

Infoblox Integrated IP Address Management Solution

**Integrated and Automated for Real-Time
Visibility, Control and Compliance**

www.infoblox.com

An Introduction to IP Address Management

IP address management (IPAM) refers to the management of allocation, administration, reporting and tracking of public and private IP space, IP devices and associated data. Enterprises typically deploy systems and processes that interact with the DNS and DHCP infrastructure in order to provide IPAM capabilities.

A majority of IT departments use manual processes, spreadsheets or home-grown tools for IP address management. A typical process for a new IP address assignment to a printer may involve several steps spanning several departments; as a result, a simple request for an IP address for a new device may require hours of work and days of elapsed time as each set of hands becomes involved in the process, with the attendant potential for introducing errors along the way.

The Infoblox IP address management solution automates and simplifies IP address management thus reducing network operating costs and eliminating configuration errors and associated downtime.

This whitepaper discusses the importance of a sophisticated IPAM solution and provides an overview of how Infoblox IPAM solution satisfies all of the key IPAM requirements for today’s organizations.

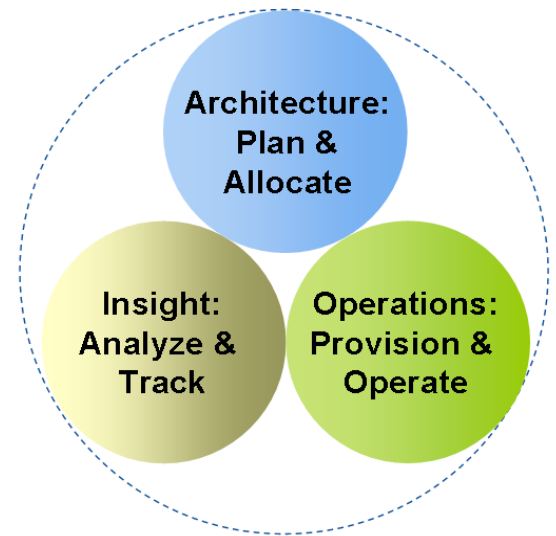


Fig 1: IPAM Lifecycle

Why Is IP Address Management Important?

The criticality of TCP/IP networks continues to increase over time. The growth in virtualization, cloud and mobile computing and the introduction of diverse IP-based devices such as IP telephones, cameras, and RFID readers means that soon virtually every business activity—from gaining access to a building to making a phone call—will be mediated by the IP network. As the networks become more dynamic, the complexity of networks increases and IP address management becomes challenging. Using manual processes and spreadsheets for IPAM is no longer adequate and leads to increased operating expenses, reduced IT flexibility, increased network outages and long troubleshooting times.

The Smoking Gun: Diseconomies of Scale Show that Today’s IPAM Processes and Tools are Obsolete

A recent survey conducted by Computer World revealed that annual costs for IPAM increase as enterprise networks grow larger. This diseconomy of scale in IPAM costs is the most clear indication that conventional solutions – be they spreadsheets, home-grown tools or 1st generation IPAM systems – cannot cope with the scale and dynamism of modern networks. The section below points out a few highlights of the challenges of conventional approaches.

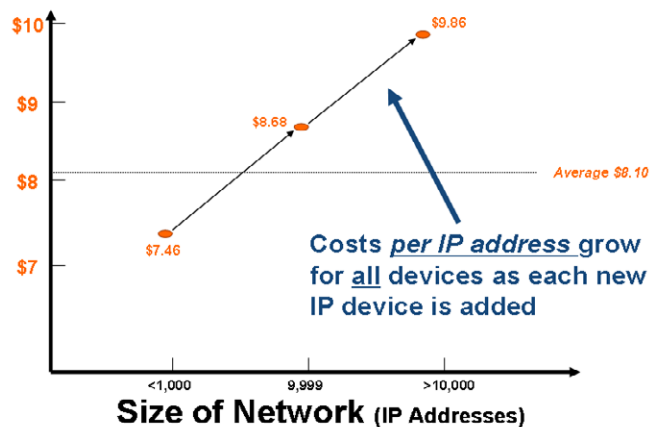


Figure 2: Results of ComputerWorld survey showing IPAM costs increase with size of network

Lack of Delegation and Workflow Management Reduces IT Organization Flexibility and Increases Turnaround Times

Manual processes associated with IPAM tasks typically require senior level expertise in operating and configuring DNS and DHCP systems as well as authority to make these changes. Due to security, accountability and compliance reasons few employees in IT are authorized to make these changes. This creates a bottleneck for IPAM requests increasing service time. In addition, senior IT staff become occupied dealing with day to day tasks taking focus away from more strategic projects. Finally, it is difficult to replace or redeploy current IPAM administrators due to the level expertise required and steep learning curve.

An effective IPAM solution allows delegation of common IPAM tasks to junior level IT employees or to the helpdesk itself while ensuring configuration integrity and security.

Configuration Errors Lack of Automated Monitoring Cause Expensive Network Outages

Even routine IPAM tasks can introduce errors and downtime if they require a large number of manual steps and require a high level of expertise to perform. In a typical environment, simply assigning an IP address to a new server can involve 3 departments and 15 independent steps. An error made at any of the steps may lead to an outage. In addition, there is no automated monitoring of these systems e.g. a DHCP range may be about to run out of IP addresses but administrators will know of it only when users start to complain about network availability and significant time is lost in troubleshooting and identifying the problem. In the meantime users have no access to network affecting business

Lack of Visibility Into DNS and DHCP Data Makes Troubleshooting Difficult

Most DNS and DHCP solutions do not provide visibility into IPAM data. Slim to nonexistent reporting capabilities make it very hard to determine causes of IP address related problems. There might be IP address conflicts in the network, unauthorized devices e.g. modems connected to corporate networks posing security risks.

Automation of IPAM reduces network operating costs and significantly and enhances network availability, allowing IT departments to focus on more strategic projects to grow the business rather than spend resources on just keeping the business running. The section below describes the Infoblox IPAM solution and highlights a number of its unique capabilities and advantages.

