Next Generation Access Network – ADDONAS Project Approach

Artur Binczewski, Wojbor Bogacki, Łukasz Dolata, Szymon Kuc, Łukasz Lechert, Łukasz Podleski, Miłosz Przywecki, Maciej Stroński, Jan Węglarz
PSNC, Noskowskiego 12/14, 61-704 Poznan, Poland
e-mail: {artur|wojbor|ldolata|skuc|llechert|docere|mprzyw|stroins|weglarz}@man.poznan.pl

John Dunne
Intune Networks Belfast Limited, 5G Weavers Court Business Park, Belfast, BT 12 5GH, Northern Ireland.
e-mail: john.dunne@intunenetworks.com

Andre Oehlschlaeger
KEYMILE GmbH, Wohlenbergstrasse 3, 30179 Hanover, Germany
e-mail: andre.oehlschlaeger@keymile.com

Dimitra Simeonidou, Georgios Zervas
University of Bristol, Merchant Venturers' Building, Woodland Road, Clifton BS8 1UB Bristol, England
e-mail: {dimitra.simeonidou | georgios.zervas}@bristol.ac.uk

Paper type
Research Paper

Abstract
The ADDONAS project proposes architecture solutions for access/metro networks in two areas - at the infrastructure level and on the software control level.

Taking into account infrastructure level innovative joint metro/access architecture has been proposed in order to allow end users to access services with high bandwidth using symmetric connections on the last mile. It is proposed to change today’s concept of an Access Network from a passive transport element into an active element in the delivery of new services.

At the software level a SDN based system for service delivery has been proposed that will allow flexible service delivery. ADDONAS extends nowadays service delivery model allowing using and controlling simultaneously number of services with guaranteed Quality-of-Experience.

Keywords
Access networks, software defined networking, openflow, optical packet switch and transport
1. Introduction

A number of last mile technologies is used nowadays to connect residential end-users to the network. Access networks are built using different technologies like cable, wireless or a number of PON and DSL variants. Most of these technologies often offer asymmetric connection providing smaller amount of bandwidth on the upstream direction than in the downstream. Moreover, the user is usually bound to the services offered by his infrastructure provider being forced to access other services in the Internet without any guarantee of the quality. In the ADDONAS project a new network architecture following Open Access Network (OAN) [OASE, OAN] concepts allowing the user to choose services from any Service Provider present in the metro architecture as well as SDN [SDN] based control has been proposed to solve most of the above mentioned problems.

2. The ADDONAS architecture

The ADDONAS project proposes architecture solutions in two areas - at the infrastructure level as well as on the software control level thus providing complete solution for access/metro networks [AD21].

![ADDONAS infrastructure and software](image)

At the software level (see Figure 1) a SDN based system for service delivery has been proposed that will allow flexible access to services. ADDONAS extends nowadays service delivery model allowing virtualization of the infrastructure for simultaneous delivery of services through multiple virtual service operators. To achieve this goal ADDONAS assumes existence of the three main roles in the service provisioning architecture:

- **Infrastructure Provider (IP)** owns and controls physical resources in the ADDONAS architecture. In particular, networking resources consist of home gateways, access and metro network, as well as IT resources
- **Virtual Service Operator (VSO)** is offering services for the user. Services are provisioned over the physical infrastructure owned by Infrastructure Provider and are operated by Service Providers. One VSO can combine (through own ‘service market’) offers from many Service Providers, and on the other hand one Service Provider can be present in several different VSOs
- **Service Provider (SP)** is providing services in the ADDONAS architecture. Services are registered in a given VSO in order to be served for the users using VSO for advertising. However, Service Providers can also advertise by themselves (e. g. via public Internet network)
Taking into account infrastructure level (figure 1) innovative joint metro/access architecture has been proposed in order to allow end users to access services with high bandwidth. It is proposed to change today’s concept of an Access Network from a passive transport element into an active element in the delivery of new services. ADDONAS achieves this by using a 3-stage distributed “Layer 2” switch to flatten the metro and access networks, and combines this with a new level of functionality in the last mile. Distributed switch provides full-mesh topology of the metro network with constant number of maximum hops. ADDONAS then proposes the placement of Distributed Data Centers throughout the combined Access/Metro architecture to provide support for the advanced services and to maintain control how these services are delivered to the end user. Distributed Data Centers and full-mesh topology allows selection of Service Provider’s server taking into consideration multiple factors, like utilization of the network. Proposed architecture also includes active Ethernet CPE devices at the customer location and advanced access aggregation devices allowing symmetric 1 Gbps transmission over a single fiber (1000BASE-BX10 standard).

