BLUECAT

Network Intelligence

A New Approach to Network and Device Management

Introduction

"The network has become an intrinsic and essential component of the IT infrastructure. Almost all enterprise applications and, thus, business processes are supported by the enterprise network."

Gartner Inc.,
"Key Issues for Communications Enterprise Strategies," Bjarne Munch and David A. Willis,
3 March 2011

There is a growing recognition that the best-connected business wins and that the network is the key to gaining real competitive advantage. To enable the always-on application access and connectivity that business now demands, you need a rock-solid network foundation. Organizations can no longer afford to dismiss their networks as simply "the plumbing." How organizations manage their networks, Internet Protocol (IP) address space and core network services has never been more critical.

The increasingly complex, dynamic and fluid relationship between networks and devices (both physical and logical) requires a new approach to IP Address Management (IPAM) – one that unifies device and network management in order to provide network intelligence and a broad span of control. Every new device your employees, contractors and guests want to connect to your network requires at least one IP address. Decades-old IPAM practices and basic tools are insufficient to keep pace with current network demands, exposing businesses to risk and impeding their growth.

The impact of outdated IPAM can be felt across the enterprise – from the front office, where desktop security teams struggle with "bring your own device" (BYOD) initiatives to the data center, where network operations and IT are focused on making the most of investments in virtualization and private clouds.

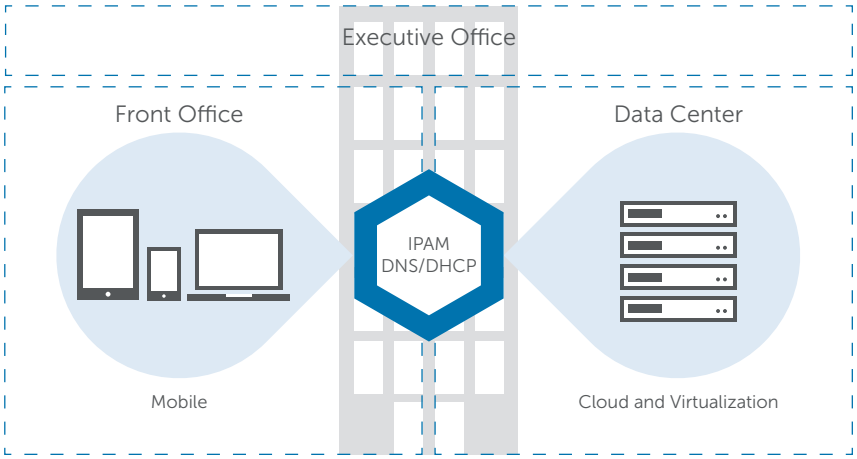

Figure 1: IPAM brings benefits in both the front office and the data center, including the ability to increase agility and realize higher returns from mobile security, virtualization and cloud investments.

Network Intelligence – The "IP" is the Key

IP address space has become an increasingly valuable financial asset that must be effectively managed. In 2011, Microsoft paid Nortel $7.5M for 667 thousand IPv4 addresses – that's $11.25 per IPv4 address (Network World, March 2011). Computerworld estimates that prices of IPv4 addresses may reach at least $70 per address (Computerworld, March 4, 2013).

The network touches everything – and no device with an IP address gets on or off the network without IPAM. This makes the IPAM platform the network intelligence authority that holds the unique and critical data relationships between IP addresses, devices, users, physical location and network activity.

The IP address is a unique network identifier assigned to each and every device on your network. As such, your IP address space holds enormous strategic value. The ability to centrally view and manage your IP addresses with IPAM is the key to gaining network intelligence and insight. The rich source of network intelligence afforded by IPAM is essential for policy enforcement and to monitor which applications are being accessed, by whom, and how your sensitive business data is being used.

Together with the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) core network services, IPAM is the lifeblood of your network:

- IPAM centrally manages and controls the network and addressing
- DNS connects any device to any Web site, application or other user
- DHCP provisions each device's connection to the network

The IPAM platform consolidates all IPAM, DNS and DHCP data within a central network intelligence repository, enabling you to better manage your networks and devices. This white paper discusses the need for more intelligent IPAM and why organizations must rethink their address management strategies. To meet ever-rising expectations for business connectivity, your IPAM platform must deliver three key solutions:

- Mobile security
- Address management
- Automation and self-service

Without these three solutions, your business will not be able to gain the network intelligence required for successful network-dependent initiatives like BYOD, virtualization and cloud – much less take advantage of emerging technologies like machine-to-machine (M2M) and software-defined networking (SDN).

