Proteus: IP Address Management Built Right

Abstract

This paper discusses the evolution of IPAM technology toward the use of purpose-built appliances. Proteus' features are discussed in the context of current IPAM solutions and future network considerations. The new approaches to this technology that Proteus embodies are explained in terms of the integration of business processes that it enables.

To view a video presentation of this document, visit our Video Centre at www.bluecatnetworks.com

BLUECAT NETWORKS™

The IPAM Intelligence Company

Use of this document

Copyright

Publisher Information

Published in Canada — No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means without the express written permission of:

BlueCat Networks, Inc.	Attention:	Product Manager
4101 Yonge Street, Suite 502	Telephone:	416-646-8400
Toronto, Ontario	Fax:	416-225-4728
Canada M2P 2C9	E-mail:	info@bluecatnetworks.com
	Website:	www.bluecatnetworks.com

No Professional Advice

This document is for convenience and informational purposes only. This document is not intended to be a comprehensive or detailed statement concerning the matters addressed; advice or recommendations, whether scientific or engineering in nature or otherwise; or an offer to sell or buy any product or service. BlueCat Networks does not warrant or make any representations regarding the use, validity, accuracy, or reliability of, or the results of the use of, this website or any materials on this document or any website referenced herein. This document is intended solely for the use of the recipient. It does not institute a complete offering and is not to be reproduced or distributed to any other person.

Executive Summary

As the Internet Protocol (IP) has gradually become the media of choice for modern networks, security issues have arisen through the sheer growth in its complexity. Version four of IP, or IPv4, has almost run out of available addresses. Despite solutions like Network Address Translation (NAT), the lack of addresses and other issues with IPv4 would be best addressed by adopting the new version of the IP protocol, IPv6, beginning now. New devices such as VoIP phones require a much richer set of configuration information from DHCP servers. The level of complexity required of DHCP services will only increase over time.

The evolution of the complexity of IP began with the use of spreadsheets to track all of the data involved. This approach was superseded at large carriers by the adoption of IP Address Management (IPAM) solutions. These early solutions were very IP-centered and did not usually manage DNS. They were also expensive. Second-generation IPAM systems have been available to enterprises as well as carriers, but they are still driven by technology constraints rather than by business models. These systems can pose integration concerns in large networks, and they do not eliminate the underlying complexity of IPAM or improve security dramatically.

Proteus represents the third and next generation of IPAM systems. Built on the heritage of the Adonis DNS/DHCP appliances, Proteus is a hardened, firewall-grade appliance. It is capable of running in network environments where other IPAM solutions could simply not be considered. Proteus uses a unique multi-core design that keeps management of IP, DNS and Deployment separate while managing interactions between these systems in the background. Proteus' XML-native design enables business considerations to be implemented without sacrifices due to technological constraints.

Proteus is IPAM Built Right.

Contents

Evolution of the “Everything” Protocol

The evolution of the TCP/IP protocol suite from the Internet Protocol to the "Everything" protocol has been fast and complex. Driven by a need to embrace interoperability, the majority of networks now support TCP/IP for at least a portion of their coverage. Organizations looking to deploy next-generation business and communications applications are looking for ways to rapidly increase the utilization of existing internet and core network resources. These rapidly changing network environments demand new management frameworks to simplify network configuration and deployment changes. Existing point-based solutions do little to help organizations address the issues of scale, usability, security and network availability at the IP level.

Currently in its second generation of evolution, IPAM (IP Address Management) software has emerged as a solution to solve these critical challenges. Mid- to large-sized enterprises are demanding a 3rd generation solution to IPAM.

IPAM software deals specifically with the management of DNS (Domain Name Service), IP Address Inventory Control and Provisioning, and DHCP (Dynamic Host Control Protocol). These services are known as IP Layer services and connect clients and servers to servers, firewalls, switches, routers, media gateways and session border controllers also at this layer.

