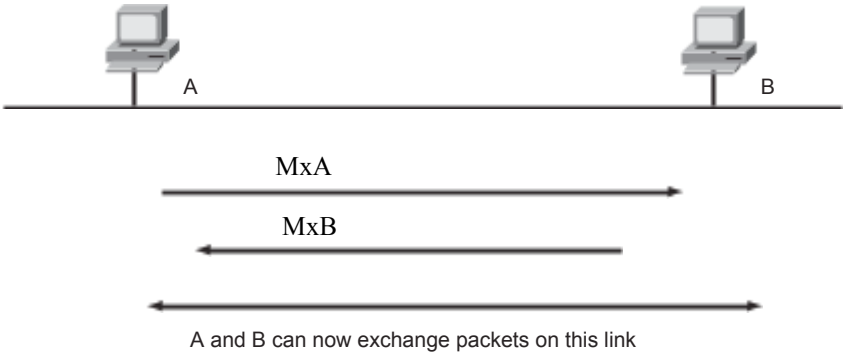
Examen Final – Parte Práctica **COMUNICACIONES** Fecha: 21/12/2020

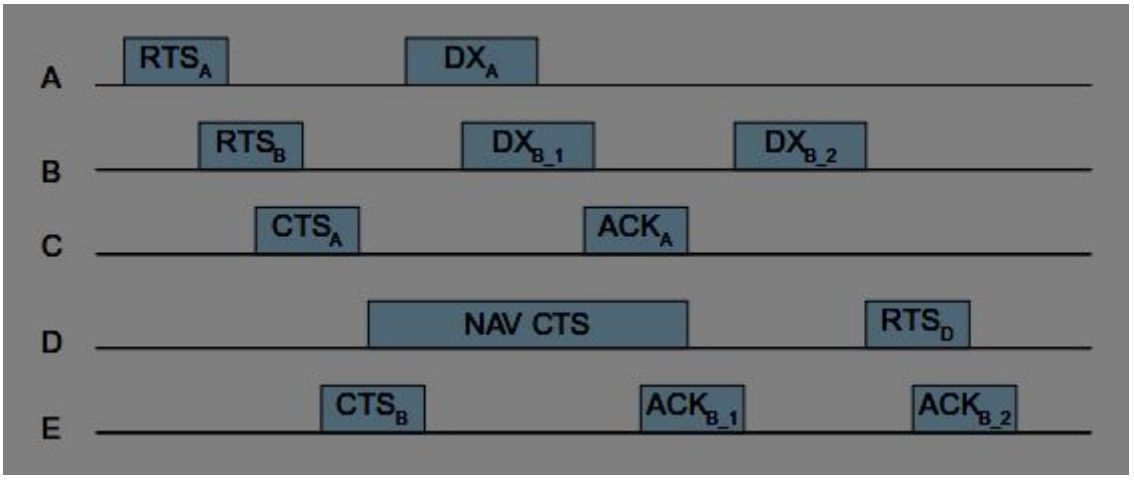
Nombre y Apellido:
Legajo: *Correo electrónico:*

1- Recuerde lo realizado en el TP y considere el siguiente gráfico que describe el "Descubrimiento de Vecinos". Explique los siguientes aspectos del mecanismo:



a) Cuál es la finalidad del Descubrimiento de Vecinos.
b) Describa cómo es el intercambio de mensajes entre A y B. Es decir, describa el contenido de MxA y MxB.
c) Indique las direcciones IPv6 que deberían estar en los mensajes. ¿A qué nivel se realiza este mecanismo?; es decir, ¿qué alcance tiene? (enlace, red, subred, etc.?)

2- Suponga que se presenta el siguiente escenario donde todas las estaciones están activas en la red:



