20-10-2021

HEAnet OAV Architecture Analysis White Paper

Grant Agreement No.:	856726
Work Package	WP6
Task Item:	Task 2
Dissemination Level:	PU (Public)
Document ID:	GN4-3-21-3072d3a

Authors: Dónal Cunningham (HEAnet), Eduardo Jacob (EHU/RedIRIS), Estela Carmona Cejudo (I2CAT/RedIRIS), Iacovos Ioannou (CYNET), Ivana Golub (PSNC), Jasone Astorga (EHU/RedIRIS), Kostas Stamos (GRNET), Maria Isabel Gandia Carriedo (CSUC/RedIRIS), Roman Lapacz (PSNC), Simone Spinelli (GEANT), Sonja Filiposka (UKIM/MARnet), Susanne Naegele-Jackson (FAU/DFN), Tim Chown (JISC)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

The document analyses the mapping of the HEAnet architecture to the TM Forum's Open Digital Architecture, aiming to provide a standardised view of the components and implementations of orchestration, automation, and virtualisation within the National Research and Education Networks (NRENs).

Table of Contents

Table of Figures

Executive Summary

Analysing National Research and Education Network (NREN) architectures from an orchestration, automation, and virtualisation (OAV) point of view, using a common reference architecture, helps align efforts, and find similarities in the way different functionalities and components are implemented, which in turn facilitates potential collaboration between organisations, and future interoperability. In pursuit of this goal, the GN4-3 *Network Technologies and Services Development* Work Package (WP6), *Network Services Evolution & Development* Task (T2) selected the TM Forum Open Digital Architecture (ODA) as a reference blueprint architecture that can be used for such cross-comparison. The rationale for that choice is described in Deliverable D6.6 *Transforming Services with Orchestration and Automation* [DEL].

The WP6T2 team is working with NRENs to perform such mappings. In this document the team reports on an analysis of the different functional aspects of the HEAnet service management architecture, and how their components map to the ODA reference model. The mapping highlights the main characteristics and capabilities of the current HEAnet architecture, and how they fit into the main functional domains of ODA. The analysis was carried out in July 2021 by the WP6T2 team, supported by HEANet network architects.

1 Introduction

This document analyses the components of HEAnet's service management architecture, focusing on the Orchestration, Automation and Virtualisation (OAV) aspects of its implementation, and how these map to the TM Forum Open Digital Architecture (ODA). The NREN community can use this analysis to compare their own components and approaches with those of HEAnet; they may find similarities which inspire them to work together on their journey towards OAV. This mapping is part of a set of mappings of different NREN management architectures against ODA, thus providing a common reference point, and the means for a cross-NREN comparative analysis of components and approaches [DIS].

HEAnet is Ireland's National Research and Education Network. It provides connectivity and additional IT services to all education and research institutions in the country - including primary and post-primary schools, universities, colleges, institutes, research organisations, etc. The NREN was initially established in 1983 and is funded by The Department of Education and the European Commission. HEAnet currently serves almost 80 clients [AHN] and is well along the path of implementing its 2020-2022 Strategic Plan whose vision is to enable Ireland's digital ambition through technology in education. The high-level network map is presented in Figure 1.1.

