TPL 1 - Configuración inicial de la red del laboratorio

Fecha de Entrega: Luján 28/03/2019

Objetivo: Conocer el procedimiento inicial y hacer habitual la práctica de configuración de un host en una red basada en el juego de protocolos TCP/IP.

Consignas

Salvo indicación en contrario, todos los comandos siguientes se deben ejecutar con permisos de usuario administrador (`root`). Para obtenerlos, utilice el comando `su`.

1. Verificar la/s interfaces físicas de red (NIC) que el sistema operativo haya detectado. Para ello, utilizar el comando `ip link show`, el cual muestra las interfaces físicas y su estado. El primer dígito en cada línea es el número de interfaz (comúnmente llamada *placa de red*), el segundo texto es el nombre de la interfaz, y lo que figura entre símbolos <> es su estado.

   Las interfaces con nombres `eth{N}`, `eno{N}`, `ens{N}f{N}`, `enp{N}s{N}`, `w{N}g{N}` son interfaces físicas (*hardware real*). Existe al menos una interfaz virtual denominada `lo` o `loopback` y es posible que existan otras interfaces virtuales con nombres diversos (`tun{N}`, `br{N}`, ...).

   El primer paso de este práctico es determinar cual de todas las interfaces es la real y tomar nota de su nombre. Aparecerá en el listado con el estado *BROADCAST*.

2. Configuración de interfaces de red para utilizar el protocolo TCP/IP.

   El paso siguiente es asignar a la interfaz física una dirección de red IP según el plano anexo. Para ello, utilizar los siguientes comandos:

   ```
   ip addr add dev {interfaz} {dirección_IP[/{prefijo_máscara]}
   ip link set dev {interfaz} up
   ```

   Por ejemplo:

   ```
   ip addr add dev {interfaz} 192.168.0.143/24
   ip link set dev {interfaz} up
   ```

   Verificar configuración con:

   ```
   ip addr show
   ```

3. Verificar que es posible contactar a otros 2 equipos de la red utilizando el comando `ping`:

   ```
   ping {DIRECCIÓN IP}
   ```

4. Configuración del nombre del equipo:

   a. Temporal: utilizando el comando `hostname`:

      ```
      hostname {nombre_equipo}
      ```

      donde `{nombre_equipo}` es el nombre que le corresponde al equipo según el diagrama establecido de la red.

   b. Permanente: Editar el archivo `/etc/hostname`, asignando el nombre que le corresponde al equipo.

5. Resolución de nombres de hosts a direcciones IP.

   a. Completar el archivo `/etc/hosts` con los nombres y las direcciones de red de al menos 2 máquinas del laboratorio para la resolución local de nombres.

   b. Verificar que es posible contactar otros 2 equipos de la red utilizando nombres de host ejecutando `ping {NOMBRE DE HOST}`

6. Ver la tabla de ruteo definida utilizando el comando `ip route show`.
   ¿Cuáles son las redes accesibles?

7. Agregar la dirección `10.4.11.30` como ruta por defecto para acceder a otras redes:

   ```
   ip route add default via 10.4.11.30
   ```

   Verificar nuevamente la tabla de ruteo.

8. Realizar una captura de las PDU intercambiadas mientras se utiliza el comando `ping` para verificar conectividad con otro equipo. Las acciones que debe realizar son:

   a. Iniciar la captura redireccionando la salida a un archivo para su posterior análisis:

   ```
   tcpdump -n -p -w NOMBRE_ARCHIVO.PCAP 'icmp && host DIRECCION_IP'
   ```

   Parámetros utilizados:

   -n no resuelve nombres de objetos de red (por ej. nombres de host, puertos TCP y UDP).
   -p no capturar en modo promiscuo.
   -w guarda paquetes capturados en el archivo indicado.
   'icmp && host DIRECCION_IP' filtrar, en este caso, sólo tramas que lleven mensajes de protocolo ICMP **y** provengan o estén destinadas a la dirección IP especificada.

   b. En otra terminal ejecutar el comando ping para enviar un mensaje ICMP Echo Request:

   ```
   ping Dirección_IP -c 3
   ```

   c. Una vez obtenida la respuesta del comando *ping* (deberán recibirse tres respuestas), detener la captura (finalizar el proceso *tcpdump* presionando **Ctrl+C**)

   d. Analizar el volcado del programa de captura utilizando la aplicación wireshark (o cualquier otro analizador de tráfico que permita leer archivos en formato *pcap*), representando en un gráfico ideado por usted el intercambio de mensajes. Indicar cuál es la función de cada uno identificando los datos de encabezados mas relevantes.

