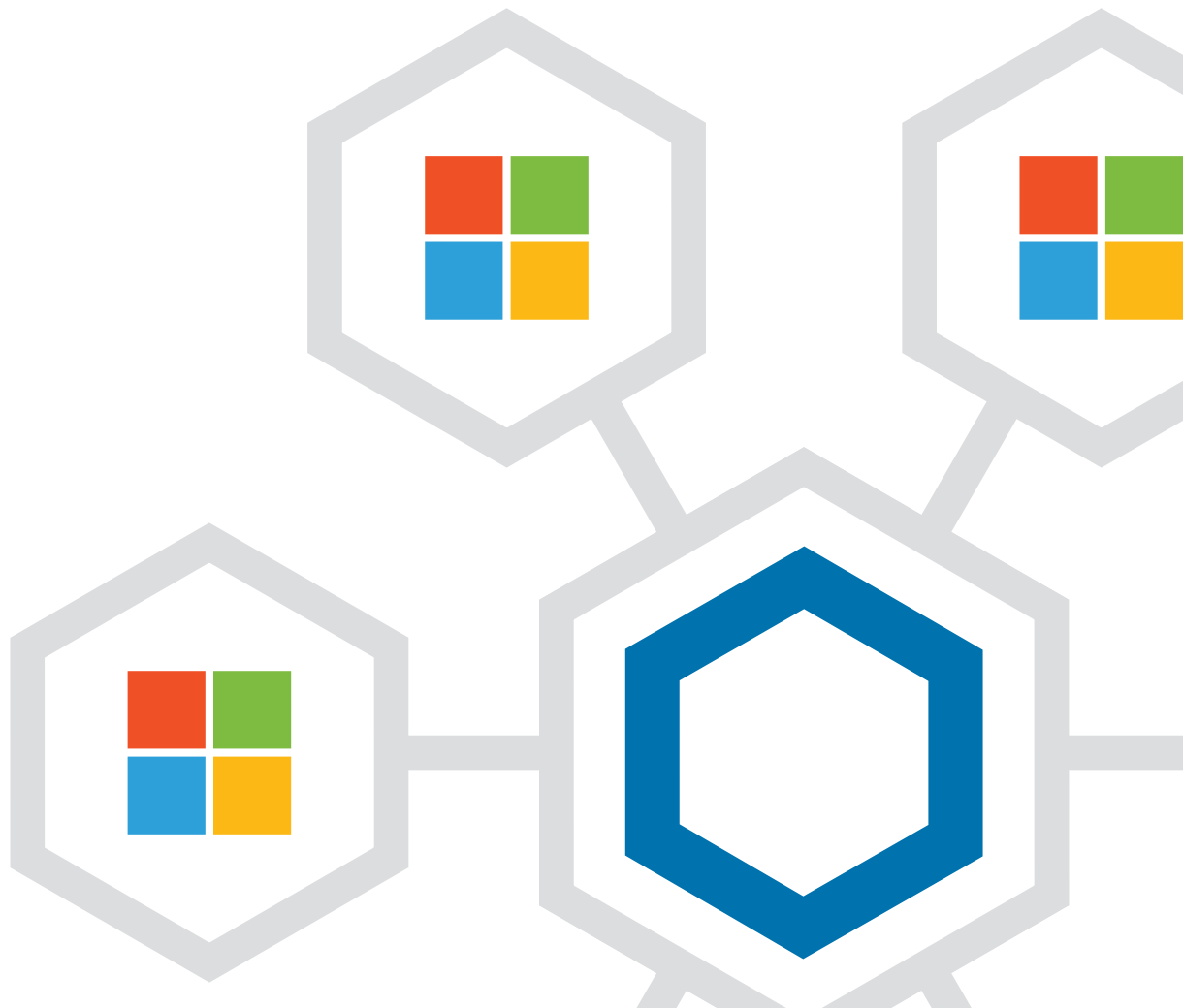# Managing Microsoft® Windows® DNS and DHCP

Extending Windows DNS and DHCP Core Services
with IP Address Management (IPAM)

Overview

When there are only a handful of Windows DNS and DHCP servers in use, managing individual hosts or addresses with Microsoft's embedded interface is relatively simple. However, tracking individual records becomes more onerous as networks grow. Larger networks with dozens of DNS and DHCP servers and a greater number of IP networks and addresses require an IP Address Management (IPAM) solution to simplify network management.

