Práctica 4 – Capa de Red

**1. ¿Qué servicios presta la capa de red? ¿Cuál es la PDU en esta capa? ¿Qué dispositivo es considerado sólo de la capa de red?**

La capa de Red permite la conexión desde un host origen a un host destino. En TCP/IP está implementada en el protocolo IP, e interviene en cada host y encaminador intermedio (router)

El PDU es el datagrama, que encapsula los segmentos de transporte agregándole las direcciones IP origen y destino entre otras cosas.

El dispositivo de capa de Red es el router.

Acorde a los dos servicios de la capa de Red, este dispositivo debe:

* Ejecutar algoritmos/protocolos de enrutamiento que seleccionen hacia dónde reenviar un datagrama recibido.
* Encaminar/conmutar los datagramas que llegan a una interfaz o puerto de entrada, a la interfaz o puerto de salida seleccionada por el algoritmo. La conmutación puede hacerse vía memoria -control directo de una CPU-, vía bus compartido en el router o vía crossbar o red de interconexión.

**2. En las redes IP el ruteo puede configurarse en forma estática o en forma dinámica. Indique ventajas y desventajas de cada método.**

Ruteo estático o dinámico: es una clasificación de los algoritmos de ruteo.

* Estático: las rutas cambian muy lentamente a lo largo del tiempo, normalmente como resultado de una intervención humana (porque la persona edita manualmente las tablas de encaminamiento).
* Las rutas son establecidas por el administrador manualmente.
* Propenso a errores.
* Si se cambia la topolog ́ıa requiere cambios manuales en los
* routers.
* Sirve cuando se tiene una red sencilla.
* No tiene problemas de seguridad ni de incompatibilidad.
* No implica costo de procesamiento extra.
* Esquema NO escalable y NO tolerante a fallos
* Dinámico: cambian los caminos de rutado según cambia la carga del trafico o la topología de la red. Un algoritmo dinámico podrá ejecutarse bien periódicamente, o bien en respuesta directa a un cambio en la topología o en los costes de los enlaces.
* Requiere una configuración inicial por el administrador.
* Si se cambia la topología se adapta de forma automática.
* Facilita cuando se tiene una red compleja.
* Implica costo de procesamiento extra.
* Esquema escalable y tolerante a fallos.

**3. Una máquina conectada a una red pero no a Internet, ¿tiene tabla de ruteo?**

Si, es la que se ve con el comando 'route' o 'netstat -r'.

**4. ¿Cuántas redes clase A, B y C hay? ¿Cuántos hosts como máximo pueden tener cada una?**

Clase A: 128 redes 16.777.214 hosts

Clase B: 16.384 redes 65.534 hosts

Clase C: 2.097.152 redes 254 hosts

**5. ¿Qué son las subredes? ¿Por qué es importante siempre especificar la máscara de subred asociada?**

La división de subredes es la obtención de otras direcciones de red basadas en una sola dirección con el uso de la **máscara de subred**, "*pidiendo bits prestados*" a la parte del host/interface (dependiendo de la cantidad de bits que se pidan, será la cantidad de subredes que se creen a partir de la original).  
Una subred es un **rango de direcciones lógicas**. Cuando una red se vuelve muy grande, conviene dividirla en subredes, para reducir el tamaño de los dominios de broadcast, y hacer la red más manejable.  
Típicamente los routers constituyen los límites entre las subredes. La comunicación desde/hasta otras subredes es hecha mediante un router específico. Sin embargo, las subredes permiten dividir lógicamente una red a pesar de su diseño físico, pudiéndose dividir en varias subredes configurando diferentes host que utilicen diferentes routers. La dirección de todos los nodos en una subred comienzan con la misma secuencia binaria, que es su ID de red e ID de subred (en IPv4, las subredes deben ser identificadas por la **base** de la dirección y una **máscara de subred**).  
Las subredes simplifican el enrutamiento, representándose típicamente cada una como una fila en las tablas de ruteo en cada router conectado. Fueron usadas antes de IPv4 para permitir a una red grande tener un número importante de redes más pequeñas dentro, controladas por varios routers.  
Permiten el Enrutamiento Interdominio Sin Clases (**CIDR**).  
Los últimos dos bits del último octeto (los menos significativos) nunca se asignan a la subred, sea cual sea la clase de dirección IP. **Como consecuencia, una dirección de subred jamás terminará en un número impar**. Por otra parte, el uso de todos los bits disponibles para crear subredes dará como resultado subredes con sólo dos Hosts utilizables (un método práctico de conservación de direcciones para el direccionamiento de enlace *punto a punto*, donde no existe otro direccionamiento más que los dos enlaces conectado entre sí).

**6. Practica**

**7. Practica**

**8. Practica**

**9. Practica**

**10.Describa qué es y para qué sirve el protocolo ICMP.**

Internet Control Message Protocol (ICMP) es un protocolo de L3. Es un protocolo “helper” de IP, ya que se utiliza para brindarle un “feedback” y resolver problemas en la red.

ICMP se encapsula en IP y no es un protocolo de transporte (ya que no fue concebido para llevar datos de usuario)

Algunos mensajes ICMP:

* Echo Request/Echo Reply (PING).
* Destino Inalcanzable.
* TTL expirado.
* Source Quench (Control de Congestión).
* Redirección de Ruta.
* Address Mask y Timestamp.

**(a) Analice como funciona el comando ping**

**ping -bfr -c *count* -i *interval -*I *interface|adress -*s *packetsize* -t *ttl* -w *deadline* -W *timeout* IPDestino**

Utiliza el protocolo ICMP para solicitar a un host/gateway una respuesta de *echo*. Envía un datagrama **ECHO\_REQUEST** al IP indicado. Útil para controlar que una interfaz este funcionando o que hay conectividad. Al terminar, muestra algunas estadísticas como cantidad de paquetes perdidos, TTL mínimo/medio/máximo...

