

Simplifying Deployment, Security and Management of DNS/DHCP Services

***IPControl™ Sapphire
DNS/DHCP Appliances***

*By Tim Rooney
Director, Product Management
BT Diamond IP*

Simplifying Deployment, Security and Management of DNS/DHCP Services

IPControl™ Sapphire DNS/DHCP Appliances

By Tim Rooney, Director, Product Management

Introduction

Many organizations have completed at least initial deployments of voice over IP (VoIP) services within their enterprises, or as a service offering for subscribers. Many others are in the process of deployment or are in the planning stages for such a deployment. Pockets of further convergence of video, conferencing, unified messaging, and related IP-based communications applications are emerging within organizations as well. With much if not all of the organization's communications applications running over an IP network, the criticality – not to mention visibility – of maintaining uptime of the network increases dramatically.

Murphy's Law fans, which include most IP network managers, will point out that whatever can go wrong managing a network will go wrong. IP network managers should display a healthy sense of paranoia, and proactively plan to eliminate threats to keeping the IP network up and running. This plan should include:

Network redundancy

Diverse network routing to key infrastructure elements and applications

Minimizing security vulnerabilities

Eliminating misconfigurations

Structured processes for network and software upgrades

Proactive monitoring

Among the key elements underpinning the foundation of the IP network, Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) are critical to proper initialization and usability of IP applications. If a user's computer cannot obtain an IP address, or a VoIP phone cannot initialize via DHCP, users will call the help desk. From their perspective, the network is down. Likewise, if they are unable to connect to applications or other voice users due to DNS failures, they will also consider the network down. There are many services and protocols used by various IP applications, but DHCP and DNS are used by nearly all IP devices for every application for proper initialization on the IP network and for easier usability for network users.

This white paper will offer approaches to streamlining efforts to keep IP networks up and running for critical DHCP and DNS services, then discuss the IPControl Sapphire appliances, which achieve the next level in protecting DHCP and DNS services. First, let's examine the key considerations for threat reduction best practices.

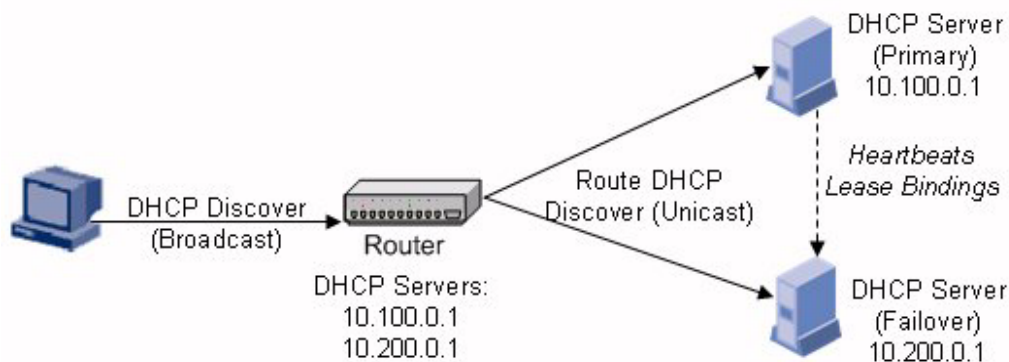
Key Considerations to Reduce Threats to DHCP/DNS

Redundancy

Redundancy has become a standard requirement in networks these days. The DNS architecture, designed over 20 years ago, is redundant by design via its ability to deploy a single master for zone data and multiple slaves, all authoritative for that zone's data. In other words, DNS clients, or resolvers, can query¹ the master or any slave to obtain an authoritative response to a query for a record in the zone in question.

From a DHCP perspective, while the DHCP failover protocol has been slowly moving through the Internet Engineering Task Force (IETF) approval process, many products already support a form of failover, including the Internet Systems Consortium's (ISC's) freely redistributable DHCP server. DHCP failover enables a DHCP client's address request (or Discover packet) to reach two DHCP servers. In the simplest configuration, one DHCP server acts as the primary server for all address pools. The failover DHCP server acts as a backup server, and is configured with the same set of address pools as the primary. Figure 1 illustrates the concept for DHCP failover.