We will also look at the strategic value of BlueCat's fully automated IPAM platform. Deployed at some of the most demanding and secure organizations in the world, BlueCat's innovative, market-leading IPAM solutions provide actionable network intelligence and a single point of control for all connected devices.

The Way Businesses Connect Has Changed

"Cloud, virtualization, M2M and BYOD will crush traditional IP management."

Andre Kindness,
Principal Analyst, Infrastructure & Operations, Forrester Research, Inc.

Over the last 10-15 years, the demand for IP addresses has increased dramatically and this trend shows no signs of slowing.

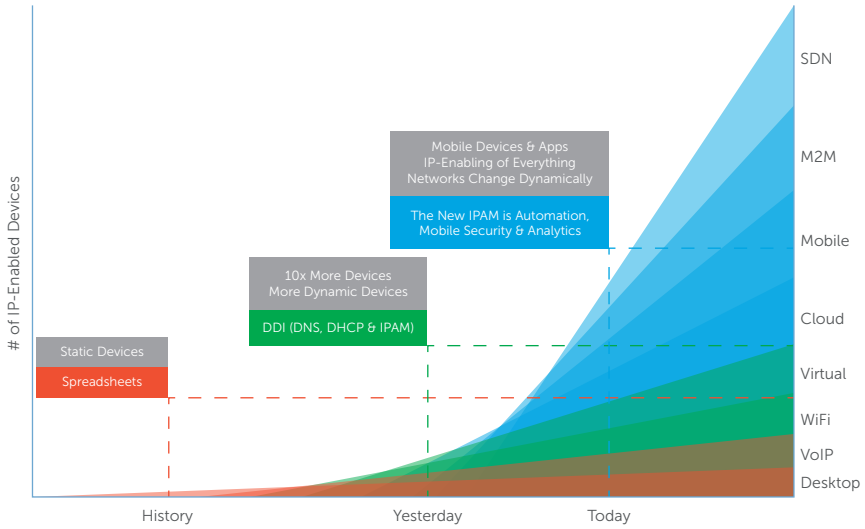

Figure 2: The network is growing steadily more complex and dynamic.

Explosive Growth of Mobile Devices

In the early 2000s, the majority of devices accessing the network were static. Desktop PCs and VoIP phones didn't move around. Wi-Fi was slow, so most laptop computers connected via Ethernet. IP addressing was relatively simple and even larger organizations could manage IP addresses and DNS for machine naming manually with spreadsheets or homegrown solutions.

Around 2005, we start to see an exponential increase in the number of network-dependent devices, due primarily to the influx of corporate-owned smart phones. This is the beginning of the mobility movement. In the data center, virtualization was expanding rapidly, contributing to the growth and dynamism of the network. Organizations realized that they needed IP Address Management tools to cope.

"In 2013, IT organizations can no longer postpone the creation of a mobile enterprise strategy that addresses data leakage, BYOD, multiple device ownership, file sharing and synchronization, safe data disposal, corporate app stores, app management and other mobility issues."

Gartner, Inc.
"Agenda Overview for Mobile Infrastructure and Operations, 2013," Leif-Olof Wallin, 2 January 2013

A More Dynamic and Complex Network Infrastructure

Today, the pace of change continues to accelerate. Almost everything is now network-dependent and dynamic – the infrastructure itself is a moving target. Virtual infrastructure now moves among networks and data centers. Winning organizations, looking for the next wave of benefits, are transitioning their virtual infrastructure to a self-service private cloud in order to increase agility and accelerate time-to-market for new products and services. In meeting rooms, tablets are replacing laptops and "bring your own device" (BYOD) has become an unstoppable trend.

Whereas managing IP addresses and names using spreadsheets, scripts and manual processes might have worked in the past, outdated IPAM processes and basic tools are completely unsustainable today.

