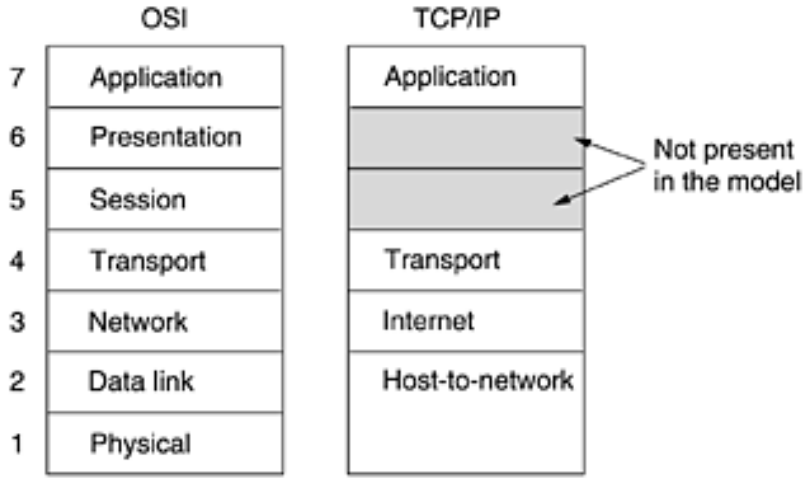
Teoría de las comunicaciones

Práctica 10: Integración

Temas

Arquitectura de capas. Modelo OSI. Modelo TCP/IP.

Definiciones



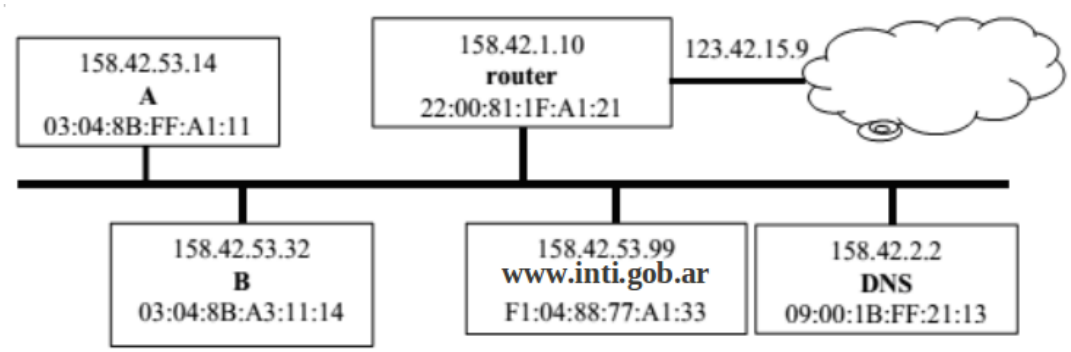
Ejercicio 1

Dada la red de la figura indicar el intercambio de tramas necesario para que desde el ordenador A un navegador (cliente WWW) solicite una página WWW al servidor www.inti.gob.ar (del que NO conoce su dirección IP). *Asumir que todas las caches están vacías.* Para cada trama especificar:

a. Direcciones físicas fuente y destino.

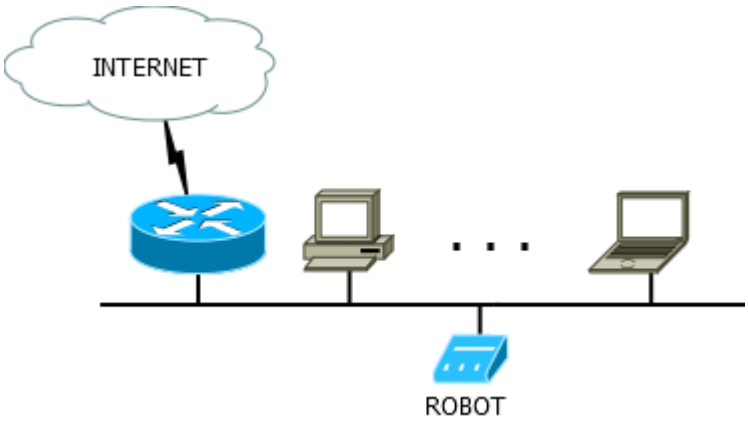
b. Protocolo al que corresponden los datos de la trama.

c. Función del paquete.



Ejercicio 2

Un robot se conecta a un medio compartido "pinchando" un cable coaxil donde hay tráfico Ethernet y comienza a capturar. Dentro el tráfico capturado se obtienen diversos tipos de tramas como ser: BPDU, ARP, ICMP, RIP, OSPF, TCP, UDP, DNS, HTTP y SMTP. El robot cuenta con todo el stack implementado (Ethernet, IP, TCP, HTTP, etc) pero no tiene configurada ninguna información del ambiente en el que está capturando.

