

Trabajo Final de Grado Superior.



PROYECTO DE IMPLEMENTACIÓN TOTAL DE RASPBERRY PI Y LOS SISTEMAS DE COMUNICACIÓN DE CISCO VOIP - ASTERISK EN LA EMPRESA.

Integrantes del Proyecto:

Roberto Torres Molina
Jorge de la Serna Garay
Ruben Lopez Carrobles

Tutor del Proyecto:

Samuel Arranz

Descripción del proyecto

El proyecto lo hemos enfocado para un bufete de abogados en el cual implementaremos su red con Cisco y sus servicios con Raspberry Pi.

Centraremos el proyecto en las comunicaciones de voip, tanto para la tecnología de Cisco como la implementación de Asterisk en una Raspberry Pi.

El objetivo es poner en práctica sin previamente haberlo estudiado ni haberlo dado en clase, la tecnología de voip en una mediana o pequeña empresa. Ahorrando costes en los servidores con Raspberry Pi.

Implementaremos la tecnología de voip en dos modos, uno con Cisco y su medio de simulación Packet Tracer y otra con la configuración en una Raspberry Pi de Asterisk (**No se podrá probar debido a que no tenemos los medios a nuestra disposición**).

Otro de los objetivos secundarios es exprimir las capacidades de Raspberry Pi y de implementar esta tecnología al mundo de la empresa con el objetivo de que ejerza el mismo servicio que un servidor normal y caro pero con un precio muy bajo y un mantenimiento muy bajo.

El bufete de abogados Carrobles nos ha pedido el diseño de sus redes para las dos sedes que tienen tanto en Madrid como en Bilbao. Nos ha pedido que dichas sedes se comuniquen entre ellas con seguridad mediante una vpn, una de las sedes albergará el servidor web del bufete por lo que tendrá una DMZ en su red.

Tendremos que implementar la seguridad de cada sede con un Firewall, cada sede tendrá un servidor propio interno y cada una tendrá su propio servicio de voip interno.

Contenido

1. Objetivo y Planificación del proyecto

- 1.1. Objetivo
- 1.2. Planificación del proyecto

2. Implementar Raspberry Pi como servidor

- 2.1. Servicio dhcp con subinterfaces
- 2.2. Servicio ssh
- 2.3. Servicio dns
- 2.4. Servicio correo
- 2.5. Servicio web

3. Diseño y configuración de las redes

- 3.1. Diseño de la red
- 3.2. Configuración de las redes
 - 3.2.1. Sede Madrid
 - 3.2.2. Protocolos utilizados en la sede
 - 3.2.3. Sede Bilbao

4. Diseño y medidas de seguridad de las redes

- 4.1. Dmz
- 4.2. Vpn

5. Configuración de VoIp en Cisco y Raspberry-Asterisk

- 5.1. Conceptos generales de VoIp
 - 5.1.1. Protocolos
- 5.2. Configuración en Cisco
 - 5.2.1. Telefonía Cisco y centralitas
 - 5.2.2. Configuración de VoIp en Cisco
- 5.3. Configuración en Raspberry-Asterisk
 - 5.3.1. Conceptos de Asterisk y Raspberry Pi
 - 5.3.2. Instalacion y configuracion de Asterisk en Raspberry Pi

6. Bibliografía

1. Objetivo y planificación del proyecto

1.1. Objetivo

Los objetivos del proyecto son ver cómo es posible el desarrollo de un sistema de comunicaciones VoIp para la empresa utilizando software libre como Asterisk integrado en dispositivos de bajo costo como son las Raspberry Pi dando un resultado óptimo si los juntamos con proveedores de servicios de telefonía IP; también el uso del sistema de comunicación de VoIp de la empresa Cisco y su implementación en la red de la empresa.

Cada sede se tendrá un servidor Raspberry Pi donde aparte de tener los servicios comunes que debe ofrecer un servidor, tendrá instalado un sistemas de VoIp ya sea libre dentro de Raspberry como es Asterisk o fuera mediante un sistemas de VoIp propio de Cisco.

Otro de los objetivos secundario aunque no principal es la implementación de Raspberry Pi en la empresa, como forma de abaratar los costos de equipamiento Informático.

Los motivos por elegir Raspberry son:

- Es un sistema barato, ya que se pueden encontrar Raspberry Pi por menos de 40€.
- Tiene un tamaño pequeño que permite transportarlo de una forma más rápida y barata.
- Es muy fácil de clonar ya que sólo tenemos que clonar la tarjeta SD del Sistema.

1.2. Planificación del PROYECTO

<i>Nombre de la tarea</i>	<i>Días</i>	<i>Comienzo</i>	<i>Fin</i>
PLAN DE TRABAJO			
Definición del plan de trabajo	5	18/11/2014	24/11/2014
Entrega del plan de trabajo	0	24/11/2014	24/11/2014
INSTALACIÓN DE LOS SERVICIOS			
Servicio dhcp (Roberto)	2	21/03/2015	22/03/2015
Servicio ssh (Roberto)	1	29/03/2015	29/03/2015
Servicio dns (Rubén)	1	22/04/2015	22/04/2015
Servicio correo (Rubén)	1	23/04/2015	23/04/2015
Servicio web	3	01/05/2015	04/05/2015
DISEÑO Y CONFIGURACIÓN DE LA RED			
Diseño de la red	3	12/02/2015	15/02/2015
Configuración de las redes	10	02/05/2015	13/05/2015
Sede Madrid	5		
Sede Bilbao	5		
DISEÑO Y MEDIDAS DE SEGURIDAD			
Dmz	7	18/05/2015	25/05/2015
Vpn	4	18/05/2015	22/05/2015
CONFIGURACIÓN VOIP			
Configuración de VoIp en Cisco	5	-	-
Instalación de Asterisk en Raspberry Pi	6	-	-
Conf de Asterisk en Raspberry Pi	3	-	-

2. Implementación de Raspberry Pi como servidor

2.1. Servicio dhcp con subinterfaces

Definición del servicio:

El servicio dhcp lo que pretende es repartir un rango de ips para varios equipos que están conectados a la red. El servidor dhcp solo reparte ip no actúa como router.

Instalación del servicio dhcp:

```
sudo apt-get install isc-dhcp-server
```

```
sudo apt-get install network-manager
```

Instalamos el isc-dhcp-server que nos permitirá utilizar la raspberry como servidor dhcp y el network-manager para proporcionar direcciones en la subred con una sola tarjeta de red eth0.

Configuración del servidor dhcp:

Explicaremos los pasos a seguir para la instalación del servidor dhcp y las sub-interfaces

1)

Iremos al fichero `/etc/default/isc-dhcp-server` y añadimos las sub-interfaces correspondientes para que por cada vlan tenga una dirección ip.

```
# Separate multiple interfaces with spaces, e.g. eth
INTERFACES="eth0.2, eth0.3, eth0.4, eth0.5, eth0.6, eth0.7"
```

2)

Ahora vamos a configurar las diferentes ip para cada vlan.

Iremos al fichero `/etc/dhcp/dhcpd.conf` pero antes haremos una copia de seguridad de dicho fichero.

```
sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.backup
```

Ahora configuramos el servicio con las características generales y luego con las demás ip para las vlans.

```
#Identificacion del servidor dhcp

ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 259200;
max-lease-time 604800;
option ip-forwarding off;
option domain-name "carroblesabogados.local";
option domain-name-servers 8.8.8.8, 8.8.4.4;
```

En este apartado definimos las distintas subredes que vamos a tener.

```
#vlan 1 router salida a internet, vpn, servidor web
subnet 192.168.1.0 netmask 255.255.255.0
{
  range 192.168.1.1 192.168.1.240;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.1.255;
  option domain-name-servers 192.168.1.1;
}

#vlan 2 administradores / servidor
subnet 192.168.2.0 netmask 255.255.255.0
{
  range 192.168.2.1 192.168.2.6;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.2.255;
  option domain-name-servers 192.168.2.1;
}

#vlan 3 departamento penal
subnet 192.168.3.0 netmask 255.255.255.0
{
  range 192.168.3.2 192.168.3.110;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.3.255;
  option domain-name-servers 192.168.3.1;
}

#vlan 4 departamento Mercantil
subnet 192.168.4.0 netmask 255.255.255.0
{
  range 192.168.4.2 192.168.4.110;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.4.255;
  option domain-name-servers 192.168.4.1;
}
```

```
#vlan 5 departamento Laboral
subnet 192.168.5.0 netmask 255.255.255.0
{
  range 192.168.5.2 192.168.5.110;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.5.255;
  option domain-name-servers 192.168.5.1;
}

#vlan 6 wifi
subnet 192.168.6.0 netmask 255.255.255.0
{
  range 192.168.6.2 192.168.6.197;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.6.255;
  option domain-name-servers 192.168.6.1;
}

#vlan 7 VoIp
subnet 192.168.7.0 netmask 255.255.255.0
{
  range 192.168.7.2 192.168.7.90;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.7.255;
  option domain-name-servers 192.168.7.1;
}
```

Lo establecemos así para poder aglutinar las diferentes redes en una misma interfaz de salida. Reiniciamos el servicio.

```
sudo service isc-dhcp-server restart
```

Ahora ya tenemos repartidas las diferentes Ip para las diferentes vlans.

NOTA - No podemos comprobar el DHCP por qué necesitamos un switch para configurar las vlans y así repartir por cada canal el rango de ip. Esta simulación lo haremos en el Packet tracer de cisco donde si tenemos los medios para simularlo aunque sea virtualmente.

2.2. Servicio ssh

Descripción del servicio:

El servicio SSH es un protocolo de comunicaciones seguras entre dos sistemas usando una arquitectura cliente / servidor que permite conectarse a un host remotamente y de forma segura. SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener la contraseña de forma no encriptada.

Nosotros lo utilizaremos de dos modos, una con entorno terminal y otra con entorno gráfico. Con esto conseguimos que el administrador del servidor puede conectarse a nuestra raspberry desde un Putty o desde VNC para solucionar problemas o instalar remotamente cosas.

Instalación del servicio:

- 1) El servidor de por sí ya viene con ssh habilitado por lo que no hace falta instalarlo.

```
pi@raspberrypi ~ $ sudo apt-get install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
ssh ya está en su versión más reciente.
Los paquetes indicados a continuación se instalaron
```

- 2) Instalaremos el cliente también para conectarnos a otro servidor.

```
pi@raspberrypi ~ $ sudo apt-get install openssh-client
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssh-client ya está en su versión más reciente.
fijado openssh-client como instalado manualmente.
Los paquetes indicados a continuación se instalaron de
```

- 3) Instalaremos por último el VNC para conexiones remotas entornos gráficos.

```
pi@raspberrypi ~ $ sudo apt-get install tightvncserver
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
tightvncserver ya está en su versión más reciente.
```

Configuración del servicio:

- 1) Configurar el fichero `/etc/ssh/sshd_config` para evitar el acceso a root.

```
# What ports, IPs and protocols we listen for
Port 22
```

```
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes no
```

2) Habilitamos para ejecutar aplicaciones gráficas, esto nos permitirá utilizar el vnc.

```
X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no
```

3) Para iniciar el servicio vnc lo haremos de la siguiente forma

```
pi@raspberrypi ~ $ sudo vncserver :1 -geometry 128x800 -depth 16 -pixelformat rgb565
New 'X' desktop is raspberrypi:1
Starting applications specified in /root/.vnc/xstartup
log file is /root/.vnc/raspberrypi:1.log
```

NOTA- Este servicio solo es utilizado por los administradores de red como medio de comunicación a distancia entre el servidor y el cliente. Por lo que los demás trabajadores no podrán conectarse al servidor sin la clave y el usuario correspondiente.