Network Management Pains

The lack of an effective, automated network infrastructure can have serious implications for your business:

- High-profile service outages caused by IP address conflicts and network configuration errors
- Lack of visibility into IP address usage and configuration creates network blind spots that increase security risks and compliance costs
- Inadequate or piecemeal automation hampers virtualization and cloud agility and erodes ROI
- A fundamental disconnect between mobile security for BYOD and network access control leads to security breaches and data loss
- Overly complex device on-boarding processes cause users to circumvent BYOD security policies, increasing risk
- Manual processes consume IT resources, time and effort better spent on more strategic initiatives
- Inability to effectively delegate network configuration workflow to staff or the helpdesk slows IT responsiveness
- Failure to integrate IPAM with self-service portals creates IT bottlenecks in provisioning new virtual and physical devices
- An incomplete or fragmented view of IPv4 networks increases IPv6 migration risks

These common network management pains can be costly, both in terms of unnecessary IT and infrastructure expenditures and subpar returns on technology investments, but also in lost business opportunities, squandered competitive advantage and slow time to market. Many organizations have learned the hard way that these management issues are impossible to overcome with their current IPAM solutions, which lack the intelligence needed to meet current and future business demands.

IPAM is Now Business-Critical

Without an effective IPAM, DNS and DHCP infrastructure, your network cannot operate. When DNS and DHCP core network services fail, business stops. Web sites are unreachable, laptops cannot access corporate applications and services, critical applications including e-mail, ERP, CRM and VoIP cannot function and users cannot find virtual machines and cloud services.

By replacing legacy IPAM solutions and manual processes with a reliable and fully automated IPAM infrastructure, you can improve core services reliability, increase IT efficiency and better respond to business demands for always-on application access and business connectivity.

Managing "Everything IP"

Situated at the heart of the network, the BlueCat IPAM platform is a central control point. BlueCat delivers actionable network intelligence that enables you to better manage every network-connected device across your organization – all from a single platform. We accomplish this by providing a unified approach to mobile security, address management, automation and self-service:

Mobile Security – Manage the explosive growth of network-dependent devices including corporate-owned and personal consumer devices and reduce the risks of BYOD by automating device on-boarding and securing both the network and devices.

Address Management – Centrally manage everything on the network and gain visibility, insight and actionable intelligence on IP address space, networks, hostnames, devices and core network services – all from a multi-tenant Web-based interface.

Automation and Self-Service – Allow IT to be more responsive to the needs of the business by integrating IPAM into existing IT processes and workflow and enabling efficient self-service. The combination of automation and self-service lessens the IT burden of managing routine IPAM changes and dramatically reduces the turnaround time for critical network requests from days to minutes.

In the following sections, we will look at why and how mobile security, address management, automation and self-service are essential to deliver the agility and security that business now demands. We will also discuss in more detail how BlueCat provides network intelligence and a broad span of control.

Mobile Security

"In a business setting, treat all mobile devices with due care as work platforms, irrespective of who owns them or the choice of operating system, screen size, or personal and fashion appeal."

Gartner, Inc.
"Top Seven Failures in Mobile Device Security,"
John Girard,
14 February 2013

An increasingly sophisticated consumer who wants to be "always-on" and connected is driving the growth of mobile device usage and BYOD. Winning organizations can harness this change to drive real competitive advantage. By empowering your employees to work wherever and whenever they are needed, you increase the responsiveness of your business and are better able to serve your customers.

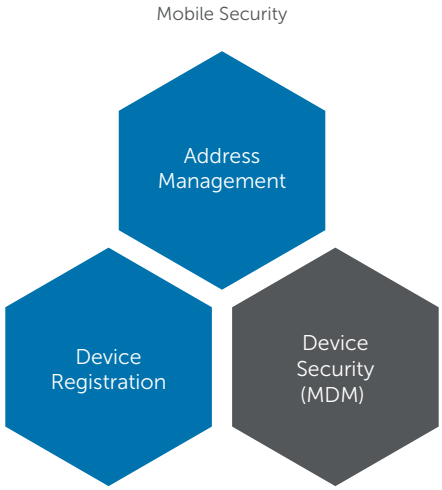

Figure 4: BlueCat Mobile Security ties device registration to address management. When coupled with an end-point Mobile Device Management Solution (MDM), BlueCat provides a broad span of control for mobile security without gaps.

However, BYOD is both an opportunity and a risk. Your organization is faced with the challenge of maintaining security and data privacy over devices that you neither own nor fully control. BYOD requires a new way of thinking about mobile security and network access:

- Mobile devices can be lost or stolen – along with the data they contain
- Malware outbreaks are increasing in both frequency and severity and mobile devices will be used to spread these software infections
- Malicious attempts to steal intellectual property and data often leverage uncontrolled DNS as an entry point
- High profile security and privacy breaches erode customer loyalty
- Unknown or "rogue" devices on your network expose your organization and data to risk
- The costs of security compliance and auditing are rising

In the past, most employees worked in the office using a company-issued device. Organizations could focus their network security strategy on protecting the perimeter. The devices themselves were also easier to manage: hardware refresh cycles for corporate-owned devices were much longer than with consumer devices today and organizations could standardize on a single operating system and device hardware type.

