IDC EXECUTIVE BRIEF

HOW DDI ENABLES KEY STRATEGIC IT INITIATIVES

Author:
Romain Fouchereau

March 2021

Sponsored by efficient iP™

IDC #EUR147507621

How DDI Enables Key Strategic IT Initiatives

Introduction

After what has been some of the most disruptive times in recent history, organizations need to focus on reigniting the business and how this can be enabled through technology and digital transformation (DX).

To take full advantage of new business opportunities, organizations will need to leverage technology and transform it as an enabler of business outcomes. As organizations face new challenges in their DX journey, there is increased pressure to remain competitive with innovation and business agility. But sometimes getting the green light for these enabling technologies to support agility, innovation, and growth, as well as boosting competitiveness, can be hard to justify or a tough "sell" to the CEO, C-suite, or the board.

Being able to demonstrate business value through the adoption of new technology and initiatives such as multicloud, SD-WAN, automation, and network security will be a key differentiator. This can be done by leveraging DDI — DNS, DHCP, and IPAM — solutions and getting direct measurable business outcomes such as improving efficiencies; reducing costs; ensuring coherence, resilience, and business continuity; improving user experience; and opening up new revenue streams.

AT A GLANCE

To grow into the new business norm, organizations must take full advantage of new business opportunities and leverage technology to enable business outcomes.

WHAT'S IMPORTANT

To be successful with new strategic IT initiatives such as multicloud, SD-WAN, automation, and network security, DDI (DNS-DHCP-IPAM) solutions are vital as they deliver measurable business outcomes:

- Time and cost savings
- Reduced risk
- Remote workforce enablement
- Improved user experience
- End-to-end automation
- Faster time to value
- Increased security

The Future Enterprise

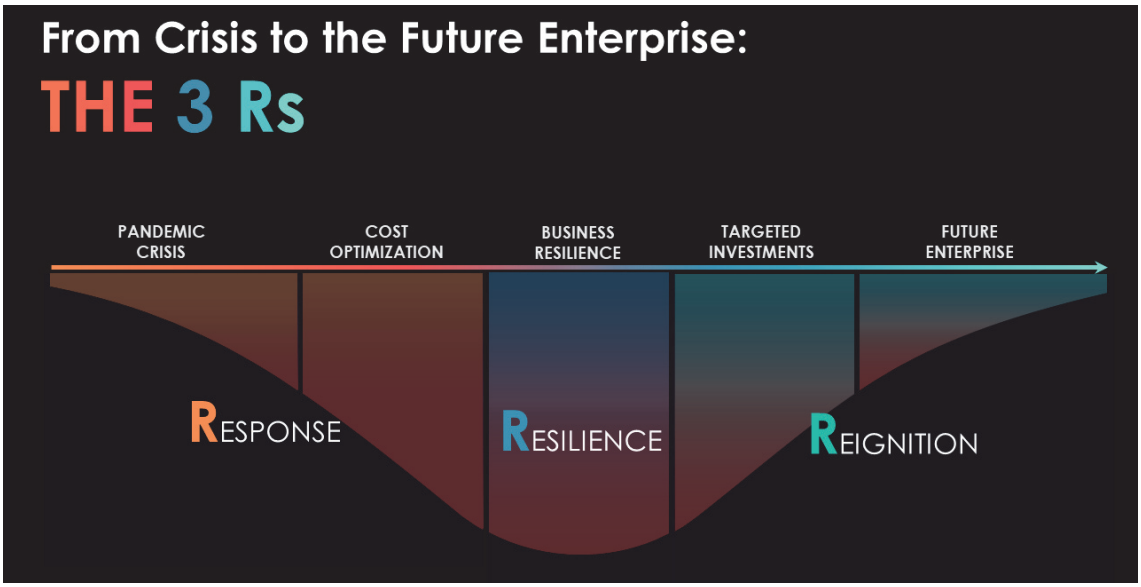
Throughout the crisis, IDC has been looking at the impact of COVID-19 on IT spend. This has enabled us to create a recovery curve model with five phases:

