DESEMPEÑO DE UNA SDWLAN IPV4/IPV6 EMPRESARIAL, A PARTIR DE LAS NECESIDADES OPERATIVAS DEL ADMINISTRADOR DE RED

Cristian Felipe Solarte Orozco

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Programa de Maestría en Telecomunicaciones
Grupo de I+D GNTT
Popayán, 2023

DESEMPEÑO DE UNA SDWLAN IPv4/IPv6 EMPRESARIAL, A PARTIR DE LAS NECESIDADES OPERATIVAS DEL ADMINISTRADOR DE RED

Trabajo de Grado para optar al título de Magister en Telecomunicaciones

Cristian Felipe Solarte Orozco

Director: Ing. José Giovanny López Perafán Ph.D.

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Programa de Maestría en Telecomunicaciones
Grupo de I+D GNTT
Popayán, 2023

INTRODUCCIÓN 1
CAPÍTULO I: REVISIÓN DOCUMENTAL 3
1.1. Redes empresariales 3
1.1.1. Estructuración básica de una red empresarial 3
1.1.2. Deficiencias en la arquitectura de una red empresarial tradicional 4
1.2. Red Inalámbrica de Área Local, WLAN 5
1.2.1. Wi-Fi: IEEE 802.11x. Fundamento de las redes WLAN 5
1.2.1.1. Componentes de la arquitectura IEEE 802.11 7
1.3. Modelos de gestión de redes inalámbricas 9
1.3.1. Modelo de referencia ITU-T FCAPS 10
1.3.2. Modelo de referencia IETF RFC-6632 13
1.3.3. Protocolos de gestión de redes 14
1.4. Redes definidas por software, SDN 15
1.4.1. Capa de datos o Infraestructura 15
1.4.1.1. OpenFlow 16
1.4.2. Capa de control 16
1.4.2.1. Controladora *FloodLight* 17
1.4.2.2. Controladora *OpenDayLight* 18
1.4.2.3. Controladora ONOS 18
1.4.3. Capa de Aplicación 18
1.5. Métodos de análisis de desempeño de red 20
1.5.1. Métricas de desempeño 20
1.5.2. Metodologías de medición 21
1.6. Herramientas de emulación y análisis de tráfico en redes SDWLAN 22
1.6.1. Mininet-WiFi 23
1.6.1.1. Creación de topologías de red 23
1.6.1.2. Modelos de propagación y movilidad 24
1.6.2. Wireshark 26
1.7. Hardware comercial para SDWLAN 27
CAPÍTULO II: DISEÑO DE SDWLAN EMPRESARIAL 28
2.1. Diseño de red SDWLAN 29
2.2. Topología SDWLAN 30
2.3. Emulación 32
2.3.1. Controladora ONOS 32
2.3.2. Emulación con Mininet-WiFi 35
2.3.2.1. Escenario de pruebas para Mininet-WiFi 37
2.3.3. Emulación y escenario de pruebas con equipos reales 39

2.3.3.1. Infraestructura de red 40
2.3.3.2. Preaprovisionamiento de conmutador y puntos de acceso 41
2.3.3.3. Configuración básica de la controladora ONOS 42
2.4. Definición de pruebas para escenario emulado con Mininet-WiFi y equipos reales 49
CAPITULO III: EMULACIÓN DE SDWLAN Y PRUEBAS DE COMPORTAMIENTO DEL MODELO SDWLAN..... 51
3.1. Emulación sobre Mininet-WiFi 51
3.1.1. Comportamiento de la interfaz gráfica de ONOS durante el handover y la salida de un a STA de la red 54
3.1.2. Comportamiento del flujo de datos ante la caída de un enlace cableado y una interfaz inalámbrica..... 58
3.1.3. Almacenamiento de históricas de las STA..... 60
3.2. Emulación sobre equipos reales 60
3.2.1. Comportamiento de la interfaz gráfica de ONOS durante el handover 63
3.2.2. Comportamiento del flujo de datos ante la caída de un enlace cableado..... 65
3.2.3. Evaluación de ancho de banda y latencia al interior de la red y hacia internet 67
3.2.4. Pruebas de control de interfaz inalámbrica mediante el protocolo NETCONF en un punto de acceso..... 68
3.3. Resumen de resultados obtenidos en las pruebas con Mininet-WiFi y equipos reales..... 70
CAPÍTULO IV: CONCLUSIONES 73
BIBLIOGRAFÍA 76
ANEXO 1..... 78
ANEXO 2..... 80

LISTA DE FIGURAS

Figura 1: Modelo de red empresarial. 4
Figura 2: Estructura del estándar IEEE 802. Fuente: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture 6
Figura 3: Concepto de IBSS. 8
Figura 4: Concepto de Infraestructura BSS. 8
Figura 5: Concepto ESS. 9
Figura 6: Modelo FCAPS Vs Modelo TMN. Fuente: Fundamentals of EMS, NMS, and OSS/BSS. 12
Figura 7: Arquitectura de redes definidas por software. Fuente: Software Defined Networking: The New Norm for Networks. 15
Figura 8: Esquema de las aplicaciones proactivas. Fuente: Software Defined Networks. A Comprehensive Approach 19
Figura 9: Esquema de las aplicaciones reactivas. Fuente: Software Defined Networks. A Comprehensive Approach 20
Figura 10: Topologías de red para el monitoreo de redes. 26
Figura 11: Topología de red empresarial donde converge la red LAN y la WLAN. 28
Figura 12: Topología SDWLAN para el proyecto en curso. 31
Figura 13: Interfaz gráfica de ONOS. 33
Figura 14: Activación de aplicaciones southbound y northbound desde líneas de comando e interfaz gráfica. 34
Figura 15: Configuración de aplicaciones mediante REST API. 34
Figura 16: Topología de red generada en miniedit. 35
Figura 17: topología de red en lenguaje python. 36
Figura 18: Asignación de nombre y ubicación de los dispositivos de red para la interfaz gráfica de ONOS. 37
Figura 19: Topología de red corriendo desde Mininet-WiFi. 38
Figura 20: Topología de red para emulación con equipos reales. 40
Figura 21: versión de firmware OpenWrt disponible para los AP mikrotik. Fuente: https://openwrt.org/toh/start 41
Figura 22: SSID dispersados por los puntos de acceso inalámbricos. 42
Figura 23: Configuración de equipos OpenFlow. 42
Figura 24: Configuración de puertos. 43
Figura 25: Configuración del servidor en ONOS. 43
Figura 26: Configuración de aplicaciones ONOS. 44
Figura 27: Presentación de la configuración de la controladora ONOS con equipos reales. 44
Figura 28: Generación de intenciones de conexión entre STA_E, el servidor y la respectiva salida a internet con IPv4. 45
Figura 29: Ping del servidor hacia los DNS de Google. 46
Figura 30: Ping de STA_E hacia el DNS de Google, punto de simulación para salida a internet de IPv6 (2800:484:2383:16de::101) y el servidor. 46

Figura 31: Configuración del servidor NETCONF en uno de los dos AP. 47
Figura 32: Topología de red para pruebas de desempeño de red. 51
Figura 33: Configuración Mininet-WiFi para pruebas de desempeño de red. 52
Figura 34: Pruebas de latencia. 53
Figura 35: Pruebas de ancho de banda. 53
Figura 36: Estado inicial de la interfaz gráfica de la controladora ONOS. 55
Figura 37: Comportamiento de las STA durante el handover. 56
Figura 38: Registro de asociación de las estaciones de trabajo al conmutador y los AP. 57
Figura 39: Resultados para las pruebas de ancho de banda y latencia en las estaciones en movimiento. 57
Figura 40: Condición inicial de los enlaces entre el conmutador y los AP. 58
Figura 41: Flujo de datos sin el enlace entre los AP. 58
Figura 42: Comportamiento de la controladora a la caída de un enlace directo al servidor 59
Figura 43: Información de las STA presente en la controladora. 60
Figura 44: Flujo de las intenciones de comunicación. 61
Figura 45: Evidencias de flujos para cada STA inalámbrica asociada a la red SDWLAN. 62
Figura 46: Flujo de datos durante transición de AP. 63
Figura 47: Cambio de posición de las STA durante la transición de AP. 64
Figura 48: estado de conectividad de la STA asociada al SSID de empleados en un segundo cambio de AP. 64
Figura 49: estado de comunicación de las STA inalámbricas al momento de perder enlace entre OFAP! y OFAP2. 65
Figura 50: estado de comunicación de las STA inalámbricas al momento de perder enlace entre OFAP1, OFAP2 y OFSW1. 66
Figura 51: Evidencias de ancho de banda obtenido hacia Internet y el interior de la red medido por Iperf y www.speedtest.net. 67
Figura 52: Comparativa de parámetros de configuración inalámbrica en el dispositivo OFAP1 y la que se obtiene con NETCONF. 68
Figura 53:Confirmación de la aplicación de cambios en la configuración del AP.. 70

LISTA DE TABLAS

Tabla 1: Resumen comparativo enmiendas del estándar IEEE 802.11 7
Tabla 2: Caracterización de controladores SDN. Fuente: Propuesta metodológica para la selección de controladores de redes SDN a nivel empresarial 17
Tabla 3: Relación de métricas usadas en IETF y ITU-T. Fuente: ETSI EG 202 765-3 V1.1.2 20
Tabla 4: Comparativa de herramientas de medición activa. 22
Tabla 5:Direccionamiento IP para la red SDWLAN 32
Tabla 6: Aplicaciones de ONOS preinstaladas y habilitadas para la emulación del escenario SDWLAN. 33
Tabla 7: Características de los routers mikrotik. Fuente: https://mikrotik.com 41
Tabla 8: Asignación de nombres y direccionamiento IP de control. 41
Tabla 9: Resumen de pruebas a realizar para cada escenario de emulación. 50
Tabla 10: Direccionamiento IP para pruebas de desempeño de red. 52
Tabla 11: Resultados para las pruebas de latencia y ancho de banda. 54
Tabla 12: Resumen de resultados obtenidos en las pruebas adelantadas en el presente capítulo 72

LISTA DE ACRÓNIMOS

ACL	*Access Control List* (Lista de Control de Acceso)
ADSL	*Asimetric Digital Subscriber Line* (Línea de Abonado Digital Asimétrica)
ANE	Agencia Nacional del Espectro
AP	*Access Point* (Punto de Acceso)
API	*Application Programming Interface* (Interfaz de Programación de Aplicaciones)
ATM	*Asynchronous Transfer Mode* (Modo de Transferencia Asíncrono)
ARP	*Address Resolution Protocol* (Protocolo de Resolución de Direcciones)
BGP	*Border Gateway Protocol* (Protocolo de Puerta de Enlace de Borde)
BSS	*Basic Service Set* (Conjunto de Servicios Básicos Independientes)
CAPEX	*Capital Expenditure* (Gastos de Capital)
CAPWAP	*Control And Provisioning of Wireless Access Points* (Control y Aprovisionamiento de Puntos de Acceso Inalámbrico)
CLI	*Command Line Interface* (Interfaz de Línea de Comandos)
COPS	*Common Open Policy Service* (Protocolo de Servicio de Política Abierta Común)
DHCP	*Dynamic Host Configuration Protocol* (Protocolo de Configuración Dinámica de Anfitrión)
DNS	*Domain Name System* (Sistemas de Nombres de Dominio)
DS	*Distribution System* (Sistema de Distribución)
EMS	*Element Management System* (Sistema de Gestión de Elementos)
EN	*Element Network* (Elementos de Red)
EPL	*Eclipse Public License* (Licencia Pública de Eclipse)
ESS	*Extended Service Set* (Conjunto de Servicios Extendidos)
GMPLS	*Generalized MultiProtocol Label Switching* (Conmutación de Etiquetas Multiprotocolo Generalizada)
GUI	*Graphical User Interface* (Interfaz Gráfica de Usuario)
IBSS	*Independent Basic Service Set* (Conjunto de Servicios Básicos Independientes)

ICMP	*Internet Control Message Protocol* (Protocolo de Control de Mensajes de Internet)
IEEE	*Institute of Electrical and Electronics Engineers* (Instituto de Ingeniería Eléctrica y Electrónica)
IETF	*Internet Engineering Task Force* (Grupo de Trabajo de Ingeniería de Internet)
IP	*Internet Protocol* (Protocolo de Internet)
IPPM	*IP Performance Metrics* (Métricas de rendimiento IP)
ISM	*Industrial, Scientific and Medical* (Industrial, Científico y Médico)
ITU-T	*International Telecommunication Union* (Unión Internacional de Telecomunicaciones - Telecomunicaciones)
JSON	*JavaScript Object Notation* (Notación de Objetos de JavaScript)
LACP	*Link Aggregation Control Protocol* (Protocolo de Control de Agregación de Enlaces)
LAN	*Local Area Network* (Red de Área Local)
MAC	*Medium Access Control* (Control de Acceso al Medio)
MAN	*Metropolitan Area Network* (Red de Área Metropolitana)
MIB	*Management Information Base* (Base de Información de Gestión)
NAT	*Network Address Translation* (Traducción de Direcciones de Red)
NBI	*Northbound Interface* (Interfaz hacia el Norte)
NETCONF	*Network Configuration* (Configuración de Red)
NTP	*Network Time Protocol* (Protocolo de Tiempo de Red)
ODL	*OpenDayLigth*
ONOS	*Open Network Operating System* (Sistema Operativo de Red Abierta)
OPEX	*Operating Expenditure*(Gastos de Operación)
OSI	*Open System Interconnection* (Interconexión de Sistemas Abiertos)
OSPF	*Open Shortest Path First* (Protocolo de enrutamiento Abra Primero el Camino más Corto)
OVS	*Open Virtual Switch* (Conmutador Virtual de código Abierto)
OVSDB	*Open Virtual Switch Database* (Protocolo de Administración de Base de Datos de Conmutador Virtual)

PAN	*Personal Area Network* (Red de Área Personal)
PBSS	*Personal Basic Service Set* (Conjunto de Servicios Básicos Personales)
PCEP	*Path-Computation Element Communication Protocol* (Protocolo de Comunicación de Elementos para Cálculo de Rutas)
PCP	*PBSS Control Point* (Punto de Control del PBSS)
PHY	*Physical Layer* (Capa Fisica)
QoS	*Quality of Service* (Calidad de Servicio)
RAN	*Regional Area Network* (Red de Área Regional)
REST	*Representational State Transfer* (Transferencia de Estado Representacional)
SBI	*Southbound Interface* (Interfaz hacia el Sur)
SDN	*Software-Defined Networking* (Red Definida por Software)
SDWLAN	*Software Define Wireless Local Area Network* (Red Inalámbrica de Área Local Definida por Software)
SLAAC	*StateLess Address Auto Configuration* (Configuración Automática de dirección Independiente del Estado)
SNMP	*Simple Network Management Protocol* (Protocolo Simple de Administración de Red)
***Southbound* API**	*Southbound Application Programming Interface* (Interfaz de Programación de Aplicaciones hacia el Sur)
SSH	*Secure Shell* (Interprete de Ordenes Seguras)
SSID	*Service Set Identifier* (Identificador de Conjunto de Servicios)
STA	*Station* (Estación)
TFTP	*Trivial File Transfer Protocol* (Protocolo Trivial de Transferencia de Archivos)
SXP	*Scalable Group Tag eXchange Protocol* (Protocolo de Intercambio de Etiquetas de Grupo Escalable)
TPC	*Transmit Power Control* (Control de Potencia Transmitida)
TMN	*Telecommunications Management Network* (Red de Gestión de Telecomunicaciones)
TWAMP	*Two-Way Active Management Protocol* (Protocolo de Administración Activa Bidireccional)
UDP	*User Datagram Protocol* (Protocolo de Datagramas de Usuarios)

VDSL	*Very high-bit-rate Digital Subscriber Line* (Línea de Abonado Digital de Alta Velocidad)
VLAN	*Virtual Local Area Network* (Red de Área Local Virtual)
VND	*Visual Network Descriptor* (Descripción visual de red)
WAN	*Wide Area Network* (Redes de Área Amplia)
Wi-Fi	*Wireless Fidelity* (Fidelidad Inalámbrica)
WLAN	*Wireless Local Area Network* (Red Inalámbrica de Área Local)
XML	*Extensible Markup Language* (Lenguaje de Marcado Extensible)
XMPP	*Extensible Messaging and Presence Protocol* (Protocolo Extensible de Mensajería y Presencia)

INTRODUCCIÓN

La tecnología Wi-Fi[1] (*Wireless Fidelity*). es una solución inalámbrica para redes de área local (LAN, *Local Area Network*) de gran popularidad, con gran impacto comercial y múltiples escenarios de aplicación. Uno de ellos es el ámbito empresarial, dado que las Redes de Área Local Inalámbricas (WLAN, *Wireless Local Area Network*) proporcionan la versatilidad y flexibilidad de implementar arquitecturas de complejidad variable, dependiendo de la densidad de terminales, área de cobertura y número de Puntos de Acceso (AP, *Access Point*), a bajo costo. Estas arquitecturas son adaptables a un sin número de necesidades de comunicación, ya sean servicios en internet o infraestructuras privadas que a medida que crecen convergen con otros tipos de redes de comunicación y los usuarios finales aumentan al igual que sus requerimientos disminuyendo la agilidad en su despliegue y control de la red, por lo cual es necesario la implementación de tecnologías con capacidad de ofrecer canales de comunicación programables, que permitan contar con una abstracción de la red y control centralizado, infraestructuras flexibles, escalables y con automatización en tiempo real; estos factores de mejora se pueden obtener en las Redes Definidas por Software (SDN, *Software-Defined Networking*).

Como propósito fundamental de este trabajo de grado se busca analizar el desempeño de una Red Inalámbrica de Área Local Definida por Software (SDWLAN, *Software Define Wireless Local Area Network*) IPv4/IPv6 empresarial, a partir de las necesidades operativas del administrador de red y procesos centralizados enfocados a la gestión de redes inalámbricas desde una controladora mencionada como Sistema Operativo de Red Abierta (ONOS, *Open Network Operating System*) que centraliza actividades como son: la ubicación de los dispositivos de red y estaciones de trabajo conectadas, configuración de parámetros inalámbricos de puntos de acceso, haciendo uso de un protocolo de Configuración de Redes (NETCONF, *Network Configuration)* y monitoreo del estado de la red, donde se pueda observar fallas en los enlaces y su impacto en el servicio de comunicación de los usuarios finales.

Este documento está compuesto por cuatro (4) capítulos, el primero describe un marco teórico para el funcionamiento del estándar IEEE[2] 802.11x, modelos de gestión de redes, conceptos y elementos de redes definidas por software, métodos para el análisis de desempeño de redes y herramientas de emulación. El segundo

[1] Wi-Fi: tecnología inalámbrica, basada en el protocolo IEEE 802.11, que permite la interconexión de dispositivos electrónicos. El termino Wi-Fi esta registrado como marca comercial de un conglomerado de empresas, de alcance mundial, que impulsan y adoptan la tecnología. www.wi-fi.org

[2] IEEE, Institute of Electrical and Electronics Engineers. www.ieee.org.co

capítulo se refiere al diseño de dos escenarios de prueba para una SDWLAN haciendo uso de Mininet-WiFi [3] y enrutadores de marca *Mikrotik* con sistema operativo OpenWrt[4]. El tercer capítulo contiene los resultados de la emulación que conllevan a la generación de las conclusiones anotadas en el cuarto capítulo.

[3] Mininet-WiFi: emulador usado en el despliegue de redes definidas por software, de instalación virtualizada. Fuente: https://mininet-wifi.github.io/

[4] OpenWrt: “sistema operativo Linux dirigido a dispositivos integrados” Fuente: https://openwrt.org/

CAPÍTULO I: REVISIÓN DOCUMENTAL

1.1. Redes empresariales

Según "*ICD Analize the Future*"[5] la primera tendencia apunta al uso de software de gestión para controlar todos los aspectos de las redes empresariales mediante plataformas que están siendo mejoradas con algoritmos de aprendizaje automático e inteligencia artificial, permitiendo mayores niveles de gestión centralizada, agilidad en las operaciones de red y garantías de que la red está funcionando a la perfección. La segunda tendencia hace referencia a como las organizaciones se sienten cada vez más cómodas con el uso de estas plataformas para gestionar sus redes [1].

1.1.1. Estructuración básica de una red empresarial

La red de datos puede clasificarse de acuerdo con diversos criterios. Algunos de ellos se rigen por el tamaño de la red o la tecnología de transmisión, como por ejemplo las LAN, las cuales funcionan sobre medios cableados. Su área de impacto está delimitada por las estructuras precisadas al interior de una casa, oficina, edificio o campus. El equivalente inalámbrico a las LAN son las WLAN y es muy común encontrar redes híbridas, cableadas e inalámbricas, al interior de estos espacios. Este tipo de redes tienen la capacidad de concentrar cientos de terminales de usuario (estaciones fijas y dispositivos móviles) y funcionar como canal de acceso a servicios publicados en Internet a través de Redes de Área Amplia (WAN, *Wide Area Network*) y nubes privadas ubicadas en servidores conectados directamente a la LAN.

Las redes empresariales centran su operación en redes de tipo LAN y WLAN y utilizan infraestructuras de comunicación robustas donde los usuarios comparten recursos como conmutadores, enrutadores, puntos de acceso, cortafuegos, servidores, aplicaciones y accesos a Internet. Un ejemplo de arquitectura de red empresarial se puede observar en la figura 1.

[5] *IDC Analyze the Future*: empresa multinacional encargada del análisis de mercados a nivel mundial.

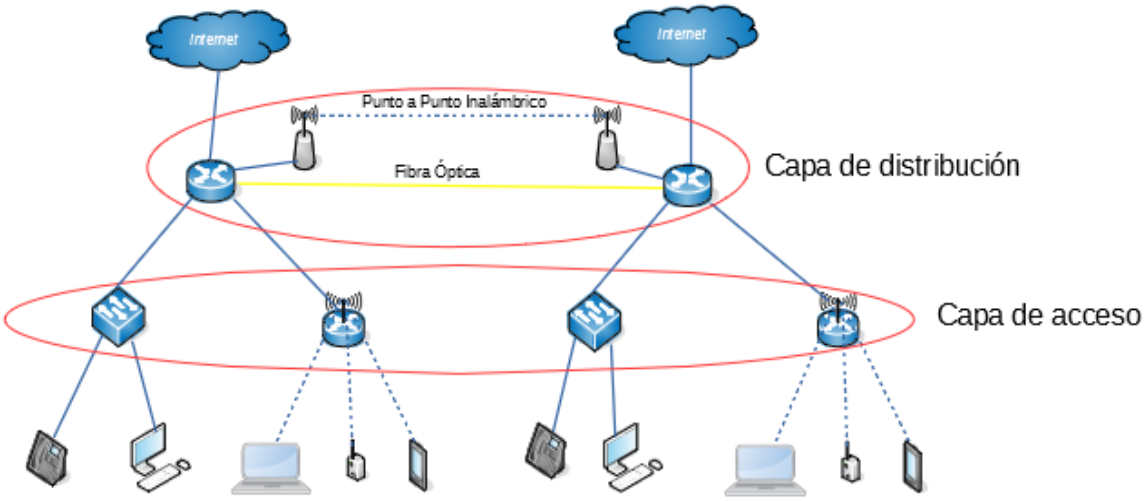


Figura 1: Modelo de red empresarial.

Con los años las WLAN han desplazado las conexiones cableadas en la capa de acceso dado que proporcionan conexiones móviles de alta velocidad, dirigida a una elevada densidad de usuarios, con coberturas más extensas y adaptables a un sin número de necesidades de comunicación, lo que permite reducir costos en Gastos de Capital (CAPEX, *Capital Expenditure*) y Gastos de Operación (OPEX, *Operating Expenditure*).

1.1.2. Deficiencias en la arquitectura de una red empresarial tradicional

En la actualidad las grandes y medianas corporaciones cuentan con una cantidad de usuarios que requieren tener acceso a redes desde diferentes terminales como teléfonos inteligentes, tabletas, computadoras portátiles, etc; a un sin número de servicios con patrones de tráfico dinámicos y de gran volumen de información, es decir, una o varias aplicación realizan peticiones y antes de recibir una respuesta acceden a múltiples bases de datos y servidores de forma simultánea, lo que requiere diseños de red complejos con grandes anchos de banda. Particularidades que hacen que las LAN y WLAN convencionales pierdan agilidad en su despliegue y control de esta, incrementando los tiempos de respuesta a eventos técnicos que afectan su desempeño y con ello su Calidad de Servicio (QoS, *Quality of Service*), disponibilidad, confiabilidad y seguridad. Por lo tanto, es necesario una tecnología capaz de ofrecer un control más flexible y dinámico para gestionar las redes de comunicación, que permita su adaptación a nuevos prospectos de red y que brinde la suficiente versatilidad y escalabilidad para soportar los modelos de negocio actuales y futuros. Una solución a estas deficiencias está en las SDN, las cuales están en la capacidad de ofrecer canales de comunicación programables, que permite contar con una abstracción de la red y

su control centralizado, sobre infraestructuras flexibles, escalables y con automatización en tiempo real [2].
El presente documento se enfoca exclusivamente en las SDWLAN aplicadas a nivel empresarial, que corresponde a redes WLAN inmersas en un contexto SDN que promete:

- ✓ Gestión Centralizada de los dispositivos de red.
- ✓ Una red ágil y adaptable a otras tecnologías de comunicación.
- ✓ Mayor rapidez para la implementación de dispositivos destinados a la concentración de alta densidad de usuarios y la improvisación para el establecimiento de flujos de datos.
- ✓ Facilidad en la consumación de funciones complejas, definiendo algoritmos basados en las necesidades del usuario.
- ✓ Mejor aprovechamiento de los recursos de red.
- ✓ Aprovisionamiento acelerado de nuevos clientes.

1.2. Red Inalámbrica de Área Local, WLAN

Una WLAN es un sistema de comunicación de datos basado en conexiones inalámbricas entre dispositivos situados en una misma área de cobertura, ya sea en interiores o exteriores. Este tipo de redes transmiten y reciben información a través de ondas electromagnéticas que usan el aire como medio de difusión. Se caracterizan por proporcionar, a los dispositivos clientes, movilidad sin perder conexión, fácil instalación (no es necesario tendidos de cable u obras civiles) y flexibilidad (llega donde el cable no alcanza, salta obstáculos y atraviesa paredes). Este tipo de redes son posibles gracias estándares como es el IEEE 802.11, más conocida como Wi-Fi.

1.2.1. Wi-Fi: IEEE 802.11x. Fundamento de las redes WLAN

El comité de normas IEEE 802 patrocina la investigación y generación de múltiples estándares y prácticas recomendadas, aprovechadas en redes LAN, Redes de Área Metropolitana (MAN, *Metropolitan Area Network*), Redes de Área Personal (PAN, *Personal Area Network*) y Redes de Área Regional (RAN, *Regional Area Network*), centrando su función en la capa de Control de Acceso al Medio (MAC, *Medium Access Control*) y la Capa Física *(PHY, Physical Layer*) del modelo de Interconexión de Sistemas Abiertos[6] (OSI, *Open System Interconnection*). La

[6] OSI, Modelo de interconexión de sistemas abierto ISO/IEC 7498-1, www.iso.org/standard/20269.html

capa MAC controla el acceso al medio inalámbrico y el envío de datos, la capa PHY se encarga de la transmisión y recepción de datos sobre el medio. En la figura 2 se observa el árbol familiar de la norma IEEE 802 y su aplicación sobre el modelo OSI. [3]

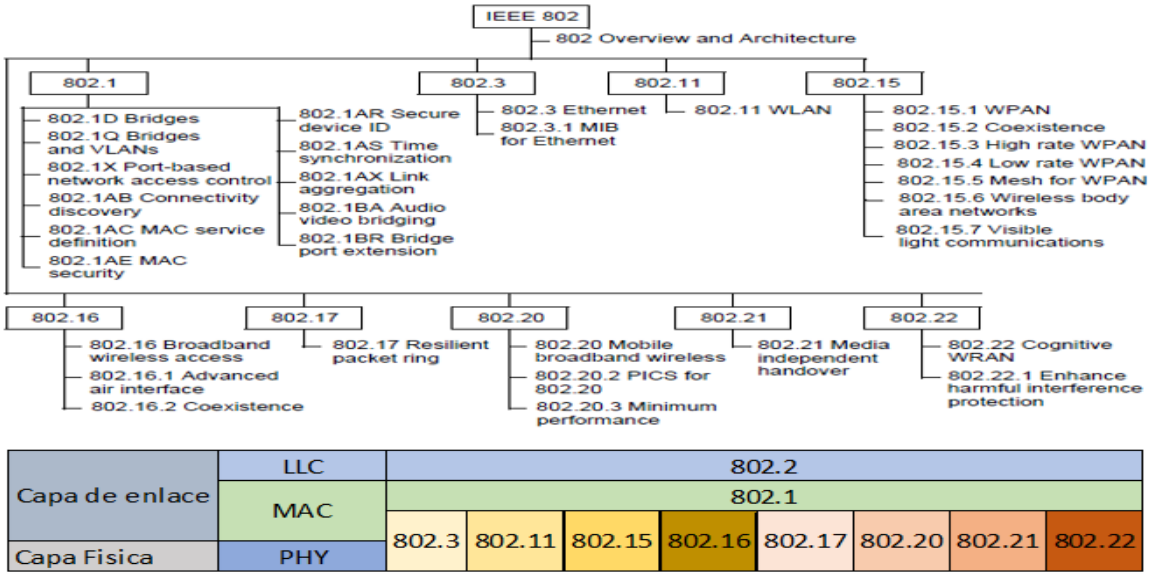


Figura 2: Estructura del estándar IEEE 802. Fuente: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture

El estándar IEEE 802.11 hace parte de la Familia IEEE 802 y se encarga de normalizar las tecnologías aplicadas a las redes WLAN y define su alcance como "el control de acceso al medio y varias especificaciones de la capa física para la conectividad inalámbrica en estaciones fijas, portátiles y móviles (*STA, Station*) dentro de una red de área local y su propósito es proporcionar conectividad inalámbrica a estaciones fijas, portátiles y móviles dentro de un área local" [3]. Su operación se centra sobre las frecuencias no licenciadas de las bandas de uso Industrial, Científico y Médico (ISM, *Industrial, Scientific and Medical*)[4]. En Colombia la entidad reguladora de espectro radioeléctrico, la Agencia Nacional del Espectro (ANE), establece que las bandas ISM permitidas que aplican al estándar son la de 2.4 GHz (2400MHz-2500MHz) y 5GHz (5150MHz-5250MHz, 5250MHz-5350MHz, 5470MHz-5725MHz, 5725MHz-5875MHz) [5].