Today, the "work anywhere" movement means there is no defined perimeter to protect. On top of this, BYOD brings an influx of different device types and operating systems including Android, iOS, Windows Phone, Surface and BlackBerry, creating a more diverse and complex threat environment. With BYOD, you must assume that devices will become infected with malware or viruses. To empower your mobile workforce without compromising security, you need:

- Visibility and control of all devices including laptops, smart phones and tablets used by employees, contractors and guests
- A way to only allow network access to secured, policy-compliant devices
- A way to rapidly quarantine unsecured or infected devices to prevent security problems from spreading

Most BYOD initiatives focus on the end-point, securing the device with a mobile device management (MDM) solution, but this alone can still permit users to access the network and sensitive data – even from a device that has been marked as non-compliant with your security policies. To avoid gaps in control, a complete security strategy must integrate both network and mobile security. With BlueCat, network access is tied to mobile security and compliance, so that you can:

- Enforce a security policy for all devices (corporate-owned, BYOD, etc.)
- Prevent connections to the corporate network from unsecured devices
- Provide intuitive self-service registration of personal devices for simple, secure BYOD
- Perform analysis and quarantine devices that are infected, non-compliant or that represent a security breach

When used in conjunction with an MDM solution, BlueCat addresses the two key challenges of mobile security and BYOD: how to tie network access to mobile security status and how to quickly and easily get personal devices onto and off of the network.

Self-Service BYOD Registration

If your BYOD security measures become too onerous and negatively impact the user experience, users will find a way to circumvent them. The security process must be as simple and familiar as connecting a device to a hotel Wi-Fi network.

BlueCat provides the only complete mobile security solution that doesn't require heavy lifting by users or IT. With BlueCat, users and guests attempting to access your network with an unknown device are automatically redirected to an intuitive self-service portal that allows them to register their own devices. Behind the scenes, a mobile device profile is used to ensure that the device is compliant with your security policies. The user experiences immediate access to the network, while IT gains the peace-of-mind that network access and mobile security are inextricably intertwined.

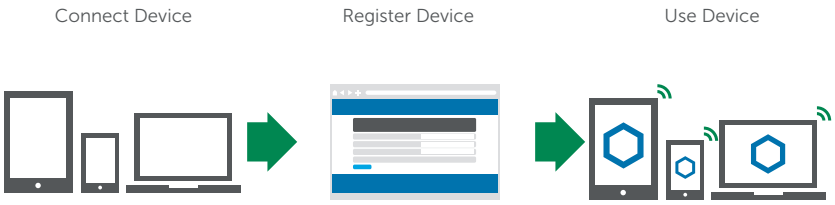

Figure 5: Self-service device registration and IPAM ensure that the mobile user experience is fast, simple and secure.

With a lightweight registration mechanism, intervention by IT staff to provision personal devices is unnecessary. Users are authenticated based on their existing network credentials. Unknown users are simply given guest access to the Internet according to pre-defined restrictions set by the administrator.

Secure Mobile Connectivity and Compliance

In evaluating security, context is king. The BlueCat IPAM platform holds the vital connection between:

Users	Corporate employee or authorized contractor
Devices	Smartphones, tablets, laptops or any other network-connected device
IP Addresses	Even for devices that might have multiple addresses
Network Location	Including the Wireless Access Point to which the device is attached
Device Name	Allows for simple end-user identification

These data points are interconnected within the Address Management solution so that they can be used to cross-correlate with the Mobile Device Manager's security policy. This results in a richer and more complete view of the security posture of all devices on the network and provides instant control over network access, application access and device quarantining.

Real-time and historical monitoring provides information on which users are on the network, what devices they are using and what they are doing with those devices. A searchable audit trail allows administrators to rapidly determine whether users are complying with your organization's code of conduct. If they are not, users and devices can be removed or blacklisted from the network with a single click. With BlueCat, you can quickly and efficiently find offending users or devices and accelerate security response.

