Universitat Oberta de Catalunya. I.T.I.S

IpViSix. Distribución LiveCD GNU/Linux con herramientas IpV6

Memoria del Trabajo de Fin de Carrera

Alumno: Guillermo Vitas Gil
Consultor UOC: Joaquín López Sánchez-Montañés

Junio 2012
Versión 1.0

Resumen

Internet, tal y como la conocemos actualmente, se enfrenta al reto que representa el agotamiento de las direcciones Ip públicas asignables por las organizaciones gestoras del direccionamiento en Internet. Es un hecho cierto que, para algunas zonas geográficas estas direcciones se han agotado [1].La solución al problema se basa en la utilización de un nuevo esquema de direccionamiento Ip que evite este agotamiento. Este nuevo esquema se basa en la evolución del protocolo TCP/IP de la versión actualmente en uso (Ip versión 4) a una nueva versión que se denomina Ip Versión 6 (Ipv6). Muchos proveedores de Internet y grandes organizaciones ya están trabajando en la adopción de este protocolo en sus redes y sistemas, pero el cambio es significativo y antes de la puesta en producción de redes y servicios basados en esta nueva versión del protocolo Ip deben probarse tanto las aplicaciones como las redes.
IpViSix es una distribución GNU/Linux que incorpora una serie de herramientas basadas en Software Libre que permiten tanto probar aplicaciones y redes como implementar servicios de red básicos en Ip versión 6.

Abstract

Internet as we know it today faces the challenge of the exhaustion of public IP addresses assignable by the organizations managing the Internet addressing. It is a fact that for some geographical areas these addresses have been exhausted [1]. The solution is based on the use of a new IP addressing scheme that avoids this exhaustion. This new scheme is based on the evolution of TCP / IP version currently in use (IP version 4) to a new version called IP Version 6 (IPv6). Many ISP and large organizations are already working on the adoption of this protocol in their networks and computers, but the change is significant and prior to the start up of networks and services based on this new version of IP protocol must be tested both applications such networks. IpViSix is a GNU / Linux distribution that incorporates a number of free software-based tools that allow both application and network to be tested, and can be used to implement basic network services in IP version 6.

Contenido

1. Introducción

A grandes rasgos podríamos definir una distribución Linux como un sistema operativo de la familia de los sistemas tipo Unix construido sobre el kernel de Linux alrededor del cual se han instalado ciertas aplicaciones con el fin de adaptar ese conjunto para una utilidad concreta, o incluso, una forma de uso concreta. Esta distribución puede presentarse en varios formatos distintos, como una imagen ISO instalable o un LiveCD como el caso que nos ocupa.
En este proyecto vamos a crear una distribución GNU/Linux con el propósito de obtener una herramienta que ayude a la realización de pruebas, diagnósticos, tareas de administración sobre una red TCP/IP basada en la versión 6 del protocolo Ip. Otro aspecto importante que se pretende cumplir con esta distribución es facilitar el aprendizaje del protocolo Ipv6, proporcionando herramientas que permitan implementar los servicios básicos de red en un entorno Ipv6 y quizá sea éste último el objetivo fundamental de la distribución.
A esta distribución la denominaremos IpViSix.

1.1 ¿Qué incluye la distribución IpViSix?

La distribución LiveCD IpViSix contendrá un conjunto de herramientas útiles para verificar el funcionamiento de aplicaciones y redes bajo el protocolo Ipv6 y también permitir la gestión de los servicios básicos de red de una red Ipv6, así como el diagnóstico de las mismas. Esta distribución también servirá como herramienta que facilite la compresión y aprendizaje de esta nueva versión de la pila TCP/IP.
En esta primera versión de la distribución los componentes principales que se incluirán son:

- Un gestor de direcciones IP (Internet Protocol Address Manager, IPAM)
- Una herramienta de captura y análisis de tráfico de red (sniffer).
- Una herramienta de escaneo de red
- Una aplicación que permita verificar el tipo de pila que usa un cliente concreto.
- Servidores de infraestructura de red compatibles con IpV6 (DNS) de tal manera que puedan permitir la implantación de los servicios básicos de una red ip v6.

Todo esto se implementa sobre una distribución GNU/Linux con doble pila configurada, de tal forma que la distribución pueda utilizarse tanto en entornos puros Ipv6 como en entornos mixtos Ipv6-Ipv4.

1.2 ¿Qué es un LiveCD?

Un LiveCD es una forma de distribución de sistemas operativos sobre un soporte CDROM desde dónde se pude iniciar por completo el sistema operativo incluido en el LiveCD, sin que se realice ningún cambio en el disco duro del ordenador dónde se ejecuta.
Esta forma de distribución presenta la ventaja de que, sin realizar ningún tipo de instalación en un ordenador, podemos trabajar con un sistema operativo completo y con todas las herramientas y utilidades que incluya. Esta característica hace de estas distribuciones una magnífica herramienta para tareas como el diagnóstico hardware, análisis de seguridad de redes o equipamiento o, simplemente para el aprendizaje o prueba de un sistema operativo.
Por el contrario los LiveCD tienen dos desventajas:

- La persistencia de los datos
- Limitación de tamaño de la distribución.

Vamos a intentar explicar estas dos desventajas y cómo podemos solventarlas.

1.2.1 La persistencia de los datos.

Un LiveCD se distribuye en un medio de solo lectura y al no hacer cambios en los discos duros de los equipos en los que se usan, no tienen por lo general la capacidad de proveer de persistencia de datos. Esta limitación se ha superado con la aparición de un soporte escribible y económico como las memorias USB. Aplicando este tipo de dispositivos podemos crear una distribución LiveUSB que tiene las mismas característica que una distribución LiveCD pero que, al estar alojada en un medio sobre el que se puede escribir, nos permite obtener persistencia de datos. Actualmente las memorias USB que se pueden usar como medio de arranque de un sistema operativo alcanzan una capacidad de almacenamiento de 8GB, lo que permite multiplicar casi por 10 el tamaño de la distribución que podría alojar frente al tamaño en un LiveCD.
Un LiveUSB no tiene la misma estructura interna que un LiveCD y se usan distintas herramientas para crearlos.
Más adelante veremos la importancia de la persistencia de datos (y configuraciones) y la implicación que eso tiene para nuestra distribución.

1.2.2 Limitación del tamaño de la distribución.

El soporte CDROM tiene una limitación en cuanto al tamaño de los datos que se pueden grabar en el soporte (700MB), lo que limita el tamaño de la distribución, es decir la cantidad de componentes y/o aplicaciones que puede incluir. Este problema se agrava por la evolución natural de los sistemas operativos, que cada día son más eficientes, robustos y fáciles de manejar, pero por el contrario coda vez incluyen más módulos, integran más aplicaciones y drivers. Esto provoca que, por lo general, éstos sean de mayor tamaño.
Este problema se puede paliar utilizando el DVD como soporte para la distribución en vez del CDROM tradicional. Así la distribución puede alcanzar hasta los 4BG de tamaño. Este cambio sólo implica cambiar el soporte sobre el que se graba la distribución y no la estructura de la misma dentro del propio soporte, de tal manera que crear un LiveCD es exactamente igual a crear un LiveDVD, salvo por el soporte empleado para la grabación, que en el caso del DVD nos permite almacenar una distribución de mayor tamaño. Por lo tanto, para nuestros propósitos, podríamos afirmar que un LiveCD y un LiveDVD son la prácticamente lo mismo. En este documento nos referiremos a los dos soportes como LiveCD.

2. Selección del sistema operativo para la distribución

IpViSix será una distribución GNU/Linux, por lo tanto la respuesta a la pregunta: ¿sobre qué sistema operativo se construirá? es evidente, al menos en un primer momento, y ésta es: GNU/Linux.
Pero esta respuesta plantea otra pregunta también inmediata y quizá no tan fácil de responder: ¿qué GNU/Linux?

Se podría partir del kernel de Linux e ir agregando o desarrollando alrededor del mismo todo un sistema operativo completo, con el soporte de red, gestión de discos, gestión de usuarios y sesiones, escritorio, gestión de paquetes, y todo lo necesario para poder ejecutar de un modo conveniente las aplicaciones que se seleccionen o desarrollen para IpViSix, pero esta es una tarea que queda completamente fuera del alcance (y de los recursos y conocimientos) de los que se podrían disponer para este Trabajo de Fin de Carrera, por lo que, al menos en esta versión del producto, nos limitaremos a seleccionar la mejor distribución GNU/Linux que seamos capaces para que IpViSix funcione adecuadamente y responda a los requisitos para los que se diseña.
La selección de la distribución GNU/Linux sobre la que se ejecutarán las aplicaciones que se incluyen en IpViSix es uno de los puntos del trabajo que se antojan más complicados, ya que se trata de elegir entre más de 300 distribuciones de GNU/Linux que actualmente podremos encontrar [2].
Para intentar responder a esta pregunta haremos un par de reflexiones previas para las que nos plantearemos dos preguntas:

- ¿Qué es una distribución GNU/Linux?
- ¿Cuáles son los requisitos con los que debe cumplir IpViSix?, o mejor ¿cuál es el uso y a quién está dirigida la distribución IpViSix?

En los siguientes apartados intentaremos dar respuesta a estas dos preguntas.

2.1 ¿Qué es una distribución GNU/Linux?

Como se indicaba en la introducción, una distribución Linux es un sistema operativo de la familia de los sistemas tipo Unix construido sobre el kernel de Linux. Una distribución, pues, consiste en el kernel de Linux y un conjunto más o menos amplio de aplicaciones que se distribuyen de forma conjunta con el fin de adaptarlo a un uso o gustos específicos. Se estima que puede haber unas 300 distribuciones activas, es decir, que se mantienen y mejoran de forma periódica o continuada [3]. La mayor parte de esas distribuciones provienen de las cuatro más importantes:

- Debian
- SlackWare
- Red Hat
- Gentoo

Las distribuciones de Linux han ido tomando a lo largo del tiempo múltiples formas con el fin de adaptarse a los gustos de los usuarios hacia los que va dirigidos o a una utilidad concreta. No obstante hay dos aspectos que marcan y distinguen las distribuciones:

- La organización que las promueve
- El sistema de gestión de paquetes que implementan

Respecto a las organizaciones que las promueven podemos distinguir entre:

- Distribuciones promovidas por organizaciones con intereses comerciales como:
    - Fedora, de Red Hat
    - OpenSuse, de Novell
    - Ubuntu, de Canonical Ltd
    - Mandriva Linux, de Mandriva
- Distribuciones promovidas por la comunidad como Debian y Gentoo.

Respecto a la gestión de paquetes la diferencia más importante está en la forma y herramientas de gestión de los propios paquetes y en la disponibilidad de los mismos. Estos dos aspectos definen la facilidad o complejidad para instalar, actualizar o desinstalar aplicaciones o componentes del propio sistema operativo (incluido el propio Kernel) y la cantidad de aplicaciones disponibles para cada distribución, o mejor dicho, familia de distribuciones.
De esta forma la elección de la distribución de GNU/Linux sobre la que se construirá IpViSix vendrá determinada por la usabilidad de la distribución para el objetivo concreto que se pretende y por la cantidad de aplicaciones que para una distribución concreta existan. Pero, ¿cuáles son las características que debe tener la distribución de GNU/Linux que sirva de plataforma a IpViSix?

2.2 Características de la plataforma para IpViSix

De alguna manera la pregunta que formulábamos al finalizar el apartado anterior quedaba respondida en el primer capítulo de esta memoria, en la propia introducción.
Por el uso que daremos a la distribución podemos deducir que el sistema operativo GNU/Linux sobre el que construyamos la distribución ha de reunir las siguientes características:

1. Ser un sistema operativo orientado a servidor de propósito general, que sea capaz de soportar la ejecución de aplicaciones de servidor como un DNS Server, un servidor Web, o quizá un gestor de bases de datos.

2. Ocupar el menor espacio posible, ya que la distribución completa debería caber en un soporte CDROM, es decir alrededor de 700 MB.

3. Debe poder funcionar sobre hardware diverso. La distribución se debe poder instalar y ejecutar tanto sobre hardware antiguo como moderno. Para la realización de pruebas o estudio de aplicaciones se suele usar hardware obsoleto o bien sistemas de virtualización (hipervisores) con, en muchas ocasiones, pocos recursos. No se debe olvidar que IpViSix también está orientada al aprendizaje de Ip versión 6 y por lo tanto a estudiantes que, en muchas ocasiones, no tienen recursos económicos para poder adquirir un hardware moderno para sus estudios o pruebas.

4. Ser lo más sencilla de usar posible, para lo que debería disponer de una buena ayuda y documentación, así como un interfaz gráfico amigable. El usuario de la distribución no tiene porqué ser un experto en GNU/Linux para poder manejarla, utilizar las aplicaciones, agregar o quitar componentes, personalizar o actualizar la distribución, realizar las configuraciones que estime convenientes.

Sobre el segundo punto de este apartado (el referente al tamaño de la distribución) hay que hacer notar que la distribución no sólo consistirá en un sistema operativo, sino que incluirá ciertas aplicaciones que pudieran consumir tanto espacio en disco como el propio sistema operativo y que por lo tanto puede que sea difícil, por no

decir imposible, que el producto final quepa en un soporte CDROM. Si este es el caso deberemos utilizar el DVD como medio para la distribución de IpViSix. Como se ha citado anteriormente los métodos de construcción y la estructura de la distribución es la misma en ambos formatos (LiveCD y LiveDVD), la única diferencia entre ambos es el propio medio o soporte.

Si lo que valoramos es el ámbito de aplicación, o lo que es lo mismo hacia qué tipo de usuario está dirigida la distribución, los requisitos no están tan claros. El motivo es que está dirigida a un universo de usuarios muy amplio, con un interés común que se focaliza en el ámbito de las redes TCP/IP, pero de conocimientos muy dispares ya que podría ser usada tanto por personas con mucha experiencia y conocimientos, tanto de redes como de Linux, pero también por estudiantes con poco conocimiento de ambos ámbitos.

Debido a esta disparidad de posibles usuarios la decisión se centra en el uso de una distribución que ofrezca unos elevados índices de usabilidad, con el fin de que los usuarios con menos conocimientos de la plataforma puedan utilizarla sin una curva de aprendizaje elevada, es decir que puedan enfocar su esfuerzo en aprender a manejar las herramientas que incluye y el protocolo de red que subyace, sin la necesidad de dedicar muchos recursos a explorar y manejar la plataforma que da soporte a las propias herramientas.

Además de lo anteriormente citado cabe indicar que uno de los posibles ámbitos de uso de la distribución sea el entorno académico de la Universitat Oberta de Catalunya, que es el ámbito académico dónde se crea la propia distribución. En este entorno la distribución más utilizada, y podríamos decir que de algún modo la de uso oficial, es Ubuntu. Esto implica que si IpViSix se basase en esta distribución GNU/Linux, la curva de aprendizaje aún sería más reducida, debido al más que probable uso previo del sistema operativo por parte de los usuarios de IpViSix.

Por todo ello la distribución GNU/Linux que se selecciona para construir la distribución es Ubuntu Server 11.10 dentro de la familia Ubuntu seleccionaremos la distribución Lubuntu [4].

2.3 Lubuntu

Lubuntu es una distribución GNU/Linux que ofrece un escritorio basado en LXDE

El escritorio es un conjunto formado por:

- Un interfaz gráfico, en este caso LXDE
- Un conjunto de aplicaciones seleccionadas por los creadores de la distribución según sus preferencias
- Un conjunto de personalizaciones, como temas de escritorio, etc.

Para nuestra distribución nos interesa desplegar un reducido número de aplicaciones por dos motivos:

1. Reducir al máximo su tamaño
2. Optimizar la distribución

No debemos olvidar que IpViSix es una distribución con vocación de plataforma servidora, el interfaz gráfico se instala por facilitar el uso de dos aplicaciones concretas que incluirá, como son Wireshark y ZenMap.

2.3.1 Plataforma IpViSix

Nuestra plataforma por lo tanto tendrá los siguientes componentes:

- Una instalación mínima de Ubuntu Server 11.10
- Una instalación mínima de Lubuntu desktop
- El navegador de Internet Mozilla Firefox
- El complemento Lxappearance (gestor de configuraciones de escritorio para LXDE)
- El descompresor de ficheros ZIP
- El gestor de conexiones de red Network-Manager

Estos serán los elementos básicos de la distribución sobre la que se instalarán las aplicaciones que se seleccionen y sus requisitos.

Una vez seleccionada la distribución de GNU/Linux y los componentes que conforman la plataforma sobre la que vamos a construir nuestro LiveCD, deberemos elegir el método y herramientas para la creación del mismo que más se ajusten a la propia distribución y para las que la propia distribución ofrezca las mejores herramientas o, incluso, aquellos métodos o herramientas desarrollados por terceros y soportados por la distribución elegida.

3. Herramientas para la creación de un LiveCD basado en Ubuntu

La creación de un LiveCD se basa en la obtención de una imagen ISO que contiene el sistema operativo y las aplicaciones instaladas sobre ella. Esta imagen ISO tiene la capacidad de se puede descomprimir e iniciar el sistema operativo y las aplicaciones contenidas en la misma.
Para crear esa imagen ISO hay dos estrategias:

- Creación de la distribución desde cero.
- Obtención de una imagen despersonalizada de un sistema existente.

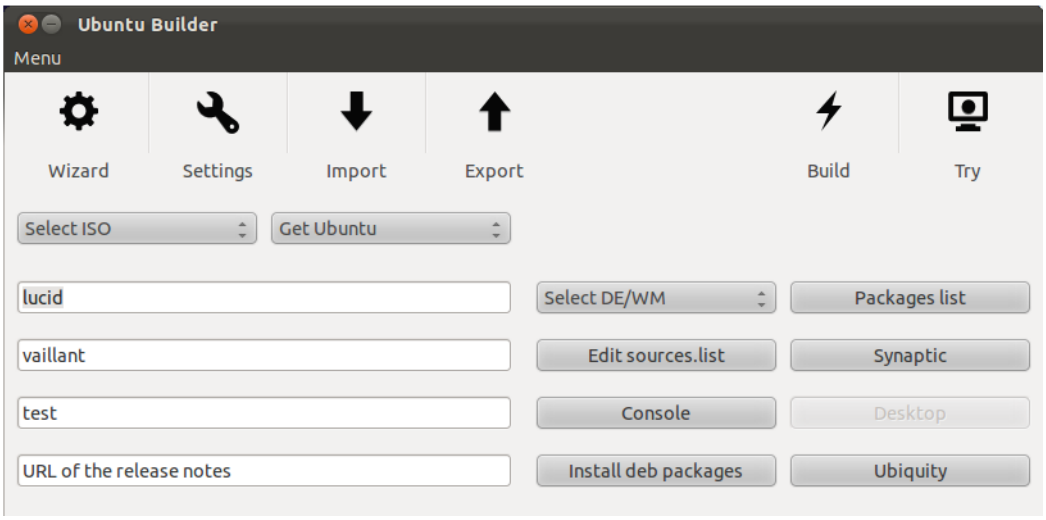
Para crear el fichero ISO usando la primera estrategia se utiliza una utilidad que se denomina Debootstrap [5] y se sigue un procedimiento de múltiples pasos que generan una instalación de Linux en un directorio del equipo donde se está creando el LiveCD.
Existe una herramienta con un interfaz gráfico que facilita todo ese proceso que se denomina Ubuntu Builder [6] que evaluaremos en su última versión, la 2.0.1 a fecha de elaboración de este documento.
Para la obtención de una imagen sin personalidad de un sistema ya instalado podemos usar utilidades como bootcd, dfsbuild o Remastersys [7]. Estas tres últimas herramientas tienen el mismo objetivo, pero Remastersys parece tener una mejor documentación y ser más fácil de utilizar que las dos anteriores, por lo que será la herramienta que evaluaremos para la obtención de un fichero imagen de un sistema ya instalado.