**I. Indique el tipo y código ICMP que usa el ping.**

Type 8 (Echo Request)

Code 0

**II. Indique el tipo y código ICMP que usa la respuesta de un ping.**

Type 0 (Echo Reply)

Code 0

**(b) Analice como funciona el comando traceroute (tracert en Windows) y como manipula el campo TTL de los paquetes IP**

**traceroute -4|6 -ITFn -f *firstTTL* -m *maxTTL* -N *squeries* -p *port* -q *nqueries* host**

Muestra la ruta que siguen los paquetes por la red hasta llegar a un destino.  
Utiliza el campo TTL de IP, enviando paquetes con valores incrementales desde TTL=1, y recibiendo las respuestas ICMP de tipo TIME\_EXCEEDED de cada gateway/router en el camino hasta el destino.  
Para cada valor de TTL envía tres paquetes, luego imprime el gateway que respondió y el RTT obtenido. Si no obtiene respuesta en 5 segundos (por defecto) para algún paquete, imprime un asterisco. Los paquetes se envían a un puerto UDP que difícilmente se utilice, de modo que al llegar al destino, éste responda un ICMP PORT\_UNREACHABLE o un segemento TCP de tipo RESET, denegando la conexión.

**I. Indique el tipo y código ICMP del cuál se vale el comando traceroute para funcionar.**

Type 11 (Time-To-Live Exceeded)

Code 0 (Time to live exceeded in transit)

**Utilizar una topologia de core para verificar el funcionamiento de estas herramientas**

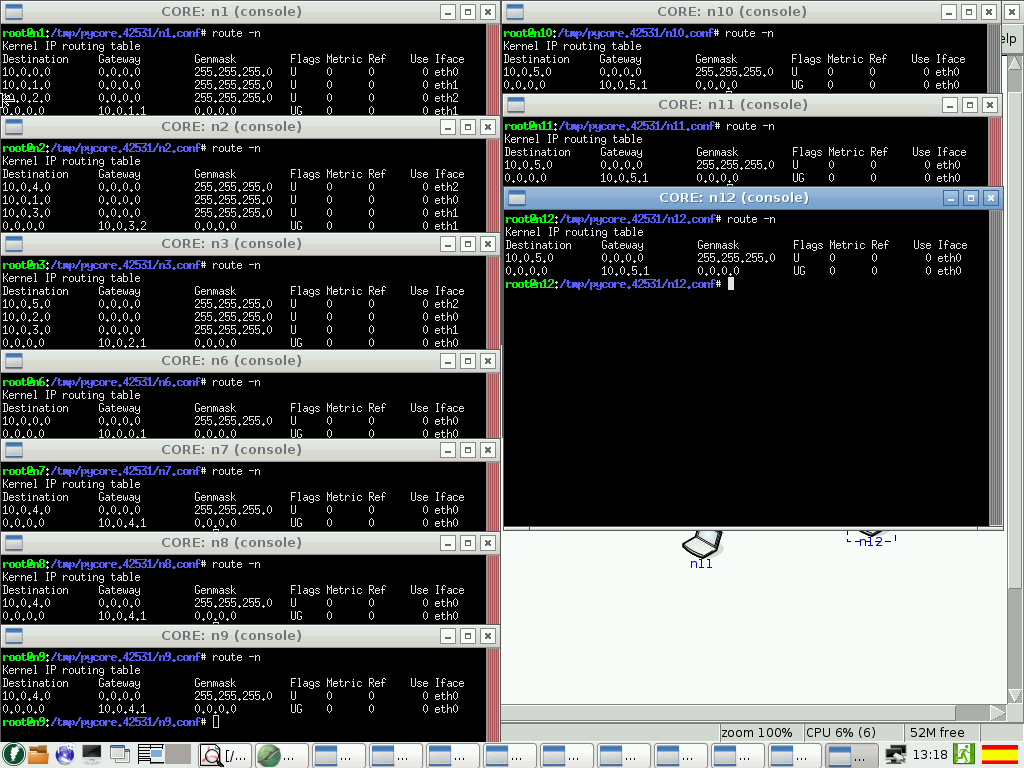
**11.¿Para que se usa el bloque 127.0.0.0/8? ¿Qué PC responde a los siguientes comandos?:**

