THE AMERICAN UNIVERSITY IN CAIRO

SCIENCES AND ENGINEERING

Seamless Mobility in IoT World using Software Defined Networks

A DISSERTATION SUBMITTED TO

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR
THE DEGREE OF

DOCTOR OF PHILOSOPHY

BY

WALAA FAROUK ELSADEK

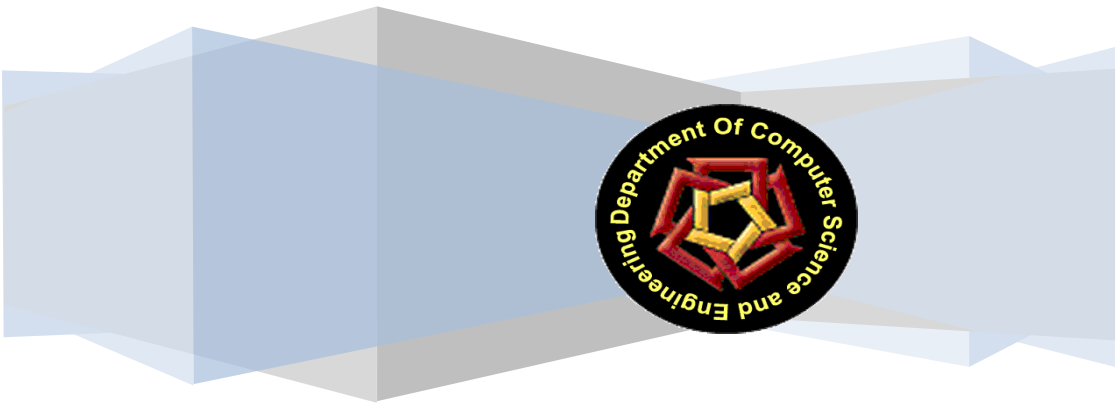
walaa.farouk@aucegypt.edu

UNDER SUPERVISION OF

PROF. MIKHAIL N. MIKHAIL

mikhail@aucegypt.edu

2/2017



ABSTRACT

ABSTRACT–Existing mobility protocols adopt centralized gateways to provide session continuity for mobile users. The centralized nature and the absence of effective selective traffic offload mechanism lead to inefficient data forwarding plane problem that congests 4G Evolved Packet Core (EPC). Despite the endless efforts of 3GPP, IETF, vendors, and researchers, these problems persist and restrict operators' offering for residential/enterprise indoor services and session continuity in wide area motion as train or cars crossing cities' boundaries. Existing mobility protocols, that struggle when connecting mobile users to static locations, can never satisfy the requirements of Internet of Things (IoT) for real time collaborative interactions between moving users and terminals attached to 5G edges as drones, robots, smart vehicles …etc. New mobility paradigm becomes a key enabler for collaborative interactions in IoT real time cognitive services as self-driving car, drones, remote health monitoring, smart homes/offices/farms …etc.

The research provides a novel mobility framework based on Software Defined Network (SDN) to solve existing mobility problems, satisfy IoT collaborative interactions, and extend mobility coverage cross service providers under Service Level Agreements (SLAs) while ensuring the security of involved entities. Mobility is achieved through dynamic establishment of SDN overlay network that can cross any type of LAN/WAN/Cellular topology. The framework is fully aligned to Next Generation Network (NGN) where mobility is offered as a service and provides smooth integration to existing infrastructure. The mobility scope incorporates both intra-domain and inter-domain mobility. The former refers to mobility within a single SDN administrative domain while the later refers to that between multiple SDN domains.

Intra-domain mobility scope targets existing mobility challenges as core network congestion problem, unified access in campus and enterprise for wireless/wired networks, and session continuity in standard and wide area motion for 3G/4G/5G mobile operators. Inter-domain mobility scope addresses three main challenges. The first is extension of indoor services for residential/enterprise using any type of communication as DSL/cable without enforcing Distributed Antenna System (DAS) or any small cell setup while ensuring the security of involved entities. The second is extending WiFi mobility cross enterprises with optimized usage of communicating WAN links while ensuring unified access to both wireless and wired networks regardless of overlapping configurations as IP subnets/VLAN that can exist in their intranets. The third is facilitating collaborative communication between static/moving users, servers, and terminals when joining from different carriers under Service Level Agreements (SLA).

Keywords—IoT; Mobility; MIP; LIPA; SIPTO; SLA; Collaborative interactions; Wide Area Motion.

ACKNOWLEDGMENT

First and foremost, my deepest gratitude and thanks are to **GOD**, the most beneficent and merciful for granting me the power to proceed and accomplish this work, regardless the limited resources available in Egypt to prototype technologies as those adopted in 5G next generation networks.

This dissertation is dedicated to the soul of **my beloved mother; Prof. Laila Fathalla.** May God forgive her, grant her peace, and admit her to the highest ranks in Paradise. I will forever be indebted to her. Thank for her selfless and endless love. She has been the main motivator for me to complete my postgraduate studies. No word can describe what she has done for me. My deepest gratitude to **my sister; Dr. Lamyaa Farouk,** for her patience and encouragement while spending endless hours in experimenting and completing my writing up.

It is an honor for me to work my PhD research under supervision of **Prof. Mikhail N. Mikhail**. I take the chance to show him my sincerest gratitude. His encouragement, guidance, and support throughout my research enabled me to develop a deep understanding of the subject. This research would not have been possible without his patience and knowledge. He has made his support available all the time while granting me a room to express my ideas and thoughts. His experience and analysis for my ideas are the key factors for developing the proposed architecture with such practical and structural vision. One simply could not wish for a better or friendlier supervisor.

I am indebted to **Prof. Amr El-Kadi** and **Prof. Sherif El-Kassas**. Their lectures in "Distributed Systems" facilitate for me the designing of such scalable architecture. Their comments during the proposal of this research definitely supported me to highlights the strength of my contributions when comparing my results to existing mobility standards.

Lastly, I would like to thank both PhD and Computer Science and Engineering departments in American University for providing me the support during my research period. Special thanks to the program director **Prof. Mohamed Moustafa**. His continuous advices and follow up have helped me to proceed faster in my research. Also, I offer my regards and thanks to all who supported me in any respect during my research completion.

Walaa Farouk

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 OVERVIEW

Technology evolution becomes the igniting factor behind knowledge-based economy [1]. Business sustainability is the vision of the next Internet of Thing (IoT) era that capitalizes on full interconnected societies. The 5G core will communicate person, servers, and smart terminals; as vehicles, robots, drones …etc. to fulfill different tasks in series of novel real time services as assisted farmers' actions, smart homes monitoring, long-distance medical surgery …etc. Next Generation Network (NGN) promises improved performance in terms of reduced latency, increased reliability and throughput under higher mobility and connectivity density through unified programmable infrastructure for both Telecom and IT [2]. Cloud/Edge Computing, Software Defined Network (SDN), and Network Function Virtualization (NFV) are the vital tools behind such transformational shift to cover existing infrastructure gaps [3].

The Open Networking Foundation (ONF) presents SDN as transforming networking architecture that decouples the logically centralized control plane, providing the network intelligence from the data plane, controlling the underlying network infrastructure. OpenFlow protocol is key enabler for SDN and the first standard SDN protocol to facilitate relay of information and packets between both control and forwarding planes [4]. OpenFlow SDN-based technology flexibility as well as ONF's initiative for building SDN-enabled LTE potentiate researchers toward inventing new network-based mobility management solutions to overcome existing protocols limitations that hinder seamless mobility and continuous connectivity to real time applications and services in the hyper interconnected IoT world [5].

1.2 MOBILITY EVOLUTION

Conventional networks were regarded as high speed infrastructure connecting users to data centers and corporate networks where services were located. Routing was solely based on fast data transfer between fixed locations mapped to IP subnets without any dynamic adaptation to moveable objects. Initially, the scope was limited to fast lookup process by matching destination IP against the routing table for instant next hop retrieval toward a static location. With the wide spreading of internet, more users get connected to World Wide Web (WWW), social, business, education, multimedia applications. Standard networks and routing mechanisms were not capable to accommodate more simultaneous users as of running out of IPv4 address. The situation enforced designing of IPv6 and the development new mechanisms as Network Address Translation (NAT) stated in RFC 2663 to solve this gap

[6]. Later, evolved network security threats increased communication complexities with wide deployments of firewalls and Intrusion Detection System (IDS). The consequences of such advancements limit direct connectivity except to servers and critical applications using firewalls for mapping their private IP addresses to the scarce public IP addresses. Users, lying behind the firewall inside zone, can initiate connections to public accessible servers without themselves being accessible from outside. Later, the rising needs for intranet and corporate services was the key behind the development of Virtual Private Networks (VPN) to facilitate direct connections from roaming employees to their home corporate services located behind the firewall and not public accessible. VPN deployments were an efficient solution for static remote users. Unluckily, mobile users suffer from continuous tunnels termination due to the change of leased IP addresses during motion. Moreover, VPN users suffer from fast battery drainage due to the high battery consumption associated with encryption. In sum, historical evolution of conventional networks design was directed to fast communication of static entities without any mobility consideration.

In 2002, discussions about user's mobility started as an initiative for enabling mobile user to keep the same IP address when traveling to different networks for ensuring continuous connectivity as stated in RFC 3344 [7]. Advancements in wireless technologies attract the focus of researchers to use Mobile IP (MIP) concept to guarantee session continuity regardless of multiple Access Points (APs) handover during motion. Both hardware vendors and Internet Engineering Task Force (IETF) devoted enormous effort in this scope till the development of Proxy Mobile IPv6 (PMIPv6) by 2008 and the updated version PMIPv4 to support IPv4 by 2010 as stated in RFCs 5213 and 5844 respectively [8][9]. Since then, PMIP becomes the widely-adopted concept in 4G Long Term Evolution (LTE) to guarantee session continuity during motion and for extending residential/enterprises indoor services referred to as LIPA (Local IP Access). For enterprise and campus access with a single administrative domain, Control and Provisioning of Wireless Access Points (CAPWAP) protocol is the proposed IEFT standard in Wireless LAN Controllers (WLCs) for centralized management of multiple APs and unified access in wired/wireless network as stated in RFC 5415 and RFC 5416 [10][11]. Unluckily both protocols struggle in real deployments as of their centralized gateways/proxies' architectures and absence of effective Selected Internet IP Traffic Offload (SIPTO) mechanism. The consequences are inefficient forwarding data plane and core network congestion. These problems limit operators' offering for LIPA service and session continuity in wide area motion [12]. Moreover, absence of feasible solution for inter-domain mobility, forces expensive hybrid mode deployments of CAPWAP and PMIP without regarding involved entities' security policies [13]. These problems are discussed in section 1.3 that analyzes existing protocols challenges.

2015 IDG Enterprise survey for "Building the Mobile Enterprise" highlights the extent to which mobility becomes a driving factor toward business prosperity. The survey reveals that 64% of organizations regard mobile as a critical tool potentiating fast decisions, facilitating internal communications, and enhancing customers' retention policy while 49% intend leveraging their Wi-Fi networks to handle more devices. Internal networks' reliability is lower in priority while the major aspect attracting 63% of enterprises and 48% of small and medium-sized business (SMB) is communication security. Intranet services become less important as employees use their smart phones to carry most of data services with the rise of COPE (Corporate Owned, Personally Enabled) and BYOD (Bring Your Own Device) policies. Thus, Wi-Fi provider's role becomes limited to internet access with continuous services migration to private clouds [14]. For maximum benefit of unlicensed spectrum and lower cost delivery of Wi-Fi services, a new framework is required to enhance poor coverage and capacity indoors while extending IoT smart Residential/Enterprise services cross outdoor hotspots for continuous accessibility and mobility without violating customers' security. Furthermore, this need is potentiated with rapid progress in IoT and urgent needs for advances cognitive capabilities through terminals moving in the globe as robots, drones …etc. Strong advancement in mobility paradigm becomes a must to support collaborate communications between moving terminals as existing protocols design principles can hardly fulfill legacy requirements for communicating moving users to static servers not moving to moving objects [1].

1.3 CHALLENGES IN EXISTING PROTOCOLS

1.3.1 CAPWAP ENTERPRISE DEPLOYMENTS' CHALLENGES

Control and Provisioning of Wireless Access Points is proposed IEFT standard, as stated in RFC 5415, in Wireless LAN Controller (WLC) for centralized management of multiple APs [10]. CAPWAP is evolution to LWAPP (Lightweight Access Point Protocol) through the introduction of full Datagram Transport Layer Security (DTLS) tunnel. The adoption of generic encapsulation and transport mechanism for pushing configuration and management information to APs makes it radio technology independent [10]. IEEE 802.11 bindings stated in RFC 5416 facilitate unified access for wireless/wired networks [11].

CAPWAP provides a method for VLAN extension on single WLC or cluster of WLCs to provide unified access between enterprise and connected branches. Using single administrative entity for managing both enterprise and connected branches is referred to as intra-domain mobility. WLC's VLANs configurations can be manually or dynamically created by AAA (Authentication, Accounting, and Authorization) server. For WAN links connecting enterprise and branches, CAPWAP uses standard VLAN

trunks or static GRE to bridge packets between connected locations without any Selected IP Traffic Offload (SIPTO) mechanism for optimizing usage of scarce WAN bandwidth. Moreover, no inter-domain mobility solution is provided by CAPWAP to provide indoor service extension for enterprise/residential, Local IP Access (LIPA) service, either through WiFi service providers or cross smart cities operators or between enterprise and branches as VLAN/GRE tunnels must be preconfigured on WAN backbone of the connected locations. Inefficient bandwidth utilization, static nature, and lack of inter-domain mobility limit CAPWAP deployments to campus and single enterprise location.

1.3.2 LTE LIPA PMIP CHALLENGES

Proxy Mobile IPv6 and IPv4 are IETF standards protocol for network-based mobility management that enables motion of Mobile Nodes (MNs) without changing their IP addresses [8][9]. Mobile IP functions are carried through network without MNs' awareness. MN can be an IPv4-only node, an IPv6-only node, or a dual-stack node. Mobile Access Gateway (MAG) is first-hop router in localized mobility management that transparently intercepts MN's communication to home agent referred to as Local Mobility Anchor (LMA) [8]. Either default LMA is stated in MAG's configuration or LMA IP address and other MN's configurations are downloaded from AAA server after authentication as in IETF RFC 5799 [15]. LMA either allocates MN's IP address or notifies MAG to relay IP allocation messages to an external DHCP server based on IETF RFC 5844 [9]. MN maintains the same IP for session continuity regardless changing the attached AP or group of APs managed by the same MAG as long tunnel is terminated by single LMA. Tunnel between LMA and MAG is shared by multiple MNs. This can either be GRE or IP-in-IP tunnel. The following paragraphs state the main challenges facing PMIP mobility solution.

1.3.2.1 EVOLVED PACKET CORE (EPC) CONGESTION PROBLEM

1.3.2.1.1 LIMONET Problem

4G LTE mobility solution within a geographical location, like city, is through a centralized gateway, called Packet Gateway (P-GW), to which all MNs' packets are directed. This gateway acts as PMIP LMA that carries IP addresses allocation responsibility and is the sole exit to internet connectivity and residential/enterprise services provided within a geographical location. In residential/enterprise IP mobility, MN is registered with a predefined private IP addresses assigned from nearest P-GW to registration location [16]. PMIP traffic classification capabilities are very basic thus most MN's packets are tunneled to home network or to initial point of attachment regardless being the shortest path to internet or not as in figure 1-1.

Several researches tried to optimize PMIP operation through the introduction of several internet breakout points to offload core network while providing indoor services extension. Such investigation is referred to by LIMONET; Local IP Access (LIPA) Mobility and SIPTO (Selected Internet IP Traffic Offload). 3GPP Releases from 9 to 12 proposes several offloading mechanisms but LTE still suffers from inefficient data forwarding due to L3 routing complexities that enforce traffic routing to centralized P-GW or TCP redirection to centralized proxy server as proposed by Multipath TCP (MPTCP) for session continuity [12][17][18][19][20][21]. Despite these efforts, existing offloading techniques are hindered by absence of an accurate runtime traffic classification mechanism to filter only active TCP sessions. Offered solutions put operators in a tie for either ensuring session continuity or making efficient usage of their core networks. These problems limit the advantages of PMIP for SIPTO over previously adopted protocol as Layer Two Tunneling Protocol (L2TP) and Static GPRS Tunneling Protocol (GRE).

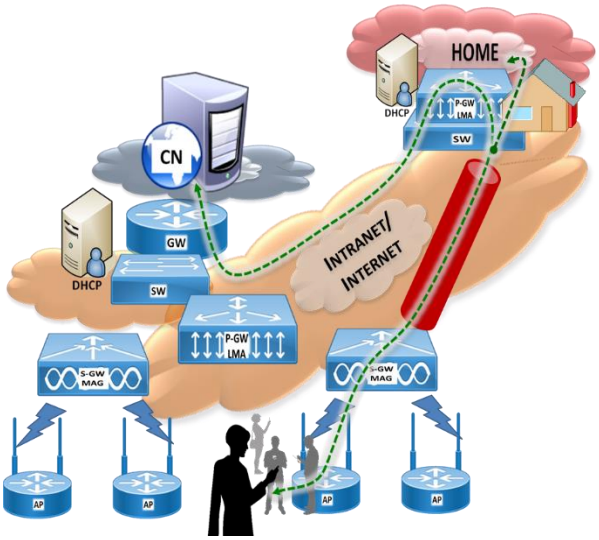


Figure 1-1: Inefficient Data Forwarding

1.3.2.1.2 Wide Area Motion PMIP Challenges

In wide area motion, MN, located inside train/vehicles while crossing cities' boundaries, undergoes handover between two PMIP P-GWs. The second crossed P-GW will allocate MN a different IP than previous P-GW. This IP will be mapped to a different Public IP for internet access. This means that all MN's active sessions will be disconnected when leasing a new IP address. To overcome this problem, after MN's re-authentication and during handover, Home Subscriber Server (HSS) instructs Serving Gateway (S-GW), acting as MAG, to tunnel

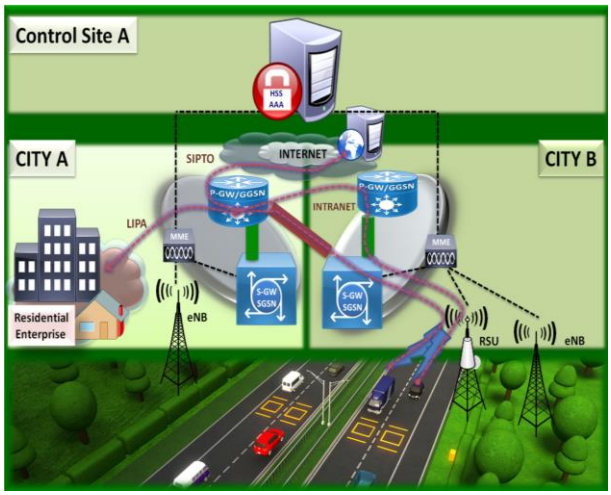


Figure 1-2: Wide Area Motion Challenge

all MN's packets to P-GW of previous location for ensuring session continuity regardless of path optimality or core congestion [22]. This problem is highlighted in figure 1-2.

1.3.2.2 SEVERAL TUNNELS REQUIREMENTS

PMIP has two main modes of deployments; Flat Domain Model and Domain Chaining Model. In Flat Domain Model, MAG tunnels MN's packets to LMA home IP address or domain name. The major drawback of this approach is that every office/home registered for residential/enterprise service must state a Public IP address or a known Private IP address to which LTE/WiFi service provider can terminate the tunnel. This solution is almost inapplicable and violates the security of involved enterprises. Domain Chaining Model adopts a hierarchical deployment of Flat Domain Model. Foreign MAG tunnels MN's packets to local LMA. The session chaining mode transfers local LMA to a MAG that tunnels MN's packets to home LMA. Then, home LMA performs another session chaining to tunnel MN's packets to office/home registered LMA. This means that at least three tunnels are created for full inter-domain mobility. PMIP Domain Chaining solution adoption in real environment induces severe latency associated with several tunnels establishments.

To avoid multiple tunnel establishment/termination to a known domain name or a private/public IPs, LTE introduces a small cell setup to allow service providers to extend service coverage indoors or at cell edge; Femtocells, picocells, and macrocells. LIPA mobility service offering is limited to residential/enterprise IP networks with valid indoor femtocells and picocells, while SIPTO is for internet access for those with femtocell and macrocell setups [12]. Later, WiFi provider small cell was introduced for providing hybrid mode solution between CAPWAP and PMIP to terminate tunnels at customer's WiFi AP managed remotely by CAPWAP WLC [23]. Small cell solution provides an instant applicability for LIPA service but reveals internal structure of residential/enterprise IP network. Enterprises with different administrative domains want to maintain their internal structures' security. Moreover, these cells have strong limitations on the number of LIPA services offered, thus full LTE inter-domain mobility cross enterprises is extremely expensive if not impossible.

1.3.2.3 WIFI PROVIDER/ENTERPRISE LIPA PMIP CHALLENGES

WiFi deployments in provider/enterprise using inter-domain PMIP for offering LIPA mobility are far more complicated than LTE's SIPTO and security problems. Wide area coverage and small cell setups provided in LTE minimized complications of several tunnels requirements in domain chaining model. This problem is hardly avoided in inter-domain mobility deployments cross WiFi provider/enterprise. Even

CAPWAP WiFi small cell suffers from inefficient bandwidth utilization. Moreover, non-LTE WiFi provider and enterprise deployments lack a unique indexed identifier as International Mobile Subscriber Identity (IMSI) provided in cellular network that facilitates instant authentication and retrieval of MN's subscription profile during both join and handover phases. These challenges hindered PMIP LIPA service offering even the IETF proposed internet draft for PMIP applicability in service provider WiFi deployments expired without standardization [23][24].

1.3.3 IEEE 802.11-BASED V2X TECHNOLOGY CHALLENGES

IEEE 802.11p is an approved enhancement to IEEE 802.11 standard for supporting Wireless Access in Vehicular Environments (WAVE) in Intelligent Transportation Systems (ITS) applications for Dedicated Short-Range Communications (DSRC). IEEE 802.11p communication technology is developed for instant exchange of object information in collaborative communication as information exchange with other vehicles (V2V), with roadside infrastructure (V2I), with Internet (V2N), and with Pedestrian (V2P) through a short-range ad hoc broadcast system. As vehicles advance toward higher automation levels, IEEE 802.11p becomes inefficient to solely support exchange of sensor data for collective perception, control information for platoons from very close driving vehicles, and vehicle trajectories to prevent collisions. These types of cooperative information require higher bandwidth and improved reliability. Thus, cellular network attracts the attention of being complementary or full replacement of IEEE 802.11p in Vehicle-to-Everything (V2X) [25]. IEEE 802.11p proved high availability as of not relying on network infrastructure except for security management and Internet access. The fully distributed architecture doesn't pose any traffic bottleneck or single points of failure, as in infrastructure-based LTE. This redirects the attention again to reconsider LTE challenges that hinder seamless mobility and decrease service reliability as centralized PMIP design, session continuity, and EPC core congestion problems.

1.4 RESEARCH OUTLINES

This research is organized as follows; Chapter 2 highlights the motivations behind this research, the problem statement, and the proposed OpenFlow SDN-based mobility solution. To ensure the feasibility of the research; the sets of evaluation methods and validation criteria are stated, as well as, the adopted performance metrics for comparing the obtained results of mobility setup and handover delays.

Chapter 3 states the literature review describing the historical evolution of mobility, 4G adopted mobility protocols, the effect of tunnels, VLAN, and MPLS overheads on performance of existing protocols. This chapter highlights SDN principles, motivation for adopting OpenFlow SDN based mobility, and major works related to this research.

Chapter 4 illustrates the proposed mobility framework scope, key entities in the distributed framework architecture, internal operation and interactions, phases of mobility service activation and handover, and physical layout of how the framework is integrated to existing and NGN infrastructure.

Chapter 5 describes the logic behind the mobility framework operation through high indexed database of profiles and tables controlling the operation of core functional modules and procedures presented in five layers model. Each layer in the presented model is described in detail to show how MN is detected in foreign network till the service is activated.

Chapter 6 describes in detail the structure of the established prototype that ensures the feasibility of the proposed mobility framework. Several real-time experiments are conducted to prototype mobility inside Radio Access Network (RAN) including mobility setup, intra-overlay, and inter-overlay handovers delays. Results are compared to those published by Cisco PMIP while performance is matched against Software Defined Wireless Network (SDWN) experimented results. The rest of experiments analyze in detail all delays and latency affecting mobility setup and performance cross carriers with direct mobility SLA and those with indirect SLA through transient carrier.

Chapter 7 provides summary of the research and the experimental results obtained from prototyping the proposed framework. Then, the section highlights major contributions that can be achieved from real deployment of the proposed SDN mobility framework. Future research directions are also stated.

2 MOTIVATIONS, PROBLEM STATEMENT, PROPOSED SOLUTION, AND VALIDATION

This chapter illustrates the motivating factors behind developing a new mobility paradigm, states the problem statement of this research, outlines the proposed OpenFlow SDN-based solution using a physical prototype for analyzing motion cross enterprises, then states the evaluation plan for validating the feasibility of the proposed mobility framework.

2.1 MOTIVATIONS FOR NEW MOBILITY PARADIGM

2.1.1 INTER-DOMAIN MOBILITY

For enhanced coverage and high availability, a uniform mobility framework is required to minimize the extremely tough negotiations advancing the establishment of mobility Service Level Agreements (SLAs) across operators/carriers. The framework must be seamless integrated to existing billing mechanisms while preserving the security of competing entities administrating different domains. SLAs facilitate orchestration between activated on-demand service in visited network and home network [26].

2.1.2 VEHICLE-TO- EVERYTHING

In IoT era, smart vehicles are regarded as hubs for interconnected services. In addition to V2V, V2I, V2N, V2V …etc. more services will evolve in V2X communication that require lower latency, higher bandwidth, and improved reliability. These services include the exchange of sensor data for collective perception and collisions prevention, the interaction with backend server providing services as pay as you drive and predictive maintenance, the indoor service extension including LIPA mobility and remote health monitoring. The current adopted IEEE 802.11-based vehicle technology is designed for instant exchange of object information in collaborative communication but inefficient to solely support V2X communication. The development of LTE Proximity Services (ProSe) as ProSe Direct Discovery, ProSe Direct Communication and ProSe UE-to-Network Relay increases 3GPP Radio Access Network (RAN) focus on enhancing LTE as in release 13 and 14 (beginning of 5G) to fulfill V2X requirements for licensed/unlicensed spectrum. Setting a Mobile Virtual Network Operators (MVNOs) with new mobility framework is an attractive idea to ensure service continuity and to guarantee QoS in V2X communication [25].

2.1.3 BIG DATA SWITCHING

Consider the enormous loss in Operational Expenditure (OPEX) costs associated with Virtual Machines (VMs) migration in NFV data centers due to lack of efficient methodology solving this problem either live or offline. VMs mobility dilemma arises from the complications of hierarchical layer 3 routing

protocols trying to find destinations that are mapped to logical subnets with no significant meaning or mapping to geographically location or revealing the nature of applications and the service offered. In offline migration, gigantic efforts and non-evitable time are lost in modifying embedded IP addresses in various configuration files. For online migration, there is almost non-feasible solution provided till now [27]. The proposed mobility architecture represents effective and efficient solution to instant migration problem either live or offline without any change in network configurations.

2.1.4 New Mobility Paradigm for 4G LTE and 5G

In the context of mobile and wireless networks, recent progresses in SDN/NFV promote network redesign, development of new operation methods, and invention of customized services using the provided Open Application Program Interface (API). The ONF initiatives to build an SDN-enabled LTE potentiate researchers to overcome existing infrastructure's limitations that hinder direct communication between mobile users and smart objects. Traffic steering and path management researches target the core network congestion problem induced by the centralized design of existing mobility protocol. Network based mobility management, efficient bandwidth utilization, mobile traffic offloading, scalable indoor service extension, and seamless handover even in challenging wide area motion as train or vehicle crossing cities' boundaries become milestones on the path toward uninterruptable experience while streaming multimedia, extending indoor services, and communicating with real time IoT applications [5].

2.1.5 Robotic Clouds

5G core networks will soon represent the IoT backbone with robots, self-driving vehicles, Autonomous Machines (AM), Artificial Intelligence (AI) interfaces and drones/Unmanned Aerial Vehicles (UAV) as terminals. Cloud/Edge Computing, Network Functions Virtualization (NFV), and Software-Defined networking (SDN) technologies are tools to increase core network flexibility for instant computing resources allocation through IT virtualization and SDN programmatic enabled core and access networks [1]. Development of sophisticated cognitive capabilities through advanced terminals attached at 5G infrastructure edges is an urgent need for cost reduction, process automation, as well as developments of future services and application for the sake of entire population. In domestic field, remotely controlled and operated robots will clean, cook, play, and communicate. In medical field, long-distance medical surgery and remote healthcare are hot research topics [28]. UC San Diego's Einstein robot is the first ever hyper-realistic robot with humanlike expressions. This robot can walk, smile, and frown. It is expected to be used for children with autism [29]. Remotely controlled AMs will be connected through low latency radio networks for instant transfer and processing of AMs' internal sensors and actuators data. Crop

inspection, pesticides, water level usage monitoring, and assisted farmers actions are samples of agriculture field applications [1]. IoT mobile users will act simultaneously as client and server for receiving direct notifications alerts, pictures, and live shows from various clients represented by smart objects as electronic home appliances, light control, surveillance camera, baby monitor, smart TVs …etc.

All these services require instant location and continuous connection to mobile users for live data exchange. Existing solutions will soon vanish for users accessing static web servers connected to smart appliances that stream live content from remote smart locations as homes, farms, offices …etc. These requirements emphasize on reinvention of new mobility concept to support collaborative interactions between static/moving terminals instead of existing centralized MIP architecture that supports only moving terminals interactions with static servers.

2.1.6 WiFi Service Provider

To extend the role of WiFi networks beyond internet access, new mobility framework is required to make advantage of lower cost service delivery as of the unlicensed WiFi spectrum for enhancing poor mobile coverage and capacity indoors. Current role of WiFi/DSL/Cable service provider is almost confined to offering megabytes at a good price without any strategic impact on customer's business or cost base. With about three-quarters of mobile voice and data sessions originating indoors, a new chance is open for operators to higher their value by launching bunches of new services [30].

The Wireless & Mobile Working Group (WMWG) researches emphasize on providing a mobility framework with unified access methodology for both wireless and wired network to ensure seamless integration to enterprise physical network or virtual cloud services [31]. Assume an employee's smart phone with installed voice IP phone application; the mobility framework must be capable to guarantee QoS with seamless integration to enterprise PBX while moving inside enterprise WLAN or through branches. For cable provider in smart cities, customers need to move freely cross WiFi provider hotspots while enjoying continuous connectivity to residential service as VoIP system, IPTV broadcasting, and remote home monitoring. Launching of Software Define Wireless Network (SDWN) paves the way toward this goal through SDN open APIs.

2.2 Problem Statement

The objective from this research is providing a uniform mobility framework with a scalable architecture based on OpenFlow SDN-based technology to satisfies 5G NGN IoT requirements which are hardly solvable with existing mobility protocols. The scope is not limited to previous concept of connecting mobile user to static location as home network, private cloud …etc. It is expanded to real time collaborative interactions between moving/static users, servers, terminals cross operators under mobility SLAs for facilitating cogitative services with minimum delay and latency. For performance enhancement, the framework eliminates mobility signaling overheads, restricts tunnel headers, and invents new routing mechanism with effective traffic offload technique to avoid the core congestion problem that restricts operators' mobility deployments in wide area motion and offerings for LIPA service.

2.3 Proposed Solution

OpenFlow SDN-based technology is used to establish mobility overlay network using three tiers of OpenFlow switches over any type of IP infrastructure managed by single or multiple operators under Service Level Agreements (SLAs) to instantly interconnect group of static/moving users, servers, and smart terminals with concurrent access to various services registered in their subscription profiles or activated on-demand in visited networks. Figure 2-1 provides a hypothetical layout for the mobility overlay. The objectives from using SDN overlay are hiding L3 routing complexities, bypassing any firewall structure, and crossing any WAN/LAN topology while ensuring the security of involved entities; private cloud, home, operators …etc.

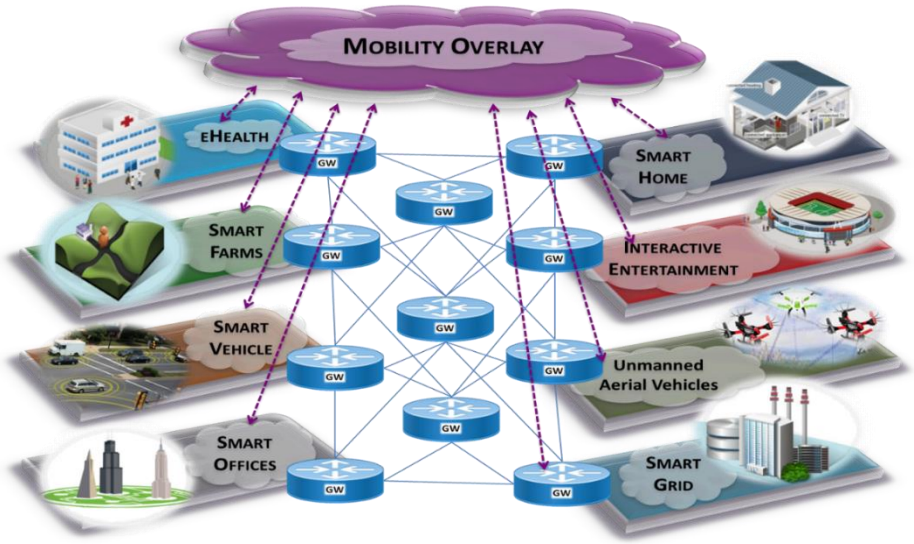


Figure 2-1: Hypothetical SDN Mobility Overlay Layout

For fully migrated SDN network, no hardware is required as of offering mobility as a service in the SDN application layer. Mobility overlay can be integrated to existing switched/routed network, LTE infrastructure, and Virtual Customer Premises Equipment (vCPE) based on Network Function Virtualization (NFV). The overlay structure is highly flexible to accommodate carrier grade deployments where each tier is represented by a set of multiple load-balanced OpenFlow switches or the three tiers functions are implemented in a single OpenFlow switch for small deployments. The design is fully aligned with ONF SDN arch 1.0, ONF OpenFlow spec 1.4, and RFC 7426 [32][33][34].

2.4 EVALUATION METHODS AND VALIDATION PLANS

The objective is assessing the feasibly of proposed mobility framework using virtual environment with real packets transfer rather than simulation. The established prototype comprises three enterprise networks; ENTERPRISE_EA, ENTERPRISE_EB, and ENTERPRISE_EC. Each has a separate SDN controller. A general layout is shown in figure 2-2. The three networks design creates a suitable media for moving hosts or terminals cross the topology. ENTERPRISE_EA has mobility SLAs with both ENTERPRISE_EB and ENTERPRISE_EC. ENTERPRISE_EC has two separate PDNs managed by the same SDN controller to represent two cities that are wide area separated. Mobility join delay, handover, and communication performance for ICMP, TCP, and UDP including throughput, latency, and jitters are measured in all experiments. Collaborative interactions' performance is measured between moving and static entities inside the established test bed to verify selected path optimality. Two criteria are measured to assess the framework feasibility.

2.4.1 MOBILITY SETUP AND HANDOVER DELAYS

- Both delays are measured with respect to two scopes; inside and cross cities' PDNs in ENTERPRISE_EC to represent standard and wide area motion. All results are compared to Cisco official benchmarks for PMIP [35]
- Mobility handover performance is compared to that of SDWN mininet-WiFi tool to emulate wireless OpenFlow/SDN. The objective is not to proof that mobility using SDN network is better than previous mobility protocols but to proof that the strength of performance improvement by simultaneous matching of results against standard and wireless OpenFlow/SDN networks. With these criteria, no complicated signaling or tunnel overhead is encountered to induce extra delay or increase latency. This ensures better performance over any existing mobility standards

2.4.2 MOBILITY PERFORMANCE

- Mobility performance is evaluated in three scopes; network managed by single SDN controller, cross controllers with direct mobility SLA, and cross controllers with indirect mobility SLA through transient operator. Communication performance through transient carrier, indirect SLA, is new feature not previously adopted in other mobility protocols. These experiments' objectives are conducted to understand SLAs' effect on performance and to estimate maximum number of indirect SLAs before performance degradation is noticed.
- Communication performance for ICMP, TCP, and UDP including throughput, latency, and jitters in all experiments are extracted from live capture files not simulation and compared to those of standard network in the prototype under the same conditions. Standard network performance is theoretically much better than VLAN, MPLS, PMIP, and GTP. This is mathematically calculated in table 3-2. From real deployment prospective, PMIP is at least 10% performance lower than standard network as of tunnel headers and signaling overheads [35]. The objective here is to highlight the dramatic performance improvement when compared to lower bound measures in all evaluations.
- The effect of SDN centralization logic is evaluated on all communication performance experiments before and after insertion of OpenFlow rules to highlight the complications if all MNs' packets are monitored by SDN controller or isolated in separate OpenFlow virtual paths.

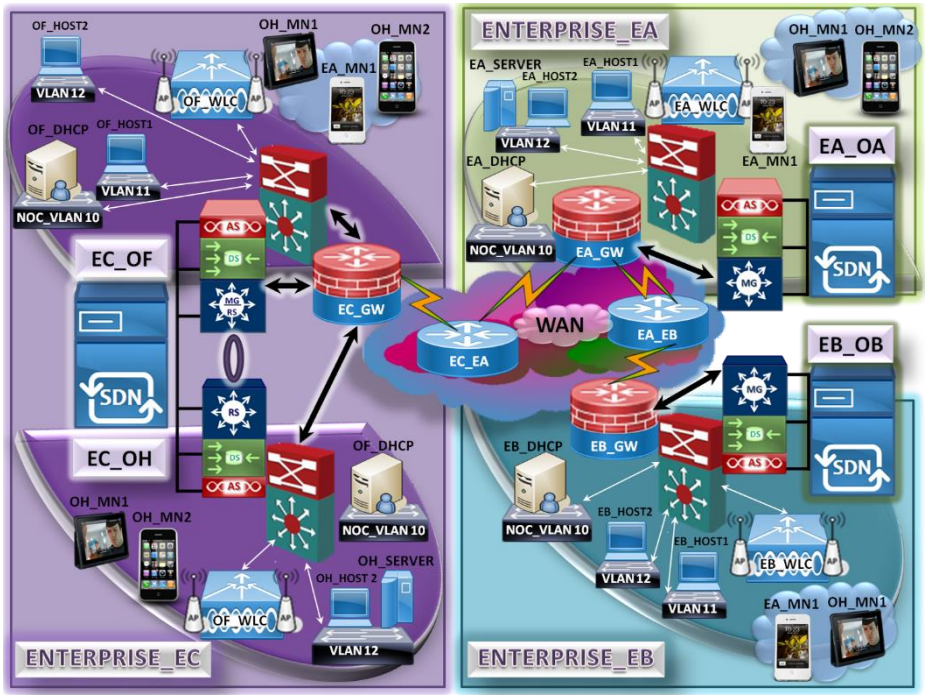


Figure 2-2: Prototype General Layout

3 REVIEW OF LITERATURE

3.1 MOBILE IP HISTORY

Mobility management is divided into two main categories; host-based and network-based architectures [36]. The former enforces MN's involvement in mobility signaling while signaling is carried through network without any MN's involvement in the later. MIP was initially defined in RFC 3344 as a way for enabling mobile user to keep the same IP address while traveling to different networks for ensuring continuous communication [7]. The initial proposed MIP was host based. Its' deployment required MN's kernel modification and introduced inefficient data forwarding, called triangle problem, that hindered its applicability in large scale deployments [37][38][39]. Later, MIPv6 was introduced in RFC 3375 as host-based mobility protocol for supporting MNs' global mobility [40]. It solved several issues in MIP; however, it suffered from large latency, complex signaling overheads, and security issues [36]. Several researches tried to decrease handover latency as in MIPv6 Fast Handover followed by proposals to decrease signaling overhead through hierarchical layout [41][42][43]. Finally, that ended with PMIPv6 and PMIPv4 release in RFC 5213 and RFC 5844 by 2008 and 2010 respectively [8][9].

PMIP was the first IETF standard network based mobility management protocol. The initial design was perceived to solve several problems as mobility inside cellular network, WiFi service provider, and inter-domain mobility. However, PMIP faces severe challenges in LTE including inefficient offload mechanism that leads to EPC congestion problem which in turn limits LIPA enterprise/residential service offering and session continuity in wide area motion as train/cars crossing cities' boundaries. Moreover, PMIP inter-domain mobility design and WiFi provider offering for LIPA service proved inefficiency and their internet draft expired without standardization [24]. PMIP challenges are described in section 1.3.2.

Latter, several IETF researches were developed to isolate TCP packets from UDP; as TCP is a reliable protocol requiring session continuity. Bell Labs presented a lightweight MultiPath TCP (MPTCP) proxy that to be inserted in the datapath for header rewriting without packet buffering or stream assembly. MPTCP tried to facilitate seamless session end-point migration across multi-provider network environments [20]. Cisco tried to extend PMIP to support TCP multipath as an initiative toward path selection on flow basis by facilitating MAG registration for multiple transport end-points with the LMA [21][44]. These trials were directed to satisfy operators' ultimate goal of finding an optimal solution that can filter indoor traffic and active TCP sessions to cross EPC core while providing instant breakout from MN's current point of attachment to both UDP and new TCP sessions for avoiding the EPC congestion problem.

3.2 MOBILITY IN 4G LTE

Together System Architecture Evolution (SAE) and LTE comprise the Evolved Packet System (EPS). The term LTE encompasses the project initiated by 3GPPP for Universal Mobile Telecommunications System (UMTS) radio access through the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), while the non-radio aspect System Architecture Evolution (SAE) includes the Evolved Packet Core (EPC) network. Unlike previous models of cellular systems supporting circuit-switching service, LTE was designed for packet-switched services only. The ultimate goal of LTE is seamless IP connectivity between User Equipment (UE) and Packet Data Network (PDN), without any disruption to end users' applications during mobility while ensuring higher data rate, lower latency, flexible bandwidth deployments, and great Quality of Service (QoS). EPS adopts IP packet flow concept with a defined QoS to route traffic between UE and PDN gateway. E-UTRAN and EPC are responsible for bearers' setup and release in accordance with applications requirements [45]. Figure 3-1 shows a layout for LTE and WiFi Interworking.

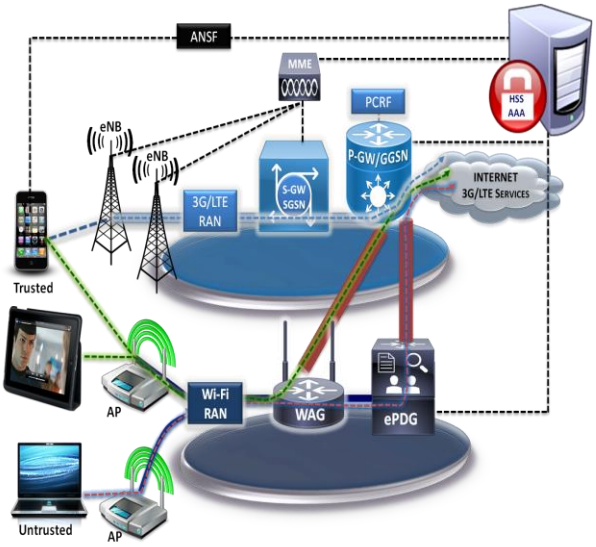


Figure 3-1: LTE and WiFi Interworking Architecture

3.2.1 MAIN FUNCTIONAL ENTITIES

- **HOME SUBSCRIBER SERVER(HSS)**
  - ➢ *Centralized Database Holding:*
    - UEs' SAE subscription data such as IMSI, subscribed QoS profile, and roaming access restrictions.
    - PDNs information database such as IP addresses and Access Point Name (APN) in DNS format.
    - Dynamic information as MME identity to which user is currently attached or registered.

  - ➢ *Authentication center (AUC)*
    - HSS can carry AUC functionality for generating authentication vectors and security keys.

- **eNodeB (e-NB):**

  Evolved base station provides wireless connection between UE and EPC to ensure both control/data integrity and security through the encryption of UE's datapath.

- **PDN Gateway (P-GW):**

  P-GW is the sole UE's exit to outside world. Each PDN is identified by AP name with an assigned P-GW to allocate IP addresses to UEs' from the PDN's IP addresses ranges. Policy Control and Charging Rules Function (PCRF) are performed for policy control and decision-making during live operation such as flow-based charging, QoS enforcement, and filtering of UE's downstream packets into different QoS-based bearers. In mobility management, P-GW serves as mobility anchor for inter S-GW handover and as LMA for interworking with residential/enterprise networks when offering indoor services.

- **Serving Gateway (S-GW):**

  S-GW forwards packets between base stations and P-GW, serves as LMA for inter-eNB and inter-3GPP handover; UE moves between eNBs or between other 3GPP technologies as GPRS and UMTS. S-GW temporarily buffers downlink data while MME initiates paging of UE for bearers' re-establishment.