Lack of physical connectivity information makes networks less secure and harder to troubleshoot

Lack of a comprehensive, enterprise wide view of network port usage and end device identification leads to several challenges including -

1. Security enforcement and audits are difficult – Lack of location information for end point devices makes it hard to enforce security when an offending device is identified. In addition, there is no audit trail for where a device connects on the network. This makes it hard to investigate security incidents.
2. Troubleshooting requires locating devices manually – Troubleshooting network incidents require identifying and locating devices on the network. It is hard to assess impact on the network when a switch is taken down for maintenance. Manual locating procedures are labor intensive and may reduce IT effectiveness by increasing resolution times.

A Tour of Infoblox IPAM Capabilities

IPAM functionality is built-in to Infoblox NIOS software and includes a comprehensive suite of functions that support address allocation, management, and reporting. Unlike conventional solutions, in which IPAM is “built-on” to DNS and DHCP servers, the Infoblox solution requires no extra appliances or software and provides powerful benefits, including real-time visibility to highly dynamic IPAM data, built-in high-availability and disaster recovery, one-button software upgrades, and an interface that makes it the easiest to use and most powerful in the industry.

Web Based Graphical User Interface Simplifies Management

Infoblox IPAM capability is accessed through an intuitive web based interface called the IP Address Manager module. The Infoblox IP Address Manager module provides a visual representation of your network and its state in addition to providing a user friendly way to perform IPAM tasks in a secure manner while eliminating configuration errors. Following are a few key elements of the IP Address Manager module.

Dashboard

The IP Address Manager Dashboard is the portal to IPAM functionality that can be customized to suit an administrator's role and responsibility. Dashboard widgets are available to provide an overview of current status of the network, IP addresses, services, network discovery status etc. In addition, widgets are available to provide easy access to frequently used functions.

Widgets can be created and added to the dashboard easily, much like with iGoogle or MyYahoo. An administrator can access only those data and functions for which they have authorization, as defined per their administrative, i.e. a DHCP administrator for a regional office can get access only to regional office network data and associated functions. About 90% of everyday IPAM tasks can be performed directly from the dashboard without having to drill down to other screens.

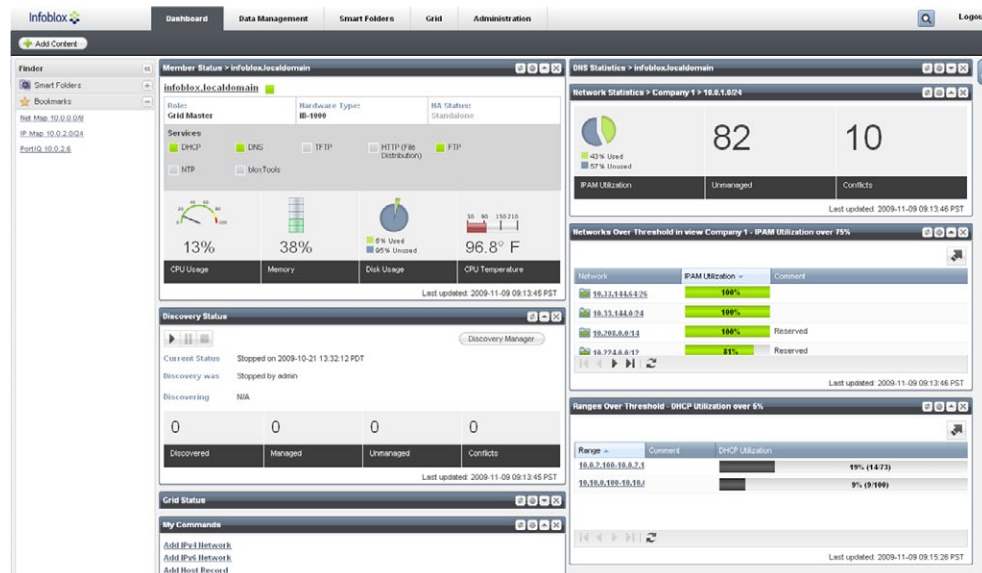


Figure 3: IP Address Manager Dashboard provides quick overview of network and access to frequent IPAM tasks

Smart Folders for Organizing IPAM Data

Smart folders provide an easy way to organize and categorize networks, similar to the way that iTunes® Dynamic Playlists make it easy to organize a constantly changing music library. In conjunction with extensible attributes that allow administrators to define and assign custom properties to objects, Smart Folders provide a powerful way to hierarchically view and manipulate IPAM data. For example, administrators may define a custom attribute called "asset-id" with syntax "devicetype-dept-xxxx" and associate this attribute with all static IP addresses. Now a Smart Folder can be created with attribute "asset-id" begins with "HP_Printer". Now to see status of all HP printers administrators have to just click on this Smart Folder. Smart Folders can be hierarchically organized, e.g. there may be a folder for all US networks containing networks for individual regional offices. Within a regional office there can be folders for different device types or any other custom attributes.

Smart Folders are dynamic in nature e.g. when a new device is added or removed from the network, it is also added to or removed from all associated smart folders automatically.