**ping 127.0.0.1**

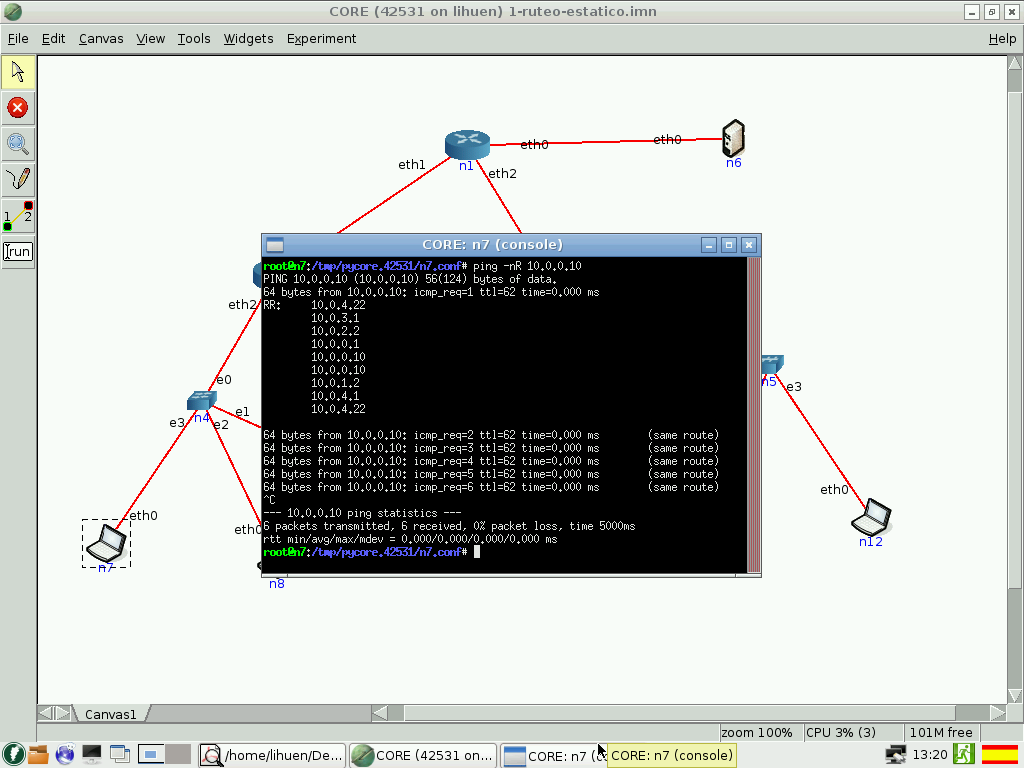
**ping 127.0.54.43**

La direccion 127.0.0.1, denominada *loopback* o *localhost*, es una dirección reservada (toda la gama 127.x.x.x tiene el mismo efecto, ya que se encuentra reservada para igual propósito) que poseen todos los dispositivos (computadoras, routers), independientemente de si disponen o no de una interfaz de red, que **apunta a si mismos**, por lo cual no llega a salir nunca por la interfaz. Sus fines pueden ser para comprobar el funcionamiento de TCP/IP haciendo *ping 127.0.0.1*, al recibir respuesta se puede asumir que el software asociado al protocolo está bien (el hardware como la tarjeta de red no lo conocemos con esta prueba, ya que no llega a salir del propioequipo).

**12. Practica**

**e.**

**e. I**

****

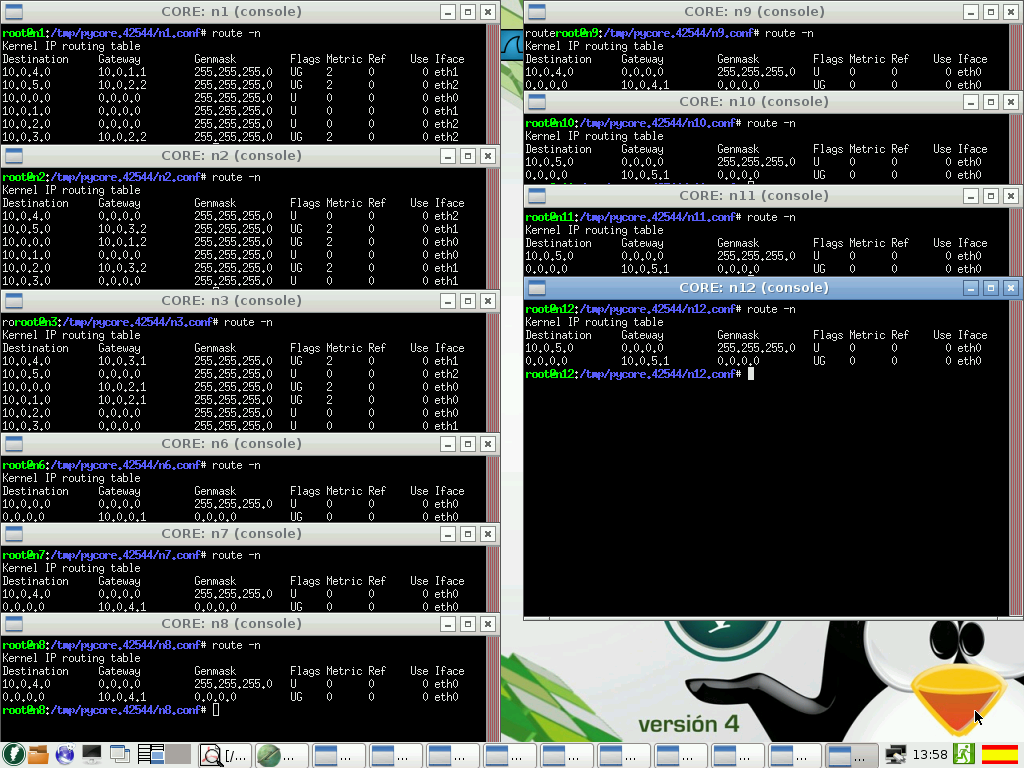
**f.** Sin hacer

**g.** Time To Live Exceeded. Lo envía 10.0.0.1 (Router n1)

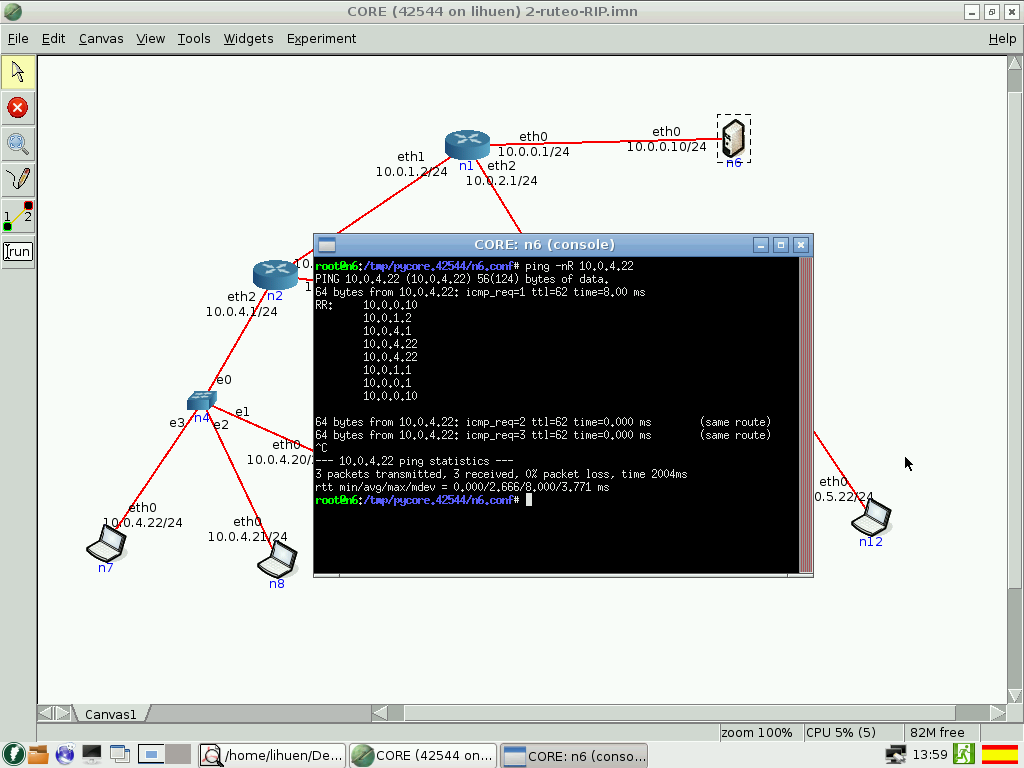
**h.** Destination Host Unreachable. Lo envía 10.0.2.2 (Router n3)