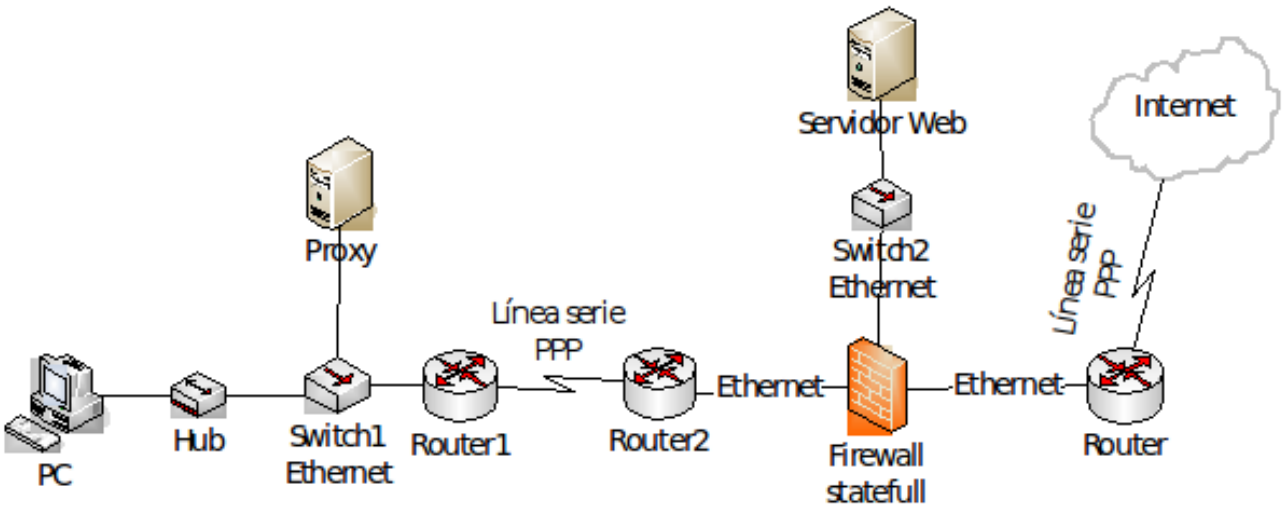


a. Mencione qué piezas de infomarción necesita *autoconfigurarse* para poder enviar un *Echo Request* a `www.google.com`.

b. Explique como podría hacer para obtener esos datos a partir del análisis del tráfico capturado.

Ejercicio 3

Desde la PC con IP privada 172.16.0.15, un usuario accede a la página principal del servidor Web que está en 200.1.17.4.



Considerando sólo desde el instante en que se solicita el acceso al navegador por parte del usuario hasta que le llega al servidor el pedido GET:

a. Describa todos los paquetes de datos que se desencadenan y el orden en el que se van dando.

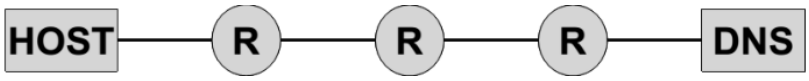
b. Para cada paquete, nombre los niveles de direccionamiento involucrados.

c. Presente los cambios en las tablas y caches que se hayan dado en los dispositivos involucrados.

Asumir: Todas las resoluciónes DNS están en las caches locales. Las caches ARP en los hosts y las tablas de forwarding en los switchs están vacías. Las tablas de forwarding de los routers están configuradas usando ruteo estático. La PC utiliza el Proxy para acceder a los recursos HTTP. El Router2 separa los rangos públicos de los privados usando NAPT.

Ejercicio 4

Dado el escencario de la figura, el **HOST** realiza una consulta DNS al servidor DNS. Las tramas correspondientes a la consulta y la respuesta DNS son de 1000 bits cada una. Las velocidades de transmisión son todas de 100 Mbps



a. Enumere todos las tramas desencadendas.

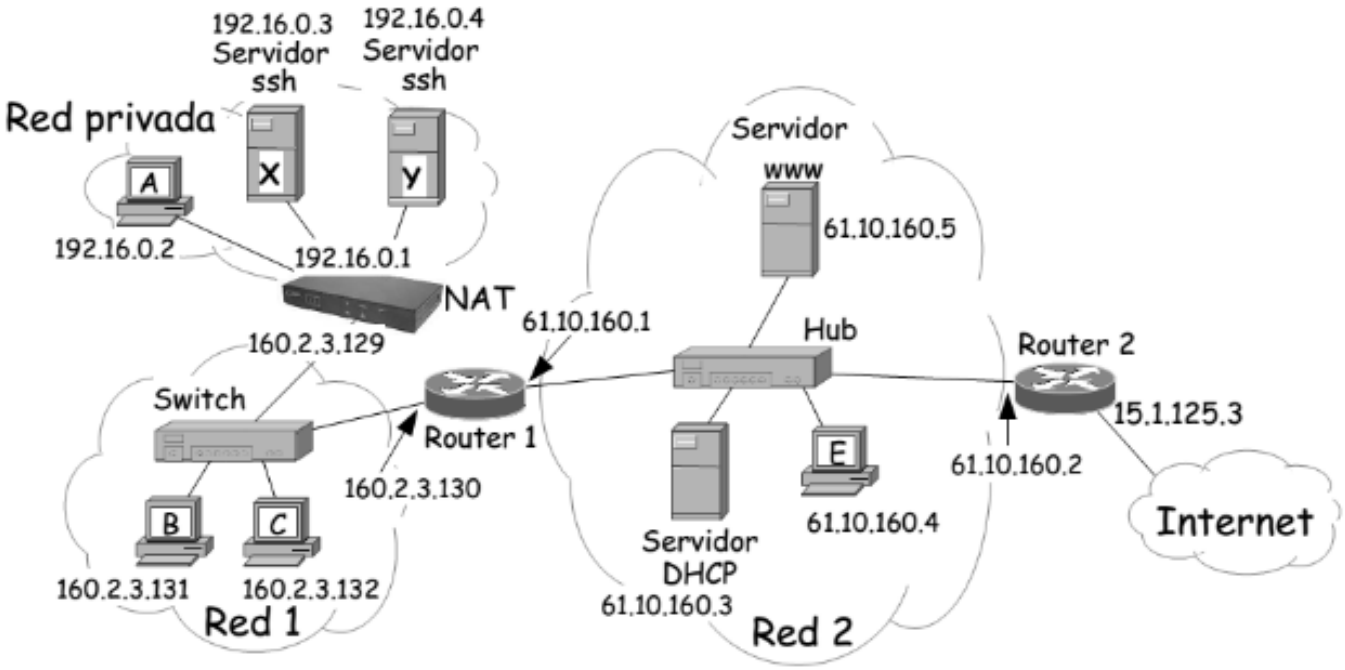
b. Descomponga el tiempo de retardo necesario para recibir la respuesta en todas sus componentes.