1. The immediate **crisis response** phase with a focus on business continuity
2. The slowdown phase, when the impact of having fewer people in the office and reduced economic activity means that return on investment and cost **optimization** are prioritized
3. The bottom of the curve, the recession phase, when **building operational resilience** is prioritized as revenue is expected to be in prolonged decline
4. The recovery phase when activity eventually picks up again and **targeted investments** are identified to accelerate this
5. The **reigniting of the enterprise** with innovation at its core to maximize new normal opportunities for organizations

Many organizations feel they are stuck in the response stage (phases 1 and 2), responding to the crisis, focusing on business continuity, and being unable to move to the next stage. As revenue

inevitably slows down in this phase, organizations are in cost-optimization mode. This suggests that for most the crisis will last some time yet before they can move on to the business resilience stage, at which point the business grows again and kick starts the reignition stage. In this reignition stage, organizations will identify targeted investments to finally reignite business and become the future enterprise that will thrive in the new normal.

FIGURE 1
The IDC Recovery Curve



Source: IDC, 2021

The five-phase framework is to be used by organizations to map out their goals toward becoming a future enterprise and reignite business to achieve a "better new normal" by leveraging the power of technology. To achieve business resilience and move into business reignition mode, it is important for organizations to accelerate their DX to focus on technology initiatives that can enable direct and measurable business outcomes.

Initiatives to Reignite the Network/IT and the Role of DDI

IDC has identified four technology areas where new initiatives can help grow into the new business norm: multicloud, SD-WAN, automation, and network security. To enable and accelerate these, DDI solutions are vital, bringing measurable business outcomes.

DNS, DHCP, and IP address management — collectively known as DDI — are core networking technologies critical for every IT organization. DNS servers deliver the association between host names and IP addresses that keeps HTTP web traffic and network traffic flowing, whereas DHCP provides a dynamic address assignment capability for nodes logging on to the network. IPAM supports these technologies by enabling efficient tracking and management of the IP addresses within a network and consolidating IP data into a central repository. An effective DDI solution helps simplify and automate the management and IP control of the relationship between DNS, DHCP, and IPAM. DDI solutions can be delivered through a dedicated hardware or software/virtual appliance form factor.

Multicloud

Cloud is the infrastructure foundation for digital enterprises, and many enterprises are shifting to cloud-centric digital infrastructures. The need to deliver infrastructure and application and data resources to edge locations will spur adoption of new, cloud-centric edge and network solutions that enable faster response to current business needs while serving as a foundation to boost long-term digital resilience, enabling business scaling and ensuring greater business operational flexibility.

However, enterprises are struggling with varied cloud APIs, data silos, millions of access points, and skills shortages leading to network configuration issues and loss of control. According to IDC, the top 3 challenges to create successful multicloud deployment are building a common control workflow (58%), lack of unified monitoring and management (55%), and an inability to drive one security policy across different cloud providers (55%).

Integrating resources deployed in the cloud with a DDI solution will help organizations make a success of their cloud projects by bringing:

- Full orchestration of IP management for faster deployment time of sites and services
- Enhanced single-viewpoint visibility of resources across on premises and clouds that will improve control and simplify network management
- The ability to automate build, run, and retire workflows and processes to bring operational time savings
- Uptime optimization of cloud resources to save on operational costs
- Application traffic routing capabilities to fully take advantage of network diversity to strengthen resilience and improve user experience
- Rationalized security with aligned security policy enforcement across the entire infrastructure

A multicloud-ready and unified DDI solution can help enterprises secure, simplify, accelerate, and de-risk their multicloud and DX initiatives. DDI solutions can improve multicloud initiatives by enhancing visibility, resilience, automation, and control.

SD-WAN

As network traffic bound for the cloud continues to increase in volume, variety, and complexity, SD-WAN's ability to dynamically route traffic based on granular application policy and real-time network conditions, across network diversity and the relative criticality of application traffic, becomes essential to the success of digital business — as does its ability to ensure reliability and resilience of business-critical network traffic over broadband networks that cost less than MPLS connections.

In its enterprise communications survey, IDC found that 68% of respondents plan to migrate to an SD-WAN architecture within the next two years. The most important factors cited to accelerate this transition were to increase the flexibility to use different networks for application delivery, and the ability to change bandwidth in near real time and reduce management complexity through automation and orchestration.

