



BlueCat's IPAM Receives

REVIEWERS CHOICE AWARD

Pros:

Powerful tracking of internal IP addresses

Cons:

Requires 2U of rack space

Performance:

A

Ease of Use:

A-

Features:

A-

Value:

B+

Price:

Varies with installation;
\$50,000 on average.

BlueCat's Proteus 5000 Keeps IP Addresses In Order

By Greg Crowe | May 04, 2009

For most network administrators, keeping track of IP addresses can be a real headache. It is daunting to find out the static addresses used by devices such as servers and printers, determine which IP ranges are covered by different Domain Name System (DNS) servers, and take an inventory of which address ranges are being leased by Dynamic Host Configuration Protocol

(DHCP) devices. Add things such as wireless devices, in addition to the security concerns raised by DHCP, and you can have a real bear on your hands.

In days gone by, all an administrator needed for keeping track of addresses in the network was a simple spreadsheet. But networks have become larger and more complex, requiring more powerful tools.

The Proteus IP Address Management (IPAM) platform from BlueCat Networks is just that sort of tool. Proteus can keep track of IP addresses and DHCP leases across several subnets. It can simplify and automate many routine IP-related tasks and allow an administrator to get a grasp on the entire network.

The Proteus 5000 is a 2U rackmount appliance, which might tax space in some crowded server rooms, but there is no way to make it any smaller, with its six hot-swappable hard drive bays. However, we were pleased to find that the Proteus had two hot-swappable power supplies.



We found setup of the Proteus to be fairly easy for a network appliance. After we changed the IP address of the appliance's management interface, we could then use the Web-based administrator console from any computer in the network. It didn't take long for the Proteus to locate every Windows DNS and DHCP server — in addition to BlueCat's own Adonis DNS/DHCP appliance — on the network, gather each one's IP address, and display them all on one screen.

At this point, it was no challenge to create and edit IPv4 or IPv6 blocks. We could partition a block into smaller child blocks or even small child networks as we saw fit. Within a block, we could quickly see which devices used specific IP addresses. We were even able, without much fuss, to move a block to another parent or resize a block or network that had already been created. Finding unassigned IP addresses — probably one of the most common tasks an administrator faces — was equally easy.

Proteus makes it easy to delegate responsibility over certain IP ranges to users who aren't necessarily trained in every aspect of the platform's inner workings. Proteus has a change approval mechanism that allows senior

administrators to approve any changes before they go live. Even without this, an administrator can restore deleted items out of a recycle bin if necessary.

Proteus also has extensive audit and reporting capabilities. We could use a variety of report formats to see the network in different ways. Proteus tracked all DNS, DHCP and IPAM changes, making auditing a much easier task.

One capability of the Proteus platform of interest to federal agencies is its support for DNS Security Extensions, the cryptographic authentication functionality all agencies are required to add to their DNS servers by December 2009. With this capability, access to an agency's DNS server monitored by Proteus will be denied without the correct electronic signature. DNSSEC is quite a hot topic in the federal arena, which could make Proteus attractive.

The company includes on-site installation by one of its engineers with the price of the Proteus system. The engineer will assess a network's configuration, install the appliances, and even give an administrator a rundown of some of Proteus' basic functions.

Although the Proteus can identify and

work with any Windows-based DNS or DHCP server, it works best with another line of BlueCat products, the Adonis DNS/DHCP server appliances.

The price of the BlueCat Proteus 5000 can vary because of many factors, such as the overall number of appliances purchased based on network size and the need for redundancy. Even so, we found the average price of \$50,000 to be reasonable and a good investment for agencies scrambling for DNSSEC compliance.

For the administrator who is short on either budget or rack space, BlueCat offers Proteus as a virtual appliance that is hosted on one of its networks and manages IP addresses remotely. The pricing of the virtual appliance is based on a three-year subscription and is 10 percent less than the cost of the standard hardware-based appliance. Of course, any administrator who needs total control of all aspects of the network will need to opt for the physical appliances.

Contact:

sales@bluecatnetworks.com

North America: +1.866.895.6931

Europe: +44.118.902.6680

www.bluecatnetworks.com

