“Implementación de un laboratorio virtual de redes de datos y simulación de una red empresarial con sucursales para prácticas de laboratorio en el laboratorio de comunicaciones de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga”

Guamán Yanez, María Esther y Loachamin Alvarez, Alexis Israel

Departamento de Eléctrica y Electrónica.

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Monografía Previo a la Obtención del Título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Caicedo Altamirano, Fernando Sebastián

09 de agosto de 2021

Latacunga

Reporte de verificación de contenido

20/9/21 16:06 Documento Final Integración Curricular Loachamin Guaman

Informe de originalidad

NOMBRE DEL CURSO
MIC-Profesionalizante NRC 6947

NOMBRE DEL ALUMNO
ALEXIS ISRAEL LOACHAMIN ALVAREZ

NOMBRE DEL ARCHIVO
ALEXIS ISRAEL LOACHAMIN ALVAREZ - Documento Final Integración Curricular

SE HA CREADO EL INFORME
20 sept 2021

Resumen

Fragmentos marcados	26	4 %
Fragmentos citados o entrecomillados	7	0,9 %

Coincidencias de la Web

openwebinars.net	6	0,5 %
ymant.com	3	0,4 %
internexa.com	3	0,4 %
1library.co	1	0,4 %
orange.es	2	0,4 %
iadb.org	3	0,3 %
welivesecurity.com	1	0,3 %
ucsg.edu.ec	2	0,3 %
eduardocollado.com	1	0,3 %
puce.edu.ec	2	0,2 %
universidadviu.com	1	0,2 %
redeszone.net	1	0,2 %
edutec.es	1	0,2 %
marketing4ecommerce.net	1	0,2 %
cisco.com	1	0,2 %
ibm.com	1	0,2 %
fs.com	1	0,2 %
elcomercio.com	1	0,1 %
gaz.wiki	1	0,1 %

1 de 33 fragmentos
Fragmento del alumno ENTRECOMILLADO

https://classroom.google.com/g/tg/Mzk2MzU5MDY1MDA5/Mzk2MzY4MjcxNzg4#u=NjMzODMyOTM5MDha&t=f 1/10

Ing. Caicedo Altamirano, Fernando Sebastián

C. C:1803935020

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que la monografía, "**Implementación de un laboratorio virtual de redes de datos y simulación de una red empresarial con sucursales para prácticas de laboratorio en el laboratorio de comunicaciones de la Universidad de las Fuerzas Armadas ESPE sede Latacunga**". Fue realizado por los señores **Guamán Yanez, María Esther** y **Loachamin Álvarez, Alexis Israel,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Latacunga, 09 de agosto del 2021

Ing. Caicedo Altamirano, Fernando Sebastián

C. C:1803935020

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de autoría

Nosotros, **Guamán Yanez, María Esther** con cédula de ciudadanía 055022255-8 y **Loachamin Alvarez, Alexis Israel**, con cédula de ciudadanía 175255206-5, declaramos que el contenido, ideas y criterios de la monografía: **"Implementación de un laboratorio virtual de redes de datos y simulación de una red empresarial con sucursales para prácticas de laboratorio en el laboratorio de comunicaciones de la Universidad de las Fuerzas Armadas ESPE sede Latacunga"** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 09 de agosto del 2021

Loachamin Álvarez Alexis Israel

C.C.: 1752552065

Guaman Yanez María Esther

C.C.: 0550222558

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Nosotros, **Guamán Yanez, María Esther** con cédula de ciudadanía 055022255-8 y **Loachamin Álvarez, Alexis Israel**, con cédula de ciudadanía 175255206-5, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: "**Implementación de un laboratorio virtual de redes de datos y simulación de una red empresarial con sucursales para prácticas de laboratorio en el laboratorio de comunicaciones de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga**" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Latacunga, 09 de agosto de 2021

Loachamin Álvarez Alexis Israel

C.C.: 1752552065

Guaman Yanez María Esther

C.C.: 0550222558

Dedicatoria

Este trabajo está dedicado en primer lugar a mi Dios, por cada día de vida, salud, favores recibidos, durante el transcurso de mi carrera. A mi madre que a pesar de ser sola logro sacarnos adelante a mi hermano y a mí. A mi linda Mamita por haber sido la abuelita más amorosa, de todo el mundo. A mi abuelito por haber ocupado el lugar de mi padre, mi viejito hermoso eres y serás mi héroe, mi ejemplo las ganas de levantarme cada día seguir luchando para que algún día pueda cumplir mis sueños y metas.

-María Guamán

Dedico este trabajo a mis compañeros de proceso académico a lo largo de mi vida, por ser las personas que me demostraron el valor de una verdadera educación, por ser las personas que me enseñaron lo que cuesta obtener un futuro, a mis amigos que me enseñaron durante este tiempo lo que significa tener un futuro.

-Alexis Loachamin

Agradecimiento

A mi madre por ser la persona más importante en mi vida, por su apoyo tanto en lo económico y moral, brindarme sus consejos, compartir mis momentos felices y tristes. Espero que mis palabras lleguen al cielo a mi hermoso ángel, Mi Mamita Esther, en vida fue mi confidente. Por haberme dado todo su amor y ternura en los momentos buenos, duros, durante toda mi vida estudiantil. A mi hermano, Papito Manuel, Mis Tíos por inspírame, a seguir esforzándome día a día para que algún día no muy lejano pueda asegurar mi futuro. A mis profesores por impartirme todos sus conocimientos en cada semestre académico.

-María Guamán

Quiero agradecer en gran medida a mi amigo Roberth Yugsi por ser mi ayuda dentro de todo el proceso de este proyecto, ha sido un apoyo incondicional en todo momento, y le debo mucho más que solo un agradecimiento.

-Alexis Loachamin

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

La implementación del laboratorio de redes virtuales en uno de los laboratorios de comunicaciones de la Universidad de las Fuerzas Armadas ESPE por medio del simulador de redes GNS3 resultaría ser totalmente beneficioso para los estudiantes de la carrera de redes y telecomunicaciones en su objetivo de cumplir con un proceso académico para lograr un perfil profesional acorde al mundo laboral actual. El software de simulación permitirá a los estudiantes realizar prácticas de laboratorio sin la necesidad de recurrir a equipos de alto costo y difíciles de conseguir, este programa tiene un potente sistema que ofrece a los estudiantes la oportunidad de trabajar en topologías de red extensas, como ejemplo el establecer la red de datos de la Universidad de las Fuerzas Armadas ESPE con sus respectivas sucursales dentro del simulador permitió evidenciar el potencial de GNS3 al emular equipos de red multimarca y aplicar diferentes protocolos bajo los cuales una arquitectura de red en la vida real funcionaria, este proceso permitió generar un manual de instalación y funcionamiento de GNS3, así como una guía de implementación de la red de datos simulada en el mismo programa, estos documentos fueron entregados a la universidad como parte de la implementación del laboratorio virtual de redes en las computadoras de uno de los laboratorios de comunicaciones de la universidad.

Palabras Clave: Laboratorio de redes virtual, GNS3, Red de datos, Emulación, Simulador

Abstract

The implementation of the virtual networks laboratory in one of the communications laboratories of the “Universidad de las Fuerzas Armadas ESPE Latacunga” through the GNS3 network simulator, would prove to be totally beneficial for the students of the networks and telecommunications career in their objective to get a academic process to achieve a professional profile according to the current world of work. The simulation software will allow students to carry out laboratory practices without the need to resort to expensive and difficult to obtain equipment, this program has a powerful system that offers students the opportunity to work on extensive network topologies. As an example, establishing the data network of the “Universidad de las Fuerzas Armadas ESPE” with its respective branches within the simulator allowed to demonstrate the potential of GNS3 by emulating multi-brand network equipment and applying different protocols under which a network architecture in life real official, this process allowed the generation of a “GNS3 installation and operation manual”, as well as a “ESPE corporate network implementation guide with branches in GNS3”, these documents were delivered to the university as part of the implementation of the virtual network laboratory in the computers in one of the university's communications labs.

Key Words: Virtual networking laboratory, GNS3, Data network, Emulation, Simulator

Capítulo I: Planteamiento del problema de Investigación.

Antecedentes

Las telecomunicaciones en la actualidad se han convertido en el pilar fundamental de las sociedades modernas, de manera que todos aquellos sistemas que representen intercambio de información serán de vital importancia para el desarrollo humano, Pero ¿Qué tan capacitados estamos como país para el desarrollo de las redes de comunicaciones y por lo tanto de la sociedad misma? Para obtener un panorama más claro de la situación Burbano (2019), presenta un análisis sobre la situación de Ecuador según un estudio realizado por la empresa.

> Surfshark denominado 'Digital Quality of Life 2019' "Ecuador es el sexto país de la medición con peor calidad de vida digital y el quinto peor en temas de ciberseguridad. En los dos parámetros somos últimos en Latinoamérica, lo cual revela que el país tiene mucho que hacer." (pág. 1)

Se realiza una breve investigación que demuestran la importancia de las telecomunicaciones, así como algunos de sus principales componentes. El señor Daniel Vallejo (2020) en su trabajo de titulación: "análisis comparativo de tecnologías para el diseño de red wlan para el laboratorio de tecnologías de la información y comunicación de la facultad de ingeniería de la pontificia universidad católica del ecuador empleando estándar 802.11n" establece que "se puede determinar que las simulaciones de redes inalámbricas, pueden contribuir al adecuado funcionamiento de WLANs, aportando datos significativos que permitan la correcta toma de decisiones al implementarlas en la realidad" (pág. 46).

De manera en que el diseño e implementación de redes de telecomunicaciones contribuye indiscutiblemente al desarrollo de las sociedades, para la actualidad ya no es necesario la construcción de grandes y aparatosos laboratorios de redes, la simulación es la

respuesta a estos inconvenientes y como lo explica la ingeniera Dulce María Vélez (2018) en su trabajo de titulación “diseño y simulación en gns3 de una red multiservicios mpls para medianas empresas en el ecuador" donde implemento una red multiservicios en el simulador GNS3 establece lo siguiente:

> Lograr conocer el funcionamiento, características de una herramienta muy útil e indispensable para los ingenieros que laboran en el área de Redes, como es el software GNS3 que fue el simulador utilizado para implementar el diseño de red del proyecto de trabajo de titulación.
>
> Se logró diseñar y simular una red de alta confiabilidad y rápida convergencia que permita transmitir varios servicios para las medianas empresas en el Ecuador. (pág. 61)

Como se puede evidenciar en los trabajos anteriormente descritos hay un gran interés en la implementación de laboratorios virtuales para las redes y telecomunicaciones, por lo cual es importante que la Universidad ESPE cuente con estos laboratorios de redes virtuales y que permitan el correcto estudio para la implementación de redes en la realidad.

Planteamiento del Problema

Una de las problemáticas a nivel Ecuador es el inadecuado proceso de incorporación hacia una sociedad moderna, esto se ve reflejado en los servicios con lo que el país cuenta, por como se explica en el informe del Inter-American Development Bank entre varios autores afirman lo siguiente:

> Ecuador todavía tiene un camino importante por delante en el fortalecimiento de su sector de conectividad digital. La penetración de los servicios de Banda Ancha (BA) fija

> y móvil es tan sólo un 10% y un 53%, respectivamente, por debajo del resto de países de ALC (13% y 65%) y muy lejos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (33% y 96%). Tan sólo el 62% de la población está cubierta por redes de BA móvil de alta velocidad (vs. 67% en ALC y 98% en la OCDE). (Rivera Zapata, Iglesias RodrigueZ, & García Zaballos, 2020, pág. 4)

De manera que la correcta capacitación hacia estudiantes de carreras técnicas en telecomunicaciones es indiscutiblemente un requisito para el progreso del país, el cual es un problema que como se describe en la revista electrónica de tecnología educativa EDUTEC en su investigación acerca de la importancia de las herramientas y entornos de aprendizaje dentro de las plataformas e-learning en las universidades del Ecuador, menciona que:

> En cuanto a las condiciones tecnológicas con las que cuentan las Universidades para hacer uso de las plataformas e-learning, la mayoría de los estudiantes, es decir, 145 para un 56,64%, la catalogan de aceptable; 45 estudiantes (17,58%) la encuentran deficiente mientras que 39 (15,23%) la encuentra buena. Solo 16 alumnos (6,25%) consideran el estado de la infraestructura tecnológica mala mientras que 11 (4,30%) la encuentra óptima. (Verdezoto Rodríguez & Chávez Vaca, 2018, pág. 9)

En la Universidad de las Fuerzas Armadas ESPE sede Latacunga se ha detectado la falta de un laboratorio de comunicaciones para la simulación de redes de datos. La falta de adecuada capacitación hacia los estudiantes ha dado como resultado un aprendizaje incompleto. Por la pandemia de covid-19 que comenzó en el año 2020, la comunidad universitaria busco alternativas para su educación, pero el problema para carreras técnicas y tecnológicas es la dificultad en el acceso a equipos y recursos tecnológicos reales que permitan cumplir con las prácticas de laboratorio necesarias para el correcto aprendizaje.

Presentado el problema que se puede evidenciar, es importante la implementación de mecanismos para el correcto desempeño en la configuración de dispositivos de manera virtual por medio del manejo de softwares de simulación de redes, con dispositivos de red multimarca utilizados en el ámbito profesional.

Justificación e importancia

¿Qué tan importante son las telecomunicaciones en la actualidad?, si bien las personas están conscientes sobre el progresivo mundo de las redes de datos y su influencia en todos los procesos de las sociedades, como lo explica la señorita Susana (2021) en el sitio web marketing4ecommerce:

> “muchos de los indicadores en el informe Digital 2021 realizado por We Are Social y Hootsuite han experimentado notables niveles de crecimiento en el último año.
>
> Para esta edición, el informe señala que el número de usuarios de internet en el mundo ha alcanzado los 4.660 millones de personas, lo que representa al 59,5% de la población (7.830 millones de personas)” (pág. 1)

Para la nueva realidad que se vive en el presente año, el teletrabajo y la educación presencial-virtual se han convertido en la principal alternativa para actividades educativas y laborales. Las universidades como centros de desarrollo académico deben garantizar un correcto aprendizaje pues como se establece en el reglamento académico del consejo de educación superior en el artículo 29 se establece que:

> **Aprendizaje práctico-experimental,** El aprendizaje práctico-experimental es el conjunto de actividades (individuales o grupales) de aplicación de contenidos conceptuales, procedimentales, técnicos, entre otros, a la resolución de problemas prácticos, comprobación, experimentación, contrastación, replicación y demás que defina la IES; de casos, fenómenos, métodos y otros, que pueden requerir uso de

> infraestructura [física o virtual), equipos, instrumentos, y demás material, que serán facilitados por las IES. (Consejo de Eduacion Superior, 2020, pág. 14)

Por lo tanto, se puede afirmar que es totalmente necesario la implementación de espacios para el aprendizaje practico-experimental, que permita a los estudiantes el desarrollo de sus habilidades prácticas.

Objetivos

Objetivo General

Implementar un laboratorio virtual de redes de datos y simular una red empresarial con sucursales para prácticas de laboratorio en el laboratorio de comunicaciones de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga.

Objetivos Específicos

- Investigar acerca del simulador de redes GNS3 y todas las características y servicios que tiene una red corporativa para establecer los parámetros de funcionamiento de la red simulada.
- Instalar el simulador de redes GNS3 e incluir dispositivos de red multimarca en las computadoras del laboratorio de comunicaciones de la ESPEL.
- Implementar una red de datos simulada, con sucursales que contengan los parámetros, servicios y protocolos de una red corporativa real.
- Implementar un manual de funcionamiento del software GNS3 y una guía de laboratorio para la implementación de la red corporativa simulada.

Alcance

En este proyecto técnico se establecerá dentro de uno de los laboratorios de comunicaciones de la Universidad de las Fuerzas Armadas sede Latacunga, la instalación del simulador de redes grafico “GNS3”, con el fin de mejorar el proceso de prácticas de laboratorio para el área de Redes y Telecomunicaciones, apoyando de recursos virtuales que son de gran ayuda a los estudiantes que necesitan experimentar bajo condiciones más reales la configuración y administración de equipos para redes de datos. Se espera incentivar a los estudiantes y a la comunidad universitaria el uso de los recursos con los que la institución académica cuenta, para evitar un aprendizaje basado únicamente en la teoría, y evitar el deterioro de los equipos de cómputo que se encuentran en los laboratorios de la Universidad.

Capítulo II: Marco teórico

¿Qué son las redes de datos? ¿Por qué las telecomunicaciones se han vuelto tan importantes? ¿Cuál es el futuro de las redes en telecomunicaciones? Para poder comprender el desarrollo de este proyecto es necesario comprender el origen de las redes como se muestra a continuación.

Las telecomunicaciones:

Siendo este concepto el punto de partida, como lo menciona el autor estadounidense William Stallings en su libro titulado Comunicaciones y Redes de computadoras, él menciona que:

> En torno a los a los años 70 y 80 se produjo una sinergia entre los campos de los computadores y las comunicaciones que ha desencadenado un cambio drástico en las tecnologías, productos y en las propias empresas que, desde entonces, se dedican simultáneamente a los sectores de los computadores y de las comunicaciones, no es arriesgado decir que la revolución ha ocurrido y que ninguna investigación dentro del campo de la transmisión de la información debería realizarse sin esta perspectiva. (Stallings, 2011, pág. 15)

Redes de datos:

Como lo establece un equipo de expertos de la Universidad Internacional de Valencia (2018) donde mencionan que:

> Las redes de datos son infraestructuras que han sido creadas para poder transmitir información a través del intercambio de datos. Es decir, son arquitecturas específicas para este fin, cuya base principal es la conmutación de paquetes y que atienden a una clasificación exclusiva, teniendo en cuenta la distancia que es capaz de

cubrir su arquitectura física y, por supuesto, el tamaño que presentan. (Equipo de Expertos, 2018, pág. 1)

Tipos de redes

Las redes al igual que muchos otros sistemas tienen una clasificación, la cual es descrita por el señor José Poveda en el blog para la empresa Internexa.

Red de área personal (PAN).

Este es el tipo de red informática más básico que existe. La red PAN se compone de un módem inalámbrico, uno o dos computadores, teléfonos, impresoras y una cantidad limitada de dispositivos que están conectados en un rango de diez metros.

Red de área local (LAN).

Seguro habrás oído hablar de ella alguna vez. Las redes de área local se componen de espacios de trabajo interconectados para compartir información y dispositivos.

Red de área amplia (WAN).

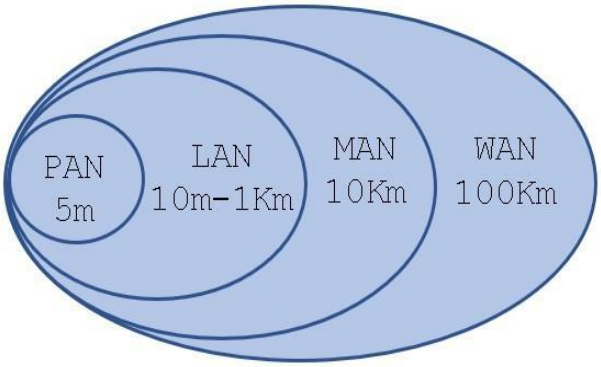
Este tipo de red informática conecta varios dispositivos que se ubican a largas distancias. De esta forma pueden comunicarse de manera remota sin importar qué tan lejos se encuentren.

(Poveda, 2020, pág. 1)

Como un esquema general sobre las redes informáticas en base a su extensión se presenta la siguiente figura.

Figura 1

*Clasificación de las redes según su extensión***.**



Nota. El gráfico presenta la distancia para cada red.

Topologías de red

Las redes en general requieren de arquitecturas lo que se denomina “topologías” que como se explica en el blog OpenWebinars con respecto a estas arquitecturas de red.

> Una estructura de cableado es considerada red informática en el momento en el que existen un conjunto de equipos o dispositivos que se conectan a ella y llegan a establecer comunicación entre sí.

Topología Bus

En esta topología se transmiten los datos por un solo canal de comunicaciones al que van conectados todos los dispositivos.

Topología Anillo

Se trata de una red de ordenadores conectados entre sí haciendo uso de un cable y formando una estructura de anillo.

Topología Estrella

A diferencia de la topología en bus, que tenía un solo canal de comunicaciones, en esta, cada dispositivo de red tiene su propio canal.

Topología Malla

Todos tienen conexiones en todas las direcciones y se encargan de enviar los mensajes por la mejor ruta o la más corta posible.

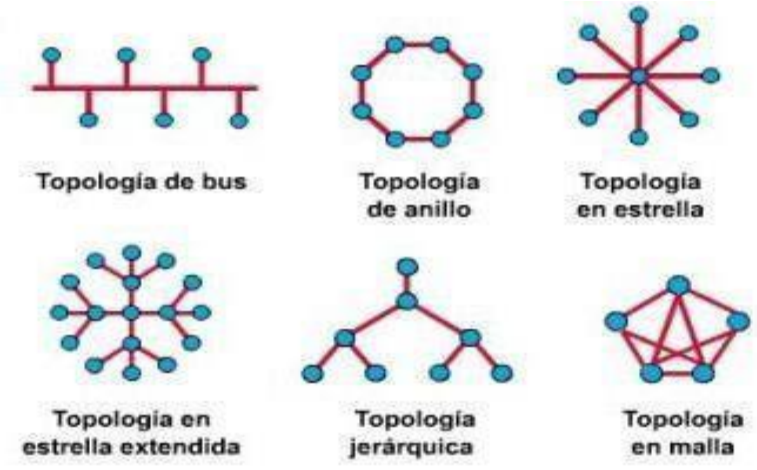
Topología Árbol

Es la unión de la topología de estrella y la de bus, ya que cuenta con un dispositivo central (switch o hub) al que conectan los nodos.

(Limones, 2021, pág. 1)

Figura 2

Topologías de red



Nota. Ejemplos de arquitecturas de red. Tomado de “Introducción a las redes de computadoras” https://alejollagua.blogspot.com/2012/12/topologias-fisicas.html

Protocolos:

Las redes al igual que muchos procesos requieren de normas y reglas que permitan su funcionamiento, para las redes y telecomunicaciones se establecen diferentes “protocolos” que

permiten su funcionamiento, esto se describe de mejor manera en la página web InterServer.net.

Protocolo de Internet (IP)

Su función de enrutamiento esencialmente establece Internet. Históricamente fue el servicio de datagramas sin conexión en el Programa de Control de Transmisión original.

Protocolo de transferencia de hipertexto (HTTP).

HTTP es la base de la comunicación de datos para la World Wide Web. El hipertexto es texto estructurado que utiliza hipervínculos entre nodos que contienen textos.

Protocolo de transferencia de archivos (FTP).

El FTP es el protocolo más común utilizado en la transferencia de archivos en Internet y dentro de redes privadas.

Telnet

Telnet es el método principal utilizado para administrar dispositivos de red a nivel de comando. A diferencia de SSH, Telnet no proporciona una conexión segura, pero proporciona una conexión básica no segura.

Sistema de nombres de dominio (DNS)

El sistema de nombres de dominio se utiliza para convertir el nombre de dominio en una dirección IP. Hay servidores raíz, TLD y servidores autorizados en la jerarquía de DNS.

(Jithin, 2016, pág. 1)

VLAN (Red de área local virtual)

Si bien las redes permiten que la información se comparta entre todos los usuarios de una red, se debe asegurar confidencialidad, como en la página web RZ redes zone lo establece Sergio de Luz (2021) con respecto a las redes locales virtuales.

> Las VLAN o también conocidas como «Virtual LAN» nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soporten VLANs para segmentar adecuadamente la red. También es muy importante que los routers que utilicemos soporten VLAN, de lo contrario, no podremos gestionarlas todas ni permitir o denegar la comunicación entre ellas (pág. 1)

Protocolo Spanning Tree

El crecimiento de las redes ah supuesto de problemas para implementar diferentes caminos hacia un mismo destino, donde la instauración de bucles suele ser un problema recurrente, como lo explica el especialista en telecomunicaciones Eduardo Collado (2018) en su página web.

> En Spanning Tree, el root bridge, el elemento central de la red, este punto será el punto central de ese árbol, o el punto desde el que todos los nodos dependerán y se convertirá en el centro de la red, por eso este equipo se suele forzar al más grande de la red y el más centrado, esto es lo más importante, es muy importante seleccionar bien el nodo que va a ser la raíz del spanning tree. (pág. 1)

PPPoE (Protocolo punto a punto sobre Ethernet)

Del inglés “Point to point protocol over ethernet” es un método se conexión utilizado para los servicios emitidos por un ISP como lo manifiesta la señorita Charlene (2020) en la página web de la empresa FS Europa.

> PPPoE es un protocolo de red utilizado para encapsular tramas PPP (protocolo punto a punto) dentro de tramas Ethernet. Combina el PPP que posee la función de autenticación y cifrado, y el protocolo Ethernet que puede admitir múltiples usuarios en una LAN. (pág. 1)

Protocolo DHCP (Protocolo de configuración dinámica de host)

De las siglas en ingles “Dynamic Host Configuración Host” es la manera en que muchos equipos obtienen una dirección IP y configuraciones, como se explica dentro del articulo por IBM Corporation (2014) para la administracion de redes.

> El protocolo de configuración dinámica de hosts (DHCP) es un estándar TCP/IP que utiliza un servidor central para gestionar direcciones IP y otros datos de configuración para toda una red.
>
> Un servidor DHCP responde a las peticiones de los clientes, asignándoles propiedades de forma dinámica. (pág. 5)

Protocolo OSPF (Abrir primero el camino más corto)

Aunque no se lo pueda notar a simple vista, pero la información que se transfiere de un punto a otro en el mundo se rige bajo protocolos de enrutamiento uno de ellos es OSPF de las siglas en inglés “Open Short Path first” y como se explica en la página web “Geeks for Geeks” por un artículo escrito por el anónimo “saurabhsharma56” (2020).

> Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace que se utiliza para encontrar la mejor ruta entre el enrutador de origen y destino utilizando su propio Shortest Path First). OSPF es desarrollado por Internet Engineering Task Force (IETF) como uno de los Interior Gateway Protocol (IGP), es decir, el protocolo que tiene como objetivo mover el paquete dentro de un gran sistema autónomo o dominio de enrutamiento (pág. 1)

VPN (Red privada virtual)

El Internet es enorme y los usuarios no pueden determinar los equipos a los que la información transmitida puede llegar, por lo que como lo explica André Goujon(2012) en el

portal web “welivesecurity” de la empresa ESET con respecto al uso de redes virtuales privadas.

> Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Como explicamos en el artículo acerca de para qué sirve una VPN, las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es tan solo una de las funciones de una VPN (pág. 1)

Encapsulamiento GRE

Para el uso de la tecnología VPN es necesario de protocolos de encapsulamiento que se explica de mejor manera en el blog del instructor de CCNA (Moisa, 2019).

> GRE (Generic Routing Encapsulation) es un protocolo desarrollado por Cisco System para crear una conexión virtual privada entre 2 puntos, lo interesante de esto es que los datos son encapsulados para poder transmitirlos a través de la conexión virtual a la cual se le conoce como: túnel (pág. 1)

Equipos para redes de datos

Las redes de datos requieren de varios dispositivos y equipos informáticos que permitan su completo funcionamiento esto se describe de mejor manera en el portal web de la empresa YMANT (2021) con respecto a los equipos de red.

> En este artículo comentaremos los dos equipos más habituales para dar conexión a Internet a una pequeña oficina. Existen otras posibilidades que cubre diferentes soluciones y tecnologías (redes inalámbricas, fibras ópticas, conexión por cable eléctrico, etc.), pero que no son tan comunes.

Router

Enrutador (o encaminador en castellano), es un equipo cuya función es interconectar dos redes diferentes. Es el equipo que separa e independiza dos segmentos de red con direccionamiento diferente.

Switch

Conmutador en castellano, es un equipo destino a conectar equipos dentro de un mismo entorno de red. Su función consiste en enviar el tráfico de datos entre equipos de una misma red o enviarlo al router de salida hacia el exterior.

(YMANT, 2021, pág. 1)

Proceso de virtualización

Poder Suplantar aquellos equipos robustos y difíciles de maniobrar comunes en una red de dato, por simple programas que realicen lo mismo, es lo que la señorita Laura (2019) que en su articulo “¿Qué es la virtualización de red y por qué se habla de ello?” explica acerca de este proceso

> La virtualización de red hace uso de dos tecnologías (NFV y SDN) y de un nuevo método de trabajo. En lugar de asignar a cada equipo físico una tarea específica (una funcionalidad), se le asocia un software que poder cambiar a futuro, dándole también la posibilidad de intercambiarlo con otros equipos de la red.
>
> Esto significa que un mismo equipo se vuelve multipropósito (hardware de propósito general) en función del software; y es en este último donde está la funcionalidad. Ahora se puede empaquetar una funcionalidad de red en una o varias “máquinas virtuales”. (pág. 1)

GNS3 (Simulador de redes gráfico).

Es un simulador de redes, el cual permite el diseño, administración, estudio para redes de datos, como lo expresa el señor Joaquín Carmona (2017) en su trabajo de diploma para la Universidad Central “Marta Abreu”de Las Villas.

> GNS3 es un emulador de redes gráfico que emplea como motor de ejecución la plataforma Dynamips/Dynagen. Para interactuar con los routers del escenario, GNS3 ofrece la posibilidad de abrir una consola Telnet. La consola ofrece una interfaz de administración real del router como resultado de ejecutar una imagen IOS de Cisco. GNS3 permite guardar tanto la configuración del escenario como la configuración de cada router en un archivo en formato texto. De este modo, cuando se vuelva a ejecutar la simulación, las configuraciones pueden ser recuperadas automáticamente. Otra funcionalidad para el diagnóstico reside en la capacidad de GNS3 para capturar tráfico enviado y/o recibido a través de una interfaz. (pág. 17)

Capítulo III: Desarrollo del Tema

Primero siendo el simulador gráfico de redes “GNS3” la base de este proyecto, se va a explicar cuál es su arquitectura, instalación, funcionalidad y los beneficios que ofrece al emular una red de datos corporativa como si se tratara de un laboratorio real.

Introducción a GNS3

GNS3 (Graphic Network Simulator) es un simulador gráfico de redes, el cual permite el diseño, administración y configuración de topologías de Red de datos, este potente software de simulación fue lanzado al mercado en 2008, realizado por Jeremmy Grosman con el objetivo de ayudarlo con las certificaciones de CCNP. Es utilizado por varias compañías como Walmart, AT&T, NASA, etc

Figura 3

Logo GNS3

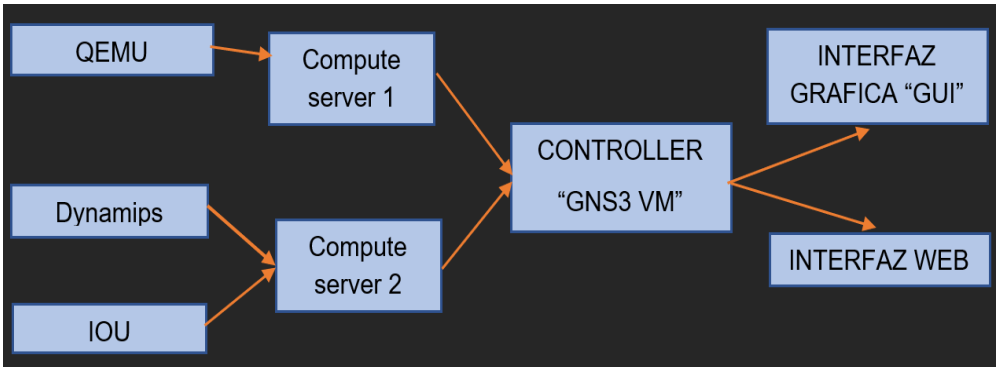
Nota. Logo del programa GNS3 año 2021. Recuperado de http://net4dd.com/guia-de-implementacion-de-gns3-en-windows/

Arquitectura de GNS3

El simulador de redes permite que se emulen redes de datos complejas lo cual pocos programas logran en la actualidad, pero ¿Cómo realiza esto?, principalmente este programa se apoya de un “controlador” lo cual gestiona los procesos de los proyectos que se creen dentro de GNS3.

Figura 4

Arquitectura de funcionamiento GNS3



Nota. La elaboración de esta figura se lo realiza en base a información compartida por la comunidad de GNS3.

De forma que la interfaz gráfica y la interfaz web son las ventanas con las que el usuario manipula el programa, que se traducen en solicitudes al controlador (GNS3 VM) lo cual a su vez permite la administración y control de los diferentes emuladores (Dynamips, QEMU, IOU) que se ejecutan en los (Compute server) que son las bibliotecas que permiten la emulación y su correspondiente administración dentro de GNS3, a este proceso de lo denomina Emulación Anidada.

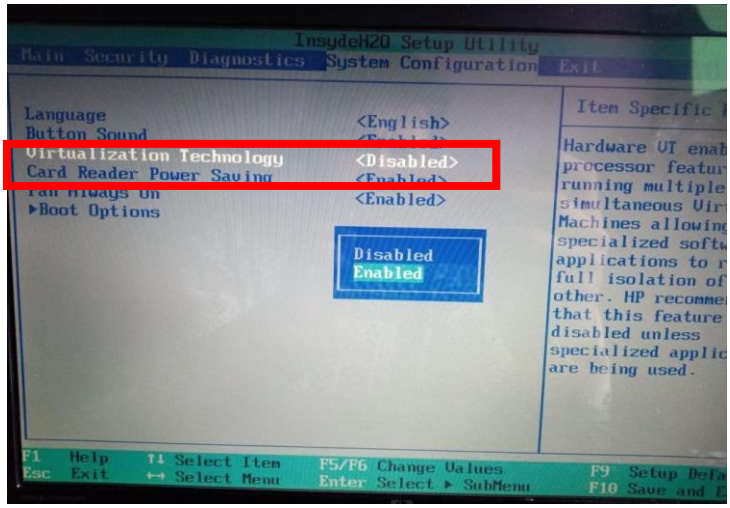
A pesar de esta arquitectura descrita en muchas ocasiones se verá al programa funcionar sin el "controlador" lo que supondría una sobrecarga al computador para cubrir las operaciones que realizaba "GNS3 VM". Por lo que se recomienda que la instalación del programa se la realice conjuntamente con el controlador, GNS3 recomienda que para la emulación de esta máquina virtual se lo realice en el programa "VMware" y su instalación se describe a continuación.

Para instalar este potente software de simulación es necesario hacer uso de un sistema operativo Linux, para lo cual GNS3 requiere de una máquina virtual que se aprovechará como servidor para la emulación de los equipos de red.

Antes de realizar descargas e instalaciones, se debe activar la opción de virtualización en la computadora a utilizar, para lo cual se debe dirigir al BIOS del equipo, y como se muestra en la figura 5, en la pestaña de “System Configuration” habilitar la opción Virtualización Technology.

Figura 5

Activación del proceso de virtualización



Nota. El sistema BIOS mostrado en la figura puede variar según la computadora.

Instalación del Software VMware

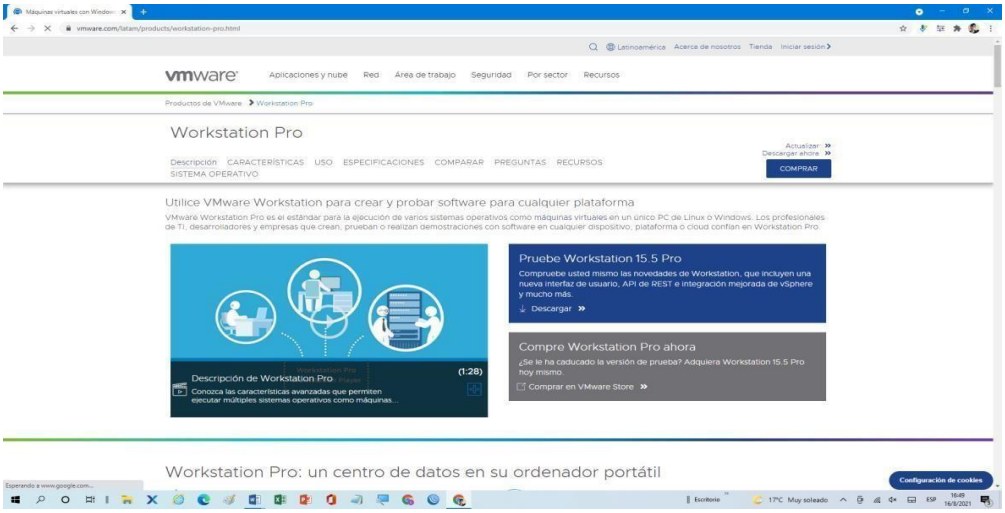
La principal ventaja para utilizar un software de virtualización de máquinas virtuales para GNS3 es disminuir el gasto hacia la maquina física, ya que el simulador requiere un esfuerzo de los recursos de esta, por lo que al usar una máquina virtual basada en un sistema operativo Linux Ubuntu los componentes como el CPU y la memoria RAM se mantienen bajo un uso moderado.

Primero es necesario descargar el instalador del software, el cual se lo puede encontrar en la página web https://www.vmware.com/latam/products/workstationpro.html por debajo de

una breve descripción sobre el programa existen dos opciones y un video explicativo, al dar clic en la opción de color azul se direccionará a una nueva ventana.

Figura 6

Página de descarga VMware Workstion Pro

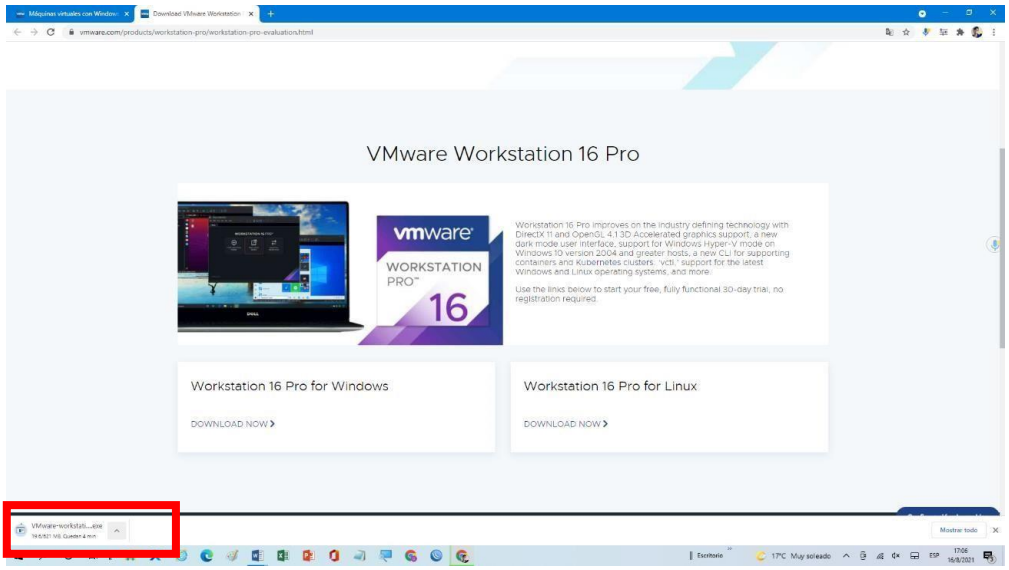


Nota. En la página de la máquina virtual existe el instalador de Workstation versión 16 Pro también un video donde explica el funcionamiento del Software.

En esta nueva ventana se podrá encontrar la última versión del software, para la fecha en que se escribe este manual, la versión es “VMware Workstation 16 Pro” y tras una breve descripción de este programa, por debajo, existen dos opciones una para la descarga del software en Windows y la segunda para Linux. De esta manera al dar clic en la opción Windows. Empezara la descarga del programa el cual pesa 621 MB, como se muestra en la figura 7.

Figura 7

VMware Workstation 16 Pro versión para Windows

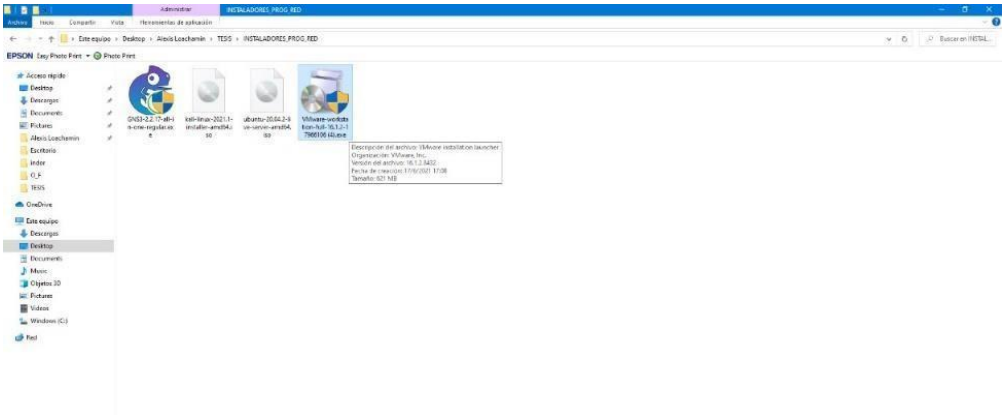


Nota. Aquí debe escoger el sistema operativo correspondiente al ordenador, comprueba si tiene espacio suficiente para la descarga e instalación.

Se recomienda que se use el software “VMware Workstation” por su compatibilidad con el simulador de redes, y de esta manera se obtendrá el siguiente archivo de instalación que se muestra en la figura 8.

Figura 8

Instalador de VMware Workstation 16



Nota. El archivo pesa 621Mb, se lo puede encontrar en fuentes no fiables.

Se debe dar clic derecho sobre este mismo archivo para “Ejecutar como administrador” al realizar esto, una nueva ventana se abrirá en medio de la pantalla con el logo del programa, como se muestra en la figura 9, de igual forma por debajo de esta ventana un pequeño recuadro muestra el avance de la instalación.

Figura 9

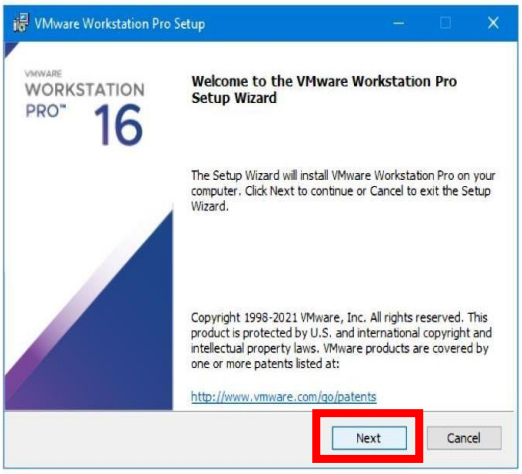
Instalación de VMware Workstation Pro 16

Nota. Es recomendable ejecutar como administrador para que la aplicación haga cambios al ordenador según los requerimientos que necesite para su funcionamiento.

A continuación, comenzara el proceso y se describirán los detalles de instalación, la página web de este para revisar la patente del programa, y el asistente de instalación solicitara una confirmación para el proceso, se debe dar clic en el botón next, como se muestra en la figura 10.

Figura 10

Interfaz de bienvenida a VMware Workstation 16 Pro

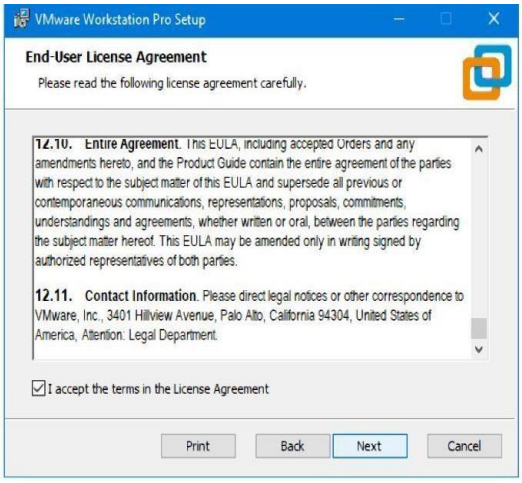


Nota. Confirmar y aceptar el proceso de instalación.

En la siguiente parte, se mostrará el acuerdo de licencia para el programa, el cual es muy importante leer, de esta forma por debajo del acuerdo una casilla se debe marcar para aceptar el acuerdo, y se debe dar clic en la opción Next. Como se muestra en la figura 11.

Figura 11

Aceptar términos y condiciones de licencia.



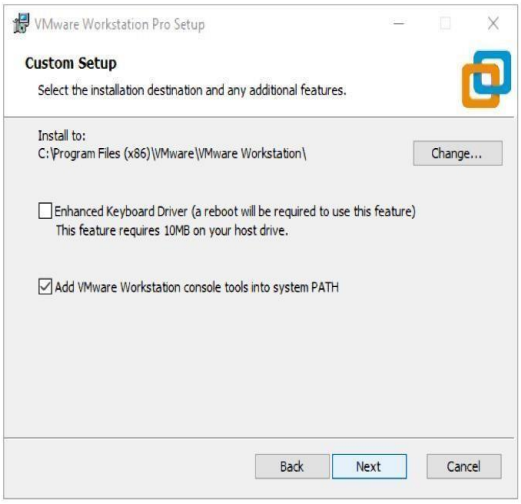
Nota. Se acepta los términos de uso impuestos por los desarrolladores.

A continuación, se debe establecer el destino de instalación del programa, al igual que muchos programas es recomendable que la ruta que se muestra por defecto sea en la que se

instale VMware, y de igual manera se debe marcar la segunda para añadir las herramientas del sistema de virtualización, como se muestra en la figura 12.

Figura 12

Asignar la carpeta donde va a contener los archivos del programa

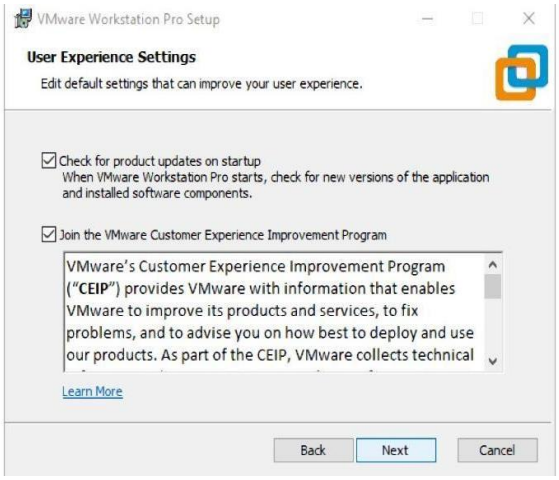


Nota. Se escoge la ubicación para almacenar los archivos de las máquinas virtuales.

Dos opciones se mostrarán una de ellas para revisar las actualizaciones del sistema y la segunda para permitir la “experiencia del usuario” al usar el programa, es recomendable que se seleccionen estas dos opciones como se muestra en la figura 13 y dar clic en next.

Figura 13.

Experiencias de usuario

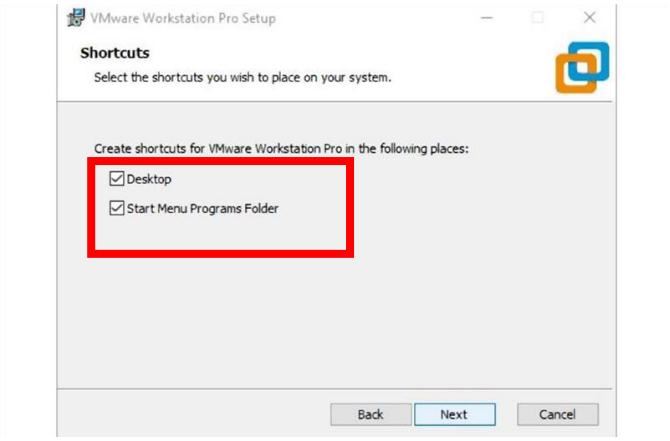


Nota. Aquí se debe escoger las dos opciones tanto como las actualizaciones y experiencia de usuario.

Para continuar se solicita escoger los atajos para el programa, se recomienda que las dos opciones se marquen para poder visualizarlos tanto en el escritorio como en el listado de programas del menú de inicio. Y se da clic en Next, Como se muestra en la figura 14.

Figura 14.

Añadir al escritorio y lista de inicio en Windows

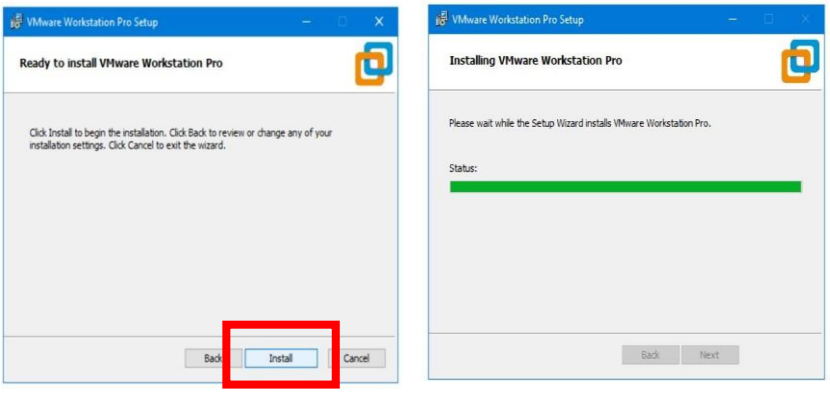


Nota. Se debe escoger el atajo para el listado del menú de Windows.

A continuación, la última ventana preguntará si todas las configuraciones son correctas y de no serlas se puede volver atrás con el botón “back”, de estar seguro se debe dar clic en Next, como se muestra en la figura 15 y el proceso de instalación comenzara donde una barra de progreso demostrara el porcentaje completado.

Figura 15

Confirmar que las configuraciones sean correctas

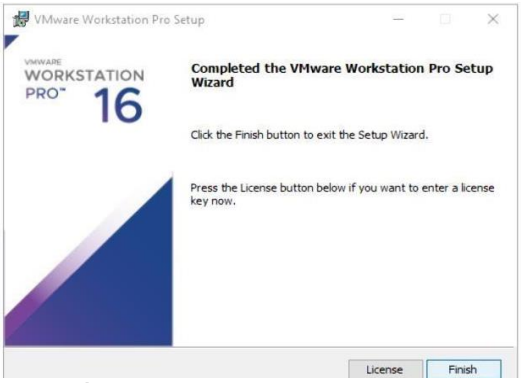


Nota. Una vez confirmado que las configuraciones estén correctas se da clic en install.

Después de unos 10 o 15 minutos el programa se habrá instalado correctamente y un cuadro de dialogo preguntará al usuario si tiene una licencia para el programa, para lo cual se puede seleccionar la opción “License”, y para finalizar el proceso dar clic en la opción Finish como se muestra en la figura 16.

Figura 16

Instalación finalizada

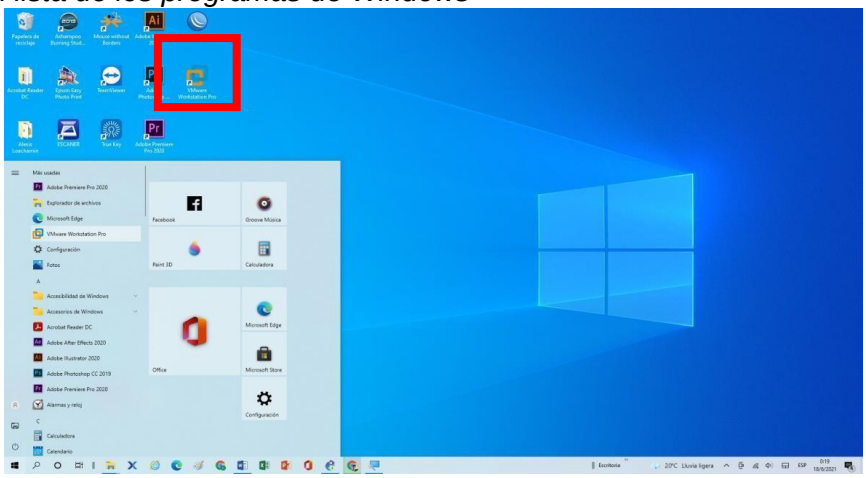


Nota. Se debe escoger la opción Finish para finalizar con la instalación.

Para finalizar esta parte, se podrá visualizar al programa instalado en el menú de inicio de Windows 10 y de igual forma en su propio icono en el escritorio de la computadora, como se muestra en la figura 17.

Figura 17.

VMware en lista de los programas de Windows



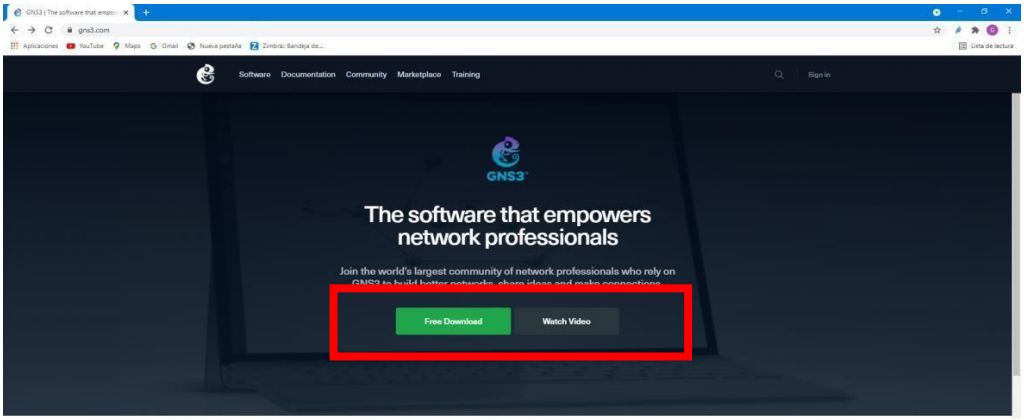
Nota. Aquí se observa el icono en la lista de todos los programas.

Instalación del Software GNS3

Primero descargar el instalador de GNS3, para esto dentro del navegador de preferencia se debe ingresar al siguiente link https://www.gns3.com/ asegurándose de que sea la página correcta y el sitio sea seguro, aparecerá la ventana que se muestra en la figura 18, donde se muestra un pequeño concepto de GNS3, por debajo de esto habrá dos opciones donde en el botón verde se podrá descargar el instalador o a su vez ver un tutorial de instalación en el botón gris de la izquierda.

Figura 18

Página de descarga de GNS3

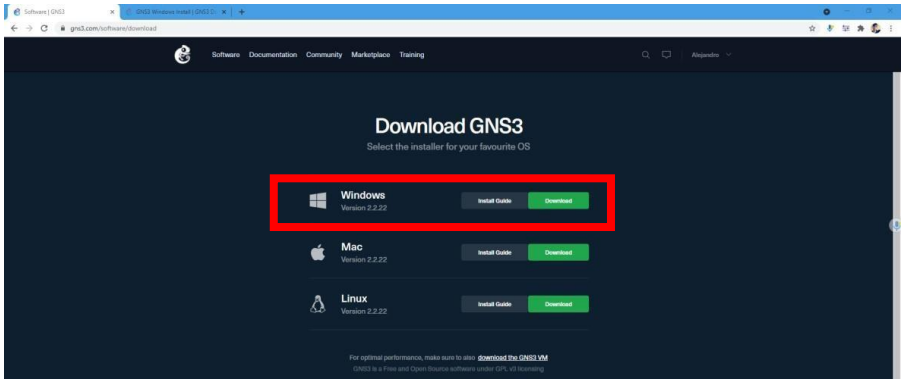


Nota. Aquí se debe crear una cuenta y contraseña para poder descargar el programa.

Al momento de dar en el botón verde “Free Download” se direccionará hacia la sección de descarga del software, una interfaz como la que se muestra en la figura 19, en donde existen diferentes opciones para el instalador dependiendo de las características de la computadora donde se vaya a instalar. Al igual que en la figura anterior existirán 2 opciones, una de ellas es un manual de instalación propio de GNS3 por otro lado se encuentra la opción para la descarga del instalador. Siendo Windows el sistema por preferencia de clic en el botón Download, y también en una nueva pestaña la “guía de instalación”.

Figura 19

Escoger el sistema operativo de Windows

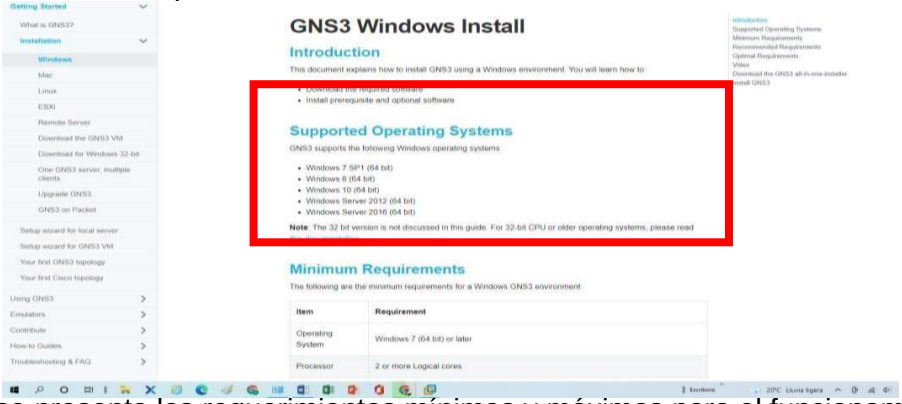


Nota. Es donde se recomienda que escoja el sistema operativo ya sea de Linux, Mac y Windows, dar clic en descarga.

Previo a instalar el programa es necesario comprobar algunos documentos que describen los requisitos y herramientas con los que cuenta GNS3 para lo cual en la ventana “Install Guide” que se abrió previamente se mostrará una página como en la figura 20, donde se explica entre varias cosas, los sistemas de Windows compatibles para GNS3, por debajo de esto estarán algunos requerimientos mínimos para el funcionamiento del sistema.

Figura 20

Sistemas operativos compatibles con GNS3



Nota. Aquí se presenta los requerimientos mínimos y máximos para el funcionamiento correcto del software GNS3 tanto como memoria, disco duro.

Los requerimientos mínimos para GNS3 son contar con un sistema operativo Windows 7, un procesador de 2 núcleos o más, tener habilitado el proceso de virtualización de la computadora, contar con una memoria RAM de 4 GB, un almacenamiento disponible de 1GB en el disco duro. Al igual que en procesos e instalaciones de otros programas mientras mejor sea la maquina física mejor funcionara el programa, en las figuras 21, 22 y 23. se muestran los requisitos mínimos, recomendables y óptimos para GNS3.

Figura 21

Requerimientos mínimos de GNS3

Nota. Muestra que es compatible con ordenadores, desde el Windows 7.

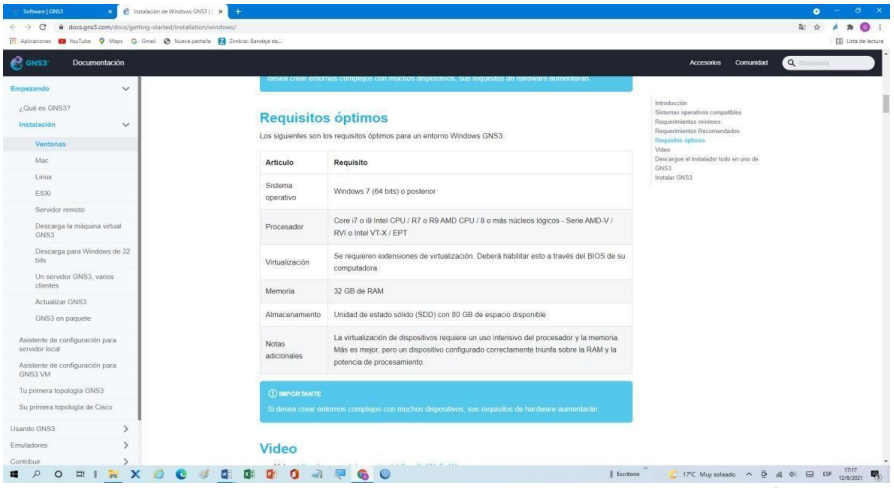
Figura 22

Requerimientos recomendados

Nota. Se recomienda contar memoria RAM de 8GB y un 1TB de disco duro.

Figura 23

Requerimientos Óptimos

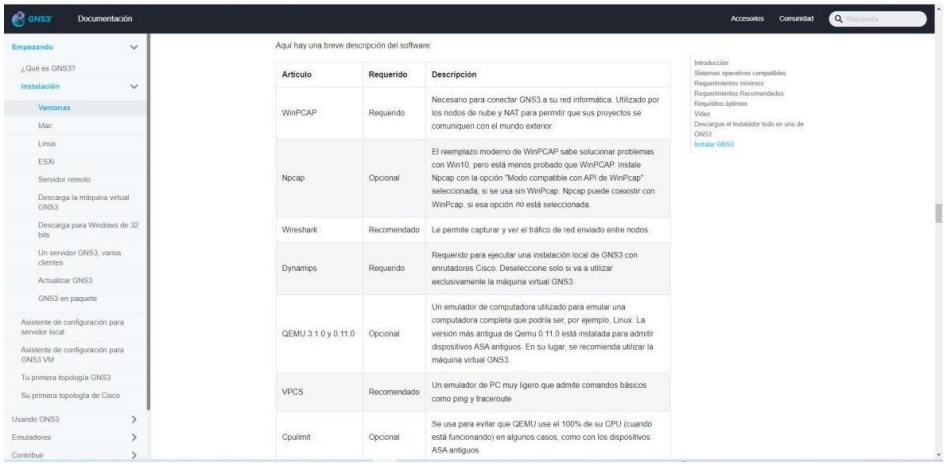


Nota. Es recomendable tener 32 GB de memoria RAM, un procesador de séptima generación con 8 núcleos, y un 1TB de disco duro.

GNS3 requiere de softwares alternos que permiten la administración y configuración de las redes dentro del simulador, que se muestran en la figura 24 y 25. programas con los cuales el instalador GNS3 está incorporado.

Figura 24

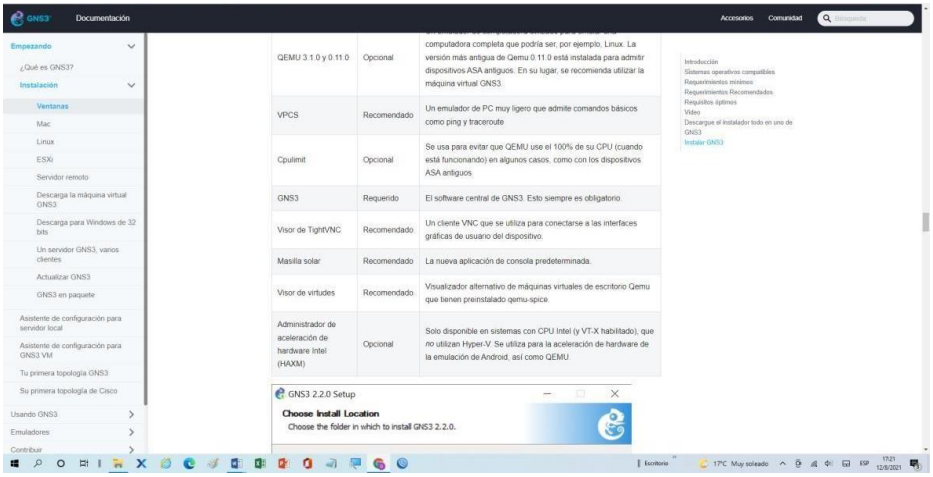
Componentes para GNS3



Nota. Está compuesta por programas de red entre otros.

Figura 25

Aplicaciones con descripción

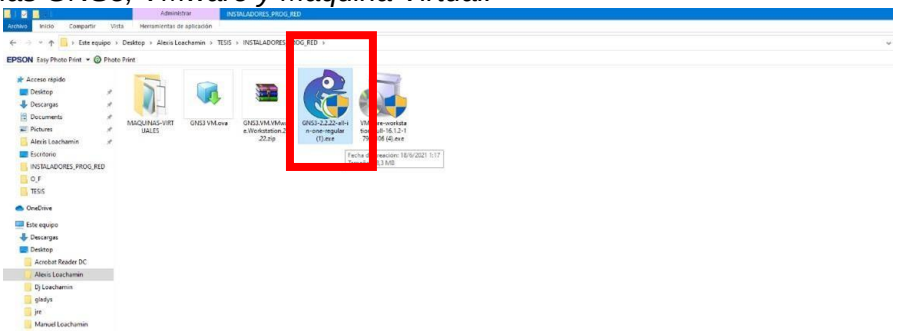


Nota. Aquí se presentan los programas recomendados, opcional, requerido.

Una vez descargado todos los componentes, se procede a la instalación, es importante verificar que los archivos sean correspondientes a las últimas versiones para evitar problemas de compatibilidad y mantenerlos en una carpeta específica, como se muestra en la figura 26.

Figura 26

Programas GNS3, VMware y Máquina Virtual.



Nota. Aquí se muestra la carpeta que contiene los instaladores de GNS3, VMware y Máquina Virtual de GNS3.

Se procede a ejecutar el instalador de GNS3 al dar clic derecho y ejecutar como administrador, una pequeña interfaz se abrirá como en la figura 27, el cual nos da la bienvenida a la guía de instalación del software.

Figura 27

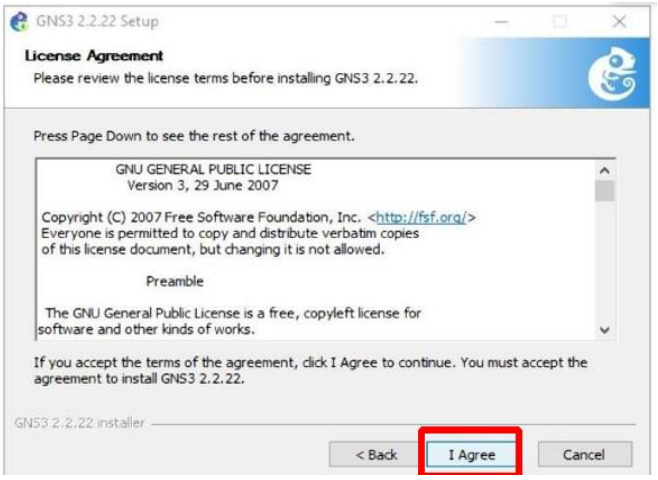
Ejecutar el instalador de GNS3.

Nota. Se procede a seguir los pasos sencillos al dar clic en la palabra Next.

A continuación, se presentará el acuerdo de licencia, el cual es gratuito, se puede verificar la versión en la parte inferior del recuadro y se procede a dar clic en “I agree” como se muestra en la figura 28.

Figura 28

Agregar en forma de icono al escritorio.

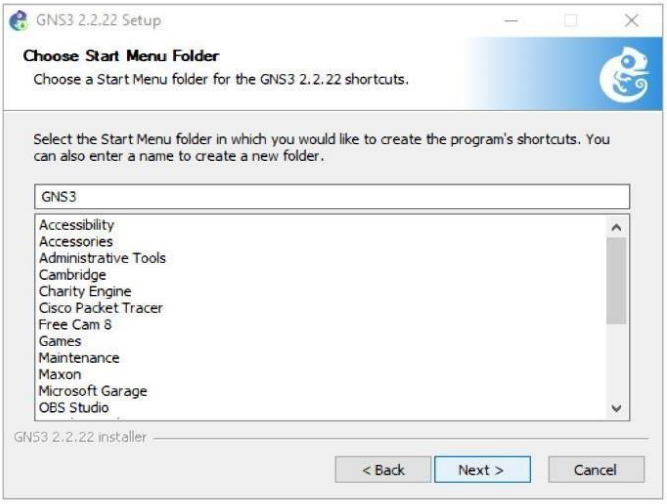


Nota. Se agrega el icono al escritorio y a la lista de todos los programas.

Realizado esto, el programa solicitará que se selecciona los espacio donde se instalarán los atajos del software, esto se lo puede dejar por defecto o de igual manera escoger una carpeta específica para su instalación, una vez escogida la carpeta se da clic en Next, como se muestra en la figura 29.

Figura 29

Carpeta de archivos GNS3

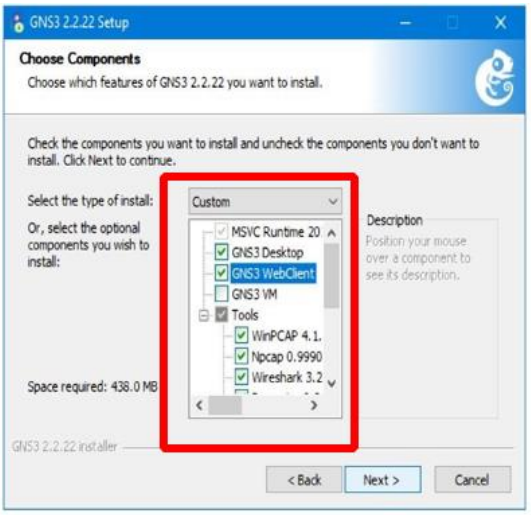


Nota. Se permanece con valores por defecto.

En el siguiente paso se detallan todos los componentes que GNS3 incorpora y que se especificó con más detalle en las figuras 30, el simulador grafico (GNS3 Desktop), la interfaz web (GNS3 WebClient), la máquina virtual (GNS3 VM) y en el apartado de Tools, todas aquellas herramientas que permitan la administración de redes, en el caso de tener una de estas herramientas ya descargada o no se desea instalar basta con borrar la casilla marcada, como se muestra en la figura 30. Donde no se instalará la máquina virtual, puesto que esto se lo hará manualmente.

Figura 30

Custom y Tools de GNS3

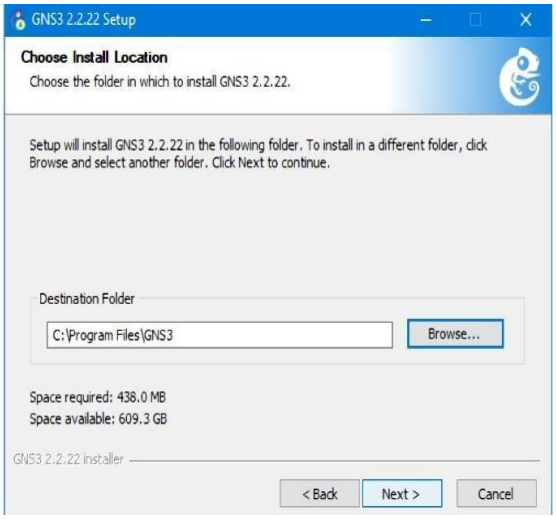


Nota. Aquí se debe dejar todas opciones señaladas por defecto.

A continuación, se solicitará que se escoja la carpeta de instalación de GNS3, de igual manera en la parte inferior se muestra cuanto es el espacio requerido para este proceso, Una vez que se haya establecido esto se da clic en next. Como se muestra en la figura 31.

