

# Carrier-Grade SDN-Controlled WLAN-Sharing: a Performance Evaluation of OpenFlow-Enabled Commodity-based Hardware Networking Nodes

Maxweel S. Carmo<sup>1,2</sup>, Thalyson L. de Souza<sup>1</sup>, Alisson Medeiros<sup>1</sup>, Augusto V. Neto<sup>1,3</sup>, Sandino Jardim<sup>1,2</sup>

<sup>1</sup>Departamento de Informática e Matemática Aplicada  
Universidade Federal do Rio Grande do Norte (UFRN), Natal-RN, Brasil

<sup>2</sup>Instituto de Ciências Exatas e da Terra  
Universidade Federal de Mato grosso (UFMT), Barra do Garças-MT, Brasil

<sup>3</sup>Instituto de Telecomunicações – Aveiro, Portugal

max@ufmt.br, {thalysonluiz, alisson}@ppgsc.ufrn.br,  
augusto@dimap.ufrn.br, sandino@ufmt.br

**Abstract.** *Advances in Internet of Things and smart cities approaches are resulting in an unprecedented number of devices requiring connectivity. Due to the ubiquitous presence of Wi-Fi networks, connectivity solutions obtained from residential WLAN-sharing are becoming increasingly popular, although they are still very restricted in scope, and offer a general connectivity service for users seeking to surf the Internet. We argue that with a proper network control plane and orchestration mechanisms like those provided by SDN, ISPs would be able to leverage the available Wi-Fi infrastructure so that it can offer network services that are tailored to the specific needs of mobile nodes and users. In this paper a general framework is set up to achieve this goal. As our approach explores low-cost commodity Wi-Fi access points and switches, we also include a study of the effects of SDN on a local network built on this class of equipment.*

## 1. Introduction

The development of 5G networks [Andrews *et al.* 2014] is being driven by the connectivity requirements of Internet of Things (IoT) [Tschofenig *et al.* 2015] applications, and its categories include both massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC). In mMTC, large numbers of low-cost devices can be defined with high scalability requirements and increased battery lifetime, whereas URLLC relates to mission-critical applications, in which an uninterrupted and robust exchange of data is of the utmost importance. In view of both aspects of high density and demand for network services with regard to IoT applications, ubiquitous connectivity plays a major role. The research community and industry are constantly searching for new solutions to suit these key requirements. According to the latest Cisco Visual Networking Index (VNI) Report [Forecast 2016], 51% of the total amount of mobile data traffic was offloaded through IEEE 802.11-based Wireless Local Area Network (WLAN) infrastructures in 2015, surpassing that of cellular traffic for the first time. Thus, the concept of the global wireless community

network is emerging as a highly promising asset among the available ubiquitous connectivity services. The guiding principle behind this concept is to create a global Wi-Fi ecosystem that can provide seamlessly, ubiquitous access to the Internet at millions of global hotspots. The success of the concept of a global wireless community network depends to a great extent on both the participation and support of Internet Service Providers (ISPs) and their corresponding customers. On the one hand, ISPs must provide carrier-grade tools to deliver a Wi-Fi service to millions of global hotspots, and thus be able to provision seamless access ubiquitously. On the other hand, customers must agree to share their own Wi-Fi WLAN with community members, thus turning a simple home WLAN into a dual-access Wi-Fi-shared infrastructure, for private (i.e. the owner) and public (i.e. community members) use. These features can make the WLAN-shared concept economically viable, as well as establishing another carrier-grade profitable service by reselling Internet connectivity [Biczók *et al.* 2011].

Traditionally, home WLANs embody commodity-based hardware networking devices, which means standard-issue off the shelf multifunctional nodes (i.e. the modem, switch, router and wireless access point functions in the same device); there are no outstanding features embedded in them and they are widely available for purchase at a low cost. However, these devices either lack appropriate tools or have inflexible proprietary software with very limited network resource control capabilities. Moreover, the customer must bear the cost of operating in-device tools, which are needed for setup network control functions (e.g., bandwidth reservation, classifying policies and queue disciplines). This is an easy task for a network professional but can be a complete nightmare for a home user who mainly wants to surf on the Internet without any concern about particular aspects of the system. For this reason, it makes sense for the WLAN-shared system to be under the carrier-grade control plane, which is likely to have expertise in this subject.