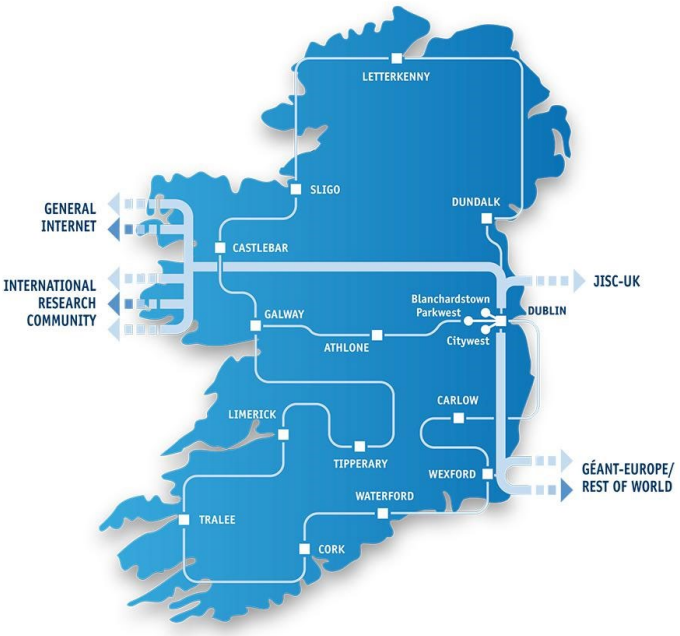

Figure 1.1: HEAnet network

The main group of services that defines HEAnet's portfolio includes:

- Network connectivity
- Identity management and authentication
- Brokerage of cloud services
- ICT security and research engagement [HNS]
- File, media and web hosting
- Federated single sign-on (SSO): Edugate
- Video streaming services

All HEAnet-provided services are based on the premise of providing common, repeatable, and shareable solutions for the whole education sector. One of the latest efforts by the NREN is the "eduroam Everywhere" project [EDU] which plans to extend eduroam coverage to public libraries, buildings, and spaces outside campuses, as well as to private commercial infrastructure such as conference centres and public transport. A pilot with Dublin Bus is underway.

The standards of service delivery provided by HEAnet are outlined in the Client Charter [HCC].

The main values championed by HEAnet are integrity, openness, collaboration, enthusiasm, and cost-efficiency. Therefore, it is of great importance to HEAnet to deliver common, repeatable, and shareable solutions to its client community. This commitment strongly shapes HEAnet's attitude towards service management and the related OAV processes.

When it comes to the network infrastructure, HEAnet continuously upgrades and expands its network. The core of this infrastructure is a flexible multi-layered national fibre network which is directly operated by HEAnet. In line with the HEAnet Strategic Plan (and capacity projections for the coming years), a new national IP backbone was rolled out in 2019. The Dublin Core Optical network was upgraded in 2020. Through a combination of traffic forecasting and network planning, HEAnet continues to provide its existing and new clients with scalable internet and cloud connectivity [HAR] at all times.

As a response to the recent pandemic and the shift to online platforms and blended learning in schools, HEAnet has also upgraded its high-speed connectivity and content filtering for Ireland's primary and post-primary schools. In this way, smooth support for extensive use of tools such as Microsoft Teams and Google Classroom has been provided. In addition, during 2020, the bandwidth of almost 350 post-primary schools was upgraded. This resulted in over 70% of post-primary schools having connectivity speeds of between 200 and 500 Mbps. HEAnet is currently working on a fast-track two-year programme to upgrade the connectivity to 679 primary schools by the end of 2022 as defined in the National Broadband Plan. Secondary schools are all connected with symmetric circuits of at least 100 Mbps. Network connections to schools are implemented using a mix of technologies, including fibre, radio, and DSL.

All HEAnet services have defined service level agreements (SLAs) and are supported via the HEAnet Service Desk with a second tier of support provided by different expert teams. HEAnet also maintains a separate "Out-Of-Band" network that enables engineers to troubleshoot issues remotely when network issues occur.

HEAnet's work is implemented through the joint efforts of several different teams:

- Technology teams:
  - Networks operational team – in charge of the national backbone network and networking hardware used in the HEAnet data centres.
  - Innovation R&D team – responsible for network design and planning, service engineering, research engagement and piloting, as well as development of network-related R&D projects.
  - Systems team – provides IT systems support, in particular, VMware and Unix system administration.
  - Services Architecture team – tasked with service design and software development, including activities such as building and piloting new services, and defining procedures and policies for service operation.
- Security team –the resident CIRT in charge of pen testing, security audits, etc.
- Finance and HR teams - support all other internal teams in the organisation.
- Support teams:
  - Client Services team –a first point of contact with new clients and service orders.
  - Service Desk team – first line of support for services.
  - Schools operational team - focused on the support of primary and post-primary schools (students approximately 5-19 years old).