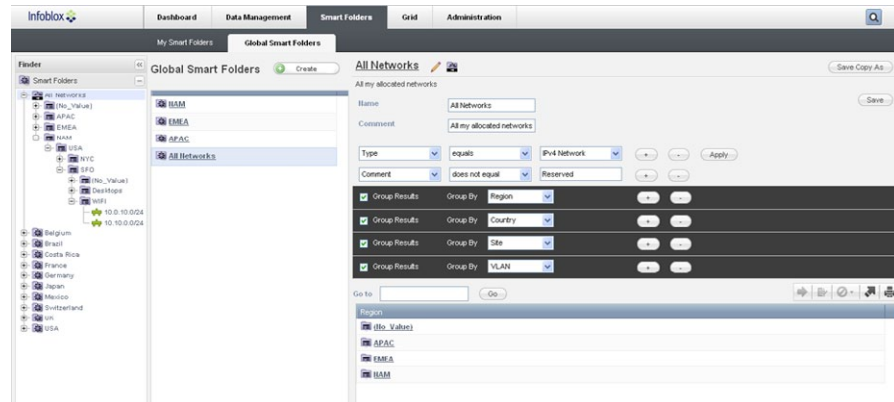


Figure 4: Smart Folders for organizing and viewing IPAM data

Net Map Makes New Network Allocation Easy

The Net Map is a patent-pending Infoblox innovation that provides a graphical depiction of the state of all defined networks within a range. A quick look at Net Map shows available and utilized networks and utilization status of each network. The Net Map also features a slider bar that can be used to allocate new networks and resize existing networks.

In addition it is also possible to directly add new networks and edit existing networks directly in the map. This allows users to create new networks faster without requiring them to do complex calculations.

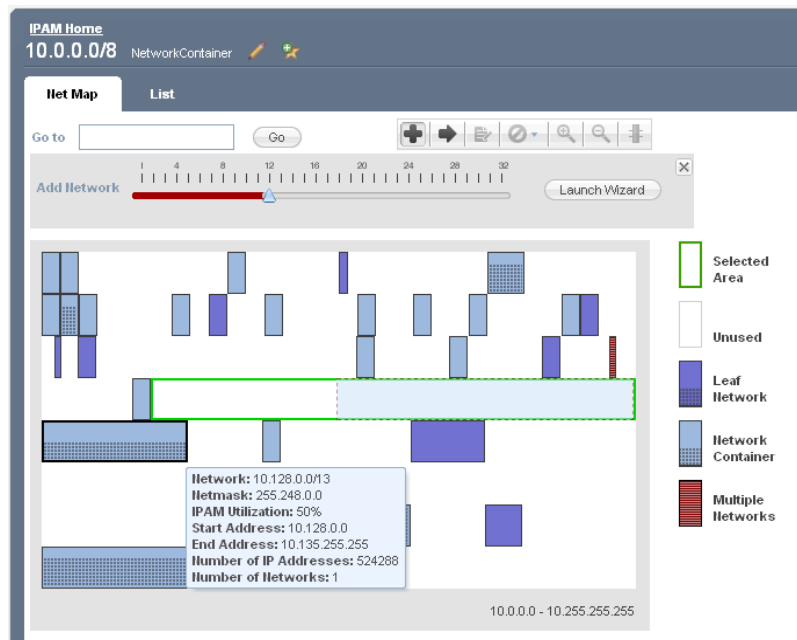


Figure 5: Net Map provides an overview of networks and allows allocation and resizing of networks

Net Map zoom in and out capability allows users to see details about small networks. This capability works similar to the zoom in and out capabilities of Google maps, where users can zoom in to see minor streets and then zoom out to get a view of the larger area. This allows users to directly see smaller networks without switching between several networks.

Network Views Supports Overlapping Address Spaces

The Infoblox IPAM system can manage two or more overlapping address ranges within the IPAM system. This is a key functionality of an IPAM system and is frequently required when managing networks created by merger and acquisition activity. During M&A activity, IT departments typically do not re-architect the whole network; therefore, if the two merging entities were using same network address ranges in their networks they end up with the same address used by multiple devices. The Infoblox IPAM system can handle this easily by using network views functionality. Using network views, administrators can keep two or more overlapping networks logically separate and still use Infoblox IPAM to manage these.

As companies expand and grow either organically or through acquisition, they need to be flexible with their DHCP networking configuration. Split/Join networks allows a company to easily adjust to the dynamic nature of today's networks. Split networks allows an administrator to quickly, easily, and accurately subdivide a network and have the resulting sub-networks inherit the configuration of the parent network. Join/Expand networks is unique in that it allows the administrator to combine smaller networks into a bigger network without losing any of the configuration including fixed addresses, dynamic ranges, etc.

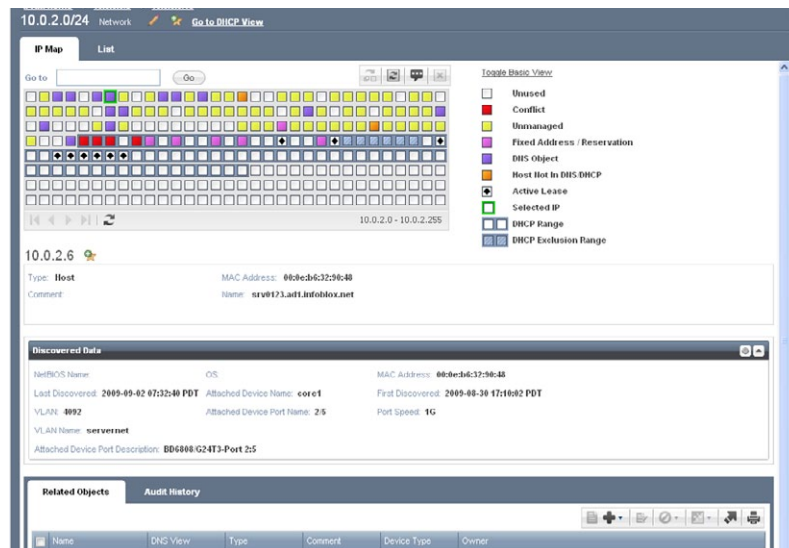


Figure 6: IP Map provides a quick view of all IPs within a range and access to IPAM functions to manipulate IP addresses

