TECHNICAL VALIDATION

BlueCat Micetro

Simplifying DDI Management and Orchestration in Hybrid and Multicloud Environments

By Alex Arcilla, Principal Analyst – Validation Services
Omdia

MARCH 2026

Contents

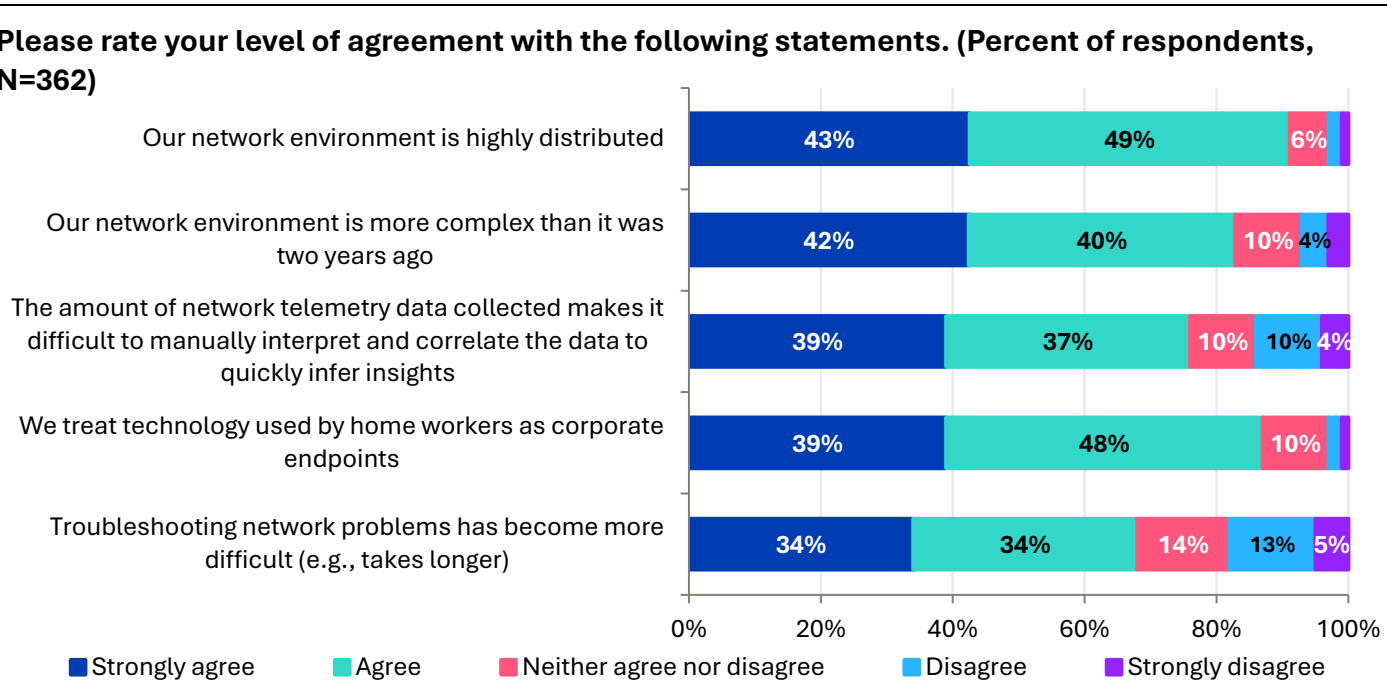
Introduction

This Omdia Technical Validation documents our evaluation of BlueCat Micetro. We review how this solution helps organizations increase the efficiency and effectiveness of managing DNS, DHCP, and IPAM (DDI) data. Using Micetro can ultimately help in maximizing network availability and reliability while decreasing both capital and operational expenses.

Background

IT environments remain highly distributed for a reported 92% of organizations, with applications hosted across on-premises, cloud, colocation, and edge environments. Given this state, it is no surprise that 82% of organizations stated that their network environment is more complex than it was two years ago (Figure 1).[1]

Figure 1. Highly distributed network environments are also considered complex



Source: Omdia

DDI management for on-premises environments is a tedious yet necessary task, as organizations need to manually stitch data from multiple silos (e.g., spreadsheets, servers, routers) to determine and update the relationships amongst the data. Maintaining this detailed level of network visibility is already difficult when dealing with multiple resources within data centers, branches, and edge locations.

As more organizations embrace hybrid and multicloud environments, DDI management becomes even more difficult, as on-premises and cloud DDI data are also maintained separately, leading to more manual work to maintain the proper relationships between the data. This results in a lack of comprehensive network visibility required for the consistent application of network and security policies along with operational inefficiencies in network management and control.

[1] Source: Enterprise Strategy Group (now Omdia) Research Report, *The Role of AI and Automation in Networking*, August 2024.