c. Calcular el delay. ¿Qué componentes son más significativas?.

Asumir: Las tablas y caches en el **HOST** están vacías y las demás están al día. El tiempo de propagación en cada uno de los enlaces atravesados es de 1 microsegundo. El tiempo de encolamiento (y procesamiento) en los routers y en el servidor de nombres es 1 milisegundo.

Ejercicio 5

Dado el escenario de la figura dónde se definen distintos dispositivos que componen una red, indicar:



a. Protocolos de trasmisión de datos, capa en que operan y tablas que utilizan.

b. Protocolos auxiliares, capa en que operan y tablas que utilizan.

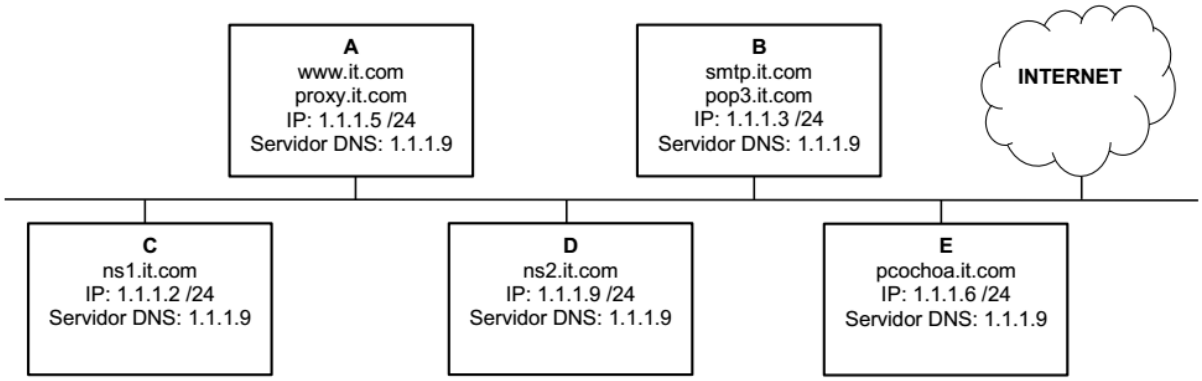
c. Indique que equipos reciben un paquete broadcast IP generado por la PC B.

d. Un usuario en la PC A se encuentra chateando con otro usuario en Internet. La conversación se transmite en texto plano (no encriptada). Indique que equipos podrían *ver* esa conversación si contaran con un sniffer instalado ejecutando en modo promiscuo.

Nota: El equipo que realiza NAT cumple además las funciones de firewall stateful, protegiendo la red privada.

Ejercicio 6

Dado el siguiente esquema de la red de un instituto de tecnología:



Se sabe que: Todos los equipos tienen correctamente configurada la ruta por defecto hacia Internet. A es el servidor web institucional y además actúa como proxy para la red. B es el servidor de correo del instituto, intercambia correo con Internet y almacena las casillas de correo del personal. C es el servidor DNS primario/master del dominio *it.com*. D es el servidor DNS secundario/slave del dominio *it.com*. E es la PC de Pedro Ochoa, empleado del instituto. El cliente local de correo electrónico de E se encuentra configurado de la siguiente manera: **Nombre: Pedro Ochoa; Dirección de mail: pedroochoa@it.com; Servidor de correo entrante: pop3.it.com; Servidor de correo saliente: smtp.it.com**

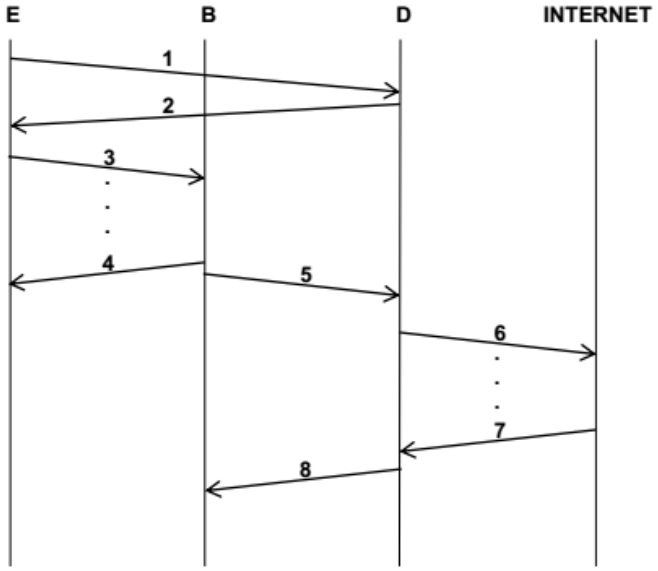
a. Muestre la base de registros DNS que debe configurar el administrador de la red en los servidores DNS.

