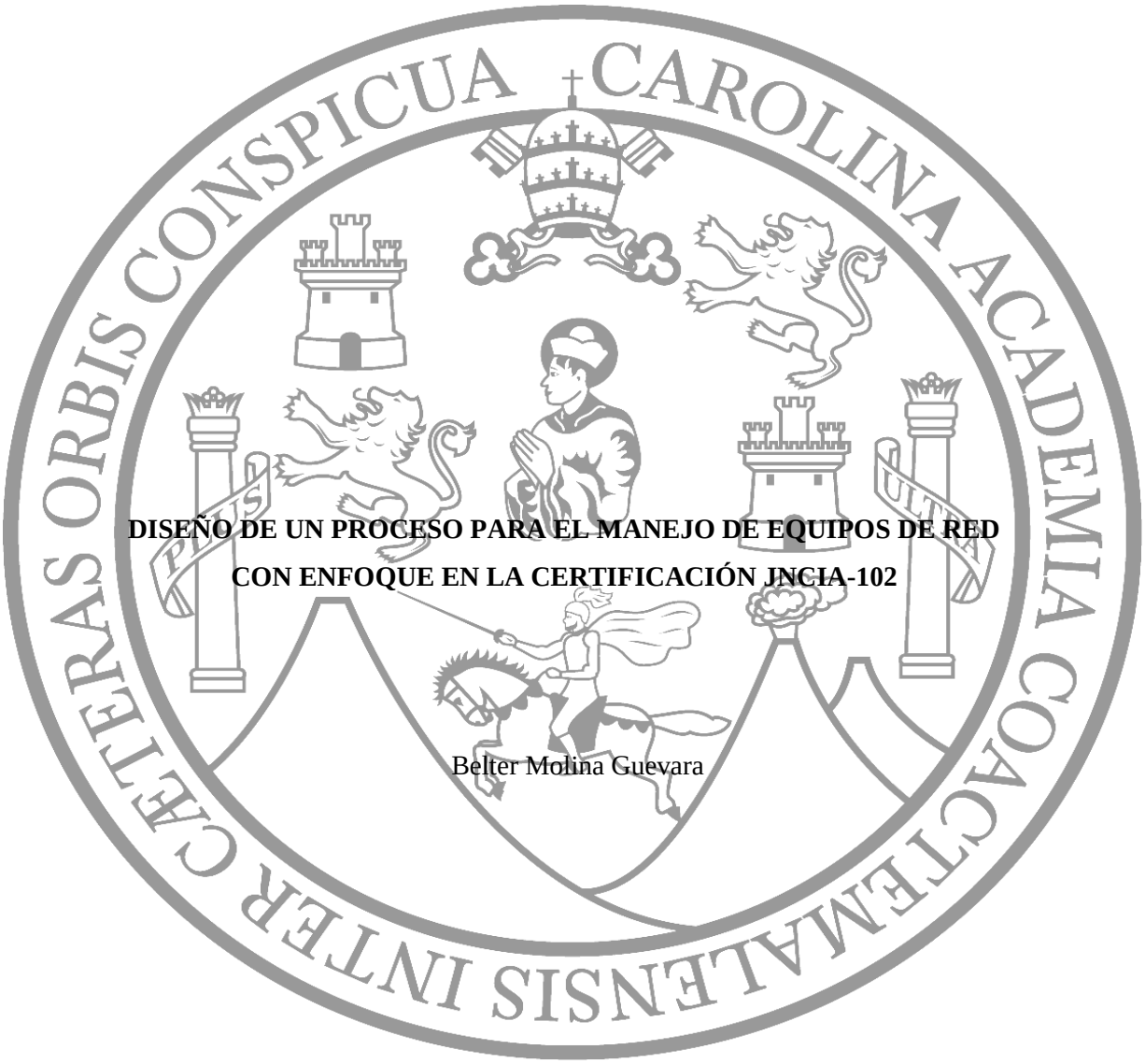
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS QUÍMICAS Y FARMACIA



DISEÑO DE UN PROCESO PARA EL MANEJO DE EQUIPOS DE RED CON ENFOQUE EN LA CERTIFICACIÓN JNCIA-102

Belter Molina Guevara

Maestría en Administración Industrial y de Empresas de Servicio

Guatemala, Mayo de 2015.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS QUÌMICAS Y FARMACIA

DISEÑO DE UN PROCESO PARA EL MANEJO DE EQUIPO DE RED CON ENFOQUE EN LA CERTIFICACIÓN JNCIA-102

Trabajo de Graduación presentado por

Belter Molina Guevara

Para optar al grado de Maestro en Artes

Maestría en Administración Industrial y de Empresas de Servicio

Guatemala, Mayo de 2015.

JUNTA DIRECTIVA

FACULTAD DE CIENCIAS QUIMICAS Y FARMACIA

Dr. Rubén Dariel Velásquez Miranda	DECANO
M.A. Julieta Salazar de Ariza	SECRETARIO
M.A. Carolina Guzmán Quilo	VOCAL I
Dr. Sergio Alejandro Melgar Valladares	VOCAL II
BR. Michael Javier Mo Leal	VOCAL IV
BR. Blanqui Eunice Flores De León	VOCAL V

CONSEJO ACADÉMICO

ESCUELA DE ESTUDIOS DE POSTGRADO

Rubén Dariel Velásquez Miranda, Ph.D.

Carolina Arévalo Valdez, Ph.D.

Roberto Flores Arzú, Ph.D.

Jorge Erwin López Gutiérrez, Ph.D

Félix Ricardo Veliz Fuentes, MSc.

ACTO QUE DEDICO A:

Mis padres, porque sabiendo que no existiría una forma de agradecer toda una vida de sacrificios y esfuerzos, quiero que sientan que el objetivo logrado también es suyo y que la fuerza que me ayudo a conseguirlo fue su apoyo. Por esta razón esta dedicatoria es para ustedes mis padres amados, especialmente a mi madre.

AGRADECIMIENTOS A:

Dios, por estar conmigo en todo momento, darme sabiduría, dirección, fuerza, protección y brindarme los padres tan maravillosos que tengo.

Mis padres, Herlindo Molina Siguina y muy especialmente a mi madre Antonia Guevara Parada, por sus múltiples sacrificios, apoyo, confianza y amor incondicional que me brindaron.

Mis hermanos, Esvin, Aracely y Robert Molina, con cariño y aprecio por su apoyo.

Mis amigos, a todos los que de una u otra forma contribuyeron con conocimientos, motivación y consejos para alcanzar este triunfo.

Universidad de San Carlos de Guatemala, en especial a la Facultad de Ingeniería, por darme la oportunidad de expandir mis conocimientos científicos, técnicos y éticos en tan prestigiosa casa de estudios y a la Facultad de Ciencias Químicas y Farmacia por abrirme sus puertas a tan enriquecedores conocimientos.

RESUMEN EJECUTIVO

Actualmente el mercado de las telecomunicaciones exige personal con alta capacidad en el manejo de diferentes equipos como lo son los de la marca Juniper, Cisco, Huawei, Alcatel etc.

En Guatemala las empresas más grandes de telefónica celular como Tigo, Claro y Telefónica utilizan diferentes equipos para el manejo de la información, sin embargo la escasa mano de obra para la administración y configuración de equipos de la marca Juniper ha hecho que pequeñas empresas subcontratadas por Tigo, Claro o Telefónica vean una oportunidad de mercado para prestar el servicio de soporte manejando y administrando equipos juniper.

A pesar que estas empresas manejan equipos Juniper no hay mucha información de donde investigar sobre estos equipos y mucho menos información para poder obtener una certificación que avale el conocimiento adquirido y experiencia sobre el manejo de estos equipos. Por ello se ha desarrollado este proceso para someterse al examen de certificación JNCIA-102.

En este trabajo se desarrollaron temas específicos que son evaluados durante la certificación, ya que el examen JNCIA-102 es la base del resto de certificaciones que proporciona la compañía Juniper Networks es necesario adquirir todos los conocimientos básicos como por ejemplo las características del sistema operativo, la jerarquía en que trabaja el sistema operativo, que son y cómo se configuran los diferentes protocolos de enrutamiento en equipos Juniper, se de comprender cuales son las ventajas y desventajas al momento de utilizar estos equipos, en el manual de certificación se verán ejemplos de cómo se configuran las diferentes interfaces del equipo, como monitorear el equipo de manera que al surgir un problema se pueda encontrar rápidamente el origen del mismo.

Todo este proceso se ha realizado con el fin de que exista mayor mano de obra calificada en el manejo de estos equipos ya que cada día las compañías de telefónica celular están adquiriendo equipos Juniper no solo por su precio sino por la robustez del equipo en sí. Esto ha generado una demanda de personal con experiencia y el conocimiento sobre este tipo de equipos. Con esto en mente la información que se presenta está enfocada en la certificación JNCIA-102 y los temas impartidos son puntos tomados directamente del programa de certificación que Juniper Networks ofrece para luego poder someterse al examen oficial.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

I. INTRODUCCIÓN

Actualmente el uso de la telefonía celular y la transferencia de datos, o compartir archivos en cualquier parte del mundo, es posible gracias a la red de redes (Internet), sin embargo para que esto se pueda llevar a cabo sin ningún inconveniente, existen una cantidad de equipos involucrados que manejan de manera correcta y segura la información. Equipos como Tellabs, Cisco, Alcatel y Juniper son los que administran el tráfico de la información en el internet, es por eso que en el mundo de las telecomunicaciones se necesita personal calificado para operar y configurar estos equipos.

Uno de los equipos en donde hay poca mano de obra calificada para su correcta configuración son los equipos Juniper, en Guatemala las empresas proveedoras de internet como Tigo, Claro y Telefónica están dispuestas a contratar o subcontratar personal que los apoye en la configuración de estos equipos. Grupo STG ve un nuevo segmento de mercado en esta área por lo que en este trabajo se realiza una guía en donde se explica paso a paso en una serie de capítulos, toda la información necesaria para la administración y configuración de los equipos Juniper, en este trabajo se abordan conceptos básicos como por ejemplo: los fundamentos de las redes, de computadora que es la base para manejar cualquier equipo de telecomunicaciones, para luego iniciar con una seria de capítulos que estarán enfocados directamente en la configuración de equipos Juniper. Luego de finalizar el trabajo el lector estará capacitado para someterse al examen de certificación JN0-102 con nombre JNCIA (Juniper Network Certified Associate) en donde le da la credibilidad a cada ingeniero del conocimiento y experiencia que ha adquirido.

El diseño de este proceso es de gran beneficio para las personas que deseen o tengan la necesidad de obtener la certificación, ya que actualmente para poder obtener esta certificación se debe pasar por un curso que lo imparte Juniper Network con un alto costo económico y con una duración de 6 meses, debido a que no todas las personas cuentan con la capacidad de absorber dicho costo se decidió realizar un proceso en donde cualquier persona que tome este curso pueda pasar el examen de certificación JNCIA-102 sin verse en la necesidad de pagar un curso y recibirlo en un tiempo relativamente corto. Todo profesional que obtenga la certificación estará en la capacidad de manejar y configurar servicios de voz, datos e internet así como diseñar e implementar redes utilizando equipo de la marca Juniper. Esto abre una gran oportunidad para ingenieros Guatemaltecos son pocas las personas que cuentan con este tipo de certificación.

II. ANTECEDENTES

A. REDES DE COMPUTADORAS

1. Historia

La historia de las redes de computadoras se remonta al año 1957 cuando los Estados Unidos creó el Advanced Reserch Projects Agency (ARPA), como organismo afiliado al Departamento de Defensa para impulsar el desarrollo tecnológico. Este organismo fue clave en el desarrollo de las redes de computadoras y su exponente más significativo que fue el internet.

Inicialmente el ARPA tenía como principal objetivo situar a los Estados Unidos como el líder mundial en tecnología que fuera aplicable al entorno militar. Posteriormente a la creación del ARPA, mientras este organismo se iba abriendo espacio, Leonard Kleinrock, un investigador del MIT (Massachusetts Institute of Technology) escribió el primer libro sobre tecnologías basadas en la transmisión por un mismo cable de más de una comunicación. Estas técnicas se denominan tecnologías de conmutación de paquetes que constituyen la base para la transmisión de información entre computadoras. Un año más tarde a la publicación de Kleinrock, dos científicos del MIt ,Linklider y Clarck, lanzaron la primera publicación llamada "Comunicaciones hombre-computadora en línea" donde se propuso la necesidad de una cooperación social a todos los niveles mediante el usos de redes de computadoras. Aunque su publicación no tuvo un carácter científico, si se tenía el enfoque de cómo debían ser las comunicaciones en el futuro. Dos años después, en 1964, Paul Baran de la RAND Corporation, realizo la primera propuesta que sería de utilizar redes basadas en conmutación de paquetes a través de su publicación con el nombre "De las redes de comunicación distribuidas (On Distributed Communications Networks)". (Garret, Aviva 2006).

En 1965, la ARPA, como consecuencia de sus programas tecnológicos de cooperación, patrocino un programa que trataba de analizar las redes de comunicación usando computadoras (cooperative network of time-sharing computers). Mediante este programa, la maquina TX-2 en el laboratorio Lincoln del MIT y la AN/FSQ-32 del System Development Corporation de Santa Mónica en California, se enlazaron directamente mediante una línea dedicada de 1.200 bits por segundo. Un bit, es la unidad mínima de transmisión de información. Para tener un punto de referencia la transmisión de una letra requiere 8 bits.

Para hacerse una idea de las características de aquella línea, hoy en día cualquier persona desde su domicilio tiene la posibilidad de comunicarse con internet a una velocidad de 36.900 bits por segundo sin necesidad de disponer de medios sofisticados.

Un año después de esta experiencia, Lawrence G.Roberts (MIT) mediante su publicación Towards a Cooperative Network of Time-Shared partido) realizo la primera propuesta sobre la construcción de una red que tuvo como nombre ARPANET (nombre de la red de computadoras del ARPA) y que sería consecuencia de las experiencias vividas un año antes.

En 1967, la ARPA convoca una reunión en Annn Arbor (Michigan), donde se discutió por primera vez aspectos sobre la futura ARPANET. Ese mismo año se celebró un congreso de la ACM (Association for Computer Machinery) en la cual Larry Roberts expuso la primera publicación donde se propusieron las guías básicas del diseño de la futura ARPANET (Redes de múltiples computadoras y de comunicaciones entre computadoras). En este mismo congreso se celebró por primera vez una reunión entre los tres grupos mundiales que trabajaron en técnicas de conmutación de paquetes que fueron: NPL (National Physics Laboratory), RAND Corporation y ARPA.

En 1968 la ARPA no espero más y convoco a empresas y universidades para que propusieran diseños con el objetivo de construir la futura red. (Garret, Aviva 2006).

La Universidad de California gano la propuesta para el diseño del centro de gestión de red y la empresa BBN (Bolt Beranek and Newmann Inc) ganó el concurso de adjudicación del contrato para el desarrollo de la tecnología de conmutación de paquetes mediante la implementación de la Interfaz Message Processors (IMP); Interfaz de mensajes para procesadores. Por parte de la ARPA Steve Crocker encabezo el grupo NWG (Network Working Group) para el desarrollo de la sintaxis de comunicación (protocolos) entre computadoras que se utilizaron posteriormente en ARPANET.

Cabe mencionar que en 1969 se creó la prime red de computadoras de la historia. Esta red se denominó ARPANET, y supone el origen del actual internet. 1969 fue un año clave para las redes de computadoras, ya que se construyó la primera red de computadoras de la historia. Esta red, fue denominada ARPANET, estaba compuesta por 4 nodos situados en UCLA (Universidad de California en los Angeles), SRI (Instituto de Investigaciones de Stanford, San Francisco,

California), UCSB (Universidad de California de Santa Barbara, Los Ángeles) y la Universidad de Utah.

La primera comunicación entre dos computadoras entre los nodos de UCLA y Stanford el 20 de octubre de 1969. El autor de este envió fue Charles Kline (UCLA). La primera letra tecleada fue la "G" cuando trataba de acceder al sistema (login) en la máquina del SRI de Stanford.

Aunque el hecho en sí supuso uno de los hitos más importantes de la historia de las redes de computadoras, sus autores se limitaron a comprobar que el experimento había salido bien. No hubo celebraciones, ni siquiera comunicaciones oficiales. Era un paso más en el proyecto, financiado por el ARPA. (Garret, Aviva 2006).

En ese mismo año, la Universidad de Michigan creo una red basada en conmutación de paquetes, con un protocolo llamado X.25 denominada Merit Network. La misión de esta red fue la de servir de guía de comunicación a los profesores y alumnos de dicha universidad, en este mismo año se empezaron a editar los primeros RFC (Request For Comments). Los RFC son los documentos basados en TCP/IP y sus protocolos asociados. Estos RFC explican con detalle cómo se realizan las comunicaciones, de manera que cualquier fabricante que quiera realizar un protocolo no tiene más que seguir sus instrucciones. El primero RFC lo edito Steve Crocker (ARPA) el 7 de abril de 1969 y tenía por título "host Software" (Software de Servidores).

En 1970 la ARPANET comienzo a utilizar para sus comunicaciones un protocolo host-to-host (maquina a máquina). Este protocolo se denomina NCP (Network Control Protocol) y es el predecesor del actual TCP/IP que se utiliza en toda la internet. En ese mismo año, Norman Abramson desarrollo la ALOHANET en la Universidad de Hawai. La ALOHANET fue la primera red de conmutación de paquetes vía radio y se unió a la ARPANET EN 1972. Ya en 1971, la joven ARPANET estaba compuesta por 15 nodos y 23 máquinas que unían mediante conmutación de paquetes computadoras situadas en UCLA, SRI, UCSB, Universidad de Utah, MIT , BBN, Corporación RAND, SDC, Harvard, Laboratorio Lincoln, Universidad de Stanford, UIU, CWRU, CMU (Carnegie-Mellon University) y NASA/AMES. En ese mismo año de 1971 Ray Tomlinson (BBN) creo un programa de e-mail (Electronic mail) para distribuir mensajes a usuarios concretos a través de la ARPANET. El programa original de e-mail no era más que la unión de un programa de e-mail para una sola maquina con un programa experimental de transferencia de archivos.

En 1972 se eligió el popular signo @ como tecla de puntuación para la separación del nombre del usuario y de la maquina donde está dicho usuario. Este mismo año, durante la celebración de Washington de la Conferencia Internacional de Comunicaciones a través de computadoras (ICCC) se realizó la primera demostración pública de la ARPANET con 40 computadoras. En esa misma demostración se realiza el primer chat (conversación interactiva) entre Stanford y la BBN. Esta chat tuvo como argumento una consulta médica. En esta conferencia se notar la necesidad de crear un grupo que profundiza en aspectos relativos a las comunicaciones entre redes. El grupo se creó con el nombre de INWG (International Network working group) y fue inicialmente dirigido por Vinton Cerf.

Ese mismo año de 1972 se emitió el RFC 318 con la especificación de la aplicación telnet para emulación remota de terminales. Mediante esta orden se podía ejecutar comandos en una maquina sin estar sentado necesariamente delante de ella.

Por otra parte, los esfuerzos en Europa por unirse al proyecto americano empezaron a producirse. En este sentido es de destacar a Louis Pouzin en Francia, que comenzaba a implementar la versión francesa de la ARPANET denominada CYCLADES. (Garret, Aviva 2006).

En 1973 se dio la primera conexión internacional de la ARPANET. Dicha conexión se hizo con el Colegio Universitario de Londres (Inglaterra) y con el NORSAR noruego. En ese mismo año Bobo Metcalfe expuso sus primeras ideas para la implementación del protocolo Ethernet como resultado de las investigaciones hechas en su tesis doctoral. Ethernet actualmente es uno de los protocolos más importantes que se utiliza en las redes locales de computadoras para la transmisión de información.

Ese mismo año la Xerox en Palo Alto (San Francisco) experimenta las ideas de Metcalfe y crea la primera red basada en la tecnología Ethernet. Esta red se denominó Alto Aloha System. Simultáneamente, Bob Kahn y Vinton cerf empiezan a exponer los problemas derivados de la comunicación entre redes. Cerf expone en la Universidad de Sussex (Brighton , Inglaterra) las primeras ideas sobre la implementación de dispositivos que unirán redes pasarelas. Como anécdota cabe destacar que esas ideas las había esbozado en un sobre de correos durante una espera en el recibidor de un hotel de San Francisco. A mediados de ese año se edita el RFC 454 con

especificaciones para la transferencia de archivos, a la vez de la Universidad de Stanford comienza a emitir noticias a través de la ARPANET de manera permanente.

En ese momento la ARPANET contaba con ya 2000 usuarios y el 75 por 100 de su tráfico lo generaba el intercambio de correo electrónico.

En 1974 Cerf y Kahn publica su artículo “A Protocol for Packet Network Interconnection” (un protocolo para interconexión de redes de paquetes), que especificaba con detalle el diseño del protocolo de control de transmisión (TCP), una de las bases más importantes de la actual internet. Un año después en 1975 se crean las primeras listas de distribución de correo en internet, cuya gestión operacional había sido transferida al DCA. La lista más popular de todas las que se publicaban era una dedicada a la ciencia ficción.

Ese mismo año John Vital desarrolla MSG el primer programa de correo que daba la posibilidad de discriminar selectivamente el correo electrónico mediante filtros, replicar y reenviar el mismo. Se prueban los primeros enlaces vía satélite cruzando dos océanos (desde Hawai hasta Inglaterra) con las primeras pruebas de TCP de la mano de Stanford, UCLA, UCL. La reina Isabel II de Inglaterra envía en 1976 un correo electrónico desde Malvern (Inglaterra) y ese mismo año se distribuyen las primeras versiones del programa UUCP (Unix- to- Unix Copy) del sistema operativo Unix por parte del AT&T.

Los años siguientes consiguen establecer, definitivamente, el ámbito de la ARPANET con la creación de la Tymnet (1977), el lanzamiento de la especificación definitiva del mail (RFC 733, 1977), la primera demostración de una red de paquetes vía radio con pasarelas en la bahía de San Francisco y la división del protocolo TCP (Protocolo de control de transmisión) en dos TCP e IP (Protocolo de Internet) (1978). (Garret, Aviva 2006).

En 1979 se crea la USENET utilizando UUCO entre Duke y la UNC par a la distribución de grupos de noticias. La jerarquía original de los grupos utilizo el sufijo net. Ese mismo año la ARPA establece la ICCB (Internet Configuration Control Board). Durante ese mismo año se producirían hechos anecdóticos como la sugerencia por parte de Kevin Mackenzie de añadir complementos simpáticos a los textos planos de las news como para expresar alegría. Los emoticons como se denominaron comienzan a ser ampliamente utilizados por toda la comunidad.