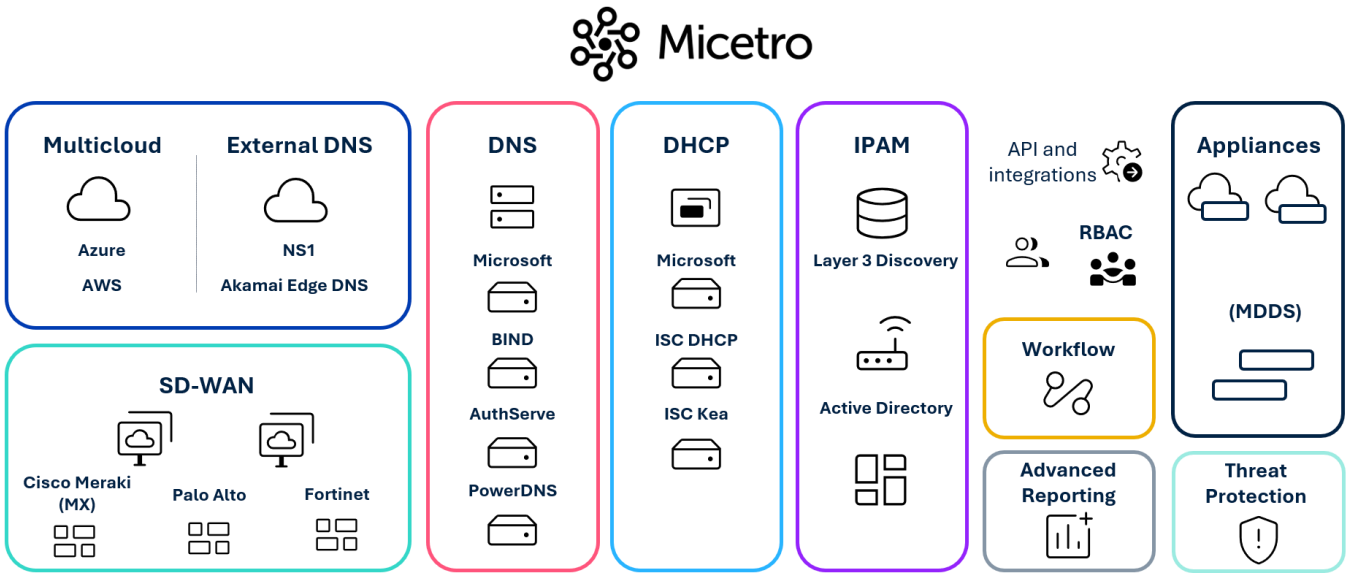
Installation of a DDI solution can also become an issue. Many follow a "rip and replace" model that requires network engineering teams to change their infrastructure to accommodate a new solution, rather than working with the existing network infrastructure.

Ideally, a DDI solution would remove the manual effort organizations typically spend on gathering DDI data, updating the relationships existing amongst the data to align with changing network requirements. The solution would centralize and update network visibility from a DDI perspective and enable workflow automation and orchestration.

BlueCat Micetro

BlueCat Micetro is designed to help organizations simplify DDI management and orchestration. The solution unifies DDI management across on-premises, hybrid, and multicloud environments (see Figure 2). Organizations can leverage Micetro as its "single source of truth" when discovering and updating the data and its relationships to achieve comprehensive network visibility and control via a single web interface.

Figure 2. BlueCat Micetro



Source: BlueCat Networks and Omdia

This vendor-agnostic solution enables organizations to work within multi-vendor networks, as DDI data originates from a broad range of DNS/DHCP server types, along with Active Directory (AD) forest integration and Cisco Meraki SD-WAN orchestration. Implementing Micetro can be accomplished without disrupting normal operations, as no "rip and replace" of existing devices occurs; the solution is simply an overlay onto an organization's existing network environment. Micetro also reduces agent sprawl by supporting agent-free management for Microsoft DNS and DHCP, where appropriate, using lightweight proxy agents only when required.

Micetro centralizes the storage of all normalized DDI metadata, relationships, and operational states within an organization's choice of Micetro database backend. Authoritative DNS and DHCP data remain on the source systems. Organizations no longer need to struggle with managing siloed data, as changes in Micetro are pushed to the source system and vice versa.

Organizations also do not need to acquire new skill sets, as BlueCat Micetro standardizes workflows across vendor-specific products. These workflows, available through the Micetro web interface, are exposed through its unified API, ensuring functional parity between manual operations and automated integrations.

