

ANALISIS Y VERIFICACION DE SERVICIOS CORPORATIVOS DE LA CAPA DE
APLICACIÓN BAJO EL PROTOCOLO IPV6.

URBINA LEAL JUAN FERNANDO
ORTEGA ROZO TEDDY ALFREDO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD INGENIERÍAS FISICOMECÁNICA
ESCUELA DE INGENIERIAS ELECTRICA, ELECTRONICA Y DE
TELECOMUNICACIONES.
ESPECIALIZACION EN TELECOMUNICACIONES.
BUCARAMANGA

2016

ANALISIS Y VERIFICACION DE SERVICIOS CORPORATIVOS DE LA CAPA DE
APLICACIÓN BAJO EL PROTOCOLO IPV6.

URBINA LEAL JUAN FERNANDO
ORTEGA ROZO TEDDY ALFREDO

TRABAJO DE GRADO PARA OPTAR EL TITULO DE ESPECIALIZACION EN
TELECOMUNICACIONES.

DIRECTOR:
FRANCISCO JAVIER DIETES
MAGISTER EN ING. AREA TELECOMUNICACION.
UPB.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD INGENIERÍAS FISICOMECÁNICA
ESCUELA DE INGENIERIAS ELECTRICA, ELECTRONICA Y DE
TELECOMUNICACIONES.
ESPECIALIZACION EN TELECOMUNICACIONES.
BUCARAMANGA

2016

Dedicamos esta Monografía a Dios y a la virgen por permitirnos culminar la monografía que nos favorece para nuestra vida profesional.

AGRADECIMIENTOS

Me gustaría expresar mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización de mi monografía, en especial al Magister Francisco Javier Dietes, director de esta investigación, por la orientación, el seguimiento y la supervisión continúa de la misma, pero sobre todo por la motivación y el apoyo recibido a lo largo de estos meses.

Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibidos de mi familia y amigos.

A todos ellos, muchas gracias.

CONTENIDO

| | |
|--|-----|
| INTRODUCCIÓN..... | 21 |
| 1. OBJETIVOS | 22 |
| 1.1 OBJETIVO GENERAL | 22 |
| 1.2 OBJETIVOS ESPECÍFICOS..... | 22 |
| 2. PLANTEAMIENTO DEL PROBLEMA | 23 |
| 2.1 DEFINICIÓN DEL PROBLEMA..... | 23 |
| 2.2 JUSTIFICACIÓN..... | 23 |
| 3. MARCO TEÓRICO | 25 |
| 3.1 IPV4..... | 25 |
| 3.2 IPV6..... | 26 |
| 3.2.1 Qué es la transición a IPv6. | 49 |
| 3.2.2 Tunels..... | 51 |
| 3.2.3 Protocolos para IPV6..... | 54 |
| 4. IMPLEMENTACION DEL PROYECTO | 59 |
| 4.1 MATERIALES | 59 |
| 4.2 METODOLOGÍA | 60 |
| 4.2.1 Manual de instalación de IOS en GNS3..... | 61 |
| 4.2.2 Manual de instalación de Linux Centos 7 en VirtualBox..... | 67 |
| 4.2.3 Manual de instalación de Servidor Web en Centos 7. | 86 |
| 4.2.4 Configuración de DCHP en gns3. | 103 |
| 4.2.5 Configuración de DNS en WINDOWS SERVER 2012. | 108 |
| 5. DESARROLLO DEL PROYECTO..... | 119 |
| 5.1 ANÁLISIS DEL DESARROLLO DEL PROYECTO..... | 119 |

| | |
|-----------------------|-----|
| 5.2 CRONOGRAMA | 120 |
| 6. CONCLUSIONES | 121 |
| BIBLIOGRAFÍA..... | 123 |

TABLA DE FIGURAS

| | | |
|------------|---|----|
| Figura 1. | Formato de direcciones de Enlace Local y Sitio Local..... | 35 |
| Figura 2. | Prefijo 2001:0410:0110::/48 | 36 |
| Figura 3. | Formato descriptivo de una direccion IPV6 compatibles con IPV4..... | 37 |
| Figura 4. | Una dirección típica de IPV6..... | 39 |
| Figura 5. | Estructura de IPV6..... | 43 |
| Figura 6. | Dual stack o pila doble | 51 |
| Figura 7. | Túnel IPV6 en IPV4..... | 52 |
| Figura 8. | Red IPV6..... | 53 |
| Figura 9. | Configuración de DHCP IPV6..... | 60 |
| Figura 10. | Iniciamos el programa GNS3..... | 61 |
| Figura 11. | Después entramos a la opción Edit y después a la opción preferences..... | 61 |
| Figura 12. | Después vamos a la opción IOS routers para poderlas agregarlas..... | 62 |
| Figura 13. | Después vamos a la opción New y como es la primera que agregamos la IOS seleccionamos la opción New Image..... | 62 |
| Figura 14. | Después vamos a la opción Browse y buscamos la IOS que deseamos instalar..... | 63 |
| Figura 15. | Buscamos donde tenemos la IOS guarda y le damos el click en Abrir..... | 63 |
| Figura 16. | Le damos el nombre del Router que vas a instalar y le damos Next..... | 64 |
| Figura 17. | Dejamos la memoria RAM en Default y le damos click en Next..... | 64 |
| Figura 18. | Es opción de configurar internamente en el Router los dispositivos que vamos a usar, le damos Next..... | 65 |
| Figura 19. | Esta opción es para configurar las consolas internas del Router que estamos configurando, le damos click en Next..... | 65 |
| Figura 20. | Le damos click en Finish..... | 66 |
| Figura 21. | Nos aparecerá esta ventana le damos click en Apply y después en OK..... | 66 |
| Figura 22. | Vamos en el icono del Router y hay aparecerá el Router que acabamos de instalar y así hacemos con todas las IOS de Router que vayamos a instalar..... | 67 |
| Figura 23. | Abrimos el programa VirtualBox, después le damos la opción Nueva..... | 67 |

| | |
|--|----|
| Figura 24. Nos pliega una ventana seleccionamos las siguientes opciones y después le damos NEXT..... | 68 |
| Figura 25. Aquí seleccionamos la memoria RAM que queremos para nuestro Linux Centos 7 y después le damos a la opción NEXT..... | 68 |
| Figura 26. En esta nueva ventana vamos a crear el disco duro para el sistema operativo Linux Centos 7 y después le damos CREAR..... | 69 |
| Figura 27. En esta nueva ventana dejamos por defecto la opción y le damos en la opción NEXT..... | 69 |
| Figura 28. En esta nueva ventana vamos a dejar por defecto y le damos en la opción NEXT..... | 70 |
| Figura 29. En esta nueva ventana vamos a cambiar el tamaño del disco duro de 8gb a 20gb y le damos en la opción CREAR..... | 70 |
| Figura 30. Finalizando ya la configuración para después crear el sistema operativo Linux..... | 71 |
| Figura 31. Aquí vamos a la opción Configuración en el cual buscamos la imagen ISO donde tengo el sistema operativo Centos, también funciona con Cd y le damos Aceptar..... | 71 |
| Figura 32. Le damos click en Iniciar y te sale la siguiente imagen..... | 72 |
| Figura 33. Le damos enter a Install Centos 7..... | 72 |
| Figura 34. Esperar que el comience con la instalación del Linux Centos 7..... | 73 |
| Figura 35. Aquí escogemos el idioma que vamos a instalar en Centos 7..... | 73 |
| Figura 36. En esta ventana nos sale para configurar el sistema operativo de modo consola o modo gráfico y vamos a la opción Destino de la Instalación..... | 74 |
| Figura 37. Esta ventana muestra en la manera de instalar particiones al Linux Centos 7..... | 74 |
| Figura 38. Vamos a la opción de + que está en la parte inferior al lado izquierdo y nos sale esta ventana..... | 75 |
| Figura 39. Vamos a configurar el swap para darle memoria RAM extra al LINUX Centos 7..... | 75 |
| Figura 40. Después de que configuramos la SWAP nos aparece así..... | 76 |
| Figura 41. Configuración del Boot para que el Linux pueda iniciar correcta..... | 76 |
| Figura 42. Después de configurar la Boot para el CENTOS 7 nos aparecerá así..... | 77 |

| | |
|--|----|
| Figura 43. Vamos a configurar el espacio donde vamos a instalar el sistema CENTOS7, le damos la opción Agregar un punto de montaje. | 77 |
| Figura 44. Después de configurar /, donde configuramos donde vamos a instalar el sistemas operativo Linux Centos 7, nos aparecerá así. | 78 |
| Figura 45. Después de configurar todas las participaciones, le damos en la opción Listo. | 78 |
| Figura 46. Después nos sale esta opción y le damos la opción Aceptar Cambios. | 79 |
| Figura 47. Después nos sale esta ventana. | 79 |
| Figura 48. Vamos a configurar el sistema operativo Linux para que sea de manera Escritorio Gnome, entonces vamos a la opción Selección de software, después escogemos las opción Escritorio Gnome y después le damos Listo. | 80 |
| Figura 49. Vamos a empezar a instalar el sistemas operativo | 80 |
| Figura 50. Vamos a configurar contraseña de root. | 81 |
| Figura 51. Después de configurar la contraseña del root, esperar que se instale el sistema operativo Centos 7. | 81 |
| Figura 52. Después de que se instaló le damos reiniciar. | 82 |
| Figura 53. Esperar que se reinicie la máquina virtual. | 82 |
| Figura 54. Despues de reiniciar la maquina virtual nos aparecera esta ventana. | 83 |
| Figura 55. Después le damos click y nos saldrá esta nueva ventana, le damos click en siguiente. | 83 |
| Figura 56. Aquí para configurar el teclado del idioma que queramos. | 84 |
| Figura 57. Aquí configuramos el usuario que le queremos dar. | 84 |
| Figura 58. Aquí configuramos la ubicación y le damos siguiente. | 85 |
| Figura 59. Aquí termina la configuración del sistemas operativo Linux Centos 7. | 85 |
| Figura 60. Ya después de haber configurado el sistema operativo aparecerá esta ventana nueva, ya podemos usar el sistema operativo Centos 7 Linux. | 86 |
| Figura 61. Vamos a la opción de aplicaciones y después buscamos la opción terminal. | 86 |
| Figura 62. Verificamos que esté instalado el servidor web. | 87 |
| Figura 63. Como vemos que está instalado una versión, vamos actualizarla si no lo tenemos toca instalar el servidor httpd, ahora vamos a entrar como super usuario para poder instalar el servidor httpd o web. | 87 |
| Figura 64. Ahora nos disponemos de instalar el servidor httpd y esperar que se actualice con el internet. | 88 |

| | |
|--|----|
| Figura 65. Aquí nos pedirá que actualice la versión del servidor httpd y esperar que actualice. | 88 |
| Figura 66. Después pedirá que estoy de acuerdo y escribimos SI..... | 89 |
| Figura 67. Aquí nos dice que quedo actualizado el servidor httpd o web..... | 89 |
| Figura 68. Vamos a iniciar el servidor httpd o web. | 90 |
| Figura 69. Vamos a verificar si quedo instalado. | 90 |
| Figura 70. Después vamos al explorador para verificar si quedo instalado..... | 91 |
| Figura 71. Vamos a terminal otra vez y digitamos este siguiente comando, nano /etc/httpd/conf/httpd.conf después nos aparecerá esta ventana. | 91 |
| Figura 72. Ahora buscamos la opción ServerAdmin root@localhost como lo muestra la imagen | 92 |
| Figura 73. Vamos a cambiar el nombre de localhost al nombre que queramos, en este momento le puse root@serverweb.com | 92 |
| Figura 74. Vamos a cambiar la opción ServerName www.example.com:80 a ServerName www.serverweb.com | 93 |
| Figura 75. Ahora vamos a guardar los cambiamos con la tecla ctrl + o y salimos del editor de httpd con ctrl + x después nos aparecerá de nuevo la ventana del terminal. | 93 |
| Figura 76. Vamos a configurar nuestra servidor web sus hosts nano serverweb-vhosts.conf | 94 |
| Figura 77. Después de que salimos vamos a digitar estos comandos en el terminal..... | 94 |
| Figura 78. Después de que ingresamos vamos ingresar estas líneas de comandos para configurar nuestro servidor web..... | 94 |
| Figura 79. Después de que agregamos las líneas vamos a guardar con ctrl + o y con ctrl + x salir del editor de hots, volvemos de nuevo a terminal. | 95 |
| Figura 80. Ahora vamos a reiniciar el servidor web. | 95 |
| Figura 81. Ahora vamos a configurar la ip de dirección ipv6..... | 95 |
| Figura 82. Ahora vamos a cambiar unos parámetros. | 96 |
| Figura 83. En el pantallazo cambiamos los parámetros y digitamos la dirección ip que vamos a usar con el nombre del servidor que pusimos. | 96 |
| Figura 84. Ahora que cambios los parámetros vamos a guardar con ctrl + o y con ctrl + x podemos salir del editor de hosts, después regresamos al menú de terminal. ... | 97 |

| | |
|---|-----|
| Figura 85. Vamos a ingresar al editor de index.html..... | 97 |
| Figura 86. Ya ingresando al editor index.html nos va aparecer de esta manera. | 97 |
| Figura 87. Vamos ingresar los parámetros para agregar la página web para nuestro servidor. | 98 |
| Figura 88. Vamos a guardar con ctrl + o y ctrl + x cerrar nuestro editor index.html..... | 98 |
| Figura 89. Ahora volvemos de nuevo a la ventana de terminal..... | 99 |
| Figura 90. Vamos a buscar la opción de configuración de la red. | 99 |
| Figura 91. Ahora vamos a configuraciones y vamos a agregar la ip. | 100 |
| Figura 92. Ahora vamos a ipv4 para poder configurar la dirección ipv6 2001:DB8:ACAD:3::1/64 , su máscara de red y su puerta de enlace como muestra en la imagen. | 100 |
| Figura 93. Vamos a configurar dirección ip 192.168.0.2 al servidor y después vamos a la opción aplicar para guardar los cambios..... | 101 |
| Figura 94. Vamos a deshabilitar y habilitar el botón azul para que tome cambio de la ip que ingresamos. | 101 |
| Figura 95. Vamos a verificar con nuestro explorador nuestra página web que agregamos con esta dirección 127.0.0.1. | 102 |
| Figura 96. Vamos a verificar con la dirección ip..... | 102 |
| Figura 97. Vamos a verificar por ultimo con nuestro servidor web que es serverweb.com, cuando no sirva el servidor web o httpd debemos subirlo con el siguiente comando: systemctl start httpd y recuerden que tienen que ser root para levantar el servicios. | 103 |
| Figura 98. Vamos a Browse el icono siguiente para agregar los router que vamos a usar para configurar DHCP. | 103 |
| Figura 99. Configurando el siguiente red en el cual vamos a configurar DHCP..... | 104 |
| Figura 100. Vamos a configurar el router DHCP_SERVER, vamos a dar doble click en DCHP_SERVER nos aparecerá la siguiente ventana..... | 104 |
| Figura 101. Vamos a ingresar estos comando para configurar el DHCP_SERVER:..... | 105 |
| Figura 102. Vamos a configurar dirección ip en la interface fastethernet 1/0, ingresando estos comandos. | 106 |
| Figura 103. Vamos a configurar dirección ip en la interface fastethernet 2/0, ingresando estos comandos. | 107 |
| Figura 104. Configurar DNS server | 108 |

| | |
|--|-----|
| Figura 105. Ya terminado de instalar DNS ahora | 108 |
| Figura 106. Vamos a crear un nuevo dominio en DNS | 109 |
| Figura 107. Configurar un servidor DNS | 109 |
| Figura 108. Después le damos siguiente | 110 |
| Figura 109. Vamos a escoger la segunda opción para que pueda soportar ipv6 y le damos siguiente. | 110 |
| Figura 110. Escogemos la primera opción y le damos siguiente. | 111 |
| Figura 111. Vamos a escoger la primera opción | 111 |
| Figura 112. Vamos a ingresar nuestra zona que es www.serverweb.com y le damos siguiente. | 112 |
| Figura 113. Vamos a escoger la primera opción y le damos siguiente. | 112 |
| Figura 114. Vamos a escoger la segunda opción y le damos siguiente. | 113 |
| Figura 115. Vamos a configurar la zona inversa y le damos siguiente. | 113 |
| Figura 116. Vamos a dejar por defecto y siguiente. | 114 |
| Figura 117. Vamos a escoger la segunda opción para que soporte IPV6. | 114 |
| Figura 118. Aquí ingresamos la dirección ipv6 del DNS | 115 |
| Figura 119. Creamos la zona www.serverweb.com | 115 |
| Figura 120. Escogemos la segunda opción y le damos siguiente. | 116 |
| Figura 121. Escogemos la opción de no reenviar consultas porque solo es un servidor que está configurado y no es necesario. | 116 |
| Figura 122. Dejamos que busque. | 117 |
| Figura 123. Le damos siguiente para finalizar para terminar de configurar el DNS. | 117 |
| Figura 124. Vamos a configurar la dirección ipv6 en nuestro server 2012. | 118 |
| Figura 125. Vamos a terminal verificando nuestra dirección ipv6. | 118 |
| Figura 126. Cronograma | 120 |

LISTA DE TABLAS

| | | |
|----------|---|----|
| Tabla 1. | Direcciones ipv4. | 26 |
| Tabla 2. | Direcciones Asignadas Multicast y su área de funcionamiento. | 38 |
| Tabla 3. | Formato preferido de dirección IPV6. | 40 |
| Tabla 4. | Formato Preferido y Formato comprimido utilizando IPV6. | 41 |
| Tabla 5. | Formato preferido y Formato comprimido..... | 42 |
| Tabla 6. | Aplicación con ambos métodos de compresión..... | 42 |
| Tabla 7. | Direcciones IPV6 y Prefijos de red. | 44 |
| Tabla 8. | Cambios y Nuevas Características de RIPng..... | 48 |
| Tabla 9. | Cambios y Nuevas Características de OSPFv3 | 49 |

GLOSARIO

DIRECCIONES IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica (normalmente abreviado como IP dinámica).

IPV4: El Internet Protocol version 4 (IPv4) (en español: Protocolo de Internet versión 4) es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala. Definida en el RFC 791. IPv4 usa direcciones de 32 bits, limitándola a $2^{32} = 4\,294\,967\,296$ direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos (ver abajo), ya hace varios años se vio que escaseaban las direcciones IPv4.

IPV6: El Internet Protocol version 6 (IPv6) (en español: Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

MAQUINA VIRTUAL: En informática una máquina virtual es un software que simula a una computadora y puede ejecutar programas como si fuese una computadora real. Este software en un principio fue definido como "un duplicado eficiente y aislado de una máquina física". La acepción del término actualmente incluye a máquinas virtuales que no tienen ninguna equivalencia directa con ningún hardware real.

Una característica esencial de las máquinas virtuales es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por ellas. Estos procesos no pueden escaparse de esta "computadora virtual".

Uno de los usos domésticos más extendidos de las máquinas virtuales es ejecutar sistemas operativos para "probarlos". De esta forma podemos ejecutar un sistema operativo que queramos probar (GNU/Linux, por ejemplo) desde nuestro sistema operativo habitual (Mac OS X por ejemplo) sin necesidad de instalarlo directamente en nuestra computadora y sin miedo a que se desconfigure el sistema operativo primario.

ROUTER: Un router es conocido como enrutador o en caminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un en caminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos.

SWITCH: Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Los switch se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

RESUMEN

TITULO: ANALISIS Y VERIFICACION DE SERVICIOS CORPORATIVOS DE LA CAPA DE APLICACIÓN BAJO EL PROTOCOLO IPV6.

AUTOR: URBINA LEAL JUAN FERNANDO
ORTEGA ROZO TEDDY ALFREDO

PALABRAS CLAVES: Direcciones IP, Máquina virtual, Router, direccionamiento, servidor, cliente.

Descripción

Las direcciones disponibles en la reserva global de IANA pertenecientes al protocolo IPv4 se agotaron oficialmente el lunes 31 de enero de 2011. Los Registros Regionales de Internet, deben manejarse con sus propias reservas, que se estima, alcanzaran hasta el 2020, por la razón vamos a realizar una transición a IPV6 Dado que el protocolo predominante en la actualidad en Internet es IPv4, el Internet se ha convertido en algo vital, no es posible su sustitución, es decir, no es posible apagar la Red, ni siquiera por unos minutos y cambiar a IPV6.

No basta con actualizar unos pocos equipos, es una operación que tendría que involucrar a cualquier organización, sea empresa, administración pública o proveedor de acceso o contenidos de una forma sincronizada, lo cual es imposible. Es como una balanza, en la que hoy en día el lado con el mayor peso representa el tráfico IPv4, pero poco a poco, gracias a esta coexistencia, conforme más contenidos y servicios estén disponibles con IPV6.

En la monografía analizamos y verificamos los servicios corporativos de la capa de aplicación Bajo del protocolo IPV6; de manera didáctica en un entorno de emulación como GNS3, esto permite llevar acabo la implementación en un entorno real para aquellas empresas que están empezando la transición de IPV4 y IPV6.

En el marco conceptual que se consigna en esta monografía permite analizar las características y funcionalidades para redes en IPV6 en los servicios corporativos.

En este trabajo se realiza el montaje de servidores en un ambiente emulado porque es muy difícil hacerlo en un entorno real ya que no hay equipos en entornos reales disponibles para configuración y adaptación de IPV4 a IPV6.

* Trabajo de Grado

** Facultad de Ingenierías Fisicomecánica. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director: Francisco Javier Dietes.

ABSTRACT

TITLE: ANALYSIS AND VERIFICATION OF CORPORATE SERVICES LAYER APPLICATION UNDER THE PROTOCOL IPV6.

AUTHORS: URBINA LEAL JUAN FERNANDO
ORTEGA ROZO TEDDY ALFREDO

KEYWORDS:

IP Addresses, IPv6 , VIRTUAL MACHINE, Router:

Description

Addresses available on the global reserve belonging to IPv4 IANA officially sold out on Monday, January 31, 2011. The Regional Internet Registries must be handled with its own reserves, which are estimated to reach up to 2020, for the reason we to make a transition to IPV6 Since the predominant protocol today on the Internet is IPv4, the Internet has become vital, can not be replaced, that is, you can not turn off the Internet, even for a few minutes switch to IPv6.

It is not enough to update a few teams, is an operation that should involve any organization, whether business, government or ISP or content in a synchronized manner, which is impossible. It is like a scale, where today the side with the greater weight represents the IPv4 traffic, but gradually, thanks to this coexistence, as more content and services are available with IPv6.

The paper analyze and verify corporate services Under the application layer protocol IPV6; didactically in an emulation environment as GNS3, it allows carry out the implementation in a real environment for companies that are beginning the transition from IPV4 and IPV6.

In the conceptual framework that is reported in this paper to analyze the features and functionality for IPV6 networks in corporate services.

In this work the server installation is performed in an emulated environment because it is very difficult to do in a real environment because there is no equipment in real environments available for configuration and adaptation of IPV4 to IPV6.

* Grade work

** Faculty the engineering fisic mecanic. School of Electrical Engineering, Electronics and Telecommunications. Director: Francisco Javier Dietes.

INTRODUCCIÓN

La monografía permite afianzar los conocimientos sobre el protocolo IPV6, facilitando la transición de IPV4 a IPV6, reconociendo la fundamentación teórica, tipos de direcciones ipv6 y stack de protocolos IPV6.

En la monografía se analiza y verifica los servicios corporativos de la capa de aplicación bajo el protocolo ipv6, evaluando su desempeño usando el emulador GNS3 para preparar un plan de implementación.

Cumpliendo con los objetivos específicos, para revisar el comportamiento de los servicios de la capa de aplicación bajo el protocolo IPV6 se emplean máquinas para sistemas operativos CENTOS 7 (GNU). Se han configurado servidores como WEB, DNS, DHCP en un entorno LAN, garantizando su conectividad y su correcto funcionamiento, finalmente se analiza y revisa las vulnerabilidades. Como producto de la monografía se entrega un manual de configuración y práctica para alumno y docente para facilitar de manera didáctica la apropiación conceptual del protocolo IPV6.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar y verificar los servicios corporativos de la capa de aplicación bajo el protocolo ipv6, evaluando su desempeño usando el emulador GNS3 para preparar un plan de implementación.

1.2 OBJETIVOS ESPECÍFICOS

- 1) Realizar la revisión del comportamiento de los servicios de la capa de aplicación bajo el protocolo IPV6 para sistemas operativos CENTOS 7 (GNU).
- 2) Configurar un escenario para las pruebas de conectividad y desempeño ente los servicios corporativos.
- 3) Análisis y configuración usando GNS3 para los siguientes servicios corporativos:
 - a) WEB.
 - b) DNS.
 - c) DHCP.
- 4) Analizar y revisar las vulnerabilidades, fortalezas para cada uno de los servicios planteados anteriormente, empleando escenarios simulados en GNS3 y CENTOS en redes LAN.
- 5) Redacción de manuales de alumno y docente para configurar de cada servidor e integración de los mismos en el escenario emulado.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

El crecimiento exponencial del Internet y el agotamiento de las direcciones IPv4, por ser un número finito, está llegando al límite que ha obligado a la **IANA** (Agencia Internacional de Asignación de Números de Internet) (Kim Davies) a implementar el direccionamiento IPv6; las redes corporativas no es ajena a esta situación debido a la poca implementación y capacitación sobre la implementación de nuevas tecnologías en protocolos de comunicaciones.

El proyecto va a abordar esta temática a través de un montaje real de servidores IPV6 interconectados con escenarios simulados que contiene equipos de Networking con características funcionales similares a equipos reales. El alcance del proyecto es mostrar de una forma didáctica el proceso de configuración de adaptación de IPV4 a IPV6.

2.2 JUSTIFICACIÓN

La realización del presente proyecto pretende analizar la situación actual de los protocolos usados en internet y plantear cuales serían las medidas a tomar en caso de que se llegue prontamente al agotamiento de direcciones IPv4 en el ofrecimiento de los servicios corporativos, con el fin de evitar un colapso de la presentación de los servicios.

Como especialista en telecomunicaciones se requiere fortalezas en el análisis técnicas de enrutamiento configuración de servicios corporativos, configuración de equipos de Networking y en general en diseño y alistamiento de equipos para redes corporativas.

Se decide implementar en GNS3 porque el software es gratuito (no es licenciado), tecnológicamente se necesita un portátil con capacidad suficiente y memoria RAM para que funciones las máquinas virtuales en las que vamos a usar.

Para las empresas no es tan costoso la implementación, solo cambiar unas formas de configuraciones en las redes LAN y WAN, con dispositivos de Networking actualizado.

3. MARCO TEÓRICO

3.1 IPV4.

IPv4 es la versión 4 del Protocolo de Internet (IP o Internet Protocol) y constituye la primera versión de IP que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicialmente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (IETF o Internet Engineering Task Force) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet).

Tiene las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de mejor esfuerzo).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicados o en desorden.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de TCP o UDP.

El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4, 294, 967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión (Multicast), etc. Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de IPv6 (actualmente en desarrollo) como reemplazo eventual dentro de algunos años para IPv4.

Tabla 1. Direcciones ipv4.

| CLASE | DIRECCIONES DISPONIBLES | | CANTIDAD DE REDES | CANTIDAD DE HOSTS | APLICACIÓN |
|----------|-------------------------|-----------------|-------------------|-------------------|----------------|
| | DESDE | HASTA | | | |
| A | 0.0.0.0 | 127.255.255.255 | 128 [*] | 16.777.214 | Redes grandes |
| B | 128.0.0.0 | 191.255.255.255 | 16.384 | 65.534 | Redes medianas |
| C | 192.0.0.0 | 223.255.255.255 | 2.097.152 | 254 | Redes pequeñas |
| D | 224.0.0.0 | 239.255.255.255 | no aplica | no aplica | Multicast |
| E | 240.0.0.0 | 255.255.255.255 | no aplica | no aplica | Investigación |

^{*} El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

Fuente: <https://teleprocesos.wikispaces.com/subneteo>

3.2 IPV6.

IPv6 es Protocolo de Internet versión 6, definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 sujeto a todas las normativas que fuera configurado –está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados—. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

A principios de 2010, quedaban menos del 10 % de IP sin asignar.¹ En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPv4 posibilita 4 294 967 296 (232) direcciones de host diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada dispositivo, teléfono, PDA, tablet, etcétera. En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) —cerca de $6,7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008.

Fundamentos de IPv6

Protocolo de Internet versión 6 (Internet Protocol version 6, IPv6):

Debido al crecimiento del Internet y la sofisticación de los dispositivos electrónicos, las soluciones propuestas con el fin de escalar el espacio de direccionamiento de Internet IPv4, no serán suficientes para cubrir la necesidad de las mismas en los

próximos años. Como consecuencia de este escenario, el Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force o IETF, por sus siglas en inglés) elaboró una serie de especificaciones para definir un protocolo IP de Siguiete Generación (IP Next Generation, IPng) que actualmente se conoce como Protocolo de Internet versión 6.

Espacio mayor de direccionamiento

El IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mucho mayor de nodos direccionales. El diseño del protocolo agrega múltiples beneficios en seguridad, manejo de calidad de servicio, una mayor capacidad de transmisión y mejora la facilidad de administración, entre otras cosas.

Mientras que IPv4 soporta 4,294,967,296 (232) direcciones que es poco menos de 4.3 billones, IPv6 ofrece 3.4×10^{38} (2128) direcciones, un número similar a $6.67126144781401 \times 10^{23}$ direcciones IP por cada metro cuadrado sobre la superficie de la Tierra. Adicionalmente, la dirección IPv6 se diseñó para ser subdividida en dominios de enrutamiento jerárquico que reflejan la topología del Internet actual.

Características de IPv6

El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos. Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet. El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso. La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de renumerado. La difusión ARP es reemplazada por el uso de multicast en el link local. El encabezado de IPv6 es

más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.

Jerarquía de direcciones

Un espacio mayor de direcciones de IPv6 permite mayores distribuciones de direcciones a las organizaciones y a los proveedores de servicios de Internet (ISPs). Al tener una gran disponibilidad de direcciones se posibilita el uso de un solo prefijo grande para toda la red de una organización y , por ende, el ISP puede sumar las rutas (agregar) de todos los prefijos de sus clientes en un solo prefijo y anunciarlo al Internet IPv6.

Cuando un usuario final cambia su proveedor de IPv6, el cual le proveía de direccionamiento IPv6, entonces también debe cambiar su prefijo de IPv6 para preservar su agregación global. Al mismo tiempo, el cambiar de proveedor implica una remuneración de la red.

Modos de configuración de IPv6

Autoconfiguración. Definida en el **RFC 2462** y también es conocida como Configuración Automática de Dirección Sin Estado IPv6. Esta funcionalidad permite que un router IPv6 envíe, a través del enlace local, la información de red a las computadoras y que ellas puedan configurarse correctamente. La información enviada es el prefijo de IPv6 del enlace local y la ruta por defecto del mismo protocolo. Mediante este mecanismo cada computadora y servidor de IPv6 añade su dirección de capa de enlace (dirección MAC) en el formato EUI-64 al prefijo de IPv6 de unicast global único anunciado en la subred.

Configuración mediante servidor. Las computadoras que utilizan IPv6 pueden obtener sus parámetros y direcciones de configuración de un servidor de DHCP versión 6. Este modo es llamado Configuración de Direcciones con Estado IPv6.

Remuneración:

El proceso de remuneración de IPv6 fue diseñado para ser transparente entre los proveedores de IPv6 unicast y los usuarios finales. Esto se logra con el mecanismo de autoconfiguración que permite una remuneración sencilla a las computadoras con sólo enviarles el nuevo prefijo IPv6 unicast para la red. Una desventaja de este mecanismo es la pérdida de las sesiones TCP y UDP que ocurren entre las computadoras y los servidores al momento exacto de la transición. Esto es algo que también ocurre actualmente con IPv4.

Multicasting

La difusión del Protocolo de Resolución de Dirección (Address Resolution Protocol, ARP) de IPv4 afecta la eficiencia de la red. Esta situación no ha sido incluida en IPv6, y en su lugar se utiliza el Multicasting el cual funciona de la siguiente manera:

Se crea un grupo Multicast, formado por conjunto de interfaces de red. Si se está interesado en que cierta computadora reciba los paquetes de difusión del grupo se agrega una interfaz de red, de esa forma se envía un paquete multicast al grupo X.

Ese paquete sólo llegará a aquellas computadoras que tengan su interfaz incluida en el grupo multicast X. Con ello se permite tener niveles de eficiencia de red superiores a los presentados en IPv4, lo cual se verá traducido en la disminución de los ciclos de procesamiento de CPU de las computadoras en la red local al no procesar paquetes de difusión que no van dirigidos a ellos y de la misma manera se estará eliminando el problema de las tormentas de paquetes de difusión de IPv4.

Encabezado eficiente

El nuevo encabezado de IPv6 es más sencillo que el de IPv4. Del encabezado de IPv4 se removieron 6 campos: Longitud de encabezado, Identificación, Banderas,

Desplazamiento por fragmentación, Suma de verificación de encabezado, Opciones y Relleno. Al pasar de un encabezado de IPv4 con longitud variable a IPv6 con menos campos y longitud fija se obtiene una reducción en los ciclos de CPU de los ruteadores al momento de enviar los paquetes de IPv6. Lo anterior conlleva un mejor desempeño de la red.

Etiqueta de flujo

Dentro del encabezado de IPv6 existe un nuevo campo llamado Etiqueta de Flujo, éste es usado por el nodo fuente para solicitar un manejo especial de secuencias específicas de paquetes. La etiqueta está dirigida al procesamiento de la estación destino, no para los ruteadores, y es de gran utilidad para aplicaciones como videoconferencias y voz sobre protocolo de Internet (VoIP). Asimismo agrupa todas aquellas que requieren un tratamiento especial de Calidad de Servicio (Quality of Service, QoS) en los ruteadores de la trayectoria.

Extensiones de encabezado

La utilización del campo Opciones en el encabezado de IPv4 presenta desventajas a la transmisión de los paquetes y a la eficiencia de la red. En lo que respecta a la variación del tamaño del encabezado es debido a que tiene campos opcionales. En el segundo caso todos los ruteadores que procesan el paquete deben computar el encabezado con su campo de longitud variable lo que introduce retardos y gasto de la capacidad del CPU en ciclos de procesamiento que son innecesarios.

Para resolver la situación anterior, IPv6 sustituye el campo Opciones al final del encabezado por las Extensiones de Encabezado, formando un encadenamiento de encabezados enlazados por un campo llamado Siguiente Encabezado. Se presenta un campo Siguiente Encabezado dentro de cada Extensión de Encabezado usado por IPv6. Este diseño con extensiones permite una mejor

eficiencia en el procesamiento de los paquetes, ya que asegura que los ruteadores y nodos computan los encabezados dirigidos a ellos a lo largo de la trayectoria.

Movilidad

Debido a que la movilidad es una característica importante y deseable por las compañías proveedoras y los consumidores finales el Protocolo de Internet Móvil (MobileIP) esta capacidad está disponible tanto en IPv4 como en IPv6. Cabe destacar que en este último la movilidad se construyó dentro del protocolo en lugar de ser una nueva función agregada como en IPv4. Ello implica que cualquier nodo IPv6 puede usar un IP Móvil tanto como lo requiera. IPv6 Móvil utiliza dos Extensiones de Encabezado: un Encabezado de Enrutamiento para el registro y un Encabezado de Destino para entrega del datagrama entre los nodos móviles y sus nodos fijos correspondientes.

Seguridad

El protocolo IPSec estandarizado por el Grupo Especial sobre Ingeniería de Internet provee las funciones de:

- A. Limitar el acceso a sólo aquellos autorizados.
- B. Certifica la autenticación de la persona que envía los datos.
- C. Encriptar los datos transmitidos a través de la red.
- D. Asegura la integridad de los datos.
- E. Invalida la repetición de sesiones, para evitar que no sean repetidas por usuarios maliciosos.

Los protocolos que respaldan el funcionamiento de IPSec son: la Autenticación de Encabezado (Authentication Header, AH) y la Carga de Seguridad Encapsulada (Encapsulated Security Payload, ESP). Al estar incluidos en cada implementación de IPv6 se provee mayor seguridad ya que IPSec está presente en todos los nodos de la red.

Mecanismos de Transición

Actualmente no existe una fecha definida para dejar de utilizar IPv4 o comenzar a utilizar IPv6 completamente, por lo que al diseñar IPv6 se optó por incluir mecanismos que permitan una coexistencia de ambos esquemas de direccionamiento y que en el largo plazo permitan tener una transición sin complicaciones hacia IPv6. Estos esquemas son los siguientes:

- a. Nodos de Doble Pila sobre redes IPv4.
- b. Islas de Nodos de Sólo IPv6 sobre redes IPv4.
- c. Nodos de IPv4 que puedan comunicarse con redes IPv6.
- d. Nodos de IPv6 que puedan comunicarse con redes IPv4.

Direccionamiento

Los cambios introducidos por IPv6 no sólo son en cantidad de direcciones sino que incluyen nuevos tipos, representaciones y sintaxis.

Tipos de direcciones IPv6:

Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados:

Unicast. Se utiliza únicamente para identificar una interface de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interface identificada por esa dirección.

Multicast. Se utiliza para identificar a un grupo de interfaces IPv6. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.

Anycast. Se asigna a múltiples interfaces (usualmente en múltiples nodos). Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.

Cada uno de los tres tipos se subdivide en direcciones diseñadas para resolver casos específicos de direccionamiento IP, los cuales a continuación se presentan y describen.

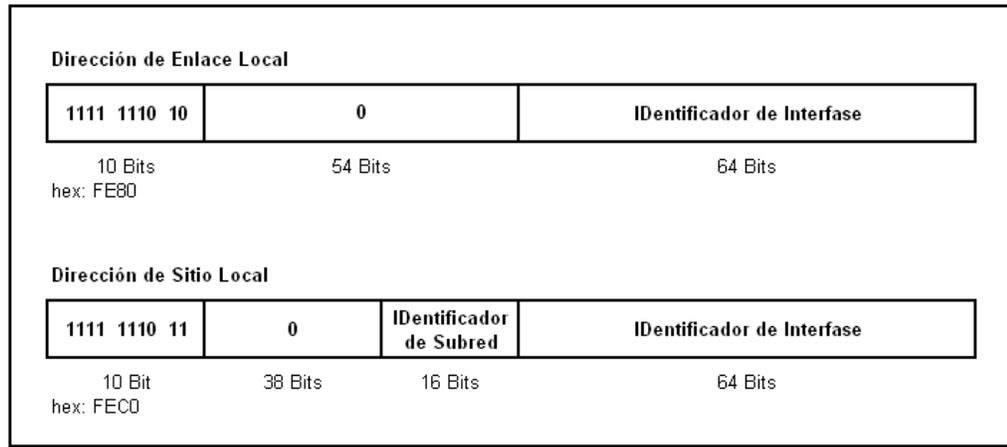
Unicast agrupa los siguientes tipos:

- A. Enlace Local (Link-Local).
- B. Sitio Local (Site-Local).
- C. Agregable Global (Aggregatable Global).
- D. Loopback.
- E. Sin-Especificar (Unspecified).
- F. Compatible con IPv4.
- G. Anycast agrupa:
- H. Agregable Global (Aggregatable Global).
- I. Sitio Local (Site Local).
- J. Enlace Local (Link Local).
- K. Multicast agrupa:
- L. Asignada (Assigned).
- M. Nodo Solicitado (Solicited Node).

Enlace Local. Se utiliza en un enlace sencillo y no debe nunca ser enrutada. Se usa para mecanismos de autoconfiguración, descubrimiento de vecinos y en redes sin ruteadores. Es útil para crear redes temporales. Puede ser utilizada sin un prefijo global.

Sitio Local. Contiene información de subred dentro de la dirección. Son enrutadas dentro de un sitio, pero los ruteadores no deben enviarlas fuera de éste. Además es utilizada sin un prefijo global.

Figura 1. Formato de direcciones de Enlace Local y Sitio Local.



Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>.

El prefijo FE80 identifica a una dirección de Enlace Local y el prefijo FEC0 identifica a un Sitio local, ambos en hexadecimal.

Agregable Global. Son las direcciones IPv6 utilizadas para el tráfico de IPv6 genéricos en el Internet de IPv6 y son similares a las direcciones unicast usadas para comunicarse a través del Internet de IPv4. Representan la parte más importante de la arquitectura de direccionamiento de IPv6 y su estructura permite una agregación estricta de prefijos de enrutamiento para limitar el tamaño de la tabla de enrutamiento global de Internet.

Cada Dirección Agregable Global consta de tres partes:

Prefijo recibido del proveedor: el prefijo asignado a una organización por un proveedor debe ser al menos de 48 bits (recomendado por el RFC 3177). El prefijo asignado a la organización es parte del prefijo del proveedor.

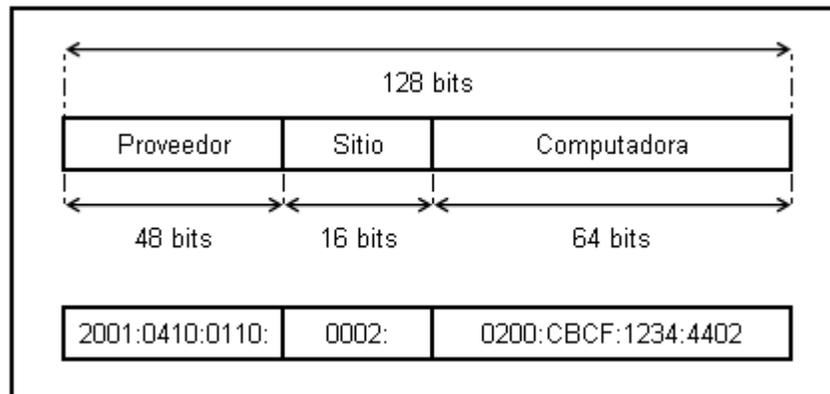
Sitio: con un prefijo de 48 bits distribuido a una organización por medio de un proveedor, se abre la posibilidad para esa organización de tener 65,535 subredes

(asignando un prefijo de 64 bits a cada una de las subredes). La organización puede usar los bits 49 a 64 (16 bits) del prefijo recibido para subredes.

Computadora: utiliza cada Identificador de interface del nodo. Esta parte de la dirección IPv6, que representa los 64 bits de más bajo orden de la dirección, es llamada Identificador de Interface.

La siguiente figura muestra como ejemplo al prefijo 2001:0410:0110::/48 que es asignado por un proveedor a una organización. Dentro de la organización el prefijo 2001:0410:0110:0002::/64 es habilitado en una subred. Finalmente, un nodo en esta subred tiene la dirección 2001:0410:0110:0002:0200:CBCF:1234:4402.

Figura 2. Prefijo 2001:0410:0110::/48



Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

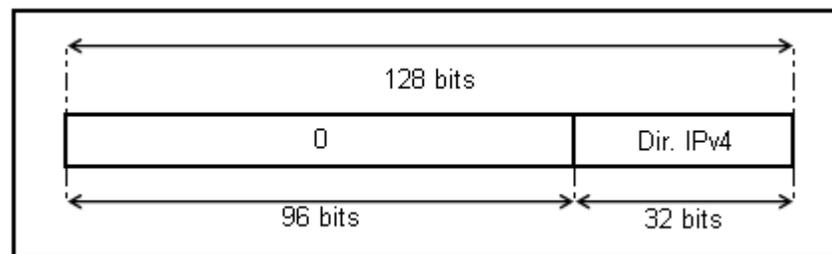
Loopback. Al igual que en IPv4, cada dispositivo tiene una dirección loopback, que es usada por el nodo mismo. En IPv6 se representa en el formato preferido por el prefijo 0000:0000:0000:0000:0000:0000:0000:0001 y en el formato comprimido por 1.