- **Mobility Management Entity (MME):**

  MME is the EPS brain and the control entity for E-UTRAN. It processes signaling between UE and HSS for UE authentication, UE location, and UE state using Non-Access Stratum (NAS) protocols through exchanging Entitlement Control Message (EMM) and Entitlement Management Message (ECM).

- **Wireless Access Gateway (WAG)**

  WAG is reference in 3GPP Industrial Wireless LAN (IWLAN) architecture as the entity to support P-GW seamless integration with UEs for trusted 3GPP WiFi authentication based on IMSI in EAP-SIM.

- **ePDG (Evolved Packet Data Gateway):**

  ePDG is responsible for securing data transmission by terminating IPsec tunnels established by UEs for connecting to EPC over un-trusted non-3GPP access.

- **Access Network Discovery and Selection Function (ANDSF):**

  ANDSF serves as UEs' assistance for discovering access networks in their neighborhood by offering information about connectivity to 3GPP and non-3GPP access networks as well as providing policies to prioritize and manage connections to these networks.

3.2.2 GTP VERSUS PMIP IN LTE

General Packet Radio Service (GPRS) core is the central part of radio network that enables 2G, 3G fexternal networks such as Internet. GPRS Tunneling Protocol (GTP) is a group of IP-based communications protocols that is initially developed by European Telecommunications Standards Institute (ETSI) in late 1990s to handle this function and is still incorporated in both Universal Mobile Telecommunications System (UMTS) and LTE networks. GTP supported mobility is specified in 3GPP networks to allow UEs to handover between several access networks while ensuring IP-session continuity. In both 3G UMTS and 4G EPC architectures, GTP maps UE's packets into separate tunnel flows from SGSN/S-GW to previous GGSN/P-WG to handle IP-sessions continuity. Home GGSN/P-GW maintains the same IP address for UE regardless the point of attachment to ensure seamless handover. Session continuity is supported in EPC architecture using MIP, GTP, and PMIP. However, due to complicated signaling and overheads introduced by host based MIP, majority of vendor overlooked interoperability of MIP in their equipment [46]. The main differences between GTP and PMIP are illustrated in figure 3-2 and stated in the following table 3-1.

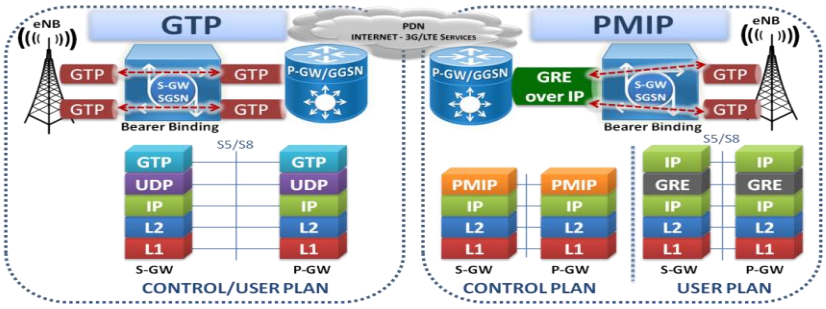


Figure 3-2: GTP versus PMIP in LTE

Table 3-1: Main Differences between GTP and PMIP

	GTP	PMIP
Bearer Base	Per PDN, QoS, UE, and Network Layer Service Access Point Identifier.	Per PDN and UE.
Bearer Notion	S-GW maps each bearer to P-GW in individual GTP tunnel.	Shared tunnel is used. S-GW determines the path based on HSS and UE's IP address to consolidate all UE's bearer packets into a single PDN connection.
S-GW⇔P-GW Tunnel	Encapsulated in GTP tunnel	Encapsulated in GRE over IP tunnel
Control Plan	UDP over IP	Directly over IP
User plane	UDP over IP	GRE over IP

3.2.3 Minimum Tunnel, VLAN, and MPLS Overheads

Calculations in table 3-2 highlight that the minimum theoretical improvement in L2/L3 standard network over GTP/PMIP is ~2% as of tunnel headers, ~0.25% over VLAN TAG, and ~0.51% over MPLS label. In real environment, PMIP tunnel induces at least 10% overhead in addition to the latency associating re-encapsulation at LTE-Uu, S1-U, S5/8, and SGi interfaces shown in figure 3-3 [35].

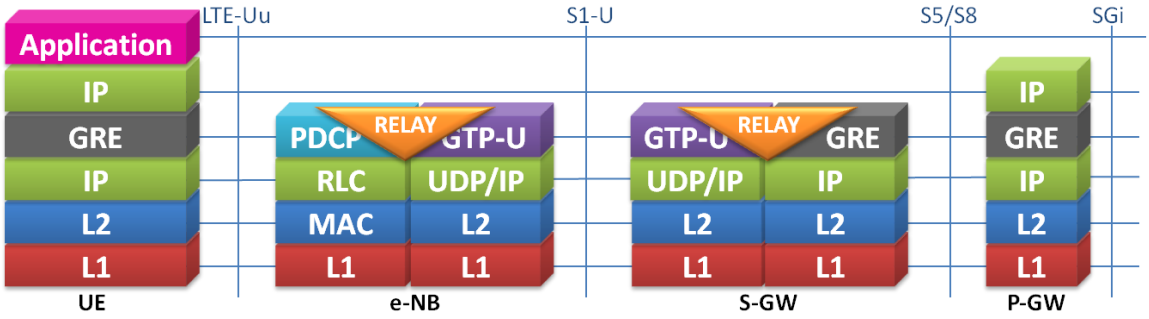


Figure 3-3: LTE PMIP User Protocol Stack

Theoretical Overheads

- Maximum Transfer Unit (MTU) in 100BASE-TX Ethernet = 1500 octet payload.
- Minimum Packet Size = 1500 (payload) + 8 (preamble) + 14 (header) + 4 (trailer) + 12 (min. gap) = 1538 octets.
- VLAN Packet Size = 1538 (min packet) + 4 (802.1Q TAG) = 1542 octets.
- Minimum MPLS Packet Size = 1538 (min packet) + 4 (top label) + 4 (bottom label) = 1546 octets.
- GRE Payload = 1500 (payload) – 20 (min IPv4) – 4 (GTP) = 1476 octets.
- GTP Payload = 1500 (payload) – 20 (min IPv4) – 8 (UDP) – 8 (GTP) = 1464 octets.

Table 3-2: Protocols Overheads

		Standard	VLAN	MPLS	PMIP	GTP
Overhead	$\frac{(Packet\ size - Payload\ size)}{(Packet\ size)}$	2.47%	2.72%	2.98%	4.03%	4.81%
Efficiency	$Payload\ size/Packet\ size$	97.53%	97.28%	97.02%	95.97%	95.19%
Throughput	$Efficiency/Net\ Bit$	97.53%	97.28%	97.02%	95.97%	95.19%

3.3 SDN PRINCIPLES

ONF introduces a novel approach called Software-Defined networking (SDN) that decouples network control plane from the underlying data forwarding plane. The open programmable North Bound Interface (NBI) facilitates development of wide range of off-the-shelf and custom network applications. SDN logically centralized control plane is considered the network brain that dramatically improves network agility and automation with significant reduction in operations' cost through the South Bound Interface (SBI) by complete manipulation of users' packets and underlying resources as switches and router switches. [4][47].

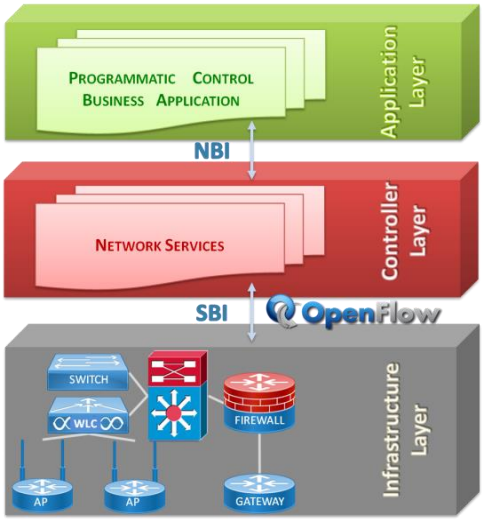


Figure 3-4: SDN Architecture

3.3.1 SDN ARCHITECTURE

ONF SDN architecture consists of three distinct layers that are accessible through open APIs. Figure 3-4 shows these layers; Application Layer, Controller Layer, and Infrastructure Layer.

3.3.1.1 APPLICATION LAYER

This layer represents end-user business applications providing SDN communications services that directly programs network behavior and devices through the SDN Controller via NBI.

3.3.1.2 CONTROL LAYER

This layer consolidates the control functionality supervising network forwarding behavior through an open interface. SDN Controller is a logically centralized entity that transfers the requirements of Application layer down to Infrastructure Layer through NBI and provides an abstract view of the network up to the Applications layer. SDN Control-Data-Plane Interface (CDPI) is the interface defined between SDN Controller and Datapath, which is responsible for network capabilities advertisement, statistics reporting, and events notifications. Physically, SDN controller has a hierarchical layout of sub-controllers and communication interfaces with virtualized framework called Network Function Virtualization (NFV) for slicing network resources. This physical layout facilitates the federation of multiple controllers.

3.3.1.3 INFRASTRUCTURE LAYER

This layer represents Network Elements (NE) and devices providing packet switching and forwarding functions. SDN Datapath is a logical network device, which exposes visibility and exceptional control over its advertised forwarding and data processing capabilities through a CDPI agent and a set of traffic forwarding engines and traffic processing functions. These engines and functions may include simple forwarding between datapath's external interfaces or internal traffic processing or termination functions [47].

3.3.2 OPENFLOW SDN-BASED TECHNOLOGY

OpenFlow protocol is key enabler for SDN and the first standard SDN protocol in SBI to facilitate relay of information and packets between control and forwarding planes through complete manipulation of network devices' forwarding plane such as switches and routers. OpenFlow adopts the concept of flows to identify network traffic based on pre-defined match rules that can be statically or dynamically programmed by the SDN controller software. For enterprises and carriers, OpenFlow SDN-based technology facilitates unprecedented programmability gain capable to trail the network behavior in a matter of hours through virtualization of network infrastructure and abstraction from individual network services. IT can define traffic policy based on usage patterns, applications, and cloud resources. Such unprecedented granular control facilitates for network instant response to real-time changes at application, user, and session levels unlike the monolithic, closed, and mainframe-like today's networking [4][5][32].

3.4 MOTIVATION FOR ADOPTING OPENFLOW SDN-BASED MOBILITY

3.4.1 SIMILARITIES BETWEEN SDN AND LTE

3.4.1.1.1 Concept of Flow

- LTE/EPC Evolved Packet System (EPS) uses the concept of IP packet flow to route packets between UE and PDN gateway.
- OpenFlow uses the concept of flows to identify network traffic based on pre-defined match rules.

3.4.1.1.2 Centralized Decision

- Existing WLAN adopts centralized WLC for management of distributed APs.
- In EPS, HSS holds a centralized database for users' subscriptions, dynamic information, and databases of PDNs and available resources.

- SDN is the logical centralized brain that holds all information of underling infrastructure through SBI with complete manipulating of MNs' packets and network resources using OpenFlow.

3.4.2 ADVANTAGES OF SDN-BASED LTE

3.4.2.1.1 Policies and QoS enforcements

- OpenFlow SDN-based architecture has inherited granular policies for effective packets isolation, service chaining, and QoS management, which exceed EPS QoS per bearer or standard network QoS [5][32].

3.4.2.1.2 Implicit Solution for MultiPath TCP (MPTCP)

- The unprecedented programmatic capability of flows through the NBI interface facilitates L2/L7 deep packet inspection in addition to L4 traffic filtration capabilities provided by OpenFlow through SBI on all network resources [48]. These features eliminate the need for any proxy services to isolate TCP from UDP traffic that can induce strong degradation in overall performance. The provided L4 traffic filtration capability is sufficient to create effective SIPTO and avoid the congestion of EPC core.

3.4.2.1.3 Virtual Path versus Bearer and Tunnels

- Considerable signaling overheads are induced during LTE bearer establishment/release, MNs' handover, mapping each bearer to either individual GTP tunnel or shared PMIP tunnel. Moreover, tunneling in general adds extra headers to MNs' packets that considerably reduce overall performance and increase latency. On the contrary, OpenFlow based SDN technology isolates flows based on L2/L4 packet headers without addition of any extra header to the flows, as in tunneling [48]. Such isolation is called in this paper virtual path. Virtual paths are expected to create a momentous improvement in overall performance and throughput when compared to any mobility framework with extra framing headers.

3.5 RELATED WORK

The enormous explosion of wireless devices, as smart phones, tablet, and laptop, increasingly captures attentions of operators and service providers to explore variety of solutions. The objective is supporting higher volumes of traffic while offering new sophisticated Value Added Service (VAS) for generating more revenues. ONF formed the Wireless & Mobile Working Group (WMWG) to assess new investigatory solutions for mobile operators and vendors. One of their core interests is mobile traffic management with strong focus on offloading mechanism. This is to accommodate subsequent exponential growth in audio and video streaming with tremendous bandwidth requirements that dramatically exceed designated budgets and Average Revenue Per User (ARPU). Such investigations are vital to make efficient usage of scarce RAN capacity though service discrimination to maximize revenues [4][5][31].

3.5.1 OPENROAD

Recently, software-defined wireless network (SDWN) becomes the focus of several researchers to increase the agility of Radio Access Network (RAN) through virtualization. Such initiative started with a prototype called “OpenRoad” that was deployed in college campuses to provide interconnection among heterogeneous wireless networks through virtualization [49][50]. The objective of this research is showing how MNs can effectively use available coverage for session continuity, effective offload, and load balance, regardless of being different wireless technologies; as WiFi and WiMAX.

This is considered a turn point in interconnecting heterogenous networks. In real deployments, different wireless technologies are expected to be owned by different carriers. “OpenRoad” needs further expansion to accommodate mobility cross PDNs managed by single controller for wide area coverage as well cross PDN of different carriers.

3.5.2 ODIN

“Odin” is a prototype built on light virtual AP abstraction to simplify client management without any modification to client side. The research uses SDN to implement enterprise WLAN services as network applications that provide seamless mobility, load balancing and hidden terminal mitigation [51].

“Odin” is considered an early initiative to replace vendor specific WLC as CAPWAP with SDN WLC. The initiative is restricted to 802.11 standard without incorporating any other radio technologies. No solution has been proposed to support mobility cross WLCs managed by different administrative domains. “Odin” doesn’t support unified access of enterprises wired/wireless LAN or mobility cross enterprise

buildings that are WAN separated with an effective offload mechanism to make efficient usage of interconnecting bandwidth.

3.5.3 OpenRadio

"OpenRadio" designs a programmable wireless dataplane implemented on multi-core hardware platform to re-factor the wireless stack into processing and decision planes. The processing plane includes directed graphs of algorithmic actions while decision plane carries the optimum directed graph logic election for particular packets. Wireless dataplane is compatible with wireless protocols including WiFi and LTE on off-shelf DSP chips with programmatic capability to modify PHY and MAC layers for further optimization [52].

This paper is not SDN-based but argues that wireless infrastructure needs a programmable dataplane to support such evolvability. "OpenRadio" resembles SDN in decoupling wireless protocol definition from the underlying hardware and designing a software abstraction layer that exposes a modular and declarative interface to program wireless protocols. However, the flexibility in SDN programable infrastructure is far beyond what is proposed in this paper as of multiple vendor support and wide range of off-shelf integrated applications.

3.5.4 OpenRF

"OpenRF" project proposes cross layer architecture for managing multiple-input and multiple-output (MIMO) signal processing with commodity WiFi cards and actual applications. "OpenRF" adopts SDN abstraction to create a self-configuring architecture that facilitates for APs on the same channel to cancel their interference at each other's clients transparently without any need for administrators' awareness of MIMO or physical layer techniques [53].

Despite being a good initiative, still real deployments of WiFi providers are not expected to rely on low commodity WiFi cards. This jeopardizes the power of SDN controllers in managing software applications for canceling interference instead of the PHY layer. Indeed, this will dramatically decrease the overall performance and position the controller as a single point of failure.

3.5.5 SOFTRAN

"SoftRAN" is the first SDN research to argue that existing LTE distributed control plane is suboptimal when allocating radio resources, implementing handovers, managing interference, balancing load between cells. The research tries to abstract all base stations in a local geographical area as a virtual big-base station comprised of a central controller and radio elements using SDN [54].

This research is based on a valid argument. Unluckily, no effective evaluation measures are proposed. In addition, the goals are directed to adopting SDN to enhance existing features performance without solving any existing challenges or proposing new features.

3.5.6 OPENRAN

"OpenRAN" argued about closeness and ossification of existing RAN to propose a new architecture that benefits from virtualization and SDN programmatic capability for efficient convergence cross heterogeneous networks [55]. The architecture contains four levels of virtualization; The first level is application virtualization that divides the flow space to several virtual spaces representing several network operators or services that are operated and managed independently. The second level is cloud virtualization, that enables SDN controller to create virtual Base Band Units (vBBU) and virtual Base Station Controllers (vBSC) through virtualization of physical processors and allocation of appropriate computing and storage resources. The third level is radio frequency Spectrum virtualization which enables several virtual Remote Radio Units (vRRUs) with different wireless protocols to coexist in one shared physical Remote Radio Units (pRRU). The fourth level is cooperation virtualization which constructs several virtual networks, including virtual nodes and virtual links to benefit from inter-cell interference elimination and facilitate communications cross different vBBUs and vBSCs.

"OpenRAN" can be considered a creative architecture. However, the research has not stated any evaluation or validation methods, or operators' cross billing mechanism, or effective measures for resources management. Thus, a realistic study to ensure its feasibility is missing.

3.5.7 ANYFI

"AnyFi" is SDN mobility framework for WiFi Carriers to support indoor mobility on available hotspots. In this framework, the SDN controllers of WiFi carriers have full power on home APs after software update. The updated home AP is called Software Defined Wireless Network (SDWN) service termination. When MN joins the home AP, details of its set including MAC address are sent to service

provider controller to make a virtual WiFi network available on the go. Also, MN stores home SSID and authentication credential of home AP in the network preferred list. When the same MAC address of MN's set comes near a foreign AP, SDWN radio software probes the SDN controller to create a home virtual SSID on visited AP thus MN's device connects automatically to it with the stored home credentials. Then, SDWN tunnels MN's packets to home AP [56].

"AnyFi" framework has real deployment in the initial launching phase. This is considered a major improvement over previous works. However, three main challenges can hinder wide expansion of "AnyFi" service. The first is lack of integration mode to cellular or LTE networks as it is restricted to WiFi technology only. Thus, both deployment scope and geographical coverage are limited. The second challenge is the enforcement of remote controlled AP without considering customers' security policies. The third challenge is lack of enterprise scale support as it will be hard to create a virtual hotspot in the street per probed MAC. In real enterprise deployment, it will take huge amount of time till identifying the home network of nearby MAC. Also, there will be strong limitation on the numbers of virtual APs that can be created on the spot.

3.5.8 CellSDN

"CellSDN" introduces a local agent to make real time decision using centralization of logic in SDN while reducing complexity in the control plan and the cost of purchased equipment during expansion. The paper argues that SDN deployment in cellular networks can facilitate isolation of subscribers' flows using MPLS or VLAN TAG instead of bearer/tunneling signaling overheard. The expectations are tremendous simplification in newer services launching process, in existing capacity expansion for acquiring more subscribers, in real-time services application and fine-grained policies enforcement, as well as in deep packet inspection and in packets header compression [57].

"CellSDN" can be considered a real transformational shift in network by converting traditional mobility bearer and tunneling signaling overheard to lower level overhead TAGs. However, the vision that the SDN controller is managing a group of OpenFlow switches not standard routed network has not been efficiently utilized. Standard routed network drops MN's hardware address after first hop router for this MPLS tags packets to avoid IP conflict cross overlapping subnets. In SDN multi-tenancy, MNs' hardware addresses are not dropped. Thus, packets can be isolated based on (IP, hardware) addresses pair without the need of either VLAN TAGs or MPLS Labels. With this fact, further performance improvement over "CellSDN" is expected.

3.5.9 SOFTCELL

"SoftCell" is the successive research of "CellSDN". This research proposes a scalable architecture to support fine grained policies' enforcement on mobile devices in cellular core networks through sequences of middle boxes using commodity switches and servers. Packets classification occurs at access switches next to base stations to guarantee that sessions belonging to the same connection traverse the same sequence of middle boxes in both directions even in the presence of mobility. The architecture prototype proves scalability and flexibility in real LTE workloads and in large-scale simulations [58].

In "SoftCell", the centralization of logic and the enforcement of fixed paths for the same connection can have dramatical side effects on performance as well as fault tolerance and load balance strategies. Further expansions for both "CellSDN" and "SoftCell" are expected. The scope should include solutions for existing LTE challenges as offload mechanism, core congestion, handover problems, roaming cross LTE providers …etc.

3.5.10 HETEROGENEOUS CLOUD RADIO ACCESS NETWORK (H-CRAN)

Latter, software-defined heterogeneous cloud radio access network presents a centralized large-scale processing for suppressing co-channel interferences. The research introduces a new communication entity, called Node C, to converge existing ancestral base stations and acts as base band unit (BBU) pool to manage all accessed remote radio heads (RRHs) [59]. "H-CRAN" is considered a good initiative for heterogeneous radio access network aggregation. This represents a future research direction for optimum resource allocation and fast handover evaluation cross heterogenous interconnected clouds.

3.5.11 DISTRIBUTED SDN CONTROL PLANE (DISCO)

"DISCO" proposes an extensible DIstributed SDN COntrol plane to cope with the distributed and heterogeneous nature of modern overlay networks to support WAN communication with resilient, scalable and extendible SDN control plane. DISCO controller manages its own network domain and communicates with other controllers to provide end-to-end network services. The framework is implemented on top of Floodlight OpenFlow controller and advanced message queuing protocol. Communication cross DISCO controllers is based on a lightweight and highly manageable control channel protocol. The feasibility of this approach is evaluated through an inter-domain topology disruption use case [60]. This research represents a starting point for negotiation cross controllers to ensure resilience and fault free network. DISCO controller represents a future direction for any mobility research for advance customization and orchestration of the services offered to roaming MNs' at visited network.

3.5.12 IMPACT OF SDN ON MOBILITY MANAGEMENT

This research proposes a new approach based on SDN concept for providing IP mobility in localized network without standard/ proxy IP mobility protocol implementation. The objective is reducing loss in packets compared to PMIP and simplifying real implementation through solving overhead problem and decreasing handover latency. In this approach, routers signal the SDN controller of MN's join and handover. In turn, the controller deletes MN's flows with corresponding nodes and creates new flow rules matching the current attached location [61]. This research has direct contribution in prototyping mobility without tunneling overheads. This is considered strong improvement in performance for solving mobility inside a single PDN. However, cross geographical separated PDNs, MN's packets need an exit from the new point of attachment. In turn, MN's packets will be mapped to a new public IP address regardless keeping the registered private IP address. This will disconnect all active sessions and destroy the proposed mobility concept. Mobility performance inside a PDN can be further improved provided canceling out-band signaling between routers and the controller. By default, new MN's flow will trigger the controller for path determination. Out-band signaling adds redundant latency that should be reduced.

3.5.13 SDN PERFORMANCE EVALUATION AND MODELLING

5G is expected to be driven by SDN thus several researches try to analyze the required performance, scalability and agility [3][25]. One of the researches debated about the ability of the controller to manipulate a significant amount of real-life traffic on being deployed in a largescale service provider. The researcher supports the argument with OFSim, an event-driven OpenFlow simulator that supports the performance evaluation of OpenFlow system with packet-level real-life traffic traces. Experimental results reveal that performance bottleneck may be located in some OpenFlow switches and flow table entry installation delay [62].

Another research proposed an analytical model to study the impact of flow table hit probability and service resource allocation in the SDN controller and switches on system performance. The model adopts Markov-Modulated Poisson Process to capture the traffic characteristics of multimedia applications. A priority queue system is used to capture the multi-queue nature of forwarding devices. A versatile method that extends empty buffer approximation has been proposed to facilitate the decomposition of such queuing system to two single server-single queue. The accuracy of the proposed model has been validated through extensive OMNeT++ simulation experiments. As stated, results revealed that both average latency and throughput predicted by the developed model reasonably match those obtained from the simulation experiments [63].

3.5.14 COMMENTS ON SELECTED PAPERS

Researches tried to re-implement PMIP with all its previously stated limitations as a service on the SDN controller but with minor modifications to make use of the logical decision centralization without in-depth consideration of the full power of OpenFlow SDN-based technology [64]. Others try to use the real-time packet re-write feature to preserve MN's IP address while communicating with remote services during handover [64]. This solution is insufficient in real deployment to solve the session continuity problem due to main reasons; First, all MN's sessions are disconnected with the lease of new IP address thus there is no reason for packet re-write. Second, when communicating to the internet, all MN's active sessions will be automatically mapped to the same public IP provided using the same exit PDN. If handover cross several PDNs, packet re-write is effective only to send packet to remote services with the same source IP address. However, reply packets will be returned to the initial PDN before handover as of the hierarchical standard routing mechanism based on subnet. Thus, reply packets will not reach MNs roaming at new PDN unless resorting to tunneling again.

With the availability of free versions of Open vSwitch and controllers for download, researchers started creating test-beds for evaluating mobility in LTE/future 5G base stations. Unluckily, misconception is clear in their evaluations. One of the researches adopts IEEE 802.3 standard switches to simulate LTE core and IEEE 802.11b/g in base stations [66]. Both protocols rely on broadcast for users' interconnectivity to shared resources/segment as LAN. This scenario is not available in LTE, as RAN is connecting individuals without shared resources/segment to remote services as internet. For this reason, UEs are not allowed to receive broadcast messages from other roaming UEs even those directly connected to the same base station. Furthermore, LTE adopts advance techniques to guarantee the highest VoIP QoS for compensating the best-effort policy in packet switching. Thus, implementations based on IEEE 802.3 and 802.11b/g to evaluate LTE mobility are almost infeasible.

4 MOBILITY FRAMEWORK SCOPE, OPERATION, AND STRUCTURE

4.1 UNIFORM MOBILITY SCOPE

This research adopts the 5G-PPP vision by presenting the concept of Mobility-as-a-Service (MaaS) using OpenFlow SDN-based architecture to interconnect moving/static group members. The framework is a superior concept of mobility incorporating collaborative communications as well as previous principles for providing session continuity to moving users communicating to static locations as private clouds, home, and corporate networks, …etc. The scope is described by uniform as the same concept is adopted for collaborative interactions, for replacement of IP mobility protocols adopted in LTE as PMIP, for substituting WLANs protocols adopted by WiFi service providers and those with unified access to both wireless and wired networks in enterprises as CAPWAP. The architecture has an effective SIPTO mechanism that solves the core network congestion problem induced from centralized gateways and proxies adopted in previous mobility protocols while ensuring session continuity and seamless handover in standard and wide area motion for LIPA and standard services.

4.2 OPERATION OVERVIEW

The proposed mobility framework adopts SDN overlay network with three tiers of OpenFlow switches in tree structure. Proprietary multicast messages are used inside the overlay for dynamic discovery of connected switches and topology layout. Mobility identifier of a joining member is sent during IP addresses allocation process using DHCP. The overlay switches extract the group identifier from the mobility identifier for dynamic discovery of the path toward the joining member's home network. The DHCP request message is relayed in recursive fashion based on the group identifier's indices. Once the DHCP message reaches home mobility overlay, the joining member's subscription profile is retrieved.

After successful authorization in the home network, DHCP request message is relayed to home DHCP server for IP address allocation to joining member. DHCP reply from home network follows the same forward path but in reverse order. When a DHCP reply with valid IP offer enters any mobility switch, an on-demand profile is activated for the joining member. With the first non-DHCP packet entering any mobility switch from a member with activated profile, OpenFlow rules are installed on the overlay switches based on member's subscription to avoid future interruption to the SDN controller. OpenFlow virtual paths are established to ensure wire speed forwarding of future packets. Inside the virtual paths, members are identified by both IP and L2 addresses thus overlapping IPs can exist without conflict.

4.3 IP ADDRESSES ALLOCATION

Every MN is offered three IP addresses. Descriptions and functions of each IP are stated bellow:

- **HOME ADDRESS (HA)**

  MN obtains this address from home network DHCP server, provided LIPA service is registered or from PDN at MN's initial point of attachment or at home operator if MN is roaming in a foreign network. This is the only IP address forwarded to MN during the join phase and is kept till MN disconnects or DHCP lease expires.

- **SDN ADDRESS (SA)**

  MN obtains this address from SDN internal DHCP service. It is non-routable address that is used with MN's L2 address to uniquely distinguish MN's packets when accessing SDN NGN applications provided through NBI.

- **CARE OF ADDRESS(COA)**

  MN obtains this address from the current attached PDN for instant breakout of UDP and new TCP sessions to offload core network and for legacy intranet/internet services accessibility in the attached PDN.

DEPLOYMENT COMMENT

To avoid several headers rewrite due to overlapping IP Ranges the following scheme can be used:

- *Reserve Class A: 10.x.x.x/8 for SA.*
- *Reserve Class B: 172.168.x.x/16 for CoA.*
- *Reserve Class C: 192.168.16-32.X/24 for HA.*

4.4 MOBILITY PREREQUISITES

As a prerequisite, DHCP_CLIENT_ID field value in DHCP_DISCOVERY/DHCP_REQUEST messages must be set to the mobility identifier of joining members as described in section 4.5, either through manual enforcement in MN's DHCP client configuration files or through AAA server after MN's authentication. In LTE, HSS can set it in "Mobile-Node-Identifier" #AVP Code 506 of the "Diameter Update Location" message as in RFC 5779 [15]. DHCP_CLIENT_ID is option field number #61 that was initially designed for DHCP clients to specify their unique identifier in an administrative domain. DHCP servers used this value to index their address bindings databases [67][68]. Latter, this option was ignored as the client's L2/hardware address specified in CHADDR field, MAC/IMSI, becomes used by DHCP servers for indexing their binding databases.

4.5 USER EQUIPMENT MOBILITY SUBSCRIPTION IDENTIFIER

User Equipment Mobility Subscription Identifier (UEMS_ID) is a unique identifier assigned to MN during subscription. Either MN sends this identifier or AAA/HSS after MN's authentication sets it in the DHCP_CLIENT_ID field of DHCP_REQUEST/DHCP_DISCOVERY messages for dynamic IP allocation. It is possible to replace UEMS_ID with IMSI. However, the framework prefers adoption of new identifier to create a uniform methodology for both 3GPP/5G-PPP trusted and un-trusted access as well as WiFi access without EAP-SIM authentication enforcement. This confides with the 5G-PPP project's vision of a unified programmable telecom and IT infrastructure [2].

UEMS-ID FORMAT

<Domain ID>-<Operator ID>-<Optional Sub-Operator ID>-<Subscription ID>-<User ID>

UEMS_ID DESIGN PURPOSES:

1) Instant Identification during MN's Join Phase

- Instant Identification of visitor MNs from local ones based on the first three prefix.
- Instant location of MNs' subscription profile.

2) Virtual Path Establishment during MN's Join Phase

- In proposed framework, VLAN and tunnels are replaced with OpenFlow virtual paths. If MN's retrieved profile in the join phase is for a roaming MN or registered for residential/enterprise service, the SDN mobility overlay network dynamically establishes the virtual path in a recursive fashion based on the indices of UEMSI_ID.

3) Instant Identification during UE Handover Phase

- When MN handoffs two PDNs serving two geographical locations in wide area motion, SDN mobility entity at the new joined access point alert the SDN controller with unknown flow from HA IP assigned from the previous point attachment as no OpenFlow rules are installed. The controller makes reverse lookup from HA to UEMS_ID through which the subscription profile is retrieved and the previous point of attachment and active sessions are identified.

4.6 MOBILITY OVERLAY STRUCTURE

SDN mobility overlay adopts a three tiers hierarchical multicast network of OpenFlow switches with tree structure. Inside the mobility overlay, OpenFlow switches use IP range from AD-HOC Block III [233.0.0.0–233.251.255.255] GLOP Block for internal communication [68]. The three tiers structure is shown in figure 4-1. The objective from adopting tree structure is eliminating any need for pruning algorithm regardless of using multicast messages during dynamic discovery of overlay layout and connected entities. The overlay structure is highly flexible to accommodate carrier grade deployments where each tier is represented by a set of multiple load-balanced OpenFlow switches or the three tiers functions are implemented in a single OpenFlow switch for small deployments. The design is fully aligned with ONF SDN arch 1.0, ONF OpenFlow spec 1.4, and RFC 7426 [47][32][33][34].

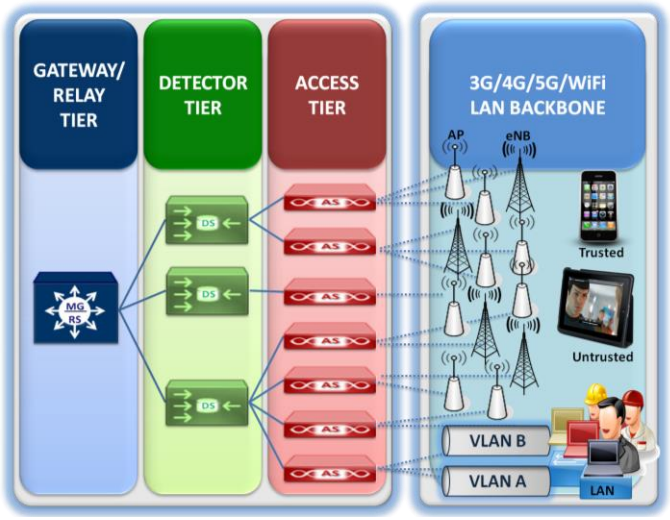


Figure 4-1: Three Tiers Structure Layout

4.6.1 ACCESS SWITCHES (AS)

AS represents the tree leaf and the first tier in the mobility overlay. This tier represents the access switches in fully migrated SDN network or broadcast listener acting a backdoor in standard network. Different integration modes are designed for standard switched/routed networks, WLAN, and LTE 4G/3G but for fully migrated SDN network nothing is required. This tier identifies new users joining the network and passes them to parent tiers to detect if valid mobility subscription exists.

4.6.2 DETECTOR SWITCHES (DS)

DS is the middle tier and AS's parent in tree structure. This tier is responsible for mapping various assigned IP addresses, offloading mechanisms, and orchestrating various services offered to group members in home/visited networks. DS carries foreign agent functions in visited network as detecting roaming mobility subscriber in addition to home agent functions in home network as spoofing members'

presence, relaying DHCP messages to home DHCP server. During virtual path establishment, if the next hop is AS then DS will carry both functions. This situation is called intra-overlay mobility.

4.6.3 Relay Switches (RS) and Mobility Gateway (MG)

This tier represents the tree root. It dynamically connects mobility overlays to provide seamless mobility extension over any LAN/WAN topology or firewalls policy. RS is responsible for inter-overlay mobility; connecting overlays managed by single SDN controller while MG is responsible for inter-domain mobility; connecting overlays managed by different SDN controller. An example of inter-overlay mobility is that of LTE operators having separate PDN per city. Mobile users can handover several PDNs while moving inside car or trains. Cross operators' mobility under SLAs for high availability and extended coverage is clear example of inter-domain mobility. A single OpenFlow switch can act as MG and RS at the same time. Inter-domain mobility can either be through a direct physical connection between two MGs or through activation of on-demand GRE/IPSec tunnels as shown in figure 4-2. MG uses inter-domain routing procedure, described in section 5.6.4, to establish virtual paths cross operators. Intra-overlay mobility adopts a bidirectional ring topology between RSs as of its self-healing nature and higher levels of resilience at lower cost. Figure 4-3 shows intra-overlay mobility layout. RS uses the overlay discovery procedure, described in section 5.6.9, for automated discovery of shortest path to any connected overlay and isolation of broadcast and multicast messages from propagating outside the connected overlay.

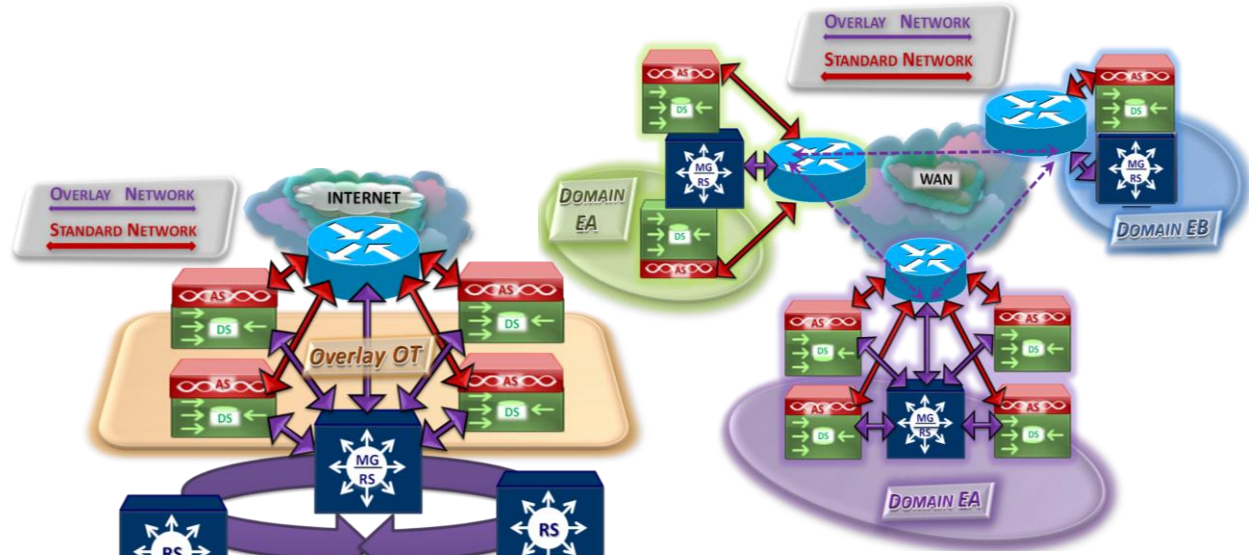


Figure 4-2: Inter-Domain Mobility

Figure 4-3: Intra-Domain Mobility

4.7 INTERNAL MOBILITY OVERLAY INTERACTION

4.7.1 MOBILITY OVERLAY IDENTIFIERS

Each mobility entity has three types of identifiers for fast location advertizing, interaction inside the mobility overlay and with the standard network entities as DHCP servers, local, remote gateways …etc.

I. IN-BAND IP

IN_BAND IP address is a standard IP used for management purpose as well as for communication with DHCP servers, local, and remote tunneling gateways. This IP address is preconfigured on the management interface of OpenFlow switch.

II. VIRTUAL IP

Virtual IP address is used only by the mobility switches for multicast communications between the overlay entities. It is not used in standard network communication. Virtual IP address uses a virtual hardware address configured in the switch profile stored in the SDN controller. Experiments are tested with AD-HOC Block III from 233.0.0.0 - 233.251.255.255 GLOP Block [69].

III. MOBILITY_ID

Mobility identifier is used to logical identity the overlay to which each OpenFlow is member. It has one to one relation with the virtual IP address. The proposed mobility framework routes packets to MOBILITY_ID not to subnet as in standard routing mechanisms. Each Mobility switch is identified by three to four ASCII characters from this pool: [A—Z], [a—z], [1—9] their decimal representation are [65—90], [97—122], [49—57] respectively.

4.7.2 LINKING MOBILITY IDENTIFIER TO PHYSICAL LOCATION

Traditional networks hinder seamless mobility by the concept of routing towards a logical destination which is the standard IP subnet. OpenFlow SDN-based technology opens the possibility of redesigning the network apart from conventional methodologies. The switch MOBILITY_ID becomes a key to tunnel flows between two geographically separated destinations (home, foreign) regardless of the enormous restrictions imposed by subnets, L3 routing protocols, firewalls, VPNs, private and public IP addresses. The proposed SDN mobility framework uses multicast overlay network for location advertizing, dynamic path discovery, and CTRL messages exchange. The following illustrates the two scopes for generating the overlay network identifiers. The difference between these scopes resembles the difference in functionality between Private and Public IP addresses.

4.7.2.1 PRIVATE OVERLAY NETWORK'S MOBILITY IDENTIFIER

This type of identifier is used for internal interaction between mobility entities managed by the same SDN controller; intra-domain. The objective is avoiding overlap configurations, preserving security, and hiding the internal structure of involved SLA operators, enterprise …etc. That is to some extent similar to private IP allocation [70]. An overlay is a branch of the tree structure with one RS, one DS, and one or more AS. Intra-domain mobility includes intra-overlay mobility managed by a single DS and inter-overlay mobility managed by one or more RS. A single overlay can represent a city in LTE or Enterprise. Each overlay is identified by two characters while each mobility switch is identified by a single character. The characters are chosen from pool of 61 characters: [A—Z], [a—z], and [1—9] with ASCII to Decimal mapping [65—90], [97—122], and [49—57] respectively. The key behind such choice is the decimal ASCII mapping occurs in range 1 ~ 254, that can be used as the last three octet of virtual IP multicast address.

For example:

- *LTE Service providers have multiple PDNs for service coverage cross the country. Each PDN serves a single city. This design is mapped to single mobility overlay per city. Service provider can choose 'OA' as prefix to the first city 'A' then the first mobility switch in the overlay 'OA' is identified by OA1'. This is translated to multicast address 233.79.65.49, where; <233>: AD-HOC Prefix, <79>: Decimal ASCII mapping of 'O', <65>: Decimal ASCII mapping of 'A', and <49>: Decimal ASCII mapping of '1'.*
- *Campus network is divided to VLAN per school as School of Engineering, School of Art …etc. Each school has its set of backbone switches incubating several VLANs for offices, labs …etc. Network administrator can choose 'SE' as overlay prefix to school of Engineering and 'SA' for School of Art. Then the first mobility switches are mapped to multicast addresses 233.83.69.49 and 233.83.65.49 respectively. Each overlay can hold up to 61 mobility entities with $2^{(12:\ VLAN\ ID\ bits)}$ = 4094 VLAN TAGs. In this case, both MOBILITY_ID and VLAN TAG identify the corresponding VLAN broadcast domain.*

From the explained logic, every overlay is represented by two characters from a pool of 61 characters. This means that a single carrier network can compose 61x61=3721 private overlay networks. Each overlay network can cover 61 logical mobility switch Identifiers and $2^{(12:\ VLAN\ ID\ bits)}$ = 4094 VLAN TAGs representing broadcast domains. The recent Virtual Extensible LAN (VXLAN) proposed in RFC 7348 uses 24-bit segment ID known as the VXLAN network identifier (VNID). This extension enables up to 16 million VXLAN segments to coexist in the same administrative domain per each of the 4094 IEEE 802.1Q VLAN [71]. Thus, each overlay of 3721 private overlay networks can cover up to $2^{(12:\ VLAN\ ID\ bits)} \times 2^{(24:\ VXLAN\ bits)} \cong$ 68,719 million VLANs. With VXLAN integration, mobility overlay becomes infinitely expandable to cover countries' level mobility not just enterprise or service provider mobility.

4.7.2.2 PUBLIC MOBILITY IDENTIFIERS

MG uses two MOBILITY_IDs. The first is private MOBILITY_ID for identification inside the overlay while the second is public MOBILITY_ID for inter-domain mobility. Public MOBILITY_ID is mapped to private IP address that is translated to public IP address using firewalls for accessing other remote WAN separated overlays. The proposed framework suggests generating MG public MOBILITY_ID from country codes ISO 3166 alpha-2 codes, published by the International Organization for Standardization (ISO). This defines codes for countries names, dependent territories, and special areas of geographical interest [72]. There are 249 current countries officially assigned ISO 3166-1 alpha-2 codes. According to security requirements and mobility design prospective, each of the subdivision names listed in ISO 3166-2 standard published by the ISO 3166 Maintenance Agency can be used as well [73].

