



UNIVERSIDAD NACIONAL DE CÓRDOBA
FACULTAD DE CIENCIAS EXACTAS FÍSICAS Y
NATURALES

PROYECTO INTEGRADOR
INGENIERÍA EN COMPUTACIÓN

**Administración de un muxponder a través
de Redes Definidas Por Software**

Autor:

Matías KLEINER
37590431
kleiner.matias@gmail.com

Director:

Ing. Hugo CARRER

Co-director:

Matthew AGUERREBERRY

Julio 2019

Para mi familia...

Administración de un muxponder a través de Redes Definidas Por Software

Matías KLEINER

Resumen

En respuesta al continuo incremento de los requerimientos en las redes de transporte, surgen no sólo avances en las capacidades de los dispositivos ópticos, sino también en los métodos de configuración en los mismos. La flexibilidad y la estandarización de las configuraciones pasan de ser una característica deseable, a ser un requerimiento funcional en los equipos. En las empresas de telecomunicaciones, donde dispositivos de diferentes características y fabricantes interactúan a la hora de brindar servicios, es crucial que exista un protocolo estándar y un ente centralizado de administración. Históricamente esta comunicación se llevó a cabo a través del protocolo *SNMP*, sin embargo las necesidades de las redes actuales involucran capacidades que exceden a este protocolo.

Este contexto da lugar al protocolo de configuraciones de red, también llamado *NETCONF*, que se establece como un protocolo estandarizado por la *Internet Engineering Task Force (IETF)*, que provee tanto funciones de control (ej. configuración del plano de datos) como así también funciones de administración (ej. acceso a información de monitoreo). Depende de *Yet Another Next Generation (YANG)* para describir las configuraciones de los dispositivos de manera estándar. Tanto *NETCONF* como *YANG*, se volvieron foco de interés de los operadores de red en busca de un estándar de configuración abierto.

Al mismo tiempo, surge un nuevo paradigma de arquitectura de redes: Las Redes Definidas por Software (*SDN* por sus siglas en inglés), una propuesta para solucionar la creciente complejidad en la administración de las redes. *SDN* propone la separación del plano de datos y el plano de control, logrando de este modo un plano de control centralizado facilitando no solo el control sino también la administración de las redes.

En este proyecto integrador se busca, en primer lugar, adquirir en su totalidad los conocimientos involucrados con *SDN* y administración de la configuración de los dispositivos de red. El objetivo será configurar un dispositivo óptico llamado muxponder, para ello se deberá adaptar el protocolo *NETCONF* al equipo. Además, será necesario implementar un *driver* en la interfaz *southbound* del controlador *SDN*. Así mismo, se genera una interfaz de usuario para la administración sencilla de los dispositivos presentes en la topología. Además, se desarrolla un ambiente para la verificación y validación de las aplicaciones. Finalmente, se brindan distintas ideas para mejorar lo aquí implementado y posibles vías para continuar trabajando en el ámbito de las redes definidas por software.

Agradecimientos

Muchas gracias a mi familia, por el apoyo incondicional a lo largo de todos estos años de estudio.

Este proyecto no hubiera sido posible sin el soporte, la confianza, la supervisión y el duro empeño de mis directores, Hugo Carrer y Matthew Aguerreberry.

Un especial agradecimiento a mis amigos y todas las personas que tuve el placer de conocer durante estos años de carrera.

Agradezco a la Fundación Fulgor y a la Fundación Tarpuy, y a todo su personal, por las oportunidades y enseñanzas compartidas.

Finalmente, agradezco a la Facultad de Ciencias Exactas Físicas y Naturales de la Universidad Nacional de Córdoba por la oportunidad de realizar esta carrera de grado.

Índice general

Resumen	V
Agradecimientos	VII
1. Introducción	1
1.1. Motivación e importancia del proyecto	2
1.2. Estado del arte	2
1.3. Objetivos propuestos	6
1.3.1. Objetivos particulares	6
1.4. Estructura del texto	6
2. Marco teórico	9
2.1. Redes tradicionales	9
2.1.1. Plano de Control	10
2.1.2. Plano de Datos	10
2.2. Redes Definidas por Software	11
2.2.1. Definición de <i>SDN</i>	11
2.2.2. Arquitectura de <i>SDN</i>	12
Plano de Datos	12
Plano de Aplicación	12
Plano de Control	12
2.3. Gestión de la Red	13
2.3.1. Protocolos de Gestión	13
<i>Command Line Interface</i>	13
<i>Simple Network Management Protocol</i>	14
Otras alternativas	15
2.3.2. <i>NETCONF</i>	15
Definición	16
Conceptos del Protocolo	17
Capacidades	17
Sesión orientada a la conexión	18
Sesión orientada a la autenticación	18
Bases de datos	18
Operaciones del protocolo	19
Notificaciones	21
2.3.3. Lenguaje de Modelado <i>YANG</i>	23
Conceptos del Lenguaje	23
Módulos y submódulos	23
Declaraciones y Definiciones de Datos	24
Identificador de instancia	24
Funcionalidades	25

2.3.4. Redes Ópticas de Transporte	25
Transponders y Muxponders	26
Aplicaciones	27
3. Análisis de las tecnologías	29
3.1. Herramientas de Hardware	29
3.1.1. <i>Muxponder 40GB</i>	29
3.1.2. Componentes del <i>muxponder</i>	31
3.1.3. Aplicaciones integradas en el dispositivo	32
3.2. Herramientas de Software	33
3.2.1. Controlador <i>ONOS</i>	33
Arquitectura del controlador	34
Interfaz <i>Southbound</i> en <i>ONOS</i>	35
Justificación de la elección del controlador	36
3.2.2. Análisis de agentes <i>NETCONF</i>	37
Sysrepo	37
Yuma123	37
Evaluación de las implementaciones	38
Justificación de elección del agente	40
4. Diseño e Implementación	43
4.1. Entorno de trabajo	43
4.1.1. Topología	43
4.1.2. Requerimientos del sistema	44
4.2. Integración del protocolo <i>NETCONF</i> al <i>muxponder</i>	47
4.2.1. Requerimientos	47
4.2.2. Compilación e instalación del agente	47
4.2.3. Diseño del módulo <i>YANG</i>	48
4.2.4. Diseño de la librería C para el agente <i>NETCONF</i>	51
4.3. Diseño del <i>driver</i>	53
4.3.1. Requerimientos	53
4.3.2. Descubrimiento del dispositivo	54
4.3.3. Descubrimiento de Enlaces	55
4.3.4. Operaciones definidas en el <i>driver</i>	57
4.4. Diseño de la interfaz <i>Northbound</i> e Interfaz de usuario	59
4.4.1. Requerimientos	60
4.4.2. Implementación de la <i>REST</i>	61
4.4.3. Implementación de la interfaz de usuario	62
5. Validación y Verificación	69
5.1. Verificación del agente <i>NETCONF</i>	69
5.1.1. Escenario	69
5.1.2. Matriz de trazabilidad	70
5.1.3. Casos de prueba y resultados	70
Caso de Prueba T-R-01	70
Caso de Prueba T-R-02	71
Caso de Prueba T-R-03	72
5.2. Verificación del <i>driver</i>	74
5.2.1. Escenario	74

5.2.2. Matriz de trazabilidad	75
5.2.3. Casos de prueba y resultados	75
Caso de Prueba T-R-04	75
Caso de Prueba T-R-05	76
5.3. Verificación de la interfaz gráfica y la interfaz <i>REST</i>	79
5.3.1. Escenario	79
5.3.2. Matriz de trazabilidad	79
5.3.3. Casos de prueba y resultados	80
Caso de Prueba T-R-06	80
Caso de Prueba T-R-07	81
Caso de Prueba T-R-08	82
Caso de Prueba T-R-09	84
6. Conclusión	89
6.1. Problemas y limitaciones	90
6.2. Continuidad del trabajo	90
6.3. Aporte personal	91
A. Tutorial para desplegar el entorno y las aplicaciones desarrolladas	93
A.1. Instalación del agente en el dispositivo	93
A.2. Inicio del controlador ONOS	94
A.3. Interfaz gráfica	94
A.4. Código fuente de la aplicación	95
Bibliografía	97

Índice de figuras

1.1.	Topología utilizada en las pruebas de	2
1.2.	Resultados obtenidos en	3
1.3.	NETCONF como protocolo para la administración.	4
1.4.	NETCONF como protocolo para el monitoreo.	4
1.5.	Topología propuesta en	5
1.6.	Escenario propuesto para las pruebas en	5
2.1.	Comportamiento de dispositivos en redes tradicionales.	9
2.2.	Arquitectura de un controlador <i>SDN</i> tradicional.	13
2.3.	Operaciones típicas en <i>SNMP</i>	15
2.4.	Separación conceptual del protocolo NETCONF.	16
2.5.	Arquitectura cliente-servidor en el protocolo NETCONF.	17
2.6.	Ejemplo de comunicación entre cliente y servidor NETCONF.	22
2.7.	Estructura de un módulo YANG.	23
2.8.	Ejemplo de identificador de instancia en YANG.	24
2.9.	Funcionamiento básico de un <i>transponder</i>	26
2.10.	Funcionamiento básico de un <i>muxponder</i>	27
2.11.	Separación de la red en capa de paquetes y capa de transporte.	28
3.1.	Vista del panel frontal del <i>muxponder</i> de 40GB utilizado.	30
3.2.	Diagrama en bloques del <i>muxponder</i> de 40GB.	31
3.3.	Vista de la circuitería del <i>muxponder</i> de 40GB.	31
3.4.	Sección XFP de la aplicación 'monitor'.	32
3.5.	Configuración mediante la aplicación ' <i>muxponder</i> '.	33
3.6.	Arquitectura distribuida de <i>ONOS</i>	34
3.7.	Arquitectura completa del controlador <i>ONOS</i>	35
3.8.	Interfaz <i>Southbound</i> en <i>ONOS</i>	36
3.9.	Demandas de recursos de las implementaciones analizadas.	40
4.1.	Topología implementada en el proyecto.	44
4.2.	Conexión física de la topología.	44
4.3.	Caso de uso desde la perspectiva del administrador.	44
4.4.	Requerimientos del sistema.	45
4.5.	Diagramas de actividad del sistema.	46
4.6.	Requerimientos para la integración del protocolo NETCONF.	47
4.7.	Diagrama de actividad de las operaciones síncronas con el cliente. . . .	52
4.8.	Diagrama de actividad de las notificaciones.	53
4.9.	Requerimientos para el <i>driver</i> de la interfaz <i>Southbound</i>	54
4.10.	Diagrama de actividad de la función <i>DeviceDescriptionDiscovery</i>	55
4.11.	Diagrama de actividad de la función <i>LinkDiscovery</i>	56
4.12.	Diagrama de actividad para la RPC 'mux-apply-config', sin vecinos. .	58

4.13. Diagrama de actividad para la <i>RPC 'mux-apply-config'</i> , con vecinos.	59
4.14. Interfaz <i>REST</i> e interfaz de usuario.	60
4.15. Requerimientos de las interfaces <i>REST</i> e interfaz gráfica.	60
4.16. Fragmento de la interfaz <i>REST</i> implementada.	62
4.17. Consulta periódica por las alarmas al controlador <i>ONOS</i>	63
4.18. Interfaz de la vista principal.	64
4.19. Agregar dispositivo a través de la APP <i>WEB</i>	64
4.20. Configurar un dispositivo a través de la APP <i>WEB</i>	65
4.21. Interfaz de la vista de alarmas.	66
4.22. Interfaz de la vista de configuración.	66
4.23. Interfaz de la vista de estado.	66
4.24. Interfaz de la vista de topología.	67
4.25. Interfaz de la vista de administración perfiles de configuración.	68
5.1. Topología utilizada para las pruebas relativas a la integración del protocolo <i>NETCONF</i>	69
5.2. Consulta al <i>container mux-state-XFP1</i>	72
5.3. Suscripción y <i>RPC 'mux-apply-config'</i>	74
5.4. Topología utilizada para las pruebas relativas al <i>driver</i>	74
5.5. Información de dispositivos presentes en la topología de <i>ONOS</i>	76
5.6. Vista de la topología de <i>ONOS</i> - Dispositivos sin configurar.	78
5.7. Vista de la topología de <i>ONOS</i> - Dispositivos configurados.	78
5.8. Vista de la topología de <i>ONOS</i> - Dispositivos configurados, con un enlace desconectado.	78
5.9. Topología utilizada para las pruebas relativas a la interfaz gráfica e interfaz <i>REST</i>	79
5.10. Alarmas visualizadas en la interfaz gráfica.	81
5.11. Alarmas visualizadas en la <i>CLI</i> del controlador.	82
5.12. Alarmas visualizadas en 'monitor' en uno de los <i>muxponders</i>	82
5.13. Datos de estado, observados desde la interfaz gráfica.	83
5.14. Datos de estado, observados desde 'monitor'.	84
5.15. Detección de configuración inconsistente entre dispositivos vecinos.	86
5.16. Prueba fallida de conectividad entre <i>host A</i> y <i>host B</i>	86
5.17. Detección de configuración consistente entre dispositivos vecinos.	87
5.18. Prueba exitosa de conectividad entre <i>host A</i> y <i>host B</i>	87

Índice de cuadros

2.1. Ejemplo de operaciones disponibles en <i>NETCONF</i>	21
5.1. Matriz de trazabilidad - Verificación del protocolo <i>NETCONF</i>	70
5.2. Caso de Prueba T-R-01	71
5.3. Caso de Prueba T-R-02	71
5.4. Caso de Prueba T-R-03	73
5.5. Matriz de trazabilidad - Verificación del <i>driver</i>	75
5.6. Caso de Prueba T-R-04	76
5.7. Caso de Prueba T-R-05	77
5.8. Matriz de trazabilidad - Verificación de la interfaz <i>REST</i> e interfaz gráfica	80
5.9. Caso de Prueba T-R-06	80
5.10. Caso de Prueba T-R-07	81
5.11. Caso de Prueba T-R-08	83
5.12. Caso de Prueba T-R-09	85

Lista de acrónimos

API	Application Programming Interface
CLI	Command Line Interface
SNMP	Simple Network Management Protocol
FIB	Forwarding Information Base
GUI	Graphical User Interface
ONF	Open Networking Foundation
IETF	Internet Engineering Task Force
RIB	Routing Information Base
SDN	Software Defined Network
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
MIB	Management Information Base
TLS	Transport Layer Security
SSH	Secure SHell
OTN	Optical Transport Network
OTU	Optical Transport Unit
ITU	International Telecommunication Union
RFC	Request For Comments
RPC	Remote Procedure Call
XML	EXtensible Markup Language
YANG	Yet Another Next Generation
NETCONF	NETwork CONFiguration Protocol
IANA	Internet Assigned Numbers Authority
FEC	Forward Error Correction
FPGA	Field Programmable Gate Array
ONOS	Open Network Operating System
REST	REpresentational State Transfer
BSD	Berkeley Software Distribution
MIT	Massachusetts Institute Technology
MB	Mega Bytes
TB	Tera Bytes
NFV	Network Function Virtualization

Capítulo 1

Introducción

Las redes de telecomunicaciones crecen a medida que surgen nuevas tecnologías (redes inalámbricas 4G y 5G, *WiMax*, *LTE*, etc), seguido de la demanda en alza del ancho de banda por parte de los usuarios, requiriendo así cada vez mayor velocidad y mejor calidad de servicio. De esta forma, los operadores de red se ven obligados a aumentar la cantidad de dispositivos para satisfacer las necesidades de los usuarios, lo que constituye un desafío y un problema para los administradores de red, donde serán necesarios mecanismos de configuración que se adapten a las nuevas necesidades.

Así, el paradigma actual de implementación de redes resulta difícil de adaptar a estos nuevos cambios en los requerimientos, por ejemplo:

- La complejidad y el tamaño de las redes ha crecido considerablemente, esto genera gran resistencia al cambio en los operadores ya que el riesgo de provocar una falla es mayor.
- Dependencia de un fabricante, la falta de compatibilidad entre fabricantes fuerza a los operadores a quedar atados a los ciclos de diseño de un fabricante determinado y no les permite configurar la red de manera óptima dadas sus necesidades particulares.

Desde el punto de vista de la infraestructura de comunicación, el mejor candidato para resolver este problema son las *SDN* con la propuesta de separar el plano de control del plano de datos de los dispositivos, logrando una interfaz abierta entre ambos. De esta forma, se logra con *SDN* que los equipos puedan ser vistos como una caja blanca, donde los mismos pueden relacionarse con independencia de fabricante.

Por otra parte y desde el punto de vista de la gestión de la configuración, *NETCONF* surge como una solución simple y estándar para la gestión de la configuración, donde el mismo proporciona a los operadores y administradores de red un *framework* y un conjunto de métodos *RPC* basados en codificación *XML* para gestionar (instalar, modificar y borrar) la configuración de los elementos de red.

En el transcurso de este capítulo se introducen los aspectos más significativos del proyecto. Se comienza describiendo las motivaciones principales que han llevado al desarrollo de este trabajo. Luego, se expone el estado actual de las tecnologías directamente relacionadas, continuando con los objetivos planteados y finalizando con una descripción de la organización del texto.

1.1. Motivación e importancia del proyecto

Se exponen a continuación las razones principales que incentivaron la realización de este trabajo de fin de grado.

- Oportunidad de incursionar en el estudio de sistemas de administración de redes de vanguardia.
- La aplicación de los conocimientos adquiridos a lo largo de la carrera de Ingeniería en Computación.
- Posibilidad de desarrollar un sistema de administración de redes en su totalidad.
- Oportunidad de trabajar en un entorno con diversos dispositivos, presentes en las distintas capas de la red y destacando la presencia de un dispositivo óptico de transporte de red, el *muxponder* de 40GB.

1.2. Estado del arte

En la presente sección se hace un estudio del estado de las tecnologías directamente relacionadas al proyecto, con el objetivo de fijar un marco de comparación y diferenciar el trabajo realizado. Particularmente, se presenta una visión global de las implementaciones existentes más relevantes relacionadas a la administración de la configuración y al esquema de redes definidas por software.

Protocol Efficiencies of NETCONF versus SNMP for Configuration Management Functions

En [4] se presenta una comparación entre el protocolo NETCONF y el protocolo SNMP. Para ello, se conforma la topología que puede verse en la figura 1.1, utilizando como agente NETCONF y agente SNMP la implementación 'ConfD' de Cisco.

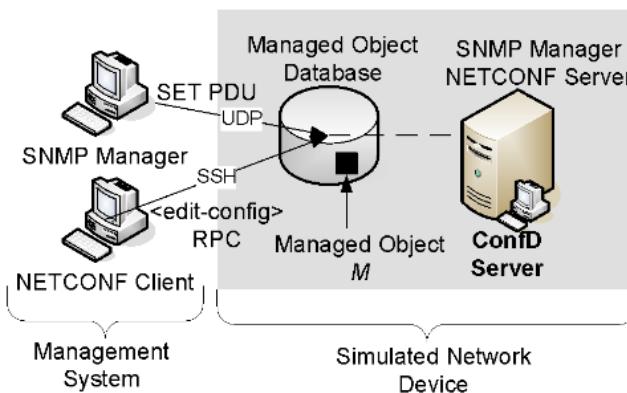


FIGURA 1.1: Topología utilizada en las pruebas de [4].

Las pruebas realizadas por los autores arrojan los resultados observados en la figura 1.2, donde M representa la cantidad de operaciones a realizar por parte del servidor. Los autores mencionan que en los resultados obtenidos no se tiene en cuenta la carga que tienen los paquetes debido a la seguridad que ofrece el transporte SSH

por parte de *NETCONF*, tampoco la carga que presenta *TCP* (*NETCONF*) frente a *UDP* (*SNMP*), entre otros.

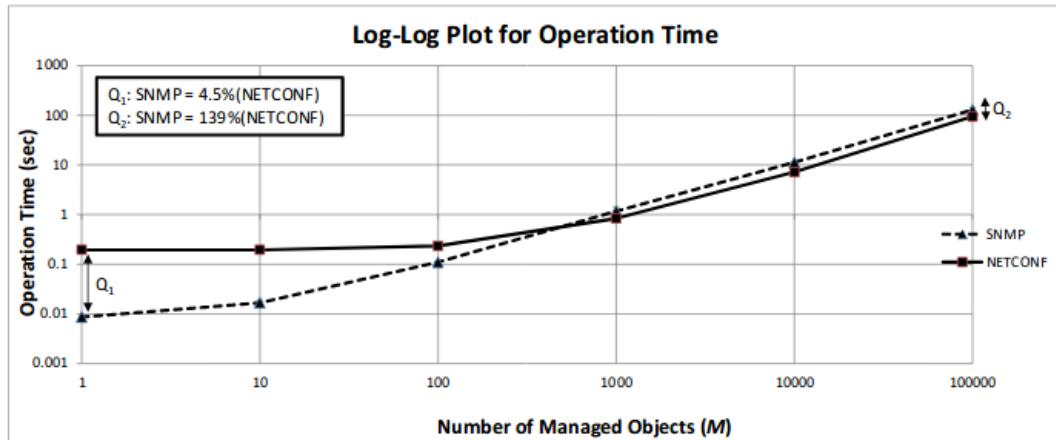


FIGURA 1.2: Resultados obtenidos en [4].

En las conclusiones de este artículo mencionan que *NETCONF* es una clara alternativa a *SNMP* en ámbitos de gestión de la configuración de la red. Además, destacan las bondades que presenta el protocolo *NETCONF* frente a *SNMP* para los proveedores de servicio como ser la seguridad de los mensajes mediante *SSH*, la capacidad de revertir una configuración, el transporte de los mensajes mediante un protocolo orientado a la conexión, etc.

Evaluating the Network Management Capabilities of YANG and NETCONF

En el artículo [37] se realiza un estudio de las diferentes alternativas existentes en el ámbito de la configuración y gestión de la red. A su vez, el autor desarrolla un prototipo de servidor *NETCONF*. Los experimentos realizados por el autor tienen como objetivo determinar la capacidad que tienen los diferentes protocolos de gestión de configuración y monitoreo para adaptarse a entornos de *SDN* y *NFV*.

Así, separa las pruebas realizadas en dos partes. En primer lugar, evalúa alternativas que permiten la configuración de un dispositivo de red. Luego, realiza un análisis de las alternativas relacionadas al monitoreo de un equipo de red.

La figura 1.3 muestra una gráfica de los resultados obtenidos para el primer caso, donde concluye que *NETCONF* se adapta bien a los entornos *NFV* ya que se encuentra específicamente diseñado para la configuración de los equipos. Sin embargo, menciona que puede presentar dificultades adaptar el protocolo *NETCONF* a entornos *SDN* ya que no cumple estrictamente con el paradigma de las *SDN*, donde el plano de control y el plano de datos se encuentran desacoplados íntegramente.

Por otra parte, la figura 1.4 muestra el análisis para el segundo caso, en donde se evalúan protocolos y alternativas para el monitoreo de la red. En este caso, el autor menciona que si bien *NETCONF* permite monitoreo en entornos *NFV* y *SDN*, el uso enfocado explícitamente a esta tarea no presenta mejores resultados que, por ejemplo, *SNMP*.

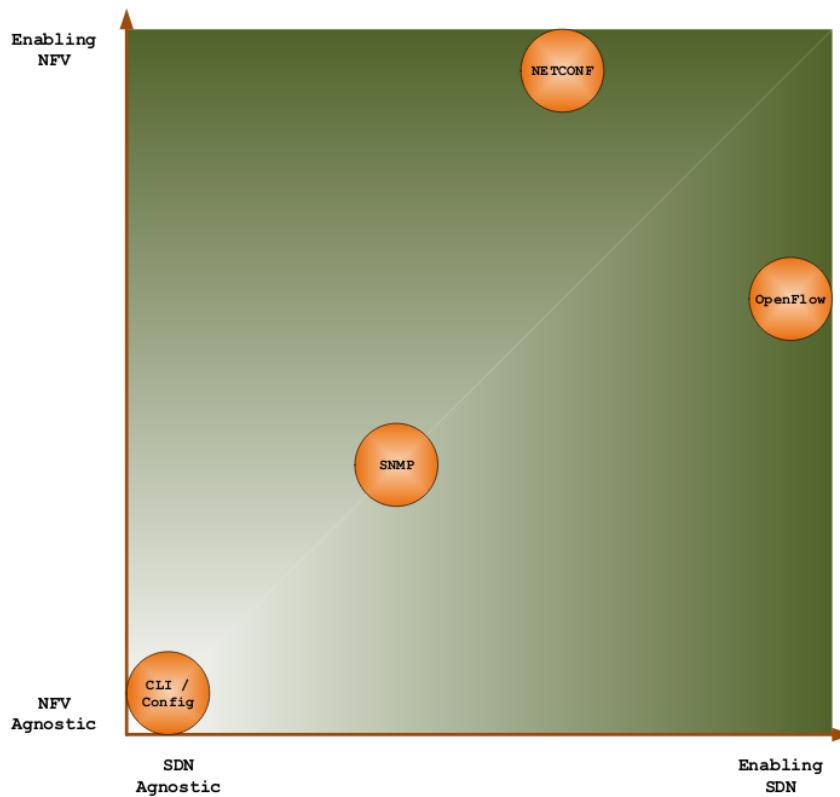


FIGURA 1.3: NETCONF como protocolo para la administración [37].

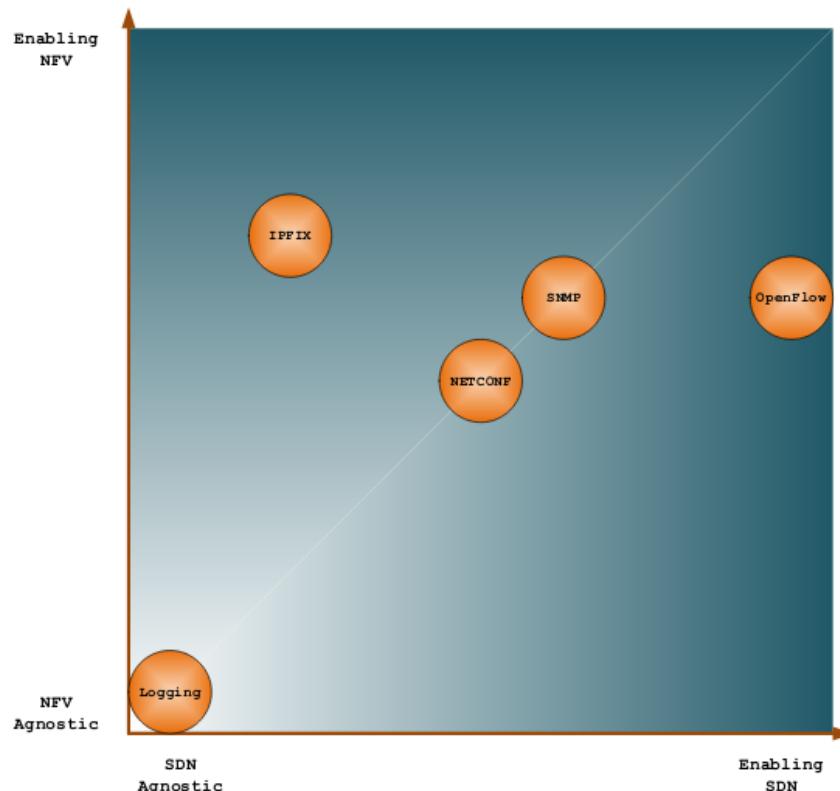


FIGURA 1.4: NETCONF como protocolo para el monitoreo [37].

Control and Management of Transponders With NETCONF and YANG

El documento [16] propone la utilización del protocolo de administración NETCONF en un ambiente SDN para administrar la configuración de un *transponder*, sugiriendo un entorno como el que se puede ver en la figura 1.5.

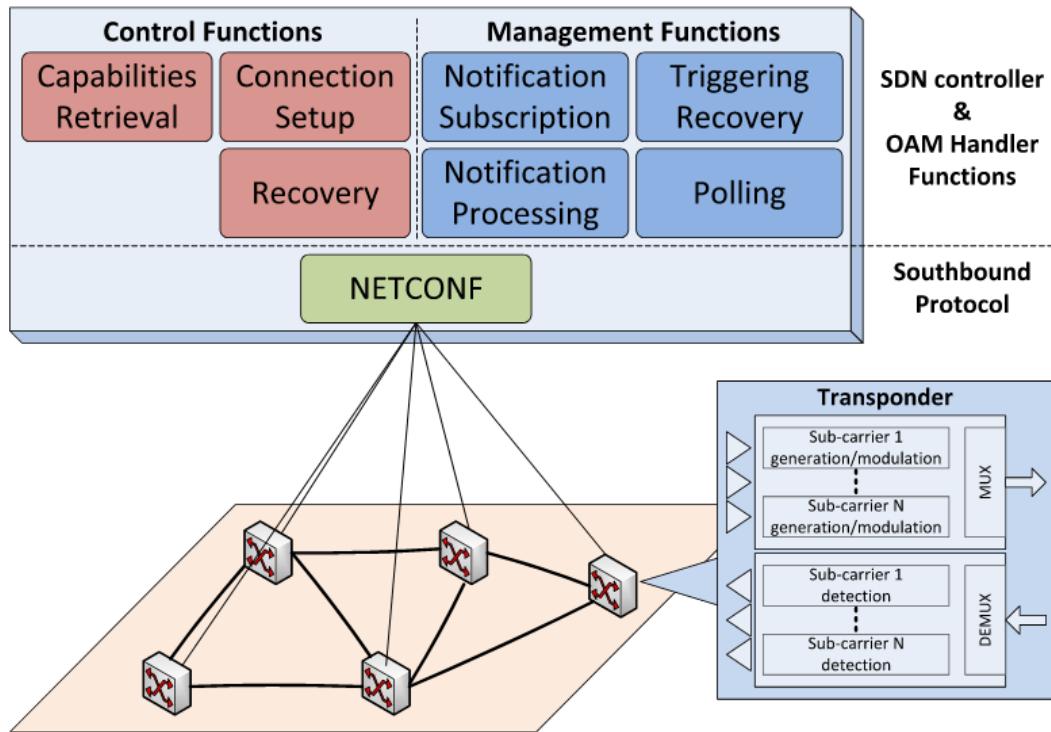


FIGURA 1.5: Topología propuesta en [16].

Sin embargo, finalmente realizan una demostración compuesta por dos *transponders* y un *switch*, los tres virtuales y sin utilización de algún controlador SDN. Esta última topología se muestra en la figura 1.6.

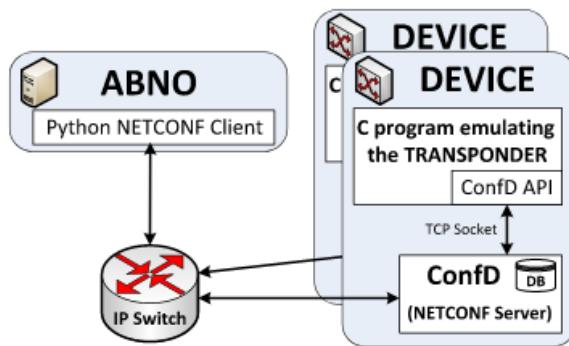


FIGURA 1.6: Escenario propuesto para las pruebas en [16].