With Micetro, organizations can reap the following benefits:

- **Improved network consistency**. Instead of managing DDI data and their interrelationships manually (e.g., via spreadsheets), Micetro gathers and maintains these records, even when changes are made to the source data. This reduces the chance of DDI-related errors that can unnecessarily cause network issues.
- **Centralized visibility and management**. Organizations can manage and control DDI data via a single web interface, as the relationships between DNS servers, DHCP servers, and IP addresses are presented without manually cross-referencing multiple data sources. Micetro eliminates the need to manually track, update, and resolve DDI errors.
- **Unified API overlay for enabling automation and orchestration**. Instead of accounting for vendor-specific APIs, schemas, and behaviors when automating operational workflows, Micetro offers a centralized API overlay that enables organizations to build automation and self-service workflows that can be applied consistently across highly distributed environments. When automating and orchestrating common tasks, organizations can reduce operational complexity and overhead.
- **Improved uptime**. Using Micetro's built-in tools for IPAM accuracy, DNS workflow transparency, DHCP reliability, xDNS redundancy for DDoS defense, and reporting for trend and vulnerability analysis, organizations can increase overall network availability by maintaining network consistency and isolating potential threats and attacks.
- **Lower expenses**. With the combination of eliminating forklift upgrades, reducing the need to acquire new skills, and automating workflows, Micetro helps decrease overall capital and operational expenses.

Omdia technical validation

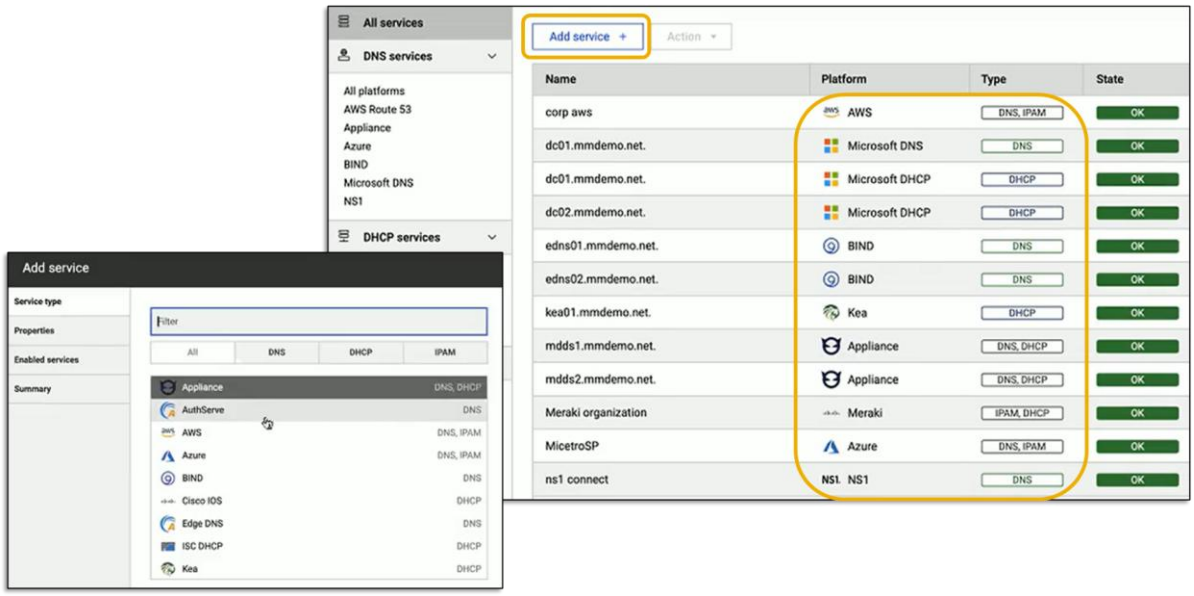
Using briefings and online demonstrations, Omdia validated the benefits that organizations can expect to gain from using BlueCat Micetro. We specifically focused on how Micetro can significantly reduce the time and effort spent on DDI management through specific use cases. To place our review into perspective, Omdia assumed that organizations rely on manually driven data gathering and updates, while records are stored electronically in one or more documents (e.g., spreadsheets).

Simplified DNS management

Before delving into Micetro's DNS management capabilities, Omdia first viewed the DDI services present in the network environment. We noted how Micetro centralizes DDI visibility, as all available services and their sources (e.g., appliances installed on-premises, public clouds) are displayed in a single interface (see Figure 3). Administrators do not need to maintain multiple documents to access this information.

Adding a new service is as simple as clicking on "Add New Service," which initiates a wizard-driven process. Once Micetro connects to the data source, whether on-premises or in a public cloud, data is pulled into the chosen central repository. This eliminates the need to manually gather data and relevant details (e.g., DNS zones, configuration, record types, IP address pools) from all available DDI services. Omdia noted the time and effort saved in manually collecting and recording such data.