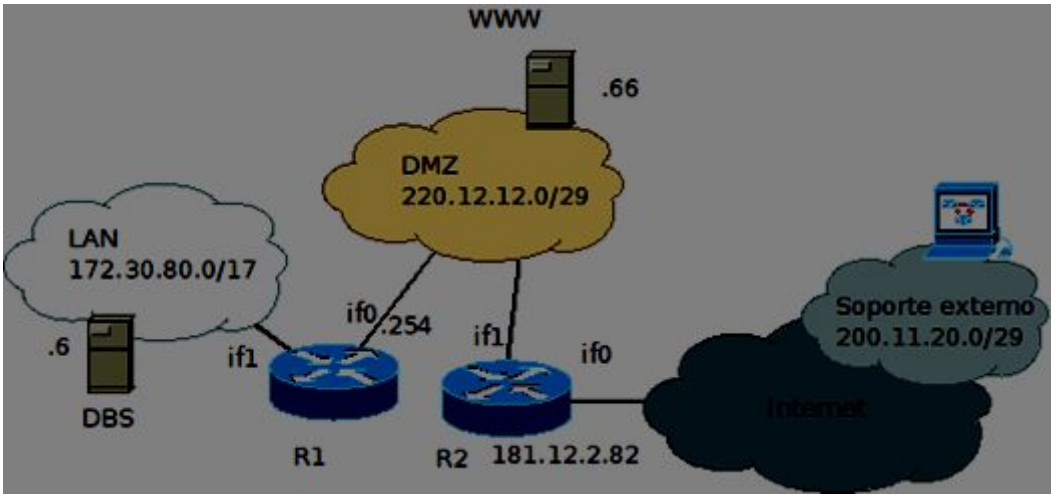
i. Explicar el comportamiento de cada estación en la red.

ii. ¿Existe una estación oculta? En caso afirmativo ¿Cuál es?

3- Realizar el archivo de resolución directa **db.flaxo.org** de la zona **flaxo.org** teniendo en cuenta las siguientes características:

I. El dominio **flaxo.org** tiene un servidor de nombre maestro dns.flaxo.org (7:3:4:153) y dos servidores de nombres ns_backup.flaxo.org (7:3:4:56) y otro dns.ezeq.edu.ar (externo: 2620:171:800:714::1).
II. El dominio **flaxo.org** tiene dos servidores de correos: info.flaxo.org (7:3:4:152) y comercial.flaxo.org (7:3:4:151).
III. El subdomnio **quant.flaxo.org** será delegado y su servidor de nombre maestro mi_dns.quant.flaxo.org estará en 7:3:4:53 y su esclavo será externo dns.ezeq.edu.ar.
IV. Se requiere que el tiempo de refresco sea de 2h, de actualización por reintento de 15m, y de expiración de 3W2h**.**
V. Los hosts desktop y mobile estan tienen las direcciones de Ipv4 7:3:4:103 y 7:3:4:104 respectivamente.

4- Ejercicio de Firewall (20201221)



En la red de la figura, la LAN tiene IP privadas y la DMZ Públicas.

1)Los puestos de la LAN solo pueden acceder a los puertos web (80 y 443 TCP) del servidor de la DMZ, y a toda Internet, pero tener en cuenta que se natean en R1. NO natear el tráfico hacia la DMZ.

2)El servidor de la DMZ puede recibir accesos a los puertos web desde cualquier lado y SSH (tcp/22) solamente desde la red de servicio soporte.

3)Los servidores de la DMZ sólo pueden consultar DNS al exterior (puertos 53 tcp y udp), y al puerto 3306 del servidor de base de datos.

Escriba reglas para las tablas Filter y Nat del router R1 de forma de cumplir esos requerimientos. No es necesario escribir las cadenas INPUT de los routers.

//SOLUCIONES

// Ejercicio 1

a)

La finalidad del descubrimiento de vecinos es encontrar las direcciones físicas de los nodos en un misma red (a nivel capa de enlace)*. Es el análogo a ARP de IPv4.

* Vale aclarar que no es la única funcionalidad que tiene (descubrimiento de routers, determinar datos de configuración de la red, redireccionar paquetes).

b) A través de las direcciones de tipo multicast es que se pueden enviar mensajes a todos los nodos de una red en IPv6 (caso particular del análogo a broadcast de IPv4). En particular para el intercambio de par de nodos de A y B puede pasar lo siguiente semánticamente

MxA: cuál es tu dirección física a nivel capa de enlace?.

MxB: mi dirección física es XX:XX:XX:XX:XX:XX (dirección MAC)

En el sentido más técnico, los mensajes son de tipo ICMPv6 y contienen dirección destino y fuente. El agregar dirección fuente permite que el envío de una respuesta no involucre otra búsqueda y que todos los nodos intermedios puedan actualizar sus buffers.

c) Las direcciones que se usan en el descubrimiento de vecinos son direcciones link-local. Estas direcciones no se routean y por lo general se generan automáticamente.

