Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería Informática

Dept. Teoría de la Señal, Telemática y Comunicaciones

Práctica 3 – Configuración de Red I y II

(0.5 puntos + 0.5 puntos)

Realización práctica (parte I)

1) Compruebe el número de isla y puesto en el que se encuentra e identifique a sus compañeros en la isla. Compruebe las direcciones IP que tiene asignadas las diferentes interfaces de red de su puesto mediante el comando `ifconfig`, ¿cómo se llaman dichas interfaces? ¿Qué direcciones de red hay definidas? ¿Qué direcciones tienen el *router* al que se conecta el equipo que está usando?

Para ver a mis compañeros miramos la figura 1 del pdf y a figura 2 del pdf.

Para ver las direcciones IP de mis interfaces de red usamos *ipconfig.* Las que tenemos son las siguientes:

Para ver las direcciones del router hay que mirar la figura 2 del pdf.

2) Introduzca las entradas de encaminamiento necesarias para comunicar todos los puestos de usuario de su isla. Compruebe la configuración de las utilidades `ping` y `traceroute`, y anote los resultados.

Ponemos el router como gateway por defecto con *route add default gw 33.2.X.1*
Comprobamos el enrutamiento con *route (-n)*
Accedemos al router poniendo la dirección IP (admin sin contraseña). Lo que hacemos es decir que para una dirección destino la puerta de enlace sea la dirección de la interfaz interna del router de dicha subred.
33.X.2.0/24 → 172.16.X.2
33.X.3.0/24 → 172.16.X.3
ping 33.X.3.2
traceroute 33.X.1.3.2

3) Introduzca las entradas de encaminamiento necesarias para comunicar todos los puestos de usuario de su isla con los puestos de usuario de otra isla. Compruebe la configuración con las utilidades `ping` y `traceroute`.

Tenemos que configurar RX_4 y RX_5 y a continuación RX_6. Aparte de configurar nuestros routers, los routers de la isla con la que queremos comunicarnos también deben ser configurados para ello.

RX_1

33.X.2.0/24 → 192.16.X.2
33.X.3.0/24 → 192.16.X.3
0.0.0.0 → 172.16.X.4
0.0.0.0 → 172.16.X.5

RX_4 y RX_5

33.X.1.0/24 → 172.16.X.1
33.X.2.0/24 → 172.16.X.2
33.X.3.0/24 → 172.16.X.3
0.0.0.0 → 172.17.X.6

RX_6

33.X.0.0/22 → 172.16.X.4
33.X.0.0/22 → 172.16.X.5
0.0.0.0 → 220.10.10.X

Realización práctica (parte II)

1) Configure el *router* con el que está directamente conectado para que no reenvíe ningún tipo de tráfico (acción "drop"). Habitualmente, al configurar un cortafuegos, inicialmente se deniega cualquier acceso, y luego se añaden reglas para el tráfico que sí se desea dejar pasar.

General > cadena "forward" // Action > drop

2) A continuación configure el cortafuegos del *router* para que permita a otros ordenadores:

a) conectarse al servidor de SSH del ordenador que tenga la dirección 33.X.Y.2.

b) iniciar una conexión al servidor de SSH del ordenador que tenga la dirección 33.X.Y.3.

a) Voy a usar de ejemplo el servidor 33.1.1.2
- Cliente → Servidor: aceptar (accept) la conexión en salida con el servidor como destino (33.1.1.2) y con puerto destino 22, protocolo de trabajo 6 (TCP) y puerto correcto.
- Servidor → Cliente: aceptar (accept) la conexión en entrada con el servidor como origen y cualquier ordenador como destino. Protocolo de trabajo 6 (TCP) y 22 como puerto origen.

b)
1. Aceptar el tráfico TCP desde cualquier dirección hacia la dirección 33.1.1.2 y puerto 22 (el puerto de la conexión SSH).
2. Aceptar el tráfico TCP desde cualquier dirección desde el puerto 22 hacia la dirección 33.1.1.3.
3. Aceptar el tráfico TCP desde la dirección 33.1.1.2 y el puerto 22 hacia cualquier dirección.
4. Aceptar el tráfico TCP desde la dirección 33.1.1.3 con cualquier dirección de destino, pero al puerto 22.

Dichas reglas son las que vamos a crear introduciendo lo siguiente:

1. General → Chain: forward / Dst. Address: 33.1.1.2 / Protocol: 6 (tcp) / Dst. Port: 22 Action → Action: accept
2. General → Chain: forward / Dst. Address: 33.1.1.3 / Protocol: 6 (tcp) / Src. Port: 22 Action → Action: accept
3. General → Chain: forward / Src. Address: 33.1.1.2 / Protocol: 6 (tcp) / Src. Port: 22 Action → Action: accept
4. General → Chain: forward / Src. Address: 33.1.1.3 / Protocol: 6 (tcp) / Dst. Port: 22 Action → Action: accept

drop al final

c) *(Opcional)* Configure el mismo *router* para que permita hacer ping de un ordenador a otro, pero no en sentido contrario. (Nota: la herramienta ping envía un mensaje ICMP de tipo “echo request”, y recibe un mensaje ICMP del tipo “echo reply”).

Advanced → *Permitimos* al ordenador destino (33.1.1.3) recibir el mensaje *echo request* y enviar *echo reply* y hemos permitido al ordenador origen (33.1.1.2) de enviar *echo request* y recibir *echo reply*.
Como por defecto hay un accion *drop* de todas las posibles conexiones, el ordenador destino no puede hacer un *ping* al ordenor origen.