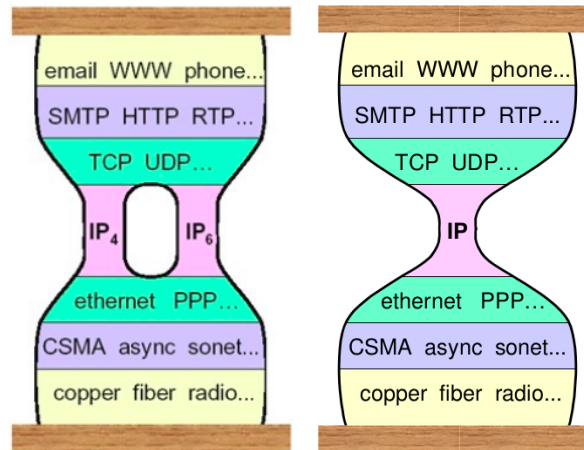


Práctica 2 - Capa de Red: IPv4 e IPv6

revisión: 2.3

1. ¿Cuál es la función de la capa de red en el modelo OSI? ¿Qué implementaciones conoce? ¿Qué es IPv6? ¿Por qué es necesaria su implementación?

¿Qué entiende por ambas gráficas (fuente: presentaciones IETF)?



2. Tomando un diagrama o una captura de un datagrama IPv4 e IPv6 indique la funcionalidad u objetivo de cada campo.
 - Si un paquete llega a un router con un TTL = 1, ¿qué hace el router? ¿Cómo se llama el campo TTL en IPv6?
 - ¿En qué se diferencia el checksum de IPv4 e IPv6? Y en cuanto a los campos checksum de TCP y UDP, ¿sufren alguna modificación? Si un paquete tiene un error de checksum cuando llega a un router ¿qué sucede en IPv4 y en IPv6?
 - ¿Por qué no es necesario el campo Header Length en IPv6?
 - Si quisiese que IPv4 soporte una nueva funcionalidad, ¿cómo lo haría? ¿y en IPv6?
3. ¿Qué es una red clase A? ¿Qué es una red clase B? ¿Qué es una red clase C? ¿Cuántas hay de cada una? ¿Cuántos hosts pueden haber en cada una? ¿Existen clases en IPv6? ¿Qué significa que el actual direccionamiento sea *classless*?
4. ¿Cuál es la función de la máscara de red? ¿Qué otra notación alternativa se puede utilizar? ¿Cuál se utiliza en IPv6 y por qué?
5. Dada la red IP 65.0.0.0/8. Se necesitan definir 934 subredes. Indique qué máscara debería ser utilizada. Indique cuál sería la subred número 817 indicando el rango de direcciones asignables, dirección de red y broadcast.
6. Dada la red IP 195.200.45.0/24. Se necesitan definir 9 subredes. Indique la máscara utilizada y las nueve subredes. Luego tome una de ellas e indique el rango de direcciones asignables en esa subred, dirección de red y broadcast

7. Indicar las clases de las siguientes direcciones, ¿Cuáles son direcciones privadas?

- 172.16.7.12
- 200.5.123.221
- 224.0.0.9
- 10.10.1.10
- 172.15.7.98
- 192.168.10.5
- 240.32.34.2
- 1.1.1.1
- 8.8.8.8
- 239.12.34.3

8. Para cada una de las siguientes direcciones obtener (si corresponde):

Dirección y Clase (A,B,C) de Red.

Pública/Privada/Reservada/Inválida.

Dirección de Subred y Dirección de Broadcast.

Cantidad posibles de redes si toda la red se hubiese “subnetado” con la misma máscara.

Cantidad de IP para hosts por subred utilizables.

- 163.10.5.66/26
- 127.0.0.1/8
- 20.6.20.1/18
- 200.5.10.3/30
- 172.18.10.0/26

9. ¿Cuáles de las siguientes no son direcciones IPv6 válidas, cuáles asignables a un host?