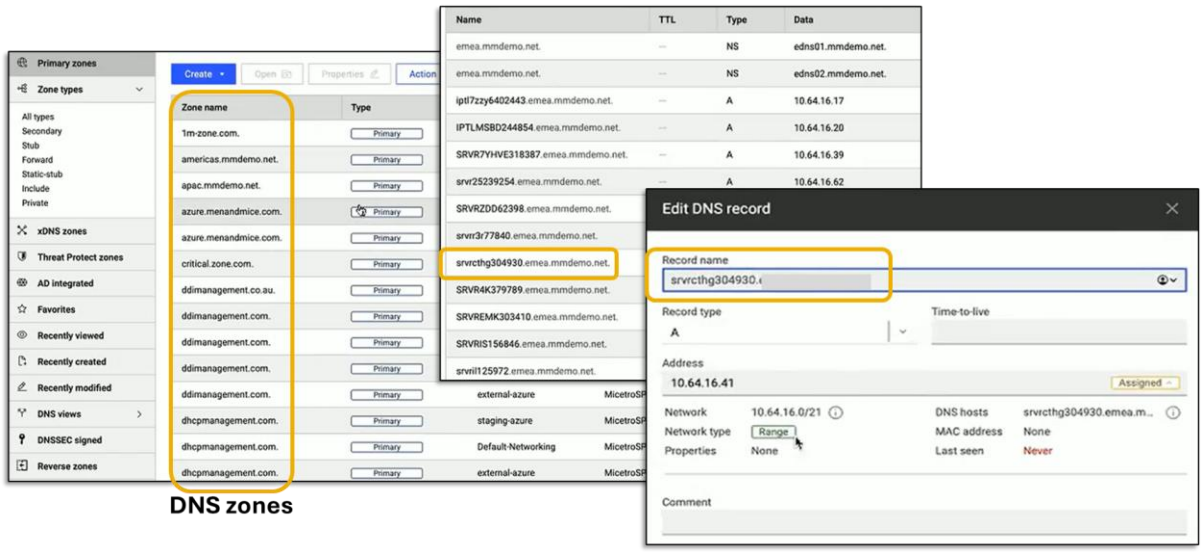
Figure 3. Centralized visibility of DDI data



Source: Omdia

Omdia proceeded to examine Micetro's DNS management capabilities. After clicking on the DNS tab, we saw that all DNS data within the network was displayed (see Figure 4).

Figure 4. Editing DNS records within a single DNS zone



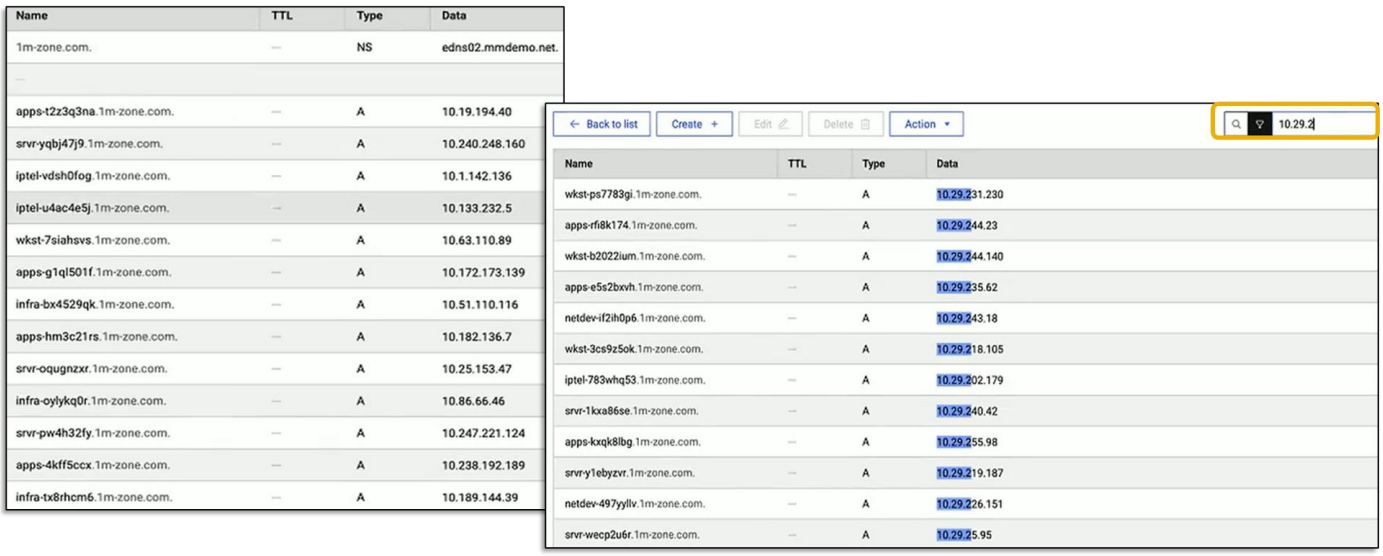
Source: Omdia

To edit any DNS records, we only needed to select and open a DNS zone, then choose the record to edit (see right of Figure 4). With this capability, the need to edit DNS records manually on the source device is eliminated. Once the changes are made in Micetro, they are pushed out to the network (and vice versa). Micetro also maintains change history to assist with traceability.

