Best Practices for Successful IP Address Management (IPAM)
Introduction

Network complexity grows as the result of organic expansion and network-intensive initiatives such as virtualization, cloud adoption, and bring your own device (BYOD). These factors increase the need for accurate and dynamic IP address management (IPAM). IPAM discovers IP addresses on a network, deploys new addresses, keeps accurate records, enables address planning, and monitors IP address usage from a central interface.

An IP address is the single, unique identifier for physical and virtual objects on the network. Ranges of IP addresses define the networks themselves. Infoblox takes IP address management to a new level by providing information that gives IT departments and organizations integrated management of network resources while advancing the concept of IP resource management.

This paper reviews the layers of information that can be built by the Infoblox IPAM solution, explains the optimal methods for adding detail, and tells how these levels of detail form a single pane of glass for viewing the network and its virtually and physically attached devices, and how it can be leveraged to support mission-critical tasks.

IPAM Today

Today’s need for IPAM begins with IP address discovery, tracking, and allocation. As networks grow, keeping track of multiple types of data pertaining to devices on the network adds complexity. IT vendors are creating new tools to help track network devices, but the information is often not centralized, eroding confidence in the data’s accuracy and timeliness.

In some cases, the data is growing more disparate and out of sync among each “ecosystem” of information, with little or no sharing between groups, making the overall picture murky. The single greatest challenge today in IP address management is to centrally track and maintain a near-real-time view of all the adds, moves, and changes occurring on the network. Every time a virtual machine is provisioned, or a tablet leaves the wireless network, the IP address landscape changes and the IPAM database needs to be up to date.

What Is Needed

Creating a central repository of all the information on networks, IP addresses and hosts alike, is critical to maintaining control of the network. The challenge with traditional tools is that there is a different one for each category of devices: one system to track virtual machines, one system to track wireless users, one system to track Windows servers, one system to track Linux machines, etc. Today’s organization needs a single repository where all the data relevant to networks, hosts, servers, dynamic clients, and virtual environments can be tracked and synchronized. The ability to search across all this information will enable network teams to quickly track changing network landscapes and rapidly troubleshoot issues as they arise. In addition, business data related to a network resource helps bind together the logical network construct and the reality of IT resources.
Deriving the Complete Picture

When considering IP address assignments, network administrators are not only interested in the utilization of the IP address space, but in the type of resource each IP address is assigned to. The IP address itself is irrelevant to the organization: the resources and services associated with that address are what matter. Using Infoblox, IPAM administrators are able to see all the pertinent meta-information related to the network resource such as hostname, device type, physical location, etc. When the same capability is applied across the organization, others gain access to service information related to the resources that are germane to their job functions.

For example:

**Server Team**
- Device type
- Device name
- Hardware
- OS
- Software or services installed
- Function
- Security profile

**Network Team**
- IP address
- Network, gateway, and netmask
- Network name
- VLAN
- Switch port and interface
- Interface speed and duplex

**Operations or Facilities**
- Hardware components
- Licensing status
- Support information
- Maintenance contract and renewal dates
- Owner or contact information
- Depreciation lifecycle
- Ticketing or approval information
- Operational status (production, testing, development, backup, etc.)
- Last seen on network

A centralized, authoritative database of resources clearly defined by metadata constitutes a huge leap forward in managing the network and in managing the business of network resources.
Bringing the Data Together

By leveraging its database along with Extensible Attributes, Infoblox ties together the various data associated with devices, networks, and services in one clear and easy-to-manage interface. Taking IPAM past the level of just IP addressing allows users to associate information to all objects in the Infoblox database and allow administrators to search, sort, and export based on any data mapped to those objects. For example, a search for everything that has the Extensible Attribute “City” equal to “Denver,” gives back all DNS entries, fixed addresses, and even network administrators, architects, and engineers that have this attribute. By allowing all-inclusive mapping of information, Infoblox accelerates inventory and troubleshooting tasks and allows organizations to map data in a way that is specific to their organizational structure, needs, and requirements.

Data is brought into the Infoblox solution through the import of protocol data such as DNS and DHCP, but can also be imported from spreadsheets and other ad hoc mechanisms maintained throughout an organization. Functions such as Infoblox DHCP Fingerprinting enrich the data captured for hosts and clients connected to the network. Once this data is ingested and mapped to the attribute structure, additional discovery tasks can be configured to validate the data and keep it up to date, keeping administrators current with the highly dynamic network landscape.