Figure 1: DHCP Failover Configuration



The router serving the network on which the DHCP client is located must be configured with DHCP relay addresses corresponding to the DHCP servers serving this subnet. The router intercepts the DHCP client's broadcast Discover packet, then unicasts it to each of the addresses in its DHCP relay address list. Hence, both DHCP servers normally receive each Discover message. The DHCP servers are configured as primary and failover, respectively, and normally the primary server responds and completes the transaction. As

¹ The resolver need not query directly of course. The originally queried server would iterate until it found an authoritative server to query on behalf of the resolver.

leases are distributed, the primary server communicates lease information to the failover server. If the failover server detects that the primary server may be down via the heartbeat mechanism in accordance with failover configuration parameters, it will assume the role of primary and begin processing lease transactions. From the DHCP client's perspective, it is served with an appropriate IP address and associated configuration options whether from the primary or failover server.

Diverse Networking

Many organizations have learned the hard way that providing diverse routing and deploying resources on multiple sites to provide high availability in the face of network outages is a must. The implementation of multiple DNS servers and DHCP failover are less effective if the multiple servers reside at the same location and/or if a single provider or set of facilities serves the location. Since DNS zone transfers and DHCP failover protocol operate over wide-area networks, deploying server across at least two locations is recommended. This enables a higher probability of reaching a DNS or DHCP server as needed, assuming the local network is not the culprit.

Referring back to Figure 1, assuming the primary and secondary DHCP servers are located in different locations, this configuration supports server redundancy as well as the potential for route and site diversity. Note that the heartbeat mechanism used can indicate server failure, but it may not indicate network unreachability status from the client's perspective. An additional set of parameters can be configured on the ISC DHCP server to enable two servers to share the load of DHCP requests. This load balancing configuration appears the same as in Figure 1. However, when each DHCP server receives the Discover packet, it performs a hash of the client's client ID or client hardware address (chaddr) field. Based on the server's configuration, it will either process the lease transaction, or not, based on whether the hash result meets its configured criteria. This split is performed on a 50/50 basis, where both the primary and failover servers in Figure 1 essentially would be primary, but for only half of the clients (assuming the client IDs or hardware addresses roughly equate to an even split).

The load-balance override parameter in the ISC DHCP server defines a threshold for the number of seconds the client has been attempting to obtain an address. This parameter is typically provided in the DHCP Discover packet header. If this threshold is exceeded for a client for whom the hash algorithm indicated should not be served by this server, it may process the transaction anyway. In this manner, even though the two servers can communicate heartbeats successfully, one server can process lease transactions for the other if clients are not be served in a timely manner, which could be indicative of a client-to-server network issue.

Minimize Security Vulnerabilities

Efforts to minimize security vulnerabilities reverberate throughout the entire IT infrastructure. No element is immune to attack, including DHCP and DNS services. In most cases today, DHCP and/or DNS "application" software are installed on a server running a particular operating system. Such installations on general-purpose computing platforms result in vulnerabilities not only in the DHCP and DNS services themselves, but also at the operating-system level. Common services available on some operating systems, such as rlogin or super user access, enable hackers to gain access to the server, which in turn exposes the DHCP and/or DNS information itself to attack. It also enables the server itself to be used as a "stepping stone" for further infiltration of other applications or servers in the organization.

Many attack types have been well documented, though new forms arise periodically. In general, with the increasing criticality of DNS and DHCP services providing the foundational services of an IP network,

running these services on dedicated servers is recommended. In other words, few if any other services should be running, even at the operating-system level. While many operating-system parameters may be configurable, such as open ports, file and user permissions, and jailed environments, others, such as the boot interrupt process, root or superuser (su) access for certain processes, and daemon or process security, are generally not configurable. Likewise, at the server daemon or application level, many parameters are configurable, although vulnerabilities, such as buffer overflows, can exist.