By updating records via the Micetro interface, not only do organizations decrease operational overhead, but they also reduce network errors, thereby maintaining high network availability.

When dealing with DNS records amongst multiple documents, locating specific zones can also be slow and cumbersome. Micetro can speed up this task, as the solution has been designed to be fast and responsive once DDI data is centralized. As shown in Figure 5, we opened up the "1m-zone.com" DNS zone and found that it contains over one million records. When searching for records containing "10.29.2," Micetro instantly displayed the 1,062 records containing the partial IP address.

Figure 5. Searching for "10.29.2" in one million DNS records



Source: Omdia

Why This Matters

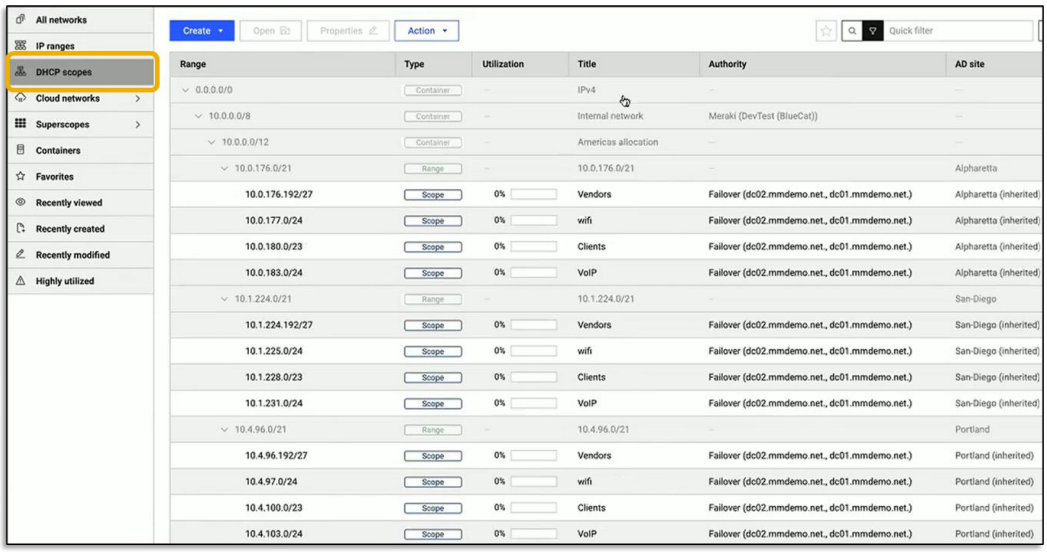
DNS data management is a critical component of network administration. If not done effectively, organizations can struggle with application and website availability, performance, and security. Yet, ensuring that IP addresses and domain names are mapped consistently and correctly can be quite cumbersome and time-consuming, specifically when gathering and resolving DNS data from multiple servers and devices. Human error can easily cause network issues.

Omdia validated that BlueCat Micetro significantly reduces the manual time and effort typically spent on gathering and resolving DNS data. Not only do organizations increase operational efficiency, but they also reduce network configuration errors, which translate directly into network availability.

Simplified DHCP Management

To evaluate how Micetro simplifies DHCP management, Omdia navigated to the "DHCP scopes" menu option and viewed the existing scopes within our test environment (see Figure 6). Centralizing DHCP scope data can help an administrator manage network configurations for multiple subnets. Manually tracking details such as available IP address ranges, subnet mask, gateway (router), and DNS servers is tedious and time-consuming, but Omdia again observed that Micetro increases operational efficiency, as manual effort is practically eliminated.