But new SD-WAN deployments bring new challenges for organizations. IP address control can become more difficult because of the routing now happening between internet sites, and the routing of IP traffic itself is also more complex due to the multiple paths between sites. SD-WAN does not address security concerns, as in most cases network security is not a native feature of the solutions. This extension of the network with many new endpoints adds a layer of complexity to network security, and one unsecured entry point could lead to a critical security breach. On top of all these challenges, the deployment of a large SD-WAN network in itself remains complex and demands rigorous planning and inventory management.

This is why SD-WAN relies on DDI services to ensure scalable, secure, and efficient connections from the edge of the network to the endpoints both internal to the enterprise and into the cloud. SD-WAN can only guarantee the connectivity to an application as served with the same IP address leveraging network diversity it provides but cannot fall back to an alternate IP/server/DC to improve or restore connectivity. This is where application-aware traffic steering solutions like edge DNS GSLB (global server load balancing) with over-the-top IP routing will help steer traffic to an alternate IP/server/DC leveraging network diversity provided by SD-WAN to augment the connectivity between users and their applications. And because DDI is central to all IP exchanges, it will help to deploy successful SD-WAN projects by providing:

- A proper IP address plan management for consistency and integrity of the IP addresses
- A rich consolidated IP data lake with metadata to offer end-to-end automation and zero-touch network operations
- More streamlined DNS security through corporate policy enforcement across the entire SD-WAN infrastructure
- Over-the-top application traffic steering to improve user experience, performance, and resilience (DRP)

All of these help to improve resilience, control, speed of deployment, operational management, and user experience in SD-WAN networks.

Automation

Networks are growing more critical and complex as organizations rise to the challenges of DX. Locations, connections, remote workers, traffic volumes, application exchanges, security threats — all of these and more are combining to drive network management to new heights in requirements and capabilities. In networking and network management, complexity is the enemy. Visibility, analysis, and automation break down this complexity for the benefit of the network staff, the greater IT organization, and the users — internal workers, external partners, and end customers.

In the *Future-Proofing the Enterprise Network Survey* from June 2020, IDC asked organizations in which area they will increase investments as a result of new business operations required because of COVID-19. The top answer, with 48% of respondents, was the increased reliance on advanced automation platforms to reduce the manual management of the network. IT automation is a high priority and a key challenge for enterprises, offering them great potential in terms of business outcome value.

An integrated DDI solution simplifies and automates management of the interactions between DNS, DHCP, and IPAM. These capabilities enable organizations to effectively cope with ever-increasing volumes of IP addresses and business dependency on core network services. But automation can be very difficult to implement, and organizations must ensure that the appropriate infrastructure is in place to develop and deploy it, and address scalability issues and solve problems linked to lack of integration of processes in the IT supply chain.

DDI with built-in automation and rich metadata from the consolidated IP data lake will enable:

- Automated provisioning and deprovisioning of services and resources on premises and in the cloud to bring significant time savings, reduce workload, and prevent misconfigurations
- The ability to plan future extensions off the network, such as new virtual cloud networks, SD-WANs, or new remote user sites
- Better management of tools like SDN and SD-WAN orchestrators to plan, execute, and test operations by changing metadata values to reflect progress and report results in a BI-like dashboard
- The leveraging of a rich set of APIs to link to the whole ecosystem for real-time integration with third-party IT systems to simplify deployment, improve compliance control and audit trails, and deliver end-to-end automation
- Enforcement and automation of security policies (in firewalls, for example)

Network automation requires comprehensive data on the configuration of a network and the state of that network, and DDI can help to establish that comprehensive IP data repository as a network source of truth. A higher adoption of integrated DDI solutions in the organization will help to automate DDI resources provisioning and deprovisioning in a centralized and standardized manner for the whole service life cycle.

Network Security

IDC's *Worldwide COVID-19 Impact on IT Spend 2020 Survey* showed how the pandemic is reordering C-suite priorities. Respondents now identify themes such as business resilience and customer experience as top priorities for their organization over the next five years, driven by 3rd Platform technologies (IoT) and a shift to working from home.

The extended enterprise is changing the role of the CISO to include managing the security and investigative control program across the entire attack surface, including IT, IoT, industrial IoT, operational technology (OT), edge computing, and 5G. Securing IoT (41%) and OT (40%) were the top 2 technology concerns for security professionals in IDC's 2020 security survey, followed by edge security (32%) and the arrival of 5G and its security implications on the network (17%).