IP Layer Services

The IP protocol is the part of the TCP/IP protocol stack that controls the movement of packets through a TCP/IP network such as the Internet. Every device on an IP network requires an IP address. These are assigned either statically, for devices such as servers, or dynamically, through DHCP. The available range of IP addresses within a network is organized into various hierarchical levels of subnetworks, each with a portion of the address range under its coverage. Addresses that will be dynamically assigned are organized into pools, waiting to be leased to a device. In order to locate a device, a user can reference the device by its IP address. This is somewhat impractical, however, as it is beyond the capacity of the average person to memorize several of these addresses. Instead, Universal Resource Locator (URL) names are used, such as www.example.com. The DNS system converts these human-readable names into the appropriate IP address, and vice-versa.

Once these conversions occur, packets need to be switched and routed between networks and subnetworks in order to reach the desired destination, which is always another device with an IP address. These are the services at the IP or Network layer. Firewalls control the access that packets have to various networks, and media gateways and session border controllers convert packeted information into other forms at this layer.

These forms could be other communication protocols such as ATM, or media protocols, or even the standard PSTN telephone system. Packet-driven IP networks now connect to a host of services that the protocol's creators could not have envisioned. This complexity is increasing the management burden faced by network administrators attempting to allocate IP resources to all of these competing technologies. One of the principal technologies behind the increasing complexity in recent times has been the rise of VoIP and mixed-mode unified communications. This technology essentially involves using a packet network to carry telephony data. VoIP technologies also connect to the telephone network, requiring conversions between media at the borders of the IP network. This technology will also branch out and become the basis for Internet multimedia distribution in the near future.

Increasing Complexity

Overnight, the adoption of new applications like VOIP is doubling the required allocation of IP addresses on core networks. Beyond VoIP, radio frequency identification (RFID)-enabled technologies, in which a radio tag is attached to products to monitor them, could be even more of a strain to the technology. The rising number and scale of the various client options required in the setup of modern network devices means vastly increased network configuration and management overhead. Issues of high availability will also only become more serious and prevalent as IP networks become the backbone for increasingly essential services.

Can the IP protocol weather the oncoming storm? IP is definitely beginning to show its age. It has been the vehicle for much technological expansion over the last 15-20 years, but that may no longer be the case unless steps are taken now to plan for future growth. The Internet is still in its early stages of growth, a stage somewhat similar to that of the auto industry in the 1920's when new models began to appear and cars no longer just came in black. The complexity of networks, especially the Internet shows little signs of abating soon, as new technologies become available that utilize the "everything" protocol as their distribution medium.

Rationing of IP Addresses

The issue that will eventually force change upon the system is the shortage of IP addresses using IPv4, the current Internet protocol. This protocol provides over four billion usable addresses. Because of the hierarchical nature of the design however, and less than efficient distribution of addresses in the early days of the protocol's usage, a shortage of addresses currently looms. One of the responses to this crisis has been CIDR (Classless Inter-domain Routing). This is a more efficient way of distributing the addresses than the previous class-based method, but it still does not provide nearly enough addresses. Another approach

has been the use of NAT (Network Address Translation) gateways. These systems use a single external IP address to represent the single point of connection for possibly hundreds of users. Internally, such a network would use a set of reserved address ranges internally, such as the 10.0.0.0/8 network space, which never appears publicly. The NAT gateway would translate all requests to appear to come from the gateway's external IP address and therefore grant clients limited access to the Internet. This access is limited in the sense that many modern protocols for services such as packet-driven multimedia and telephony have difficulty operating in an environment that employs a NAT gateway. Also, the use of NAT translation continually taxes the limits of available routers as they attempt to manage all of the packets for larger and larger networks. Therefore, there is another proposed solution to this dilemma on the horizon: IPv6, the next generation Internet protocol.

The Emergence of IPv6

IPv6 is a modern protocol that provides an almost unlimited number of available addresses within its framework. It addresses issues such as mobility and security that were just not conceptualized as issues when the IPv4 protocol was being designed. So, with all of this going for it, it might seem like foregone conclusion that the migration would begin as soon as possible. This is where the current situation gets sticky. Switching to IPv6 would mean that much current network equipment would be rendered unusable. After the infrastructure spending that occurred around Y2K, organizations are not as anxious to embark on wholesale infrastructure upgrades. Also, the new addressing scheme for IPv6 is not as human-readable as the scheme for IPv4. This begins to get at the issue behind this paper. Many administrators can simply not even contemplate moving to IPv6, as their processes could not handle the transition. Many networks are currently running without any documentation at all. Others manage the entire IP space in a series of Excel spreadsheets. Although it does not present any IP management capabilities, this is one of the oldest methods of tracking IP addresses, and it is still practiced on many networks around the world.