La parada generalizada de la ARPANET el 27 de octubre de 1980 da los primeros avisos sobre los peligros de la misma. En 1981 de crea la BITNET (Because It´s Time NETwork) como una red particular que proporcionaba correo electrónico y listas de distribución. Ese mismo año se crean redes particulares como la CSNET (Computer Science Network) que proporcionan servicios de red a científicos sin acceso a la ARPARNET o Minitel en Francia por parte de la France Telecom. También se realiza el plan para la transmisión desde el viejo NCP al recién protocolo TCP/IP (RFC 801). (Garret, Aviva 2006).

1982 es el año en el que la DCA y la ARPA nombra a TCP e IP como el conjunto de protocolos TCP/IP de comunicación a través de la ARPAENT . En Europa se crea la EUnet (European UNIX Network) para proporcionar servicios de USENET y correo electrónico entre Inglaterra, Dinamarca, Holanda y Suecia. Se especifica el protocolo de comunicación de pasarelas entre redes (EGP-RDC 827) Al año siguiente se desarrollarían en la Universidad de Wisconsiin los primero conceptos sobre servidores de nombres para identificar la computadoras TCP/IP de manera más cómoda. El 1 de enero de 1983 se abandona la etapa de transición de NCP a TCP/IP pasando este último a ser el único protocolo de la ARPANET. Se comienza a unir redes y países ese mismo año como la CSNET, la MINET Europa, o países como Cores; se crean nuevas redes como la EARN (European Academic and Research Network) o Fidonet por Tom Jennings. La ICCB es reemplazada por la IAB (Internet Activities Board) que en el futuro se encargaría de todas las actividades y regulaciones de protocolos que tuvieran que ver con la ARPANET.

En 1984 se introduce, finalmente, el sistema de nombres de dominio (DNS Domain Name System) que se sigue utilizando en la actualidad para la conversión entre nombres de máquinas y direcciones IP. En ese momento el número de máquinas conectadas rondaba las 1.000. Se empieza a producir hechos que hablan de la importancia que va adquiriendo la red, como la creación de la JUNET (Red unix japonesa), JANET (Red académica Unida) en Inglaterra, NetNorth (Red del Norte) en Canadá o el anuncio por parte de la URSS de su unión a la Usenet.

En 1985 se establecen responsabilidades para el control de los nombres de dominio y así el ISI (Instituto de ciencias para la información) asume la responsabilidad de ser la raíz para la resolución de nombres de dominio, mientras que la SRI asume las responsabilidades de asignar estos nombres en los que se conoce como registros NIC (Network Information Center). El 15 de marzo de 1985 se produce le primer registro de nombre de dominio (symbolics.com) a los que

seguirían cmu.edu,rice.edu,ucla.edu y uk. En 1986 se crearía la primera red troncal de internet. Este tipo de grandes redes troncales que une multitud de pequeñas redes se denominan backbones. El nombre del primer backbone fue NSFNET (Red de la fundación nacional de ciencias), tenía un ancho de banda de 56.000 bits por segundo unía cinco centros de supercomputadoras (Princeton, Pittsburgh, San Diego, Illinois y Cornell).

Nota: El primer nombre de dominio registrado fue symbolics.com y se produjo el 15 de marzo de 1985. Hoy día, la guerra por los nombres de dominio es una de las acciones especulativas más complejas y conflictiva de internet.

Posteriormente, la IAB creó dos nuevos organismos que han resultado decisivos para el crecimiento de Internet: IETF (Grupo de Tareas de Ingeniería de Internet) e IRTF (Grupo de tareas de investigación de Internet). Ese mismo año se presentó el protocolo NNTP (Network News Transfer Protocol) para mejorar el rendimiento de la gestión y envió de noticias a través de Internet y se desarrollaron los MX records (Mail eXchange Records) para permitir a las maquinas sin dirección IP de red ser capaces de tener nombres de dominios. (Garret, Aviva 2006).

Internet a partir de ese año se construye en una realidad social indiscutible que va aglutinando a todos los países del mundo en torno a una malla de comunicación que ha permitido construir lo que se ha dado en llamar la “aldea global”. Internet es, hoy por hoy, según los datos sobre obras de ingeniería, la mayor obra tecnológica realizada por el ser humano en toda su historia.

A partir de 1987 se han sucedido numerosos acontecimientos que han convertido a las redes de computadoras en general, y a internet en particular, en una nueva revolución cultural y social que ha afectado prácticamente todas las facetas de la vida cotidiana. Su impacto es indiscutible, la sociedad de información se presentó como una alternativa real a muchas pautas de comportamiento desarrolladas en el siglo XX que han redefinido su forma de ver las cosas.

El gran impacto que ha traído el desarrollo de las redes es indiscutible ya que esto a permite que la sociedad evolucione cada día más y que todo este a un solo click de distancia. Sin embargo se debe tomar muy en cuenta la protección de los datos a través de cualquier tipo de red ya se publica o no, de lo contrario personas ajenas podrían capturar los datos y alterarlos durante su transmisión.

2. Fundamentos de red

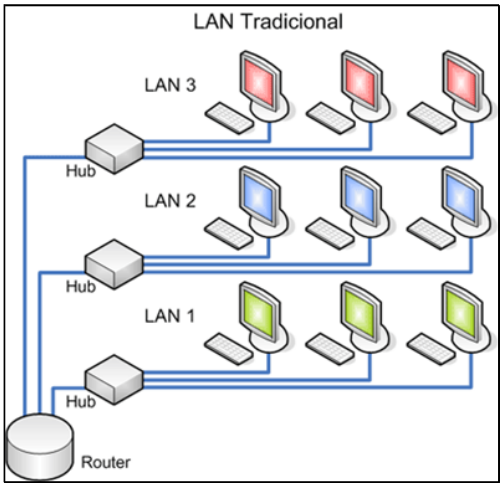
En la informática de hoy en día, solemos encontrar una gama de herramienta, aplicaciones y programas que hacen de la vida cotidiana o laboral más eficaz. Aunque estas no aparecen de la nada para emplear o crear tales cosas debe saberse los distintos componentes que componen las redes de datos y de telecomunicaciones.

2.1 Redes de datos

Una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. Los enlaces conectados con los dispositivos se denominan a menudo canales de comunicación.

Las redes usan procesamiento distribuido en el aspecto en que una tarea está dividida entre múltiples computadoras. En lugar de usar una única máquina grande responsable de todos los aspectos de un proceso, cada computadora individual (habitualmente una computadora personal o una estación de trabajo) maneja un subconjunto de ellos, esto permite que una sola tarea pueda realizarse en diferentes equipos, pero al momento de compartir información dentro entre diferentes redes de computadoras, es cuando entra en juego el Router y el manejo del mismo (Odon, 2004).

Figura 1. Estructura de una red básica



Fuente. Cisco CCNA intro

2.2 Tarjeta de red

Es un periférico que permite la comunicación de aparatos conectados entre sí, al igual que compartir recursos entre dos o más computadoras, discos duros, CD-ROM, impresoras o cualquier otro sistema, incluyendo la preparación y control de datos en la red. Las tarjetas de red presentan configuraciones que pueden modificarse. Algunas de estas son: los interruptores de hardware (IRQ) la dirección de E/S y la dirección de memoria (DMA).

2.3 Protocolo de red

Un protocolo de red, se define como un conjunto de normas a seguir utilizadas para regular la comunicación entre distintos componentes existentes en una red de informática o red de ordenadores. Hay dos tipos de protocolos: de nivel bajo y protocolos de red

Los protocolos de bajo nivel mantienen el control de las señales que se transmiten por el cable o por el medio físico. Los de red organizan la información para llevar a cabo su transmisión por el medio físico a través de los protocolos de nivel bajo.

2.4 Topología de red

Definida como una familia de comunicación que es usada por las computadoras que son parte de una red para intercambiar datos. Las topologías de red indican de qué manera están organizados los dispositivos de una red. Dichas topologías son arquitecturas lógicas, esto significa que señalan la dirección en la que las señales van entre los dispositivos que forman parte de la red, pero, los cables que han de conectar estos dispositivos pueden no estar conectados de la misma manera como la señalada por la topología, por ejemplo; las topologías de redes en bus y en anillo son comúnmente organizadas físicamente como una red en estrella. (Odon 2004)

Entre las ventajas de las topologías de red en general están: la facilidad de crecimiento de nodos en la red, la simplicidad de arquitectura y en algunos casos el requerimiento de cableado será menor.

Entre las desventajas de las topologías de res se encuentran: dependiendo de qué topología de red se implemente pueden ocurrir mayor número de colisiones entre mensajes lo que produce graves pérdidas en la transmisión.

3. Tipos de redes

3.1 Redes de área local

Una red de área local o Local Área Network (LAN) es una red de computación que está diseñada para interconectar computadores en una área limitada, como sería un colegio, un hogar, un

laboratorio de informática o un edificio de oficina usando medios de comunicación de redes. Las características que definen las redes de área local, en contraste con otras redes, incluyen sus usualmente altas tasas de transferencia de datos y que esas redes cubren áreas geográficas más pequeñas. Estas redes se pueden lograr con conexiones de red de tipo inalámbrica y cables de red trenzados, que son ideales para anular interferencias que perturban la experiencia de usuario. (Odon 2004)

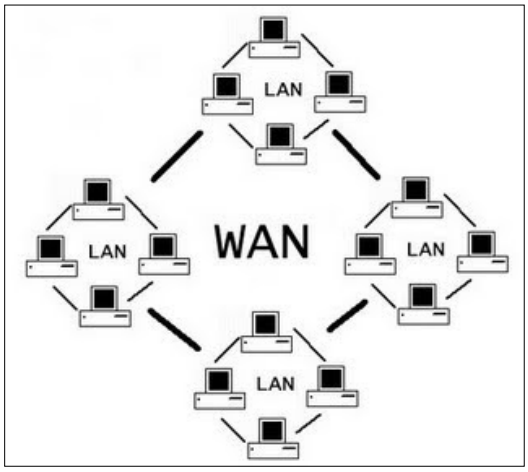
3.2 Red de área amplia

Una red de área amplia (WAN, por sus siglas en inglés) es una red que cubre un espacio amplio, por ejemplo; cualquier red de telecomunicación que vincule metrópolis, conurbaciones o áreas de carácter regional o nacional haciendo uso de redes de transporte de datos, que pueden ser públicas o privadas. Los comercios, las empresas y las entidades públicas hacen uso de las redes de área amplia para distribuir información importante entre sus trabajadores, clientes, compradores y proveedores de diversas ubicaciones geográficas. En esencia, este tipo de telecomunicación le permite a un comercio el llevar a cabo las funciones del día a día eficazmente independientemente de la ubicación, es decir, es posible para un empresario gestionar correctamente los datos relacionados a su empresa aun cuando no se está ahí. (Stalings, 2000)

Este tipo de redes permiten compartir dispositivos y tener un acceso rápido y eficaz, lo que la diferencia de las de más redes es que proporciona un medio de transmisión a larga distancia de datos, voz, imágenes, videos, sobre grandes áreas geográficas que pueden llegar a extenderse hacia un país, un continente o el mundo entero, es la unión de dos o más redes LAN.

Dentro de las características de esta se encuentran, la operación dentro de un área geográfica extensa, permite el acceso a través de interfaces seriales que operan a velocidades más bajas y suministra velocidad parcial y continua, entre otras.

Figura 2. Red de área amplia



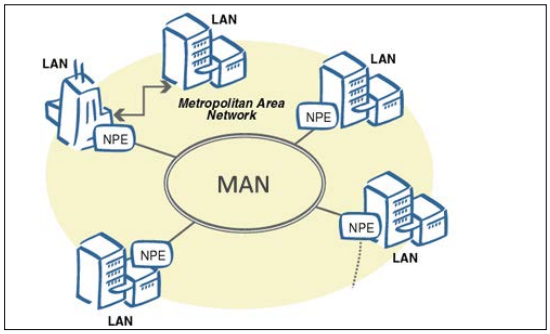
Fuente: Juniper JNCIA Intro

3.3 Redes de área metropolitana MAN

Estas redes han sido diseñadas para que se pueda extender a lo largo de una ciudad entera.

Puede ser una red única como una red de televisión por cable, o puede ser una forma de conectar un cierto número de LAN en una red mayor, de forma que los recursos puedan ser compartidos de LAN a LAN y de dispositivo a dispositivo. Una empresa puede usar una MAN para conectar las LAN de todas sus oficinas dispersas por la ciudad, como puede observar siempre abra un punto central en donde se da la comunicación entre sucursales, una de las ventajas de este tipo de redes es la capacidad de reconfiguración cuando se producen fallas. (Costas y Weber 2004).

Figura 3. Red MAN



Fuente: Juniper JNCIA Intro

4. Equipos de Red

4.1 Router

Un router es un dispositivo de red que como su propio nombre indica se encarga de llevar por la ruta adecuada el tráfico. En la mayoría de los hogares seguramente se encuentra uno de estos equipos que es el que te conecta con la red Internet. (Costas y Weber 2004).

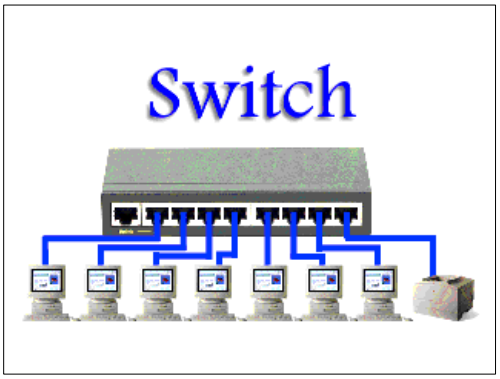
Figura 5. Router

Fuente: Cisco CCNA

4.2 Switch

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de Rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

Figura 6. Switch



Fuente. Juniper JNCIA Intro

4.3 Hub

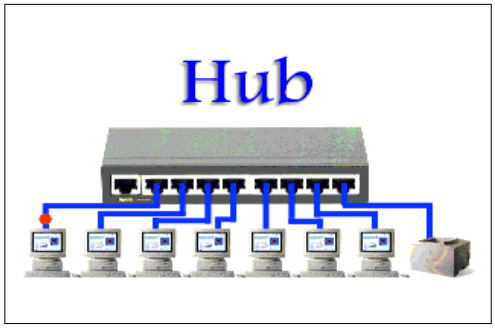
El funcionamiento de un concentrador está dado por la repetición de un mismo paquete de datos en todos sus puertos, de manera que todos los puntos accedan a la misma información al mismo tiempo. El hub es fundamental para el tipo de redes en estrella. Otra alternativa para este tipo de redes son los repetidores multipuerto. Un sistema en el que los ordenadores en comunicación se conectan en serie a una línea que los entre sí. Los repetidores multipuerto pueden ser pasivos (no necesitan energía eléctrica), activos (sí la necesitan), o inteligente (que incluyen un microprocesador y son llamados smart hubs).

Tradicionalmente, los concentradores sufrieron el problema de sólo podían soportar una única velocidad. Si los ordenadores de PC son fácilmente actualizables, otros ordenadores pueden ser difíciles de actualizar. Una relación entre un conmutador y un concentrador o hub se considera un concentrador de doble velocidad.

En competencia con un conmutador, el concentrador solía ser una opción de precio más económico. Si bien hoy en día los conmutadores también son accesibles, el concentrador sirve para ocasiones especiales. Por ejemplo, un hub es útil para analizar todo el tráfico de un segmento de redes. Otro caso es que con un conmutador es más fácil para un usuario inexperto provocar un bucle de datos en la red. En cambio, con un concentrador, es más difícil que esto ocurra. (Costas y Weber 2004).

Los hub sobrecargan la red reenviando todos los paquetes de información al conjunto de máquinas conectadas.

Figura 7. Hub



Fuente. Juniper JNCIA Intro

B. ADMINISTRADOR DE RED

Es la persona responsable de la configuración y administración de la red. El administrador generalmente configura la red, asigna contraseñas, permisos y ayuda a los usuarios.

Es la persona responsable de supervisar y controlar el hardware y software de una red; incluye el control del esquema de seguridad y administración de procesos y aplicaciones en red.

En la actualidad vivimos en una sociedad que depende de los Sistemas de Información (SI), que se encuentran tanto en la parte interna de cualquier organización (utilizada para la toma de decisiones por ejemplo) como hacia la exterior (la internet), sin embargo para poder acceder a esta información es necesario que estos sistemas se encuentren interconectados por medio de un recurso llamado red. Si analizamos más a fondo este recurso, veremos que se encuentra constituido por diversidad de equipos de red como por ejemplo routers, bridges, switches. etc. (Soricelli, Joseph M 2006).

Adicionalmente las redes internas de las empresas por lo general se deben conectar a otras redes (estas pueden ser corporativas e incluso la misma red interna) lo que hace que se vuelvan más complejas y heterogéneas, es en este punto es en donde entra la capacidad del ingeniero a cargo de administrar la red de computadoras de la empresa ya que debe de contar con la expertis necesaria.

Frecuentemente se ve al administrador de red como el profesional que se especializa en el mantenimiento de redes de computadoras, es como decir que el administrador de red es el equivalente al administrador de sistemas: que se especializa en el mantenimiento del hardware y el software. El perfil que define al administrador de red es el de un profesional técnico que es él quien se encarga de mantener optimizado la red de ordenadores, ampliar la red de ordenadores dentro de la empresa, el que maneja que usuarios acceden a cierto programas, impresiones y a su vez este está en constante interacción con el técnico que da soporte a sus servicios.

Dentro de las funciones principales de una administrador de red están: la detección de fallas, diagnostico de problemas, seguimiento y control, además de administrar los cambios, es decir, que de comprender la planeación y programación de evento ocurridos dentro y fuera de la red para actuar de manera eficiente.

1. Características del administrador de red

- El administrador de red debe ser una persona con los conocimientos y la experiencia necesaria para instalar, configurar y administrar los elementos de una red.
- Disponer de servicios de soporte en dispositivos de red y sistemas computacionales.
- Instalar sistemas de cableado de dispositivos alámbrico e inalámbricos de comunicación.
- El trabajo de un administrador de red también incluye el mantenimiento de la infraestructura de autenticación de la red.
- Instalaciones tales como los controladores (particularmente un controlador es un programa que permite al sistema operativo interactuar con una interfaz o acceder a una red)
- Es el encargado de los ajustes en los computadores y a veces de las impresoras.
- A veces se vincula con la configuración de los sistemas detectores de intrusos.
- El administrador de red también es el encargado de mantener la información de cuentas de usuarios segura.
- Es el encargado de la interacción que tenga la red con el exterior.
- El administrador de red debe ser el encargado de la instalación de la red con respecto a los recursos, el tamaño de la empresa, número de ordenadores dentro de la empresa para que la empresa no sobreexceda en gastos de instalación de red.
- El administrador de la red debe tener la capacidad de tomar las decisiones más adecuadas de acuerdo a cada situación.
- Debe ser una persona capaz de tomar la mejor decisión en caso de cómo se va a instalar el cableado dentro de la empresa para que así a la hora de unir o enlazar los diferentes departamento dentro de una organización no sea tan difícil y que a su vez no conlleve un gasto innecesario de los fondos de la empresa.
- Debe ser una persona capaz de mantener la calma en un estado de presión muy alto. Por ejemplo: En caso de que la red colapse por algún motivo Medioambiental, eléctrico o por el acceso de hacker o ataques informáticos al sistema deberá mantener la calma para dar resolución al problema ya sea de pequeña escala o por el contrario de gran escala.
- Es una persona que tiene como objetivo mantener segura la red ya sea a nivel de hardware o a nivel de software.
- Persona que debe estar en constante capacitación de nuevas tecnologías.
- Gestionar cualquier cambio de software y/o hardware en la red.

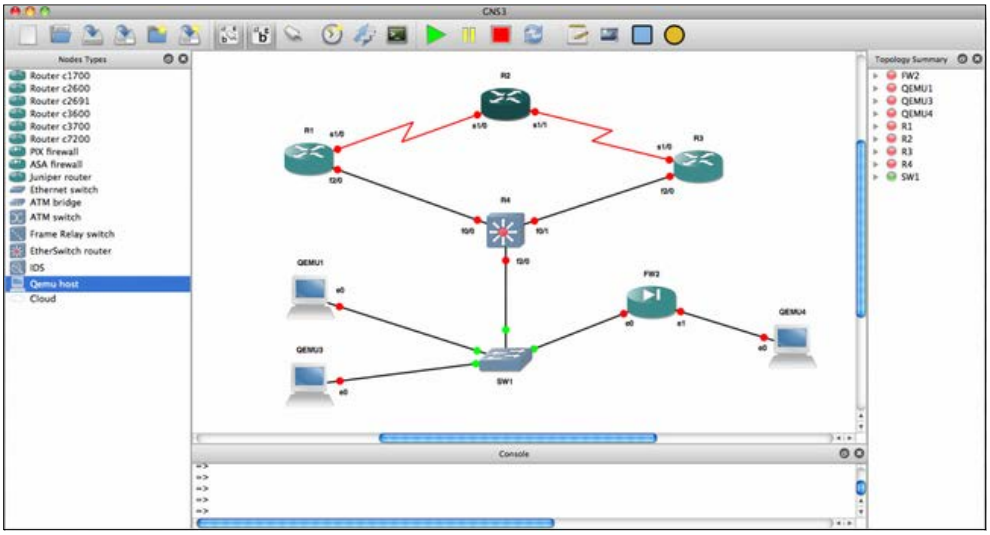
C. SIMULADORES

1. Simulador GNS3

GNS3 es un simulador grafico de redes (http://www.gns3.net/) de código abierto y libre distribución que se puede utilizar en múltiples sistemas operativos, incluyendo Windows, Linux y MacOS X. En particular, permite crear redes a través de un entorno grafico usando dispositivos de red que emulan CISCO IOS y Juniper JunOS. (Garret, Aviva 2006). GNS3 es una excelente herramienta complementaria a los laboratorios de red. Tambien se puede utilizar para experimentar o verificar las configuraciones de equipos de red antes de implementarlo más adelante en routers reales. Actualmente su versión más estable es la 0.7.4. La versión "all-in-one" proporciona todas las herramientas útiles para el simulador excepto los sistemas operativos a simular como CISCO IOS, JunOS, etc. Estos sistemas operativos no son de libre distribución y el usuario de GNS3 debe proporcionar las imágenes de los sistemas operativos que necesita simular.

En la siguiente figura muestra un ejemplo de red creada a partir del entorno grafico de GNS3. El menú de selección de los dispositivos disponibles se encuentra en la ventana de la izquierda. Una vez arrastrados en la ventana central, estos dispositivos se pueden conectar entre sí a través de enlaces que pueden usar tecnologías distintas, bien fastethernet, gigabitethernet, serial, etc.