With regard to the question of provisioning dynamic resource control in WLAN-shared systems, the Software-defined Networking (SDN) [Boucadair and Jacquenet 2014] has emerged as an asset for ISPs. Through their approach to SDN network programmability, central controllers have the capacity to initialize, control, change, and manage the network behavior of the targeted networking devices dynamically, via open interfaces. The WLAN-shared systems that adopt the network programmable approach can be controlled by ensuring that the corresponding ISP installation embeds SDN controllers that feature appropriate carrier-grade network control applications, whilst home Wi-Fi routers must embed an open SDN control interface such as OpenFlow [ONF 2013]. Through this ecosystem, a given ISP can deploy customized SDN controllers featuring fine-grained resource control mechanisms that are tailored to its WLAN-shared community. In this way, it can obtain the capacity to provision optimal resource allocation at the carrier-grade level.

This paper makes an advance on our previous work [Carmo *et al.* 2017] by examining a real testbed that comprises a network topology of nine OpenFlow-capable commodity-based networking devices of different hardware platforms (instead of a single isolated router that was studied previously). The aim is to assess the suitability and resulting performance when carrying out SDN network programmable functions on commodity-based networking devices (beyond the domain of WLAN home devices), but from the perspective of a holistic network with redundant communication opportunities. In this kind of scenario, targeted devices run other networking services

apart from Wi-Fi APs, e.g. dynamic routing in the presence of redundant paths, which can provide a more accurate view of the SDN capabilities that can be exploited by commodity-based routers, and are suitable for different use cases.

The remainder of this paper is structured as follows Section II provides an overview of WLAN-shared Internet access. Section III introduces our SDN-based framework, while the preliminary results obtained from an assessment of the WLAN switches are discussed in section IV. Finally, the last section concludes the article.

## 2. Overview of WLAN-Shared Internet Access Solutions

The wide availability of home Wi-Fi networks has led to initiatives aimed at expanding Wi-Fi coverage for a community of customers. Among these initiatives (e.g., Comcast Xfinity<sup>1</sup> and WLAN to Go<sup>2</sup>), the most notable and successful WLAN-shared provider is FON<sup>3</sup>. During the last 10 years, FON has built the world's largest Wi-Fi network community, which comprises millions of people who have agreed to share their WLAN broadband connection with external users for seamless experience when accessing. FON relies on the partnership of leading carriers and Wi-Fi providers around the globe, and seeks to boost seamless connectivity service provisioning for member customers at millions of hotspots worldwide. An OpenWrt customized version has been deployed specifically for use in the FON Community to provide home customers with a FON WLAN-shared service. Following the installation of this FON-tailored OpenWrt version, the commodity-based Wi-Fi router becomes a "Fonera 2.0", and thus allows consumers to share their broadband connection and connect to other FON Spots around the world. With the Fonera device, two different Wi-Fi signals are created, one for private access and another for public access. In the former, the FON Spot owner has exclusive access and is thus able to leverage encrypted traffic service. In the latter, only registered FON users have the right to access an open (unencrypted) network system.

Although this system enhances opportunities for seamless connectivity, in our view existing WLAN-shared infrastructures are far from ideal as a means of providing an appropriate support for emerging scenarios like those involving IoT, smart cities, and the ever-increasing demand for connectivity by mobile users. For instance, FON only makes available one network per AP for public usage. We believe that to offer appropriate network services that can cater for the individual demands of mobile (and heterogeneous) nodes, it would be more appropriate to make multiple virtual networks available, each tailored to meet specific needs, i.e., the different V-WLANs could have different bandwidth capabilities and deploy different network functions to cope with the required behavior of the system, technical requirements and so on.