Sin-Especificar. Es una dirección unicast sin asignar a alguna interfase. Indica la ausencia de una dirección y es usada para propósitos especiales. Es representada en el formato preferido con el prefijo 0000:0000:0000:0000:0000:0000:0000:0000 y con :: en el formato comprimido.

Compatible con IPv4. Es utilizada por los mecanismos de transición en computadoras y ruteadores para crear automáticamente túneles IPv4. De esa forma se entregan paquetes IPv6 sobre redes IPv4.

En la siguiente figura se muestra el formato descriptivo de una dirección IPv6 compatible con IPv4. En éste el prefijo se crea con el bit puesto a cero del de más alto nivel de los 96 bits, y los restantes 32 bits de menor nivel representan la dirección en formato decimal.

Figura 3. Formato descriptivo de una dirección IPV6 compatibles con IPV4.



Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Asignada Multicast. Está definida y reservada por el RFC 2373 para la operación del protocolo IPv6. Dichas direcciones asignadas son usadas en el contexto de mecanismos específicos del protocolo. En la siguiente tabla se presentan las Direcciones Asignadas Multicast y su área de funcionamiento.

Tabla 2. Direcciones Asignadas Multicast y su área de funcionamiento.

| Dirección Multicast | Área de Funcionamiento | Significado | Descripción |
|---------------------|------------------------|-----------------------|---|
| FF01::1 | Nodo | Todos los nodos | Todos los nodos en la interfase local |
| FF01::2 | Nodo | Todos los enrutadores | Todos los enrutadores en la interfase local |
| FF02::1 | Enlace Local | Todos los nodos | Todos los nodos en el enlace local |
| FF02::2 | Enlace Local | Todos los enrutadores | Todos los enrutadores en el enlace local |
| FF05::2 | Sitio | Todos los enrutadores | Todos los enrutadores en un sitio |

Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Nodo Solicitado Multicast. Es una dirección a la que se debe unir cada nodo por cada dirección unicast y anycast asignada. La dirección se forma tomando los 24 bits de bajo nivel de una dirección IPv6 (es la última parte del identificador de la computadora). La dirección los juntamos con el prefijo FF02:0:0:0:1:FF00::/104, de esa manera el rango de direcciones Multicast de Nodo Solicitado va de FF02:0:0:0:1:FF00:0000 a FF02:0:0:0:1:FFFF:FFFF.

Reglas de Utilización

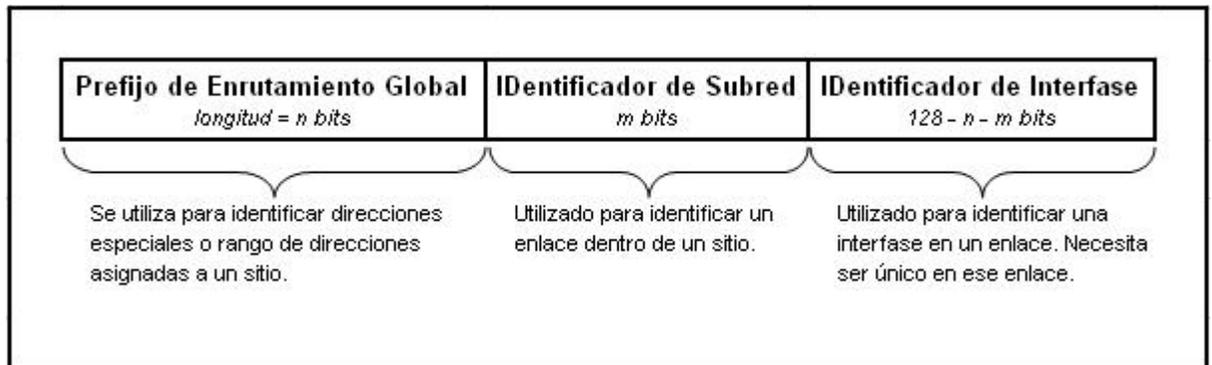
Las direcciones IPv6 son asignadas a interfaces, no a nodos, por lo que cada interface de un nodo necesita al menos una dirección unicast. A una sola interface se le pueden asignar múltiples direcciones IPv6 de cualquier tipo (unicast, anycast, multicast). Por lo cual un nodo puede ser identificado por la dirección de cualquiera de sus interfaces.

Existe la posibilidad de asignar una dirección unicast a múltiples interfaces para balanceo de cargas.

Una dirección típica de IPv6 consiste de tres partes como se muestra en la figura de abajo:

- a. El prefijo de enrutamiento global
- b. El Identificador de subred
- c. El Identificador de interfase

Figura 4. Una dirección típica de IPV6.



Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Notación de Direcciones

Como lo define el RFC 2373 Arquitectura del Direccionamiento del Protocolo de Internet versión 6, existen tres formatos para representar direcciones IPv6.

El formato preferido es el método más largo. Este representa los 32 caracteres hexadecimales que forman la dirección. Es el más cercano a la forma en que la computadora procesa la dirección.

Mediante una representación comprimida que se utiliza para simplificar la escritura de la dirección. El tercer método es el relacionado con los mecanismos de transición donde una dirección IPv4 está incluida dentro de una dirección IPv6. Este método es el menos importante de los tres y sólo es útil si se utiliza algún mecanismo de transición como NAT-PT.

Formato preferido de dirección IPv6

Es también conocido como formato completo y se compone de los ocho campos de 16 bits hexadecimales separados por dos puntos. Cada campo de 16 bits representa cuatro caracteres hexadecimales y los valores que puede tomar el campo de 16 bit van de 0x0000 a 0xFFFF. A continuación se presentan ejemplos de direcciones IPv6 en el formato preferido.

Tabla 3. Formato preferido de dirección IPV6.

| Ejemplos de direcciones IPv6 en formato preferido |
|---|
| 0000:0000:0000:0000:0000:0000:0000:0000 |
| 0000:0000:0000:0000:0000:0000:0000:0001 |
| 2001:0410:0000:1234:FB00:1400:5000:45FF |
| 3FFE:0B00:0C18:0001:0000:1234:AB34:0002 |
| FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF |

Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Formato comprimido

En IPv6 es común que se presenten cadenas grandes de ceros dentro de las direcciones. Para simplificar su escritura se ha convenido en utilizar una sintaxis especial en donde se suprimen los valores consecutivos de ceros ante dos situaciones: campos sucesivos de ceros y campos con ceros al inicio.

Campos sucesivos de ceros

Para simplificar la longitud de una dirección IPv6, cuando se presentan de uno a múltiples campos de ceros, es legal representar estos como ceros o :: (doble dos puntos). Sin embargo, es permitido usarlo una sola vez en la escritura de la dirección. En la siguiente tabla se presenta del lado izquierdo las direcciones en formato preferido y resaltado en negro los campos sucesivos de ceros que son

sustituidos por los dos puntos dobles y del lado derecho se presenta la dirección en su formato comprimido.

Tabla 4. Formato Preferido y Formato comprimido utilizando IPV6.

| Formato Preferido | Formato comprimido utilizando :: |
|--|---|
| 0000:0000:0000:0000:0000:0000:0000:0000 | :: |
| 0000:0000:0000:0000:0000:0000:0000:0001 | ::0001 |
| 2001:0410: 0000 :1234:FB00:1400:5000:45FF | 2001:0410::1234:FB00:1400:5000:45FF |
| 3FFE:0B00:0C18:0001: 0000 :1234:AB34:0002 | 3FFE:0B00:0C18:0001::1234:AB34:0002 |
| FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF | FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF |

Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

La dirección FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF es una dirección que no puede ser comprimida.

Campos con ceros al inicio

El segundo método para comprimir direcciones se aplica a cada uno de los campos hexadecimales de 16 bits que tienen uno o más ceros al inicio. Ello involucra que si hay uno o más ceros al inicio de cada campo, estos pueden ser suprimidos para simplificar su longitud y facilitar su lectura y escritura.

No obstante, si cada carácter del campo es cero al menos uno debe de ser mantenido. La siguiente tabla muestra del lado izquierdo las direcciones en su Formato Preferido con los ceros iniciales resaltados en negro y del lado derecho están las direcciones en su Formato comprimido con los ceros suprimidos.

Tabla 5. Formato preferido y Formato comprimido.

| Formato Preferido | Formato comprimido |
|---|--|
| 0000:0000:0000:0000:0000:0000:206.123.31.2 | 0:0:0:0:0:0:206.123.31.2 o ::206.123.31.2 |
| 0000:0000:0000:0000:0000:0000:ce7b:1f01 | 0:0:0:0:0:0:ce7b:1f01 o ::ce7b:1f01 |
| 0000:0000:0000:0000:0000:FFFF:206.123.31.2 | 0:0:0:0:0:FFF:206.123.31.2 o ::FFFF:206.123.31.2 |
| 0000:0000:0000:0000:0000:FFFF:ce7b:1f01 | 0:0:0:0:0:FFFF:ce7b:1f01 o ::FFFF:ce7b:1f01 |

Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Combinación de ambos métodos de compresión

Se pueden combinar la compresión de campos sucesivos de ceros con la compresión de campos con ceros al inicio para simplificar la longitud de la dirección IPv6. En la siguiente tabla se muestra un ejemplo de la aplicación con ambos métodos de compresión. Al igual que en ejemplos anteriores, los caracteres resaltados en negro son los valores que serán suprimidos.

Tabla 6. Aplicación con ambos métodos de compresión.

| Formato Preferido | Formato comprimido |
|--|------------------------------------|
| 0000:0000:0000:0000:0000:0000:0000:0000 | :: |
| 0000:0000:0000:0000:0000:0000:0000:0001 | ::1 |
| 2001:0410: 0000 :1234:FB00:1400:5000:45FF | 2001:410::1234:FB00:1400:5000:45FF |
| 3FFE: 0B00:0C18:0001:0000 :1234:AB34: 0002 | 3FFE:B00:C18:1::1234:AB34:2 |
| FE80:0000:0000:0000:0000:0000:0000:0009 | FE80::9 |

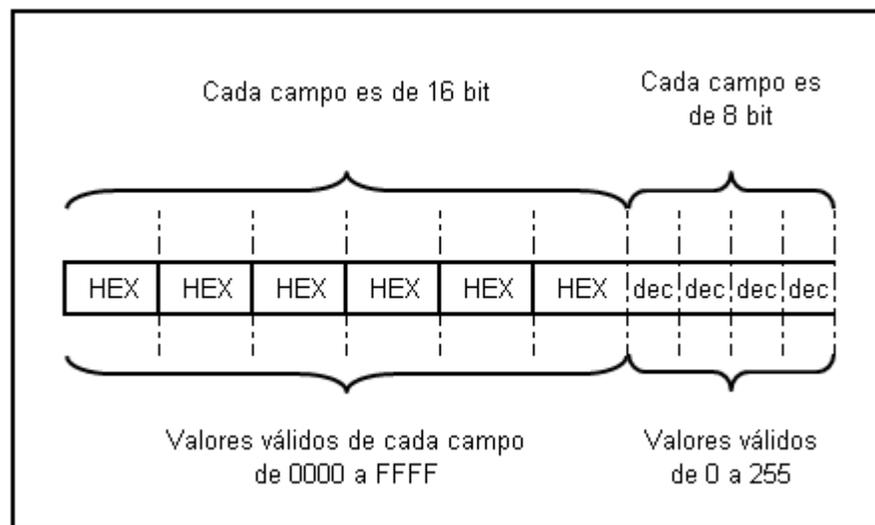
Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Direcciones IPv6 con direcciones IPv4 incrustadas

Este cuarto tipo de representación es utilizado en una dirección IPv4 incrustada dentro de una dirección IPv6. La primera parte de la dirección IPv6 utiliza la representación hexadecimal y el otro segmento de IPv4 está en formato decimal. Esta es una representación específica de una dirección usada por mecanismos de transición.

La dirección se divide en dos niveles, superior e inferior, y estos a su vez se subdividen. El nivel superior se fragmenta en seis campos con valores hexadecimales de 16 bits seguidos del nivel inferior compuesto de 4 campos con valores decimales de 8 bits. La siguiente imagen muestra la distribución de la dirección IPv6 con una dirección IPv4 incrustada.

Figura 5. Estructura de IPV6



Fuente. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Existen dos tipos de direcciones IPv6 que tienen direcciones IPv4 incrustadas:

Dirección IPv6 compatible con IPv4. Es utilizada para establecer un túnel automático que lleva paquetes IPv6 sobre redes IPv4. Esta dirección está vinculada con un mecanismo de transición del protocolo IPv6.

Dirección IPv6 mapeada a IPv4. Se utiliza sólo en el ámbito local de nodos que tienen las direcciones IPv4 e IPv6. Los nodos usan direcciones IPv6 mapeadas a IPv4 de forma interna solamente. Estas direcciones no son conocidas afuera del nodo y no llegan al cable de comunicación como direcciones IPv6.

En la siguiente tabla se muestran ejemplos de direcciones IPv4 incrustadas en direcciones IPv6, ellas se presentan en el formato comprimido. La primera dirección exhibida es del tipo Dirección IPv6 compatible con IPv4 y la segunda es una Dirección IPv6 mapeada a IPv4.

IPv6 y Subredes

En IPv6 la única forma aceptable de representar una máscara de red es mediante notación CIDR. Aunque las direcciones estén en formato hexadecimal, el valor de la máscara de red se mantiene como un valor decimal. La siguiente tabla muestra ejemplos de direcciones IPv6 y prefijos de red utilizando el valor de red en notación CIDR.

Tabla 7. Direcciones IPV6 y Prefijos de red.

| Prefijo IPv6 | Descripción |
|-----------------------------|--|
| 2001:410:0:1:0:0:0:45FF/128 | Representa una subred con una sola dirección IPv6 |
| 2001:410:0:1::/64 | El prefijo de red 2001:410:0:1::/64 puede manejar 2^{64} nodos. Esta es la longitud por defecto de un prefijo para una subred. |
| 2001:410:0::/48 | El prefijo de red 2001:410:0::/48 puede manejar 2^{16} prefijos de red de 64 bit. Esta es la longitud por defecto de un prefijo para un sitio. |

Fuente. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

En el apartado de subredes los puntos sobresalientes son los siguientes:

De la misma forma que sucede con IPv4, en IPv6 el número de bits puestos a 1 en la máscara de red define la longitud del prefijo de red y la parte restante es para el direccionamiento del nodo. Esto es importante para las IPs, ya que define cuándo los paquetes van a ser enviados al ruteador por defecto o a un nodo específico en la misma subred.

En IPv6 se suprime el concepto de dirección reservada en un rango de red. A diferencia de IPv4 donde se reservaba la primera (dirección de red) y la última (dirección de difusión) de un rango, en IPv6 no existen estos conceptos.

El número de bits para el direccionamiento del nodo dentro de un prefijo de sitio (48 bits) en IPv6 resulta ser tan grande que no es necesario hacer un plan de direccionamiento para un sitio utilizando diferentes valores de máscara de red. De ahí que el cálculo de máscara de red para cada subred y el uso de VLSM no son requeridos.

Seguridad en IPv6

La seguridad dentro del protocolo IPv6 está basada en el protocolo IPSec, el cual está disponible tanto en IPv4 como en IPv6. Una implementación de IPv6 incluye inserciones de Encabezados de Autenticación (AH, Authentication Headers) y extensión de encabezados de Carga de Seguridad Encapsulada (ESP, Encapsulating Security Payload). El tener IPSec en cualquier nodo IPv6 debe permitir sesiones de seguridad de extremo a extremo.

Para los ruteadores con soporte IPv6, IPSec puede ser usado en diferentes áreas:

- **OSPFv3** – utiliza AH, la extensión de encabezados maneja ESP como un mecanismo de autenticación en lugar de la variedad de esquemas de autenticación y procedimientos definidos en OSPFv2.
- **IPv6 Móvil** – Esta especificación de protocolo es un proyecto de la IETF propuesto para usar IPSec para hacer obligatoria la autenticación de actualización.
- **Túneles** – Los túneles IPSec pueden ser configurados entre sitios (ruteadores IPv6) en lugar de que cada computadora utilice IPSec.

· **Administración de Red** – IPsec se puede utilizar para garantizar el acceso del router para la gestión de la red.

IPsec está definido en dos extensiones de encabezado separados de IPv6 que pueden ser puestas juntas dentro del mismo paquete IPv6. Las dos extensiones son Autenticación de Encabezado IPsec (AH) y extensión de encabezados de Carga de Seguridad Encapsulada (ESP).

A. Autenticación de Encabezado IPsec (AH)

El primer encabezado es el de Autenticación (AH), el cual provee integridad, autenticación del nodo fuente y protección contra repetición. La Autenticación de Encabezado IPsec protege la integridad de la mayoría de los campos de encabezado de IPv6, excepto a aquellos que cambian sobre la trayectoria, tal como lo hacen el campo Límite de Salto. Además, el AH IPsec autentica la fuente a través de un algoritmo basado en una firma.

La diferencia clave entre la seguridad de IPv4 e IPv6 es el hecho de que IPsec es obligatorio para IPv6 tal como lo indica el RFC 2460. Éste es la Especificación del Protocolo de Internet versión 6, traducándose en que todas las comunicaciones IP extremo-a-extremo pueden ser seguras si existe suficiente infraestructura para hacerlo en una gran escala.

B. Carga de Seguridad Encapsulada IPsec (ESP)

Es el segundo encabezado IPsec, éste provee confidencialidad, autenticación del nodo fuente, integridad interna del paquete y protección contra repetición.

Enrutamiento con IPv6

El protocolo IPv6 no cambió los fundamentos del enrutamiento del protocolo IP, el cual todavía se basa en:

- La coincidencia del mayor prefijo.
- El posible uso de enrutamiento fuente.
- Re direcciona con ICMP.
- Los mismos protocolos de enrutamiento: RIP, OSPF, IS-IS y BGP.

No hay cambios mayores en el enrutamiento, de esa forma el cambio a IPv6 es transparente para el administrador de redes. Únicamente se realizaron modificaciones a la forma en que se maneja el enrutamiento para hacerlo más eficiente o para hacer uso de las características de IPv6.

Rutas Estáticas – Son utilizadas para forzar el enrutamiento de algunos prefijos a través de ruteadores específicos. La ruta por omisión (::/0) es un ejemplo de ruta estática. Las rutas estáticas en una tabla de enrutamiento tienen una mayor preferencia sobre rutas aprendidas por protocolos de enrutamiento.

Una ruta estática contiene el prefijo a ser enrutador y la dirección IP del ruteador. Dicha ruta tiene como nombre el siguiente salto, es el responsable de enrutar cualquier paquete con un destino dentro del rango de prefijo dado. No existen diferencias entre IPv4 e IPv6 para las rutas estáticas, sin embargo, se debe usar una dirección de enlace local como la dirección de siguiente salto.

RIP –(RFC 1058) es un protocolo para redes de tamaño de pequeño a mediano.

La versión mejorada para IPv6 conocida como RIP Siguiete Generación (RIPng, RIP next generation) (RFC 2080 y 2081) está basada en RIP versión 2 (RFC 1723) y hereda las mismas características genéricas:

Algoritmo vector-distancia Bellman-Ford.

- Actualizaciones cada 30 segundos.
- Tiempo de expiración de 180 segundos para rutas desconectadas.
- Métricas fijas.

- Diámetro de red de 15 saltos.
- Horizonte dividido y envenenamiento en reversa de trayectoria.
- Etiquetas de ruta.
- zLa siguiente tabla muestra los cambios realizados al protocolo RIP:

Tabla 8. Cambios y Nuevas Características de RIPng

| Característica | Descripción |
|----------------------------|---|
| Rutas Anunciadas | RIPng anuncia rutas IPv6 compuestas de prefijos IPv6 con longitud y métrica. |
| Siguiente Salto | La dirección de Siguiente Salto es la dirección de enlace local IPv6 de la interfase del ruteador que anuncia el prefijo. |
| Transporte de Protocolo IP | IPv6 es utilizado para llevar datagramas RIP usando UDP como protocolo de transporte. |
| Dirección IPv6 Fuente | La actualización RIP de la dirección fuente IPv6 es la dirección de enlace-local de la interfase del ruteador fuente. Con excepción de cuando se contesta un Mensaje de Solicitud unicast desde un puerto distinto al puerto RIPng, en dicho caso, la dirección fuente es una dirección global válida). |
| Dirección IPv6 Destino | La dirección destino de la actualización RIP es FF02::9, que es la dirección multidifusión de todos los ruteadores RIP. Únicamente los ruteadores RIPng atienden esta dirección multidifusión. Es una dirección multidifusión con alcance de enlace-local, la cual no es retransmitida a otros enlaces. |
| Límite de Salto = 255 | Las actualizaciones RIP tienen el Límite de Salto de paquete IPv6 configurado en 255. Esto permite a los involucrados verificar si las actualizaciones vienen de ruteadores externos falsos. |
| Número de Puerto = 521 | El puerto UDP es 521, en lugar de 520 para RIPv1 y 2. |
| RIPng versión = 1 | El número de versión RIPng en el paquete RIP es 1, lo que representa que es la primera versión de RIPng. Se utiliza un puerto de transporte distinto. Los involucrados pueden diferenciar entre paquetes RIPv1, RIPv2 y RIPng. |
| Tabla de Enrutamiento | La tabla de enrutamiento de Pv6 es distinta de la tabla de enrutamiento de IPv4 para RIPv1 o RIPv 2. La ruta por omisión es anunciada como ::/0. |
| Autenticación | La autenticación RIPng se basa en la seguridad proveída por IPsec. |

Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

OSPF – (RFC 2328). Como versión 2, es un protocolo sólo para IPv4. OSPFv3 (RFC 2740) es un protocolo de red independiente, similar a IS-IS. De esta manera puede incluir rutas IPv6. OSPFv3 comparte los fundamentos de OSPFv2:

- Inundación (flooding).
- Elección de ruteador designado.
- Área de soporte.

- Cálculos de Dijkstra para abrir la trayectoria más corta primero.
- Soporte de circuito en demanda.
- Áreas Stub y NSSA.
- Extensiones multidifusión (MOSPF).

Tabla 9. Cambios y Nuevas Características de OSPFv3

| Características | Descripción |
|--|--|
| LSAs de ruteador y red | Estos no tienen semántica de direccionamiento y sólo llevan información de topología. |
| Nuevo LSA-con-Prefijo-Intra-Area | Este lleva direcciones y prefijos IPv6. |
| Direcciones en LSA | Estas son descritas como prefijo con una longitud de prefijo. La ruta por omisión es ::/0. |
| Identificación de Ruteador | ID del Ruteador es un valor de 32 bit sin importar si es dirección IPv4 o IPv6. Se usa en DR, BDR, LSAs, base de datos. |
| Alcance de la Inundación | Enlace, Area o AS. |
| Siguiente-Salto | La dirección de Siguiente-Salto es la dirección de enlace-local IPv6 de la interfase de ruteador que anuncia el prefijo. |
| Nuevo LSA de Enlace-Local | Este lleva la dirección de enlace local de la interfase de ruteador, los prefijos del enlace y las opciones. |
| Ejecución por cada enlace, en lugar de cada IP de subred | Ahora una interfase OSPF se puede conectar a un enlace en lugar de una subred IP. Están soportadas múltiples instancias en un enlace sencillo. |
| Usa IPv6 para el transporte de paquetes OSPF | Encabezado Siguiente = 89 para identificar un paquete IPv6 OSPFv3. |
| Paquetes OSPF con dirección IPv6 fuente | La dirección fuente del paquete OSPF es la dirección enlace-local de la interfase del ruteador origen. |
| Paquetes OSPF con dirección IPv6 destino | Todos los ruteadores OSPF envían paquetes Hello y atienden a FF02::5, que es la dirección multidifusión con enlace a todos-los-ruteadores-ospf. |
| Límite de Salto = 1 de paquetes OSPF | 1 significa de enlace-local. |
| OSPF versión = 3 | Versiones previas son iguales a 1 o 2. |
| La Autenticación es realizada con IPSec | Se quitaron todos los datos de autenticación interna OSPF y ahora se provee seguridad con IPSec para proteger la integridad y ofrecer autenticación. |

Fuente: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

3.2.1 Qué es la transición a IPv6. No se trata de una migración como erróneamente se indica en muchas ocasiones, sino que ambos protocolos, IPV4 e IPV6, existirán durante algún tiempo, es decir se produce una coexistencia.

Teniendo en cuenta que Internet se encuentra implementado en su totalidad por el protocolo IPV4, y que su uso es muy frecuente e importante en todo el mundo, no sería posible su sustitución inmediata, es decir no es posible apagar la Red, ni siquiera por un par de minutos para realizar la transición a IPV6.

No es suficiente con actualizar parte de los equipos, es un proceso que tendría que involucrar a cualquier organización, sea empresa, administración pública o proveedor de acceso o contenidos de una forma sincronizada, lo cual es imposible.

Precisamente por ello, la organización encargada de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), diseñó junto con el propio IPV6, una serie de mecanismos que llamamos de transición y coexistencia.

Es importante entender lo que ello implica. No se trata de una migración como erróneamente se indica en muchas ocasiones, sino que ambos protocolos, IPV4 e IPV6, existirán durante algún tiempo, es decir se produce una coexistencia. Es como una balanza, en la que hoy en día el lado con el mayor peso representa el tráfico IPV4, pero poco a poco, gracias a esta coexistencia, conforme más contenidos y servicios estén disponibles con IPV6, el peso bascula hacia el otro lado hasta que IPV6 sea predominante. Esto es lo que llamamos la transición.

El diseño del protocolo IPV6 da preferencia a IPV6 frente a IPV4, si ambos están disponibles (IPV4 e IPV6). De ahí que se produzca ese desplazamiento del peso en "nuestra balanza", de una forma natural, en función de múltiples factores, y sin que podamos determinar durante cuánto tiempo seguirá existiendo IPV4 en la Red y en qué proporciones. Posiblemente podamos pensar, intentando mirar en la bola de cristal, que IPV6 llegará a ser predominante en 3-4 años, y en ese mismo entorno de tiempo, IPV4 desaparecerá de Internet, al menos en muchas partes de ella.

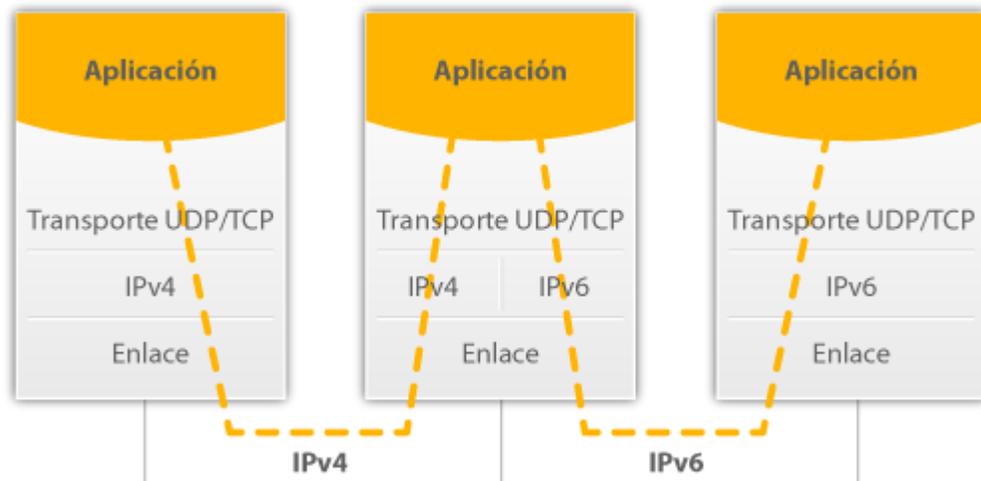
Es importante recordar que el 3 de Febrero de 2011 se agotaron las direcciones IPV4 en el registro central de IANA (Autoridad de Asignación de Números en Internet), por lo que los proveedores de servicios de Internet están acelerando el despliegue de IPV6 en sus redes para que tanto los nuevos usuarios como los existentes sigan disfrutando de un uso habitual y continuado de Internet.

3.2.2 Tunels

Dual stack o pila doble

Es el método propuesto originalmente para tener una transición suave hacia IPv6. En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red.

Figura 6. Dual stack o pila doble



Fuente: <http://portalipv6.lacnic.net/mecanismos-de-transicion/>

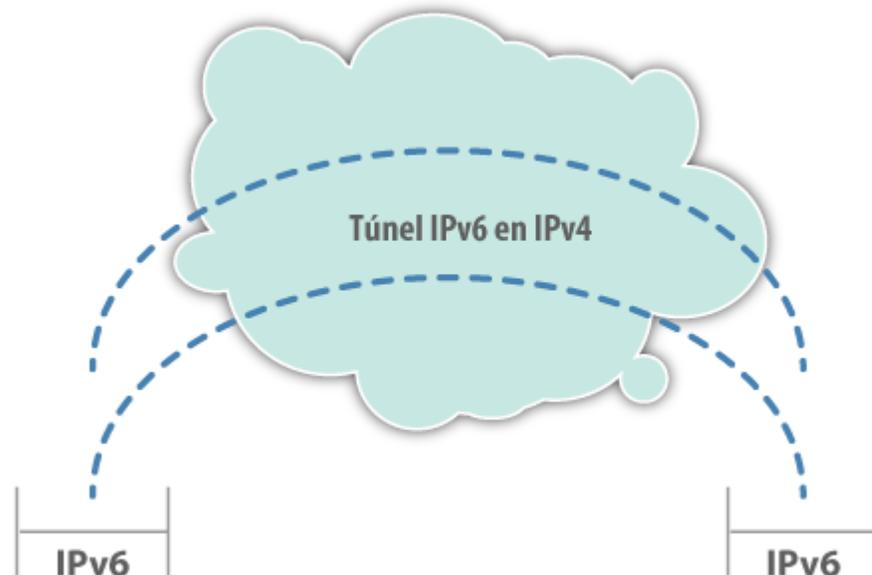
De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se

preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4 (si bien esto se ha ido modificando para solucionar problemas de timeouts, ver “happy eyeballs”).

Túneles/Encapsulamiento

Es uno de los mecanismos mas antiguos para poder atravesar redes que no tienen soporte nativo del protocolo que se está utilizando. En general se utilizan túneles encapsulando IPv6 dentro de IPv4, permitiendo de esta forma atravesar redes que no manejan IPv6, pero también podemos encontrar la situación inversa. Los paquetes originales son transportados hasta un punto de la red por medio del protocolo original, luego encapsulados para atravesar la porción de red que no lo soporta y luego des-encapsulados en el otro extremo para ser enviados al destino final en forma nativa.

Figura 7. Túnel IPV6 en IPV4.

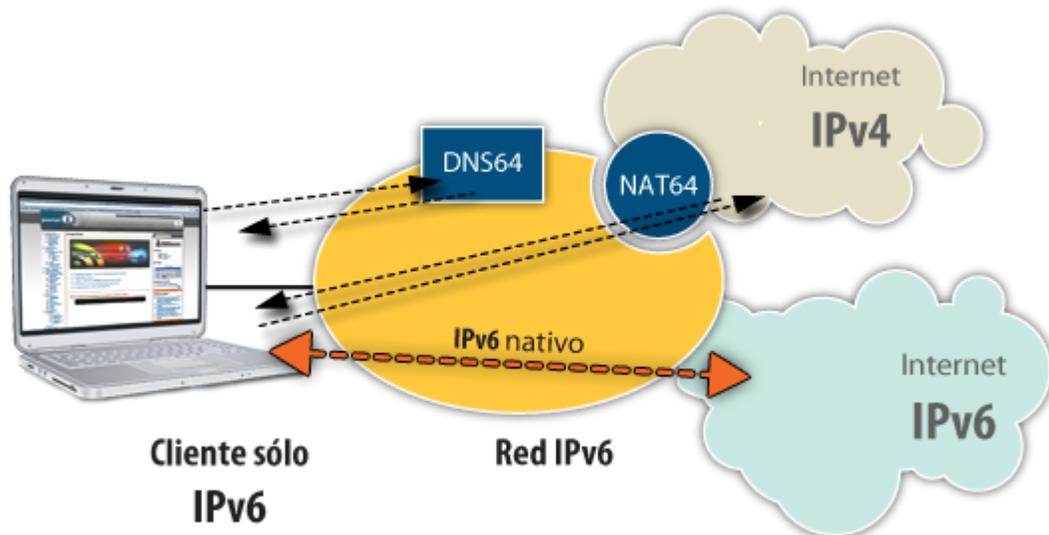


Fuente: <http://portalipv6.lacnic.net/mecanismos-de-transicion/>

Los túneles más habituales son los túneles manuales y los túneles automáticos. Los túneles manuales se deben configurar explícitamente en algún equipo de la red, mientras que los automáticos se configuran automáticamente en algunos sistemas operativos. En el caso de los primeros, podemos citar los túneles manuales entre dos equipos o mediante “tunnel brokers”. En el segundo caso, los más conocidos son 6to4 y Teredo.

Dentro de los mecanismos de encapsulado podemos mencionar también la técnica conocida como 6PE/6VPE, que se utiliza para encapsular el tráfico IPv6 por parte de carriers que tienen redes MPLS.

Figura 8. Red IPv6.



Fuente: <http://portalipv6.lacnic.net/mecanismos-de-transicion/>

Vale la pena mencionar que una de las propuestas iniciales de mecanismos de traducción fue NAT-PT (RFC 2766), que al día de hoy ha sido desaconsejado

debido a sus fallas (ver RFC 4966) y ha sido reclasificado como “histórico” por la IETF.

Guillermo Cicileo

Referencias:

Técnicas de Transição IPv6 – parte 01 (Túneis)

Técnicas de Transição IPv6 – parte 02 (NAT444)

Técnicas de Transição IPv6 – parte 03 (NAT64, DNS64 e 464XLAT)

Pila doble y túneles, mecanismos básicos de traducción: RFC4213

Teredo RFC4380, 6to4 RFC3056, tunnel broker RFC3053, MPLS 6PE RFC4798

Traducción, NAT64 y DNS64: RFC6144, RFC6145, RFC6146, RFC6052, RFC6147

Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment:

RFC6180

Presentación de Antonio Moreiras en

LACNICXVII:https://www.dropbox.com/s/6rs1ci17bpsirax/Moreiras_IPv6.pdf

3.2.3 Protocolos para IPV6

Protocolo de configuración dinámica de host v6

SLAAC y DHCPv6

De manera similar a lo que ocurre con IPv4, las direcciones IPv6 de unidifusión global pueden configurarse manualmente o de forma dinámica. Sin embargo, existen dos métodos en los que las direcciones IPv6 de unidifusión global pueden asignarse dinámicamente:

Configuración automática de dirección sin estado (SLAAC), como se muestra en la ilustración.

Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

Introducción a SLAAC.

SLAAC es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP:

Mensaje de solicitud de router (RS): cuando un cliente está configurado para obtener la información de direccionamiento de forma automática mediante SLAAC, el cliente envía un mensaje RS al router. El mensaje RS se envía a la dirección IPv6 de multidifusión de todos los routers, FF02::2.

Mensaje de anuncio de router (RA): los routers envían mensajes RA para proporcionar información de direccionamiento a los clientes configurados para obtener sus direcciones IPv6 de forma automática. El mensaje RA incluye el prefijo y la longitud de prefijo del segmento local. Un cliente utiliza esta información para crear su propia dirección IPv6 de unidifusión global. Los routers envían mensajes RA de forma periódica o en respuesta a un mensaje RS. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos. Los mensajes RA siempre se envían a la dirección IPv6 de multidifusión de todos los nodos, FF02::1.

Como lo indica el nombre, SLAAC quiere decir “sin estado”. Un servicio sin estado significa que no hay ningún servidor que mantenga la información de la dirección de red. A diferencia de DHCP, no hay servidor de SLAAC que tenga información

acerca de cuáles son las direcciones IPv6 que están en uso y cuáles son las que se encuentran disponibles.

Protocolo de configuración dinámica de host v6

SLAAC y DHCPv6

La decisión de si un cliente se configura para obtener su información de direccionamiento IPv6 de forma automática mediante SLAAC, mediante DHCPv6 o mediante una combinación de ambos depende de la configuración dentro del mensaje RA. Los mensajes RA ICMPv6 contienen dos indicadores para señalar cuál es la opción que debe utilizar el cliente.

Los dos indicadores son el indicador de configuración de dirección administrada (indicador M) y el indicador de otra configuración (indicador O).

Mediante distintas combinaciones de los indicadores M y O, los mensajes RA tienen una de tres opciones de direccionamiento para el dispositivo IPv6, como se muestra en la ilustración:

SLAAC (anuncio de router solamente)

DHCPv6 sin estado (anuncio de router y DHCPv6)

DHCPv6 con estado (DHCPv6 solamente)

Independientemente de la opción que se utilice, en RFC 4861 se recomienda que todos los dispositivos IPv6 realicen la detección de direcciones duplicadas (DAD) en cualquier dirección de unidifusión, entre las que se incluyen las direcciones configuradas mediante SLAAC o DHCPv6.

Nota: aunque el mensaje RA especifique el proceso que debe utilizar el cliente para obtener una dirección IPv6 de forma dinámica, el sistema operativo cliente

puede elegir omitir el mensaje RA y utilizar los servicios de un servidor de DHCPv6 exclusivamente.

Protocolo de configuración dinámica de host v6

SLAAC y DHCPv6

Opción de SLAAC (anuncio de router solamente)

SLAAC es la opción predeterminada en los routers Cisco. Tanto el indicador M como el indicador O están establecidos en 0 en el RA, como se muestra en la ilustración.

Esta opción le indica al cliente que utilice la información que se incluye en el mensaje RA de manera exclusiva. Esto incluye información del prefijo, de la longitud de prefijo, del servidor DNS, de la MTU y del gateway predeterminado. No se encuentra disponible ninguna otra información de un servidor de DHCPv6. La dirección IPv6 de unidifusión global se crea combinando el prefijo del mensaje RA y la ID de interfaz mediante EUI-64 o mediante un valor generado aleatoriamente. Los mensajes RA se configuran en una interfaz individual de un router. Para volver a habilitar una interfaz para SLAAC que pudo haberse establecido en otra opción, se deben restablecer los indicadores M y O a sus valores iniciales de 0. Esto se realiza mediante los siguientes comandos del modo de configuración de interfaz:

```
Router(config-if)# no ipv6 nd managed-config-flag
```

```
Router(config-if)# no ipv6 nd other-config-flag
```

Protocolo de configuración dinámica de host v6

SLAAC y DHCPv6

Si bien DHCPv6 es similar a DHCPv4 en cuanto a lo que proporciona, los dos protocolos son independientes respecto sí. DHCPv6 se define en RFC 3315. Se

trabajó mucho en esta especificación a través de los años, como lo indica el hecho de que RFC DHCPv6 tiene el número de revisión más alto que cualquier borrador de Internet.

Opción de DHCPv6 sin estado (anuncio de router y DHCPv6)

La opción de DHCPv6 sin estado informa al cliente que utilice la información del mensaje RA para el direccionamiento, pero que hay más parámetros de configuración disponibles de un servidor de DHCPv6.

Mediante el prefijo y la longitud de prefijo en el mensaje RA, junto con EUI-64 o una IID generada aleatoriamente, el cliente crea la dirección IPv6 de unidifusión global.

A continuación, el cliente se comunica con un servidor de DHCPv6 sin estado para obtener información adicional que no se proporciona en el mensaje RA. Puede tratarse de una lista de direcciones IPv6 del servidor DNS, por ejemplo. Este proceso se conoce como DHCPv6 sin estado, debido a que el servidor no mantiene información de estado del cliente (es decir, una lista de direcciones IPv6 asignadas y disponibles). El servidor de DHCPv6 sin estado solo proporciona parámetros de configuración para los clientes, no direcciones IPv6.

Para DHCPv6 sin estado, el indicador O se configura en 1 y el indicador M se deja en la configuración predeterminada de 0. El valor 1 del indicador O se utiliza para informarle al cliente que hay información de configuración adicional disponible de un servidor de DHCPv6 sin estado.

Para modificar el mensaje RA enviado en la interfaz de un router e indicar DHCPv6 sin estado, utilice el siguiente comando:

```
Router(config-if)# ipv6 nd other-config-flag
```

4. IMPLEMENTACION DEL PROYECTO

4.1 MATERIALES

Los materiales que usaron en el desarrollo de la Monografía fueron los emuladores GNS3, el programa Virtual Box y el sistema operativo Linux Centos 7.

ESPECIFICACIONES DEL PC

Intel Core i5 Tercera Generación, Memoria RAM 16GB, Tarjeta de Video de 2gb.

Sistema Operativo es Windows Seven Ultimate Service Pack 1 en donde se corre el programa GNS3.

Los nombres de los Router o switch son:

.Router: C7200.

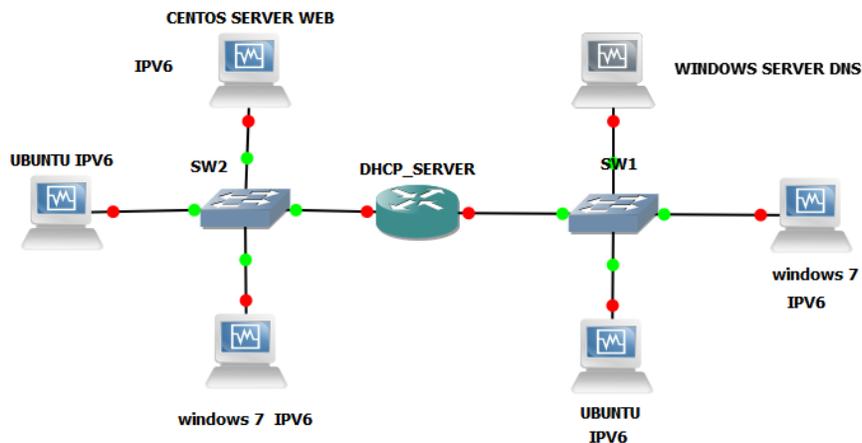
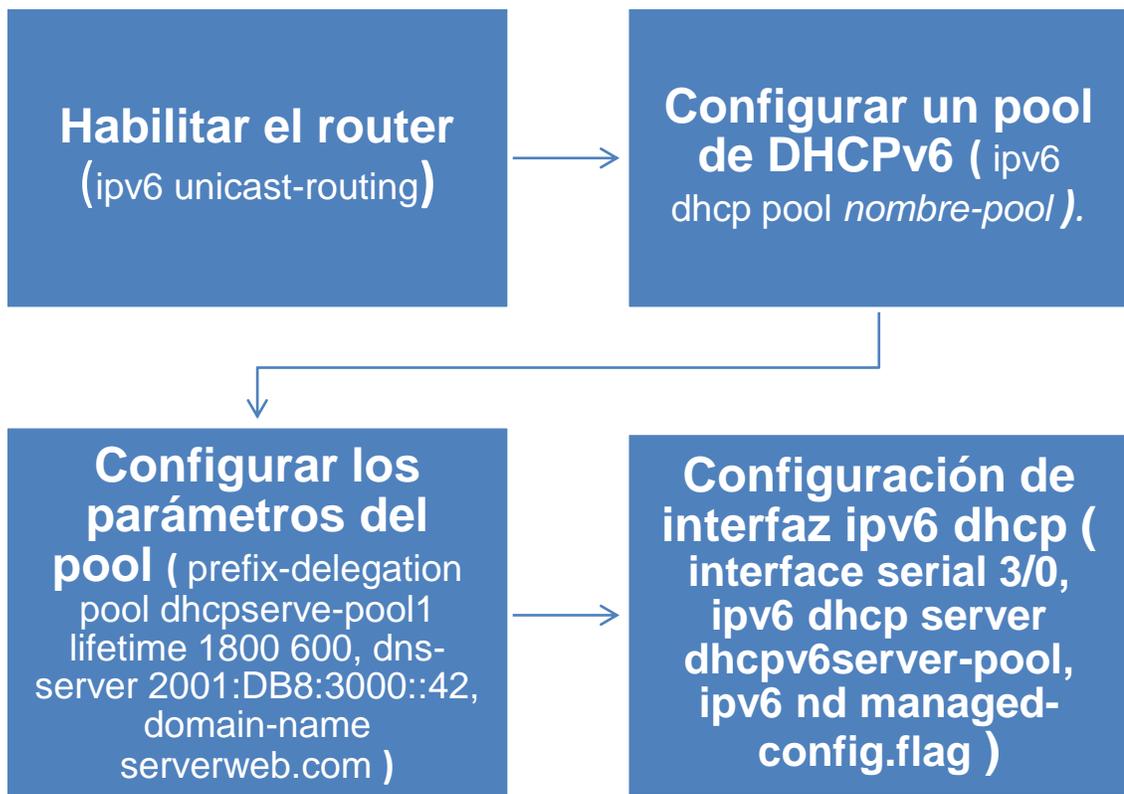
.Switch: C3725.