SDN approach combined with ADDONAS physical infrastructure provides support for user’s services as well as enables establishment of user’s networks. Symmetric links to the metro network allow users to provide their own services from the home. For example, users will be able to access their storage device located at home from their friend’s home or just create a VPN-like connection between two homes to share the files (without need of uploading photos on to external server).

3. SDN based architecture for service provisioning

Software Defined Networking is an emerging concept allowing users or applications to dynamically control the networks. In the ADDONAS this concept has been adapted to allow flexible control of the merged metro/access infrastructure. Detailed picture of the architecture is depicted on figure 2.

The main component of the architecture is Slice Controller (VSO) that enables service delivery for the users. It is divided into two sub-layers – Control Layer and Service Layer.

Service Layer is responsible for managing the users and services. It provides an open market where multiple service providers can offer their services for the end users and where users can also introduce their own services. It also processes users’ requests and performs service requirements assessment in order to setup, modify or teardown of the services. To deliver access to services each VSO uses own slice of the resources offered by the
Infrastructure Provider.

Management of the resources is done by the lower sub-layer of the Slice Controller – a Control Layer. A Control Layer is using an extended OpenFlow [OF] controller to define and manage flows for services that are provisioned within the slice. In general, two main types of services are defined in Control Layer – a virtual network that is used for access to the services and sub-slice which is autonomous part of VSO slice dedicated to the user. Control Layer is responsible for a creation of virtual networks interconnecting Service Providers and set of users endpoints taking into account network requirement. VSO slices can be dynamically extended to adapt usage of the resources thus allowing smooth addition of the new services.

Management of VSO slices is done by the Slice Supervisor responsible for handling the requests related to creation, modification or deletion of the slices as well as for inter VSO communication. Slice Supervisor updates slice policies in the Hardware Virtualization Layer in order to support separation of different VSOs. Hardware Virtualization Layer is responsible for virtualization of both network and IT resources. In HVL FlowVisor [FV] is used to virtualize the network. It receives requests from multiple controllers (VSO) using OpenFlow protocol and configures underlying hardware accordingly. An agent, located between the FlowVisor and the hardware, translating OpenFlow protocol into device-specific language will be also developed in the project in order to control hardware not supporting OpenFlow protocol.

The following subsections provide more details of ADDONAS architecture

### 3.1 Slice Controller (VSO) – Service Layer

The main function of VSO is to collect services offered by various Service Providers and to deliver these services as a single, combined solution. One VSO can combine offer of many Service Providers, and on the other hand one Service Provider can publish own offer in a few different VSOs. ADDONAS solution assumes operation one of multiple VSOs.

Service Layer in the ADDONAS project consists of the following components:

- Slice Management (SM),
- User Management (UM),
- SPs Management (SPSM),
- Service Assessment (SA),
- Authentication, Authorization and Accounting (AAA),
- Service Layer Resources Database.

The general view of components and most important interfaces has been shown on the Figure 3.

![Figure 3 Service Layer interfaces – general view](image-url)
The Service Layer manages the services using internal service definitions related to service types. Service types are directly related with service properties and its network and traffic requirements. Since underlying sublayer (Control Layer) is using OpenFlow protocol, each service needs to have own flow policy description. Flow policy is used for establishment of network connections but it can also be used to differentiate business offer.

The main element of the Service Layer is Slice Management, which is responsible for parsing and processing requests coming from the Application Layer over two interfaces: user (EXT-ASL.U) and service (EXT-ASL.SP) interface. Those interfaces allow management of the users’ accounts as well as management of Service Providers and their service offering. Additionally, Slice Manager, it is responsible for handling and delegating requests over the internal interfaces to the appropriate components. Basically the SM is a global proxy which hides the technical details and interacts with the other internal SL elements.