2.3. Servicio dns

Definición del servicio:

DNS (Domain Name Server) es un sistema de nomenclatura para computadoras, asocia una información variada con nombres de dominio asignado a cada participante, función principal, traducir los nombres inteligibles en identificadores binarios.

Instalación del servicio:

```
pi@raspberrypi ~ $ sudo apt-get install dnsmasq
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  dnsmasq-base
Paquetes sugeridos:
  resolvconf
Se actualizarán los siguientes paquetes:
  dnsmasq dnsmasq-base
2 actualizados, 0 se instalarán, 0 para eliminar y 82 no actualizados.
Necesito descargar 372 kB de archivos.
Se liberarán 159 kB después de esta operación.
```

Configuración del servicio:

1) Configuramos el `/etc/dnsmasq.conf`

```
pi@raspberrypi ~ $ nano /etc/dnsmasq.conf
```

```
# Never forward plain names (without a dot or domain part)
domain-needed
# Never forward addresses in the non-routed address spaces.
bogus-priv
```

2) Configuramos el interfaz `eth0` y la lista de direcciones a la `192.168.1.0`

```
# If you want dnsmasq to listen for DHCP and DNS requests only on
# specified interfaces (and the loopback) give the name of the
# interface (eg eth0) here.
# Repeat the line for more than one interface.
interface=eth0
# Or you can specify which interface _not_ to listen on
#except-interface=
# Or which to listen on by address (remember to include 127.0.0.1 if
# you use this.)
listen-address=192.168.1.0
listen-address=127.0.0.1
```

3) Como direccion de dominio `carroblesabogados.org` seguidos por la ip de red

```
# Add domains which you want to force to an IP address here.
# The example below send any host in double-click.net to a local
# web-server.
address=/carroblesabogados.org/192.168.1.0
```

4) Modificamos el fichero `/etc/hosts`

```
pi@raspberrypi ~ $ sudo nano /etc/hosts
```

```
GNU nano 2.2.6 Fichero: /etc/hosts
127.0.0.1 localhost
127.0.0.1 raspberrypi
192.168.1.0 carroblesabogados.org
```

5) Modificamos el fichero `/etc/resolv.conf`

```
GNU nano 2.2.6 Fichero: /etc/resolv.conf
domain carroblesabogados.org
search carroblesabogados.org

nameserver 80.58.61.250
nameserver 80.58.61.254
nameserver 192.168.1.0
nameserver 127.0.0.1
```

2.4. Servicio de correo

Definición del servicio:

Un servidor de correo es una aplicación de red ubicada en un servidor de internet, el servidor de correo tiene como fin transportar una información entre distintos usuarios, habitualmente el uso del correo electrónico ha tenido y tiene como fin que un usuario pueda enviar información a otro, en nuestro caso implementaremos el servidor de correo mediante **Mozilla Thunderbird**.

Instalación del servicio (Postfix y Dovecot):

Primer paso realizamos un update del sistema para verificar que está actualizado.

```
pi@raspberrypi ~ $ sudo apt-get install postfix
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
postfix ya está en su versión más reciente.
```

Configuración del servicio Postfix:

```
pi@raspberrypi ~ $ sudo apt-get install dovecot-pop3d
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
dovecot-pop3d ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 84 no actualizados.
```

1) Para configurar postfix entraremos en `/etc/postfix/main.cf`,

```
pi@raspberrypi ~ $ nano /etc/postfix/main.cf
```

2) Crearemos el dominio para nuestro bufete el cual se llama **carroblesabogados.org**

```
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = raspberrypi
mydomain = carroblesabogados.org
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = $mydomain
mydestination = carroblesabogados.org, raspberrypi, localhost.localdomain
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = Maildir/
```

Configuración del servicio Dovecot:

1) Accedemos a `/etc/dovecot/dovecot.conf` y ajustamos para que solo haya servicio IPV4

```
# A comma separated list of IPs or hosts where to listen in for connections.  
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.  
# If you want to specify non-default ports or anything more complex,  
# edit conf.d/master.conf.  
listen = *
```

2) El protocolo que utilizaremos para el correo será POP3

```
# A config file can also be tried to be included without giving an error if  
# it's not found:  
!include_try local.conf  
protocols = pop3  
mail_location = maildir:~/Maildir
```

3) Para finalizar reiniciamos tanto **Postfix** como **Dovecot**

```
pi@raspberrypi ~ $ sudo service dovecot restart  
[ ok ] Restarting IMAP/POP3 mail server: dovecot.
```

```
pi@raspberrypi ~ $ sudo service postfix restart  
[ ok ] Stopping Postfix Mail Transport Agent: postfix.  
[ ok ] Starting Postfix Mail Transport Agent: postfix.
```

Mozilla Thunderbird



2.5 Servicio Web

1. Para crear una página web con PHP y Mysql, necesitaremos actualizar la raspberry antes de instalar los servicios correspondientes.

```

pi@raspberrypi ~ $ sudo apt-get update
Des:1 http://raspberrypi.collabora.com wheezy Release.gpg [836 B]
Des:2 http://mirrordirector.raspbian.org wheezy Release.gpg [490 B]
Des:3 http://raspberrypi.collabora.com wheezy Release [7.493 B]
Des:4 http://archive.raspberrypi.org wheezy Release.gpg [490 B]
Des:5 http://mirrordirector.raspbian.org wheezy Release [14,4 kB]
Des:6 http://archive.raspberrypi.org wheezy Release [15,4 kB]
Obj http://repository.wolfram.com stable Release.gpg
Des:7 http://raspberrypi.collabora.com wheezy/rpi armhf Packages [2.214 B]
Obj http://repository.wolfram.com stable Release
Des:8 http://mirrordirector.raspbian.org wheezy/main armhf Packages [6.903 kB]
Des:9 http://archive.raspberrypi.org wheezy/main armhf Packages [129 kB]
Ign http://raspberrypi.collabora.com wheezy/rpi Translation-es_C0
Ign http://raspberrypi.collabora.com wheezy/rpi Translation-es
Obj http://repository.wolfram.com stable/non-free armhf Packages
Ign http://raspberrypi.collabora.com wheezy/rpi Translation-en
Ign http://archive.raspberrypi.org wheezy/main Translation-es_C0
Ign http://archive.raspberrypi.org wheezy/main Translation-es
Ign http://archive.raspberrypi.org wheezy/main Translation-en
  
```

2. Después de haber actualizado el sistema, procedemos a instalar los servicios correspondientes.

Ejecutaremos el comando “sudo apt-get install apache2 php5 libapache2-mod-php5 “
También ejecutamos el comando “sudo apt-get install mysql-server mysql-client php5-mysql”

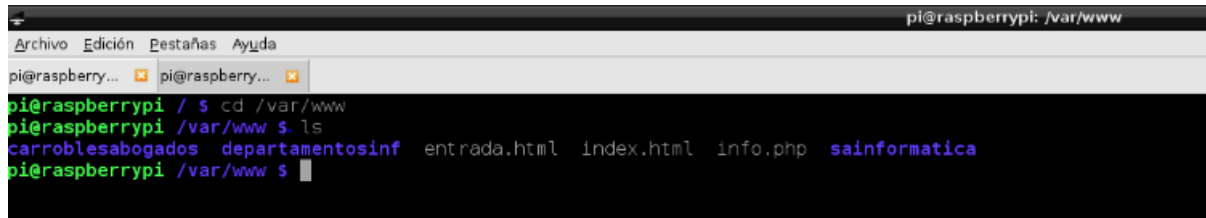
```

pi@raspberrypi ~ $ sudo apt-get install apache2 php5 libapache2-mod-php5
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya
libgnutls-openssl27 liblockfile-bin liblockfile1 squid-common squid-lang
Use 'apt-get autoremove' to remove them.
Se instalarán los siguientes paquetes extras:
php5-cli php5-common
  
```

```

pi@raspberrypi ~ $ sudo apt-get install mysql-server mysql-client php5-mysql
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya
libgnutls-openssl27 liblockfile-bin liblockfile1 squid-common squid-langpac
Use 'apt-get autoremove' to remove them.
Se instalarán los siguientes paquetes extras:
libhtml-libgd-perl perl-libgd-perl perl-libhtml-template-perl libimage-ident
  
```

3. Una vez hayamos instalado el servicio php5-mysql, nuestra web deberá estar guardada en la ruta “/var/www/nombre_de_la_web” para que podamos acceder a la web desde cualquier ordenador.

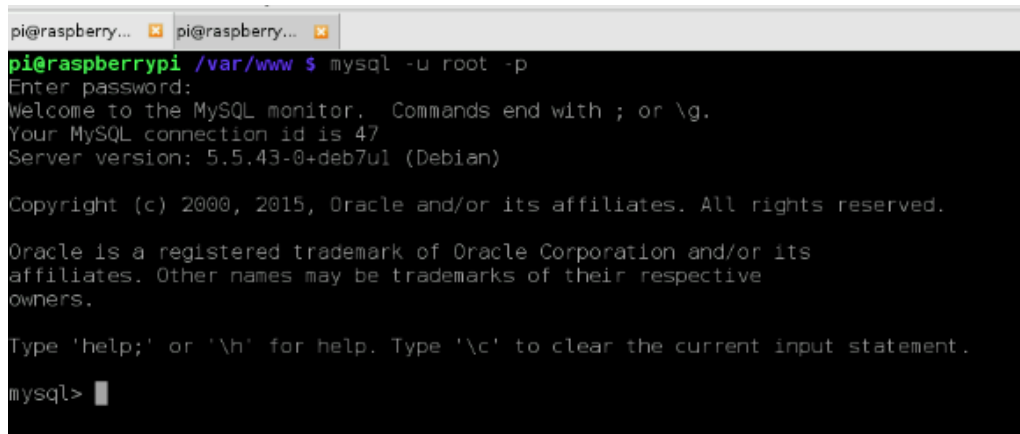


```

pi@raspberrypi: /var/www
Archivo Edición Pestañas Ayuda
pi@raspberrypi... x pi@raspberrypi... x
pi@raspberrypi / $ cd /var/www
pi@raspberrypi /var/www $ ls
carroblesabogados departamentosinf entrada.html index.html info.php sainformatica
pi@raspberrypi /var/www $

```

4. Una vez hayamos instalado los servicios necesarios para crear una página web con base de datos, comprobamos que podemos acceder a la base de datos de la página web.



```

pi@raspberrypi /var/www $ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 47
Server version: 5.5.43-0+deb7u1 (Debian)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

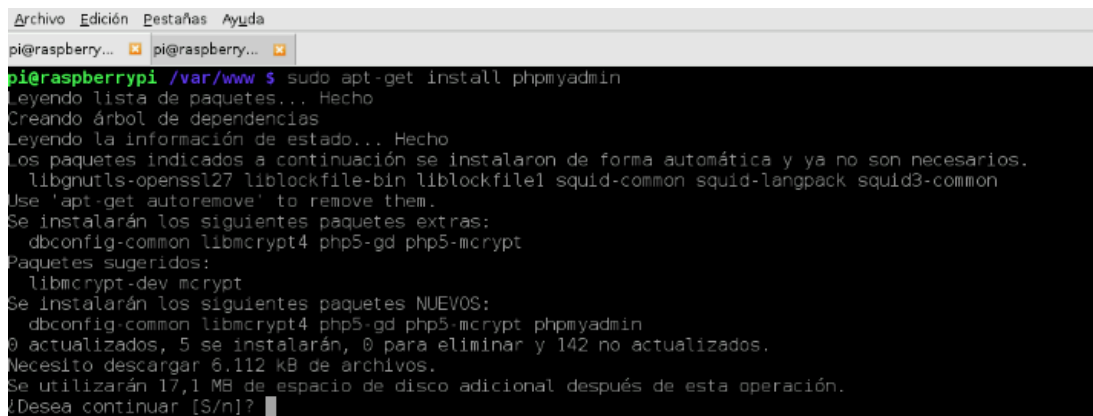
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

```

5. Si necesitamos instalar el entorno gráfico de la base de datos, utilizamos el comando “sudo apt-get install phpmyadmin”.