Oracle VM VirtualBox:

Sistema Operativo: Centos7.

4.2 METODOLOGÍA

Figura 9. Configuración de DHCP IPV6.



4.2.1 Manual de instalación de IOS en GNS3.

Figura 10. Iniciamos el programa GNS3.

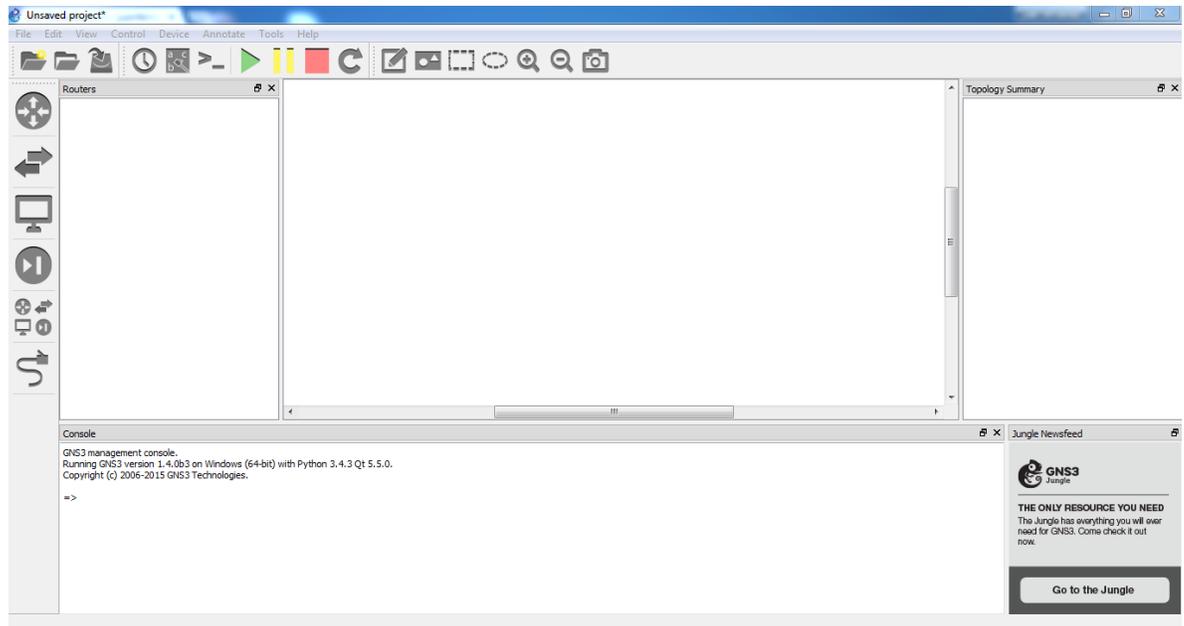


Figura 11. Después entramos a la opción Edit y después a la opción preferences.

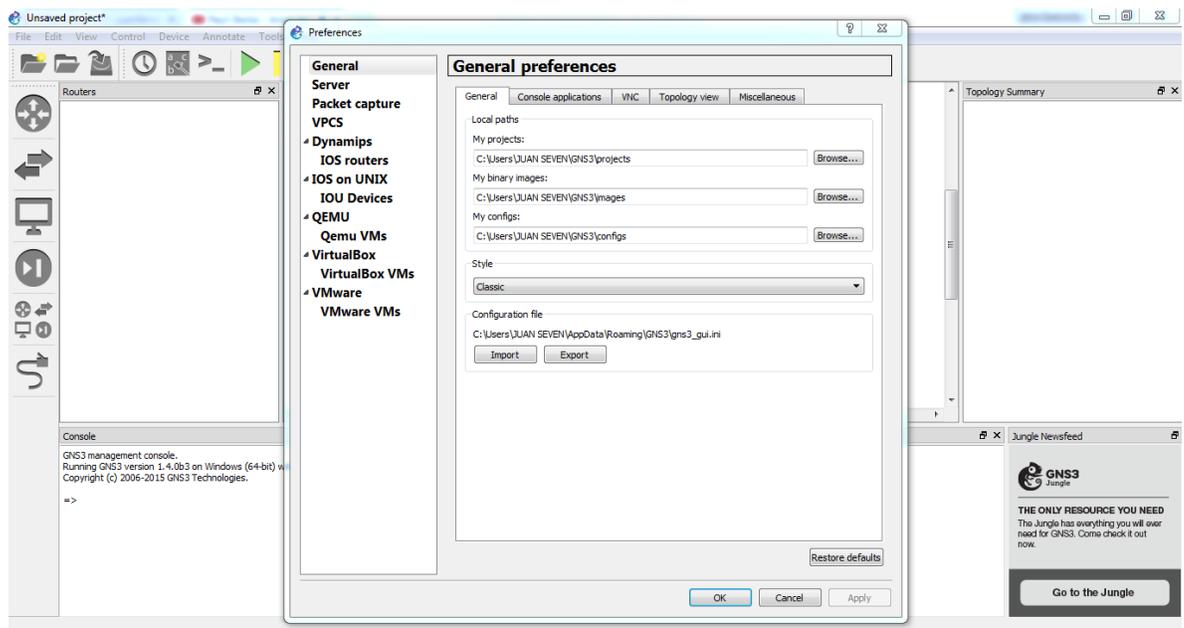


Figura 12. Después vamos a la opción IOS routers para poderlas agregarlas.

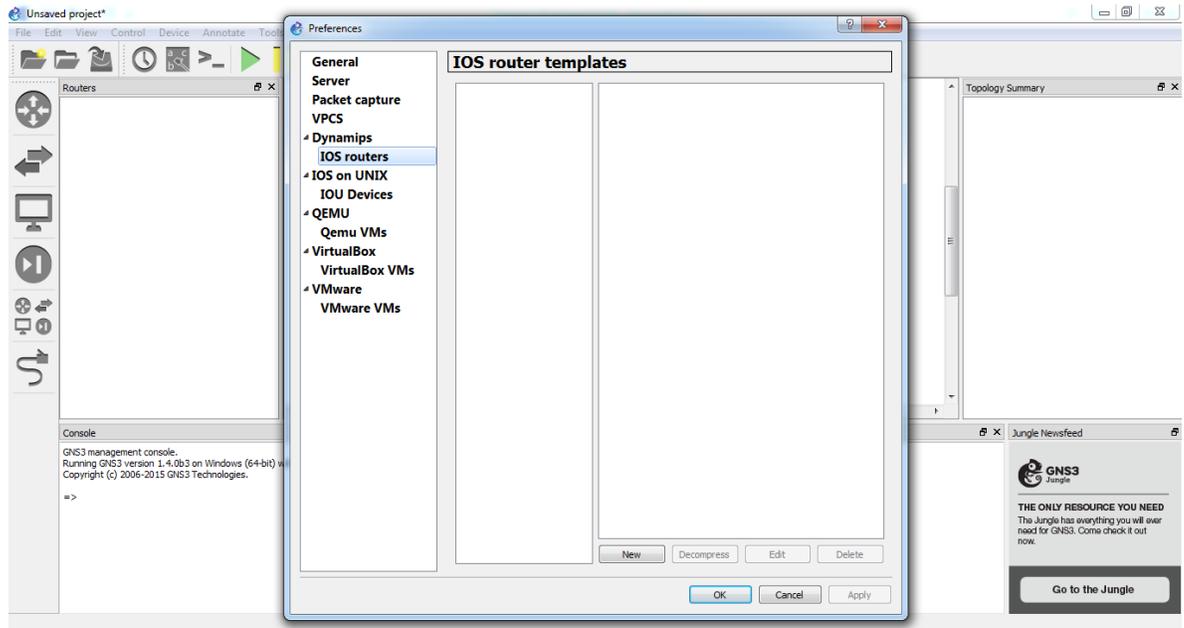


Figura 13. Después vamos a la opción New y como es la primera que agregamos la IOS seleccionamos la opción New Image.

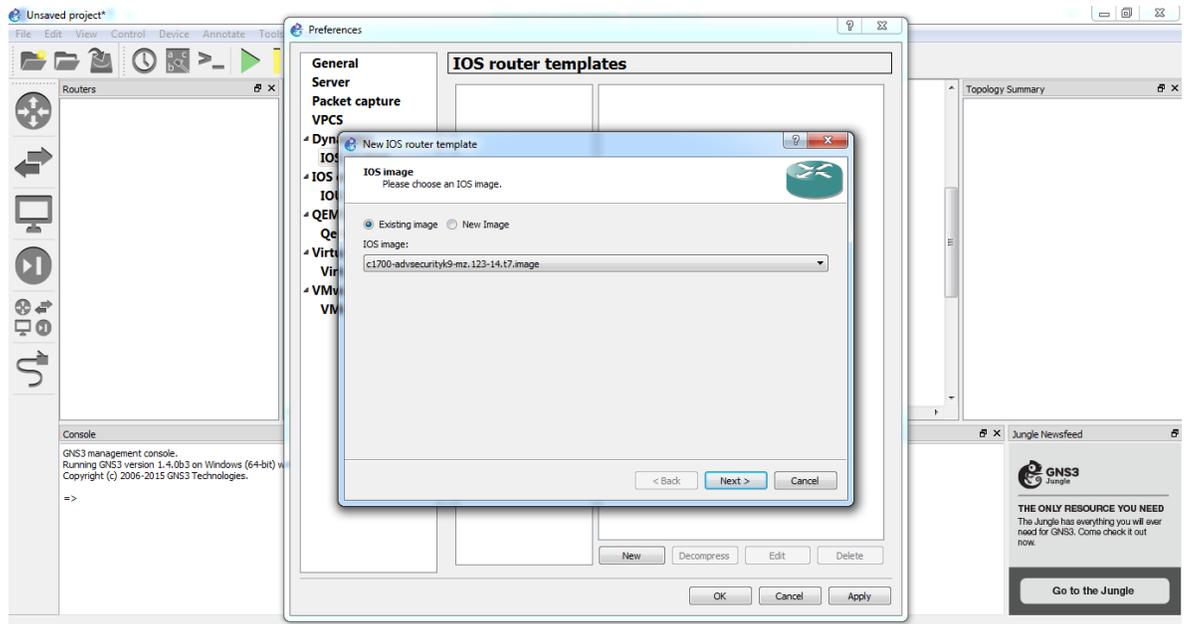


Figura 14. Después vamos a la opción Browse y buscamos la IOS que deseamos instalar.

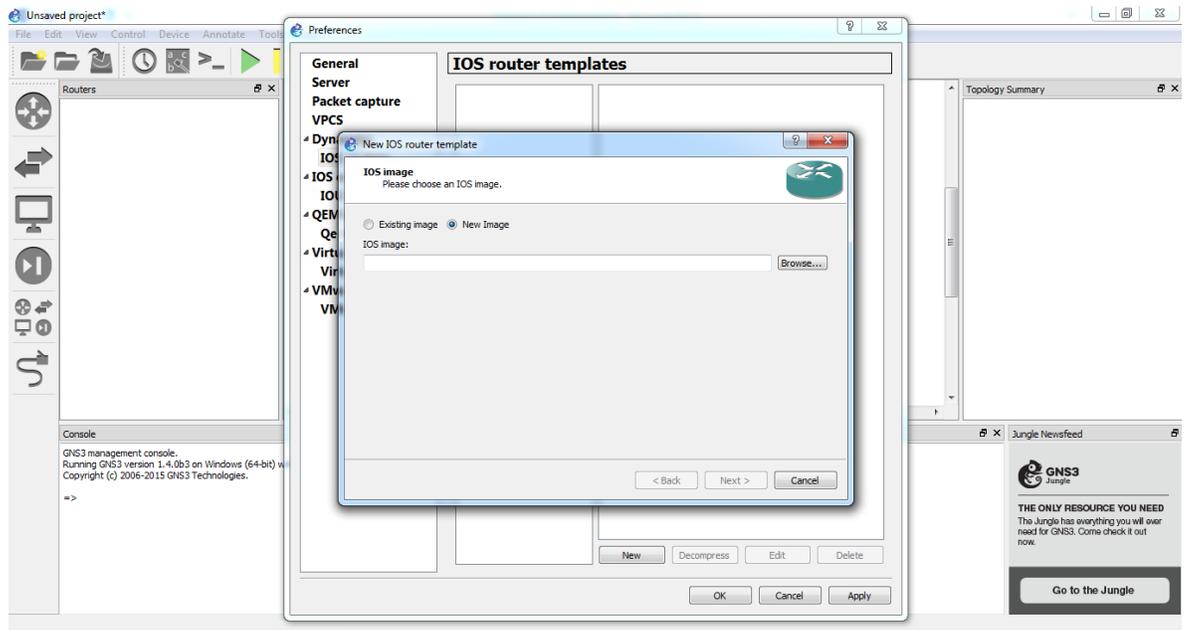


Figura 15. Buscamos donde tenemos la IOS guardada y le damos el click en Abrir.

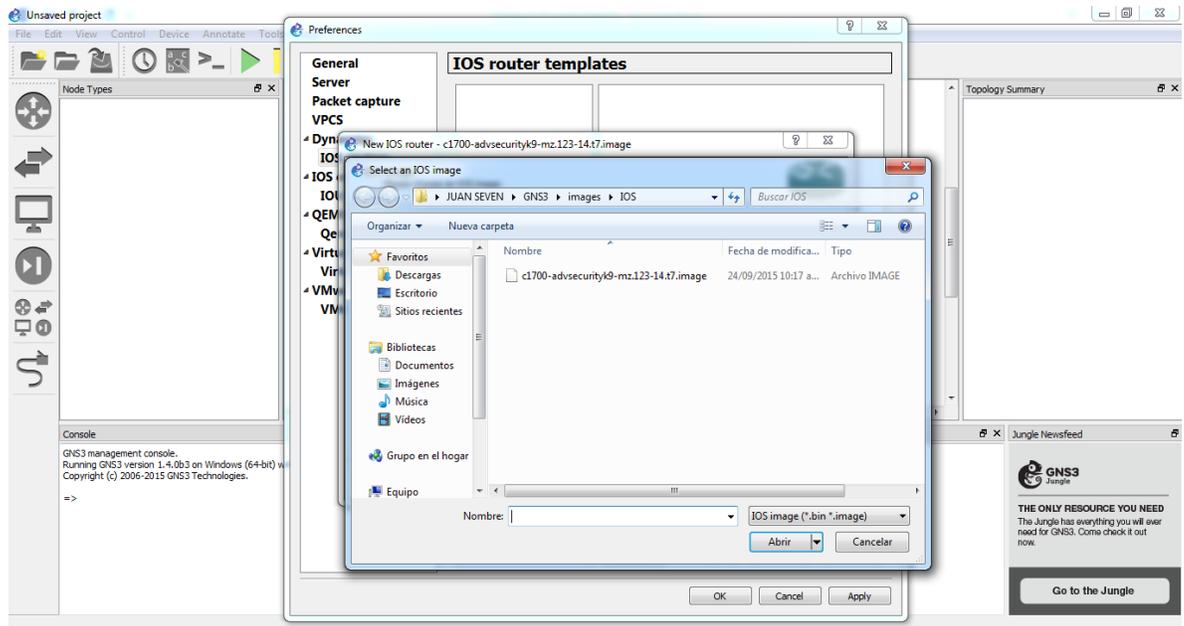


Figura 16. Le damos el nombre del Router que vas a instalar y le damos Next.

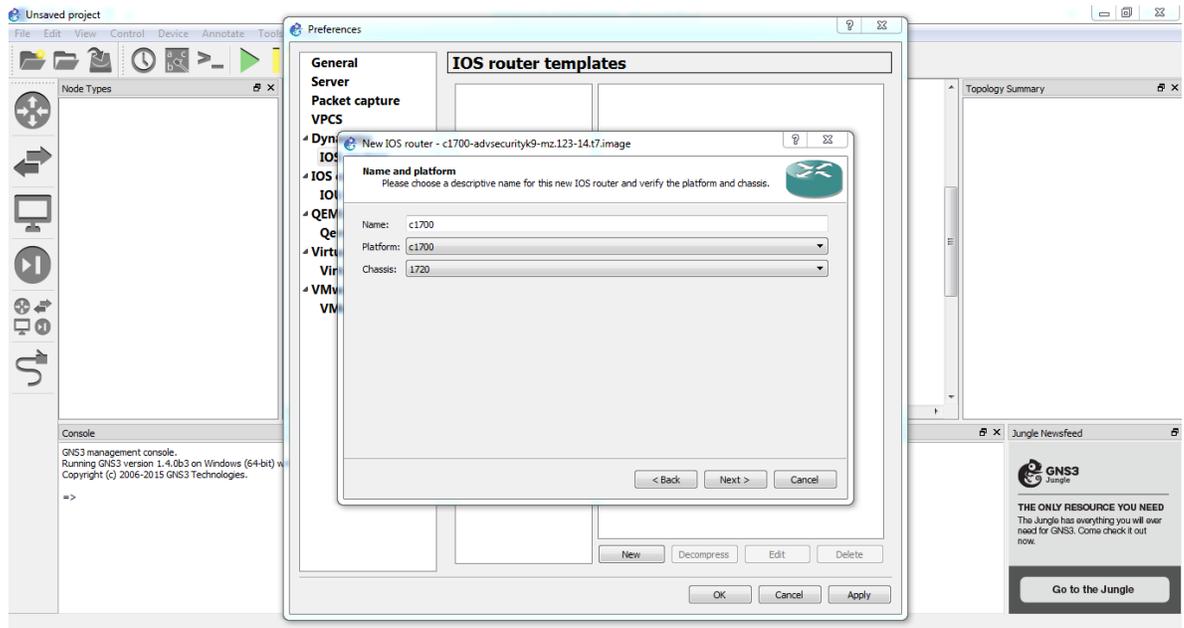


Figura 17. Dejamos la memoria RAM en Default y le damos click en Next.

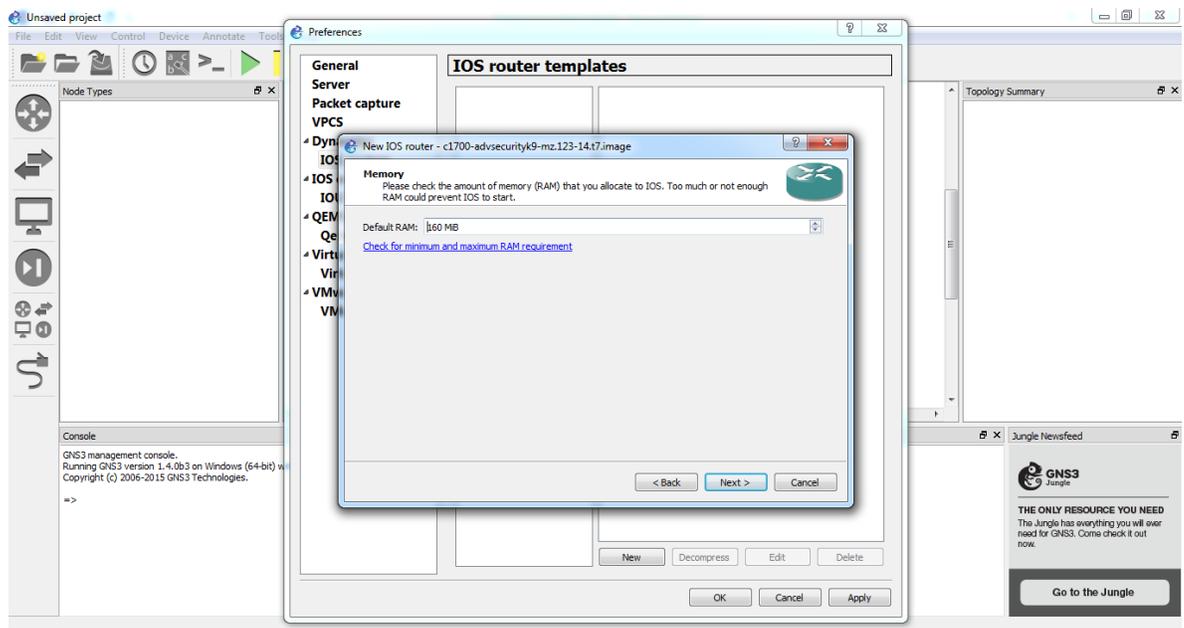


Figura 18. Es opción de configurar internamente en el Router los dispositivos que vamos a usar, le damos Next.

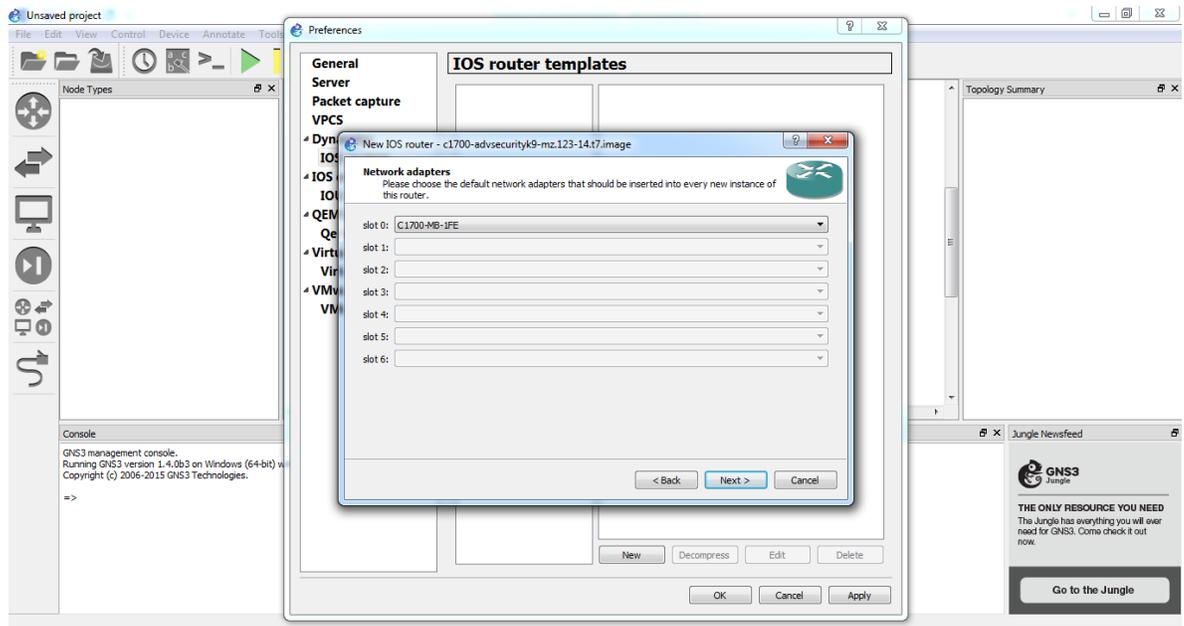


Figura 19. Esta opción es para configurar las consolas internas del Router que estamos configurando, le damos click en Next.

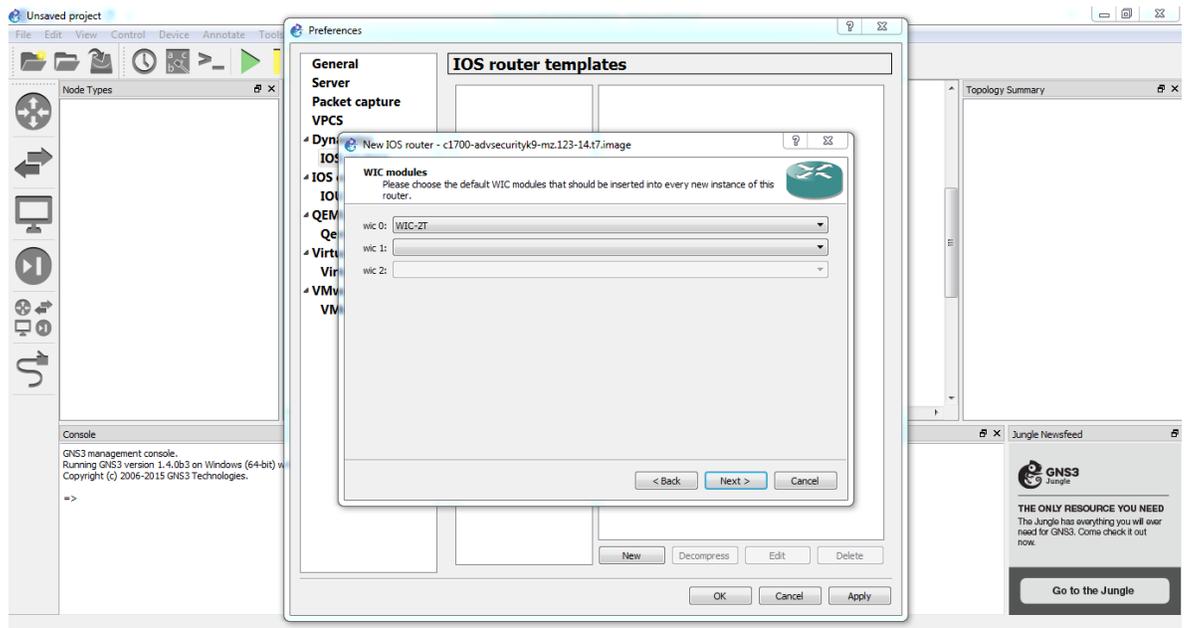


Figura 20. Le damos click en Finish.

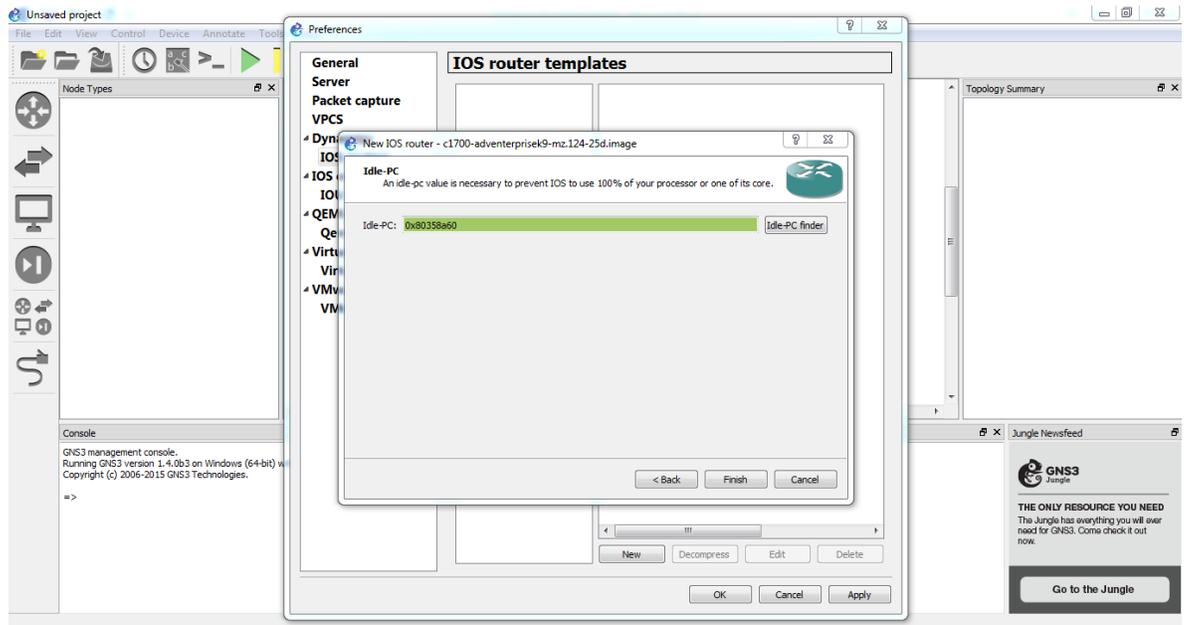


Figura 21. Nos aparecerá esta ventana le damos click en Apply y después en OK.

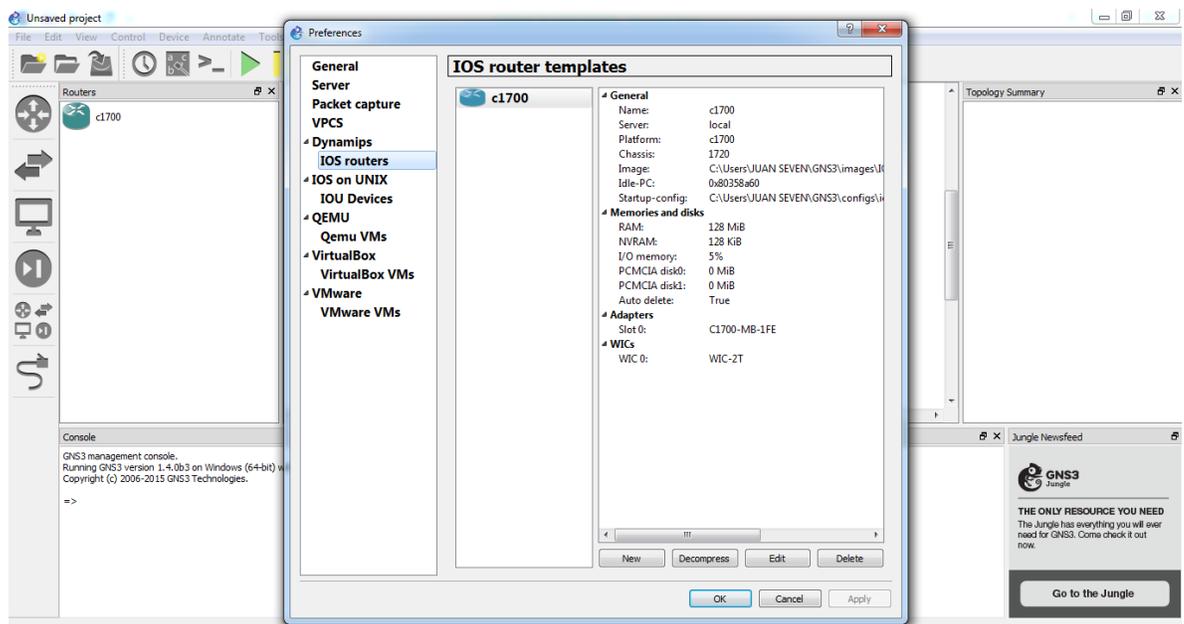
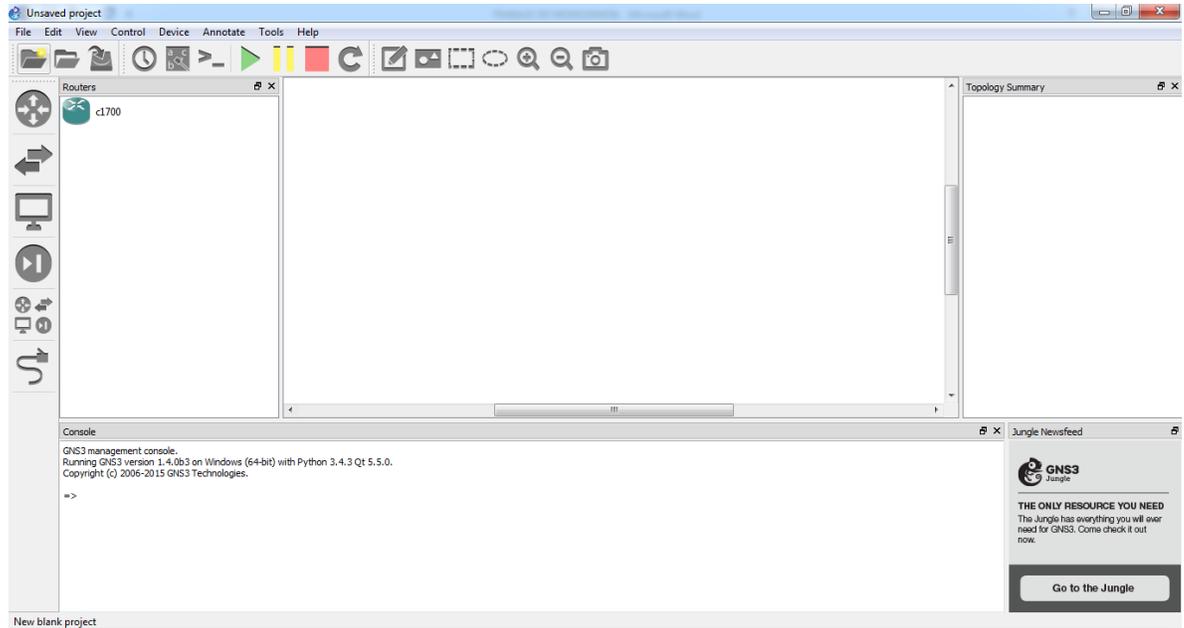


Figura 22. Vamos en el icono del Router y hay aparecerá el Router que acabamos de instalar y así hacemos con todas las IOS de Router que vayamos a instalar.



4.2.2 Manual de instalación de Linux Centos 7 en VirtualBox.

Figura 23. Abrimos el programa VirtualBox, después le damos la opción Nueva.

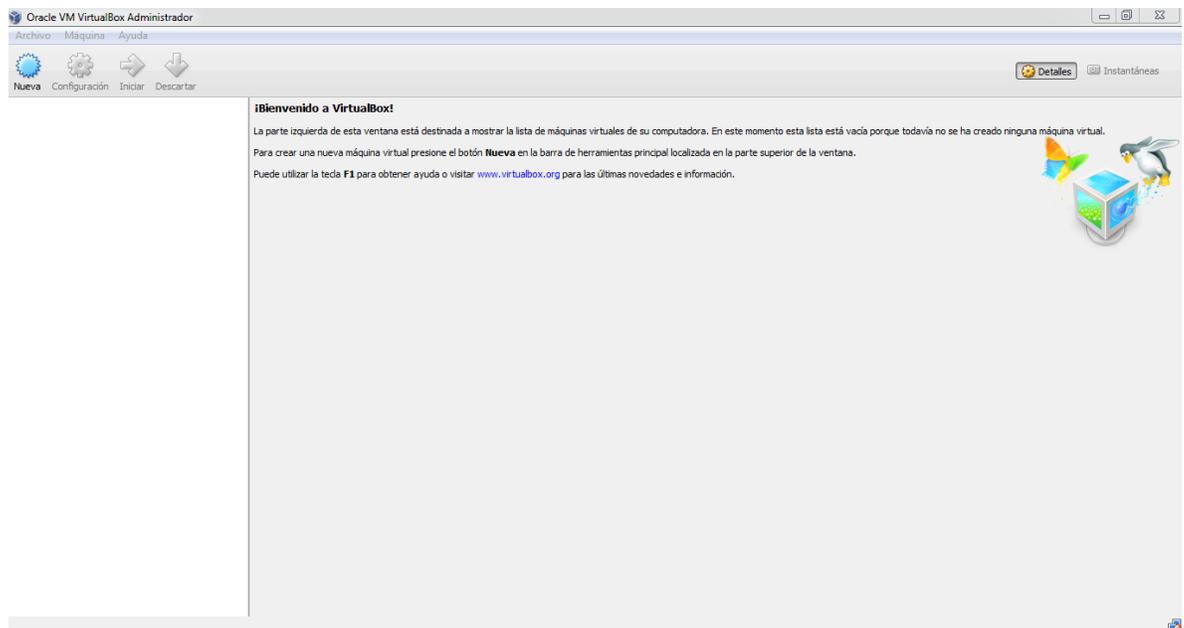


Figura 24. Nos pliega una ventana seleccionamos las siguientes opciones y después le damos NEXT.

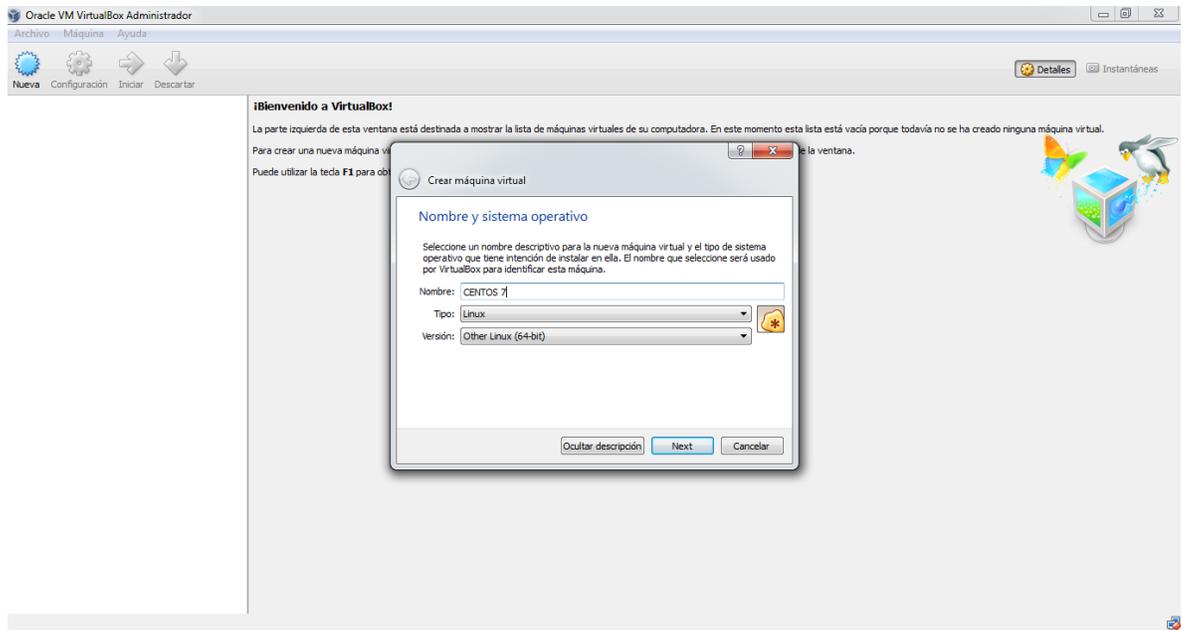


Figura 25. Aquí seleccionamos la memoria RAM que queremos para nuestro Linux Centos 7 y después le damos a la opción NEXT.

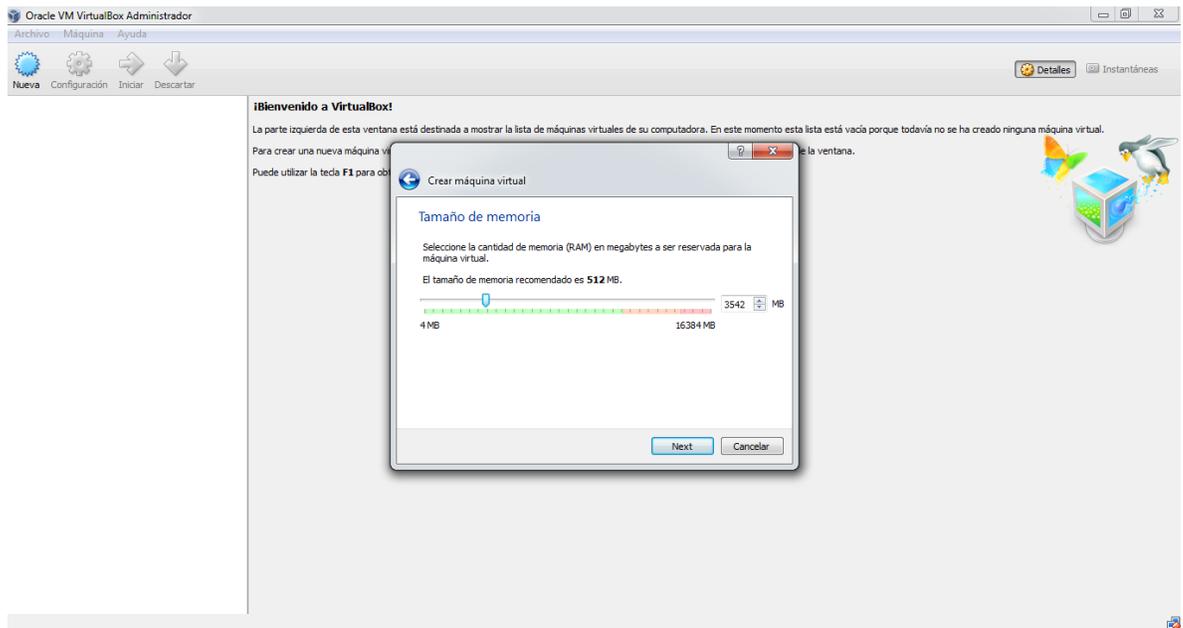


Figura 26. En esta nueva ventana vamos a crear el disco duro para el sistema operativo Linux Centos 7 y después le damos CREAM.

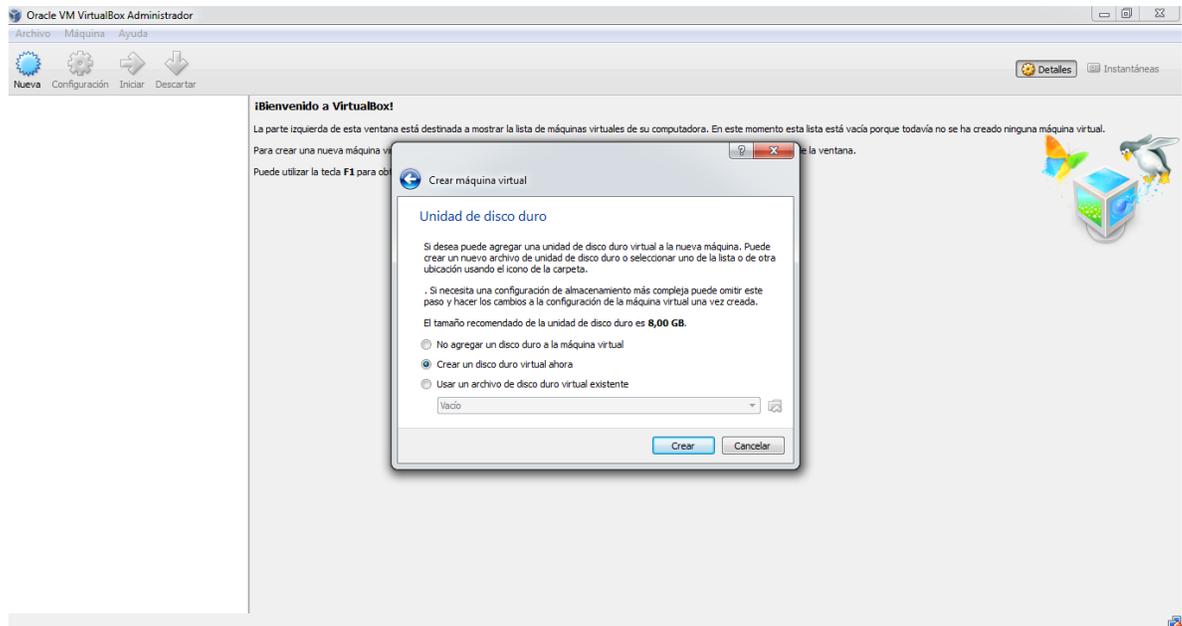


Figura 27. En esta nueva ventana dejamos por defecto la opción y le damos en la opción NEXT.

