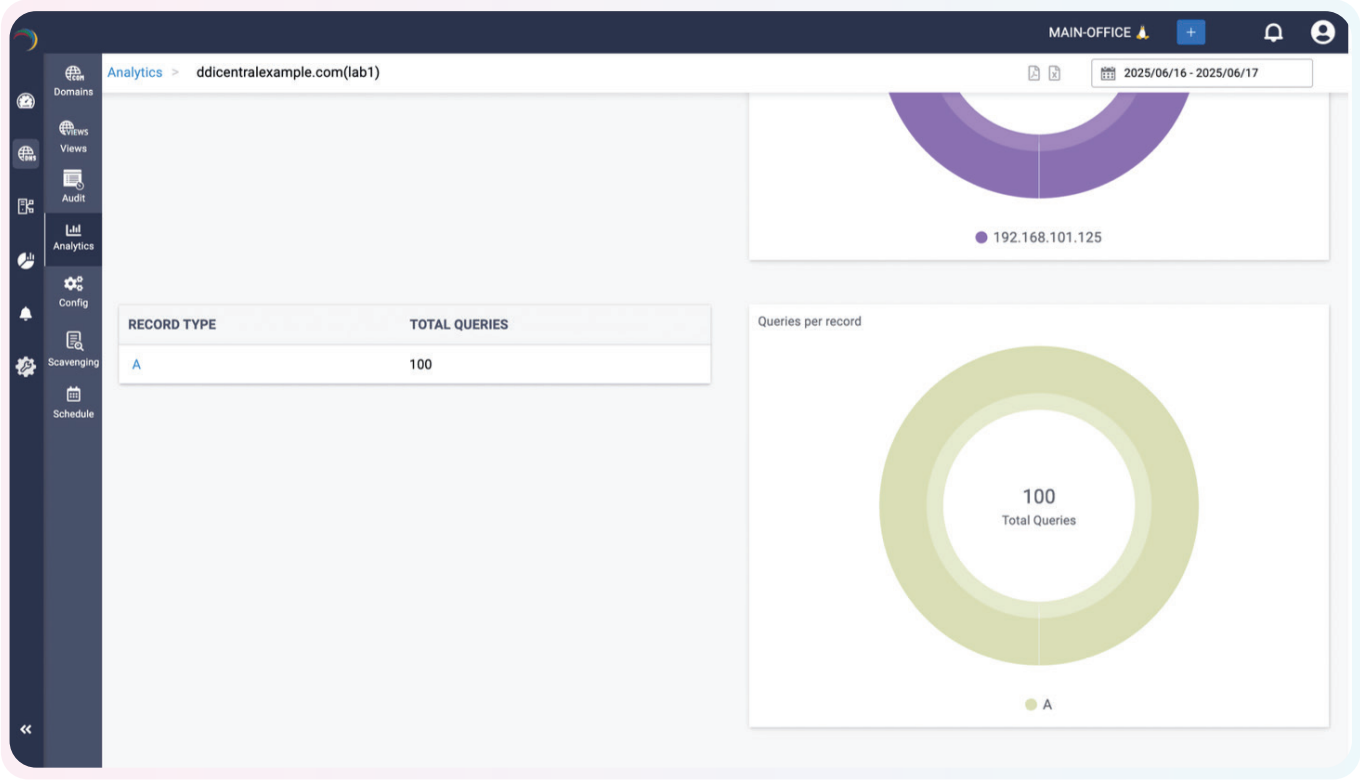
Domain view analytics



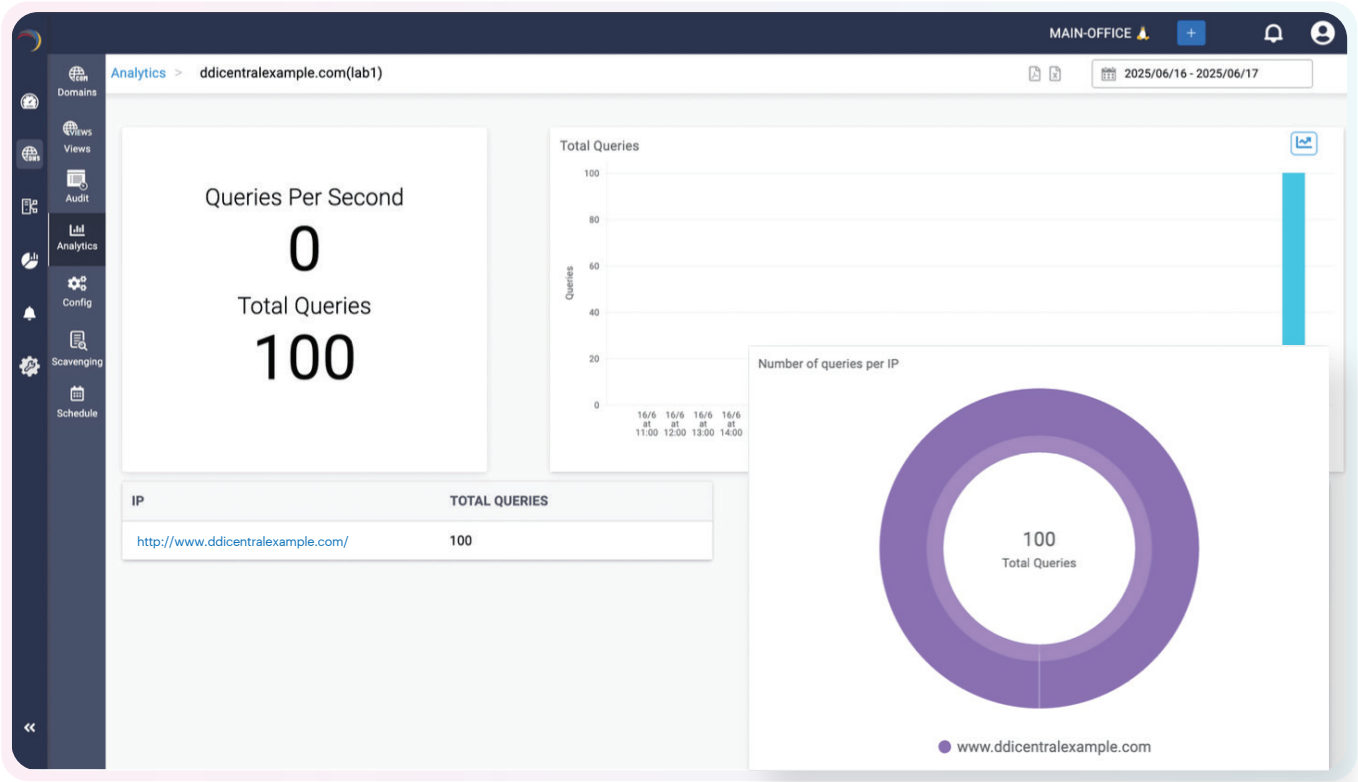
DDI Central's Domain Query Analytics provides administrators with comprehensive visibility into DNS activity, including the number of queries per session, per domain view, and per IP address. Admins can monitor and analyze DNS queries across both hosted and non-hosted domains configured in the system.



By selecting a specific domain or view, admins can access detailed performance metrics, such as the hourly query load over a defined period. Additionally, the platform displays information about the IP addresses leased for that domain, including lease duration, MAC address of the host, and vendor details of the host device.



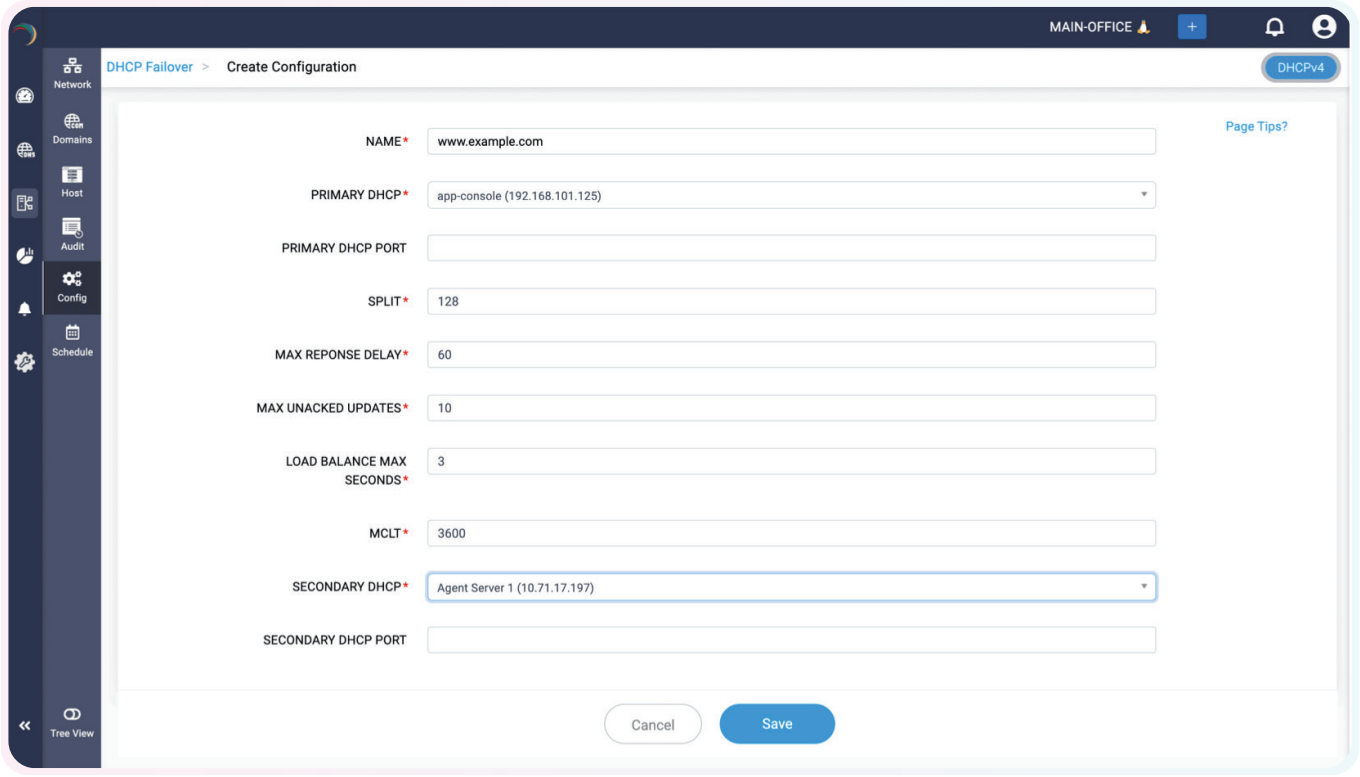
Query traffic is visually represented through intuitive donut charts, one chart showing the total and individual query loads by IP address, and another breaking down query volume by DNS record types.



