

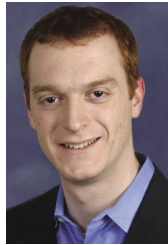
May 10, 2007

Taking IP From A Commodity To A Utility

by Robert Whiteley

TRENDS

TRENDS



May 10, 2007

Taking IP From A Commodity To A Utility

Network Operations Must Master DHCP, DNS, And RADIUS To Support IT

by **Robert Whiteley**

with Galen Schreck and Christine E. Atwood

EXECUTIVE SUMMARY

Today's networks are part of a mission-critical IT infrastructure fabric. They provide the "dial tone" of IT — an always-on, always-available service for connecting to data and applications. But most companies don't invest in the infrastructure that's needed to support this dial tone. Forgotten services like DHCP, DNS, and RADIUS are critical network services components that dictate availability. Yet most are woefully out of date, stagnating on non-enterprise-grade infrastructure, with few security mechanisms. To prevent your network from becoming an IT bottleneck, you must build a utility-grade network; one where devices and services just plug in and work. How? By first transitioning your services off commodity hardware to newer appliances and, secondly, investing in the proper IP address management (IPAM) tools.

TABLE OF CONTENTS

2 **The Plight Of The Network Renaissance Man**

Today's Networks Rely On An IP Services Backbone Of DHCP, DNS, And RADIUS . . .

. . . But Few Firms Invest In These Enterprise-Grade Network Foundations

5 **Empower Network Ops And Invest In A Utility-Grade Network**

Three Companies That Typify Utility-Grade Networks

RECOMMENDATIONS

7 **Decide If You're Striving For A Homogeneous Or Heterogeneous IP Fabric**

WHAT IT MEANS

8 **DNS Is The New Black Art**

NOTES & RESOURCES

Forrester interviewed several vendor and user companies, including: BlueCat, BT, DNSstuff, Infoblox, and Secure64.

Related Research Documents

["IP Address Management \(IPAM\)"](#)

December 4, 2006, Essentials

["The Evolving Branch Office: Intelligently Reducing Your Network Infrastructure Footprint"](#)

October 4, 2006, Best Practices

["IP Address Management"](#)

June 18, 2004, Market Overview

TARGET AUDIENCE

IT infrastructure and operations professional

THE PLIGHT OF THE NETWORK RENAISSANCE MAN

Today's network operations group is under revolution. Ten years ago a network was pretty simple: routers, switches, hubs, and some plumbing connecting it all together. But fast-forward to today, and it's an entirely different story.

- **Applications are no longer an overlay.** Networks aren't just simple transport. Today's networks are truly converged, offering voice, video, and data services. But it doesn't stop at collaboration applications. Vendors like Cisco, with its Service-Oriented Network Architecture (SONA), and 3Com, with its Open Services Networking (OSN) initiative, are now offering the ability to host applications directly in network-resident middleware. Although not suited for all applications, these new platforms blur the line for virtualization, location-based, and presence-aware apps.
- **Security is part of the fabric.** Just as voice is an embedded network application, security is an embedded part of the architecture. Today's switches, routers, and appliances all serve up firewall, intrusion prevention, access control, and wire-speed anti-x technologies. The network embeds these functions directly into the infrastructure, providing a coordinated security control plane for a defense-in-depth strategy across the enterprise.
- **Management is real-time visibility.** Network management tools have also evolved. Rather than just basic element management, today's systems now give a single, comprehensive view into today's operating environment. Many use network probes or NetFlow to build a detailed statistical view of network performance. Similarly, popular devices like WAN optimization appliances provide real-time windows into the behavior of traffic leaving the data center. Coupling this visibility with emerging network change and configuration management tools provides a feedback loop for managing the full network life cycle.¹

So what does this mean for today's network administrators and engineers? First, it means that they need to evolve skills to cope with modern network architecture. Security, voice, and performance monitoring merge with existing responsibilities like chasing down network outages and troubleshooting misconfigured routers. But more important, it means that the tools must evolve as well. Today's network operators must refocus on core network infrastructure — namely DHCP, DNS, and RADIUS — to lay the foundation for the next generation of IT services.

Today's Networks Rely On An IP Services Backbone Of DHCP, DNS, And RADIUS . . .

