IES Fernando Aguilar Quignon

2º Administración de Sistemas Informáticos en Red

MPT03. Despliegue de servicios en red

José María Riol Sánchez

8 de marzo de 2023

Índice

Introducción al miniproyecto.

En este documento vamos a plasmar cual es mi idea de proyecto para el MPT03, su esquema de red, herramientas usadas, describir y simular la conexión física de los dispositivos, así como la demostración y explicación de uso de mi idea.

En este trabajo tenemos que plasmar el despliegue de una red explicando lo que hemos usado y cómo lo hemos realizado, así como la generación de un vídeo y unas diapositivas con las que presentar el trabajo el día que sea.

Nosotros hemos pensado en el siguiente escenario:

Tenemos un colegio al que queremos ofrecer un servicio de máquinas virtuales con Proxmox, con el objetivo de dar a los alumnos la posibilidad de poder trabajar en clase sin importar el dispositivo portátil que dispongan. Esto es, los alumnos no necesitarán un gran ordenador pues su portátil lo van a usar para conectarse a la red, logearse en Proxmox con su usuario y tendrá a su disposición una máquina virtual donde poder hacer sus tareas y demás. Por tanto la carga de trabajo caerá sobre el servidor que tengamos montado de Proxmox y no en local.

Más adelante hablaremos con más profundidad sobre cómo está organizado Proxmox para hacer que los alumnos solo tengan acceso a su sistema solamente mientras que los profesores puedan tener acceso a todos, con el objetivo de evitar que los alumnos puedan hacerse bromas entre ellos y los profesores puedan mirar sus pantallas ya sea para controlar lo que hacen o para ayudarles con alguna tarea, corregir algo, ayudarles con alguna actividad, etc...

En cuanto al laboratorio de Kathara, ahí mostraremos como los dispositivos están conectados a la red y como procederían a obtener una IP, etc...

Cabe decir que el laboratorio de Kathara se podrá encontrar en mi **GitHub**, por si se quisiera echar un vistazo a la configuración establecida de forma libre. Además también se añadirá este documento PDF y el vídeo junto con la presentación para tenerlo todo agrupado y accesible en cualquier momento.

1. Herramientas utilizadas para la simulación.

Para poder proceder con nuestro escenario hemos pensado usar un laboratorio de Kathara con el que poder simular la conexión física de los dispositivos y hacernos una idea del posible escenario que tenemos delante, además de realizar la configuración de ciertos protocolos y demostrar que comunicación tendrán entre ellos.

Por otro lado, tendremos el ordenador blanco del instituto en el que tenemos alojado Proxmox. Se accederá a este mediante la IP que tenga configurada y dentro de Proxmox VE haremos las configuraciones necesarias para desplegar la infraestructura de máquinas virtuales que pueda satisfacer las necesidades del Instituto.

Es necesario comentar que estos escenarios son simplificados con la idea de hacer una pequeña demostración, en la realidad es totalmente obvio que el escenario completo es muchísimo más complejo y grande.

Con el fin de demostrar la funcionalidad de esta red no usaremos todos los equipos mostrados en el esquema, solo usaremos lo necesario para demostrar lo suficiente para que el escenario sea explicado y emulado.

Procederemos pues con la explicación en detalle además de mostrar esquemas de red si los hubiera y demás información de utilidad.

