UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

DOCUMENTO FINAL

CÁTEDRA: REDES II

PROYECTO A REALIZAR:

"Firewall con Balanceador de dos Enlaces de Internet"

CATEDRATICO:

Ing. Manuel Flores Villatoro

INTEGRANTES DE GRUPO

Nº	APELLIDOS	NOMBRES	CARNET	PORCENTAJE %
1	Monterroza Vasquez	Edwin Antonio	(MV02110335)	100%
2	Menjivar Ochoa	Carlos Ernesto	(MO02110328)	100%
3	Martínez García	Eduardo de Jesús	(MG02110337)	100%
4	García Ramos	Herly Antonio	(GR02110333)	100%

San Salvador, 23 de Noviembre de 2013

Contenido

INTRODUCCION

En el Proyecto: “Firewall con Balanceador de dos Enlaces de Internet”, se busca hacer las configuraciones necesarias para tener dos conexiones a internet. Se debe proporcionar equilibrio de carga y la redundancia de una red de área ancha, tal como Internet, a una red de área local.

En éste proyecto se puede pensar en él como varias rutas por defecto a internet.

En la implementación de éste proyecto, se detallarán sus beneficios como también de las configuraciones mínimas. Para su implementación se utilizará el entorno Linux con el sistema operativo Debian 0.7 wheezy.

OBJETIVOS

OBJETIVO GENERAL

Implementar y configurar correctamente el proyecto (Firewall con Balanceador de dos Enlaces de Internet), y así mismo garantizar el funcionamiento de éste.

OBJETIVOS ESPECÍFICOS

- Identificar todos los procesos a realizar en la implementación y configuración del proyecto.
- Configurar de manera adecuada todos los procesos y aplicaciones requeridas para dicho proyecto.
- Contar con herramientas seguras que respalde el desarrollo Y funcionamiento del proyecto.

MARCO TEÓRICO

¿QUE ES UN FIREWALL?

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewal es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewal examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.
Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

Fig.1 Esquema común de un Firewall.

Beneficios de tener un Firewall con Balanceador de dos Enlaces de Internet.

1-Mayor ancho de Banda: Varias conexiones simultáneas, en promedio, todas juntas tienen acceso a un mayor ancho de banda, que se extenderá a la suma de los anchos de banda de Internet de todos los enlaces que están siendo equilibrados.

2-Tolerancia a Fallos: Cuando tenemos una o más conexiones y cuando falla una salimos automáticamente por la otra que si funciona. Si una de las líneas falla, el router continúa automáticamente la conexión utilizando exclusivamente la segunda.

2-Balanceo de Carga: Se puede repartir ancho de banda, podemos usar una conexión a internet para un propósito y la segunda para otro.
A través de Linux es posible lo siguiente:

1) Balancear un pool de servidores, como por ejemplo servidores Webs a Internet, proxies, DNS's, FTP's, etc. Esto es lo mismo que hacen los equipos de F5 o CISCO.
2) Atrapar conexiones que pasan por Linux y luego bombearlas al servidor u otra máquina.

Un router Linux con firewall para salir a Internet tiene puede controlar el consumo de ancho de banda empleando la herramienta TC, que es parte del paquete IPFilter.

Otra de las características más importantes de un firewall no solo se basa en su capacidad para decidir que entra (INPUT), que sale (OUTPUT) o que pasa entre interfaces (FORWARD). La implementación de las reglas para un firewall necesita saber que está pasando por nuestras interfaces, y es ahí donde un firewall provee la capacidad de saber que está ocurriendo o que ocurrió en un determinado momento.

Es posible hacer que Linux filtre de modo transparente todo el tráfico web que entra a un Router+Firewall en Linux ocupando un proxy Open Source llamado Squid.

Descripción del Proyecto

El proyecto consiste en la configuración de un firewall que utilice dos enlaces de internet para brindar acceso a internet a todos sus clientes.
En donde, un cliente pueda acceder a internet y lo pueda hacer a través de cualquier enlace.