b. El diagrama de abajo es una secuencia de intercambio de mensajes de aplicación que desencadena un usuario en E en la red anterior. Se sabe que 5 es **request hotmail.com. MX"**. Se pide que describa detalladamente cada mensaje de aplicación indicando todos los protocolos de las capas inferiores utilizados para transportarlo. En caso de DNS, indique si las consultas son iterativas o recursivas y si las respuestas son autoritativas o no. Todas las cachés se encuentran vacías. Tenga en cuenta describir los mensajes intercambiados entre las flechas con puntos suspensivos.

c. Muestre el contenido de todas las cachés y tablas luego de finalizado el intercambio.

d. Enumere todos los tipos de paquetes (protocolos) que puede encontrar con un programa de captura en esta red en particular.

e. Enumere de todos los protocolos que conoce cuáles no encontrará en esta red en particular.



Ejercicio 7

En la red de la figura, todos los equipos tienen correctamente configurada la ruta por defecto hacia Internet. A es el servidor web institucional y además actúa como proxy para la red. B es el servidor de correo del instituto. Intercambia correo con Internet y almacena las casillas de correo del personal. C es el servidor DNS primario/master del dominio *it.com.*. D es el servidor DNS secundario/slave del dominio *it.com.*. E es la PC de Pedro Ochoa, empleado del instituto. Ya se han realizado las tranferencias de zonas entre C y D.

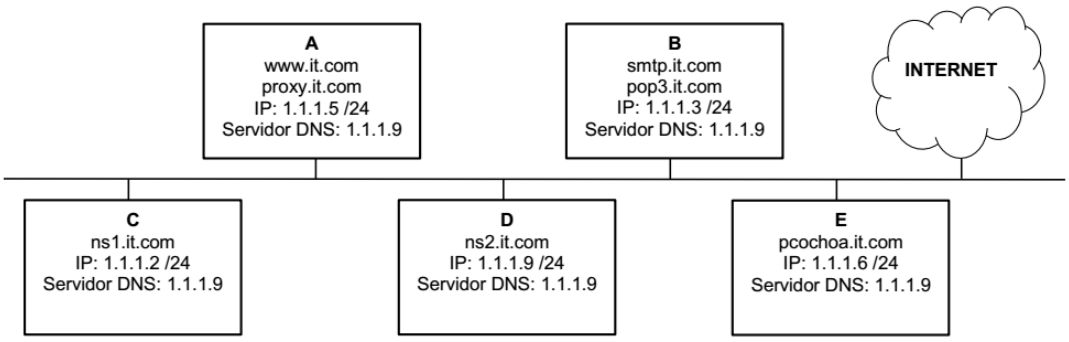
a. ¿Qué respuestas recibiría E si realizara las siguientes consultas? Indique si serían autoritativas o no:
   1. request it.com. A
   2. request it.com. MX
   3. request www.uba.ar. A
   4. request pop3.it.com. CNAME
   5. request www.dc.uba.ar. A
   6. request admin.it.com. NS

b. ¿Qué actividades recientes en la red se pueden inferir de los datos en la caché de D?

c. ¿Falta algún equipo en el esquema? Si es así, indique cuál es, sus datos básicos de configuración y sus funciones.

d. Muestre mediante una figura el encapsulamiento completo (todas las capas) de la respuesta al mensaje 6.

Red del Instituto:



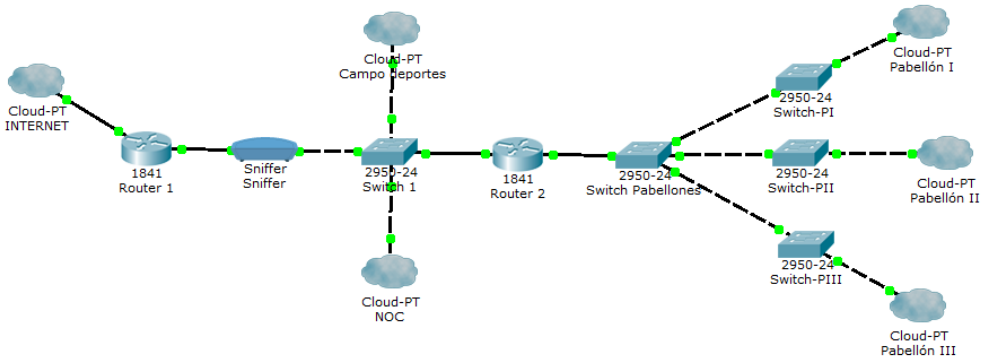
Datos DNS:

```
Configuración de C realizada por el administrador de la red.

it.com.                 IN      SOA   ns1.it.com. hostmaster.it.com.
(
                                      1996011501 ; Serial  201706260439
                                      86400      ; Refresh    24 horas
                                      7200       ; Retry       2 horas
                                      2592000    ; Expire     30 dias
                                      172800 )   ; Minimum     2 dias

it.com.                 IN      NS      ns1.it.com.
it.com.                 IN      NS      ns2.it.com.
ns1                     IN      A       1.1.1.2
ns2                     IN      A       1.1.1.9
it.com.                 IN      MX  10  smtp.it.com.
it.com.                 IN      MX  20  relay2.miprov.es.
www                     IN      A       1.1.1.5
proxy                   IN      CNAME   www.it.com.
smtp                    IN      A       1.1.1.3
pop3                    IN      CNAME   smtp.it.com.
pcochoa                 IN      A       1.1.1.6
admin.it.com.           IN      NS      ad1.admin.it.com.
ad1.admin.it.com.       IN      A       1.1.1.8

Datos en caché de C
(Vacío)

Datos en caché de D
www.uba.ar A 157.92.5.125
medicus.com.ar  MX 10 edge7.medicus.com.ar
medicus.com.ar  MX 1 edge1.medicus.com.ar
edge7.medicus.com.ar A 138.36.54.169
edge1.medicus.com.ar A 138.36.54.164
```