The Service Assessment component is one of the most important components of the Service Layer as it responsible for direct interaction with Control Layer, establishing the connections for the ordered services, notification of the accounting and billing services.

The User Management component is responsible for the end-customers management. The major functionalities of the UM are: registering new users and existing users from another VSOs, handling of the login and logout processes, management of user profiles and providing interface for the parent components.

The next component called SPs Management offers interfaces for the external Service Providers. It supports the registration process for service providers and provides functionalities responsible for the processing of basic assets (master data) i.e. services and service types.

Authentication, authorization and accounting (AAA) in the ADDONAS Service Layer is used to authenticate actors, and their privileges are determined by the authorization element. Accounting is used for providing information about usage of services in time and billing purposes.

The Service Layer Resources Database stores information about service providers, service types, services and end-customers as well as endpoints available in . It is a central data storage for a VSO and it means the VSO owns single SL Resources DB containing consistent operational data.

3.1.1 Service Layer interaction with the Service Provider and User

Currently there is a number of services available today both for residential and business customers. Support of these services in the last mile is typically provided by overprovisioning of available bandwidth along with some prioritization of the traffic (e.g. by using DiffServ\(^1\) or CoS field in the Ethernet frame).

In the ADDONAS architecture reservation of bandwidth (even on per service basis) should be possible to guarantee appropriate quality level by separation of different flows. Between VSO and Service Provider an interface has been designed in order to allow setup of combined network and IT services. As described in D2.1 [D2.1] there two main models of communication between USER, SP and VSO can be considered:

- User requests a service through VSO

![Figure 4 VSO as a proxy](image)

User requests a service through SP

![Diagram](image.png)

**Figure 5 VSO as an authorization node**

Depending on a chosen model a different approach is needed. In the first case, a complex interface between SP and VSO might be needed, capable of controlling all possible services. For example if user requests the access to the virtual PC in the cloud through VSO, SP should be notified in order to prepare a suitable virtual machine for that purpose. In the latter case (when user requests a service through SP) SP can perform all service-related steps in their own system and just ask VSO for providing necessary resources.

<table>
<thead>
<tr>
<th>Model</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>User requests a service through VSO</td>
<td>User contacts with VSO only</td>
<td>Complex control of services (actions specific for a particular service)</td>
</tr>
<tr>
<td></td>
<td>Uniform way of service presentation can be assured</td>
<td>Introduction of new types of services may require extension of the interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>between service provider and VSO</td>
</tr>
<tr>
<td>User requests a service through SP</td>
<td>Independent control of services (Service Provider can setup the service, VSO is used to provide the network).</td>
<td>Authorization has to be done through VSO</td>
</tr>
<tr>
<td></td>
<td>Introduction of new services shouldn’t require modification of SP-VSO interface</td>
<td></td>
</tr>
</tbody>
</table>

Service Providers can also request additional resources from VSO in order to extend their service offering and users can also register their own services.

### 3.2 Slice Controller (VSO) – Control Layer

The main function of the Control Layer is to provide mechanisms for resources provisioning for services. The Control Layer is responsible for configuration and controlling of the following elements: Data Center, Metro and Access network devices. Slice Controller is built with use of Network Operating System which consists of six components: Control Management, Monitoring, Network & IT Resources DB, Virtualized Resources DB, Virtualization and Service Composition.

The overall architecture has been shown on the figure below.
Virtualization is responsible for a calculation of Virtual Network (V2N) between specified endpoints. In the path computation process heterogeneity of the services (which imposes different requirements on the parameters of the network) as well as current resources utilization is taken into consideration. Information about all Virtual Networks (V2Ns) created within the VSO slice is stored in the Virtualized Resources Database. It can be considered as a database storing logical topology of the services established within the VSO slice.

Network & IT Resources Database contains physical topology, over which Virtual Networks can be created. However, this topology is limited to information received from the Hardware Virtualization Layer (FlowVisor) and it is topology of the own VSO slice. Within ADDONAS architecture there is also a possibility to create a sub-slice, which is part of the physical infrastructure (unlike Virtual Networks (V2Ns), which are created as a set of flows to support services). Information regarding these sub-slices is also stored in this database. Apart from information about network devices, connections between them and flows Network & IT Resources Database stores also information about endpoints (in the form of physical service providers machines as well as user CPEs) as well as information about resources utilization within a slice.