The BIND DNS service provides a number of configurable parameters to control DNS application access, file system access, as well as access controls on DNS level input/output. While there are a number of such features, including transaction signatures, views, ACLs, options for the server, view, and zone, and control channel access controls, configuring them accurately and consistently across your servers may be challenging. Using a centralized management tool can help with correlation of information across multiple servers, and provide some level of error checking on these parameters to the extent supported by the product deployed.

Beyond supporting transaction signatures to sign DNS updates to a DNS server, most DHCP servers rely on server or operating-system access controls to protect DHCP server information integrity. The bottom line is that the ability to minimize security vulnerabilities is available to a partial degree on today's commercial DHCP/DNS software products. Eliminating misconfigurations of these server products, though, is a challenge.

Eliminate Misconfigurations

Let's face it, configuring DNS and DHCP services properly is complex. And deployment of even mildly complex technologies like transaction signature keys, let alone views, requires a high degree of interserver configuration coordination and correlation to ensure that complementary configurations meet their intended goals. Despite this complexity, many of these configurations should be implemented to protect DNS and DHCP services. Even a basic server configuration can be rather complicated; consider the fact that BIND supports over 90 options and/or configuration directive statements, each with its own set of parameters. An error in configuration can lead to security holes or even the inability to resolve particular host names. Given the criticality of DNS and DHCP to an IP network, misconfigurations are unacceptable, and with the variety of configuration software products on the market, largely avoidable.

A centralized configuration tool can vastly reduce misconfigurations, and help reduce the time it takes to configure a number of DNS and DHCP servers accurately and consistently. Centralizing upgrade and patch management functions can also help simplify that process.

Software and Network Upgrade Process

As bugs are identified and fixed, and new technologies are implemented within DHCP and DNS servers, upgrades must be performed to incorporate these fixes and new features. Oftentimes, compatibility issues arise with respect to supported operating-system versions and patch levels per DHCP and DNS version. Resolving these issues relies on availability of compatible operating system, DHCP/DNS software, and even any hardware upgrades from respective vendors, as well as coordinating the upgrade process for each affected server. This may also require coincident upgrade of more than one server at a time if new interserver features or updates are included in the upgrade. This overall upgrade process can be excruciatingly difficult in terms of vendor coordination, internal interorganizational coordination, testing, deployment, and contingency planning. And if anything goes awry during the upgrade, the backout plan

must be rolled into effect, and the upgrade reattempted later. Ironically, many upgrades result in downtime for particular servers. A mechanism for managing and better planning of upgrades, which will be discussed subsequently, can reduce the headaches involved in this DHCP/DNS upgrade process.

Proactive Monitoring

Keeping an inventory of DHCP and DNS servers operating on the network is certainly a good idea. Beyond a listing of server names, IP addresses, and perhaps login credentials, it is also helpful to understand the current release versions of each server's operating system, DHCP/DNS server software release, and hardware configuration. In addition to these inventory-focused attributes, it is also beneficial to monitor the services themselves to proactively identify servers that may be down or experiencing performance bottlenecks. There have been various tools available to view process states or scan logs or inventory DHCP and DNS servers, but until recently, none of these tools integrated these functions to enable holistic management of key attributes of your DHCP and DNS servers. This shortcoming has been resolved by IPControl Sapphire appliances.

Centralized IP Management with IPControl Sapphire Appliances

In today's environment, where DHCP and DNS software is commonly installed on general-purpose hardware with commercial operating systems, there are still many shortcomings and manual processes involved in effectively managing a number of distributed DHCP and DNS servers. Software-based approaches generally lend themselves well to redundancy and site diversity, but are less comprehensive in terms of security configuration, cross-server configuration, upgrade management, and monitoring capabilities.



Sapphire 10 Series Appliance

BT Diamond IP offers a new approach to solve these DHCP/DNS and IP management issues: IPControl IP address management software and IPControl Sapphire appliances. IPControl software enables centralized configuration, deployment, management, and monitoring for multivendor DHCP and DNS servers, including support of Sapphire appliances. Sapphire appliances

provide extensive security features to minimize vulnerabilities, an additional high-availability option, services monitoring, and more.