Protocol Data

Much of the basic IPAM information is provided by the protocol data in the form of DNS and DHCP entries. Administrators do not have to start from scratch. DNS and DHCP data provides a good portion of the IP address landscape. Having integrated access to protocol data reduces the legwork of maintaining an IPAM database as DNS and DHCP entries are updated. As the server team provisions a new server, and in the process create a DNS entry for it, or as the network team creates a new network serving DHCP, that data is also captured in the IP address database. Because IP address and names are the most searched and tracked information about hosts connected to the network, this is the best starting place to bring objects into the database.

DHCP Fingerprinting for Richer IP Data

Analysis of the DHCP information gathered from DHCP helps characterize the dynamic hosts on your network. By analyzing the data provided by the client, Infoblox can identify and label clients based on common criteria. When a client sends a DHCP discovery or request packet, Infoblox processes the request and can “fingerprint” the type of client making the request. This becomes an important part of the overall information tracked related to the hosts on the network and provides a means to enforce access policies at the edge of the network.
Below is the process in which Infoblox takes information included in client DHCP discovery and request messages and adds it to the IPAM view.

DHCPDISCOVER Option Sequence 1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43

DHCPDISCOVER Option Sequence 1, 3, 6, 15, 119, 78, 79, 95, 252

Figure 1. Device fingerprinting for enforcing network-access policy

Figure 2. DHCP-fingerprint/MAC-address pairs that have had changes should be treated as risks and investigated.

DHCP Fingerprinting also provides a mechanism to detect and track changes to fingerprints, allowing it to detect MAC spoofing in the network. One common way to gain unauthorized access to a network is to find an existing client on that network and spoof its MAC address. By tracking DHCP fingerprinting and MAC address pairs, the system can determine if the associated fingerprint has changed. The storage of MAC address and fingerprint pairs prevents access to potentially malicious behavior on a network.
Network administrators can easily see what devices are attached to their network using an Infoblox dashboard widget. The Infoblox dashboard widget gives the administrator a quick view of network elements germane to their tasks. Granular role-based administration lets administrators define which widgets they see when logging into the system, and be proactive with their first cup of coffee.

Extensible Attributes

Extensible Attributes are categories of information or metadata related to the objects in the Infoblox solution. Infoblox supports the addition and maintenance of Extensible Attributes to allow merging of information about hosts from different groups in an organization. Infoblox goes past traditional IP-centric IPAM and these attributes can, at the discretion of the user, be applied to any type of object in the architecture.
As shown in Figure 4, the values for Extensible Attributes can be in drop-down lists for users, or could be in any of the pre-defined data formats such as date, email address, number (integer), or a free-form text string. Each Extensible Attribute can be configured to be required, recommended, or not required for any object type. For example, the attribute “VLAN” can be set up as a required field whenever an IPv4 network is being added, because without specifying the required VLAN information, administrators will not be able to save the IPv4 network.

### Extensible Attribute Inheritance

Another way Infoblox allows for the quick application of Extensible Attributes is through the concept of inheritance. When an IPAM object such as a network is created, users can opt to have objects within that object inherit these attributes, thus allowing application of the attributes to all child objects at one time and ensuring that parent and child objects get the same attributes. If a network is in the “City” of “Denver,” users don’t have to manually add that attribute to every DHCP range, fixed address, or host object in that network.

![Figure 5. Inheritance of Extensible Attributes](image)

### Smart Folders

Smart Folders are a powerful way to organize and categorize information collected on the Infoblox Grid™. IPAM information can be organized based on the built-in values or Extensible Attributes. It is not necessary to use Extensible Attributes in order to use Smart Folders, although having them greatly enhances the Smart Folder experience. Using Smart Folders is similar to creating play lists based on meta-info of your music library, such as “80’s Movie Sound Tracks.” For example, a network administrator can create Smart Folders based on the location of the networks, and then under each city, organize by the network usage. Screenshots in Figure 6 show different views of the same data set.

![Figure 6. Smart Folder examples using Extensible Attributes](image)
CSV Import
While protocol data and device-fingerprint data are automatically captured by Infoblox DNS and DHCP services, other groups inside organizations also maintain a variety of information about the devices connected to the network. All of the data related to network devices can be brought into Infoblox to create a single, authoritative source of information. The Infoblox CSV import tool can be used to migrate and import this data to give a complete picture of network entities. CSV import can bring in additional information for new and existing hosts.

