16-04-2015

Deliverable D12.2 (DJ1.3.1) Network Architectures for Aggregation of High-Speed Mobile Networking

Deliverable D12.2 (DJ1.3.1)

Contractual Date:	31-01-2015
Actual Date:	16-04-2015
Grant Agreement No.:	605243
Activity:	JRA1
Task Item:	Task 3
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	LITNET
Document Code:	GN3PLUS14-976-36
Authors:	Raimundas Tuminauskas (editor), LITNET; Chrysostomos Tziouvaras, GRNET; Frans Panken, SURFnet; Hao Yu, NORDUnet; Marcin Garstka, PSNC; Nicholas Garnier, RENATER; Zbigniew Oltuszyk, PSNC

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Abstract

This deliverable outlines the studies performed by JRA1 Task 3 on network architectures for the aggregation of high-speed wireless and mobile networking. It focuses on the technology enablers for high-speed access in the R&E environment. The concept of "wirefree" access is introduced to denote widespread, integrated high-speed wireless and mobile access, and a network architecture for seamless handover between different network domains is proposed as an integral part of wirefree.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This deliverable outlines the studies performed by JRA1 Task 3 on network architectures for the aggregation of high-speed wireless and mobile networking. High-speed Wi-Fi and mobile technologies shape current access networks, and immediately affect the personal experience of each user. The Task has focused its research on the technology enablers for high-speed access within the ecosystem that is comprised by GÉANT, the NRENs and their constituencies. The concept of "wirefree" access is introduced to denote widespread high-speed wireless and mobile access, considered as a key development factor in the field of modern education and research.

Section 2 of the document analyses the current situation with high-speed Wi-Fi and mobile networking. The successful deployment of eduroam AAI federation is shown as a prime example of the unique capabilities of the R&E community to extend the reach of conventional technologies, an experience which can be capitalised on by GÉANT and the NRENs to extend coverage to public areas and smaller institutions. The study also notes the complexity of planning Wi-Fi implementation within any organisation that does not possess the necessary in-house expertise. The expected growth in number of devices and traffic will be a factor in planning the future capacities of NRENs' and GÉANT's core and backbone networks. Proposed network architecture solutions to address the issues identified are presented in sections 3 to 5. JRA1 T3 considers high speed Wi-Fi and mobile to be access technologies, and that most of the new network architectures will be implemented in the access layer. Expansion of eduroam to the public areas, and implementation of Wi-Fi as a service, are good examples of such architectures. The requirements for backhaul through R&E core and backbone networks are within the range of currently implemented network architectures. However, implementing wirefree, seamless connectivity, which spans across different technologies and the boundaries of individual organizations' networks, requires the federated use of network resources and an extension of current protocols.

Architecture proposals are complemented with the results of Proof of Concept (PoC) implementations and computer simulations of proposed network architectures. Some architectural approaches, such as the establishment of eduroam in public areas, have already seen a number of implementations. A summary of current findings is provided using the example of the Wi-Fi implementation in the public areas of the city of Poznan. Only one PoC of Wi-Fi as a service (WaaS) was carried out by SURFNET. This proved the usefulness of the service, but also showed that there is no single, common architecture enabling WaaS implementation across the whole European R&E community. Proposed extensions of the PMIPv6 protocol were simulated using an OPNET network simulation engine in an artificial environment of two administrative domains. Results proved that it is possible to achieve seamless connectivity without mandatory switching of IP context as user equipment moves from

network to network. A brief discussion on possible further developments and a further research outline can be found in Section 6.

Two main conclusions were derived from the study:

- There is no single architecture that will allow flip-the-switch implementation of seamless wirefree access. The gradual evolution of network architectures towards the federated simultaneous use of all available technologies will eventually provide the needed level of service across the board.

- The R&E networking ecosystem has shown itself to be capable of using network resources in a federated way. This capability fundamentally differentiates it from the commercially-operated networks where monetary factors play a primary role. GÉANT and the NRENs should capitalise on this aspect to pioneer true wirefree access for their constituencies, to be ultimately extended to all members of the R&E community.

1 Introduction

This document outlines networking architectures for aggregating high-speed mobile and wireless networks. The concept of a high-speed mobile and wireless network spans beyond technological and organisational boundaries, and the creation of mobile learning environments is just one area that illustrates the requirements of the R&E community [Anderson, T.]. More advanced learning environments are currently under discussion [Wong, L.H.]. Mobile learning involves much more than the use of devices. It presents unique attributes compared to conventional e-learning: it is personal, portable, collaborative, interactive, contextual and situated. Mobile learning places high requirements on both learning content and ICT infrastructure. The deployment of these mobile learning environments has three major implications for networking:

1. **Ubiquitous access to content.** This implies that users require sufficient connectivity for their learning activities both on and off their institutions' premises. It requires integration of Wi-Fi and mobile (3GPP LTE, LTE-A), as a basis for all content and ICT services.

2. **Access to network resources.** Easy access to the network from any device makes mobile learning portable and personal and accessible from any device. This requires the integration of authentication solutions that are used both in the mobile world (SIM cards) and in educational environments (combination of user name and passwords and certificates).

3. **Widening of the user base**. Mobile learning environment implementations such as Brand's & Kinash's pilot test of the iPad [Brand, J. Kinash, S.], target primary and high schools rather than universities and research centres. This implies that sufficient Wi-Fi and mobile network connectivity should be provided for all learning environments, particularly as small organisations, such as schools and vocational training centres, are less likely to have the resources to deploy their own infrastructure and will rely on commercial operators unless the R&E community can respond to these requirements.

The term "wireless" itself is often intended with different meanings depending on the context it is used in: in the enterprise/university context it usually refers to Wi-Fi, while in mobile communications it is used to mean 3G/LTE radio. The definition "wirefree" is used throughout this document to refer to a network architecture where high-speed Wi-Fi and mobile access are available as an integrated service. This document outlines the requirements for providing such a level of service and considers the development of high-speed wireless/mobile network architectures from the organisational and technological point of view, as illustrated in Figure 1.1:

- **Expanding coverage**: Widening the user base through extending eduroam to smaller organizations and public areas.
- **Expanding technologies**: Incorporating mobile access to achieve seamless connectivity across different technologies.

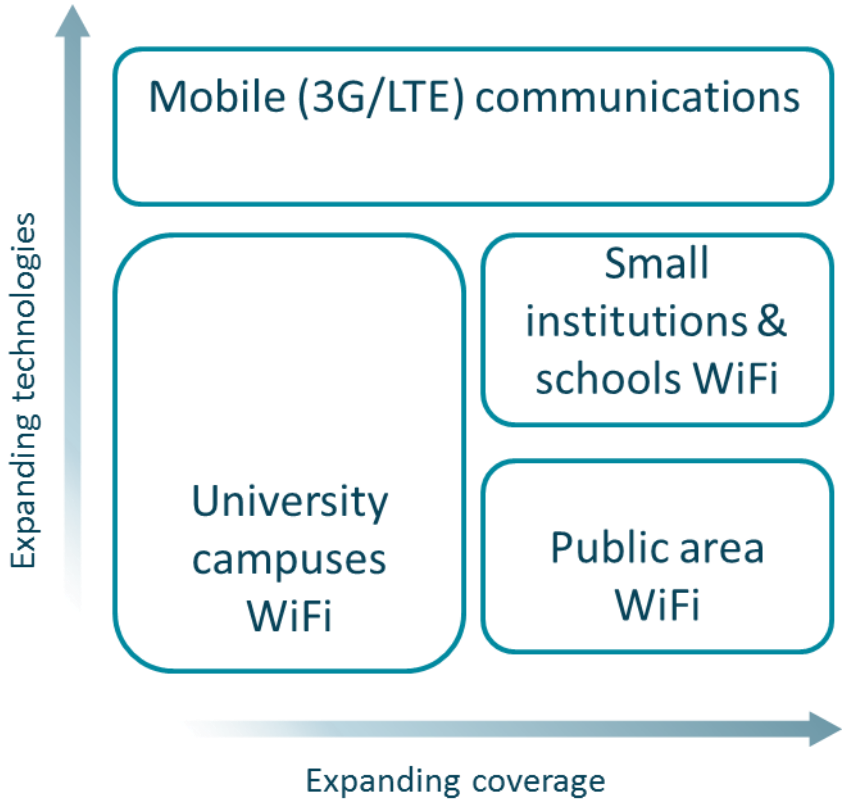

Figure 1.1 Directions of development of R&E wirefree architecture

The assumptions and modelling for this study consider the environment of European R&E networking. The ecosystem consisting of GÉANT and the European NRENs presents both challenges and opportunities for the implementation of a seamless, integrated, wirefree access concept:

- Its decentralised, multi-domain nature, offers these domains the highest freedom of choice in terms of preferred architectures and policies for their networks. Any proposed unified architecture for access would cut vertically across these domains. The experience with the deployment of eduroam indicates that any proposed architectures will have to deliver both significant value and a federated approach for their implementation to be successful.
- The high-level technical expertise of the NRENs and GÉANT, combined with their substantial user base, create an opportunity for these networks to become early adopters of new emerging architectures.

This document analyses the technologies required to achieve the envisioned wirefree service. The focus is not on a specific architecture as an ultimate means to implement an integrated service, but rather on technology solutions as enablers for wirefree. Section 2 examines the current state of the technology and outlines directions for development. Section 3 focuses on development across technologies through integration with 3GPP/LTE mobile at the core/backbone level, with seamless handover considered as an indispensable component of wirefree implementation. Two directions of expansion of Wi-Fi/eduroam are considered in sections 4 and 5 respectively: extending eduroam coverage to public areas and extending Wi-Fi access to smaller R&E institutions. Each section contains the results of the PoC modelling and actual implementations, along with recommendations. A brief discussion on further work is provided in Section 6.

GÉANT and the NRENs should reach a commercial settlement with commercial operators that will allow them to extend their wirefree footprint using the providers' networks. This paper focuses on the technology enablers for such an expansion, while an actual business model has yet to be defined. Some examples of potential settlements for new services may be found in the results of the MEAL open call project (GN3plus: MEAL). Business models for the NREN community are not considered to fall within the scope of this research.

2 Current State of Technology and Latest Developments

2.1 Access and Aggregation Networks

Radio-over-Fiber (RoF) technologies expedite the formation of heterogeneous radio access networks (HRANs), where different radio frequencies are transmitted over the same fiber connection to the remote antenna, to provide different types of wireless access, e.g. 4G (LTE), 3G (UMTS W-CDMA, UMTS TD-SCDMA, CDMA2000), and WLAN (Wi-Fi). Integrating different kinds of wireless access technology to provide users with data services, i.e. those of Wi-Fi and mobile networks across which operators provide data services to their users, results in the creation of such HRANs. User Equipment (UE) is usually capable of managing one interface for Wi-Fi, and another for mobile communications (4G/3G).

Moving from one wireless domain to another causes traffic to be switched from one interface to another. This may require IP network contexts to be switched as well, and all network connections to be re-established. Automated reconnection can be implemented at the application level, otherwise there will be a need to resort to manual mode where the user him/herself has to restart the application or reconnect. Frequent handovers will mean applications require increased resources, running the risk of degrading application performance, which could undoubtedly jeopardise the quality of the user experience. This vertical handover problem is not a trivial one, as mobility is becoming a dominant factor in communications.

3GPP has proposed a set of protocols for terminal mobility management [ETSI 29.275] based on Proxy Mobile IPv6 (PMIPv6) [RFC5213]. This enables a common mobility management platform for both wireless and cellular domains using PMIPv6. Since in PMIPv6 the Home Address of a MN is not changed during the change of attachment, it is possible to implement seamless vertical handover within one LMD. However, the industry currently lacks solutions for cross-domain (from one LMD to another), vertical handover. Seamless handover between different operators will become an inevitable and unavoidable need in the future, especially for the NREN community, where the eduroam authentication mechanism makes the infrastructure transparent to users.

2.2 Expansion of eduroam

eduroam has already established its success, with a constantly growing number of connected sites, currently 12298 in 69 countries on all continents except Antarctica [eduroam], and a large number of researchers and students using eduroam for their specific research needs as well as simply to gain Internet access. eduroam is available in most R&E institutions in the EU and many outside the EU. Figure 2.1 below shows the countries within and outside Europe where eduroam is available, highlighting the potential for global distribution of the service.

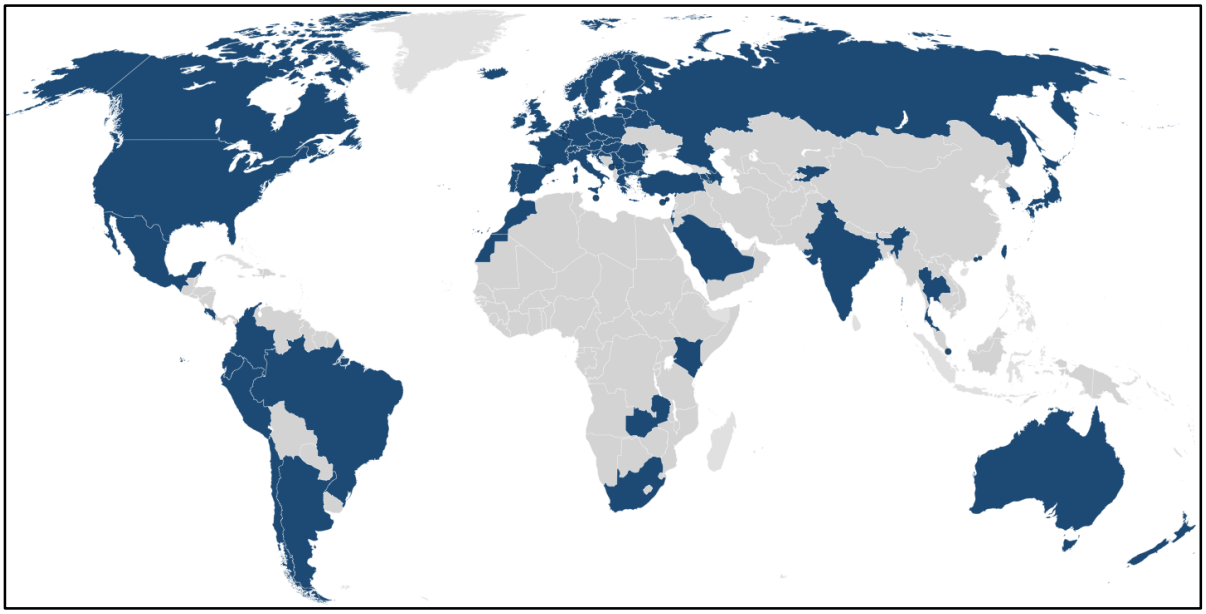

Figure 2.1: Countries with eduroam coverage (shown in dark blue) as of December 2014

eduroam is usually available in the areas covered by the Wi-Fi networks of the participating institutions – mainly university campuses. In a few instances, eduroam has also been implemented outside the campuses of participating institutions, at public locations such as city centres and airports, and is supported onsite at main R&E community events:

1. In the city of Luxembourg, eduroam is offered by a commercial provider using a Wi-Fi infrastructure built by the municipality. eduroam traffic is backhauled to RESTENA (the NREN), which provides a single fibre connection to the technical headquarters of the Wi-Fi provider. The main goal of the Wi-Fi provider in offering eduroam was to achieve a reputation as being student-friendly. eduroam is also offered at Luxembourg airport. In this case the goal of providing eduroam access was to increase the competitive position of the airport.