IP Map to View and Allocate IP Addresses

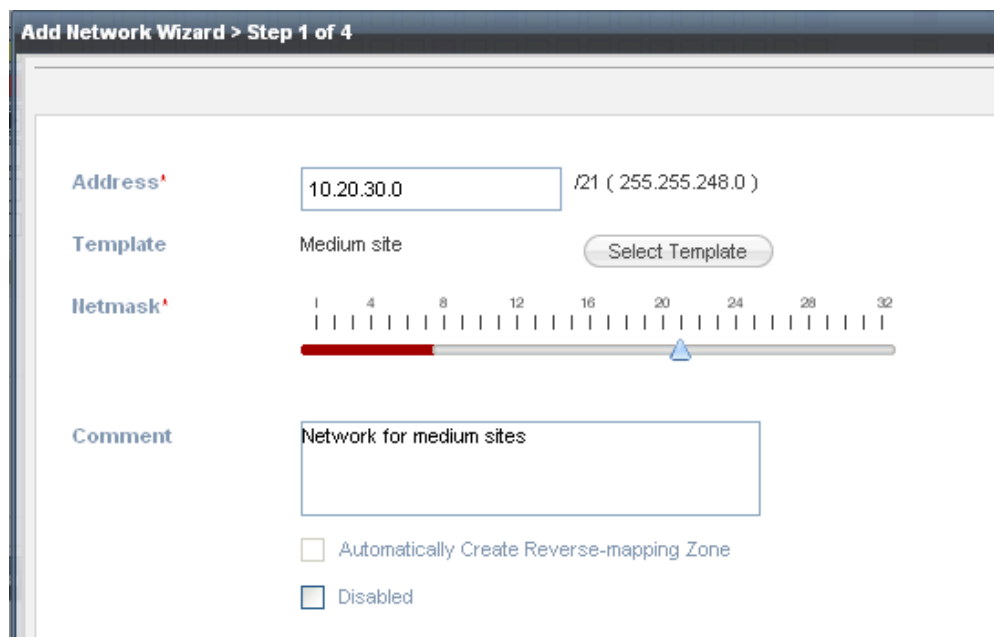
The IP Map shows status of all IP addresses within a network. Each small square in the IP Map represents one IP address. At a glance, administrators can quickly see how many addresses are free just by looking at the relative number of white boxes. Other items of interest, such as IPs that are in use but that were not provisioned in the IPAM system (yellow squares), as well as IPs that report data from network discovery scans in conflict with what's in the database, such as different MAC addresses (red squares). The visual nature of the IP Map is much more effective and efficient than the typical list or tree-view of a network. In addition, many common tasks such as IP allocation, reservation of IP addresses, adding DNS records for IP addresses and

more can be performed directly from the IP Map. The Infoblox IP Map also provides the ability to manipulate addresses and their status, such as converting a dynamically assigned DHCP lease to a DHCP fixed address or Infoblox Host object. For example, this allows administrators to deploy new devices on the network using a common workflow:

- Letting network devices such as servers, desktops, printers, and IP phones obtain IP address settings automatically using DHCP;
- Viewing the DHCP leases in the IP address management console, clicking on the entry, and then converting the lease to a DHCP fixed-address or Infoblox Host.

Wizards to Make Configuration Error Free

Common IPAM tasks can be performed easily by using simple wizards. This makes configuration error free and can be easily delegated to junior level employees not familiar with DNS, DHCP configuration. The IP Address Manager includes wizards for adding Networks, Hosts, DNS records, Reserve IP address etc.



Add Network Wizard > Step 1 of 4

Address* /21 (255.255.248.0)

Template Medium site

Netmask* (1 4 8 12 16 20 24 28 32)

Comment

Automatically Create Reverse-mapping Zone

Disabled

Figure 7: Add DHCP network wizard for easily allocating networks

Workflow with role based administration streamlines delegation of IPAM tasks

Role based administration allows alignment of real world job responsibilities of the administrators with the permissions to carry out tasks. Infoblox NIOS software allows creation of administrative roles and assignment of different administrators to these roles. An administrative role can be defined based on flexible criteria e.g. DHCP administrators in the Phoenix data center or Printer administrators worldwide etc. Once the role has been defined, administrator accounts can be added to specific roles.

IPAM features on NIOS recognize permissions associated with these roles and function accordingly e.g. if an administrator with permission to assign static IP addresses uses the “Next available IP” function in order to allocate an IP address to a printer, the IP address returned will be compliant with the permissions of the role of the administrator. Similarly, when the administrator assigns the new printer a name and IP address, host name syntax checking will be activated to ensure that the name complies with the naming rules as specified by the central administrator.

The Infoblox workflow capability allows adaptation of Infoblox IPAM in the normal workflow of IT departments. Using workflow, junior level staff members can make network configuration changes and have them automatically submitted for review by network administrators, which approve or reject the change. Approved changes are queued in holding areas, where they can get reviewed and tested before being published to the production environment. Changes can occur immediately or can be scheduled. Infoblox workflow is implemented using the highly customizable bloxTools™ framework and can be configured to suit the workflow of any IT organization. For additional description of bloxTools environment, please see the section titled “bloxTools Environment for Extending and Integrating IPAM” in this document.

Workflow and role based administration combined provide a powerful way to delegate complex IPAM tasks to other departments with technical oversight from IPAM owners. E.g. helpdesk attendees can be provided a custom interface to be able to allocate IP addresses from a given address pool with oversight from network team. And of course, all administrative changes are thoroughly logged and auditable.

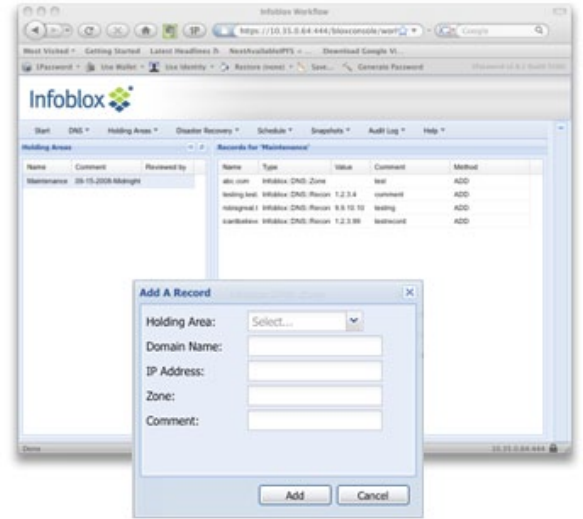


Figure 8: Infoblox IPAM workflow in action

Network Discovery to Find and Manage Devices on Your Network

Network Discovery allows administrators to search for active devices on their networks and populate the IPAM database with information discovered during the process. The discovery process gathers various pieces of information about connected devices including MAC address, NetBIOS name, operating system and last discovered time. Discovery functionality can be directly accessed from the dashboard. Discovered data is seen in the IP Map and can be directly acted on from there.