Los autores concluyen que NETCONF como protocolo de gestión y YANG como modelado de datos, son estándares viables para la configuración, gestión y monitoreo de los datos en dispositivos de red como los *transponders*. Además, resaltan el alto rendimiento obtenido en sus pruebas para la configuración y monitoreo de los *transponders* haciendo uso de estos protocolos.

1.3. Objetivos propuestos

El objetivo general de este proyecto integrador es adquirir los conocimientos relacionados con administración de redes, particularmente con el esquema conocido como Redes Definidas por Software y el protocolo de administración de la configuración NETCONF. Para esto, se propone usar como vehículo de prueba un entorno constituido por ambas tecnologías para lograr la administración y monitoreo del estado de un *muxponder*. Se prestará particular atención al estudio y comparación de las diferentes opciones abiertas disponibles para la implementación del protocolo NETCONF.

1.3.1. Objetivos particulares

Las tareas a realizar en este trabajo de fin de grado llevarán a:

- Adquirir un amplio conocimiento de las tecnologías existentes en SDN.
- Tener un conocimiento acabado en el protocolo de administración de red NETCONF.
- Desarrollar una librería en el controlador SDN que permita la comunicación, a través de NETCONF, con un dispositivo óptico.
- Compilar e instalar en un dispositivo óptico un agente del protocolo NETCONF y una librería que relacione las variables de configuración y estado del dispositivo con dicho agente.
- Desarrollar una aplicación de interfaz de usuario para administrar de manera simple los dispositivos de red.

1.4. Estructura del texto

Aquí se listan los distintos capítulos que conforman el proyecto, presentando una breve descripción de su contenido. El escrito está compuesto por 6 capítulos, los apéndices y la bibliografía.

- **Capítulo 1 - Introducción:** Se exponen en este capítulo los aspectos más significativos del proyecto, donde se incluye las motivaciones que llevaron a realizar el mismo junto con una revisión del estado del arte relacionado y los objetivos propuestos para el trabajo de fin de grado.
- **Capítulo 2 - Marco teórico:** Aquí se abordan los conceptos necesarios para comprender las tecnologías utilizadas por el proyecto, además los mismos presentan una fundamentación para las posteriores implementaciones prácticas.
- **Capítulo 3 - Análisis de las tecnologías:** Se estudia y analiza en este capítulo todas las herramientas que permiten la implementación de las aplicaciones desarrolladas en este proyecto, abarcando tanto herramientas de software como de hardware.

- **Capítulo 4 - Diseño e implementación:** En este capítulo se abordan los procesos de diseño e implementación de todas las aplicaciones realizadas. Se presentan los requerimientos de las mismas y los diferentes diagramas realizados que explican el funcionamiento de cada pieza de software.
- **Capítulo 5 - Validación y verificación:** Aquí, se exponen los diferentes casos de prueba desarrollados con el objetivo de validar y verificar que se cumplan los requerimientos de las diferentes aplicaciones.
- **Capítulo 6 - Conclusión:** Se presenta en este capítulo las conclusiones obtenidas tras la realización del trabajo, posibles vías de trabajos futuros y una apreciación personal del proceso abordado.
- **Apéndices:** En los apéndices se proporciona al lector un tutorial de como desplegar el entorno de trabajo y las aplicaciones desarrolladas en este proyecto.
- **Bibliografía:** En esta parte final del documento, se muestran todas las referencias que se han consultado para el desarrollo del proyecto.

Capítulo 2

Marco teórico

En este capítulo se comprenderán conceptos teóricos sobre las tecnologías claves en las cuales se basa el proyecto. Como introducción, se analizará el funcionamiento de las redes tradicionales, donde se dejará en evidencia la necesidad de un nuevo paradigma.

Luego, se analizarán los fundamentos en los que se basan las Redes Definidas por Software y por qué este paradigma resuelve los problemas presentados por el enfoque de las redes tradicionales.

También, se introducirán conceptos de lenguajes de modelado y se abordará la importancia de la gestión de la red. Se estudiará NETCONF como protocolo de gestión de red. Finalmente, se abordan conceptos de dispositivos ópticos de transporte.

2.1. Redes tradicionales

La infraestructura actual de las redes tradicionales basa su funcionamiento íntegramente en los dispositivos de red [8]. Cada dispositivo lleva su propia gestión sobre el plano de datos y el plano de control de manera local y comunica a los demás dicha información de ser necesario.

Un ejemplo de esto se puede observar en la figura 2.1, donde dos dispositivos intercambian información referente al plano de control.

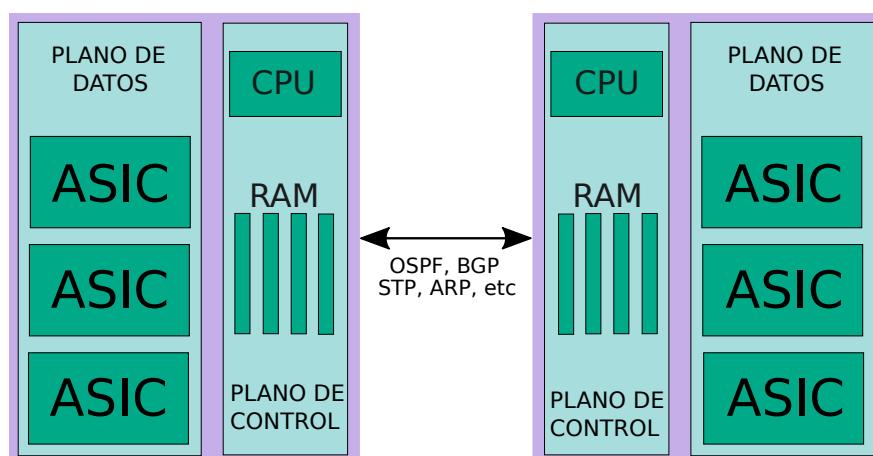


FIGURA 2.1: Comportamiento de dispositivos en redes tradicionales.

2.1.1. Plano de Control

Comprende la configuración del sistema, la administración y el intercambio de información de ruteo entre los dispositivos [38]. Es el responsable de administrar la configuración del equipo y de programar el camino que será usado para el flujo de los paquetes. En otras palabras, es en este plano donde se calculan y se toman las decisiones de enrutamiento y reenvío. En las redes tradicionales, cualquier aplicación que utilice el dispositivo para administrar su configuración reside en esta capa.

El proceso de establecimiento de la topología de red utilizando un plano de control que se ejecuta localmente, es compleja debido a que no existe ningún dispositivo que sea conocido por toda la red. Para gestionar cambios o actualizaciones en cada dispositivo se debe estar conectado a su plano de control de forma individual, lo que no resulta en un enfoque inteligente.

2.1.2. Plano de Datos

También conocido como plano de usuario o plano de reenvío [36], es el encargado de transportar el tráfico de usuario hacia el destinatario final. Tiene como objetivo el reenvío de los paquetes hacia el próximo salto basándose en las decisiones tomadas por la capa de control.

El enfoque dado por las redes tradicionales cumplió con las necesidades de una época donde las arquitecturas cliente-servidor eran dominantes. Tiene como ventaja ser simple a nivel lógico, mientras que el plano de control implica el uso de microprocesadores para tratar los paquetes y conformar las tablas, el plano de datos se desarrolla en silicio. A pesar de ello, presenta una serie de problemas [10]:

- **Funcionalidad de la red integrada en los dispositivos:** El plano de control se encuentra íntegramente en los dispositivos de red, lo que resulta en una configuración de red estática, inflexible y descentralizada.
- **Escalabilidad:** La escalabilidad resulta afectada y no apropiada para la explosión de las nuevas tecnologías como *Big Data*, *Cloud Computing* y el *Streaming*, donde la complejidad de la red incrementa rápidamente debido a que cada dispositivo agregado debe ser configurado y administrado.
- **Políticas inconsistentes:** Si las políticas de configuración cambian a nivel de red, implica un cambio en todos los dispositivos que la componen por parte de los administradores de red.
- **Dependencia del fabricante y personalización:** El plano de control integrado a los dispositivos de red resulta en una dependencia a los ciclos de producción de equipamientos por parte de los fabricantes para incorporar nuevas funcionalidades. Además, con la finalidad de asegurar la calidad de servicio y brindar alta *perfomance*, la industria define los protocolos de red de forma específica y aislada, sin el beneficio de una acción conjunta e incapacitando a los operadores a personalizar la red para sus entornos individuales y específicos.

2.2. Redes Definidas por Software

A diferencia de las aplicaciones y los nuevos requerimientos de los usuarios, las redes no han cambiado mucho respecto a los últimos 30 años [9]. El desarrollo de las SDN se inició en 1990 donde se introdujo el concepto de funciones programables en la red, teniendo gran innovación en 2001-2007 donde se propone separar el plano de datos del plano de control. El próximo gran paso de las SDN llegó en 2007-2010, con la implementación de la *API OpenFlow*.

Las redes definidas por software nacen en respuesta a la dinámica y flexibilidad que requieren las nuevas tendencias, donde el enfoque presentado por las redes tradicionales no cumple dado su naturaleza estática.

2.2.1. Definición de SDN

Según la ONF [10], la red definida por software, también conocida como red programable o automatizada, consiste en una arquitectura donde el plano de datos se encuentra separado del plano de control y donde este último a su vez puede controlar varios dispositivos.

Tal como destaca *SDx Central* en su reporte [15], este nuevo paradigma presenta las siguientes ventajas:

- **Plano de control centralizado:** A diferencia del enfoque presentado por las redes tradicionales donde se tenía un plano de control distribuido entre los diferentes equipos que conforman la red, ahora se tiene un plano de control centralizado y presente a nivel lógico en un mismo punto. De esta forma, se tiene una visión general y global de toda la red, relajando las comunicaciones entre los dispositivos y las complejidades introducidas por las configuraciones individuales de cada uno. Además, el plano de control ahora es directamente programable, sin tener que usar como intermediario el plano de datos. Todo el tráfico ahora está bajo la supervisión de este nuevo plano de control centralizado, transformando a la red en una red programable.
- **Costos:** Los costos relacionados al control de la gestión del tráfico y de configuración de los diferentes equipos se ven reducidos en tiempo y esfuerzo dado el plano de control centralizado.
- **Automatización:** Un beneficio indirecto de tener un plano de control centralizado, es poder tomar diferentes decisiones y políticas en base a la visibilidad global de la red en tiempo real, aplicando configuraciones en los diferentes equipos de forma automática.
- **Escalabilidad:** SDN admite topologías dinámicas con capacidades para adaptarse a cambios, debido a la automatización de la configuración de los dispositivos. Con la capacidad de ajustar los picos y las bajas en la carga del tráfico, las empresas pueden crear e implementar nuevos servicios y aplicaciones sin demora debido a la infraestructura más flexible.
- **Mantenimiento y monitoreo:** Por medio del controlador SDN se puede conocer, en cualquier momento, el estado actual de la red incluyendo los dispositivos que la componen.

- **Seguridad:** Dado que la administración de toda la red se realiza en un solo punto, se asegura que no existan debilidades o inconsistencias en las configuraciones de las aplicaciones y los equipos.

2.2.2. Arquitectura de SDN

En las redes tradicionales, cada dispositivo tiene integrado tanto el plano de datos como el plano de control. En *SDN*, el plano de datos se encuentra desacoplado del plano de control y, además, se puede diferenciar un nuevo plano llamado *plano de aplicación* [39]. A continuación, se analizará cuál es la función que cumple cada plano en esta nueva arquitectura propuesta por las *SDN*.

Plano de Datos

Comprende la misma funcionalidad que en las redes tradicionales. Consiste en un conjunto de dispositivos de red con funcionalidades de reenvío de paquetes.

Plano de Aplicación

Con el enfoque de las redes tradicionales, el plano de aplicación se encontraba integrado en el plano de control. En *SDN*, el plano de aplicación se desacopla al igual que el plano de control. En este plano se encuentran las aplicaciones de red que implementan las funcionalidades de más alto nivel y que participan en las decisiones de administración y control de ruteo.

Plano de Control

Toda la función de control se encuentra centralizada fuera de los dispositivos, permitiendo a los desarrolladores de aplicaciones utilizar las capacidades de la red pero haciendo una abstracción de su topología o sus funciones. Tiene como objetivo mediar, organizar y facilitar la comunicación entre los diferentes equipos y las aplicaciones. Además, este plano ahora está disponible para poder ser programado desde un software externo al controlador.

En la figura 2.2, se expone la anatomía de un controlador *SDN*. En ella, se puede observar dos interfaces comprendidas por el plano de control [44]: *Southbound* y, *Northbound*.

- ***Southbound API:*** necesaria por la separación del plano de control del plano de datos. Define la *API* de comunicación entre el controlador y los diferentes dispositivos de red, en otras palabras, entre el plano de control y el plano de datos.
- ***Northbound API:*** funciona como interfaz tanto de alto como de bajo nivel, es necesaria para permitir que las aplicaciones que se ejecutan en la parte superior de *SDN* puedan comunicarse con el mismo. En el primer caso, la interfaz provee una abstracción de la red en sí misma, permitiendo a los desarrolladores no tener que preocuparse por los dispositivos individuales, sino manejar la red como un todo. En el segundo caso, la interfaz advierte a las aplicaciones sobre la existencia de los dispositivos individuales y sus enlaces, pero oculta las diferencias entre los dispositivos.

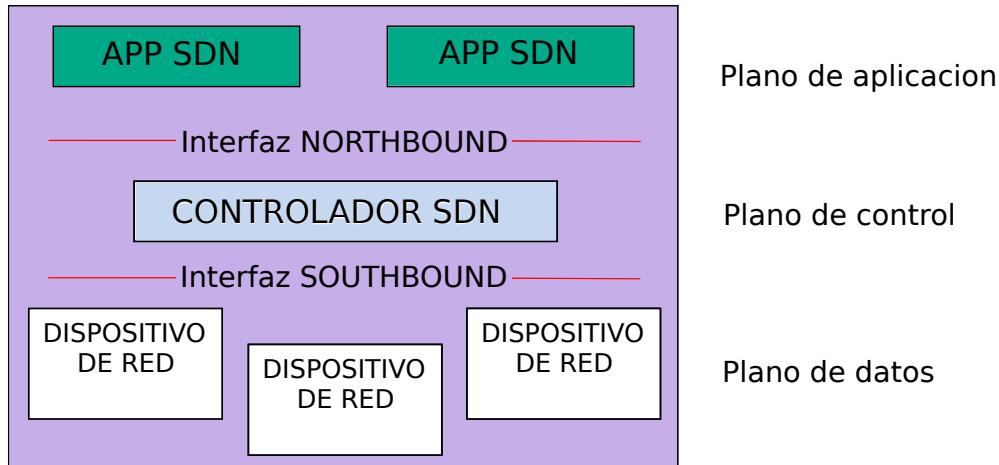


FIGURA 2.2: Arquitectura de un controlador SDN tradicional.

2.3. Gestión de la Red

En la actualidad se puede encontrar una gran variedad de redes, desde pequeñas redes domésticas de intranet hasta redes empresariales o de proveedores de servicios. Cada una de estas redes tiene diversos requerimientos de gestión. Las pequeñas redes domésticas, que consisten en unos pocos dispositivos conectados, requieren una sobrecarga de administración baja, y con frecuencia, pueden gestionarse manualmente de forma eficiente. No así las redes más grandes, que podrían contener cientos de dispositivos conectados requiriendo un enfoque más sistemático para hacer frente a las complejidades que surgen debido al tamaño de la red. A medida que la red crece en estructura y complejidad, se hace evidente la necesidad de una solución eficiente para la gestión de la misma [43].

2.3.1. Protocolos de Gestión

Existen múltiples formas de llevar a cabo la administración de la configuración en los diversos dispositivos que conforman la red. En esta sección, se analizarán dos alternativas: *CLI* y *SNMP*.

Command Line Interface

CLI es el enfoque más común en el ámbito de gestión de la configuración, adoptado por múltiples empresas. Consiste en un método para comunicarse con las aplicaciones que la subyacen, a través de una interfaz de usuario simple basada en texto. De esta forma, permite que el administrador pueda ingresar instrucciones en una línea de comandos a través de una terminal y recibir las respuestas en la misma. La aplicación subyacente es la encargada de procesar la instrucción y devolver alguna respuesta al usuario. Generalmente, las respuestas están orientadas a que resulten fácil de entender para las personas, sin embargo, no se encuentran orientadas a las API's, ya que no existe un formato o un estándar de cómo representar dichas respuestas. Además, las implementaciones internas podrían ser diferentes entre los distintos dispositivos, incluso entre dispositivos del mismo fabricante, de modo que tanto los comandos como las respuestas podrían variar significativamente entre los

equipos.

Un ejemplo de una operación en *CLI* puede verse en la figura 2.1. La primera línea ingresada, hace referencia a un acceso al modo de configuración de un dispositivo cualquiera. En la segunda, se agrega una entrada estática a la tabla de ruteo y en la tercera se abandona el modo de configuración.

LISTING 2.1: Interacción típica con un dispositivo mediante *CLI*.

```
> configure terminal
#> ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4
#> !
```

Este enfoque presenta una serie desventajas [35]. En primer lugar, la implementación de las aplicaciones subyacentes a la *CLI* no están estandarizadas, por lo que las operaciones varían drásticamente entre dispositivos de diferentes fabricantes e incluso en implementaciones *CLI* del mismo fabricante. A su vez, los fabricantes podrían brindar una actualización de software del dispositivo, donde los comandos *CLI* de la versión anterior se vean modificados o eliminados, lo que no solo se traduce a problemas para el administrador de red, sino también para las *API's* que hagan uso de la *CLI*.

En segundo lugar, realizar un cambio en el estado de un dispositivo podría requerir múltiples transacciones, y en el caso de que alguna de estas falle, el dispositivo podría quedar en un estado inconsistente. Por ejemplo, en la figura 2.1 se observó que para realizar una operación sencilla como agregar una entrada a la tabla de ruteo, implicó el uso de al menos tres comandos. De forma similar, podrían existir operaciones que requieran de transacciones con una mayor cantidad de instrucciones. *CLI* no define de forma estándar una solución para deshacer los cambios aplicados en el dispositivo.

Simple Network Management Protocol

SNMP es un protocolo de monitoreo y administración de red, estandarizado por primera vez en 1988 por la *IETF* [1]. Su funcionamiento se basa en una arquitectura cliente-servidor, donde los mensajes se intercambian a través del protocolo de transporte no orientado a la conexión *UDP*. Consiste en una colección de agentes y administradores formando entre ellos una red, donde se denomina administrador a aquel dispositivo que tiene el rol de ejecutar aplicaciones de administración de red, mientras que los dispositivos que requieren ser administrados se denominan agentes [2].

Las capacidades para administrar la red en *SNMP*, quedan representadas en lo que se conoce como *MIB*. Una *MIB*, es una base de datos que contiene información jerárquica y estructurada en forma de árbol de todos los parámetros gestionables de la red. Dicha base de datos se debe cargar en el administrador *SNMP*, para ello cada agente *SNMP* expone al administrador *SNMP* una serie de módulos *MIB*. Con esta información el administrador podría alterar dinámicamente la configuración del agente.

El uso de *SNMP* como monitoreo es una práctica común desde su publicación, sin embargo, se desalentó su uso en áreas de gestión de configuración por las siguientes razones [31]:

- Problemas inherentes al protocolo de transporte *UDP*, donde los mensajes pueden perderse o llegar desordenados, así como también la falta de mecanismos de seguridad para los mismos jugaron un papel importante para reemplazar *SNMP* por otros protocolos de administración de red.
- No existe una estandarización de los módulos *MIB* para configurar las funciones de red. El trabajo de descubrir correctamente los módulos *MIB* para cada dispositivo es tarea del usuario, lo que resulta compleja y no eficiente.

La figura 2.3 muestra las operaciones más comunes de *SNMP*.

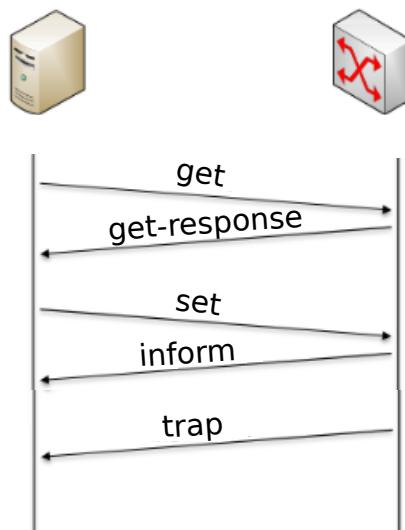


FIGURA 2.3: Operaciones típicas en *SNMP*.

Otras alternativas

Algunos enfoques para la gestión de la red pueden incluir soluciones basadas en páginas web, que permiten al administrador modificar las configuraciones en el dispositivo de forma gráfica y más amigable, pero generalmente resultan más limitadas que las *CLI*. Además, algunos dispositivos pueden brindar soluciones propietarias para la gestión de la configuración, sin embargo, estas soluciones suelen ser muy específicas a un dispositivo o una familia de dispositivos, y rara vez suelen ser compatibles entre sí. Estos últimos también representan una carga para los administradores, donde cada solución requiere que el administrador aprenda otra manera de configurar las funcionalidades de la red.

2.3.2. NETCONF

Esta sección repasa brevemente los conceptos y las características principales que ofrece el protocolo *NETCONF*. Además, aspectos de seguridad, transporte y control de acceso del protocolo se discuten en detalle.

Definición

NETCONF fue estandarizado por la *IETF* por primera vez en el 2006, en el *RFC 4741* [19]. Actualmente está siendo adoptado por los principales proveedores de dispositivos de red y ha ganado el apoyo de la industria. Según detalla Carl Moberg [17], podemos encontrar que fabricantes como Juniper, Huawei, Cisco, entre otros, brindan soporte desde hace tiempo del protocolo *NETCONF*.

La *IETF* define a *NETCONF* como un protocolo estándar para instalar, manipular y borrar configuraciones en un dispositivo [20]. Permite implementar una *API* formal utilizando el lenguaje de modelado *YANG* para administrar y monitorear las funcionalidades de la red. *NETCONF* utiliza el paradigma de las *RPC*, donde construye los mensajes que intercambian información como un flujo con codificación *XML*. Funciona con una arquitectura cliente-servidor, donde los mensajes son transportados utilizando algún protocolo orientado a la conexión. El *RFC 6241*, en la sección 1.2, menciona una partición conceptual del protocolo en cuatro capas, dicha partición se refleja en la figura 2.4.

A continuación, se explica qué función cumple cada una de estas capas.

- **Capa de transporte seguro:** provee mecanismos de comunicación entre cliente y servidor.
- **Capa de mensajes:** encargada de la codificación y partición de los mensajes.
- **Capa de operación:** define las operaciones admitidas por el protocolo.
- **Capa de contenido:** relaciona la representación y el modelado de los datos en el protocolo.

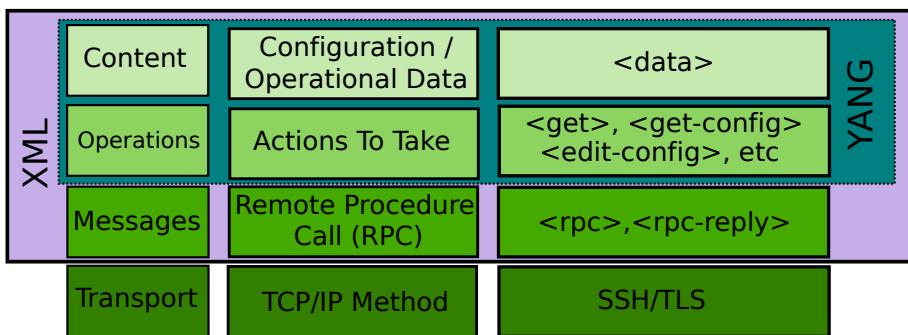


FIGURA 2.4: Separación conceptual del protocolo *NETCONF*.

Las características que destacan a *NETCONF* como protocolo de administración de red son [22]:

- Capacidad de restauración de los datos y *backup* de la configuración.
- De uso fácil, presentando la información de forma estructurada con una codificación entendible para las personas y las *API's*.
- Implementa mecanismos de control de errores mediante validación de sintaxis y semántica.

- Separación clara de los datos de configuración y los datos de estado.
- Posibilidad de gestionar la configuración en un dispositivo de manera reactiva mediante notificaciones del mismo.

NETCONF separa los datos de configuración de los datos de estado de un dispositivo. Según lo detallado en la sección 1.1 y 1.4 del *RFC 6242*, se define a cada uno como:

- **Datos de configuración:** información que se puede leer o escribir y que se utiliza para llevar al dispositivo de un estado inicial a un estado deseado. Un ejemplo es la velocidad del ventilador del cpu del dispositivo.
- **Datos de estado:** representa información de sólo lectura y estadísticas brindadas por el dispositivo. Por ejemplo, la temperatura del cpu del equipo.

Conceptos del Protocolo

Como se mencionó anteriormente, *NETCONF* define un protocolo de administración de red con arquitectura cliente-servidor, donde el cliente en este caso es el sistema de administración de la red o el administrador del sistema, mientras que el dispositivo que contiene una o más funciones de red que deben ser administradas, actúa de servidor. El cliente y el servidor inician la sesión de protocolos mediante un primer mensaje que da lugar al intercambio de capacidades o *capabilities*, donde se definen qué operaciones estarán disponibles para su uso. Este primer mensaje recibe el nombre de *HELLO* [20]. La figura 2.5 ejemplifica la arquitectura presentada por el protocolo.

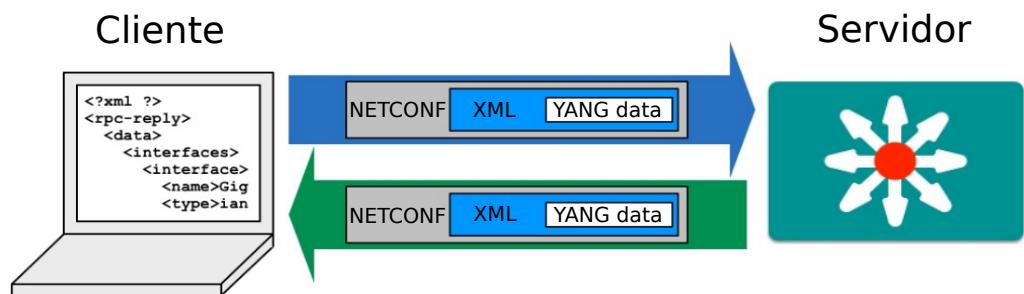


FIGURA 2.5: Arquitectura cliente-servidor en el protocolo *NETCONF*.

Capacidades

El protocolo *NETCONF* está diseñado para ser altamente extensible y, con este fin, es compatible con el intercambio inicial de capacidades entre cliente y servidor [20]. Este intercambio de información permite al cliente ajustar sus comportamientos basándose en las funcionalidades que admite el servidor. Cada capacidad establecida por el protocolo recibe un nombre asignado por la *IANA*. Además, también se incluye el intercambio de los modelos *YANG* que tiene implementado el servidor, lo cual es necesario no solo para que el cliente pueda aprender de los mismos, sino

también para reconocer las diferentes revisiones implementadas en el servidor.

La utilidad de esta característica reside en que a través del intercambio de las capacidades entre el cliente y el servidor, el protocolo define cuáles serán las operaciones admitidas desde el inicio de la sesión, evitando así el ingreso de comandos de configuración incorrectos o no soportados.

Sesión orientada a la conexión

La sección dos del *RFC 6242*, referida a protocolos de transporte, detalla que *NETCONF* no está vinculado a ningún protocolo de transporte específico. El requisito necesario de *NETCONF* para el protocolo de transporte subyacente es que el mismo sea orientado a la conexión.

Esta es una de las principales ventajas frente a *SNMP*, donde los mensajes en este último eran transportados a través del protocolo no orientado a la conexión, *UDP*. Además, el hecho de que *NETCONF* no especifique el uso de un único protocolo de transporte orientado a la conexión, se traduce a una mayor flexibilidad y personalización para el administrador, pudiendo optar por aquella que mejor se ajuste a las necesidades de los equipos involucrados.

Sesión orientada a la autenticación

El protocolo *NETCONF* es orientado a la sesión con autenticación, utilizando una arquitectura cliente-servidor donde el servidor escucha un puerto asignado para recibir las conexiones con los clientes.

Según la sección dos del *RFC 6242* referida a seguridad, el protocolo mínimamente debe ofrecer autenticación, confidencialidad e integridad. Cualquier mensaje *NETCONF*, incluido el mensaje *HELLO*, se envían únicamente si el cliente y servidor se han autenticado de forma correcta. No se especifica un protocolo en particular, pudiendo utilizarse alguno de los múltiples protocolos de transporte seguros existentes en la actualidad como *TLS*, *SSH*, *BEEP*, etc. Cualquier implementación de *NETCONF* debe, al menos, soportar *SSH* como protocolo de transporte seguro.

Además, según el *RFC 6536* relacionado al control de acceso de usuarios, *NETCONF* admite una jerarquía de niveles de usuarios. Por ejemplo, es posible definir dos grupos de usuarios donde uno tenga permisos de configuración más limitados que el otro.

Bases de datos

NETCONF define en la sección cinco del *RFC 6242*, la existencia de uno o más *datastores*, los cuales cumplen el papel de una base de datos conceptual que puede ser utilizada para almacenar y acceder tanto a los datos de configuración como a los datos de estado. El protocolo especifica y define tres tipos de base de datos: *running*, *startup* y *candidate*, de las cuales únicamente es obligatorio que se implemente la primera. Si la implementación admite otras bases de datos, como por ejemplo *startup* o *candidate*, el servidor informará al cliente esta capacidad en el mensaje *HELLO*. Cada operación en *NETCONF* debe especificar la base de datos a la cual se realizará la

consulta o modificación.

A continuación, se detalla cada uno de los almacenes de datos mencionados.

- **startup:** según lo especificado en la sección 8.7 del RFC 6242, dicha base de datos se utiliza para almacenar de forma persistente la información de configuración del dispositivo. El contenido de esta es copiado de manera automática a la base de datos conocida como *running* en el inicio del servidor NETCONF. De esta forma, el protocolo brinda una herramienta para poder aplicar una configuración al inicio del equipo.
- **running:** refleja la configuración actualmente en uso por el dispositivo. Es la única base de datos conceptual que admite la presencia tanto de datos de estado como datos de configuración. A alto nivel, esta base de datos se diferencia del estado de *startup*, puesto que no es una configuración que será aplicada al inicio sino que refleja la configuración actual del dispositivo.
- **candidate:** se encuentra definido en la sección 8.3 del RFC 6242. Puede ser utilizado para realizar cambios que no se van a aplicar al dispositivo de forma directa, sino que lo harán una vez se realice un *commit* sobre dicha base de datos. De esta forma, el contenido de *candidate* es copiado a *running*. Si de lo contrario se desea descartar los cambios realizados en este *datastore*, la operación *discard-changes* copia el contenido de *running* a *candidate*. A diferencia del *datastore running*, en esta base de datos conceptual únicamente se admiten datos de configuración. En otras palabras, la utilidad de esta base de datos reside en que permite brindar al administrador un entorno de pruebas, donde se podría aplicar una configuración temporal en el equipo, con capacidad de volver a la configuración anterior en caso de fallas.