// Ejercicio 2

i)

Estación A: A envía un Request to Send a C. Luego de recibir el Clear to Send de C procede a enviar los datos. Finalmente recibe el ACK de C.

Estación B: B envía una Request to Send a E. Luego procede a enviar los datos como una ráfaga (fragmentados con un protocolo de parada y espera para el envío de cada fragmento): cada fragmento se confirma individualmente y se espera a la n-ésima confirmación para enviar el n+1-ésimo fragmento.

Estación C: es la contraparte de la comunicación con A. Ver estación A

Estación D: D se pone en NAV al escuchar el CTS de C por lo que se puede deducir que D está al alcance de C. El NAV termina cuando C envía un ACK.

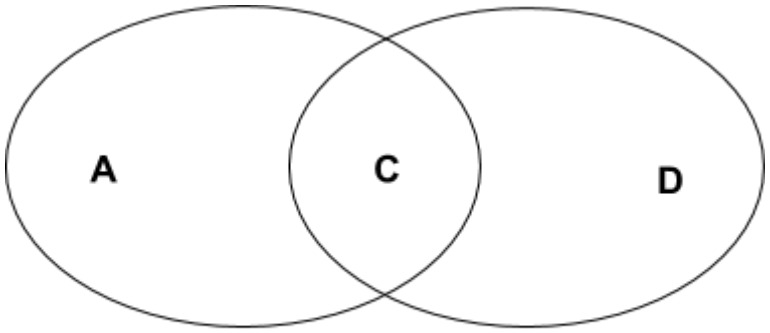
Estación E: es la contrapartida de B. Ver estación B

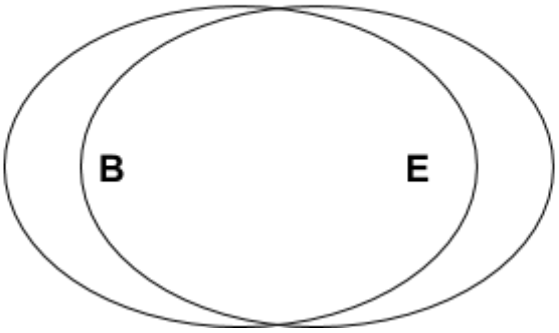
Una disposición posible de este escenario es la siguiente:

* B está al alcance de E y viceversa

* A y D están al alcance de C pero D no está al alcance de A y A no está al alcance de D.

Entre sí la unión de los alcances de B y E por un lado y de A, C y D por el otro pueden no tener intersección. Ilustro esto en un gráfico.





ii)

La estación oculta se produce cuando dos estaciones están al alcance de una tercera pero entre si no se alcanzan. Cuando una de las dos quiere enviar a la tercera, la otra piensa que puede enviar porque escucha el canal inactivo. Esto se produce principalmente porque las conexiones de radio son half-duplex y porque una estación no puede escuchar y enviar al mismo tiempo en la misma frecuencia.

Este escenario se da entre las estaciones A, C y D. Como A comenzó la comunicación con C y la efectivizó. D es la estación oculta.

// Ejercicio 3

// Datos
Dominio: flaxo.onr
Servidor DNS Maestro: dns.flaxo.org (red:7:3:4:56)
Servidor DNS Externo: dns.ezeq.edu.ar (2620:171:800:714::1)

Servidor de correo: info.flaxo.org (red:7:3:4:152)
Servidor de correo comercial: comercial.flaxo.org (red:7:3:4:151)
//Nota: le doy más prioridad al correo comercial

Subdominio: quant.flaxo.org delega a
  * maestro: mi_dns.quant.flaxo.org (red:7:3:4:53)
  * externo: dns.ezeq.edu.ar

Hosts Desktop - IP red:7:3:4:103
Hosts Mobile - IP red:7:3:4:104

// ---------------------------------------
// En etc/bind/db.flaxo.org

flaxo.org. IN SOA dns.flaxo.org. mailAdmin.flaxo.org {20201221-00; 2h;
15m; 3W2h; 604800};

flaxo.org. IN NS dns.flaxo.org.
flaxo.org. IN NS dns.ezeq.edu.ar.
flaxo.org. IN MX 10 comercial.flaxo.org. //Mayor prioridad
flaxo.org. IN MX 20 info.flaxo.org.