Although IPv6 adoption has been slow, the market will drive its eventual acceptance. Needs such as QOS (Quality of Service) monitoring and advanced traffic shaping that come with hosting telephony and multimedia applications on IP-based networks, along with more traditional forms of packeted data, will be drivers for adoption. This can already be seen in locales in Asia, such as Japan, where IPv6 networking has been embraced for devices such as IP-enabled phones and game consoles. The explosion in requirements there around traffic handling and sophisticated IP layer configurations has led to widespread IPv6 adoption and networks that run IPv6 and IPv4 in parallel. Many organizations such as the US military are specifying IPv6 capability as a requirement for new networking equipment in anticipation of eventual adoption. The movement to IPv6 is not a matter of if, but of when.

Using Spreadsheets is Not the Answer

When an organization is fairly small, and the network is not extremely extensive, tracking the IP space using a spreadsheet seems like a fairly manageable task. There are few domains, and thus the DNS records make sense and there are few subnets connected to fewer address blocks. Even if a CIDR sub-netting scheme is in place, the number of available addresses and the management of their provisioning is still a pretty straightforward task. One person can pretty much conceptualize this network in his or her head. This is where most networks start out. Then things happen; the DNS space gets more complicated with new record types and complex inter-dependant relationships. The IP address space starts to push the boundaries of available addressing and needs to be restructured, requiring planning and forecasting. Many of these same networks are also using a command line interface and a simple text editor to configure these systems. This is has been standard practice with DHCP and BIND DNS servers from ISC, the most popular DHCP and DNS servers in the world. This method of operation is no longer just common to small networks. Many large networks still use these methodologies in the perceived absence of a better alternative.

This practice is not something that can be counted as the first generation of IPAM, despite its widespread usage for so long. Spreadsheets can track IP address space in a non-dynamic fashion, but they involve no management of the DNS or IP address spaces that they enumerate. Since spreadsheets are a tracking tool, the actual management of the system is going on in the network administrator's head. There are very few other mission-critical areas within business today where this would be considered responsible. Indeed, the policy frameworks that drive modern business demand tracking and accountability. Where only the largest carriers demanded this type of monitoring and control in the past, enterprises now realize that proper control and monitoring of the IP layer are a needed extension of network hygiene and security. Also, compliance with new measures such as Sarbanes-Oxley requires that policy-based retention of IP-related information become the norm, not the exception. The reason so many administrators may have stayed with this practice for so long could have had to do with the available alternatives.

The First Generation — An Attempt at IP Address Management

There were multiple attempts by large vendors to address this need for IPAM as the turn of the century approached. However, these first generation systems were centered much more toward IP Provisioning than DNS management, and they were not designed to manage the type of dynamic environments that are commonplace now. The centralized design of these systems meant that networks were limited in their design and their ability to respond dynamically to change. At least one offering is tied to the use of particular routing hardware. These large, extremely expensive and difficult-to-implement systems have not satisfied the business requirements of the large networks they are managing. Networks must be redesigned to match the

requirements of the technology rather than with business goals at the center of planning. The low ROI of these systems, with their high and often ongoing licensing costs, makes them less appealing as time goes on. Also, where these systems are offered as an off-site service rather than a software package, there can be concerns around what kind of information is leaving the company's private network.

Software-Based IPAM

These systems often consist of software that is meant to run on one or more generic server operating systems. While these server operating systems can be made relatively secure, this involves using the server for a single purpose, and spending a great deal of time optimizing the server for the assigned purpose and security profile. Portions of the operating system that will not be used should be removed, and all unnecessary access locked down. Hardware must also be analyzed for vulnerabilities. This is a time-consuming process that must be carried out by the most highly trained and expensive of network staff. This adds further complexity and expense to the implementation of these first generation solutions. Appliance-based systems have been the answer to the issue of server configuration for many mission-critical server technologies such as routing, firewalls, DNS and DHCP. Appliances can ensure higher platform security, managed updates, and more intuitive configuration and management that a generic server could. Coupled with economic value in terms of saved labor and decreased downtime, the argument for purpose-built appliances for some network functions is clear.