2. In the public areas of the city of Poznan, in Poland, eduroam access is provided by a Wi-Fi infrastructure built and owned by the municipality. eduroam traffic is backhauled to the PIONIER network (the Polish NREN), which provides fibre connections to several access points in the city. By providing eduroam access, the municipality hopes to promote the city among students and researchers worldwide.

3. Examples of non-European cities with eduroam coverage in public areas are: Tokyo in Japan, Wellington in New Zealand, and Porto Alegre in Brazil. eduroam in Tokyo is offered by a commercial provider aiming to promote its other services through it. In Wellington, it is offered by a commercial operator in cooperation with the NREN, while in Porto Alegre it is offered by a municipal network operator.

4. eduroam was also offered at some conference centres in Europe and the United States, either as a permanent service or to support specific events, mainly conferences attended by networkers. Some examples of such conferences are the Terena Networking Conference, organised yearly at different locations in Europe, Future Internet Week in Poznan in 2011, Supercomputing 2013 in Denver in the United States, and the 14th Annual Global LambdaGrid Workshop in Queenstown, New Zealand, in 2014. eduroam is provided throughout the year at the WTC conference centre in Rotterdam, thereby lowering the threshold for the organisation of events for the R&E community at this location.

These examples show that motivations for extending the eduroam footprint vary depending on the case. The main benefit for Wi-Fi providers in providing eduroam is to promote themselves among students and the research community. Other benefits for Wi-Fi providers may include increased security, as eduroam users are authenticated, in contrast to public Wi-Fi users who usually are not, as well as a cost reduction from backhauling eduroam traffic to the research network as mentioned previously.

On the other hand, the technical implementations share some similar features:

- Network access is offered by third party (non-R&E) providers, but user authentication is carried out by the research networks. This means that the network access provider's own users are not eligible to access eduroam and the extension of eduroam into third-party access networks is better suited for "public" or "free" Wi-Fi hotspots rather than private networks.
- eduroam access is free for the users and also for the research network operators, who do not pay Wi-Fi providers.
- In some cases, research networks backhaul eduroam traffic from the Wi-Fi infrastructure. In this way the Wi-Fi providers can save on their Internet subscription while eduroam users receive potentially better service as their traffic to their home institutions uses research networks that should ensure better transmission parameters (bandwidth, packet delay, etc.).

The examples given above prove that eduroam access does not have to be limited to campuses, and can be provided in wider areas without any significant costs to the research community. Third-party Wi-Fi infrastructures can be successfully used for eduroam access outside campuses with benefits for the research and education community. National Research and Education Networks should consider promoting eduroam to Wi-Fi providers and aggregating eduroam traffic from their Wi-Fi infrastructures.

2.3 High-Speed Access Aggregation in the Core

2.3.1 Bandwidth per Device and per Cell / Access Point

The maximum theoretically-available bandwidth per single spatial stream is 867 Mbps for IEEE 802.11ac, and the absolute maximum throughput is 403 Mbps for 3GPP LTE FDD on the physical layer [Johnson, C.]. However, these maximum capabilities require all resources to be dedicated to the one channel without redundancy on the physical layer.

In the mobile (3GPP, LTE) environment, terminals (UE) are typically dispersed over the cell area, so it is realistic to assume that all three possible modulations (Table 2.1) will be used. Assuming that 10% of the mobile terminals are close to eNodeB, 30% are at an intermediate distance, and 60% on the cell borders, for the 4x4 MIMO configuration the maximum downstream cell bandwidth is estimated at 163,2 Mbps.

LTE Configuration	Close distance to eNodeB 64QAM (Mbps)	Average distance to eNodeB 16QAM (Mbps)	Maximum distance to eNodeB QPSK (Mbps)
2x2 MIMO 20Mhz	172,8	115,2	57,6
4x4 MIMO 20Mhz	326,4	217,6	108,8

Table 2.1. Maximum mixed downstream bitrate for a single LTE cell as a functions of the distance of mobile terminal (UE) from the base station (eNodeB)

Taking into consideration that most LTE eNodeBs consist of three cells, based on the analysis provided above the maximum mixed rate of the eNodeB is estimated at 500 Mbps. There are IEEE 802.11ac access points (APs) capable of reaching 1300 Mbps on the side of wireless PHY, but only when using a 1 Gbps Ethernet as uplink [NetGear AC1900].

The current bandwidth available per device and per cell / access point is in the range of hundreds of Mbps. 10 Gbps, or n-times 10 Gbps network connections are required to feed an average metropolitan or campus network consisting of 100<=k<=999 Wi-Fi/LTE cells.

2.3.2 Traffic Patterns

Standards for 3GPP LTE-A [E-UTRA] use IP as primary transport for both voice and data services. They specify 9 QoS classes. Each class is assigned an identifier, priority, packet delay budget, and packet error loss rate. Class parameters vary from a delay budget of 100 ms and packet error loss rate of 10^{-2} for conversation services to a 300 ms delay budget and no specified error loss rate. IP networks must support at least some of these classes. Percentage data for voice traffic with a strict QoS requirement was not available to the Task. The main services considered in the study are those related to data transport offered by NRENs to LTE users within the community. The GÉANT mobile data service

implemented in SA7 Task 5, and those NRENs that offer mobile connectivity to their users (Carnet, HEANET, JANET, SURFNET), only backhaul data transport.

Detailed traffic data from the Wi-Fi network of Kaunas University of Technology (KTU) was analysed. The results are summarized in Table 2.2.

Provider type	Weekly		24h	
	Gbytes	Percent	Gbytes	Percent
Cloud providers (Google, Amazon, Microsoft, etc.)	98.5	14.30%	33.7	25.70%
Local traffic	111.6	16.20%	32.9	25.11%
Internet service provider networks	285.3	41.41%	36.5	27.86%
Content providers	79.5	11.54%	6.6	5.06%
Unknown type networks	11.5	1.67%	8.8	6.69%
Below TOP 50	102.6	14.89%	12.5	9.57%
Total traffic	689		131	

Table 2.2: Summary of top-50 ASNs by the bytes transferred to the Wi-Fi network at KTU

The traffic data does not show any distinctive characteristics in terms of locality and directionality. Hence it is safe to assume that high-speed mobile terminals produce/consume the same amount of traffic as regular fixed computers connected to a high-speed network (e.g. FTTH), where the vast majority of the traffic is directed to the commodity Internet.
The Task considers that the traffic pattern will remain unchanged during the timeframe of the study, i.e. an estimated 80 percent of all access traffic will originate from campus, NREN and GÉANT networks. The increase of access traffic will therefore impose requirements on the bandwidth of feeds from the backbone.

3 Integration with High-Speed Mobile Networking

3.1 Network Architecture Proposal for Seamless Handover

The proposed solution for vertical handover aims at making the handover process to User Equipment (UE) transparent and fast so that the UE does not have to perform any complex algorithm or application restart. The proposed methodology is to utilise the Software Defined Networking (SDN) approach to implement cooperation between the existing Proxy Mobile IPv6 (PMIPv6) solution in the Wireless Local Area Network (WLAN) domain and the Evolved Packet Core (EPC) in the cellular domain. In order to do so, the OpenFlow protocol can be implemented in several functions/nodes: Local Mobility Anchor (LMA), Mobile Access Gateway (MAG), Evolved Node B (eNodeB), and Remote Radio Head (RRH). By adopting a single OpenFlow controller in the Heterogeneous Radio Access Network (HRAN), handover information can be centrally processed by the controller and the corresponding changes in behaviour can be applied in order to provide seamless vertical handover.

The architecture is depicted in the figure below. Given the assumption that LMA and MAG equipment is SDN-enabled, one SDN controller (SDNC) is located in each domain, connected to the LMA and MAGs. Signalling is exchanged between the two SDNCs so that the home LMA can be notified about the handover of its UE from another domain. Interdomain tunnels between two LMAs are jointly created by the two SDNCs in order to enable traffic bound for the UE to be routed to the new location. Traffic bound for the UE is still received first by the home LMA, as the UE remains within the same IP context regardless of the change of attachment. Traffic is then sent out from the home LMA to the other LMA, and in turn routed to the UE.

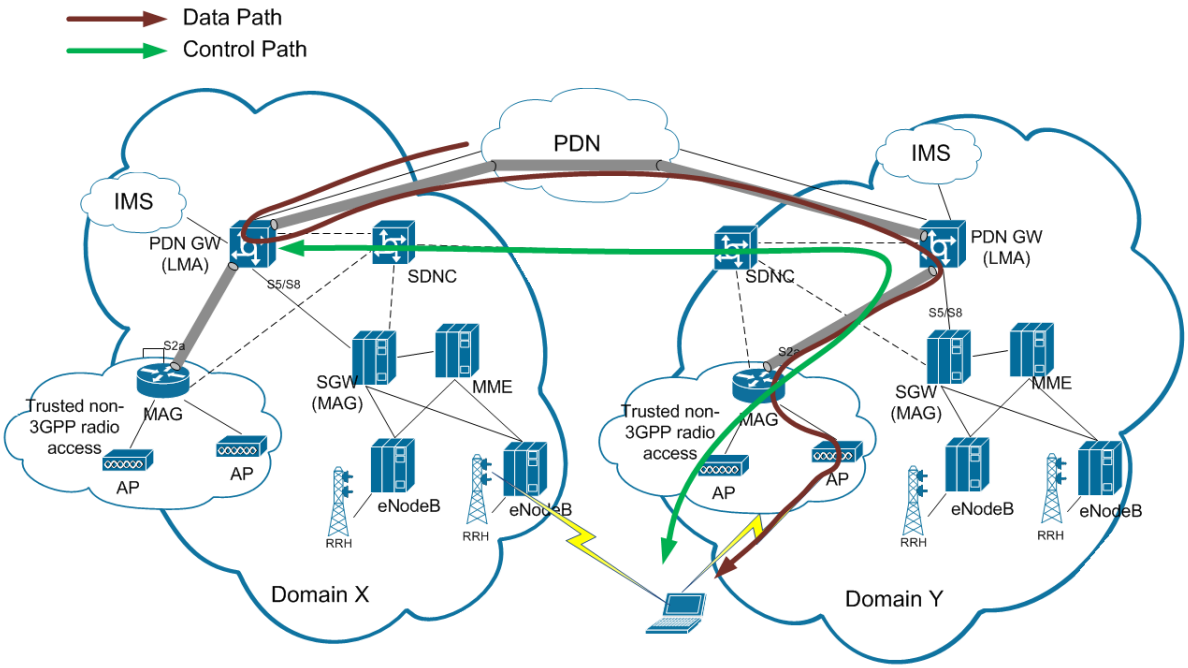

Figure 3.1. Network diagram for seamless handover

It should be noted that the tunnelling may produce a sub-optimal data path, causing an increase in round-trip time (RTT) and possible degradation of performance in terms of latency. However, this traffic detour ensures that the home IP address of the UE remains unchanged so that no TCP traffic is interrupted. Since the proposed architecture is vulnerable to latency, it is most applicable for adjacent domains, e.g. adjacent university premises or university Wi-Fi networks and mobile operators. The data path may be optimised by establishing physical connections between LMAs of adjacent wireless/mobile access providers.

3.2 Model of HRAN Handover Process using SDN Architecture

The proposed solution consists of improvements on two paths, the signalling path and the data path. For the signalling path, improved PMIPv6 is needed. For the data path, SDNCs are required to cooperate on multidomain tunnels. Since the idea promoted to solve the multidomain handover problem requires new areas to be evaluated and developed, modelling and simulation work is preferred at this stage. A model for the signalling path has been built in OPNET Modeler to evaluate the complexity of the protocol. The proposed protocol of vertical handover across different domains is outlined below.