**i.** Time To Live Exceeded. Lo envía 10.0.0.1 (Router n1)

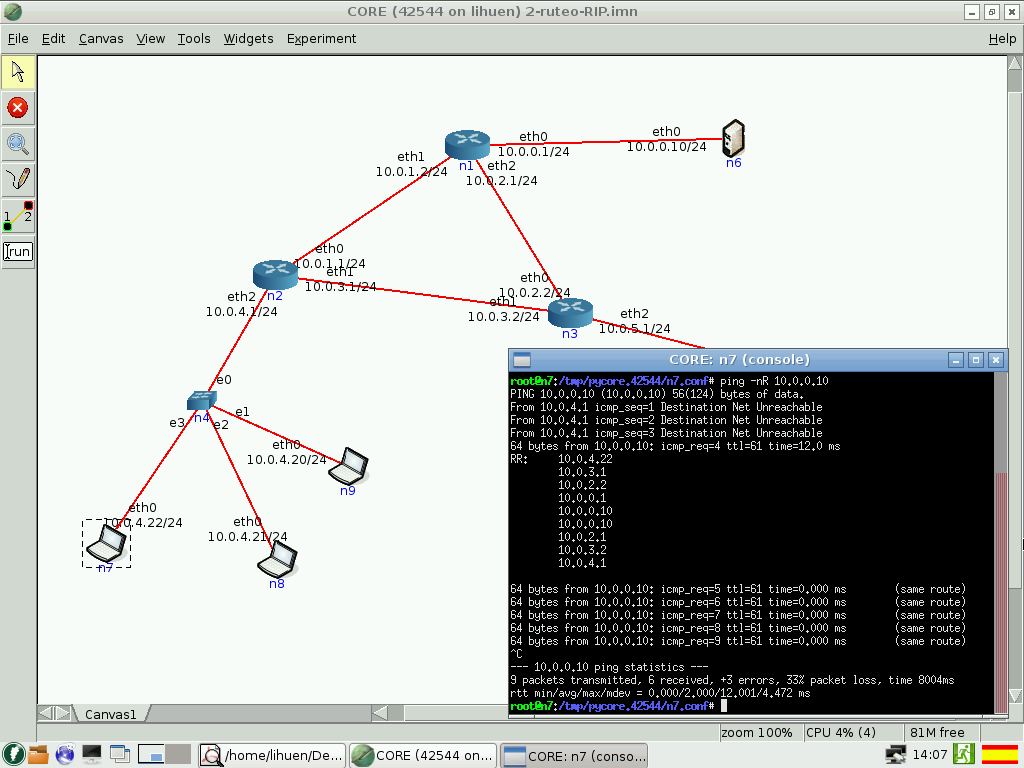
**13. ALGORITMO RIP**

**c.**

**c.i.**

****

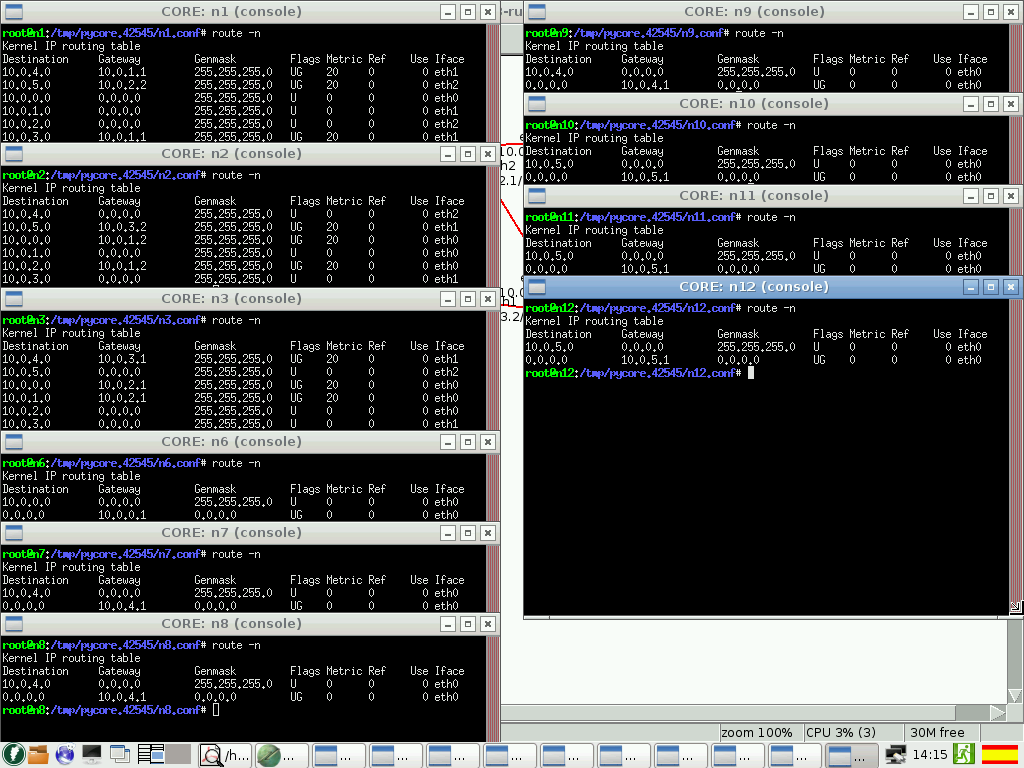
**d.**

****

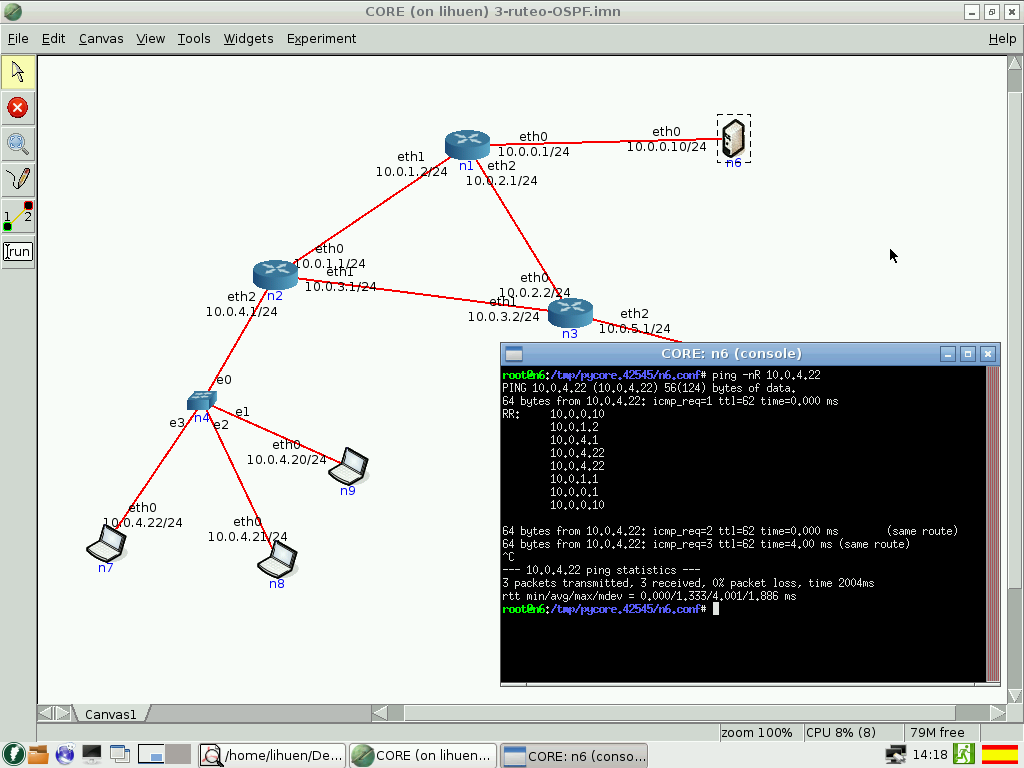
Sigue funcionando, toma otra ruta.

