White Paper

Higher Education IT Challenges and How DDI Solves Them

Three Axis of Optimization for Higher Service Efficiency

"With universities becoming ever more competitive and students and staff becoming reliant on network and Internet access, the flexible and effective solution that EfficientIP provides for IPAM and business continuity/disaster recovery gives Leeds Metropolitan a real advantage."

Steve Whitaker,
Senior Infrastructure Consultant
Leeds Metropolitan University

Outline:

Today, institutions of higher education are facing increasingly tough competition. Beyond academic excellence, a University's ability to compete depends largely on its ability to offer modern facilities, online cursus, remote exams, e-learning, self-service portal, lecture capture and high value-added services for students, professors, and researchers, while at the same time reducing operational costs.

The impact on the educational market is profound and transformative, driving a new technology-centered business model and innovative programs that include Massive Open Online Courses (MOOC), adaptive learning tools, and videoconferencing. Unlimited internet access and school supplied resources have become essential student services.

Because these programs and services have become vital to the fundamental existence of the institution, IT is a significant factor in its success. The increasing diversity and complexity of users and services make managing both IP services and the overall infrastructure a dynamic challenge.

The advent of MOOC and the boom in smartphones and tablets (BYOD) have considerably upped the ante on the network services required to manage and control IP enabled devices. Mobility offers users greater flexibility, but it has also made infrastructures more vulnerable to attack by exposing Universities' internal networks to access by non-controlled devices and users. BYOD enabling initiatives therefore must include a plan for securing internal infrastructure with tools like NAC, DNS firewall and client filtering, captive portal, and equipment inventory and tracking.

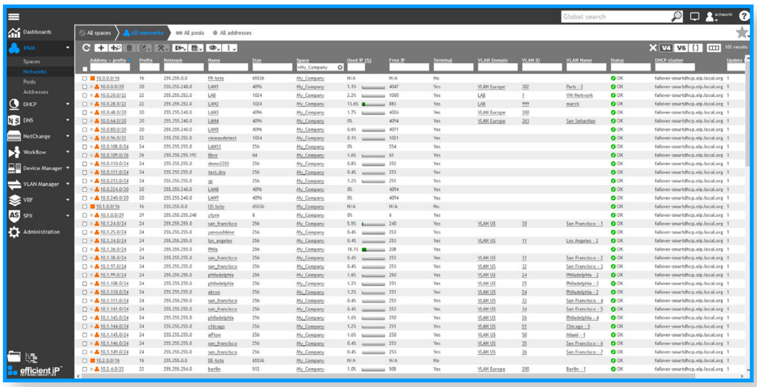
Yet another evolving challenge is the addition of IPv6 addressing and routing on the campus network and Internet accesses. Universities have been on the frontline of IPv6; experimenting, piloting, innovating, and partnering with other organizations worldwide. This has led to the development of new initiatives for the planning and deployment of large-scale IPv6 implementations. These initiatives require new administrative tools to successfully manage IPv4 and IPv6 coexistence, as well as structure an effective transition plan.

All these current challenges need to be addressed in a context of high security pressure on the data storage and digital transformation for students, staff and researchers. Malware and cryptolocker type of attacks are disastrous for universities who are storing high value information about their students, like id numbers, bank accounts, addresses and profiles. Digital transformation and remote studying provide even more attack possibilities, but are mandatory to support students through their digital learning journey (e.g. course enrollment, follow educational goals, device registration for network access, professional development planning).

This white paper analyzes the various issues surrounding DDI services (DNS, DHCP and IP Address Management) in the unique context of higher education and shows how unified management and automation address the need for reliable, secure, and cost effective services.

1» The Importance of a Structured Addressing Plan to Support New Services

University computer networks are characterized by diverse logical and physical organizations. This translates into a complex and highly segmented network infrastructure requiring daily administration to ensure the University's ability to deploy new sites and services including BYOD, remote learning, campus IoT and communication.



