UNIVERSIDAD NACIONAL DEL CENTRO DE LA PROVINCIA DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS

INGENIERIA DE SISTEMAS



**Trabajo Práctico Especial**

**Comunicación de Datos I**

**Alumnos**: Bocchio Montes de Oca Esteban, Bertino Ariel Eugenio.

**Nº de grupo**: 15.

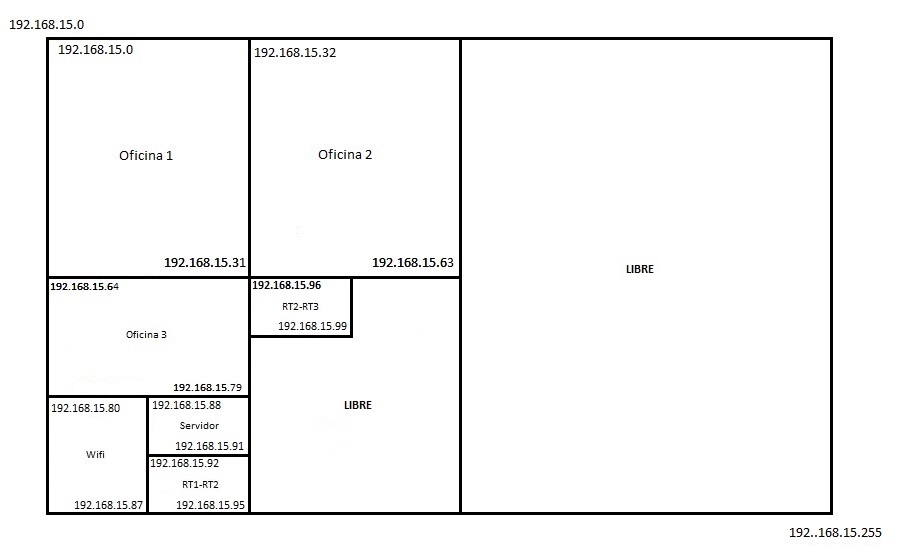
**Ayudante asignado**: Fernando Mayorano

Introducción

En el presente trabajo practico especial de la materia comunicación de datos I, nos enfocaremos en la configuración de una red mediante un simulador de redes llamado core incorporado en la máquina virtual Vcore. Esto es configurar 4 redes de trabajo, un servidor, un proveedor de internet (ISP) y la red de una casa y asignando direcciones IP a las redes necesaria junto a sus máquinas y dispositivos (router, hub, switch, etc).

Para llevar un orden iremos desarrollando cada inciso de la guía y adjuntando imágenes (capturas de pantalla) según sea necesario.

1. VLSM (Mascara de subred de longitud Variable)  
   Aclaración: para dividir las redes tuvimos en cuenta que para cara red se necesitan la dirección base de la red, la dirección broadcast y la dirección del dispositivo conectado (ejemplo: la dirección del router). También expresaremos la máscara de cada subred con el formato *ipbase*/*mascara.* En la división de subredes no tuvimos en cuenta las redes de casa ni las ip públicas del router 3, router 4 ni ISP (proveer de internet).



Oficina 1: red 192.168.15.0/27 (25=32 direcciones)

192.168.15.0 dirección base de la red

192.168.15.1

… … … …

192.168.15.31 dirección broadcast de la red

Oficina 2: red: 192.168.15.32/27 (25=32 direcciones)

192.168.15.32 dirección base de la red

192.168.15.33

… … … …

192.168.15.64 dirección broadcast de la red

Oficina 3: red 192.168.15.65/28 (24=16 direcciones)

192.168.15.65 dirección base de la red

192.168.15.66

… … … …

192.168.15.79 dirección broadcast de la red

Wifi: 192.168.15.80/29 (23=8 direcciones)

192.168.15.80 dirección base de la red

192.168.15.81

… … … …

192.168.15.87 dirección broadcast de la red

Servidor: 192.168.15.88/30 (22=4 direcciones)

192.168.15.88 dirección base de la red

192.168.15.89

192.168.15.90

192.168.15.91 dirección broadcast de la red

RT1-RT2: 192.168.15.92/30 (22=4 direcciones)

192.168.15.92 dirección base de la red

192.168.15.93

192.168.15.94

192.168.15.95 dirección broadcast de la red

RT2-RT3: 192.168.15.96/30 (22=4 direcciones)

192.168.15.96 dirección base de la red

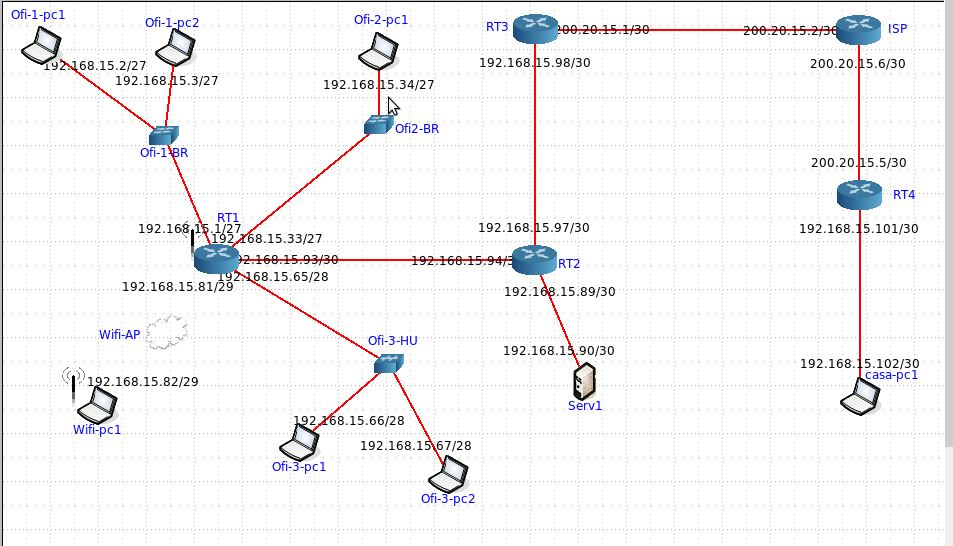
192.168.15.97

192.168.15.98

192.168.15.99 dirección broadcast de la red

2. Esquema de las redes visualizando las direcciones IP correspondientes

La distribución de los equipos no es idénticas a la presentada en el trabajo para facilitar la vista de las direcciones.