3.1 Debootstrap

La utilidad Debootstrap, creada por Anthony Towns, instala un sistema Debian muy básico sobre un subdirectorio en el disco duro de nuestra instalación GNU/Linux. Una vez instalado este sistema mínimo instalaremos sobre él los módulos y aplicaciones que nos interesen, para lo cual deberemos tener acceso a los repositorios de la distribución GNU/Linux que deseemos utilizar. Una vez creada la distribución debemos obtener una imagen de la misma para insertarla en el LiveCD.
Esta es la forma de obtener una distribución lo más reducida y controlada posible, ya que incorpora sólo los paquetes que nos interesen, pero a la vez es un proceso con cierta complejidad y que exige un conocimiento alto de los paquetes que se necesitan instalar para una determinada funcionalidad y de sus dependencias.
Es oportuno remarcar que en nuestro caso, en la distribución IpViSix, el número de paquetes a instalar para dar soporte a las aplicaciones puede ser tan elevado que el resultado final no se diferencie en exceso de una instalación mínima estándar de Lubuntu, por lo que se hace necesario valorar si el esfuerzo necesario para la creación del sistema a partir de Debootstrap aporta algún beneficio.

3.2 Ubuntu Builder

Ubuntu Builder es una herramienta creada por Francesco Muriana y publicada bajo licencia GNU GPL versión 2 que permite la creación de un LiveCD de una forma sencilla e intuitiva. La herramienta incluye un interfaz gráfico y un asistente para la creación de la distribución. Permite personalizar todos los componentes de la distribución, desde el interfaz gráfico hasta los paquetes instalados en la propia distribución, y no solo eso, sino que permite probar el funcionamiento de la distribución antes de grabarla un soporte a través de una integración con un motor de virtualización como Qemu o KVM.



Ubuntu Builder es una herramienta potente y fácil de usar, pero con una limitación importante: solo es capaz de crear distribuciones que se basen en la versión desktop de Ubuntu. En la versión probada no permite la creación de distribuciones basadas en Ubuntu server.
Esto convierte a esta herramienta en inutilizable para nuestros propósitos, ya que tratamos de crear la distribución partiendo de Ubuntu server.
Podríamos basar IpViSix en una distribución de Ubuntu desktop y posteriormente sustituir el propio kernel de Ubuntu para instalar el kernel optimizado para servidor, instalando el paquete linux-image-server pero podríamos perder estabilidad en la distribución y es un riesgo no asumible. Además una de las grandes ventajas usar como base una distribución server es que éstas llevan integradas muchos menos paquetes de software que las distribuciones desktop, lo que facilita el correcto funcionamiento y mejora la seguridad ya que no hay elementos innecesarios.

No obstante hay que hacer notar que está en el roadmap de desarrollo de la herramienta el soporte de Ubuntu server, con lo que es una herramienta que se deberá tener en cuenta para futuras versiones de IpViSix.

3.3 Remastersys

Remastersys es una herramienta creada por Tony Brijeski [5] y publicada bajo licencia GNU GPL versión 2, que tiene dos usos fundamentales sobre sistemas basados en Debian, Ubuntu o distribuciones derivadas:

- La primera utilidad es la realización de una copia de seguridad de un sistema operativo completo, incluyendo los datos y las aplicaciones, hacia un soporte LiveCD o LiveDVD que se puede usar para volver a instalar el sistema tal y como estaba en el momento en el que se realizó la copia de seguridad.

- La segunda utilidad es realizar una copia distribuible de un sistema (Debian, Ubuntu o derivados) sin los datos personales, es decir permite generar un LiveCD a partir de una instalación concreta, incluyendo las aplicaciones y paquetes incluidos en la misma.

Remastersys se puede ejecutar tanto en modo comando como a través de un interfaz gráfico (GUI) que incorpora, y el resultado de la ejecución es un fichero ISO con la imagen del sistema sobre el que se ha ejecutado.
Remastersys se apoya en utilidades del propio sistema operativo, como Casper, que es la herramienta que permite arrancar un LiveCD, o genisoimage que permite crear la imagen ISO y otras herramientas como Ubiquity que aportan la

funcionalidad de realizar una instalación de la distribución sobre un disco duro, ya sea de una máquina física o virtual.

Para que Ubiquity opere correctamente la plataforma debe cumplir con dos requisitos:

- Tener instalado y configurado por defecto un tema de escritorio basado en GTK3
- Tener conexión a Internet en el momento de la instalación (es decir cuando se ejecuta Ubiquity)

Estas dos características nos van a obligar a, por un lado configurar un tema de escritorio concreto en la distribución, y por otro a tener en cuenta que, si deseamos instalar IpViSix en disco, en vez de usarlo únicamente como LiveCD, como paso previo deberemos cambiar la configuración de red de la distribución y verificar que tiene conectividad a Internet.

4. Selección de aplicaciones de la distribución

Como se indicaba en la introducción en esta distribución se incluyen una serie de aplicaciones como:

- Un gestor de direcciones IP (Internet Protocol Address Manager, IPAM)
- Una herramienta de captura y análisis de tráfico de red (sniffer).
- Una herramienta de escaneo de red
- Una aplicación web sencilla que permita verificar el tipo de pila que usa un cliente concreto.
- Servidores de infraestructura de red compatibles con IpV6 (DNS) de tal manera que puedan permitir la implantación de una red ip v6.

Podrían incluirse muchas más herramientas y utilidades que pudiesen ofrecer alguna ventaja para el propósito de esta distribución pero, como también se indica en la introducción en esta fase incluiremos algunas herramientas básicas y llegado el caso, en otras versiones de la distribución se podrían incluir más herramientas que se consideren útiles.
Las herramientas que se incluyan en la distribución deben cumplir dos requisitos básicos:

- Publicarse bajo licencia GNU GPL o similares
- Soportar el uso de IpV6, o mejor dicho, ser capaces de funcionar correctamente en un entorno IpV6 puro.

Con estos dos requisitos podremos encontrar múltiples herramientas en las categorías que se desean incluir en la distribución. En los siguientes apartados se evaluarán distintas herramientas para obtener la funcionalidad deseada.

4.1 Gestor de Direccionamientos IP (IPAM)

Uno de los aspectos principales de Ipv6 es que aporta un espacio de direcciones realmente grande. El tamaño de este espacio de direcciones implicará que los segmentos de direccionamiento que se asignen a las organizaciones usuarias sean grandes. Es previsible que, al disponer de direccionamientos de red grandes, las organizaciones tiendan a segmentar estos direccionamientos con el fin de hacerlos manejables y poder organizar sus redes. Estos dos aspectos, unidos a la longitud de las propias direcciones Ipv6 (128 bits) harán que la gestión de los direccionamientos y las propias direcciones se vuelva una tarea compleja. De ahí la necesidad de herramientas que nos ayuden a gestionar el espacio de direcciones disponible de forma eficiente, y eso es lo que tratan de hacer los Gestores de Direcciones IP (IPAM).

Además a las herramientas IPAM actuales se les están añadiendo cada vez más funcionalidades que las hacen más interesantes, como el descubrimiento automático de redes y hosts, la verificación ICMP de los hosts, la generación de planes de direccionamiento, la generación de informes, etc...

Actualmente hay varios proyectos Open Source que focalizan sus esfuerzos hacia la obtención de herramientas IPAM, como son el caso de: IPPlan [8], OpenNetAdmin [9] y GestióIP [10] entre otras.

Las tres herramientas citadas cumplen con el primero de los requisitos indicados como criterio de selección: se publican bajo un licenciamiento GNU GPL o similar.

Hay varias herramientas con esta funcionalidad cuyo uso está muy extendido, como por ejemplo InfoBlocks [11] que ofrecen versiones gratuitas de sus productos, pero no bajo el licenciamiento GNU GPL, por lo que no entraremos a analizarlas.

De estas herramientas: IPPlan, OpenNetAdmin y GestióIP, sólo una cumple (o al menos así lo afirma su desarrollador) con el segundo requisito: tener soporte completo IpV6.
IPPlan y OpenNetAdmin, a fecha de elaboración de este trabajo, incluyen este soporte en fase beta, y tan sólo GestióIp lo incluye como funcionalidad completa desde la última versión del producto, liberada en noviembre de 2011 así que el producto elegido para incluir en IpViSix será GestióIP en su versión 3.0.10

4.1.1 GestiólP

GestióIP, desarrollada por Marc Ueber y liberada bajo licenciamiento GNU GENERAL PUBLIC LICENSE versión 3 (GPLv3), es un gestor IPAM que según su creador incluye las siguientes características [SIC]:
"

- *Facilidad de uso y una presentación de los datos bien estructurada*
- *Búsqueda rápida y potente para redes y para host accesible desde cada página Web que permite expresiones equivalentes a los de las máquinas de búsqueda de Internet como "match exacto" o -string_para_ignorar*
- *Gestión de clientes independientes con redes que se solapan*
- *Sistema automatizado de gestión de VLANs integrado*
- *Sistema para gestionar leased or dial-up lines*
- *sistema para gestionar "autonomous systems"*
- *Exploración de redes y de VLANs vía SNMP*
- *Exploración de hosts vía SNMP y DNS*
- *Muestra el estatus de los hosts*
- *Chequeo si una dirección IP responde a "ping" y si tiene entradas DNS PTR y A configuradas*
- *Interfaces para unir/dividir/aumentar/disminuir redes (con la posibilidad de mantener las entradas hosts)*
- *Muestra rangos libres*
- *Calculadora de subnet (calculadora de subnet online)*
- *Reserva de rangos de direcciones de IP para un uso especial*
- *Formulario Web que permite migrar con facilitad desde una gestión con hojas de cálculo (.xls - MS Excel) a GestióIP*
- *Formulario Web que permite importar redes vía consulta SNMP*
- *Formulario Web que permite exportar redes y hosts a ficheros CSV*
- *Actualización automática vía SNMP*
- *Actualización automática contra DNS*
- *Actualización automática contra OCS Inventory NG*
- *Auditable*
- *Estadísticas*
- *Instalación fácil basada en script*
- *Bien documentado*
- *Plurilingüe (Alemán, Brasileño-Portugés, Catalán, Español, Francés, Holandés, Inglés, Italiano, Ruso)*
- *Soporte completa para IPv4 y IPv6* "

En líneas generales tiene todas las funcionalidades que cabría esperar en una aplicación de este tipo, no obstante habría que hacer notar dos aspectos respecto a las funcionalidades que se indican en la página web principal del proyecto:

1. Documentación: la aplicación está bien documentada, los manuales revisados son precisos y exactos, pero sólo están disponibles en formato

PDF, lo cual dificulta su acceso en ciertos entornos. Son de agradecer los ejemplos de configuración que aporta para escenarios concretos pero muy usados, como la integración de la autenticación de la aplicación en entornos Microsoft Active Directory y otros servidores LDAP.

2. Soporte de lenguajes: la traducción al español es algo deficiente y tanto ésta como la traducción al Catalá presentan errores funcionales, que se han reportado al desarrollador y del que se ha obtenido respuesta casi inmediata, lo que también es de agradecer.

4.1.2 Requisitos para la instalación de GestióIP

La herramienta IPAM que se instale en la plataforma, en este caso GestióIP, será sin duda la que más exija al propio servidor, y por la tanto la que marque los requisitos mínimos que deba cumplir la plataforma servidora. Estos requisitos se indican a dos niveles diferentes, a nivel de hardware y a nivel de software, y son los que se describen a continuación.

4.1.2.1 Requisitos de hardware

Los requisitos mínimos de hardware para que la aplicación funcione son:

- Procesador: CPU de 2GHz
- Memoria RAM: 1GB
- Espacio en disco: 1.5 GB

Estos son los requisitos mínimos y los que van a servir de base a la distribución.

4.1.2.2 Requisitos de software

A nivel de software tendremos requisitos tanto de sistema operativo como de componentes instalados en el mismo. A nivel de sistema operativo GestióIP corre sobre las siguientes distribuciones Linux:

- Debian
- Ubuntu
- Fedora
- Redhat
- CentOs
- SuSe Linux

Como hemos visto en la descripción de la herramienta GestióIP es una aplicación escrita en Perl, que ofrece un interface web y que almacena los datos en una base de datos MySQL. Esto nos define claramente los requisitos a nivel de aplicaciones que debe cumplir el host que lo aloje, que debe tener instalado:

- El servidor web Apache 2
- El módulo mod_perl de Apache 2
- Perl
- El gestor de base de datos MySQL en versiones 4.x o 5.x (recomendada la versión 5.x)
- La utilidad make

No es obligatorio que el gestor de base de datos MySQL esté instalado en el propio host, ya que GestióIP es capaz de atacar a una base de datos en red, pero en nuestro caso instalaremos MySQL en la misma máquina.

Respecto a la instalación de Perl cabe destacar que el propio script de instalación que incluye verifica si están instalados los módulos de Perl que necesita y, si no lo están, nos ofrece instalarlos, lo que simplifica el cumplimiento de los prerrequisitos de software.

4.2 Herramienta de captura y análisis de tráfico de red (sniffer).

Una de las herramientas básica de análisis y resolución de problemas de red son los sniffers, y como tal no podían faltar en esta distribución.
Este tipo de herramientas nos permite capturar rodo el tráfico que se produce en una red LAN para, bien en tiempo real o bien a posteriori, analizarlo y detectar posibles problemas.
Actualmente uno de los sniffers de red más usados es WireShark [12], y es la herramienta que incluiremos en IpViSix, máxime siendo una de las herramientas que se utilizan en algunas de las asignaturas que se imparten en la UOC, de tal manera que se aprovecha ese esfuerzo de aprendizaje ya realizado.
WireShark incluye un interfaz gráfico que permite analizar de una forma más cómoda la información obtenida, este es uno de los motivos que nos impulsa a incluir un GUI en la distribución que estamos creando.

La versión de WireShark que se incluirá en la distribución será la 1.6.2

4.3 Herramienta de escaneo de red.

Otra de las herramientas básicas de análisis de red son los scanners. Estas herramientas nos ofrecen la capacidad de poder revisar un host concreto en busca de los puertos que tiene abiertos en red. De igual forma podemos buscar hosts en un segmento de red o en toda la red y encontrar dispositivos que respondan a un puerto concreto y bajo un protocolo concreto.
Esta es una utilidad interesante ya que nos permitirá hacer descubrimientos de hosts con la pila IpV6 activa y puertos a la escucha en esa pila.
Sin ningún tipo de duda la herramienta de este tipo que incluiremos en la distribución será Nmap [13], junto a su interfaz gráfico ZenMap [14], que nos permitirá realizar estas tareas y analizar la información obtenida por Nmap de una forma mucho más amigable.
Al igual que WireShark, Nmap (y ZenMap) son herramientas que se utilizan en varias de las asignaturas de redes que se imparten en la UOC, por lo que se garantiza una curva de aprendizaje de las herramientas muy reducida.

- La versión de Nmap que se instalará en IpViSix será la 5.2
- La versión de ZenMap que se instalará en IpViSix será la 5.21

4.4 Verificación de tráfico usado.

Una de las funcionalidades de las que se desea dotar a la distribución IpViSix es una sencilla herramienta que nos permita saber si desde una estación de trabajo o servidor concreto se está usando una pila TCP u otra. En otras palabras, una utilidad de verificación de la pila TCP que usa un cliente concreto.

Para ello lo más sencillo es armar una página web en el servidor IpViSix que recoja datos de las conexiones de clientes que reciba y devuelva esa información en pantalla.
De esta forma si queremos saber si una máquina concreta usa la pila IpV4 o la IpV6 bastaría con iniciar un navegador y conectarnos a una URL concreta publicada en el servidor IpViSix para que la página nos mostrase en la ventana del navegador información sobre la pila que el cliente ha usado para la conexión contra el servidor web.

4.5 Servidor DNS (Domain Name Server)

Un servidor DNS (Domain Name Server) es un servicio de red que se utiliza para resolver nombres de host (entendibles por los humanos) a direcciones Ip (entendibles por las máquinas). El servidor DNS aloja una base de datos con distintos tipos de registros, que son los mecanismos que mapean direcciones Ip con nombres de host, de una manera jerárquica.
En las redes Ipv6 aparecen unos nuevos tipos de registros (como los registros AAAA) que son específicos para esta versión de la pila TCP/IP.
La distribución Ubuntu y sus derivadas permiten la instalación, a través del repositorio del servidor DNS Bind versión 9.
Bind 9 es actualmente unos de los servidores DNS más usados y de mejor reputación, por lo que es el producto que usaremos para instalar en la distribución.
Bind 9 es posible instalarla con Synaptic o con la herramienta tasksel.

5. Instalación y configuración de la plataforma y aplicaciones

En este capítulo detallaremos la instalación de la plataforma de sistema operativo y las aplicaciones de la creación del LiveCD con la distribución IpViSix.

Este capítulo lo dividiremos en las siguientes secciones:

- Instalación de la plataforma
- Configuración del tema de escritorio
- Configuración de red del servidor
- Configuración de DNS
- Instalación de las aplicaciones

Para, en siguientes capítulos, describir cómo crear el LiveCD

5.1 Instalación de la plataforma

En este apartado detallaremos la instalación y la configuración básica de la plataforma sobre la que instalaremos las aplicaciones que hemos seleccionado.

5.1.1 Instalación del sistema operativo

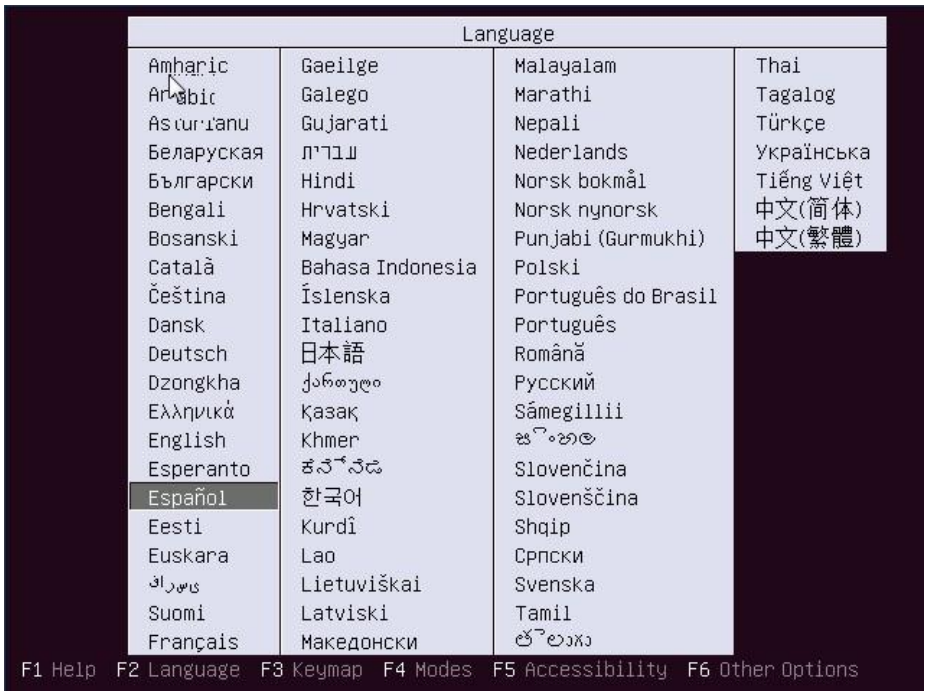
Para instalar el sistema operativo usaremos una Imagen ISO de Ubuntu Server 11.10 y realizaremos una instalación mínima del mismo.

Para que la instalación se desarrolle correctamente es necesario que el equipo dónde vamos a instalar Ubuntu tenga un interfaz de red y pueda conectarse a Internet.

En este documento sólo se detallarán los pasos relevantes para la instalación y personalización correcta del sistema operativo, omitiendo el resto de pasos, para los que se usarán las configuraciones que propone el proceso de instalación o se dejarán indicados los valores de las mismas.

Comenzaremos la instalación insertando el soporte con la imagen del sistema operativo en un medio extraíble desde el que podamos arrancar el sistema.

Tras el inicio la instalación de Ubuntu nos presenta un asistente que nos solicitará que configuremos el lenguaje del servidor.



Seleccionaremos como lenguaje principal el "***Español"***, como se puede apreciar en la imagen anterior.

Una vez seleccionado el lenguaje pulsaremos la tecla ***F4*** para seleccionar el modo de instalación, aparecerá un menú del que seleccionaremos la opción "***Instalar un sistema mínimo"***.