In addition, the one-size-fits-all public network made available by current WLAN-sharing systems, is designed for mobile users that want to surf the Internet. There is no differentiation of services on the basis of applications or types of devices. Moreover, there is no concern about optimizing the network resources at a global level to efficiently serve a larger number of users/devices. For instance, a number of people

---

<sup>1</sup> <https://www.xfinity.com>

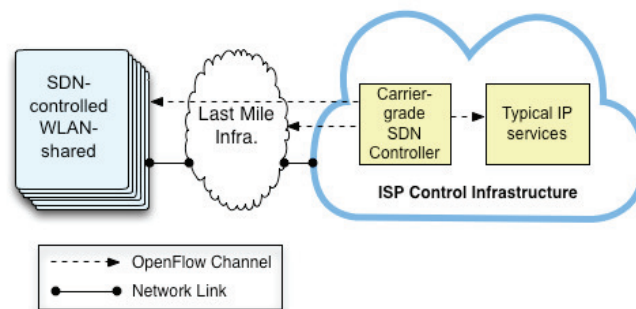
<sup>2</sup> <http://www.telekom.de/wlan-to-go>

<sup>3</sup> <https://fon.com>

spend most of the day at work, which means their WLAN infrastructure is probably left with the minimum use. Thus, ISPs could set the private V-WLAN with minimum bandwidth allocations, and leave the remainder of the resources for the Public V-WLAN with the prospect of providing enhanced connectivity for the community members. When the WLAN owner reports back to his network, the ISP can re-adapt the bandwidth, and even use smart mechanisms to allocate the required resources in advance. In addition, there is no support for mobility management in the current systems, which can for instance, help devices to connect to the best public network available at a particular moment. All these requirements call for a networking control plane that is able to act on a globally perceived network topology to meet the diverse needs of the mobile nodes.

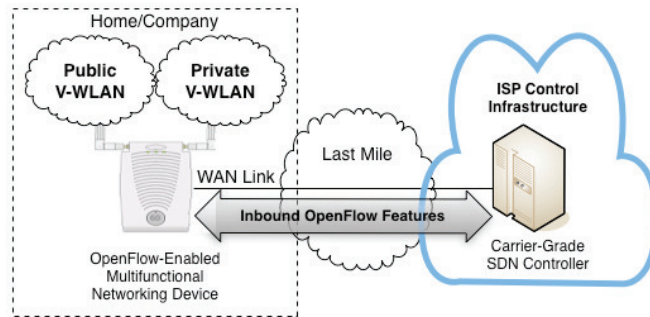
### 3. SDN-Controlled WLAN-Shared Framework

As highlighted in Section I, the WLAN-shared software for resource control envisions controlling the behavior of the corresponding networking devices to provision optimal use by private and open community members. In our opinion deploying the control plane at the carrier-grade level is the most appropriate manner to provide a fine-grained approach that can enable the WLAN owner to keep "surfing" the net with an acceptable quality of experience. Moreover, WLAN-shared residential infrastructures feature commodity-based Wi-Fi access points that are generally performance-constrained and low-cost to suit the needs of the end-user. Hence, the addition of the SDN approach to these types of nodes will certainly provide the prospect of overcoming additional performance issues, and ensuring suitability. Figure 1 illustrates our proposed carrier-grade SDN-controlled WLAN-shared architecture.



**Figure 1. Carrier-grade SDN-Controlled WLAN-shared Ecosystem**

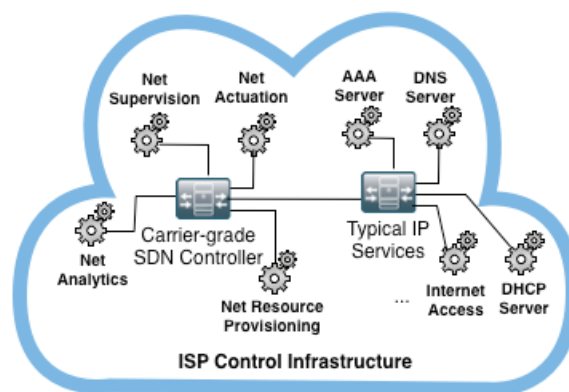
The architecture depicted in Figure 1 shows the key systems of our proposed Carrier-Grade SDN-Controlled WLAN-Shared ecosystem. The WLAN-shared system is responsible for the provision of wireless connectivity, generally through Private (customer owner) and Public (community-members) Wi-Fi networks that seek to provide broadband communications to mobile and/or fixed nodes. Traditionally, ISPs include a multifunctional device to manage the connectivity at the WAN link of varying data rates (from 54Mb/s to 300 Mb/s). With regard to our SDN-controlled WLAN-Shared system, on the customer side there is a multifunctional device provided by the ISP, which is responsible for the provisioning of different Wi-Fi networks and “net-programmable” capabilities. Our view of a targeted customer network infrastructure is shown in Figure 2.