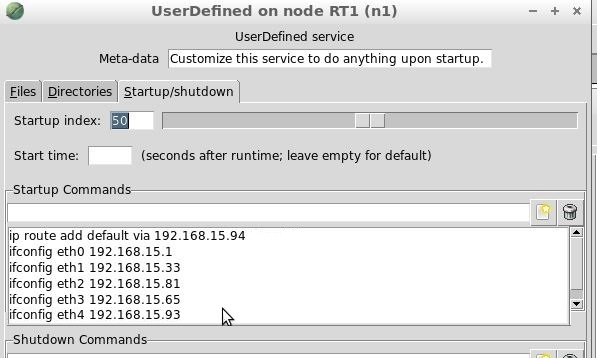


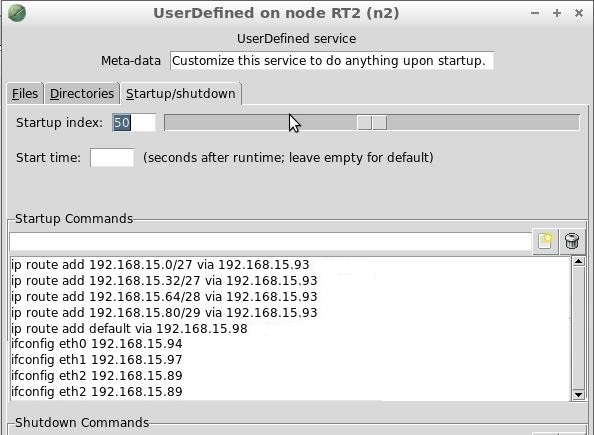
3. La implementación de la red en el emular Core se encuentra en el archivo .imn.

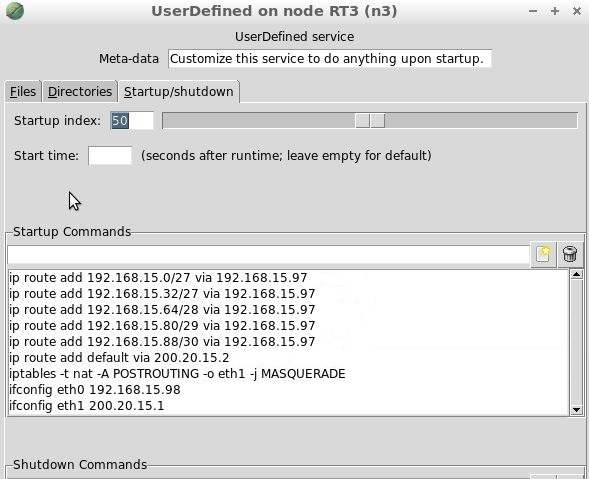
4. A continuación mostramos las capturas de la configuración de los *Userdefine* en la sección *Startaup/shutdown* de cada dispositivo con el siguiente orden RT1, RT2, RT3, RT4 e ISP. Las configuraciones se realizaron con los siguientes comandos:

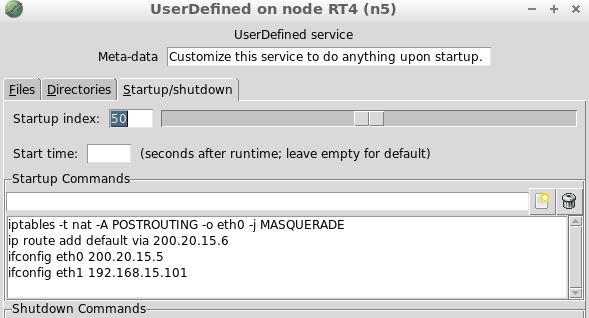
Ip route add *ipRed/mascara* via *ipProxRouterAinternet* dev *interfaz*: agrega una entrada a la tabla de reenvío de un router particular.

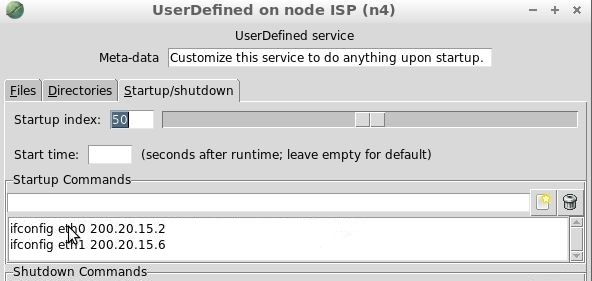
Ifconfig *interfaz ip*: Asigna interfaz a una ip particular











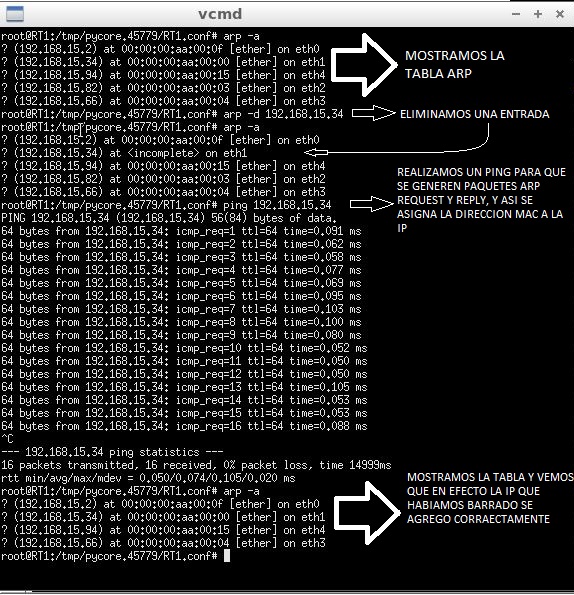
5. En la primer imagen mostramos la tabla ARP, en este caso del router 1, borramos una entrada de esa tabla (IP 192.168.15.34) y luego al hacer un ping a esa misma dirección se generaron paquetes ARP request de ida y ARP reply de vuelta, reconstituyendo la tabla nuevamente. En la siguiente imagen (captura de wireshark) se puede observar que se envía un ARP request en broadcast, esto significa que se envía una petición a todos los equipos de la red preguntando qué equipo tiene dirección requerida; y solo responderá el equipo con dicha dirección.

