Chandelle: Smooth and Fast WiFi Roaming with SDN/OpenFlow

Sergey Monin
Applied Research Center For Computer Networks
smonin@arccn.ru

Alexander Shalimov
Applied Research Center For Computer Networks
ashalimov@arccn.ru

Ruslan Smeliansky
Applied Research Center For Computer Networks
rsmeliansky@arccn.ru

Abstract

In this paper we present Chandelle system that shows the benefits of having WLAN networks on top of SDN/OpenFlow infrastructure: faster and smooth migration procedure and cost reduction of wireless access points.

1 Introduction/Motivation

As IEEE 802.11 Wireless LAN (WLAN) [1] technology matures, large scale deployment of WLAN networks is highlighting certain technical challenges such as management, monitoring and control of large number of Access Points (APs). Distributing and maintaining a consistent configuration throughout the entire set of APs in the WLAN is a difficult task. The shared and dynamic nature of the wireless medium also demands effective coordination among the APs to minimize radio interference and maximize network performance. Network security issues, which have always been a concern in WLAN's, present even more challenges in large deployments and new architectures.

To address above mentioned problems centralized IEEE 802.11 WLAN architectures have been emerged: simple APs are managed by an Access Controller (AC). There is an open protocol to AC-AP communication called CAPWAP [2, 4]. Such controller-based WLAN networks have a lot benefits like seamless roaming, but they have some overheads that can be eliminated by integrating Access Controller with SDN/OpenFlow controller [3].

In this paper we present Chandelle system that allows to faster roaming procedure even more taking benefits of integration WLAN solutions with SDN/OpenFlow networks.

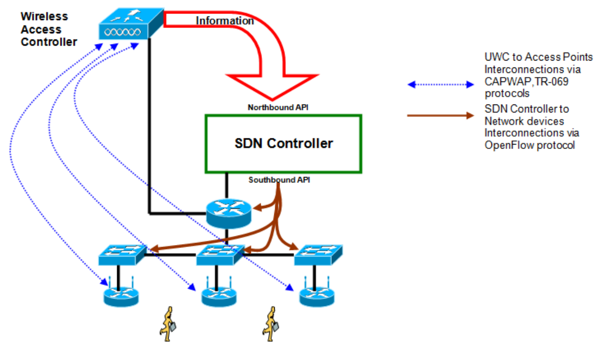

Figure 1: The basic scheme of integrating CAPWAP wireless controller with SDN/OpenFlow controller.

2 Proposed approach

In traditional solutions, once the AP understands the client signal is weak, it sends CAPWAP Controller notification that the client is leaving the area. CAPWAP Controller sends to the client recommendation of new AP right after it is selected. When the client connects to the new AP, the AP sends notification to the CAPWAP controller which checks client's credentials and responses to the AP with an authorization keys. Then AP initializes four-handshake protocol which establishes connection with the new AP. On that stage roaming is done and user is able to send packets.

Despite the fact everything is done already, traditional networks is not ready for roaming. At this moment switches still have old rules and reconfiguration takes time and brings additional delays for the client. SDN/OpenFlow networks are able to cover this drawback (see Figure 3) as network prepare work can be started at the moment of connection finalization between client and new AP. In such case CAPWAP controller tells the SDN/OpenFlow controller about the client migration and necessity to push new flows to the switches.

Figure 2 explains the same procedure with a router be-

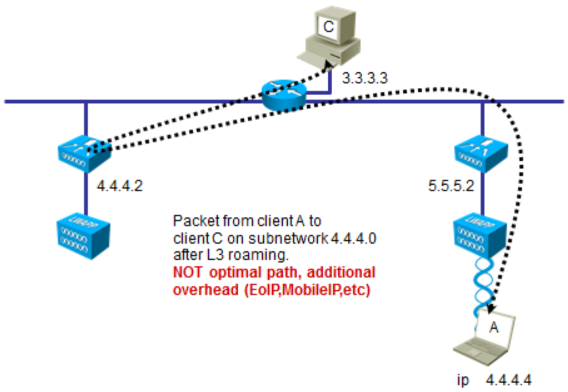

Figure 2: Motivation example: the client is migrating to AP resided in other subnet than the old AP.

