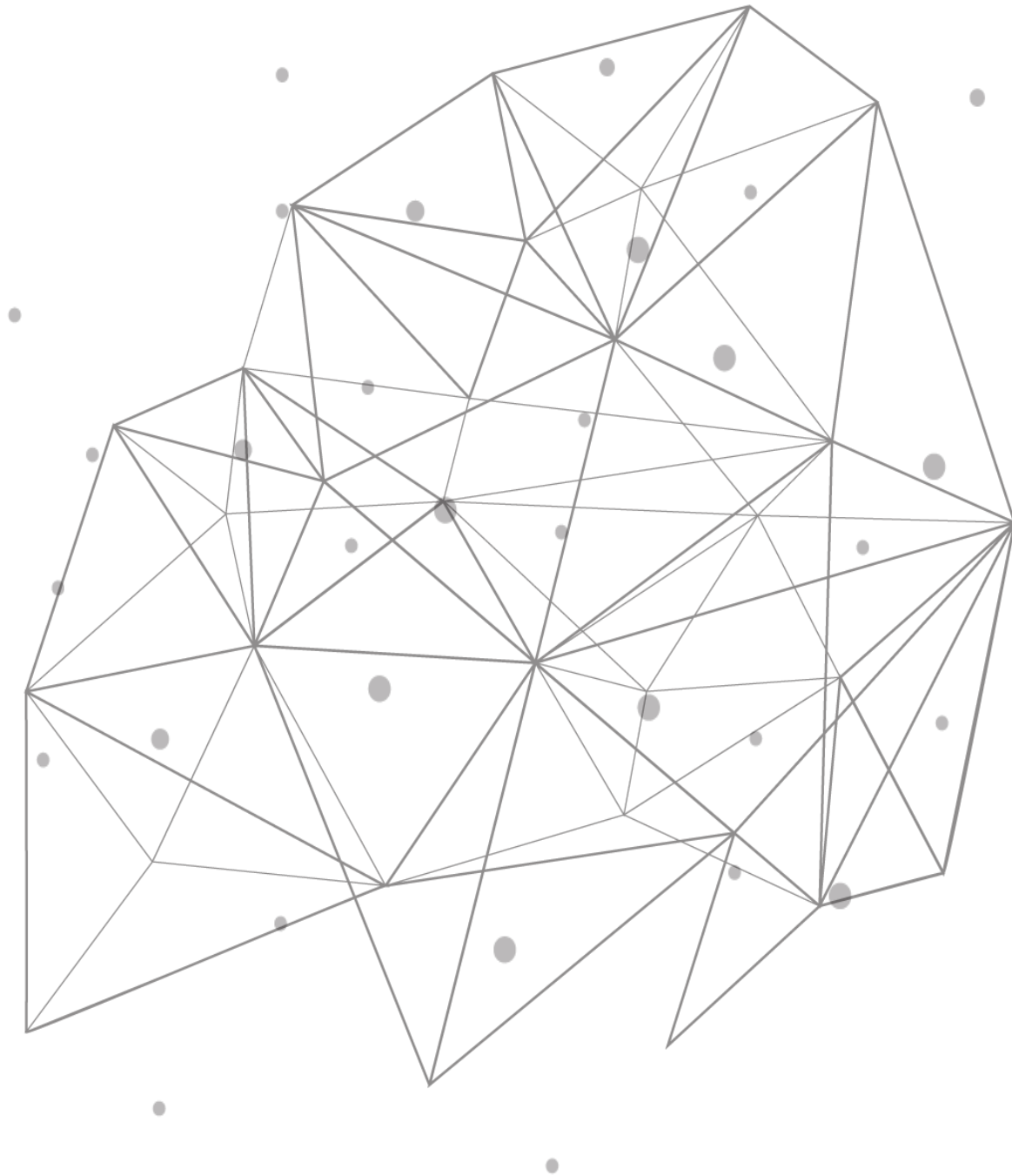


---

# TCPWave IPAM

## Managing Microsoft DNS & DHCP Services – Solution Note



## Table of Contents

<b>Introduction.....</b>	<b>3</b>
<b>Importance Of IPAM.....</b>	<b>3</b>
<b>Manual Management – Challenges.....</b>	<b>3</b>
What Is Required.....	4
Centralized IPAM Management.....	4
Delegation of Authority.....	4
Report & Alert Management.....	4
<b>TCPWave IPAM Solution.....</b>	<b>5</b>
Integration.....	5
Management – Microsoft DNS Data.....	5
Centralized Management – Microsoft DNS and DHCP.....	6
<b>Conclusion.....</b>	<b>6</b>

---

## Introduction

The DNS and DHCP services are two essential and mission-critical services for any enterprise as they are the basis of network connectivity and various applications. Many enterprises worldwide use the Microsoft DNS and DHCP services to manage the network connectivity and services. All devices in the network require IP addresses, and only DHCP can manage the distribution of IP addresses in the most cost-effective way. But managing these services has become a challenge since networks continue to add thousands of applications and devices on an unparalleled level. Therefore, it's exceptionally vital to manage these services.

## Importance Of IPAM

In today's dynamic enterprises, the network administrators find it challenging to manage the cumulative number of DNS and DHCP data with the existing tools due to the following issues:

- Rely on manual spreadsheets to manage IP addresses.
- Time-consumption.
- Prone to errors.
- Increased operational costs.
- No option to control the visibility and authority over the information available.
- Data security and compliance issues during audits.
- Reduced operational efficiency in managing IP addresses and DNS data with unwanted delays and duplicate IP addresses and security threats.