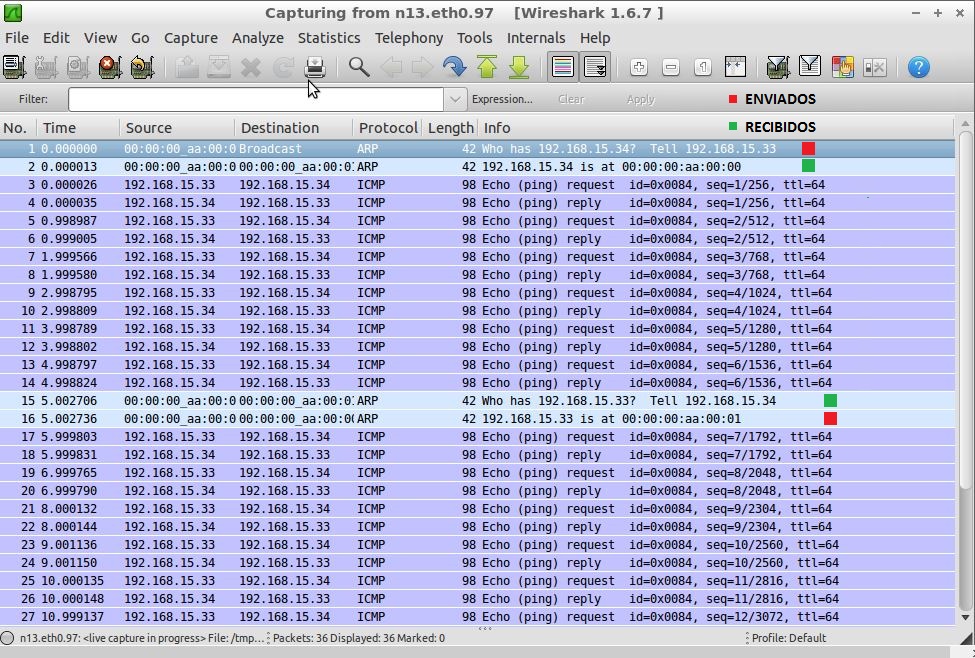
Los comandos que utilizamos en la consola son:

arp -a: muestra la tabla ARP del dispositivo en uso

arp -d *IP*: borra la *IP* de la tabla.

Ping *IPdestino*: envía paquetes *echo request* que serán respondidos con *echo reply* por el destino.





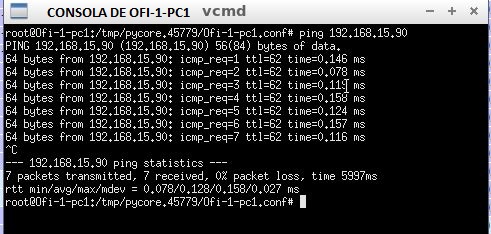
6. La función del NAT (Cambio de dirección de red – Network Address Traslation) se sitúa en el router de salida de una intranet hacia la internet.consiste en cambiar las direcciónes y puertos de los paquetes que entran o salen de la intranet. En las imágenes del inciso 4 del router RT3 y RT4 se puede ver el comando que implementa el NAT en dicho router

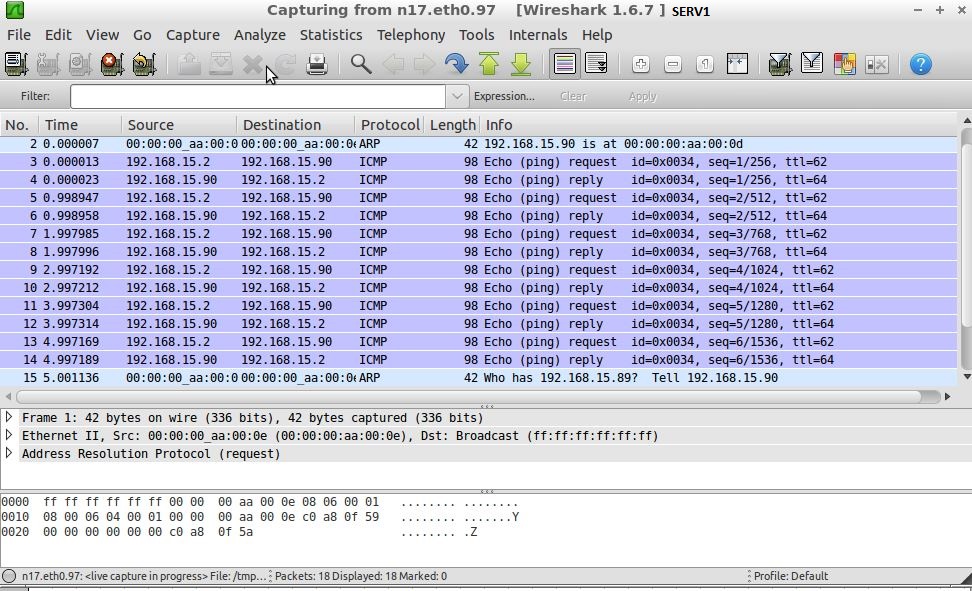
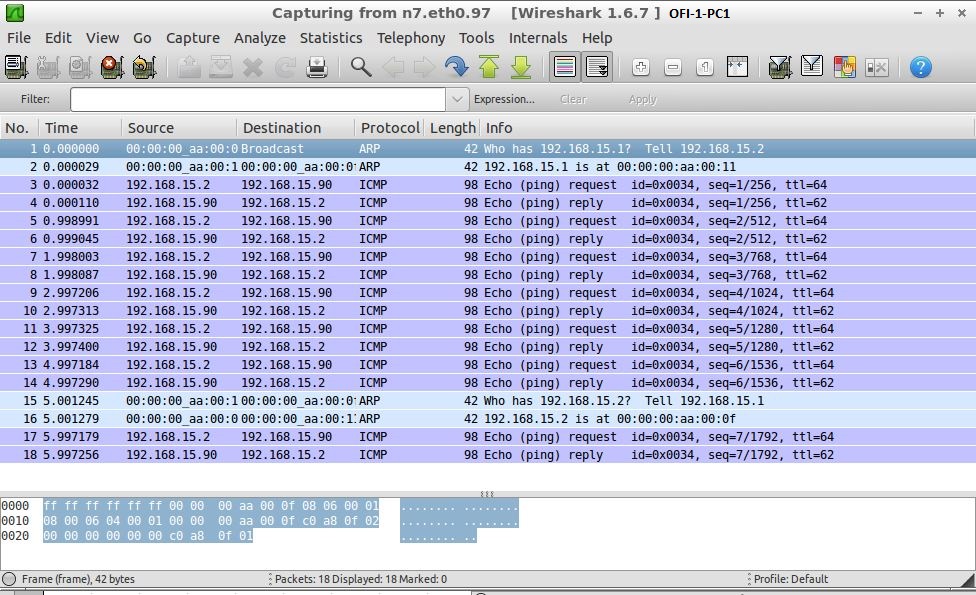
Comando usado:

Iptables -t nat -A POSTROUTING -o *interfaz* -j MASQUERADE: esto hace que todo lo que salga por la interfaz se enmascare(o cambie) su dirección IP por la dirección de esa interface del router.

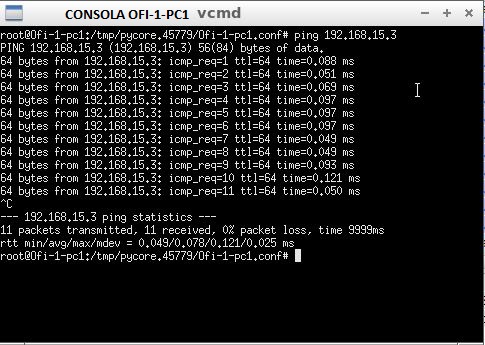
7. Aquí mostraremos ping realizados de un host específico a otro mediante capturas de consola y wireshark (analizador/monitor de tráfico de la red).

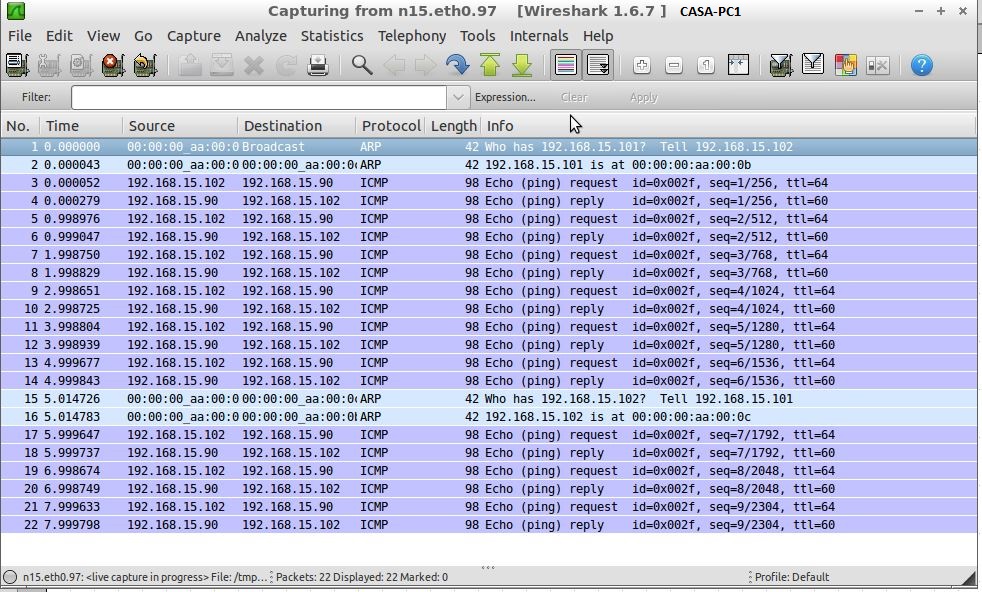
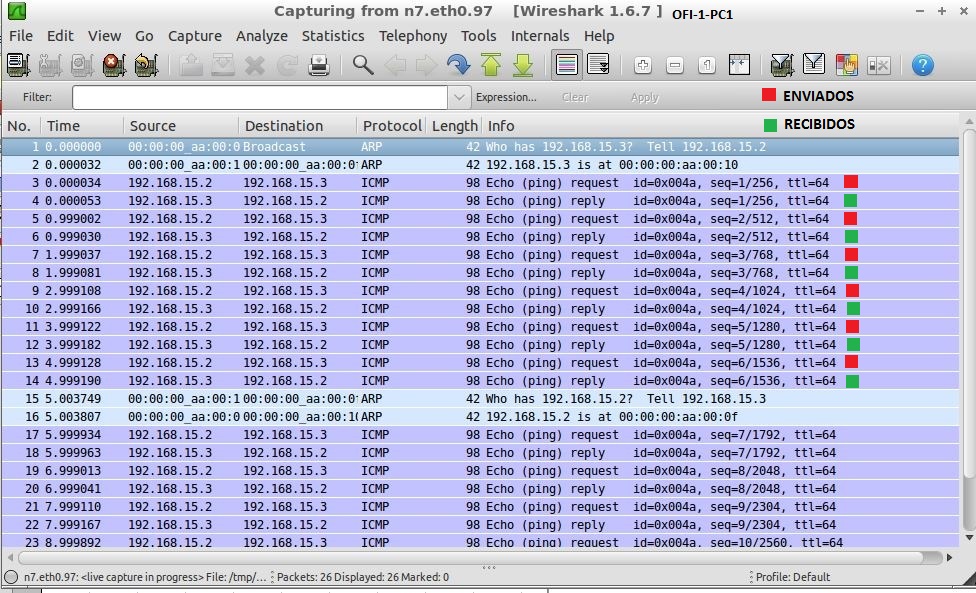
a) Ping desde Ofi-1-pc1 a serv1