Monitoring element is responsible for monitoring of all devices status as well as monitoring of resources utilization. In the case of change of the resources or device status (e.g. up/down/failure) appropriate change is made in the Network & IT Resources DB. This module also communicates with the Virtualized Resources Database in order to update status and statistics regarding Virtual Networks (flows).

### 3.2.1 Control Layer endpoints, services and virtual networks architecture

Control Layer uses two fundamental entities which are present in the physical infrastructure: endpoint (both generic one – like a physical server and home-gateway endpoint – like users CPE) and OF Switch. Switches are interconnected with links, which are represented in the form of two elements list: switches DPIDs (or endpoints) and theirs physical ports.

List of switches and list of links between them are obtained from Slice (VSO) Supervisor and based on that information – decision regarding slice definition is made by Service Layer. Each VSO is reserving some...
resources (e.g. bandwidth, VLAN id, IP addresses and so on) on the number of ports of the physical switches.

Bandwidth on the links is defined as a reserved throughput on the corresponding ports. Bandwidth on the physical link reserved by multiple VSOs is shown on the Figure 7.

Figure 7 Bandwidth allocated to multiple VSOs (Slice Supervisor view)

From the services point of view – in the Control Layer two main abstract entities has been defined:

- **Service (ServiceVN)** – it is definition of the service. Definition includes pointer to the Service Provider Endpoint, traffic definition (e.g. UNICAST/MULTICAST, P2P/P2MP/MP2MP), flows definition (for each stream – UPSTREAM and DOWNSTREAM – fields which will be taken into consideration during virtual network setup need to be specified) and network definition (maximum throughput in the whole network). Service registration doesn’t reserve any resources (VLAN tags, IP addresses etc.). Resources are allocated during Virtual Network setup process.

- **Virtual 2 Network (V2N)** – represents physical connection between two endpoints: customer endpoint and service providers endpoint. During virtual network setup, despite pointers to the appropriate endpoints (customer endpoint ID is given directly, however service providers endpoint is taken from the pointer to the ServiceVN), network parameters are needed. Network parameters among others defines throughput for a specific virtual network.

Model of the services has been presented on the figure Figure 8. On this figure relation between services and virtual networks has been shown. Initial configuration of the service contains maximum network parameters, pointer to the service providers endpoint and service traffic definition and empty list of pointers to the established virtual networks. When virtual networks is setup, then service entity is updated.

ADDONAS architecture allows endpoints to provide (host) multiple services and at the same time be a member of many virtual networks. Relation between endpoint physical resources and defined services / virtual network resources are showed on the figure below.

Figure 8 Service overall model
Figure 9 Services provided (service provider) and consumed (service client) by endpoint within one VSO

Physical bandwidth is constrained by multiple factors. Throughput reserved by VSO in the Slice Supervisor cannot be greater than physical bandwidth on the link. Bandwidth allocated to the endpoint within VSO (one physical device might be present in multiple VSOs simultaneously) cannot be greater than throughput reserved by VSO. Each defined Service cannot have bandwidth greater than available bandwidth on the endpoint, which has been defined as a service provider. Network parameters of Virtual Networks to the endpoints cannot exceed endpoint’s available throughput resources. These constraints has been depicted on the Figure 10.

Figure 10 Overall bandwidth reserved by Endpoint in one VSO

Since network throughput is one of the most important elements of the resources utilization, in the Control-Layer the following terms are used:

- **Reserved bandwidth** – bandwidth, which has been allocated to an endpoint
- **Allocated bandwidth** – amount of reserved bandwidth, which has been already allocated for services and virtual networks.
- **Used bandwidth** – current, real-time bandwidth utilization, which has been obtained directly from the device.

Figure 10 shows differences between above mentioned terms. From the Endpoint point of view – reserved bandwidth has been marked on the left hand-side. Allocated bandwidth is a sum of bandwidth for all registered services and virtual networks. Because of that, available bandwidth is difference between reserved and allocated one. Used Bandwidth reflects how much traffic is generated (upstream bandwidth) and received (downstream bandwidth) by this endpoint.