Se utilizará como software de servidor proxy para web, el **Squid**. La forma en que un firewall filtra los paquetes son las denominadas “reglas”. Un firewall con una sola interfaz de red puede bloquear la entrada y salida de paquetes. Un firewall con más de una interfaz de red puede filtrar paquetes que pasan de una interfaz a otra y que comúnmente se conoce como ruteo.

Un proxy de conexión a Internet es un servidor que hace de intermediario entre los PCs de la red y el router de conexión a Internet, de forma que cuando un usuario quiera acceder a Internet, su PC realiza la petición al servidor Proxy y es el proxy quien realmente accede a Internet.

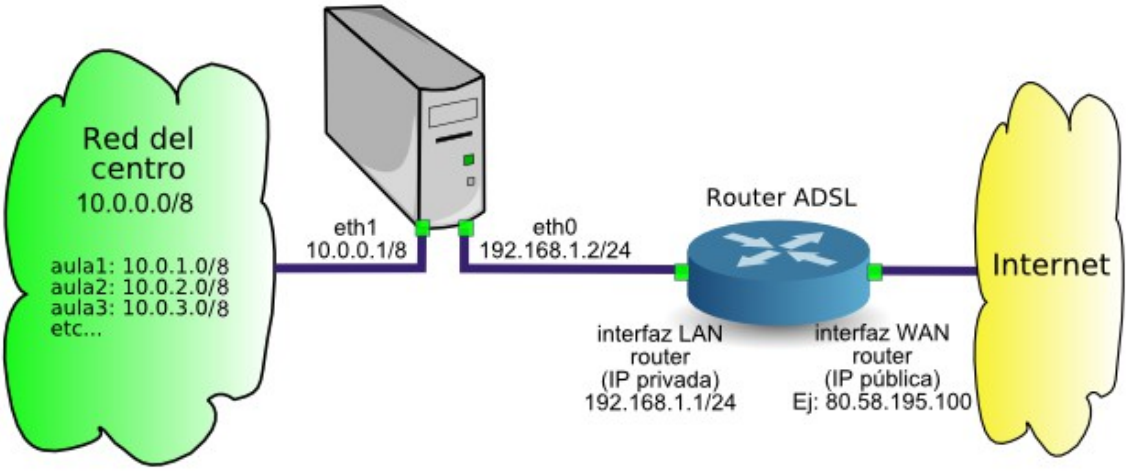


Fig. 2 Diagrama de proxy de conexión a internet

Se implementará en Sistema Operativo GNU/Linux, ya que es un Sistema Operativo muy versátil. Su kernel implementa en un módulo el proceso de filtrado de paquetes y eso lo hace de manera directa, en el sentido que es poco el overhead que pone sobre una máquina.

Overhead: Es el desperdicio de ancho de banda, causado por la información adicional (de control, de secuencia, etc.) que debe viajar además de los datos, en los paquetes de un medio de comunicación.

Se utilizará el NAT, que es un protocolo para enmascarar varias direcciones IP, puerto y protocolos sobre otras direcciones IP, puertos y protocolos. Esa característica de NAT es nos facilitará que las estaciones de trabajo salgan a Internet sin tener miles de direcciones IP públicas para cada una de ellas.

¿Qué es iptables?

Iptables – IP packet filter administration (administración de filtro de paqueteIP), es la herramienta que nos permite configurar, mantener e inspeccionar las tablas de reglas de filtrado de paquetes IP en el kernel de Linux, desde su versión 2.4 (en 2.2 era ipchains). Con esta herramienta, podremos crearnos un firewall adaptado a nuestras necesidades.

Del manual de iptables se pueden definir diferentes tablas. Cada tabla contiene un número de cadenas propias y también puede contener cadenas definidas por el usuario. Cada cadena es una lista de reglas las cuales pueden encajar con un conjunto de paquetes. Cada regla especifica qué hacer con un paquete que encaja. Esto es llamado un `objetivo', el cual puede ser un salto a una cadena definida por el usuario en la misma tabla.