Como se mencionó anteriormente, cualquier implementación de NETCONF debe admitir al menos el *datastore running*, esto es necesario ya que los datos de estado (necesarios para monitorear el dispositivo) únicamente se encuentran admitidos en dicho *datastore*.

Por último, se podría hacer una analogía entre la separación de los datos de estado y los datos de configuración con la separación conceptual de dichas bases de datos lógicas. En el primer caso, se busca distinguir entre un dato de solo lectura de otro que admite la escritura, mientras que el segundo trata de diferenciar entre un conjunto de estados bien definidos que puede alcanzar el dispositivo. Por ejemplo, distinguir la configuración que va a aplicarse únicamente en el inicio del dispositivo a través del *datastore startup*, de la configuración que podría llevar en un determinado momento a través del *datastore running*.

Operaciones del protocolo

Las operaciones en el protocolo NETCONF se definen como *RPC* en los modelos YANG relevantes. En dichos modelos también se definen los argumentos de entrada y los contenidos de salida para cada operación. Todas las operaciones están codificadas en XML dentro de los mensajes *RPC* que son, de hecho, los únicos mensajes

que los clientes pueden enviar en las sesiones de NETCONF después del intercambio inicial del mensaje *HELLO*.

Como las operaciones son *RPC*, cada mensaje enviado por los clientes tendrá una respuesta por parte del servidor. Este resultado normalmente contiene *ok* para indicar que la operación resultó según lo esperado, o *error* indicando las razones por la cual falló dicha operación.

El protocolo define en la sección 7 del RFC 6241 nueve operaciones básicas y necesarias para cualquier implementación del mismo, las cuales se describen a continuación:

- ***get***: utilizado para consultar tanto datos de configuración como datos de estado al servidor NETCONF.
- ***get-config***: operación que devuelve los datos de configuración del dispositivo. Puede incluir filtros para limitar la información enviada por parte del servidor.
- ***edit-config***: definida para crear, actualizar o borrar datos de configuración en el servidor. Únicamente se admite esta operación en las bases de datos *running* o *candidate*.
- ***copy-config***: crea o reemplaza completamente el contenido de una base de datos por otra. El caso de uso más común de esta operación es para copiar el contenido del *datastore running* al *datastore startup*.
- ***delete-config***: Elimina completamente el contenido de un *datastore* determinado. No se admite esta operación para la base de datos *running*.
- ***lock***: permite al cliente bloquear la configuración completa de un *datastore* específico en un dispositivo. Tales bloqueos son destinados a ser de corta duración, de esta forma un cliente puede realizar un cambio sin temor a la interacción con otros clientes de NETCONF. Además, como el protocolo es orientado a la sesión, todos los recursos tomados por la misma tales como los *datastores*, deben ser liberados en el momento de la finalización o cierre de la sesión.
- ***unlock***: permite a la sesión liberar el recurso tomado por la operación *lock*.
- ***close-session***: utilizada para finalizar la sesión entre cliente y servidor NETCONF. Cualquiera de las operaciones mencionadas en esta sección, quedan inhabilitadas una vez finalizada la sesión.
- ***kill-session***: permite al administrador de red finalizar alguna sesión inactiva que tiene recursos tomados.

Además de estas nueve operaciones descritas por el protocolo, pueden proporcionarse operaciones adicionales basado en las capacidades anunciadas por el dispositivo, como por ejemplo operaciones *RPC* definidas en los módulos YANG.

También, NETCONF admite operaciones con capacidades más avanzadas. No es obligatorio que las diferentes implementaciones del mismo soporten las siguientes características, más bien, de hacerlo deben ser expuestas como capacidades admitidas en el mensaje *HELLO*. Dichas operaciones se describen a continuación:

- **commit:** operación utilizada para copiar atómicamente el contenido del *datastore candidate* al *datastore running*. Además, puede incluirse la operación *confirmed-commit*, esta última funciona como un *backup* de la configuración previa al *commit*, la cual se restablece al cabo de un *timeout* si no se recibe la operación *confirmed-commit*. NETCONF describe a esta última como una 'confirmación de la confirmación'.
- **discard-changes:** revierte una operación que está en espera de confirmación. En otras palabras, se copia el contenido del *datastore running* al *datastore candidate*.
- **validate:** consiste en una operación que verifica la correctitud semántica y sintáctica de una configuración antes de aplicar el cambio en el dispositivo.

La tabla 2.1 resume las diferentes operaciones disponibles en NETCONF y a qué *datastore* podría aplicarse cada una de ellas.

Capacidad	Operación	Base de datos afectada
writable-running	lock	running
	edit-config	running
	unlock	running
	copy-config	running -> startup
candidate	lock	candidate
	edit-config	candidate
	commit	candidate -> running
	validate	candidate
	unlock	candidate
	copy-config	running -> startup
confirmed-commit	lock	candidate
	edit-config	candidate
	commit	candidate
	confirmed-commit	candidate -> running
	validate	candidate
	unlock	candidate
	copy-config	running -> startup

CUADRO 2.1: Ejemplo de operaciones disponibles en NETCONF

Notificaciones

Si bien NETCONF está diseñado principalmente para la administración de la configuración de la red mediante las operaciones expuestas anteriormente, existe una poderosa herramienta de monitoreo implementada en el protocolo llamada notificaciones. La RFC 5277 define a las mismas como un servicio de entrega de mensajes asíncronos a los clientes mediante suscripción. Esta característica no es obligatoria para las diferentes implementaciones del protocolo. De soportarlo, el servidor deberá comunicar a los clientes dicha característica como una capacidad del servidor en el mensaje *HELLO*.

Esta herramienta es similar a las notificaciones en el protocolo *SNMP*, pero tiene la ventaja de que, en *NETCONF*, el cliente puede especificar a qué notificación particular se desea suscribir, lo que permite un monitoreo más flexible. Además, como se mencionó anteriormente el servidor puede declarar permisos para los diferentes usuarios y sesiones por lo que las notificaciones serán enviadas únicamente a aquellos clientes suscritos y que cumplan con el nivel de acceso requerido por el servidor.

La importancia de las notificaciones reside en que los dispositivos de red tienen variables críticas que deben ser monitoreadas, por ejemplo la temperatura del equipo, el estado de los enlaces, la conectividad entre los mismos, etc. Dichas variables críticas reciben el nombre de alarmas.

De no existir un mecanismo de mensajes asíncronos, el monitoreo de las alarmas de un dispositivo podría implicar una sobrecarga en la red, debido a la cantidad de consultas periódicas que existirían sobre los dispositivos.

De esta forma, las notificaciones que define el protocolo *NETCONF* no solo implica un monitoreo eficiente mediante mensajes asíncronos, sino que permite al protocolo poder tomar medidas de forma reactiva a las diferentes alarmas que se presenten. Por ejemplo, se podría configurar al cliente *NETCONF* para que, de recibir una alarma de exceso de temperatura en el equipo, configure de forma automática una velocidad mayor en el ventilador del mismo.

Para finalizar, la figura 2.6 refleja una interacción típica entre cliente y servidor donde se observa el intercambio de capacidades en los mensajes *HELLO*, el uso de diferentes operaciones con respuestas *RPC* y las notificaciones.

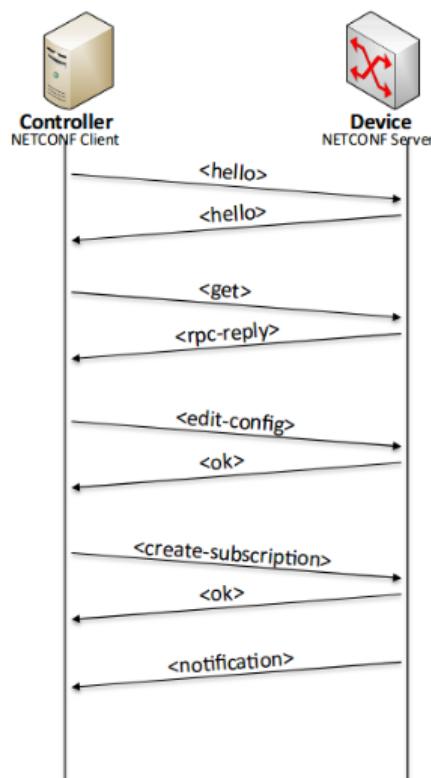


FIGURA 2.6: Ejemplo de comunicación entre cliente y servidor NET-CONF.

2.3.3. Lenguaje de Modelado YANG

Como se mencionó anteriormente, NETCONF utiliza YANG para modelar los datos de estado, los datos de configuración, las RPC y las notificaciones. *Yet Another Next Generation* es un lenguaje de modelado de datos desarrollado y estandarizado en la RFC 6020 por la IETF en el año 2010 [47]. Si bien existen en la actualidad lenguajes de modelado como XML Schema, SMI, UML, entre otros, la ventaja que presenta YANG frente a los demás es que es un lenguaje de modelado específico para gestión de la configuración de red.

Conceptos del Lenguaje

YANG define, en la sección 4.1 de la RFC 6020, las funcionalidades de la red separando los datos de estado de los datos de configuración y presentando la información como una estructura de árbol jerárquica. Consiste en una serie de declaraciones y tipos que pueden ser usadas para definir los datos que se quieren modelar. Estas definiciones son contenidas en un módulo y describen qué tipo de datos admite una variable. A su vez, un módulo puede heredar definiciones de otro módulo.

Módulos y submódulos

Definen una estructura para el modelado de datos. Tienen un diseño predefinido que se debe seguir. Este diseño comienza con un encabezado, siguiendo de las declaraciones que contenga el módulo y por último las revisiones y comentarios respecto al mismo.

Se define el nombre del módulo, un prefijo para identificarlo, las dependencias, información de contacto al autor, descripción y revisiones. La declaración '*include*' permite referenciar material que se describe en un submódulo, mientras que la declaración '*import*' permite referenciar material que se encuentra descrito en un módulo externo. La estructura básica de un módulo puede verse en la figura 2.7.

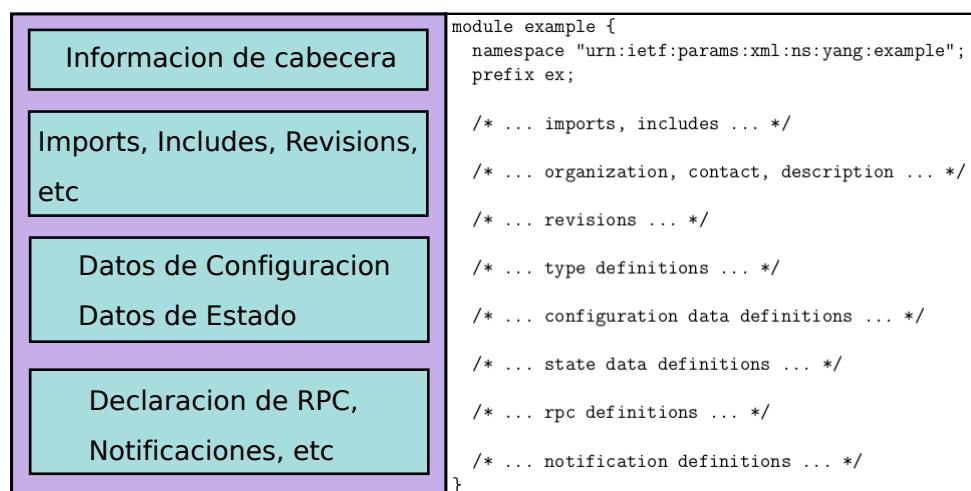


FIGURA 2.7: Estructura de un módulo YANG.

Declaraciones y Definiciones de Datos

A continuación, se describen algunas sentencias que podría contener un módulo YANG. Cada sentencia contiene la definición del tipo de dato y puede contener además algún valor para ese tipo de dato. Siempre representan a datos de configuración o datos de estado, realizando dicha distinción con la sentencia llamada '*config*'.

- ***leaf***: contiene un dato simple como un entero o un *string*. Admite exactamente un valor para un tipo de dato particular y opcionalmente puede incluir una descripción.
- ***leaf-list***: describe una secuencia de datos tipo *leaf*. Cada *leaf* admitirá un solo valor para el tipo de dato que especifique el *leaf-list*.
- ***container***: es utilizado para agrupar datos lógicamente relacionados. Un *container* no admite un valor, pero sí admite cualquier número de tipos de datos como *leaf*, *leaf-list*, *container* o *list*.
- ***list***: define una secuencia de tipo de datos donde cada tipo de dato es única, identificado por la sentencia *key*. Puede contener múltiples identificadores *key* y cualquier cantidad de tipo de datos *leaf*, *leaf-list*, *container*, etc.
- ***choices - cases***: no describen algún tipo de dato, más bien ofrecen ramificaciones condicionales en la estructura del módulo. La sentencia *choice* es una condición que asegura que, como máximo, se cumplirá una de las declaraciones dadas por *case*.

Las declaraciones y sentencias descritas anteriormente pueden ser utilizadas en conjunto para poder formar una estructura de datos tipo árbol más compleja. Además, YANG admite la reutilización de sentencias mediante las declaraciones *include* e *import* reduciendo así los posibles errores en el modelado de datos.

Identificador de instancia

Cada dato en YANG, así como el propio módulo, tiene un identificador único de instancia que se puede utilizar para referirse a él. Los identificadores se denominan *namespace*, y admiten un prefijo para poder acortar el nombre.

Por ejemplo, Bjorklund [3], definió un módulo YANG para la administración de interfaces. Dicho modelo tiene una estructura de datos de tres niveles para una interfaz básica. En el nivel superior del modelo se encuentra definido el *container* llamado '*interface*', seguido de la *list* '*interface*' que contiene múltiples instancias de una interfaz, identificada por la *key* '*name*'. Además, cada interfaz tiene una *leaf* '*enabled*' que describe el estado de la misma. Un ejemplo de identificador para una instancia de '*interface*' llamada '*eth0*' puede verse en la figura 2.8.

```
/if:interface/if:interface['eth0']/if:enabled
```

FIGURA 2.8: Ejemplo de identificador de instancia en YANG.

Funcionalidades

YANG ofrece características especiales que lo distinguen de un documento JSON, permitiéndole describir de forma eficiente las funcionalidades de la red. Estas características incluyen la validación de modelos, una forma estandarizada de extender a los módulos y compatibilidad entre las diferentes revisiones de los mismos. En esta sección, se analizarán las principales funcionalidades ofrecidas por YANG.

- **Validación:** una de las características más importantes de YANG es la posibilidad de validar automáticamente todos los datos descritos en el modelo. Resulta importante ya que la validación de los datos es una tarea difícil. Dicha afirmación está respaldada por el hecho de que introducir datos erróneos y tomarlos como válidos, está catalogada como la principal amenaza de seguridad según OWASP [32], organización sin ánimo de lucro a nivel mundial dedicada a mejorar la seguridad de las aplicaciones y del software en general. Cada dato introducido en el modelo YANG puede ser validado semánticamente y sintácticamente. La validación de sintaxis es automática y garantiza que el dato contenga una secuencia de *bytes* válida, puesto que cada dato en el modelo tiene asociado un *type* (*string*, *int*, *uint*, etc). Por otra parte, la validación semántica resulta más compleja y puede ser usada para describir dependencias entre datos. YANG también admite sentencias como '*when*' o '*must*' que pueden ser usadas para evaluar condicionalmente un dato.
- **Compatibilidad:** cada módulo admite la indicación de una revisión, esto permite a YANG distinguir las versiones soportadas y adaptarse a la situación cuando la misma no es soportada. También, se describen reglas de actualización en los módulos que deben respetarse para mantener compatibilidad entre los modelos de datos anteriores. Por ejemplo, cualquier cambio en un módulo debe indicar una revisión en la cabecera, tanto el nombre del mismo como el *namespace* debe mantenerse, como así también las definiciones de datos obsoletas, lo que permite compatibilidad con modelos de datos anteriores. Esta característica permite a los módulos evolucionar con el paso del tiempo, sin romper aplicaciones existentes con versiones anteriores.
- **Extensión:** permite extender las funcionalidades de los módulos con nuevas definiciones de datos. Existen muchas razones por las cuales utilizar la extensión en YANG, como por ejemplo, desarrollar un nuevo módulo a partir de uno existente o con el fin de reducir errores reutilizando un módulo funcional. Una ventaja importante que tiene utilizar la extensión, es que al agregar nueva información en un módulo, se mantiene compatibilidad con el heredado.

2.3.4. Redes Ópticas de Transporte

La explosión del tráfico digital provocado por los nuevos enfoques como *Big Data* o el *Streaming*, y los requerimientos de los usuarios donde existe un constante crecimiento de aplicaciones con alta demanda de ancho de banda, requieren de una nueva tecnología de transporte que pueda ocuparse de los patrones de tráfico y los contenidos de datos modernos. Para ello, se han realizado numerosos avances en los últimos años referente al plano de control y el plano de datos de las redes ópticas [34], surgiendo protocolos como SONET o OTN. En esta sección, se analiza las redes

ópticas utilizadas para el transporte de los datos como así también los dispositivos que funcionan sobre dichas redes.

Una red de transporte óptica, es un tipo de red de comunicaciones de datos que utiliza la luz como medio de transporte para la información [29]. A diferencia de las redes basadas en cobre, los pulsos de luz de una red óptica pueden transportarse a una distancia considerable e incluso regenerarse a través de un dispositivo repetidor óptico. Después de que una señal óptica es recibida en su red de destino, la misma se convierte en una señal eléctrica a través de un receptor óptico, para luego ser enviado al nodo de la capa de paquetes.

Un sistema de comunicaciones ópticas puede incluir diversos dispositivos, como ser:

- **Amplificadores ópticos.**
- **Switches ópticos**, encargados de comutar de un canal a otro.
- **Divisores de luz**, cuya tarea comprende dividir la señal en diferentes caminos de fibra óptica.
- **Fibra óptica**, que cumple de medio de transporte de la información entre los diferentes equipos.
- **Transponders y Muxponders**, encargados de enviar y recibir las señales ópticas por las fibras. Generalmente son caracterizados por el ancho de banda que pueden transportar y la distancia que puede alcanzar la transmisión.

Transponders y Muxponders

El *transponder*, es un dispositivo que recibe múltiples señales ópticas a través de sus puertos clientes, dichas señales ópticas pueden tratarse de servicios diferentes como por ejemplo, *Ethernet*, *SONET*, *OTN*, entre otros. Luego, transforma estas señales en flujos de datos eléctricos, las procesa y regenera las mismas para nuevamente convertirlas en señales ópticas compatibles con el estándar *ITU*. De esta forma, realiza la función de recepción, amplificación y reemisión de una señal óptica en un proceso que comúnmente se denomina *optical electrical optical* (OEO) [18].

La figura 2.9 exemplifica el proceso OEO típico de un *transponder*.

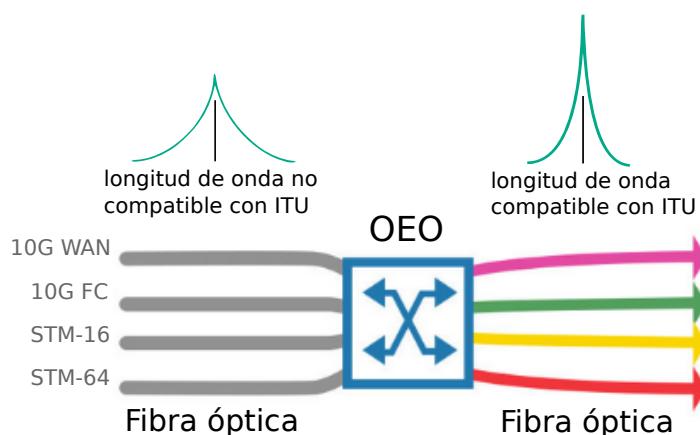


FIGURA 2.9: Funcionamiento básico de un *transponder*.

Por otra parte, los *muxponders* realizan una función similar a los *transponders*. También incluyen el proceso *OEO*, con la diferencia de que combinan múltiples servicios en una sola longitud de onda que luego se multiplexan en la misma fibra [18]. Por lo tanto, en lugar de asignar a cada servicio una longitud de onda dedicada, permite que varios servicios diferentes comparten la misma longitud de onda. Estos dispositivos maximizan la utilización de la fibra y ofrecen soluciones de bajo costo para empresas y transportistas. La figura 2.10 muestra el comportamiento de un *muxponder*.

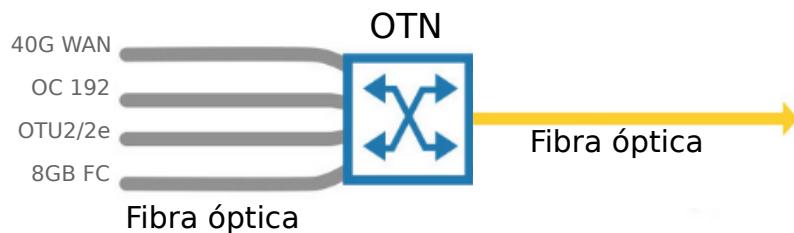


FIGURA 2.10: Funcionamiento básico de un *muxponder*.

Aplicaciones

Resulta importante ahora separar la red en dos capas diferentes: la capa de paquetes o de *IP/MPLS*, y la capa óptica o de transporte [40]. La figura 2.11 muestra dicha separación. Los dispositivos mencionados anteriormente se utilizan en la capa de transporte mientras que los *routers* y *switches* convencionales se encuentran en la capa *IP/MPLS*.

La función que tienen los *muxponders* es la de proveer una conexión lógica entre los diferentes *routers*, quienes podrían estar separados por enormes distancias donde los protocolos como *Ethernet* no proveen un buen servicio de transporte.

De esta forma, los dispositivos de la capa *IP/MPLS* tienen conocimiento de sus vecinos pero no de la forma en la que se encuentran conectados ni de cómo se está realizando dicha comunicación, mientras que los equipos de la capa óptica esencialmente emparejan a los dispositivos de la capa *IP/MPLS* pero sin tener conocimiento sobre los diferentes servicios que se prestan.

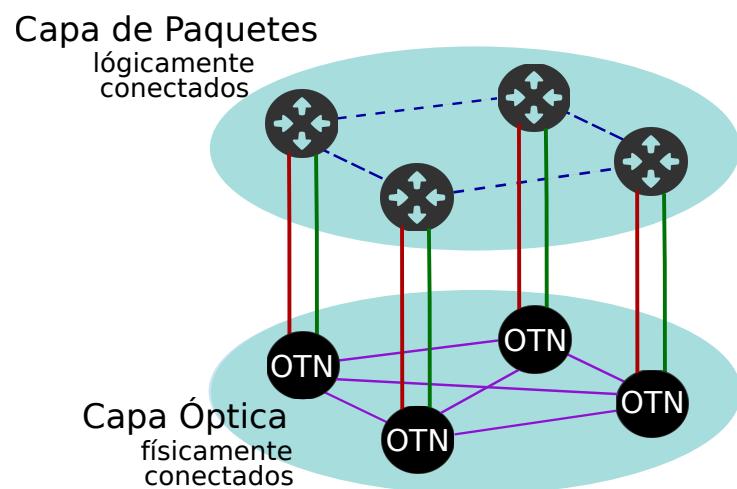


FIGURA 2.11: Separación de la red en capa de paquetes y capa de transporte.

Capítulo 3

Análisis de las tecnologías

Teniendo en cuenta los conceptos revisados en el capítulo anterior, en este se estudiarán las herramientas que permitirán la realización del proyecto.

En la primera sección, se realizará un análisis del dispositivo utilizado, un *muxponder* óptico coherente de 40GB desarrollado por la institución donde se realizó el proyecto.

Luego, en la segunda sección se examinarán las herramientas de software involucradas. La misma se encuentra dividida en dos partes; la primera detalla el funcionamiento del controlador *SDN* utilizado, *ONOS*; la segunda refiere al estudio de dos agentes *NETCONF*: *Sysrepo* y *Yuma123*.

3.1. Herramientas de Hardware

Para cumplir con el objetivo del proyecto, será de suma importancia conocer las bondades y las limitaciones del equipo con el que se cuenta. Así, esta sección comprende el estudio de uno de los dispositivos mencionados en el capítulo anterior, un *muxponder*. Concretamente, se analizarán aspectos técnicos relacionados tanto al hardware como al software de un *muxponder* de 40GB. El interés del análisis resulta en que es en este dispositivo en donde se integrará el protocolo de gestión *NETCONF*.

3.1.1. *Muxponder 40GB*

El muxponder con el que se cuenta es capaz de realizar una transmisión óptica de 40GB/s sobre una señal de línea *OTU3*. La misma es lograda cumpliendo el estándar *ITU-T G.709* [11], utilizando una modulación coherente *DP-QPSK* o *DP-DQPSK*. Dispone de cuatro clientes ópticos asíncronos totalmente independientes de 10GB/s cada uno, a través de módulos ópticos *XFP* removibles. Las longitudes de ondas soportadas para los clientes son 850/1310/1550 nm y admite los tipos de cliente 10GB *Ethernet LAN/WAN*, *OTU2* y *OTU2e*.

Además, incorpora el mecanismo de corrección de errores *FEC* para todas las señales, tanto para clientes como para línea. Mediante el mismo, el *muxponder* es capaz de realizar correcciones sin necesidad de retransmitir la información.

En términos de potencia, alcanza típicamente los 93 Watts. También, el dispositivo puede alcanzar una distancia de hasta 2000Km.

Las interfaces de conexión soportadas para realizar configuración y monitoreo en el dispositivo son:

- 2 puertos *Ethernet*.
- 1 puerto serial *RS232*.
- 1 puerto *USB 2.0*.

En la figura 3.1 se puede observar en el panel frontal del equipo con las diferentes interfaces mencionadas anteriormente.

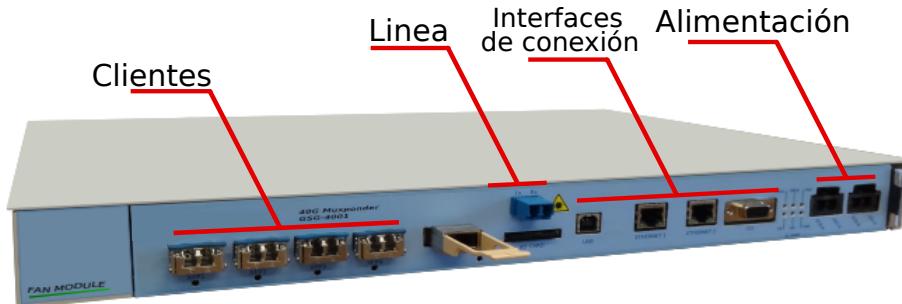


FIGURA 3.1: Vista del panel frontal del *muxponder* de 40GB utilizado.

Por otra parte, el *muxponder* de 40GB integra un total de 128MB de memoria RAM y 512MB de almacenamiento, con capacidad de extender esta última mediante una tarjeta SD. Además, cuenta con un sistema operativo Linux '*Buildroot*', el cual ocupa gran parte de estos recursos mencionados, dejando libre para las aplicaciones de usuario un total de 100MB de RAM y 270MB de almacenamiento.

El hecho de que presente dicho sistema operativo resulta en una ventaja por varios motivos, en primer lugar porque el mismo es un entorno conocido por el alumno, donde además podrán ejecutarse en él la mayoría de las aplicaciones *UNIX* típicas. En segundo lugar, el sistema operativo integra bibliotecas y herramientas que facilitarán el desarrollo del proyecto, como por ejemplo la biblioteca *SSH*, necesaria por el protocolo *NETCONF*.

Por último, el procesador que incorpora es un *NIOS II* de primera generación fabricado por *Intel* [21]. El mismo funciona a 125 Mhz y se encuentra integrado en una *FPGA*. Es importante destacar que la arquitectura de este procesador no es una arquitectura típica de una máquina de propósito general (por ejemplo *x86_64*), por lo tanto, las distintas aplicaciones que se ejecuten en esta plataforma deberán estar compiladas específicamente para la arquitectura *NIOS*.

Además, debido a las capacidades de la memoria primaria y secundaria del equipo, resulta imposible realizar la compilación de las aplicaciones sobre el mismo. Por lo tanto, se deberá realizar lo que se conoce como compilación cruzada, que consiste en preparar un sistema huésped (donde generalmente dicho sistema cuenta con mayores recursos y capacidades) para generar todos los binarios y bibliotecas que requiere el dispositivo objetivo donde finalmente se ejecutarán las aplicaciones.

3.1.2. Componentes del *muxponder*

Los componentes más significativos del dispositivo se listan a continuación:

- Módulo de 40GB.
- Los 4 puertos clientes (XFP).
- Unidad de ventilación.
- Chip cortina.
- Unidad de alimentación.
- Interfaces de control.
- *FPGA*, con el procesador *NIOS II* instanciado.

Además, se presenta en la figura 3.2 un diagrama en bloques del *muxponder*, donde se pueden observar los principales componentes que conforman el mismo.

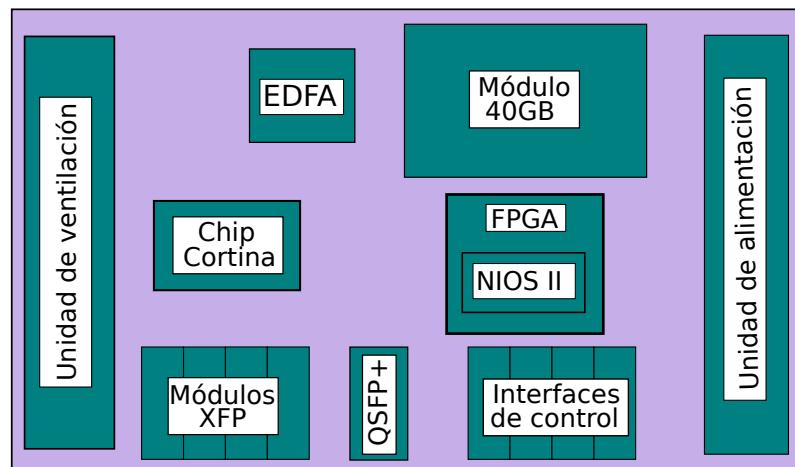


FIGURA 3.2: Diagrama en bloques del *muxponder* de 40GB.

Por otra parte, una vista de la circuitería del equipo se puede observar en la figura 3.3.



FIGURA 3.3: Vista de la circuitería del *muxponder* de 40GB.

3.1.3. Aplicaciones integradas en el dispositivo

Será importante explicar la utilidad de dos binarios que incorporan los *muxponders* de 40GB: 'monitor' y 'muxponder'.

- '**monitor**': aplicación que permite mostrar información del dispositivo a través de la *CLI*. Con el fin de agrupar y ordenar los datos relacionados, los mismos se encuentran divididos en secciones. Por ejemplo, se tiene una sección dedicada a mostrar la temperatura de los diferentes módulos, las alarmas relacionadas a la transmisión y recepción, otra sección referida a la presencia de los módulos XFP del equipo, entre otros. De esta forma, el administrador podría conocer el estado del dispositivo ejecutando dicha aplicación y observando la salida producida en pantalla.