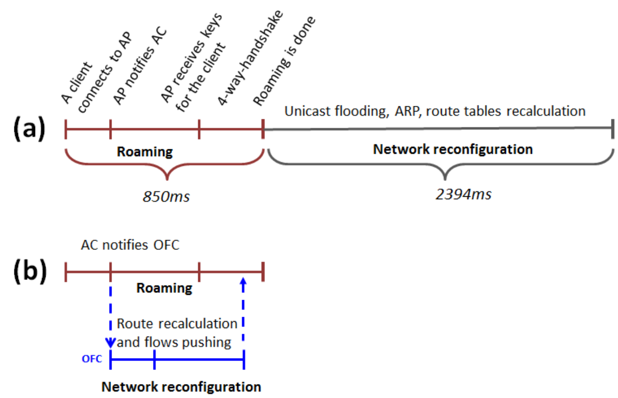

Figure 3: The roaming timelines with (a) traditional networks and (b) SDN/OpenFlow networks.

tween APs and the new AP which belongs to other subnet than the old AP. The new AP encapsulates each packet from the client using any Ethernet over IP (EoIP) techniques to send it through the tunnel to the old AP, where the packet is forwarded according to the old rules. This significantly decreases network communication characteristics for the migrated client such as delay and bandwidth. Moreover a tunneling requires additional CPU resources at an AP. In SDN/OpenFlow, a router does not exist as a separate device. In contrast, there are OpenFlow switches supporting L1-L4 addressing that can be configured by the SDN/OpenFlow controller. Such solution allows to send the client's packets directly to the destination without packets hooking on the old AP. We have to forget about this complex roaming Chandelle stunt[1].

The other interesting example to consider is wireless clients access control. The examples of restrictions that access control can provide can be formulated as following: "guests have only access to the Internet", "the interns have access to the Internet and to a mail server", etc. In tradition WLAN, APs must check all of ACL rules that leads to significantly increasing cost of APs. In SDN/OpenFlow, these ACL rules can be verified in the border OpenFlow switches that dynamically configured from the SDN/OpenFlow controller. Thus, an AP might be less powerful and less expensive. We use AP that 10 cheaper than vendors' solutions.

3 Evaluation

We have implemented our approach in the ARCCN Universal Wireless Controller (UWC) integrated with ARCCN OpenFlow Controller (OFC). The controllers communicate with each other through queue based northbound API. The UWC notifies OFC about client migration and tells new ACL rules applied to appropriate client. The OFC knows all previous routes for a client and seamlessly rewrites them for the new AP.

The testbed for our evaluation consists of a single client, two APs on the same subnet (TP-LINK), three hardware OpenFlow switches (NEC) in one line and the server that runs both controllers. The switches work in hybrid mode in order to evaluate both cases: legacy and OpenFlow networks. In all experiments, we measure the network congestion time right after the roaming. The client runs ping utility with request timeout equal to 100ms.

Our results show that the legacy network needs in average 2.394 seconds to reconfigure, while the SDN/OpenFlow network doesn't bring additional delay. This is because the migration in UWC requires 850ms and the OFC has enough time to reconfigure the switches. Finally, we have got 70% faster roaming with SDN/OpenFlow!

[1] Chandelle is a steep climbing turn executed in an aircraft to gain height while changing the direction of flight. Widely use in air fights.

References

[1] IEEE 802.11-2012, http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[2] IETF CAPWAP Architecture, http://tools.ietf.org/html/draft-ietf-capwap-arch

[3] M. Casado, T. Koponen, D. Moon, S. Shenker, *Rethinking Packet Forwarding Hardware*. In Proc. of HotNets, 2008

[4] L. Suresh , J. Schulz-Zander, R. Merz, A. Feldmann, T. Vazao, *Towards programmable enterprise WLANS with Odin*, Proceedings of the SIGCOMM HotSDN, August 13-13, 2012, Helsinki, Finland