The ICT security services provided by HEAnet focus on supporting and improving the security posture of its clients by providing them with risk profile analysis, threat defence readiness, and up-to-date intelligence on future threats. Since 2019 all higher education clients have been subscribed to the service, and HEAnet acts as the focal security service provider. HEAnet's ICT Security Service comprises a number of individual security services such as ICT security and risk assessment, ICT policy review and development, provision of network security perimeter assessments (including penetration testing and vulnerability scanning), phishing simulation campaigns and reporting, security awareness training, and collaboration and provision of a Security Forum. All of these are provided by a dedicated HEAnet ICT Security Services team that also delivers security awareness training - both on-campus and online.

EduCampus is a special HEAnet subsidiary that provides consolidated business-critical ICT application services and Management Information Systems (MIS) systems to the Higher Education and Research sectors in Ireland [HAR]. These include a Student Records Management System, an HR and Payroll Management System, a Finance Management System, and a Library Management System.

2 Architecture Analysis

2.1 High-Level OAV Approach

HEAnet's OAV architecture analysis has been conducted using the TM Forum Open Digital Architecture's (ODA) [ODA] functional blocks as a reference point. The TM Forum ODA is promoted as a blueprint for new digital industry architectures, and the rationale for its selection as a reference model by the GN4-3 WP6T2 team is given in Deliverable D6.6 *Transforming Services with Orchestration and Automation* [DEL]. The ODA documentation set provides common terminology, a minimum set of core design principles, and groups of decoupled functionalities. Together they define the requirements for the implementation of an agile model-driven service management architecture that incorporates orchestration and automated operations - across both virtualised and hybrid environments.

The main idea behind ODA is component decoupling and integration. This enables an independent choice of solutions for each component while at the same time maintaining a unified overall approach that supports the full end-to-end service lifecycle (including interoperability). The high-level ODA functional architecture maps the main components by their capabilities to the ODA function blocks (see Figure 2.1).

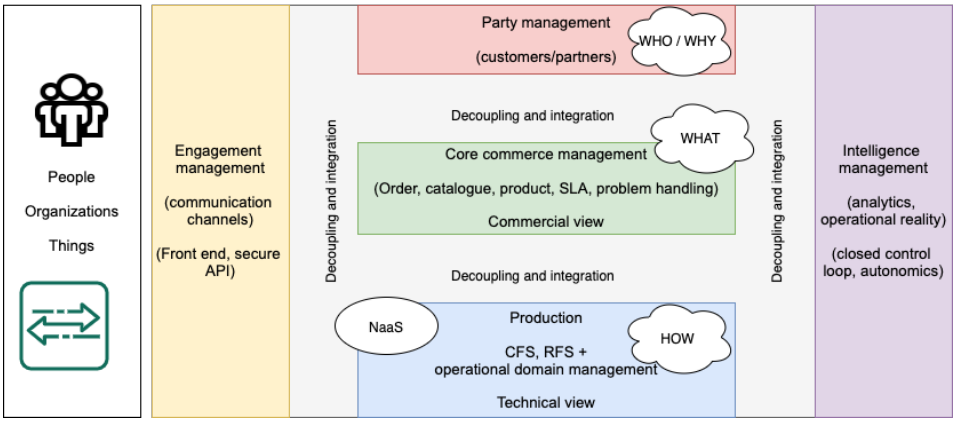

Figure 2.1: The TM Forum ODA functional architecture

In a nutshell:

- The Party Management functional block handles the processes that are related to all parties that interact with the organisation, defining their roles and relationships.
- The Intelligence Management functional block describes the implementation of data analytics processes and, based on an analysis of these processes, provides closed control loops for full automation wherever possible.
- The Core Commerce Management functional block focuses on the placement of products and services to the customers, and manages the product lifecycle.
- The Production functional block manages the delivery and lifecycle of all customer-facing and resource-facing services that can be based on different technologies or might be a combination of multiple operational domains, including multi-domain services provided in cooperation with other parties.