Adding Network Discovery Data
Protocol data and CSV imports alone may not cover all the needs of an organization’s IPAM implementation. There are hosts outside of the realm of DNS and DHCP that are difficult to identify, and there is valuable attribute information beyond that which is provided by protocol data. Infoblox provides additional discovery methods, including network discovery and virtual machine (VM) discovery in the core DDI solution; however, in a best practice for IPAM scenario, Infoblox expands discovery data with Infoblox Network Insight.

The discovery performed by Network Insight is very efficient, customizable on a very granular basis regarding what is discovered when and is integrated into existing workflows in DDI to make it efficient. Network Insight discovers missing hosts, detects address assignment conflicts, provides additional information about the existing entries in the IPAM database, and equally important, provides information on network assets not reflected in the IPAM database.

Enhanced IPAM with Infoblox Network Insight
You can deliver more efficient workflows using a single source of network infrastructure and IPAM data. Infoblox Network Insight enhances Infoblox IPAM by integrating infrastructure device data with IP address management. The collection and correlation of this data provides exceptional visibility, helping network administrators gather information, analyze it, and then take the appropriate action to:
• Reduce mean time to repair (MTTR)
• Exclude the network as a root cause
• Validate designs
• Identify errors
• Improve operational efficiencies through seamless workflows for device and IP address
• Reduce security and service interruption risk
• Detect rogue devices
• Bring unmanaged networks and devices back to a managed state within the IPAM database

Network Insight resides on physical or virtual appliances that are Infoblox Grid members, making them part of a unified system with a single point of management, common updates, built-in security, and resiliency.

Integrated Discovery Data
The integration of Network Insight into DDI makes discovery part of the administrator’s standard workflow. Discovery is active and connectivity-aware. For example, Infoblox uses its awareness default gateways to seed the discovery process and help it run efficiently.

Different discovery techniques are necessary to discover all devices and related information. Infoblox Network Insight uses multiple ways to discover what is on the network and uses these methods in efficient ways. Network scanning is a common method and uses technologies such as ping to sweep the network for connected devices. Infoblox uses ping to perform network scanning, but it can also use more efficient and predictable tools such as SNMP-based discovery with layer-2 and layer-3 devices. These are less-intrusive methods, work better with large address space like IPv6, and can still be leveraged if a system has a local firewall that prevents scanning. This method leverages the information that routers and switches already possess about connected devices to bolster IPAM data. This unique, layered approach and the integration of device data provides deeper and richer data that is especially valuable to network administrators in a Microsoft Windows environment.

Figure 8. Infrastructure devices within the Acme network

Figure 9. Drill-down into discovered device data
Infoblox DDI Automates Network Services for the Cloud

Infoblox provides the industry’s widest range of supported platforms for managing DNS, DHCP, and IP address integration with private cloud platforms. Private clouds gained traction because they enable agile and scalable delivery of IT services. To fully exploit the advantages of private clouds, organizations must quickly add and remove applications and services, shifting workloads across sites, running workloads in multi-tenant architectures, and making the underlying networks resilient to failures. While many of these processes are automated today from a server and storage perspective, network services are still largely managed manually, complicating and impeding private cloud operations.

Infoblox DDI automates network services for private-cloud deployments by providing network services without needless delay. Virtual machines (VMs) can be provisioned with IP addresses and DNS records in minutes, instead of the hours or days that manual processes can require. These IP addresses can be recovered and reused, and DNS records cleaned up automatically when VMs are retired. Infoblox DDI integrates with these seven cloud platforms, orchestrators, and products:

- VMware: vCenter Orchestrator, vCloud Suite, and vRealize Automation (vRA)
- Microsoft: System Center Orchestrator and Virtual Machine Manager (VMM)
- HP: Operations Orchestration and Cloud Service Automation (CSA)
- Cisco: Cisco Intelligent Automation for Cloud (CIAC)
- BMC: Atrium Orchestrator and Cloud Lifecycle Manager
- CA: CA Process Automation and Auto Suite for Cloud (ASC)
- ElasticBox: ElasticBox Enterprise Edition

Visibility, Control, and Centralized Management

The Infoblox IPAM solution delivers centralized and unified IP address management of physical, virtual, and cloud environments. High availability ensures datacenter survivability and improves uptime. It also lowers operating costs and allows IT organizations to do more with less. The Infoblox solution is delivered through a single pane of glass for visibility across multiple datacenters, so network administrators can keep track of VMs in each datacenter, identify problems easily, and reduce MTTR. It also provides classification of VMs using metadata, which enables better tracking of resources and improves overall datacenter efficiency. Because Infoblox IPAM is part of the Infoblox Grid, it is highly available, reliable, and scalable; the data related to Infoblox integration is stored in the Grid, providing unmatched reliability by eliminating single points of failure.