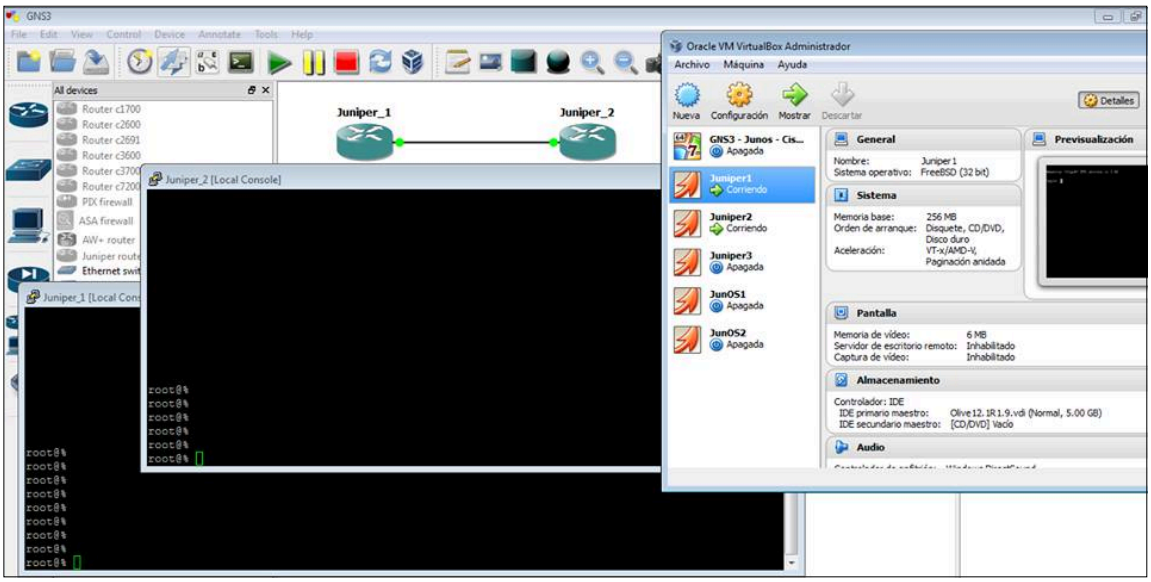
Figura 8. Enlaces GNS3



Fuente. GNS3

En esta otra figura se muestra cómo se puede acceder a la consola de un router. El router es realmente emulado, así que está corriendo realmente el sistema operativo del router y lo que aparece es la consola para configurarlo. Como las imágenes de los sistemas operativos son las reales, los comandos de configuración son exactamente iguales a los de un dispositivo real. (Garret, Aviva 2006). Con GNS3 se puede crear escenarios reales, es decir se puede montar una red con el diseño o topología deseada luego se configura y luego se carga la configuración a equipos reales.

Figura 9. Simulación equipos juniper



Fuente: Elaboración propia

Para virtualizar los dispositivos de red (routers, switches, etc.) son necesarias las imágenes del sistema operativo IOS. Sin embargo, por restricciones de licencia, el simulador no viene con las IOS de routers Cisco, las cuales deben ser proporcionadas al simulador y pueden ser descargadas de desde internet.

Dentro de las características más importante de GNS3, se puede destacar: su diseño de topología de red emular, emulación de redes Ethernet, ATM y switches Frame Relay, emulación de una gran variedad de IOS de Cisco, JunOS, IPS y firewalls, conexión de la red simulada a un entorno real, integración con Qemu y VirtualBox para emular hosts además de capturar paquetes integrando el uso de wireshark, esto permite hacer un estudio más profundo de los protocolo de comunicación que puede dar en una red y ver el compartimiento de los equipos que están operando.

D. IMPORTANCIA DE LA CERTIFICACIÓN JUNIPER JNCIA-102 (Juniper Networks Certified Internet Associate)

En la actualidad, las empresas buscan constantemente personas que sean altamente competitivas y cuenten con las certificaciones necesarias. La mayoría de las empresas de hoy en día buscan personas que hayan aprobado la certificación.

La certificación JNCIA-102 es la prueba de que un candidato cuenta con las habilidades necesarias para trabajar correctamente en un ambiente en redes. En realidad, esto le ahorra a las empresas tiempo y esfuerzo en la realización de pruebas y otras investigaciones de antecedentes necesarias para la contratación de personal.

Además, esto también les ahorrara dinero y tiempo en la capacitación de sus empleados. Las empresas también pueden prevenir problemas innecesarios en el sistema debido a la contratación de un JNCIA-102, ya que esta certificación asegura que la persona conoce muy bien los pasos básicos para la solución de problemas y la instalación de equipos. En las empresas de hoy en día, el tiempo es oro. Contratiempos y retrasos significan menos productividad, por lo tanto, menos ingresos para la compañía.

Las funciones esenciales de la mayoría de los puestos de trabajo de un JNCIA-102 incluyen la coordinación de recursos para incorporar los requisitos de red de la empresa y prestar apoyo en la red. Esto también incluye la asistencia en la planificación, la ejecución, la previsión y el reconocimiento de los requisitos de la red del sistema. Participar en la ingeniería, la arquitectura y la planificación son importantes en los trabajos relacionados con JNCIA-102.

Es por esto que hoy en día las empresas buscan candidatos que tengan la capacidad para realizar las funciones más importantes de TI. También deben tener la experiencia en los sistemas de información, tecnología de las telecomunicaciones, saber cómo diseñar redes e integrar sistemas. De hecho, las empresas regularmente mencionan con frecuencia en los anuncios de sus puestos de trabajo que requieren que los posibles candidatos tengan aprobadas las certificaciones JNCIA entre otros.

Una persona no necesita tener ningún título universitario para obtener la certificación JNCIA-102. Lo que se requiere es conocimiento de computación y mucho deseo de aprender. Mantener la competitividad en las empresas requiere de la contratación de personal altamente calificado. Es por esto que es muy importante para los profesionales de TI completan las certificaciones necesarias para suplir las necesidades demandadas en el mercado laboral y seguir avanzando en sus carreras como profesionales en TI.

La certificación JNCIA ayuda al profesional a entender cómo operan las redes de computadoras, es decir, como estas funcionan, se instalan y se administran. También aprenderá como opera la industria de las redes, lo cual será para el profesional un mundo lleno de nuevas posibilidades.

Si una persona o profesional desea ser contratado por una empresa en vez de convertirse en un consultor, este se encontrara que las destrezas adquiridas durante su preparación para ser un profesional certificado le hacen ser un candidato más atractivo para la posición que la persona o profesional desea desempeñar dentro de una organización. Se debe tomar en cuenta que los empleadores valoran mucho la experiencia "Real World" que pueda tener un posible candidato. Cabe mencionar que actualmente existe una gran demanda de personal calificado para el manejo de este tipo de equipos y por la falta de esta mano de obra, este tipo de trabajo se considera bien remunerado a para cualquier persona que cuente con los conocimientos necesarios.

III. JUSTIFICACIÓN

La calidad del servicio que una empresa presta a los usuarios, está respaldada por políticas internas de capacitación, que le permite a la organización incursionar en mercados cada vez más amplios, en Guatemala la oferta de telefonía celular a alcanzado niveles altamente competitivos, lo que obliga a las empresas a ofrecer valor agregado a su servicio y garantizar la prestación del mismo con personal calificado.

La certificación JNCIA que se identifica con el código JN0-102 de Juniper es una de las certificaciones más importante dentro de la industria de la Tecnología de la Información. Esta certificación representa el nivel Asociado, es decir, la certificación JNCIA sirve como punto de partida para que cualquier persona pueda emprender una gran carrera como especialista en redes en el manejo de equipos Juniper. Para que una persona pueda acreditarse como profesional certificado lo único que necesita hacer es pasar el examen de certificación de JNCIA, pero antes de intentar pasar dicho examen, el candidato debe de estar debidamente preparado para ello. Una de las razones por la que este trabajo se está realizando es para diseñar un trabajo que brinde todas las herramientas necesarias para que toda persona con el deseo y compromiso de adquirir este conocimiento no solo obtenga la certificación sino que también adquiera cierto grado de experiencia, equivalente a estar trabajando en el campo directamente.

En Guatemala existen muchas empresas que buscan posicionarse en el área de telecomunicaciones ya que ven una oportunidad de mercado en este sector, sin embargo para que una empresa tenga mayor credibilidad debe demostrar que su personal está altamente preparado para cualquier tipo de trabajo que se le presente y esto únicamente lo pueden realizar certificando a su personal.

IV. OBJETIVOS

Objetivos generales

Diseñar un proceso para certificar al equipo de ingenieros de “datos” e “implementación” de la empresa Grupo STG de Guatemala, S.A. según los requisitos requeridos por el examen con código JN0-102 referente a la configuración y administración de equipos Juniper.

Objetivos específicos

1. Diseñar el contenido programático del curso para ingenieros de la empresa Grupo STG.
2. Definir los pasos de un proceso de capacitación para que Grupo STG cuente con mano de obra calificada en equipos marca Juniper.
3. Definir la información necesaria que cumpla con los requisitos que requiere el proceso de certificación JN0-102 de Juniper.
4. Establecer los aspectos necesarios para abordar en un taller de capacitación, casos reales y de laboratorio dirigidos a ingenieros.

V. METODOLOGÍA

El trabajo de graduación se realizó cumpliendo la siguiente metodología con la cual se pretende realizar un manual para obtener la certificación JNCIA-102. En este se muestran aspectos como los requisitos para la certificación, temas que se evalúan en la certificación y procedimientos que se utilizaran para llevar a cabo dicho manual.

A. Tipo de estudio

Aplicada o constructiva

B. Universo

Área de telecomunicaciones

1. Muestra

Personal del área de telecomunicaciones específicamente en el área de redes, administrando equipos Juniper.

C. Método de recolección de información

Inicialmente se verificó en la página oficial del vendor, cuales son los temas y los requisitos que se requerían para obtener la certificación, a partir de esto se analizó y desarrollo cada tema de manera que cualquier ingeniero con poco o nada de conocimiento en el tema comprenda la información proporcionada por cada tema desarrollado, al final de cada capítulo se hizo una serie de preguntas enfocadas a la certificación para que el lector pudiera ir reforzando su conocimiento y poco a poco fuera preparándose para el examen de certificación.

D. Método de análisis de la información

El estudio propuesto se adecuó a los propósitos de la investigación experimental y no experimental. En función de los objetivos definidos en el presente estudio, donde se planteó la

optimización de un proceso mediante el desarrollo de diferentes temas para que cualquier persona interesada no solo obtenga la certificación sino que tenga mucha practica durante el curso.

E. Parte no experimental

Para la parte no experimental o teórica se realizó una recolección de la mayor cantidad de información, con el fin de obtener un conocimiento más amplio de la realidad del problema.

Por la naturaleza del estudio se requirió de recopilación documental, de los antecedentes relacionados con la investigación. Para tal fin se consultaron documentos escritos, formales e informales sobre los temas que evalúan en la certificación JNCIA-102, esto para garantizar la correcta interpretación de la información.

F. Parte experimental

Se utilizaron simuladores gráficos como GNS3 (Graphical Network Simulator) para emular equipos juniper, se crearon topologías específicas para que el ingeniero pudiera practicar los diferentes comandos o instrucciones para configurar y/o administrar los equipos.

VI. RESULTADOS

A. RESULTADO No.1

MANUAL PARA LA CERTIFICACIÓN JUNIPER JNCIA (JUNIPER NETWORKS CERTIFIED ASSOCIATE) CON CODIGO JN0-102, PARA PERSONAS QUE LABOREN EN EL AMBITO DE LA REDES EN TELECOMUNICACIONES

MANUAL PARA LA CERTIFICACIÓN JUNIPER JNCIA (JUNIPER NETWORKS CERTIFIED ASSOCIATE) CON CODIGO JN0-102, PARA PERSONAS QUE LABOREN EN EL AMBITO DE LA REDES EN TELECOMUNICACIONES

Autor: Belter Molina Guevara

Fecha: 21 de noviembre del 2014

Contenido

INTRODUCCIÓN

A continuación se desarrollaran diversos temas sobre el manejo de los equipos juniper, estos temas han sido desarrollados con el objetivo que cualquier profesional con poco conocimiento de redes, pueda optar por el examen de certificación JNCIA-102. En este manual se verán temas como la configuración inicial de un equipo juniper, manejo de las interfaces, saber distinguir entre las diferentes jerarquías dentro del equipo juniper, como por ejemplo el modo operación y el modo configuración entre otros. Un punto muy importante a discutir es el usuario root y su contraseña por defecto, estos y otros temas son requisitos que se deben conocer para poder enrolarse al examen de certificación.

1. FUNDAMENTOS DEL SISTEMA OPERATIVO JUNOS

1.1 Robustes, Modular y Escalable

La funcionalidad del Sistema Operativo Junos está dividida en múltiples procesos de software. Cada proceso se encarga de un parte de la funcionalidad del dispositivo. Cada proceso se ejecuta en su propio espacio de memoria protegida, asegurando que un proceso no pueda interferir directamente en otro. Cuando un solo proceso falla, todo el sistema no necesariamente tiene que fallar. Esta modularidad también se asegura que nuevas características se puedan agregar con menos probabilidad de romper la funcionalidad actual.

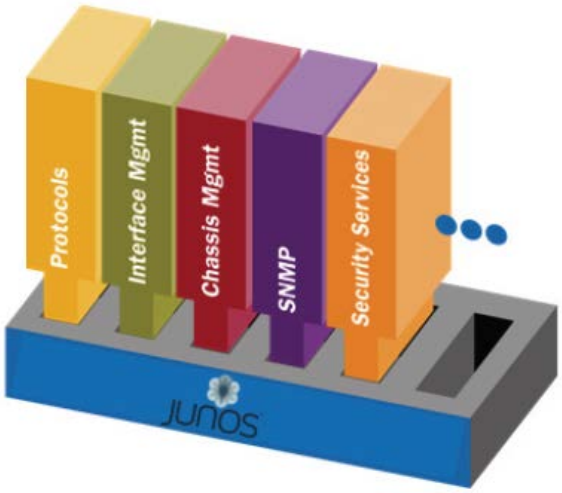


Figura 1. Modularidad Juniper

El sistema operativo Junos es un sistema de confianza, asegura una red operativa capaz de alimentar la infraestructura de red de alto rendimiento que ofrece Juniper Networks. El kernel de Junos se basa en el sistema operativo FreeBSD UNIX, que es un sistema de software de código abierto.

1.2 Un solo código base fuente

Todas las plataformas que ejecutan el sistema operativo Junos utilizan la misma base de código fuente del software dentro de sus imágenes específicas de la plataforma. Este diseño asegura que las características centrales funcionan de una manera consistente a través de todas las plataformas que ejecutan el sistema operativo Junos. Debido a que muchas características y servicios están configurados y gestionados de la misma manera, las tareas de instalación, mantenimiento y operación dentro de su red son simplificadas.

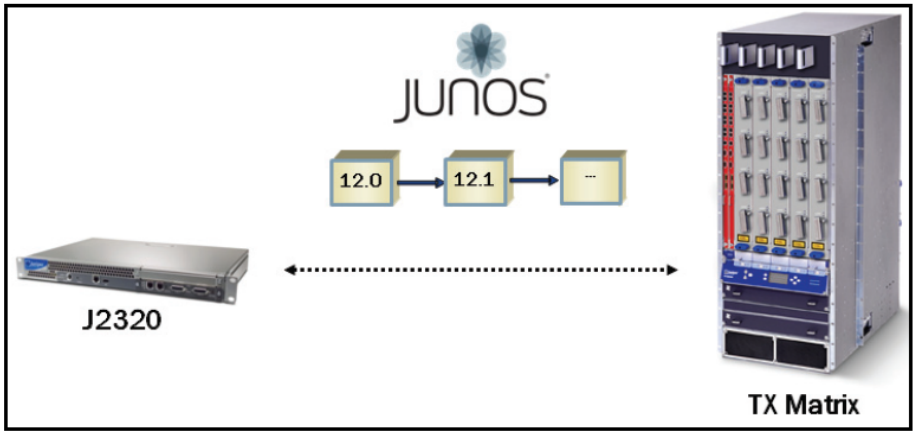


Figura 2. Plataformas con IOS Junos

Planos de Control y Reenvió separados

Otro aspecto de la modularidad de Junos es la separación del plano de control y el plano de reenvió de datos. Los procesos que controlan los protocolos de enrutamiento están separados de los procesos que reenvían las tramas, paquetes o de ambos a través del dispositivo que ejecuta el sistema operativo Junos. Este diseño le permite sintonizar cada proceso para el máximo rendimiento y fiabilidad. La separación de los planos de control y reenvío es una de las razones clave por las que el sistema operativo Junos puede soportar diferentes plataformas desde una base de código fuente común.

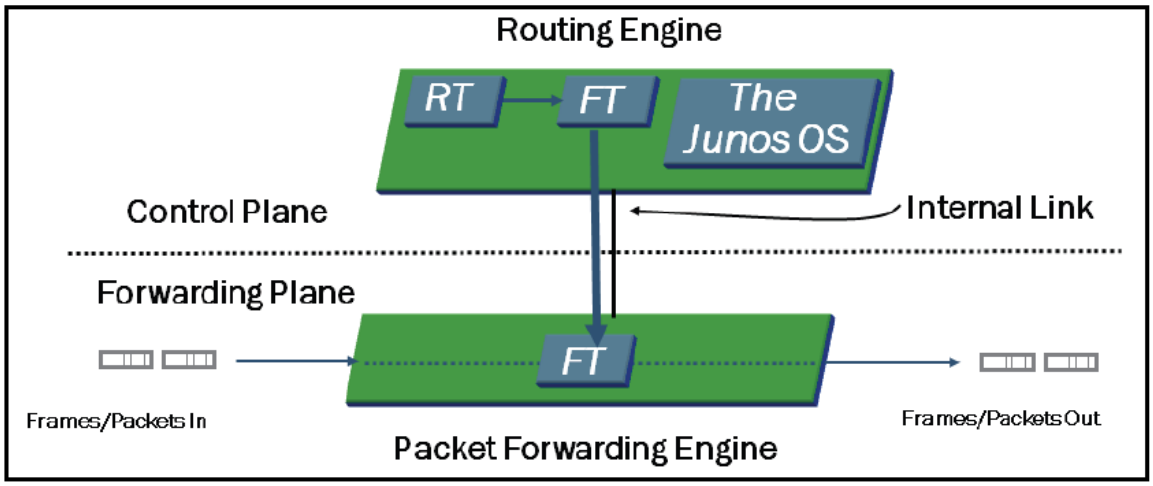


Figura 3. Plano de control y Reenvió

La grafica anterior muestra una visión básica de la arquitectura Junos y destaca el control y planos de reenvío. El plano de control, que se muestra por encima de la línea de puntos en el gráfico, se ejecuta o tiene lugar la Rounting Engine (RE). La RE es el cerebro de la plataforma; es la responsable de realizar actualizaciones del protocolo y la gestión del sistema. La RE ejecuta varios procesos de protocolo y software de gestión que residen dentro de un entorno de memoria protegida. La RE se basa en una arquitectura x86 o PowerPC, dependiendo de la plataforma específica de ejecutar el sistema operativo Junos. La RE mantiene las tablas de enrutamiento, establece una tabla de puenteo, una tabla de reenvío primaria y se conecta a la Packet Forwarding Engine (PFE) a través de un enlace interno. Aunque todos los dispositivos Junos comparten este objetivo de diseño común, los componentes reales que componen los planos de control y expedición varían entre los diferentes dispositivos Junos.

La Packet Forwarding Engine, que se muestra por debajo de la línea de puntos en el gráfico, por lo general se ejecuta en hardware independiente y es responsable de reenviar el tráfico de tránsito a través del dispositivo. En muchas plataformas que ejecutan el sistema

operativo Junos, la PFE utiliza circuitos integrados de aplicación específica (ASIC) para un mayor rendimiento. Esta arquitectura permite separar las operaciones de control tales como, gestión del sistema, operaciones de reenvío, actualización de protocolos etc. Las plataformas con sistema operativo Junos puede ofrecer un rendimiento superior y altamente fiable.

La Packet Forwarding Engine recibe la tabla de reenvío (FT) de la rounting engine a través de un enlace interno. Estas actualizaciones son una alta prioridad para el kernel del sistema operativo Junos y se realizan de forma incremental.

Dado que la inteligencia del sistema la provee la Routing Engine, La Packet Forwarding Engine simplemente realiza el reenvío de tramas, paquetes o ambos con algo grado de estabilidad y rendimiento.

1.3 Mantenimiento de la Routing Engine

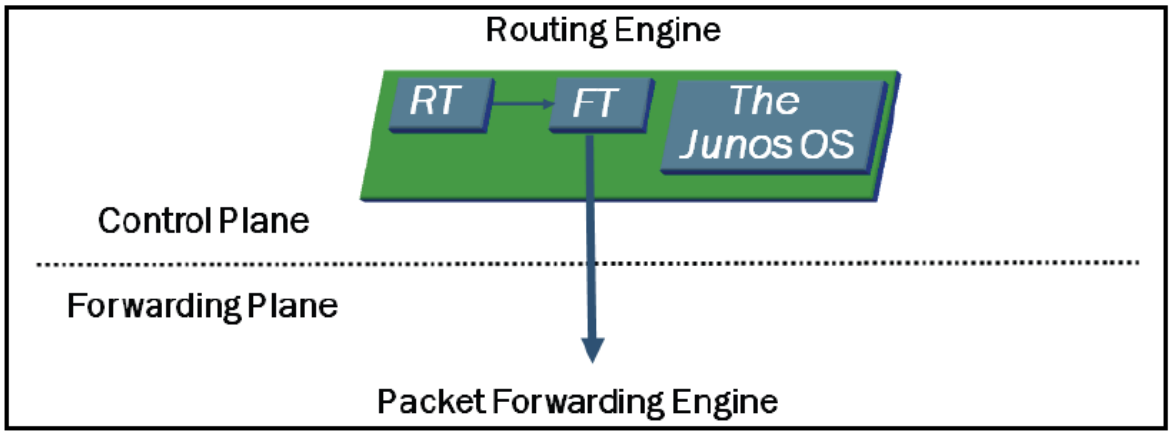


Figura 4. Mantenimiento de la Routing Engine

La Routing Engine se encarga de todos los procesos de protocolo, además de otros procesos de software que controlan las interfaces del dispositivo, los componentes del chasis, la gestión del sistema y el acceso del usuario al dispositivo. Estos procesos de software se ejecutan en la parte superior del kernel Junos, que interactúa con la PFE. El

software dirige todo el tráfico de protocolo de la red a la RE para el procesamiento requerido.