Address + prefix	Prefix	Netmask	Name	Size	Space	Used IP (%)	Free IP	Terminal	VLAN Domain	VLAN ID	VLAN Name	Status	DHCP cluster	Update
					=My_Company									
10.0.0.0/16	16	255.255.0.0	FR-toto	65536	My_Company	N/A	N/A	No				OK	failover-smartdhcp.eip.local.org	1
10.0.0.0/20	20	255.255.240.0	LAN1	4096	My_Company	1.1%	4047	Yes	VLAN Europe	302	Paris - 2	OK	failover-smartdhcp.eip.local.org	1
10.0.20.0/22	22	255.255.252.0	LAB	1024	My_Company	2.2%	1000	Yes	LAB	1	VM Network	OK	failover-smartdhcp.eip.local.org	1
10.0.28.0/22	22	255.255.252.0	LAN2	1024	My_Company	13.6%	883	Yes	LAB	999	marck	OK	failover-smartdhcp.eip.local.org	1
10.0.48.0/20	20	255.255.240.0	LAN3	4096	My_Company	1.7%	4026	Yes	VLAN Europe	300		OK	failover-smartdhcp.eip.local.org	1
10.0.64.0/20	20	255.255.240.0	LAN4	4096	My_Company	0%	4094	Yes	VLAN Europe	263	San Sebastian	OK	failover-smartdhcp.eip.local.org	1
10.0.80.0/20	20	255.255.240.0	LAN5	4096	My_Company	0.6%	4071	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.96.0/22	22	255.255.252.0	reseaudetest	1024	My_Company	0.1%	1021	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.108.0/24	24	255.255.255.0	LAN11	256	My_Company	0%	254	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.109.0/26	26	255.255.255.192	libre	64	My_Company	1.6%	61	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.110.0/24	24	255.255.255.0	demo2203	256	My_Company	0.8%	252	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.111.0/24	24	255.255.255.0	test.dns	256	My_Company	0.4%	253	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.213.0/24	24	255.255.255.0	sp	256	My_Company	1.2%	251	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.224.0/20	20	255.255.240.0	LAN8	4096	My_Company	0%	4094	Yes				OK	failover-smartdhcp.eip.local.org	1
10.0.240.0/20	20	255.255.240.0	LAN9	4096	My_Company	0%	4094	Yes				OK	failover-smartdhcp.eip.local.org	1
10.1.0.0/16	16	255.255.0.0	US-toto	65536	My_Company	N/A	N/A	No				OK	failover-smartdhcp.eip.local.org	1
10.1.0.0/29	29	255.255.255.248	ytyre	8	My_Company	0%	6	Yes				OK	failover-smartdhcp.eip.local.org	1
10.1.24.0/24	24	255.255.255.0	san_francisco	256	My_Company	5.5%	240	Yes	VLAN US	30	San Francisco - 1	OK	failover-smartdhcp.eip.local.org	1
10.1.25.0/24	24	255.255.255.0	yanoushkine	256	My_Company	0.4%	253	Yes				OK	failover-smartdhcp.eip.local.org	1
10.1.34.0/24	24	255.255.255.0	los_angeles	256	My_Company	0.4%	253	Yes	VLAN US	11	Los Angeles - 2	OK	failover-smartdhcp.eip.local.org	1
10.1.36.0/24	24	255.255.255.0	Phila	256	My_Company	18.1%	208	Yes				OK	failover-smartdhcp.eip.local.org	1
10.1.38.0/24	24	255.255.255.0	san_francisco	256	My_Company	0.4%	253	Yes	VLAN US	31	San Francisco - 2	OK	failover-smartdhcp.eip.local.org	1
10.1.97.0/24	24	255.255.255.0	san_francisco	256	My_Company	0.4%	253	Yes	VLAN US	32	San Francisco - 3	OK	failover-smartdhcp.eip.local.org	1
10.1.99.0/24	24	255.255.255.0	philadelphia	256	My_Company	1.6%	250	Yes	VLAN US	24	Philadelphia - 2	OK	failover-smartdhcp.eip.local.org	1
10.1.108.0/24	24	255.255.255.0	philadelphia	256	My_Company	1.2%	251	Yes	VLAN US	25	Philadelphia - 3	OK	failover-smartdhcp.eip.local.org	1
10.1.110.0/24	24	255.255.255.0	akron	256	My_Company	1.2%	251	Yes	VLAN US	24	Philadelphia - 2	OK	failover-smartdhcp.eip.local.org	1
10.1.111.0/24	24	255.255.255.0	san_francisco	256	My_Company	0.4%	253	Yes	VLAN US	33	San Francisco - 4	OK	failover-smartdhcp.eip.local.org	1
10.1.141.0/24	24	255.255.255.0	san_francisco	256	My_Company	0.4%	253	Yes	VLAN US	34	San Francisco - 5	OK	failover-smartdhcp.eip.local.org	1
10.1.143.0/24	24	255.255.255.0	philadelphia	256	My_Company	1.6%	250	Yes	VLAN US	26	Philadelphia - 4	OK	failover-smartdhcp.eip.local.org	1
10.1.144.0/24	24	255.255.255.0	chicago	256	My_Company	1.2%	251	Yes	VLAN US	51	Chicago - 5	OK	failover-smartdhcp.eip.local.org	1
10.1.145.0/24	24	255.255.255.0	affton	256	My_Company	1.6%	250	Yes	VLAN US	50	Miami - 1	OK	failover-smartdhcp.eip.local.org	1
10.1.146.0/24	24	255.255.255.0	san_francisco	256	My_Company	0.4%	253	Yes	VLAN US	35	San Francisco - 6	OK	failover-smartdhcp.eip.local.org	1
10.1.149.0/24	24	255.255.255.0	san_francisco	256	My_Company	0.4%	253	Yes	VLAN US	36	San Francisco - 7	OK	failover-smartdhcp.eip.local.org	1
10.2.0.0/16	16	255.255.0.0	DE-toto	65536	My_Company	N/A	N/A	No				OK	failover-smartdhcp.eip.local.org	1
10.2.4.0/23	23	255.255.254.0	berlin	512	My_Company	1.0%	505	Yes	VLAN Europe	200	Berlin - 1	OK	failover-smartdhcp.eip.local.org	1