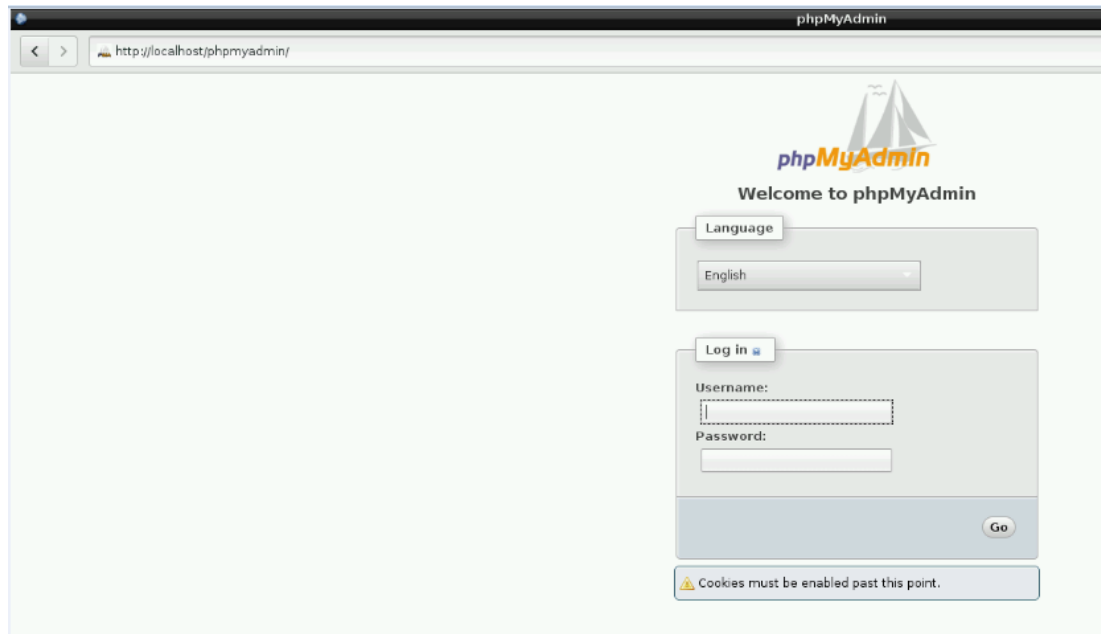


```

pi@raspberrypi /var/www $ sudo apt-get install phpmyadmin
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libgnutls-openssl17 liblockfile-bin liblockfile1 squid-common squid-langpack squid3-common
Use 'apt-get autoremove' to remove them.
Se instalarán los siguientes paquetes extras:
  dbconfig-common libmcrypt4 php5-gd php5-mcrypt
Paquetes sugeridos:
  libmcrypt-dev mcrypt
Se instalarán los siguientes paquetes NUEVOS:
  dbconfig-common libmcrypt4 php5-gd php5-mcrypt phpmyadmin
0 actualizados, 5 se instalarán, 0 para eliminar y 142 no actualizados.
Necesito descargar 6.112 kB de archivos.
Se utilizarán 17,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?

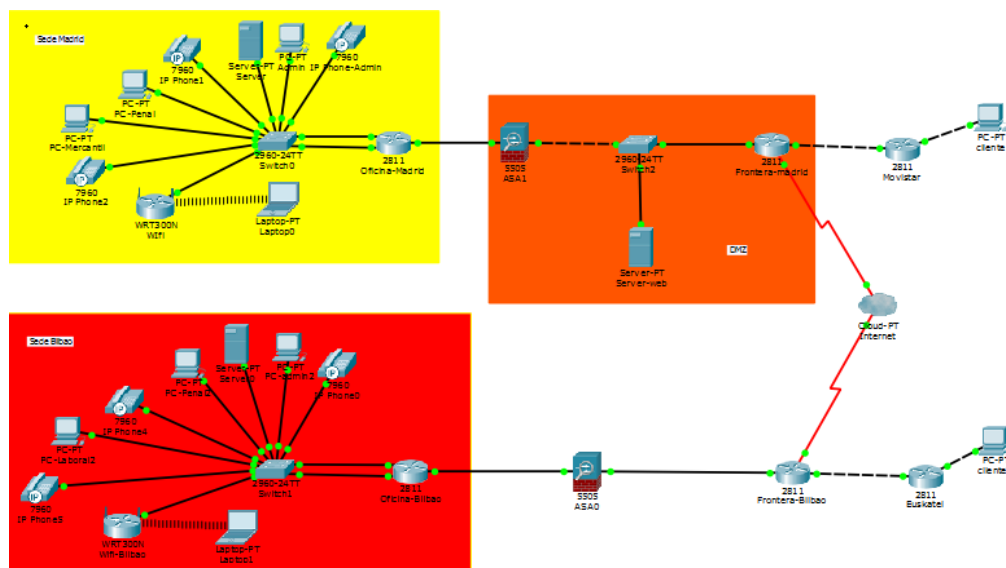
```

6. Podemos comprobar desde la url “localhost/phpmyadmin” que accedemos al entorno gráfico de la base de datos de la web.



3. Diseño y configuración de las redes

3.1. Diseño de la red



El diseño se ha centrado en la unión de las dos sedes, por medio de una vpn. Cada sede es independiente de la una aunque tengan un canal de comunicación vpn.

Cada sede tiene repartida la siguiente distribución:

- Directivo General
- Departamento de informática

- Departamento Laboral
- Departamento Mercantil
- Departamento Judicial
- Telefonía Voip
- Servidor
- Wifi

También tendrá cada sede un Firewall como medida de protección para no permitir las conexiones desde el exterior al interior de las oficinas evitando los ataques a la red.

La sede Madrid albergará el servidor web, donde como medida de seguridad se pondrá una dmz para hacer accesible a los clientes a la web pero así evitar la intrusión de atacantes a la red interna

3.2 Configuración de las redes

3.2.1. Sede Madrid

- Configuración básica de los routers:

Router frontera de la sede Madrid

```
Router(config)#hostname Frontera-Madrid
Frontera-Madrid(config)#enable secret class
Frontera-Madrid(config)#line con 0
Frontera-Madrid(config-line)#password cisco
Frontera-Madrid(config-line)#login
Frontera-Madrid(config-line)#exit
Frontera-Madrid(config)#line vty 0 4
Frontera-Madrid(config-line)#password cisco
Frontera-Madrid(config-line)#login
Frontera-Madrid(config-line)#end
Frontera-Madrid#
!SYS-5-CONFIG_I: Configured from console by console

Frontera-Madrid#copy runn
Frontera-Madrid#copy running-config star
Frontera-Madrid#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Router de la oficina de Madrid

```

Router(config)#hostname Oficina-Madrid
Oficina-Madrid(config)#enable se
Oficina-Madrid(config)#enable secret class
Oficina-Madrid(config)#
Oficina-Madrid(config)#line
Oficina-Madrid(config)#line con 0
Oficina-Madrid(config-line)#pass
Oficina-Madrid(config-line)#password cisco
Oficina-Madrid(config-line)#login
Oficina-Madrid(config-line)#line au
Oficina-Madrid(config-line)#line vty 0 4
Oficina-Madrid(config-line)#pass
Oficina-Madrid(config-line)#password cisco
Oficina-Madrid(config-line)#login
Oficina-Madrid(config-line)#end
Oficina-Madrid#
%SYS-5-CONFIG_I: Configured from console by console

Oficina-Madrid#
Oficina-Madrid#
Oficina-Madrid#copy runn
Oficina-Madrid#copy running-config str
Oficina-Madrid#copy running-config star
Oficina-Madrid#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

- Configuración de la subinterfases del Router.

1) Configuración de la subinterfases en la interfaz Fa0/1

```

Oficina-Madrid(config)#inter fa0/1.10
Oficina-Madrid(config-subif)#encapsulation dot1Q 10
Oficina-Madrid(config-subif)#ip address 192.168.10.1 255.255.255.0
Oficina-Madrid(config-subif)#exit
Oficina-Madrid(config)#inter fa0/1.11
Oficina-Madrid(config-subif)#encapsulation dot1Q 11
Oficina-Madrid(config-subif)#ip address 192.168.11.1 255.255.255.0
Oficina-Madrid(config-subif)#exit
Oficina-Madrid(config-subif)#inter fa0/1.12
Oficina-Madrid(config-subif)#encapsulation dot1Q 12
Oficina-Madrid(config-subif)#ip address 192.168.12.1 255.255.255.0
Oficina-Madrid(config-subif)#exit
Oficina-Madrid(config)#inter fa0/1.16
Oficina-Madrid(config-subif)#encapsulation dot1Q 16
Oficina-Madrid(config-subif)#ip address 192.168.16.1 255.255.255.0
Oficina-Madrid(config-subif)#exit

```

2) Configuración de la subinterfaces en la interfaz Fa1/1

```
Oficina-Madrid(config-if)#inter fa1/1.13
Oficina-Madrid(config-subif)#encapsulation dot1Q 13
Oficina-Madrid(config-subif)#ip address 192.168.13.1 255.255.255.0
Oficina-Madrid(config-subif)#exit
Oficina-Madrid(config)#inter fa1/1.14
Oficina-Madrid(config-subif)#encapsulation dot1Q 14
Oficina-Madrid(config-subif)#ip address 192.168.14.1 255.255.255.0
Oficina-Madrid(config-subif)#exit
Oficina-Madrid(config)#inter fa1/1.15
Oficina-Madrid(config-subif)#encapsulation dot1Q 15
Oficina-Madrid(config-subif)#ip address 192.168.15.1 255.255.255.0
Oficina-Madrid(config-subif)#exit
```