**Figure 2. SDN-controlled WLAN-shared system on the customer side, interoperating with the carrier-grade SDN controller**

The multifunctional device must support an SDN interface to comply with our SDN-based WLAN-shared ecosystem, in this case, OpenFlow. There is a wide selection of APs available in the market, with prices ranging from tens to even hundreds or thousands of dollars. A number of low-cost commodity-based Wi-Fi router manufacturers already supply proprietary embedded operating systems featuring OpenFlow, mostly version 1.0. Alternatively, an open source environment can be adopted through OpenWrt<sup>4</sup>, along with Open VSwitch (which offers support for all versions of the OpenFlow protocol) [Pfaff *et al.* 2015].

The last mile infrastructure mostly comprises broadband telecommunication devices, which are responsible for carrying signals from the broad telecommunication backbone to and from the home or business networks. As robust devices are used in these types of systems (and have high-performance and networking capabilities), SDN is not a problem, and thus their study is beyond the scope of this paper. Figure 3 depicts the ISP-level Control system infrastructure.



**Figure 3. ISP-level control, key infrastructural systems and networking management functions**

The ISP system adopts an approach to a fully integrated Internet system approach that allows it to provide a wide range of IP services and applications to a limited amount of customers seeking personal and business access to the Internet. The list of typical IP services includes the following: Internet access, domain name hosting,

<sup>4</sup><https://openwrt.org>



network broadband access, Authentication Authorization and Accounting – AAA, web hosting, emailing, transit, among other services. In attempting to cope with SDN, the ISP infrastructure must integrate the SDN controller so that it can act in the network control plane.

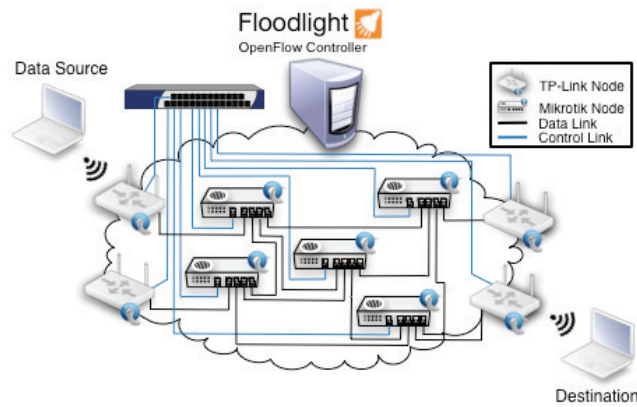
We believe that even though the ISP incurs extra costs because it requires investing in additional infrastructure, it will be able to exploit the customer network infrastructure and resell Wi-Fi Internet access. Apart from providing traditional Internet-access for users, the Internet of Everything (IoE) [Evans 2012] application scenario can benefit from this wireless networking opportunity. IoE is turbinated by devices, ranging from connected coffee makers, cars, or sensors on cattle to connected machines in a production plant, and can thus leverage broadband wireless/wired home network systems. Network operators can exploit this scenario to apply opportunistic Internet access, by sharing the bandwidth of WLANs with nearby devices. In addition the network providers can handle the systems to maintain WLAN QoS, for example by using NFV technology [Hawilo et al. 2014, Mijumbi et al. 2016] to virtualize different wireless networks, and allocate resources to each of them by taking account of their needs, contracts, and so on. Thus, network providers can offset the additional costs, and earn more revenue at the same time.

#### **4. Performance Assessment**

We carried out a set of experiments to analyze whether it was feasible for ISP to enable the SDN functions to be used with networking nodes that feature commodity-based hardware capabilities, while taking into account the SDN-controlled WLAN-shared scope. To the best of our knowledge, there are no studies in the literature that make a performance evaluation of OpenFlow in a network topology comprising a set of interconnected commodity-based networking devices. However, the literature has authors who include a single device at the center of their targeted assessment. Examples of initiatives taken in this area include [Gharakheili *et al.* 2015], where the authors designed, implemented and evaluated an SDN-controlled system that allows a third-party to define which subscribers can easily customize Internet sharing within their household. The evaluations demonstrated the feasibility and utility of the proposal in the real world, and included home router equipment featuring an OpenFlow protocol. In [Lima *et al.* 2015], the authors evaluated the OpenFlow performance of a commodity-based wireless router running Open vSwitch linked to different SDN controllers. The evaluation was of a set of client hosts connected at the router, with the aim of sending data traffic towards a sink server. The key networking metrics included: throughput, delay, jitter, and packet loss. The outcome suggested that commodity-based wireless routers should be used in smaller networks, such as homes and small -to -medium sized organizations.