Three services are necessary for network operations to ensure that it can scale to meet today's applications: dynamic host configuration protocol (DHCP), domain name service (DNS), and remote-access dial-in user service (RADIUS). Combined, they are the "dial tone" of your IP network. None of these technologies are new, though — on the contrary, these technologies are all a decade or more old. But each is a key component in the success of IT's networked initiatives (see Figure 1).

Figure 1 Your IP Network Requires Three Foundational Services: DHCP, DNS, And RADIUS

Component	Critical underpinning for . . .	What clients are saying
DHCP	IP communications, mobility, network access control	"Our M&A activity out-paces our ability to assign new resources." — Health insurance firm
DNS	SIP-enabled communications; Web services and applications	"SIP rollout of 6,000 desktop phones is like a DoS attack on our DNS server." — Large retail bank
RADIUS	Guest access, secure remote access	"Our NAC deployment didn't enjoy our 10-year-old, freeware RADIUS." — Oil and gas company

42151

Source: Forrester Research, Inc.

- **DHCP gets you on the network: It provides digital connectivity.** After any device has physically connected to a network, its next step is to request an IP address. No device can transfer data — or many cases even compute — without this level of logical connectivity; this includes traditional systems like PCs, printers, phones, and handheld devices and also covers an ever-expanding world of refrigerators, life-support machines, and HVAC systems. More advanced solutions go further and leverage DHCP combined with services like TFTP to automate configuration provisioning, not just IP addressing.
- **DNS directs you around the network: It provides the new routing layer.** DNS kicks in as networks evolve beyond basic transport to application-savvy platforms.² It transforms a complex web of numbers into plain-English phrases — a necessary abstraction layer to support SIP-based communications, Web services, and any Active Directory-enabled application.
- **RADIUS controls where you can go: It provides necessary tracking.** With a foundation of connectivity and routing set, next up is authorization, authentication, and accounting (AAA). The triple-A services are critical for providing secure access from remote, wired, and wireless mediums. Coupled with built-in functions like 802.1X, RADIUS is part of a good network access control (NAC) solution as part of a layered defense.³

. . . But Few Firms Invest In These Enterprise-Grade Network Foundations

DHCP, DNS, and RADIUS — which we refer to as foundational network services — make up the base of your firm's IP fabric. Yet enterprises use a hodgepodge of technology to build this foundation. The result? A network that is (see Figure 2):

- **Unreliable.** Most DHCP, DNS, and RADIUS servers are not deployed on enterprise-grade components. These foundational network services often share resources on a general-purpose server with other services like file sharing, printing, and caching. Even if you dedicate server resources, most firms tend not to use redundant components nor architect systemwide failover options. The unintentional consequence is a faulty set of core services.

- **Non-scalable.** Scaling network services in an increasingly flat world is difficult. DNS is the backbone of a globally distributed company, but are your DNS servers scalable themselves? Few companies invest in the necessary distribution of DHCP, DNS, and RADIUS servers to scale services, often keeping them centralized. And even if firms have distributed these servers, they often find it hard to control them in a cohesive manner; adding additional capacity is equally difficult.
- **Insecure.** We’ve come a long way in embedding security into our network infrastructure. Yet we still see several cases annually of DNS servers — often running the aged BIND service — that have been compromised.⁴ Most foundational network services have no built-in security mechanisms, since they were designed in an era when IP networks were controlled by a handful of trusted government, carrier, and educational organizations. Even fewer services are protected with the standard array of threat protection technologies that secure Web and application servers.
- **Unmanageable.** Non-strategic assets can be entrusted to freeware and shareware components with lackluster management and support. But the rise in importance of foundational network services means you should rethink that strategy. Network professionals used to just worry about Cisco-like CLIs for router configuration, but today they need sophisticated management GUIs for zone, domain, and user policy configuration.