Figura 31

Carpeta de destino de GNS3

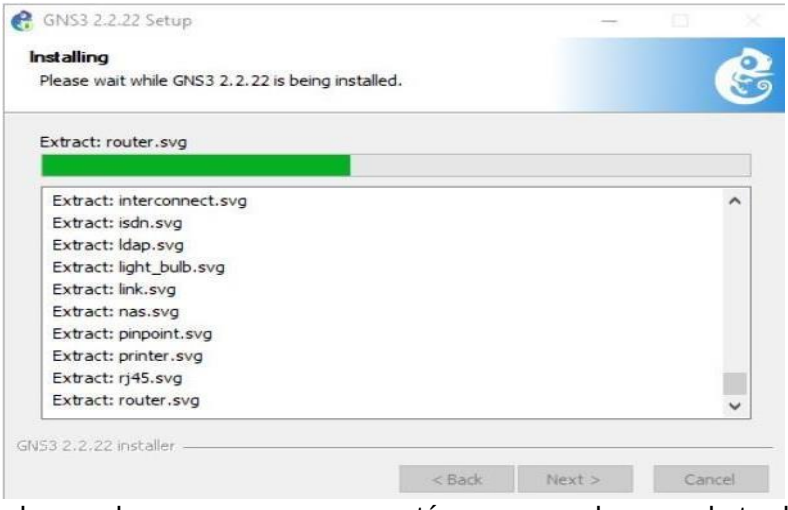


Nota. Se solicita escoger la carpeta de GNS3 para guardar los requerimientos de archivos.

Posterior a esto se comenzará con el proceso de instalación donde se detallará en una pequeña ventana los procesos que se están ejecutando, así como el avance de la instalación, tal y como se muestran en la figura 32. Este proceso puede tardar de 10 a 15 minutos.

Figura 32

Proceso de instalación de GNS3

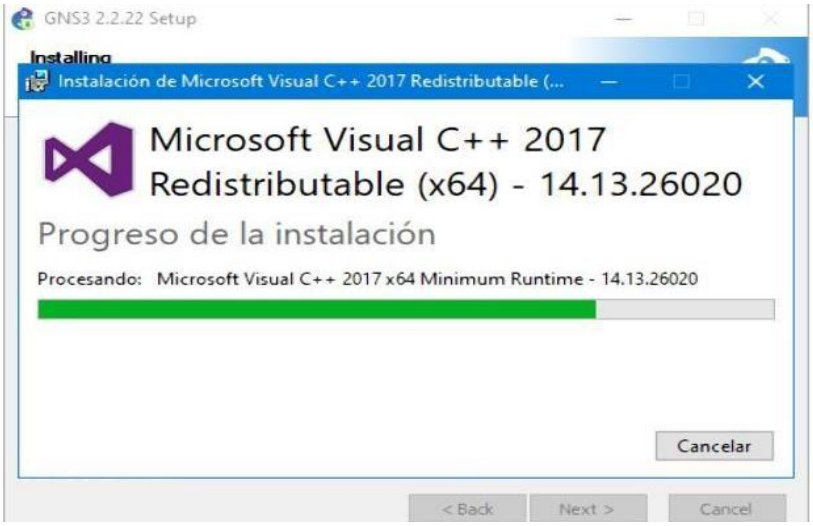


Nota. Aquí se observa los procesos que se están procesando y puede tardar un tiempo.

Durante el proceso irán apareciendo pequeñas interfaces de instalación las cuales son los componentes que GNS3 necesita para su funcionamiento, algunos de los mismos pedirán su propia confirmación de instalación como se muestran en las figuras 33 y 34, se debe leer el acuerdo de licencia de cada uno y dar clic en next o dependiendo del caso “I agree”

Figura 33

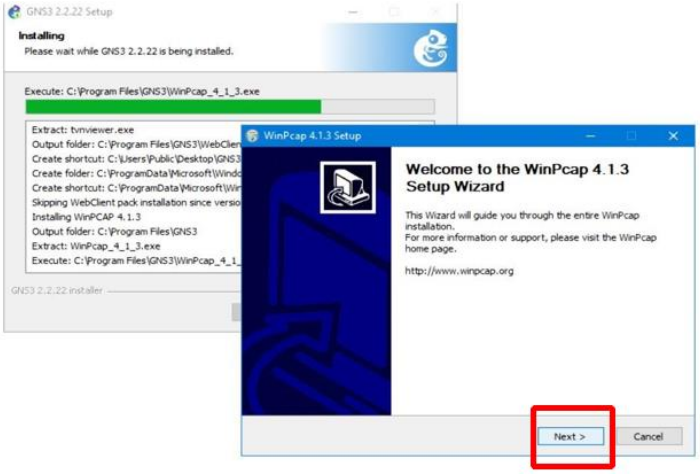
Instalación de Microsoft Visual C++ 2017



Nota. Aquí muestra el progreso de instalación.

Figura 34

Instalación de WinPcap versión 4.1.3

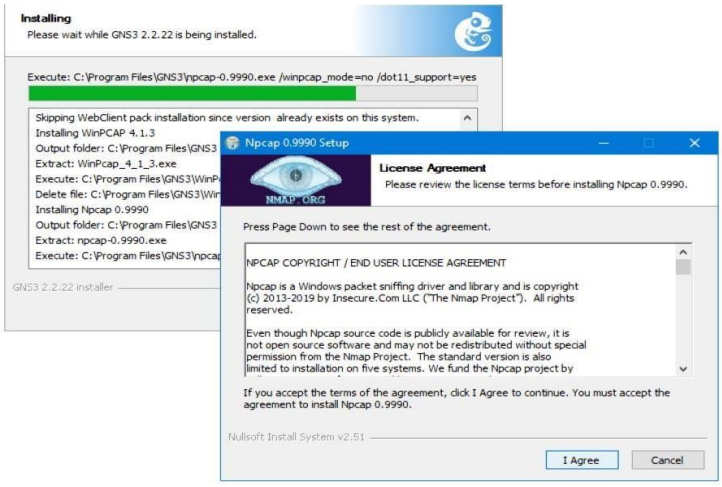


Nota. Con “I agree” se muestra el proceso de instalación y requerimiento de licencia.

Muchos de estos programas solicitaran que se llenen algunos campos como es el caso de “NpCAP” el cual es una librería que permite realizar la captura de paquetes en Windows. Como se muestra en la figura 35, se da clic en “I agree” y luego se debe seleccionar “support raw 802.11 traffic…” Como se muestra en la figura 36

Figura 3

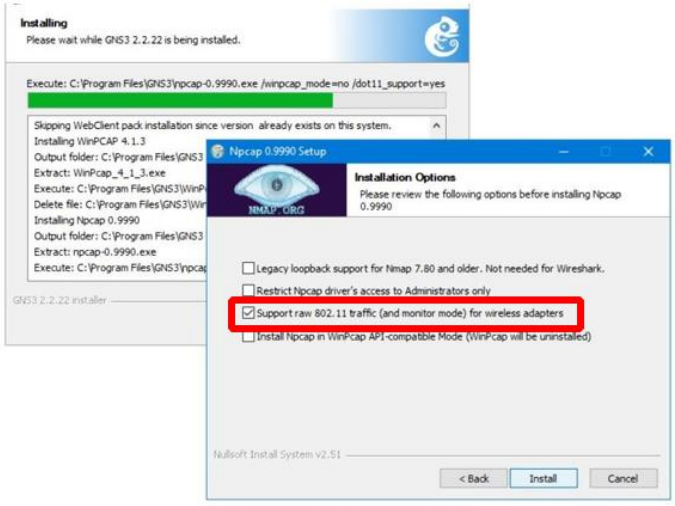
Instalación NpCap



Nota. Se observa la instalación y la respectiva licencia.

Figura 36

Proceso de instalación de NpCap.

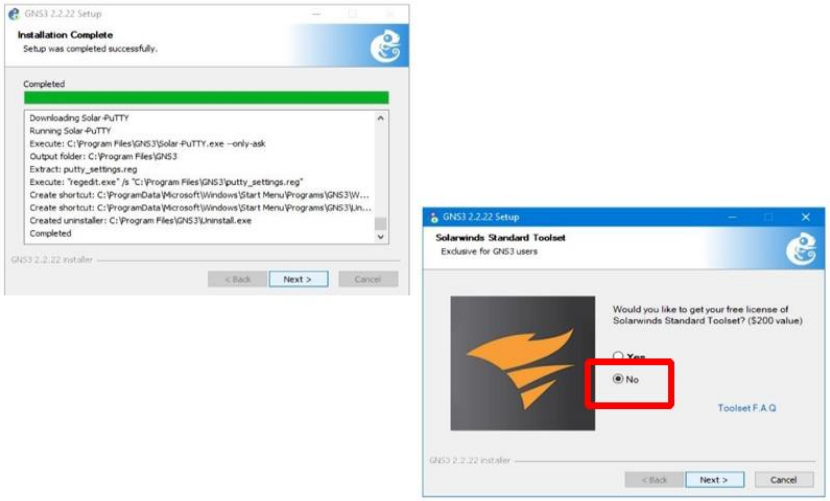


Nota. Aquí se marca la tercera opción de support raw 802.11 traffic.

Es muy posible que se emita la instalación para el programa Solar Winds como se muestra en la figura 37, En ese último cuadro de instalación se pide marcar la casilla para obtener la licencia del programa la cual tiene un valor de $200.

Figura 37

Instalación de Solar Winds.



Nota. Aquí se muestra el programa de instalación completado, en la siguiente imagen se no comprar la licencia.

A continuación, a esto se mostrará una ventana en la cual se notificará la instalación exitosa del programa y una casilla para iniciar el programa, se desmarca esta opción y se presiona en el botón Finish, como se muestra en la figura 38.

Figura 38

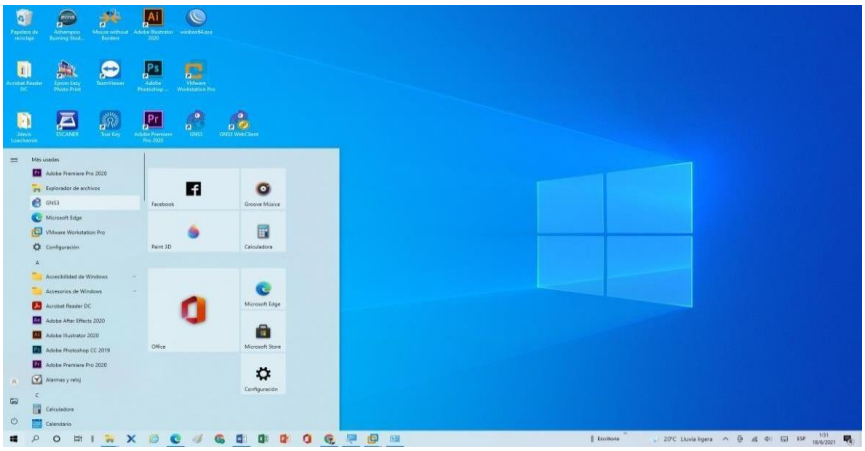
Instalación completada de GNS3

Nota. Aquí se aprueba la instalación.

Para abrir el programa, se lo podrá encontrar en uno de los iconos del escritorio o a su vez entrando al menú de inicio de Windows 10 en la lista de programas añadidos recientemente como se muestra en la figura 39.

Figura 39

Icono añadido al escritorio y lista de todos los programas.

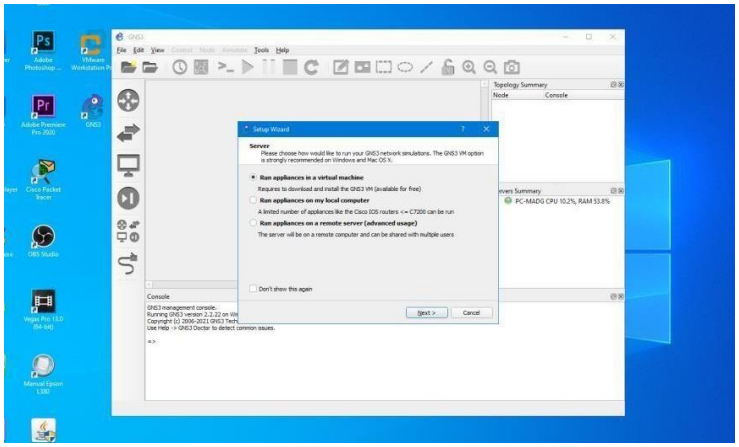


Nota. Se muestra los iconos en el escritorio y en la lista de programas.

Uno de estos iconos es la interfaz gráfica de GNS3 para el simulador de redes, y el otro es la interfaz web de GNS3, por el momento se dará doble clic en el icono de GNS3 y siendo la primera vez que se abre el programa una ventana como la que se muestra en la figura 40 aparecerá.

Figura 40

Corrido de GNS3

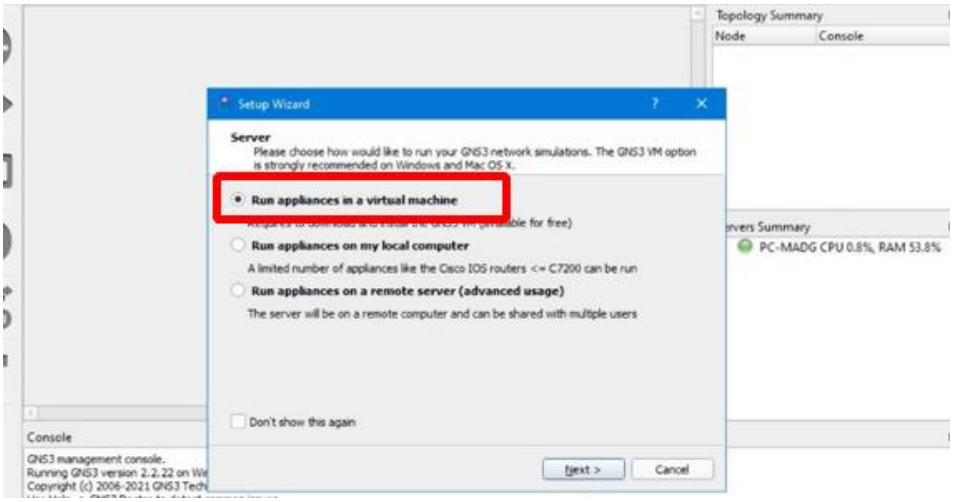


Nota. Aquí se presenta el corrido automático del programa GNS3.

Al ser la primera vez en abrirse el programa un cuadro de dialogo con opciones pedirá que se escoja donde ejecutar los accesorios para GNS3, se marca la primera casilla con la opción “Run appliances in a virtual machine” Marcada las opciones se da clic en la opción NEXT como se muestra en la figura 41.

Figura 41

Run Appliances



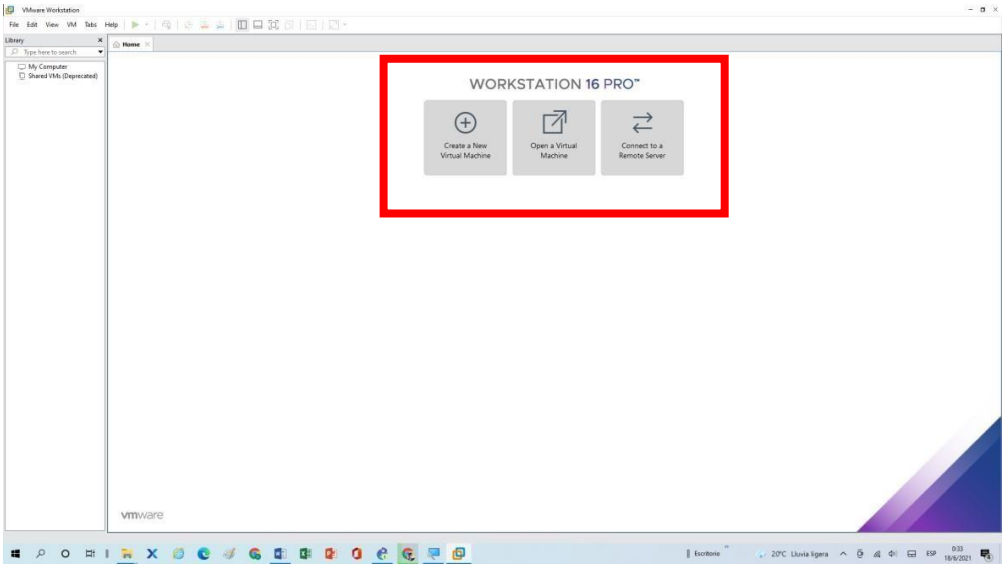
Nota. Primera muestra dentro de GNS3.

Instalación de la máquina virtual de GNS3

Al ejecutar el programa VMware Workstation se mostrará una interfaz como en la figura 42, en la parte superior se observa la barra de opciones, en la cual se puede añadir equipos, configuraciones, herramientas de conexión entre otras opciones, por debajo de esta barra al lado izquierdo esta la librería de donde una vez instaladas las máquinas virtuales se mostrarán en forma de lista. Y al lado derecho la interfaz muestra 3 opciones principales para abrir, crear máquinas virtuales y conectarse a un servidor.

Figura 42

Interfaz gráfica de VMware Workstation 16 Pro

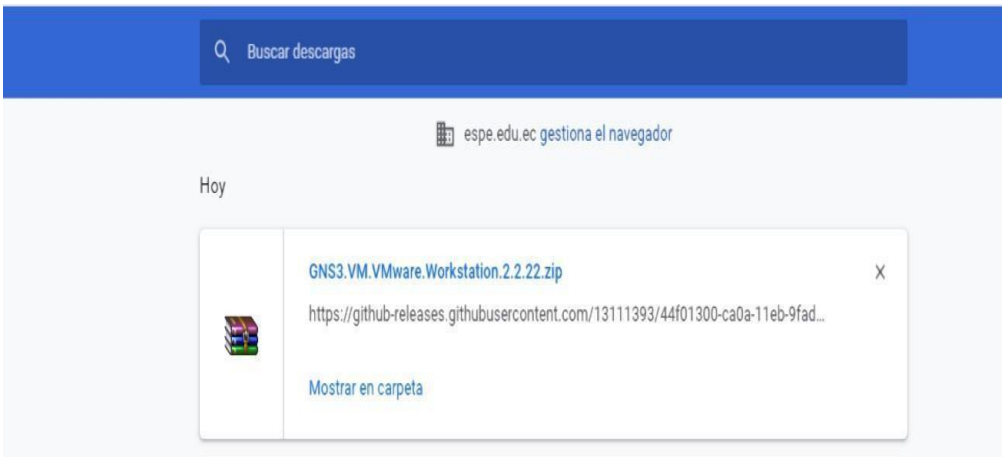


Nota. Aquí se muestra donde se puede crear nuevas máquinas virtuales, abrir maquinas descargadas como es el caso de la máquina virtual de GNS3.

Previo debe descargarse la máquina virtual de GNS3 que se mostró previamente, como parte de los componentes principales, que se muestran en la figura 43. Asegurándose de que los archivos estén en una carpeta especifica.

Figura 43

Descarga de la Máquina Virtual de GNS3.

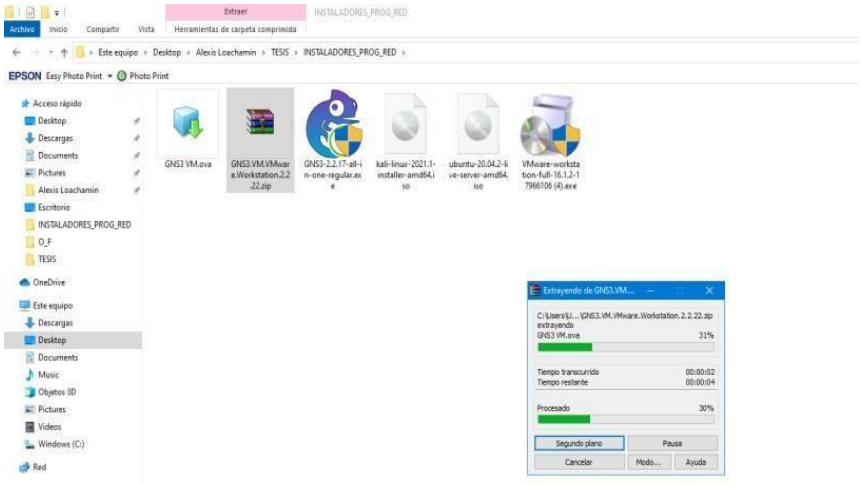


Nota. La descarga de la Máquina Virtual de GNS3 es formato RAR.

Posterior a esto, el archivo descargado es de tipo RAR por lo que es necesario que se extraiga el componente, al finalizar el proceso un pequeño archivo de formato ".ova" y un símbolo de cubo será la máquina virtual a instalar, como se muestra en la figura 44 y 45.

Figura 44

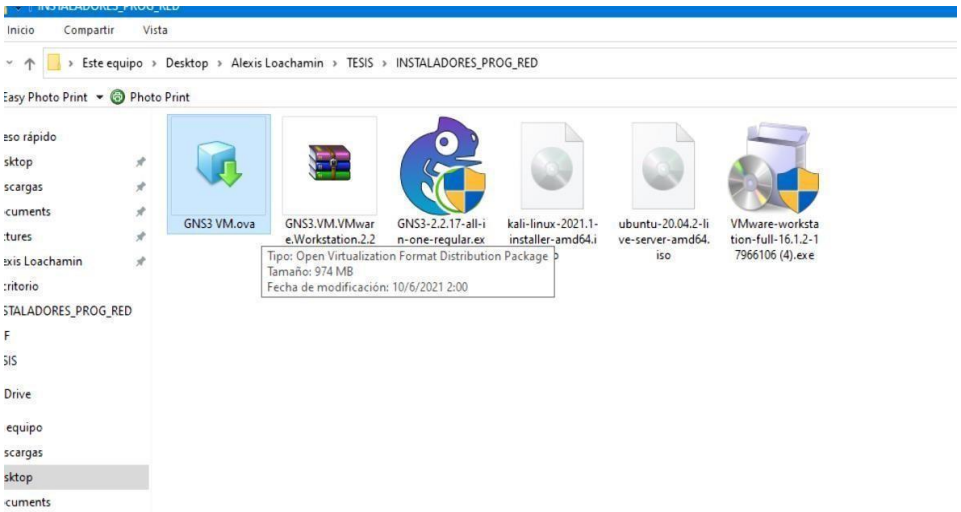
Extracción de archivo de Máquina Virtual.



Nota. Se muestra el porcentaje del archivo de Máquina Virtual.

Figura 45

Open Virtualization Format Distribution Package

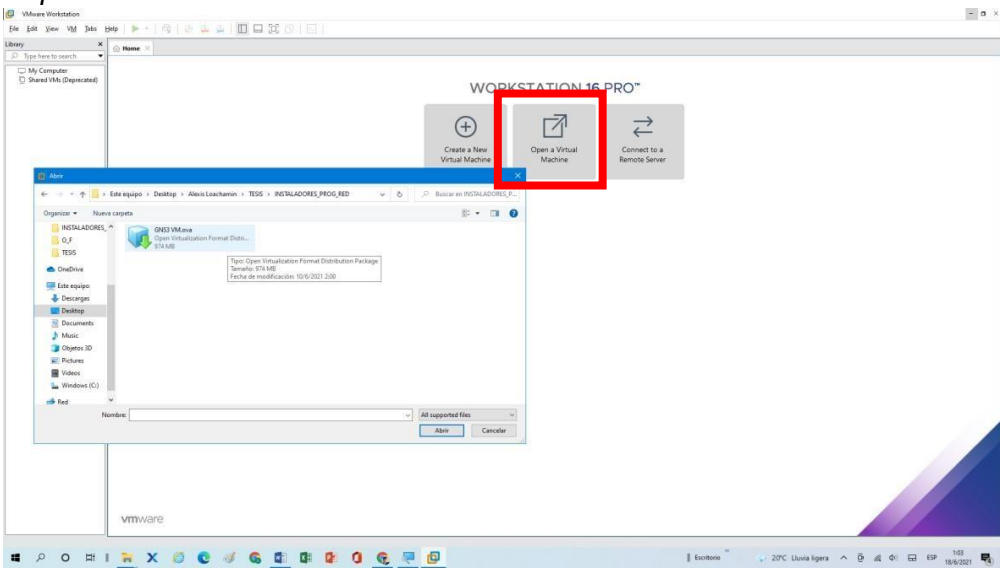


Nota. Muestra la Máquina Virtual descomprima lista para arrancar.

Para instalar la máquina virtual se debe dar clic en la opción “Open a Virtual Machine” de la interfaz de VMware y un explorador de archivos se abrirá para buscar el archivo de formato “.ova” y se da clic en abrir como se muestra en la figura 46.

Figura 46

Abrir la Máquina Virtual en VMware Workstation 16 Pro.

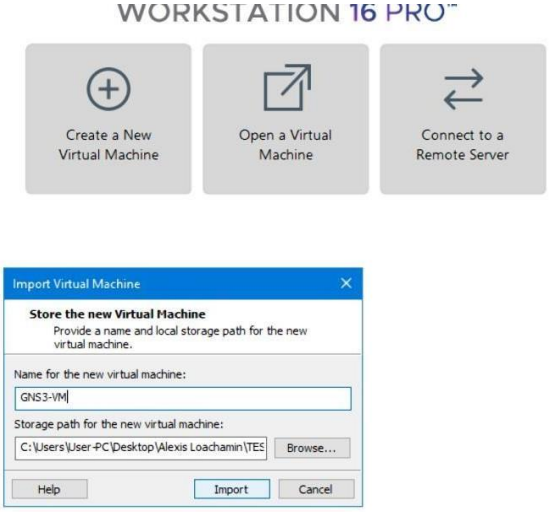


Nota. Muestra en la pestaña Open Virtual Machine sirve para abrir un archivo de este tipo ya existente.

A continuación de esto el programa detectará algunas especificaciones del archivo, así como su nombre y la ubicación, se puede cambiar el nombre con el que aparecerá la máquina virtual, una vez realizado esto se debe presionar en la opción Import. Como se muestra en la figura 47. Y el programa empezara con la instalación y se muestra el progreso en una barra de color verde como en la figura 48.

Figura 47

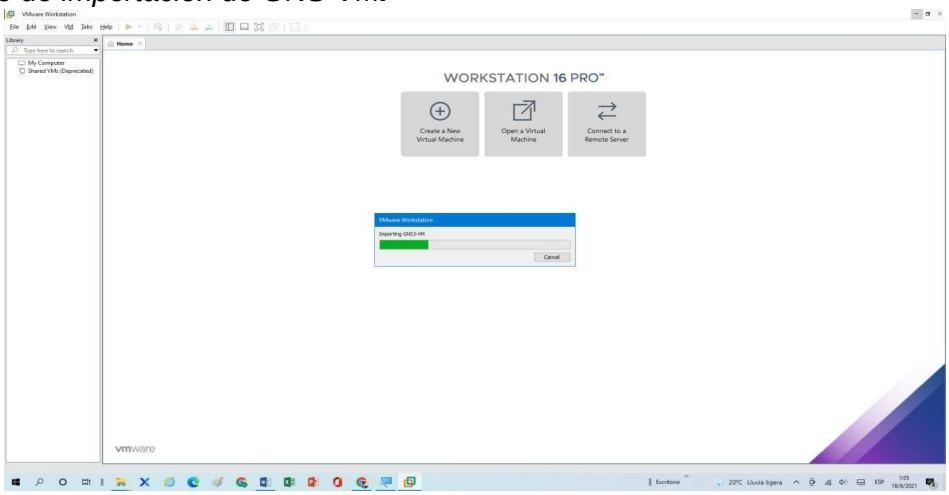
Importar Virtual Machine



Nota. Aquí se coloca el nombre de la máquina virtual, en la siguiente opción se elige el disco, carpeta.

Figura 48

Proceso de importación de GNS-VM.

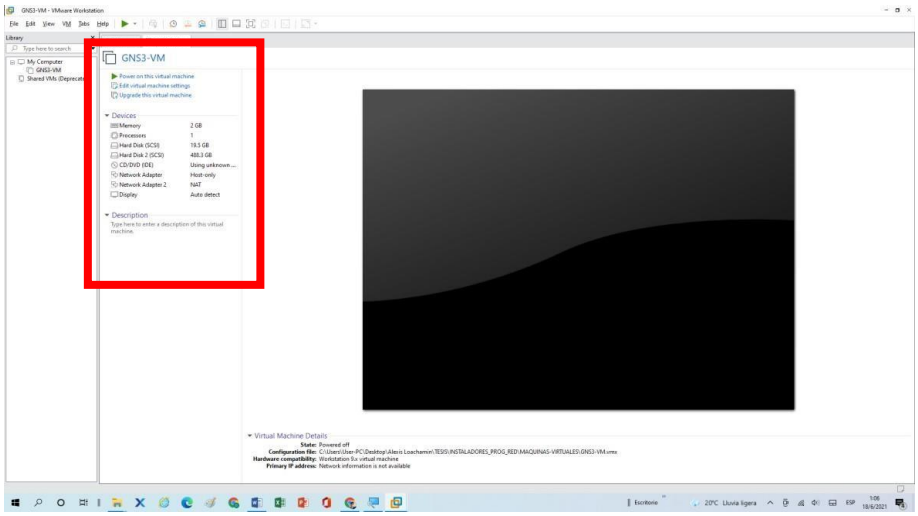


Nota. Es donde está especificado el avance de importación de GNS3-VM.

Siguiente a esto una interfaz aparecerá la cual simularía el aspecto de una maquina física además de que se describe algunas características de la misma en el costado izquierdo, como se muestra en la figura 49.

Figura 49

GNS3-VM con especificaciones similares a máquina física.

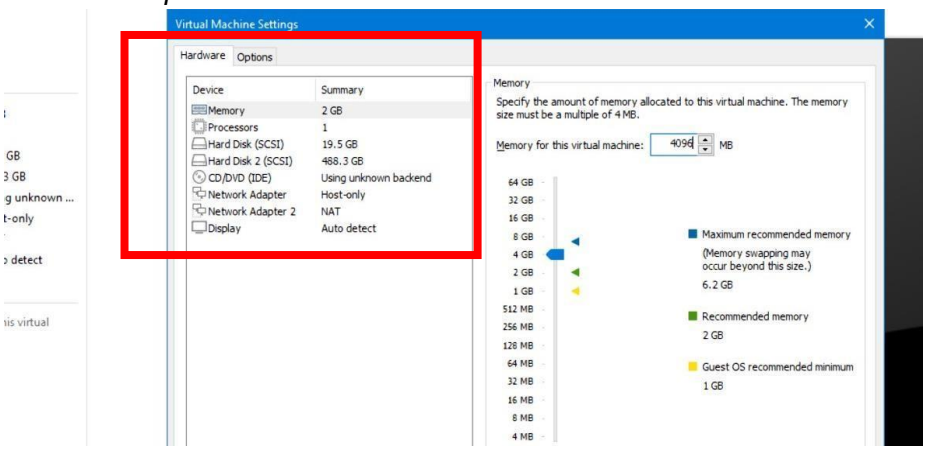


Nota. Se muestra la cantidad de memoria RAM, procesador, adaptador de red.

Se debe realizar un cambio ingresando a la opción “edit virtual machine settings” en la cual se mostrará ciertas configuraciones se debe aumentar la memoria de la máquina virtual, en el apartado Memory como se muestra en la figura 50, se encuentra en un valor de 2GB, si es posible se debe aumentar este valor, dependiendo de la cantidad de memoria que la maquina física tenga. Para el ejemplo se aumentará al doble este valor, ya que la maquina física cuenta con una memoria RAM de 8GB.

Figura 50

Especificaciones máquina

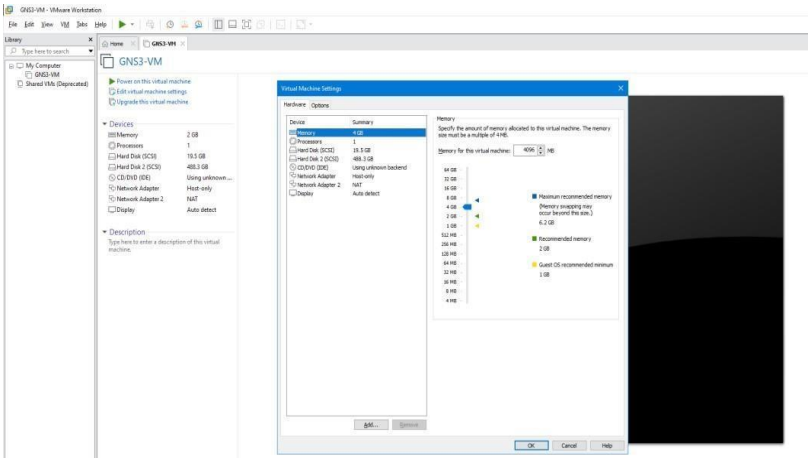


Nota. Se muestra la cantidad de memoria, procesador, adaptador de red.

Y para guardar los cambios bastará con hacer clic en otro apartado de las configuraciones y se debe evidenciar como en el listado principal de la izquierda la memoria debe mostrar un valor de 4 GB, como se presenta en la figura 51. Y para salir de la ventana se debe dar clic en “OK”.

Figura 51

Guardar cambios.

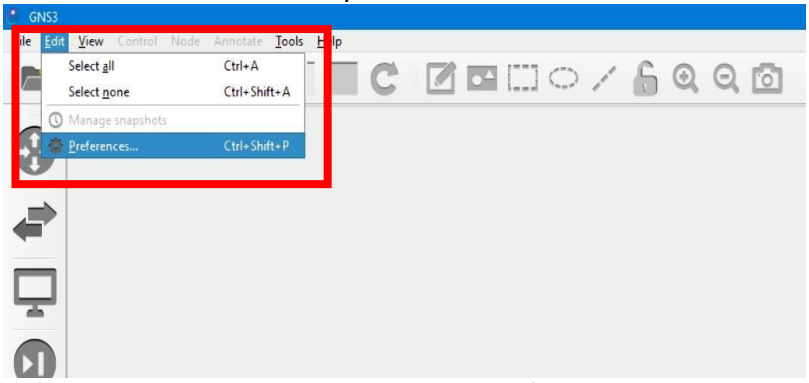


Nota. Se puede cambiar la cantidad de memoria RAM.

A continuación, se conectará la máquina virtual de GNS3 con la interfaz gráfica, para realizar esto se debe ubicar la opción EDIT en la parte superior izquierda de la interfaz del programa GNS3, donde un pequeño menú se desplegará y se debe presionar en la opción “preference”, tal como se muestra en la figura 52.

Figura 52

Editar la conexión de GNS3 con su máquina virtual.

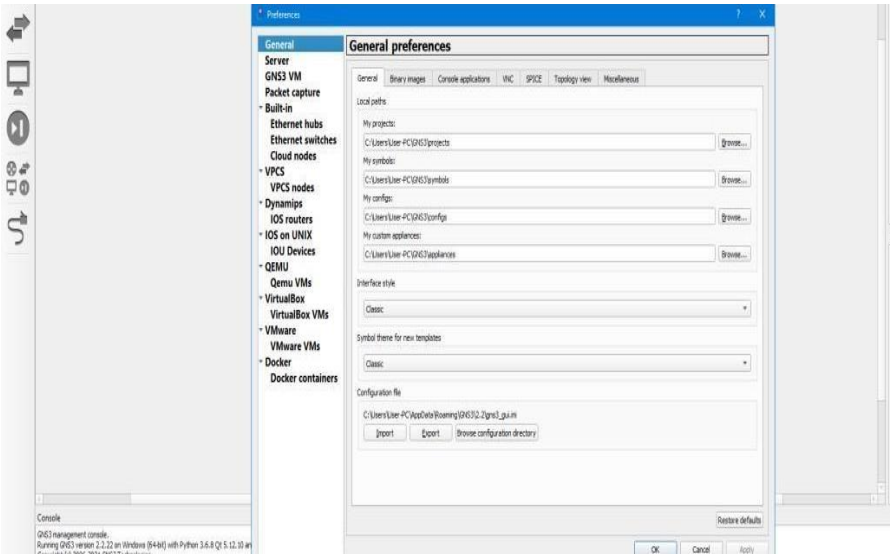


Nota. Esta opción presenta la forma de conectar la máquina virtual con GNS3.

Posterior a esto, como se muestra en la figura 53, Una ventana la cual es el espacio donde se puede configurar desde las imágenes IOS para los componentes de redes, dependiendo del sistema de emulación, las máquinas virtuales que se desean conectar, y otras opciones que integra GNS3

Figura 53

Preferences con la opción de General

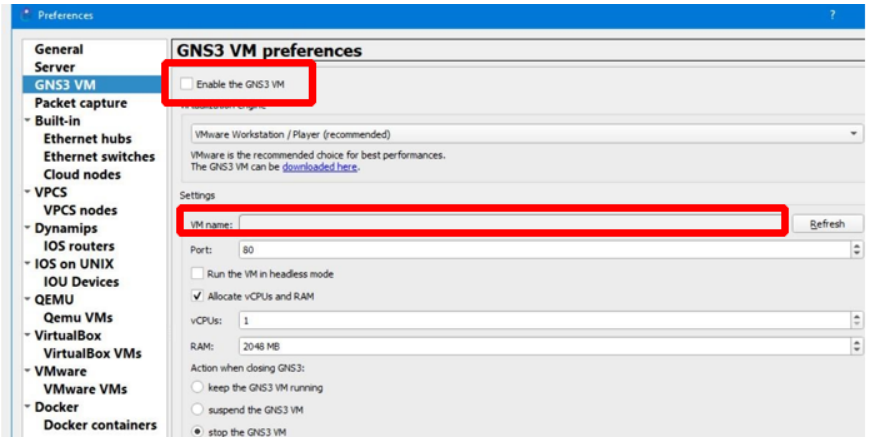


Nota. La ventana preferente administra el “controlador”.

Por el momento se debe dar clic en la opción del menú izquierdo con el nombre GNS3 VM donde como se muestra en la figura 54, primeramente, la casilla “ENABLE THE GNS3 VM” debe estar desmarcada, por otro lado, el virtualizador por defecto debe mostrar VMware Workstation y debajo de eso se encontrará una barra que por el momento debe estar vacía.

Figura 54

GNS3 VM preferences

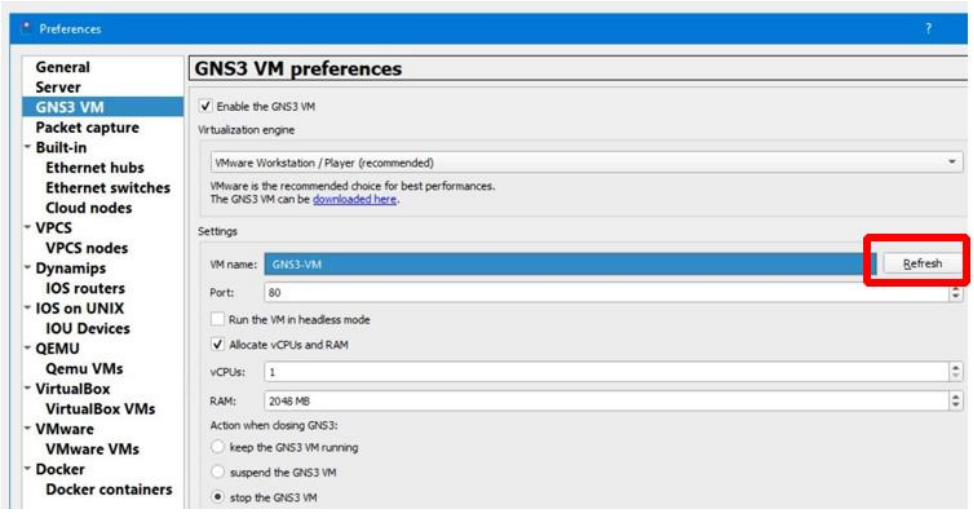


Nota. Aquí existe un puerto, VM name, settings, cantidad de memoria.

Si se presiona el botón refresh del lado derecho el listado de máquinas virtuales disponibles se actualizará y se debe mostrar el nombre con el que se guardó la máquina virtual de GNS3 en VMware, como se muestra en la figura 55 se selecciona la maquina correspondiente, y se marca el casillero superior “Enable the GNS3 VM” para habilitar la máquina virtual al momento de encender el programa GNS3.

Figura 55

Habilitar la máquina virtual “GNS3 VM”



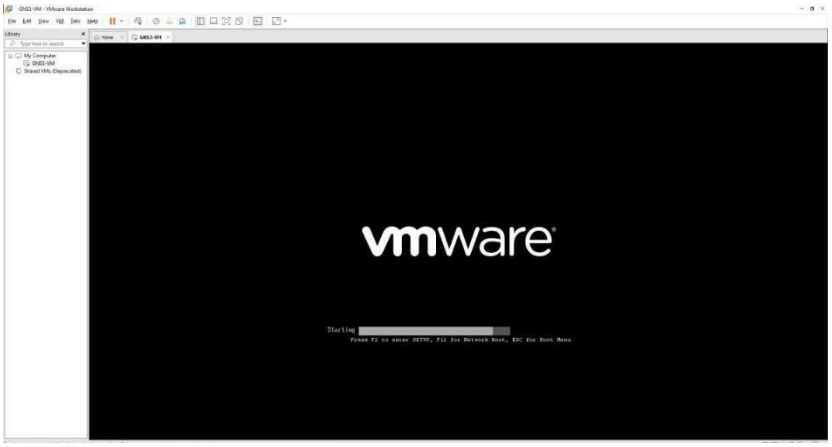
Nota. Se habilita por medio del checkbox “enable the GNS3 VM”

Realizado lo anterior, automáticamente el programa VMware ejecutara la máquina virtual de GNS3, si es necesario después de haber guardado los cambios realizados previamente cerrar todo y reiniciar el equipo, al momento de iniciar el simulador de redes GNS3

también debe prenderse su respectiva máquina virtual en VMware como se muestra en la figura 56.

Figura 56

Arranque de la Máquina Virtual GNS3 VM

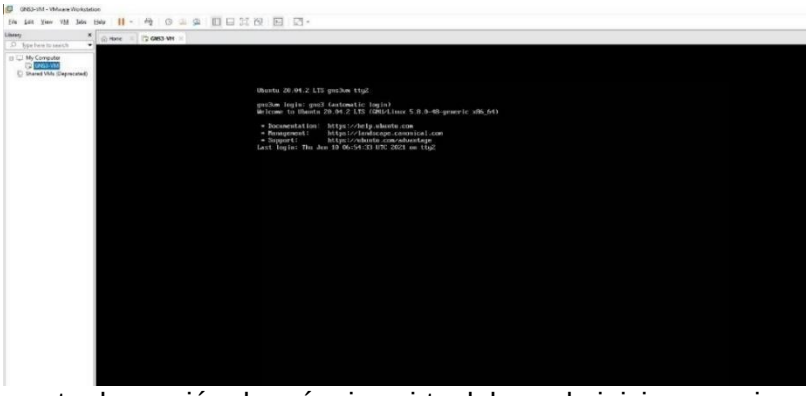


Nota. Se muestra como carga la Máquina Virtual de GNS3.

Una vez que la máquina virtual se haya encendido, un pequeño proceso de instalación comenzara al cual no se debe digitar nada, solo se muestran datos de la máquina virtual, como se muestra en la figura 57.

Figura 57

Versión de Ubuntu Linux



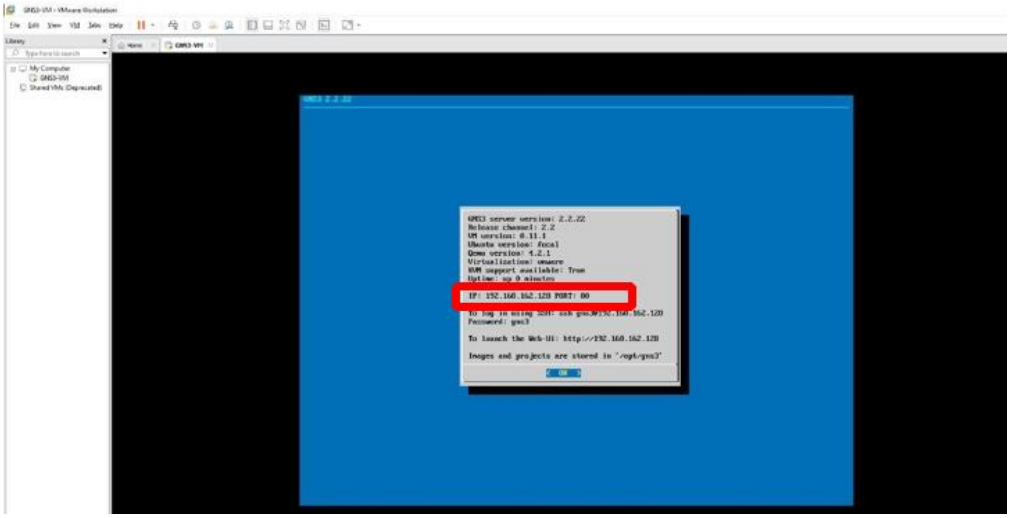
Nota. Se muestra la versión de máquina virtual, hora de inicio, usuario, etc.

Finalmente, después de unos 5 minutos se mostrará una pequeña pantalla azul donde se muestra la versión de la máquina virtual de GNS3 instalada; debe mostrarse también una

dirección IP la cual es la dirección que la máquina virtual ha recogido a partir del adaptador de red de la maquina física, como se muestra en la figura 58.

Figura 58

Dirección IP servidor Ubuntu Linux

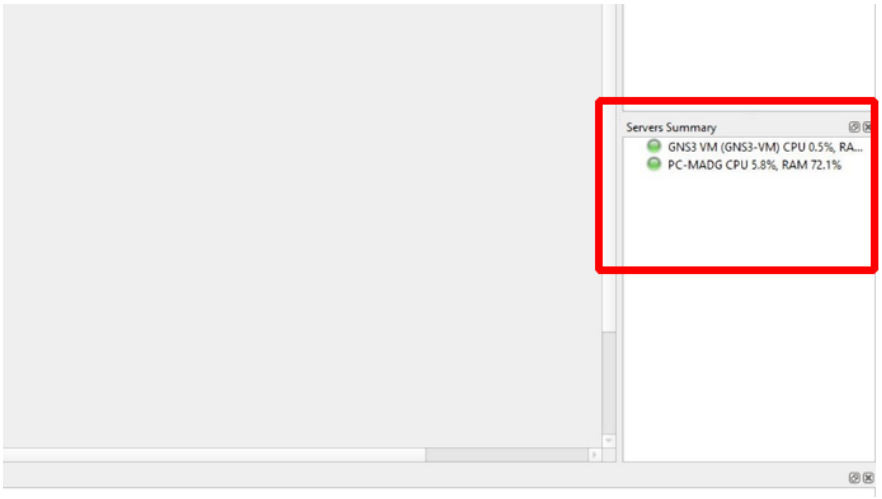


Nota. Arranque de máquina virtual de GNS3 con IP, puerto.

Finalmente, dentro de la interfaz gráfica de GNS3 se mostrará en la parte derecha un pequeño listado acerca de los servidores que se están ejecutando al momento de trabajar en GNS3. En las figuras 59, se puede evidenciar que la conexión es correcta hacia la máquina virtual puesto que tiene un indicador de color verde, además de que se muestra cuanto es porcentaje de Ram y CPU que está usando dicha máquina virtual y la maquina física.

Figura 59

GNS3 VM preferences



Nota. Ya se visualiza encendido la Maquinva virtual, cantidad de memoria y procesamiento.

Funcionamiento del simulador GNS3

Funcionamiento de GNS3(Interfaz de trabajo)

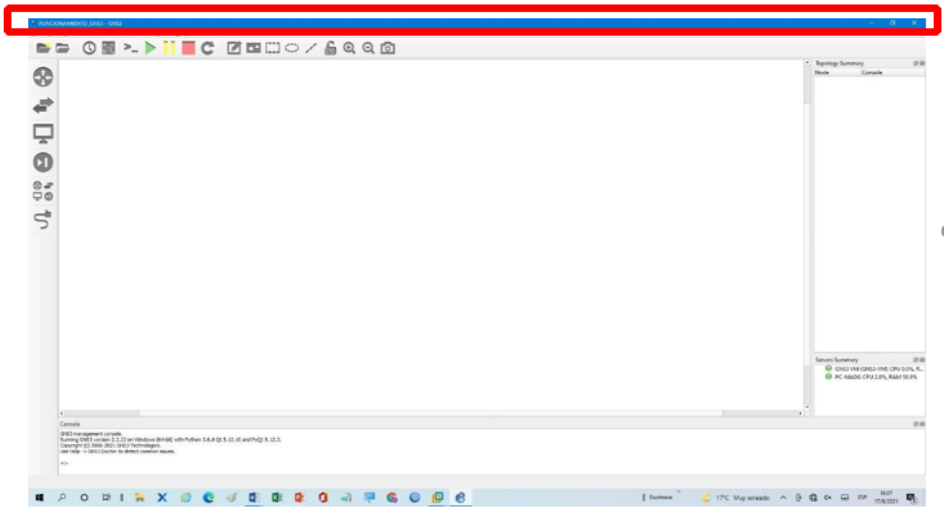
GNS3 permite la simulación de varios dispositivos usados en redes de datos y telecomunicaciones, construyendo topologías y arquitecturas de red complejas para su estudio y administración.

Primeramente, se va a describir la interfaz de trabajo del simulador y las principales opciones con las que cuenta.

La interfaz con la que trabaja GNS3 es minimalista y óptima para cualquier usuario, como se muestra en la figura 60, en la parte superior se encontrará el nombre con el cual el proyecto de GNS3 se ha creado y en la esquina derecha los botones de minimizar, maximizar y cerrar el programa, típicos en cualquier interfaz visual.

Figura 60

Interfaz de trabajo de GNS3.

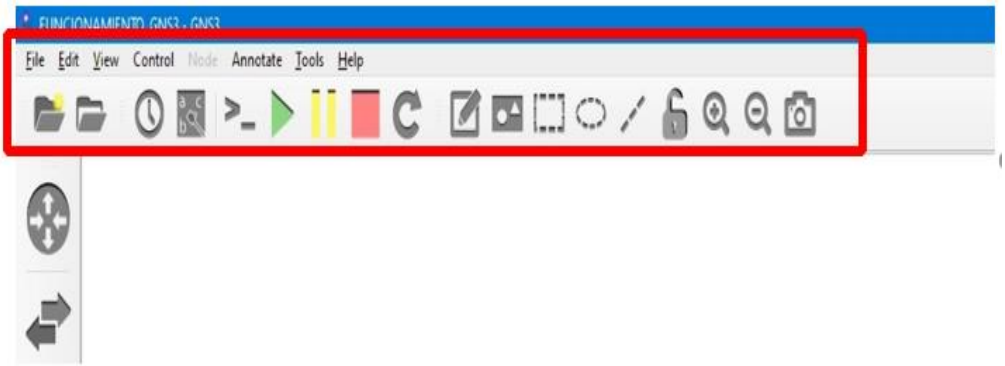


Nota. Aquí se muestran los datos del proyecto de GNS3.

Por debajo de la barra de título se establece la barra de opciones con algunas etiquetas como “FILE”, “EDIT”, “VIEW”, “CONTROL”, entre otros. Por otro lado, debajo de estas se tendrá la barra de herramientas, las cuales son muy útiles, y los símbolos ayudan a entender su funcionamiento. De igual forma en la tabla 1 se describen estos símbolos.

Figura 61

Barra de opciones



Nota. Aquí se muestran las imágenes de la barra de herramientas.

Tabla 1

Opciones en el menú de herramientas gns3

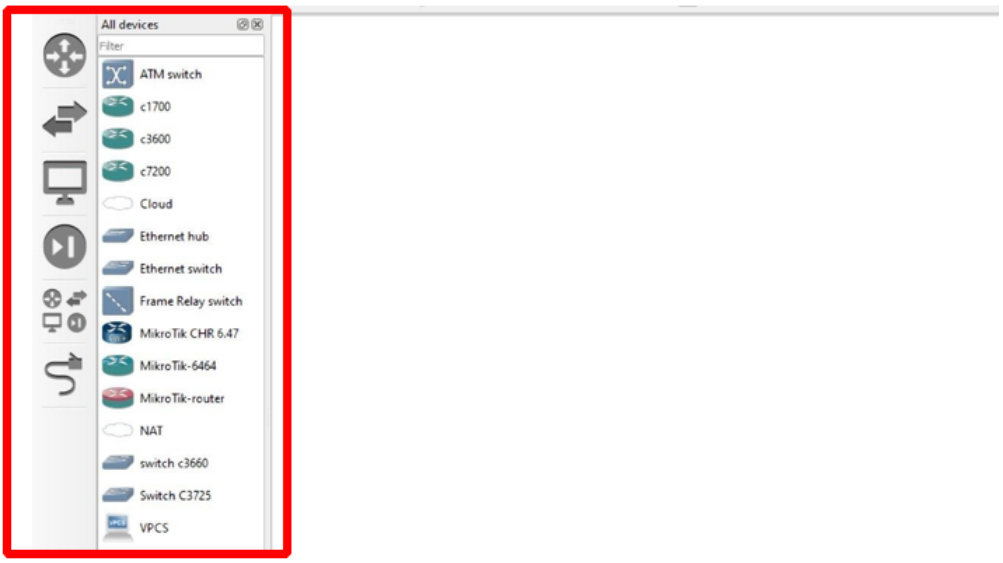
Símbolo	Descripción	Símbolo	Descripción
	Abrir proyecto en blanco		Añadir notas a la topología
	Abrir un proyecto realizado		Añadir imágenes a la topología
	“Snapshots” puntos de restauración		Dibujar un rectángulo en la topología
	Mostrar las etiquetas de los puertos		Dibujar un círculo en la topología
	Modo consola de todos los equipos		Dibujar una línea en la topología
	Encender todos los equipos		Bloquear el movimiento de los equipos
	Suspender todos los equipos		Zoom para acercar
	Apagar todos los equipos		Alejar zoom
	Reiniciar todos los equipos		Captura de pantalla

Nota. Esta tabla muestra la barra de herramientas de GNS3 para su versión “2.2.22” en el año 2021.

La barra lateral en el lado izquierda con símbolos muestra todos los equipos que se pueden emular en la red, donde se muestra tanto los equipos por defecto y los que se hayan instalado como en la figura 62.

Figura 62

Equipos para emulación



Nota. Se encuentran los dispositivos descargados.

Por debajo se encuentra un pequeño espacio con el nombre “console”, donde se puede configurar la red por comandos y se muestran notificaciones o mensajes de alerta, como se muestra en la figura 63.

Figura 63

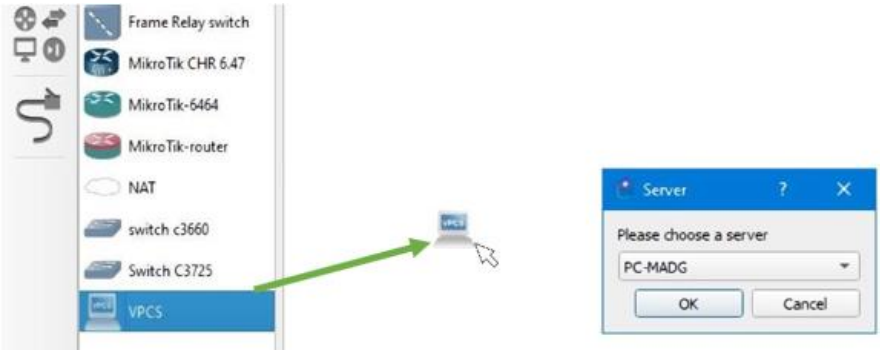
Espacio de nombre console

Nota. Aquí se configura las notificaciones y mensajes de alerta con comandos de muestra.

Para realizar topologías, primero, se selecciona el equipo a establecer en la red, se lo arrastra desde la barra de dispositivos y se lo suelta en el espacio del centro de la interfaz, un pequeño cuadro de dialogo preguntara al usuario si se desea emular el dispositivo en la maquina física o en la virtual, tal y como se muestra en la figura 64.

Figura 64

Selección del equipo para topología

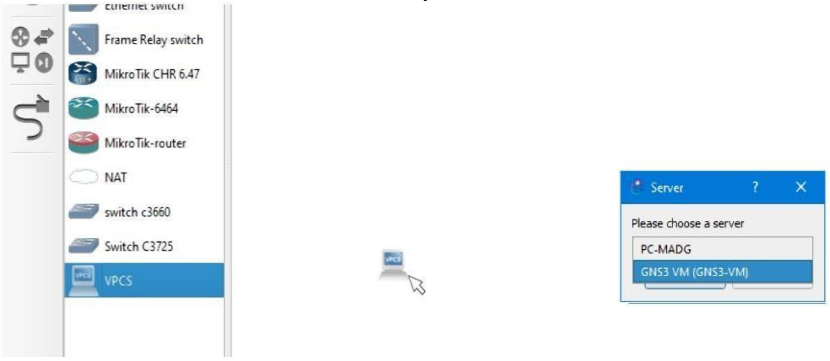


Nota. Se arrastra la imagen de VPCS sosteniendo el clic.

Dentro de las opciones para la emulación de los dispositivos debe estar tanto la maquina física y la máquina virtual que previamente se ha instalado en VMware, es preferible que los dispositivos se ejecuten dentro del servicio de la máquina virtual como se muestra en la figura 65.

Figura 65

Elección del servidor en este caso la máquina virtual de GNS3.



Nota. Al momento de arrastrar las VPCS se debe escoger GNS VM para no sobrecargar la memoria y proceso de maquina física.

Se realiza el mismo proceso con un ethernet switch, de tal manera que la topología debe quedar como se muestra en la figura 66, al lado derecho de la interfaz se encuentra el apartado “Topología Sumary” en el cual se describen en forma de lista todos los componentes que se encuentren en la red, si estos están prendidos o apagados y el modo de consola con el que cuentan.

Figura 66

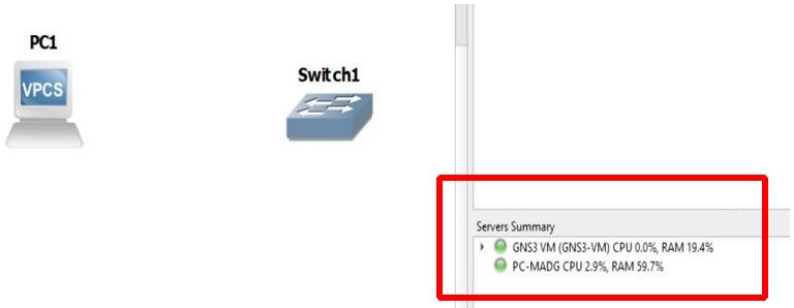
Topología Summary.

Nota. Topología Sumary, donde se describe en lista todos los componentes de red.

Por debajo de esto, se encuentra el apartado “Server Summary” es donde se detalla el estado de los servidores como la maquina física y la máquina virtual y el rendimiento de estos con respecto al desarrollo de la red. Mientras más equipos se encuentren en la red, se consumirá más recursos, como se muestra en la figura 67.

Figura 67

Server Summary.

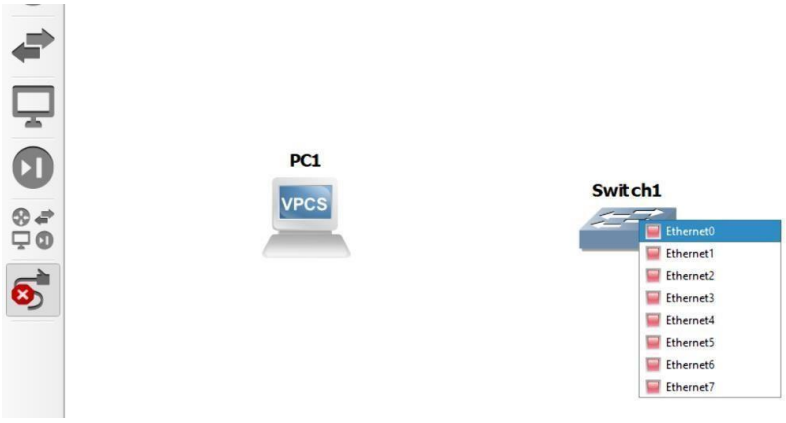


Nota. Aquí se detalla el rendimiento con respecto de desarrollo de la red cuando los equipos se encuentren en la red.

Para terminar con la explicación de la interfaz, se va a conectar los dispositivos e ingresar al modo consola de estos. Para conectar los equipos se hace uso de la herramienta en la parte izquierda “ADD A LINK” y se hace clic sobre uno de los equipos para seleccionar el puerto al cual se va a conectar como se muestra en la figura 68.

Figura 68

Asignación de puertos ethernet de switch

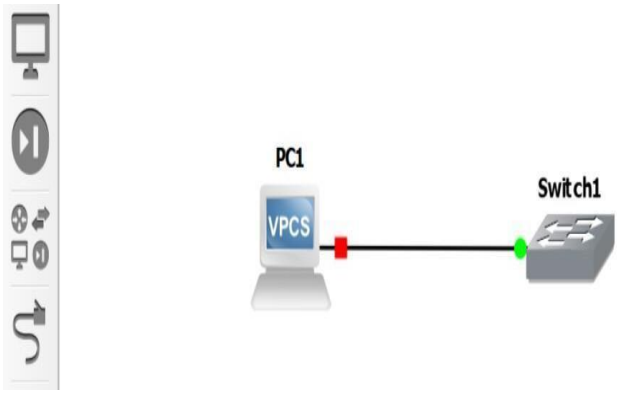


Nota. Aquí se muestra los conectores de red Ethernet de Switch1 a VPCS.

Una representación de cable se extiende desde el componente seleccionado, y se conectara a la PC1 de igual forma haciendo clic sobre el dispositivo y seleccionando el puerto como se muestra en la figura 69, la cantidad y el tipo de puertos dependerán de la configuración del equipo lo cual se explicará en este manual más adelante.

Figura 69

Conexión VPCS a Switch1

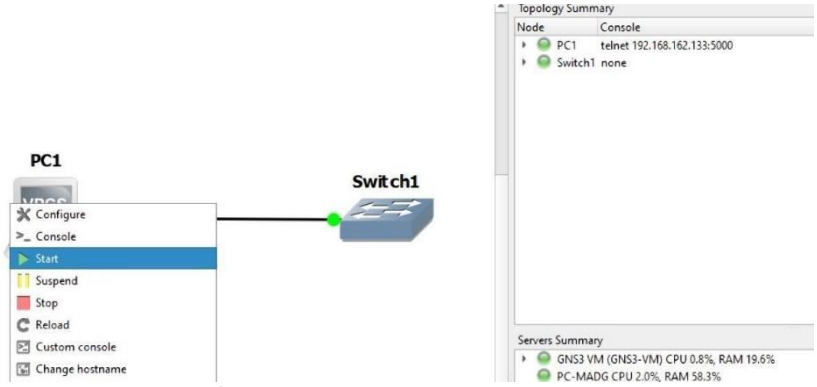


Nota. Extendido de cable ethernet de conexión de PC1 a Switch1.

Para encender un solo equipo se puede dar clic derecho sobre el mismo y ejecutar la opción “start”, al momento de realizar esto se observará como en el servidor de la máquina virtual existe un ligero incremento en el uso del CPU y la RAM como se muestra en la figura 70.

Figura 70

Arranque de PC1



Nota. Al arrancar la PC1 también se puede iniciar la consola.

Para ingresar al modo consola, se da clic derecho sobre el equipo en cuestión, y se ejecuta la opción “Console” inmediatamente aparecerá, el programa SolarPuTTY de la empresa Solarwinds, esta interfaz dependerá tanto del dispositivo como de la configuración que se establezca, como se muestra en la figura 71.

Figura 71

Consola PC1.

Nota. Aquí se asigna de forma manual la IP con mascara de subred.

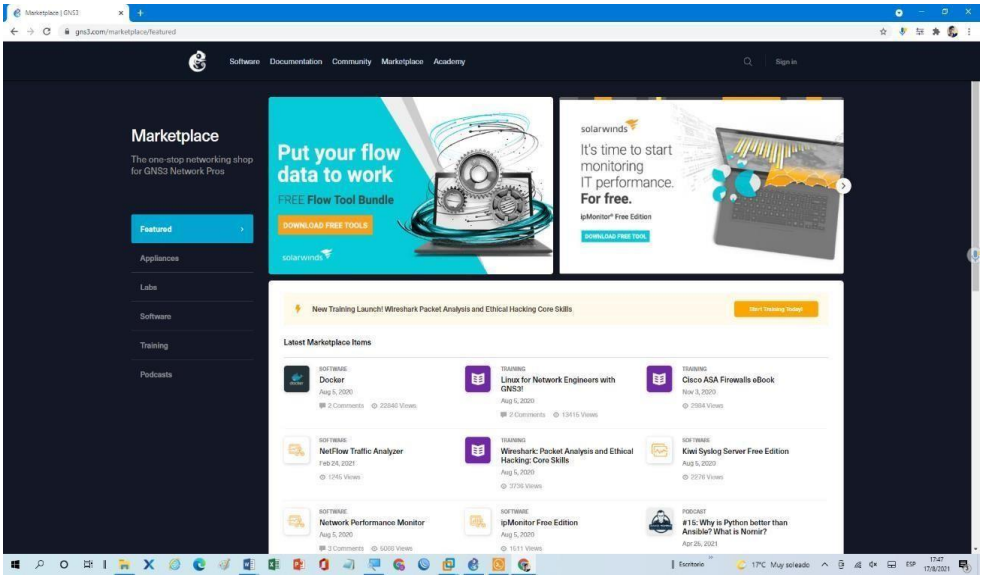
Funcionamiento de GNS3(Emulación de Dispositivos por Dynamips)

Existe una diferencia entre Simulación y Emulación, en GNS3 aquellos dispositivos que son simulados solo representan el procedimiento del dispositivo, pero los equipos y dispositivos que se emulan en GNS3 reproducen el comportamiento especifico de dicho equipo, es por lo que los equipos que vienen por defecto en GNS3 solo cumplen con la función de simulación.

Los equipos CISCO son los más utilizados para las redes de telecomunicaciones, para integrar uno de estos equipos a GNS3 se debe seguir el siguiente proceso. Existe en internet paginas donde se pueden descargar los archivos para la simulación en GNS3, incluso la misma empresa tiene una página llamada “MarketPlace” como se muestra en la figura 72, donde se puede obtener muchos de estos archivos. Algunos son pagados y otros gratis.

Figura 72

MarketPlace de GNS3

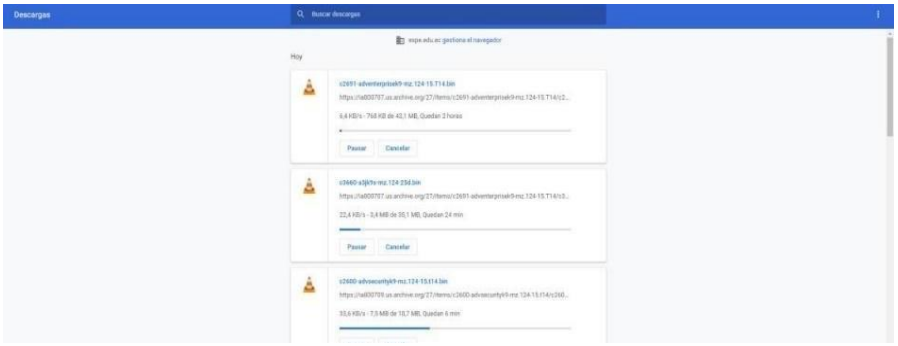


Nota. Aquí se muestra las distintas imágenes tanto como CISCO, Mikrotik, para simulación en GNS3.

GNS3 permite la carga de IOS CISCO por medio del programa de emulación Dynamips un software para los equipos de enrutamiento y conmutamiento de la misma empresa CISCO, estas imágenes se los puede descargar desde el siguiente link https://www.telectronika.com/descargas/cisco-imagenes-iospara-gns3dynamips-y-vm/ .

Figura 73

Descarga de imágenes IOS Cisco

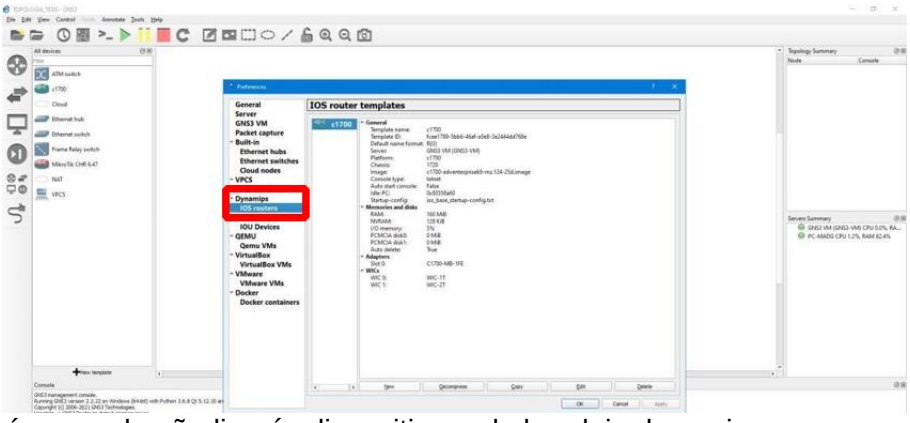


Nota. En este enlace se muestra la descarga de imágenes IOS Cisco.

Para incorporar estos equipos, dentro de la interfaz de GNS3 se debe abrir la ventana "Preferences" como se muestra en la figura 74, es aquí donde se estableció previamente la máquina virtual, pero ahora por debajo del apartado Dynamips se da clic en la opción "IOS Routers" y la ventana debe estar vacía si es que no se han añadido equipos previamente como se muestra en la figura 74.

Figura 74

Añadir imagen IOS de Router templates.

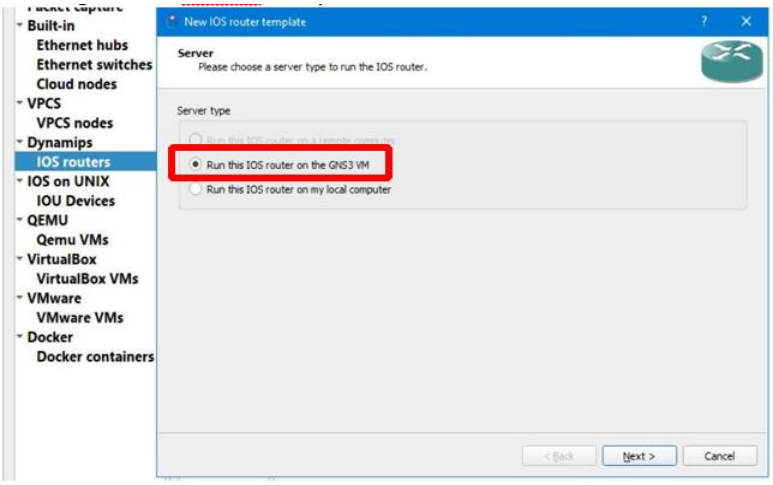


Nota. Aquí se puede añadir más dispositivos a la bandeja de equipos.

Al dar clic en el botón “new” en la parte inferior, otra ventana aparecerá en la cual se puede seleccionar si el equipo a emular sea dentro la máquina virtual o a su vez de la maquina física, es importante escoger la segunda opción como se muestra en la figura 75. Y dar clic en Next.