Although the dual-access WLAN-shared service is provisioned by a Wi-Fi home AP, there are a number of environments featuring a Wi-Fi network composed of several APs that form a bridge (such as restaurants, hotels, clubs, and the like). This has led us to carry out studies in both suitability and performance, which involves having commodity-based networking devices, interconnected with each other to form a wired mesh topology that is used to deploy OpenFlow networking functions. With this goal in mind, the methodology employed for the performance assessments defines a real testbed

for allowing highly accurate benchmarking perspectives. The network topology of the testbed is depicted in Figure 4.



**Figure 4. The Testbed Topology adopted in the experiments**

The testbed configuration set includes 9 commodity-based networking nodes that are marketed throughout the world at a low cost. The network border embodies 4 TP-Link type nodes set at IEEE 802.11n access points, whilst the core network infrastructure features 5 Mikrotik type nodes that target switching functions. The control data communication takes place through dedicated links. We replaced the original firmware devices with the OpenWrt operating system and installed the Open vSwitch to implement OpenFlow capabilities. The configuration of the network elements is shown in Table I.

**Table I. Key Specifications of hardware**

Manufacturer	Hardware Capabilities		
	Model	CPU	RAM
TP-LINK	TL-WR1043ND v3	720 MHz	64 MB
Mikrotik	951G-2HnD	600 MHz	128 MB

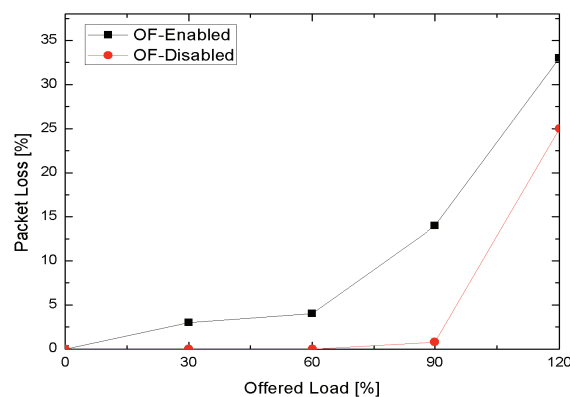
The methodology employed for the performance evaluation entailed incorporating a number of individual flow traffic data to obtain the specific load rates (30, 60, 90, and 120% of the maximum network bandwidth capacity). In carrying this out, the D-ITG tool [16] which was running on the client and server machines, generated UDP data flows at a constant rate of 407 Kbps each, which amounted to a total of 293 UDP flows per heavy workload (120%). A specific network application is deployed in compliance with the Floodlight<sup>5</sup> SDN controller. All the new packets arriving at the border switches were directed to the application, which in turn installed a corresponding flow for each of the switches along the path between the client and server machines. Two different sets of experiments are carried out to check the networking behavior at both flow-level and level of video streaming quality.

<sup>5</sup>[www.projectfloodlight.org/floodlight](http://www.projectfloodlight.org/floodlight)

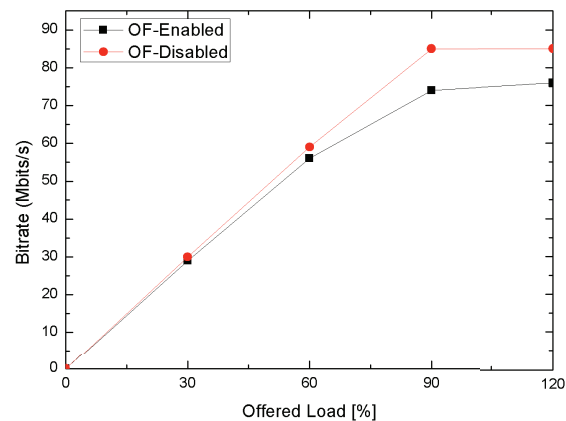
#### 4.1. Flow-Level Networking Set of Experiments

The goal of the experiments was to evaluate how the OpenFlow software layer affects the performance of the devices in terms of packet loss and throughput.