En un principio, el estándar original se dio a conocer en 1997 y especifica tasas de transmisión de 1 a 2 Mbps sobre la frecuencia de los 2.4GHz. Posteriormente, salieron a la luz los modelos IEEE 802.11a e IEEE 802.11b, no compatibles entre sí, ya que su funcionalidad se ubica en la frecuencia de los 5GHz (transmisiones de hasta 54Mb/s) y los 2.4GHz (transmisiones de hasta 11Mb/s), respectivamente.

Consecuente a la evolución de la tecnología y la gran acogida del estándar por la industria y comercio mundiales, nacieron esquemas que buscan satisfacer los nuevos y estrictos requisitos del mercado en términos de velocidad de datos, densidad de usuarios, seguridad de red y calidad de servicio, como se aprecia en la tabla 1.

ESTÁNDAR	FECHA DE SALIDA	VELOCIDAD MÁXIMA Mb/s	FRECUENCIA GHz	ANCHO DE CANAL MHz	MODULACIÓN	MULTIPLEXACIÓN	MIMO
IEEE 802.11	1997	1 y 2	2.4	22	GFSK, DBQPSK, DQPSK	FHSS y DSSS	NO
IEEE 802.11b	1999	11	2.4	22	GFSK, DBQPSK, DQPSK	FHSS y DSSS	NO
IEEE 802.11a	1999	54	5	20	BPSK, QPSK, 16QAM, 64QAM	OFDM	NO
IEEE 802.11g	2003	54	2.4, 5	20	BPSK, QPSK, 16QAM, 64QAM	FHSS, DSSS, OFDM	NO
IEEE 802.11n	2009	600	2.4, 5	20, 40	BPSK, QPSK, 16QAM, 64QAM	FHSS, DSSS, OFDM	SI, hasta 4x4
IEEE 802.11ac	2013	3400	5	20, 40, 80, 160	BPSK, QPSK, 16QAM, 64QAM, 256QAM	OFDM	SI, hasta 8x8
IEEE 802.11ax	2019	4800	5	20, 40, 80, 160	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM	OFDMA	SI, hasta 8x8

Tabla 1: Resumen comparativo enmiendas del estándar IEEE 802.11

1.2.1.1. Componentes de la arquitectura IEEE 802.11

La arquitectura IEEE 802.11 está compuesta por varios elementos que interactúan para conformar una WLAN, permitiendo que el movimiento físico de las STA sea transparente para las capas superiores del modelo OSI. El estándar define el concepto de Conjunto de Servicios Básicos (*BSS, Basic Service Set*) como un grupo de estaciones ubicadas dentro de una misma área de cobertura, que se reconocen una a otra, y pueden transmitir información entre ellas de forma inalámbrica; a partir de esta noción, el estándar genera cuatro topologías [4].

a. Modo Conjunto de Servicios Básicos Independientes (IBSS, *Independent Basic Service Set*): el funcionamiento de este modo parte de la comunicación directa entre dos estaciones inalámbricas (Punto a Punto), sin control alguno, como se observa en la figura 3.

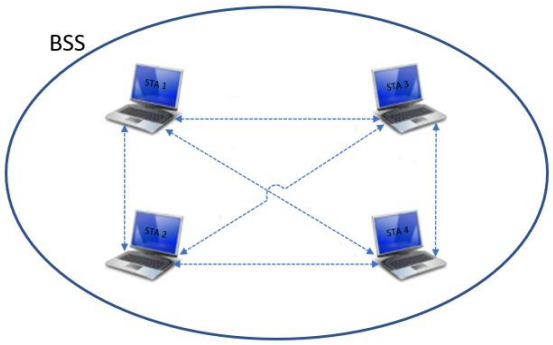


Figura 3: Concepto de IBSS.

b. Modo Conjunto de Servicios Básicos Personales (PBSS, *Personal Basic Service Set*): este modo se basa el IBSS, y permite una comunicación directa entre todas las estaciones de una BSS definiendo una STA como Punto de Control del PBSS (*PCP, PBSS Control Point*), el cual proporciona la sincronización básica de tramas, asigna periodos de servicio y periodos de acceso.

c. Modo Infraestructura BSS: este modo presenta dos componentes básicos, un BSS y en su interior un dispositivo denominado punto de acceso. Un AP es una estación a la cual se asocian las STA de la BSS bajo un mismo Identificador de Conjunto de Servicios (*SSID, Service Set Identifier*) a través de un medio inalámbrico y sirve de pasarela para instituir un nexo con otras BSS o redes LAN, como se observa en la figura 4.

Figura 4: Concepto de Infraestructura BSS.

d. Modo Conjunto de Servicios Extendidos (ESS, *Extended Service Set*): la necesidad para establecer un vínculo entre dos o más BSS y la integración con otro tipo de redes LAN cableadas hacen que se cree una topología que permita la creación de redes inalámbricas de tamaño y complejidad arbitrarias. Una ESS está compuesta por múltiples BSS asociadas mediante

un mismo sistema de distribución (DS, *Distribution System*) pero el DS no hace parte del ESS. Este modo brinda la posibilidad de realizar *roaming* entre celdas, de esta forma se consigue la ampliación del área de cobertura de una BSS.

Figura 5: Concepto ESS.

1.3. Modelos de gestión de redes inalámbricas

Gran parte de la operación de las empresas modernas dependen de los servicios de red, los cuales cobran importancia de acuerdo con el proceso o función corporativa a la que están ligados, resaltando los componentes de hardware donde se ejecutan las instrucciones lógicas que permiten la operación mercantil y administrativa de cada compañía. Lo anteriormente descrito genera la necesidad de monitorear el hardware de red y los servicios que prestan, de tal manera que sea posible evaluar el rendimiento y eficiencia de la red en general, y tolere responder a eventualidades.

Los sistemas de gestión de red se diseñan siguiendo un modelo que garantice que la infraestructura de comunicación vaya de la mano con los pilares de la seguridad de la información (Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad y No Repudio), proporcionen un conjunto de actividades y procesos que permiten desempeñar funciones de planificación, diseño, instalación, mantenimiento, operación, control y monitoreo de recursos de red, y se adapten a la evolución de las arquitecturas de red que emergentes.

1.3.1. Modelo de referencia ITU-T FCAPS[7]

Uno de los modelos más antiguos pero aún vigente es el emitido por la Unión Internacional de Telecomunicaciones en su recomendación M.3010 plantea el modelo de Red de Gestión de Telecomunicaciones (TMN, *Telecommunications Management Network*) sobre el cual se busca definir un estándar multimarca que permita generar soluciones de gestión y recopilación de información estadística de los Elementos de Red (NE, *Network Element*) donde se ejecuta un proceso o conjunto de procesos que ofrecen un servicio o pluralidad de servicios. El modelo cuenta con una arquitectura lógica de 5 capas jerárquicas [6].

a. Capa de elementos de red: hace referencia a los EN que se necesita gestionar.
b. Capa de gestión de elementos: esta capa aplica un Sistema de Gestión de Elementos (EMS, *Element Management System*) es decir una metodología técnica de gestión de los dispositivos de red activos, ya sean firewalls, enrutadores, conmutadores, puntos de acceso, etc.
c. Capa de administración de red: este nivel estructura la relación física y lógica entre los NE, buscando crear una vista general de la red, supervisar su rendimiento y eficacia, correlacionar eventos y gestionar el tráfico basado en atributos y comportamiento de cada elemento de red.
d. Capa de gestión de servicios: en esta capa se concentra la función de prestación de servicios al cliente (usuario final), tal como: aprovisionamiento de estaciones de trabajo, gestión de cuentas de usuario, QoS e Inventario.
e. Capa de gestión comercial: a este nivel le pertenecen las funciones de planificación de alto nivel, establecimiento de metas, estudio de mercado, presupuesto y decisiones empresariales.

La ITU-T en su recomendación M.3400 asocia al modelo TMN a 5 áreas funcionales derivadas del modelo ISO/IEC 7498-4 FCAPS donde se precisa la gestión redes de acuerdo con [7].

a. Gestión de Fallas: función dedicada a detectar, aislar y corregir una avería o condición anómala en los NE o en su entorno. Esta área depende de la siguiente información:

   - ✓ Generación y atención de condiciones de alarma
   - ✓ Localización de las condiciones de alarma

[7] ITU-T FCAPS: Unión Internacional de Telecomunicaciones en su apartado para la normalización de las Telecomunicaciones, haciendo uso del modelo de gestión (Fallas, Configuración, Contabilidad, Desempeño y Seguridad) de la organización internacional de estandarización, ISO.

- ✓ Lectura de registro de errores
- ✓ Pruebas de diagnostico
- ✓ Reparación de averías

b. Gestión de Configuración: función dedicada ejercer control sobre los parámetros de configuración y operación de los NE. El cometido de esta área se cumple de acuerdo con las siguientes capacidades:

- ✓ Parametrización de condiciones en el preaprovisionamiento de NE
- ✓ Descubrimiento automático de los NE
- ✓ Aprovisionamiento y configuración a través de interfaces interactivas
- ✓ Medición de la eficiencia de configuraciones
- ✓ Generación de copias de copias de seguridad y restauración de datos de configuración de los NE
- ✓ Levantamiento de inventarios

c. Gestión Contable: función dedicada a medir el uso de servicios de red y determinar el costo para el proveedor de servicios, así como la cantidad que se le ha de cobrar al cliente por el uso del recurso. La funcionalidad de esta área está asociada a la recopilación de la siguiente estadística:

- ✓ Medición de recursos utilizados por cada usuario
- ✓ Tarificación
- ✓ Restricciones de uso
- ✓ Facturación convergente por el uso de múltiples EN sobre una sola cuenta de cobro
- ✓ Auditorías
- ✓ Informes de fraude

d. Gestión del Desempeño: función dedicada a evaluar y reportar el comportamiento y eficacia de los EN entorno al rendimiento de la red. Esta evaluación se realiza mediante:

- ✓ Pruebas periódicas de utilización, rendimiento, disponibilidad, latencia y Jitter
- ✓ Identificación de indicadores de desempeño y establecimiento de umbrales de evaluación
- ✓ Análisis de datos de rendimiento y eficacia
- ✓ Identificación de tendencias y mejores configuraciones
- ✓ Generación de informes que permitan dar por terminada una situación anómala

e. Gestión de Seguridad: función dedicada a la generación de un entorno protegido para los NE y el sistema de gestión de red. El aseguramiento de la red depende del control y cumplimiento de políticas como son:

- ✓ Autenticación
- ✓ Control de acceso
- ✓ Confidencialidad de datos
- ✓ Integridad de datos
- ✓ Prevención de intrusos
- ✓ Detección y contención de ataques
- ✓ Recuperación ante una perpetración
- ✓ Análisis forense

Cada una de las 5 capas del modelo TMN está asociada con una de las funciones del modelo FCAPS, como se aprecia en la figura 6, donde las capas inferiores (elementos de red y gestión de elementos de red) alimentan la funcionalidad de las capas superiores y su implementación es de carácter obligatorio, aunque las superiores no lo son, ver figura 6.

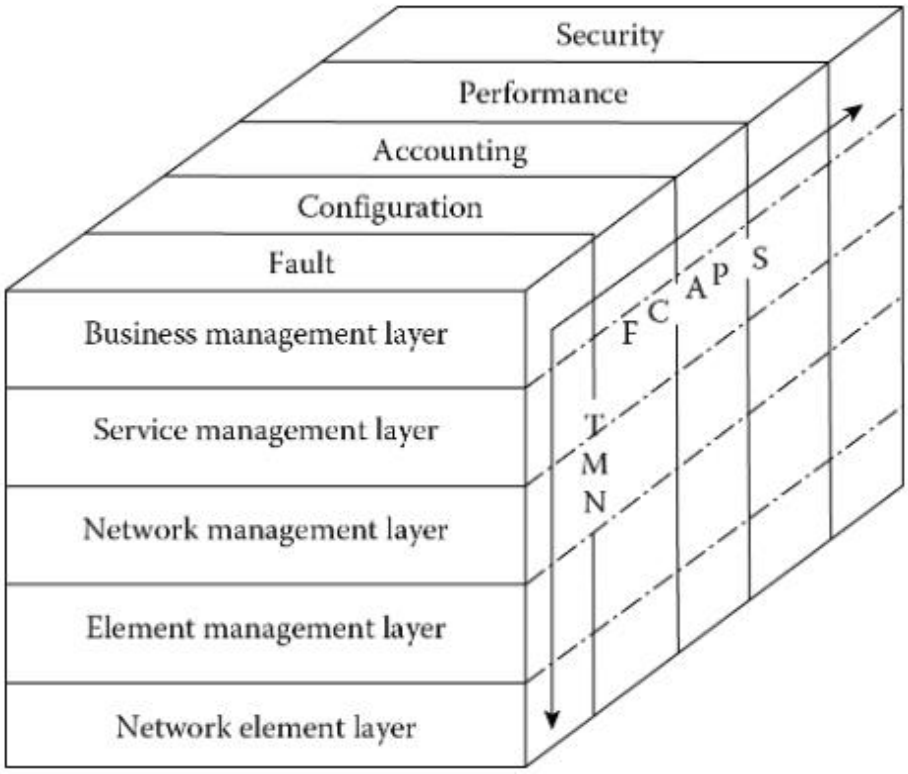


Figura 6: Modelo FCAPS Vs Modelo TMN. Fuente: Fundamentals of EMS, NMS, and OSS/BSS.

1.3.2. Modelo de referencia IETF RFC-6632[8]

Dado el crecimiento de las redes individuales, cantidad de dispositivos y diversidad de fabricantes que componen la Internet, el Grupo de Trabajo de Ingeniería de Internet (IETF, *Internet Engineering Task Force*) ha mostrado gran interés en la generación de estándares enfocados a la gestión automatizada de tareas de administración de redes, muestra de ello esta es el estándar RFC-6632.

IEFT estandariza dos modelos de gestión de datos, el primero apunta a una concepción genérica para modelos que definen su operación en categorías o capas fundamentada en abstracciones de gestión centralizada con interfaces contenidas en la IF-MIB RFC-2863[9] y Entity-MIB RFC-4133[10]. El segundo hace referencia al modelo FCAPS para aplicaciones y tareas de administración por fuera de IETF, es decir no es un principio organizacional para sus modelos de gestión de datos, pero si es tomado en cuenta por motivos de compatibilidad.

El modelo definido por IEFT está estructurado en 4 categorías jerárquicas [8]:

a. Capa de enlace: este nivel tiene a cargo la supervisión de los enlaces de comunicación (ADSL, VDSL, GMPLS, ISDN, ATM, Ethernet, Wi-Fi y Cable modem) entre los NE por donde sea posible pasar el Protocolo de Internet (IP, *Internet Protocol*) y se utiliza para gestionar funciones de fallas, rendimiento y seguridad.

b. Capa de red: este nivel se encarga de suplir funciones de configuraciones de los NE y medir e informar la calidad, rendimiento, y confiabilidad de la entrega de datos mediante métricas de conectividad como latencia, pérdidas, Jitter y ancho de banda de los enlaces.

c. Capa de transporte: en esta capa se discriminan estadísticas de rendimiento extendidas del nivel anterior aplicadas a protocolos TCP y UDP. Su función se centra en diagnosticar problemas de red y aplicaciones.

d. Capa de aplicación: la función de esta capa es la gestión de fallos, configuración y rendimiento de las aplicaciones a partir de parámetros como

[8] IEFT RFC6632: Grupo de Trabajo de Ingeniería de Internet y su estándar de gestión de red RFC 6632
[9] IF-MIB RFC-2863: estándar encargado de definir los objetos que componen la Base de Información de Gestion (MIB, *Management Information Base*) usada en el Protocolos de Administración Simple de Red (SNMP, *Simple Network Management Protocol*)
[10] Entity-MIB RFC-4133: estándar encargado de definir los elementos lógicos y físicos a gestionar al interior de una red por el agente SNMP

son el inicio o cierre de sesión y atributos de software que requieren cooperación del mismo software en evaluación.

1.3.3. Protocolos de gestión de redes

Para el cumplimiento de los objetivos del presente proyecto los protocolos de gestión relevantes se ubican en las capas inferiores (configuración de NE, aprovisionamiento IP, supervisión de enlaces y gestión de fallas de red) de cualquiera de los dos modelos descritos en apartes anteriores. Los protocolos de administración, configuración y aprovisionamiento de puntos de acceso y estaciones de trabajo son mencionados en el RFC-6632 y de describen como [8]:

a. Protocolo Simple de Administración de Redes, SNMP: es un protocolo diseñado para la administración y monitoreo remoto y centralizado de dispositivos de red, servidores y estaciones de trabajo. Su operación depende del agente SNMP instalado y configurado en equipos a monitorear y los módulos MIB disponibles.

b. Protocolo de Configuración de Red, NETCONF: es un protocolo que proporciona mecanismos configuración y control de dispositivos de red. Se basa en Lenguaje de Marcado Extensible (XML, *Extensible Markup Language*) y proporciona funcionalidad total sobre la línea de comandos nativa de un dispositivo. Adicionalmente alberga un sistema de notificaciones para el Protocolo Simple de administración de red SNMP.

c. Lenguaje de modelado de datos YANG - NETCONF: Yang es un lenguaje de modelado de datos jerárquico para el protocolo NETCONF diseñado para la configuración de servicios y dispositivos pertenecientes a una red de comunicación.

d. Protocolo de Configuración Dinámica de Anfitrión (DHCP, *Dynamic Host Configuration Protocol*): este protocolo se encarga del aprovisionamiento de direccionamiento IPv4/IPv6, puertas de enlace e indicar cual es la dirección IP de los Sistemas de Nombres de Dominio (DNS, *Domain Name System*) y servidores de Protocolo de Tiempo de Red (NTP, *Network Time Protocol*) a las STA y/o interfaces de los dispositivos de red que lo soliciten.

e. Protocolo de Control y Aprovisionamiento de Puntos de Acceso Inalámbrico (CAPWAP, *Control And Provisioning of Wireless Access Points*): es un estándar que permite la administración, control y aprovisionamiento centralizado de múltiples AP dentro de una misma red. Las principales

características que brinda el protocolo es el control de acceso a la red dirigido a las STA que solicitan asociación y la movilidad entre puntos de acceso, handover.

1.4. Redes definidas por software, SDN

En una red de comunicaciones convencional, el control de esta se distribuye sobre cada uno de los dispositivo que la compone, aspecto que toma la arquitectura SDN y la desacopla del reenvío de datos en cada equipo y lo lleva a una controladora basada en software, proporcionando la posibilidad que el control de la red pueda ser programable, centralizado y con una visión global de la misma [9].

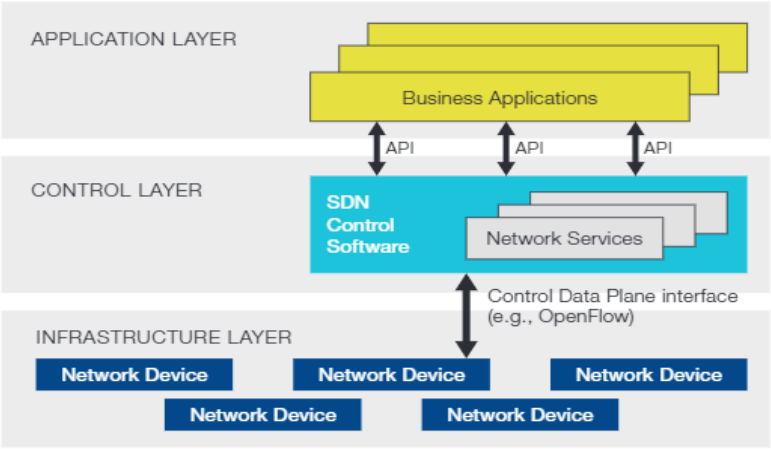


Figura 7: Arquitectura de redes definidas por software. Fuente: Software Defined Networking: The New Norm for Networks.

En la figura 7 se muestra una visión lógica de la arquitectura SDN, compuesta por tres capas jerárquicas (Aplicación, Control e Infraestructura).

1.4.1. Capa de datos o Infraestructura

La capa de datos hace referencia a los elementos físicos de red como son conmutadores, enrutadores, puntos de acceso, etc. Los cuales se encargan, exclusivamente de la recepción y reenvió de datos. Estos equipos al unirse a este tipo de redes son denominados conmutadores y son gestionados por el controlador SDN, de igual manera que los flujos de paquetes. El control es establecido desde la capa adyacente a través una Interfaz hacia el Sur (SBI, *Southbound Interface*) establecidas por la Interfaz de programación de Aplicaciones hacia el Sur (Southbound API, *Southbound Application Programming Interface*). La API más común y distribuida es OpenFlow, pero hay software enfocado a la gestión de redes,

heredadas de las redes tradicionales, como son YANG-NETCONF, CAPWAP y SNMP, entre otros.

1.4.1.1. OpenFlow

Open Flow es un protocolo de propósito general, no propietario, orientado a establecer comunicación entre capas dentro de la arquitectura SDN. Consiste en un conjunto de mensajes que se envían desde el controlador SDN a los equipos de la red y viceversa. Los mensajes permiten que el controlador programe el conmutador para permitir un control detallado sobre el flujo de información de los usuarios, entendiendo como flujo el conjunto de paquetes que poseen características en común y se transfieren desde un punto a otro. Cuando el controlador define un flujo, le proporciona al conmutador la información necesaria para saber cómo tratar los paquetes que coincidan con ese flujo, siendo sus posibilidades: reenviar el paquete a uno o más puertos de salida, descartar el paquete o pasar el paquete al controlador [10].

El protocolo ha evolucionado desde la versión 0.2.0 desarrollada en 2008 hasta la versión 1.5.0 publicada en 2014. Las versiones más relevantes para el trabajo que se adelanta son las que implementan tablas de flujos donde se caracterizan entradas de rendimiento, escalabilidad, redundancias, soporte IPV6 y QoS. Estas son las superiores a la versión 1.2

1.4.2. Capa de control

Su unidad fundamental es un controlador SDN que traduce las peticiones impartidas por la capa de aplicación a la capa de datos o infraestructura. De igual manera, proporciona a la capa de aplicación la información necesaria de la red para que esta se mantenga enterada de su comportamiento y necesidades.

Según Carlos Julio Quimbayo en su trabajo de investigación [11] “Propuesta metodológica para la selección de controladores de red SDN a nivel empresarial”, en la actualidad se cuenta con 35 controladores SDN documentados, y los caracteriza haciendo uso de 23 variables. De acuerdo con esta investigación existen 3 controladores de gran interés para el desarrollo del proyecto que se adelanta, *FloodLight*, ONOS y *OpenDayLight*; los cuales se describen en la tabla 2.

VARIABLE	FLOODLIGHT	ONOS	OPENDAYLIGHT
Soporte OpenFlow	V 1.0, 1.1, 1.2, 1.3, 1.4, 1.5	V 1.0, 1.3	V 1.0, 1.3, 1.4

Southbound API	OpenFlow, Indigo Agent and Oxyagent	OpenFlow, NETCONF, PCEP, OVSDB, BGP, P4[11], TL1, SNMP	OpenFlow, OVSDB, SNMP, PCEP, BGP, YANG, NETCONF, LACP, Cisco Opflex, CAPWAP, P4, SXP, USC, COPS
Northbound API	REST API, Java API, RPC, Quantum.	REST API, Java API.	REST API, Java API, Restconf, XMPP, Maven
Tipo de Interfaz	CLI, WEB GUI	CLI, WEB GUI	CLI, WEB GUI
Incluye aplicaciones de Enrutamiento	Enrutamiento (OSPF), OVS, Balanceo de carga, Calidad de servicio, NAT, Balanceador de costos, DHCP, Proxy ARP, SE-Floodlight, HAND	Enrutamiento (BGP)	Enrutamiento (OSPF), Balanceo de carga
Incluye aplicaciones de Medición	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Gestión de estadísticas y equipos
Incluye aplicación de Seguridad	ACL, Firewall, Autenticación, autorización y seguimiento de aplicaciones, Detección de anomalías, VLAN, Gestión de fallos	Gestión de fallos	Autenticación, autorización y limitación de Administradores de red
Flujo soportado	2.5 M/s	1 M/s	2.5 M/s
Código Abierto	Si	Si	Si
Sistema operativo	Linux, MAC OS, Windows	Linux, MAC OS, Windows	Linux, MAC OS, Windows
Multihilos	Si	Si	Si
Consistencia de la Información	No	Alta	Débil
Ambientes de uso	Redes empresariales, Data center, Infraestructura en la Nube	Redes empresariales, Data center, Infraestructura en la Nube	Redes empresariales, Data center, Infraestructura en la Nube
Distribuido o Centralizado	Centralizado	Distribuido	Distribuido
Tolerancia a Fallos	No	Si	Si
Documentación	Buena	Alta	Alta
Licencia	Apache 2.0	Apache 2.0	EPL V1.0
Actualización de Pagina WEB	2018	2019	2019

Tabla 2: Caracterización de controladores SDN. Fuente: Propuesta metodológica para la selección de controladores de redes SDN a nivel empresarial

1.4.2.1. Controladora *FloodLight*

Este controlador es uno de los primeros en entrar en la escena de la arquitectura SDN, y se mantiene gracias a los ingenieros de “Big Switch Networks”.

[11] P4: es un lenguaje de programación de enfocado a expresar lógica de procesamiento de paquetes orientado a dispositivos de red como son los conmutadores y enrutadores.

Es un software de código abierto basado en Java que utiliza OpenFlow para coordinar flujos de datos. Está en la capacidad operar con conmutadores físicos y virtuales que acepten OpenFlow. Entre sus componentes se encuentran [12]:

- ✓ Gestor de topología, descubre terminales OpenFlow y no OpenFlow.
- ✓ Gestor de dispositivos, ya sea por MAC o IP.
- ✓ Cálculo de rutas
- ✓ Interfaz de administración web.

1.4.2.2. Controladora *OpenDayLight*

El proyecto *OpenDayLight* se centra en el desarrollo de una plataforma multiprotocolo, modular, escalable, con alta disponibilidad y de código abierto, diseñada para personalizar y automatizar redes de cualquier tamaño y escala, bajo el concepto SDN. Este proyecto es liderado por "*Linux Foundation Projects*", autores independientes e industria privada como Cisco, Brocade, Ericsson, Citrix, Intel, HP, Dell, Red Hat, IBM, Huawei, NEC, VMware, entre otros. ODL es un software de Máquina Virtual Java (JVM, *Java Virtual Machine*) y se puede ejecutar desde cualquier sistema operativo [13].

1.4.2.3. Controladora ONOS

Sistema Operativo de Red Abierta (ONOS, *Open Network Operating System*) es un controlador SDN distribuido, modular, extensible, de código abierto, y con una arquitectura horizontal que proporciona flexibilidad y escalabilidad. Enfatiza en el uso del protocolo OpenFlow y la implementación de características de alta confiabilidad. A diferencia de ODL no prioriza la reutilización de equipos de red y protocolos heredados de diseños de red convencionales. Este controlador es desarrollado por "*Open Networking Foundation*", ha ganado adeptos como AT&T, NEM, CIENA y Fujitsu. El controlador está dirigido a proveedores de servicios, donde se desee o se resalte la creación de aplicaciones hacia el norte basadas en el protocolo OpenFlow [10].

1.4.3. Capa de Aplicación

La capa de aplicación aloja los programas que realizan las tareas de control de acceso, gestión de enlaces, balanceo de cargas, monitoreo de tráfico, seguridad, enrutamiento, mapeo de red, QoS, y demás servicios propios de la red. Esta capa se comunica con la capa de control mediante una o más Interfaces hacia el Norte (NBI, *Northbound Interface*). Las interfaces pueden ser establecidas por protocolos de código abierto o privados, algunos son mencionados en la tabla 2.

