

VIRTUALIZED DDI

Dipl.-Math. Jürgen Joswig

EMEA Sales Director
Nixu Software
Immenkamp 3
30926 Seelze OT Velber
Jurgen.Joswig@nixu.com
emea-sales@nixusoftware.com

Abstract: When talking about virtualized computing environments, virtualization of the IP and core network services such as DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol) and IP Address Management are rarely thought of. This document provides a brief introduction to the Why & How of an end-to-end virtualized DDI solution with related technical, administrative and commercial benefits. It further discusses the advantages of adhering to emerging networking standards, including significantly increased level of security.

1 Introduction to Server Virtualization

The hardware of today's x86 computer was designed to run a single operating system and a single application, leaving resources of these machines most time in idle mode. Using virtualization multiple virtual machines are available on one single physical computer and all virtual machines share the real resources of this one physical computer. High flexibility is given as different virtual machines can run different operating systems and multiple applications on the same physical computer.

Today's virtualization platforms provide a business-ready architecture and "virtualize" hardware resources of x86-based machines - including CPU, RAM, HDD, Controller and Interfaces - to create fully functional virtual machines that can run their own applications on different operating systems and so behave like 'real' computers with each of these virtual machines providing a complete system.

A thin layer of software dynamically allocates hardware resources and multiple operating systems run concurrently on a single physical computer, sharing hardware resources with each other. By encapsulating an entire machine, including CPU, memory, operating system and network devices, a virtual machine is completely compatible with all standard x86 operating systems, applications and device drivers. Thanks to this innovative approach, one can build an entire virtual infrastructure, scaling across hundreds of interconnected physical computers and storage devices utilizing proven virtualization systems. This results in a platform that can be used to build clouds, without the need to assign servers, storage, network bandwidth and priority permanently to each application. The virtualization 'Hypervisor' dynamically allocates hardware resources when and where they are needed within the cloud.

Because of this flexibility, server virtualization simplifies platform management by separating the hardware and thin software layer allocating system resources, thereby translating to significant savings in terms of computing platform TCO and OPEX. Furthermore, by separating the hardware platform from the applications and services run on the virtualized computing platform, virtualization environments allow organizations to increase the level of availability of network services and applications and cut costs.

2 Introduction to Emerging Network Standards: IPv6, DNSSEC

2.1 IPv6

According to recent reports by NRO (Number Resource Organization), the allocation of available IPv4 blocks has seen a significant increase during Q1 2010. In early Q2 2010, only 7.8% of IPv4 space remained free for allocation, and the available IPv4 space is now expected to exhaust by as soon as 2011. Although IPv4 is expected to co-exist with IPv6 well into the 2010s and early 2020s, a gradual shift to IPv6-based networking seems inevitable, especially as organizations such as OECD are now promoting global adaptation of the second generation IP protocol.

In comparison to IPv4, IPv6 will add a significant amount of complexity into managing DDI services. The added complexity stems from the fact that while IPv4 addresses were simple enough for network administrators and other users to remember and enter manually, the syntax of IPv6 addresses and the vast size of IPv6 spaces introduces new complexities into network management routines and processes that cannot be coped with manually. Due to this, the introduction of IPv6 and dual-stack networks is likely to bring about the use of next generation DDI management solutions and tools.

2.2 DNSSEC

After the Kaminsky vulnerability was made public in the summer of 2008, it became widely accepted that the inherent design of DNS is not secure, making this core network service vulnerable to man-in-the-middle, DNS cache poisoning and other similar forms of malicious attacks. While the related risks were mitigated for the time being by randomizing the source ports used in name resolution, the mitigation was in fact bypassed by Russian physicist Polyakov shortly after patches to widely used DNS server types were released. While Polyakov's approach to bypass the randomization of source ports was based on brute force possible only in laboratory environment, it is likely that the introduced method can be also used against production DNS servers in the future as more powerful CPUs and higher amount of bandwidth become available.

To address this issue, the global networking community is now making a move towards the worldwide deployment of DNSSEC (DNS Security Extensions), a standard allowing DNS zone data to be signed in order to assure the authenticity of the name resolution process. The implementation of DNSSEC relies on public and private keys used to sign zone data – much in the same way as in PKI (Public Key Infrastructure) – allowing a chain of trust to be established all the way from the root DNS servers to the client resolving domain names. The DNS root will be signed on July 2010, preceded and followed by a number of ccTLDs (country code Top Level Domain) and gTLDs (generic Top Level Domains) such as .se, .bg and .org.

At the time of the writing, it seems quite likely that most of the 296 TLDs will be signed by the end of 2012.