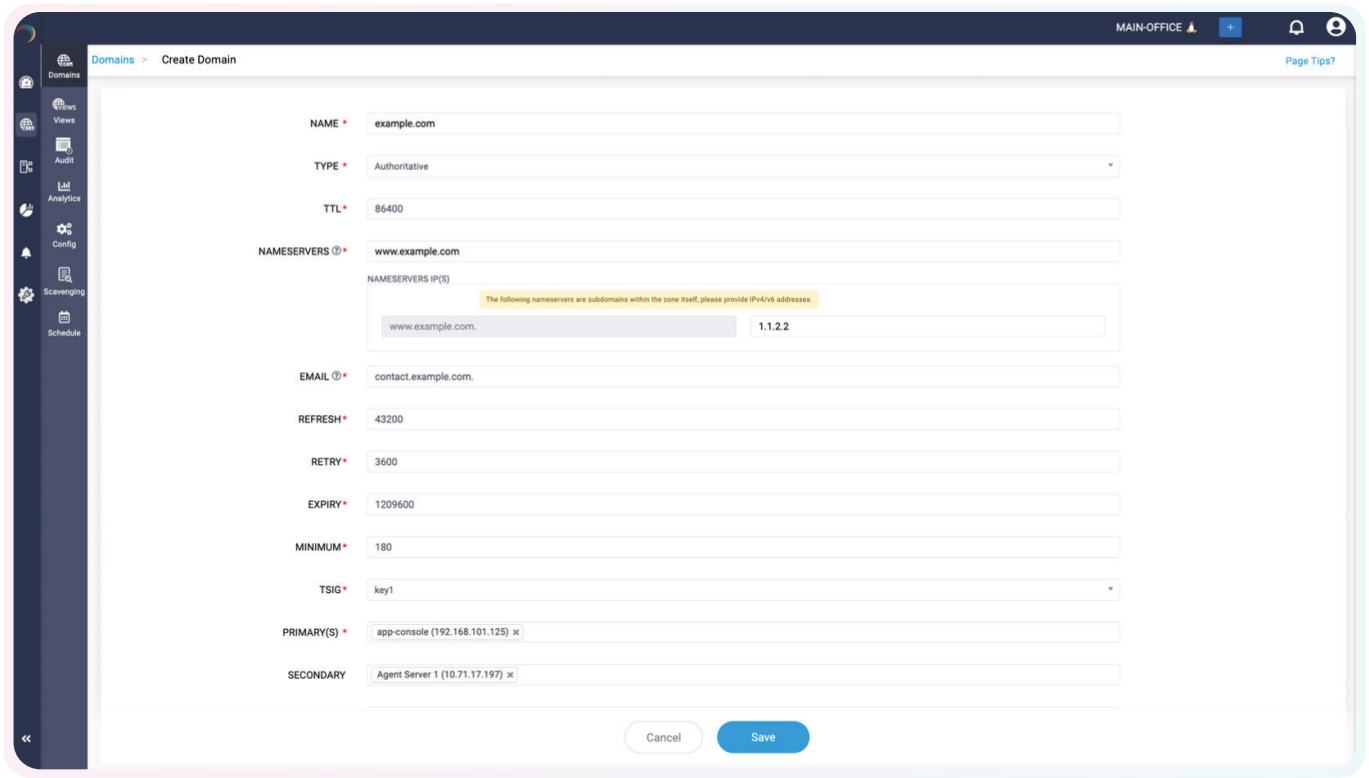
Clicking on a specific record type reveals a detailed list of all zones queried for that record, along with key performance indicators such as hourly query volume, queries per second, and total query count for that zone.

Further drilling down into a selected zone within the record type displays a visual summary of query analytics specific to that zone's records.

High availability of DNS and DHCP services



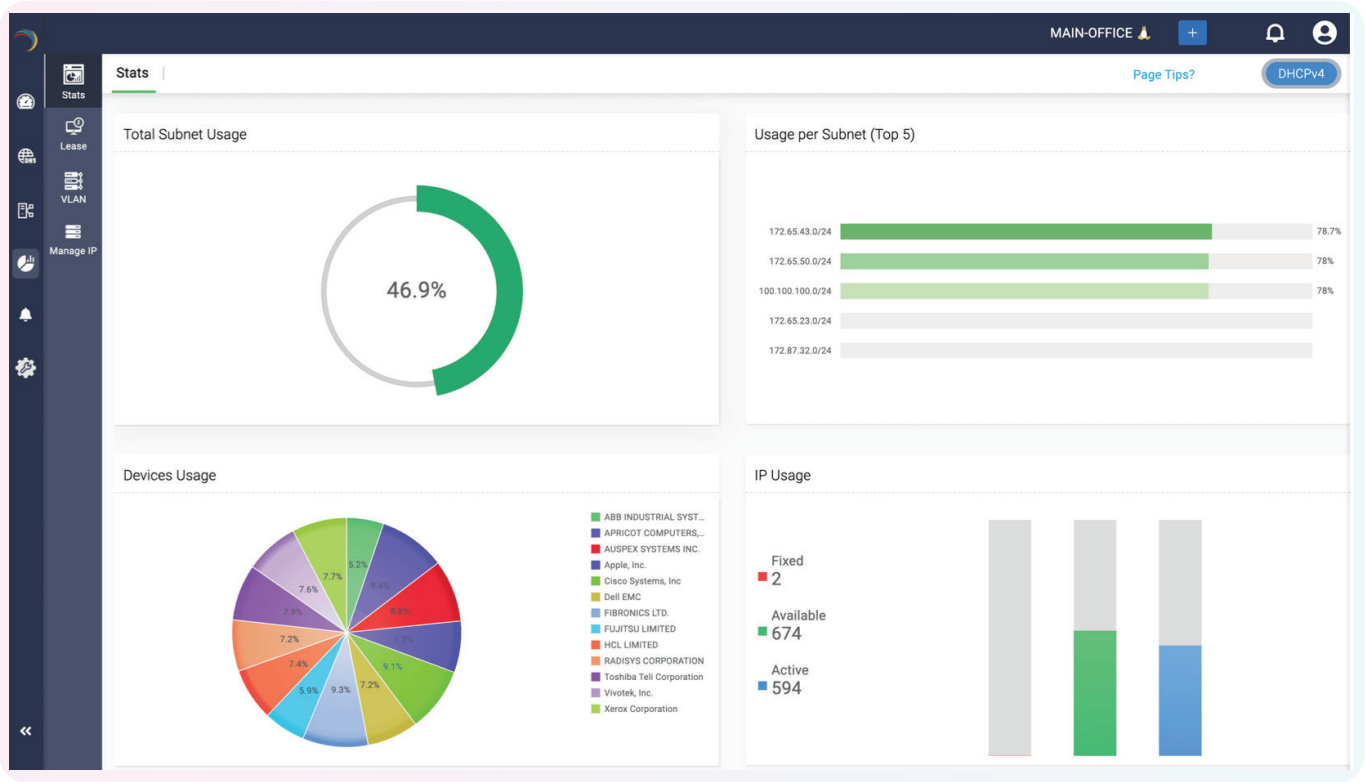
DDI Central's auto failover configurations for DNS and DHCP services are essential for maintaining network continuity, especially in critical situations where the primary server goes down at a retail store. Network administrators can set up both primary and multiple secondary servers for DNS and DHCP , ensuring redundancy and high availability.



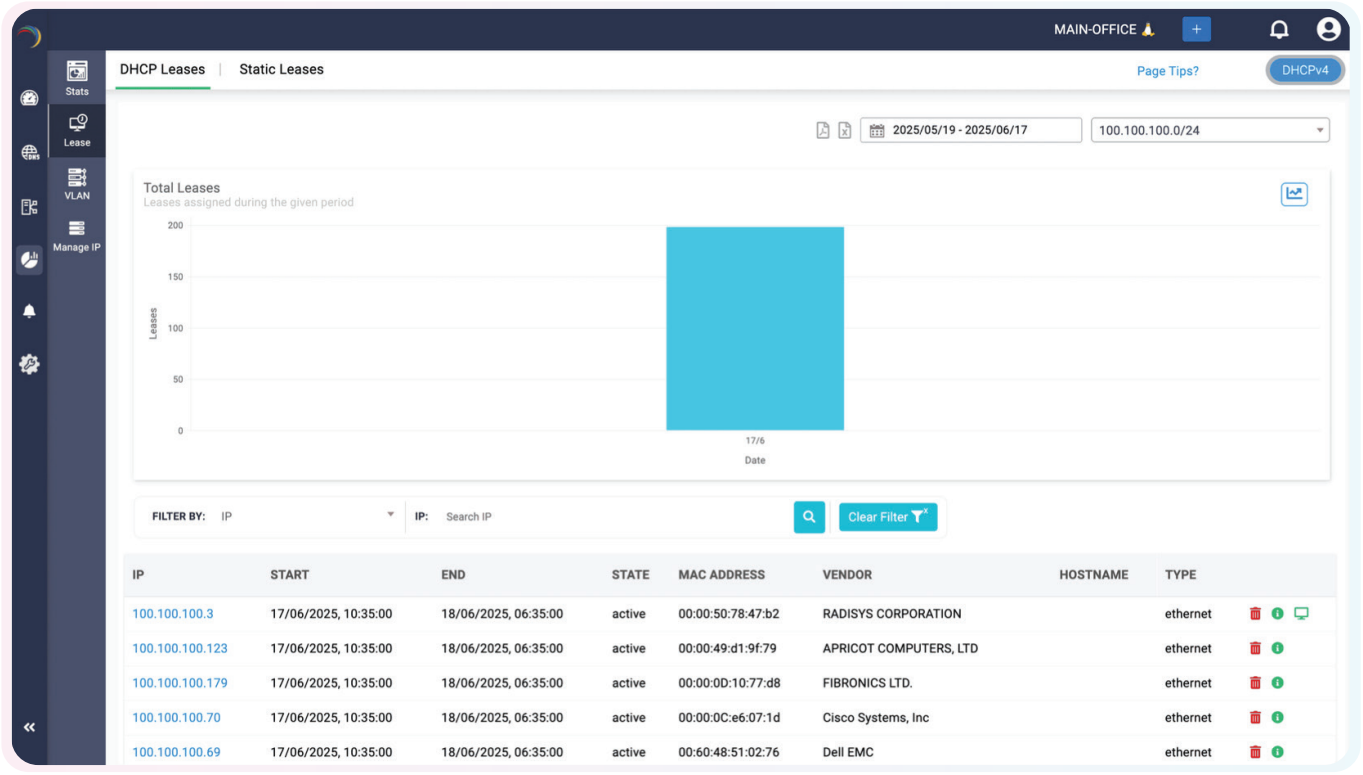
If the primary server fails, the designated secondary servers automatically take over, ensuring uninterrupted handling of network traffic and preserving service stability. Additionally, primary and secondary servers can be configured to share the query load, enabling effective load balancing and improved performance.