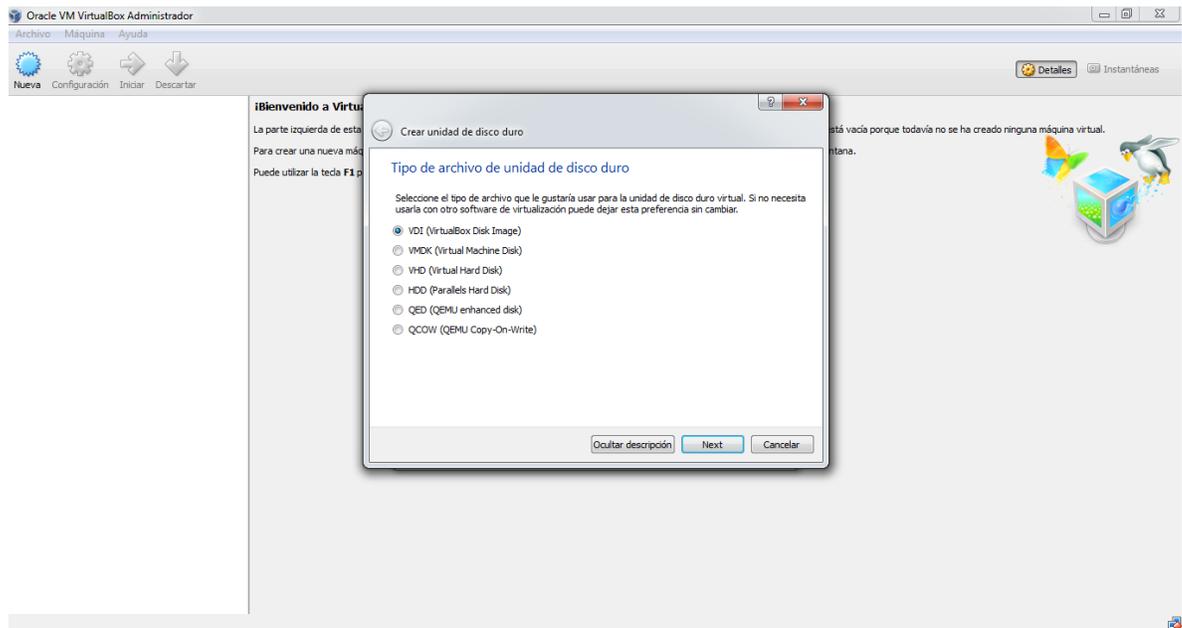


Figura 28. En esta nueva ventana vamos a dejar por defecto y le damos en la opción NEXT.

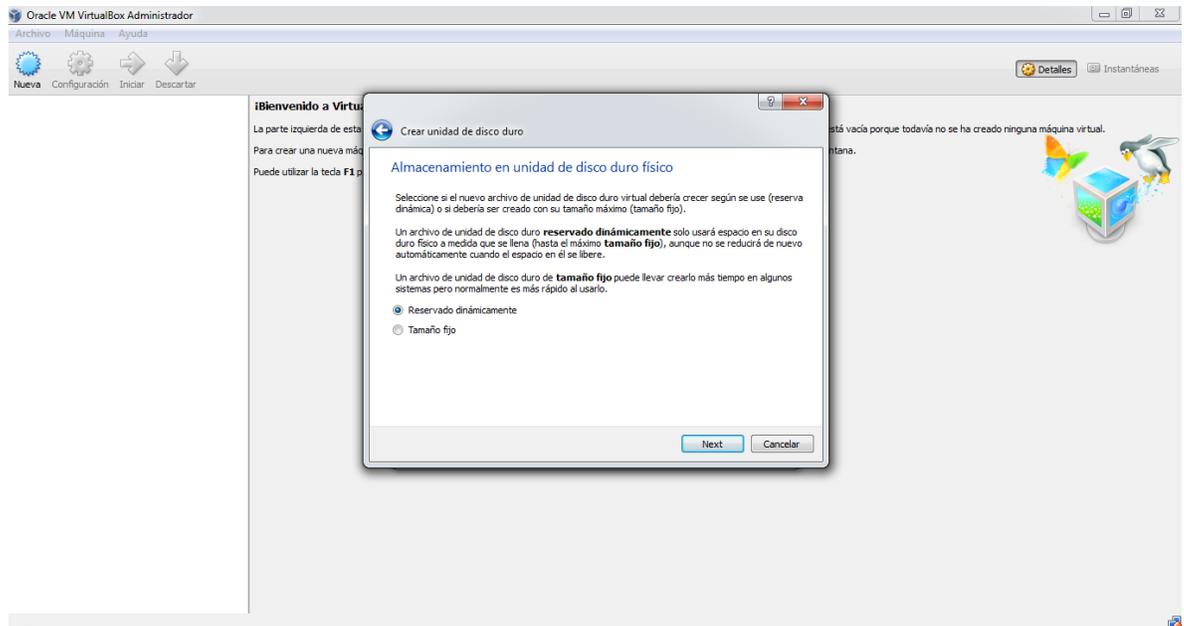


Figura 29. En esta nueva ventana vamos a cambiar el tamaño del disco duro de 8gb a 20gb y le damos en la opción CREAR.

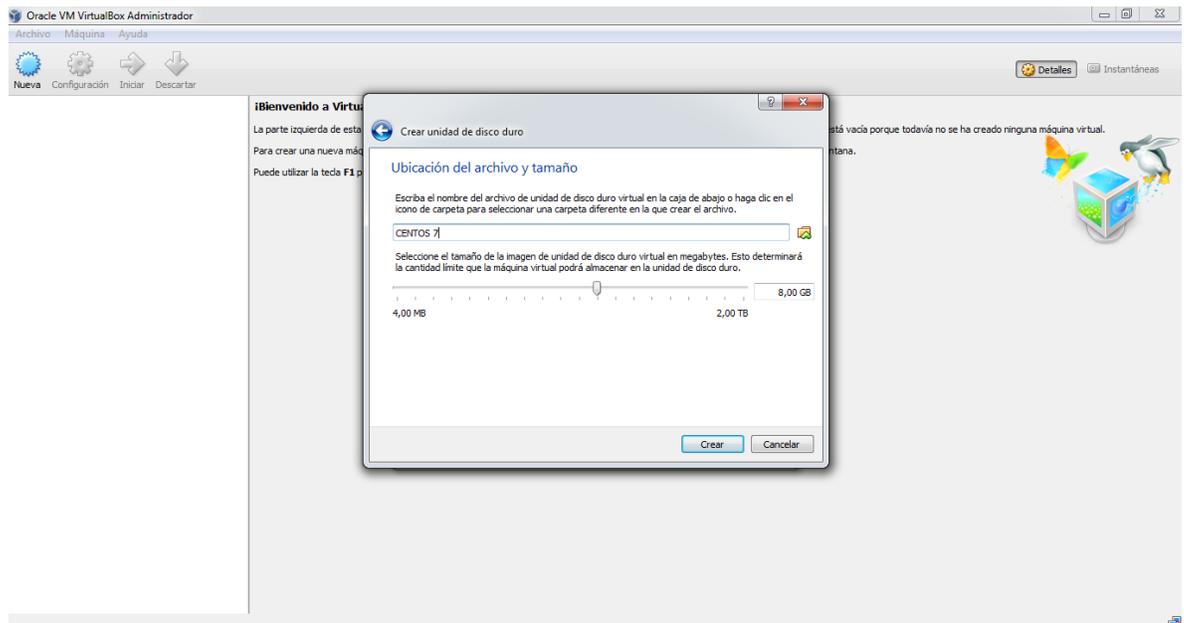


Figura 30. Finalizando ya la configuración para después crear el sistema operativo Linux.

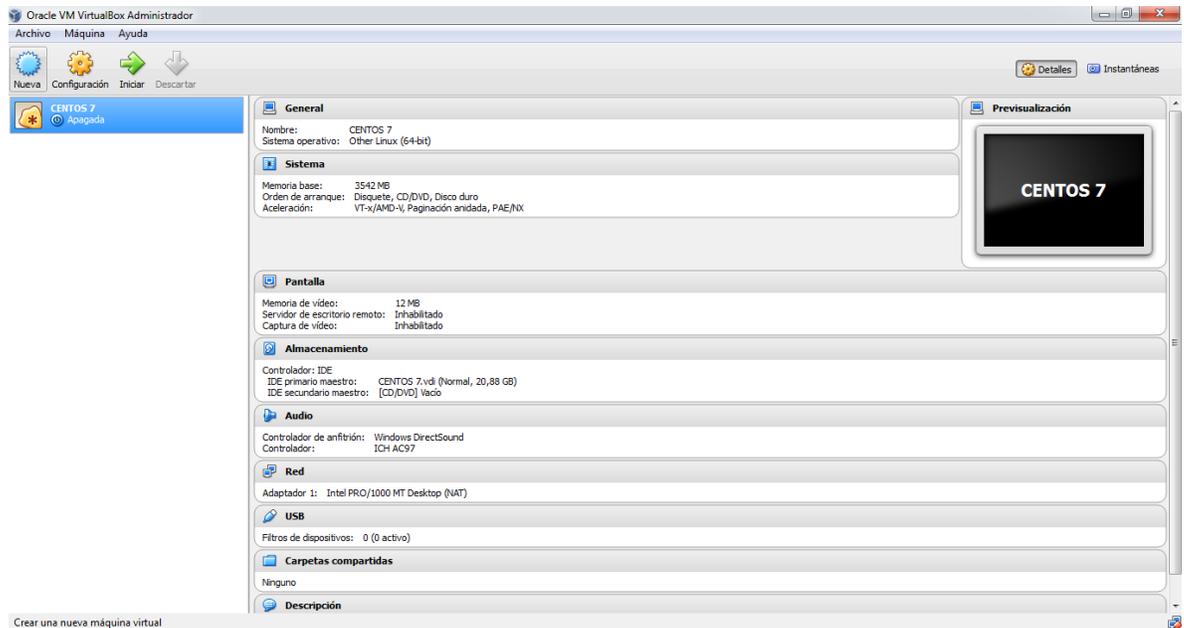


Figura 31. Aquí vamos a la opción Configuración en el cual buscamos la imagen ISO donde tengo el sistema operativo Centos, también funciona con Cd y le damos Aceptar.

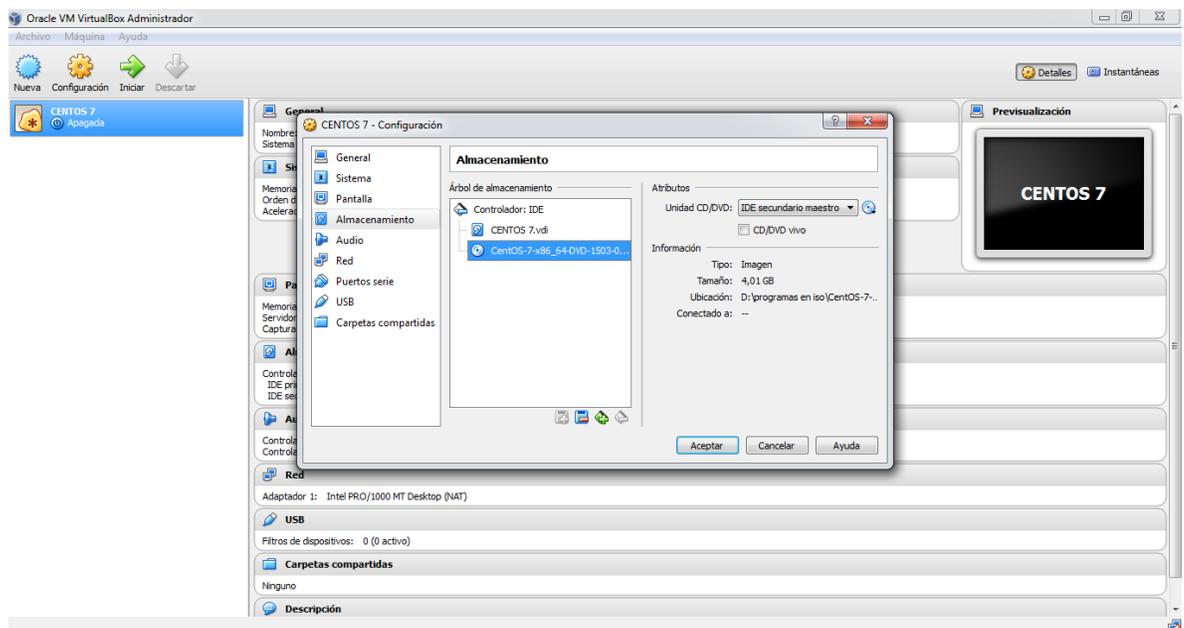


Figura 32. Le damos click en Iniciar y te sale la siguiente imagen.

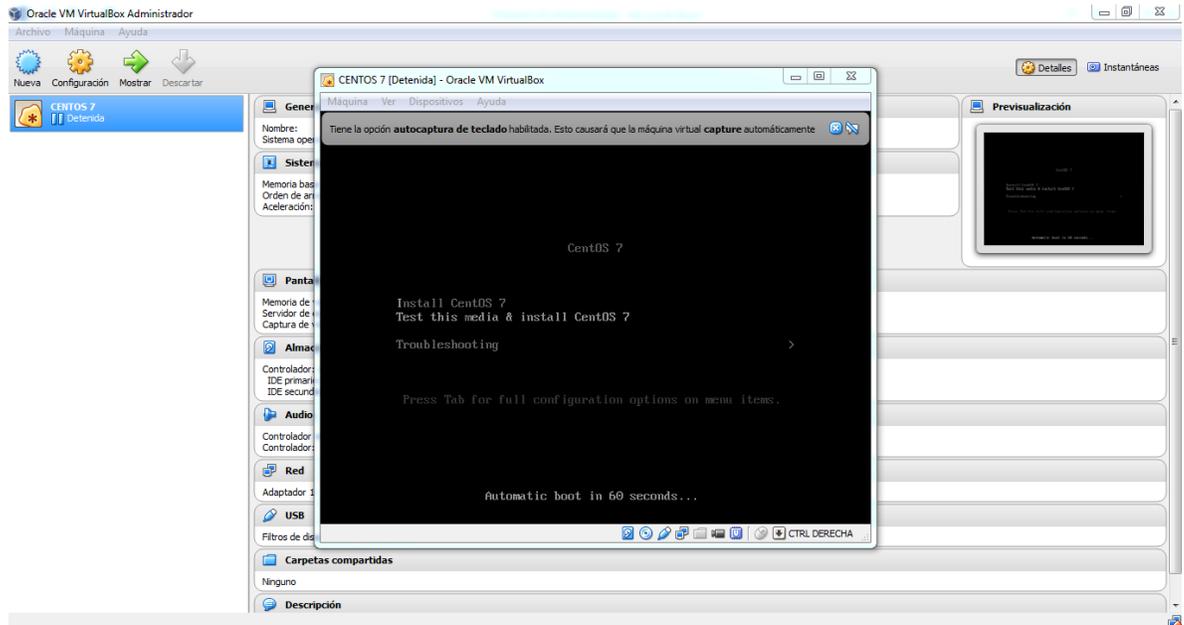


Figura 33. Le damos enter a Install Centos 7

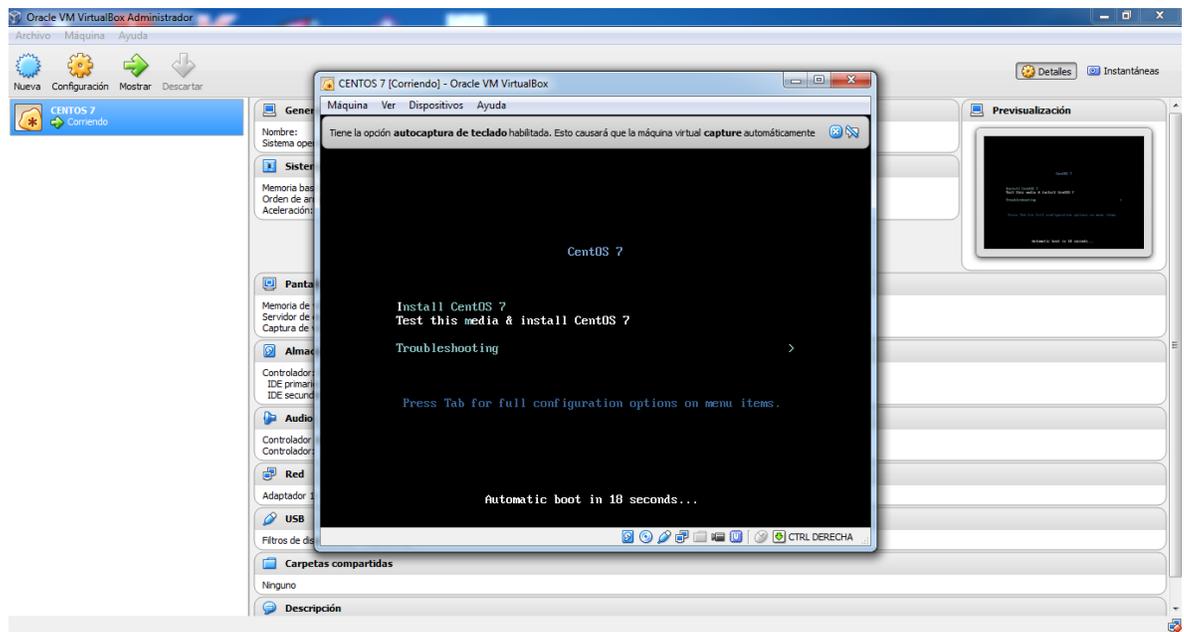


Figura 34. Esperar que el comience con la instalación del Linux Centos 7.

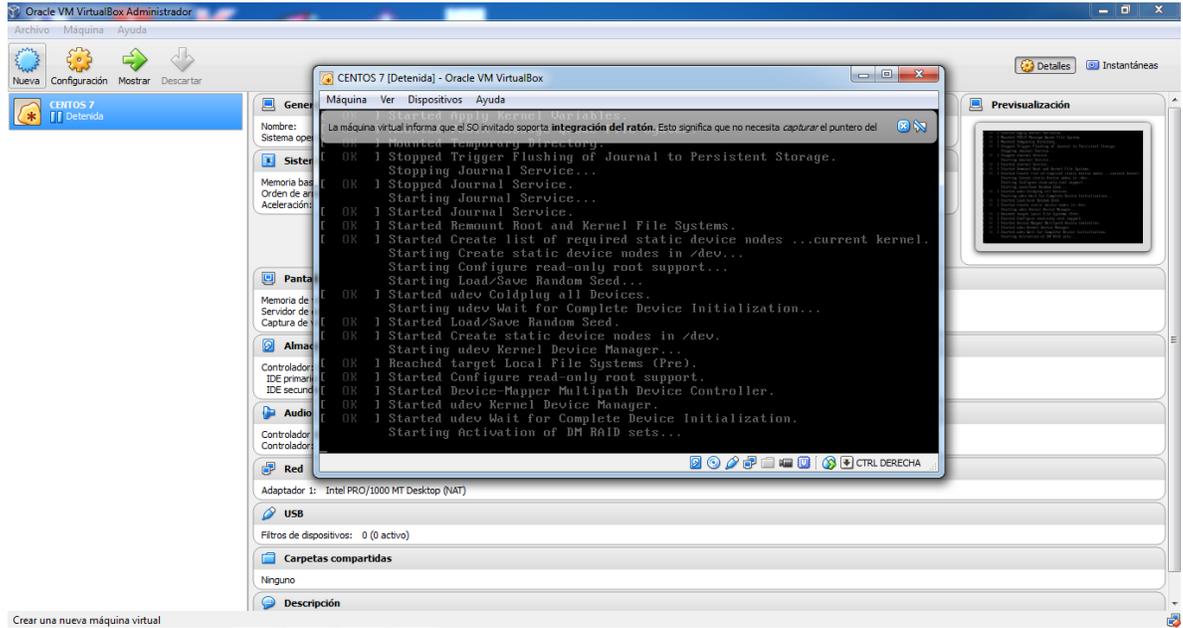


Figura 35. Aquí escogemos el idioma que vamos a instalar en Centos 7.

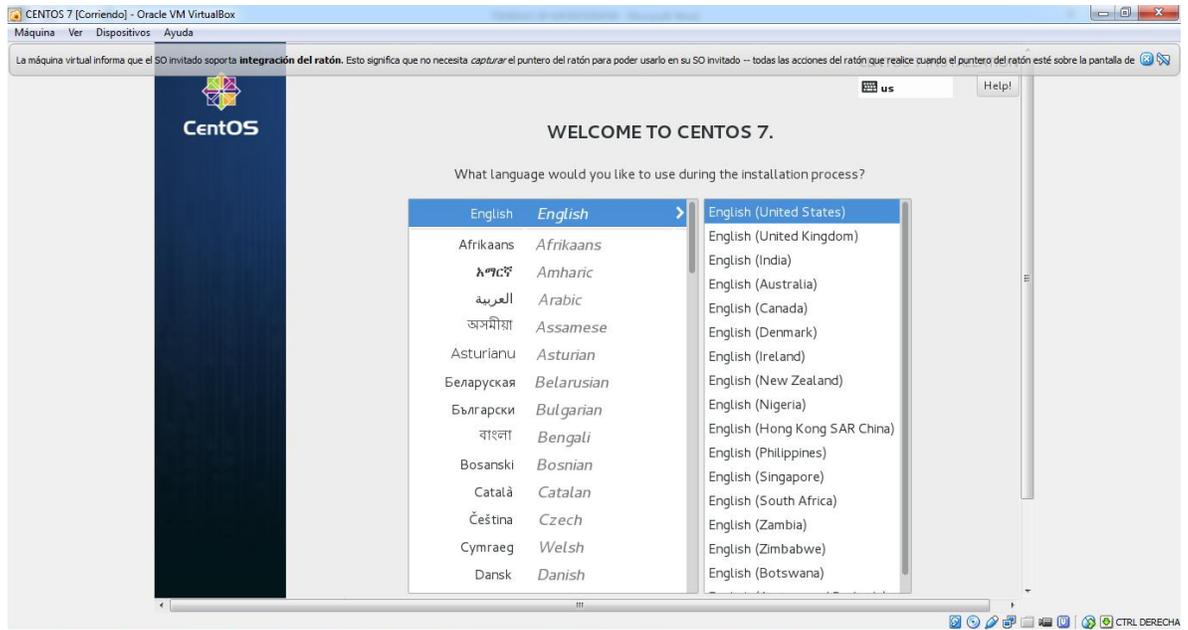


Figura 36. En esta ventana nos sale para configurar el sistema operativo de modo consola o modo gráfico y vamos a la opción Destino de la Instalación.

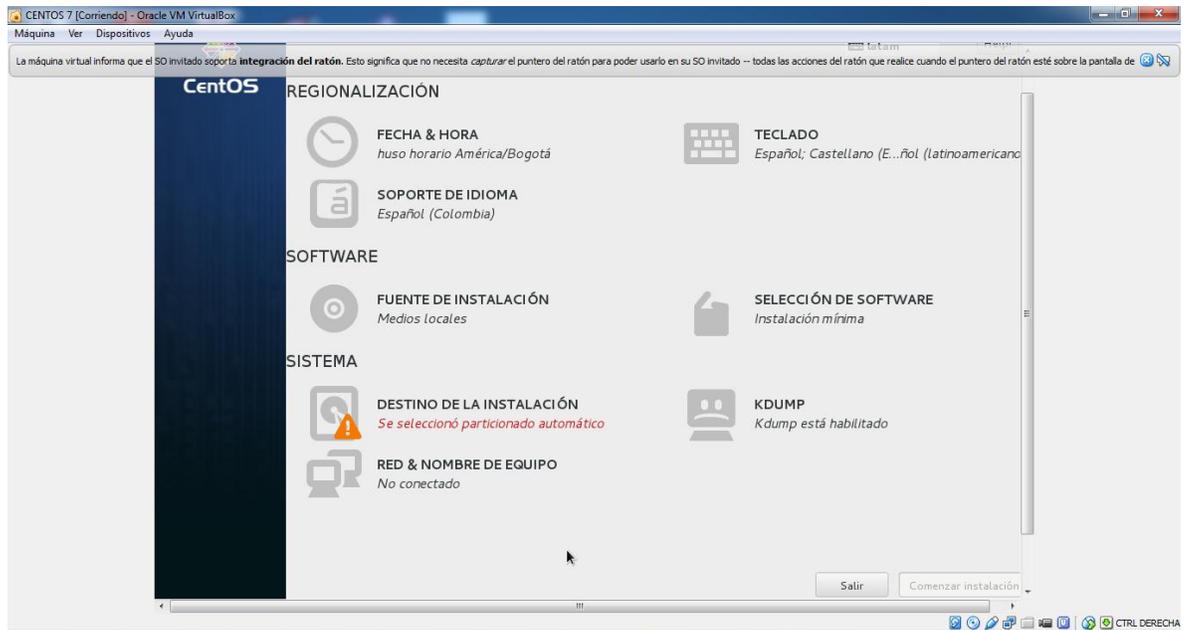


Figura 37. Esta ventana muestra en la manera de instalar particiones al Linux Centos 7.

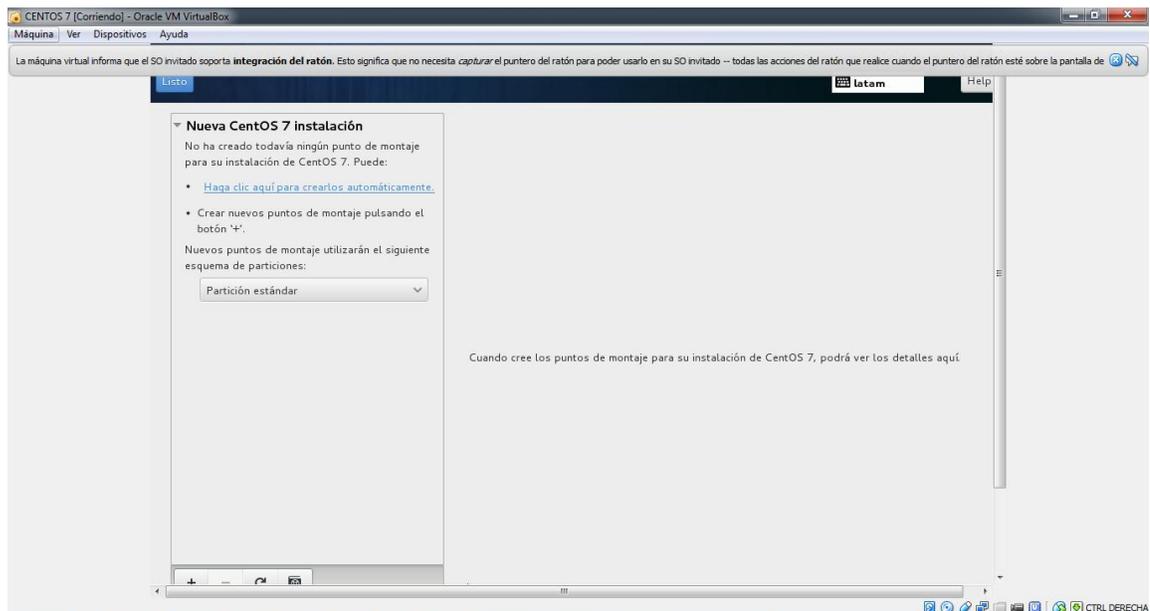


Figura 38. Vamos a la opción de + que está en la parte inferior al lado izquierdo y nos sale esta ventana.

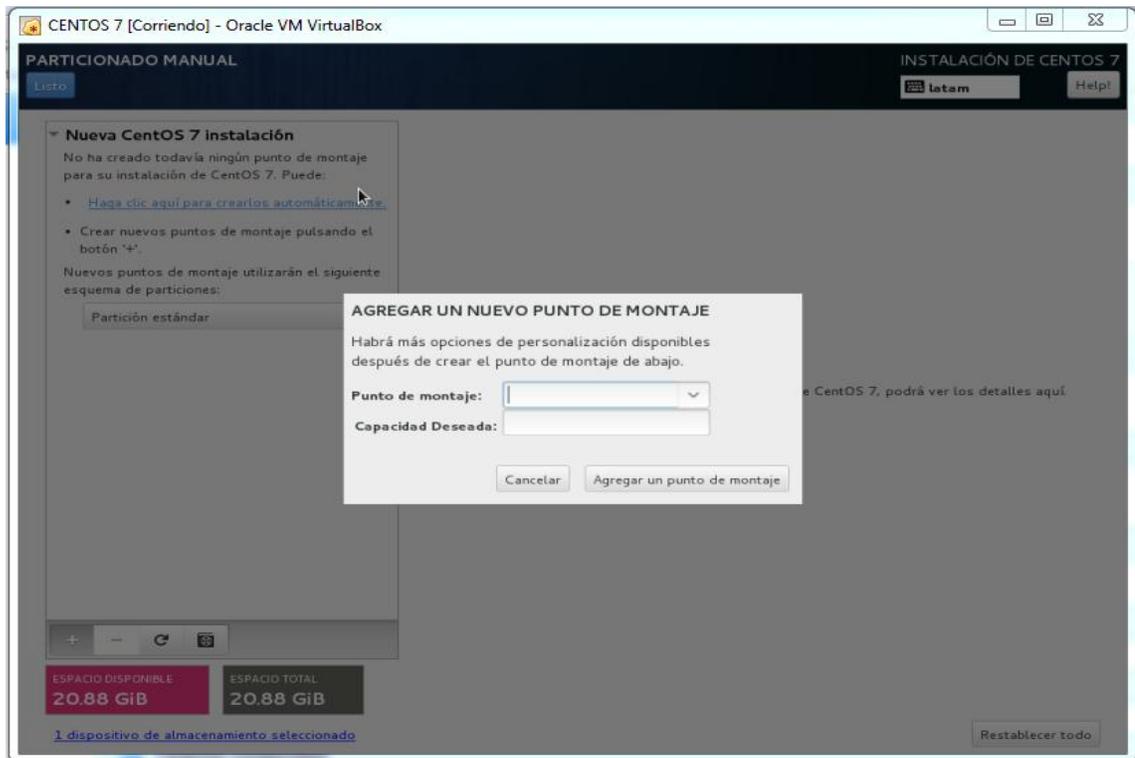


Figura 39. Vamos a configurar el swap para darle memoria RAM extra al LINUX Centos 7.

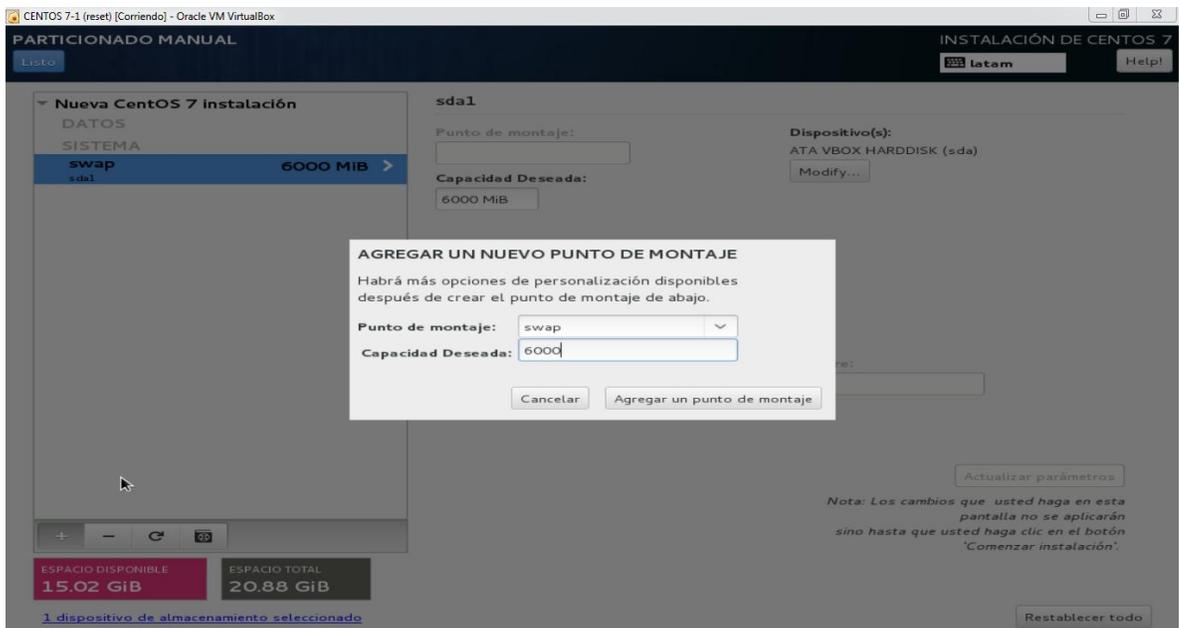


Figura 40. Después de que configuramos la SWAP nos aparece así.

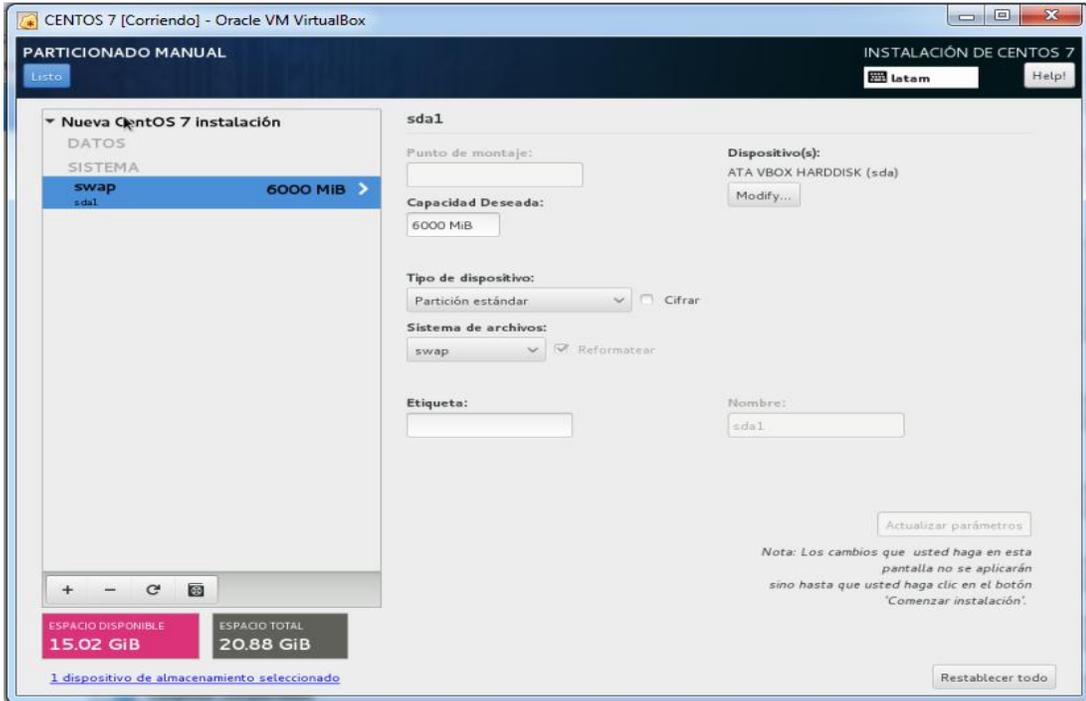


Figura 41. Configuración del Boot para que el Linux pueda iniciar correcta.

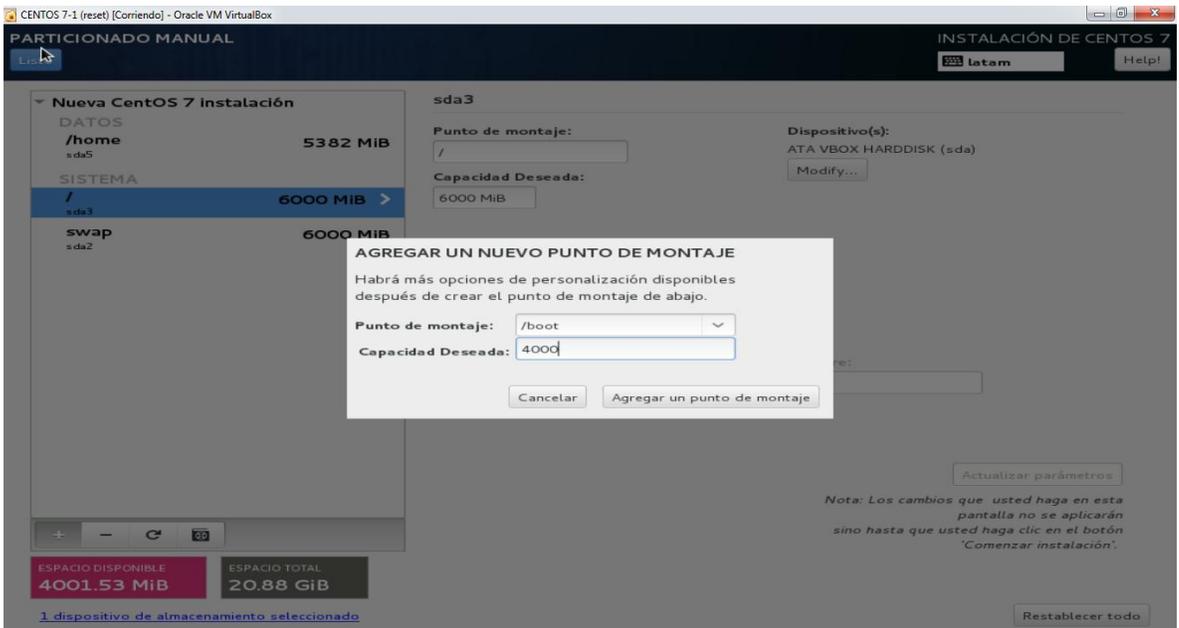


Figura 42. Después de configurar la Boot para el CENTOS 7 nos aparecerá así.

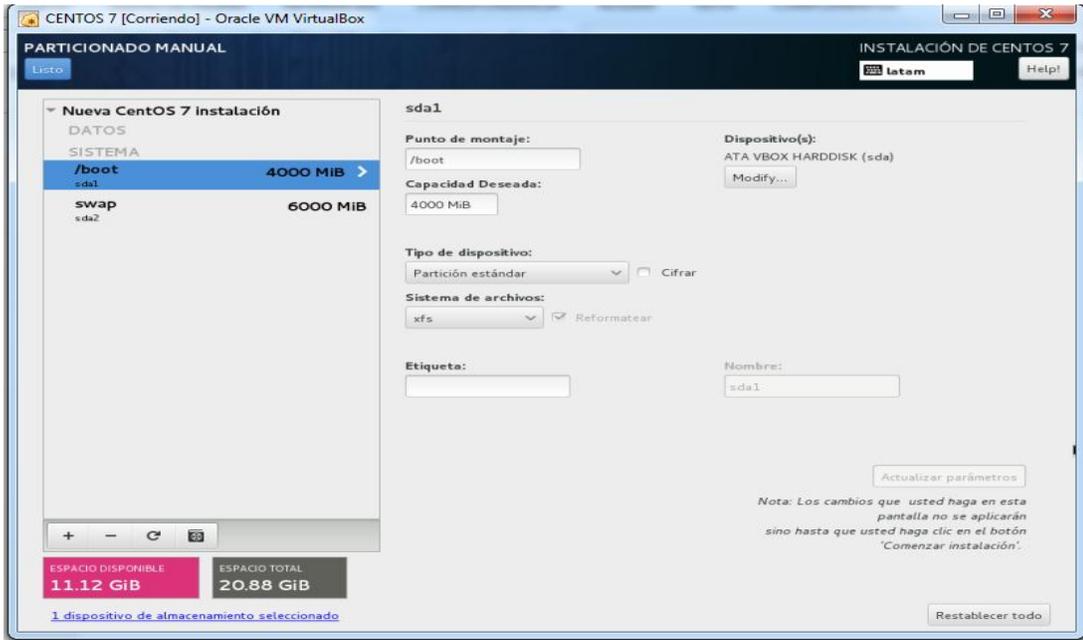


Figura 43. Vamos a configurar el espacio donde vamos a instalar el sistema CENTOS7, le damos la opción Agregar un punto de montaje.

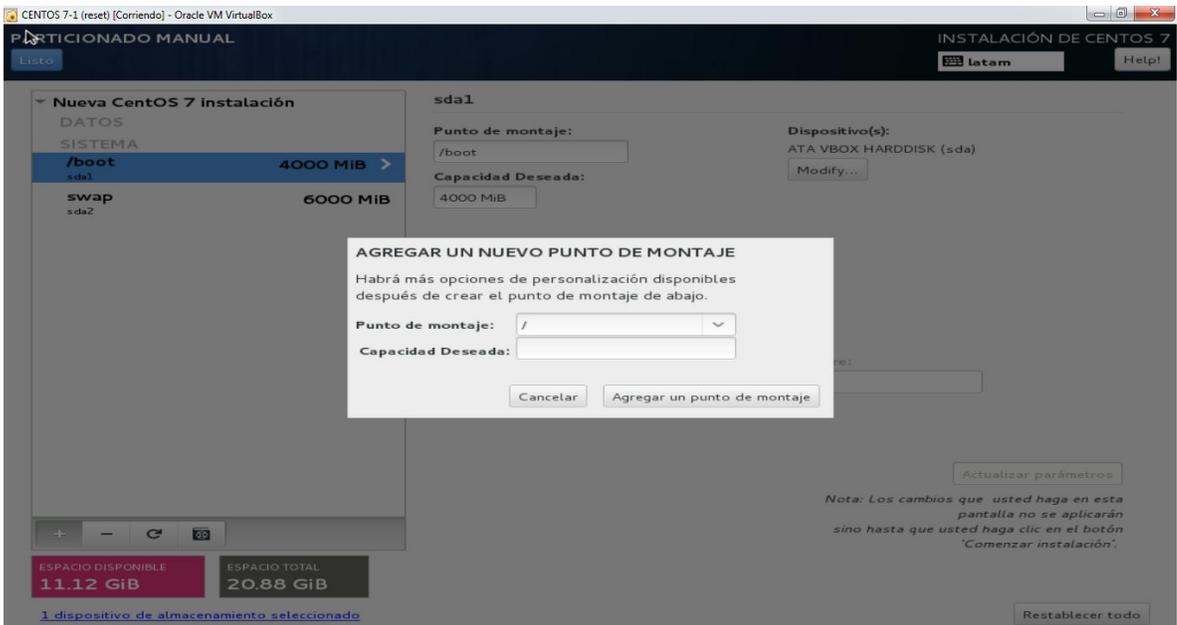


Figura 44. Después de configurar /, donde configuramos donde vamos a instalar el sistemas operativo Linux Centos 7, nos aparecerá así.