2.2 Mapping to ODA Functional Architecture

When put into context of the TM Forum ODA functional representation, the HEAnet service management architecture components can be represented as shown in Figure 2.2. The white boxes in the diagram represent HEAnet architecture components, and their placement within the ODA functional blocks is defined based on their main functions. If a component contains complex multi-faceted functions, it is broken down into sub-components which are placed in the respective functional block.

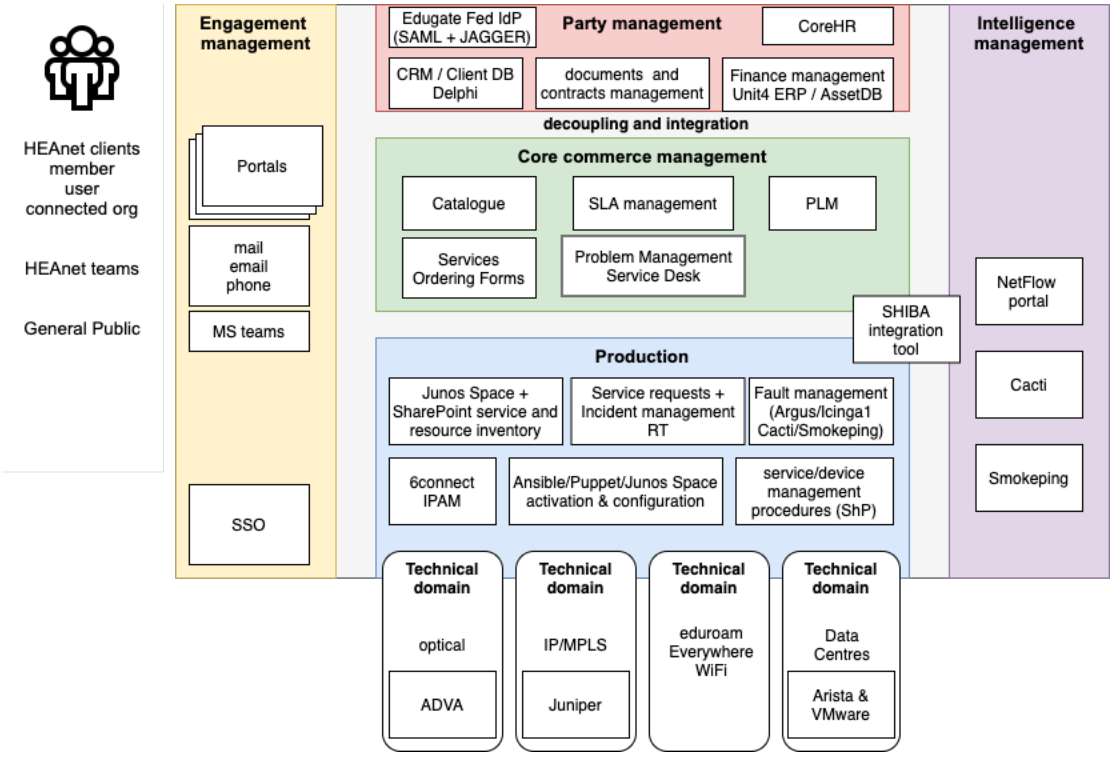

Figure 2.2: HEAnet management components mapped to the TM Forum ODA

2.2.1 Engagement Management

HEAnet hosts a number of web portals hosted that provide all the information related to the services offered to their clients, including general and marketing information, links to order forms for the various services, and contact information for reporting problems and submitting queries. The main website [HNW] is the starting place for the client journeys that can then continue via email, phone, or post-communication channels. There is also a managed Netflow portal for more detailed traffic analysis. This portal has proven to be useful for troubleshooting security and technical concerns, and also provides insights into the network utilisation. The portal also provides a link to the public tickets that are published by the Network Operations Centre (NOC).

The Client Services team is responsible for any initial enquiries from prospective clients together with the HEAnet NOC Service Desk where any issues can be reported (via phone or email).

Internally, HEAnet teams use Microsoft Teams to communicate and synchronise their work.

All detailed information provided to clients via the portals is accessible after going through a single sign-on (SSO) process integrated with federated identity management tools. The Edugate service partners with eduGAIN which is run by GÉANT, and enables easy access to federated services in the education sector via a network of over 2600 identity providers and 1800 service providers [EDG].