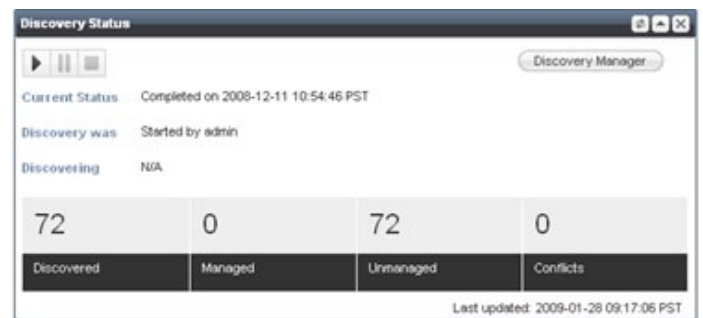


Figure 9: Network discovery widget provides status of discovery process

An administrator can take following actions upon completion of discovery:

Add new devices to the IPAM Database – Network discovery provides a quick mechanism to add unmanaged devices to the IPAM system without requiring administrators to manually input this information.

Resolve conflicts between the IPAM system and actual network state – If the IPAM system has one view of the system but the actual IP address use on the network differs from this e.g. the IPAM system shows that a fixed IP address should have a particular MAC address however in reality it has a different MAC address, a network discovery will show this as a conflict that administrators can correct.

Discover unauthorized devices on the network – Periodically, administrators will discover unauthorized devices on their network that may pose a security risk. Network discovery will show this as an unmanaged device in IPAM report.

Reclaim unused IP Addresses – The Infoblox network discovery process reports when an IP was last discovered. This information helps in determining whether an IP address can be claimed back and reused.

Find device connectivity information – The Infoblox PortIQ appliance enhances IPAM data by synchronizing additional information such as device location, switch, port, VLAN etc. into the Infoblox IPAM system. Armed with this additional information, network engineers can quickly associate an IP address with a VLAN and switch port to pinpoint trouble spots and resolve problems. This has many applications, including quickly shutting infected devices off the network when virus or worm attacks occur or quickly locating and removing an unauthorized device from the network when discovered by the Infoblox discovery process.

The PortIQ appliance associates the following information for each IP and MAC address in the Infoblox IPAM database:

Switch Name, Switch Port, Switch Description, VLAN Name, VLAN Number, Switch status, Port Speed/Duplex, Link status, First seen and Last seen times.

Infoblox network discovery functionality allows administrators to run discovery on networks from grid member appliances that are remote or may be behind firewalls. This is a distinct benefit when compared to alternatives available in the market. Additionally, Infoblox network discovery uses various techniques including ICMP, TCP and NetBIOS enabling administrators to gather IP Address, MAC Address, NetBIOS names, OS version and when an object was last seen on the network. Administrators can fully control which discovery methods are used and can easily start, pause and end the discovery process.

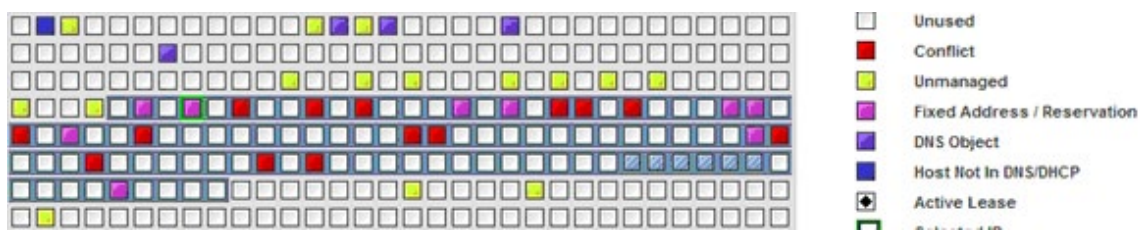


Figure 10: IP Map showing discovered IP conflicts

IPAM Monitoring and Reporting for security, compliance and troubleshooting

Accurate reporting of IP address usage is of paramount importance to maintaining an auditable, secure and outage free network. Infoblox NIOS provides an array of reporting capabilities to provide an accurate picture of current network configuration as well as historical information. In addition to smart folders and dynamic search capabilities, the following are the key reporting capabilities available in the NIOS solution.

DHCP Lease History Tracking

The Infoblox DHCP Lease History enables administrators to track and report on addresses based on a range of parameters, including IP address status (dynamic, fixed, available, and reserved/disabled), hostnames, MAC Address, and DHCP Lease information including lease date/time, time left on lease, time of last renewal, and forced release of IP address.