1.4 Reenvío de tráfico

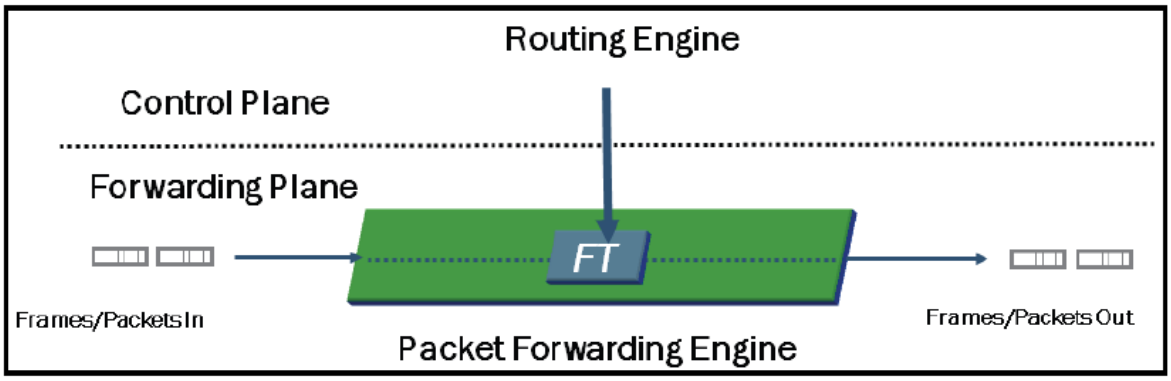


Figura 5. Reenvío de trafico

La Packet Forwarding Engine es el componente central de procesamiento del plano de reenvío. La PFE reenvía sistemáticamente tráfico en función de su copia local de la tabla de reenvío. La tabla de reenvío de la PFE es una copia sincronizada de la información creada y proporcionada por el RE. El almacenamiento y el uso de una copia local de la tabla de reenvío permiten a la PFE que transmita el tráfico de manera más eficiente y elimina la necesidad de consultar la RE cada vez que un paquete necesita ser procesado. Al utilizar la copia local de la tabla de reenvío, también permite a las plataformas que ejecutan el sistema operativo Junos continuar con el reenvío de tráfico durante las inestabilidades del plano de control.

1.5 Trafico de Transito

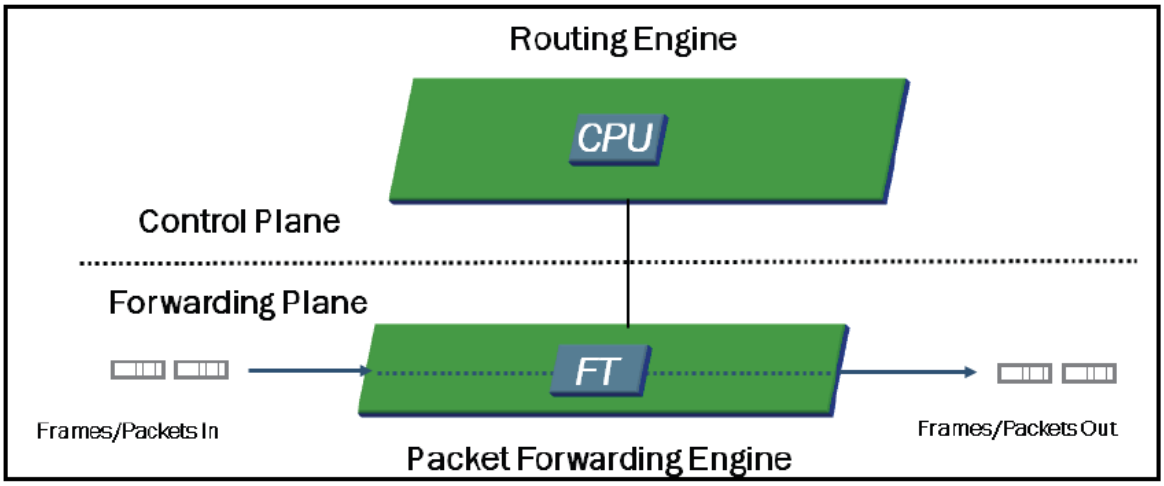


Figura 6. Trafico de transito

El tráfico de tránsito consiste de todo el tráfico que entra en un puerto de red, se compara con las entradas de la tabla de reenvío, y finalmente se reenvía a un puerto de red de salida que dirige el tráfico hacia su destino.

Una entrada en la tabla de reenvío hacia un destino debe de existir para que el dispositivo que está ejecutando el sistema operativo Junos envíe el tráfico de tránsito hacia ese destino.

El tráfico de transito puede ser tanto unicast como trafico multicast. El tráfico de tránsito Unicast entra en un puerto de ingreso y se transmite exactamente hacia un puerto de salida hacia su destino. Aunque el tráfico de tránsito Multicast también entra en el dispositivo de tránsito a través de un único puerto de entrada, que puede ser replicado y enviado a múltiples puertos de salida.

1.6 Trafico de Excepción:

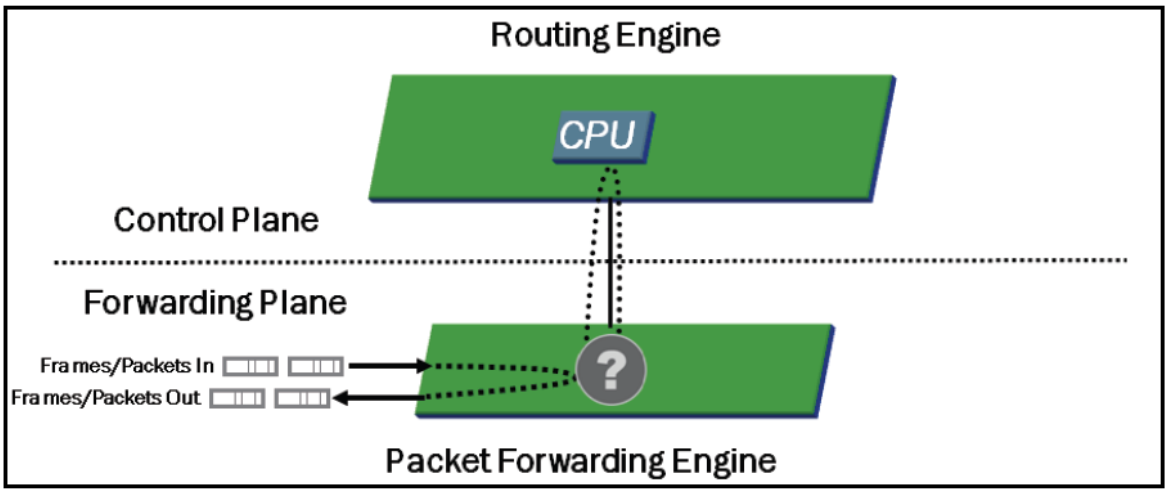


Figura 7. Trafico entrante al plano de reenvió

A diferencia del tráfico de tránsito, el tráfico de excepción no pasa a través del dispositivo local, sino que requiere algún tipo de tratamiento especial.

Ejemplos de tráfico de excepción son las siguientes:

- Los paquetes dirigidos al chasis, tales como actualizaciones de protocolos de enrutamiento, sesiones de Telnet, pings, las trazas de ruta, y las respuestas al tráfico procedente de la RE.
- Los paquetes IP con el campo de opciones IP (opciones en la cabecera IP del paquete son raramente vistos, pero la PFE fue específicamente diseñada para no manejar opciones IP; paquetes con las opciones IP deben ser enviadas a la RE para el procesamiento)
- El tráfico que requiere la generación de Protocolo de Control de Mensajes de Control de Internet (ICMP)

Los mensajes ICMP son enviados a la fuente del paquete para reportar diversas condiciones de error y para responder a las solicitudes de ping. Ejemplos de errores ICMP incluyen mensajes de destino inaccesible, que son enviados cuando no hay entradas presentes en la tabla de reenvío por la dirección destino del paquete, y tiempo de vida (TTL) expirado del mensaje, que se envía cuando un paquete de TTL se decrementa a cero. En la mayoría de los casos, el proceso de la PFE se encarga de la generación de mensajes IMCP.

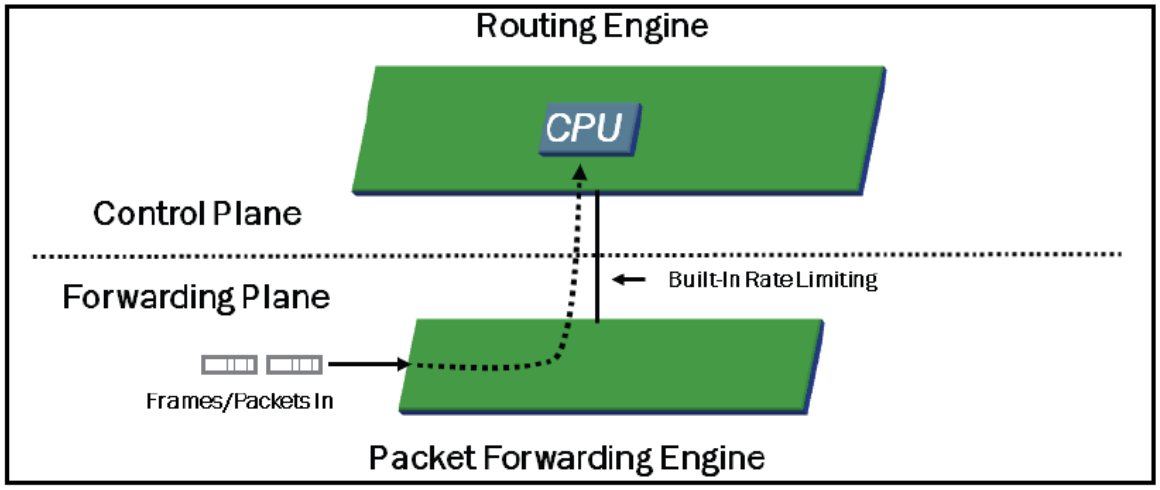


Figura 8. Trafico entre plano de control y plano de reenvió

El sistema operativo Junos envía todo el tráfico de excepción destinado a la RE sobre el enlace interno que conecta los planos de control y reenvío. El sistema operativo Junos limita el tráfico de excepción que atraviesa en enlace interno para proteger la RE de ataque de denegación de servicio (DoS). Durante el tiempo de congestión, el sistema operativo Junos da preferencia al tráfico local y de control destinado a la RE. El limitador de velocidad Built-in no es configurable.

1.7 Visión general de los dispositivos Junos

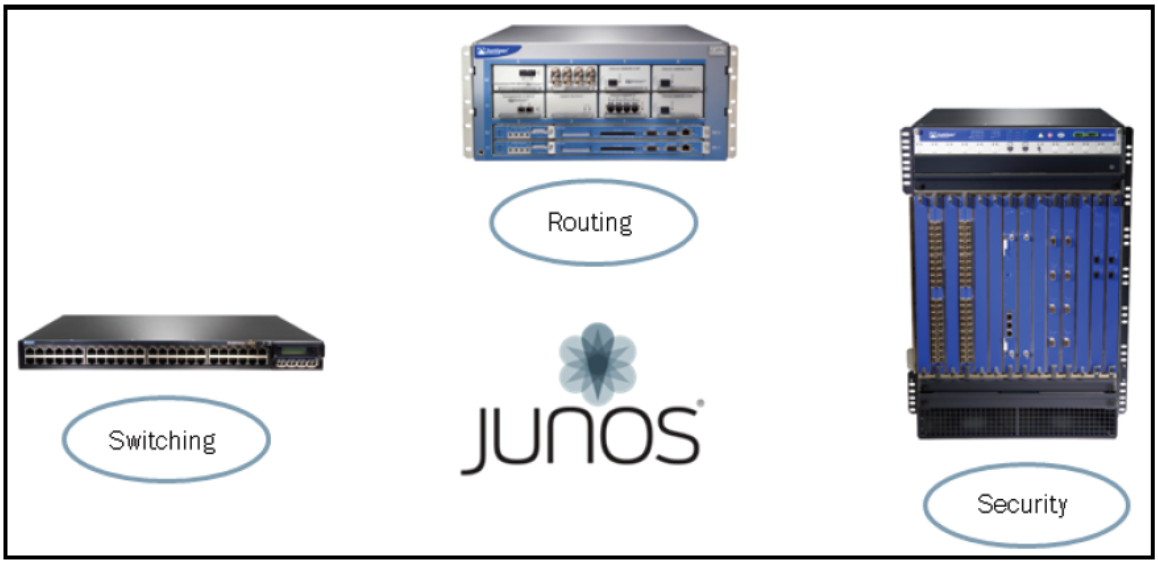


Figura 9. Dispositivos Juniper

Las plataformas que corren el sistema operativo Junos vienen en muchas formas y tamaños y son objeto de una serie de escenarios de implementación. Estas plataformas ejecutan el enrutamiento del tráfico se encargan de la seguridad y son muy adecuadas para una variedad de entorno de red. Como el corazón de todas estas plataformas, el sistema operativo Junos provee una consistente infraestructura IP end-to-end en entornos empresariales pequeños y también con los proveedores de red más grandes.

1.8 Dispositivos de Enrutamiento Junos

Figura 10. Dispositivos de enrutamiento

- Los productos de la serie ACX entregan provisionamiento de extremo a extremo de manera simplificada, con funcionalidad para trabajar en la capa 2 y capa 3 con ingeniería de trafico IP/MPLS.
- Las series LN proporcionan enrutamiento de alto rendimiento en la red, firewall y el servicio de detección de intrusos (IDS) para entornos adversos.
- Los routers multiservicio de la serie M proveen hasta 320 Gbps de rendimiento agregado en modo half-duplex. Esta familia puede se puede implementar en empresas de gama alta y entornos de proveedores de servicios. Muchas compañías utilizan este tipo de equipos para diferentes funciones como por ejemplo puerta de enlace, conectividad WAN del router, como router central del campus y como routers de backbone.

- Los routers de servicios MX Ethernet proporcionan hasta 960 Gbps de rendimiento agregado en Half-Duplex. Esta familia de equipos esta dirigía por los servicios de acceso y agregación.
- Los conmutadores de transporte de paquetes de la serie PTX proporcionan hasta 16 Tbps de procesamiento en un solo chasis. La familia PTX es ideal para servicios que fácilmente son cambiantes en el patrón de tráfico, como lo es el video, la movilidad y los servicios basados en la nube.
- Los routers de núcleo de la seria T proporcionan hasta 25.6 Tbps de procesamiento. La familia de la serie T es ideal para entornos de proveedores de servicios y se ha implantado en seno de esas redes.

2. OPCIONES DE INTERFACE DE USUARIO

2.1 Línea de comando de Junos (CLI)

La línea de comando de Junos es un Shell de comandos basada en texto. Una de las opciones para acceder a la CLI es a través de la conexión en serie del equipo, este tipo de conexión se llama por fuera de banda. La configuración del puerto de la consola está predefinida y no es configurable por el usuario.

Una segunda opción para acceder a la CLI es través de la red (en banda) utilizando protocolos de acceso tales como Telnet o SSH. A diferencia de la conexión de consola, las opciones de acceso requieren la configuración de un puerto de red y el protocolo de acceso.

2.2 Interface J-Web

La conexión J-Web es una interfaz gráfica de usuario basada en Web (GUI) que se usa mediante el uso de cualquiera de Protocolo de transferencia de hipertexto (HTTP) o HTTP a través de Secure Sockets Layer (HTTPS). Proporciona asistentes de configuración rápida para simplificar las tareas de configuración más comunes. Para configuraciones más

complicadas, la interfaz gráfica de usuario J-Web le permite editar directamente el archivo de configuración de texto del sistema. La GUI J-Web está instalada y habilitada por defecto en la mayoría de las plataformas que ejecutan el sistema operativo Junos.

2.3 Logeo en Equipo juniper

Usuarios sin privilegios de administrador son colocados automáticamente en la CLI

```
router (ttyu0)

login: user
Password:

--- JUNOS 12.1R1.9 built 2012-03-24 12:12:49 UTC
user@router>
```

Figura 11. Usuario juniper

El usuario root debe de iniciar la CLI desde la Shell del equipo junos.

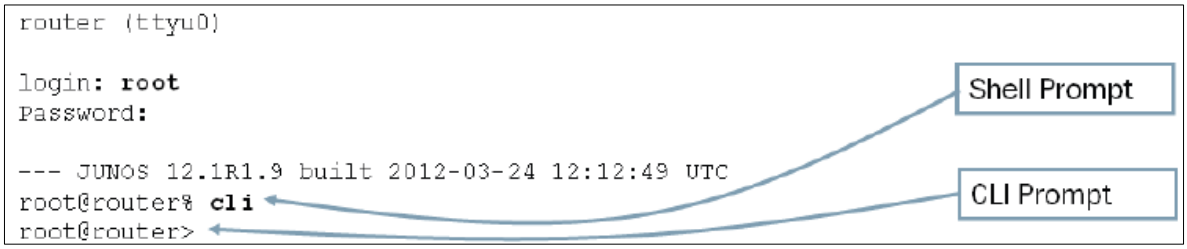


Figura 12. Usuario root

El sistema operativo Junos requiere un nombre de usuario y una contraseña para el acceso. El administrador crea cuentas de usuario y asigna permisos. Todas las plataformas que ejecutan el sistema operativo Junos tienen sólo el usuario root configurado por defecto, sin ningún tipo de contraseña.

Cuando se configura, la consola de inicio de sesión se muestra el nombre de host del dispositivo. Si no se ha configurado un nombre de host, como es el caso de una

configuración predeterminada de fábrica, el software muestra Amnesiac en lugar del nombre de host:

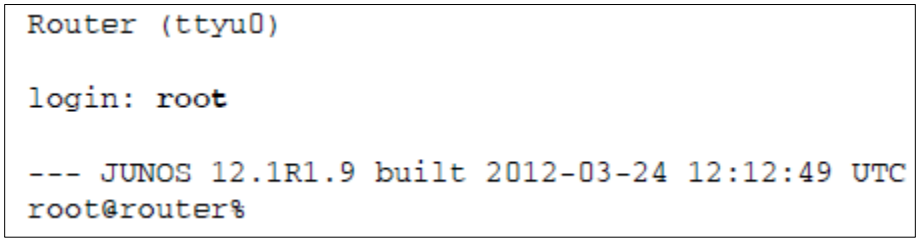


Figura 13. Amnesiac root

El usuario root tiene acceso completo y control del dispositivo. Cuando se inicia una sesión como usuario root, el software ingresa en el shell de UNIX. Debe iniciar ingresar a la línea de comando mediante el comando CLI. Para salir tanto de la Shell en el que opera el comando root y de la línea de comandos como tal, ingresar la palabra exit ya que garantiza más seguridad

2.3.1 Modo operación

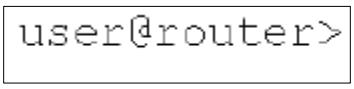


Figura 14. Símbolo de modo operacional

El carácter “ > ” identifica este modo de trabajo. Este modo de operación, se utiliza la CLI para supervisar y solucionar problemas del dispositivo. Los comandos del monitor, ping, show, test y traceroute nos permiten mostrar la información y la conectividad del dispositivo.

2.3.2 Modo Configuración

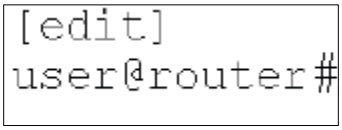


Figura 15. Símbolo modo configuración

El carácter " # " identifica este modo de trabajo. En el modo de configuración, se pueden configurar todas las propiedades del sistema operativo Junos, incluyendo interfaces, protocolos y acceso de los usuarios, así como varias propiedades de hardware del sistema.

2.3.3 Opción Help en Junos

```
user@router> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  help                 Provide help information
  . . .

user@router> clear ?
Possible completions:
  amt                  Show AMT Protocol information
  arp                  Clear address resolution information
  auto-configuration   Clear auto-configuration action
  bfd                  Clear Bidirectional Forwarding Detection information
  . . .
```

Figura 16. Opción ayuda

La CLI proporciona ayuda contextual en cualquier punto en una línea de comandos. Ayudarle a que las opciones son aceptables en el punto actual en el comando le indica y proporciona una breve descripción de cada opción de comando o comandos.

Para obtener ayuda de algún comando en el equipo, únicamente escribir el signo de interrogación (?). No es necesario pulsar Enter. Si se escribe el signo de interrogación en el indicador de línea de comandos, la CLI muestra los comandos y las opciones disponibles, incluyendo las variables definidas por el usuario en el contexto apropiado. Si se escribe el

signo de interrogación después de introducir el nombre completo de un comando o una opción, la CLI muestra los comandos y las opciones disponibles y luego vuelve a mostrar el nombre del comando y las opciones que escribió. Si se escribe el signo de interrogación en medio de un nombre de comando, la CLI enumera posibles terminaciones de comandos que coinciden con las letras que ha introducido hasta el momento y luego vuelve a mostrar las letras que escribió.

2.3.4 Ayuda con conceptos generales

```
user@router> help topic interfaces ?
Possible completions:
  accept-data           Accept packets destined for virtual address
  accept-source-mac     Policers for specific source MAC addresses
  access-profile-chap   CHAP profile associated with physical interface
  accounting            Packet counting for transit traffic
  accounting-profile    Accounting profile
  acfc                  Compression of Address and Control fields in PPP header
  ...

user@router> help topic interfaces address
                        Configuring the Interface Address

   You assign an address to an interface by specifying the address when
   configuring the protocol family. For the inet family, configure the
   interface's IP address. For the iso family, configure one or more
   addresses for the loopback interface. For the ccc, tcc, mpls, tnp, and
   vpls families, you never configure an address.
   ...
```

Figura 17. Extensión del comando ayuda

Se Puede utilizar el comando de ayuda (help) de varias maneras. El comando help topic se puede utilizar para desplegar información acerca de un comando específico. En el ejemplo de la gráfica anterior, vemos que la ayuda que se observa es con respecto a la configuración de dirección en una interface.

2.4 Ayuda con la estructura en la configuración de comando en Junos

```
user@router> help reference interfaces address
address

 Syntax

     address address {
         arp ip-address (mac | multicast-mac) mac-address <publish>;
         broadcast address;
        ...
  Hierarchy Level

     [edit interfaces interface-name unit logical-unit-number family family],
     [edit logical-routers logical-router-name interfaces interface-name unit
     logical-unit-number family family]

...
```

Figura18. Comando help reference interfaces address

El comando help reference muestra información resumida para la declaración de la configuración de referencia. En el ejemplo de la gráfica, una vez más, estamos buscando ayuda para la posible configuración de la interfaz. Este comando también muestra una lista completa de las opciones de configuración, junto con varios otros detalles específicos de la declaración de comandos a la que se hace referencia.