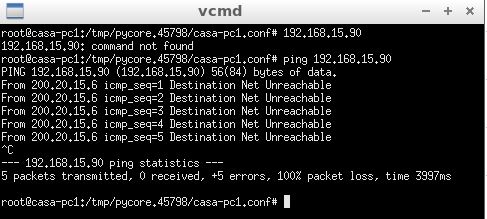


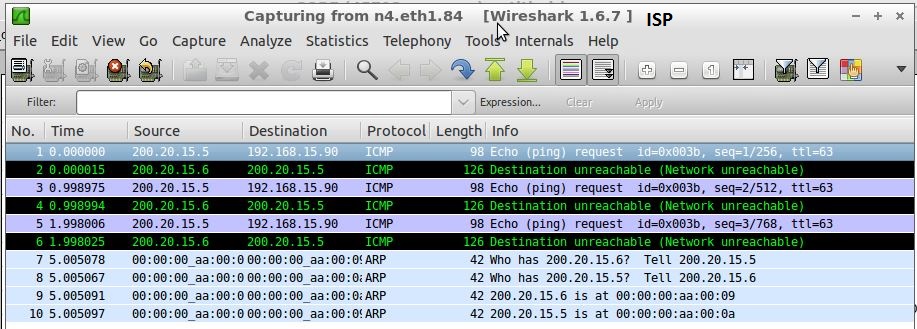


b) Ping desde Ofi-1-pc1 a Ofi-1-pc2

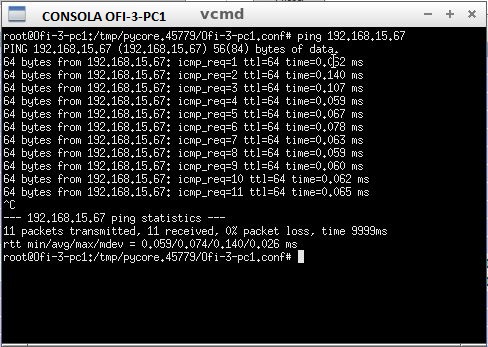


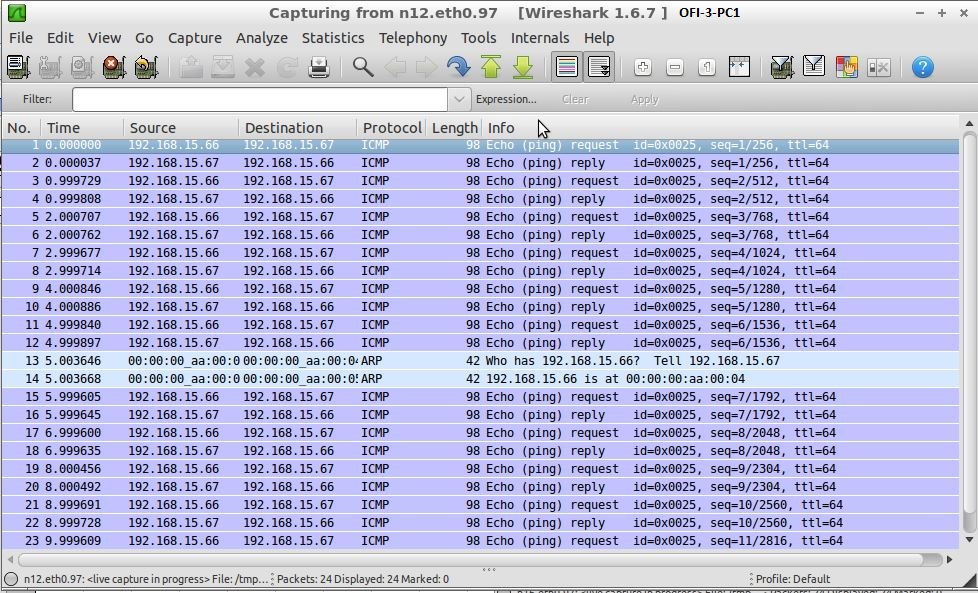
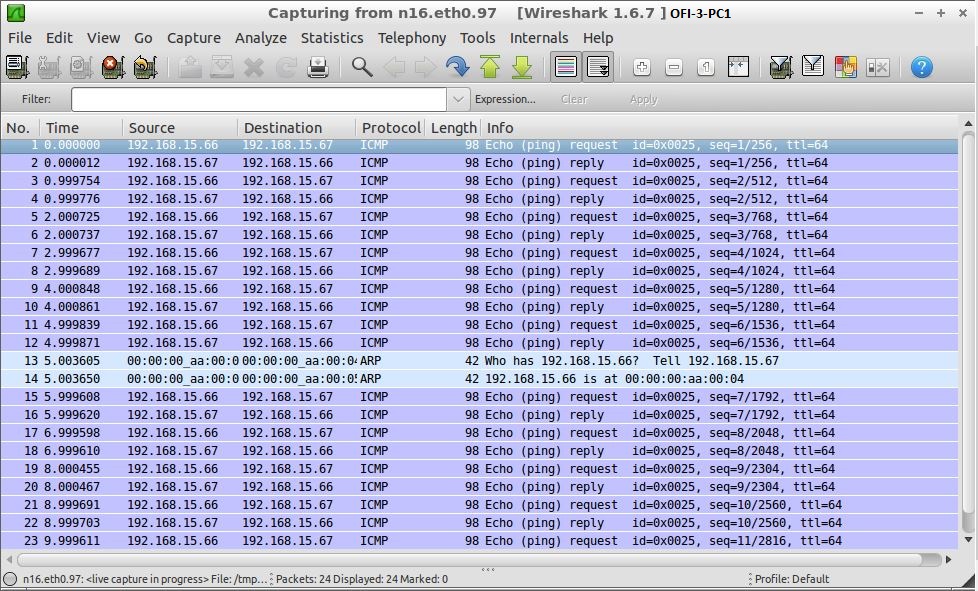