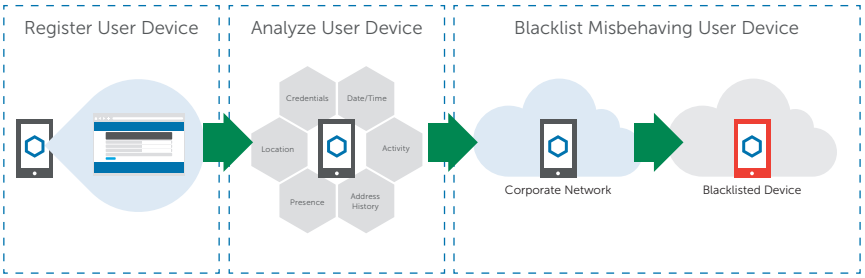

Figure 6: The network security afforded by BYOD registration and IPAM delivers accelerated security response in three easy steps.

"Having a single management console instead of a separate console in each location has tremendous advantages in terms of efficiency and making things easier for our staff. It's like having a cockpit heads-up display for all network-related topics and tasks."

Markus Vetter,
System Administrator,
TYROLIT, A Company of the SWAROVSKI Group

Address Management

Address management provides centralized visibility and control of "everything IP" including IP addresses and core network services. BlueCat's Address Management solution reduces network administration time by as much as 80% by enabling you to quickly and easily manage, track and assign IP addresses, networks and hostnames – all from a single Web-based interface. But the benefits extend beyond merely simplifying network management.

As a central control point, IPAM provides an authoritative source for information about the network, allowing you to capture the network intelligence you need to answer the "who, what, where and when" questions and quickly make informed management and security decisions. This intelligence extends across wired and wireless networks, virtual environments and mobile end points, and encompasses DHCP scopes, IP address utilization, DNS host records, zones, subzones and devices, to provide a comprehensive span of control.

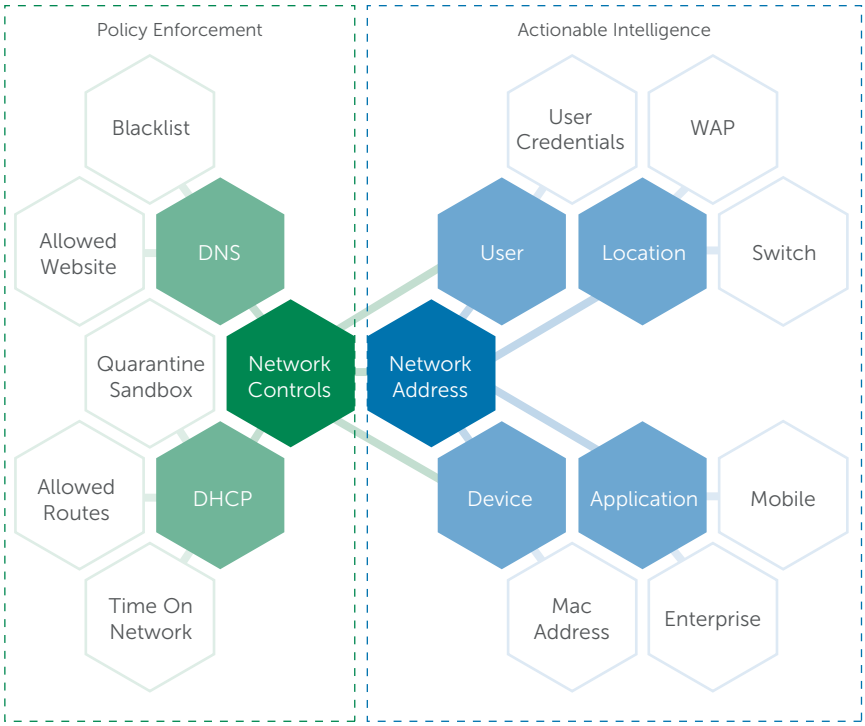

Figure 7: IPAM provides actionable network intelligence and control by tying the IP address to the user, physical location, applications being accessed and data being used.

To deliver actionable network intelligence and complete visibility and control over all aspects of your network and core services infrastructure, your IPAM solution must provide two key capabilities: automatic network discovery and network reconciliation.

Network Discovery

Automatic network discovery retrieves key information directly from routers and switches, enabling the IPAM solution to automatically augment its own data, which already includes the device's unique MAC address, IPv4/IPv6 addresses and DNS records, with valuable network-sourced data. Information such as switch port data can be appended to the IP address stored within the IPAM repository to provide a richer source of network intelligence.

With network discovery, you can quickly and easily identify changes to connected devices across geographically dispersed networks and find IP addresses that have been newly added and/or recently removed from the network.