Además de los comandos help topic y help reference, el sistema operativo Junos también ofrece

El comando help apropos, este comando muestra los contextos que hacen referencia a una variable especifica (típicamente comandos set). A continuación se muestra un ejemplo de este comando:

```
[edit system archival configuration]
user@router# help apropos archive
set archive-sites
    List of archive destinations
set archive-sites <url> password <password>
    Password for login into the archive site
```

Figura 19. Ejemplo de comando help

En la figura anterior se muestra que el comando help apropos únicamente despliega los contextos que son relevantes con respecto al nivel jerárquico que se encuentra posicionado el usuario.

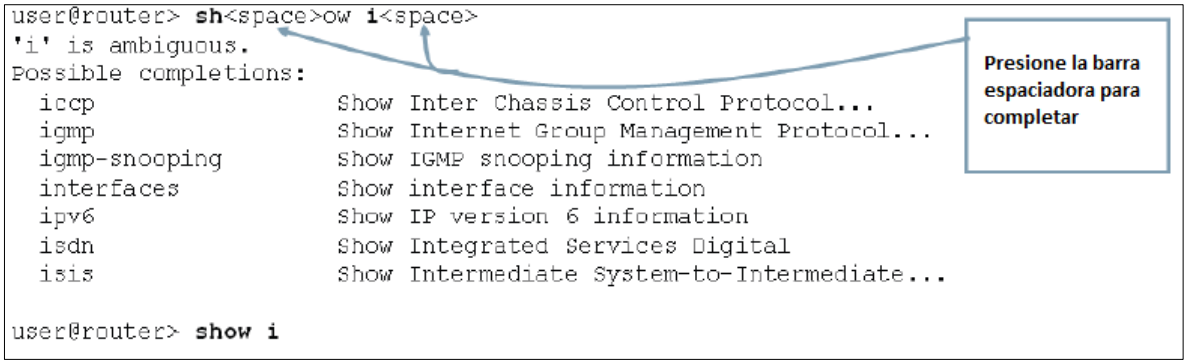


Figura 20. Completación de comandos

La CLI proporciona una función de completado. Por lo tanto, no está siempre estamos obligados a escribir el comando completo o el nombre de la opción de comandos de la CLI para reconocerlo.

Para completar un comando u opción que se ha escrito parcialmente, se pulsa la barra espaciadora. Si las letras mecanografiadas parcialmente comienzan una cadena que identifica de forma exclusiva un comando, la CLI muestra el nombre de comando completo. De lo contrario, la CLI emite un sonido para indicar que se ha ingresado un comando incorrecto, y muestra las posibles terminaciones.

El comando para completar el texto ingresado está activado por defecto, pero se puede desactivar. Para deshabilitar el comando para completar el texto ingresado para una sesión de usuario individual, se puede utilizar el comando set cli complete-on-space off.

Ejemplo:

```
user@router> set cli complete-on-space off
Disabling complete-on-space
```

Figura 21. Deshabilitar completado sesión individual

Autocompletarían con la tecla Tab para comandos y variables

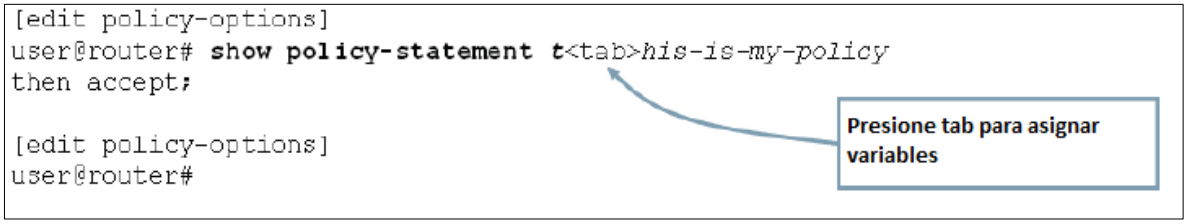


Figura 22. Tecla Tab para completar variables

Se puede utilizar la tecla Tab para completar los comandos del sistema y variables definidas por el usuario. Ejemplos de variables incluyen nombres de políticas, como las rutas, nombres de la comunidad, y las direcciones IP. La tecla Tab también ofrece una lista de terminaciones posibles en caso existan varias opciones incorrectas. La completación de comandos permite ahorrar tiempo al reducir la escritura completa del comando y evita errores al escribir el comando.

2.5 Secuencia de teclas CRTL

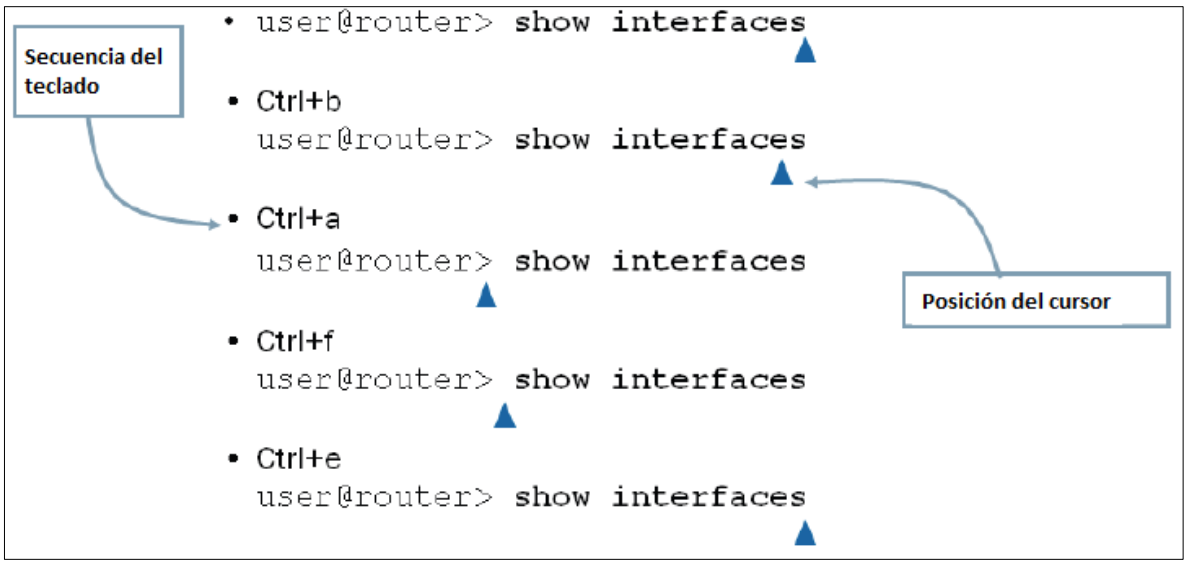


Figura 23. Secuencia de teclas CRTL

La línea de comandos soporta secuencias de teclas que permiten mover el cursor sobre una línea de comando y borrar caracteres o palabras específicas. Las siguientes secuencias son soportadas por Junos:

Ctrl+b: Mueve el cursor un carácter hacia la izquierda;

Ctrl+a: Mueve el cursor hacia el inicio de la línea de comando;

Ctrl+f: Mueve el cursor un carácter hacia la derecha;

Ctrl+e: Mueve el cursor hacia el final de la línea de comando;

Ctrl+d: Elimina el carácter sobre el cursor;

Ctrl+k: Elimina desde los caracteres desde el cursor hacia el final de la línea;

Ctrl+u: Elimina todos los caracteres;

Ctrl+w: Elimina una palabra completa a la izquierda del cursor;

Ctrl+l: Reescribe la línea actual;

Ctrl+p, Ctrl+n: Repite el comando previo según el historial de comandos;

Esc+d: Elimina una palabra hacia la derecha del cursor;

Esc+b: Mueve el cursor una palabra hacia atrás sin eliminar;

Esc+f: Mueve el cursor una palabra hacia adelante sin eliminar;

Hay que tener en cuenta que cuando se utiliza la tecla Esc, debe soltar la tecla y volver a pulsar para cada caso. Esta acción se diferencia de la tecla Ctrl, que puede mantener pulsado para múltiples ocurrencias.

2.6 Terminal tipo VT100

El sistema operativo Junos utiliza por defecto una terminal de tipo VT100. Este tipo de terminal habilita el uso de las flechas del teclado sin ninguna sesión o modificación en la configuración.

Uso del carácter Pipe "|"

```
user@router> show route | ?
Possible completions:
  count                Count occurrences
  display              Show additional kinds of information
  except               Show only text that does not match a pattern
  find                 Search for first occurrence of pattern
  hold                 Hold text without exiting the --More-- prompt
  last                 Display end of output only
  match                Show only text that matches a pattern
  no-more              Don't paginate output
  request              Make system-level requests
  resolve              Resolve IP addresses
  save                 Save output text to file
  trim                 Trim specified number of columns from start of line
```

Figura 24. Uso del carácter pipe

Para los comandos de operación y configuración la salida desplegada, tal como las mostradas por el commando show, puede ser filtrada. Cuando se visualiza la ayuda de estos comandos, una de las opciones que aparecen es |, llamada pipe, que permite que la salida del comando pueda ser filtrada.

Para filtrar la salida de un comando en modo operación o configuración, se agrega el signo pipe y una opción al final del comando. A continuación se muestran algunas opciones:

compare (***filename*** | **rollback** ***n***): Disponible en el modo de configuración usando solamente el comando show. Compara los cambios de configuración con otro archivo de configuración.

Count: muestra el número de líneas en la salida.

Display commit-scripts: Muestra los datos después de que el sistema operativo Junos aplica los cambios al script.

Display detail: Muestra información adicional sobre el contenido de la configuración.

Display set: muestra los comando set que crearon la configuración

Find *regular-expression*: muestra la salida a partir de la primera ocurrencia del texto haciendo match con la expresión regular. Si la expresión regular contiene espacios, operadores o caracteres se debe de encerrar entre comillas.

Hold: Mantiene el texto sin salir – (more) – prompt

Last: Muestra la última pantalla de información

Match *regular-expression*: Busca texto que coincide con una expresión regular. Si la expresión regular contiene espacios, operadores o caracteres comodín, se deben encerrar entre comillas.

no-more: Visualiza la salida de una sola vez en lugar de una pantalla a la vez.

Request message: muestra la información de la pantalla a varios usuarios

Resolve: convierte las direcciones IP de sistema en nombre de dominio (DNS)

Save *filename*: Guarda la salida a un archivo o URL

Se puede configurar en cascada múltiples instancias de la funcionalidad pipe en la línea de comandos, que puede ser muy beneficioso cuando se debe buscar amplias salidas que aparecen a través de la línea de comandos para obtener una información específica.

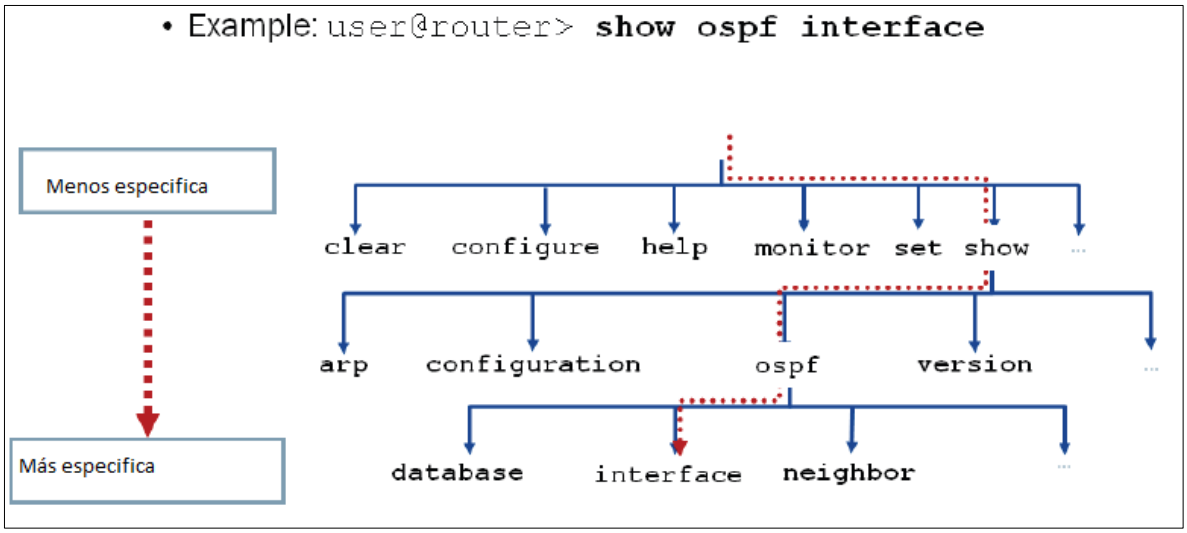


Figura 25. Nivel de estructura dentro de un comando

Se puede utilizar el modo operativo de la CLI para supervisar y controlar el funcionamiento de un dispositivo que ejecuta el sistema operativo Junos. Existen los comandos del modo de funcionamiento en una estructura jerárquica, como se muestra en la gráfica. Por ejemplo, el comando show muestra diferentes tipos de información sobre el sistema y su entorno. Una de las posibles opciones para el comando show es ospf, que muestra información sobre el primer protocolo de ruta libre más corta (OSPF).

El sistema operativo Junos también agrega flexibilidad a través del comando run, que permite utilizar comandos del modo operacional mientras se está en el modo configuración.

2.7 Capacidades de modo operación

Cuando se habla de capacidades de modo operación se quiere decir que tanto se puede realizar tanto el modo operacional del equipo como en el modo de configuracion.

```
user@router> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

Figura 26. Signo de ayuda “?”

Las capacidades del modo operación incluyen lo siguiente:

- Modo de configuración
- Control del entorno CLI
- Salir de la CLI

Monitoreo y resolución de problemas

Clear

Monitor

Trace

Ping

Show

Test

Traceroute

Conectar sistemas con otras redes

Copiar archivos

Reiniciar procesos de software

Realización de las operaciones a nivel de sistema

Cambios en la configuración Batch

A diferencia del software de otros proveedores, los cambios de configuración realizados en el sistema operativo Junos no entran en vigor de inmediato. Esta característica de diseño permite agrupar y aplicar varios cambios de configuración como una sola unidad.

Configuración Activa

La configuración activa es la configuración actualmente en funcionamiento en el sistema y es la configuración de la carga del sistema durante la secuencia de arranque. Este concepto es análogo al tanto de la configuración en ejecución y de la configuración de inicio en el software de otros proveedores.

Configuración candidata

La configuración candidata es una configuración temporal que posiblemente podría convertirse en la configuración activa. Cuando se configura un dispositivo que ejecuta el sistema operativo Junos, el software crea una configuración candidata y en un principio lo llena con la configuración activa en ejecución en ese dispositivo. Posteriormente, se deberá modificar la configuración candidata. Una vez satisfecho con sus modificaciones, puede

confirmar los cambios. Esta acción hace que la configuración candidata para convertirse en la configuración activa.

2.7.1 Tiempo de vida de archivo de configuración: Revisión general

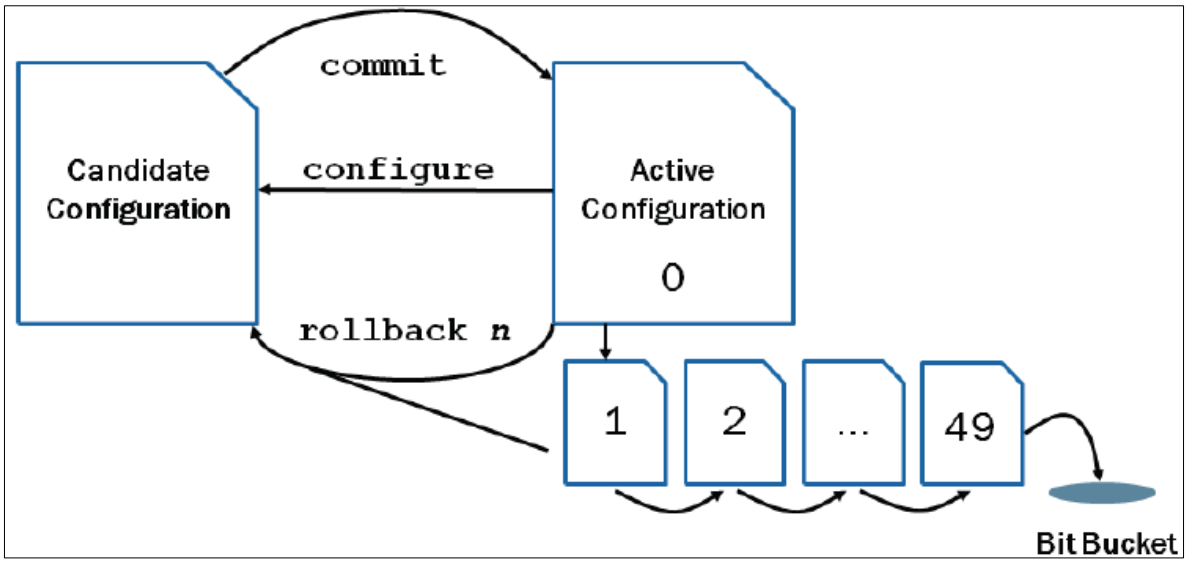


Figura 27. Tiempo de vida de un archivo

La comando “configure” permite que la configuración candidata sea creada y llenada con el contenido de la configuración activa. Usted puede modificar la configuración candidata con los cambios que desee.

Para que una configuración candidata tome efecto, se deben confirmar los cambios. Cuando esto se da el sistema operativo Junos comprueba la configuración candidata para que sintaxis se la correcta y luego se instala como la configuración activa. Si la sintaxis no es la correcta, aparecerá un mensaje de error indicando la ubicación del error, y el software no se activa en ninguna parte de la configuración. Se debe tomar en cuenta que se tienen que corregir los errores antes de confirmar los cambios de configuración una vez más.

Usted puede recuperar fácilmente las configuraciones anteriores mediante el uso del comando “rollback n”. El sistema operativo Junos mantiene un historial de configuración mediante el almacenamiento de configuraciones previamente activos. El software guarda un máximo de 50 configuraciones. Este número incluye la configuración activa actual, que también se conoce “rollback 0” y hasta 49 configuraciones previamente activas.

Si realiza una operación de rollback, hay que tener en cuenta que la configuración relacionada no se activa hasta que se ejecute el comando “commit” para guardar los cambios.

Iniciando el modo Configuración

```
user@router> configure
Entering configuration mode

[edit]
user@router#
```

Figura 28. Modo de configuración

Para ingresar al modo configuración se debe ingresar el comando “configure” desde la línea de comandos. Si, cuando ingresamos al modo de configuración y otro usuario también se encuentra en el modo de configuración, un mensaje indica qué usuario es y qué parte de la configuración, el usuario está viendo o editando.

En el modo de configuración, el prompt cambia de (>) al signo (#), precedidas por el nombre del usuario y el nombre del dispositivo.

Configuración Exclusiva

Utilizar la configuración exclusiva para aislar a otros usuarios para que no puedan editar la configuración, en este caso cualquier cambio es descartado cuando el usuario sale del equipo.

```
user@router> configure exclusive
warning: uncommitted changes will be discarded on exit
Entering configuration mode