The explosive growth of IP-enabled applications and devices such as tablets, smart phones and virtual machines has created significant network management challenges for organizations. As Windows networks grow larger and more complex, organizations often struggle to manage Windows DNS and DHCP core services effectively using the Microsoft Management Console (MMC) alone.

DNS and DHCP are key technologies that enable the Internet and IP-based networks to operate. When DNS and DHCP core services fail, business stops. Inefficient, error-prone network management processes can also hinder the successful launch of new services and IT initiatives such as virtualization, cloud computing, Voice over IP (VOIP) and Unified Communications (UC).

To increase the reliability of services, reduce risk and avoid costly business disruptions, organizations need flexible, resilient and easy-to-use solutions for cohesively managing IP addresses, DNS and DHCP.

By deploying an IP Address Management (IPAM) solution to manage Microsoft Windows DNS and DHCP environments, organizations can achieve more reliable service delivery and greater efficiencies in network operations.

This white paper will discuss the key management challenges associated with Microsoft DNS and DHCP core services and how IP Address Management can extend and enhance Microsoft DNS and DHCP in four key operational areas: network management, visibility, planning & modeling and process automation.

The paper will also look at the key features and benefits of BlueCat Address Manager, BlueCat's industry-leading enterprise IP Address Management (IPAM) solution. BlueCat Address Manager can be easily incorporated into Microsoft networks to complement and extend the capabilities of the Microsoft Management Console (MMC). BlueCat Address Manager provides sophisticated management tools, greater visibility, enhanced service continuity and improved automation and control – all in a single integrated solution.

Background

Today's organizations rely on DNS and DHCP for the delivery of mission-critical applications and services. The ability to react quickly to server downtime is crucial to minimize service disruptions. Each minute spent resolving a DNS or DHCP issue is a minute of downtime that impacts business operations.

With the proliferation of IP-enabled devices, network administrators face the daunting task of managing an ever-increasing number of IP addresses. In many organizations, administrators continue to use cumbersome spreadsheets and manual processes to manage their IP address space and map allocations of IP subnets to hosts. Spreadsheets and manual processes lack the scalability to accommodate the growing size and complexity of today's networks and the volume of required IP addresses. The lack of an effective management solution creates frustration, increases the risk of errors and impedes the rollout of new services and IP-dependent technologies.

Device proliferation has also placed greater demands on Windows DNS and DHCP core services. As dynamic networks continue to grow, administrators are realizing that it is no longer effective to administer IP address space, DNS and DHCP services separately.

Spreadsheets are static and lack the ability to integrate dynamic DHCP content, which means that organizations cannot keep current with address and device changes and can never gain an up-to-the-minute picture of their network.

Managing static content with spreadsheets and dynamic content using the DHCP server necessitates the use of multiple tools to manage IP addresses and troubleshoot issues, adding unneeded complexity. With network demands for IP addresses increasing exponentially, this complexity places an even greater strain on traditional management methods and tools.

In addition to dynamic address allocation, IP-enabled devices also register DNS names dynamically. Dynamic DNS (DDNS) removes the need to manually assign hostnames to clients, helping to ease the burden of DNS administration. As a result, DNS and DHCP services are now so closely intertwined that consolidated management and global visibility is essential.

The Microsoft Management Console (MMC), a component of Windows Server operating systems, provides system administrators with an interface for configuring and monitoring network services. While a single instance of MMC can monitor and manage multiple DNS and DHCP servers, administration is performed on a server-by-server basis, each via its own module. This means that service options and data are segregated across multiple servers. Server data must be viewed, managed and maintained separately on a server-by-server basis, which prevents administrators from gaining a comprehensive view of their entire network. There is no way to gain a complete picture of the network without amalgamating information from various servers throughout the network.

The Critical Role of IP Address Management (IPAM)

To address the management needs outlined above, Windows-based organizations need a solution for centrally managing all IP address space, DNS and DHCP services.

BlueCat Address Manager is an IPAM solution that centralizes IP, DNS and DHCP information into a single pane of glass to simplify network management, reduce costs and increase the reliability of core services. Below, we'll look at how BlueCat Address Manager can be quickly and easily added to your existing Windows network to provide flexible role-based access controls, automation, change control, delegation and auditing.

