## End-to-End DDI Services

Technologies such as IPv6 and DNSSEC along with rapidly increasing use IoT devices and BYOD (Bring Your Own Device) concepts are making manual IP address management processes obsolete. By automating these tasks, organizations can reduce overheads while simplifying troubleshooting and gaining transparent view of network resources. FusionLayer offers the best value in DDI industry by creating virtualization-ready DNS, DHCP and IP address management software appliances that set the benchmark for combined security, ease of use and low cost of ownership.

IPAM for Microsoft AD Environment

A high percentage of organizations continue to run Microsoft Windows Server 2008 and 2012 to provide DNS and DHCP services in their enterprise networks. In environments such as this, allocation, tracking and management of IP address spaces are often carried out manually using Excel spreadsheets. This manual approach is tedious, inefficient, prone to error, costly and unscalable. The conventional approach to solve this problem has been to introduce drastic architecture change and forklift the Microsoft DNS and DHCP servers. Microsoft, on the other hand, does not recommend this tactic as it could cause compatibility and configuration issues. As depicted by the figure on the right, FusionLayer's strategy has been to install a DDI-IPAM management layer on top of Microsoft AD that communicates with the Microsoft environment via an API. This ingenious approach allows us to have a centralized DNS, DHCP and IP address management system without having to give up on existing Microsoft AD Servers.
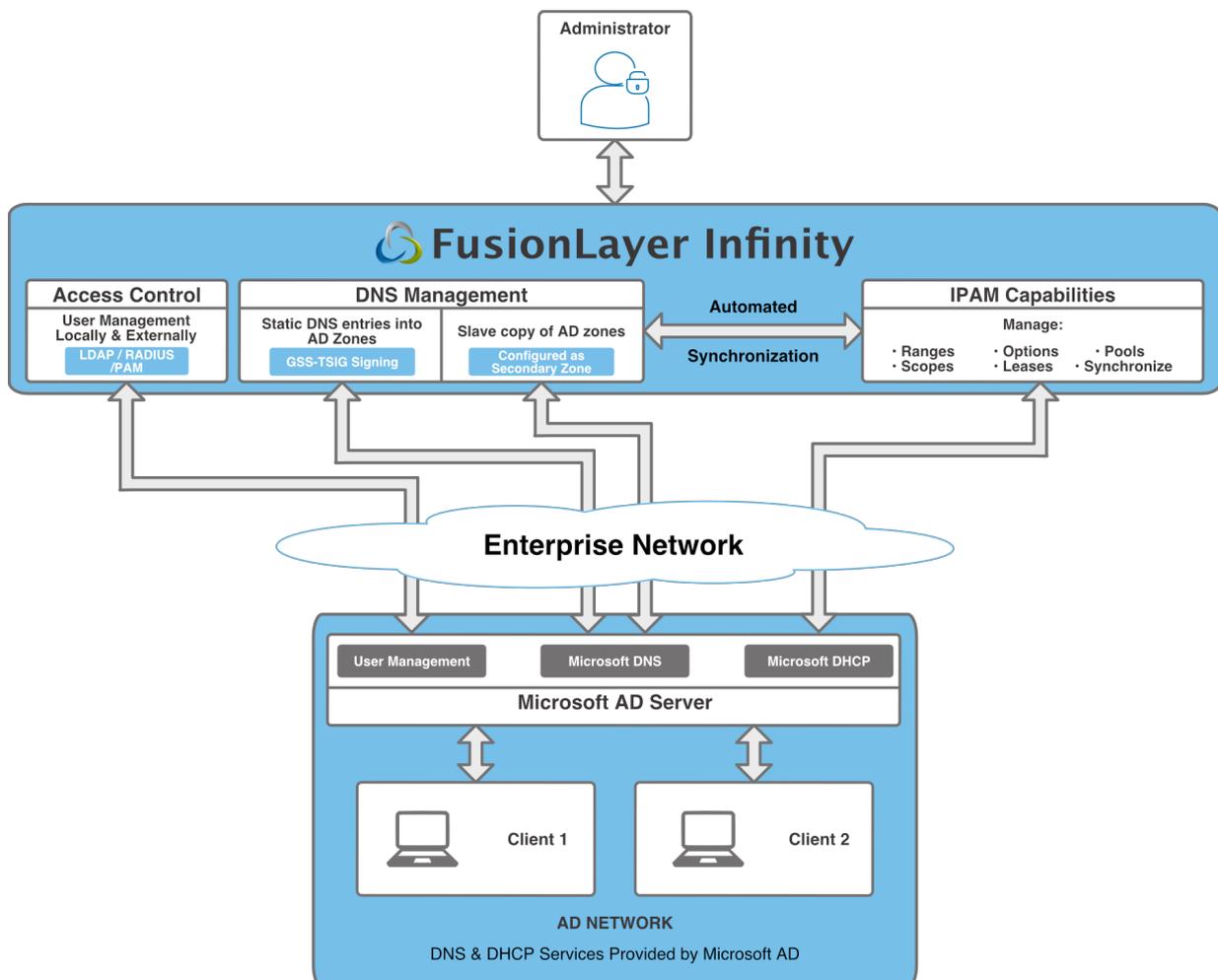
DNSSEC and IPv6

IPv4 had its last free top-level block assigned on 3 February 2011, putting a stamp date on the long anticipated exhaustion process of this protocol. In comparison to IPv4, its successor IPv6 adds a significant amount of complexity into managing DOI services, requiring a next generation of DOI management solutions and tools. Anticipating this need, all FusionLayer products are developed with full functionality and support for dual stack networks.

DNSSEC has been designed to protect Internet and network community from exposures to DNS cache poisoning and man-in-the-middle attacks. It allows the end-user to verify that the DNS data received has in fact originated from a trusted DNS server and that the information has not been changed while traveling through the network. DNSSEC requires the DNS zone data to be signed in order to ensure the authenticity of the name resolution process. As of 15 July 2010, the signed Root zone became available which facilitated the verification of a chain of trust from the Root Zone Public Key. FusionLayer products provide a simple, secure and affordable DNSSEC solution ensuring that your organization's network architecture is on the par with the latest industry security standards.

Cloud Computing

In traditional network environments, DNS and DHCP services are typically run on industry standard servers that host a number of different network services. This deployment strategy has several disadvantages including limited scalability, increased exposure to vulnerabilities, inevitable compromise in server and system management and inflexible deployment processes. 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. FusionLayer products are delivered as electronically distributed ISO images, software appliances, which can be used to jump-start a new virtual machine in a matter of minutes. As a result, FusionLayer's virtualization-ready product line help to reduce cost, increase data center utilization, simplify management and provide enhanced disaster recovery support as services can easily be relocated from one server to another.

Contact Information

FusionLayer, Inc. Tel. +358 75 325 2992 Email: info@fusionlayer.com