IPControl Sapphire appliances provide DNS and/or DHCP services with a prebundled, hardened Linux operating system on a 1U rack-mountable hardware platform. The operating system and associated file system and services are purpose-built, and restricted to those services and functions required to support the appliance's DHCP and DNS operation in a secure environment. The Sapphire appliance's rack-mountable hardware configuration enables deployment as a standalone unit or in a TwinMirror™ configuration with dual back-to-back servers for hardware redundancy. Sapphire appliances provide a common look and feel with sibling IPControl products, and are centrally managed with IPControl.

IPControl Sapphire appliances provide the added benefit of simple deployment – just plug them in and configure them from IPControl. Upgrades are also a snap with the EasyUpdate™ feature, which enables staging and selective deploying of the operating



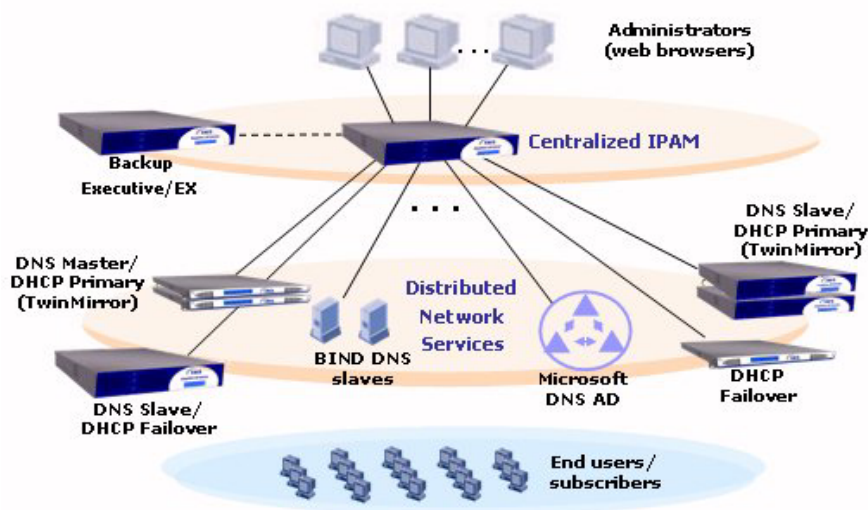
Sapphire 20 Series Appliance

system, IPControl, and DHCP and DNS software updates as they become available. This feature enables lights-out configuration, management, and upgrades to streamline your processes and operations costs.

IPControl Centralized Management

IPControl products provide a comprehensive feature set to streamline overall IP address management tasks. IPControl centralizes IP address block and individual IP address inventory (Figure 3) for rigorous and consistent inventory tracking. Unlike other IP management tools, IPControl includes the ability to discover at the network and individual IP address level with exception reporting to quickly identify discrepancies between the inventory and network actuals. IPControl also supports the deployment of DHCP and DNS configurations to multivendor, multiplatform servers, including native Microsoft and ISC services, as well as the Sapphire appliances from BT Diamond IP. IPControl can scale to manage IP networks from as few as 1000 nodes up to tens of millions of nodes.

Figure 3: IPControl Basic Architecture



The user interface is purely web-browser based with no client software required. Administrator privileges are settable to restrict access to particular resources, addresses, and/or functions within the system. Command line and web services API interfaces are provided with IPControl along with the innovative Callout Manager service to promote integration with external applications.

Redundancy

In addition to supporting multiple authoritative DNS servers and multiple DHCP servers in a failover configuration, IPControl Sapphire appliances can be deployed in a TwinMirror™ configuration, as shown in Figure 4 for a pair of 10 series appliances. TwinMirror capability features two co-located appliances interconnected via a high-speed interface. In this configuration, the appliances mirrors OS and server-level updates to maintain synchronization. The TwinMirror servers appear to DNS and DHCP clients as one server, with one IP address. However, both appliances are independently addressable from IPControl for monitoring purposes. In this active-standby configuration, when a failure is detected, the standby unit assumes the active role, providing seamless DHCP and DNS services to clients.

