

Comprehensive Monitoring of DNS and DHCP Keeps Administrators in Control

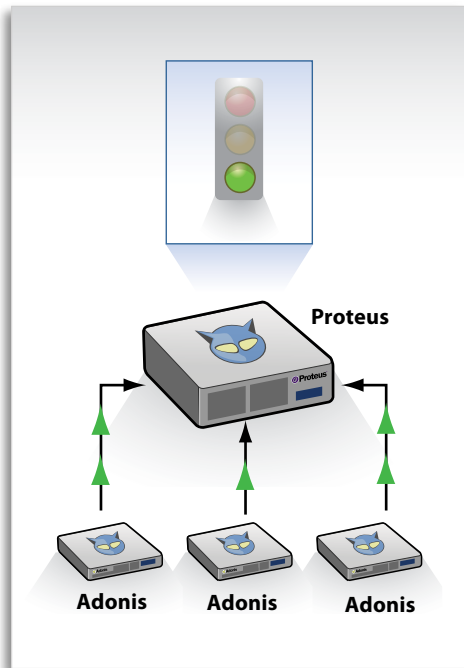
- Real-time, centralized monitoring of local and remote DNS and DHCP services identifies potential problems and threats;
- Custom SNMP MIB provides a granular view of DNS and DHCP services;
- Event notification via email or SNMP traps ensures issues are detected and corrected proactively;
- Analysis of historical network usage allows for better forecasting of growth and capacity requirements; and,
- Centralized logging system and on-demand report generation help demonstrate compliance with IT governance regulations.

Market Drivers

DNS and DHCP, key technologies enabling the Internet and IP-based corporate networks, are more pervasive than ever.

- Application builders continue to choose DNS as their application's database or directory for scalability reasons;
- New services like IP telephony and new applications like RFID tags are driving the next phase of DNS growth;
- An increasingly number of network services are standardizing on DHCP for IP address allocation; and,
- A greater variety of network-attached devices are leasing DHCP issued addresses.

As these trends continue, a complete, real-time view of DNS and DHCP services is critical to network management and planning. Without an accurate view of network activity, solving DNS or DHCP related problems is more difficult and time consuming. Analysis of historical network usage is required to forecast growth and capacity



requirements. Without a capacity plan, your network may reach a 'tipping point' with service outages as the consequence.

Busy network administrators require sufficient information to track configuration changes – 'who made the change,' 'when did it happened,' and 'from where was it was made.' This information can prove invaluable in diagnosing configuration errors, particularly those that cause network disruptions.

Equally important for publicly traded companies and those in regulated industries are the emerging IT governance regulations. Network monitoring, reporting, and auditing features are necessary to demonstrate compliance with regulations. These features allow administrators to state with confidence who had access what IP addresses and when, and assess the consequences of such access.

Unfortunately, generic DNS and DHCP servers often do not provide real-time visibility into dynamic DNS and DHCP updates. They do not provide the tools for network administrators to assess future requirements or to quickly resolve configuration errors. Fortunately, BlueCat's Proteus and Adonis appliances provide comprehensive reporting and monitoring tools to address these issues.

Real-Time Visibility into DNS and DHCP Services

Proteus's easy-to-read, easy-to-navigate user interface monitors DNS and DHCP services both locally and remotely. Remote monitoring provides a real-time, centralized perspective of performance and overall service availability across the entire network. It helps ensure operational efficiency by instantly notifying administrators of any change in the state of a service, such as an outage or a capacity issue. Administrators can proactively monitor their entire IP space to identify trends or potential threats. It gives them the tools they need to ensure reliable network performance.

Proteus provides real-time visibility to active DHCP leases, host name usage (through DNS), active DNS zones, hardware assets through MAC addresses, and network location through port mapping. Event notification helps keep administrators aware of issues before they become problems. As events occur on Proteus, administrators are instantaneously notified via email or Simple Network Management Protocol (SNMP) traps to ensure that issues are detected and corrected proactively.

Custom SNMP MIBs

SNMP is an effective tool for actively monitoring DNS and DHCP services. While standard SNMP Management Information Bases (MIBs) provide an accurate view of overall system health, they do not offer status information or statistics specific to DNS or DHCP services. BlueCat's DNS/DHCP management appliances include proprietary SNMP MIBs that provide a very granular view of DNS/DHCP services, such as:

- DNS/DHCP uptime;
- DNS/DHCP performance and usage statistics; and,
- High availability status and statistics.

Graphical illustration of this information, presented on an SNMP monitoring service, provides an active perspective of DNS/DHCP status. It also allows for easy forecasting of network growth and identification of other trends.

Logging and Reporting

Proteus contains a centralized logging system that captures all transactions and system-generated alerts. Specific services like Data Checker and DHCP Alerter will post events that require an administrator's attention.

All events generated within Proteus are filtered and processed by 'rules engine' to determine how and when administrators are to be notified. The notification system can filter by source and/or severity and inform users via email or SNMP traps.

On-demand report generation is available through Proteus's web-based management console. Proteus's reporting system provides visibility into a variety of parameters, ranging from network and DHCP utilization to administrative changes. Administrators can customize reports by defining which parameters are required and how each parameter is sorted. Reports come in a variety of formats including PDF, HTML, CSV, XLS and RTF.

Proteus API

The Proteus Application Programming Interface (API) allows for direct access to the Proteus' database. Complex data analysis and granular reports can be developed utilizing the API.



©2008. BlueCat Networks, the BlueCat Networks logo, Proteus Enterprise IPAM Appliance, Adonis DNS/DHCP Appliance, the Adonis logo, XHA, and IPAM Intelligence are trademarks of BlueCat Networks, Inc. Microsoft, Windows, and Active Directory are registered trademarks of Microsoft Corporation. Any product photos shown are for reference only and are subject to change without notice. All other product and company names are trademarks or registered trademarks of their respective holders. Printed in Canada. DOC. NO. MON/2509