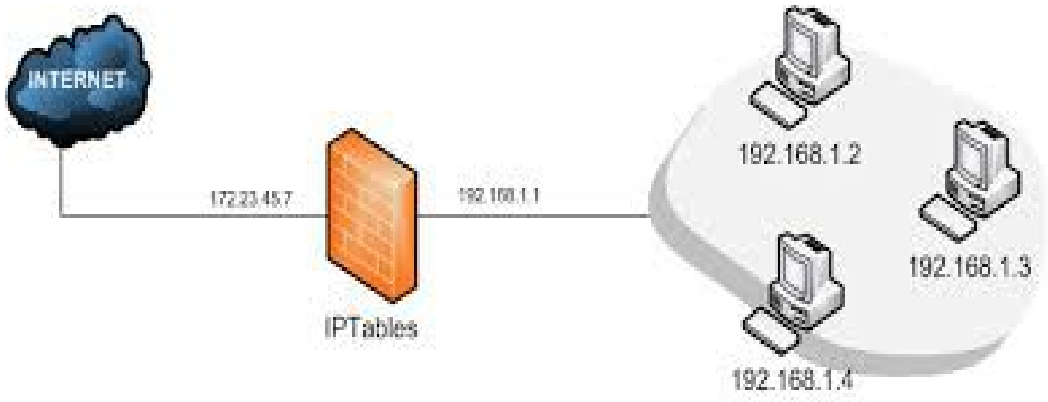


Fig. 3 Diagrama configuración de ip tables.