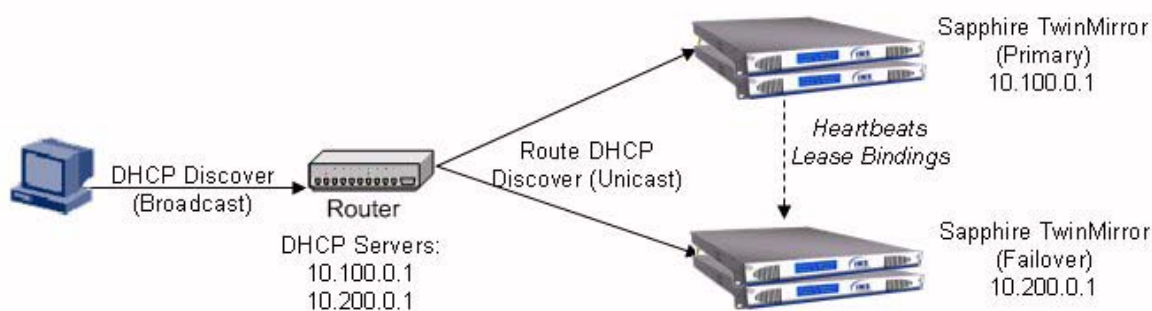
Figure 4: Sapphire TwinMirror

Diverse Networking

The TwinMirror configuration provides additional redundancy beyond DHCP failover and multiple DNS servers as illustrated in Figure 5. TwinMirror deployments provide hardware-level redundancy on top of the respective DNS server-level redundancy and DHCP failover feature. IPControl supports centralized configuration of site-diverse DHCP and DNS servers as single unit deployments per site and/or in TwinMirror configurations. In addition, IPControl eases the configuration of the load-balancing algorithm with automated full load assumption mechanism discussed previously. This enables sharing the DHCP load across servers or server pairs and the ability to assume the full load for the other server or pair based on configurable parameters. This feature streamlines the process and provides an additional redundancy check against network reachability outages.



Figure 5: Site Diverse TwinMirror Failover



Minimize Security Vulnerabilities

IPControl Sapphire x-series appliances are designed as dedicated DHCP and/or DNS servers, while the EX series appliances are designed for centralized management functionality. Both models enable strict control and elimination of extraneous operating system services and structure, as well as extraneous services, users, and ports. Sapphire appliances provide four levels of security:

Kernel security – Sapphire’s Linux-based kernel is purpose-built for the appliance hardware. It provides complex packet filtering and manipulation and does not support file systems not used directly by the appliance. In addition, the kernel implements a controlled and uninterruptible boot process.

File system security – Sapphire includes only the necessary DHCP, DNS, and IPControl binaries, and these binaries and associated data files have no privileged attributes. These services run in a sterile jailed environment, which provides no access to other components on the appliance or via network connections from the appliance in the unlikely event an attacker gains access.

Process security – DNS and DHCP services startups are controlled by a managed launch binary, which performs over eight different security checks during the startup process. DNS and DHCP libraries are separate from system libraries and DHCP, DNS, and IPControl services run in a sterile environment. In addition, DNS and IPControl services run as unprivileged processes.

Network security – Sapphire opens only network ports required for use by SSH, DHCP, DNS, and IPControl; all other ports operate in stealth mode, not responding to packets. The management interface is secured via an SSH connection. TwinMirror high availability and data mirroring traffic is run over a private high-speed network between the nodes.

Sapphire’s multiple levels of security minimize the risk of intrusion into critical DHCP and DNS services. And should an attacker gain access to the appliance, there is little to nothing that can be leveraged within the sterile environment.