In environments where continuous access to network or application services is vital, auto failover setups play a key role in delivering seamless, reliable, and uninterrupted service without compromise.

IPAM as NSoT

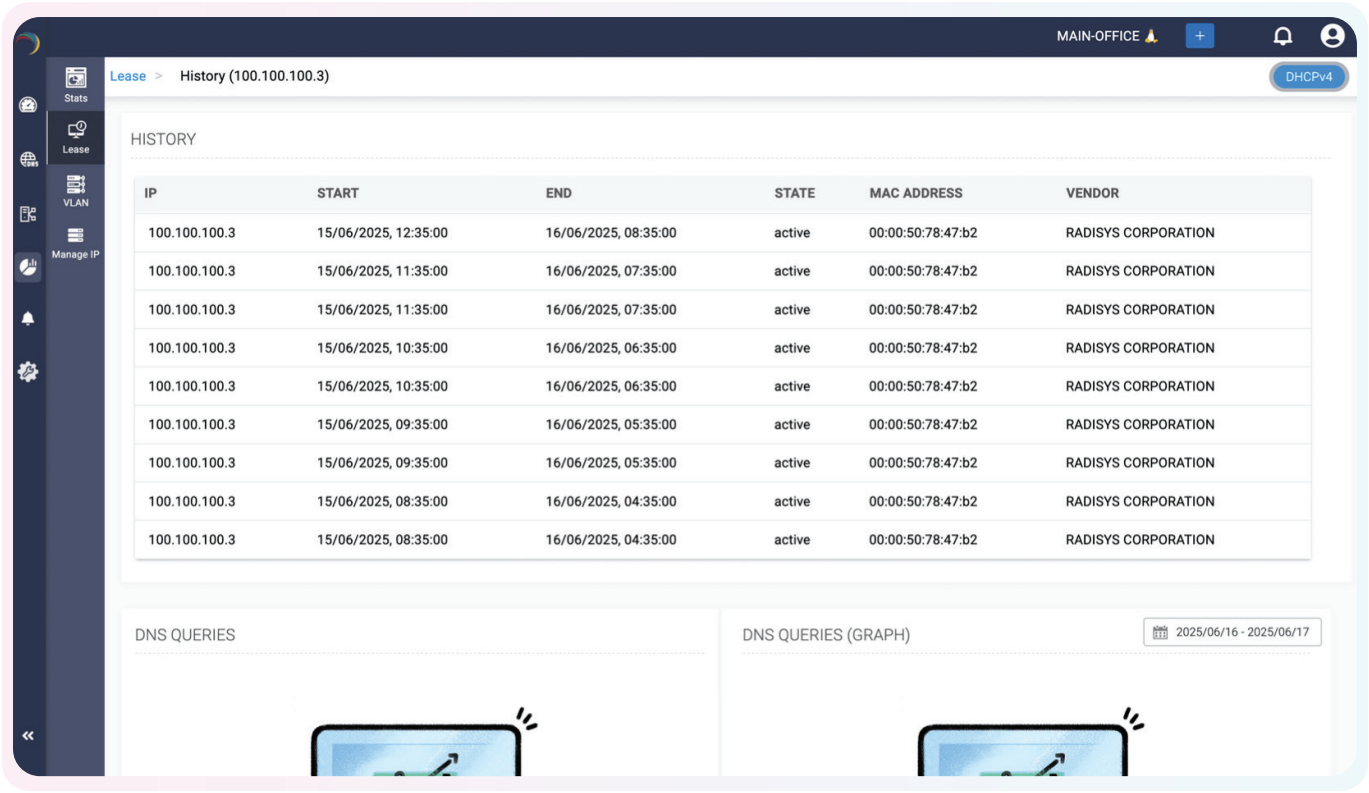


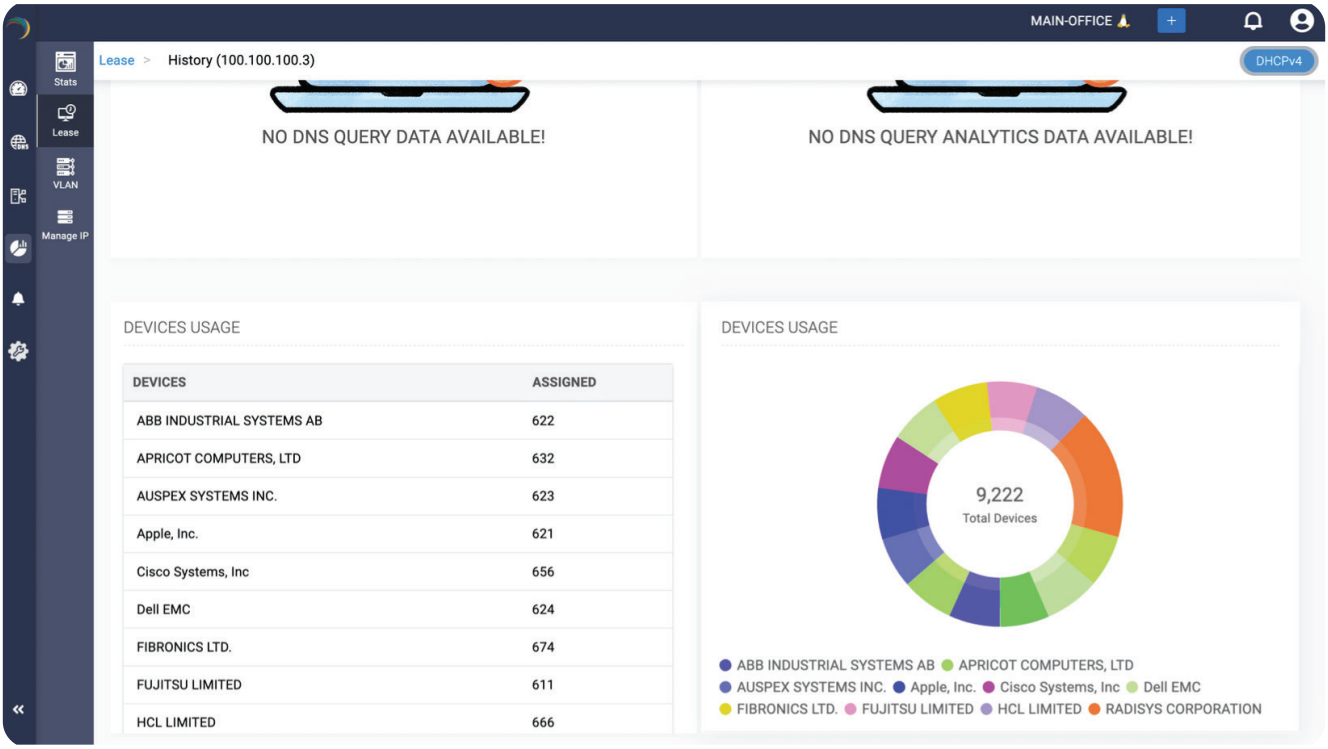
IP address management in DDI Central aggregates and correlates DNS and DHCP data across all clusters, providing a contextualized view of network services and acting as a network source of truth (NSoT). It enables network administrators to gain deeper insights into IP address usage and related services. Metadata such as DNS records, DHCP leases, and IP address allocations are visualized through interactive charts, streamlining data-driven decision-making and simplifying troubleshooting.

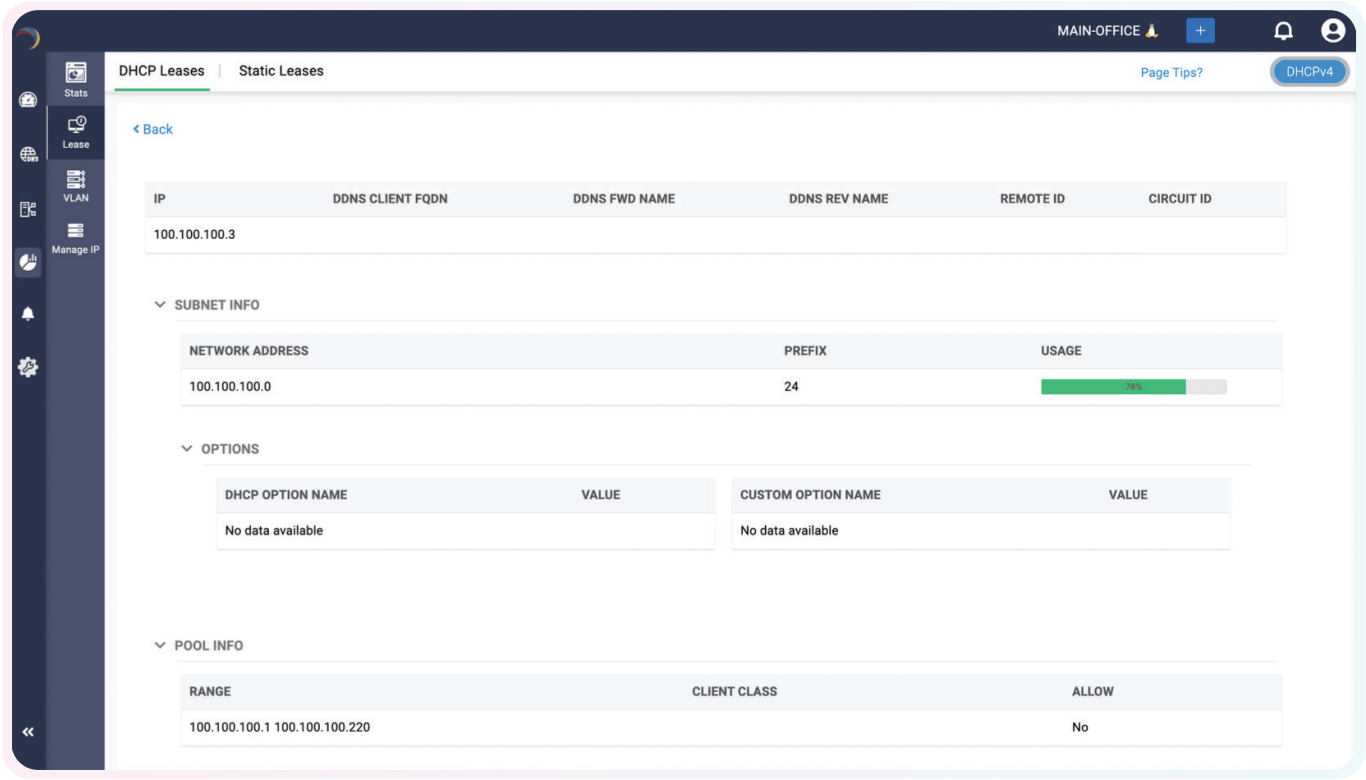


In the DHCP Leases section, admins can monitor the number of leases that have been assigned within the past hour using graphical views. A detailed table displays information such as IP address, lease period, status, device MAC address, hostname, vendor, and connection type. If ManageEngine Endpoint Central is integrated, a Monitor icon appears alongside the Info and Delete options, indicating that the device is listed in the Endpoint Central database.

