Policy Management and Inter-domain Mobility for eduroam through virtual Access Points (vAPs)

Daniel Camps-Mur (daniel.camps@i2cat.net), I2CAT Foundation, ES
Ilker Demirkol (ilker.demirkol@entel.upc.edu), Universitat Politecnica de Catalunya, ES
Raimundas Tuminauskas (raimundas.tuminauskas@ktu.lt), Kaunas University of Technology, LT
Zbigniew Ołtuszyk (zbigniew.oltuszyk@man.poznan.pl), Poznan Supercomputing and Networking Center, PL

Keywords

Virtual Access Points (vAPs), Inter-domain Mobility, Wireless Policing, Open Mobility Exchange

Abstract

This work studies the application of the virtual Access Point (vAP) technology to the eduroam [1] service. The vAP technology is based on instantiating multiple Access Point instances over a single physical WLAN radio, without requiring support for any special feature on the mobile devices. In this work vAPs are used for the purpose of enabling per-realm policies at the wireless segment, and facilitating inter-domain mobility.

Using vAPs for multi-vendor policy provisioning

Given the increasing demand on mobile data, situations where an eduroam Access Point can become congested at the radio level are more likely to occur. An eduroam service provider (SP) thus has to be able to define and enforce per realm policies in the wireless segment, such as prioritizing users from its home eduroam realm when congestion occurs. Several QoS mechanisms could be applied to enforce per realm policies at the radio level [2], but these mechanisms are not standardized across vendors. Hence, in this paper we propose the usage of the vAP technology, supported across major WLAN vendors [3,4,5], as a mechanism to enforce per-realm QoS policies.

A WLAN Access Point controls the channel access priority of its associated users including the WMM Parameter Set in the Beacon frames it transmits, which contains the Contention Window (CW) settings used by the associated stations to access the wireless channel. Thus, if a (group of) eduroam realm(s) is represented by a vAP, the wireless access priority of the users attached to that vAP can be controlled by appropriately configuring the WMM Parameter Set broadcasted by the vAP. Notice that major WLAN vendors already provide tools to configure these parameters [6].

The challenge is how to force users of a specific eduroam realm to attach to a particular vAP, since in eduroam all vAPs advertise “eduroam” as their SSID, regardless of the realm they represent. In order to steer users across vAPs we propose to use black and white listing mechanisms based on the mobile device’s MAC address. The challenge though is how to

dynamically populate the access control lists of each vAP given that it is not possible to know *a priori* all the MAC addresses of the users of a given eduroam realm. Instead, any practical solution needs to identify the eduroam realm a given user belongs to first, and only afterwards configure the access control lists of the vAPs.