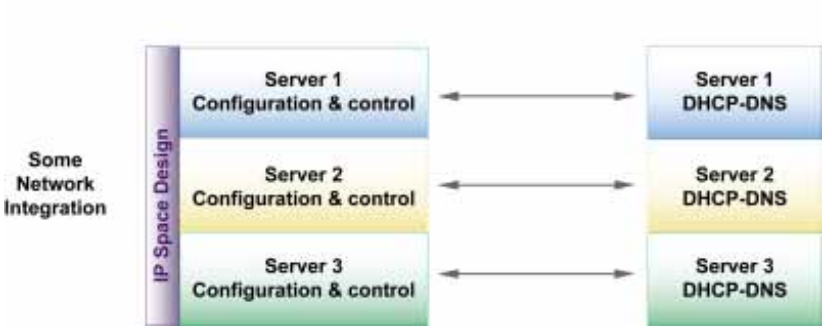
Second Generation – Getting Closer to an IPAM Solution

Second generation IPAM solutions have dealt with many of the frustrations of earlier solutions. Support for Dynamic DNS and Microsoft Active Directory and a more graphical and less complicated solution have been hallmarks of this generation of solutions. Some second-generation solutions are software-based, and they suffer from the same issues described above for first-generation solutions that require a server to be optimized for them. The appliance approach adopted for DNS and DHCP servers was introduced to the IPAM market in the second generation, but it used a very limited form of IPAM. Some of these approaches regarded IPAM as just a matter of dealing with more servers, even though the way to manage a substantially larger number of servers is not just to do more of the same thing. A larger perspective must be adopted, that recognizes that planning must occur at the logical level before implementation can be contemplated, when a network is sufficiently complicated. Modern IPAM systems require sophisticated tracking technology that

links into reporting capabilities and an alerts engine. They also require a planning and design environment for activities such as re-allocating, editing complicated zones, and merging entire networks. Combine this with modern network security and interoperability challenges, and these systems also begin to pale in comparison to the business requirements they are trying to meet.

Some second-generation systems also suffered from a bias toward IP provisioning and accounting, with DNS management being an added feature. Many of these systems were designed to support large networks, but the structures they used for this support were fixed and standardized. In order for organizations to use this type of system, the organization must understand how the technology is organized and then map this to the structures within the organization. The technology demands that the business meet it, instead of the other way around. User management and data modeling on these systems represent early attempts at a solution, and they are not extremely flexible. Some of these systems lack adequate planning or design tools, while others fail in the areas of monitoring or reporting. Many of these systems offer support for IPv6 and VoIP, but mixed networks are still a challenge.

Figure 1: Second Gerneration IPAM



All of the second-generation systems are very technical solutions oriented towards a technical audience. Anyone using a second-generation IPAM system is considered to be a DNS or DHCP expert with familiarity with the terminology involved, and is assumed to be responsible enough to be given control over the part of the IP network given into their care. This is not always the case, as management tasks may need to be delegated to managers or even small business owners who have little time to learn DNS completely. A management system must be capable of saving these users from themselves, while providing enough hints and familiar terms to allow them to accomplish required tasks. Pursuing only a technical user base will not satisfy requirements in the type of complex modern networks that are currently being developed.

Modern network infrastructures will involve parallel networks differentiated by IPv4 vs. IPv6, and data vs. VoIP, and SIP-enabled multi-media in situations where a single network exists today. Second generation systems, while being able to accommodate these technologies, are simply not able to complete the complex modeling required to design supporting networks that incorporate all of these requirements. Second

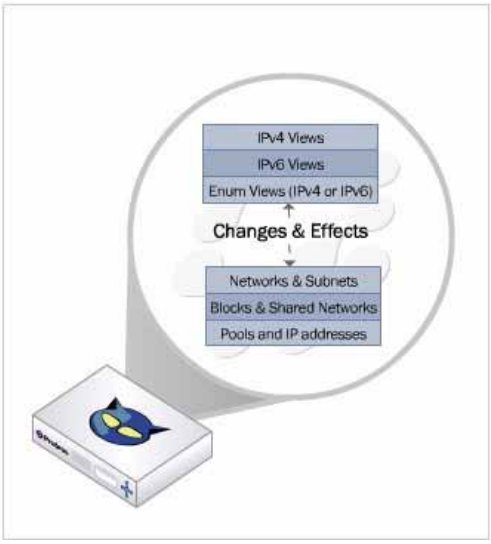
generation IPAM systems have not successfully addressed issues of network interoperability either. This issue is two-fold, with part of the problem being the interoperability of IPAM-generated data. The other main part of the problem is providing perorational supports for interoperability through services like SNMP and SOAP. All second-generation IPAM systems have demonstrated poor performance in at least one of these areas.

