UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD:

CIENCIAS DEL HOMBRE Y LA NATURALEZA

CARRERA:

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

TEMA:

INTRANET CON SERVICIOS DE DHCP, DNS, LDAP, WEB Y PROXY WEB, FIREWALL,

INTEGRANTES:

N°	APELLIDOS, NOMBRES	CARNET
1	MONTECINOS SEGOVIA, JOSÉ LUIS	MS01121287
2	SERRANO MENJIVAR, WILBER JAVIER	SM02110153

ASIGNATURA:

ESPECIALIZACIÓN ADMINISTRACIÓN DE SERVIDORES 2017

CATEDRÁTICO/A:

ING. MANUEL DE JESÚS FLORES VILLATORO

FECHA DE ENTREGA: Sábado 20, de enero del 2018

INDICE

INTRODUCCIÓN.

A lo largo de nuestro proyecto se da a conocer una configuración de distintos servidores para una red intranet como herramienta y dispositivos tecnológicos referentes al área de informática comúnmente aparecen redes en donde la información es privada para el correcto funcionamiento de las empresas, instituciones, centros de informática, se debe tener al menos los servidores básicos más útiles y necesarios en una Intranet tanto que como estudiantes de la Universidad Luterana Salvadoreña consideramos realizar este proyecto de investigación y echando en marcha los conocimientos adquiridos en la carrera de Licenciatura en Ciencias de la Computación de la facultad de Ciencias del Hombre y la Naturaleza

En el presente documento se muestra el uso y correcto funcionamiento en una Red Intranet la instalación y configuración correspondientes de los diferentes tipos de servidores DHCP, DNS, FIREWALLS, PROXY WEB Y LDAP. Se detallan los procedimientos y pasos a seguir para lograr dicho propósito a demas surge la necesidad de realizar este proyecto como actividad final en la especialización de servidores linux.

OBJETIVOS

GENERAL:

- Aprender el manejo y funcionamiento específicamente para la instalación y configuración de los diferentes servidores, DHCP, DNS, PROXY WEB, CORTAFUEGOS Y LDAP. Dando a conocer sus funciones, así como también aprender la administración y manejo de este ámbito a fin de incrementar la productividad y eficiencia en las diferentes funciones que puedan ser útiles para los clientes que estén conectados a dicha red.

ESPECÍFICOS:

- Lograr un fácil uso y configuración de los servidores en una Intranet por parte del administrador de sistema.
- Automatizar los servicios que una Intranet debe tener.
- aplicar los conocimientos adquiridos durante la especialización.

DESCRIPCIÓN DEL PROYECTO.

Nombre del proyecto

INTRANET CON SERVICIOS DE FIREWALL, DHCP, DNS, LDAP, WEB Y PROXY WEB

Problemática o necesidad a cubrir por el proyecto en la Universidad Luterana Salvadoreña se vio la necesidad de investigar y configurar los servidores básicos para una red local(intranet) como proyecto final de la carrera licenciatura en ciencias de la computación. Surge la necesidad de mejorar las prestaciones de la conexión en una misma red, siendo como objetivos principales poder garantizar el conocimiento en como funcionan dichos servidores en una misma red, a la misma vez ser capaces de instalarlos y configurarlos

MARCO TEÓRICO.

La Intranet se refiere a una red interna(local) de una organización, institución o empresa con estándares basados en Internet, en la que las computadoras se encuentran conectadas o mas bien haciendo uso de diferentes servicios(servidores),para resolver tareas cotidianas del quehacer laboral o empresarial dependiendo del lugar, dado a conocer esto nosotros como estudiantes de la carrera de Licenciatura en ciencias de la computación de la Universidad Luterana Salvadoreña (ULS) y cursando la especialización de Administración de Servidores GNU/Linux sabemos que es preciso obtener y aplicar el conocimiento adquirido durante dicho curso es por ello que decidimos tomar el proyecto de INTRANET CON SERVICIOS DE FIREWALL, DHCP, DNS, LDAP, WEB Y PROXY WEB, y con el desarrollar los servicios básicos con los que debe contar una INTRANET.

SERVIDOR DHCP.

¿Qué es el DHCP?

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Si disponemos de un servidor DHCP, la configuración IP de los PCs puede hacerse de forma automática, evitando así la necesidad de tener que realizar manualmente uno por uno la configuración TCP/IP de cada equipo.

Un servidor DHCP es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los clientes autoconfigurar. Para que un PC solicite la configuración a un servidor, en la configuración de red de los PCs hay que seleccionar la opción 'Obtener dirección IP automáticamente'.

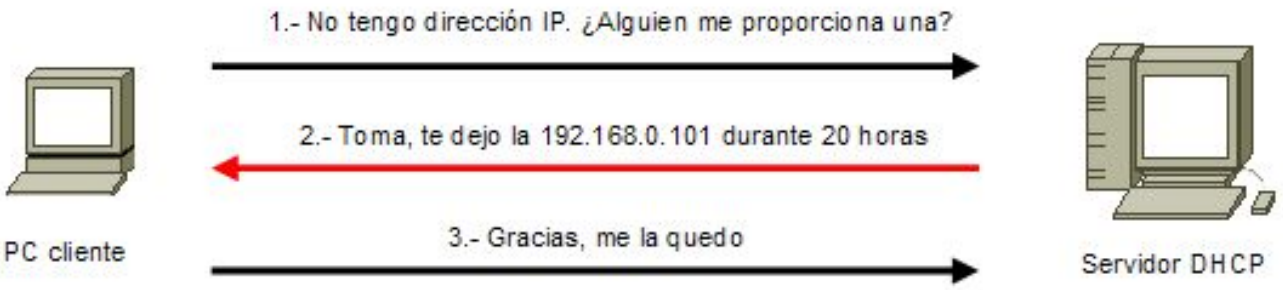
El servidor proporcionará al cliente al menos los siguientes parámetros:

- Dirección IP
- Máscara de subred

Opcionalmente, el servidor DHCP podrá proporcionar otros parámetros de configuración tales como:

- Puerta de enlace
- Servidores DNS
- Muchos otros parámetros más

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red.



Funcionamiento de una petición DHCP

El servidor solo asigna direcciones dentro de un rango prefijado. Si por error hemos configurado manualmente una IP estática perteneciente al rango gestionado por nuestro servidor DHCP, podría ocurrir que dicha dirección sea asignada dinámicamente a otro PC, provocándose un conflicto de IP. En ese caso el cliente solicitará y comprobará, otra dirección IP, hasta que obtenga una dirección IP que no esté asignada actualmente a ningún otro equipo de nuestra red.

La primera vez que seleccionamos en un PC que su configuración IP se determine por DHCP, éste pasará a convertirse en un cliente DHCP e intentará localizar un servidor DHCP para obtener una configuración desde el mismo. Si no encuentra ningún servidor DHCP, el cliente no podrá disponer de dirección IP y por lo tanto no podrá comunicarse con la red. Si el cliente encuentra un servidor DHCP, éste le proporcionará, para un periodo predeterminado, una configuración IP que le permitirá comunicarse con la red. Cuando haya transcurrido el 50% del periodo, el cliente solicitará una renovación del mismo.

Cuando arrancamos de nuevo un PC cuya configuración IP se determina por DHCP, pueden darse dos situaciones:

- Si la concesión de alquiler de licencia ha caducado, el cliente solicitará una nueva licencia al servidor DHCP (la asignación del servidor podría o no, coincidir con la anterior).
- Si la concesión de alquiler no ha caducado en el momento del inicio, el cliente intentará renovar su concesión en el servidor DHCP, es decir, que le sea asignada la misma dirección IP.

Antes de comenzar con los procesos de instalación y configuración de nuestro servidor DHCP, vamos a definir algunos términos que utilizaremos a lo largo de dicho proceso.

Ámbito servidor DHCP: Un ámbito es un agrupamiento administrativo de equipos o clientes de una subred que utilizan el servicio DHCP

Rango servidor DHCP: Un rango de DHCP está definido por un grupo de direcciones IP en una subred determinada, como por ejemplo de 192.168.0.1 a 192.168.0.254, que el servidor DHCP puede conceder a los clientes.

Concesión o alquiler de direcciones: es un período de tiempo que los servidores DHCP especifican, durante el cual un equipo cliente puede utilizar una dirección IP asignada.

Reserva de direcciones IP: Consiste en reservar algunas direcciones IP para asignarlas siempre a los mismos PCs clientes de forma que cada uno siempre reciba la misma dirección IP. Se suele utilizar para asignar a servidores o PCs concretos la misma dirección siempre. Es similar a configurar una dirección IP estática pero de forma automática desde el servidor DHCP. En el servidor se asocian direcciones MAC a direcciones IP. Es una opción muy interesante para asignar a ciertos PCs (servidores, impresoras de red, PCs especiales...) siempre la misma IP.[1]

[1] "Servidor DHCP y Servidor DNS | Redes Linux."
http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/index.html. Se consultó el 11 dic.. 2017.

SERVIDOR DNS.

¿Qué es un servidor DNS?

Un servidor DNS (Domain Name System - Sistema de nombres de dominio) es un servidor que traduce nombres de dominio a IPs y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PCs. Es equivalente a las redes de telefonía en las que cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.

Trabajar con direcciones IP es incómodo para las personas, ya que requeriría conocer en todo momento las direcciones IP de los equipos a los que queremos conectarnos. En su lugar utilizamos nombres de dominio que son más fáciles de recordar y utilizar como por ejemplo www.google.es, www.educacion.gob.es, etc...

Cada equipo y cada servidor conectado a Internet, dispone de una dirección IP y de un nombre perteneciente a un dominio. Internamente, la comunicación entre los PCs se realiza utilizando direcciones IP por eso es necesario algún sistema que permita, a partir de los nombres de los PCs, averiguar las direcciones IPs de los mismos. Ejemplo, cuando queremos acceder a la página web del Ministerio de Educación, en la barra de direcciones del navegador escribimos:
http://www.educacion.gob.es

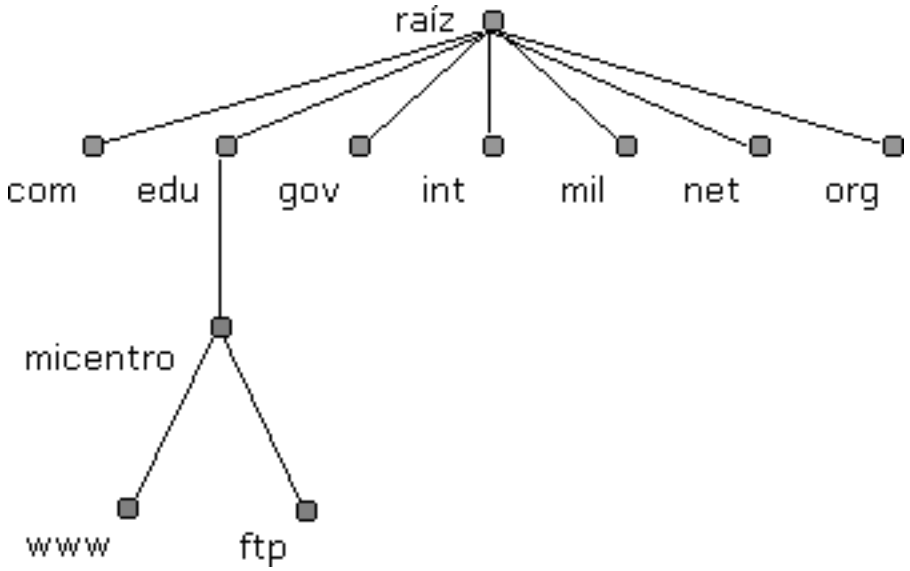
Nuestro PC tendrá que averiguar cual es la IP correspondiente a www.educacion.gob.es y una vez que ha averiguado que su IP es 193.147.0.112, se conecta con el servidor para adquirir la página web principal y mostrarla al usuario. Si en el navegador escribimos:
http://193.147.0.112

Ahorraremos el paso de averiguar la IP y directamente nos mostrará la página web del Ministerio de Educación.

Un servidor DNS es un servidor que permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio

No existe una base de datos única donde se almacenan todas las IPs existentes en el mundo, sino que cada servidor almacena las IPs correspondientes a su dominio. Los servidores DNS están dispuestos jerárquicamente de forma que cuando nuestro servidor más inmediato no puede atender nuestra petición, éste la traslada al DNS superior.

En el proceso de resolución de un nombre, hay que tener en cuenta que los servidores DNS funcionan frecuentemente como clientes DNS, consultando a otros servidores para resolver completamente un nombre consultado.



Linux dispone de varios paquetes de software que permiten poner en marcha un servidor DNS. En este capítulo hablaremos de dos de ellos: el paquete dnsmasq que es un sencillo servidor DNS ideal para redes pequeñas como las que podemos encontrar en los centros educativos y el paquete bind que es un completo servidor DNS utilizado por muchos servidores DNS en Internet.[2]

SERVIDOR PROXY WEB.