TCPWave provides an industry-leading IPAM solution to manage Microsoft DNS and DHCP environments. IPAM for Microsoft delivers robust IP address management capabilities for Microsoft DNS and DHCP services, enables the network administrators to switch from spreadsheets, multiple tools, manual labor force, and processes to cost-effective, security-oriented solutions. It does not mean that the enterprises must compromise or relinquish the existing Microsoft DNS and DHCP solution investment. With TCPWave IPAM, one has the privilege to manage the DNS and DHCP data of the entire organization, enable data security using authority delegation, audit and monitor the data with the help of centralized reporting management without any additional costs.

## Manual Management – Challenges

Manual management of DNS and DHCP services in a Microsoft server causes time consumption and additional resources. When the tasks are repetitive and include numerous steps to complete, leaving to other team members to manage these changes without substantial security repercussions would make it even cumbersome as it requires the involvement of senior staff members.

Example: Provisioning static IP to a network device such as a printer. In a typical Microsoft DNS and DHCP environment, the following steps are involved in managing the activity:

- The administrators require to look through the spreadsheet to find the free IP address in a network.
- Manually scan to confirm the IP address is indeed free.
- Update the spreadsheet with the IP address and device details.
- Provide the IP address to the requestor or configure the printer.
- Update DNS data with the device name and IP.

- The manual labor also involves scanning the network for unused IP addresses at regular intervals, reclaiming the new IP addresses, removing the obsolete DNS data, etc.
- Update the spreadsheet to make them available to use. In case of unavailability of IP addresses, creating new networks/pools, updating spreadsheets, etc., consumes time and effort from the administrators and affects their efficiency.
- Manual configuration may lead to an error and subsequent service outages.
- In case of changes required in the configuration on several servers, it adds an extra burden on the administrators.

## What Is Required

Due to the challenges mentioned above, many enterprises look for a centralized management tool which includes:

- Manage DNS and DHCP data.
- Provide visibility to all aspects of the DNS and DHCP services.
- Delegation of authority over data.
- Report management.
- Alert management.

### Centralized IPAM Management

Centralized IPAM Management helps the enterprises in the following ways:

- To manage IP address allocation.
- Track IP addresses for efficient reclamation and address duplicate IP addresses.
- Track devices and related DHCP and DNS data, reporting, etc., to avoid several tools.
- To automate some tasks of provisioning IP addresses, reclamation, and managing DNS data.

### Delegation of Authority

DNS, DHCP, and IP address management involve different teams. An efficient way of managing the services would be distributing the tasks to other people or groups with specific responsibilities and skills. An administrator should delegate the obligations to different administrator and administrator groups and provide permissions to different DDI functions without affecting other Microsoft DNS and DHCP functionalities.

**Example:** The IPAM administrator can create an administrator group to provide specific permission to Microsoft DNS data and deny permission to Microsoft DHCP data and vice versa. Additionally, the administrator can give granular level permission to networks and zones with read/write privileges, ensuring that unauthorized changes are not affecting the data.

### Report & Alert Management

To avoid service outages and ensure compliance, alerts and reports are essential. Microsoft DNS and DHCP servers must have reports which detail the IP address space status, subnet, and pool usage statistics. It should also enable the network to discover to help the network administrators find the actual status of an IP address without manually scanning IP addresses periodically. Reports help the system and network security administrators to audit compliance to several regulatory requirements. The logs allow the administrators to identify security events and mitigate internal threats proactively.

---

## TCPWave IPAM Solution

The TCPWave IPAM enables the administrators to manage Microsoft DNS and DHCP servers, DNS and DHCP remotes centrally and efficiently. The TCPWave IPAM provides the following privileges to the network administrators:

- **Templates:** Usage of templates avoids several manual steps and errors in configuration while provisioning networks and DNS zones. Managing Microsoft DNS and DHCP data from TCPWave ensures configuration across several servers is streamlined, error-free, and avoids manual configuration of individual servers.
- **Identity Administration (IA) Management:** With the TCPWave IA, the administrators can create different administrator groups with read or write privileges to specific services or components of the services.
- **Example:** The permissions can be given to networks, subnets, even to specific network objects.
- **Report Management:** TCPWave provides reporting framework that is built part of the core DDI product. Customers need not have to purchase an additional add-on device or a license for reporting. It ensures that administrators have complete visibility to network usage statistics, DHCP statistics, events reports, and audit reports.

### Integration

TCPWave IPAM provides an option to integrate your existing Microsoft DNS and DHCP servers and uses Microsoft Winrm to fulfill agentless transactions between TCPWave and Microsoft. TCPWave uses HTTPS to communicate with Microsoft servers to ensure secure data transactions. TCPWave won't have issues with the administrator to manage the Microsoft DNS and DHCP data from the Microsoft server itself as it provides Read Only and Read/Write modes.

### Management – Microsoft DNS Data

Unlike any other DDI vendors, TCPWave provides the option of creating non-administrator privileges for the service account to manage the Microsoft DNS and DHCP servers. It ensures that the account has sufficient privileges to integrate the server with TCPWave. TCPWave IPAM controls allow the administrator to create user and administrator groups and manage permissions to each group with specific privileges at the granular level.

### Centralized Management – Microsoft DNS and DHCP

Additionally, using TCPWave IPAM, administrators can manage the Microsoft DNS and DHCP servers, networks, and zones using a web-based administration window. It gives options to manage the DNS/DHCP templates for various aspects like subnet, zone, options, etc. It helps to avoid manual errors and manage configuration easily.

### Conclusion

TCPWave's DDI solution helps our customers manage and modernize their enterprise-grade solutions by ensuring they have the most innovative technology with minimal risks.

For a quick demo, contact the [TCPWave Sales Team](#).