[edit]
user@router#
```

Figura 29. Modo de configuración exclusiva

De forma predeterminada, varios usuarios pueden entrar en el modo de configuración y confirmar los cambios. Utilizar el comando "configure exclusive" para permitir que únicamente un usuario pueda editar la configuración. Los cambios no confirmados siempre se descartan con el uso del comando "configure exclusive". A diferencia, de que los cambios no confirmados son retenidos cuando se utiliza el comando estándar "configure".

Configuración privada

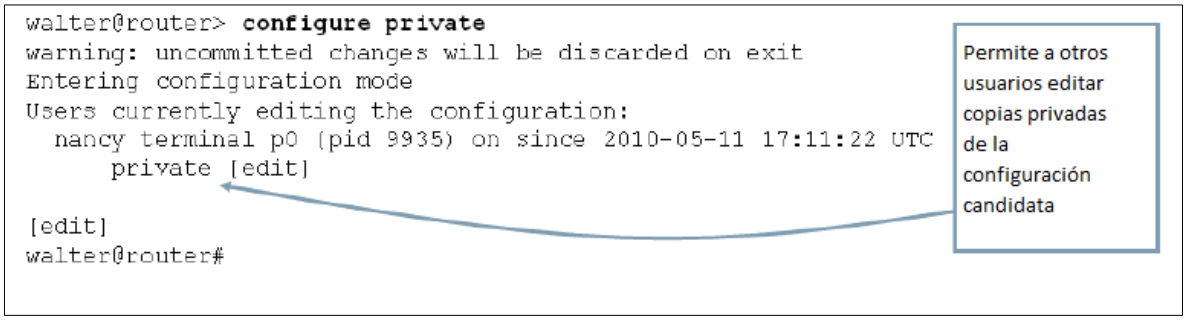


Figura 30. Modo de configuración privada

Para entrar a este modo de configuración se utiliza el comando "configure private" este permite que múltiples usuarios puedan editar la configuración mientras los cambios únicamente se confirman de forma privada. Se debe utilizar el comando "commit" desde la jerarquía adecuada. Si el usuario privado utiliza el comando rollback 0, el software descarta solo los cambios que ese usuario a realizado.

Cuando un usuario se encuentra en el modo privado, otros usuarios deben ingresar al modo privado o utilizar una configuración exclusiva para convertirse en “master” de lo contrario no podrá modificar la configuración candidata. Salirse del modo de configuración privada sin confirmar los cambios causa la perdida de cualquier modificación que se haya realizado en la configuración candidata.

Si dos usuarios están en modo privado y ambos hacen el mismo cambio (por ejemplo un usuario cambia el nombre del sistema a MANZANA mientras otro usuario configura el nombre del sistema a NARANJA). La segunda confirmación de cambios (commit) fallara con un mensaje de error para evitar conflictos en la configuración. El software coloca los cambios del segundo usuario en reserva si el usuario 2 emite un segundo mandato de confirmación.

Si un usuario está en el modo de configuración y se ha modificado la configuración candidata, otros usuarios no pueden entrar en el modo de configuración mediante las opciones “exclusive” o “privates”.

2.8 Jerarquía de declaración

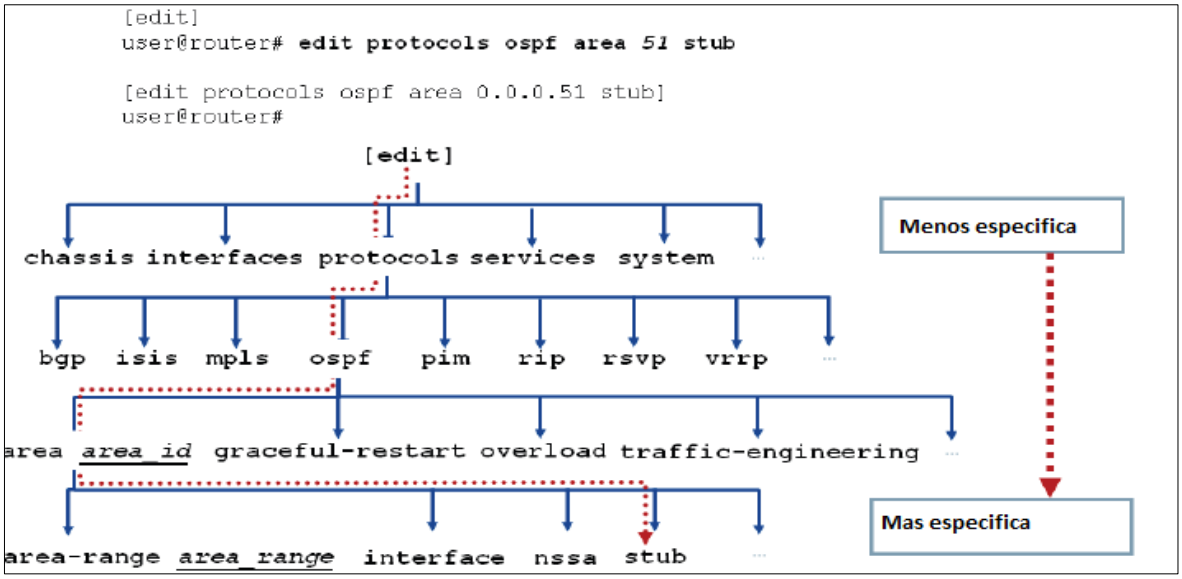


Figura 31. Jerarquía de declaración

En el modo de configuración, nosotros ingresamos los comandos que afectan el estado jerárquico. La sentencia jerárquica almacena la información de configuración y es independiente la línea de comando. Los comandos disponibles en el modo de configuración también son independientes de los comandos disponibles en el modo de operación.

Por ejemplo, en el modo operativo la CLI incluye un comando “show” para mostrar información operativa específica, mientras que el modo de configuración la CLI proporciona un comando “show” para mostrar la jerarquía de la declaración. Los dos comandos son independientes el uno del otro.

El software organiza la jerarquía declaración en una estructura de árbol similar a las carpetas de Windows o directorios UNIX, agrupando información relacionada en una determinada rama del árbol.

2.8.1 Configuración Jerárquica

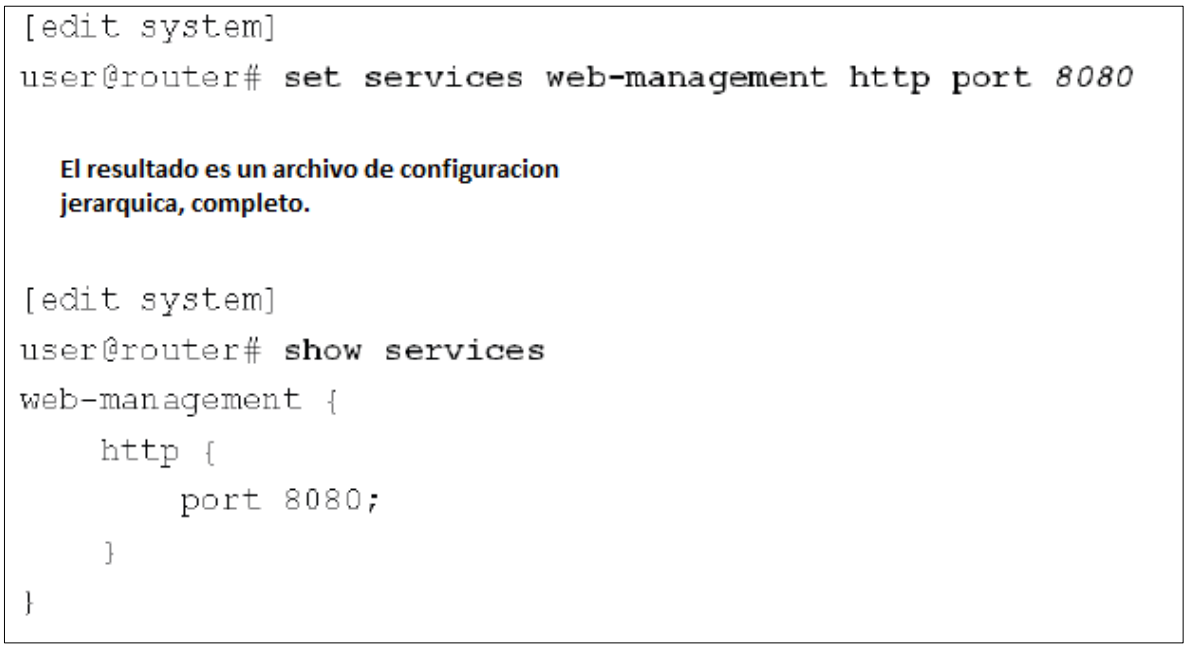


Figura 32. Resultado de una configuración jerárquica

Use el comando set en la CLI de modo de configuración para modificar la configuración candidata. Use el comando "show" para desplegar la configuración candidata. Ambos comandos son en relación a la jerarquía de la configuración actual, mostrada por el prompt [edit].

Los archivos de configuración utilizan llave ({ }) y sangría para mostrar visualmente la estructura jerárquica de la configuración. La terminación de declaraciones en la configuración se muestran con un punto y coma final (;).

2.8.2 Desplazamiento entre niveles, equivalente al cambio de directorios

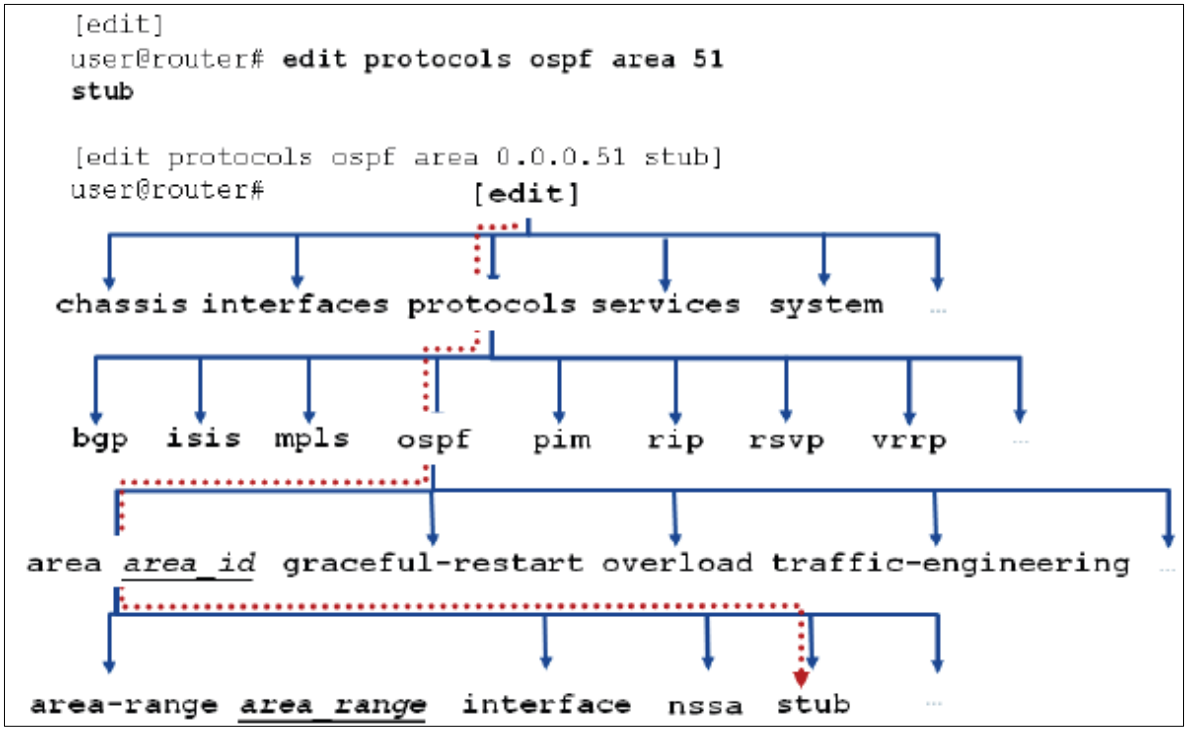


Figura 33. Desplazamiento entre niveles

Para desplazarse hacia abajo a través de una jerarquía de declaración configuración existente o para crear una jerarquía y bajar a ese nivel, se debe utilizar el comando "edit".

2.8.3 Movimiento un nivel hacia arriba en las diferentes jerarquías

Para subir un nivel desde la posición actual en la jerarquía, utilice el comando “up”.

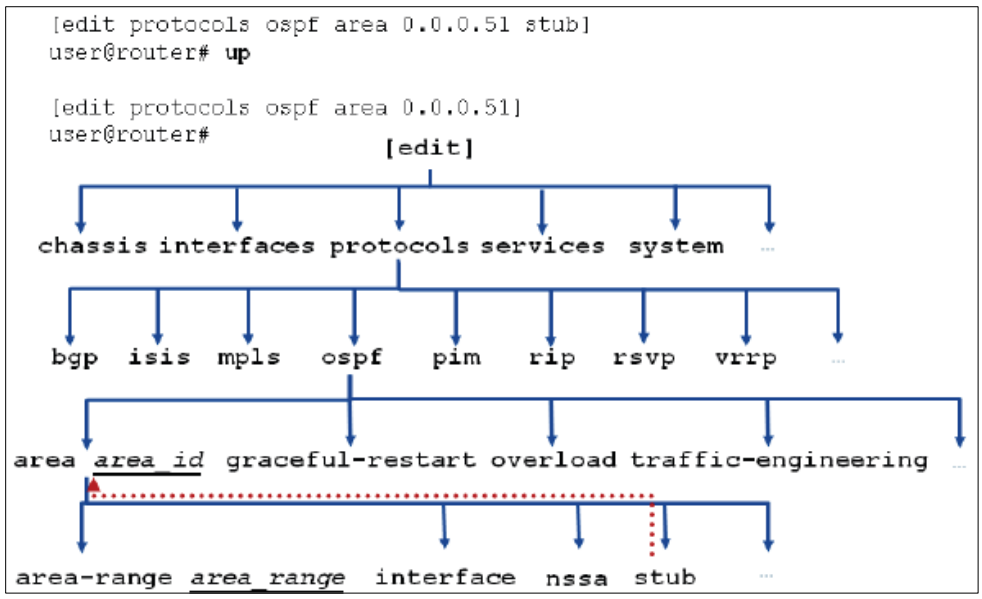


Figura 34. A. Comando up, (subir de nivel dentro de la jerarquía de la CLI)

2.8.4 Moverse hacia arriba más de un nivel

Para mover más de un nivel desde una posición en la jerarquía, es necesario indicar un número opcional que especifica la cantidad de niveles a subir. El software mueve hacia arriba el número de niveles especificados.

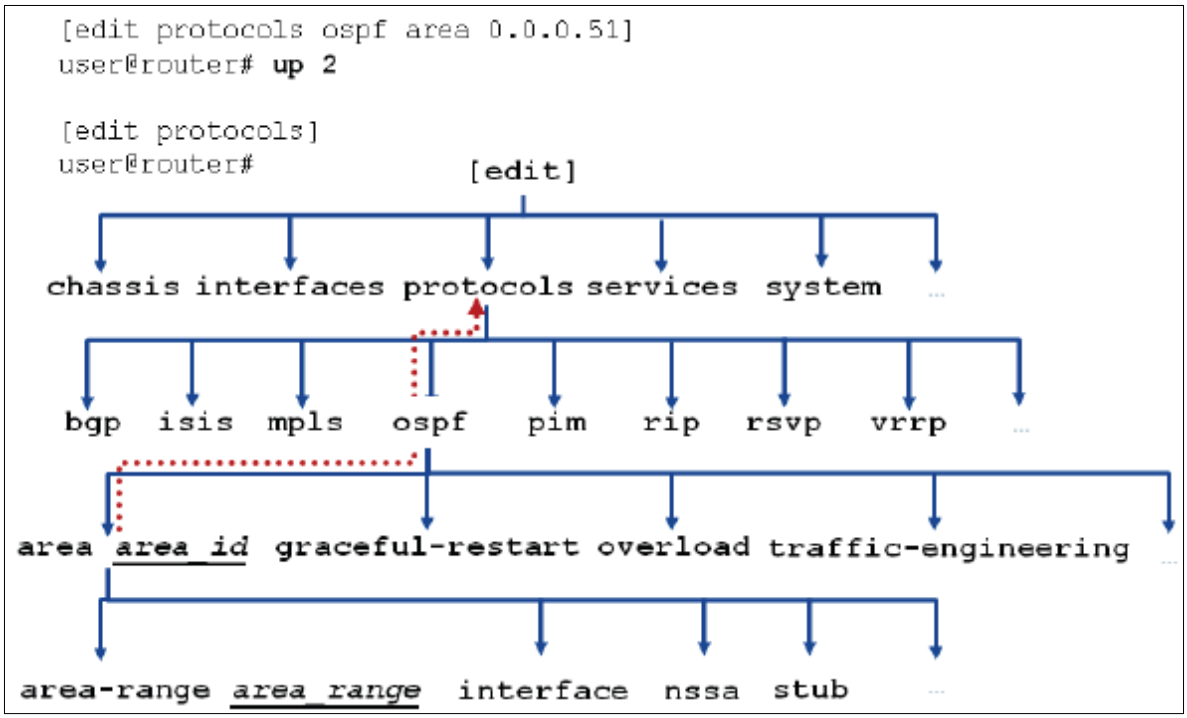


Figura 34. B. Comando up, (subir de nivel dentro de la jerarquía de la CLI)

2.8.5 Moverse hacia el primer nivel de la jerarquía

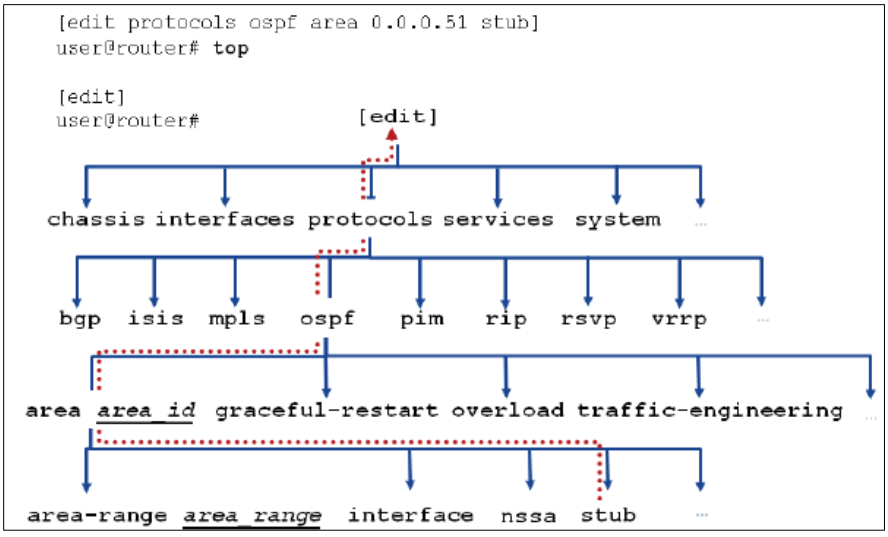


Figura 35. Comando top

El comando “top” mueve rápidamente hacia el primer nivel de la configuración jerárquica. Se pueden combinar los comandos “top”con “edit” para moverse rápidamente entre las diferentes jerarquías o también con el comando “show” para desplegar detalles de la configuración en las diferentes jerarquías, como se aprecia en el siguiente ejemplo:

```
[edit protocols ospf area 0.0.0.0 interface ge-0/0/0.0]
user@router# top edit system login

[edit system login]
user@router# top show system services
ftp;
ssh;
```

Figura 36. Comando “top” en convinacion con el comando “show”

2.8.6 Regresar al punto anterior

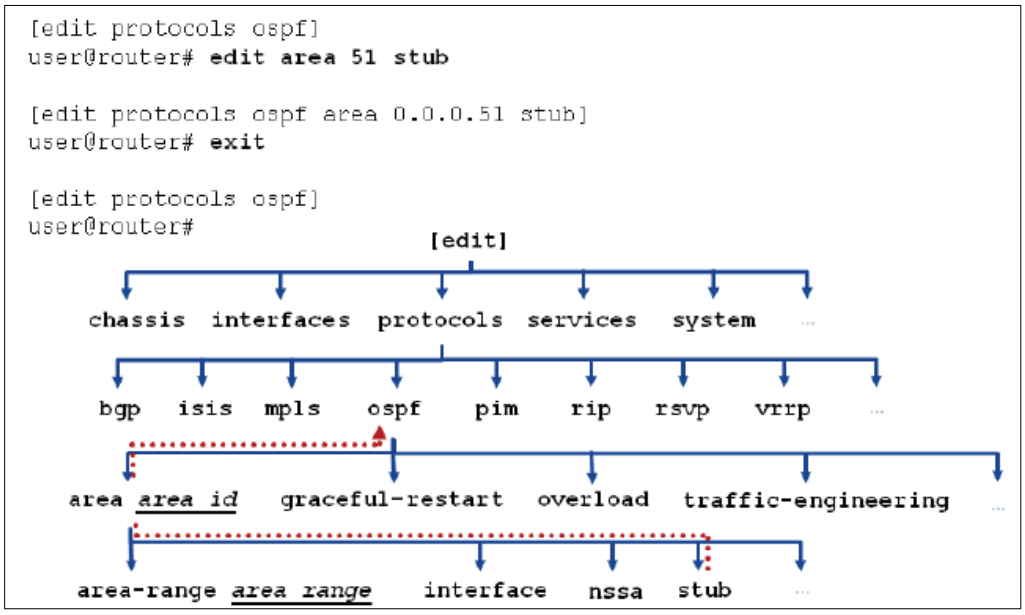


Figura 37. Regresar un nivel anterior con comando “exit”

Como se observa en la figura anterior, el comando “exit” regresa al usuario más reciente al nivel más alto en la jerarquía. Al momento de ingresar el comando “exit” en el nivel superior de la jerarquía automáticamente se sale del modo de configuración, por ejemplo:

```
[edit]
user@router# exit
Exiting configuration mode

user@router>
```

Figura 38. Salir del modo operacional

Ingresando el comando “exit configuration-mode” desde cualquier nivel de la jerarquía, permite que el usuario salga del modo de configuracion, por ejemplo:

```
[edit protocols ospf area 0.0.0.0 interface ge-0/0/0.0]
user@router# exit configuration-mode
Exiting configuration mode

user@router>
```

Figura 38. Comando “exit configuration-mode”

Agregando otras configuración

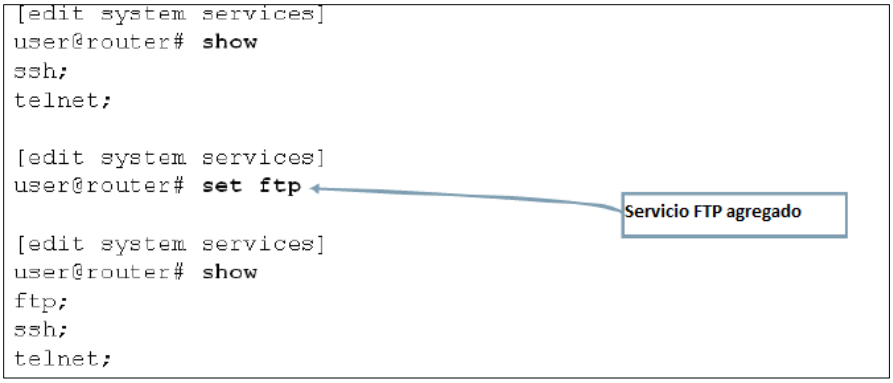


Figura 39. Comando “set”

Se debe utilizar el comando “set” en el modo de configuración CLI para modificar la configuración candidata.

Remover estados de configuración

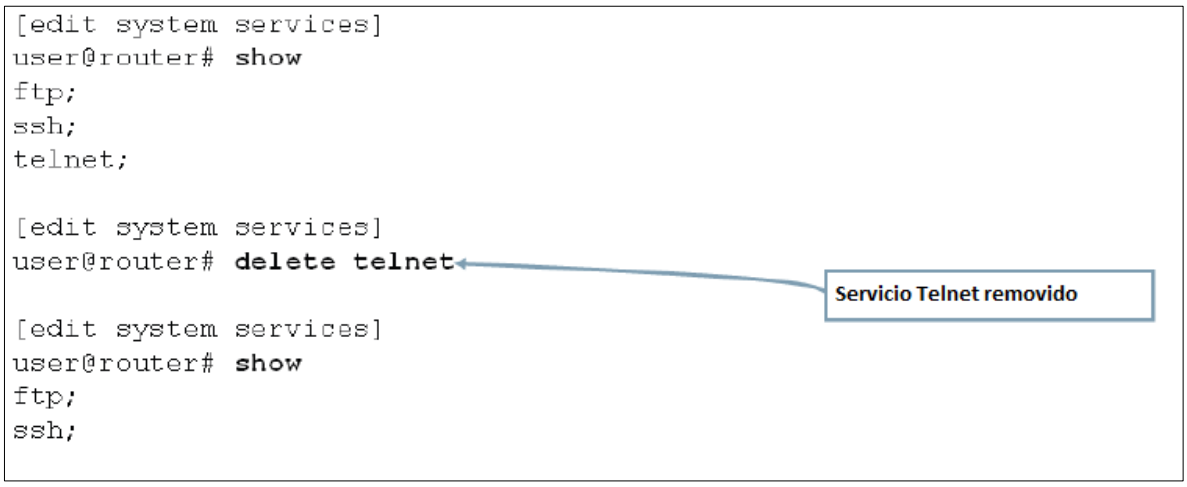


Figura 40. Comando “delete”

Se debe utilizar el comando “delete” desde el modo de configuración para eliminar los estados que previamente fueron agregados a la configuración con el comando “set”. Este comando la declaración y todos los subestados y sus identificadores. Al eliminar una declaración o un identificador se desconfigura de manera efectiva la funcionalidad asociada con esa declaración o identificador, volviendo esa funcionalidad a su condición predeterminada.

Considerar el uso de la función “wildcard delete” cuando la eliminación de estados individuales es demasiado ardua y la eliminación de una configuración sub-jerárquica carece de la granularidad que se necesita. El siguiente ejemplo muestra un ejemplo para eliminar un comodín:

```
[edit]
user@router# wildcard delete interfaces ge-1/*
  matched: ge-1/0/0
  matched: ge-1/0/1
Delete 2 objects? [yes,no] (no) yes

[edit]
user@router#
```

Figura 41. Eliminando wildcard

Además de eliminar las declaraciones de configuración, también se debe considerar el uso del comando de desactivación para hacer que la parte especificada de la jerarquía de configuración a ser ignorado al tiempo que conserva la configuración original. Emitir una activación mandar a colocar la configuración nuevamente en vigencia. Proporcionamos un ejemplo de la desactivación y activar comandos en una página posterior.

Verificación de la sintaxis en la configuración

Cuando se confirma o se guarda la configuración candidata, el software activa la configuración completa en su forma actual. Se debe utilizar el comando “commit check” para validar la sintaxis de la configuración candidata sin llegarla a poner en marcha.