Un proxy (representante) es un agente o sustituto autorizado para actuar en nombre de otra persona (máquina o entidad) o un documento que lo autoriza a hacerlo es un tipo de servidor que lleva a cabo algunas funciones como representante de otros clientes (computadoras) en la red para incrementar el rendimiento de ciertas operaciones (por ejemplo, servir como caché de documentos y otros datos) o para servir como barrera de seguridad (por ejemplo, navegación anónima, o filtrado de los datos de entrada peligrosos).

Los servidores proxy no permiten un tráfico directo entre las partes.

SERVIDOR WEB.

Básicamente, un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP.

[2] "Servidor DNS | Redes Linux - Ministerio de Educación, Cultura y ...."
http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns.html. Se consultó el 11 dic.. 2017.

SERVIDOR LDAP.

LDAP (Lightweight Directory Access Protocol), (Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

FIREWALLS.

Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de trafico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.[3]

TECNOLOGÍAS A USAR O TÉRMINOS GENERALES DEL PROYECTO

DEBIAN 9:

Debian o Proyecto Debian Es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra precompilado, empaquetado y en formato deb para múltiples arquitecturas de computador y para varios núcleos.[4]

VIRTUALBOX:

Es un software de virtualización para arquitecturas x86. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como “sistemas invitados”, dentro de otro sistema operativo “anfitrión”, cada uno con su propio ambiente virtual.[5]

[3] "A History and Survey of Network Firewalls - CiteSeerX." http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7152&rep=rep1&type=pdf. Se consultó el 13 dic.. 2017.
[4] "Debian - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Debian. Se consultó el 15 ene.. 2018.
[5] "VirtualBox - EcuRed." https://www.ecured.cu/VirtualBox. Se consultó el 15 ene.. 2018.

IPTABLES:

Iptables es el componente más conocido del proyecto netfilter y es una herramienta que funciona en el espacio de usuario y que permite definir reglas para el filtrado y la modificación de paquetes TCP/IP que pasen por cualquiera de las interfaces de red de un equipo.[6]

CRON: CRONTAB

En el sistema operativo Unix, cron es un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero crontab.

DNSMASQ:

Proporciona servicios como caché DNS y como servidor DHCP. Como un servidor de nombres de dominio (DNS), puede almacenar en caché las consultas DNS para mejorar las velocidades de conexión a los sitios visitados anteriormente, y, como un servidor DHCP.[7]

NSLOOKUP:

Es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs. Se utiliza con el comando nslookup, que funciona tanto en Windows como en UNIX para obtener la dirección IP conociendo el nombre, y viceversa.[8]

DIG:

Esta herramienta viene en el paquete BIND (Berkeley Internet Name Domain) que es una implementación de protocolos DNS y sirve para diagnosticar problemas con los DNS. Por lo general se invoca de la siguiente forma:[9]

HOST:

Permite realizar búsquedas en DNS.

---

[6] "NAT con iptables | Desde lo alto del Cerro." 9 ene.. 2009, https://albertomolina.wordpress.com/2009/01/09/nat-con-iptables/. Se consultó el 16 ene.. 2018.

[7] "dnsmasq (Español) - ArchWiki." https://wiki.archlinux.org/index.php/Dnsmasq_(Espa%C3%B1ol). Se consultó el 16 ene.. 2018.

[8] "Nslookup - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Nslookup. Se consultó el 17 ene.. 2018.

[9] "dig - Linux Comandos | francisconi.org." 16 ene.. 2015, http://francisconi.org/linux/comandos/dig. Se consultó el 17 ene.. 2018.

SQUID:

Squid es un servidor proxy para web con caché. Es una de las aplicaciones más populares y de referencia para esta función, software libre publicado bajo licencia GPL.

Reduce el ancho de banda y mejora los tiempos de respuesta mediante el almacenamiento en caché y la reutilización de páginas web solicitadas con frecuencia. Squid tiene amplios controles de acceso y es un excelente acelerador de servidores.[10]

APACHE:

Es un poderoso servidor web, cuyo nombre proviene de la frase inglesa “a patchy server” y es completamente libre, ya que es un software Open Source y con licencia GPL. Una de las ventajas más grandes de Apache, es que es un servidor web multiplataforma, es decir, puede trabajar con diferentes sistemas operativos y mantener su excelente rendimiento.

[10] "Find Squid Proxy Server - SquidProxy.org." https://squidproxy.org/. Se consultó el 19 ene.. 2018.

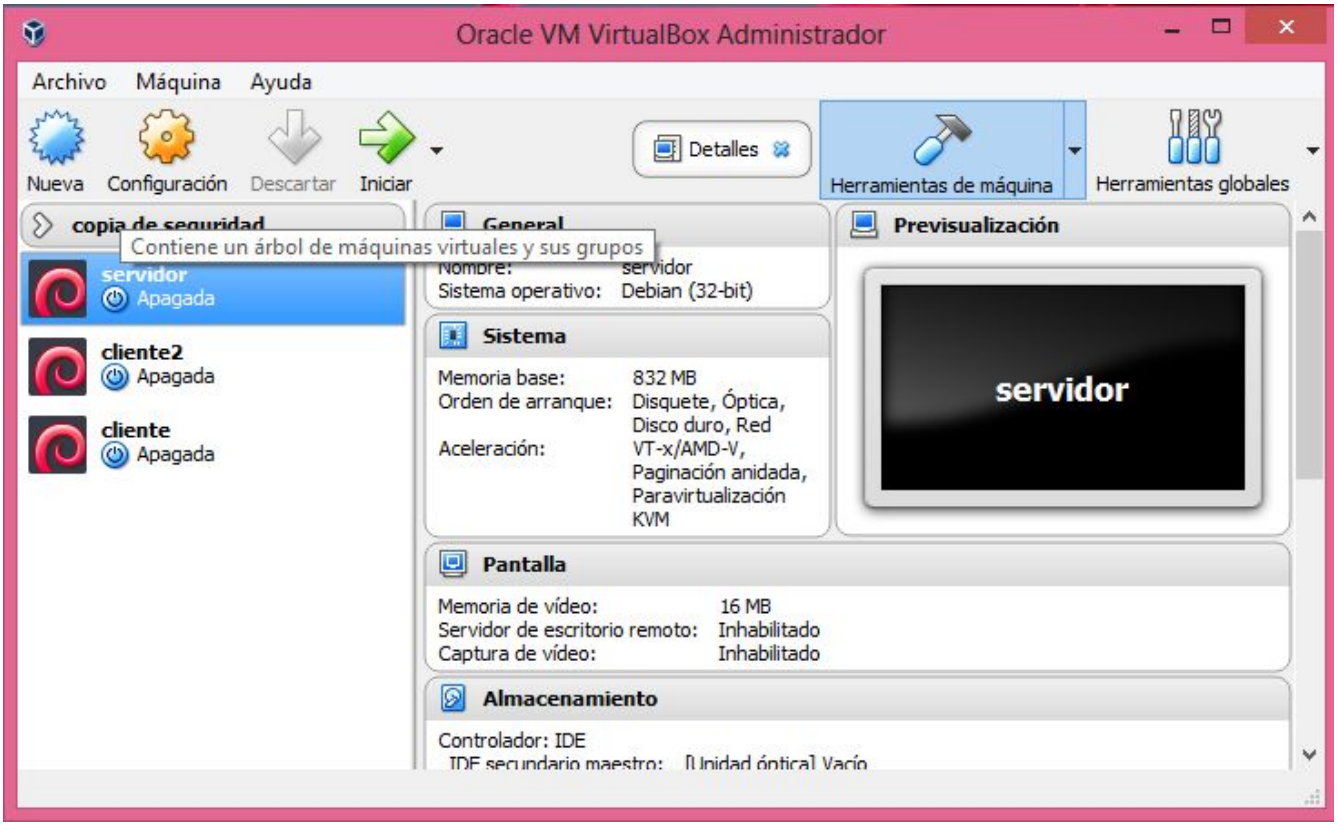
DETALLES SOBRE LA CONSTRUCCIÓN DEL PROYECTO

(pasos, comandos, artefactos, procedimientos)

- **CREACIÓN DE AMBIENTE DE TRABAJO.**

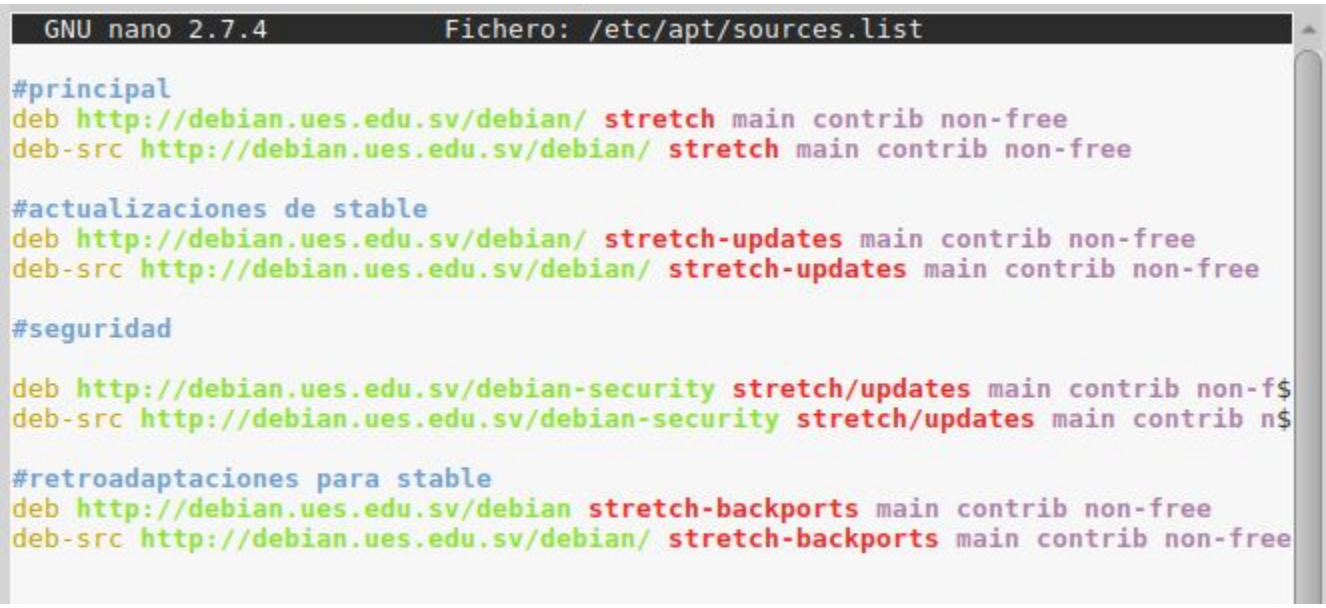
- Descargar debian en su versión más reciente se encuentra en: https://www.debian.org/CD/http-ftp/ una imagen iso para hacer instalaciones del sistema operativo en Virtualbox.

- Instalar imagen iso de Debian en virtualbox, instalación mínima con entorno de escritorio tanto para el servidor como para sus clientes.



En servidor dejar 2 adaptadores de red una en modo puente y otra en red interna para compartir internet con sus clientes. los clientes tienen solo un adaptador de red en red interna. (verificar que cables estén conectado).

- Actualizar Los repositorios se encuentran en el archivo /etc/apt/sources.list para añadir o modificar debemos abrir el editor nano como root.