BlueCat Address Manager: How It Works

BlueCat Address Manager overlays onto your Windows network quickly and easily. There is no need to upgrade or replace your existing Windows servers. You simply install BlueCat Address Manager and the BlueCat Connector for Windows DNS/DHCP. BlueCat Address Manager will then remotely connect to your Windows DNS and DHCP servers to give you complete control. There is nothing to install on domain controllers or on Windows DNS/DHCP servers.

When BlueCat Address Manager first synchronizes with your Microsoft DNS/DHCP servers, DNS and DHCP information is automatically added to the BlueCat Address Manager server, mapping and cataloguing the entire network environment into the IPAM database. From that point forward, BlueCat Address Manager acts as IPAM mission control, allowing you to view and manage all of your DNS and DHCP servers from a single Web-based interface. Smart, simple and scalable, BlueCat Address Manager makes it easy to centrally manage even the largest Windows network.
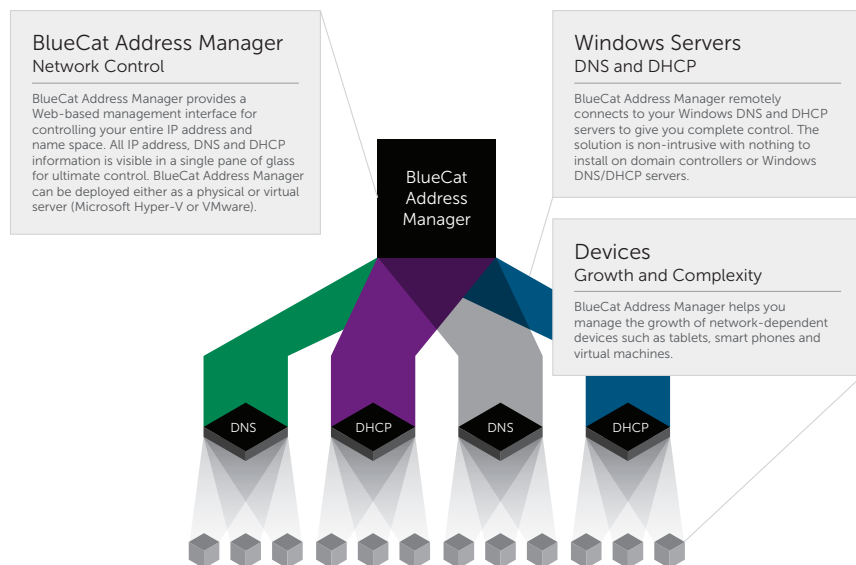
BlueCat Address Manager
Network Control

BlueCat Address Manager provides a Web-based management interface for controlling your entire IP address and name space. All IP address, DNS and DHCP information is visible in a single pane of glass for ultimate control. BlueCat Address Manager can be deployed either as a physical or virtual server (Microsoft Hyper-V or VMware).

Windows Servers
DNS and DHCP

BlueCat Address Manager remotely connects to your Windows DNS and DHCP servers to give you complete control. The solution is non-intrusive with nothing to install on domain controllers or Windows DNS/DHCP servers.

BlueCat
Address
Manager

Devices
Growth and Complexity

BlueCat Address Manager helps you manage the growth of network-dependent devices such as tablets, smart phones and virtual machines.

DNS   DHCP   DNS   DHCP

Figure 1: BlueCat Address Manager provides centralized management and control for all your Microsoft Windows DNS and DHCP servers.

Benefits of the BlueCat Address Manager Platform

BlueCat Address Manager delivers benefits in four key areas: efficient network management, global visibility, planning & modeling and process automation.

1. Efficient Network Management

BlueCat Address Manager allows IT to do more with less by reducing the load on expert administrators and enabling common tasks to be automated and delegated with flexible role-based authentication, change control, rollback and auditing.

Flexible Role-Based Access Control

With BlueCat Address Manager, you can define permissions to objects throughout the system, allowing senior network administrators to assign or restrict access rights to those who need it – regardless of their physical location or logical area of responsibility. This is useful when organizations have a distributed service environment with DNS and DHCP servers in multiple locations, or a large number of administrators to whom tasks are delegated.