The choice between the main assigned ISO 3166-1 alpha-2 codes and the subdivision is a design issue. Two Tunnels are needed in both cases. For main codes, the two tunnels are (Foreign, Local Carrier) and (Local Carrier, Home). For subdivisions codes, the two tunnels are (Foreign, Local Carrier Subdivisions) and (Local Carrier Subdivisions, Home). Using main codes can increase overlay networks' complexities. High mobility traffic load is a design issue but not critical as each Alpha-2 codes MG MOBILITY_ID can be mapped to several public IP addresses where each represents a cluster of OpenFlow load balanced switches. Thus, the main alpha-2 codes without subdivision are still enough to support tremendous traffic load while providing distributed load balancing criteria, fault tolerance mechanism, and instant disaster recovery. A single record per remote ISO 3166-1 alpha-2 is stored at the SDN controller database to map remote ISO 3166-1 alpha-2 code to multiple Public IP addresses. An alternative design is keeping the database on a separate server for dynamic retrieval and update. This database is straightforward as of having 249 countries registered code only or 10,000 entries at maximum if subdivision names are included. Moreover, MG public MOBILITY_ID mapping to ISO 3166-1 alpha-2 codes simplifies linking MNs' UEMS_IDs to their land line or their mobile number that is mapped to national identity number. If this is achieved, the proposed framework scope becomes global mobility crossing countries' boundaries associated with unique identification mechanism for MNs' packets while roaming in the globe

For example:

- *United States of America ISO 3166-1 alpha-2 code is 'US' then the record stored in remote countries' controllers: {'US':{Public IP 1, Public IP 2, Public IP 3 ---etc} }*
- *Florid subdivision of ISO 3166-1 alpha-2 code for the United States of America is 'US-FL' then the record stored in remote countries' controllers: {'US-FL':{Public IP 1, Public IP 2, Public IP 3 ---etc} }*

4.7.3 HOME NETWORK LOCATION EXAMPLE

Assume a roaming MN with subscription belonging to "American University in Cairo" has MOBILITY_ID: 'EG-C-2615-1000-05-01' is detected roaming in another Foreign Carrier as in figure 4-4. Foreign AS forwards MN's DHCP_REQUEST message to parent DS. Foreign DS extracts DHCP_CLIENT_ID from DHCP_REQUEST message and matches it against local "Mobility Routing Table" to find next hop with maximum match. In this situation, there will be a complete mismatch. Foreign DS forwards DHCP_REQUEST to virtual IP mapped to foreign MG MOBILITY_ID. Again, foreign MG routing tables detects a complete mismatch and that 'EG' is ISO 3166-1 alpha-2 code of Egypt is mapped to a Public IP <a.b.c.d>. Foreign MG tunnels DHCP_REQUEST to 'EG' MG Public IP. 'EG' MG detects that 'EG-C' is Cairo ISO 3166-2: EG and that '2615-1000' corresponds to the landline of American University. 'EG' MG tunnels DHCP_REQUEST to Private/Public IP of "EG-C-American University". American University gateway has two roles: the first is MG receiving tunneled packets and the second is RS forwarding packet inside the mobility overlay of "American University". American University RS detects that '2615-1000-05' corresponds to DS with MOBILITY_ID 'SE5' connected to School of Engineering. RS forwards the message to the corresponding multicast address '233.83.69.53'. Again, DS 'SE5' detects that '2615-1000-05-01' corresponds to AS with MOBILITY_ID 'SE1'. DS checks that hardware address and UEMS_ID belong to a valid subscription profile linked to 'SE1'. If valid subscription exists, DS 'SE5', acting as DHCP Relay manipulates DHCP_REQUEST message to be destinated to the DHCP server connected to home AS 'SE1'. DS 'SE5' uses its IN-BAND IP to relay the message to home DHCP server attached to this broadcast domain. DHCP server reply takes the same path but in reverse direction. DHCP reply serves as mobility service activation/declination for roaming MN. On acceptance, OpenFlow rules are installed on all the mobility switches in the virtual path for wire speed forwarding of future packets.

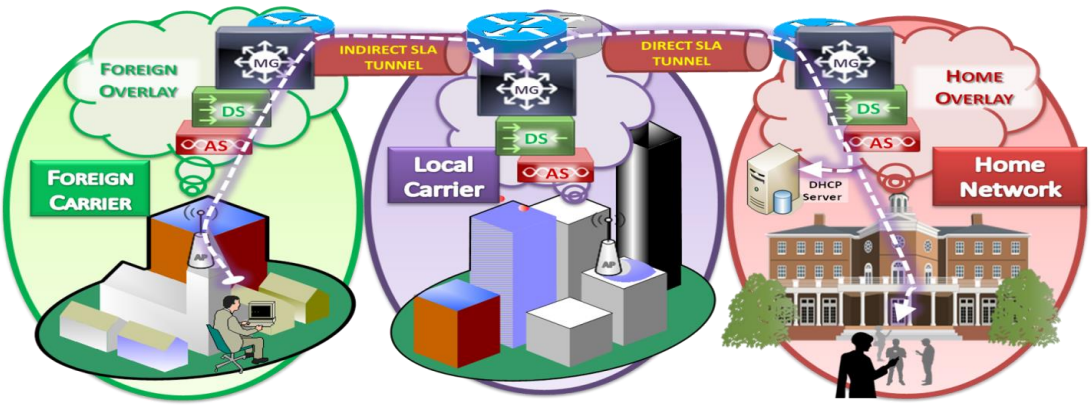


Figure 4-4: Roaming in Foreign Carrier

4.8 MOBILITY OVERLAY PHASES

4.8.1 MOBILITY SETUP PHASE

4.8.1.1.1 Authentication

The framework support several methods for authenticating MNs:

- MN can be authenticated through Authentication, Accounting, and Authorization (AAA) proxy service located in external server or provided in the SDN controller of visited network. MN sends its UEMS_ID in the username field to guide visited network AAA to use proxy authentication with home AAA server. If DHCP Proxy Client or DHCP Relay Agent is integrated to visited AAA service, AAA server must be placed on mobility AS acting as standard learning switch with filtering capabilities to relay DHCP messages from foreign MNs to their home DHCP servers instead of visited network DHCP server [74][75].
- MN can be authenticated through a web proxy client/domain controller in the home network for unified access between wire/wireless networks. In this case, when home DS receives a DHCP_REQUEST message from any MN with valid mobility subscription, it triggers home AAA service. After successful authentication, the DHCP message is relayed to home DHCP server.
- In LTE, the visited network HSS AUC service can authenticate MN as usual through Extensible Authentication Protocol (EAP) using USIM/SIM profile [76][77]. However, the framework stops HSS from guiding both mobility and handover processes. HSS enforces DHCP_CLIENT_ID value to UEMS_ID in DHCP_REQUEST/DHCP_DISCOVERY if MN is not configured for this.

4.8.1.1.2 Recursive Relay Procedure

When MN joins the network, it sends broadcast DHCP_REQUEST/DHCP_DISCOVERY message. Initially, the attached AS has no OpenFlow rules installed for this MN thus it consults the SDN controller which matches UEMS_ID field in DHCP_CLIENT_ID against AS mobility routing table for finding next hop toward home network. The output of match process directs the message to parent DS MOBILITY_ID. A temp profile is created for MN in AS database stored in the SDN controller. DS repeats the same process. In intra-overlay mobility, DS mobility routing table relays the message to PDN designated DHCP server for HA allocation. In inter-overlay and inter-domain mobility, the next hop is parent RS and MG, respectively, if MN is registered to residential/enterprise service. Again, a temp profile is created for MN in DS database. The process is repeated till correct relaying of the message to home DHCP server.

4.8.1.1.3 Service Activation

Once a valid DHCP_OFFER for MN enters any mobility entity storing a temp MN's profile, the status is converted to active profile containing both input and output ports required for directing standard non-DHCP IP packets. This avoids future consultation of mobility routing table. DS, managing MN's current attached PDN, requests SA address from the controller and CoA address from the PDN's DHCP server.

4.8.1.1.4 Virtual path Establishment

With the first MN non-DHCP packet entering any mobility entity, the active profile is converted to OpenFlow rules based on the subscription profile that are installed on mobility entities for wire speed forwarding of future packets without further interruption to the SDN controller. By this, the virtual path is established in a recursive fashion with OpenFlow rules installed for wire speed forwarding.

4.8.2 HANDOVER PHASE

4.8.2.1.1 Intra-Overlay Handover

This refers to MN's handover when crossing multiple ASs with the same parent DS connected to a single PDN. New AS has no OpenFlow rules installed, thus, it performs reverse map of HA address to UEMS_ID using the global SDN database. If a tie exists, IP address is allocated to multiple MNs, L2 address is used to resolve this issue. Once UEMS_ID is retrieved, MN's global profile and parent DS profiles are updated to reflect the current point of attachment. OpenFlow rules are installed based on subscription profile and packets are forwarded to parent DS. This is a direct process that introduces minor latency for profile update and does not oblige MN's renewal of HA address.

4.8.2.1.2 Inter-Overlay Handover

This refers to MN's handover in wide area motion when crossing multiple DSs with the same parent RS connected to two separate PDNs ruled by the same SDN controller. The process resembles intra-overlay handover in consulting SDN global profiles followed by update of mobility profiles and installation of OpenFlow rules. An extra step is added to ensure session continuity and to provide instant breakout. This step in inter-Overlay handover eliminates the need for MPTCP as all MN's active sessions are retrieved from the switch flow table of DS in the previous PDN. These sessions are filtered by L4 parser. Both parser's output and MN's subscription profile create a new set of OpenFlow rules that are installed on the new attached DS. The parsing process facilitates redirection of active TCP sessions and indoor packets only to previous DS. This provides instant breakout for new TCP sessions and UDP packets using new CoA allocated from MN's current attached PDN to avoid core network congestion.

4.8.3 VIRTUAL PATHS AND RELAY FEATURE

After activation the mobility profile, MN's packets become divided into three main OpenFlow virtual paths as shown in figure 4-5 and another path for relaying DHCP messages.

4.8.3.1.1 Internet and Intranet Paths

In this path, DS maps HA and CoA addresses for internet and intranet service accessibility. This creates an instant breakout for selective traffic and avoids the core network congestion problem. In LTE, several CoAs can be concurrently assigned to a single MN as of crossing several PDNs. In figure 4-5, two addresses are assigned when handover occurs as of crossing the cities' boundaries. Previous CoA (PCoA) is still used to continue active TCP sessions while a New CoA (NCoA) is leased from the new attached PDN to provide instant break out to new TCP sessions, UDP, and other non-reliable traffic. Intra-overlay handover is described in section 4.8.2.1.1 Moreover, the architecture facilitates further breakdown of CoA virtual path in V2V communication. NCoA facilitates V2V communication between two vehicles directly through AS without going upward to the parent DS. This is considered an effective solution to avoid core network congestion problem described in section 1.3.2.1, figure 1-1 & 1-2, while offering wide area motion, V2V communication, and LIPA service.

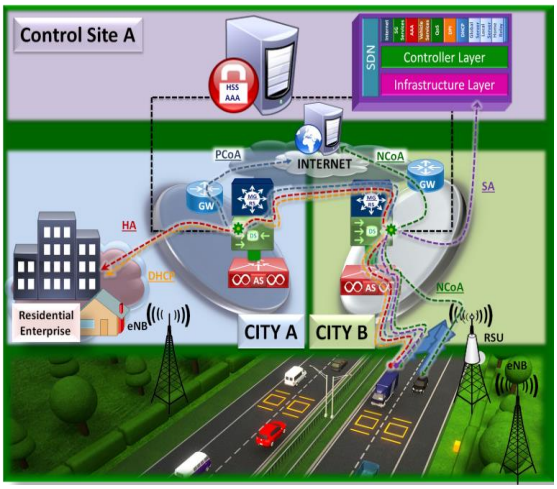


Figure 4-5: Virtual Paths and Relay Feature

4.8.3.1.2 DHCP Path

In this path, DHCP messages are relayed between roaming MN at foreign network and home DHCP server serving the initial point of attachment. The objective from this path is ensuring that HA is the only IP address forwarded to MN regardless the point of attachment for session continuity. If authentication occurs using the home web proxy client, authentication messages take the same path. No OpenFlow rule is installed to keep the SDN controller aware of MN's current lease status and authorizations.

4.8.3.1.3 Home Path

This flow is identified by HA subnet. OpenFlow rules are installed on all the mobility entities in the virtual path between visited and home network for wire speed forwarding of MN's packets.

4.8.3.1.4 SDN Path

SA is no routable IP assigned by the controller and is never changed till MN disconnects. This path uses SA to ensure continuous accessibility to various applications and services provided by SDN controller.

4.9 MOBILITY OVERLAY INTEGRATION TO EXISTING AND NGN INFRASTRUCTURE

For fully migrated SDN network, no hardware is required as of providing mobility as a service in the SDN application layer. This section highlights how the mobility overlay can be integrated to existing infrastructure as an out-band network to preserve existing investments and to provide smooth migration to NGN with SDN-based technology. The proposed mobility framework is highly adaptable to any IP infrastructure. This section presents integration to standard wireless/wired network, LTE, and vCPE in SDN/NFV technology.

4.9.1 INTEGRATION TO STANDARD WIRELESS/WIRED NETWORK

The objective from integrating the proposed mobility framework to enterprise backbone network is providing continuous accessibility to smart office/home services as IP phone, video conference, lighting, access control …etc while moving across WLAN's APs with unified access to both wireless/wired networks.

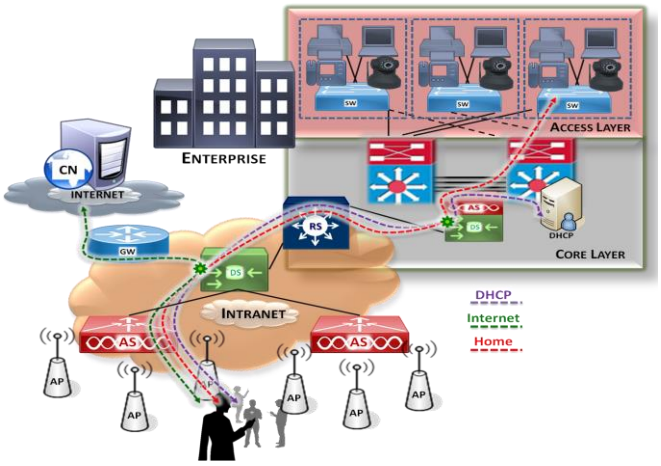


Figure 4-6: Integration to Standard Switched Network

Standard Wireless LAN Controller (WLC) needs firmware updating to support OpenFlow SDN based technology. This is currently offered by most of network vendors. Concerning backbone network, a standard OpenFlow representing AS tier is installed in the access aggregation/core layer as shown in figure 4-6. This AS acts as a standard learning switch for creating a backdoor connection to MN's home broadcast domain/VLAN. It is possible that AS is attached as a single trunk port carrying all backbone switch VLANs using IEEE 802.1Q VLAN tagging for Ethernet frames or that AS has several ports each is attached to single VLAN [78]. Both AS MOBILITY_ID and VLAN TAG or port are considered the identity of broadcast domain/VLAN. Home AP/Switch/DSL can install separate firewall rules restricting the traffic forwarded to AS port for security policy compliance without need for SDN migration or backbone networks upgrade. Figure 4-6 shows the

established virtual paths and the DHCP relay path to the home network. It is clear that internet packets are offloaded to nearest internet gateway without traversing home VLAN to avoid congesting backbone network. Moreover, such implementation ensures unified access to both wireless and wired networks.

4.9.2 MOBILITY DEPLOYMENT IN CELLULAR NETWORK

The proposed SDN mobility framework represents a strong contribution toward SDN-enabled LTE. The distributed structure of the mobility overlay facilitates several breakout points for offloading the core network and ensuring seamless handover in both standard and wide area motion without deploying MPTCP proxy. Moreover, OpenFlow SDN-based architecture has granular policies for effective traffic isolation, service chaining, and QoS management which exceed the EPS QoS per bearer [5][48].

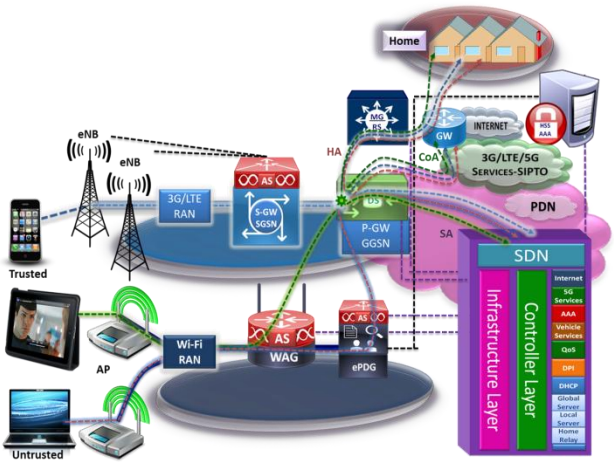


Figure 4-7: Hybrid Mode Deployment and Virtual Paths

Figure 4-7 highlights the proposed changes in existing LTE network, demonstrated in figure 3-1, to have SDN-enabled LTE. AS tier carries the same S-GW functionality as inter-eNB and inter-3GPP handover as well as forwarding packets between base stations and next DS tier. DS resembles P-GW in being PDN's exist to external world and intranet services. Unlike P-GW, DS don't allocate any IP to MN but it is responsible for relaying MN's DHCP messages to the DHCP server of attached PDN for CoA allocation and to home DHCP server or that at the initial point of attachment for HA allocation. SDN controller assigns SA address based on UEMS_ID regardless of the point of attachment. DS is responsible for services orchestration and re-writing of MN's packets' headers to map the three assigned IPs; HA, SA, and CoA.

OpenFlow based-SDN mobility framework has a unique advantage over existing LTE standards which is the capability of isolating traffic per hardware address without extra tunnel or VLAN header. In other word a single virtual path between two OpenFlow switches carries packets from two MNs having the same IP address but different hardware address without conflict. Basic OpenFlow virtual paths are illustrated in figure 4-7. Accordingly, PMIP/GTP bearers are replaced with OpenFlow virtual paths. This feature has a dramatically improvement in overall performance thus mobility framework handover experiments in both standard and wide area motion crossing LTE PDNs are compared to L2 handover of

Software Defined Wireless Network (SDWN) without tunneling or signaling overhead to ensure wire speed performance with negligible latency. Further splitting is possible at the AS level to facilitates instant V2V communication between two vehicles through AS without going to parent DS. NCoA virtual path, in figure 4-5, represents the V2V path. More details are illustrated in section 4.8.3.

4.9.3 Integration to Virtual Customer Premise Equipment (vCPE)

The next generation network is expected to provide a transformational change through automated service delivery by shifting existing networks from "Service Provisioning through Controlled Ownership of Infrastructure" to a "Unified Control Framework through Virtualization and Programmability of multi-tenant networks and services" [3]. The prospect from such notable variations is tremendous increase in networks revenue-generating capabilities and efficient control of operations. SDN facilitates realization of the above goal through logical centralization of control functions while NFV paves the way for enterprise virtualization. vCPE is the logical extension for such competitive service delivery model. Remarkable simplification in service providers' processes for business services deployments using vCPE is anticipated as of eliminating unnecessary equipment at customers' premises.

Figure 4-8 shows the direct compatibility of SDN mobility overlay to vCPE architecture proposed in ETSI SDN/ NFV framework [79]. Access aggregation cloud of vCPE represents the meeting point for integrating SDN mobility architecture. Mobility AS, acting as WLC of service provider hotspots, detects DHCP_REQUEST with valid UEMS_ID from a roaming MN joining the network. The message is automatically directed to foreign DS acting as service orchestrator. DHCP message is relayed by the mobility overlay to home vCPE where roaming MN is authenticated by home web portal. With a valid home DHCP server offer for HA, SDN controller installs OpenFlow rules for MN on the virtual path to home network for wire speed forwarding. Foreign DS starts orchestrating home vCPE registered services and on-demand service at visited WiFi hotspot vCPE then maps HA⇔CoA for instant breakout of internet packets.

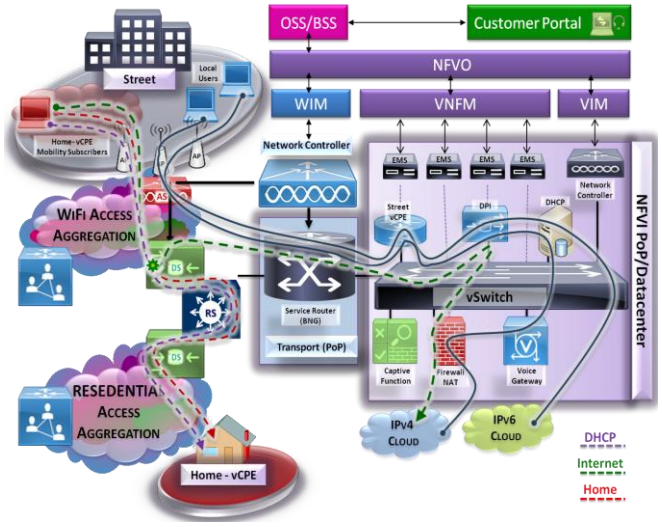


Figure 4-8: Integration to Virtual Customer Premise Equipment

5 SDN MOBILITY MODEL'S LAYOUT

5.1 OVERVIEW

The proposed SDN mobility framework is presented as a service in the application layer of the SDN architecture described in section 3.3.1. Several core profiles, tables, and functional modules control the operation of mobility services. Section 5.2 highlights how the database stored in the controller is indexed by datapath identifier of each mobility entity in the three tiers structure to control runtime operation through sets of profiles and tables. The fields in these database sets are either filled with pre-registered values or dynamically learned during runtime. The logic behind the core functional module is presented in five layered model shown in figure 5-1. Detection layer, described in section 5.3, is responsible for identifying roaming MNs in foreign networks and spoofing their presence in home networks. Classification layer, described in section 5.4, ensures that only correctly categorized MNs' packets are forwarded to upper layers' parsers while broadcast and non-mobility packets are filtered out. Parsing layer, described in section 5.5, converts raw packets to vectors containing vital information required to trigger certain procedure in the upper layer. Action layer, described in section 5.6, contains all procedures affecting the mobility overlay operations and runtime decisions. Activation layer, described in section 5.7, is responsible for activating MN's mobility profiles, orchestrating the service offered in foreign and home networks while ensuring correct billing systems cross operators.

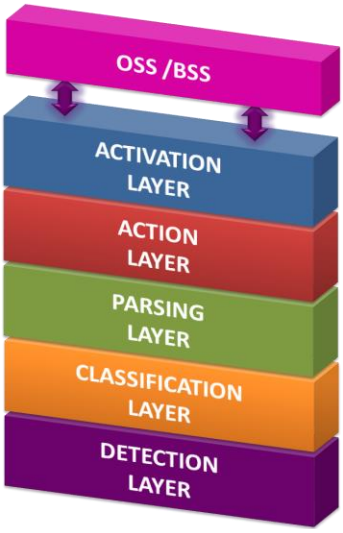


Figure 5-1: SDN Mobility Model

5.2 MOBILITY PROFILES AND ROUTING TABLES

5.2.1 MOBILITY SERVICE PROFILE

MNs' mobility profiles are divided into two main categories; Home and Foreign. "Home Profiles" are always preconfigured on Home detectors while "Foreign Profiles" are either preconfigured with valuable parameters required for identification of roaming MNs or created on-the-fly during virtual path establishment between home and foreign networks. Preconfigured profiles include "Static Profiles" to identify MNs with static IP addresses and "Dynamic Profiles" to identify MNs with dynamic IP addresses allocation mechanism. "Static Profiles" are pre-configured on all mobility switches in the virtual path while

"Dynamic Profiles" must be pre-configured on home detectors only. It is optional to configure this type on foreign detector if more services than those assigned to default subscription home group are required. "On-Demand Profiles" are created on-the-fly on all mobility entities in the virtual path during the service activation process. More details are illustrated in section 5.5.2.3.

REGISTERED FORMAT

<DPID>#<PROFILE>#<STATE>#<RECORD>#<HOME>#<UEMS>|[HW_LIST]|[IP_LIST]|<SIN>|<DIN>|<FOREIGN>|<STAMP>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
PROFILE	Profile type: HOME – FOREIGN.
STATE	Profile status: IDLE – ACTIVE – ROAM.
RECORD	Record type: STATIC – Dynamic – On-Demand.
HOME	Home network MOBILITY_ID.
UEMS	Registered MN's UEMS_ID.
HW LIST	List of HW addresses mapped to MN's UEMS_ID and flow layer. Either filled during runtime or statically pre-configured with pointer to special services requested.
IP LIST	List of IP addresses mapped to the index of MN's HW in HW List. Either filled during runtime or statically preconfigured.
SIN	Switch port identifying packets with MN's in the source field.
DIN	Switch port identifying packets with MN's in the destination field.
FOREIGN	Foreign network MOBILITY_ID.
STAMP	Timestamp of the last update on the profile.

Table 5-1: Mobility Service Profile

5.2.2 PORT ROAMING PROFILE

A profile assigned to each port in the mobility switch for fast (re)activation of mobility service, provided OpenFlow timers expire or this is the first non-DHCP packet forwarded by dynamic MNs.

REGISTERED FORMAT

<DPID>#<PORT>#<TYPE>#[NODE LIST: <HW>#<IP>#<OUTPORT>|<INDEX>|<LAYER>|<STAMP>]

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
PORT	Physical port identifier and logical VLAN TAG.
TYPE	SIN: Match source address – DIN: Match destination address
NODE LIST	List of roaming MNs registered to this port with index to their mobility profiles & output ports.

5.2.3 DHCP SERVER PROFILE

SDN controller stores a record per detector switch to authorize communication with its in-band IP address to/from registered DHCP server IP address using real time identified DHCP hardware address and port detected by the recursive relay procedure described in section 5.6.5.

REGISTERED FORMAT

<DPID>#<MOBILITY_ID>#<DHCP_IP>#<DHCP_HW>|<PORT>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
MOBILITY ID	Home MOBILITY_ID to which the registered DHCP server is assigned.
DHCP IP	Authorized DHCP server IP address.
DHCP HW	DHCP hardware address identified during runtime.
PORT	Physical port connected to DHCP port identified during runtime.

Table 5-2: DHCP Server Profile

5.2.4 MOBILITY SWITCH PROFILE

SDN controller stores a record per mobility switch in its internal database to identify various parameters required for real time interactions to identify MNs, establish the virtual paths, and in-band communications inside/cross mobility overlays.

REGISTERED FORMAT

<DPID>#<PRIVATE_ID>|<SW_MASK>|<REAL_ID>|<TYPE>|<SW_NAME>|<SW_HW>|<SW_IP>|<HW_TYPE>|<PORT>|<USERNAME>|<PASSWORD>|<KEYS>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
PRIVATE ID	Private MOBILITY_ID assigned to the Open vSwitch.
SW MASK	Mobility mask to differentiate between intra-overlay and inter-overlay mobility CTRL messages.
REAL ID	Public MOBILITY_ID assigned to the Open vSwitch.
TYPE	Tier type of the mobility switch: ACCESS: <1>, DETECTOR: <2>, GATEWAY: <4>, AP: <8>
SW NAME	Logic name assigned to the Open vSwitch that is logged in error and billing systems.
SW HW	Virtual hardware address assigned to the Open vSwitch.
SW IP	In_band IP address assigned to the Open vSwitch.
HW TYPE	Hardware Type as Ethernet, HSPDA interface ...etc
PORT	Management port number to be located during runtime
USERNAME	Management username assigned to the Open vSwitch.
PASSWORD	Management password assigned to the Open vSwitch.
KEY	Cryptography Keys if encryption is required

Table 5-3: Mobility Switch Profile

5.2.5 REMOTE GATEWAY PROFILE

SDN controller stores a record per mobility gateway in its internal database to identify various authorized remote gateways allowed to accept tunneled packets from/to this mobility gateway.

REGISTERED FORMAT

<DPID>#<GATEWAY_IP>#<NXT_HW>|<TUNNEL_ID>|<TUNNEL_TYPE>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
GATEWAY IP	Authorized mobility gateway IP address.
NXT HW	Next hop physical hardware address identified during runtime.
TUNNEL ID	Virtual tunnel identifier assigned during runtime.
TUNNEL TYPE	Tunnel type IPSec, GRE, ...etc.

Table 5-4: Remote Gateway Profile

5.2.6 LOCAL GATEWAY PROFILE

SDN controller stores a record per mobility gateway to authorize communication with its in-band IP address to/from registered local gateway IP address using real time identified hardware address and port detected by the overlay discovery procedure described in section 5.6.9.

REGISTERED FORMAT

<DPID>#<GATEWAY_IP>#<HW_TYPE>|<GW_HW>|<PORT>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
GATEWAY IP	Authorized local gateway IP address.
HW TYPE	Hardware Type as Ethernet, HSPDA interface ...etc
GW HW	Local gateway hardware address identified during runtime.
PORT	Physical port connected to local gateway identified during runtime.

Table 5-5: Local Gateway Profile

5.2.7 MOBILITY ROUTING TABLE

SDN controller stores a routing table per mobility switch to identify the next stage by AND operation between NETWORK_MASK field and HOME MOBILITY_ID retrieved from static users' profiles or DHCP_CLIEND_ID field in DHCP messages of dynamic IP users to match with NETWORK field representing target network group identifier. The output of this operation directs input packets to either overlay switching procedure or inter-domain routing procedure described in sections 5.6.3 and 5.6.4 respectively.

REGISTERED FORMAT

<DPID>#<NETWORK>|<NETWORK_MASK>|<DESTINATION>|<NEXTHOP_IP>|<ACTION>|<KEY>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
NETWORK	Target Network Group Identifier to matched with output of 'AND' operation.
NETWORK MASK	Network mask used in 'AND' operation.
DESTINATION	Learned MOBILITY_ID during dynamic discovery of mobility overlays topology layout.
NEXTHOP IP	Next hop gateway IP address used in tunneling decision.
ACTION	**SWITCH:** intra_overlay and inter_overlay switching -- **GATE:** inter-domain tunneling
KEY	Encryption key used in tunneling decision to next hop gateway IP address.

Table 5-6: Mobility Routing Table

5.2.8 CONTENT ADDRESSABLE MEMORY TABLE

SDN controller stores a table per access switch in its internal database for fast mapping of learned source hardware address to input port. This ensures optimum switching functions while minimizing broadcast. The record is cached for a default timeout that is renewed automatically with each packet entering the switch from a sourced hardware address that is previous mapped to the input port.

REGISTERED FORMAT

<DPID>#<HW_TYPE>#<SRC_HW>#<PORT><TIMEOUT>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
HW TYPE	Hardware Type as Ethernet, HSPDA interface ...etc
SRC HW	Packet source hardware address as identified during runtime.
PORT	Packet input port as identified during runtime.
TIMEOUT	States the time validity for each learned record.

Table 5-7: Content Addressable Memory Table

5.2.9 MOBILITY TO PORT TABLE

SDN controller stores a table per mobility switch containing the learned MOBILITY_ID during the process for dynamic discovery of mobility overlays topology layout mapped to the corresponding virtual IP and hardware addresses for instant switching during DHCP recursive relay process.

REGISTERED FORMAT

<DPID>#<MOBILITY_ID>#<MOBILITY_IP>|<MOBILITY_HW>|<PORT>|<TYPE>

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
MOBILITY ID	Learned MOBILITY_ID during dynamic discovery of mobility overlays topology layout
MOBILITY IP	IP address of mobility switch advertizing this MOBILITY_ID as detected during runtime.
MOBILITY HW	Hardware address of mobility switch advertizing this MOBILITY_ID as detected during runtime.
PORT	Output port directed to this MOBILITY_ID as identified during runtime.
TYPE	**IA:** intra_overlay, **IR:** inter-overlay, and **ID:** inter-domain as identified during runtime.

Table 5-8: Mobility To Port Table

5.2.10 MOBILITY TUNNEL TABLE

SDN controller stores a table per mobility gateway to identify active tunnels information and a list of active MNs per home MOBILITY_ID using this tunnel as well as those pending authorization.

REGISTERED FORMAT

<DPID>#<TUNNEL_ID>#<TUNNEL_PORT>|<GW_HW>|<RM_IP>|<RM_MASK>|<GW_IP>|[ROAM_LIST]|[PEND_LIST]

Field	Purpose
DPID	Datapath identifier required by SDN controller to communicate with Open vSwitch through SBI.
TUNNEL ID	Virtual tunnel identifier assigned during runtime.
TUNNEL PORT	Physical tunnel port assigned during runtime.
GW HW	Mobility gateway hardware address used in tunneling.
RM IP	Remote gateway IP address used in tunneling.
RM MASK	Remote subnets mask in default routing.
GW IP	Default gateway IP address used in routing.
ROAM LIST	List of active MNs using this tunnel per Home MOBILITY_ID.
PEND LIST	List of pending MNs waiting authorization to use this tunnel per Home MOBILITY_ID.

Table 5-9: Mobility Tunnel Table

5.3 Detection Layer

5.3.1 Overview

Detection Layer is the first layer in proposed SDN mobility model that plays a vital role in forwarding broadcast messages to upper layers for identifying roaming MNs at foreign networks. Moreover, this layer is responsible for spoofing roaming MNs' presence at their home networks when communicating with local users as well as tracing control messages between home and foreign networks to update mobility timers and to trigger mobility service deactivation if mobility timers expire. To achieve these goals, Detection Layer is designed to fulfill six vital functions as illustrated in figure 5-2. Detailed descriptions of these functions are explained in the sections bellow.

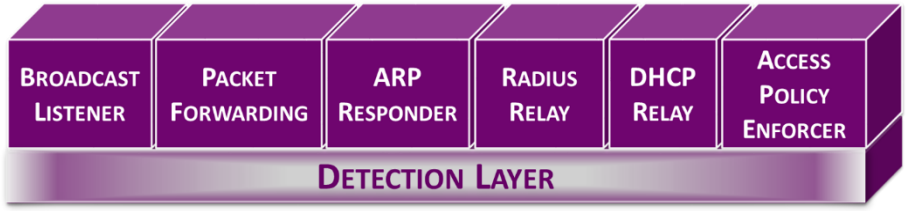


Figure 5-2: Detection Layer Functions

5.3.2 Switch Broadcast Listener

This function is designed for backward compatibility with existing non-migrated SDN networks. The mobility overlay is connected to existing infrastructure via an OpenFlow switch representing DS that is directly connected to L2 standard access switches via standard port or trunk port if IEEE 802.1Q VLAN TAG exits [78]. Standard L2 switches' core function is bridging Ethernet frames cross Ethernet segments. Ethernet bridging was initially defined in 802.1D IEEE standard for local and metropolitan area networks [80]. L2 switches map the source MAC addresses in Ethernet frames to the input switch ports. Mapping records are stored in switches' forwarding tables or CAM tables. When an Ethernet frame enters the switch, the frame is transfered to the switch port mapped to destination MAC address in the forwarding table. If destination MAC address is not mapped to any switch port, the switch broadcasts the frame to all ports. When a reply arrives, the switch adds a new entry mapping reply input switch port to reply source MAC address in forwarding table to avoid future broadcast.

Standard L2 switch operation concept is the clue behind the operation of detection Layer. If a node is roaming outside the home network or recently joined a foreign network, neither home nor foreign access switches has any previous record stored in their forwarding tables about this node. Therefore, foreign access switch broadcasts the first packet of this node to all switch ports including detector switch

port connected to access switch port. Foreign detector intercepts the packet and alerts the SDN controller for action determination. Classification Layer picks the packet to identify if it belongs to a roaming MN. If this packet is from a foreign MN, a dynamic virtual path is established between home and foreign networks through home and foreign detectors for future packets exchange. Home access switch automatically adds in forwarding table a new entry mapping roaming MN's hardware address to the port connected to home detector. Also, foreign access switch automatically adds in forwarding table new entries mapping hardware address of hosts communicating with roaming node to foreign detector port. The rest of packets to/from roaming mobility node are forwarded using the same virtual path between home and foreign networks.

5.3.3 PACKET FORWARDING FUNCTION

This function is designed for installing OpenFlow rules on the mobility entities for a roaming MN with already activated mobility profile. This function is triggered in two scenarios; the first non DHCP packet from an activated MN entering the mobility switch or expiry of OpenFlow rules timers while mobility timers are still valid when a packet sent to/from a pre-activated MN is encountered. Both scenarios trigger 'packet-in' events of SDN controller to automatically install OpenFlow rules on the mobility switch as previously determined by the mobility profile during activation to avoid re-triggering mobility route detection procedure as described in the Action Layer section 5.6.2. After installing flow rules, the mobility switch forwards all packets to/from roaming MN at wire speed without re-consulting the controller or the upper layers of mobility service. This guarantees wire speed hardware forwarding by OpenFlow not software speed as in routed L3 network.

5.3.4 DHCP RELAY FUNCTION

In standard network, DHCP relay extends the operation of DHCP servers by converting clients DHCP_DISCOVERY or DHCP_ REQUEST broadcast packets to unicast packets and forwards them to DHCP servers outside DHCP clients broadcast domain. DHCP sever replies to DHCP relay with DHCP_OFFER or DHCP_ACKNOWLEDGE message. DHCP relay forwards DHCP reply to DHCP client. With this feature, a single DHCP server can serve multiple broadcast domains [67][68]. If mobility profile of a roaming MN is enabled by SDN controller, the implemented DHCP relay function uses the output of recursive relay procedure that was triggered during MN's activation process for forwarding DHCP packets between roaming MNs and DHCP servers. This function is vital for mobility service to track DHCP lease period for successful activation/deactivation of MNs. The recursive relay procedure is described in Action Layer section 5.6.5.

5.3.5 RADIUS RELAY FUNCTION

Recent networks technologies as UMTS, DSL, modems, access points, VPNs, network ports, web servers, web portals …etc. incorporate Remote Authentication Dial-In User Service (RADIUS) as default mechanism for Network Access Control (NAC). RADIUS Relay function substitutes DHCP RELAY function in recent networks. The major difference between the two functions is that RADIUS ACCESS_REQUEST messages are unicast messages between NAS and RADIUS server not like DHCP_DISCOVERY or DHCP_REQUEST broadcast messages [81][82]. These unicast messages can never be intercepted by a detector switch connected to broadcast domains of access switch. For this reason, RADIUS server is placed on a separate detector switch for intercepting these messages. Future SDN networks will not need a separate detector switch as RADIUS feature will be directly incorporated to SDN controller of switched network. For existing networks adopting RADIUS as default protocol for triple AAA access (authentication authorization, and accounting), RADIUS relay function uses the recursive relay procedure triggered during MN's activation process to relay foreign NAS RADIUS messages to home detector switch which relays them to home RADIUS server. This function is vital for mobility service to keep tracking of MN's authentication messages for successful activation/deactivation process as well as accounting messages to synchronize Operations Support Systems (OSS)/Business Support Systems (BSS) of both foreign and home networks.

5.3.6 ADDRESS RESOLUTION PROTOCOL RESPONDER FUNCTION

Home user trying to initiate communication with MN roaming outside its home network sends broadcast ARP_REQUEST message to discover MN hardware address. The problem here is that this message contains broadcast address "FF:FF:FF:FF:FF:FF" in the destination field. Packets without a valid registered hardware address are not forward to MN as IP addresses are not enough to authorize communication especially if using DHCP. ARP responder function has a listener on home detector switch to detect ARP_REQUEST messages for MNs with activated mobility profiles. Home detector responds with spoofed ARP_REPLY messages on behalf of roaming MNs. Spoofed ARP_REPLY messages contain MNs' hardware address to hide their status from communicating partners.

5.3.7 ACCESS ENFORCER FUNCTION

With activation of MN's mobility profile, the default access policy for MN's home network is determined. Foreign SDN controller enforces MN's home group policy on both foreign AS and DS to tag all traffic from/to roaming MN with home VLAN TAG. By this enforcement, foreign AS enables all roaming MNs from the same home network to communicate without redirecting their packets to home networks.

5.4 Classification Layer

5.4.1 Overview

This Intermediate layer between detection and parsing layers acts as a strong filter protecting against suspicious activities to off load upper layers from processing meaningless packets. Packets are classified according to their L2/L3 headers. Only significant ARP and IP packets are forwarded to upper layers while other packets are dropped. Further filters can be added in the future. This layer has four main functions as shown in Figure 5-3. These functions are illustrated in the sections bellow.

Figure 5-3: Classification Layer Functions

5.4.2 Parser Selection and Prioritization Function

Packets are classified into three main classes according to L2 and L3 headers. Parser with the highest degree matching certain classification class is elected from the upper layer. If a parser fails to recognize certain packet, the packet is forward to the second matching degree parser. If all parsers fail, the packet can be either dropped or forward to a sniffer for more analysis. The three main classification classes are:

I. **Mobility Control Class:**

- **OVERLAY_CTRL message:** This type of control message is responsible for handling control messages inside the mobility overlay networks. This type is identified by 'AD-HOC' Prefix '233' in both source and destination IP addresses fields of the message [69]. Mobility overlays use ARP and ICMP packets for internal communication.
- **IN_BAND_CTRL message:** This type of control message is responsible for handling control messages between mobility switches' management interfaces and standard network devices as DHCP, RADIUS servers, local, and remote gateways. This type is identified by detecting IN-BAND mobility switch IP address in either message source or destination IP addresses.

II. **STANDARD SWITCHING CLASS:**

This class is restricted to access switches. Packets of standard users are filtered out by DS and not processed elsewhere in the mobility overlay. On the other hand, SDN migrated access switches parse only INTRA_OVERLAY_CTRL messages. The rest are considered normal switch packets or frames that need processing according to standard switch operation.

III. MOBILITY INITIATION CLASS:

This class is responsible for initiating the process required to activate/deactivate mobility service. This layer classifies detected packets in two sub-classes dynamic and static. Dynamic represents MNs using DHCP for IP address allocation while static represents those with preconfigured IP addresses. DHCP packets are classified dynamic while ARP_REQUEST and standard IP packets are classified static.

IV. MOBILITY MONITORING CLASS:

This class is responsible for activating modified or expired switch OpenFlow rules. Detection layer can activate non-populated or expired flows provided MN's attachment port is not changed or a new IP address lease has occurred. Reactivation of expired switch OpenFlow rules happens when OpenFlow timer expires while mobility profile timer is still valid. This can happen if a roaming MN is inactive for a while and moved to a different access point. In both cases, the parameters stored in mobility profile are retrieved for fast re-activation or de-activation of the service according to permissions in the subscription profiles.

5.4.3 BROADCAST AND MULTICAST ELIMINATION FUNCTION

Standard switched networks suffer from tremendous amount of broadcast and multicast packets that can waste the processing power of DS with meaningless frames or packets. These include routing protocol packets, multicast group discovery, datalink discovery protocols, non IP packets, and broadcast packets without L2/L3 addresses in both source and destination fields. Default SDN controller action for these packets is drop. This action will not conflict DHCP_DISCOVERY and DHCP_REQUEST as datalink source address is not a broadcast address. Also, it will not conflict ARP_REQUEST as of having broadcast at destination Datalink address only. OpenFlow rule for any of the previous cases is propagated to the switch from the SDN controller when a frame matching preconfigured criteria enters DS. An exception is made for the following two cases:

- The first case is the multicast packets using the prefix of overlay mobility network to identify mobility switches and to send OVERLAY_CTRL message.

- The second case occurs when a foreign MN requires a special access to multicast home services. Exception rule is updated by Activation Layer when mobility profile is enabled.

5.4.4 EXEMPTION POLICY FUNCTION

Regardless the network design, there will be tremendous list for those not requiring the mobility service. The exempted list can include local gateway, switches, IP phones, users, servers …etc. Without the exemption policy, the system keeps parsing huge number of packets that can either jeopardize high availability and overall system performance or enforce using expensive hardware devices.

There exists two criteria's for exemption policy. The first is a static policy for a list of hardware addresses configured by administrator for permanent service denial. The second is a dynamic policy enforced by a list of flow rules. OpenFlow rules for both criteria are propagated to switch from the SDN controller when a frame matching pre-configured hardware address in the static policy or a dynamic policy rule enters the detector switch. If matching OpenFlow rule is propagated to detector switch, similar frames will be automatically dropped without being forwarded to the SDN controller. If any of the mobility profiles is manually updated, conflicting OpenFlow rules will be removed automatically. The demand for dynamic exemption policy enforcement will be an urging need for administrators of carrier grade networks. The reason for this is the unattainable job of making a survey list for datalink addresses that need exemption. On the other hand, carrier grade performance is critical and should be maintained with minimum number of hardware equipment. The following specifies the rules in the dynamic exemption policy according to the type of mobility detector switch.

HOME MOBILITY DETECTOR:

- This case illustrates a registered MN that is active at its home network. The rule drops frames from an input switch port and source hardware addresses belonging to MN with a stored mobility profile entering from home access switch port.
- This case illustrates a standard frame sent to a host connected to mobility AS connected to home detector. The rule drops frames with destination hardware addresses not in the stored home mobility profiles and not belonging to a Virtual IP in the mobility overlay network and not mapped to the IN-BAND IP of this mobility DS.

Foreign Mobility Detector:

- This case illustrates standard frames or packets from non-roaming foreign MNs. This rule drops frames from source hardware addresses of unicast packets if both conditions bellow are matched:

a. Frame input port is connected to an access switch connected to mobility DS.

b. Source hardware addresses is not configured in foreign mobility profiles or in permitted list.

This rule does not contradict the activation of foreign DHCP MN as both DHCP_DISCOVERY and DHCP_REQUEST are broadcast packets not unicast packets as stated by the rule.

5.4.5 ACCESS SAFEGUARD

Frequent activation requests with rejected replies can adversely impact the mobility service performance and subject the system to implicit Distributed Denial of Service Attack (DDoS). Addressing the diversity of threats confronting the mobility service with effective security countermeasures becomes a priority for feasibility of the proposed architecture. MNs with activated mobility profiles are subjected to identity spoofing, DDoS attacks, and unauthorized manipulation of their home resources. Dropping suspicious node's activities and handling DDoS attempts are vital for service trustworthiness, maintenance of carrier grade performance and guarantee of high availability. These goals are achieved through the classification layer by inserting OpenFlow rules with timers equal to hold activity period. During this period, MNs' packets with rejected join replies from their home networks are automatically dropped in addition to packets from nodes with suspicious activities. Packets are marked suspicious if:

- Packets are originating from MN with enabled mobility profile and entering from a different switch port while the initial port is still connected to the roaming MN.
- There is conflict or variation in IP address mapped to the activated hardware layer address.
- MN is pervasively trying to exploit more than its profile's authorized services.

