|  |  |
| --- | --- |
| ***Despliegue de Aplicaciones Web***  **UD 1. Arquitectura de red** |  |
| **Práctica 1: Configurar Protocolo TCP/IP** |

**El fichero de entrega se debe llamar Practica\_1\_1\_Apellido1\_Apellido2\_Nombre.pdf .**

**Rellena al principio del fichero la siguiente información:**

Nombre del alumno:

ServidorLinuxXXX

◦ DirecciónIP

◦ Nombre del equipo

◦ Contraseña de usuario

◦ Contraseña de root

Equipo físico:

◦ DirecciónIP

◦ Nombre del equipo

Después inserta todas las capturas de pantallas en el enunciado correspondiente con la explicación correspondiente.

**La evaluación se realizará en base a los siguientes criterios:**

* Entrega el documento, contienen lo solicitado y los contenidos **son originales**.
* En los pantallazos se debe ver con **claridad fecha y hora**.
* Cuida la documentación, portada, índice, paginación, (sugerencia: puedes utilizar una plantilla para todos tus trabajos)

• Una vez terminada la práctica, sube el archivo en formato PDF a la plataforma Moodle.

**A) Creación de máquina virtual:**

La máquina virtual de Ubuntu-server que hemos realizado en las clases anteriores. (**Recordad tener siempre una copia disponible**)

La máquina debe estar configurada como si estuviera físicamente conectada a la red del aula. Para ello, tendremos que configurar la tarjeta de red del equipo virtual como ***“***adaptador puente” y seleccionar la tarjeta de red del equipo anfitrión que queremos utilizar. Sería conveniente refrescar las MAC de los equipos para evitar que puedan estar duplicadas en la red del aula.

Toma una captura de pantalla del inicio de sesión de la máquina virtual Ubuntu-server.

**B) Configuración con la red IP del Aula**

Vamos a configurar la dirección IP estática para que haya comunicación dentro del aula.

◦ Configuración IP estática

Entra con permiso de superusuario y averigua el nombre que el sistema ha asignado a las interfaces de red (puede ser eth0, eth1, eth2, eth3..., enp0s3, enp0s8) usando el comando

***..> ifconfig -a***

El resultado será la interfaz **lo** del **bucle local** y otra interfaz con el formato **ethX o enp0s3** (eth0,eth1,eth2,eth3...).

Toma una captura de pantalla del resultado de ejecutar el comando ifconfig.

Edita el fichero de configuración **/etc/netplan/00-installer-config.yaml** (por defecto, este fichero usa el protocolo DHCP para asignar una IP dinámica a la máquina linux) y modifícalo para que quede como el siguiente, sustituyendo ethX o enp0sXpor el nombre de tu interfaz de red cableada (siendo X el número asignado a tu interfaz de red, el cual obtuviste en el paso anterior).

**No olvides hacer una copia de la configuración anterior.**

# This is the network config written by 'subiquity'

network:

ethernets:

**enp0sX**:

**dhcp: no**

**addresses: [192.168.1.2xx/24]**

**gateway4: 192.168.1.1**

**nameservers:**

**addresses: [80.58.0.33]**

version: 2

dónde XX es el número de puesto en el que te encuentras.

Explicación:

* **addresses: [192.168.1.10/24]**: Establece que la *dirección IP* de equipo será siempre 192.168.1.10. Como es lógico, deberás adecuar este valor a tus propias necesidades. También indica que la máscara de red utiliza 24 bits (lo que equivale a **255.255.255.0**). Este valor también puede cambiar según las características de tu red.
* **gateway4: 192.168.1.1**: Determina que la dirección de la puerta de enlace para TCP/IPv4. En nuestro caso, el dispositivo que nos facilita el acceso a Internet. Para este ejemplo, 192.168.1.1, aunque su valor también dependerá de la dirección que tenga este dispositivo en tu instalación.

Recuerda que en **Ubuntu 22.04** ha cambiado la directiva por routes

routes:

- to: default

via: 192.168.1.1

* **nameservers**: Configura la dirección (o direcciones) de *Internet* donde se encuentra el *servidor DNS* que usaremos para convertir los nombres de dominio en *direcciones IP*. En este caso utilizaremos el servidor primario de [OpenDNS](https://www.opendns.com/).

Toma una captura de pantalla del fichero modificado.

Aplicar los cambios:

***..>*** sudo netplan apply

Verifica la nueva configuración:

***..>* ifconfig –a**

***..>*** ip addr

Consulta el fichero de configuración **/etc/resolv.conf** (este fichero contiene el servidor DNS que usará la máquina linux para resolver las URL y las direcciones IP, en próxima práctica usaremos nuestro propio servidor DNS) y comprueba que se usa el servidor **DNS**que has definido previamente. Puedes usar el comando **cat**

Toma una captura de pantalla del resultado.

Edita el fichero de configuración ***/etc/hostname*** *(guarda el nombre con el que se identificará la máquina en la red)*. En el fichero únicamente debes escribir el nombre que deseamos que tenga la máquina: **servidorXXX** (donde XXX son tus iniciales en minúsculas).

Edita el fichero **/etc/hosts (**guarda la correspondencia entre un dominio y una IP, lo usaremos más adelante**)** y asocia el nombre **servidorXXX** con la dirección IPde bucle interno (127.0.1.1):

**127.0.0.1 localhost**

**127.0.1.1 servidorXXX**

***….***

Toma una captura de pantalla de la modificación del fichero.

Reinicia la máquina con **reboot.**

**C) Comprobar la configuración**

Desde cada máquina (**servidorXXX y tu propia máquina física**), envía un comando ping para comprobar que existe comunicación con la otra a:

Toma una captura de pantalla de cada ejecución del comando ping.

- Cada una de la otra máquina

- Con la puerta de enlace

- Con internet

¿Existe algún problema?

**D) Habilitar respuesta ping en los Firewall de Windows**

• En **Windows 10**, con privilegios de administrador:

En **Menú Inicio, Panel de Control, Sistema y seguridad, Firewall de Windows, Configuración avanzada, Reglas de entrada**: habilita la regla **Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)**

Vuelve a ejecutar los **ping** del apartado anterior.

Toma una captura de pantalla de cada ejecución del comando ping.

**E) Puertos TCP y UDP**

• En **Windows 10**, con privilegios de administrador:

Averigua los puertos TCP a la escucha con **netstat -a -p TCP -n**

Averigua los puertos UDP a la escucha con **netstat -a -p UDP -n**

Toma una captura de pantalla de cada ejecución del netstat.

Abre el navegador y accede a una web de internet

Muestra las conexiones establecidas con **netstat -p TCP -n**

Toma una captura de pantalla de cada ejecución del netstat.

¿Qué puerto(s) ha asignado el sistema operativo al navegador web para establecer la(s) conexion(es) **TCP**?

¿Qué puerto(s) utiliza(n) el(los) servidor(es) con los que se establecen las conexiones?

***.***

• En ***Linux***, con privilegios de administrador:

Averigua los puertos TCP a la escucha con el comando **netstat -a -p TCP -n**

Averigua los puertos UDP a la escucha con el comando **netstat -a -p UDP -n**

Toma una captura de pantalla de cada ejecución del comando netstat.