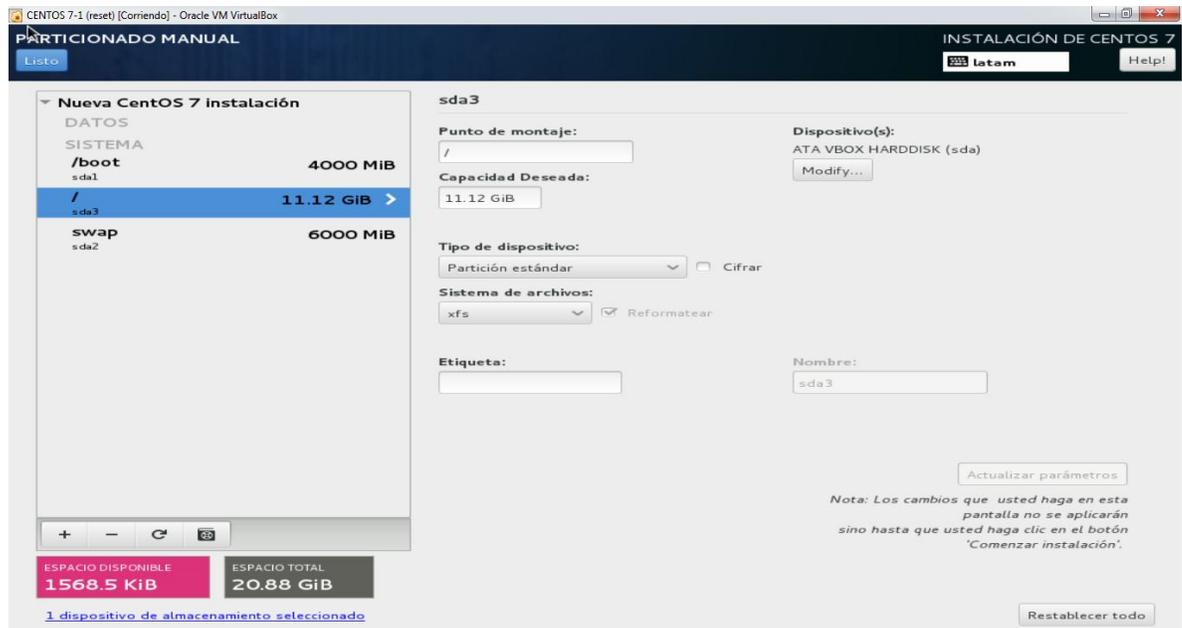


Figura 45. Después de configurar todas las participaciones, le damos en la opción Listo.

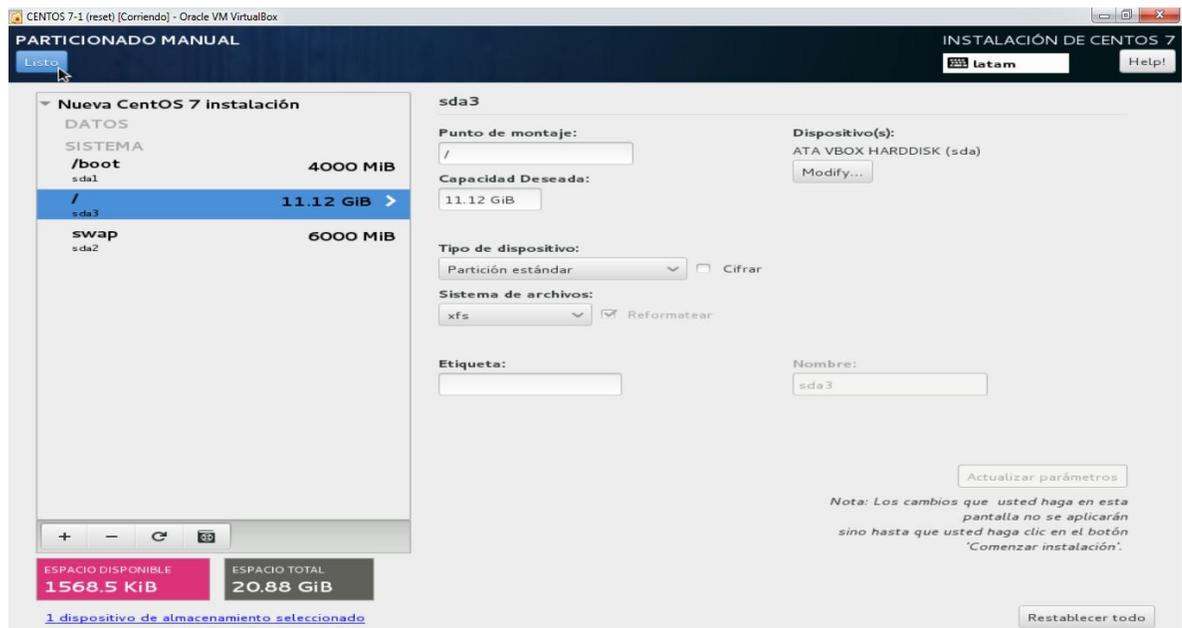


Figura 46. Después nos sale esta opción y le damos la opción Aceptar Cambios.

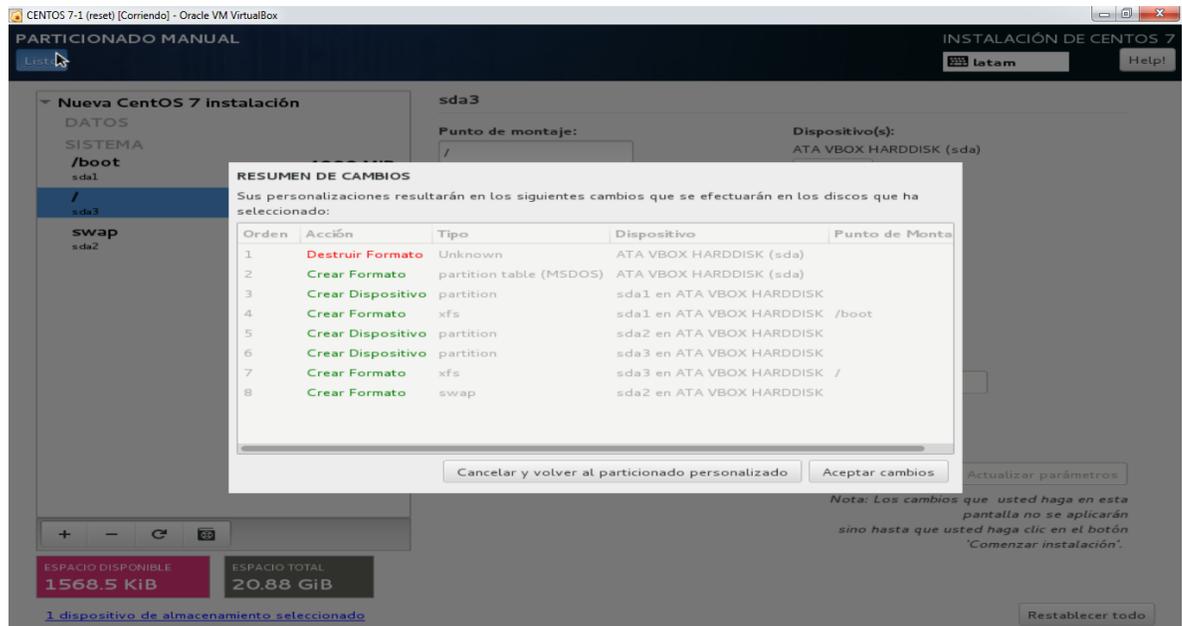


Figura 47. Después nos sale esta ventana.



Figura 48. Vamos a configurar el sistema operativo Linux para que sea de manera Escritorio Gnome, entonces vamos a la opción Selección de software, después escogemos las opción Escritorio Gnome y después le damos Listo.

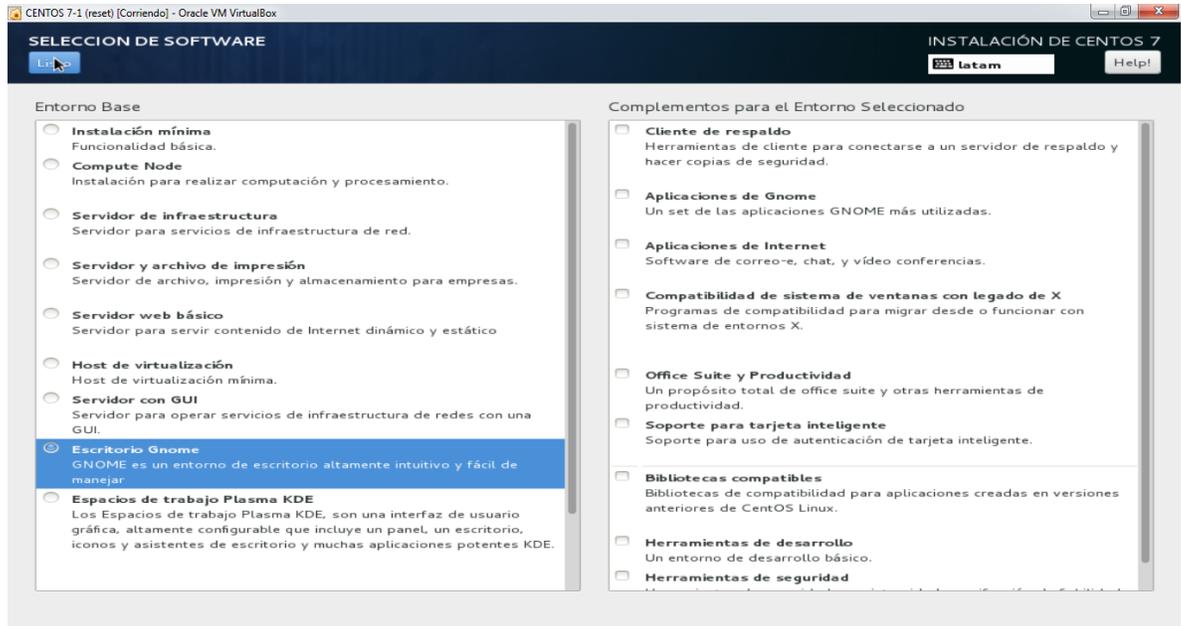


Figura 49. Vamos a empezar a instalar el sistemas operativo

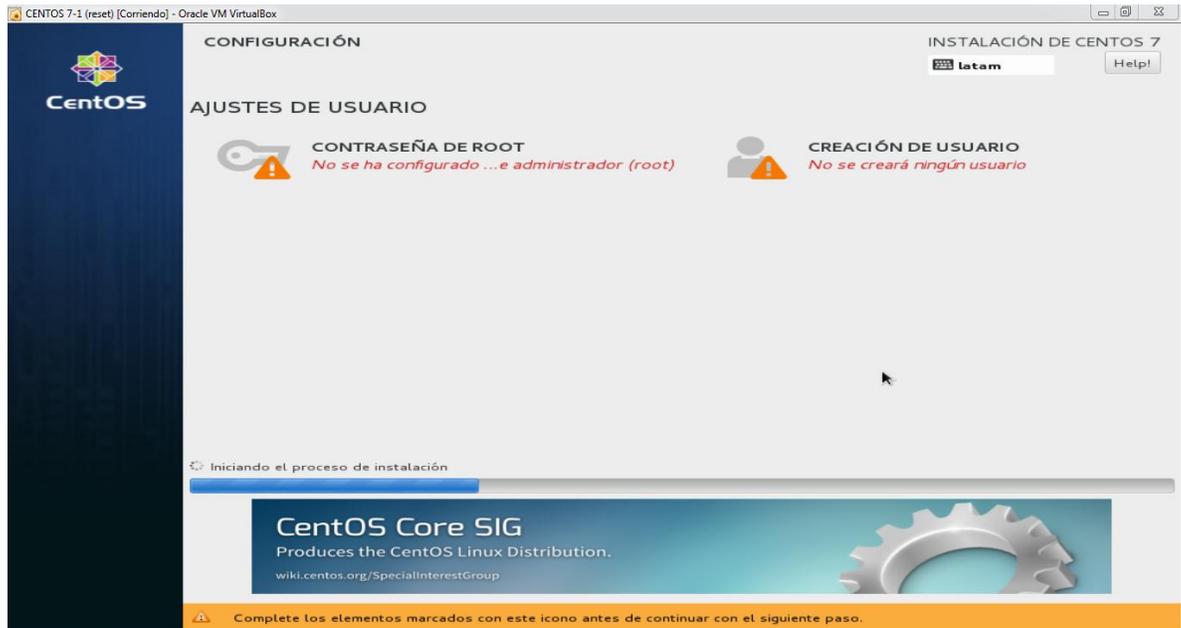


Figura 50. Vamos a configurar contraseña de root.

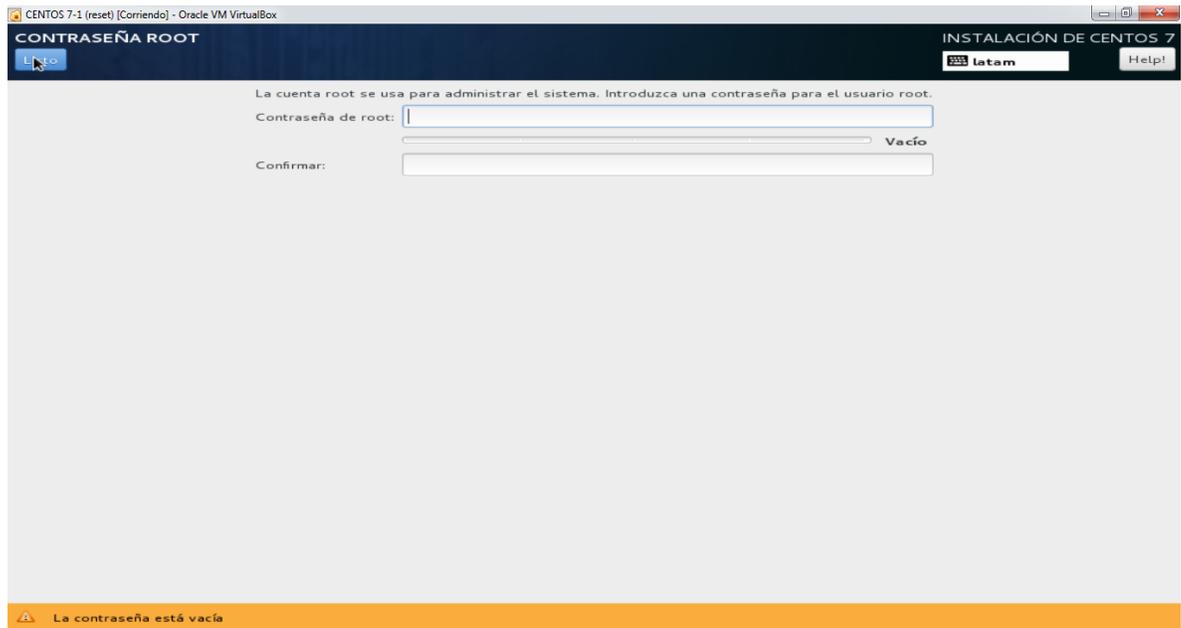


Figura 51. Después de configurar la contraseña del root, esperar que se instale el sistema operativo Centos 7.

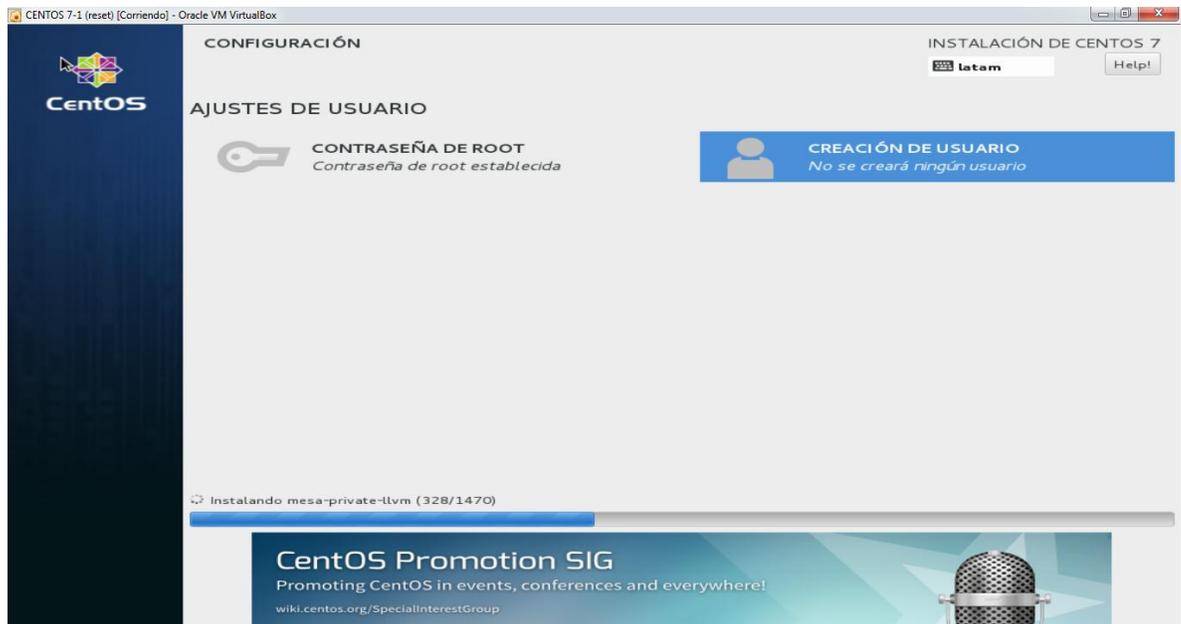


Figura 52. Después de que se instaló le damos reiniciar.

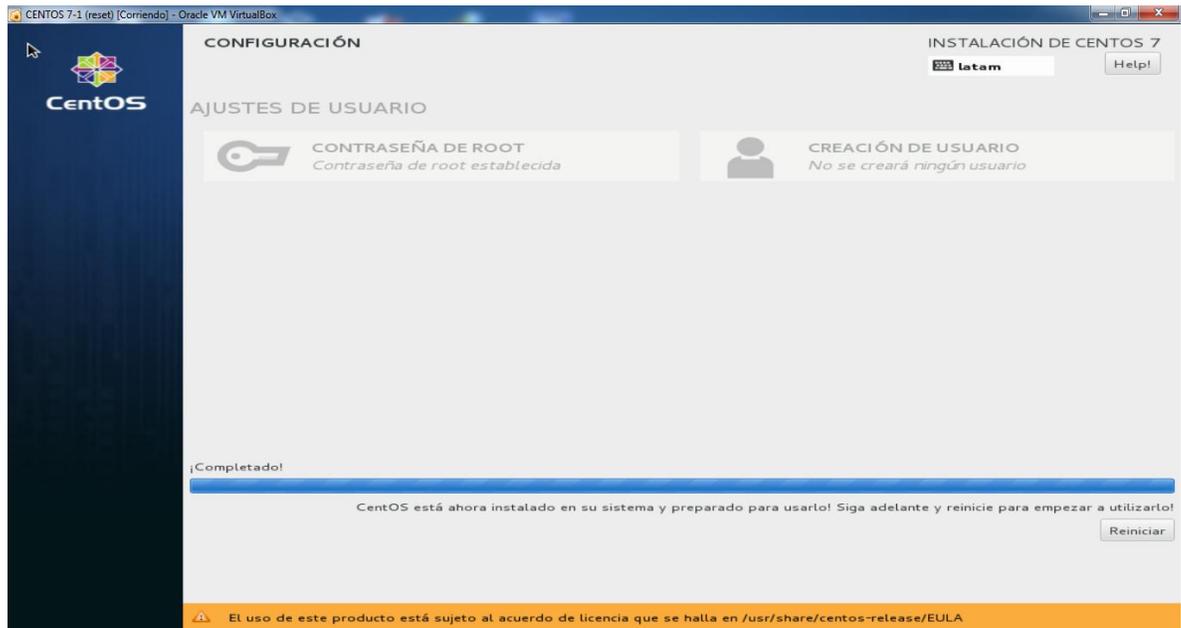


Figura 53. Esperar que se reinicie la máquina virtual.

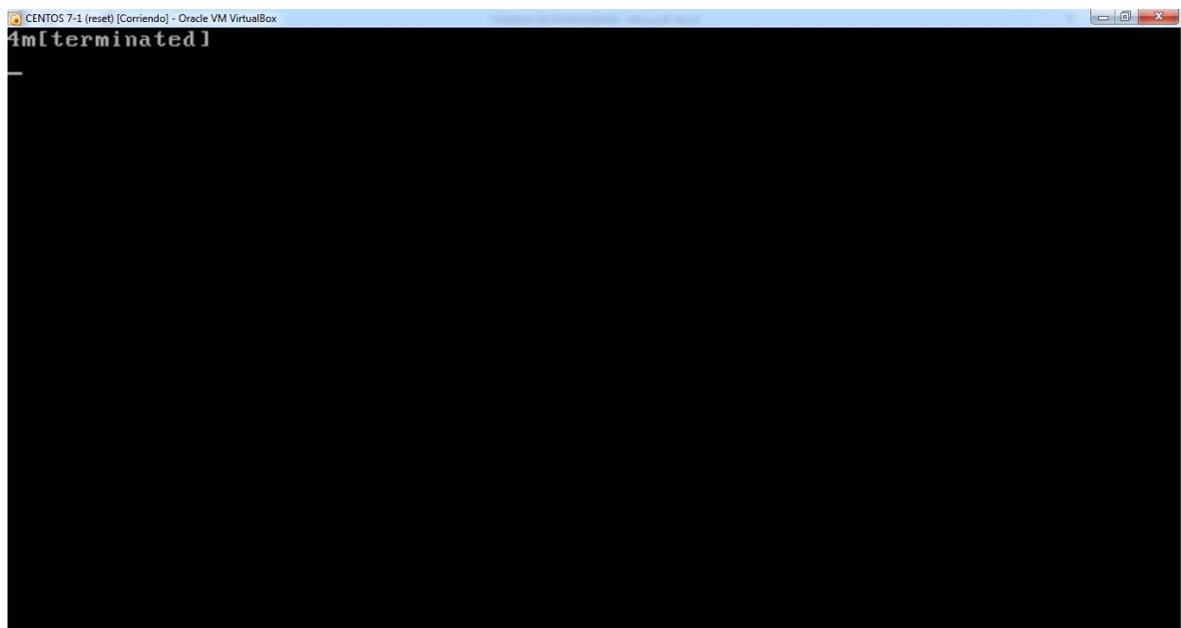


Figura 54. Después de reiniciar la maquina virtual nos aparecera esta ventana.



Figura 55. Después le damos click y nos saldrá esta nueva ventana, le damos click en siguiente.

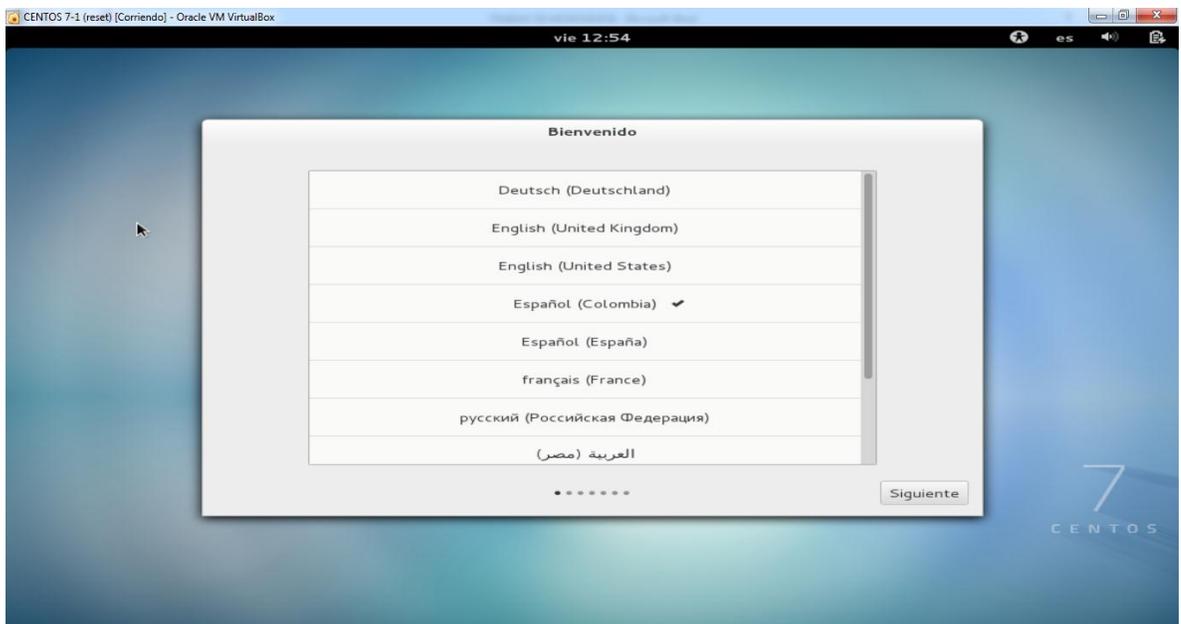


Figura 56. Aquí para configurar el teclado del idioma que queremos.

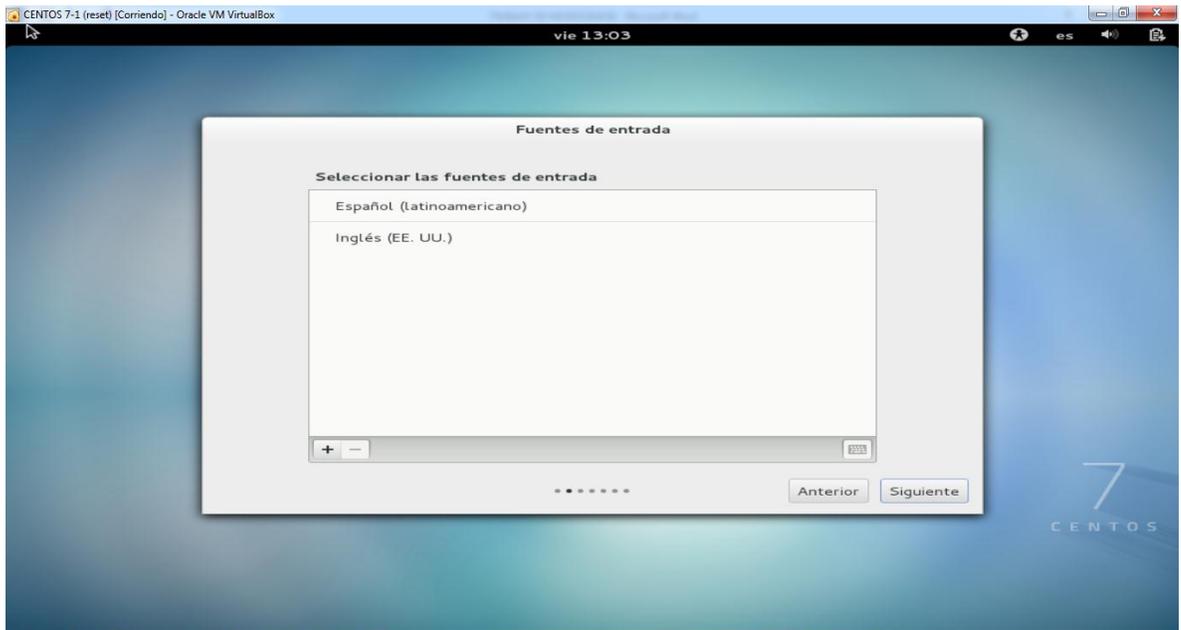


Figura 57. Aquí configuramos el usuario que le queremos dar.

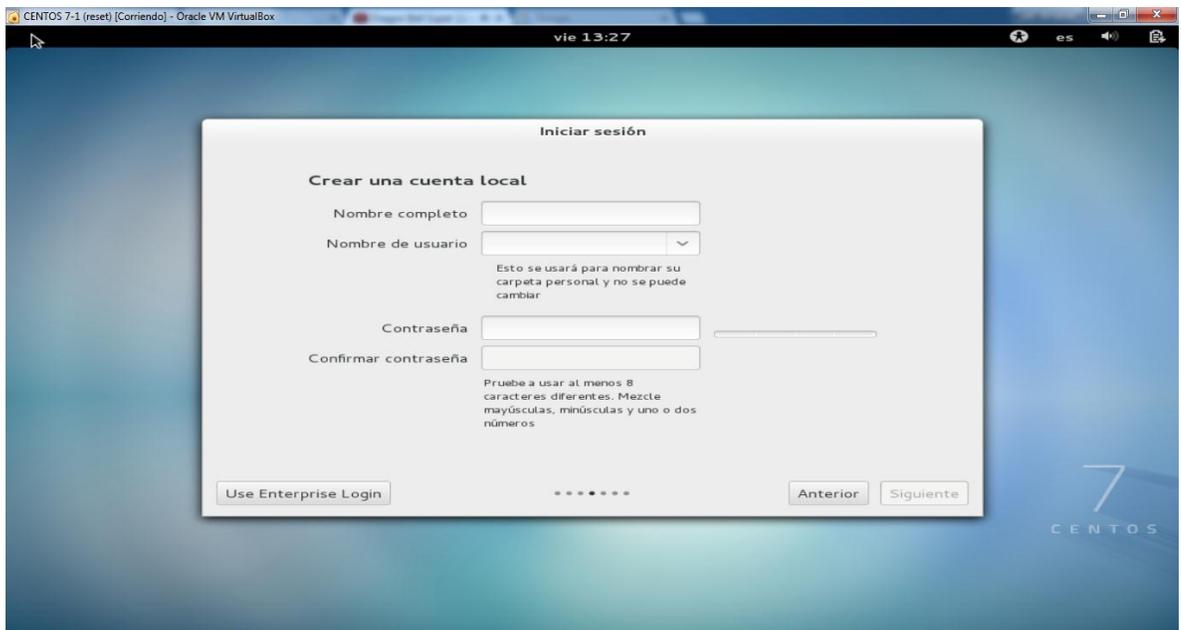


Figura 58. Aquí configuramos la ubicación y le damos siguiente.

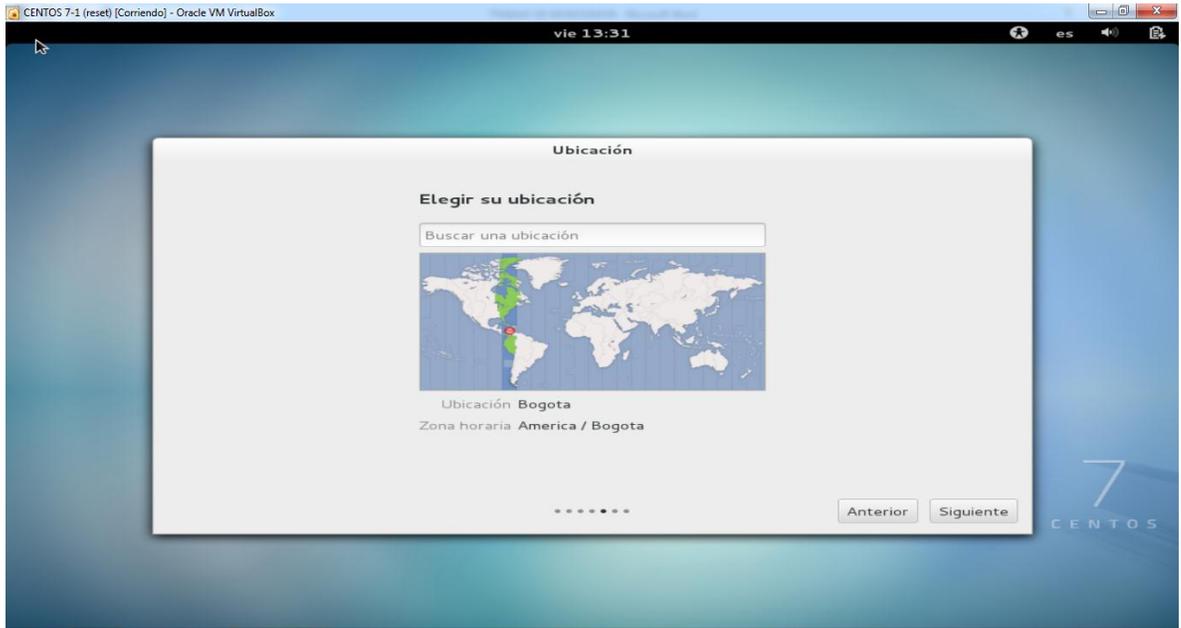


Figura 59. Aquí termina la configuración del sistemas operativo Linux Centos 7.

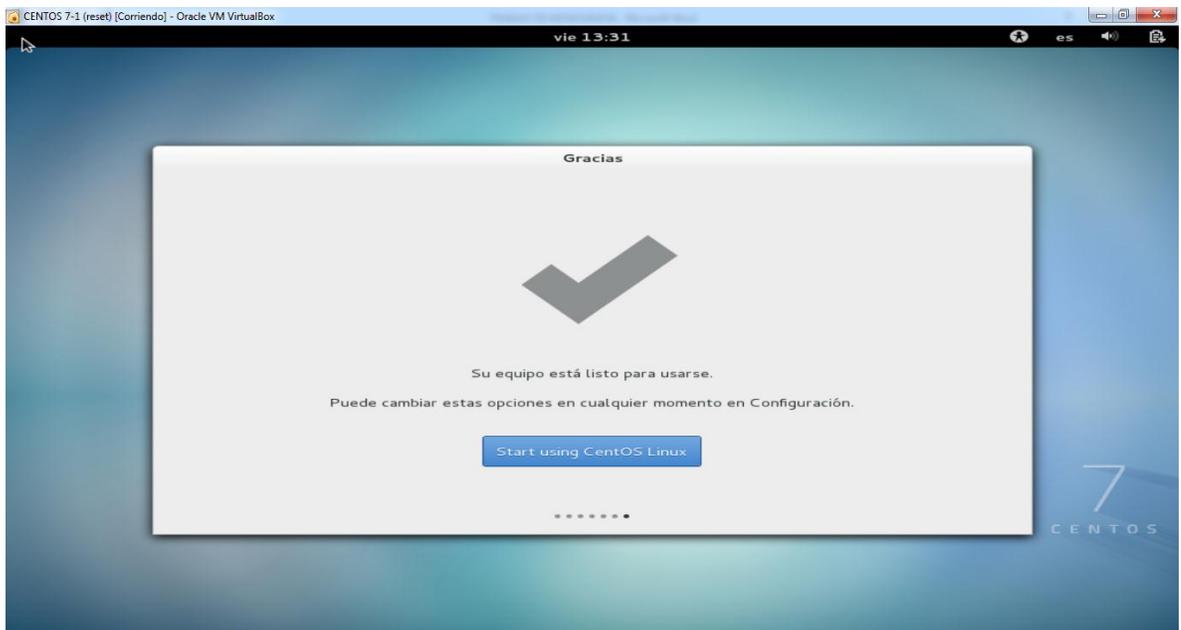
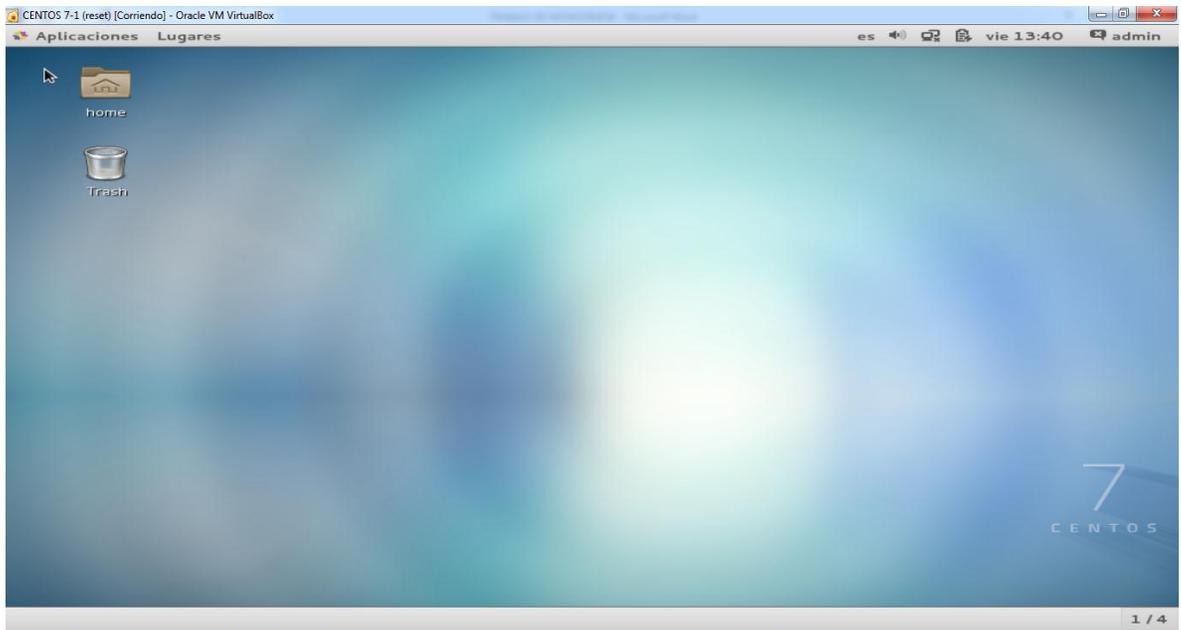


Figura 60. Ya después de haber configurado el sistema operativo aparecerá esta ventana nueva, ya podemos usar el sistema operativo Centos 7 Linux.



4.2.3 Manual de instalación de Servidor Web en Centos 7.

Figura 61. Vamos a la opción de aplicaciones y después buscamos la opción terminal.

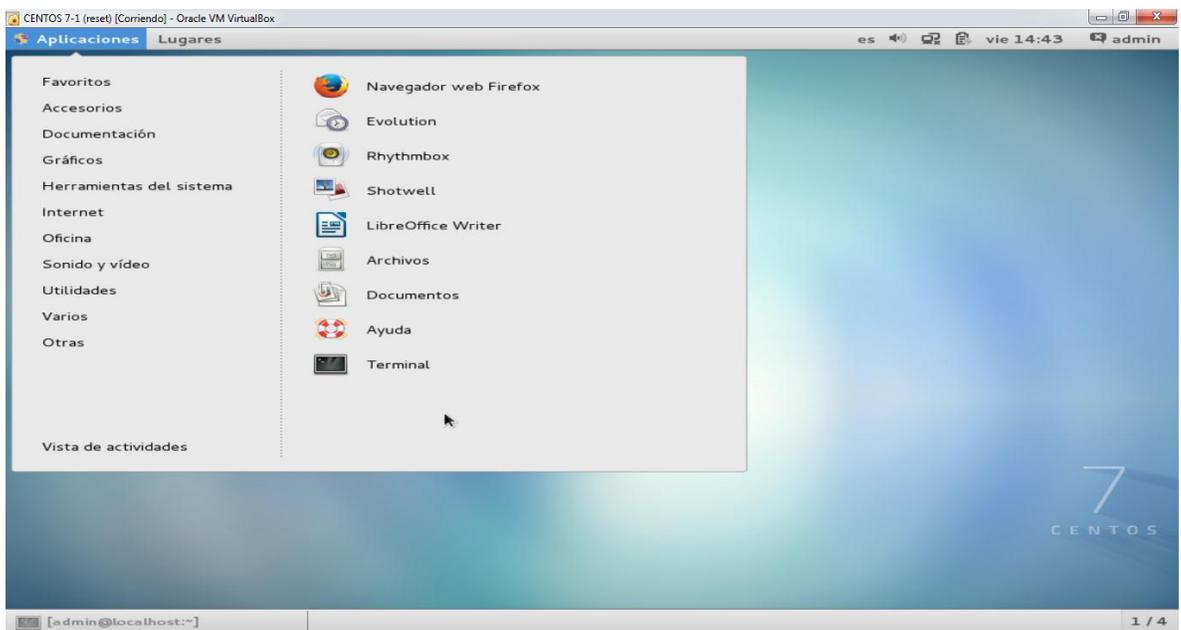


Figura 62. Verificamos que esté instalado el servidor web.

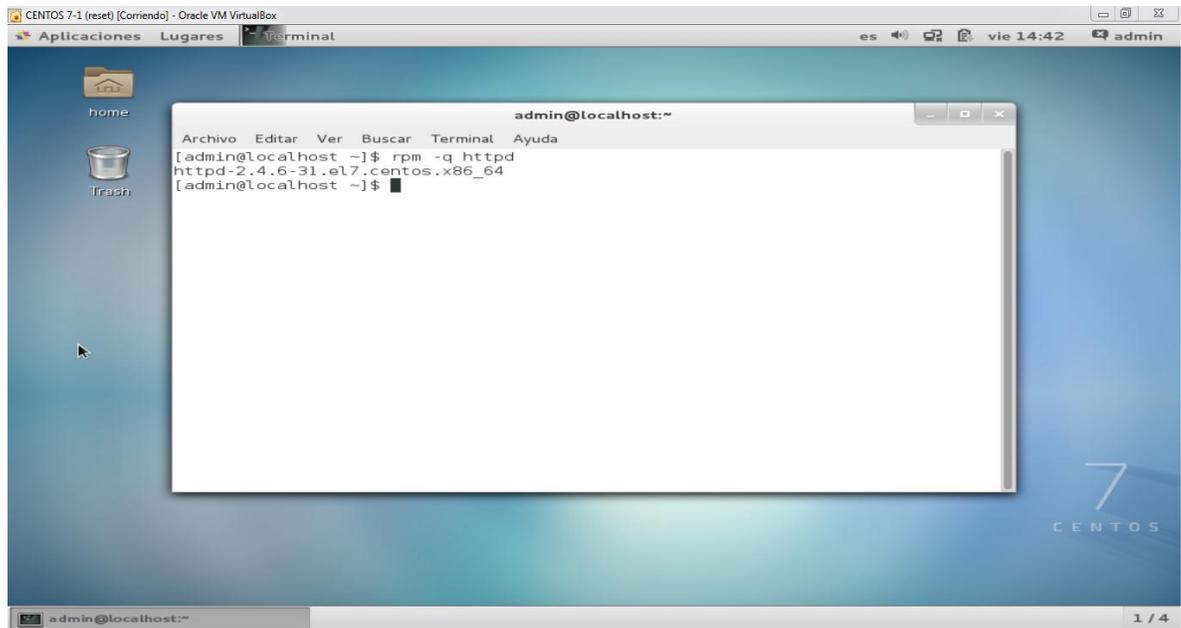


Figura 63. Como vemos que está instalado una versión, vamos actualizarla si no lo tenemos toca instalar el servidor httpd, ahora vamos a entrar como super usuario para poder instalar el servidor httpd o web.

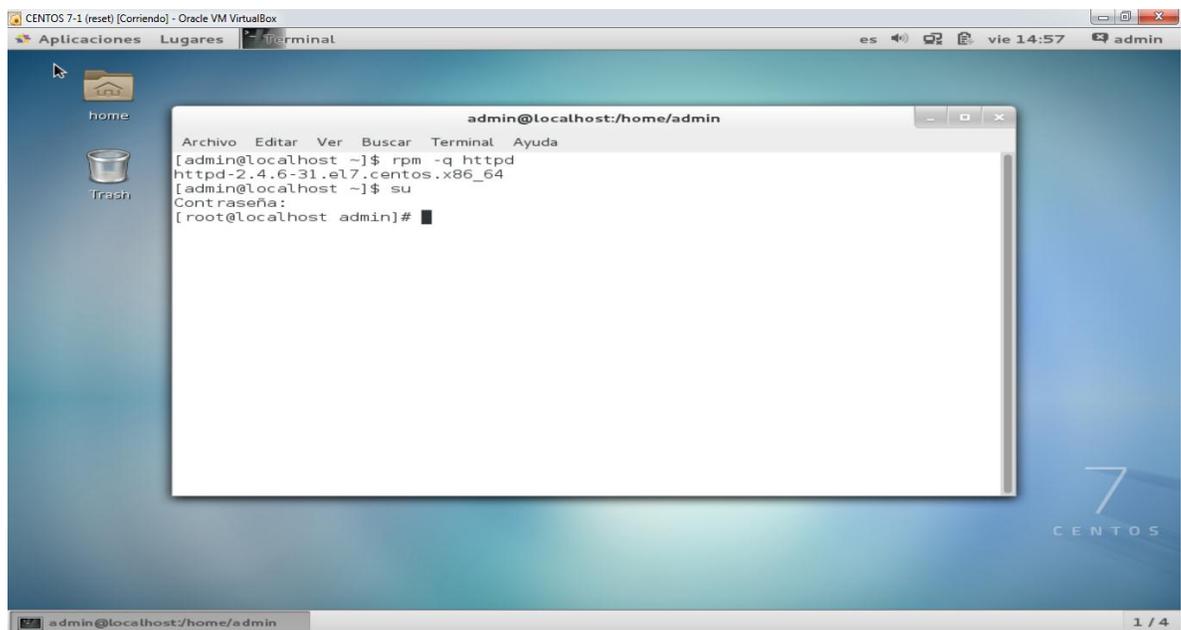


Figura 64. Ahora nos disponemos de instalar el servidor httpd y esperar que se actualice con el internet.