Desde que nació el concepto de SDN, han surgido dos clases de aplicaciones, proactiva y reactivas, cuya diferencia básica está centrada en el hecho de que las aplicaciones reactivas reciben los mensajes directamente del dispositivo de red. Esta discrepancia genera una preocupación sobre la escalabilidad, confiabilidad y susceptibilidad a ataques de denegación de servicio en este tipo de aplicación, por ende, los diseños de las aplicaciones tienden a ser proactivos [10].

a. Aplicaciones proactivas: este tipo de aplicación configura los conmutadores o dispositivos de la red con entradas de flujo o atributos de configuración apropiados para manejar el tráfico entrante antes de que los flujos de datos lleguen al conmutador. Los eventos que requieran cambios en las tablas de flujo o cambios de configuración en los conmutadores provienen de mecanismos de monitoreo (otras aplicaciones que pueden ser internas o externas al controlador) que están fuera del alcance del canal de comunicación principal, entre el dispositivo de red y el controlador, ver figura 8.

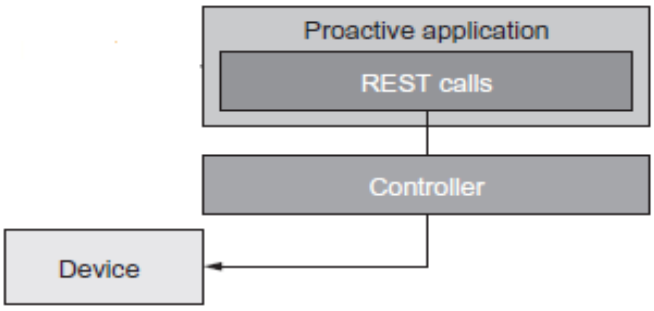


Figura 8: Esquema de las aplicaciones proactivas. Fuente: Software Defined Networks. A Comprehensive Approach

b. Aplicaciones reactivas: este tipo de aplicaciones reciben, periódicamente, paquetes reenviados desde el conmutador o dispositivo de red, para ser procesadas y resueltas con la acción respectiva para el tratamiento de flujos. La acción que tomar, suele ser la creación de una nueva entrada de flujo en el conmutador para que la próxima vez que llegue este tipo de paquete, pueda ser manejado localmente. La aplicación programará varios conmutadores al mismo tiempo para que cada conmutador contenga un conjunto consistente de entradas de flujo, ver figura 9.

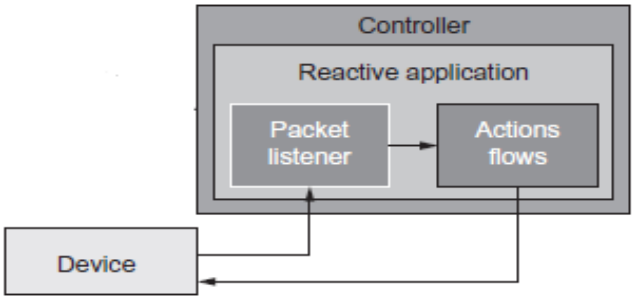


Figura 9: Esquema de las aplicaciones reactivas. Fuente: Software Defined Networks. A Comprehensive Approach

1.5. Métodos de análisis de desempeño de red

El análisis de desempeño una red consiste en estudiar el tráfico circulante en la misma, con el fin de determinar su capacidad, métricas bajo las cuales se comporta y la calidad de experiencia de los usuarios finales.

1.5.1. Métricas de desempeño

Los administradores de red, en su cotidianidad, se enfrentan a la necesidad de medir el desempeño de su infraestructura de telecomunicaciones, para lo que la ITU-T en su comisión número 12 y el IETF en su comisión de Métricas de rendimiento IP (IPPM, *IP Performance Metrics*) han definido algunos parámetros y metodologías de medición, con énfasis diferentes. La ITU-T hace hincapié en la evaluación de calidad de servicio y la IETF se enfoca en medir el rendimiento y la confiabilidad de una red. Pero los conceptos en las métricas son muy similares, como se muestra en la tabla 3.

MÉTRICAS	IETF RFCs	Ref. ITU-T
Marco de trabajo	RFC 2330	Y.1540
Perdidas	RFC 2680	Y.1540 Y.1020
Retardos	RFC 2679, RFC 2681	Y.1540 G.1020 G.114
Variación de retardos	RFC 3393	Y.1540 G.1020
Conectividad y Disponibilidad	RFC 2678	Y.1540
Capacidad y Disponibilidad de ancho de banda	RFC 5136	

Tabla 3: Relación de métricas usadas en IETF y ITU-T. Fuente: ETSI EG 202 765-3 V1.1.2

- ✓ Retardo unidireccional (*One Way Delay*): este parámetro es usado para medir el tiempo que un paquete IP se demora en atravesar la red desde un host[12] a otro.

[12] Host: hace referencia a dispositivos conectados a una red de comunicaciones.

- ✓ Retardo de ida y vuelta (*Round Trip Delay*): este parámetro es usada para medir la expectativa de tiempo que un paquete IP se demora en ir y volver desde un host a otro.
- ✓ Variación del retardo de paquetes IP (*IP Packet Delay Variation*): este parámetro es usado para medir la variación en la latencia, en una secuencia de retardos a lo largo del tiempo.
- ✓ Perdida de paquetes unidireccionales (*One Way Packet Loss*): este parámetro es usado para medir la probabilidad esperada para que un paquete llegue de un host a otro. Es una medida de confiabilidad en la entrega en la red.
- ✓ Conectividad: este parámetro es usado para medir la probabilidad de que un host pueda llegar a otro. Es una medida de confiabilidad del transporte de datos en la red.
- ✓ Capacidad y Disponibilidad de ancho de banda: estas métricas hacen referencia a atributos en los enlaces pertenecientes a una estructura de red y describen la capacidad por unidad de tiempo para el transporte de datos para una conexión y cuanto de esa capacidad no está en uso en un momento determinado.

1.5.2. Metodologías de medición

Cada métrica de desempeño está definida en dos tipos de metodología de medición. En este documento no se enfatizará en cómo se realiza la medición de cada parámetro, pero si se enfatiza en algunos protocolos de red que ejecutan estas metodologías.

a. Mediciones activas: los métodos de medición activos son aquellos métodos que inyectan tráfico a una red y sus métricas se basan en la respuesta que se tenga. Este tipo de tráfico puede afectar otros flujos de datos, por lo que es necesario que su programación y volumen sean configurado cuidadosamente [14].

   Entre los protocolos más comunes que realizan este tipo de mediciones son:

   - ✓ Paquete de Internet Groper (Ping, *Packet Internet Groper*): es una herramienta de diagnóstico que verifica la conectividad entre dos hosts pertenecientes a una red IP. Hace uso del Protocolo de mensajes de control de Internet (ICMP, *Internet Control Message Protocol*) para el envío de paquetes.
   - ✓ Protocolo de Medición Activa Bidireccional (TWAMP, *Two-Way Active Measurement Protocol*): es un estándar de nueva generación, documentado por el grupo IPPM, que admite protocolos de capa 3 del

modelo de referencia OSI, y se utiliza para medir parámetros de rendimiento bidireccionales, entre dos hosts, al interior de una red IP.

- ✓ IPERF: es un software de código abierto con arquitectura cliente-servidor, que basa su funcionamiento en la creación de flujos de datos TCP y UDP para medir el rendimiento de una red IP. Está en la capacidad de realizar mediciones unidireccionales y bidireccionales.

En la tabla 4 se puede observar una comparativa de las tres herramientas.

HERRAMIENTA	PROTOCOLO	ANCHO DE BANDA	RETARDOS	VARIACIONES EN LOS RETARDOS	PERDIDAS	CONECTIVIDAD
Ping	ICMP	X	P	X	P	P
TWAMP	TCP/UDP	X	P	P	P	P
IPERF	TCP/UDP	P	X	P	P	P

Tabla 4: Comparativa de herramientas de medición activa.

b. Mediciones pasivas: los métodos de medición pasiva proporcionan información sobre el tráfico de red mediante capturas de todos o solo un conjunto de paquetes IP que atraviesan un punto de monitoreo. Dado que no se genera tráfico de prueba, las mediciones pasivas solo se pueden aplicar cuando el tráfico de interés ya está presente en la red [14].

   Los resultados de estas mediciones reflejan la experiencia del usuario final y son mucho más precisa que las mediciones activas, pero no tiene mucha acogida debido a que se manejan grandes volúmenes de datos, adicionalmente se considera que podría existir una violación a la confidencialidad de la información.
   Una de las aplicaciones más conocidas que hace uso de metodologías de medición pasiva es wireshark, la cual será abordada más adelante.

1.6. Herramientas de emulación y análisis de tráfico en redes SDWLAN

Una de las herramientas más utilizadas para experimentar sobre redes SDN son los entornos de emulación, ya que permite adelantar un desarrollo previo a la implementación de redes y estudiar su comportamiento a múltiples estímulos inducidos con intención, que intentar recrear diferentes escenarios de operación. Mininet-WiFi y wireshark son dos programas de computadora que se encargan de emulación de redes inalámbricas y análisis de tráfico, respectivamente, que tienen muy buena acogida en la comunidad investigativa a nivel mundial.

1.6.1. Mininet-WiFi

Mininet es un emulador de SDN de código abierto, diseñado para realizar pruebas en ambientes de investigación. Permite virtualizar host, conmutadores, controladores y enlaces cableados de red. Los hosts ejecutan software de red Linux estándar y los conmutadores admiten protocolo OpenFlow para el reenvio de paquetes. El software es desarrollado en gran porcentaje en Python, excepto por una pequeña porción que hace uso de lenguaje C [15].

Mininet-Wifi es una bifurcación de mininet que busca emular redes inalámbricas definidas por software. Se caracteriza por permitir el uso de aplicaciones de terceros sin modificación del código fuente y protocolos como IEEE 802.11x. El software hereda las capacidades de mininet y añade un driver[13] Wi-Fi denominado SoftMac.

El comportamiento de las redes inalámbricas, en las emulaciones, depende de la función que realizan, es decir, los AP y STA operan en modo maestro esclavo respectivamente, al igual que en un entorno real. Las STA se comunican con el AP mediante un proceso de autenticación y asociación.

De forma predeterminada, cada estación tiene una interfaz inalámbrica y pueden agregarse más si es necesario, adicionalmente pueden generar tráfico y comportarse como maquinas reales. Una vez conectadas al AP cada estación puede comunicarse con las demás estaciones asociadas a la red.

Los puntos de acceso funcionan como conmutadores SDN pero con la diferencia que posee interfaces Wi-Fi y son responsables de gestionar las estaciones asociadas a ellos.

1.6.1.1. Creación de topologías de red

La creación de topologías para Mininet-WiFi, por efecto se realizan mediante guiones escritos en Python, pero es posible realizarlos con la ayudad de interfaces gráficas de usuario (GUI, *Graphic User Interface*) como “Visual Network Descriptor” (VND[14]) y MiniEdit.

[13] Driver: componente de software que conecta un sistema operativo con el hardware de una máquina.
[14] VND*:* es un software con una interfaz gráfica, basada en web, utilizada para la creación de escenarios de red definidas por software.

- ✓ Visual Network Descriptor, VND: herramienta de software capaz de generar guiones en Python para Mininet-WiFi a través de un navegador web. Esta herramienta no viene dentro del paquete de instalación de Mininet-WiFi.
- ✓ MiniEdit: es una herramienta escrita en Python para mininet, pero con el tiempo se actualizó para ser usada en Mininet-WiFi, y viene incluida en su código fuente.

1.6.1.2. Modelos de propagación y movilidad

El software es capaz de emular las condiciones a las cuales puede estar expuesta una estación inalámbrica calculando la potencia de recepción de acuerdo con dos variables, las pérdidas de potencia en un determinado ambiente de propagación y la movilidad que pueda tener las STA dentro de un área de cobertura. Para el cálculo de las pérdidas de potencia de transmisión en el medio, se cuenta con cinco (5) modelos:

- ✓ Pérdidas por propagación en espacio libre (*Free Space Propagation Loss*): se utiliza para predecir la potencia recibida en una estación cuando existe una línea de vista directa entre el transmisor y el receptor, sin obstáculos cercanos que puedan afectar la propagación electromagnética de las señales de radio.
- ✓ Pérdidas por propagación en distancia logaritmica (*Log-Distance Propagation Loss*): de forma general este modelo es una extensión del modelo anterior, donde incluye a la ecuación variables que buscan evaluar escenarios más realistas por donde deba viajar una señal electromagnética, como son áreas urbanas, edificaciones, fabricas, etc.
- ✓ Pérdidas por propagación de dos rayos terrestres (*Two Ray Ground Propagation Loss*): el modelo de dos rayos de reflexión terrestre se basa en óptica geométrica, y considera tanto la transmisión directa como una componente de propagación reflejada en la tierra entre el transmisor y el receptor. Este modelo es muy usado en la evaluación de pérdidas de propagación en radioenlaces donde transmisor y el receptor de encuentra a alturas distintas.
- ✓ Pérdidas por propagación en sombreado logarítmico normal (*Log-Normal Shadowing Propagation Loss*): es un modelo aplicable a diseños de red desplegados al interior de un edificio. Calcula las pérdidas en la señal basado en la distancia del transmisor y el receptor, asumiendo que el entorno puede ser de tres tipos: visión directa, sin visión directa y separado de uno a tres pisos.
- ✓ Pérdidas por propagación propuesto por la Unión Internacional de Telecomunicaciones (ITU, *International Telecommunication Union*): es un modelo diseñado para el cálculo de la potencia recibida en una STA al interior

de un edificio. Los cálculos se realizan teniendo como base la sumatoria de las pérdidas que pudiese tener una señal por penetración de muros y pisos antes de llegar al receptor.

El patrón de movimiento de las estaciones es de suma importancia en el análisis del desempeño de las redes inalámbricas, Mininet-WiFi cuenta con 5 métodos, documentados, para modelar el comportamiento de los enlaces mientras una STA está en movimiento:

- ✓ Modelo de Movilidad de Caminata Aleatoria (RWM, *Random Walk Mobility*): en este modelo una STA se mueve desde una posición a una nueva posición con una dirección y velocidad aleatorias. Este modelo no tiene memoria es decir no se guardan registros de las posiciones donde estuvo y puede volver a estar en esa posición de forma indeterminada lo cual es poco realista, y por lo tanto, no coincide con aplicaciones de la vida real [16].
- ✓ Modelo de Movilidad de Punto de Ruta Aleatorio (RWPM, *Random WayPoint Mobility*): en este modelo una STA se mueve desde su posición a una nueva posición de manera aleatoria y se desplaza hacia ella con una velocidad constante, elegida de manera uniforme y aleatoria de entre un rango preestablecido. Cuando la STA llega a su destino se vuelve estacionaria por un tiempo, luego vuelve y elige otro destino y se mueve hacia allá, el proceso se repite hasta el final de la emulación. Este tipo de modelo es ampliamente aceptado por su simplicidad de implementación y análisis, sin embargo, presenta problemas de dependencia temporal, espacial y geográfica, es decir, la velocidad, patrón de movimiento y obstaculización de las estaciones puede verse influenciado y correlacionado con estaciones adyacentes [16].
- ✓ Modelo de Movilidad de Dirección Aleatoria (RDM, *Random Direction Mobility*): en este modelo una STA se mueve a una velocidad constante en una dirección aleatoria, hasta un límite, donde la STA queda inmóvil por un tiempo determinado, luego elige otra dirección y se mueve con una velocidad diferente. Este tipo de movimiento genera una distribución de STAs más estable en el área de cobertura del AP, en comparación al RWPMM [16].
- ✓ Modelo de Movilidad de Grupo de Punto de Referencia (RPGM, *Reference Point Group Mobility*): este modelo está diseñado para emular el comportamiento de grupos de estaciones al interior del área de cobertura de un AP, cada grupo tiene una estación líder la cual determina la ubicación, dirección y velocidad de movimiento para el grupo [16].
- ✓ Modelo de Movilidad *Gauss-Markov* (GMM, *Gauss-Markov Mobility*): en este modelo se le asigna a una STA una velocidad y dirección, e inicia su movimiento, luego de un tiempo, la STA recalcula su dirección y velocidad basado en sus parámetros anteriores, lo que reduce la posibilidad de cambios brucos de dirección y paradas inesperadas. El modelo incluye una variable de aleatoriedad en un marco de tiempo, cuanto menor sea este valor

mayor será el grado de aleatoriedad y en el caso contrario la respuesta será muy parecida al modelo de movilidad de punto de ruta aleatorio [17].

1.6.2. Wireshark

Los sniffers o capturadores de tráfico son herramientas de software utilizadas para capturar el tráfico que entra y sale por una interfaz de red, con el fin de ser analizado con posterioridad. La anterior definición implica que para lograr analizar el flujo de datos al interior de una red es necesario estructurar una topología en particular. La primera es la estructuración de un puerto espejo, aplicado a un conmutador o enrutador, es decir todos los paquetes dirigidos a un puerto tienen una copia a su puerto espejo, en esta última interfaz, se conecta el sniffer. La segunda requiere instalar el sniffer antes del enrutador que recibe la red a analizar. En la figura 10 se puede observar cómo serían las conexiones de las dos topologías.

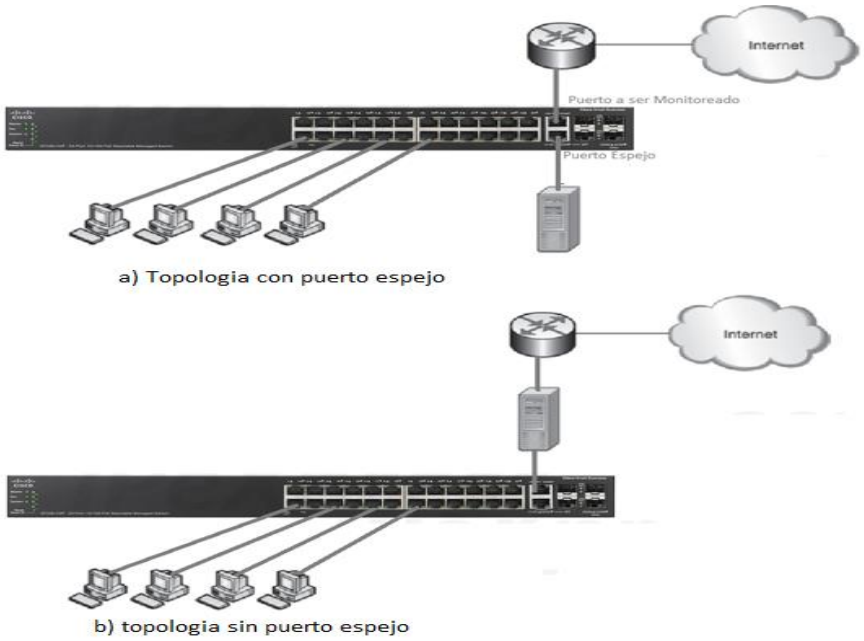


Figura 10: Topologías de red para el monitoreo de redes.

Wireshark es un software de análisis de tráfico que puede ser usado en infraestructuras cableadas o inalámbricas, que también sirve como herramienta para la solución de problemas de red. La aplicación toma cada paquete capturado y lo filtra de acuerdo con el protocolo al que pertenece y lo descompone conforme a su estructura (campos y subcampos) [18].

1.7. Hardware comercial para SDWLAN

En esta parte de la revisión documental, se referencian algunas marcas y modelos de dispositivos inalámbricos, comerciales en Colombia, que operan como puntos de acceso en redes tradicionales, pero poseen al interior de su sistema operativo un protocolo abierto para ser gestionados desde una controladora SDN.

Teniendo como entorno de función la gestión de una SDWLAN y siguiendo los estándares de IETF (RFC-5415 CAPWAP) y ONF (OpenFlow) la selección de un fabricante compatible con estas características tiene múltiples aristas como son:

a. Los protocolos antes mencionados son abiertos y estandarizados para la IEE802.11x, en el caso de CAPWAP, proveedores como Cisco, Aruba, Juniper, Fortinet y Ubiquiti, lo integra en su firmware y crean su plataforma de gestión privada con parámetros de asociación únicos en cada marca, lo que lo imposibilita para una operación multimarca con la misma controladora de código propietario. La integración de estos AP con una controladora de SDN de código abierto es posible si se hace a un lado las claves y métodos de encriptación.

b. Con el AP aprovisionado y asociado a la controladora es necesario controlar el tráfico, por ende, en un entorno SDN se requiere gestionar el tráfico mediante otro protocolo como OpenFlow que debe estar embebido en el firmware lo que reduce el mercado de dispositivos de conexión inalámbrica con esta caracterización.

Las posibilidades de gestionar uno o varios AP de forma centralizada están ligadas al firmware embebido en su hardware y su programabilidad la define el proveedor, pero existe una opción de cambiar el sistema operativo por uno con más flexibilidad y totalmente escribible con administración de paquetes; OpenWrt es un proyecto de software libre basado en linux con licencia GPL. Cuenta con dos tipos de interfaz de usuario, línea de comandos y WEB. La lista de marcas compatible se pueden encontrar en el siguiente link https://openwrt.org/es/toh/start, entre las más conocidas y comerciales se encuentra algunos modelos de *Mikrotik*, *Ubiquiti*, *Aruba, Cisco, DLink, Huawei, Linksys, Meraki, Raspberry*, etc [19].

CAPÍTULO II: DISEÑO DE SDWLAN EMPRESARIAL

La base funcional de una red inalámbrica empresarial responde a una estructura compuesta por dos capas, acceso y distribución, la primera la conforman múltiples puntos de acceso que propagan diferentes SSID, destinados a agrupar las STA, con el fin de permitir o denegar tráfico de red de acuerdo con el rol que se le asigna a cada terminal al momento de conectarse.

Las STA pueden movilizarse en el área de cobertura de diferentes AP y pasar de uno a otro sin perder la conexión o tener la necesidad de unirse a otro SSID, manteniendo siempre los mismos permisos asignados a la red de asociación. El aprovisionamiento IPv4 e IPv6 es independiente al AP al cual está asociado por lo cual es necesario la operación un servidor DHCP centralizado o la Configuración Automática de Dirección sin Estado (SLAAC, *StateLess Address Auto Configuration*) en el caso del protocolo de internet versión 6.

La capa de distribución hace referencia a la infraestructura de red que permite a las solicitudes de las STA llegar a su destino al interior de la red o hacia otras redes en Internet, por diferentes rutas teniendo en cuenta características como la distancia más corta, el camino con mejor eficiencia de ancho de banda y/o prioridad para el servicio requerido.

Partiendo de la caracterización anteriormente descrita como requerimientos de diseño se define un escenario de red empresarial a emular, figura 11.

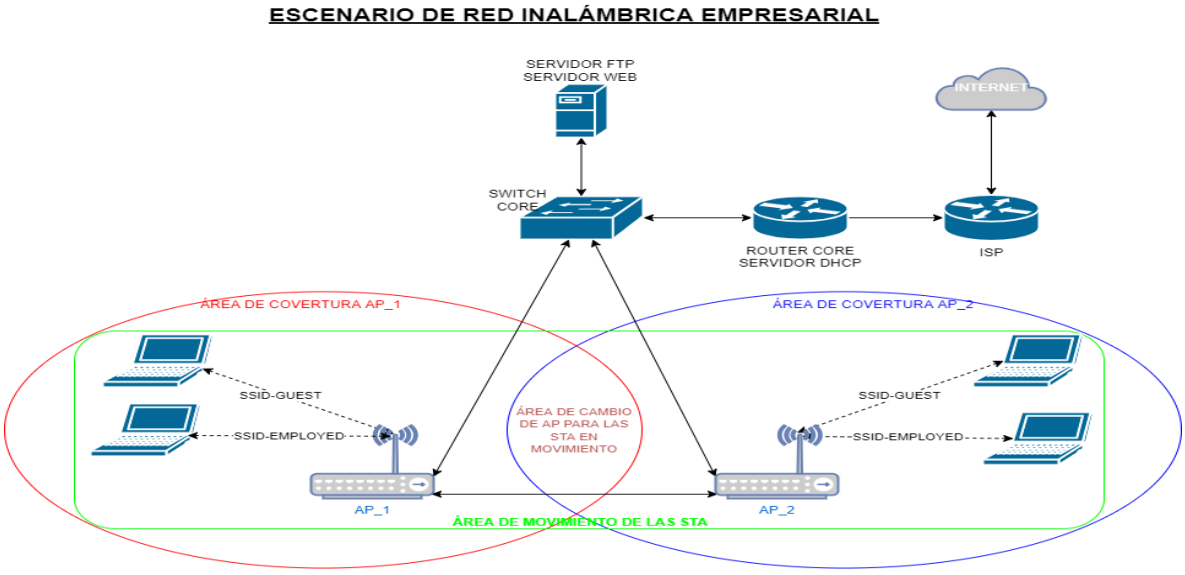


Figura 11: Topología de red empresarial donde converge la red LAN y la WLAN.

2.1. Diseño de red SDWLAN

Transmutar el modelo de red mostrado en la figura 11 en una SDWLAN requiere descomponerlo en elementos que puedan ser ubicados dentro de las tres capas de la arquitectura SDN, cabe tener en cuenta que los dispositivos que operan como enrutadores (“Router_Core” e “ISP”) juegan un papel importante para el diseño a tratar en el presente proyecto, pero no hacen parte de los dispositivos sensibles a protocolos *southbound* o *northbound*.

a. Capa de control: el corazón de una red definida por software es la controladora, que para el diseño en cuestión es ONOS. Fue elegido por su alta compatibilidad con “OpenFlow”, “YANG-NETCONF”, “REST API” y sus las cualidades a nivel de interfaz gráfica y línea de comandos al momento de monitorear flujos de datos, dispositivos de red, estaciones de trabajo y control de tráfico. Adicionalmente tiene una gran comunidad de colaboradores con una amplia bibliografía en *GitHub*.

b. Capa de infraestructura: en este nivel se ubican los dispositivos de red encargados de la conmutación y encaminamiento de paquetes, que para el caso son los dos AP (“AP_1” y “AP_2”) y un conmutador (“Switch_Core”). Se establece OpenFlow y YANG-NETCONF como el protocolo southbound, dado que son interfaces abiertas, compatible con mininet e incluida en el sistema operativo de los routers mikrotik y OpenWrt.

c. Capa de aplicaciones: el requerimiento de diseño para este proyecto a nivel de aplicaciones se centra en software que permita el aprovisionamiento de direccionamiento IPv4/IPv6 en las STA, control de tráfico, enrutamiento IP, lectura de parámetros inalámbricos y control de acceso en los AP. Este es el nivel de mayor exigencia para la formulación de la topología de red, ya que es necesario conocer la forma de operar de las aplicaciones a usar como se menciona a continuación:

   - ✓ Servidor DHCP: dentro de la suite de ONOS se encuentra un programa que funciona como servidor de solicitudes de STA para obtener parámetros de red como dirección IPv4, máscara, DNS y una puerta de enlace.
   - ✓ Anuncio de enrutador IPv6: proporcionar parámetros de direccionamiento IPv6 en las STA se realiza a través de la aplicación “*Router*

Advertisement" la cual habilita funcionalidades de Mensaje de Solicitud de Router[15], RS y Mensaje de Anuncio de Router[16], RA.

- ✓ Enrutamiento IP: esta actividad es realizada por un protocolo de Enrutamiento Reactivo (RR, *Reactive Routing*) que opera con un software denominada "SDN-IP", cuya base funcional es dada por un "iBGP Speaker" encargado de anunciar información de enrutamiento.
- ✓ Control de tráfico de datos: ONOS posee un subsistema que permite establecer comunicaciones, entre estaciones, de acuerdo a flujos de datos definidos en forma de política y no como un mecanismo de enrutamiento o lista de control de acceso, denominado Intención (*Intent*).
- ✓ Lectura de parámetros inalámbricos y control de acceso a los AP: la lectura y configuración remota de las AP no se puede realizar mediante el protocolo CAPWAP dado que no es un protocolo que se encuentra entre las librerías de la controladora ONOS, pero si admite el protocolo NETCONF, con el que es necesario instalar un agente en el AP y permita su gestión desde la controladora.

2.2. Topología SDWLAN

El esquema de red que se trata en el proyecto se muestra en la figura 12, la cual refleja una controladora que establece comunicación con los dos AP, el conmutador OpenFlow y el enrutador *iBGP-Speaker* a través de un conmutador tradicional, donde cada uno de los elementos posee una dirección IPv4 del mismo segmento, informándole a ONOS cuales son los dispositivos activos presentes. Cada uno de los componentes incluidos en la figura 12 uno se describe a continuación:

a. Enrutador *iBGP-Speaker*: este dispositivo es un enrutador tradicional que se encarga de informarle a ONOS que él es la puerta de enlace para la computadora que emula un servidor y las STA inalámbricas, enruta el tráfico de un equipo a otro (al interior de la red o hacia internet) si existe intención de establecer flujo de datos especifico o general.

b. Enrutador ISP: este elemento de red proporciona la salida a internet a través de un operador de red comercial.