Network Reconciliation

Network reconciliation makes the data captured through network discovery actionable, allowing you to better monitor and control devices, IP addresses, names and locations. Changes to discovered IPv4/IPv6 data can be compared in order to identify unused IP addresses for reclamation and/or unauthorized IP addresses that can create security vulnerabilities, such as non-compliant ad hoc wireless access points set up by employees.

Network reconciliation also identifies conflicts based on DNS hostname and device MAC address, allowing you to accept or investigate changes in your infrastructure. Your IP address space is a valuable business asset and with supplies of IPv4 addresses dwindling, organizations have begun buying additional IPv4 address space on the open market. BlueCat allows you to make the most of your IP address space by reclaiming unused network space to support growth. BlueCat makes it easy to define reconciliation policies and automate the entire network reconciliation process. Unauthorized or unused IP addresses can be put back into the pool of available addresses for reuse, saving you time and effort while introducing robust policy control.

All of BlueCat's sophisticated network intelligence capabilities including discovery and reconciliation can be integrated with your existing systems via a Web Services API for trouble ticketing, automation and asset/configuration tracking. In the next section, we'll look at how BlueCat goes a step further by providing a unique automation and self-service solution that makes integrating IPAM with your existing IT systems as easy as drag and drop.

"Each network change simply takes much less time with BlueCat.... The ability to centrally view and manage 'everything IP' using BlueCat has resulted in huge time and cost savings."

Martin Hierling,
Dipl.-Ing.
Hochschule Ostwestfalen-Lippe

Automation and Self-Service

Business users now demand immediate response for common IT requests such as on-boarding a new mobile device, spinning up a new virtual machine (VM), provisioning a new server, or launching a new application. IT must manage an ever-growing volume of network change requests, while at the same time trying to keep up with the need for speed.

In order for network operations to move at the speed of business, routine DNS, DHCP and IPAM tasks must be automated. The challenge is that these network changes are only the beginning in a chain of tasks needed to complete the full IT request – and each manual handoff in the chain lengthens turnaround times. Only by automating the entire end-to-end process and integrating with best-of-breed systems like virtual infrastructure, asset management, ticketing, MDM and Network Change and Configuration Management (NCCM) can IT deliver the rapid turnaround times that business demands.

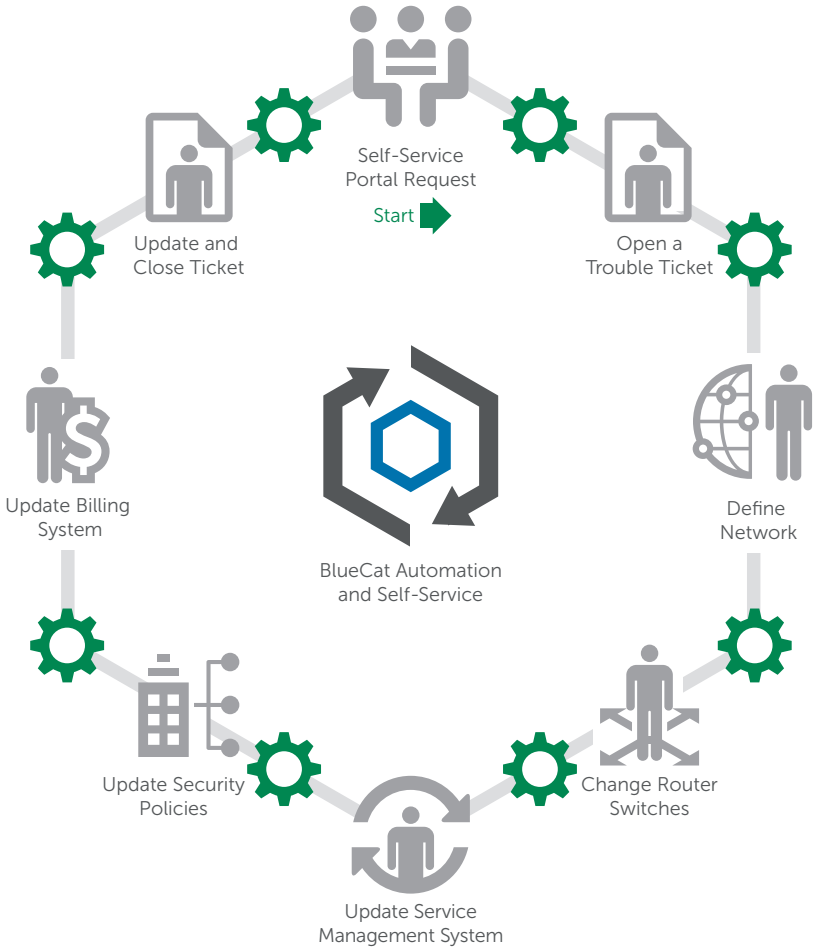

Figure 8: BlueCat Automation and Self-Service accelerates IT response times for fulfilling requests by automating the interactions between people, processes and applications.