Because DNS is at the intent of all IP communications, DNS has the potential to analyze client behavior and make decisions on application access using filtering and UBA (user behavior analysis), providing valuable insights and analytics for threat detection on an IoT deployment, for example. DNS gathers a lot of application usage from users and with the massive shift to remote working, secure remote access has become one of the top use cases for security. Encryption of

traffic is highly recommended when using home networks, using a VPN back to the organization network or with DNS ciphering with DoH or DoT (DNS-over-HTTPS or DNS-over-TLS).

DDI will help overcome some of the security challenges faced by many organizations by facilitating segregation of network flows and enabling corporate policy enforcement across their infrastructure.

DNS as part of the overall security strategy can be used to detect threats, simplify and accelerate mitigation, and be leveraged to:

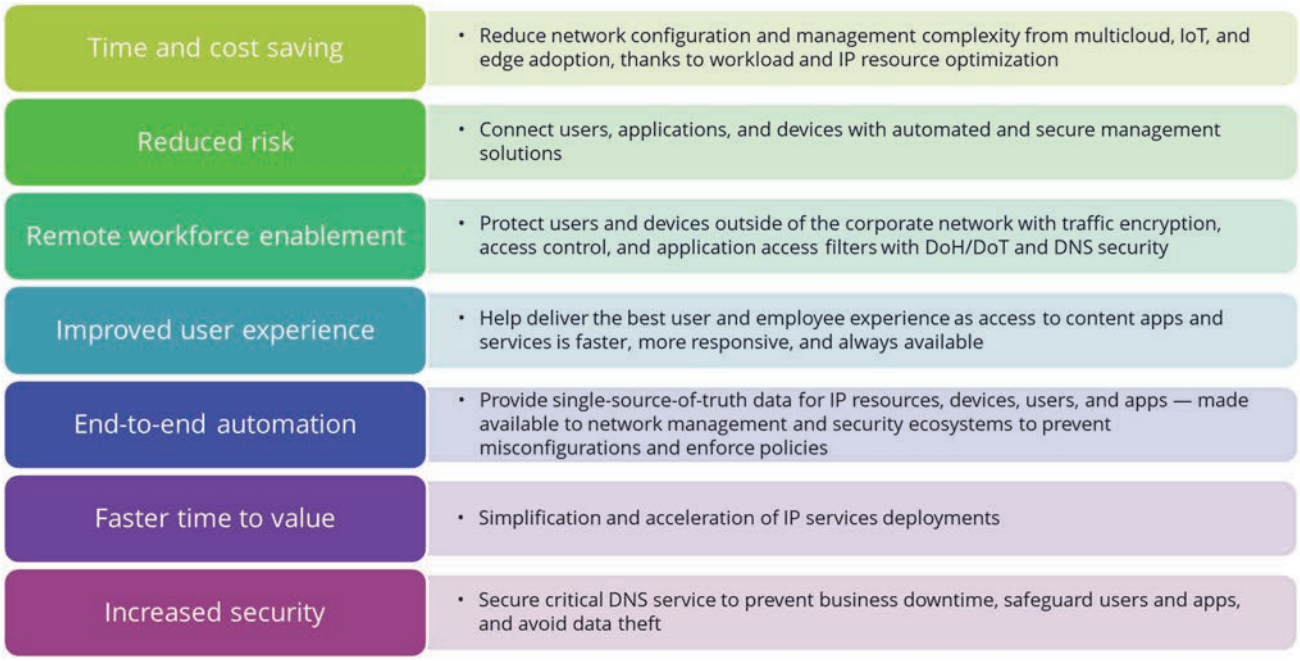
- Be the first line of defense as it sees the intent of virtually all IP traffic
- Overcome security holes that are often left by firewalls and IPS
- Improve application access control to help with zero-trust strategies
- Feed security events into an organization's SIEM and SOC

Secured DNS services will protect from data theft, protect users' privacy, and filter access to applications hosted in cloud and on premises.

A Robust DDI Strategy Can Drive Direct Business Outcomes

Through the implementation of a robust DDI strategy, organizations can expect to gain direct business benefits from technologies and initiatives such as multicloud, SD-WAN, automation, and network security mentioned earlier, but also other areas such as IoT, edge, and 5G planning and adoption.