Lease Issue	IP Address	MAC Address	Host Name	Action	Start	Stop	Member
2009-11-19 10:17:16 PST	10.65.16.86	0e:19:51:0a:6d:e4	h18217954941426917356	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:16 PST	10.65.16.85	52:ee:4d:67:60:2f	h310132826907325911	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:16 PST	10.65.16.84	32:ba:1b:04:f7:ee	h17391776471918978266	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:16 PST	10.65.16.83	41:96:01:4a:08:36	h4650961171185198998	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:16 PST	10.65.16.82	8e:23:42:6b:99:33	h1968737911128315415	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:16 PST	10.65.16.81	d7:4c:02:9e:30:01	h18183230501737652300	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:16 PST	10.65.16.80	e9:1a:8c:78:ac:a9	h160198532825539627	Freed	2009-11-19 10:17:06 PST	2009-11-19 10:17:16 PST	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.146	1c:9a:2e:45:05:c1	h315146541257401465	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.148	62:f3:48:26:9c:06	h124438746796151058	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.151	5d:1b:d4:57:6c:45	h289614818890430842	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.157	48:f6:85:23:85:09	h16356940701204733114	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.156	54:95:68:58:e6:b2	h1747634192937775978	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.159	1d:72:a1:65:38:18	h19121236371227042523	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.158	4c:c0:c8:25:2e:b3	h19188523222110248531	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.161	02:46:b2:3c:a7:31	h12950719892085741428	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.160	28:a5:e2:23:80:93	h130139801742183155	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain
2009-11-19 10:17:12 PST	10.0.2.163	84:10:66:39:f6:ad	h1954019688180822306	Issued	2009-11-19 10:17:12 PST	2010-09-15 11:17:12 PDT	infoblox.localdomain

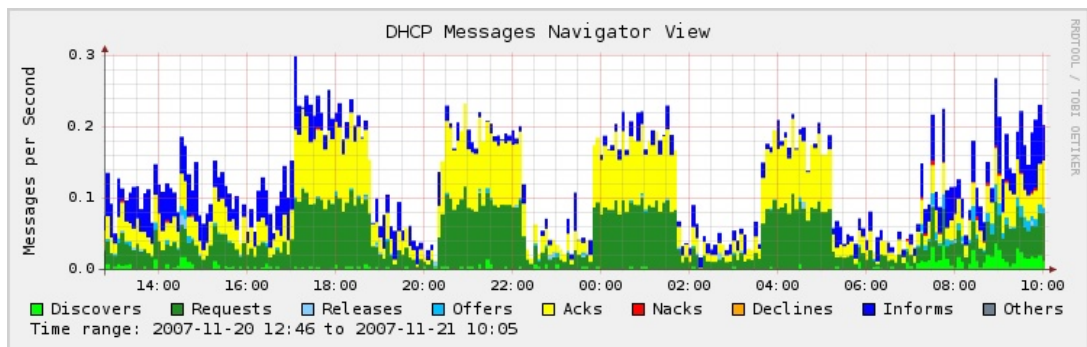
Figure 11: DHCP lease history report

Port Connection History Tacking

Using the Infoblox PortIQ™ appliance in conjunction with the IPAM database, administrators can track which switch port a device has connected to during the specified period of time. This capability is helpful in investigating security incidents.

IPAM and DNS Trends Reporting for Early Diagnosis of Problems

These two reports are very helpful in identifying potential network problems before they cause widespread impacts. In the following figure, which shows DHCP protocol activity, gaps can be seen between bursts of DHCP activity. This kind of behavior is possible if a network is experiencing periodic outages e.g. a wireless router rebooting due to some problem.



Time range: to

Figure 12: DHCP traffic report

The DNS query report below can be used to determine unusual activity e.g. DNS attacks on the network.

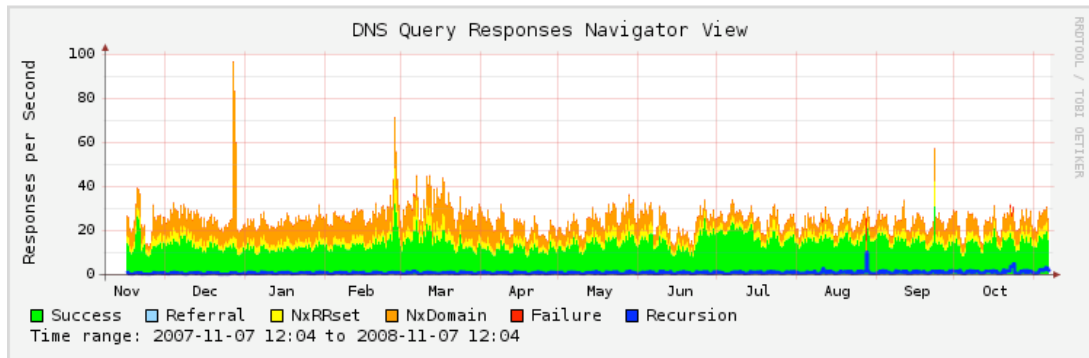


Figure 13: DNS query response trends report

Administrator Audit Reporting

A key requirement when delegating administration is the ability to track and report on changes by the administrators. All changes made by administrators are logged in a detailed centralized audit log. The audit log contains all the details of changes which can be searched and exported. Superusers can run reports on the audit log to obtain information such as: which administrator(s) made changes to a specific object and when the change was made or provide a list of all changes with dates and times and detailed change information for each administrator. This information is invaluable when performing any investigation for compliance.

IPAM Statistics Reporting and DHCP Threshold Alerts

The IPAM statistics viewer enables administrators to allocate IP address ranges more efficiently and effectively by displaying the number of static and dynamic IP addresses in use and the percent utilization for each network assigned to each Infoblox appliance.

If DHCP threshold limits are exceeded, alerts can be sent using e-mail and SNMP traps so that administrators can take preventive action, such as re-allocating networks. “Low water” thresholds are also useful for detecting network anomalies: For example, if a network that is normally fully populated with IP phones suddenly passed a low-water DHCP threshold, it would indicate that phones were not renewing their leases and that there was likely a problem with the phones or the IP telephony network.