Figure 5 shows a comparison between the packet loss ratios in scenarios where OpenFlow is enabled and disabled. In the case of any offered load, the network experiences a higher packet loss when OpenFlow is running; this is mainly due to the time needed for the controller to configure the switches along the path (the packets are buffered at the ingress switch till the controller installs the flows at the appropriate switches). Figure 6 depicts the corresponding bitrate. In an offered load of 60%, the OF-enabled scenario has a performance that is just 5% lower than when OF is disabled. The difference increases to 13% for 90% of the offered load.



**Figure 5. Impact of the variations in the offered load on the behavior of the packet loss**



**Figure 6. Impact of the variations in the offered load on the throughput behavior**

#### 4.2. Video Streaming Quality Set of Experiments



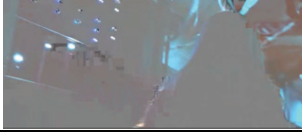
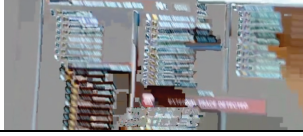


We carried out a second set of experiments in the testbed to assess its performance when a multimedia streaming session is connected along with the D-ITG background data traffic. This set of experiments is run at the testbed where it is configured with 120% of offered load, and seeks to allow subjective benchmarking in heavy saturation networking conditions. The methodology employed involves scaling



the testbed with a multimedia streaming service based on the VLC Media Player<sup>6</sup>, in addition to D-ITG data flow traffic model. The “Source Node” of the testbed is set so that it can stream a H.264 encoded real video file using RTP/UDP towards the “Destination” node. No Quality of Service (QoS) control functions are included, since this paper is only concerned with assessing the OpenFlow performance on the testbed.

The video streaming session is invoked by the "Destination" node during the 15 seconds of the running time for the experiment, and keeps running till the end of the experiment (i.e., 33 seconds). With regard to the methodology employed for assessing the impact caused by the over-saturation networking conditions during the video streaming session, we observed degradation of the streaming-level quality caused by an event occurrence during the workflow experiment. Moreover, we calculated the time taken in both testbed configurations (i.e., OF-enabled and OF-disabled) for the VLC client to setup the video streaming session with the VLC server and check the influence of OpenFlow on the additional features of OpenFlow in the setup time of the session. Table II shows three video samples obtained during both sets of experiments.

**Table II. Video samples during the workflow experiment**

<i>OF-enabled</i>	<i>OF-disabled</i>
Video Sample 1.1	Video Sample 2.1
	
Video Sample 1.2	Video Sample 2.2
	
Video Sample 1.3	Video Sample 2.3
	

With regard to the OF-enabled testbed configuration, a grey screen with no viewable video motion (Video Sample 1.1 of Table II) appears after 6 seconds of the request for the VLC client stream session, probably on account of the VLC bufferization. The grey screen remains the same for about 4.2 seconds, and then starts showing a low-quality video streaming (Video Sample 1.2 of Table II) for about 4.3 seconds. From this time on (14.9 seconds), the video starts streaming with good quality (Video Sample 1.3 of Table II) until the end of the workflow experiment. As expected, the over-saturation networking conditions caused degradation occurrences in the video quality (e.g., frame loss), but these were very slight and short-term which meant that on the whole, it was a very good streaming session.

<sup>6</sup><http://videolan.org/vlc>

The same screen patterns experienced during the OF-disabled set of workflow experiments also occurred in the OF-enabled one. The grey screen (Video Sample 2.1 of Table II) appears after 5.7 seconds of the VLC client request, and switches to a low-quality video (Video Sample 2.2 of Table II) after 3.9 seconds. After 3.8 seconds (making a total of 13.4 seconds for the streaming setup time), the video streams maintain a good quality till the end of the workflow experiment with slight and short-term quality degradation occurrences for the same reason i.e. networking over-saturation.

The numerical results of the multimedia assessment reveal that there are slight differences in performance in the video streaming on top of OpenFlow at both the OF-enabled and OF-disabled testbed configurations. On the one hand, the session setup time for the OF-enabled set of experiments was 6 seconds, whereas for the OF-disabled set it was 5.7 seconds (5%). With regard to the video streaming session with good quality, the OF-disabled set of experiments took around 19.1 seconds, whilst the OF-enabled set averaged 20.5 seconds. Hence, video streaming on top of the OpenFlow approach and in oversaturated networking conditions displays, slightly higher latency (5% in session setup time, and 7% for VLC buffering when starting the video with good quality) than when running in a conventional system (i.e., without OpenFlow). On the other hand, the video streaming quality remains the same.