5.5 PARSING LAYER

5.5.1 OVERVIEW

This layer focuses on parsing packets headers and contents according to their Classification Layer classes. This process undergoes three main phases: "Identification Phase", "Dynamic Learning Phase", and "Action Triggering Phase" as shown in figure 5-4. "Identification phase" ensures that packets are correctly classified. If a packet is misclassified, the Parsing Layer either drops it or triggers the Classification Layer for correction. After parsing the packet, SDN profile of encountered mobility entity is updated in "Dynamic Learning Phase" with the parameters required for faster communication of future packets and for protection from spoofing attacks. The output of "Identification phase" is a vector called SYNOPSIS_VECTOR for identifying essential fields in the packet to avoid further analysis. Based on the output of this phase, Parsing Layer forwards the SYNOPSIS_VECTOR to matching procedure in the Action Layer according to "Action Triggering Phase". That is to determine what is needed to be done with the identified packets.

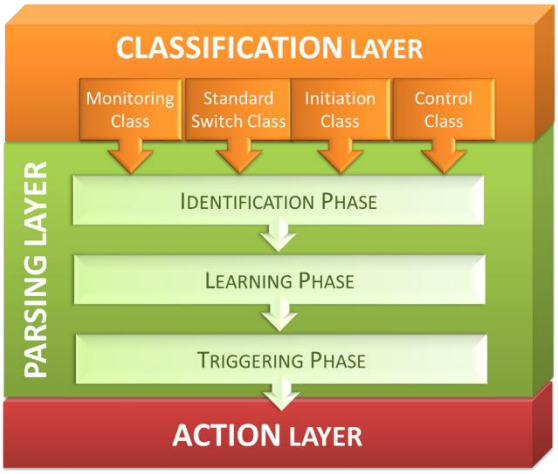


Figure 5-4: Parsing Layer Phases

5.5.2 IDENTIFICATION PHASE

5.5.2.1 MOBILITY CONTROL CLASS

This class controls the mobility service operation. Dropping any control message can leads to partial or complete system failure. There are two types of control messages:

5.5.2.1.1 Overlay Network Control Messages

This type includes control messages for intra-Overlay and inter-overlay mobility. Packets are forwarded to the Parsing Layer if the Classification Layer detects 'AD-HOC' prefix '233' in source and destination fields [69]. Parsing Layer checks if the packet is valid overlay control message using the conditions listed below. If the packet does not match any of the following conditions, the packet is dropped. Otherwise, the packet overlay type is identified to be forward to the correct procedure in the Action Layer.

VALID OVERLAY CONTROL MESSAGE CONDITIONS

- Packet has a valid Address Resolution Protocol (ARP) header [83].
- Packet has a valid Internet Control Message Protocol (ICMP) header and value of Internet Header Length (IHL) in IP header is greater than five [84][85] .

Mobility overlay subnet is the result of 'AND' operation of the mobility overlay mask and the virtual IP. This 'AND' operation differentiates between intra-overlay and inter-overlay messages. If the classification layer fails to place a packet in any of these two categories, the packet is dropped. The conditions below are required for control messages differentiation.

INTRA-OVERLAY MESSAGE DETECTION CONDITION

- Mobility overlay subnet of packet source and destination IPs are retrieved using the switch mobility mask stored in the SDN controller "Mobility Switch Profile" described in section 5.2.2. Match process output must be equivalent to the switch mobility subnet.

INTER-OVERLAY MESSAGE DETECTION CONDITION

- Mobility overlay subnet of packet source IP must match any of the overlay subnet stored in the SDN controller "Mobility Inter-Overlay Table" for this switch.
- Mobility overlay subnet of packet destination IP must match either the switch overlay subnet or any of the overlay subnet stored in the SDN controller "Mobility To Port Table" described in section 5.2.7.

5.5.2.1.2 IN-BAND Control Messages

This type includes the mobility overlay network control messages required for communicating with the switched network as routers, RADIUS, DHCP server …etc. using a standard Private IP. IN-BAND IP is physically configured on the management interface. For security purpose, this IP address is prohibited from communication with any entity unless explicitly permitted in the mobility profiles. The two allowed entities for IN_BAND_CTRL messages are illustrated bellow:

LOCAL GATEWAY CONTROL MESSAGES

ARP and ICMP packets are allowed between mobility and default network gateways provided that their Private IP addresses are explicitly stated in the "Local Gateway Profile" described in section 5.2.4. If any ARP_REQUEST packet is dropped for unknown reason, the gateway will consider the mobility overlay network down and will drop any future packet directed to this mobility gateway.

REMOTE GATEWAY CONTROL MESSAGES

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems and Juniper Networks. The protocol encapsulates a wide variety of the Network Layer protocols inside virtual point-to-point links over any IP network. Standard GRE packet header structure defined in RFC 2784 and RFC 2890 uses IP protocol type 47. GRE protocol is widely used in conjunction with IPSec VPNs for preserving communication privacy [86][87]. GRE packets are allowed between mobility and remote tunneling gateways provided their Public IP addresses are explicitly stated in "Remote Gateway Profile" described in section 5.2.3. If any GRE packet is dropped for unknown reason, remote gateway can consider the mobility overlay domain down and drops future packet directed to this mobility gateway.

5.5.2.2 STANDARD SWITCH CLASS

This class is restricted to access switches only. Parser of these mobility switches is limited to processing INTER_OVERLAY_CTRL messages with ARP headers only. The rest of packets or frames are considered standard network packets that are processed using conventional switching methodologies.

5.5.2.3 MOBILITY INITIATION CLASS

This class parses the initial packets sent from any foreign MN and triggers matching procedure in the Action Layer for authenticating and authorizing this MN at the origin home network before activating the mobility service. Classification Layer divides this class into two subclass; dynamic and static. DHCP packets are classified dynamic while ARP_REQUEST and standard IP packets are classified static.

STATIC MOBILITY NODE

This sub-parser is responsible for MNs with a static virtual path between home and foreign networks. Any mobility switch in this virtual path must have preconfigured profiles stored in the SDN controller indexed with MNs' hardware addresses. These profiles store authentication and authorization fields required for instant activation of these MNs once matching packets enter the mobility switch.

Either IP packets or ARP_REQUEST packets can initiate the activation process for a detected MN provided the stored registration profile type is 'STATIC' with 'IDLE' status. IP address field in the profile must match current IP address of detected MN. Registered values for the output port, HOME_ID, and DHCP_ CLIENT_ID are extracted from matching profile then appended to SYNOPSIS_VECTOR. The vector is forward directly to "Action Triggering Phase" for identifying suitable procedure in the Action Layer.

DYNAMIC MOBILITY NODE

This sub-class characterizes a roaming MN with dynamic virtual path between home and foreign networks. Home detector must have a preconfigured profile stored in the SDN Controller indexed with the roaming node's hardware address. Configuration defines the triple AAA (Authentication, Authorization, and Accounting) access controlling the roaming MN's foreign activities. It is optional to have a preconfigured profile in foreign detector. Mobility profiles of other switches in the dynamic virtual path can be pre-configured or created on-the-fly. Preconfigured profiles are called "Dynamic Profiles" while those established on-the-fly are called "On-Demand Profiles". Dynamic profiles have two types; home and foreign. "Home Dynamic Profile" is associated with home detector while "Foreign Dynamic profile" is associated with foreign detector. On-Demand Profile has only one type; that is "Foreign On-Demand Profile" regardless of the mobility entity to which it is associated.

"Identification Phase" parses DHCP message according to RFC 2131 [67][68]. DHCP message is identified according to "Optional Parameters Field" (OP_CODE) TAG 53 to be dispatched to matching sub-parser. There are two types of sub-parsers; DHCP_CLIENT Parser and DHCP_SERVER Parser. DHCP_CLIENT Parser is responsible for packets sent by MNs while the DHCP_SERVER Parser is responsible for packets sent by DHCP servers. The main DHCP parser creates a DHCP FIELD_VECTOR that is forwarded to matching sub-parsers. This vector represents the extracted DHCP fields required by next Parsing Layer phases. FIELD_VECTOR is appended by sub-parsers to SYNOPSIS_VECTOR and then forwarded to Action Layer. The following is the format of FIELD_VECTOR:

- **FIELD_VECTOR Format:** *{'STATE', 'NODE', 'IDENTIFIER', 'VENDOR', 'TIMEOUT':{ 'LEASE', 'RENEWAL', 'REBIND'}}*
  - ***'STATE'**: refers to 'DHCP Message Type' field used to convey the type of DHCP message. This field uses OP CODE TAG = 53.*
    - ✓ *CLIENT_DHCP Parser accepts the following legal values:*

      1: DHCPDISCOVER 3: DHCPREQUEST 4: DHCPDECLINE 7: DHCPRELEASE 8: DHCPINFORM
    - ✓ *SERVER_DHCP Parser accepts the following legal values:*

      2: DHCPOFFER 5: DHCPACK 6: DHCPNAK
  - '***NODE'***: *represents an order pair of ('CHADDR',' CIADDR'/ 'YIADDR') where;*
    - *'CHADDR': Client Hardware Address*
    - *'YIADDR': 'Your' (client) IP address with DHCP_OFFER message before 'BOUND' state.*
    - *'CIADDR': Client IP Address; the IP address of client requesting IP lease. This field is only filled in if client is in 'BOUND', 'RENEW' or 'REBINDING' state and can respond to ARP_REQUEST `.*

- ***'VENDOR'**: VENDOR_CLASS_ID field is optionally used by DHCP clients to identify vendor type and configuration of the DHCP client. This field uses OP_CODE TAG = 60.*
- ***'IDENTIFIER'**: DHCP_CLIENT_ID field is optionally used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. This field uses Op Code Tag = 61. For "On-Demand Profile", only extracted field is matched with "Mobility Route Detection Procedure" in the Action Layer. For "Dynamic profiles", the valid value for the preconfigured DHCP_ CLIENT_ID takes precedence over HOME_ID. If no route is found, the extracted DHCP_ CLIENT_ID field triggers a second search for next hop in the route to home network. This field is absent in DHCP_SERVER messages. Thus, the server reply uses reverse path of DHCP_CLIENT messages forward path.*
- '***RELAY'*** : *This represents an order pair of ('GIADDR',' GMOBID')*
  - *'GIADDR': Relay Agent IP address. This entity is responsible for forwarding DHCP messages between client and remote DHCP servers located outside the clients connected broadcast domains.*
  - *'GMOBID': This value is set to MOBILITY_ID of RELAY_AGENT_IP address provided this relay is a valid mobility entity.*
- ***'TIMEOUT'**: {'LEASE','RENEWAL','REBIND'}*

  This is a sub-vector representing all the timers that need tracking for activating/deactivating mobility service of roaming MN.
  - *'LEASE': Accepted period granted from DHCP server to DHCP client for retaining an offered IP address. Before lease expires, DHCP server must renew lease for DHCP client. This field uses OP_CODE TAG = 51.*
  - *'RENEWAL': Renewal timer is set by default to 50% of the lease period. When the timer goes off, the client transitions from 'BOUND' state to 'RENEWING' state. This field uses OP_CODE TAG = 58.*
  - *'REBIND': During 'RENEWING' state, the client keeps sending DHCP_REQUEST till receiving a reply from DHCP server. During this period of time, the client is still operating normally, from communicating users' perspectives. If no response from the server is received, eventually the 'REBINDING' timer expires. When timer goes off, client transitions from 'RENEWING' state to 'REBINDING' state. This field uses OP_CODE TAG = 59.*

- The following illustrates the operation of two DHCP sub-parsers in "Dynamic Mobility Node Class":
  - **DHCP_CLIENT Parser**

    This parser is responsible for DHCP messages sent from roaming MN. The goal is identifying MN's mobility profile type then formulating a SYNOPSIS_VECTOR to support "Action Triggering Phase" in selecting the right Action Layer's procedure as well as to update mobility overlay profile during "Dynamic Learning Phase". MN's message must match any of the conditions listed bellow with the same sequence, otherwise the packet is dropped.

    - ✓ MN's hardware address matches one of those indexing "Dynamic Idle Profiles".
    - ✓ Input port and VLAN TAG of the message as well as MN's hardware addresses match the indexes of a record in "Port Roaming Profiles".
    - ✓ MN's hardware address matches one of those indexing "Dynamic Roaming Profiles".
    - ✓ MN's hardware address matches one of those indexing "On-Demand Roaming Profiles".

    The idea behind giving idle nodes higher priority than roaming MNs is that OpenFlow switch rules handle activated MNs without resorting to SDN controller unless timeout difference occurs between mobility and OpenFlow timers. By default, this will lead that most of messages directed to SDN controller are from idle nodes. For "Port Roaming Profiles", these profiles require less search complexity as of using two indexes; port and VLAN before MN's hardware address. Activated roaming MN must find a matching record located unless moving to different location. Next two match processes are for detecting motion of roaming MN. Roaming Dynamic Profiles are by default higher priority than On-Demand profiles created on the fly without pre-configuration. "DHCP_CLIENT Parser" responds in two different ways to match process output:

    - ✓ Case 1: Match occurs:
      - Significant filled fields are extracted to be appended to SYNOPSIS_VECTOR. These fields include output port and motion status.
    - ✓ Case 2: No match occurs but valid DHCP_CLIENT_ID exists in the message:
      - Message is categorized 'ON-DEMAND' in SYNOPSIS_VECTOR. It is up to Action Layer to drop or forward the message.

    In both cases, SYNOPSIS_VECTOR bypasses "Dynamic Learning Phase" and is forwarded directly to "Action Triggering Phase". "Dynamic Learning Phase" is delayed till receiving a DHCP_ACKNOWLEDGE message. This delay is vital to avoid false join attempts and to identity spoofing and DDoS attacks.

- **DHCP_SERVER Parser**

This parser is responsible for DHCP messages sent from DHCP servers. The objective of this parser is validation of message fields that are vital for activation or deactivation or tracking roaming MN's leases. Valid server messages must satisfy one of the cases bellow:

- ✓ Case 1: The message is DHCP_REPLY and the bellow condition are satisfied:
  - DHCP switch buffer of mobility services is storing SYNOPSIS_VECTOR for a previous sent DHCP_REQUEST or DHCP_DISCOVERY indexed with mobility MN's hardware address.
  - Input port of DHCP_REPLY is the output port in SYNOPSIS_VECTOR. That's to guarantee using the same virtual path and to protect against any spoofing attacks.
  - Output port of DHCP_REPLY is the input port field of SYNOPSIS_VECTOR stored in switch buffer for DHCP_REQUEST or DHCP_DISCOVERY.
- ✓ Case 2: DHCP server message is for an already activated roaming MN.
  - Port roaming profile is retrieved with the input port of DHCP server message as an index followed by VLAN TAG followed by hardware address of roaming MN.
  - Output port of DHCP server message is extracted from the roaming profile.

In case 2, SYNOPSIS_VECTOR is forwarded directly to "Action Triggering Phase" bypassing the "Dynamic Learning Phase" as of being updated during the activation process. For DHCP_REPLY messages with valid offers in case 1; both SYNOPSIS_VECTOR of DHCP_REPLY message and that of delayed DHCP_REQUEST message are passed to "Dynamic Learning Phase" then to "Action Triggering Phase". On the other hand, DHCP_REPLY message with rejected status or those not belonging to any of the two stated cases are passed directly to "Action Triggering Phase".

5.5.2.4 MOBILITY MONITORING CLASS

This class is responsible for activating non populated or expired switch OpenFlow rules. Non populated switch OpenFlow rules are activated when a roaming MN with activated 'ON-DEMAND' or 'DYNAMIC' profile initiates standard communication. SDN controller populates OpenFlow rules to the switch to establish the virtual path between foreign and home networks. After flow is installed on all switches, no packet is forward to the controller till flow timers expire.

Reactivation of expired switch OpenFlow rules happen when OpenFlow timer expires while mobility service timer is still valid. This can occurs frequently as of roaming MN inactivity. In both cases, the parameter stored in roaming mobility profile is retrieved for fast re-activation.

MN's hardware address is matched against the roaming profiles in the following sequence; 'STATIC' – 'PORT' – 'DYNAMIC' – 'ON-DEMAND'. In this class, no SYNOPSIS_VECTOR is created for 'STATIC' – 'PORT' profiles. The message is returned to the Detection Layer for fast switching using the profile output port. For 'DYNAMIC' or 'ON-DEMAND' profiles, SYNOPSIS_VECTOR is created to identify if roaming MN performed an accepted motion. SYNOPSIS_VECTOR is forwarded directly to "Action Triggering Phase".

5.5.3 DYNAMIC LEARNING PHASE

In this phase, "Local Gateway Profile" and "Remote Gateway Profile" use IN_BAND_CTRL messages to dynamically register local and remote gateways' hardware addresses, respectively, as well as their connected ports to other side mobility gateways. The update process happens with the first parsed packet entering the mobility switch from a registered gateway IP address if the hardware field value is missing. The same learning mechanism is used to update "Mobility Switch Profile" with the mobility switch management port and hardware address and to update "Mobility To Port Table" with the overlay network devices' hardware addresses and their connected ports extracted from the OVERLAY_CTRL messages. Moreover, in mobility activation messages, MOBILITY_ID of DHCP_RELAY in SYNOPSIS_VECTOR of dynamic roaming MN is used to update the mobility overlay profiles with hardware addresses and connected port of the entity relaying the DHCP messages.

Once registered profiles are updated, these fields are never changed unless mobility service in the SDN Controller is restarted. This precaution is enforced as a security countermeasure to filter out spoofing attacks directed to the registered entities. The mobility security policy drops future packets sourced from any registered IP address entering from a different port or with a different hardware address than those registered. The dynamic learning process is critical to eliminate broadcast of future packets to all the switch ports and to avoid re-triggering of dynamic topology discovery procedures of Action Layers' procedures as identity discovery procedure and overlay discovery procedure described in sections 5.6.6 and 5.6.9 respectively.

5.5.4 ACTION TRIGGERING PHASE

After Parsing Layer successfully finishes "Identification Phase" and "Dynamic Learning Phase", the output port mapped to the destination field is retrieved from registered profile if previously learned. Based on the output of "Identification Phase", Parsing Layer triggers a selected procedure in the Action Layer to determine next action based on SYNOPSIS_ VECTOR. The following summarizes the relation between "Identification Phase" and "Triggering Phase".

1. **MOBILITY CONTROL MESSAGES**
   a. **OVERLAY CTRL MESSAGES**
      i. **INTRA_OVERLAY_CTRL MESSAGES**
         - ARP HEADER ➢ TRIGGER Action Layer: "Identity Discovery Procedure"
         - ICMP HEADER & IHL > 5 ➢ TRIGGER Activation Layer: "Service Orchestration Procedure"

      ii. **INTER_OVERLAY_CTRL MESSAGES**
         - ARP HEADER ➢ TRIGGER Action Layer: "Overlay Discovery Procedure"

      iii. **OTHERWISE** ➢ LOG ERROR
         ➢ DROP PACKET

   b. **IN_BAND_CTRL MESSAGES**
      i. **LOCAL GATEWAY CONTROL MESSAGES**
         - ARP/ICMP HEADER ➢ TRIGGER Action Layer: "Standard Switching Procedure"

      ii. **REMOTE GATEWAY CONTROL MESSAGES**
         - GRE HEADER sourced from a registered Remote Gateway with no configured GRE tunnel
            ➢ TRIGGER Action Layer: "Inter-Domain Routing Procedure"
         - GRE HEADER sourced from a registered Remote Gateway with Active GRE tunnel
            ➢ TRIGGER Action Layer: "Standard Switching Procedure"

      iii. **OTHERWISE** ➢ LOG ERROR
         ➢ DROP PACKET

2. **STANDARD SWITCH CLASS**
   ✓ Access switch **AND** non OVERLAY_CTRL message
      ➢ TRIGGER Action Layer: "Standard Switching Procedure"

3. **MOBILITY INITIATION CLASS**
   a. **STATIC MOBILITY NODE**
      ✓ IP Packet **OR** ARP for MN matching STATIC profile with IDLE status
         ✓ Output Port registered
            ➢ TRIGGER Action Layer: "Mobility Switching Procedure"
         ✓ Valid DHCP_CLIENT_ID **OR** HOME_ID registered
            ➢ TRIGGER Action Layer: "Mobility Route Detection Procedure"
         ✓ Invalid Record ➢ LOG ERROR
            ➢ DROP PACKET
      ✓ OTHERWISE ➢ TRIGGER Classification Layer: "Mobility Monitoring Class"

b. DYNAMIC MOBILITY NODE

i. DHCP_CLIENT Messages

- DYNAMIC Profile **AND** valid DHCP_CLIENT_ID or HOME_ID
  - ✓ Home Detector ➢ PUSH SYNOPSIS_VECTOR to DHCP switch buffer
    ➢ TRIGGER Action Layer: "Recursive Relay Procedure"
  - ✓ Output Port registered
    ➢ TRIGGER Action Layer: "Recursive Relay Procedure"
  - ✓ OTHERWISE ➢ TRIGGER Action Layer: "Mobility Route Detection Procedure"
- ON_DEMAND Profile AND valid DHCP_CLIENT_ID or HOME_ID extracted
  ➢ TRIGGER Action Layer: "Mobility Route Detection Procedure"
- PORT_ROAMING Profile ➢ TRIGGER Action Layer: "Recursive Relay Procedure"
- OTHERWISE ➢ LOG ERROR
  ➢ DROP PACKET

ii. DHCP_SERVER Messages

- PORT_ROAMING Profiles ➢ TRIGGER Action Layer: "Recursive Relay Procedure"
- POP SYNOPSIS_VECTOR of DHCP_CLIENT message from DHCP switch Buffer
  ➢ TRIGGER Action Layer: "Recursive Relay Procedure"
  ➢ TRIGGER Action Layer: "Direct Activation Procedure"
- OTHERWISE ➢ LOG ERROR
  ➢ DROP PACKET

4. MOBILITY MONITORING CLASS

- STATIC/ PORT_ROAMING Profiles
  ➢ TRIGGER Action Layer: "Mobility Switching Procedure"
- STATIC/DYNAMIC/ON_DEMAND Roaming Profiles
  ➢ TRIGGER Action Layer: "Motion Detection Procedure"
- OTHERWISE ➢ LOG ERROR

➢ DROP PACKET

5.6 ACTION LAYER

5.6.1 OVERVIEW

The utmost objective of this layer is dynamic learning of forward virtual path between foreign and home networks. Backward virtual path is the reverse direction of forward path. Learning process is fulfilled by integrating the output of nine procedures in the Action layer, shown in figure 5-5. The parsing layer triggers the mobility route detection procedure. The output of this procedure triggers the rest of procedures till reaching a conclusion of either dropping packets or forwarding to the Activation layer.

Figure 5-5: Action Layer Procedures

The driving force behind virtual path creation is the urgent need for wire speed hardware switching while hiding the complexity of traditional software routing mechanisms. This path is composed of mobility switches' hardware ports found in the path between foreign and home networks. The process for identifying hardware ports directed to a specific home network is run once per switch despite the number of roaming MN using this path. In other word, the virtual path serves the connectivity between foreign and home networks and uses dynamic procedure to locate the members' ports. The first MN using this virtual path suffers from the time complexity required for running Action Layer's procedures. Once the output port is determined to next hop, mapping of NEXTHOP_ID and HOME_ID are stored according to the type of communication in mobility intra-overlay or inter-overlay or inter-domain table for instant forwarding of future packets using this virtual path.

On initiation of standard packet to home network, the SDN controller installs OpenFlow rules on switches for wire speed forwarding. Home network is identified by MOBILITY_ID of home access switch for intra-overlay mobility or by that of home relay switch for inter-overlay mobility or by that of home gateway for inter-domain mobility. On the other hand, foreign network is identified by MOBILITY_ID of foreign detector switch in intra-overlay or by that of foreign relay switch in inter-overlay mobility or by that of foreign gateway in inter-domain mobility.

Action Layer uses two-phase methodologies to dynamically discover virtual path toward MN's home network. The first phase is to identify next hop identifier or next hop IP address using "Mobility Route Detection Procedure" while the second phase is to locate next hop port toward home network based on action selected in the first phase. There are two types of actions, 'SWITCH' action for port identification in inter-overlay or intra-overly mobility and 'TUNNEL' action for port identification in inter-domain mobility. Figure 5-6 shows an illustrative flow chart for two-phase methodologies.

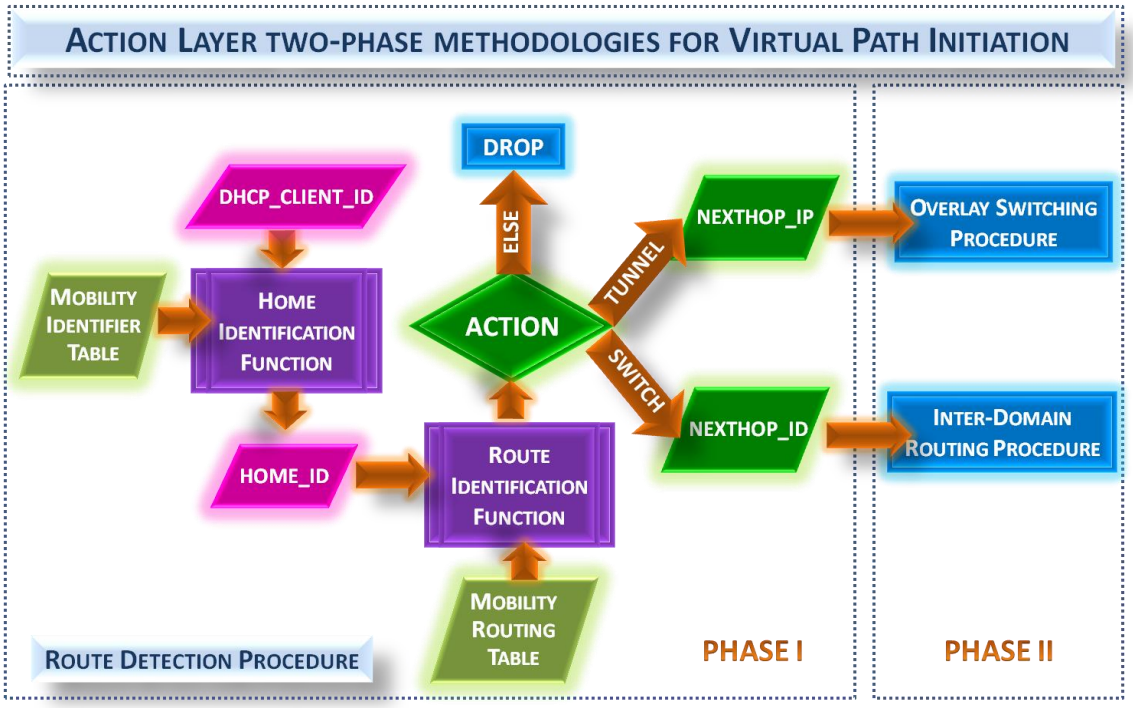


Figure 5-6: Action Layer Two-Phase Methodologies for Virtual Path Initiation

5.6.2 MOBILITY ROUTE DETECTION PROCEDURE

This procedure represents the first phase in the Action Layer two-phase methodologies. The objective is the identification of next hop and action required to reach it. To accomplish both targets; the valid values for DHCP_ CLIENT_ID and HOME_ID are extracted from SYNOPSIS_VECTOR generated by Parsing Layer. If both exist then DHCP_CLIENT_ID takes precedence over HOME_ID. If two DHCP_ CLIENT_IDs are detected, the one extracted from the preconfigured "Dynamic Profile" takes precedence over preconfigured HOME_ID while last precedence is for extracted DHCP_CLIENT_ID from DHCP_REQUEST message.

PROCEDURE PSEUDOCODE

MAIN FUNCTION:

- Place valid Identifiers in an ordered list sorted by precedence
- For each VALUE in Identifiers ordered list:
  - IF VALUE == DHCP_CLIENT_ID:
    - HOME_ID = PARSE "Mobility Identifier Table" using HOME IDENTIFICATION FUNCTION[VALUE]
      - ✓ IF SUCCESS; MOBILITY_ID = HOME_ID

    ELSE: MOBILITY_ID = VALUE
  - IF MOBILITY_ID == HOME_ID:
    - NEXTHOP_ID = ROUTE IDENTIFICATION FUNCTION[MOBILITY_ID]
      - ✓ IF SUCCESS:

        ROUTE [ACTION] == 'SWITCH'➢TRIGGER Action Layer "Overlay Switching Procedure"

        ROUTE [ACTION] == 'TUNNEL'➢TRIGGER Action Layer "Inter-Domain Routing Procedure"
      - ✓ ELSE: FALSE

5.6.2.1 HOME IDENTIFICATION FUNCTION

This function uses "Mobility Identifier Table" and DHCP_CLIENT_ID, as shown in figure 5-6, for finding HOME_ID mapped to the longest matched sequence in DHCP_ CLIENT_ID.

- ***EXAMPLE:***

  MOBILITY IDENTIFIER TABLE: {'0020':{'120':'CP1'},'DEFAULT':'000'}

  This means:
  - *Any DHCP_CLIENT_ID in format 0020-120-xxxxxxxx will be mapped to HOME_ID: CP1*
  - *Non matching DHCP_CLIENT_ID will use DEFAULT_HOME_ ID: '000'*

FUNCTION PSEUDOCODE

- GENERATE an ARRAY by splitting DHCP_CLIENT_ID according to defined splitter character.
- Records = "Mobility Identifier Table"
- For each ITEM in ARRAY:
  - ✓ IF ITEM in RECORDS ➢ RECORDS = RECORDS [Item]
  - ✓ ELIF DEFAULT EXISTS: ➢ NEXTHOP = RECORDS [DEFAULT] ➢ RETURN NEXTHOP
  - ✓ ELSE: RETURN None
- IF Records is valid MOBILITY_ID ➢ NEXTHOP = Records ➢ RETURN NEXTHOP
- RETURN None

5.6.2.2 ROUTE IDENTIFICATION FUNCTION

This function uses "Mobility Routing Table" and HOME_ID for finding best matched route and action toward next hop in the virtual path to home network. The second phase is responsible for determining the output port toward home network. There are several methods for parsing "Mobility Routing Table" to get the best matching route toward home network but the one selected here is similar to that used for parsing standard routing tables. The selection might not be optimum but is guided by simplicity for future expansions if variable length subnet is introduced for sub-domain or sub-overlay identification. Either HOME_ID belongs to Private Overlay MOBILITY_ID Class or to Public MOBILITY_ID Class; the same searching mechanism is used. Pseudocode below shows how "Mobility Routing Table" is parsed.

FUNCTION PSEUDOCODE

- Best = None
- Home Virtual IP = VIRTUAL_IP_FUNCTION[HOME_ID]
- FOR each Record in "Mobility Routing Table":
  - Destination Virtual IP = VIRTUAL_IP_FUNCTION [Record Destination IP]
  - ✓ IF Destination VIRTUAL_IP == Home VIRTUAL_IP: ➢ Best = Record [Route] ➢ Break
  - ✓ IF (Destination VIRTUAL_IP AND Destination Mask) == (Home VIRTUAL_IP AND Destination Mask)
    - ✓ IF Best Match AND (Record Mask >> Best Match(Destination Mask)):
      - ➢ Best = Record [Route]
- RETURN Best

5.6.2.3 VIRTUAL IP FUNCTION

This function maps input MOBILITY_ID to a virtual IP in the format of standard IP address using ASCII decimal mapping of MOBILITY_ID. If length of MOBILITY_ID is three, Ad-hoc prefix '233' is in the first octet to create multicast virtual IP for intra-overlay and inter-overlay communications. MOBILITY_ID of length 4 is used for inter-domain communications

FUNCTION PSEUDOCODE

- ✓ Length(MOBILITY_ID) == 3
  - ➢ CLASS_ID = PRIVATE_OVERLAY_MOBILITY_IDs
  - ➢ Last 3 Octets = Decimal ASCII (MOBILITY_ID [CHAR [1~3])
  - ➢ VIRTUAL_IP = [AD-HOC Prefix<233>]. Last 3 Octets
- ✓ Length(MOBILITY_ID) == 4
  - ➢ CLASS_ID = PUBLIC_OVERLAY_MOBILITY_IDs
  - ➢ VIRTUAL_IP = Decimal ASCII (MOBILITY_ID [CHAR [1~4])
- RETURN VIRTUAL_IP, CLASS_ID

5.6.3 Overlay Switching Procedure

The first phase in two-phase methodologies of the Action Layer either ends with 'TUNNEL' or 'SWITCH' action to reach next hop in the virtual path between home and foreign networks. "Overlay Switching Procedure" represents the second phase response toward 'SWITCH' action triggered to discover the switch port that is member of the virtual path for either inter-overlay or intra-overlay mobility. The flow chart in figure 5-7 summarizes the sequence of "Overlay Switching Procedure".

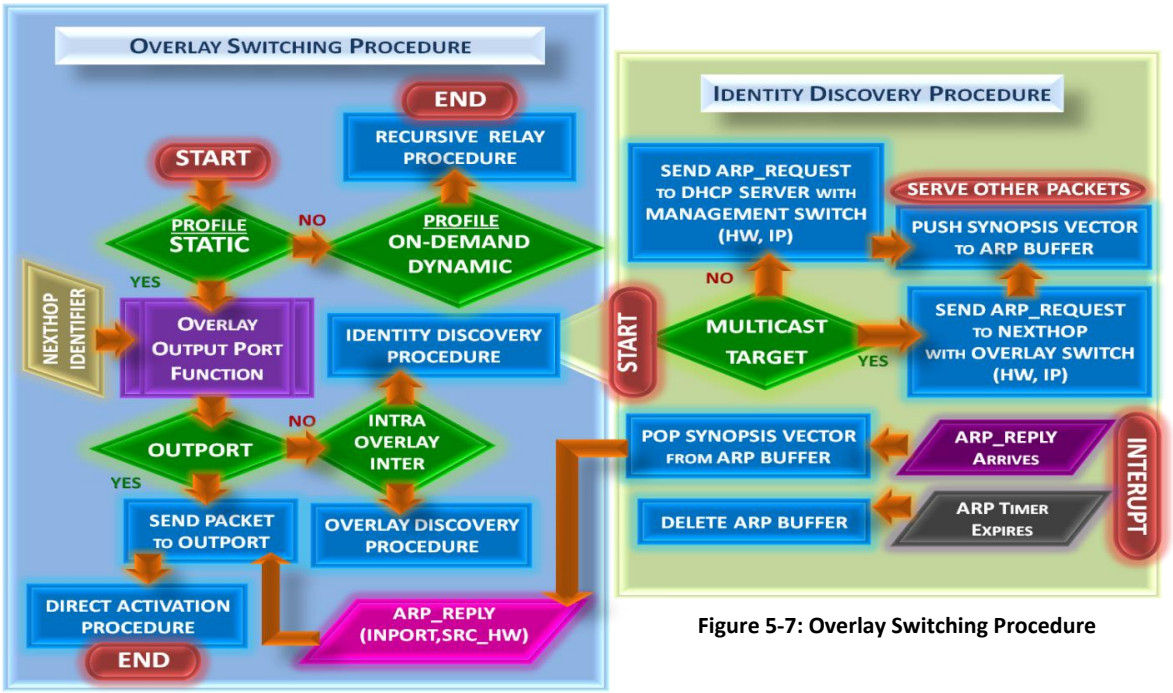


Figure 5-7: Overlay Switching Procedure

Procedure Pseudocode

Main Function:

- IF Profile type == 'STATIC'
  - ➢ NEXTHOP_VECTOR = OVERLAY_OUTPUT_ PORT_FUNCTION[Profile, NEXTHOP_ID]
  - ✓ IF NEXTHOP_VECTOR == None:
    - ✓ IF Intra-Overlay ➢ TRIGGER "Identity Discovery Procedure"→ OUTPORT, NEXTHOP_HW
    - ✓ IF Inter-Overlay ➢ TRIGGER "Overlay Discovery Procedure"→ OUTPORT, NEXTHOP_HW
  - ➢ SEND Packet through OUTPORT ➢ RETURN "Direct Activation Procedure"
- ELIF Profile type == 'Dynamic' or 'On-Demand': ➢ RETURN "Recursive Relay Procedure"

5.6.3.1 OVERLAY OUTPUT PORT FUNCTION

This function tries to map input OVERLAY_ID to output type, next hop output port, next IP address, and next hardware address. These parameters are required to forward initial packets used to identify the overlay virtual path between home and foreign networks.

FUNCTION PSEUDOCODE

- IF NEXTHOP_ID in "Mobility Intra-Overlay Table" :
  - RETURN {INTRA, OUTPORT, NEXTHOP_IP, NEXTHOP_HW}
- ELIF NEXTHOP_ID in "Mobility Inter-Overlay Table":
  - RETURN {INTER, OUTPORT, NEXTHOP_IP, NEXTHOP_HW}
- ELSE: RETURN None

5.6.4 INTER-DOMAIN ROUTING PROCEDURE

"Inter-Domain Routing Procedure" represents the preliminary step toward initialization of virtual path in inter-domain mobility across local and remote gateways. Tunneled virtual path can be a direct path between home and foreign networks or a recursive path edged with home and foreign mobility gateways and cored with transient mobility gateways. In either case, the same sequence is adopted but the covert behind recursive design is trust relation between home and foreign networks. For small deployment, direct path is enough as remote public gateways IP can be statically registered in both networks. Authentication, authorization, and encryption enforcement between gateways are straight forward as of the simplicity in statically registering of shared secrets or integrating public key public key cryptography.

Enterprise deployments are far more complicated. Preserving enterprise privacy and security policy enforce resorting to certificate authority trust relationship or creating dynamic keys exchange protocol for authentication, authorization, and encryption to establish tunnel on the fly. Bearing in mind these impedances, recursive tunnels become a straight forward solution without any key exchange complications as mobility gateways can simply accept dynamic tunnel initiation from registered gateways. For this reason, the architecture adopts trust relationship with dynamic recursive hierarchical form for tunnel establishment in enterprise roaming mobility service. First level is trust relation cross countries regulators then followed by second level countries regulators and operators …etc.

Prototyping experiments in this research are a proof of concept thus simple GRE tunnels with a previous defined list of accepted remote tunnel gateways. For enterprise deployments, IPSec encrypted tunnels can be adopted with Diffie-Hellman or RSA signatures and RSA encrypted nonces to ensure privacy

and integrity cross communicating peers. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel [88]. RSA is public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provide non-repudiation and RSA encrypted nonces provide repudiation [89].

There are two different methods for triggering "Inter-Domain Routing Procedure". The first method is response to first phase in Action Layer two-phase methodologies for virtual path initiation. Once the SDN controller detects a roaming MN at foreign gateway, the procedure is triggered to establish a virtual path toward remote SDN controller for inter-domain mobility. In case of direct virtual path, tunnel initiator is foreign gateway while terminator is home gateway. The second method is recursive virtual path establishment. In this case, the initiator can be foreign or transient gateway while the terminator can either be a transient or a home gateway. The terminator side of tunnel dynamically triggers this procedure once detecting IN_BAND_CTRL tunnel message. Parsing Layer triggers this procedure to forward IN_BAND_CTRL message to the management interface of remote registered gateway. Management interface is responsible for GRE header de-encapsulation or decryption of IPSec header if encryption exists. This interface re-forwards the message without IPSec or GRE header to terminator gateway as a standard packet to be switched through overlay network or re-tunneled again till reaching home detector. The flow chart in figure 5-8 summarizes "Inter-Domain Routing Procedure".

PROCEDURE PSEUDOCODE

MAIN FUNCTION:

- (STATUS,GRE PORT) = ACTIVATE_TUNNEL_FUNCTION
- IF TUNNEL STATUS == 'FULL': ➢ LOG ERROR ➢ DROP PACKET
- IF IN_BAND_CTRL Packet ➢ Fast Switching to Management Int. ➢ RETURN
- IF STATIC ➢ APPEND Node to "Tunnel Roaming List"
  ELIF Profile Type == ON-DEMAND' OR 'DYNAMIC' ➢ APPEND Node to "Tunnel Pending List"
- IF TUNNEL STATUS == 'NEW': ➢ PUSH SYNOPSIS_VECTOR to GRE buffer
  ➢ SERVE Other Packets
  ➢ PORT REGISTERED EVENT: ➢ GRE PORT = Register GRE Port
  ➢ POP SYNOPSIS_VECTOR from GRE buffer
- IF STATIC ➢ RETURN "Direct Activation Procedure"
  ELIF Profile Type=='ON-DEMAND' OR 'DYNAMIC': ➢ PUSH Synopsis Vector to GRE Buffer
  ➢ Fast Switching to GRE Port ➢ RETURN

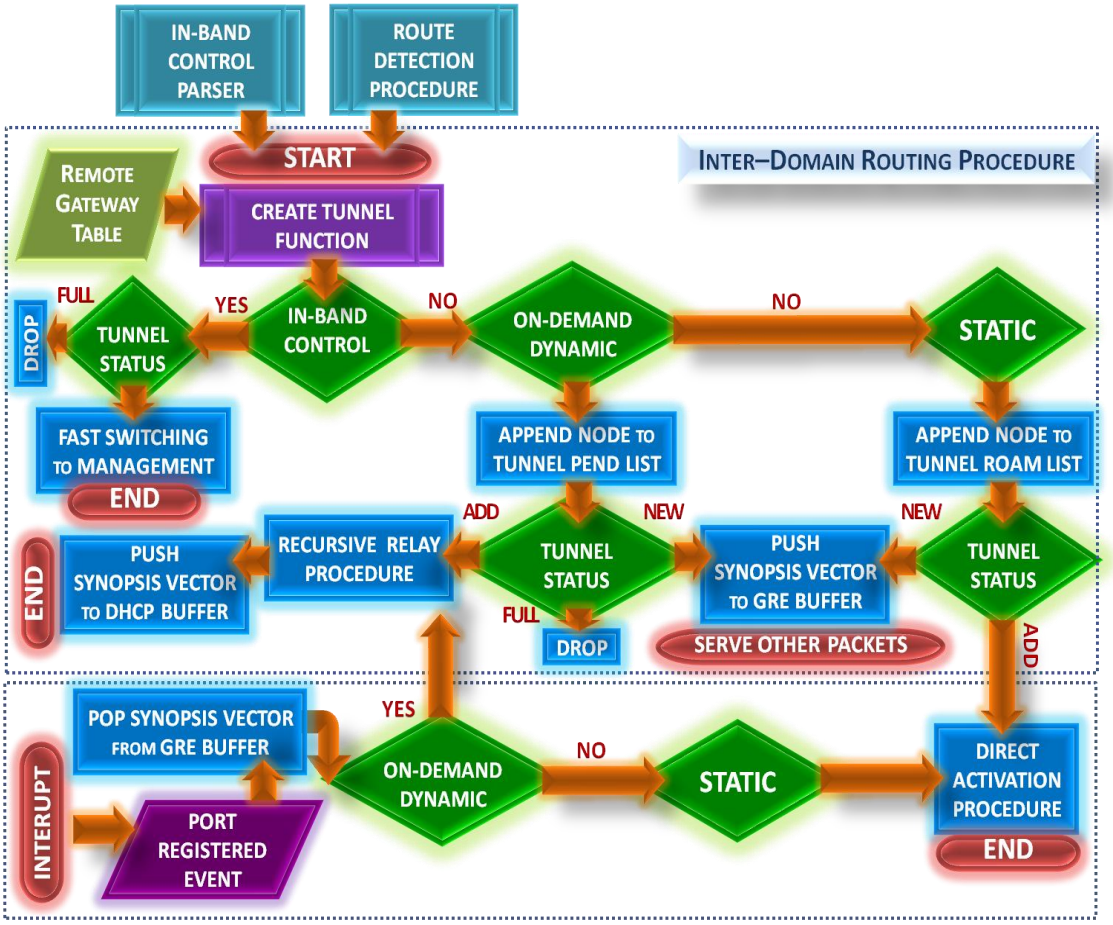


Figure 5-8: Inter-Domain Routing Procedure

5.6.4.1 CREATE TUNNEL FUNCTION

This function creates a logical tunnel port on the management interface of mobility gateway to communicate with remote mobility gateway. The SDN controller checks "Mobility Tunnel Table" to see if an active tunnel is already connected to remote mobility gateway. If active tunnel exists, the logical port is returned with status 'ADD'. The status instructs the calling procedure to append roaming MN if exists to tunnel roaming list if MN has a static profile or to pending list if MN has 'On-Demand' or 'Dynamic' profile. If tunnel has never exists, the SDN controller generates a random logical identifier for the required tunnel. If maximum number of tunnels is reached, the function returns 'FULL' status. For each logical identifier, the SDN controller creates an OpenFlow tunnel port on the management interface to communicate with the remote gateway then update both "Mobility Tunnel Table" and "Remote Gateway Profile". After successful configuration, the function returns 'NEW' status.