```
[edit]
user@router# commit check
[edit interfaces ge-0/0/10 unit 0]
  'family'
    When ethernet-switching family is configured on an interface, no
other family type can be configured on the same interface.
error: configuration check-out failed
```

Figura 42. Uso del comando “commit check”

Evitar riego en una configuración remota

```
[edit]
user@router# commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless
confirmed
commit complete
```

Figura 43. Uso del comando “commit confirmed”

Por supuesto el comando “commit check” no puede localizar errores lógicos en la configuración. ¿Qué ocurre cuando está configurando un dispositivo de forma remota y comete un error que deja ese dispositivo inaccesible para conexiones remotas? Este escenario puede ser resuelto utilizando el comando “commit confirmed”. Cuando se utiliza el comando “commit confirmed time-out” el sistema inicia un tiempo, durante el cual se espera que se confirme el guardado de los datos en este caso será necesario ingresar el comando “commit”. Si este “commit” no ocurre durante el tiempo establecido el sistema hará un rollback 1, es decir regresara la configuración del equipo al estado anterior.

Vida de una archivo de configuración

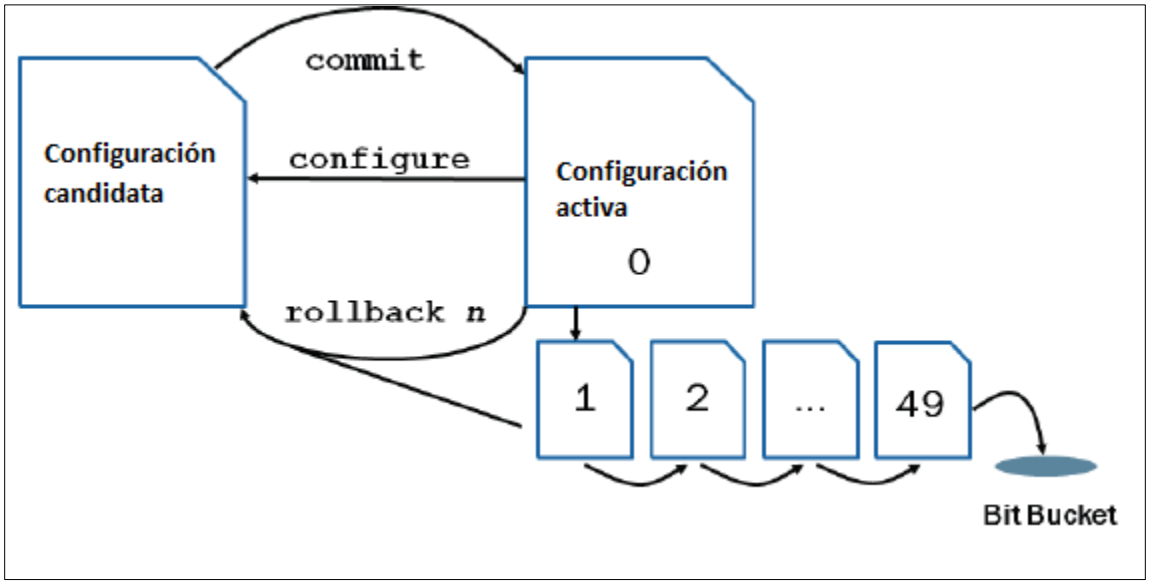


Figura 44. Archivos de configuración

3. Configuración Inicial de un Equipo Juniper

Todas las plataformas que ejecutan el sistema operativo Junos tienen una configuración predeterminada de fábrica. Todas las configuraciones por defecto de fábrica permiten el acceso utilizando la cuenta de root. La cuenta de root no incluye una contraseña por defecto. Por lo tanto se requiere establecer una contraseña root antes de realizar cualquier cambio en el archivo de configuración.

Todas las configuraciones por defecto de fábrica también incluyen un registro de las actividades en el sistema, que permite rastrear los eventos del sistema y escribe los eventos a los archivos de registro predefinidos. El siguiente es un ejemplo de una configuración syslog típico encontrado dentro de una configuración predeterminada de fábrica:

```
[edit]
user@router# show system syslog
user * {
any emergency;
}
file messages {
any any;
authorization info;
}
file interactive-commands {
interactive-commands any;
}
```

Las configuraciones de fábrica por defecto pueden variar de una plataforma a otra familia o incluso entre los diferentes modelos dentro de la misma familia de plataformas.

Todas las plataformas que ejecutan el sistema operativo Junos están diseñadas para funciones específicas dentro de un entorno de red y su configuraciones por defecto se crean con roles específicos. Un ejemplo son los switches de la serie EX, que están diseñados para funcionar como conmutadores de capa 2 según el modelo OSI.

Otras plataformas no tienen las mismas necesidades de funcionamiento por defecto y por lo tanto no incluyen los parámetros de configuración en sus configuraciones de fábrica.

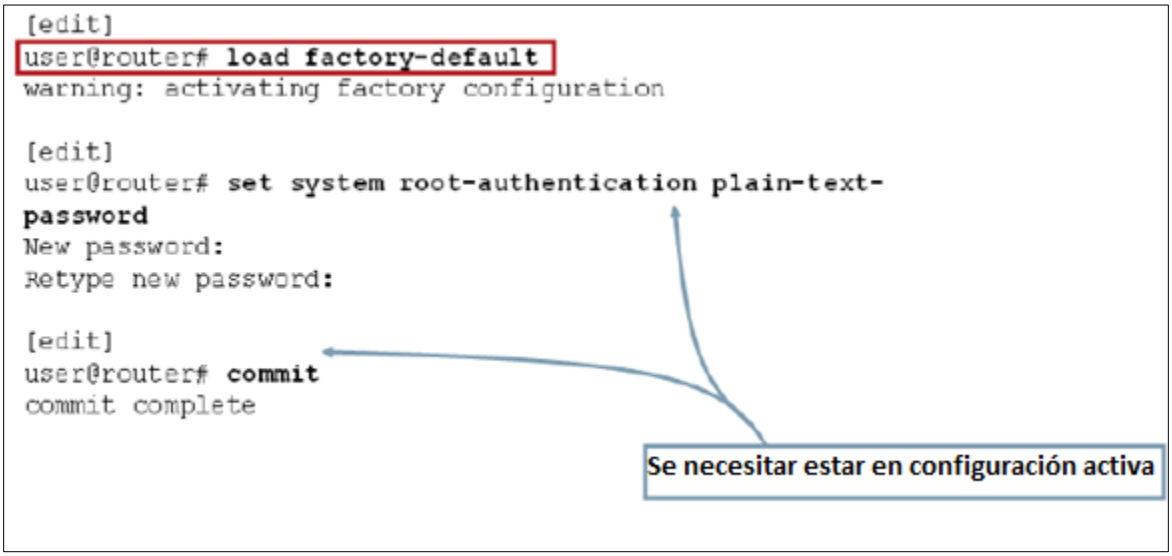


Figura 45. Comando “load factory-default”

Bajo ciertas condiciones, es posible que desee devolver un dispositivo que ejecuta el sistema operativo Junos a su configuración predeterminada de fábrica. Se puede sobrescribir la configuración candidata, estando en modo de configuración se utiliza el comando “load factory-default”. El sistema operativo Junos no permite guardar la configuración hasta que configure la información de autenticación del usuario root. Luego se debe emitir el comando “commit” guardar los cambios.

3.1.1 Poniendo en marcha un dispositivo que corre el sistema operativo Junos

Siempre se debe consultar la documentación específica de la plataforma y seguir las pautas de seguridad cuando se conecte la energía y la alimentación del dispositivo con sistema operativo Junos. Una vez que el dispositivo que ejecuta Junos OS esta encendido el equipo estará operando de forma normal pero si la fuente de poder que mantiene al equipo es interrumpida, el dispositivo encenderá automáticamente hasta que se reestablezca la alimentación. En otras palabras, no se requiere intervención manual para que el sistema se reinicie.

3.1.2 Apagar de forma ordenada el sistema operativo Junos

El sistema operativo Junos es un entorno multitarea y para garantizar la integridad del sistema de archivos, siempre se deben cerrar correctamente las plataformas que ejecuta el sistema operativo Junos. Aunque es poco probable, el no cerrar correctamente el sistema podría dejarlo incapaz de arrancar. Como se muestra en la gráfica, se debe utilizar el comando “request system halt” para cerrar correctamente el sistema operativo Junos.

Este comando proporciona opciones que permiten programar el apagado en un número determinado de minutos o en una hora exacta. Los dispositivos Junos ofrecen redundancias para las Routing Engines (REs), ambas REs pueden estar funcionando simultáneamente utilizando el comando “request halt both-routing-engines”. Si en el entorno de red hubieran Switches de la serie EX, que están participando en un chasis virtual, es decir en el escenario en que varios switches trabajan como un único dispositivo, si este fuese el caso, el comando a utilizar es “request halt all-members” para detener el proceso de todos los miembros del chasis virtual.

```
user@router> request system halt ?
Possible completions:
  <[Enter]>            Execute this command
  at                   Time at which to perform the operation
  in                   Number of minutes to delay before operation
  media                Boot media for next boot
  message              Message to display to all users
  |                    Pipe through a command
```

Figura 46. Activar redundancia de la Routing Engine

Comprobando la configuración inicial de un dispositivo Junos