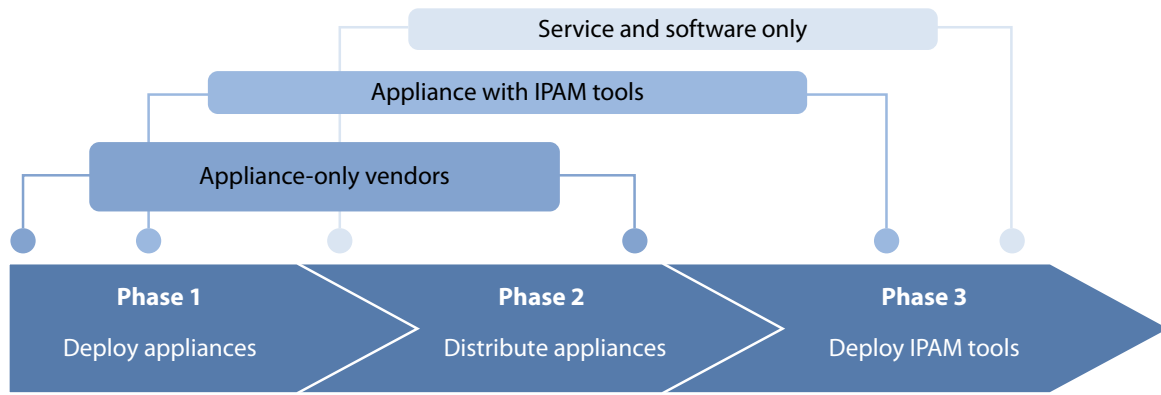
Figure 2 Networks Suffer From Investment And Architectural Neglect Of Foundational Services

Attribute	Where typical network services fall short	Questions you should be asking about your foundational services
Unreliable	Lack of dedicated infrastructure and architectural redundancy	Do your foundational network services seamlessly failover to backups — on a global basis?
Non-scalable	Lack of global distribution or cohesive control to scale services	Do your servers scale to all of your branches, even if your WAN link is severed? Can you scale services during disasters, even when 80% of users are working remotely?
Insecure	Unpatched systems and lack of built-in DoS mitigation	Have you sufficiently protected servers from exploits and denial-of-service (DoS) attacks?
Unmanageable	Predominantly older shareware and freeware components	Do your servers have sophisticated management interfaces? Do they have enterprise-class support?

EMPOWER NETWORK OPS AND INVEST IN A UTILITY-GRADE NETWORK

Overcoming flaws in your foundational network services means proper investment and a solid architecture. But how do you get started? First, put your network operations team in charge. Many companies still keep DHCP and DNS as a server admin function. We don't recommend this, as it creates too many inefficiencies in identifying, isolating, and resolving IP issues. Besides, everybody is pointing fingers at the network staff anyway; you might as well empower them to properly troubleshoot. With network operations firmly in charge, we then recommend a three-phase approach (see Figure 3):

- **Phase 1: Deploy purpose-built hardware.** The first step is to remove the aging freeware and end-of-life software that run your IP fabric.⁵ With or without your network staff in charge, you should dedicate appliances to the task. They overcome the reliability, scalability, and security woes that plague most foundational network infrastructure. Look to BlueCat and Infoblox, which both supply top-notch integrated appliances.⁶ BT Diamond IP (formerly International Network Services or INS) and Lucent offer solid software solutions supported on appliance; BT supports its own appliance, and Lucent partners with Infoblox.⁷ And finally, emerging vendors like Secure64 also show promise for creating ultra high-end hardware platforms.
- **Phase 2: Distribute components for scale and performance.** The next step is to scale your entire network by distributing the appliances. At a minimum, you should focus on a redundant architecture that supports failover among all your global data centers. However, consider application and user performance. If you have a critical application like point-of-sale software or a large set of mobile field agents, then consider deploying appliances to all your remote and branch offices. We recently spoke with a large North American grocer deploying 6,000 appliances to cover its retail footprint.
- **Phase 3: Layer on management software.** A distributed, appliance-based architecture is the bedrock of your utility-grade network. To truly solidify your network, though, it needs to be well-managed. IP address management (IPAM) tools from the same appliance vendors mentioned above — BlueCat, Infoblox, and BT — are a good start. If you're sticking with servers, consider telco specialists like Nominum and Men & Mice, which that are now targeting the enterprise space. Finally, consider an outsourced alternative like NeuStar if you're too resource-strapped to manage the appliances in-house.

Figure 3 Map Vendors To The Appropriate Phase Given Their Appliance, IPAM, Or Services Heritage

42151

Source: Forrester Research, Inc.

Three Companies That Typify Utility-Grade Networks

Utility-grade IP is critical for today's enterprise. These three examples all typify our three-phase approach. Each deployed a hardened appliances and IPAM combination.