Organizational diversity implies large numbers of diverse subnets and therefore drives the need to employ VLANs to protect and isolate networks, groups, projects, etc. To be successful, VLAN initiatives need to be coordinated and consistent with the IP addressing plan. Inconsistent alignment will jeopardize network security and the continuity of services to users. By extension, VLAN management can be enriched with VxLAN with adoption of networking fabrics and software defined networking which like using overlay networks to ease their deployments.

Ensuring Applications Availability with State of the Art DNS-DHCP Services

Students and faculty alike rely upon immediate and quality access to network-driven technology. Voice and data services have become a standard by which institutions are measured. Secure and reliable network access has become an expected amenity in the same way that dorm facilities are expected to provide beds and lavatories.

As in any network infrastructure, high availability of DNS and DHCP services guarantees users continuity of access to the network and to applications (e-mail, online courses, videos, and internet). Special University assets, such as laboratories, may require those services locally whereas general and centralized DNS-DHCP service is adequate for classrooms and lecture halls. In all cases the service has to be efficient and dependable at an affordable cost.

Control Network Infrastructures Automating IPAM-DNS-DHCP Management

Poorly managed services lead to a loss of visibility for the entire network infrastructure. In situations like this, there is a real risk of deploying conflicting networks, blocking communications and leading to service unavailability. Maintaining control over these service-interruption risks requires in-depth knowledge of the network and how it is structured. By unifying and automating management of the IP plan, VLANs, and DNS-DHCP services, it provides the visibility that is essential for ensuring the overall consistency of the server configurations and eliminates all risks of network downtime.

With the adoption of new security solutions like NAC (Network Access Control) in addition to traditional firewall filtering, the integration of the DDI solution as the central repository of information into the overall networking ecosystem is essential. API and webhooks are mandatory on all the solutions to be able to automate actions, configuration and ease troubleshooting now that most university activities rely on a functional, secure and powerful IP network.

2» MOOC & BYOD means Service Control and Security

Meeting the Need for Autonomy While Maintaining Centralized Control

Within Universities, disparate entities require autonomy when administering their network. For example, labs or research units need to be able to quickly deploy equipment in order to set up their experiments. For administrators, this has to be done without risking impact on the production network. This requires maintaining visibility and control over the deployments that are done locally.

