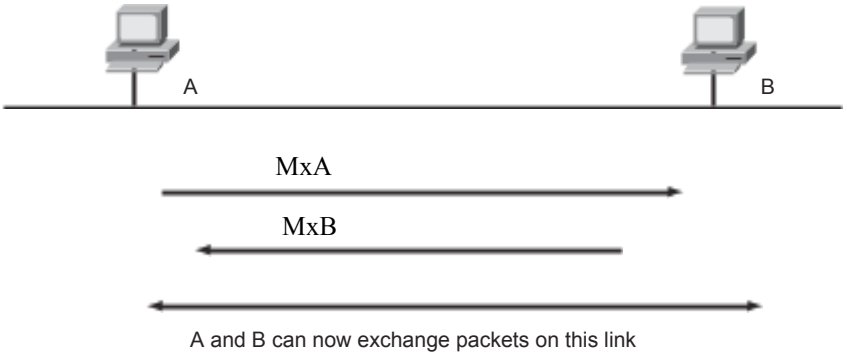
Examen Final – Parte Práctica **COMUNICACIONES** Fecha: 21/12/2020

Nombre y Apellido: Díaz Agustín.
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.?)

Solución:

a) La finalidad del descubrimiento de vecinos es conocer las direcciones físicas(MAC) de los nodos vecinos en la misma red (análogo a ARP en IPv4), detectar direcciones duplicadas y acceder a los routers. Se utilizan mensajes ICMP de Multicast Solicited Node con el par (IP, MAC) del emisor y se espera la respuesta de la request de los vecinos, así se cachean las direcciones entre sí.
b)

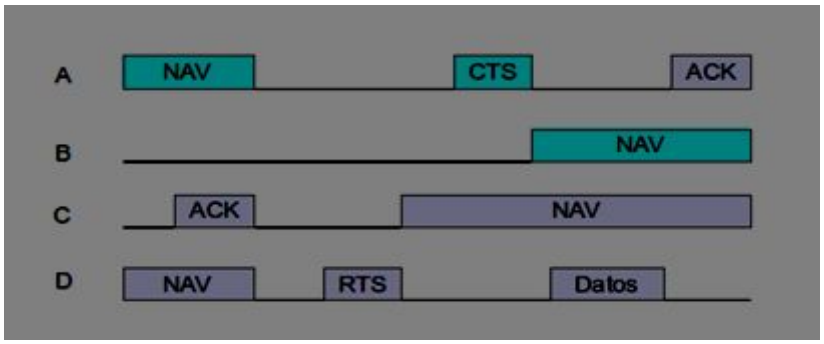
-MxA envía un mensaje ICMPv6 del tipo Neighbour Discovery, con su dirección IPv6 como Source, Multicast Solicited Node como Destino, y con su dirección de enlace MAC como DATA

-MxB responde con el mismo tipo de mensaje ICMPv6 del tipo Neighbour Discovery, señalando su dirección IPv6 en Source, la dirección de A como Destino y su dirección de enlace MAC como DATA

De esta manera tanto A como B conocen las (IP, MAC) de cada una

c) Las direcciones están mencionadas en el apartado b. El alcance es red (por la dirección IPv6 del protocolo de capa de red) y enlace subcapa MAC (por la dirección física en la DATA de los mensajes)

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?

iii. ¿El NAV es una trama que se envía por el canal? Justifique su respuesta.

Solución:

i)

- A y D estaban esperando el fin de una transmisión hacia C (por eso sus NAV que terminan con el ACK de C).
- D quiere enviar a A, por lo cual envía un RTS y D responde con CTS
- C comienza su NAV a partir del RTS de D
- Como B está al alcance de A, comienza su NAV a partir del CTS de A
- D envía Datos a A y A responde con ACK, finalizando la transmisión y cerrando el NAV de B y C

Entonces nos quedó que

-B está al alcance de A,

-C, D y A se pueden alcanzar entre sí.

ii) Existe ya que B está al alcance de A pero no de D(y C), y A está al alcance de D(y C). Si no utilizáramos las tramas de control CSMA/CA estilo MACAW podría pasar que D(o C) se esté comunicando con A y cuando B quiere comunicarse con A, escucha el medio y no ve la señal de D(o C). D(o C) sería la estación oculta de B y viceversa.

iii) Existe el campo NAV que se envía dentro de una trama que avisa el tiempo que deberán estar inactivas las estaciones cuando se comienza una transmisión, y el NAV en sí mismo que es el Network Allocation Vector que es un contador que van disminuyendo las estaciones por sí solas (en base al campo NAV recibido).