**13. OSPF**

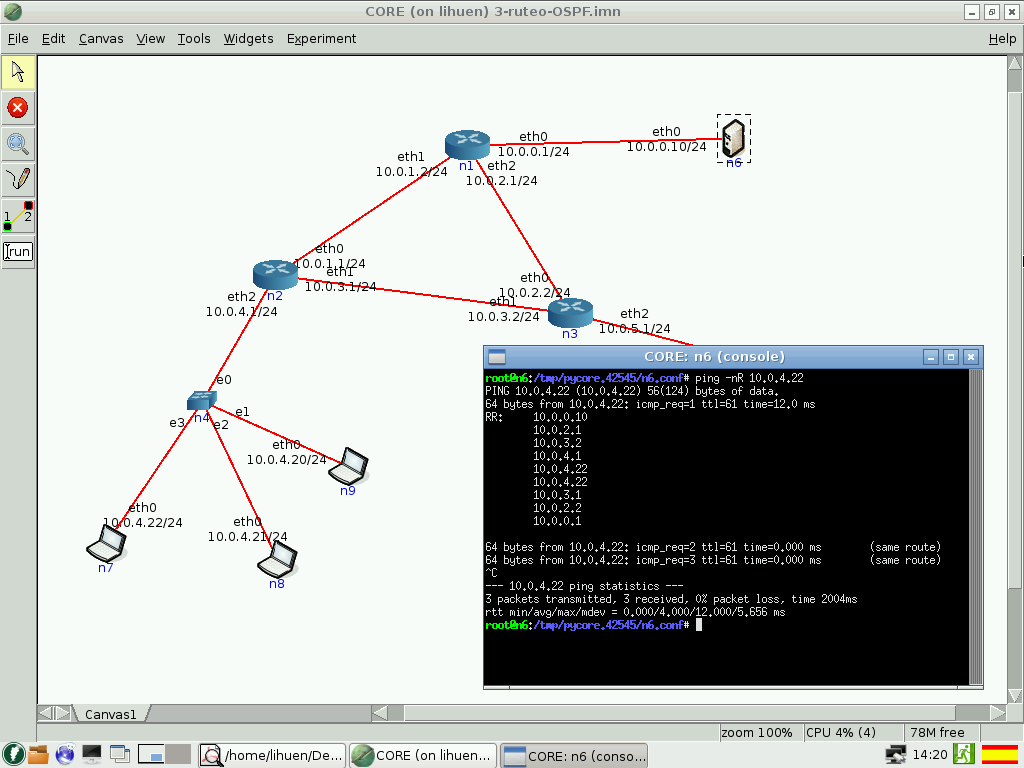
**c.**

****

**c.i.**

****

**d.**

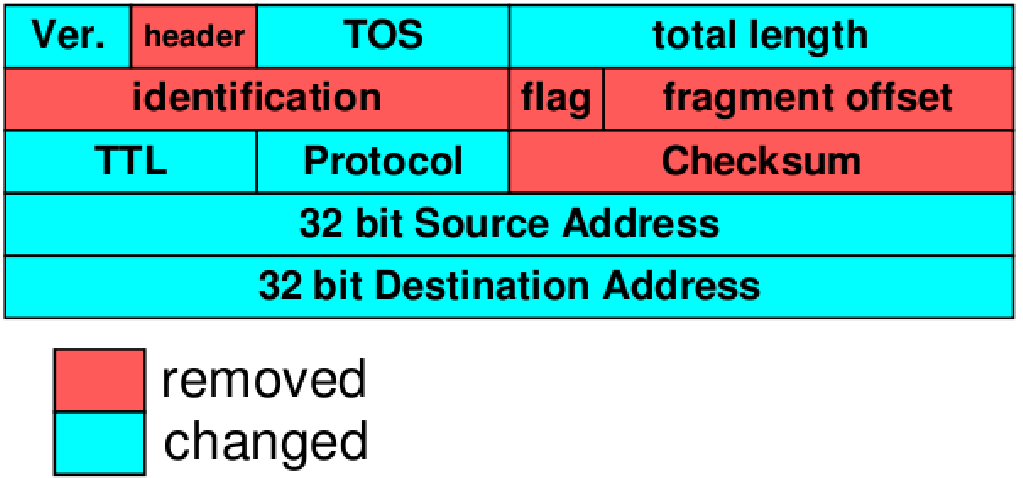
****

Sigue funcionando tomando otra ruta.

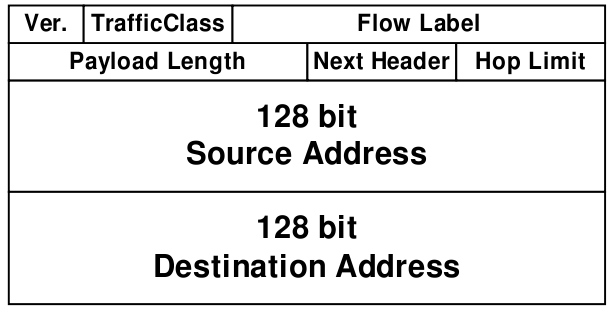
**14.¿Qué es Ipv6? Enumere diferencias existentes en el formato de datagramas respecto de IPv4**

El protocolo Internet versión 6 (IPv6) es una nueva versión de IP (Internet Protocol), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, actualmente en uso dominante.  
IPv4 posibilita 4.294.967.296 (2³²) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera.

En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2¹²⁸ o 340 sixtillones de direcciones) —cerca de 3.4 × 