Access rights can be assigned system-wide or on a per object basis. Senior administrators can hide certain services, networks, zones and even records from junior staff. With these restrictions in place, junior administrators, once authenticated, are limited to the IPAM data for which they have access rights. You can define permissions for any number of zones or networks right down to the record level.

Workflow

Organizations looking to reduce IT management costs prefer that their highly-paid senior staff not expend undue time and effort on mundane or repetitive chores that could be handled by more junior administrators. While DNS and DHCP administration requires skilled resources, there are many tasks that can be delegated to junior administrators – provided the proper workflow and change controls are in place.

Windows DNS and DHCP services do not include these controls natively. As a result, Microsoft network administrators rarely delegate change management responsibilities for DNS/DHCP to junior staff. Their rationale is understandable. Not all administrators have the skills or experience required to properly manage DNS/DHCP and there is no means to limit the scope of changes that junior administrators could make.

Similarly, there is no easy way to restrict the types of modifications that could be made to DHCP systems. On the DNS side, a permissions schema to restrict modifications to DNS data is only available through Active Directory-integrated DNS. Individual changes are not tracked through logging or change management.

The risk of a configuration error resulting in a service outage is simply too great to allow an inexperienced network administrator unfettered access to configuration utilities. Best practices in network governance dictate strict controls and oversight on network configuration changes.

BlueCat Address Manager includes a fully integrated change control system for managing workflow, network changes and delegation. This allows more senior administrators to enforce change approval within BlueCat Address Manager. Using such a system, a senior administrator would need to approve a change made by a workflow user to a workflow-enabled object before that change was added to the system. This helps to safeguard the system against configuration mistakes by requiring changes to be approved before they are implemented into the system. This allows organizations to take advantage of a larger pool of personnel to suggest changes, while ensuring that accountability for the actual changes remains clear.

As well, BlueCat Address Manager's granular permissions structure allows permissions to be delegated down to the resource record level, while giving senior administrators a higher comfort level when delegating critical tasks within the organization.

Tracking and Auditing

BlueCat Address Manager includes comprehensive transaction auditing to provide the real-time and historical data you need to answer important questions such as who, what, where and when. Each DNS and DHCP change is listed with user names and time stamps associated with it. Tracking user transactions helps you to comply with internal policies and key external regulations such as the Health Insurance Portability Accounting Act (HIPAA) and Sarbanes-Oxley (SOX).

Another advantage of BlueCat Address Manager is the ability to provide concurrent administration within the system. Many administrators can log into BlueCat Address Manager and make changes to the configuration data at the same time.

BlueCat Address Manager uses session data to track the changes being made. Each time an administrator signs into BlueCat Address Manager, a session is created, tying every database transaction to a session. Session information includes the administrator's identity, authentication system, the IP address used to sign into BlueCat Address Manager and any user-supplied comments. With this detailed information, BlueCat Address Manager creates an audit trail describing the information that was changed and by whom.

BlueCat Address Manager also tracks dynamic updates, such as DHCP lease changes and Dynamic DNS (DDNS) host registrations from Windows servers. These updates are recorded in the audit trail and are available for administrators to browse. Change information can be reviewed on a system-wide basis, per object and per user for enhanced control.

Monitoring, Logging and Reporting

BlueCat Address Manager provides a real-time, centralized view of overall service availability across the entire DNS and DHCP network. BlueCat Address Manager can be configured to send notifications by email and/or through SNMP alerts. On-box monitoring reports key events such as DHCP scope usage to preempt network capacity issues ahead of time. These proactive measures prevent network outages and allow for rapid response when problems do occur.

BlueCat Address Manager includes a centralized logging system, which captures all transactions and system-generated events including alerts. Actions and events such as successful deployments, system errors and informational messages are gathered. All events are filtered by a configurable notification system that stipulates rules for how administrators are to be notified. The system can filter by source and/or severity and inform administrators via e-mail notifications or SNMP traps.

A host of reports can be configured within BlueCat Address Manager to allow administrators to quickly view key information regarding their IP infrastructure. Reports include system-wide DHCP usage, configuration changes and statistical DNS information. To offer additional flexibility, reports can be prepared in several file formats including PDF, HTML, CSV, XLS and RTF.