Por otra parte, el equipo utiliza el método de comunicación entre procesos llamado memoria compartida. El mismo consiste en una región de memoria donde se permite que otras aplicaciones puedan, por ejemplo, leer información. Así, la aplicación 'monitor' también es la encargada de actualizar en memoria compartida los valores de todos los datos a monitorear, permitiendo que otras aplicaciones puedan leer y acceder a dicha información.

A continuación, se muestra en la figura 3.4 una porción de la salida en pantalla producida por la aplicación 'monitor'. En ella se puede observar la sección relacionada a los módulos XFP del *muxponder*.

	Power B	Power A	Fan 1	Fan 2
Status	Off	On	On	On
	XFP 1	XFP 2	XFP 3	XFP 4
Presence	Yes	Yes	Yes	Yes
Loss	No	Yes	Yes	Yes
Ready	No	No	No	No
Interrupt	Yes	Yes	Yes	Yes
Tx Power [dBm]	-inf	-2.31	-2.29	-2.27
Rx Power [dBm]	-13.23	-40.00	-40.00	-40.00
Temp. [C]	15.50	17.47	19.57	19.23
Low Tx Power Alarm	--	--	--	--
High Tx Power Alarm	--	--	--	--
Low Rx Power Alarm	--	Alarm	Alarm	Alarm
High Rx Power Alarm	--	--	--	--
Rx CDR Loss of Lock	--	Alarm	Alarm	Alarm
Tx CDR Loss of Lock	--	Alarm	Alarm	Alarm
Laser Fault	--	--	--	--

FIGURA 3.4: Sección XFP de la aplicación 'monitor'.

- '**muxponder**': Por otra parte, la aplicación 'muxponder' es utilizada por el administrador para poder configurar el dispositivo mediante ciertos parámetros que son especificados haciendo uso de la *CLI* del equipo. Por ejemplo, con esta aplicación el administrador podría cambiar la configuración de un *muxponder* que tiene un tipo de tráfico *otu2* por un tipo de tráfico *xge* a través de la *CLI*, tal como se muestra en la figura 3.5.

```
# ./muxponder --configuracion --xge --cerofec --cerofec_cliente
40G Module: Reset.
40G Module: Registers Reset Start ...
Configurando EDFA...
Reset por hardware...
Reset por software a valores de fabrica...
Reboot de firmware...
Configuracion modo y valor EDFA: talog Num.: 50-11-0236-01R
Product Date: FEB 04 2014
>mode p 4.000000
>
Modo y valor EDFA: mode
MODE: P 4.0 dBm
>>
Potencia de entrada EDFA: pin
```

FIGURA 3.5: Configuración mediante la aplicación '*muxponder*'.

3.2. Herramientas de Software

Además del estudio del hardware utilizado, resulta de interés realizar un análisis de los componentes de software que conforman el proyecto. Para ello, la primer parte de esta sección estará dedicada a estudiar el controlador *SDN* empleado, mientras que en la segunda parte se analizarán dos agentes *NETCONF* disponibles de código abierto.

3.2.1. Controlador ONOS

El controlador *ONOS*, desarrollado y mantenido por la *ONF* [28], es uno de los controladores abiertos más comunes en la industria, donde destacan miembros como Google, Intel, AT&T, Samsung, entre una numerosa lista [30]. Está diseñado específicamente para los proveedores de servicios, donde sus principales objetivos son la escalabilidad y el alto rendimiento [13].

Las licencias compatibles con *ONOS* son *Apache 2.0*, *MIT* y *BSD* [14]. El hecho de que sea un proyecto *open-source*, supone ventajas como ser interoperabilidad, personalización, flexibilidad e independencia del fabricante.

Antes de detallar cómo funciona y realizar un análisis de su arquitectura, es importante explicar el problema que enfrentan los controladores *SDN* para poder entender las ventajas que supone el mismo.

Debido al crecimiento del consumo de tráfico en las redes y la demanda del ancho de banda en alza, es necesario para los proveedores de servicio que el rendimiento y la escalabilidad de sus redes no se vean afectadas por estos motivos. De este modo, los controladores *SDN* deben poseer tres atributos claves: escalabilidad, rendimiento y alta disponibilidad [27].

- **Escalabilidad:** como se explicó en el capítulo anterior, *SDN* introduce una autoridad de control centralizada. La misma, debe ser capaz de escalar de igual forma que las funcionalidades de la red, manteniendo su rendimiento.
- **Alta disponibilidad:** el plano de control que se encuentra centralizado en el controlador, juega ahora un papel crítico. Esto es así ya que si el mismo se

encuentra sobrecargado o deja de estar disponible por alguna razón, la funcionalidad de la red se vería afectada. Por lo tanto, las diferentes soluciones *SDN* deberán brindar disponibilidad ininterrumpida del controlador.

- **Rendimiento:** el controlador también tiene que ser capaz de proveer mecanismos para adaptarse dinámicamente ante las fluctuaciones en la carga del tráfico y la congestión de la red, evitando que el rendimiento del mismo se vea afectado.

Arquitectura del controlador

Las características más importantes de la arquitectura presentada por ONOS [13] se detallan a continuación:

- **Núcleo distribuido:** la solución que propone ONOS para proveer escalabilidad, alto rendimiento y disponibilidad, se basa en un núcleo distribuido por los diferentes nodos que conforman un *cluster*, lo que implica la posibilidad de soportar enormes cantidades de dispositivos de red. Esto último es así ya que ONOS permite la incorporación dinámica de nuevos nodos, con lo que la carga del controlador podría distribuirse entre ellos de forma adaptativa.

La figura 3.6 ejemplifica dicha distribución. El hecho de agregar esta redundancia implica una mayor disponibilidad del controlador. A su vez, permite realizar un balanceo de carga, lo que se traduce en mayor rendimiento y escalabilidad.

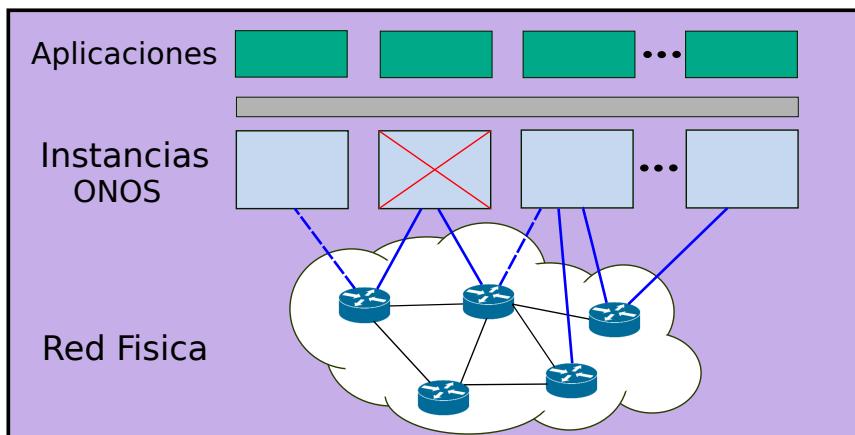


FIGURA 3.6: Arquitectura distribuida de ONOS.

- **Abstracción *Northbound*:** el plano aplicación explicado en el capítulo anterior, se comunica con ONOS a través de una interfaz brindada por el controlador. El mismo, brinda a las aplicaciones gráficos y estadísticas de la red como así también aplicaciones basadas en *intents* para facilitar el control, administración y configuración de los equipos.
- **Abstracción *Southbound*:** de forma similar, el controlador ofrece una interfaz para comunicarse con el plano de datos. Cabe destacar que si bien ONOS basa su funcionamiento en el protocolo *OpenFlow*, también brinda soporte a otros como *NETCONF*, *REST*, *SNMP*, etc, con el fin de mantener compatibilidad con dispositivos más antiguos.

Una aproximación más detallada de la arquitectura que presenta ONOS puede verse en la figura 3.7. En la misma, se observan las interfaces mencionadas anteriormente junto a una serie de componentes que pertenecen a la interfaz *Southbound*. Estos componentes se analizarán más adelante.

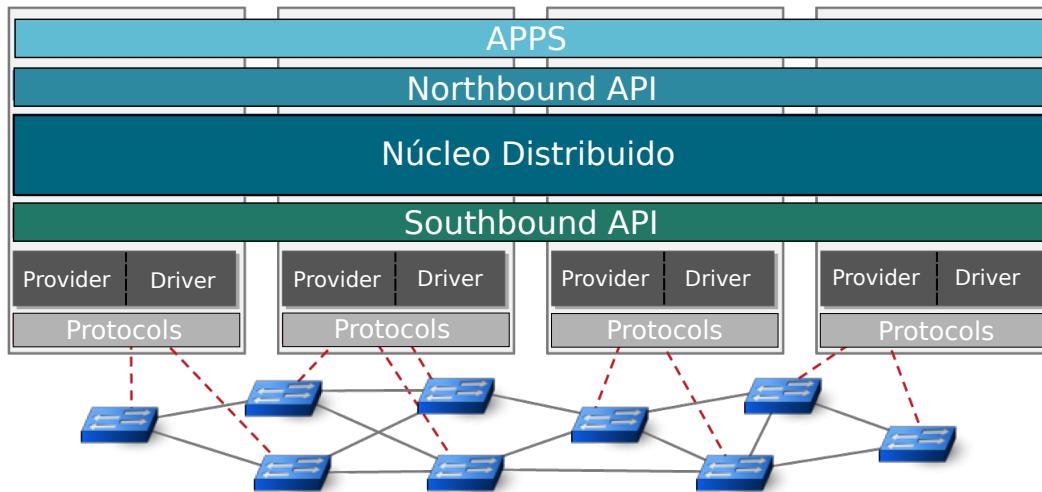


FIGURA 3.7: Arquitectura completa del controlador ONOS.

- **Modularidad:** el controlador se encuentra desarrollado en *Java*, y mediante el *framework OSGi* obtiene las características de una arquitectura modular. De esta forma, se provee a los desarrolladores facilidad para brindar actualizaciones a sus aplicaciones, poder monitorearlas, realizar depuración y mantenimiento.

Interfaz *Southbound* en ONOS

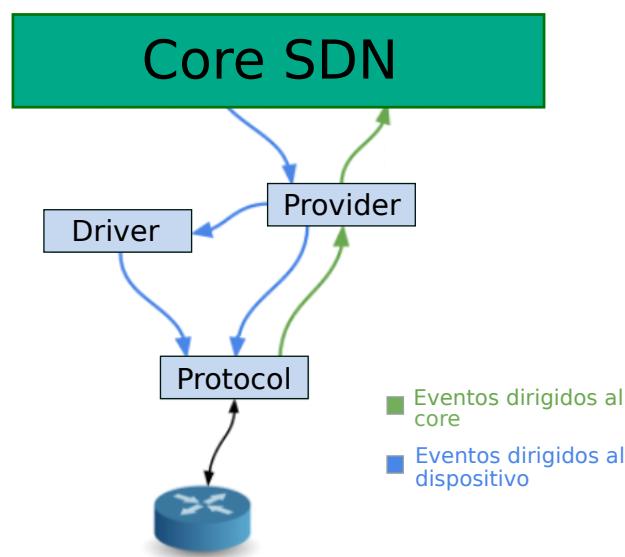
Tal como se explicó anteriormente, el objetivo del proyecto es gestionar la configuración de un *muxponder* de 40GB a través del protocolo *NETCONF*.

Para ello, será necesario explicar con más detalle la interfaz *Southbound* de ONOS. La misma se encuentra dividida en una serie de componentes que se detallan a continuación:

- **Providers:** son aplicaciones independientes que residen en el núcleo de ONOS y que pueden activarse o desactivarse dinámicamente en tiempo de ejecución. El propósito principal de esta capa es abstraer al *core* las complejidades de los protocolos, brindando interfaces de las operaciones típicas y generales de los mismos. Un ejemplo de un *provider* en ONOS es el llamado '*NetconfAlarmProvider*', encargado de transformar cada notificación de los dispositivos en una alarma registrada en ONOS.
- **Protocols:** es la capa de más bajo nivel en la interfaz *Southbound* y es la única que tiene contacto directo con los dispositivos conectados al controlador. Aquí se implementan los diferentes protocolos necesarios para la comunicación como ser *NETCONF*, *REST*, *SNMP*, etc. Comúnmente en esta capa se utilizan librerías de terceros como *openflowj*, *snmp4j*, *thrift*, entre otras.
- **Drivers:** al igual que los *providers*, los *drivers* pueden cargarse dinámicamente al núcleo del controlador y proveen mecanismos para comunicarse con los diferentes dispositivos a través de algún protocolo. La diferencia principal con

los *providers*, es que aquí no se implementan generalidades de los protocolos, sino comportamientos específicos de los dispositivos. Además, sirve de interfaz entre las aplicaciones que se encuentran en la capa *Northbound* y los diferentes equipos de red. El propósito principal de este subsistema es el de aislar el código específico del dispositivo, de tal manera de que el mismo no se extienda por el resto del núcleo de ONOS. Dado que dicho código será necesario para cualquier futuro previsible, este subsistema proporciona medios para contenerlo y permitir que otros subsistemas (por ejemplo, la capa de aplicación) interactúen con él a través de abstracciones independientes del protocolo y del dispositivo. Por último, presenta una ventaja para los desarrolladores de hardware dado que al ser un componente modular, permite la herencia de funcionalidades de otros *drivers* con el fin de compartir características con una familia de dispositivos en común.

La figura 3.8 esclarece la participación que tiene cada componente tanto con el *core* como con el dispositivo.



Justificación de la elección del controlador

En la actualidad, existe una diversidad de controladores *SDN*, como ser *Ryu* (*Python*), *Floodlight* (*Java*), *POX* (*Python*), e incluso implementaciones propietarias.

Se destaca *OpenDaylight* (*Java*), un controlador abierto que soporta una gran lista de protocolos y que, según [12], junto a *ONOS* es uno de los controladores más utilizados en la industria.

La razón determinante por la cual se optó por *ONOS* como controlador *SDN* radica en que el mismo cuenta con una documentación más clara y organizada. Además, se poseía experiencia previa trabajando con dicho controlador. Todo esto facilitó la curva de aprendizaje de las distintas herramientas, donde se pudo tener una rápida interacción con el controlador dada su facilidad de instalación y puesta en marcha.

Otro motivo reside en que las redes de los proveedores de servicio son complejas y multicapas, donde se requiere una separación clara de la capa de paquetes y de la

capa de transporte, tal como se vió en el capítulo anterior. ONOS ha logrado brindar soporte a las redes ópticas según lo demuestra el caso de uso aquí descripto [13].

3.2.2. Análisis de agentes NETCONF

Con el fin de poder gestionar la configuración del *muxponder* de 40GB a través de NETCONF, se estudiará en esta sección dos implementaciones del protocolo: Sysrepo y Yuma123.

Las mismas son *open-source*, lo que facilita el estudio y comprensión de los agentes. Finalmente, se justificará la elección de Yuma123 como servidor NETCONF para el proyecto.

Sysrepo

El proyecto Sysrepo proporciona las funcionalidades de una base de datos lógica a las diferentes aplicaciones Unix-Linux. De esta forma, las aplicaciones pueden gestionar sus datos de configuración y de estado utilizando YANG como modelado de datos, a través de las API's e interfaces que expone Sysrepo [41]. Así, la implementación garantiza mediante YANG la consistencia de los datos y la correctitud de los mismos.

A su vez, Sysrepo integra *Netopeer2* [6] como agente NETCONF. *Netopeer2* es la evolución del proyecto *Netopeer* [5] (discontinuado) y ofrece tanto un cliente como un servidor NETCONF.

Sysrepo fue la primera implementación del protocolo instalada y manipulada en una máquina de propósito general por el alumno. Tiene la ventaja de contar con una gran documentación, como así también una variedad de ejemplos y casos de usos. Además, otra ventaja que presenta es que el hecho de que Sysrepo exponga API's implica una posibilidad de adaptar cualquier aplicación Unix existente al protocolo NETCONF sin mayores cambios.

Yuma123

En el 2011, el proyecto *open-source* YUMA, también conocido como OpenYUMA, sufrió un cambio en su licencia donde esta dejó de ser *BSD*. A partir de entonces, el proyecto tuvo dos ramificaciones: YumaPro [48], ahora perteneciente a YumaWorks, y Yuma123, su versión *open-source*.

Yuma123 nace a partir de la última *release* *BSD* del proyecto OpenYUMA, con el fin de continuar con el soporte de dicha implementación mientras se mantiene la licencia *BSD*. Al igual que Sysrepo, ofrece tanto un cliente (*yangcli*) como un servidor (*netconfd*) NETCONF. La diferencia con la implementación anterior es que aquí no se exponen API's a las aplicaciones, sino que las mismas son directamente compiladas como librerías *SIL* y son dependientes de Yuma123.

Según la documentación [45], se agregaron las siguientes funcionalidades con respecto a la versión original de OpenYUMA:

- Un sistema de compilación más eficiente, basado en las herramientas *autoconf* y *automake*.

- Se han corregidos *bugs* críticos reportados en OpenYUMA.
- Soporte de las nuevas funcionalidades del protocolo agregadas por la IETF (ietf-nacm, ietf-system, etc.).

Evaluación de las implementaciones

A la hora de efectuar una comparación entre ambos proyectos, se tendrán en cuenta los siguientes criterios: las diferencias relativas al protocolo NETCONF; las herramientas y características extras que brinda cada una; y los recursos que demandan.

- **Diferencias relativas al protocolo NETCONF:** Como se detalló en el capítulo anterior, NETCONF define una serie de operaciones que no son obligatorias para las diferentes implementaciones del protocolo, sino que son opcionales y las mismas deberán ser explícitamente anunciadas en el mensaje *HELLO* del servidor. Es importante repasar cuáles de estas operaciones admite cada proyecto.

Tanto Yuma123 [46] como Sysrepo [41] implementan el estándar NETCONF 1.0 y NETCONF 1.1, definidos en los RFC 4741 [19] y RFC 6241 [20] respectivamente.

Sin embargo, mientras que Sysrepo admite el transporte seguro mediante *SSH* y *TLS*, Yuma123 únicamente soporta *SSH*. Esto último, es una ventaja para Sysrepo ya que brinda flexibilidad y personalización al administrador sobre el protocolo de transporte seguro.

Por otra parte, Sysrepo admite únicamente la operación *commit* sobre la base de datos *candidate*, mientras que Yuma123 además de soportar dicha operación también incorpora las capacidades *confirmed-commit* y *validate*, lo que provee a esta última de potentes herramientas para corroborar la correctitud de los datos ingresados y a su vez restaurar la funcionalidad de la red en caso de ingresar una configuración incorrecta.

Para finalizar, cabe destacar que ambos proyectos soportan las bases de datos *startup* y *candidate*.

- **Herramientas y características extras al protocolo:** Ambas implementaciones integran tanto un cliente como un servidor NETCONF. Sin embargo, cada una incorpora una serie de herramientas que resulta de importancia mencionarlas.

- **Sysrepo**

- sysrepoctl: aplicación que permite administrar los módulos YANG desde una *CLI*. Brinda opciones para instalar, eliminar y listar los módulos que tiene activo el servidor.
- sysrepocfg: utilidad para exportar o importar datos de configuración de las diferentes bases de datos. De esta forma se podría editar, por ejemplo, el contenido de la base de datos *startup* desde un navegador *WEB* o editor de texto cualquiera, sin que sea necesario utilizar el protocolo *NETCONF* para dicho propósito.

- **Yuma123**

- yangdiff: herramienta que permite comparar dos revisiones de un mismo módulo YANG. El nivel de detalle con el cual se exponen las diferencias puede ajustarse hasta con tres niveles de reporte. Además, puede generar de forma automática la declaración '*revision*' del módulo con detalles de los cambios.
- yangdump: posibilita validar módulos YANG y convertirlos a otros formatos. De esta forma, mediante un módulo YANG la herramienta genera el esqueleto del código *SIL* (lenguaje C) que necesita para relacionar la instrumentación del dispositivo con el modelado de los datos.

Para finalizar el análisis de este criterio, se menciona que ambas implementaciones permiten parametrizar opciones en el servidor *NETCONF*, como por ejemplo el número máximo de sesiones admitidas, el tiempo de espera para una respuesta *RPC* y el tiempo de espera de una sesión inactiva antes de finalizarla. Además, anteriormente se mencionó que mientras Sysrepo expone *API's* a las diferentes aplicaciones Unix, Yuma123 las integra como librerías *SIL* dependientes de la implementación. Esto último es una ventaja para Sysrepo, ya que tanto Sysrepo como la aplicación funcionarían como procesos diferentes que se comunican mediante interfaces, donde la falla de uno de estos procesos no necesariamente involucra el bloqueo completo del otro. Esto último no sucede en el caso de Yuma123, donde es el servidor quien realiza las llamadas a las librerías *SIL* previamente compiladas, formando un solo proceso.

- **Demanda de recursos:** Al inicio de este capítulo, se estudiaron las características técnicas del *mxp ponder* utilizado para este proyecto. Será de suma importancia que las implementaciones mencionadas se adapten a los recursos que dispone el equipo, por lo que se hará foco principal en demanda de la memoria RAM y de la memoria de almacenamiento.

Dicho esto, es importante mencionar que para el siguiente análisis se iniciaron los binarios con la configuración por defecto. Además, los datos obtenidos corresponden a la ejecución de los mismos en una máquina de escritorio, sin realizar algún tipo de optimización en recursos.

- **Sysrepo:** según la documentación [42], se requiere de una extensa lista de librerías de terceros para poder efectuar la compilación e instalación del proyecto. Teniendo en cuenta dichas librerías necesarias para el funcionamiento de Sysrepo, la implementación demanda un espacio total en memoria secundaria de 250MB. Cabe destacar que en este análisis se incluye

no solo el servidor Netopeer2 sino también el cliente, ya que Sysrepo necesita de ambos para funcionar. En el caso de memoria RAM, Sysrepo ocupa 270MB.

- **Yuma123:** en este caso, la cantidad de librerías de terceros que requiere el proyecto [45] es menor. Además, se destaca que Yuma123 no necesita de ambos binarios (cliente y servidor) para funcionar, pudiendo iniciarse uno u otro según sea necesario. Teniendo en cuenta esto último, únicamente se analizan los recursos que demanda el servidor (llamado *netconfd*), ya que en el dispositivo no será necesario ejecutar un cliente NETCONF. Así, Yuma123 requiere en memoria secundaria un espacio de 50MB, mientras que en memoria principal alcanza los 73MB aproximadamente.

En figura 3.9, en la primer columna, puede verse una comparativa de la memoria RAM que demanda cada implementación, la expresión está dada en el orden de los Kb. El proceso '*netconfd*' corresponde al servidor NETCONF del proyecto Yuma123, mientras que el proceso '*sysrepod*' corresponde a Sysrepo e integra tanto el cliente como el servidor.

VIRT	RES	SHR	S	%CPU	%MEM	HORA+	ORDEN
72108	7856	6084	S	0,0	0,0	0:00.04	<i>netconfd</i>
263260	4484	3820	S	0,0	0,0	0:00.01	<i>sysrepod</i>

FIGURA 3.9: Demanda de recursos de las implementaciones analizadas.

Justificación de elección del agente

Presentado el análisis y las diferencias entre ambos proyectos, en esta sección se justificará la elección de Yuma123 como servidor que se instalará en el *muxponder* de 40GB.

Como se mencionó anteriormente, Sysrepo fue la primera implementación con la que se tuvo contacto y manipulación del protocolo NETCONF. La razón por la que se optó empezar a familiarizarse con este, fue porque se encontró una gran cantidad de ejemplos y casos de uso a la hora de realizar los módulos YANG y relacionarlos con la instrumentación y las aplicaciones Unix. Además, la instalación del proyecto en una computadora de escritorio fue sencilla (debido a la extensa documentación y las diferentes alternativas de instalación que brinda como ser *dockers*, *scripts* de instalación, etc).

Sin embargo, no resultó de igual forma a la hora de realizar la compilación cruzada. La razón se debe a que Sysrepo tiene gran cantidad de dependencias como ser *libyang*, *Google Protocol Buffers*, *protobuf-c*, *libev*, entre otros. Específicamente, se tuvo problemas para compilar la librería '*protobuf-c*' para la arquitectura NIOS, por lo que se abandonó el uso de esta herramienta. Además, como se vio anteriormente, la demanda de memoria principal y secundaria en Sysrepo excede a los recursos disponibles en el muxponder.

En el caso de Yuma123 se logró compilar e instalar de manera correcta todas las librerías requeridas. Además, se realizaron scripts que facilitan dicha tarea para las siguientes arquitecturas: *ARM*, *NIOS* y *x86_64*. Cabe destacar que si bien los recursos que demanda Yuma123 son menores frente a Sysrepo, los mismos siguen siendo excesivos para el muxponder. Por lo tanto, se realizaron optimizaciones en la compilación del proyecto. Por ejemplo, se ha omitido la compilación de la librería *SSH*, ya que el *muxponder* ya la integra. Además, el proyecto incorpora una gran cantidad de módulos *YANG* a modo de ejemplo, estos no son necesarios para el funcionamiento del mismo, por lo que también fueron omitidos. Por último, se destaca la herramienta *yangdump* brindada por Yuma123, la cual facilita de forma significativa el desarrollo de las librerías *SIL* en *C*.

De esta forma, el factor determinante a la hora de elegir entre las distintas implementaciones *NETCONF* fue tener en cuenta las limitaciones técnicas del equipo, siendo Yuma123 el agente que mejor se adaptó a las mismas.

Capítulo 4

Diseño e Implementación

Para el desarrollo del proyecto será necesario implementar un sistema donde se puedan realizar pruebas y evaluar la correctitud del mismo.

De esta forma, la primera sección de este capítulo comprende tanto el análisis del sistema como la topología utilizada. Específicamente, se estudiará su estructura, su comportamiento y sus requerimientos.

En las secciones siguientes, se detallarán las aplicaciones desarrolladas que permiten cumplir con el objetivo del proyecto. En primer lugar, se hará un estudio del módulo YANG implementado, el cual caracteriza y modela los datos del equipo. A continuación, se detallará el *driver* implementado para lograr la comunicación entre el controlador y el dispositivo. Por último, se analizará la interfaz REST y la GUI desarrollada.

4.1. Entorno de trabajo

En esta sección se detallan las características del sistema a implementar, descriptas en el lenguaje de especificación de sistemas SysML [23]. Se optó por este lenguaje de modelado ya que brinda una extensión a UML permitiendo combinar elementos del mundo físico (*hardware*) con elementos del mundo lógico (*software*).

4.1.1. Topología

Se conformará una topología con el fin de poder identificar en una primera instancia, los requerimientos que debe cumplir el sistema. La misma, está basada en un caso de uso simple, en el cual se quiere brindar conectividad a dos clientes a través de un enlace óptico, este último conformado por dos *muxponders*.

Es importante identificar la presencia del controlador *ONOS*, el cual gestionará la configuración de los equipos mediante el protocolo NETCONF. En la figura 4.1 se muestra de forma general la topología planteada.

Los dispositivos terminales A y B, se encuentran conectados al puerto cliente del *muxponder* C y D, respectivamente. A su vez, el transmisor del *muxponder* C se encuentra conectado al receptor del *muxponder* D, y viceversa. Esto permite una comunicación bidireccional, donde ambos clientes pueden tener conectividad.

Por otra parte, el controlador tiene una conexión con los *muxponder* a través de los puertos de control de los mismos.

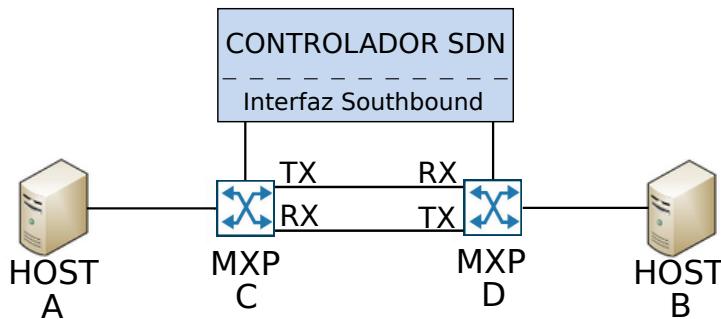


FIGURA 4.1: Topología implementada en el proyecto.

En la figura 4.2 se presenta cómo está dispuesta la conexión física de los equipos. En ella, se puede observar la alimentación de los equipos, los puertos clientes los cuales estarán conectados a los *host* A y B antes mencionados. También, se observa las interfaces de línea conectadas entre sí, de tal manera que se permita una comunicación bidireccional entre los clientes. Por otro lado, las interfaces de control se conectan al controlador ONOS tal como se mencionó anteriormente.

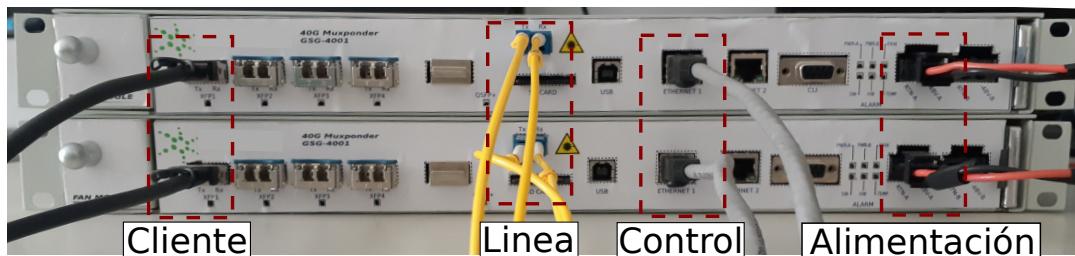


FIGURA 4.2: Conexión física de la topología.

4.1.2. Requerimientos del sistema

Para establecer los requerimientos funcionales del sistema, se presentará en primer lugar un diagrama de caso de uso. Como se puede observar en la figura 4.3, el objeto principal del sistema es poder brindar al administrador un entorno donde pueda gestionar la configuración de los *muxponders* mediante sus aplicaciones.

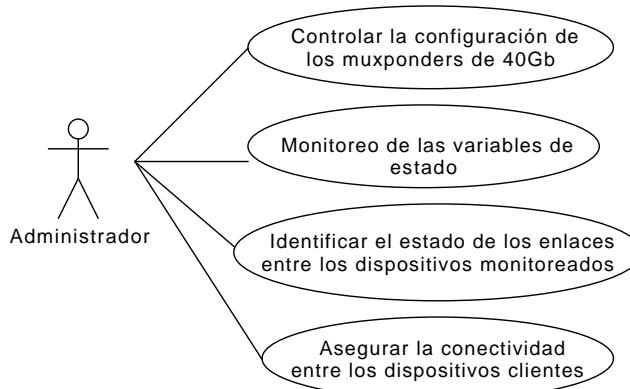


FIGURA 4.3: Caso de uso desde la perspectiva del administrador.

En base a este diagrama, se pueden definir los requerimientos funcionales a nivel de sistema. La figura 4.4 muestra una lista de los mismos.

Como requerimiento no funcional, se puede identificar la adición de nodos virtuales, los cuales no afectan a la funcionalidad del sistema pero brindan más flexibilidad y permiten conformar una topología más compleja.