[15] Mensaje de solicitud de router, RS: mensaje propio del protocolo ICMPv6 definido para el descubrimiento de vecinos enfocado a obtener la información de direccionamiento de forma automática mediante SLAAC.
[16] Mensaje de anuncio de router, RA: mensaje propio del protocolo ICMPv6 destinado a anunciar parámetros como prefijo y duración del mismo, a las STA que lo soliciten.

c. Conmutador OpenFlow: dispositivo encargado conmutar el flujo de datos desde los AP, hacia la computadora que emula un servidor y enrutador *iBGP-Speaker*.

d. Puntos de Acceso: componente de red SDN encargado de establecer las conexiones inalámbricas de las STA, a los cuales tienen dos rutas físicas hacia el servidor y enrutador iBGP. Propagan dos SSID denominados “Empleados” e “Invitados”, y las terminales que posean una interfaz inalámbrica pueden asociarse a una o la otra conociendo la contraseña adecuada. La seguridad a nivel de control de acceso es de tipo WPA2.

e. Computadora que emula un servidor: estación de trabajo que simula un servidor WEB, no tiene ninguna función aparte de responder a las peticiones que las STA realizan a los del puerto 80 e ICMP.

Esta topología requiere de un direccionamiento IP que haga posible llevarla a un ambiente emulado o real, y es descrito en la tabla 5, cabe aclarar que existen 4 tipos de segmentos de red, uno para la capa de control (10.10.10.0/24) y los otro 3 para la capa de datos (192.168.100.0/24, 192.168.200.0/24 y 2800:484:2383:16de::/120).

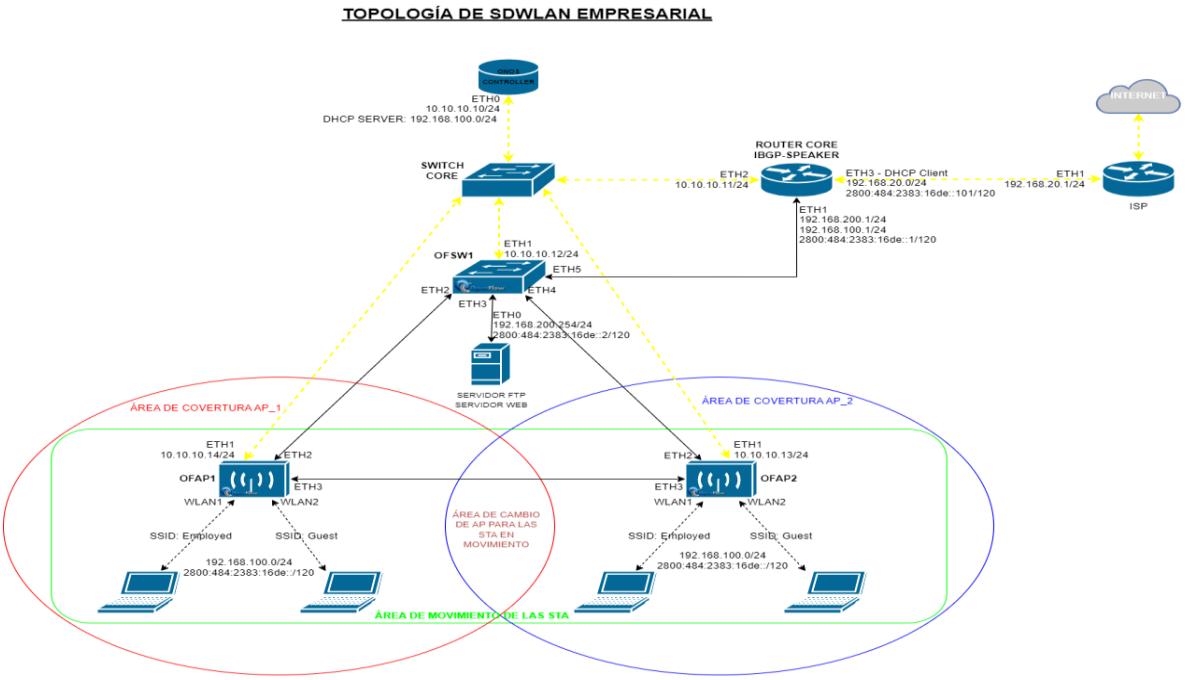


Figura 12: Topología SDWLAN para el proyecto en curso.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	PUERTA DE ENLACE
Router core	ETH1	192.168.100.1/24	N/A
		2800:484:2383:16de::1/120	N/A
		192.168.200.1/24	N/A
	ETH2	10.10.10.11/24	N/A
	ETH3	DHCP Client	192.168.20.1
OFAP1	ETH1	10.10.10.14/24	N/A
	WLAN2	192.168.100.1/24	N/A
	WLAN3		
OFAP2	ETH1	10.10.10.13/24	N/A
	WLAN2	192.168.100.1/24	N/A
	WLAN3		
OFSW1	ETH1	10.10.10.12/24	N/A
	ETH3	192.168.200.1/24	N/A
Servidor	ETH0	192.168.200.254/24	192.168.200.1
		2800:484:2383:16de::2/120	2800:484:2383:16de::1/120
ONOS	ETH0	10.10.10.10/24	N/A

Tabla 5:Direccionamiento IP para la red SDWLAN

2.3. Emulación

Esta parte del proyecto se realiza en dos formas, con finalidades diferentes, la primera se desarrolla haciendo uso del software Mininet-WiFi, su objetivo primordial es evaluar el comportamiento de la controladora SDN y la interfaz gráfica cuando las STA asociadas a un AP se mueven dentro de su área de cobertura y al momento de realizar el "handover" al otro AP. La segunda parte reproduce el diseño SDWLAN con equipos reales de uso comercial, marca *Mikrotik,* tratando de emular la operación inalámbrica una red empresarial a gran escala, y busca evaluar los siguientes temas:

- ✓ Aprovisionamiento IPv4/IPv6 de las STA
- ✓ Enrutamiento interno, salida a internet y priorización de tráfico
- ✓ Balanceo de datos sobre los dos enlaces que tiene cada AP
- ✓ Interfaz gráfica de monitoreo de la controladora
- ✓ Gestión de parámetros inalámbricos en los AP

2.3.1. Controladora ONOS

Para los dos escenarios de emulación se establece la instalación de la controladora ONOS en su versión 2.5.1, sobre un sistema operativo linux (Lubuntu 18.04 LTS) cuyo proceso de virtualización e instalación se describe en el anexo 1.

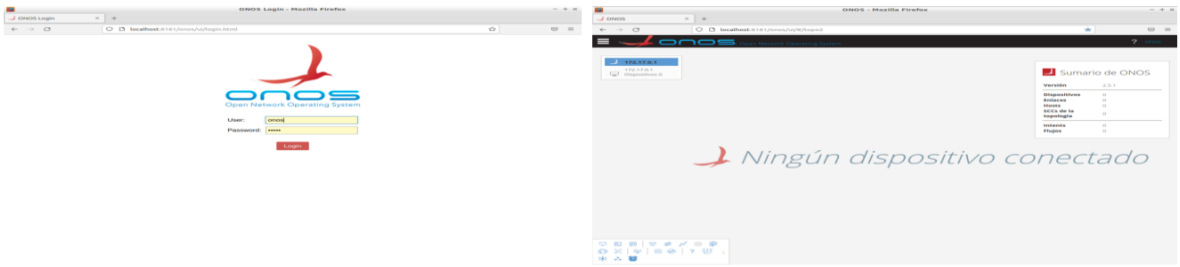


Figura 13: Interfaz gráfica de ONOS.

ONOS cuenta con una amplia gama de aplicaciones preinstaladas, pero en un estado inicial desactivadas. Para los dos escenarios a emular se presentan algunas librerías en común listadas en la tabla 6.

DESCRIPCIÓN	APLICACIÓN	APLICACIÓN RELACIONADA
Interfaz gráfica	org.onosproject.gui2	
Controladores por defecto	org.onosproject.drivers	
Suite OpenFlow	org.onosproject.openflow	org.onosproject.hostprovider
		org.onosproject.ldpprovider
		org.onosproject.openflow-baser
		org.onosproject.optical-model
Enrutamiento ARP[17]	org.onosproject.proxyarp	
Proveedor NETCONF	org.onosproject.netconf	org.onosproject.faultmanagement
Controladores NETCONF	org.onosproject.drivers.netconf	
Movilidad para flujo de datos	org.onosproject.mobility	

Tabla 6: Aplicaciones de ONOS preinstaladas y habilitadas para la emulación del escenario SDWLAN.

La activación de cada aplicación puede realizarse desde la interfaz gráfica o por la línea de comandos, como se muestra en la figura 14.

[17] ARP, Protocolo de Resolución de Aplicaciones encargado de establecer la relación de la dirección IP y la MAC de una interfaz de red.

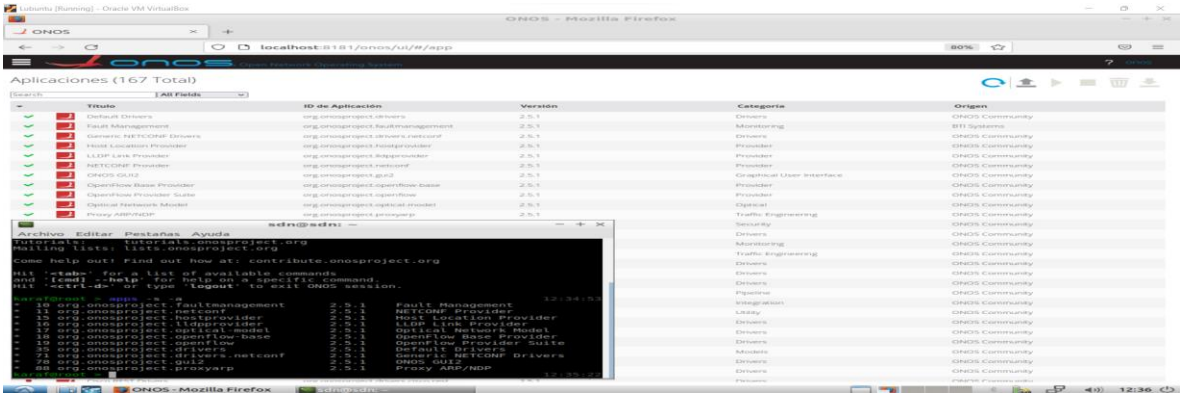


Figura 14: Activación de aplicaciones southbound y northbound desde líneas de comando e interfaz gráfica.

Estas aplicaciones no requieren de una configuración especifica o intervención del administrador de red, ya que definen su operación de forma automática por las conexiones físicas de los dispositivos de acuerdo con la información que se obtiene mediante el protocolo OpenFlow al momento de la asociación con la controladora, excepto cuando se hace uso de la aplicación NETCONF ya que esta requiere de una configuración inicial.

Las instrucciones de operación para los REST API de ONOS son impartidas en notación de objetos de JavaScript (JSON, *JavaScript Object Notation*) y está definida como la forma de configurar las aplicaciones northbound; la interfaz gráfica de la controladora permite introducir estos scripts, como se puede observar en la figura 15. Ingresando a la url "http://localhost:8181/onos/v1/docs/", en la opción "/network/configuration" es posible definir dispositivos, enlaces, puertos, estaciones de trabajo, entre otros.

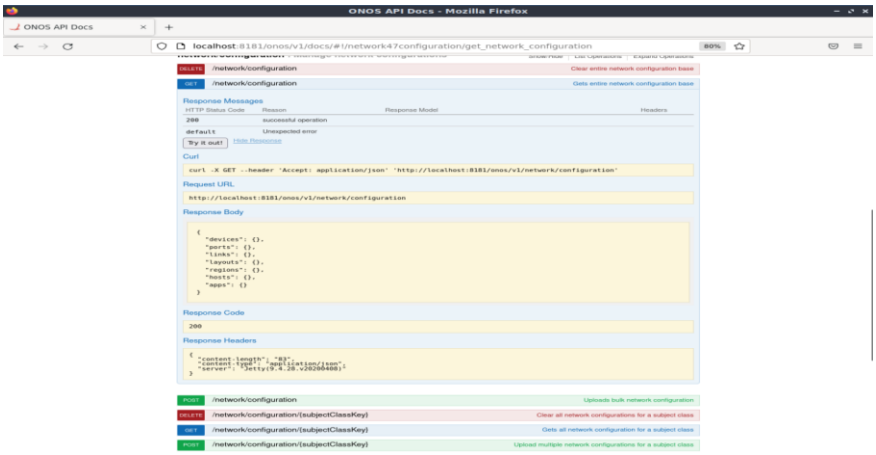


Figura 15: Configuración de aplicaciones mediante REST API.

2.3.2. Emulación con Mininet-WiFi

La administración de redes inalámbricas embebidas en ambientes empresariales contemplan, entre otros aspectos, la necesidad de conocer las STA asociadas a los puntos de acceso y el “handover” entre AP desde una consola centralizada; por ende se propone un modelo de emulación basado en la topología SDWLAN anteriormente planteada, haciendo uso del software Mininet-WiFi desplegado sobre los recursos de una máquina virtual y un sistema operativo linux, Lubuntu 18.04 LTS (el proceso de instalación se expone en el anexo 1), con el fin evaluar estas características en una red definida por software.

El inicio del proceso de emulación es llevar el modelo de red a líneas de código de programación en lenguaje python, esto se obtiene con la herramienta “Miniedit”, integrada en las librerías de Mininet-WiFi, de donde se genera la topología y a su vez es posible emularla, pero no es viable aprovechar al máximo las cualidades del software, por lo cual se genera el código base desde miniedit pero se completa con un editor de texto como se apreciar en la figura 16 y 17.

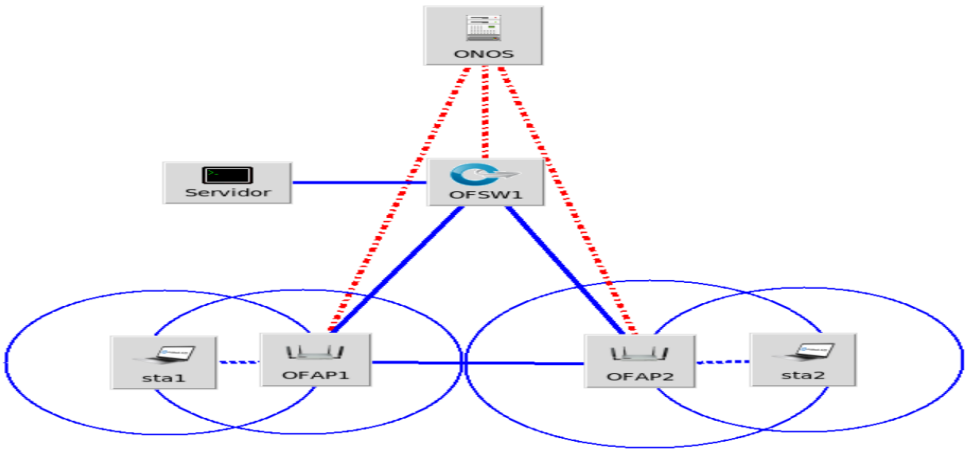
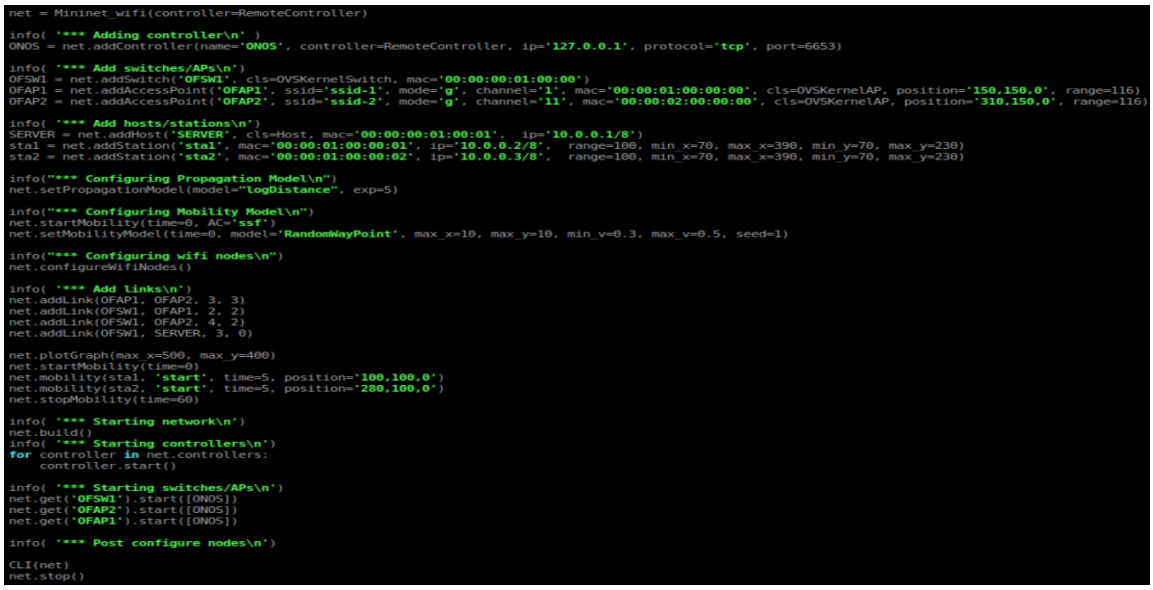


Figura 16: Topología de red generada en miniedit.



```
net = Mininet_wifi(controller=RemoteController)

info( '*** Adding controller\n' )
ONOS = net.addController(name='ONOS', controller=RemoteController, ip='127.0.0.1', protocol='tcp', port=6653)

info( '*** Add switches/APs\n')
OFSW1 = net.addSwitch('OFSW1', cls=OVSKernelSwitch, mac='00:00:00:01:00:00')
OFAP1 = net.addAccessPoint('OFAP1', ssid='ssid-1', mode='g', channel='1', mac='00:00:01:00:00:00', cls=OVSKernelAP, position='150,150,0', range=116)
OFAP2 = net.addAccessPoint('OFAP2', ssid='ssid-2', mode='g', channel='11', mac='00:00:02:00:00:00', cls=OVSKernelAP, position='310,150,0', range=116)

info( '*** Add hosts/stations\n')
SERVER = net.addHost('SERVER', cls=Host, mac='00:00:00:01:00:01',  ip='10.0.0.1/8')
sta1 = net.addStation('sta1', mac='00:00:01:00:00:01', ip='10.0.0.2/8',  range=100, min_x=70, max_x=390, min_y=70, max_y=230)
sta2 = net.addStation('sta2', mac='00:00:01:00:00:02', ip='10.0.0.3/8',  range=100, min_x=70, max_x=390, min_y=70, max_y=230)

info("*** Configuring Propagation Model\n")
net.setPropagationModel(model="logDistance", exp=5)

info("*** Configuring Mobility Model\n")
net.startMobility(time=0, AC='ssf')
net.setMobilityModel(time=0, model='RandomWayPoint', max_x=10, max_y=10, min_v=0.3, max_v=0.5, seed=1)

info("*** Configuring wifi nodes\n")
net.configureWifiNodes()

info( '*** Add links\n')
net.addLink(OFAP1, OFAP2, 3, 3)
net.addLink(OFSW1, OFAP1, 2, 2)
net.addLink(OFSW1, OFAP2, 4, 2)
net.addLink(OFSW1, SERVER, 3, 0)

net.plotGraph(max_x=500, max_y=400)
net.startMobility(time=0)
net.mobility(sta1, 'start', time=5, position='100,100,0')
net.mobility(sta2, 'start', time=5, position='280,100,0')
net.stopMobility(time=60)

info( '*** Starting network\n')
net.build()
info( '*** Starting controllers\n')
for controller in net.controllers:
    controller.start()

info( '*** Starting switches/APs\n')
net.get('OFSW1').start([ONOS])
net.get('OFAP2').start([ONOS])
net.get('OFAP1').start([ONOS])

info( '*** Post configure nodes\n')

CLI(net)
net.stop()
```

Figura 17: topología de red en lenguaje python.

La figura 17 expresa dos AP que operan dentro de un entorno SDN mediante el protocolo OpenFlow, que propagan un diferente SSID dentro de un área de cobertura circular con un radio de 116m, siguiendo el modelo de estimación de pérdidas de propagación "*log-distance*". La ubicación de estos dispositivos se dispone de tal forma que exista un espacio rectangular de 320m de largo por 160m de alto, en donde se pueden mover las STA sin perder conexión. Las STA se configuran con un alcance de señal de 100m, cuyo mecanismo de asociación se establece de acuerdo con la señal más fuerte y su movilidad sigue el modelo de punto de caminata aleatoria (*Random Way Point*). Para este primer escenario de emulación no es necesario sistemas de autenticación y control de acceso a la red, por lo cual no se tiene en cuenta.

Terminando el proceso de construcción de la topología de red en Mininet-WiFi es necesario adecuar la controladora, activando la aplicación "org.onosproject.fwd"; causal de la comunicación IP de todas las estaciones de trabajo que están dentro del segmento de red "10.0.0.0/8", determinado por defecto en Mininet-WiFi.

Haciendo uso de REST API se define la ubicación y nombre de los dispositivos activos de red, esto último responde a las líneas de código presentes en la figura 18:

```
devices : {
    "of:0000000000000001" : {
        "basic" : {
            "name" : "OFSW1",
            "locType" : "grid",
            "gridX" : 500,
            "gridY" :500
        }
    },
    "of:1000000000000001" : {
        "basic" : {
            "name" : "OFAP1",
            "locType" : "grid",
            "gridX" : 200,
            "gridY" :650
        }
    },
    "of:1000000000000002" : {
        "basic" : {
            "name" : "OFAP2",
            "locType" : "grid",
            "gridX" : 800,
            "gridY" :650
        }
    }
}

"hosts" : {
    "00:00:00:01:00:01/-1" : {
        "basic" : {
            "name" : "SERVIDOR",
            "locations" : ["of:0000000000000001/3"]
        }
    }
}
```

Figura 18: Asignación de nombre y ubicación de los dispositivos de red para la interfaz gráfica de ONOS.

2.3.2.1. Escenario de pruebas para Mininet-WiFi

El ambiente de pruebas aplicadas al escenario de emulación desarrollado con Mininet-WiFi y la controladora ONOS destaca dos aspectos, donde para cada uno de ellos se definen unas preguntas que ayudan a enfatizar los puntos de inflexión a evaluar que no son evidentes en las condiciones iniciales de experimentación:

a. Descubrimiento automático de los dispositivos de red y STA por parte de la controladora: como se muestra en la figura 19 la interfaz gráfica de la controladora detecta, de forma inmediata, los AP, el conmutador, los enlaces cableados y las STA, pero es necesario dar respuesta a las siguientes preguntas:

   - ✓ Durante el movimiento de una STA entre un AP y otro ¿cómo es la respuesta en la interfaz gráfica?
   - ✓ ¿Qué sucede con los enlaces inalámbricos y los flujos preestablecidos, si uno o ambos enlaces cableados en los AP se desconectan?

- ✓ Si una STA renuncia a la asociación con los AP, ¿cómo es el comportamiento de la controladora?
- ✓ ¿Qué información histórica y en tiempo real se puede obtener de las STA asociadas?

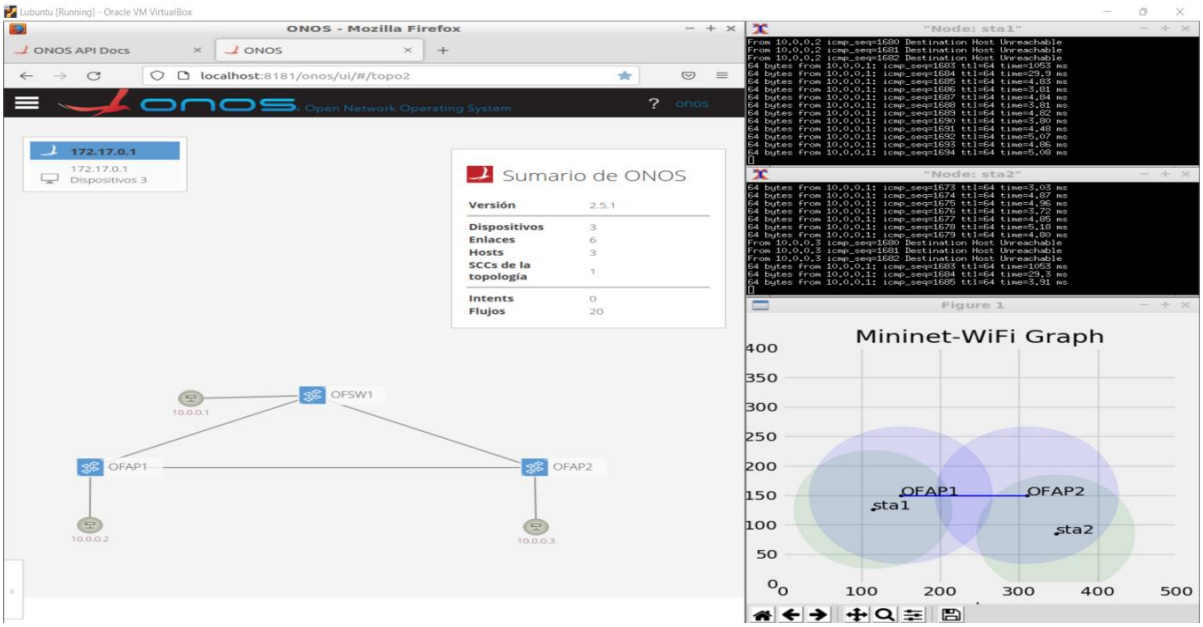


Figura 19: Topología de red corriendo desde Mininet-WiFi.

b. Evaluación de métricas de desempeño (Latencia, pérdida de paquetes y ancho de banda) entre estaciones de trabajo: dado el movimiento constante y cambio de AP de las STA es necesario evaluar el desempeño de las comunicaciones entre estas y la estación conectada de forma cableada; con el fin de observar y evaluar el rendimiento de la arquitectura SDWLAN diseñada, para lo que se estructura un esquema de interrogantes definidos a continuación:

- ✓ ¿La interfaz gráfica de ONOS permite observar parámetros de desempeño de los enlaces alámbricos e inalámbricos?
- ✓ ¿Las variaciones en la latencia y ancho de banda dentro la comunicación de las STA inalámbricas y la STA cableada, refleja la distancia entre ellas?
- ✓ ¿Durante el handover existen pérdida de paquetes?

- ✓ ¿Como es el comportamiento del flujo de datos (balanceo de cargas) entre una STA inalámbrica y la STA cableada durante la caída de una de las dos rutas definidas para cada punto de acceso?

2.3.3. Emulación y escenario de pruebas con equipos reales

SDN tienen como ventaja arquitectónica la posibilidad de establecer una red basada en intenciones, es decir redes que aprenden y se adaptan constantemente, centrándose en políticas de servicio definiendo un marco de operación de la red en función de lo que se espera de ella. El proceso de adaptación y optimización de servicios responden a un ciclo de retroalimentación constante, siguiendo los siguientes pasos jerárquicos [7].

a. Ubicación de los dispositivos de red donde es necesario realizar configuración para levantar un servicio o petición de comunicación, es decir el mapeo de la topología de red. En el caso de la topología SDWLAN a trabajar los dispositivos son los AP, el conmutador Openflow y estaciones de trabajo.

b. El siguiente paso es la automatización y centralización de las solicitudes de conexión de las STA a un servicio específico y administración de los AP, desde una controladora.

c. La tercera fase es el monitoreo, con telemetría, del estado de la red, donde se pueda observar fallas y cambios de configuración.

d. Por último, se analiza los datos obtenidos en la tercera fase y se evalúa su impacto en el servicio, se aísla el problema y se establece una solución.

Teniendo en cuenta el diseño de redes basado en intenciones, anteriormente descrito, para dar cumplimiento a los objetivos del proyecto existen dos servicios fundamentales, el primero es la gestión de los AP y conmutador, siguiendo una línea de actividades como son: preaprovisionamiento, sin el cual los dispositivos no podrán conectarse a la red y la comunicación de los protocolos OpenFlow y NETCONF no operarían, posteriormente, se debe garantizar un mecanismo de acceso, lectura y control de parámetros en los AP como frecuencia de transmisión, SSID y control de acceso, esto último se desarrolla desde una Interfaz de línea de comandos (CLI, *Command Line Interface*) de ONOS. Terminado este proceso las STA podrán asociarse conociendo las contraseñas de cada SSID y se le es asignada una dirección IPv4 e IPv6, una dirección de puerta de enlace y DNS.

El segundo servicio es garantizar la comunicación desde las STA que se asocian a los SSID de empleados hacia internet (puerto 80 y 443) y el servidor interno (puertos 21, 22 e ICMP), y los asociados al SSID de invitados solo tengan acceso a Internet.

2.3.3.1. Infraestructura de red

La implementación de la topología SDWLAN empresarial propuesta se realiza haciendo uso de un conmutador D-Link modelo DES-1008A, encargado de comunicar la controladora ONOS y cuatro enrutadores marca Mikrotik, dos de estos cumplen las funciones de punto de acceso inalámbrico en la banda de los 2.4GHz, el tercer mikrotik se encarga de cumplir las funciones de conmutador OpenFlow y el cuarto es el IBGP speaker. La conectividad de estos equipos se puede observar en la figura 20.