2. Global Visibility and Scope

In a pure Microsoft DHCP environment, information is stored in a server-centric approach. Administrators must first navigate to the server where the DHCP range is hosted, then find the specific details. BlueCat Address Manager's business-centric approach stores data on the system in its entirety rather than on a server-by-server basis. Since everything is stored in one place, administrators can more easily access data and see the global "big picture view" of their network.

BlueCat Address Manager provides a centralized, consolidated view of IP address space, DNS and DHCP. All DNS, DHCP and the IP address space changes are made through a Web-based interface and logged to the BlueCat Address Manager relational database. This allows administrators to gain a complete view of the entire address and name space regardless of which server actually holds the data or provides the service. The easy-to-use BlueCat Address Manager interface provides you with a view of every device on your network including its MAC address, its DHCP lease information and its DNS host record.

Within BlueCat Address Manager, DNS and DHCP data is deployed to servers through an innovative concept known as deployment roles. Deployment roles determine which server is responsible for a given DHCP scope or DNS zone. Roles are defined at the data level (IP networks and blocks for DHCP and views and zones for DNS), so you can define server roles without sacrificing a central view of the data.

The BlueCat Address Manager interface is "multi-core," meaning that DNS changes are reflected immediately in the IP address space and DNS changes made at the IP address level are updated within DNS zones. For example, when a host record is added to DNS, its associated IP address is updated within the IP address space view. Similarly, changing a host record's IP address information is automatically updated in the proper DNS zone. Changes in one core are automatically reflected in the other, eliminating the need to update each service individually and/or update spreadsheets.

In addition to being able to track network assets by their DNS hostnames, IP addresses and MAC addresses, administrators can organize information by serial numbers, asset tags, department names or just about any other relevant criteria. This intuitive business-centric information is useful when tracking assets, locating systems or troubleshooting problems. With BlueCat Address Manager, administrators can use any browser-based device to view and manage all IP assets across the network. They can make changes, view network details and approve change requests all from their smart device or Web browser – anywhere, anytime.

3. Network Planning and Modeling

Within many organizations, network designs and IP allocation plans were developed years ago and may not scale for network growth and complexity. Network architects face the imposing task of redefining the IP space – breaking it up, calculating new subnets, or possibly transitioning from public IP address structures to private IP addressing – in order to accommodate current and future requirements.

Using spreadsheets to remodel IP address space can be a highly manual and time-consuming task. While there are tools to help calculate and divide the IP space, there is still a significant amount of administrative effort needed. BlueCat Address Manager allows administrators to plan and model their public, private and test networks with sophisticated tools that track, partition, resize, move and split IP network space as required.

Administrators can model the space using different scenarios to determine the best long-term configuration. These scenarios can co-exist in BlueCat Address Manager along with the current configuration – the production network is not affected by BlueCat Address Manager's modeling utilities.

When modeling network changes, it is not necessary to calculate IP subnets manually or to determine how many hosts would reside on each. BlueCat Address Manager performs these calculations and allocations automatically. Once the optimal scenario is established, it is ready for deployment.

BlueCat Address Manager further simplifies modeling tasks through network templates, which accelerate network design by automating configuration information common to multiple subnets. Network templates can include default gateway addresses, reserved ranges, DHCP ranges and DHCP options. Templates are then applied to the appropriate networks to implement the settings instantly. When a common setting requires change, the administrator makes the change in the template and then re-applies it to all affected networks.

Zone templates for DNS apply a similar principle – common zone information such as resource records and DNS options can be configured in a zone template and then applied to multiple DNS zones.

For example, a set of MX records may be responsible for handling the mail in several hundred domains. Configuring a zone template with these MX records allows administrators to apply changes to all domains quickly and easily. Templates save time for administrators who no longer have to manually configure hundreds or even thousands of networks.

4. Multiple Levels of Process Automation

BlueCat Address Manager provides multiple levels of process automation to make routine tasks faster, while reducing user-driven errors. Automation features such as Next Available Address or Next Available Network reduce the time and effort required to carry out daily tasks. Administrators can easily allocate new addresses and provision new networks with the click of a button. There is no longer a need to search through hundreds of networks and addresses, or to scroll through spreadsheets to find available resources.