FUNCTION PSEUDOCODE

- CHECK "Remote Tunnel Profile":
  - ✓ IF Tunnel exists: ➢ RETURN (GRE PORT, 'ADD')
- GENERATE Tunnel Logical Identifier:
  - ✓ IF Failure: ➢ RETURN (None, 'FULL')
- SSH to Management Interface of Mobility Gateway:
  - ✓ CREATE Tunnel Interface ➢ UPDATE Routing Table
  - ✓ UPDATE Remote Tunnel Profile ➢ UPDATE Mobility Tunnel Table
  - ➢ RETURN (None, 'NEW')

5.6.5 RECURSIVE RELAY PROCEDURE

This procedure enforces mobility switches, relays, and gateways to act as proxies or relay agents of roaming MNs with Dynamic or On-Demand profiles for initializing the virtual paths and tracing the exchange of control messages like DHCP_REQUEST, DHCP_REPLY, DHCP_ACKNOWLEDGMENT …etc. Proxies or relay agents feature facilitates for the SDN controller traceability of authentication, authorization, and accounting messages exchanged between roaming MNs and home networks while delivering maximum network throughput and wire-speed performance for activated roaming profiles. The clue behind such major accomplishments is the separation of OpenFlow rules for standard MN's packets from activation and control messages. No OpenFlow rules are populated to mobility switches for activation and control messages to keep them traced by the SDN controllers for activation, deactivation, and accounting of mobility service. OpenFlow rules are only populated for MN's standard packets guided by the Activation Layer.

The presence of relay feature reliefs the SDN controller from parsing all MNs' packets. Only the relayed packet between mobility switch and gateways as well as the first standard packet from MN, that triggered virtual path activation, are forwarded to the SDN controller while the rest of packets are wire speed forwarded by OpenFlow rules installed on the mobility switches. Experiments results reveal dramatic performance improvement with such approach compared to full packets forwarding to the SDN controller. Moreover, the performance of roaming MNs with enabled mobility services inside the overlay are not only equivalent to that estimated between foreign and home networks using standard network communications but can also exceed if Quality of Service (QoS) is enforced for guaranteed bandwidth service with maximum reliability. Figure 5-9 shows a brief flow chart of the Pseudocode stated bellow.

PROCEDURE PSEUDOCODE

MAIN FUNCTION:

- MANEUVER_VECTOR = RETRIEVE_DHCP_NEXT_FUNCTION

✓ IF NOT valid OUTPORT: ➢ OUTPORT = BROADCAST

✓ IF NOT NEXTHOP _ HW:

➢ (OUTPORT, NEXTHOP _ HW) = "Identity Discovery Procedure"

- SERIALIZE New DHCP Message from MANEUVER_VECTOR
- FORWARD Serialized DHCP Message

✓ IF DHCP_CLIENT Message:

➢ PUSH SYNOPSIS_VECTOR to DHCP Buffer ➢ RETURN

✓ IF DHCP_SERVER Message:

➢ RETURN "Dynamic Activation Procedure"

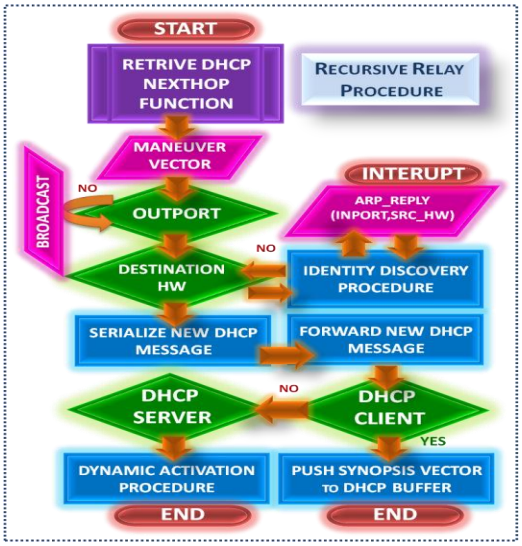


Figure 5-9: Recursive Relay Procedure

5.6.5.1 RETRIEVE DHCP NEXT FUNCTION

This function is the core of "Recursive Relay Procedure" responsible for separation between control messages, monitored by the SDN controller, and MNs' standard packets. This function identifies valuable parameters in SYNOPSIS_VECTOR created by the Parsing Layer. These parameters include the type of route to next hop as well as foreign, home, relay, and next hop mobility identifiers. Based on these parameters a new vector is created. This vector is called MANEUVER_VECTOR. Its function is instructing which value inside the message to change before forwarding to next hop. This ensures that DHCP message can never be forwarded by OpenFlow rules and is always traced by the SDN controller. The following Pseudocode describes what is identified in SYNOPSIS_VECTOR to create MANEUVER_ VECTOR.

FUNCTION PSEUDOCODE

- IF ROUTE == GATEWAY:
  - ✓ IF CASE == DHCP_CLIENT Message:
    - ➢ RETURN {RELAY_IP=VIRTUAL_IP_FUNCTION[Public MOBILITY_ID], SOURCE=(VIRTUAL_HW, RELAY_IP)}
  - ✓ IF CASE == DHCP_SERVER Message:
    - ✓ IF NEXTHOP_ ID in "Mobility Inter-Zone Table":
      - ➢ RETURN {DESTINATION = (NEXTHOP_HW, NEXTHOP_IP), OUTPORT = NEXTHOP_PORT}
- IF ROUTE == SWITCH:
  - SWITCH_VIRTUAL= (SWITCH_VIRTUAL_HW, VIRTUAL_IP_FUNCTION [Private MOBILITY_ID])

- ✓ IF CASE == DHCP_SERVER Message AND Foreign Detector: ➢ RETURN { DESTINATION = NODE }
- ✓ ELIF CASE == DHCP_CLIENT Message AND Home Detector:
  - ➢ RETURN {SOURCE=SWITCH_MANAGEMENT,DESTINATION=DHCP_SERVER, OUTPORT=DHCP_PORT, RELAY = SWITCH_MANAGEMENT_IP, UDP_SRC = UDP_DST = DHCP_SERVER_PORT}
- ✓ IF NEXTHOP_ ID in "Mobility Intra-Overlay Table" or in "Mobility Inter-Overlay Table":
  - ➢ DESTINATION = (NEXTHOP _HW, NEXTHOP_IP) ➢ OUTPORT= NEXTHOP _PORT
  - ✓ IF NOT Home Detector AND DHCP_SERVER Message : ➢ RETURN {DESTINATION, OUTPORT}
  - ✓ IF DHCP_SERVER Message AND Home Detector:
    - ➢ RETURN { SOURCE=SWITCH_MANAGEMENT, DESTINATION,UDP_SRC = DHCP_SERVER_PORT, UDP_DST = DHCP_CLIENT_PORT, OUTPORT}
  - ✓ IF DHCP_CLIENT Message:
    - ✓ IF NOT Foreign Detector: ➢ RETURN {DESTINATION, RELAY= SWITCH_VIRTUAL_IP, OUTPORT}
    - ➢ RETURN {SOURCE=SWITCH_VIRTUAL,DESTINATION,RELAY=SWITCH_VIRTUAL_IP, OUTPORT}

RETURN False

5.6.6 IDENTITY DISCOVERY PROCEDURE

The proposed mobility architecture is scalable for carrier grade deployments. In enterprise deployment, an overlay domain representing a branch in the overlay network can include hundreds of access switches connected to several detectors switches anchored at mobility RS connecting other branches in the same overlay. Creating a virtual path between home and foreign networks enforces every mobility detector or relay or gateway to map its switch ports to the MOBILITY_ID of connected entity from other tiers. Furthermore, MG tier needs to keep track of MOBILITY_ID of both DS and AS tiers. The home Access switch MOBILITY_ID serves as HOME_ID of MN, while foreign DS MOBILITY_ID serves as MN's foreign MOBILITY_ID. Static mapping between switch ports and MOBILITY_IDs of connected entities from other tiers is almost impossible in enterprise deployment thus the architecture procedure developed "Identity Discovery procedure" for dynamic mapping. "Overlay Switching Procedure" and "Recursive Relay Procedure" trigger this procedure to dynamically discover the virtual path between home and foreign network in intra-overlay communication. The same ideology is adopted by "Overlay Discovery Procedures" for inter-overlay communication. Furthermore, "Recursive Relay Procedure" triggers this procedure but with the switch IN-BAND IP address to discover connected ports and hardware address of target networks entities as DHCP servers, mobility gateway, …etc.

To accomplish the dynamic discovery process for hardware address as well as connected port of a target network entity or a target mobility switch that the initiator mobility switch needs to communicate with, the calling procedure updates SYNOPSIS_VECTOR with the current status then pushes the vector to ARP switch buffer indexed with requested entity IP address. The SDN controller sends standard ARP_REQUEST to the target entity that requires identification through certain port or port group or to all of initiator switch ports if nothing is instructed. ARP_REQUEST message uses the virtual multicast IP address of the initiator mobility switch for overlay control messages and the management switches IP for IN-BAND control messages. The initiator mobility switch serves other packets till ARP_REPLY message arrives. Once a matching record is popped out of the buffer, SYNOPSIS_VECTOR is updated with input port and source address of ARP_REPLY message then forwarded to the calling procedure. The flow chart in figure 5-7 describes this procedure sequence and its integration with "Overlay Switching Procedure". All mobility switches in the path between initiator and target entities use source address and input port of ARP_REQUEST and ARP_REPLY messages to update mobility inter-overlay, intra-overlay, and inter-domain tables for future usage.

PROCEDURE PSEUDOCODE

MAIN FUNCTION:

- IF TARGET _IP NOT VIRTUAL_IP:
  - ➢ SEND ARP_REQUEST to DESTINATION _IP using Management Switch (HW, IP)

  ELSE: ➢ SEND ARP_REQUEST to DESTINATION _IP using Virtual Switch (HW, IP)
- PUSH SYNOPSIS_VECTOR to ARP Switch Buffer ➢ SERVES Other Packets

  ➢ IF ARP_REPLY Arrives ➢ POP ARP Switch Buffer

  ➢ RETURN (INPUT PORT of ARP_REPLY, SOURCE_HW of ARP_REPLY)

  ➢ INTERRUPT: ARP Timer Expires ➢ LOG ERROR ➢ DROP PACKET ➢ DELETE BUFFER

5.6.7 STANDARD SWITCHING PROCEDURE

This procedure is responsible for standard learning switch functionality. Once a packet enters the switch, the source hardware address is learned then stored in the switch Content Addressable Memory (CAM) mapped to the input port. Destination hardware address is identified by the calling procedure to determine the output port. If no output port is given when triggering this procedure, CAM is checked as well for a match. If no match, the packet is broadcasted to all ports. However, if an output port is detected, the packet is forwarded through this port and OpenFlow rules are installed on the switch to avoid interrupting the SDN controller again.

PROCEDURE PSEUDOCODE

- MAP SOURCE_HW to INPORT in CAM TABLE

✓ IF NO OUTPORT: ➢ MATCH Destination HW with CAM TABLE to retrieve Output port

✓ IF OUTPORT: ➢ FORWARD Packet

➢ POPULATE OpenFlow Rule

ELSE: ➢ BROADCAST Packet to all switch ports

5.6.8 MOTION DETECTION PROCEDURE

The motion of roaming MN with enabled mobility profile can simply be detected by matching the packet input port against that stored in roaming 'Static' or 'Dynamic' or 'On-Demand' profiles during Identification Phase of Parsing Layer. Once motion is confirmed, SYNOPSIS_VECTOR is updated during the Parsing Layer Identification phase to triggering this procedure. The response to motion detection varies according to the type of mobility switch and port registration in 'Static' or 'Dynamic' profile.

PROCEDURE PSEUDOCODE

- IF Profile Type == 'STATIC' OR 'DYNAMIC' AND Source Input Port Registered:
  - ➢ ADD OpenFlow Rule to DROP Packets from HW address and Input Port
  - ➢ LOG ERROR
  - ➢ DROP Packet
  - ➢ RETURN FAILURE
- ELIF Foreign Detector:
  - ➢ PUSH SYNOPSIS_VECTOR to ARP switch buffer
  - ➢ SEND ARP_REQUEST to DESTINATION _IP using Management Switch (HW, IP) on Previous Port

IF ARP_REPLY Arrived ➢ POP ARP switch buffer

- ➢ ADD OpenFlow Rule to DROP Packet from HW address and Input Port of Buffered Packet
- ➢ LOG ERROR
- ➢ DROP Buffered Packet
- ➢ RETURN False

Interrupt: ARP Timer Expired ➢ POP ARP switch buffer

✓ IF DYNAMIC OR On-Demand Profile:

✓ IF DHCP_SERVER Message: ➢ UPDATE Registered Port Profile

➢ TRIGGER "Recursive Relay Procedure"

ELSE: ➢ Forward Buffered Packet ➢ UPDATE "Registered Port Profile"

- ELIF 'DYNAMIC' OR 'ON-DEMAND' Profile:
  - ✓ IF DHCP_SERVER Message: ➢ UPDATE "Registered Port Profile"
  - ➢ TRIGGER "Recursive Relay Procedure"
- ELSE: ➢ Forward Buffered Packet
  - ➢ UPDATE "Registered Port Profile"

5.6.9 OVERLAY DISCOVERY PROCEDURE

This procedure is responsible for automated discovery of shortest path to any connected overlay in the bidirectional ring topology for inter-overlay communication. Mobility relay has two ports registered for ring communication. The topology layout is illustrated in figure 4-3. It is obvious in ring topology that any of the connected two ports mobility switch can reach the target overlay as of resilience and fault tolerance features. What matter here is both propagation delay and hop counts. This procedure is triggered by "Overlay Switching Procedure" to know which port is nearer. ARP_REQUEST message is sent on the nearest RS ports after updating "Mobility Inter-Overlay Table" with the message source address as well as the input port. Once ARP_REQUEST message arrives at target overlay, connected RS sends ARP_REPLY through input port of ARP_REQUEST message. This step is significant to register the identities of communicating RS. Afterward the initiator relay sends two ICMP pings to target RS on its two connected ring ports. ICMP delay and hop count of both replies are compared to choose best connected port for future communication. The other port is used as backup port in self-healing rings.

PROCEDURE PSEUDOCODE

- PUSH SYNOPSIS_VECTOR to ARP switch buffer ➢ SERVES Other Packets
- SEND ARP_REQUEST to DESTINATION _IP using Switch Virtual (HW, IP)
  - IF ARP_REPLY Arrived ➢ POP ARP switch buffer
    - ➢ REGISTER (SOURCE_HW of ARP_REPLY)
  - Interrupt: ARP Timer Expires ➢ LOG ERROR
    - ➢ DELETE BUFFER
    - ➢ RETURN FAILURE
- SEND ICMP to DESTINATION _IP using Switch Virtual (HW, IP) on both ports:
  - IF ICMP_REPLY Arrived ➢ Consider the input port of the first ICMP the active port
    - ➢ REGISTER (INPUT PORT of first ICMP, SOURCE_HW of ICMP_REPLY)

5.6.10 MOBILITY SWITCHING PROCEDURE

This procedure is used by the SDN controller to install OpenFlow rules that guide virtual path establishment on mobility switches for roaming MNs with enabled mobility profiles. These flow rules forward next packets directly to pre-determined port to avoid re-interrupting the SDN controller and to preserve OpenFlow hardware forwarding. Rules are setup based on Layer number stated in "Port Roaming Profile". Layer field is stated in SYNOPSIS_VECTOR generated by "Parsing Layer Identification Phase". The value is updated in "Port Roaming Profile" during MN's profile activation process. The following table translates the Layer field to the corresponding OpenFlow rule that to be installed on the mobility switches in the virtual path.

Table 5-10: Layer Field Translated to OpenFlow Rules

Layer #	Description	OpenFlow Rule
0	Packets needs monitoring by the SDN controller	➢ No Rule
1	All packets input from certain port must be output to a specific port and vice versa.	➢ Create a Multiplexer Rule binding two ports. Packet input from one port is forward to opposite port and vice versa.
2	If MN's IP address is not stated explicitly in IDLE MN profile, Layer 2 is selected	➢ <u>Creates two Rules:</u> 1. Hardware Address in Source field from specific Input port is forwarded to certain Output Port 2. Hardware Address in Destination field from specific Input port is forwarded to certain Output Port
3	If MN's IP Address is stated explicitly in IDLE node profile, Layer 3 is selected	➢ <u>Creates Four Rules:</u> 1. ARP_REQUEST from registered source (HW, IP) and registered input port is forwarded to pre-configured output Port. 2. ARP_REPLY with registered destination (HW, IP) and registered input port is forwarded to pre-configured output port. 3. IP packet from registered source (IP, HW) and registered input port is forwarded to pre-configured output Port. 4. IP packet with registered destination (HW, IP) and registered input port is forwarded to pre-configured output port.

5.7 ACTIVATION LAYER

Activation Layer represents the final stage in SDN mobility layered model where all requirements to enable roaming MN's mobility service have been fulfilled. Activation process involves two main procedures; Service Activation Procedure and Service Orchestration Procedure as shown in figure 5-10. Service Activation Procedure is responsible for generating "Port Roaming profiles", creating "On-Demand profile", and updating existing profiles with valuable parameters extracted from SYNOPSIS_VECTOR produced by the Parsing Layer then updated by the Action Layer. Service activation procedure triggers service orchestration procedure of home DS to initiate the orchestration process for synchronizing foreign DS profiles with Value Added Service (VAS) registered in MN profile at home network.

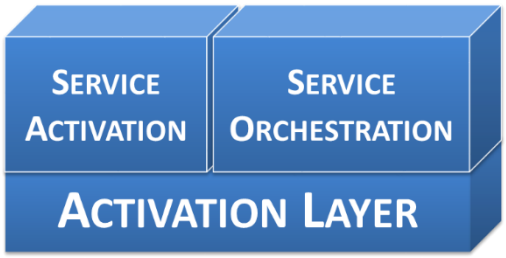


Figure 5-10 Activation Layer Procedures

5.7.1 SERVICE ACTIVATION PROCEDURE

The activation of mobility profile for a 'STATIC' MN with idle status triggers this procedure using either overlay switching procedure or inter-domain routing procedure while activation of 'On-Demand' or 'Dynamic' profile is triggered by the recursive relay procedure". For MNs with idle status, static/dynamic profile is updated with mobility status. On the other hand, a new mobility "On-Demand profile" is created for DHCP node if the idle profile is absent. Activation process involves generation of two port roaming profile per MN; source and destination input ports. The first profile is for identifying the port closer to roaming foreign MN that is called source input port while the second profile is for identifying the port directed to home network that is called destination input port. Source input port refers to packets/frames sourced from MNs entering the switch while destination input port refers to packets/frames entering the switch and destinated to MN. Each profile holds an index stating the opposite port and another index pointing to roaming 'Dynamic'/ 'Static'/'On-Demand' profile for fast retrieval. Moreover, both profiles store the selected Layer of OpenFlow rules for fast population to the switches once the mobility switching procedure is triggered.

For MN with static profile, SYNOPSIS_VECTOR containing all valuable parameters generated by Parsing Layer and modified by Action Layer is used directly in the activation process. While MN with 'Dynamic'/'On-Demand' profile, SYNOPSIS_VECTOR is popped from DHCP switch buffer once a DHCP_ACKNOWLEDGE server type message arrives. Then, all valuable parameters exchanged between

MN and home DHCP server are inserted in the vector for activation process. Furthermore, this procedure activates ARP responder service at the Detection Layer if mobility switch is home DS. This service responds to any enquires for hardware address of MN initiated by home co-responders. Finally, home detector service triggers service orchestration procedure to instruct foreign DS on how to enforce access policy and how to support various end-to-end telecommunication services for Operations Support Systems (OSS)/ Business support systems (BSS).

Mobility service is activated for a configurable period that is factor of OpenFlow 'IDLE_TIMEOUT' period. This period is configurable to maximum triple of 'IDLE_TIMEOUT' period or equal to 'HARD_TIMEOUT' period of OpenFlow at foreign DS. Mobility timer is automatically reset with the renewal of 'IDLE_TIMEOUT'. If 'HARD_TIMEOUT' period is reached, an ARP_REQUEST is sent to MN on foreign access switch. ARP_REPLY arrival resets mobility service timer. However, if ARP timer expires, mobility service for this MN is deactivated. For MN with 'Dynamic'/'On-Demand' profiles, a second mobility timer is set to expire after 75% of DHCP lease period if not receiving a new DHCP_ACKNOWLEDGE from home DHCP server. If 75% of lease period expired without renewal, the service is deactivated. Deactivation process involves updating profiles' status from 'roaming' to 'idle', deleting "Port Roaming profiles" and "On-Demand Profile", and triggering the service orchestration procedure of the foreign detector to inform home network and OSS/BSS services of deactivation.

PROCEDURE PSEUDOCODE

- IF Mobility Timer Expires (HARD_TIMEOUT or 75% Lease):
  - ✓ IF Foreign Detector AND HARD_TIMEOUT expires:
    - ➢ SEND ARP_REQUEST to Mobility NODE using Management Switch (HW, IP)
    - ➢ IF ARP_REPLY Arrived: ➢ RESET Mobility Timers ➢ RETURN Success
    - ➢ ARP_TIMERS Expires: ➢ RESUME Procedure
  - ✓ IF Dynamic or Static Profile: ➢ UPDATE Profile from Roaming to IDLE Status.

    ELSE: ➢ DELETE On-Demand Profile
  - ➢ DELETE SOURCE and Destination Input Port Roaming Profile
  - ✓ IF Home Detector: ➢ DEACTIVATE ARP responder service
  - ✓ IF Foreign Mobility Detector: ➢ DEACTIVATE using "Service Orchestration Procedure"
- ELSE: ➢ UPDATE Profile from Roaming to IDLE Status:
  - ➢ CREATE Source and Destination Input Port Roaming Profile
  - ✓ IF Home Mobility Detector: ➢ ACTIVATE Detection Layer ARP responder service
  - ➢ ACTIVATE "Service Orchestration Procedure"

5.7.2 SERVICE ORCHESTRATION PROCEDURE

Service orchestration procedure is the core of Activation Layer as for playing vital role in policy enforcement as well as service synchronization between home and foreign detectors. Policy enforcement happens in similar way to that of AAA service. SDN controller takes the role of AAA server in sending an ACCESS_ACCEPT message to mobility AS. This message includes user authorizations to particular network resources using access credentials. The credentials are passed to mobility ASs via Datalink Layer protocol as Point-to-Point Protocol (PPP) in dialup or DSL providers or posted in an HTTPS secure web form. TUNNEL_PRIVATE_GROUP identifier in ACCESS_ACCEPT message specifies VLAN identifier representing HOME_ID that should be applied to MN in case of Wi-Fi hotspots, Ethernet switches. …etc, as in RFC 2868 [90]. When network access is granted, mobility AS signals the SDN controller to start accounting user's activities as well as OSS/BSS services. Foreign SDN controller signals home SDN controller to initiate OSS/BSS services' synchronization.

6 PROTOTYPING SDN MOBILITY FRAMEWORK

6.1 PROTOTYPE LAYOUT

A prototype is established to assess the feasibly of SDN proposed mobility framework. The prototype is comprised of three enterprises; ENTERPRISE_EA, ENTERPRISE_EB, and ENTERPRISE_EC. Each has its own SDN controller. ENTERPRISE_EA has mobility SLAs with both ENTERPRISE_EB and ENTERPRISE_EC. A detailed layout for this prototype is shown in figure 6-1 and explained bellow.

6.1.1 ENTERPRISE_EC DETAILED STRUCTURE

ENTERPRISE_EC is comprised of two PDNs separated by EC_ROUTER with LAN bandwidth 100Mbps and connected with single WAN link of bandwidth 2Mbps to the outside world. Each PDN is comprised of L3 switch to represent standard L2/L3 network. These switches are OF_SWL3 and OH_SWL3. The former is connected to EC_OF PDN while the later is connected to EC_OH PDN. More details are illustrated bellow.

6.1.1.1 EC_OF PDN STRUCTURE

OF_SWL3 PDN is comprised of four VLANs. Server OF_SERVER1 is connected to VLAN11 while server OF_SERVER2 and host OF_HOST2 are connected to VLAN12. The centralized WLC in VLAN14 runs SDWN for mobility cross the three APs to serve wireless MNs' connections. OF_MN1 and OF_MN2 are wireless hosts roaming cross OF_SWL3 PDN with continuous connectivity to their home network VLAN12. ENTERPRISE_EC acts as the cable networks offering residential/enterprise services. VLAN10 represents the Network Operation Center (NOC) where the centralized DHCP server OF_DHCP is located. Separate IP address pools are assigned to WLC, VLAN11, and VLAN12.

Mobility overlay 'OF' is connected via two AS mobility entities to OF_SWL3 switch. The first AS has two MOBILITY_IDs. These are 'OF1' and 'OF2' to create backdoor to VLAN11 and VLAN12 respectively. The second AS has a single MOBILITY_ID 'OF4' to monitor MNs' join requests on the WLC. Both mobility ASs are connected to a single DS with MOBILITY_ID 'OF5'. This DS has two extra ports. The first port is in_band port connected to intranet/internet services of OF_SWL3 PDN to create instant breakout for MNs' to offload the core network. The second port is connected to parent tier MG with MOBILITY_IDs 'OF0'. This MG is responsible inter-domain mobility cross enterprises thus it has an in_band port connected to EC_ROUTER that performs NAT of MG private IP address to public IP address for WAN accessibility by other enterprises.

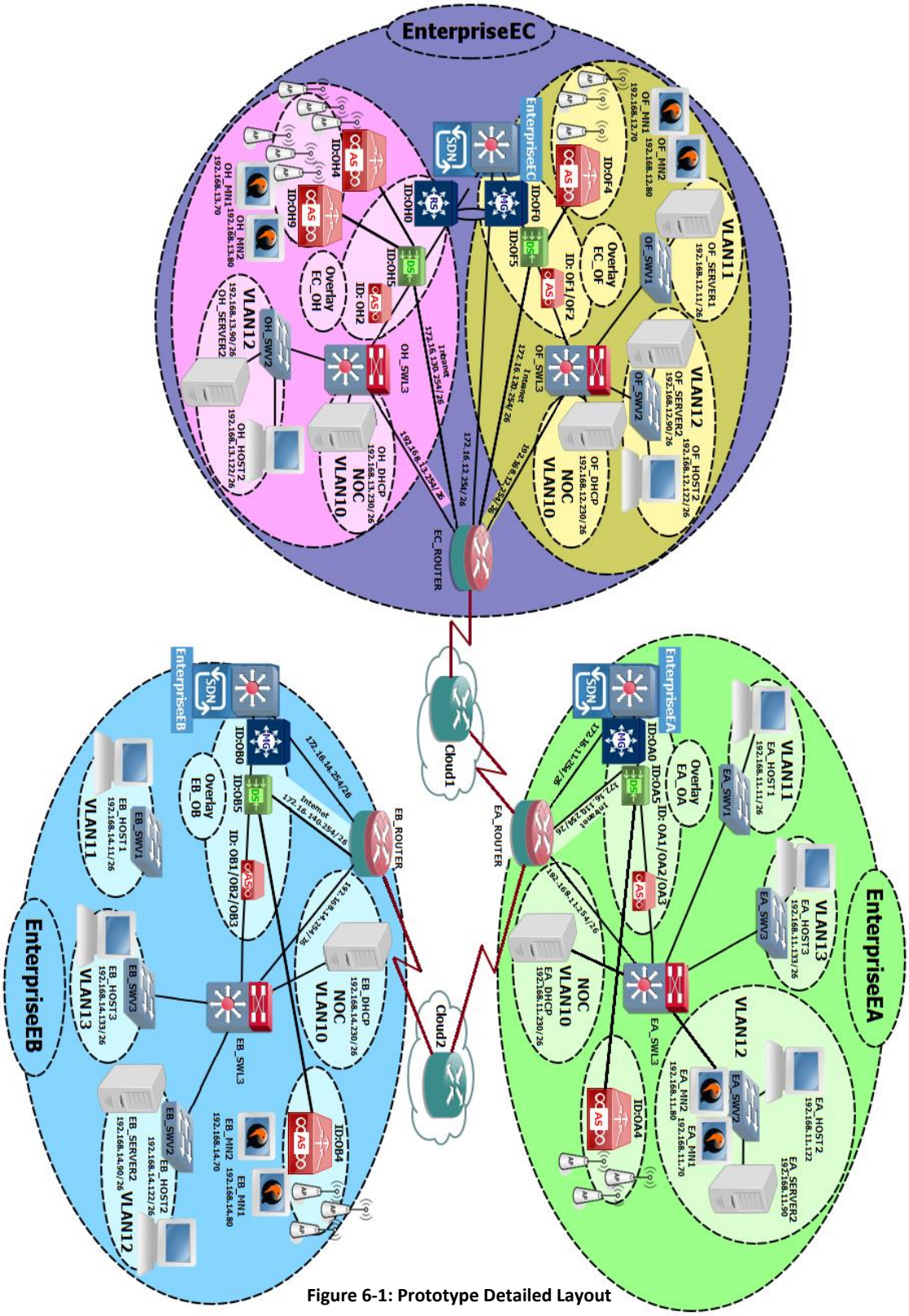


Figure 6-1: Prototype Detailed Layout

6.1.1.1.1 EC_OF PDN IP Configuration

EC_OF PDN (Subnet 192.168.12.0/26)				
Name	**Description**	**IP**	**MAC**	**IDENTIFIER**
		NOC VLAN 10		
EC_ROUTER:Fa0/0.10	Gateway	192.168.12.254	c2:01:3f:20:00:00	--
OF_DHCP	DHCP Server	192.168.12.230	c2:07:14:38:00:00	--
		VLAN11		
EC_ROUTER:Fa0/0.11	Gateway	192.168.12.62	c2:01:3f:20:00:00	--
OF_SERVER1	Local Server	192.168.12.11	00:00:00:00:12:11	--
		VLAN12		
EC_ROUTER:Fa0/0.12	Gateway	192.168.12.126	c2:01:3f:20:00:00	--
OF_SERVER2	Local Server	192.168.12.90	c2:10:1f:a8:00:00	--
OF_HOST2	Static Host	192.168.12.122	00:00:00:00:12:22	--
OF_MN1	Mobile Node	192.168.12.70	00:00:00:00:12:70	0020-120-020-070
OF_MN2	Mobile Node	192.168.12.80	00:00:00:00:12:80	0020-120-020-080

Table 6-1: IP Configuration of EC_OF PDN

6.1.1.1.2 EC_OF PDN Overlay Configuration

EC_OF : *<Domain ID>-<Operator ID>-<Sub-Operator ID>: <0020>-<120>-<020>*						
Role	**Private MOBILITY_ID**	**Overlay IP**	**Public MOBILITY_ID**	**IN_BAND IP**	**Public IP**	**MAC**
DS	OF5	233.79.70.53	--	172.16.120.240	--	00:00:00:00:01:25
AS	OF1	233.79.70.49	--	--	--	00:00:00:00:01:21
	OF2	233.79.70.50	--	--	--	00:00:00:00:01:22
	OF4	233.79.70.52	--	--	--	System
MG	OF0	233.79.70.48	EC_OF	172.168.12.240	10.10.2.240	00:00:00:00:01:20

Table 6-2: Overlay Configuration of EC_OF PDN

MOBILITY ROUTING TABLE --- MG OF0					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	10.10.1.240	172.16.12.254	GATE	--
OH0	255.255.255.0	OH0	--	SWITCH	--
OF0	--	--	--	SWITCH	--
MOBILITY ROUTING TABLE --- DS OF5					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	OF0	--	SWITCH	--
OF1	--	--	--	SWITCH	--
OF2	--	--	--	SWITCH	--
OF4	--	--	--	SWITCH	--

Table 6-3: Routing Configuration of EC_OF PDN

6.1.1.2 EC_OH PDN STRUCTURE

OH_SWL3 PDN is comprised of three VLANs. Server OH_SERVER2 is connected to VLAN12. VLAN14 has two WLCs with three APs running SDWN to evaluate intra-overlay mobility. OH_MN1 and OH_MN2 are wireless hosts roaming cross OH_SWL3 PDN with continuous connectivity to their home networks VLAN12. ENTERPRISE_EC acts as the cable networks offering residential/enterprise services. VLAN10 represents NOC where the centralized DHCP server OH_DHCP is located. Separate IP address pools are assigned to WLC and VLAN12. Mobility overlay 'OF' is connect via two AS mobility entities to OH_SWL3 switch. Despite VLANs existing in the two PDNs have similar TAGs, VLANs are not extended cross EC_ROUTER. The objective from similar TAGs is showing how mobility can be seamless extended cross PDN with overlapping configuration without conflict. This ensures that involved entities' privacies are preserved.

Mobility overlay 'OH' is connected via two AS mobility entities to OH_SWL3. The first AS has MOBILITY_ID 'OH2' to create backdoor to VLAN12 while the second AS has MOBILITY_ID 'OH4' to monitor MNs' join requests on the WLC. Both ASs are connected to a single DS with MOBILITY_ID 'OH5'. This DS has two ports. The first port is in_band port connected to intranet/internet services of OH_SWL3 PDN to create instant breakout to offload the core network. The second port is connected to parent tier RS mobility with MOBILITY_IDs 'OH0'. This RS is responsible inter-overlay mobility cross ENTERPRISE_EC PDNs thus it has another port connected to MG with MOBILITY_IDs 'OF0' located at OF_SWL3 PDN.

6.1.1.2.1 EC_OH PDN IP Configuration

EC_OF PDN (Subnet 192.168.13.0/26)				
Name	**Description**	**IP**	**MAC**	**IDENTIFIER**
		NOC VLAN 10		
EC_ROUTER:Fa1/0.10	Gateway	192.168.13.254	c2:01:3f:20:00:10	--
OH_DHCP	DHCP Server	192.168.13.230	c2:0f:3d:48:00:00	--
		VLAN12		
EC_ROUTER:Fa1/0.12	Gateway	192.168.13.126	c2:01:3f:20:00:10	--
OH_SERVER2	Local Server	192.168.13.90	c2:11:62:bc:00:00	--
OH_HOST2	Static Host	192.168.13.122	00:00:00:00:13:22	--
OH_MN1	Mobile Node	192.168.13.70	00:00:00:00:13:70	0020-130-020-070
OH_MN2	Mobile Node	192.168.13.80	00:00:00:00:13:80	0020-130-020-080
OH_STA1	Mobile Station	192.168.13.70	00:00:00:00:13:70	0020-130-020-070
OH_STA2	Mobile Station	192.168.13.80	00:00:00:00:13:80	0020-130-020-080

Table 6-4: IP Configuration of EC_OH PDN

6.1.1.2.2 EC_OH PDN Overlay Configuration

EC_OH : *<Domain ID>-<Operator ID>-<Sub-Operator ID>: <0020>-<120>-<020>*						
Role	**Private MOBILITY_ID**	**Overlay IP**	**Public MOBILITY_ID**	**IN_BAND IP**	**Public IP**	**MAC**
DS	OH5	233.79.72.53	--	172.16.120.240	--	00:00:00:00:01:25
AS	OH2	233.79.72.50	--	--	--	00:00:00:00:01:22
	OH4	233.79.72.52	--	--	--	System
RS	OH0	233.79.72.48	EC_OH	172.168.12.240	--	00:00:00:00:01:20

Table 6-5: Overlay Configuration of EC_OH PDN

6.1.1.2.3 EC_OH PDN Routing Configuration

MOBILITY ROUTING TABLE --- RS OH0					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	OF0	--	SWITCH	--
OH0	255.255.255.0	--	--	SWITCH	--
MOBILITY ROUTING TABLE --- DS OF5					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	OH0	--	SWITCH	--
OH2	--	--	--	SWITCH	--
OH4	--	--	--	SWITCH	--

Table 6-6: Routing Configuration of EC_OH PDN

6.1.2 ENTERPRISE_EA DETAILED STRUCTURE

ENTERPRISE_EA is comprised of a single PDNs terminated by EA_ROUTER with two WAN links of bandwidth 2Mbps M to communicate with the outside world. ENTERPRISE_EA has mobility SLA with both ENTERPRISE_EB and ENTERPRISE_EC. EA_SWL3 PDN is comprised of five VLANs. Host EA_HOST1 is connected to VLAN11. Host EA_HOST3 is connected to VLAN13 while server EA_SERVER2 and host EA_HOST2 are connected to VLAN12. The centralized WLC in VLAN14 runs SDWN for mobility cross the three APs. EA_MN1 and EA_MN2 are wireless hosts roaming cross EA_SWL3 PDN with continuous connectivity to their home network VLAN12. VLAN10 represents NOC where the centralized DHCP server EA_DHCP is located. Separate IP address pools are assigned to WLC, VLAN11, VLAN12, and VLAN13.

Mobility overlay 'OA' is connected via two AS mobility entities to EA_SWL3 switch. The first AS has three MOBILITY_IDs. These are 'OA1', 'OA2', and 'OA3' to create backdoor to VLAN11, VLAN12 and VLAN13 respectively. The second AS has a single MOBILITY_ID 'OA4' to monitor MNs' join requests on the WLC. Both mobility ASs are connected to a single DS with MOBILITY_ID 'OA5'. This DS has two extra ports. The first port is in_band port connected to intranet/internet services. The second port is connected to parent tier MG with MOBILITY_IDs 'OA0'. MG has an in_band port connected to EA_ROUTER that performs NAT of MG's private IP address for WAN accessibility.

6.1.2.1 EA_OA PDN IP CONFIGURATION

EA_OA PDN (Subnet 192.168.11.0/26)				
Name	**Description**	**IP**	**MAC**	**IDENTIFIER**
NOC VLAN 10				
EA_ROUTER:Fa0/0.10	Gateway	192.168.11.254	c2:03:43:0c:00:00	--
EA_DHCP	DHCP Server	192.168.11.230	c2:08:1a:d0:00:00	--
VLAN11				
EA_ROUTER:Fa0/0.11	Gateway	192.168.11.62	c2:03:43:0c:00:00	--
EA_HOST1	Static Host	192.168.11.11	00:00:00:00:11:11	--
VLAN12				
EA_ROUTER:Fa0/0.12	Gateway	192.168.11.126	c2:03:43:Oc:00:00	--
EA_SERVER2	Local Server	192.168.11.90	c2:0b:54:b4:00:00	--
EA_HOST2	Static Host	192.168.11.122	00:00:00:00:11:22	--
EA_MN1	Mobile Node	192.168.11.70	00:00:00:00:11:70	0010-110-020-070
EA_MN2	Mobile Node	192.168.11.80	00:00:00:00:11:80	0010-110-020-080
VLAN13				
EA_ROUTER:Fa0/0.13	Gateway	192.168.11.190	c2:03:43:Oc:00:00	--
EA_HOST3	Static Host	192.168.11.133	00:00:00:00:11:33	--

Table 6-7: IP Configuration of EA_OA PDN

6.1.2.2 EA_OA PDN OVERLAY CONFIGURATION

EC_OH : *<Domain ID>-<Operator ID>-<Sub-Operator ID>: <0010>-<110>-<020>*						
Role	**Private MOBILITY_ID**	**Overlay IP**	**Public MOBILITY_ID**	**IN_BAND IP**	**Public IP**	**MAC**
DS	OA5	233.79.65.53	--	172.16.110.240	--	00:00:00:00:01:15
AS	OA1	233.79.65.49	--	--	--	00:00:00:00:01:11
	OA2	233.79.65.50	--	--	--	00:00:00:00:01:12
	OA3	233.79.65.51	--	--	--	00:00:00:00:01:13
	OA4	233.79.65.52	--	--	--	System
MG	OA0	233.79.65.48	EA_OA	172.168.11.240	10.10.1.240	00:00:00:00:01:10

Table 6-8: Overlay Configuration of EA_OA PDN

6.1.2.3 EA_OA PDN ROUTING CONFIGURATION

MOBILITY ROUTING TABLE --- MG OF0					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	10.10.4.240	172.16.11.254	GATE	--
EC00	0.0.0.0	10.10.2.240	172.16.11.254	GATE	--
OA0	255.255.255.0	--	--	SWITCH	--
MOBILITY ROUTING TABLE --- DS OF5					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	OA0	--	SWITCH	--
OA1	--	--	--	SWITCH	--
OA2	--	--	--	SWITCH	--
OA2	--	--	--	SWITCH	--
OA4	--	--	--	SWITCH	--

Table 6-9: Routing Configuration of EC_OF PDN

6.1.3 ENTERPRISE_EB DETAILED STRUCTURE

ENTERPRISE_EB is comprised of a single PDNs terminated by EB_ROUTER with a single WAN link of bandwidth 2Mbps to communicate with the outside world. ENTERPRISE_EB has mobility SLA with ENTERPRISE_EA. EB_SWL3 PDN is comprised of five VLANs. Host EB_HOST1 is connected to VLAN11. Host EB_HOST3 is connected to VLAN13 while server EB_SERVER2 and host EB_HOST2 are connected to VLAN12. The centralized WLC at VLAN14 runs SDWN for mobility cross the three APs. EB_MN1 and EB_MN2 are wireless hosts roaming cross EB_SWL3 PDN with continuous connectivity to their home network VLAN12. ENTERPRISE_EB acts as the cable networks offering residential/enterprise services. VLAN10 represents NOC where the centralized DHCP server EB_DHCP is located. Separate IP address pools are assigned to WLC, VLAN11, VLAN12, and VLAN13. Mobility overlay 'OB' is connect via two AS mobility entities to EB_SWL3 switch. The first AS has three MOBILITY_IDs. These are 'OB1', 'OB2', and 'OB2' to create backdoor to VLAN11, VLAN12 and VLAN13 respectively. The second AS has a single MOBILITY_ID 'OB4' to monitor MNs' join requests on the WLC. Both mobility ASs are connected to a single DS with MOBILITY_ID 'OB5'. This DS has two extra ports. The first port is in_band port connected to intranet/internet services. The second port is connected to parent tier MG with MOBILITY_IDs 'OB0'. MG has an in_band port connected to EB_ROUTER that performs NAT of MG's private IP address for WAN accessibility.

6.1.3.1 EB_OB PDN IP CONFIGURATION

EB_OB PDN (Subnet 192.168.14.0/26)				
Name	**Description**	**IP**	**MAC**	**IDENTIFIER**
		NOC VLAN 10		
EB_ROUTER:Fa0/0.10	Gateway	192.168.14.254	c2:05:0f:c8:00:00	--
EB_DHCP	DHCP Server	192.168.14.230	c2:0c:68:70:00:00	--
		VLAN11		
EB_ROUTER:Fa0/0.11	Gateway	192.168.14.62	c2:05:0f:c8:00:00	--
EB_HOST1	Static Host	192.168.14.11	00:00:00:00:14:11	--
		VLAN12		
EB_ROUTER:Fa0/0.12	Gateway	192.168.14.126	c2:05:0f:c8:00:00	--
EB_SERVER2	Local Server	192.168.14.90	c2:12:31:94:00:00	--
EB_HOST2	Static Host	192.168.14.122	00:00:00:00:14:22	--
EB_MN1	Mobile Node	192.168.14.70	00:00:00:00:14:70	0040-140-020-070
EB_MN2	Mobile Node	192.168.14.80	00:00:00:00:14:80	0040-140-020-080
		VLAN13		
EB_ROUTER:Fa0/0.13	Gateway	192.168.14.190	c2:05:0f:c8:00:00	--
EB_HOST3	Static Host	192.168.14.133	00:00:00:00:14:33	--

Table 6-10: IP Configuration of EB_OB PDN

6.1.3.2 EB_OB PDN OVERLAY CONFIGURATION

EB_OB : *<Domain ID>-<Operator ID>-<Sub-Operator ID>: <0040>-<140>-<020>*						
Role	**Private MOBILITY_ID**	**Overlay IP**	**Public MOBILITY_ID**	**IN_BAND IP**	**Public IP**	**MAC**
DS	OB5	233.79.66.53	--	172.16.140.240	--	00:00:00:00:01:45
AS	OB1	233.79.66.49	--	--	--	00:00:00:00:01:41
	OB2	233.79.66.50	--	--	--	00:00:00:00:01:42
	OB3	233.79.66.51	--	--	--	00:00:00:00:01:43
	OB4	233.79.66.52	--	--	--	System
MG	OB0	233.79.66.48	EB_OB	172.168.14.240	10.10.4.240	00:00:00:00:01:40

Table 6-11: Overlay Configuration of EB_OB PDN

6.1.3.3 EB_OB PDN ROUTING CONFIGURATION

MOBILITY ROUTING TABLE --- MG OB0					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	10.10.1.240	172.16.14.254	GATE	--
OB0	255.255.255.0	--	--	SWITCH	--
MOBILITY ROUTING TABLE --- DS OB5					
NETWORK	**NETWORK MASK**	**DESTINATION**	**NEXTHOP IP**	**ACTION**	**KEY**
000	0.0.0.0	OB0	--	SWITCH	--
OB1	--	--	--	SWITCH	--
OB2	--	--	--	SWITCH	--
OB2	--	--	--	SWITCH	--
OB4	--	--	--	SWITCH	--

Table 6-12: Routing Configuration of EB_OB PDN

6.1.4 CLOUD DETAILED STRUCTURE

WAN complexities and lack of direct connections are analyzed by using two clouds for inter-connecting the three enterprises. ENETERPRISE_EA is connected to ENETERPRISE_EC via CLOUD1 while ENETERPRISE_EA is connected to ENETERPRISE_EB via CLOUD2. Each cloud contains a single router with two 2Mbps serial interfaces connected to the enterprises' edge routers. Configuration details is illustrated in table 6-13 bellow.