3) La empresa Magenta(R) cuenta con el dominio magenta.com

El servidor maestro para magenta.com es ns1.magenta.com y su dirección IP 192.168.0.1
El primer servidor esclavo es ns2.magenta.com y su dirección de IP es 192.168.0.66.
El segundo servidor esclavo externo ns3.impresiones.com para el dominio magenta.com
Los servicios FTP y www son provisto por 192.168.0.2
Hay dos hosts llamados color y monocromo (192.168.0.3 y 192.168.0.4).
El servicio de mail es externo al dominio magenta.com (mail.impresiones.com)
La resolución inversa se realiza en ns1.magenta.com

i) Escribir el archivo named.conf del servidor maestro magenta.com
ii) Escribir el archivo de zona directa e inversa de ns1.magenta.com

Solución:
i) named.conf para ns1.magenta.com

```
zone “magenta.com”{
        type master;
        file “/etc/bind/db.magenta”;
}

zone “0.168.192.in-addr.arpa”{
        type master;
        file “/etc/bind/rev.magenta”;
}
```

ii) db.magenta: zona directa en ns1.magenta.com

```
$ TTL 1D
$Origin magenta.com.
@ IN SOA ns1        adminMail (2020122100; 5h; 15m; 3W12h; 2h20m)

        IN NS ns1
        IN NS ns2
        IN MX 10 impresiones.com.

ns1     IN A    192.168.0.1
ns2     IN A    192.168.0.66

FTP     IN A    192.168.0.2
www     IN A    192.168.0.2 Usar CNAME

color   IN A    192.168.0.3
monocromo  IN A    192.168.0.4
```

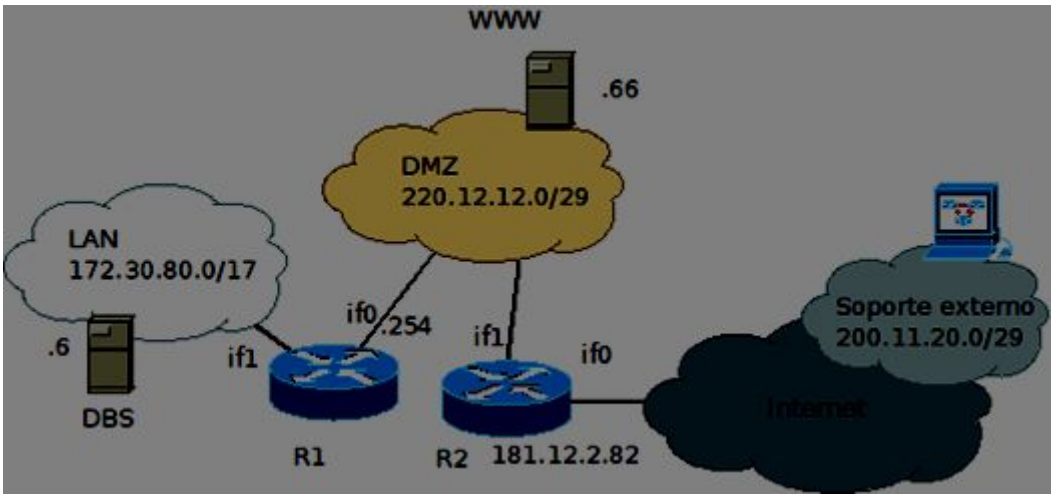
// rev.magenta: zona inversa en ns1.magenta.com

```
$ TTL 1D
$Origin 0.168.192.in-addr.arpa.
@ IN SOA ns1        adminMail (2020122100; 5h; 15m; 3W12h; 2h20m)
```

IN NS ns1.magenta.com

1	IN PTR	ns1.magenta.com.
2	IN PTR	FTP.magenta.com.
2	IN PTR	www.magenta.com.
3	IN PTR	color.magenta.com.
4	IN PTR	monocromo.magenta.com.
66	**IN PTR**	**ns2.magenta.com.**

4- Ejercicio de Firewall (20201221)



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

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.

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.

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.

Solución:

```
I = /sbin/iptables

# Constantes

LAN=172.30.80.0/17

IF_LAN=if1

DMZ=220.12.12.0/29

IF_DMZ=if0

SOP=200.11.20.0/29

INET=181.12.2.82

DBS=172.30.80.6

# Flush de reglas anteriores
```

```
$I -F

$I -F -t nat


case $1 in

        start)

# Política por defecto: Drop

$I -P FORWARD DROP

# Reglas de estado para ser un firewall stateful

$I -A FORWARD -m state --state INVALID -j DROP

$I -A FORWARD -m state --state RELATED, ESTABLISHED -j ACCEPT

# A partir de aquí son sólo paquetes NEW


######### Tabla Filter

# LAN accede a los puertos web (80 y 443 TCP) del servidor de la DMZ

$I -A FORWARD -s $LAN -i $IF_LAN -d $DMZ -o $IF_DMZ \

        -m multiport -p tcp --dports 80, 443 -j ACCEPT

# LAN accede a Internet

$I -A FORWARD -s $LAN -i $IF_LAN -d $INET -j ACCEPT


# El servidor de la DMZ puede recibir accesos a los puertos web desde cualquier lado
$I -A FORWARD -d $DMZ -o $IF_DMZ \
        -m multiport -p tcp --dports 80, 443 -j ACCEPT

# y SSH (tcp/22) solamente desde la red de servicio soporte. Es trabajo de R2


# Los servidores de la DMZ sólo pueden consultar DNS al exterior (puertos 53 tcp y udp). Es trabajo del R2

# y al puerto 3306 del servidor de base de datos.

$I -A FORWARD -s $DMZ -i $IF_DMZ -o $IF_LAN -d  $DBS\
        --dport 3306 -j ACCEPT
```

######### Tabla Nat
LAN accede a Internet, pero tener en cuenta que se natean en R1. NO natear el tráfico hacia la DMZ.

$I -t nat -A POSTROUTING -s $LAN -d $INET -o $IF_DMZ -j SNAT --to $INET

;;

stop)

$I -F

$I -F -t nat

;;

*)

echo "Error de sintaxis"

exit 1

;;

esac