- 2001:0:1019:afde::1
- 2001::1871::4
- 3ffg:8712:0:1:0000:aede:aaaa:1211
- 3::1
- 3ffe:1080:1212:56ed:75da:43ff:fe90:affe
- ::
- 2001::
- 3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001

10. ¿Cómo se podrían sumarizar las siguientes direcciones aplicando CIDR?

200.10.0.0/24

200.10.1.0/24

200.10.2.0/24

200.10.3.0/24

11. ¿Cómo quedará la sumarización si necesita agrupar las 8 primeras redes (hasta las 200.10.7.0/24)

12. Y las siguientes:

195.80.0.0/24

195.80.1.0/24

195.80.2.0/24

13. Dada la red IP 195.200.45.0/25. Se necesitan definir 6 subredes de 6 host c/u. Indique la máscara utilizada y la subred número 4.
14. Dado el siguiente gráfico, y según los datos brindados, para cada segmento de red, responda:

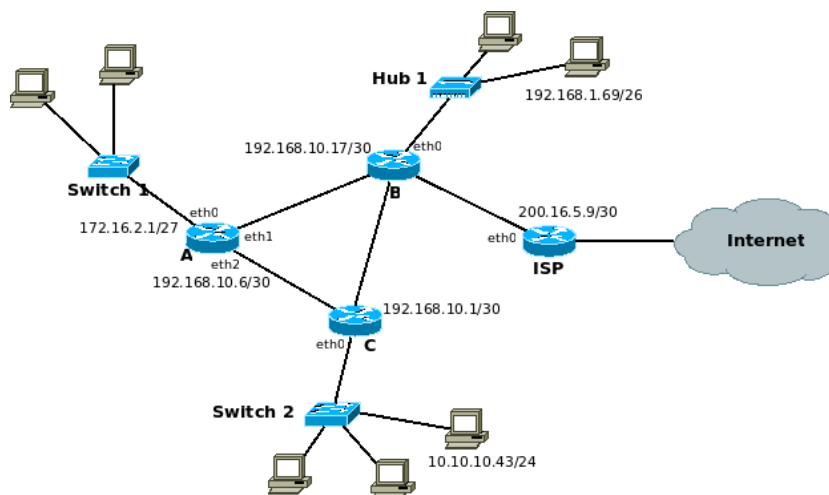


Figura 1

- Dirección y Clase (A,B o C) de Red
 - Dirección y Máscara de Subred. Dirección de Broadcast
 - Cantidad de direcciones utilizables en cada subred
 - ¿Cuántos dominios de colisión y de broadcast encuentra en el gráfico?
 - Asigne una dirección adecuada a cada interfaz de red de los routers
 - Defina la tabla de ruteo para cada router de manera que todos los dispositivos en la red puedan comunicarse y, además, salir a Internet
15. ¿Qué significa y cuál es el uso de la dirección 127.0.0.1?
 16. Describa qué es y para qué sirve ICMP. ¿Qué hacen los comandos **ping(8)** y **traceroute(1)**? (**tracert** en Windows).
 - Indique el tipo y el código ICMP de un ping.
 - Indique el tipo y el código ICMP de la respuesta de un ping.
 - Indique el tipo y el código ICMP del cual se vale el comando traceroute para funcionar.
 - Estos comandos, ¿funcionan igual en Linux y en Windows? ¿En qué se diferencian si es que lo hacen? Hint: usar un “capturador” de tráfico como wireshark/tshark o tcpdump.
 17. Indique qué funcionalidad difiere entre ICMP (sobre IPv4) e ICMPv6.
 18. Utilizando la herramienta CORE indicada por la cátedra, configurar el ruteo estático en la red que se muestra en el gráfico a continuación (fig. 2):