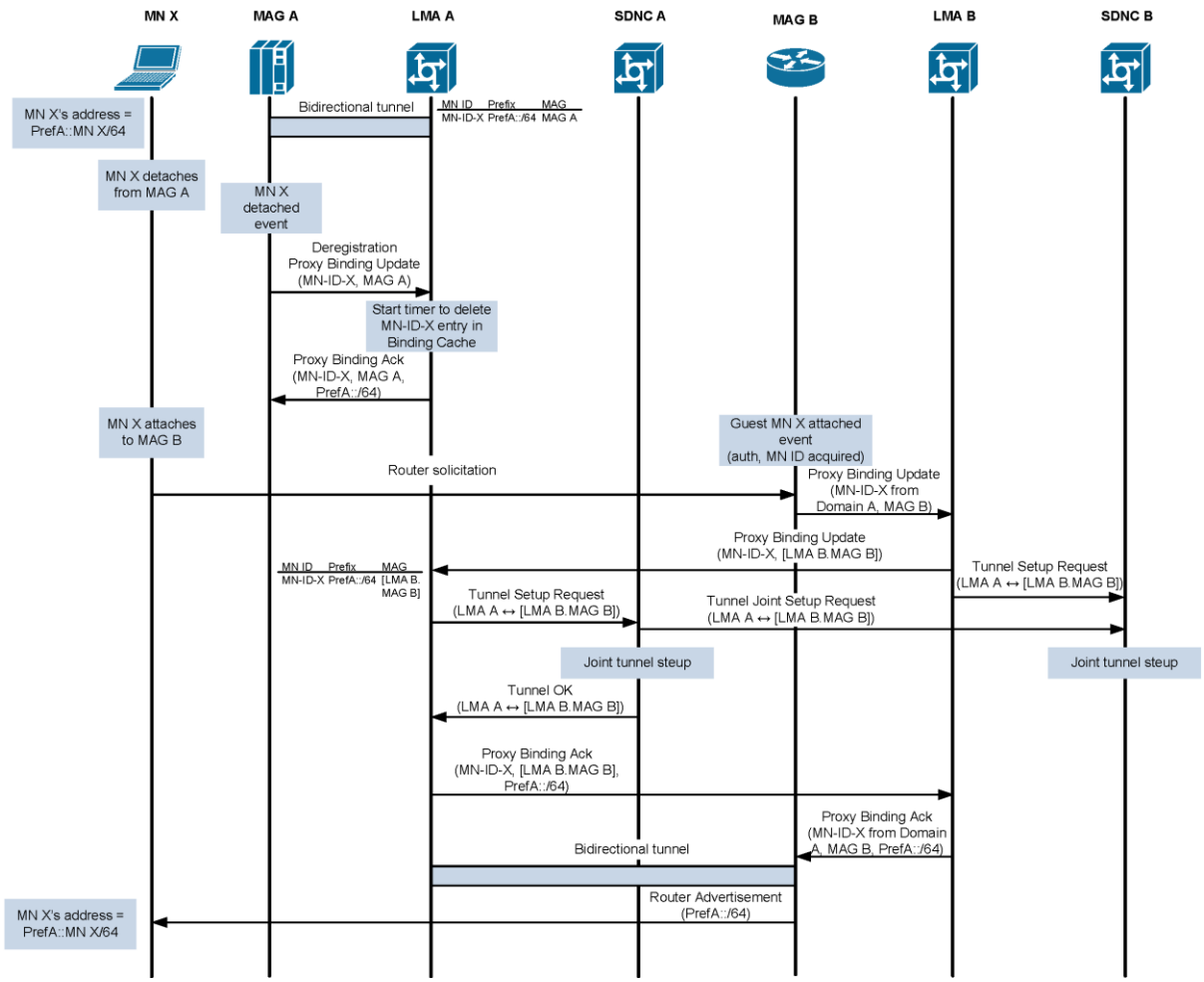

Figure 3.2. Signalling exchange in vertical handover between different LMAs

When Mobile Node X (MN X) detaches from MAG A in Domain A and enters Domain B, MAG A should deregister MN X from the Binding Cache of LMA A. As MAG B in Domain B detects an attachment event from MN X, MAG B proceeds to identify MN X, and checks whether it is authorised to use the network-based mobility management service. If it is, MAG B performs mobility signalling on behalf of MN X. MAG B sends a Proxy Binding Update (PBU) to LMA B, associating its own address with the identity of MN X.

It should be noted that since MN X does not belong to Domain B, its Home Domain should be included in the PBU. Upon receiving the request from MAG B, LMA B adds its own address in another PBU and forwards the request to LMA A. From the PBU sent from LMA B, LMA A discovers that MN X has entered another domain and immediately requests SDN Controller A in its domain to set up a tunnel from LMA A to MAG B.

Since the tunnel is multidomain, SDNc A should request SDNC B to jointly set up the tunnel in its domain. After the tunnel is established, SDNC A returns an OK message to LMA A. Upon receiving the confirmation from SDNC A, LMA A sends to LMA B a Proxy Binding Ack (PBA) including the prefix, which should not be changed. LMA B then sends a PBA including the prefix to MAG B to confirm the previously received PBU from MAG B. A bidirectional tunnel (which may have several segments) is

established between LMA A and MAG B. MAG B sends Advertisement messages including the prefix to the MN Router, so that the node can configure an address

Downlink traffic sent to the MN is first received by the LMA in its home domain (LMA A) because of the unchanged Home Address of the MN. The home LMA should forward the traffic to the correspondent LMA (LMA B) through the tunnel created by the SDNCs. After receiving the traffic from the home LMA, the correspondent LMA should forward the traffic through the tunnel bound for the MAG (MAG B) that the MN has attached to. Uplink traffic originated from the MN is sent to the correspondent LMA and is forwarded to the home LMA through the tunnel.

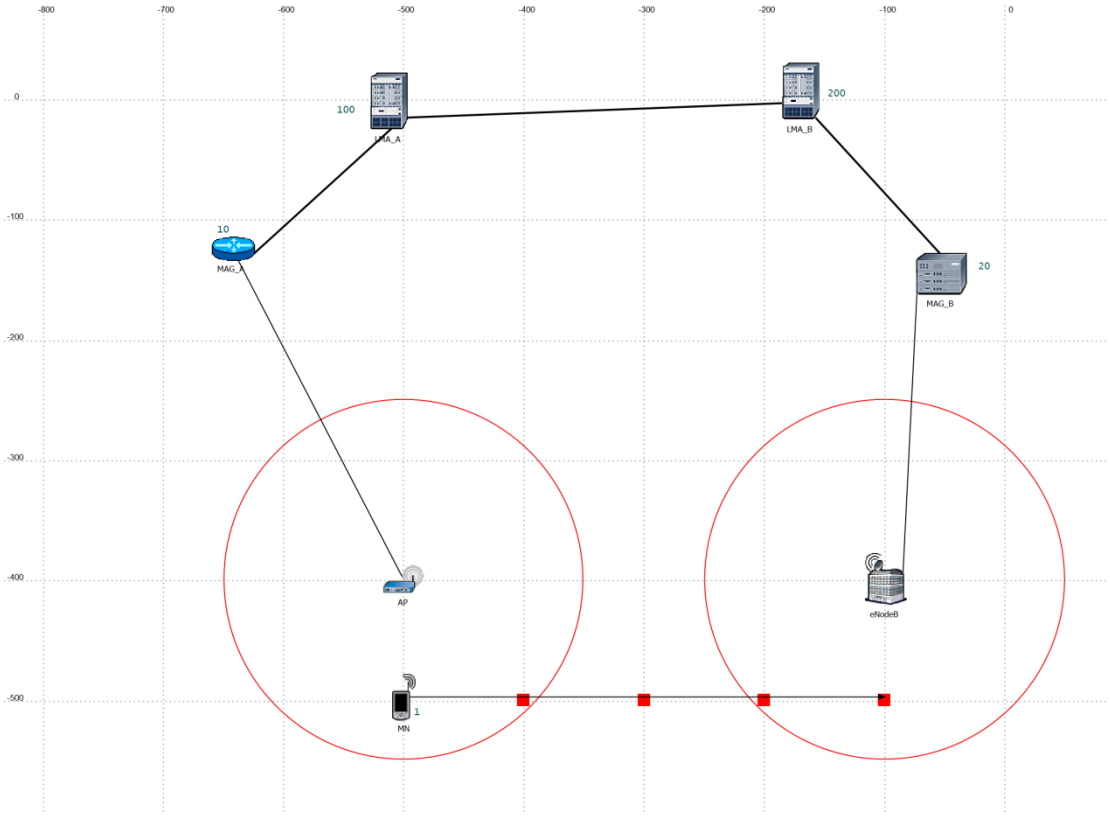

Figure 3.3. OPNET simulation topology for vertical handover

The MN is modelled to change its position at 12-minute intervals, indicated by the red dots, as shown in Figure 3.3 above. The signal ranges of the AP and the eNodeB are assumed to be 150 m, shown by the red circle. As the MN enters the access range of the eNodeB, it will attach to the new point and the aforementioned signalling exchange will take place to ensure a successful handover. The simulation procedures are shown below. Note that the MN successfully receives the home address (prefix 100) from the home LMA in the handover domain. The figure below shows the binding status vs. the distances from the MN to AP and eNodeB. As the MN moves out of the signal range of AP, it loses connection to LMA_A and therefore the binding status becomes 0 (unbound). The MN attaches to eNodeB as soon as it enters its range and binds to the LMA_A again through LMA_B. Thus the binding status turns back to 1.

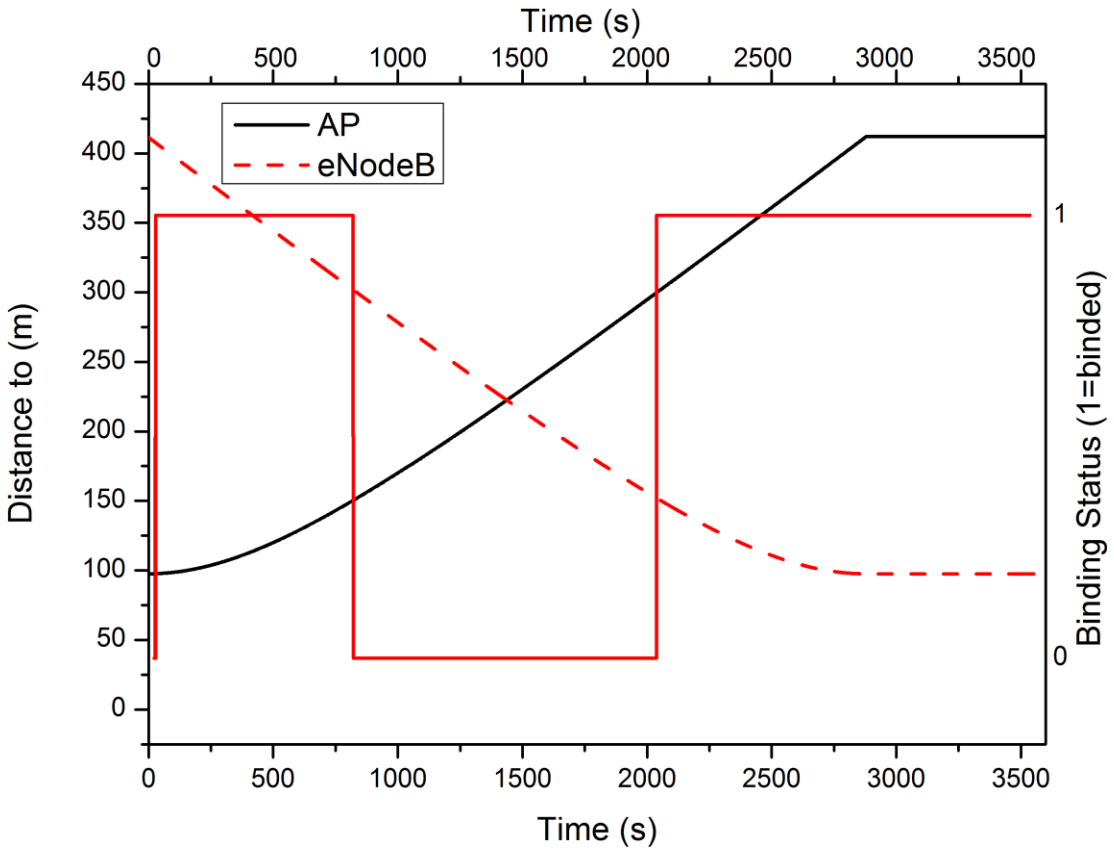

Figure 3.4. Context switching simulation results

3.3 Aggregation of High-Speed Mobile in NREN networks

There follow some basic recommendations for core network design for efficient aggregation of high-speed mobile data, taking into consideration the specifics of the R&E networking environment:

1. Capacity dimensioning of the core network must take into consideration the fact that during peak periods the additive traffic load due to high-speed mobile data backhauling may scale to multi-Gbps speeds. It is best for an NREN to handle this additional traffic at a low layer instead of dealing with it at the IP layer, as explained below.

2. Investigate the economics of sustaining peerings with the commercial Internet close to the interconnection point of the aggregation network and the NREN network. In this way the NREN network is offloaded from carrying large amounts of data which would require considerable investments (e.g. DWDM transponders, router linecards).

3. Where the required investment for sustaining multiple peerings with the commercial Internet would not be advantageous, the NREN could examine the option of establishing direct tunnels to the closest Internet peering, so as to minimize packet processing and achieve improved

delay performance. This can be achieved by installing either dedicated wavelength or lower granularity OTN circuits connecting an NREN router that directly interconnects with the aggregation network, with an NREN router that peers with the Internet (Figure 3.5). Both options guarantee low delay and respect of the QoS constraints; with dedicated wavelengths, imposed delay is dominated by the unavoidable propagation delay and, to a lesser extent, by the FEC processing. In OTN circuits, the additive delay of OTN switching is also imposed; in all cases imposed delay is lower than using layer 2 protocols such as MPLS-TP or regular layer 3 IP routing. By comparison with the established practice of using direct wavelengths with OTN circuits, it should also be noted that, despite the fact that the direct wavelengths solution can offer higher bandwidth, it does not present adequate protection performance characteristics unless the expensive 1+1 protection scheme is adopted. More specifically, wavelength restoration requires deployment of directionless ROADM filters which are quite expensive and can be reconfigured in the sub-second range, while OTN circuits enable activation of protection paths within less than 50 msec, thereby providing better switchover characteristics.