Figura 75

Nueva imagen IOS Router Templates

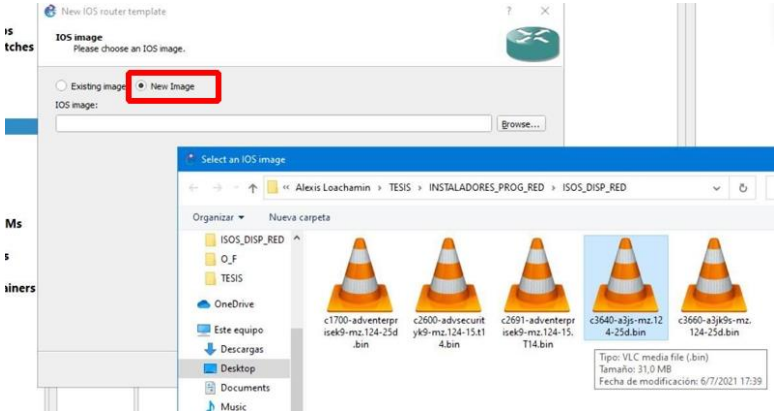


Nota. Aquí es donde se puede añadir imágenes de CISCO.

A continuación, se establece el archivo que contiene la imagen ISO, para esto se debe marcar primero en la casilla “New image” y dar clic en la opción “browse” donde un explorador de archivos permitirá abrir el archivo correspondiente como en la figura 76

Figura 76

Explorador de archivos

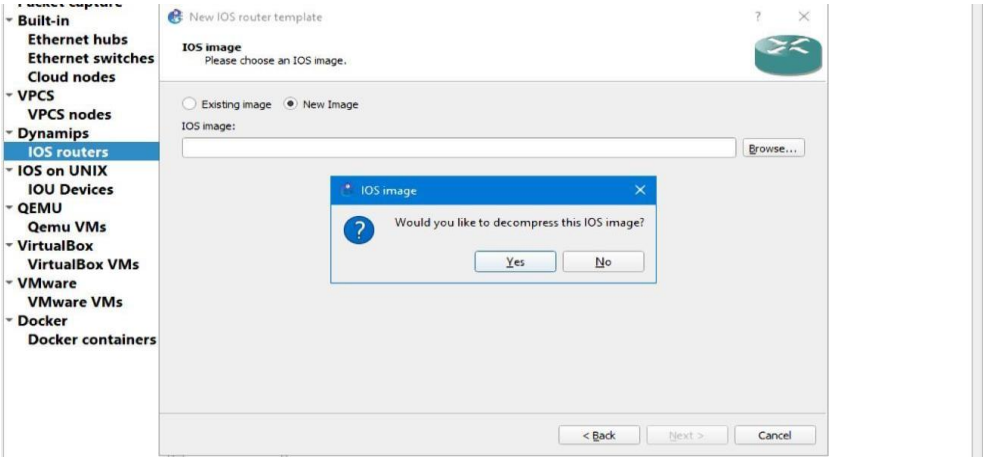


Nota. Los archivos descargados se encuentran comprimidos.

Al ser un archivo comprimido, el mismo programa determinara esto, y le preguntara al usuario si desea que se extraiga la imagen que contiene el archivo, se da clic en la opción “Yes” como se muestra en la figura 77, y en la ventana principal ya se establecerá el archivo IOS y a continuación de esto se debe dar clic en Next, como se muestra en la figura 78.

Figura 77

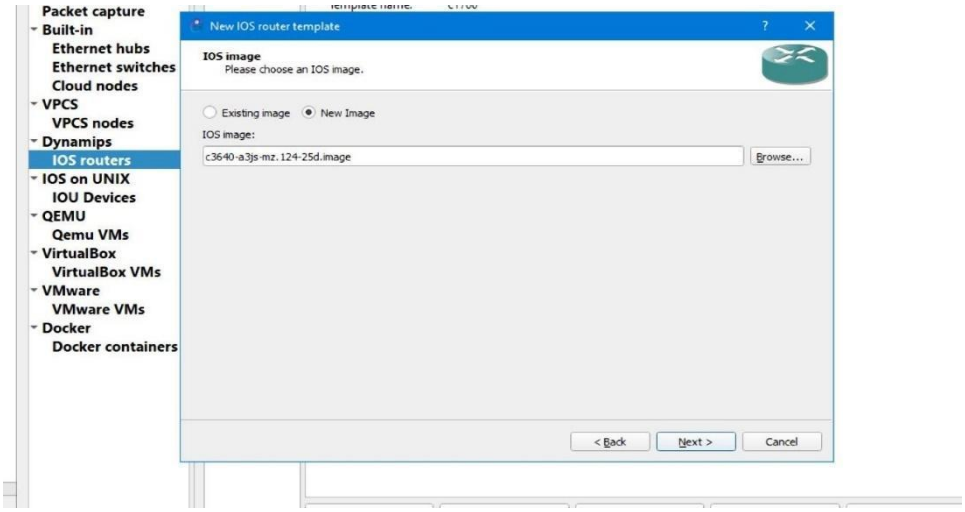
Extracción de imagen.



Nota. Aquí es donde pregunta si quiere descomprimir la imagen IOS.

Figura 78.

Nombre imagen ISO

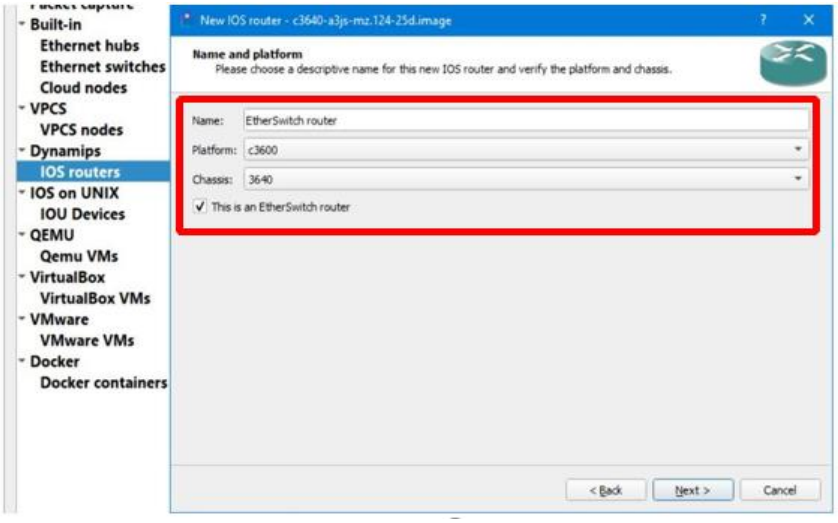


Nota. Aquí es donde se añade el nombre de la imagen ISO.

Posterior a esto la ventana mostrara el menú para cambiar el nombre, por debajo de esta opción existen dos campos “platfform” y “chassis” los cuales por defecto están establecidas por el archivo previamente seleccionado, lo cual se puede cambiar según sea criterio del usuario, de manera que para este caso, emularemos este dispositivo como un “EtherSwitch router”, para lo cual debajo de los campos previos se debe marcar la casilla “This is an EtherSwitch router” como se muestra en la figura 79, y posterior a esto clic en el botón Next.

Figura 79

Name and platform.

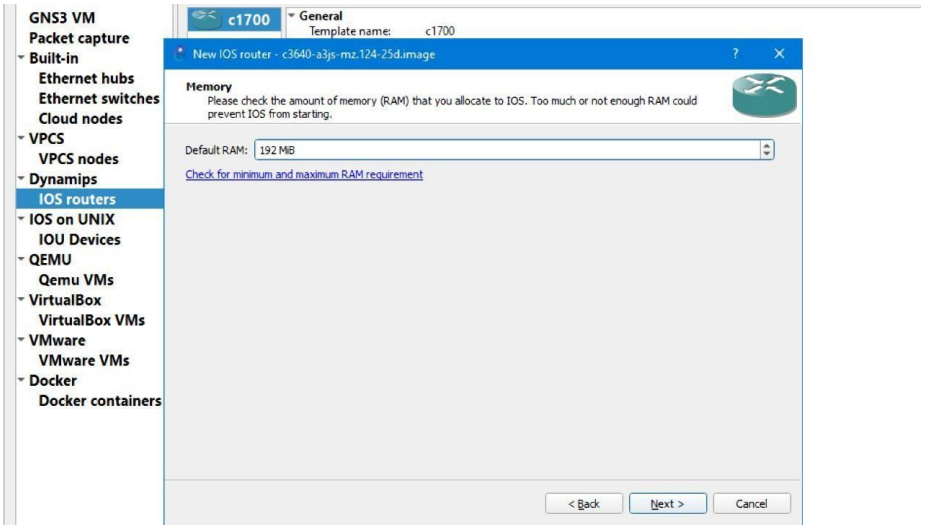


Nota. Aquí se puede cambiar el nombre de la imagen, la plataforma y chasis.

La siguiente ventana mostrara la configuración para la memoria del equipo, en la cual por defecto muestra el valor que el archivo IOS permite, pero esto se puede aumentar dependiendo el criterio del usuario, se recomienda manejar el valor por defecto y dar clic en Next como se muestra en la figura 80.

Figura 80

Apartado Memory

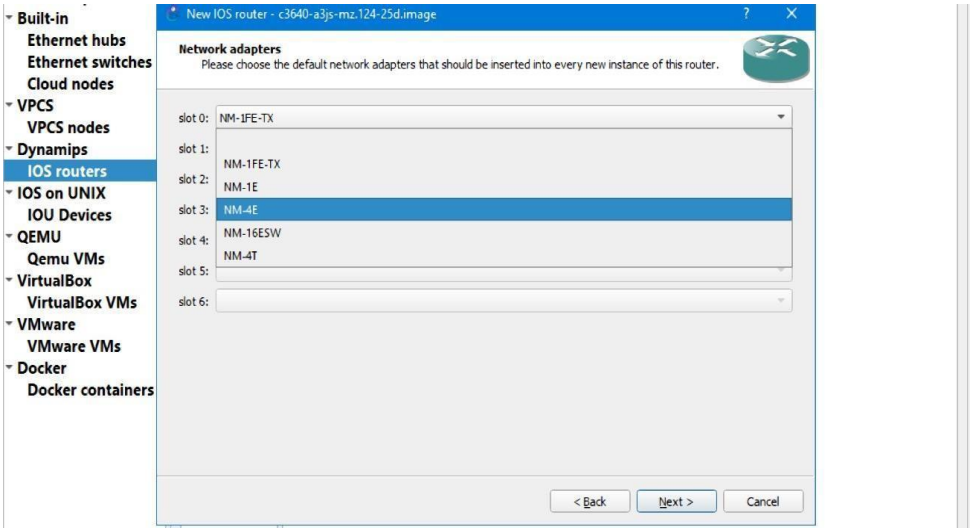


Nota. En default RAM se puede cambiar o dejar por defecto la memoria.

Después la ventana mostrara una serie de menús para configurar los adaptadores de red, en el cual existe una variedad de “slots” a los cuales se les puede asignar un adaptador diferente, pero se recomienda ampliar estos adaptadores como se muestra en la figura 81. Y dar clic en Next.

Figura 81

Network adapters

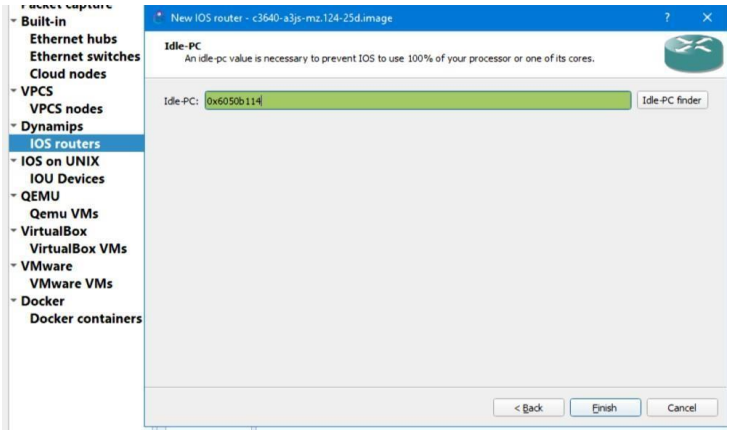


Nota. La cantidad de puertos depende del slot que se añade.

Por siguiente se mostrará el “Idle-PC” el cual es un valor que evita que la emulación por Dynamips consuma el 100% de los procesadores, es muy importante contar con uno, por lo cual en el lado derecho existe una opción “Idle-PC finder” para establecer este campo, y se da clic en Finish.

Figura 82

Idle-PC.

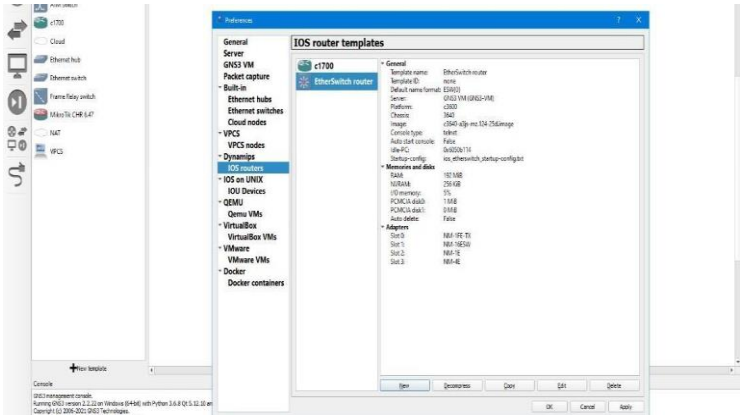


Nota. Se evita el consumo al 100% de memoria y del procesador.

De esta manera se habría completado la instalación de un equipo emulado por Dynamips en GNS3, para comprobar que el equipo se encuentre disponible en la ventana de Preferences se podrá observar a todos los equipos CISCO que pueden extraerse hacia GNS3, tal y como se muestra en la figura 83.

Figura 83

Descarga de equipo Cisco.

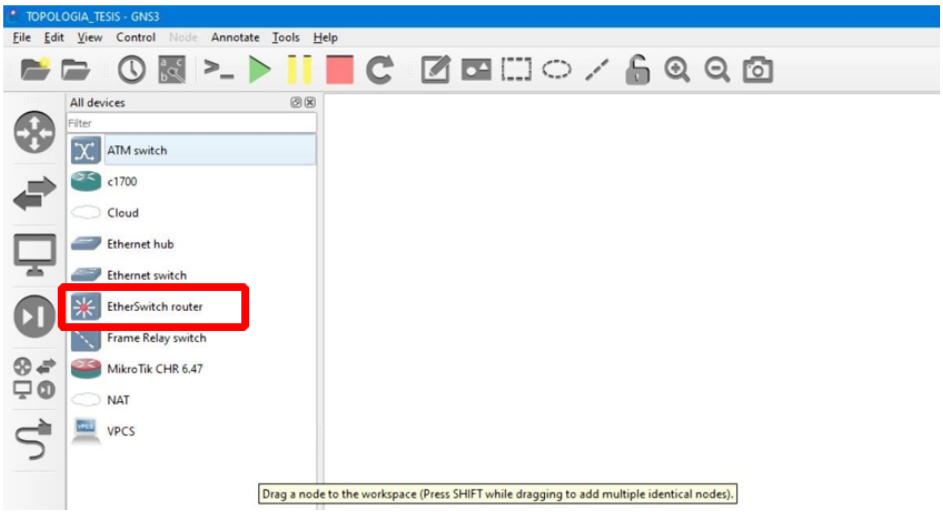


Nota. Aquí puede añadir las imágenes IOS para luego observarse en la parte izquierda.

Y de igual forma en la barra de todos los dispositivos ya se podrá encontrar listo el dispositivo para poder arrastrarlo a la mesa de trabajo y poder trabajar con él, como se muestra en la figura 84.

Figura 84

Imagen añadida a la interfaz de trabajo



Nota. Aquí se muestran las imágenes descargadas, e incluidas en GNS3.

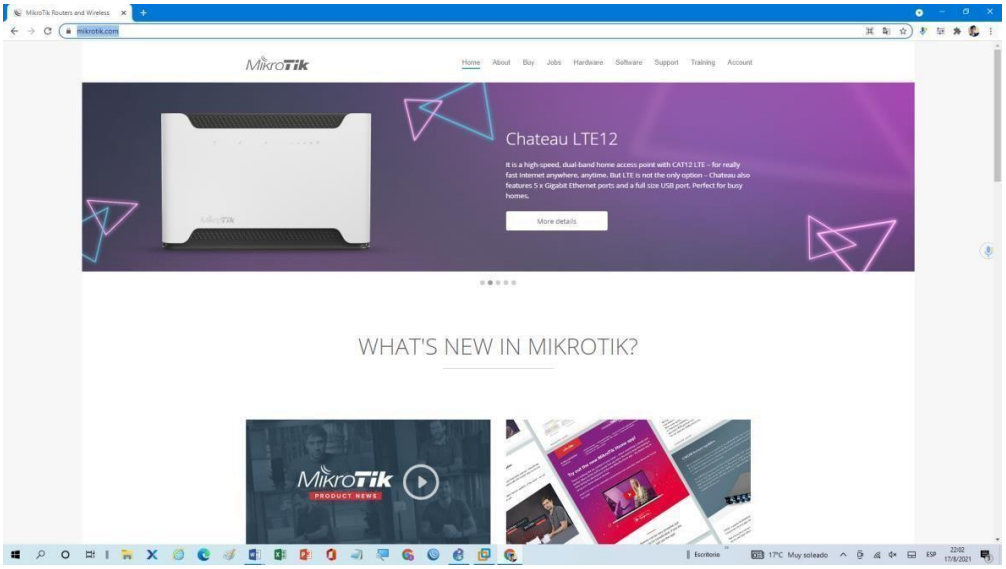
Funcionamiento de GNS3(Emulación de Dispositivos por QEMU)

Para emular equipos marca MikroTik o Juniper se hace uso del software QUEMU el cual es un emulador de sistemas operativos por medio de la traducción dinámica de binarios, un proceso muy útil para la emulación de dispositivos. Para permitir la incorporación de un equipo MikroTik se debe seguir el siguiente proceso.

Se puede obtener los archivos de descarga directamente de la página de MikroTik con el siguiente link https://mikrotik.com/ en el navegador de preferencia, y como se muestra en la figura 85 se debe dar clic en la opción software del menú superior.

Figura 85

Página oficial de Mikrotik



Nota. Aquí se encuentra dispositivos compatibles con GNS3.

En esta nueva página se encontrarán varios tipos de softwares que son muy importantes para el mundo de las redes de datos, debajo se podrá encontrar una gran cantidad de opciones, para la emulación, se requiere descargar el archivo de la sección Cloud Hosted Router, en el apartado Raw Disk image en la columna 6.48.3(estable) como en la Figura 86.

Figura 86

Archivos de imágenes Routeros a descargar.

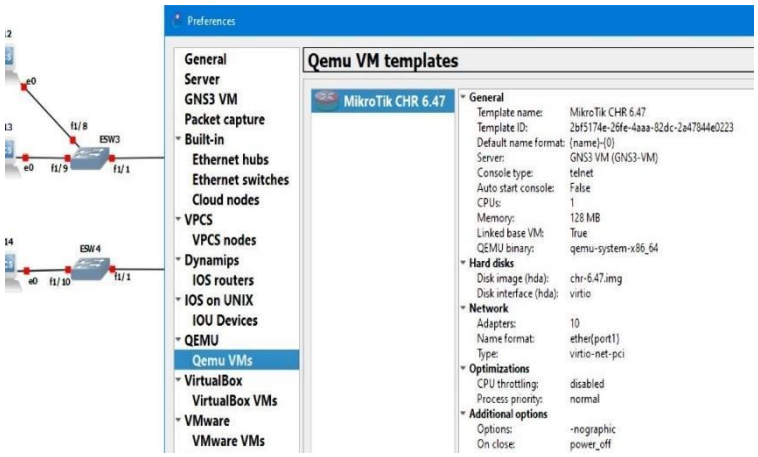
	6.47.10 (Long-term)	6.48.3 (Stable)	6.49beta54 (Testing)	7.1beta6 (Developm
Images	vmdk, vhdx, vdi, ova, img			
Main package				
VHDX image				
VMDK image				
VDI image				
VirtualPC image				
OVA template				
Raw disk image				
Extra packages		Download		
The Dude server				-
The Dude client				
Changelog				

Nota. se encuentra diferentes archivos que se puede emular.

Una vez descargado se debe ingresar a la ventana preference de GNS3 la cual se puede ingresar por medio del comando Ctrl+Shift+P como se muestra en la figura 87 y se dirige a la opción “Qemu VMs” en la cual se describen todos los equipos que se emulen por medio de este programa.

Figura 87

Qemu VM templates

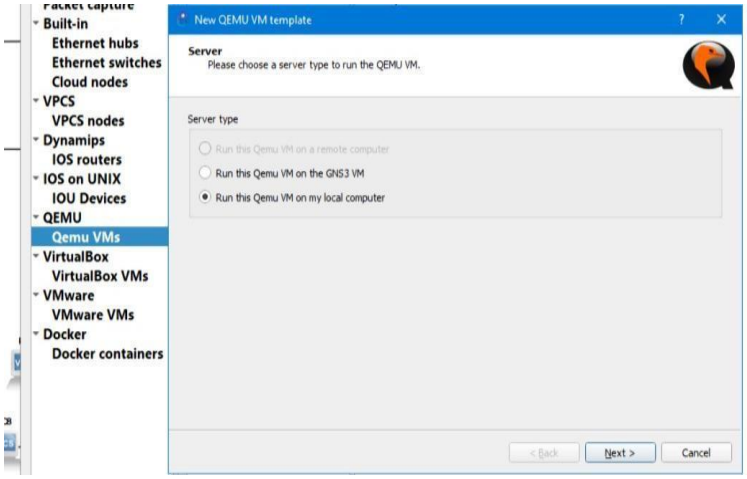


Nota. Aquí se repite los pasos anteriores para añadir imágenes IOS.

Al igual que con los dispositivos anteriores para añadir un nuevo equipo se debe dar clic en el botón new, y una nueva ventana aparecerá para escoger el destino para la emulación del equipo, que se recomienda sea en la máquina virtual de GNS3, como se muestra en la figura 88.

Figura 88

*New Qemu template***.**

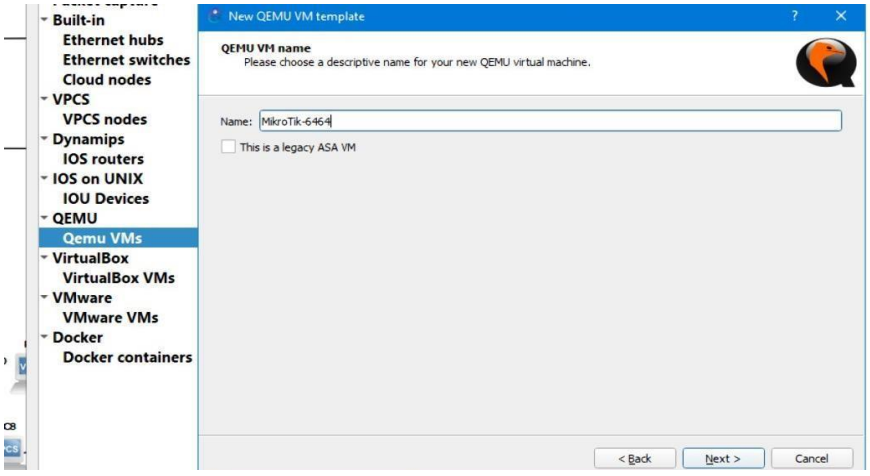


Nota. Se escoge la segunda opción para que arranque con la GNS3VM.

A continuación, la ventana pedirá que se establezca el nombre del dispositivo a emular, como se muestra en la figura 89 y seguido a esto se da clic en la opción Next.

Figura 89

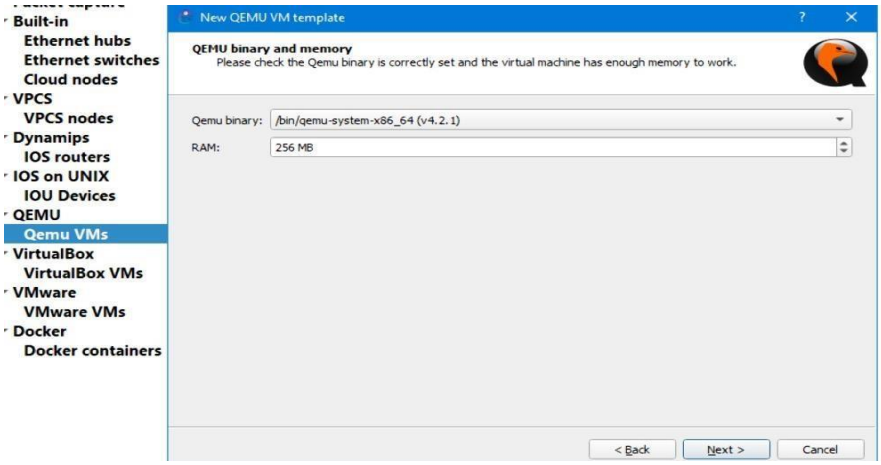
Añadir nombre QEMU.



Posterior se pedirá que se determine la versión de Qemu y la cantidad de RAM para este equipo, estos campos suelen presentarse por defecto y se recomienda dar clic en next. Como se muestra en la figura 90.

Figura 90.

QEMU binary and memory.

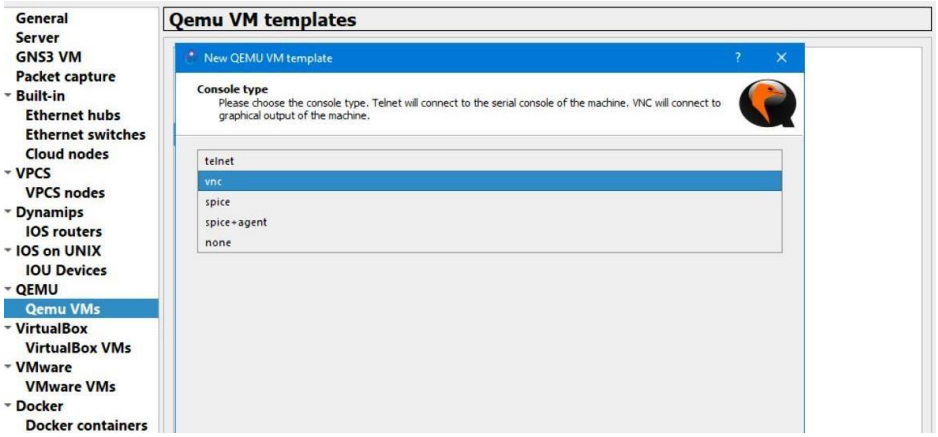


Nota. Opciones para procesadores de 86 y 64 bits.

El programa solicitara que se establezca el modo de consola para trabajar con el equipo, esto depende del gusto del usuario, hay diferentes opciones desde telnet, vnc, spice, etc. Como se muestra en la figura 91.

Figura 91

*Console type par QEMU templates***.**

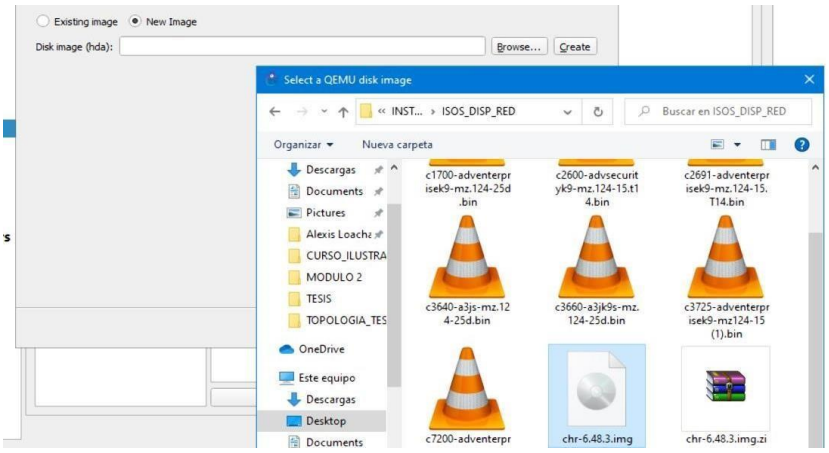


Nota. Aquí se debe escoger la seguridad de Telnet.

De manera que a continuación, el programa solicitara al usuario escoger el archivo a instalar, es importante marcar la casilla “New image” y de igual forma extraer el archivo comprimido que se descargó de MikroTik, como se muestra en la figura 92.

Figura 92

Extraer equipo comprimido descargado de Mikrotik

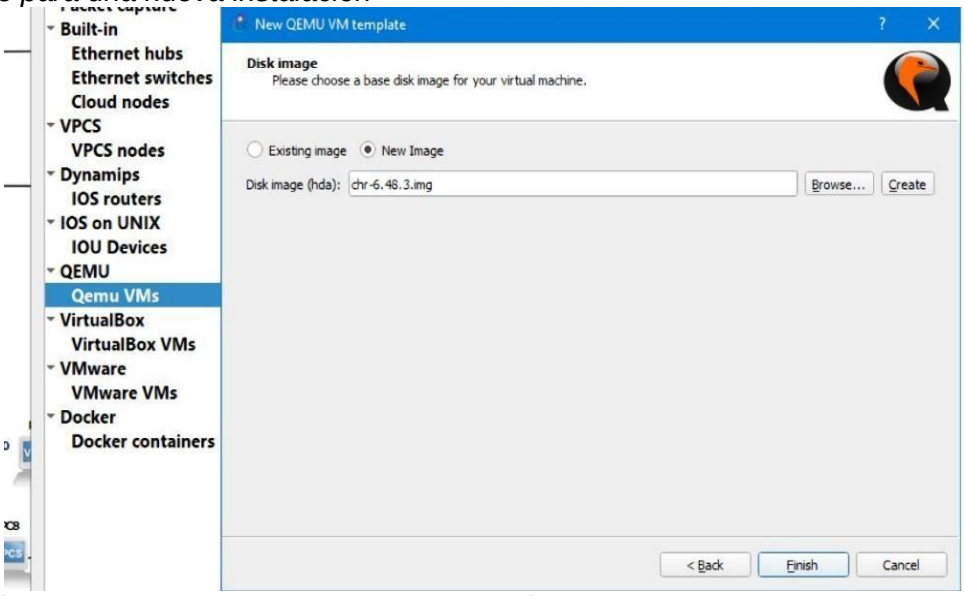


Nota. Se escoge el archivo a añadir a GNS3.

Para finalizar se verificar que todo sea correcto y presiona “finish” como se muestra en la figura 93. Y se podrá comprobar al nuevo dispositivo en el listado de equipos.

Figura 93

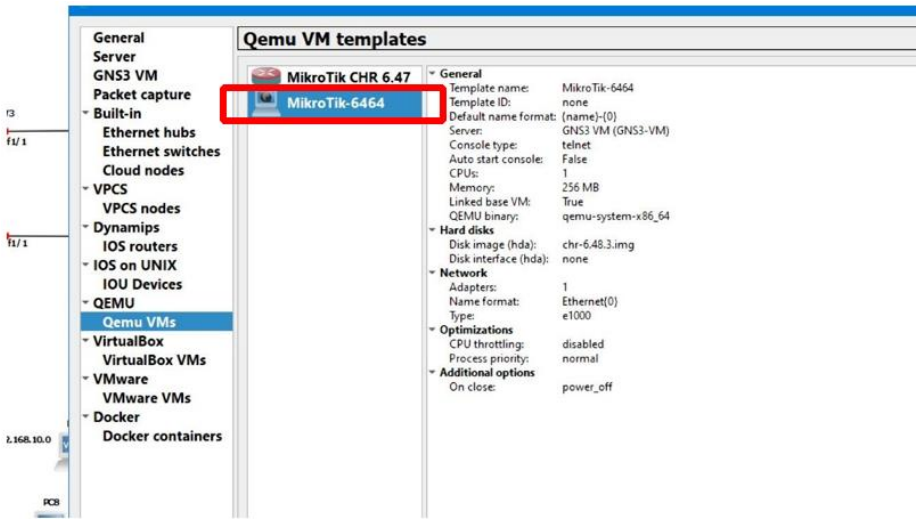
Disk Image para una nueva instalación



Nota. Aquí se añade la imagen de disco en la opción de Qemu VMs.

Figura 94

Nuevo equipo Mikrotik-6464.



Nota. Aquí se añade una nueva imagen Qemu VMs.

Funcionamiento de GNS3 (Otros equipos y componentes)

GNS3 permite la emulación de diferentes componentes y sistemas operativos, dependiendo de la necesidad del usuario, en la ventana “Preferences” que se muestra en la figura 95, es el espacio donde se puede incorporar los equipos que se requieran, de acuerdo al software de emulación correspondiente. En la siguiente tabla se muestra una descripción para cada preferencia disponible en GNS3.

Tabla 2

Opciones de la ventana "preferences" gns3

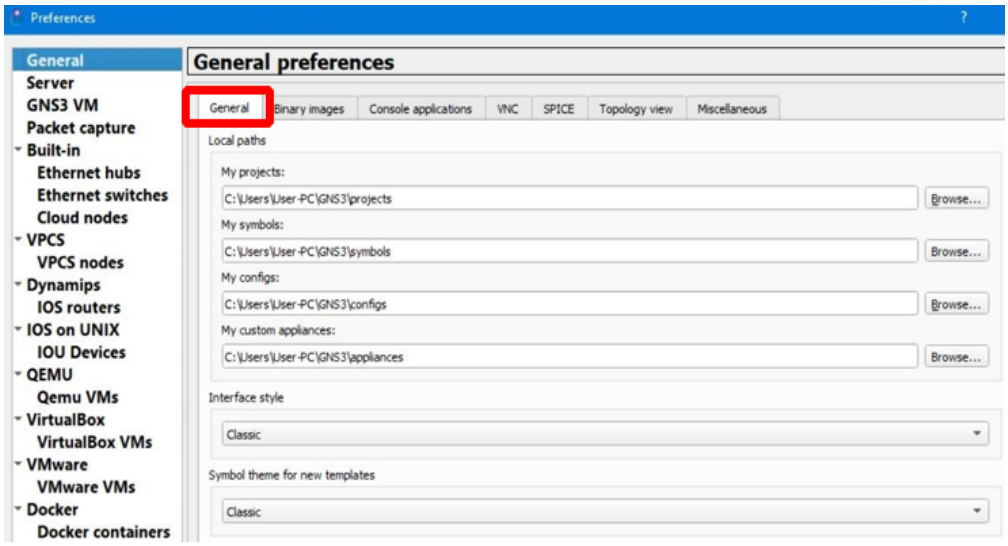
PREFERENCIA	EQUIPOS
Server	Servidores locales (computadora física) o remotos (conectador en red hacia el programa GNS3)
GNS3 VM	Máquina virtual propia de GNS3 para la emulación de equipos.
Packet Capture	Analizador de paquetes, por defecto GNS3 incorpora el programa Wireshark, el cual es utilizado para el análisis de datos y protocolos, que permitan dar solución a problemas de red.
Built-in Ethernet hubs Ethernet	Espacio para la simulación de dispositivos HUB, Switch y nubes, donde la configuración es totalmente básica y se permite únicamente la simulación de equipos de capa 2 y nube.
VPCS nodes	Equipos terminales, permite la emulación de computadoras, por defecto GNS3 utiliza un programa escrito por Paul Meng, el cual simula una PC con características y protocolos básicos, el cual consume un mino de 2 MB de memoria RAM. Es posible aumentar VPCS, pero esto demandaría más recursos para su emulación, se recomienda se use el nodo por defecto
Dynamips IOS router	Es un programa que permite la emulación para enrutadores CISCO IOS, los cuales consumen menos memoria y CPU, por lo que se los puede añadir el número de routers a la topología según sea la necesidad y la capacidad del servidor donde se esté ejecutando.
IOS on UNIX IOU devices	UNIX es un sistema operativo portable, en GNS3 utiliza este software, el cual permite emular equipos de tipo IOS bajo un sistema de tareas múltiples, pero de operación única; lo que reduce el consumo de recursos en su emulación. algunos equipos y softwares que aplican UNIX son Solaris Oracle, NetBSD, macOS, etc.

PREFERENCIA	EQUIPOS
QEMU **Qemu VMs**	QEMU s un emulador de procesadores, el cual puede virtualizar a partir de la traducción dinámica de binarios, la mayoría de fabricantes brindan imágenes QEMU, incluso GNS3 recomienda que se utilice esta emulación.
VirtualBox **VirtualBox VMs**	VirtualBox es un software para la simulación de sistemas operativos basados en arquitecturas x86/amd64, desarrollado por Oracle, principalmente se usa para máquinas virtuales, para GNS3 se lo puede usar para emular computadoras con su respectivo sistema operativo.
VMware **VMware VMs**	Al igual que VirtualBox, VMware es recomendado por GNS3 para la emulación de máquinas virtuales con sistemas operativos, por su compatibilidad con el programa.
Docker **Docker containers**	Docker es un programa en el cual los softwares o aplicativos como topologías de red en GNS3 puedan ser totalmente operativas independiente de la maquina donde se vaya a ejecutar, gracias a su arquitectura de “contenedores” permite que se reduzcan los costos de operatividad.

Nota. Esta tabla muestra las opciones de la ventana de configuración “preference” con respecto a la versión GNS3 2.2.22 del 2021.

Figura 95

*General Preferences***.**

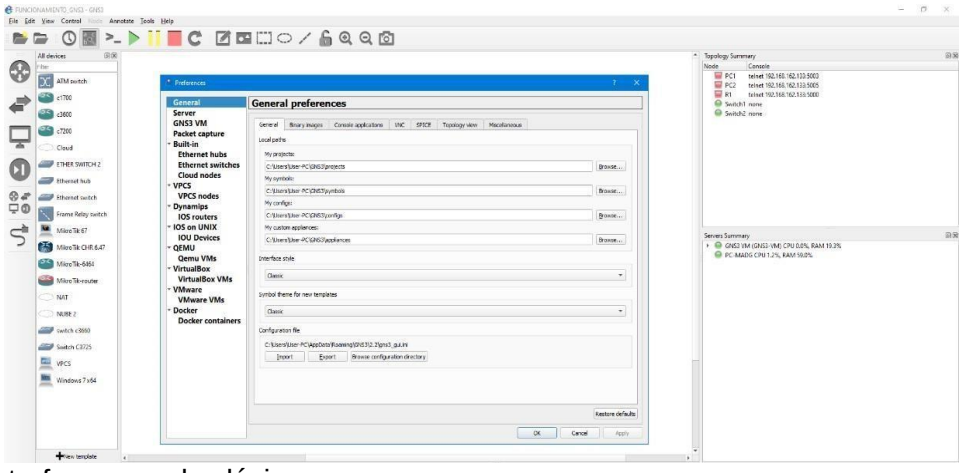


Nota. Aquí se repiten pasos ya vistos anteriormente en dispositivos Cisco

También se debe mencionar un apartado que, si bien no es como tal una herramienta de simulación o un programa de emulación, en el apartado “General” de la misma ventana se podrán realizar configuraciones en cuanto al entorno de trabajo, como es el caso del estilo de interfaz con que se puede trabajar y que se muestran en las figuras 96, 97 y 98.

Figura 96

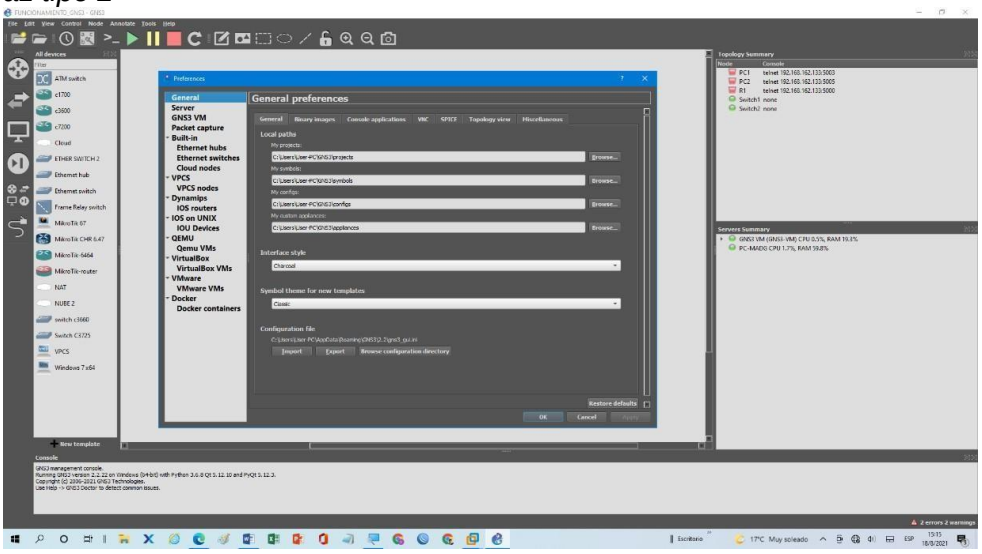
Apartado General.



Nota. Interfaz en modo clásico.

Figura 97

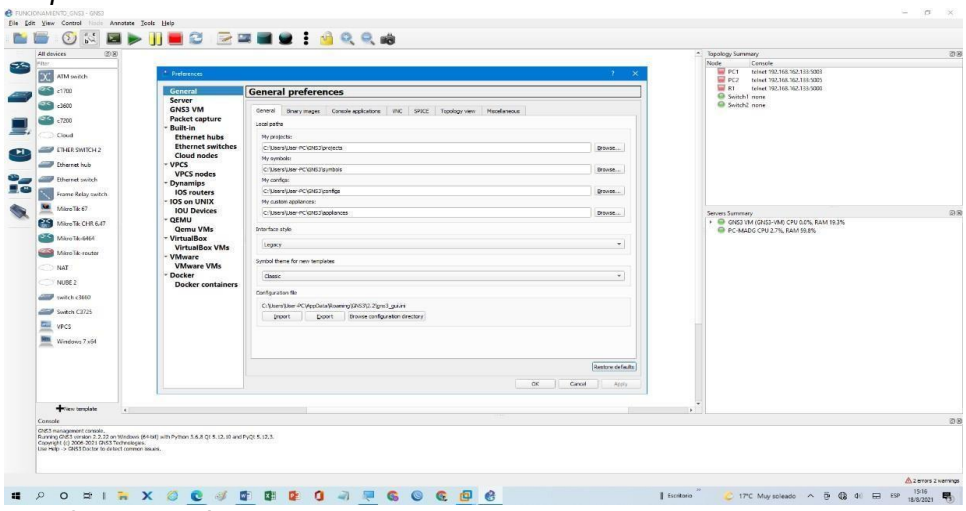
Interfaz tipo 2



Nota. Interfaz en modo Charcoal.

Figura 98

Interfaz tipo 3.

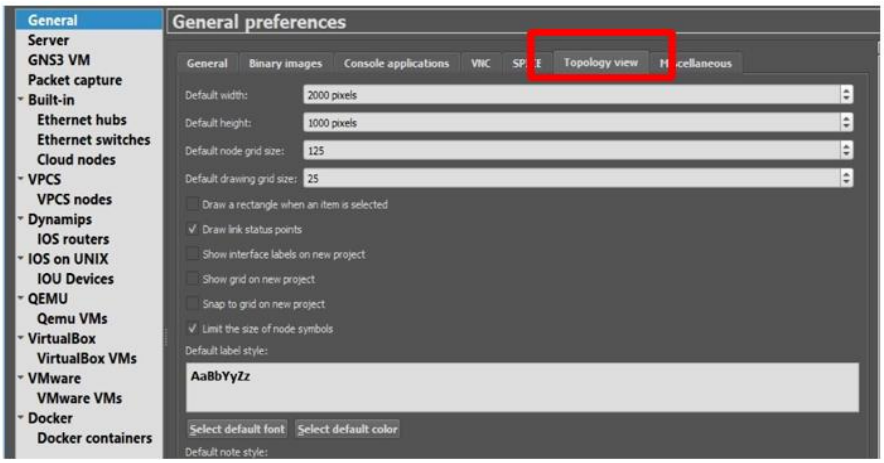


Nota. Interfaz en modo Legacy.

También en el apartado de “topology view” se podrá cambiar la visualización del campo de trabajo de la interfaz de GNS3, como se muestra en la figura 99, además también se podrá cambiar la fuente que se quiere establecer para los textos entre otras opciones como mostrar el nombre de los puertos que se encuentren utilizados en la topología.

Figura 99

Topology view de GNS3.

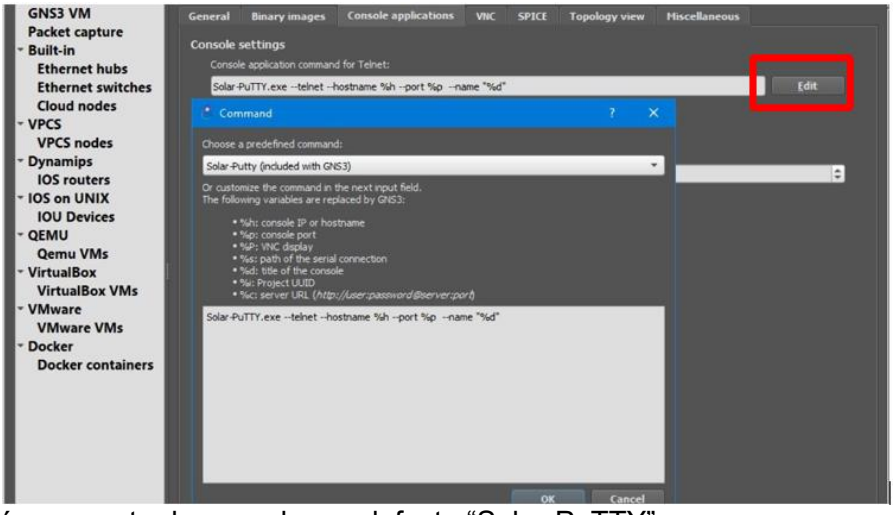


Nota. Aquí se añaden nuevas configuraciones para emulación.

En la pestaña “Console applications” se podrá cambiar el tipo de consola que emularan los programas respectivamente, como se muestra en la figura 100, la consola por defecto es el programa Solar-PuTTY, se puede cambiar esto si se da clic en el botón “Edit” al lado derecho de la barra, donde una nueva ventana demostrara cual es la configuración para esta consola.

Figura 100

Consola Solar-PuTTY.

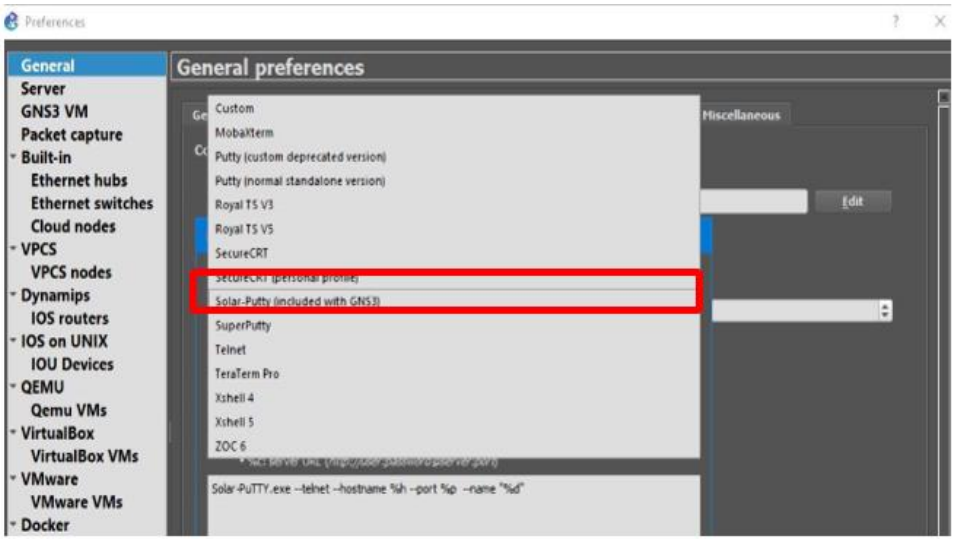


Nota. Aquí se muestra la consola por defecto “Solar-PuTTY”

Si se despliega la lista con un clic sobre el nombre de la consola, aparecerán muchos programas externos a GNS3 por lo que es necesario que se instalen de forma manual, pero estos tienen un valor monetario, la selección del tipo de consola depende del usuario.

Figura 101

*Consola Solar-PuTTY***.**

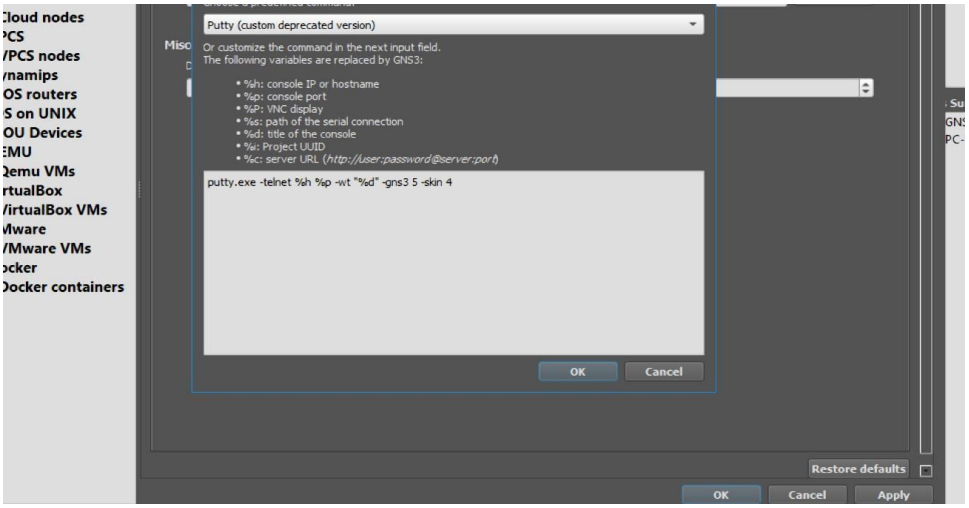


Nota. Se debe seleccionar las consolas dependiendo del gusto del usuario.

GNS3 permite la consola PuTTY (custom decrapted versión), para guardar el nuevo tipo de emulación seleccionada, basta con dar clic en el botón OK, como se muestra en la figura 102 y dar clic en “APLLY” y luego en “OK” cuando se ejecute la consola de algún dispositivo se podrá observar que esta tiene un aspecto diferente, como se muestra en la figura 103.

Figura 102

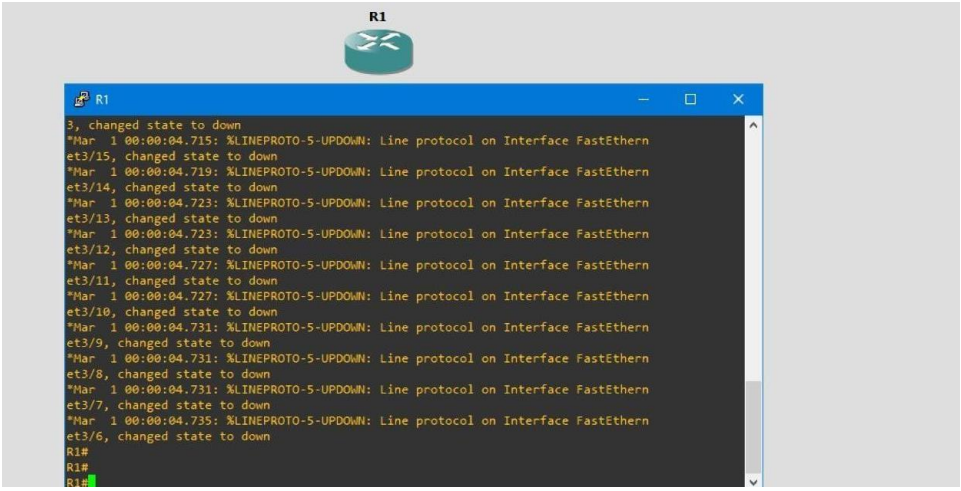
PuTTY (custom decrapted versión)



Nota. Aquí se debe seleccionar las consolas nativas de GNS3..

Figura 103

Consola de Router 1



Nota. Esta consola es parecida a la de dispositivos Cisco.

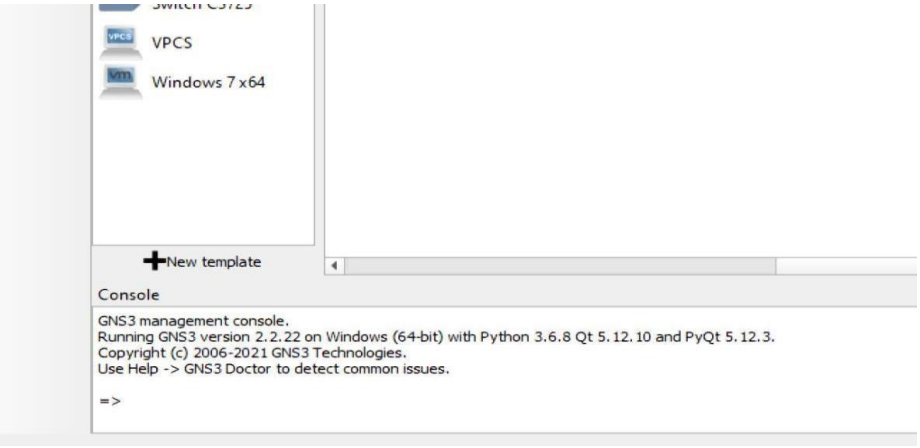
Acceso a dispositivos por plantillas "Template"

El programa GNS3 tiene un completo historial acerca de los dispositivos que se pueden integrar para su emulación dentro de la interfaz, por medio del proceso "Template" se puede establecer el dispositivo que se necesite, desde routers, switches, nodos, Firewalls, entre otros. Para lograr esto se tomará como ejemplo la integración de un navegador Firefox al listado de equipos para emulación en GNS3, por medio del siguiente proceso.

Primero como se muestra en la figura 104, por debajo del listado de equipos que ya se encuentren listos para su emulación en el programa, existe una opción con una etiqueta "+New template"

Figura 104

*New templete***.**

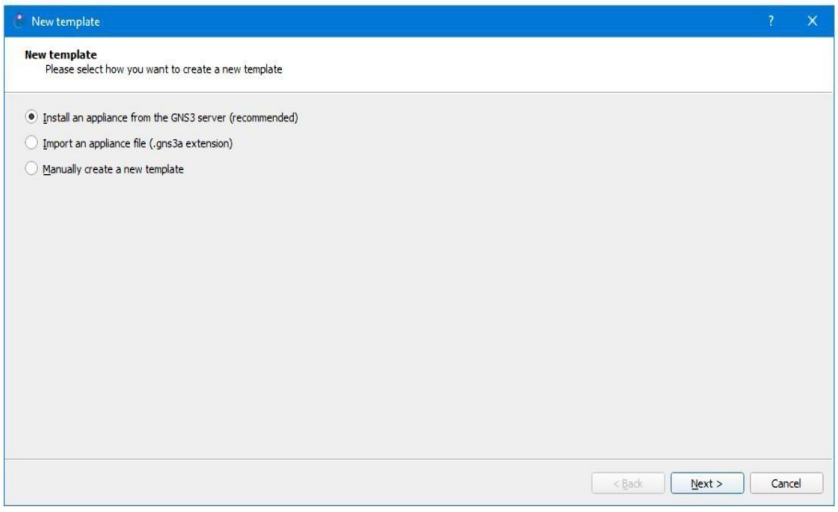


Nota. Aquí se muestra el listado de todos los equipos.

Al dar clic una nueva ventana la cual es muy parecida a la instalación de equipos para emulación por Dynamips y Qemu aparecerá, en donde se debe establecer el servidor para la emulación del equipo en cuestión. Se debe marcar la casilla para la opción de la máquina virtual, como se muestra en la figura 105 y a continuación dar clic en "Next"

Figura 105

New template Install appliances.

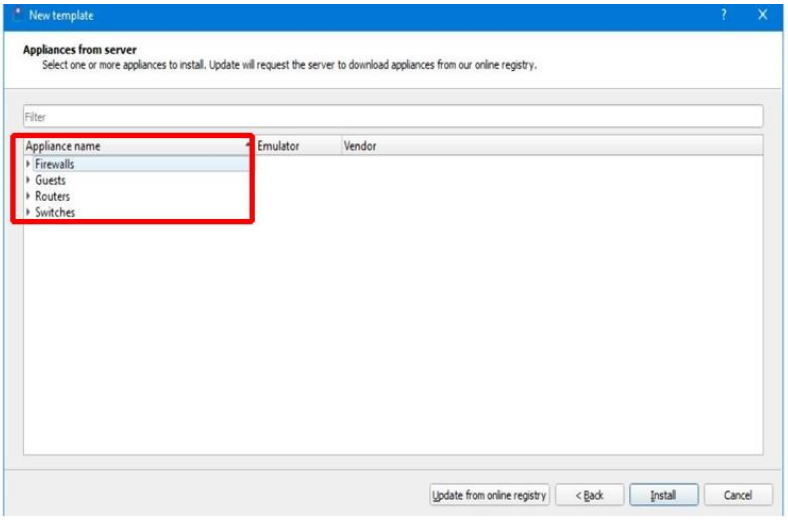


Nota. Se instala el dispositivo para GNS3 server por que recomendado.

Por consiguiente, la ventana mostrará etiquetas para desprender todos los equipos que se pueden atribuir dentro de GNS3, existen cuatro campos principales como se muestran en la figura 106 y 107, para encontrar el navegador Firefox se debe desprender el listado de la opción “Guests”. Una vez seleccionada el equipo se da clic en la opción “Install”.

Figura 106

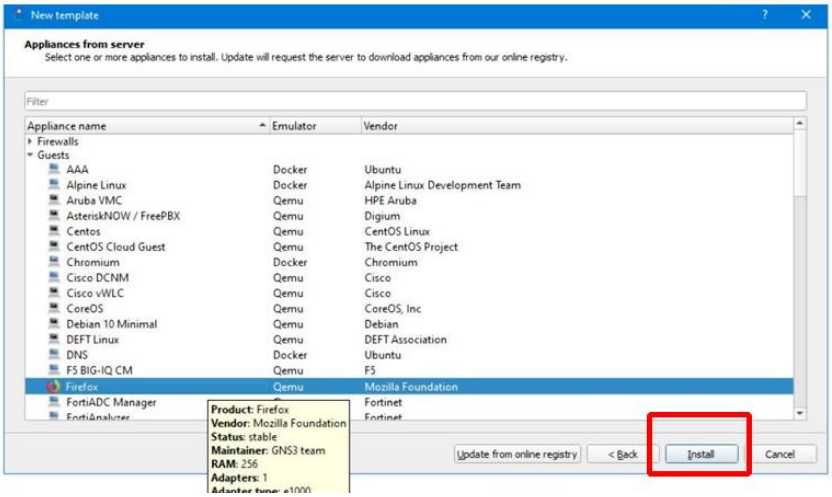
Appliance from server.



Nota. Aquí muestra los equipos como Firewalls, Guests, Routers, Switches.

Figura 107

Appliance de Guest

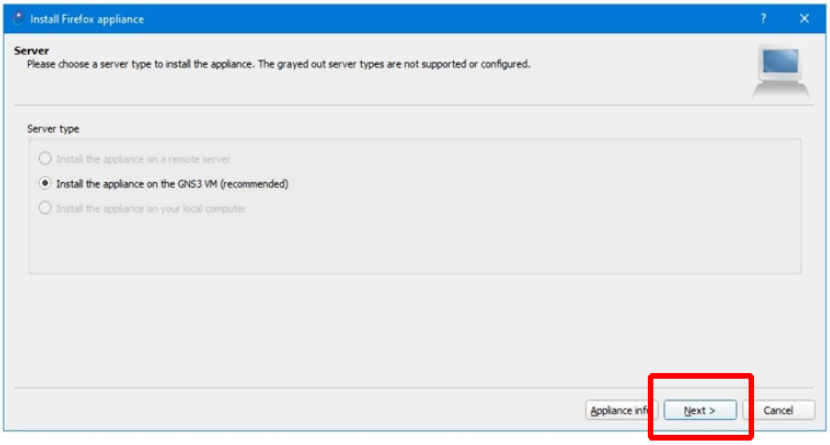


Nota. Aquí muestra en forma de emulador Qemu al navegador Firefox.

Lo cual desplegara una nueva ventana como se muestra en la figura 108, la cual simplemente describe el servidor que se ha escogido previamente para el dispositivo. se debe avanzar haciendo clic en el botón “Next”.

Figura 108

Navegador Firefox por medio de emulador Qemu.

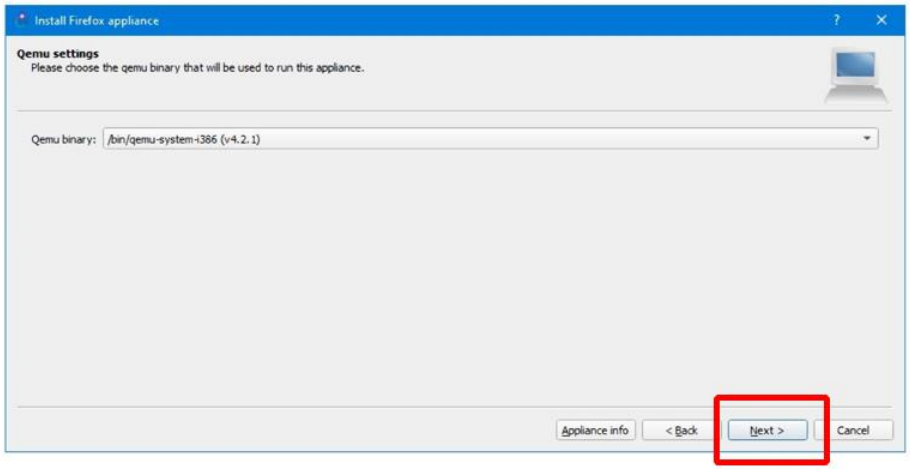


Nota. Aquí se debe escoger la segunda opción que dice que debe instalar el equipo en GNS3 VM ya está recomendado.

A continuación, el usuario debe seleccionar el sistema de Qemu binary, lo cual como muestra la figura 109, se establece por defecto, a pesar de que se puede cambiar esta opción es recomendable dejarlo en el sistema preestablecido. Se debe dar clic en el botón “Next”.

Figura 109

Qemu Settings par QEMU binnary

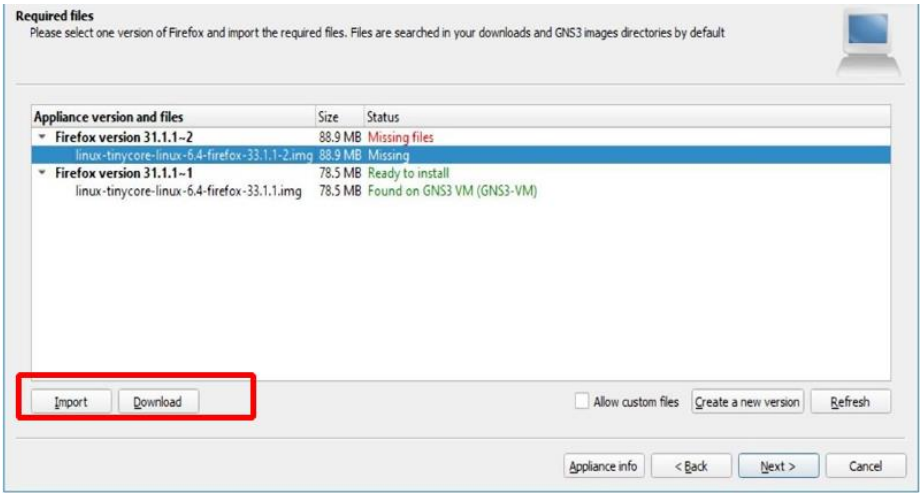


Nota. Aquí se observa en la versión de Qemu binary.

Para el navegador Firefox existen dos versiones, pero como se podrá evidenciar en la figura 110, en la columna status con letras rojas demostrara si los archivos correspondientes se encuentran importados en letras rojas el mensaje “Mising Files” que quiere decir la falta del archivo de incorporación, de forma que, GNS3 ofrece direccionar al usuario hacia el link donde se puede descargar el archivo. Por debajo se encontrará dos opciones “Importa” y “Download”.

Figura 110.

Required files for templates

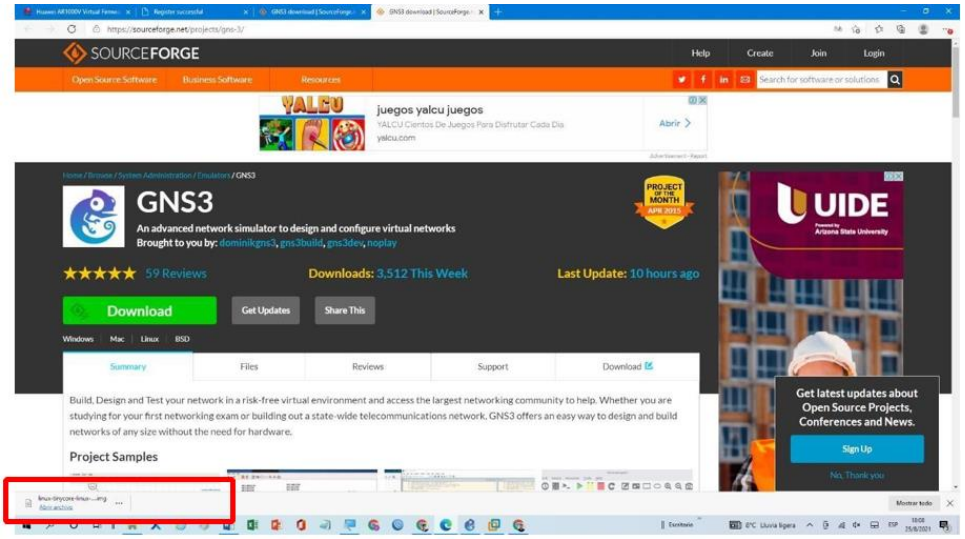


Nota. Se muestra el estado de los archivos que se encuentran importados.

Se seleccionará la versión “Linux-tyncore-linux-6.4-firefox-331.1.1.img” y se da clic en la opción Download, donde un pequeño cuadro de dialogo advertirá al usuario para direccionarlo a la página que se muestra en la figura 111, para este caso el archivo se descargara gratuitamente existen casos donde se necesitará la compra de la imagen a descargar.

Figura 111

Linux-tyncore-linux-6.4-firefox-331.1.1.img

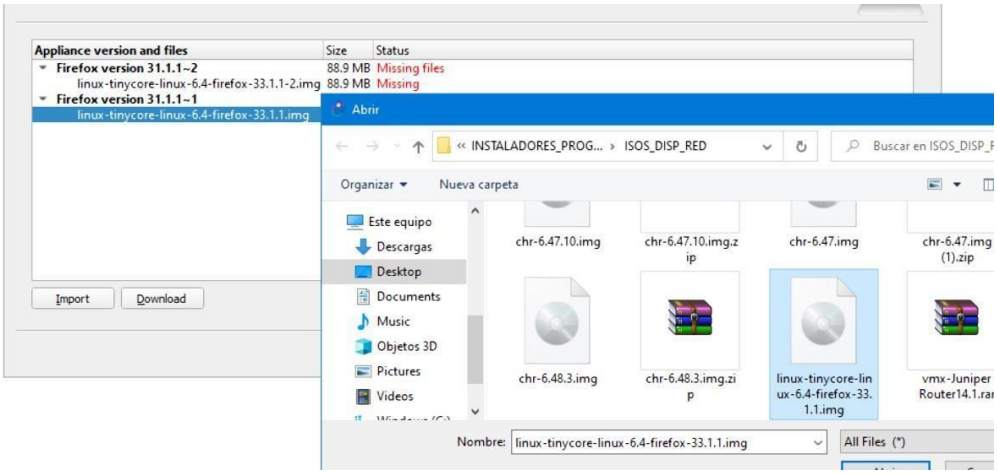


Nota. Aquí muestra la página de descargas para la imagen ISO.

Una vez descargado el archivo y especificado la ubicación de este de regreso en la ventana de instalación de Firefox en GNS3 ahora se da clic en la opción “import” donde un explorador de archivos se abrirá y permitirá al usuario que se escoja el archivo previamente descargado. Como se muestra en la figura 112.

Figura 112

Importación de archivo previamente descargado.

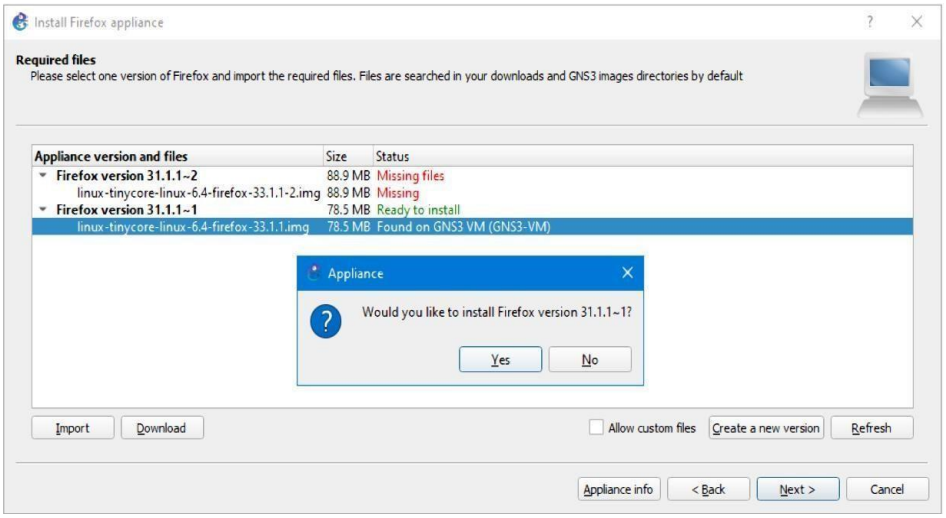


Nota. Se encuentra guardado en la carpeta destinado para el almacenamiento de imágenes ISO.

Una vez que se haya seleccionado el archivo el mensaje en el estado de la plantilla debe enunciar “Ready to install” como se muestra en la figura 113, de esta forma y seleccionada la plantilla se debe dar clic en “Next”, donde un cuadro de dialogo solicitara al usuario si se desea instalar la versión seleccionada previamente. Y se da clic en “YES”.

Figura 113

Ready to install

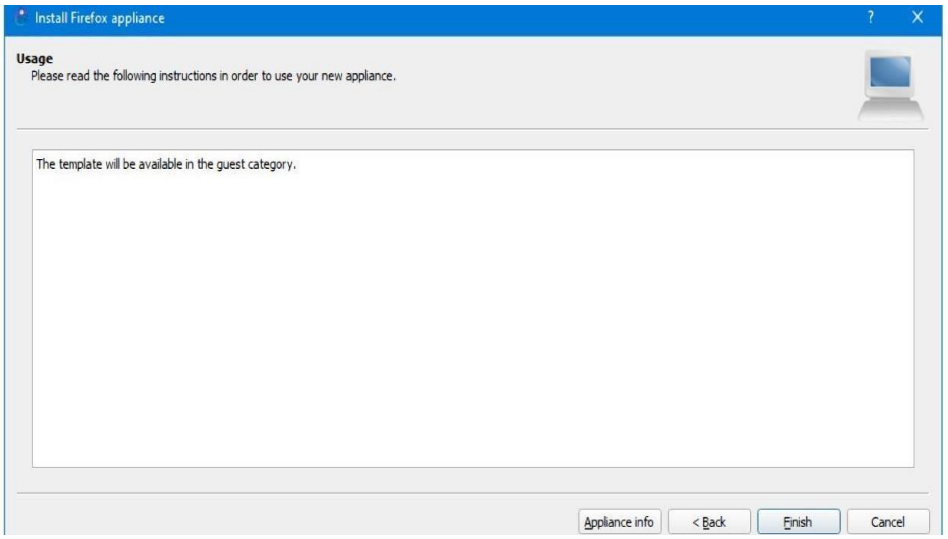


Nota. Aquí muestra si quiere instalar el navegador Firefox versión 31.1.1-1.