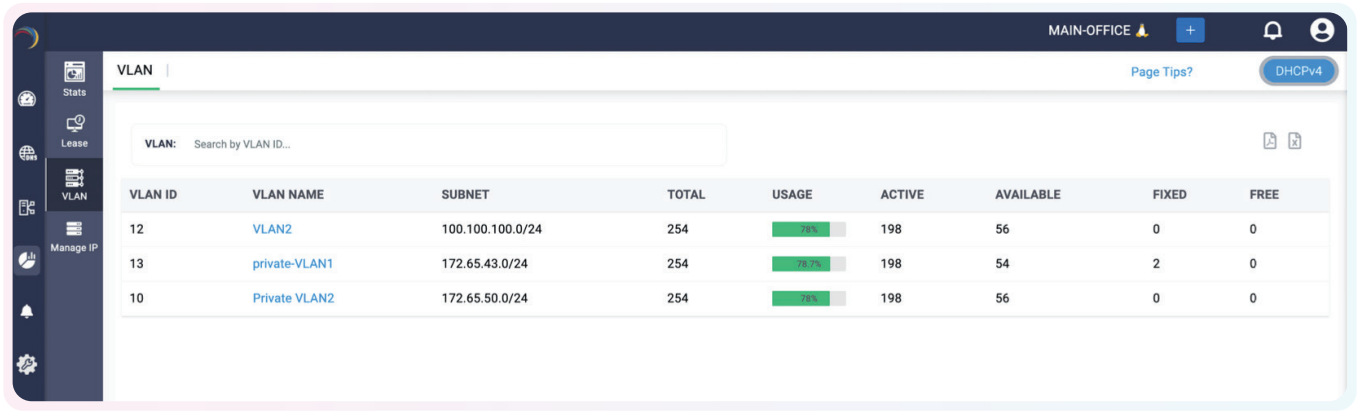
Clicking the Monitor icon opens a contextual view with comprehensive device insights, including patch and vulnerability data, OS details, disk usage, patch summary, severity-based missing patches, and vulnerability scores based on CVSS.

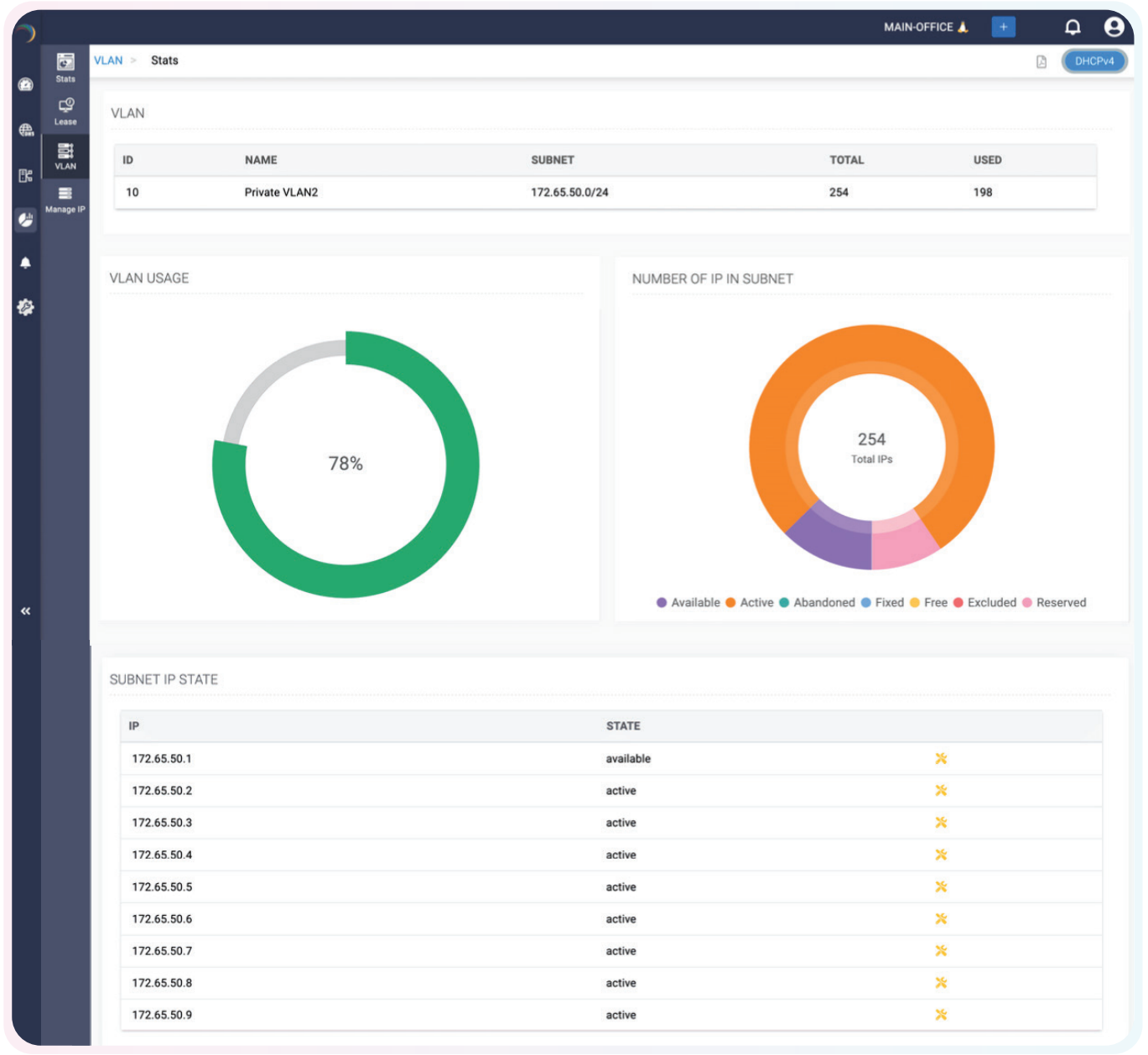

MAIN-OFFICE
Stats
Lease
VLAN
Manage IP
Lease > History (100.100.100.3)
DHCPv4
HISTORY
IP START END STATE MAC ADDRESS VENDOR
100.100.100.3 15/06/2025, 12:35:00 16/06/2025, 08:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 11:35:00 16/06/2025, 07:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 11:35:00 16/06/2025, 07:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 10:35:00 16/06/2025, 06:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 10:35:00 16/06/2025, 06:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 09:35:00 16/06/2025, 05:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 09:35:00 16/06/2025, 05:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 08:35:00 16/06/2025, 04:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
100.100.100.3 15/06/2025, 08:35:00 16/06/2025, 04:35:00 active 00:00:50:78:47:b2 RADISYS CORPORATION
DNS QUERIES
DNS QUERIES (GRAPH)
2025/06/16 - 2025/06/17


MAIN-OFFICE
Stats
Lease
VLAN
Manage IP
Lease > History (100.100.100.3)
DHCPv4
NO DNS QUERY DATA AVAILABLE!
NO DNS QUERY ANALYTICS DATA AVAILABLE!
DEVICES USAGE
DEVICES ASSIGNED
ABB INDUSTRIAL SYSTEMS AB 622
APRICOT COMPUTERS, LTD 632
AUSPEX SYSTEMS INC. 623
Apple, Inc. 621
Cisco Systems, Inc 656
Dell EMC 624
FIBRONICS LTD. 674
FUJITSU LIMITED 611
HCL LIMITED 666
DEVICES USAGE
9,222
Total Devices
ABB INDUSTRIAL SYSTEMS AB
APRICOT COMPUTERS, LTD
AUSPEX SYSTEMS INC.
Apple, Inc.
Cisco Systems, Inc
Dell EMC
FIBRONICS LTD.
FUJITSU LIMITED
HCL LIMITED
RADISYS CORPORATION

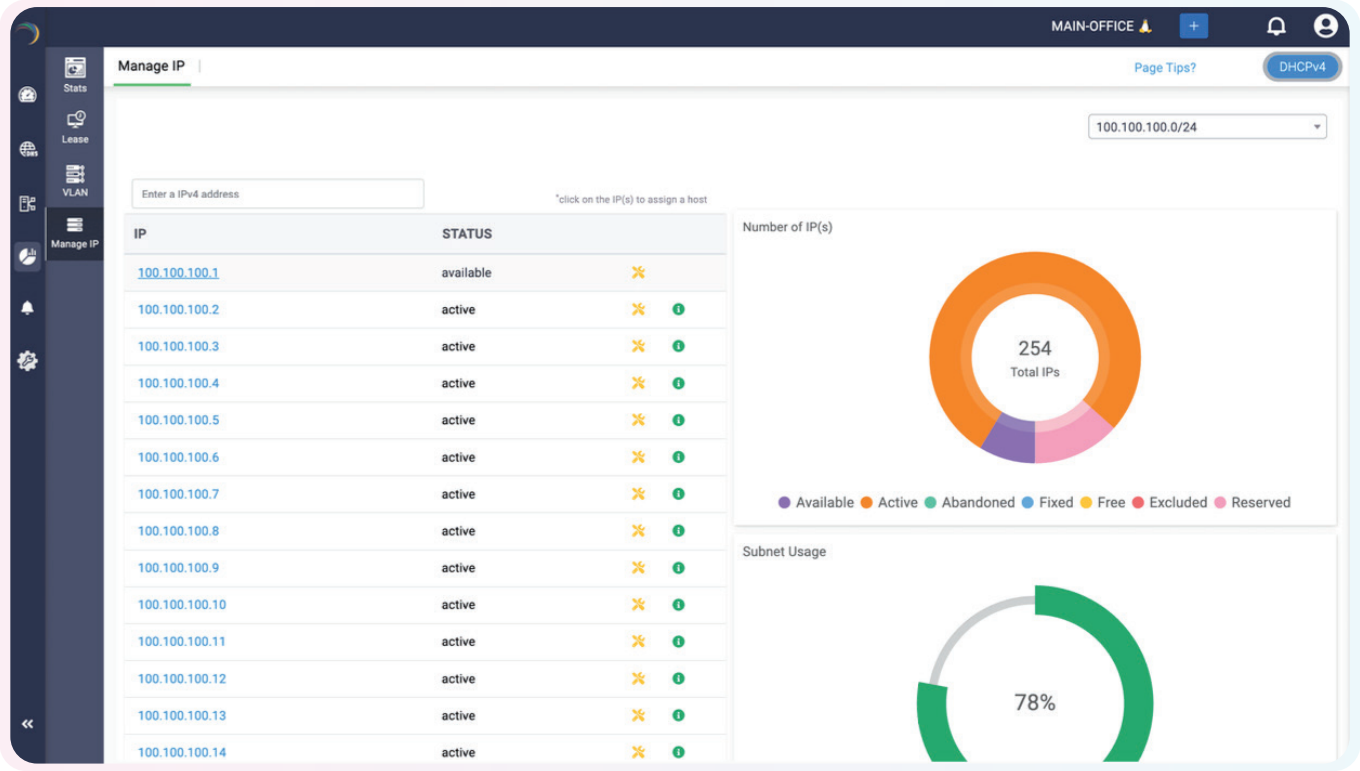


Selecting a specific IP address in the DHCP Leases section reveals comprehensive data including lease history, DNS query activity for that IP , and assignment frequency, presented in both tabular and graphical formats.