2. Nuestro laboratorio de Kathará.

2.1. Esquema del laboratorio.

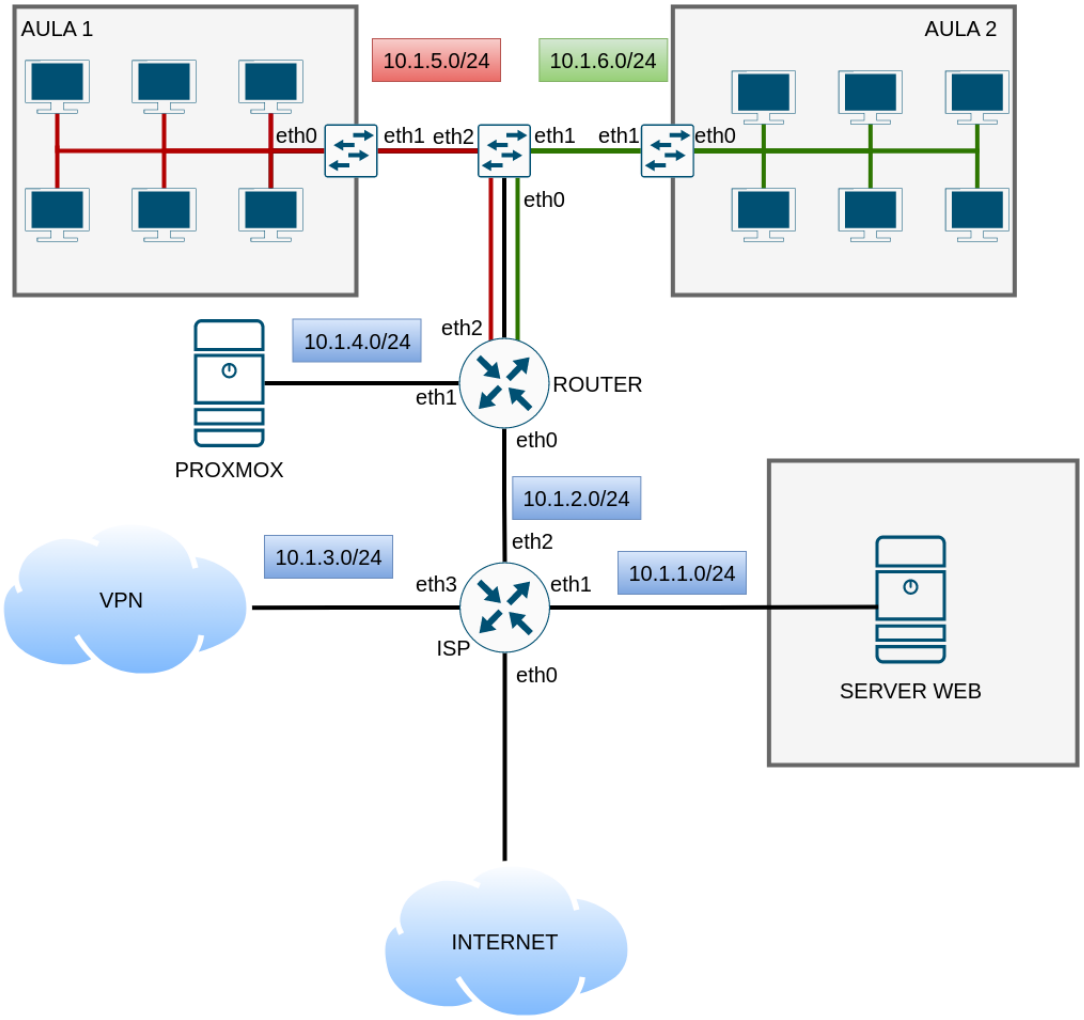

Figura 1: Esquema de la red.

2.1.1. Explicación del esquema.

Nuestra red va a contar con dos Routers, uno que permitirá el acceso al exterior y el otro router interno que se encargará del tráfico interno además del posible tráfico de salida por parte de los equipos de la red interna.

- ISP: Este router es el router externo que además de permitir el acceso al exterior y filtrar los paquetes externos al servidor Web, dispondrá de una VPN para que los alumnos puedan acceder a sus MV desde el exterior por si necesitan seguir trabajando desde casa, al igual que los profesores. Este router contará con **4 interfaces**:
  - eth0 con IP **172.17.0.2** que será la conexión a la WAN permitiendo el tráfico de salida desde la red interna o el tráfico de entrada cuyo destino será el servidor Web del colegio.
  - eth1 con IP **10.1.1.1/24** subred en la que se encontrará el Servidor Web.
  - eth2 con IP **10.1.2.1/24** subred que conectará con el router interno dando paso las respuestas a los paquetes salientes de la red interna.
  - eth3 con IP **10.1.3.1/24** que es la interfaz con la que conectará con la VPN.

