

PRÁCTICA DE ARQUITECTURA DE RED

**Protocolo TCP-IP**



GRADO SUPERIOR D.A.W.

ÍNDICE

Ejercicio A Creación Máquina Virtual…………………….………………………….2-4

Ejercicio B Configuración con la red IP del Aula………..…………………5-10

Ejercicio C Comprobar la configuración……………………….……………….10-13

Ejercicio D Habilitar respuesta ping en los Firewall………………….13-17

Ejercicio E Puertos TCP y UDP………………………………..…………………………17-22

**Ejercicio 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.

Crea un usuario administrador para la máquina Ubuntu server que sea **Apellido1\_Apellido2**.

La CONTRASEÑA para dicho usuario ha de ser: **velazquez**

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

Configuramos la pestaña Red de la Máquina Virtual (dentro de Configuración) con Adaptador Puente y refrescamos la dirección Mac.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ahora entramos con el usuario

Texto

Descripción generada automáticamente

Creamos el usuario silva\_mulero y lo convertimos a administrador

Texto

Descripción generada automáticamente

Reiniciamos la máquina virtual

Texto

Descripción generada automáticamente

Ya estamos dentro del usuario silva\_mulero

Texto

Descripción generada automáticamente

**Ejercicio 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** (eth0,eth1,eth2,eth3...).

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

Miramos la ip

Texto

Descripción generada automáticamente

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: [172.26.XX.1/16]**

**gateway4: 172.26.0.2**

**nameservers:**

**addresses: [8.8.8.8]**

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.

Modificamos el archivo /etc/netplan/00-installer-config.yaml



Texto

Descripción generada automáticamente

Aplicar los cambios:

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

Verifica la nueva configuración:

***..>* ifconfig –a**

***..>*** ip addr

Texto

Descripción generada automáticamente

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.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Aquí ya está modificado

Texto

Descripción generada automáticamente

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: **ServidorLinuxXXX** (donde XXX son tus iniciales en minúsculas).



Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

**127.0.0.1 localhost**

**127.0.1.1 ServidorLinuxXXX**

Toma una captura de pantalla de la modificación del fichero.



Texto

Descripción generada automáticamente

Reinicia la máquina con **reboot.**

**Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja**

**Texto

Descripción generada automáticamente**

**Ejercicio C - Comprobar la configuración**

Desde cada máquina (**ServidorLinuxXXX 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?

**Texto

Descripción generada automáticamente**

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

**Ejercicio 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.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Habilitamos los “Archivos e impresoras (particiones eco: ICMPv4 de entrada)”

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Hacemos de nuevo los pings anteriores

Imagen que contiene Texto

Descripción generada automáticamente

Imagen que contiene Texto

Descripción generada automáticamente

**Ejercicio 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.

Antes de ello, nos vamos a “Administrador de dispositivos, Ver, Mostrar Dispositivos Ocultos”

***Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente***

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Miramos el TCP

Texto

Descripción generada automáticamente

Ahora el UDP

Texto

Descripción generada automáticamente

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.

***Interfaz de usuario gráfica

Descripción generada automáticamente***

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

El puerto TCP

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

El puerto HTTP que se usa para la comunicación del sistema de cliente a sitio es el puerto 80 y el 443 para HTTPS

***.***

• 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.

Miramos el TCP

******

***Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media***

Ahora el UDP



**Imagen que contiene Texto

Descripción generada automáticamente**

• Crea un fichero que se llame **Practica1\_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



![Texto

Descripción generada automáticamente]()