Virtual LAN details created by administrators, such as VLAN ID, name, associated subnet, total subnets, usage, and status, are also visually represented, providing deeper network insights.



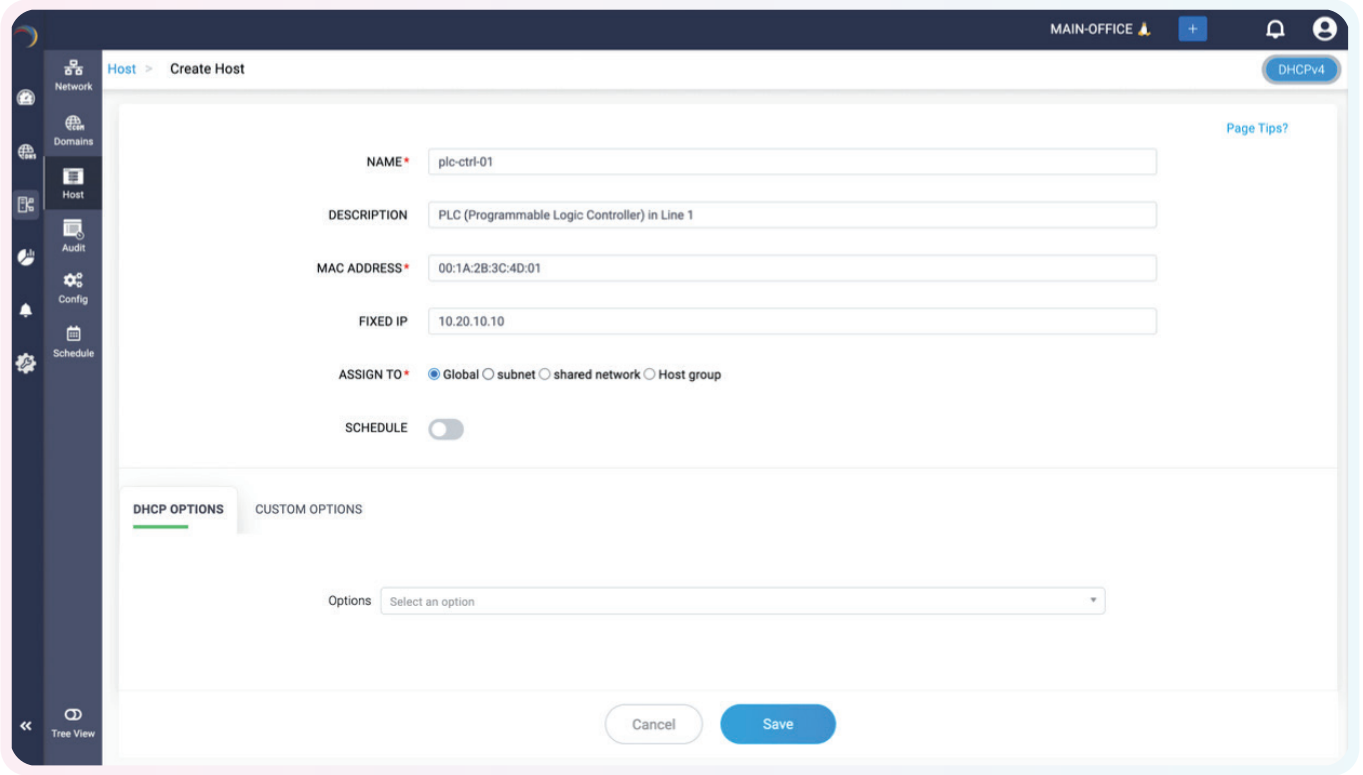
These details are mirrored in the Manage IP section. Here, clicking the Tools icon next to the Info button offers options like Ping, Telnet, and DNS Relation.

Choosing DNS Relation displays key information such as the status of the IP or host, associated domain, mapped record type, and the zone to which the IP is linked, enabling administrators to gain clear, end-to-end visibility of their DNS infrastructure.

DDI as an automation hub

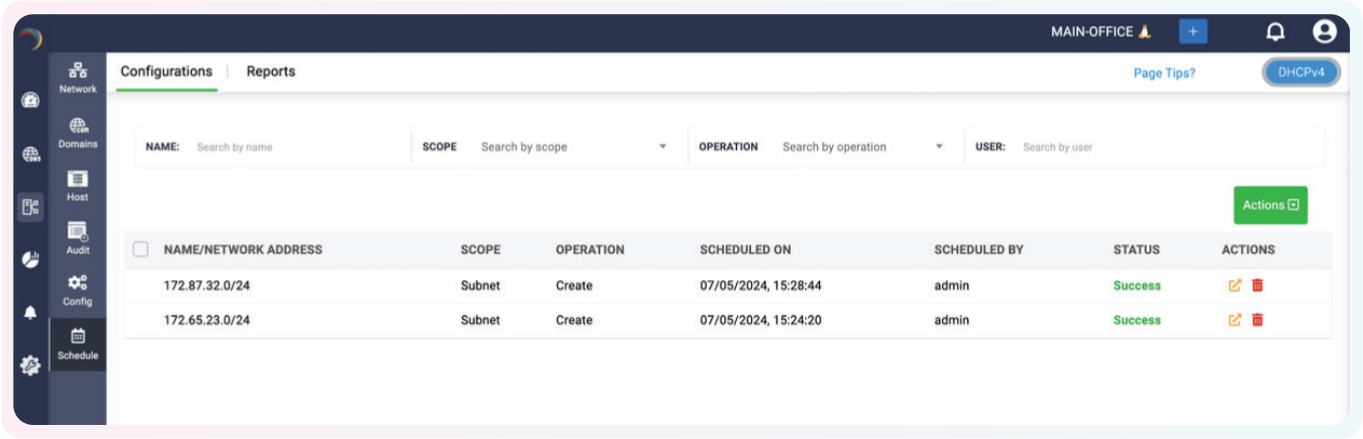
When a retail network automates crucial DNS and DHCP tasks, such as assigning IP addresses to essential devices, updating DNS records dynamically, maintaining an up- to-date IP inventory, scheduling network changes, and configuring failover, manual management by IT admins is not scalable. These tasks, if handled manually, are time- consuming and can delay progress. To overcome this, organizations need a robust network solution that automates and simplifies routine operations.

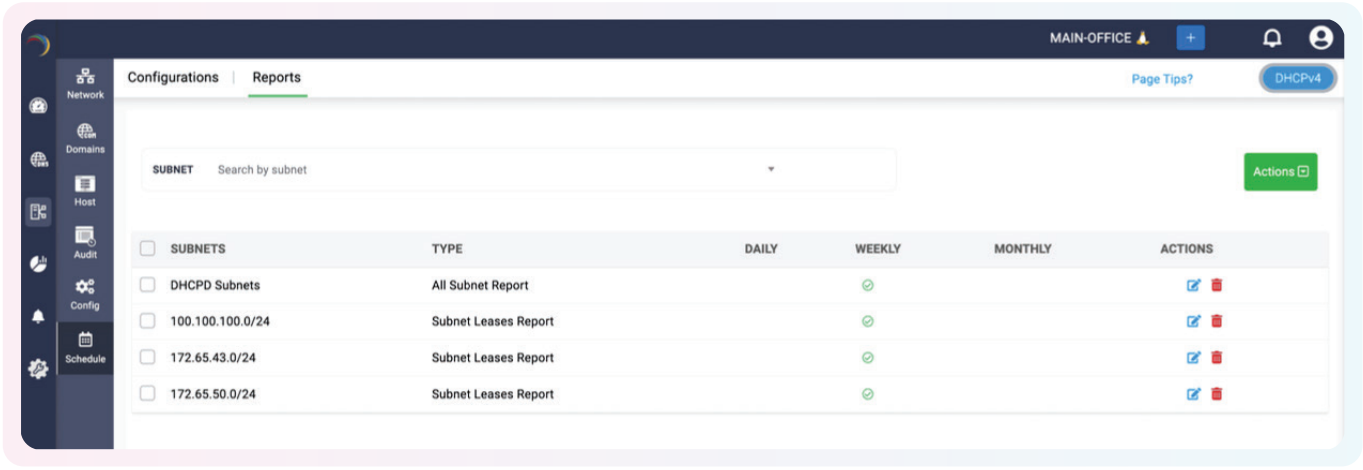
DDI Central provides network administrators with a unified platform for end-to-end automation of core DNS and DHCP functions. Here's how:



Automated IP assignment: IP addresses can be reserved and automatically assigned to crucial devices, like surveillance cameras, printers, and IoT sensors, using DHCP host reservations. This minimizes outages and prevents IP exhaustion for devices that must remain consistently connected.

IP conflict resolution and inventory management: DDI Central automatically detects and resolves IP conflicts, while maintaining a real-time, accurate inventory of all IP address allocations. This ensures reliable connectivity and helps avoid operational downtime.