Ejercicios de Parcial

Ejercicio 8

a. Considere la siguiente red TCP/IP/Ethernet con enlaces cableados. Se sabe que un host en la red se encuentra infectado por un programa troyano que esta enviando información sensible mediante el protocolo TCP con destino al sitio www.afi.com.ar:5005 ubicado en Internet. Describa y explique una secuencia de acciones que puede realizar el administrador de la red desde su puesto de trabajo en el NOC (Network Operations Center) para determinar la ubicación física del equipo en cuestión. El administrador solamente tiene acceso a los comandos del equipamiento de red (routers, switches, sniffers, etc.) mediante una aplicacion de login remoto. No tiene ningún tipo de acceso a los hosts. No se le permite realizar ninguna acción física sobre los equipos (apagarlos, reiniciarlos, desconectar cables, etc.) y se trata de minimizar los cortes de servicio en la red durante todo el procedimiento.



Ejercicio 9

Dada la siguiente información que ha sido obtenida de distintos equipos de una red TCP/IP funcionando correctamente, se pide:

Red	Máscara	Próximo salto
192.168.13.0	255.255.255.0	FastEthernet0/1
158.42.52.0	255.255.252.0	FastEthernet0/0
168.254.0.0	255.255.0.0	158.42.55.243
0.0.0.0	0.0.0.0	158.42.55.250

Mac Address	Ports
0004.9aa4.7b48	Fa0/3
0004.9ad7.5882	Fa0/4
000c.cfc7.d401	Fa0/1
00d0.ff9e.db01	Fa0/2

Address	Age (min)	Hardware Addr	Interface
158.42.52.20	3	0004.9aa4.7b48	FastEthernet0/0
158.42.52.253	-	000c.cfc7.d401	FastEthernet0/0
158.42.53.125	4	0004.9ad7.5882	FastEthernet0/0
158.42.55.243	2	00d0.ff9e.db01	FastEthernet0/0
192.168.13.1	-	000c.cfc7.d402	FastEthernet0/1

Age (min): edad, en minutos, de la entrada de la caché. El guión (-) significa que la dirección es local.

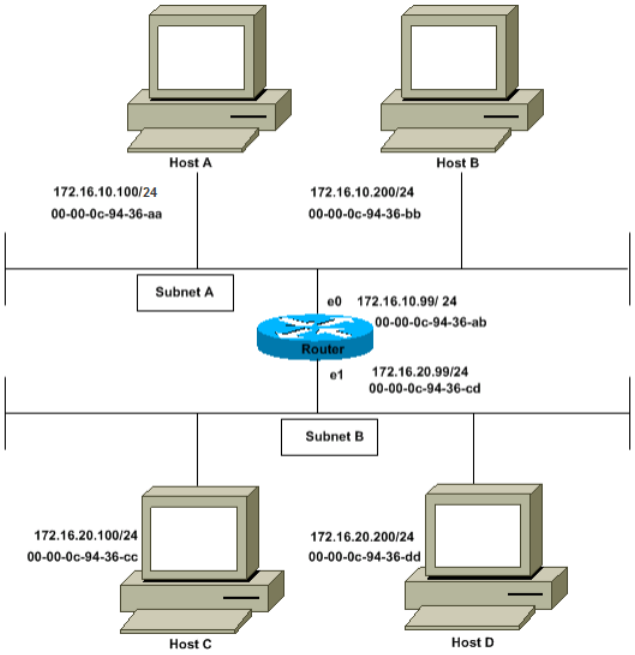
Active Connections

Proto	Local Address	Foreign Address	State
TCP	158.42.53.125:80	158.42.52.20:1025	ESTABLISHED
TCP	158.42.53.125:443	158.42.52.20:1026	CLOSED
TCP	158.42.53.125:25	158.42.52.20:1030	ESTABLISHED
TCP	158.42.53.125:110	158.42.52.20:1031	CLOSED

Realizar un esquema gráfico que muestre cómo están conectadas las redes, routers, switches y hosts que se deducen de las tablas, así como sus direcciones IP, máscaras, mac-address y servicios. Para las direcciones de las redes utilizar formato CIDR. NOTA: Hay que asignar sólo los datos que pueden conocerse a partir de las tablas, no es necesario añadir información extra.