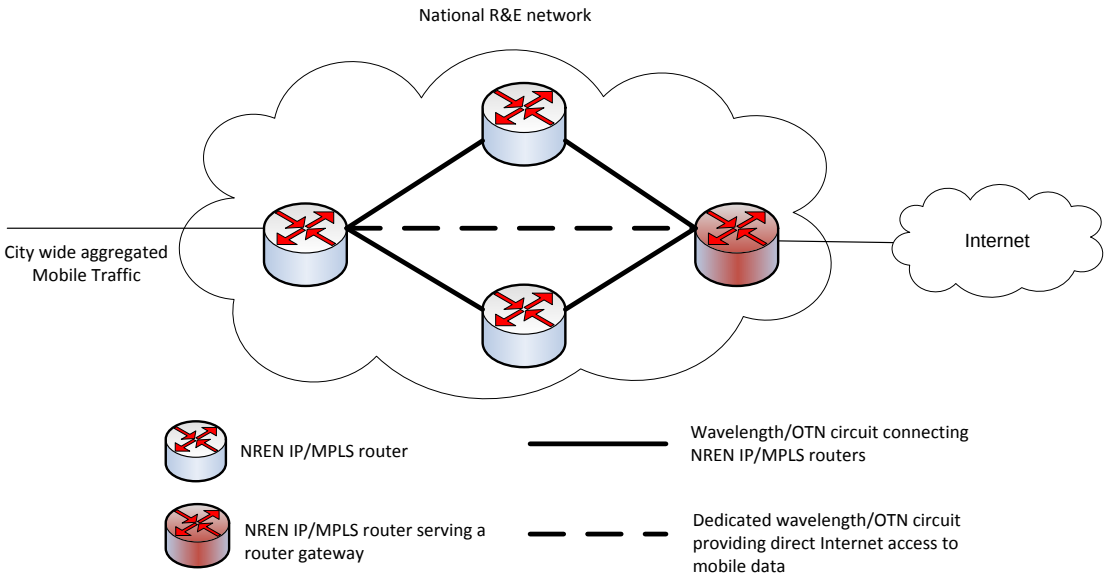

Figure 3.5 Providing dedicated wavelength/OTN circuits for Internet access

4 Extension of eduroam footprint

4.1 Network Architecture for Backhauling eduroam Wi-Fi Access

Different architecture solutions are proposed depending on whether the NREN in question is backhauling eduroam traffic from the Wi-Fi infrastructure. In the simplest scenario, the NREN is only responsible for the authorisation of users and does not participate in the data transmission. In the more complex scenarios, the NREN backhauls eduroam traffic itself. The first scenario does not require any investment and does not introduce any additional costs, while the latter requires a transmission connection between the NREN and the Wi-Fi provider. This connection must either be built (investment) or leased (recurring costs). On the other hand, backhauling traffic to the NREN may reduce the costs of Internet upstream for the Wi-Fi provider. It is expected that traffic backhauling will be used for large Wi-Fi infrastructures with large amounts of traffic, especially for metropolitan Wi-Fi networks which can easily access an NREN PoP. Two examples of eduroam traffic backhauling to an NREN are those of the cities of Poznan and Luxembourg. For small Wi-Fi infrastructures, on the other hand, the cost reduction would not offset the additional costs of a data connection with the NREN, so it is expected that in these scenarios the 'authorisation only' model will be used.

Figure 4.1 shows where the three possible architectures fall in terms of operating costs of the Wi-Fi infrastructure (costs of Internet upstream) and the needed level of cooperation between the NREN and the Wi-Fi provider where the higher the level of participation of the NREN, the lower the cost.

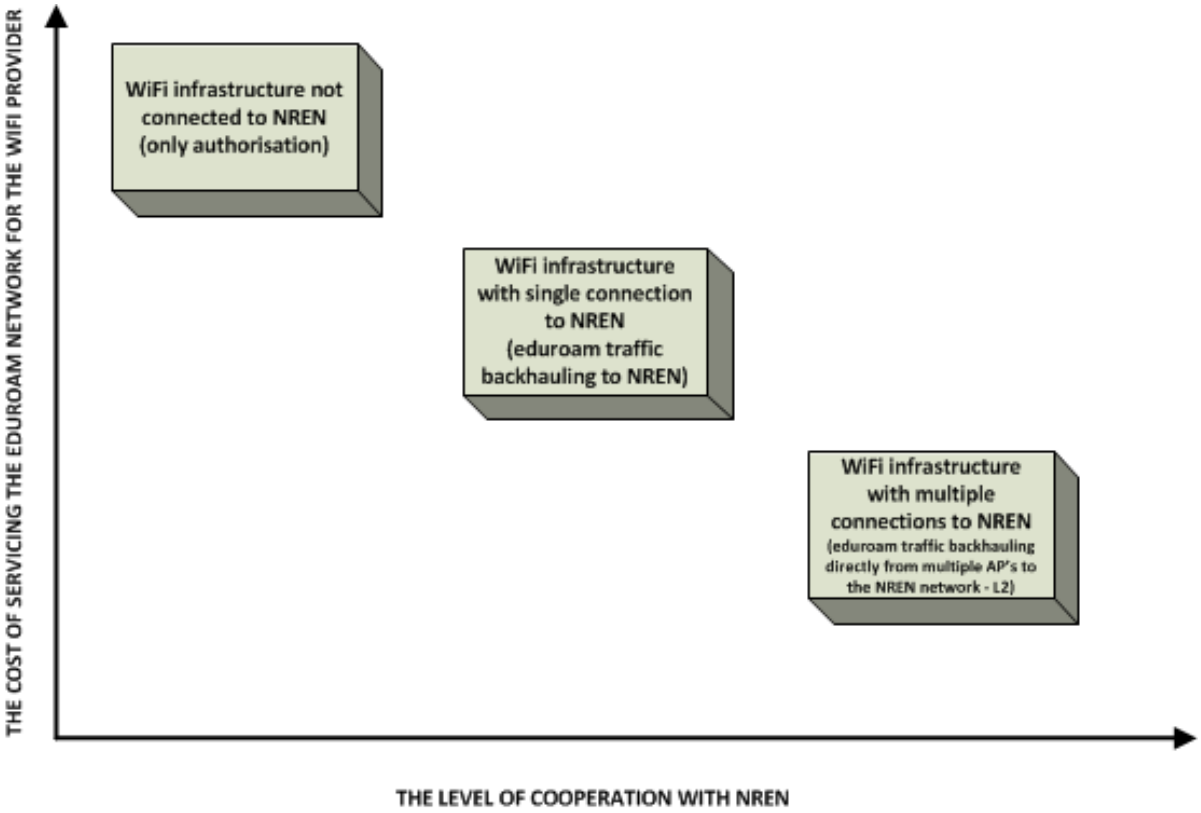

Figure 4.1: Possible architectures for offloading eduroam traffic from Wi-Fi infrastructure to the NREN

4.1.1 Authorisation-only by NREN

In the simplest scenario, the NRENs only provide the authorisation of eduroam users and do not backhaul the traffic generated by eduroam users in the Wi-Fi provider networks. The traffic is carried by the Wi-Fi provider and transmitted to its upstream providers like all other traffic from the Wi-Fi network.

No data link between the Wi-Fi provider and the NREN is needed so the solution can be accomplished without any major investment. Only the authorisation data must be transmitted between the Wi-Fi provider and the NREN but this traffic can be tunnelled over the Internet. This architecture is especially useful for small Wi-Fi providers and Wi-Fi infrastructures located rather far from the NREN infrastructure.

In this solution, the Wi-Fi provider will not benefit from backhauling the traffic to the NREN network but this will not be crucial for small Wi-Fi providers who do not generate much traffic and do not spend much on upstream links. Another potential drawback is that the eduroam traffic will be carried by commercial carriers and will probably use a longer path to the user's home institutions than when transmitted directly to an NREN, using research networks for transmission to the home institution. Figure 4.2 shows the architecture of the authorisation only model (yellow line) and the architecture of the authorisation and traffic backhauling model with a single connection between the NREN and the Wi-Fi infrastructure (blue line).

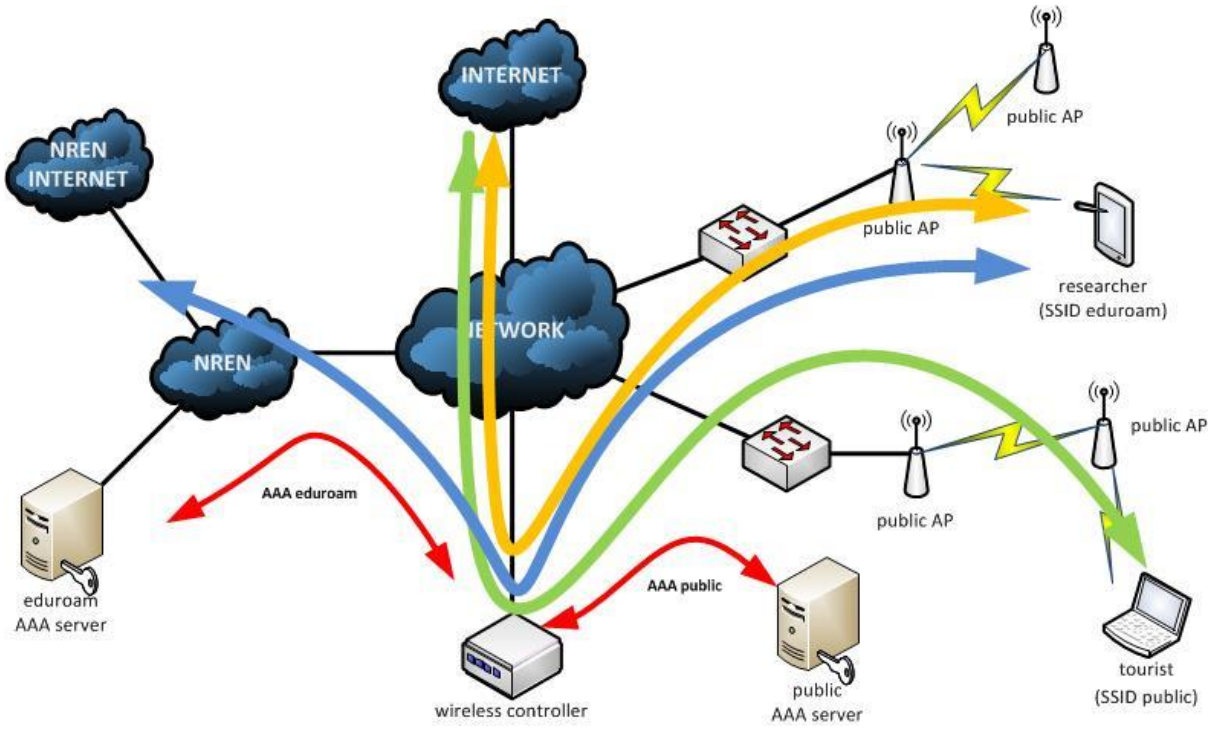

Figure 4.2: Architecture of the authorisation only model (yellow line) and the authorisation and traffic backhauling model with a single connection between the NREN and the Wi-Fi infrastructure (blue line)

4.1.2 Authorisation and traffic backhauling to NREN

In this scenario, traffic generated by eduroam users is transmitted from the Wi-Fi provider's network directly to an NREN via a data link. This solution is especially useful for big Wi-Fi providers with a large amount of traffic and metropolitan or regional Wi-Fi infrastructures that can easily access an NREN PoP.

In this scenario the Wi-Fi provider derives an advantage from sending eduroam traffic to an NREN and decreasing the amount of traffic exchanged with its commercial upstream provider. The major benefit for eduroam users is that their traffic will be sent to an NREN and reach their home institutions via research networks, which should guarantee greater bandwidth and shorter transmission times compared to those of commercial networks.

Traffic between the Wi-Fi infrastructure and the NREN can be exchanged via a single interconnection, two interconnections for redundancy, or multiple interconnections, in order to decrease the traffic on the Wi-Fi backbone. The latter option will be useful for large Wi-Fi networks, such as municipal or regional Wi-Fi infrastructures.

Figure 4.2 shows the architecture of this model with a single data connection between the NREN and the Wi-Fi infrastructure (blue line), while Figure 4.3 shows a possible architecture with multiple

connections between the NREN and the Wi-Fi infrastructure. For the solution with multiple connections, it is assumed that eduroam traffic will not pass the Wi-Fi controller of the Wi-Fi provider. The traffic will be backhauled to the NREN as close to the access points as possible in order to decrease the amount of traffic on the Wi-Fi provider's network.

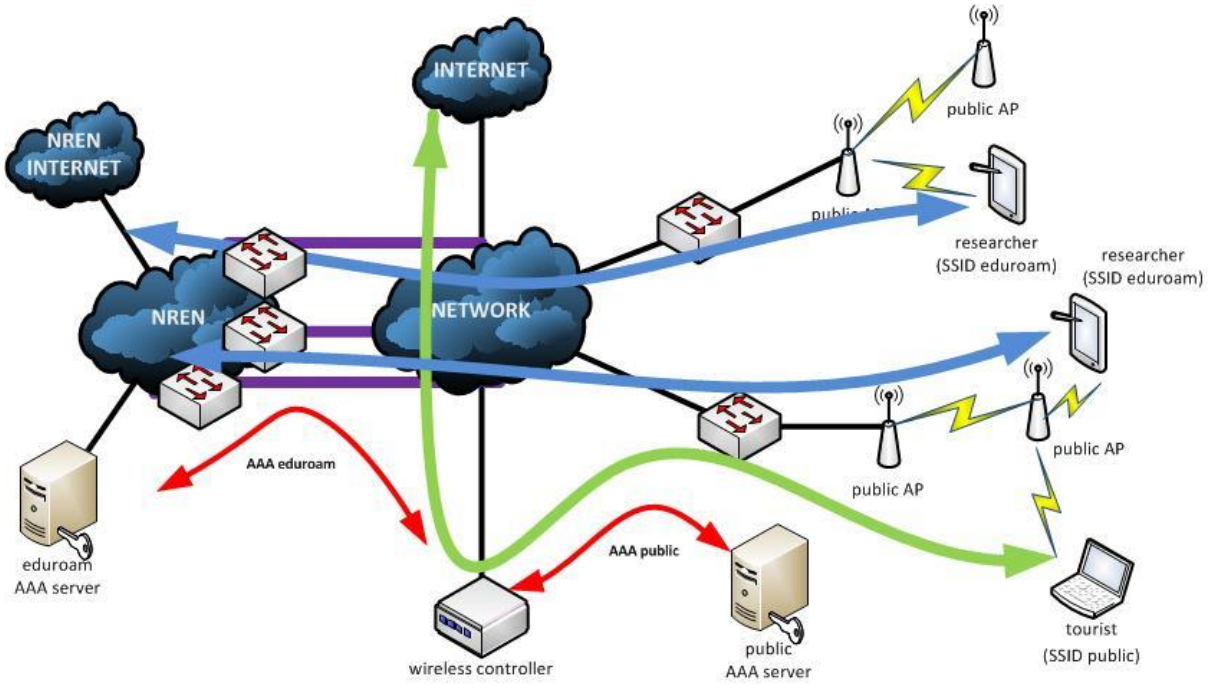

Figure 4.3: Multiple data connections between the NREN and the Wi-Fi infrastructure

4.1.3 Other recommendations

For traffic to be carried by an NREN, there should be at least one high-speed interconnection between it and the Wi-Fi provider. For redundancy, the Wi-Fi provider should have at least two interconnections with the NREN. No interconnection is needed if traffic is not forwarded to an NREN.