- Actualizar lista de repositorios con: apt-get update

- **CONFIGURAR RED PARA MÁQUINAS VIRTUALES.**

Para ello consultar interfaces que tenemos con sus respectivas caracteristicas.

consultar con ifconfig

```
root@myserver:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe80:476d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:80:47:6d  txqueuelen 1000  (Ethernet)
        RX packets 18659  bytes 23254805 (22.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8649  bytes 608822 (594.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.1  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe70:5c80  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:70:5c:80  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59  bytes 7998 (7.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 6524  bytes 438696 (428.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6524  bytes 438696 (428.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

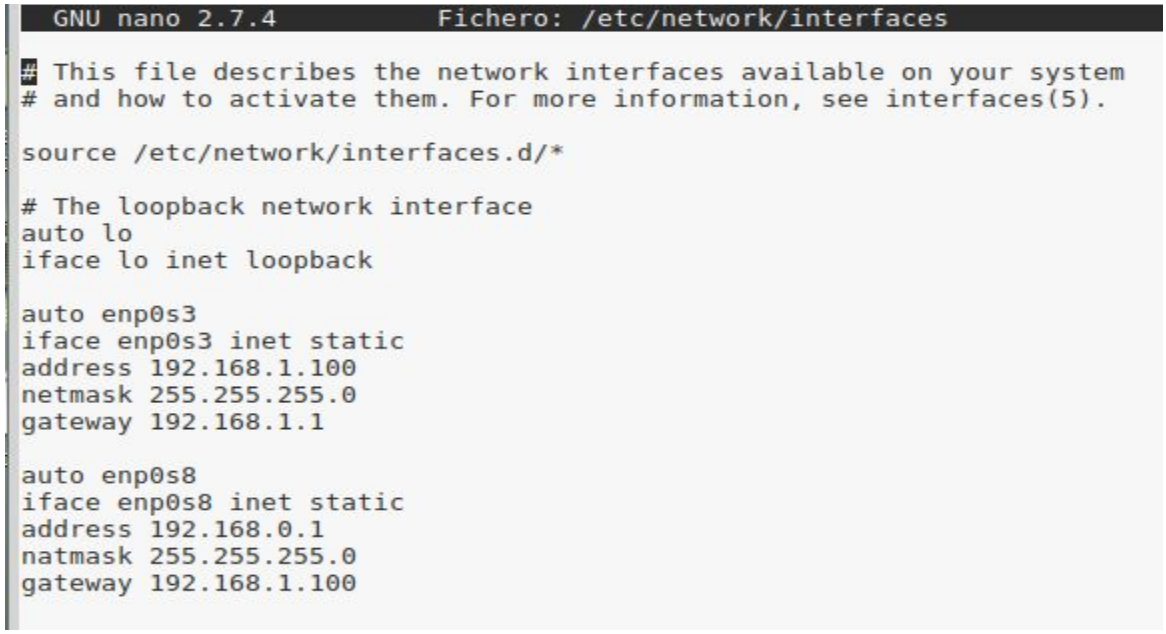
Se puede consultar también con ip addrees o ip add

```
root@myserver:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:80:47:6d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe80:476d/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:70:5c:80 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.1/24 brd 192.168.0.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe70:5c80/64 scope link
       valid_lft forever preferred_lft forever
root@myserver:~#
```

- **ASIGNAR IP ESTÁTICAS A LAS INTERFACES DE RED.**

En el fichero /etc/network/interfaces esta el archivo para configurar las interfaces de red de la siguiente manera:

Editar con nano y guardar:



```
  GNU nano 2.7.4          Fichero: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1

auto enp0s8
iface enp0s8 inet static
address 192.168.0.1
natmask 255.255.255.0
gateway 192.168.1.100
```

Desactivamos y activamos las configuraciones permanentes de interfaces de red con los siguientes comandos:

ifdown enp0s3
ifup enp0s3

Reiniciar la red con el comando /etc/init.d/networking restart y comprobar que la configuración de red es como la necesitamos.

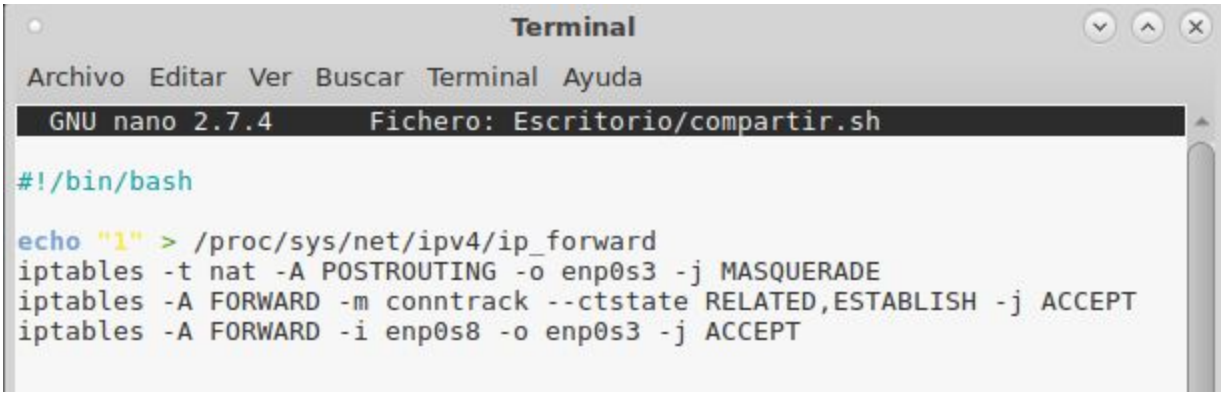
ip add.

Para las maquinas cliente ya que estas solo disponen de un adaptador de red, en red interna dejar las configuraciòn que trae por defecto ya que posteriormente se encargara de eso el servidor DHCP.

- **COMPARTIR INTERNET CON CLIENTES.**

NAT con iptables

Hacemos un proceso de Nateo para ello creamos el siguiente script y lo correremos:



- Con este script le dice a Debian que se comporte como un enrutador. cambiamos el valor binario del fichero /proc/sys/net/ipv4/ip_forward a “1”.
- Iptables manipular la tabla nat en la cola de post enrutamiento en la interfaz WAN enp0s3 (internet) y que haga traducciones de tip NAT (MASQUERADE).
- Iptables todo lo que llega a la cola forward le siga el rastro a la conección con RELATED,ESTABLISH lo acepte.
- Iptables todo lo que llegue a la cola forward desde la interfaz LAN (red interna) enp0s8 hacia la interfaz WAN enp0s3 (internet) lo acept.

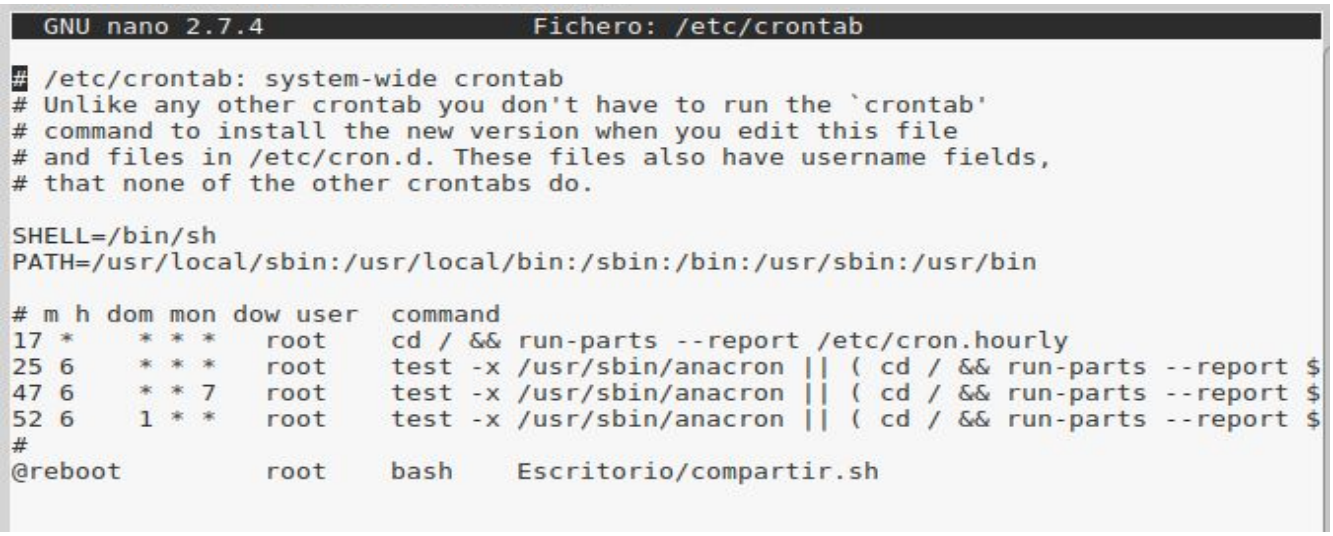
- **EJECUTAR SCRIPT AL INICIAR O REINICIAR LA PC.**

- Para ello instalar el programa CRON probablemente por defecto se encuentre instalado.

apt-get install cron

- editar el fichero /etc/crontab

nano /etc/crontab



En este fichero se puede agregar una linea al final con la que se define el momento en el que ejecuta un comando establecido. En este archivo se define el usuario con el que CRON ejecuta cierta tarea.

cuando se vuelva a reiniciar la pc se ejecuta una vez el proceso en el script Escritorio/compartir.sh

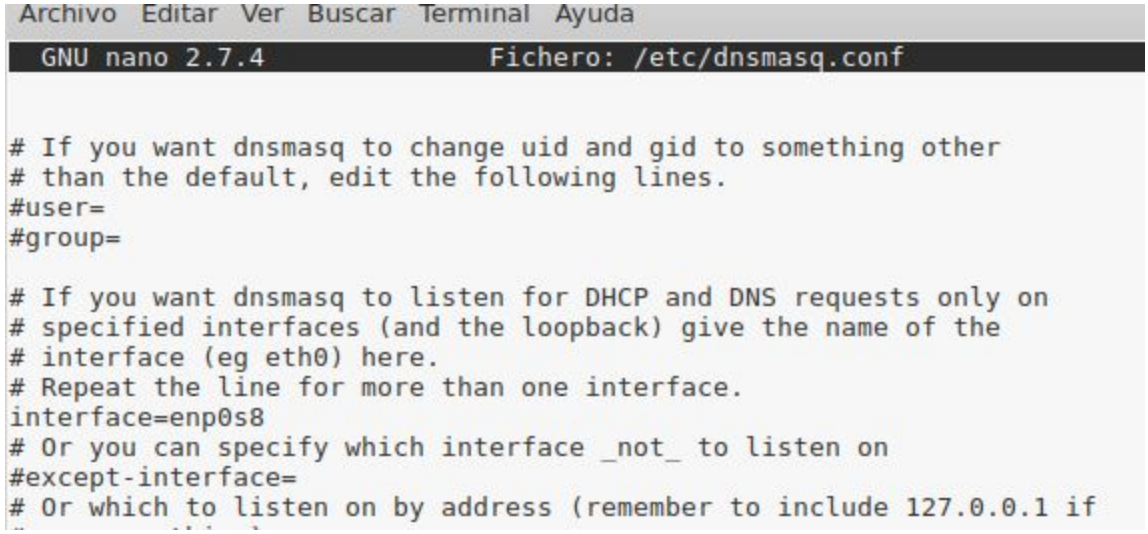
- **INSTALAR Y CONFIGURAR UN SERVIDOR DHCP.**

apt-get install dnsmasq

Para configurar dnsmasq como DHCP.

- Establecer la interfaz con la que dnsmasq resolver peticiones de los clientes que soliciten direcciones IP para ello editar el fichero /etc/dnsmasq.conf

nano /etc/dnsmasq.conf

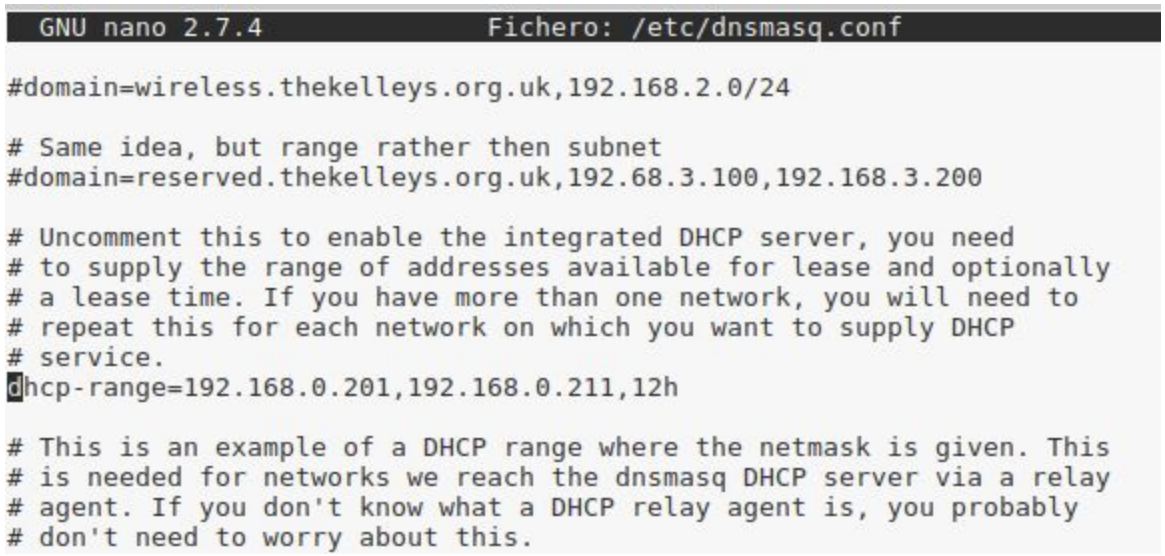


- Editar la linea que dice #interface=
- Borrar el numeral y especificar interfaz en el caso:

interface=enp0s8

Que és la interfaz de LAN (área local).

Por defecto, DHCP está desactivado. Esto es una buena cosa, ya que puedes derribar cualquier red a la que estés conectado si no tienes cuidado. Para habilitarlo, al menos habrá que editar una línea en el archivo /etc/dnsmasq.conf que tambien sirve para establecer el rango de ip que distribuirán las direcciones IP y el tiempo de alquiler.



En el proyecto solo distribuirán 11 direcciones IP con un tiempo de alquiler de 12 horas.

dhcp-range=192.168.0.201,192.168.0.211,12h

Reiniciar servicio DNSMASQ.

/etc/init.d/dnsmasq restart

En el cliente ejecutamos:

dhclient -v

Para recibir una IP y una máscara de red del rango y bloque de direcciones que nos ofrece el servidor DHCP.

De esta manera se tiene un servicio DHCP resolviendo peticiones.[11] Esta configuración es muy util y pensada para intranet pequeñas.

- **CONFIGURAR UN SERVIDOR DNS.**

Para que dnsmasq pueda ser un servidor caché DNS, es necesario que nuestro servidor tenga en el archivo de /etc/resolv.conf configurado al menos un servidor DNS externo. Normalmente los servidores DNS externos nos los proporciona el operador de telecomunicaciones que nos da servicio de Internet.

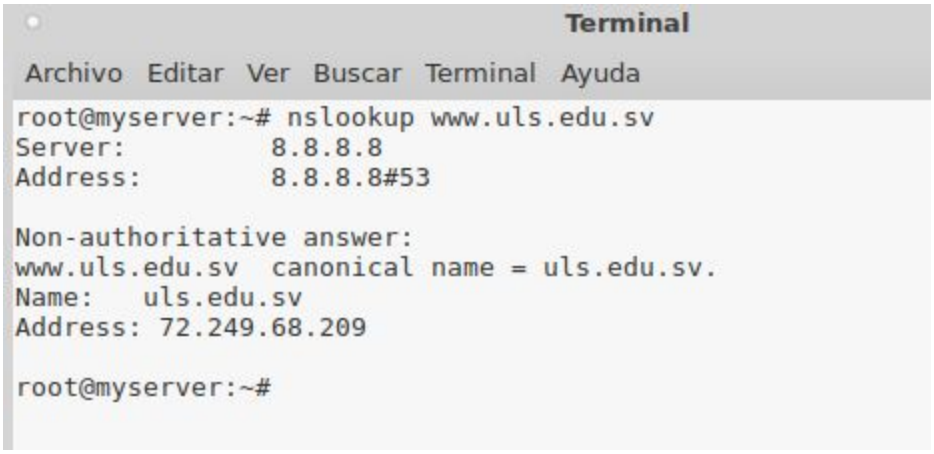
- Agregar al script compartir.sh para que cuando se reinicie la pc tambien tenga en cuenta escribir el fichero /etc/resolv.conf el servidor DNS 8.8.8.8 de google.com

- Comprobar que el DNS de google está funcionando en nuestra pc.

nslookup www.uls.edu.sv

[11] "HowTo/dnsmasq - Debian Wiki." 21 ene.. 2016, https://wiki.debian.org/HowTo/dnsmasq. Se consultó el 17 ene.. 2018.

Responde de la siguiente manera la petición: con la direcciòn IP del nombre de dominio de www.uls.edu.sv

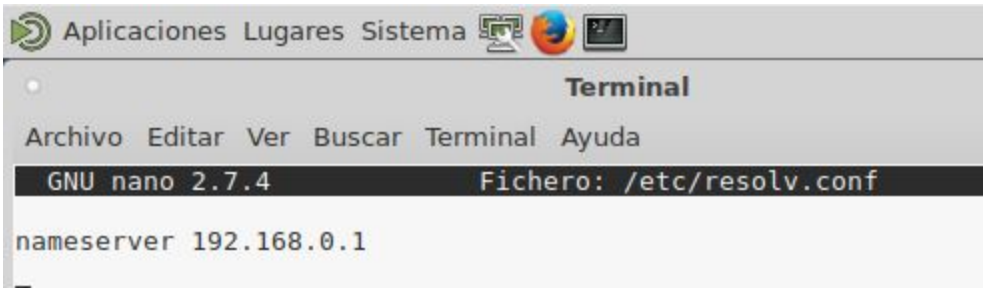


También se pueden hacer pruebas con host y dig.

