



4.3.- SDN VLAN.

¿Qué es una VLAN?

Dirección Origen	Dirección Destino	Tipo de trama	Datos (46-1500)	Frame Check Sequence (FCS/CRC)
------------------	-------------------	---------------	-----------------	--------------------------------

Trama Ethernet

[Eduardo Taboada \(Tecnocratica.net\)](#) Trama Ethernet. Capa 2 de TCP/IP (Todos los derechos reservados)

VLAN o también conocidas como **redes de área local virtuales**, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física, es decir, sobre una mismo dominio de broadcast (LAN) segmentaremos la red física en redes virtuales y esto lo lograremos poniendo una "Tag" etiqueta dentro de la trama Ethernet indicando el número de VLAN asignada (0 a 4096, es decir 12 bits)

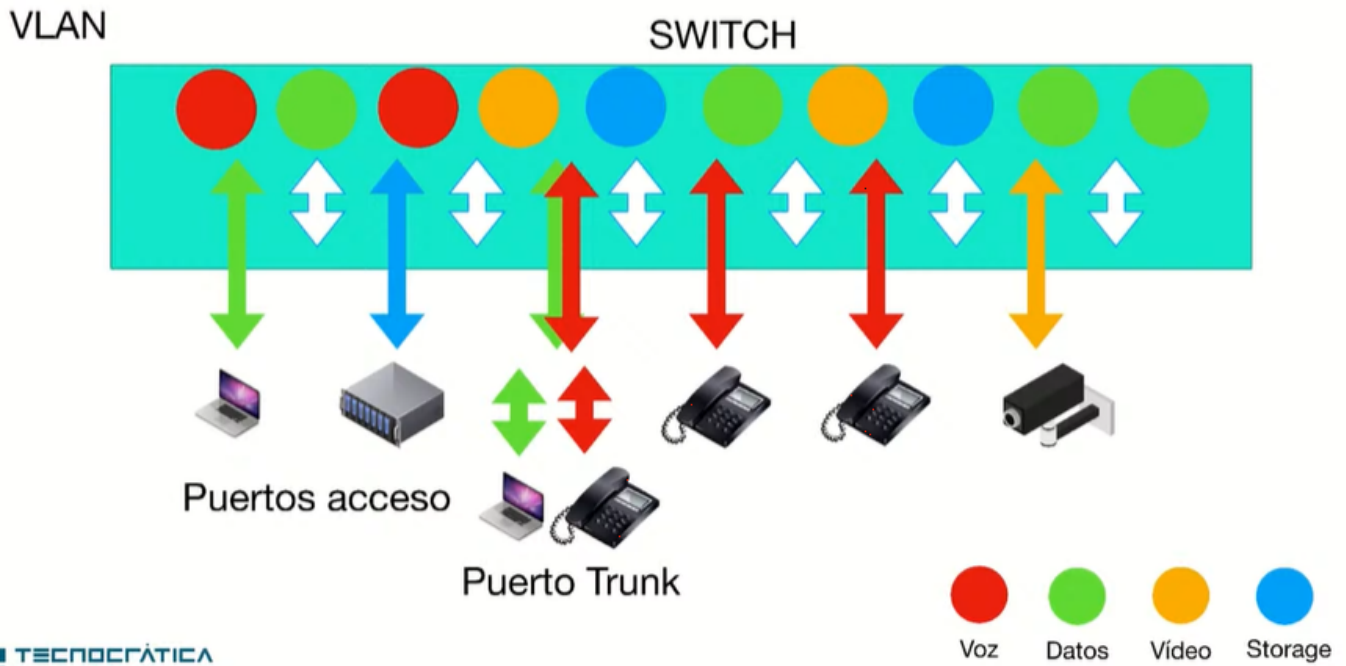
Las VLAN nos permite crear redes lógicamente independientes, por tanto, podemos aislarlas para que solamente tengan conexión a Internet, y denegar el tráfico de una VLAN a otra. Por defecto no se permite a las VLANs intercambiar tráfico con otra VLAN, es totalmente necesario ascender a nivel de red (Capa 3 de TCP/IP) con un router o un switch multicapa, con el objetivo de activar el inter-vlan routing, es decir, el enrutamiento entre VLANs para sí permitir la comunicación entre ellas siempre que lo necesitemos.

Tengamos en cuenta que la Capa 2 de Ethernet está preparada para detectar colisiones en el medio de transmisión y para ello necesita una longitud de trama de datos (o MTU) mínima de 46 bytes y un máximo de 1500 más los encabezados y el CRC para que sean compatibles con la mayoría de los switch comerciales.