From the network and DNS management perspective, DNSSEC presents three challenges to system and network administrators. First, when zones are signed, the number of resource records increases by the factor of 4-5, increasing the number of resource records in one's DNS. Second, formerly static DNS entries will become dynamic when signed, because the keys used to sign zones have to be rolled-over on regular intervals. Third, as signed zones contain resource records that are effectively very long keys, adding the keys manually becomes increasingly error-prone and tedious. Given these complexities, successful deployment of DNSSEC requires that the DNS management processes are automated. However, once automated, managing DNSSEC enabled environments is not more difficult than managing traditional DNS environments. In fact, the introduction of DNSSEC support to one's DNS management process is actually likely to reduce the related network management overheads, because the automation is not restricted to DNSSEC only but covers the entire process.

3 Virtualized DNS and IP Addressing Environments

Much of the discussion around virtualization has insofar focused on APPLICATIONS and STORAGE; virtualized DEVELOPMENT PLATFORM; and the NETWORK itself through virtual switches. Core network services such as DNS, DHCP and IP Address Management rarely come up in this context. However, considering the mission critical nature of core network services as well as the scalability and reliability requirements associated with them – and the fact that dedicated servers used to run network services utilize a rather low percentage of their CPU most of the time – running core network services in virtualized environments that optimize the use of computing resources available to them is often the most cost-efficient way of tackling these requirements.

As organizations initiate server virtualization projects in their operating environments, core network services such as **DNS** and **DHCP** make a perfect candidate for virtualization. Because of the high costs and inflexibilities associated with traditional, hardware based DNS and IP addressing computing appliances, most organizations have implemented existing D-services (DNS, DHCP) by utilizing unsupported open source software (BIND, DHCPD) or generic Microsoft server products (Microsoft AD) on industry standard servers. These home-grown servers typically utilize a very low percentage of their CPU. They are also prone to vulnerabilities, unnecessarily tedious to manage, and require on-going maintenance. Virtualization is an excellent way to streamline these inefficiencies.

Furthermore, when preparing the introduction of emerging network technologies such as DNSSEC and IPv6, organizations running TCP/IP networks are required to re-design and re-think their existing network architecture and network management processes as far as DNS, DHCP and IP Address Management is concerned. This creates a logical discontinuity point during which the DDI environment can easily be migrated to virtual computing environment. When deploying a virtualized DDI environment, rather than re-building new virtual machines manually, the easiest way to virtualize any network service is to use productized software packages known as **virtual** or **software**

appliances. A software appliance is a self-installing server optimized for a specific task. It contains all software components required for an installation from a hardened operating system to all necessary tools and application(s). Distributed as an installation media (ISO image) that can be used to boot up new virtual machines in just minutes, software appliances automate installation and maintenance processes thereby translating to higher productivity and lower total cost of ownership.

3.1 Benefits of Virtual DNS and DHCP Infrastructure

1. Optimization of CPU utilization and consolidation of computing resources as DNS and DHCP servers are migrated on virtual platforms
2. Savings in hardware and maintenance costs through decreased number of physical servers in the network, software appliance usage, and centralized management
3. Enhanced availability through continuous uptime offered by advanced virtual environments
4. Rapid and flexible deployment, improved scalability through software appliance usage
5. Higher level of information security thanks to purpose-built, hardened software appliances optimized for a specific service

3.2 Virtualization Enables Better Security, Efficiencies

In traditional network environments, DNS and DHCP services are typically run on industry standard servers that host a number of different network services. While pragmatic, this deployment strategy involves several disadvantages:

1. Scalability issues: running several network services on a single server translates to limited scalability during busy-hours and traffic peaks.
2. Single point of failure: if the hardware platform fails, all network services provided by that server will become unavailable.
3. Vulnerabilities: when running several network services on a single server, vulnerability in any one piece of software can make all services running on that server vulnerable to exploitations.
4. Compromises in server and system management: running several network services on a single server translates to compromises in management and maintenance processes.
5. Inflexible deployment processes: making changes or new additions to network architecture is unnecessarily complicated as different network services have been bundled together.

The easiest and the most cost-efficient way to eliminate these problems is to install and run DNS and DHCP software appliances in virtual infrastructure as dedicated virtual machines. Thanks to their purpose-built design and automated software updates, software appliances are less prone to vulnerabilities and provide efficient tools for uncompromised server and system management. By auto-installing on advanced

virtualization platforms they offer better scalability, higher availability, and flexible deployment options.