Bibliografía

- Guía del comando TCPdump. Jeremy Stretch. Traducido al español por el equipo de LabRedes http://www.labredes.unlu.edu.ar/files/site/data/tyr/tcpdump-esp-draft1.pdf
- "Redes globales de información con Internet y TCP/IP". Tercera Edición. Douglas E. Comer, Prentice Hall. Capítulo 4: "Direcciones Internet".
- "Redes globales de información con Internet y TCP/IP". Tercera Edición. Douglas E. Comer, Prentice Hall. Capítulo 5: "Transformación de direcciones Internet en direcciones físicas".
- "Comunicaciones y Redes de Computadoras", Sexta Edición, William Stallings, Prentice Hall. Capítulo 14.1: "Ethernet (CSMA/CD)"
- El manual del Administrador de Debian. Raphaël Hertzog, Roland Mas. Freexian. 2016. Apéndice B: "Curso breve de emergencia" https://debian-handbook.info/browse/es-ES/stable/short-remedial-course.html

- Tcpdump Examples: Practical examples to lift your network troubleshooting. Hacker Target Pty Ltd. 2018 https://hackertarget.com/tcpdump-examples/
- Páginas de manual de cada comando utilizado.

Mapa de la red del laboratorio

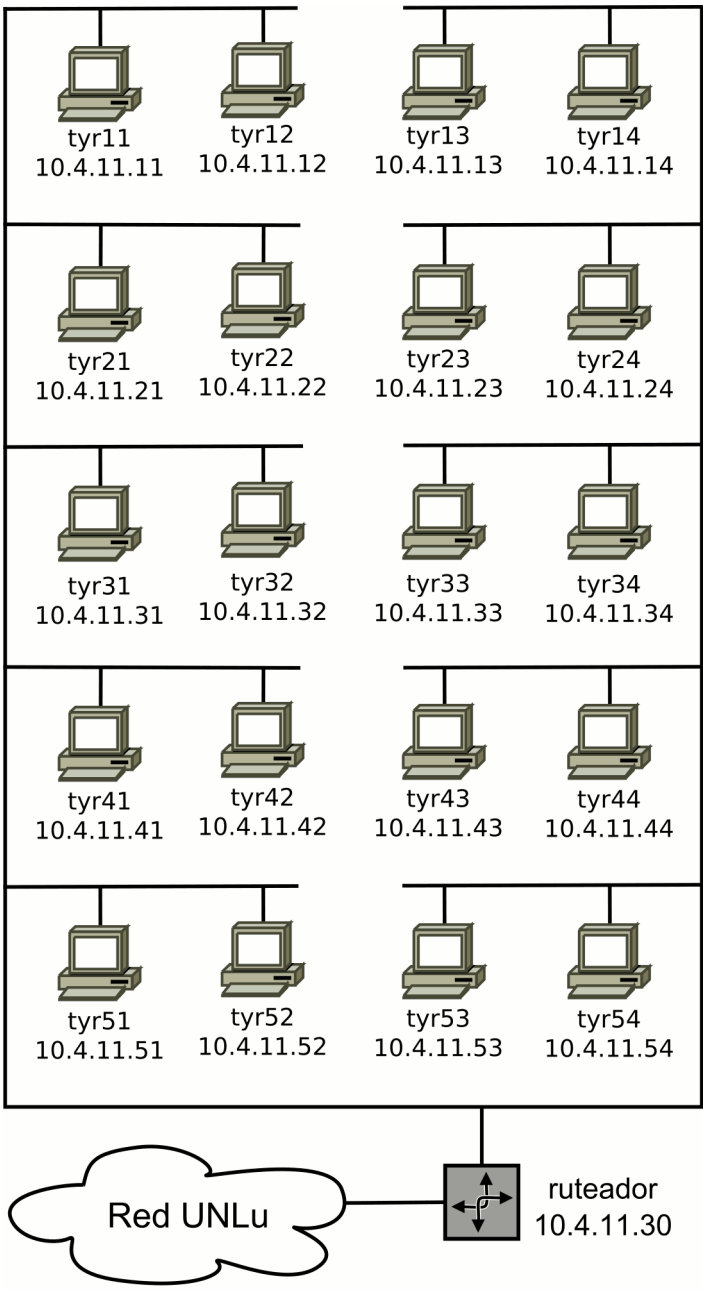

Figura 1:

- Dirección de red: **10.4.11.0**
- Máscara de red: **/24** o bien **255.255.255.0**
- Dirección de broadcast: **10.4.11.255**