CLOUD1		CLOUD2	
Name	**IP**	**Name**	**IP**
EC_ROUTER:S0/2	10.10.2.254	**EA_ROUTER:S0/3**	10.10.3.254
CLOUD1:S0/2	10.10.2.253	**CLOUD2:S0/3**	10.10.3.253
CLOUD1:S0/1	10.10.1.254	**CLOUD2:S0/4**	10.10.4.254
EA_ROUTER:S0/1	10.10.1.254	**EB_ROUTER:S0/4**	10.10.4.254

Table 6-13: CLOUD IP Configurations

6.2 MOBILITY SETUP DELAY ESTIMATION

The time elapsed for activation of MN's mobility service after authentication is affected by both processing and network propagation delays. The established prototype is formed of back to back devices thus the propagation delays, ranging from ~1-2ms, is almost negligible when compared to the processing delay. In real environment, the processing delay can be lower than the estimated value in this research as of using network equipment with higher processing power. On the contrary, propagation delay can be a major factor as of network speed, utilization, and links' quality. Processing delay is affected by several factors including the number of encountered mobility entities in the virtual path between foreign and home networks, the method of IP allocation for MNs, the shared tunnel requires establishment or already active …etc. The following describes the different types of processing delays encountered while testing the SDN mobility framework. The estimated value per delay stated bellow is the calculated average from running each experiment several times.

6.2.1 ACCESS DELAY

Access Delay is the estimated processing delay by any standard learning switch for searching the Content Addressable Memory (CAM) table and identifying the output port if OpenFlow rules are not installed. The average calculated value for this delay from several runs is ~**0.01s** per mobility switch.

6.2.2 STATIC DELAY

Static Delay is the estimated processing delay in the SDN controller of mobility DS to activate MN with static IP address. This process includes the delay to retrieve stored profile, identify next hop and output port toward home network, activate mobility profiles, and install OpenFlow rules on mobility switches. The average calculated value for this delay from several runs is ~**0.02s** per mobility switch.

6.2.3 DHCP RELAY DELAY

DHCP Relay Delay is the estimated processing delay in the SDN controller of mobility DS to retrieve stored profile of DHCP mobility subscriber, create an on-demand if pre-registered profile is not found, identify next hop toward home network, rewrite DHCP message, identify output port, activate mobility profiles, and forward DHCP message. The average calculated value for this delay is ~**0.03s** per mobility switch in the forward path from foreign to home networks and ~**0.02s** in the backward path.

6.2.4 ACTIVE FLOW DELAY

Active Flow Delay is the estimated processing delay of any OpenFlow switch to forward packets after installing flows rules. OpenFlow hardware abstraction guarantees wire speed forwarding. Any encountered delay depends mainly on the hardware of the mobility switch.

6.2.5 TUNNEL DELAY

Tunnel delay has two definitions according to the role of MG. The first is the time consumed by the SDN controller of initiator MG to determine next hop gateway toward MN's home in addition to the time to establish tunnel then to forward packet to output port. The second definition is the time consumed by the SDN controller of recipient MG to activate tunnel when receiving initiation request in addition to that required for identifying next hop toward MN's home and for forwarding packet to output port. The average calculated value for this delay from several runs is ~**1s** per MG for both definitions.

6.2.6 FORWARD ACTIVATION DELAY

Forward Activation Delay is the summation of all delays encountered during activation process by all mobility entities in the forward virtual path starting from foreign AS and ending with home AS. The calculation of this delay is dependent on network layout and is estimated per topology.

6.2.7 BACKWARD ACTIVATION DELAY

Backward Activation Delay is the summation of all delays encountered during activation process by all mobility entities in the backward virtual path starting from home AS and ending with foreign AS. The calculation of this delay is dependent on network layout and is estimated per topology.

6.2.8 MOBILITY SETUP DELAY

This represents the total delay encountered by each mobility entity to activate MN's profile. Its value is the sum of Forward and Backward Path delays.

6.2.9 MOBILITY RE-ACTIVATION DELAY

Re-Activation Delay is the estimated processing time in the SDN controller of any mobility entity to retrieve the record of an active MN, reinstall OpenFlow rules, and forward packet to the registered output port. This delay is encountered in two scenarios. The first scenario happens when the flow timer on the switch expires while the mobility timer is still valid. The second scenario is limited to mobility subscribers using DHCP and RADIUS. The SDN controller keeps track of DHCP lease messages and RADIUS authentication messages. Therefore, no flows rule is installed during activation of MNs using DHCP and

RADIUS as these messages are relayed with the virtual IP of mobility switches. In this scenario, the activation process only updates mobility profiles and changes MN's status to roaming. The flows rules are installed on the switches to establish virtual path with the first non DHCP or RADIUS packet entering the mobility switches from an active MN. The average calculated value for roaming delay from several runs is almost ~**0.01s** per mobility switch in either scenario. Roaming Activation Period is the sum of roaming delays of all mobility entities in the forward virtual path.

6.3 EXPERIMENT 1: PROTOTYPING MOBILITY INSIDE RAN

6.3.1 OVERVIEW

This experiment evaluates the performance of the proposed SDN mobility framework in an environment similar to radio networks as 4G LTE. ENTERPRISE_EC is designed in way to evaluate various mobility parameters and compare them with Cisco delay budget for PMIP default bearer establishment that are listed in table 6-14 [35]. These parameters include mobility setup, intra-overlay and inter-overlay handover delays. Mobility setup delay is the time elapsed to establish OpenFlow virtual path between home and foreign networks which is equivalent to the total bearer setup time in LTE. Intra-overlay handover is equivalent to LTE handover cross S-GW. Inter-overlay handover is designed to ensure session continuity during handover cross separate PDNs in wide area motion. Currently, LTE does not support this type of handover. Existing solutions overcome this challenge by either enforcing session disconnect as of new IP lease or tunneling MN's packets through the new attached PDN S-GW to previous PDN P-GW which in turn leads to EPC congestion problem discussed in section 1.3.2.1.

Nodes	Interface Name	Nodes Involved	Delay Budget
eNB	S1-MME/NAS	eNodeB-MME	**~50ms**
MME	S6a	MME-HSS	**~100ms**
MME	DNS	MME-DNS (APN)	**~50ms**
MME	S11	MME-SGW	**~50ms**
SGW	S5/S8	SGW-PGW	**~50ms**
PGW	Gx	PGW-PCRF	**~100ms**
PGW	Gy	PGW-OCS	**~100ms**
Total Bearer Setup Time			**~500ms**
eNodeB	X2	eNB-eNB	**~20ms**

Table 6-14: Cisco Delay Budget for Default Bearer

ENTERPRISE_EC is designed with two mobility overlays managed by single SDN controller, as described in section 6.1.1. The first overlay EC_OH represents the PDN of City H while overlay EC_OF represents that of City F. Two mobile stations, OH_STA1 and OH_STA2 are attached to City H WLC AS

ID:OH4 with simultaneous connections to OH_SERVER2 located at their home network VLAN12 on OH_SWL3. EC_OH overlay has two ASs, ID:OH4/OH9. Each AS has three overlapping APs to compare intra-overlay handover performance against that of SDWN inside City H. EC_OF overlay has a single AS, ID:OF4, to compare inter-overlay handover performance against that of SDWN when crossing City H AS, ID:OH4 to City F. A symbolic layout for RAN mobility prototype is shown in figure 6-2.

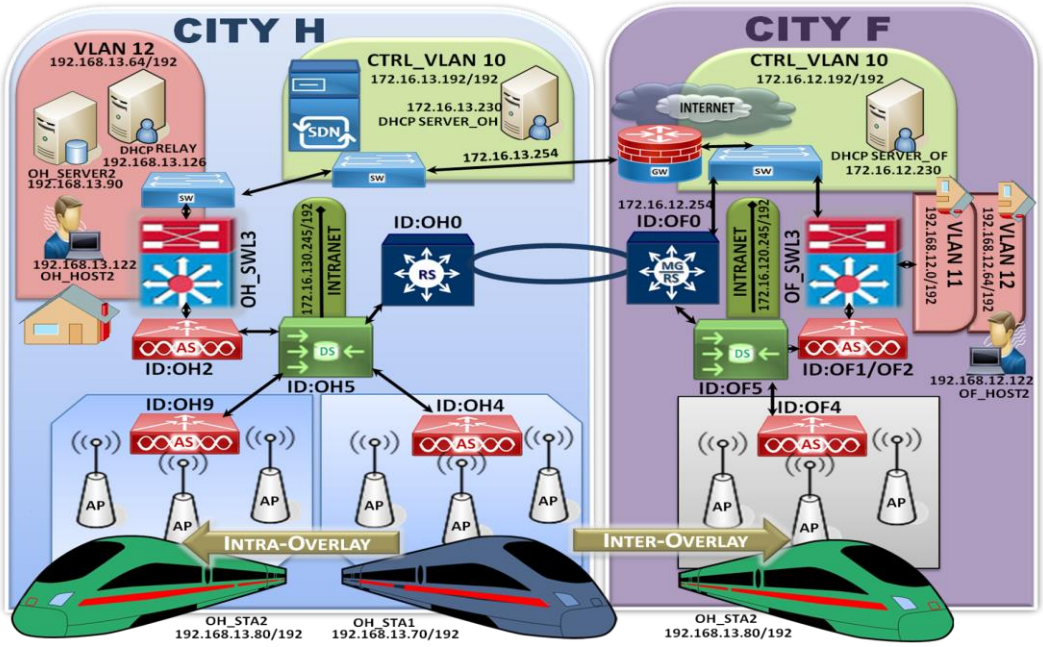


Figure 6-2: Layout of RAN Mobility Prototype

Mobility handover scenarios of overlapping APs in intra-overlay, ID:OH4/OH9, and inter-overlay, ID:OH4/OF4 are shown in figure 6-2. To avoid interference, each of AS sets with ID:OH4/OH9/OF4 uses separate channel and different SSID. Two mobile stations registered for residential mobility service; OH_STA1 and OH_STA2, move across the topology as shown in figures 6-2 and 6-3. Both stations are assigned IP addresses from home DHCP server. During motion, both stations establish sessions with OH_SERVER2 located at their home network VLAN12 of City H. Experiments ensure that both stations cover the same distance with the same velocity but in different directions. OH_STA1 moves in a straight path that handovers the three APs of AS ID:OH4 to evaluate standard SDWN handover performance while OH_STA2 starts at AS ID:OH4 and undergoes SDWN handover followed by either intra-overlay or inter-overlay handover to ASs ID:OH9 or OF4 respectively. Both OH_STA1 and OH_STA2 results are compared to highlight the difference between the three handover types in TCP/UDP packets loss, throughput, latency, UDP jitter and TCP sessions throughput restoration.

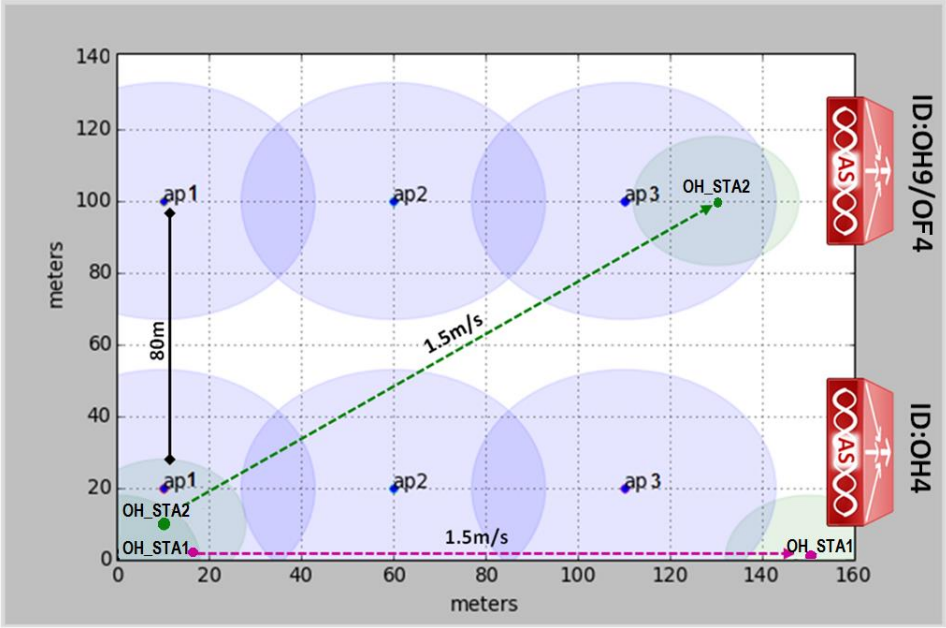


Figure 6-3: Handover with APs at 80m Apart

6.3.2 INTRA-OVERLAY MOBILITY SETUP DELAY

OH_STA1 and OH_STA2, initially located on AP1 at WLC AS ID:OH4, establish virtual paths to their home network VLAN12 during IP addresses allocation from home DHCP server. Recursive relay procedure, in section 5.6.5, and OpenFlow rules re-installation induce **intra-overlay mobility setup delay** of **~0.2s**. This delay is much better than **PMIP total bearer setup delay of ~0.5s** stated in table 6.14 [35].

JOIN VIRTUAL PATH

Overlay EC_OH [AS ID:OH4 ↔DS ID:OH5↔AS ID:OH2]

6.3.3 INTRA-OVERLAY HANDOVER DELAY

OH_STA1 undergoes SDWN handover cross APs of a single WLC AS ID:OH4, thus the virtual path is not re-established. OH_STA2 undergoes intra-overlay handover between WLC AS ID:OH4⇔AS ID:OH9. Reverse lookup procedure, described in section 4.8.2, and OpenFlow rules re-installation induce **intra-overlay handover delay** of **~0.1s**. This is better than **PMIP S-GW handover** that counts to eNodeB-MME (50ms) + MME-HSS (100ms) + MME-DNS (50ms) + MME-SGW (50ms) = **~0.25s** as in table 6.14 [35].

HANDOVER VIRTUAL PATH

Overlay EC_OH [AS ID:OH9 ↔DS ID:OH5↔AS ID:OH2]

6.3.4 Intra-Overlay ICMP Latency and Packets Loss

Figure 6-4 shows results of 250 pings of (OH_SERVER2⇔OH_STA1) and (OH_SERVER2⇔OH_STA2). OH_STA1 represents SDWN handover performance at WLC AS ID:OH4. It experiences two handovers; the first between (AP1⇔AP2) almost at ~13-15s while the second between (AP2⇔AP3) almost at ~47-49s. On the other hand, OH_STA2 experiences two handovers; the first is SDWN handover at AS ID:OH4 between (AP1⇔AP2) almost at ~9-13s while the second is intra-overlay handover between (AP2 at AS ID:OH4⇔AP2 at AS ID:OH9) almost at ~46-48s. Figures 6-3 and 6-4 highlight that ~4s is the worst latency and packets loss experienced by OH_STA2 during SDWN handover. The large value is correlated to the large distance crossed in the overlapping region between AP1 and AP2 of WLC AS ID:OH4. On the other hands, OH_STA1's SDWN handover latency and packets loss are ~2s. This is equivalent to that experienced by OH_STA2 in intra-overlay handover.

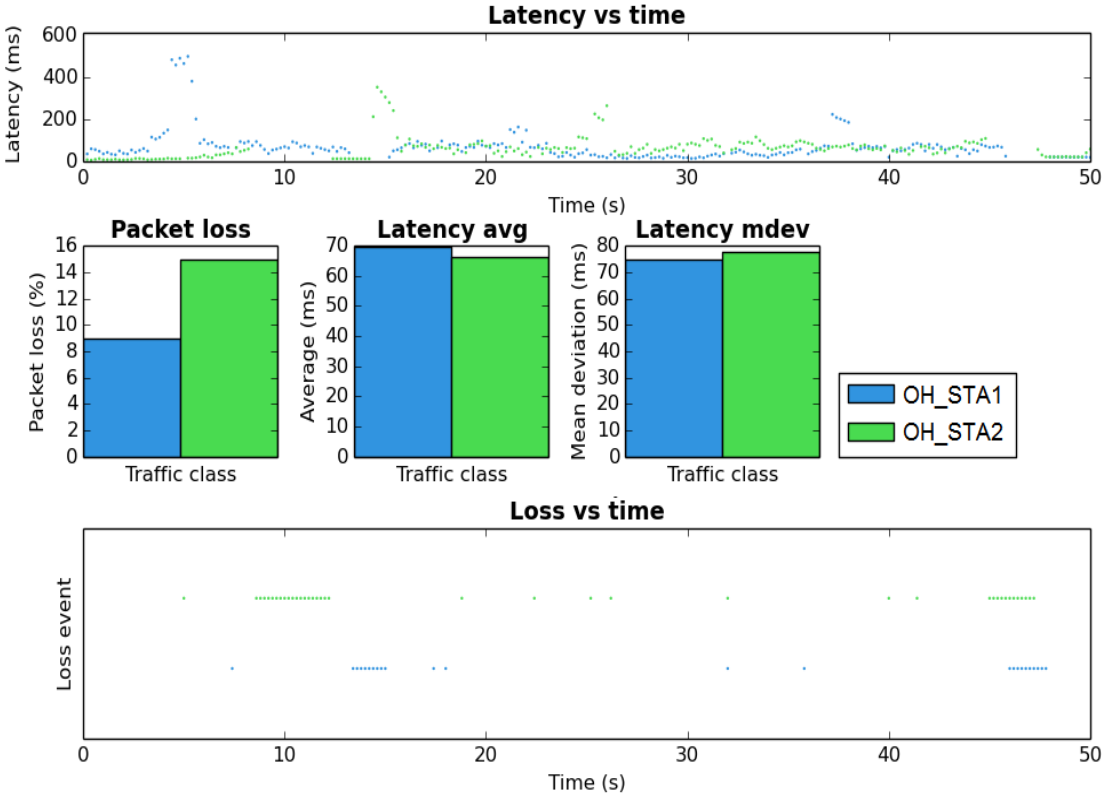


Figure 6-4: Intra-Overlay Handover ICMP Performance

6.3.5 INTRA-OVERLAY TCP PERFORMANCE

Figure 6-5 highlights that inter-overlay handover latency is almost equivalent to that of SDWN handover. Several consecutive handovers negotiate lower TCP windows size without TCP sessions disconnect. This decreases the average throughput. Between ~48-54s, OH_STA2 undergoes intra-overlay handover while OH_STA1 undergoes SDWN handover between ~51-56s. OH_STA2 throughput ~330KB/s drops to ~25.7KB/s for ~6s while OH_STA1 throughput ~151KB/s drops to ~17.82KB/s for ~5s. At ~75-90s, both stations become stationary. Figures 6-3 and 6-5 show that TCP throughput of OH_STA2, near AP center, becomes much higher than OH_STA1 at edge. This emphasizes that average TCP throughput depends mainly on how far stations are from AP center not on the handover process itself.

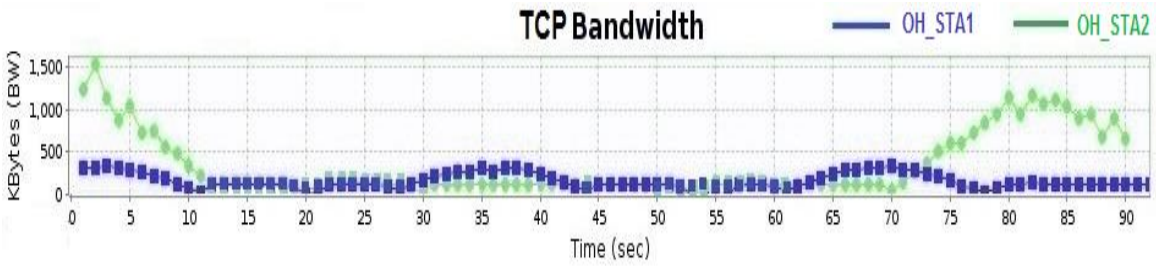


Figure 6-5: Intra-Overlay Handover TCP Throughput

6.3.6 INTRA-OVERLAY UDP PERFORMANCE

Between ~41-44s, OH_STA1 undergoes SDWN handover while OH_STA2 undergoes intra-overlay handover between ~43-46s. Both types of handovers induce instant decrease in average UDP throughputs due to dropping some packets. During handover, UDP jitters depend mainly on how far station is from AP center rather than handover type.

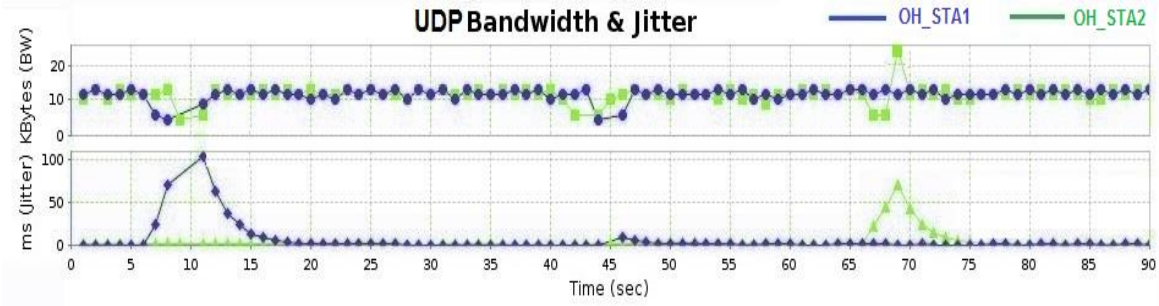


Figure 6-6: Intra-Overlay Handover UDP Throughput

6.3.7 INTER-OVERLAY HANDOVER DELAY

OH_STA1 undergoes SDWN handover cross APs of a single WLC AS ID:OH4, thus the virtual path is not re-established. OH_STA2 undergoes inter-overlay handover between WLC AS ID:OH4⇔WLC AS ID:OF4. Reverse lookup procedure, described in section 4.8.2, and OpenFlow rules re-installation in **inter-overlay handover delay** of **~0.15s**. In LTE, no handover occurs cross P-GWs in wide area motion. Two solutions are possible. The first is sessions disconnect followed by bearer re-establishment to the new PDN P-GW while the second is bearer re-establishment between new PDN S-GW and old PDN P-GW to preserve session continuity. The second solution induces EPC congestion problem. In both scenarios, **PMIP** delay is equal to **total bearer setup** of **~0.5s**.

HANDOVER VIRTUAL PATH

Overlay EC_OF [AS ID:OF4 ↔DS ID:OF5↔MG ID:OF0]

Overlay EC_OH [RS ID:OH0 ↔DS ID:OH5↔AS ID:OH2]

6.3.8 INTER-OVERLAY ICMP LATENCY AND PACKETS LOSS

Figure 6-7 shows results of 250 pings of (OH_SERVER2⇔OH_STA1) and (OH_SERVER2⇔OH_STA2). OH_STA1 performs SDWN handover at WLC AS ID:OH4 (AP2⇔AP3) at ~27-29s while OH_STA2 performs inter-overlay handover between (AP4: AS ID:OA4⇔AP2: AS ID:OB4) at ~26-29.5s. Figure 6-7 highlights that inter-overlay handover induces ~1.5s latency higher than SDWN.

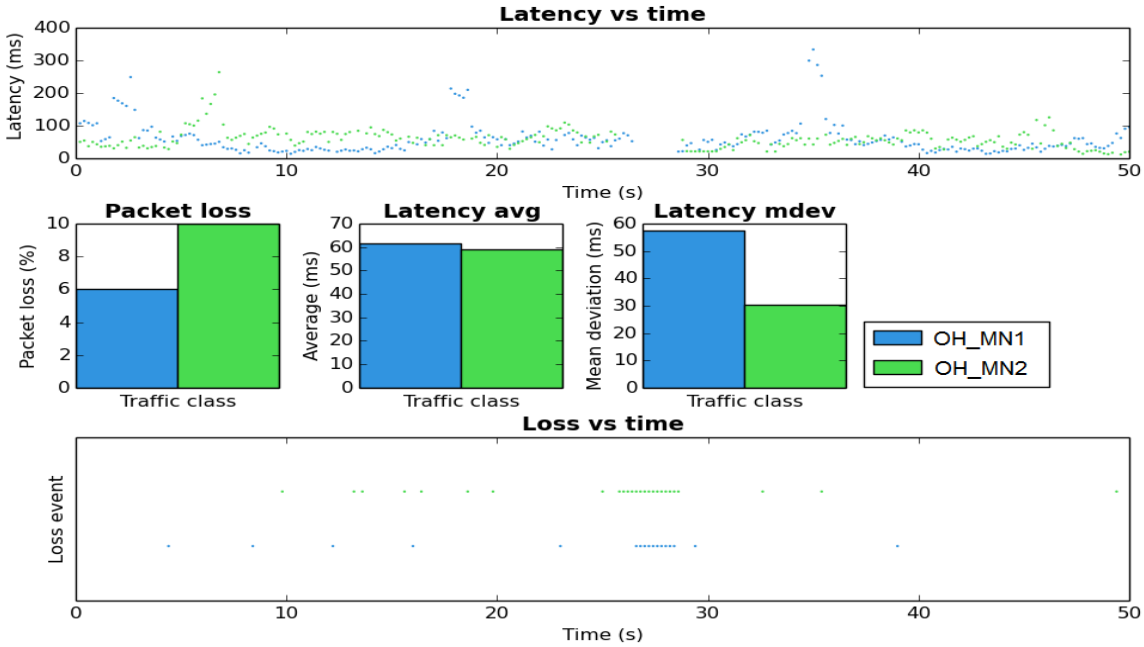


Figure 6-7: Intra-Overlay Handover ICMP Performance

6.3.9 INTER-OVERLAY TCP PERFORMANCE

Figure 6-8 highlights that inter-overlay handover introduces ~2s latency more than SDWN handover till resuming moving stations' average throughput. OH_STA2 undergoes inter-overlay handover between ~42s-47s while OH_STA1 undergoes SDWN handover between ~47s-50s. During handover, OH_STA2's average throughput 276KB/s drops to ~0.848KB/s for ~5s while OH_STA1's average throughput 144KB/s drops to ~27.8KB/s for ~3s. Again, figure 6-8 emphasizes that TCP average throughput depends mainly on how far the stations are from AP center not on handover.

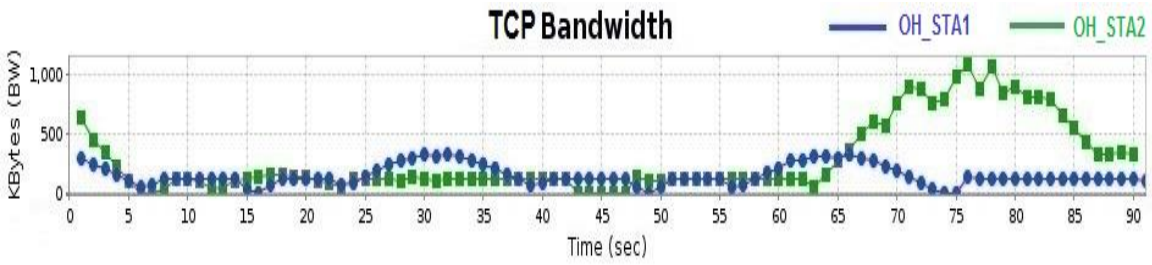


Figure 6-8: Inter-Overlay Handover TCP Throughput

6.3.10 INTER-OVERLAY TCP PERFORMANCE

Results are similar to intra-overlay handover. OH_STA1 undergoes SDWN handover between ~47-50s while OH_STA2 undergoes inter-overlay handover between ~51-55s. Both handovers induce instant decrease in average UDP throughput due to packets drop. UDP jitters depend mainly on how far stations are from AP center rather than on handover.

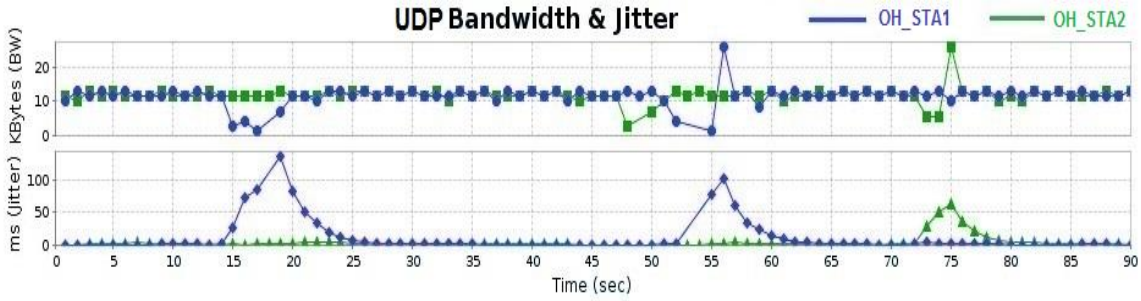


Figure 6-9: Inter-Overlay Handover UDP Throughput

6.4 EXPERIMENT 2: PROTOTYPING INTER-OVERLAY MOBILITY

6.4.1 OVERVIEW

This experiment prototypes inter-overlay mobility cross the two PDNs of ENTERPRISE_EC; EC_OH and EC_OF that are shown in figure 6-1. OH_MN1 and OH_MN2 move from their home network VLAN12 monitored by overlay EC_OH at PDN OH_SWL3 to foreign PDN OF_SWL3 monitored by mobility overlay EC_OF managed by the same SDN controller of ENTERPRISE_EC. Bandwidth is limited 2Mbps. Both OH_MN1 and OH_MN2 attached in foreign PDN OF_SWL3 initiate communication to OH_SERVER2 at their home network VLAN12. The virtual path to home network is established in different ways as OH_MN1 uses static IP while OH_MN2 uses DHCP for dynamic allocation of IP address. All activated MNs use the same established virtual path connecting home and foreign networks.

As OH_MN1 uses static IP address, each mobility entity in the path between foreign and home networks has a pre-register 'STATIC' profile stored in the SDN controller indexed by the hardware address of OH_MN1. Most likely the first packet to initiate the virtual path to home network is ARP_REQUEST for finding the hardware address of OH_SERVER2 or standard IP packet to OH_SERVER2 if the hardware address of OH_MN1 is stored in ARP cache of OH_SERVER2. In either case, the access switch broadcasts the packet to all ports as ARP_REQUEST has hardware destination broadcast address while the hardware destination address in standard IP packet is not mapped to any port in the CAM table of access switch. Thus, mobility DS connected to the access switch receives the packet and forwards it to the SDN controller to match the packet source hardware address with the DS's stored profiles. If match occurs, the output port is identified using HOME_ID stored in OH_MN1 profile and dynamic procedures for identifying the overlay topology. On identifying the output port, OH_MN1's mobility profile is activated and OpenFlow rules are installed on mobility DS to avoid future controller interruption. This process is repeated when the packet enter any mobility entity in the virtual path till reaching home access switch. Thus, the virtual path is recursively established and OH_SERVER's reply is wire speed forwarded using installed Open flow rules.

On the other hand, OH_MN2 uses DHCP for dynamic allocation of IP address. Unlike MN with static IP address, only home mobility DS needs to have a pre-registered 'DYNAMIC' profile for DHCP MN's that is stored in the home DS database at the SDN controller. 'ON_DEMAND' profile is created on the fly for successful activated DHCP MNs on other mobility entities without pre-configured profiles. The first packet for OH_MN2 is DHCP_DISCOVERY or DHCP_REQUEST message. Both messages are broadcast messages to find the DHCP server. Thus, both messages are always detected by mobility DS and forwarded to the SDN

controller to extract DHCP_CLIENT_ID. If DHCP_CLIENT_ID is mapped to valid HOME_ID and output port is determined using the dynamic procedures for identifying overlay topology, the message is relayed with the virtual IP of mobility switch to next hop. A record containing valuable parameters about DHCP_DISCOVERY or DHCP_REQUEST message is stored in mobility DS's switch buffer. This process is repeated when the DHCP message enters any mobility switch till reaching home access switch. OH_MN2's mobility profile is activated when receiving DHCP_ACKNOWLEDGE matching the record of DHCP_REQUEST message stored in the switch buffer. The virtual path is established by installing OpenFlow rules with the first non DHCP packets entering the mobility switch for an activated MN.

6.4.2 Inter-Overlay Mobility Setup Delay

The virtual path established between foreign and home networks passes through these entities:

Overlay EC_OF [AS ↔ DS ↔ MG] ↔ Overlay EC_OH [RS ↔ DS ↔ AS]

6.4.2.1 Mobility Setup Delay for OH_MN1 using Static IP

Activation of OH_MN1's mobility profile suffers from these delays:

Access	~0.01s	Static	~0.02s

- **Forward Setup Delay:**
  ≅ (0.01s [AS: access] + 2 x 0.02s [DS & MG/RS: static]) x 2 [EC_OF & EC_OH] ≅ 0.1s
- **Backward Setup Delay:** Total Active Flow + Propagation ≅ Wire Speed
- **Mobility Setup Delay:** ≅ **<u>0.1s</u>**

6.4.2.2 Mobility Setup Delay for OH_MN2 using DHCP

Activation of OH_MN2's mobility profile suffers from these delays:

Access	~0.01s	DHCP Relay	FD	~0.03s	BK	~0.02s

- **Forward Setup Delay:**
  ≅ (0.01s [AS: access] + 2 x 0.03s [DS & MG/RS: DHCP FD]) x 2 [EC_OF & EC_OH] ≅ 0.14s
- **Backward Setup Delay:**
  ≅ (0.01s [AS: access] + 2 x 0.02s [DS & RS/MG]: DHCP BK]) x 2 [EC_OF & EC_OH] ≅ 0.1s
- **Mobility Setup Delay:** ≅ 0.14s + 0.1s ≅ **<u>0.24s</u>**

6.4.3 Inter-Overlay Mobility Re-Activation Delay

Mobility re-activation delay for expired OpenFlow rule is the same for OH_MN1 and OH_MN2.

Re-Activation	0.01s	Access	0.01s

- **Mobility Re-Activation Delay:**
  ≅ (0.01s [AS: access] + 2 x 0.01s [DS & MG/RS: re-active]) x 2 [EC_OH & EC_OF] ≅ 0.06s

6.4.4 INTER-OVERLAY ICMP LATENCY AND PACKETS LOSS

This section analyzes the performance of inter-overlay mobility versus that of standard network connecting foreign and home networks of OH_MN2 at ENTERPRISE_EC. This is achieved through comparing performance of OH_MN2 and OF_HOST2 located on the same switch OF_SWL3 when communicating to OH_SERVER2. OH_MN2 is an active mobility subscriber using the mobility overlay while OF_HOST2 is a standard host using standard L3 network. This section compares the latency experienced in 100 ICMP pings sent from OF_HOST2 to OH_SERVER2 through standard network and those sent from OH_MN2 to OH_SERVER2 through the mobility overlay with and without OpenFlow rules installation on the mobility entities.

6.4.4.1 WITHOUT OPENFLOW RULES

The comparison in figure 6-10 reveals that L3 network induces ~17ms average latency with deviation of ~3-4ms while that of mobility overlay is in range of ~47ms average latency with deviation of ~15ms without OpenFlow rules installation on the mobility switch. The large value of standard deviation in mobility overlay sounds reasonable as it represents the utilization of SDN controller not a fixed problems facing the mobility overlay.

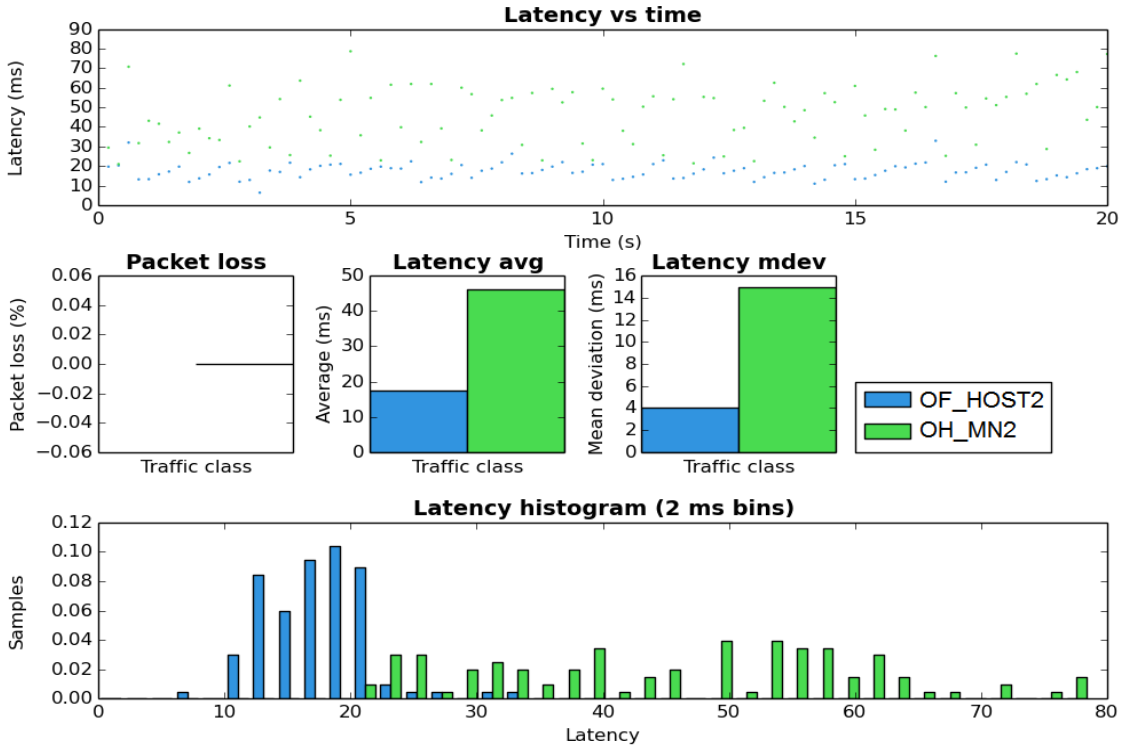


Figure 6-10: Inter-Overlay ICMP Performance – No OpenFlow

6.4.4.2 WITH OPENFLOW RULES

The recursive relay feature presented in the mobility framework separates between OH_MN2's standard packets and DHCP messages that require continuous monitoring by the SDN Controller. With this feature, OpenFlow rules make advancement to latency in the mobility overlay network as shown in figure 6-11. After installation of OpenFlow rules, the mobility overlay's performance reaches wire speed with ~0ms average latency and deviation of ~0.1ms in comparison to ~17ms average latency with ~3-4ms deviation in standard network.

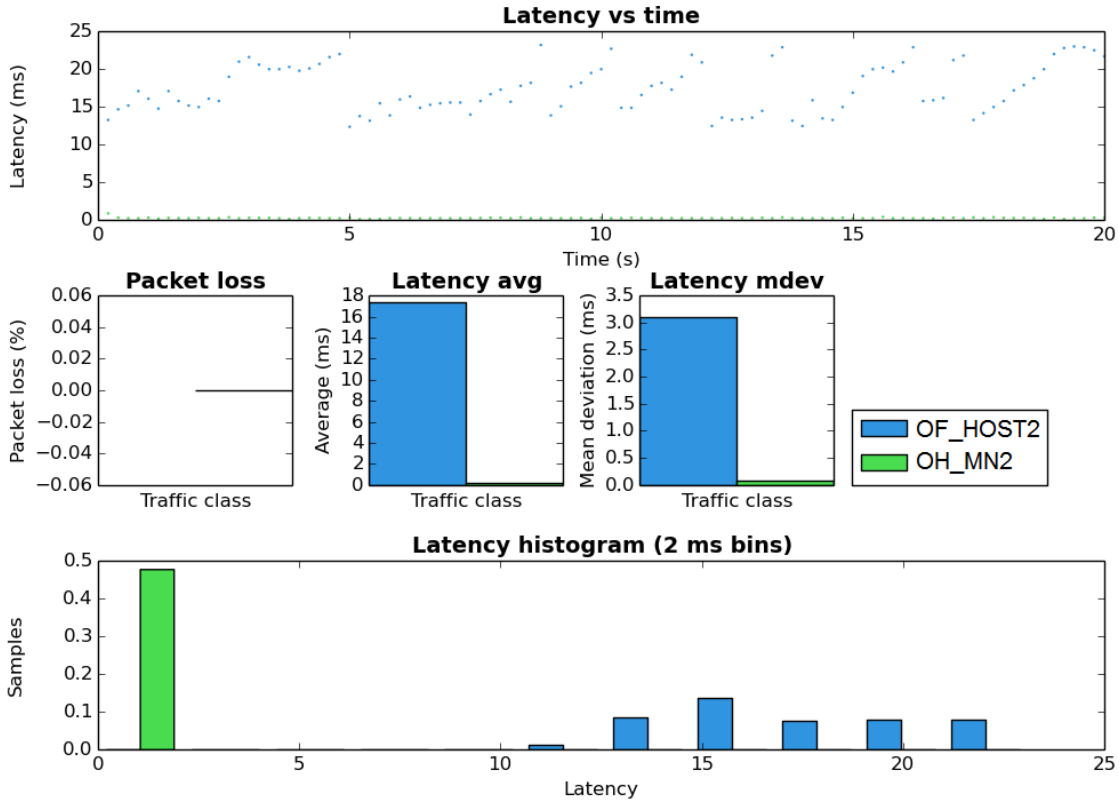


Figure 6-11: Inter-Overlay ICMP Performance – OpenFlow

6.4.5 INTER-OVERLAY TCP AND UDP PERFORMANCE

6.4.5.1 WITHOUT OPENFLOW RULES

The comparison in figure 6-12 reveals that both standard network and inter-overlay mobility, without installation of OpenFlow rules, almost have the same performance in UDP but inter-overlay mobility suffers from higher jitter than standard network. Concerning TCP performance, inter-overlay mobility's throughput is slightly better than standard network.

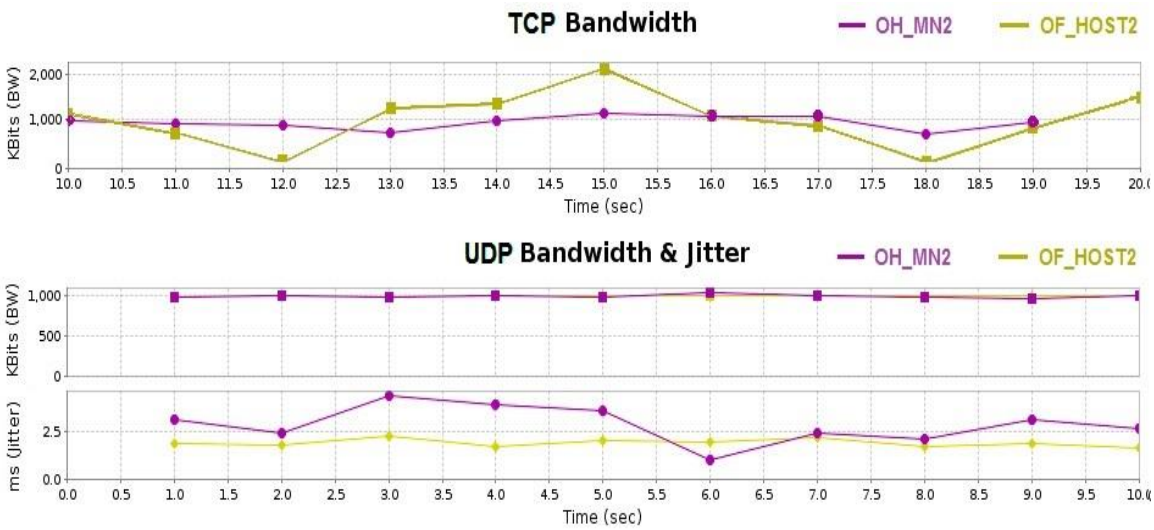


Figure 6-12: Inter-Overlay vs. Standard Network in TCP and UDP - No OpenFlow

6.4.5.2 WITH OPENFLOW RULES

The comparison in figure 6-13 reveals that installation of OpenFlow rules dramatically improves the performance of inter-overlay mobility over standard network. Concerning TCP performance, inter-overlay mobility's throughput exceeds double (~62%) of standard network. On the hand, UDP performance is still the same but the inter-overlay mobility's jitter level is dramatically improved till being almost negligible. In summary, installation of OpenFlow rules in the mobility overlay improves inter-overlay's performance to wire speed and removes jitter from UDP communications.