The BlueCat IPAM platform includes a flexible and extensible automation and self-service solution that can be tailored to your existing tools and processes to deliver immediate value with no staff retraining required. The BlueCat solution can be used to streamline network operations and automate a broad range of everyday IT tasks:

- Create or teardown a virtual environment
- Self-provision a new workload in the cloud
- Self-register and onboard a new personal device (BYOD)
- Provision a new server
- Create a new application environment
- Provision a new branch office or retail location
- Update and synchronize IT requests and tickets between systems
- Assign and delegate network configuration workflow
- Configure and set IP addresses and ranges

Automation and self-service allows organizations to complete critical network requests instantaneously. Non-technical business users can request IT changes via an easy-to-use self-service portal and ensure that those requests are complete and validated.

In addition to eliminating repetitive tasks and busywork that can bog down IT staff, automation and self-service makes your network infrastructure more reliable by connecting the IT tools you are using today to the centralized IPAM data needed to validate network changes. This dramatically reduces the likelihood of manual network configuration errors that can disrupt services.

While the potential applications of the BlueCat automation and self-service solution are practically unlimited, below we'll drill down into a couple of the most common use cases where BlueCat can deliver immediate value: virtualization and cloud automation.

Virtual Automation

Today's dynamic virtual environments have placed an enormous strain on IT. With virtualization, it is possible to stand up a new virtual server in minutes, but this is of no benefit if it still takes days for IT to manually look up an IP address to give to the virtual server, update their spreadsheet and create a new DNS record. Ineffective automation and manual IP address management can impede performance and add to the cost of every virtual machine's lifecycle.

Virtualization also brings new security and compliance challenges. Many organizations lack visibility into how the virtual infrastructure is using networks and IP address space. As virtualization is used for more and more workloads, this lack of visibility becomes a serious risk for both service outages and compliance breaches.

BlueCat includes a connector that links VMware directly to IPAM so that each request for a new VM calls the IPAM solution and automatically provisions the correct IP address and DNS name. The solution can provision IP addresses and DNS names for VMs with multiple network interfaces (NICs), as well provision multiple VMs simultaneously to reduce manual intervention and increase agility.

To ensure security, reliability and continuity of service, you can access real-time network usage statistics to ensure that your virtual environment is never at risk of running out of IP addresses.

The BlueCat automation and self-service solution brings real agility, visibility and control to your virtual environment. BlueCat accelerates the allocation of an IP address and DNS name to every workload. Central visibility for all provisioned VMs prevents outages caused by accidental addressing conflicts or networks that have run out of free address space. It also simplifies compliance audits by holding detailed address and naming information on all devices, physical or virtual, in the central IPAM system.

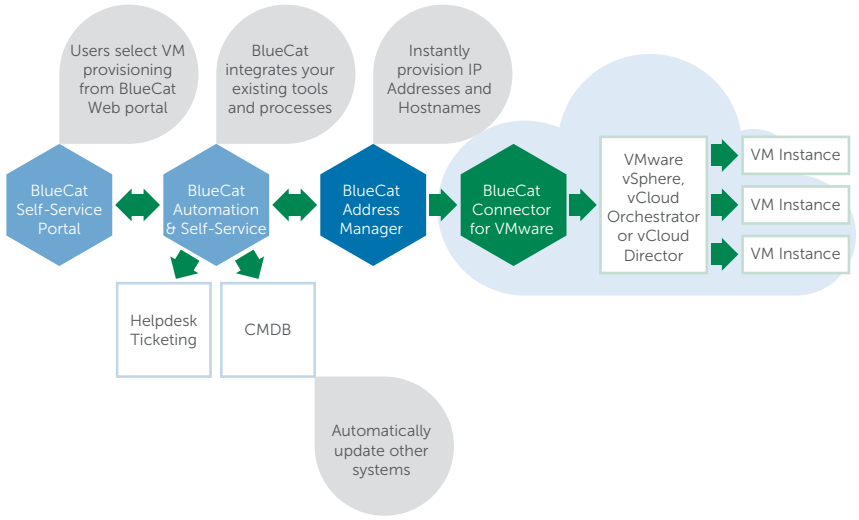

Figure 9: IPAM increases agility in the virtual data center by providing end-to-end automation of the entire workload lifecycle from activation to retirement.