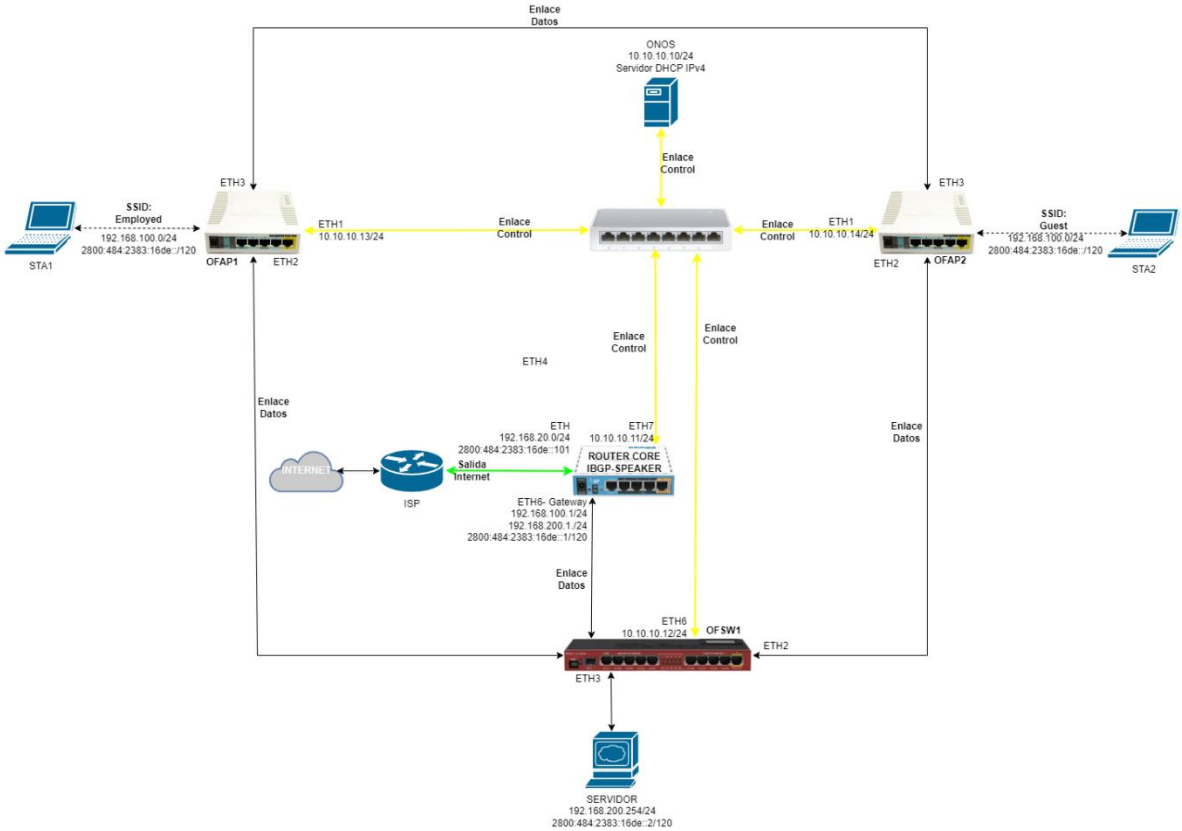


Figura 20: Topología de red para emulación con equipos reales.

Los dos enrutadores que operan como puntos de acceso y el conmutador OpenFlow se les debe cambiar el sistema operativo anfitrión a OpenWrt (el proceso de instalación y alistamiento de paquetes se puede apreciar en el anexo 2), es

importante aclarar la paquetería adicional hace referencia a OpenVSwitch[18], Netopeer2-Server[19] y un modelo YANG de código abierto aplicado a interfaces inalámbricas (*terastream-wireless*), por lo cual es de relevancia verificar sus características físicas y compatibilidad del firmware a instalar, como se puede observar en la tabla 7 y figura 21.

MODELO DE ENRRUTADOR	CPU	N° DE NUCLEOS	FRECUENCIA DE CPU	RAM	TAMAÑO ALMACENAMIENTO
RB951-2nD-TC	AR9344	1	600MHz	128	NAND 128MB
RB2011UAS-2HnD-IN	AR9349	1	600MHz	128	NAND 128MB

Tabla 7: Características de los routers mikrotik. Fuente: https://mikrotik.com

Figura 21: versión de firmware OpenWrt disponible para los AP mikrotik. Fuente: https://openwrt.org/toh/start

El router que opera como "IBGP Speaker" mantiene su sistema operativo mikrotik en la versión 6.49.7, tan solo se le realiza la programación adecuada para su operación, la cual se puede observar en el anexo 2.

2.3.3.2. Preaprovisionamiento de conmutador y puntos de acceso

La preparación de los equipos se inicia con la asignación de una contraseña para el acceso desde SSH y la interfaz gráfica, un nombre, dirección IP para el control y la configuración de la ubicación de la controladora ONOS y puerto de escucha, tal como se muestra en la tabla 8. (El proceso se puede observar de forma más detallada en el anexo 2)

NOMBRE	IP DE CONTROL	IP CONTROLADORA
OFSW1	10.10.10.12	10.10.10.10
OFAP1	10.10.10.14	
OFAP2	10.10.10.13	

Tabla 8: Asignación de nombres y direccionamiento IP de control.

Como parte del alistamiento corresponde la configuración de las interfaces inalámbricas de los AP (El proceso se puede observar de forma más detallada en el anexo 2), pero estos dispositivos tienen la particularidad de poseer solo una interfaz física de este tipo y el requerimiento de la topología responde a la disipación de dos SSID, uno para empleados y otro para visitantes, por lo cual sobre la misma

[18] OpenVswitch: software de código abierto diseñado para establecer un conmutador virtual que responde al protocolo de comunicación OpenFlow.
[19] Netopeer2-Server: son un conjunto de herramientas NETCONF basadas en la librería "libnetconf" que permiten conectarse a un dispositivo de red y obtener su control, es decir, es el agente NETCONF instalado en los AP.

interfaz se crean los dos SSID lo cual implica que deben compartir la misma frecuencia y ancho de canal, tal como se muestra en la figura 22.

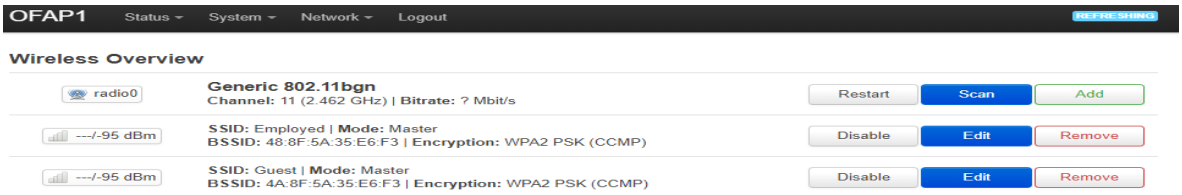


Figura 22: SSID dispersados por los puntos de acceso inalámbricos.

2.3.3.3. Configuración básica de la controladora ONOS

La configuración de la controladora ONOS que permitiría cumplir con los objetivos del proyecto para esta parte de la emulación la componen tres procedimientos, el primero es una base proporcionada mediante REST API y está compuesta por 4 apartes:

a) Dispositivos: esta parametrización asigna un nombre, su ubicación dentro de la interfaz gráfica de ONOS y la designación de los AP como "*Router Advertisement*", a estos últimos se adiciona el acceso SSH al protocolo NETCONF tipo cliente-servidor, donde el cliente es la controladora y los servidores son los puntos de acceso. La configuración se puede observar en la figura 23.

Figura 23: Configuración de equipos OpenFlow.

b) Puertos: esta parametrización asigna a las interfaces físicas donde se conecta el servidor y las STA la dirección IP de su puerta de enlace, y la

dirección MAC donde la pueden encontrar (IBGP-SPEAKER). La configuración se puede observar en la figura 24.


```
ports : {
    "of:0000d4ca6d991d7e/2" : {
        "interfaces" : [
        {
            "name" : "OFSW2-2",
            "ips" : ["192.168.200.1/24", "2800:484:2383:16de::1/120"],
            "mac" : "64:D1:54:32:44:F6"
        }
        ]
    },
    "of:0000488f5a35e6e9/5" : {
        "interfaces" : [
        {
            "name" : "OFAP1-5",
            "ips" : ["192.168.100.1/24", "2800:484:2383:16de::1/120"],
            "mac" : "64:D1:54:32:44:F6"
        }
        ]
    },
    "of:0000488f5a35e6e9/6" : {
        "interfaces" : [
        {
            "name" : "OFAP1-6",
            "ips" : ["192.168.100.1/24", "2800:484:2383:16de::1/120"],
            "mac" : "64:D1:54:32:44:F6"
        }
        ]
    },
    "of:000064d154f817e8/5" : {
        "interfaces" : [
        {
            "name" : "OFAP2-5",
            "ips" : ["192.168.100.1/24", "2800:484:2383:16de::1/120"],
            "mac" : "64:D1:54:32:44:F6"
        }
        ]
    },
    "of:000064d154f817e8/6" : {
        "interfaces" : [
        {
            "name" : "OFAP2-6",
            "ips" : ["192.168.100.1/24", "2800:484:2383:16de::1/120"],
            "mac" : "64:D1:54:32:44:F6"
        }
        ]
    }
}
```


Figura 24: Configuración de puertos.

c) Hosts: esta parametrización asigna un nombre al equipo que cumple las funciones de servidor dentro de la controladora ONOS y su conexión en el conmutador Openflow. La configuración se puede observar en la figura 25.


```
"hosts" : {
    "B8:AC:6F:67:B2:2D/-1" : {
        "basic" : {
            "name" : "Servidor",
            "locations" : ["of:0000d4ca6d991d7e/2"]
        }
    }
}
```


Figura 25: Configuración del servidor en ONOS.

d) Aplicaciones: esta parametrización define a la controladora ONOS como servidor DHCP IPv4 para la red inalámbrica mediante la aplicación “org.onosproject.dhcp” y la configuración del servicio de enrutamiento interno realizado por otra aplicación propia de la controladora como es “org.onosproject.reactive.routing”. La configuración se puede observar en la figura 26.

```
"apps": {
    "org.onosproject.reactive.routing" : {
        "reactiveRouting" : {
            "ip4LocalPrefixes" : [
                {
                    "ipPrefix" : "192.168.100.0/24",
                    "type" : "PRIVATE",
                    "gateway" : "192.168.100.1"
                }
            ],
            "ip4LocalPrefixes" : [
                {
                    "ipPrefix" : "192.168.200.0/24",
                    "type" : "PRIVATE",
                    "gateway" : "192.168.200.1"
                }
            ],
            "ip6LocalPrefixes" : [
                {
                    "ipPrefix" : "2800:484:2383:16de::/120",
                    "type" : "PRIVATE",
                    "gateway" : "2800:484:2383:16de::1"
                }
            ],
            "virtualGatewayMacAddress" : "64:D1:54:32:44:F6"
        }
    },
    "org.onosproject.dhcp" : {
      "dhcp" : {
        "ip": "10.10.10.10",
        "mac": "08:00:27:d2:32:ab",
        "subnet": "255.255.255.0",
        "broadcast": "10.10.10.255",
        "router": "192.168.100.1",
        "domain": "8.8.8.8",
        "ttl": "63",
        "lease": "100",
        "renew": "150",
        "rebind": "200",
        "delay": "2",
        "timeout": "150",
        "startip": "192.168.100.10",
        "endip": "192.168.100.254"
      }
    }
}
```


Figura 26: Configuración de aplicaciones ONOS.

En la figura 27 se puede apreciar como la interfaz gráfica de ONOS toma el arreglo expuesto en esta primera parte de la configuración. Se observa la topología SDWLAN gestionada por el protocolo OpenFlow, los dos AP que reportan por NETCONF, el servidor con su direccionamiento IPv4 e IPv6, el puerto del router iBGP que posee la puerta de enlace para dada segmento de red en la capa de datos y una STA asociada al SSID de empleados que en adelante será llamado “STA_E”.

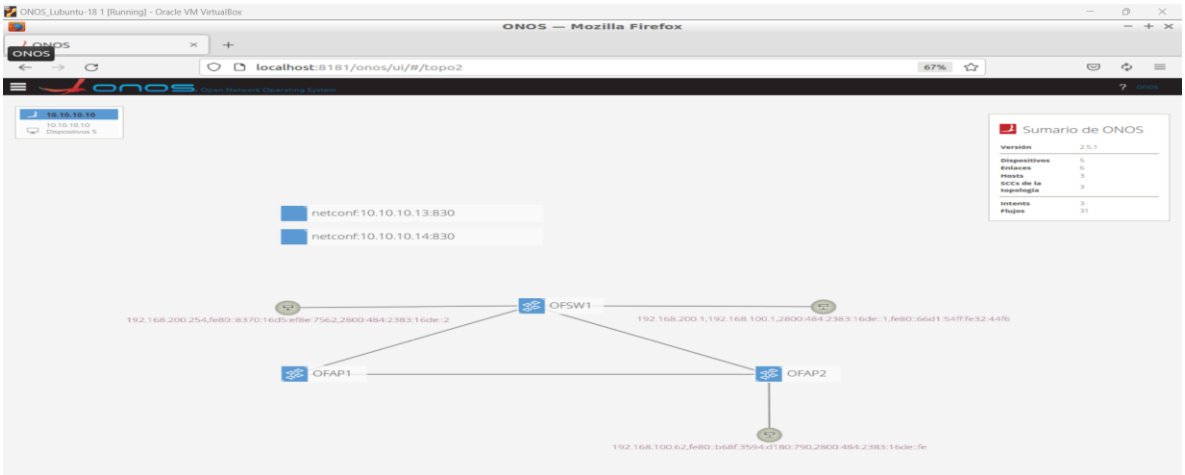


Figura 27: Presentación de la configuración de la controladora ONOS con equipos reales.

El segundo procedimiento está determinado como el establecimiento de políticas de comunicación definidas por intenciones para cada STA que se asocia a los SSID propagados. Es importante aclarar que el direccionamiento IP asignado por el servidor DHCP o el "*Router Advertisement*" no cobra relevancia hasta el momento que se defina una política de conexión entre las la estación de trabajo y su puerta de enlace (para la salida a internet) y/o el servidor (para la comunicación interna), con parámetros claros que pueden ser una o varias opciones como son, protocolo TCP, dirección IP, ancho de banda, interface física y prioridad, pero siempre definiendo el identificador de origen y destino que es la dirección MAC ya sea del puerto de un dispositivo de red o una STA; esta es la razón por la que solo hay un segmento de red para el SSID de Empleado e Invitados.

La comunicación entre terminales es verificada con la creación de 3 intenciones, como se muestra en las figura 28, 29 y 30, sin determinar puertos o servicios en específico:

- ✓ La salida a internet del servidor
- ✓ La salida a internet de la STA asociada a el SSI de Empleados
- ✓ La comunicación entre la STA_E y el servidor

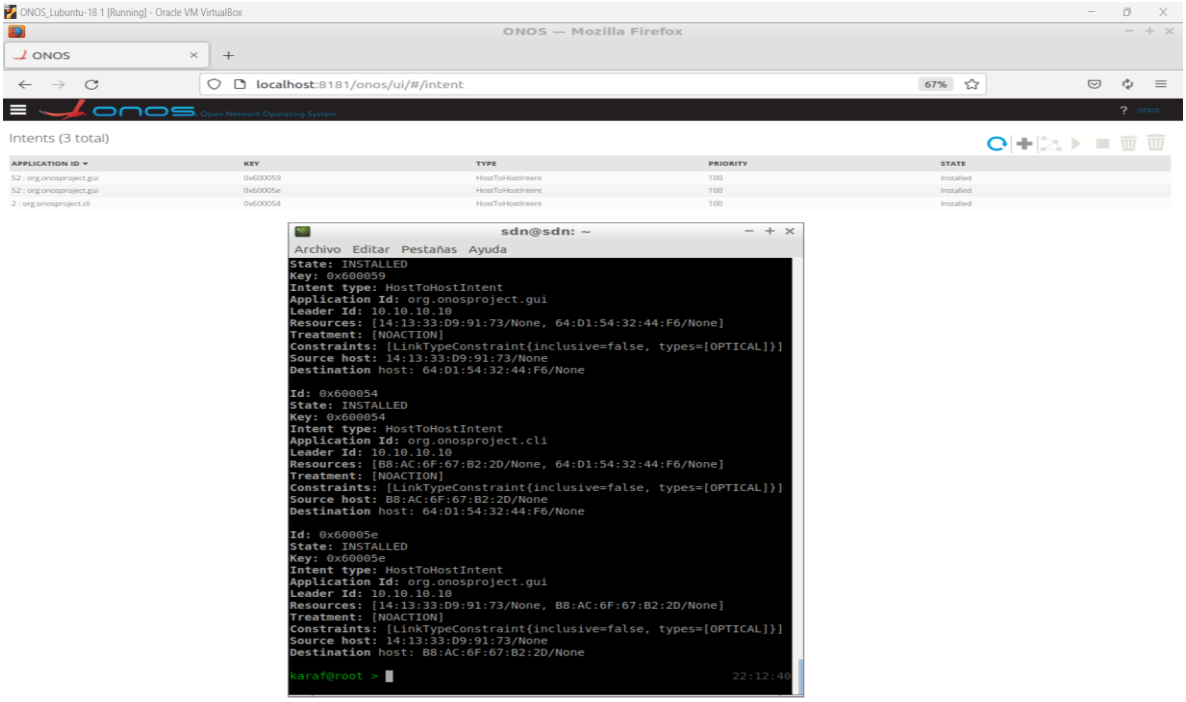


Figura 28: Generación de intenciones de conexión entre STA_E, el servidor y la respectiva salida a internet con IPv4.

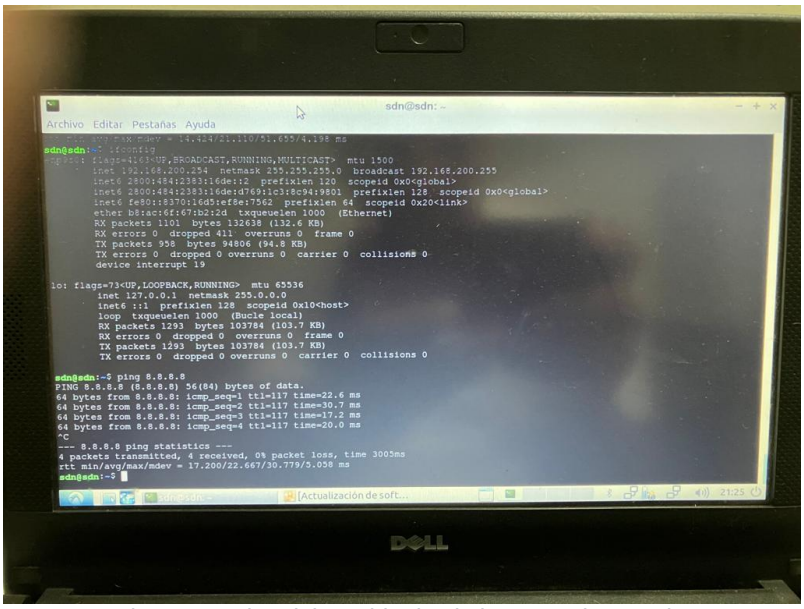


Figura 29: Ping del servidor hacia los DNS de Google.

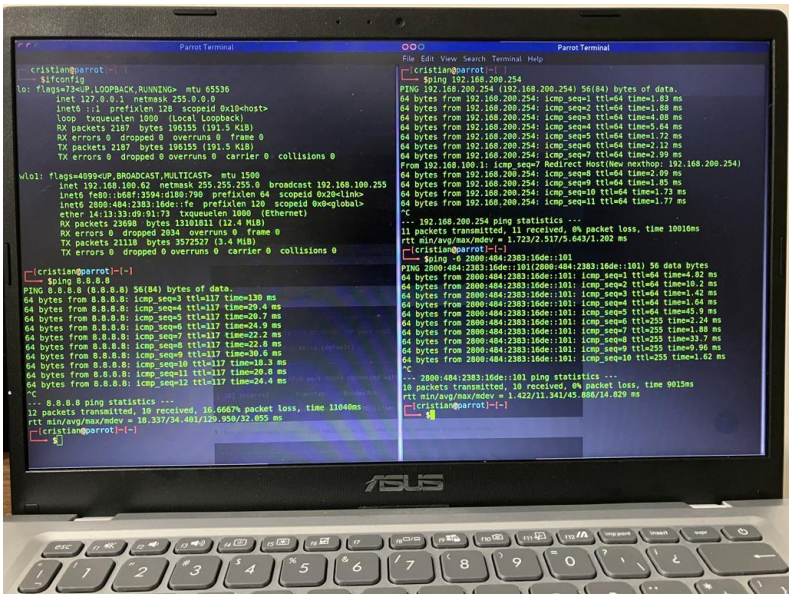


Figura 30: Ping de STA_E hacia el DNS de Google, punto de simulación para salida a internet de IPv6 (2800:484:2383:16de::101) y el servidor.

La salida a internet del direccionamiento IPv6 se simula con un *ping* a la dirección 2800:484:2383:16de::101 ya que no se cuenta con un segmento real conocido en la red del ISP.

El tercer componente de la configuración básica de la controladora ONOS está relacionada con la parametrización de la estructura de gestión

NETCONF/YANG. Inicialmente se verifica la conectividad entre la controladora y los AP como se aprecia en la figura 31.

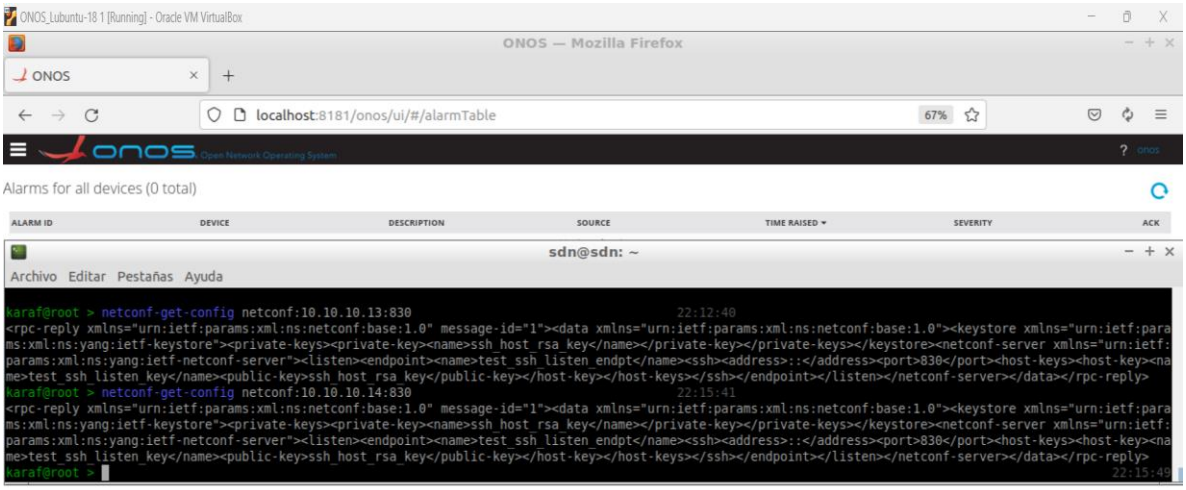


Figura 31: Configuración del servidor NETCONF en uno de los dos AP.

Posteriormente se estructura los archivos con extensión “xml” que permiten la extracción de los parámetros de operación de la interfaces inalámbricas y el cambio de estos, actividad que se logra mediante el módulo *terastream-wireless*, bajo las siguientes instrucciones:

Solicitud de parámetros inalámbricos corriendo sobre una interfaz inalámbrica (“*state-wireless-interface.xml*”)

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
   <get-config>
      <source>
         <startup/>
      </source>
      <filter type="subtree">
         <ts-ws:apsteering xmlns:ts-ws="http://terastrm.net/ns/yang/terastream-wireless"/>
         <ts-ws:bandsteering xmlns:ts-ws="http://terastrm.net/ns/yang/terastream-wireless"/>
         <ts-ws:devices xmlns:ts-ws="http://terastrm.net/ns/yang/terastream-wireless"/>
      </filter>
    </get-config>
</rpc>
```

Configuración de parámetros inalámbricos (*“edit-wireless-config.xml”)*

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
      xmlns:ts-ws="http://terastrm.net/ns/yang/terastream-wireless"
      message-id="1">
  <edit-config>
```

```
<target>
  <candidate/>
</target>
<config>
  <devices xmlns="http://terastrm.net/ns/yang/terastream-wireless">
    <device>
      <name>radio0</name>
      <type>mac80211</type>
      <country>CO</country>
      <frequencyband>2.4</frequencyband>
      <bandwidth>20</bandwidth>
      <channel>11</channel>
      <scantimer>15</scantimer>
      <wmm>true</wmm>
      <wmm_noack>false</wmm_noack>
      <wmm_apsd>true</wmm_apsd>
      <txpower>30</txpower>
      <rateset>default</rateset>
      <frag>0</frag>
      <rts>0</rts>
      <dtim_period>1</dtim_period>
      <beacon_int>100</beacon_int>
      <rxchainps>false</rxchainps>
      <rxchainps_qt>10</rxchainps_qt>
      <rxchainps_pps>10</rxchainps_pps>
      <rifs>false</rifs>
      <rifs_advert>false</rifs_advert>
      <maxassoc>32</maxassoc>
      <dfsc>true</dfsc>
      <hwmode>11g</hwmode>
      <enabled>true</enabled>
      <beamforming>true</beamforming>
      <doth>1</doth>
      <interface>
        <name>default_radio0</name>
        <ifname>wlan0</ifname>
        <network>lan</network>
        <mode>ap</mode>
        <ssid>Employed</ssid>
        <encryption>psk2</encryption>
        <cipher>auto</cipher>
        <key>1234567890</key>
        <gtk_rekey>600</gtk_rekey>
        <wps_pbc>true</wps_pbc>
        <wmf_bss_enable>true</wmf_bss_enable>
        <bss_max>32</bss_max>
        <macfilter>0</macfilter>
      </interface>
      <interface>
        <name>wifinet1</name>
        <ifname>wlan0-1</ifname>
        <network>lan</network>
        <mode>ap</mode>
        <ssid>Guest</ssid>
        <encryption>psk2</encryption>
        <cipher>auto</cipher>
        <key>1234567890</key>
```

```
                <gtk_rekey>600</gtk_rekey>
                <wps_pbc>true</wps_pbc>
                <wmf_bss_enable>true</wmf_bss_enable>
                <bss_max>32</bss_max>
                <macfilter>0</macfilter>
              </interface>
            </device>
          </devices>
      </config>
  </edit-config>
</rpc>
```