Network	Comment	Site	VLAN	DHCP Utilization	IPAM Utilization
1.2.3.0/24				0% (0/0)	0%
10.0.1.0/24		SFO	Desktops	7% (2/28)	43%
10.0.2.0/24		SFO		20% (15/75)	59%
10.0.10.0/24	Lab	SFO	WiFi	0% (0/0)	31%
10.0.95.16/28	Reserved			0% (0/0)	0%
10.10.0.0/24		SFO	WiFi	9% (9/100)	55%
10.10.100.0/24				0% (0/0)	0%
10.16.0.0/17	Reserved			0% (0/0)	0%
10.24.0.0/18	Reserved			0% (0/0)	0%
10.24.64.0/18	Reserved			0% (0/0)	0%
10.24.128.0/18	Reserved			0% (0/0)	0%

Figure 14: DHCP pool usage report and monitoring

bloxTools™ Environment for Extending and Integrating IPAM

The Infoblox bloxTools environment enables customers to extend the capabilities of Infoblox IPAM system by providing a way to create custom applications (called Snapins) that run in a virtual environment on Infoblox appliances. Using bloxTools Snapins, customers can integrate the Infoblox IPAM system with their other IT systems if required. Additionally, the bloxTools developer community provides an array of innovative Snapins free of charge. Some examples of these community supported Snapins include, the GeoViewer, pictured below, that allows administrators to locate all of their Infoblox devices on a map and see status of these devices in real time, the Web Operator Console that provides simple, customizable, Web-based interfaces to allow delegation of day to day tasks, such as finding the next available IP and assigning it to a printer, to helpdesk or other less-skilled personnel. For more details on the bloxTools community and Snapins please visit www.bloxtools.com.

Following figure shows an example of bloxTools snapin called GeoViewer. This snapin is a mashup of IPAM data with Google maps and it shows location and connection status of Infoblox grid members on a Google map. Additionally, moving cursor above Infoblox members shows provides various reports.



Figure 15: bloxTools GeoViewer Snapin

Additional Ease of Management and Automation Features

Next Available IP

The Next Available IP feature produces the next unused IP address in a given network. This feature is extremely useful in assigning fixed IP addresses to network devices such as printers, security cameras etc. Availability of this feature reduces management effort in finding an unused IP address and assigning it to a device. Further the risk of future conflict with another device is reduced since IPAM system will not give out the same IP address for a different device.

Data Consistency Checking

The Infoblox software will automatically perform multiple levels of data consistency checking. With a “Host object,” the administrator can keep DNS forward and reverse zone records in sync to avoid inconsistent zone data. Infoblox also has a flexible hostname checking mechanism that allows administrators to develop custom templates for hostnames or choose from three defaults. The template is then applied to a zone so requirements can be customized for different zones. The software also performs data formatting checks for IP addresses and any other structured fields. Notably, the system prevents invalid data from being entered.

Shared Record Groups

Shared Record Groups (SRGs) enable administrators to create groups of DNS records and then associate these groups with multiple views and zones. When a shared record is changed, it is dynamically updated in all associated views and zones. A unique icon identifies shared records both in the shared record group view and the regular DNS zone view and a unique icon identifies any zone with shared records. Using Shared Record Groups you can simplify and expedite the administration of resource records.

Name Server Group Templates

Name Server Group Templates simplify the initial configuration and the ongoing lifecycle management of a Grid. For example, when adding a new DNS zone, it can be created, mapped to several appliances (as name servers), configured with specific zone parameters, and even have the contents imported from an existing DNS server without needing to make changes to individual appliances.

Network Templates

By using templates for networks, companies can automate and standardize the creation of DHCP configurations across their network. For example, if companies want the same configuration for each new branch or store, they can create a template that includes fixed addresses, DHCP ranges, exclusion ranges, DHCP options, and anything that can be configured for DHCP. When creating a new network, the administrator can pick a template and all the information for that network will be pre-populated according to the chosen template. Network templates can include any number of DHCP Range and DHCP Fixed Address templates.

Ranges and Fixed Address Templates

Ranges and fixed address templates further simplify DHCP administration. Users can create DHCP ranges and fixed addresses based on the pre-defined templates. This allows for a more homogenous use of IP address ranges throughout the enterprise, resulting in ease of troubleshooting network issues. For example, a standard Fixed Address template can be defined for printers with custom options and DHCP lease times. Or, a DHCP Range template can be defined for Voice Over IP phones with the correct custom DHCP options.

On-the-fly Assignment of Ownership

Using Infoblox Grid technology, administrators can select an appliance within the grid to be primary or secondary for a DNS zone or the owner of a DHCP network and range. All data are automatically replicated to the appliances that serve the data.

Summary

IP address management functions have become essential on modern corporate networks. However, the cost and complexity of traditional IPAM software has prevented many companies from deploying such solutions. Infoblox IPAM provides a complete, easy to use solution built on the strong foundation of Infoblox NIOS operating system. Using Infoblox IPAM, enterprises can significantly reduce their network operation costs and increase services availability while focusing on more strategic projects to grow the business rather than just keeping the lights on.

Appendix - A

Infoblox Core Technology Advantage

Infoblox IPAM is built on the foundation of NIOS operating system. NIOS operating system with Grid technology provides the following key advantages over other commercial IPAM systems.

Integration with DNS and DHCP Data with embedded database

Infoblox manages the IPAM data as well as the DNS and DHCP server configurations using a distributed, real-time database. The DNS and DHCP protocol servers have been enhanced to directly read and write to the database so that all data are accurate and distributed in real time.

The Infoblox bloxSDB database, stores the IP address and DNS data in a structure known as a ‘Host object’, which models devices as they would exist on a network. Other systems treat IP address/DHCP data and DNS data as two separate entities. In most cases, an IP device has a hostname, IP address, MAC address, and may also have alias names for easier naming access. In order to identify devices by names instead of IP addresses—or to identify a device name by an IP address—DNS forward records (A records) and DNS reverse records (PTR records) are configured on DNS servers. Furthermore, DHCP fixed addresses that are tied to a specific device are configured to always receive the same IP address based on the device MAC address. Since all this information is related to a single device, it is inefficient to designate the information that defines a unique IP address in multiple records. Doing so can lead to errors when the information stored in one record is modified but corresponding information stored in other records is not—such as may occur when dynamic DNS updates are allowed from clients on the network. The Infoblox Host object combines all the information about a single device into a single record, so all elements related to the object stay in sync.