- Configuración red DMZ y conexión exterior

```
Oficina-Madrid(config)#inter f0/0
Oficina-Madrid(config-if)#ip address 192.168.5.2 255.255.255.0
Oficina-Madrid(config-if)#no shutdown
```

- Configuración del DHCP en el Router

```
Oficina-Madrid(config)#ip dhcp pool servidor
Oficina-Madrid(dhcp-config)#network 192.168.10.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.10.1
Oficina-Madrid(dhcp-config)#exit
Oficina-Madrid(config)#ip dhcp pool voip
Oficina-Madrid(dhcp-config)#network 192.168.15.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.15.1
Oficina-Madrid(dhcp-config)#exit
Oficina-Madrid(config)#ip dhcp pool wifi
Oficina-Madrid(dhcp-config)#network 192.168.14.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.14.1
Oficina-Madrid(dhcp-config)#exit
Oficina-Madrid(config)#ip dhcp pool penal
Oficina-Madrid(dhcp-config)#network 192.168.11.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.11.1
Oficina-Madrid(dhcp-config)#exit
Oficina-Madrid(config)#ip dhcp pool mercantil
Oficina-Madrid(dhcp-config)#network 192.168.12.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.12.1
Oficina-Madrid(dhcp-config)#exit
```

```
Oficina-Madrid(config)#ip dhcp pool laboral
Oficina-Madrid(dhcp-config)#network 192.168.13.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.13.1
Oficina-Madrid(dhcp-config)#exit
Oficina-Madrid(config)#ip dhcp pool administración
Oficina-Madrid(dhcp-config)#network 192.168.16.0 255.255.255.0
Oficina-Madrid(dhcp-config)#default-router 192.168.16.1
Oficina-Madrid(dhcp-config)#exit
```

- Excluir ips y rangos de ips en el dhcp

```
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.10.1
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.11.1
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.12.1
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.13.1
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.14.1
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.15.1
Oficina-Madrid(config)#ip dhcp excluded-address 192.168.16.1
```

- Configuración de las vlans del swicht-Madrid
- Creación de las Vlans

```
Swicht-Oficina-Madrid#vlan database
Swicht-Oficina-Madrid(vlan)#vlan 10 name servidor
VLAN 10 added:
Name: servidor
Swicht-Oficina-Madrid(vlan)#vlan 11 name penal
VLAN 11 added:
Name: penal
Swicht-Oficina-Madrid(vlan)#vlan 12 name mercantil
VLAN 12 added:
Name: mercantil
Swicht-Oficina-Madrid(vlan)#vlan 13 name laboral
VLAN 13 added:
Name: laboral
Swicht-Oficina-Madrid(vlan)#vlan 14 name wifi
VLAN 14 added:
Name: wifi
Swicht-Oficina-Madrid(vlan)#vlan 15 name Voip
VLAN 15 added:
```

Name: Voip

Swicht-Oficina-Madrid(vlan)#vlan 16 name administracion

VLAN 16 added:

Name: administracion

- Enlaces troncales

Swicht-oficina_Madrid(config)#interface gigabitEthernet 0/2

Swicht-oficina_Madrid(config-if)#switchport mode trunk

Swicht-oficina_Madrid(config-if)#exit

Swicht-oficina_Madrid(config)#interface gigabitEthernet 0/1

Swicht-oficina_Madrid(config-if)#switchport mode trunk

Swicht-oficina_Madrid(config-if)#exit

- Configuración de la vlans en la interfaces.

Swicht-Oficina-Madrid(config)#interface fa0/2

Swicht-Oficina-Madrid(config-if)#switchport access vlan 10

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

Swicht-Oficina-Madrid(config)#interface fa0/3

Swicht-Oficina-Madrid(config-if)#switchport access vlan 15

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

Swicht-Oficina-Madrid(config)#interface fa0/4

Swicht-Oficina-Madrid(config-if)#switchport access vlan 11

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

Swicht-Oficina-Madrid(config)#interface fa0/5

Swicht-Oficina-Madrid(config-if)#switchport access vlan 15

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

Swicht-Oficina-Madrid(config)#interface fa0/6

Swicht-Oficina-Madrid(config-if)#switchport access vlan 12

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

Swicht-Oficina-Madrid(config)#interface fa0/7

Swicht-Oficina-Madrid(config-if)#switchport access vlan 15

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

Swicht-Oficina-Madrid(config)#interface fa0/8

Swicht-Oficina-Madrid(config-if)#switchport access vlan 13

Swicht-Oficina-Madrid(config-if)#switchport mode access

Swicht-Oficina-Madrid(config-if)#exit

```
Swicht-Oficina-Madrid(config)#interface fa0/9
Swicht-Oficina-Madrid(config-if)#switchport access vlan 14
Swicht-Oficina-Madrid(config-if)#switchport mode access
Swicht-Oficina-Madrid(config-if)#exit
Swicht-Oficina-Madrid(config)#interface fa0/10
Swicht-Oficina-Madrid(config-if)#switchport access vlan 16
Swicht-Oficina-Madrid(config-if)#switchport mode access
Swicht-Oficina-Madrid(config-if)#exit
```

- Poner los enlaces troncales

```
Swicht-Oficina-Madrid(config)#interface gi0/1
Swicht-Oficina-Madrid(config-if)#switchport mode trunk
Swicht-Oficina-Madrid(config-if)#exit
Swicht-Oficina-Madrid(config)#interface gi0/2
Swicht-Oficina-Madrid(config-if)#switchport mode trunk
Swicht-Oficina-Madrid(config-if)#exit
```

1. Router frontera Madrid
- Configuración salida al proveedor de internet

```
Frontera-Madrid(config)#interface fa0/1
Frontera-Madrid(config-if)#ip address 200.69.216.2 255.255.255.252
Frontera-Madrid(config-if)#no shutdown
```

- Configuración conexión con la sede de Bilbao

```
Frontera-Madrid(config)#interface se1/0
Frontera-Madrid(config-if)#ip address 200.45.0.2 255.255.255.252
Frontera-Madrid(config-if)#no shutdown
```

3.2.2. Protocolos utilizados en las sedes

- Protocolo NAT

NAT es un protocolo para enrutar direcciones públicas de internet, por eso solo es viable con direcciones externas no internas o privadas.

- Configuración router frontera Madrid

```
Frontera-Madrid(config)#ip nat pool Red-internet 200.69.216.2 200.45.0.2 netmask
255.255.255.252
```

```
%Pool Red-internet mask 255.255.255.252 too small; should be at least 0.0.0.0
%Start and end addresses on different subnets
```

- Lista de acl para la nat

```
Frontera-Madrid(config)#ip access-list extended NAT
Frontera-Madrid(config-ext-nacl)#permit ip 0.0.0.0 0.0.0.0 any
Frontera-Madrid(config-ext-nacl)#exit
```

- Introducir la nat en las interfaces

```
Frontera-Madrid(config)#ip nat inside source list NAT pool Red-internet
Frontera-Madrid(config)#inter se1/0
Frontera-Madrid(config-if)#ip nat inside
Frontera-Madrid(config-if)#exit
Frontera-Madrid(config)#interface fa0/1
Frontera-Madrid(config-if)#ip nat inside
Frontera-Madrid(config-if)#exit
```

- **Protocolo RIP**

El protocolo Routing Information Protocol (RIP) es un protocolo de enrutamiento del tipo vector distancia. Los protocolos de enrutamiento vector distancia calculan la mejor ruta para encaminar los paquetes IP hacia su destino correspondiente utilizando como métrica el número de saltos (Hop Count). RIP soporta un máximo de 15 saltos. Cualquier ruta que esté a más de 15 saltos se considera inalcanzable.

Otra característica de los protocolos de enrutamiento vector distancia es que utilizan un reloj (Timer) para anunciar la tabla de enrutamiento a los demás routers en la red WAN.

- Configuración de en el router oficina madrid.

```
Oficina-Madrid(config)#router rip
Oficina-Madrid(config-router)#version 2
Oficina-Madrid(config-router)#net
Oficina-Madrid(config-router)#network 192.168.10.0
Oficina-Madrid(config-router)#network 192.168.11.0
Oficina-Madrid(config-router)#network 192.168.12.0
Oficina-Madrid(config-router)#network 192.168.13.0
Oficina-Madrid(config-router)#network 192.168.14.0
Oficina-Madrid(config-router)#network 192.168.15.0
Oficina-Madrid(config-router)#network 192.168.16.0
Oficina-Madrid(config-router)#exit
```

NOTA- Estos protocolos son los mismos empleados en la sede de Bilbao, nos abstenemos en ponerlo de nuevo ya que es lo mismo solo que cambian las sedes.

3.2.3 Sede Bilbao

- Configuración básica de los routers:

Router frontera de la sede Bilbao

```

Router_Salida_Bilbao#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Salida_Bilbao(config)#hostname Router-Salida_Bilbao
Router-Salida_Bilbao(config)#enable secret cisco
Router-Salida_Bilbao(config)#line con 0
Router-Salida_Bilbao(config-line)#passw
Router-Salida_Bilbao(config-line)#password cisco
Router-Salida_Bilbao(config-line)#login
Router-Salida_Bilbao(config-line)#exit
Router-Salida_Bilbao(config)#line vty 0 4
Router-Salida_Bilbao(config-line)#password class
Router-Salida_Bilbao(config-line)#login
Router-Salida_Bilbao(config-line)#end
Router-Salida_Bilbao#
%SYS-5-CONFIG_I: Configured from console by console

Router-Salida_Bilbao#copy r
Router-Salida_Bilbao#copy running-config s
Router-Salida_Bilbao#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Router de la oficina de Bilbao

```

Oficina_Bilbao#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Oficina_Bilbao(config)#hostname Oficina-Bilbao
Oficina-Bilbao(config)#enable secret cisco
Oficina-Bilbao(config)#line con 0
Oficina-Bilbao(config-line)#password cisco
Oficina-Bilbao(config-line)#login
Oficina-Bilbao(config-line)#exit
Oficina-Bilbao(config)#line vty 0 4
Oficina-Bilbao(config-line)#password class
Oficina-Bilbao(config-line)#login
Oficina-Bilbao(config-line)#end
Oficina-Bilbao#
%SYS-5-CONFIG_I: Configured from console by console

Oficina-Bilbao#cop r
Oficina-Bilbao#cop running-config s
Oficina-Bilbao#cop running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

- Configuración de la subinterfaces del Router.

