



Field Testing an Internet IP Address Management System

Number Allocation

Manuel Schmitt

For many companies, managing and distributing IP address ranges is a time-consuming challenge for the IT department and often results in a patchwork system. Proper IP address management can save time and money.

Many enterprises start small, with a handful of workstations and a single switch, router, and networked printer. Network topology is generally defined in just two places: in the devices themselves and in the administrator's head. Over time, devices are added, and occasionally someone does a makeshift replacement or assigns this or that new address.

When a new administrator comes on or replaces the old one, the first order of business is often searching and asking before clearing errors or expanding the existing network. Administrators wanting to plan ahead or better organize the work of their predecessors start by documenting the network in a way that matches the actual situation (static or DHCP-allocated IP addresses, DHCP and DNS servers). The most commonly used

tools for this are text editing or spreadsheet documents, or possibly Wikis.

As the networks get larger, come to include several locations, or when multiple administrators are on the job, these provisional measures quickly hit a wall. There's one basic shortcoming: There's no direct connection between the technology, that is, the DNS and DHCP servers, and the documentation. And in connection with that, there's no access limitation. This type of documentation procedure often has no history, making productive collaboration practically impossible.

IP address management systems, such as the Proteus/Adonis series of appliances from BlueCat Networks, promise relief from the administrator's daily grind. The concept behind them is

as simple as it is logical. One management unit (Proteus) with an overview of the entire corporate network controls the DHCP and DNS servers (Adonis), which can be spread across multiple locations, even continents apart.

Automated Address Allocation

Administrator(s) typically operate using the Proteus server web interface, which independently controls and monitors the connected Adonis servers. This design makes particularly good sense for companies with multiple offices, where every site ought to have DHCP/DNS servers.

At first glance, the idea seems simple and might tempt experienced programmer-administrators to spend a few hours with a script language on a project of their own. However, the two products offer an immense functional range - practically everything that a harried administrator needs to take control of his job, leaving little incentive to reinvent the wheel.

Bringing the two products on line is not difficult, even for beginners. Anyone familiar with UNIX-type operating systems will immediately feel at ease with the easy console-based network configuration. Proteus and Adonis are then ready for operation, and everything else is done directly through the Proteus web interface.

A Simple Interface with a View

If you were expecting a complicated Web GUI requiring manuals or training, think again. Despite a list of features as long as your arm, the first glance at the administrator interface is more sobering than discouraging.

After setup, Proteus can import any existing data, such as MAC and IP addresses, in CSV files. Anyone wanting to adapt database fields or insert specific data (such as location information for MAC addresses) needs to have some programming experience. This task is done via XML data exchange. Ongoing administration using Proteus primarily covers management of MAC and IP



Bluecat Networks equips its Proteus with redundant power supplies and updates the hardware in three-year cycles (Fig. 1).

addresses, as well as DNS.

All the connected network devices are captured based on their MAC addresses. As it should be, this is where you create all the devices located throughout the entire network, i.e., workstations, servers, network devices, etc. In addition to their MAC addresses, each "device" can by default be given a user-defined name and a static IP address, if needed.

It would be nice if Proteus expanded every MAC address automatically with the manufacturer's name as soon as it was created; after all, prefix assignments are fully accessible. This would be most helpful precisely when migrating an existing large network.

IP addresses are organized by blocks per CIDR (Classless Inter-Domain Routing), and broken down hierarchically so that you can - but don't have to - group larger ranges and classify partial and sub-ranges in tree arrangements. IPv4 and IPv6 blocks can be managed in parallel and with the same range of functions.

Masters, Slaves, and Zones

In order to simplify the act of adding network ranges, e.g., 192.0.2.0/24, administrators can create any number of individual templates - an ideal option when you want to assign gateways fixed IP addresses such as .1 (or an offset from the network address), or want to reserve certain ranges for switch management.

In addition to IP and MAC addresses, Proteus can be used to control individual DNS Master and Slave zones. A current BIND runs on the Adonis servers, making the full RFC functional range of the DNS available. The Proteus management interface recognizes all RFC-compliant resource record types. Separate entries can also be created.

Anyone who likes BIND views will be

pleased. Proteus even offers them in the form of hierarchically structured zone name administration. Thus, the zone "example.com" can be found under "com" and then under "example." The levels can be expanded to any depth desired. In its coming version, BlueCat is planning to have the display appear as a tree diagram.

Having a (definitively) authoritative name server is particularly important for companies that want to manage their company domain(s) under their own roof, so as to remain independent from the hosting provider. Thanks to the web interface, even administrators with no BIND experience can find their way around. In the typical setup scenario, however, an Adonis server acts not only as an authoritative name server, but also (generally simultaneously) as DNS resolver/recursor for the connected clients. In this case, of course, security-conscious administrators would prefer to see two separate DNS instances used for this on the Adonis machines.