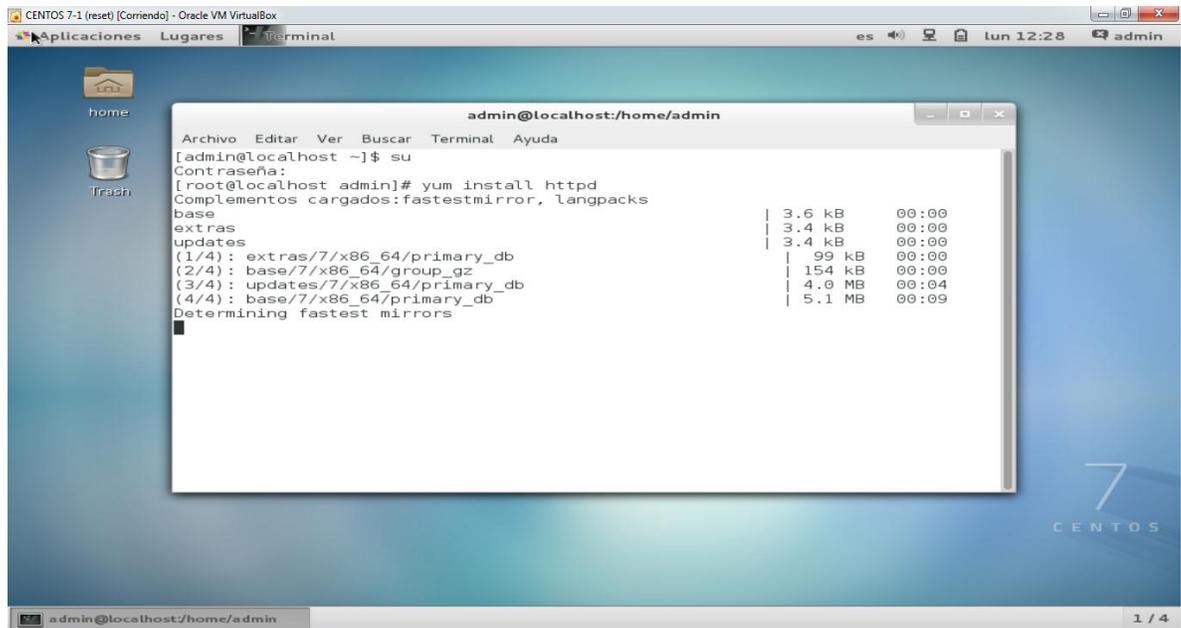


Figura 65. Aquí nos pedirá que actualice la versión del servidor httpd y esperar que actualice.

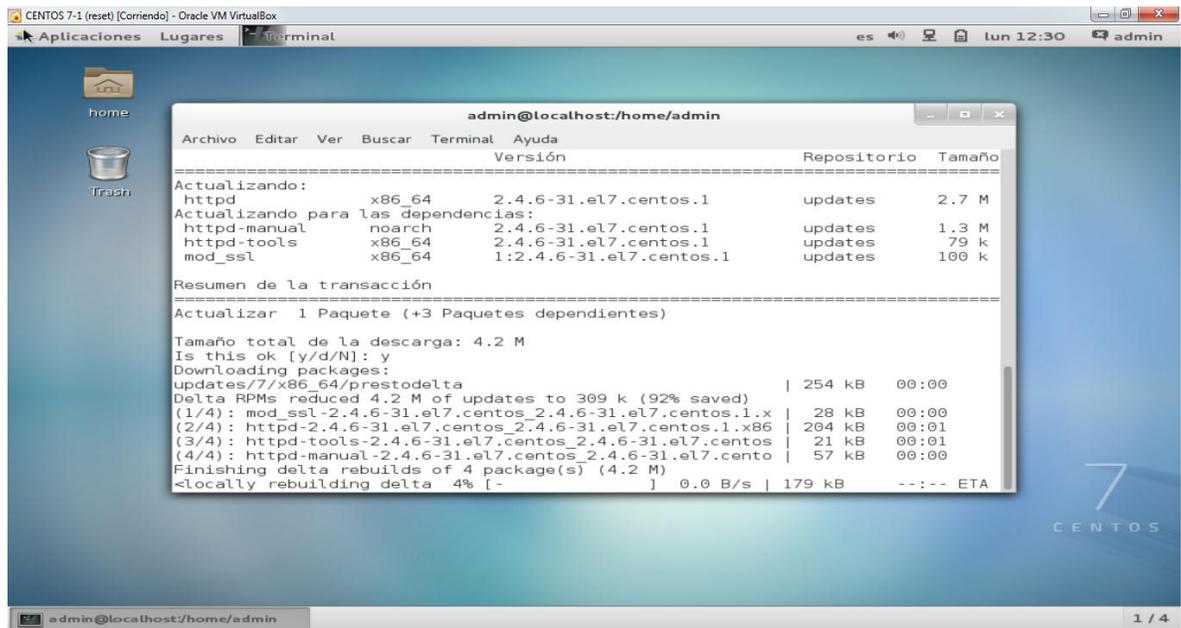


Figura 66. Después pedirá que estoy de acuerdo y escribimos SI.



Figura 67. Aquí nos dice que quedo actualizado el servidor httpd o web.

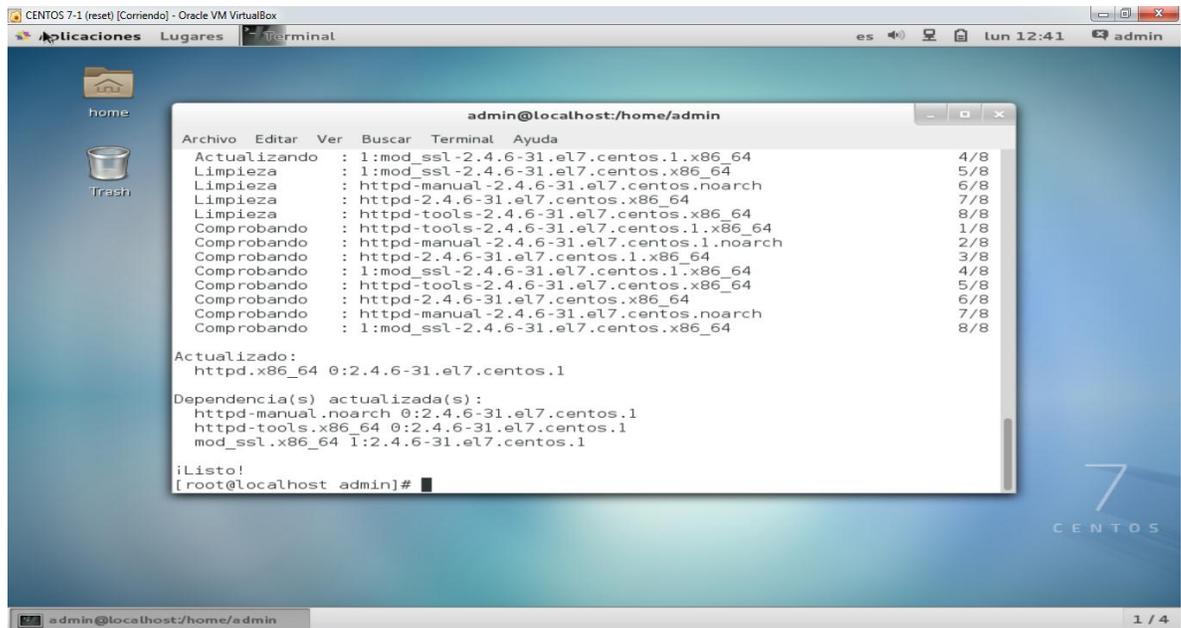


Figura 68. Vamos a iniciar el servidor httpd o web.

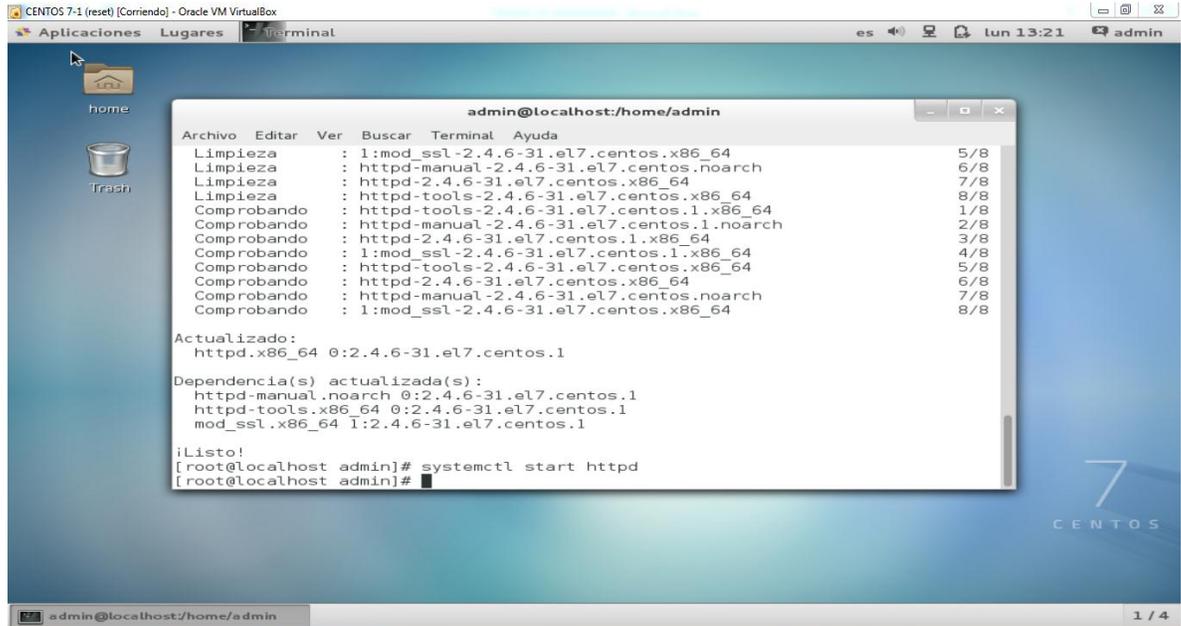


Figura 69. Vamos a verificar si quedo instalado.

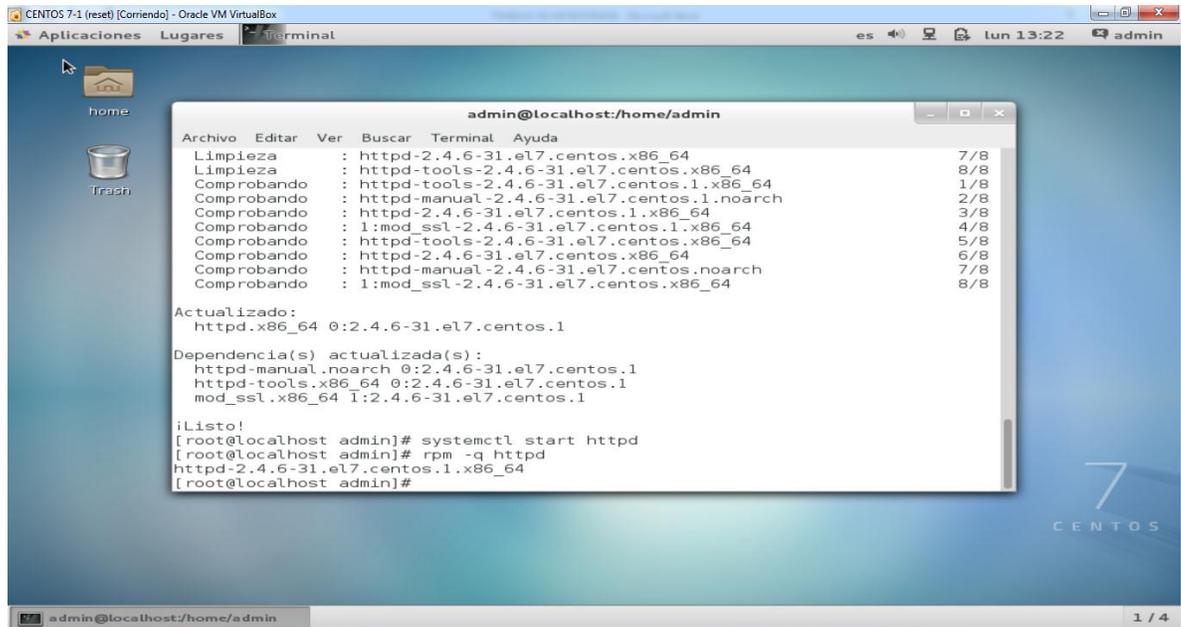


Figura 70. Después vamos al explorador para verificar si quedo instalado.

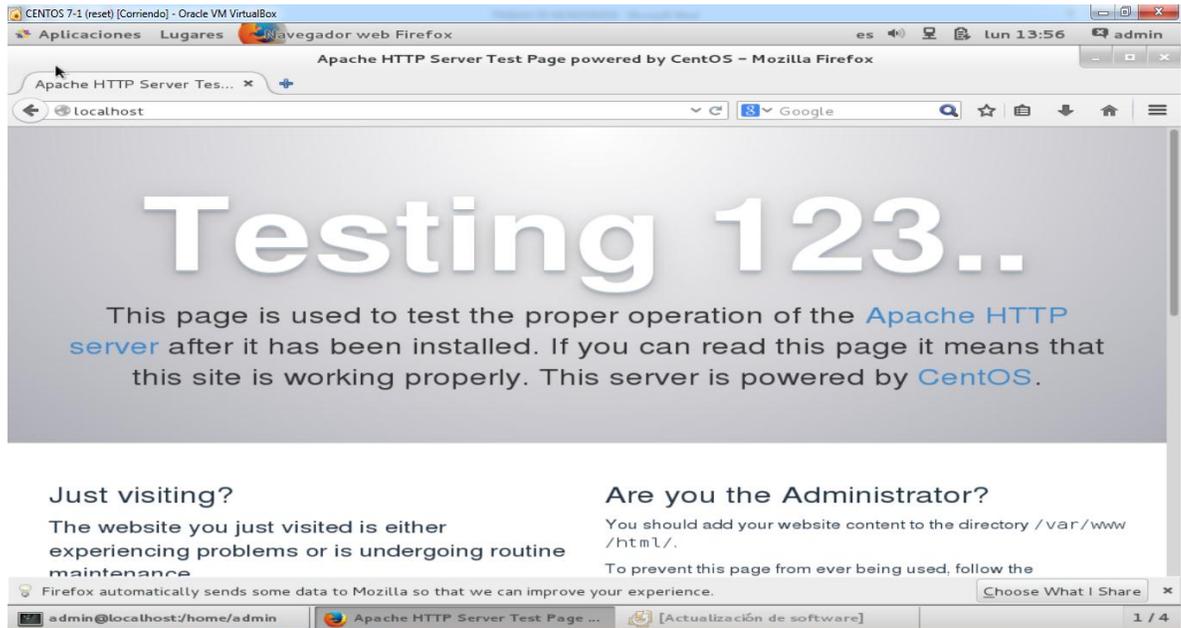


Figura 71. Vamos a terminal otra vez y digitamos este siguiente comando, nano /etc/httpd/conf/httpd.conf después nos aparecerá esta ventana.

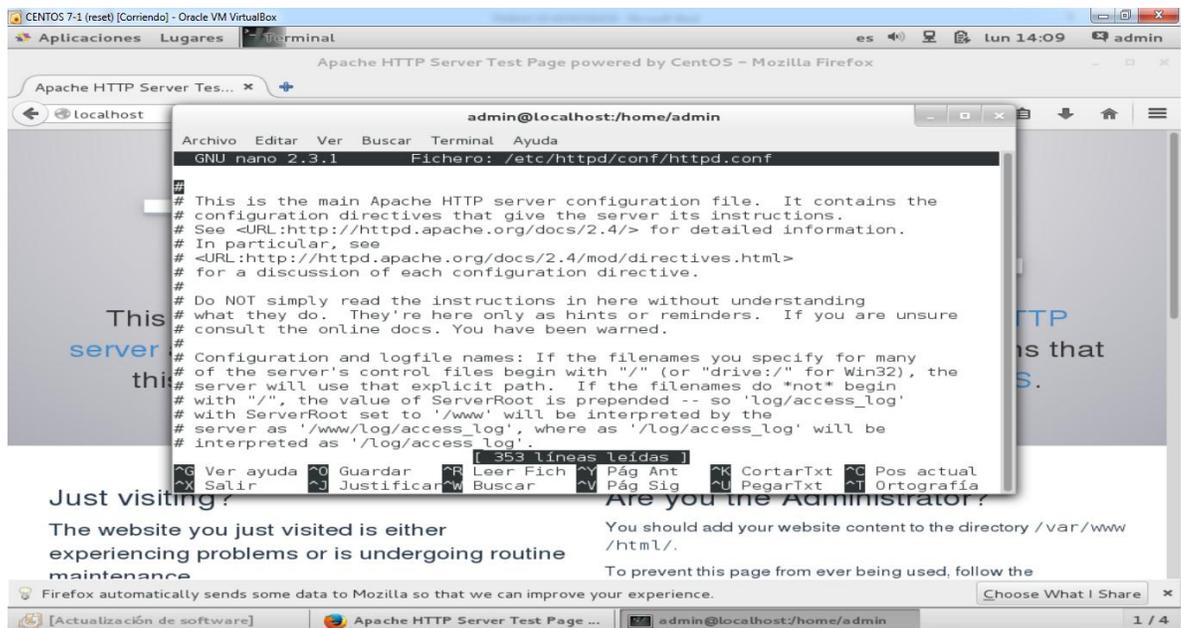
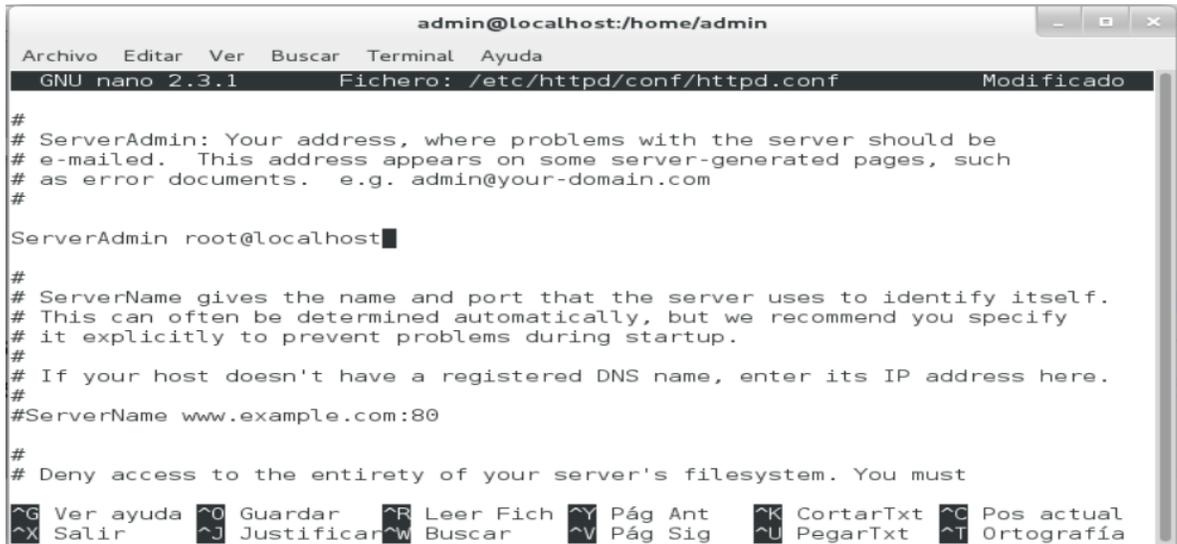
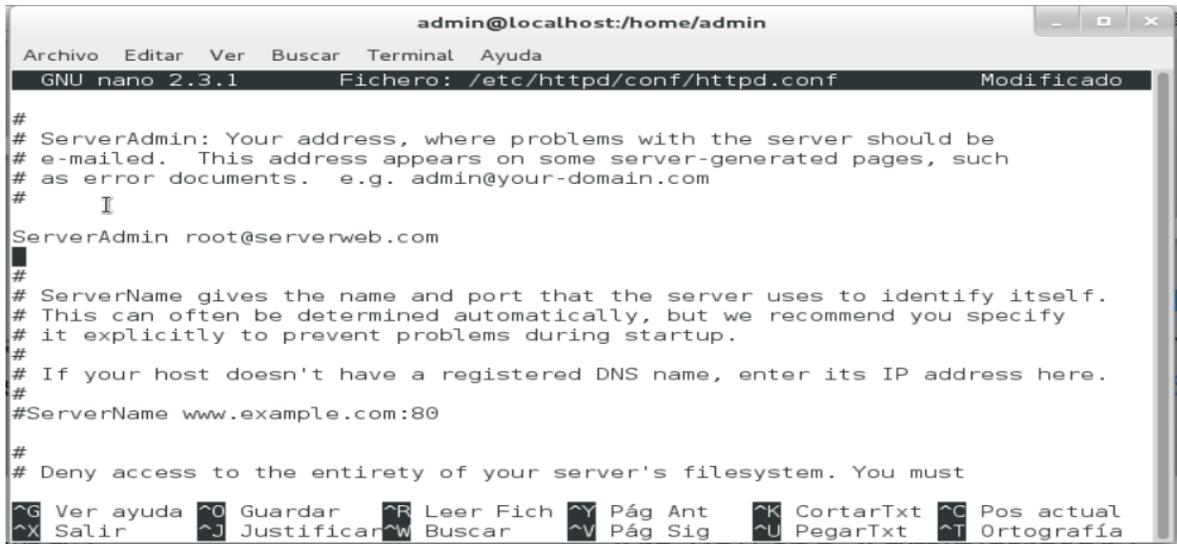


Figura 72. Ahora buscamos la opción ServerAdmin root@localhost como lo muestra la imagen



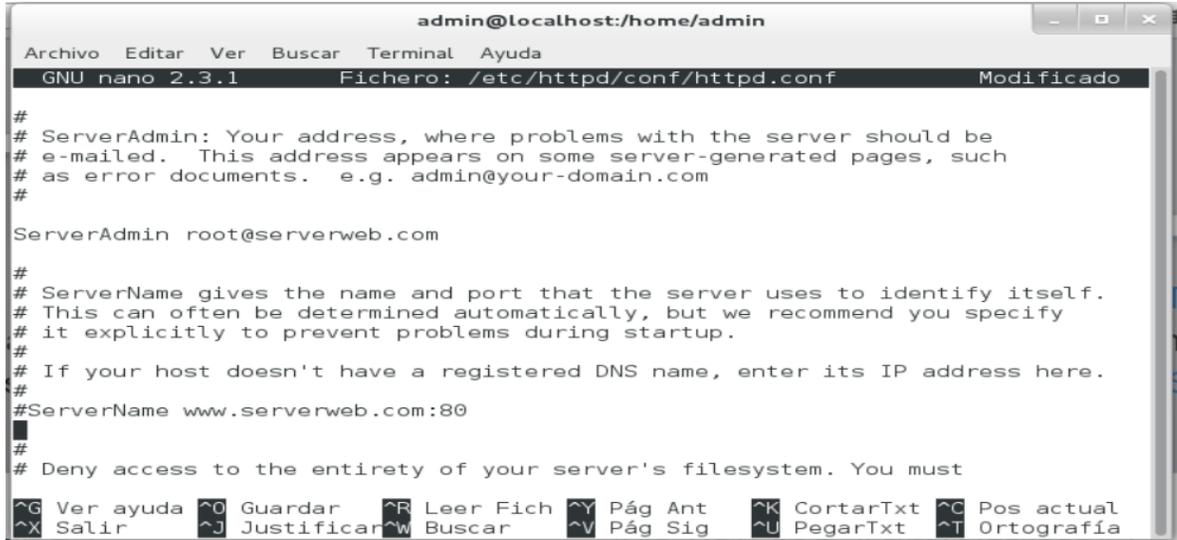
```
admin@localhost:/home/admin
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.3.1  Fichero: /etc/httpd/conf/httpd.conf  Modificado
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
ServerAdmin root@localhost
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
#
# Deny access to the entirety of your server's filesystem. You must
^G Ver ayuda  ^O Guardar  ^R Leer Fich  ^Y Pág Ant  ^K CortarTxt  ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág Sig  ^U PegarTxt  ^T Ortografía
```

Figura 73. Vamos a cambiar el nombre de localhost al nombre que queramos, en este momento le puse root@serverweb.com



```
admin@localhost:/home/admin
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.3.1  Fichero: /etc/httpd/conf/httpd.conf  Modificado
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
#
ServerAdmin root@serverweb.com
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
#
# Deny access to the entirety of your server's filesystem. You must
^G Ver ayuda  ^O Guardar  ^R Leer Fich  ^Y Pág Ant  ^K CortarTxt  ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág Sig  ^U PegarTxt  ^T Ortografía
```

Figura 74. Vamos a cambiar la opción ServerName www.example.com:80 a ServerName www.serverweb.com

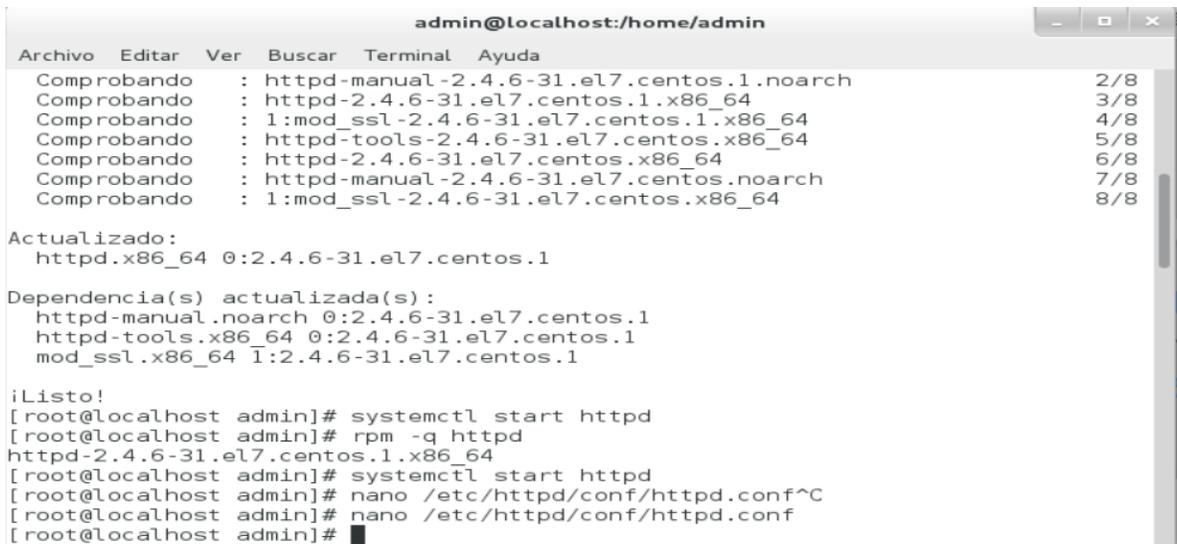


```

admin@localhost:/home/admin
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.3.1 Fichero: /etc/httpd/conf/httpd.conf Modificado
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@serverweb.com
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.serverweb.com:80
#
# Deny access to the entirety of your server's filesystem. You must
^G Ver ayuda ^O Guardar ^R Leer Fich ^V Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^Y Pág Sig ^U PegarTxt ^T Ortografía

```

Figura 75. Ahora vamos a guardar los cambios con la tecla ctrl + o y salimos del editor de httpd con ctrl + x después nos aparecerá de nuevo la ventana del terminal.



```

admin@localhost:/home/admin
Archivo Editar Ver Buscar Terminal Ayuda
Comprobando : httpd-manual-2.4.6-31.el7.centos.1.noarch 2/8
Comprobando : httpd-2.4.6-31.el7.centos.1.x86_64 3/8
Comprobando : 1:mod_ssl-2.4.6-31.el7.centos.1.x86_64 4/8
Comprobando : httpd-tools-2.4.6-31.el7.centos.x86_64 5/8
Comprobando : httpd-2.4.6-31.el7.centos.x86_64 6/8
Comprobando : httpd-manual-2.4.6-31.el7.centos.noarch 7/8
Comprobando : 1:mod_ssl-2.4.6-31.el7.centos.x86_64 8/8

Actualizado:
 httpd.x86_64 0:2.4.6-31.el7.centos.1

Dependencia(s) actualizada(s):
 httpd-manual.noarch 0:2.4.6-31.el7.centos.1
 httpd-tools.x86_64 0:2.4.6-31.el7.centos.1
 mod_ssl.x86_64 1:2.4.6-31.el7.centos.1

¡Listo!
[root@localhost admin]# systemctl start httpd
[root@localhost admin]# rpm -q httpd
httpd-2.4.6-31.el7.centos.1.x86_64
[root@localhost admin]# systemctl start httpd
[root@localhost admin]# nano /etc/httpd/conf/httpd.conf^C
[root@localhost admin]# nano /etc/httpd/conf/httpd.conf
[root@localhost admin]#

```

Figura 76. Vamos a configurar nuestro servidor web sus hosts nano serverweb-vhosts.conf



```
admin@localhost:/etc/httpd/conf.d
Archivo Editar Ver Buscar Terminal Ayuda
Comprobando : httpd-2.4.6-31.el7.centos.1.x86_64 3/8
Comprobando : 1:mod_ssl-2.4.6-31.el7.centos.1.x86_64 4/8
Comprobando : httpd-tools-2.4.6-31.el7.centos.x86_64 5/8
Comprobando : httpd-2.4.6-31.el7.centos.x86_64 6/8
Comprobando : httpd-manual-2.4.6-31.el7.centos.noarch 7/8
Comprobando : 1:mod_ssl-2.4.6-31.el7.centos.x86_64 8/8

Actualizado:
httpd.x86_64 0:2.4.6-31.el7.centos.1

Dependencia(s) actualizada(s):
httpd-manual.noarch 0:2.4.6-31.el7.centos.1
httpd-tools.x86_64 0:2.4.6-31.el7.centos.1
mod_ssl.x86_64 1:2.4.6-31.el7.centos.1

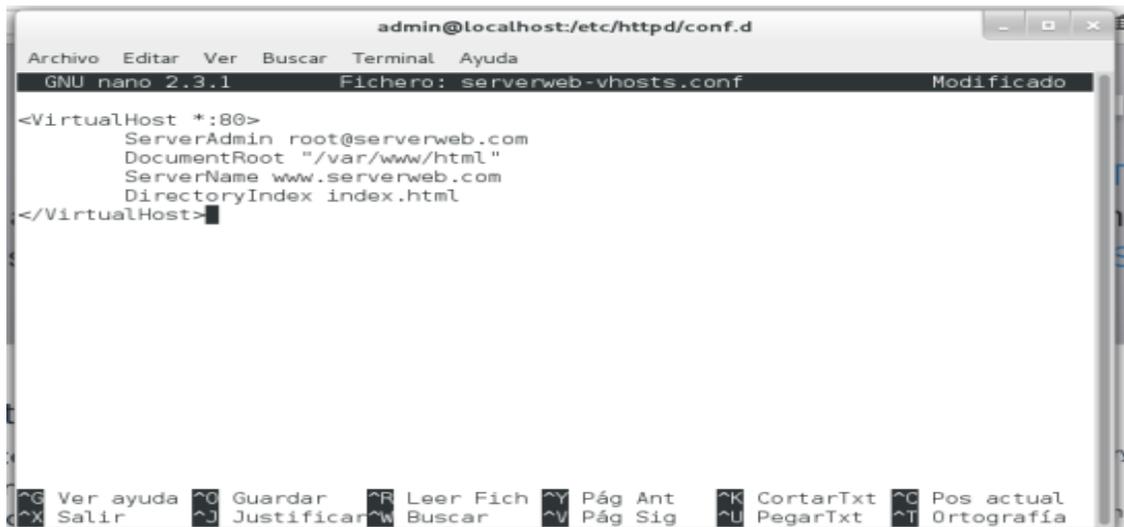
¡Listo!
[root@localhost admin]# systemctl start httpd
[root@localhost admin]# rpm -q httpd
httpd-2.4.6-31.el7.centos.1.x86_64
[root@localhost admin]# systemctl start httpd
[root@localhost admin]# nano /etc/httpd/conf/httpd.conf^C
[root@localhost admin]# nano /etc/httpd/conf/httpd.conf
[root@localhost admin]# cd /etc/httpd/conf.d/
[root@localhost conf.d]# nano serverweb -vhosts.conf
```

Figura 77. Después de que salimos vamos a digitar estos comandos en el terminal.



```
[root@localhost admin]# nano /etc/httpd/conf/httpd.conf
[root@localhost admin]# cd /etc/httpd/conf.d/
[root@localhost conf.d]# nano serverweb -vhosts.conf
```

Figura 78. Después de que ingresamos vamos ingresar estas líneas de comandos para configurar nuestro servidor web.



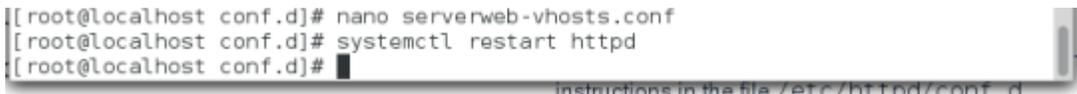
```
admin@localhost:/etc/httpd/conf.d
GNU nano 2.3.1 Fichero: serverweb-vhosts.conf Modificado
<VirtualHost *:80>
  ServerAdmin root@serverweb.com
  DocumentRoot "/var/www/html"
  ServerName www.serverweb.com
  DirectoryIndex index.html
</VirtualHost>
```

Figura 79. Después de que agregamos las líneas vamos a guardar con ctrl + o y con ctrl + x salir del editor de nano, volvemos de nuevo a terminal.



```
admin@localhost:/etc/httpd/conf.d
Archivo Editar Ver Buscar Terminal Ayuda
-i --autoindent Indentar automáticamente nuevas líneas
-k --cut Cortar desde el cursor al final de línea
-l --nofollow No seguir enlaces simbólicos, sobrescri
birlos
-m --mouse Habilitar el uso del ratón
-o <dir> --operatingdir=<dir> Establecer el directorio de operación
-p --preserve Conservar teclas XON (^Q) y XOFF (^S)
-q --quiet Silently ignore startup issues like rc f
ile errors
-r <núm> --fill=<núm> Fijar el límite de ajuste de líneas en n
úm columnas
-s <prog> --speller=<prog> Habilitar corrector alternativo
-t --tempfile Autosalvar al salir, no preguntar
-u --undo Allow generic undo [EXPERIMENTAL]
-v --view Modo visualización (sólo lectura)
-w --nowrap No wrappear líneas largas
-x --nohelp No mostrar las dos líneas de ayuda
-z --suspend Habilitar suspensión
-$ --softwrap Enable soft line wrapping
-a, -b, -e,
-f, -g, -j (se ignora, está por compatibilidad con
Pico)
[root@localhost conf.d]# nano serverweb-vhosts.conf
[root@localhost conf.d]#
```

Figura 80. Ahora vamos a reiniciar el servidor web.



```
[root@localhost conf.d]# nano serverweb-vhosts.conf
[root@localhost conf.d]# systemctl restart httpd
[root@localhost conf.d]#
```

Figura 81. Ahora vamos a configurar la ip de dirección ipv6.



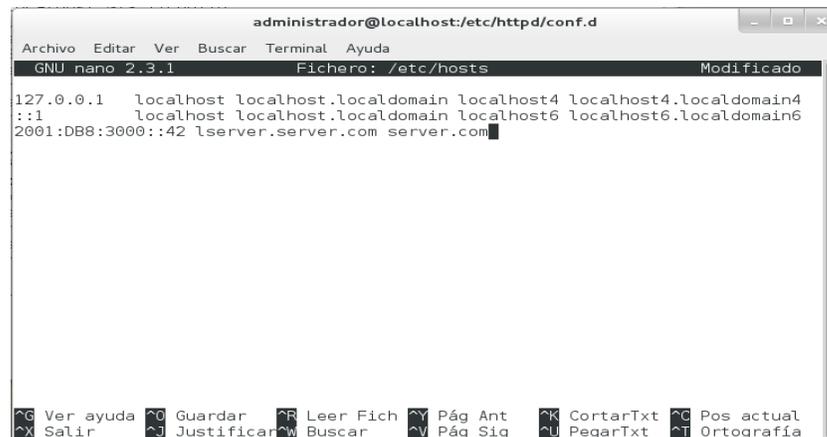
```
[root@localhost conf.d]# nano /etc/hosts
```

Figura 82. Ahora vamos a cambiar unos parámetros.



```
admin@localhost:/etc/httpd/conf.d
GNU nano 2.3.1 Fichero: /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
[ 2 líneas leídas ]
Ver ayuda Guardar Leer Fich Pág Ant CortarTxt Pos actual
Salir Justificar Buscar Pág Sig PegarTxt Ortografía
```

Figura 83. En el pantallazo cambiamos los parámetros y digitamos la dirección ip que vamos a usar con el nombre del servidor que pusimos.



```
administrador@localhost:/etc/httpd/conf.d
GNU nano 2.3.1 Fichero: /etc/hosts Modificado
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
2001:DB8:3000::42 lserver.server.com server.com
Ver ayuda Guardar Leer Fich Pág Ant CortarTxt Pos actual
Salir Justificar Buscar Pág Sig PegarTxt Ortografía
```

Figura 84. Ahora que cambiamos los parámetros vamos a guardar con `ctrl + o` y con `ctrl + x` podemos salir del editor de hosts, después regresamos al menú de terminal.

```

admin@localhost:/etc/httpd/conf.d
Archivo Editar Ver Buscar Terminal Ayuda
-l --nofollow No seguir enlaces simbólicos, sobrescri
birlos
-m --mouse Habilitar el uso del ratón
-o <dir> --operatingdir=<dir> Establecer el directorio de operación
-p --preserve Conservar teclas XON (^Q) y XOFF (^S)
-q --quiet Silently ignore startup issues like rc f
file errors
-r <núm> --fill=<núm> Fijar el límite de ajuste de líneas en n
úm columnas
-s <prog> --speller=<prog> Habilitar corrector alternativo
-t --tempfile Autosalvar al salir, no preguntar
-u --undo Allow generic undo [EXPERIMENTAL]
-v --view Modo visualización (sólo lectura)
-w --nowrap No wrappear líneas largas
-x --nohelp No mostrar las dos líneas de ayuda
-z --suspend Habilitar suspensión
-$_ --softwrap Enable soft line wrapping
-a, -b, -e,
-f, -g, -j (se ignora, está por compatibilidad con
Pico)
[root@localhost conf.d]# nano serverweb-vhosts.conf
[root@localhost conf.d]# systemctl restart httpd
[root@localhost conf.d]# nano /etc/hosts
[root@localhost conf.d]#

```

Figura 85. Vamos a ingresar al editor de index.html

```

[root@localhost conf.d]# nano /var/www/html/index.html

```

Figura 86. Ya ingresando al editor index.html nos va aparecer de esta manera.

```

admin@localhost:/etc/httpd/conf.d
GNU nano 2.3.1 Fichero: /var/www/html/index.html
[ Nuevo Fichero ]
Ver ayuda  Guardar  Leer Fich  Pág Ant  CortarTxt  Pos actual
Salir      Justificar  Buscar    Pág Sig  PegarTxt   Ortografía

```

Figura 87. Vamos ingresar los parámetros para agregar la página web para nuestro servidor.

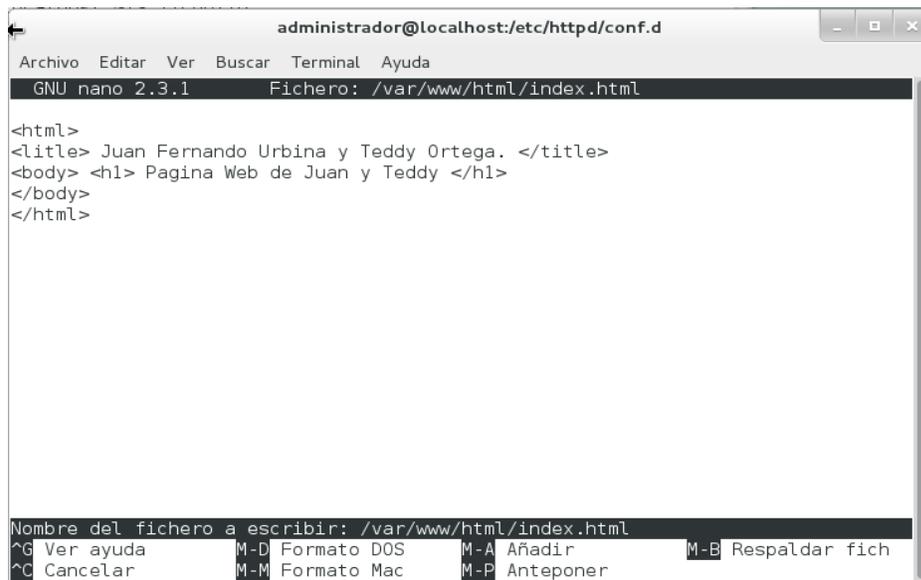


The screenshot shows a terminal window titled "administrador@localhost:/etc/httpd/conf.d". The nano editor is open to the file "/var/www/html/index.html". The content of the file is:

```
<html>
<title> Juan Fernando Urbina y Teddy Ortega. </title>
<body> <h1> Pagina Web de Juan y Teddy </h1>
</body>
</html>
```

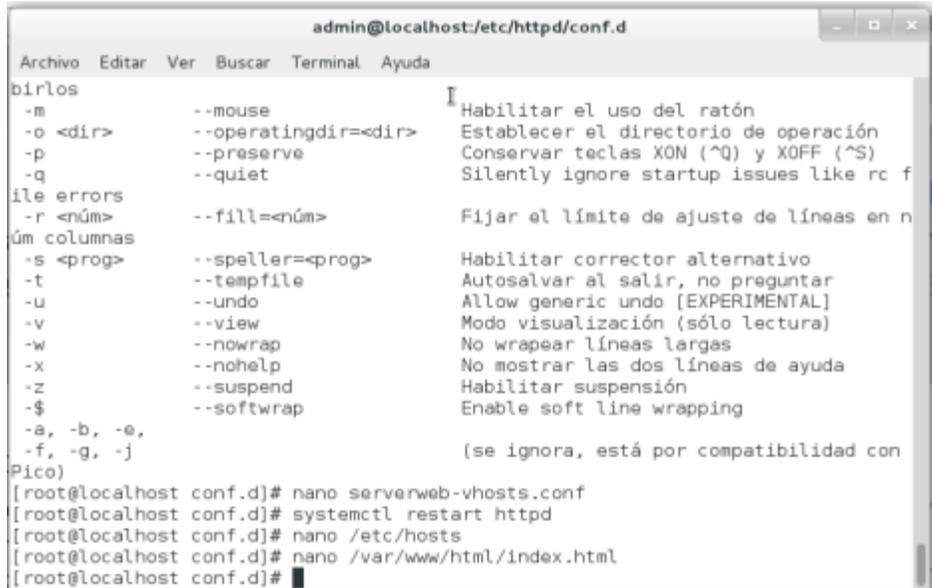
The status bar at the bottom indicates "[5 líneas leídas]" and lists various keyboard shortcuts such as ^G Ver ayuda, ^O Guardar, ^R Leer Fich, ^Y Pág Ant, ^K CortarTxt, ^C Pos actual, ^X Salir, ^J Justificar, ^W Buscar, ^V Pág Sig, ^U PegarTxt, and ^T Ortografía.