- Router: Esté será el router interno de la red que permitirá la conexión del Proxmox con las diferentes aulas divididas en VLANS además de tener los servicios DNS y DHCP. En él encontramos:
    - eth0: con IP **10.1.2.2/24** conecta con el router frontera de la red haciendo posible las conexiones al Proxmox con VPN y que las máquinas de la red interna puedan acceder al exterior y al servidor Web.
    - eth1: con IP **10.1.4.1/24** es la subred que conecta con la máquina Proxmox donde se van a alojar las máquinas virtuales de los alumnos que podrán usar tanto desde las propias aulas como desde sus casas con la VPN.
    - eth2: está conectado al Switch que contiene las VLANS del instituto permitiendo que cada aula sea una subred y todas puedan tener acceso al Prxomox y al exterior, además de al Servidor Web. Las IPS de eth2.10 y eth2.20 son respectivamente **10.1.5.1/24** y **10.1.6.1/24**

Una vez comentado cada uno de los routers de nuestro esquema ya solo nos quedarían los Switches que dividirán las aulas en subredes gracias al uso de las VLANs, siendo cada aula una subred y mediante el uso de interfaces virtuales el router será capaz de comprobar de qué VLAN vienen los paquetes y permitir que todos los posibles dispositivos puedan conectarse al Proxmox desde allí.

La idea de montarlo de esta forma es la siguiente:

Disponemos de un Servidor Web que podrá ser accedido incluso desde el exterior, motivo por el cual lo tenemos situado en la DMZ, para dar servicios al exterior y sobre todo es accesible desde el interior de la red.
Con la VPN daremos acceso al Proxmox desde el exterior también pero sin exponerlo públicamente, si no que con un túnel seguro los alumnos podrán realizar sus conexiones y acceder a los equipos siempre que quieran.
Por otro lado tenemos los equipos de la red interna que se conformarán por los equipos de los alumnos que no tienen por qué ser potentes pues la potencia de cálculo residirá en el Proxmox que tengamos montado. Por tanto los alumnos al conectar por cable sus sistemas a las rosetas de nuestras aulas, el servidor DHCP de nuestro router interno irá asignando direcciones IPs a todos y cada uno de ellos además de resolver los posibles nombres que haya, permitiendo también la conexión al exterior.

3. Despliegue de Proxmox.

Como ya se ha mencionado anteriormente, Proxmox será una computadora de grandísima potencia que albergará las MV de los alumnos. La idea de uso es la siguiente:

Tenemos pensado crear plantillas de diferentes MV con la idea de satisfacer las necesidades de un alumno de ASIR, un alumno de DAW... los cuales tienen necesidades distintas. Es por ello que la máquina virtual de un alumno de ASIR contendrá herramientas, software y una configuración ligeramente distinta a la que tendría una MV de un alumno de DAW. Es por ello que creamos una MV y la configuramos para el uso adecuado de un alumno de ASIR y lo convertimos en una plantilla. A partir de esa plantilla iremos clonando las máquinas para generar nuevas MV según los nuevos alumnos que vayamos teniendo. Si el alumno deja el grado se procedería a borrar la máquina y si el alumno tiene pensado seguir hasta terminar pues tan solo hay que dejar la MV para que el alumno pueda usarla hasta que finalice sus estudios.

Los alumnos solo podrán tener acceso a su máquina virtual sin poder ni siquiera ver las máquinas de los demás alumnos (en el Proxmox). Los profesores en cambio sí podrán ver las MV de todos sus alumnos e incluso entrar en ellas por el motivo que sea, mirar algún ejercicio, ayudarle en algo, corregirle etc... parecido al uso que se hace con el Epoptes. Los profesores contarán también con sus propias MVS. Ni alumnos ni profesores podrán configurar sus máquinas virtuales, solo el administrador de la red podrá modificar las MVs además de poder ver las MVS de todo el mundo, al fin y al cabo es el encargado del sistema y debe tener todo tipo de privilegios, mientras que

profesores y alumnos lo tienen limitado.