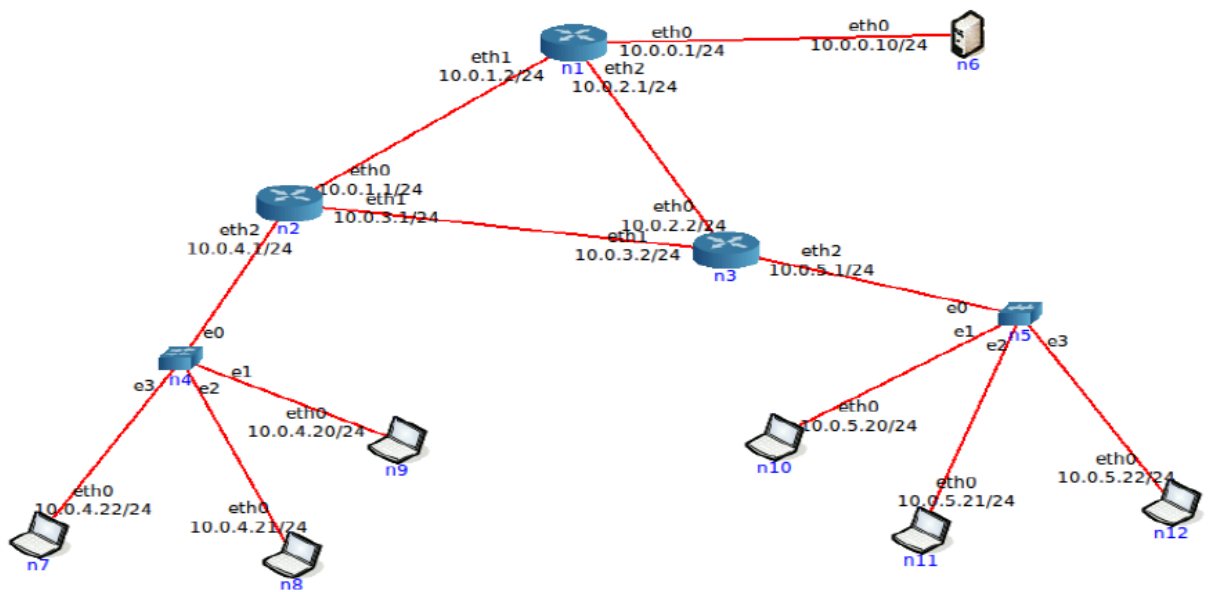


Figura 2

- Inicie la herramienta CORE y abra el archivo `1-ruteoestatico.imn`
- Inicie la virtualización de la topología.
- Configure cada uno de los equipos considerando:
 - Para entrar a configurar cada equipo (PC o router) debe hacer doble click sobre el mismo, lo cual abre una terminal de comandos.
 - Utilice el comando `ifconfig` para configurar las direcciones IP de equipo según las interfaces indicadas en el gráfico. Por ejemplo, en la PC n6 debe configurar la interfaz `eth0` con la IP `10.0.0.10`, en Router n1 debe configurar la `eth0` con la IP `10.0.0.1`, la `eth1` con la IP `10.0.1.2` y la `eth2` con la `10.0.2.1`
 - Cada vez que configure los extremos de un enlace, por ejemplo la interfaz `eth0` de la PC n6 y la interfaz `eth0` del Router n1, compruebe conectividad utilizando el comando `ping`.
 - Utilice el comando `route/ip route` para configurar las rutas estáticas necesarias en cada equipo. En el caso de los routers debe considerar:
 - Router n1 envía todo el tráfico desconocido a Router n2.
 - Router n2 envía todo el tráfico desconocido a Router n3.
 - Router n3 envía todo el tráfico desconocido a Router n1.
 - Función de ruteo: Un router o una PC puede configurarse para rutear paquetes entre sus placas de red.
 - Verificar `IP_FORWARD` en los routers y las PCs. Para obtener el valor, ejecutar:


```
cat /proc/sys/net/ipv4/ip_forward o sysctl net.ipv4.ip_forward
```