Figura 88. Vamos a guardar con ctrl + o y ctrl + x cerrar nuestro editor index.html



The screenshot shows the same nano editor window. The content of the file is identical to the previous image. The status bar at the bottom now shows "Nombre del fichero a escribir: /var/www/html/index.html" and lists additional keyboard shortcuts: ^G Ver ayuda, M-D Formato DOS, M-A Añadir, M-B Respaldar fich, ^C Cancelar, M-M Formato Mac, and M-P Anteponer.

Figura 89. Ahora volvemos de nuevo a la ventana de terminal.



```
admin@localhost:/etc/httpd/conf.d
Archivo Editar Ver Buscar Terminal Ayuda
dirlos
-m --mouse Habilitar el uso del ratón
-o <dir> --operatingdir=<dir> Establecer el directorio de operación
-p --preserve Conservar teclas XON (^Q) y XOFF (^S)
-q --quiet Silently ignore startup issues like rc f
file errors
-r <núm> --fill=<núm> Fijar el límite de ajuste de líneas en n
úm columnas
-s <prog> --speller=<prog> Habilitar corrector alternativo
-t --tempfile Autosalvar al salir, no preguntar
-u --undo Allow generic undo [EXPERIMENTAL]
-v --view Modo visualización (sólo lectura)
-w --nowrap No wrappear líneas largas
-x --nohelp No mostrar las dos líneas de ayuda
-z --suspend Habilitar suspensión
-$_ --softwrap Enable soft line wrapping
-a, -b, -e,
-f, -g, -j (se ignora, está por compatibilidad con
Pico)
[root@localhost conf.d]# nano serverweb-vhosts.conf
[root@localhost conf.d]# systemctl restart httpd
[root@localhost conf.d]# nano /etc/hosts
[root@localhost conf.d]# nano /var/www/html/index.html
[root@localhost conf.d]#
```

Figura 90. Vamos a buscar la opción de configuración de la red.

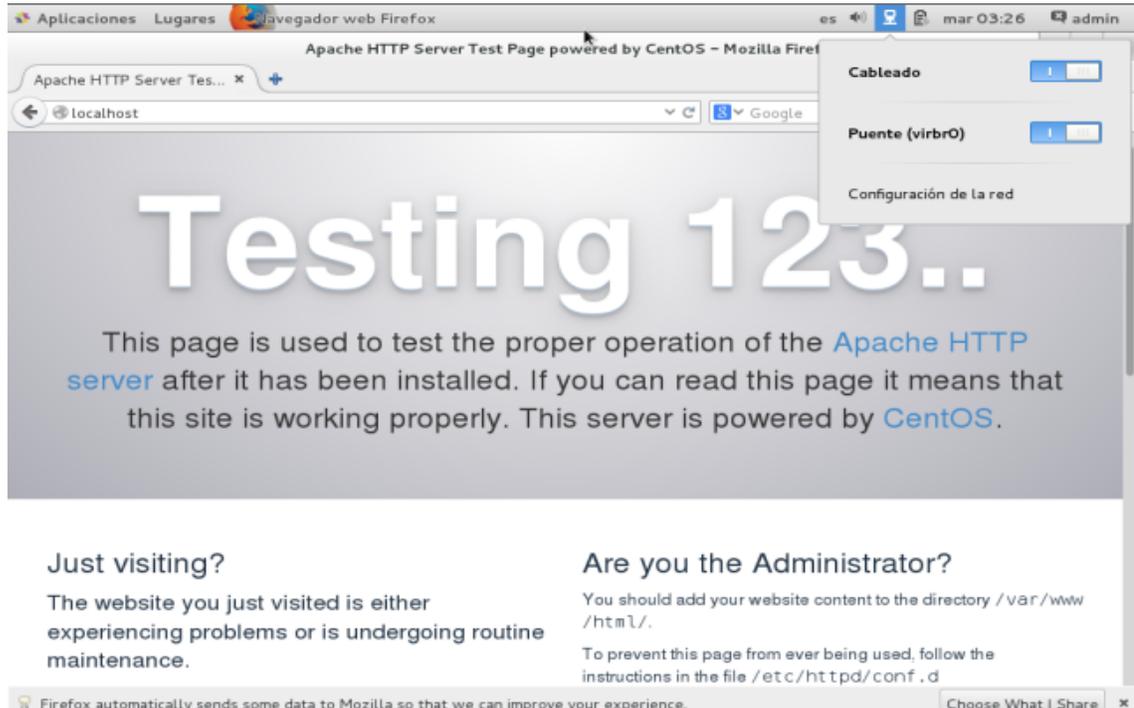


Figura 91. Ahora vamos a configuraciones y vamos a agregar la ip.

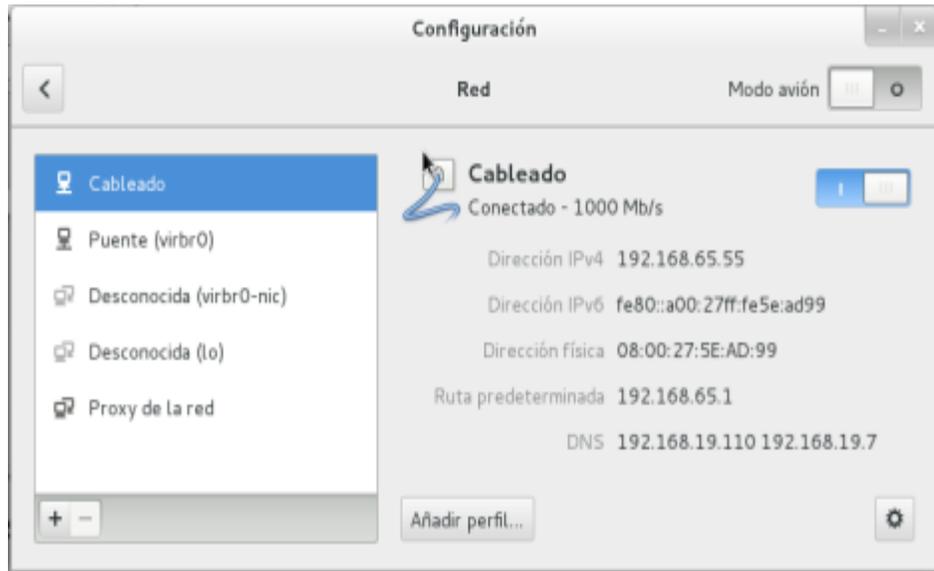


Figura 92. Ahora vamos a ipv4 para poder configurar la dirección ipv6 2001:DB8:ACAD:3::1/64 , su máscara de red y su puerta de enlace como muestra en la imagen.

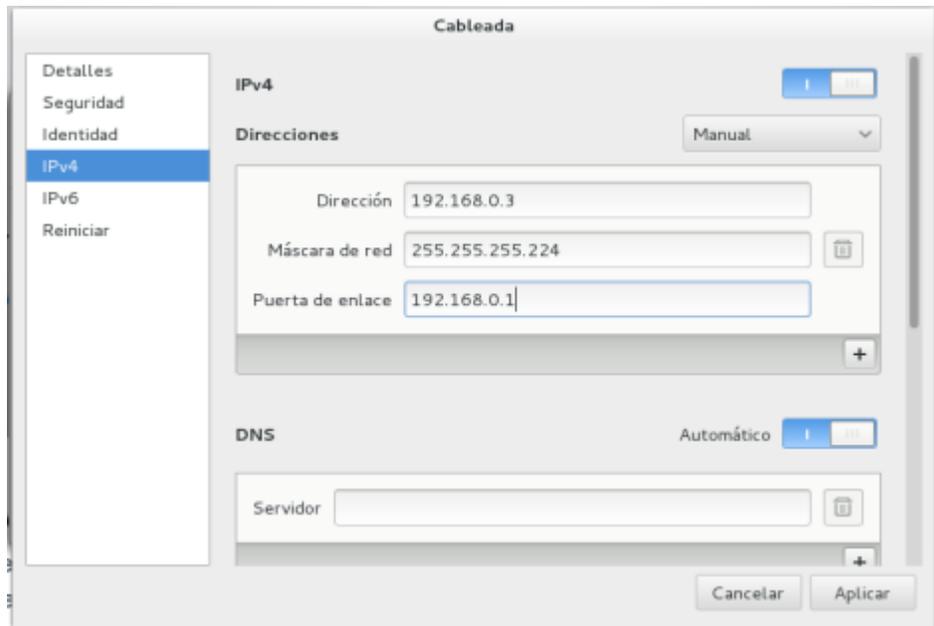


Figura 93. Vamos a configurar dirección ip 192.168.0.2 al servidor y después vamos a la opción aplicar para guardar los cambios.

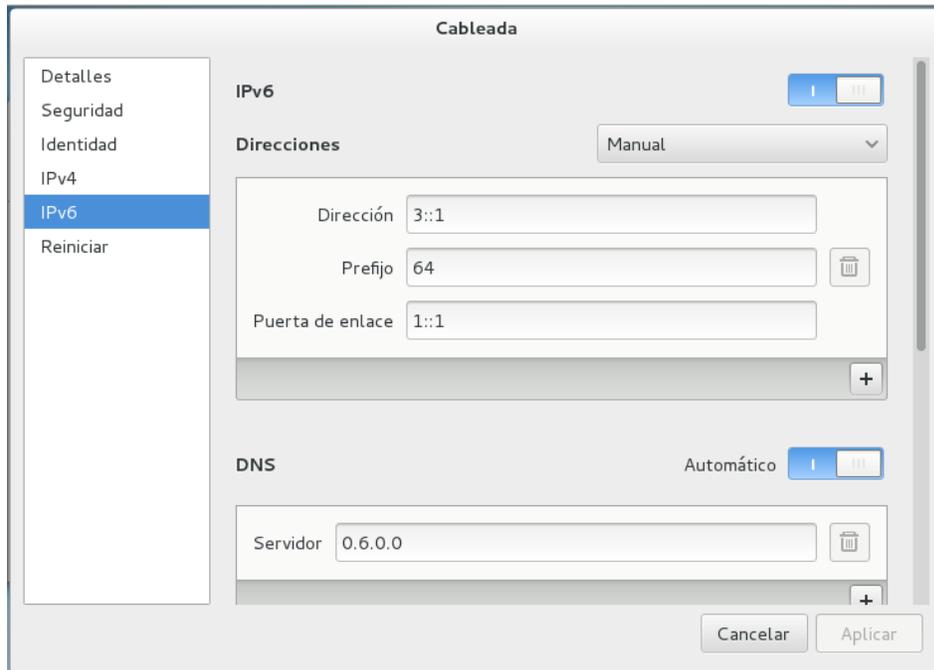


Figura 94. Vamos a deshabilitar y habilitar el botón azul para que tome cambio de la ip que ingresamos.

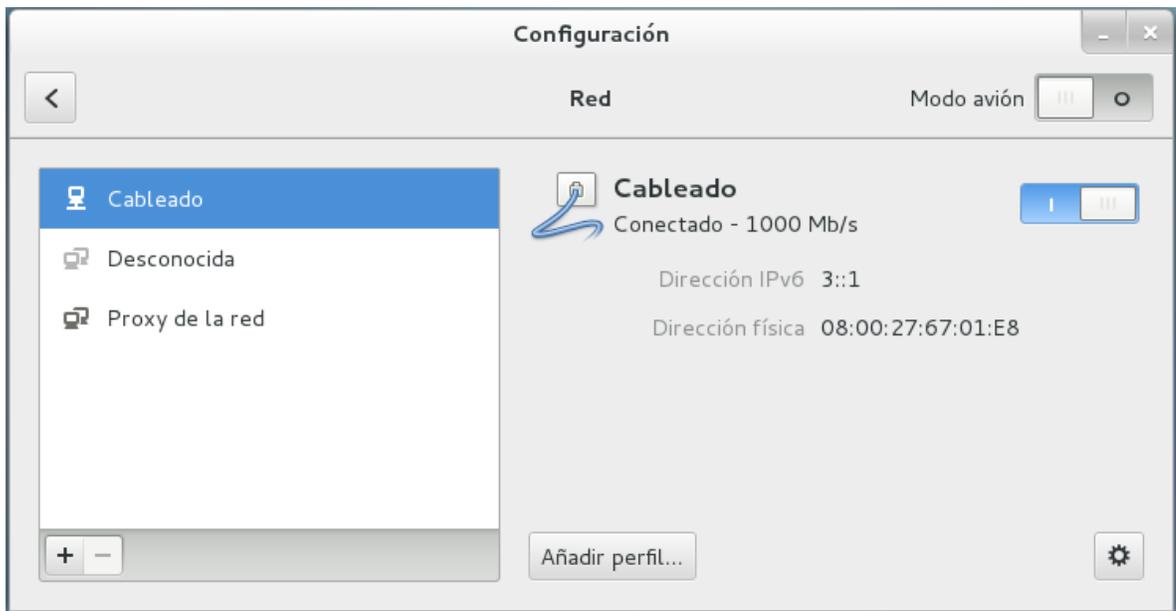


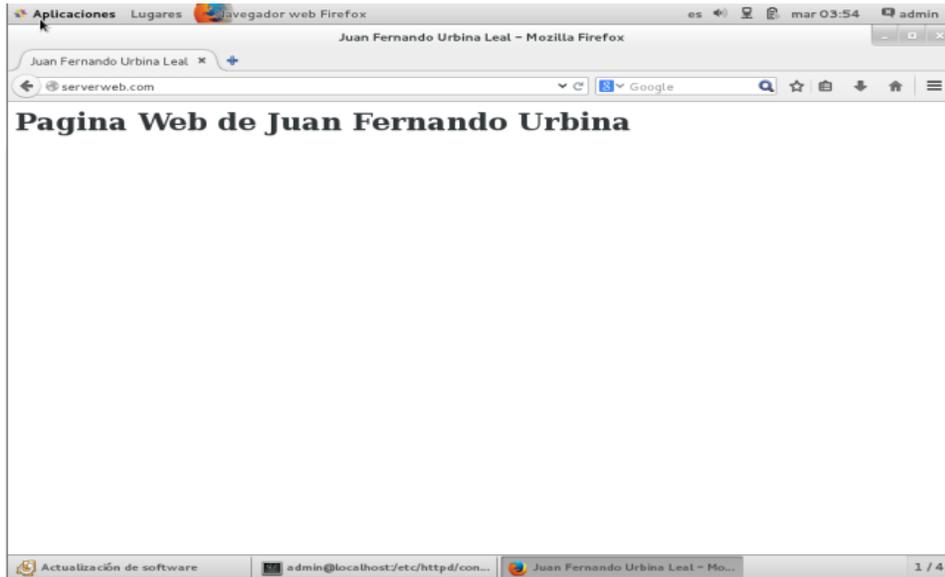
Figura 95. Vamos a verificar con nuestro explorador nuestra página web que agregamos con esta dirección 127.0.0.1.



Figura 96. Vamos a verificar con la dirección ip.



Figura 97. Vamos a verificar por ultimo con nuestro servidor web que es serverweb.com, cuando no sirva el servidor web o httpd debemos subirlo con el siguiente comando: `systemctl start httpd` y recuerden que tienen que ser root para levantar el servicios.



4.2.4 Configuración de DHCP en gns3.

Figura 98. Vamos a Browse el icono siguiente para agregar los router que vamos a usar para configurar DHCP.



Figura 99. Configurando el siguiente red en el cual vamos a configurar DHCP.

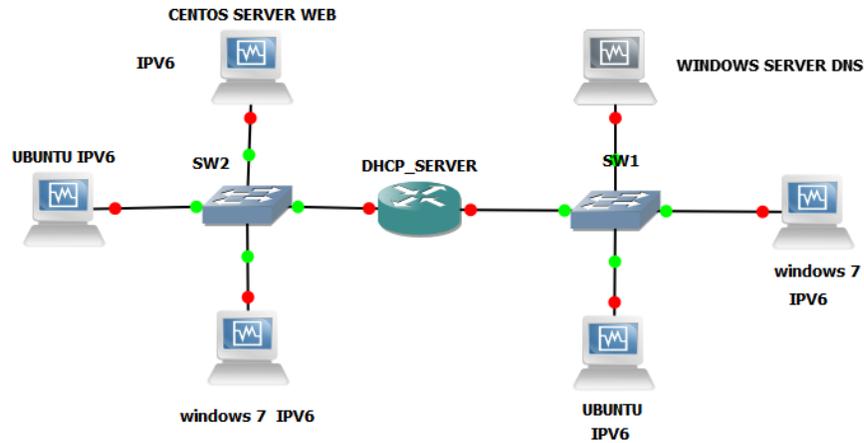


Figura 100. Vamos a configurar el router DHCP_SERVER, vamos a dar doble click en DCHP_SERVER nos aparecerá la siguiente ventana.

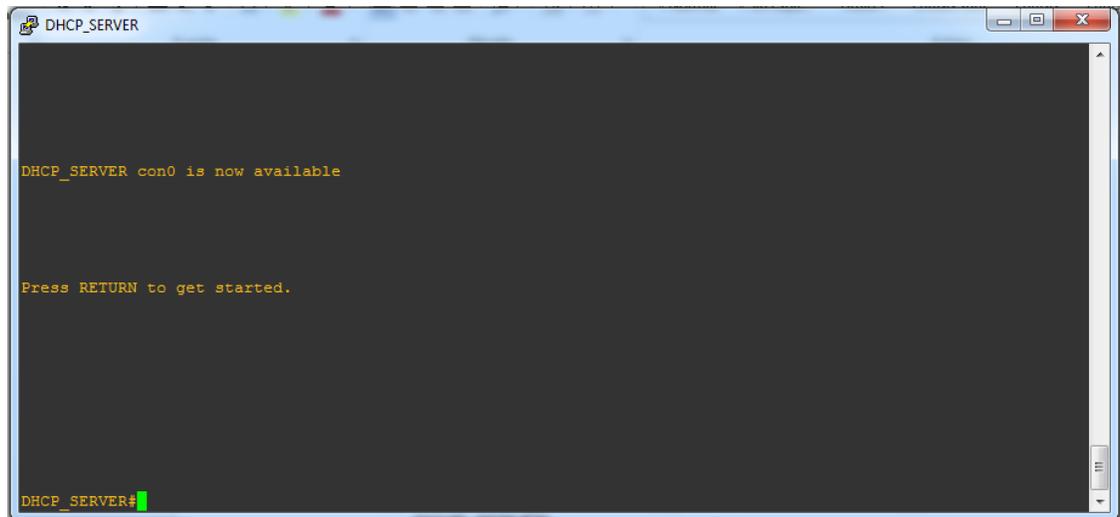
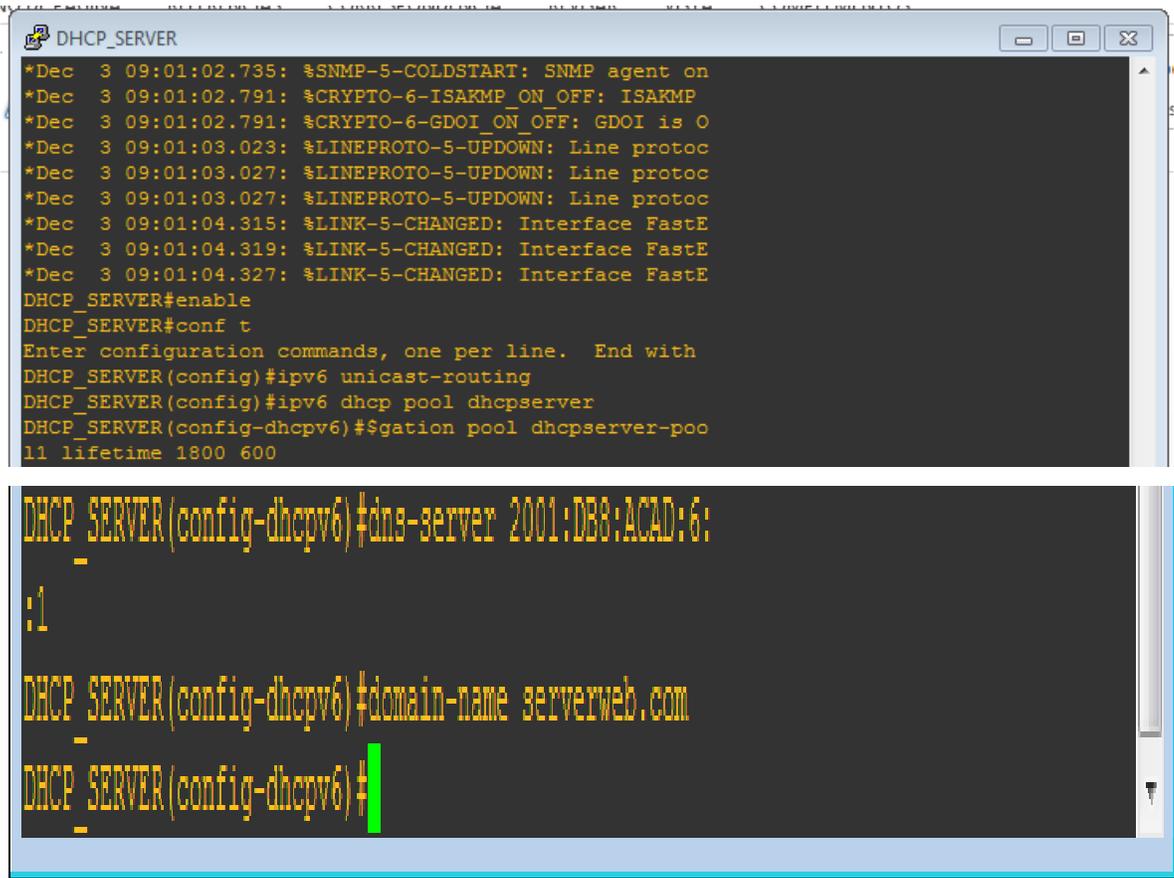


Figura 101. Vamos a ingresar estos comando para configurar el DHCP_SERVER:

```
DHCP_SERVER (config)# ipv6 unicast-routing
DHCP_SERVER (config)# ipv6 dhcp pool dhcpserver
DHCP_SERVER (config-dhcp)# prefix-delegation pool dhcpserve-pool1 lifetime
1800 600
DHCP_SERVER (config-dhcp)# dns-server 2001:DB8:ACAD:6::1
DHCP_SERVER (config-dhcp)# domain-name serverweb.com
```



```
DHCP_SERVER
*Dec 3 09:01:02.735: %SNMP-5-COLDSTART: SNMP agent on
*Dec 3 09:01:02.791: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP
*Dec 3 09:01:02.791: %CRYPTO-6-GDOI_ON_OFF: GDOI is O
*Dec 3 09:01:03.023: %LINEPROTO-5-UPDOWN: Line protoc
*Dec 3 09:01:03.027: %LINEPROTO-5-UPDOWN: Line protoc
*Dec 3 09:01:03.027: %LINEPROTO-5-UPDOWN: Line protoc
*Dec 3 09:01:04.315: %LINK-5-CHANGED: Interface FastE
*Dec 3 09:01:04.319: %LINK-5-CHANGED: Interface FastE
*Dec 3 09:01:04.327: %LINK-5-CHANGED: Interface FastE
DHCP_SERVER#enable
DHCP_SERVER#conf t
Enter configuration commands, one per line. End with
DHCP_SERVER(config)#ipv6 unicast-routing
DHCP_SERVER(config)#ipv6 dhcp pool dhcpserver
DHCP_SERVER(config-dhcpv6)#$gation pool dhcpserver-poo
l1 lifetime 1800 600
DHCP_SERVER(config-dhcpv6)#dns-server 2001:DB8:ACAD:6:
:1
DHCP_SERVER(config-dhcpv6)#domain-name serverweb.com
DHCP_SERVER(config-dhcpv6)#
```

Figura 102. Vamos a configurar dirección ip en la interface fastethernet 1/0, ingresando estos comandos.

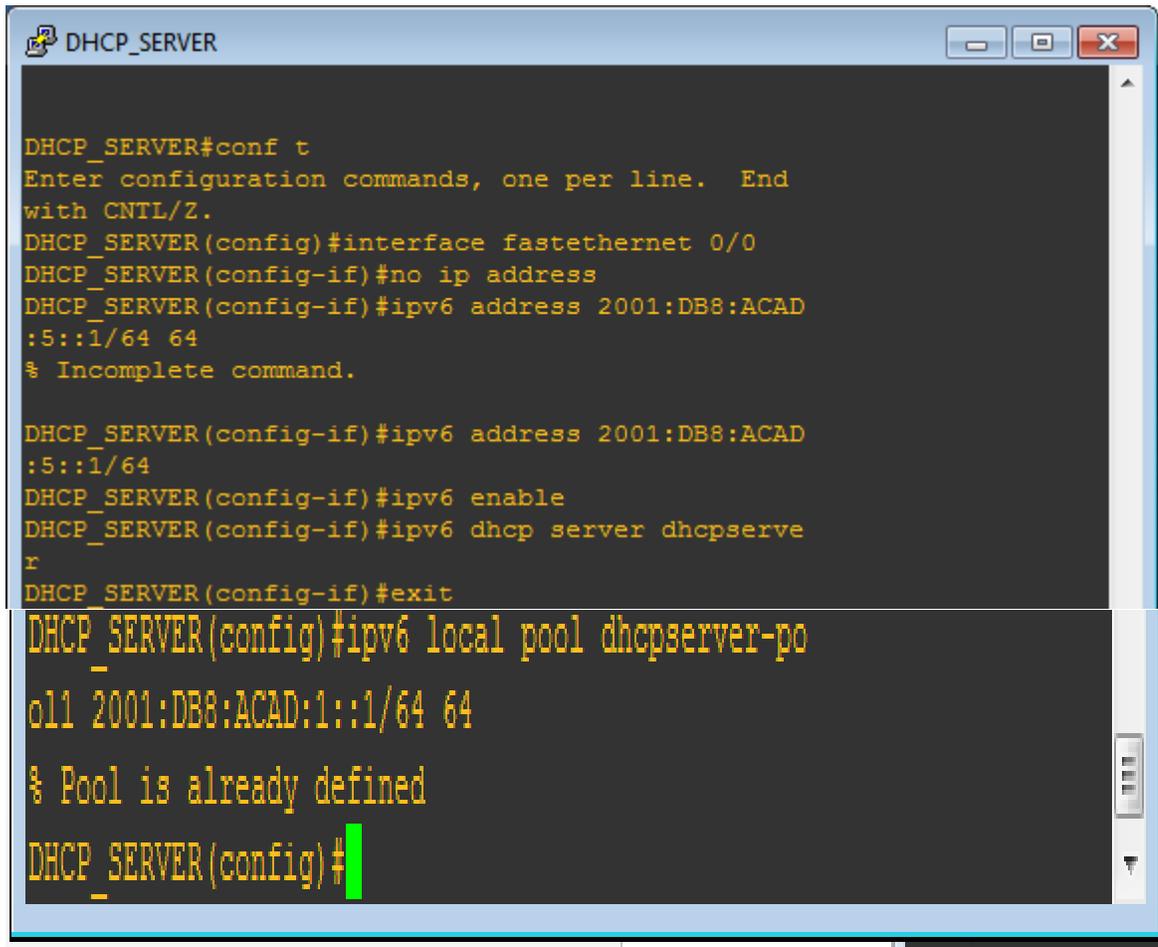
```
DHCP_SERVER (config)# interface fastethernet 1/0
DHCP_SERVER (config-if)# no ip address
DHCP_SERVER (config-if)# ipv6 address 2001:DB8:ACAD:4::1/64
DHCP_SERVER (config-if)# ipv6 enable
DHCP_SERVER (config-if)# ipv6 dhcp server dhcpserver
DHCP_SERVER (config-if)# exit
DHCP_SERVER (config)# ipv6 local pool dhcpserver-pool1
2001:DB8:ACAD:1::/64 64
```



```
DHCP_SERVER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DHCP_SERVER(config)#inter fastethernet 1/0
DHCP_SERVER(config-if)#no ip address
DHCP_SERVER(config-if)#ipv6 address 2001:DB8:ACAD:4::1/64
DHCP_SERVER(config-if)#ipv6 enable
DHCP_SERVER(config-if)#ipv6 dhcp server dhcpserver
DHCP_SERVER(config-if)#exit
DHCP_SERVER(config)#ipv6 local pool dhcpserver-pool1
11 2001:DB8:ACAD:1::/64 64
DHCP_SERVER(config)#
```

Figura 103. Vamos a configurar dirección ip en la interface fastethernet 2/0, ingresando estos comandos.

```
DHCP_SERVER (config)# interface fastethernet 0/0
DHCP_SERVER (config-if)# no ip address
DHCP_SERVER (config-if)# ipv6 address 2001:DB8:ACAD:5::1/64
DHCP_SERVER (config-if)# ipv6 enable
DHCP_SERVER (config-if)# ipv6 dhcp server dhcpserver
DHCP_SERVER (config-if)# exit
DHCP_SERVER (config)# ipv6 local pool dhcpserver-pool1
2001:DB8:ACAD:1::1/64 64
```



```
DHCP_SERVER#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
DHCP_SERVER(config)#interface fastethernet 0/0
DHCP_SERVER(config-if)#no ip address
DHCP_SERVER(config-if)#ipv6 address 2001:DB8:ACAD
:5::1/64 64
% Incomplete command.

DHCP_SERVER(config-if)#ipv6 address 2001:DB8:ACAD
:5::1/64
DHCP_SERVER(config-if)#ipv6 enable
DHCP_SERVER(config-if)#ipv6 dhcp server dhcpserve
r
DHCP_SERVER(config-if)#exit
DHCP_SERVER(config)#ipv6 local pool dhcpserver-po
ool1 2001:DB8:ACAD:1::1/64 64
% Pool is already defined
DHCP_SERVER(config)#
```

4.2.5 Configuración de DNS en WINDOWS SERVER 2012.

Figura 104. Configurar DNS server

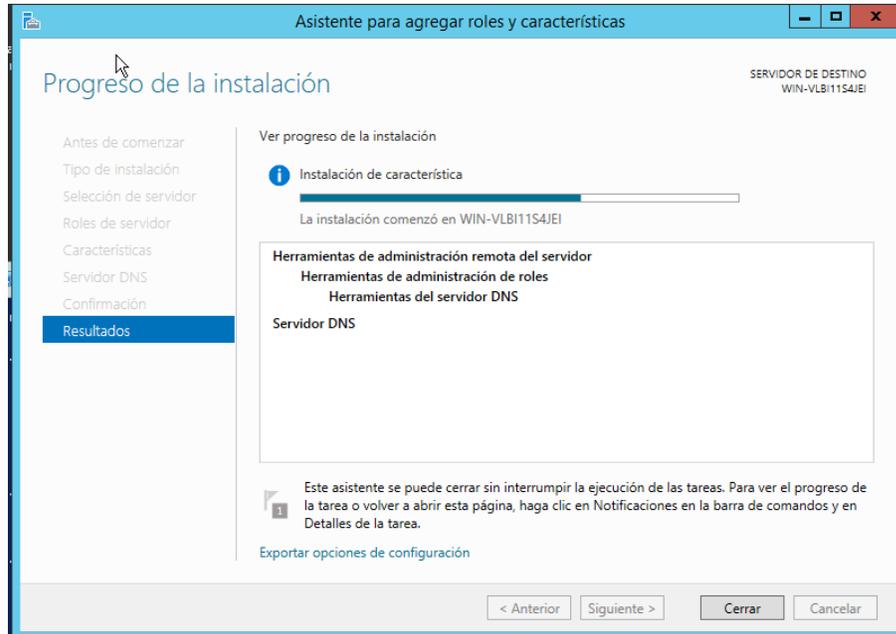


Figura 105. Ya terminado de instalar DNS ahora

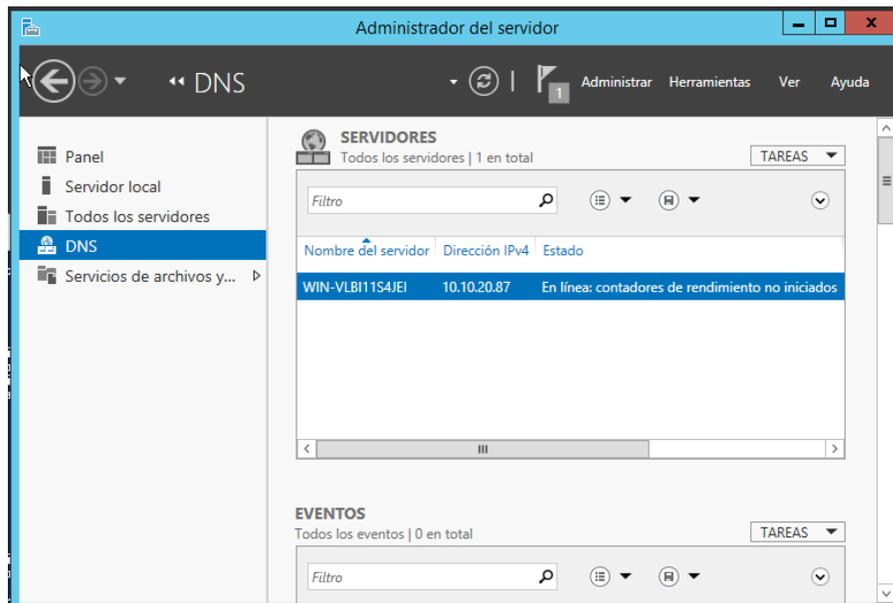


Figura 106. Vamos a crear un nuevo dominio en DNS

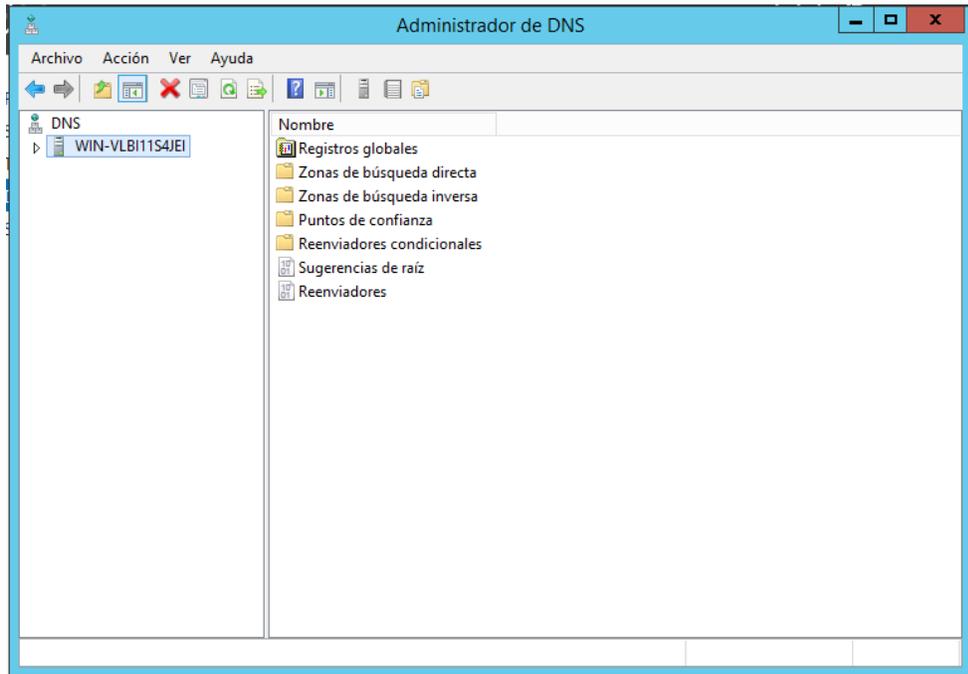


Figura 107. Configurar un servidor DNS.

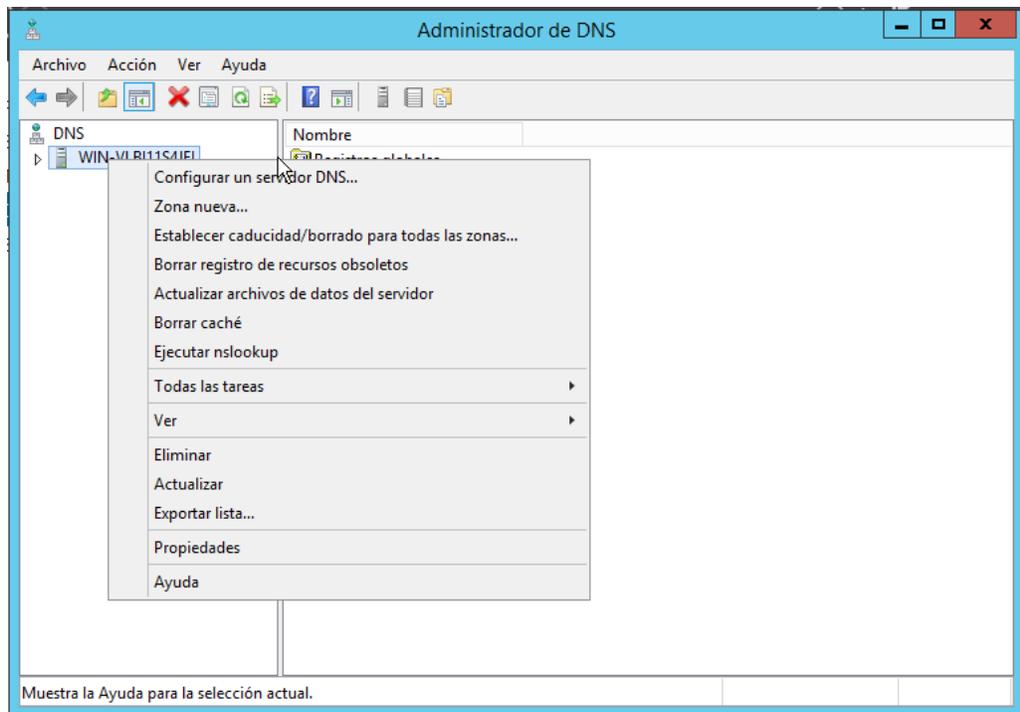


Figura 108. Después le damos siguiente

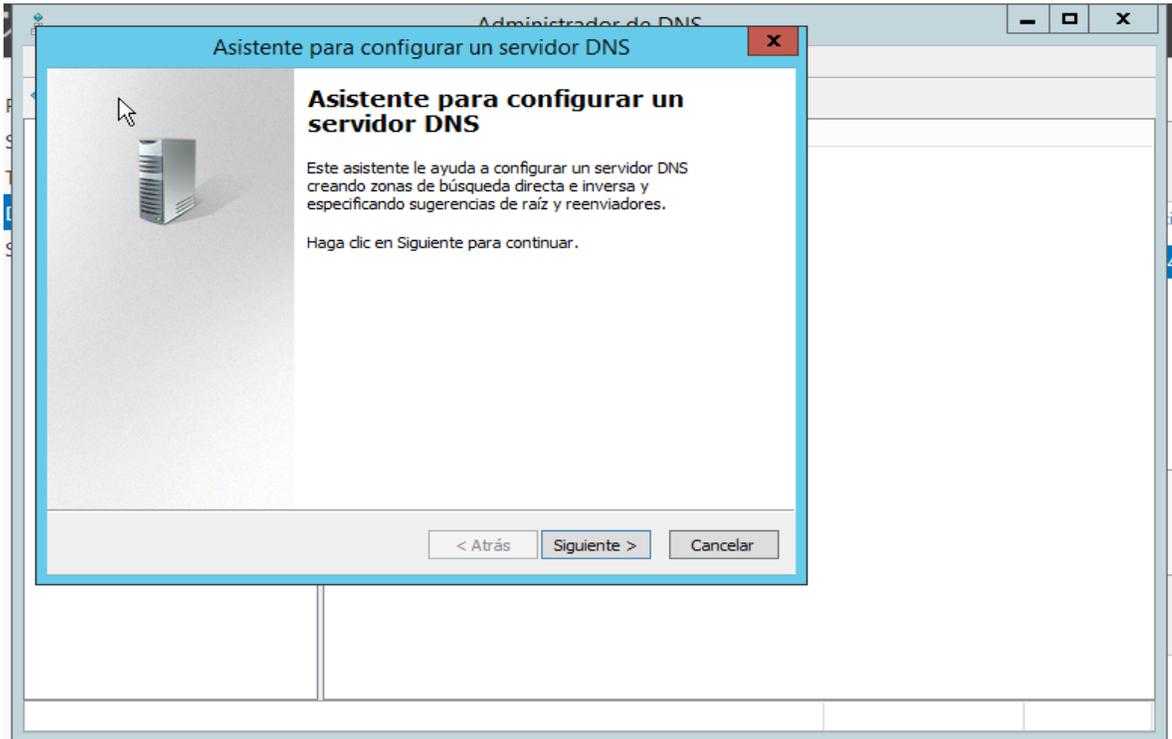


Figura 109. Vamos a escoger la segunda opción para que pueda soportar ipv6 y le damos siguiente.

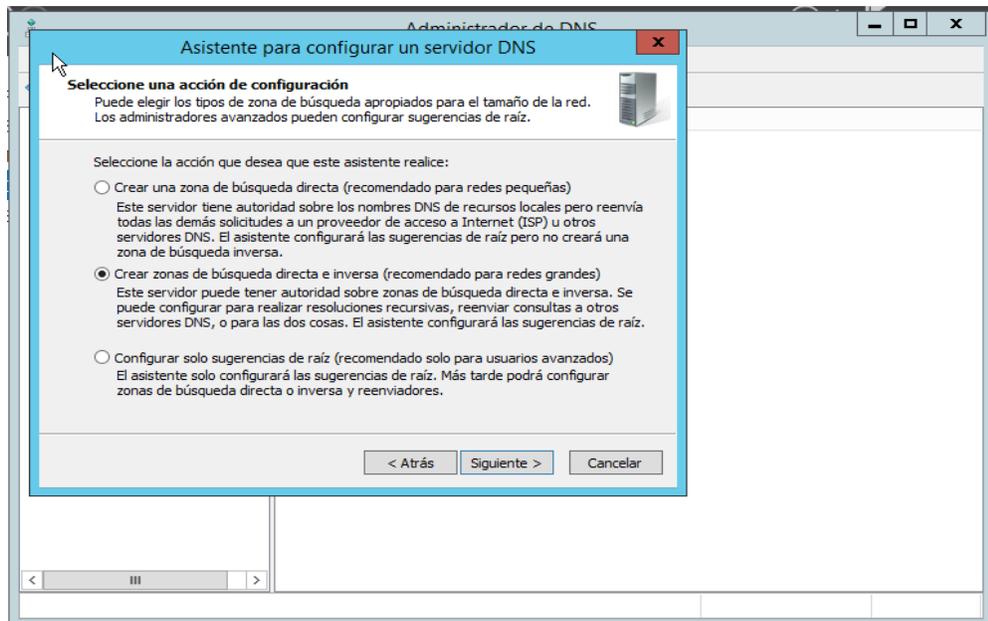


Figura 110. Escogemos la primera opción y le damos siguiente.