Configurar router con Linux e Iptables

MATERIALES QUE SE UTILIZARAN

CABLE UTP

ENCRIPTADORA

CAPUCHONES

SWICHS

MODEM

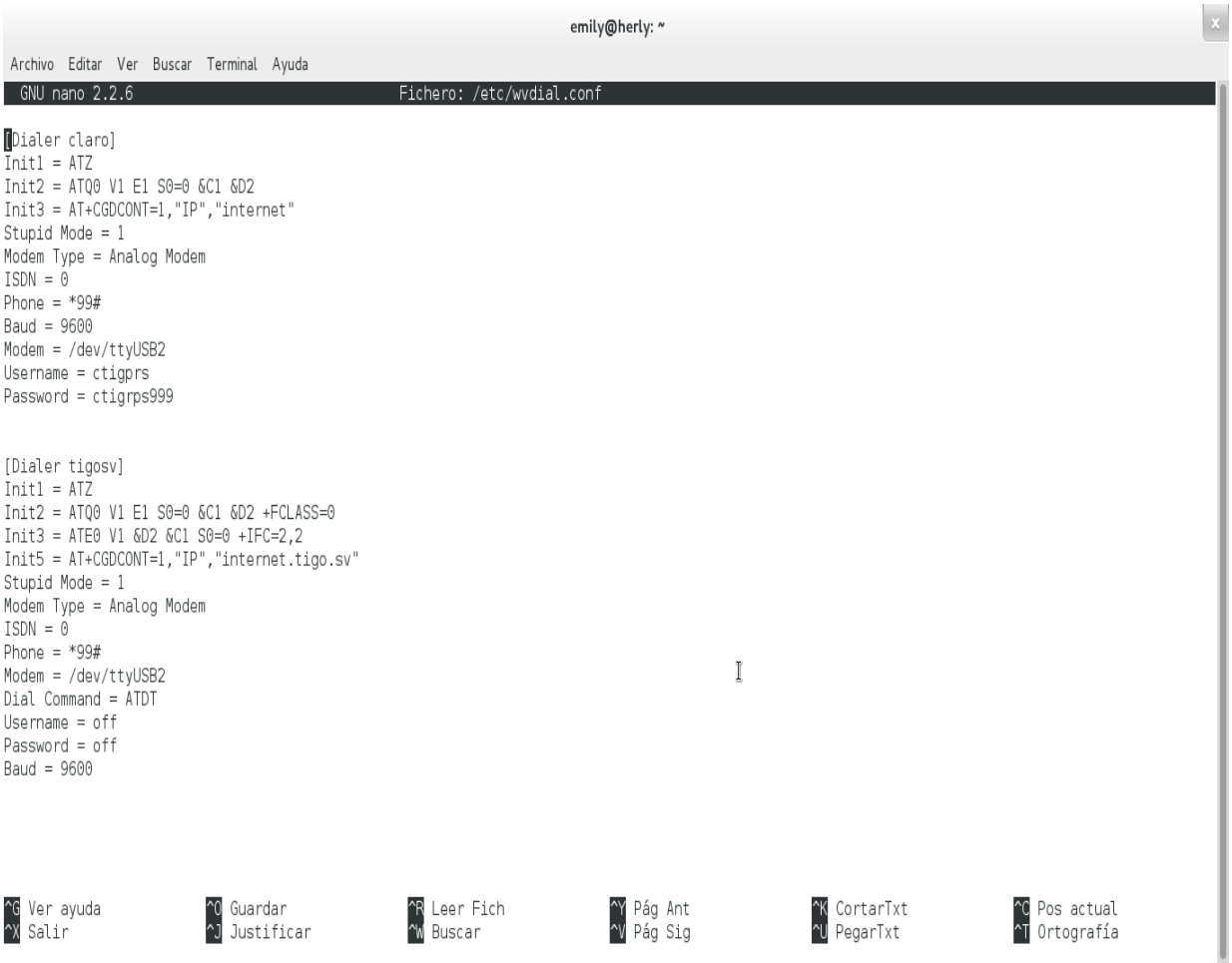
PC como Router

PC como cliente

	IP	NetMask	Broadcast	Getaway
PC 01	10.0.0.1	255.255.255.0	10.0.0.255	
PC 02	10.0.0.2	255.255.255.0	10.0.0.255	10.0.0.1
Modem	(Varia según el modelo	255.255.255.255		

Tabla: Descripción de dirección Ip

CONFIGURACION DE LOS DOS MODEM (CLARO Y TIGO)



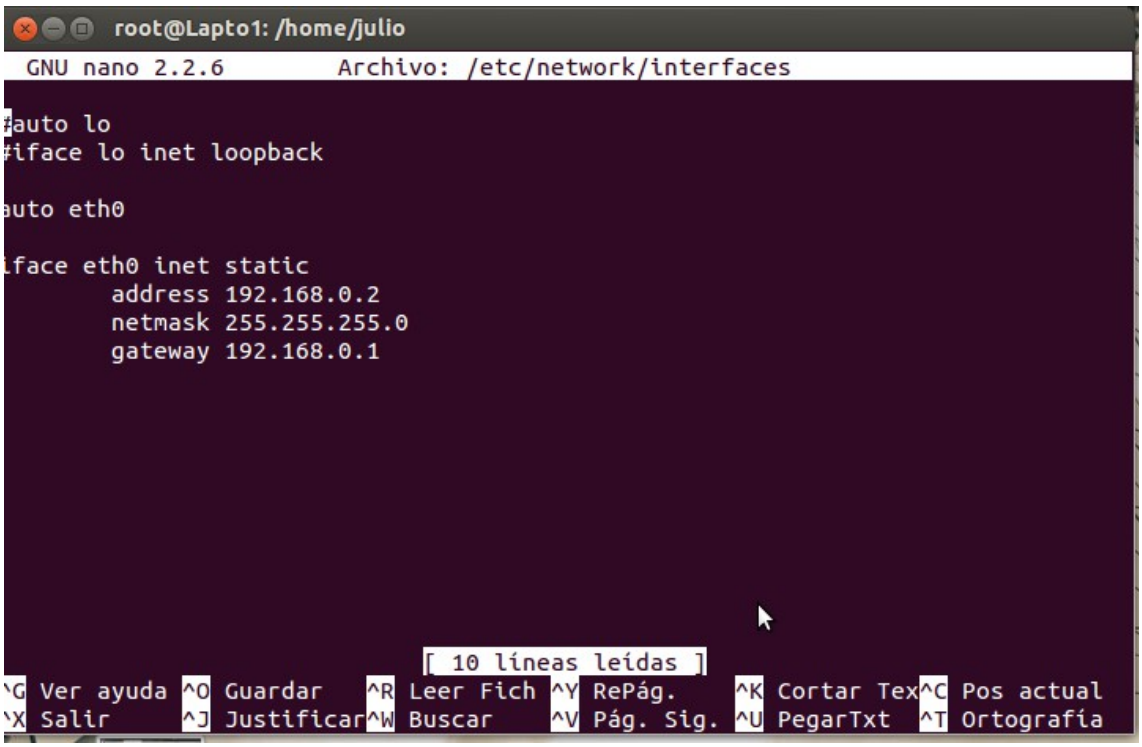
Configurando la Pc 1 (router)