From the Service point of view – reserved bandwidth is amount of bandwidth that has been reserved for all service traffic (e.g. for service SID 1) and total amount of bandwidth allocated for virtual networks bandwidth established within that service cannot exceed that value. Allocated bandwidth is a sum of bandwidth of the
virtual networks within this service. Used bandwidth is a real-time bandwidth utilization (like in an endpoint case).

From the Virtual Network point of view – reserved and allocated bandwidth points on the same value, because within virtual network user cannot create/setup another services. Used bandwidth as in the previous cases – shows current utilization.

Taking above into consideration Endpoint’s generic model despite reserved resources and maximum network parameters also contains references to the defined services and established virtual networks. Moreover HomeGateway Endpoint has an additional list of references to the Endpoints connected to the CPE on the particular port. Model of endpoints has been presented on the Figure 11.

![Figure 11 Generic and HomeGateway Endpoint models](image)

### 3.2.2 Control Layer’s resources abstraction (definition)

Service Traffic Definition (STD) defines network traffic in the terms of flows applied on the switches along the path. STD is defined per Control Layer service (identified by Service ID – SID) and is common for each V2N established between clients endpoint and service. Depending on the definition – service might contain endpoint hosting some content/service (when is defined as a E-LINE or E-Tree service) or contain no service endpoint reference (E-LAN service). When E-LAN service is defined, then V2N is established not between two endpoints, but among the group of endpoints, where none of it is designated as a content server (endpoints are equal). List of endpoints is obtained from established virtual networks to the particular service and it’s may change during service live-time.

![Figure 12 Class diagram of the Service Traffic Definition](image)
Figure 12 shows class diagram of the Service Traffic. STD consists of the list of several links definition. Each link definition might refer to the upstream or downstream traffic (Link Type). Several definitions might be defined into the same direction (e.g. with different flow policy). Moreover each definition consist of type of network (Network Type – P2P / P2MP / MP2MP), type of traffic (Traffic Type – UNICAST / MULTICAST) and set of flow polices defining pattern for traffic matching and further processing (like frames VLAN tagging on the access switch, tagged frames forwarding on the core switches and tagged frames VLAN stripping on the edge switch). Frames (L2) / packet (L3) / datagrams (L4) processing algorithm is based on the path policies, which are defined internally in the Control Layer.

3.2.3 Control Layer external north interface

For communication with the Service Layer two interfaces has been distinguished: main interface (using RESTful paradigm) and additional notification interface (using external message broker). The main (RESTful) interface is the primary way of communication with the Control Layer. All required functionality has been contained in this interface. Notification interface is an addition increasing request processing performance. This interface is used for any asynchronous notifications (e.g. hardware or Virtual Network failures). Moreover information regarding status of the asynchronous requests might be obtained.

3.3 Slice supervisor

Slice supervisor is responsible for the management of VSOs in the architecture. In particular, it manages the usage of the resources and is processing requests related to creating, modifying or destroying a slice. A slice consists of networking resources (metro and access devices) and IT resources owned by the Infrastructure Provider. Virtualization is used in order to provide separate pools of resources for each VSOs. FlowVisor [FV] is used for virtualization of the network resources while OpenStack has been selected for the management of the virtualized IT resources.

Slice Supervisor stores information about network topology and resource pools assigned to different VSOs. It stores information about flowspace specifications applied to FlowVisor in order to allow different VSOs access to their slices and to serve requests related to modification or extension of the slices. It also updates slice policies each time VSO requests change in the resource pool. Second important function of the Slice Supervisor is to enable communication between different VSOs (which are not communicating directly with each other). In case user would like to get access to the service from VSO A, which is not his ‘home VSO’ VSO A has to obtain information about user’s equipment based on source IP address of the request. VSO A requests information about the equipment from the Slice Supervisor. Slice Supervisor has the knowledge about pools of IP addresses assigned to different VSOs so can request information from user’s ‘home VSO’. This information is sent back to VSO A.