In the case of the generally unspectacular DHCP, the Adonis products offer an important feature that cannot be solved very easily with open source tools: a true DHCP failover that takes the already allocated leases into consideration.

For old hands among the BIND administrators, the DNS deployment option will certainly require a bit of an adjustment, but it is practical and makes good sense. Any changes made are not immediately active on the Adonis servers; they do not take effect until a definitive "deploy!" has been issued. That's something that could prevent many an inconsistent DNS setup. Optionally, deployment can be automated and time-delayed, so that already overworked administrators don't have to spend their evenings

mouse-clicking.

According to the manufacturer, the entire web administration, which appears to be completely unified, and the back end behind it, have been object-oriented programmed and implemented. Users will notice that as well. Proteus sees all entries as individual objects: IP and MAC addresses, network blocks, DNS zones, etc. This means easy implementation of the hierarchies described above.

The advantages and disadvantages can be seen clearly using a practical example. An MX entry in a DNS zone is seen as an individual object. If the same mail server functions in more than one zone, such as "mail.example.com," then it changes automatically in all zones if you rename it to "mx," for example. This feature generally makes good sense, but administrators must be careful here not to accidentally make more changes than necessary.

Object-Oriented in its Purest Form

In addition to everything else, the object-orientation lays the groundwork for object-based permissions allocation. In Proteus, you can create any number of users and limit their permissions in every respect to one or more objects.

Thus, it's conceivable that you could have a second administrator who is only allowed to access the IP addresses (but who has unlimited privileges there). Or one who can only create and edit DNS zones. It's even possible and conceivable to create users who can only see DNS zones, but can't change them - e.g., helpdesk support employees.

The fact that Proteus is implementing a kind of "view-like" configuration context makes it possible, for example, to manage several locations, company divisions, or customers in one individual "configuration." Each configuration can have several administrators, subadministrators, etc. There are almost no limits to this feature; the objects and their hierarchy make it all possible.

Each object has a detailed log that records all the changes made to it - and who made the changes. Unfortunately, there's no automated undo/rollback

system or “snapshotting” - at least not yet. The manufacturer has already announced that these functions are on the way.

Other features beyond these that are worthy of mention (and there are many) include reporting in PDF format that makes the IP address block capacity visible. Address ranges can be broken down and grouped. Favorites enable any user quick access to important personal settings. Using tagging, you can quickly search for objects without having to browse for them with the GUI.

Mission: Critical

Redundancy and high availability play a critical role precisely in medium- and large-sized companies, wherever the focus is on selecting suitable products. The hierarchical structure allows integration of almost any number of Adonis servers, and depending on the configuration (in the master-slave case), they are completely redundant and in any case not dependent on Proteus.

Proteus as well, according to the manufacturer, has an (active-active) redundancy scenario linked with a storage system where the Proteus master data are located (linked by ISCSI or fiber channel).

For the test we used a Proteus 5000 and two Adonis XMBs. The test scenario employed corresponds to a list price of around US\$ 80,000, according to the manufacturer. The smaller Proteus 2150

has a list price of US\$ 40,000, and the Adonis servers range from around US\$ 2,000 to US\$ 18,000. As is normal with these types of devices, support, hardware service, and updates are for the most part available under an annual support contract, the cost of which is linked to the purchase price. The “evergreen” approach offered by the manufacturer is a definite plus: They not only replace defective hardware, but also update devices every three years if a contract of corresponding length is in place.

Anyone using SSH to access the machines will see (as described on the manufacturer’s web site) that they are based on slightly modified Debian Linux. Only the system kernels are adapted to the special requirements.

The Proteus web administration runs on a JBoss server. Adonis has a firewall implemented using iptables that the system administrator can expand to include useful entries, e.g., related to connection rate limiting.

Conclusion

Adonis and Proteus are particularly well-suited for use by small enterprises. They greatly reduce workload, are logically structured, and thus easy to understand. By using several systems of both product series, users can create a level of redundancy that is also well-suited for large companies or mission-critical applications.

The one drawback is the cost of the

systems. Most small and many medium-sized companies are likely to shy away from investments in the five-digit range. The more likely solution for small and medium-sized companies is open-source software running customized scripts. In larger companies, this investment could pay for itself and free up system administrators for more stimulating tasks, such as distributing and documenting IP addresses.

Data and Pricing

Proteus/Adonis

IP Address Management Appliances
Manufacturer: Bluecat Networks,
www.bluecatnetworks.com

Proteus 5000: Dual Opteron 270
with 4 GByte RAM and two 73 GByte
SCSI hard drives

Adonis XMB: Intel Celeron (1 GHz),
512 MByte RAM, one IDE hard drive
(40 GByte)

List prices: Proteus starts from US\$
39,995, Adonis starts from US\$
1,995

Operating system: modified
Debian Linux

iX Rating

- + Intuitive interface
- + Well-conceived, flexible design
- High price