2.2.2 Party Management

HEAnet provides services to three categories of client organisations: member, user, and connected organisations. Member organisations have an active role in the HEAnet management, are connected to the network, and are eligible to subscribe to any service. User organisations are types of organisations that are connected to the network, and are eligible to subscribe to services as decided by the HEAnet Board. Connected organisations are only eligible to connect to the HEAnet network.

SSO is provided via HEAnet's Edugate service which is the cornerstone of Federated Identity for education in Ireland. The Edugate federated access is implemented using the SAML protocol and an additional tool, JAGGER, which was developed in-house by HEAnet. In addition to SAML and Shibboleth, HEAnet also offers managed IdP service support for Microsoft's Azure Multi-Factor Authentication (MFA) and Cisco's Duo MFA. They also support Microsoft's cloud-based user directory management platform.

For customer management purposes, an internal database called ClientDB was developed. It is owned by the Client Services team and stores information about clients including:

- Contact info (with several well-defined roles)
- Mailing lists
- Postal Address
- Services information including sites, circuit ID, domains, IP addresses, etc.

HEAnet is in the process of moving to a new Microsoft-based CRM that will take over storing client information from clientDB. However, clientDB will still be the place where the connection between customers and services, i.e. subscription information, is maintained.

In 2020, the HR team migrated their work to a newly developed Human Resource Information System (CoreHR). The Finance team uses a specialised finance system, Unit4 ERP.

HEAnet also developed an internal tool, assetDB, to track the financial information about significant purchases (including network devices): quantities, locations, decommissioning and disposal information, related invoices, etc.

2.2.3 Core Commerce Management

The catalogue of available services is provided on the main HEAnet website [HNW] which displays basic information about each service as well as detailed service specification documentation. All services are divided into five different service levels:

- level 1: brokered agreements
- level 2: services provided by third party
- level 3: pilot services
- level 4: managed services with client-side responsibility
- level 5: fully managed services

There are also links to each service's SLA documents which can be accessed via SSO. The primary SLA metric is service availability. Clients receive quarterly SLA reports for the network services.

HEAnet has also established a services pipeline that defines the product lifecycle management (PLM) process, from new service proposals to the design, pilot, and production stages.

As a part of the service catalogue, links to application forms for requesting/ordering services are available, for example, for ordering web hosting [HSO]. Once these forms are completed and the order is submitted, the HEAnet Client Services team is notified, and the established process for service fulfilment is started. The Client Services team also prepares all agreements as necessary and liaises with the Finance team for billing purposes.

The Service Desk team is the first point of contact for all technical issues and queries. The team provides support during business hours, while out-of-hours support is handled via on-call rotas of engineers. During office hours, the Service Desk Manager and Service Desk Engineers respond to queries, problems, and reported incidents according to clearly stated time frames that are defined in the Client Charter [HCC]. In cases when a more complex issue needs to be resolved, the team forwards the information to the appropriate HEAnet team.

Any information that is considered to be important for public dissemination is provided in a specialised Public ticket list [PTL] which also includes a full historical archive of all public tickets.

To support schools in case of a problem, there is a separate dedicated Schools Broadband Service Desk operated by a third party that provides first-line support. If a ticket is escalated, HEAnet provides support through the HEAnet Service Desk (that in turn contacts the Schools NOC team) or out-of-hours via an on-call rota.

2.2.4 Production

All technical work related to services is done by the Operational teams which use the RT ticketing system to track and synchronise their activities. Every action is announced by sending an email to the official NOC email address (which automatically generates a ticket), and different types of work are categorised into different ticket queues. The internal HEAnet knowledge base contains detailed procedures for the activation, configuration, and fault management of both services and resources.

The Service Desk triages any tickets in the system that have been created from external queries, such as service problems or incident reporting. Based on the type of problem (network, systems, or security), they assign the ticket to the appropriate team. The Service Desk is also responsible for linking the ticket and the customer whose services are affected.