1) Configuración de la subinterfaces en la interfaz Fa0/0

```
Oficina-Bilbao(config)#inter fa0/0.18
Oficina-Bilbao(config-subif)#encapsulation dot1Q 18
Oficina-Bilbao(config-subif)#ip address 192.168.18.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
Oficina-Bilbao(config)#inter fa0/0.19
Oficina-Bilbao(config-subif)#encapsulation dot1Q 19
Oficina-Bilbao(config-subif)#ip address 192.168.19.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
Oficina-Bilbao(config-subif)#inter fa0/0.20
Oficina-Bilbao(config-subif)#encapsulation dot1Q 20
Oficina-Bilbao(config-subif)#ip address 192.168.20.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
Oficina-Bilbao(config-subif)#inter fa0/0.21
Oficina-Bilbao(config-subif)#encapsulation dot1Q 21
Oficina-Bilbao(config-subif)#ip address 192.168.21.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
```

2) Configuración de la subinterfases en la interfaz Fa0/1

```
Oficina-Bilbao(config)#inter fa0/1.22
Oficina-Bilbao(config-subif)#encapsulation dot1Q 22
Oficina-Bilbao(config-subif)#ip address 192.168.22.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
Oficina-Bilbao(config-subif)#inter fa0/1.23
Oficina-Bilbao(config-subif)#encapsulation dot1Q 23
Oficina-Bilbao(config-subif)#ip address 192.168.23.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
Oficina-Bilbao(config)#inter fa0/1.24
Oficina-Bilbao(config-subif)#encapsulation dot1Q 24
Oficina-Bilbao(config-subif)#ip address 192.168.24.1 255.255.255.0
Oficina-Bilbao(config-subif)#exit
```

- Configuración del DHCP en el Router

```
Oficina-Bilbao(config)#ip dhcp pool servidor
Oficina-Bilbao(dhcp-config)#network 192.168.18.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.18.1
Oficina-Bilbao(dhcp-config)#exit
Oficina-Bilbao(config)#ip dhcp pool voip
Oficina-Bilbao(dhcp-config)#network 192.168.19.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.19.1
Oficina-Bilbao(dhcp-config)#exit
```

```
Oficina-Bilbao(config)#ip dhcp pool wifi
Oficina-Bilbao(dhcp-config)#network 192.168.24.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.24.1
Oficina-Bilbao(dhcp-config)#exit
Oficina-Bilbao(config)#ip dhcp pool penal
Oficina-Bilbao(dhcp-config)#network 192.168.21.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.21.1
Oficina-Bilbao(dhcp-config)#exit
Oficina-Bilbao(config)#ip dhcp pool mercantil
Oficina-Bilbao(dhcp-config)#network 192.168.23.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.23.1
Oficina-Bilbao(dhcp-config)#exit
Oficina-Bilbao(config)#ip dhcp pool laboral
Oficina-Bilbao(dhcp-config)#network 192.168.22.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.22.1
Oficina-Bilbao(dhcp-config)#exit
Oficina-Bilbao(config)#ip dhcp pool administración
Oficina-Bilbao(dhcp-config)#network 192.168.20.0 255.255.255.0
Oficina-Bilbao(dhcp-config)#default-router 192.168.20.1
Oficina-Bilbao(dhcp-config)#exit
```

- Excluir ips y rangos de ips en el dhcp

```
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.18.1
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.19.1
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.20.1
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.21.1
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.22.1
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.23.1
Oficina-Bilbao(config)#ip dhcp excluded-address 192.168.24.1
```

- Configuración de las vlans del swicht-Madrid
- Creación de las Vlans

```
Swicht-Oficina-Bilbao#vlan database
Swicht-Oficina-Bilbao(vlan)#vlan 18 name servidor
VLAN 18 added:
Name: servidor
Swicht-Oficina-Bilbao(vlan)#vlan 19 name Voip
VLAN 19 added:
Name: Voip
Swicht-Oficina-Bilbao(vlan)#vlan 20 name administracion
```

VLAN 20 added:

Name: administracion

Swicht-Oficina-Bilbao(vlan)#vlan 21 name penal

VLAN 21 added:

Name: laboral

Swicht-Oficina-Bilbao(vlan)#vlan 22 name laboral

VLAN 22 added:

Name: laboral

Swicht-Oficina-Bilbao(vlan)#vlan 23 name mercantil

VLAN 23 added:

Name: mercantil

Swicht-Oficina-Bilbao(vlan)#vlan 24 name wifi

VLAN 16 added:

Name: wifi

- Enlaces troncales

Swicht-oficina_Bilbao(config)#interface gigabitEthernet 0/1

Swicht-oficina_Bilbao(config-if)#switchport mode trunk

Swicht-oficina_Bilbao(config-if)#exit

Swicht-oficina_Bilbao(config)#interface gigabitEthernet 0/2

Swicht-oficina_Bilbao(config-if)#switchport mode trunk

Swicht-oficina_Bilbao(config-if)#exit

- Configuración de la vlans en la interfaces.

Swicht-Oficina-Bilbao(config)#interface fa0/1

Swicht-Oficina-Bilbao(config-if)#switchport access vlan 20

Swicht-Oficina-Bilbao(config-if)#switchport mode access

Swicht-Oficina-Bilbao(config-if)#exit

Swicht-Oficina-Bilbao(config)#interface fa0/2

Swicht-Oficina-Bilbao(config-if)#switchport access vlan 18

Swicht-Oficina-Bilbao(config-if)#switchport mode access

Swicht-Oficina-Bilbao(config-if)#exit

Swicht-Oficina-Bilbao(config)#interface fa0/3

Swicht-Oficina-Bilbao(config-if)#switchport access vlan 19

Swicht-Oficina-Bilbao(config-if)#switchport mode access

Swicht-Oficina-Bilbao(config-if)#exit

Swicht-Oficina-Bilbao(config)#interface fa0/4

Swicht-Oficina-Bilbao(config-if)#switchport access vlan 21

Swicht-Oficina-Bilbao(config-if)#switchport mode access

Swicht-Oficina-Bilbao(config-if)#exit

Swicht-Oficina-Bilbao(config)#interface fa0/5

Swicht-Oficina-Bilbao(config-if)#switchport access vlan 19

Swicht-Oficina-Bilbao(config-if)#switchport mode access

```
Swicht-Oficina-Bilbao(config-if)#exit
Swicht-Oficina-Bilbao(config)#interface fa0/6
Swicht-Oficina-Bilbao(config-if)#switchport access vlan 22
Swicht-Oficina-Bilbao(config-if)#switchport mode access
Swicht-Oficina-Bilbao(config-if)#exit
```

```
Swicht-Oficina-Bilbao(config)#interface fa0/7
Swicht-Oficina-Bilbao(config-if)#switchport access vlan 23
Swicht-Oficina-Bilbao(config-if)#switchport mode access
Swicht-Oficina-Bilbao(config-if)#exit
Swicht-Oficina-Bilbao(config)#interface fa0/8
Swicht-Oficina-Bilbao(config-if)#switchport access vlan 19
Swicht-Oficina-Bilbao(config-if)#switchport mode access
Swicht-Oficina-Bilbao(config-if)#exit
Swicht-Oficina-Bilbao(config)#interface fa0/9
Swicht-Oficina-Bilbao(config-if)#switchport access vlan 24
Swicht-Oficina-Bilbao(config-if)#switchport mode access
Swicht-Oficina-Bilbao(config-if)#exit
```

- Poner los enlaces troncales

```
Swicht-Oficina-Bilbao(config)#interface gi0/1
Swicht-Oficina-Bilbao(config-if)#switchport mode trunk
Swicht-Oficina-Bilbao(config-if)#exit
Swicht-Oficina-Bilbao(config)#interface gi0/2
Swicht-Oficina-Bilbao(config-if)#switchport mode trunk
Swicht-Oficina-Bilbao(config-if)#exit
```

2. Router frontera Bilbao

- Configuración salida al proveedor de internet

```
Frontera-Bilbao(config)#interface fa0/1
Frontera-Bilbao(config-if)#ip address 200.69.218.2 255.255.255.252
Frontera-Bilbao(config-if)#no shutdown
```

- Configuración conexión con la sede de Madrid

```
Frontera-Bilbao(config)#interface se1/0
Frontera-Bilbao(config-if)#ip address 200.45.0.1 255.255.255.252
Frontera-Bilbao(config-if)#no shutdown
```

4. Diseño y medidas de seguridad de las redes

4.1. Configuración Asa-Dmz

- DMZ es una zona segura que se ubica entre la red interna de la oficina y la red externa (internet). El objetivo de la DMZ es que las conexiones de la red interna y externa estén permitidas.
- Ejecutando este comando, deshabilitamos el dhcp para que no nos de problemas a la hora de configurar el DMZ.

```
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside  
ciscoasa(config)#no dhcpd auto_config outside
```

- Configuramos cada vlan con su IP y nombre correspondiente.

```
ciscoasa(config)#interface vlan1  
ciscoasa(config-if)#ip address 192.168.5.1 255.255.255.0  
ciscoasa(config-if)#exit  
ciscoasa(config)#interface vlan2  
ciscoasa(config-if)#ip address 192.168.4.2 255.255.255.0  
ciscoasa(config-if)#nameif outside-madrid  
ciscoasa(config-if)#security-level 0  
ciscoasa(config-if)#exit  
ciscoasa(config)#interface vlan3  
ciscoasa(config-if)#no forward interface vlan2  
ciscoasa(config-if)#nameif dmz-madrid  
ciscoasa(config-if)#security-level 50  
ciscoasa(config-if)#ip address 192.168.4.10 255.255.255.0  
ciscoasa(config-if)#exit  
ciscoasa(config)#interface ethernet 0/0  
ciscoasa(config-if)#switchport access vlan 1  
ciscoasa(config-if)#exit  
ciscoasa(config)#interface ethernet 0/1  
ciscoasa(config-if)#switchport access vlan 2  
ciscoasa(config-if)#exit  
ciscoasa(config)#interface ethernet 0/2  
ciscoasa(config-if)#switchport access vlan 3  
ciscoasa(config-if)#exit
```

- Configuración NAT para permitir que los hosts salgan a Internet

```
ciscoasa(config)#object network inside-subnet
ciscoasa(config-network-object)#subnet 192.168.0.0 255.255.0.0
ciscoasa(config-network-object)#nat (inside,outside-madrid) dynamic interface
ciscoasa(config-network-object)#exit
ciscoasa(config)#object network dmz-subnet
ciscoasa(config-network-object)#subnet 192.168.4.0 255.255.255.0
ciscoasa(config-network-object)#nat (dmz,outside-madrid) dynamic interface
ciscoasa(config-network-object)#exit
ciscoasa(config)#object network webserver
ciscoasa(config-network-object)#host 192.168.4.10
ciscoasa(config-network-object)#nat (dmz,outside-madrid) static 192.168.4.2
ciscoasa(config-network-object)#exit
```

NOTA-Este proceso se hará también en la sede de Bilbao, se omite repetir los pasos de Bilbao pero serían los mismos nada más que modificando las IPS, interfaces, etc.....