Una vez seleccionado el tipo de instalación seleccionaremos y confirmaremos la opción "***Instalar Ubuntu Server***" que nos presenta el asistente.

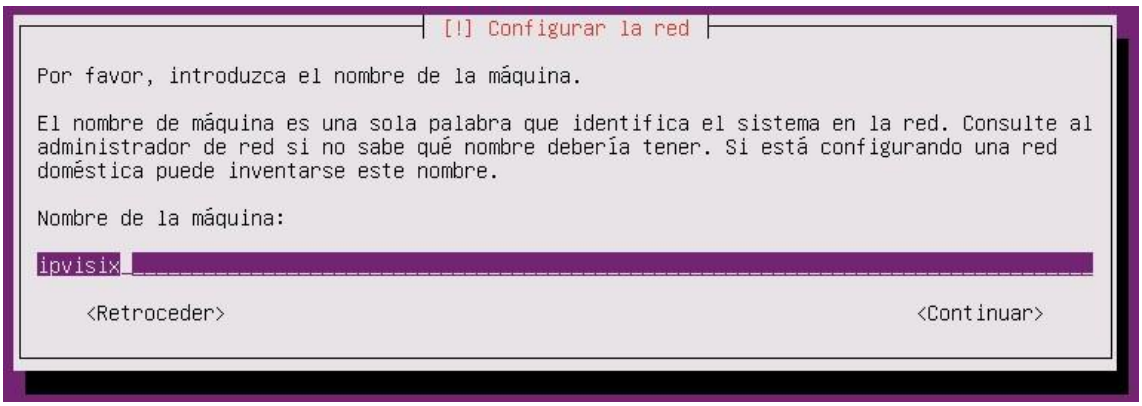
Con lo que comenzará la instalación del sistema operativo propiamente dicha. Esta instalación estará guiada por un asistente que nos irá solicitando valores para la configuración del sistema en función de la evolución de la propia instalación.

Los siguientes datos que nos pedirá el asistente son:

Confirmación de la Zona Horaria: Selecionaremos la zona horaria en la que nos encontremos, en este caso: España.

Configuración del teclado: Si no hemos seleccionado el tipo de teclado en la pantalla inicial de instalación (pulsando la tecla F3 y seleccionando el modelo de la lista) el instalador nos guiará para detectar el mapa de teclas correcto para nuestro teclado.

Tras instalar algunos componentes del sistema el asistente de instalación nos solicitará que introduzcamos el nombre de host para configurar las propiedades de la red.



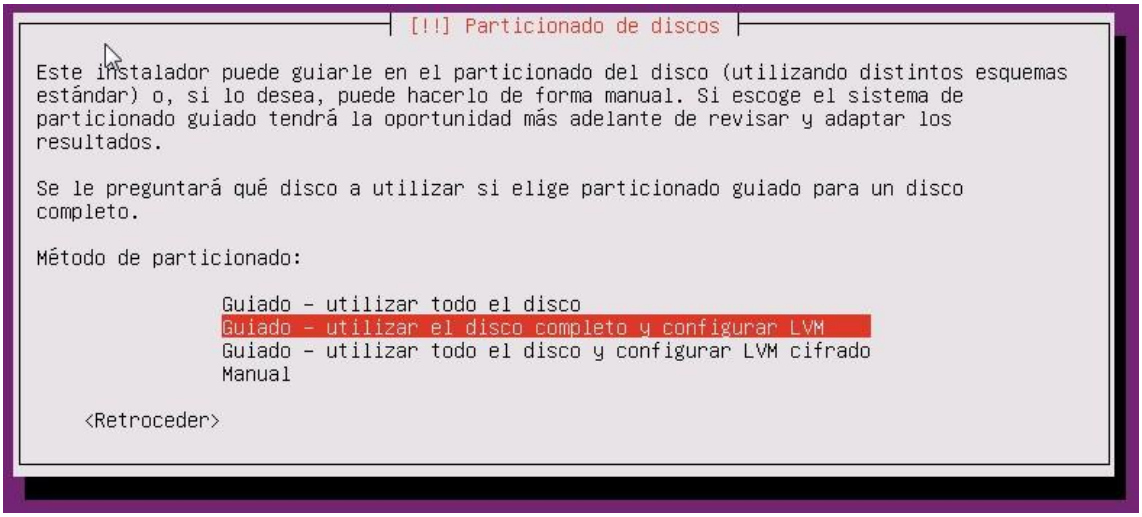
Como nombre de máquina introduciremos "***ipvisix***", seleccionaremos la opción continuar y pulsaremos la tecla "***Enter***".

Los siguientes pasos son:

Configuración del reloj del sistema: en realidad es confirmar la zona horaria en la que está ubicado el servidor

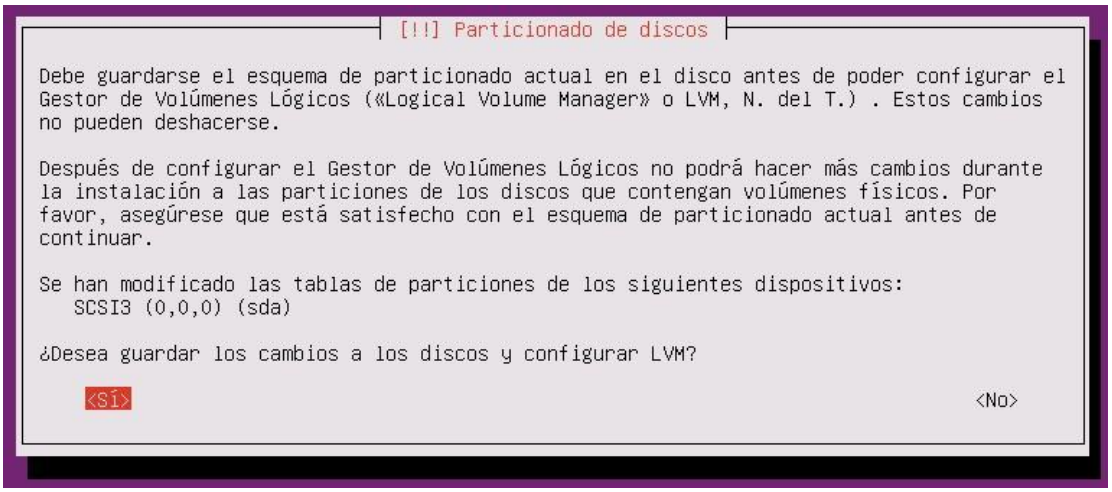
Definir la configuración de los discos. Esta configuración podemos hacerla de forma manual o de forma guiada. En el ejemplo la haremos de forma guiada, aunque la configuración será sencilla ya que usaremos la recomendación del asistente.

Lo primero que haremos es indicar al asistente que usaremos el disco completo para la instalación y que no guíe en el proceso.

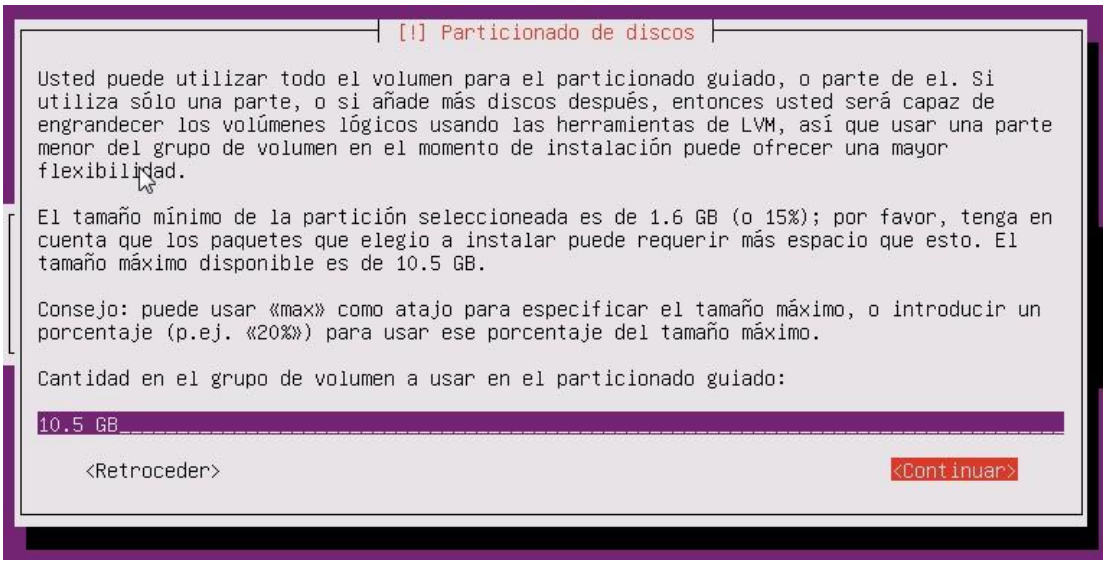


Luego deberemos indicarle el disco sobre el que instalaremos Ubuntu

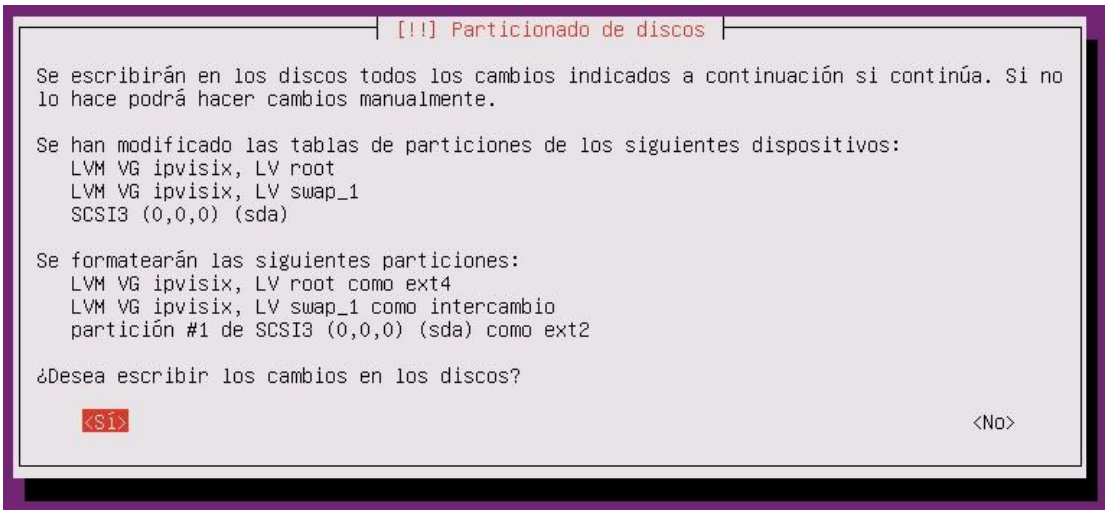
El asistente nos solicitará que, antes de realizar ningún cambio al esquema de particionamiento del disco, salvemos el actual. Aunque en el disco sobre el que vamos a trabajar no hay definido ningún esquema de particionamiento, le indicaremos al gestor de volúmenes lógicos que salve la configuración del disco.



En el siguiente paso indicaremos a LVM que use todo el tamaño de disco para la instalación.



Tras seleccionar la opción "***Continuar***" LVM nos mostrará los cambios que va a realizar sobre el disco y nos solicitará que confirmemos los cambios.



Seleccionaremos la opción "***Si***" para que se realicen los cambios propuestos sobre el disco.

En el siguiente paso de la instalación es el diálogo "***Configurar usuarios y contraseñas***". El asistente nos solicitará los datos necesarios para la creación de un usuario con el que posteriormente podamos iniciar sesión en el sistema. Los datos que proporcionaremos serán:

Nombre completo del usuario: Usuario IpViSix

Nombre de usuario para la cuenta: ipvisix (ver nota *)

Contraseña: Passw0rd

Cifrar la carpeta personal: no

***Nota:** este es el identificador que usaremos para iniciar sesión en el sistema. Se recomienda escribir este nombre sólo en minúsculas, por un problema con Remastersys relacionado al uso de letras mayúsculas en el nombre de inicio de sesión en algunos escenarios.

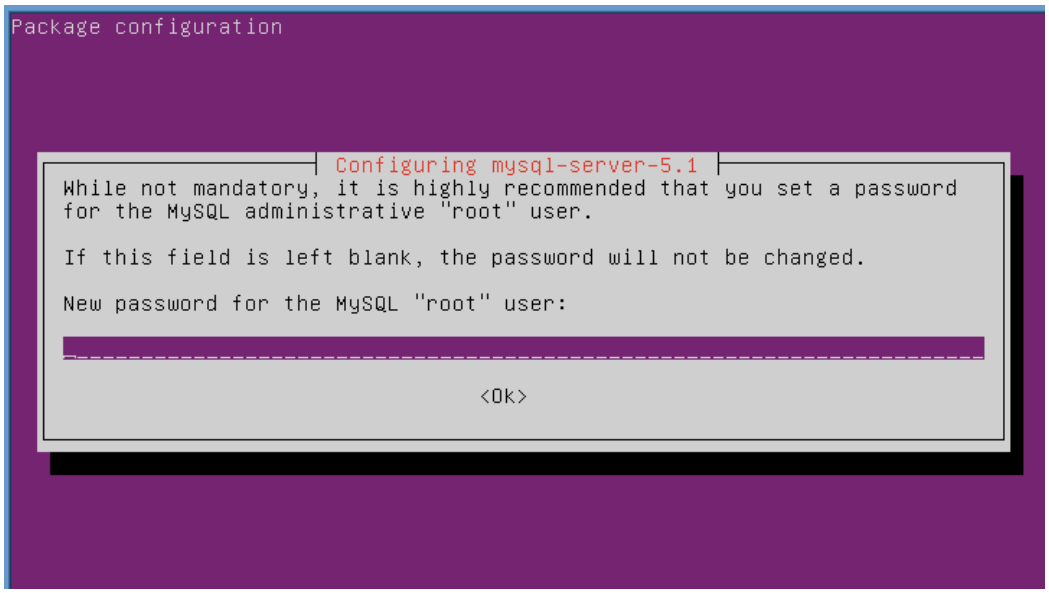
Los tres últimos pasos de la instalación son:

"**Configuración de tasksel**". En este paso se configura el modo de actualizar el sistema. En nuestro caso elegiremos la opción "Sin actualizaciones automáticas".

"**Selección de programas**" dónde se nos presenta una ventana de la utilidad tasksel dónde instalar programas adicionales a nuestra plataforma.

En este momento seleccionaremos e instalaremos los componentes DNS Server y LAMP Server y adelantamos así la instalación de requisitos de las aplicaciones.

Durante la instalación del componente MySQL de servidor LAMP se nos solicitará que indiquemos y confirmemos una contraseña para el usuario root de MySQL

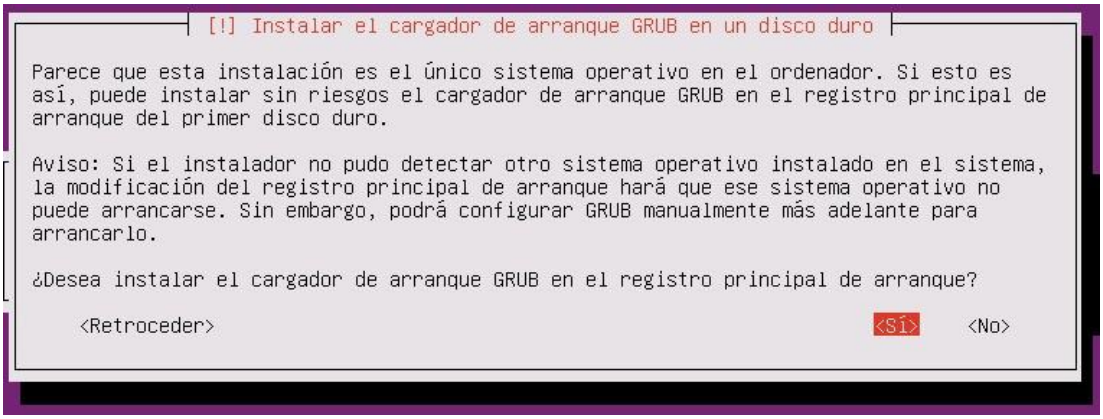


Para esta instalación usaremos la contraseña Passw0rd.

Pulsaremos la opción "***Ok***" y el instalador nos solicitará que volvamos a escribir la contraseña a modo de confirmación.

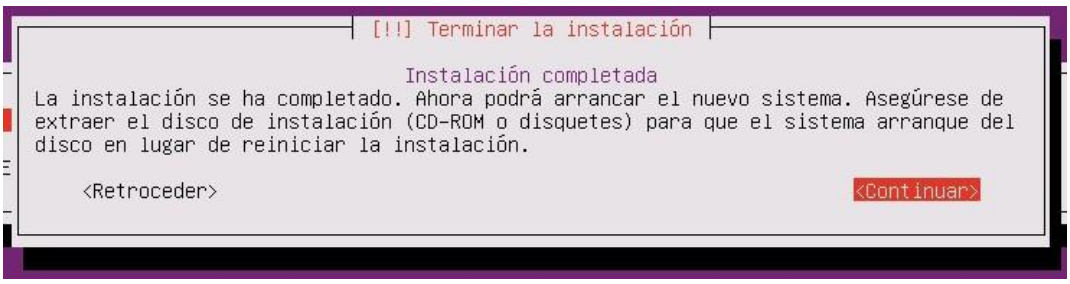
Una vez introducida y confirmada la contraseña para el usuario administrador de MySQL Server 5.1 tasksel continuará con la instalación de los paquetes seleccionados.

Tras instalar las aplicaciones seleccionadas aparecerá el cuadro de diálogo "***Instalar el cargador de arranque GRUB en el disco duro***". Al instalar GRUB estamos haciendo de nuestro disco duro un disco de inicio de Linux.



Seleccionaremos la opción "***Si***" para modificar los sectores de arranque del disco duro.

Una vez realizadas estas tareas habrá finalizado la instalación del sistema operativo.



Retiraremos los soportes de instalación, seleccionaremos la opción "***Continuar***" y pulsaremos la tecla ***Enter***, tras lo cual el sistema se reiniciará y arrancará el nuevo sistema operativo.

Una vez instalado el sistema operativo deberemos instalar y configurar el resto de la plataforma.

5.1.2 Instalación de componentes de la plataforma

Una vez instalado el sistema operativo base procederemos a instalar el resto de componentes de la plataforma que, como hemos indicado antes son:

- Una instalación mínima de Lubuntu desktop
- El navegador de Internet Mozilla Firefox
- El complemento Lxappearance (gestor de configuraciones de escritorio para LXDE)
- El descompresor de ficheros ZIP
- El gestor de conexiones de red Network-Manager

Para instalar estos componentes una vez reiniciado el servidor y como paso previo deberemos actualizar la caché de contenidos de los repositorios de aplicaciones que se genera durante la instalación.
Para lo que usaremos el siguiente comando:

```
apt-get update
```

Una vez actualizado el cache del contenido de los distintos repositorios podremos comenzar a instalar las últimas versiones de los componentes.
Comenzaremos par la instalación del entorno gráfico mínimo de Lubuntu que instalaremos con el siguiente comando:

```
sudo  apt-get install –no-install-recommends lubuntu-desktop
```

Una vez instalado el escritorio básico instalaremos el resto de componentes, para lo que usaremos el siguiente comando:

```
sudo apt-get install firefox zip lxappearance network-manager
```

Una vez instalado estos paquetes reiniciaremos el servidor. Al arrancar de nuevo debe aparecernos la pantalla del gestor de sesiones de Lubuntu.