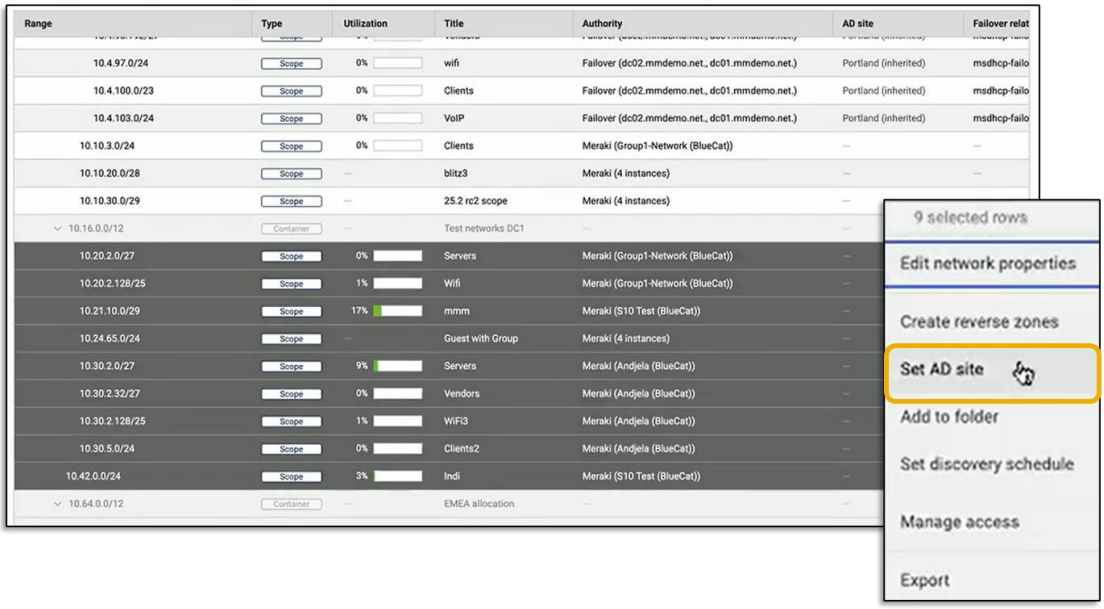
Figure 6. Centralizing visibility and management of DHCP scopes



Source: Omdia

Organizations that use AD want to ensure that network access requests are authenticated before an IP address is assigned. To ensure that all scopes are associated with the appropriate AD site, we sorted the list to uncover those scopes not yet assigned (see Figure 7). Assigning the uncovered scopes to an AD site only required that we select those scopes, right-click, and choose "Set AD site" from the pop-up menu. Assigning scopes helps increase AD reliability and efficiency so that access is granted without unnecessary delay. If not, organizations can face issues such as increased client login times and delayed access to network resources, which can affect normal operations (e.g., data replication between data centers).

Figure 7. Assigning DHCP scopes to an AD site



Source: Omdia

Without Micetro's centralized visibility, an administrator would most likely discover unauthorized access after the fact. Instead, uncovering unassigned IP addresses proactively closes this gap.

Why This Matters

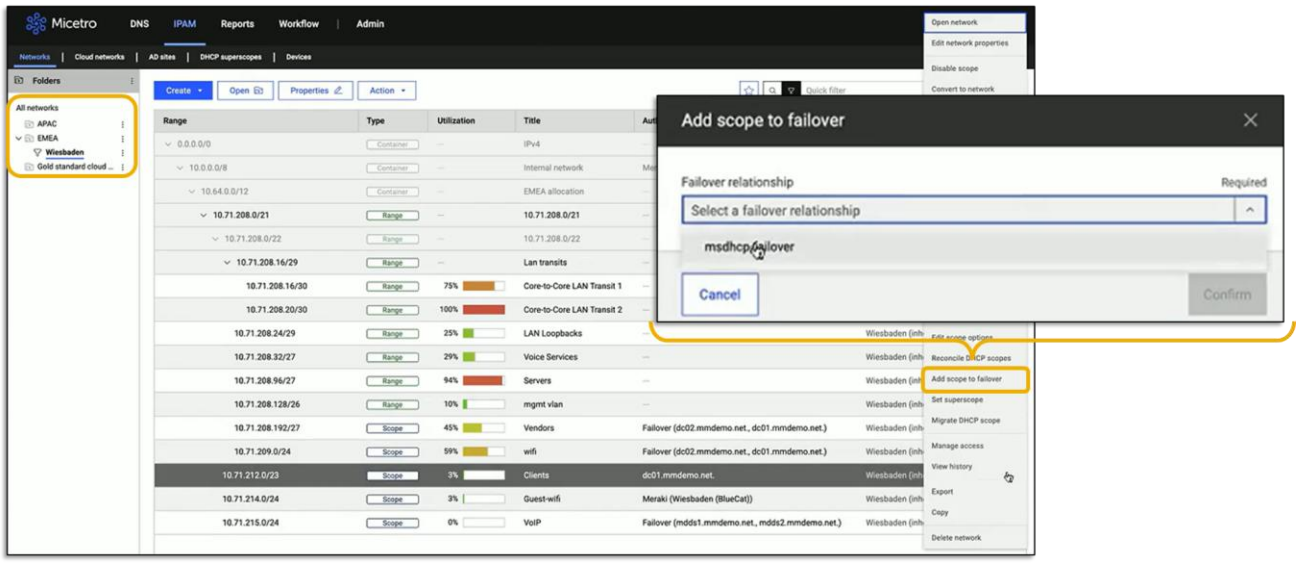
Controlling DHCP server data effectively ensures that IP addresses are allocated without inadvertently causing network conflicts. Yet, as the number of DHCP servers grows, ensuring that DHCP data is up to date becomes more difficult to accomplish.

