Redes y Comunicaciones 2017
Práctica 8

Autor: Fermín Minetto (http://www.github.com/ferminmine)

2) Diferencias, pros y contras del ruteo estático y dinámico

Hay dos formas de definir las tablas de ruteo de los routers que componen una red, y estas pueden ser de manera estática o dinámica. En la manera de ruteo estática el administrador de la red configura las tablas de ruteo de los routers que componen la red de manera manual, es decir, añadiendo cada una de las entradas para que cada subred pueda comunicarse con otra. Lo bueno de esto es que resulta al administrador más fácil de comprender y configurar, aunque sea más propenso a errores y poco escalable.

En cambio, en el ruteo dinámico, el administrador de la red se vale de ciertos algoritmos de ruteo para que los routers puedan definir sus tablas de ruteo de manera automática. Lo bueno de esto es que es mucho más escalable, y no requiere de la mano del administrador ante cambios en la red, y que la configuración suele ser menos propensa a errores. La desventaja es que se usan recursos del router y ancho de banda de los enlaces, y que el administrador requiere más conocimientos para su configuración.

Característica	**Enrutamiento dinámico**	**Enrutamiento estático**
Complejidad de configuración	Por lo general, es independiente del tamaño de la red.	Depende del tamaño de la red.
Conocimientos requeridos por el administrador	Se requiere de un conocimiento avanzado.	No se requieren conocimiento adicionales.
Cambios de topología	Se adapta automáticamente a los cambios en la topología.	Requiere la intervención del administrador de la red ante cambios.
Escalabilidad	Resulta ideal para redes que sufren de cambios o se incrementan constantemente.	Resulta mucho menos escalable.
Seguridad	Es menos seguro	Resulta más seguro
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlces.	No se requieren recursos adicionales.
Capacidad de predicción	La ruta depende de la topología actual.	La ruta hacia el destino es siempre la misma.

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

Si, debería tener tabla de ruteo en caso de querer comunicarse con otros dispositivos de otra subred, por ejemplo, una impresora en otra oficina alejada de un edificio, u otros dispositivos dentro de la misma red.

4) Ejercicio práctico de ruteo

- Cambiar una dirección IP: **`ifconfig eth0 192.168.99.14 netmask 255.255.255.0 up`**
- Listar entradas en la tabla de ruteo: **`route -n`**
- Agregar una entrada a tabla de ruteo: **`route add -net 192.168.98.0 netmask 255.255.255.0 gw 192.168.99.1`**
- Agregar una entrada a tabla de ruteo conectada directamente: **`route add -net 192.168.98.0 netmask 255.255.255.0 dev ethx`**
- Borrar entrada en tabla de ruteo: **`route del -net 192.168.98.0 netmask 255.255.255.0 gw 192.168.99.1`**
- Agregar ruta por defecto: **`route add default [gw 192.2.1.1] [dev eth0]`**

El **IP_FORWARD** es una configuración que sirve para que una PC rutee paquetes entre sus distintas placas de red, normalmente es deseable tener esto activado. La configuración de esto en los routers y las PCs, esta en:cat /proc/sys/net/ipv4/ip_forward.

RP_FILTER: Este parámetro, por seguridad, evita la recepción de paquetes por una interfaz que vengan de una IP de una red que el router no rutearía a través de esa interfaz. Este valor debe deshabilitarse en caso que el enrutamiento circular propuesto cause problemas. Para obtener el valor:
cat /proc/sys/net/ipv4/conf/all/rp_filter
El valor en 0 deshabilita su funcionalidad. Un 1 lo habilita. Para cambiar el valor:
echo 0 >/proc/sys/net/ipv4/conf/all/rp_filter.

Si se realiza un ping a la dirección 5.5.5.5, se va a recibir un mensaje "Time to Live exceeded", esto significa que posiblemente el paquete quedó en loop infinito entre los routers y como no pertenecía a ninguna de las subredes directamente conectadas a estos routers o en sus tablas de ruteo, quedó dando vueltas hasta que acabó "muriendo".
Si se realiza un ping a un host desconocido dentro de una red conocida, el que responderá con host unreachable en ICMP será un router conectado directamente a la red. En cambio, si se hace un ping a una subred desconocida, el paquete se quedará dando vueltas hasta que "muera".
Si se activa en el router n1 el RP_FILTER, y luego se hace un ping desde n6 hasta n11, el ping se enviará, pero no se recibirá la respuesta puesto que el router n1 no routeará el paquete recibido desde la subred 10.0.5.0/24 ya que no aparece en la

tabla de ruteo. Esto podría solucionarse sin cambiar la configuración añadiendo en el router n1 la entrada de ruteo para la subred correspondiente 10.0.5.0/24.