Para finalizar con la instalación la ventana que se muestra en la figura 114, menciona al usuario seguir instrucciones para iniciar con el dispositivo, esto dependiendo de lo que se haya instalado, al dar clic en “Finish” ya se podrá encontrar al dispositivo en el listado izquierdo de equipos como se muestra en la figura 115.

Figura 114

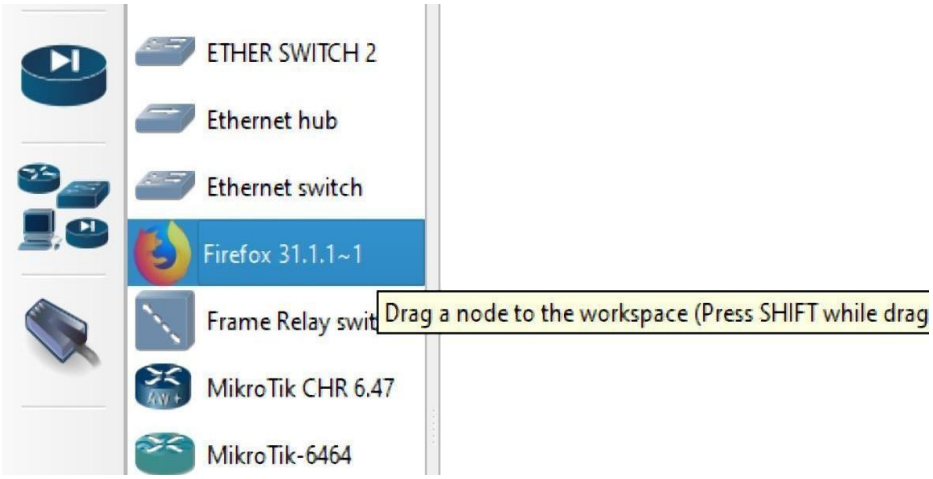
Final de instalación de Firefox.



Nota. Aquí se observa el final de la instalación del navegador de Firefox.

Figura 115

*Firefox en la bandeja de dispositivos***.**

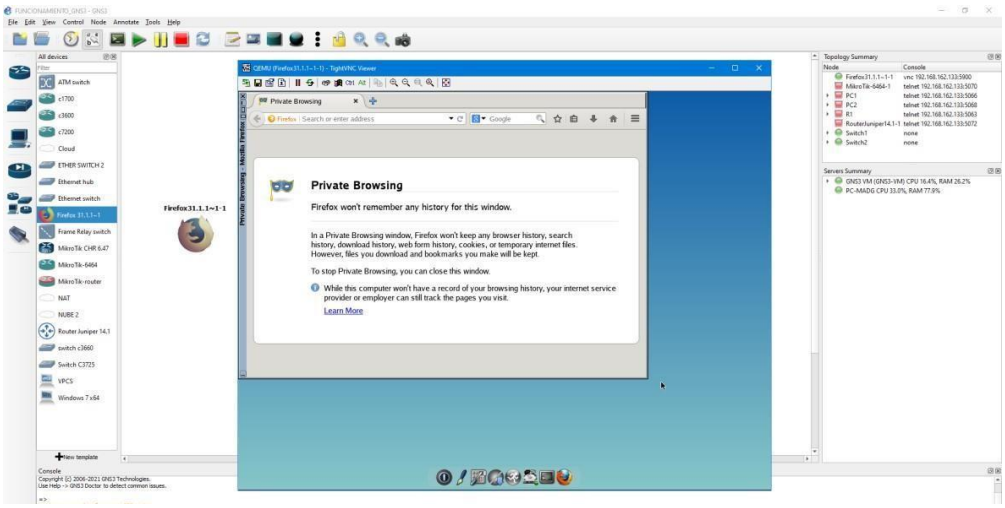


Nota. Por defecto ya se visualiza en todos los dispositivos.

Se arrastra la nueva emulación hacia el espacio de trabajo, se lo enciende, para ejecutar la “consola” como si de un equipo de red se tratará, como se muestra en la figura 116, este equipo accede al modo consola por medio de la interfaz de Qemu. Es importante mencionar que esta clase de equipos consume gran parte de los recursos disponibles.

Figura 116

Firefox ejecutado con consola



Nota. Una vez arrastrado al entorno de trabajo, es encendido y arrancado la consola.

Manejo del Simulador GNS3 (Topologías de red)

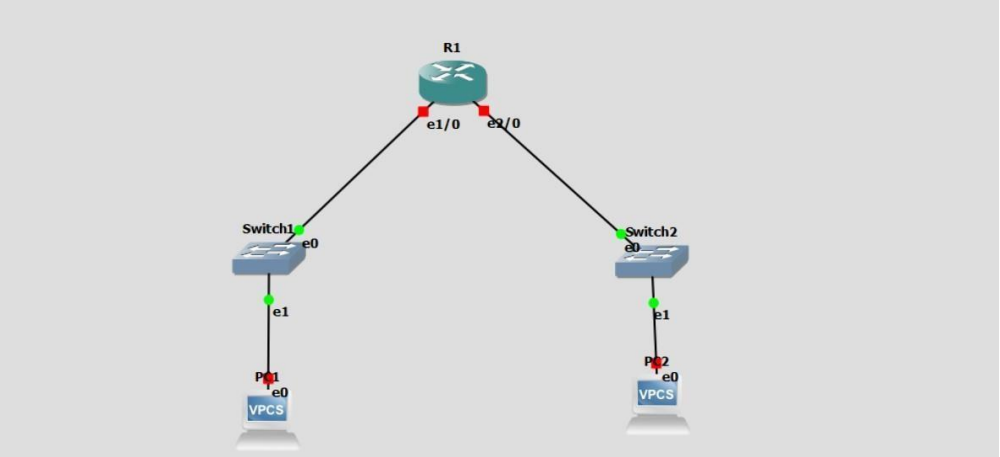
El simulador de redes grafico por las siglas en ingles GNS3 tiene una amplia cantidad de opciones y herramientas disponibles que permiten la administración, configuración, y análisis de redes de datos.

Para explicar el manejo real de este programa, se realizará una demostración por medio de la creación de una red LAN la cual hará uso de diferentes protocolos para su funcionamiento, y a medida se avance con la red se ira explicando el correcto manejo de GNS3.

Teniendo en cuenta las imágenes de los dispositivos que el usuario prefiera, la red que se va a crear es la que se muestra en la figura 117, una topología simple pero que permitirá demostrar el manejo de GNS3, primeramente, se deben arrastrar los equipos hacia el espacio de trabajo y como se mostró previamente en este mismo manual en la sección interfaz de trabajo de GNS3, se conectan los equipos por el puerto que se prefiera.

Figura 117

Topología de ejemplo.



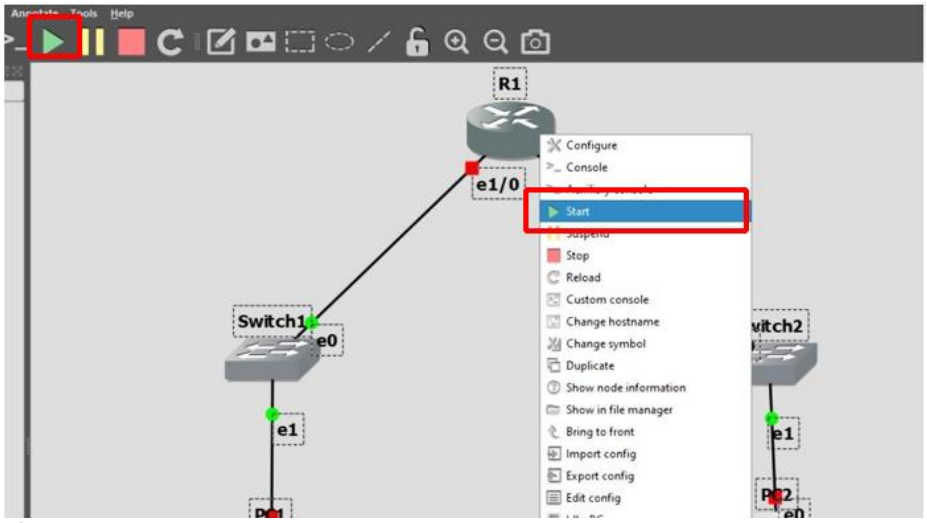
Nota. Los dispositivos se encienden uno por uno para no sobrecargar a la máquina física.

Para encender los equipos existe dos opciones en la barra de herramientas en la parte superior el botón “start/resume all nodes” prendera todos los equipos, esto puede ser un poco

riesgoso, puesto que si existen muchos equipos al iniciar su emulación podría sobrecargar los servidores que se estén usando (máquina virtual y física) de forma que lo óptimo es iniciar cada dispositivo dando clic derecho sobre cada uno y presionar la opción Start. Como se muestra en la figura 118.

Figura 118

Arranque de los dispositivos

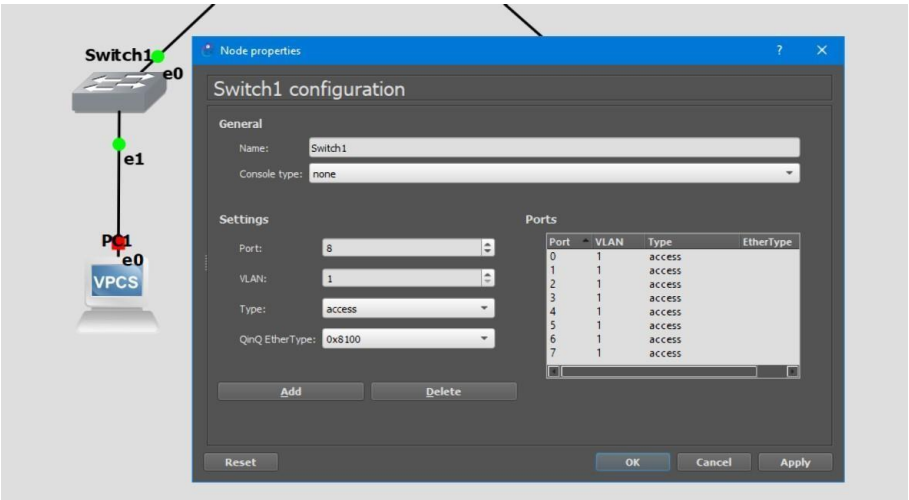


Nota. Aquí se arranca el Router 1 dando clic derecho sobre el equipo.

Esto se realizara con los equipos que se encuentren apagados, se puede apreciar en la figura 118, que los swtichs parecerían ya están ejecutados, esto se debe a que al ser equipos solo de simulación, únicamente cumplen con funciones básicas si se intenta abrir la consola este proceso no funcionara, por lo que para este tipo de switch se los puede configurar únicamente por la opción “configure” donde una ventana permitirá configuraciones básicas como cambiar el nombre, la cantidad de puertos, vlans, etc. como se muestra en la figura 119.

Figura 119

Configuración de Switch.

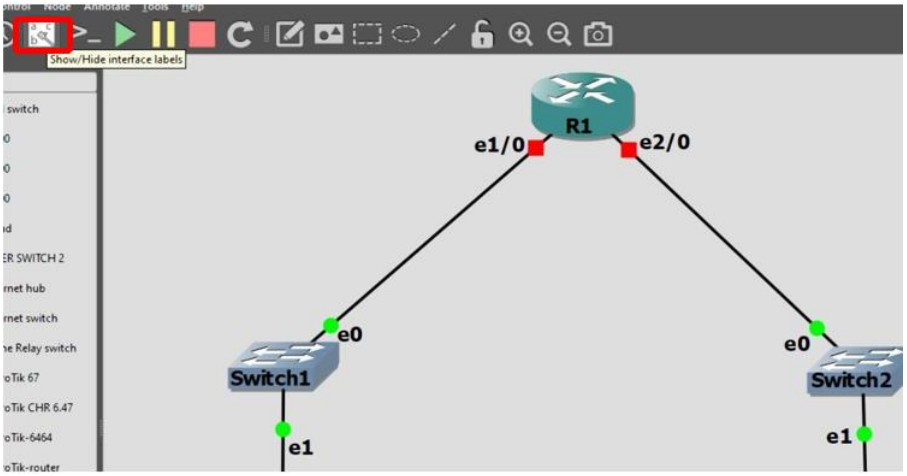


Nota. Aquí se configura el Switch 1 en modo de configuración.

Para poder mostrar las etiquetas de los puertos se debe dar clic sobre la opción “show/hide interface labels” en el menú superior. Esto permite que se visualice el nombre y el número de puerto en que se ha conectado un equipo. Como se muestra en la figura 120.

Figura 120

Número de puertos conectados

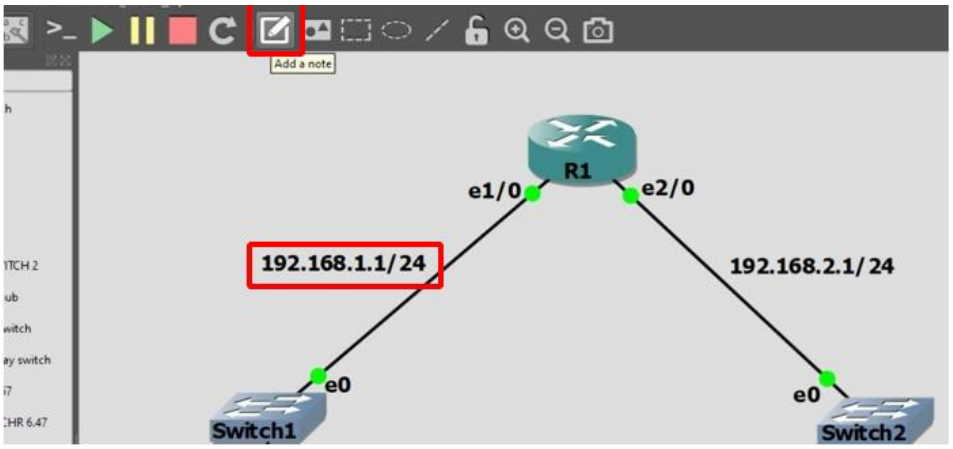


Nota. Aquí se encienden los puertos del switchs y se muestran los puertos ethernet.

Una vez que se hayan encendido los equipos, la topología estará lista para ser configurada, primero se escribirá la dirección IP, se puede escribir esto dentro de la topología por medio de la opción “add note” como se muestra en la figura 121.

Figura 121

Establecer dirección IP.

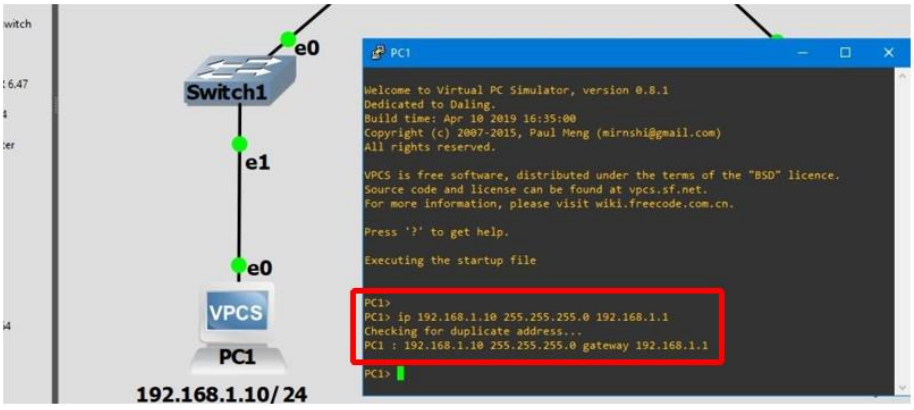


Nota. Aquí se debe dar clic en el icono del cuadrado con un lápiz para escribir notas.

Primero se va a establecer las direcciones IP, para lo cual se debe entrar al modo consola de los PC y por medio de los siguientes comandos establecer la respectiva dirección IP lo que se muestra en la figura 122.

Figura 122

Establecer las direcciones IP a las VPCS.

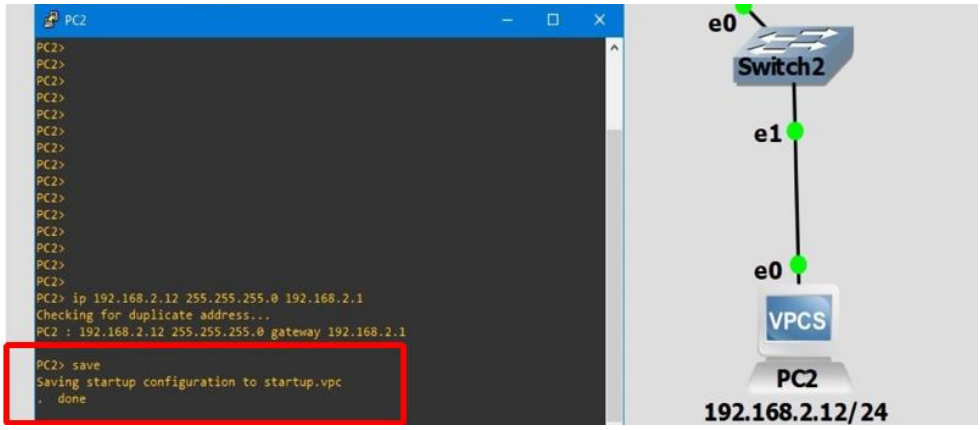


Nota. Primero se comienza con el direccionamiento en VPCS.

De esta forma se establece tanto la dirección IP con su respectiva mascara y la dirección Gateway, y para guardar las configuraciones realizadas se ejecuta el comando “save” como se muestra en la figura 123.

Figura 123

Establecer la dirección de Gateway

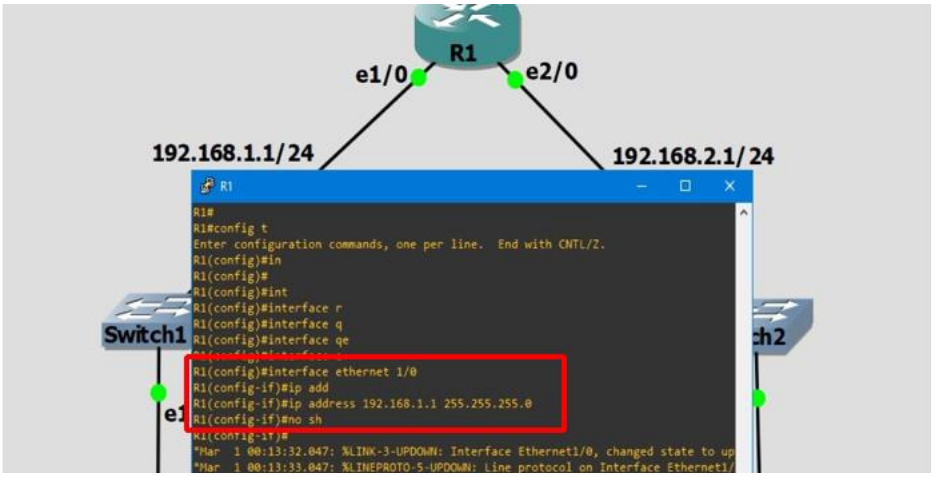


Nota. Comando save en PC2.

Ahora se debe establecer las direcciones IP en los puertos correspondientes en el router 1, para lo cual se debe ingresar al modo consola de este y ejecutar los comandos que se muestran en la figura 124, instrucciones que se usan en la práctica para equipos CISCO.

Figura 124

*Establecer direcciones IP en Router 1***.**

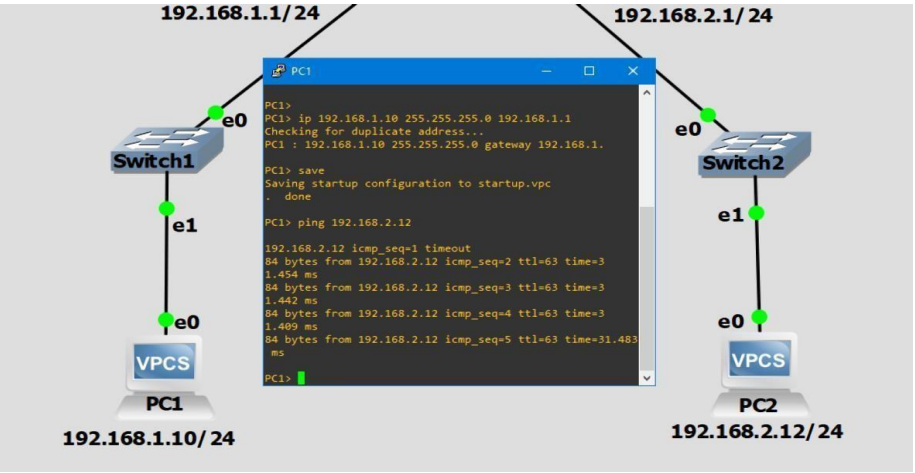


Nota. Se habilita las interfaces de ethernet y habilitar.

Una vez que se hayan establecido las direcciones correspondientes en ambos puertos, se comprueba el funcionamiento realizando un envío de paquetes desde la PC1 hacia la PC2 como se muestra en la figura 125.

Figura 125

Ping de PC1 a PC2



Nota. Aquí se comprueba que exista conexión de PC1 a PC2.

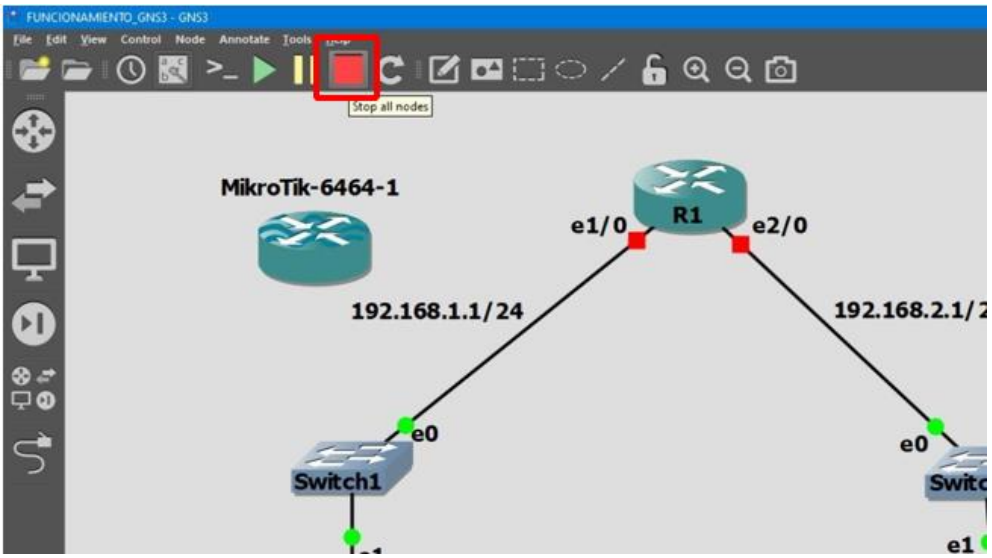
Archivos/Proyectos de GNS3 (Puntos de restauración "Snapshots")

GNS3 al ser un programa que emula dispositivos de red, técnicamente no habría información a guardar, ya que en los equipos ya sean routers, switches, maquinas PC, etc. se debe guardar su propia configuración de manera manual lo cual depende de cada equipo emulado en la topología.

GNS3 ofrece una opción en la cual se pueden crear puntos de restauración de la red creada, el programa lo denomina "Snapshots" y a continuación de muestra como añadir estos puntos de restauración al proyecto. Bajo la topología que se esté trabajando para producir un "snapshot" es necesario que todos los equipos estén apagados, previo a esto recordar guardar la configuración realizada en cada uno de ellos. Para detener a los equipos se puede dar clic en la opción "stop all nodes" en la barra de herramientas. Como se muestra en la figura 126.

Figura 126

Ejemplo de snapshot

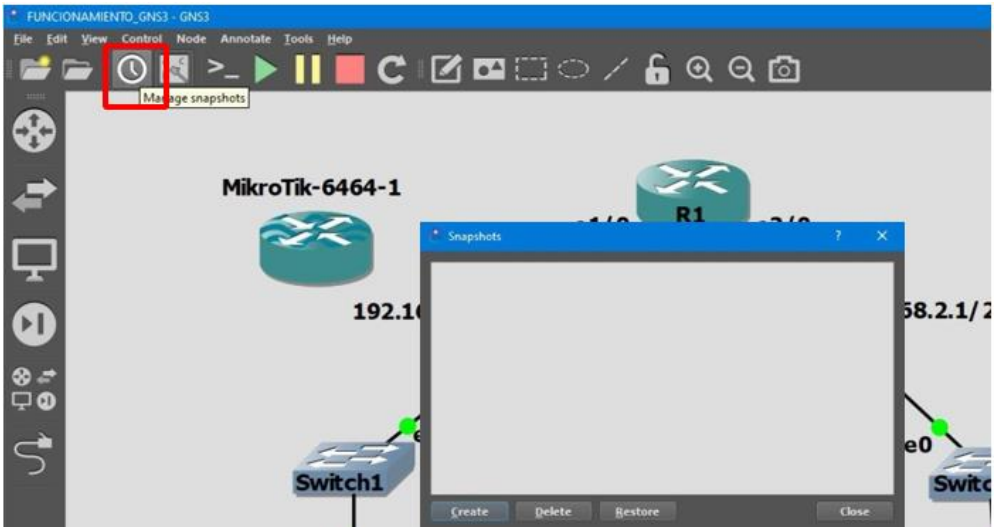


Nota. Con el botón rojo se puede suspender los equipos de la red.

A continuación, se debe dar clic en la herramienta “Manage snapshots” el cual se muestra con el símbolo de un reloj. En el cual una ventana aparecerá en el medio de la interfaz de trabajo con el título Snapshots, tal y como se muestra en la figura 127.

Figura 127

Herramienta Manage snapshots

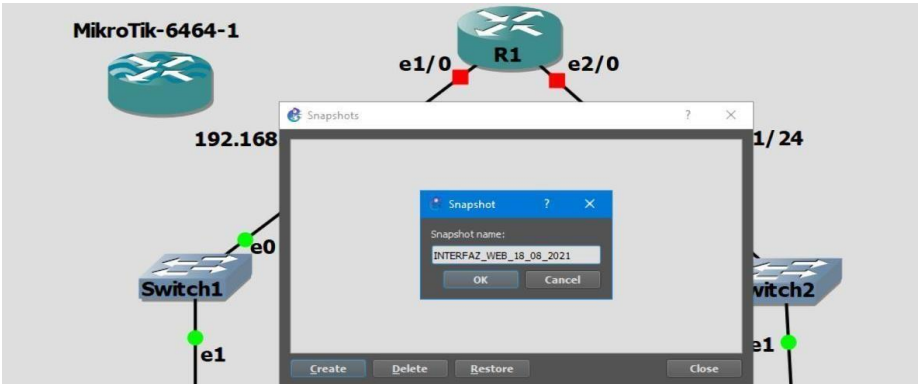


Nota. El icono del reloj representa los snapshots.

Para crear un punto de restauración se da clic en la opción “créate” el cual solicitara al usuario que se establezca el nombre con el cual se va a guardar el snapshot, se recomienda poner el nombre de una configuración en específico para determinar el momento en que se establece la restauración, así como se muestra en la figura 128.

Figura 128

Crear punto de restauración.

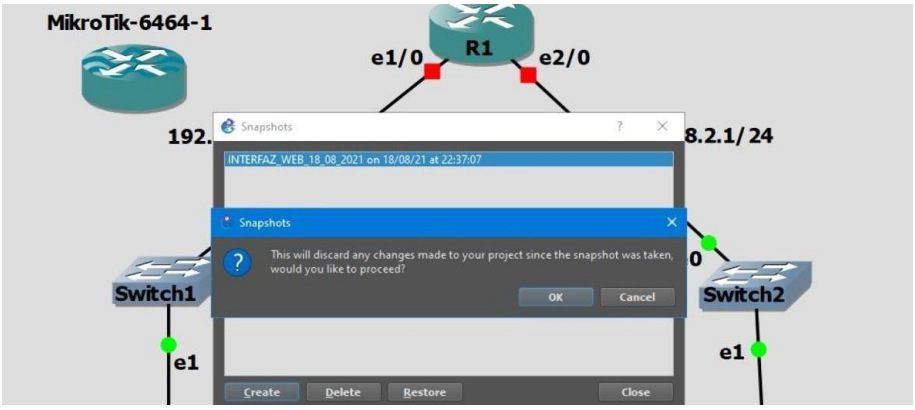


Nota. En caso de que se dañe la red se puede regresar al punto de “snapshot”

Por siguiente, se da clic en OK y se podrá observar que existe un listado sobre todos los snapshots creados para el proyecto. Y al momento de abrir uno de estos puntos de restauración se mostrará una alerta, así como se presenta en la figura 129.

Figura 129

Puntos de restauración creados.



Nota. Se puede regresar a los puntos de restauración anteriores**.**

Ese mensaje notifica al usuario que cualquier cambio realizado sobre la topología de red será eliminado y la red volverá al estado en que se estableció el punto de restauración.

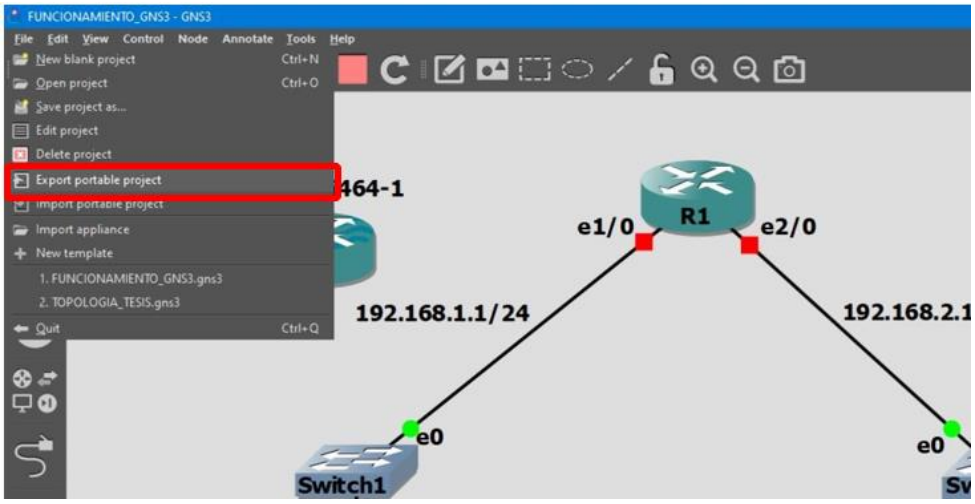
Archivos/Proyectos de GNS3 (Importación y Exportación de proyectos)

Los trabajos en GNS3 se pueden exportar como proyectos y ser instalados en otras computadoras, esto es muy útil para continuar los procesos de red sin importar donde se encuentre el usuario. Para Exportar un proyecto de GNS3 se debe seguir el siguiente proceso.

Primero todos los nodos que se involucren en la red deben estar apagados, teniendo en cuenta que los equipos deben guardar su propia configuración, respecto a cada dispositivo, y para exportar el proyecto se debe dar clic en la opción FILE del menú principal como se muestra en la figura 130.

Figura 130

Exportar proyecto portable.

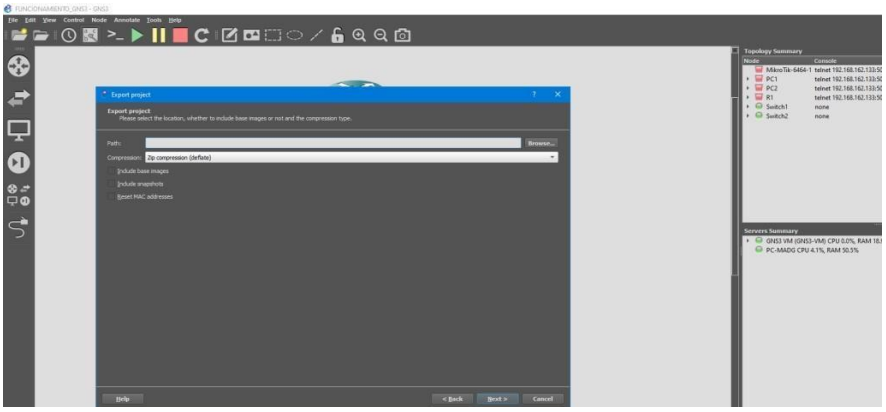


Nota. Aquí se puede importar proyectos que fueron creados en otra máquina se da clic en la opción import portable Project para poder abrir en otro computador diferente.

Al dar clic en la opción “Export portable Project” una ventana se abrirá como la que se muestra en la figura 131, donde se pide al usuario que se establezca la ubicación donde el archivo del proyecto se guardará.

Figura 131

Export portable Project.

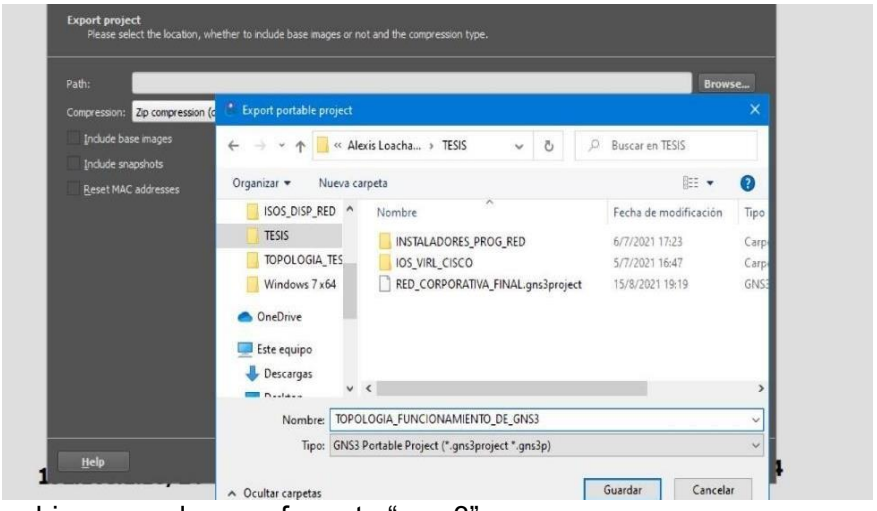


Nota. Se abre la carpeta y se guarda en el computador.

Por medio del botón “browse” un explorador de archivos permitirá al usuario determinar la ubicación para el proyecto, también es importante escribir el nombre del archivo. Tal y como se muestra en la figura 132.

Figura 132

Buscar los archivos en el ordenador.

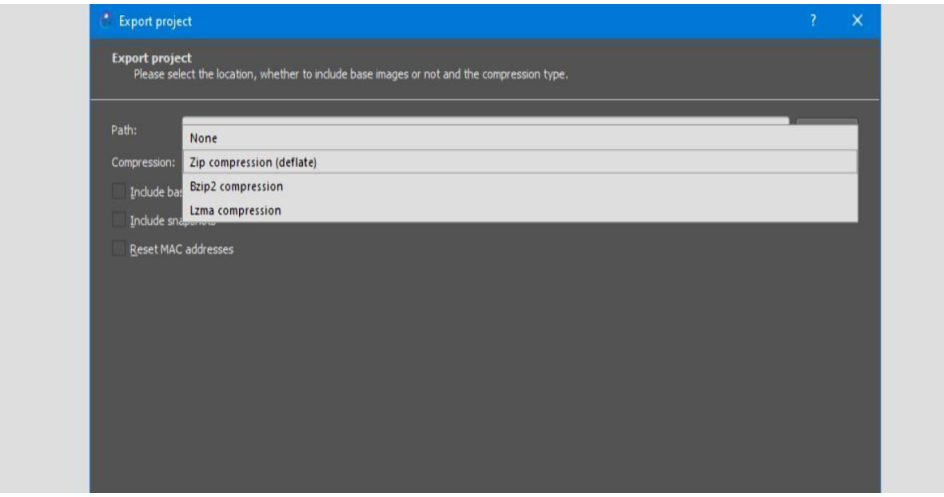


Nota. Los archivos creados son formato “.gns3”.

Por debajo de la ubicación del proyecto, el programa permite que se establezca la compresión que se quiere aplicar al archivo, a pesar de que se establezcan como archivos ".gns3" la compresión permite que todos los equipos, así como su respectiva configuración se guarden. Existen varias opciones para esta compresión, pero se recomienda que se establezca el tipo "Zip compression(deflate)"

Figura 133

Export Project.

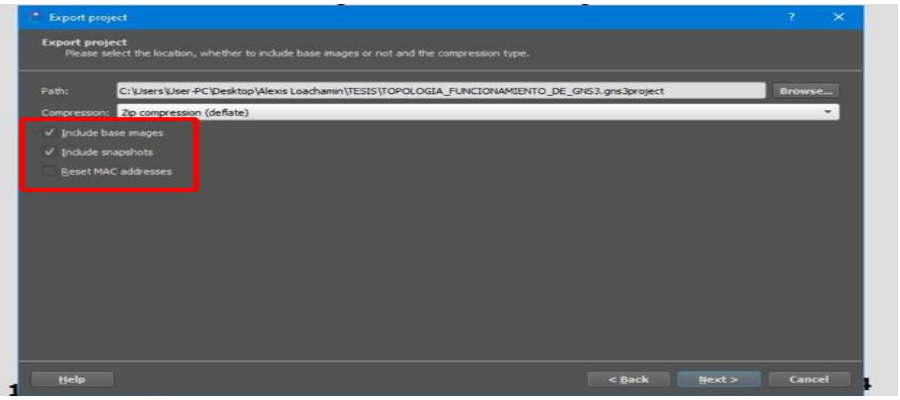


Nota. Otro tipo de compresiones son "Bzip2" y "Lzma".

A parte de estas configuraciones el programa permite que se guarden opciones extras, como las imágenes que se han instalado y usado en la topología, y de igual forma los respectivos snapshots que se han creado, la tercera opción permite al usuario que al importar el archivo en una nueva computadora se reinicie las direcciones MAC, se recomienda marcar las dos primeras opciones como se muestra en la figura 134.

Figura 134

Opciones extra.

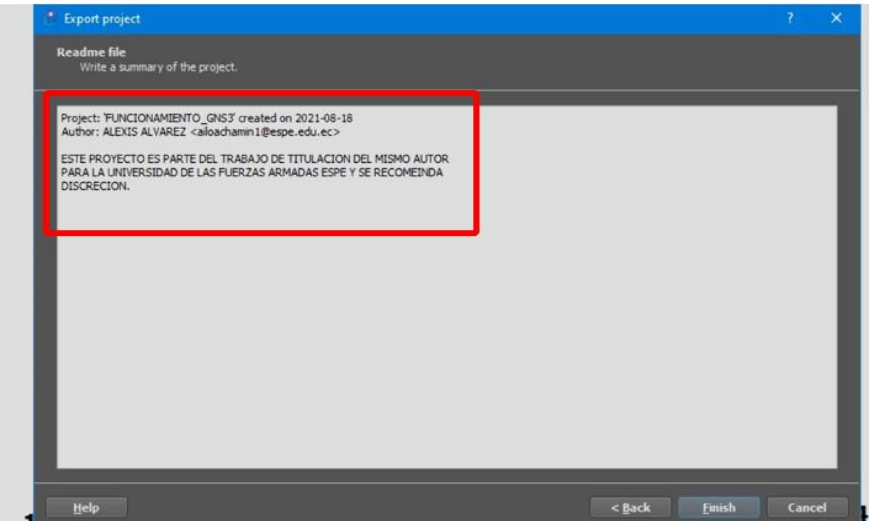


Nota. Se puede incluir otras opciones necesarias.

Finalmente se debe dar clic en la opción “Next” en donde se describe detalles por defecto acerca proyecto, así como al autor del mismo, se debe cambiar estos detalles por los del usuario que realizo la topología, así como se muestra en la figura 135 y al finalizar se debe dar clic en FINISH

Figura 135

Exportar Proyecto con datos

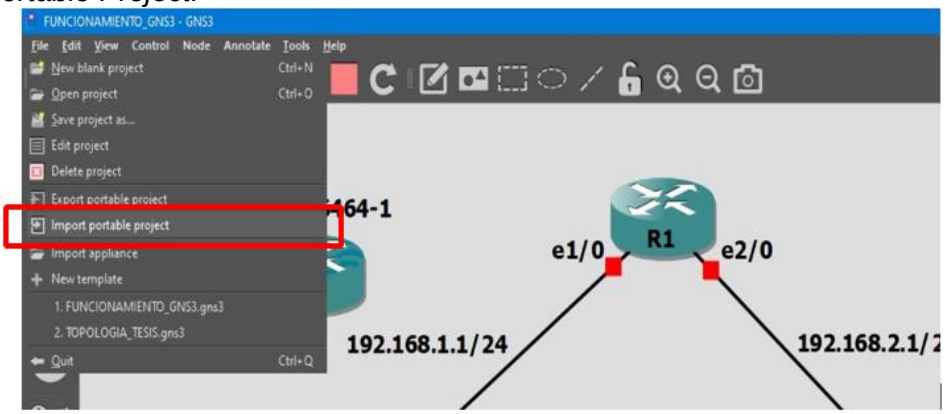


Nota. Se asigna los datos de los colaboradores de la red.

Y finalmente el archivo portable se habrá creado, en el destino establecido, y para poder importar estos archivos únicamente basta con dar clic en la opción “import portable project” del menú desplegable de la opción “file” así como se muestra en la figura 136.

Figura 136

Import portable Project.

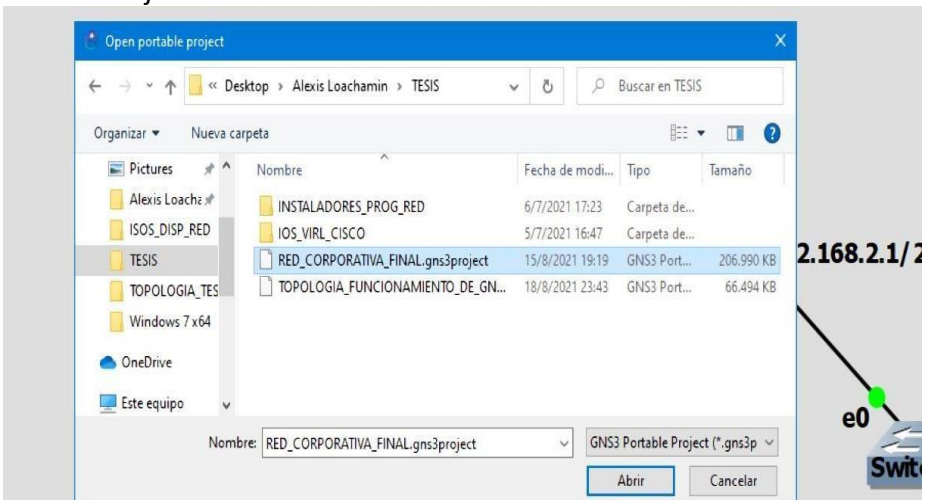


Nota. Los archivos serán tan pesados como la topología de red se haya dispuesto.

Un explorador de archivos permitirá abrir los archivos portables, así como se puede mostrar en la figura 137, lo que cargará todos los componentes, las imágenes, la topología, así como en la figura 138.

Figura 137

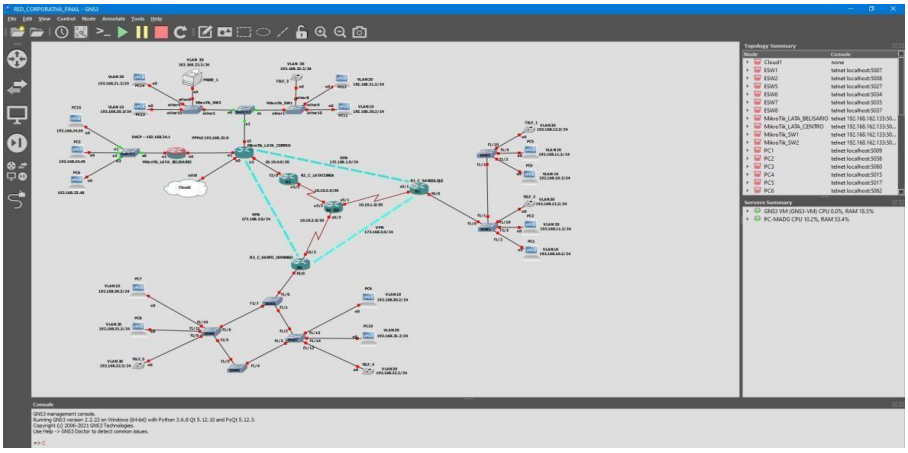
Open portable Project.



Nota. En el explorador de archivos se puede encontrar varios archivos de GNS3.

Figura 138

Red corporativa.



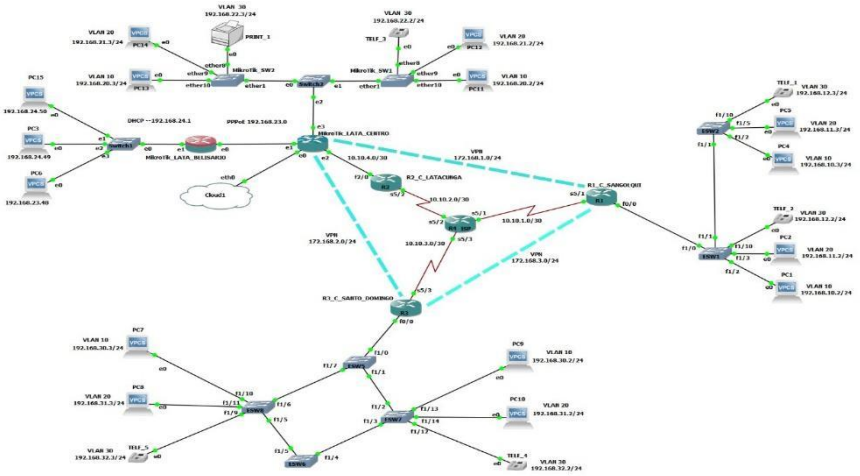
Nota. Se puede abrir archivos de distinto ordenador ya sea la topología más compleja con todos los dispositivos de la red y respectivas configuraciones.

Implementación Red Corporativa ESPE en GNS3

Para demostrar la capacidad del programa GNS3 se realizará una red de datos de la Universidad de las Fuerzas Armadas ESPE con sus respectivos campus en las ciudades correspondiente, contemplando diferentes protocolos, equipos, situaciones bajo las cuales una red de datos real funciona.

Figura 139

*Topología general Red de datos ESPE***.**



Nota. Ejemplo de la interfaz de trabajo de GNS3 que se denomina GUI.

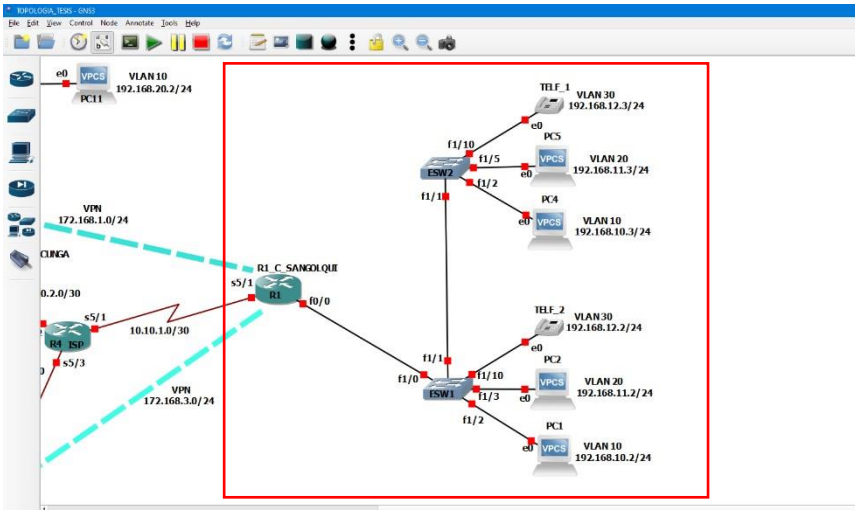
Red Sucursal Sangolquí

Primero se establecerá la red del campus ESPE-Sangolqui siguiendo el diagrama organizacional de la Universidad, se decide implementar protocolos VLANS y su respectivo enrutamiento, la topología a trabajar para este campus es la que se muestra en la figura 140.

Se arrastra los componentes y se los conecta según se muestra en la figura 139, se comienza con la red LAN de Sangolquí la cual se detalla en la figura 140, se inicia todos los dispositivos correspondientes a esta red con clic derecho sobre el equipo y presionando la opción “start”, como se muestra en la figura 141.

Figura 140

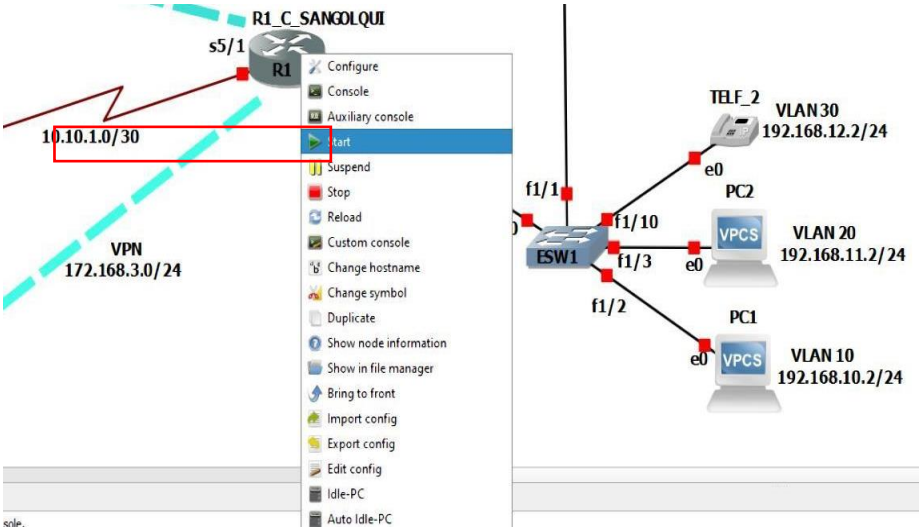
Red de área local de ESPE Sangolquí.



Nota. No representa en realidad la red de la institución ESPE

Figura 141

Encender R1_C_S ANGOLQUI.

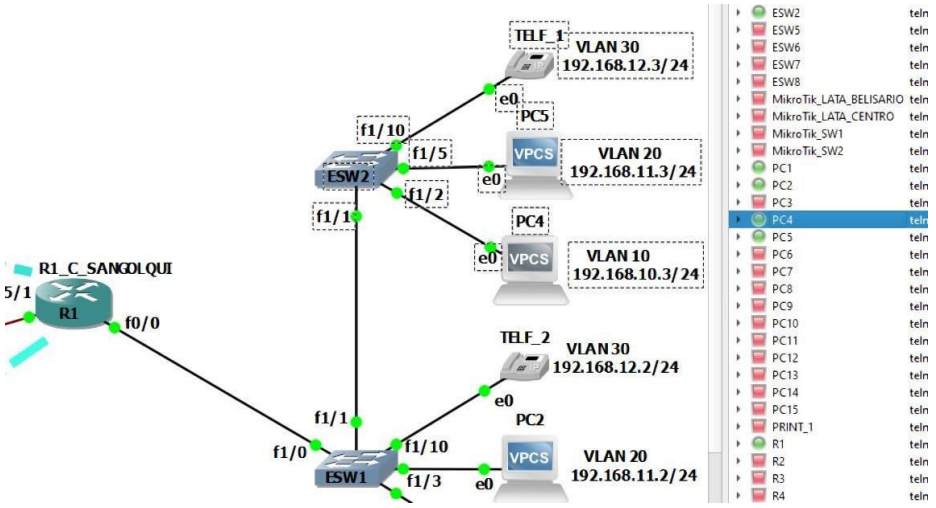


Nota. Para encender el equipo es por medio del símbolo de triangulo verde.

Una vez encendidos los equipos se observa en la derecha el estado de los mismos, si están encendidos, o suspendidos, a diferencia del resto de equipos que se encuentran apagados.

Figura 142

Estado de los equipos en red LAN Sangolquí.

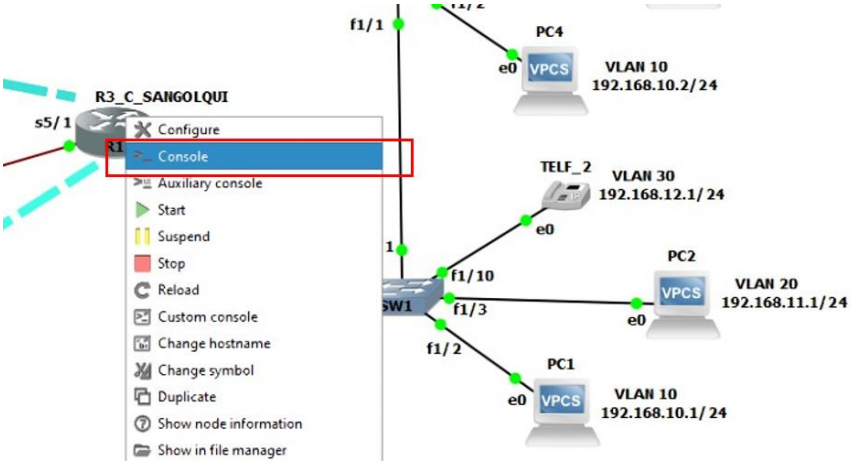


Nota. Topology Sumary muestra el estado de todos los equipos.

Para configurar cada uno de los equipos para esto se tendrá que dar clic derecho sobre los mismos y presionar la opción “CONSOLE” como se muestra en la figura 143.

Figura 143

Entrada por consola de los equipos.

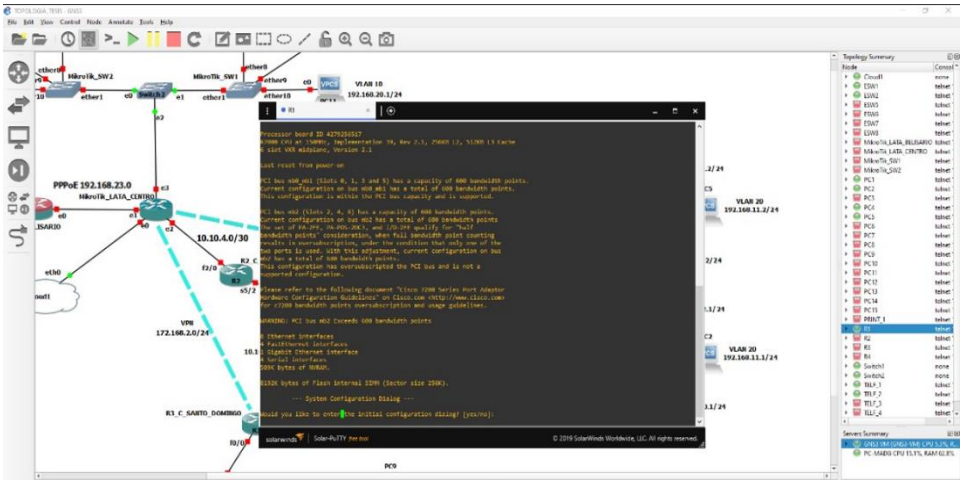


Nota. El acceso a la consola es para equipos en emulación.

Enseguida abrirá el programa Solar-PuTTY por parte de la empresa Solarwinds, este aplicativo permite visualizar la consola de comandos de los diferentes dispositivos. Tal y como se muestra en a la figura 144.

Figura 144

Acceso a la consola Solar Putty.

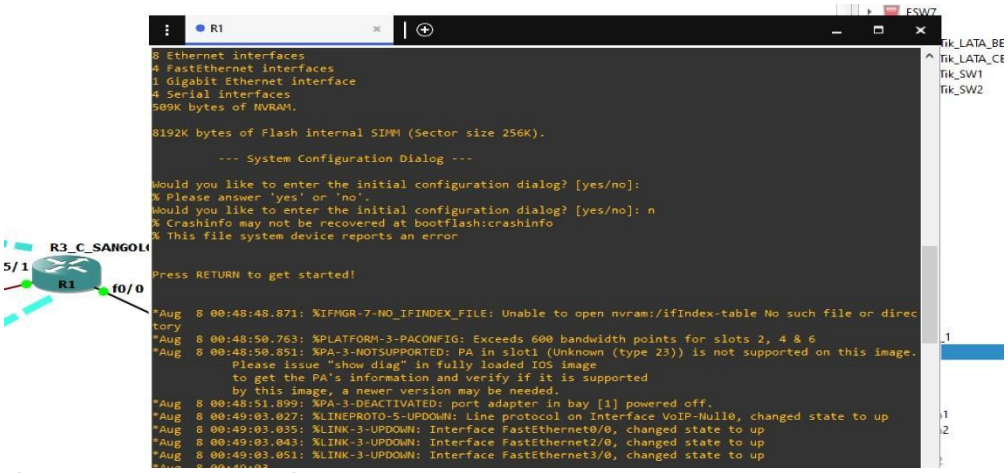


Nota. Solar-Putty pertenece a la empresa Solar winds.

Si es la primera vez en la consola del equipo es muy posible que un cuadro de dialogo requiera la confirmación para configuraciones iniciales, para esta red corporativa no se hará uso del mismo y se digita “no” o “n” como en la figura 145.

Figura 145

Consola para equipos CISCO en Solar-PuTTY.



Nota. Díalogo de configuración inicial denegado.

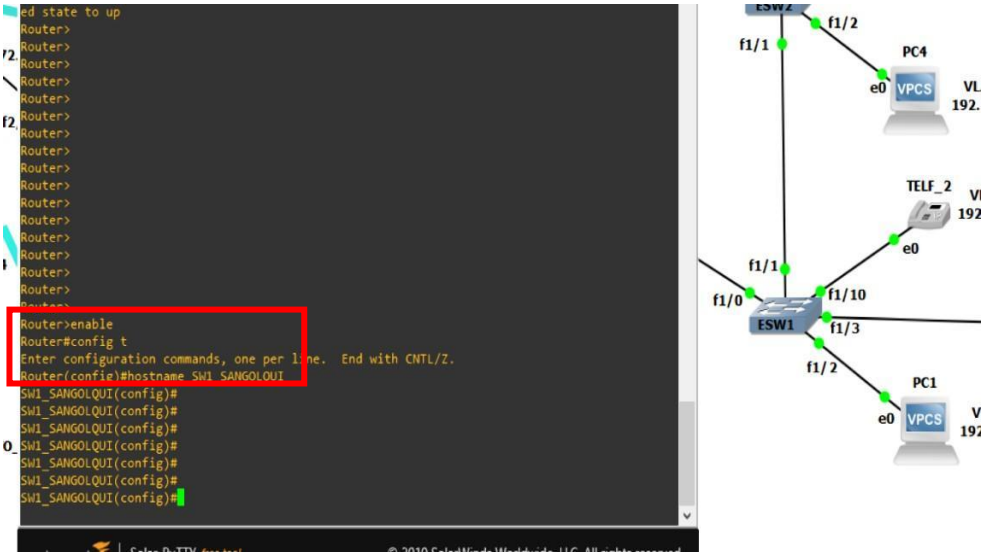
Red Sucursal Sangolquí (Implementación de VLANS)

Para iniciar se ingresa a los switchs para cambiar el nombre por defecto ya que los mismos al ser routers emulados como switchs las etiquetas no corresponden de manera en que ejecutando los siguientes comandos, asigna los nombres a estos dos equipos, como se muestra en la figura 146.

```
Router> enable
Router# configure terminal
Router(config)# hostname SW1_SANGOLQUI
```

Figura 146

Cambió de nombre de equipos CISCO



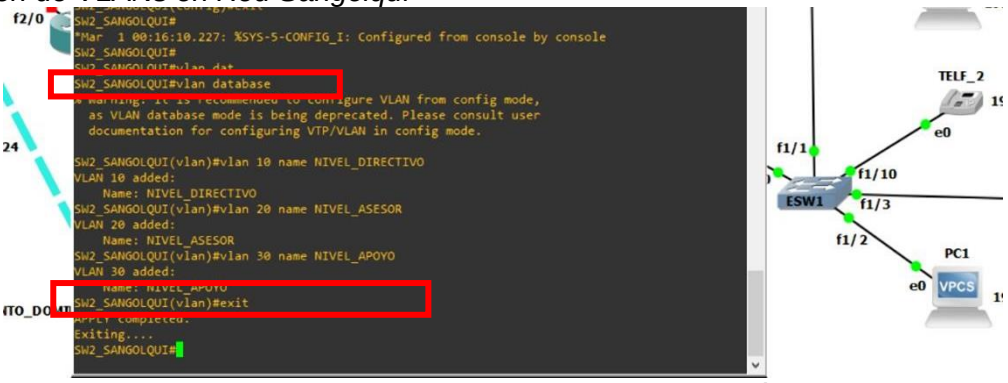
Nota. Una vez establecido los comandos, el nombre cambiara inmediatamente.

Ahora se crearán VLAN's dentro de los switchs en la configuración global se ejecutan los siguientes comandos donde se asigna los nombres e identificación por número de las redes de área local virtuales, se realizará este proceso hasta completar 3 vlans con los nombres que se muestran en la figura 147

```
SW1_SANGOLQUI#vlan database
SW1_SANGOLQUI(vlan)# vlan 10 name NIVEL_DIRECTIVO
```

Figura 147

Creación de VLANs en Red Sangolquí



Nota. Al ejecutar el primer comando un mensaje de recomendación aparece.

Esto realiza en los dos equipos de conmutación (switch) que estén dentro de la red LAN de Sangolquí, con los mismos números y nombres. Para mostrar que las redes virtuales se hayan creado correctamente se ejecuta el siguiente comando.

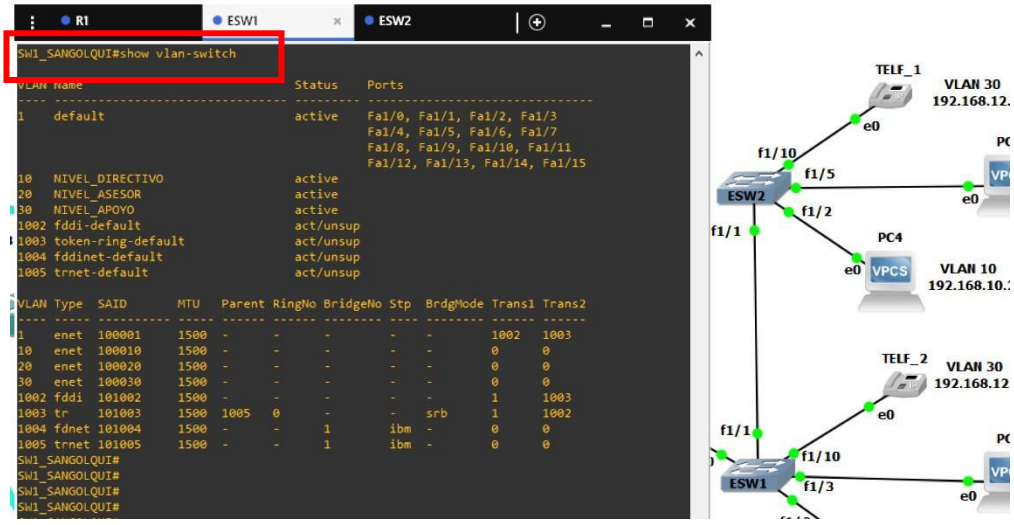
```
SW1_SANGOLQUI#show vlan-switch
```

Si se desea observar de manera más resumida el estado de las vlans creadas también se puede ejecutar el siguiente comando.

```
SW1_SANGOLQUI#show vlan-switch brief
```

Figura 148

*Verificación de vlans creadas***.**



Nota. Los comandos que se muestran en la figura 158 pueden cambiar dependiendo del equipo.

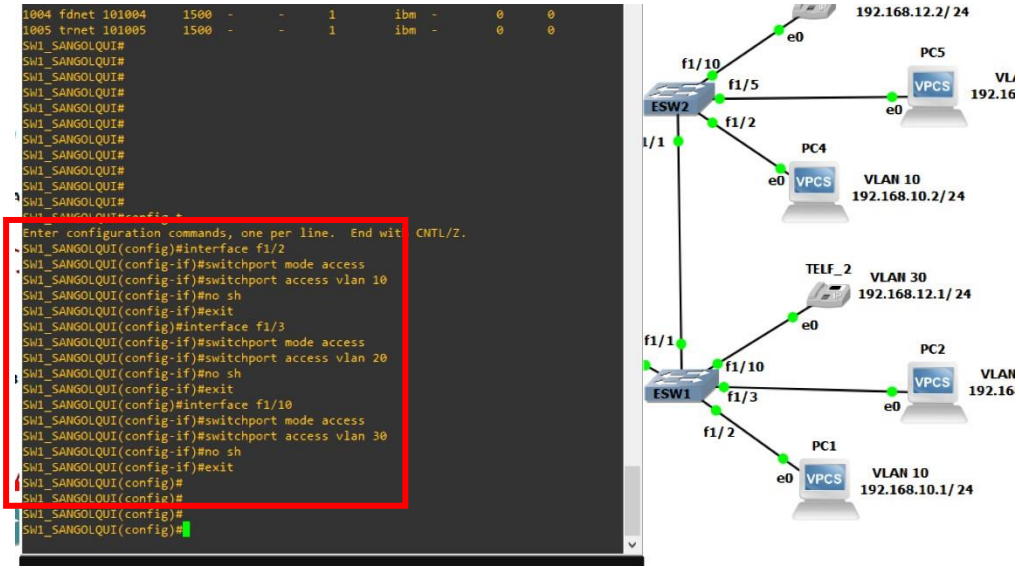
Ahora dentro de los equipos switch se debe asignar las interfaces que deben estar configuradas en modo acceso las cuales deben ser las conexiones que se dirijan a las las PCs las cuales están asignadas para cada VLAN como se muestra en la figura 148. Y para realizar esto se digitan los siguientes comandos.

```
SW1_SANGOLQUI#config t
SW1_SANGOLQUI(config)#interface f1/2
SW1_SANGOLQUI(config-if)#switchport mode access
SW1_SANGOLQUI(config-if)#switchport Access vlan 10
SW1_SANGOLQUI(config-if)#no sh
```

Cabe mencionar que los comandos descritos previamente y en anteriores puntos sirven como ejemplos de demostración por lo que es importante seguir el proceso según sea el seguimiento de la topología, por ejemplo, en la figura 149 se establece la configuración para el resto de interfaces.

Figura 149

Interfaces en modo acceso para SW1_SANGOLQUI

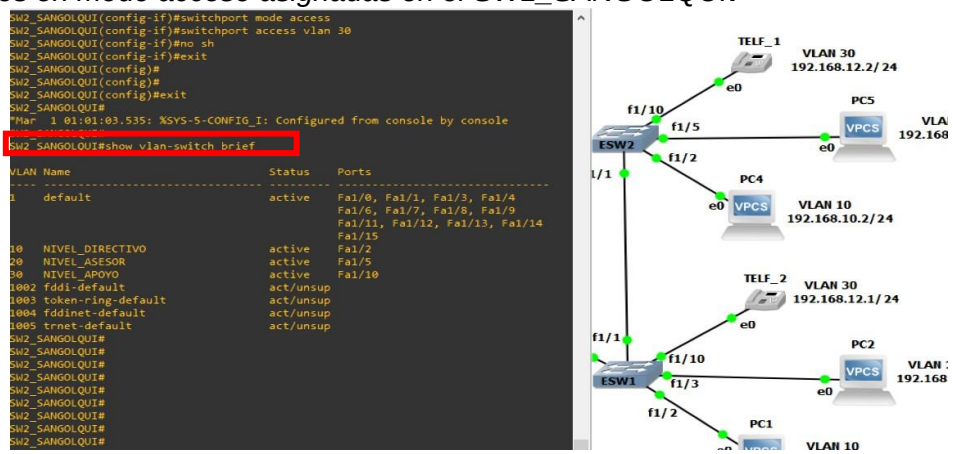


Nota. Se debe realizar el mismo proceso en SW2_SANGOLQUI.

Se vuelve a verificar las vlans por el comando #**show vlan-switch brief y** en ambos switchs se deberá mostrar las interfaces en modo acceso hacia las vlans correspondientes. Como se muestra en la figura 150.

Figura 150

*Interfaces en modo acceso asignadas en el SW1_SANGOLQUI***.**



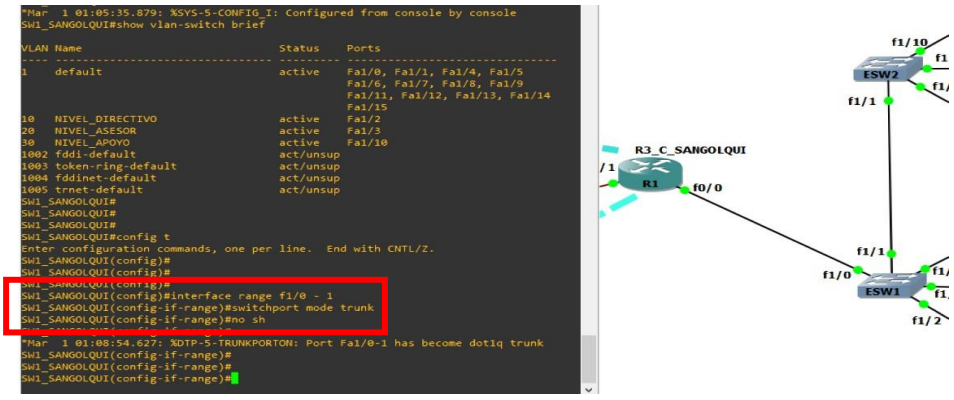
Nota. El resto de interfaces están asignados a la vlan 1 por defecto.