```
root@myserver:~# host www.uls.edu.sv
www.uls.edu.sv is an alias for uls.edu.sv.
uls.edu.sv has address 72.249.68.209
uls.edu.sv mail is handled by 10 aspmx3.googlemail.com.
uls.edu.sv mail is handled by 1 aspmx.l.google.com.
uls.edu.sv mail is handled by 5 alt1.aspmx.l.google.com.
uls.edu.sv mail is handled by 5 alt2.aspmx.l.google.com.
uls.edu.sv mail is handled by 10 aspmx2.googlemail.com.
root@myserver:~# dig www.uls.edu.sv

; <<>> DiG 9.10.3-P4-Debian <<>> www.uls.edu.sv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47021
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.uls.edu.sv.                        IN      A

;; ANSWER SECTION:
www.uls.edu.sv.         2100    IN      CNAME   uls.edu.sv.
uls.edu.sv.             2100    IN      A       72.249.68.209

;; Query time: 88 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jan 17 00:11:44 CST 2018
;; MSG SIZE  rcvd: 73
```

DNSMASQ también nos sirve para usar un servidor DNS local, En este punto, ya tendremos en nuestro servidor un servidor DNS caché funcionando. Para probar su funcionamiento, configuraremos el archivo /etc/resolv.conf del resto de los PCs de nuestra red pero en lugar de indicar el DNS de google (8.8.8.8) indicaremos el nuestro 192.168.0.1 ya que nuestro servidor tiene la IP estática, lo añadiremos en el archivo /etc/resolv.conf de cada PC.

nano /etc/resolv.conf



Al igual que hicimos con nuestro cliente podemos comprobar haciendo peticiones de tipo DNS con los comandos nslookup, host y dig si nuestro servidor funciona nos respondera con IP de dichas peticiones. aunque es recomendable introducir también un segundo DNS externo por si este falla.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@cliente:~# nslookup ues.edu.sv
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   ues.edu.sv
Address: 168.232.49.155

root@cliente:~# nslookup www.uls.edu.sv
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
www.uls.edu.sv  canonical name = uls.edu.sv.
Name:   uls.edu.sv
Address: 72.249.68.209

root@cliente:~# host www.ues.edu.sv
www.ues.edu.sv has address 168.232.49.178
root@cliente:~# ping www.twitter.com
PING twitter.com (104.244.42.1) 56(84) bytes of data.
64 bytes from 104.244.42.1: icmp_seq=1 ttl=52 time=59.4 ms
64 bytes from 104.244.42.1: icmp_seq=2 ttl=52 time=59.1 ms
64 bytes from 104.244.42.1: icmp_seq=3 ttl=52 time=58.4 ms
64 bytes from 104.244.42.1: icmp_seq=4 ttl=52 time=62.8 ms
64 bytes from 104.244.42.1: icmp_seq=5 ttl=52 time=60.2 ms
^X^C
--- twitter.com ping statistics ---
```

Pruebas nslookup salir a internet desde red interna, ues.edu.sv, www.uls.edu.sv, host www.ues.edu.sv, ping a www.twitter.com desde cliente.

```
root@myserver:~# host www.uls.edu.sv
www.uls.edu.sv is an alias for uls.edu.sv.
uls.edu.sv has address 72.249.68.209
uls.edu.sv mail is handled by 10 aspmx3.googlemail.com.
uls.edu.sv mail is handled by 1 aspmx.l.google.com.
uls.edu.sv mail is handled by 5 alt1.aspmx.l.google.com.
uls.edu.sv mail is handled by 5 alt2.aspmx.l.google.com.
uls.edu.sv mail is handled by 10 aspmx2.googlemail.com.
root@myserver:~# dig www.uls.edu.sv

; <<>> DiG 9.10.3-P4-Debian <<>> www.uls.edu.sv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47021
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.uls.edu.sv.                        IN      A

;; ANSWER SECTION:
www.uls.edu.sv.         2100    IN      CNAME   uls.edu.sv.
uls.edu.sv.             2100    IN      A       72.249.68.209

;; Query time: 88 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jan 17 00:11:44 CST 2018
;; MSG SIZE  rcvd: 73
```

host www.uls.edu.sv
dig a www.uls.edu.sv desde cliente.

Con Servidor DNS funcionando editar el archivo /etc/hosts del servidor, para que nuestro servidor DNS resuelva los nombres y las ip de nuestra red. de esta manera DNSMASQ hace que este fichero funcione también como un DNS maestro.

nano /etc/hosts

```
  GNU nano 2.7.4                Fichero: /etc/hosts

127.0.0.1       localhost
127.0.1.1       servicios
192.168.43.1    miinternet.com
192.168.0.1     servidorlan

192.168.0.201   cliente01
192.168.0.202   cliente02
192.168.0.203   cliente03
192.168.0.204   cliente04
192.168.0.205   cliente05
192.168.0.206   cliente06
192.168.0.207   cliente07
192.168.0.208   cliente08
192.168.0.209   cliente09
192.168.0.210   cliente10
192.168.0.211   cliente11
```

Definir nombres del loopback (localhost), del hostname, para los adaptadores de red de nuestra interfaz WAN y LAN y para cada máquina cliente para las IP que son arrendadas por nuestro servidor DHCP.

Al realizar cambios en el fichero /etc/hosts reiniciar los servicios de DNSMASQ con el comando:

/etc/init.d/dnsmasq restart

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@cliente:~# dig servidorlan

; <<>> DiG 9.10.3-P4-Debian <<>> servidorlan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6859
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;servidorlan.                   IN      A

;; ANSWER SECTION:
servidorlan.            0       IN      A       192.168.0.1

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Wed Jan 17 01:33:37 CST 2018
;; MSG SIZE  rcvd: 56

root@cliente:~# nslookup servidorlan
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   servidorlan
Address: 192.168.0.1
```

dig servidorlan
nslookup servidorlan

De esta manera se tiene un servicio DNS resolviendo peticiones. Esta configuración es muy util y pensada para intranet pequeñas y facilmente configurable. para redes con grado mas alto de complejidad se recomienda utilizar BIND9.[12]

[12] "Servidor DNS y DHCP sencillo con dnsmasq | Redes Linux." http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_y_dhcp_sencillo_con_dnsmasq.html. Se consultó el 17 ene.. 2018.

INSTALACIÓN Y CONFIGURACIÓN DE UN PROXY

Para instalación servidor proxy squid podemos hacerlo de la siguiente ejecutar:

apt-get install squid

Cambiamos de directorio a /etc/squid

cd /etc/squid

Primero realizamos una copia de respaldo para el archivo de configuración para guardar la configuración por defecto por cualquier error en el proceso de configuración:

cp /squid.conf /squid.conf.backup
a
Para configurar abrimos el editor nano o el archivo donde realizaremos las configuraciones:

nano squid.conf

En la linea que dice que **http_port 3128**

Indica que por defecto Proxy Squid escucha por este puerto la configuraciones en este caso Listas de control de acceso (ACL).

Estas se definen de la siguiente manera:

acl redglobal src 192.168.43.0/24 es el control de acceso para nuestra red WAN:

acl redlocal src "/etc/squid/redlocal" define la ruta en donde se encuentran las IP de nuestra red local.

acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados" define la ruta donde se encuentra la lista de sitios que seran bloqueados en nuestro servidor proxy squid.

las ACL que hemos indicado tienen el mismo nombre que los archivos de listas pero no es necesario en este caso se hace así para evitar confusión.

Pero estas listas por si solas no hacen nada.

Se tendra que definir el control de acceso HTTP para cada una de estas listas:

```
#LISTAS DE CONTROL DE ACESS
acl redglobal src 192.168.43.0/24
acl redlocal src "/etc/squid/redlocal"
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"