## 5. Conclusion and Suggestions for Future Work

In this study, a general framework was established that was based on SDN and aimed at allowing ISPs to leverage the already existing WLAN infrastructure in urban centers. The purpose of this was to offer tailored connectivity services to mobile nodes through dynamic sharing of these networks between the owner and third parties. The framework includes low-cost commodity hardware, switches and wireless routers. A set of experiments was conducted to show that these devices were suitable for supporting the framework, and the OpenFlow protocol was used to control a network that consists of these devices. Although it has incurred some performance penalties, the SDN approach is still a good choice in view of the benefits it can provide to WLAN sharing-based Internet access.

The next steps of our work will focus on prototyping the carrier-grade SDN-controlled WLAN-shared approach by means of a Wi-Fi router featuring commodity-based hardware capabilities. Afterwards, we will assess the prototype to determine its suitability and performance.

## Acknowledgments

This work was partly supported by the SMART (CNPq Universal grant number 457051/2014-0) and Smart Metropolis research projects. The authors would like to thank the Coordination for the Improvement of Personnel in Higher Education (CAPES), the National Council for Scientific and Technological Development (CNPq) and the Mato Grosso State Research Foundation (FAPEMAT). The experiments were carried out at NPITI/UPLab of Instituto Metropole Digital (IMD) and we are grateful to all the personnel at the laboratory for their help.

## References

- Andrews, J.G., Buzzi, S., Choi, W., Hanly, S.V., Lozano, A., Soong, A.C. and Zhang, J.C. What will 5G be? Selected Areas in Communications, IEEE Journal on, 32(6), 2014
- Tschofenig, H., Arkko, J., Thaler, D., and McPherson, D. "Architectural Considerations in Smart Object Networking". Internet Architecture Board (IAB) Request for Comments (RFC) number 7452, March 2015
- Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper. Feb. 2016
- Biczók, G., Toka, L., Gulyás, A., Trinh, T., and Vidács, A. "Incentivizing the global wireless village". Computer Networks, Vol. 55, Issue 2, Feb. 2011, pp. 439-456. DOI=<http://dx.doi.org/10.1016/j.comnet.2010.08.014>
- Boucadair, M., Jacquenet, C. "Software-Defined Networking: A Perspective from within a Service Provider Environment", Internet Engineering Task Force (IETF) Request for Comments (RFC) number 7149, March 2014
- Open Networking Foundation, "The OpenFlow Switch Specification, Version 1.4.0", October 2013. [online]. Available at: <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf>
- Carmo, M., de Souza, T., and A. Neto, "On Expanding Carrier-Grade SDN Control-Plane to WLAN customer-side Systems: Performance Evaluation of Commodity-Based Wireless Nodes", 5th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE'17), Evry, France, Jan 2017
- Gharakheili, H., Exton, L., Sivaraman, V., Matthews, J., and Russell, C. "Third-party customization of residential Internet sharing using SDN," 2015 International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, 2015, pp. 214-219. Doi: 10.1109/ATNAC.2015.7366815
- Lima, L., Azevedo, D., and Fernandes, S. "Performance evaluation of OpenFlow in commodity wireless routers," 2015 Latin American Network Operations and Management Symposium (LANOMS), Joao Pessoa, Brazil, 2015, pp. 17-22. Doi: 10.1109/LANOMS.2015.7332664
- Pfaff, B., Pettit, J., Koponen, T., Jackson, E. J., Zhou, A., Rajahalme, J., ... & Amidon, K. (2015, May). The Design and Implementation of Open vSwitch. In NSDI (pp. 117-130).
- Evans, D. "The internet of everything: How more relevant and valuable connections will change the world." Cisco IBSG (2012): 1-9
- Hawilo, H., et al. "NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC)." IEEE Network 28.6 (2014): 18-26
- Mijumbi, R., Serrat, J., Gorricho, J. L., Bouten, N., De Turck, F., & Boutaba, R. (2016). Network function virtualization: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 18(1), 236-262.