Eliminate Misconfigurations

While employing an appliance solution provides many security and ease-of-deployment benefits, each appliance must still be configured accurately. This is where many appliance-based solutions fall short. While some require per-server configuration, which is minimally better than editing BIND or DHCP configuration text files, others do provide the ability to configure “like” configurations across more than one server. However, this approach is still services-focused and not IP address-focused, in that it enables configuration of DNS independent of DHCP and independent of the IP address plan.

Only IPControl enables centralized modeling of your entire IP address space, with hierarchical and topological allocations and derivation of associated DHCP and DNS configurations from the same consistent inventory. This functional integration saves time and improves accuracy as it leverages a common inventory database to create consistent configurations and updates for DHCP and DNS, while facilitating IP address and capacity management.

Software and Network Upgrade Processes

Depending on your hardware, operating system, and DHCP/DNS vendors of choice, upgrades may be required at different times with varying levels of compatibility. A wider breadth of compatibility would enable use of the same DHCP/DNS software on multiple (broader) numbers of operating systems versions and patch levels. While this may ease the burden during intermediate upgrades, ultimately it's difficult if not impossible to escape the tedium of multiplatform upgrades planning and execution. However, this tedium can be greatly reduced with the use of IPControl and Sapphire appliances.

If this sounds too good to be true, it isn't! IPControl provides visibility into each appliance deployed on your network in terms of the current operating system, DHCP version, DNS version, and IPControl services version. BT Diamond IP provides proactive updates at each of these levels to enable downloading and staging of updates, and then deploying them to either all appliances, or a subset of appliances as deemed necessary – all from the IPControl interface. This functionality, along with a selectable backout option, vastly simplifies the overall upgrade process while providing complete control. Updates, patches and changes are logged by the system for reporting and auditing. And all software updates at these levels are tested on Sapphire hardware to assure compatibility with the appliance hardware configuration.

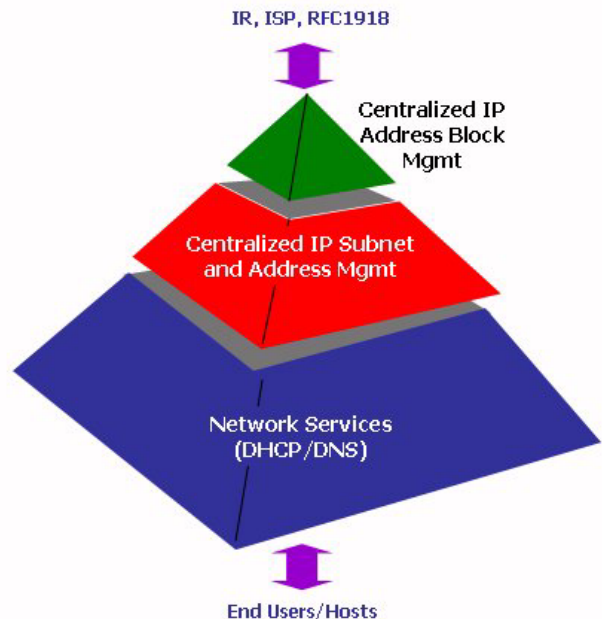
Figure 6: IPControl IP Address Management Breadth

Proactive Monitoring

In addition to managing version levels of each Sapphire appliance, IPControl provides monitoring of the status of each appliance to assure services operation. IPControl provides a dashboard summary of the status of all appliances, broken down by service status for DHCP, DNS, IPControl and system. The IPControl dashboard enables drill-down into detailed state and event information and execution of services start, stop, reload, and more. This proactive approach provides a single window into all of your DHCP/DNS appliances to simplify configuration, management, and monitoring of these critical services.

Why Not a Server-Level Approach?

A number of vendors in the IP management marketplace feature DHCP/DNS server level approaches that provide many of the security, deployment, and upgradeability benefits discussed in this paper. However, these products provide limited to no centralized management, with a few providing only cross-server services-based configuration and management. BT Diamond IP offers the best of both worlds with all the security, deployment, and upgradeability benefits of an all-appliance-based approach with IPControl's holistic, centralized management solution.