Resultaría poco escalable si hubiera 20 routers.

6 y 7) Algoritmos de ruteo

¿Cual converge más rapido? ¿Que hay que notar de diferencia? Para mi se ven iguales. Las tablas de ruteo van a ser los caminos mas cortos en ambos algoritmos, o no?

	¿Cada router conoce la topología completa?	**¿Converge rápidamente?**	**Protocolos que lo implementan**
Vector de distancias	Cada router conoce a sus vecinos y las redes alcanzables	Puede llegar a tener un tiempo de convergencia bastante lento.	RIP
Estado de enlaces	Cada router conocela topología completa y el estado de los enlaces	Si, converge rápidamente.	OSPF

8) DHCP

El Dynamic Host Configuration Protocol permite que a un host se le asigne de forma automática una dirección de IP sin necesidad que un administrador de redes tenga que configurarla de manera manual. Un administrador de red puede configurar DHCP de manera que un host determinado reciba siempre la misma dirección IP temporal que será diferente cada vez que el host se conecte a la red.
A medida que los hosts se unen a la red y salen de ella, el servidor DHCP necesita actualizar su lista de direcciones IP disponibles. Cada vez que un host se une a la red, el servidor DHCP asigna una dirección arbitraria de su conjunto actual de direcciones disponibles.

1. Cuando un host llega a la red debe encontrar un servidor DHCP con el que interactuar. Esto se hace mediante un *mensaje de descubrimiento DHCP* que envía un cliente dentro de un paquete UDP al puerto 67 a la dirección de difusión.
2. Un servidor que recibe un mensaje de descubrimiento DHCP responde al cliente con un mensaje de oferta DHCP, que se difunde a todos los nodos de la subred utilizando de nuevo la dirección IP de difusión (255.255.255.255). Cada

mensaje de oferta de dirección contiene la dirección IP propuesta, la máscara de red y el tiempo de arrendamiento de la dirección IP.
3. El cliente seleccionará de entre las ofertas de servidor y responderá a la oferta seleccionada con un mensaje de solicitud DHCP, devolviendo los parámetros de configuración.
4. El servidor contesta al mensaje de solicitud DHCP con un mensaje ACK DHCP, que confirma los parámetros solicitados.

Ejecutando el comando *sudo /sbin/dhclient eth0* dispara varios mensajes de descubrimiento DHCP. La información intercambiada contiene lo mencionado antes del protocolo DHCP.
El archivo /var/lib/dhcp/dhclient.leases guarda información de los "arrendamientos" de IP de la computadora. Por ejemplo, la interface, la dirección IP y máscara de subred, el tiempo del arrendamiento, etc...