4. Servicios proporcionados en nuestra red.

Los servicios que tenemos pensado prestar en nuestra red son los siguientes:

- **VPN**. La Red Privada Virtual permitirá crear un túnel seguro en un canal público/inseguro que permitirá a los alumnos entrar al Proxmox desde sus casas sin exponer los servicios al exterior.
- **DNS**. El DNS permitirá a los equipos de nuestra red poder resolver los nombres de dominio que pueda haber en nuestro sistema además de realizar las consultas DNS en caso de que la consulta deba salir de nuestra red.
- **DHCP**. Los equipos de nuestras aulas necesitarán una dirección IP con la que poder identificarse dentro de la red. De eso se encargará el DHCP que tenemos en el router interno.
- WEB. El Servidor Web alojará una aplicación Web con lo necesario para satisfacer una Web de un Instituto, temas de exámenes, matrículas, notas...

4.1. Configuración de VPN.

Para la VPN hemos pensado usar Wireguard. Para este caso necesitamos instalar en el ISP el Wireguard de la siguiente forma, añadiendo dichas lineas al fichero isp.startup de nuestro laboratorio de Kathara.

```
echo "deb http://deb.debian.org/debian buster-backports main contrib
                non-free»>/etc/apt/sources.list
          apt update && apt install wireguard-tools -y
```

Así al iniciar el laboratorio tendremos preparado Wireguard. El siguiente paso es crear las claves públicas y privadas tanto de la parte cliente como de la parte servidor. Para ello hacemos uso del comando

```
sudo wg genkey | tee NOMBRECLAVEPRIVADA | wg pubkey >NOMBRECLAVEPUBLICA
```

Cuando tengamos el par de claves para cliente y servidor tendremos que crear el fichero wg0.conf, dentro de la carpeta isp de nuestro laboratorio de Kathara en **/etc/wireguard/wg0.conf** y también en los clientes. El contenido del mismo es el siguiente. Por parte del servidor...

```
[Interface]
Address = 10.1.3.2/24
SaveConfig = true
PrivateKey = AFTbOPvkdfzTQISFbuVlI1RFfzCfin5IL9piLjvZU30=
ListenPort = 51820

[Peer]
PublicKey = iKjTqzgyqhj2+0iOKu7aui64veAOwHll27EgMUAxyn8=
AllowedIPs = 10.1.3.3/32
```

Por parte del cliente...

```
[Interface]
PrivateKey = AO4AboejoQSJvJsBMEZ9FrGD4DcITbo246aRXy0C42Y=
Address = 10.1.3.3/24
DNS = 10.1.2.2

[Peer]
PublicKey = SP7/lq7YV2qqOsso4LybS1bCnRdSR4OFXB4TFXMp6gA=
AllowedIPs = 0.0.0.0/0
Endpoint = 172.17.0.2:51820
PersistentKeepalive = 21
```

Siendo las claves públicas intercambiadas, el servidor tendía la clave pública del cliente y el cliente el del servidor.

4.2. Configuración de DNS.

En cuanto a la configuración de DNS, tenemos que añadir en el archivo router.startup las siguientes líneas:

```
apt install dnsmasq -y
/etc/init.d/dnsmasq start
```

De esta forma instalaremos e iniciaremos el servicio de DNS en nuestro router cuando iniciemos el laboratorio de Kathara. Una vez hecho esto, tenemos que pasar a la configuración del dnsmasq, para ello meteremos dentro de la carpeta router del laboratorio de Kathara el fichero dnsmasq.conf **/etc/dnsmasq.d/dnsmasq.conf**, que contendrá la configuración del DNS de nuestra red.

```
#PUERTO, INTERFACES VIRTUALES Y CARGA DE SERVIDORES DNS
port=53
interface=eth2.10
interface=eth2.20
interface=eth1
resolv-file=/etc/dnsmasq.d/listaserv.conf

#RESERVAS

host-record=web.inf.faq, 10.1.1.2
cname=web.faq, web.inf.faq

host-record=proxmox.inf.faq, 10.1.4.2
cname=proxmox.faq, proxmox.inf.faq
```

Aquí indicamos el puerto, las interfaces virtuales que tendrá en cuenta el servidor DNS, que al ser una VLAN pues son varias interfaces virtuales, luego la interfaz física del router y por último pasamos un fichero en el que tendremos los servidores DNS de la jerarquía DNS.

