WHITE PAPER

IDG
INTERNATIONAL DATA GROUP

Strengthen the Foundation of Your Network

With network demands increasing every day, companies must apply new best practices to automate infrastructure reliability and security.

At the heart of every business is the network. The network contributes to the overall health of the business by pumping data the way the heart pumps blood. When the network is sound, the business is sound. But what makes the network sound?

At the heart of every network — and the foundation of the Internet — is the IP protocol. Three key components, together known as DDI, help maintain the IP protocol within corporate networks: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and Internet Protocol Address Management (IPAM). Each of these components is highly important for maintaining the health of the network and the IT infrastructure.

The business connection may seem tenuous, but it's not. An efficient infrastructure contributes to an efficient enterprise. (Indeed, how many corporate mergers have been undermined by the inability to integrate systems?) DDI is the foundation of the IP infrastructure upon which business efficiency rests. It's also a critical contributor to risk mitigation, availability, security and IT accountability. A company is only as agile as its DDI.

Therefore, as demands on the network increase, demands on DDI increase. The spate of new IP-based devices attached to corporate networks is making DDI management more important than ever. Only by understanding these demands and managing these DDI components properly can enterprises ensure — and enhance — the efficiency and continuity of their IT and business operations.

efficient iP™
DEFINING SMART DDI

THE NETWORK CONTRIBUTES TO THE OVERALL HEALTH OF THE BUSINESS BY PUMPING DATA THE WAY THE HEART PUMPS BLOOD.

New Demands on the Network

Every IT department can bear witness to the dramatic increase in demands placed on the network. Clearly, there has been a boom in IP-based devices connected to the network in recent years. And the list is growing:

- employee-owned mobile devices accessing corporate data
- customer-owned mobile devices engaged in transactions or social media activities
- video cameras feeding security images
- access control badges recording comings and goings
- medical devices in hospitals
- electrical meters in homes
- ATMs and other kiosks
- robotic devices in factories
- intelligent sensors transmitting data from inaccessible locations

In addition, virtualization is boosting the complexity of managing IP-based devices. With numerous virtual machines running on one piece of hardware, enterprises lose visibility into devices; it's no longer possible to monitor what IP traffic travels along a particular cable, which affects capacity planning. Virtualization enables the rapid deployment of servers, which has brought unparalleled agility. But it has also dramatically increased the need for visibility of IP addresses when it comes to monitoring traditional ports, switches and VMs running on servers.

Multiply the numbers of VMs, as so many enterprises are by deploying ever-more complex data centers, and the challenges multiply as well. Private clouds and increased consolidation concentrate key applications requiring reliability and security of the IP network infrastructure.

Reliability and security are especially crucial now that enterprises are allowing employees to access the network through their own mobile devices in bring-your-own-device scenarios. DDI solutions can confirm that a mobile device requesting access to the network is approved and authentic. If not, the solution can deny access.

DDI solutions also step in when a device infected with malware connects to the network. Beyond eradicating the malware, network administrators must be able to identify how the infected device was connected to the network in order to mitigate risks of malware propagation. That requires visibility into IP address connections. On a grander scale, having that kind of visibility can help IT ensure that the infrastructure is designed as securely as possible, without unnecessary or unknown connections between devices and services; the more obscure connections in an infrastructure, the more vulnerabilities hackers can exploit.

The importance of deploying a solution that can handle DDI on an automated basis becomes particularly apparent when opening a new building, whether it's a retail store, a medical clinic or a branch office. Enterprises need to efficiently deploy IP infrastructure to ensure reliable business operations without manual tinkering. With a DDI solution that creates a template of all IP resources typically found within any given structure, IT technicians can take that template and apply its configuration and associated best practices for managing devices to the new facility's architecture. That significantly reduces the time it takes to ensure that the facility and its technologies are ready for secure, authenticated use.

DDI automation is also important for external reasons, such as changes to the IP protocol itself. Managing the rollout of the latest version, IPv6, will increase the cost of network infrastructure management for those companies that aren't prepared.

Why DDI's Key Components Are Crucial for IT Strategy

The first D in DDI stands for DNS, the Internet's hierarchical distributed system for naming and identifying computers, services or resources connected either to the public Internet or a private network. The second D stands for DHCP, the network protocol used to configure devices (known as hosts) connected to a network so they can communicate across the IP network. The I stands for IPAM, the means of planning, tracking and managing the Internet Protocol address spaces found in any given network.

Though rooted in technical realms, these components have a crucial impact on the applications every employee is familiar with. Companies need to simplify, streamline and industrialize their IT operations in order to reduce their time to market and increase their global revenues. That's why business process management should incorporate the capability to model, automate and monitor IT processes related to DDI services.

With DDI – and especially state-of-the-art DDI management solutions – supporting business operations, enterprises can achieve a more agile network infrastructure. This applies to when they acquire new companies, open new facilities, deploy the latest applications and virtualize different aspects of the network. That said, these solutions must also integrate smoothly with other management applications (asset management, monitoring and activation). Deployed properly, DDI solutions can help companies ensure end-to-end visibility into IT process automation.