Para los equipos switch de la red Sangolquí se debe entra a la configuración privilegiada y a asignar los puertos troncales con las respectivas interfaces que se muestran en la topología. Por medio de los siguientes comandos.

```
SW1_SANGOLQUI(config)#interface range f1/0 - 1
SW1_SANGOLQUI(config-if)#switchport mode trunk
SW1_SANGOLQUI(config-if)#no sh
```

Figura 151

Puertos de enlace troncal para SW1_SANGOLQUI



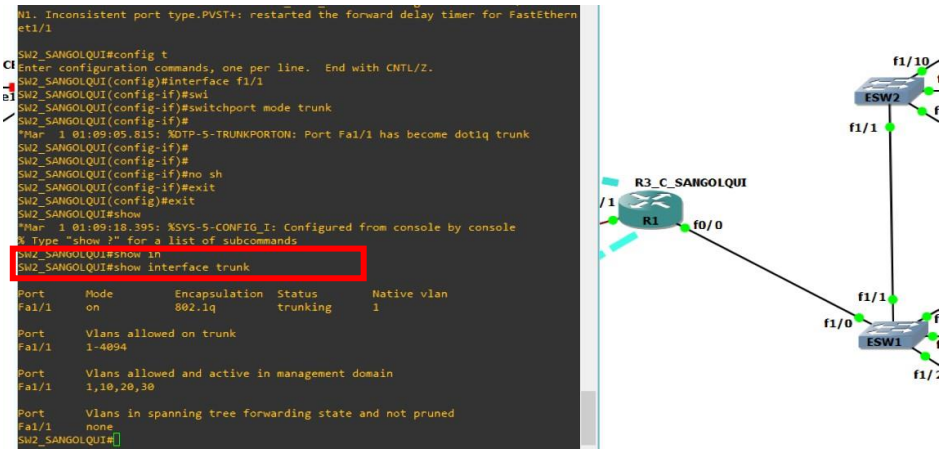
Nota. Para configurar interfaces consecutivas se usa el comando **interface range.**

Se realiza el mismo proceso en SW2_SANGOLQUI y para verificar que las configuraciones han sido correctas por medio del siguiente comando

```
SW1_SANGOLQUI# show interface trunk
```

Figura 152

Demostración de interfaces troncales en SW2_SANGOLQUI



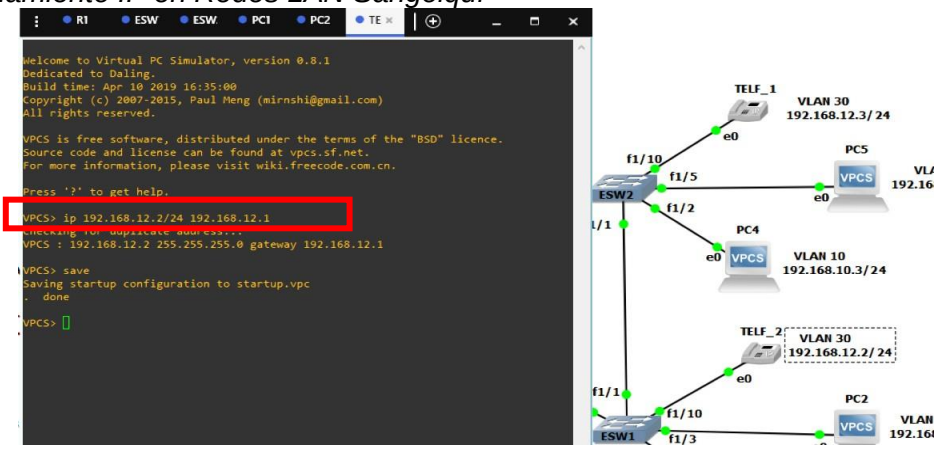
Nota. Para SW2_SANGOLQUI se muestra una interfaz en modo troncal.

Ahora las vlans pueden hacer conexión punto a punto para comprobarlo se asigna las direcciones IP en las PCs dependiendo de la VLAN correspondiente. para lo cual se entra al modo consola de los mismos y se digita el siguiente comando.

```
VPCS> ip 192.168.12.2/24 192.168.12.1
```

Figura 153

Direccionamiento IP en Redes LAN Sangolquí

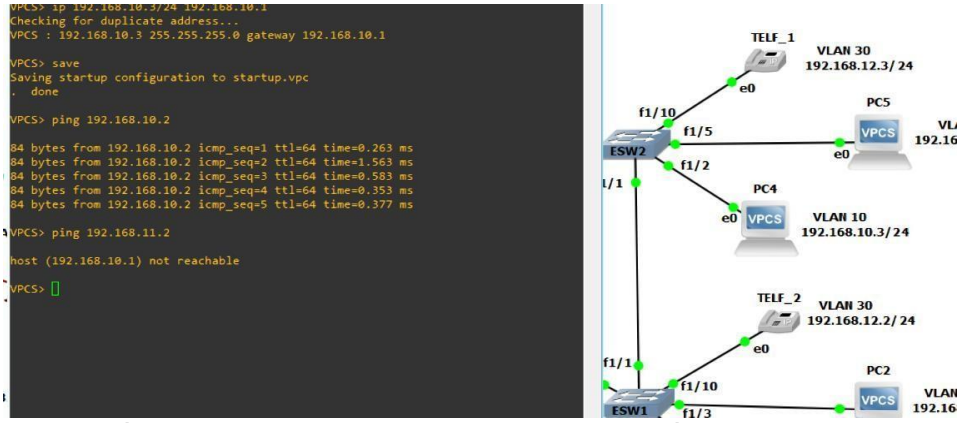


Nota. Se asigna la dirección de Gateway para su enrutamiento.

Se realiza envió de paquetes hacia destinos bajo el mismo segmento de red la conexión se realiza con éxito sin embargo si se intenta realizar conexión hacia otros dispositivos la conexión no realizara,

Figura 154

Conexión entre vlans sin enrutamiento.



Nota. La conexión por vlans elimina los dominios de difusión.

Red Sucursal Sangolquí (Enrutamiento de VLANS)

Para obtener conexión entre todas las VLANs es necesario un proceso de enrutamiento, para configurar este proceso debe dirigirse a la consola del router de la red Sangolquí y configurar las subinterfaces asignadas para cada VLAN's por medio de los siguientes comandos.

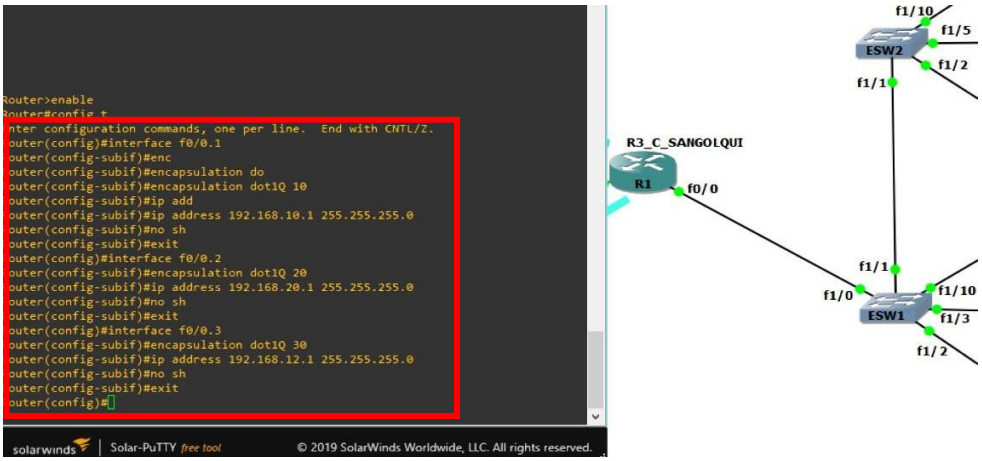
```
Router(config)#interface f0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.68.10.1 255.255.255.0
Router(config-subif)#no sh
```

Es importante tener en cuenta que el proceso de los comandos anteriores active las subinterfaces, las cuales son interfaces virtuales dentro de una interfaz física, por lo que es importante ejecutar el siguiente comando. cómo se presenta en la figura 155

```
Router(config)#interface f0/0
Router(config-if)#no sh
```

Figura 155

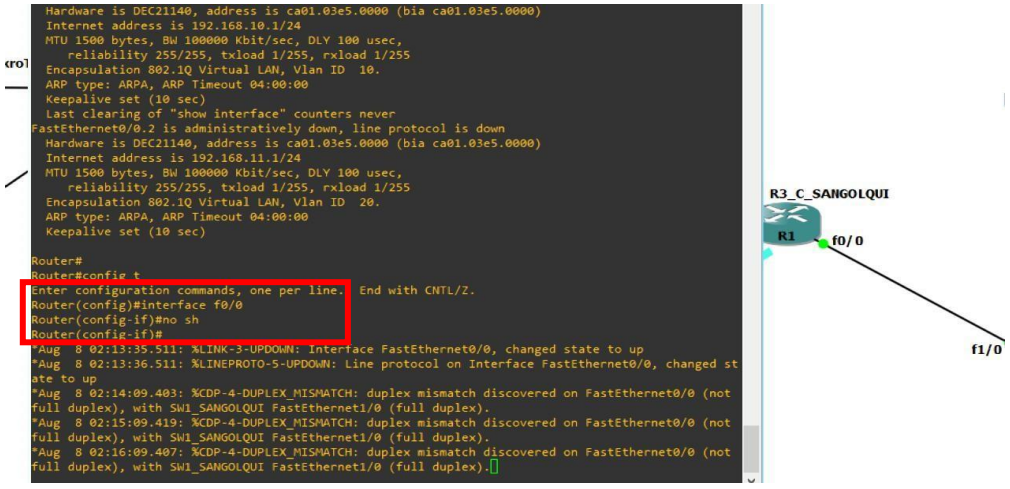
Enrutamiento de vlans en R1



Nota. Los identificadores en el comando encapsulación es el mismo que el número de las vlans.

Figura 156

Levantamiento de interfaz física.



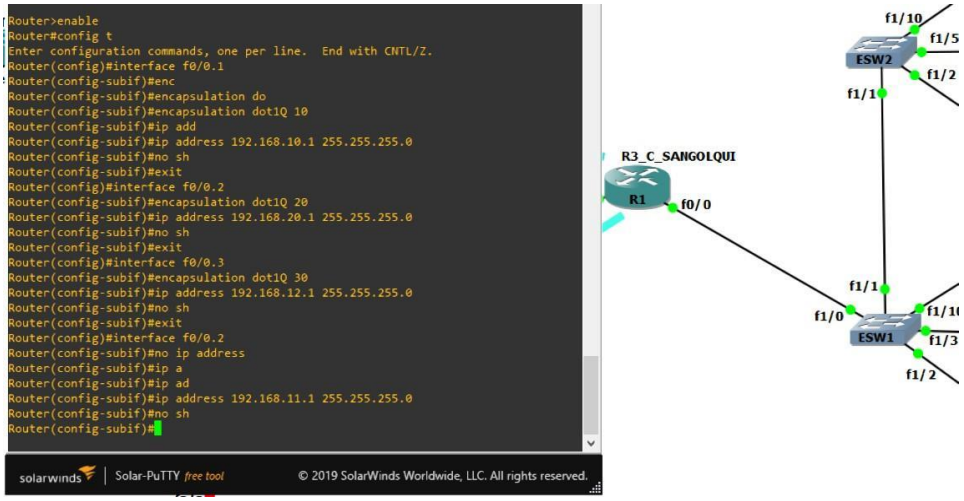
Nota. La interfaz física no se debe asignar como modo troncal.

Los errores de digitación pueden ser comunes como en la anterior figura la subinterface f0/0.2 tiene una dirección IP incorrecta para corregir se ejecuta el comando

```
Router(config-subif)#no ip address
```

Figura 157

Corrección de IP en encapsulación para vlan 20.



Nota. Es importante verificar las direcciones IP.

Para comprobar que la configuración es correcta ejecuta el comando **"#show run"** dentro de la configuración global, y debe buscar las subinterfaces que deben mostrar la dirección IP correspondiente, como en la figura 158.

Figura 158

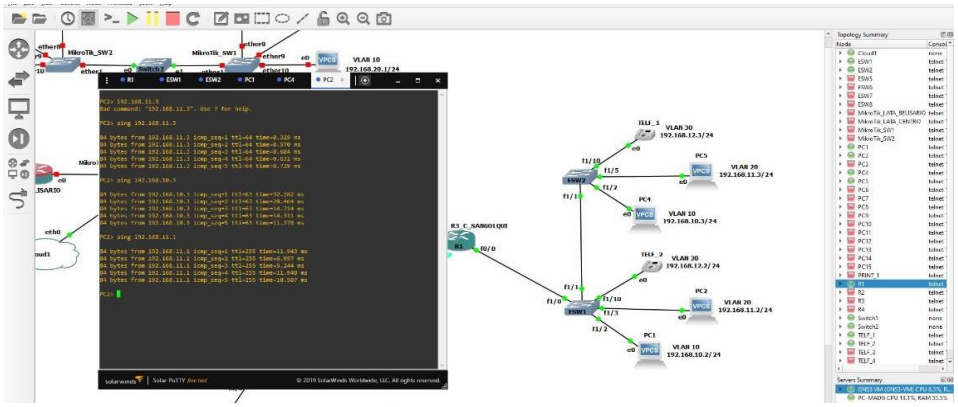
*Verificación de enrutamiento de vlans en R1***.**

Nota. Las subinterfaces deben aparecer por debajo de la interfaz física.

De esta manera se obtendrá todo el proceso de enrutamiento de VLans correspondiente. Y si se intenta realizar un ping desde distintos puntos de la red la conexión se realizará con éxito. Como se muestra en la figura 159.

Figura 159

Enrutamiento entre VLANs exitoso en Red Sangolquí.



Nota. El enrutamiento entre vlans permite conexión y seguridad.

Una vez concluida la Red LAN de Sangolquí se debe guardar las configuraciones en cada dispositivo para evita que todo el proceso se pierda, para esto ejecuta el siguiente comando. En los dispositivos de capa 2 y 3

```
SW2_SANGOLQUI#copy running config startup-config
```

Figura 160

Guardar configuración en Red Sangolqui

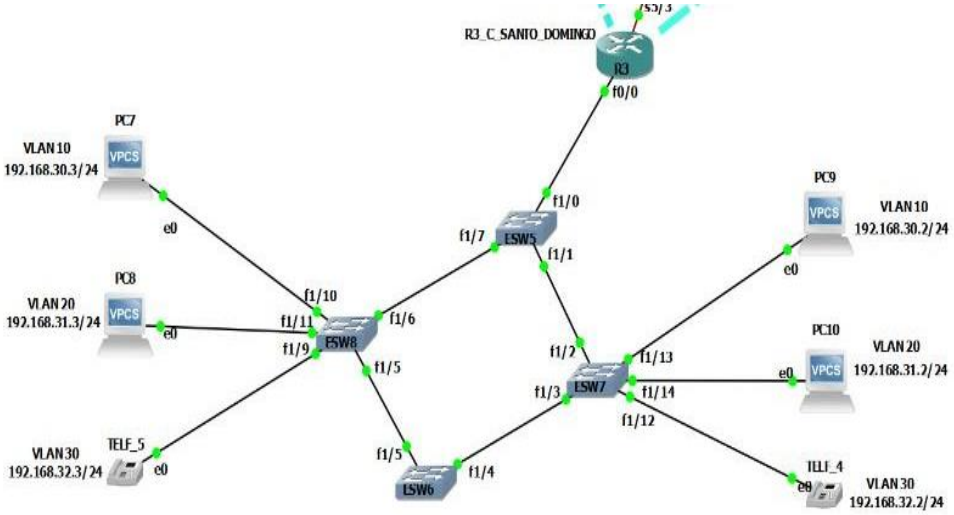
Nota. La configuración se graba en la memoria ROM.

Red Sucursal Santo Domingo

Para la red de santo domingo se configura el protocolo SPANNING TREE el cual permite la eliminación de bucles de transmisión cuando existe la conexión entre varios switchs. La red de santo domingo está establecida como se muestra en la figura 161.

Figura 161

Red ESPE Santo Domingo.



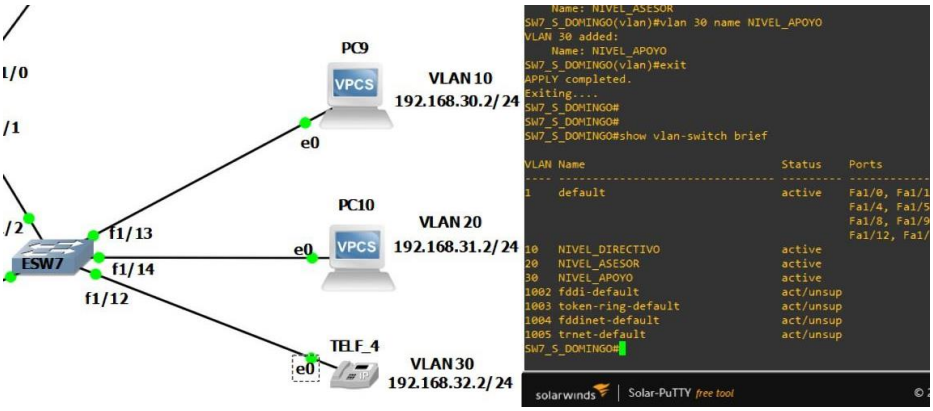
Nota. También se establecerá el uso de VLANS.

Red Sucursal Santo Domingo (Implementación de VLANS)

Una vez encendidos los dispositivos se crean las vlans correspondientes en cada uno de los switchs. Con el mismo proceso que haya visto en las redes de sucursales anteriores.

Figura 162

VLANS en red Santo Domingo.

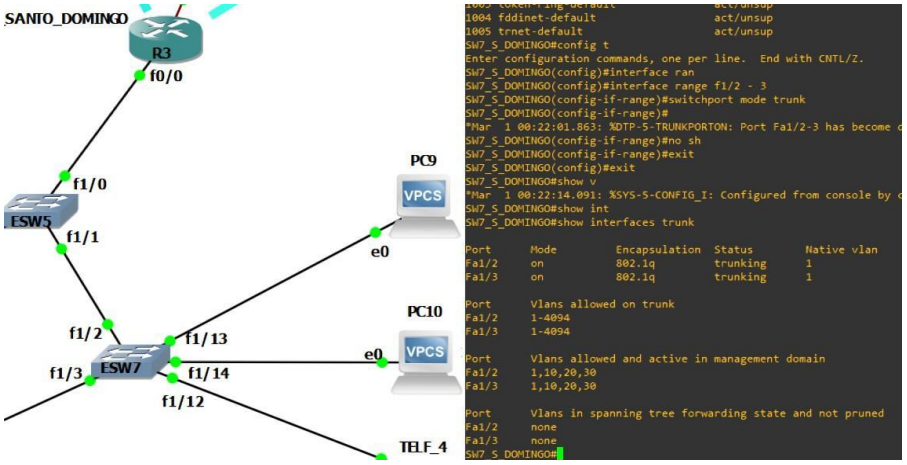


Nota. Las vlans mantienen los mismos detalles de la red anterior.

Se debe asignar los puertos troncales en los switches teniendo en cuenta que todas aquellas interfaces que sean destinadas para conexiones entre dispositivos del mismo tipo son configuradas en modo troncales como se muestra en la figura 163.

Figura 163

Interfaces en modo troncal para SW7_S_DOMINGO.



Nota. Las conexiones troncales se establecen para todas las vlans.

Red Sucursal Santo Domingo (Implementación de Spanning Tree)

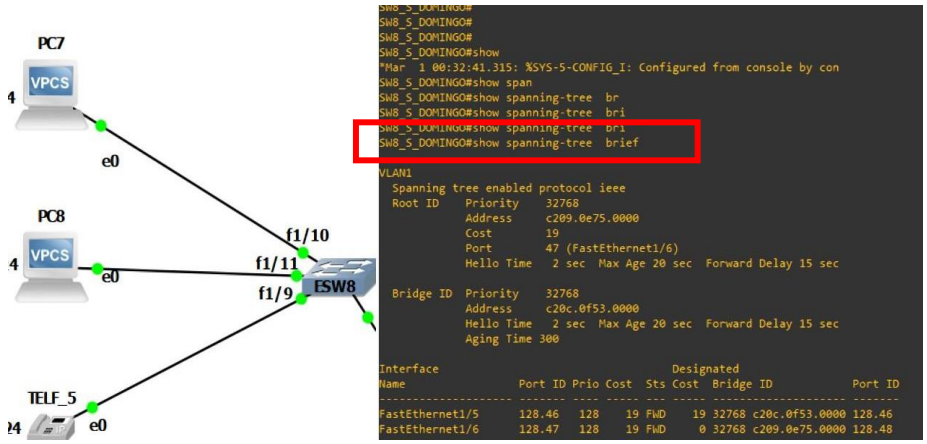
Para los equipos CISCO el protocolo Spanning Tree se encuentra por defecto iniciado y para verificar este parámetro se ejecuta el siguiente comando.

```
SW8_S_DOMINGO#show spanning tree
```

En donde la consola mostrara cual es la configuración para las prioridades de conmuta miento que tienen las vlans creadas previamente, como se muestra en la figura 164.

Figura 164

Spanning Tree por defecto en SW8_S_DOMINGO



Nota. Es importante valorar la prioridad y el costo.

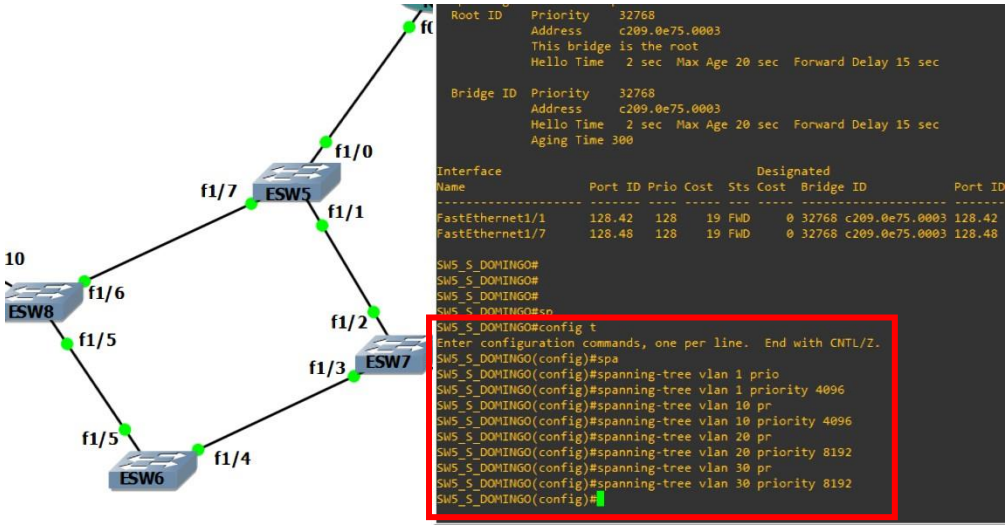
En este caso se puede observar las prioridades están asignadas automáticamente sin que ningún switch sea la raíz de ningún segmento de red por lo tanto se realiza la siguiente configuración ejecutando los siguientes comandos.

```
SW5_S_DOMINGO#config t
SW5_S_DOMINGO#spanning-tree vlan 10 priority 4096
```

Esto se debe repetir para el resto de redes virtuales (vlans) se hayan creado. Como se muestra en la figura 165.

Figura 165

Asignación de prioridades en SW5_S_DOMINGO

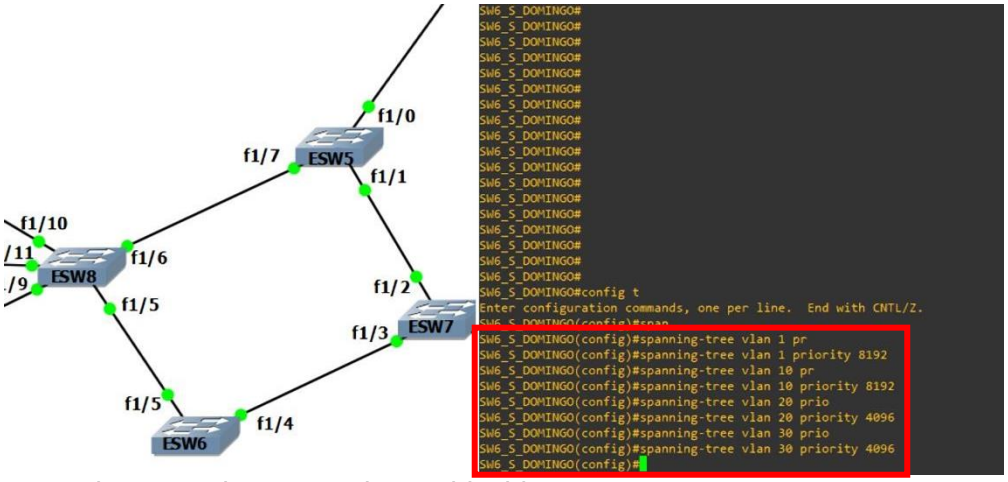


Nota. Las prioridades obtienen valores de 0 a 61440 en incrementos de 4096.

Esto determina en que nodos de la red las vlans deben tener más prioridad, de esta manera en el swtich 5 se le asigna una prioridad mayor para las vlans 20 y 30 pero este proceso lo invierte el switch 6, como se muestra en la figura 166.

Figura 166

Asignación de prioridades en SW6_S_DOMINGO.



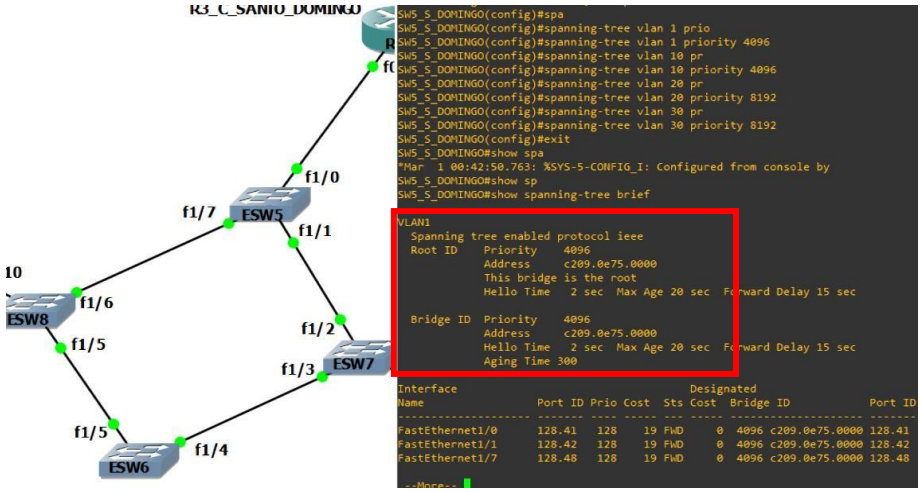
Nota. Los valores son inversos a lo establecido en SW5.

Al ejecutar el comando **“#show spanning-tree brief”** se observa como las prioridades para cada vlan han cambiado. En donde la prioridad “root” y del “bridge” es idéntica el switch en

cuestión será el “camino” por defecto, como se muestra en la figura 167. Pero para la figura 167 se observa como las vlans con diferente prioridad no presentan el mensaje “This bridge is the root” (este puente no es la raíz)

Figura 167

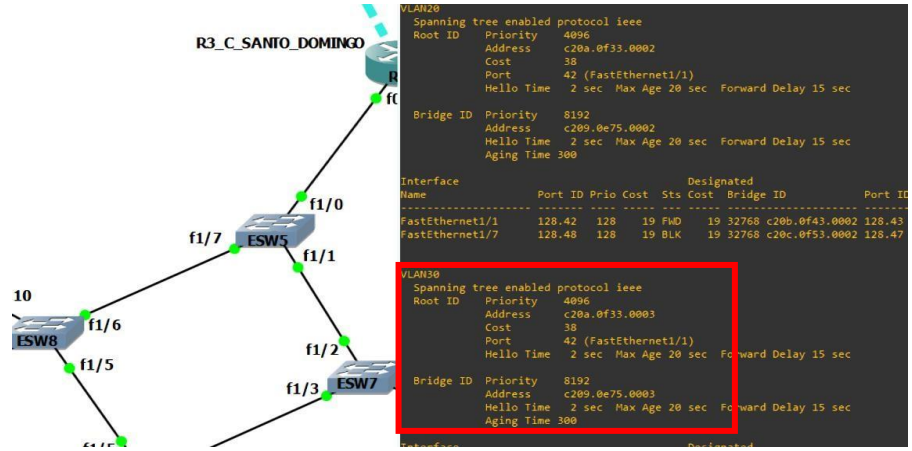
Nuevas prioridades iguales en SW5_S_DOMINGO



Nota. Para un costo de 19 la velocidad en el puerto será de 100MBs.

Figura 168

Nuevas prioridades diferentes en SW5_S_DOMINGO

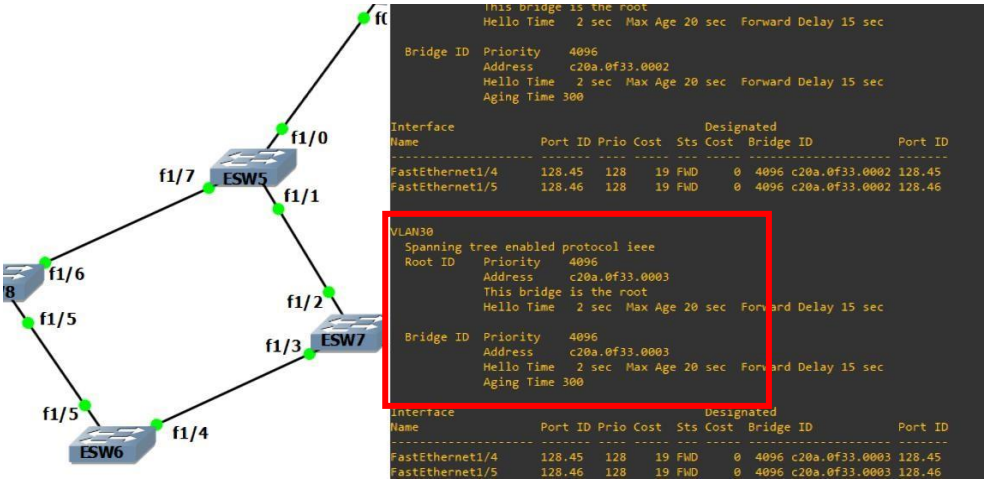


Nota. Para prioridades diferentes no se muestra el mensaje “this bridge is the root”.

La configuración debe ser contraria para el SW6_S_DOMINGO y se lo comprueba emitiendo el comando como en la siguiente imagen **“#show spanningtree brief”** en la configuración global del equipo. Como se muestra en la figura 169.

Figura 169

Nuevas prioridades en SW6_S_DOMINGO

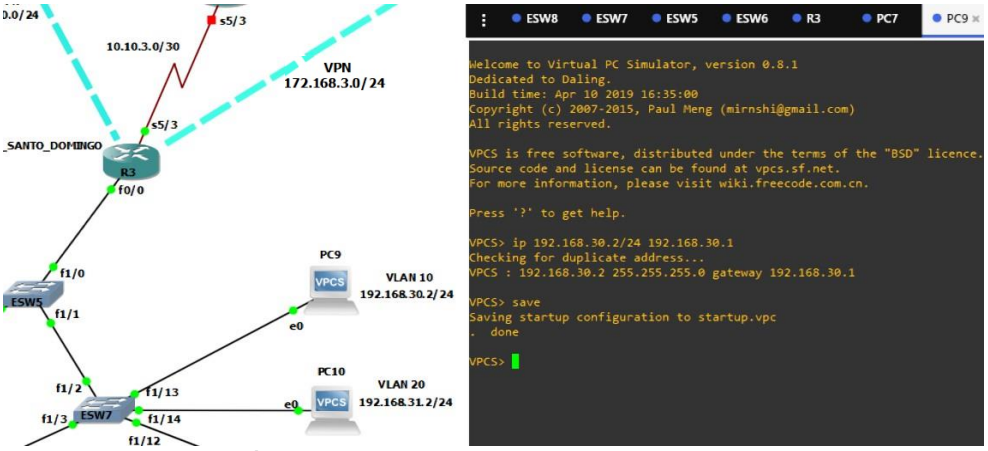


Nota. Spanning tree permite equilibrar las conexiones troncales para las vlans.

Para comprobar el funcionamiento de **spanning tree** se procede a asignar los puertos del switch en modo acceso correspondientemente a la vlan que pertenecen, así como la dirección IP de las PCs como se muestra en la figura 170.

Figura 170

*Direccionamiento IP en Red santo domingo***.**



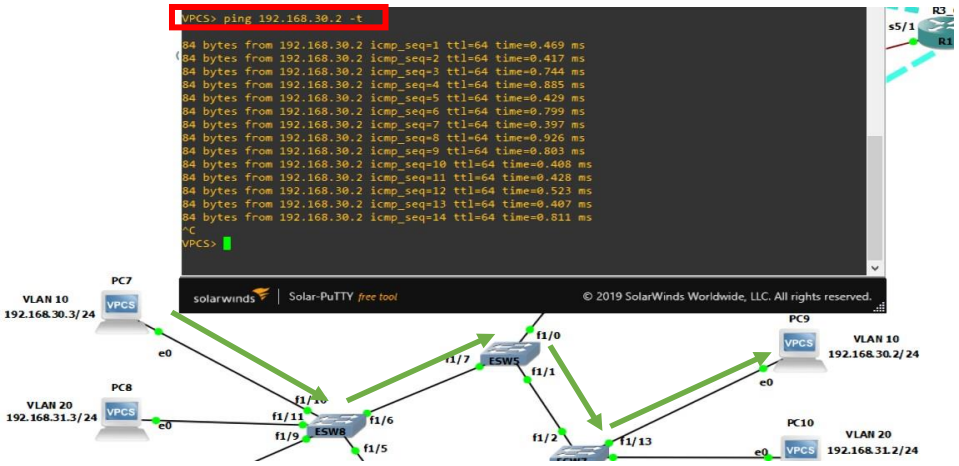
Nota. Se asigna la dirección Gateway para su enrutamiento.

Para realizar un envío de paquetes continuo entre equipos terminales como ejemplo desde la PC7 hacia la PC9 se ejecuta el siguiente comando. Como se muestra en la figura 171. Para finalizar el envío de paquetes se presiona “ctrl + c”

```
VPCS> ping 192.168.30.2 -t
```

Figura 171

Envió de paquetes continuo en Red Sangolquí

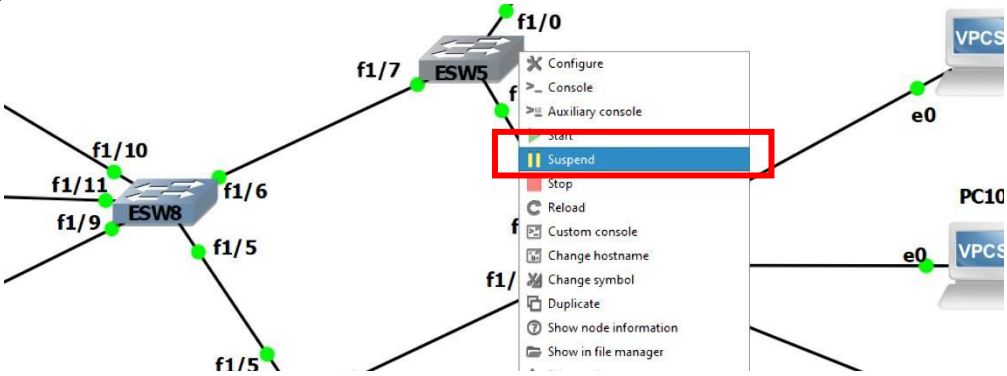


Nota. No hay enrutamiento hacia otras redes.

Ahora bien, mientras el ping se esté procesando se suspende el switch 5 y se observa el comportamiento que tiene él envió de paquetes. Los puertos que están de color verde pasaran a un color amarillo como en la figura 173.

Figura 172

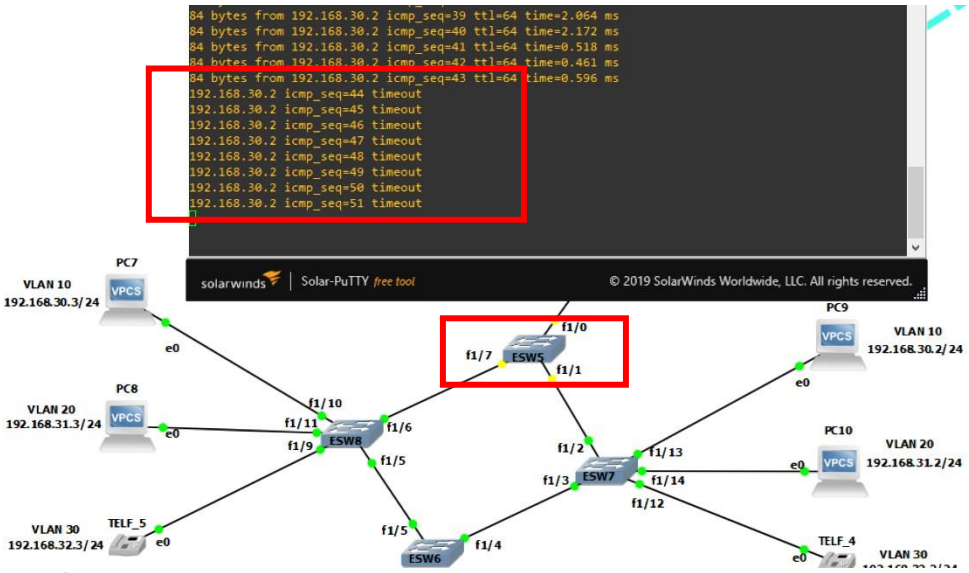
Suspender switch SW5_S_DOMINGO



Nota. para suspender un equipo hacer clic derecho y presionar “suspender”.

Figura 173

*SW5_S_DOMINGO suspendido y paquetes detenidos***.**

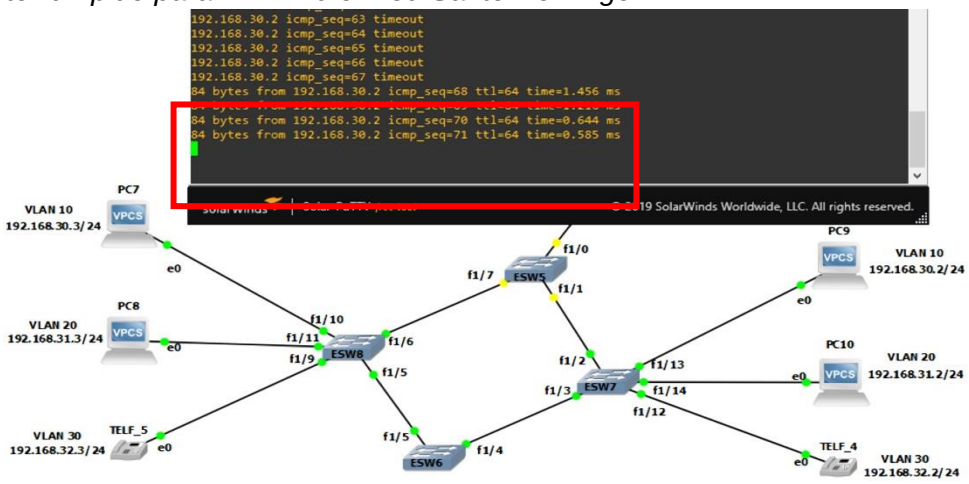


Nota. El envío de paquetes se suspende tras unos segundos.

Después de unos cuantos segundos los paquetes quedan sin conexión por que el camino por defecto está interrumpido para lo cual spanning tree busca una ruta alterna y vuelve enviar los paquetes como se muestra en la figura 174.

Figura 174

*Camino interrumpido para VLAN10 en red Santo Domingo***.**



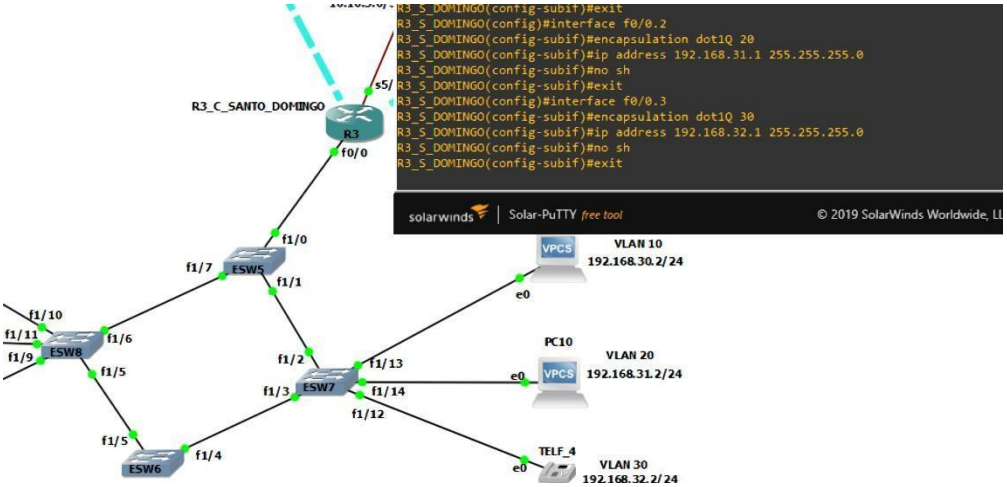
Nota. Tras unos segundos el envío de paquetes se restaura.

Red Sucursal Santo Domingo (Enrutamiento de VLANS)

De esta manera se comprueba el funcionamiento de spanning tree ahora se procede a enrutar las VLANS por medio del router 3, un proceso ya revisado en la red de Sangolquí mediante los comandos que se muestran en la figura 175 y su verificación en la figura 176.

Figura 175

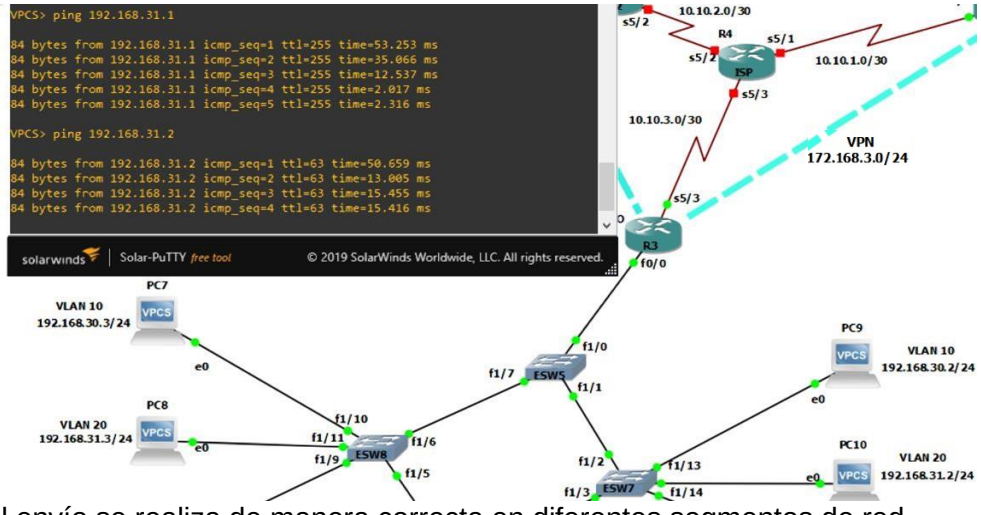
*Enrutamiento de VLANS en red Santo domingo***.**



Nota. En la figura se muestra el enrutamiento de las vlans 20 y 30.

Figura 176

Envió de paquetes en diferentes VLANS red Santo Domingo.



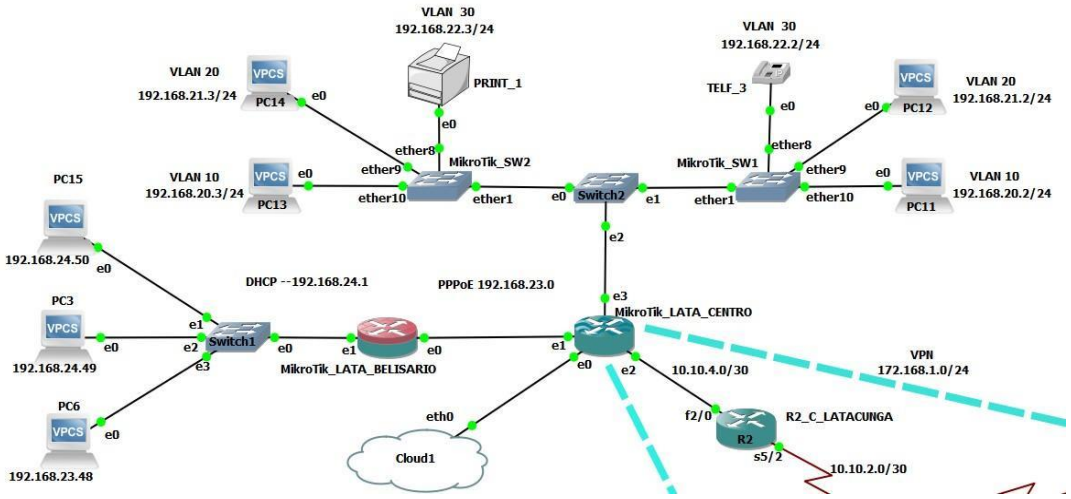
Nota. El envío se realiza de manera correcta en diferentes segmentos de red.

Red Sucursal Latacunga

Para la red Latacunga la cual tiene dos campus se realizará una topología utilizando dispositivos MikroTik, protocolos de conexión por banda ancha PPPoE y de igual manera que en el resto de topologías hará uso de la tecnología VLAN y su respectivo enrutamiento. La topología de red LAN que se utilizará para Latacunga ESPE será la que se muestra en la figura 177.

Figura 177

*Red LAN de ESPE Latacunga***.**



Nota. En esta red también se usará los equipos de simulación “switch”, los cuales no requieren configuración extra.

Red Sucursal Latacunga (Ingreso a Dispositivos MikroTik y WinBox)

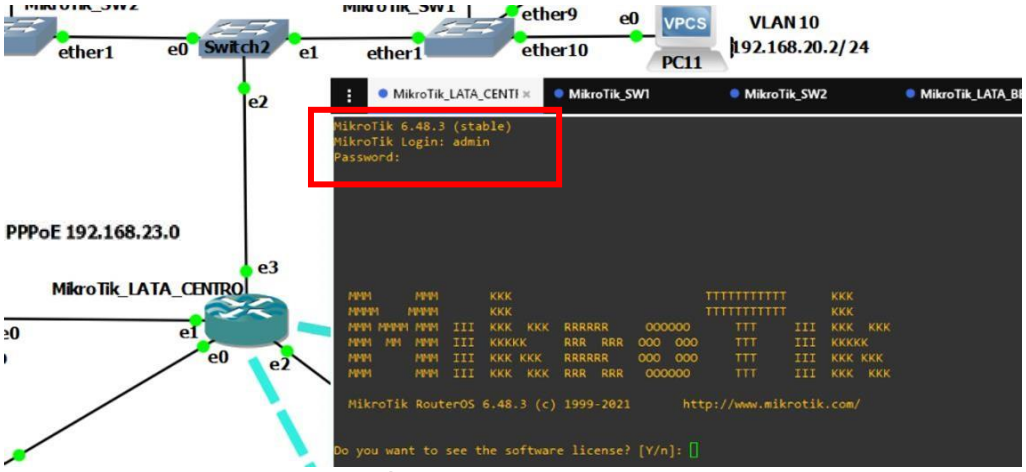
Algo muy importante a mencionar para esta topología es que al ser dispositivos MikroTik estos requieren conectarse a una interfaz de la computadora física para poder ser administrados, esta conexión está establecida por la nube o

“cloud1” la cual le permite configurar los routers y switchs MikroTik a partir del software “WINBOX” una interfaz gráfica para la interacción con el usuario. Enciende los dispositivos y entra el modo consola de los routers y switchs.

La primera vez que ingresa en estos dispositivos la consola solicitara un usuario y una contraseña al ser la primera vez, las claves por defecto es usuario: admin y sin contraseña como se muestra en la figura 178 se desplegara un logo de la marca y de igual forma un cuadro de dialogo pregunta para comprar la licencia para este dispositivo, según sea el criterio digitar YES o NO.

Figura 178

Ingreso en dispositivo MikroTik.



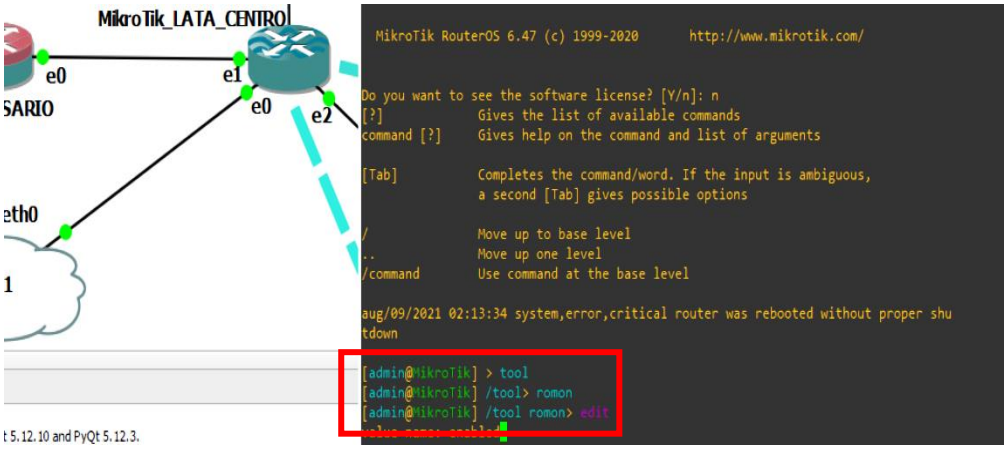
Nota. La consola por defecto será Solar-PuTTY.

Mikrotik permite administrar los dispositivos por medio de la herramienta RoMON, un protocolo que permite ingresar a los dispositivos sin necesidad de que el resto esté conectado a la nube. Para activarlo se debe seguir los siguientes comandos. Los cuales se muestran en la figura 179.

```
[admin@MikroTik]> tool
[admin@MikroTik]/tool> romon
[admin@MikroTik]/tool romon> edit
      value-name: enabled
```

Figura 179

Activación de ROMOn en MikroTik.

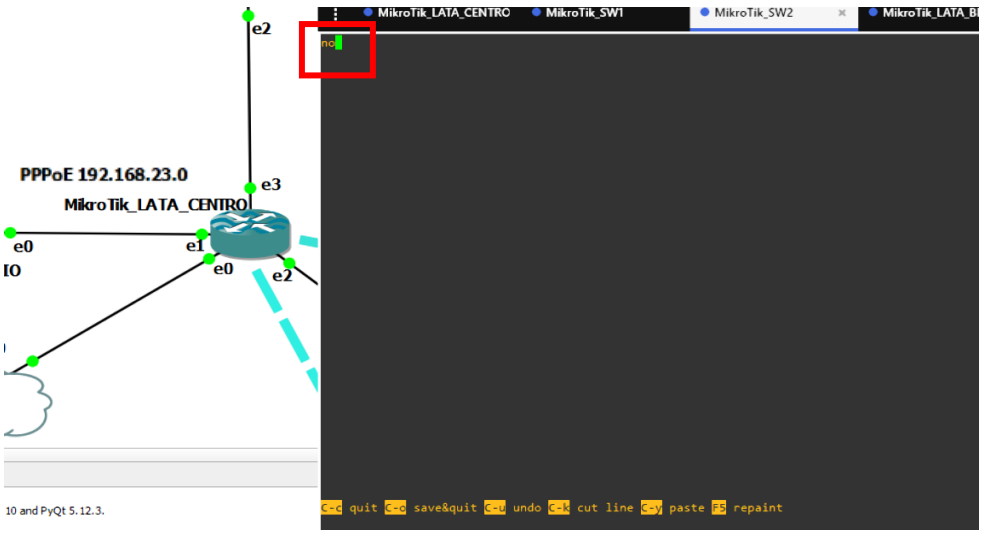


Nota. Los comandos en MikroTik son diferentes a lo revisado en CISCO.

Cuando se ingrese el valor enabled" la consola mostrara una pantalla casi vacia donde se muestra la palabra "no", y se debe cambiar por "yes", luego presionar el comando crtl + o con lo que se regresa a la ventana anterior y para verificar que la configuración esta correcta se debe el siguiente comando el cual también se muestra en la figura 182.

Figura 180

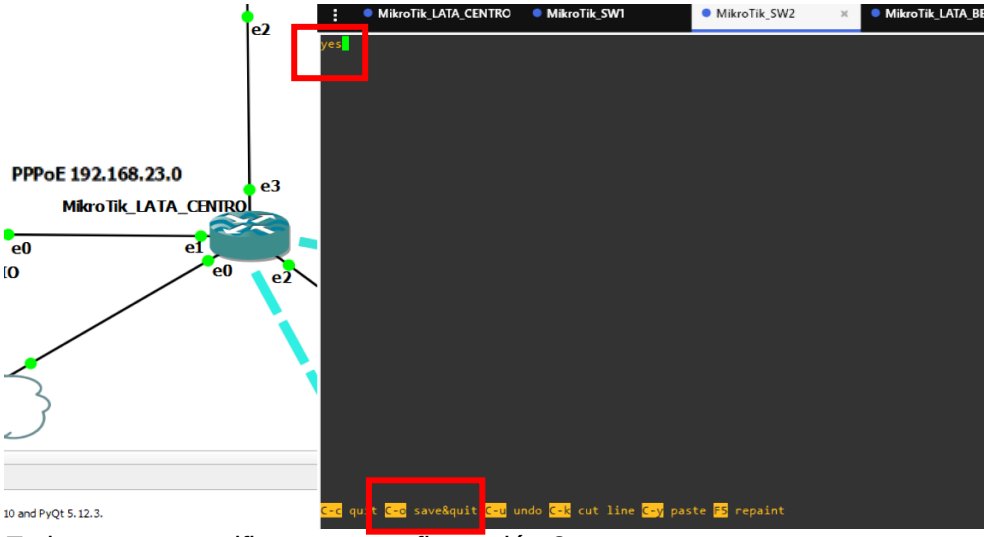
Ventana enabled para RoMON



Nota. Por debajo se muestran comandos para guardar las configuraciones.

Figura 181

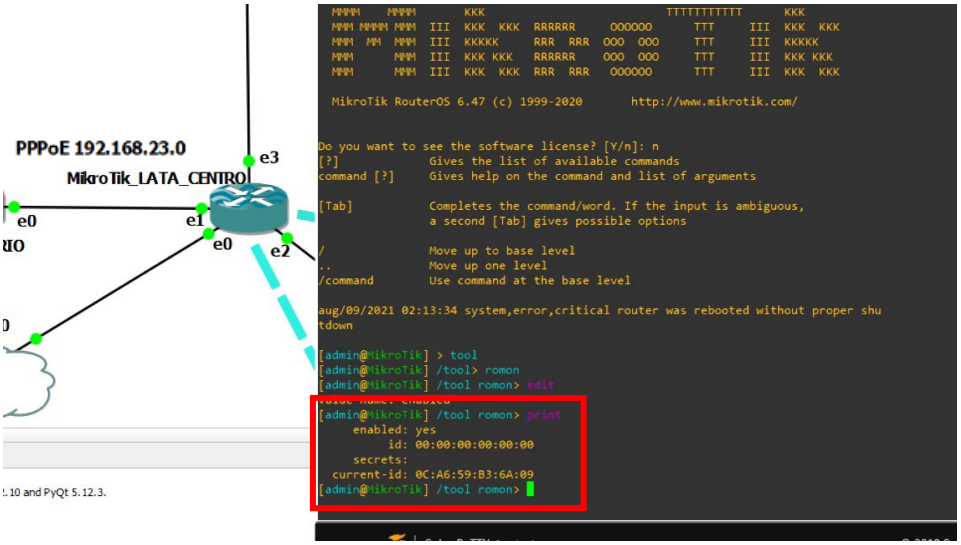
*Edición en la opción yes en RoMON***.**



Nota. Es importante verificar esta configuración 2 veces.

Figura 182

RoMON activado en MikroTik_LATA_CENTRO

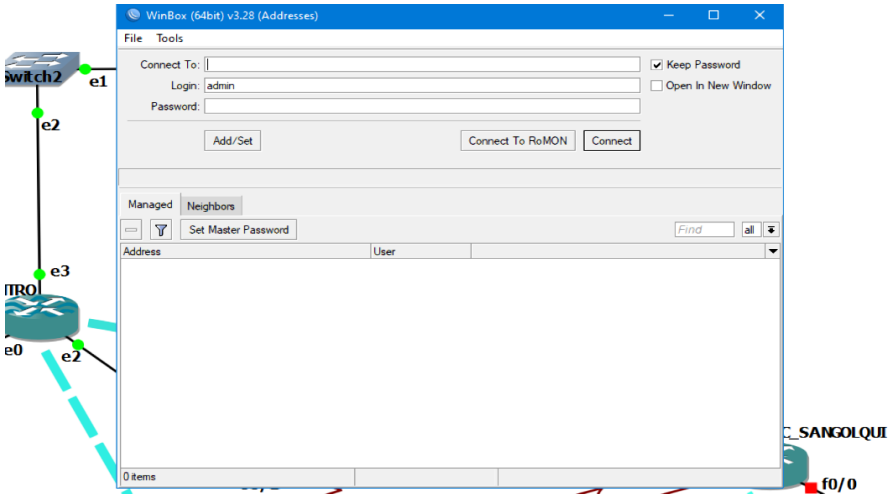


Nota. Se podrá observar que también se emite un current-id.

Una vez realizado esta activación en todos los equipos MikroTik se ejecuta la interfaz gráfica WINBOX para lo cual una vez descargada la aplicación y ejecutada como administrador, se mostrará la pantalla como en la figura 183.

Figura 183

Interfaz del programa WinBox

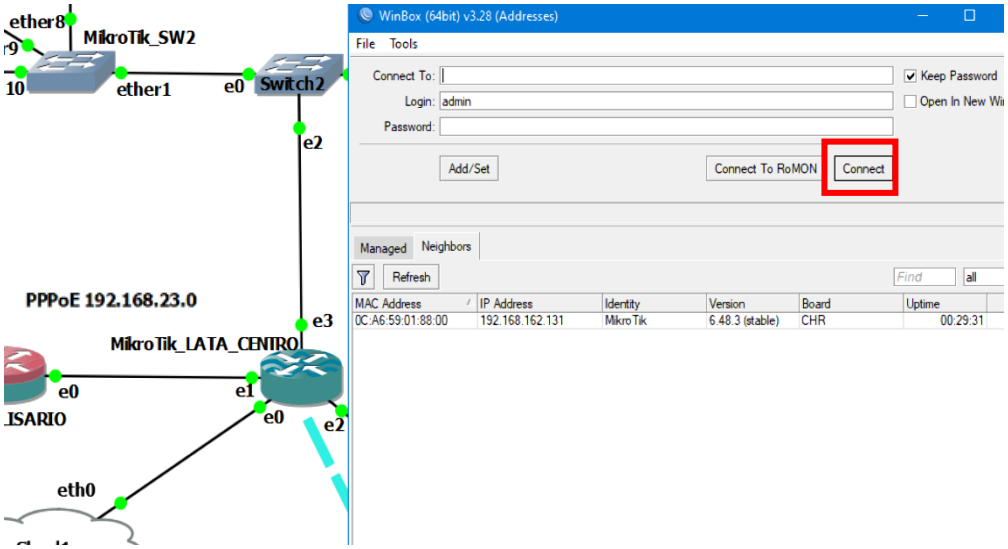


Nota. El programa es un ejecutable por lo que no requiere de instalación.

Winbox hace un reconocimiento de aquellos dispositivos MikroTik que se encuentren conectados a la red, como se mencionó antes se podrá acceder a los mismos en un proceso de cascada, para esto se debe dar clic en el apartado Neighbors donde se desplegara una lista de los equipos conectados y accesibles, como en la figura 184.

Figura 184

*Listado Neighbors en MikroTik_LATA_CENTRO***.**

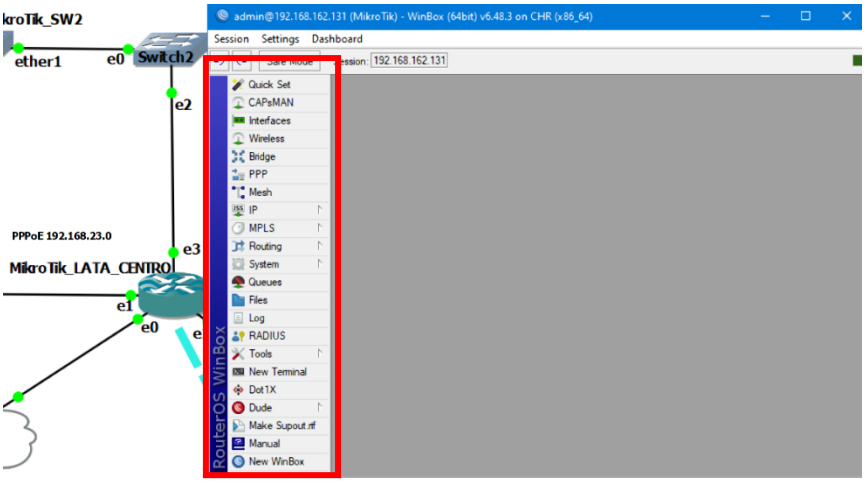


Nota. Se muestra dentro del listado el router conectado principalmente a la nube.

Seleccionando el equipo en cuestión se debe dar clic en el botón “Connect” que está en la parte superior la ventana, la figura 184 es la interfaz de configuración del router donde se realizan todo tipo de protocolos de una manera más cómoda para el usuario, si se necesita abrir un nuevo equipo, dar clic en la penúltima opción de la columna de la izquierda “open a new winbox”, y volverá a mostrarse la ventana del principio pero sin cerrar la interfaz del router a trabajar, como en la figura 186

Figura 185

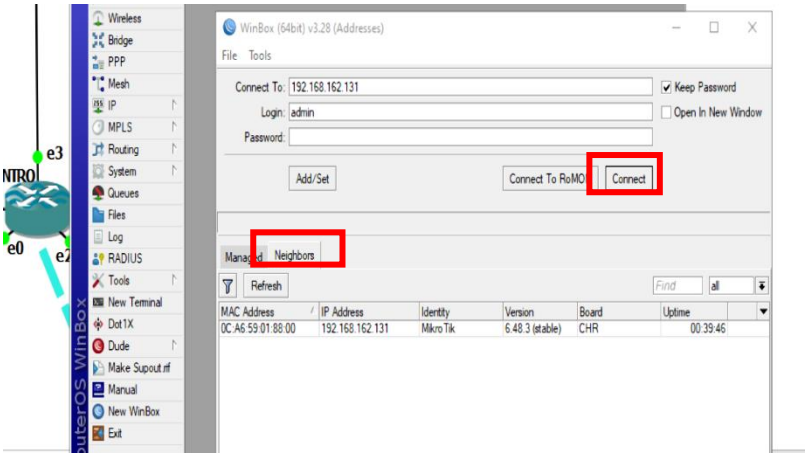
Interfaz de trabajo por WinBox para el equipo MikroTik_LATA_CENTRO



Nota. En la columna de la izquierda se detallan opciones del programa WinBox.

Figura 186

Acceder a una nueva interfaz de WinBox.

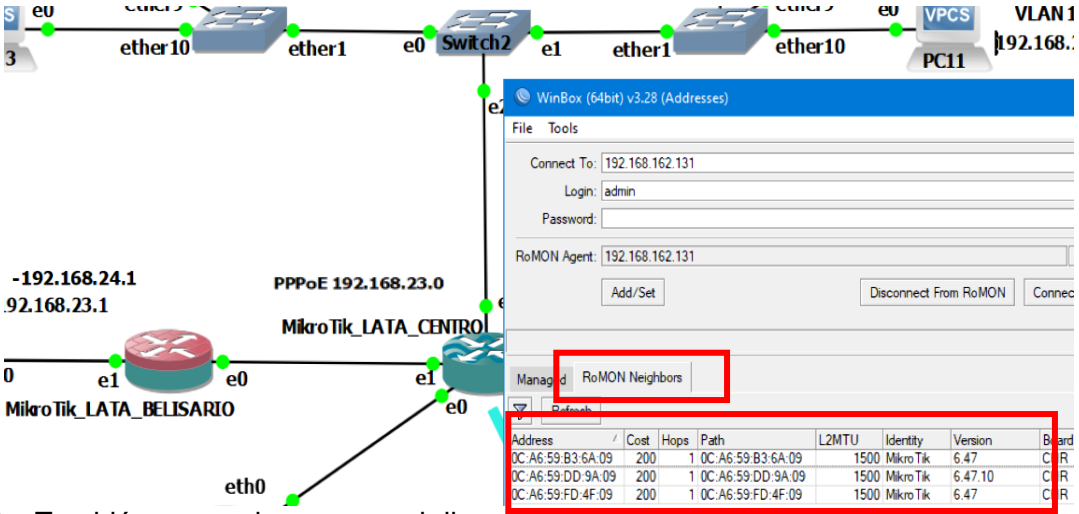


Nota. La interfaz también muestra el usuario (admin) y la contraseña de acceso al equipo, y de igual forma se detalla la versión, y marca del equipo.

Como se mencionó anteriormente RoMON permite conectar al resto de dispositivos que estén conectados al router LATA_CENTRO, para ingresar se debe dar clic en la opción Connect to RoMON de esta manera el listado inferior cambiara y se deberán mostrar todos aquellos dispositivos mikrotik que estén conectados a ese router principal. Como se muestra en la figura 187.

Figura 187

Listado de equipos conectados por RoMON al router LATA_CENTRO



Nota. También se puede regresar al dispositivo principal por medio del botón “disconnect from RoMON”.

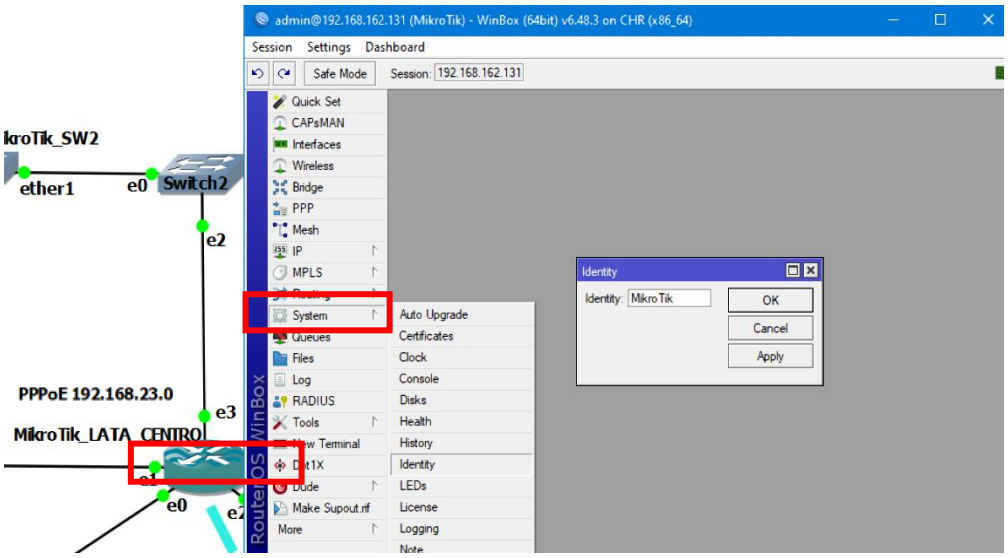
Para abrir la interfaz gráfica de configuración se debe dar clic únicamente en la opción Connect, seleccionado el equipo a inicializar, es importante mencionar que en la parte de arriba cuando se da clic en alguno de los equipos estos parámetros cambian según el equipo, pero como aún no se han configurado ningún usuario aparte de Admin ni mucho menos alguna contraseña estos campos se mantienen iguales.

Como aún no se ha identificado los nombres de los dispositivos correspondientes a cada ventana de WinBox, puede haber confusiones, para lo cual la primera configuración será cambiar el nombre a los mismos según el nombre de la topología, para lo cual se debe dar clic en la opción SYSTEM del menú izquierdo y en el submenú que aparece presionar en la

etiqueta IDENTITY, se mostrará un pequeño cuadro en el medio de la interfaz como se muestra en la figura 188.

Figura 188

Cuadro Identity en router LATA_CENTRO

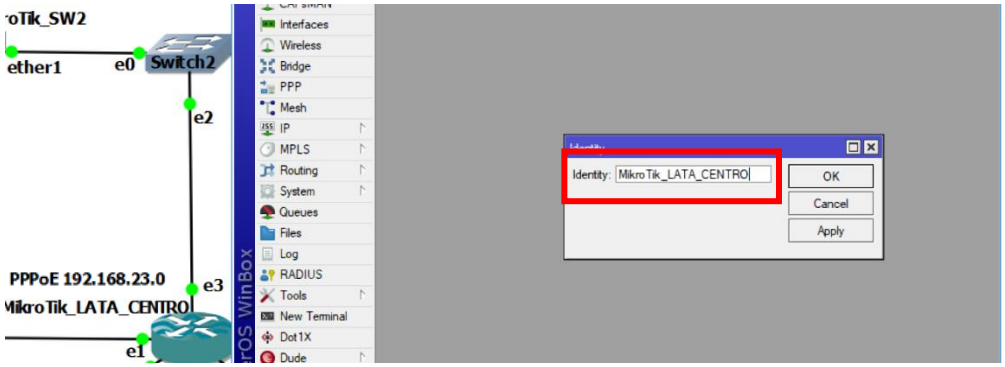


Nota. Gran parte de las opciones se irán mostrando como cuadros o interfaces visuales más grandes en medio de esta interfaz de WinBox.

En este cuadro se cambia el nombre del equipo según la topología. Una vez escrito el nombre se da clic en “Apply” y luego en “OK” de esta manera se puede ver como en la parte superior el nombre también habrá cambiado, como en la figura 189.

Figura 189

Cambio de nombre para MikroTik_LATA_CENTRO



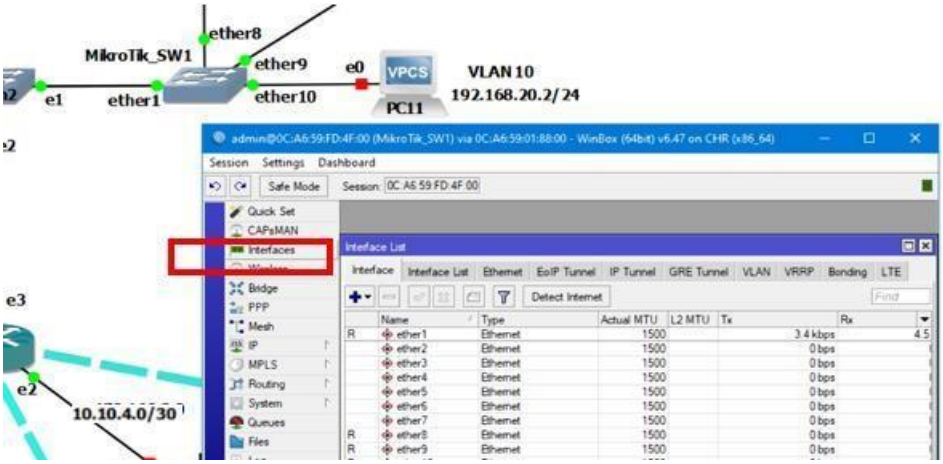
Nota. Se puede apagar los equipos y encenderlos para reconocimiento.

Red Sucursal Latacunga (Implementación de VLANS en MikroTik)

Una vez que se hayan establecido los nombres, configurar las VLANS de los switchs MikroTik, teniendo en cuenta las direcciones y los puertos asignados en la topología, dentro de la interfaz de Winbox para SW1 se debe dar clic en el apartado “Interfaces” en el menú izquierdo, donde se mostrará la ventana como en la figura 190 en donde se detallan el estado de todas las interfaces del switch.