3.3 Software Appliances for DNS, DHCP and IP Address Management

- **Nixu NameSurfer Suite (NSS)** is a secure management system designed for efficient, distributed management of organizations' DNS data and IP address space, supporting emerging technologies such as DNSSEC and IPv6.
- **Nixu Secure Name Server (SNS)** is a secure stand-alone server that can be operated as authoritative and/or as caching/recursive DNS server, supporting emerging network technologies such as IPv6 and DNSSEC.
- **Nixu DHCP Server** is a secure, stand-alone DHCP server with configuration validations and built-in support for DHCP failover pairs, supporting emerging network technologies such as DHCPv6.

3.4 Solution Architecture and Related Considerations

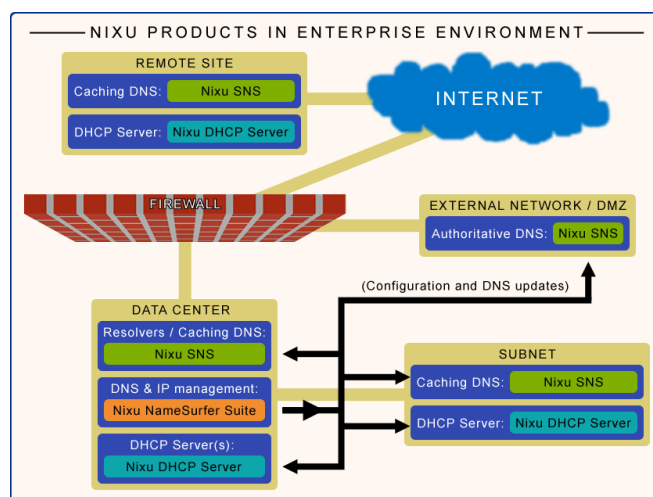


Illustration 1: DNS and DHCP services in a typical enterprise network

The above diagram provides a simplified illustration of DNS and DHCP services in an enterprise network environment. The descriptions below provide general guidelines on how DNS and DHCP services can be virtualized in a typical enterprise network environment.

1. **Data Centre:** A virtual infrastructure provides an excellent foundation for virtualizing DNS and/or DHCP services in enterprises. In order to ensure redundancy and availability, Nixu Software recommends the following solution architecture:
 - I. Centralized DNS, DHCP and IP Address Management system that is used to manage the entire name and address space. This system would consist of a

single virtual machine with support for DNS views, so that internal and external authoritative DNS zones can be managed separately.

- II. Two or more virtual machines for internal authoritative DNS
- III. Two or more virtual machines for internal recursive/caching DNS
- IV. Two or more virtual machines running DHCP servers as failover pair

If an enterprise has several data centers, it is recommended that a number of DNS and/or DHCP servers are distributed to different geographical locations for added redundancy.

2. **Subnets:** oftentimes, subnets are workstation networks that rely on Microsoft AD for DNS and DHCP services. An alternate solution for providing DHCP and caching/recursive DNS services in subnets is to run software appliances as dedicated virtual machines. If use of Microsoft AD is mandatory, management of the Microsoft AD zone as well as the administrative management of the clients in MS AD subnet can be carried out centrally using Nixu IPAM (Nixu NameSurfer Suite) described in paragraph 1 above.
3. **External network / DMZ:** external authoritative DNS servers residing in DMZ can be run in virtual infrastructure as dedicated virtual machines. The data (authoritative external DNS zones) on these servers is managed using the centralized management system described in paragraph 1.
4. **Remote Site(s):** typically, remote sites are small(ish) networks that rely on Microsoft AD for DNS and DHCP services. An alternate solution for providing DHCP and caching/recursive DNS services in subnets is to run software appliances as dedicated virtual machines. By adopting the alternate approach, also other network services and resources can be run as virtual machines on the same virtualization platform.

4 About Nixu Software

Nixu Software is a VMware Technology Alliance Partner and Citrix Ready Partner specializing in virtualization-ready DNS, DHCP and IP Address Management (DDI) software appliances. All Nixu Products are certified as VMware and Citrix Ready, and can be used to build centrally managed end-to-end DDI environments.

Headquartered in Espoo, Finland, and with regional sales offices in Central Europe and Asia-Pacific, Nixu Software's mission is to offer the best value in industry by creating virtualization-ready DDI solutions that set the benchmark for combined security, ease of use and low cost of ownership.

Nixu Products have an installed base of more than 3.000 instances worldwide, used by:

- one third of all 2.5G and 3G mobile operators worldwide
- enterprises large and small from practically all industry verticals
- well known research and education institutions all over the world.

For further details and contact requests, please visit www.nixusoftware.com.