4.3. Configuración de DHCP.

Lo primero es indicar en el archivo.startup del router que se instale DHCP e inicie el servicio de la siguiente forma:

```
apt update
apt install -y isc-dhcp-server -o Dpkg::Options::=-force-confdef"
/etc/init.d/isc-dhcp-server start
```

Para la configuración del DHCP hemos metido en el laboratorio de Kathara dentro de la carpeta de "router" (porque queremos el servidor DHCP en el router interno) el archivo dhcpd.conf que contiene la configuración de nuestro DHCP **etc/dhcp/dhcpd.conf**, para que al cargar el laboratorio cargue la configuración DHCP que queremos que se aplique. La configuración sería la siguiente:

```
#INDICAMOS CADA UNA DE LAS VLAN, SU SUBRED, EL RANGO DE IPs...
subnet 10.1.5.0 netmask 255.255.255.0 {
    range 10.1.5.5 10.1.5.253;
    option subnet-mask 255.255.255.0;
    option routers 10.1.5.1;
    option domain-name-servers 10.1.5.1;
}
subnet 10.1.6.0 netmask 255.255.255.0 {
    range 10.1.6.5 10.1.6.253;
    option subnet-mask 255.255.255.0;
    option routers 10.1.6.1;
    option domain-name-servers 10.1.6.1;
}
```

De esta forma las máquinas que pertenezcan a las distintas VLANS tendrán una ip cuando se conecten a nuestra red.

4.4. Configuración de WEB.

En realidad para el servicio WEB no hay demasiada configuración para este escenario de prueba, la idea es en el archivo web.startup poner las siguientes líneas:

```
apt update
apt install apache2 -y
/etc/init.d/apache2 start
```

Con esto habilitamos el servidor Apache2 en el cual alojaríamos nuestra aplicación web con la que ofrecer los servicios del colegio, ya sea mostrar notas, matriculación, etc...

5. Log de cabezazos.

Mala configuración de Switch

Me pasé buena parte del tiempo buscando el motivo por el que el DHCP no funcionaba, esto es, los usuarios no obtenían una IP de forma automática ni nada. Después de echarle tiempo a la configuración del DHCP (destripe: para nada) me di cuenta que la configuración del DHCP no era el problema, estaba todo bien y correcto, el problema fue que había en el fichero swlan.startup una línea mal puesta, entonces ese switch no estaba funcionando realmente.

¿Cómo nos dimos cuenta? La forma fue proceder a seccionar el problema, esto es, limitar el escenario para saber dónde puede estar el problema y esto lo hicimos dándole una IP estática al pc2 e intentamos hacer ping al router interno. Al ver que no comunicaban pensamos que el error estaba entonces a nivel de capa de enlace, en los switchs y efectivamente. Una vez solucionado la línea errónea del switch se podía hacer ping al router interno y al reiniciar el laboratorio recibía la IP de forma automática por fin.

Mala configuración del archivo dnsmasq.conf

Este error se debió a que escribí mal las interfaces virtuales que tenía que tener en cuenta el DNS para ofrecer sus servicios. Como las interfaces virtuales estaban mal escritas, el DNS no resolvía los nombres de ninguna forma. Una vez arreglado el problema y haber escrito un dominio totalmente ficticio tanto para el servidor web como para proxmox ya podíamos hacer ping de la siguiente forma:

```
ping proxmox.faq
ping web.faq
```

Mala configuración del wireguard

Tenía mal puestas las claves públicas, dando un error de claves cuando levantaba el cliente y trataba de hacer ping. Además tenía mal la máscara del AllowedIPs que es /32 y yo tenía /24.