«Requerimiento» Controlador SDN	«Requerimiento» Conexión con el controlador
id: R-01 El sistema debe brindar el servicio de un controlador SDN.	id: R-02 Se debe establecer una conexión entre los muxponders y el controlador.
«Requerimiento» Servidor web	«Requerimiento» Soporte NETCONF
id: R-03 El sistema debe proveer el servicio de una interfaz web para administrar los dispositivos.	id: R-04 Los dispositivos y el controlador deben soportar el protocolo NETCONF.
«Requerimiento» Nodos físicos	«Requerimiento» Nodos virtuales
id: R-05 El sistema debe soportar la conexión de nodos físicos.	id: R-06 El sistema debe soportar la conexión de nodos virtuales.

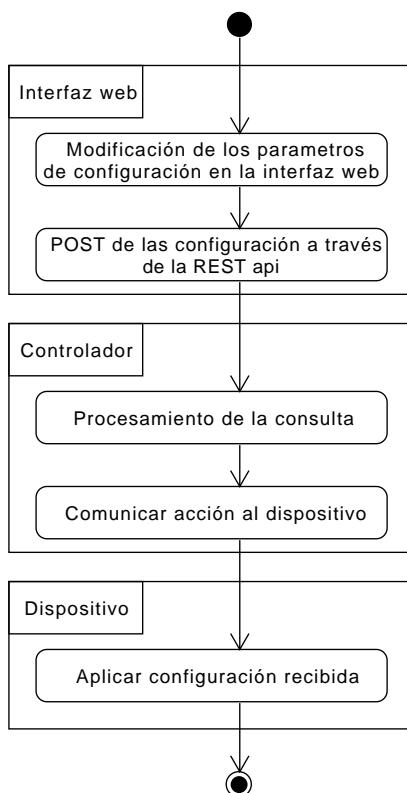
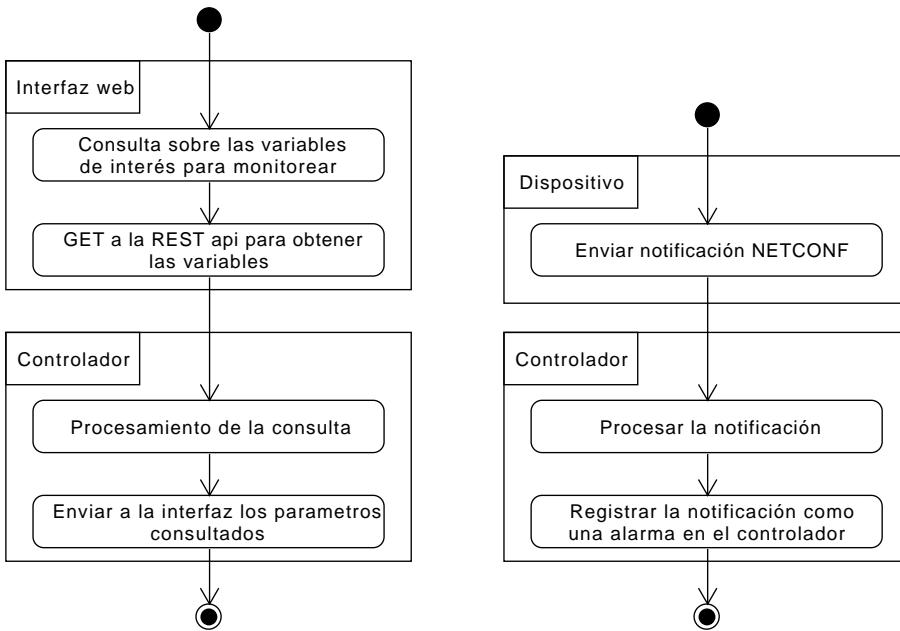
FIGURA 4.4: Requerimientos del sistema.

Además, a partir del diagrama de caso de uso de la figura 4.3, se pueden identificar tres diagramas de actividades relacionadas. La figura 4.5, muestra los flujos de actividad típicos que tendrá el sistema.

Para la actividad relacionada al monitoreo 4.5 (A), la aplicación WEB realiza consultas periódicas al controlador con el fin de obtener información sobre los dispositivos. Así, se envía un mensaje HTTP con la operación GET desde la aplicación, el controlador procesa la petición y responde dicha consulta.

Por otra parte, para el flujo de actividad relacionado a las notificaciones que puede verse en la figura 4.5 (B), es el dispositivo quien emite inicialmente el mensaje mediante una notificación NETCONF. En el controlador se procesa la notificación y se la registra como alarma.

Por último, se tiene el diagrama de actividad relacionado a la configuración del equipo 4.5 (C). El evento inicial para este caso, es la adición de una configuración desde la aplicación WEB. Dicha configuración, una vez procesada se traduce en una solicitud POST HTTP que se envían hacia la *Northbound interface* del controlador. Una vez recibida la solicitud, se realiza su procesamiento y se envía el mensaje de configuración NETCONF a los dispositivos involucrados a través de la *Southbound interface*.



(C) Actividad de configuración.

FIGURA 4.5: Diagramas de actividad del sistema.

4.2. Integración del protocolo NETCONF al muxponder

La sección anterior deja claro que uno de los requerimientos de sistema será que tanto el controlador ONOS como los dispositivos a monitorear soporten NETCONF como protocolo de gestión de la configuración.

Como se vio en el capítulo anterior, el controlador soporta dicho protocolo, por lo que para cumplir con este requerimiento de sistema únicamente será necesario adaptar NETCONF al dispositivo.

4.2.1. Requerimientos

Los requerimientos que deberá cumplir la integración del protocolo son los que se observan en la figura 4.6.

«Requerimiento» Adaptar NETCONF al equipo	«Requerimiento» Monitoreo de datos de estado
id: R-07 Se deberá instalar algún agente del protocolo en el dispositivo.	id: R-08 Se debe poder monitorear cualquier variable de memoria compartida del dispositivo a través de NETCONF.
«Requerimiento» Alarmas mediante notificaciones	«Requerimiento» Gestionar datos de configuración
id: R-09 Las alarmas emitidas por el dispositivo deberán notificarse mediante el protocolo NETCONF.	id: R-10 Se debe poder realizar cambios en la configuración del equipo mediante el protocolo NETCONF.

FIGURA 4.6: Requerimientos para la integración del protocolo NETCONF.

4.2.2. Compilación e instalación del agente

Siendo Yuma123 el agente que se eligió para integrar el protocolo en el equipo, en esta sección se detalla el procedimiento que se llevó a cabo para la compilación e instalación del agente en el *muxponder*, con el fin de poder cumplir el requerimiento R-07.

En primer lugar, toda la tarea de compilación se realizó en una computadora de propósito general debido a los recursos limitados con los que cuenta el dispositivo. Para facilitar la compilación e instalación, se realizaron tres scripts los cuales se describen a continuación:

- **Dockerfile:** el objetivo de este *script*, es el de realizar la compilación del proyecto Yuma123, dejando todas las librerías y los binarios en una carpeta que luego deberá copiarse en el dispositivo. Dockerfile [7], es un archivo de texto que contiene los pasos e instrucciones que la herramienta Docker deberá seguir para construir una imagen. En el mismo, se indica una imagen de referencia (ubuntu:16.04) que servirá como base para la construcción. Luego, se descargan todas las librerías requeridas por el proyecto Yuma123 junto con

los compiladores necesarios para realizar la compilación cruzada. A partir de aquí, se compila cada una de las librerías para la arquitectura objetivo (por ejemplo, NIOS II) y finalmente se compila también el proyecto Yuma123. Todos los binarios, librerías y cabeceras resultantes se encuentran en la carpeta '/root/usrapp' de la imagen Docker construida. Cabe destacar que se realizaron tres versiones del *script*, de esta forma compilar para las arquitecturas NIOS II, ARM y x86_64.

- **remote_install_yuma.sh**: *script bash* que tiene la tarea de realizar la instalación del protocolo, compilado previamente con Docker y Dockerfile. Para ello, requiere de tres parámetros: usuario del dispositivo remoto, dirección IP del dispositivo remoto y la arquitectura deseada. Con estos parámetros, el *script* realiza la instalación del agente mediante SSH y SCP [33], copiando el contenido necesario de '/root/usrapp' que se generó con la construcción de la imagen Docker, al directorio '/root/usrapp' del dispositivo. Es importante mencionar que muchas de las librerías requeridas por Yuma123 son necesarias únicamente para la compilación y no para el funcionamiento del protocolo, por lo que este *script* omitirá dichas librerías con el fin de reducir el tamaño que ocupa el agente en memoria.
- **remote_uninstall_yuma.sh**: requiere dos parámetros los cuales son el usuario del dispositivo remoto y la dirección IP del mismo. El objetivo de este *script* es facilitar la desinstalación de todas las librerías relacionadas a Yuma123 del dispositivo.

4.2.3. Diseño del módulo YANG

Para poder cumplir con los requerimientos R-08, R-09 y R-10 que se muestra en la figura 4.6, se diseñó un módulo YANG que contiene cinco secciones bien definidas, las cuales se describen a continuación:

- **Cabecera del módulo y declaraciones**: aquí se declara la estructura inicial del módulo YANG. Se define un nombre y un prefijo, se realiza una descripción del mismo y por último se realiza la definición de los datos utilizados por el módulo. Cabe destacar que se definieron tres tipos de datos: 'restricted-tipo-trafico', 'restricted-tipo-fec-linea' y 'restricted-tipo-fec-cliente'. En ellos, se especifica a través de la directiva 'enum' cuales serán los valores aceptados que pueden tomar dichos tipos de datos. Por ejemplo, dado que la configuración del tipo de tráfico para este dispositivo únicamente admite dos valores ('otu2' y 'xge'), es importante restringir el ingreso de algún otro valor ya que podría ocasionar errores en la configuración. Se puede observar una porción de esta sección en el código 4.1, donde se detalla la cabecera del módulo y sus declaraciones.

LISTING 4.1: Cabecera del módulo YANG.

```

module cli-mxp {
    namespace 'http://fulgor.com/ns/cli-mxp';
    prefix 'cli-mxp';
    description
        'CLI para configurar el muxponder de 40G';
    revision '2018-06-24' {
        description
            'Version 0.1.0';
    }

    typedef restricted-tipo-trafico {
        type enumeration {
            enum 'otu2';
            enum 'xge';
        }
    }
    ...
    ...
    ...

```

- **Container YANG de configuración:** en esta sección se declara un *container* llamado ‘mux-config’. Aquí se describen todos los parámetros que admiten una configuración (por ejemplo, el tipo de fec de línea), a través de las declaraciones ‘leaf’. Un fragmento de esta sección puede observarse en el código 4.2, donde además se puede ver el uso de los tipos de datos definidos en la cabecera del módulo.

LISTING 4.2: Container de configuración.

```

container mux-config {
    description 'Parametros de la CLI';

    leaf tipo_trafico {
        description
            '[otu2|xge] especifica el tipo de átrfico.';
        type restricted-tipo-trafico;
    }

    ...
    ...
    ...

    list ports {
        key 'port';
        leaf port {
            type int16{
                range '0 .. 6';
            }
            mandatory true;
        }

        leaf neighbor {
            mandatory true;
            type string;
        }

        leaf port_neighbor {

```

```

        mandatory true;
        type string;
    }
}
}

```

- **Container YANG de estado:** de igual forma, se realizaron *containers* para los datos de estado los cuales no admiten una escritura de valores y son necesarios para monitorear el dispositivo. El código 4.3 presenta una parte de esta sección del módulo, donde puede apreciarse la directiva 'config false', la cual indica que el *container* no admitirá datos de configuración.

LISTING 4.3: Container de estado.

```

container mux-state {
    description 'Representa a datos de estado del dispositivo.';

    config false;

    leaf fpga_temperature_state {
        description 'Temperatura de la FPGA';
        type decimal64 {
            fraction-digits 2;
        }
    }

    leaf device_boardId {
        description 'Identificador unico del dispositivo';
        type string;
    }
    ...
    ...
    ...
}

```

- **Definición de RPC:** como se estudió en capítulos anteriores, NETCONF permite definir RPC propias de un módulo con el fin de extender la funcionalidad de los dispositivos. Se define así una RPC cuya utilidad será la de poder indicar al agente cuándo debe aplicar la configuración que contiene el *container* 'mux-config' en el dispositivo. El código 4.4 muestra dicha sección del módulo. En ella, se puede notar que la RPC admite una respuesta de la operación solicitada, la cual está contenida en la *leaf* 'respuesta-mux-apply-config' y es de tipo *String*. En este mensaje se indica el resultado de la operación.

LISTING 4.4: Declaración de RPC.

```

rpc mux-apply-config {
    description 'RPC que aplica los cambios de configuracion';
    output {
        leaf respuesta-mux-apply-config {
            type string;
        }
    }
}

```

- **Definición de notificación:** por último, el módulo tiene una sección donde se declara una notificación. Dicho mensaje será utilizado para indicar a las sesiones conectadas y suscritas las diferentes alarmas que produzca el dispositivo. Estos mensajes se transportan mediante notificaciones del protocolo NETCONF. El propósito de estos mensajes es el de, por ejemplo, reportar mediante una alarma si un enlace con un dispositivo vecino se cayó, si el dispositivo supera la temperatura umbral, etc. Se puede observar en el código 4.5 la declaración de la notificación en el módulo. El mensaje estará contenido dentro de la *leaf* 'INFO', en la cual se especifica de forma obligatoria con la directiva 'mandatory' cuál será el mensaje que se enviará como notificación.

LISTING 4.5: Declaración de notificación.

```
notification mux-notify {
    leaf INFO {
        type string;
        mandatory 'true';
    }
}
```

4.2.4. Diseño de la librería C para el agente NETCONF

Teniendo en cuenta las aplicaciones integradas en el *muxponder* las cuales fueron explicadas en el capítulo anterior, se procede a detallar el diseño de la librería en el lenguaje C. Para ello, se utilizó la herramienta *yangdump* del proyecto Yuma123, la cual genera un esqueleto de la aplicación a partir de un módulo YANG dado. Se forman así dos archivos, uno con extensión '.h' (*headers*) y otro con extensión '.c' (código fuente).

En el primero, la herramienta declara todas las variables, funciones y los tipos de datos que va a utilizar la librería.

Por otra parte, el segundo archivo contiene la estructura de la aplicación en sí. En él, se encuentran implementadas todas las funciones declaradas en el archivo con extensión '.h', las cuales llamará el agente en caso de que ingrese un mensaje referido al módulo YANG en cuestión. Todo el desarrollo de la aplicación y la relación entre la instrumentación del dispositivo con el módulo YANG se encuentra en este archivo.

Con el fin de explicar cómo se desarrolló esta aplicación, se distinguen dos flujos de actividades bien definidos, uno para las operaciones que son sincrónicas con los mensajes que envía el cliente, y otro para aquellas que sean asíncronas a los mensajes del mismo.

Para el primer grupo, se tiene entonces las operaciones como obtención de un dato de estado o de configuración, modificación de un dato de configuración y ejecución de *RPC*, mientras que el segundo grupo contempla el envío de notificaciones, las cuales son asíncronas a las operaciones del cliente.

Se muestra el comportamiento de este primer grupo en el diagrama de actividad de la figura 4.7. Cada vez que llega un mensaje NETCONF al agente Yuma123, el mismo procesa y verifica a qué módulo YANG hace referencia el mensaje y qué tipo de operación requiere el cliente.

Si la operación es una consulta por una variable de estado o de configuración, el agente realiza una llamada a una función relacionada a la variable consultada. En

dicha función, lo que se hace es tomar el valor de memoria compartida del dispositivo, castear el mismo según indique el modulo YANG (*string*, *int*, *uint*, etc) y por último, emitir una respuesta al cliente con el valor del dato consultado.

Por otra parte, si la operación es la de editar una variable de configuración, el agente llama a una función de la librería C relacionada al módulo en cuestión, donde se actualiza el valor de dicha variable. Además, el agente emite un mensaje con el resultado de la operación.

Por último, si la operación trata de una *RPC* definida en el módulo YANG, el agente llama a la función relacionada a la *RPC* la cual contiene las instrucciones para efectuar la tarea solicitada. En este caso, se tiene una *RPC* que indica cuándo se deberá aplicar la configuración en el dispositivo. Así, al momento de llamar a esta *RPC* el agente copia los valores de los datos de configuración necesarios (tipo de tráfico, tipo fec de cliente, tipo fec línea, etc) y los aplica haciendo uso del binario 'muxponder'.

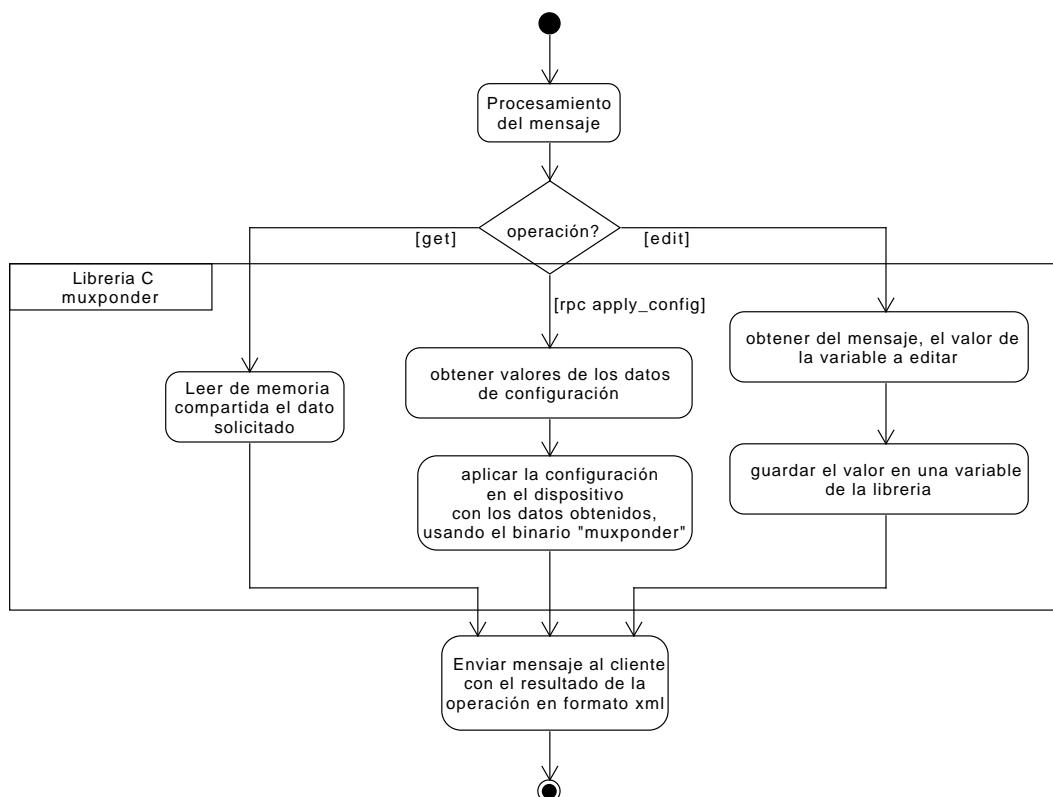


FIGURA 4.7: Diagrama de actividad de las operaciones síncronas con el cliente.

Por otra parte, el grupo relacionado a las operaciones asíncronas con los mensajes del cliente, no es otra cosa que la operación de envío de notificaciones mediante el protocolo NETCONF. Para ello, la librería desarrollada en C crea un hilo que examina periódicamente cada tres segundos la memoria compartida del dispositivo.

La razón por la cual se examina cada tres segundos está relacionada con la aplicación 'monitor', la cual actualiza los valores de memoria compartida con esa frecuencia.

Al examinar los valores de las alarmas, las compara con la información antigua que se tenía almacenada sobre las mismas. Si la información es igual, no se envían notificaciones a las sesiones. En cambio, si la información actual es diferente a la información anterior, será necesario notificar a las sesiones suscritas este nuevo estado de las alarmas. Así, tanto el nombre de la alarma como su nuevo estado son enviados a través de la notificación definida en el código 4.5, haciendo uso de la *leaf* INFO.

Un diagrama de actividad de estas operaciones se puede observar en la figura 4.8.

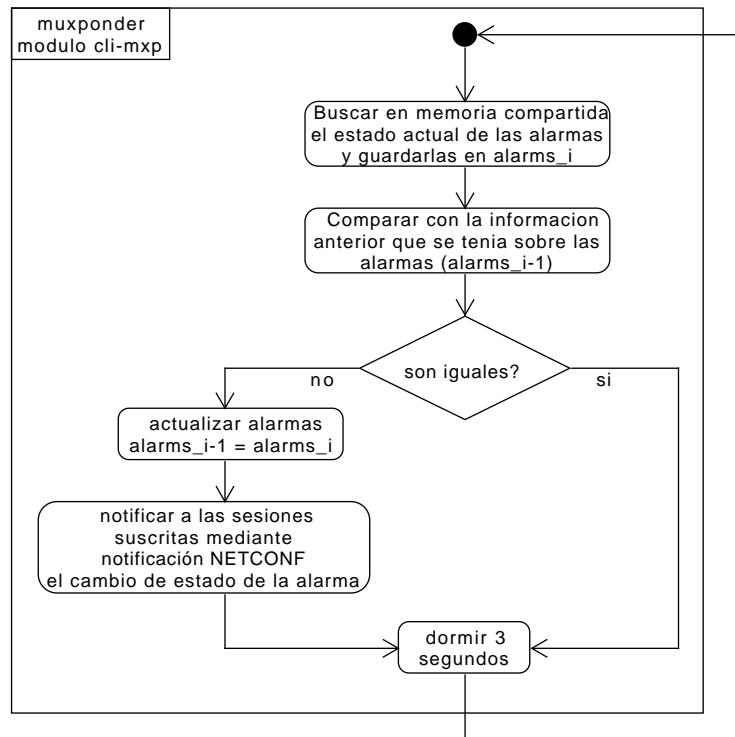


FIGURA 4.8: Diagrama de actividad de las notificaciones.

4.3. Diseño del driver

Como se vio en capítulos anteriores, ONOS se comunica con los dispositivos a través de tres componentes de la interfaz *Southbound*: *Providers*, *Protocols* y *Drivers*.

Así, para poder indicar al controlador cuáles serán las operaciones y los comportamientos específicos del *muxponder* de 40GB, será necesario desarrollar un *driver* (Java) en la interfaz *Southbound* del controlador.

4.3.1. Requerimientos

A fin de cubrir las necesidades del administrador, visto en el caso de uso de la figura 4.3, el *driver* desarrollado deberá cumplir con los requerimientos funcionales de la figura 4.9.

<p>«Requerimiento»</p> <p>Descubrimiento del dispositivo</p> <p>id: R-11 El driver desarrollado deberá ser capaz de identificar las características básicas del equipo en el momento de la conexión.</p>	<p>«Requerimiento»</p> <p>Descubrimiento de enlaces</p> <p>id: R-12 El driver debe proveer mecanismos e indicaciones al controlador sobre cómo están conformado los enlaces con los dispositivos vecinos.</p>
<p>«Requerimiento»</p> <p>Soporte a las RPC</p> <p>id: R-13 El driver deberá brindar soporte a todas las RPC definidas en el módulo YANG del dispositivo.</p>	<p>«Requerimiento»</p> <p>Comandos CLI de ONOS</p> <p>id: R-14 El driver debe exponer comandos CLI a las operaciones típicas del dispositivo, con el fin de poder administrar el mismo desde la consola de ONOS.</p>

FIGURA 4.9: Requerimientos para el *driver* de la interfaz *Southbound*.

4.3.2. Descubrimiento del dispositivo

El controlador ONOS reconoce la presencia de un nuevo dispositivo a través de un mensaje en formato JSON, el cual contiene información como la dirección IP del equipo, el *driver* que describe sus comportamientos, el protocolo que utiliza, entre otra información de utilidad.

Un ejemplo de este mensaje se muestra en el código 4.6. Dicho mensaje, es enviado al controlador haciendo uso del comando de ONOS 'onos-netcfg' [26].

LISTING 4.6: Mensaje JSON con información del dispositivo.

```
{
  'devices': {
    'netconf:172.16.0.141:830': {
      'netconf': {
        'ip': '172.16.0.141',
        'port': 830,
        'username': 'user',
        'password': 'pass',
      },
      'basic': {
        'driver': 'altura-netconf'
      }
    }
  }
}
```

Al momento de indicar al controlador ONOS la presencia de un nuevo dispositivo, el mismo hace una llamada por única vez a la función *DeviceDescriptionDiscovery*, la cual se encuentra implementada en el *driver* indicado por el archivo JSON.

Esta función, tiene la tarea de descubrir las características más generales del equipo, como ser la versión de *software* y de *hardware* del mismo, el número de puertos disponibles, el identificador único del dispositivo, etc.

Con más detalle, la función inicia la sesión SSH del protocolo NETCONF, espera a que termine el intercambio de capacidades entre cliente y servidor y por último envía un mensaje NETCONF al servidor solicitando con la operación 'GET' los siguientes datos de estado:

- información del fabricante.
- versión de *hardware*.
- versión de *software*.
- identificador único del equipo.
- alarmas activas en el equipo.

La figura 4.10 muestra el flujo de actividad típico que tendría el controlador ONOS al momento de agregarse un nuevo dispositivo administrado por el *driver* desarrollado.

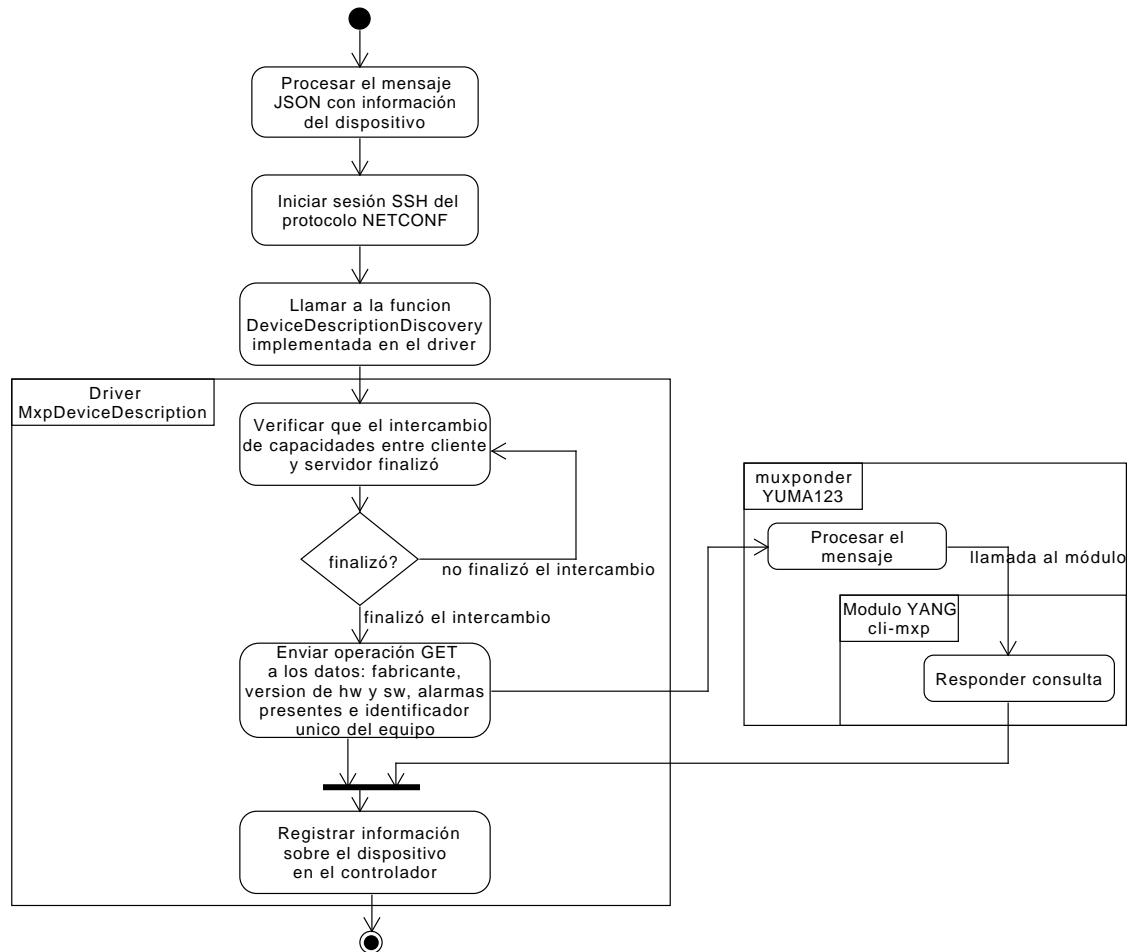


FIGURA 4.10: Diagrama de actividad de la función *DeviceDescriptionDiscovery*.

4.3.3. Descubrimiento de Enlaces

El *driver* también debe proveer un mecanismo para indicar al controlador cómo se componen los enlaces entre los diferentes dispositivos administrados. Para ello, el controlador ONOS brinda una interfaz llamada *LinkDiscovery*, la cual se deberá implementar en el *driver*.

Así, el controlador llama periódicamente a esta función (cada 30 segundos de forma predeterminada, pudiéndose cambiar este tiempo desde la *CLI*) para corroborar el estado de los enlaces.

Con más detalle, lo que realiza esta función es enviar periódicamente a los dispositivos un mensaje NETCONF con la operación GET-CONFIG, consultando por los datos 'port', 'neighbor' y 'port-neighbor' del container 'mux-config', estos datos pueden verse representados en el módulo YANG, en el código 4.2. A continuación, se explica de forma breve la función de cada uno de estos datos:

- **port**: indica el puerto del dispositivo local al cual se conectará un vecino.
- **neighbor**: contiene el identificador único del dispositivo vecino.
- **port-neighbor**: indica el puerto del dispositivo vecino que se conectará en 'port' y con el que deberá formar el enlace.

Con esta información, el *driver* informa al controlador que forme un enlace óptico entre ambos dispositivos. Si alguno de los dispositivos involucrados contiene alarmas registradas respecto al enlace de línea del *muxponder*, concretamente alarmas relativas al receptor, el enlace no se forma. El diagrama de actividad de la figura 4.11 muestra lo explicado anteriormente.