#HTTP ACESS
http_access allow redglobal
http_access allow redlocal !sitiosdenegados
```

Abajo de las acl se crea lo que son http_access con estas bloquean (deny) o permiten (allow) las listas de control de acceso que proxy está escuchando.

http_access allow redglobal permite acceso a nuestra redglobal (192.168.43.0/24) al squid proxy.

http_access allow redlocal !sitiosdenegados permite el acceso a nuestra redlan (192.168.0.0/24) que esta especificida en el archivo externo "/etc/squid/redlocal" y acepción de las lista de control de acceso que está en "/etc/squid/sitiosdenegados"

También descomentar esta línea que por defecto esta comentada, que deniega las solicitudes a ciertos puertos inseguros

#http_access deny !Safe_ports

Por último descomentar las configuraciones de caché

cache_mem 256 MB

cache_dir ufs /var/spool/squid 1000 16 256
(Agregar más dependiendo la capacidad de la máquina física)

Eso seria todo en las configuraciones del archivo /etc/squid/squid.conf recordemos que también tenemos un backup.

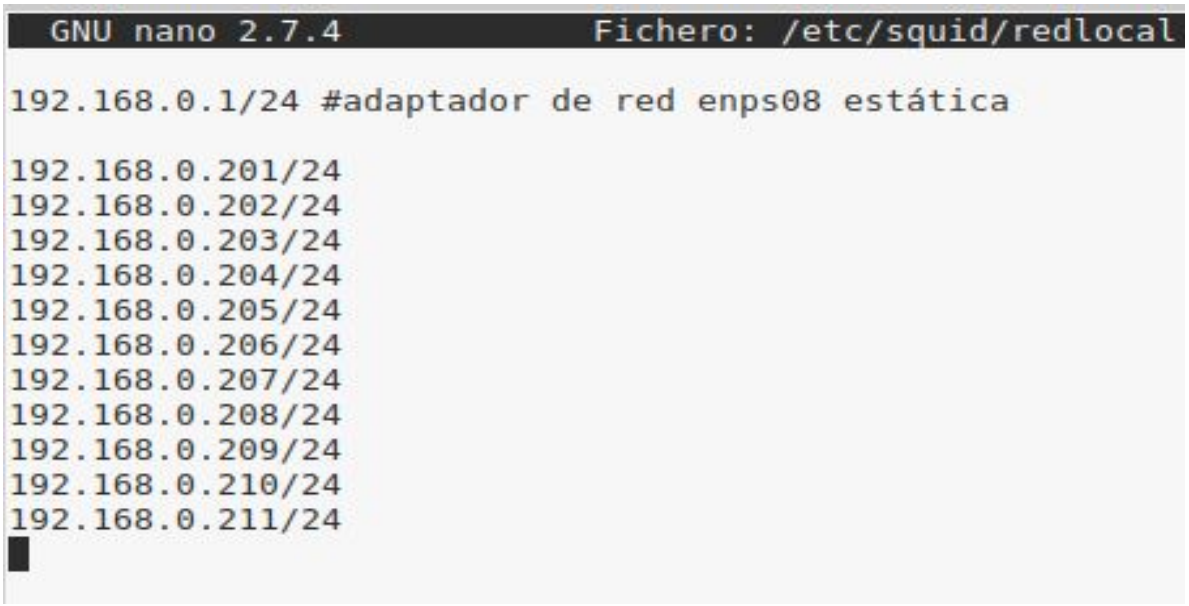
Posteriormente reiniciamos el servicio de squid como lo hacemos con los demás servicios en linux.

Crear el fichero que tiene las IP de nuestra red local para la ACL “redlan” que tienen acceso al proxy

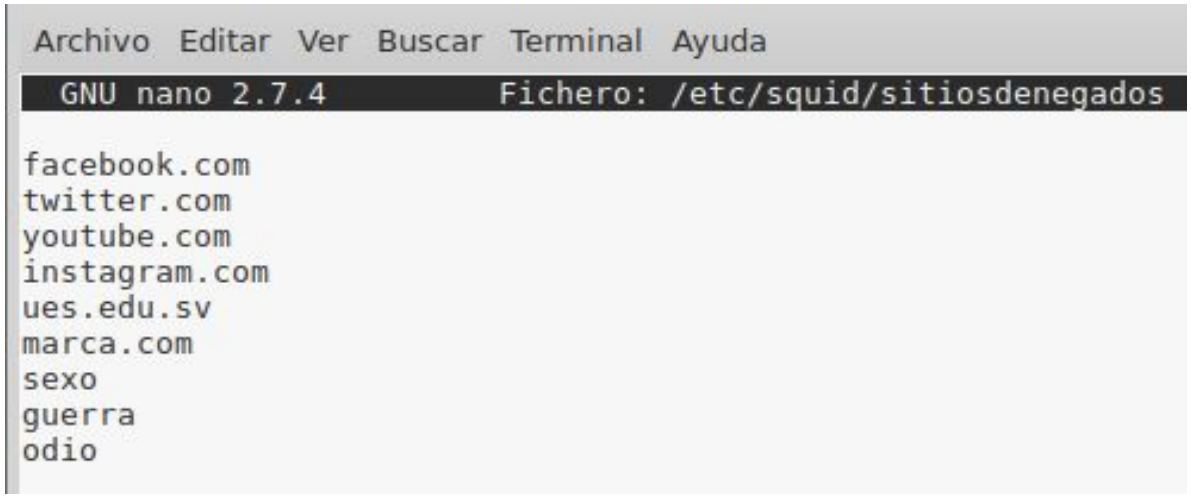
nano redlocal

Crear el fichero que tiene las paginas o nombres de dominio que conforman la ACL “sitiosdenegados”

nano sitiosbloqueados



También agregar la IP de la interfaz enp0s8



En este caso agregar algunas paginas para denegar el acceso a ellos.

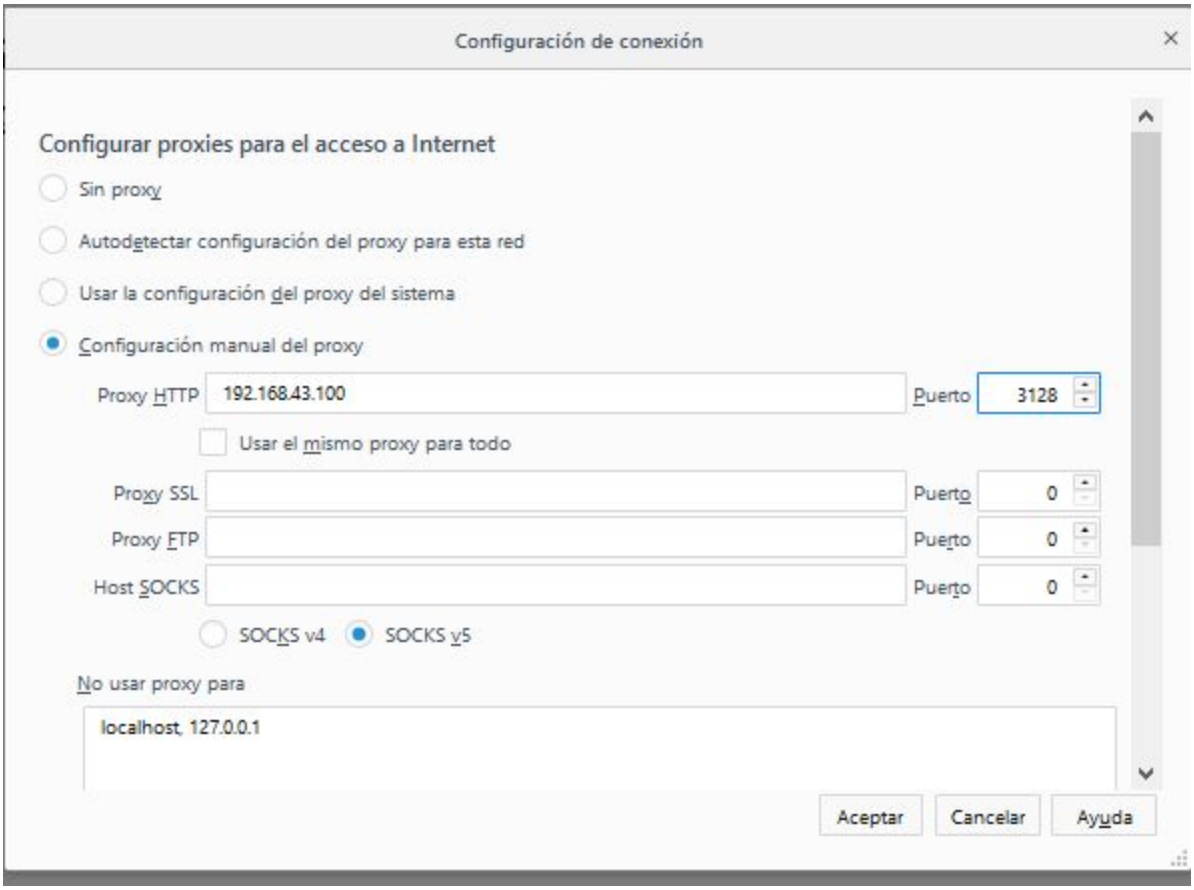
/etc/init.d/squid restart

ó también podemos elegir entre

service squid restart

Configurar navegador cliente para que uso el squid

En el caso de Firefox **Preferencias, Configuración de conexión**



Pondremos la IP de nuestro servidor proxy 192.168.43.100 y usamos el mismo proxy para todo y aceptamos.

En el caso de Google Chrome vamos a Configuración, en la caja de busqueda pones proxy nos aparecera para abrir la configuración de proxy de nuestro sistema operativo eh igual pondremos ahí nuestra IP.

CONFIGURACIÓN DE IPTABLES COMO FIREWALL

La herramienta o programa IPTABLES ya esta por defecto instalada en el sistema debian 9 stretch pero es necesario la instalación de herramientas para el fácil desarrollo y comprenciòn de las siguientes configuraciones por lo tanto.

Instalación de herramientas necesarias para el desarrollo de un cortafuegos con IPTABLES:

apt-get install nmap net-tools telnet

Nmap: Es un programa de código abierto que sirve para efectuar rastreo de puertos[13]
Net-tools. El paquete Net-tools contiene una colección de programas que forman la base del trabajo en red en Linux[14]

Lo que se gestiona de forma básica con **iptables** comprende lo siguiente:

Listar la reglas de bloqueo o acceso:

iptables -L

INPUT(ENTRADAS)

Cambiar la política a bloquear todo el tráfico entrante
iptables -P INPUT DROP

Cambiar la política a aceptar todo el tráfico entrante
iptables -P INPUT ACCEPT

Escanear puertos TCP abiertos
nmap -n 192.168.0.1

Agregar una regla para bloquear conexiones entrantes a un puerto especifico (puerto 80)
iptables -A INPUT -p tcp --destination-port 80 -j DROP

Eliminar una regla para bloquear conexiones entrantes a un puerto especifico (puerto 80)
iptables -D INPUT -p tcp --destination-port 80 -j DROP

Agregar una regla para bloquear conexiones entrantes a desde una IP específica
iptables -A INPUT -s 192.168.0.1 -j DROP

Eliminar una regla para bloquear conexiones entrantes a desde una IP específica

[13] "Nmap - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Nmap. Se consultó el 19 ene.. 2018.
[14] "Net-tools - Es.comp.os.linux." http://www.escomposlinux.org/lfs-es/lfs-es-5.0/appendixa/net-tools.html. Se consultó el 19 ene.. 2018.

iptables -D INPUT -s 192.168.0.1 -j DROP

Agregar una regla para bloquear todo un bloque de direcciones IP de una red.
iptables -A INPUT -s 192.168.0.1/24 -j DROP

Eliminar una regla para bloquear todo un bloque de direcciones IP de una red.
iptables -D INPUT -s 192.168.0.1/24 -j DROP

Mostrar en pantalla las reglas creadas para poder guardarlas.
iptables-save

OUTPUT(SALIDAS)

Cambiar la política a bloquear todo el tráfico saliente
iptables -P OUTPUT DROP
443
Cambiar la política a aceptar todo el tráfico saliente
iptables -P OUTPUT ACCEPT

Agregar una regla para bloquear conexiones salientes a un puerto especifico (puerto 443)
iptables -A OUTPUT -p tcp --destination-port 443 -j DROP

Eliminar una regla para bloquear conexiones salientes a un puerto especifico (puerto 4443)
iptables -D OUTPUT -p tcp --destination-port 443 -j DROP

