

DNSONE PACKAGE FEATURES AND BENEFITS

The DNSone package delivers reliable, manageable, scalable, and secure core network services at a lower cost and with higher security than server-software and with greater network availability than any competing solution. The services included in the DNSone package include:

DNSone Advantages

- Combined management views and automation of tasks through integration of DNS and DHCP services
- Industry-standard DNS services using the latest BIND implementation
- One-button software upgrades that make it easy to add new features and to remain secure
- High availability with fast network failover and database synchronization
- Enhanced security with DNS attack detection and mitigation features
- Secure management using SSL-based VPN that works from anywhere, through any firewall
- Infoblox Views—an enhanced version of BIND Views—that provides virtual DNS services and allows a single Infoblox appliance to respond differently to DNS queries based on the source of the query
- Built-in TFTP, FTP, and HTTP server for distributing firmware and configuration files to network devices, such as VoIP phones and wireless access points, during the booting (start-up) process
- Support for network quarantine applications like Authenticated DHCP in large environments

- Naming services via Domain Name System (DNS);
- Addressing services via Dynamic Host Configuration Protocol (DHCP);
- Network visibility and control via IP address management (IPAM);
- Authentication, authorization, and accounting services via RADIUS Proxy;
- File delivery services via Trivial File Transfer Protocol (FTP, HTTP, TFTP);
- Time synchronization services via Network Time Protocol (NTP)

ADDITIONAL BENEFITS

High-availability Services: The DNSone package runs on the reliable Infoblox appliance platforms, which are designed for nonstop operation in high-performance networks. High-availability (HA) services are supported by bloxHA™ technology—which uses industry-standard Virtual Router Redundancy Protocol (VRRP) for sub 5-second network failover—and bloxSYNC™ technology to ensure real-time database synchronization with no loss or duplication of data. Together, these two technologies allow critical name server and DHCP services to always remain responsive and up-to-date and eliminate common but challenging problems such as issuing duplicate IP addresses.

Integrated, Zero-admin Database: The DNSone package stores all DNS and DHCP data in the integrated bloxSDB™ database, which is built into the Infoblox NIOS™ operating system software provided on all Infoblox appliances. The bloxSDB database is designed specifically to support integrated core network services and provides unmatched consistency between service and management views of IP-address-centric network services data without compromising performance.



Easy-to-use GUI: The DNSone package includes the ID Device Manager that can be run from a PC running Windows XP, Vista or Linux OSes. The abstracted, data-centric interface streamlines complex and repetitive management operations and enables administrators to focus on data and services rather than boxes and protocols. This reduces management time and eliminates many common data entry errors. The Infoblox GUI can be locally installed on MS Windows devices.

Integrated Management: The DNSone package provides practical operational efficiencies that lower total cost of ownership. For example, creating a DHCP range automatically creates an associated DNS record, reducing the number of tasks required of network administrators.

Granular, Role-based Administration: Role-based administration is a powerful way to ensure that administrators are only given access to view and modify specific core network services attributes consistent with their organizational and functional role. For example, this means that a senior DNS administrator could have the ability to define new domains and add new appliances to a grid, while a help desk administrator might only have the ability to view specific subnets and issue IP addresses to new devices by picking from a pre-defined list. Infoblox has created a very scalable, yet very granular role-based administration framework. The framework provides customers the ability to delegate administration down to the object level and yet maintain permissions for a large, complex administration model. Some specifics include:

- Easy workflow to manage permissions. The administrator can quickly set permissions by right-clicking on any object to bring up a list of permissions. This is much easier than having to switch to a separate administration panel. It also provides a comprehensive list of which permissions have been granted to each administration group.
- Administration is also eased through the use of roles. Roles can be mapped to an organization or job (e.g., Printer Admins, DNS Admins) and then roles can be assigned to administrative groups. This abstraction model allows a set of permissions to be defined once such that any changes to the role are inherited by all groups that are associated with it.

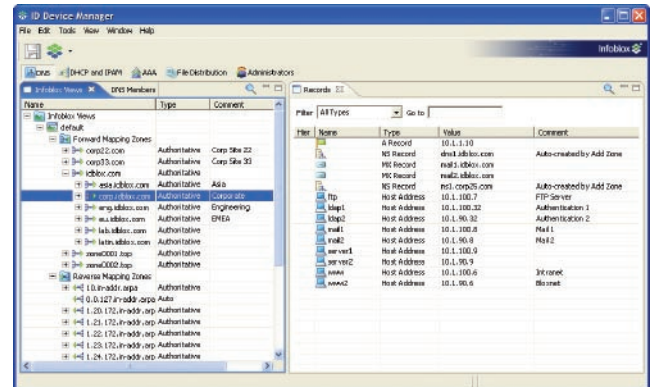
Enhanced Security: The Infoblox NIOS software is hardened and consistently withstands security scans and attacks from the most demanding government and military organizations. The DNS and DHCP services provided by the DNSone package can be upgraded easily to support the latest versions of BIND and DHCP, ensuring minimum exposure to security threats. In the event that a new exploit is discovered, the underlying Infoblox NIOS software can be upgraded in minutes via a single, simple operation. This makes it much more difficult to penetrate than general-purpose operating systems with known vulnerabilities. Management communication is secured using Secure Sockets Layer (SSL)-encrypted VPNs for protection against management compromise.

DNS Attack Detection and Mitigation: Infoblox provides the ability to detect, alert and mitigate any attacks against members that are configured as recursive DNS servers. The NIOS software will monitor two key parameters that are indicators of an attack: mis-matched DNS message IDs and mis-matched UDP ports on DNS responses. This happens when an attacker is guessing on those parameters to “spoof” a response with the poisoned data. The administrator can set a threshold for both parameters and when either is exceeded the system will send an email alert and/or SNMP trap (whichever is configured for the system). This feature will give administrators an early warning that one of their servers is under attack.