 c) Ping desde casa-pc1 a serv1

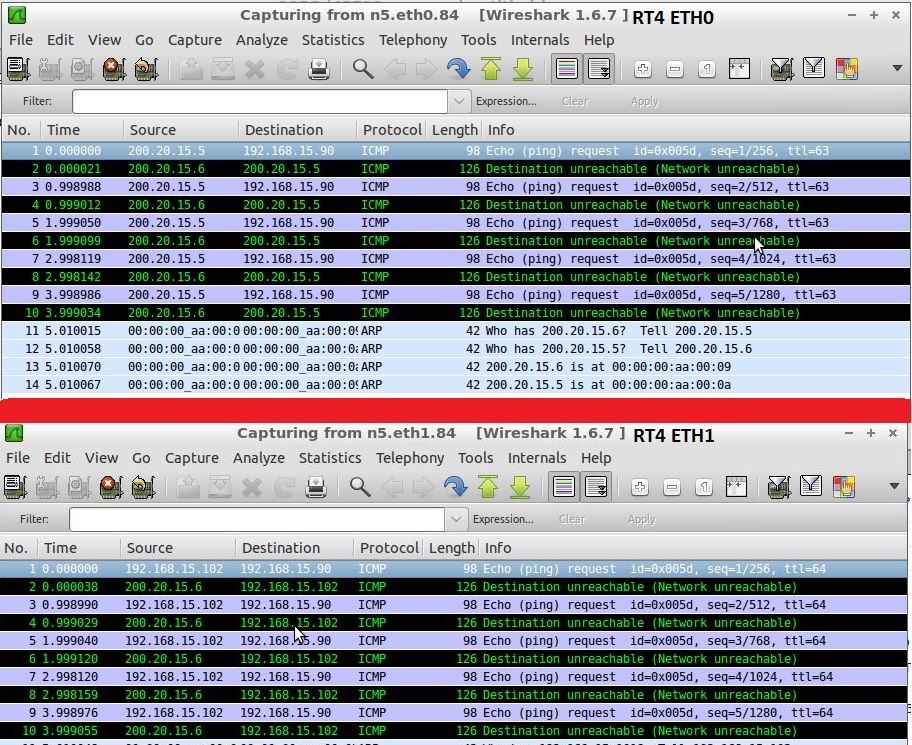


d) Ping desde Ofi-3-pc1 a Ofi-3-pc2





8. En la captura de abajo se puede observar que el router RT4 por la interfaz eth1 recibe paquetes ICMP request IP 192.168.15.102 (ping desde casa-pc1) con destino IP 192.168.15.90 (serv1) y lo envía a través de interfaz eth0 con la dirección 200.20.15.5 (enmascaro el paquete con su propia IP). Cuando recibe las respuestas ISP, la dirección de destino es la 200.20.15.5 pero el router sabe que el paquete es para casa-pc1 (IP 192.168.15.102), por el número de puerto que también bien incluido en el paquete.

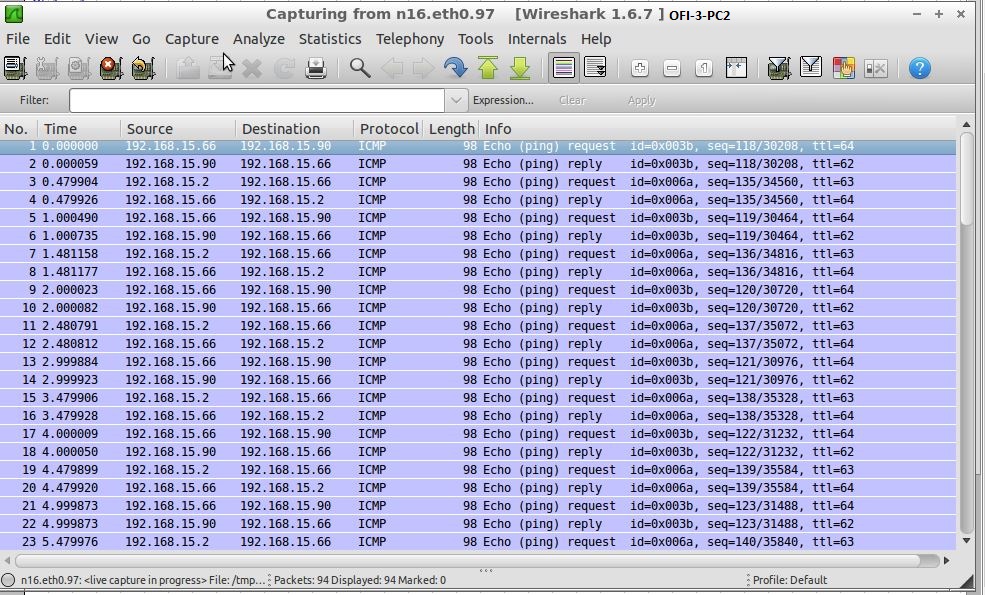
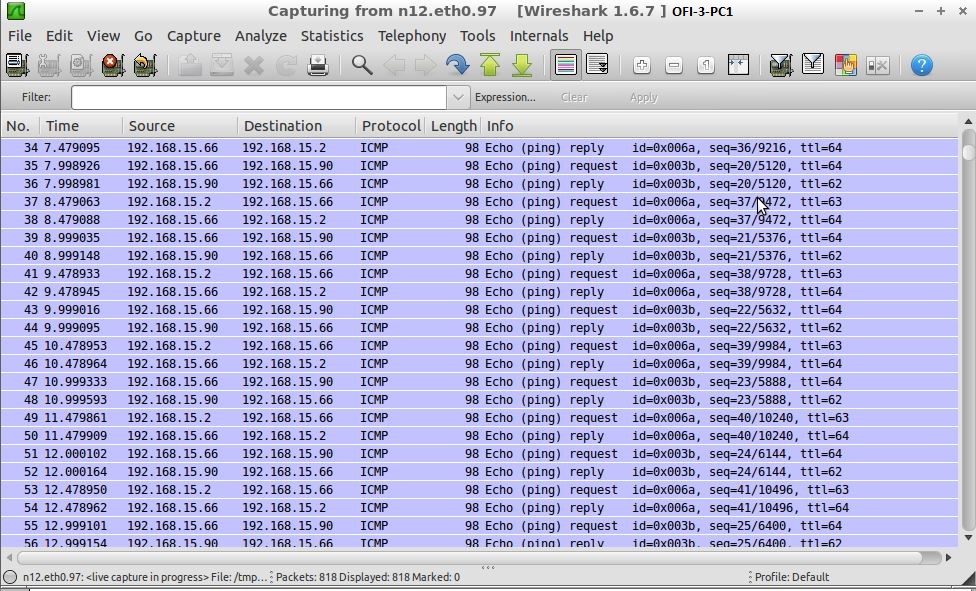