Ejercicio 10

Dada la siguiente red TCP/IP funcionando correctamente y con tráfico constante entre todos los hosts excepto el A que se encuentra apagado desde hace una semana, se pide:



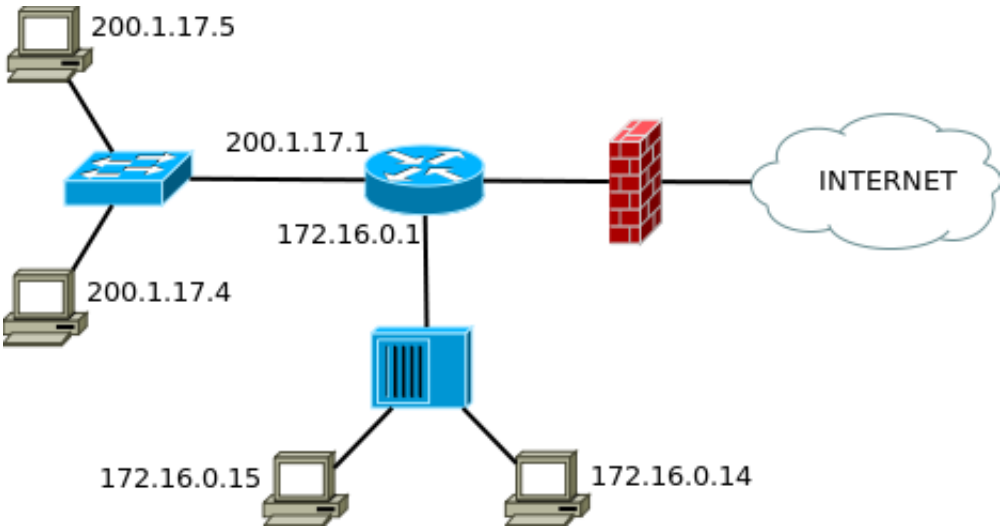
a. Mostrar el contenido completo de las tablas ARP y de forwarding (ruteo) IP del Router y del Host D.

b. Dado que la subred A se encuentra implementada mediante un switch Ethernet, mostrar la representación gráfica del switch, las conexiones de sus puertos y el contenido de su tabla de forwarding. Explicar brevemente cómo construye esa tabla.

c. Sea un mensaje de consulta DNS de 40 bytes enviado desde el host C hacia el host B. Mostrar gráficamente como se transporta el mensaje encapsulado en los distintos protocolos, o sea, mostrar el contenido más relevante de las cabeceras de todos los protocolos en el instante en que el mensaje circula por la subred B. Se deben mostrar, como mínimo, las direcciones origen y destino de cada protocolo.

Ejercicio 11

En la red de la figura, hay un router que separa dos redes. Una de las redes esta conectada mediante un hub y la otra mediante un switch. Además, el router separa los rangos públicos de los privados usando NATP. Por último un firewall separa ambas redes de Internet.



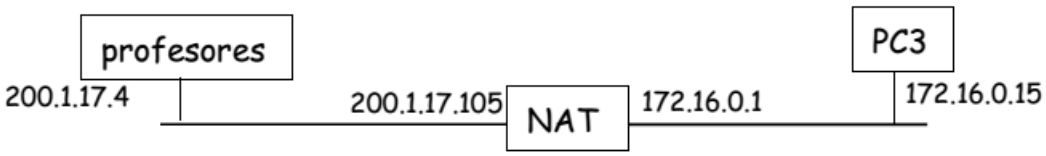
a. Para cada nodo en la red, mencione hasta qué capa del modelo OSI debe saber interpretar para realizar su función.

b. En un momento dado, la pc con IP 172.16.0.15 inicia una conexión TCP al puerto 80 de la pc con IP 200.1.17.4. Mencione todas las tramas deseancadenadas y qué dispositivos podrían "verlas", hasta que se establece la conexión.

Asumir que todas las tablas dinámicas y las caches están vacías

Ejercicio 12

En la red de la figura, desde la PC3, se accede a un sitio web que está en 200.1.17.4.



a. Diagrame la secuencia de intercambio de paquetes que ocurren cuando PC3 accede al sitio web mencionado hasta que le llega la primera trama al servidor. Especifque direccionamiento y tipo de mensaje al nivel de capa enlace, capa de red y eventualmente transporte.

b. Mencione los cambios en las tablas dinámicas presentes en los dispositivos, luego del intercambio del item anterior.

c. Indique -si es posible determinarlo- que tipo de equipo (hub, switch, router) es el equipo que está realizando NAT.

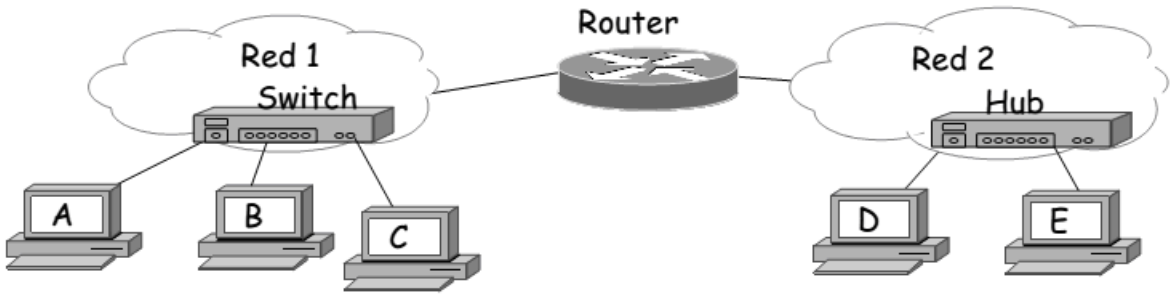
Nota: Asuma que la resolución DNS está en el caché de su máquina y todas las tablas ARP se encuentran vacías.