 El valor en 0 deshabilita su funcionalidad, 1 lo habilita.
 Para cambiar el valor, ejecutar:


```
sysctl net.ipv4.ip_forward=1
```
 - Verificar `RP_FILTER`. Este parámetro es de seguridad y evita la recepción de paquetes por una interfaz que tengan una IP de origen que pertenezca a una red que el router no "rutearía" a través de la misma. Este valor podría necesitar deshabilitarse en los routers para realizar la práctica. Para obtener el valor:

`sysctl net.ipv4.conf.all.rp_filter` El valor en 0 deshabilita su funcionalidad. Un 1 lo habilita.
Para cambiar el valor:
`sysctl net.ipv4.conf.all.rp_filter=1`

- Verifique conectividad entre las PCs:
 - I. Utilizando el comando **ping**
 - II. Utilizando el comando **tracert**
 - III. Utilizando el comando **ping -nR**
 - IV. Otros comandos: **tracert -l**, **mtr** (investigue las diferencias)
 - V. Mientras realiza ping desde una PC, capture paquetes en un router intermedio y verifique qué paquetes pasan por la interfaz. Por ejemplo, mientras una PC corre el comando ping a otra PC, analice los paquetes que se visualizan en eth0 y en eth1 de algún router por el que parte o todo el tráfico pasa. La captura de paquetes puede hacerse con el comando `tcpdump -i <interfaz>` o con *wireshark* por ejemplo: `tcpdump -i eth0`
- Relevamiento: Utilizando el comando `route -n`, `netstat -nr` o `ip route show` indique la configuración de las tablas de rutas tanto de los routers como la de las PCs especificando para cada dispositivo:

Red Destino	Gateway	Máscara de Red	Interface
-------------	---------	----------------	-----------

- I. Si la estación PC n7 le envía un ping a la estación PC n6:
 1. ¿Cuál es el camino por el que viaja el requerimiento?
 2. ¿Cuál es el camino por el que viaja la respuesta?
 - II. Evalúe lo mismo para comunicaciones entre otras PCs.
- Mantenimiento de la red: Suponiendo que en el Router n1 se agregó una interfaz de red con la dirección IP 163.10.10.1/24:
 - I. Identifique los cambios que deberían ser necesarios al ruteo estático para que todas las PCs puedan comunicarse con hosts en la nueva red.
 - II. En base a lo anterior, ¿qué puede decir respecto del mantenimiento del ruteo en una red que tiene más de 20 routers?
 - ICMP y RUTEO 1: Desde la PC n6, realice un ping a la dirección IP 5.5.5.5
 - I. ¿Qué indica el mensaje de error recibido?, ¿Quién lo envía?
 - ICMP y RUTEO 2: Desde la PC n6, realice un ping a la dirección IP 10.0.5.23
 - I. ¿Qué indica el mensaje de error recibido?, ¿Quién lo envió?
 - ICMP y RUTEO 3: Provoque un loop de enrutamiento entre los routers con una nueva red, por ejemplo la red 200.100.11.0/24 y luego desde la PC n6, realice un ping a la dirección 200.100.11.5
 - I. ¿Qué indica el mensaje de error recibido?, ¿Quién lo envía?
19. ¿Para qué sirve el protocolo ARP? ¿En qué protocolos de enlace no sería necesario? ¿Es necesario en IPv6? ¿Qué se utiliza en IPv6?
20. ¿A qué dirección L2 se envían los mensajes ARP Request? ¿Y los ARP Reply?
21. Los mensajes ARP, ¿son re-enviados por los routers? Justifique.