Integrated Data Validation Tools

Manual configuration changes are susceptible to human errors and, within Microsoft DNS and DHCP environments, configuration changes are applied instantly. A configuration error such as a mistyped host entry or missing value can have an immediate and potentially devastating effect on the network. Administrators must exercise care when implementing changes, but even the most meticulous people can still occasionally make mistakes. With BlueCat Address Manager, DNS and DHCP data is not "live" until you choose to deploy it to your Windows servers.

BlueCat Address Manager provides multiple levels of error and data checking to ensure data integrity within the system. As you add new data into the system, BlueCat Address Manager validates it for syntactical or logical errors. This built-in intelligence significantly reduces errors within the system and proactively prevents administrators from deploying changes that would otherwise have an adverse effect on their network.

You can also schedule BlueCat Address Manager's Data Checker to periodically examine DNS and DHCP data for industry best practices and configuration errors that might prevent deployment within DNS or DHCP environments. The Data Checker utility runs in the background to examine the configuration and compares it against best practices to reveal instances where settings might be less than ideal.

When a questionable setting is detected, it is automatically analyzed to determine the impact it will have on the system. A setting that results in an error state is flagged and deployment is suspended until an administrator can resolve the issue. Being able to safeguard against common misconfigurations and error helps to ensure that only clean data is passed on to the DNS and DHCP server, reducing potential outages.

Scheduled and On-Demand Deployments

Depending on your organizational needs, you can deploy changes on demand or schedule deployments to occur at off-peak hours. For example, you can schedule accumulated changes to be deployed during the evening.

Automatic Discovery and IP Reconciliation

Because DHCP data and information only extends to dynamic clients, this limits visibility into network address usage and allocation. In a Windows DNS and DHCP server based environment, all static network allocations and changes have to be maintained and documented manually by administrators.

Without an accurate representation of network activity, solving DNS or DHCP-related problems become more difficult and time-consuming. Without sufficient tools, organizations are forced to spend unnecessary amounts of time and resources managing their DNS and DHCP infrastructure. The ability to quickly identify a dynamic client's IP and MAC address from a single view or identify recent DNS changes in a timely fashion can be critical to the successful resolution of an issue.

The BlueCat Address Manager network discovery tool uses SNMP to talk directly to routers and layer 3 switches, enabling BlueCat Address Manager to automatically find changes to connected devices across geographically-dispersed networks. BlueCat Address Manager finds newly added and recently removed addresses, as well as identifying conflicts based on DNS hostname and MAC address. After discovery, the network reconciliation component compares the changes to identify unused IP addresses for reclamation and help uncover unauthorized IP addresses that can create security vulnerabilities.

BlueCat Address Manager provides administrators with powerful tools to reconcile the data in the IPAM system with the current state of their networks. BlueCat Address Manager's network reconciliation algorithm:

- Discovers new nodes on the network
- Alerts on nodes which have been unexpectedly decommissioned or taken offline that are still allocated
- Uncovers mismatch conditions where an IP address/MAC address/hostname port location association has changed (i.e. an IP address that was associated with one MAC address, but is now associated with a different one)

One of the primary benefits of network reconciliation is the ability to reclaim unused IP addresses, which is particularly useful in light of IP address scarcity. Also valuable is the ability to discover unauthorized IP addresses, which can represent security vulnerabilities or unauthorized changes.

Administrators can define network reconciliation policies for a particular network or at the configuration level. The discovered information is compared to data in the system to ensure the validity and integrity of all IPAM-related data. After the discovery process is complete, administrators are presented with several options to deal with addresses that are either unknown, no longer in use, or require updating. These policies can be defined on a schedule to ensure that network data is continually reconciled for greater consistency and accuracy.

Network Continuity and Resilient Core Services

The continuity of network operations ensures that your organization is always ready to do business. To shield organizations from costly network downtime and disruption of mission-critical services, DNS and DHCP services need to be safeguarded against mis-configurations and errors that can bring down services. In the event that a DNS or DHCP outage does occur, organizations need to be able to quickly recover in order to bring everything back online and minimize service and business disruption.

BlueCat Address Manager allows administrators to selectively restore configuration changes carried out on the system. This functionality, unavailable in Windows DNS and DHCP, can be used to quickly restore deleted items without requiring time-consuming restoration procedures or guesswork to manually restore lost configuration data.

To enhance the resiliency and reliability of core services, BlueCat Address Manager servers can be deployed in three-unit clusters with data replication between the systems in the cluster. Administrators access the primary system to make configuration changes and updates. Any change made to one unit will automatically be replicated to all other systems.