Omdia validated that organizations can use Micetro to simplify how DHCP is managed and maintained. While we noted that Micetro can decrease operational overhead, we also observed that organizations can bolster network access security by verifying that all DHCP scopes are properly assigned.

Simplified IPAM

To evaluate Micetro's IPAM management capabilities, Omdia navigated to the IPAM tab of the Micetro interface. While all DHCP scopes can be displayed at once, Micetro can enable users to organize them into folders. In this demo, scopes were grouped according to regions and cities where on-premises networks are located (e.g., APAC, Wiesbaden in EMEA) along with public cloud resources (see top left of Figure 8).

Figure 8. Selecting IP address scope for failover purposes



Source: Omdia

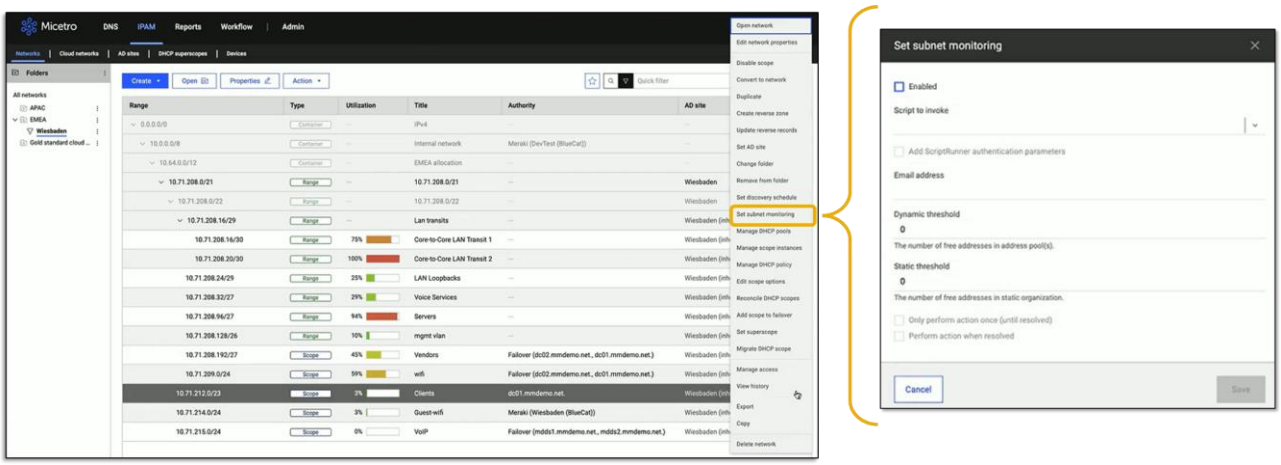
While scopes are prominently displayed, Micetro records other data from the routers (beyond data recorded in DHCP servers) such as subnets associated with the router interface, VLANs to which IP addresses are assigned, VRF[2] instances, and ARP tables.[3] With this level of detail, administrators have a comprehensive view of the network.

Instead of discovering configuration errors when a network issue occurs, Micetro can flag issues that can be resolved proactively. To illustrate, Omdia observed that a scope (range) of IP addresses, assigned to "Clients," did not have any redundancy in case a connection failed (see Figure 8). With Micetro, we simply right-clicked on the relevant line item, selected "Add Scope to Failover," and chose from the available options to function as a failover connection(s). Administrators no longer need to search through documents to find and validate the availability of an appropriate scope to be a failover option or access the relevant network devices to implement these changes.

From this view, we could also monitor subnet utilization by right-clicking on any scope and selecting "Set subnet monitoring" (see Figure 9). Here, we selected the scope named "Client." By activating this alert setting, an administrator can track real-time utilization of IP addresses within the selected scope. This helps to proactively ensure that users always have connectivity to that specific subnet.

[2] Virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to coexist within the same router at the same time. This allows for overlapping IP addresses.
[3] An address resolution protocol (ARP) table acts as temporary storage of IP-to-MAC mappings, enabling a host to contact a router.

Figure 9. Monitoring subnet utilization



Source: Omdia

Omdia then examined the IP addresses associated with a single DHCP scope. We selected the line item associated with "10.71.209.0/24" and revealed all IP addresses within the scope (see Figure 10). This view provided details such as whether an IP address is available or reserved, DNS names, and last-known MAC address. We could also monitor DNS PTR status to ensure that the mapping of an IP address to a fully qualified domain name (FQDN) was the same as in reverse. Administrators only need to check those IP addresses flagged with "Verify" under "PTR Status," eliminating the need to review all IP addresses. Once discovered, administrators can use Micetro to resolve any issues with automation.