Eliminar una regla para bloquear conexiones salientes a desde una IP específica
iptables -D OUTPUT -s 192.168.0.1 -j DROP

Agregar una regla para bloquear todo un bloque de direcciones IP de una red.
iptables -A OUTPUT -s 192.168.0.1/24 -j DROP

Eliminar una regla para bloquear todo un bloque de direcciones IP de una red.
iptables -D OUTPUT -s 192.168.0.1/24 -j DROP

OTROS CONCEPTOS

Para borrar toda la configuración del firewall para volver a configurarlo de nuevo debemos teclear:
• iptables -F

Permitir firewall para que reenvíe el tráfico de la red local a través de internet. Para ello escribiremos:

• iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

Consultar los paquetes rechazados por iptables
Para saber los paquetes que iptables ha rechazado debemos teclear:
• iptables -N LOGGING
• iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP
• iptables -A INPUT -p icmp –icmp-type echo-request -j DROP

Ejemplo:
• sudo ufw allow 1234/tcp (permite las conexiones del puerto 1234 en tcp)
• sudo ufw deny 4321/udp (bloquea las conexiones del puerto 4321 en udp)

INSTALACIÓN DE SERVIDOR WEB APACHE

- Instalación

apt-get get install apache2

- Esto será suficiente para tener apache corriendo en nuestra red.

INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR LDAP

Para poder instalar LDAP en Linux tendremos que introducir el siguiente comando actualizamos.

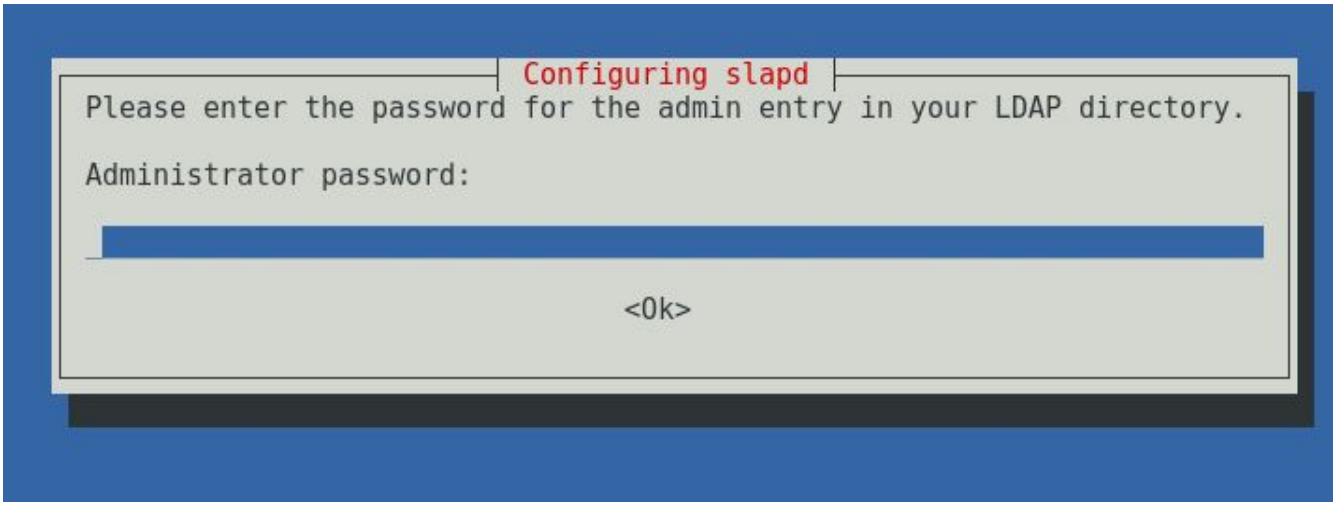
(Como superusuario)

apt-get update

instalamos slapd y ldap-utils

apt-get install slapd ldap-utils

Una vez introducido el comando de instalación nos pedirá en un asistente la clave del administrador que le vamos a asignar para que pueda gestionarlo correctamente.



Acto seguido nos pedirá que confirmes la clave que hemos introducido (aunque de todos modos más adelante lo configuraremos todo de nuevo correctamente así que más adelante la tendremos que configurar de nuevo).

Una vez configurada la contraseña tendremos instalado el servicio LDAP y nos habra configurado automáticamente un directorio con dos entradas de LDAP que lo podremos ver con el siguiente comando.

slapcat

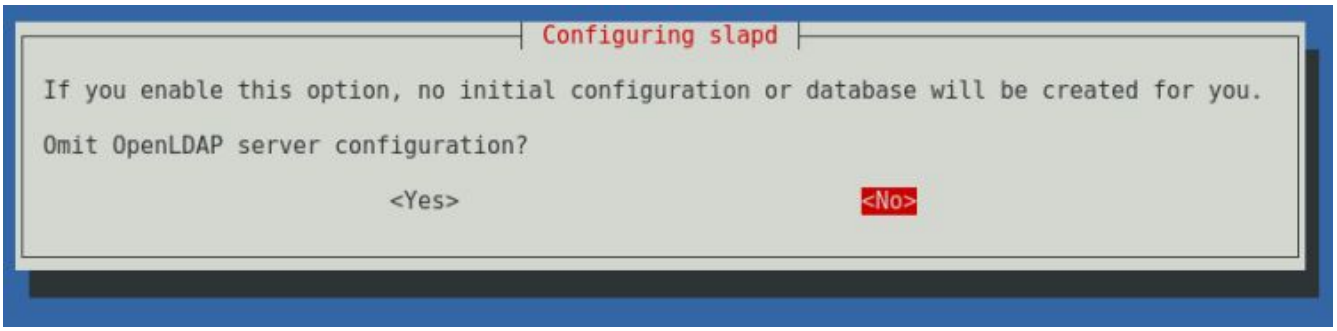
Hay que saber que cada entrada se etiqueta de manera única con la etiqueta dn (Distinguished Name) además si introducimos el siguiente comando podemos ver la cantidad de entradas de LDAP existentes.

ldapsearch -x -h localhost

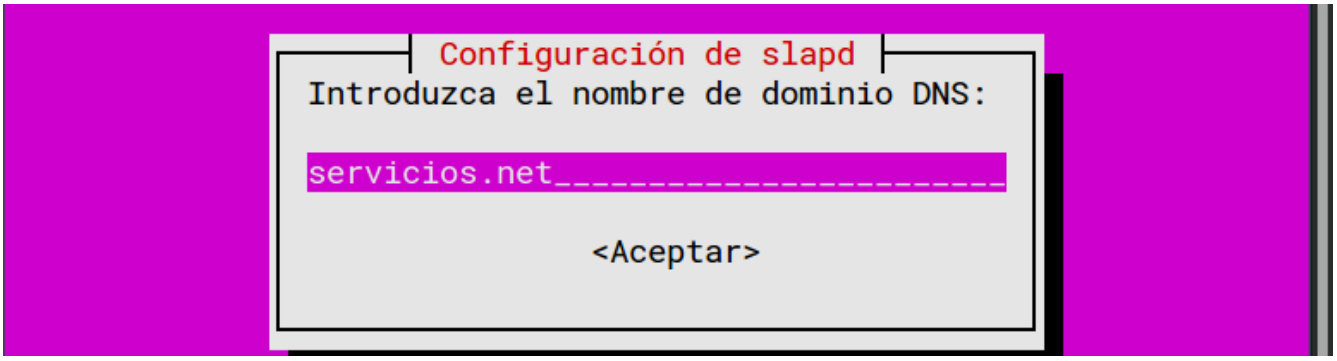
A continuación procederemos a configurar nuestro LDAP y para ello vamos a introducir el siguiente comando.

dpkg-reconfigure -plow slapd

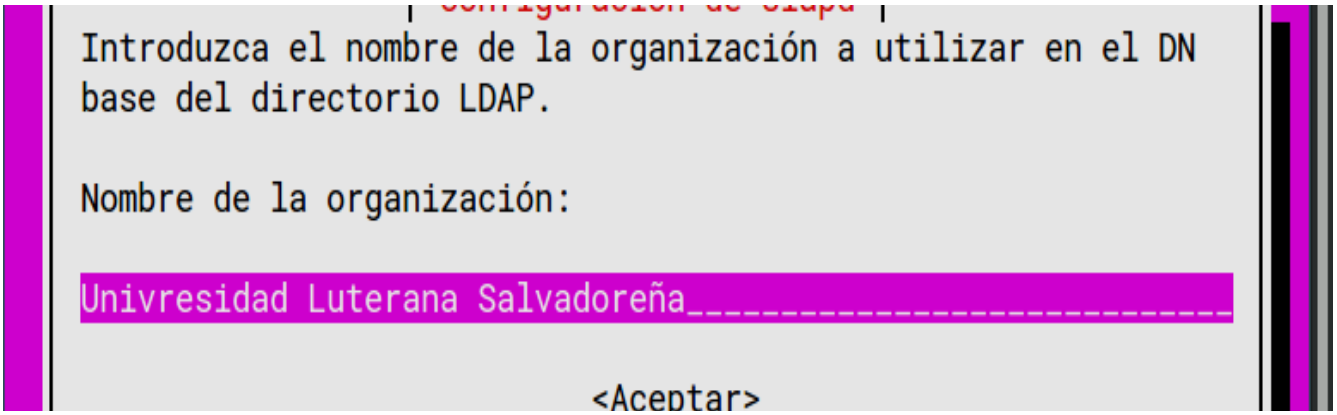
Una vez que hayamos ejecutado esta instrucción tendremos que indicar que deseamos realizar la configuración de LDAP para ello indicaremos que no deseamos omitir la configuración del servidor OpenLDAP.



Seleccionamos No, procederemos a indicar nuestro nombre de dominio DNS siendo en nuestro caso servicios.net

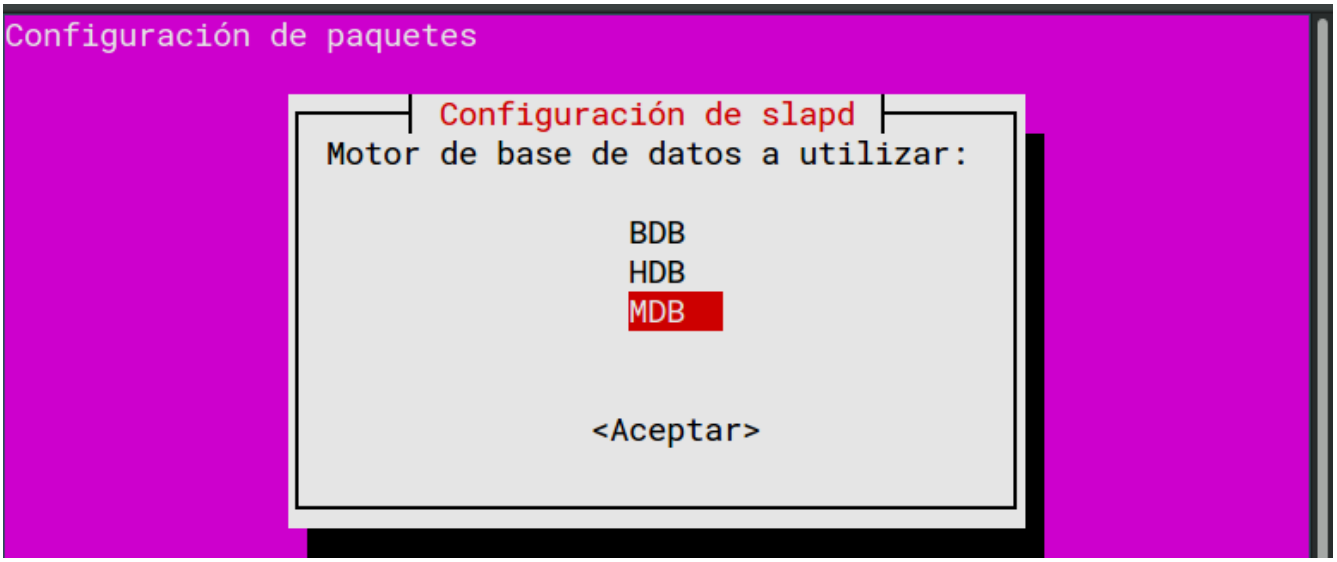


Seguidamente una vez indicado el nombre de dominio nos pedirá el nombre de la organización, siendo en nuestro caso Universidad Luterana Salvadoreña.

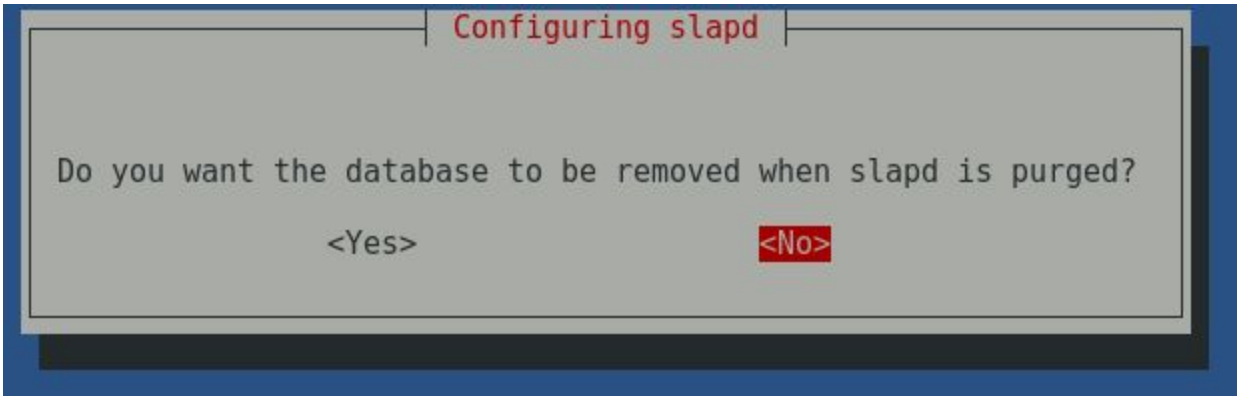


Acto seguido nos pedirá que le indiquemos una contraseña de administrador para tener nuestro LDAP seguro, esta contraseña es para lo mismo que nos pidió en el proceso de instalación pero como estamos reconfigurando nuestro LDAP pues la vamos a definir de nuevo.

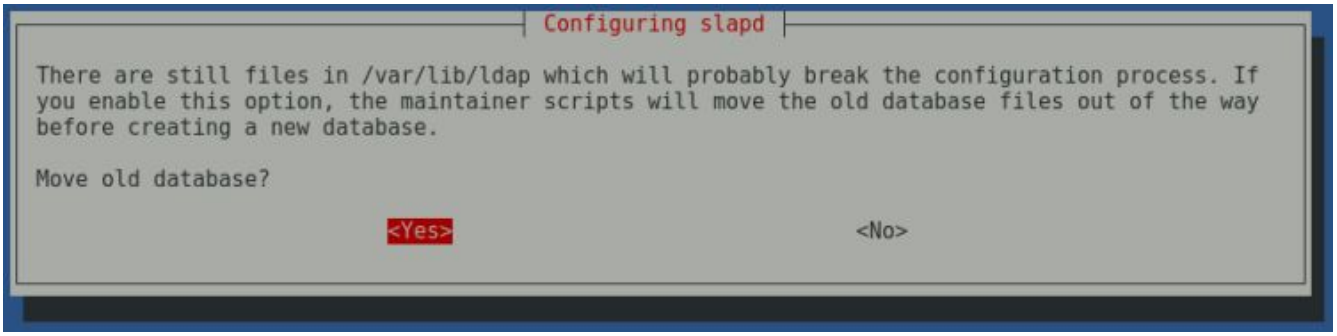
Después de haber definido la contraseña tendremos que indicar el motor de base de datos que en nuestro caso vamos a dejar la opción que viene por defecto seleccionada que es MDB.



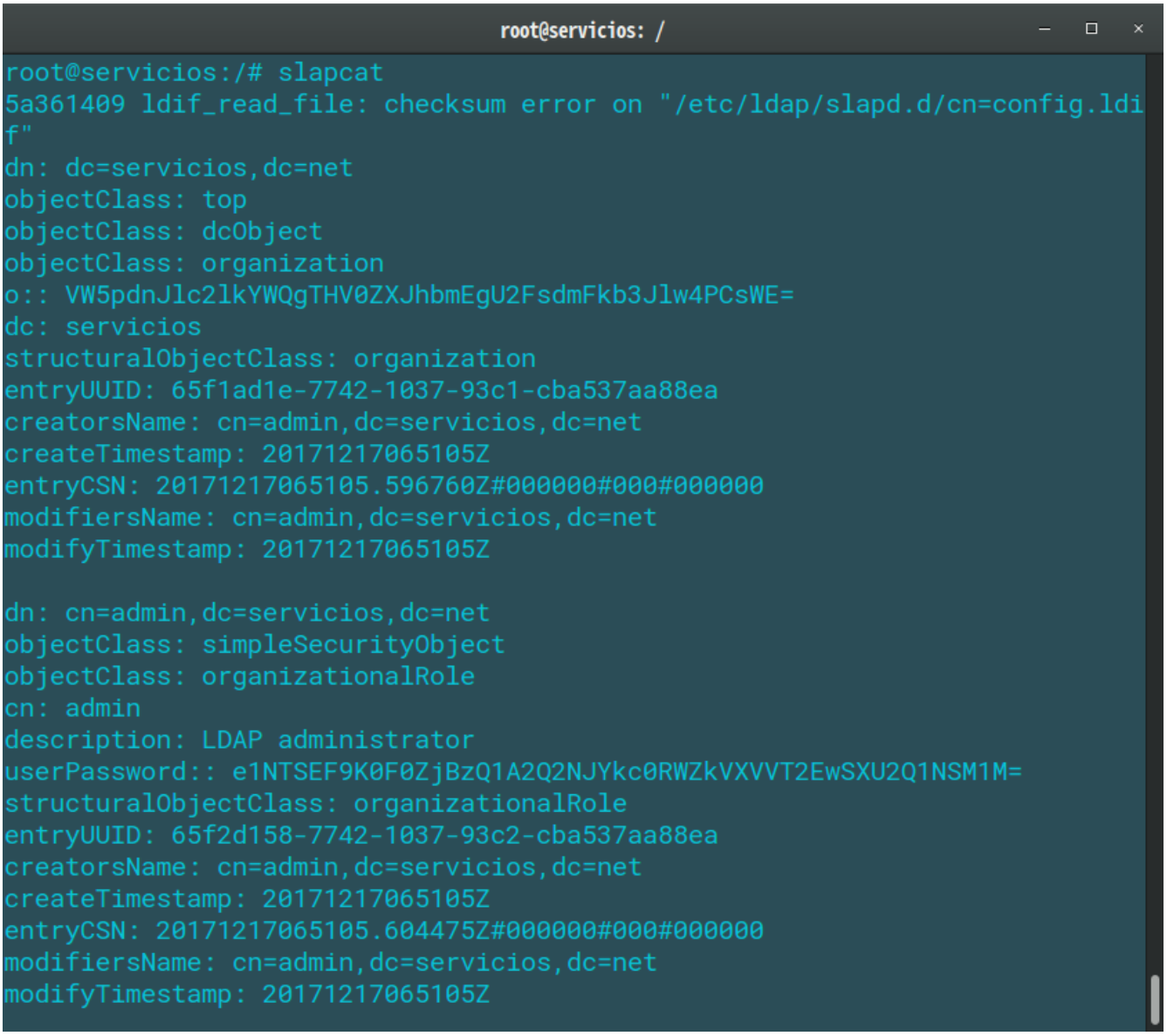
A continuación dejamos la opción por defecto en el apartado que nos indica que si deseamos que se elimine el directorio slapd de la base de datos cuando slapd sea eliminado, siendo esa opción por defecto que sea no, que no deseamos que se elimine.



El la siguiente opción configurable definimos que si deseamos que se mueva el antiguo directorio dejando como opción la que viene por defecto que es si.



Una vez que ya hayamos definido todos estos parámetros, tendremos nuestro LDAP configurado correctamente. Para la comprobación de que lo configurado es correcto tendremos que volver a introducir el comando que hemos introducido anteriormente que es slapcat y comprobaremos como los cambios han sido aceptados.



Cuando ya hayamos comprobado que todo esta correcto nos disponemos a realizar la creación de usuarios, grupos y unidades organizativas para ir poblando el LDAP.

Creación y configuración de Usuario, Grupos y U. Organizativas en LDAP.