Figura 190

Ventana Interface para configurar VLANS en MikroTik_SW1

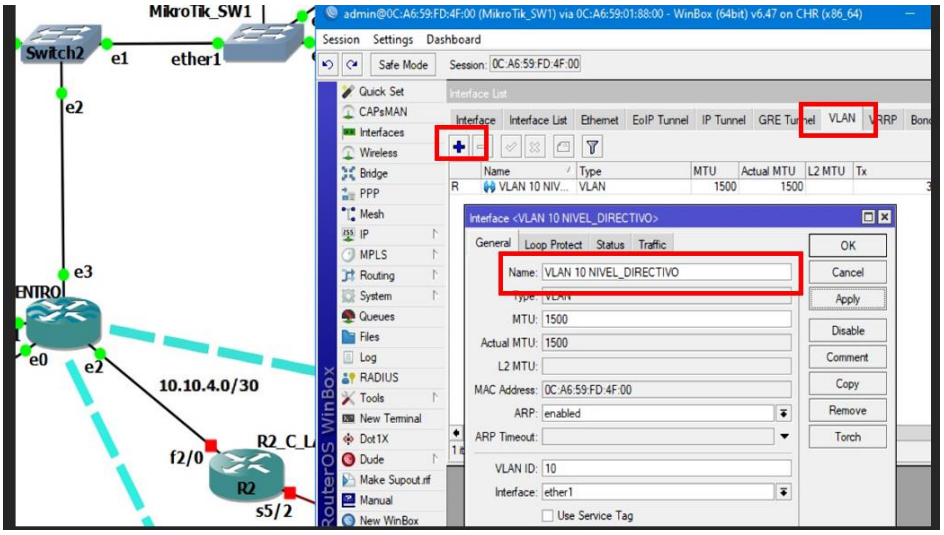


Nota. Las ventanas se pueden cambiar de tamaño.

Para la creación de las redes virtuales se debe dar clic en la pestaña VLAN dentro de la ventana de interfaces, dentro de este apartado en la barra de opciones existe un símbolo más con el cual se aumentan interfaces dependiendo del tipo sección en la que se encuentre. De esta manera si da clic se mostrará una nueva ventana donde se crearán las VLAN 10, 20 y 30 con las mismas características que en las redes LAN anteriores, llenando los campos como en la figura 191.

Figura 191

Creación de VLANS en MikroTik_SW1

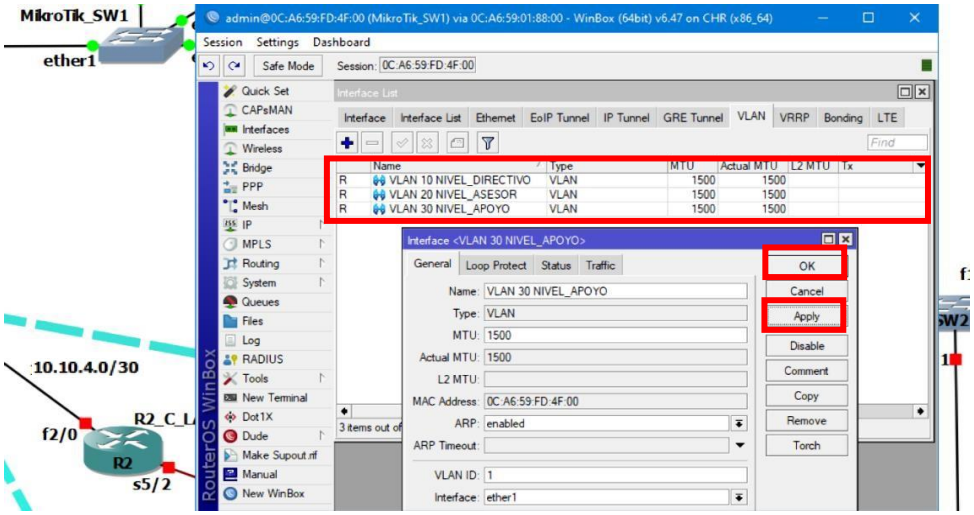


Nota. En esta ventana también se encuentran pestañas para revisar algunas opciones como el estado “status” o el tráfico que pasa por la red virtual “Traffic”.

Se está creando las vlans y se las está asignando un puerto especifico de tráfico es decir la conexión en modo troncal, con respecto a la red es el puerto ether 1 por eso este se mantiene igual para todas las vlans. La ventana de Interface List se detallarán todas las vlans creadas como se muestran en la figura 192.

Figura 192

Creación de conexión troncal para vlans en MikroTik_SW1

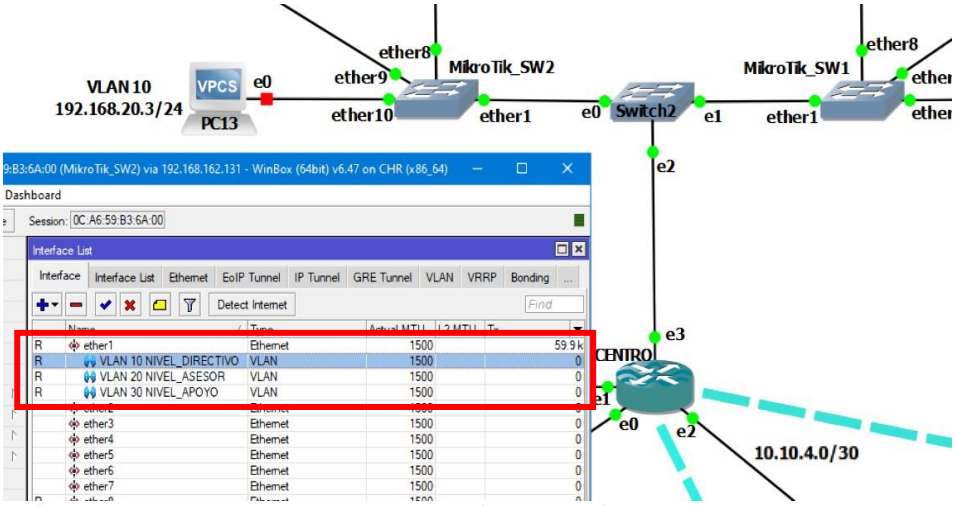


Nota. Una vez llenado los campos dar clic en “Apply” y “Ok”.

Se realiza el mismo proceso en el Switch 2 (SW2) y se verifica que para la ventana de Interface List por debajo de la interfaz física Ether 1 se encuentran creadas las VLANS como en la figura 193 puesto que “ether 1” funciona como el puerto troncal. Hay que tomar en cuenta que entre estos dos switchs hay un tercero, este funciona como intermedio de conexión para el switch principal por lo que no se requiere de una configuración especial, puesto que es un equipo de simulación.

Figura 193

Ventana Interface para configurar VLANS en MikroTik_SW2

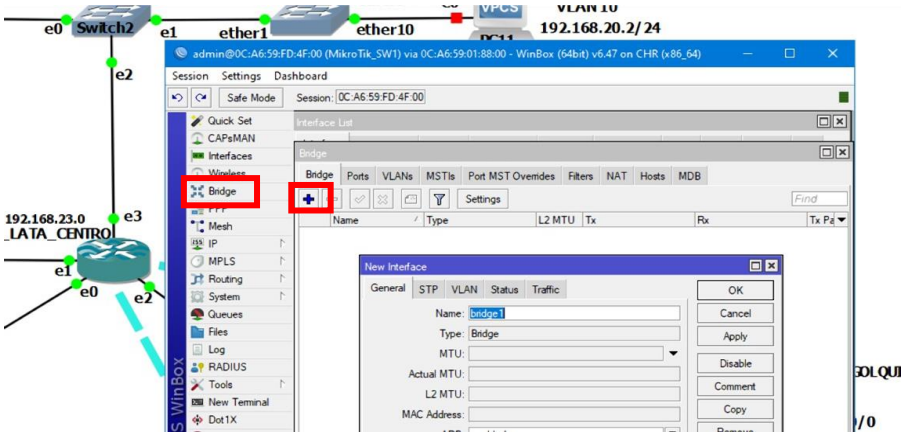


Nota. Aquí se puede mostrar las interfaces lógicas y físicas.

Una vez realizado este proceso, y al igual que el resto de redes LANs que se configuradas previamente, se debe crear las interfaces en modo acceso para las correspondientes vlans, para esto debe dirigirse al apartado bridge del menú de los switchs, donde se crean los puertos de acceso siguiendo a la figura 194.

Figura 194

Creación de conexiones en modo acceso para MikroTik_SW1

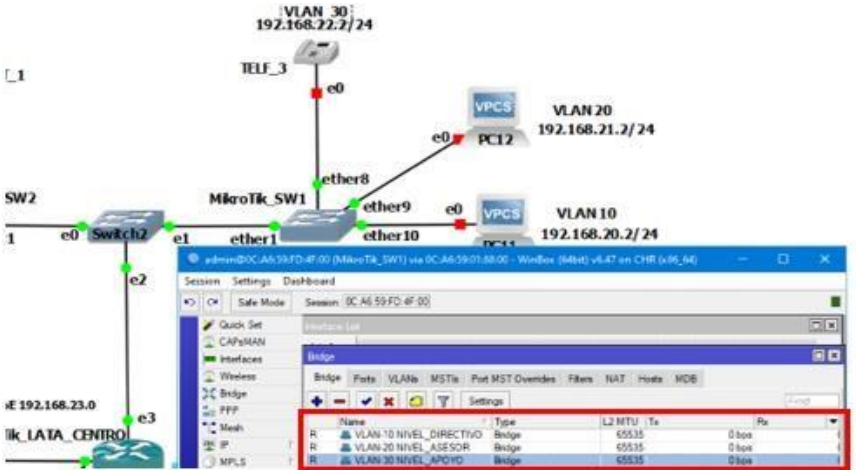


Nota. Primero dar clic en “+” donde se abrirá una ventana y se llena el campo “Name”.

Los nombres de estos puertos de acceso deben ser ligeramente diferente al de las vlans creadas para el modo troncal, esto es realizado para las tres vlans las cuales aparecen en el listado “Bridge”, como se muestra en la figura 195.

Figura 195.

Creación de VLANS en modo acceso para SW1

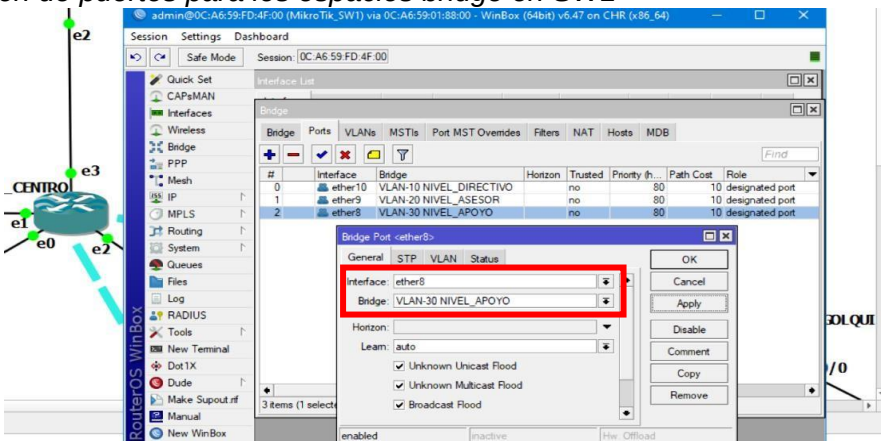


Nota. Añadir un guion al nombre creado en esta sección, para evitar confusiones.

Ahora se debe realizar la asignación de los puertos físicos de los switches a los espacios bridge creados, dentro de la pestaña PORTS de la interfaz Bridge se dirige al botón añadir, y se establece los puertos como se muestran en la figura 196.

Figura 196

Asignación de puertos para los espacios bridge en SW1

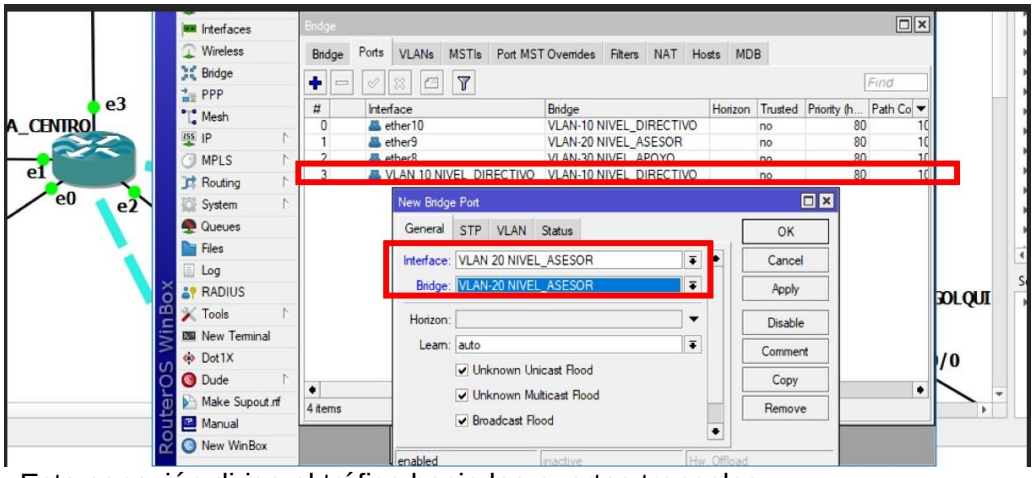


Nota. Se debe asignar el puerto del listview disponible y de igual manera la vlans en modo acceso creada previamente.

Las redes VLANS se deben asignar a sus propias interfaces de acceso, para lo cual dentro de esta asignación también se debe establecer el proceso de vlansbridge como muestra en la figura 197.

Figura 197

Conexión VLAN_Bridge en SW1.

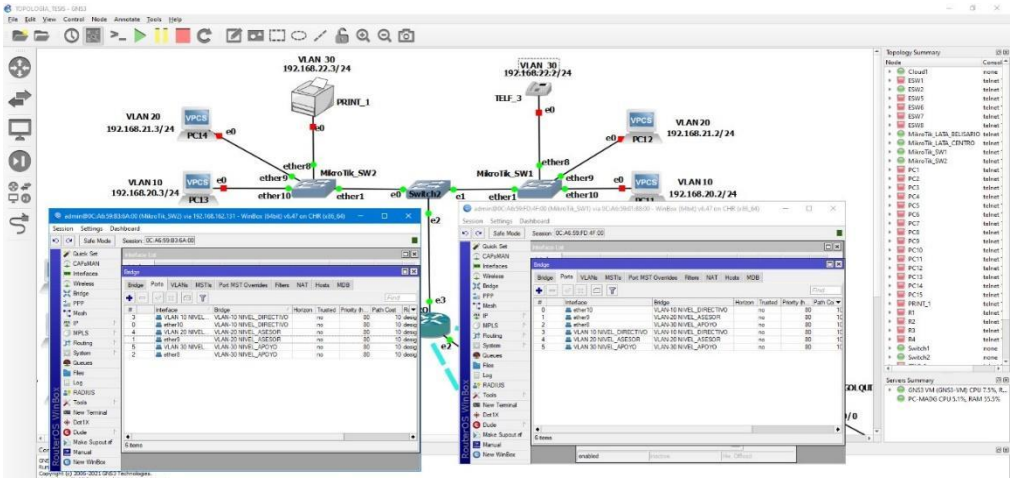


Nota. Esta conexión dirige el tráfico hacia los puertos troncales.

El mismo proceso se debe realizar en MikroTik_SW2 y se verifican los canales de bridge y puertos de vlans, como se muestran en la figura 198 siguiendo las interfaces establecidas en la topología.

Figura 198

VLANS y conexiones en MikroTik_SW2



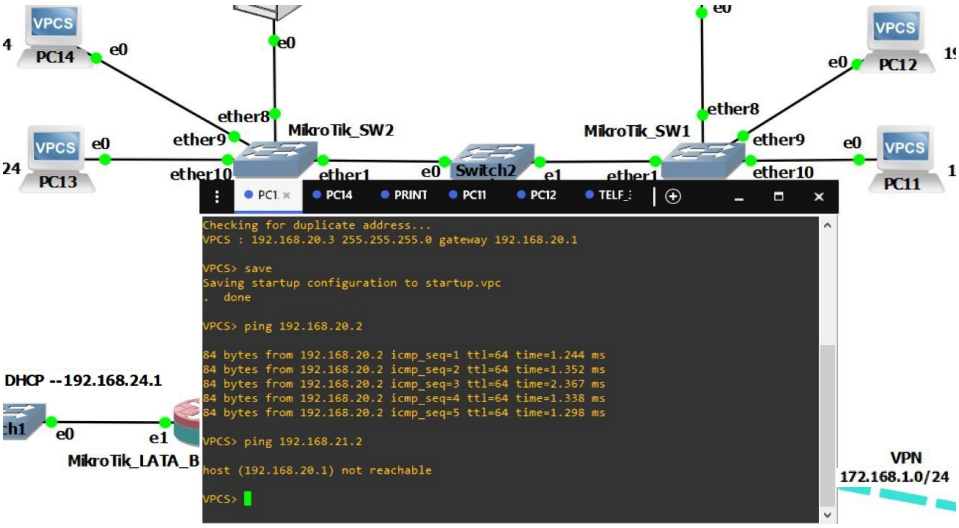
Nota. Deben existir en total 6 puertos Bridge creados.

El siguiente paso es asignar las direcciones IP correspondientes a las VLANS de cada VPCS, este proceso ya se ha descrito en las redes anteriores y de igual forma la dirección debe contener el Gateway para su posterior enrutamiento.

Para comprobar que solo exista conexión entre las vlans se realiza un ping desde la PC13 hacia la PC11 los cuales se encuentran en la misma VLAN y para comprobar que no exista conexión hacia otros destinos se realiza un ping hacia la PC12 como se muestra en la figura 199.

Figura 199

Envió de paquetes en VLANS sin enrutamiento Red Latacunga



Nota. Las direcciones IP se muestran de mejor manera en la figura 187.

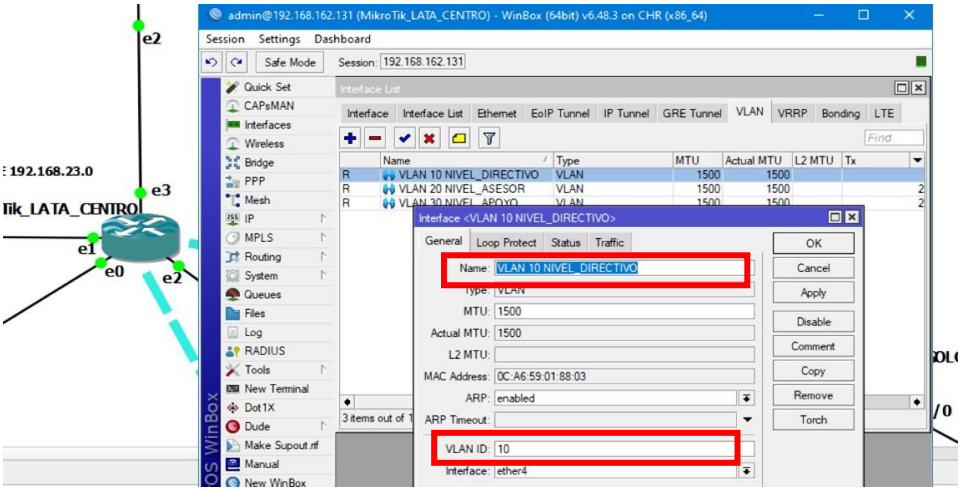
Red Sucursal Latacunga (Enrutamiento de VLANS en MikroTik)

A continuación, debe realizar la configuración del enrutamiento entre vlans, para los dispositivos MikroTik este proceso debe realizarse de la siguiente manera, primeramente, entrar al router principal que será el encargado de enrutar los segmentos de red.

Una vez que ingrese en la interfaz WinBox del router principal, en el menú de la izquierda se debe dar clic en la opción “interfaces” para crear el puerto de enlace troncal hacia el router siguiendo en gran medida el proceso que ya se ha revisado previamente con los mismos dispositivos. Y debe aplicarse como se demuestra en la figura 200.

Figura 200

Creación de enlaces en modo troncal en router LATA_CENTRO

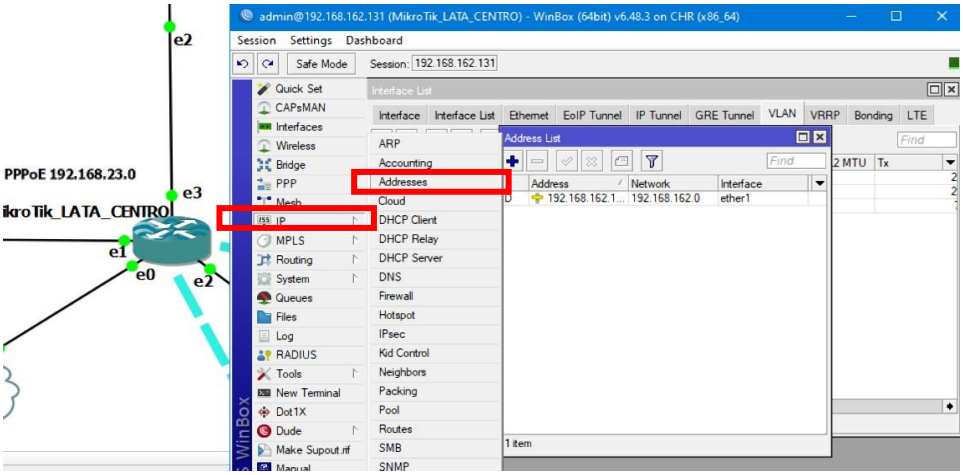


Nota. Aquí es donde la interfaz debe cambiar por el puerto ether4.

Una vez establecido el enlace troncal, debe asignar las direcciones IP correspondientes a cada puerto de VLANS y para lo mismo debe dirigirse al menú de la izquierda dando clic en IP y en el submenú presionar en la opción “Addresses” y una nueva ventana aparecerá, como se muestra en la figura 201.

Figura 201

Interfaz “Address list” en MikroTik_LATA_CENTRO

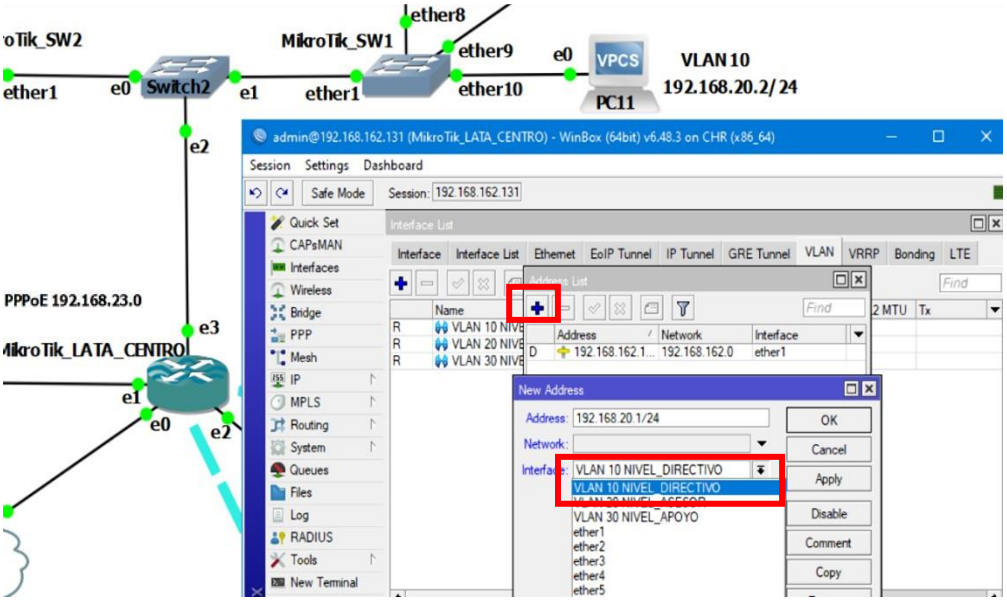


Nota. Al ser el router principal debe mostrarse en el listado la dirección IP que nos ofrece la nube.

Es en esta ventana donde se asignan cada una de las direcciones de Gateway que ya se habían asignado en los VPCs, para añadir las direcciones basta con dar clic en el botón añadir, digitar a la dirección IP correspondiente con el prefijo de su máscara y asignar esta dirección a la VLAN correspondiente, como en la figura 202.

Figura 202

Enrutamiento de VLANS en router LATA_CENTRO

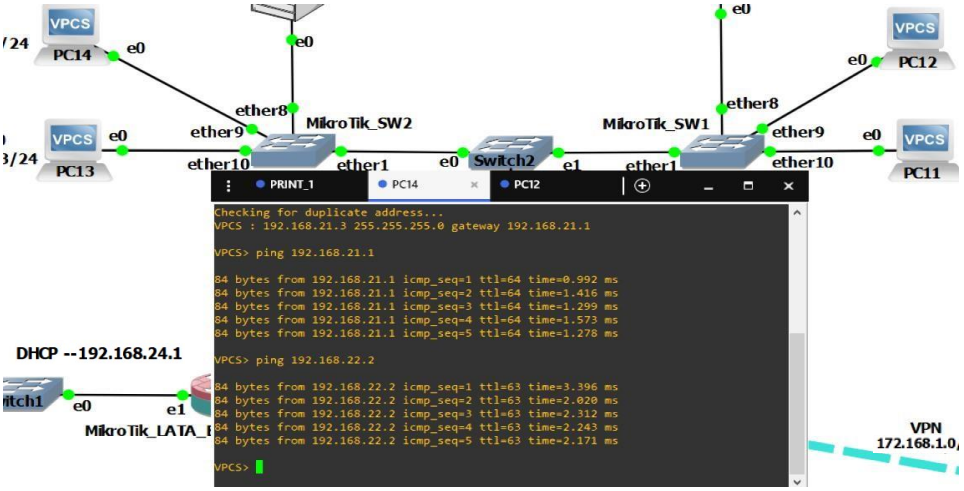


Nota. Se debe realizar esto según las vlans creadas.

Se debe verificar que en el listado de las direcciones general de la ventana “Address list” se muestren todas las creadas para las VLANS, de esta manera habrá terminado con el proceso para el enrutamiento de VLans, si se desea verificar conexión hacia el router y hacia otros segmentos de VLans, desde un VPCS se realiza un ping hacia cualquiera de los dispositivos, como se muestra en la figura 203.

Figura 203

Enrutamiento entre VLANS para red Latacunga exitoso.



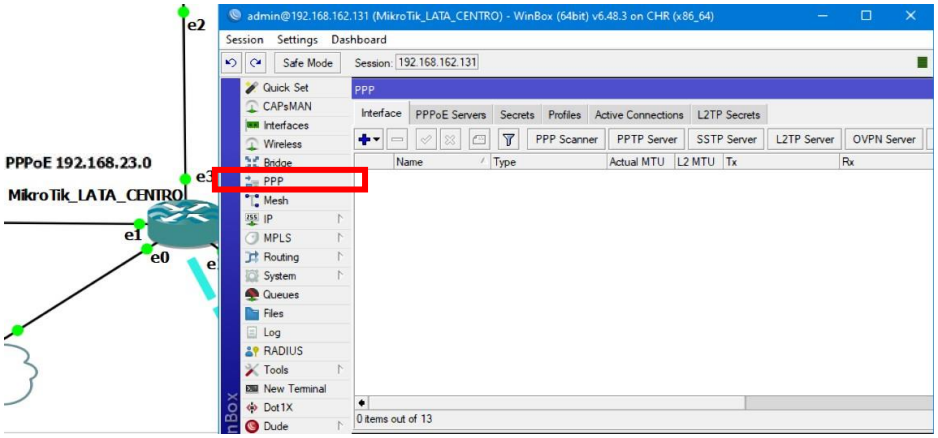
Nota. Las direcciones IP se muestran de mejor manera en la figura 187.

Red Sucursal Latacunga (Implementación del protocolo PPPoE)

Para el campus Belisario se utiliza el protocolo PPPoE para la conexión entre servidor y cliente, administrando autentificación, el ancho de banda requerido, y el pool de direcciones. Primero se crea el servidor PPPoE en el router centro. Se dirige al menú de la izquierda presionando la opción PPP y se mostrara la ventana como en la figura 204.

Figura 204

Interfaz PPP del router LATA_CENTRO

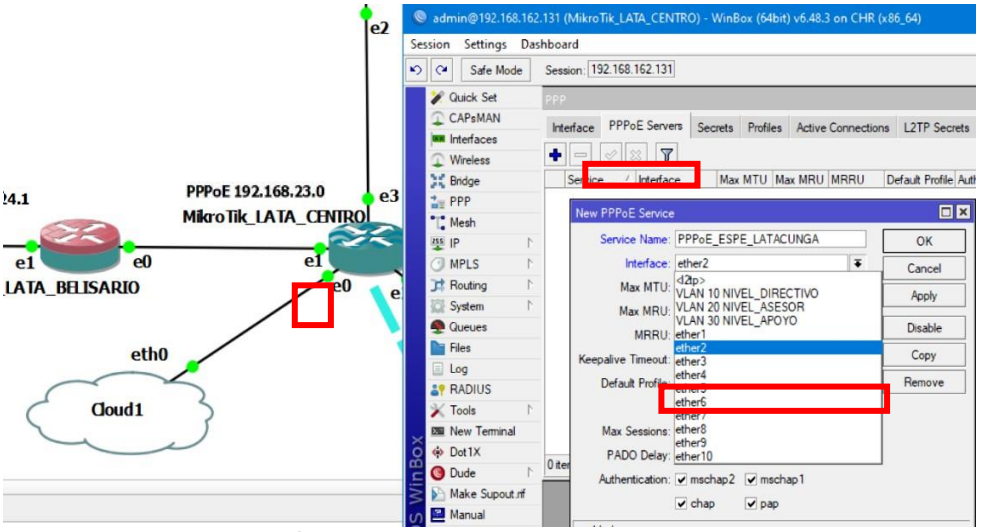


Nota. Las interfaces de las opciones a configurar son bastante similares.

Como siguiente paso en la pestaña PPPoE server en el botón añadir selecciona la opción se abre una subinterfaz donde se digita el nombre y el puerto a la cual se conecta con el router cliente que es el Router LATA_BELISARIO, como se muestra en la figura 205 es importante determinar que para gns3 la interfaz es la ether 1 pero para winbox es la ether 2.

Figura 205

*Creación de PPPoE server en router LATA_CENTRO***.**

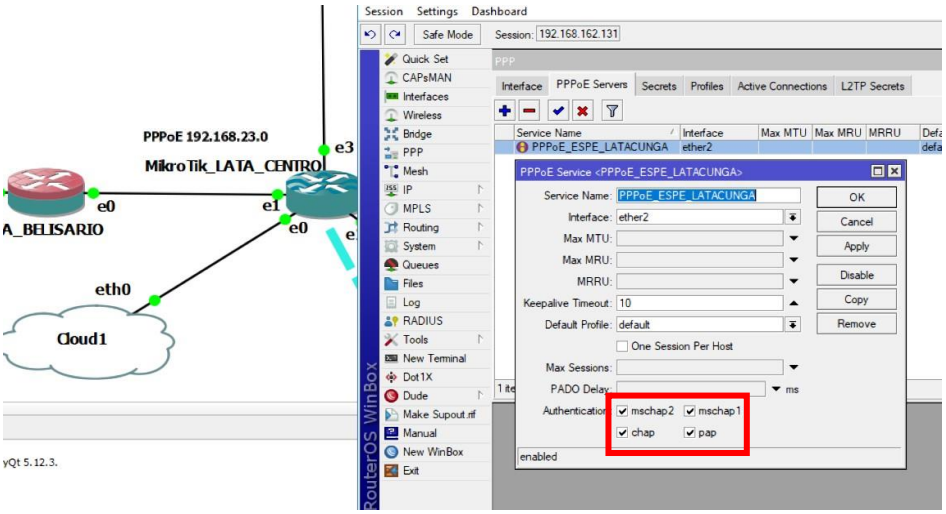


Nota. Las interfaces son un número mayor en WinBox.

Por debajo de esto se encuentra los tipos de autenticaciones para el protocolo PPP, por defecto se marcan todas las casillas que incluyen CHAP, PAP, MSCHAP 1, etc. Siguiente a esto se debe guardar los cambios y observar el listado de PPPoE server donde se encuentra el servidor recién creado como se muestra en la figura 206.

Figura 206

Servidor PPPoE creado en router LATA_CENTRO

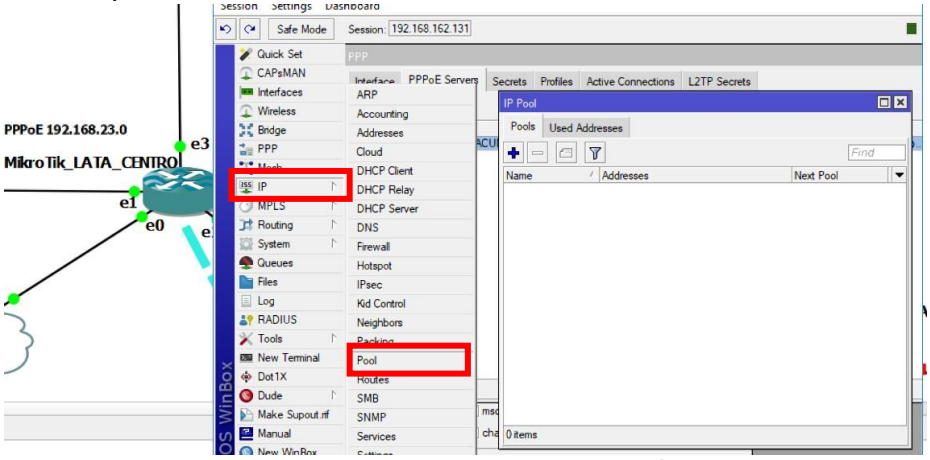


Nota. Para guardar los cambios dar clic en Apply y Ok.

Una vez creado el servidor, se debe generar un pool de direcciones, es decir un fondo de direcciones a las cuales se les va a entregar a los routers que se conecten por PPPoE, para esto se debe dirigir al apartado IP del menú izquierdo y en el submenú que aparece presionar en la opción POOL donde se desplegara una pequeña interfaz como la que se muestra en la figura 207.

Figura 207

Interfaz IP Pool para router LATA_CENTRO

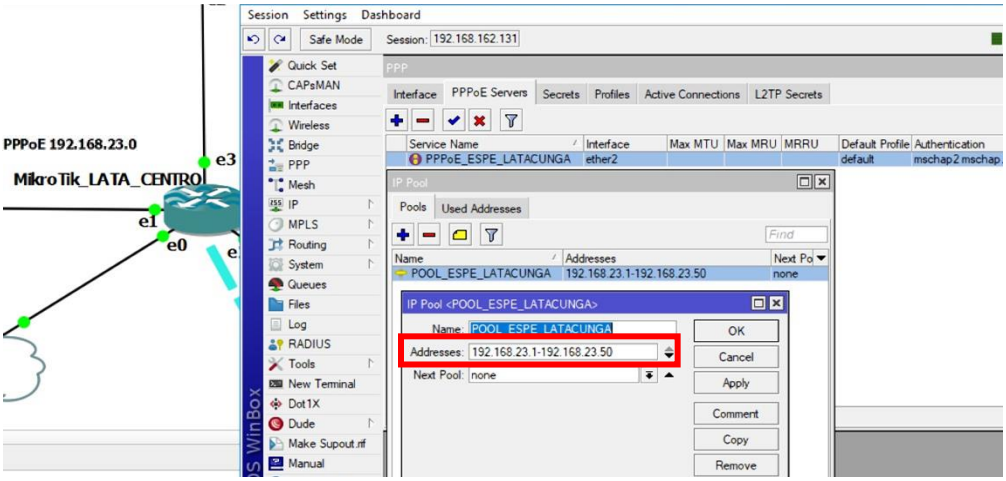


Nota. El fondo de direcciones debe responder a la dirección principal que se asigna en el segmento de red.

Aquí se añade un nuevo pool de direcciones en el botón más, se le asigna un nombre y el rango de direcciones que se van a otorgar hacia los clientes, separados por un guion medio y para guardarlo se debe dar clic en APPLY y OK, como se muestra en la figura 208.

Figura 208

Creación del pool de direcciones para el router LATA_CENTRO

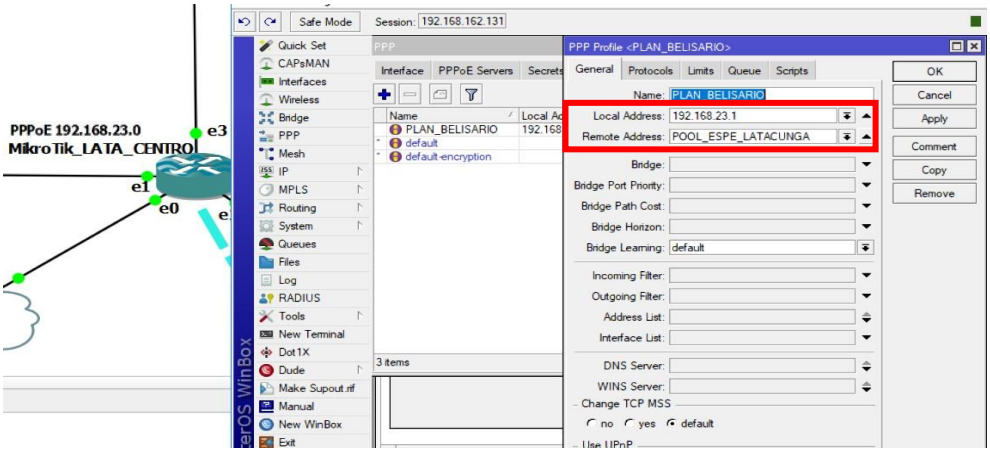


Nota. Se pone el rango de direcciones separado por un guion.

Dentro de la interfaz de PPP, se debe asignar el Pool de direcciones creado, para lo cual se accede a la pestaña Profiles y se da clic al botón +, se digita un nombre para el servicio de PPPoE, una dirección IP dentro del segmento establecido y el pool de direcciones que ya se muestra en el listview como en la figura 209.

Figura 209

Perfil PPP en el servidor con dirección local y pool

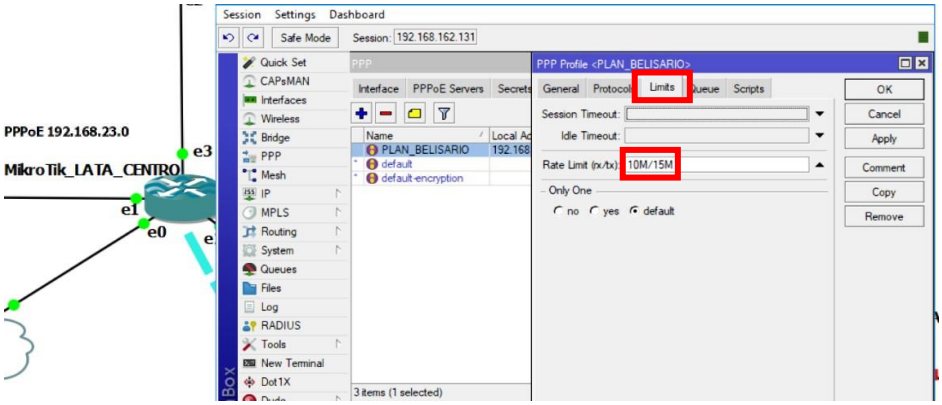


Nota. La dirección IP sirve como referencia para el servidor PPPoE.

En la pestaña “limits” en el apartado “Rate limit”, se establece cuanto ancho de banda obtendrá el cliente, para establecer el campo se lo hace como se muestra en la figura 210.

Figura 210

Ancho de banda par PPPoE plan Belisario.

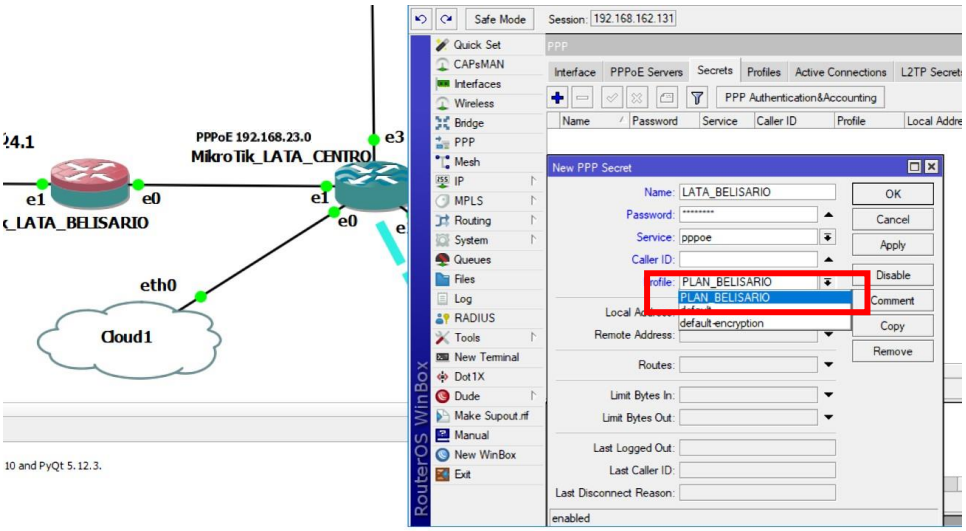


Nota. En la opción “Only one” se marca para un único inicio.

Una vez creados los planes se debe generar los clientes que estarán en el servicio, en la ventana de PPP y en el apartado de “Secrets” con el botón añadir se muestra la ventana como en la figura 211, se digita el nombre del cliente una contraseña de seguridad, el servicio al que se establecerá y el perfil que obtendrá.

Figura 211

Asignación de clientes en PPPoE server.



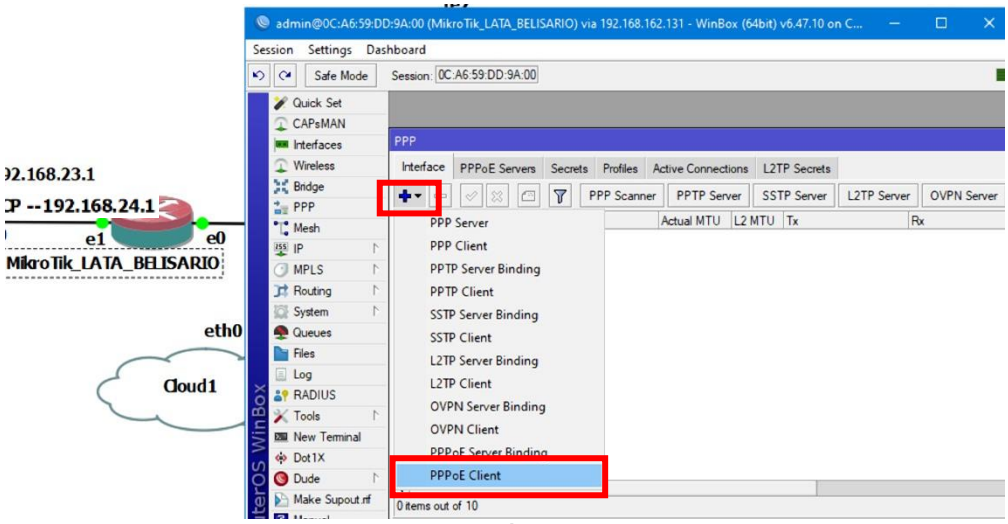
Nota. Los campos a establecer permiten que se reconozca lo configurado con un listview donde las opciones disponibles se muestran.

De esta manera lo que resta es la creación de los clientes que serán los que se conecten por medio de PPPoE a el router servidor y se les otorgue los servicios previstos. Para esto dentro de la interfaz WinBox del router

MikroTIk_LATA_BELISARIO se dirige a la interfaz de PPP y se da clic en el botón añadir donde un pequeño menú permitirá crear el cliente PPPoE en la última etiqueta que se muestra, como se presenta en la figura 212.

Figura 212

Creación del PPPoE cliente en MikroTik_LATA_BELISARIO

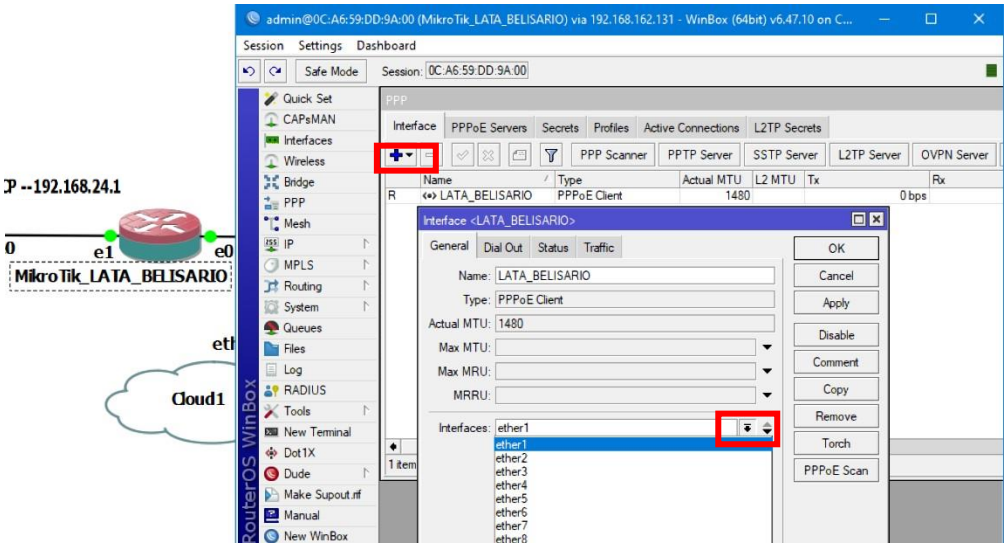


Nota. Es importante verificar que sea la opción PPPoE client.

De esta manera una interfaz de configuración permitirá que se digite el nombre del cliente el cual debe ser el mismo que se había asignado en el servidor PPPoE y de igual manera la interfaz con la que se conecta a dicho servidor, como se muestra en la figura 213.

Figura 213

*Asignación del servicio de PPPoE en MikroTik_LATA_BELISARIO***.**

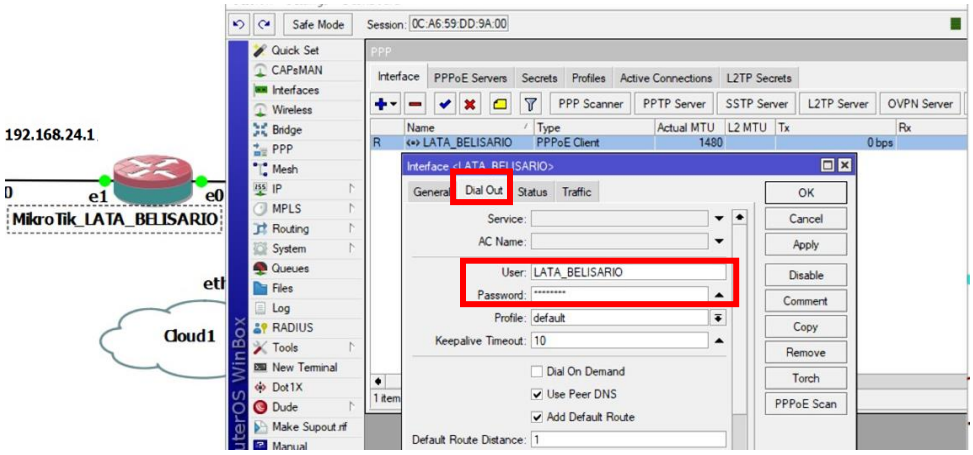


Nota. Seleccionar la interfaz correspondiente en WinBox.

En la siguiente pestaña “Dial out” se debe asignar el usuario y la contraseña del perfil que se había creado en el servidor PPPoE, al guardar los cambios se podrá observar el usuario en la lista de interfaces de PPP como en la figura 214.

Figura 214

Asignación de usuario en el cliente LATA_BELISARIO

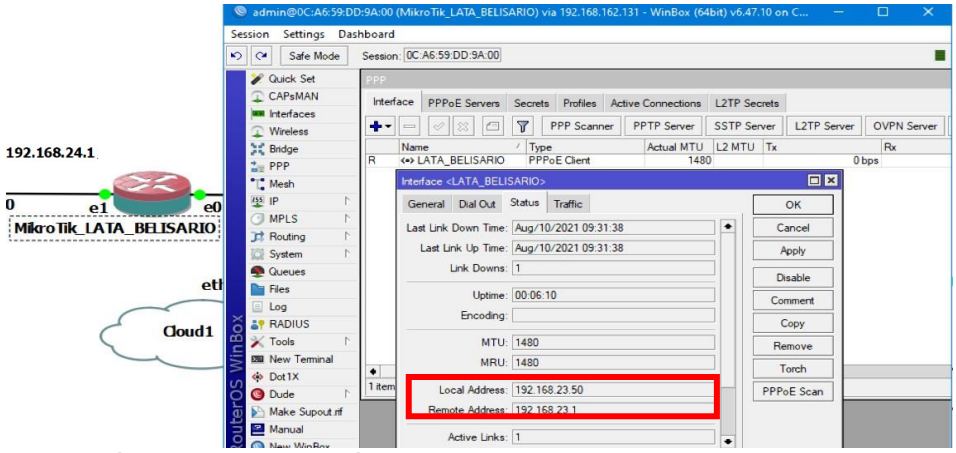


Nota. Para guardar los cambios se presiona Apply y OK.

Junto al cliente creado la letra “R” debe aparecer, lo cual significa que ya existe la conexión hacia el servidor PPPoE, para comprobarlo se ingresa al usuario creado y en la pestaña “status” se debe mostrar la fecha en que se realizó la conexión y la dirección que se ha asignado al cliente, como en la figura 215.

Figura 215

Conexión exitosa en PPPoE LATA_BELISARIO

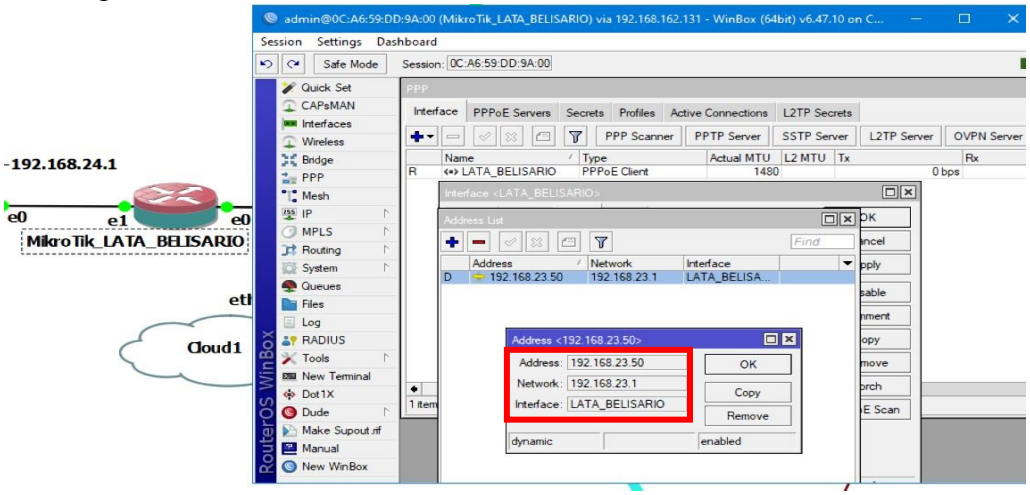


Nota. La dirección asignada es la última del pool de direcciones.

De igual forma puede comprobar que dirección y la red que se han asignado por PPPoE si se dirige al manu de la izquierda, se da clic en IP y luego en la opción **addresses** de esta manera se comprueba que la dirección que el servidor LATA_CENTRO ha otorgado al cliente LATA_BELISARIO.

Figura 216

Dirección asignada en el cliente LATA_BELISARIO



Nota. La dirección “Network” se lo puede tomar como un Gateway.

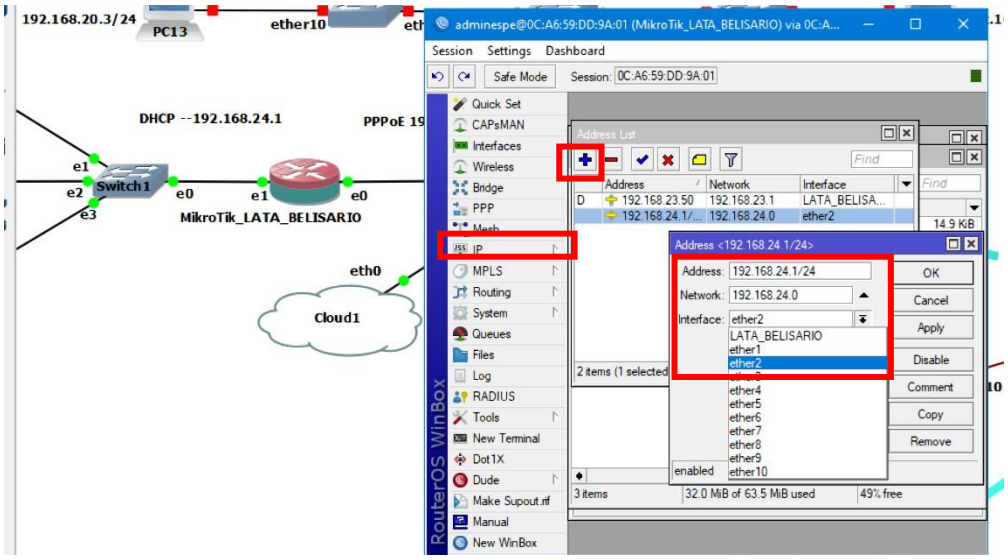
Red Sucursal Latacunga (Implementación del protocolo DHCP)

Ahora para que los equipos obtengan una dirección IP automáticamente, se hará uso del protocolo DHCP, un protocolo de configuración dinámica que permite al host obtener un servicio de red de tipo cliente/servidor, en la cual el servidor es el router Belisario quien otorgara una dirección IP a cada dispositivo.

Primero se debe asignar una dirección IP para el segmento de red a manejar, por lo que dentro de la ventana Adresses, haciendo clic en el botón añadir se digita la dirección que se desea. Así como la máscara correspondiente. Como se muestra en la figura 217.

Figura 217

Dirección IP para el segmento de red Lata_Belisario

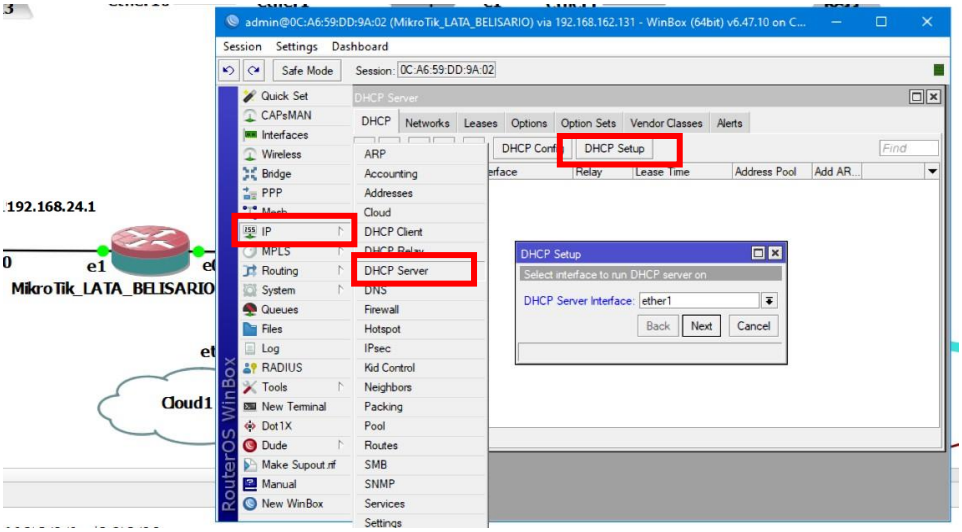


Nota. Procurar sea el puerto correspondiente en WinBox.

Para establecer el protocolo DHCP en el router Belisario sedespliega la opción IP del menú izquierdo, en la nueva ventana que se presente se da clic en la opción DCHP setup donde se mostrara una ventana de establecimiento para el puerto en la cual este protocolo va a funcionar, debe establecerse como lo muestra la figura 218.

Figura 218

Interfaz para servidor DHCP en MikroTik_LATA_BELISARIO

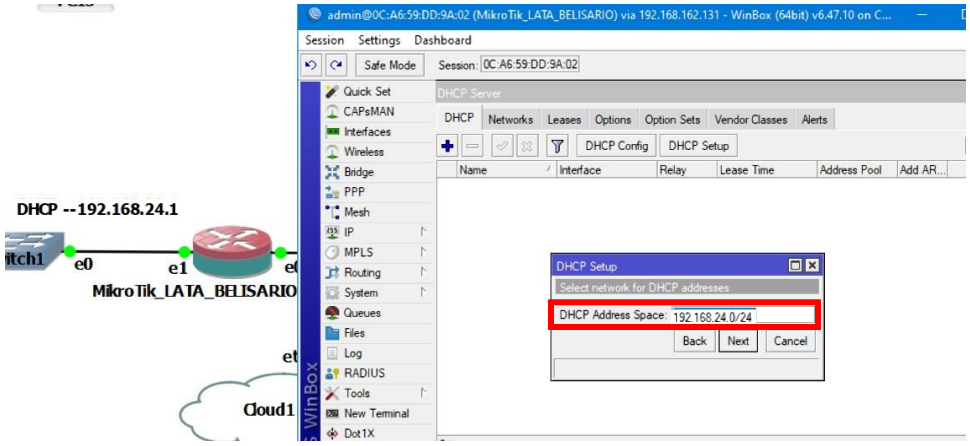


Nota. En este caso el puerto de Winbox si corresponde al puerto en GNS3.

Ahora al presionar Next se mostrará la dirección IP que está asignada para ese espacio la cual ya se estableció antes, se da clic en next y se establece automáticamente el Gateway como lo muestra la figura 219, luego se determinará el rango de direcciones fijas para los hosts, donde se puede reducir o ampliar el rango según. Como se muestra en la figura 220.

Figura 219

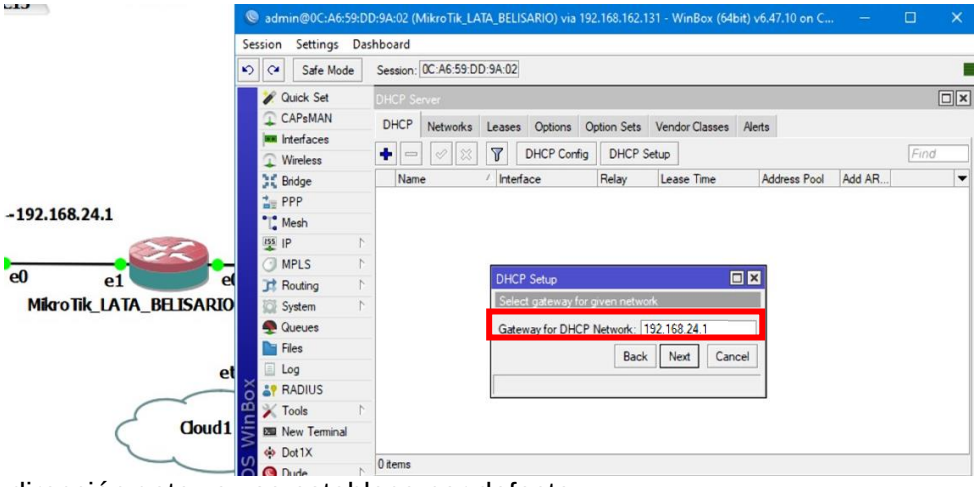
*Dirección IP para el segmento***.**



Nota. También se establece la máscara correspondiente.

Figura 220

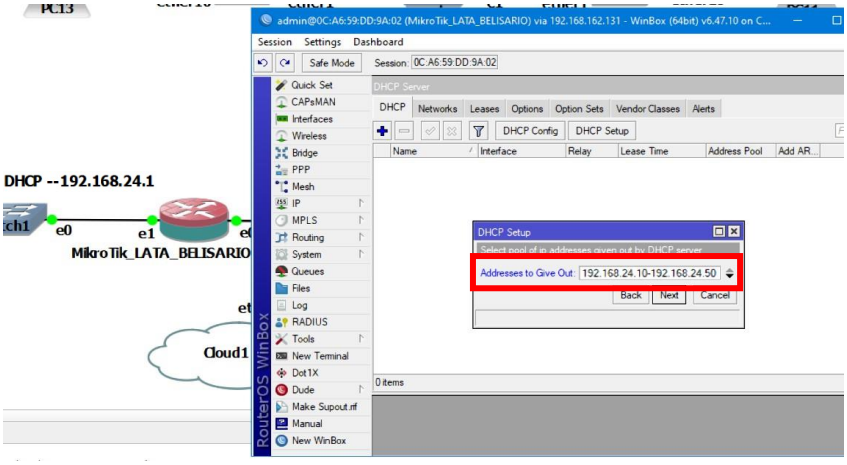
Dirección IP Gateway para el servicio DHCP



Nota. La dirección gateway se establece por defecto.

Figura 221

Rango de direcciones permitido para DHCP

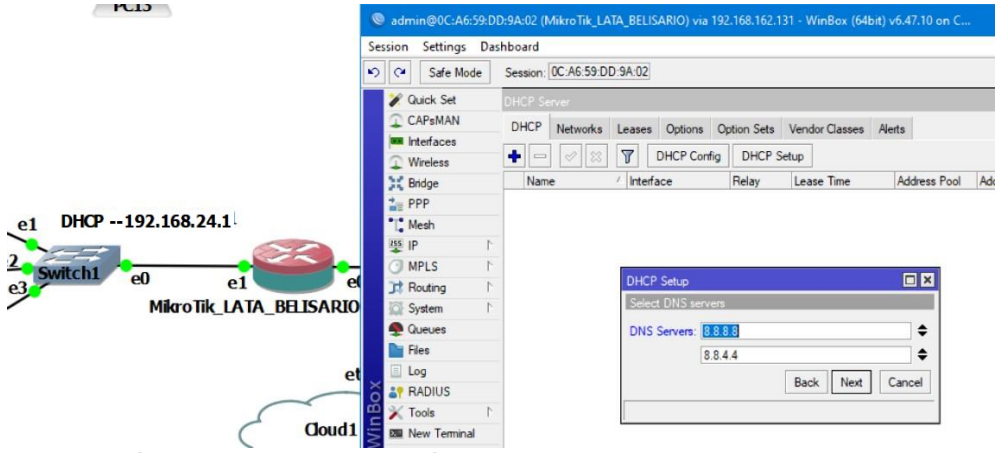


Nota. Se separa los limites por medio de un guion.

Al dar clic en Next se pedirá que se establezcan las direcciones de DNS, es aquí donde se pondrá las direcciones de Google para el servicio de internet, si se necesita aumentar otra dirección en la parte derecha del recuadro aparecen unas flechas donde se logra aumentar o reducir los campos, como se muestra en la figura y siguiente a esta configuración se pide el “lease time” que es el tiempo que transcurre hasta que la dirección IP otorgada al host cambie, para esta red se establece un tiempo de 40 minutos, como se muestra en la figura 223.

Figura 222

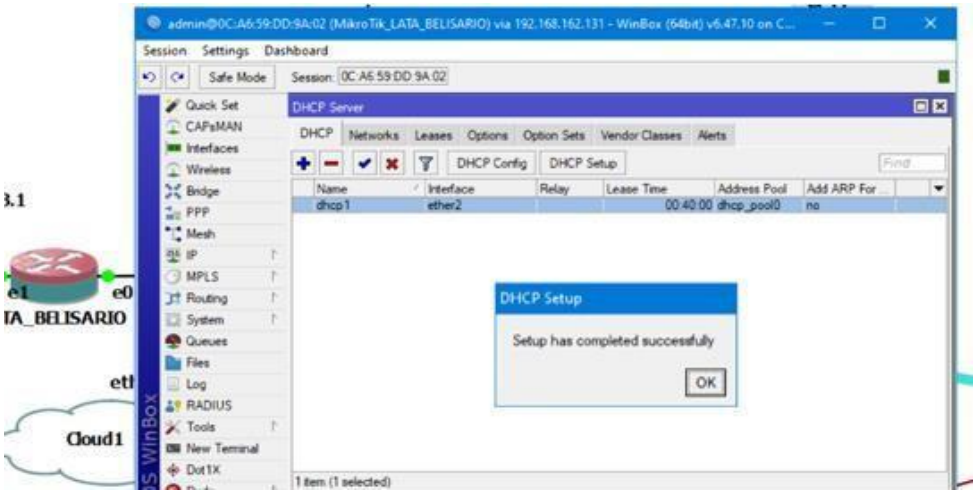
Direcciones DNS para DHCP



Nota. La conexión a internet dependerá de la interfaz conectada a la nube.

Figura 223

Creación del servidor DHCP en el router MikroTik_LATA_BELISARIO



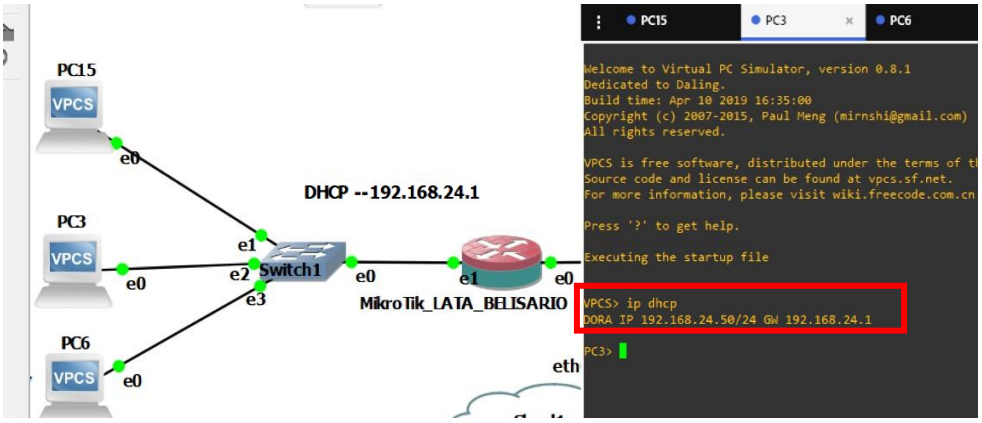
Nota. se puede realizar el proceso descrito si se hace clic en el botón añadir que presentara una interfaz para la configuración del servidor.

Una vez llegado a este punto se debe configurar a las VPCs para que obtengan una dirección IP bajo el protocolo DHCP, para esto se debe entrar al modo consola de los equipos y ejecutar el siguiente comando, el cual se muestra en la figura 224.

```
VPCS> ip dhcp
```

Figura 224

Asignación de dirección IP por medio de DHCP exitoso.



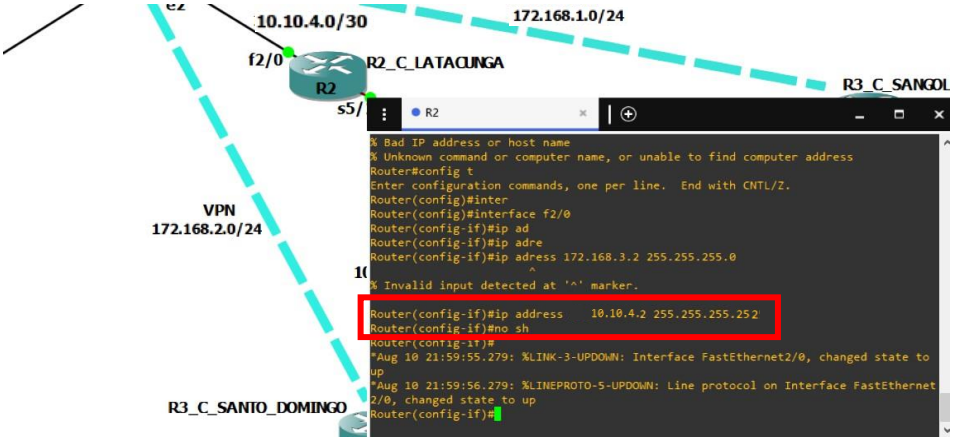
Nota. se establece la máscara y la dirección Gateway.

Red Sucursal Latacunga (Conexión entre equipo CISCO y MikroTik)

Es importante tener en cuenta que en partes de las redes de una topología van a necesitar de un segmento de red estático para que les permita conexión, como es el caso del segmento entre el R2_C_LATACUNGA y el router MikroTik_LATA_CENTRO, para el equipo CISCO se asigna una dirección ip como se muestra en la figura 225 y para el router mikrotik como se detalla en la figura 226.

Figura 225

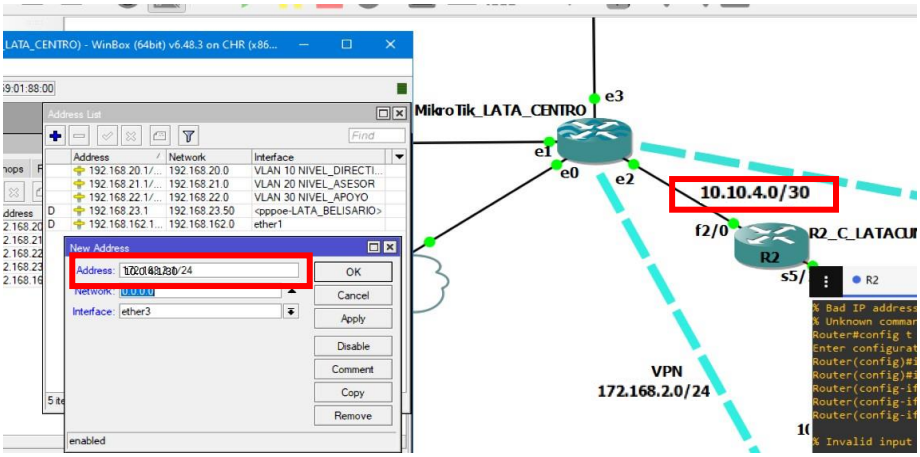
Dirección IP estática en R2_C_LATACUNGA



Nota. Los comandos ejecutados se han revisado previamente en este documento.

Figura 226

Dirección IP estática en MikroTik_LATA_CENTRO



Nota. los comandos ejecutados en esta figura se han revisado previamente en este mismo documento.