Confirmación de configuración enviada al AP (*"commit.xml")*

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
      <commit xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
</rpc>
```

2.4. Definición de pruebas para escenario emulado con Mininet-WiFi y equipos reales

El diseño de la topología de red SDWLAN empresarial y los escenarios de emulación que buscan cumplir con los objetivos del presente proyecto definen un sondeo inicial de la operación de la controladora ONOS, los dispositivos de red asociados, el software de emulación y los protocolos OpenFlow y NETCONF, de tal manera que se consideran una evaluación iniciales que da el punto de partida para la elaboración del plan de pruebas.

Los resultados iniciales apuntan a las siguientes aseveraciones que son demostradas con función inicial presentada a lo largo del capítulo de diseño:

a) La controladora ONOS permite presentar sobre una interfaz gráfica y controlar mediante REST API los equipos de red OpenFlow, al igual que visualizar a que conmutador o punto de acceso está conectada una estación de trabajo.

b) El enrutamiento natural y nativo de una topología de red SDN controlada por ONOS es posible sobre un solo segmento de red sin necesidad de acudir a la activación aplicaciones o protocolos adicionales aparte de "org.onosproject.fwd".

c) La asignación de direccionamiento IPv4 e IPv6 es posible y efectiva mediante las aplicaciones de servidore DHCP y *Router Advertisement* de la controladora ONOS.

d) El enrutamiento adelantado por la aplicación de enrutamiento reactivo de la controladora ONOS cumple con la función de comunicar diferentes segmentos de red y permitir la salida a redes externas como la internet.

e) El establecimiento de intenciones de comunicación globales (no discrimina servicio o puerto) entre estaciones de trabajo es totalmente eficiente y restrictivo al sentido de la comunicación que se define.

Lo anteriormente mencionado denota un marco de trabajo que admite realizar un plan de pruebas más contundente como se describe en la tabla 9.

PRUEBA	ESCENARIO DE PRUEBAS	
	MININET-WiFi	EQUIPOS REALES
Asignación de direccionamiento IPv4 e IPv6 de forma automática	IPv4	IPv4 e IPv6
Enrutamiento dinámico		BGP
Presentación de los componentes de red estáticos y en movimiento (conmutadores, puntos de acceso, enlaces y estaciones de trabajo) en la interfaz gráfica de ONOS	X	X
Relación de latencia y ancho de banda con la distancia al AP	X	X
Comportamiento del flujo de datos durante el handover de las STA inalámbricas	X	X
Comparativa de latencia y ancho de banda de las STA inalámbricas en estado estático y en movimiento.	X	X
Evaluación del redireccionamiento del flujo de datos de una STA dada la perdida un enlace físico	X	X
Evaluación del comportamiento de la GUI de ONOS ante la caída de la interfaz inalámbrica de algún AP	X	X
Almacenamiento de históricas de las STA asociadas a los AP	X	X
Evaluación de la capacidad del protocolo de intenciones de comunicaciones para definir flujos de datos a puertos específicos desde determinadas STA		X
Comportamiento del protocolo de Intenciones de comunicación con STA estáticas y en movimiento		X
Control de parámetros como son la frecuencia, ancho de canal, SSID y control de acceso a la red inalámbrica		X

Tabla 9: Resumen de pruebas a realizar para cada escenario de emulación.

El diseño de la SDWLAN empresarial mostro una perspectiva muy prometedora para los diferentes entorno de pruebas, logrando emular el movimiento de las STA y su asociación con cualquiera de los dos AP haciendo uso de un mismo SSID, de acuerdo con el alcance de la señal emitida por cada uno de ellos, lo cual fue reflejado de forma gráfica por la controladora, adicionalmente se comprobó la comunicación entre las estaciones móviles, la internet y la terminal fija. Estos resultados iniciales y la definición del plan de pruebas estructuran un concepto base del desempeño de la SDWLAN diseñada, para continuar con las evaluaciones del comportamiento del modelo SDWLAN contemplado en este capítulo.

CAPITULO III: EMULACIÓN DE SDWLAN Y PRUEBAS DE COMPORTAMIENTO DEL MODELO SDWLAN

Una de las etapas de mayor importancia durante la evaluación del desempeño de una red de comunicaciones es la captura de información estadística que describa su comportamiento en situaciones de tráfico de red en su punto de saturación, su capacidad para priorizar flujos en pro de brindar calidad de servicio, monitoreo de red y su respuesta a fallas. En la ausencia de la posibilidad de realizar estas mediciones sobre una infraestructura de comunicaciones y tráfico de datos real, se ejecutan en escenarios emulados, que, para el presente documento, definen como herramienta el software Mininet-WiFi y puntos de acceso inalámbrico con capacidades de hardware reducidas[20].

3.1. Emulación sobre Mininet-WiFi

Antes de entrar a realizar pruebas con la controladora ONOS ante un escenario de red inalámbrico donde las estaciones de trabajo están en constante movimiento, se hace necesario medir la latencia y ancho de banda de una STA en referencia a la intensidad de señal recibida por el AP, con el fin de observar si es posible relacionar los parámetros de desempeño mencionados, con la ubicación de cada dispositivo asociado a la red inalámbrica y si los resultados obtenidos de la emulación son confiables.

La topología de pruebas está compuesta por 12 STA ubicadas una tras otra a 10 metros de distancia cada una hasta llegar al punto de acceso, dibujando una línea recta. Al interior de la red hay un conmutador OpenFlow que comunica el AP y una terminal que hace las veces de servidor, los dos dispositivos activos están asociados a una controladora ONOS. En la figura 32 se aprecia el escenario de pruebas.

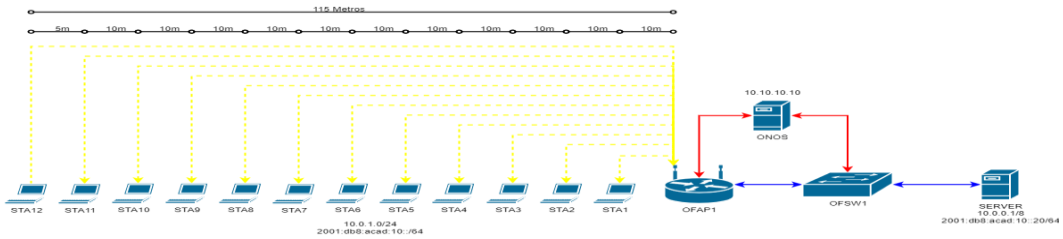


Figura 32: Topología de red para pruebas de desempeño de red.

[20] AP con características de hardware limitadas, con capacidad de atender pocos usuarios y un rendimiento reducido, no usados comúnmente en ambientes empresariales.

Las STA y el servidor apropian direccionamiento IP en las versiones 4 y 6 (Tabla 8), la primera dirección IP es asignada mediante el script de Mininet-WiFi. La segunda es asignada cuando la emulación está corriendo con la instrucción “staX ifconfig staX-wlan0 inet add 2001:db8:acad:10::2/64”, donde la X es el número asignado a cada estación de trabajo.

ESTACIÓN DE TRABAJO	IPv4	IPv6
STA1	10.0.1.1	2001:db8:acad:10::2/64
STA2	10.0.1.2	2001:db8:acad:10::3/64
STA3	10.0.1.3	2001:db8:acad:10::4/64
STA4	10.0.1.4	2001:db8:acad:10::5/64
STA5	10.0.1.5	2001:db8:acad:10::6/64
STA6	10.0.1.6	2001:db8:acad:10::7/64
STA7	10.0.1.7	2001:db8:acad:10::8/64
STA8	10.0.1.8	2001:db8:acad:10::9/64
STA9	10.0.1.9	2001:db8:acad:10::10/64
STA10	10.0.1.10	2001:db8:acad:10::11/64
SERVER	10.0.0.1	2001:db8:acad:10::20/64

Tabla 10: Direccionamiento IP para pruebas de desempeño de red.

En relación con la configuración del espectro inalámbrico, en el aparte del script presentado en la figura 33, se define un AP con un SSID propagado sobre la frecuencia 2412Mhz haciendo uso del estándar IEEE 802.11g, con un rango de operación de 116 metros. Cada STA está configurada con una potencia de transmisión para un rango de 100 metros.

```
OFSW1 = net.addSwitch('OFSW1', cls=OVSKernelSwitch)
OFAP1 = net.addAccessPoint('OFAP1', cls=OVSKernelAP, ssid='ssid-1', channel='1', mode='g', position='200,100,0', range=116)