Con el comando **nano /etc/network/interfaces**

Configuraremos la Pc 2 (Cliente)

Configuramos la IP
nano /etc/network/interfaces
/con el comando nano editamos el archivo interfaces

Configuramos la ruta por defecto (Getaway)
en nuestro caso: **192.168.0.1**



Vemos la tabla de enrutamiento
ip route
/con el comando ip router vemos el contenido de la tabla de enrutamiento

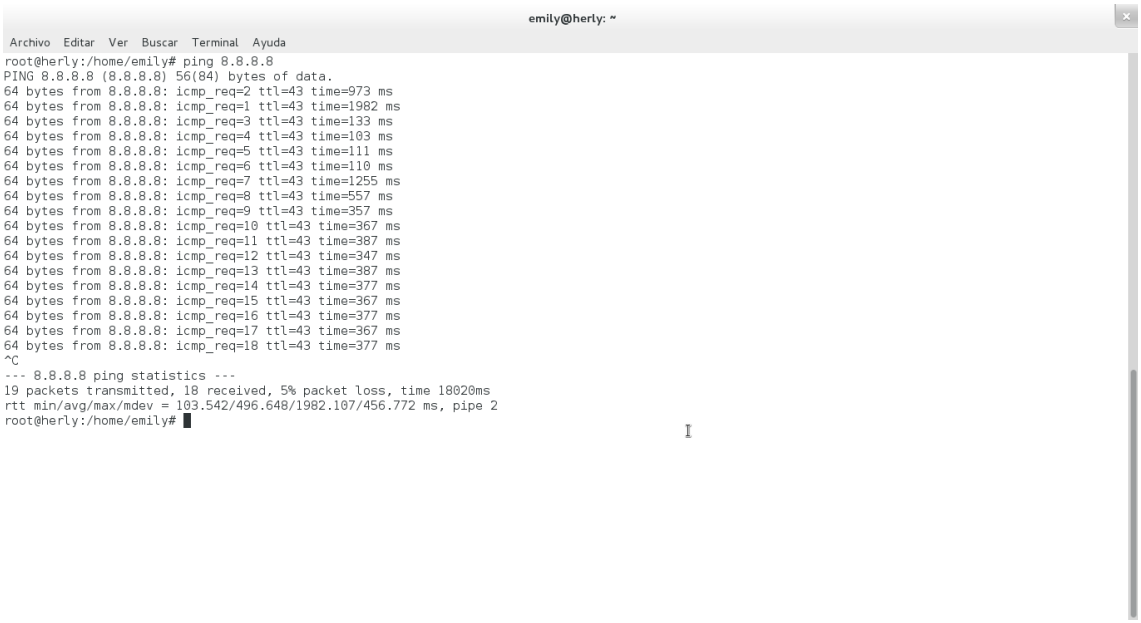
```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@herly:/home/emily# ip route
default via 192.168.0.1 dev eth0  scope link
default via 192.168.0.2 dev eth0
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.1
root@herly:/home/emily#
```

Verificamos si las ip 192.168.0.1 y 192.168.0.2 están correctamente configuradas

Ifconfig

```
emily@herly: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@herly:/home/emily# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1f:16:5b:e1:f6
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:16ff:fe5b:e1f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:624 errors:0 dropped:0 overruns:0 frame:0
          TX packets:420 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:121908 (119.0 KiB)  TX bytes:39449 (38.5 KiB)
          Interrupt:42 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:15568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15568 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2347825 (2.2 MiB)  TX bytes:2347825 (2.2 MiB)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.137.36.19  P-t-P:10.64.64.64  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:4832 (4.7 KiB)  TX bytes:4892 (4.7 KiB)

ppp1      Link encap:Point-to-Point Protocol
          inet addr:10.230.34.144  P-t-P:10.64.64.65  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:350 errors:0 dropped:0 overruns:0 frame:0
          TX packets:393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:140425 (137.1 KiB)  TX bytes:45027 (43.9 KiB)

root@herly:/home/emily#
```

Con el comando Ping verificamos si tenemos conexión con internet hacemosPing a la 8.8.8.8 la pagina de Google.