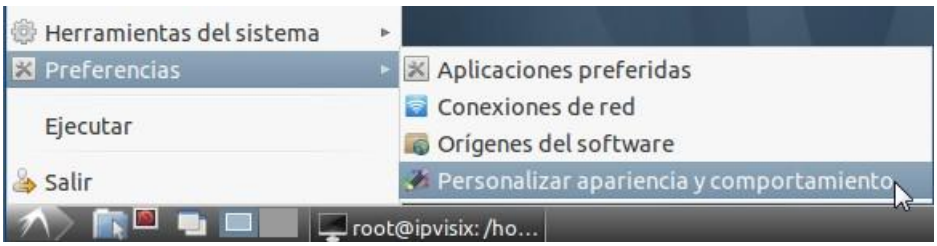
5.2 Configuración del tema de escritorio

Como se indicaba anteriormente es requisito de Ubiquity que el escritorio del usuario tenga configurado por defecto un tema con soporte GTK3. Para configurar el tema de escritorio usaremos Lxappearance, para lo cual:

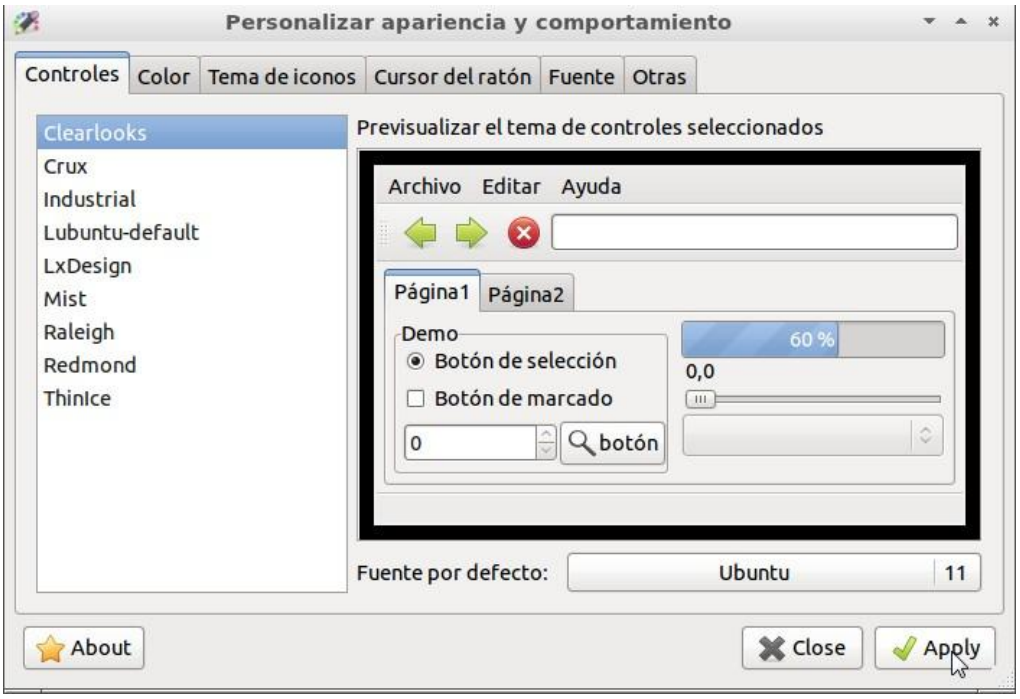
Iniciaremos sesión con las siguientes credenciales:

- **Usuario**: ipvisix
- **Contraseña**: Passw0rd

Iniciaremos Lxappearance, para lo cual pulsaremos sobre el icono ***LXDE*** de la barra de tareas, seleccionaremos el menú "***Preferencias"*** y ejecutaremos "***Personalizar apariencia y comportamiento"***.



Aparecerá la ventana del complemento "***Personalizar apariencia y comportamiento***"



Seleccionaremos el tema "***Clearlooks"*** y pulsaremos el botón "***Apply"***, con lo que tendremos configurado el tema del escritorio.

5.3 Configuración de red del servidor

IpViSix es una plataformas servidora con figurada con doble pila TCP/IP, esto significa que en el mismo adaptador de red tiene configurado direccionamiento Ipv4 e IpV6. Como plataforma servidor que es el direccionamiento configurado es un direccionamiento fijo, con el fin de poder enlazar los servicios a una Ip concreta y que éstos funcionen apropiadamente.

Para el direccionamiento IpV4 del servidor usaremos uno de los rangos de direccionamiento privado de los que el propio protocolo nos ofrece, en concreto usaremos la red 192.168.200.0/24.

En Ipv6 no existen rangos de direccionamiento privado, todas las direcciones se consideran públicas, pero sí existe un rango especial, el 2001:db8/64 que es el rango de documentación. Este es el rango de direcciones IpV6 que usaremos para esta plataforma.

En los siguientes apartados detallaremos las configuraciones de la plataforma tanto de los adaptadores (direccionamiento de red) como de los servicios básicos de red que se incorporan (DNS)

5.3.1 Direccionamiento de red

En este apartado se detallan las configuraciones del adaptador de red y nombres de servidor.

5.3.1.1 Configuración IpV4

La configuración IpV4 será la siguiente:

Dirección de red: 192.168.200.11

Máscara de red: 255.255.255.0

DNS primario: 192.168.200.11

La plataforma no tendrá configurado ningún Gateway por defecto, lo que impedirá que pueda enviar tráfico a otras redes, incluida Internet.

5.3.1.2 Configuración IpV6

La configuración IpV6 del servidor será:

Dirección de red: 2001:db8:1::fede

Prefijo de red: /48

DNS primario: 2001:db8:1::fede

Al igual que en IpV4, plataforma no tiene configurado ningún Gateway por defecto, lo que impedirá que pueda enviar tráfico a otras redes.

5.3.1.3 Nombre de Host

El nombre de host es: ipvisix

El nombre FQDN del servidor es: ipvisix.ipvisix.lcl

5.3.2 Configuración de la red

El primer paso es deshabilitar la configuración automática en el protocolo IPv6, ya que este protocolo tiene la característica de que los Gateway de la red se anuncian usando un protocolo denominado RA (Router Advertisement) y el adaptador de red toma su gateway de esta forma. En un servidor como IpViSix esto puede ser un problema, así que deshabilitamos la auto configuración para IPv6 con el siguiente comando ejecutado desde una consola de terminal:

```
sudo sysctl –w  net.ipv6.conf.all.autoconf=0
```

tras ejecutar el comendo Ubuntu nos devolverá el estado del parámetro modificado:

```
net.ipv6.conf.all.autoconf=0
```

Para la configuración de estos parámetros editaremos el fichero:

```
/etc/network/interfaces
```

Lo primero que haremos es una copia de seguridad del fichero de configuración con el comando

```
sudo cp /etc/network/interfaces  /etc/network/interfaces.backup
```

una vez hecha la copia de seguridad modificaremos el fichero, para lo que podemos usar el editor nano.

```
sudo nano /etc/network/interfaces
```

y añadiremos las líneas siguientes:

```
auto eth0
### inicio config. IPv4
iface eth0 inet static
address 192.168.200.11
netmask 255.255.255.0
network 192.168.200.0
broadcast 192.168.200.255
### Fin config. IPv4
### inicio config. IPv6
iface eth0 inet6 static
```

```
address 2001:db8:1::fede

netmask 48

### Fin config. IPv6
```

Salvaremos el fichero modificado y reiniciaremos el interfaz de red con el siguiente comando:

```
sudo ifdown eth0 && ifup eth0
```

Una vez hechos los cambios podremos probar si el adaptador responde a las nuevas ip con los siguientes comandos:

```
ping 192.168.200.11

ping6 2001:db8:1::fede
```

Deberemos obtener respuesta positiva desde el servidor.

Una vez configuradas las direcciones ip configuraremos los servidores DNS que usará el adaptador. Para ello deberemos editar el fichero **/etc/resolv.conf** y añadiremos las siguientes líneas:

```
search ipvisix.lcl

nameserver 192.168.200.11

nameserver 2001:db8:1::fede
```

Salvaremos el fichero modificado y volveremos a reiniciaremos el interfaz de red con el siguiente comando:

```
sudo ifdown eth0 && ifup eth0
```

Tras realizar estas configuraciones ya tendremos los adaptadores de red del servidor configurados.

5.4 Configuración de DNS

Uno de los componentes instalados en la plataforma es el servidor DNS BIND9. La configuración de este componente incluirá la creación de una zona de resolución directa (ipvisix.lcl) y una zona de resolución inversa para el rango de direccionamiento IpV6 que se usará.

El servidor BIND9 tendrá listeners definidos en ambos protocolos. Por defecto BIND9 escucha en sockets IpV4, para habilitar el soporte a IpV6 deberemos modificar el fichero **/etc/bind/named.conf.options**, dónde se deben añadir, si no existe, la siguiente línea en la sección **options**:

```
listen-on-v6 {any;} ;
```

Una vez reiniciado el servicio y para verificar si BIND9 ofrece listeners en las dos pilas TCP/IP podremos usar el comando:

```
netstat –tan
```

En la salida del comando podremos ver en qué puertos está publicado el servicio DNS.

```
root@ipvisix-virtual-machine:/etc/bind# netstat -tan
Conexiones activas de Internet (servidores y establecidos)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp        0      0 127.0.0.1:3306          0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:80              0.0.0.0:*              ESCUCHAR
tcp        0      0 192.168.200.11:53       0.0.0.0:*              ESCUCHAR
tcp        0      0 127.0.0.1:53            0.0.0.0:*              ESCUCHAR
tcp        0      0 127.0.0.1:953           0.0.0.0:*              ESCUCHAR
tcp6       0      0 :::53                   :::*                   ESCUCHAR
tcp6       0      0 ::1:953                 :::*                   ESCUCHAR
```

Como podemos apreciar en la captura de pantalla los DNS (TCP/53) está a la escucha tanto en IPv4 como en IPv6.

5.4.1 Zonas DNS

Tal y como se indicaba crearemos dos zonas primarias. Estas zonas se deben definir editando el fichero **/etc/bind/named.conf.local**, dónde crearemos un registro que apunte al fichero de cada zona y el tipo de zona (primaria o secundaria). Los registros serán:

```
zone "ipvisix.lcl" {
 type master;
 file "ipvisix.lcl.zone";
};

zone "1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
 type master;
 file "2001-db8-1.zone";
};
```

5.4.1.1 Zona de resolución directa ipvisix.lcl

El fichero de zona **/var/cache/bind/ipvisix.lcl.zone** tendrá el siguiente contenido:

```
$TTL 86400
@ IN SOA ipvisix.ipvisix.lcl. dnsadmin.ipvisix.lcl (
 2012052001 ; serial
 28800 ; refresh
 7200 ; retry
 604800 ; expire
 86400 ) ; Minimun TTL


            IN     NS    ipvisix.ipvisix.lcl.

ipvisix     IN     A     192.168.200.11
            IN     AAAA  2001:db8:1:0:0:0:0:fede
ipvx        IN     A     192.168.200.11
            IN     AAAA  2001:db8:1:0:0:0:0:fede
ipv6        IN     AAAA  2001:db8:1:0:0:0:0:fede
ipv4        IN     A     192.168.200.11
```

5.4.1.1 Zona de resolución inversa

El fichero de zona **/var/cache/bind/2001-db8-1.zone** tendrá el siguiente contenido:

```
$TTL 86400
@ IN SOA ipvisix.ipvisix.lcl. dnsadmin.ipvisix.lcl (
 2012052001 ; serial
 28800 ; refresh
```

```
 7200 ; retry
 604800 ; expire
 86400 ); Minimun TTL

IN NS ipvisix.ipvisix.lcl.
e.d.e.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR ipv6.ipvisix.lcl.
```

Después de crear los dos ficheros de zona es conveniente verificar su sintaxis, ya que BIND9 es muy estricto y si detecta errores en los ficheros de zona no se iniciará. Para verificar la sintaxis de los ficheros usaremos la herramienta named-checkzone. Para la verificación usaremos los siguientes comandos:

sudo cd /var/cache/bind

named-checkzone ipvisix.lcl ipvisix.lcl.zone

named-checkzone 1.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA .2001-db8-1.zone

Si la herramienta detecta errores en la sintaxis de los ficheros nos indicará el tipo de error. Una vez verificados los ficheros deberemos reiniciar el servicio DNS Server, para lo que usaremos el siguiente comando:

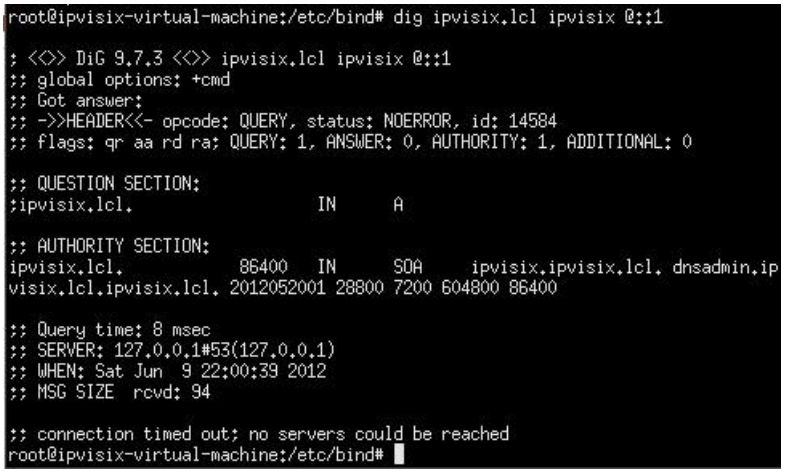
sudo /etc/init.d/bind9 restart

Una vez reiniciado el servicio deberemos verificar que funcione correctamente. Esta verificación podremos hacerla con las utilidades "ping" o "dig".

Si usamos "dig" la sintaxis del comando será:

dig ipvisix.lcl ipvisix @::1

Este comando debe devolver la configuración de la zona ipvisix.lcl



5.5 Instalación de aplicaciones

En este apartado detallaremos el proceso seguido para instalar las aplicaciones que incluirá la distribución.

5.5.1 Instalación de BIND 9

Este componente se ha instalado junto con el sistema operativo, por lo que nos referimos al apartado de instalación de la plataforma servidor para más detalles.

5.5.2 Instalación de WireShark, Nmap y ZenMap

La instalación de estas herramientas es muy sencilla y el proceso en sí mismo no presenta mayor interés, así que nos limitaremos a indicar los comandos que se

usarán para la instalación. Estos comandos es necesario ejecutarlos desde una consola de terminal con elevación de privilegios.

Podemos instalar las dos aplicaciones de forma conjunta, para lo que usaremos el siguiente comando:

```
sudo apt-get install wireshark zenmap
```

Tras lo cual se descargarán e instalarán los paquetes necesarios para el funcionamiento de ambas herramientas.

5.5.3 Instalación de GestióIP

En éste apartado se detalla la instalación tanto de los prerrequisitos de GestióIP como de la propia aplicación.

5.5.3.1 Instalación de los prerrequisitos de GestióIP

Tal y como se ha indicado en el punto 5.1.2.2 de este mismo documento los prerrequisitos para la instalación de GestióIP son:

- El servidor web Apache 2
- El módulo mod_perl de Apache 2
- Perl
- La utilidad make
- El gestor de base de datos MySQL en versiones 4.x o 5.x (recomendada la versión 5.x

Tanto Apache 2 como MySQL server 5.1 como PHP se han instalado junto con el sistema operativo, por lo que nos referimos al apartado de instalación de la plataforma servidor para más detalles.

Otro de los requisitos es la herramienta make, que nos permite recompilar el kernel. El último de los prerequisitos es la instalación de Apache 2 mod_perl. Para la instalación de estos dos componentes de forma conjunta usaremos también apt. Desde una consola de terminal teclearemos el comando:

```
sudo apt-get install libapache2-mod-perl2 make
```

Apt creará la lista de dependencias para ambos componentes y nos solicitará confirmación para la descarga e instalación de los paquetes necesarios del repositorio de Ubuntu. Una vez finalizada la instalación apt devolverá el control a la consola.

Con estos pasos finalizamos la instalación de prerequisitos para la aplicación GestióIP. No se ha instalado Perl, que también es necesario, porque el instalador de GestióIP es capaz de detectar la falta de esos módulos e instalarlos automáticamente.
Una vez instalados todos los prerequisitos es recomendable reiniciar el sistema, para lo que podemos usar, desde una consola de terminal, el siguiente comando:

```
sudo shutdown –r now
```

Cuando la máquina se reinicie podremos continuar con la instalación de las aplicaciones.

5.5.3.2 Instalación de GestióIP

La instalación de GestióIP está muy bien descrita en los manuales de la aplicación, por lo que en este documento no detallaremos todos los pasos del proceso sino solo los más significativos, refiriéndonos al manual indicado para el resto.

Esta instalación se divide en dos partes:

- Una instalación en modo comando, que realiza ejecutando un script desde un terminal con privilegios root
- Creación de la base de datos y configuración de los parámetros básicos de la solución.

A continuación detallaremos los pasos más importantes de la instalación.

El primer paso es descargar desde el repositorio de la aplicación el fichero comprimido de la instalación, en nuestro caso, que instalaremos la versión 3.0, el fichero se denomina ***gestioip_3.0.tar.gz***.

Una vez descargado el fichero con la instalación, abriremos una consola, cambiaremos al directorio dónde hemos descargado el instalador y descomprimiremos el paquete con el comando siguiente:

```
tar -vzxf gestioip_3.0.tar.gz
```

al descomprimir el fichero se creará una carpeta llamada gestioip_3.0, cambiaremos a esa carpeta con el comando siguiente:

```
cd gestioip_3.0
```

y ejecutaremos el fichero setup_gestioip.sh con permisos de root, para lo que usaremos el comando siguiente:

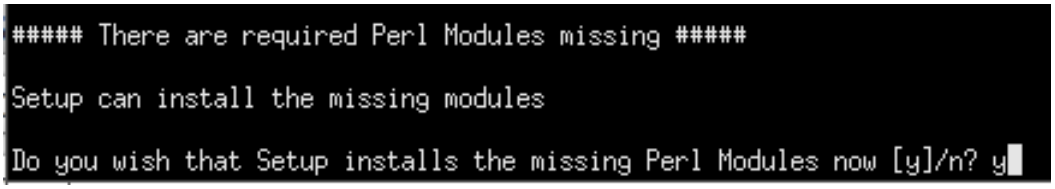
```
sudo ./setup_gestioip.sh
```

La ejecución de este comando inicia la primera fase de la instalación que se realiza desde consola, el instalador solicitará confirmación para proceder a instalar GestióIP

Tras confirma el comienzo de la instalación el script solicitará confirmación en varios puntos, que se omiten por brevedad. Para más detalle se deberá revisar el documento de instalación.

En un momento de la instalación el script nos preguntará si tenemos planeado importar direccionamientos y redes desde hojas de cálculo.

Le indicaremos que sí (pulsando la tecla "***Y***" y pulsando "***Enter".*** El script detecta que faltan módulos de Perl por instalar y nos ofrece descargarlos e instalarlos.



Confirmaremos esta opción y el script descargará de los repositorios de Ubuntu los módulos Perl necesarios y los instalará.

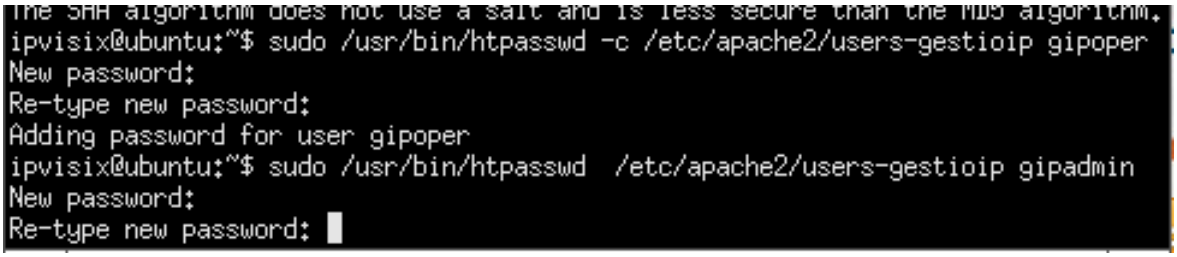
El siguiente punto relevante de la instalación se produce tras verificar que la instalación de Apache 2 es correcta. En ese momento el script de instalación solicita la creación de dos usuarios para la aplicación: un usuario operador (gipoper) y un usuario administrador (gipadmin)

Para crear los usuarios en Apache 2 deberemos abrir otra consola de terminal y, con permisos de root, ejecutar los comandos que nos indica (tal y como nos los indica) el script de instalación. En este ejemplo los comandos son:

sudo /usr/bin/htpasswd –c /etc/apache2/users-gestioip gipoper

sudo /usr/bin/htpasswd /etc/apache2/users-gestioip gipadmin

En la segunda consola la ejecución de los comandos crea los dos usuarios descritos y solicita que se les asigne una contraseña



Una vez creados los dos usuarios necesarios y asignadas contraseñas a los mismos volveremos a la primera consola y pulsaremos la tecla Enter.