In addition, Infoblox NIOS allows attack mitigation by implementing query rate-limiting. The administrator can implement a filter on a specific IP or network to limit or stop all traffic. This will slow down or stop the attack, the success of which is based on the attacker’s ability to try as many response “guesses” as possible before the legitimate DNS server can respond.

SCALABLE, INTEGRATED MANAGEMENT

The flexible ID Device Manager user interface provides the visibility and control needed to manage all core network services in dynamic IP networks. The ID Device Manager simplifies the management of the appliance, services, and data—and provides summary and drill-down views with a simple click. Granular, role-based management capabilities enable administrators to delegate specific networks, ranges, hosts, and devices to junior or departmental personnel. The ID Device Manager makes it easy to cope with fast-changing networks, and because all data reside in the Infoblox appliance database, the status of devices and services shown in the ID Device Manager always reflects the actual, real-time state of the network.



Manage appliances, services, and data using the ID Device Manager.

NONSTOP INFRASTRUCTURE FOR CRITICAL NETWORK SOLUTIONS

Infoblox network services appliances include a range of special capabilities that serve key network applications:

A Foundation for Network Access Control (NAC)

The Infoblox NAC Foundation module—included in the Infoblox NIOS software—provides intelligent, policy-based control over Infoblox’s DHCP services and, as such, provides a foundation for a wide variety of NAC solutions using components from multiple vendors. It also provides basic NAC functionality, such as guest access and network quarantine out of the box. The NAC Foundation module—which includes a captive Web portal for user and guest registration—interfaces with third-party authentication and endpoint policy assessment systems, and contains a built-in policy engine. It is fully integrated with the other Infoblox NIOS software modules as well as Infoblox grid technology, benefiting from the native grid benefits, including central administration and high-availability failover.

Voice over IP

Users demand dial-tone reliability for voice communications. To deliver this level of reliability in an IP environment requires a nonstop DHCP service for assigning IP addresses to voice-over-IP handsets and IP soft phones, as well as file delivery services for providing updated phone firmware and configurations. The DNSone package delivers a combination of features that provides an easy-to-manage, high-availability solution for IP voice applications:

High-availability DHCP

Infoblox supports industry-standard DHCP failover that works across distributed WANs. In addition, pairs of Infoblox appliances can be easily configured in “HA mode” to provide fast failover and real-time data synchronization without requiring inefficient allocation of IP addresses.

Built-in TFTP, FTP, and HTTP

Historically, TFTP has been provided by stand-alone servers managed individually at each location with no centralized control and no high-availability capabilities. The DNSone package extends the benefits of network services appliances to managing IP telephony by providing a reliable, easy-to-manage TFTP service. Firmware and configuration files are uploaded to the appliance and served to IP phones when they boot up. Added reliability, expected in a telephony environment, can be provided using an HA pair of appliances to provide reliable TFTP services.

Reliable DNS Infrastructure for Microsoft Active Directory (AD)

Infoblox is a Microsoft Certified Partner and the Infoblox DNSone package includes special support for easy integration into Microsoft AD environments. This enables enterprises to ensure that the critical DNS services needed for their Microsoft and non-Microsoft applications are always available and secure.



Performance and Capacity Specifications

	Infoblox-250	Infoblox-550	Infoblox-1050	Infoblox-1550/2	Infoblox-2000
DNS Queries Per Second	3,000	12,000	24,000	36,000	75,000
DHCP Leases Per Second	25	75	150	225	750

DNS Technical Specifications

RFCs supported 1034 and 1035
 Dynamic update, RFC 2136
 Incremental zone transfer, RFC 1995
 Notification of zone changes, RFC 1996
 Secret key transaction authentication (TSIG), RFC 2845
 Classless IN-ADDR.ARPA delegation, RFC 2317

Protocol engine BIND 9.3.4

- Additional Capabilities**
- Secure dynamic DNS updates using TSIG
 - Conditional forwarding
 - Microsoft Active Directory support
 - Infoblox Views
 - IP-address-based access lists on queries, zone transfers, and dynamic updates
 - Zone import tools
 - Customizable TTL settings

DHCP Technical Specifications

RFCs supported RFCs 3046, 2131 and 1531
 BOOTP, RFCs 1534, 2132, and RFC 4388

Protocol engine DHCPD 3.1

- Additional Capabilities**
- VLSM (Variable Length Subnet Mask) support
 - CIDR (Classless Inter-Domain Routing) support
 - Multiple subnets per segment (supernetting)
 - “Static leases” based on MAC address (manual allocation)
 - MAC-address-based filtering
 - Address availability checking before assignment
 - DHCP relay agent/Option 82 support
 - DHCP Vendor Class Identifier/Option 60 support
 - Secure DHCP-DNS integration updates DNS when leases are issued
 - Advanced DHCP Options Editor
 - Windows, Unix, and Mac OS compatibility
 - External syslog server support

Part Numbers

Infoblox-250 with DNSone Package, 100 Leases	IB-250-100-DNS
Infoblox-250 with DNSone Package, 300 Leases	IB-250-300-DNS
Infoblox-550 with DNSone Package	IB-550-DNS
Infoblox-1050 with DNSone Package	IB-1050-DNS
Infoblox-1550 with DNSone Package	IB-1550-DNS
Infoblox-1552 with DNSone Package	IB-1552-DNS
Infoblox-2000 with DNSone Package	IB-2000-DNS

Infoblox product warranty and services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.