In large Wi-Fi infrastructures, it is recommended that the Wi-Fi hardware should not be forced to transfer all traffic from access points (APs) to the wireless controller. Traffic should be able to bypass the controller, allowing interconnection with the NREN at any point of the infrastructure as well as multiple interconnections.

In order to enable eduroam traffic to be separated from other traffic generated in the same Wi-Fi infrastructure, the infrastructure should be able to map the eduroam SSID to a unique VLAN ID in the fixed network.

4.2 Implications for the NRENs

The solution without eduroam traffic backhauling does not impact NRENs' networks, as only traffic for authorisation is exchanged between the NREN and the Wi-Fi infrastructure. This is a small amount

of traffic that does not have any specific requirements. It can be exchanged by a dedicated link but it can also be tunnelled through the Internet without requiring any additional investment or cost.

Backhauling eduroam traffic from the Wi-Fi infrastructure to an NREN requires a data connection. It is possible to use a leased line (dark fibre, lambda or capacity) or own infrastructure (fibre with a transmission system). Any transmission technology that is capable of transporting IP packets can be used and the only consideration is the bandwidth needed to efficiently transmit the traffic.

The NREN should assign a pool of IP addresses for the eduroam traffic sourced in the "foreign" Wi-Fi infrastructure. Network Address Translation (NAT) will probably be used to translate private IP addresses (used within the Wi-Fi infrastructure) to public IP addresses from the NREN pool. NAT allows multiple wireless users to share the same public IP address in order to reduce the size of the public IP pool needed for wireless users. It also increases the security of wireless users by blocking incoming connections. NAT can be provided either by the NREN devices or by the Wi-Fi provider.

At least two independent connections are recommended for redundancy. In the case of a single connection, the Wi-Fi infrastructure should allow eduroam traffic to use the Internet upstream when the connection to the NREN is not available. In this case eduroam traffic should use source IP addresses from the Wi-Fi provider's pool.

The NREN policy and operations framework should foresee the possibility of servicing eduroam through third-party access networks. The AUP and formal procedures should not impede cooperation with commercial operators that may be required to extend the eduroam footprint. In some cases universities and institutes may find themselves in a better position for cooperation and federated use of resources than NRENs, e.g. it can be easier for a local university to convince the municipality to support eduroam in the municipal Wi-Fi infrastructure than for an NREN which may be based in another city and not be regarded as a partner for the local authorities.

R&E institutions should seek mutual collaborative agreements with the operators and providers of public area Wi-Fi networks and avoid the public procurement of Wi-Fi access services. Collaboration agreements have proven to provide the most flexibility in current implementations. Public area networks are operated by a wide variety of companies across each country, and the sheer complexity of such an undertaking would make any generalised national or international procurement procedure impossible.

4.3 Implementation of eduroam in Public Areas

This section describes the proof-of-concept experience of implementing eduroam access in the public areas of the city of Poznan in Poland.

Rationale: The city's municipality expressed the intention of implementing free Wi-Fi access in the public areas of the city, and opted for eduroam as one of the SSIDs in the Wi-Fi network. The other SSIDs are intended for public users and for the employees of the municipality. The use of the network is available to everybody free of cost, but the quality of service (bandwidth and duration of the session) for public users is restricted. Such restrictions are required by Polish law in order to prevent competition with commercial Internet providers.

The idea behind the introduction of eduroam in public areas was to build Poznan's reputation as being a student- and researcher-friendly city.

The main benefits for eduroam users, compared to users of the public SSID, are easy access to the service (authentication using their eduroam credentials rather than a mobile phone number and password received by SMS) and lack of QoS restrictions (eduroam users get the full available bandwidth and unlimited session duration).

Architecture: The traffic from the eduroam SSID is backhauled directly onto the NREN network. Backhaul is engineered at every point of presence where there is dark fibre connectivity. The Wi-Fi access network uses radio-linked access points to distribute access from the points of backhaul. Figure 4.4 shows a diagram of chains of access points connected with radio links. A single vendor solution is adopted with an off-data-path controller.

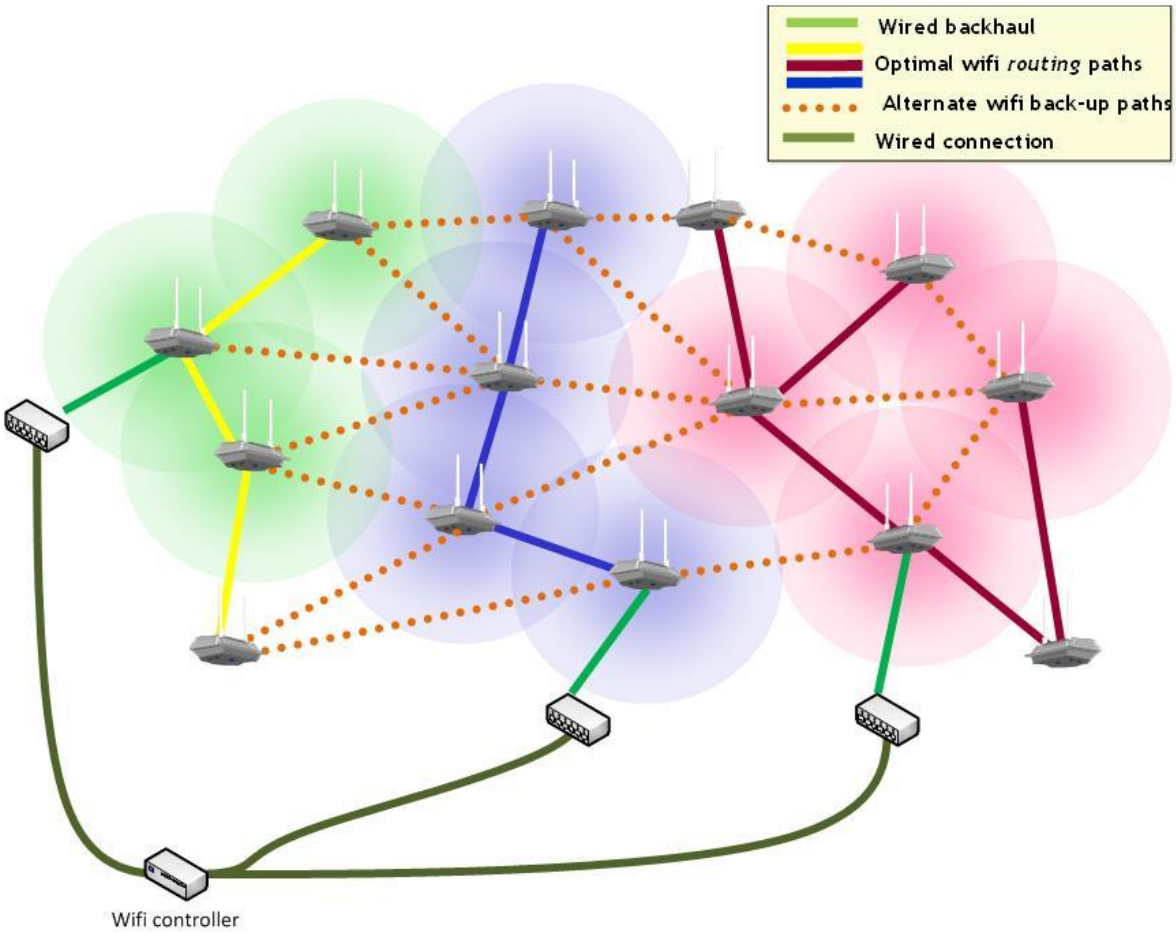

Figure 4.4 Diagram of chains of access points.

Authorisation requests from the eduroam SSID are forwarded by the municipality Radius server to the Radius of the Polish NREN. The municipality server acts as a proxy.

Implementation: Figure 4.5 is a map of the City of Poznan [POZnan] showing the areas of the city with radio coverage. Currently coverage consists of less than 200 access points located in the most popular

areas. The Wi-Fi network covers the centre of the city, three main arteries, bus terminals, and a zoo. Figure 4.6 shows the location of access points in the Poznan city centre [POZnan]. The access points are located on buildings that belong to the municipality (e.g. schools and bus terminals) as well as on traffic lights. There are also 2200 "foreign" (i.e. not belonging to the municipal Wi-Fi infrastructure) access points located in the same area covered by the municipal infrastructure. These Wi-Fi access points are located in hotels, cafes, shops and other outlets in the area. The distribution of access points for radio coverage must be studied carefully to avoid any interference that would result in a degradation of quality.

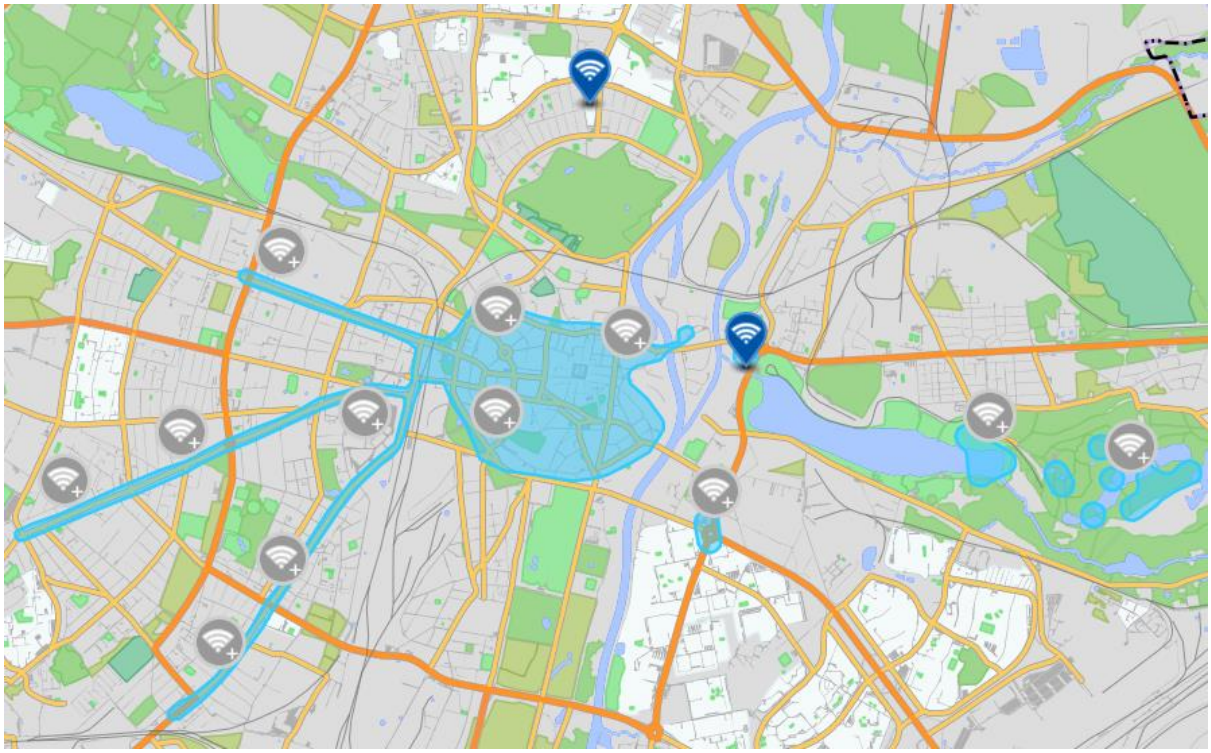

Figure 4.5 Public Wi-Fi coverage in Poznan

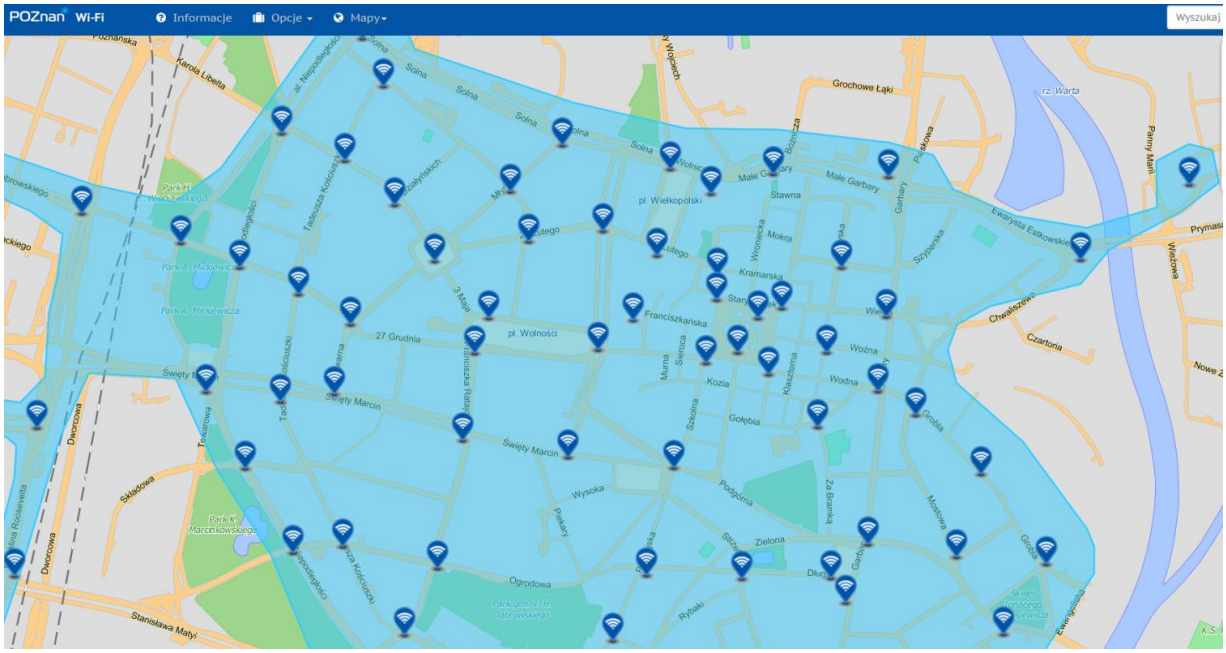

Figure 4.6 Access point locations in the centre of Poznan

"Foreign" (not belonging to the infrastructure) Wi-Fi is not the only source of interference. Tram lines, electrical power fluctuations and electrical objects generate additional interference that can only be overcome through density of coverage grid. Availability of power at certain locations (e.g. city lights) may also be an issue.