The Infoblox database creates a true representation of a host device. Instead of maintaining separate configurations where information is duplicated in DNS, DHCP, and IPAM device classifications, entries are only added once. This enables derived records, such as A, CNAME, and PTR records to be generated and maintained automatically by the system. When queried from DNS or DHCP, the database supplies the answer for the queried object by building it from the information in the Host model. This prevents any chance for data inconsistencies that occur when different instances of the same data are out of synch.

Seamless Software Upgrades

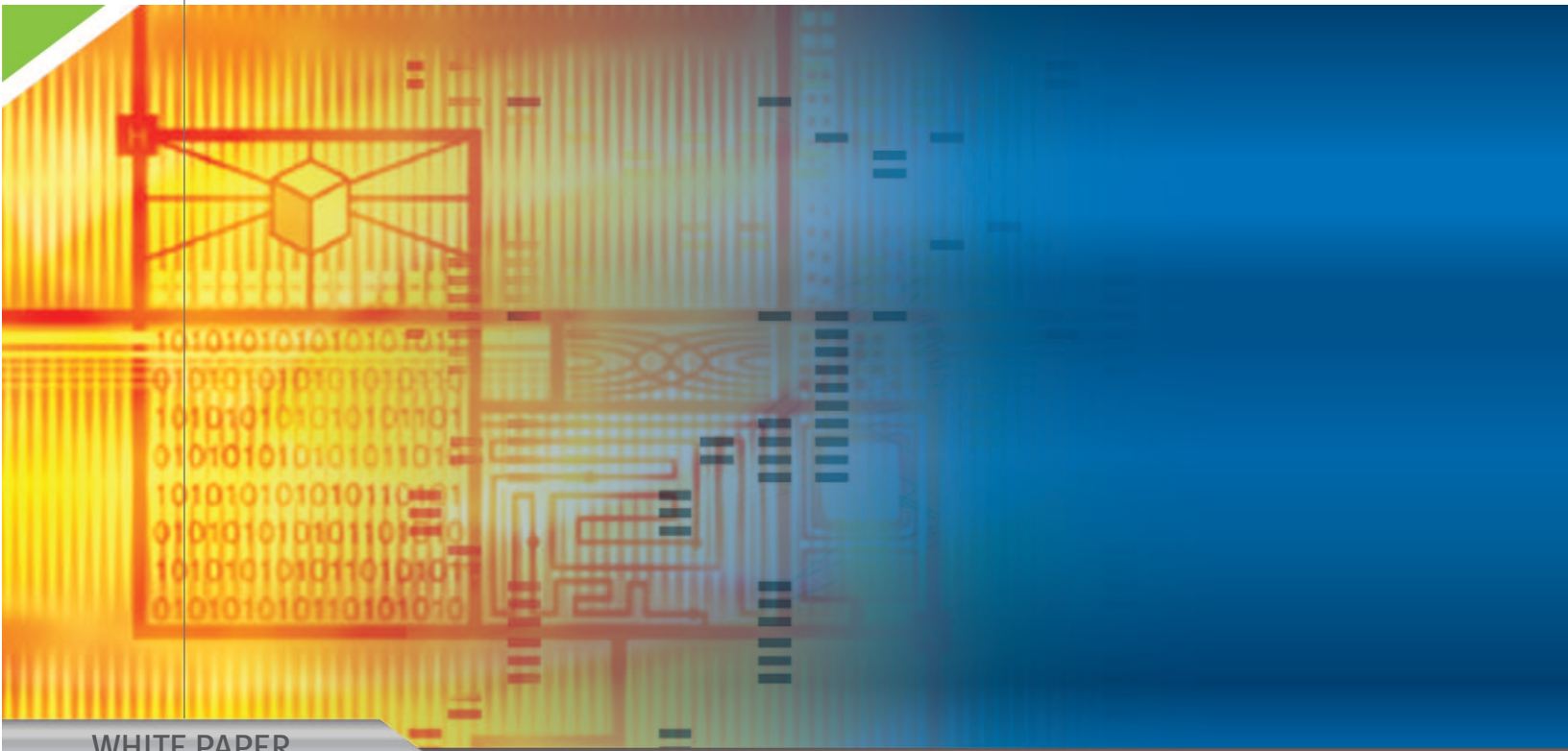
The upgrade process can be the “Achilles heel” of any large IT system. Upgrading some IPAM systems is a complex process that can involve upgrading the overlay IPAM application, the database, the server OS, the remote agent, and the DNS/DHCP server software. Upgrading all of these software components requires verifying that each specific version of each component is compatible. It also requires that the organization have access to all systems with the appropriate permissions to perform the upgrade. This can be daunting if the company has tens or hundreds of servers. In fact, because the upgrade process is so complex, some customers become stuck at the same release of software for years.

Inability to upgrade IPAM system and associated core network services devices may lead to security issues.

Infoblox appliances can be updated grid-wide to a new release of software with a simple two-step operation that distributes the code and then upgrades. It is also possible to roll-back appliances to prior releases, and to centrally backup and restore all data and configurations across an Infoblox grid.

Reliable Data Backup, Restore, and Disaster Recovery

IPAM data in Infoblox grids is exactly the same data being served in the network at any given time. In addition, the backup devices in Infoblox grids, known as “master candidates,” always contain an exact replica of the authoritative data on the grid master. A failover to a disaster recovery site simply involves “promoting” a master candidate to become the grid master. Member appliances automatically “re-home” to the new master with none of the manual, client-side intervention required with conventional systems. The process takes seconds, synchronization is nearly immediate, and services continue to run on remote servers at all times. This unique, nonstop approach to real-time data backup and restore and seamless failover enables Infoblox to provide the fastest time-to-recovery of any system available. Locally, Infoblox appliances can be configured in high-availability (HA) pairs to ensure continued service delivery even if an appliance should fail.



WHITE PAPER

For More Information:
+1.408.625.4200
1.866.463.6256
(toll-free, U.S. and Canada)
info@infoblox.com
www.infoblox.com