dns.flaxo.org. IN AAAA netID:7:3:4:56
dns.ezeq.edu.ar. IN AAAA 2620:171:800:714::1
comercial.flaxo.org IN AAAA netID:7:3:4:151
info.flaxo.org IN AAAA netID:7:3:4:152

desktop IN AAAA netID:7:3:4:103
mobile IN AAAA netID:7:3:4:104

//Ejercicio 4

```
#!/bin/bash
# Nota: siempre que sea posible fuente e input o destino y output
# como una medida extra de seguridad

#Constantes
LAN = 172.30.80.0/17
DMZ = 220.12.12.0/29
INET = 200.11.20.0/29

#Interfaces del Router1
IF_DMZ = eth0
IF_LAN = eth1

DB = 172.30.80.6/17
WEB = 220.12.12.66/29

I=/sbin/iptables

# Flusheeo reglas anteriores
$I -F #tabla filter
$I -F -t nat

case $1 in
  start)

        # Política por defecto: droppear/ignorar paquetes
        $I -P FORWARD DROP

        # Reglas de estado, se necesitan para un router stateful
        $I -A FORWARD -m state --state INVALID -j DROP
        $I -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
        # Si llega hasta acá es porque los paquetes son NEW


        #---------------------
        # Tabla filter

        # Ej 1 - Las PCs en LAN tiene acceso al servidor WEB de la DMZ
        # tcp - puertos http (80) y https (443)
        $I -A FORWARD -s $LAN -i $IF_LAN -d $WEB -o $IF_DMZ -p tcp -m multiport \
        --dports 80,443 -j ACCEPT
        # Como el router1 no tiene salida a internet, el acceso de la LAN a internet
        # se lo deberá garantizar el Router 2

        # Ej 2 - El servidor WEB de la DMZ puede recibir acceso desde cualquier lado
        # Para el Router 1 es importante que la LAN tenga acceso al servidor
        # Este comportamiento está garantizado por el ejercicio 1
        # Ej 2 - El servidor WEB de la DMZ puede recibir acceso SSH desde la red
        # de servicio de soporte. Como el router no tiene salida a internet, este
        # comportamiento no es relevante para el R1 (sí para el router 2)

        # Ej 3 - Los servidores de la DMZ pueden hacer consultas DNS al exterior
        # Nuevamente como el router no tiene salida a internet, este
        # comportamiento no es relevante para el R1 (sí para el router 2)
```

```
        # Ej 3 - Los servidores de la DMZ pueden hacer consultas sql (puerto 3306)
        # al servidor de base de datos de la LAN
        # La siguiente regla va a permitir consultas sql desde cualquier servidor
        # de la DMZ. Si en un futuro se agregan más servidores, tendrán acceso.
        # Si se quisiera restringir a solamente el servidor WEB se tendría que
        # reemplazar la fuente DMZ por la fuente WEB (definida como constante)
        $I -A FORWARD -s $DMZ -i $IF_DMZ -d $LAN -o $IF_LAN -p tcp --dport 3306 -j ACCEPT

        # Se podría pensar que al final del conjunto de comportamientos que se espera
        # que agreguemos al firewall hay un "y nada más".
        # Esto se verifica por la política por defecto
        # Los paquetes que no matchean se ignoran y no se envía ningún mensaje ICMP respuesta
        # (Diferencia entre DROP y REJECT)

        #--------------------
        # Tabla NAT

        # Postrouting - No está disponible -i
        # Ej 1 - Nateo fuente (de la LAN a la DMZ)
        $I -t nat -A POSTROUTING -s $LAN -d $WEB -o $IF_DMZ -p tcp -m multiport \
        --dports 80,443 -j SNAT --to $DMZ

        # Prerouting - No está disponible -o
        # Ej 2 - Nateo destino (de la DMZ a la LAN)
        $I -t nat -A PREROUTING -s $DMZ -i $IF_DMZ -d $LAN -p tcp --dport 3306 \
        -j DNAT --to $LAN
;;
  stop)
        $I -F #tabla filter
        $I -F -t nat
;;
  *)
        echo "Error de sintaxis"
        exit 1
;;
esac
```