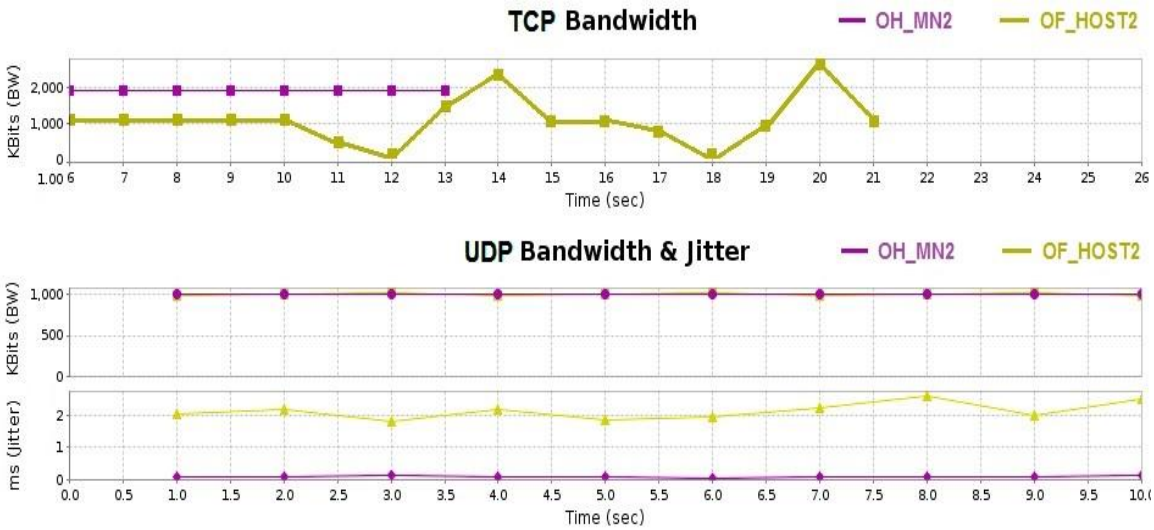


Figure 6-13: Inter-Overlay vs. Standard Network in TCP and UDP - OpenFlow

6.5 EXPERIMENT 3: PROTOTYPING DIRECT INTER-DOMAIN MOBILITY

6.5.1 OVERVIEW

This experiment prototypes direct inter-domain mobility cross ENTERPRISE_EA and ENTERPRISE_EB. Each enterprise has a separate SDN controller. Mobility overlays EA_OA and EB_OB are connected to access aggregation switches of ENTERPRISE_EA and ENTERPRISE_EB, respectively, for dynamic establishment of the tunnels required for direct inter-domain mobility when detecting trials from EA_MN1 and EA_MN2 of ENTERPRISE_EA to join ENTERPRISE_EB. The bandwidth between ENTERPRISE_EA and ENTERPRISE_EB is limited to 2Mbps. Both EA_MN1 and EA_MN2, roaming at ENTERPRISE_EB, initiate sessions with EA_SERVER2 located at their home network VLAN12 in ENTERPRISE_EA. The activated virtual path is used by both EA_MN1 and EA_MN2 thus the first subscriber initiating the path suffers from tunnel delay; ENTERPRISE_EB → ENTERPRISE_EA. Once the virtual path is active, no more tunnel delay is added to the activation delay of other MNs. Mobility setup delays for EA_MN1 and EA_MN2 are different as the former uses static IP address while the latter uses DHCP for dynamic allocation of IP address.

6.5.2 DIRECT INTER-DOMAIN MOBILITY SETUP DELAY

The virtual path established through the mobility overlay network between foreign network, ENTERPRISE_EB, and home network, ENTERPRISE_EA, passes through these mobility entities:

Overlay EB_OB [AS ↔ DS ↔ MG] ↔ Overlay EA_OA [MG ↔ DS ↔ AS]

6.5.2.1 MOBILITY SETUP DELAY FOR EA_MN1 USING STATIC IP

Activation of EA_MN1's mobility profile suffers from these delays:

ACCESS	~0.01S	STATIC	~0.01S	TUNNEL	SETUP	~1S	PROPAGATION	~0.02S

- **FORWARD SETUP DELAY:**

  – INACTIVE TUNNEL:
  ≅ (0.01S [AS: ACCESS] + 0.02S [DS: STATIC] + 1S [MG: TUNNEL.S]) X 2 [EB_OB & EA_OA] ≅ 2.06S

  – ACTIVE TUNNEL:
  ≅ (0.01S [AS: ACCESS] + 2 X 0.01S [DS & MG/RS: STATIC] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EA_OA] ≅ 0.1S

- **BACKWARD SETUP DELAY:**
  ≅ TOTAL ACTIVE FLOW + PROPAGATION ≅ 0.02 [MG: TUNNEL.P] X 2 [EA_OA & EB_OB] ≅ 0.04S

- **MOBILITY SETUP DELAY:**
  – INACTIVE TUNNEL: ≅ 2.06S + 0.04S ≅ **2.1S**

  – ACTIVE TUNNEL: ≅ 0.1S + 0.04S ≅ **0.14S**

6.5.2.2 MOBILITY SETUP DELAY FOR EA_MN2 USING DHCP

Activation of EA_MN2's mobility profile suffers from these delays:

ACCESS	~0.01S	DHCP RELAY	FD	~0.03S	BK	~0.02S	TUNNEL	SETUP	~1S	PROPAGATION	~0.02S

- **FORWARD SETUP DELAY:**

  – INACTIVE TUNNEL:
  ≅ (0.01S [AS: ACCESS] + 0.03S [DS: DHCP FD] + 1S [MG: TUNNE.S]) X 2 [EB_OB & EA_OA] ≅ 2.08S

  – ACTIVE TUNNEL:
  ≅ (0.01S [AS: ACCESS] + 2 X 0.03S [DS & MG: DHCP FD] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EA_OA]
  ≅ 0.18S

- **BACKWARD SETUP DELAY:**
  ≅ (0.01S [AS: ACCESS] + 2 X 0.02S [DS & MG]: DHCP BK] + 0.02 [MG: TUNNEL.P]) X 2 [EA_OA & EB_OB]
  ≅ 0.14S

- **MOBILITY SETUP DELAY:**
  – INACTIVE TUNNEL: ≅ 2.08s + 0.14s ≅ **2.22s**

  – ACTIVE TUNNEL: ≅ 0.18s + 0.14s ≅ **0.32s**

6.5.3 DIRECT INTER-DOMAIN MOBILITY RE-ACTIVATION DELAY

Mobility re-activation delay for expired OpenFlow rule is the same for OA_MN1 and OA_MN2.

RE-ACTIVATION	~0.01S	ACCESS	~0.01S	TUNNEL PROPAGATION	~0.02S

- **MOBILITY RE-ACTIVATION TIME:**
  ≅ (0.01S [AS: ACCESS] + 2 X 0.01S [DS & MG: RE-ACTIVE] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EA_OA]
  ≅ 0.1S

6.5.4 DIRECT INTER-DOMAIN ICMP LATENCY AND PACKETS LOSS

This section analyzes the performance of direct inter-domain mobility versus that of standard network connecting foreign network, ENTERPRISE_EB, and home network, ENTERPRISE_EA of EA_MN2. This is achieved through comparing performance of EA_MN2 and EB_HOST2, located on the same switch EB_SWL3 of ENTERPRISE_EB, when communicating to EA_SERVER2. EA_MN2 is an active mobility subscriber using the mobility overlay while EB_HOST2 is a standard host using standard L3 network. This experiment compares the latency experienced in 100 ICMP pings sent from EB_HOST2 to EA_SERVER2 through standard network and those sent from EA_MN2 to EA_SERVER2 through the mobility overlay with and without OpenFlow rules installation on the mobility entities.

6.5.4.1 WITHOUT OPENFLOW RULES

The comparison in figure 6-14 reveals that standard network induces ~14-17ms average latency with deviation of ~4ms while that of mobility overlay is in range of ~52 average latency with deviation of ~13ms without OpenFlow rules installed on the mobility switch. The average latency has increased from ~47ms in inter-overlay to ~52ms as of the induced WAN propagation and tunnel delays. The large value of standard deviation in the mobility overlay sounds reasonable as it represents the utilization of the SDN controller not fixed problems facing the mobility overlay.

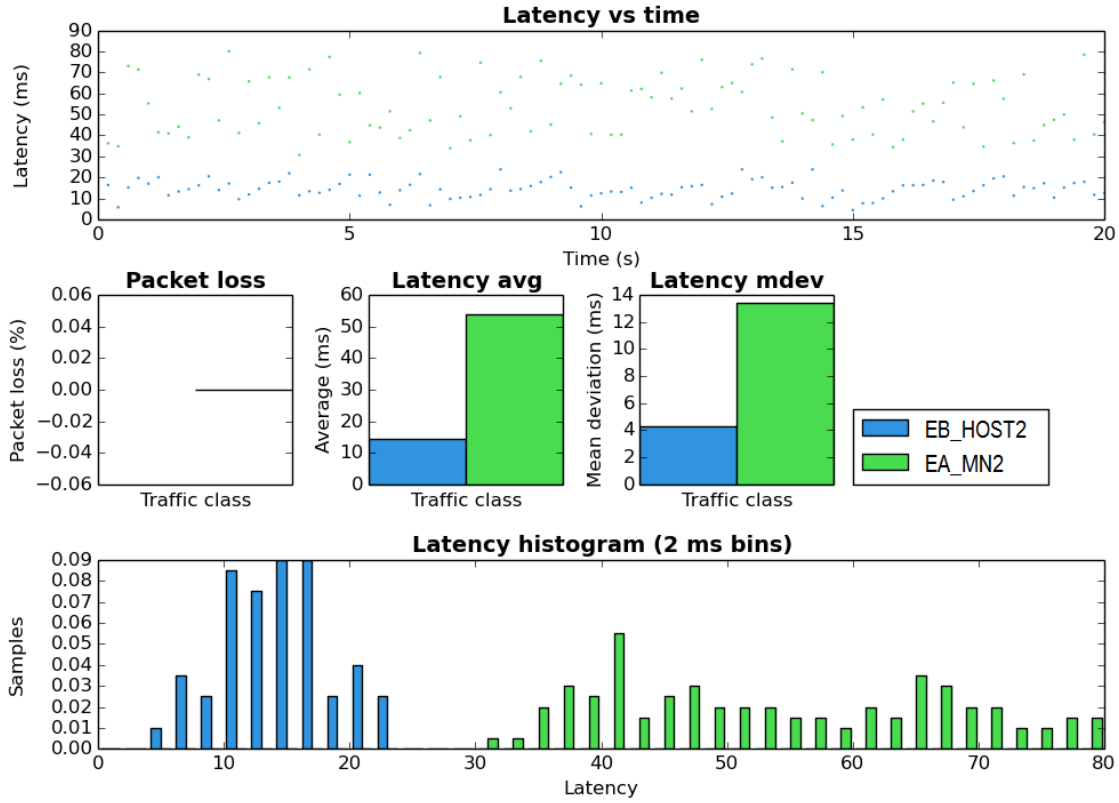


Figure 6-14: Direct Inter-Domain ICMP Performance – No OpenFlow

6.5.4.2 WITH OPENFLOW RULES

The recursive relay feature presented in the mobility framework separates between EA_MN2's standard packets and DHCP messages that require continuous monitoring by the SDN Controller. With this feature, OpenFlow rules make advancement to latency in the mobility overlay as shown in figure 6-15. After installation of OpenFlow rules, the mobility overlay network's average latency decreases from ~52ms with deviation ~13ms to average latency of ~16ms with deviation ~4.5ms which is almost equivalent or slightly better than that standard network.

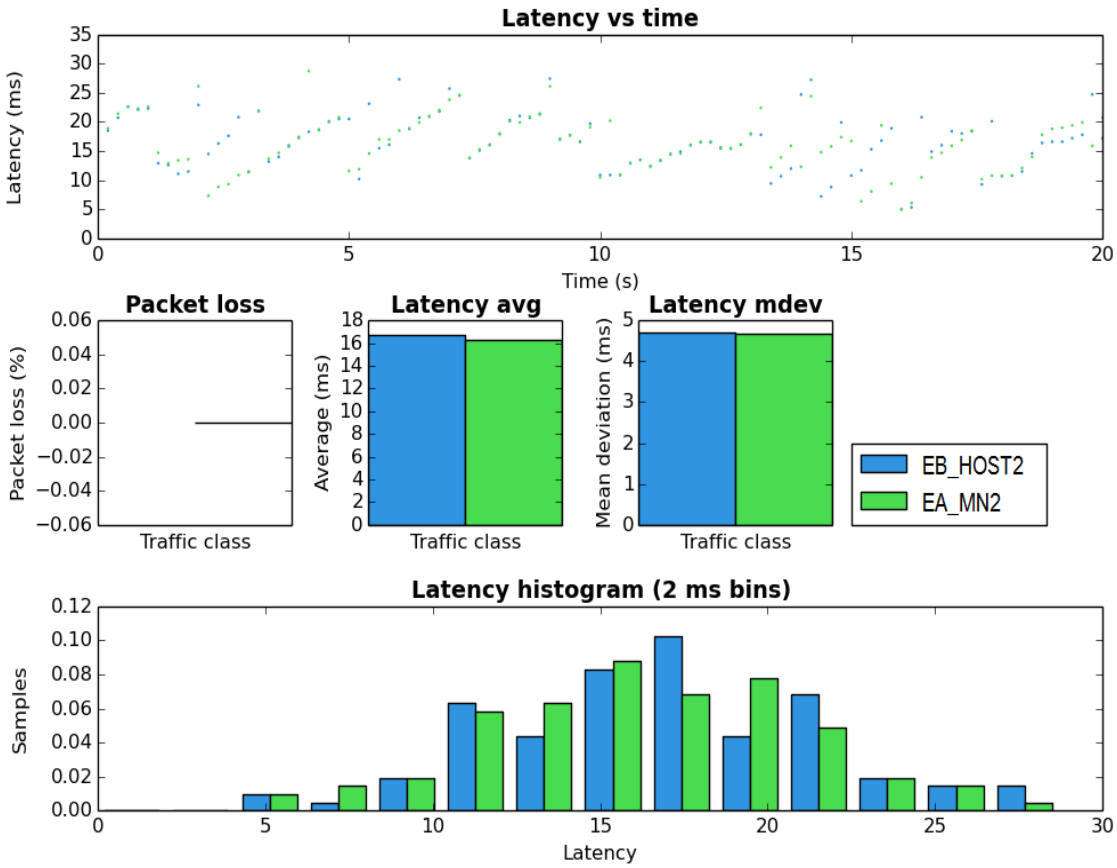


Figure 6-15: Inter-Domain ICMP Performance – OpenFlow

6.5.5 DIRECT INTER-DOMAIN TCP AND UDP PERFORMANCE

6.5.5.1 WITHOUT OPENFLOW RULES

The comparison in figure 6-16 reveals that standard network has higher TCP throughput than direct inter-domain mobility, without installation of OpenFlow rules. Moreover, UDP performance has slightly lower throughput with higher jitter level in direct inter-domain mobility without installation of OpenFlow rules when compared to standard network performance.

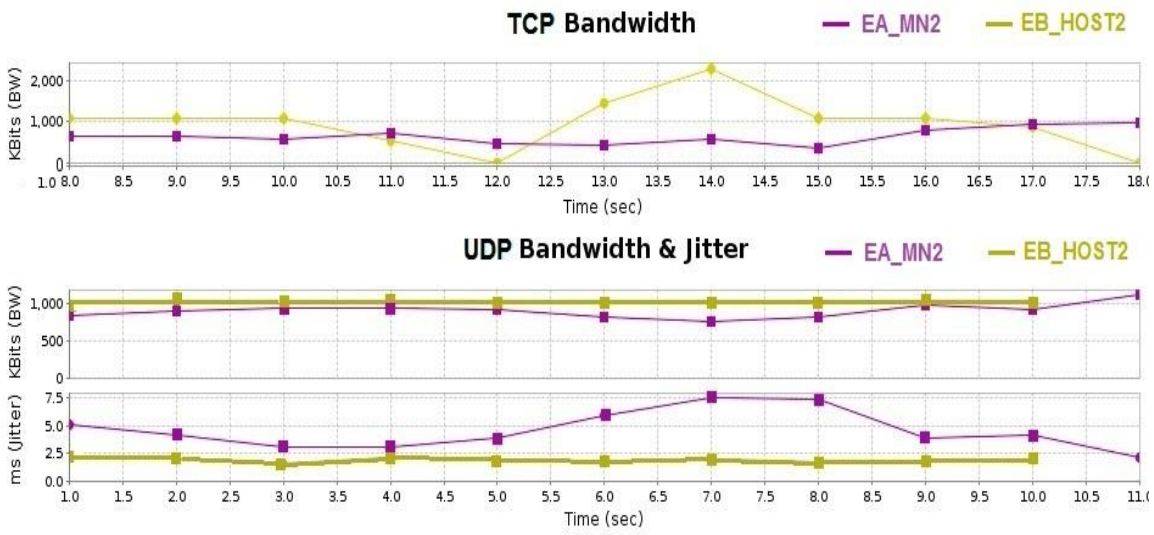


Figure 6-16: Direct Inter-Domain vs. Standard Network in TCP and UDP - No OpenFlow

6.5.5.2 WITH OPENFLOW RULES

The comparison in figure 6-17 reveals that installation of OpenFlow rules dramatically improves the performance in direct inter-domain mobility network over standard networks. Concerning TCP performance, inter-domain mobility's throughput becomes slightly better than standard network. On the hand, UDP throughput and jitter level becomes equivalent to that of standard network.

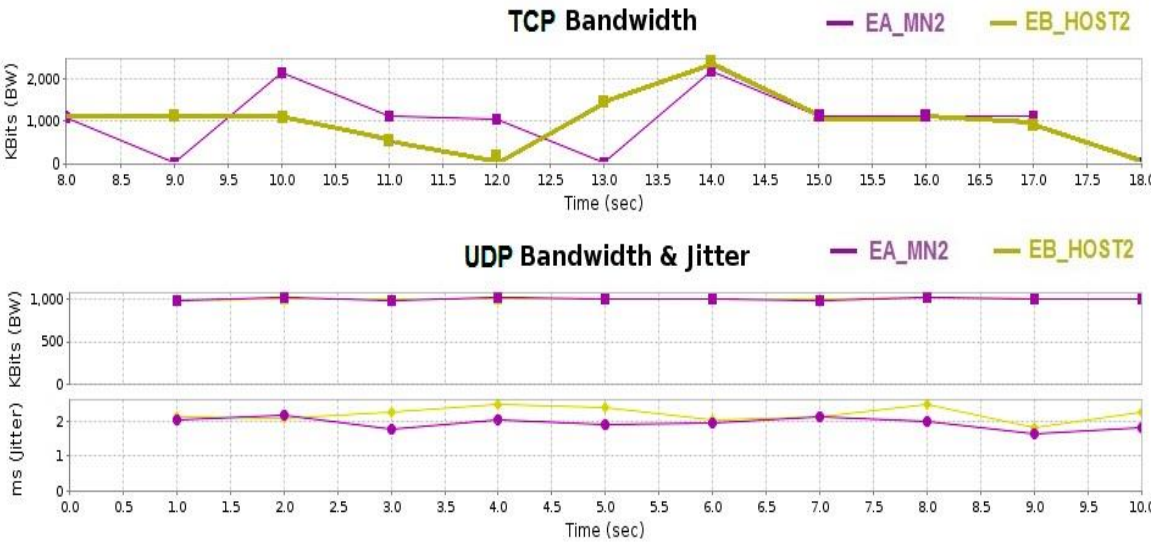


Figure 6-17: Direct Inter-Domain vs. Standard Network in TCP and UDP - OpenFlow

6.6 EXPERIMENT 4: PROTOTYPING INDIRECT INTER-DOMAIN MOBILITY

6.6.1 OVERVIEW

This experiment prototypes indirect inter-domain mobility cross ENTERPRISE_EB and ENTERPRISE_EC through the transient network of ENTERPRISE_EA. Each enterprise has a separate SDN controller. Mobility overlay EA_OA, EB_OB, and EC_OC are connected to the access aggregation switches of ENTERPRISE_EA, ENTERPRISE_EB and ENTERPRISE_EC respectively. These overlays dynamically establish the tunnels required for indirect inter-domain mobility when detecting trails from OF_MN1 and OF_MN2, from ENTERPRISE_EC to join ENTERPRISE_EB. MG routing table of ENTERPRISE_EB identifies that the next hop to ENTERPRISE_EC is MG of ENTERPRISE_EA, thus a transient tunnel is established to ENTERPRISE_EA which in turn establish another tunnel to ENTERPRISE_EC. The bandwidth cross ENTERPRISE_EA, ENTERPRISE_EB and ENTERPRISE_EC is 2Mbps. Both OF_MN1 and OF_MN2, roaming at ENTERPRISE_EB, initiate sessions with EC_SERVER2 at their home VLAN12 in ENTERPRISE_EC. The activated virtual path is used by both OF_MN1 and OF_MN2 thus the first subscriber initiating the path suffers from the delay of establishing two tunnels; ENTERPRISE_EB → ENTERPRISE_EA and ENTERPRISE_EA → ENTERPRISE_EC. If ENTERPRISE_EA has an active tunnel to ENTERPRISE_EC, the first subscriber at ENTERPRISE_EB initiating the path suffers from the delay of establishing one tunnel only; ENTERPRISE_EB → ENTERPRISE_EA. Once the tunnels are active, no more tunnel delay is added to the activation of other MNs. Mobility setup delays for OF_MN1 and OF_MN2 are different as the former uses static IP address while the latter uses DHCP for dynamic allocation of IP address.

6.6.2 INDIRECT INTER-DOMAIN MOBILITY SETUP DELAY

The virtual path established between foreign network ENTERPRISE_EB and home network ENTERPRISE_EC through ENTERPRISE_EA passes through these mobility entities:

Overlay EB_OB [AS ↔ DS ↔ MG] ↔ Overlay EA_OA [MG] ↔ Overlay EC_OF [MG ↔ DS ↔ AS]

6.6.2.1 MOBILITY SETUP DELAY FOR OF_MN1 USING STATIC IP

Activation of OF_MN1's mobility profile suffers from these delays:

ACCESS	~0.01S	STATIC	~0.01S	TUNNEL	SETUP	~1S	PROPAGATION	~0.02S

- **FORWARD SETUP DELAY:**
  - **– INACTIVE TUNNEL:**
    ≅ (0.01S [AS: ACCESS] + 0.01S [DS: STATIC] + 1S [MG: TUNNEL]) X 2 [EB_OB & EC_OF]
    + 2 X 1S [EA_OA MG: TUNNEL] ≅ 4.04s

– **ACTIVE TUNNEL:**
≅ (0.01S [AS: ACCESS] + 2 X 0.01S [DS & MG: STATIC] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EC_OF]
+ (0.01S [MG: STATIC] + 2 X 0.02S [MG: TUNNEL.P]) [EA_OA] ≅ 0.15S

- **BACKWARD SETUP DELAY:**
≅ TOTAL ACTIVE FLOW + PROPAGATION ≅ 0.02 [MG: TUNNEL.P] X 4 [EC_OC & 2XEA_OA & EB_OB] ≅ 0.08S
- **MOBILITY SETUP DELAY:**
– **INACTIVE TUNNEL:** ≅ 4.04S + 0.08S ≅ **4.12S**
– **ACTIVE TUNNEL:** ≅ 0.15S + 0.08S ≅ **0.23S**

6.6.2.2 MOBILITY SETUP DELAY FOR OF_MN2 USING DHCP

Activation of OF_MN2's mobility profile suffers from these delays:

ACCESS	~0.01S	DHCP RELAY	FD	~0.03S	BK	~0.02S	TUNNEL	SETUP	~1S	PROPAGATION	~0.02S

- **FORWARD SETUP DELAY:**
– **INACTIVE TUNNEL:**
≅ (0.01S [AS: ACCESS] + 0.03S [DS: DHCP FD] + 1S [MG: TUNNEL.S]) X 2 [EB_OB & EC_OC]
+ 2 X 1S [EA_OA MG: TUNNEL.S] ≅ 4.08S
– **ACTIVE TUNNEL:**
≅ (0.01S [AS: ACCESS] + 2 X 0.03S [DS & MG: DHCP FD] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EC_OC]
+ (0.03S [MG: DHCP FD] + 0.02 [MG: TUNNEL.P]) X 2 [EA_OA]≅ 0.28S
- **BACKWARD SETUP DELAY:**
≅ (0.01S [AS: ACCESS] + 2 X 0.02S [DS & MG: DHCP BK] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EC_OC]
+ (0.02S [MG: DHCP BD] + 2 X 0.02 [MG: TUNNEL.P]) [EA_OA]≅ 0.2S
- **MOBILITY SETUP DELAY:**
– **INACTIVE TUNNEL:** ≅ 4.08S + 0.2S ≅ **4.28S**
– **ACTIVE TUNNEL:** ≅ 0.28S + 0.2S ≅ **0.48S**

6.6.3 INDIRECT INTER-DOMAIN MOBILITY RE-ACTIVATION DELAY

Mobility re-activation delay for expired OpenFlow rule is the same for OF_MN1 and OF_MN2.

RE-ACTIVATION	~0.01S	ACCESS	~0.01S	TUNNEL PROPAGATION	~0.02S

- **MOBILITY RE-ACTIVATION TIME:**
≅ (0.01S [AS: ACCESS] + 2 X 0.01S [DS & MG: RE-ACTIVE] + 0.02 [MG: TUNNEL.P]) X 2 [EB_OB & EA_OA]
+ (0.01S [MG: RE-ACTIVE] + 2 X 0.02 [MG: TUNNEL.P]) [EA_OA] ≅ **0.13S**

6.6.4 INDIRECT INTER-DOMAIN ICMP LATENCY AND PACKETS LOSS

This section analyzes the performance of indirect inter-domain mobility versus that of standard network connecting foreign network, ENTERPRISE_EB, and home network, ENTERPRISE_EC, through transient network ENTERPRISE_EA. This is achieved through performance comparison of OF_MN2 and EB_HOST2, located on the same switch EB_SWL3 of ENTERPRISE_EB, when communicating with OF_SERVER2 at VLAN12 on switch OF_SWL3. OF_MN2 is an active mobility subscriber using the mobility overlay while EB_HOST2 is a standard host using standard network. This experiment compares the latency experienced in 100 ICMP pings sent from EB_HOST2 to OF_SERVER2 through standard network and those sent from OF_MN2 to OF_SERVER2 through mobility overlay with and without OpenFlow rules installation on mobility entities.

6.6.4.1 WITHOUT OPENFLOW RULES

The comparison in figure 6-18 reveals that standard L3 network induces ~18-19ms average latency with deviation of ~5-6ms while that of mobility overlay network is in range of ~79ms average latency with deviation of ~9-10ms without OpenFlow rules installed on the mobility switch. WAN propagation and tunnel delays lead to increase in the average latency from ~47ms in inter-overlay to ~52ms in direct inter-domain to ~79ms in indirect-zone mobility. Latency standard deviation in indirect inter-domain decreased than the previous two cases. This decrease sounds reasonable as WAN propagation and tunnel delays have almost fixed deviation at low link utilization which in turn decreases the variable effect of the SDN controller's utilization.

6.6.4.2 WITH OPENFLOW RULES

The recursive relay feature presented by the mobility framework separates between OF_MN2's standard packets and DHCP messages that require continuous monitoring by the SDN Controller. With this feature, OpenFlow rules make advancement to latency in the mobility overlay as shown in figure 6-19. After installation of OpenFlow rules, the mobility overlay network's average latency decreased from ~79ms with deviation of ~10ms to average latency of ~30ms with deviation ~7ms. Despite the dramatic improvement in indirect inter-domain mobility performance, standard network is still better due to the enormous latency imposed by the presence of two tunnels. With the adoption of OpenFlow advanced QoS techniques, indirect inter-domain mobility performance can be further improved.

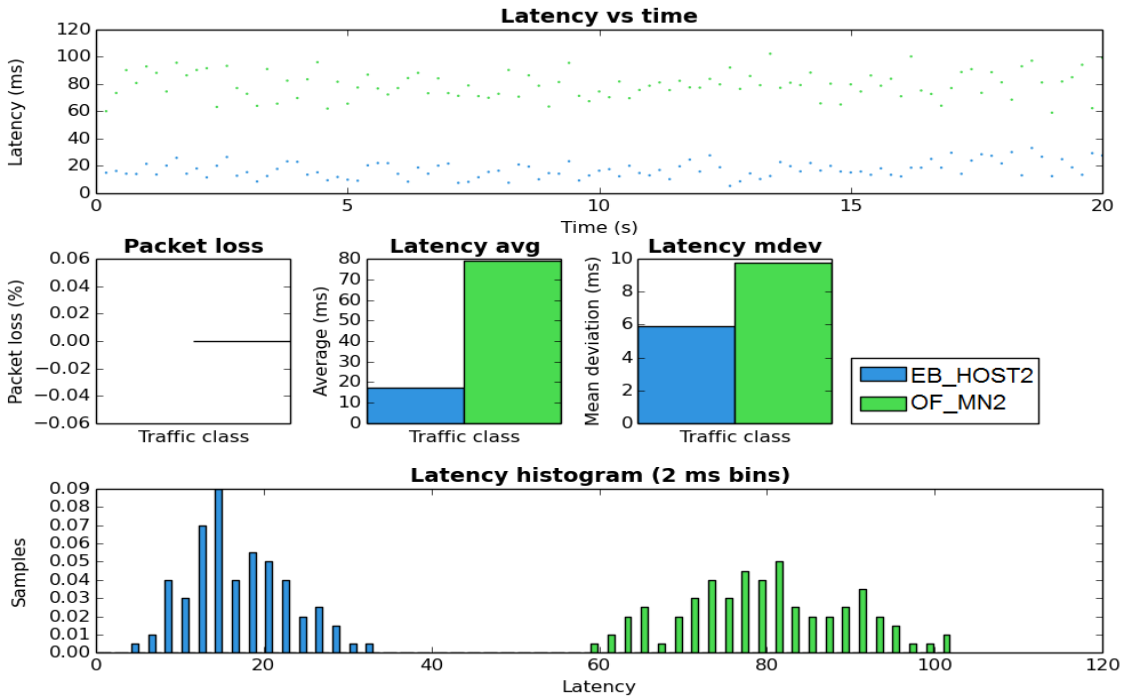


Figure 6-18: Indirect Inter-Domain ICMP Performance – No OpenFlow

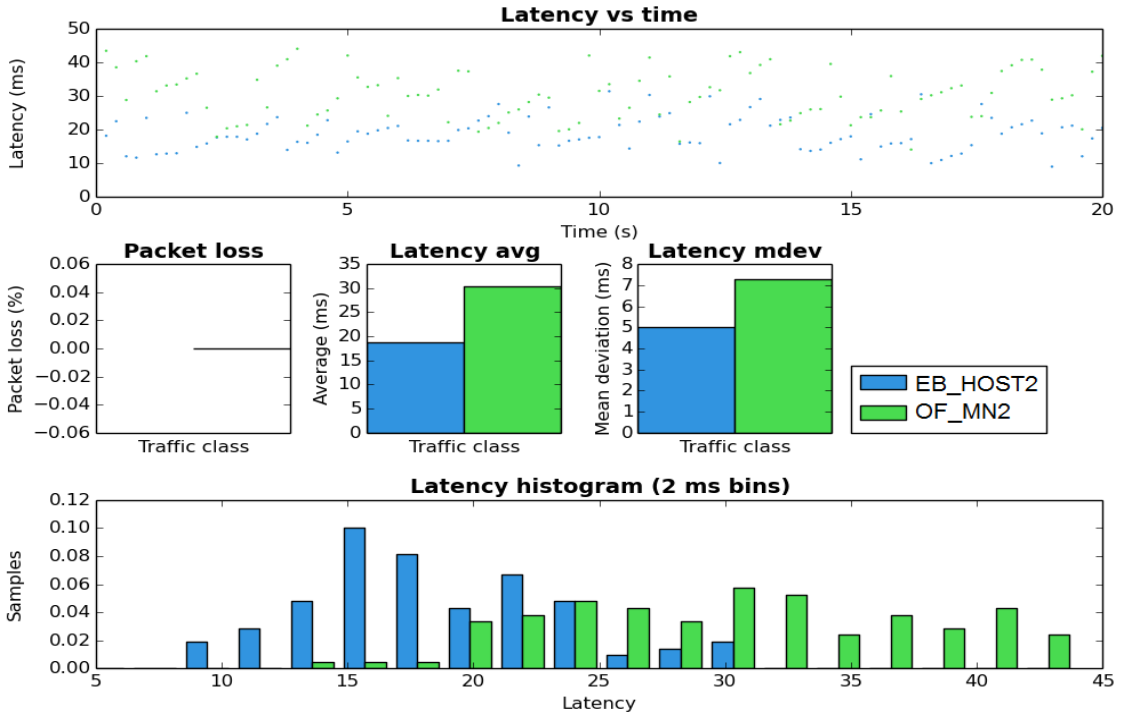


Figure 6-19: Indirect Inter-Domain ICMP Performance – OpenFlow

6.6.5 INDIRECT INTER-DOMAIN TCP AND UDP PERFORMANCE

6.6.5.1 WITHOUT OPENFLOW RULES

The comparison in figure 6-20 reveals dramatic decrease in the throughput of indirect inter-domain mobility without OpenFlow to almost ~53-56% of standard network. The presence of two tunnels decreases the effective utilization of available bandwidth to almost 25% in TCP and 40% in UDP when compared to standard network. Moreover, UDP jitter in inter-domain mobility is higher by ~25ms. These results would have been a major threat to the mobility framework feasibility in enterprise provided the separation of MNs' standard packets from the DHCP messages using the relay feature was not present.

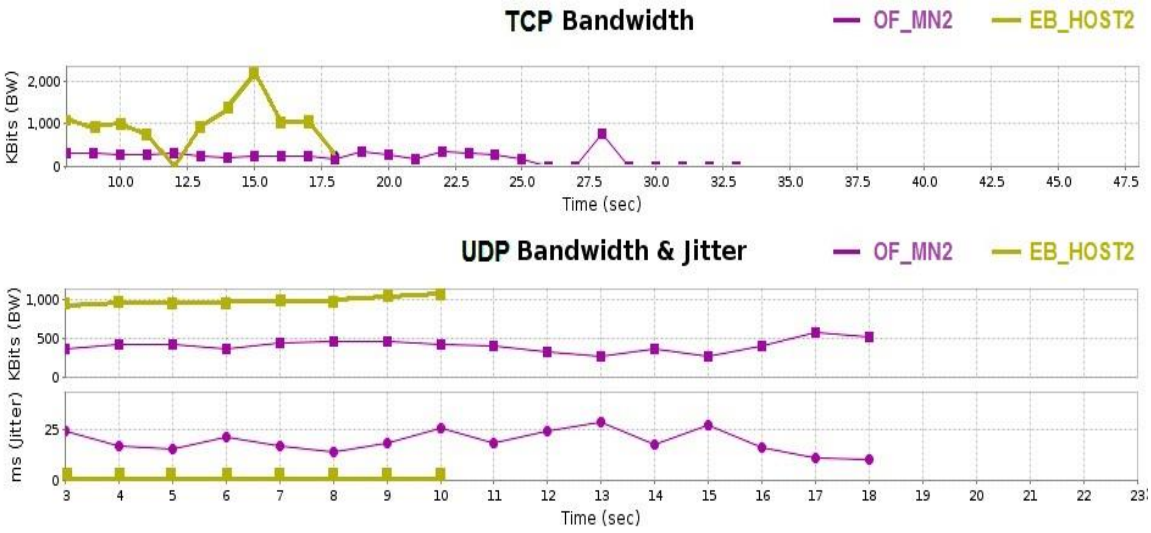


Figure 6-20: Indirect Inter-Domain vs. Standard Network in TCP and UDP - No OpenFlow

6.6.5.2 WITH OPENFLOW RULES

The comparison in figure 6-21 reveals that installation of OpenFlow rules creates tremendous improvement in the performance of indirect inter-domain mobility especially in UDP. Throughput and jitter levels of UDP in indirect inter-domain mobility become almost equivalent to that of standard L3 network. Concerning TCP performance, indirect inter-domain mobility throughput is improved from 53% of standard network to 82% after OpenFlow rules installation. These results emphasize the feasibility of the mobility frame cross enterprises with indirect mobility SLA as TCP throughput can be improved by adopting advance OpenFlow QoS techniques to guarantee effective bandwidth utilization in two tunnels virtual path cross the three enterprises.

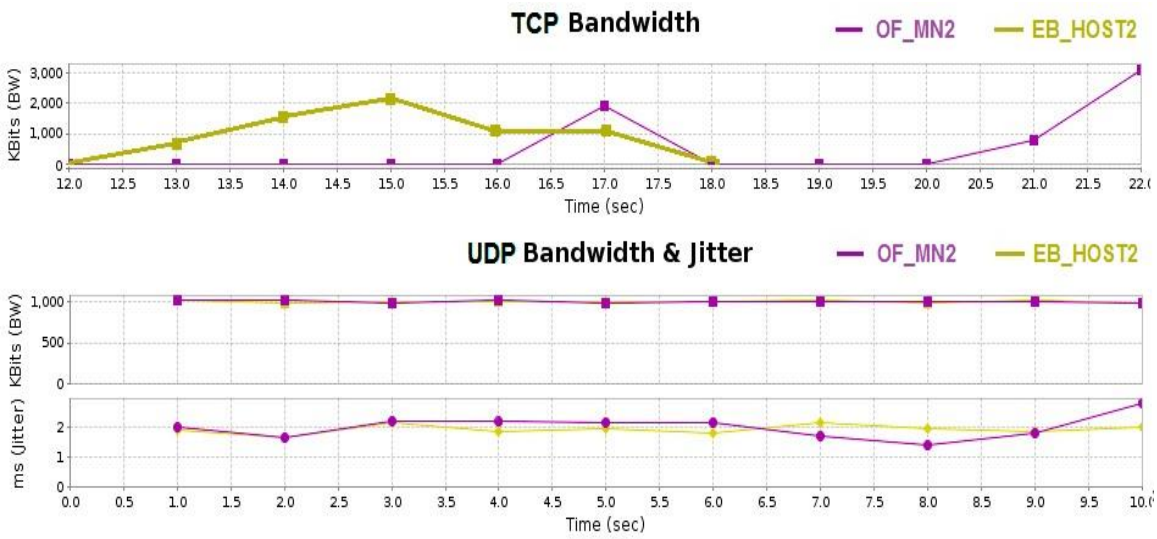


Figure 6-21: Indirect Inter-Domain vs. Standard Network in TCP and UDP - OpenFlow

7 SUMMARY, CONTRIBUTIONS, AND FUTURE WORKS

7.1 THESIS SUMMARY

Creating a mobility platform for collaborative interactions cross terminals and for continuous accessibility of smart residential/enterprises real time services through Wi-Fi/Cellular providers or cross carriers is no longer a dream with SDN in existing and next generation networks. The proposed mobility framework adopts OpenFlow SDN-based technology that is expected to be the 5G base. The research addresses the challenges hindering indoor services' accessibility and session continuity of static and mobile users/terminals in challenging situations as crossing cities' boundaries in car or train. These challenges include; the initial design concept that limits mobility to a method for preserving moving users' IP address to ensure continuous accessibility of static services not moving to moving terminals. Adoption of centralized tunnel gateways and lack route optimization techniques in mobility standard produce inefficient data forwarding plan that congests core networks. The complicated signaling and tunnels overheads increase latency and lead to non-inefficient bandwidth utilization. Existing mobility concept is limited to motion within a single carrier domain ignoring the urgent need for seamless services expansion cross carriers under service level agreements. Numerous motivating factors require overriding these challenges as collaborative interactions in IoT robotic clouds, increasing the role of WiFi to accommodate COPE and BYOD policies in full inter-domain mobility, session continuity for multimedia and real time services during wide area motion, and complimentary solution for IEEE 802.11p to support V2X services.

The objectives of this research are providing a uniform mobility framework with a scalable distributed architecture adopting OpenFlow SDN-based technology to eliminate mobility signaling overheads, restrict tunnel headers, synchronize network response and facilitate the invention of new routing mechanism with effective traffic offload technique to avoid the core congestion problem which restricts operators' mobility deployments in wide area motion and offerings for LIPA service. The scope is not limited to previous mobility concept of connecting mobile user to static location as home network, private cloud …etc but expanded to real time collaborative interactions between moving/static users, servers, terminals for facilitating cogitative services with minimum delay and latency and extending mobility coverage to cross operators under mobility SLAs to satisfy IoT requirements that are hardly solvable with existing mobility protocols.

Mobility is proposed as a service in the SDN application layer. During runtime, SDN controller transfers the rules instructed by the mobility service using API provided by the north bound interface to

hard coding rules that are forwarded by the south bound interface using OpenFlow to the infrastructure layer that controls real time operation of routers and switches. The proposed framework assigns three IP address and a unique identifier to MNs. The first is home address that is assigned by home DHCP service and the only IP address registered on MN's set. The second is care of address that is dynamically obtained from visited network to provide instant break out of new TCP sessions and UDP packets to avoid congesting core networks. The third is the SDN address that is used with MN's L2 address to uniquely distinguish MN's packets when accessing SDN NGN applications. A unique identifier is assigned to MN during subscription. This identifier is sent by MN in the DHCP_CLIENT_ID field of DHCP_REQUEST and DHCP_DISCOVERY messages during dynamic IP allocation process. This identifier guides virtual path establishment by next hop lookup process that is based on the indices of this identifier not subnet. A reverse lookup process is adopted to locate this identifier to guide the handover process. The framework suggests mapping the indices of this unique identifier to ISO 3166-1 alpha-2 codes for cross countries mobility in realistic deployment to create global mobility concept cross countries' boundaries.

OpenFlow virtual paths are established using a fully distributed tree structure of three tiers of OpenFlow switches. The first level is the access tier that controls widely geographically deployed access points in WLAN and cellular networks or acts as a backdoor to the access aggregation switches in standard networks. The second level is the detector tier representing the aggregation parent of several deployed access switches. Detector tier is responsible for orchestrating and mapping the various IP addresses assigned to MNs. The third level is relay and mobility gateway tier. The former is responsible for connecting several detector switches managed by a single SDN while the later is responsible for mobility cross carriers administrated by different SDN controllers. Such highly distributed tree structures facilitates dynamic establishment of overlay networks that extend mobility cross carriers under mobility service level agreement while hiding underlying infrastructure's complexities. The architecture is extremely scalable to accommodate the three tiers functions in a single OpenFlow switch for small deployment or each tier is represented by a set of multiple load-balanced OpenFlow switches to support carrier grade deployments. Moreover, a backward compatibility mode is proposed to integrate the three tiers structure to existing non-SDN infrastructure as LTE and standard networks. No hardware is required for fully migrated SDN infrastructure as mobility is provided as a service on deployed infrastructure as in virtual customer premises equipment and 5G that are SDN based. The design is fully aligned with ONF SDN arch 1.0, ONF OpenFlow spec 1.4, and RFC 7426 [32][33][34].

The logic behind mobility service is illustrated with five layers model describing the implementation detail of core functional modules. The first is detection layer that identifies foreign mobility subscribers and spoofs their presence in home networks. The second is classification layer that categorizes network packets to different classes matching the upper layers for faster processing while eliminating broadcasts and false detected packets from interrupting the SDN controller in the future. The third is parsing layer that undergoes three phases on input raw packets. The initial phase is identification of all valuable information from raw packets then generating summary vector. The output verifies if the packet is correctly classified or not. For improper classification, the packet is forward to lower layer again to identify the second best matching class. The identification phase is followed by learning phase to filter spoofing attacks and to identify if action is previously determined to similar packets to avoid wasting extra processing in the upper layers. The learning phase is followed by the triggering phase that selects matching action procedure in the upper layers. The fourth is the action layer which comprises the various switching and routing procedures for intra-domain and inter-domain mobility. Moreover, this layer is responsible for dynamic discovery of mobility topology and virtual path between home and foreign networks. After successful discovery of the virtual path, the fifth layer is triggered for activating the mobility service and orchestration of the VAS offered to roaming MNs. Service activation includes activation of mobility profiles and installation of OpenFlow rules to avoid future processing by SDN controller. The orchestration includes synchronization of billing systems cross carriers and activation of on-demand services in foreign network beyond the home registered group profile.

A prototype is established to show the feasibility of the proposed framework inside and cross carriers with direct/indirect mobility agreements. Mobility cross carriers is referred to as inter-domain mobility while that inside carrier is referred to intra-domain mobility. The second type is divided into intra-overlay and inter-overlay mobility. The former represents MNs' handover cross multiple access mobility switches connected to a single detector mobility switch. This is equivalent to handover cross S-GW in LTE connected to a single P-GW. The latter is equivalent to handover cross carriers' PDNs that are wide geographically located. This situation is faced during motion inside car or train crossing cities' boundaries. In existing mobility solution, either MN's sessions are disconnected as of new IP lease from a different PDN or all MN's packets are tunneled to previous PDN leading to the congestion of core networks. The framework shows how it overcomes this challenge with inter-overlay handover while preserving existing sessions and establishing virtual paths with effective offload mechanism. The next section gives a brief summary of the results obtained from mobility experiments on the established prototypes.

7.2 SUMMARY OF EXPERIMENTS RESULTS

7.2.1 MOBILITY INSIDE RAN

The objective from this experiment is prototyping the proposed mobility platform in an environment similar to 4G LTE and comparing results versus those published by Cisco PMIP and those obtained from experimenting standard SDWN. Results reveals that inside carriers, wire speed forwarding is guaranteed as of signaling overhead elimination, tunnel headers removal, and SDN-OpenFlow hardware abstraction. Session continuity is assured for standard and wide area motion in challenging mobility situations as cars or train crossing cities' boundaries. LTE GTP/PMIP tunnels prove to be ~2-10% lower than standard network performance. In the established prototype, OpenFlow SDN-based structure shows higher throughput with lower latency and more agility over standard network. Mobility setup delay is improved from ~0.5s LTE bearer setup to ~0.2s as of recursive virtual path establishment using inline DHCP messages without any GTP/PMIP out-band control messages. New routing mechanism based on UEMS_ID next hop lookup instead of destination subnet is adopted to convert intra-overlay and inter-overlay handovers to profile update processes. Intra-overlay handover inside city is ~0.1s which is equivalent to standard SDWN but better than LTE S-GWs handover of ~0.25s. Inter-overlay handover ensures session continuity when crossing several cities' PDNs with seamless extension of residential/enterprise services using effective L4 parser to offload UDP packets and new TCP sessions at the new attached PDN. Only pre-established TCP sessions and home packets traverse core network to avoid the congestion problem. Inter-overlay handover cross cities is ~0.15s. In LTE, handover cross cities' P-GWs is not supported. Total bearer setup of ~0.5s is required. After handover, results show that jitters level and throughput restoration depend mainly on the distance to AP center rather than handover process. Figure 7-1 summarizes all mobility results inside RAN as stated in experiment 1. Table 7-1 compares the prototype mobility results inside carriers versus those published by Cisco for PMIP [35].