4.2. Vpn

- VPN es una red privada virtual que permite una conexión segura entre una red interna e internet.
- Para crear la VPN, utilizaremos una clave -precompartida, encriptación AES, con tiempo de vida de 86400 segundos, con la llave "VPN" y parámetro que define las políticas de seguridad con el nombre REDES.

```
Frontera-Madrid(config)#crypto isakmp policy 10
Frontera-Madrid(config-isakmp)#authentication pre-share
Frontera-Madrid(config-isakmp)#has sha
Frontera-Madrid(config-isakmp)#encryption aes 256
Frontera-Madrid(config-isakmp)#group 2
Frontera-Madrid(config-isakmp)#lifetime 86400
Frontera-Madrid(config-isakmp)#exit
Frontera-Madrid(config)#crypto isakmp key vpn address 200.46.0.2
Frontera-Madrid(config)#crypto ipsec transform-set REDES esp-aes esp-sha-hmac
Frontera-Madrid(config)#access-list 101 permit ip 192.168.0.0 0.0.31.255 192.168.0.0
0.0.31.255
Frontera-Madrid(config)#crypto map GESTION 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Frontera-Madrid(config-crypto-map)#set peer 200.46.0.2
Frontera-Madrid(config-crypto-map)#match address 101
Frontera-Madrid(config-crypto-map)#set transform-set REDES
Frontera-Madrid(config-crypto-map)#exit
```

```
Frontera-Madrid(config)#interface serial 1/0
Frontera-Madrid(config-if)#crypto map GESTION
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Frontera-Madrid(config-if)#exit
```

```
Frontera-Bilbao(config)#crypto isakmp policy 10
Frontera-Bilbao(config-isakmp)#authentication pre-share
Frontera-Bilbao(config-isakmp)#has sha
Frontera-Bilbao(config-isakmp)#encryption aes 256
Frontera-Bilbao(config-isakmp)#group 2
Frontera-Bilbao(config-isakmp)#lifetime 86400
Frontera-Bilbao(config-isakmp)#exit
Frontera-Bilbao(config)#crypto isakmp key vpn address 200.45.0.2
Frontera-Bilbao(config)#crypto ipsec transform-set REDES esp-aes esp-sha-hmac
Frontera-Bilbao(config)#access-list 101 permit ip 192.168.0.0 0.0.31.255 192.168.0.0 0.0.31.255
Frontera-Bilbao(config)#crypto map GESTION 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Frontera-Bilbao(config-crypto-map)#set peer 200.45.0.2
Frontera-Bilbao(config-crypto-map)#match address 101
Frontera-Bilbao(config-crypto-map)#set transform-set REDES
Frontera-Bilbao(config-crypto-map)#exit
Frontera-Bilbao(config)#interface serial 1/0
Frontera-Bilbao(config-if)#crypto map GESTION
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Frontera-Bilbao(config-if)#exit
```

5. Configuración de VoIP en Cisco y Raspberry-Asterisk

5.1. Conceptos generales de VoIp

- **¿Qué es voip?**

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La telefonía IP en general son, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportados vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

La VoIP (Voz sobre IP) esta sigla designa la tecnología empleada para enviar información de voz en forma digital en paquetes a través de los protocolos de Internet, en vez de hacerlo a través de la red de telefonía habitual.

Con VoIP podemos conseguir:

- Acceso a las redes corporativas desde pequeñas sedes a través de redes integradas de voz y datos conectadas a sucursales.
- Directorios corporativos basados en la Intranet con servicios de mensajes y números personales para quienes deben desplazarse.
- Servicios de directorio y de conferencias basadas en gráficos desde el sistema de sobremesa.
- Redes privadas y gateways virtuales gestionados para voz que sustituyen a las Redes Privadas Virtuales (VPN).

5.1.1 Protocolos

Los protocolos son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Estos protocolos serán.

- **SIP**

El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales (salvo el enrutado de los mensajes SIP).

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP.

- **SCCP**

El protocolo SCCP (Skinny Client Control Protocol), es un protocolo propietario de Cisco, el cual realiza la señalización entre el Call Manager y los teléfonos IP. Un cliente skinny utiliza TCP/IP para conectarse a los Call Managers y así poder transmitir las llamadas. Para transportar el audio utiliza RTP, UDP e IP.

- **H.323**

H.323 es una recomendación del ITU-T (International Telecommunication Union), que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

H.323 es utilizado comúnmente para Voz sobre IP y para videoconferencia basada en IP. Es un conjunto de normas ITU para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP.

- **IAX**

El protocolo IAX (Inter-Asterisk eXchange protocol) fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo.

- **Otros protocolos**

- *MGCP - Protocolo propietario de Cisco*
- *Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype*
- *Jingle - Protocolo abierto utilizado en tecnología XMPP*
- *Megaco (También conocido como H.248) y MGCP - Protocolos de control*

- **Parámetros VOIP**

1. Codecs

La comunicación de voz es analógica, mientras que la red de datos es digital. El proceso de convertir ondas analógicas a información digital se hace con un codificador decodificador (el CODEC). El proceso de la conversión es complejo. Es suficiente decir que la mayoría de las conversiones se basan en la modulación codificada mediante pulsos (PCM) o variaciones.

Además de la ejecución de la conversión de analógico a digital, el CODEC comprime la secuencia de datos, y proporciona la cancelación del eco. La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda.

Entre los codecs más utilizados en VoIP encontramos:

-
- *G.711: bit-rate de 56 o 64 Kbps.*
-
- *G.723: bit-rate de 5,3 o 6,4 Kbps.*
-
- *G.729: bit-rate de 8 o 13 Kbps.*

2. Qos

Los problemas de la calidad del servicio en VoIP vienen derivados principalmente por dos factores:

- 1) Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino.*
- 2) Las comunicaciones VoIP son en tiempo real lo que produce que efectos como el eco, la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deben ser evitados.*

Los principales problemas en cuanto a la calidad del servicio (QoS) de una red de VoIP son:

- *Latencia: El tiempo que tarda un paquete en llegar desde la fuente al destino.*
- *Jitter: La variación en el tiempo de llegada de los paquetes, causada por congestión de red o pérdida de sincronización.*
- *La pérdida de paquetes: Las comunicaciones en tiempo real están basadas en el protocolo UDP.*
- *Eco*
- *Ancho de banda: La cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.*

5.2. Configuración en cisco

5.2.1 Telefonía Cisco, centralitas

Para conseguir realizar la conexión y configuración de la telefonía IP con tecnología Cisco utilizaremos:

- Cisco Unified Communications Manager 7.1

Son los servidores que hacen de centralita. Aquí entre otras cosas se configuran las extensiones, su comportamiento y los permisos de llamada de cada una.

Nuestros Communications Manager, también llamados Call Manager permiten una escalabilidad desde 1 hasta 30.000 teléfonos IP por clúster y el equilibrado de carga y redundancia en servicio de procesamiento de llamadas, lo que significa un mejor rendimiento y que todas las llamadas no las procese un único Call Manager.

Las características funcionales de centralita de Cisco Unified Callmanager son:

- Retrollamada
- Desvío incondicional
- Desvío si no contesta
- Desvío si ocupado
- Llamada en espera
- Capturas de llamada
- Aparcamiento de llamadas
- Transferencias
- Conferencias
- Grupos de salto
- Música en espera
- Servicio Nocturno

5.2.2 Configuración VoIp en Cisco

1) configuramos el router

- Asignamos la ip la interfaz y la levantamos

```
interface faX/x  
ip address x.x.x.x x.x.x.x.x  
no shutdown
```

- Configuramos el dhcp para voip

```
Oficina-Madrid(config)#ip dhcp pool voip  
Oficina-Madrid(dhcp-config)#network 192.168.15.0 255.255.255.0  
Oficina-Madrid(dhcp-config)#default-router 192.168.15.1  
Oficina-Madrid(dhcp-config)#option 150 ip 192.168.15.1
```

Oficina-Madrid(dhcp-config)#exit

- **Configurar el TME o call manager express del router**

Oficina-Madrid(config)#telephony-service

Oficina-Madrid(config-telephony)#max-dn 10

Oficina-Madrid(config-telephony)#max-ephones 10

Oficina-Madrid(config-telephony)#ip source-address 192.168.15.1 port 2000

Oficina-Madrid(config-telephony)#auto assign 6 to 10

Oficina-Madrid(config-telephony)#auto assign 1 to 5

Oficina-Madrid(config-telephony)#exit

- **Configurar los terminales y los números de los teléfonos**

Oficina-Madrid(config)#ephone-dn 1

Oficina-Madrid(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Oficina-Madrid(config-ephone-dn)#number 54001

Oficina-Madrid(config-ephone-dn)#exit

Oficina-Madrid(config)#ephone-dn 2

Oficina-Madrid(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Oficina-Madrid(config-ephone-dn)#number 54002

Oficina-Madrid(config-ephone-dn)#exit

Oficina-Madrid(config)#ephone-dn 3

Oficina-Madrid(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

Oficina-Madrid(config-ephone-dn)#number 54003

Oficina-Madrid(config-ephone-dn)#exit

Oficina-Madrid(config)#ephone-dn 4

Oficina-Madrid(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up

Oficina-Madrid(config-ephone-dn)#number 54004

Oficina-Madrid(config-ephone-dn)#exit

Oficina-Madrid(config)#ephone-dn 5

Oficina-Madrid(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 5.1, changed state to up

Oficina-Madrid(config-ephone-dn)#number 54005

Oficina-Madrid(config-ephone-dn)#exit

```

ephone 1
 device-security-mode none
 mac-address 0001.635B.ACD4
 type 7960
 button 1:1
 !
ephone 2
 device-security-mode none
 mac-address 0001.6305.2A26
 type 7960
 button 1:2
 !
ephone 3
 device-security-mode none
 mac-address 0004.9ABA.8096
 type 7960
 button 1:4
 !
ephone 4
 device-security-mode none
 mac-address 00E0.F771.2186
 type 7960
 button 1:3

```

NOTA- El Call Manager recoge automáticamente cada mac de cada teléfono, el modo de seguridad y su asignación numérica como se muestra en la imagen final. Esta configuración es la misma empleada en la sede Bilbao nada más que cambiando la red.

5.3. Configuración con Raspberry-Asterisk

5.3.1 Conceptos de Asterisk y Raspberry Pi

El objetivo es la instalación de una centralita de voip en raspberry pi, sacando el mayor rendimiento y poniendo en práctica una centralita a tamaño muy reducido pero potente de voip.

En este caso instalaremos en la raspberry-asterix que nos hara la funcion de centralita de llamadas. Todo esto no se podrá probar por no tener recursos para la instalación de los elementos de pruebas por los que haremos una configuración y lo dejaremos listo y preparado para su uso, en cambio la pruebas se harán en un simulador de red de CISCO.