The Next Generation: Proteus Enterprise IPAM Appliance

Proteus by BlueCat Networks represents the third generation in the evolution of IPAM systems. BlueCat Network's world-renowned DNS, DHCP and DNS Caching appliances represent the evolution of DNS and DHCP servers from early homemade servers with text editor interfaces to powerful purpose-built DNS and DHCP appliances that represent a blend of high security and simplicity. They are packed with features such as BIND Views, intuitive interfaces, and sophisticated control over zones, records, allocations, access control and authentication, real-time reporting and alerts, TSIGs, MAC filtering, DHCP Failover, DNS High Availability, interoperability, and many other areas. This evolution in the DNS and DHCP server market has been well publicized and their ascendancy in popularity is the new status quo. Since IPAM is simply a larger and more sophisticated context for managing DNS, DHCP and IP address allocations and their interactions with the rest of the IP layer, it was only a matter of time before this 21st century approach resulted in the evolution of a full-featured IPAM appliance.

Proteus has been designed as a secure appliance server with the hardware redundancy required for operation in mission-critical environments. It supports the full Adonis feature set and legacy features that will still be with us for some time such as IPv4, CIDR and NAT. It is also designed to support other newer technologies in parallel to this, such as IPv6, and ENUM for VoIP, dynamic QOS monitoring and traffic shaping for applications such as VoIP and SIP-enabled multimedia and many other supports for future requirements.

Figure 2: Multi-Core functionality maintains consistency between DNS and DHCP



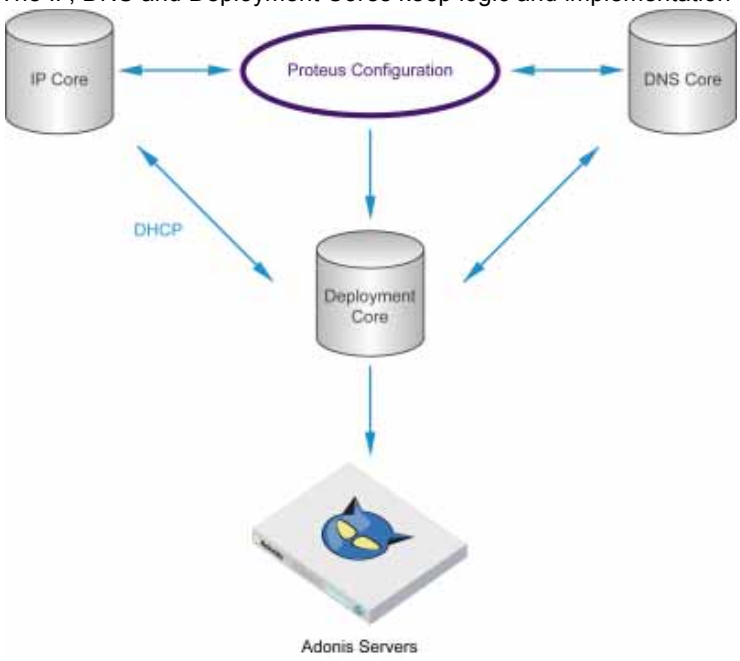
Reporting in Proteus enables complex network management and forecasting, as well as ensuring compliance with policies. Policy modeling within the Proteus framework can accommodate almost any set of business requirements.

Alerts within Proteus draw on information from both SNMP traps and database triggers. This can alert an administrator that a server has crashed, or that a pool of IP addresses is running low on availability.

User management on Proteus implements a seven-level model, with object- and type-based permissions customizable for any object in the system. Users can be authenticated against Proteus itself, or external Radius, Kerberos, LDAP and RSA resources. Transaction logging maintains a complete record of system usage, and any transaction can be rolled back independently of the other transactions around it as long as they are not dependant on it.