	PROTOTYPE		PMIP	
MOBILITY INSIDE CITY	MOBILITY SETUP DELAY	**~0.2s**	TOTAL BEARER SETUP (TBS)	**~0.5s**
	INTRA-OVERLAY HANDOVER	**~0.1s**	S-GW HANDOVER	**~0.25s**
CROSS CITIES	INTER-OVERLAY HANDOVER	**~0.15s**	NO P-GWS HANDOVER ⇘TBS	**~0.5s**
FORWARDING	OPENFLOW	**Wire Speed**	TUNNELS OVERHEADS	**~2-10%**

Table 7-1: Prototype Performance versus PMIP

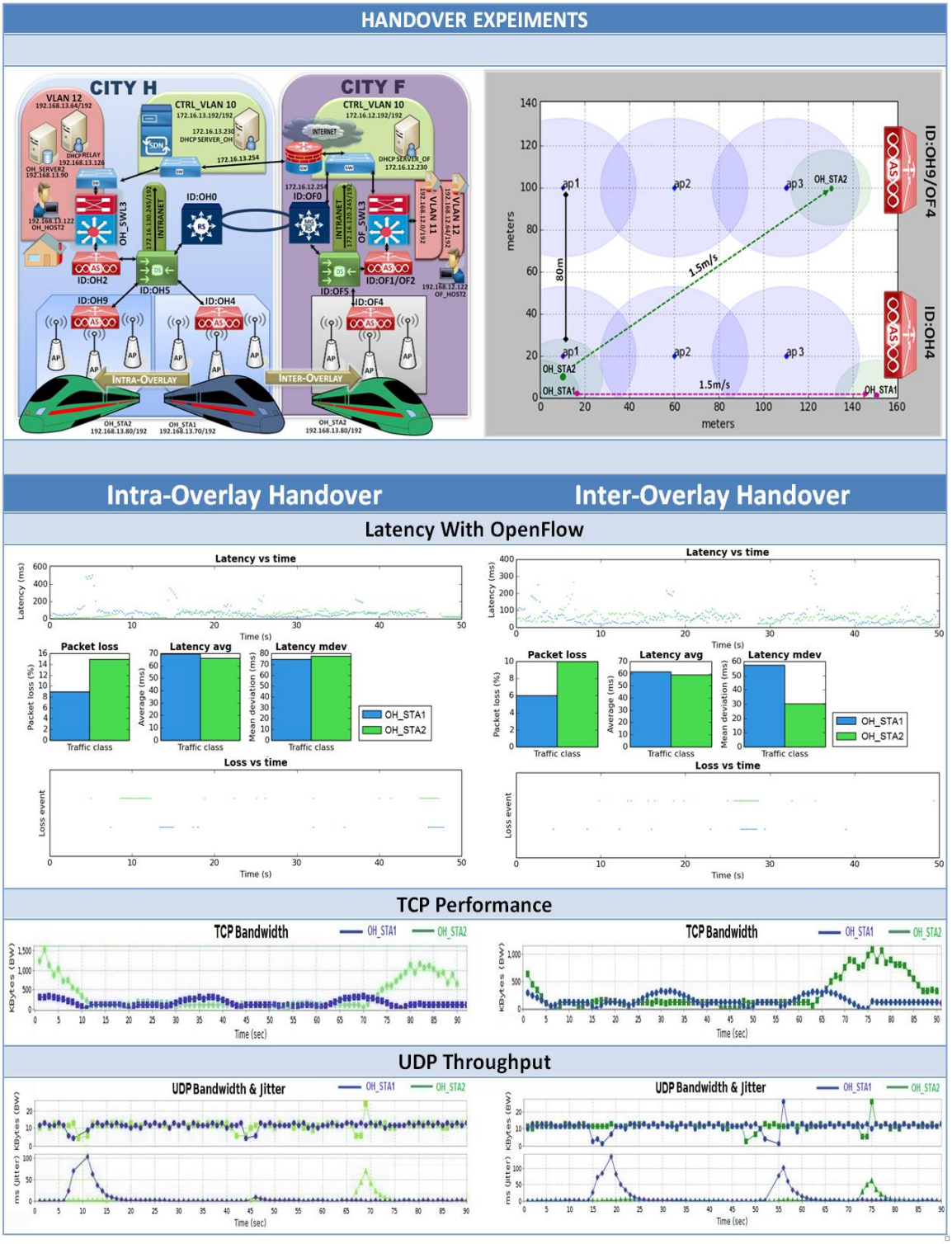


Figure 7-1: Summary of RAN Mobility

7.2.2 MOBILITY INSIDE AND CROSS CARRIERS

The objectives from these experiments are highlighting major delays affecting virtual path establishment inside and cross carriers with direct and indirect mobility service level agreements in addition to comparing ICMP, TCP, and UDP performance versus that of standard network acting as a lower bound metric. The calculation in table 3-2 as well as Cisco PMIP published benchmarks in table 6-14 shows that standard network performance is at least ~2-10% better than any mobility standard adopting MPLS label or VLAN TAG or Tunnel overheads.

Inter-overlay mobility inside carriers is almost wire speed with zero latency. This is clear improvement over standard network or existing mobility protocols as of tunnels' overheads elimination and OpenFlow hardware abstraction. Existing mobility solutions inside carriers suffers at least from one tunnel for bearer setup per mobility user. This decreases the overall performance. With direct mobility agreement cross two carriers, TCP throughput becomes slightly better than standard network after installation of OpenFlow rules. On the other hand, ICMP and UDP throughputs and jitter levels become equivalent to that of standard network. Thus. direct inter-domain mobility's performance that requires a single shared tunnel cross two carriers is still much better than existing mobility protocols that requires at least three separate tunnels per mobility user as in PMIP domain chaining model.

The framework successfully extends indoor services cross two carriers with indirect mobility agreements through a transient carrier. This is currently impossible in existing mobility standards. UDP throughput and jitter levels in indirect inter-domain mobility is almost equivalent to that of standard L3 network while TCP and ICMP throughputs are still lower as of the latency imposed by two tunnels establishments. Indirect inter-domain mobility's performance can be easily restored by adopting advance OpenFlow QoS techniques to guarantee effective bandwidth utilization in two tunnels virtual path cross carriers. Figures 7-2 summarizes all performance measures in inter-overlay, direct inter-domain, and indirect inter-domain mobility of experiments 2, 3, and 4 respectively. Table 7-2 summarizes the delays facing mobility virtual path setup and service reactivation of mobile users with both static and dynamic IP allocation mechanisms in inter-overlay, direct inter-domain, and indirect inter-domain mobility as shown in experiments 2, 3, and 4 respectively.

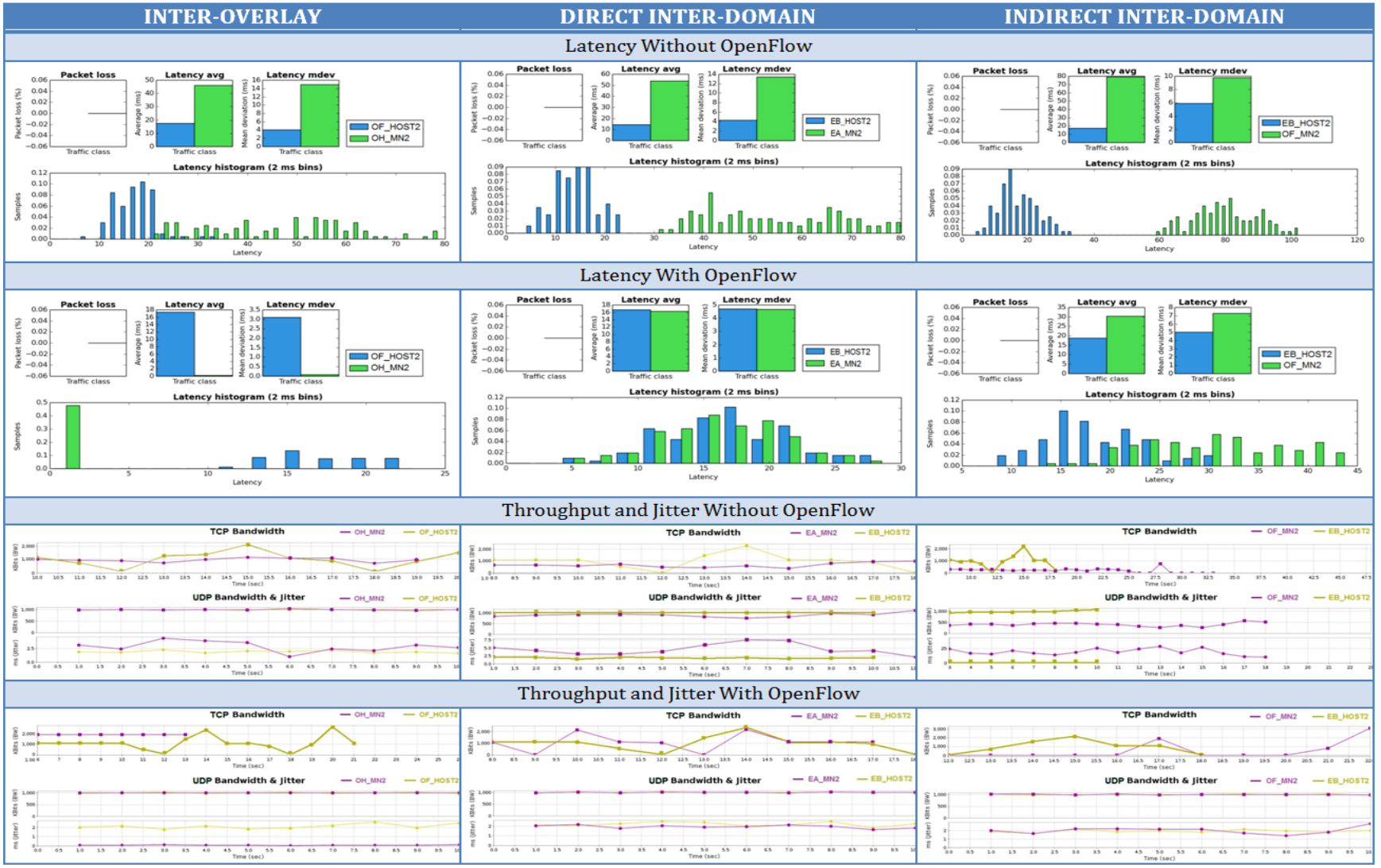


Figure 7-2: Summary of Inter-overlay, Direct Inter-domain, & Indirect Inter-domain Mobility

Table 7-2: Mobility Setup and Reactivation Delay Summary

		Inter-Overlay	Direct Inter-Domain			Indirect Inter-Domain		
STATIC	Forward Path	~0.1s	Tunnel	Inactive	~2.06s	Tunnel	Inactive	~4.04s
				Active	~0.1s		Active	~0.15s
	Backward Path	Wire			~0.04s			~0.08s
	Mobility Setup Delay	~0.1s	Tunnel	Inactive	~2.1s	Tunnel	Inactive	~4.12s
				Active	~0.14s		Active	~0.23s
DHCP	Forward Path	~0.14s	Tunnel	Inactive	~2.08s	Tunnel	Inactive	~4.08s
				Active	~0.18s		Active	~0.28s
	Backward Path	~0.1s			~0.14s			~0.2
	Mobility Setup Delay	~0.24s	Tunnel	Inactive	~2.22s	Tunnel	Inactive	~4.28s
				Active	~0.32s		Active	~0.48s
STATIC DHCP	Mobility Re-Activation Delay	~0.06s	~0.1s			~0.13s		

Table 7-3: Performance of Mobility Overlay versus Standard Network

		Inter-Overlay	Direct Inter-Domain	Indirect Inter-Domain
Latency		Wire Speed ~1.5ms vs. ~17ms	Equivalent	~30ms vs. ~17ms
Throughput	TCP	Major Improvement	Minor Improvement	~18% Degradation
	UDP	Equivalent	Equivalent	Equivalent
Jitter		Wire Speed ~0ms vs. ~2ms	Equivalent	Equivalent

7.3 HIGHLIGHTING MOBILITY FRAMEWORK CONTRIBUTIONS

This research proposes a novel framework for supporting moving to moving objects in addition to standard moving to static concept with seamless expansion cross carriers under SLAs. The following highlights the major contributions of the proposed SDN mobility frameworks.

7.3.1 STRUCTURE FLEXIBILITY

The framework is presented by three tiers of OpenFlow switches in fully distributed tree structure. The frameworks is scalable to accommodate carrier grade deployments where each tier is represented by a set of multiple load-balanced OpenFlow switches or the three tiers functions are implemented in a single OpenFlow switch for small deployments. In fully migrated SDN network; no hardware is required as of offering mobility inform of a service provided by the SDN application layer. The structure flexibility facilitates seamless integration to existing switched/routed network, 4G LTE infrastructure, and vCPE NFV technology in NGN.

7.3.2 EFFICIENT DATA FORWARDING PLANE

Established OpenFlow virtual paths are well designed to support effective traffic offload mechanisms that ensure efficient data forwarding plane while avoiding the core network congestion problem existing in LTE and the inefficient bandwidth utilization in inter-domain mobility. The following are summary of core principles behind such achievement that dramatically affect NGN scalability and quality of services offered.

7.3.2.1 NEW FORWARDING MECHANISM

The adopted forwarding mechanism inside the mobility overlay uses the indices of the proposed UEMS_ID to search for next hop MOBILITY_ID. This completely differs from existing routing mechanisms that search for next hop IP address toward destination subnet. The processing delay occurs during virtual path establishment only while latter packets follow the same path after installation of OpenFlow rules to ensure wire speed forwarding.

7.3.2.2 SEAMLESS HANDOVER MECHANISM

Seamless handover is ensured even in wide area motion with minimum latency as of transforming handover from bearer setup/release to a profile update process and simplifying L4 TCP sessions continuity problem to L2 forwarding of MN's packets.

7.3.2.3 TRAFFIC OFFLOADING MECHANISMS

The framework adopts an effective offload mechanism as of its scalable three tiers overlay distributed architecture. The flexibility in the overlay structure is emphasizes in the capability of having multiple breaks out and the usage of at least three IP addresses for fast services accessibility. Figure 4-5 shows that core network is traversed only for LIPA mobility and for continuity of active TCP sessions while the rest of packets are offloaded through the nearest PDN. Even V2V communications can be offloaded through AS without passing by parent DS.

7.3.3 ELIMINATING SIGNALING OVERHEADS AND RESTRICTING TUNNEL HEADERS

Unlike previous protocols, mobility activation occurs in-line during IP address allocation from home DHCP server without mobility signaling overhead. Moreover, no tunnel/MPLS/VLAN header is required for isolating user's packets as OpenFlow virtual paths isolate traffic based on IP and L2 addresses. Experiments results confirm the agility of OpenFlow SDN-based technology and reveal performance improvement over standard network as of hardware abstraction. This emphasizes that the performance of the proposed SDN mobility framework is better than existing mobility standard as CAPWAP and PMIP. The former adopts VLAN TAG that is theoretically ~0.25% performance lower than standard network while GRE tunnel of PMIP is theoretically ~2% and experimentally ~10% performance lower as in shown in table 3-2 . In the proposed SDN mobility framework, tunnels are used for connecting MGs of different operators or connecting mobility entities that are WAN separated to hide L3 routing complexities. These tunnels are established without signaling overhead based on SLAs, pre-defined configurations, and security policies.

7.3.4 INTRA-DOMAIN MOBILITY

Successful deployment for real time services enforces end to end Quality QoS. Thus, existing infrastructure with COPE and BYOD policies cannot support real time service offering to various employees' devices as laptop, tablet, smart phone…etc. These limit existing WiFi role in enterprise to fast internet access. The proposed framework identifies mobility users with their UEMSI_ID. L2 hardware address and IMSI are extra options for enhanced security. With this scope, intra-domain WiFi mobility can identify infrastructure access policy based on UEMSI_ID with end to end QoS in the established virtual path regardless of the device used. This opens new market for indoor mobility services as integrating smart phones to internal PBX, light and access control …etc. Moreover, it extends existing markets of both WiFi and cable service providers in smart cities to enhance their offering for vCPE and LIPA mobility services. Users can roam freely in WiFi hotspots with complete accessibility to their private cloud services.

7.3.5 COLLABORATIVE INTERACTIONS

One of the top achievements in the proposed SDN mobility framework is real time collaborative interactions between moving/static users, servers, terminals for facilitating cogitative services and cloud robotic interaction with minimum delay and latency and extending mobility coverage to cross operators under mobility SLAs to satisfy IoT requirements that are hardly solvable with existing mobility protocols. Figure 7-3 shows how the mobility overlay can be dynamically established between home network, carrier with direct SLA, and those with indirect SLA to communicate moving vehicle, static user, and home services with highest optimality in the established virtual paths. This eliminates the need for centralized servers/gateways concept as of direct communication between moving vehicle and roaming MNs.

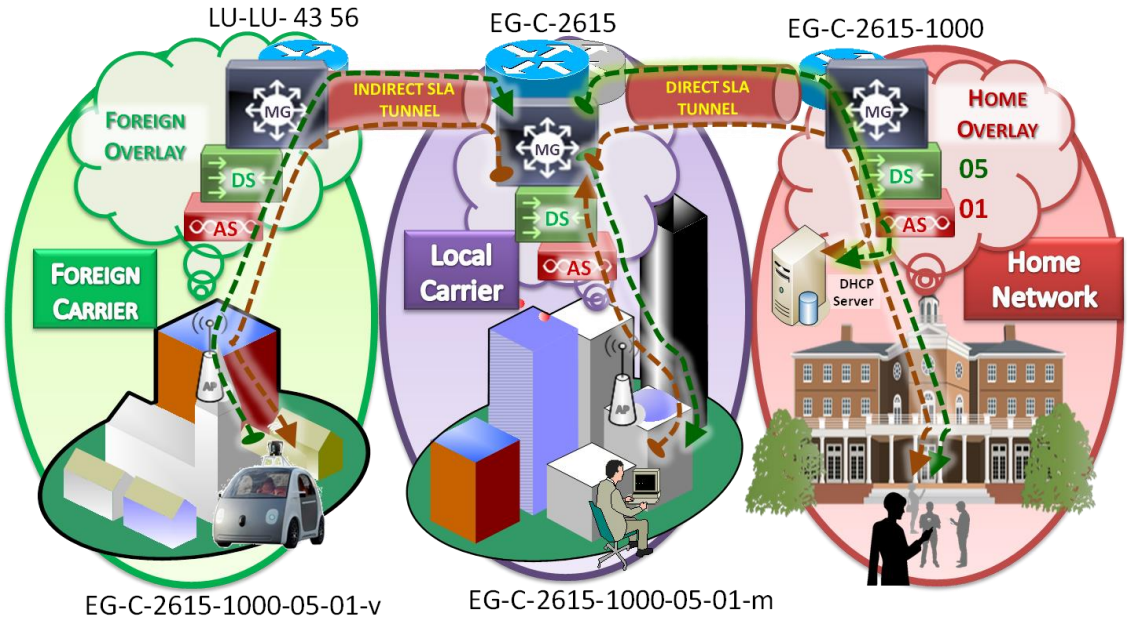


Figure 7-3: Collaborative Interactions

7.3.6 INTER-DOMAIN MOBILITY

When PMIP domain chaining model was developed, service provider aimed for seamless extension of residential/enterprise services through LTE and WiFi service provider. Unluckily inter-domain mobility suffers from tremendous delay as of several tunnels establishment. This enforces expensive solutions as DAS and small cell setups that violate customers' security in LTE and even failed in WiFi service providers [12][23][24]. More details are illustrated in section 1.3.2. The following highlights the framework's contributions toward this problem.

7.3.6.1 FULL INTER-DOMAIN MOBILITY INTERACTIONS

The adopted mobility concept is based on UEMSI_ID. Thus, only authorized MNs can use the virtual paths to ensure efficient utilization of scare bandwidth between networks with different administration. Moreover, this feature distinguishes mobility overlay over CAPWAP with single administration domain and over PMIP that requires at least three tunnels in domain chaining model. In the proposed framework, maximum one shared tunnel is required between two domains with direct SLAs to hide L3 routing complexities if no direct connection exists. Within an administrative domain, OpenFlow ensures wire speed forwarding inside the virtual path.

7.3.6.2 SECURITY POLICY COMPLIANCE

PMIP flat domain model enforces small cell setups in inter-domain mobility. These are almost remote controlled APs deployed at the customer premises which in turn violate customers' security policy. In the proposed framework, MGs' public MOBILITY_IDs are mapped to accessible public/private IP addresses and only UEMS_ID and HA address are exposed to other parties. No exposure of involved parties' internal structures as VLANs, private IP addresses, security policies …etc. This facilitates SLAs cross operators and open new market for residential/enterprise LIPA mobility with regained customers' trust.

7.4 FUTURE DIRECTIONS

The proposed framework has several contributions in NGN IoT mobility as stated in the previous sections. Still research work is endless and there is a lot of fields that can expand this research. The following highlights the main directions in future works.

- Integrating the proposed framework to IEEE 802 OmniRAN to ensure compatibility with heterogeneous access networks.
- Evaluating the feasibility of the proposed framework in load balancing, session continuity, and offload mechanism when multiple MN's cards are active.
- Evaluating cross controllers' negotiation for advance value added service offering to MNs roaming at visited networks.
- Integrating the framework to LTE Proximity Services and evaluating performance against IEEE 802.11p V2X communication.
- Adopting QoS to enhance direct and indirect inter-domain mobility performance.

7.5 PUBLICATION LIST

- "Inter-Domain Mobility Management using SDN for Residential/Enterprise Real Time Services," in proceeding of 4th IEEE Future Internet of Things and Cloud Workshops (wFiCloud), August 2016, Vienna, Austria, DOI 10.1109/W-FiCloud.2016.25.
- "Toward Hyper Interconnected IoT World using SDN Overlay Network for NGN Seamless Mobility", Ph.D consortium, in proceeding of 8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Luxembourg, December 2016, DOI: 10.1109/CloudCom.2016.0078.
- "SRMIP: A Software-Defined RAN Mobile IP Framework for Real Time Applications in Wide Area Motion," Int. J. of Mobile Computing and Multimedia Communications (IJMCMC) –IGIP, 7(4):28-49, A3, Oct. 2016, DOI: 10.4018/IJMCMC.2016100103.

REFERENCES

[1] A. Manzalini, C. Lin I, J. Huang, C. Buyukkoc, M. Bursell, P. Chemouil, ... S. Sharrock, "Towards 5G Software-Defined Ecosystems Technical Challenges, Business Sustainability and Policy Issues," IEEE SDN White Paper, July 2016, [Online]. Available: http://sdn.ieee.org/publications .

[2] R. E. Hattachi, J. Erfanian, B. Daly, A. Annunziato, K. Holley, C. Chen, ... L. Ibbetson, "5G White Paper - Executive Version by NGMN Alliance," NGMN Board, V 1.0, December 2014.

[3] Korhonen, "5G Vision –The 5G Infrastructure Public Private Partnership: The Next Generation of Communication Networks and Services," whitepaper, European Commission, 5G-PPP, February 2015.

[4] ONF White Paper, "Software-Defined Networking: The New Norm for Networks," Open Networking Foundation, April 13, 2012.

[5] C. Kolias –Ed., S. Ahlawat, C. Ashton, M. Cohn, S. Manning, and S. Nathan, "ONF Solution Brief: OpenFlow™-Enabled Mobile and Wireless Networks," Open Networking Foundation, September 2013.

[6] P. Srisuresh, M. Holdrege –Lucent Technologies, "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, August 1999.

[7] C. Perkins –Ed., Nokia Research Center, "IP Mobility Support for IPv4," RFC 3344, August 2002.

[8] S. Gundavelli –Ed., K. Leung - Cisco Systems, V. Devarapalli –Wichorus, K. Chowdhury –Starent Networks, and B. Patil –Nokia, "Proxy Mobile IPv6," IETF RFC 5213, August 2008.

[9] R. Wakikawa – Toyota ITC and S. Gundavelli –Cisco, "IPv4 Support for Proxy Mobile IPv4," ISSN: 2070-1721, IETF RFC 5844, May 2010.

[10] P. Calhoun –Cisco Systems, M. Montemurro –Research In Motion, and D. Stanley –Aruba Networks, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification," IETF proposed standard, RFC 5415, March 2009.

[11] P. Calhoun –Cisco Systems, M. Montemurro –Research In Motion, and D. Stanley –Aruba Networks, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," IETF proposed standard RFC 5416, March 2009.

[12] R. Gupta and N. Rastogi, "LTE ADVANCED – LIPA AND SIPTO," Aricent, 2012.

[13] Cisco 8500 Series Wireless Controller Deployment Guide, Document ID: 113695, Jun 2015.

[14] IDG Enterprise, "Tech Insights: Building the Mobile Enterprise Survey," September 2015. IDG Enterprise, Retrieved May 30, 2016, [Online]. Available: http://www.idgenterprise.com/resource/research/2015-idg-enterprise-building-the-mobile-enterprise-survey/

[15] J. Korhonen, Ed. –Nokia Siemens Network, J. Bournelle –Orange Labs, K. Chowdhury –Cisco Systems, A. Muhanna –Ericsson, and U. Meyer –RWTH Aachen "Diameter Proxy Mobile IPv6: Mobile Access

Gateway and Local Mobility Anchor Interaction with Diameter Server," RFC 5779, proposed standard, February 2010.

[16] NMC, "LTE IP Address Allocation Schemes I: Basic," Netmanias Technical Document, February 2015.

[17] ETSI, Small Cell LTE Plugfest, -Annual Report, July 2016. Retrieved August 2016, [Online]. Available: http://www.etsi.org/about/10-news-events/events/1061-small-cell-lte-plugfest-2016

[18] H. Wang, S. Chen, H. Xu, M. Ai, and Y. Shi "SoftNet: A Software Defined Decentralized Mobile Network Architecture Toward 5G," IEEE Network 2(2):16-22, March/April 2015.

[19] 3GPP TS 29.061 V9.3.0, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (Release 9), June 2010.

[20] G. Hampel –Qualcomm, A. Rana, and T. Klein –Bell Labs, Alcatel-Lucent, "Seamless TCP mobility using lightweight MPTCP Proxy," MobiWac '13, Pages 139-146, 2013.

[21] Cisco, "PMIP: Multipath Support on MAG and LMA", IP Mobility: Mobile IP Configuration Guide, Cisco IOS XE, updated April 2016, retrieved June 2016. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob_pmipv6/configuration/xe-16/mob-pmipv6-xe-16-book/imo-pmipv6-multipath-support.html .

[22] NMC, "LTE IP Address Allocation Schemes II: A Case for Two Cities," Netmanias Technical Document, February 2015.

[23] D. Linegar, "Service Provider WiFi and Small Cell," Cisco Systems Technical presentation, April 2014, retrieved June 2016, [Online]. Available: http://www.cisco.com/c/dam/global/en_ca/assets/ciscoconnect/2014/pdfs /service_provider_wifi_derek_linegar.pdf

[24] S. Gundavelli, B. Pularikkal, and R. Koodli –Cisco, "Applicability of Proxy Mobile IPv6 for Service Provider Wi-Fi Deployments," Internet-Draft, released October 2013 expired April 2013.

[25] A. Kwoczek, B. Rech, T. Hehn, T. Buburuzan, R. Alieiev, M. Abdulhussein, … D. Trossen, "5G Automotive Vision," ERTICO, European Commission, 5G PPP, October 2015.

[26] F. Hu, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations", CRC Press, 2016, pp.281.

[27] V. Mann, A. Vishnoi, K. Kannan and S. Kalyanaraman –IBM Research –India, "CrossRoads: Seamless VM Mobility Across Data Centers through Software Defined Networking," IEEE Network Operations and Management Symposium (NOMS), 2012.

[28] L. Riazuelo, M. Tenorth, D. D. Marco, M. Salas, D. Gálvez-López, L. Mösenlechner, ..., J. M. M. Montiel, "RoboEarth Semantic Mapping: A cloud enabled knowledge-based approach," IEEE Trans. Autom. Sci. Eng., 12(2):432-443, Apr. 2015.

[29] Science News, "Robot Learns To Smile And Frown," University of California –San Diego, July 2009. Retrieved 30 July 2016. [Online]. Available: https://www.sciencedaily.com/releases/2009/07/090708181206.htm

[30] C. Gabriel, Small Cells Inside the Enterprise –"The Who, What & Where." Maravedis - Rethink, SpiderCloud Wireless, June 2013.

[31] P. Congdon –Tallac Networks and C. Perkins –Huawei, "Wireless & Mobile – OpenFlow. Wireless & Mobile Working Group (WMWG) Charter Application," Open Networking Foundation, 2015.

[32] A. Nygren, B. Pfa, B. Lantz, B. Heller, C. Barker, C. Beckmann, … Z. L. Kis, "The OpenFlow Switch Specification," Version 1.4.0, ONF, Wire Protocol 0x05, ONF TS-01, October 2013.

[33] M. Betts, N. Davis, R. Dolin, P. Doolan, S. Fratini, D. Hood, … Z. Dacheng, "SDN Architecture," Issue 1, Open Networking Foundation, ONF TR-502, June 2014.

[34] S. Denazis, O. Koufopavlou, E. Haleplidis, Ed. –University of Patras, K. Pentikousis, Ed. –EICT, J. Hadi Salim –Mojatatu Networks, and D. Meyer –Brocade, "Software-Defined Networking (SDN): Layers and Architecture Terminology," RFC 7426, January 2015.

[35] Z. Savic, "LTE Design and Deployment Strategies," Technical Presentation, Cisco Systems, pp.30,61, 2011, retrieved June 2016, [Online]. Available: http://www.cisco.com/c/dam/global/en_ae/assets/expo2011/saudiarabia/pdfs/lte-design-and-deployment-strategies-zeljko-savic.pdf

[36] I. Al-Surmi, M. Othman, and B. M. Ali, "Review on Mobility Management for Future IP-based Next Generation Wireless Networks," International Conference on Advanced Communication Technology, ICACT 2010, Korea, February 2010; pp.89–94.

[37] A. Weyland, "Evaluation of Mobile IP implementations under Linux," Computer and Distributed Systems Group Project, IAM, University of Berne, December 2002, retrieved July 2016, [Online]. Available: http://rvs.unibe.ch/publications/projekt_attila_weyland.pdf

[38] B. Esmat, M. N. Mikhail, and A. El-Kadi –American University in Cairo, "Enhanced Mobile IP Protocol," Proceedings of Mobile and Wireless Communication Networks, IFIP-TC6/European, Commission NETWORKING 2000 International Workshop, MWCN 2000, Lecture Volume 1818/2000, pp.158-173, May 2000.

[39] M. N. Mikhail, B. Esmat, and A. El-kadi, "A New Architecture for Mobile Computing," Proceedings vol IV, Mobile and Wireless Computing, SCI 2001, Orlando, Florida, July 2001.

[40] D. Johnson –Rice University, C. Perkins –Nokia Research Center, and J. Arkko –Ericsson, "Mobility Support in IPv6," RFC 3775, June 2004.

[41] R. Koodli, Ed. –Starent Networks, "Mobile IPv6 Fast Handovers," RFC 5568, July 2009.

[42] T. Schmidt, Ed. – HAW Hamburg, M. Waehlisch –Link-Lab & FU Berlin, R. Koodli –Intel, G. Fairhurst – University of Aberdeen, D. Liu –China Mobile, "Multicast Listener Extensions for Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6) Fast Handovers," IETF RFC 7411, November 2014.

[43] H. Soliman –Flarion, C. Castelluccia –INRIA, K. El Malki –Ericsson, L. Bellier –INRIA, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," RFC 4140, August 2005.

[44] P. Seite –Orange, A. Yegin –Samsung, S. Gundavelli –Cisco, "MAG Multipath Binding Option", Internet-Draft March 2016.

[45] Alcatel-Lucent, "The LTE Network Architecture - A Comprehensive Tutorial," Strategic White Paper, 2009.

[46] Ruckus Wireless, "The Choice of Mobility Solutions Enabling IP-Session Continuity Between Heterogeneous Radio Access Networks," Interworking Wi-Fi and Mobile Networks White Paper, 2013.

[47] S. Bailey, D. Bansal, L. Dunbar, D. Hood, Z. L. Kis, B. Mack-Crane, J. Maguire, D. Malek, D. Meyer, M. Paul, S. Schaller, F. Schneider, R. Sherwood, J. Tonsing, T. Tsou, and E. Varma, "SDN Architecture Overview," Open Networking Foundation, Version 1.0 –draft v08, December 2013.

[48] C. Zhang -Huawei, S. Addepalli, N. Murthy –Freescale, L. Fourie –GS, M. Zarny, and L. Dunbar Huawei, "L4-L7 Service Function Chaining Solution Architecture," Open Networking Foundation, ONF TS-027, June 2015.

[49] K. K. Yap, M. Kobayashi, R. Sherwood, T. Y. Huang, M. Chan, N. Handigol, and N. McKeown, "OpenRoads: Empowering Research in Mobile Networks," SIGCOMM 2010, Rev. 40(1):125-126.

[50] K. K. Yap, R. Sherwood, M. Kobayashi, T. Y. Huang, M. Chan, N. Handigol, N. McKeown, and G. Parulkar, "Blueprint for Introducing Innovation into Wireless Mobile Networks," Proceedings of 2nd ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures, 2010, pp.25-32.

[51] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, "Towards Programmable Enterprise WLANS with Odin," Proceedings of the First Workshop on Hot Topics in Software Defined Networks, ser. HotSDN 2012, pp.115-120.

[52] M. Bansal, J. Mehlman, S. Katti, and P. Levis, "OpenRadio: A Programmable Wireless Dataplane", Proceedings of the First Workshop on Hot topics in Software Defined Networks, HotSDN 2012, pp. 109-114.

[53] S. Kumar, D. Cifuentes, S. Gollakota, and D. Katabi, “Bringing Cross-Layer MIMO to Today’s Wireless LANs,” SIGCOMM 2013, Rev. 43(4):387-398.

[54] A. Gudipati, D. Perry, L. Erran Li, and S. Katti, “SoftRAN: Software Defined Radio Access Network,” Proceedings of Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, HotSDN, 2013, pp.25-30.

[55] M. Yang, Y. Li, D. Jin, L. Su, S. Ma, and L. Zeng, “OpenRAN: A Software-Defined RAN Architecture via Virtualization,” SIGCOMM Comput. Commun, 2013, Rev. 43(4): 549-550.

[56] Anyfi, “Software-Defined Wireless Networking: Concepts, Principles and Motivations,” Whitepaper, Anyfi Networks, 2014.

[57] L. Erran Li –Bell Labs, Z. M. Mao –University of Michigan, J. Rexford –Princeton University, “Toward Software-Defined Cellular Networks,” European Workshop on Software Defined Networking (EWSDN), Berlin, Germany, 2012, pp.7-12.

[58] X. Jiny, L. Erran Li, L. Vanbevery, and J. Rexfordy –Princeton University, Bell Labs, “SoftCell: Scalable and Flexible Cellular Core Network Architecture,” Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT), New York, USA, 2013, pp.163-174.

[59] M. Peng, Y. Li, Z. Zhao, and C. Wang, “System Architecture and Key Technologies for 5G Heterogeneous Cloud Radio Access Networks,” IEEE Network, 29(2):6-14, ISSN: 0890-8044, April 2015.

[60] K. Phemius, M.Bouet, and J. Leguay –Thales Communications & Security, “DISCO: Distributed Multi-Domain SDN Controllers,” In IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, May 2014, pp. 1-4.

[61] K. Tantayakul, R. Dhaou, and B. Paillassa, "Impact of SDN on Mobility Management," IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), March 2016, pp.260-265, DOI: 10.1109/AINA.2016.57.

[62] X. Kong, Z. Wang, X. Shi, X. Yin, and Dan Li, “Performance evaluation of software-defined networking with real-life ISP traffic,” IEEE Symposium on Computers and Communications (ISCC), 2013, pp.541-547, DOI: 10.1109/ISCC.2013.6755002.

[63] W. Miao, G. Min, Y. Wu, H. Wang, and J. Hu., "Performance Modelling and Analysis of Software-Defined Networking under Bursty Multimedia Traffic," ACM Trans. Multimedia Comput. Commun. Appl. 12(5s): 77, December 2016, DOI 10.1145/2983637.

[64] L. M. Contreras –Telefónica, L. Cominardi –IMDEA Networks Institute, H. Qian –Grabtalk Ltd., and C. J. Bernardos –Universidad Carlos, “Software-Defined Mobility Management: Architecture Proposal and

Future Directions," Mobile Netw Appl, Springer, 21(2): 226-236, April 2016, DOI:10.1007/s11036-015-0663-7.

[65] Y. Wang, J. Bi, and K. Zhang, "Design and Implementation of a Software-Defined Mobility Architecture for IP Networks," Mobile Netw Appl, Springer, 20(1):40–52, February 2015, DOI 10.1007/s11036-015-0579-2.

[66] L. M. Contreras, L. Cominardi, H. Qian and C. J. Bernardos, "Software-Defined Mobility Management: Architecture Proposal and Future Directions," Mobile Netw Appl 21:226–236, 2016, DOI 10.1007/s11036-015-0663-7.

[67] S. Alexander –Silicon Graphics and R. Droms –Bucknell University, "Dynamic Host Configuration Protocol," RFC 2131, March 1997.

[68] S. Alexander –Silicon Graphics, Inc., R. Droms –Bucknell University, "DHCP Options and BOOTP Vendor Extensions," RFC 2132, March 1997.

[69] D. Meyer and P. Lothberg –Sprint, "GLOP Addressing in 233/8," RFC 3180, September 2001.

[70] Y. Rekhter –Cisco Systems, B. Moskowitz –Chrysler Corp., E. Lear D. –Silicon Graphics, and Karrenberg and G. J. de Groot –RIPE NCC, "Address Allocation for Private Internets," RFC 1918, February 1996.

[71] Mahalingam –Storvisor, D. Dutt –Cumulus Networks, K. Duda –Arista, P. Agarwal –Broadcom, L. Kreeger –Cisco, T. Sridhar –Vmware, M. Bursell –Intel, and C. Wright –Red Hat, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," RFC 7348, ISSN: 2070-1721, August 2014.

[72] ISO, "Country Codes - ISO 3166," International Organization for Standardization (ISO), retrieved 13 August 2016, [Online]. Available: http://www.iso.org/iso/country_codes .

[73] IANA, "Qualifying top-level domain strings: Eligible categories of top-level domains," Internet Assigned Numbers Authority (IANA), retrieved August 2016, [Online]. Available: https://www.iana.org/help/eligible-tlds.

[74] B. Aboba –Microsoft Corporation, and J. Vollbrecht –Merit Networks, "Proxy Chaining and Policy Implementation in Roaming," RFC 2607, June 1999.

[75] G. Zorn, Ed. –Network Zen, "Diameter Network Access Server Application," IETF RFC 7155, April 2014.

[76] H. Haverinen, Ed. –Nokia and J. Salowey, Ed. Cisco Systems, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)," RFC 4186, January 2006.

[77] J. Arkko, V. Lehtovirta –Ericsson, and P. Eronen –Nokia, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 5448, May 2009.

[78] IEEE Standard for Local and metropolitan area networks, "Virtual Bridged Local Area Networks (VLAN)," LAN/MAN Standards Committee, IEEE Std 802.1Q™-2005.

[79] M. P. Odini –Ed., A. Sahai, A. Veitch, A. Gamela, A. Khan, B. Perlman, … Z. Lei. "Network Functions Virtualization (NFV); Ecosystem"; Report on SDN Usage in NFV Architectural Framework, ETSI GS NFV-EVE 005 V1.1.1. pp. 95-98, December 2015, retrieved June 2016, [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_nfv-eve005v010101p.pdf

[80] IEEE Std 802.1D™- 2004, (Revision of IEEE Std 802.1D-1998), 802.1DTM, IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Bridges, IEEE Computer Society, sponsored by LAN/MAN Standards Committee, 9 June 2004, PDF: SS95213.

[81] C. Rigney, S. Willens –Livingston, A. Rubens –Merit, W. Simpson –Daydreamer, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.

[82] J. Vollbrecht, "The Beginnings and History of RADIUS," Interlink Networks, 2006, retrieved June 2016, [Online]. Available: https://www.interlinknetworks.com/app_notes/History%20of%20RADIUS. pdf

[83] J. Arkko –Ericsson and C. Pignataro –Cisco Systems, "IANA Allocation Guidelines for the Address Resolution Protocol (ARP)," proposed standard, RFC 5494, April 2009.

[84] J. Postel -ISI, "Internet Control Message Protocol," DARPA internet program, protocol specifications: 2070-1721, internet standard, RFC 792, September 1981.

[85] F. Gont –UTN-FRH/SI6 Networks and C. Pignataro –Cisco Systems, "Formally Deprecating Some ICMPv4 Message Types," proposed standard, IETF RFC 6918, April 2013.

[86] D. Farinacci, T. Li –Procket Networks, S. Hanks –Enron Communications, D. Meyer –Cisco Systems, and P. Traina –Juniper Networks, "Generic Routing Encapsulation (GRE)," proposed standard, RFC 2784, March 2000.

[87] G. Dommety - Cisco Systems, "Key and Sequence Number Extensions to GRE," proposed standard, RFC 2890, September 2000.

[88] E. Rescorla –RTFM, "Diffie-Hellman Key Agreement Method," RFC 2631, June 1999

[89] J. Jonsson and B. Kaliski, RSA Laboratories, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography," RFC 3447, February 2003.

[90] G. Zorn –Cisco Systems, D. Leifer, A. Rubens –Ascend Communications, J. Shriver –Intel Corporation, M. Holdrege –IpVerse, I. Goyret –Lucent Technologies, "RADIUS Attributes for Tunnel Protocol Support," RFC 2868, June 2000.

ABBREVIATIONS

3GPP/3GPP2	3rd Generation Partnership Project
5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Accounting, and Authorization
AI	Artificial Intelligence
AM	Autonomous Machines
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
API	Application Program Interface
APN	Access Point Name
ARP	Address Resolution Protocol
ARPU	Average Revenue Per User
AS	Access Switch
AUC	Authentication center
AVP	Attribute-Value Pairs
BSC	Base Station Controllers
BSS	Business Support Systems
BBU	Base Band Units
BYOD	Bring Your Own Device
CAPWAP	Control and Provisioning of Wireless Access Points
CDPI	Control to Data-Plane Interface
CHADDR	Client's Hardware Address
CoA	Care of Address
COPE	Corporate Owned, Personally Enabled
DAS	Distributed Antenna System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DS	Detector Switch
DSRC	Dedicated Short-Range Communications
DTLS	Datagram Transport Layer Security
e-NB	e-nodeB
ECM	Entitlement Management Message
EMM	Entitlement Control Message
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
ePDG	Evolved Packet Gateway
EPS	Evolved Packet System
GPRS	General Packet Radio Service
GGSN	Gateway GPRS Support Node
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
HA	Home Address
HSS	Home Subscriber Server
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ITS	Intelligent Transportation Systems
IWLAN	Industrial Wireless LAN
LIPA	Local IP Access
LMA	Local Mobility Anchor
LWAPP	Lightweight Access Point Protocol
LTE	Long Term Evolution
MAG	Mobile Access Gateways
MaaS	Mobility-as-a-Service
MAC	Media Access Control
MG	Mobility Gateway
MIP	Mobile IP
MME	Mobility Management Entity
MN	Mobile Nodes
MPTCP	MultiPath TCP
MVNO	Mobile Virtual Network Operators
NAC	Network Access Control
NAS	Non-Access Stratum
NAT	Network Address Translation
NBI	North Bound Interface
NE	Network Elements
NFV	Network Function Virtualization
NGN	Next Generation Network
NOC	Network Operation Center
NSAPI	Network Layer Service Access Point Identifier

ONF	Open Networking Foundation
OPEX	Operational Expenditure
OSS	Operations Support Systems
P-GW	PDN Gateway
PCRF	Policy Control and Charging Rules Function
PDN	Packet Data Network
PMIP	Proxy Mobile IP
ProSe	Proximity Services
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RFC	Request for Comments
RS	Relay Switch
RRU	Remote Radio Units
S-GW	Serving Gateway
SA	SDN Address
SAE	System Architecture Evolution
SDN	Software Defined Network
SDWN	Software Defined Wireless Network
SBI	South Bound Interface
SIPTO	Selected Internet IP Traffic Offload
SLA	Service Level Agreements
SMB	Small and Medium-sized Business
SGSN	Serving GPRS Support Node
UAV	Unmanned Aerial Vehicles
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
V2N	Vehicle to Internet
V2P	Vehicle to Pedestrian
V2X	Vehicle to Everything
VAS	Value Added Service
VLAN	Virtual Local Area Network
VM	Virtual Machine
WAG	Wireless Access Gateway
WAVE	Wireless Access in Vehicular Environments
WCDMA	Wideband Code Division Multiple Access
WLC	Wireless LAN Controllers
WMWG	Wireless & Mobile Working Group
WWW	World Wide Web