Figure 10. All IP addresses associated with 10.71.209.0/24

Address	State	Client	Client ide...	Lease exp...	DDNS hos...	Last known MAC address	DNS names	PTR status	Last seen
10.71.209.1	Assigned	—	—	—	—	15:2A:BB:D4:F0:F2	—	—	2025-11-27 07:35:13
10.71.209.2	Assigned	—	—	—	—	7B:C0:2E:68:25:15	WKST3NLZ359876.emea.m...	OK	2025-11-27 10:35:10
10.71.209.3	Free	—	—	—	—	—	—	—	—
10.71.209.4	Free	—	—	—	—	B6:05:04:E6:4D:00	—	—	2025-05-25 12:35:07
10.71.209.5	Free	—	—	—	—	—	—	—	—
10.71.209.6	Free	—	—	—	—	—	—	—	—
10.71.209.7	Free	—	—	—	—	—	—	—	—
10.71.209.8	Reserved	WKSTU4...	2E:43:FC:...	INACTIVE	—	2E:43:FC:FE:27:11	WKSTU48EXF489388.emea...	OK	2025-11-27 09:35:10
10.71.209.9	Free	—	—	—	—	—	—	—	—
10.71.209.10	Reserved	WKSTO4...	F3:EF:7A:...	INACTIVE	—	F3:EF:7A:97:C8:B0	WKSTO4ZV380413.emea.m...	OK	2025-11-27 10:35:10
10.71.209.11	Reserved	WKSTK4...	14:40:79:...	INACTIVE	—	14:40:79:68:E5:4E	WKSTK42Z146507.emea.m...	OK	2025-11-27 10:35:10
10.71.209.12	Free	—	—	—	—	—	—	—	—
10.71.209.13	Reserved	WKSTDU...	79:28:40:...	INACTIVE	—	79:28:40:08:92:07	WKSTDUC450407.emea.m...	OK	2025-11-27 08:35:09
10.71.209.14	Reserved	WKST32...	BA:F1:5E...	INACTIVE	—	BA:F1:5E:1E:CC:E7	WKST3212H177987.emea....	OK	2025-11-27 10:35:10
10.71.209.15	Reserved	WKST81...	60:7A:09:...	INACTIVE	—	60:7A:09:22:0F:A6	WKST8183X88437.emea.m...	OK	2025-11-27 10:35:10
10.71.209.16	Reserved	WKST1T...	E3:1A:3D...	INACTIVE	—	E3:1A:3D:98:57:43	WKST1TRCXX37795.emea....	OK	2025-11-27 09:35:10
10.71.209.17	Free	—	—	—	—	—	netdev-fwgj82ya.1m-zone.c...	Verify	—
10.71.209.18	Reserved	wkstlk54...	D3:3B:20...	INACTIVE	—	D3:3B:20:9C:19:29	wkstlk5460383.emea.mmd...	OK	2025-11-27 10:35:10

Source: Omdia

Why This Matters

When managing IP addresses, organizations must regularly ensure that duplicate IP conflicts do not exist, unauthorized devices do not access network resources, and IP address utilization is optimal to accommodate authorized users requiring network access. Yet, the large number of IP addresses existing in any organization's network makes accomplishing such tasks without any errors difficult.

Omdia validated that Micetro streamlines how organizations manage, update, and orchestrate IP addresses. By centralizing the visibility of all IP addresses, organizations can significantly reduce the time and effort spent on IPAM. All relevant details (such as subnets and assigned VLANs) are embedded within each IP address record, providing a comprehensive network view. With Micetro, detecting and resolving IP address issues is easier to achieve.

Conclusion

DDI management is a tedious yet necessary task, as organizations typically rely on manually driven processes to manage and update DDI data. Yet, the emergence of hybrid and multicloud environments makes DDI management more difficult. This results in a lack of comprehensive network visibility required for the consistent application of network and security policies along with operational inefficiencies in network management and control.

BlueCat Micetro is designed to simplify DDI management and orchestration. The solution unifies DDI management across on-premises, hybrid, and multicloud environments, and an organization can leverage Micetro as its "single source of truth" when discovering and updating the data and its relationships to achieve comprehensive network visibility and control via a single web interface.

Based on our observations of how Micetro operates in specific use cases, Omdia validated that this solution benefits organizations by increasing the efficiency of DDI management. Instead of gathering data from multiple devices and updating those devices individually to reflect the proper relationships between DDI data, organizations can use Micetro to centralize the visibility and control of DDI data. By doing so, organizations can:

- Increase website availability, performance, and security when ensuring that the mapping between domain names and IP addresses is correct.
- Eliminate network conflicts when ensuring that IP addresses are available and allocated properly, as well as prevent unauthorized devices from gaining network access.
- Scale visibility and control without the need to add more infrastructure.

Omdia's validation reinforces that BlueCat Micetro can significantly simplify DDI management, regardless of network complexity and size. We are confident that Micetro can support your organization should you face challenges in implementing and operating a DDI management solution and strongly suggest placing this solution on your shortlist.

Get in touch: www.omdia.com askananalyst@omdia.com