FIGURE 2
Business Outcomes and Benefits From DDI Solutions



Source: IDC, 2021

IDC View and Analysis

The CEO plays a direct, major role in DX strategies, according to IDC's *Future-Proofing the Enterprise Network Survey, 2020* (see Figure 3).

FIGURE 3
CEO Involvement in Digital Transformation

Source: *IDC Future-Proofing the Enterprise Network Survey*, 2020

It is therefore important for the CEO and the whole C-suite to understand the benefits that an integrated DDI solution can bring to their business and that automation and security of DNS, DHCP, and IPAM core network services are foundational to enable and accelerate strategic initiatives:

- **DDI as an enabler of network transformation.** Cloud and multicloud have created a new model to host and access applications, and have driven IT organizations to modernize their network operations to increase agility on their own premises. These network transformation efforts increasingly incorporate software-defined networking tools, advanced network management platforms, and private cloud services. DDI platforms are essential components of building a modern datacenter that relies heavily on accurate dynamic data (network source of truth), automation, visibility, and simplification of management.
- **DDI and the overall security-by-design strategy.** Evolution and awareness of DNS security is growing, but costs and the average number of attacks have remained high. The cloudified era has contributed to most organizations being directly impacted by cloud and application downtime when facing DNS attacks — from enterprises to service providers and even into the midmarket — and DDI platforms can help to secure their networks, applications, and data. DDI must become an integral part of organizations' security-by-design approach and work hand in hand to support and secure the day-to-day functions of the business.
- **DDI to enable a focus on business outcomes.** Awareness of how DDI is changing networking and security is increasing for IT professionals. But there are still opportunities to prove the value of this integrated approach to the C-level suite as it relates to business outcomes mentioned earlier such as reduced TCO, lower opex and improved operational efficiency and time savings, improved user experience, strengthened resilience and disaster recovery plans, better quality assurance and compliance, improved service assurance and continuity, and application availability.

Conclusion

IT and security teams need to shift their vision and focus on business outcomes to demonstrate business value in the reignited future enterprise, and that includes integrating DDI solutions into the overall DX strategy:

- **DX to accelerate business initiatives:** Improved simplicity, agility, and speed with investment in continuous innovation
- **Convergence of networking and security:** Adding further telemetry, analytics, and automation on top of software-defined networking and security tools
- **Expanding impact through ecosystems:** The ecosystem of partners that are assembled to support customers' broader requirements

The ongoing pressure caused by these challenges and the challenges linked to new initiatives such as multicloud, SD-WAN, IoT, edge, mobility, and managing a growing remote workforce create further complexity. There is now greater demand for approaches to reduce this complexity and a need for operational excellence to provide solutions that can reduce the burden on overstretched IT and security teams. Without the implementation of DDI as part of the business reignition strategy, organizations will not be able to address the challenges they face with the design and implementation of their new IT strategic initiatives to take full advantage of what multicloud, SD-WAN, automation, and network security will bring to their business.

MESSAGE FROM THE SPONSOR

EfficientIP is a network automation and security company, specializing in DNS-DHCP-IPAM (DDI) solutions, with the goal of helping organizations worldwide to drive business efficiency through agile, secure, and reliable infrastructure foundations. Its SOLIDserver platform simplifies network management, while patented technology secures DNS services to safeguard data and ensure application access from anywhere at any time. Companies rely on EfficientIP to help control the risks and reduce the complexity of challenges they face with key IT initiatives such as cloud, zero trust, and IoT. For more information, please visit https://www.efficientip.com.

About the Analyst

Romain Fouchereau, Research Manager, European Security, IDC

Romain Fouchereau has a specific focus on network security and the security technologies linked to the extended enterprise such as IoT, edge, and IT/OT convergence. He monitors the development, evolution, and penetration of these technologies and vendors' approaches to stimulating adoption at both channel and end-user levels. He manages IDC's security appliance market tracker for Europe, which provides market size, vendor shares, and forecasts for network security products such as unified threat management (UTM), firewall, IDP, and content management (web and messaging) appliances. He also co-leads the European Future of Operations practice, looking at the shift in operational mindset for European organizations to a market-driven outlook leveraging digital capabilities to build a resilient organization. He has a specific interest in the role of security as a business enabler for IT/OT integration strategies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters

5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright and Restrictions