Slice supervisor consists of two main elements: VSO Manager and AAA. VSO Manager is the main element of the Slice Supervisor and is handling all VSO requests. AAA element is used for authentication and authorization of all VSO requests, and accounts usage of system resources.

4. Summary

Solutions proposed in the ADDONAS project enable creation of metro-access environment capable of providing open access to the network and multiple service providers. Utilization of the SDN concepts and virtualization of the network resources also enable creation of Virtual Service Operators having own marketplace for Service Providers. At the same time, symmetrical access (the same amount of bandwidth on upstream as on downstream) enables regular users to become a Service Provider. Usage of OpenFlow protocol to control the network also facilitates setting up the network for different services. Utilization of features of higher versions of OpenFlow protocol (e.g. usage of additional queues) will enable further enhancements of the service delivery.

Acknowledgements

Work in the ADDONAS project is financially supported by Narodowe Centrum Badan i Rozwoju (PL), The Technology Strategy Board (UK) and Bundesministerium für Bildung und Forschung (DE) under the FP7 PIANO+ initiative.
References


Biographies

Artur Binczewski received the M.Sc. degree in Computer Science from the Poznan University of Technology in 1993. He is the Manager of Network Division at the PSNC. He was involved in several EC projects: SEQUIN (IST-1999-20841), ATRIUM (IST-1999-20675), 6NET (IST-2001-32063). He coordinated the Porta Optica Study (RI026617), PHOSPHORUS (IST034115), ADDONAS (PIANO+) projects and ALIEN (317880). He is author or co-author of papers in major professional journals and conference proceedings.

Wojbor Bogacki received the M.Sc. degree in Computer Science: Artificial Intelligence from the Wrocław University of Technology in 2001. He works in Poznan Supercomputing and Networking Center in Network Division as a Senior Network Systems Analyst. He participated in several EC and Polish networking projects: GN3 (Project no. 238875), 6NET (IST-2001-32063), PHOSPHORUS (IST034115). His main interests concern networking and software developing technologies.

Łukasz Dolata received the M.Sc. degree in Electrical Science from Poznań University of Technology in 2002 and in the same year joined the Network Division of Poznan Supercomputing and Networking Center as a Networking Systems Analyst. He participated in several EC networking projects 6net(IST-2001-32603), Geant2 (IST511082), FEDERICA (RI-213107). Currently he is involved in the national project “Engineering of Future Internet” where leads the main task responsible for design and development of management services for PL-LAB Network. He participate also in two FP7 projects GN3 (Project no. 238875) and BonFIRE (Project no.257386). His main interests are in advanced networking technologies, network protocols, design and development techniques.

John Dunne is the CTO and Co-Founder of Intune Networks, a telecommunications switch manufacturer that builds optical packet switched solutions. John co-founded Intune in 1999 with Tom Farrell following EU-funded research work at University College Dublin. John has a first class honors electronics degree and a PhD in the field of tunable lasers from UCD and has spent his career working on the application of these devices into telecommunications systems. He is a co-inventor on some of Intune’s core intellectual property on network systems and is published internationally in the field of optoelectronics.
Szymon Kuc received the M.Sc. degree in Electronics and Telecommunications from Poznan University of Technology (Poland) and the M.Sc. degree in Computer and Communication Networks Engineering from Polytechnic University of Turin (Italy) – both in 2011. He joined the Network Division of the Poznan Supercomputing and Networking Center as a network systems analyst in 2011. He is currently involved in the ADDONAS European project which aims to improve access to network and services in the last mile. In the project he takes part in the development of the control plane for the OPST-based metropolitan network using the Software Defined Networking approach and the OpenFlow protocol. His main interests concern networking (SDN in particular) and software development (both high and low level programming).

Andre Oehlschlaeger is head of R&D Hardware at KEYMILE GmbH. He also leads research and development projects for optical transmission in the access network. Andre has been active in the telecommunication industry since 1995.

Łukasz Podleski received his M.A. in Musicology in 2012 and B.Sc. degree in Computer Science in 2012 from the Adam Mickiewicz University in Poznan, Poland. He is a Computer System Analyst in Polish NREN – Poznan Supercomputing and Networking. From 2011 he is involved in the ADDONAS project working on technologies for improving access to network and multiple services in the last mile. His main interests are in advanced networking technologies (especially Software Defined Networking) and Software Engineering. He is an ANSI C/C++/Java architect and developer with experience in enterprise-class real-time systems for industry.