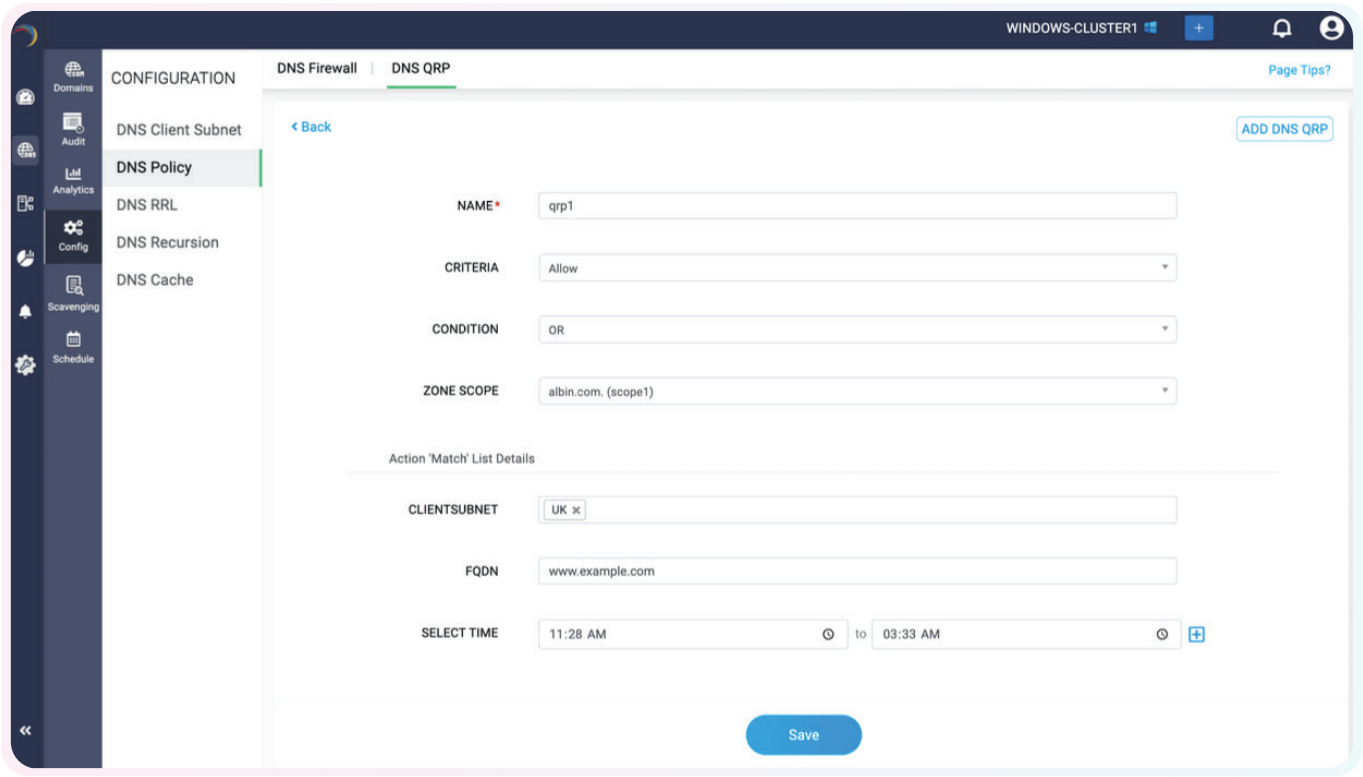


Scheduled network configurations: Network admins can enroll DHCP scopes and DNS records in a "schedule-and-forget" mode. This allows pre-planned network expansions or changes to occur automatically, ensuring consistent service delivery.

Automated reporting: DNS and DHCP reports can be generated at regular intervals, providing insights into subnet utilization and DNS query analytics. This helps with proactive capacity planning and network optimization.

Failover automation: Admins can configure automated failover setups for DNS and DHCP services to ensure business continuity during server or infrastructure failures, especially critical for operations in the retail network.

DNS Query Resolution Policy



DDI Central's DNS Query Resolution Policies (QRP) for Microsoft Windows servers empowers network administrators to configure DNS query responses with greater precision. These policies enable admins to redirect client queries based on criteria such as time, IP address, transfer protocol, as well as streamline query handling, and strengthen DNS security.

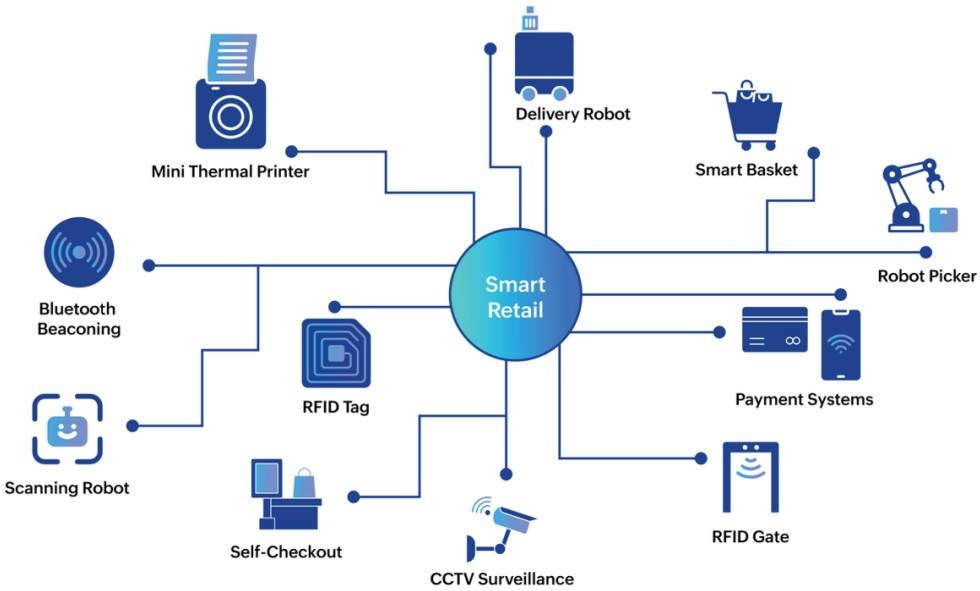
DNS-based attacks often exploit servers that respond to unauthorized users or domains, leading to breaches that can compromise sensitive data. To mitigate such risks, it's essential to have granular control over DNS resolution.

With DDI Central for Microsoft Windows, organizations can define zone scopes to tailor DNS responses for specific applications or departments. Admins can also configure Actions match lists and Actions exemption lists to govern query resolution behavior.

These lists instruct DNS servers to resolve only those queries that meet the specified conditions, while redirecting non-matching queries to a safer destination. This targeted control enables organizations to restrict access, prevent unauthorized resolution, and reduce vulnerability to threats like DNS amplification attacks and DNS cache poisoning.

Additionally, this setup supports split-brain DNS configurations, allowing separate internal and external DNS views. This segmentation helps manage traffic efficiently and ensures that different departments receive appropriate DNS responses, enhancing both security and operational control.

IoT auto-provisioning



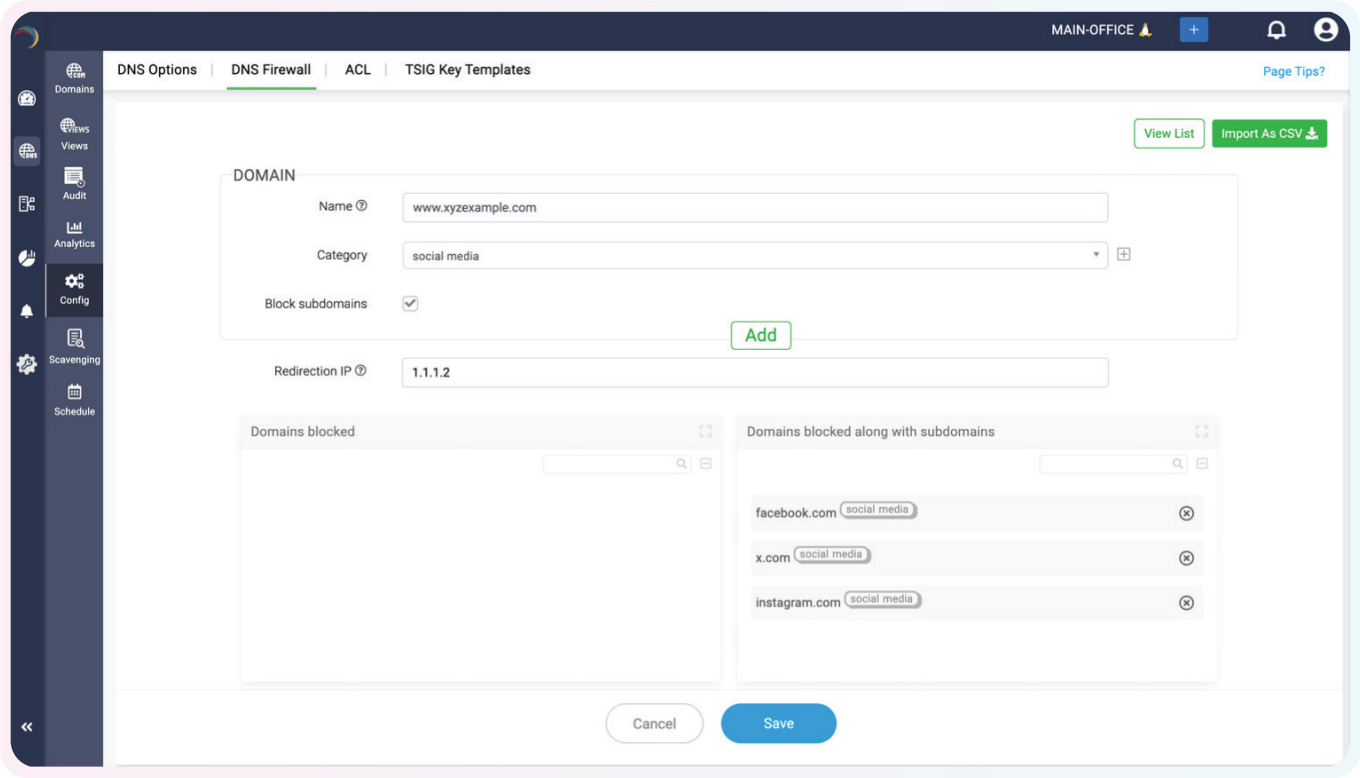
Retail environments often consist of a wide variety of devices, such as POS systems, barcode scanners, digital signage, and inventory trackers, each needing to connect to specific network segments for security, performance, and management purposes. As subnets are divided to support different departments or store functions, it's essential that each device connects to the appropriate subnet allocated for its role.

DDI Central streamlines this process through DHCP fingerprinting using Client Classes. Network administrators can create a Client Class, assign IP addresses at the global or subnet level, and define matching rules based on device MAC address values.

When a device connects to the network and its MAC address matches the values defined in a Client Class, it is automatically categorized and assigned an IP address according to that class. This ensures accurate IP allocation and enables policy-based configurations by segregating devices based on their type or function.

Additionally, using toggle-based configuration, admins can import values from Preboot Execution Environment (PXE) templates into a client class. This enables efficient distribution of essential boot files tailored to the device's OS type. As a result, firmware and operating system files can be automatically deployed to the appropriate retail devices, based on their identified architecture.

DNS firewall



The DNS firewall acts as the network's first line of defense, providing multiple layers of protection against malicious activity. It uses response policy zones (RPZs) to redirect unauthorized DNS queries and actively block access to harmful domains through domain blocking mechanisms.

With RPZs, network administrators can customize DNS responses for known domains by defining specific security policies. DDI Central evaluates incoming DNS queries against these RPZ policies. If a query matches the configured rules, it is resolved to the specified IP address. If it doesn't match, the query is blocked, and the user is redirected to a safe landing page.