- **Fortune 200 financial services company reduced DHCP and DNS support load by 85%.** One of the US's largest financial services firms with more than 300 sites needed to support 30,000 to 40,000 total users and devices on its network. In doing so, its Unix-based system — comprised of DNS, DHCP, and IPAM running on Solaris with a Sybase database — was maxed out and reaching end-of-life. Moreover, the network team was in a constant tug of war with its server admin colleagues. Why? Because network operations didn't have the necessary root-level access to make changes to the DNS and DHCP servers. To solve the problem, the company turned to Infoblox and deployed 20 of its appliances in its two-data-center architecture. With the right hardware and management tools in place, network operations reduced 85% of the burden of supporting its foundational network services. The company further cited its new utility-grade network as aiding in the seamless migration to enterprisewide VoIP.
- **Whirlpool consolidates 10 to 15 disparate systems down to one.** As a result of supporting 80,000 users, Whirlpool's network had grown to include 10 to 15 disparate DNS and DHCP systems sprinkled across its 277 locations. These included built-in Microsoft services, Cisco's Network Registrar, and more than six implementations of BIND alone. Whirlpool's network team selected BlueCat as its standard DHCP, DNS, and IPAM appliance vendor. Ultimately, Whirlpool will support 10 appliances: two centralized management consoles supporting eight appliances across its two data centers. Whirlpool dedicates redundant pairs to internal (employee) and external (partner) connectivity in each data center. Its business case for a utility-grade network rests on three tenets of a centrally managed system: 1) quickly integrating assets from its 2006 Maytag acquisition; 2) reducing ongoing maintenance costs; and 3) reducing configuration issues with automated error checking and role-based access. Next up: Whirlpool's network operations team is working with its Active Directory team to standardize on BlueCat for all foundational network services.

- **Global shipping and logistics company looks to consolidate 4,000 servers down to 30.** One of the world's largest shipping and logistics companies supports more than 100,000 users in 200 countries. It used to have 3,500 DNS zones on more than 4,000 servers running a mix of BIND and Microsoft. Why so many? Because it's averaging a global acquisition every year, with each introducing legacy infrastructure, its own unique DNS layout, and associated operations. To simplify the environment, this company selected INS' IP Control (now part of BT). It's currently consolidating its core DNS infrastructure to 30 appliances across three global data centers. The INS deployment — with each appliance processing 12,000 queries per second, which is less than 1% load — provides secure foundational services that will accommodate the company's aggressive growth plans. Specifically, its new simplified three-tier hierarchy increases reliability, improves performance, and decreases operational costs. The solution is run by its networking operations team with responsibilities to scale and secure all ingress and egress networking technologies.

RECOMMENDATIONS

DECIDE IF YOU'RE STRIVING FOR A HOMOGENEOUS OR HETEROGENEOUS IP FABRIC

The majority of utility-grade DHCP, DNS, and RADIUS technologies are produced by the IPAM vendors. IPAM was a software-only technology three years ago, but now all vendors supply solutions that replace commodity hardware and software with a unified suite of services. All the vendors above are worth shortlisting, but we recommend that you go with:

- **Infoblox or BlueCat, if you're replacing and bulletproofing infrastructure.** If you haven't started the three-phase approach — or you have a greenfield opportunity to build a utility-grade network — then start with an appliance-oriented vendor like Infoblox or BlueCat. Why? Because these vendors offer a one-stop solution for core services like DHCP and DNS, in addition to the real-time management for plug-and-play utility-grade infrastructure.⁸ Infoblox goes a step further to integrate RADIUS on its infrastructure. Both vendors have unparalleled hardware platforms and are rounding out impressive IPAM capabilities. These vendors provide the best foundation and investment protection.
- **BT Diamond IP, if you're skipping the first two phases.** You may already have a strong enough DHCP, DNS, and RADIUS infrastructure. Or perhaps you've just made a very large investment in Microsoft Active Directory and feel you have "good enough" foundational network services with your Windows servers. If that's the case, BT/INS' heritage in the IPAM space (although it does make appliances) and its ability to seamlessly layer management software on existing architectures are best-suited for your heterogeneous environment.
- **A DNS specialist, if you need post-sales support.** You may still need help with configuring your deployment after you've laid the technology groundwork. DHCP and RADIUS are straightforward, but getting DNS right is a complicated procedure. The pre- and post-sales

support of your infrastructure vendor is the right place to start, but we also recommend engaging the professional services arm of a vendor like Infoblox or explore resources online like DNSstuff.com. The additional tools and consulting services will verify your deployment and develop an ongoing methodology for operations staff to continuously audit the configuration.