Nota:

En esta instalación se han usado como contraseñas las mismas que el nombre de usuario. Si se realiza una instalación del LiveCD se deberán cambiar estas contraseñas por otras que cumplan unos mínimos requisitos de seguridad.

El script de instalación continuará con su tarea hasta que finalice, momento en el que mostrará la siguiente pantalla

```
Installation of GestioIP successfully finished!

Please, review /etc/apache2/conf.d/gestioip.conf
to ensure all is good and

RESTART Apache daemon!

Then, point your browser to

http://server/gestioip/install

to configure the database server.
Access with user "gipadmin" and the
the password which you created before
```

En este momento deberemos reiniciar el demonio Apache2 y continuaremos la segunda parte de la instalación, la creación y configuración de la base de datos.

Para reiniciar el demonio Apache2 ejecutaremos el siguiente comando desde una consola de terminal:

`/etc/init.d/apache2 restart`

Después de reiniciar Apache2 deberemos abrir el navegador de internet que tengamos instalado, en la distribución es Firefox, e iremos a la siguiente URL:

`http://ipvisix/gestioip/install`

Cuando se establezca la conexión contra el servidor la aplicación nos solicitará credenciales, insertaremos las credenciales del usuario administrador, es decir:

Usuario: gipadmin
Password: gipadmin

Una vez autentificados contra la aplicación veremos la ventana de bienvenida, que nos indica los pasos que se ejecutarán a continuación.

Pulsaremos en el botón [Sic] "**delante**" (como se puede apreciar hay algunos errores en la traducción al español) y la aplicación nos mostrará un formulario para la creación de la base de datos.

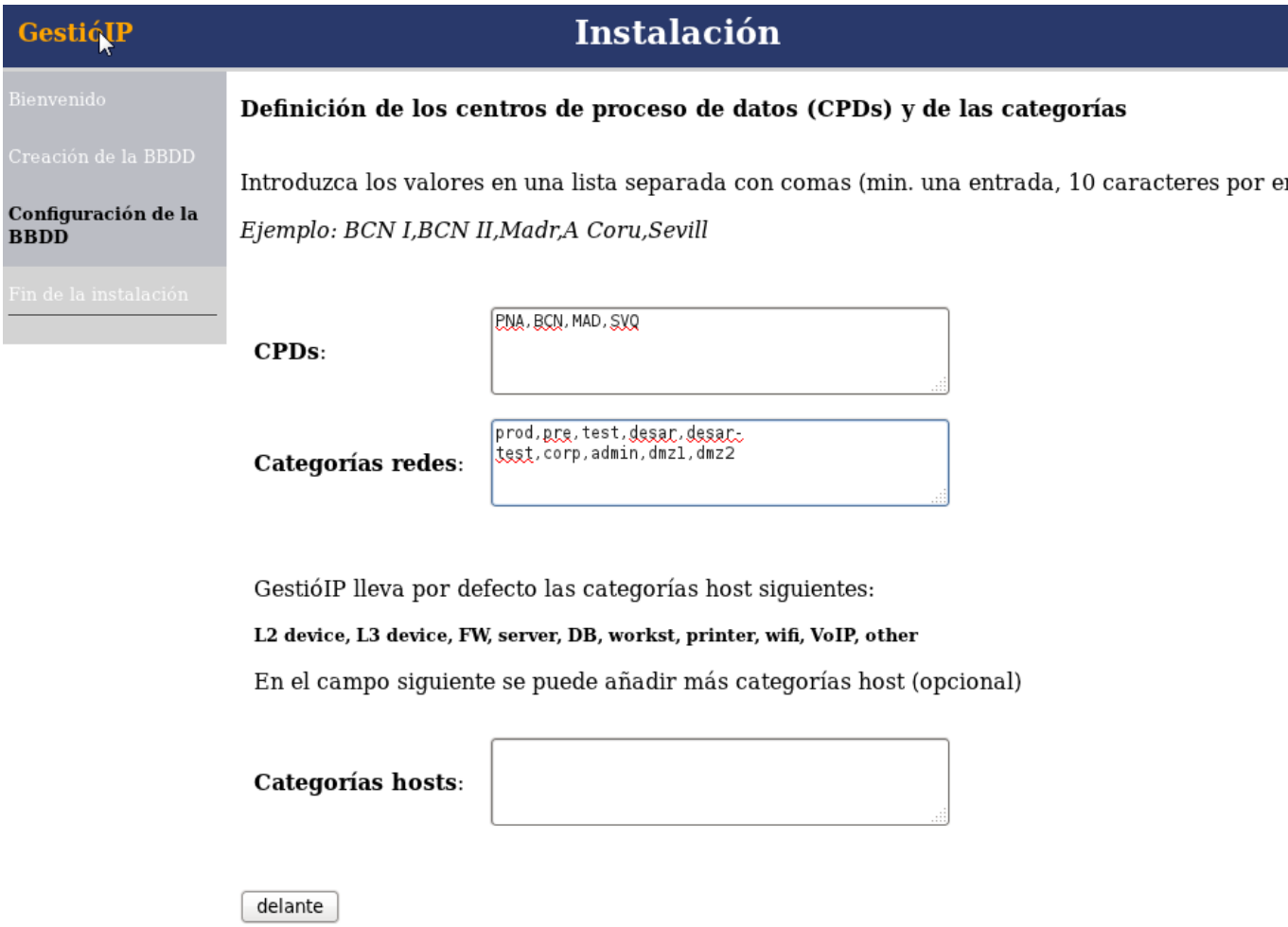
Deberemos cumplimentar los datos del formulario según las indicaciones del propio formulario.

Una vez cumplimentados los datos del formulario pulsaremos el botón "**enviar**".

Nota:
La contraseña asignada a los usuarios es:
Usuario: ipvisix
Contraseña: Passw0rd

Usuario: gestioip
Contraseña: gestioip

El siguiente paso es la personalización de la aplicación.
GestióIP nos muestra un formulario dónde podemos comenzar a introducir datos de nuestra instalación, como las distintas ubicaciones físicas de nuestra red, las categorías o tipos de redes de las que se disponen y también podemos añadir categorías de hosts personalizadas. Como mínimo es obligatoria la introducción de una ubicación o CPD.



una vez cumplimentado pulsaremos el botón [Sic]"**delante**".

Con el siguiente paso finalizaremos la instalación de la aplicación. Se trata de, siguiendo las indicaciones del interfaz de instalación, eliminar los rastros que deja la misma. Además se elimina la propia web desde la que se lanza la herramienta de instalación, por lo que esta utilidad no podrá volver a ejecutarse.

Abriremos una consola de terminal y ejecutaremos el comandos que nos indica la instalación, en este caso:

```
sudo rm –r /var/www/gestioip/install
```

Con esta última tarea ya dispondremos de la aplicación a la que podremos acceder con cualquier navegador utilizando la URL:

```
http://ipvisix.ipvisix.lcl/gestioip
```

5.5.4 Instalación de Remastersys

La herramienta Remastersys puede instalarse tanto con el gestor de paquetes Synaptic, con la herramienta apt o descargando los paquetes de instalación desde la página web del desarrollador.
Para instalar Remastersys con las herramientas Synaptic o apt deberemos añadir el repositorio de descarga la lista de repositorios del gestor de paquetes, bien con el propio interfaz gráfico de Synaptic o editando el fichero **/etc/apt/sources.list**. A continuación indicaremos los pasos a dar par la instalación de Remastersys desde la consola, es decir, con apt:

En primer lugar descargaremos e instalaremos la clave gpg del repositorio, para lo cual ejecutaremos el siguiente comando desde una consola de terminal con permisos de root:

```
sudo wget –O - http://www.remastersys.com/ubuntu/remastersys.gpg.key | apt-key add -
```

Una vez descargada e instalada la clave gpg del repositorio deberemos modificar la lista de fuentes del gestor de paquetes.
Para realizar esto cambios podemos usar el editor de textos "nano" por poner un ejemplo, es conveniente recordar que se pretende tener una distribución lo más ajustada en tamaño posible, por lo que se dispone únicamente de una selección de herramientas.
En el fichero **/etc/apt/sources.list** insertaremos las siguientes líneas:

```
# Remastersys Oneiric
deb http://www.remastersys.com/ubuntu oneiric main
```

Una vez realizada la modificación en la lista de repositorios deberemos actualizarla localmente, esta tarea puede hacerse utilizando la herramienta Synaptic o ejecutando el comando `apt` desde un terminal. Para obtener la lista actualizada del software en los repositorios desde un terminal (iniciado con root o elevación permisos) ejecutaremos:

```
apt-get update
```

Una vez actualizada la lista de paquetes en los repositorios instalaremos Remastersys, para lo que usaremos el comando siguiente:

```
apt-get install remastersys remastersys-gui
```

El gestor de paquetes apt verificará la lista de dependencias y nos solicitará confirmación para la descarga e instalación del software. En realidad se están instalando dos paquetes: Remastersys propiamente dicho y el interfaz gráfico de la herramienta.
A partir de este momento ya dispondremos de las herramientas para la creación del LiveCD.

6. Herramienta de verificación de la pila TCP cliente

Una de las utilidades que se incluye en IpViSix es una herramienta que nos permite verificar si un host remoto establece una conexión contra el servidor IpViSix usando una pila TCP/IP versión 4 o TCP/IP versión 6.
Se trata de provocar una conexión TCP desde el host remoto hacia el host IpViSix contra un servicio bien conocido, que se pueda publicar tanto para IpV4 como para IpV6 y del que se pueda obtener suficiente información como para devolver un resultado rápido y coherente.

6.1 Propuesta de solución

Tras un somero análisis la forma más sencilla y eficiente de implementar esta utilidad es a través de un script que se invoque al acceder a una página web especialmente creada. De esta manera podemos fácilmente lograr los objetivos de la utilidad:

- Podemos provocar la conexión a demanda contra un servicio bien conocido, como el servicio HTTP (TCP/80).

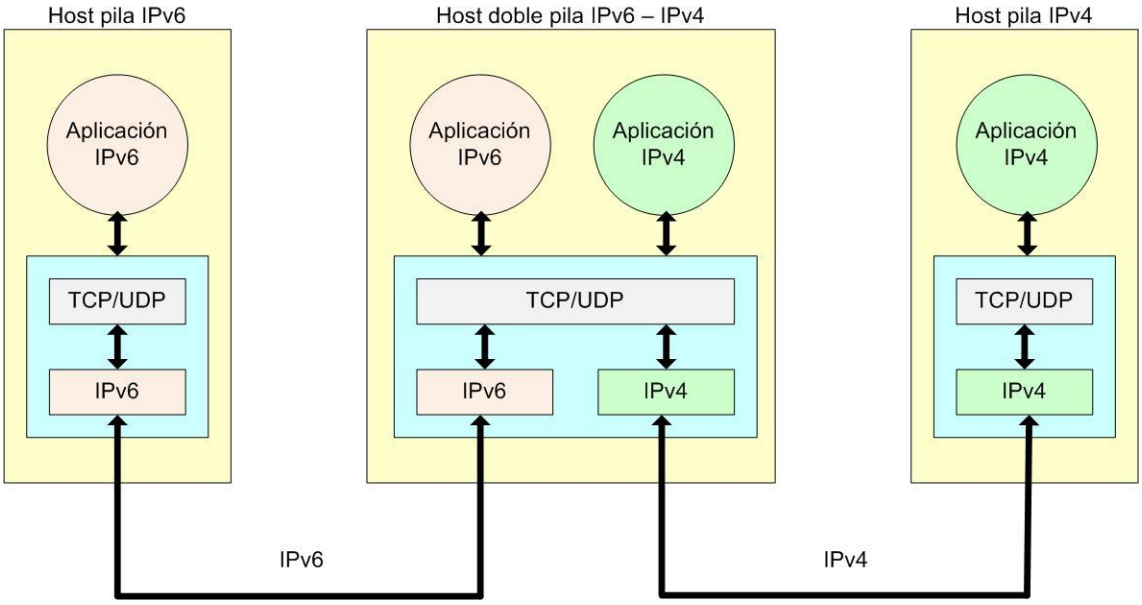
- Tomar información de la propia conexión ya que, los navegadores en las propias cabeceras del protocolo HTTP, incluyen mucha información sobre el origen del tráfico, que es relativamente sencilla de explotar.

- Podemos devolver la información al usuario de una forma clara y concisa en la misma página web a la que se ha conectado, o en otra hacia la que redirija la conexión.

- No es necesario instalar ningún componente adicional a la plataforma servidora, ya que se puede usar tanto el servidor Apache como la plataforma PHP que ya se incluyen para dar soporte a otras aplicaciones.

A la aplicación la denominaremos "***Reconocimiento de Pila Cliente***".
La utilidad no sólo nos permitirá saber con qué tipo de pila TCP se inicia una conexión, sino también si una pila concreta, en este caso IpV6, puede funcionar sin problemas en un entorno de red concreto. Esto es posible ya que en un servidor web como Apache nos permite crear distintos sitios web que responden a distintas IP y con ayuda del servicio DNS podemos ser capaces de dirigir el tráfico a un sitio web u otro simplemente creando registros para las distintas Ip asignadas al servidor web.
De esta manera, si en un Host cliente configurado adecuadamente con doble pila TCP podemos acceder al servidor IpViSix con el servicio de reconocimiento de pila cliente activo, usando IpV4 y no IpV6 podemos sospechar de que algún elemento de red por la que circulan los paquetes TPC/IP no soporta el tráfico IpV6.

De forma gráfica el comportamiento de la aplicación frente a la pila de conexión es la que se puede apreciar en la siguiente imagen:



El host con doble pila publica aplicaciones para cada una de ellas y sólo los clientes con la pila correcta acceden a la aplicación. En nuestro caso cada Virtual Host definido en Apache es una aplicación.

6.2 Reconocimiento de Pila Cliente

Esta aplicación se basa en:

- Un servidor Apache con dos Virtual Hosts creados cada uno respondiendo a una pila TCP/concreta.
- Tres Web Sites creados a los que se accede desde los distintos Virtual Hosts
- Un script PHP, ubicado en cada uno de los Web Sites.

A continuación detallaremos la configuración de cada elemento de la aplicación:

6.2.1 Script PHP

El script es una pequeña utilidad que se ejecuta al recibir una conexión cliente.
De la conexión extrae:

- El nombre del Virtual Host contra el que se realiza la conexión
- La ip de origen de la conexión
- El puerto de origen
- El navegador con el que se ha realizado la conexión

En función de los patrones de la dirección Ip de origen de tráfico, el script indica en pantalla la pila que se está usando para la conexión y los datos extraídos de la misma.
El código del script es el siguiente:

```
<?php
echo "<font color='#154983' size=18 face='verdana'>Utilidad de verificación de
pila TCP cliente.</font><br><br>";

echo "<font color='#FF0000' size=12 face='verdana'>Se ha conectado al virtual
host: (".$_SERVER['SERVER_NAME']).</font><br><br>";

 if(strpos($_SERVER['REMOTE_ADDR'],".")===false)
{
echo "<font color='#154983' size=2 face='verdana'>Su conexión se ha realizado
usando la pila IPv6.</font><br><br>";
```

```
}else{
$DIRv4=str_replace("::ffff:","",$REMOTE_ADDR);
echo "<font color='##154983' size=2 face='verdana'>Su conexión se ha realizado
usando la pila IPv4.</font><br><br>";
}
echo "<font color='#FF0000' size=2 face='verdana'>Su dirección Ip es:
(".$_SERVER['REMOTE_ADDR']).</font><br><br>";
echo "<font color='#FF0000' size=2 face='verdana'>El puerto de origen es:
(".$_SERVER['REMOTE_PORT']).</font><br><br>";
echo "<font color='#FF0000' size=2 face='verdana'>El navegador utilizado es:
(".$_SERVER['HTTP_USER_AGENT']).</font><br><br>";

?>
```

6.2.2 Instalación de la aplicación

La instalación de la aplicación es un proceso externadamente sencillo, ya que basta con crear las carpetas correspondientes para cada Web Site, copiar en ellas el mismo fichero index.php que contiene el script y configurar el servidor Apache.

Importante:
Antes de crear estas configuraciones deberemos asegurarnos de que la red del servidor y las zonas DNS están correctamente configuradas.

Los comandos que usaremos para la creación de las carpetas y copia de los ficheros son:

```
sudo mkdir /var/www/testip
sudo mkdir /var/www/testip/ipvx
sudo mkdir /var/www/testip/ipv4
sudo mkdir /var/www/testip/ipv6
sudo cp index.php /var/www/testip/ipvx
sudo cp index.php /var/www/testip/ipv4
sudo cp index.php /var/www/testip/ipv6
```

Estos comandos los lanzaremos desde una consola de terminal ubicados en el directorio dónde se encuentre el fichero `index.php`

6.2.1 Configuración del servidor web Apache

En el servidor Web Apache deberemos realizar las siguientes tareas:

Creación del fichero **/etc/apache2/sites-available/ipvx**, que contendrá las siguientes líneas:

```
NameVirtualHost [2001:db8:1::fede]
NameVirtualHost 192.168.200.11

<VirtualHost [2001:db8:1::fede]>
      DocumentRoot /var/www/testip/ipvx
      ServerName ipvx.ipvisix.lcl
</VirtualHost>

<VirtualHost 192.168.200.11>
      DocumentRoot /var/www/testip/ipvx
      ServerName ipvx.ipvisix.lcl
</VirtualHost>


<VirtualHost 192.168.200.11 >
      DocumentRoot /var/www/testip/ipv4
      ServerName ipv4.ipvisix.lcl
</VirtualHost>
```

```
<VirtualHost [2001:db8:1::fede]>
      DocumentRoot /var/www/testip/ipv6
      ServerName ipv6.ipvisix.lcl
</VirtualHost>
```

Con esta configuración creamos los virtual hosts y provocamos que:

- El sitio **ipvx.ipvisix.lcl/index.php** responda tanto por IPv4 como por IPv6, cargando la página ubicada en **/var/www/testip/ipvx**

- El sitio **ipv4.ipvisix.lcl/index.php** responda sólo por IPv4, cargando la página ubicada en **/var/www/testip/ipv4**

- El sitio ipv6.ipvisix.lcl/index.php responda sólo por IPv6, cargando la página ubicada en **/var/www/testip/ipv6**

Deshabilitaremos la característica SendFile, que es un método para acelerar el tráfico de datos, pero que puede dar algunos problemas con IPv6. Para ello editaremos el fichero **/etc/apache2/httpd.conf** y agregaremos la línea:

```
EnableSendfile  off
```

Por último deshabilitaremos el Sitio Web por defecto y habilitaremos el que hemos creado, para lo que usaremos los siguientes comandos:

```
sudo a2ensite ipvx
sudo a2dissite default
```

Una vez realizadas estas configuraciones deberemos reiniciar el servidor Apache

```
service apache2 reload
```

o bien

```
sudo /etc/init.d/apache2 restart
```

Ya sólo resta verificar que todo funciona adecuadamente para lo que será suficiente abrir el navegador Firefox en el propio servidor y acceder a las siguientes URL

http://ipvx.ipvisix.lcl/index.php

http://ipv4.ipvisix.lcl/index.php

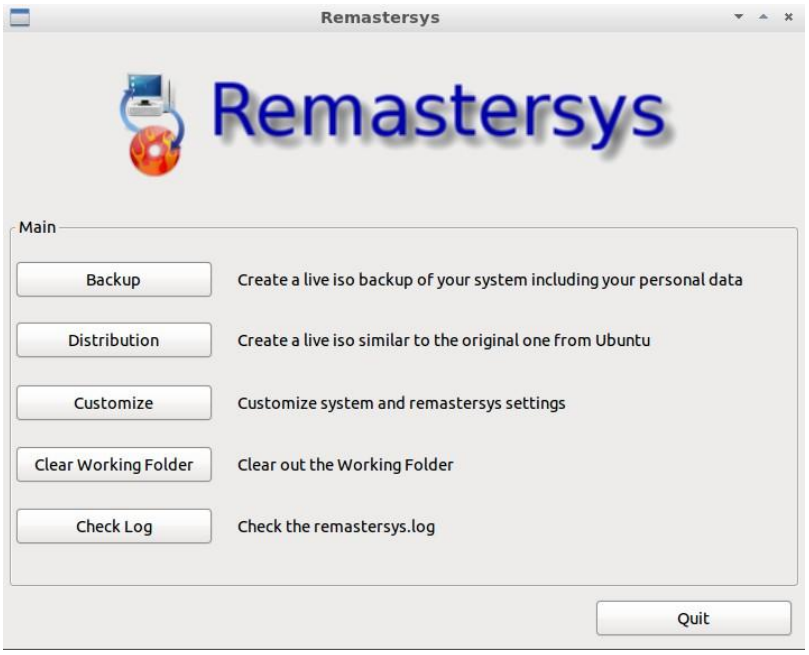
http://ipv6.ipvisix.lcl/index.php

Las páginas nos devolverán información acerca de la pila y dirección Ip de la conexión.