Figure 4.7 and Figure 4.8 show the number of eduroam user authentications in the Poznan municipal network in 2013 and 2014. The rapid growth in the number of authorisations in 2013 is connected to the expansion of the Wi-Fi coverage to new areas of the city. Any R&E institution undertaking implementation should take into account the rapid increase in network usage that will occur as coverage grows.

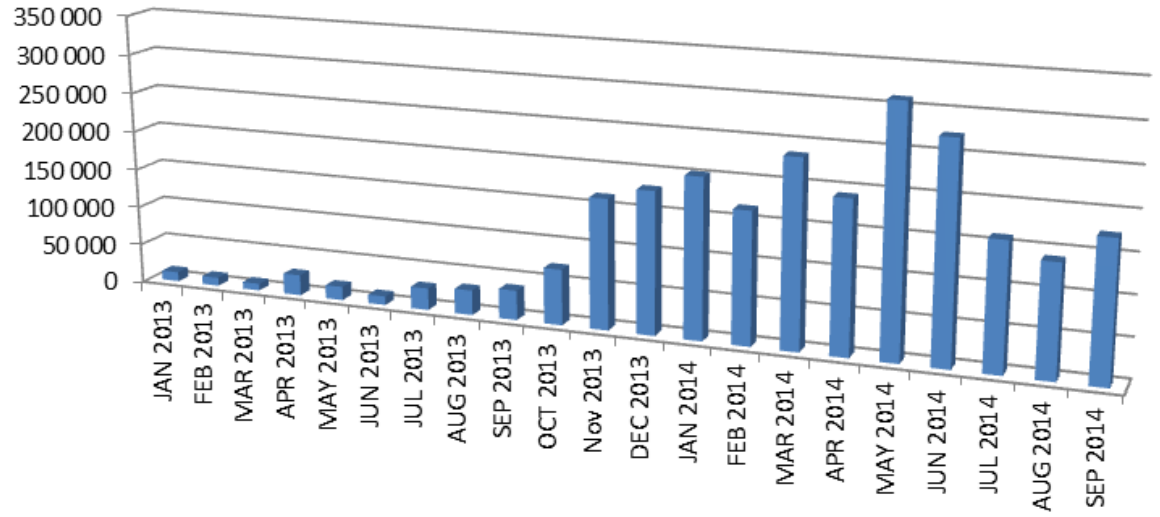

Figure 4.7 Number of eduroam user authentications in the Poznan municipal network

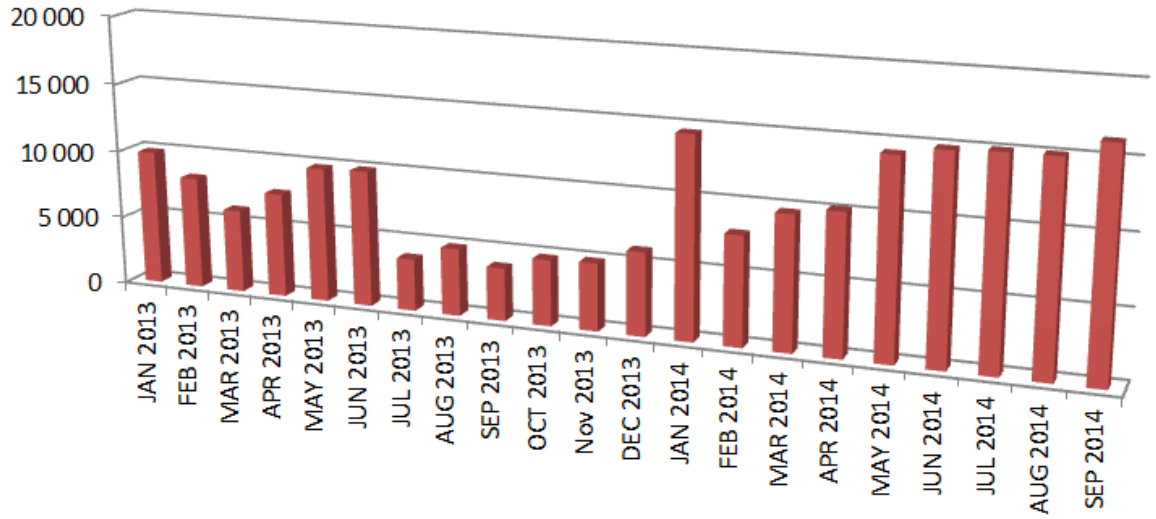

Figure 4.8 Number of "foreign" eduroam user authentications in the Poznan municipal network.

Results and further work. Making eduroam available outside campuses promotes a location (city, airport, etc.) as being student- and researcher-friendly, thereby potentially attracting a greater number of students. The eduroam community will also benefit from eduroam availability in public places as such availability promotes eduroam among potential users and those research/education institutions that are not yet connected to it.

5 Wi-Fi as a Service (WaaS)

5.1 Rationale and proposed network architecture

The deployment of a high-speed Wi-Fi network in an R&E institution is a complex task that requires a wide variety of network architecture parameters to be taken into consideration. Not all institutions and still very few schools and vocational training centres have such expertise. Institutions have implemented a common wireless architecture based on thin access points (APs) that are connected to one or multiple controllers [Eertink, H.]. This current solution effectively means that the same Wi-Fi wheel is re-invented at each institution. It causes duplication of equipment and licenses, but also duplication of expertise and capacity needed to deploy and maintain the equipment at each institution. While the Wi-Fi requirements of the R&E community differ significantly from those of private homes, small businesses or corporations in terms of number of simultaneously connected users, time-scale for the use of network resources and density of areas where Wi-Fi signals are needed, these requirements do not differ greatly between the various educational institutes that belong to the community. By offering Wireless as a service (WaaS), an NREN uses its fixed infrastructure to expand its service offering to also include integrated wireless services.

WaaS is not a new concept in itself; there are already cloud providers who offer this service on a commercial basis, e.g. [Open-Mesh]. They can do this because vendors sell controllers that can handle tens of thousands of clients and 6000+ access points. For NRENs – who are used to clear and simple demarcation points – WaaS is however very new. Various WaaS solutions are possible, ranging from solely delivering a controller backend to offering a complete managed service that includes the procurement and installation of access points.

The implementation of a WaaS solution on a European scale is expected to encounter potentially blocking challenges in terms of organisation, support, and technical and regulatory constraints. However, NRENs share commonalities, which make cooperation among them in delivering WaaS potentially very fruitful. The task has identified the following ‘check-list’ of issues that must be resolved by NRENs in order to implement WaaS:

1. **Define the optimal system architecture for WaaS**. Proper system architecture is the key element towards ensuring future technical success. It is not sufficient to just specify what the architecture should do, but it becomes increasingly important how easy it is to use, how scalable it is and whether it can adapt over time (in capacity, usage, etc.) to guarantee availability of the WaaS service as well as support various migration scenarios.

2. **Define common functional requirements and policies**. Institutions should be in the driving seat and define policies that must be enforced by the Wi-Fi network. It is important to determine, understand and implement a common denominator for the most important policies from the R&E community, as the desire to offer a unified solution may lead to a situation where it will not be possible to enforce all policies.

3. **Guarantee the best possible end-user experience**. This includes easy access to the Wi-Fi network (for students, staff and guests), a common way to identify rogue devices and to place them in quarantine, helping individuals when they experience problems with Wi-Fi performance or availability, and quality/capacity planning that ensures hassle-free access from all places.

4. **Establish the prerequisites for the application of WaaS**. The prerequisites for offering WaaS to an institution may include availability of good access switches that are connected with (two) proper cables (> cat 6e), support of PoE, and no restrictions on placement of access points. WaaS may also be used to offer Wi-Fi during events, in which case setting-up a tunnel between access points and controller that carries both signalling and data is important because this limits the need for support at the location where the event is organised. Ultimately, these prerequisites should be captured in a WaaS service level agreement.

5. **Establish service contracts**. The rationale for WaaS stems from the principle that it is more cost effective to manage a Wi-Fi network from a central location, rather than at each individual institution, which also leads to a better user experience. This requires a common set of conditions and policies that prevent the Wi-Fi service from becoming unmanageable over time. These include a clear separation of responsibilities: What falls under the responsibility of the NREN and where does this responsibility end? Who fixes what, if the service is not available? What actions should the institution take? When can an institution contact the NREN (if an access point does not function, if users cannot authenticate, if users cannot get on-line, if only some of the users cannot gain access, etc.)? These aspects should be formalised in a service contract.

6. **Run and manage the Wi-Fi as a Service**. As soon as the contracts are in place and the equipment is installed and deployed, the service can start. Design is expected to change over time – extra VLANs, additional SSIDs, and added sites are some of the factors that may result in changes in deployment. The details and best practices for change management should be described in the service contracts. Securing users and WaaS components is another important topic. The first action is blocking incoming traffic. The rationale for this is that Wi-Fi clients should not run web or data service and so that there is no need to access Wi-Fi clients from the internet. Other actions depend on the architecture chosen and the functionalities that reside within the WaaS service (DHCP, firewall, etc.). A situation where data from a Wi-Fi client break-out from the access point (or from a slave controller that resides within the domain of the institution) results in the institution handing out IP addresses to the Wi-Fi client. This means security incidents will be traced back to the institution. In an architecture where all access points are connected to a centrally located controller, the institute's firewall is bypassed. In addition, the DHCP functionality is under the responsibility of the NREN that offers WaaS. In this case, the NREN must take measures to implement a secure solution.

5.2 Wi-Fi as a Service Implementation

This section covers the implementation choices made for the proof-of-concept service implemented by SURFNET at a vocational training school in Arnhem, in the Netherlands. An optimal Wi-Fi network

can only be realised based on a proper RF-plan and a correct Wi-Fi design methodology. Information from the institution was collected to draw up a document listing a specific set of design requirements and constraints. The information gathered includes: the physical area to be covered, the estimated number of devices and the device count increase over time, device density in specific areas and applications in use, and sources of interference. Location of new access points was determined by placing an access point on a stick and using performance diagnostic tools to determine the effect of the AP's location.

System Architecture for WaaS

The system architecture for Wi-Fi as a Service has to be decided and implemented for the entire service, as no case-by-case variations may be possible unless they are foreseen in the initial architecture outline. Wi-Fi as a Service aims to realise a simplified and unified Wi-Fi solution for R&E institutions. It aims to provide a Wi-Fi service that can be centrally monitored and managed for all institutions simultaneously. The starting point for an NREN is determining its service offering as it is essential to know the scope of WaaS required so as to make the correct architectural choice. Will the WaaS be limited to making a controller backend available which institutions can plug APs into, for example, or is it a complete managed Wi-Fi service that includes the procurement and installation of access points and management of the Wi-Fi environment? This choice will depend on the type of service the NREN wants to offer and may well differ between different NRENs. A combination of different service offerings should be avoided, mainly because this prevents offering a unified Wi-Fi service. There are various architectural designs, including namely: stand-alone APs, controller-based architecture with data and signalling traffic flow through the controller, and the split tunnelling variant where the controller is only involved in the signalling traffic. In one possible scenario, all Wi-Fi clients 'live' at the centralised controller of the NREN, whereas in another the access points connect to a trunk and allow clients to break out to the institution's local ICT infrastructure. There is no one-size-fits-all architecture. The design of the solution should optimise the desired WaaS offering. By choosing the eduroam network federation as a starting point, various security and association parameters are defined. The common denominator for all architectural flavours is the effort needed for WaaS management (including the effort needed for troubleshooting).

For the WaaS pilot, SURFnet used a resilient controller-based Wi-Fi design, shown in Figure 5.1. The controller – a Cisco 8500 series allowing the connection of 6000 access points – is located in SURFnet's data center. This data center is connected to the SURFnet core (SURFnet7). It should be noted that this means that the controller is located outside the domain of the institutions where the access points reside. In addition to the controller, DNS and Radius components were also installed. A Cisco prime server was added to monitor the health and availability of the most critical WaaS components, namely the controller and access points.
Each access point is connected to the controller via the institution's regular internet connection. By using the Cisco's 3702 access points, Wi-Fi clients can connect via the new 802.11ac standard. From the perspective of the local ICT infrastructure, each AP functions as an Ethernet end-point. APs use option 43 from the local DHCP server to find the centrally located controller. Upon finding the controller, each AP sets-up a capwap tunnel to exchange signalling information and data.

Wi-Fi clients that connect to an AP make use of the Radius server that is associated with the controller. This Radius server is used for all clients, including those from the institution that participates with WaaS. If a client authenticates successfully via eduroam, the DNS server connected to the controller provides the client with an IP address. This IP address comes from the pool reserved by SURFnet. This

means eduroam clients “live” at the central controller. On the other hand the APs receive an address from the local IP pool.

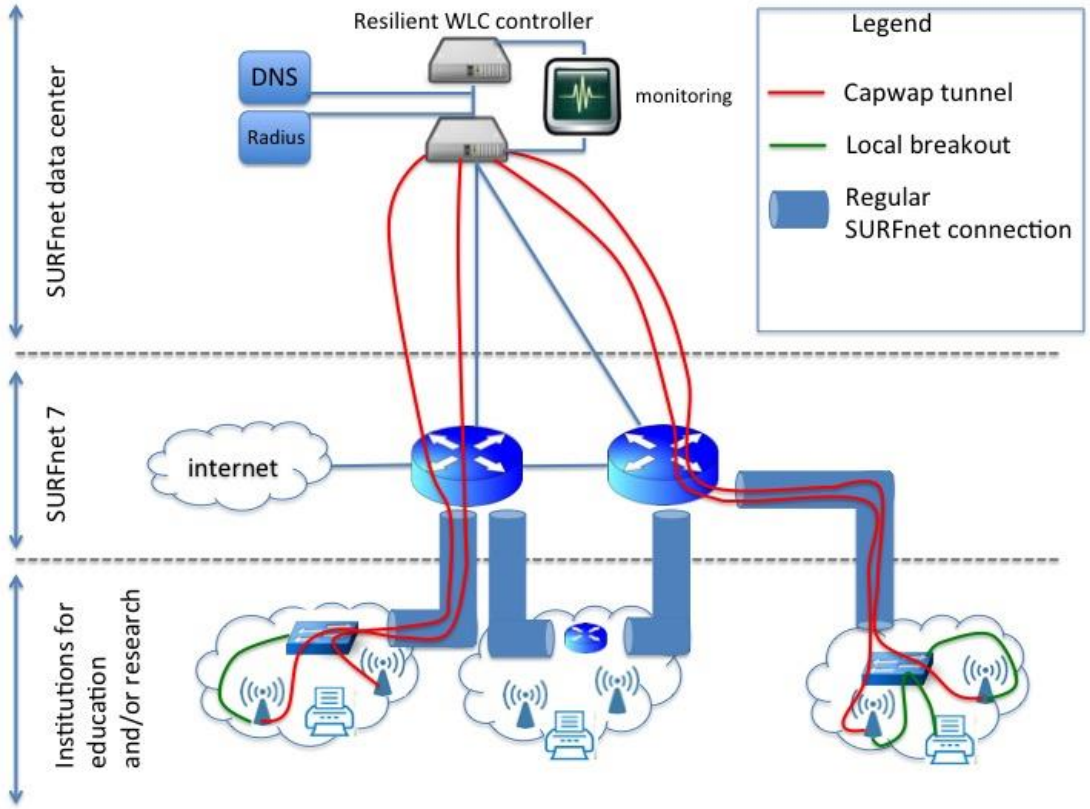

Figure 5.1 WaaS architecture used in pilot implementation

Common Functional Requirements and Policies

- **Role of local ICT support:** ICT personnel at institutions must be able to support basic network-related troubleshooting for issues related to client access to Wi-Fi, client authentication fails, client failure to receive IP address, or the client experiencing limited up- and downstream data rates. They must also be able to produce reports that show how well the Wi-Fi solution is performing. It is essential that local ICT staff have access to information (and tools) to perform such basic troubleshooting.