All alarms that come from HEAnet monitoring systems are pushed to a web page and are also copied to the NOC email where they generate/update trouble tickets. The ticket correlation process is executed manually - teams collaborate and decide which tickets need to be combined.

Overall network monitoring is done using the network status page which can be set to be viewed as a web browser sidebar by the engineers [HSB]. The sidebar includes information on Edugate servers, DDoS alarms (DDoS mitigation service is provided by Jisc), internal services, network services (such as P2P), and systems (e.g., IdP servers, hosts, reboot info, etc.). When a problem is spotted, team members react accordingly.

HEAnet's fault monitoring systems are based on a distributed instance of Icinga2 referred to internally as Argus. It is used to monitor both service components and the devices which provide them. The 24/7 monitoring (mostly done using SNMP but starting to use streaming telemetry) covers both virtual and physical hosts, hardware devices such as PDUs and webcams, Virtual Machines, Jarvis, 6Connect, data centre health (including Arista switches), AssetDB, and instances in the AWS and Microsoft Azure clouds.

6connect [IPP], which has its own web GUI, is the commercial tool of choice for IP address management (IPAM), supporting both IPv4 and IPv6 addresses . The IP address allocation process is mostly manual; however, the 6connect API is used to provision some network reverse DNS ranges.

Documentation relating to the network and client-facing services is held in SharePoint.

2.2.4.1 *Automation and Integration Tools*

In the backbone network all IP services, L3VPNs, and E-lines are created using Junos Space's Connectivity Services Director (CSD) component, typically using a web GUI and a library of predefined templates. Junos Space also acts as a backbone network device inventory for storing attributes and version-controlled configurations of Juniper devices, and as the single source of truth for all non-data centre equipment [HNO].

Once a circuit is created, an internally developed integration tool named SHIBA (Space/HEAnet Integration Broker Application, see Figure 2.3) takes information from both Junos Space and 6connect, and notifies Argus to start monitoring the new circuit. In addition to the automated provisioning of Icinga and Cacti, it also integrates related DNS information.

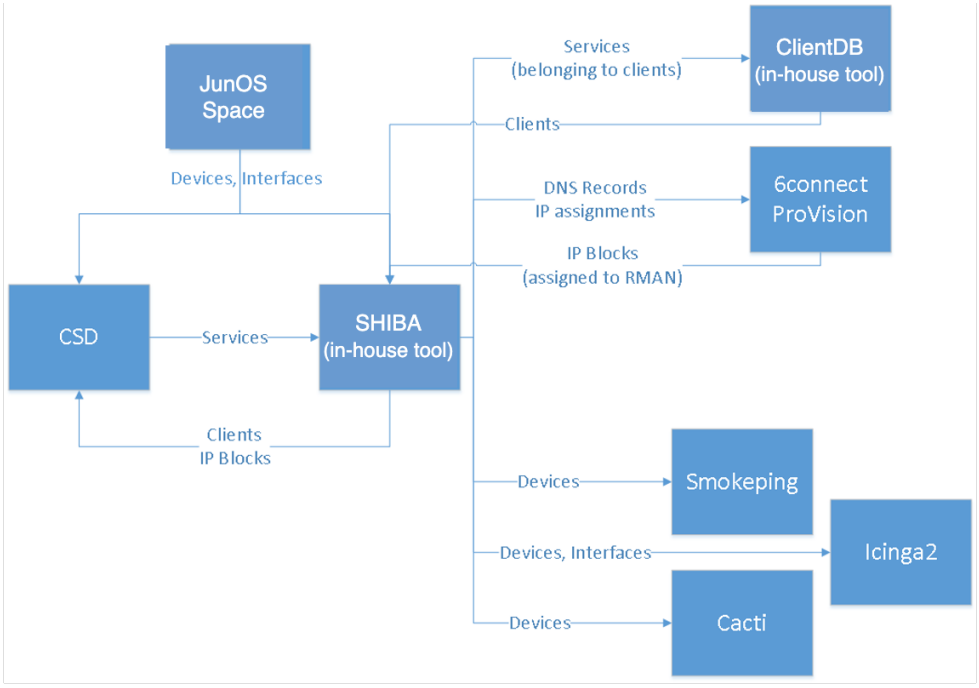

Figure 2.3: SHIBA integrating with other components [TNC]