Milosz Przywecki received the M.Sc. degree in Electronics and Telecommunications from Poznan University of Technology in 2003 and joined the Network Division of Poznan Supercomputing and Networking Center as a Networking Systems Analyst in 2005. Currently he is involved in several national and international projects: Future Internet Engineering, GN3, ORIENTplus and ADDONAS. In the ADDONAS project he is a workpackage leader responsible for delivery of SDN based system for flexible service delivery. His main interests are in advanced networking technologies, Software Defined Networking, network protocols and services.

Prof. Dimitra Simeonidou is the Head of the High Performance Networks Group at University of Bristol. She joined Bristol as Chair of High Performance Networks in 2012 after fourteen years at University of Essex and four years with Alcatel Submarine Networks. At Bristol, she is leading a group of 30 researchers and PhD students and currently involved in numerous National and EU funded projects. Her research is focusing in the fields of optical networks, Grid and cloud computing and Future Internet. She is the author and co-author of over 300 papers, 11 patents and several standardization documents.

Maciej Stoński is the Technical Director of Poznań Supercomputing and Networking Center, Vicepresident of the PIONIER Consortium – Polish Optical Internet, and member of the Supervisory Board. He is also lecturer in the Institute of Computing Science of the Poznań University of Technology. His research interests concern networking, quality of service, network protocols and management, Grid related topics. He is author and co-author of over 150 papers in major professional journals and conference proceedings. Maciej Stoński is the co-author of the Pionier Programme accepted by the Polish State Committee for Scientific Research and announced as the official Polish programme in 2000. He is a member of Programme and Steering Committees of national and international conferences and editor of Computational Methods in Science and Technology journal. Maciej Stoński has participated in several networking and Grid-related EU and national projects, co-operating with well-known IT companies. He has established the Sun Center of Excellence and Microsoft Innovation Center in PSNC.

Jan Weglarz Academician, Professor (Ph.D. 1974, Dr. Habil. 1977), in years 1978-83 Associate Professor and then Professor in the Institute of Computing Science, Poznań University of Technology, member of the Polish Academy of Sciences (PAS), Director of the Institute of Computing Science, Poznań University of Technology and its predecessors since 1987, Director of Poznan Supercomputing and Networking Center, President and Scientific Secretary of the Poznań Branch of the PAS, Vice President of the Committee for Computer Science of the PAS, member of the State Committee for Scientific Research, Principal Editor of the Foundations of Computing and Decision Sciences, member of several editorial boards, among others Internat. Trans. Opnl. Res. and European J. Opnl. Res. Representative of Poland in the Board of Representatives of IFORS and in EURO Council (President of EURO in years 1997-98). Member of several professional and scientific societies, among others the American Mathematical Society and the Operations Research Society of America. Author and co-author of 11 monographs, 3 textbooks (3 editions each) and over 200 papers in major professional journals and conference proceedings. Frequent visitor in major research centers in Europe and the USA. Co-laureate of the State Award (1988) and the EURO Gold Medal (1991), laureate of the Foundation for Polish Science Award (2000).
Georgios Zervas is currently a Lecturer in Optical and High Performance Networks at University of Bristol. He received MEng with distinction and PhD degrees from the University of Essex in 2003 and 2009 respectively. He then held the positions of Research Fellow and Lecturer prior to joining University of Bristol. He has been involved in several current and past EC and UK-EPSRC funded projects as a research/task leader, work-package leader and principal investigator. He is the author and co-author of over 100 international peer-reviewed journals and conferences including prestigious post-deadline papers at ECOC/OFC. He has also published invited papers and given invited talks at several international conferences. His research interests include but not limited to flexible multi-dimensional (space/frequency/time) optical nodes/networks, programmable and cognitive network systems, FPGA-based opto-electronic on-chip and off-chip networking, software/hardware defined network transport/control/management. He is also involved in standardization activities in IETF and OGF. He has filed two patents.