WHAT IT MEANS

DNS IS THE NEW BLACK ART

IP is the dominant protocol of networking. Even the supporting cast of protocols — networking heavyweights like Ethernet, TCP, and MPLS — are emerging as clear standards. So networks truly are a commodity, right? Wrong. Transitioning to a utility-grade network means that the emphasis is no longer on layers 1 through 4 in the OSI stack. DNS is the new black art of networking, not routing. Few companies do it well, and even fewer have the skill set to scale it; best practices are rarely documented, never mind automated. The next wave of acquisitions will include traditional network equipment makers feasting on the IPAM appliance vendors that help tame this emerging skills gap. BT's acquisition of INS was just the start.

ENDNOTES

- ¹ The use of IT governance and improved management processes frameworks — in combination with the right management tools — prevent downtimes due to network configuration errors. Forrester recommends implementing automated tools — which we call network change and configuration management (NCCM) — from vendors like AlterPoint, Voyence, or Opsware. See the February 14, 2007, Tech Choices “[Who Has Changed My Network?](#)”
- ² We surveyed companies to see if they prefer a “smart” network (one with embedded intelligence like security, virtualization, and optimization technologies) or a “dumb” network (one with simple “plumbing” that just routes and switches). According to our survey respondents, this debate has been settled: Smart networks have won. Companies, regardless of size, region, or industry, overwhelmingly prefer to use smart networks in their architecture. Hardware advancements, more sophisticated network software, and better management tools mean that firms can reliably embed intelligent security, mobility, virtualization, and acceleration directly into the network. See the September 8, 2006, Trends “[The Debate Is Over: Businesses Prefer Smart Networks.](#)”
- ³ Forrester defines network access control (NAC) as a mix of hardware and software technologies that dynamically control, based on their compliance with policy, client systems’ access to networks. NAC supports pre- and post-admission compliance checks that effectively block the bad guys from getting on the network and show the door to legitimate users who don’t comply with company policy. See the December 4, 2006, Essentials “[Network Access Control \(NAC\).](#)”
- ⁴ In 2007 we’ve already seen a slew of DNS-related issues like GoDaddy’s March outage (affecting millions of Web sites) and DreamHost’s April outage. This adds the major Internet companies like Google, Akamai, and Comcast, which have all suffered DNS outages in the last two years.

- ⁵ It's more common to see strong vendor support for DHCP and RADIUS servers, including solutions from vendors like Cisco, Microsoft, and Juniper. But the most infamous open source component is BIND's (Berkeley Internet Name Domain) version nine DNS server. Although a tested platform, BIND often needs additional security and management capabilities layered on top.
- ⁶ MetaInfo is another appliance vendor worth mentioning, but it was acquired by NeuStar in January 2007. NeuStar is currently looking to offer an internally managed service. For more information, see the MetaInfo announcement: www.metainfo.com/index.cfm/page/AboutUs.
- ⁷ BT announced its intent to acquire International Network Services (INS) on February 1, 2007. INS specializes in four major areas: enterprise architecture and governance, business productivity, information risk management, and infrastructure transformation. Its Diamond IP (DHCP, DNS, and IPAM) products will be folded into BT's Global Services. For more information, see the INS February 1, 2007, press release, "BT to Acquire INS, Expanding Professional Services and U.S. Footprint" (<http://www.ins.com/about/pressroom/pr.aspx?id=2061>).
- ⁸ Infoblox and Blue Cat both offer an integrated appliance with DNS, DHCP, and IPAM tools. Infoblox also offers RADIUS. The solutions differ, however, in that BlueCat supplies a two-tier solution where a "master" appliance named Proteus manages the distributed Adonis appliances that run the network services. Infoblox offers a solution where no "master" management appliance is needed and is instead a distributed function across all of its network services appliances.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations,
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (NASDAQ: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 23 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.