9. Comparación entre tráfico a través del hub de Ofi-3-HU y el switch de Ofi-2-BR. En primer lugar mostraremos capturas del wireshark de ofi-3-pc1 y ofi-3-pc1 y luego las capturas de wireshark de ofi-1-pc1 y ofi-1-pc2. Optamos mostrar las capturas de la oficina 1 para mostrar la diferencia entra comportamiento de un hub y un switch ya que en el esquema se solicitaba que la ofi2 solo tenga una sola pc haciendo imperceptible alguna diferencia. En lo que respecta al hub cuando le llega un paquetes lo que hace es reenviarlo por todas sus interfaces exceptuando la interfaz por la cual ese paquete llegó, de esta manera todos los dispositivos que esten conectados al hub recibirán el paquete, pero al analizar la ip destino del paquete y no concordar con esta ese paquete es rechazado; obviamente será aceptado por el destino que tenga la ip destino en dicho datagrama. Por otro lado el switch de alguna manera se da cuenta o sabe que por tal interfaz esta tal ip así solo es destinatario correcto recibirá ese paquete.

Para crear un poco de tráfico hicimos ping desde:

* Ofi1-pc1 hacia ofi3-pc1
* Ofi3-pc1 hacia serv1

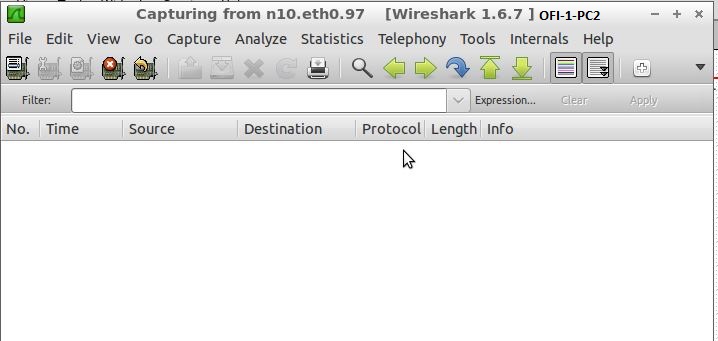
En las siguientes dos capturas podemos observar que tanto la pc1 y la pc2 reciben los mismos paquetes, que solo deberían ser recibidos por pc1.



EL trafico se genero con los siguientes ping

* Ofi-pc1 hacia RT2
* De ofi3-pc1 hacia ofi1-pc1

Por otro lado vemos que en la captura del wireshark de la red switcheada(Offi 1), solo la pc1 recibe los paquetes que envía el RT1 al switch, notándose asi la diferencia entre un HUB y un switch.





10. Los precios que a continuación listaremos son relativos, esto es que pueden variar con el tiempo o con la economía del país. Más precisamente nos basamos en precio que están actualmente en MercadoLibre

1 Hub Officeconnect 8 puertos $180 (oficina 3)

2 Switch Tp-Link de 16 pouertos $539 (oficina 1 y 2)

1 Router inalámbrico(wifi) Tp-Link 4 puertos $648 (red wifi)

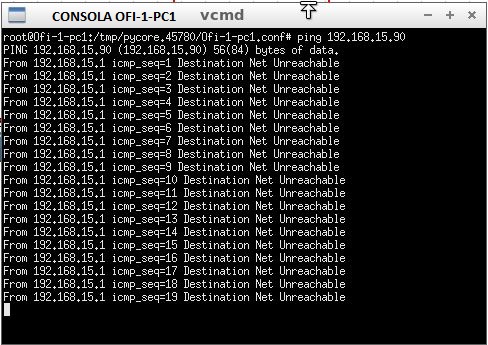
1 Router LinkSys 4 puertos $500 (RT1)