```
[edit]
user@router# set system root-authentication plain-text-password
New password: ***
error: minimum password length is 6
error: require change of case, digits or punctuation
```

Figura 47. Password usuario root

Cuando se obtiene un dispositivo ejecutando el sistema operativo Junos de fábrica, el sistema operativo ya ha sido preinstalado. Una vez el dispositivo sea encendido, estará listo para ser configurado. Cuando configura por primera vez, la autenticación del usuario root debe ser incluida de lo contrario no se podrá avanzar. Además de configurar esta autenticación se debe tomar en cuenta lo siguiente:

Configurar el nombre del equipo (Hostname)

Configurar el tiempo del sistema (System time)

Configurar los servicios de acceso remoto (Telnet, SSH)

Configurar la interface de gestión y ruta estática para el tráfico administrativo

El sistema operativo Junos hace cumplir restricciones de contraseña. Todas las contraseñas están obligadas a ser no menos de seis caracteres y debe incluir dígitos y signos puntuación.

3.1.3 Inicio de sesión como usuario root

Cuando se configura por primera vez una plataforma que ejecuta el sistema operativo Junos , la contraseña de root no está establecida. Para iniciar sesión en la línea de comandos (CLI) por primera vez se debe acceder a través del puerto de consola utilizando el nombre de usuario “root” sin contraseña ya que los equipos no la traen por defecto. Se debe tomar en cuenta que cuando no se configura el nombre de host como lo es el caso de una configuración predeterminada de fábrica, lo que se muestra en lugar del nombre es lo que se conoce como Amnesiac.

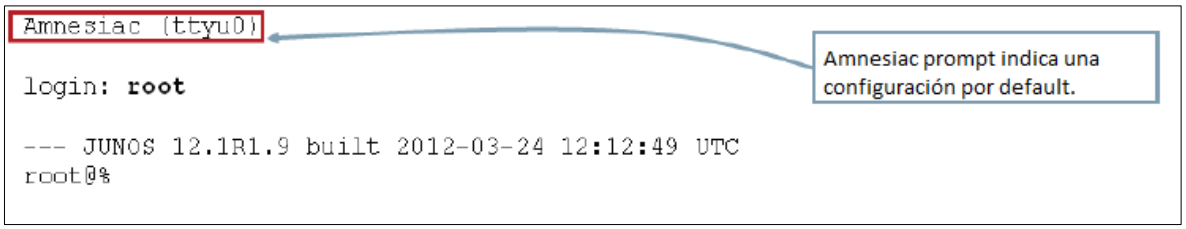


Figura 48. Amnesiac root

Inicio a la línea de comando

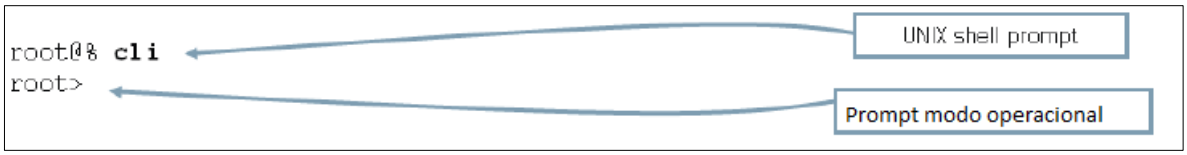


Figura 49. Unix Shell prompt

Luego de ingresar el usuario root y presionar la tecla enter, el usuario es colocado en la Shell UNIX. Luego de esto se debe ingresar el comando “cli”. Tal y como se muestra en la figura anterior. Cuando se sale de la línea de comando, se regresa a la Shell UNIX (root@%). Por razones de seguridad, se debe de teclear el comando “exit” para finalizar sesión en el equipo.

3.1.4 Iniciando en el modo de configuración

Después de iniciar la CLI, la sesión se encuentra en la jerarquía de modo operativo. Usted puede hacer cambios en la configuración únicamente estando en el modo configuración que se representa por el símbolo "#". Para ingresar al modo de configuración se debe ingresar el comando "configure" desde el modo operación, tal y como se muestra en la figura anterior.

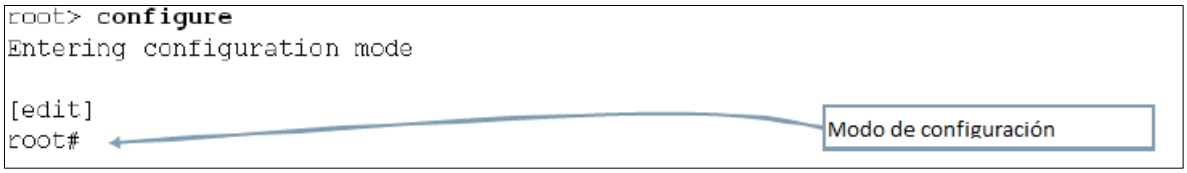


Figura 50. Signo "#" (modo de configuración)

3.1.5 Activando la configuración

Una vez que haya completado la configuración inicial, utilice el comando "commit" para aplicar los cambios. Puede incluir la opción "and-quit"como se muestra en la figura, para volver al modo operacional. En el ejemplo que muestra la gráfica, vemos que una vez que los cambios de configuración son activados y el usuario regresa al modo operacional, se muestra el nombre del host configurado. Si este cambio aparece es porque los cambios se hicieron de manera exitosa

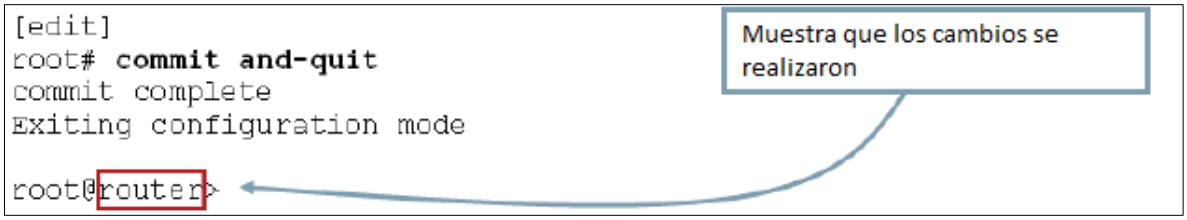


Figura 51. Comando commit and-quit

B. RESULTADO No.2

DISEÑO DEL CONTENIDO PROGRAMÁTICO CONSIDERANDO LOS SIGUIENTE TEMAS

Fundamentos del sistema operativo Junos:

Se refiere a la arquitectura típica del software JunOS. También abarca los componentes de hardware en un dispositivo Juniper como la Routing Engine y la Packet Forwarding Engine, sus funciones y que tráfico se procesa en cada uno de los componentes.

Opciones de la interface de usuario:

Aquí se discuten opciones comunes de las interfaces de usuario disponibles en plataformas que ejecutan un sistema operativo Junos, el sistema de línea de comando (CLI), sus modos y características.

Configuración inicial:

Son las tareas de configuración iniciales que se realizan en dispositivos que corren el sistema operativo Junos, los tipos de interface y la configuración básica de las interfaces además de la configuración por defecto de los dispositivos Junos.

Repaso de conceptos CCNA (Cisco Certified Network Associate):

Son términos específicos como domino de colisión, dominio de broadcast, subneteo de redes que se requieren como conocimiento básico antes de someterse a la certificación JNCIA-102.

Configuración del sistema secundario:

Se discuten los métodos de autenticación de usuario y configuración, configuración y monitoreo del equipo, operación y configuración del protocolo NTP (Network Time Protocol).

Operación de mantenimiento y monitoreo:

Recuperación de claves, mantenimiento del sistema operativo Junos y el monitoreo de la operación de las interfaces.

La interface J-web:

Interface Gráfica de Usuario (GUI) y sus funciones como configuración básica, agregar usuario etc.

Fundamentos de enrutamiento:

Protocolos de enrutamiento como RIP, EIGRP, BGP.

Filtros firewall:

Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

C. RESULTADO No. 3

LOS PASOS DEL PROCESO DE CAPACITACIÓN SE ENUMERARON CONSIDERANDO QUE EN UNA SEMANA EL PERSONAL PUDIERA ABSORBER LA INFORMACIÓN SIN NINGÚN INCONVENIENTE. EN TOTAL FUERON 5 SEMANAS ENTRE LECTURA Y PRACTICA POR SEMANA, EN LA SEMANA 6 SE CREÓ UN EXAMEN TIPO CERTIFICACIÓN.

Figura 10. Cronograma de actividades

AÑO 2014			jul-14																			ago-14						
			7	8	9	10	11	14	15	16	17	18	21	22	23	24	25	28	29	30	31	1	4	5	6	7	8	11
			L	M	Mi	J	V	L	M	Mi	J	V	L	M	Mi	J	V	L	M	Mi	J	V	L	M	Mi	J	V	L
	Fecha de Inicio	Fecha de Fin																										
Fundamentos del sistema operativo Junos	07/07/2014	11/07/2014																										
Opciones de la interface de usuario	07/07/2014	11/07/2014																										
Configuración Inicial	14/07/2014	18/07/2014																										
Repaso de Conceptos CCNA	14/07/2014	18/07/2014																										
Operación de mantenimiento y monitoreo	21/07/2014	25/07/2014																										
La interface J-Web	21/07/2014	25/07/2014																										
Fundamentos de Enrutamiento	28/07/2014	01/08/2014																										
Filtros firewall	04/08/2014	11/08/2014																										
Examen	11/08/2014																											

Fuente: Elaboración propia

D. RESULTADO No. 4

EL PROCESO DE CERTIFICACIÓN JNCIA-102 DE JUNIPER REQUIERE QUE SE ABSORBA LA SIGUIENTE INFORMACIÓN.

A continuación se detallan los temas en lo que se debe poner especial atención ya que Juniper Networks se basa en estos conocimientos para obtener la certificación.

- Se debe tener un sólido conocimiento en la Interfaz de Línea de Comandos (CLI), las tareas de configuración típicamente asociadas a la configuración inicial de los dispositivos, como por ejemplo el colocar el nombre del equipo, configuración de contraseña, configuración del usuario root etc.

- Es de suman importancia conocer el modo de navegar en la CLI y el modo de configuración en cualquier dispositivo administrado por el sistema operativo Junos, esto sería la base para poder enrolarse a esta certificación.

- Entender las jerarquías que subyacen a cada modo, es decir modo operacional y modo de configuración.

- Utilizar los métodos abreviados de teclado para acelerar su trabajo.

- Mostrar el estado del dispositivo, alarmas, y otra información útil en el modo de funcionamiento.

- Modificar, guardar y cargar archivos de configuración con un riesgo mínimo para las operaciones.

- Utilice el modo de configuración de los comandos básicos, como mostrar, establecer y eliminar.

- Encontrar información adicional acerca de estos temas de la CLI.

- Realizar las tareas dentro de los modos de funcionamiento y la configuración de la CLI.

- Realizar tareas de configuración inicial.

- Configurar y monitorizar las interfaces de red.
- Describir la configuración de usuario y opciones de autenticación.
- Ver y describir las tablas de enrutamiento y reenvío.
- Configurar y monitorizar el enrutamiento estático.
- Configurar y monitorizar OSPF.
- Escribir y aplicar filtros de servidor de seguridad

E. RESULTADO No. 5

PARA LA IMPLEMENTACIÓN DE UN TALLER DE CAPACITACIÓN SE CONSIDERARON CASOS REALES Y DE LABORATORIO LOS SIGUIENTES ESCENARIOS.

Dado la importancia de la práctica en el manejo de los equipos Juniper, y con el objetivo de que el personal pusiera en práctica los conocimientos adquiridos se crearon laboratorios virtuales utilizando el programa GNS3 (Graphical Network Simulator) ya que GNS3 es un software de alto nivel que permite emular sistemas operativos Junos reales, es decir que cualquier comando que se ingrese en los equipos que se utilizan en GNS3 es el equivalente a estar ingresando comandos a un equipo Juniper real, de hecho se pudiese configurar un equipo Juniper virtual a través de GNS3 y luego copiar automáticamente la configuración realizada hacia un equipo Juniper real.

Se consideraron casos de laboratorio a las configuraciones básicas que requiere un equipo Juniper como por ejemplo:

- Configurar y resetear el usuario root de los equipos Juniper
- Restaurar a la configuración por defecto que traen los equipos juniper de fabrica
- Configurar usuarios locales
- Configurar el nombre del equipo
- Configurar la fecha y la hora

Se consideraron casos reales las configuraciones que se hicieron a través de GNS3 pero la configuración fue literalmente copiada en equipos reales comprobando luego que su funcionamiento era el correcto, algunos de las prácticas realizadas fueron:

- Configuración básica del protocolo OSPF
- Configuración básica del protocolo RIP
- Configuración del protocolo RSTP (Rapid Spanning Tree)
- Configuración básica del protocolo BGP

VII. DISCUSIÓN DE RESULTADOS

Debido a la escases de información y de no llevar un proceso correcto y adecuado para obtener la certificación JNCIA-102, los ingeniero del departamento de Implementación y de Datos no han podido obtener esta certificación la cual es de suma importancia para beneficio de la empresa, esta es una de las razones por las cuales se lleva a cabo la realización de un manual para solventar esta situación.

A. Análisis de la problemática y la programación del contenido

Uno de los inconvenientes para desarrollar el contenido fue que la mayoría de información para esta certificación se encontraba en inglés, esto fue un inconveniente ya que si bien hoy en día todos deberíamos dominar este idioma aún existen personas que no está muy familiarizado con el inglés. Sin embargo se visitó la página de la empresa Juniper (http://www.juniper.net/us/en/training/certification /junosintro_track.page) para ver los requisitos que este solicitaba y los temas que ellos evaluaban para obtener esta certificación, luego de esto se procedió a diseñar el contenido del curso. Este fue realizado de una manera sencilla y comprensible, esto se pudo notar ya que no se recibió ninguna queja de los ingenieros con respecto a la dificultad del contenido. Por cada tema desarrollado al final se hizo una serie de preguntas estas se realizaron en el idioma ingles por el hecho que el examen para poder obtener la certificación es únicamente en inglés y no en español, esto ayudo a los ingenieros a familiarizarse con las preguntas en ingles que pudieran venir en la certificación.

B. Preguntas de examen, tipo certificación

La preguntas que se realizaron fueron hechas en base a los requisitos de la certificación y a la experiencia que se ha tenido en certificaciones anteriores, con esto se pretende que los estudiantes se familiaricen con el tipo de preguntas que pueden esperar al momento de tomar el examen, algunas de las preguntas se muestran a continuación.

- What are some advantages of the Junos OS ?
  (Cuales son las ventajas del Sistema Operativo Junos)

- What are the primary functions of the control plane and the forwarding plane on Junos devices ?
  (Cuales son las principales funciones del Plano de Control y el Plano de Reenvío en los dispositivos Junos)
- How are transit and exception traffic processed ?
  (Como es el tráfico de Transito y Excepción)
- Name three platforms that run the Junos OS.
  (Mencione tres plataformas que corren el Sistema Operativo Junos)
- List two methods for monitoring devices running the Junos OS.
  (Escriba dos métodos para monitorear dispositivos que ejecutan el Sistema Operativo Junos)
- Which command do you use to view interface usage details in real time ?
  (Cual comando utilizas para ver a detalle y en tiempo real el uso de una interface)
- Which command do you use to perform packet captures?
  (Que comando utilizas para capturar paquetes)
- Describe the upgrade procedure.
  (Describe el procedimiento de actualización)
- Which network mask is the equivalent of 255.255.248.0?
  (Cuál es la máscara de red equivalente de 255.255.248.0)
- Which login class permission will allow a user to use the telnet utility?
  (Qué nivel de privilegio se requiere para que un usuario utilice Telnet)
- Which command do you issue to upgrade the current software on Junos devices?
  (Que comando utilizas para actualizar el software actual en un dispositivo Junos)
- What is the decimal equivalent of 10101010?
  (Cuál es el equivalente en decimal de 10101010)
- Two devices on an Ethernet segment sent frames at the same time causing a collision.
  (Dos dispositivos en un segmento Ethernet que envían tramas al mismo tiempo causan una colisión)
- What is the default SNMP permission level on Junos devices?
  (Cuál es el nivel de permiso SNMP por defecto en un dispositivo Junos)
- Which two statements are true of a network mask? (Choose two.)
  (Cuales de los siguientes estados son verdaderos en una máscara de red, Elegir 2 opciones)

A. A subnet mask specifies the portion of an IP address that is in a binary format.

(Una máscara de subred especifica la porción de una dirección IP que está en formato binario)

B. A subnet mask specifies the portion of an IP address that is in a decimal format.
(Una máscara de subred especifica la porción de una dirección IP que está en formato decimal)

C. A subnet mask specifies the portion of an IP address that represents a network prefix.
(Una máscara de subred especifica la porción de una dirección IP que representa un prefijo de red)

D. A subnet mask specifies the portion of an IP address that represents network hosts.
(Una máscara de subred especifica la porción de una dirección IP que representa los Hosts de la red)

- How can you verify that you have correctly configured SSH access to your Junos device?
(Como se puede verificar que se haya configurado correctamente el acceso SSH en un dispositivo Junos)

A. user@router# show system services

B. user@router> show configuration services

C. user@router# show configuration system services

D. user@router# show system login

C. Recomendaciones para agilizar operaciones matemáticas y comandos de importancia para la certificación.

Por propia experiencia en esta certificación, se hizo énfasis a los temas que los ingenieros debían poner atención y practicarlos constantemente como lo es la división de subredes, manejo de la línea de comandos (CLI) y protocolos de enrutamiento. Las operaciones de división de redes son relativamente fáciles pero al momento de la certificación el tiempo es un factor clave que puede jugar en contra o a favor de la persona, por ello fue que se diseñó una tabla con todos los posibles valores para la división de subredes, con esto el ingeniero tuvo la oportunidad de practicar cualquier tipo de operación y que al momento de someterse al examen no tenga absolutamente ningún problema.

Tabla 1. Mascaras de red

MÁSCARAS DE RED				
Binario	Decimal	Cidr	No. hosts	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32	1	
11111111.11111111.11111111.11111110	255.255.255.254	/31	2	
11111111.11111111.11111111.11111100	255.255.255.252	/30	4	
11111111.11111111.11111111.11111000	255.255.255.248	/29	8	
11111111.11111111.11111111.11110000	255.255.255.240	/28	16	
11111111.11111111.11111111.11100000	255.255.255.224	/27	32	
11111111.11111111.11111111.11000000	255.255.255.192	/26	64	
11111111.11111111.11111111.10000000	255.255.255.128	/25	128	
11111111.11111111.11111111.00000000	255.255.255.0	/24	256	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	512	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1024	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2048	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4096	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8192	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16384	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32768	
11111111.11111111.00000000.00000000	255.255.0.0	/16	65536	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131072	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262144	
11111111.11111000.00000000.00000000	255.248.0.0	/13	524288	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048576	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097152	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194304	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388608	
11111111.00000000.00000000.00000000	255.0.0.0	/8	16777216	A
11111110.00000000.00000000.00000000	254.0.0.0	/7	33554432	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67108864	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134217728	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268435456	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536870912	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1073741824	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2147483648	
00000000.00000000.00000000.00000000	0.	/0	4294967296	

Fuente: Elaboración propia

De todos los posibles comandos que se vieron a lo largo del curso se obtuvo una lista de comandos que el ingeniero en proceso de certificación debe de tomar como importantes para poder ganar el examen.

Tabla 2. Comandos Juniper

Comando Juniper	Descripción
ping	comando para probar conectividad hacia otro equipo
traceroute	muestra los saltos o equipos por los que pasa un paquete
show system uptime	actualizar la hora
show chassis environment	muestra información como alarmas, temperatura etc. del chasis del equipo.
show cli history	muestra el historial de la línea de comandos
show log	muestra el historial de los usuarios que han accesado al equipo
show configuration	muestra la configuración candidata del equipo
show version	muestra la versión del sistema operativo
show arp	muestra la tabla de dirección IP que están asociadas a un dirección MAC
show interfaces	muestra un estado general de todas la interfaces del equipo
show interfaces detail	muestra un resumen de las características de la interface
show interfaces extensive	muestra todas las características de las interfaces
show route	muestra todas las rutas configuradas
show interfaces terse	muestras el estado de las interfaces
show policy	muestra las políticas configuradas
show route summary	muestra un resumen de todas las rutas
commit	guardar los cambios
show | compare	compara la configuración actual con una anterior
top	para regresar a la jerarquía más baja ">"
request system configuracion rescue	para solicitar una configuración guardada anteriormente
rollback	para regresar a un estado de configuración anterior
help topic interfaces ?	despliega ayuda de las interfaces
deactive interfaces	desactivar una interface
commit check	antes de guardas los cambios verificar si no hay inconsistencia
set root-authentication plain-text-password	establecer clave al usuario root
set family inet address	configurar una dirección ip
monitor interfaces traffic	monitorear el tráfico en una interface especifica
show route protocol static	mostrar las rutas estáticas
show ospf neighbor	mostrar los equipos vecinos que tiene ospf configurado

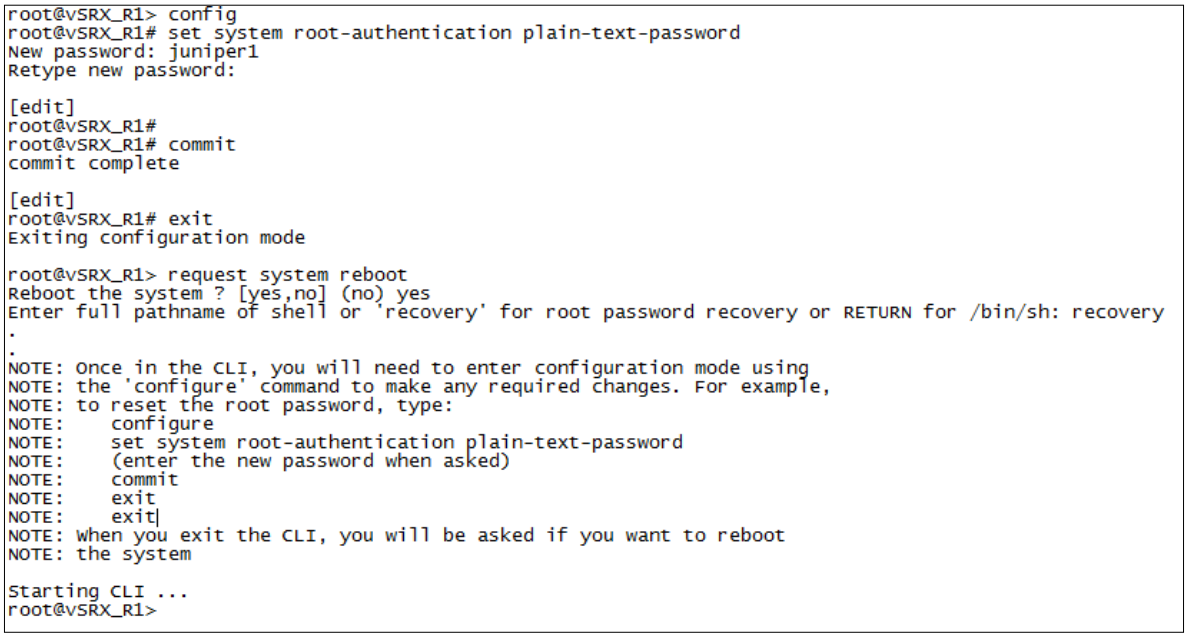
Fuente: Elaboración propia

D. Laboratorios con GNS3

Con los laboratorios realizados los ingenieros están en la capacidad practica de someterse al examen JNCIA-102, los laboratorios fueron diseñados específicamente para que los ingenieros se familiarizaran con el sistema operativo de Juniper, cabe cuando se instala el software GNS3, se tiene una capacidad ilimitada para configurar equipos ya que se pueden crear diferentes escenarios y luego implementarlos directamente en equipos juniper reales.

El primer laboratorio que se realizó y que es el primer paso que debe ser configurado en todo equipo juniper, es establecer una clave de seguridad para el usuario root o raíz del equipo, de lo contrario la seguridad de la información del equipo estaría seriamente afectada.

Figura 11. Configuración de usuario root



Fuente: Elaboración propia

VIII. CONCLUSIONES

1. Se elaboró un manual que registra el proceso de como poder obtener la certificación JNCIA-102 definido para empresas de telecomunicaciones como lo es Grupo STG, con la finalidad de preparar a sus ingenieros en esta área, sin necesidad de recurrir a costos elevados en capacitaciones.

2. Se dividió la información a impartir en el proceso de certificación de manera que los ingenieros del curso pudieran asimilar poco a poco esta información, los temas fueron seleccionados según los requisitos por parte de la empresa juniper networks, cabe mencionar que la información del curso es en el idioma español, sin embargo el examen final que se propuso se realizó completamente en inglés para ayudar a los ingenieros en asimilar el tipo de preguntas que pueda incluir el examen.

3. Se estableció que la información necesaria para la certificación debe incluir las operaciones matemáticas de la división de redes en subredes, para esto se debe de practicar hasta dominar el tema, también especial énfasis en la jerarquía de los comandos es decir, si un comando se ingresa en modo operacional o modo configuración.

4. Dentro del proceso de certificación se estableció que las personas del proceso deben enfocarse según los temas oficiales que se evalúan durante la certificación cabe mencionar la importancia de realizar prácticas de configuración utilizando uno de los programas más sofisticados hasta el momento como lo es GNS3 (Graphical Network Simulator) ya que este permite simular sistemas operativos reales de manera que la única diferencia entre lo real y lo virtual sea el equipo físico como tal, mas no el comportamiento del equipo configurado. Lo que equipo necesario para implementar un laboratorio o taller de virtualización, fue un equipo con el sistema operativo Windows 7, el software de simulación VirtualBox y el IOS de cualquier dispositivo Juniper.

IX. RECOMENDACIONES

1. El proceso de certificación tiene un validez de 2 años, por lo que en el año 2016 es muy probable que cierta información y requisitos para obtener esta certificación varíen, si este fuese el caso se debe actualizar esta información, siempre respetando el tiempo en que se imparte el curso.

2. Durante la certificación hay un tiempo límite de 90 minutos para que se pueda completar el examen y este se aprueba con un valor de 60 puntos, por lo que se debe practicar lo suficiente para poder realizar cualquier operación y/o configuración tan rápido como sea posible.

3. Es importante realizar un listado de comandos con su descripción y operación, también es importante memorizar la tabla () de subneteo ya que garantiza que cualquier operación que pueda venir en el examen de certificación se pueda realizar sin ningún contratiempo.

4. Crear distintos escenarios, con distintos equipos como por ejemplo se podría crear una topología que opere tanto con equipos Juniper como con equipos Cisco de esta manera se afianzara más el conocimiento y el personal estará aún más preparado ya que en el mundo real no solo existe ni trabaja una sola familia de equipos.

X. REFERENCIAS BIBLIOGRÁFICAS

1. Andersen, A. (1998.) Prácticas de gerencia del siglo XXI. España: Editorial La Palma

2. Barca, G. (2001) Control Estadístico de Procesos. Macgraw - Hill, tercera edición.

3. Caballero, J. (1988) Redes de banda Ancha. Barcelona, España. Editorial Marcombo.

4. Courcoubetis, C. y Weber, R. (2003). Pricing communication networks: economics, technology, and modelling. Willey

5. Fleitman, J. (2000) Negocios exitosos. Mc Graw - Hill, primera edición.

6. Lera, E. y Caballero P. (1993) Planificación de redes digitales. Colección Técnica Ahciet-Ici.

7. Oppenheimer, P. (2004) Top - down network design, Cisco Press. Segunda edición.

8. Odon, W. (2004) CCNA INTRO, Cisco Press. Séptima edición.

9. Odon, W. (2004) CCNA ICND, Cisco Press. Séptima edición.

10. Panko, R. (2004) Business data networks and telecommunications quinta edition. McGraw-Hill.

11. Stalings, W. (2000) Comunicaciones y redes de computadores. 6ta. edición. Prentice Hall.

12. Taub, H. & Schilling D. (1986.) Principles of communication systems. Segunda edición. McGraw-Hill.

13. Weber, Joseph. (2007) IPTV Crash Course. Editorial McGraw – Hill, Segunda edición.

14. Umich. (2013), Changing economic nature of network resources due to network convergence. Recuperado de http://web.si.umich.edu/tprc/papers/2004/312/KwonNam

15. Tau. (2013), Curso de redes. Recuperado de http://www.tau.org.ar/base/lara.pue.udlap.mx/redes/rede196.htm#2

16. Soricelli, Joseph M (2006). Juniper Networks Certified Internet Associate Study Guide. United States: sybex. P. 640.

17. Clarke, Sean (2011). Configuring Junos Basics. Juniper Networks Books: United States.

18. Wessles Tyler, Jacobs John y Ringwelski Jeff (2003). Targeting JNCIA . AuthorHouse: UK . P. 288.

19. Goralski Walter, Gadecki Cathy y Bushong Michael (2011). Junos for Dummies, (2a ed). For Dummies: Canada. P. 408.

20. Garret, Aviva (2006). Junos cookbook (1a ed). O'Reilly Media: United States of America. P. 684.

21. Lammle, Todd (2011). CCNA Cisco Certified Network Associate Study Guide (7a ed). Sybex: Canada. P. 864.

22. Bryant, Chris (2013). Mastering Binary Math And Subnetting . Amazon Digital Services: United States. P. 86.

23. Angelescu, Silviu (2010). CCNA Certification All-In-One For Dummies (1a ed). John Wiley & Sons: Canada. P. 1008.

24. Browning, paul (2014). Cisco CCNA in 60 Days (2a ed). Reality Press Ltd: UK. P.700.

25. M. Kozierok, Charles (2005).The TCP/IP Guide. No Starch Press: United States of America. P.1616.

26. Forouzan, Behrouz (2009). TCP/IP Protocol Suite (4a ed). MacGraw-Hill: UK. P. 928

27. George, Matthew (2012) Junos Workbook. Fecha de consulta: 17 de Julio de 2014. URL: http://www.junosworkbook.com/

28. Certification Tracks. Fecha de consulta: 17 de Julio de 2014. URL: http://www.juniper.net/us/en/training/certification/certification-tracks/

29. Grafical Network Simulator. Fecha de consulta: 17 Junio de 2014. URL http://www.gns3.net

30. Fuente: Couch II, Leon W. Sistemas de Comunicación Digitales y Analógicos. p. 107.

XI. ANEXOS

Especificaciones equipo Juniper M20

Specifications

Specification	Description		
Physical	Height	14 in / 35.56 cm	
	Width	19 in / 48.26 cm	
	Depth	21 in / 53.34 cm	
	Weight	Maximum configuration 150 lbs / 60.04 kg	
	Mounting	Front or center rack mount	
FPC	■ 3.2-Gbps throughput (full duplex) ■ I/O Manager ASIC for wire-rate parsing, prioritizing, and queuing of packets		
SSB	■ One Internet Processor or Internet Processor II ASIC for 40-Mpps packet lookup ■ Two Distributed Buffer Manager ASICs for coordinating pooled, single-stage buffering ■ PowerPC 603e processor running at 200 MHz for handling exception packets ■ 33-MHz PCI bus, which connects the PowerPC 603e processor and the Internet Processor or Internet Processor II ASIC ■ Four slots of 1-MB SSRAM ■ 64-MB DRAM ■ 512-KB boot flash EPROM (programmable on the board)		
Routing Engine	■ Compact PCI industrial form factor ■ 333-MHz Intel Pentium II ■ 80-MB flash drive for primary storage ■ 6.4-GB hard drive for secondary storage ■ 110-MB flash PC card for tertiary storage ■ 10/100 Base-T auto-sensing RJ-45 Ethernet port for out-of-band management ■ Two RS-232 (DB9 connector) asynchronous serial ports for console and remote management		
Power Requirements	DC	Maximum power	1,200 watts
		Maximum current	24 A at -48 VDC
		Input voltage	-40.5 to -72 VDC operating range
	AC	Maximum power	1,200 watts
		Maximum current	12 A at 100 VAC, 6 A at 240 VAC
		Input voltage	100 V to 240 VAC rms
Environmental	Temperature	32 to 104 degrees F / 0 to 40 degrees C	
	Maximum Altitude	No performance degradation to 10,000 ft / 3,048 m	
	Relative Humidity	5 to 90 percent noncondensing	
	Seismic / Earthquake	Designed to meet Bellcore Zone 4 earthquake requirements	
	Thermal Output	3,850 BTU/hour	

XII. GLOSARIO

Acceso remoto Es el poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora geográficamente en otro lugar, a través de una red local o externa.

Ancho de banda Cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

Autenticación Es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

ADSL Por las siglas en ingles Asymmetric Digital Subscriber Line es una tecnología de acceso a internet de banda ancha, lo que implica una velocidad superior a una conexión por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa.

ATM Tecnología de *switching* basada en unidades de datos de un tamaño fijo de 53 bytes llamadas celdas. ATM opera en modo orientado a la conexión, esto significa que cuando dos nodos desean transferir deben primero establecer un canal o conexión por medio de un protocolo de llamada o señalización.

Browser Software que permite el acceso a internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.

Byte Unidad fundamental de datos en los ordenadores personales, un byte son ocho bits contiguos.

Cifrado Procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender la estructura

	lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.
Datagrama	Fragmento de un paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes.
Firewall	Software o hardware que comprueba la información procedente de internet o de una red y, a continuación, bloquea o permite el paso de esta al equipo, en función de la configuración del firewall.
Frame Relay	Tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.
Gateway	Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. El propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.
Hacker	Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como internet por personas no ajenas al sistema.
Host	Se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.
ISP	Por las siglas en ingles internet Service Provider es una empresa que brinda conexión a internet a los clientes.

IPSec	Por las siglas en ingles Internet Protocol Security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos
Modelo OSI	Modelo que define los métodos y protocolos para lograr una comunicación entre los equipos de una red. Este método define el funcionamiento de la redes en 7 capas.
Protocolo Punto	Protocolo que opera en la capa 2 del modelo OSI proporciona conexiones entre dos equipos, estas pueden ser de Router a Router, de Host a Red.
Protocolo de Control	Conjunto de protocolos estándar de la industria que está diseñado para redes de gran tamaño compuestas por segmentos de red conectados mediante enrutadores. TCP/IP es el principal conjunto de protocolos usado en internet.
Protocolo	Designa el conjunto de reglas que rigen el intercambio de información a través de una red de ordenadores.
Protocolo Datagrama	Protocolo que permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en la cabecera.
Red privada	Es aquella red exclusiva de una sola compañía u organización ya que la información no se comparte con otras compañías.
Red publica	Es una red por la cual circula información de muchas compañías y organizaciones en consecuencia es una red poco segura pero resulta más económico. La internet es una red pública.

Router	Dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. La función principal consiste en enviar o encaminar paquetes de datos de una red a otra.
Red privada virtual (VPN)	Tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas.

Belter Molina Guevara

AUTOR

Dra. Carolina Arévalo Valdez

DIRECTORA

Dr. Ruben Dariel Velásquez Miranda

DECANO