22. Utilizando el CORE, arme la siguiente topología (fig. 3):

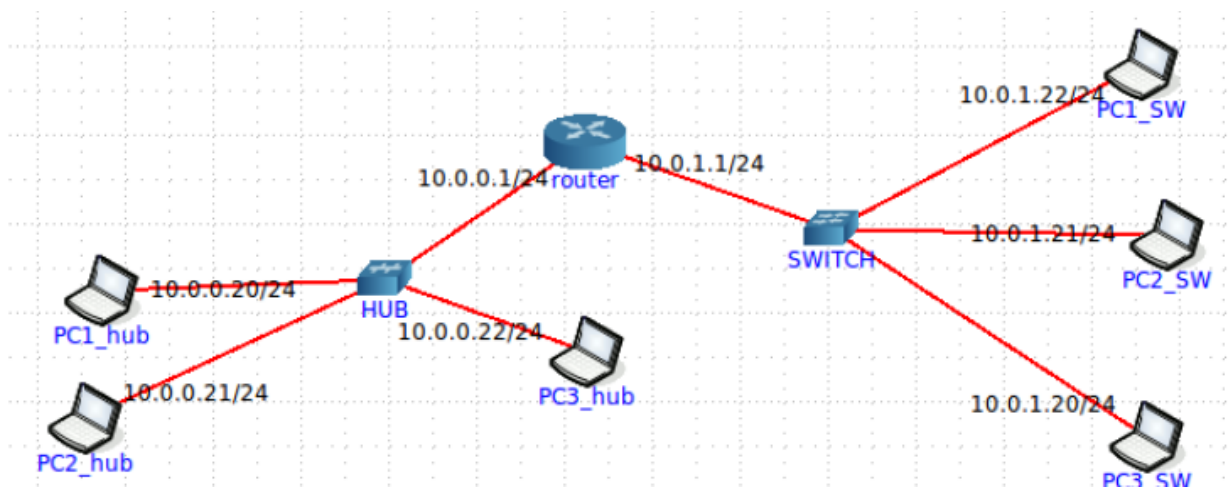


Figura 3

- Si una PC se desea conectar a otra PC en una red distinta, ¿es necesario ejecutar ARP? ¿A quién le envió el ARP Request?
- Suponga que PC1_hub, que tiene la tabla ARP vacía, le quiere enviar un ping a PC2_hub. ¿Cuál es la secuencia de mensajes? Indique los mensajes ARP Request y Reply completando los campos de la trama Ethernet y de los mensaje ARP.

Paquete ARP

MAC Destino	MAC Origen	MAC Origen:.....	IP Origen:.....
		MAC Destino:.....	IP Destino:.....

Frame Ethernet

- ¿Cómo quedarían los mensajes ARP si el ping ahora es desde PC1_hub hacia PC2_SW? (Suponer que las tablas ARP están vacías)
- Para analizar los paquetes del protocolo ARP realice las siguientes tareas:
 - I. Ejecute el comando `ifconfig -a` o `ip addr show` en la PC1_hub.
 - II. Luego ejecute el comando `arp -n` o `ip -4 neigh show` en la PC1_hub para ver su tabla ARP.
 - III. Monitoree el tráfico ARP desde la PC3_hub ejecutando `tcpdump -i eth0 -p arp / tshark -i eth0 arp`
 - IV. Envíe un ping desde la PC1_hub a PC2_hub y vuelva a observar la tabla ARP de PC1_hub.
 - V. Vea los resultados en la consola de PC3 a fin de observar las características de los paquetes ARP (MAC Origen, MAC Destino, etc).
 - VI. Monitoree el tráfico ARP desde la PC3_SW ejecutando `tcpdump -i eth0 -p arp / tshark -i eth0 arp`
 - VII. Haga un ping a la PC2_SW y vuelva a observar la tabla ARP de la PC1_SW.
 - VIII. Vea los resultados en la consola de PC3_HUB a fin de observar cuáles son las diferencias respecto a lo observado en el punto (V) en cuanto a cuáles son los paquetes que se ven en este caso.