5.3.2 Instalación y configuración de Asterisk en Raspberry Pi

- 1) Procederemos a la instalación de complementos previo a instalar Asterisk, para ello instalaremos:

```

pi@buffet_abogados-madrid ~ $ sudo apt-get install libsqlite3-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libxml2-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libssl-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libiksemel-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libgnutls-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libcurl3-dev

```

```
pi@buffet_abogados-madrid ~ $ sudo apt-get install libspandsp-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install mysql-client
pi@buffet_abogados-madrid ~ $ sudo apt-get install mysql-server
```

```

##### Configuraci3n de mysql-server-5.5 #####
Se recomienda que configure una contrase1a para el usuario 1root1 (a
aunque no es obligatorio.
No se modificar1 la contrase1a si deja el espacio en blanco.
Nueva contrase1a para el usuario 1root1 de MySQL:
****
<Aceptar>

```

```

##### Configuraci3n de mysql-server-5.5 #####
Nueva contrase1a para el usuario 1root1 de MySQL:
****
<Aceptar>

```

```

pi@buffet_abogados-madrid ~ $ sudo apt-get install libmysqld-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install unixodbc-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libmyodbc
pi@buffet_abogados-madrid ~ $ sudo apt-get install libical-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libneon27-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install portaudio19-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libspeex-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libvorbis-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install libsrtp-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install iptables-persistent

```

```

##### Configuraci3n de iptables-persistent #####
Las reglas actuales de iptables se pueden guardar en el archivo de configuraci3n
1/etc/iptables/rules.v41. Estas reglas se cargar1n autom1ticamente durante
el arranque del sistema.
Las reglas s1lo se guardan autom1ticamente durante la instalaci3n del paquete
iptables si se especifican las instrucciones para mantener el archivo de reglas actualizado en la p1gina
de configuraci3n 1/etc/iptables/rules.v41.
1¿Desea guardar las reglas de IPv4 actuales?
[SA-] <No>
#####

```

```

[ ok ] Loading iptables rules... IPv4... skipping IPv6 (no rules to load).
pi@buffet_abogados-madrid ~ $ sudo apt-get install libsox2
pi@buffet_abogados-madrid ~ $ sudo apt-get install libsox-dev
pi@buffet_abogados-madrid ~ $ sudo apt-get install sox
pi@buffet_abogados-madrid ~ $ sudo apt-get install sendmail

```

```

[ ok ] Starting Mail Transport Agent (MTA): sendmail
Configurando sensible-mdm (8.14.4-4) ...
Configurando sendmail (8.14.4-4) ...

```

2) Descargamos el certificado de Asterisk 13.1

```
pi@buffet_abogados-madrid /usr/src $ sudo wget http://downloads.asterisk.org/pub/telephony/certified-asterisk/certified-asterisk-13.1-cert2.tar.gz
--2015-04-11 07:35:29-- http://downloads.asterisk.org/pub/telephony/certified-asterisk/certified-asterisk-13.1-cert2.tar.gz
Resolviendo downloads.asterisk.org (downloads.asterisk.org)... 76.164.171.238, 2001:470:e0d4::ee
Conectando con downloads.asterisk.org (downloads.asterisk.org)[76.164.171.238]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 31908316 (30M) [application/x-gzip]
Grabando a: certificado-asterisk-13.1-cert2.tar.gz
37% [----->] 11.994.890 623K/s T.E. 34s
```

3) Descomprimos el archivo y entramos en la carpeta:

```
buffet_abogados-madrid /usr/src $ sudo tar -xvf certified-asterisk-13.1-cert2.tar.gz
@buffet_abogados-madrid /usr/src $ cd certified-asterisk-13.1-cert2
@buffet_abogados-madrid /usr/src/certified-asterisk-13.1-cert2 $
```

4) Compilamos:

```
pi@buffet_abogados-madrid /usr/src/certified-asterisk-13.1-cert2 $ sudo ./configure
checking build system type... armv6l-unknown-linux-gnueabi
checking host system type... armv6l-unknown-linux-gnueabi
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
```

Nos dará un error de que nos falta un paquete por instalar, para ello instalamos el paquete que nos falta.

```
sudo ./contrib/scripts/install_prereq install
```

Aquí debemos de decirle el prefijo internacional de nuestro país en este caso España utiliza el prefijo +34.

```
Configuración de libvpb0
Este valor es el código numérico de la región en la que su sistema telefónico está operando (p. ej. 61 para Australia o 33 para Francia). Se utiliza para configurar los estándares regionales predeterminados con los que el hardware de telefonía de Voicetrónix deberá cumplir.
Código telefónico de la ITU-T:
34
<Aceptar>
```



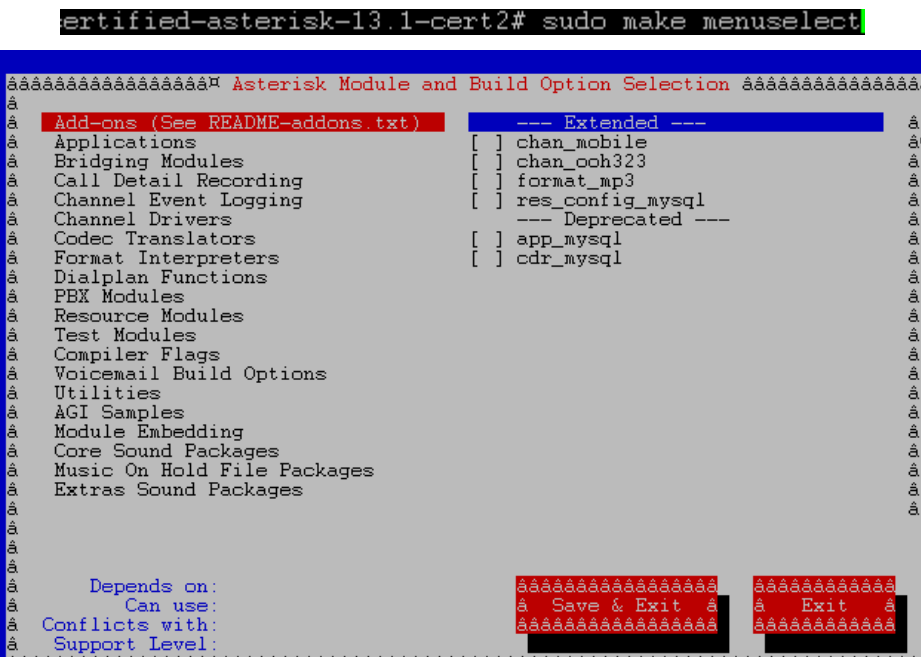
```
Estado actual: 31 actualizados [-2].  
#####  
## install completed successfully  
#####
```

Ejecutas otra vez y marcamos después la siguiente orden para seleccionar los módulos

sudo ./configure



- 5) Después ejecutaremos una orden para que nos salga el menú para seleccionar los módulos correspondientes.



6) Seguidamente ejecutaremos los siguientes make

```
certified-asterisk-13.1-cert2# sudo make
```

```
Building Documentation For: channels pbx apps codecs formats cdr cel bridges funcs tests main
res addons
+----- Asterisk Build Complete -----+
+ Asterisk has successfully been built, and +
+ can be installed by running:           +
+                                         +
+         make install                   +
+-----+

```

```
certified-asterisk-13.1-cert2# sudo make install
```

```
+----- Asterisk Installation Complete -----+
+
+   YOU MUST READ THE SECURITY DOCUMENT   +
+
+ Asterisk has successfully been installed. +
+ If you would like to install the sample  +
+ configuration files (overwriting any     +
+ existing config files), run:            +
+
+         make samples                    +
+
+----- or -----+
+
+ You can go ahead and install the asterisk +
+ program documentation now or later run:   +
+
+         make progdocs                   +
+
+ **Note** This requires that you have     +
+ doxygen installed on your local system   +
+-----+

```

```
certified-asterisk-13.1-cert2# sudo make samples
```

Si nos sale un error al instalar el make config nos situamos en el directorio.

```
certified-asterisk-13.1-cert2/contrib/init.d
```

Copiamos el fichero rc.debian.asterisk en la ruta init.d de etc

```
cp rc.debian.asterisk /etc/init.d/asterisk
```

y modificamos con nano etc/init.d/asterisk

```
# Full path to asterisk binary
DAEMON=/usr/sbin/asterisk
ASTVARRUNDIR=/var/run/asterisk
ASTETCDIR=/etc/asterisk
TRUE=/bin/true
```

7) Después de guardar los cambios del fichero se carga el script como servicio

```
sudo update-rc.d asterisk defaults
```

8) Activar el servicio asterisk

```
certified-asterisk-13.1-cert2# sudo service asterisk start
```

```

[ ok ] Starting Asterisk PBX: asterisk.
root@buffet-abogados-madrid: /etc/asterisk/

```

- **Configuración de Asterisk (Plan de marcación, teléfonos SIP y troncales IAX, troncales SIP y buzón de voz)**

Ahora procederemos a la modificación de los siguientes ficheros; extensions.conf, sip.conf, voicemail.conf e iax.conf. Mostraremos la configuración de Asterisk de la sede de madrid, en el caso de Bilbao es lo mismo nada más que se modifican algunas de las ramas que luego diremos.

1) Configuración Asterisk sede Madrid

- Configuramos el fichero extensions.conf como primer paso

```

buffet@buffet-abogados-madrid /etc $ cd /etc/asterisk/

```

- Estos son parámetros globales y generales que ya vienen definidos y ejecutados en el fichero.

```

buffet@buffet-abogados-madrid /etc $ sudo nano extensions.conf

```

```

[general]
static=yes
writeprotect=no

```

```

[globals]
TRUNK=SIP/sarevoz
TRUNKMSD=1

```

- Procederemos a escribir las extensiones necesarias de cara para poner en marcha asterisk

```

[macro-stdexten]

```

```

; Extensión estandar macro:

```

```

; ${ARG1} - Extension (podríamos haber usado

```

```

; ${MACRO_EXTEN} aquí ; además ; ${ARG2} - Dispositivo(s) a sonar ;

```

```

exten => s,1,Dial(${ARG2},20) ; Suena el equipo, 20 segundos maximo
exten => s,2,Goto(s-${DIALSTATUS},1) ; Salto basado en el estado
exten => s-NOANSWER,1,Voicemail(u${ARG1}) ; Si no está disponible, enviar a ; buzón de voz
exten => s-NOANSWER,2,Goto(default,0,1) ; Si se pulsa #, ir a ; operadora
exten => s-BUSY,1,Voicemail(b${ARG1}) ; Si ocupado, enviar al buzón de voz ; con el
mensaje de ; ocupado

```

```

exten => s-BUSY,2,Goto(default,0,1) ; Si se pulsa #, ir a ; operadora
exten => s-CHANUNAVAIL,1,Voicemail(u${ARG1})
exten => s-CHANUNAVAIL,2,Goto(default,0,1)
exten => s-,1,Goto(s-NOANSWER,1) ; Trata cualquier otra cosa como ; no hay respuesta
exten => a,1,VoicemailMain(${ARG1}) ; Si se pulsa *, enviar a ; buzón de voz

```

[macro-novm]

```
exten => s,1,Dial(${ARG1},30) ;suena el dispositivo durante 30 segundos
exten => s,2,Goto(default,s,1)
exten => s,102,Goto(default,s,1)
```

[incoming]

```
exten => s,1,Goto(default,300,1) ;Número principal suena en ;la operadora
exten => t,1,Goto(default,300,1);
exten => i,1,Goto(default,300,1);
```

[from-sarenet]

```
exten => s,1,Answer
exten => s,n,Wait(1)
exten => s,n,Goto(IVR,s,1)
```

ignorepat => 0

```
exten => _09XXXXXXXX,1,Goto(trunkdial,${EXTEN},1)
exten => _08XXXXXXXX,1,Goto(trunkdial,${EXTEN},1)
exten => _06XXXXXXXX,1,Goto(trunkdial,${EXTEN},1)
exten => _07XXXXXXXX,1,Goto(trunkdial,${EXTEN},1)
```

include => default

[longdistance]

```
ignorepat => 0
exten => _000XXXXXXXXXXXX,1,Goto(trunkdial,${EXTEN},1)
include=>local
```