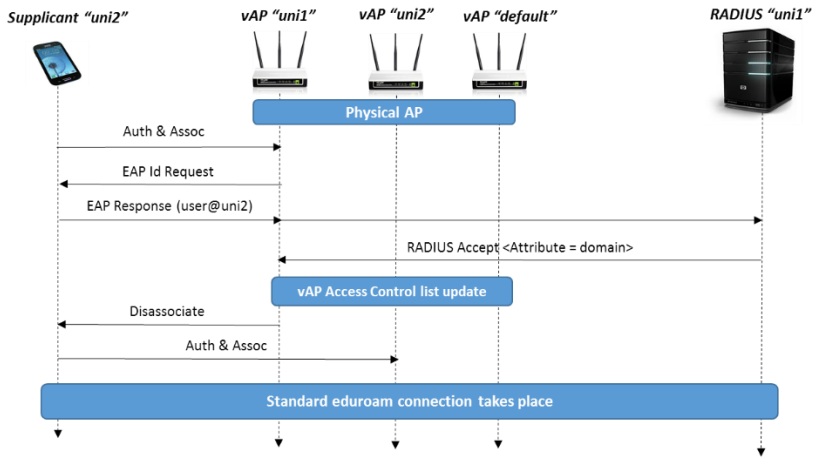

Figure 1. User steering to the appropriate vAP

Figure 1 illustrates a mechanism devised to steer a requesting user to the vAP representing its realm. We can see a physical AP where three vAPs have been pre-instantiated, one to represent each of the major universities offering eduroam services in a city, "uni1" and "uni2", and another one to represent any other eduroam realm ("default"). Thus, when a mobile device from a user belonging to the "uni2" realm connects to the AP for the first time, it will do so through any of the vAPs, since none of the vAPs have the user's MAC address in their black list, e.g. the "uni1" vAP. Consequently, the user will associate and proceed with the normal eduroam authentication process, whereby the home AAA server identifies the requesting user's realm, which is then notified to the WLAN controller using a RADIUS AV pair in the RADIUS ACCEPT response. Hence, the WLAN controller pushes the user to the corresponding vAP by blacklisting its MAC address in the other vAPs. The experimental evidence gathered so far indicates that existing mobile devices in the market persistently try to connect to all vAPs advertising the same SSID, which confirms the validity of this approach. Ongoing work is focused on testing the validity of this approach over a larger sample of smartphones, and evaluating the delay introduced by the proposed mechanism in the standard eduroam association procedure.

Finally, it is worth noticing that in any practical deployment the number of vAPs instantiated in a given physical AP should be limited, e.g. below five, in order to reduce the introduced over the air overhead in terms of transmitted Beacon and Probe Request/Response frames.

Leveraging vAPs to enable L2 inter-domain mobility

Although not strictly necessary to achieve inter-domain mobility, the proposed vAP concept naturally extends to a layer two inter-domain mobility solution, whereby the WLAN controller binds traffic generated from a vAP corresponding to a home eduroam realm to a

layer two tunnel between the visited and home eduroam realms. In order to limit the effect of remote broadcast traffic traversing the layer two tunnel over the radio channel, vAPs should implement Proxy ARP functionalities [7]. Candidate technologies to implement the required layer two tunneling are for instance Ethernet over GRE (EoGRE), which is also supported by major networking vendors [8], and can be secured using IPSEC.

In a practical implementation both vAPs and the corresponding EoGRE tunnels for the target eduroam relams should be pre-instantiated, for instance one for each realm coexisting in a given city. Notice though, that pre-instantiated EoGRE tunnels do not scale if the number of tunnels is large. In this case, we propose to introduce a new entity implementing an Open Mobility Exchange (OMX), which maintains EoGRE tunnels with all existing eduroam realms. Thus, the OMX routes the packets received from an EoGRE tunnel to their corresponding home domains, by inspecting in-packet information, e.g. a VLAN tag, indicating the target eduroam realm. A detailed implementation of the OMX is left as future work.

Figure 2 illustrates the setup of the EoGRE tunnels to ensure inter-domain mobility, by routing user traffic always through their corresponding home network.

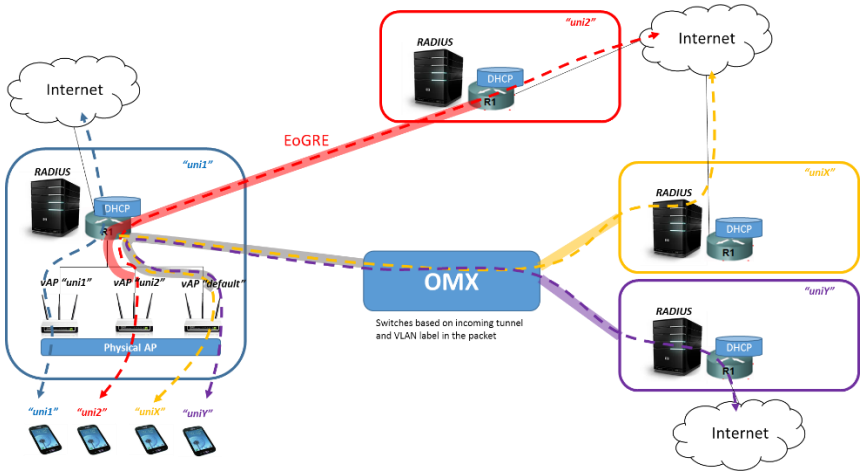

Figure 2. L2 tunnelling for inter-domain mobility, comprising direct tunnels and OMX routed tunnels

