Chapter 10
Software-Defined Networking (SDN): An Emerging Technology

L. Naga Durgaprasad Reddy
Sri Yerramilli Narayanamurthy College, India

ABSTRACT

This chapter researches in the area of software-defined networking. Software-defined networking was developed in an attempt to simplify networking and make it more secure. By separating the control plane (the controller)—which decides where packets are sent—from the data plane (the physical network)—which forwards traffic to its destination—the creators of SDN hoped to achieve scalability and agility in network management. The application layer (virtual services) is also separate. SDN increasingly uses elastic cloud architectures and dynamic resource allocation to achieve its infrastructure goals.

I. INTRODUCTION

In the early days of basic Internet protocols development no native support for access control was provided at the network level. It was expected that applications would connect to each other in the global network without any restrictions. Along with the growth of commercial use of Internet mechanisms for L3 (and higher) network access control became necessary for normal operations, and packet filtering solutions were developed (including software implementations in operating systems) — firewalls, Intrusion Prevention Systems (IPS), network anti viruses (V. Yazici, M. O. et.al, 2014).

DOI: 10.4018/978-1-5225-9493-2.ch010

In terms of client devices mobility, network configuration is changing rapidly and the information about network topology changes could not be used directly for access control. That is why the problem of network access control based on the information about the expected behavior (flows) of network applications is becoming more and more important.

SDN is a step in the evolution towards programmable and active networking and allows network administrators to have programmable central control over the entire network.

II. SOFTWARE DEFINED NETWORKING

Software-defined networking (SDN) is a new emerging technology for networking in which control is Decoupled a hardware and given to software part called a controller[1]. When a packet arrives at a switch in a foreseeable network rule built into the switch patented firmware tell the switch where to forward the packet. The switch sends every packet going to the same destination along the same path and treats all the packets the exact same way. In the campus network, smart switches designed with application-specific integrated circuits (ASICs) are Refined enough to recognize different types of packets and treat them differently, but such switches can be quite expensive (H. Kim and N. Feamster,2013).

The aim of SDN is to allow network administrators respond quickly to changing to the requirements. In a software-defined network, a network administrator can shape traffic from a centralized control software without having to touch individual switch. The administrator can change any network switch rules when necessary ordering, de-ordering or even blocking specific types of packets with a very level gritty of control (M, Algarni, 2013). Currently, the most popular specification for creating a software-defined network is an open standard called Open Flow. Open Flow lets network administrators remotely control routing tables.

A . *Open Flow Switches*

Open Flow provides an open protocol to program the flow table in different switches and routers. A network administrator can partition traffic into production and research fellows. Researchers can control their own flows by choosing the routes their packets follow and the processing they receive. In this way, researchers can try new routing protocols, security models, addressing schemes, and even alternatives to IP. On the same network, the production traffic is isolated and processed in the same way as today. The data path of an Open Flow Switch consists of a Flow Table, and an action associated with each flow entry. The set of actions supported by an Open