Leveraging a Complete Picture

Having the complete picture of network assets lets administrators quickly and easily identify resources and answer questions on location, ownership, or whatever is important to the organization. In a graphical or list view, administrators manage these resources and can easily re-assign any attributes associated with the objects. The complete picture is much more than just IP and name: it incorporates information from virtually all organizations. By combining this disparate information, Infoblox IPAM delivers the true “complete picture.”

In Figure 10, operations information and network information are applied to the same hosts. Users can look for expiring maintenance, specific device type, and manufacturer and model information.
Having all data in a single place gives every team in the organization easy access to information. All a user have to do is enter a phrase or a description, and the IPAM system will find everything that matches the search terms. For example, a user can enter “San” in Global Search, and it will search in every available field and show everything that it finds, be it the location of a network, or a part of a hostname, a comment, or a user name.

By using Smart Folders leveraging the IPAM information, organizations can proactively find issues. For example, users can organize networks by VLAN number and usage, and use Smart Folders to visually organize them to quickly check compliance with policies such as: “All voice networks should be using VLAN 200 plus the 3rd octet of the IP” (Network 10.45.57.0 would be 200+57=257.). Figure 11 shows that one of the wireless networks in Denver is not using this company standard for VLAN assignment.

Smart Folders can also leverage IPAM information to reduce troubleshooting times. For example, a user calls the help desk to say that she’s having problems connecting to the wireless network in Denver, Colorado. The help desk staff can open Smart Folders, use the Organization to quickly see the wireless network allocated for Denver, CO is 192.168.4.0/23—click to expand the IPAM...
view, and see whether or not DHCP ranges are full, or how many active DHCP leases are out. The help desk can also switch from this view to syslog quickly to see if there are error messages from the DHCP server, or to see if the user did receive a DHCP lease, but is getting an IP conflict because another device has taken that IP address without authorization. This can also be remediated in the same place by resolving this conflict within Infoblox IPAM.

Users and Maintenance

Infoblox provides granular role-based administration at the object level, letting administrators give just the access needed so users can manage the information relevant to them. Giving users access not to zones and networks but just to specific object types allows work to be distributed to teams with oversight by more senior and core administrators. And as a central point of IPAM, administrators can safely allow read access to those groups and individuals that need quick access to information about the assets on the network, such as help-desk and support engineers. With authentication and authorization options for leveraging existing Active Directory, LDAP, RADIUS, TACACS, and OCSP, Infoblox IPAM lets administrators leverage the existing user structure with a simplified interface to map users to role-based groups. By using IPAM information, administrators can also map the assets under their control to allow these groups to do the work they are tasked to do.

By including Infoblox workflows, access can be granted to those users who are responsible for day-to-day changes while allocating the responsibility for executing changes to senior staff. Creating an approver group allows users to manage their own data, freeing up key resources to
focus on managing the network. Approvers will receive email alerts when changes are submitted and can approve changes in compliance with relevant policies.

Using the previous example, tying group permissions to IPAM makes it possible to create a group with write access (RW) to the Denver Wireless IPv4 Networks and read-only access (RO) to everything else.

The Infoblox Advantage

The Infoblox database allows for searching managed and grouped objects across all of the data and information that has been imported. By creating a single store for all the information about the network connected hosts, Infoblox provides unprecedented ease of management. Many IPAM solutions are IP-centric, but Infoblox has taken IPAM much further. Admins don’t always know the IP addresses of the assets they are looking for, and Infoblox allows users to identify assets regardless of which information is used to start the search.

Infoblox IPAM can import or integrate with the managed information from other solutions. If a spreadsheet is used to keep track of the point-of-sales devices that are deployed, Infoblox can import the data from the spreadsheet and preserve all data fields (converted to Extensible Attributes). If proprietary ERP software is used in the organization, admins can leverage the

Figure 13. Selecting an object to apply group permissions
Infoblox API to update the IPAM database when a new item is added that changes the IP address landscape. This is a good example of how a single pane of glass is utilized for all types of information about networks and clients.

Maintaining accuracy is central to a truly effective IPAM solution. With discovery functions that can monitor the network, VM-specific discovery, and Network Insight, users can be assured that the information in the Infoblox IPAM solution is up to date and accurate.