Offering Flexibility While Blocking External Threats

Meeting the needs of a highly mobile, and oftentimes remote, student population offers more flexibility through distance learning and by authorizing the use of smartphones, tablets, and personal computers, but raises problems in managing equipment and security. The balance between an open network and strong security is a challenge that Universities cannot avoid.

Establishing a Framework for Use of Mobile Devices

University network capacity planning typically provides for an average of 10 pieces of equipment per capita, including laptops, telephones, and tablets. In fact, while the University replaces its own equipment every three to five years, users replace their devices every one or two years. So, even if the number of users is not increasing greatly, the number of connected devices is undergoing exponential growth. To limit infrastructure security risk, it is crucial that these devices be identified and tracked on the network.

3» New Trends and Capacity Planning

MOOCs have been adopted by universities and students, and this trend has been accentuated by the 2020 pandemic, so we are seeing new trends that may change the way knowledge is shared and acquired with a mix of in-person and online activities and perhaps changes to how the academic year is organized for students and therefore for teachers and staff. All the major universities (e.g. Ivy League Schools in USA) now have content available, full graduation programs and have adopted digital approaches. The way the IT infrastructure will be solicited by users is changing with cloud adoption, wireless networking, high speed access and new usages. So the I&O teams need to adapt their approach and their solutions accordingly.

The University population is a uniquely mobile one. Students typically change buildings several times a day between classrooms, library, association offices, the cafeteria, and even outdoors or remotely for online courses. Observing consumption trends on equipment like switches and wireless access points enables the network team to determine the infrastructure’s hot points and then adapt the deployment of resources and equipment accordingly.

For example, the vast majority of devices are connected to a University’s infrastructure via Wi-Fi. By analyzing the consumption trends of IP addresses, the network team determines which areas of the campus need to be equipped with Wi-Fi infrastructure on a priority basis (library, leisure spaces, etc.) and sets the required performance levels. This analysis optimizes resource use and load distribution while preventing unnecessary investments in new equipment. DHCP scopes can therefore be adjusted accordingly to support massive student moves between lecture rooms. In addition, DHCP needs to provide leases at a high pace to accommodate these moves, by offering short lease duration generally associated with such scopes.

In order to protect students and researchers on their Internet journey, DNS security with a complete set of solutions like behavioral analysis, reputation filtering and allow/deny list management can increase confidence in using the university network rather than any other available public one.

Precise DDI services monitoring provides a critical view into resource consumption trends which in turn ensures a high-quality user experience by enabling the institution's ability to quickly deploy new infrastructures, services, and sites.

Where DDI Meets BUSINESS

EfficientIP Comprehensive DDI, VLANs and Device Interfaces Management Solution

EfficientIP's SMART DDI solution offers comprehensive and integrated management of DNS/DHCP/IPAM and VLANs/VRF with devices and their network interfaces in a single process. The SOLIDserver™ DDI appliance defines and manages the complex relationships between all IP related resources. This unique and holistic solution ensures unrivaled automation of DDI deployment processes, delivering true support of business operations objectives.

EfficientIP provides a comprehensive suite of features that intelligently simplify and automate design, deployment, and management of IP network infrastructure:

- Unified and integrated management of IPAM, DNS, and DHCP with VLANs/VRF organizations and a network device interface repository
- Native capacity to integrate Enterprise policies, automating best practices enforcement
- Enterprise provisioning, process modeling, and automation
- Complete reconciliation management of the network infrastructure
- DNS security for device and application protection

SOLIDserver™ SMART DDI technology ensures high availability, security, and automation to guarantee that your network infrastructure will actively support your business requirements.

This revolutionary and comprehensive DDI solution delivers high availability, elastic scalability, and advanced security, all built on a foundation of policy-driven management and automation. This is how EfficientIP defines the next generation of DDI solutions. This is SMART DDI.

Smart DDI Key Benefits

- Universal visibility, control, and management of the network infrastructure
- Decrease operating costs; efficiently support company growth and productivity with intelligent and policy-driven deployment automation
- Increase network reliability and security with error-free configurations, centralized management, and best practices enforcement
- Anticipate problems with proactive services monitoring, user-defined reports, and network asset tracking
- Increase efficiency with smart task delegation and DDI workflow management
- Secure network users and protect infrastructure using advanced DNS security solutions

efficient iP™

REV: C-210111

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.