1020 (340 trillones de direcciones) por cada pulgada cuadrada (6.7 × 1017 o 670 mil billones de direcciones/mm2) de la superficie de La Tierra.  
  
Cambios en el datagrama con respecto a IPv4:



Mensaje IPv6:



* Datagramas de 40B.
* Se saca la fragmentación, se deja solo de extremo a extremo como opción.
* Se saca checksum de cabecera.
* Se deja de tamaño fijo el header, se sacan opciones.
* Flowlabel: id de flujo.
* Renombres, TrafficClass, HopLimit, NextHeader.
* Cabeceras de extensión.

**15.**

**D.**

**I.** Tanto en la pc n6 como n7 se observan 2 IPv6 en la interfaz eth0 (1 ip más para la interfaz lo).

**II.** No. No se.

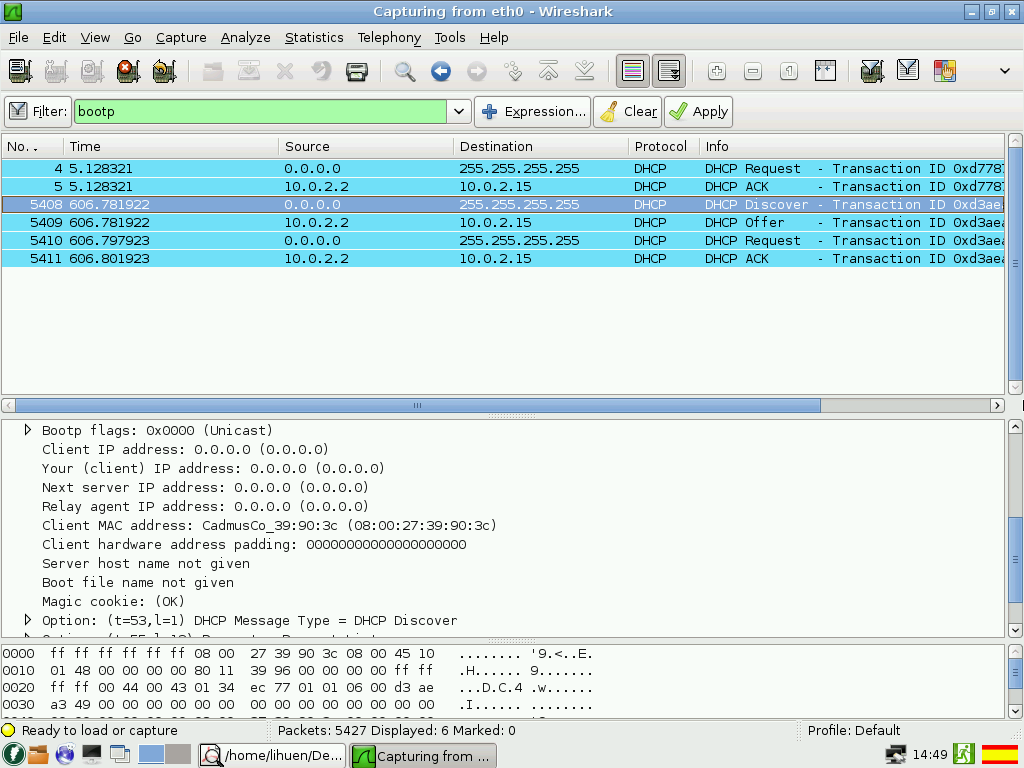
**III.** No se.