By automating and accelerating the workload lifecycle, BlueCat makes managing virtual environments more stable, agile and efficient. IPAM eliminates the need for error-prone and time-consuming spreadsheet lookups and manual updates to core services. With this level of automation and integration of IPAM into the service request system, organizations can effectively realize the full advantages of virtualization.

Cloud Automation

"Cloud computing will hasten the use of tools and automation in IT services as the new paradigm brings with it self-service, automated provisioning and metering, etc., to deliver industrialized services with the potential to transform the industry from a high-touch custom environment to one characterized by automated delivery of IT services."

Gartner, Inc.
"Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency,"
November 2010

As you expand your use of virtualization, moving to the cloud is a natural next step. BlueCat makes moving from a virtual environment to a self-service private cloud a simple operation.

Private clouds are heavily dependent on the availability of IP addresses and core services. To improve the user experience and quality of service from your cloud, all of the automated provisioning capabilities discussed above must be extended directly to users via self-service.

BlueCat provides a simple and secure self-service Web portal that empowers users to rapidly self-provision a new cloud service. The self-service portal can be fully customized and easily branded to your organization's look and feel. You can also provide region-specific workflows and language in line with local regulations and regional business needs.

If you already have a self-service portal, BlueCat's automation and self-service solution can simplify the task of connecting it to your various network systems– allowing you to quickly automate the entire end-to-end cloud provisioning and de-provisioning process.

One of the most common reasons private clouds fail is that the underlying IP address infrastructure is unable to accommodate an unforeseen spike in demand. BlueCat mitigates the risk of cloud service outages by providing visibility into, and real-time control over, network usage. You can establish a low and high watermark for IP address utilization and the BlueCat solution will automatically notify you when it is crossed.

BlueCat delivers "on demand" scalability by allowing you to quickly find the next available network, apply a pre-configured template to it and deploy it to a DHCP server in a matter of seconds. The solution provides the ability for one network to easily overflow onto another in order to avoid service outages or disruptions caused by a lack of IP addresses.

The Next Generation Network will run on IPv6

"Looking ahead, IPv6 will be the next big challenge for us. Having a central repository of all IP address information means that we are much better prepared for the inevitable transition to IPv6."

Markus Vetter,
System Administrator,
TYROLIT, A Company of
the SWAROVSKI Group

The transition to IPv6 is another looming driver for smarter IPAM. The enormous growth of networks and connected devices has already depleted the limited pool of IPv4 address space in several regions of the world and global reserves are rapidly declining.

IPAM is an indispensable technology for planning, implementing and managing IPv6 and IPv4/IPv6 dual-stacked networks. Your IT staff and network administrators will need to keep track of thousands or even millions of IPv6 addresses. With such an enormous address pool and complex subnet structure, IPv6 simply cannot be tracked on a spreadsheet – finding a specific address in a seemingly endless list of IPv6 addresses in Excel would be like finding a needle in a haystack. Everyday tasks such as determining the next available network will become anything but trivial.

The transition to IPv6 will require an advanced IPAM platform to insulate administrators and end users from the complexities of defining, allocating and managing networks and addresses. Without a robust, IPv6-ready IPAM solution, you will be unable to cope. While IPv6-only Internet traffic represents a small amount of all traffic today, the transition to IPv6 is inevitable and you must be prepared with IPAM.

Summing Up – IPAM is Strategic

The best-connected business wins. The ability to centrally manage "everything IP" is the key to ensuring always-on application access and business connectivity. The IP address is the axis around which effective mobile security, address management, automation and self-service are driven. This makes IP Address Management a fundamental technology for gaining network intelligence and real competitive advantage.

Outdated, basic IPAM tools and spreadsheets may have worked in the past, but a true IPAM platform is now business-critical to manage today's increasingly complex and dynamic networks. IPAM allows you to build a smarter network and realize higher business returns from network-dependent initiatives including BYOD, virtualization and cloud.

By linking devices, users and network activity, the BlueCat IPAM platform provide a rich source of network intelligence. This strategic insight and actionable intelligence allows you to drive more reliable service delivery, greater agility, improved security, and lower infrastructure and IT labor costs. With the BlueCat IPAM platform, you will be better equipped to manage the growth of networks and devices, better able to respond to business demands and better prepared to benefit from emerging technologies including IPv6, M2M and SDN.

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