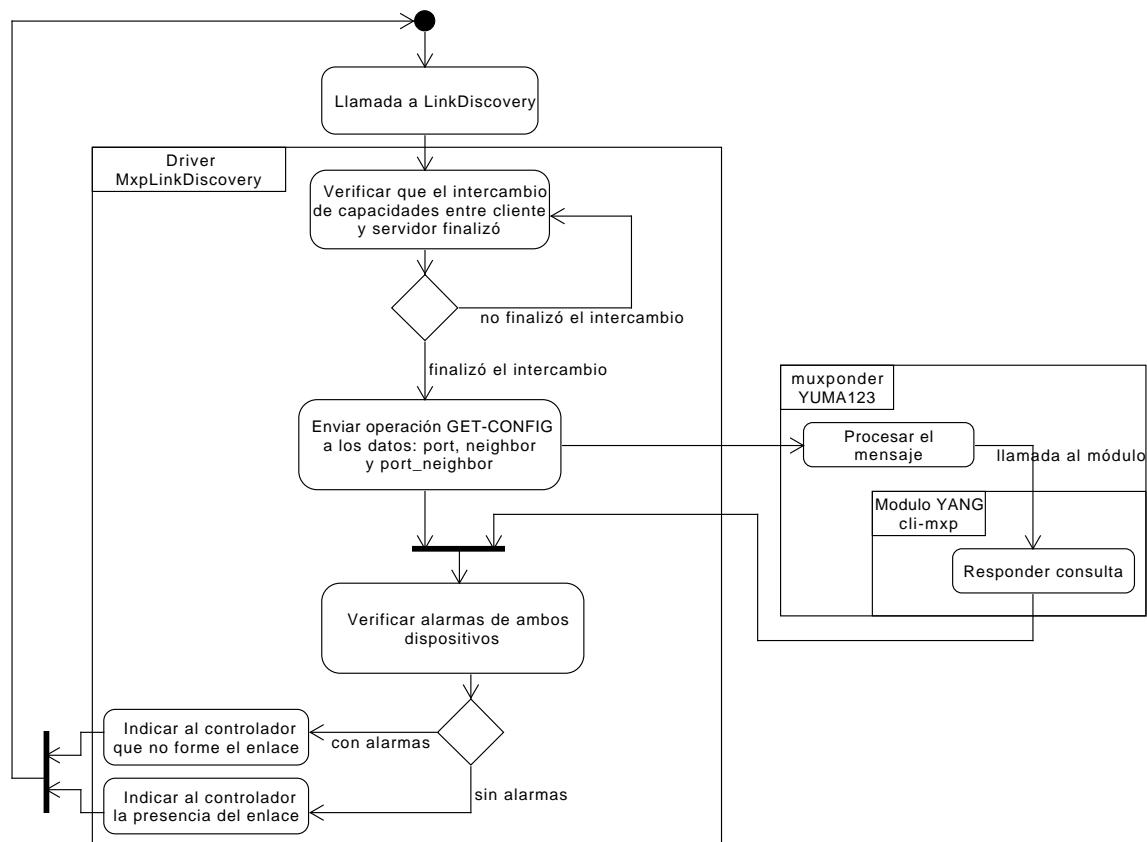


FIGURA 4.11: Diagrama de actividad de la función *LinkDiscovery*.

Es importante mencionar que en esta instancia, no se consulta al dispositivo por sus alarmas con un mensaje NETCONF ya que las mismas son enviadas asíncronamente mediante notificaciones por el dispositivo, y registradas por el controlador

como alarmas. Por lo tanto, para verificar el estado de las alarmas de un dispositivo solo se consulta internamente en el *core* de ONOS.

4.3.4. Operaciones definidas en el *driver*

El *driver* desarrollado brinda, además de las implementaciones de *LinkDiscovery* y *DeviceDescriptionDiscovery* explicadas anteriormente, la posibilidad de ejecutar cualquier operación admitida por el módulo del dispositivo, entre ellas la *RPC* que se describió en el código 4.4. Se explica así el funcionamiento de la interfaz implementada para la operación *RPC* 'mux-apply-config'.

Al momento de llamar a la función *rpcApplyConfig*, la cual describe el comportamiento que tendrá la *RPC* 'mux-apply-config' en el *driver*, el mismo envía un mensaje al *muxponder* solicitando que aplique la configuración que tiene el *datastore running* haciendo uso del binario 'muxponder', tal como se mostró en la figura 4.7.

Luego, dado que se puede indicar la presencia de dispositivos vecinos, es necesario que el *driver* corrobore que la configuración aplicada entre ellos sea la misma para garantizar la conectividad entre los clientes conectados a los *muxponders*. Así, si se aplica una configuración en un *muxponder*, el controlador deberá consultar y comparar la configuración que llevan los dispositivos vecinos. Si la configuración resulta ser la misma, no se genera ninguna alarma, de lo contrario se deberá generar y registrar una alarma en el controlador indicando una configuración inconsistente entre los dispositivos.

Teniendo en cuenta esto, el diagrama de la figura 4.12 muestra el flujo de actividad que sigue el *driver* cuando recibe una llamada a 'mux-apply-config' para el *muxponder A*. En primer lugar, el *driver* envía un mensaje al dispositivo con la operación *RPC* que define el módulo YANG. El agente Yuma123 recibe este mensaje, lo procesa y aplica la configuración en el equipo haciendo uso de los datos de configuración que tenga el *datastore running*. Por último, se envía un mensaje con la respuesta de esa operación.

Luego, el *driver* consulta al mismo *muxponder* si tiene algún vecino conectado. Para este primer caso, el *muxponder A* no tiene especificado ningún vecino, por lo que no se generará alguna alarma sobre configuración inconsistente, de hecho se verifica que no tenga alarmas de este tipo y de tenerlas se eliminan.

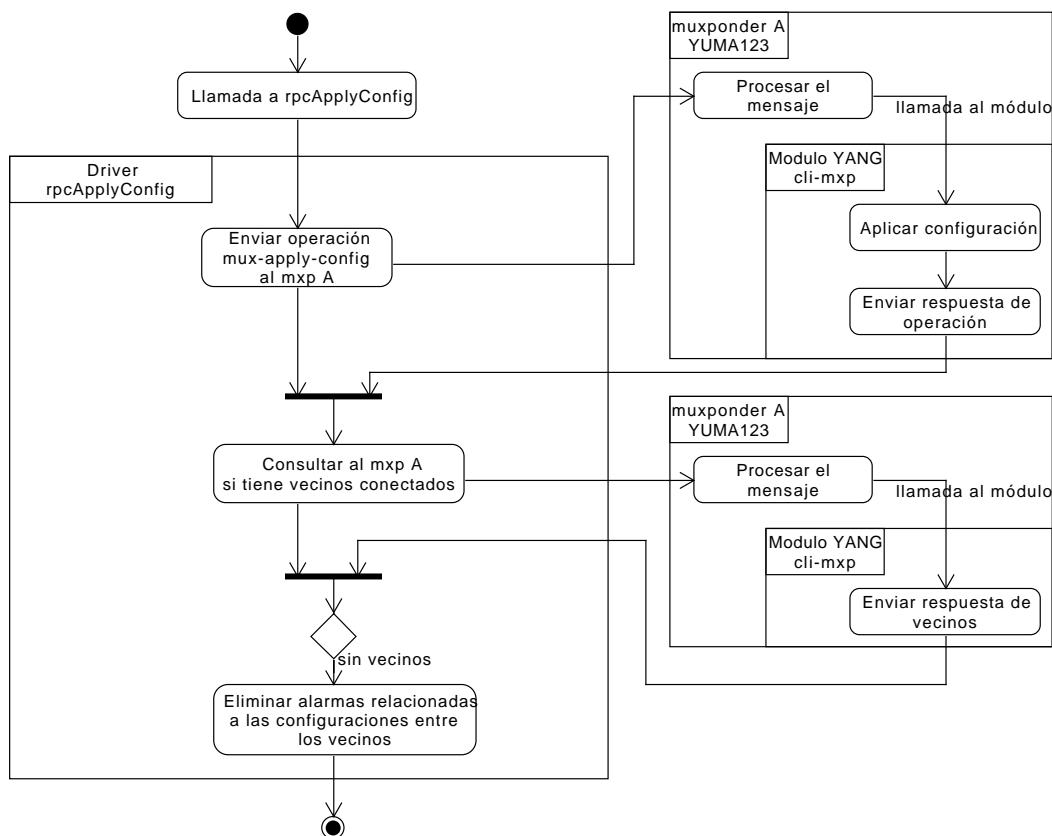


FIGURA 4.12: Diagrama de actividad para la RPC 'mux-apply-config', sin vecinos.

En caso de que el *muxponder A* tenga vecinos conectados, el flujo de actividad es el que se muestra en la figura 4.13. Se consulta al dispositivo vecino (*muxponder B*) su configuración y se la compara con la configuración aplicada recientemente al dispositivo local (*muxponder A*). Si las configuraciones resultan ser las mismas, se buscan las alarmas relacionadas a configuración inconsistente entre el *muxponder A* y *B*, y de existir, se eliminan. Por el contrario, si la configuración es distinta, se crea una alarma y se la registra en el controlador.

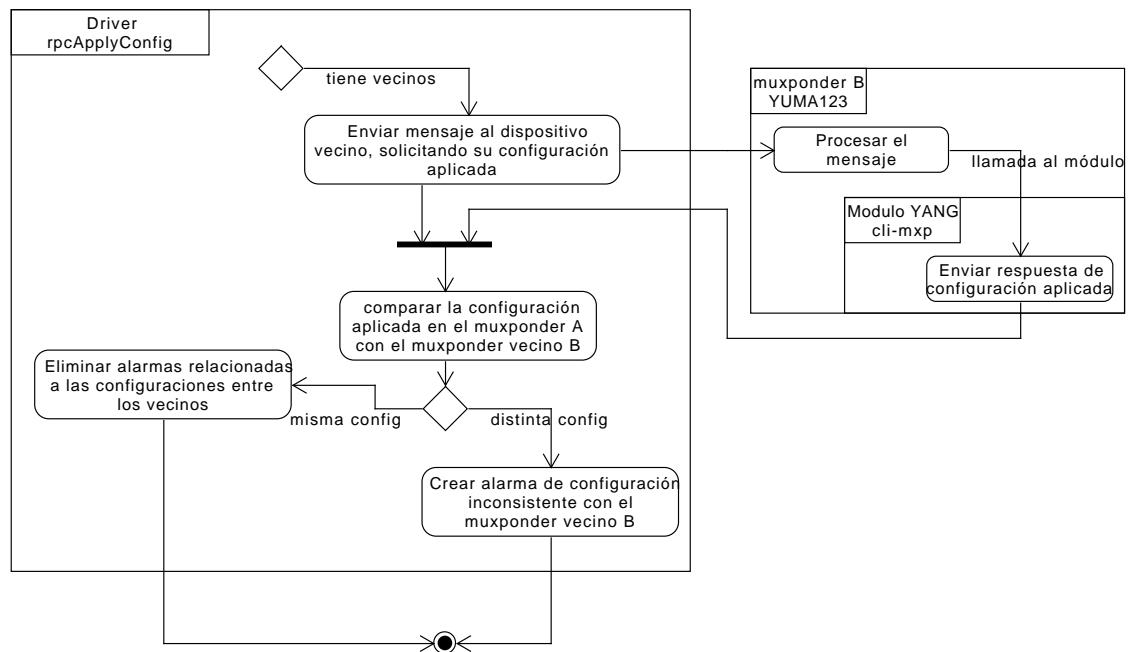


FIGURA 4.13: Diagrama de actividad para la RPC 'mux-apply-config', con vecinos.

Por último, es importante mencionar que con el fin de cumplir con el requerimiento R-14 de la figura 4.9, se implementaron comandos *CLI* para que el administrador pueda interactuar con los dispositivos a través del *driver*, haciendo uso de la consola de ONOS. De esta forma, el administrador puede llamar a cualquiera de las funciones explicadas anteriormente, permitiéndole así poder gestionar la configuración de los dispositivos a través de la consola.

4.4. Diseño de la interfaz Northbound e Interfaz de usuario

Para cumplir con los requerimientos del sistema, será necesario crear en primera instancia una interfaz *REST API* a las aplicaciones externas, para que las mismas puedan comunicarse con los dispositivos administrados (*muxponders*) por el controlador. Como se estudió en capítulos anteriores, ONOS utiliza una interfaz llamada *Northbound* para comunicarse con la capa de aplicación, y es aquí donde se encuentra implementada la aplicación *REST*.

También, se deberá diseñar y crear una aplicación *WEB* que sirva como interfaz de usuario al administrador, y a diferencia de la aplicación *REST*, la *GUI* desarrollada residirá en la capa de aplicación. La figura 4.14 esclarece la ubicación de las aplicaciones mencionadas anteriormente.

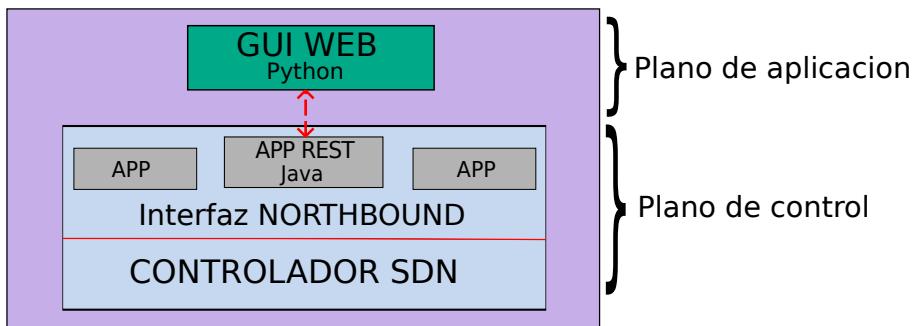


FIGURA 4.14: Interfaz REST e interfaz de usuario.

4.4.1. Requerimientos

A continuación, se listan en la figura 4.15 los diferentes requerimientos que deberán cumplir la interfaz REST y la GUI. Los requerimientos R-15, R-16 y R-17 corresponden a la interfaz REST, mientras que los requerimientos R-18 a R-21 pertenecen a la GUI desarrollada.

«Requerimiento» Interfaz a las operaciones de consulta	«Requerimiento» Interfaz a las operaciones de modificación	«Requerimiento» Interfaz a la RPC mux-apply-config
<p>id: R-15 ONOS debe proveer una REST API en la interfaz Northbound, para que aplicaciones externas puedan realizar tareas de monitoreo relativas al muxponder mediante consultas NETCONF</p>	<p>id: R-16 ONOS debe proveer una REST API en la interfaz Northbound, para que aplicaciones externas puedan realizar cambios en la configuración de los equipos, a través de mensajes NETCONF</p>	<p>id: R-17 ONOS debe proveer una REST API en la interfaz Northbound para que aplicaciones externas puedan aplicar los cambios en el muxponder a través de la RPC mux-apply-config</p>

(A) Requerimientos para la aplicación REST.

«Requerimiento» Sección de visualización de alarmas en la GUI	«Requerimiento» Sección de visualización de la configuración en la GUI
<p>id: R-18 Se deberá poder visualizar en una sección de la aplicación web, las alarmas activadas en los dispositivos.</p>	<p>id: R-19 Se deberá poder visualizar en una sección de la aplicación web, la configuración aplicada en los equipos.</p>
«Requerimiento» Sección de cambios de configuración en la GUI	«Requerimiento» Sección de visualización de los datos de estado en la GUI
<p>id: R-20 La aplicación web debe contar con una sección donde se pueda cambiar la configuración de los muxponders mediante perfiles de configuración.</p>	<p>id: R-21 Todos los datos de estado de los equipos se deben poder visualizar en una sección de la aplicación web.</p>

(B) Requerimientos para la aplicación WEB.

FIGURA 4.15: Requerimientos de las interfaces REST e interfaz gráfica.

4.4.2. Implementación de la REST

Para el desarrollo de la aplicación que se ejecuta en la interfaz *Northbound* del controlador, se utilizó la herramienta *onos-create-app* [24]. La misma, crea un esquema de una aplicación simple con una interfaz *REST*, a partir de la cual se realizaron modificaciones para poder cumplir con los requerimientos R-15, R-16 y R-17.

Así, la aplicación *REST API* se encuentra dividida en cinco clases de Java, las cuales se detallan a continuación.

- **AppComponent:** esta clase resulta del uso de la herramienta *onos-create-app*. Aquí se define el comportamiento que tendrá la aplicación al momento de su activación y desactivación. En este caso, cuando se activa la aplicación en el controlador, la misma inicia un objeto *Listener* para poder imprimir mensajes de log y *debug*.
- **AppWebApplication:** también resulta del uso de la aplicación mencionada anteriormente. El objetivo de esta clase, es la de indicar cuáles serán las funciones de la aplicación que serán expuestas en la *Northbound interface* de ONOS.
- **GetWebResource:** en esta clase se definen las operaciones de consulta que son expuestas, a través de la clase *AppWebApplication*, a la interfaz *Northbound* del controlador. En ella, se definen funciones que tienen operaciones GET de HTTP, las cuales aceptan ciertos parámetros dependiendo de la operación (por ejemplo, indicar a qué dispositivo se quiere realizar la consulta). Seguidamente, la función llama al *driver* del dispositivo con los parámetros que recibió, y devuelve una respuesta a las aplicaciones que la llamaron.
- **RpcWebResource:** de forma similar, esta clase expone una interfaz *REST API* a la *RPC 'mux-apply-config'* definida en el módulo *YANG*. Así, las aplicaciones externas especifican el id de un dispositivo, para que luego la interfaz *REST* se comunique con el mismo mediante el *driver* desarrollado.
- **SetWebResource:** por último, se expone una interfaz con operaciones PUT de HTTP, con las cuales se posibilita que las aplicaciones externas puedan realizar cambios en las bases de datos *running*, *candidate* o *startup* de los dispositivos.

Se muestra en la figura 4.16 un ejemplo de la interfaz *REST*. En la misma, se puede observar las diferentes operaciones expuestas explicadas anteriormente.

The screenshot shows a web-based REST API documentation for 'Altura APP'. At the top, there's a header with a logo, the text 'Altura APP', and a red 'Explore' button. Below the header, the title 'Altura APP' is displayed, followed by the subtitle 'REST API PARA ADMINISTRAR MXP40GB'. The main content is organized into sections based on HTTP methods:

- SET : Setea datos de configuracion**
 - PUT /SET/Tipo de Trafico/{uri},{TIPO_TRAFICO} Setea tipo trafico
 - PUT /SET/Neighbor/{uri},{puerto_local},{vecino},{puerto_vecino} setDeviceNeighbor in mxp
 - PUT /SET/RemoveNeighbor/{uri},{puerto_local} Elimina un vecino del mxp, especificado por el puerto del dispositivo local
 - PUT /SET/Time to Notify/{uri},{time_to_notify} setTimeToNotify in mxp
 - PUT /SET/Tipo Fec de Cliente/{uri},{TIPO_FEC_CLIENTE} Setea tipo fec cliente
 - PUT /SET/Tipo Fec de linea/{uri},{TIPO_FEC_LINEA} Setea tipo fec linea
- RPC : Diferentes RPC disponibles a ejecutar en MXP40GB**
 - PUT /RPC/Apply Config/{uri} Aplica la configuracion en el MXP40GB
 - PUT /RPC/Apply Settings/{uri} Ejecuta comando -setting- en el MXP40GB
- GET : Obtiene datos de estado y configuracion de los diferentes container**
 - GET /GET/EDFA Container/{uri} Get state edfa container in mxp
 - GET /GET/Tx&Rx Alarms Container/{uri} Get state tx/rx alarm container in mxp

Each API entry includes a small orange or blue button indicating the method (PUT, GET) and a detailed description of the operation.

FIGURA 4.16: Fragmento de la interfaz REST implementada.

4.4.3. Implementación de la interfaz de usuario

A fin de cumplir con los requerimientos R-18 a R-21 de la figura 4.15, se realizó una aplicación WEB basada en el *microframework* Flask [25]. La misma, se desarrolla en Python y hace uso de lenguajes como HTML, JavaScript y CSS para presentar la interfaz de usuario. Cada sección listada en los requerimientos de la figura 4.15 (B), corresponde a un archivo HTML que contiene la estructura de la aplicación y los datos que se presentan en la interfaz.

Es importante mencionar que todas las vistas realizan una tarea común. Dicha tarea consiste en consultar periódicamente al controlador las alarmas activas que tiene ONOS relativas a los *muxponders*. Se puede observar el diagrama de actividad de la tarea mencionada en la figura 4.17.

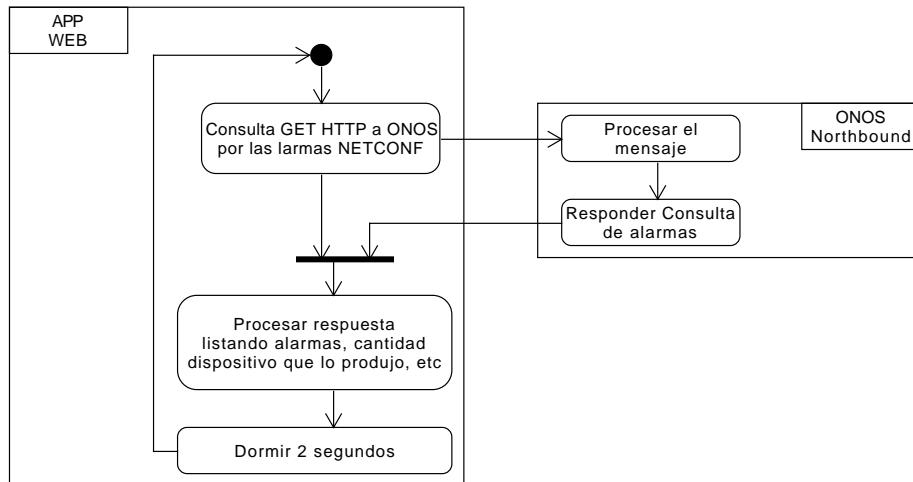


FIGURA 4.17: Consulta periódica por las alarmas al controlador ONOS.

Como ya se explicó en este capítulo, las alarmas son enviadas por los dispositivos a través de las notificaciones NETCONF. Luego, el controlador las registra internamente, por lo que no es necesario hacer uso de la interfaz *Southbound* para consultar a los equipos por el estado de las alarmas. De esta forma, los mismos se ven aliviados al no tener que procesar periódicamente estas consultas.

Teniendo en cuenta esta actividad común, el desarrollo de la *GUI* se divide en las siguientes secciones:

- **Vista principal:** tal como se puede observar en la figura 4.18, esta vista muestra la cantidad de las alarmas presentes en el controlador, sin entrar en detalles. A su vez, en la parte inferior se permite agregar nuevos dispositivos a la topología, indicando la dirección IP y el puerto. Por último, en la zona superior se brinda un campo donde puede seleccionarse un conjunto de equipos para posteriormente aplicar una configuración con un perfil dado.

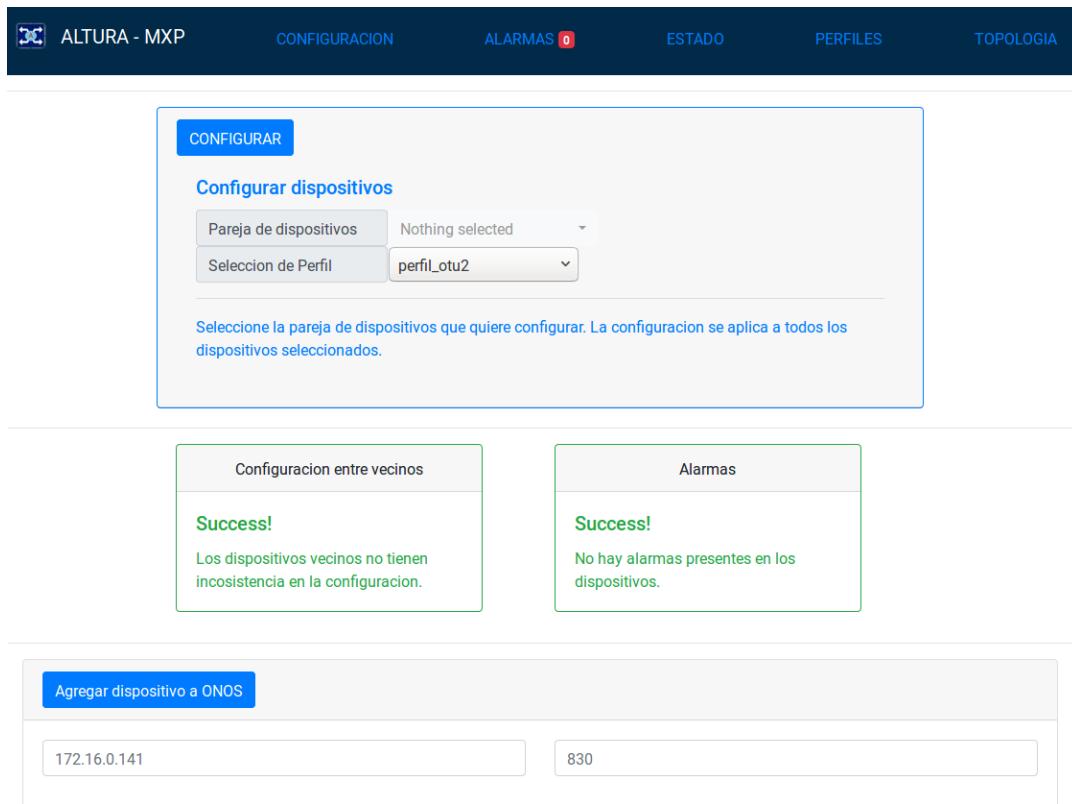


FIGURA 4.18: Interfaz de la vista principal.

Por otra parte, en el diagrama de la figura 4.19 se muestra cómo la aplicación WEB conforma un mensaje JSON con la información del equipo (dirección IP, puerto) y la envía al controlador a través de la interfaz REST. Finalmente, el controlador procesa el mensaje dando inicio al descubrimiento del dispositivo.

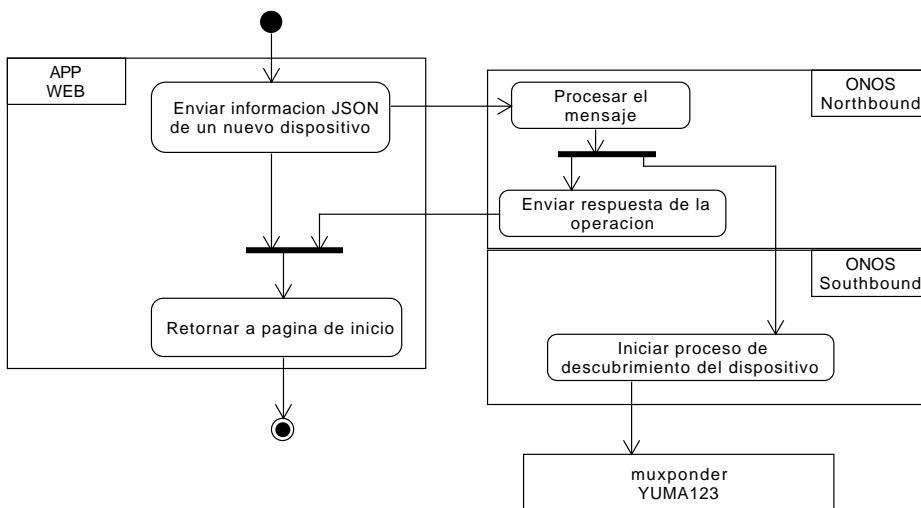


FIGURA 4.19: Agregar dispositivo a través de la APP WEB.

Por último, la figura 4.20 muestra como es el proceso de configuración de un *muxponder* a través de la aplicación WEB. Primeramente, se envía el perfil de

configuración. Una vez que la información es almacenada en el *datastore running*, se envía la RPC 'mux-apply-config' para que se apliquen los cambios en el dispositivo.

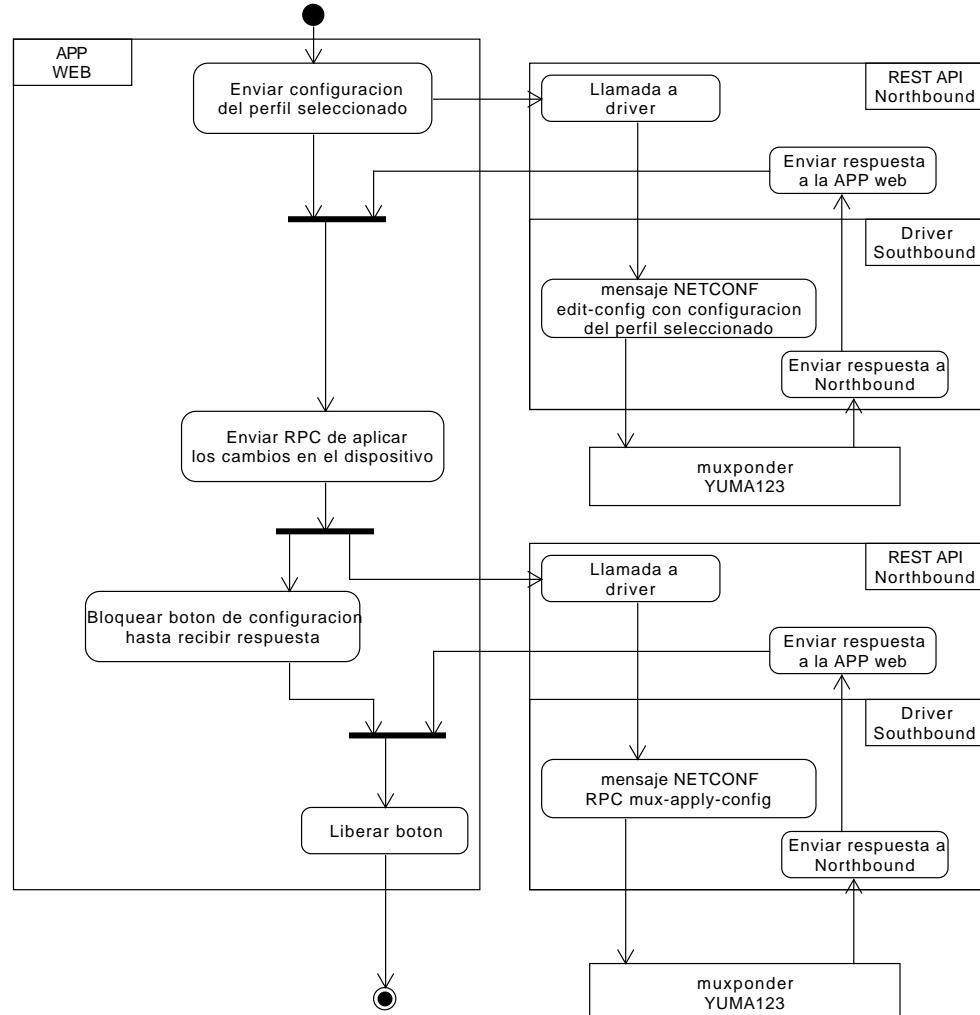


FIGURA 4.20: Configurar un dispositivo a través de la APP WEB.

- **Vista de alarmas:** la figura 4.21 detalla el contenido de dicha sección. Aquí se muestra una información más detallada de las alarmas. El administrador puede identificar el tipo de alarma, el dispositivo que lo originó y la cantidad de alarmas totales que presenta la topología. El diagrama de actividad que refleja el comportamiento que realiza la interfaz WEB en esta sección, se mostró en la figura 4.17.