info( '*** Add hosts/stations\n')
SERVER = net.addHost('SERVER', cls=Host, ip='10.0.0.1', defaultRoute=None)
sta1 = net.addStation('sta1', ip='10.0.1.1', position='190,100,0', range=100)
sta2 = net.addStation('sta2', ip='10.0.1.2', position='180,100,0', range=100)
sta3 = net.addStation('sta3', ip='10.0.1.3', position='170,100,0', range=100)
sta4 = net.addStation('sta4', ip='10.0.1.4', position='160,100,0', range=100)
sta5 = net.addStation('sta5', ip='10.0.1.5', position='150,100,0', range=100)
sta6 = net.addStation('sta6', ip='10.0.1.6', position='140,100,0', range=100)
sta7 = net.addStation('sta7', ip='10.0.1.7', position='130,100,0', range=100)
sta8 = net.addStation('sta8', ip='10.0.1.8', position='120,100,0', range=100)
sta9 = net.addStation('sta9', ip='10.0.1.9', position='110,100,0', range=100)
sta10 = net.addStation('sta10', ip='10.0.1.10', position='100,100,0', range=100)
sta11 = net.addStation('sta11', ip='10.0.1.11', position='90,100,0', range=100)
sta12 = net.addStation('sta12', ip='10.0.1.12', position='85,100,0', range=100)
```

Figura 33: Configuración Mininet-WiFi para pruebas de desempeño de red.

Las pruebas y resultados se muestran en las figuras 34, 35 y tabla 11, consistentes con la latencia y ancho de banda promedio al término del envío de 100 paquetes y 100 segundos respectivamente, haciendo uso de las herramientas PING e IPERF, desde cada STA hacia el servidor. La latencia no muestra un patrón o factor diferenciador a distintos niveles de recepción de señal, al contrario del ancho de banda, donde si se plasma un incremento en los rangos comprendidos entre -77dBm y -87 dBm, lo que implica sin importar la latencia la mejor velocidad se obtiene entre los 40 y 90 metros de distancia entre la STA y el AP.

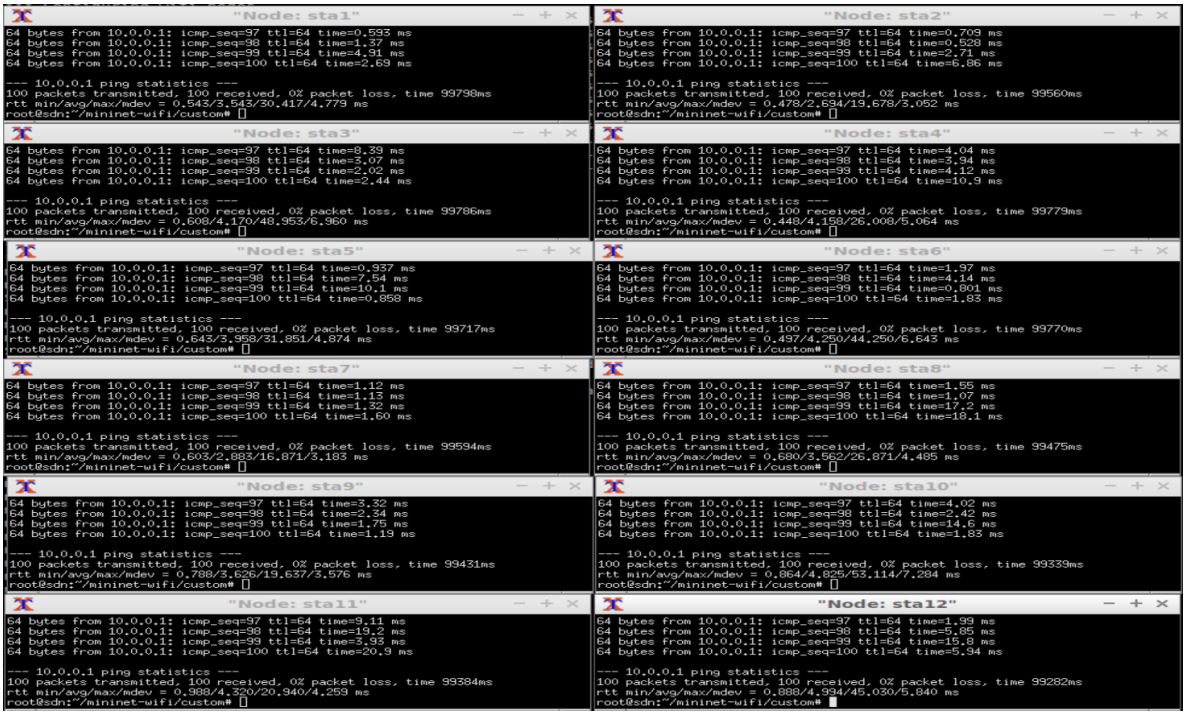


Figura 34: Pruebas de latencia.

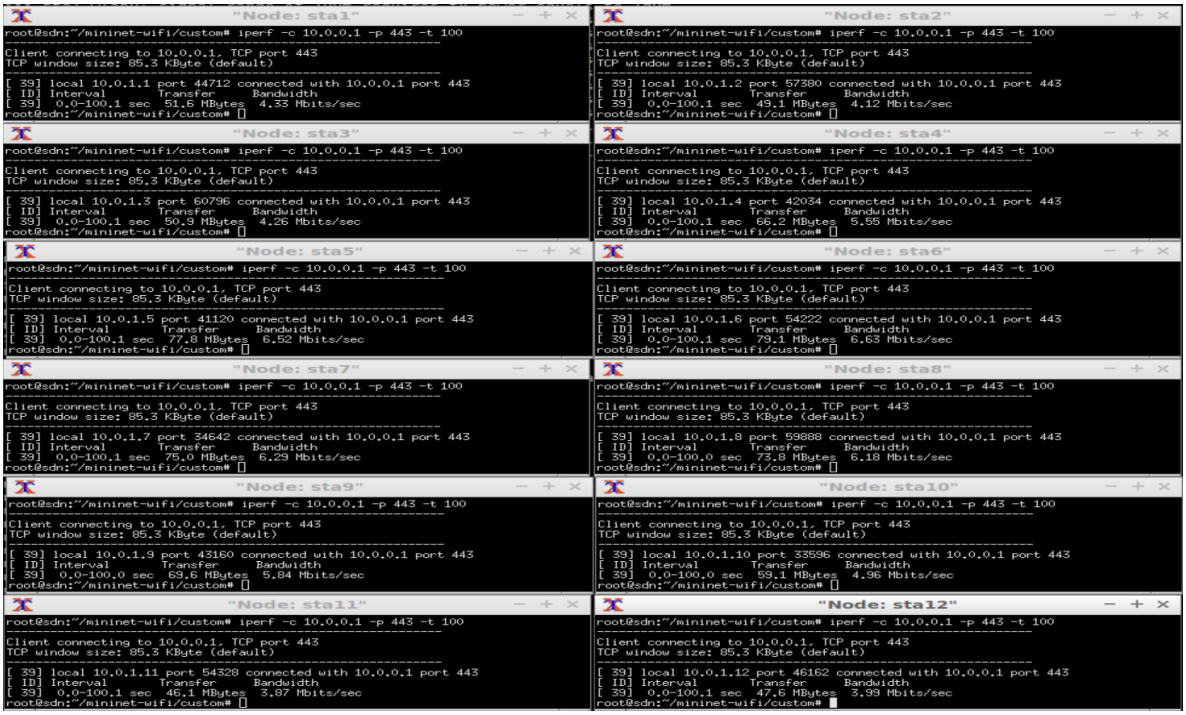


Figura 35: Pruebas de ancho de banda.

ESTACIÓN DE TRABAJO	DISTANCIA DEL AP (METROS)	SEÑAL RECEPCIÓN (dBm)	LATENCIA (ms)	ANCHO DE BANDA (Mbps)
STA1	10	-59	3.5	4.33
STA2	20	-68	2.6	4.12
STA3	30	-73	4.1	4.26
STA4	40	-77	4.1	5.55
STA5	50	-80	3.9	6.52
STA6	60	-82	4.2	6.63
STA7	70	-84	2.8	6.29
STA8	80	-86	3.5	6.18
STA9	90	-87	3.6	5.84
STA10	100	-89	4.8	4.96
STA11	110	-90	4.3	3.87
STA12	115	-90	4.9	3.99

Tabla 11: Resultados para las pruebas de latencia y ancho de banda.

3.1.1. Comportamiento de la interfaz gráfica de ONOS durante el handover y la salida de un a STA de la red

Al inicio de la emulación el conmutador y los AP son detectados de forma automática por la controladora, pero las STA inalámbricas y el servidor requieren generar tráfico para ser detectadas, lo cual se realiza mediante la instrucción “pingall” desde la consola de Mininet-WiFi. Esta instrucción solo genera un paquete ICMP desde cada terminal, luego de esto termina la transmisión de datos, causando que la controladora se quede con el registro de la asociación de la STA con el AP desde donde se realizó la petición y aunque ella se esté moviendo entre los dos puntos de acceso sin perder asociación con ningún SSID, no hay cambio en la interfaz gráfica, como se muestra en la figura 36.

Figura 36: Estado inicial de la interfaz gráfica de la controladora ONOS.

Dado que sin flujo de tráfico desde las STA la controladora no puede mostrar su ubicación, se establece un ping indefinido desde cada una, lo que cambia el comportamiento de la interfaz gráfica, mostrando el tránsito de los dispositivos de una AP a otro, como se puede observar en las figuras 37 y 38. Con esta prueba se encontró de durante el tiempo que dura el handover el flujo de datos se pierde (aproximadamente de 3 a 5 paquetes) en una cantidad que puede despreciarse.

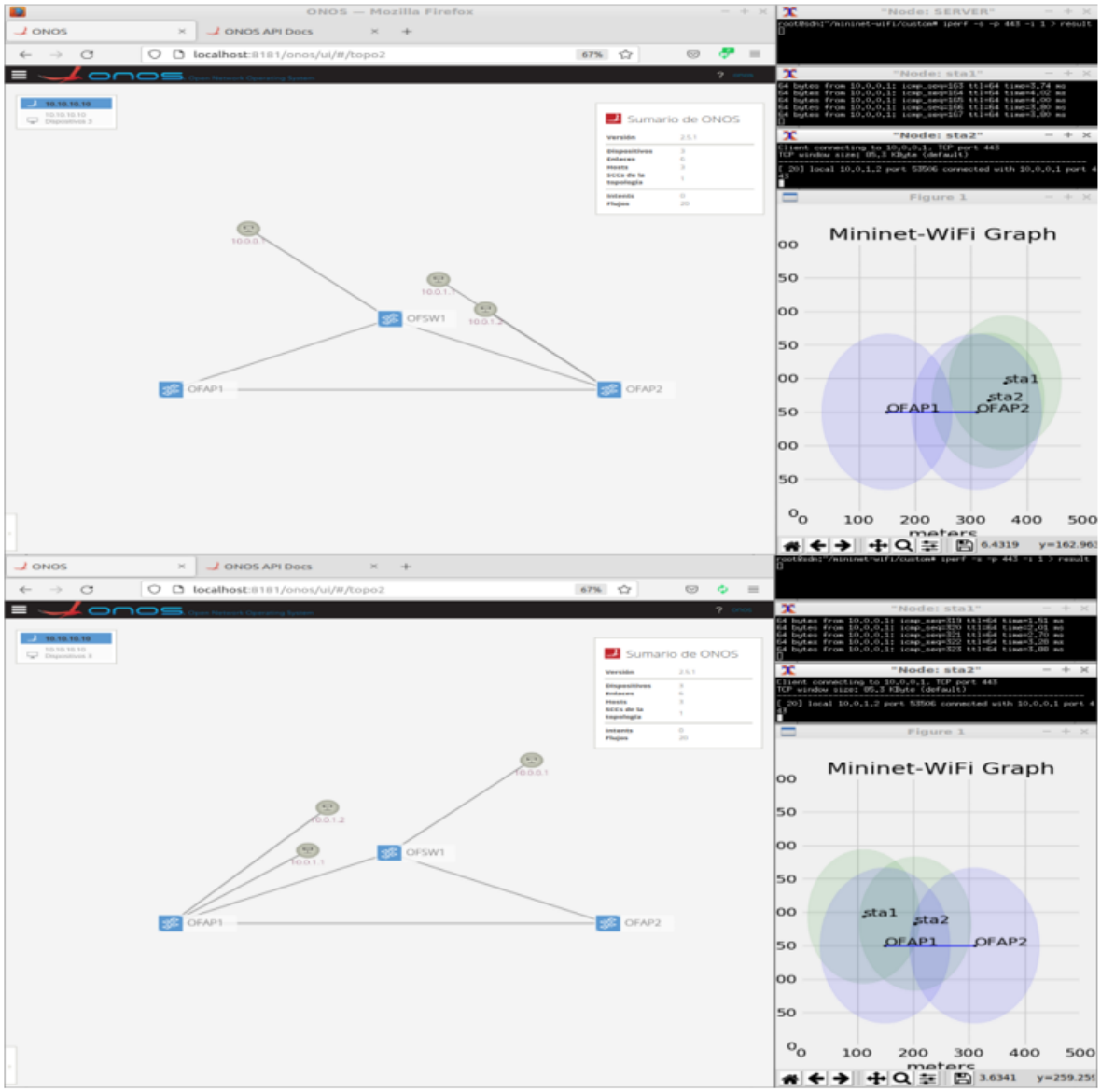


Figura 37: Comportamiento de las STA durante el handover.

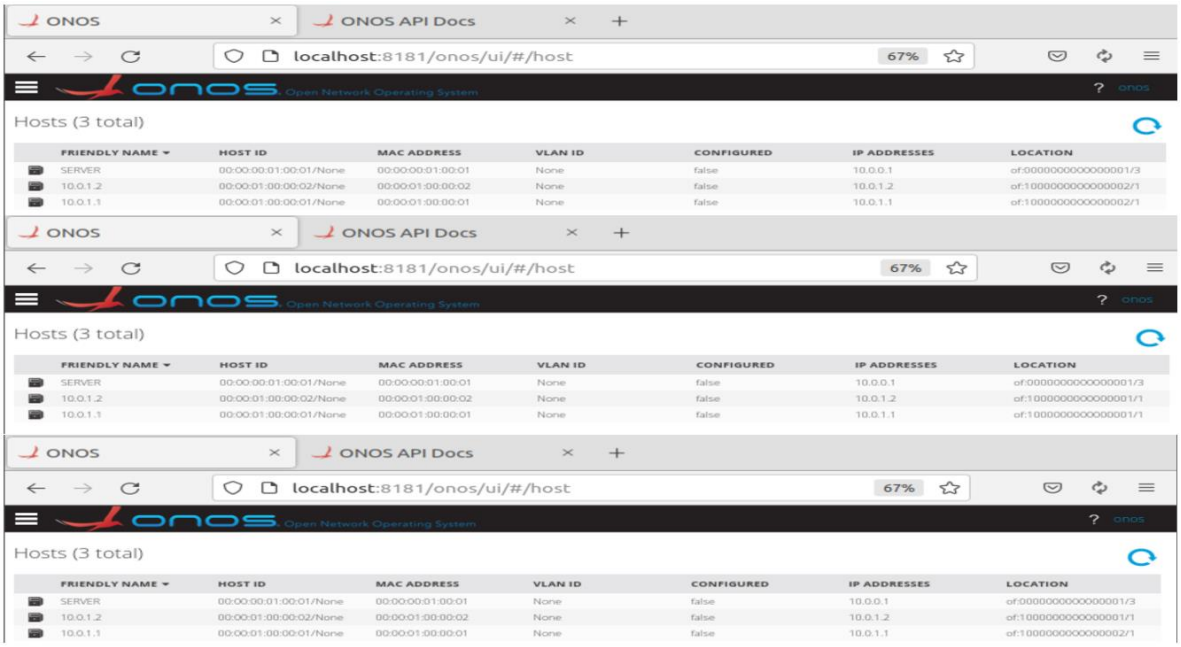


Figura 38: Registro de asociación de las estaciones de trabajo al conmutador y los AP.

El ancho de banda disponible para las STA durante las pruebas es de 6 Mbps, algo muy congruente con los resultados obtenidos en las pruebas para estaciones fijas, con lo que se podría afirmar que el movimiento no afecta este parámetro, al contrario de la latencia, la cual fue, en promedio, de 24ms que comparada con los 4ms de las estaciones fijas el incremento fue 6 veces más, ver figura 39.

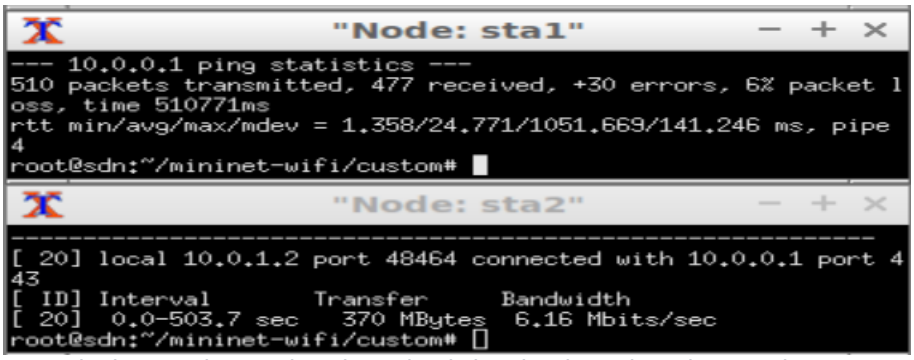


Figura 39: Resultados para las pruebas de ancho de banda y latencia en las estaciones en movimiento.

3.1.2. Comportamiento del flujo de datos ante la caída de un enlace cableado y una interfaz inalámbrica

La topología inicial establece tres enlaces cableados como se muestra en la figura 40, dos de ellos se establecen entre los AP y el conmutador, el tercero se ubica entre los dos AP. Hay un aspecto muy importante de la controladora ONOS con respecto a los enlaces inalámbricos establecidos entre las STA y los AP, el cual está relacionado con el hecho que la controladora los ve como conexiones cableada, mas no como enlaces en el espectro radio eléctrico, por lo cual es imposible obtener parámetros como frecuencias o SSID de asociación. El flujo de datos, por defecto, la controladora lo define por ruta más corta. Para la prueba se establece un ping indefinido desde las STA inalámbricas al servidor.

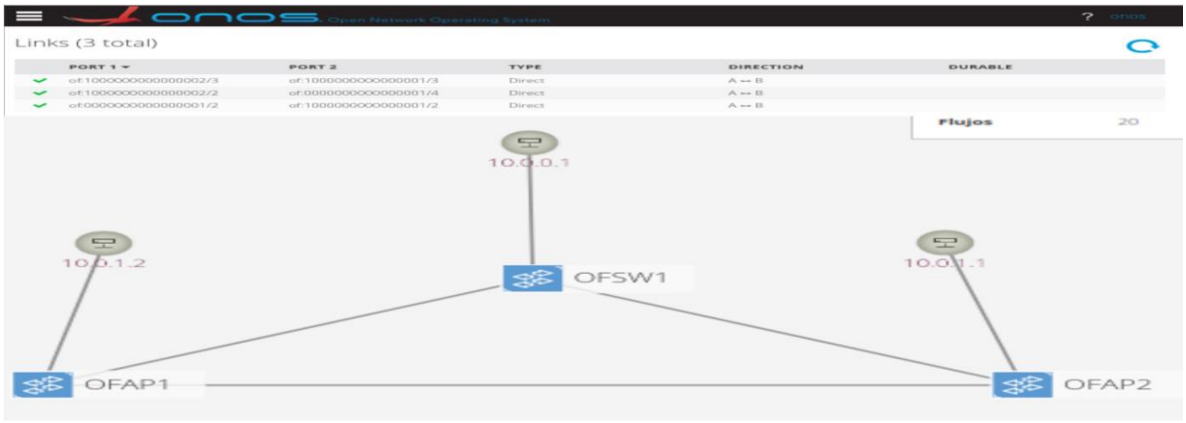


Figura 40: Condición inicial de los enlaces entre el conmutador y los AP.

En la primera prueba se baja el enlace entre los dos AP, en la cual no se observa incidencia en el flujo de datos, no existen pérdida de paquetes desde ninguna STA, como es mostrado en la figura 41, lo que comprueba que la controladora define la ruta más corta.

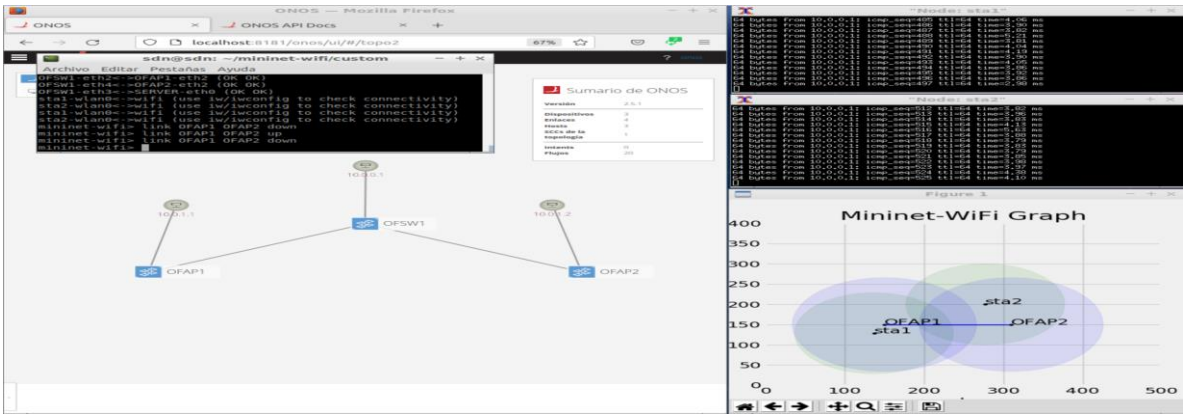


Figura 41: Flujo de datos sin el enlace entre los AP.

Al contrario de las pruebas anteriores, la controladora responde de forma automática cambiando el flujo de datos, ante la caída de un enlace directo desde cualquiera de los AP hacia el conmutador que conecta el servidor como se observa en la figura 42. La pérdida de paquetes es de 2 a 3 unidades, pero se restablece casi de forma inmediata.

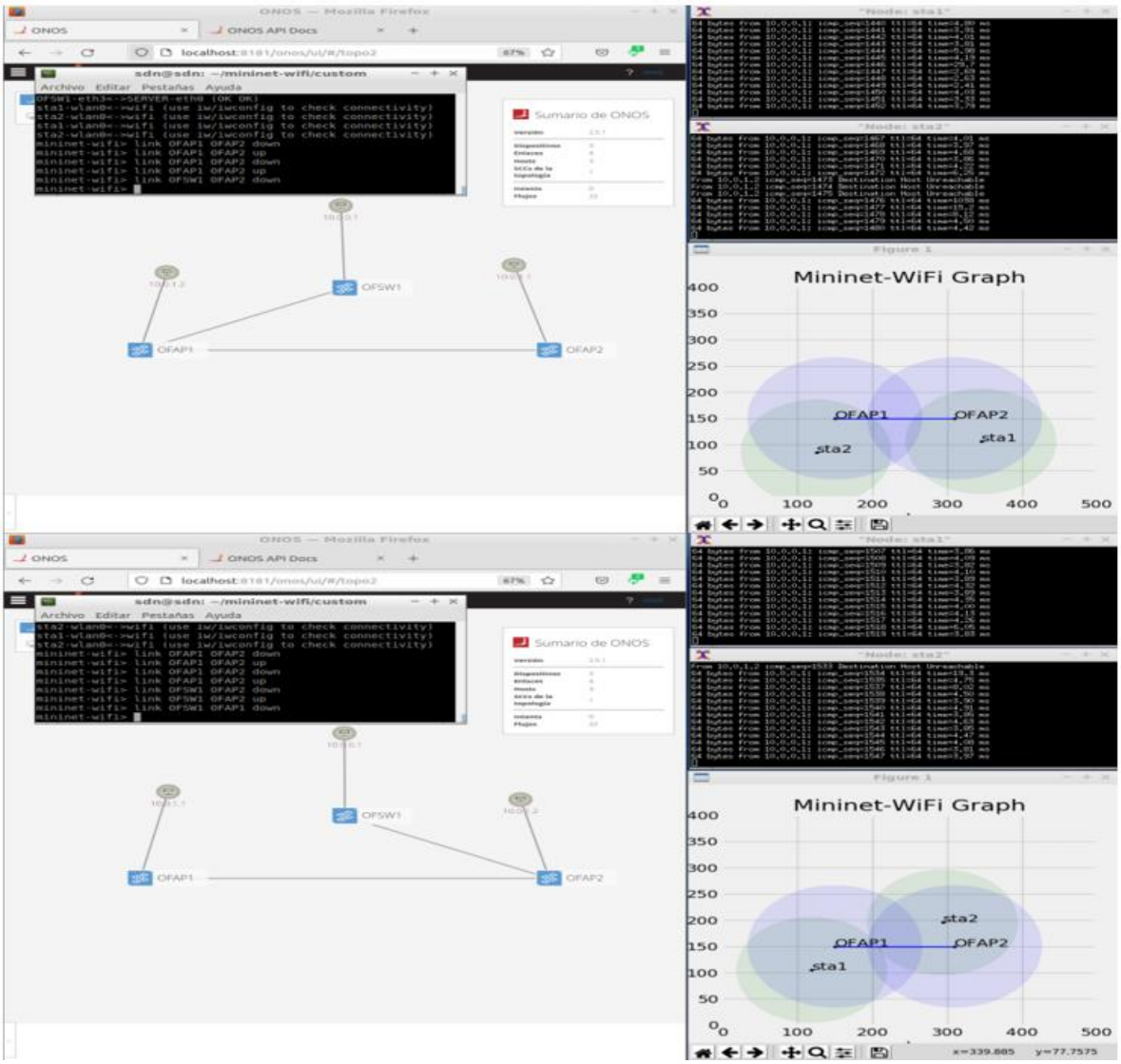


Figura 42: Comportamiento de la controladora a la caída de un enlace directo al servidor.

La última prueba comienza con la caída de la interfaz inalámbrica de una de las dos STA asociadas a los AP, encontrando que la controladora guarda el registro de la última conexión y la deja visible en la interfaz gráfica, pero no informa que la STA salió de la red.

3.1.3. Almacenamiento de históricas de las STA

Una particularidad de la controladora ONOS es que no brinda más información acerca de las estaciones asociadas a la red, aparte del puerto al cual está conectado, la dirección IP y la dirección MAC, como se muestra en la figura 43.

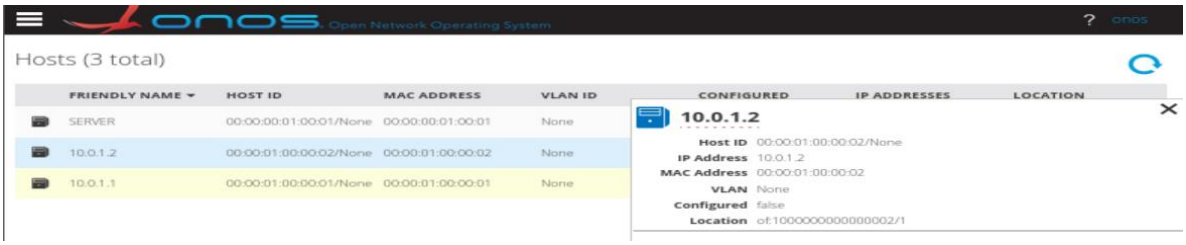


Figura 43: Información de las STA presente en la controladora.

3.2. Emulación sobre equipos reales

La primera instancia de análisis con equipos reales consiste en definir las reglas para las intenciones de comunicación establecidas en la controladora ONOS cuando dos STA están asociadas al SSID de empleados e invitados y requieren generar flujo de datos hacia la internet y/o la estación de trabajo que simula ser un servidor mediante direccionamiento IPv4 e IPv6.

Las condiciones iniciales respondes a los siguientes requerimientos:

a) La STA de pruebas solo estará conectada al punto de acceso OFAP1 de forma estática.

b) La STA asociada al SSID de Empleados debe acceder a internet mediante direccionamiento IPv4, y comunicación ICMP a su puerta de enlace para el direccionamiento IPv6 y al servidor web instalado en la estación que simula ser un servidor al interior de la red.

c) La STA asociada al SSID de Invitados debe acceder a internet mediante direccionamiento IPv4, y comunicación ICMP a su puerta de enlace para el direccionamiento IPv6, adicionalmente debe estar restringido su acceso a la estación que simula ser un servidor.

Inicialmente se define intenciones de comunicación "*host to host*" desde cada STA inalámbrica y el servidor web hacia sus puertas de enlace, con el fin de dará salida a internet y permitir el enrutamiento entre los segmentos de red internos entre

la STA asociada al SSID de empleados y el servidor web. Este proceso se realiza desde la interfaz gráfica de ONOS como se muestra en la figura 44.

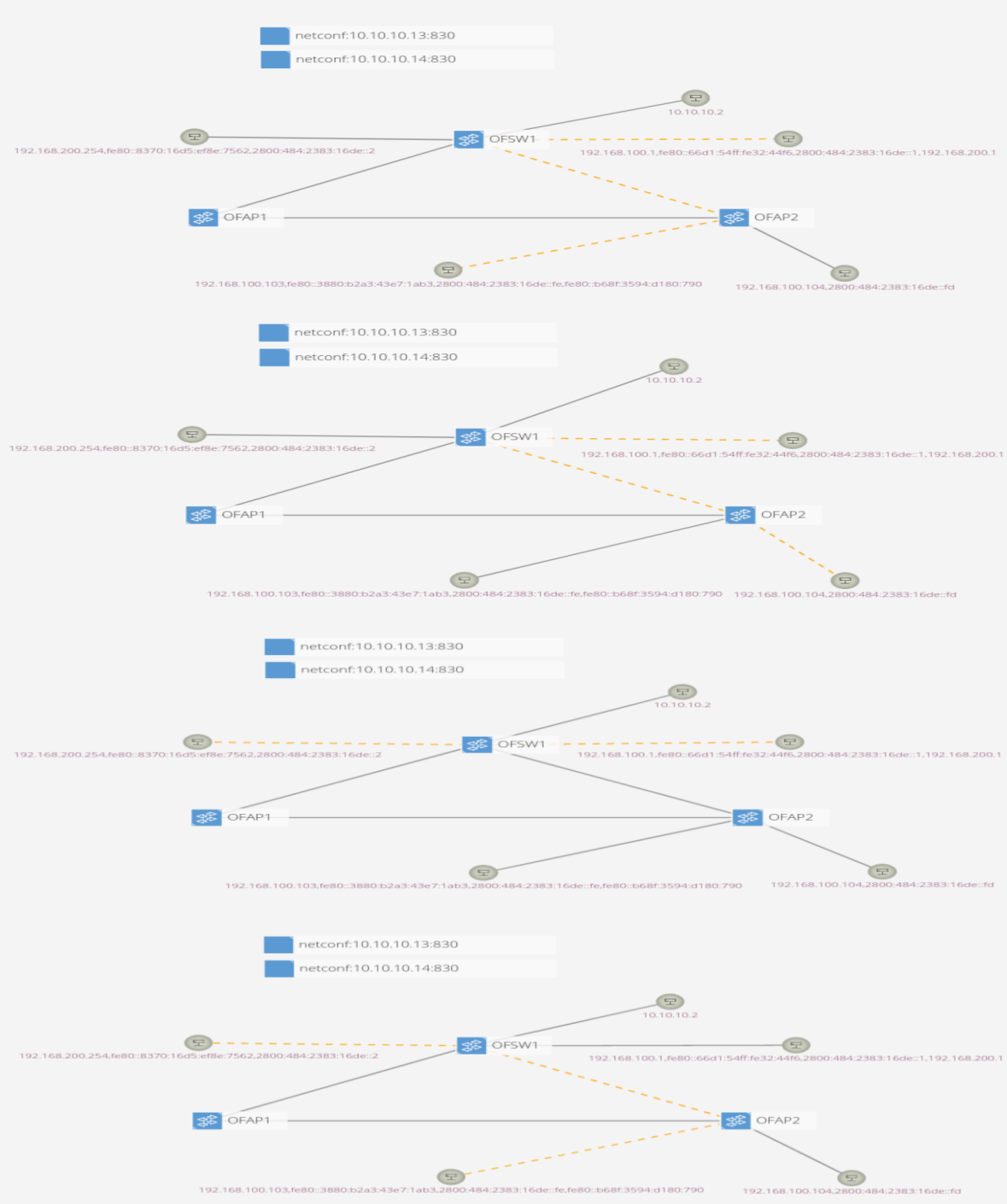


Figura 44: Flujo de las intenciones de comunicación.

Posteriormente se verifica las conexiones y las restricciones para la STA asociada al SSID de Invitados, como se puede observar en la figura 45.

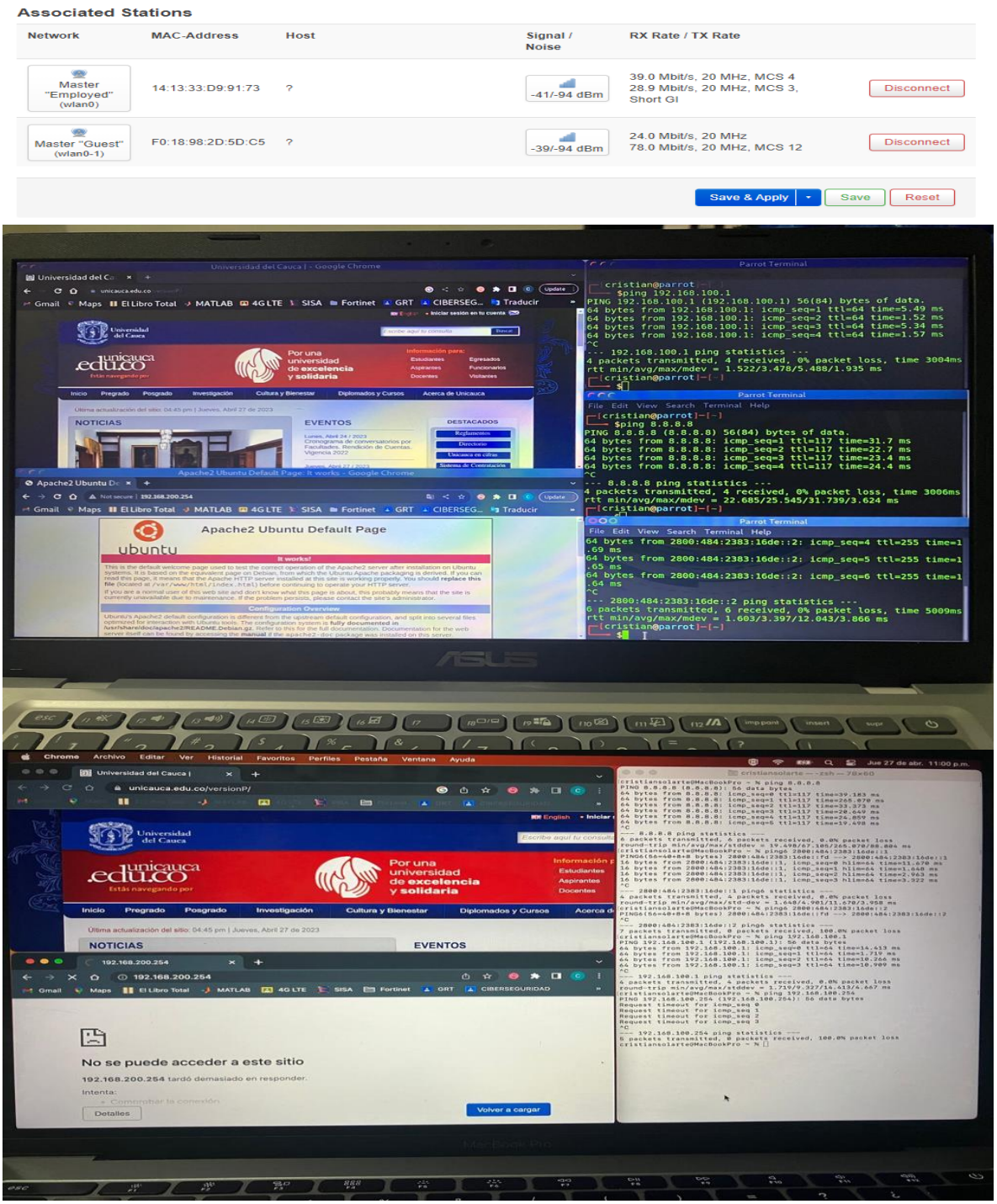


Figura 45: Evidencias de flujos para cada STA inalámbrica asociada a la red SDWLAN.

De forma general los flujos establecidos siguieron las intenciones definidas, pero se evidenció que por instantes la STA asociada al SSID de invitados lograba pasar algunos paquetes al servidor web, lo cual proporciona una incertidumbre de eficiencia en el bloqueo, muy pequeña pero latente.

3.2.1. Comportamiento de la interfaz gráfica de ONOS durante el handover

En cuanto una STA se asocia al cualquiera de los dos AP y se aprovisiona con una dirección IP es detectada por la controladora ONOS y mostrada por su interfaz gráfica. Para las pruebas de handover se ubicará una estación de trabajo en cada AP, asociando una al SSID de empleados y el otro al de invitados, para la primera establece un flujo de comunicación ICMP a la maquina 192.168.200.254 y para la segunda a la IP pública 8.8.8.8.

La primera vez en la que las STA inalámbricas se cambian de AP se observa una pérdida de paquetes de 2 y 6 unidades durante la transición, pero el flujo continua y la controladora muestra el cambio de conexión como se observa en la figura 46 y 47. Pero al realizar un segundo movimiento de AP se pierde el flujo de datos totalmente, la STA asociada al SSID de empleados pierdo la conexión al 192.168.200.254 pero la mantiene hacia su puerta de enlace e internet como se puede verificar en la figura 48, y la STA asociada al SSID de invitados su conectividad en capa 3 se pierde totalmente y para restablecerla fue necesario borrar las intenciones de conectividad y volverlas a configurar.

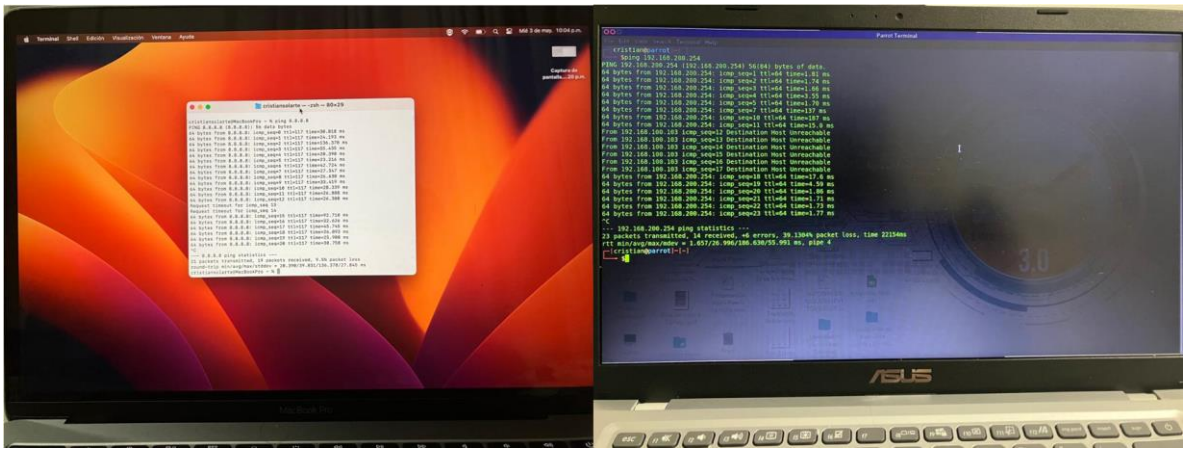


Figura 46: Flujo de datos durante transición de AP.

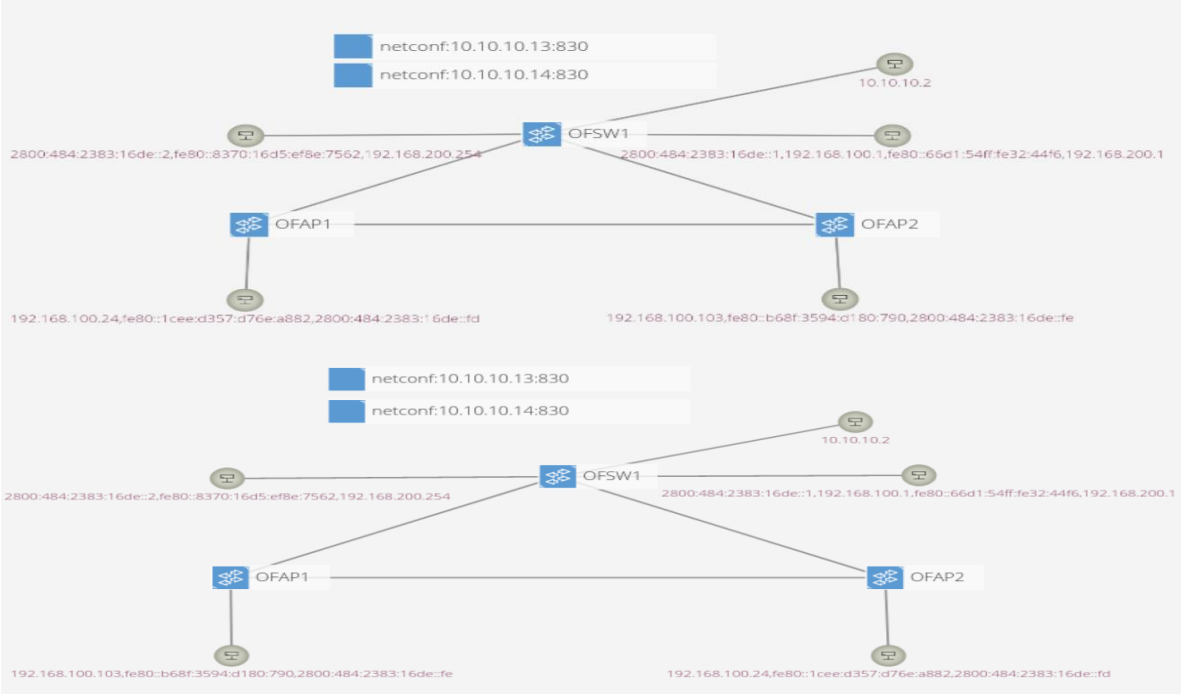


Figura 47: Cambio de posición de las STA durante la transición de AP.

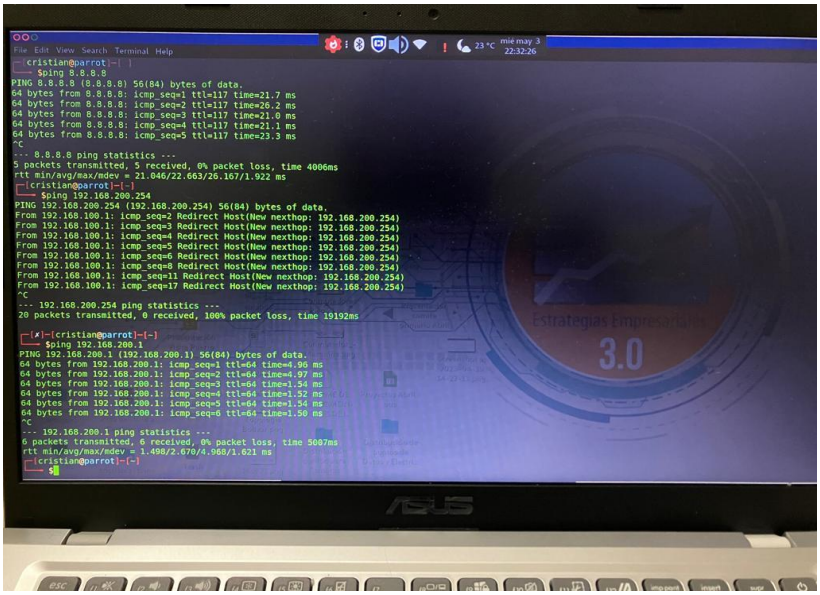


Figura 48: estado de conectividad de la STA asociada al SSID de empleados en un segundo cambio de AP.

Es válido aclarar que la controladora siempre mantuvo actualizada la conexión física a los AP, no hubo perdida de asignación de direccionamiento IP por parte del DHCP y la interfaz gráfica siempre realiza el cambio de flujos del OFAP1 al OFAP2 y viceversa, las intenciones de conexión no se perdieron, simplemente el protocolo dejo de funcionar.

3.2.2. Comportamiento del flujo de datos ante la caída de un enlace cableado

La evaluación del sistema de enrutamiento ante la caída de un enlace cableado inicia con la ubicación de dos STA asociadas a los SSID de empleados e invitados y conectados a puntos de acceso distintos. La STA asociada al SSID de empleados establecerá una comunicación ICMP a la IP 192.168.200.254 y la STA asociada al SSID de invitados se establecerá un ping a la IP 8.8.8.8 en internet.

La primera prueba es la desconexión del enlace entre OFAP1 y OFAP2 como se muestra en la figura 49, encontrando que la intención de conectividad establece como prioridad la distancia más corta.

Figura 49: estado de comunicación de las STA inalámbricas al momento de perder enlace entre OFAP! y OFAP2.

La segunda prueba es la desconexión del enlace del OFAP1 con el OFSW1, encontrando que el flujo cambia, pero existe pérdida de la comunicación con la IP 8.8.8.8, la cual se restablece borrando y configurando nuevamente la intención. Lo mismo ocurre cuando se genera la desconexión del enlace entre el OFAP2 y

OFSW1. En la figura 50 se puede observar el cambio de flujos y la pérdida de conectividad.

Figura 50: estado de comunicación de las STA inalámbricas al momento de perder enlace entre OFAP1, OFAP2 y OFSW1.

3.2.3. Evaluación de ancho de banda y latencia al interior de la red y hacia internet

La pruebas de medición de ancho de banda se compone de dos partes, la primera esta basa da en la aplicación iperf y es medida desde una STA hacia la dirección IP 192.168.200.254 y la segunda la medida obtenida desde internet por una página web www.speedtest.net.

En la figura 51 se evidencia que el ancho de banda del canal inalámbrico establecido por el AP para la STA es de 80Mbps aproximadamente (40mbps de subida y 40 mbps de bajada) y latencias de 20ms a la dirección IP 192.168.200.254, y el ancho de banda proporcionado en los enlaces cableados es de 1.24Gbps.

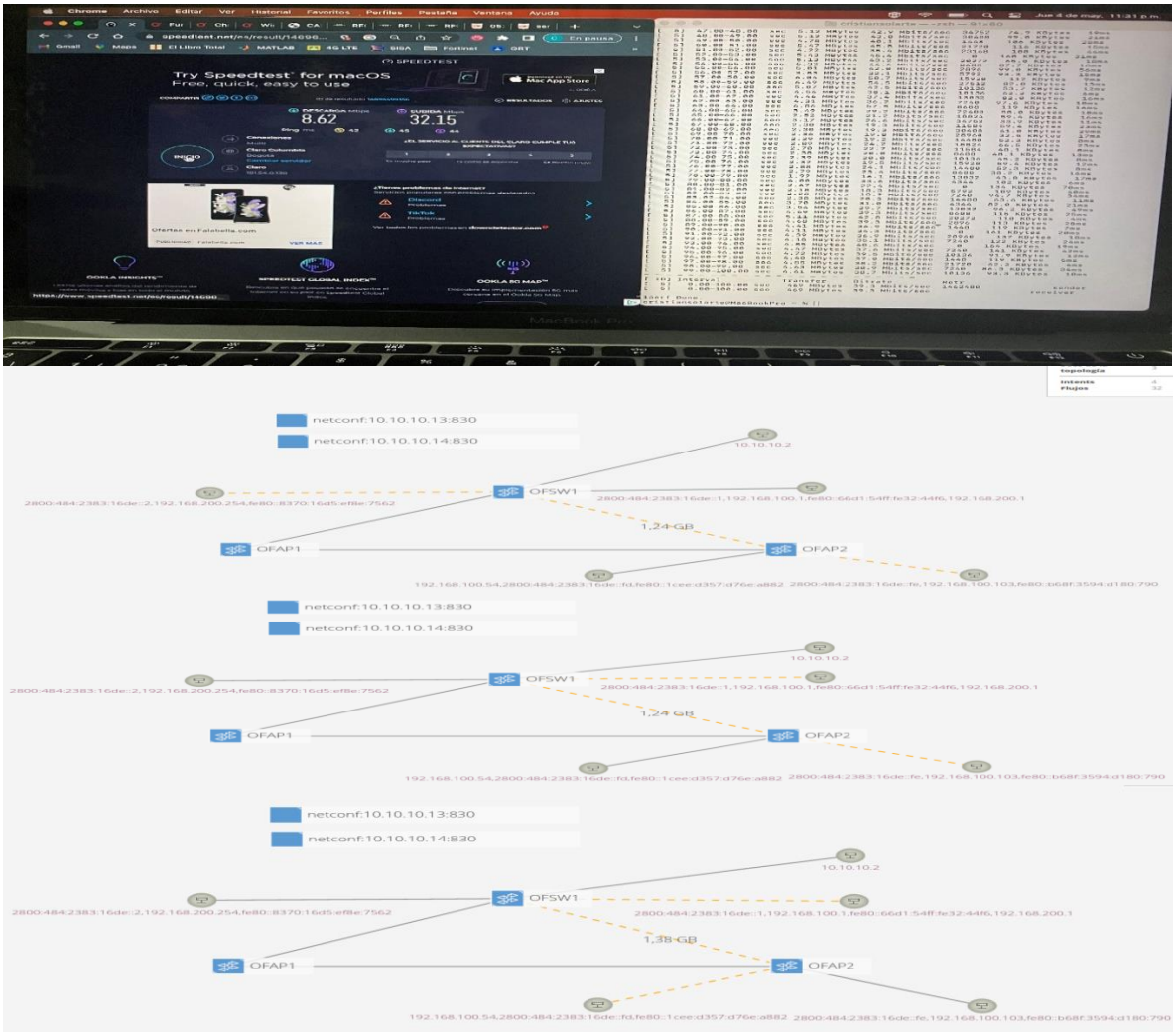


Figura 51: Evidencias de ancho de banda obtenido hacia Internet y el interior de la red medido por Iperf y www.speedtest.net.

3.2.4. Pruebas de control de interfaz inalámbrica mediante el protocolo NETCONF en un punto de acceso

La gestión de una interfaz inalámbrica en un punto de acceso inicia con la verificación del estado su estado, haciendo uso de la siguiente instrucción asociada al script denominado "*state-wireless-config.xml*" enviada desde la consola de líneas de comandos de la controladora.

netconf-rpc-test netconf:10.10.10.14:830 /tmp/state-wireless-config.xml

Figura 52: Comparativa de parámetros de configuración inalámbrica en el dispositivo OFAP1 y la que se obtiene con NETCONF.

En la figura 52 se puede observar la comparativa de la configuración que está corriendo sobre el AP y la que se obtiene desde el cliente NETCONF, encontrando

que veracidad en la información extraída. El contenido de la figura se organizó con ayuda de la página web https://jsonformatter.org/xml-formatter para ser descrita a continuación.