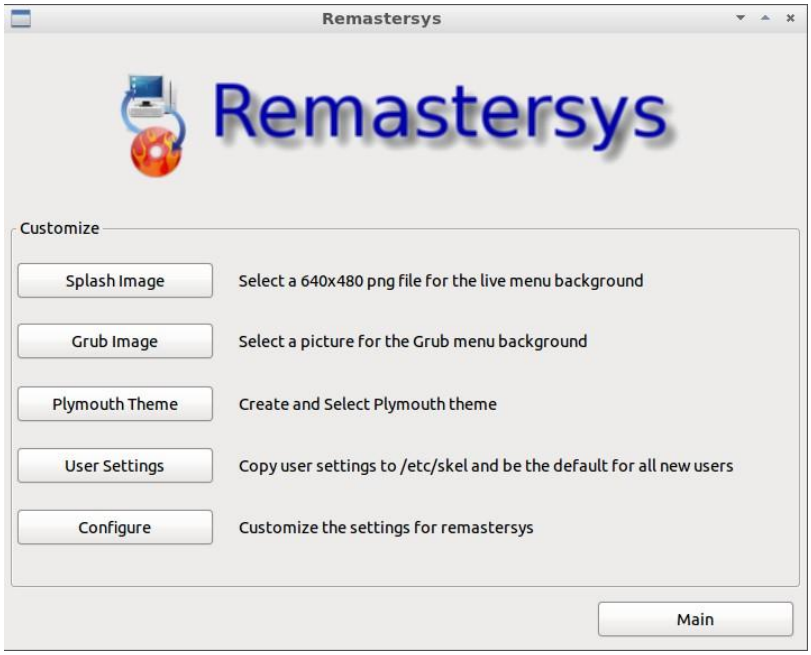
7. Creación del LiveCD

Una vez instalado el sistema operativo, las aplicaciones de la distribución, y realizada la personalización y optimización de la misma podemos crear el LiveCD. Para ello usaremos la herramienta Remastersys en modo gráfico. El procedimiento que seguiremos será:

Iniciaremos Remastersys. Una vez iniciada la herramienta se nos presentará la pantalla del GUI (Graphic User Interface), desde dónde realizaremos la configuración y la creación de la imagen del sistema.



Pulsando el botón "***Customize***" accederemos a la configuración de las opciones de la herramienta:



En esta pantalla inicial configuraremos:

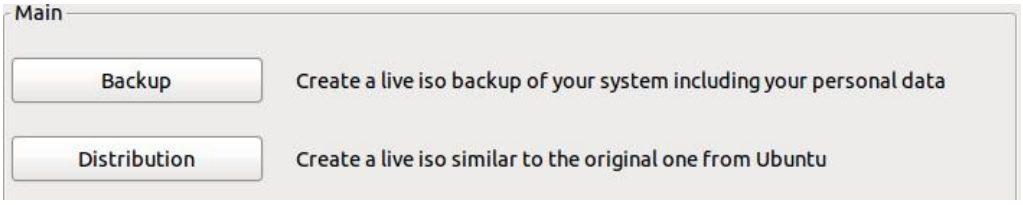
- **Splash Image**: la imagen del menú de arranque del LiveCD

- **Grub Image**: la imagen del menú de arranque para el sistema instalado (la que se usará en el caso de que se instale el LiveCD en disco duro)
- **User Settings**: el usuario del que tomaremos la configuración del escritorio, que será el usuario ipvisix.
- **Configure**: las opciones de creación del LiveCD

Si pulsamos el botón Configure, aparecerán las opciones de configuración para la creación del LiveCD.
Remastersys nos mostrará una pantalla como la que se presenta en la imagen siguiente:

Las opciones de creación del LiveCD que configuraremos serán:
- **Nombre de usuario**: escribiremos el nombre de usuario (en minúsculas) ipvisix
- **Etiqueta del CD**: Nombre del CD y texto que aparecerá en el menú de arranque del LiveCD.
- **Nombre de archivo**: nombre del archivo .ISO que crearemos

Una vez configurados estos parámetros pulsaremos el botón "***Save"*** para volver a la pantalla "***Customize"***, dónde pulsaremos el botón "***Main"*** para acceder a la pantalla inicial de la aplicación y lanzar la creación del LiveCD que se iniciará tras pulsar el botón "***Distribution"***



Una vez finalice el proceso en la carpeta **`/home/remastersys/remastersys`** dispondremos del fichero .iso con la imagen del sistema. Este fichero lo podemos usar para iniciar una máquina virtual con el hipervisor que elijamos (VmWare Player, Oracle VirtualBox, Quemu, KVM, etc..) y probar que todo funciona adecuadamente antes de grabarlo en un CDROM y obtener así el LiveCD.
Para grabar la imagen .iso en un soporte CDROM podremos usar la herramienta que consideremos oportuna, IpViSix no incluye ninguna de esas utilidades.

8. Escenarios de uso de la distribución

Los escenarios para los que se plantea el uso de la distribución son fundamental mente tres:

1. Aprendizaje y experimentación de las funcionalidades básicas de IpV6

2. Implementación de servicios básicos y de gestión de redes de IpV6 en entornos productivos.

3. Verificación del funcionamiento de aplicaciones en entornos IPv6 puros.

A continuación detallaremos loa casos de uso de cada uno de estos escenarios.

8.1 Escenario 1: Aprendizaje y experimentación de IpV6

Este escenario es el principal caso de uso de la distribución IpViSix y el que nos anima a implementarla. El objetivo es que se pueda disponer de una plataforma, con un esfuerzo mínimo para el estudiante, sobre la que se puedan estudiar, probar y analizar los fundamentos básicos de IpV6 desde un punto de vista práctico. Es decir, un laboratorio básico IpV6.

Para ello IpViSix ofrece un conjunto de herramientas que posibilitan:

- La generación de tráfico IpV6
- La captura y análisis de paquetes de red
- El análisis de puertos abiertos
- El estudio y configuración de servicios básicos de red como DNS
- El estudio y creación de planes de direccionamiento para redes IpV6

Además, y siguiendo el objetivo que ya se marcaba en la introducción de este mismo documento, este estudio se puede realizar en gran medida con herramientas que el estudiante del entorno de la Universitat Oberta de Catalunya es muy posible que conozca, ya que son herramientas que se usan en varias asignaturas impartidas en la Universidad en el ámbito de las TIC, con lo cual la curva de aprendizaje se reduce, al no ser necesario aprender nuevas herramientas como vehículo didáctico.
Para la realización de las tareas de este escenario no será necesario instalar la distribución, bastará con iniciar, bien un equipo hardware o bien una máquina virtual, con el LiveCD de IpViSix para disponer de una plataforma con todas las herramientas necesarias instaladas y configuradas.
Hay que hacer notar que el LiveCD con la distribución IpViSix (o el archivo .ISO equivalente) se ha probado sobre los siguientes hipervisores:

- Oracle VirtualBox versión 4.1.16
- VmWare Player versión 4.0.3

Ambos corriendo sobre un host Microsoft Windows 7 SP1 32 bits.
Los requisitos mínimos para la máquina virtual sobre la que se ejecutará la distribución son:

- Memoria: 1GB RAM
- Procesador: 1 Procesador virtual
- Red: Un adaptador de red preferiblemente configurado en modo “Bridged”, o en una red privada. Lo que importa realmente es que el adaptador de red

virtual se inicie correctamente para que todos los servicios de red arranquen sin problemas. No están soportados los adaptadores de red inalámbricos.

No hay requerimientos a nivel de disco duro ya que no es necesario instalar la plataforma, sólo iniciarla en modo LiveCD.

Una vez iniciado el LiveCD ya dispondremos de un servidor configurado según las configuraciones de red descritas en este documento.

8.1.1 Diseño del escenario

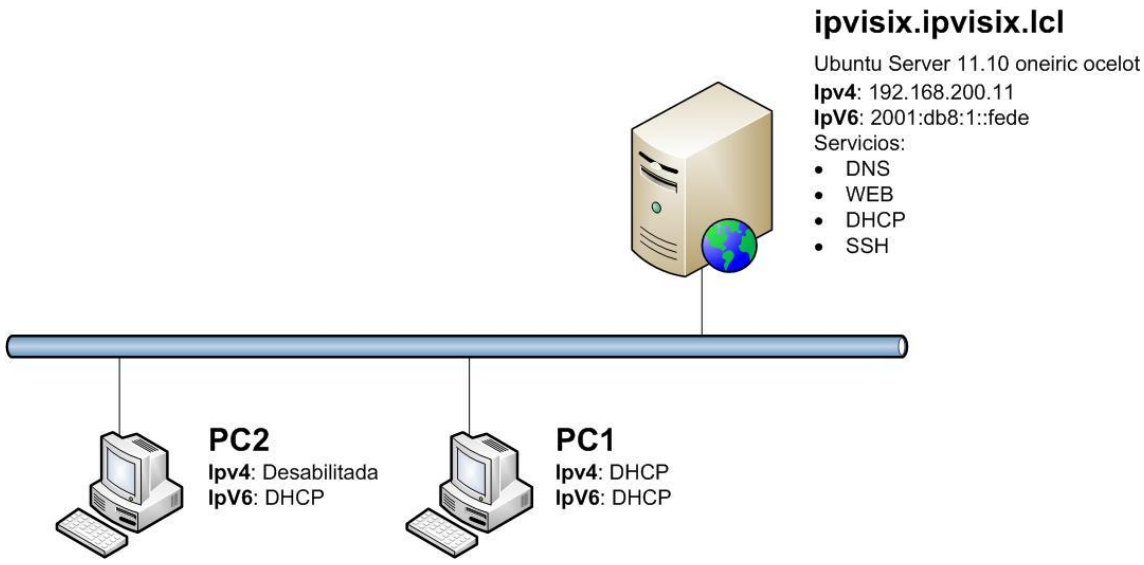
El diseño de este escenario es muy sencillo y puede tener dos variantes:

- Laboratorio con un único host
- Laboratorio con dos o más hosts

El primero de los escenarios es el más simple, ya que sólo consta del propio servidor Ipvisix. Usando las herramientas incluidas en el host atacaremos los servicios instalados en el propio host, para observar los resultados, realizar capturas de tráfico y poder analizar así los paquetes que genera este tráfico para poder estudiar las cabeceras, campos, secuencias, etc..

8.1.1.1 El esquema del laboratorio con dos o más hosts

El esquema para este escenario es el que se presenta en la siguiente imagen:



En la propuesta de laboratorio se aprecian los siguientes componentes:

- Servidor ipvisix.ipvisix.lcl
- PC1
- PC2

Estos tres hosts se conectan entre sí en el mismo segmento de LAN, para evitar configuraciones más complejas.

En el escenario se plantean dos host clientes (PC1 y PC2) pero bastaría con usar únicamente el configurado con doble pila TCP/IP e ir desactivando, según las pruebas a realizar, la pila TCP/IP v4 o la v6.

El sistema operativo de los host PC1 y PC2 es irrelevante, siempre que soporte le protocolo IpV6, por lo que no se especifica nada al respecto, no obstante en los ejemplos siguientes supondremos que son host que tienen instaladas una distribución desktop de GNU/Linux Ubuntu.

A continuación vamos a describir actividades o casos de uso para este escenario que nos pueden ayudar a comprender los fundamentos del protocolo IpV6 y su administración. No vamos a profundizar en los aspectos de configuración de los servicios DNS que ya se han descrito convenientemente en capítulos anteriores. Los casos de uso son válidos para las dos variantes del escenario, pero son más fáciles de entender y reproducir en la variante que contempla dos o más hosts.

8.1.2 Generación de tráfico IpV6.

La plataforma servidor IpViSix ofrece varios servicios de red contra los que se puede generar tráfico desde un cliente, e incluso desde el propio servidor. Así contra IpViSix podemos generar tráfico:

- DNS
- HTTP
- ICMP

Estos tráficos representan una variedad significativa de protocolos que podemos analizar.
Para generar cada uno de estos tráficos podemos usar las siguientes herramientas contra IpViSix:

DNS
El tráfico DNS puede ser tanto TCP como UDP hacia el puesto origen 53
Para generar este tipo de tráfico bastará con que ejecutemos consultas contra el servicio DNS instalado en el servidor. Para ello podemos usar el comando DIG

```
dig any ipv6.ipvisix.lcl @::1
```

Este comando obtiene todos los registros asociados al nombre ipv6.ipvisix.lcl contra la máquina local (::1).
En la siguiente captura de pantalla podremos observar el resultado del comando

```
ipvisix@ipvisix:~$ dig any ipv6.ipvisix.lcl @::1

; <<>> DiG 9.7.3 <<>> any ipv6.ipvisix.lcl @::1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59418
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;ipv6.ipvisix.lcl.              IN      ANY

;; ANSWER SECTION:
ipv6.ipvisix.lcl.       86400   IN      AAAA    2001:db8:1::fede

;; AUTHORITY SECTION:
ipvisix.lcl.            86400   IN      NS      ipvisix.ipvisix.lcl.

;; ADDITIONAL SECTION:
ipvisix.ipvisix.lcl.    86400   IN      A       192.168.200.11
ipvisix.ipvisix.lcl.    86400   IN      AAAA    2001:db8:1::fede

;; Query time: 59 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sat Jun  9 23:26:40 2012
;; MSG SIZE  rcvd: 128
```

HTTP
El tráfico HTTPS es TCP hacia el puerto origen 80 (por defecto). IpViSix tiene un listener para ese protocolo tanto para direccionamiento Ipv4 como Ipv6 y una aplicación que es capaz de discriminar que pila se ha usado en el origen del tráfico, así que bastará con abrir un navegador y, desde un host configurado con doble pila atacar a las url de la aplicación, que son:

- **`http://ipvx.ipvisix.lcl/index.php`** para verificar la pila por defecto del host cliente
- **`http://ipv4.ipvisix.lcl/index.php`** para verificar la pila Ipv4 del cliente
- **`http://ipv6.ipvisix.lcl/index.php`** para verificar la pila Ipv6 del cliente

ICMP

El tráfico ICMP se puede generar con utilidades como ping o tracert.
Si usamos ping podemos generar tanto tráfico IPv4 o IPv6.
Para generar tráfico IPv4 usaremos el comando:

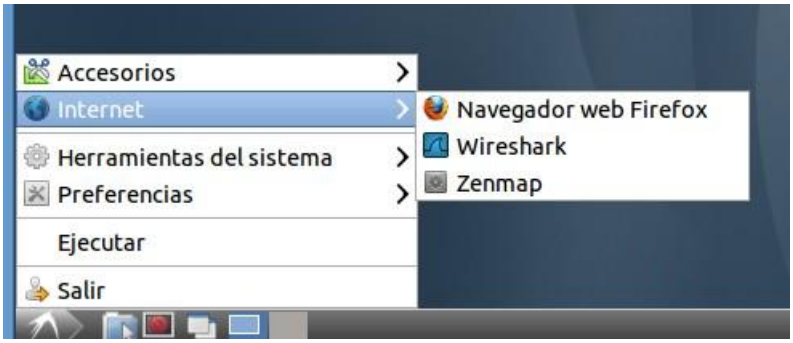
```
ping ipv4.ipvisix.lcl
```

Para generar tráfico IPv6 usaremos el comando:

```
ping6  ipv4.ipvisix.lcl
```

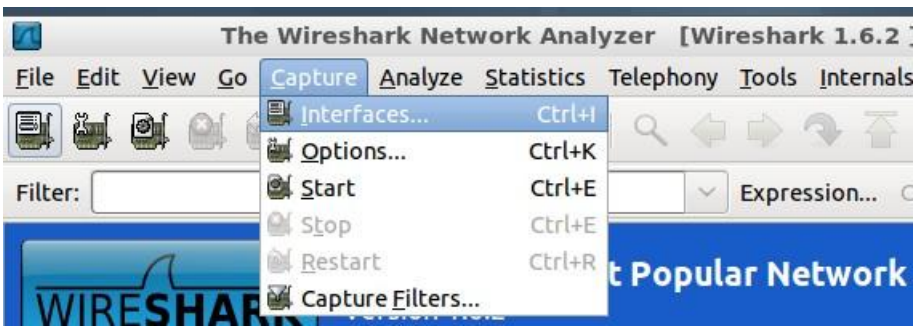
8.1.3 Captura y análisis de paquetes de red.

Para capturar el tráfico de red usaremos la herramienta Wireshark, incluida en la distribución.