ALTURA - MXP		CONFIGURACION	ALARMAS 36	ESTADO	PERFILES	TOPOLOGIA
#	ALARM_ID					ALARM_DEVICE
1	netconf:172.16.0.141:830:Tx CDR Loss of Lock XFP3					netconf:172.16.0.141:830
2	netconf:172.16.0.141:830:Low Rx Power Alarm XFP3					netconf:172.16.0.141:830
3	netconf:172.16.0.142:830:Rx CDR Loss of Lock XFP4					netconf:172.16.0.142:830
4	netconf:172.16.0.141:830:Rx CDR Loss of Lock XFP4					netconf:172.16.0.141:830
5	netconf:172.16.0.142:830:Rx POW ALM					netconf:172.16.0.142:830
6	netconf:172.16.0.142:830:Tx CDR Loss of Lock XFP4					netconf:172.16.0.142:830
7	netconf:172.16.0.142:830:Low Rx Power Alarm XFP4					netconf:172.16.0.142:830
8	netconf:172.16.0.141:830:Rx POW ALM					netconf:172.16.0.141:830
9	netconf:172.16.0.141:830:Tx CDR Loss of Lock XFP4					netconf:172.16.0.141:830

FIGURA 4.21: Interfaz de la vista de alarmas.

- **Vista de datos de configuración:** la interfaz que muestra la misma es la que se observa en la figura 4.22. Presenta así una sección donde se puede observar una lista de los equipos que conforman la topología con sus respectivas configuraciones aplicadas.

ALTURA - MXP		CONFIGURACION	ALARMAS 36	ESTADO	PERFILES	TOPOLOGIA
DEVICE	TIPO DE TRAFICO	TIPO DE FEC DE LINEA	TIPO FEC DE CLIENTE	VECINO		
netconf:172.16.0.141:830	XGE	CEROFEC	CEROFEC_CLIENTE	142		
netconf:172.16.0.142:830	XGE	CEROFEC	CEROFEC_CLIENTE	141		

FIGURA 4.22: Interfaz de la vista de configuración.

- **Vista de datos de estado:** a continuación, se muestra la figura 4.23 la interfaz que presenta dicha vista. De forma similar a la anterior, aquí se muestra información relacionada a los datos de estado de los equipos. En la parte superior se puede observar los diferentes *containers* de estado que se implementaron en el módulo YANG.

ALTURA - MXP		CONFIGURACION	ALARMAS 36	ESTADO	PERFILES	TOPOLOGIA
GENERAL MISC POWER DSP EDFA TEMP/HUM XFP						
ID	Temp. Around	Temp. Case	Temp. TX Laser	Temp. RX Laser	Loss	Interrupt
netconf:172.16.0.141:830	31.25	30.00	43.00	43.00	Yes	Yes
netconf:172.16.0.142:830	30.62	30.00	41.00	41.00	Yes	Yes

FIGURA 4.23: Interfaz de la vista de estado.

- **Vista de topología:** tal como se observa en la figura 4.25, aquí se permite realizar cambios en la topología de la red a través de mensajes NETCONF a los

dispositivos. Así, se puede especificar una pareja de equipos para que el controlador, mediante la función *LinkDiscovery*, pueda formar o eliminar los enlaces entre los mismos.

Configurar vecinos MXP-TO-MXP

Dev 1 (TX - PORT 0) netconf:172.16.0.141:830

Dev 2 (RX - PORT 1) netconf:172.16.0.141:830

Dev1 como transmisor (PORT 0) y Dev2 como receptor (PORT 1)

Configurar vecinos MXP-TO-SWITCH

MXP netconf:172.16.0.141:830
PUERTO MXP CLI 1 (PORT 2)
SWITCH

Se empareja el puerto del cliente MXP con el OFSwitch indicado.

Eliminar vecino

Dispositivo local netconf:172.16.0.141:830
Eliminar vecino conectado al puerto:
Puerto TX (PORT 0)

Se elimina un vecino en el dispositivo, especificando el puerto que se elimina.

FIGURA 4.24: Interfaz de la vista de topología.

- **Vista de perfiles:** por último, en la figura 4.25 se presenta una sección donde se permite agregar o eliminar perfiles de configuración. La idea básica de los perfiles de configuración es la de agrupar una serie de parámetros de tal forma que el administrador pueda identificar fácilmente cuál será la configuración que se aplique en el dispositivo. Además, permite guardar dicho perfil con el fin de poder reutilizarlo en un futuro.

The screenshot shows a web-based administrative interface for managing configuration profiles. At the top, there is a navigation bar with tabs: ALTURA - MXP, CONFIGURACION, ALARMAS 36, ESTADO, PERFILES, and TOPOLOGIA. Below the navigation bar, the main title is "Administrador de perfiles de configuracion." A sub-instruction states: "Esta sección permite agregar un nuevo perfil, eliminarlo o ver la configuración que aplica el mismo." The interface is divided into three main sections:

- Agregar nuevo perfil:** This section contains four input fields: "Nombre del perfil" (AaBbCcDd), "Tipo de tráfico" (xge), "Tipo fec de linea" (cerofec), and "Tipo fec de cliente" (cerofec_cliente). A blue button labeled "Agregar nuevo perfil" is located above these fields.
- Eliminar perfil:** This section features a red-bordered box containing a blue button labeled "Eliminar perfil" and a dropdown menu showing "perfil_otu2". A red message at the bottom of the box reads: "Seleccione el perfil que desea eliminar."
- Mostrar configuracion del perfil:** This section contains a dropdown menu showing "perfil_otu2" and a blue button labeled "Mostrar configuracion del perfil". A blue message at the bottom of the box reads: "Seleccione el perfil que desea mostrar la configuración."

FIGURA 4.25: Interfaz de la vista de administración perfiles de configuración.

Capítulo 5

Validación y Verificación

En el capítulo anterior se explicó y caracterizó el diseño de las diferentes aplicaciones que conforman el sistema. A fines de validar su funcionamiento, será necesario poner a prueba los requerimientos de cada una de las aplicaciones desarrolladas.

De esta forma, este capítulo propone una serie de casos de prueba determinantes para verificar el funcionamiento del proyecto.

En primer lugar, se pondrá a prueba el agente Yuma123 instalado en el dispositivo. Luego, se verifica el funcionamiento del *driver* desarrollado en el controlador ONOS. Por último, se pone a prueba tanto la interfaz REST como la interfaz gráfica desarrollada.

5.1. Verificación del agente NETCONF

En esta sección se pondrá a prueba el agente que se instaló en el dispositivo. Para ello, las evaluaciones realizadas tendrán como objetivo asegurar el cumplimiento de los requerimientos vistos en la figura 4.6.

5.1.1. Escenario

La figura 5.1 muestra la topología utilizada para las pruebas. Se tendrá una computadora de propósito general conectada a la interfaz de control del *muxponder*. Por otra parte, el *muxponder* ejecutará el agente 'netconfd' de Yuma123 mientras que el *host* ejecutará el cliente 'yangcli', también de Yuma123.



FIGURA 5.1: Topología utilizada para las pruebas relativas a la integración del protocolo NETCONF.

Además, para poder poner a prueba la integración del protocolo con el dispositivo se realizan las siguientes suposiciones y condiciones previas:

- El *host* y el *muxponder* deben tener conectividad entre sí.
- Se debe tener instalado en el *host*, el cliente 'yangcli'.
- Tener instalado en el *muxponder*, el agente 'netconfd'.
- Tanto el módulo YANG como la librería desarrollada para el *muxponder*, deben estar instalados en el mismo.
- La aplicación 'monitor' debe estar iniciada en el *muxponder*.
- El equipo no debe tener ninguna configuración previa aplicada.

5.1.2. Matriz de trazabilidad

Se conformarán tres casos de pruebas. El primero tiene como objetivo verificar el inicio de sesión entre el cliente y el servidor NETCONF. Por otra parte, la segunda prueba consiste en obtener el valor de cualquier variable visible en 'monitor'. Por último, se pone a prueba realizar un cambio en la configuración del equipo.

De esta forma, la matriz de trazabilidad resultante es la que se observa en el cuadro 5.1.

	T-R-01	T-R-02	T-R-03
R-07	X	X	X
R-08		X	
R-09			X
R-10			X

CUADRO 5.1: Matriz de trazabilidad - Verificación del protocolo NETCONF

5.1.3. Casos de prueba y resultados

A continuación, se describirán los procedimientos llevados a cabo para probar esta pieza de software. Algunos de los casos de pruebas pueden estar acompañados por imágenes para esclarecer su funcionamiento.

Caso de Prueba T-R-01

Se pondrá a prueba el inicio de la sesión NETCONF entre el cliente y el servidor. El cuadro 5.2 presenta la descripción, los procedimientos y los resultados del mismo.

ID T-R-01	
Título	Inicio de sesión en NETCONF.
Objetivo	Poder conectarse desde el cliente NETCONF al servidor instalado en el <i>muxponder</i> .
Procedimiento	<ul style="list-style-type: none"> ■ En el <i>muxponder</i>, iniciar el agente NETCONF. ■ En el host, haciendo uso de la <i>CLI</i> del cliente 'yangcli', indicar usuario <i>SSH</i>, <i>password</i>, dirección IP y puerto para iniciar sesión en el servidor NETCONF del dispositivo.
Resultados esperados	Se debe observar el proceso de intercambio de capacidades entre el cliente y el servidor. Una vez finalizado dicho intercambio, deben quedar habilitadas las operaciones <i>RPC</i> que describe tanto el protocolo como el módulo <i>YANG</i> instalado en el dispositivo.
Estado	APROBADO

CUADRO 5.2: Caso de Prueba T-R-01

Caso de Prueba T-R-02

En este caso, se pone a prueba las consultas por los datos de estado y de configuración del módulo *YANG*. Los procedimientos para esta prueba y sus resultados se presentan en el cuadro 5.3.

ID T-R-02	
Título	Monitoreo de datos en NETCONF.
Objetivo	Obtener información sobre las variables de estado y de configuración del dispositivo.
Procedimiento	<ul style="list-style-type: none"> ■ Iniciar sesión entre un cliente y servidor NETCONF, tal como se describió en T-R-01. ■ Desde el cliente, realizar consultas con las <i>RPC</i> <i>get</i> y <i>get-config</i> al contenedor <i>mux-state-XFP1</i> y <i>mux-config</i> respectivamente.
Resultados esperados	El servidor deberá responder, para el primer caso, valores idénticos a los que presente el binario 'monitor' respecto al módulo XFP1. Para el segundo caso, el servidor deberá retornar los valores de los datos de configuración que tenga el <i>datastore running</i> .
Estado	APROBADO

CUADRO 5.3: Caso de Prueba T-R-02

Por otra parte, la figura 5.2 ejemplifica el resultado de una operación de consulta al *container mux-state-XFP1*, el cual contiene información de estado de dicho módulo XFP.

```
yangcli root@172.16.0.142> sget /mux-state-XFP1/  
  
Filling container /mux-state-XFP1:  
RPC Data Reply 4 for session 1:  
  
rpc-reply {  
    data {  
        mux-state-XFP1 {  
            Presence Yes  
            Loss No  
            Ready No  
            Interrupt Yes  
            Tx_Power_dBm -inf  
            Rx_Power_dBm -13.32  
            Temp_c 20.00  
            Low_Tx_Power_Alarm --  
            High_Tx_Power_Alarm --  
            Low_Rx_Power_Alarm --  
            High_Rx_Power_Alarm --  
            Rx_CDR_Loss_of_Lock --  
            Tx_CDR_Loss_of_Lock --  
            Laser_Fault --  
        }  
    }  
}
```

FIGURA 5.2: Consulta al *container mux-state-XFP1*.

Caso de Prueba T-R-03

Del mismo modo, el cuadro 5.4 detalla los procedimientos que se siguieron para verificar el funcionamiento de la *RPC 'mux-apply-config'* y las notificaciones. Cabe destacar que como se aclaró en las suposiciones para las pruebas, el equipo no se encuentra configurado. Por lo tanto se tendrán alarmas referidas a la transmisión y la recepción, entre otras.

ID T-R-03	
Título	Prueba de cambio de configuración y notificaciones en NETCONF.
Objetivo	Poder realizar un cambio en la configuración del dispositivo a través de la RPC 'mux-apply-config' y verificar el funcionamiento de las notificaciones implementadas en el módulo YANG.
Procedimiento	<ul style="list-style-type: none"> ■ Iniciar sesión entre un cliente y servidor NETCONF, tal como se describió en T-R-01. ■ Desde el cliente NETCONF, enviar un mensaje al servidor con la RPC 'create-subscription'. ■ Desde el cliente NETCONF, enviar un mensaje al servidor con la RPC 'mux-apply-config', para que el mismo aplique la configuración que se encuentra en el <i>datastore running</i>.
Resultados esperados	En primer lugar, se espera que el cliente se suscriba correctamente a las notificaciones, recibiendo un mensaje OK de parte del servidor. Además, luego de que se envíe la RPC 'mux-apply-config' y se termine de aplicar la configuración en el equipo, en el cliente 'yangcli' se debe observar el ingreso de las notificaciones debido a que las alarmas del equipo cambiaron de estado, producto de la configuración aplicada.
Estado	APROBADO

CUADRO 5.4: Caso de Prueba T-R-03

La figura 5.3 muestra en primer lugar cómo el cliente se suscribe a las notificaciones mediante la RPC 'create-suscription'. Luego, se puede observar el envío de la RPC 'mux-apply-config'. Seguidamente se muestran las notificaciones entrantes, producto del cambio de estado de las alarmas presentes en el equipo.

```

yangcli root@172.16.0.142> create-subscription
RPC OK Reply 3 for session 1:

yangcli root@172.16.0.142> mux-apply-config
RPC Data Reply 4 for session 3:

rpc-reply {
    respuesta-mux-apply-config OK
}

yangcli root@172.16.0.142>

Incoming notification:
notification {
    eventTime 1915-12-04T10:28:21Z
    mux-notify {
        INFO '[ALARM] EOL ALM'
    }
}

```

FIGURA 5.3: Suscripción y *RPC 'mux-apply-config'*.

5.2. Verificación del *driver*

A continuación, en este ensayo se comprueba el funcionamiento del *driver* desarrollado para el controlador ONOS. Los requerimientos que se deben asegurar su cumplimiento son los que se observan en la figura 4.9.

5.2.1. Escenario

En este caso, la topología utilizada para las pruebas es la que se muestra en la figura 5.4. Se tendrán dos *muxponders* conectados entre sí a través de las interfaces de línea de los mismos. Por otra parte, el controlador ONOS estará conectado a la interfaz de control de ambos dispositivos.

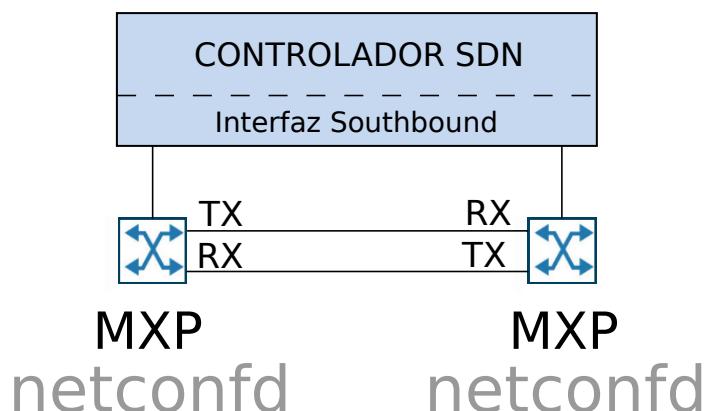


FIGURA 5.4: Topología utilizada para las pruebas relativas al *driver*.

Además, se realizan las siguientes suposiciones:

- Los agentes 'netconfd' se encuentran iniciados en ambos dispositivos.
- Tanto el módulo YANG como la librería en C desarrollada para los *muxponders*, están instaladas en los mismos.
- La aplicación 'monitor' está iniciada en ambos *muxponders*.
- Los dispositivos no tienen una configuración previa instalada.
- Los equipos no tienen información relacionada a la presencia de vecinos.

5.2.2. Matriz de trazabilidad

A fines de poner a prueba el cumplimiento de los requerimientos para esta pieza de software, se desarrollan dos casos de prueba.

En el primero, se verifica que el controlador sea capaz de descubrir correctamente la información de los dispositivos agregados a la topología, a través de la función *DeviceDescriptionDiscovery*. La segunda prueba abarca la verificación tanto de la función *LinkDiscovery* como la RPC 'mux-apply-config'. Además, para ambas pruebas se utilizan los comandos CLI implementados en el *driver*.

De esta forma resulta la matriz de trazabilidad que se observa en el cuadro 5.5.

	T-R-04	T-R-05
R-11	X	
R-12		X
R-13		X
R-14	X	X

CUADRO 5.5: Matriz de trazabilidad - Verificación del *driver*

5.2.3. Casos de prueba y resultados

Caso de Prueba T-R-04

Se pondrá a prueba la función llamada *DeviceDescriptionDiscovery*, la cual como se explicó en el capítulo anterior 4.3.2, es la encargada de registrar en el controlador información adicional de los equipos. Tanto la descripción como los procedimientos llevados a cabo y los resultados de los mismos se presentan en el cuadro 5.6.

ID T-R-04	
Título	Prueba de añadir <i>muxponders</i> a la topología de ONOS.
Objetivo	Comprobar que los dispositivos se agregan correctamente al controlador, mostrando información sobre fabricante, versión del hardware y del software, identificador único, etc.
Procedimiento	<ul style="list-style-type: none"> ■ Haciendo uso del comando 'onos-netcfg', enviar al controlador un mensaje JSON con información de los dispositivos a añadir a la topología de ONOS. ■ Ejecutar el comando 'devices' en la <i>CLI</i> del controlador. El mismo devuelve una lista con información de todos los dispositivos agregados.
Resultados esperados	Una vez que el proceso de descubrimiento de los dispositivos haya finalizado, el comando 'devices' deberá arrojar información sobre los equipos, mostrando correctamente los datos nombrados anteriormente (información del fabricante, versión de hardware y de software e identificador único).
Estado	APROBADO

CUADRO 5.6: Caso de Prueba T-R-04

Por otra parte, la figura 5.5 muestra los dispositivos agregados a la topología de ONOS. Al hacer click sobre cualquiera de ellos, el controlador despliega un cuadro del dispositivo seleccionado mostrando la información mencionada anteriormente.

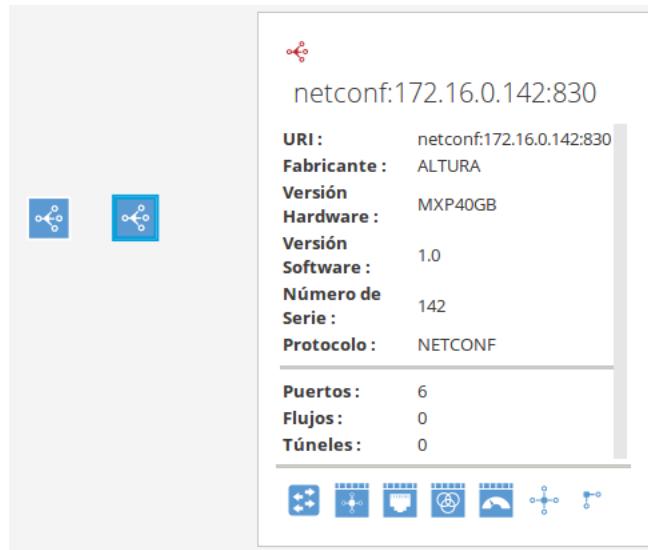


FIGURA 5.5: Información de dispositivos presentes en la topología de ONOS.

Caso de Prueba T-R-05

Este caso pone a verifca tanto la función *LinkDiscovery*, la cual es la encargada de formar los enlaces entre los distintos dispositivos 4.3.3, como la *RPC* 'mux-apply-config', encargada de aplicar los cambios en el dispositivo 4.3.4. En el cuadro 5.7 se

detalla la descripción del caso de prueba mencionado. Se asumirá que los dispositivos ya se encuentran añadidos al controlador.

ID T-R-05	
Título	Prueba de formar enlaces entre <i>muxponders</i> vecinos.
Objetivo	Comprobar que el controlador muestra correctamente la información referida a los enlaces entre los dispositivos.
Procedimiento	<ul style="list-style-type: none"> ■ Desde el controlador, agregar información del vecino a cada uno de los dispositivos presentes en la topología. ■ Haciendo uso de la RPC 'mux-apply-config', aplicar una misma configuración a todos los equipos. ■ Desconectar el transmisor de alguno de los <i>muxponders</i>.
Resultados esperados	<p>Al agregar a cada dispositivo la información referente a su vecino, se deberá observar en la interfaz gráfica de ONOS que los enlaces no se forman. Esto es así ya que como los dispositivos no están configurados, existirán alarmas referidas a la transmisión y recepción, y como se explicó en el capítulo anterior el <i>driver</i> no formará los enlaces si dichas alarmas están presentes.</p> <p>Luego, al enviar la RPC 'mux-apply-config' a ambos dispositivos y una vez que se termine de aplicar la configuración, las alarmas mencionadas anteriormente deberían desaparecer. Por lo tanto, en la interfaz gráfica del controlador se debe observar los enlaces formados entre los equipos, ya que no existen alarmas relacionadas a la transmisión y recepción. Por último, el hecho de desconectar la línea del transmisor en alguno de los dos <i>muxponders</i> genera alarmas en los dispositivos, por lo que la interfaz gráfica debe mostrar un cambio en la topología debido a que el enlace no se encuentra presente.</p>
Estado	APROBADO

CUADRO 5.7: Caso de Prueba T-R-05

La figura 5.6 muestra la topología presente en el controlador una vez se le indicó a cada dispositivo la presencia de un vecino. Como se puede notar, el controlador no forma los enlaces entre los mismos ya que los dispositivos contienen alarmas debido a que no están configurados.

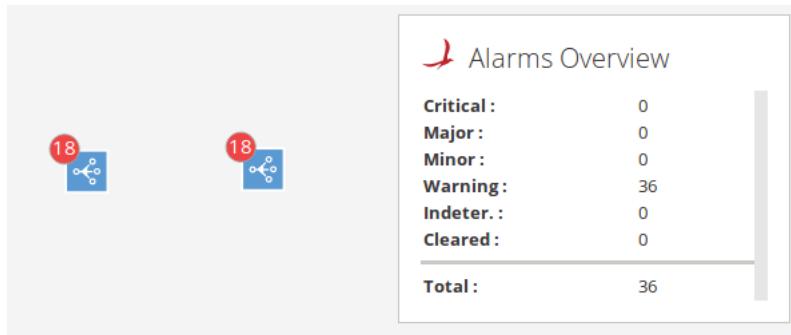


FIGURA 5.6: Vista de la topología de ONOS - Dispositivos sin configurar.

A su vez, en la figura 5.7 se observa que una vez aplicada la configuración en ambos dispositivos, la cantidad de alarmas presentes se reducen. Luego, al no existir alarmas referidas a la transmisión y recepción de los equipos, el controlador puede formar correctamente el enlace entre los mismos.

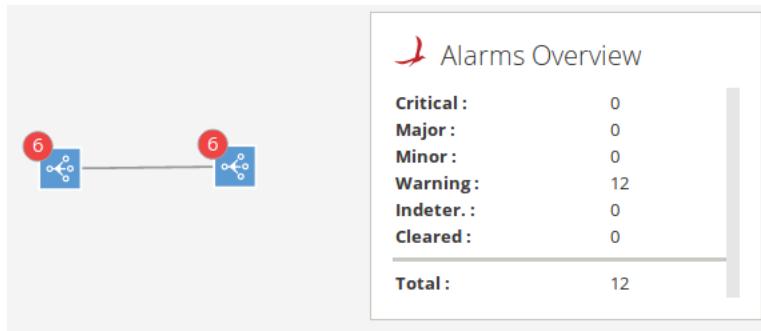


FIGURA 5.7: Vista de la topología de ONOS - Dispositivos configurados.

Por último, la figura 5.8 ejemplifica lo que sucede cuando se desconecta el transmisor en alguno de los dispositivos, provocando así la caída de un enlace en la topología de ONOS.

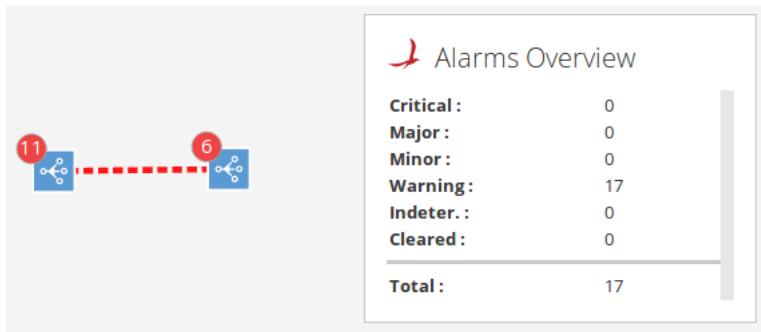


FIGURA 5.8: Vista de la topología de ONOS - Dispositivos configurados, con un enlace desconectado.

5.3. Verificación de la interfaz gráfica y la interfaz REST

Finalmente, en esta sección se pondrán a prueba ambas interfaces desarrolladas. Para ello, las pruebas realizadas tendrán como objetivo validar el cumplimiento de los requerimientos vistos en la figura 4.15.

Además, los casos de prueba presentados a continuación harán uso tanto del *driver* como de la aplicación C desarrollada para el agente NETCONF.

5.3.1. Escenario

La topología utilizada para las pruebas mencionadas anteriormente se muestra en la figura 5.9. Se tendrán dos *muxponders* conectados entre sí a través de las interfaces de línea de los mismos. Además, el controlador ONOS estará conectado a la interfaz de control de ambos dispositivos. Por último, se tienen dos computadoras de propósito general conectadas a los módulos XFP1 de los *muxponders*.

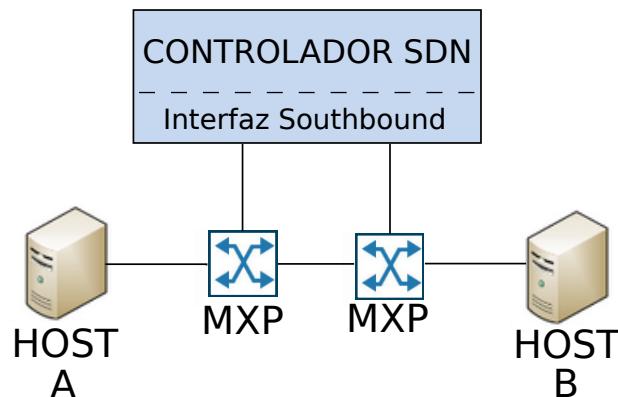


FIGURA 5.9: Topología utilizada para las pruebas relativas a la interfaz gráfica e interfaz REST.

Además, se realizan las siguientes suposiciones:

- Los agentes 'netconfd' se encuentran iniciados en ambos dispositivos.
- Tanto el módulo YANG como la librería en C desarrollada para los *muxponders*, están instaladas en los mismos.
- La aplicación 'monitor' está iniciada en ambos *muxponders*.
- Los dispositivos no tienen una configuración previa instalada.
- Los equipos no tienen información relacionada a la presencia de vecinos.

5.3.2. Matriz de trazabilidad

Se presenta a continuación en el cuadro 5.8 la matriz de trazabilidad para las pruebas realizadas.

En la primera prueba, se verifica poder agregar dispositivos a través de la interfaz gráfica y configurar a ambos como vecinos. Luego, se verifica en la prueba T-R-07 que puedan visualizarse las alarmas en la aplicación WEB. Por otra parte, en la prueba T-R-08 se comprueba que sea posible visualizar, a través de la interfaz gráfica, cualquier dato de estado de los dispositivos. Por último, se ensaya realizar un

cambio en la configuración en los dispositivos de tal forma que se permita la conectividad entre los *host A* y *B*.

	T-R-06	T-R-07	T-R-08	T-R-09
R-15		X	X	X
R-16	X			X
R-17				X
R-18		X		
R-19	X			X
R-20				X
R-21			X	

CUADRO 5.8: Matriz de trazabilidad - Verificación de la interfaz REST e interfaz gráfica

5.3.3. Casos de prueba y resultados

Caso de Prueba T-R-06

A continuación, se asegura agregar nuevos dispositivos a la topología del controlador desde la interfaz gráfica y configurarlos como vecinos. Los procedimientos llevados a cabo para dicha prueba se observan en el cuadro 5.9.

ID T-R-06	
Título	Añadir <i>muxponders</i> a la topología de ONOS desde la interfaz gráfica y configurarlos como vecinos.
Objetivo	Comprobar que los dispositivos se agregan correctamente al controlador haciendo uso de la interfaz gráfica y que es posible agregar información de vecinos a cada uno de ellos desde la misma.
Procedimiento	<ul style="list-style-type: none"> ■ Desde la aplicación WEB, agregar un nuevo dispositivo indicando dirección IP y puerto. ■ Desde la aplicación WEB, hacer click en 'TOPOLOGIA' y configurar ambos equipos como vecinos. ■ En el controlador, ejecutar el comando 'devices'. ■ Desde la aplicación WEB, hacer click en 'CONFIGURACION'.
Resultados esperados	Luego de ejecutar el comando 'devices' en la CLI del controlador, se debe mostrar la información de fabricante, versión del hardware y software e identificador único de ambos dispositivos agregados. Por otra parte, la sección 'CONFIGURACION' debe mostrar la información mencionada anteriormente junto con el identificador único del vecino agregado.
Estado	APROBADO

CUADRO 5.9: Caso de Prueba T-R-06

Caso de Prueba T-R-07

El objetivo del caso de prueba presentado en el cuadro 5.10, es el de verificar que la interfaz gráfica presente de forma correcta la información relacionada a las alarmas en los dispositivos. Se hará uso tanto de la aplicación 'monitor' como de los comandos 'alarms' y 'alarms-count' de ONOS para validar las alarmas presentes.

ID T-R-07	
Título	Prueba de visualización de alarmas desde la interfaz gráfica.
Objetivo	Comprobar que la aplicación WEB muestra correctamente las alarmas de todos los <i>muxponders</i> presentes en la topología.
Procedimiento	<ul style="list-style-type: none"> ■ En la aplicación WEB, hacer click sobre 'ALARMAS'. ■ En el controlador, ejecutar los comandos 'alarms' y 'alarms-counts'. ■ En la CLI de cada uno de los <i>muxponders</i>, verificar con la aplicación 'monitor' la presencia de alarmas.
Resultados esperados	La cantidad de alarmas presentes anunciadas en la interfaz gráfica debe ser la misma que las anunciadas por el controlador al ejecutar el comando 'alarms-counts'. Además, la información referida a cada alarma, como por ejemplo el dispositivo de origen y el nombre de la misma, debe ser igual a las que muestre el comando 'alarms' en el controlador ONOS. Finalmente, las alarmas presentes en cada dispositivo deben poder visualizarse en la aplicación 'monitor' de los <i>muxponders</i> relacionados.
Estado	APROBADO

CUADRO 5.10: Caso de Prueba T-R-07

Tal como se puede ver en la figura 5.10, se tienen 12 alarmas presentes referidas a los módulos XFP2, XFP3 y XFP4 de ambos dispositivos.