Ejercicio 13

En la red de la figura todos los adaptadores de red utilizados son Ethernet. Se supone que las computadoras y el router están correctamente configurados y que tras un periodo de funcionamiento, el switch conoce la ubicación de todas las máquinas. Las caches ARP están vacías en todos los sistemas. Sea la siguiente asignación de direcciones IP:

A:192.168.44.135/26; Router:192.168.44.150/26

D:192.168.48.171/26; E:192.168.48.175/26; Router:192.168.48.178/26



a. Enumere en orden cronológico las cosas que ocurren al nivel de capa enlace, capa de red y eventualmente transporte, cuando desde su computadora A una aplicación realiza una consulta DNS corta a su resolver configurado, en este caso D. Considere sólo desde el instante en que D responde la consulta y hasta que llega la respuesta a la computadora A. Muestre las direcciones de origen y destino de las unidades de datos de cada protocolo. Explique todo detalladamente.

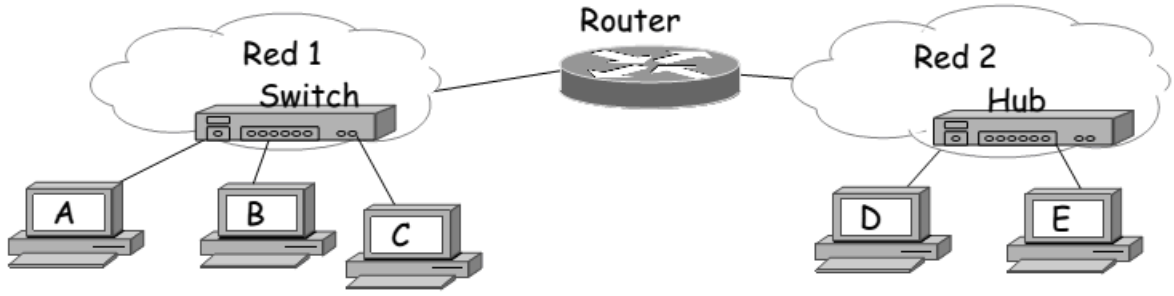
b. ¿Podría un usuario en C ver con un sniffer la consulta DNS que realizó la computadora? ¿Y un usuario en E? Explique detalladamente. Mediante un gráfico muestre los encabezados de los protocolos que encapsulan al mensaje que contiene la consulta.

Ejercicio 14

En la red de la figura todos los adaptadores de red utilizados son Ethernet. Se supone que las computadoras y el router están correctamente configurados y que tras un periodo de funcionamiento, el switch conoce la ubicación de todas las máquinas. Las caches ARP están vacías en todos los sistemas y la resolución DNS está en el caché de su computadora.

a. Enumere en orden cronológico las cosas que ocurren al nivel de capa enlace, capa de red y eventualmente transporte, cuando desde su computadora A (172.16.0.15 /16) accede a la página web que está en el servidor E (200.1.17.4 /24). Considere sólo desde el instante en que usted presiona retorno en el navegador y hasta que le llega la primera trama al servidor.

b. ¿Puede A transmitir un datagrama a B mientras C transmite otro a D? ¿Por qué?