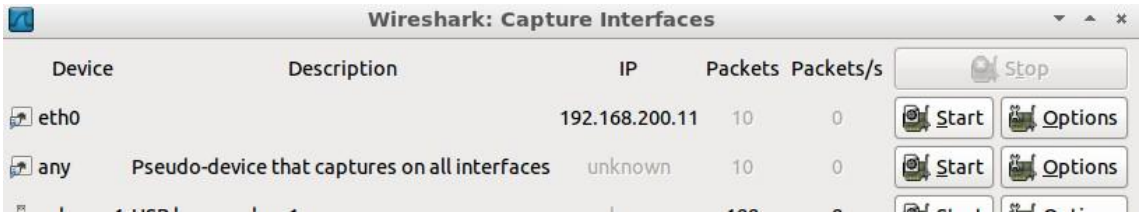


No obstante para realizar capturas de red necesitaremos ejecutar la utilidad con permisos de root, por lo que deberemos iniciar la herramienta desde una consola de terminal, ejecutando el comando **`sudo wireshark`**

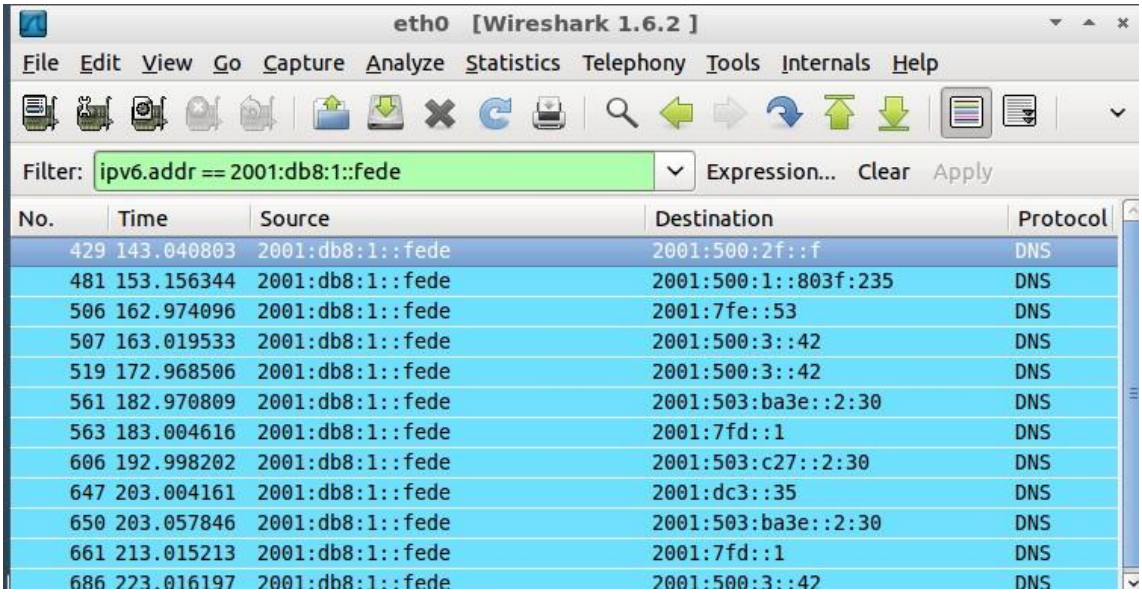
Una vez que la herramienta esté en ejecución deberemos seleccionar uno de los interfaces de red del servidor sobre el que hacer las capturas de red



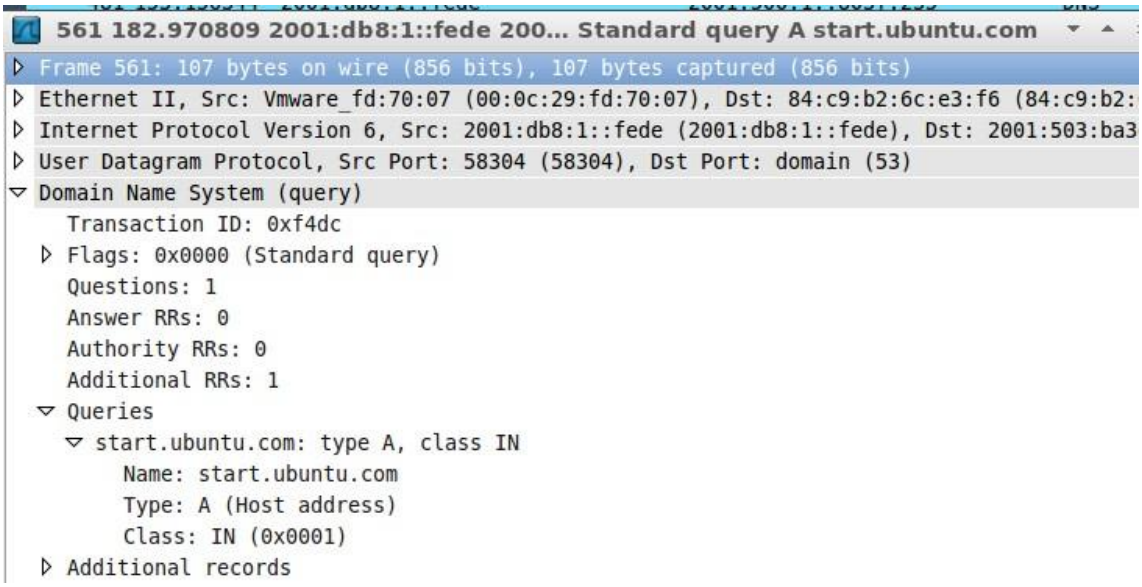
Wireshark nos mostrará una lista de los interfaces disponibles para la captura de tráfico.



Pulsaremos sobre el botón "***Start***" en el interfaz que nos interese, en este caso el interfaz eth0 y comenzará la captura de paquetes de red.
En el ejemplo hemos generado tráfico DNS con origen ipvisix y como podemos apreciar en la imagen se han capturado varios paquetes.



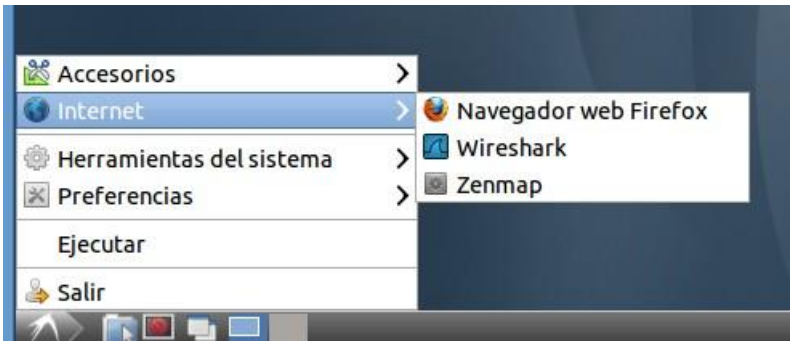
Haciendo doble clic sobre cualquiera de ellos podríamos analizar su contenido.



En este caso se trata de una consulta DNS para la obtención de la IP de la máquina start.ubuntu.com

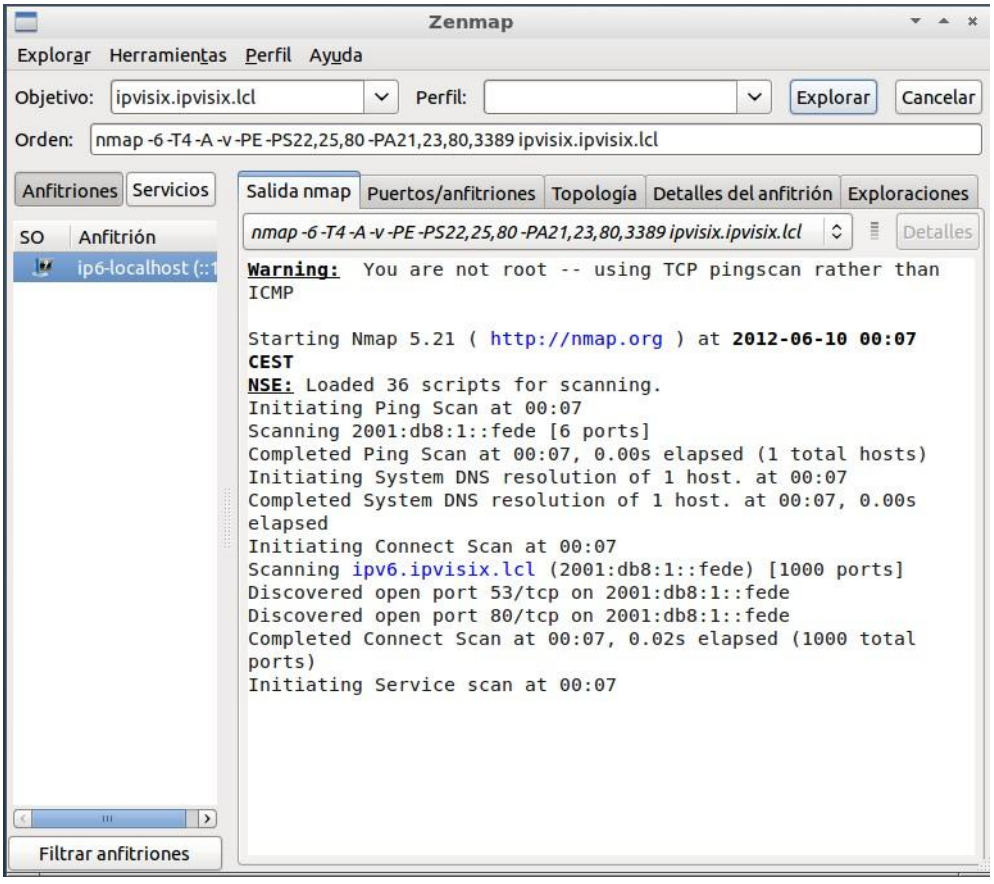
8.1.4 Análisis de puertos abiertos.

ZenMap es en interfaz gráfico de la herramienta de seguridad Nmap. Esta herramienta es muy útil en escenarios de descubrimiento de servicios de red publicados y vulnerabilidades en host. Para iniciar la herramienta podemos usar el icono en el menú de arranque

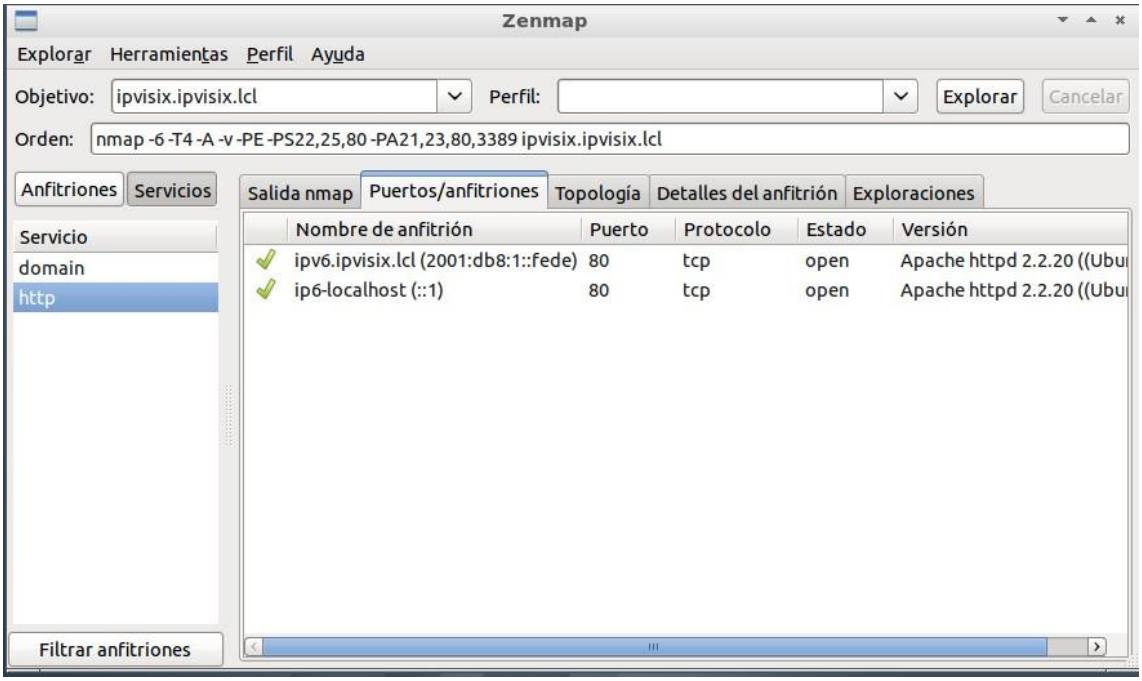


También podemos iniciar la herramienta con permisos de administrador ejecutando el comando **`sudo zenmap`** desde una consola de terminal. Se abrirá el interfaz de Zenmap.

Si seleccionamos un objetivo para el escaneo, por ejemplo el host **`ipvisix.ipvisix.lcl`** y unos parámetros para el descubrimiento y pulsamos el botón "***Explorar***", Nmap comenzará el escaneo de puertos, según las opciones seleccionadas.
En las siguientes capturas de pantalla se puede apreciar un escaneo de ejemplo del host **`ipvisix.ipvisix.lcl`**.



Al finalizar el escaneo Zenmap nos devolverá la información obtenida. En este caso nos muestra los servicios publicados por el servidor para la pila IPv6.



Para más información sobre las opciones de escaneo de Nmap podemos consultar la web de los desarrolladores en [14].

8.1.5 Estudio y configuración de servicios básicos de red.

Con esta distribución se incluye uno los servicios básicos de red en cualquier entorno TCP/IP: DNS como sistema de resolución de nombres de Host.
Esta característica nos da la oportunidad de poder estudiar con detenimiento este servicio en un entorno IpV6 puro o de doble pila IPv6 IPv4.
El demonio DNS que se incluyen (Bind9) está muy extendido y bien documentado, por lo que será fácil reutilizar el conocimiento que se alcance en el mundo real.
Para la gestión de este servicio no se ha incluido, de forma intencionada, ninguna herramienta gráfica.
En capítulos anteriores de este documento se detalla la configuración de éste servicio realizada en la distribución, por lo que, como indicábamos anteriormente no profundizaremos más en ello.

8.1.6 Creación de planes y administración del direccionamiento para redes IpV6

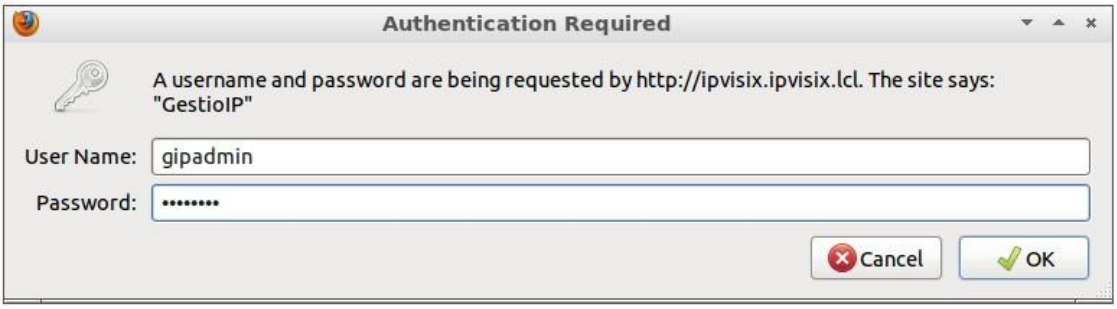
Una de las facetas más importantes de la gestión de una red es el diseño del direccionamiento de la misma y la posterior gestión del mismo. En redes pequeñas estas tareas no presentan demasiada complejidad, especialmente en un entorno IpV4, pero en redes medianas y grandes conviene disponer de un mecanismo que nos ayude en estas tareas. Aquí es donde entra en juego la aplicación GestióIp.

En este apartado veremos algunas de las opciones más interesantes de las muchas que ofrece y no pretende ser una guía exhaustiva de la aplicación, por lo que para tener un detalle mayor de las operaciones deberemos acudir a los manuales de operación de la aplicación escritos por el desarrollador de la herramienta, que están disponibles en formato .pdf.

Las operaciones que veremos son:

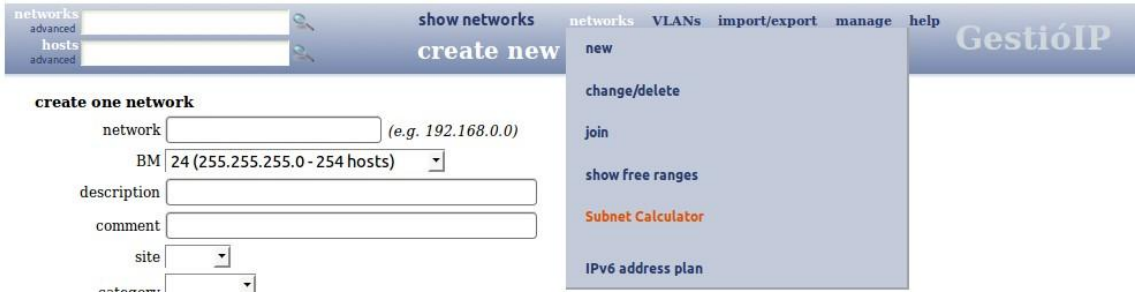
- Uso de la calculadora de redes
- Crear un plan de direccionamiento y las redes que se definan

Lo primero que deberemos hacer el acceder a la herramienta y logarnos en ella.
En el navegador introduciremos la url ***http://ipvisix.ipvisix.lcl/gestioip***.
Para iniciar sesión usaremos las credenciales siguientes:
Usuario: gipadmin
Password: gipadmin

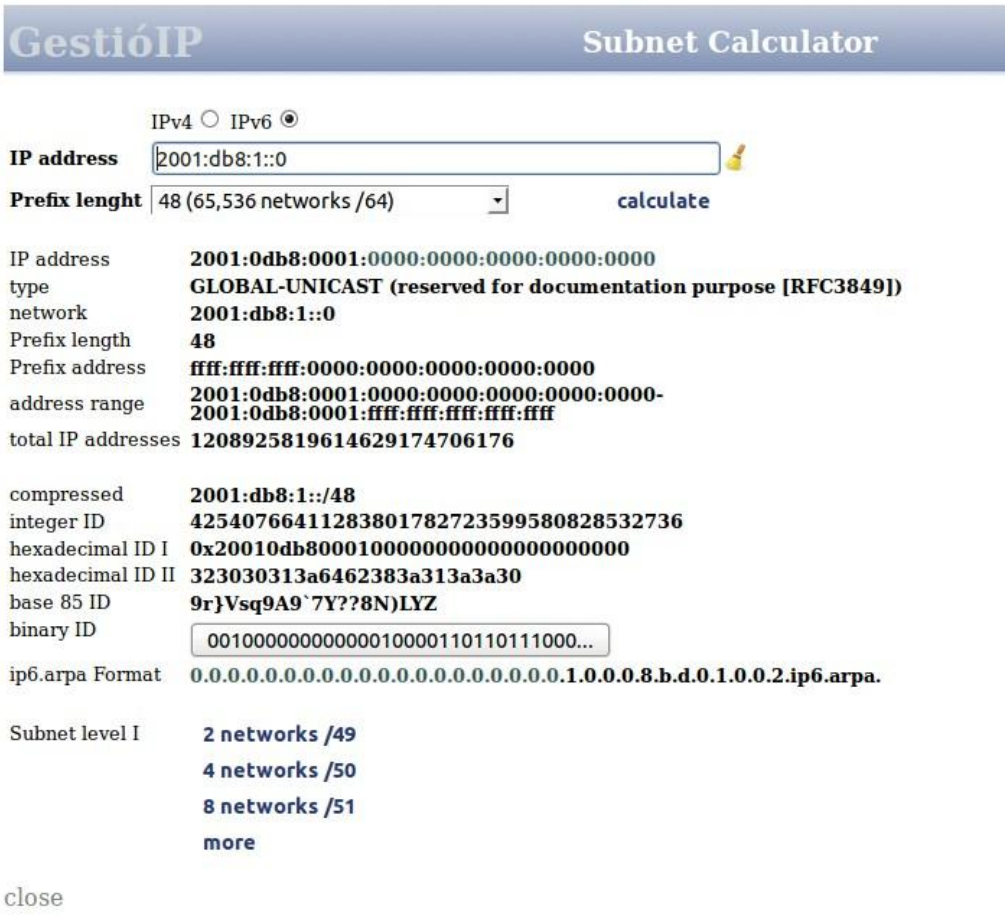


Una vez que tenemos acceso a la herramienta ya podemos trabajar con ella.

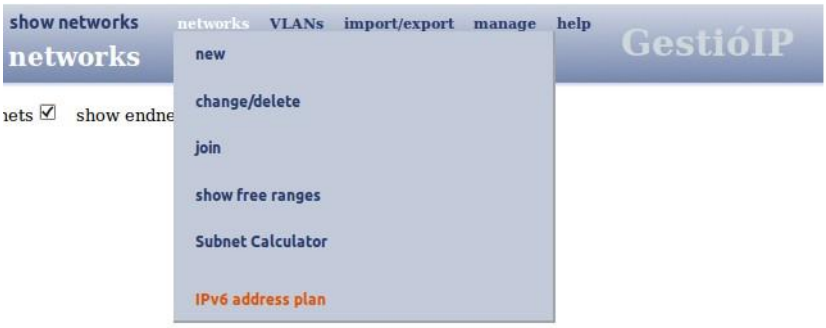
El primer ejemplo será el uso de la calculadora de redes.
Para iniciarla iremos al menú "***Networks"*** y seleccionaremos "***Subnet Calculator***"



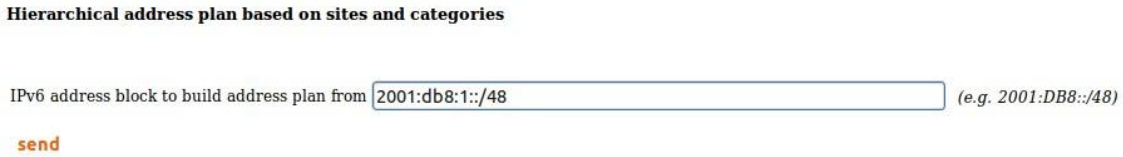
Se abrirá el interfaz de la calculadora. Si queremos estimar cómo segmentar la red IPv6 2001:db8:1::0/48 , seleccionaremos el tipo de red Ipv6, en el campo "***Ip Address*** " escribiremos la dirección de la red y en el campo "***Prefix lenght"*** el tamaño del perfil, tras lo cual pulsaremos el botón "***Calculate***".
La calculadora nos devolverá la información solicitada, como se puede apreciar en la captura de pantalla.