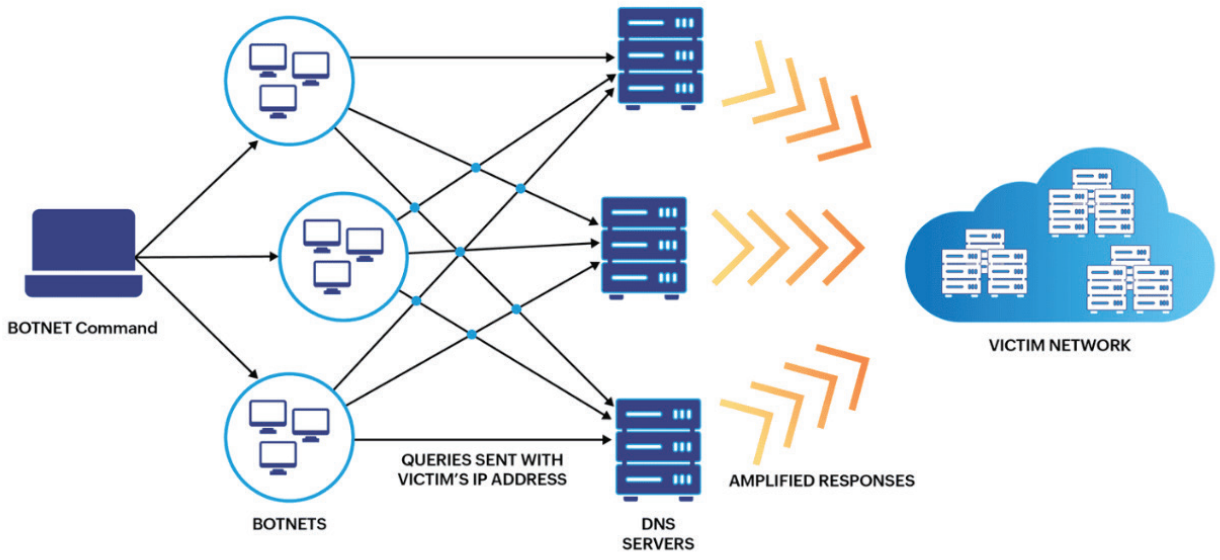
This approach allows admins to control DNS resolution behavior and restrict access to unauthorized or harmful domains. Additionally, RPZs log blocked query attempts, offering valuable insight into attempted security breaches and helping identify patterns of malicious activity.

Domain blocking in DDI Central is especially effective during malware incidents. Certain malware strains, once inside the network, attempt to contact command-and-control servers or other malicious domains through the DNS resolver. To prevent this, the DNS firewall uses a deny-list of known malicious domains.

When a query is received, the resolver checks the domain against this deny-list before fetching any IP address from external DNS servers. If there's a match, the request is blocked, and the user is safely redirected, avoiding any connection to the malicious site.

Through the DNS firewall's analytics dashboard, network admins gain visibility into policy violations, including which hosts attempted access to blocked domains, and when. These insights allow for real-time alerts and rapid response to potential threats, strengthening the overall network security posture.

Response rate limiting

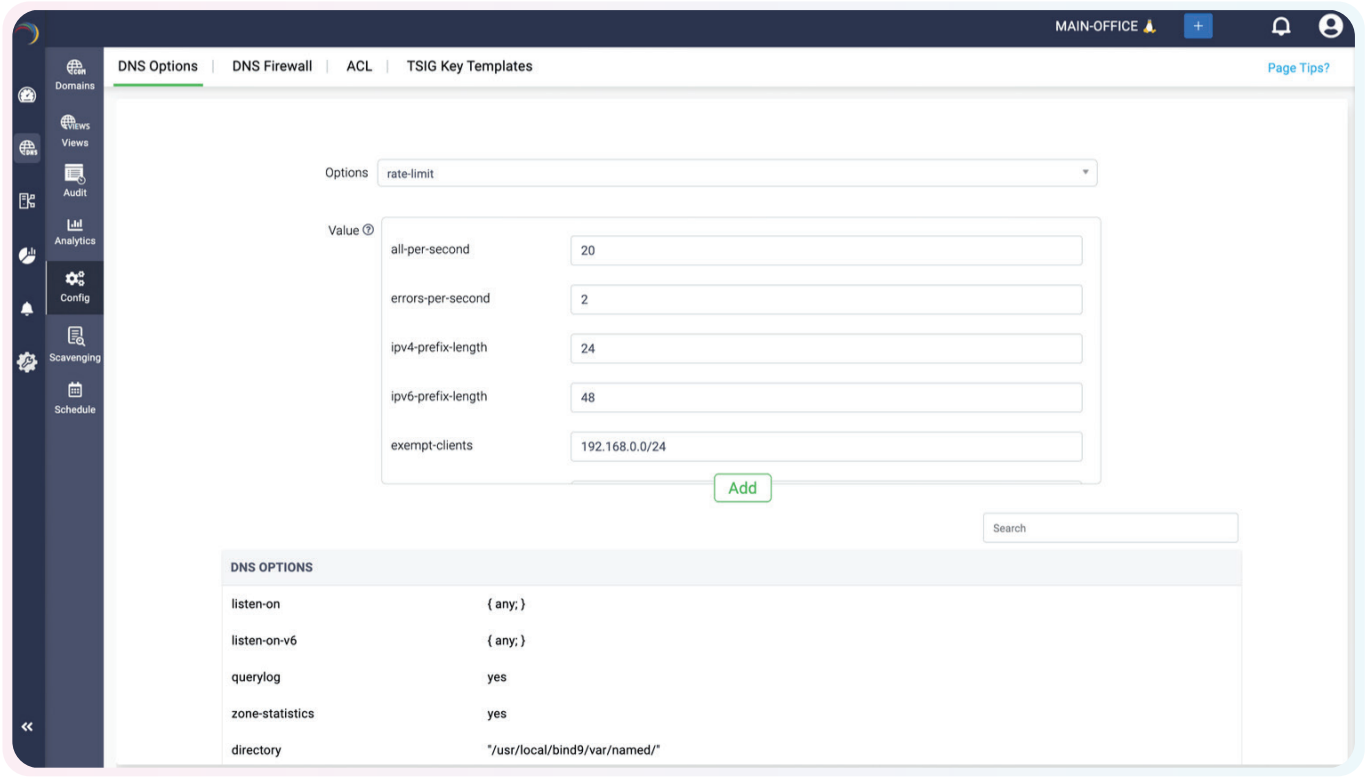


Let's break down a common cyberattack scenario, a DDoS attack targeting a retail network. In this case, a botnet command center selects a retail store's network as its target and begins issuing commands to a large network of infected devices, or botnets.

These botnets begin launching an attack on the DNS servers by sending an overwhelming number of malicious queries using IP spoofing, where the victim's IP address is faked. The DNS servers, unaware of the malicious nature of these queries, respond as they normally would.

However, due to the structure of the attack, these responses are amplified, meaning each small query results in a disproportionately large response.

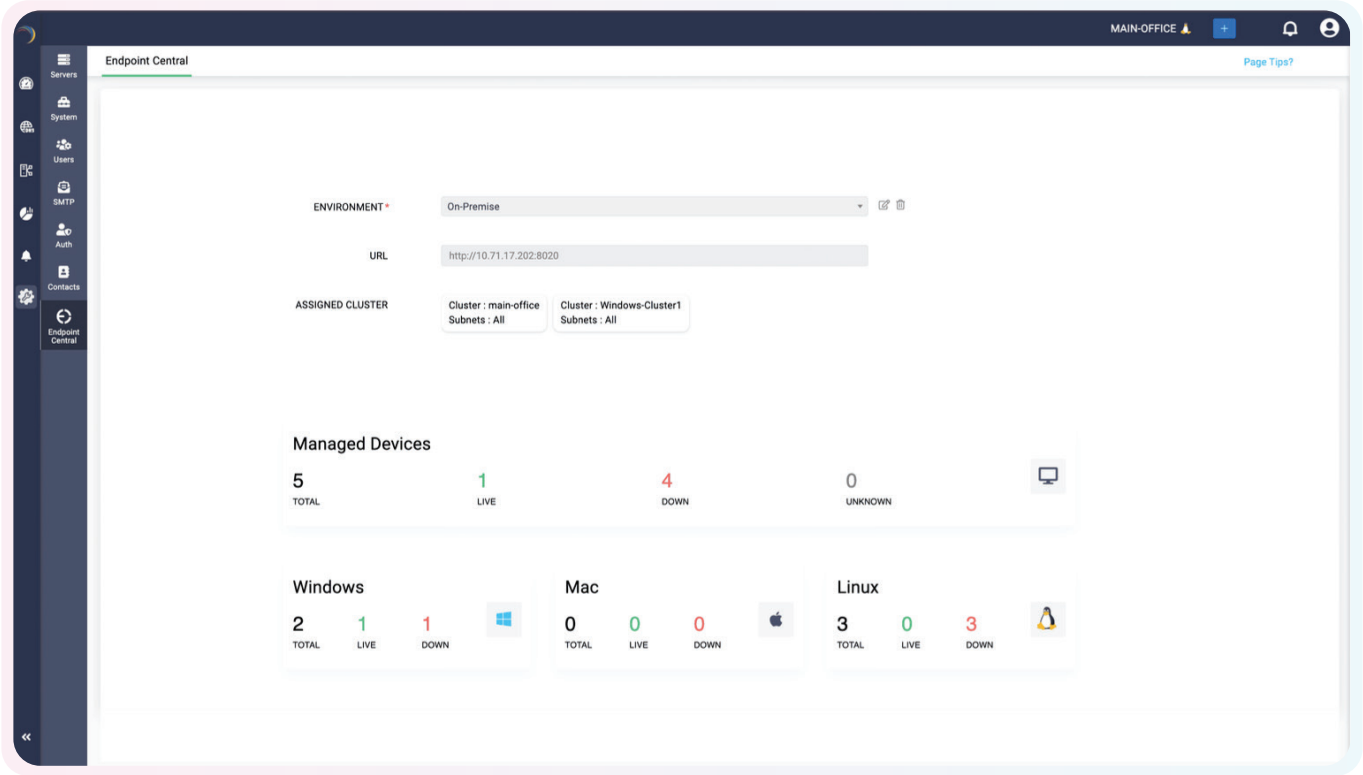
As the volume of these responses increases, the DNS servers become overloaded, leading to network disruption, service outages, and a degraded retail experience for both staff and customers.