Data replication keeps all BlueCat Address Manager units synchronized and ensures any unit can substitute for the other. Should one BlueCat Address Manager server fail, its partner can continue functioning for both, ensuring there is no administration downtime.
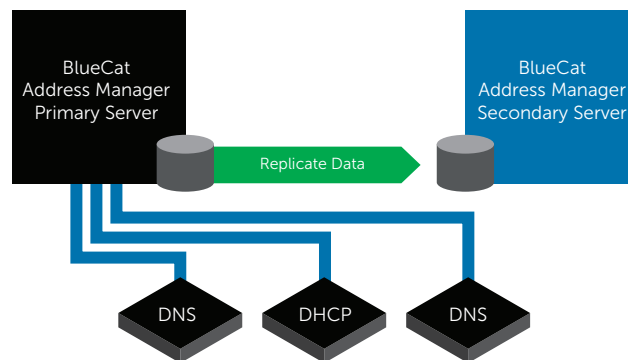

Figure 2a: BlueCat Address Manager clustering with replication allows two physically separate BlueCat Address Manager servers to maintain identical copies of all DNS, DHCP and IPAM data.
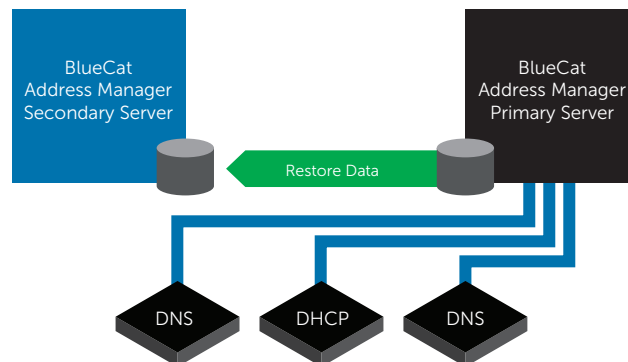

Figure 2b: In the event of a failure, data replication ensures that one BlueCat Address Manager server can failover to the other to ensure continued management of your critical DNS, DHCP and IPAM environment.

Administrators can configure BlueCat Address Manager to maintain local backups and transfer them automatically via secure means to an offsite server. This ensures all IPAM data is kept safe and available should a hardware failure occur. In the event of a failure, or if a previous configuration needs to be rolled-back, the database can be restored and deployed down to Windows servers. With its backup, clustering and failover capabilities, BlueCat Address Manager ensures that DNS and DHCP core services are resilient and available.

Summing Up

In today's network-dependent world, organizations need to ensure that their Windows DNS and DHCP infrastructures remain reliable, effective and efficient. BlueCat Address Manager complements and enhances Microsoft DNS and DHCP services by providing visibility into all DNS and DHCP activity, sophisticated tracking and modeling tools, increased service continuity and centralized IP Address Management.

BlueCat Address Manager is easy to deploy in your existing Microsoft DNS and DHCP infrastructure, so you can keep your existing service infrastructure, but lose the need for cumbersome spreadsheets and inefficient management processes.

BlueCat Address Manager introduces new efficiencies and cost savings by streamlining workloads, enabling the delegation of responsibilities and simplifying the network infrastructure. By providing sophisticated network management capabilities that are lacking in the current Windows DNS/DHCP interface, BlueCat Address Manager saves you time and resources, while making the most of your Windows technology investments.

⊗ BLUECAT

At BlueCat, we believe the explosive growth of connected devices requires a more intelligent network to ensure reliable, secure, always-on application access and connectivity. BlueCat IP Address Management (IPAM) solutions provide a smarter way to connect mobile devices, applications, virtual environments and clouds. With unified mobile security, address management, automation and self-service, BlueCat offers a rich source of network intelligence that can be put into action to protect your network, reduce IT costs and ensure reliable service delivery.

Enterprises and government agencies worldwide trust BlueCat to manage millions of devices and solve real business and IT challenges – from secure, risk-free BYOD to virtualization and cloud automation. Our innovative solutions and expertise enable organizations to build a network infrastructure that is more scalable, reliable and secure, as well as simplify the transition to next-generation technologies including IPv6, DNSSEC, M2M and SDN.

www.bluecatnetworks.com