ICONO	ALTURA - MXP	CONFIGURACION	ALARMAS 12	ESTADO	PERFILES	TOPOLOGIA
#	ALARM_ID				ALARM_DEVICE	
1	netconf:172.16.0.141:830:Rx CDR Loss of Lock XFP4				netconf:172.16.0.141:830	
2	netconf:172.16.0.141:830:Rx CDR Loss of Lock XFP2				netconf:172.16.0.141:830	
3	netconf:172.16.0.141:830:Low Rx Power Alarm XFP3				netconf:172.16.0.141:830	
4	netconf:172.16.0.142:830:Rx CDR Loss of Lock XFP4				netconf:172.16.0.142:830	
5	netconf:172.16.0.142:830:Rx CDR Loss of Lock XFP3				netconf:172.16.0.142:830	
6	netconf:172.16.0.142:830:Low Rx Power Alarm XFP4				netconf:172.16.0.142:830	
7	netconf:172.16.0.141:830:Rx CDR Loss of Lock XFP3				netconf:172.16.0.141:830	
8	netconf:172.16.0.142:830:Low Rx Power Alarm XFP2				netconf:172.16.0.142:830	
9	netconf:172.16.0.141:830:Low Rx Power Alarm XFP4				netconf:172.16.0.141:830	
10	netconf:172.16.0.142:830:Low Rx Power Alarm XFP3				netconf:172.16.0.142:830	
11	netconf:172.16.0.142:830:Rx CDR Loss of Lock XFP2				netconf:172.16.0.142:830	
12	netconf:172.16.0.141:830:Low Rx Power Alarm XFP2				netconf:172.16.0.141:830	

FIGURA 5.10: Alarmas visualizadas en la interfaz gráfica.

Se puede observar lo mismo al ejecutar los comandos '*alarms*' y '*alarms-counts*', los cuales listan las alarmas presentes en el controlador. De esta forma, se puede ver en la figura 5.11 la salida del comando '*alarms-counts*', la cual anuncia la misma cantidad de alarmas presentes en el controlador.

```
Welcome to Open Network Operating System (ONOS)!

[ONOS]

Documentation: wiki.onosproject.org
Tutorials: tutorials.onosproject.org
Mailing lists: lists.onosproject.org

Come help out! Find out how at: contribute.onosproject.org

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown ONOS.

onos> alarms-counts
WARNING, 12
onos> █
```

FIGURA 5.11: Alarmas visualizadas en la *CLI* del controlador.

Por último, se muestra en la figura 5.12 la salida del binario '*monitor*' de uno de los *muxponder*. En ella, es posible observar 6 etiquetas '*Alarm*' en la sección de módulos XFP. Teniendo en cuenta que se tiene el mismo resultado en el otro dispositivo, se tienen las 12 alarmas en total.

	XFP 1	XFP 2	XFP 3	XFP 4
Presence	Yes	Yes	Yes	Yes
Loss	No	Yes	Yes	Yes
Ready	No	No	No	No
Interrupt	Yes	Yes	Yes	Yes
Tx Power [dBm]	-inf	-2.29	-2.28	-2.28
Rx Power [dBm]	-13.30	-40.00	-40.00	-40.00
Temp. [C]	24.75	28.23	27.84	27.79
Low Tx Power Alarm	--	--	--	--
High Tx Power Alarm	--	--	--	--
Low Rx Power Alarm	--	Alarm	Alarm	Alarm
High Rx Power Alarm	--	--	--	--
RX CDR Loss of Lock	--	Alarm	Alarm	Alarm
TX CDR Loss of Lock	--	--	--	--
Laser Fault	--	--	--	--

FIGURA 5.12: Alarmas visualizadas en '*monitor*' en uno de los *muxponders*.

Caso de Prueba T-R-08

Se presenta la verificación que se observa en el cuadro 5.11, la cual tiene como objetivo examinar que sea posible observar cualquier dato de estado del dispositivo a través de la interfaz gráfica.

Al igual que en la prueba anterior, se hará uso del binario '*monitor*' para comprobar su funcionamiento.

ID T-R-08	
Título	Prueba de visualización de los datos de estado desde la interfaz gráfica.
Objetivo	Verificar que desde la aplicación WEB se pueda obtener información de los datos de estado de cada <i>mxpander</i> presente en la topología.
Procedimiento	<ul style="list-style-type: none"> ■ En la aplicación WEB, hacer click sobre 'ESTADO'. ■ En el controlador, consultar por los datos de estado de cada dispositivo presente haciendo uso del comando 'get'. ■ Verificar con 'monitor' los valores para los datos de estado.
Resultados esperados	La información que presenta la sección 'ESTADO' de la interfaz gráfica debe tener valores idénticos a los obtenidos por el controlador luego de ejecutar el comando 'get'. Además, la información que muestra 'monitor' debe coincidir con la que se observa en la sección de 'ESTADO' en la aplicación WEB.
Estado	APROBADO

CUADRO 5.11: Caso de Prueba T-R-08

A continuación, en la figura 5.13 se muestran los valores obtenidos por la interfaz gráfica referidos al container '*misc*' de ambos dispositivos.

ID	Temp. Around	Temp. Case	Temp. TX Laser	Temp. RX Laser	Loss
netconf:172.16.0.141:830	34.88	34.00	43.00	43.00	No
netconf:172.16.0.142:830	34.25	33.00	41.00	42.00	No

FIGURA 5.13: Datos de estado, observados desde la interfaz gráfica.

Por otra parte, se observa en la figura 5.14 la sección referida a '*misc*' en 'monitor', los cuales tienen los mismos valores que los obtenidos por la interfaz gráfica. Es importante aclarar que debido a la cantidad de los datos presentes en este container, las figuras nombradas anteriormente solo muestran una porción de los datos.

Por lo tanto, se observan únicamente los primeros cinco valores.

Misc.	Value
Temp. Around	34.88
Temp. Case	34.00
Temp. Tx Laser	43.00
Temp. Rx Laser	43.00
Loss	No

(A) 'monitor' del *muxponder* '141'.

Misc.	Value
Temp. Around	34.25
Temp. Case	33.00
Temp. Tx Laser	41.00
Temp. Rx Laser	42.00
Loss	No

(B) 'monitor' del *muxponder* '142'.

FIGURA 5.14: Datos de estado, observados desde 'monitor'.

Caso de Prueba T-R-09

Por último, el caso de prueba mostrado en el cuadro 5.12 tiene como objetivo verificar que es posible configurar los *muxponders* de tal manera que los *host* A y B tengan conectividad entre sí.

ID T-R-09	
Título	Prueba de conectividad entre los <i>hosts</i> A y B.
Objetivo	Poder configurar a través de la interfaz gráfica ambos <i>muxponders</i> , con el objetivo de que los <i>hosts</i> tengan conectividad entre ellos.
Procedimiento	<ul style="list-style-type: none"> ■ Desde la sección 'TOPOLOGÍA' en la aplicación WEB, configurar ambos dispositivos como vecinos. ■ Hacer click en la sección 'PERFILES' y añadir dos perfiles, uno con tipo de tráfico 'xge' y otro con un tipo de tráfico 'otu2'. ■ Hacer click en 'ALTURA-MXP'. En el cuadro de configuración, aplicar a uno de los dispositivos el perfil de configuración 'xge' mientras que al otro aplicar el perfil de configuración 'otu2'. ■ En cada uno de los <i>hosts</i>, verificar si tienen conectividad entre ellos utilizando la aplicación 'ping'. ■ Hacer click en 'CONFIGURACION'. Verificar la configuración aplicada en los dispositivos. ■ Hacer click en 'ALTURA-MXP'. En el cuadro de configuración, seleccionar el <i>muxponder</i> configurado anteriormente con el perfil 'otu2' y aplicarle ahora la configuración 'xge'. ■ En cada uno de los <i>hosts</i>, verificar si tienen conectividad entre ellos utilizando la aplicación 'ping'.
Resultados esperados	<p>Luego de configurar a los dispositivos como vecinos y aplicar un perfil de configuración diferente a cada uno de ellos, la interfaz deberá mostrar en la sección principal una advertencia de que existen dispositivos presentes en la topología con una configuración diferente.</p> <p>Si los <i>muxponders</i> tienen aplicada una configuración diferente entre ellos, no existirá conectividad entre los host, por lo que los dispositivos no podrán realizar un 'ping' entre ellos.</p> <p>Luego, al configurar ambos dispositivos con el mismo perfil de configuración, la interfaz gráfica debe mostrar en la sección principal que la alarma referida a configuración inconsistente desapareció. Además, la prueba de 'ping' debe mostrar ahora que los <i>host</i> pueden alcanzarse.</p>
Estado	APROBADO

CUADRO 5.12: Caso de Prueba T-R-09

La figura 5.15 muestra la sección principal de la interfaz gráfica. En ella, es posible observar un recuadro en amarillo indicando que se detectó una configuración inconsistente entre los dispositivos (o sea, que los dispositivos vecinos no tienen la

misma configuración).

The screenshot shows a network management interface with the following sections:

- Header:** ALTURA - MXP, CONFIGURACION, ALARMAS 13, ESTADO, PERFILES, TOPOLOGIA.
- Configuración (Configuration) Tab:**
 - CONFIGURAR (Configure) Button:**
 - Configurar dispositivos (Configure devices) Section:**
 - Pareja de dispositivos: Nothing selected
 - Selección de Perfil: perfil_otu2

Seleccione la pareja de dispositivos que quiere configurar. La configuración se aplica a todos los dispositivos seleccionados.
- Estado de la configuración (Configuration status) Box:**

Warning!
Algunos dispositivos vecinos tienen configuración inconsistente.
- Alarmas (Alarms) Box:**

Oops!
Algunos dispositivos podrían contener alarmas. Alarmas en total: 13.
- Agregar dispositivo a ONOS (Add device to ONOS) Box:**

172.16.0.141 830

FIGURA 5.15: Detección de configuración inconsistente entre dispositivos vecinos.

En este estado, si los *host* A y B tratan de realizar un ping entre ellos el resultado es el que se puede ver en la figura 5.16. Como se esperaba, los *hosts* no tienen conectividad entre ellos debido a la configuración inconsistente aplicada a los dispositivos.

```
usuario@ruka:~$ ping 11.0.0.2 -c 3
PING 11.0.0.2 (11.0.0.2) 56(84) bytes of data.
--- 11.0.0.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2049ms
```

FIGURA 5.16: Prueba fallida de conectividad entre *host* A y *host* B.

Luego, al configurar ambos dispositivos con el perfil de configuración xge, la interfaz muestra que la alarma debido a configuración inconsistente desapareció, tal como se muestra en la figura 5.17.

The screenshot shows the 'CONFIGURACION' (Configuration) tab of the ALTURA - MXP interface. At the top, there are tabs for 'ALTURA - MXP', 'CONFIGURACION', 'ALARMAS 12', 'ESTADO', 'PERFILES', and 'TOPOLOGIA'. Below the tabs, a blue button labeled 'CONFIGURAR' (Configure) is visible. A section titled 'Configurar dispositivos' (Configure devices) contains two dropdown menus: 'Pareja de dispositivos' (Device pair) set to 'Nothing selected' and 'Seleccion de Perfil' (Profile selection) set to 'perfil_otu2'. A note below says: 'Seleccione la pareja de dispositivos que quiere configurar. La configuracion se aplica a todos los dispositivos seleccionados.' (Select the device pair you want to configure. Configuration applies to all selected devices). Below this, two boxes are shown: 'Configuracion entre vecinos' (Configuration between neighbors) with a green border and 'Success!' message: 'Los dispositivos vecinos no tienen inconsistencia en la configuracion.' (The neighbor devices do not have inconsistency in the configuration); and 'Alarms' with a red border and 'Oops!' message: 'Algunos dispositivos podrian contener alarmas. Alarmas en total: 12.' (Some devices may contain alarms. Total alarms: 12). At the bottom, a 'Agregar dispositivo a ONOS' (Add device to ONOS) button is present, with input fields containing '172.16.0.141' and '830'.

FIGURA 5.17: Detección de configuración consistente entre dispositivos vecinos.

Por último, se realiza nuevamente la prueba de conectividad realizando un ping entre los *hosts*. Como se puede ver en la figura 5.18, los clientes ahora tienen conectividad entre ellos debido a la configuración consistente entre los dispositivos vecinos.

```
usuario@ruka: ~
usuario@ruka:~$ ping 11.0.0.2 -c 3
PING 11.0.0.2 (11.0.0.2) 56(84) bytes of data.
64 bytes from 11.0.0.2: icmp_seq=1 ttl=64 time=0.356 ms
64 bytes from 11.0.0.2: icmp_seq=2 ttl=64 time=0.362 ms
64 bytes from 11.0.0.2: icmp_seq=3 ttl=64 time=0.368 ms

--- 11.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.356/0.362/0.368/0.005 ms
```

FIGURA 5.18: Prueba exitosa de conectividad entre *host A* y *host B*.

Capítulo 6

Conclusión

En este proyecto, se ha realizado una vasta investigación para adquirir conocimientos relacionados particularmente con la gestión de la configuración de los equipos de red y también con el esquema denominado Redes Definidas por Software. Así, se realizó una comparación entre dos implementaciones abiertas del protocolo NETCONF y un estudio del controlador ONOS. Luego, se propuso utilizar ambas tecnologías con el fin de poder monitorear y configurar un dispositivo óptico, precisamente un *muxponder* de 40GB. Para materializar esto, se construyó un ambiente de trabajo conformado por el controlador SDN ONOS, switches virtuales, computadoras de propósito general e integrando el agente NETCONF Yuma123 en el *muxponder* de 40GB.

A continuación, se listan las principales reflexiones finales obtenidas tras el desarrollo de este proyecto.

- Al finalizar este trabajo, se adquirió un conocimiento acabado del nuevo esquema de red que plantea SDN. Se ha generado un documento donde se recopilan todas las características, el principio de funcionamiento y beneficios de este innovador y prometedor enfoque. A su vez, este escrito contiene un análisis del controlador ONOS, mostrando su diseño y como implementa este las diversas cualidades de un controlador SDN.
- En el proyecto integrador se ha realizado un estudio sobre la gestión de la configuración de los equipos de red. Se logró integrar y adaptar al *muxponder* una implementación de código abierto del protocolo NETCONF llamada Yuma123.
- Con el fin de poder administrar la configuración del equipo, se realizó un módulo YANG que describe y modela los datos del dispositivo. También fue necesario realizar una librería en C que relacione los comportamientos típicos y las variables del equipo con el agente Yuma123.
- Para lograr una comunicación entre los dispositivos y el controlador, se desarrolló un *driver* en la interfaz *southbound* de ONOS. Además, se realizó también una aplicación que reside en la interfaz *northbound* del mismo, con el fin de exponer interfaces a las aplicaciones externas para que estas puedan comunicarse con los dispositivos.
- Finalmente, haciendo uso de lenguajes como *Python*, *HTML*, *JavaScript* y *CSS*, se desarrolló una aplicación que presenta una interfaz gráfica al administrador. En la misma, se muestra información de los dispositivos y permite al administrador realizar cambios en la configuración. Para ello, dicha aplicación se comunica a través de la interfaz *northbound* del controlador.

6.1. Problemas y limitaciones

A continuación, se presentan algunos de los problemas y limitaciones del proyecto:

- Al ser una tecnología nueva, el controlador *ONOS* recibe modificaciones constantemente. Desde su primera entrega en diciembre de 2014, existen diecisiete versiones distintas del controlador. Así, a la hora de desarrollar una aplicación interna al controlador, esto presenta un problema ya que uno debe prestar atención a la versión del mismo que está utilizando porque por el momento, ejecutar una misma aplicación en otra versión del controlador requiere modificaciones no despreciables.
- Sin duda uno de los problemas que más ralentizó el avance del proyecto fueron las limitaciones en cuanto a recursos disponibles del dispositivo utilizado, el *muxponder* de 40GB. Se tuvo dificultades a la hora de integrar algún agente del protocolo *NETCONF* debido a las capacidades del equipo y las diferentes librerías necesarias por las implementaciones. Precisamente, se tuvieron problemas con la utilización de la memoria principal y secundaria del *muxponder*, como así también la arquitectura que presenta el procesador *NIOS II*.
- Otro problema menor encontrado fue la interfaz gráfica que brinda el controlador *ONOS*, donde se puede ver que la topología controlada ante sucesivos cambios abruptos en ella queda desactualizada y es necesario recargarla. Sin embargo, al ser una interfaz web, no representa gran inconveniente.
- Por último, se detectó un problema a la hora de establecer el inicio de sesión y el intercambio de capacidades entre el controlador y el agente *NETCONF* del dispositivo. Sucede que el inicio de sesión entre ambos demora unos segundos debido a las capacidades del *muxponder*, y durante ese momento el controlador no bloquea otras operaciones *NETCONF* con el dispositivo. Esto provocaba que el servidor del dispositivo cierre inmediatamente la sesión *SSH* con el controlador, por lo que para solucionar el inconveniente se tuvo que realizar una espera en la función *DeviceDescriptionDiscovery* hasta que el intercambio finalice correctamente antes de llamar cualquier otra operación *NETCONF*.

6.2. Continuidad del trabajo

En el transcurso del trabajo han surgido propuestas para mejorar y continuar en el ámbito de este proyecto integrador. Algunas de ellas son:

- **Optimizaciones en el *driver*.** Observando el resto de las aplicaciones y *drivers* que provee *ONOS*, se detectó que todas poseen una estructura de directorios y archivos común. En el desarrollo del *driver* no se siguió estrictamente esta estructura, lo cual es una posible mejora para la implementación.
- **Adaptación del módulo *YANG* a *OpenConfig*.** *OpenConfig* propone un modelo que busca ser estandarizado por la *IETF* para homogeneizar los datos de configuración y estado de los dispositivos de red, entre ellos dispositivos ópticos

como el *muxponder*. De esta forma, adaptar el esquema que propone *OpenConfig* al módulo YANG desarrollado supondría una ventaja a los proveedores de servicios que requieren una comunicación con diversos dispositivos de diferentes fabricantes.

- **Auto descubrimiento de los vecinos.** El procedimiento que el controlador lleva para formar los enlaces de los dispositivos dependen de la información y la configuración de los mismos (es decir, el equipo debe contar con información de número de serie del vecino, puerto vecino y puerto local para formar un enlace). Una posible mejora podría ser mejorar este proceso para hacerlo independiente de la configuración y por lo tanto independiente del administrador, haciendo que los dispositivos auto descubran sus vecinos.

6.3. Aporte personal

A modo de cierre de este proyecto integrador de la carrera de Ingeniería en Computación, se exponen algunas opiniones y valoraciones personales que han surgido con la finalización de este trabajo.

El proyecto integrador tiene como objetivo desarrollar e integrar los conocimientos adquiridos y la formación lograda a lo largo de la carrera. Es el punto culmine de un camino de 5 años para la obtención del título de grado de Ingeniero en Computación.

Durante la ejecución del trabajo de fin de carrera, se presentaron diversas situaciones donde fue necesario demostrar creatividad, constancia, responsabilidad y criterio profesional para hacer frente a ellas.

Con la ayuda de los múltiples conocimientos en redes de computadoras, programación orientada a objetos e ingeniería de software incorporados durante la carrera, se logró diseñar e implementar el sistema deseado. En materia de investigación y aprendizaje, más allá de la adquisición de los conceptos del innovador esquema de redes definidas por software, se realizó un estudio de los protocolos de gestión de la configuración de los dispositivos de red, entre ellos *NETCONF*, de los cuales se tenía un conocimiento insuficiente para llevar acabo su implementación en un entorno *SDN*.

Para finalizar, con perseverancia y esfuerzo, se ha cumplido con éxito un proyecto desafiante sobre tecnología de vanguardia, alcanzando así una satisfacción tanto a nivel personal como profesional.

Apéndice A

Tutorial para desplegar el entorno y las aplicaciones desarrolladas

En este apéndice, se detalla el procedimiento en el cual se configura el entorno sobre el que se llevan a cabo todos los desarrollos del trabajo. Luego se explica el procedimiento que se debe seguir para instalar las aplicaciones e iniciar la interfaz gráfica.

A.1. Instalación del agente en el dispositivo

A continuación se listan y explican los pasos que se deben seguir para poder instalar e iniciar el agente NETCONF en el dispositivo.

- **Compilar el agente Yuma123:** En primer lugar, se deberá compilar el agente para la arquitectura deseada. Para ello, se usarán los *scripts* realizados con *Dockerfile*. Un ejemplo de compilación para la arquitectura *NIOS II* (arquitectura del procesador del *muxponder* de 40GB) se muestra a continuación.

```
$ cd .../NETCONF-SDN/compile_yuma123/
$ make all TARGET=nios2
```

- **Instalar el agente en el dispositivo:** Una vez compilado exitosamente, se deberá instalar el agente. Para ello se hace uso de un *script* en *bash*, al cual se le especifica un usuario *SSH*, dirección IP y arquitectura deseada. Un ejemplo de uso se puede ver a continuación.

```
$ cd .../NETCONF-SDN/compile_yuma123/utils_scripts/
$ bash ./remote_install_yuma.sh @user @host @arch
```

- **Instalar el módulo YANG y librería desarrollada:** Luego, se debe instalar tanto el módulo *YANG* como la librería en C desarrollada. Existe otro *script* en *bash* que facilitará esta tarea. Para su uso, se debe especificar un usuario *SSH*, dirección IP, nombre del módulo a instalar y la arquitectura deseada. Dicho script se encarga no solo de pasar a la carpeta requerida tanto el módulo como la librería, sino que también las compila previamente. Un ejemplo de su uso es el que se observa:

```
$ cd .../NETCONF-SDN/examples_modules/utils_scripts/
$ bash ./remote-install-module.sh @user @host @module @arch
```

- **Inicio del agente en el dispositivo:** Una vez instalado el agente y la librería, se puede iniciar el servidor *netconfd* en el dispositivo. Para ello, indicamos el módulo a iniciar junto con el servidor, el nivel de debug deseado y el *container target* de las operaciones por defecto.

```
$ cd ~/usrapp/sbin/
$ ./netconfd --module=cli-mxp --log-level="debug2" --target=
running --superuser=root --with-startup=true
```

A.2. Inicio del controlador ONOS

En esta sección se muestra como iniciar el controlador *ONOS* que se comunicará con los dispositivos.

- **Compilación del controlador:** En primer lugar, se deberá compilar el controlador. Para ello, se ejecutará el comando que se muestra a continuación. El controlador cargará de forma automática el *driver* desarrollado.

```
$ cd $ONOS_ROOT && tools/build/onos-buck run onos-local -- clean
debug
```

- **Instalación de la interfaz REST en el controlador:** Luego, se deberá compilar e instalar en el controlador la aplicación que provee una interfaz REST para la interfaz gráfica desarrollada. Los pasos a seguir para este objetivo se muestran a continuación.

```
$ cd ../../NETCONF-SDN/onos/app-altura/altura/ && mvn clean install
&& onos-app localhost reinstall! target/altura-1.0-SNAPSHOT.
oar
```

- Algunos comandos útiles:

```
http://localhost:8181/onos/ui/login.html#/topo //interfaz
gráfica de ONOS
$ cd $ONOS_ROOT && tools/test/bin/onos karaf@localhost // To
attach to the ONOS CLI console
```

A.3. Interfaz gráfica

Por último, se muestra cómo iniciar la interfaz gráfica desarrollada.

- **Entorno virtual de Python:** Para no interferir con el binario de Python instalado en el host local, primeramente se deberá instalar un entorno virtual de Python junto con las librerías requeridas por la interfaz gráfica. Para ello se ejecuta:

```
$ cd ../../NETCONF-SDN/python-app/
$ virtualenv2 altura-gui
$ ./altura-gui/bin/pip2.7 install -r requirements.txt #(or in
Windows - sometimes python -m pip install -r requirements.txt
)
```

- **Inicio de la interfaz:** Una vez preparado el entorno virtual, se ejecuta la aplicación WEB de la siguiente forma:

```
$ ./altura-gui/bin/python2.7 altura.py
```

- Algunos comandos útiles:

```
http://127.0.0.1:5000/ //Para acceder a la interfaz gráfica
```

A.4. Código fuente de la aplicación

El código fuente de las aplicaciones y el controlador, requeridos para las pruebas mencionadas anteriormente, puede obtenerse clonando los repositorios

```
git clone https://github.com/ragnar-l/NETCONF-SDN
```

```
git clone https://github.com/ragnar-l/onos-fork
```


Bibliografía

- [1] *A Simple Network Management Protocol (SNMP)*. URL: <https://tools.ietf.org/html/rfc1157>.
- [2] *A Simple Network Management Protocol (SNMP)*. URL: <https://tools.ietf.org/html/rfc1157#section-3>.
- [3] M. Bjorklund. *A YANG Data Model for System Management*. URL: <https://www.ietf.org/rfc/rfc7317.txt>.
- [4] Siddharth Sakthidharan Brian Hedstrom Akshay Watwe. *Protocol Efficiencies of NETCONF versus SNMP for Configuration Management Functions*. URL: <https://pdfs.semanticscholar.org/5664/44aa2023ac8cf9910cc33ead8582ace4c9c4.pdf> (visitado 03-05-2019).
- [5] CESNET. *Netopeer*. URL: <https://github.com/CESNET/netopeer>.
- [6] CESNET. *Netopeer2*. URL: <https://github.com/CESNET/Netopeer2>.
- [7] Docker. *Docker Documentation*. URL: <https://docs.docker.com/engine/reference/builder/> (visitado 03-05-2019).
- [8] Nikesh Dubey. *From Static Networks to Software-driven Networks*. URL: <https://www.isaca.org/Journal/archives/2016/volume-4/Pages/from-static-networks-to-software-driven-networks-an-evolution-in-process.aspx>.
- [9] Nick Feamster. *The Road to SDN - An intellectual history of programmable networks*. URL: <https://queue.acm.org/detail.cfm?id=2560327>.
- [10] Open Networking Foundation. *Software-Defined Networking: The New Norm for Networks*. Inf. téc. ONF, 2013.
- [11] G.709 : *Interfaces para la red óptica de transporte*. URL: <https://www.itu.int/rec/T-REC-G.709/es>.
- [12] Paul Göransson, Chuck Black y Timothy Culver. *Software Defined Networks A Comprehensive Approach*. Second edition. Elsevier, 2017.
- [13] *Introducing ONOS -a SDN network operating system for Service Providers*. URL: <http://onosproject.org/wp-content/uploads/2014/11/Whitepaper-ONOS-final.pdf>.
- [14] *License, Patents, and Contributor Agreement*. URL: <https://onosproject.org/agreement/>.
- [15] SDNCentral LLC. *2017 Network Virtualization Report SDN Controllers, Cloud Networking and More*. Inf. téc. SDx Central, 2017.
- [16] MDallaglio. *Control and Management of Transponders With NETCONF and YANG*. URL: <http://147.102.16.1/orchestra/07899261.pdf> (visitado 03-05-2019).

- [17] Carl Moberg. *A 30-minute Introduction to NETCONF and YANG*. URL: <https://www.slideshare.net/cmoberg/a-30minute-introduction-to-netconf-and-yang>.
- [18] *Muxponder: Take a Fresh Look at 100G*. URL: <http://www.fiberopticshare.com/muxponder-take-fresh-look-100g.html>.
- [19] *NETCONF Configuration Protocol*. URL: <https://tools.ietf.org/html/rfc4741>.
- [20] *Network Configuration Protocol (NETCONF)*. URL: <https://tools.ietf.org/html/rfc6241>.
- [21] *Nios® II Processors*. URL: <https://www.intel.com/content/www/us/en/programmable/products/processors/support.html>.
- [22] Karim Okasha. *Network Automation and the Rise of NETCONF*. URL: <https://medium.com/k.okasha/network-automation-and-the-rise-of-netconf-e96cc33fe28>.
- [23] Object Management Group OMG. *What is SysML?* URL: <http://www.omg.sysml.org/what-is-sysml.html> (visitado 02-01-2018).
- [24] ON.LAB. *Template Application Tutorial*. URL: <https://wiki.onosproject.org/display/ONOS/Template+Application+Tutorial> (visitado 03-05-2019).
- [25] ON.LAB. *Template Application Tutorial*. URL: <http://flask.pocoo.org/> (visitado 03-05-2019).
- [26] ON.LAB. *The Network Configuration Service*. URL: <https://wiki.onosproject.org/display/ONOS/The+Network+Configuration+Service> (visitado 03-05-2019).
- [27] ONOS: *Towards an Open, Distributed SDN OS*. URL: <https://onosproject.org/wp-content/uploads/2014/11/HotSDN-paper-2014-ONOS-Towards-an-Open-Distributed-SDN-OS.pdf>.
- [28] Open Networking Foundation. URL: <https://www.opennetworking.org/>.
- [29] Optical Network - Definition - What does Optical Network mean? URL: <https://www.techopedia.com/definition/23643/optical-network>.
- [30] Organizations supporting the Open Network Operating System. URL: <https://onosproject.org/members/>.
- [31] Overview of the 2002 IAB Network Management Workshop. URL: <https://www.ietf.org/rfc/rfc3535.txt>.
- [32] OWASP Top Ten Cheat Sheet. URL: https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet.
- [33] Linux man page. SCP. URL: <https://linux.die.net/man/1/scp> (visitado 03-05-2019).
- [34] Sterling Perrin. *SDH Network Modernization With MultiserviceOTN*. URL: <http://www-file.huawei.com/~/media/CORPORATE/PDF/white%20paper/sdh-network-modernization-with-multiservice-otn.pdf>.
- [35] Christos Rizos. *Why use NETCONF/YANG when you can use SNMP and CLI?* URL: <https://snmpcenter.com/why-use-netconf/>.
- [36] Margaret Rouse. *The Data Plane*. URL: <https://searchnetworking.techtarget.com/definition/data-plane-DP>.

- [37] JOONAS RUOHONEN. *Evaluating the Network Management Capabilities of YANG and NETCONF*. URL: <https://pdfs.semanticscholar.org/5906/d503dfbbb9017901f51ef.pdf> (visitado 03-05-2019).
- [38] Brent Salisbury. *The Control Plane, Data Plane and Forwarding Plane in Networks*. URL: <http://networkstatic.net/the-control-plane-data-plane-and-forwarding-plane-in-networks/>.
- [39] *SDN architecture*. URL: https://www.opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf.
- [40] *Software-Defined Multilayer Networks*. URL: <https://www.ecitele.com/wp-content/uploads/2018/10/trains-planes-and-more-fibre-systems-spring-2017.pdf>.
- [41] Sysrepo. *Sysrepo*. URL: <https://github.com/sysrepo/sysrepo>.
- [42] Sysrepo. *Sysrepo*. URL: <https://github.com/sysrepo/sysrepo/blob/master/INSTALL.md>.
- [43] *Understanding NETCONF and YANG*. URL: <https://www.networkworld.com/article/2173842/understanding-netconf-and-yang.html>.
- [44] *Understanding the SDN Architecture – SDN Control Plane and SDN Data Plane*. URL: <https://www.sdxcentral.com/networking/sdn/definitions/inside-sdn-architecture/>.
- [45] Vladimir Vassilev. *Yuma123*. URL: <https://github.com/vlvassilev/yuma123>.
- [46] Vladimir Vassilev. *Yuma123*. URL: http://yuma123.org/wiki/index.php/Yuma_netconfd_Manual#Features.
- [47] *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*. URL: <https://tools.ietf.org/html/rfc6020>.
- [48] YumaWorks. *YumaPro*. URL: <https://www.yumaworks.com/features/open-source/>.