**E. ?**

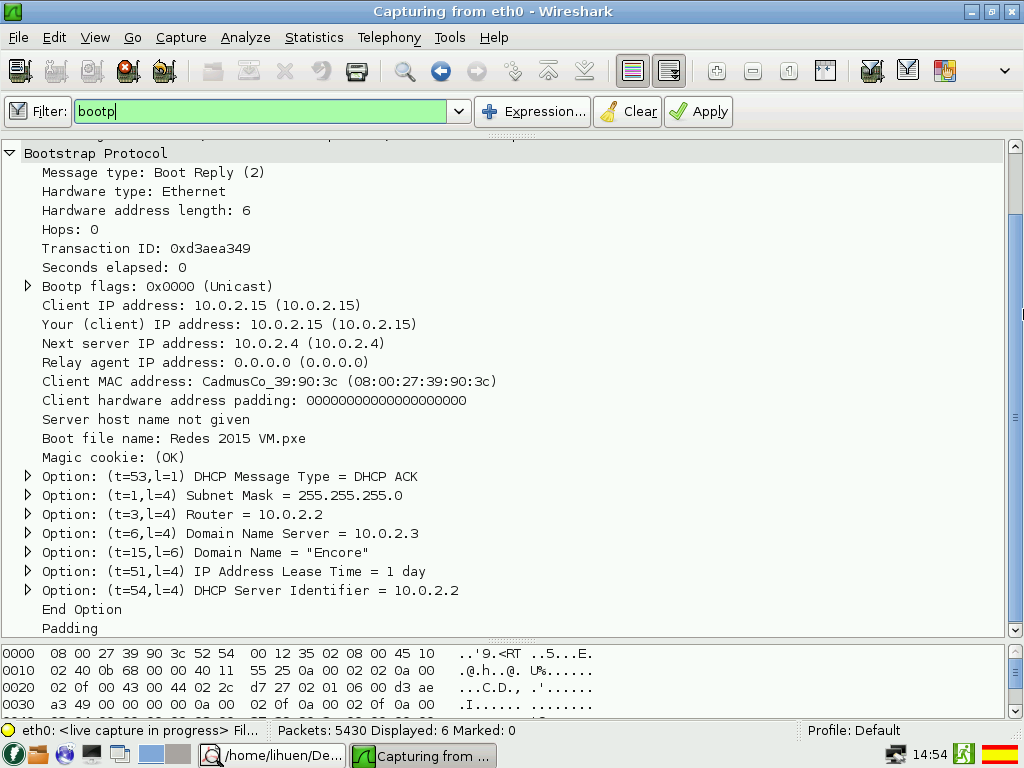
**16. Practica**

**C.** El archivo dhclient.leases guarda los últimos arrendamientos (leases) dhcp que todavía son válidos. En caso de haber más de uno, utiliza el último.

**D.** Tras eliminar el archivo dhclient.leases y ejecutar dhclient eth0, se capturó otro tráfico DHCP en el que se pide dirección ip a la red (Discover). En el anterior no pasó eso (solo se capturó request y response), ya que la máquina ya tenía una ip asociada en su archivo dhclient.leases.



**f.** El DHCP ACK es la respuesta que le llega al host que inicio el pedido. Este mensaje contiene la siguiente información:



**17.¿Qué es NAT y para qué sirve? De un ejemplo de su uso y analice cómo funcionaría en ese entorno.**

**Ayuda: analizar el servicio de Internet hogareño en el cual varios dispositivos usan Internet**

**simultáneamente.**

**NAT** (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados.   
Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único (PAT). Estas traducciones de dirección se **almacenan en una tabla**, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la **red interna** no existe en la tabla de traducciones, entonces es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina NAT inverso o DNAT (Destination NAT).  
NAT tiene muchas formas de funcionamiento, entre las que destacan: estatico, dinamico y de sobrecarga.  
  
En un hogar con un router y 3 maquinas conectadas a el, las mismas tienen la misma IP publica (en internet) que es la que asigna el ISP local; pero “adentro” de la LAN tienen IPs privadas (del rago reservado para direcciones privadas de cada clase A, B, C o D). Entonces el router hace NAT, esto es editar cada paquete emitido por alguna maquina, cambiando la IP origen (que viene de la LAN y es privada) por la IP publica, también puede hacer PAT (traducción de puertos).

**18.¿Qué especifica la RFC 1918 y cómo se relaciona con NAT?**

Especifica el rango de direcciones privadas dentro de cada clase de direcciones IP.  
  
10.0.0.0 - 10.255.255.255 (prefijo 10/8)   
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)   
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)  
  
“Nos referiremos al primer bloque como "bloque de 24 bits", al segundo como "bloque de 20 bits" y al tercero como "bloque de 16 bits".

Dese cuenta que (en la notación anterior a CIDR) el primer bloque no es más que un único número de red de clase A, mientras que el segundo bloque es un conjunto de 16 números de red de clase B contiguos, y el tercer bloque es un conjunto de 256 números de red de clase C contiguos.”  
  
Esto se relaciona con NAT dándole uso a las direcciones privadas en una red local y a través de NAT traducirlas a IP publicas.

**19.¿Que es CIDR (Class Interdomain routing)? ¿Por qué resulta útil?**

**Classless Inter-Domain Routing** (**CIDR** Encaminamiento Inter-Dominios sin Clases) es una mejora en el modo como se interpretan las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas, reemplazando la sintaxis previa para nombrar direcciones IP, las **clases** de redes.  
CIDR usa la técnica **VLSM** (**Variable-Length Subnet Masking** - Máscara de Subred de Longitud Variable), para hacer posible la asignación de prefijos de longitud arbitraria (la división red/host puede ocurrir en cualquier bit de los 32 que componen la dirección IP).  
Un gran beneficio de CIDR es la posibilidad de agregar prefijos de encaminamiento -**supernetting**-. Por ejemplo, dieciséis redes /24 contíguas pueden ser agregadas y publicadas en los routers como una sola ruta /20 (si los primeros 20 bits de sus respectivas redes coinciden). Dos redes /20 contiguas pueden ser agregadas en una /19, etc. Esto permite reducir significativamente el número de rutas que los routers tienen que conocer (reduciendo memoria, recursos, etc.) y previene una explosión de tablas de encaminamiento.  
Decimos que una dirección IP **está incluida** en un **bloque CIDR**, y que **encaja** con el prefijo CIDR, si los N bits iniciales de la dirección y el prefijo son iguales. Por tanto, para entender CIDR es necesario visualizar la dirección IP en binario.