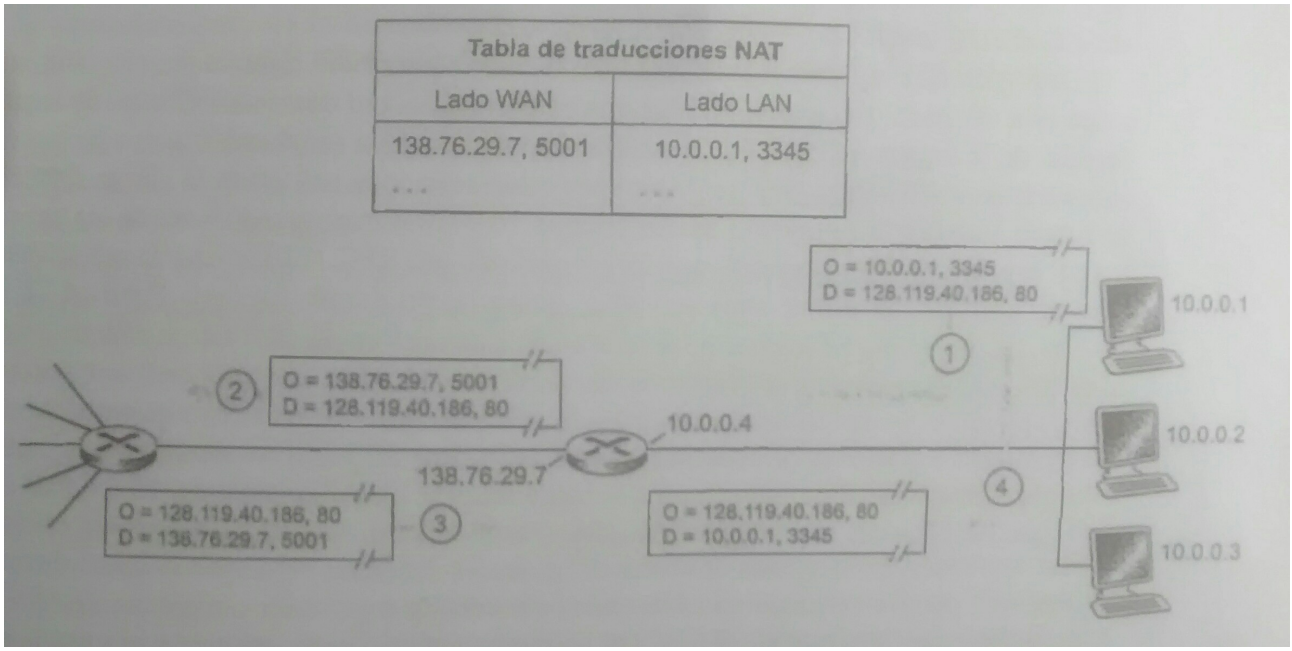
Diferencia: *consultar.*

9 y 10) NAT y RFC-1918

El NAT, o Network Adress Translation es un servicio que provee un router mediante el cual se traducen direcciones IP privadas a IP públicas y viceversa. Unas *direcciones IP privada hacen referencia a una red cuyas direcciones solo tienen significado dentro de los dispositivos internos de dicha red*. Se pueden ahorrar muchísimas direcciones IP si los dispositivos de pequeñas oficinas y redes hogareñas pueden compartir la misma dirección IP pública en lugar de asignársele a cada dispositivo una dirección pública.

Los router NAT no parecen routers a ojos del mundo exterior. En su lugar, un router NAY se comporta de cara al exterior como un único dispositivo con una dirección IP única. Todo el tráfico que sale de una subred sale por el router NAT con una dirección IP pública única, y todo el tráfico que entra tambíen. El router NAT oculta los detalles de la red doméstica al mundo exterior.
Un router NAT obtiene su dirección del servidor DHCP del ISP y el router ejecuta un servidor DHCP para proporcionar direcciones a las computadores (privadas), dentro del espacio de direcciones de la red doméstica controlada por el router NAT-DHCP.

¿Cómo sabe el router a qué host interno debería reenviar un datagrama dado? El truco consiste en utilizar la tabla de traducciones NAT almacenada en el router NAT, e incluir los números de puerto, así como las direcciones IP en las entradas de la tabla.



En una red hogareña, todos nuestros dispositivos tienen distintas direcciones IP privadas, que cuando realizan un requerimiento a direcciones IP públicas de Internet van a necesitar una traducción para que puedan comunicarse con dipositivos con IP públicas asignada. Entonces, cuando nuestros dispositivos hacen un requerimiento a una dirección IP pública, el router de salto capta nuestra IP privada y la convierte a una IP pública para hacer el requerimiento a nombre de la IP pública asignada. Cuando vuelva la respuesta a un requerimiento, el router de salto realizará un proceso inverso de conversión de IP pública a una privada para devolver la respuesta al host correspondiente dentro de la subred (que tiene asignada una IP privada).

La RFC-1918 determina que bloques de IP privadas le corresponde a cada clase de red.

Nombre	Rango de direcciones IP	Cantidad de IP	Descripción de la clase
bloque de 24 bits	10.0.0.0 – 10.255.255.255	16.777.214	red simple clase A
bloque de 20 bits	172.16.0.0 – 172.31.255.255	1.048.574	16 redes clase B continuas
bloque de 16 bits	192.168.0.0 – 192.168.255.255	65.534	256 redes clase C continuas
bloque de 16 bits	169.254.0.0 – 169.254.255.255	65.536	clase B simple