Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 94 (2016) 497 – 501

Procedia Computer Science

International Workshop on Applications of Software-Defined Networking in Cloud Computing (SDNCC)

MAC Based Dynamic VLAN Tagging with OpenFlow for WLAN Access Networks

Marc Koerner[a], Odej Kao[a]

[a]*Technische Universitaet Berlin, Einsteinufer 17, 10587 Berlin, Germany*

Abstract

Many network device vendors are providing a vendor specific VLAN based access solutions for WLAN clients. This applications allows network operators to specify WLAN devices which automatically fall into their department specific networks ans allows them to access their local resources like e.g. printers. The configuration of these VLAN mappings is usually manufacturer specific and depends also on the local VLAN policies. However, the presented OpenFlow approach on the other hand presents a solution to encapsulate this functionality as network application. Thus, an architecture, implementation, and evaluation is presented in order to demonstrate that this particular functionality can be easily realized in an OpenFlow network application.

Keywords: Software Defined Networking; OpenFlow; VLAN tagging

1. Introduction

Software-defined networking (SDN)[1] is continuously evolving nowadays networks and network applications. Researchers and network operators are focused on integrating traditional network solutions on this innovative technology. One of the main challenges are applications for productive environments, so vendors are more and more promoting SDN applications and products for enterprise networks. SDN provides a basic opportunity to evolve these networks in general, since all packets are now processed by a centralized management entity. This mechanism provides the opportunity for several new network applications covering all network management functions from a loop free path deployment up to the virtual local area network (VLAN) separation.

VLANs are an useful tool to fragment a network into different segments and reduce the size of a broadcast domain. Moreover, they are an opportunity to enforce security and control client access within the network. Usually the network operation control (NOC) department in a company or university is using this to segregate the different departments. Moreover, an additional MAC to VLAN mapping mechanism is utilized in order to embed mobile clients

* Corresponding author. Tel.: +49-30-314-78583; fax: +49-30-314-21060.
E-mail address: marc.koerner@tu-berlin.de

doi:10.1016/j.procs.2016.08.077

into their department network independently where the access the WLAN infrastructure. Therefor usually the NOC operator just adds the mapping information to authentication, authorization and accounting (AAA) system. Thus, if a known user connects his traffic will be VLAN tagged and routed within the network into his associated department network.

The remaining paper is structured as follows. Section 2 explains the background of this work. In sec. 3 is briefly explained how the proposed MAC to VLAN mapping concept is used and how it is working. In contrast, in sec. 5 a detialed evaluation based on Mininet is presented. Finally, in sec. 6 the concept and evaluation is concluded.

2. Background

The SDN paradigm offers by default a separation of the control- and data-plane for packet forwarding elements. It builds a logical separation between the packet forwarding hardware and the control logic. The concept further extends this control approach by introducing a centralized control entity called controller or network operating system (NOS). It follows a similar approach like the host based operating systems, where the business logic runs on top. This is an excellent opportunity to encapsulate all network functionalities in virtual network functions (NFV).

MAC-based dynamic VLAN tagging is a procedure where the switch usually detects the VLAN affiliation of a host which gets connected to one of its ports. The VLAN affiliation is detected based on the hosts MAC address. Cisco implementation uses a mechanism called VLAN Membership policy Server (VMPS). This is basically a database which stores the MAC / VLAN mapping information entered by the NOC operator. If a new device is connected to a switch port of the access network switches, the regarding switch queries the VMPS for the concerning MAC address of the new host. Thus, the VMPS browses its database using the obtained MAC address for the corresponding VLAN ID. Afterwards the switch adapt its internal port configuration according the new VLAN assignment. This flexibility makes dynamic VLAN the ideal solution for networks whose composition often changed[2] .

3. Architecture

As introduced in the previous section, there exist proprietary hardware solution which provide dynamic VLAN tagging. However, in the remaining paper an open source solution is introduced providing the same features on community OpenFlow[3,4] hardware.

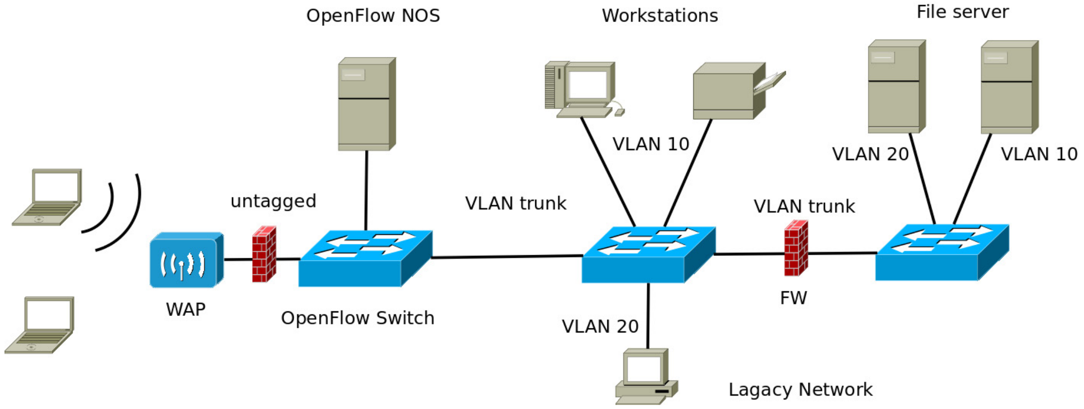

Fig. 1. Typicall campus network department based use-case

Figure 1 illustrates the proposed OpenFlow based solution for a typical campus network. It shows a network basically composed out of two legacy switches and OpenFlow switch behind an wireless access point (WAP). This is a typical SDN-legacy hybrid network. The legacy switches use port-based VLANs to separate workstations, printers and file servers on a department level. These devices do not change frequently and have a fixed VLAN mapping. In contrast to the mobile systems, such as laptops. These systems change often their locations within the university area.