- **External communication policies:** Each institute may have its own security policy. One institution may decide that the ICT facilities may not be used for downloading large files from Netflix or news servers, or via peer-to-peer applications. Other institutions may allow this but not over the Wi-Fi network (as it functions as a shared resource and large file up- and downloads result in excessive usage over clients). Finally, some institutions do not impose any restrictions on their ICT infrastructure. The WaaS solution must support a range of security policies in a flexible and scalable manner. When requesting WaaS, institutions should provide information in this respect, and may want to define which services or ICT resources can be discovered via Wi-Fi, who has access to them, and which applications they can access and where from.

- **Internal communication policies:** Institutions may have their own data centres. This includes shares or storage facilities that are used, for example, for automatic backup, and may store education/research-related information that can be accessed by students. Other resources accessed may include printer facilities and Apple TV. The Wi-Fi infrastructure offered through a WaaS offering must enable students and staff to have easy access to the ICT resources they are allowed to use in line with their institution's security policy. While the WaaS solution should simplify the life of institutions, it should not lead to a lack of support for their most common policies. The best way to achieve this is for the NREN to create a template in which to collect this information, to then be used in the technical design of the WaaS implementation. Basic ICT knowledge (no detailed Wi-Fi knowledge should be required) should be sufficient to fill in the templates. Since in the pilot implementation each packet is sent to the central controller, accessing local resources means that traffic has to travel back from the controller to the institution where the client resides. By making use of a VPN, packets could be routed selectively. Those making use of data facilities are routed to the institutions and others are routed directly to the internet. However, this means that the institution has to facilitate VPN connections for these clients. It was decided that data packets from personnel and students should be treated differently. All data packets from staff avoid the capwap tunnel. These packets break-out from the AP to the local infrastructure. At Rijn Ijssel College, this was realised using an extra SSID in addition to eduroam. As an alternative, Radius could have been used to assign data packets from students at a different VLAN. Since personnel from Rijn Ijssel already used a separate SSID for this purpose, this was the preferred solution. The AP uses a trunk to connect to the switch. One of the VLANs of this trunk is associated with data packets form the extra SSID.

  Radio access policies: Ideally, the Waas solution uses a single SSID only, preferably eduroam. This does not mean that all users should be handled equally. Policies may depend on whether the Wi-Fi clients serve students or staff. Radius can be used to distinguish the various user groups. Based on the Radius attributes (users names or vendor-specific attributes stored in the active directory, LDAP or other user database), the Radius server may implement a local policy that assigns these users to different VLANs leading to redefining the network policy. So that clients can break out locally, all APs are used in Cisco's Flexconnect mode. FlexConnect is Cisco's wireless solution for branch office and remote office deployments. It enables to configure and control APs in a branch or remote office from the corporate office through a WAN link, without requiring the deployment of a controller in each office. A separate FlexConnect local switched group will be needed for each institution that makes use of WaaS.

- **Integration with existing infrastructures**: Many institutions already have a Wi-Fi network installed. To ensure the Wi-Fi as a Service offering does not conflict with existing Wi-Fi (in particular eduroam) implementations, it may best to deploy it step-by-step on a per-building basis, as new access points may need to be installed that cannot be managed simultaneously with previously installed ones of different brands. In this case, any old access points that need to be removed that have not reached end-of-life could be reused in other buildings.

The preliminary conclusion drawn from the pilot WaaS implementation is that the unified service that NRENs have in mind cannot be realised without differentiating the service profiles of each institution. Requirements in terms of support of additional SSIDs, clients that break-out on VLANs that make use of the trunk that connects the access points, and the support of networking components such as DHCP,

DNS and Radius, may differ for each institution. For example, the settings of an active directory may not need to be changed as a result of using WaaS. A policy will need to be defined which establishes which deviations from the unified service may be allowed, based on the estimated time that would be required for troubleshooting any issues that may potentially arise as a result of allowing such deviations.

Guarantee the Best Possible End-User Experience

The most important parameter in determining whether a WaaS implementation is successful is customer satisfaction. The customer is not represented by the institution in itself but rather by all the users (students and staff) of an institution. It is the level of satisfaction of the individual users that determines the level of satisfaction of the institution as a whole, as people who are not satisfied tend to have a louder voice than those who are. ICT personnel should have an accurate and objective perception of the level of user satisfaction. This can be achieved by measuring the performance of the Wi-Fi infrastructure in terms of how the Wi-Fi network is experienced by regular clients. Examples of tools that allow this are Epitiro StreetWise or 7signal's Saphire. These tools use dedicated test probes that behave like real users, continuously logging in and measuring network and application performance. This provides information about the Wi-Fi service as actually experienced by the end user. A drawback of these probes is that their positions are fixed so that they provide no insight into how clients experience performance when roaming between access points. Figure 5.2 shows daily performance of the network as experienced by one of these probes. Predefined threshold values are set for each application. The figure shows how often these threshold values are met. The example in Figure 5.2 reveals that the performance is satisfactory for most applications, except for VoIP applications. The VoIP Mean Opinion Score (MOS) does not meet the threshold of 3.7 in all situations. In other words, users experience unsatisfactory performance in the uplink direction (when the user speaks) as a result of the configuration of the Wi-Fi network.

▾ Floor5/eduroam surfnet account (NW-7), 5 GHz Go to top of the page

Hide/show numbers Hide/show KPI-names Hide/show KPI-codes Rotate KPI-codes Even width

	eduroam surfnet account (NW-7)/Floor5, 5 GHz										
DAY	AV008 Beacon availability in managed AP scan	AC001 Radio attach success rate	AC002 IP address retrieval success rate	QURT007 Ping success rate	RE004 TCP test success rate	RE005 VoIP test success rate	QURT004 Ping RTT	QUAP001 TCP DL throughput	QUAP002 TCP UL throughput	QUAP005 VoIP MOS downlink (listening)	QUAP006 VoIP MOS uplink (talking)
2014-09-24	100.0%	100.0%	100.0%	100.0%	99.6%	96.8%	100.0%	100.0%	98.4%	100.0%	68.9%
2014-09-23	100.0%	99.8%	100.0%	71.0%	96.7%	96.2%	100.0%	97.2%	96.9%	100.0%	65.9%
2014-09-22	100.0%	100.0%	100.0%	87.8%	97.0%	99.2%	100.0%	93.1%	96.5%	100.0%	73.6%
2014-09-21	100.0%	100.0%	100.0%	100.0%	98.7%	98.9%	100.0%	100.0%	99.6%	100.0%	68.4%
2014-09-20	100.0%	100.0%	100.0%	93.2%	99.3%	97.4%	100.0%	100.0%	100.0%	100.0%	73.6%
2014-09-19	100.0%	100.0%	100.0%	100.0%	100.0%	92.9%	100.0%	100.0%	100.0%	100.0%	92.3%
2014-09-16	100.0%	100.0%	100.0%	93.8%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	80.0%
2014-09-15	100.0%	100.0%	100.0%	95.2%	99.4%	100.0%	100.0%	91.0%	100.0%	100.0%	66.7%
2014-09-14	100.0%	100.0%	100.0%	100.0%	99.4%	98.7%	100.0%	100.0%	100.0%	100.0%	76.9%
2014-09-13	100.0%	100.0%	100.0%	100.0%	99.4%	97.5%	100.0%	100.0%	100.0%	100.0%	84.2%
2014-09-12	100.0%	100.0%	100.0%	95.2%	98.0%	100.0%	97.5%	98.7%	100.0%	100.0%	73.0%
2014-09-11	100.0%	100.0%	100.0%	95.2%	99.3%	100.0%	100.0%	98.7%	100.0%	100.0%	86.8%
2014-09-10	100.0%	100.0%	100.0%	100.0%	96.2%	98.8%	100.0%	100.0%	100.0%	100.0%	62.5%
2014-09-09	100.0%	100.0%	100.0%	95.2%	97.5%	97.4%	100.0%	100.0%	100.0%	100.0%	71.1%

Figure 5.2 Example of performance measurements as experienced by Wi-Fi clients

Based on these performance measurements, the Wi-Fi network can be examined objectively. These results also show in which area performance is unsatisfactory. An important benefit of these tools is that, as they provide the NRENs with a means to quantify service levels as they are experienced by their users, they allow them to differentiate individual client complaints from the overall satisfaction offered by the Wi-Fi service.

Establish the Prerequisites for the Application of WaaS

Since WaaS is deployed in a situation where an institution already makes use of the network services offered by the NREN, an existing (campus) infrastructure is assumed to be present. WaaS therefore makes use of the ICT infrastructure of institutions. If this infrastructure does not function properly, WaaS will not function optimally. The following prerequisites apply:

- Switches must support PoE+ (the new 802.03at standard that support up to 28Watt power). If not, APs may either not function or function sub-optimally.
- There must be a sufficient number of switch ports (and wall outlets) to connect all APs. A site survey will establish the number of APs needed, which is determined by the service levels that the wireless network must offer (capacity, high density, VoIP and location based).
- VLANs within the ICT infrastructure of the institution must be configured according to the data plan as dictated by the NREN.

- Access switches must connect each AP with a Gb/s connection. The rest of the infrastructure must also support Gb/s connectivity and must be interconnected with at least cat5e cables.

- Preferably the institution should not make use of NAT. The WaaS architecture connects various institutions and the presence of NAT would cause an overlap in address ranges that would result in conflicts.

Establish Service Contracts

The service contract describes the Wi-Fi service in terms of what is expected, and how issues should be reported as well as how long it should take to resolve them. These expectations must be described in a SMART manner, so that institutes can determine objectively whether the service complies with their proposed offering. The designated area where Wi-Fi will be offered as a service must be clearly described. Examples of defining expectations in a SMART way include:

- The Wi-Fi signal within the designated area is at least -62 dbm

- The data rate per successfully associated client is at least xx Mbit/s in the upstream direction and yy Mbit/s in the downstream direction.

- Detailed description of what the change process looks like (extra VLAN, internal changes of the Wi-Fi area, extra SSID, etc.)

Run and Manage the Wi-Fi Network as a Service

The health and availability of the WaaS system should be properly monitored. If access points or other components are not available, the personnel monitoring WaaS should take action. The monitoring system should generate alarms if components fail. Some components may not be part of the management service. Examples are Radius servers, DNS, or DHCP. The WaaS management team can use various parameters and measurements to make these observations, e.g., the number of associated clients, or data sent in the upstream and downstream directions. If deviations occur from ‘normal usage’, action should be taken.