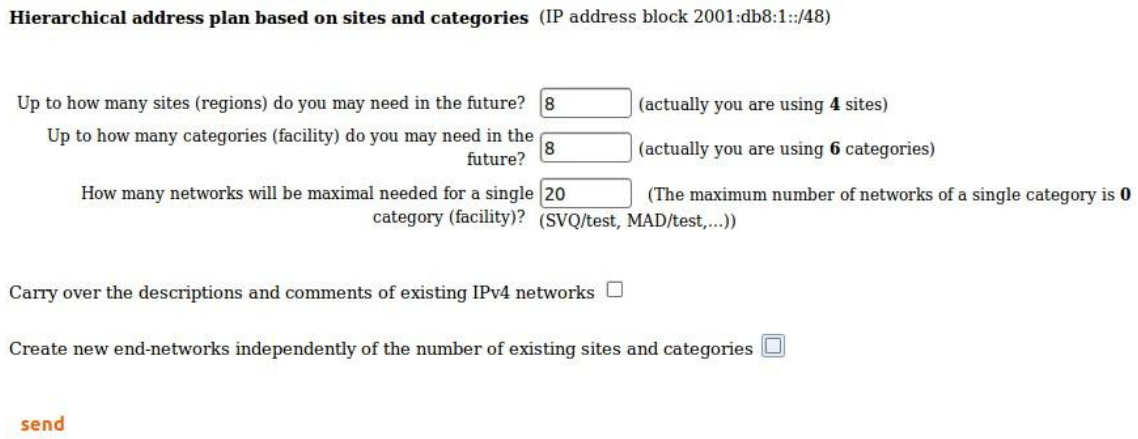
El plan de direccionamiento que crearemos será un plan jerárquico, es decir dividiremos el rango que tengamos asignado (en este ejemplo el 2001:db8:1::/48) en cuatro sedes distintas (Barcelona, Madrid, Sevilla y Pamplona) y dentro de cada sede segmentaremos la red en zonas. GestióIp nos propondrá direccionamientos para cada red y creará las redes. Para comenzar el plan de direccionamiento iremos al menú Networks, opción IPv6 Address plan.



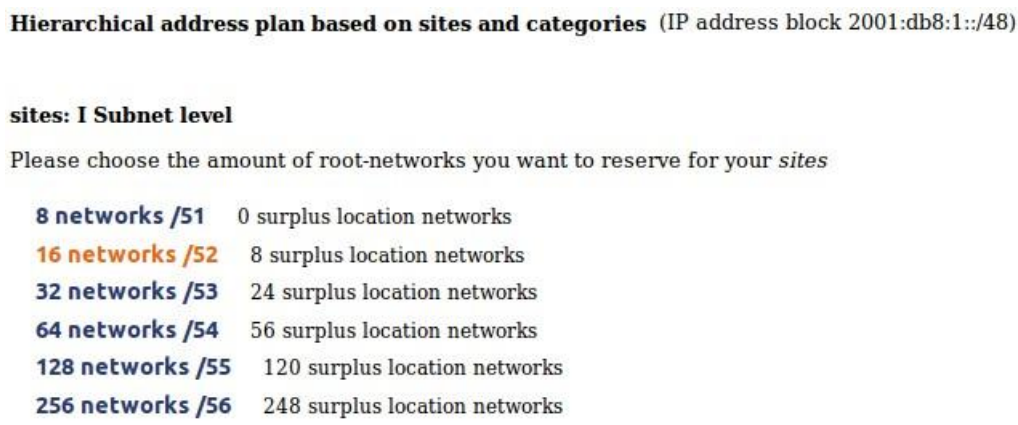
Insertaremos el rango de direcciones que tengamos asignado a nuestra red (2001:db8:1::/48).



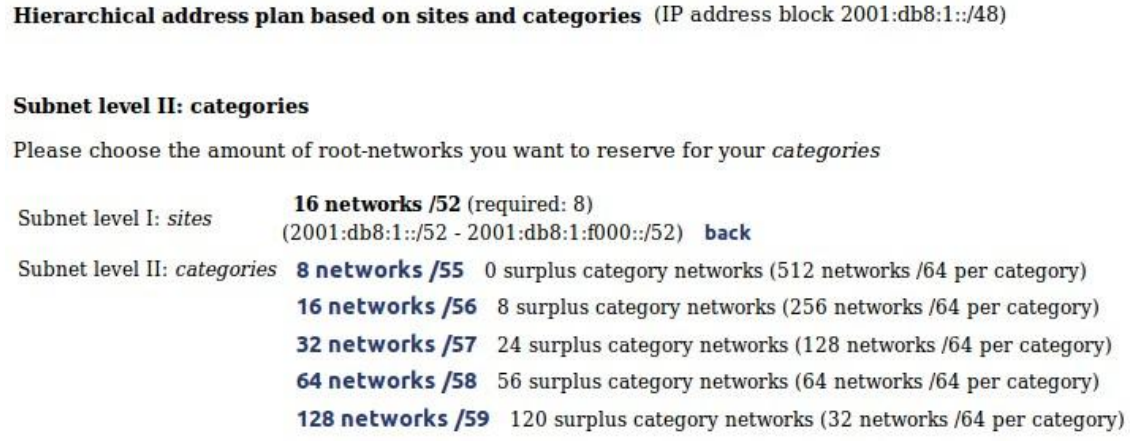
Pulsaremos el botón "***Send***" e indicaremos el número de ubicaciones y de redes que usaremos en nuestra organización.



Pulsaremos el botón "***Send***". En la siguiente pantalla introduciremos el número de localizaciones que deseamos dejar de reserva, para futuras ampliaciones. La selección la haremos haciendo clic sobre el enlace del número de redes de reserva deseado.



En el siguiente paso seleccionaremos el número de redes en cada ubicación, en nuestro ejemplo seleccionaremos 16.



GestióIP nos mostrará un resumen de las selecciones realizadas

Hierarchical address plan based on sites and categories (IP address block 2001:db8:1::/48)

Please click "send" to show the address plan

Subnet level I: *sites*	**16 networks /52** (required: 8) (2001:db8:1::/52 - 2001:db8:1:f000::/52)
Subnet level II: *categories*	**16 networks /56** (required: 8) (2001:db8:1::/56 - 2001:db8:1:ff00::/56)
Subnet level III: *end-networks per category*	**256 networks /64** (required: 20) (2001:db8:1::/64 - 2001:db8:1:ffff::/64) back

send

Si estamos conformes pulsaremos el botón "**Send**", la aplicación nos mostrará las redes a crear en función de las ubicaciones y tipos de redes configuradas. En esta pantalla podemos asignar descripciones a cada red que se va a crear.

SVQ - dev-test

IP address	prefix length	description	site	category	comment
2001:0db8:0001:7200:0000:0000:0000:0000	56	Q pruebas dispositivos especiales	SVQ	dev-test	

no networks

SVQ - pre

IP address	prefix length	description	site	category	comment
2001:0db8:0001:7300:0000:0000:0000:0000	56	SVQ pre-producción	SVQ	pre	

no networks

SVQ - prod

IP address	prefix length	description	site	category	comment
2001:0db8:0001:7400:0000:0000:0000:0000	56	SVQ producción	SVQ	prod	

no networks

SVQ - test

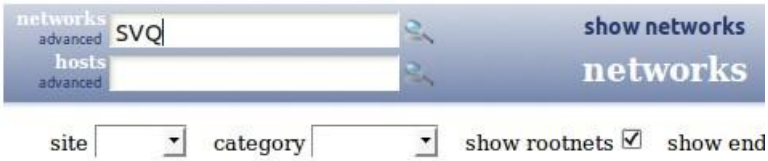
IP address	prefix length	description	site	category	comment
2001:0db8:0001:7500:0000:0000:0000:0000	56	SVQ pruebas	SVQ	test	

no networks

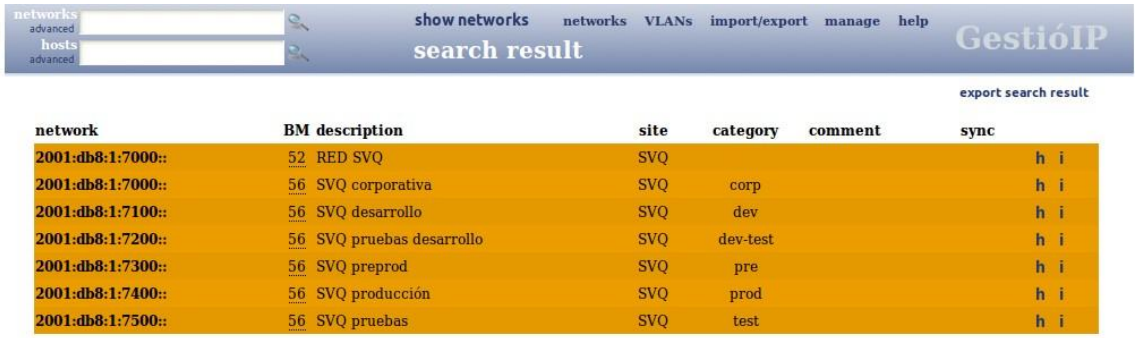
insert export

Una vez asignadas las descripciones y comentarios para cada red, que es muy útil para las documentaciones de las redes, pulsaremos el botón "***Insert***" y la aplicación creará las redes definidas.

Para ver las redes creadas, en una de las ubicaciones, por ejemplo Sevilla (SVQ) iremos a la herramienta de búsqueda y en el campo Search networks escribiremos SVQ y pulsaremos el botón de búsqueda



La aplicación nos mostrará las redes creadas para esa ubicación.



network	BM	description	site	category	comment	sync
2001:db8:1:7000::	52	RED SVQ	SVQ			h i
2001:db8:1:7000::	56	SVQ corporativa	SVQ	corp		h i
2001:db8:1:7100::	56	SVQ desarrollo	SVQ	dev		h i
2001:db8:1:7200::	56	SVQ pruebas desarrollo	SVQ	dev-test		h i
2001:db8:1:7300::	56	SVQ preprod	SVQ	pre		h i
2001:db8:1:7400::	56	SVQ producción	SVQ	prod		h i
2001:db8:1:7500::	56	SVQ pruebas	SVQ	test		h i

Con lo que sólo nos restaría agregar hosts a cada red, que podemos hacerlo de forma automática con las funcionalidades de la propia herramienta.
Para realizar más operaciones con la herramienta podemos consultar los manuales de la aplicación, disponibles en línea [15] y en la propia distribución (/home/ipvisix/documentos).

8.2 Escenario 2: Implementación de servicios básicos de red

El segundo caso de uso o escenario para el que podemos usar la distribución IpViSix es como servidor ya preparado para ofrecer los servicios básicos de red (resolución de nombres con DNS) para una red IpV6 pura, que se puede instalar tanto en un entorno de laboratorio como en un entorno productivo.
Además de estos servicios básicos de red la distribución nos ofrece una herramienta para gestión de los direccionamientos con capacidad de descubrimiento de hosts y redes a través de SNMP, como es GestióIp y dos herramientas básicas de análisis de red como son Wireshark y el binomio Nmap – Zenmap.

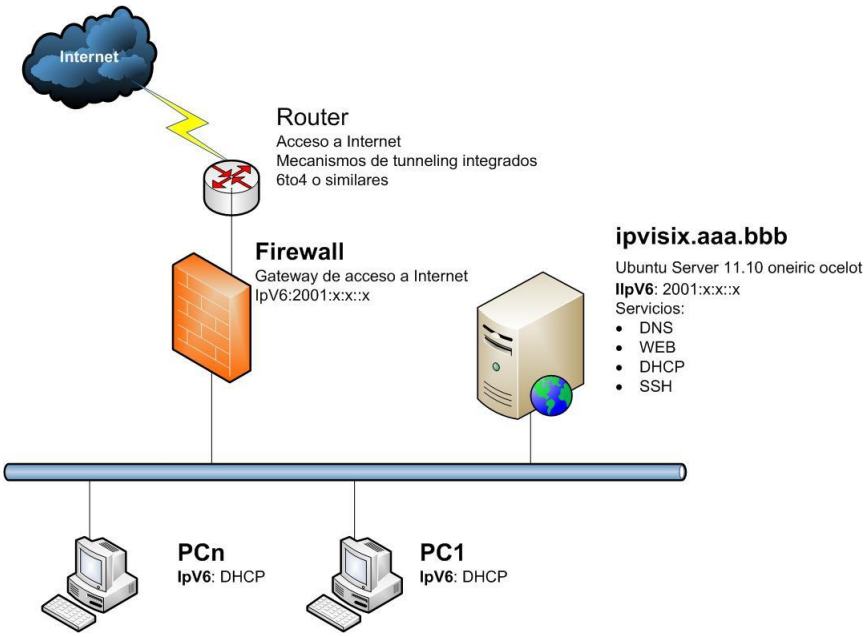
Antes de continuar con la descripción de este escenario es necesario tener en cuenta dos consideraciones importantes, una acerca de la seguridad y la otra respecto a la configuración de red.

Respecto a la seguridad.
Es importante recordar que todos los usuarios que usa la distribución (la cuenta de servicio de MySQL, los usuarios operadores de GestióIp, las credenciales que usa GestióIp para acceso a MySQL y el propio usuario definido en la distribución "usuario IpViSix") presentan unas políticas de seguridad bastante débiles, en cuanto a la configuración de contraseñas de esos usuarios y que además esas cuentas y contraseñas están publicadas en este documento, por lo que, de alguna manera, ya son públicas. Esto, desde el punto de vista de la seguridad es inaceptable, y antes de instalar una plataforma con esta distribución en un entorno productivo es necesario cambiar estas contraseñas y usuarios por otros a los que se apliquen políticas de seguridad más fuertes y acordes con el entorno dónde se vaya a instalar la plataforma.
Si esta plataforma se instala en un entorno controlado de laboratorio, queda a elección del usuario el endurecer o no las políticas de seguridad aplicadas a las cuantas de usuario que incluye la distribución.

Respecto a la configuración de red.
Es necesario recordar también que, por defecto, la plataforma se ha configurado para que use un rango de direcciones Ipv6 reservado para tareas de documentación, y por lo tanto no válido fuera de un entorno aislado de laboratorio. De esta forma será necesario reconfigurar el direccionamiento de red de la plataforma y de las aplicaciones, con direccionamientos IpV6 válidos que nos hayan sido asignados por la organización que nos provea del acceso a Internet, de hecho en el espacio de direcciones IpV6 no existen rangos privados dedicados, tal y como existían en IpV4, si no que todos los rangos (a excepción del reservado para documentación) son rangos públicos.

8.2.1 Descripción del escenario.

Este escenario pudiese tener sentido en redes pequeñas en las que se precise un ejemplo ya realizado de configuración de servicios básicos de red. Se aprovecharían las capacidades de instalación del LiveCD para instalar el servidor en una plataforma hardware o entorno virtualizado. El esquema de instalación se detalla en la siguiente imagen:



Se debería tener asignado un rango de direccionamiento IpV6 para configurar la red.
En este escenario sería necesario, además de reconfigurar la red del servidor IpViSix y tener en cuenta las recomendaciones previas sobre seguridad y configuración de red, reconfigurar los siguientes servicios:

DNS
Sería necesario:

- Reflejar la nuevas direcciones Ip de los hosts de la red
- Configurar los servidores forwarders para la resolución de nombres DNS en internet

8.3 Escenario 3: Verificación de aplicaciones

El tercer escenario es el relacionado con la verificación de las aplicaciones en un entorno IpV6 puro.
IpViSix es, en el fondo, un servidor de aplicaciones LAMP, que son las siglas de:

- Linux
- Apache
- MySQL
- PHP

Esto quiere decir que tenemos un servidor básico de aplicaciones con soporte completo IpV6 sobre el que podríamos instalar y configurar las aplicaciones que deseemos probar en un entorno controlado de red.

Si usamos el LiveCD para instalar la distribución sobre una plataforma hardware o sobre una máquina virtual, podríamos añadir los componentes necesarios para hacer funcionar una aplicación cliente servidor.
Una vez instalada la aplicación a probar se puede deshabilitar la pila IpV4 del servidor IpViSix y hacer funcionar todos los servicios en un entorno de pila única IpV6. Además podremos instalar, siguiendo la variante segunda del primer escenario, hosts adicionales y utilizarlos como clientes de la aplicación.

Es cierto que el rango de aplicaciones que podrían probarse quizá no sea muy elevado, por los componentes básicos que se incluyen en la distribución, pero también es cierto que esos componentes se pueden ampliar según las necesidades de la aplicación y que la distribución incluye herramientas de análisis de tráfico de red y escaneo de puertos que pueden ser útiles a la hora de diagnosticar los posibles problemas de una aplicación en entorno IpV6 Puro.

Hay una limitación que se debe tener en cuenta, y es que si se utiliza IpViSix tal y cómo está configurado por defecto, sólo es útil en un entorno de laboratorio y que la plataforma no puede acceder a Internet. En el caso que fuese necesario este acceso deberíamos reconfigurar la plataforma IpViSix para adaptarla a los direccionamientos y requisitos de la red.

9. Bibliografía

[1] HUSTON, Geoff. "IPv4 Address Report" [en línea]. Se actualiza automáticamente. URL: http://www.potaroo.net/tools/ipv4/index.html.[Consulta: 8 de junio de 2012]

[2] DistroWatch.com. "DistroWatch Page hit Ranking" [en línea]. Se actualiza diariamente. URL: http://distrowatch.com/dwres.php?resource=popularity. [Consulta: 5 de Abril de 2012].

[3] WIKIPEDIA. "Linux distribution" [en línea]. Última actualización 8 de mayo de 2012, 9:40. URL: http://en.wikipedia.org/wiki/Linux_distribution .[Consulta: 8 de mayo de 2012].

[4] LUBUNTU.NET."Lubuntu simplify your computer".[en línea]. URL: http://lubuntu.net/ .[Consulta: 2 de abril de 2012].

[5] KRAAI, Matt. "UBUNTU manuals". [en línea].
URL: http://manpages.ubuntu.com/manpages/lucid/man8/debootstrap.8.html.
[Consulta: 9 de abril de 2012].

[6] MURIANA, Francesco. "Ubuntu-builder. A handy tool to build an Ubuntu based GNU/Linux distribution" [en línea]. URL:http://code.google.com/p/ubuntu-builder/ [Consulta: 10 de abril de 2012].

[7] BRIJESKI, Tony. "Remastersys. A Unique Linux Backup to Live Media Tool for Debian and Ubuntu" [en línea]. URL: http://www.remastersys.com/ubuntu.html [Consulta: 10 de abril de 2012].

[8] IpPlan."IP addresses managing and tracking" [en línea]. URL: http://iptrack.sourceforge.net/ [Consultado: 12 de abril de 2012].

[9]OpenNet Admin. "Track. Automate. Configure" [en línea]. URL: http://opennetadmin.com/ [Consulta: 13 de abril de 2012].

[10]UEBEL, Marck. "GestióIP. IP address management (IPAM) software" [en línea]. Última actualización: 9 de mayo de 2012. URL: http://www.gestioip.net [Consulta: 14 de abril de 2012]

[11]INFOBLOX. Inc. "Free IPAM software".[en línea] URL: http://www.infoblox.com/en/landing/ipam-freeware.html .[Consulta: 14 de mayo de 2012]

[12]WIRESHARK Fundation. Wireshark. [en línea] URL: http://www.wireshark.org/

[Consulta: 20 de abril de 2012]

[13] LYON, Gordon (Fyodor). "Nmap Security Scanner"[en línea] URL: http://nmap.org/ [Consulta: 8 de junio de 2012]

[14] LYON, Gordon (Fyodor). "Zenmap. Official Nmap Security Scanner GUI"[en línea] URL: http://nmap.org/zenmap/ [Consulta: 8 de junio de 2012]

[15] UEBEL, Marck. "GestióIP. IP address management (IPAM) software usage guide" [en línea]. Última actualización: 9 de mayo de 2012. URL: http://www.gestioip.net/docu/Documentacion_GestioIP_30_en.pdf .[Consulta: 9 de junio de 2012]