Data Modeling on Proteus involves mixing global objects with multiple network Configurations containing interdependent IP, DNS and Deployment Multi-Core settings and information. This enables enough abstraction to correctly model any required topology.

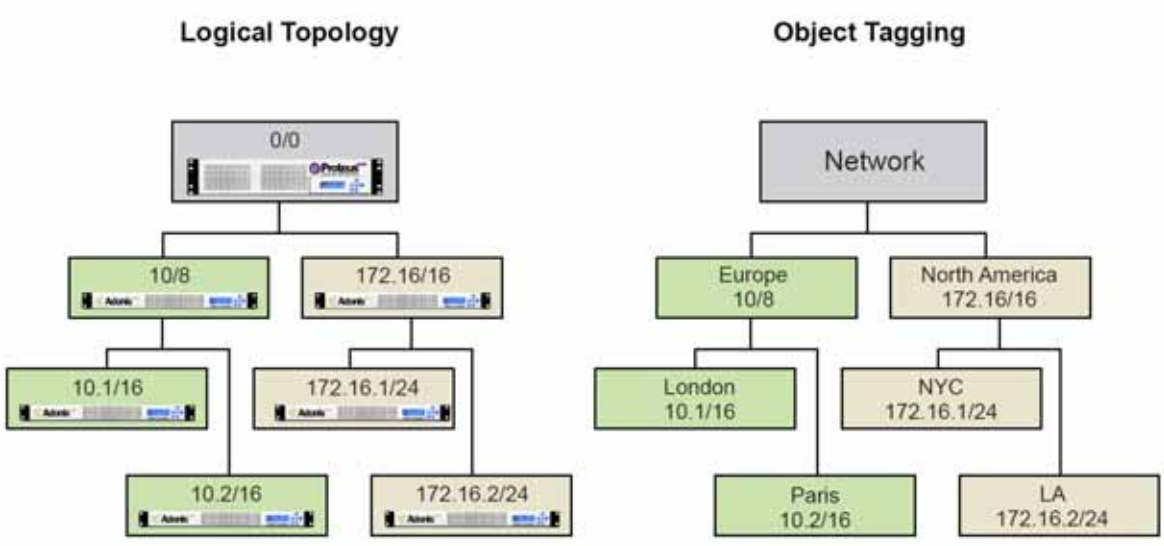
Figure 3: The IP, DNS and Deployment Cores keep logic and implementation separated.



Multi-core functionality guides the design process toward success by managing some underlying complexity and aiding in decision making. Data is also checked logically, syntactically, and in a deployment simulation before being implemented.

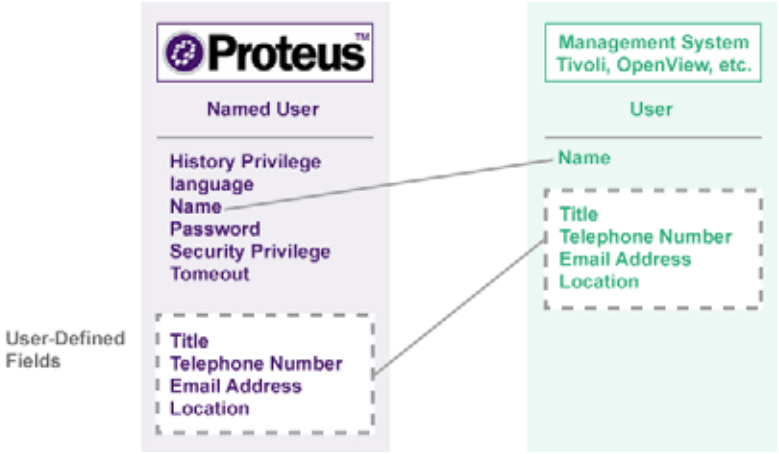
Organizations can create XML structures called Object Tags that are applied to configuration components. This enables interaction with Proteus based on organizational structures rather than the dictates of particular technologies or implementations.