**20. Practica**

**21. Practica**

**22. Practica**

**23.**

**Con OISPF (estado de enlace) = 1:37.83 seg**

**Con RIP (vector distancia) = 1:34.77 seg**

**24. Los algoritmos de ruteo dinámico se dividen en estado enlace y vector distancia.**

**Dado el siguiente cuadro compare:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ¿Cada router conoce la topología de la red completa? | ¿Converge rápidamente? | Protocolos que lo implementan |
| Vector distancia | No | No | RIP |
| Estado de enlace | Si | Si | OISPF |

**25.¿Qué son los sistemas autónomos? ¿Qué es necesario para que los distintos sistemas autónomos puedan rutear tráfico entre hosts que pertenecen a diferentes sistemas autónomos?**

Un Sistema Autónomo (en inglés, Autonomous System: AS) es un conjunto de redes y dispositivos router IP que se encuentran administrados por una sola entidad (o en algunas ocasiones varias) que cuentan con una política común de definición de trayectorias para Internet.

Los Sistemas Autónomos se comunican entre sí mediante routers BGP y se intercambian el tráfico de Internet que va de una red a la otra. A su vez cada Sistema Autónomo es como una Internet en pequeño, ya que su rol se llevaba a cabo por una sola entidad, típicamente un Proveedor de Servicio de Internet (ISP) o una gran organización con conexiones independientes a múltiples redes, las cuales se apegaban a una sola y clara política de definición de trayectorias definida.

Técnicamente un Sistema Autónomo se define como “un grupo de redes IP que poseen una política de rutas propia e independiente”. Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet.

Aún considerando que el ISP podía soportar múltiples sistemas autónomos, Internet solo considera la política de definición de trayectorias establecida por el ISP. Por lo tanto, el ISP debería contar con un ASN registrado. Un número de AS o ASN se asigna a cada AS para ser utilizado por el esquema de encaminamiento BGP, este número identifica de manera única a cada red dentro del Internet.  
Los protocolos de ruteo que utilizan internamente se denominan **IGP** (Interior Gateway Protocol), y pueden ser: RIP, IGRP, EIGRP, OSPF, IS-IS...  
Los SA permiten el **ruteo jerárquico**. Cada SA se conecta a un *router de borde* o *gateway*, que lo conecta a otros. Se denominan **EGP** (Exterior Gateway Protocols) a los protocolos entre distintos AS (GGP, EGP, BGP).  
El **ruteo jerárquico** permite salvar los problemas que supondrían utilizar los mismos protocolos entre diferentes subredes:

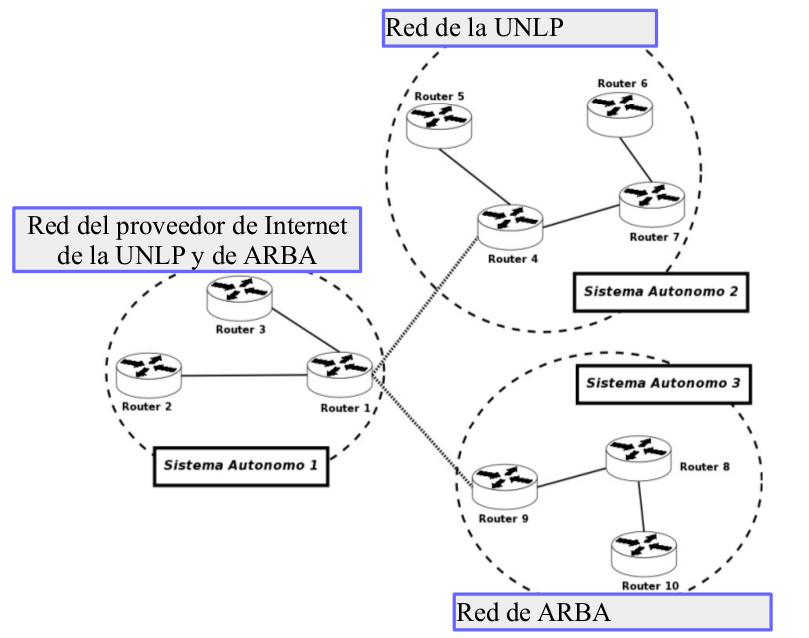
* **Escala:** El enorme **tamaño** que alcanzarían las tablas de ruteo, el **overhead** de intercambiar información entre los routers para una red de grandes dimensiones y el enorme **tiempo de convergencia** que se tendría.
* **Autonomía administrativa**: La imposibilidad de elegir un protocolo específico por parte de los administradores de las redes.

**26. Los algoritmos de ruteo también se pueden clasificar como IGP y EGP.**

**Dado el siguiente cuadro complete:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ¿Implementaciones más  conocidas? | ¿Donde se usan? (dentro de  un sistema autónomo / entre  sistemas autónomos) | ¿Pueden ser sustituidos por  configuración manual (Si,  Depende, No)? ¿Por qué? |
| IGP | RIP, IGRP, EIGRP, OSPF, IS-IS | Dentro de un SA | ? |
| EGP | GGP, EGP, BGP | Entre SAs | ? |

**27.A partir del siguiente gráfico indique:**



* **¿Qué tipo de algoritmo se utiliza para compartir información entre los routers 4 y 7?**

IGP

* **¿Qué tipo de algoritmo se utiliza para compartir información entre los routers 1 y 4?**

EGP

* **¿Qué tipo de algoritmos alimentan las tablas de ruteo de los routers 3 y 10?**

IGP y luego EGP

* **¿Qué tipo de algoritmos alimentan las tablas de ruteo de los routers 1 y 4?**

IGP