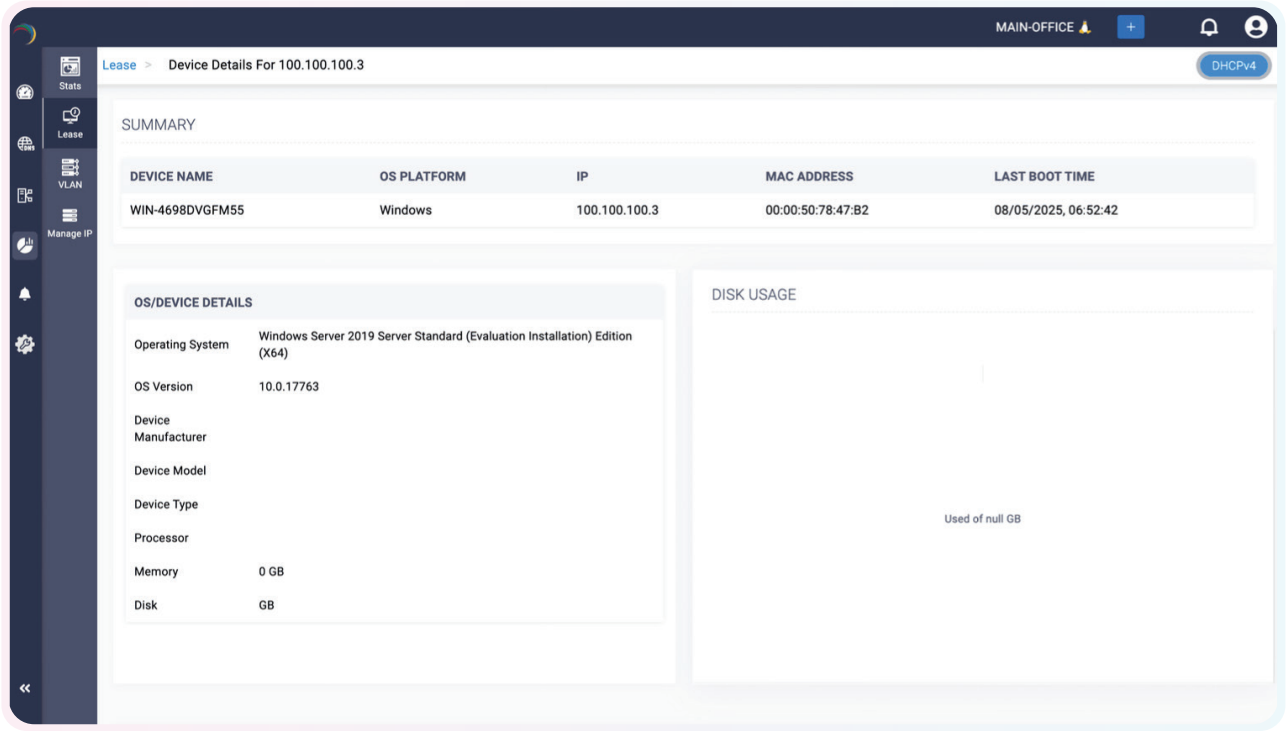
DDI Central helps mitigate such threats using a feature called response rate limiting. With RRL, network administrators can configure DNS servers to limit the number of responses sent for specific queries or IP addresses within a set time frame. This prevents the servers from becoming amplifiers in a DDoS attack and reduces the risk of malware spreading from compromised endpoints to critical systems such as POS terminals, databases, or cloud services.

RRL is a smart DNS security mechanism that throttles excessive responses, helping protect against DNS amplification attacks while still maintaining availability for legitimate users. It supports a selective response strategy, balancing security with performance, ensuring the retail network remains resilient, responsive, and secure for day-to-day operations.

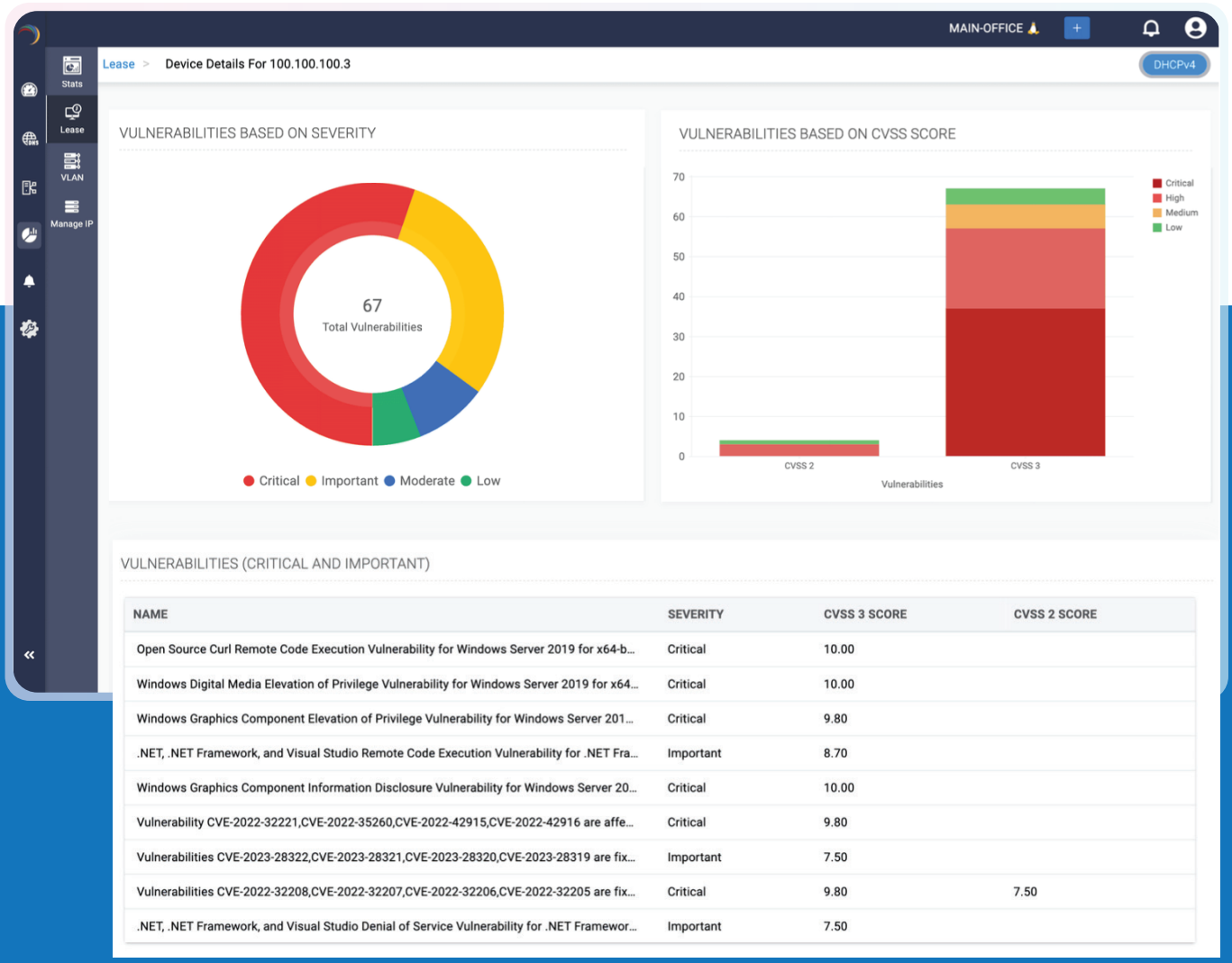
Endpoint Central



DDI Central provides seamless integration with ManageEngine Endpoint Central, enabling network administrators to connect the Endpoint Central application database directly within the DDI Central dashboard. This integration provides enhanced visibility into DHCP-leased devices, including their vulnerability status and patch levels.



By identifying which endpoint devices are assigned specific DHCP leases and detectingunpatched or high-risk systems, admins can take proactive measures, such as blocking DNS resolution or reclaiming IP leases to isolate compromised devices and reduce potential threats. This significantly enhances the overall security posture of the network.



NAME	SEVERITY	CVSS 3 SCORE	CVSS 2 SCORE
Open Source Curl Remote Code Execution Vulnerability for Windows Server 2019 for x64-b...	Critical	10.00	
Windows Digital Media Elevation of Privilege Vulnerability for Windows Server 2019 for x64...	Critical	10.00	
Windows Graphics Component Elevation of Privilege Vulnerability for Windows Server 201...	Critical	9.80	
.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability for .NET Fra...	Important	8.70	
Windows Graphics Component Information Disclosure Vulnerability for Windows Server 20...	Critical	10.00	
Vulnerability CVE-2022-32221,CVE-2022-35260,CVE-2022-42915,CVE-2022-42916 are affe...	Critical	9.80	
Vulnerabilities CVE-2023-28322,CVE-2023-28321,CVE-2023-28320,CVE-2023-28319 are fix...	Important	7.50	
Vulnerabilities CVE-2022-32208,CVE-2022-32207,CVE-2022-32206,CVE-2022-32205 are fix...	Critical	9.80	7.50
.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability for .NET Framewor...	Important	7.50	

Detailed visualizations of device vulnerabilities and missing patches help admins quickly prioritize and address critical issues before they escalate into disruptions. With this integration, DDI Central ensures a more secure, well-monitored, and manageable network environment.

Managing hybrid resources in DDI Central

ManageEngine DDI Central manages and monitors the hybrid IT infrastructure of modern retail environments. With its multi-vendor DNS integration capabilities, DDI Central provides centralized control over a multi-cloud DNS setup, enabling admins to configure and control domains hosted across different cloud providers through a unified interface. Changes made within DDI Central are reflected on both ends via bidirectional sync, ensuring consistency across platforms.

For instance, if a retail organization utilizes Amazon Web Services for its cloud operations, DDI Central delivers full visibility into key AWS resources. This includes components like Elastic Compute Cloud instances, Elastic IPs, Elastic Network Interfaces, Relational Database Service instances, Elastic Container Service clusters and tasks, Virtual Private Clouds, and subnets.

By displaying a consolidated view of the entire cloud ecosystem, DDI Central simplifies cloud network management and reduces the dependency on multiple cloud-native tools, empowering IT teams in retail to manage infrastructure efficiently and securely from a single platform.

Conclusion

A full-stack DDI solution brings together all crucial network management tools into a unified interface, simplifying administration and boosting operational efficiency. While many retail stores still rely on freeware or open-source DNS and DHCP tools, or even manage their IP infrastructure using spreadsheets, these methods often fall short when handling dynamic, multilocation retail environments.

By adopting a DDI solution, retail IT teams can eliminate these inefficiencies and reduce manual overhead, gaining centralized visibility and control over their entire network across distributed branches or outlets. A robust DDI system integrates security, management, and operational workflows, providing strong defense against cyberthreats and ensuring smooth network operations.

As retail networks grow more complex with increasing digital services, e-commerce platforms, and in-store connectivity, the need for DDI becomes even more vital. Implementing a full-stack DDI solution isn't just a technical upgrade, it reflects a retailer's commitment to delivering fast, secure, and reliable digital experiences that both employees and customers rely on.