Figure 4: Object Tagging keeps interfaces business-focused



Proteus brings the dynamic control of functionality such as IPv6 and ENUM for VoIP into the IPAM realm. Proteus also integrates into large network environments using SNMP and XML data interoperability through user-defined fields. These fields can be attached to any object type in Proteus and ensure that external data schemas are supported.

Figure 5: User-Defined Fields Enable Data Integration



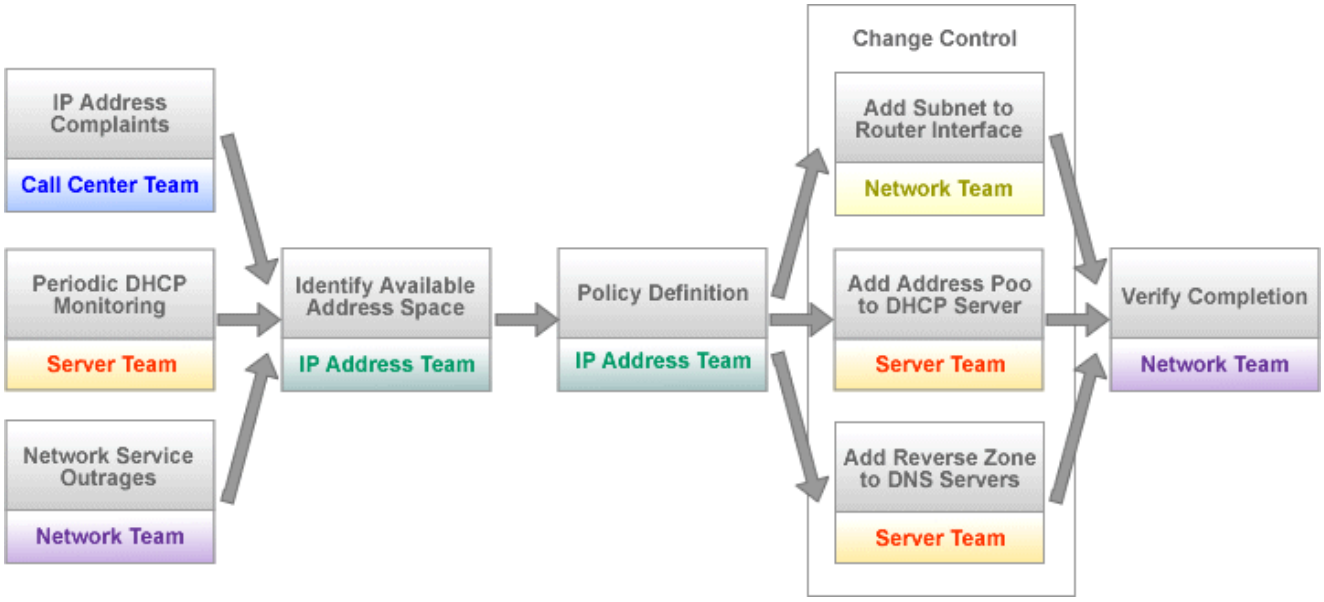
While implementing the most advanced features currently available at the IP layer, Proteus offers future abilities to link into other devices at this layer through web services using the SOAP protocol. Many routers and more firewalls and session border controllers are utilizing this technology to interoperate. Proteus is the only device in the IPAM market to use SOAP as its primary method of communication.

Proteus is quite simply the next generation of IPAM that organizations have been eagerly awaiting. The best illustration of this can be seen in an examination of the typical IPAM workflow in a large organization.