Los parámetros de configuración para poblar el LDAP se realizan a través de ficheros de texto plano cuya extensión es .ldif y dicha información es separada por una línea en blanco para que así se acepte los parámetros indicados. Mostrándose igual que lo muestra el comando slapcat.

Estos ficheros con esta extensión se cargan en el LDAP a través de un comando y además de ello podremos organizar los fichero como mas cómodo nos sean por ejemplo tener un fichero .ldif para cada tipo de información que va a almacenar siendo de la siguiente forma: usuario.ldig, grupos.ldif, u_organizativas.ldif, que es como lo vamos a realizar en nuestro caso.

A continuación vamos a ir configurando los ficheros de forma escalonada empezando por las unidades organizativas, pasando por los grupos y terminando en los usuarios (todos estos ficheros los vamos a crear en el directorio personal).

nano u_organizativas.ldif

dn: ou=People,dc=lopez,dc=gonzalonazareno,dc=org
objectClass: top
objectClass: organizationalUnit
ou: People

nano grupos.ldif

dn: cn=Usuarios,ou=People,dc=lopez,dc=gonzalonazareno,dc=org
objectClass: top
objectClass: posixGroup
gidNumber: 2000
cn: Usuarios

En el caso de los usuarios tendremos que indicar en la variable **userpassword** la contraseña cifrada que la tendremos que cifrar con el comando **slappasswd** y el resultado lo pegamos en ese campo.
Ejemplo del comando:
slappasswd -v

New password:
Re-enter new password:
{SSHA}Z5CT5PNeCA1oPCqxxxoAH54SVZCSZnkw

Y en el caso de introducir las palabras o nombre con tildes tendremos que indicar dicho nombre codificado en base64 como suele ocurrir con el campo CN que es el nombre completo con apellidos, SN que es el apellido o el givenName que es el nombre de pila. Para ello tendremos que poner el nombre y los apellidos con el comando base64 y si deseamos hacer la codificación inversa tendremos que indicar el comando base64 -d y dicho resultado lo copiamos y pegamos en el fichero .ldif.

Ejemplo del comando:
echo Rocio | base64
Um9jaW8gTMOzcGV6Cg==
Este resultado tendremos que indicarlo con dos :: en la etiqueta deseada para así indicar que esta en base64.

nano usuarios.ldif

dn: uid=juanjo,ou=People,dc=lopez,dc=gonzalonazareno,dc=org
objectClass: top
objectClass: posixAccount

objectClass: inetOrgPerson
objectClass: person
cn:: SnVhbiBKb3PDqSBMw7NwZXogUm9sZMOhbgo=
uid: juanjo
uidNumber: 2001
gidNumber: 2000
homeDirectory: /home/nfs/juanjo
loginShell: /bin/bash
userPassword: {SSHA}LiKe/KvY1CgL5axLB7vEqbclZ
sn:: TMOzcGV6IJbTDoW4K
mail: juanjo@gmail.com
givenName: juanjo

Una vez creado todos los fichero de configuracion.ldif nos dispondremos a agregar los datos al LDAP y para ello utilizaremos el siguiente comando que nos permitirá añadir esta información, cuando introducimos el comando nos pedirá la clave del administrador del ldap para validar dicha introducción de datos.

- Introducción de datos de la unidad organizativa:
- ldapadd -x -D cn=admin,dc=lopez,dc=gonzalonazareno,dc=org -W -f u_organizativas.ldif
- Introducción de datos del grupo:

ldapadd -x -D cn=admin,dc=lopez,dc=gonzalonazareno,dc=org -W -f grupos.ldif

- Introducción de datos del usuario:
- ldapadd -x -D cn=admin,dc=lopez,dc=gonzalonazareno,dc=org -W -f usuario.ldif

Si deseamos eliminar algún usuario que hemos introducido tendremos que realizarlo de la siguiente manera (ldapdelete -x -D ‘Usuario con permisos para poder eliminar’ ‘Objeto a eliminar’ -W)
ldapdelete -x -D 'cn=admin,dc=lopez,dc=gonzalonazareno,dc=org' 'uid=Juanjo,ou=People,dc=lopez,dc=gonzalonazareno,dc=org' -W

Si deseamos realizar modificaciones en el ldap tendremos que realizarlo de la siguiente manera:
En este ejemplo vamos a realizar el cambio de directorio de usuario para el usuario rocio.

nano usuario2.ldif

dn: uid=rocio,ou=People,dc=lopez,dc=gonzalonazareno,dc=org
changetype:modify
replace: homeDirectory
homeDirectory: /home/nfs/rocio

ldapmodify -x -D 'cn=admin,dc=lopez,dc=gonzalonazareno,dc=org' -f usuario2 -W

Si deseamos realizar búsquedas se realiza de la siguiente manera:
ldapsearch -x -h mikey -b "dc=lopez,dc=gonzalonazareno,dc=org"

Acto seguido para comprobar que todos los datos introducidos son los correctos y se han introducido nos dispondremos a introducir de nuevo el comando que ejecutamos anteriormente llamado slapcat para verificar la veracidad de los datos.

En el caso que deseemos realizar copias de seguridad de nuestro ldap siempre podremos redireccionar a un fichero el resultado de este comando para así tener en todo momento una copia del mismo.

INSTRUCCIONES USADAS EN EL PROYECTO

LINUX(DEBIAN)	FUNCIÓN
ping	Verifica conexión entre dos host
ifconfig	Muestra y permite configurar la interfaz de red
dig	Convierte nombre a ip y viceversa
whois	Consulta sobre dominio en internet
nslookup	Resuelve nombres de dominio para direcciones IP