Después de haber hecho Ping con el Servidor nos muestra todos los Paquetes

Diagrama de Red propuesto:

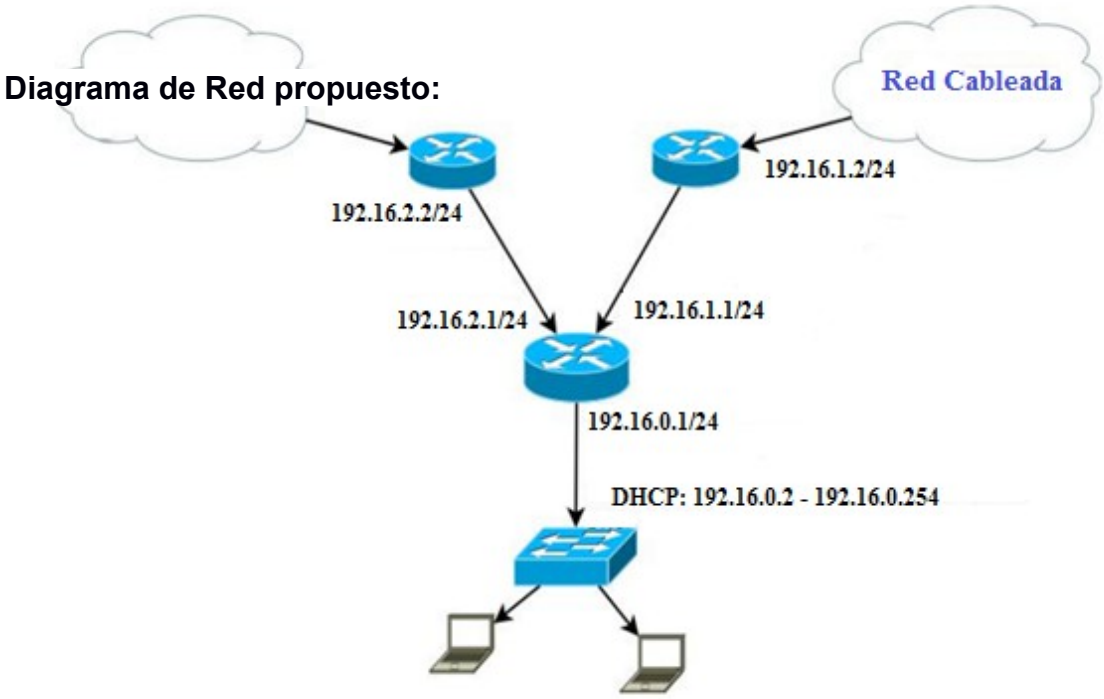
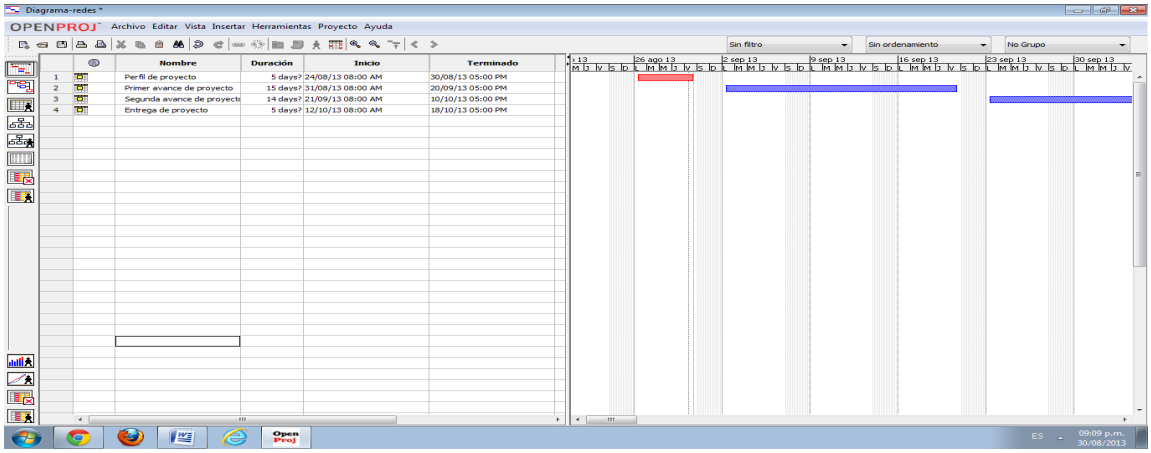
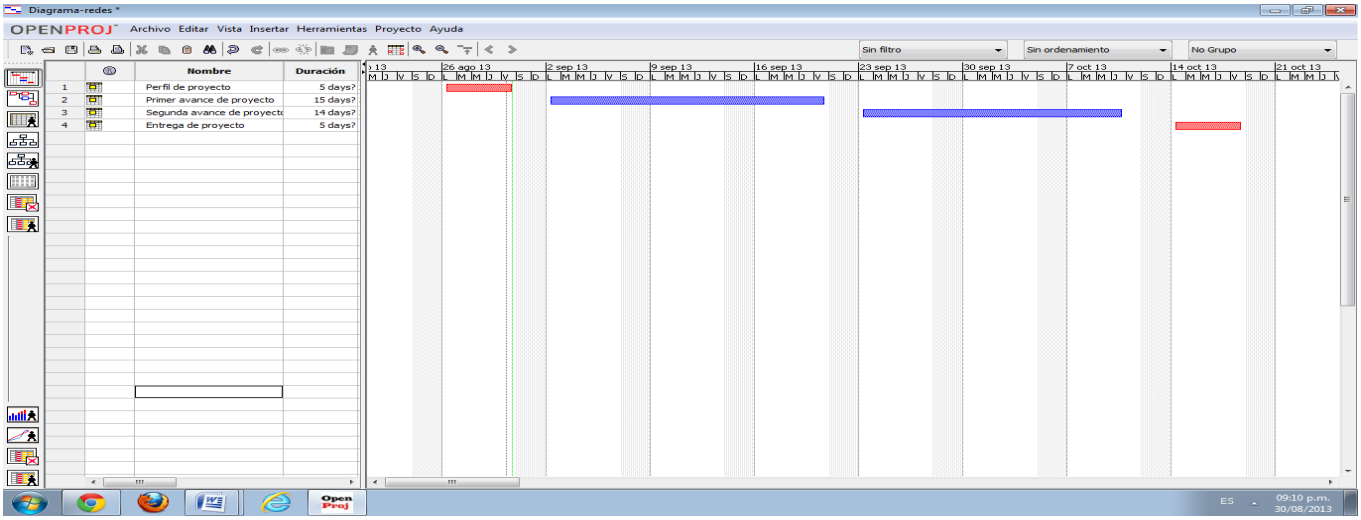


Diagrama de Gantt





CONCLUSION

El desarrollo de este tipo de proyectos nos permite adquirir conocimientos de mucha importancia ya que mas adelante nos seran de mucha importancia cuando nos toque en la practica tener que realizarlo

Hay que destacar que realizar un Firewall con balanceador de dos enlaces a internet, y en un sistema operativo GNU/Linux, es un poco difícil; ya que se parte desde cero. En donde se debe de crear un firewall que nos permite acceder a un punto de internet más cerca y esto facilita nuestra conexión más factible y viable.

BIBLIOGRAFIAS

- Titulo: Iptables
- Url: ttp://es.scribd.com/doc/92257303/IPTABLESwww.netfilter.org
- Autor: Nicolas Contador
- fecha de 02/07/2012