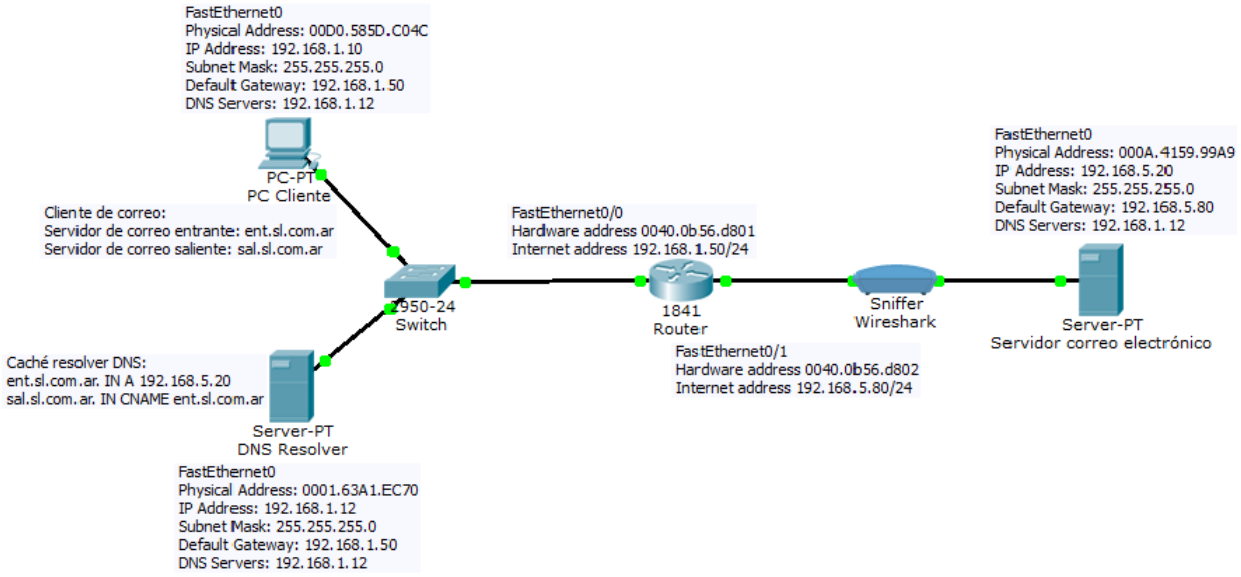


Ejercicio 15

Un usuario en la *PC Cliente* utilizando software de correo instalado localmente (i.e. no Webmail) escribe un mensaje dirigido a otro usuario cuya casilla de correo reside en el *Servidor correo electrónico*.
NOTA: Todos los cachés se encuentran vacíos, excepto el indicado en la figura para el resolver DNS.
Se pide que desarrolle una respuesta para los siguientes puntos:

a. Suponga que todos los enlaces físicos tienen un RTT fijo de 3 segundos para todos los paquetes. Estime el tiempo total que transcurre desde el momento en que el usuario oprime el botón *enviar* hasta que el primer mensaje del protocolo de transporte llega al servidor. Considere despreciable el tiempo transmisión de los paquetes, y el de encolamiento y procesamiento de los mismos en los distintos equipos.

b. Para cada uno de los equipos, describa el formato y contenido de sus tablas DNS, ARP y de forwarding en el instante en que el primer mensaje del protocolo de transporte llega al servidor.

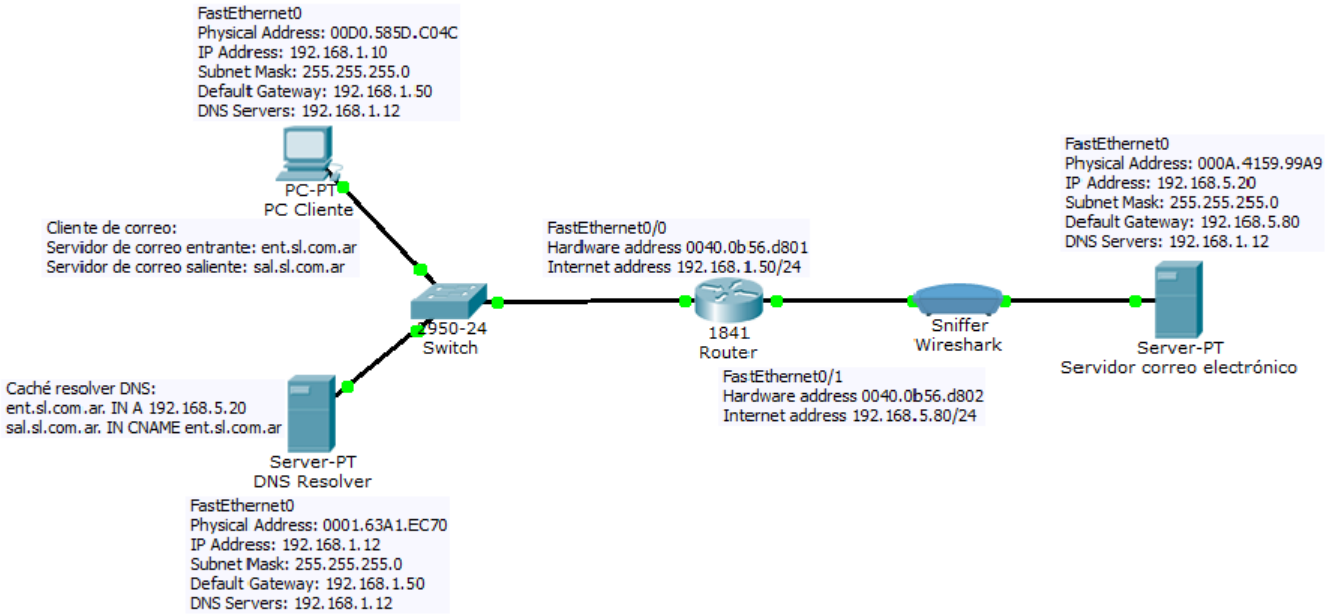


Ejercicio 16

La *PC Cliente* envía un email a otro usuario cuya casilla reside en el *Servidor correo electrónico*. Considerar desde el momento en que el usuario oprime el botón *enviar* en la aplicación de email hasta que el primer mensaje del protocolo de aplicación llega al servidor.
NOTA: Todos los cachés se encuentran vacíos, excepto el indicado en la figura para el resolver DNS.
Se pide:

a. Describir con un gráfico, para cada equipo, la pila de **todos** los protocolos involucrados en esta transferencia.

b. Mostrar la traza de paquetes de todos los protocolos que pasan por el "Wireshark". Indicar protocolo, capa, direcciones de origen y destino, y toda otra información que considere relevante.



Bibliografía

Computer Networks: A Systems Approach Fifth Edition. Larry L. Peterson and Bruce S. Davie. 2012 Elsevier, Inc.

Redes de Computadoras. Quinta edición. Andrew S. Tanenbaum & David J. Wetherall. PEARSON EDUCACIÓN, México, 2012.

The TCP/IP Guide: http://www.tcpipguide.com/free/t_toc.htm