Summary

The paper at hand proposes to introduce virtual Access Points (vAPs) to the eduroam architecture, with the goal of enabling policy management in the wireless domain and layer two inter-domain mobility. Ongoing work is devoted to validate the proposed architecture using open source WLAN and AAA implementations, while future work will focus on porting the proposed solution to a commercial WLAN implementations.

Acknowledgements

The research leading to these results has received funding from European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1). This proposal was prepared as a part JRA1 Task2 “Interworking of Technologies and Organisational Entities”

References

[1] Info about the eduroam (**edu**cation **ro**aming), available at: https://eduroam.org

[2] Cisco airtime fairness, available at: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_010100100.html

[3] Cisco Meraki, Multi-SSID deployment considerations, available at: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Multi-SSID_Deployment_Considerations

[4] Aruba, Virtual APs, available at: http://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/VirtualAPs.php

[5] Linux Wireless vifs, available at: https://wireless.wiki.kernel.org/en/users/documentation/iw/vif

[6] Cisco, Configuring QoS, available at: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4_3g_JA/configuration/guide/ios1243gjaconfigguide/s43qos.html

[7] Cisco Proxy ARP, http://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13718-5.html

[8] Cisco Ethernet over GRE, available at: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ir-eogre.html

Vitae

Daniel Camps Mur is currently leading the Mobile and Wireless Internet Group (MWI) at the I2CAT Foundation. His research interests lie generally in the wireless domain, specifically on the Internet of Things (IoT) and on wireless SDN, where he investigates architectures and algorithms to improve the capacity of mobile communication networks, focusing on Wi-Fi. Previous to working at I2CAT, Daniel was a researcher at NEC Networks Laboratories in Heidelberg, Germany, where he was involved in standardization for wireless LANs contributing both to the Wi-Fi Alliance and to the IEEE 802.11 working group.

Ilker Demirkol is Ramon y Cajal Research Professor in Network Engineering Department at Universitat Politecnica de Catalunya. His research targets communication protocol development for wireless networks, along with performance evaluation and optimization of such systems. Demirkol received his B.Sc., M.Sc., and Ph.D. degrees in Computer

Engineering from the Bogazici University, Istanbul, Turkey. Over the years, he has worked in a number of research laboratories and companies, where he held positions such as Network Engineer, System and Database consultant, and Lecturer.

Raimundas Tuminauskas joined Kaunas University of Technology as a full time network engineer in July 1997. He has soon become responsible for the high capacity switching and routing in Lithuanian NREN LITNET backbone. He currently heads backbone networks unit, in charge operations and planning of LITNET network and services. Being deeply involved in the creation of long-term plans, he is directing the efforts towards optical communications, future networking, open architectures, open network technologies, federated use of network infrastructure, and integrated radio access. Raimundas has a MSc degree in Computer Sciences.

Zbigniew Ołtuszyk received an M.Sc. degree in Computer Science from Poznan University of Technology in 1999. He joined PSNC in 1998. He is a leader of wireless network team. He is responsible for network operations, network planning and service provisioning. Since 2004 he has been the involved in the eduroam project in Poland, responsible for RADIUS national server infrastructure. He has been involved in the PLATON project, responsible for eduroam. He participated in the GN2, GN3, GN3plus EU co-funded projects, in the field of wireless networking technology testing and development. He has been a coordinator of the GN3plus Open Call project - SENS. He is currently involved in the GN4 EU co-funded project. He currently involved as a contract engineer of Metropolitan Wireless Network in Poznan.