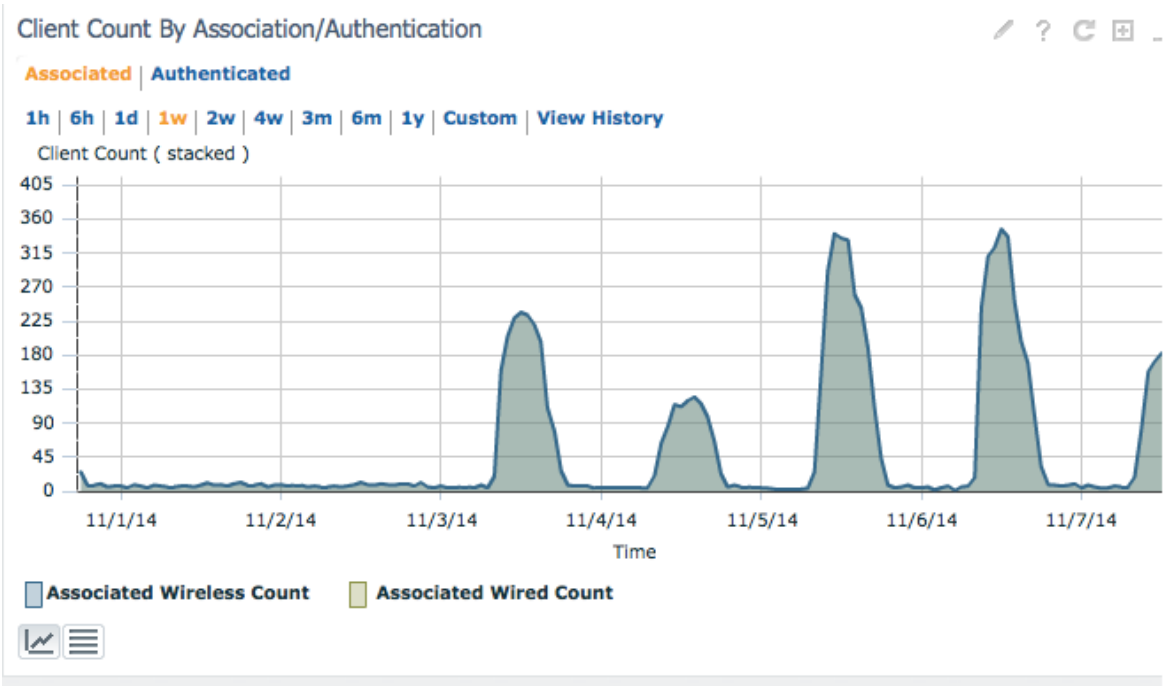

Figure 5.3 Number of WaaS clients per day

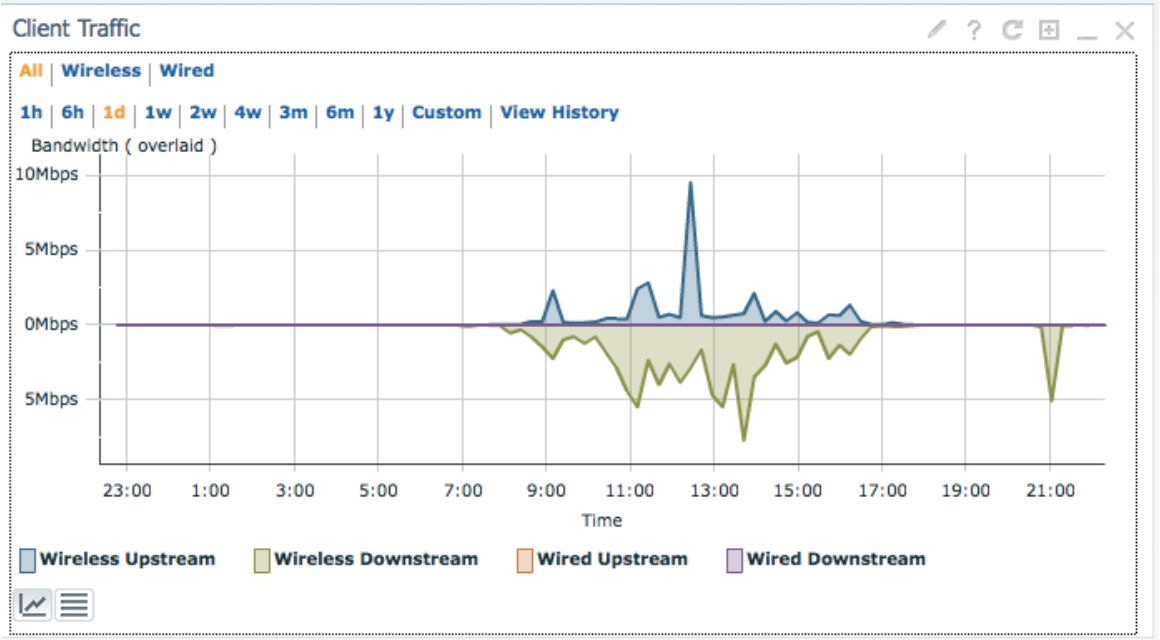

Figure 5.4 Example of data usage

While the Wi-Fi service runs, the conditions may change (radio settings, changes in the Wi-Fi design or changes in the network environment). A service change process should be installed for this purpose. This should distinguish between the different variants of service change. Adding a new building to the WaaS service for example, is not of the same order of magnitude as changing a VLAN or adding an SSID.

6 Further work: NRENs in a Connected World

JRA1 T3's ultimate vision is to define the best possible communication technologies to use the radio spectrum as a substrate to provide seamless connectivity. At this point in time, services and technologies are moving increasingly towards seamless wireless/Wi-Fi access. Further development of mobile/Wi-Fi connectivity may take a few different directions:

- **The key for integrating Wi-Fi and mobile technologies will lie in coupling the authentication process.** A dedicated SIM for the R&E community would be a giant step forward in realising this. If the R&E community had a mobile network code, a SIM could be placed on their users' own smart cards. This would prevent any problems linked to having to change SIMs when selecting a new mobile network operator. As a result, the R&E community could innovate directly on the smart card, opening up a wide range of possibilities, including easy and more secure access to federated services on mobile devices, easy and more secure access to eduroam, the ability to integrate private GSM on an Ethernet infrastructure (e.g., by upgrading existing access points), and access to printers/buildings/rooms and other facilities.
- **Integrated wirefree access service for the R&E community may be achieved in part.** Seamless mobility and vertical handover between Wi-Fi domains, and between Wi-Fi and mobile domains, will not reach maturity so long as the authentication process for different access networks remains fragmented across multiple organisations. Users will most likely have to rely on mobile communications to ensure access everywhere (mobile onload). In this case, regardless of whether such a service is provided by NRENs as mVNOs or by commercial parties, its quality level is likely to suffer somewhat. Technologies are advancing at such a pace that the actual means of communications of user equipment will be soon be hidden from the user altogether. NRENs will likely need to outsource all radio access to mobile providers (as customers or as mVNOs).
- **Trials and proofs-of-concept may still be needed to develop the technology so that it can exploit to full advantage the particular characteristics of the R&E community**, including closed user groups and the mutual trust between all the participants that derives from shared development needs. Seamless integrated wirefree access proposals from the NREN community can foster the federated use of network resources among R&E institutions. It will not be possible to integrate the Wi-Fi and mobile domains without NRENs actively being involved in mobile service provision, either as mVNOs or through some other form of joint service proposal for the R&E communities. Close collaboration with industry providers is required in order to perform PoC tests and installations. This approach will place the greatest workload on the NREN/GÉANT community, but offers the most opportunities to foster development in the field.

The Task considers that future development towards an integrated wirefree proposal is imminent within the community irrespective of which of these foreseen scenarios will take shape in the future.

Network modelling and simulation is the recommended method for the project since plans must be thoroughly evaluated before prototyping or actual development take place. Before an extension to PMIPv6 RFC is drafted, the network model requires refinement and additional simulations must be carried out. Future work will consider the inclusion of prototyping and actual implementation within the testbed. In addition, east- and westbound SDN API requirements have to be specified in order to establish interdomain tunnels on the data path by the SDN controllers.

7 Conclusions

The work of the Task has focused on the technical implementation architectures for the individual enablers of Wi-Fi and mobile access and aggregation. No unified integrated network architecture currently exists to establish seamless services, and GÉANT and the NRENs will have to make several strategic decisions regarding the direction to be taken to integrate/aggregate Wi-Fi and mobile access.

Modern education processes and technologies already require seamless connectivity. The patterns of usage show that the demand for Wi-Fi and mobile data access is unlikely to decrease.

The study and the PoC implementations tested show that the community formed of the NRENs and GÉANT possesses the capabilities and is in the position to provide a fundamental contribution to the expansion of the connectivity footprint further afield within the R&E community and across technological boundaries into the mobile domain.

The technologies for extending the Wi-Fi and mobile connectivity footprints for the R&E community are not yet in place, let alone mature enough or widely implemented. Therefore NRENs can pave the way for future development towards the federated use of the radio spectrum to achieve seamless connectivity.

The Wi-Fi and mobile service offering of GÉANT and the NRENs directly to individual R&E community members diffuses the established organisational boundaries of R&E networking. NRENs are relying on campus networks to provide the underlying infrastructure needed to offer WaaS, or offload public area traffic at the aggregation level. The federated use of network resources should be adopted by the community to facilitate operation of both local and centralised services on the same physical infrastructure. Wi-Fi and mobile (2G/3G/4G) services complement one another. Integration of these radio technologies results in improved services for the R&E community, including mobile learning.

If NRENs offer services (such as WaaS) on the premises of institutions, the traditional network boundaries shift. NRENs may choose to offer the network infrastructure of an institution or may use the campus network as prerequisite.

The best Wi-Fi design for WaaS in a given scenario is strongly determined by the service that an NREN wants to offer. A centralised solution that uses a controller allows a generic Wi-Fi service offering. This is most cost effective if the NREN hosts the controller, though NRENs have to be ready to support different design options to accommodate a wide range of requirements.

Offering Wi-Fi as a Service will require NRENs to adapt service profiles to suit the different needs of individual institutions, finding a balance between offering as wide a range of services as possible and

providing a manageable set of solutions in terms of effective operation of the network. The ICT departments of R&E institutions and providers should be directly involved in the implementation of each extension.

Seamless interdomain handover has been shown to be possible through the extension of PMIPv6:

- Given the assumption of a unified profile in the future, such as eduroam on LTE, academic and education users, i.e. students and researchers, will be highly likely to use their eduroam profile wherever they are. In such a use case, seamless handover between LTE and Wi-Fi networks becomes necessary to guarantee user QoE. Currently, as soon as a mobile device switches the point of attachment, especially to a different domain, the new network assigns a different IP address from the previous one to the mobile device. The change of IP address results in TCP connections being re-established and all applications/services using TCP connections having to restart the handshake. This reconnection will in some cases affect the user QoE, e.g. by their having to login again or by disrupting online communication. In order to avoid such a disturbance, PMIPv6 is deployed within a domain to handle the vertical handover (change the LMA domains). However, PMIPv6 requires that the mobile device move within a single domain. This will not be the case, for example, when an eduroam user moves from a commercial LTE network to a university Wi-Fi network, since these two networks belong to different administrative organisations.
- The research on HRANs aims at improving PMIPv6 by proposing an extension to the protocol to help different network domains perform network-based handover for mobile devices. The proposed extension introduces handshake messages sent by a guest LMA to the home LMA. It has been demonstrated that the handover is possible while maintaining the home IP address unchanged. Consequently, the ongoing TCP connection between the mobile device and a remote server can be preserved, and user QoE therefore guaranteed. Further research in this direction will focus on the scalability and performance of this extension.
- In addition to the PMIPv6 extension on the signalling path, the use of SDN is considered on the data path to assist in setting up multidomain IP tunnels. To enable this change on the data path, SDN controllers are to be deployed in the networks, and communications between different SDN controllers are required so that they can jointly establish the multidomain tunnels. West- and eastbound SDN controller APIs are therefore needed for such communications. Current SDN technology has not yet established a standard on how west- and eastbound APIs are defined. However, the research carried out by the Task will continue to follow the development status of SDN controller APIs.

This report concludes that no mature architectures exist as yet to offload and aggregate high-speed mobile and Wi-Fi to extend the R&E access footprint. Further study will define the principles, in terms of architecture and operations, for developing the federated use of R&E campus, provider and NREN networks.

References

[Anderson, T.] Terry Anderson "The Theory and Practice of Online Learning, Second Edition", AU Press, Athabasca University, Australia, 2008 [pp 183-235]

[Brand, J.-Kinash, S.] Brand, J. & Kinash, S. (2010). Pad-agogy: A quasi-experimental and ethnographic pilot test of the iPad in a blended mobile learning environment. In C.H. Steel, M.J. Keppell, P. Gerbic & S. Housego (Eds.), Curriculum, technology & transformation for an unknown future. Proceedings ascilite Sydney 2010 (pp.147-151).

[eduroam] https://www.eduroam.org

[Eertink, H.] Henrik Eertink, "Trend report of fixed/wireless networking: Centralized management and control of Wi-Fi networks", Surfnet report MOB-12-07c, 19 March 2013.

[ETSI 29.275] Universal Mobile Telecommunications System (UMTS); LTE; Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3 (3GPP TS 29.275 version 12.4.0 Release 12) http://www.3gpp.org/DynaReport/29275.htm

[E-UTRA] Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures, 3GPP specification 36.213., December 2012

[Gundavelli, S., Leung K., Devarapalli, V., Chowdhury, K., Patil, B.] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", IETF RFC 5213, August 2008.

[Horizon2020] Horizon 2020 Advanced 5G Network Infrastructure for Future Internet PPP Industry Proposal (Draft Version 2.1) (http://www.networks-etp.eu/fileadmin/user_upload/Home/draft-PPP-proposal.pdf)

[Interworking Wi-Fi and Mobile Networks] "Interworking Wi-Fi and Mobile Networks", Ruckus wireless, 2013, http://c541678.r78.cf2.rackcdn.com/wp/wp-interworking-Wi-Fi-and-mobile-networks.pdf

[Johnson, C.] Chris Johnson "Long Term Evolution IN BULLETS", CreateSpace Independent Publishing Platform; 2 edition (6 July 2012).

[Kreibich, Ch. et al] Ch. Kreibich, et.al. "Netalyzr: Illuminating The Edge Network", IMC'10, November 1–3, 2010

[Meyer, D. et al] D. Meyer, et.al. "Report from the IAB Workshop on Routing and Addressing", RFC 4984, Informational, September 2007

[NetGear AC1900] NetGear AC1900 Nighthawk Smart WiFi Router model R7000 product description. http://www.netgear.com/home/products/networking/wifi-routers/R7000.aspx#tab-techspecs

[Open-Mesh] http://www.open-mesh.com

[POZnan] http://www.poznan.pl/plan/plan.html?mtype=wireless

[Pries, R. et al] Rastin Pries, et al. "A Seamless Vertical Handover Approach", EuroNGI network of excellence, www3.informatik.uni-wuerzburg.de

[Q4 HE IT WLAN Survey] Q4 Higher Education IT WLAN Survey", Meru Educational Business Unit, Meru Networks, December 2012

[RFC5213] https://tools.ietf.org/html/rfc5213

[Soliman, H.] Soliman "Mobile IPv6 Support for Dual Stack Hosts and Routers", IETF RFC 5555, June 2009

[Trouve, E. et al] Eleni Trouve, et. al. "IS THE INTERNET AN UNFINISHED DEMO? MEET RINA!", paper presented at the TERENA Networking Conference 2011, Prague. https://tnc2011.terena.org/core/presentation/63

[Wong, L.H.] Lung-Hsiang Wong "A learner-centric view of mobile seamless learning", British Journal of Educational Technology; Volume 43, Issue 1, pages E19–E23, January 2012

Glossary

AP	access point
API	Application Programming Interface
eNB	see ‘eNodeB’
eNodeB	Evolved Node B (also abbreviated ‘eNB’)
EPC	Evolved Packet Core
HRAN	heterogeneous radio access network
IP	Internet Protocol
IPv6	Internet Protocol version 6
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MA	mobility anchor
MAG	mobile access gateway
MNO	mobile network operator
MVNO	mobile virtual network operator
NREN	National Research and Education Network
PMIPv6	Proxy Mobile IPv6
QoS	Quality of Service
R&E	Research and Education
RINA	Recursive Inter Network Architecture
RRH	remote radio head
SDN	Software-Defined Networking
SMART	Criteria to guide in the setting of objectives: *Specific, Measurable*, *Assignable, Realistic, Time-related*
UE	user equipment
WaaS	Wi-Fi-as-a-Service