Puppet is used to automate the commissioning and configuration of systems and hosts. Ansible is used to build network device configurations. Terraform is used for cloud provisioning. Network device configuration is done using Ansible, but circuit builds are done using CSD. The device information is kept in the internal Ansible inventory which is managed manually. Connecting to devices via SSH is only allowed for troubleshooting purposes. However, once the problem is identified, the fix is retroactively applied to the Ansible configuration files.

Capirca is also used for ACL generation for HEAnet's Data Centre infrastructure [CAP], where it protects the services that are running on VMWare virtual servers. This is an open-source project that was originally developed by Google to enable fast development and deployment of network access control lists for a wide variety of platforms.

2.2.5 Technical Domains

Considering the implementation specifics, the HEAnet network infrastructure can be divided into four main technical domains:

- **Optical Network** – as the national backbone network is built using ADVA optical equipment, ADVA kit is used to multiplex connections onto the single pairs of fibres. There are two loops of fibre around the country, while a third has been deployed in Dublin. Circuits on the optical layer are built using an ADVA GUI app.

- **IP/MPLS Network** – the IP/MPLS network consists of Juniper MPLS routers. Dual stack (IPv4 and IPv6) is supported, and IP routing is done in the Juniper global inet.0 and inet.6 tables. E-lines are implemented using MPLS Layer 2 tunnels, and L3VPN services are available. MP-BGP is also used for advertising different types of addresses. The network is based on Juniper devices, and Ansible is used for initial device installation and configuration. CSD is used for circuit provision and modification.
- **Data centre** – HEAnet has an active project that aims to consolidate and optimise data centre space until 2025. The project aims to remove two of the six PoPs in use by migrating the services to the rest of the locations. The project started as a result of the recent trend of moving to commercial cloud platforms. The project also includes a process for integrating data centre and network administrators. The data center networks are built using Arista DCS switches and support a significant VMWare footprint. A recent upgrade cycle has allowed HEAnet to implement network function virtualisation (NFV). In addition, HEAnet is increasing its use of Docker virtualisation and has already spun up several clusters to support this work. HEAnet hosts its own distributed Gitlab repository, and considerable use is made of its CI/CD capabilities.
- **eduroam** – At the moment, eduroam is offered via more than 160 locations across Ireland, such as libraries, sports venues, and public transport. HEAnet's ambition is to make eduroam Wi-Fi available to students as much as possible, everywhere. In pursuit of this goal, the eduroam Everywhere project (currently underway) seeks to expand the number of sites at which eduroam is made available.

2.2.6 Intelligence Management

At the moment HEAnet does not use any prediction methods or intelligence-based analysis on the gathered log files. The information is stored for enhanced visualisation, in-depth fault analysis, correlation, and capacity planning.

In addition to the tools referred to in the previous section, a separate NetFlow portal provided by Kentik is available to all clients. The portal helps clients to obtain a high-level view of their network traffic. Visualisation portals showing traffic graphs (based on Cacti [CVP]) and latency (Smokeping [SVP]) are also made available to clients.

3 Conclusions

HEAnet serves over a million Irish learners at all stages of their lives - whether in schools, colleges, or universities - as well as the Irish research community. Given the ever-growing number of services, users, and devices, HEAnet must leverage the benefits of OAV to maximise its impact and reach, while minimising cost, downtime, and engineering resources.

The HEAnet methodology for developing and implementing services is based on the premise of common, repeatable, and shareable solutions. All three are necessary for the effective digital transformation of an organisation, and the recognition of this need enables the creation of an environment that can easily adapt to dynamic changes and drive higher rates of customer satisfaction. This attitude towards services has enabled HEAnet to implement automation wherever repeatable tasks are found while also recognising the importance of moving to virtual infrastructures for hosting services (whether on-premise or using cloud solutions).