[trunkdial]

```
exten => _0.,1,Dial(${TRUNK}/${EXTEN:${TRUNKMSD}})
exten => _0.,2,Congestion(5)
exten => _0.,3,Hangup
```

- Ahora estableceremos las extensiones para cada departamento y cada teléfono:

[default]

```
include=>local
include=>incoming
```

```
exten => s,1,Goto(default,300,1)
exten => t,1,Goto(default,300,1)
exten => i,1,Goto(default,300,1)
```

;Departamento informatico extension 300

```
exten => 300,1,Macro(stdexten,${EXTEN},SIP/${EXTEN})
```

```
;Director general del buffet  
exten => _30[25],1,Macro(stdexten,${EXTEN},SIP/${EXTEN})
```

```
;Departamento penal, extensiones 305-309  
exten => _30[5-9],1,Macro(stdexten,${EXTEN},SIP/${EXTEN})
```

```
;Departamento mercantil, extensiones 310-313  
exten => _31[0-3],1,Macro(stdexten,${EXTEN},SIP/${EXTEN})
```

```
;Departamento laboral, extensiones 314-317  
exten => _31[4-7],1,Macro(stdexten,${EXTEN},SIP/${EXTEN})
```

```
;Administracion, ext 320, no necesita buzón de voz  
exten => 320,1,Macro(novm,SIP/${EXTEN})
```

- Configurar la extensión para el buzón de voz

```
;Para entrar en el menú del buzón de voz marcamos extensión 800  
exten => 800,1,Answer  
exten => 800,2,VoicemailMain  
exten => _85X,1,Answer  
exten => _85X,2,MeetMe(${EXTEN})  
exten => 888,1,Goto(dialext,s,1)
```

- Configurar las conexiones de llamadas a otras sedes

```
; Si llamamos al patron de las extensiones de cada una de las otras sedes  
; salimos por el troncal IAX2 definido para cada una de las sedes (usuario y cocontrasena)
```

```
;Oficina de Bilbao  
exten => _2XX,1,Dial(IAX2/bilbao:bil1234id@10.64.2.100/${EXTEN})
```

```
[dialext]  
include => default
```

```
exten => s,1,Answer  
exten => s,2,DigitTimeout(5)  
exten => s,3,ResponseTimeout(20)  
exten => s,4,Background(pleaseenterextension)  
que  
exten => 9,1,Directory(default)
```

```
; "Por favor introduzca la ; extensión del usuario  
quiere llamar."  
; pulse 9 para entrar en el directorio
```

```
exten => 9,2,Goto(dialext,9,1)
exten => 0,1,Goto(default,100,1) ; envía a la operadora como cortesía
                                   ; si se pulsa la tecla 0

exten => i,1,Playback(privacy-incorrect)
exten => i,2,Goto(dialext,s,1)
exten => t,1,Goto(dialext,i,1)
```

- Ahora configuraremos el fichero sip.conf

En el fichero sip.conf definiremos cada extensión para cada telefono y para cada personal de la oficina.

```
etc/asterisk# nano sip.conf
```

Definiremos algunas de las extensiones de teléfono no todas, pondremos una de cada

```
[general]
```

```
context=default
port=5060
bindaddr=0.0.0.0
disallow=all
allow=ulaw
```

```
[sarevoz]
```

```
type=peer
host=sarevoz.com
disallow=all
allow=g729
allow=alaw
defaultuser=24162
fromuser=24162
fromdomain=sarevoz.com
secret=iwonttellyou
directmedia=no
sendrpid=pai
```

```
[300]
```

```
type=friend
context=default
callerid=Antonio Palacios<300>
host=dynamic
secret=123456
dtmfmode=inband
mailbox=300
```

```
[325]
```

```
type=friend
context=default
callerid=Javier Garcia<325>
host=dynamic
```

```
secret=123456  
dtmfmode=inband  
mailbox=325
```

```
[305]  
type=friend  
context=default  
callerid=Elena Sanchez<305>  
host=dynamic  
secret=123456  
dtmfmode=inband  
mailbox=305
```

```
[312]  
type=friend  
context=default  
callerid=Juan Crespo<312>  
host=dynamic  
secret=123456  
dtmfmode=inband  
mailbox=312
```

```
[315]  
type=friend  
context=default  
callerid=Leonor Sanchez<315>  
host=dynamic  
secret=123456  
dtmfmode=inband  
mailbox=315
```

```
[320]  
type=friend  
context=default  
callerid=Cristina Morales<320>  
host=dynamic  
secret=123456  
dtmfmode=inband  
mailbox=320
```

- El siguiente fichero a configurar es el voicemail.conf, donde configuraremos los parámetros del buzón de voz.

```
etc/asterisk# nano voicemail.conf
```

```
[general]  
; Enviar archivos en las notificaciones de e-mail  
attach=yes  
; Usar el formato wav para los mensajes de voz  
format=wav  
; Limitar el tiempo máximo del mensaje de voz a 180 segundos
```

```
maxmessage=180
; Limitar el tiempo minimo del mensaje a 3 segundos
minmessage=3
; Anunciar el numero que llamó antes de repetir el mensaje
saycid=yes
; Limitar el numero de intentos de registro a 3
maxlogins=3
; Define los contextos internos para especificar que vienen de una extensión interna
cidinternalcontexts=default,
[zonemessages]
madrid=Europe/Paris|vm-received' Q 'digits/at' R
europa=Europe/Berlin|vm-received' Q 'digits/at' kM
```

- En el siguiente apartado pondremos un buzón de voz a cada usuario y redireccionar un aviso a su correo.

```
[default]
```

```
300 => 4321,Antonio Palacios,antpalacios@abogados-carroble.com,,delete=1
305 => 4321,Elena Sanchez,elsanchez@abogados-carroble.com,,delete=1
312 => 4321,Juan Crespo,jucrespo@abogados-carroble.com,,delete=1
315 => 4321,Leonor Sanchez,lesanchez@abogados-carroble.com,,delete=1
320 => 4321,Cristina Morales,cmorales@abogados-carroble.com,,delete=1
325 => 4321,Cristina Casas,ccasas@abogados-carroble.com,,delete=1
```

- Pasamos a configurar el fichero `iax.conf`, este fichero es para configurar las conexiones entre sedes, con su autenticación y demás métodos de seguridad.

```
etc/asterisk# nano iax.conf
```

```
[general]
port=4569
bandwidth=low
disallow=all
allow=gsm
jitterbuffer=yes
tos=lowdelay
```

```
[bilbao]
```

```
type=peer
host=dynamic
trunk=yes
auth=md5,plaintext,rsa
secret=bi1234ao
```



```
username=bilbao
qualify=yes
context=default
```

- Ahora creamos el último fichero el IVR, este fichero que se crea desde cero meteremos las extensiones del lenguaje, conexiones con las sedes y configuración de las teclas de los telefonos, tiempo de espera.

```
etc/asterisk# nano IVR
```

[IVR]

```
exten => s,1,Wait(1) ;espera un segundo
exten => s,2,Set(CHANNEL(language)=es) ; pone como predefinidas las voces en español
exten => s,3,Set(TIMEOUT(digit)=7) ; 7 segundos es el tiempo que espera entre el primer dígito ; y los sucesivos
exten => s,4,Set(TIMEOUT(response)=10) ; 10 segundos es el tiempo que espera para que ; el llamante pulsa una tecla

exten => s,5,BackGround(custom/espeng) ;presenta el menu vocal y al mismo tiempo escucha si el llamante ;pulsa alguna tecla
exten => s,6,WaitExten() ; espera que el llamante presione alguna tecla
exten => 1,1,goto(IVR1,s,1) ; si presiona 1 va al contexto IVR1, extension s, prioridad 1
exten => 2,1,goto(IVR2,s,1) ; si presiona 2 va al contexto IVR2, extension s, prioridad 1
exten => i,1,Playback(invalid) ; si el numero digitado no es valido (ni 1 ni 2) comunica el error
exten => i,2,Playback(goodbye) ; se despide
exten => i,3,Hangup ; cuelga la llamada
exten => t,1,goto(IVR,s,2) ; si dentro de 10 segundo el llamante no presiona ;ninguna tecla vuelve a presentar el menu vocal
exten => h,1,Hangup ; si el llamante cuelga ejecuta la extension h
```

[IVR1]

```
exten => s,1,Set(TIMEOUT(digit)=7) ;
exten => s,2,Set(TIMEOUT(response)=10)
exten => s,3,Set(CHANNEL(language)=en) ; define como idioma predefinido el ingles y usas las ;voces en este idioma
exten => s,4,BackGround(custom/engmenu) ; presenta en menu en ingles
exten => s,5,WaitExten() ; Espera que el llamante pulse una tecla

exten => 1,1,Playback(pls-wait-connect-call) ; Si presiona 1 lo pone en comunicacion con ;la oficina de Bilbao (extension 100)
exten => 1,2,Dial(IAX2/bilbao:bi1234ao@10.64.3.100/100)
```

```
exten => i,1,Playback(invalid)
exten => i,2,Playback(goodbye)
exten => i,3,hangup
exten => t,1,goto(IVR1,s,1)
exten => h,1,Hangup
```

[IVR2]

exten => s,1,Set(TIMEOUT(digit)=7)

exten => s,2,Set(TIMEOUT(response)=10)

exten => s,3,Set(CHANNEL(language)=es) ; define como idioma predefinido el ingles y usas las voces en este idioma

exten => s,4,BackGround(custom/espmenu) ; presenta en menu en espanol

exten => s,5,WaitExten() ; espera a que el llamante pulse una tecla

exten => 1,1,Playback(pls-wait-connect-call) ; Si presiona 1 lo pone en comunicacion con ;la oficina de Bilbao (extension 100)

exten => 1,2,Dial(IAX2/bilbao:bi1234ao@10.64.3.100/100)

exten => i,1,Playback(invalid)

exten => i,2,Playback(goodbye)

exten => i,3,hangup

exten => t,1,goto(IVR1,s,1)

exten => h,1,Hangup

NOTA-Este proceso se hará también en la sede de Bilbao, se omite repetir los pasos de Bilbao pero serían los mismos nada más que modificando los números, personal, etc.....

6. Bibliografía

Configuración Voip en cisco

<http://d4nnr.blogspot.com.es/2013/09/configurando-topologia-voip-cisco.html>

<http://www.packettracernetwork.com/tutorials/voipconfiguration.html>

Configurar e instalar Asterisk en raspberry pi

<https://www.voztovoice.org/?q=node/655>

<http://rsppi.blogspot.com.es/2012/05/asterisk-en-el-raspberrypi.html>

<http://www.raspberry-asterisk.org/documentation/>

Configurar ASA en cisco

<http://es.slideshare.net/websyo/practica-con-firewall-asa-14114092>

http://www.cisco.com/cisco/web/support/LA/111/1118/1118174_asa-config-dmz-00.html

Configurar VPN en cisco

<http://es.slideshare.net/VanesaPercy/vpn-site-to-site-cisco>