```
<rpc-reply
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="9">
    <data
        xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <apsteering
            xmlns="http://terastrm.net/ns/yang/terastream-wireless">
            <enabled>false</enabled>
        </apsteering>
        <bandsteering
            xmlns="http://terastrm.net/ns/yang/terastream-wireless">
            <enabled>false</enabled>
            <policy>false</policy>
        </bandsteering>
        <devices
            xmlns="http://terastrm.net/ns/yang/terastream-wireless">
            <device>
                <name>radio0</name>
                <type>mac80211</type>
                <country>CO</country>
                <frequencyband>2.4</frequencyband>
                <bandwidth>20</bandwidth>
                <hwmode>11g</hwmode>
                <channel>11</channel>
                <scantimer>15</scantimer>
                <wmm>true</wmm>
                <wmm_noack>false</wmm_noack>
                <wmm_apsd>true</wmm_apsd>
                <txpower>20</txpower>
                <rateset>default</rateset>
                <frag>0</frag>
                <rts>0</rts>
                <dtim_period>1</dtim_period>
                <beacon_int>100</beacon_int>
                <rxchainps>false</rxchainps>
                <rxchainps_qt>10</rxchainps_qt>
                <rxchainps_pps>10</rxchainps_pps>
                <rifs>false</rifs>
                <rifs_advert>false</rifs_advert>
                <maxassoc>32</maxassoc>
                <beamforming>true</beamforming>
                <doth>1</doth>
                <dfsc>true</dfsc>
                <interface>
                    <name>default_radio0</name>
                    <network>lan</network>
                    <mode>ap</mode>
                    <ssid>Employed</ssid>
                    <encryption>psk2</encryption>
                    <cipher>auto</cipher>
                    <key>1234567890</key>
                    <gtk_rekey>600</gtk_rekey>
                    <macfilter>0</macfilter>
```

```
                    <wps_pbc>true</wps_pbc>
                    <wmf_bss_enable>true</wmf_bss_enable>
                    <bss_max>32</bss_max>
                    <ifname>wlan0</ifname>
                </interface>
                <interface>
                    <name>wifinet1</name>
                    <network>lan</network>
                    <mode>ap</mode>
                    <ssid>Guest</ssid>
                    <encryption>psk2</encryption>
                    <cipher>auto</cipher>
                    <key>1234567890</key>
                    <gtk_rekey>600</gtk_rekey>
                    <macfilter>0</macfilter>
                    <wps_pbc>true</wps_pbc>
                    <wmf_bss_enable>true</wmf_bss_enable>
                    <bss_max>32</bss_max>
                    <ifname>wlan0-1</ifname>
                </interface>
            </device>
        </devices>
    </data>
</rpc-reply>
```

La anteriores líneas de código ayudan a la generación de nuevo código que permita cambiar los parámetros de configuración y transmitirlo al dispositivo, siguiendo las siguientes instrucciones:

netconf-rpc-test netconf:10.10.10.14:830 /tmp/edit-wireless-config.xml
netconf-rpc-test netconf:10.10.10.14:830 /tmp/commit.xml

Durante la prueba se obtiene cambios de la configuración de forma satisfactoria como, la cual es comprobada a traves del mensaje observable en la figura 53

Figura 53:Confirmación de la aplicación de cambios en la configuración del AP.

3.3. Resumen de resultados obtenidos en las pruebas con Mininet-WiFi y equipos reales

De acuerdo con los resultados obtenidos en las pruebas realizadas en la emulación con Mininet-WiFi y con equipos reales se genera la tabla 12, donde se resumen los hallazgos de forma cualitativa.

PRUEBA	RESULTADO
Asignación de direccionamiento IPv4 e IPv6 de forma automática	La asignación de parámetros de red IPv4 e IPv6 se realiza mediante las aplicaciones de DHCP y *Router Advertisement* y mantienen ese direccionamiento en cada STA sin importar a que SSID se asocien o en que AP estén conectadas
Enrutamiento dinámico	El enrutamiento entre diferentes segmentos de red al interior de la SDWLAN y hacia internet funciona de forma exitosa mediante el protocolo BGP tanto para IPv4 como para IPv6
Presentación de los componentes de red estáticos y en movimiento (conmutadores, puntos de acceso, enlaces y estaciones de trabajo) en la interfaz gráfica de ONOS	Los dispositivos como conmutadores, puntos de acceso y enlaces físicos mientras estén conectados siempre son visibles. Las STA se mantienen perceptibles a la GUI de ONOS mientras generan algún tipo de tráfico de datos o mantengan viva la asociación con el AP.
Relación de latencia y ancho de banda con la distancia al AP	No de encontró un patrón en los resultados que definiera las distancias de los enlace inalámbrico.
Comportamiento del flujo de datos durante el handover de las STA inalámbricas	En la emulación con Mininet-WiFi el flujo de datos no es totalmente transparente, se observa la perdida de menos de 5 paquetes que pueden ser despreciables, en una red con equipos reales la controladora SDN evidencia el cambio de AP, pero el flujo de datos es interrumpido.
Comparativa de latencia y ancho de banda de las STA inalámbricas en estado estático y en movimiento.	No se encontró una diferencia relevante, para las métricas de latencia o ancho de banda, durante las pruebas de comunicaciones entre las STA, en condición de movimiento o estáticas, y la terminal fija que opera como servidor, excepto algunas perdidas de paquetes en el borde del área de cobertura de cada AP.
Evaluación del redireccionamiento del flujo de datos de una STA dada la pérdida un enlace físico entre los AP y/o el conmutador.	En la emulación con Mininet-WiFi el flujo de datos es redireccionado y la comunicación entre el origen y el destino no se pierden, pero el comportamiento de la controladora con equipos reales muestra el cambio de flujo, pero la comunicación se pierde totalmente, no se tiene una explicación certera del fenómeno.
Evaluación del comportamiento de la GUI de ONOS ante la caída de la interfaz inalámbrica de algún AP	La GUI muestra la caída del enlace entre la STA y el AP, pero la STA se sigue observando en la GUI con alerta de desconexión.
Almacenamiento de históricas de las STA asociadas a los AP	La controladora ONOS no almacena ningún tipo de información de las STA asociadas, aparte de la relación dirección MAC y direcciones IPv4 e IPv6 con las que se ha operado al interior de la red
Evaluación de la capacidad del protocolo de intenciones de comunicaciones para definir flujos de datos a puertos específicos desde determinadas STA	Las intenciones de comunicación definen flujos específicos de origen a destino restringiendo las comunicaciones y creando QoS, pero se hace necesario definir políticas específicas para cada puerto TCP y/o UDP incluyendo sistemas de enrutamiento, DNS y asignación automática de direccionamiento IPv4 e IPv6.
Comportamiento del protocolo de Intenciones de comunicación con STA estáticas y en movimiento	Las intenciones de comunicación funcionan muy bien mientras las STA estén estáticas, en el momento de realizan handover dejan de funcionar
Control de parámetros como son la frecuencia, ancho de canal, SSID y control de acceso a la red inalámbrica	La administración de parámetros inalámbricos mediante el protocolo NETCONF es totalmente posible con limitantes para ejecutar herramientas de análisis de espectro propias del sistema operativo OpenWrt. Adicionalmente la lectura de configuraciones se hace un

	poco dispendiosa ya que no se cuenta con la posibilidad de una interfaz gráfica.

Tabla 12: Resumen de resultados obtenidos en las pruebas adelantadas en el presente capítulo

La experiencia obtenida durante la ejecución del plan de pruebas y emulación de la SDWLAN empresarial con Mininet-WiFi, diseñados en el capítulo tres y su comportamiento sobre equipos reales, presentan dos diferencias de operación transcendentales. La primera radica en la perdida de comunicación de las STA móviles hacia internet o la terminal fija al momento de realizar el handover pero no se disipa su la asociación con los AP. La segunda diferencia es la falla de la controladora ONOS para mantener el flujo de datos dada la ausencia de un enlace físico entre los AP y el conmutador OpenFlow, pero cabe resaltar que la posee herramientas, como son los protocolos OpenFlow y NETCONF, de gestión y control programables que permitieron aprovisionar los AP, graficar la topología de red e identificar los flujos de datos que circulan por la red.

CAPÍTULO IV: CONCLUSIONES

Este proyecto proporciona una perspectiva del desempeño de una red SDWLAN embebida en un entorno empresarial, a partir de las necesidades de un administrador de red que busca una administración centralizada, escalable en tamaño, adaptable a múltiples tecnologías de comunicación, con una alta disponibilidad y la posibilidad de establecer comunicaciones basadas en intenciones, dentro de un marco de gestión de redes estandarizado; enfocando la investigación en la observación del comportamiento de una controladora SDN, como es ONOS, y su integración con puntos de acceso inalámbricos operados por un sistema operativo OpenWrt, donde se despliegan protocolos de comisión como son OpenFlow (OpenVSwitch) y NETCONF (Netopeer2).

Bajo el contexto anteriormente descrito se concluye:

El diseño e implementación de una red definida por software cuya plataforma de control está fundamentada en una controladora ONOS, donde la capa de acceso está compuesta por puntos de acceso inalámbricos conectados a conmutadores OpenFlow de forma cableada, que ofrezcan redundancia y cuyo objetivo es establecer flujos de comunicación específicos de origen a destino, al interior de la red y/o internet, dispone de las siguientes apreciaciones:

- ✓ La controladora ONOS no está equipada con aplicaciones que atiendan enlaces de tipo inalámbrico, ya que las conexiones entre una STA y su AP son consideradas como un canal físico de cobre, desestimando la posibilidad de evaluar parámetros propios de la propagación de ondas electromagnéticas. De igual manera, su interfaz gráfica no permite aprovisionar los AP o realizar control de acceso a los mismos. Esto implica la búsqueda de opciones como YANG/NETCONF, que, si están embebidas en la controladora, requieren de desarrollo de software que centralice la gestión y operen como aplicación *northbound*, de lo contrario se debe realizar mediante secuencias de comandos desde una terminal por conexión SSH a la controladora.
- ✓ Controladoras como *OpenDayLigth* poseen aplicaciones nativas de control y aprovisionamiento de puntos de acceso inalámbricos, CAPWAP, pero no es fácil encontrar en el mercado dispositivos que operen el protocolo de forma libre, están amarrados a licenciamiento o certificados propios de la marca fabricante, lo que no permite la realización de pruebas con software de licenciamiento público.
- ✓ La concepción de enrutamiento en una red definida por software cambia de forma conceptual con respecto a las redes tradicionales o heredadas, ya que

la idea de puerta de enlace física y dominio de *broadcast*[21] no existen, es decir, una STA que desea establecer comunicación con otra STA desconoce totalmente la dirección MAC de su destino y si este pertenece a otro segmento de red no puede definir quién es su siguiente salto, impidiendo la construcción de paquetes e imposibilitando su envío. Por lo cual aplicaciones *northbound* como SDN-IP controlan las solicitudes ARP y permiten que las STA accedan a su puerta de enlace virtual. Este software debe ir acompañado de sistemas de enrutamiento dinámico como BGP para poder comunicar diferentes subredes, ya sean IPv4 o IPv6.

- ✓ El aprovisionamiento dinámico de requerimientos de direccionamiento IP, puerta de enlace y DNS en las STA, responden a protocolos estandarizados (DHCP, para IPv4 y *Router Advertisement*, para IPv6) y son controlados por aplicaciones *northbound,* pero su aplicación a conceptos de Red de Área Local Virtual (VLAN, *Virtual Local Area Network*) no son prácticos para redes inalámbricas, ya que no existe dominio de broadcast, son aplicables a un aprovisionamiento estático apoyado por aplicaciones de reenvío.
- ✓ La emulación de red SDN en Mininet-WiFi coinciden con las pruebas realizadas en equipos reales en aspectos como la medición de métricas de desempeño como latencia y ancho de banda, pero difieren en el handover, ya que para Mininet-WiFi nunca se pierde la comunicación entre el origen y el destino, sobre equipos reales se pierde la comunicación, aunque los flujos se muestran cambiantes de un AP a otro. Y el cambio de ruta, dada la caída de un enlace físico, tiene el mismo comportamiento.

La administración de una interfaz inalámbrica real a través de la controladora ONOS se lleva a cabo en un entorno de líneas de comandos, independiente de la interfaz gráfica. Este entorno posee la capacidad de recuperar información relacionada con la frecuencia de operación, SSID y el control de acceso a la red (contraseña de acceso) en la que el hardware está actualmente operando. Aunque es posible efectuar modificaciones en esta configuración, no se logra ejecutar herramientas propias del punto de acceso, diseñadas para escanear el espectro radioeléctrico. Esta limitación impide al administrador de la red evaluar el nivel de saturación de los canales de frecuencia radioeléctrica y establecer las condiciones óptimas de operación.

Mininet-WiFi es un aplicación muy versátil para la emulación, que depende de la interfaz inalámbrica física de la computadora donde está instalada y de acuerdo con las características de esta última se limitan las posibilidades de

[21] Dominio de *broadcast*: mensaje punto multipunto que no tienen un destino en específico y en su trama no existen direccionamiento IP, que se transmite desde una terminal de trabajo hacia otras que pertenezcan a la misma red, es decir que compartan la puerta de enlace y están dentro de la misma LAN.

operación como es el protocolo IEEE 802.11x que se requiere trabajar y por ende la frecuencia, la velocidad de transmisión y ancho de banda.

En posibles nuevos proyectos de investigación o profundizaciones que tomen como referencia bibliográfica el presente documento se recomienda:

- ✓ La integración de la controladora ONOS con el lenguaje P4 en lugar de OpenFlow, por su capacidad para brindar una programabilidad total del plano de datos de las SDN y la posibilidad de una interacción directa con las interfaces físicas de los dispositivos de red, lo cual facilita la generación de agentes de control y gestión a partir de una consola de monitoreo centralizada, especialmente en redes inalámbricas. Adicionalmente P4 es un lenguaje que se integra muy bien con el software de emulación Mininet.
- ✓ Hacer uso de Docker [22] para instalación de Conmutadores Virtuales de Código Abierto (OVS [23] ,Open Virtual Switch), Mininet y ONOS, ya que facilitaría entornos de emulación donde sea necesaria la manipulación de los puertos pertenecientes a los conmutadores virtuales y establecer redes de comunicación, independientes, para las capa de control y la cada de datos, propias de las redes definidas por software.

[22] Docker: herramienta de software que crea contenedores para la instalación de aplicaciones, independientemente del sistema operativo.
[23] OVS: software de código abierto utilizado como conmutador virtual capaz de reenviar trafico entre diferentes máquinas virtuales instaladas en la misma computadora.

BIBLIOGRAFÍA

[1] B. Butler, R. Costello, M. Leary y R. Mehra, «International Data Corporation (IDC),» Abril 2020. [En línea]. Available: https://resources.enterprisetalk.com/ebook/Aruba-HR-Marketing-ES-2.pdf. [Último acceso: 2021 04 29].

[2] P. Morreale y J. Anderson, Software Defined Networkink. Desingn and Deployment, Boca Raton, FL: CRC Press, 2014.

[3] Institute of Electrical and Electronics Engineers, «IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture,» IEEE, New York, 2014.

[4] Institute of Electrical and Electronics Engineers, «Part 11: Wireless LAN Medium Access Control,» IEEE, New York, 2016.

[5] Agencia Nacional del Espectro (ANE), «Resolución 181 de 2019,» ANE, Bogotá D.C., 2019.

[6] J. Sathyan, Fundamentals of EMS, NMS and OSS/BSS, Auerbach Publications, 2016.

[7] B. Claise, J. Clarke y J. Lindbalad, Network programmability with YANG: The structure of network automation with YANG, NETCONF, RESTCONF, and gNMI, Addison-Wesley Professional, 2019.

[8] M. Ersue y C. Benoît, «RFC6632,» Internet Engineering Task Force (IETF), 2011.

[9] Open Network Foundation, «Software Defined Networking: The new norm for networks,» Open Network Foundation, 13 04 2012. [En línea]. Available: https://opennetworking.org/sdn-resources/whitepapers/software-defined-networking-the-new-norm-for-networks/. [Último acceso: 25 04 2021].

[10] P. Goransson, C. Black y T. Culver, Software Defined Networks. A Comprehensive Approach, New York: Morgan Kaufmann, 2016.

[11] C. J. Quimbayo Rodríguez, «Propuesta metodológica para la selección de controladores de redes SDN a nivel empresarial,» Universidad Santo Tomas, Bogotá D.C., 2020.

[12] T. Nadeau y K. Gray, SDN: Software Defined Networks, O'Reilly Media, 2013.

[13] Linux Foundation Projects, «OpenDayLight,» [En línea]. Available: https://www.opendaylight.org. [Último acceso: 05 05 2021].

[14] Instituto Europeo de Normas de Telecomunicaciones, ETSI, «Speech and multimedia Transmission Quality (STQ); QoS and network performance metrics andmeasurement methods; Part 3: Network performance metrics andmeasurement methods in IP networks,» Sophia Antipolis, 2010.

[15] Open Networking Foundation, «Mininet,» 2021. [En línea]. Available: http://mininet.org. [Último acceso: 30 04 2021].

[16] A. Alshanyour y U. Baroudi, «A simulation study: The impact of random and realistic mobility models on the performance of bypass-AODV in Ad hoc wireless networks,» *EURASIP journal on wireless communications and networking,* vol. 2010, nº Article ID 239370, p. 10, 2010.

[17] D. Perdana, R. Munadi y R. Manurung, «Performance evaluation of Gauss-Markov mobility model in hybrid LTE-VANET networks,» *Telkomnika,* vol. 15, nº 2, pp. 606-621, 2013.

[18] R. Sharpe, E. Warnicke y U. Lamping, «Wireshark user's guide,» Wireshark, [En línea]. Available: https://www.wireshark.org/docs/wsug_html_chunked. [Último acceso: 02 05 2021].

[19] OpenWrt, «OpenWrt,» 13 12 2020. [En línea]. Available: https://openwrt.org/. [Último acceso: 02 09 2022].

[20] J. Minella y S. Orr, Wireless security architecture, Wiley, 2022.

ANEXO 1

1. Prerrequisitos del sistema operativo

Inicialmente el sistema operativo debe tener las librerías de Python, Git, Curl y Java-11, las instrucciones de instalación se mencionan a continuación:

```
sudo apt-get update && apt-get upgrade
sudo apt-get install python
sudo apt-get install python3
sudo apt-get install python-pip python-dev python-setuptools
sudo apt-get install python3-pip python3-dev python3-setuptools
sudo pip3 install—upgrade pip
sudo apt-get install python-matplotlib
sudo apt-get install curl
sudo apt-get install zip
sudo apt-get install git
sudo apt-get install git-review
sudo apt-get install git-core
sudo apt-get install net-tools
sudo apt install software-properties-common
sudo add-apt-repository ppa:linuxuprising/java
sudo apt-get update
sudo apt install default-jdk
java -version
set JAVA_HOME
update-alternatives-config java
sudo su
cat >> /etc/environment <<EOL
JAVA_HOME=/usr/lib/jvm/java-11-openjdk-amd64
EOL
exit
```

Por último, al navegador Firefox se le instala el complemento “Auto Refresh Page” con el fin de obtener actualizaciones automáticas cada determinado tiempo de la interfaz gráfica de ONOS.

2. Instalación de Mininet-WiFi

La instalación de Mininet-WiFi requiere de la instalación previa de Mininet. El proceso sigue las siguientes instrucciones:

```
git clone https://github.com/mininet/mininet
cd mininet
git tag
git checkout -b 2.2.1
sudo ~/mininet/util/install.sh -a
cd ..
git clone https://github.com/intrig-unicamp/mininet-wifi
cd mininet-wifi
git tag
```

```
git checkout -b 2.2.1
sudo ~/mininet-wifi/util/install.sh -Wlnfv
```

3. Instalación de ONOS

La instalación de la controladora ONOS sigue el proceso descrito en la pagina oficial https://wiki.onosproject.org/display/ONOS/Installing+and+running+ONOS para administradores, la cual es descrita a continuación:

```
cd /opt
sudo wget -c https://repo1.maven.org/maven2/org/onosproject/onos-releases/2.5.1/onos-2.5.1.tar.gz
sudo tar xzf onos-2.5.1.tar.gz
sudo mv onos-2.5.1 onos
sudo cp /opt/onos/init/onos.initd /etc/init.d/onos
sudo cp /opt/onos/init/onos.service /etc/systemd/system/
sudo systemctl daemon-reload
sudo systemctl enable onos
sudo systemctl start onos.service
```

ANEXO 2

1. Instalación y configuración de OpenWrt, OpenVSwitch y NETCONF en los puntos de acceso inalámbrico y conmutador

La instalación del sistema operativo de OpenWrt se realiza desde una estación de trabajo Linux (Lubuntu 18.04 LTS) que opera como servidor de Protocolo de Transferencia de archivos Trivial (TFTP, *Trivial File Transfer Protocol*) y DHCP. Inicialmente se descargan de la página de https://openwrt.org el kernel de arranque y el script de actualización del sistema operativo en su versión 19.07.10 de acuerdo con las características del hardware de los AP. Y se transfieren al dispositivo mediante las siguientes instrucciones:

Script de arranque

```
#!/bin/bash
USER=root
IFNAME=enp1s0
FILENAME=openwrt-ipq40xx-mikrotik-mikrotik_hap-ac2-initramfs-kernel.bin
/sbin/ip addr replace 192.168.1.10/24 dev $IFNAME
/sbin/ip link set dev $IFNAME up
/usr/sbin/dnsmasq --user=$USER \
--no-daemon \
--listen-address 192.168.1.10 \
--bind-interfaces \
-p0 \
--dhcp-authoritative \
--dhcp-range=192.168.1.100,192.168.1.200 \
--bootp-dynamic \
--dhcp-boot=$FILENAME \
--log-dhcp \
--enable-tftp \
--tftp-root=$(pwd)
```

El script de arranque corre sobre la memoria flash del equipo un Kernel básico que permite copiar el archivo de instalación del sistema operativo y el acceso por Intérprete de Órdenes Seguro (SSH, *Secure Shell*) para su instalación bajo las instrucciones:

```
Scp openwrt-ipq40xx-mikrotik-mikrotik_hap-ac2-squashfs-sysupgrade.bin root@192.168.1.1:/tmp
ssh root@192.168.1.1
sysupgrade /tmp/openwrt-ipq40xx-mikrotik-mikrotik_hap-ac2-squashfs-sysupgrade.bin
```

Al terminar el reinicio del equipo es necesario acceder a través de SSH e instalar una interfaz gráfica denominada Luci, OpenVSwitch, Netopeer2-Server y algunas otras librerías:

**Configuración de contraseña para el usuario root y asignación de nombre para el equipo

```
opkg update
passwd
set system.@system[0].hostname='X'  // La X hacen referencia al nombre que se le asignara al equipo
uci commit
reload_config

**Intalación de herramientas adicionales
opkg install coreutils
opkg install coreutils-install
opkg install nano
opkg remove wpad-basic
opkg install hostapd

**Instalación de interfaz grafica
opkg install luci

**Intalación de conmitador openflow virtual
opkg install openvswitch
uci set openvswitch.ovs.disabled=0
uci set network.ovsbr=interface
uci set network.ovsbr.ifname=ovsbr
uci set network.ovsbr.proto=static
uci set network.ovsbr.type=bridge
uci commit
reload_config
/etc/init.d/openvswitch start

**Intalacion de servidor Netconf
opkg install netopeer2-server

**Borrado de reglas de firewall pre-existentes
while $(uci delete firewall.@rule[-1] 2>/dev/null); do :; done
while $(uci delete firewall.@zone[-1] 2>/dev/null); do :; done
while $(uci delete firewall.@forwarding[-1] 2>/dev/null); do :; done
uci commit
reload_config

**Borrado de servidores DHCP pre-instalados
uci delete dhcp.lan
uci delete dhcp.wan
uci commit
reload_config
```

Lo anteriormente mencionado aplica para los dos AP y el conmutador, pero la configuración de interfaces físicas e inalámbricas es diferente en los dos tipos de dispositivos. En el caso del conmutador OpenFlow se define de la siguiente manera:

```
nano /etc/config/networt
config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'
config interface 'lan'
        option type 'bridge'
        option ifname 'eth1.1'
```

```
        option proto 'static'
        option ipaddr '10.10.10.X' //Dirección IP asignada para el control
        option netmask '255.255.255.0'
config switch
        option name 'switch0'
        option reset '1'
        option enable_vlan '1'
        option ar8xxx_mib_type '0'
        option ar8xxx_mib_poll_interval '500'
config switch
        option name 'switch1'
        option reset '1'
        option enable_vlan '1'
config switch_vlan
        option device 'switch1'
        option vlan '1'
        option ports '1 2 3 4 5 0t'


config switch_vlan
        option device 'switch0'
        option vlan '2'
        option ports '1 0t'
config interface 'lan1'
        option ifname 'eth0.1'
        option proto 'static'

config switch_vlan
        option device 'switch0'
        option vlan '3'
        option ports '2 0t'
config interface 'lan2'
        option ifname 'eth0.2'
        option proto 'static'

config switch_vlan
        option device 'switch0'
        option vlan '4'
        option ports '3 0t'
config interface 'lan3'
        option ifname 'eth0.3'
        option proto 'static'

config switch_vlan
        option device 'switch0'
        option vlan '5'
        option ports '4 0t'
config interface 'lan4'
        option ifname 'eth0.4'
        option proto 'static'

config switch_vlan
        option device 'switch0'
        option vlan '6'
        option ports '5 0t'
config interface 'lan5'
        option ifname 'eth0.5'
```

```
        option proto 'static'

config interface 'ovsbr'
        option ifname 'br-lan'
        option proto 'static'
        option type 'bridge'
```

Para los AP la configuración de interfaces de red se establece de la siguiente forma:

```
nano /etc/config/networt
config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'
config interface 'wan'
        option ifname 'eth0'
        option proto 'static'
        option ipaddr '10.10.10.X' // Dirección IP asignada para el control
        option netmask '255.255.255.0'
        option gateway '10.10.10.1'
        list dns '8.8.8.8'
config switch 'eth1'
        option enable '1'
        option enable_vlan '1'
config switch_vlan
        option device 'eth1'
        option vlan '2'
        option ports '0t 1'
config interface 'lan1'
        option ifname 'eth1.1'
        option proto 'static'
config switch_vlan
        option device 'eth1'
        option vlan '3'
        option ports '0t 2'
config interface 'lan2'
        option ifname 'eth1.2'
        option proto 'static'
config switch_vlan
        option device 'eth1'
        option vlan '4'
        option ports '0t 3'
config interface 'lan3'
        option ifname 'eth1.3'
        option proto 'static'
config switch_vlan
        option device 'eth1'
        option vlan '5'
        option ports '0t 4'
config interface 'lan4'
        option ifname 'eth1.4'
        option proto 'static'

nano /etc/config/wireless
```

```
config wifi-device 'radio0'
        option type 'mac80211'
        option channel '11'
        option hwmode '11g'
        option path 'platform/ar934x_wmac'
        option htmode 'HT20'
config wifi-iface 'default_radio0'
        option device 'radio0'
        option mode 'ap'
        option ssid 'Employed'
        option encryption 'none'
config wifi-iface 'wifinet1'
        option device 'radio0'
        option mode 'ap'
        option ssid 'Guest'
        option encryption 'none'
reload_config
wifi up
```

Seguido de la configuración de las interfaces físicas se prosigue con la configuración de parámetros en el conmutador OpenFlow virtual:

```
ovs-vsctl --may-exist add-br ovsbr -- \
    set bridge ovsbr other-config:disable-in-band=true -- \
    set bridge ovsbr fail_mode=secure
ovs-vsctl --may-exist add-port ovsbr eth1.1 -- set Interface eth1.1 ofport_request=1
ovs-vsctl --may-exist add-port ovsbr eth1.2 -- set Interface eth1.2 ofport_request=2
ovs-vsctl --may-exist add-port ovsbr eth1.3 -- set Interface eth1.3 ofport_request=3
ovs-vsctl --may-exist add-port ovsbr eth1.4 -- set Interface eth1.4 ofport_request=4
ovs-vsctl --may-exist add-port ovsbr wlan0 -- set Interface wlan0 ofport_request=5
ovs-vsctl --may-exist add-port ovsbr wlan0-1 -- set Interface wlan0-1 ofport_request=6
ovs-vsctl show
ovs-ofctl show ovsbr | grep dpid
ovs-vsctl set-controller ovsbr tcp:10.10.10.10:6653
ovs-vsctl --may-exist add-br ovsbr -- \
    set controller ovsbr connection-mode=out-of-band
```

Por último, desde el enlace https://github.com/sartura/wireless-plugin/tree/master/yang se descargan el siguiente paquete:

terastream-wireless@2017-08-08.yang

Se transfieren a cada uno de los AP de la siguiente manera:

```
scp terastream-wireless@2017-08-08.yang root@X.X.X.X:/tmp
```

Posteriormente se ingresa al punto de acceso inalámbrico y se instalan bajo las siguientes instrucciones:

```
sysrepoctl --install --yang= terastream-wireless@2017-08-08.yang --owner=root:root --permissions=666
```

2. Configuración de IBGP SPEAKER

La preparación de este dispositivo se realiza desde al aplicativo WinBox, herramienta propia de mikrotik, que brinda una interfaz gráfica para su configuración. Para lo cual se abre una terminal y se ingresa las siguientes líneas de comando:

```
/interface ethernet
   set [ find default-name=ether1 ] name="ether1 - IBGP-->OFSW1"
   set [ find default-name=ether2 ] name="ether2 - IBGP-->SwitchCore"
   set [ find default-name=ether3 ] name="ether3 - IBGP-->ISP"
/routing bgp instance
   set default as=100 router-id=10.10.10.11
/ip address
   add address=192.168.100.1/24 interface="ether1 - IBGP-->OFSW1" network=\ 192.168.100.0
   add address=10.10.10.11/24 interface="ether2 - IBGP-->SwitchCore" network=\ 10.10.10.0
   add address=192.168.200.1/24 interface="ether1 - IBGP-->OFSW1" network=\ 192.168.200.0
/ip dhcp-client
   add add-default-route=no disabled=no interface="ether3 - IBGP-->ISP" \ use-peer-dns=no use-peer-
ntp=no
/ip firewall nat
   add action=masquerade chain=srcnat out-interface="ether3 - IBGP-->ISP"
/ip route
   add distance=1 gateway=192.168.20.1
/routing bgp network
   add network=192.168.100.0/24
   add network=192.168.200.0/24
/routing bgp peer
   add name=ONOS remote-address=10.10.10.10 remote-as=100 remote-port=2000
/system identity
   set name=IBGP-SPEAKER
/system routerboard settings
   set boot-protocol=dhcp force-backup-booter=yes reformat-hold-button=30s
```