mtr	Muestra saltos y hace ping(traceroute+ping)
netsat	Muestra la lista de conexiones activas en una pc
ip add o ip address	Muestra las ip y mascaras

COSTO DEL PROYECTO

DURACIÓN DE PROYECTO:

Fecha de inicio el de julio del año 2017

Fecha de finalización Enero del año 2017.

INVESTIGADORES:

José Luis Montecinos Segovia.

Wilber Javier Serrano Menjivar.

PRESUPUESTO:

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES. DNS, DHCP, LDAP, FIREWALL Y PROXY			
ACTIVIDAD	**CANTIDAD**	**PRECIO**	**TOTAL**
Computadoras	**2**	**$500.00**	**$1,000.00**
Energía Eléctrica	**5**	**$8.00**	**$40.00**
Viáticos	**5**	**$40.00**	**$200.00**
Uso de internet	**5**	**$10.00**	**$50.00**
Otros gastos	**1**	**$45.00**	**$45.00**
Materiales didácticos	**5**	**$10.00**	**$50.00**
MONTO TOTAL DEL PROYECTO			**$1,385.00**

CRONOGRAMA DE ACTIVIDADES

actividades	Junio				Diciembre			
Integración de grupos de trabajo								
Elección de proyecto								
Elaboración del perfil								
Pruebas de verificación de recursos								
Instalación de prueba del proyecto								
Instalación final								
Pruebas y seguimiento								

CONCLUSIÓN:

A lo largo de este proyecto aprendimos como estudiantes de la Universidad Luterana Salvadoreña la forma correcta de instalación y configuración de los servidores básicos para una red intranet, básicamente son en una red local en donde trabajan varias personas que comparten una misma finalidad laboral.También adquirimos habilidades de instalación de servicios, su función y como lo podemos configurar para tener una buena administración de servicios de red y cuales son las características de cada uno. La configuración de los servidores DHCP, DNS, LDAP, PROXYS Y FIREWALL la seguridad de nuestros equipos tecnológicos, concluimos que es de vital importancia de utilizar aprender a gestionar este tipo de servicios ya que sin ellos seria muy complicado lograr que el trabajo en una area de labores sea eficiente y eficaz para la gestión de los diversos servidores por su fácil manejo y configuración.

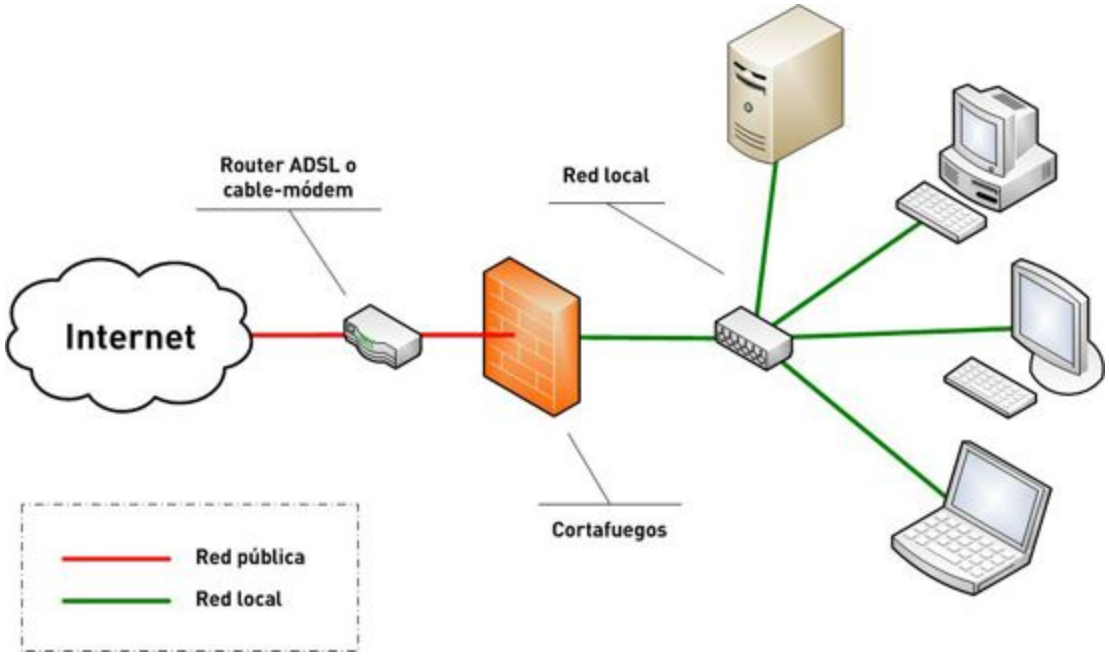
REFERENCIAS BIBLIOGRÁFICAS

Enlaces de Internet:

#	Enlace	Tema
1	http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/index.html. Se consultó el 11 dic.. 2017.	DNS y DHCP
2	http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns.html. Se consultó el 11 dic.. 2017.	Servidor DNS
3	http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7152&rep=rep1&type=pdf. Se consultó el 13 dic.. 2017.	Firewalls
4	https://es.wikipedia.org/wiki/Debian. Se consultó el 15 ene.. 2018	Debian
5	https://www.ecured.cu/VirtualBox. Se consultó el 15 ene.. 2018.	VirtualBox
6	https://albertomolina.wordpress.com/2009/01/09/nat-con-iptables/. Se consultó el 16 ene.. 2018.	NAT con iptables
7	https://wiki.archlinux.org/index.php/Dnsmasq_(Espa%C3%B1ol). Se consultó el 16 ene.. 2018.	DNSMASQ
8	https://es.wikipedia.org/wiki/Nslookup. Se consultó el 17 ene.. 2018.	Nslookup
9	http://francisconi.org/linux/comandos/dig. Se consultó el 17 ene.. 2018.	DIG
10	https://squidproxy.org/. Se consultó el 19 ene.. 2018.	Squid Proxy
11	https://wiki.debian.org/HowTo/dnsmasq. Se consultó el 17 ene.. 2018.	DNSMASQ
12	http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_y_dhcp_sencillo_con_dnsmasq.html. Se consultó el 17 ene.. 2018.	DNS y DHCP
13	https://es.wikipedia.org/wiki/Nmap. Se consultó el 19 ene.. 2018	NMAP
14	http://www.escomposlinux.org/lfs-es/lfs-es-5.0/appendixa/net-tools.html. Se consultó el 19 ene.. 2018.	Net-tools

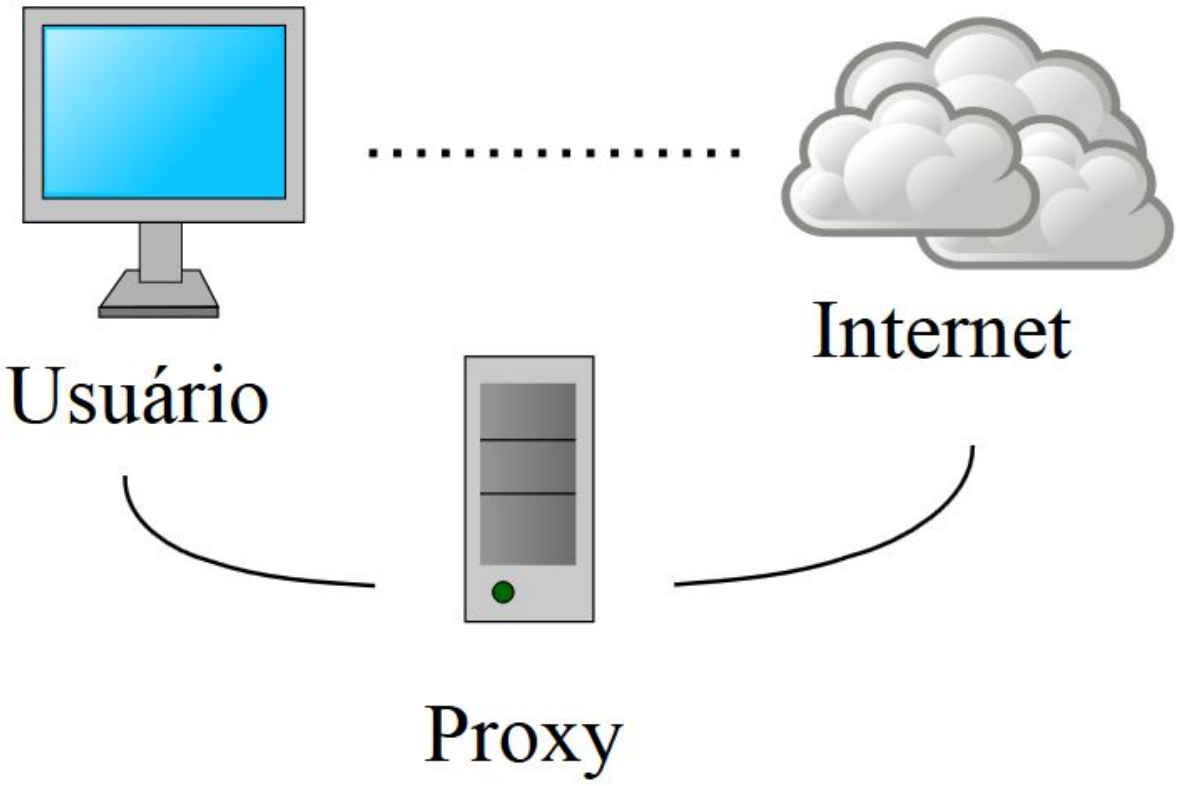
ANEXOS

Función del Firewall

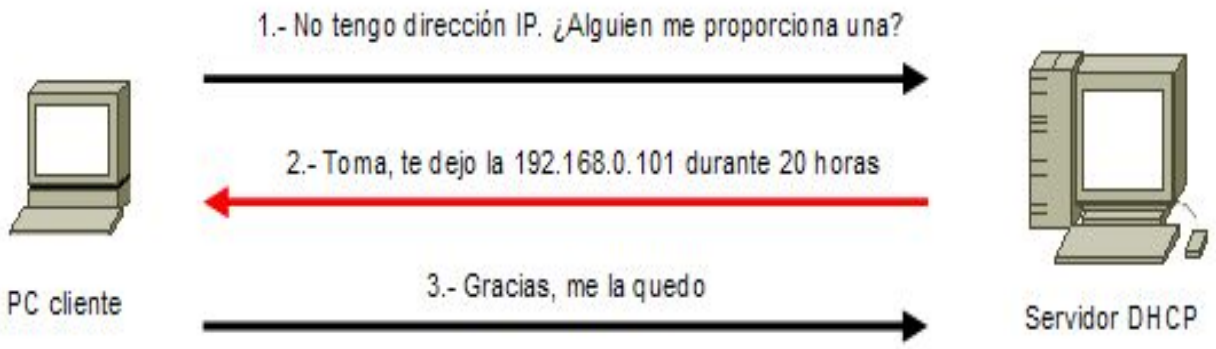


Función del DNS

Función Proxy

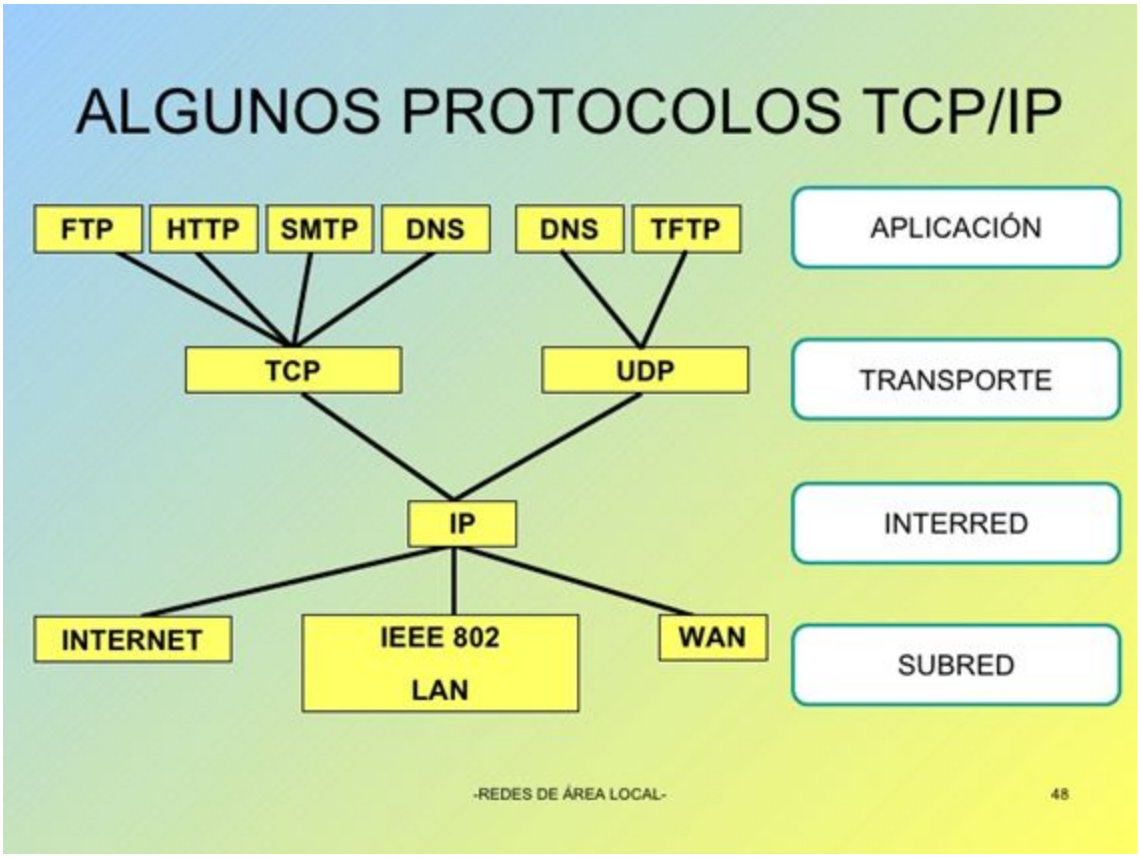


Función DHCP



Función del LDAP

www.SomeBooks.es



DESCRIPCIONES CORTAS DE HERRAMIENTAS QUE COMPRENDE NET-TOOLS

arp se usa para manipular la caché ARP del núcleo, usualmente para añadir o borrar una entrada o volcar la caché completa.

dnsdomainname muestra el nombre del dominio DNS del sistema.

domainname muestra o establece el nombre del dominio NIS/YP del sistema.

hostname muestra o establece el nombre del sistema actual.

ifconfig es la utilidad principal usada para configurar las interfaces de red.

nameif nombra interfaces de red basándose en las direcciones MAC.

netstat se usa para mostrar las conexiones de red, tablas de encaminamiento y estadísticas de las interfaces.

nisdomainname hace lo mismo que domainname.

rarp se usa para manipular la tabla RARP del núcleo.

route se usa para manipular la tabla de encaminamiento IP.

slattach conecta una interfaz de red a una línea serie. Esto permite usar líneas de terminales normales para crear enlaces punto a punto con otras computadoras.