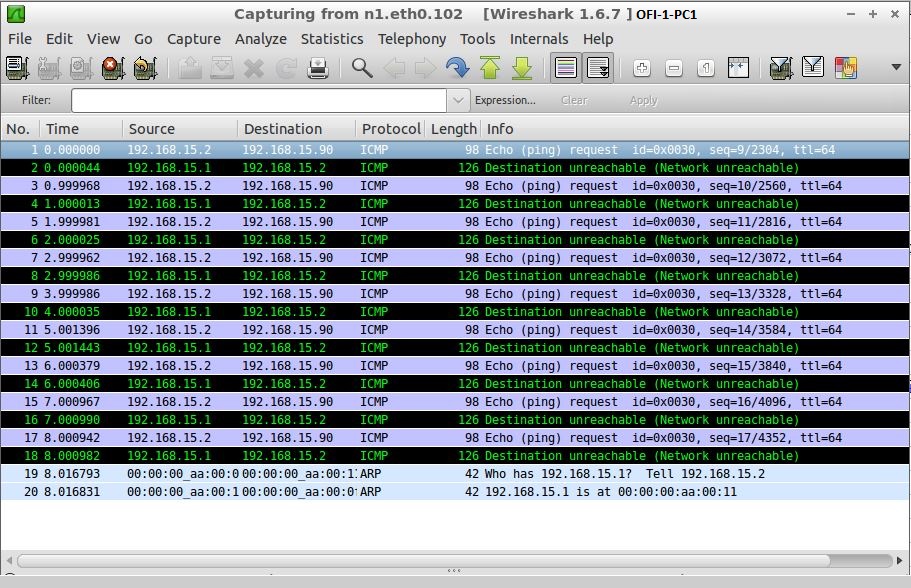
1 route TpLink 2 puertos $340

Total: $2746

11. Se deben generan error de distinto tipo mediante configuraciones erróneas de router o mediante alguna opción de un comando especifico por la consola.

a) Destination network unreachable: este error se da cuando no se puede entregar los paquetes, esto es cuando el router no encuentra la ruta se acceso o el paquete no puede ser fragmentado. Se le hizo ping desde ofi-1-pc1 a serv1, habiendo borrado la entrada default del router. De esta forma el router no puede resolver el reenvío de los paquetes, que genera el error, Destination network unreachable, enviado del router RT1 a ofi-1-pc1 como respuesta.

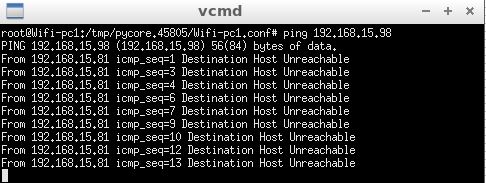




b) Parecido al anterior. Con ‘ifconfig’ indicamos que la red WIFI se encontraba a traves de la interface de otra red en RT1.



Luego hicimos un ping desde La pc de la red WIFI hacia el RT3 y nos muestra el siguiente error:

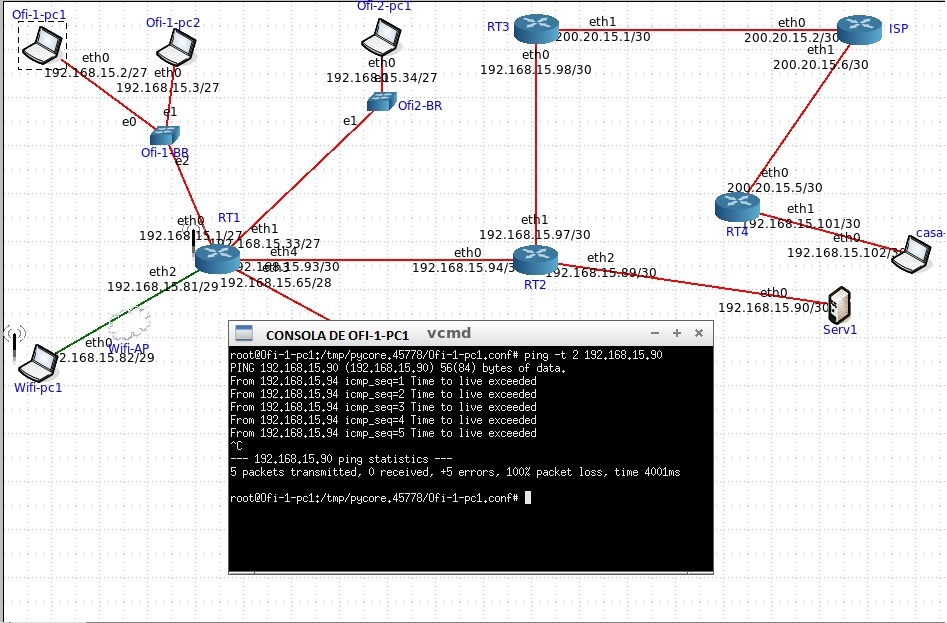


c) Time Exceeded: este error de debe generan utilizando un tratamiento especial del comendo -ping *ipdestino*- de la siguiente forma:

ping -t *nºTTLarbitratio ipdestino.*

De esta forma le indicamos que esos paquetes tengan una TTL (tiempo de vida) asignado por nosotros. El TTLfunciona de la siguiente manera si tenemos por ejemplo la siguiente red: hostA-Router1-Router2-hostB y asigno un TTL de 2 el paquete nunca va a llegar a destino ya que el TTL se disminuye en uno al llegar a un dispositivo en este caso a un router entonces, cuando el paquete llega al Router1 TTL = 1, cuando llega al Router2 TTL = 0. Al querer el Router2 enviarlo al hostB el TTL no puede disminuir (también se dice que el paquete murió) entonces se produce el error Time Exceeded.

Para mostrar esto en la simulación en Core lo que hicimos fue querer hacer un ping desde Ofi-1-pc1 a Serv1 con un TTL = 2 con el comando: ping -t 2 192.168.15.90 desde la consola de ofi-1-pc



12. Traceroute. El comando traceroute *ip/interfazDestino* funciona de la siguiente manera: La fuente envía una serie de segmentos UDP al destino usando TTL = 1 luego TTL = 2, etc y un numero de puerto (quizá) no utilizado por el destino. Cuando el datagrama n llega al router n, el router descarta el datagrama y envía a la fuente un mensaje ICMP “TTL expirado”, este mensaje incluye el nombre del router y dirección IP. En el momento que el mensaje ICMP llega, la fuente calcula el RTT (Round Trip Time). El traceroute hace este procedimiento 3 veces. Los criterios de parada son: el segmento UDP eventualmente llega a destino, el host destino retorna un paquete ICMP “unreachable port” (puerto inalcanzable) y cuando la fuente recibe este mensaje.