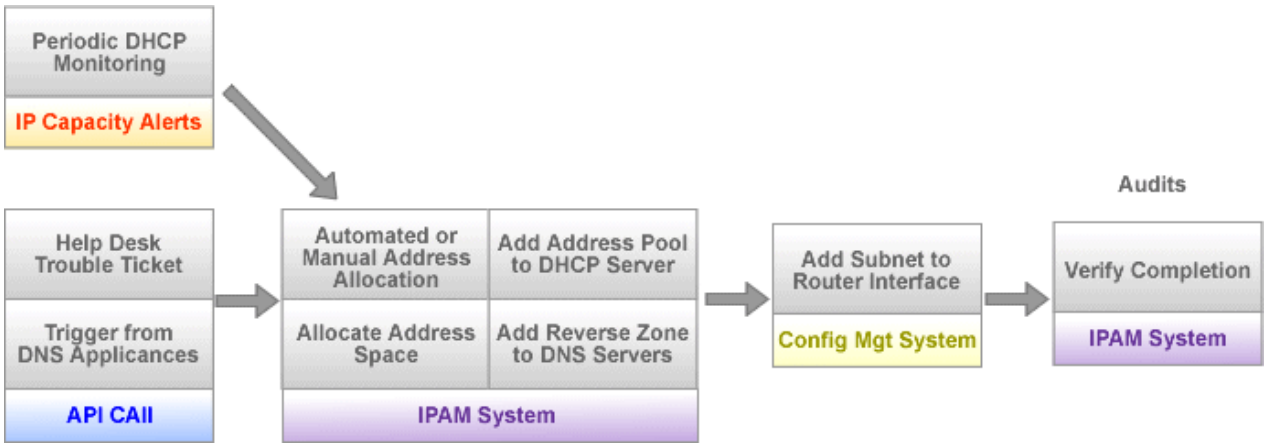
Proteus: IP Address Management Done Right

The efficiency gains seen through using a properly integrated IPAM system are apparent when it follows through an operation such as the re-allocation of an IP block. Within a large organization, this operation requires the co-operation of several staff members from various teams, and may take some time to have approved. Often, the chain of events would look like this: The call center could take a call complaining of IP Address issues, or periodic DHCP monitoring by the server team might reveal the issue, or, perhaps the network team is alerted due to network service outages. This would result in the IP Address team identifying available address space and allocating it for this DHCP server. The server team would then need to add the

address space to the DHCP server and the reverse zones for the space to the DNS server. The router team would add the new subnet to the router interface, and then the network team would verify completion of all of the work. This is a very complex set of steps because of the amount of coordination of resources required to complete the process.



With a Proteus IPAM system in place, the process could be triggered by an API call from the call center's call tracking software, or an IP Capacity Alert from the monitor on the DHCP server, or an API call from a DNS appliance. The IPAM system could then allocate IP address space, or have an administrator design and allocate the address space. The IPAM system would then add the address pool to the DHCP server, and the reverse DNS zones to the DNS server, as well as sending information about the required addition of the new subnet to the router interface to the router's configuration management system using SOAP, and to the router team using e-mail. The IPAM system would then verify completion of the tasks involved. All stages of this process would be logged and all of the transactions available for rollback if required within a Proteus system.



Proteus embraces the evolutionary advantages of the DNS and DHCP servers that it descended from without falling victim to an appliance mentality. Instead of being a closed, proprietary architecture, Proteus is designed to be implemented in pre-existing network topologies and to interconnect with all of the devices required. By basing Proteus on very standard technologies such as XML, SOAP, and Relational Database, BlueCat Networks has ensured that Proteus will be prepared to adapt to future situations not even envisioned yet. The tools used in designing a network should be able to open new possibilities as well as find the best compromises. Proteus succeeds brilliantly at this. It also manages to monitor and control the network without being overly involved in the actual delivery of service. This provides the right balance of control and delegation. Proteus has embraced all of the strongest qualities of current solutions and packaged them with some 21st century thinking into the most advanced IPAM system available.

Proteus, It's All About the Details.

Additional White Papers

- DNS Best Practices
- Proteus: IP Address Management Built Right
- How to Integrate Active Directory and DNS
- Adonis: DNS/DHCP for Small to Medium Sized Business
- DNS and DHCP Services for Voice over IP
- DNS/DHCP High Availability
- Realizing Secure Networks by Overcoming Complexity: The Proteus IP Address Management System
- Defense-In-Depth: Comprehensive Security with Authenticated
- Network Access Control
- Is It Really Part of My Network? Adonis DHCP and MAC-Based Security
- Cache Poisoning Raises Cash Crop for DNS Pharmers
- Secure DNS and DHCP Management - An Integrated Solution

To view a video presentation of this document, visit our Video Centre at
www.bluecatnetworks.com

BlueCat Networks (USA), Inc.
info@bluecatnetworks.com
www.bluecatnetworks.com
Toll Free: 1-866-895-6931
Document #: BuiltRight 1.1 - 2/07

BLUECAT NETWORKS™
The IPAM Intelligence Company