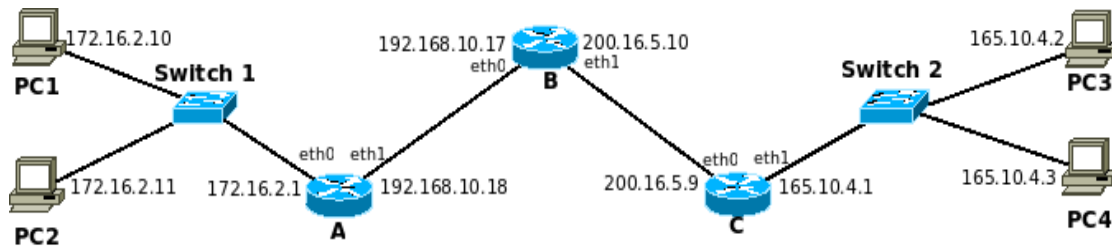


Figura 4

- Observando el gráfico anterior (fig. 4) , conteste las siguientes preguntas:
 - I. Si PC1 envía un ARP Request para saber la dirección MAC de PC2, ¿qué dispositivos los recibirán? ¿Y a la respuesta de PC2?
 - II. Agregue una entrada estática como superusuario en la tabla ARP de PC1 para que pueda llegar a su router sin utilizar el protocolo. Usar el comando `arp -s <IP> <MAC> / ip neigh add <IP> lladdr <MAC> dev <DEV>`
 - III. Si PC3 le envía un ping a PC4, ¿cuál es toda la secuencia de mensajes suponiendo que las tablas ARP están vacías? ¿Cómo estarían compuestos estos mensajes?
 - IV. Si PC1 le envía un ping a PC4, ¿cuál sería toda la secuencia de mensajes suponiendo que las tablas ARP contienen los datos de la consulta anterior? ¿Cómo estarían compuestos estos mensajes? ¿Cambian las direcciones IP en los paquetes IP? ¿Y las direcciones MACs en las tramas Ethernet?

NOTA: para indicar la MAC de los dispositivos utilice Equipo:Interfaz (por ej.: PC1:eth0)

23. ¿Qué funcionalidad cumplen las direcciones de tipo link-local en IPv6? ¿Qué analogía se puede hacer con IPv4?
24. Transforme las siguientes direcciones MACs en Identificadores de Interfaces de 64 bits de alcance link-local.
 - 00:1b:77:b1:49:a1
 - e8:1c:23:a3:21:f4
25. ¿Cuál sería una abreviatura correcta de 3f80:0000:0000:0a00:0000:0000:0000:0845?
 - 3f80::a00::845
 - 3f80::a:845
 - 3f80::a00:0:0:0:845:4567
 - 3f80:0:0:a00::845
 - 3f8:0:0:a00::845
26. Indique si las siguientes direcciones son de link-local, global-address, multicast, etc.
 - fe80::1/64
 - 3ffe:4543:2:100:4398::1/64
 - ::
 - ::1
 - ff02::2
 - 2818:edbc:43e1::8721:122
 - ff02::9

27. Dado el siguiente diagrama (fig. 5), ¿qué direcciones IPv6 será capaz de auto-configurar el nodo A en cada una de sus interfaces? ¿Cuáles son recomendadas y cuáles sus alcances?

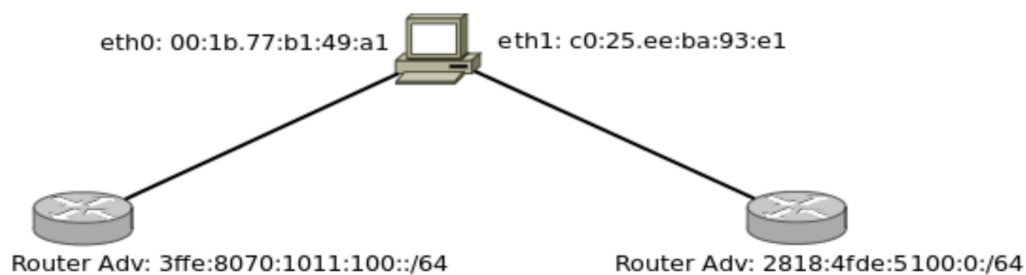


Figura 5

NOTA: Ejercicios más específicos sobre IPv6 se verán en las siguientes prácticas.