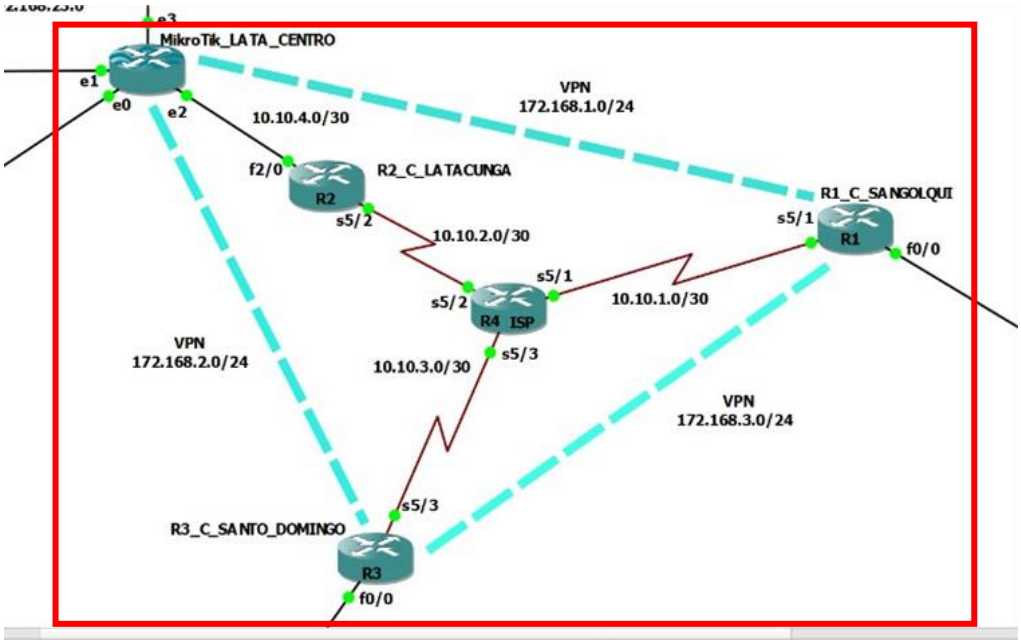
Red WAN

Ahora para la creación de una RED WAN donde se deben conectar todas las sucursales, se utilizará el protocolo OSPF, para conectar los 3 routers principales de cada ciudad y permitir la conexión desde cualquier punto de la red.

Para establecer esto la topología a configurar es la que se muestra en la figura 227, siendo el centro de intercambio de información entre las redes de cada campus o ciudad y los cuales contaran con una conexión por VPN que se configurara más adelante.

Figura 227

Red WAN para la topología de red corporativa.



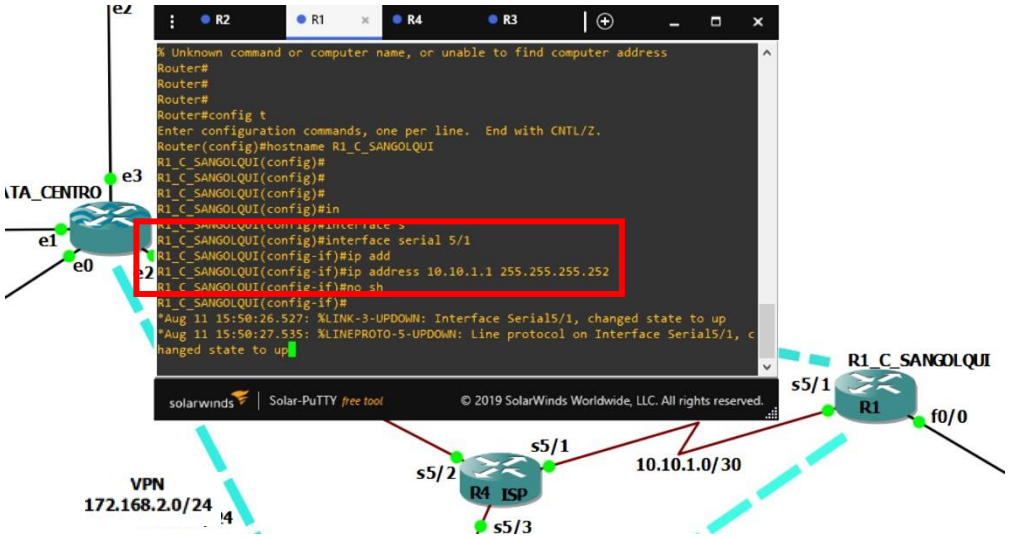
Nota. Se deben encender los equipos a utilizar en esta parte de la topología.

Red WAN (Implementación de protocolo OSPF)

Una vez que se hayan inicializado todos los routers, se debe entrar al modo consola de los mismos, el primer router a configurar será el R1_C_SANGOLQUI, y se le asigna un segmento de red para su conexión hacia el Router ISP con los comandos que previamente revisados y que se muestran en la figura 228.

Figura 228

Dirección IP en puerto de salida a red WAN en R1_C_SANGOLQUI

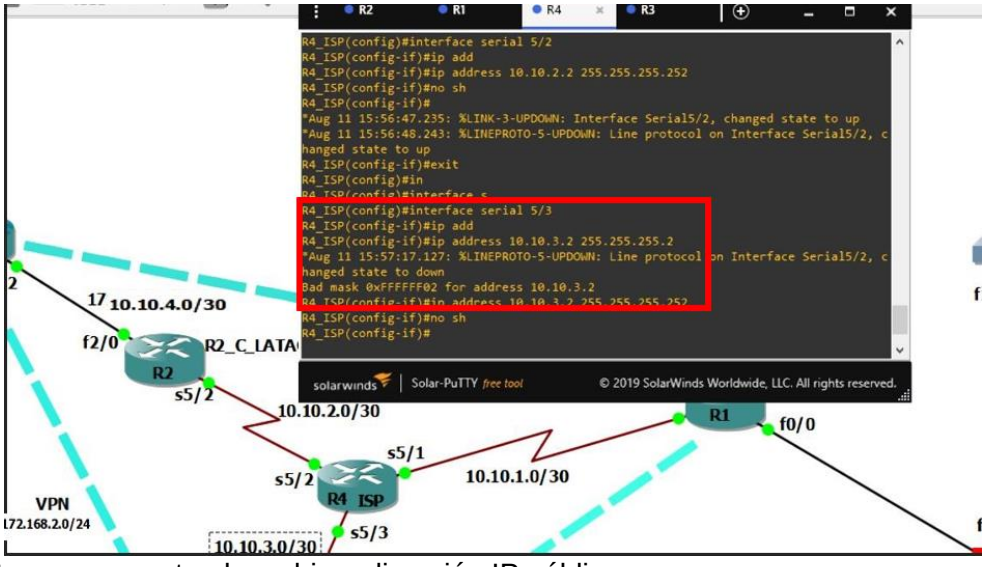


Nota. tener en cuenta el cambio a dirección IP pública.

De igual forma realiza el direccionamiento correspondiente en el router ISP que al ser el router central debe contar con 3 direcciones en las respectivas interfaces, los cómo se muestra en la siguiente figura 229 y de igual manera el direccionamiento en el R2 y R3 que se muestran en las figuras 230 y 231.

Figura 229

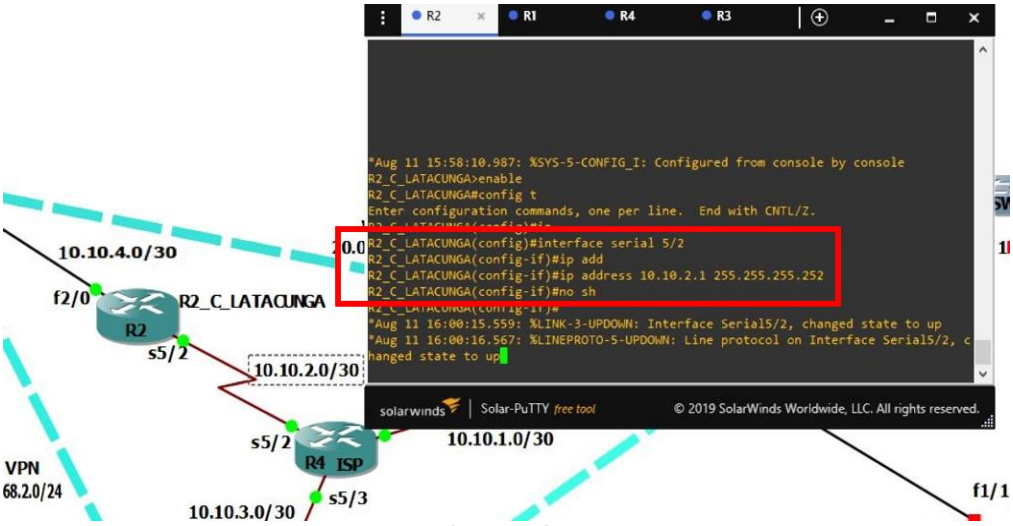
Direccionamiento en R4_ISP.



Nota. tener en cuenta el cambio a dirección IP pública.

Figura 230

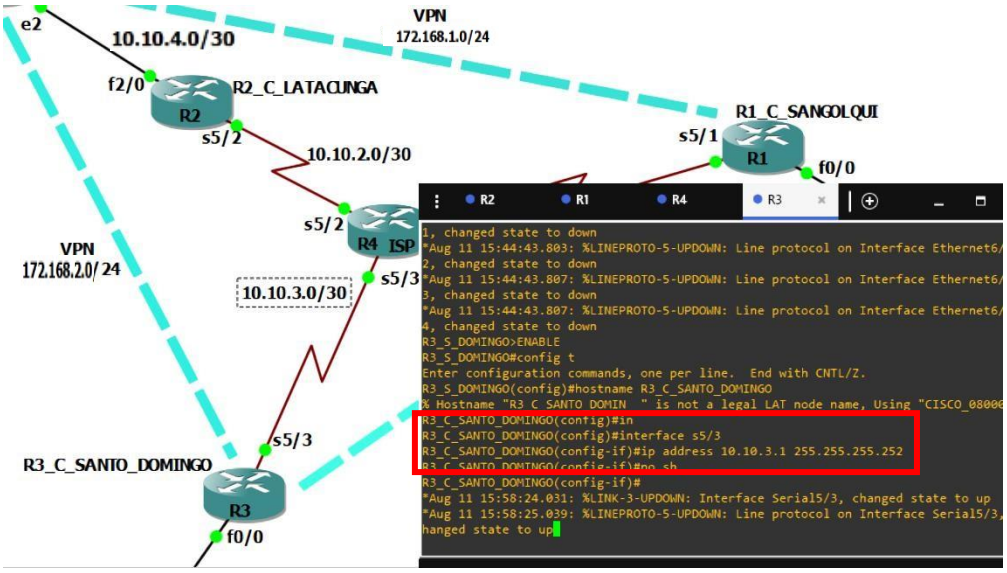
Direccionamiento en R2_C_LATACUNGA



Nota. tener en cuenta el cambio a dirección IP pública.

Figura 231

Direccionamiento en R3_C_SANTO_DOMINGO



Nota. tener en cuenta el cambio a dirección IP pública.

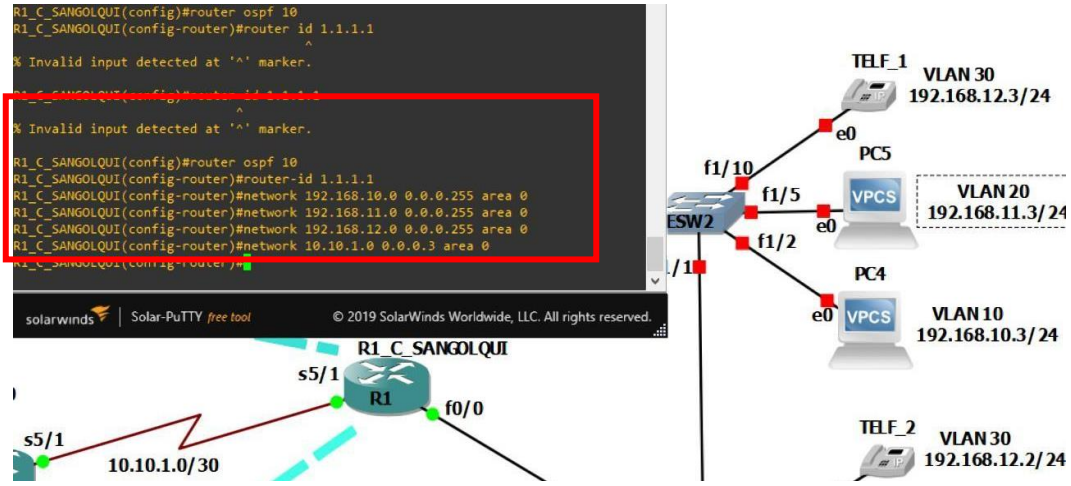
Ahora para el enrutamiento se utilizará el protocolo de enrutamiento OSPF el cual se inicia con el Router 1 y dentro de la configuración global se habilita OSPF por de los siguientes comandos

```
R1_C_SANGOLQUI#config t
R1_C_SANGOLQUI(config)#router ospf 10
R1_C_SANGOLQUI(config-router)#router id 1.1.1.1
R1_C_SANGOLQUI(config-router)#network 192.168.10.0 0.0.0.255area 0
```

Como se muestra en la figura 232 además de eso se debe otorgar un identificador dentro del proceso de OSPF, posterior a esto se debe configurar las redes conectadas al router, siendo estas las direcciones de VLANs para la red Sangolquí, además de la dirección de red para la conexión con el router ISP que se había establecido previamente.

Figura 232

Protocolo OSPF en R1_C_SANGOLQUI

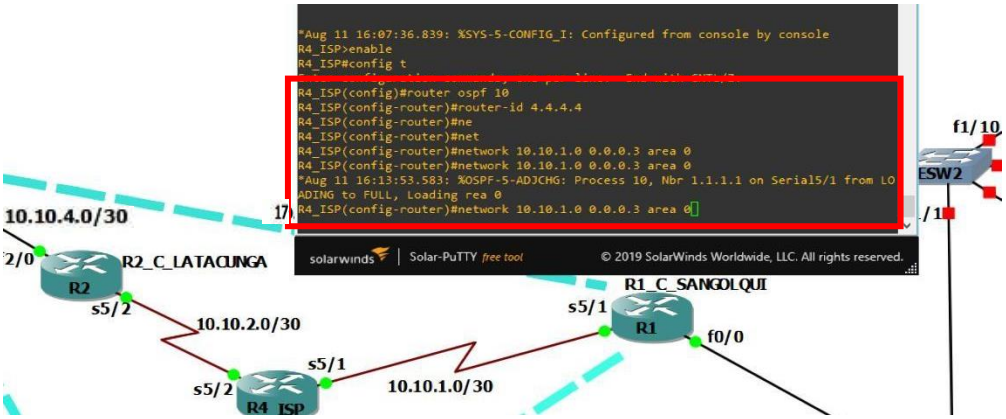


Nota. Se debe establecer todas las direcciones IP que intervengan en el router, con su máscara wildcard correspondiente.

El proceso de OSPF en el router 1 estaría completo, este proceso se lo realiza en el equipo R4_ISP con sus respectivas redes, como se muestra en la figura 233 cuando se haya establecido una de las direcciones IP que ya cuenten con el servicio de OSPF en el router correspondiente la consola indicara un mensaje como se muestra en la misma figura

Figura 233

Protocolo OSPF en R4_ISP

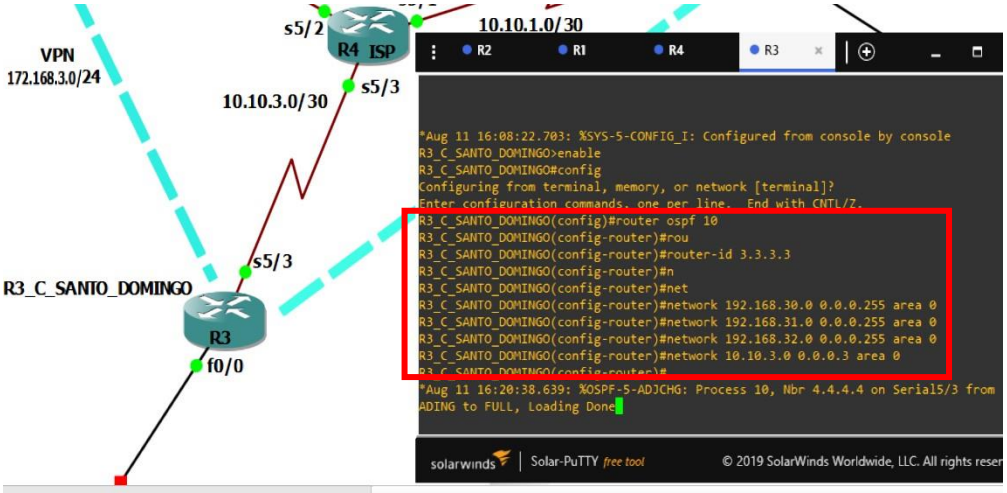


Nota. El mensaje muestra el identificador con la abreviatura NBR.

Como ultima demostración se establece el mismo proceso de configuración para el router 3 con sus respectivas redes de VLANS y de conexión al router ISP como se muestra en la figura 234, en donde se emite el mensaje por su conexión a R4_ISP

Figura 234

Protocolo OSPF en R3_C_SANTO_DOMINGO



Nota. se recomienda el ID sea el numero previsto para el equipo.

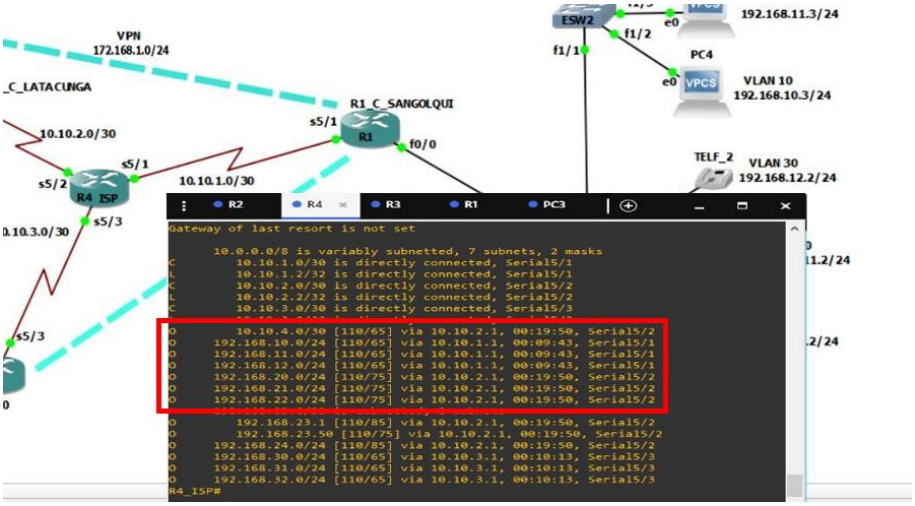
La mejor manera de comprobar el enrutamiento realizado es ejecutando el siguiente comando en el cual se describe la conexión de cada ruta establecida en el equipo, por medio de que puerto y el protocolo que se está usando para esa conexión

```
R4_ISP# show ip route
```

Como se muestra en la figura 235 para el router R4_ISP se observa las redes conectadas directamente y las redes tanto de sangolqui como de santo domingo a las cuales tiene acceso por medio del protocolo OSPF

Figura 235

Comando show Ip route en R4_ISP



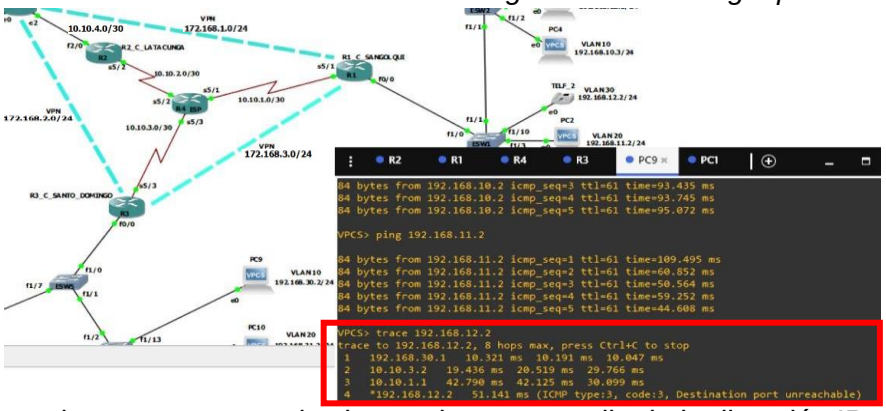
Nota. por delante de las direcciones con acceso se encuentra la letra O que hace referencia al protocolo OSPF.

Para este punto debe existir conexión desde las redes LAN tanto de Santo Domingo como de Sangolquí, se puede emitir un envío de paquetes hacia los hosts para determinar si la conexión es correcta, se realiza en la figura 236 por medio del siguiente comando denominado “traza de ruta”

```
VPCS> trace 192.168.12.2
```

Figura 236

Comando Trace router desde la red Santo domingo hacia red Sangolquí.

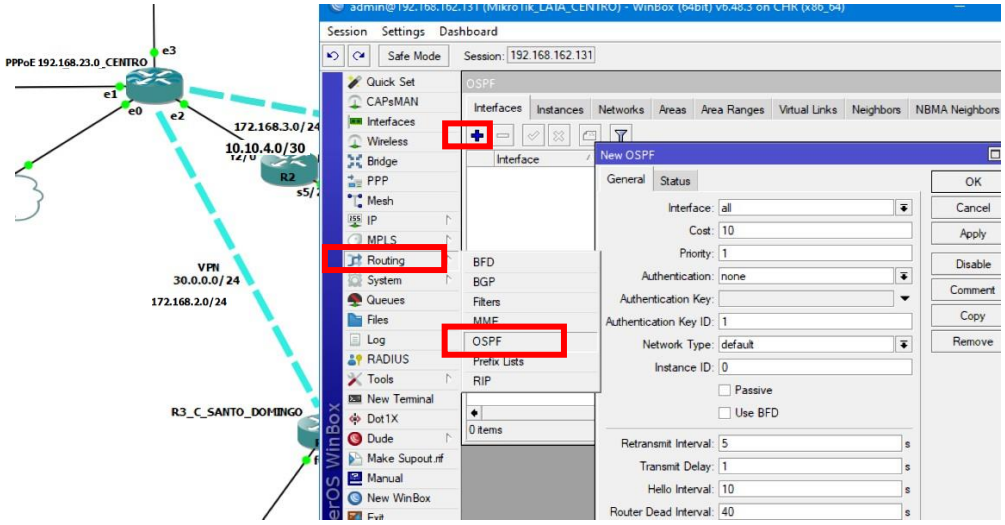


Nota. la traza de ruta muestra todos los equipos por medio de la dirección IP.

Con respecto a la red LAN de Latacunga la cual está dominada por dispositivos MikroTik para establecer OSPF, primero dentro del software WinBox se debe dar clic en la opción routing y en el submenú que aparezca ingresar en la opción OSPF, en la pestaña interfaces se añade el protocolo. Como se muestra en la figura 237.

Figura 237

Interfaz OSPF en router MikroTik_LATA_CENTRO.

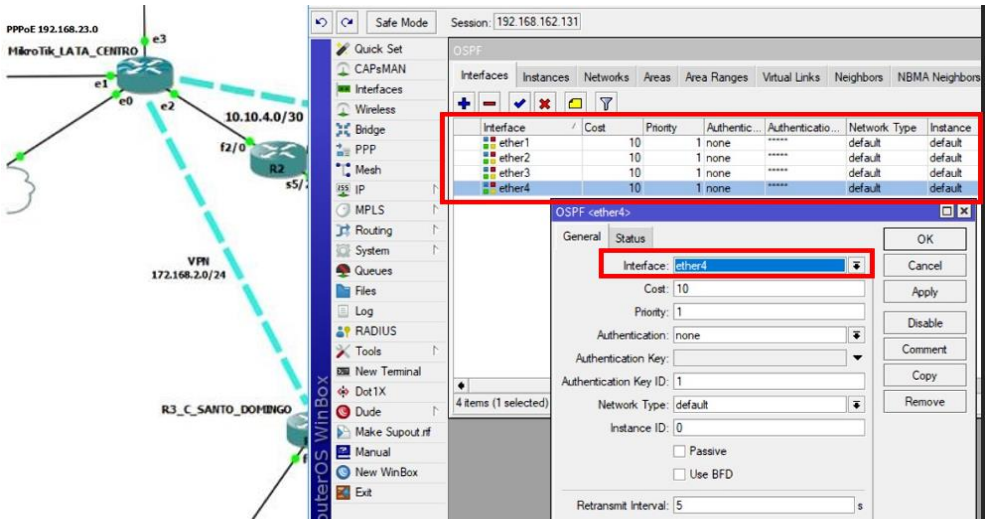


Nota. se debe establecer OSPF en todas las interfaces.

En este punto se ubican los puertos que deben tener habilitado el protocolo de OSPF esto incluye la red PPPoE de Belisario, la red LAN de Latacunga centro donde se encuentran las VLANS y de igual manera la interfaz de conexión a la WAN, en el campo de “interface” selecciona los respectivos puertos y se da clic en apply y OK. Como se muestra en la figura 238.

Figura 238

*Asignación de puertos con OSPF en router MikroTik_LATA_CENTRO***.**

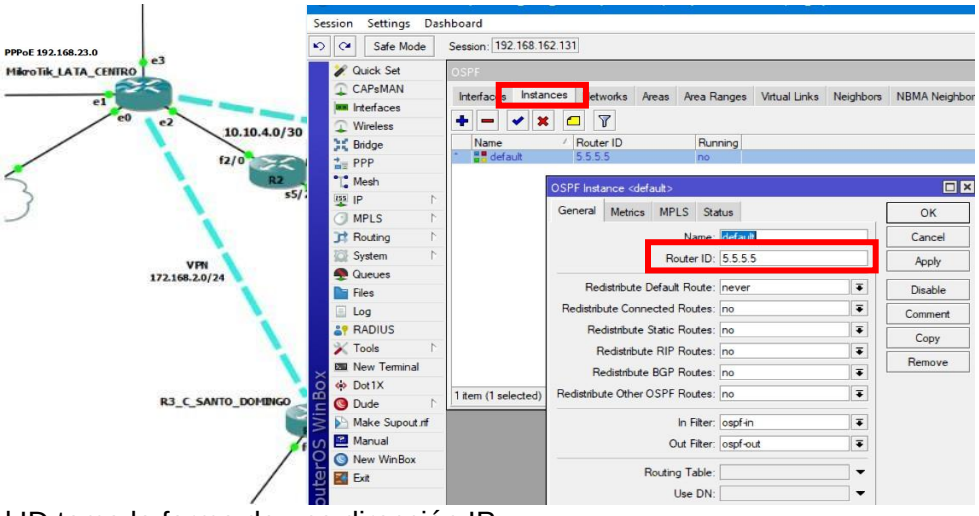


Nota. las interfaces ya establecidas con OSPF se mostrarán en el listado general.

Además de esto se debe configurar un identificador al router lo que se denominaba “ID” en los routers CISCO, para esto se da clic en la pestaña “instances” de la interfaz de OSPF donde se muestra que ya existe un ID por defecto, es preferible cambiar esta identificación como se muestra en la figura 239.

Figura 239

Identificación para OSPF del router MikroTik_LATA_CENTRO

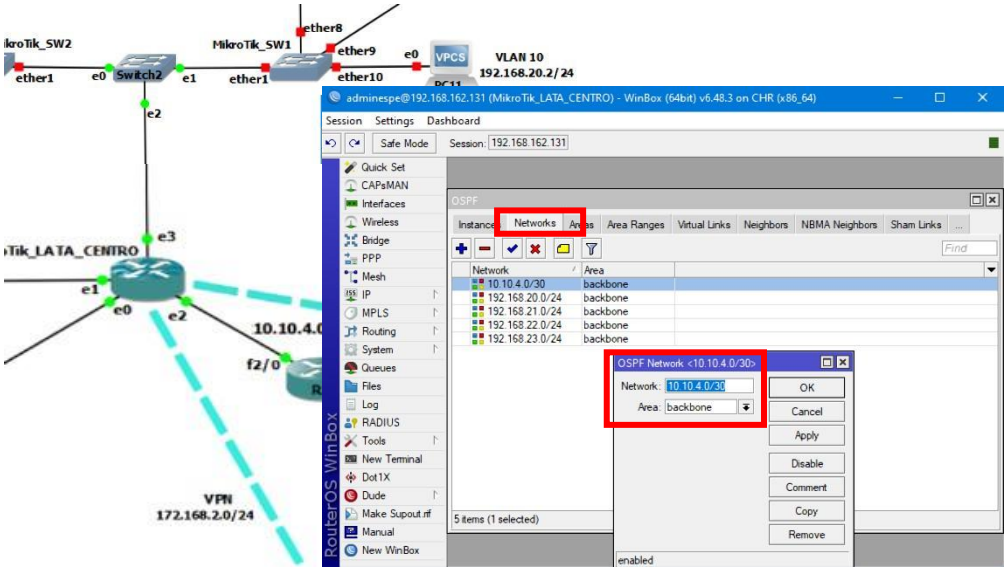


Nota. el ID toma la forma de una dirección IP.

Después se debe realizar el enrutamiento de las direcciones de red a las cuales OPSF deben tener acceso, para este caso dentro de la pestaña NETWORKS se añade una nueva red y en la pequeña ventana que se muestre se digita las diferentes direcciones que estén conectadas, como se muestra en la figura 240.

Figura 240

Enrutamiento de redes por OSPF en router MikroTik_LATA_CENTRO

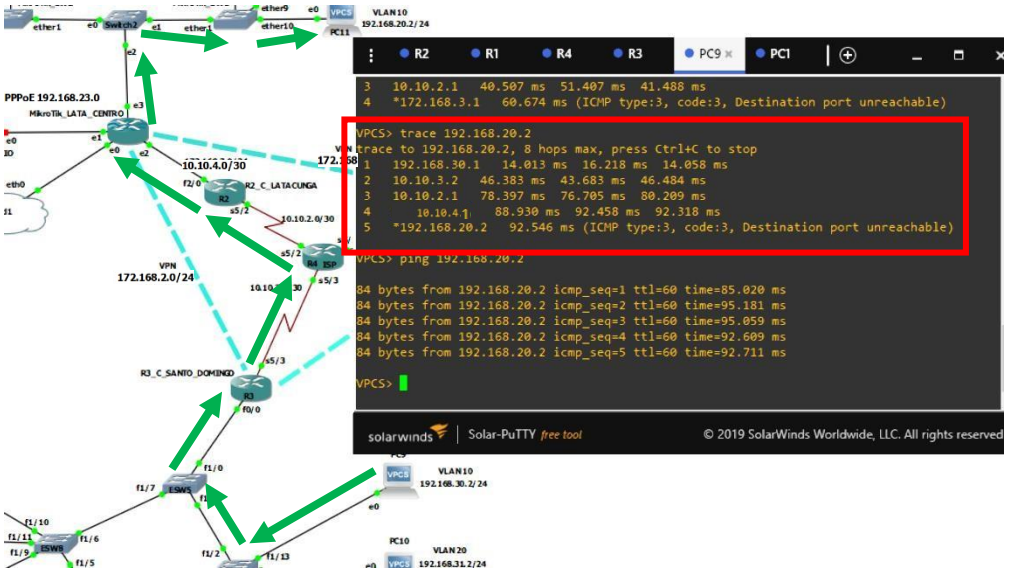


Nota. al ser una red no tan extensa se puede asignar el área “backbone”.

De esta manera ya estaría establecido el proceso de OSPF dentro de la red de Latacunga si se desea comprobar la conexión entre todas las redes se realiza un ping desde la PC9 hasta la PC1, y como se muestran en las figuras 241 y 242. La conexión es exitosa.

Figura 241

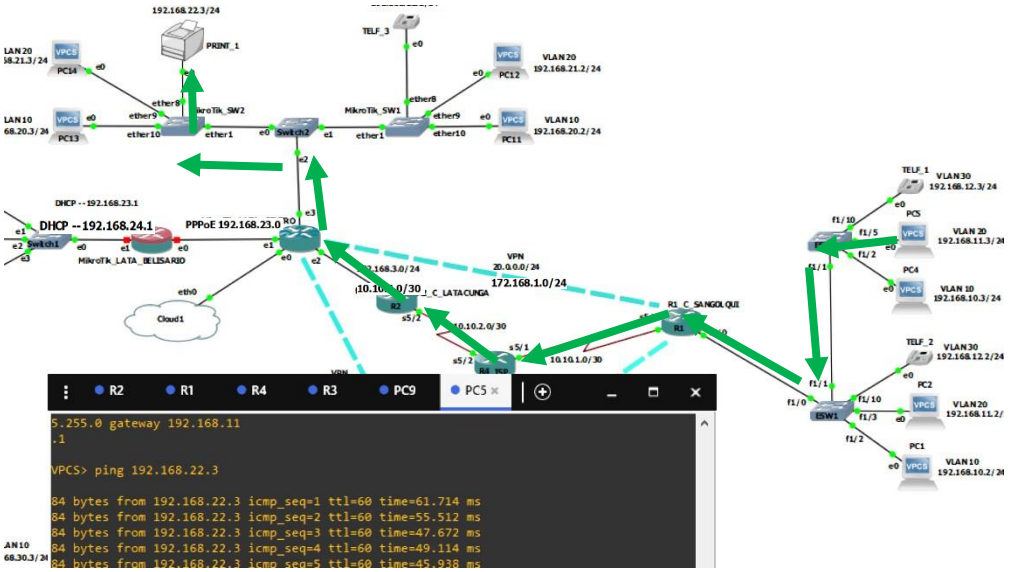
Envió de paquetes exitoso por medio de OSPF en la red LATACUNGA



Nota. el comando trace demuestra los equipos que intervienen.

Figura 242

Envió de paquetes exitoso por medio de OSPF en la red LATACUNGA



Nota. El comando ping no demuestra los equipos que intervienen.

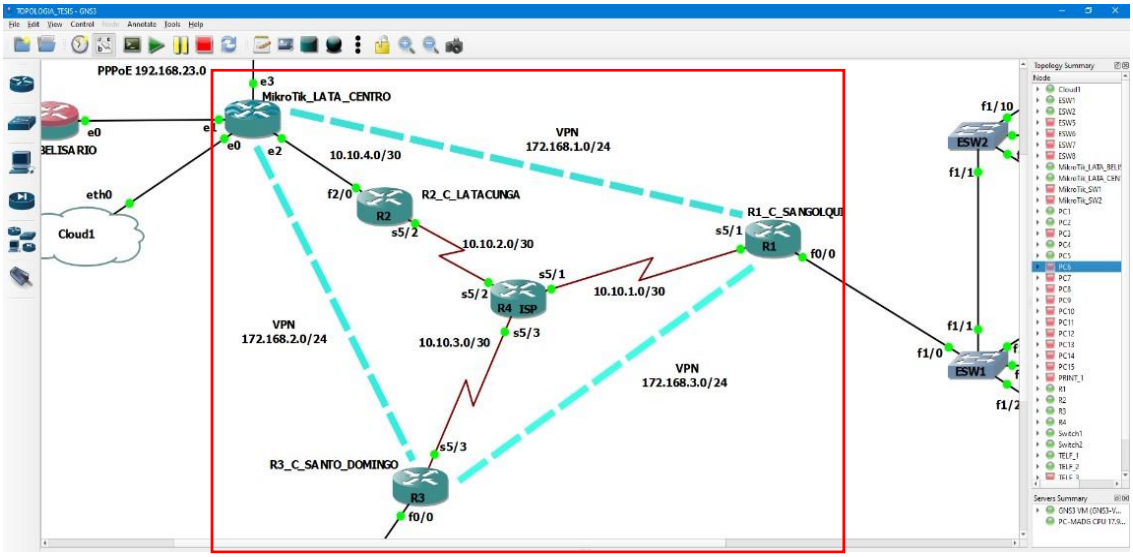
Red WAN (Implementación de VPN por túneles GRE)

Si bien el protocolo OSPF permite la conexión entre las distintas REDES LAN en la realidad existen muchos más componentes que se encuentran en medio de las sucursales de una red corporativa de manera en que el envío de conexiones puede retardarse y ser inseguro.

Para lo mismo se hará uso de la tecnología VPN (Virtual Private Tunnel) el cual reduce los caminos de enrutamiento entre dos destinos establecidos, los túneles que establece se realizan en los routers principales de cada red LAN. Como se muestra en la topología y en la figura 243 a continuación.

Figura 243

Muestra de la red para el uso de VPN



Nota. la tecnología VPN se utiliza para el intercambio entre las sucursales de la RED corporativa ESPE.

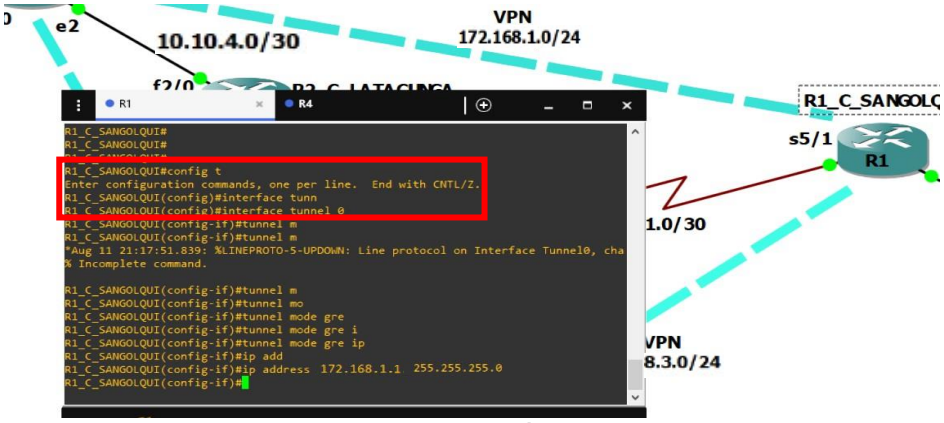
Para la configuración de VPNs es necesario que en cada uno de los routers se establezca una subinterfaz virtual de tipo túnel, para esto se debe ingresar en el modo consola y ejecutar los siguientes comandos como se muestran en la figura 244.

```
R1_C_SANGOLQUI(config)# interface túnel 0
```

```
R1_C_SANGOLQUI(config-if)# tunnel mode gre ip
R1_C_SANGOLQUI(config-if)#ip add 172.168.1.1 255.255.255.0
```

Figura 244

Creación de la interfaz túnel 0 en R1_C_SANGOLQUI



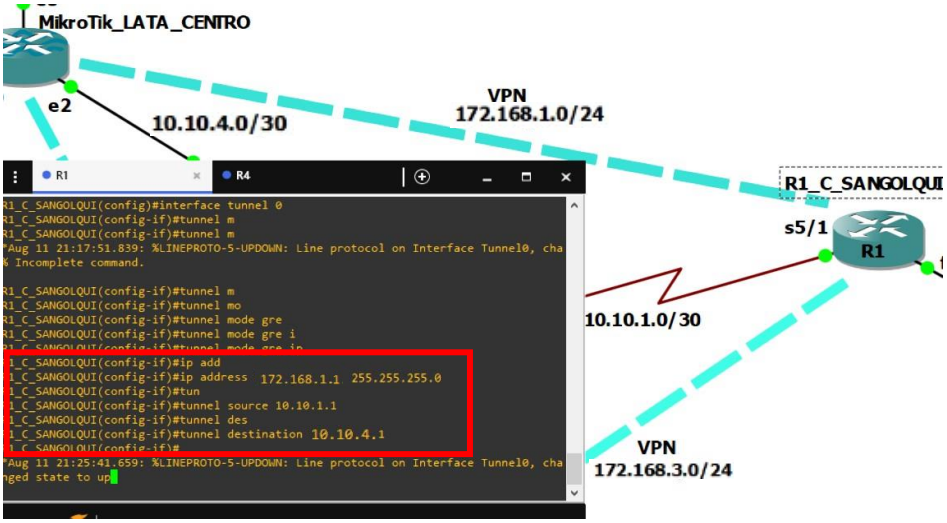
Nota. el modo GRE es un protocolo para conexión de sitio a sitio.

La interfaz debe contar con una dirección IP como ya se estableció en la figura anterior, para las interfaces de tipo túnel en su configuración se debe determinar el puerto o dirección de origen y de destino, de manera en que se deben ejecutar los siguientes comandos, que se muestra en la figura 245.

```
R1_C_SANGOLQUI(config-if)#tunnel source 10.10.1.1
R1_C_SANGOLQUI(config-if)#tunnel destination 10.10.4.1
```

Figura 245

Destino y origen del túnel 0 para R1_C_SANGOLQUI

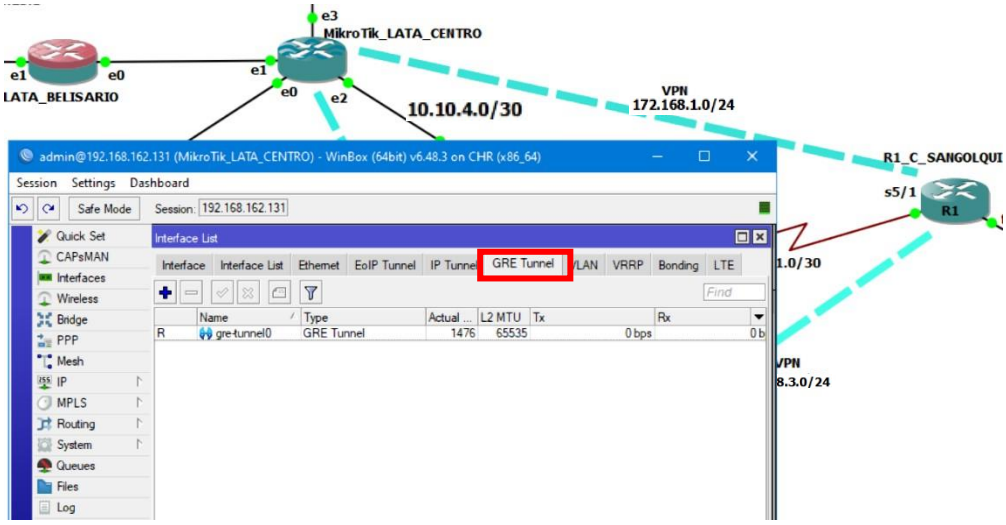


Nota. Para estos parámetros no es necesario la máscara de red.

Es en este punto de la configuración donde se establece el origen y el destino, los cuales se pueden establecer al digitar la dirección IP o el nombre del puerto, se debe realizar la misma configuración por el lado del router Mikrotik de Latacunga. Para esto se debe dar clic en la opción interfaces del programa WinBox del router LATACUNGA_CENTRO y entrar en la pestaña GREE TUNNEL

Figura 246

Interfaz para la creación del túnel 0 en MikroTlk_LATA_CENTRO

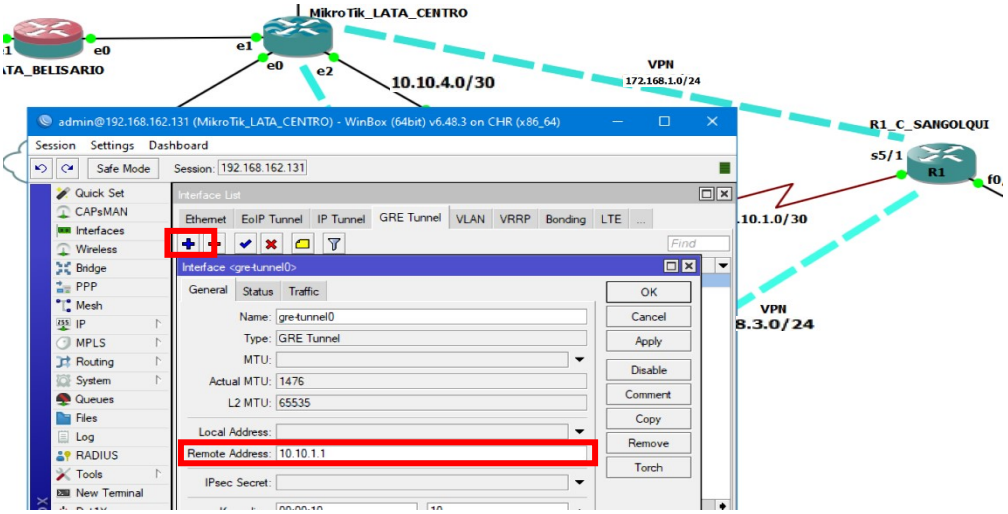


Nota. En MikroTik se puede observar todas las opciones de interfaces.

Al dar clic en el botón añadir se presenta una interfaz donde se digita los principales detalles del túnel GRE a crear, primeramente, establecer el nombre “gretunnel 0”, por otro lado, también se muestra el tipo del túnel el cual es GRE. Y por debajo de estos campos también se solicita el “REMOTE ADDRESS” en donde se digita la dirección IP de destino, que en este caso en la dirección del puerto serial 5/1 del router R1_C_SANGOLQUI. Una vez que se llenen estos campos se da clic en APPLY y OK, como se muestra en la figura 247.

Figura 247

Creación de la interfaz túnel 0 en MikroTIk_LATA_CENTRO

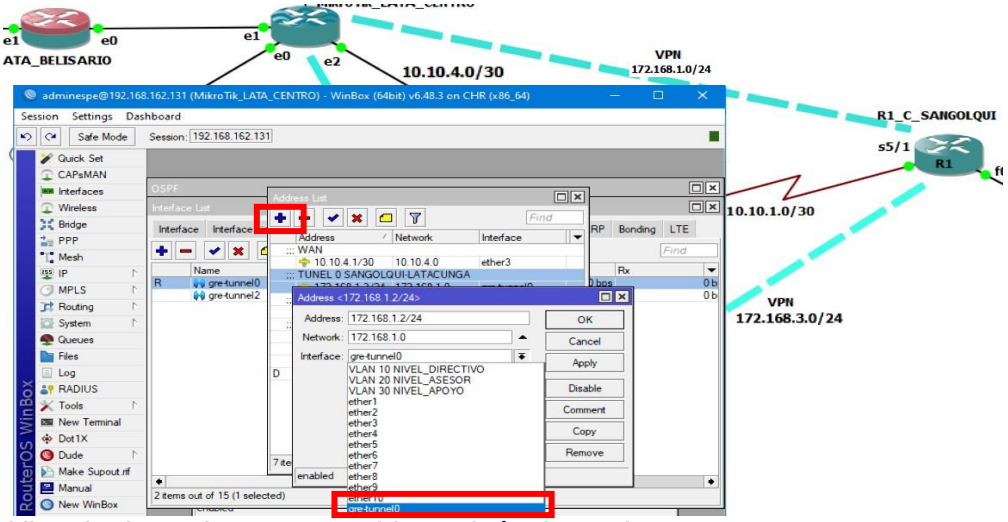


Nota. la dirección de destino no requiere mascara.

A continuación, se debe establecer la dirección IP de origen para la interfaz “gre-tunnel0” recién creada, para esto dentro del menú IP-ADDRESS dando clic en el botón añadir se digita la dirección IP correspondiente y seleccionar la interfaz por medio del listado de opciones como se muestra en la figura 248.

Figura 248

Origen del túnel 0 para MikroTIk_LATA_CENTRO

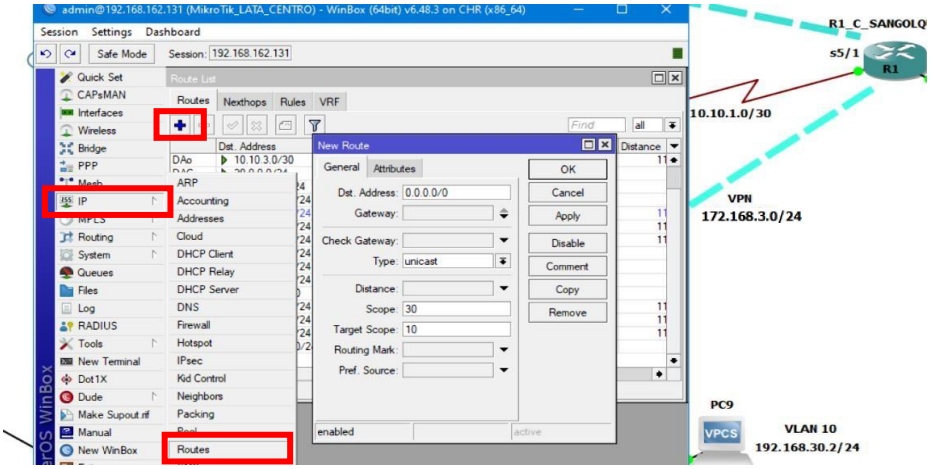


Nota. el listado de opciones ya establece el túnel creado.

Ahora se establecen las rutas a las cuales la tecnología VPN deberá conectar, para esto es necesario que se determinen las rutas de los dos lados, para el router MikroTik se debe dar clic en IP-route del menú de la izquierda, se da clic en el botón añadir y una sub-interfaz solicitara los campos que se muestra en la figura 249.

Figura 249

Interfaz "IP route" del router MikroTlk_LATA_CENTRO

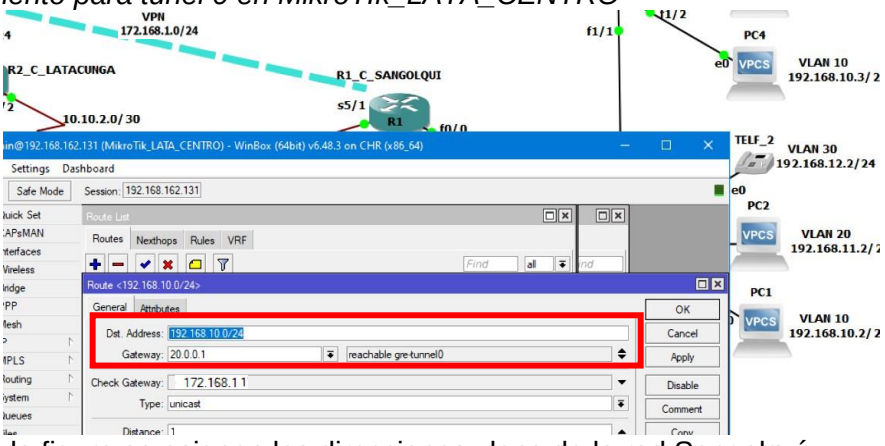


Nota. la interfaz muestra las rutas que el router tiene acceso.

Es aquí donde se colocará las direcciones de la red LAN de Sangolquí, y en el apartado Gateway se pondrá la dirección de destino del túnel 0, a un lado de este campo se debe determinar la interfaz de túnel, como se muestra en la figura 250.

Figura 250

Enrutamiento para tunel 0 en MikroTlk_LATA_CENTRO

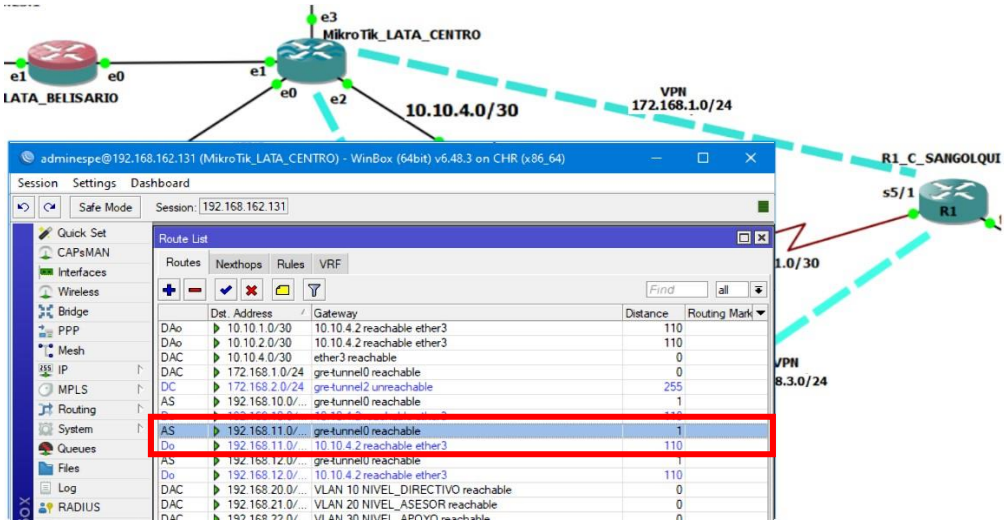


Nota. en la figura se asignan las direcciones vlans de la red Sangolquí.

Una vez que se hayan establecido los campos y guardada la configuración en el listado de IP routes por debajo del túnel GRE se establecen todas las rutas con acceso para esa interfaz virtual “gre-tunnel0”, como se muestra en la figura 251.

Figura 251

Rutas para el tunel 0 en MikroTIk_LATA_CENTRO por VPN



Nota. Las rutas por OSPF se muestran de color azul.

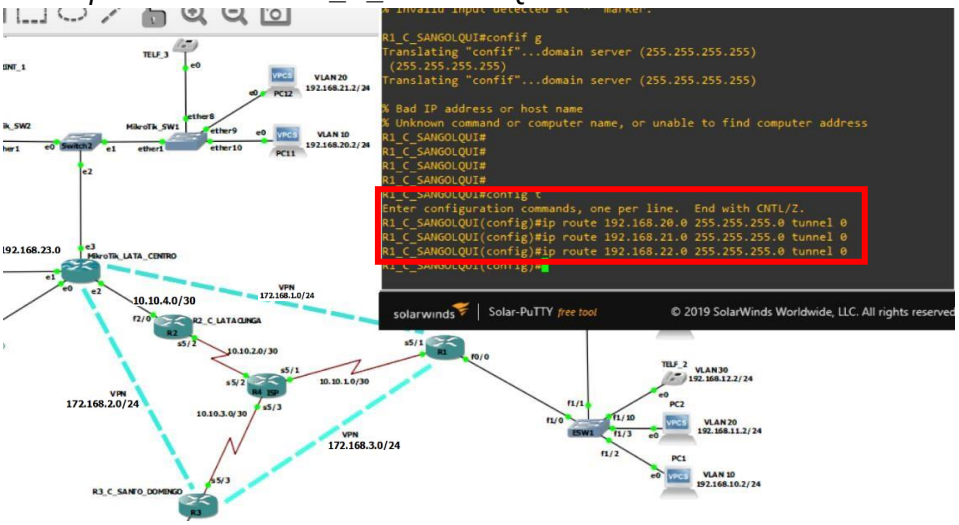
Es muy posible que aquellas rutas de tunnel GRE que se crearon muestren a su izquierda la etiqueta “AS” de Activas y Estáticas. Ahora se realiza el mismo proceso de enrutamiento para el tunnel 0 en R1_C_SANGOLQUI, dentro del modo consola del equipo y en la configuración privilegiada se ejecutan los siguientes comandos.

```
R1_C_SANGOLQUI(config)#ip route 192.168.20.0 255.255.255.0 tunnel 0
R1_C_SANGOLQUI(config)#ip route 192.168.21.0 255.255.255.0 tunnel 0
R1_C_SANGOLQUI(config)#ip route 192.168.22.0 255.255.255.0 tunnel 0
```

Donde es necesario establecer la dirección IP seguido por su correspondiente mascara y la interfaz por la cual estas redes van a ser enrutadas que es el túnel 0, esto se muestra en la figura 252.

Figura 252

Enrutamiento para túnel 0 en R1_C_SANGOLQUI



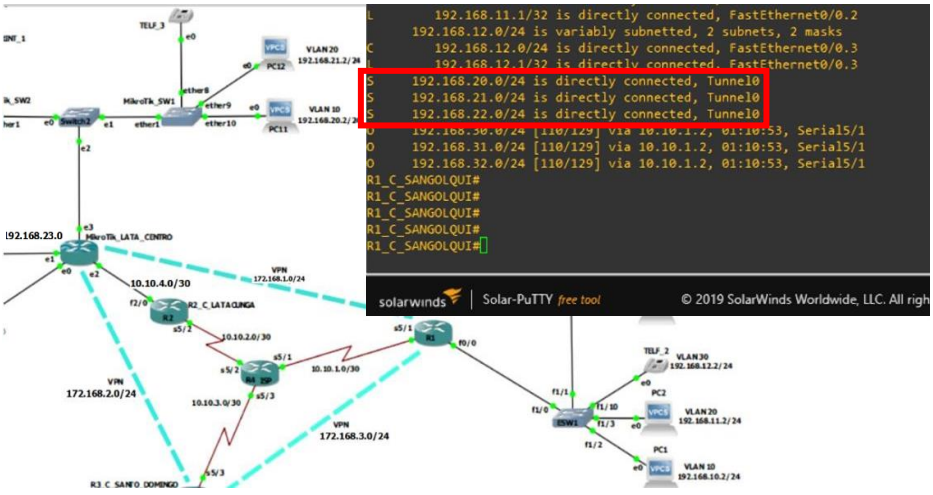
Nota. Se establece las direcciones vlans que se encuentran en Latacunga.

Para revisar el estado en que se encuentran las rutas se ejecuta el siguiente comando en el modo de configuración global, como se muestra en la figura 253 y en las últimas líneas debería mostrarse las rutas creadas con el prefijo S de estáticas.

```
R1_C_SANGOLQUI #show ip route
```

Figura 253

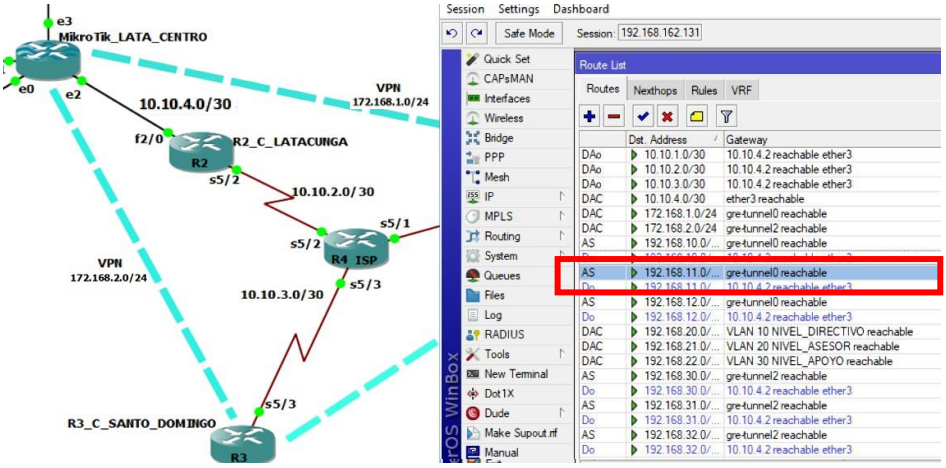
Rutas para el tunel 0 en R1_C_SANGOLQUI por VPN



Nota. también se debe mostrar la asignación de rutas al tunel 0.

Se repite el proceso anterior creando nuevos túneles de VPN para la conexión entre todas las sucursales, estableciendo las direcciones IP correspondientes, en las figuras 254 y 255 se muestra la tabla de enrutamiento tras este proceso para el equipo R3 Y MIKROTIK_LATA_CENTRO, por el momento no se tomará en cuenta a la red de BELISARIO, con el fin de comparar OSPF y VPN

Figura 254

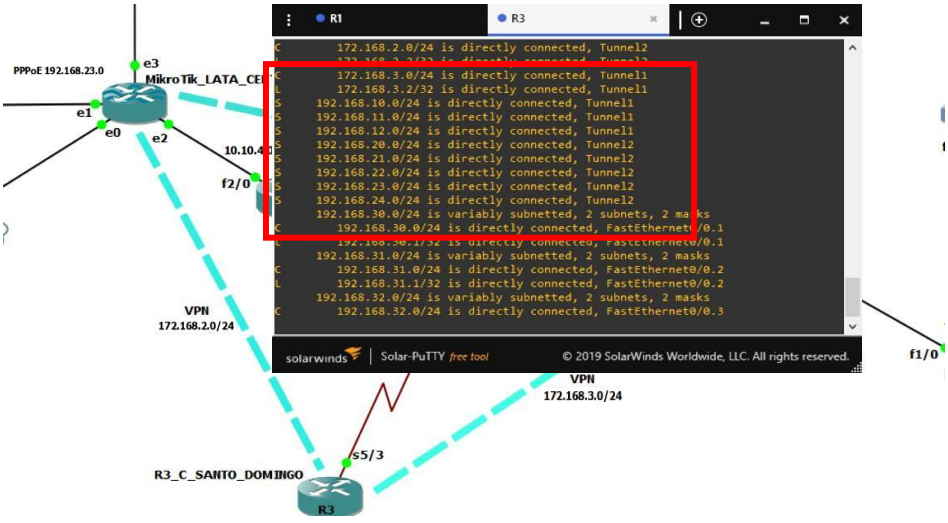


Rutas para el túnel 2 en MikroTik_LATA_CENTRO por VPN

Nota. túnel 2 corresponde a conexión Latacunga-S. Domingo.

Figura 256

Rutas para el túnel 1 y túnel 2 en R3_C_SANTO_DOMINTO por VPN

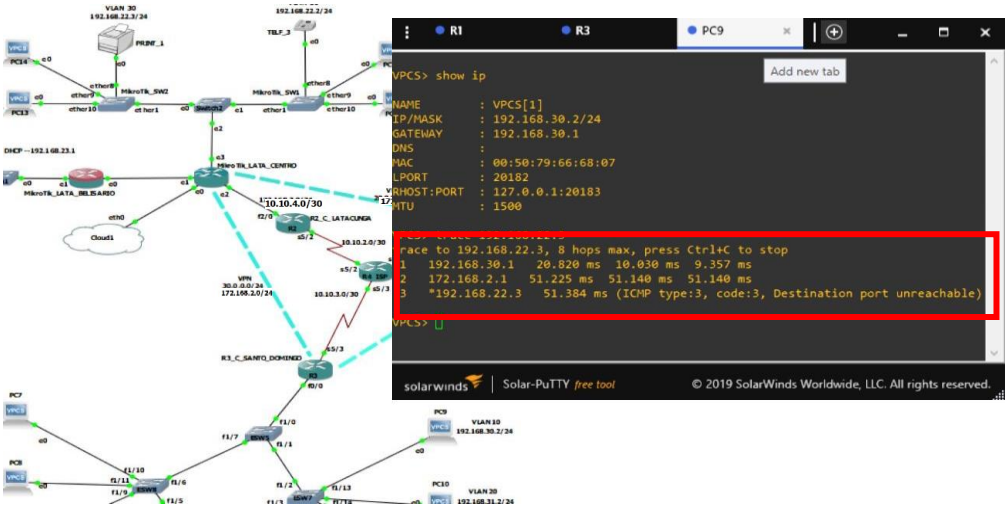


Nota. Túnel 1 corresponde a conexión S. Domingo-Sangolquí y túnel 2 corresponde a conexión S. Domingo-Sangolquí.

Ahora para comprobar el funcionamiento y la utilidad de la tecnología VPN. Se realiza un trace route desde la red de santo domingo hacia la red de Latacunga y se compara el proceso a partir del protocolo OSPF y el uso de las rutas estáticas hacia los túneles de VPNs creados, como en la figura 257.

Figura 257

Funcionamiento exitoso de VPN por el túnel 2



Nota. El proceso ahorra dos destinos intermedios de red, R2 y R4_ISP.

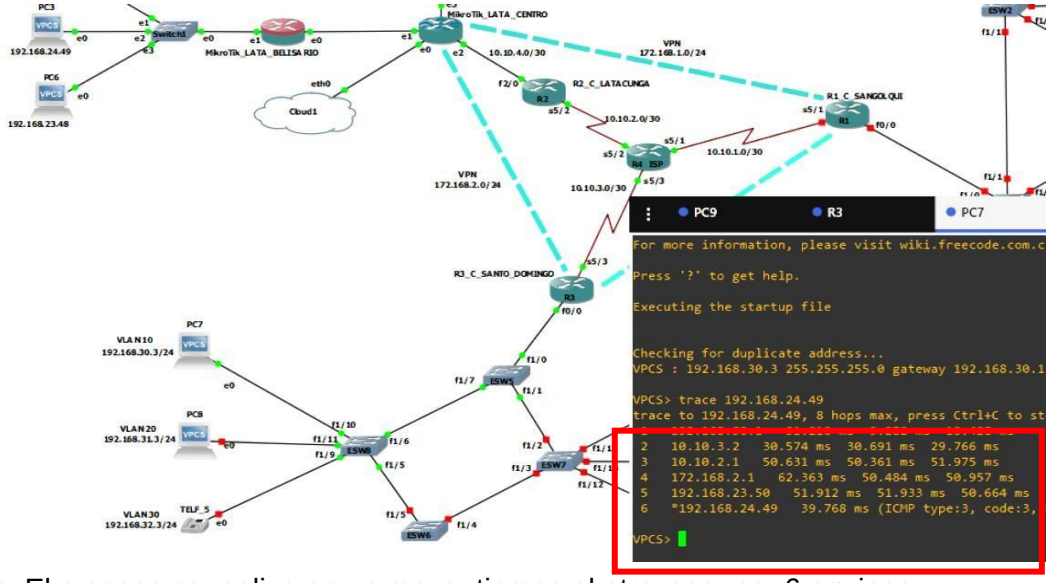
Desde la PC9 se dirige al router de santo domingo y este envía los paquetes directamente hacia el router Mikrotik_LATA_CENTRO, y finalmente hacia el host de destino que es el print_1, de esta forma los túneles de VPN ahorran él envió de paquetes hacia dos routers dentro de la red WAN. Por cuanto al protocolo OSPF realizaría un enrutamiento hacia todos los terminales que se encuentren en la red.

Para comprender la utilidad de los túneles GRE implementados se realizará un envío de paquetes de la red Santo Domingo hacia la red del campus Belisario en Latacunga la cual no se había establecido en las rutas estáticas del túnel 2 en R3_C_SANTO DOMINGO. Como lo

muestra la figura 258 el protocolo OSPF determina la conexión por todos los equipos que se encuentran en la red.

Figura 258

Comparación de enrutamiento sin túnel 2



Nota. El proceso se realiza en un mayor tiempo al atravesar por 6 equipos.

Seguridad y Configuraciones en la Red

La seguridad es muy importante para cualquier red de datos, y esta topología no es la excepción, como ejemplo primero se establecerá la seguridad los routers de cada campus.

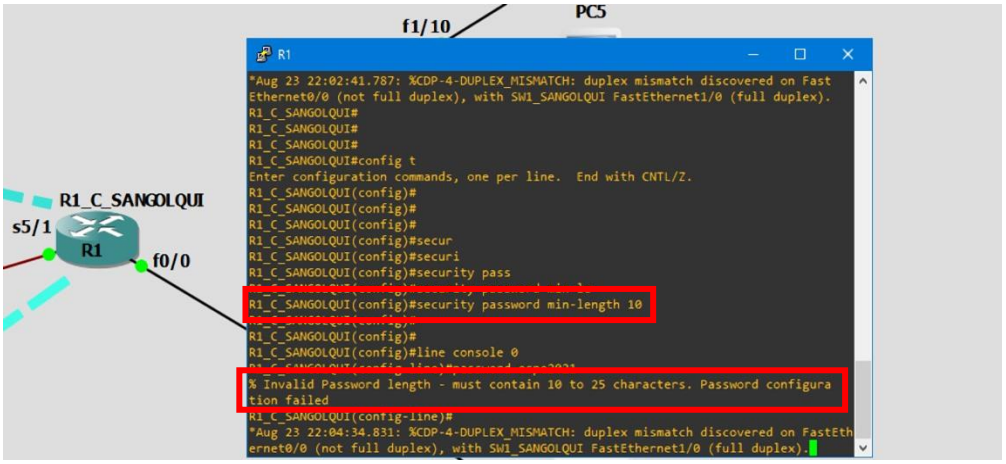
Seguridad en equipos CISCO

Por medio de los siguientes comandos, primero se definirá el mínimo de caracteres a establecer para las contraseñas en el proceso, si se determina una contraseña por debajo del máximo se emitirá un mensaje como se muestra en la figura 259.

```
R1_C_SANGOLQUI#config t
R1_C_SANGOLQUI(config)# security password min length 10
```

Figura 259

Mínimo de caracteres en una contraseña equipos CISCO



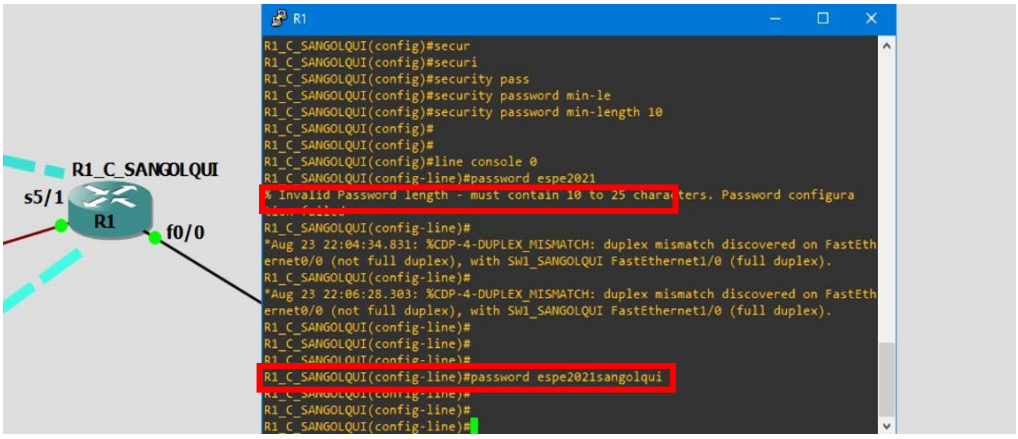
Nota. Se establece el mínimo y máximo para las contraseñas.

De manera que la contraseña para la línea de consola 0 del equipo R1_C_SANGOLQUI será la siguiente “espe2021sangolqui”, y como se muestra en la figura 260, los comandos para establecer la contraseña para este nivel de seguridad son los siguientes.

```
R1_C_SANGOLQUI#config t
R1_C_SANGOLQUI(config)# line console 0
R1_C_SANGOLQUI(config-line)# password espe2021sangolqui
```

Figura 260

Contraseña en línea de consola 0



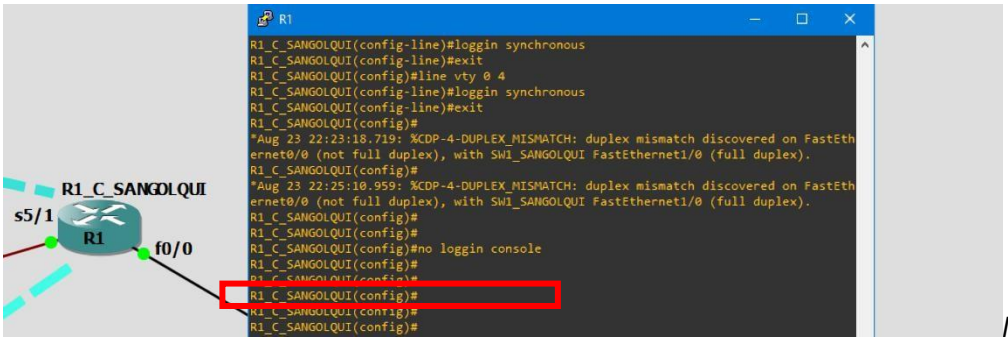
Nota. Las contraseñas deben escribirse sin espacios. Elaboración propia.