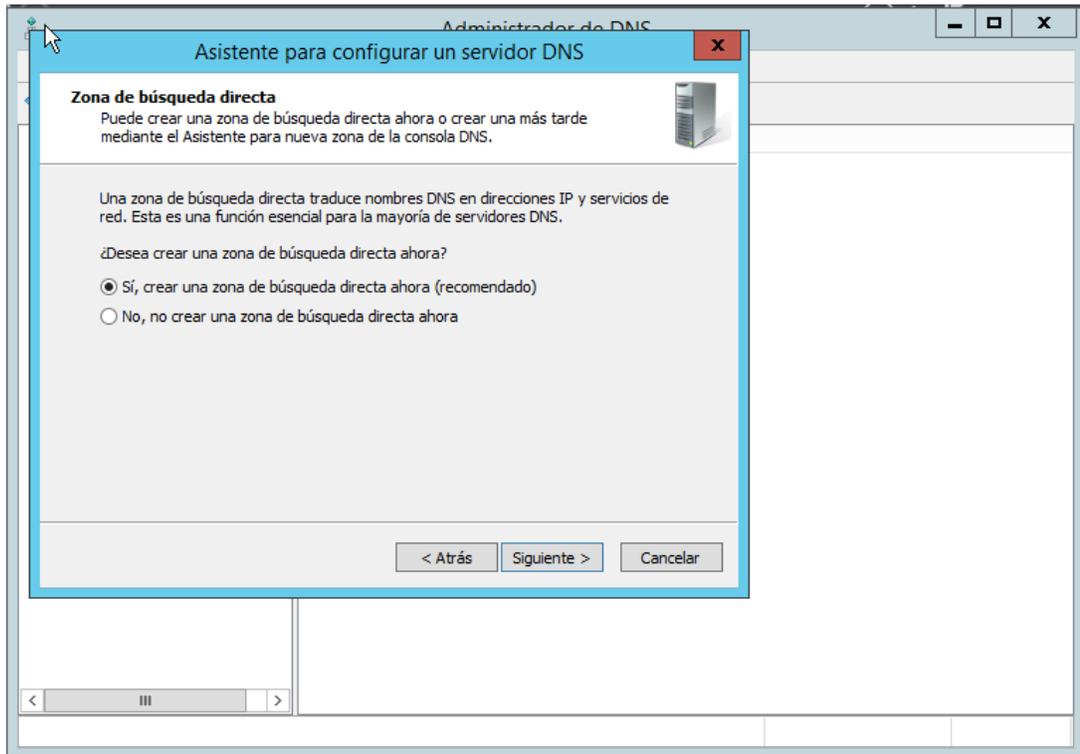


Figura 111. Vamos a escoger la primera opción.

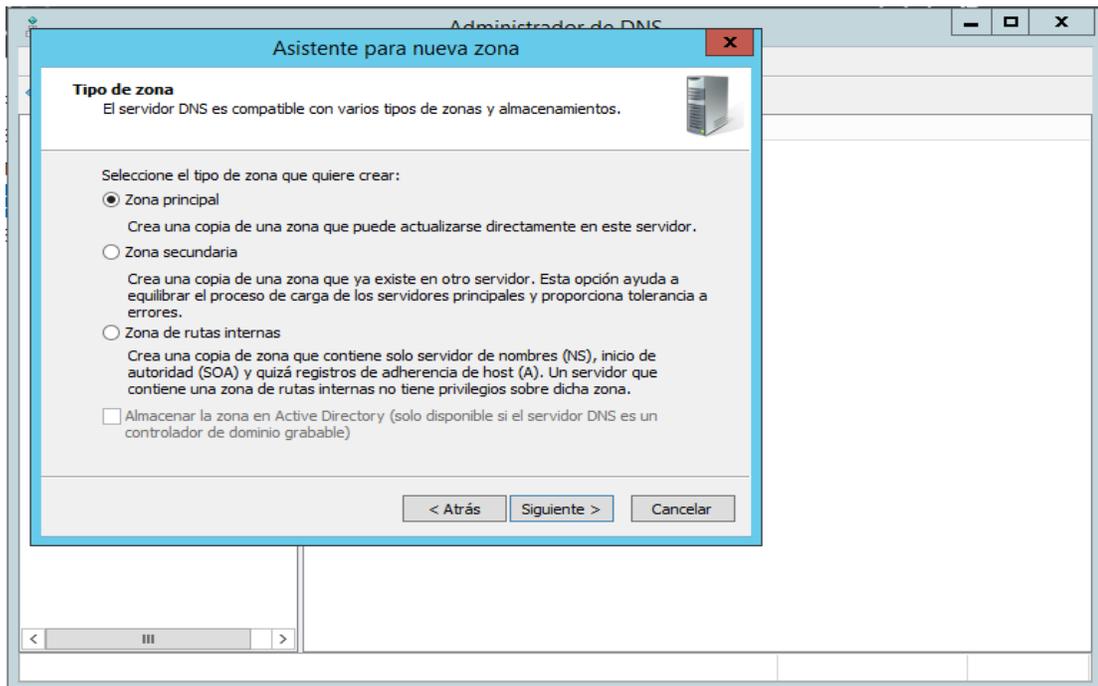


Figura 112. Vamos a ingresar nuestra zona que es www.serverweb.com y le damos siguiente.

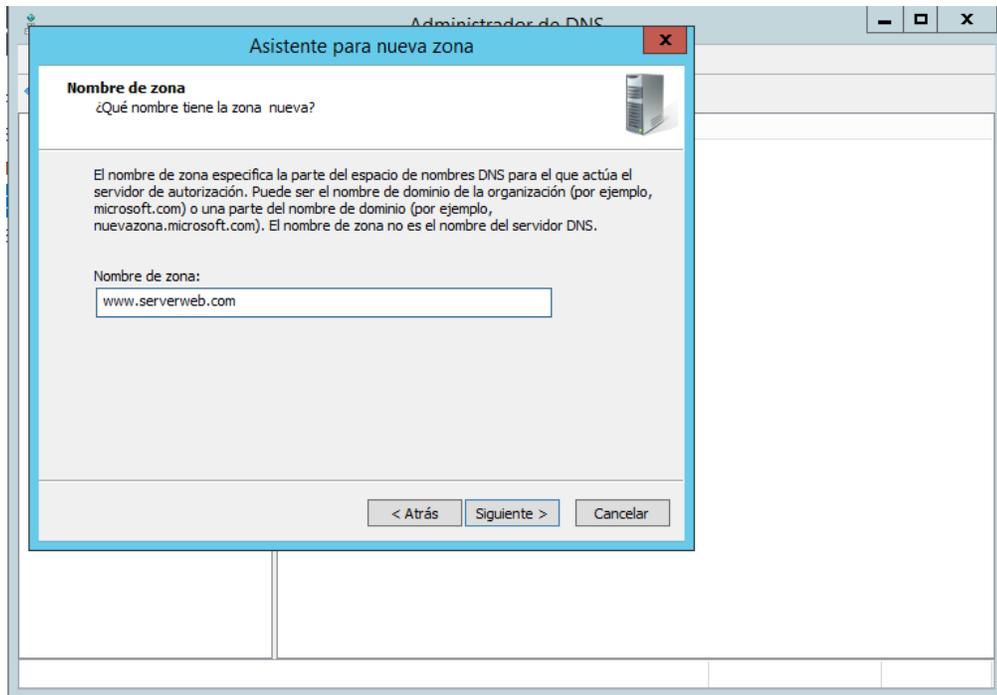


Figura 113. Vamos a escoger la primera opción y le damos siguiente.

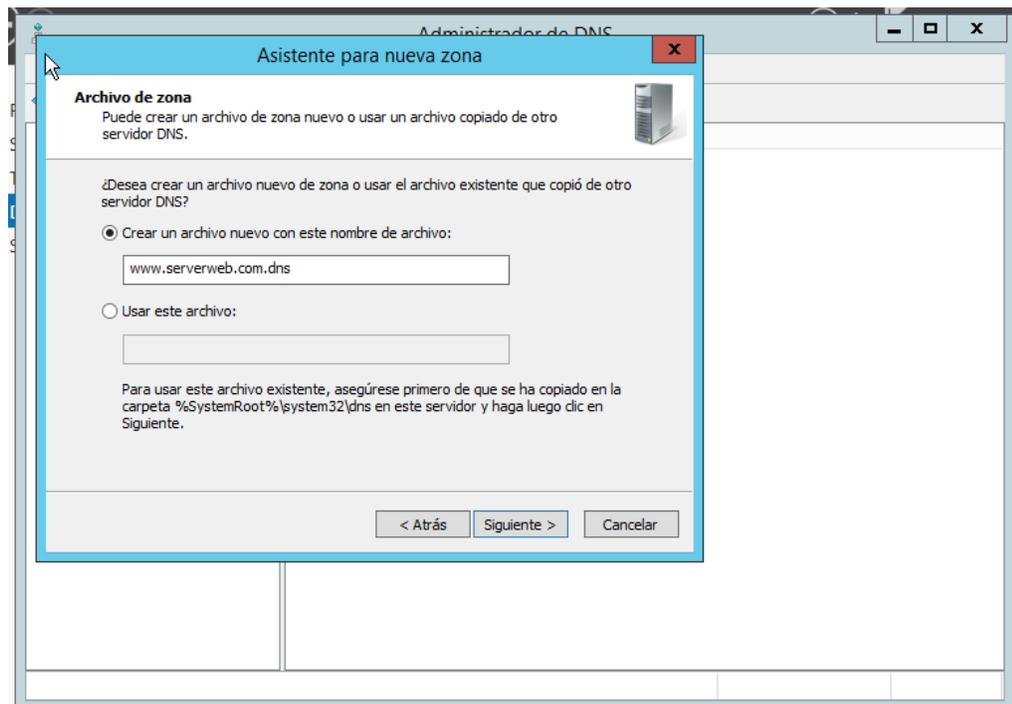


Figura 114. Vamos a escoger la segunda opción y le damos siguiente.

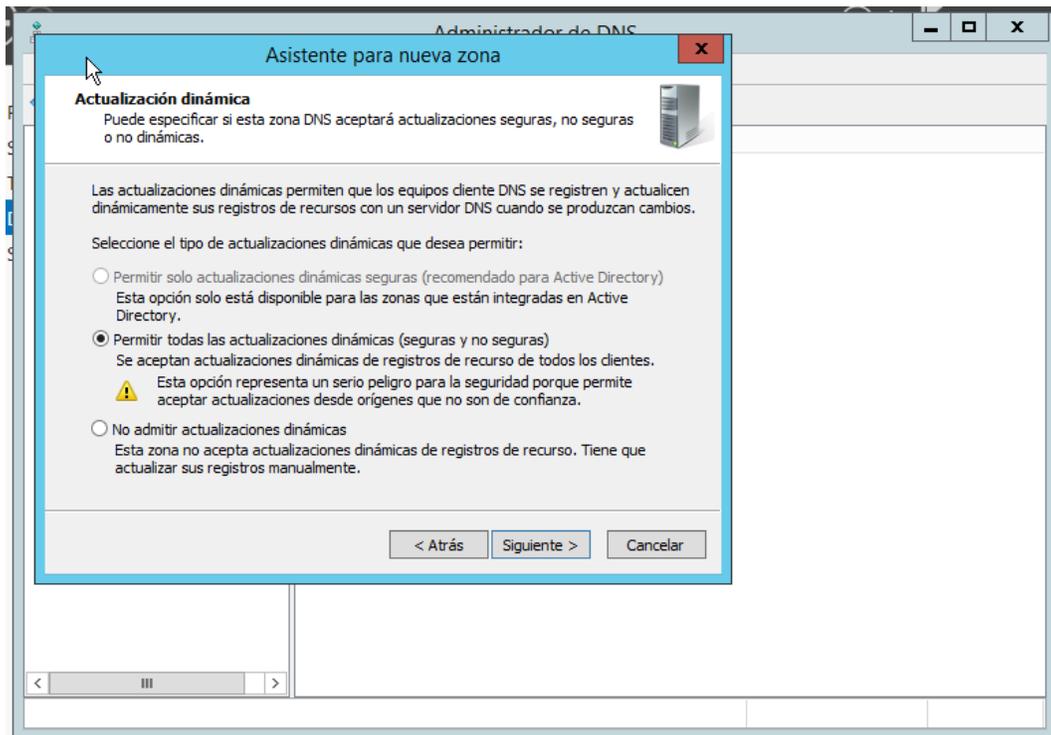


Figura 115. Vamos a configurar la zona inversa y le damos siguiente.

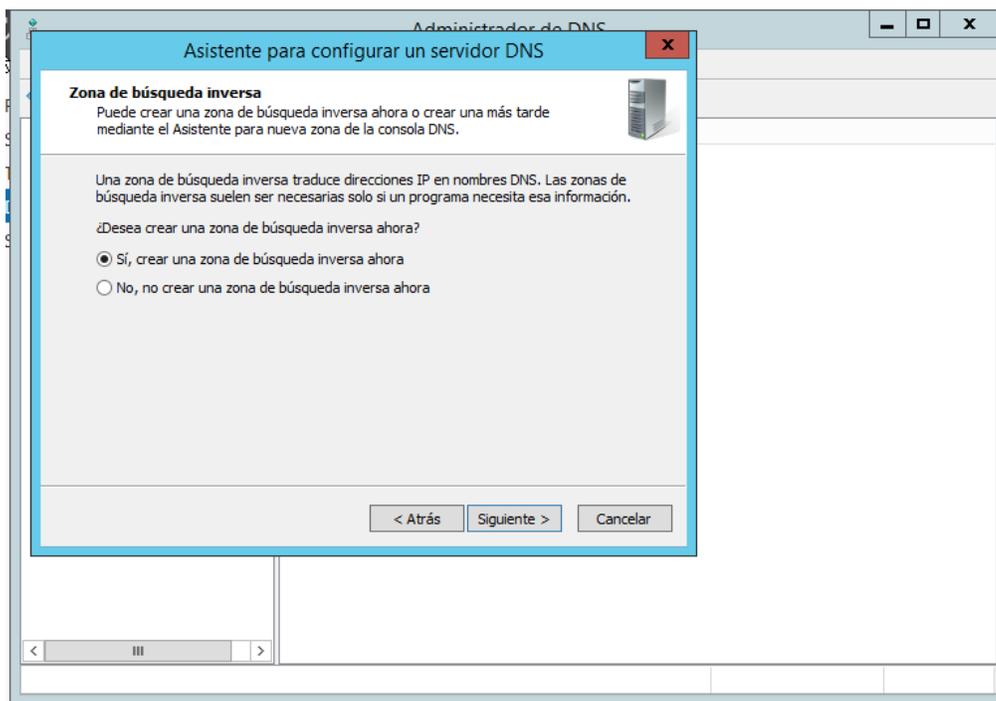


Figura 116. Vamos a dejar por defecto y siguiente.

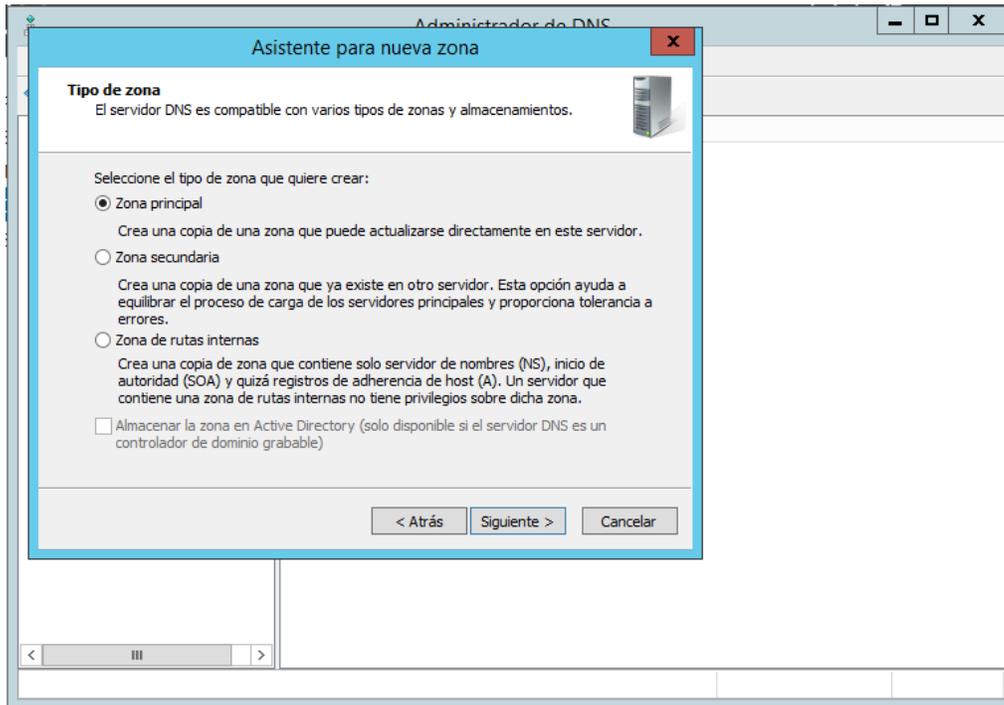


Figura 117. Vamos a escoger la segunda opción para que soporte IPV6.

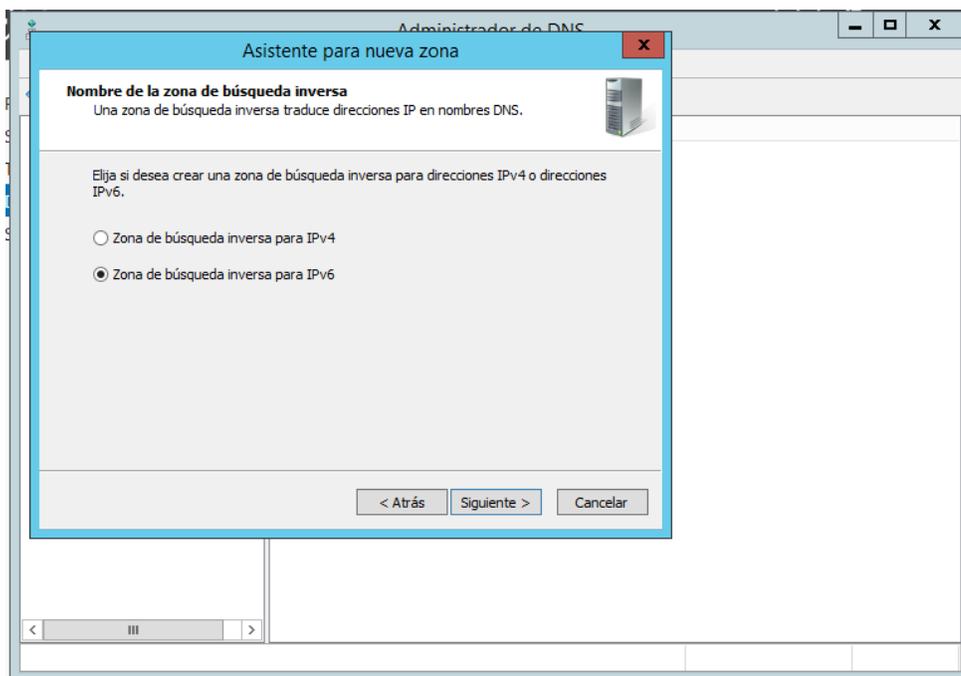


Figura 118. Aquí ingresamos la dirección ipv6 del DNS

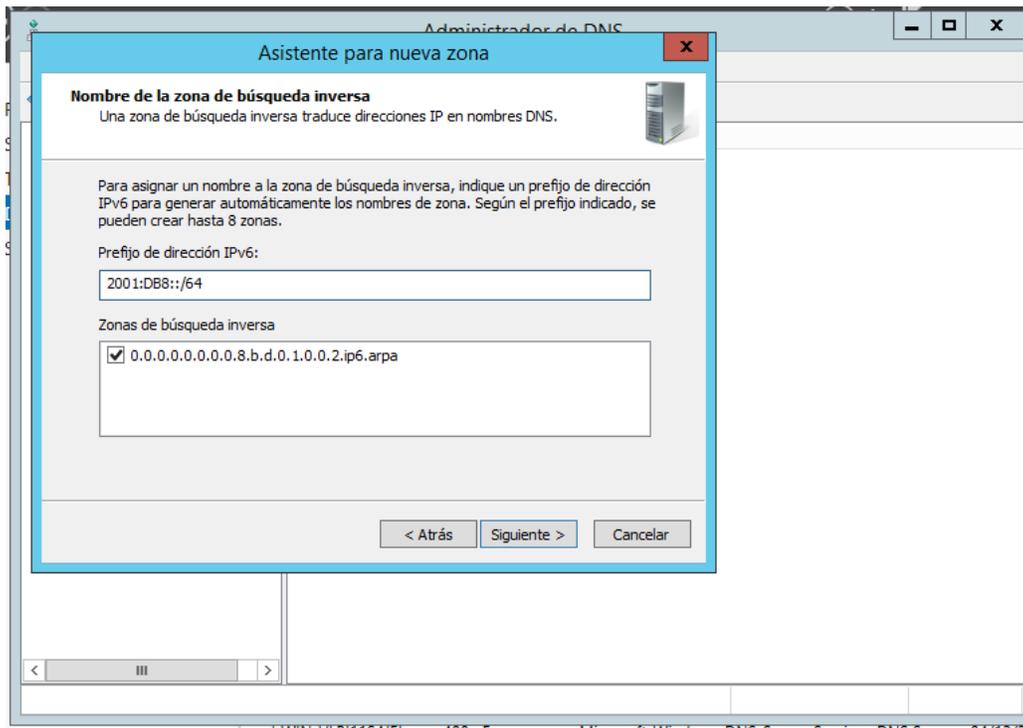


Figura 119. Creamos la zona www.serverweb.com

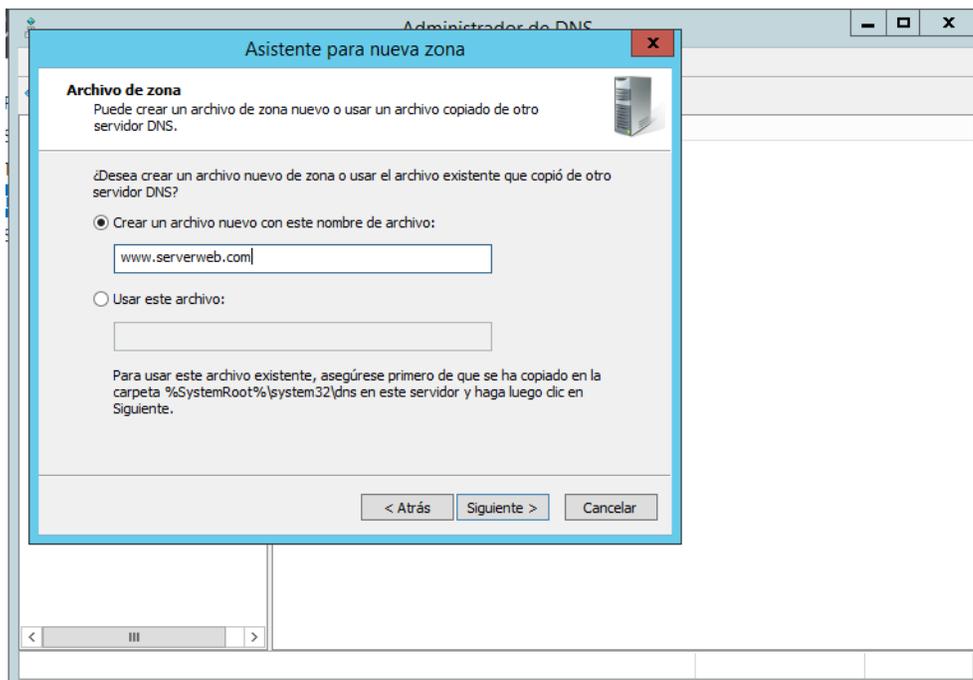


Figura 120. Escogemos la segunda opción y le damos siguiente.

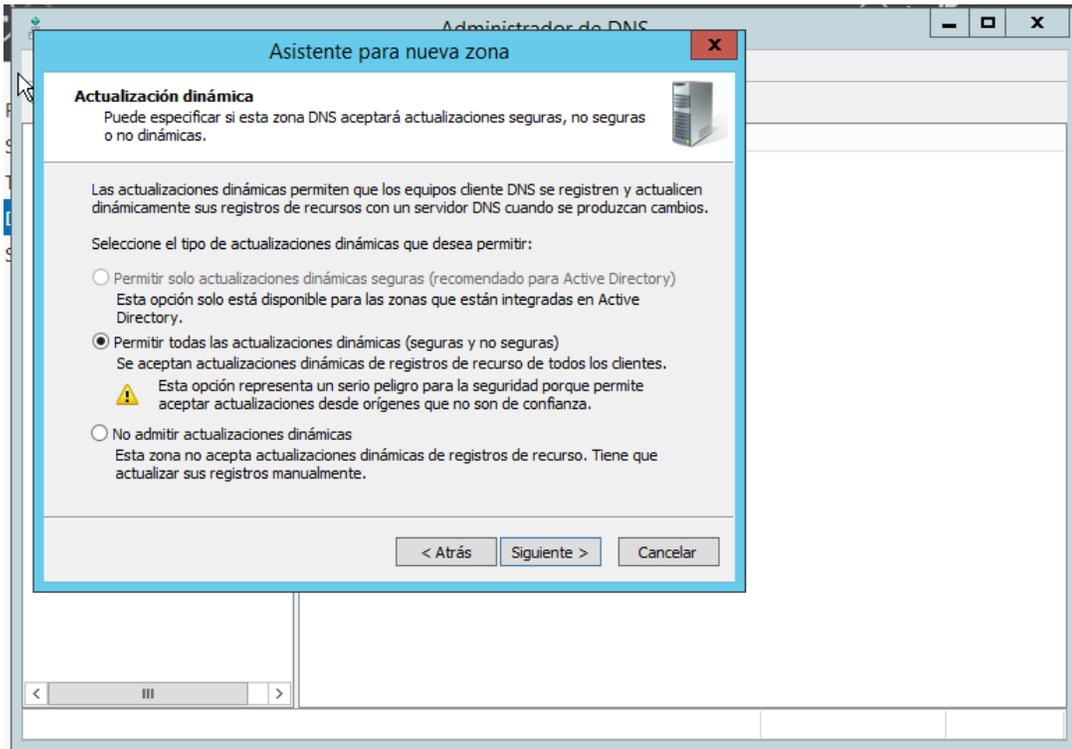


Figura 121. Escogemos la opción de no reenviar consultas porque solo es un servidor que está configurado y no es necesario.

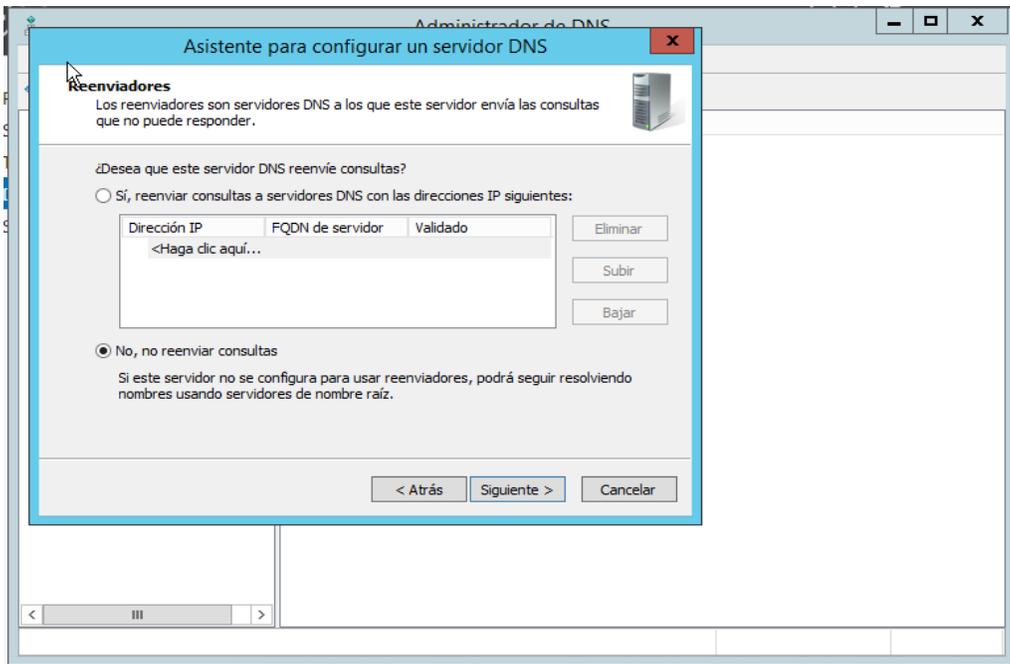


Figura 122. Dejamos que busque.

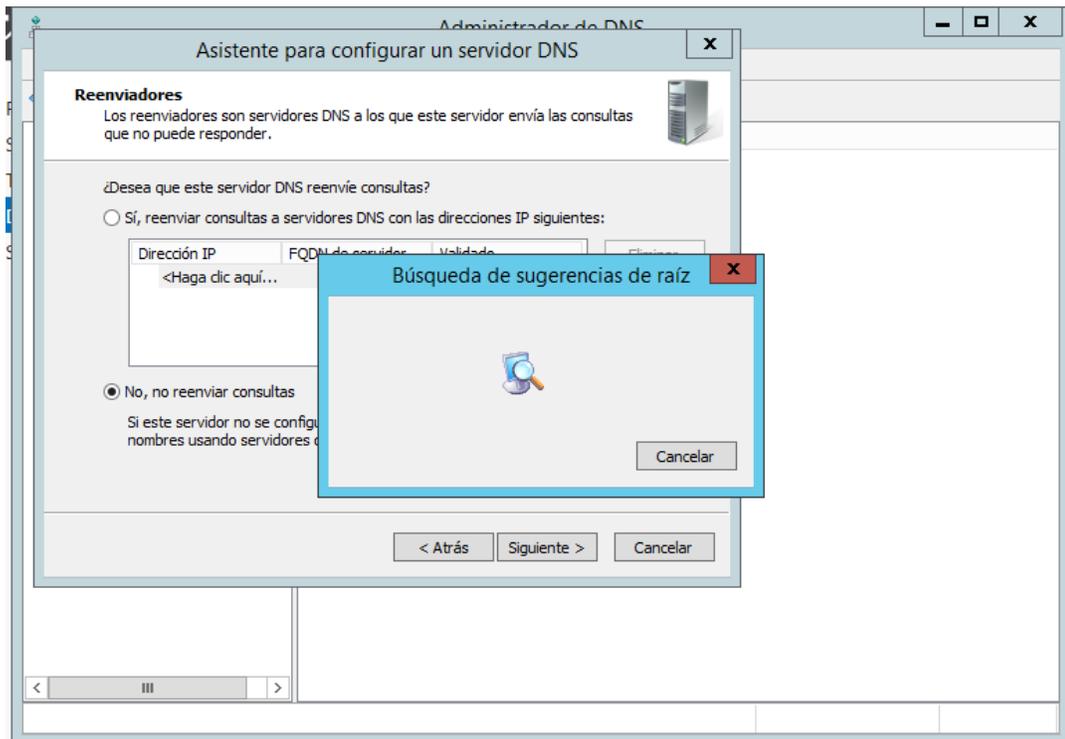


Figura 123. Le damos siguiente para finalizar para terminar de configurar el DNS.

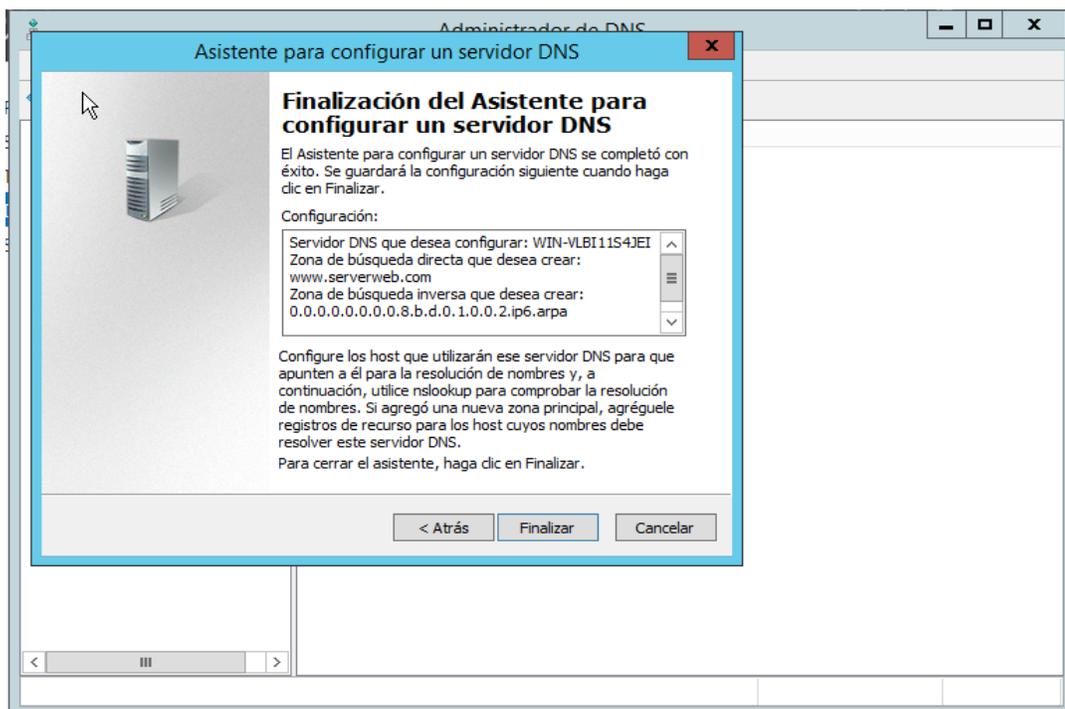


Figura 124. Vamos a configurar la dirección ipv6 en nuestro server 2012.

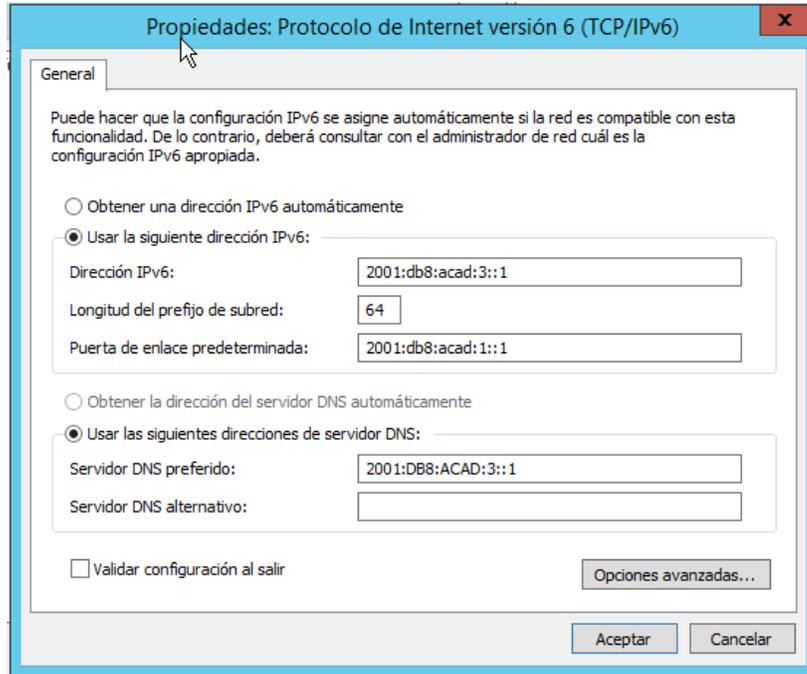
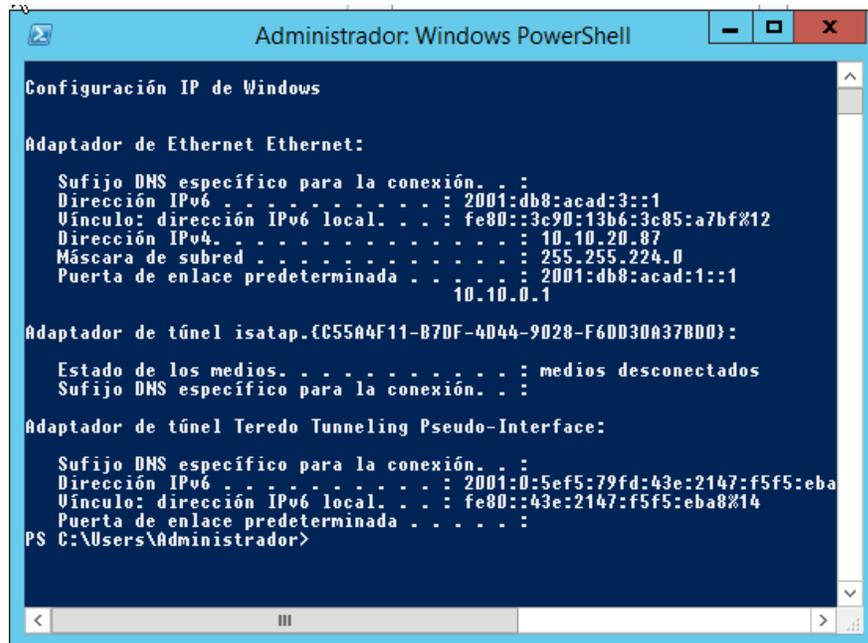


Figura 125. Vamos a terminal verificando nuestra dirección ipv6.



5. DESARROLLO DEL PROYECTO

Recopilación de información sobre los servidores DNS, Server Web, DHCP, las máquinas virtuales.

5.1 ANÁLISIS DEL DESARROLLO DEL PROYECTO

- 1) Configuramos los router C7200 configurando el servidor DHCP.
- 2) Configuramos el switch C3725 con la IOS.
- 3) Instalamos las máquinas virtuales: WINDOWS 7, UBUNTU, CENTOS 7, WINDOWS SERVER 2012.
- 4) Configuramos la máquina virtual CENTOS 7 para el SERVER WEB.
- 5) Configuramos la máquina virtual WINDOWS SERVER 2012 para el SERVIDOR DNS.
- 6) Se comprobó que las maquinas virtual tomaran las dirección ipv6 con el DHCP en el rango correspondiente.
- 7) Verificación de los servicios DHCP, DNS y SERVER WEB.

5.2 CRONOGRAMA

Figura 126. Cronograma

| ACTIVIDADES | MESES | AGOSTO | | | | SEPTIEMBRE | | | | OCTUBRE | | | | NOVIEMBRE | | | | DICIEMBRE | | | | |
|--|-------|--------|---|---|---|------------|---|---|---|---------|---|---|---|-----------|---|---|---|-----------|---|---|---|--|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| SELECCION DEL TEMA | | X | | | | | | | | | | | | | | | | | | | | |
| ELABORACION Y APROBACION MONOGRAFIA | | | X | | | | | | | | | | | | | | | | | | | |
| PLANTEAMIENTO PROBLEMA | | | | X | X | | | | | | | | | | | | | | | | | |
| ELABORACION DE OBJETIVOS | | | | X | X | | | | | | | | | | | | | | | | | |
| RECOLECCION DE INFORMACION | | | | | | X | X | X | | | | | | | | | | | | | | |
| BIBLIOGRAFIA | | | | | | | | X | X | X | | | | | | | | | | | | |
| ELABORACION MARCO TEORICO | | | | | | | | | | X | X | X | X | | | | | | | | | |
| PRACTICAS Y SIMULACIONES | | | | | | | | | | | X | X | X | X | X | | | | | | | |
| REVISION Y CORRECCIONES | | | | | | | | | | | | | | | X | X | X | X | | | | |
| ELABORACION Y PRESENTACION DE MONOGRAFIA | | | | | | | | | | | | | | | | | | | X | X | X | |

6. CONCLUSIONES

- Hoy en día la mayoría de los sistemas operan bajo IPv4 por la necesidad de evolución de las redes a IPV6, usando la técnica de tunelización.
- El recorrido para implementar los cambios necesarios de IPv4 a IPv6 no es una cuestión de transición ni de migración, sino de evolución, de integración, todos estos procesos deben ser ejecutados por medianos y grandes proveedores de internet.
- El futuro es IPV6 y la necesidad de disponer de direcciones IP por persona se incrementara en muy poco tiempo por la evolución de la tecnología.
- Este nuevo protocolo IPV6 incorpora funcionalidades que mejoran su comportamiento en aspectos de seguridad entre ellas no utilización de direccionamiento de broadcast y la fragmentación de paquetes permitidas en los hosts terminales.
- Al incorporar IPV6 una gran cantidad de direcciones, no será necesario utilizar NAT y sus nuevas capacidades de Plug and Play, seguridad y QoS implicaran mejores conexiones de voz.
- Con simulaciones sobre cómo implementar estos nuevos cambios aportamos para que se pueda ir masificando estos cambios y mucho más personas del área de Networking pueden avanzar sobre los nuevos cambios que depara el acelerado mundo de internet.
- El servidor DHCP SERVER es más sencillo configurarlo que los otros servidores, se instaló en un Router (C7200) por lo cual es más robusto que

instalarlo en una máquina virtual.

- El servidor WEB SERVER se configuro en el sistema operativo en Linux CENTOS 7 por razón de licencias, configuración más sencilla y robustez, este servicio va integrado con el Servidor DNS.
- El servidor DNS se configuro en un Sistema Operativo WINDOWS SERVER 2012 de prueba por asunto de la licencia, es un poco estable y operación restringida por ser sistemas operativo Windows no licenciado.
- GNS3 presenta un entorno muy didáctico y emula la realidad para diferentes escenarios en redes LAN, tanto en IPV4 como IPV6

BIBLIOGRAFÍA

Academy, C. N. (s.f.). Capítulo 10: DHCP. Consultado el 12 de octubre de 2015. Disponible en: <http://ecovi.uagro.mx/ccna2/course/module10/index.html# 10.1.3.3>

Comunicaciones, M. d. (s.f.). ¿Qué es la transición a IPv6? Consultado el 15 de octubre de 2015. Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-5893.html>

Kim Davies, G. d. (s.f.). Una introducción a IANA. Consultado el 17 de octubre de 2015. Disponible en: <https://www.iana.org/about/presentations/davies-atlarge-iana101-paper-080929-es.pdf>:<http://www.icann.org/en/general/iana-contract-14aug06.pdf>

Lacnic. (s.f.). Mecanismos de transición. Consultado el 17 de octubre de 2015. Disponible en: <http://portalipv6.lacnic.net/mecanismos-de-transicion/>

LacnicLabs. (s.f.). IPv6 HandsOn - Tuneles y servidores web en IPv6. Consultado el 20 de octubre de 2015. Disponible en: <http://labs.lacnic.net/site/ipv6-handson-tunnel-web>

Marcelo., B. (s.f.). Historia del protocolo TCP/IP y IPv4 - IPv6. Consultado el 20 de octubre de 2015. Disponible en: <http://redesiuv.blogspot.com.co/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html>

S.C., N. I. (s.f.). Fundamentos de IPv6. Consultado el 21 de octubre de 2015. Disponible en: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

Team, M. P. (s.f.). IPv6 para el administrador de Windows: Como funciona la resolución de nombres en un escenario dual IPv4/IPv6. Consultado el 31 de octubre de 2015. Disponible en: <http://blogs.technet.com/b/ask-pfe-latamplat/archive/2013/11/15/ipv6-para-el-administrador-de-windows-como-funciona-la-resoluci-243-n-de-nombres-en-un-escenario-dual-ipv4-ipv6.aspx>

IPv6. Consultado el 31 de octubre de 2015. Disponible en: Wikipedia®. (s.f.). IPv6. <https://es.wikipedia.org/wiki/IPv6>

Router. Consultado el 31 de octubre de 2015. Disponible en: Wikipedia®. (s.f.). Router. <https://es.wikipedia.org/wiki/Router>