Centralized management of IP address space and DHCP and DNS servers simplifies and integrates the IP management functions within an organization, saving time, automating tasks, and reducing configuration errors in the process. In addition, many customers operate a number of DHCP and DNS products from different vendors.

IPControl provides overall IP block allocation and management, individual IP address inventory and management, along with multivendor DHCP and DNS configuration and management, including Microsoft, BT Diamond IP, ISC, and Sapphire appliances. IPControl is the only comprehensive solution!

Conclusion

Table 1 compares the basic approaches to best practices outlined in this paper with respect to keeping DHCP and DNS services up and running. As the table shows, the IPControl Sapphire solution provides many advantages over a software-only and appliance-only approach.

Table 1: Comparison of IP Management Solutions

Best Practice	Software-Only Approach	Server-Only Approach	IPControl Sapphire Approach
Redundancy	Multiple DNS servers and DHCP failover	Multiple DNS servers, DHCP failover, and hardware redundancy	Centralized configuration of multiple DNS servers, DHCP failover, and hardware redundancy
Diverse Networking	Deployment of multiple servers across multiple sites Limited load balancing	Deployment of multiple servers across multiple sites Load balancing varies by vendor	Deployment of multiple servers across multiple sites with centralized configuration of multiple servers, failover, and load balancing
Security	Limited DNS options support for ACLs No tools for OS config.	Improved OS- and DHCP/DNS-level security	Four levels of advanced security for kernel, file system, process, and network security with centralized configuration of complex DNS security features and directives
Eliminate Misconfigurations	1-2 centralized solutions available to improve consistent and accurate configurations	General configuration integrity checks for DNS and DHCP independently Little cross-server or IP address integrity checking	Centralized cross-server configuration consistent with the IP address plan simplifies policy and configuration deployment and improves accuracy
Upgrades	Challenging coordination of hardware, OS, and server level software versions with no central, per-server version tracking	Most appliance vendors provide automated OS and server upgrades, though limited central per-server version tracking	Automated upgrades of OS and server versions with ability to track and selectively deploy specific versions per server

Monitoring	No integrated OS, services and server monitoring	Limited to no availability	Centralized view of all appliances with state information, drill-down, and action points
------------	--	----------------------------	--

The IPControl suite of software and Sapphire appliances provide an advanced, next-generation IP management solution that enables automation of many tedious, error-prone, yet crucial IP management functions across the entire lifecycle of an IP address. This lifecycle spans from obtaining address blocks from Internet Registries or ISPs, to automated address block allocations across the network topology, to IP subnet and individual address inventory management, to DHCP and DNS server configuration and deployment, to DHCP/DNS server software and/or Sapphire appliances. IPControl provides unsurpassed extensibility and user-definability to enable management of IP address space and is available as a total appliance, total software, or mixed and multi-vendor deployment configuration. To learn more about how IPControl products can automate more of the IP management functions you need at an exceptional ROI, email diamondip@bt.com.

About BT Diamond IP

BT Diamond IP is a leading provider of software and appliance products that help customers effectively manage complex IP networks. Our next-generation IP management solutions help businesses more efficiently manage IP address space across mid-to-very large sized enterprise and service provider networks. These products include IPControl™ for comprehensive IP address management, Sapphire Appliances for DNS/DHCP services deployment and NetControl™ for full-cycle IP address block management and utilization. Our cable firmware management product, ImageControl™, helps broadband cable operators automate and simplify the process of upgrading and maintaining firmware on DOCSIS devices in the field. Our customers include regional, national and global service providers and enterprises in all major industries. For additional information, please visit bt.diamondip.com or contact BT Diamond IP at 1-800-390-6295 in the U.S. or 1-610-423-4770 worldwide.

Diamond IP, IPControl, TwinMirror, and EasyUpdate are trademarks of BT INS, Inc.

Copyright © 2007, BT INS, Inc.

This is an unpublished work protected under the copyright laws.
All trademarks and registered trademarks are properties of their respective holders.
All rights reserved.