This architectural analysis has shown that HEAnet uses a mix of commercial, open source, and in-house-developed tools to implement different parts of the established working processes of the full service lifecycle. The specific highlights include a well-established PLM pipeline for the development of new services, and the development of an in-house integration tool (SHIBA) that enables the orchestration of the service-provisioning process by forwarding the necessary information to the monitoring tools that are used to track a service's SLA once it is in place.

HEAnet also has considerable automation and orchestration experience - developed through managing both the backbone network and the data centre network through the use of Ansible, Puppet, and the successful use of device configuration change tracking and reconciliation. HEAnet's journey towards OAV can be used as an inspiration by other NRENs that are starting to implement OAV in their network management procedure.

References

[AHN]	https://www.heanet.ie/who-we-are/who-we-are
[CAP]	https://github.com/google/capirca
[CVP]	https://graphs.heanet.ie
[DEL]	GN4-3 D6.6 *Transforming Services with Orchestration and Automation*, November 2020, https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D6.6-Transforming_Services_with_Orchestration_and_Automation.pdf
[DIS]	(White) Papers, Milestones and Other Documents, OAV wiki, https://wiki.geant.org/display/NETDEV/Dissemination
[EDU]	https://www.heanet.ie/services/connectivity/eduroam-everywhere
[EDG]	GEANT eduGAIN service, https://www.heanet.ie/services/identity-access/edugate#how-to-join-edugate
[HAR]	HEAnet Annual Report & Financial Statements for 2020, https://www.heanet.ie/wp-content/uploads/2021/06/AR2020.pdf
[HCC]	HEAnet Client Charter, 2020, https://www.heanet.ie/wp-content/uploads/2020/08/HEAnet-Client-Charter.pdf
[HNO]	Donal Cunningham, *HEAnet OAV Overview*, TNC 2021 OAV BoF, https://events.geant.org/event/903/contributions/716/attachments/517/694/HEAnet-Donal-OAV_summary_v3.pdf
[HNS]	https://www.heanet.ie/services
[HNW]	https://www.heanet.ie/
[HSB]	https://sidebar.heanet.ie
[HSO]	https://webforms.heanet.ie/webhosting
[IPP]	https://6connect.heanet.ie
[ODA]	TM Forum, GB998 *Open Digital Architecture (ODA) Concepts & Principles* v2.1.0, March 2021, https://www.tmforum.org/resources/reference/gb998-open-digital-architecture-oda-concepts-principles-v2-1-0/
[PTL]	https://ticketing.heanet.ie/public/index.html
[SVP]	https://smokeping.heanet.ie
[TNC]	Eoin Kenny, *Orchestration, Automation & Virtualisation BoF*, TNC, 2019, https://wiki.geant.org/display/NETDEV/OAV+BoF+@+TNC19?preview=/123793644/123793889/TNC19-OAV-HEANet-v1.pdf

Glossary

ACL	Access-Control List
API	Application Programming Interface
AWS	Amazon Web Services
BGP	Border Gateway Protocol
CI/CD	**C**ontinuous Integration / Continuous Delivery
CIRT	Computer Incident Response Team
CRM	Customer Relationship Management
CSD	Connectivity Services Director
DB	Database
DDoS	Distributed Denial of Service
DNS	Domain Name System
DSL	Digital Subscriber Line
GUI	Graphical User Interface
HR	Human Resources
ICT	Information and Communications Technology
IdP	Identity Provider
IP	Internet Protocol
IPAM	IP Address Management
Mbps	Megabits per second
MFA	Multi-Factor Authentication
MIS	Management Information Systems
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
NFV	Network Function Virtualisation
NOC	Network Operations Centre
NREN	National Research and Education Network
OAV	Orchestration, Automation and Virtualisation
ODA	Open Digital Architecture
PLM	Product Lifecycle Management
PoP	Point of Presence
PTL	Public Ticket List
R&D	Research and Development
SAML	Security Assertion Markup Language
SHIBA	Space/HEAnet Integration Broker Application
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSO	Single Sign-On

T	Task
VM	Virtual Machine
VPN	Virtual Private Network
WP	Work Package