Improving Day-to-day Operations

Having an accurate and complete IPAM solution is one thing, but Infoblox has created a system designed for ease of use in both day-to-day tasks as well as troubleshooting. With a constant focus on security and usability, users will leverage IPAM information in a variety of ways to increase productivity while decreasing troubleshooting and support times.

Data Consistency

Infoblox can enforce policies on the data-entry process to ensure that as the organization grows, its IPAM data grows along with it. For example, whenever a DNS entry is being made, Infoblox can require users to provide a ticket number, email the administrative contact, and await approval from another group. Infoblox can also require that whenever an IPv6 network is being added, that users must provide information about its physical location, city of deployment, network usage, etc. To minimize user entry errors, Infoblox allows the extensible attributes to be configured as drop-down lists rather than free-form text. These enforcement policies will ensure IPAM data maintains consistent quality.

Identifying and Resolving Conflicts

Infoblox IPAM not only allocates and tracks resources, but can be configured to actively validate its own accuracy against live data on the network to identify conflicts between what is allocated and what is deployed. Infoblox can identify conflicts through network discovery, protocol data, VM discovery, or other methods. For example, an administrator may allocate three IP addresses to the Windows server team, but through various discovery methods, the administrator might see that the server team has only used two of the allocated IP addresses and took a third IP address that was not allocated to them. Another example is unauthorized use of network address space. As we saw in the Network Discovery section of this document, administrators can identify IP addresses that are currently in use but were never allocated or authorized. This could be due to misconfiguration on the server, but more importantly it could lead to network conflicts later. Infoblox IPAM helps identify and resolve these allocation conflicts.

Troubleshooting

Infoblox provides physical connectivity information through Network Insight, dramatically reducing troubleshooting time. Too often, the network connectivity information is out of date or was not kept in the first place. Network administrators may need to rely on comments in configuration files if they exist, or worse, resort to manually tracing the connection whenever an issue arises. Infoblox IPAM not only provides connectivity level information, but also other metadata that helps administrators quickly determine the nature of the problem. For example, if someone reports an IP address is generating excess network traffic, an admin can search Infoblox IPAM for the IP address and discover the switch port it is connected to, the VLAN it is on and meta-information such as that it is running embedded Windows XP, is located in Las Vegas, and is a cash register in a test environment owned by R&D.
Additional Examples
Suppose a trouble ticket is opened indicating that all Canon Model “XYZ” printers are exposed to a virus and need to be patched. In a global organization that could involve talking to four or five groups to identify where these printers are deployed and if they are still in use. With Infoblox IPAM, making a simple global search of all objects where “Manufacturer” is “Canon” and “Model” is “XYZ” returns the location and owners of the devices, enabling admins to quickly get patches on the printers.

Future Planning Enabled with the Solution

IP Space Visualization
The Infoblox map view provides quick visualization of how network allocations are being handled. With the setting of thresholds users can be alerted when DHCP ranges reach pre-set levels, allowing proactive remediation of IP allocation needs.

Figure 14. IPAM network map

IP Network Visualization
Infoblox NetMap allows you to visualize the network you have allocated and easily find room for new networks when needed. The GUI tool allows for selecting regions and allocating right from the network map. With tools to zoom and select and color codes to show utilization, Infoblox provides unprecedented ease of network allocation.

Figure 15. NetMap for viewing overall address space allocation
Summary

Infoblox provides a significant advantage for IPAM that goes beyond allocating space and assigning addresses. Infoblox IPAM manages all IP network resources and provides the means to centralize information with tools to leverage knowledge, creating efficient IT teams. Infoblox IPAM build an authoritative database of actionable information by gathering network data from protocol services, by importing data, and through network discovery and user-provided metadata. Utilizing Smart Folders, the Infoblox solution ensures the right data is quickly and easily accessed in support of adds, moves, and changes as well as troubleshooting. The solution supports the automation of virtual environments, the creation of auditable work flows, and granular, role-based administration in order to drive collaboration across IT and support teams.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.
CORPORATE HEADQUARTERS
+1.408.986.4000
+1.866.463.6256
(toll-free, U.S. and Canada)
info@infoblox.com
www.infoblox.com

EMEA HEADQUARTERS
+32.3.259.04.30
info-emea@infoblox.com

APAC HEADQUARTERS
+852.3793.3428
sales-apac@infoblox.com