How Enterprises Should Incorporate DDI Solutions

Given the importance of DDI, and the growing demands on IP networks, enterprises must look for DDI appliances that accomplish two key capabilities.

The first relates to reliability and security. These appliances must be able to control overall data consistency to eliminate network outages due to conflicting configurations. They must incorporate security mechanisms that protect against attacks and ensure data integrity. And they must support high availability of corporate data and disaster recovery mechanisms. If the DNS server fails, employees' access to applications, email and the Internet is severed, and productivity plummets. Similarly, if assembly devices on a factory floor are IP-enabled and the DNS server fails, products don't get produced.

The second capability relates to the increasing complexity of managing growing IP networks themselves. By applying corporate-defined DDI policies, enterprises can identify configuration errors quickly and address problems before users notice them. In new deployments, these configuration issues can be avoided entirely, because automated DDI policies reduce the need for IT intervention.

Companies derive multiple advantages from this automation. They're not reliant on employees with specific knowledge about configurations who may leave the company. Less human intervention translates to fewer errors. And with a reliable infrastructure foundation on which to build, their new locations — whether in new cities or new countries — can start contributing revenue faster.

It's also essential that organizations deploy DDI solutions that provide unified management of all DDI-related protocols, supplying a global visibility, consistency control and automated management of the IP infrastructures and services. In addition, the solutions must interoperate with other tools within the infrastructure, such as asset management tools, so that companies don't have to replace what they've already installed. A high level of interoperability means that the DDI solutions can easily accept data from those systems and disseminate best practices to those systems anywhere within the IT architecture.

Interoperability is also important when it comes to creating a comprehensive inventory of the enterprise devices already existing on the network. With this insight, enterprises can accurately track their devices, avoiding investments in new ones that are unnecessary and identifying network equipment or a port no longer in use. This increased visibility also helps with the business-related demand of governance.

SOLIDSERVER HAS A RECONCILIATION CAPABILITY THAT DETECTS AND IDENTIFIES INCONSISTENCIES, MITIGATES SECURITY PROBLEMS AND NETWORK OUTAGES, AND SIMPLIFIES TROUBLESHOOTING.

What EfficientIP SOLIDserver Brings

In developing its SOLIDserver appliance, EfficientIP has incorporated all of the important aspects of DDI: intelligent automation, configuration, device management and more. SOLIDserver helps IT support the business by enabling the crucial IP-specific technologies. It helps IT with both the deployment and management of IP devices. During deployment, it facilitates the inventory and provisioning of devices, using interoperable APIs to integrate IPAM with network management and asset management tools. And it automates all the business processes associated with network and device management, so that IT is freed from time-consuming, manual monitoring and configuration activities.

The SOLIDserver appliance also creates a best-practices framework and ensures that DDI resources are allocated and configured based on strict alignment with business needs.

After deployment, SOLIDserver has a reconciliation capability that detects and identifies inconsistencies, mitigates security problems and network outages, and simplifies troubleshooting. The more visibility a DDI solution has into a network, the more an enterprise can avoid downtime and the costs associated with it.

Of course, the true indication of such a tool's value comes from real-world use. A major worldwide retail chain has standardized on SOLIDserver to support its expansion strategy. The chain uses EfficientIP's DDI solution before it opens a new location, defining how IPAM resources should be named and where they should be located, and then identifying that location within its DNS and DHCP architecture.

The solution also helps the chain launch the provisioning of multiple IP subnets and IP addresses according to the geographical location of the store, and then reserves IP addresses for the necessary network devices within the store. These include everything from traditional network devices (such as servers, routers and switches) to cash registers, refrigeration units and closed-circuit cameras.

According to the chain, the provisioning process used to take up to four weeks because of the collaboration needed between systems and network administrators. With SOLIDserver, the process now takes just a few minutes, allowing the chain to bring stores up and begin deriving revenue from them in a much shorter period of time.

In advancing its DDI technology, EfficientIP has also developed its SmartArchitecture™ to further simplify the deployment and administration of network services relating to DNS and DHCP services at both the server and architecture level through a policy-driven approach. SmartArchitecture provides templates that allow IT to automatically deploy servers based on best practices and then manage the architecture as a single, integrated entity. Also newly added to SOLIDserver: device inventory features for efficient port allocation management. This helps confirm that devices are properly configured within IPAM.

With EfficientIP's state-of-the-art technology, enterprises get the benefit of unified management of DNS, DHCP, IPAM and network device management, including the management of policies and processes for deployment, delegation and reconciliation. As a result, they can ensure that their network infrastructure truly supports the business imperatives, ranging from business continuity and availability to reduced time-to-market for new products, services and locations. For IT's benefit, this provides security, capacity planning and governance. Most important, and benefiting all, it provides visibility into the deep recesses of the all-important IP protocol. ■