Es muy posible que al momento de emitir comandos en la consola del router, varios mensajes se emitan de manera consecutiva lo cual puede ser molesto para evitar esto se debe ejecutar el siguiente comando, así como se muestra en la figura 261 que detendrá los constantes mensajes de interrupción.

```
R1_C_SANGOLQUI(config)# no loggin console
```

Figura 261

Comando para detener mensajes de interrupción en CISO



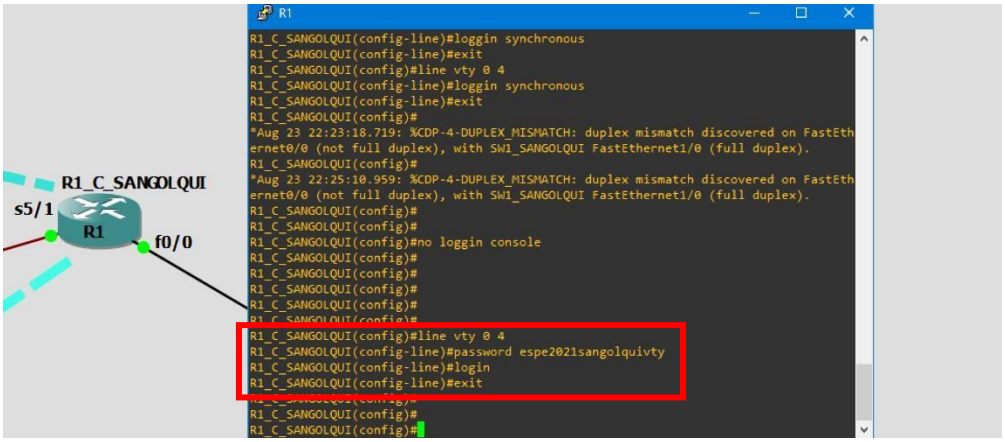
Nota. El comando puede varias según el equipo CISCO.

Ahora se debe establecer la contraseña por acceso remoto, es muy común que se puede acceder a los equipos de manera indirecta a través de estas líneas de consola de, para emitir la contraseña se deben ejecutar los siguientes comandos que se muestran en la figura 262.

```
R1_C_SANGOLQUI(config)#line vty 0 4
R1_C_SANGOLQUI(config-line)#password espe2021sangolquivty
R1_C_SANGOLQUI(config-line)#login
```

Figura 262

Contraseña para líneas de consola de acceso remoto.



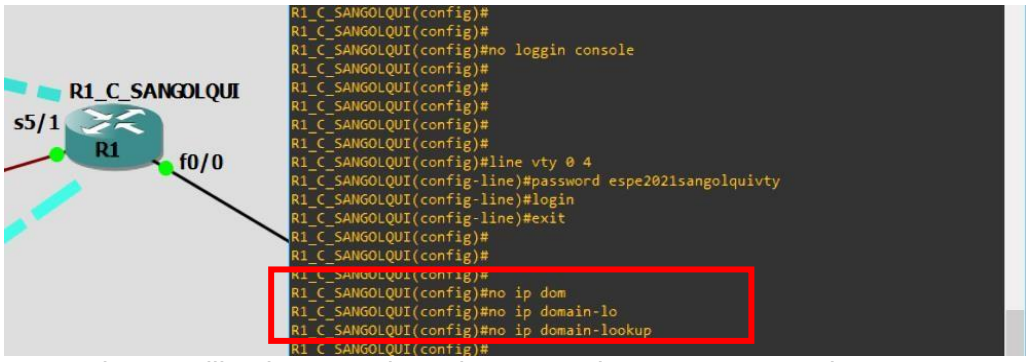
Nota. El rango de líneas depende del equipo CISCO.

Cuando se presiona “tab” al digitar una parte de los comandos la consola los autocompleta, sin embargo, cuando estos comandos no se digitan correctamente el sistema busca resultados lo cual al no ser correcto puede tardar varios minutos en determinar el error, para evitar este problema se debe digitar el siguiente comando, que se muestra en la figura 263.

```
R1_C_SANGOLQUI(config)#no ip domain-lookup
```

Figura 263

Desactivar la traducción de nombres

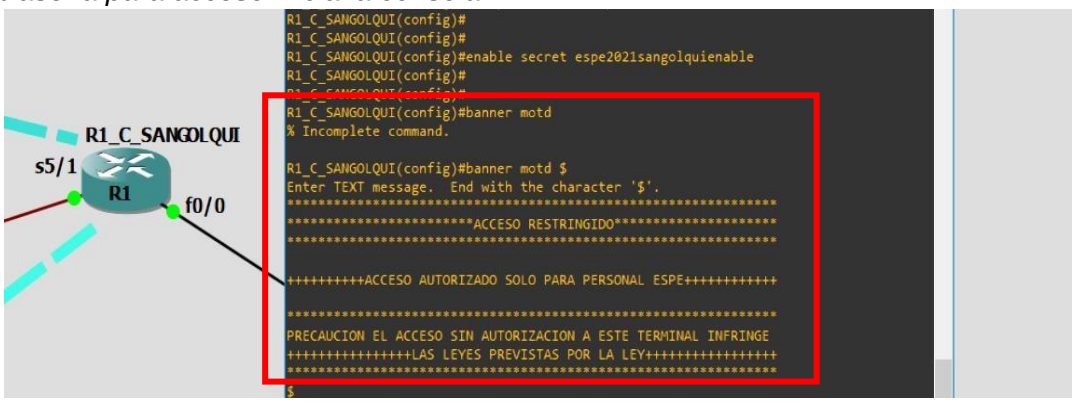


Nota. Puede ser utilizado en equipos de enrutamiento y conmutamiento.

De igual forma para permitir el acceso hacia el modo de configuración global se debe emitir los siguientes comandos para establecer la contraseña, como lo presenta la figura 264 además es importante que también se establezca un mensaje de previsión para el acceso al sistema es lo que se denomina “banner motd”.

Figura 264

Contraseña para acceso inicial a consola

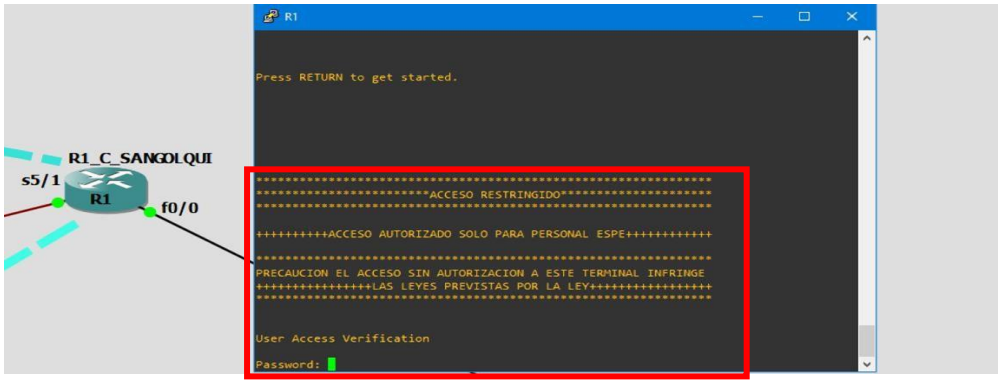


Nota. La consola indica los caracteres para cerrar el mensaje.

Para revisar todas las configuraciones realizadas hasta este momento se debe retroceder en el sistema por medio del comando “exit” hasta llegar al inicio del sistema y primeramente debe mostrase el banner motd que se estableció en el paso anterior como se muestra en la figura 265.

Figura 265

Demostración de Baner motd y contraseñas

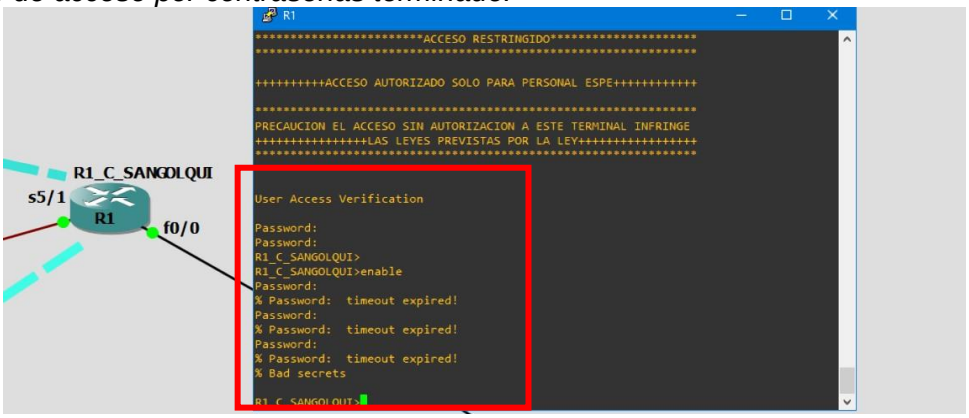


Nota. Primero se pide la contraseña de inicio al sistema.

También se podrá observar como si no se digita a tiempo la contraseña el sistema arrogara un mensaje como el que se muestra en la figura 266 y se deberá establecerla de nuevo y si no se digita en tres oportunidades el sistema arrojara al usuario fuera del sistema.

Figura 266

Tiempo de acceso por contraseñas terminado.

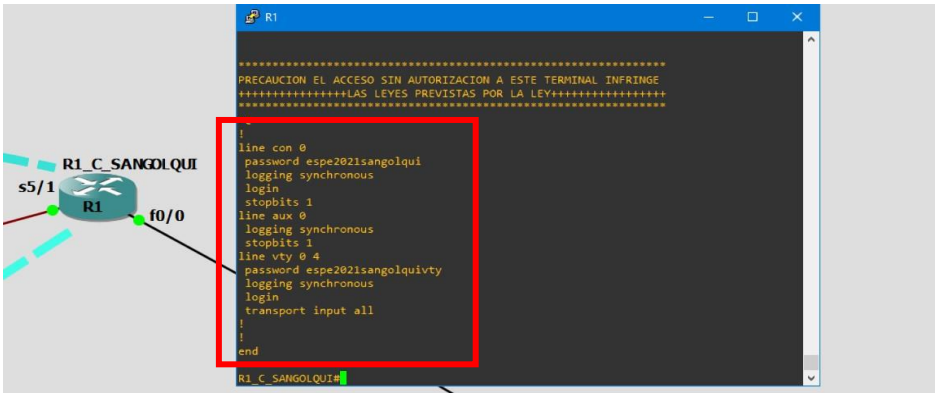


Nota. Si la contraseña es incorrecta se arroja fuera del sistema.

No se podrá observar lo que se escribe en las contraseñas es un nivel de seguridad extra por defecto, pero aun así las contraseñas serán visibles una vez dentro del sistema para comprobar esto se debe digitar el comando “show run” como se muestra en la figura 267.

Figura 267

*Ejecución del comando show run para comprobar configuraciones***.**



Nota. Las contraseñas se encuentran sin encriptación.

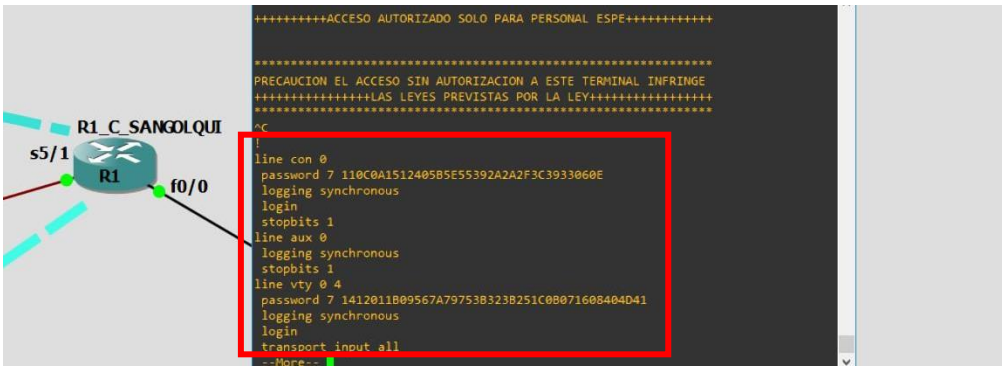
Para encriptar las contraseñas se debe ejecutar los siguientes comandos, lo cual impide a cualquier usuario de la red conocer estas seguridades de manera ilegal, y si se vuelve a

ejecutar el comando show run, se podrá ver como las contraseñas ahora están cifradas como en la figura 268.

```
R1_C_SANGOLQUI(config)#service password-encryption
```

Figura 268

*Contraseñas encriptadas***.**



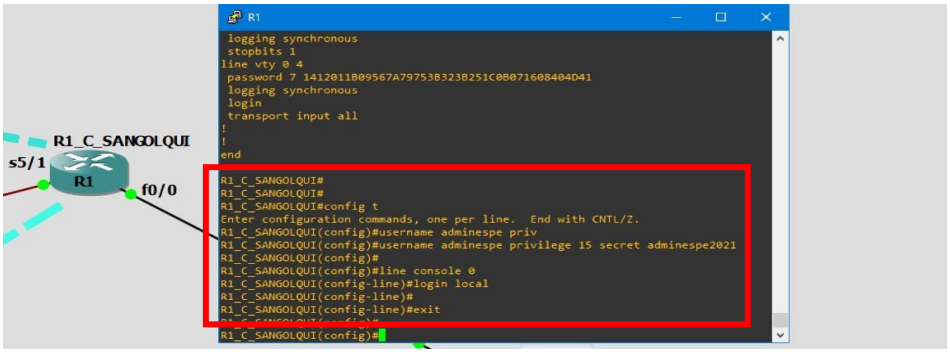
Nota. La encriptación por este comando no es segura. Elaboración propia.

A continuación, se va a establecer el acceso por usuarios con su respectiva contraseña, por medio de los siguientes comandos se establece estos parámetros y el nivel de privilegio que tienen, como se muestra en la figura 269.

```
R1_C_SANGOLQUI(config)#username adminespe privilege 15 secret adminespe2021
```

Figura 269

Comandos para acceso por usuario al sistema.



Nota. Los privilegios determinan la capacidad del usuario para realizar cambios

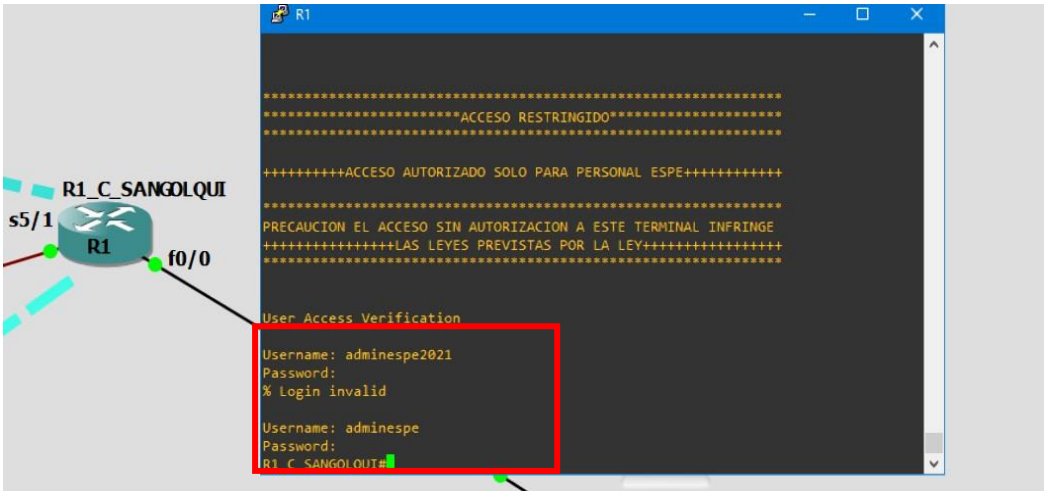
Para que el sistema solicite un usuario y una contraseña al momento de entrar al sistema se ejecutan los siguientes comandos que se muestran en la misma figura 269.

```
R1_C_SANGOLQUI(config)#line console 0
R1_C_SANGOLQUI(config-line)#login local
R1_C_SANGOLQUI(config-line)#exit
```

De manera que, si se retrocede en el sistema para llegar al inicio, se podrá observar como el sistema pide un nombre de usuario y su respectiva contraseña, tal y como lo presenta la figura 270.

Figura 270

Acceso por usuario y contraseña

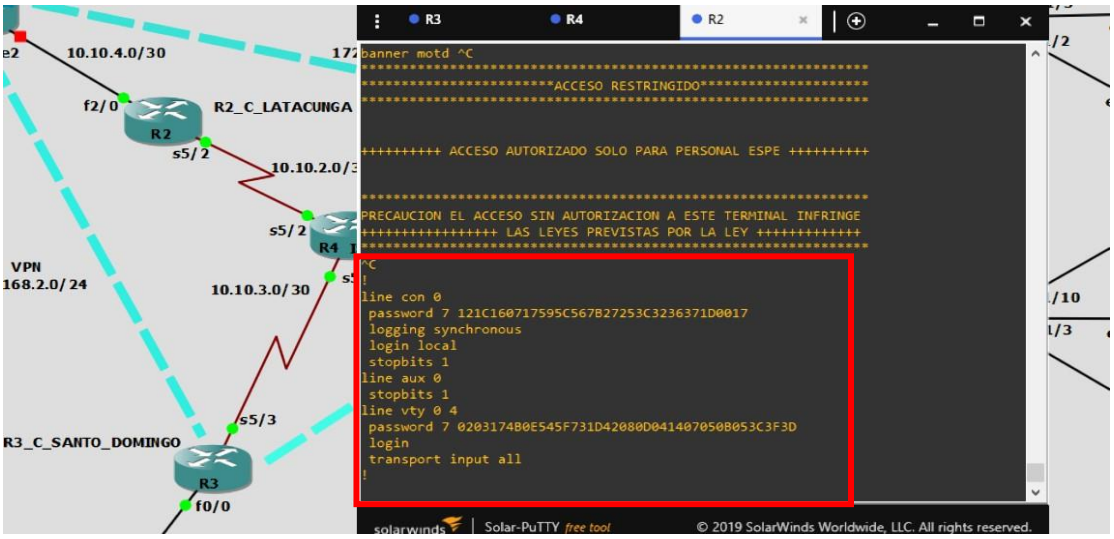


Nota. Se dirige al usuario directo a la configuración privilegiada.

Este proceso se lo realiza en todos los equipos routers de marca CISCO, y como se muestra en las figuras 271,272 y 273 a continuación

Figura 271

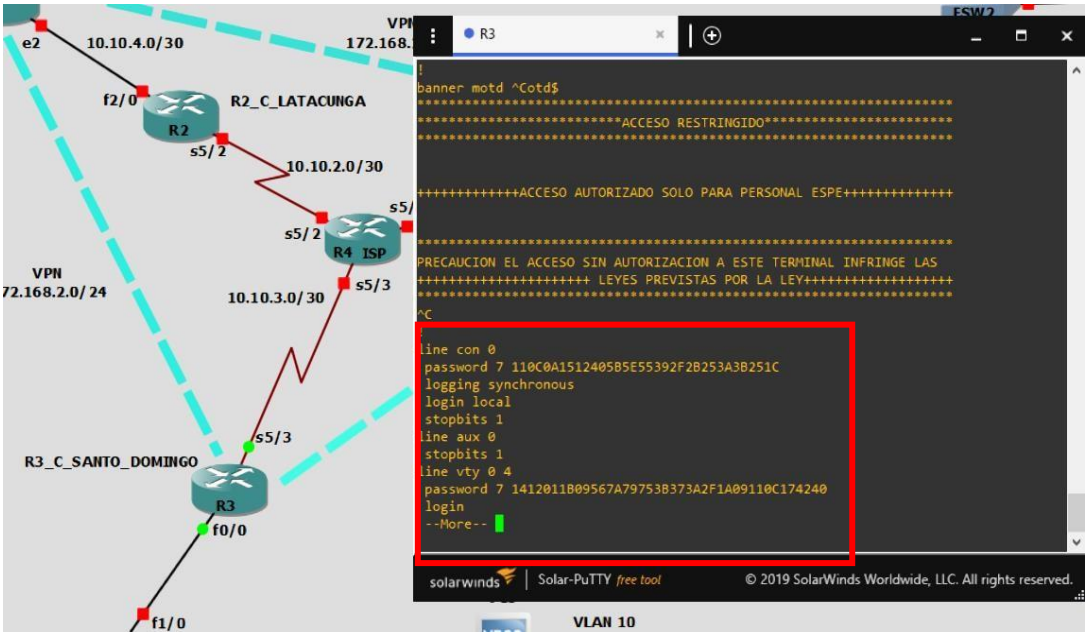
Seguridad en R2_C_LATACUNGA



Nota. Se mantiene los mismos mensajes “banner motd”.

Figura 272

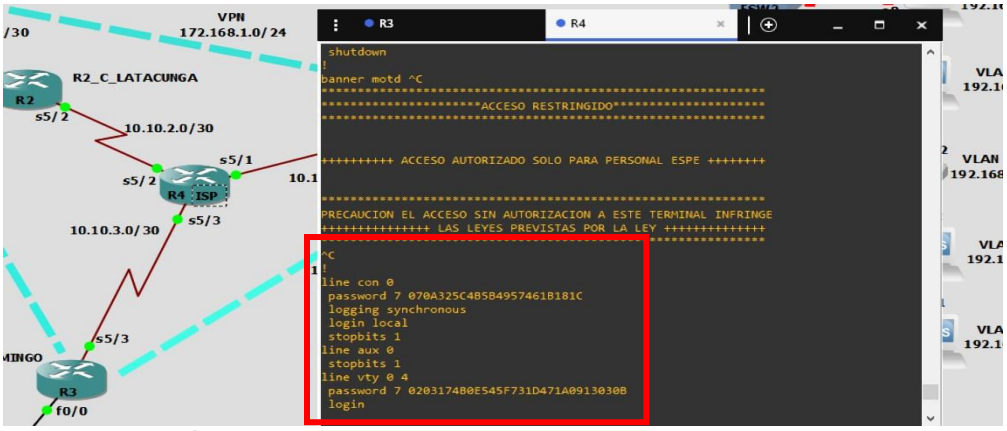
Seguridad en R3_C_SANTO_DOMINGO



Nota. El usuario se mantiene igual en toda la red.

Figura 273

Seguridad en R4_ISP

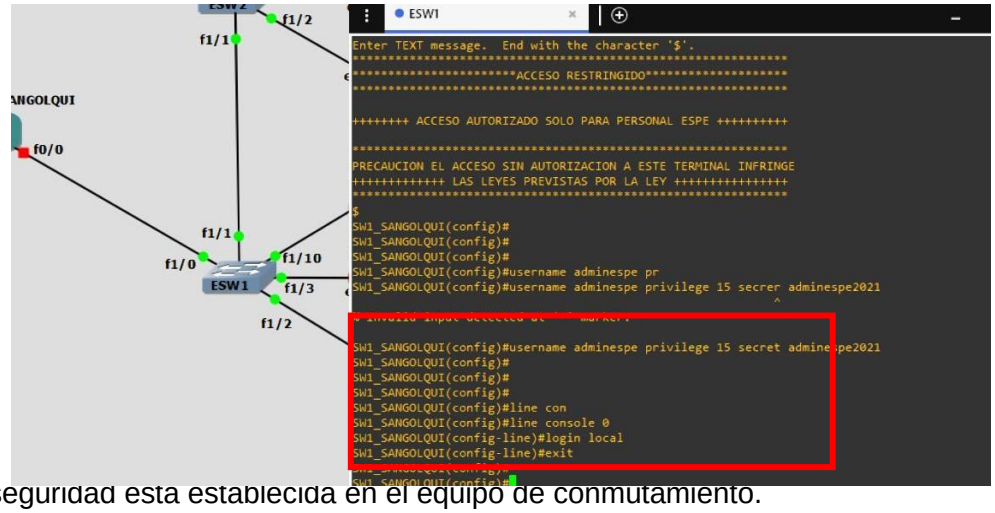


Nota. La seguridad está establecida en la red WAN.

Para los equipos de conmutamiento (Switchs) se otorgará la seguridad a través de un usuario y una contraseña, la cual será la misma que se estableció previamente para los equipos routers, esto con el propósito de evitar una larga lista de seguridad con sus respectivas contraseñas. Y como se demuestra en las figuras que corresponden a los switches de la red de Sangolqui y Santo domingo, además de que se les asignó un banner motd

Figura 274

Seguridad en SW1_SANGOLQUI



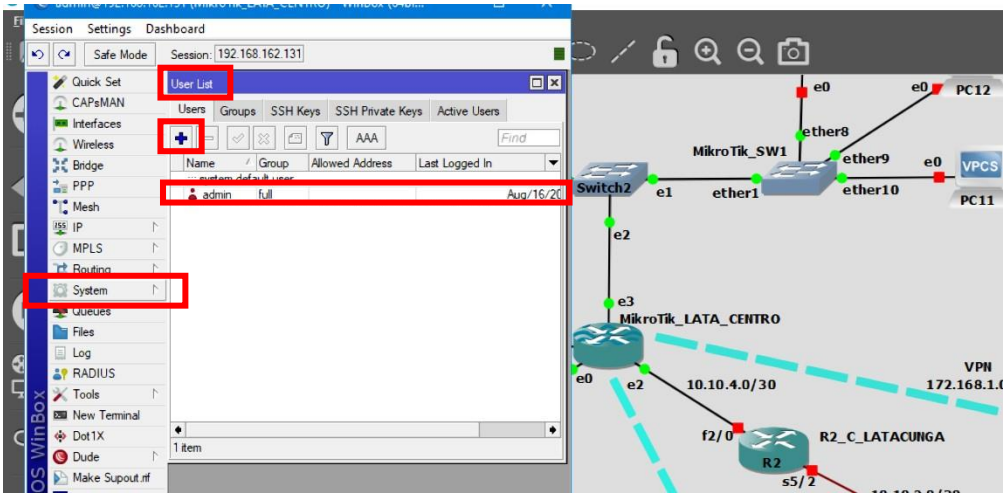
Nota. La seguridad esta establecida en el equipo de conmutamiento.

Seguridad en equipos MikroTik

Para los equipos MikroTik es importante tener en cuenta que conforme al avance de esta red de datos, la manera de ingresar a estos dispositivos era muy insegura, por lo cual se va a asignar un usuario nuevo y una contraseña para los equipos, para esto se debe ingresar al programa Winbox y abrir la interfaz gráfica del equipo en cuestión, como se muestra en la figura 275 dentro de la opción system para el menú emergente existirá una etiqueta con el nombre “USERS” el cual al presionarlo mostrará la siguiente figura.

Figura 275

Interfaz de usuarios en MikroTik_LATA_CENTRO

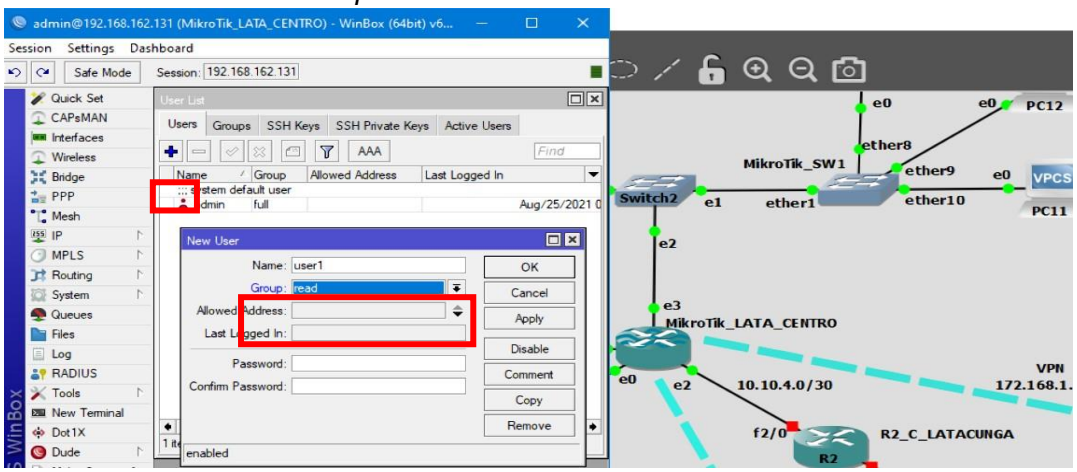


Nota. Otras pestañas permiten crear grupos de usuario, claves, y revisar los usuarios activos.

Cuando se logra entrar a un equipo MikroTik, por defecto el usuario es admin, puesto que es la configuración por defecto de estos equipos, lo cual incluye a todos los equipos de esta marca, de manera que puede ser vulnerable a ataques, para cambiar esta configuración se creará otro usuario dando clic en la opción añadir, donde un nuevo cuadro de dialogo permitirá ingresar el nombre del usuario tal y como lo muestra la figura 276.

Figura 276

Creación de usuario "adminespe"

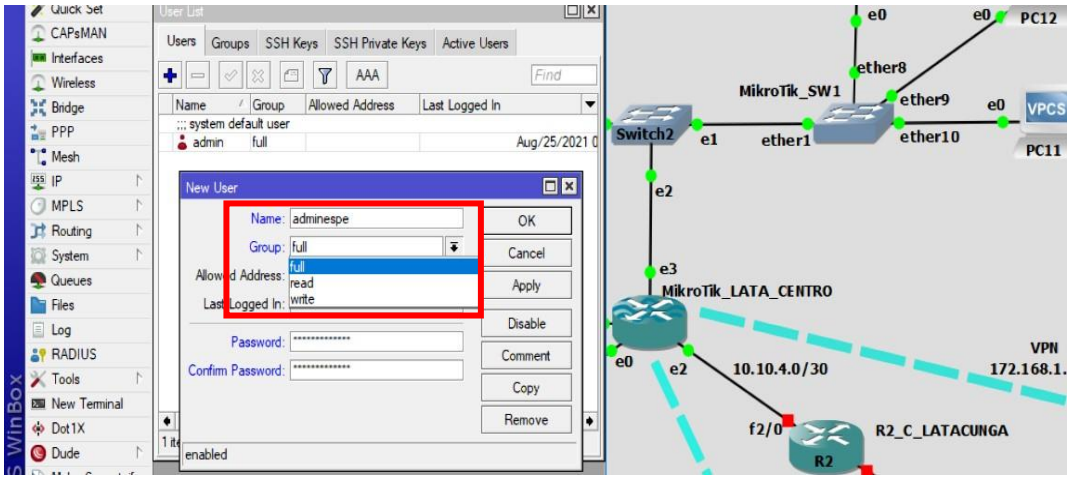


Nota. "Group" es lo mismo que la configuración "privilege" en los equipos CISCO.

Se debe cambiar el nombre que se establece por defecto (user1) y de igual forma en el campo "group" otorgar los correspondientes privilegios a este usuario por medio de un list view. Por debajo de estas configuraciones está el apartado "password" en el cual se establece la contraseña de acceso a este equipo, y como se demuestra en la figura 277 se debe confirmar en el apartado "confirm password".

Figura 277

Usuario y contraseña creado en MIkroTik_LATA_CENTRO

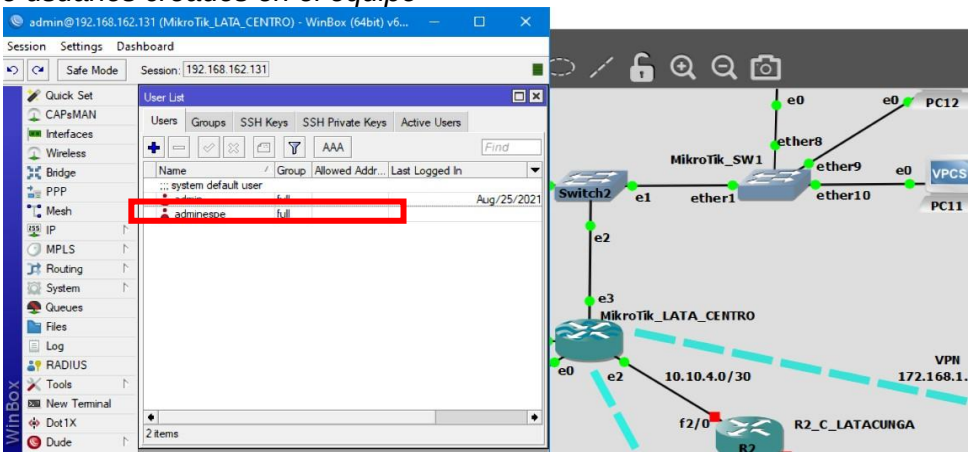


Nota. Las contraseñas de esta marca de equipos ya se encuentran encriptadas.

Finalmente, para guardar este usuario se da clic en APPLY y OK de forma que en la ventana anterior por debajo del usuario por defecto “admin” se encontrara el nuevo usuario creado como lo muestra la figura 278.

Figura 278

Lista de usuarios creados en el equipo

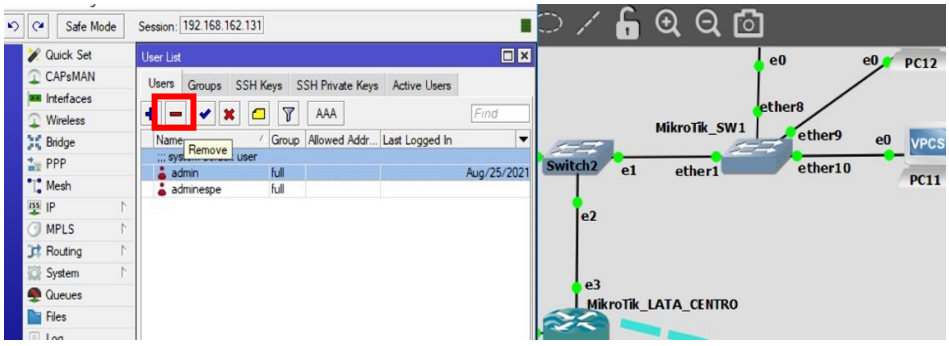


Nota. También se mostrará cuando fue el último inicio de sesión el usuario en la columna “last logged in”.

Para eliminar un usuario se debe seleccionarlo del listado general, donde se marcará de azul, y en la barra de opciones se habilitará la etiqueta “remove” para eliminar el usuario seleccionado, como en la figura 279 donde para asegurar la confidencialidad del equipo, se decide eliminar el usuario por defecto.

Figura 279

Eliminación del usuario por defecto.

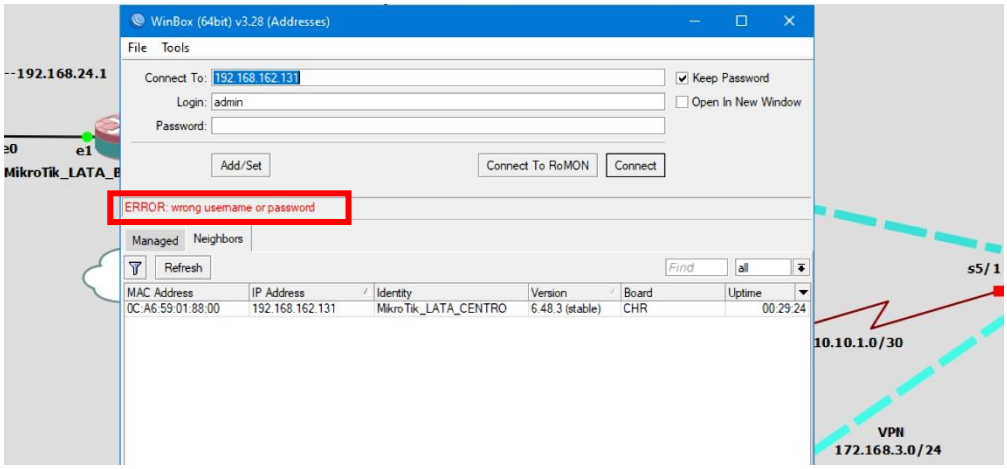


Nota. Algunas opciones necesitan seleccionar el usuario.

Para comprobar que la configuración de seguridad se haya guardado efectivamente, se cierra el programa Winbox, y al abrirlo de nuevo se observara la figura 280 que es la interfaz de administración general para el acceso a los dispositivos, que cuenta con el usuario y contraseña por defecto, si se presiona el botón Connect, un mensaje de error se mostrará

Figura 280

Ingreso a MIkroTIK_LATA_CENTRO con usuario adminespe.

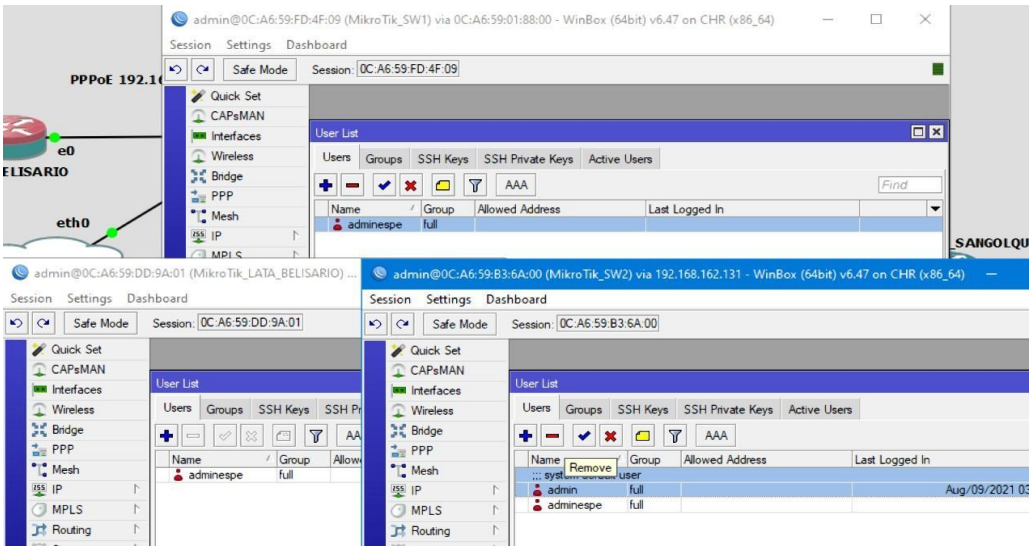


Nota. Se debe cambiar el usuario y la contraseña por defecto.

El mensaje advierte al usuario de que el usuario y la contraseña son incorrectos, lo cual verifica que la configuración realizada es correcta, simplemente se cambia los campos correspondientes asegurando que el equipo seleccionado sea el correcto y permitirá la conexión normal hacia el equipo. Esto se realizará con todos los equipos de marca MikroTik que se encuentren en la red, como se muestran en las siguientes figuras con respecto a los switches de la red LAN de Latacunga centro y el router de LATA_BELISARIO, como se muestra en la figura 281.

Figura 281

Usuario “adminespe” en todos los equipos MikroTIK.



Nota. Procurar eliminar el usuario por defecto de los equipos.

Implementación del laboratorio virtual en el laboratorio de comunicaciones ESPEL

Primero se comprobó el estado en que las computadoras del laboratorio de comunicaciones se encontraban, y los recursos con que contaban para determinar la compatibilidad con el programa de simulación. Tras revisar los recursos de hardware y software con los que contaban las computadoras se detallan en la siguiente tabla.

Tabla 3

Recursos en las maquinas del laboratorio de comunicaciones ESPEL.

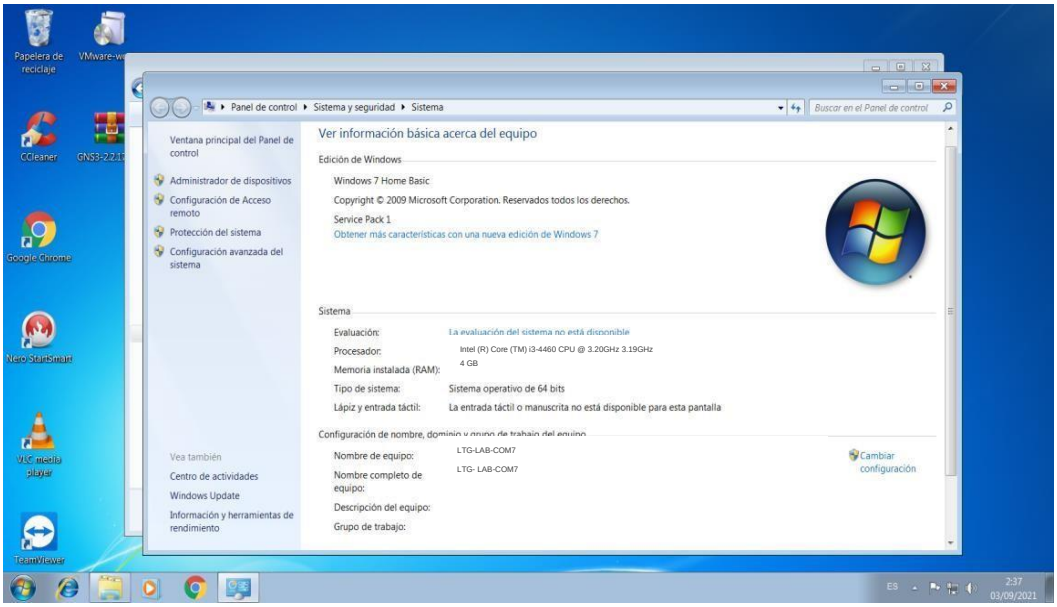
Recurso	Detalle
Sistema Operativo	Windows 7
Procesador	Intel Core I3
Memoria RAM	4 GB
Almacenamiento (Disco Duro)	235 Gb
Virtualización	Desactivada

Nota. La tabla muestra los recursos para la instalación de los programas de GNS3

Los recursos de los equipos cumplen con los requerimientos mínimos para la implementación del laboratorio virtual, sin embargo, se encontró el problema de compatibilidad para el programa VMware, ya que al contar con un sistema Windows 7 debe requerir de una versión menor a la actual y la que se detalló previamente, y de igual forma es muy posible que para la conexión con GNS3 exista errores de compatibilidad de la máquina virtual, por lo que también se decide instalar una versión menor a la detallada en este mismo documento.

Figura 282

Recursos de Maquinas físicas del laboratorio de comunicaciones ESPEL

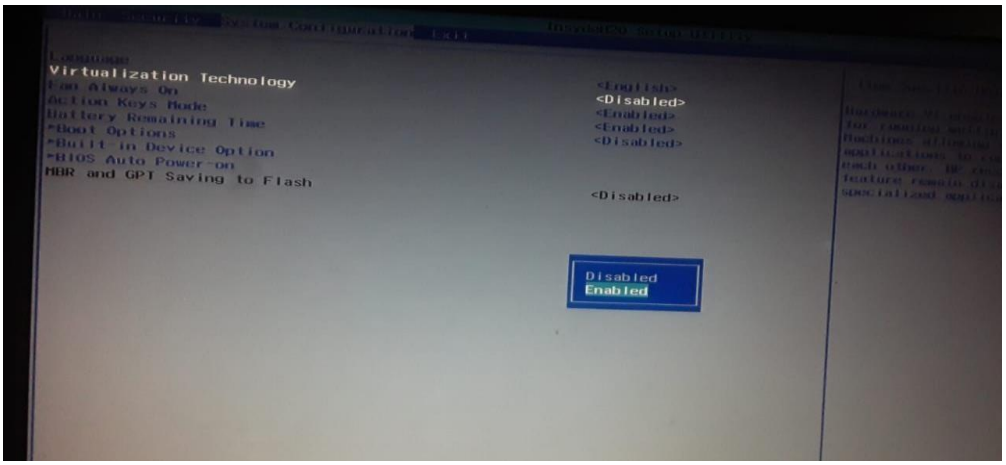


Nota. El equipo puede adquirir mejores capacidades. Elaboración propia.

Primero se debe activar la virtualización de los equipos, para lo cual se debe entrar en el sistema BIOS de la computadora y activar la opción “enable virtualization”, como se muestra en la figura 283.

Figura 283

*Activación del proceso de virtualización en los equipos***.**

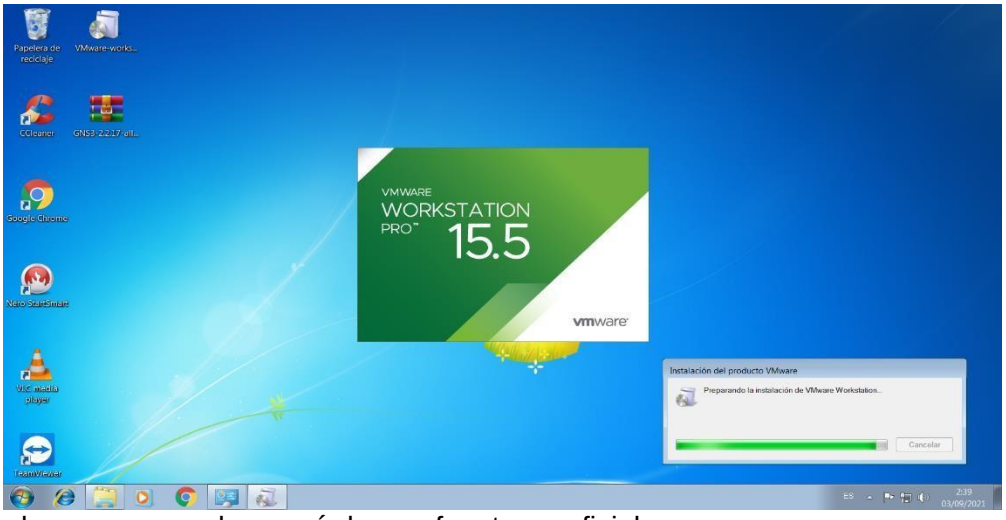


Nota. el BIOS se encuentra desactualizada.

Una vez dentro del sistema operativo, se instalará los programas necesarios, primeramente, el software VMware, para las computadoras será necesario descargar la versión “Workstation 15.5 pro”. Como se muestra en la figura 284.

Figura 284

*Instalación del programa VMware Workstation 15.5 pro***.**



Nota. el programa se descargó de una fuente no oficial.

Ahora se debe instalar el programa GNS3, debido a los recursos de la computadora se instalará la versión 2.2.17 la cual se puede encontrar de fuentes no oficiales de internet.

Figura 285

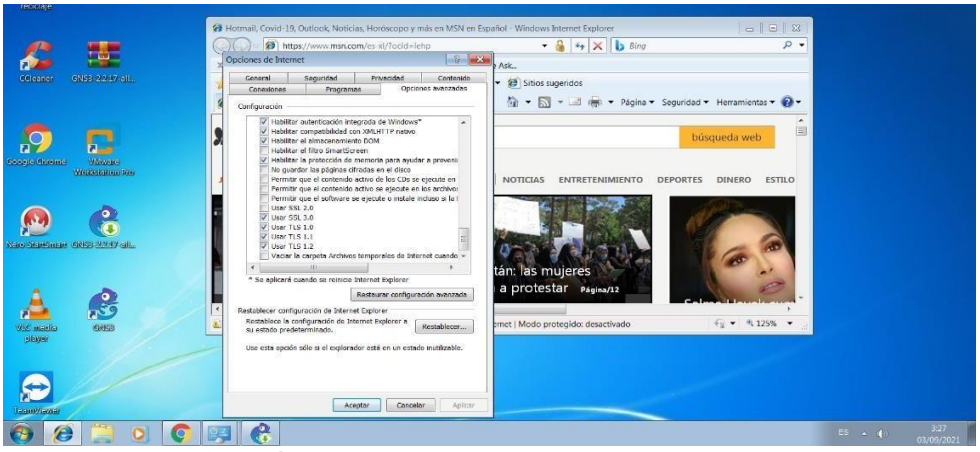
*Instalación del programa GNS3 versión 2.2.17***.**

Nota. La versión puede ser encontrada en GITHUB.

Durante la instalación de GNS3 se descubrió una pequeña falta de actualización de forma que algunas opciones de internet, impedían la instalación del programa, para lo cual se activó estas configuraciones.

Figura 286

*Activación de la característica TSL 1.2***.**



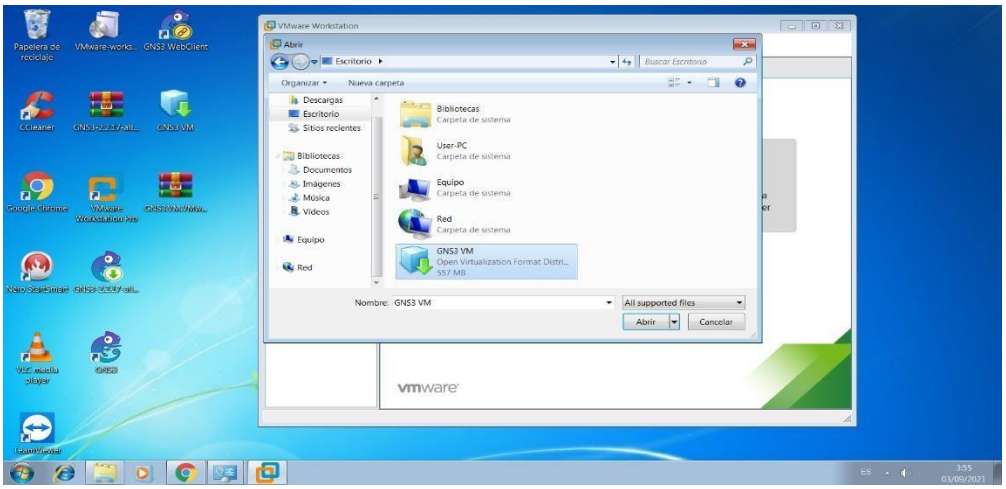
Nota. Se encuentran con más problemas de conectividad.

Finalizado la instalación de GNS3 se procede a conectar la máquina virtual con la interfaz de trabajo. Primero abriendo la máquina virtual en el programa Workstation, como se

muestra en la figura 287 y habilitar la opción “Enable GNS3 VM” en la interfaz “preferences deGNS3” como se muestra en la figura 288.

Figura 287

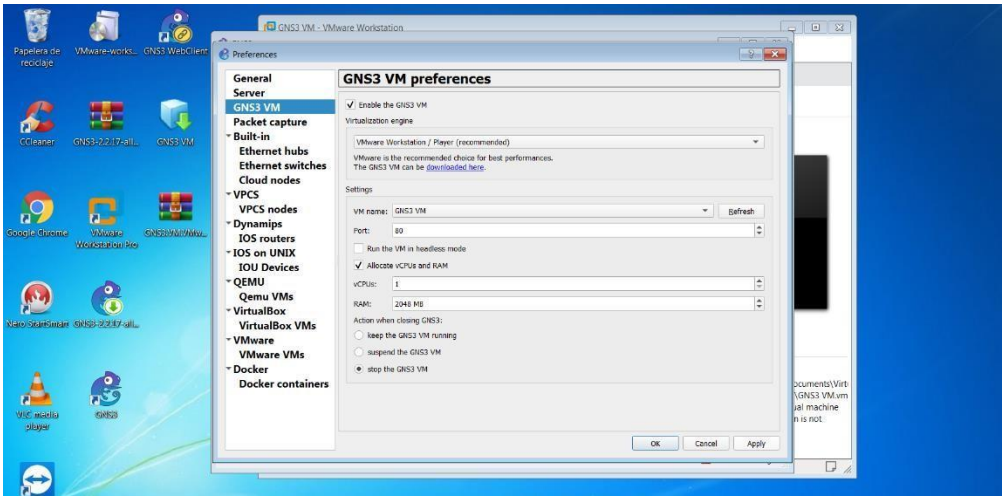
Funcionamiento de la máquina virtual propia de GNS3



Nota. La máquina virtual se puede obtener en la misma descarga del programa.

Figura 288

Conexión entre GNS3 interfaz y la máquina virtual

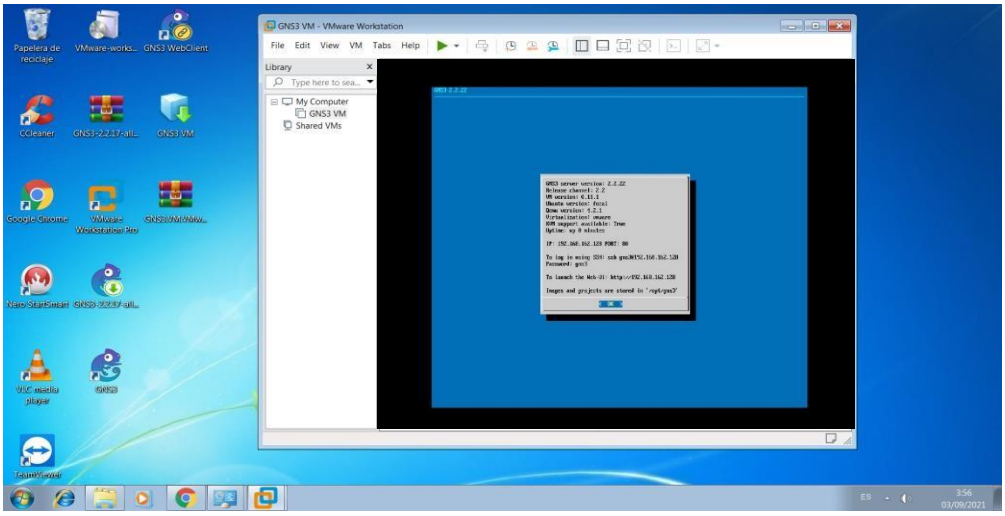


Nota. Verificar que los programas no arrojen errores.

Finalmente se verifica la conexión entre el servidor y el programa y como se muestra en la figura 289 es exitosa. Ya que ambos servidores están operativos.

Figura 289

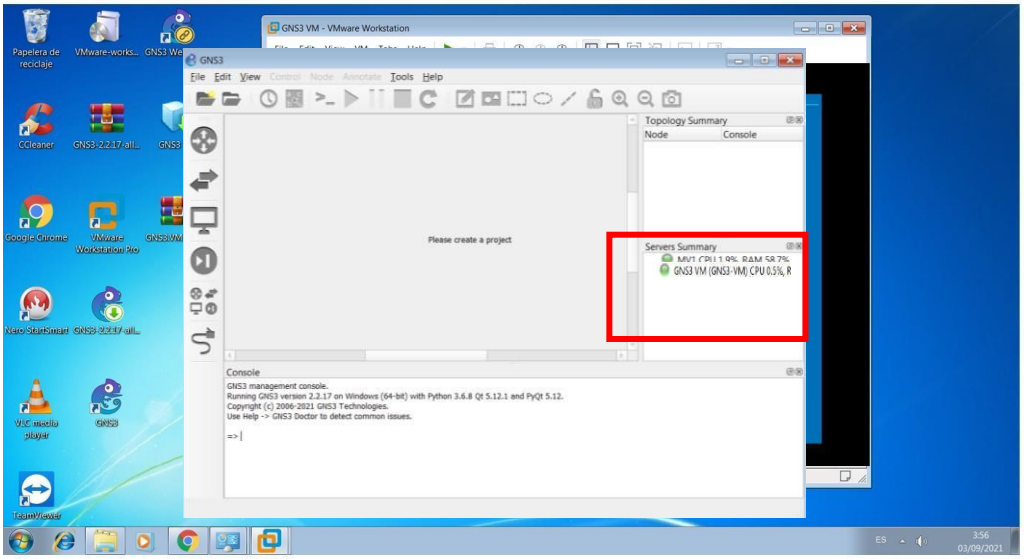
GNS3 VM completamente funcional



Nota. Máquina virtual versión 2.2.17

Figura 290

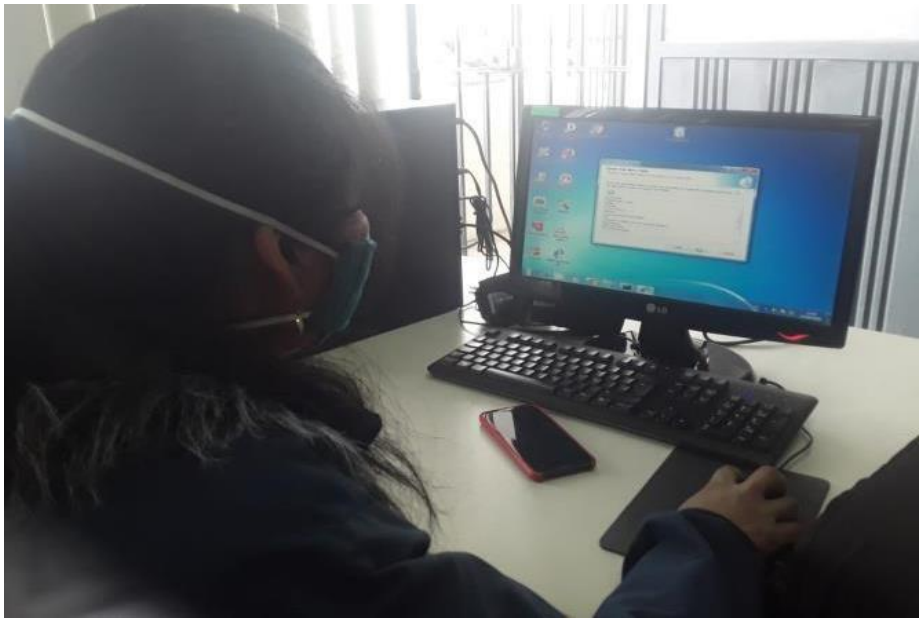
Arquitectura de GNS3 completa



Nota. La cantidad de memoria RAM para los procesos se vio limitada.

Figura 291

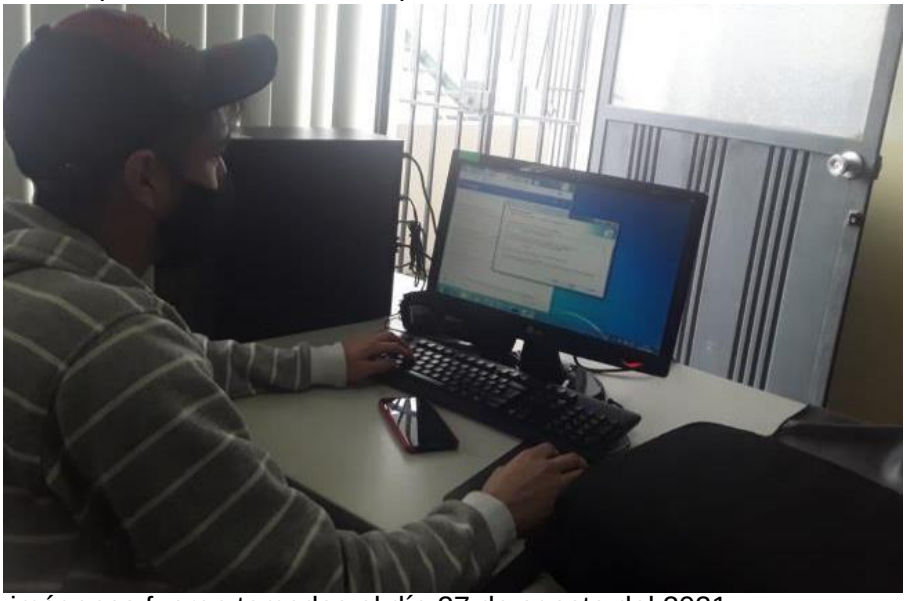
Estudiante instalando el programa GNS3



Nota. Las imágenes fueron tomadas por los mismos estudiantes creadores de esta monografía.

Figura 292

Descarga de máquina virtual GNS3 compatible con el sistema.



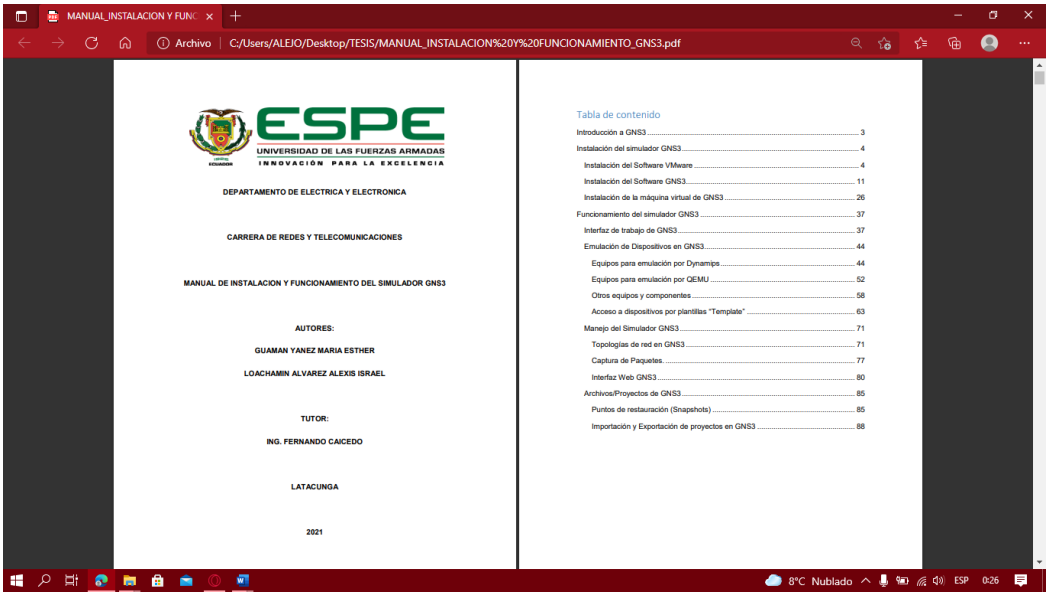
Nota. Las imágenes fueron tomadas el día 27 de agosto del 2021.

Manual de funcionamiento de GNS3 y guía de laboratorio para la implementación de red corporativa en GNS3

En base a lo planteado en esta monografía se ha recopilado un manual de instalación y funcionamiento del programa GNS3 con sus correspondientes componentes. Tomando en cuenta que en el manual se añaden más detalles sobre el funcionamiento del programa.

Figura 293

Manual de instalación y funcionamiento del simulador GNS3

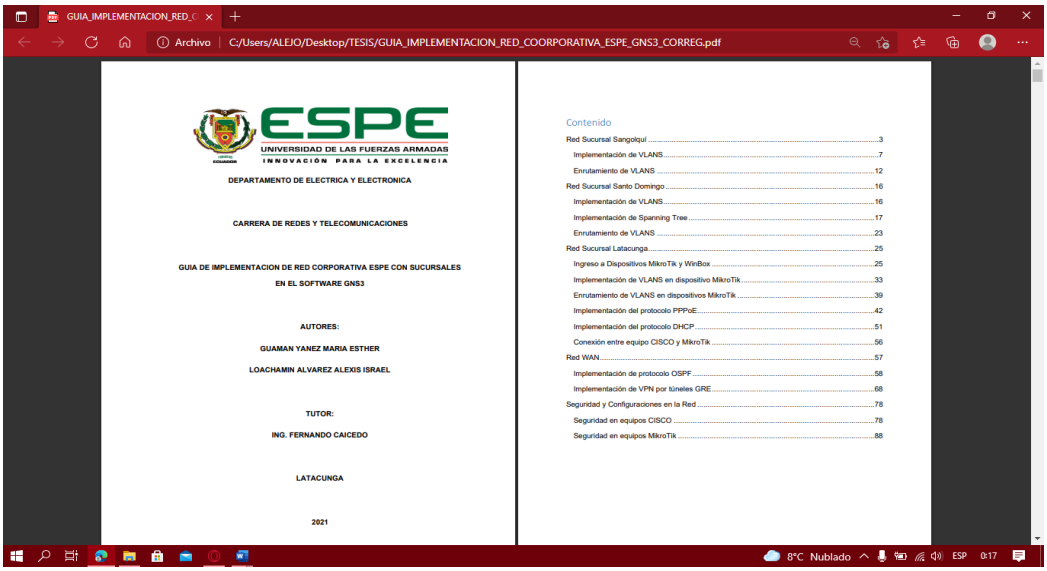


Nota. El manual cubre gran parte de lo detallado en esta monografía.

De igual forma según lo establecido en esta monografía y proyecto técnico, se ha generado una guía de implementación para la simulación de una red de datos corporativa, tomando como referencia la arquitectura de la Universidad de las Fuerzas Armadas y sus correspondientes sucursales.

Figura 294

Guía de implementación de red corporativa ESPE en el software gns3



Nota. La guía cubre gran parte de lo detallado en esta monografía.

Conclusiones

- Se puede concluir en base a la investigación realizada en esta monografía, que GNS3 es un programa de simulación y emulación para el estudio de telecomunicaciones y muy útil para la elaboración de redes de datos a gran escala, permitiendo desde la simulación de equipos multimarca con varios requerimientos hasta el uso de múltiples protocolos de red. Su arquitectura de emulación anidada permite al usuario cumplir con parámetros que una red de datos reales necesite.
- Por cuanto se puede concluir, la instalación de GNS3 y la incorporación de dispositivos multimarca como CISCO, MikroTik, Juniper, entre otros. Permiten que se obtenga una amplia variedad de equipos a manipular, obteniendo un panorama de los diferentes equipos que se usan en la implementación de redes de datos, poniendo en práctica lo aprendido en el área de redes en el laboratorio de comunicaciones de la ESPEL.
- De igual forma se puede concluir que la elaboración de la red corporativa dentro del simulador GNS3, tomando como referencia la estructura de la Universidad de las Fuerzas Armadas con sus diferentes campus a nivel nacional, permite determinar los alcances del mismo programa, haciendo uso de diversos protocolos de conmutamiento y servicios de enrutamiento utilizados en redes reales se puede reconocer el funcionamiento del software.
- La elaboración del manual de funcionamiento para el programa GNS3 y la guía de implementación para la red corporativa de la ESPE dentro del mismo programa, permiten que se expliquen detalles muy importantes y que las personas puedan comprender la manera en que funciona y la utilidad del software, así como la el funcionamiento de redes de datos.

Recomendaciones.

- Se recomienda que las redes incorporadas en GNS3 obtengan una medida del gasto a suponer para los servidores establecidos, es decir, tener en cuenta la cantidad de equipos a disponer en la topología y la cantidad de memoria y procesamiento que demandarán estos equipos al ser ejecutados, puesto que puede existir fallas de procesamiento al no existir más recursos disponibles.
- Tras haber realizado la instalación de los programas y la elaboración de los manuales y guías en este proyecto técnico, Hacer uso de los mismos pues suponen una gran mejoría en el proceso académico de los estudiantes de la carrera de Redes y Telecomunicaciones.
- Se recomienda realizar una optimización de los equipos informáticos en los laboratorios de comunicaciones de la Universidad, ya que además de la poca limpieza que se pudo encontrar en las instalaciones, los equipos contaban con sistemas operativos que para la actualidad son prácticamente obsoletos. Esto permitiría una mayor capacidad hacia el programa GNS3 y su correspondiente ayuda hacia los estudiantes.

Bibliográfia

Burbano, A. R. (27 de Agosto de 2019). *DPL News.* Recuperado el 5 de Julio de 2021, de DPL News: https://digitalpolicylaw.com/ecuador-reprueba-en-el-indice-de-calidad-de-vida-digital/

Carmona, J. G. (2017). *Propuesta de manual de prácticas de laboratorio de redes.* Santa Clara. Recuperado el 04 de Julio de 2021

Charlene. (9 de Enero de 2020). *Fs. Community*. Recuperado el 04 de Julio de 2021, de Fs. Community: https://community.fs.com/es/blog/pppoe-vs-dhcp-what-is-the-difference.html

Collado, E. (22 de Enero de 2018). *WordPress: Chronus de ThemeZee.* Recuperado el 04 de Julio de 2021, de WordPress: Chronus de ThemeZee.: https://www.eduardocollado.com/2018/01/22/podcast-98-spanning-tree/

Equipo de Expertos Universidad Internacional de Valencia. (9 de Octubre de 2018). *VIU Universidad Internacional de Valencia.* Recuperado el 4 de Julio de 2021, de VIU Universidad Internacional de Valencia: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas

Galeano, S. (28 de Enero de 2021). *Marketing4Ecommerce.* Recuperado el 09 de Agosto de 2021, de Marketing4Ecommerce: https://marketing4ecommerce.net/usuarios-de-internet-mundo/

Goujon, A. (10 de Septiembre de 2012). *WeliveSecurity ©ESET.* Recuperado el 6 de Junio de 2020, de WeliveSecurity ©ESET: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

IBM Corporation. (2014). *Redes Protocolo de configuración dinámica de hosts (DHCP).* España: IBM. Recuperado el 4 de Julio de 2021, de Redes Protocolo de configuración dinámica de hosts (DHCP).

Jithin. (4 de Agosto de 2016). *InterServer.Net*. Recuperado el 09 de Agosto de 2021, de InterServer.Net: https://www.interserver.net/tips/kb/common-network-protocols-ports/

Laura. (11 de Abril de 2019). *By Orange.* Recuperado el 09 de Agosto de 2021, de By Orange. A blog site: https://blog.orange.es/red/la-virtualizacion-red-se-habla-ello/

Limones, E. (7 de Abril de 2021). *Topología de redes informáticas*. Recuperado el 21 de Agosto de 2021, de Topología de redes informáticas: https://openwebinars.net/blog/topologia-de-redes-informaticas/

Luz, S. d. (12 de Agosto de 2021). *Redes Zone.* Recuperado el 15 de Agosto de 2021, de Redes Zone.: https://www.redeszone.net/autor/sergio/

Moisa, J. E. (2 de Febrero de 2019). *Comunidad CISCO.* Recuperado el 13 de Agosto de 2021, de Comunidad CISCO: https://community.cisco.com/t5/documentos-routing-y-switching/túnel-gre/ta-p/3181793

Poveda, J. M. (6 de Noviembre de 2020). *Internexa una empresa ISA.* Recuperado el 13 de Agosto de 2021, de Internexa una empresa ISA: https://www.internexa.com/blogs/conectividad/como-funciona-el-internet/

Rivera Zapata, C., Iglesias RodrigueZ, E., & García Zaballos, A. (2020). *Estado Actual de las telecomunicaciones y la banda ancha en Ecuador.* SN: Banco Interamericano de Desarrollo. Recuperado el 23 de Agosto de 2021

Saurabhsharma56. (14 de Mayo de 2020). *geeksforgeeks.* Recuperado el 23 de Agosto de 2021, de geeksforgeeks: https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/

Stallings, W. (2011). *Computaciones y Redes de Computadores.* Madrid: Pearson Prentice Hall. Recuperado el 21 de Agosto de 2021

SUPERIOR, C. D. (2020). *Reglamento de Régimen Academico.* Quito: CONSEJO DE EDUCACIÓN SUPERIOR. Recuperado el 29 de Julio de 2021

VARGAS VALLEJO, D. (2020). *ANÁLISIS COMPARATIVO DE TECNOLOGÍAS PARA EL DISEÑO DE RED WLAN PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERÍA DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR EMPLEANDO ESTÁNDAR 802.11N.* Quito: Trabajo propio. Recuperado el 30 de Agosto de 2021

Vélez Vera, D. (2018). *Diseño y simulación en GNS3 de una red multiservicios MPLS para medianas empresas en el Ecuador.* Guayaquil: Trabajo Propio. Recuperado el 23 de Agosto de 2021

Verdezoto Rodríguez, R., & Chávez Vaca, V. (2018). IMPORTANCE OF THE TOOLS AND LEARNING ENVIRONMENTS WITHIN THE E-LEARNING PLATFORM AT THE UNIVERSITIES OF ECUADOR. *EDUTEC. Revista Electronica de Tecnolgia Educativa.*, 9. Recuperado el 24 de Agosto de 2021

YMANT. (17 de Marzo de 2021). *YMANT Servicios Informaticos.* Recuperado el 23 de Agosto de 2021, de YMANT Servicios Informaticos: https://www.ymant.com/blog/equipos-de-red/