Es evidente que cuanto mayor sea el campo de datos de las tramas (MTU) mayor será el rendimiento pero cuidado con superar el MTU de 1500, porque muchos fabricantes de switch



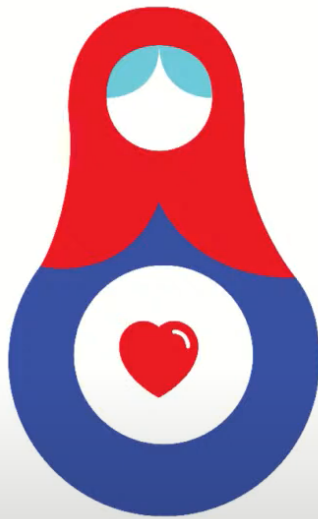
comerciales no lo soportan.



Voz Datos Video Storage

Eduardo Taboada (Tecnocratica.net) Puertos de acceso y puertos Trunk para una VLAN (Todos los derechos reservados)

Para conectar un interfaz de red a una VLAN lo realizaremos a través de los "puertos de acceso" para ello debemos configurar la interfaz de red con el número de "Tag" de la VLAN que le corresponda y así el switch sabrá dividir el tráfico de red entre las distintas VLAN. Cuando en un mismo enlace queremos conectar varias VLAN del switch al host, necesitaremos hacerlo mediante un "puerto Trunk", para ello debemos habilitar en el switch el soporte a varias VLAN por el mismo puerto de salida.



Dirección Origen	Dirección Destino	Tipo de trama	Datos (46-1500)	Frame Check Sequence (FCS/CRC)
------------------	-------------------	---------------	-----------------	--------------------------------

Trama Ethernet

Dirección Origen	Dirección Destino	Tag	Tipo de trama	Datos (46-1500)	Frame Check Sequence (FCS/CRC)
------------------	-------------------	-----	---------------	-----------------	--------------------------------

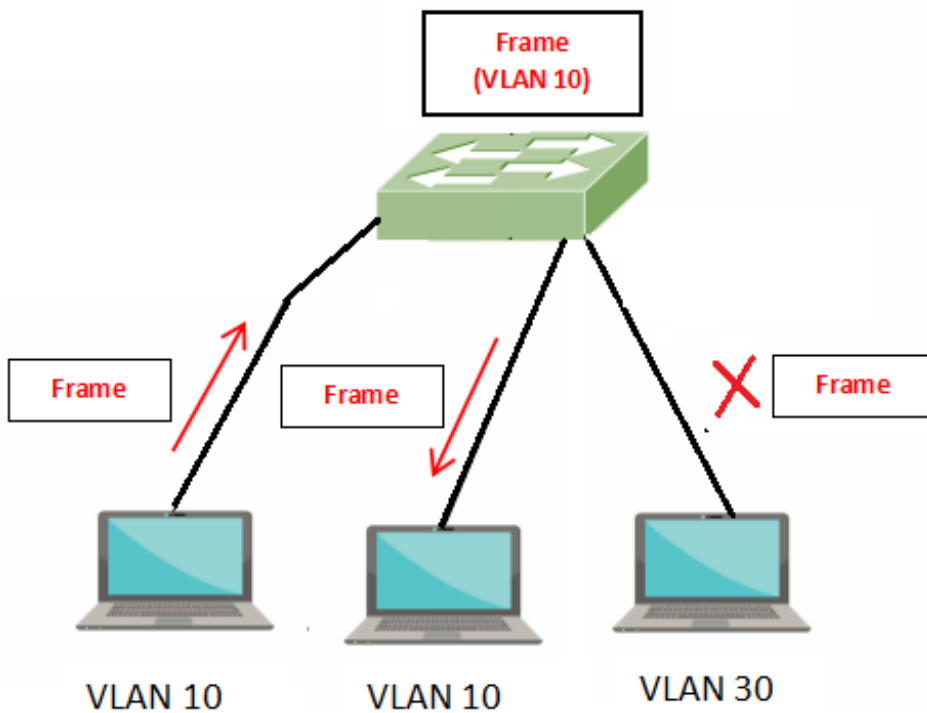
Trama Ethernet con VLAN (voz)



Eduardo Taboada (Tecnocratica.net) Esquema de trama Ethernet VLAN (Todos los derechos reservados)

Si queremos tener plena compatibilidad con todos los switch comerciales debemos reducir el tamaño MTU de 1500 para no tener problemas al haber agregado el "Tag" de la VLAN.

VLAN





Implementación de una SDN VLAN entre las MV y contenedores de dos nodos Proxmox

Cuando las máquinas virtuales de diferentes nodos necesitan comunicarse a través de una **red aislada**, la zona VLAN permite el aislamiento a nivel de red mediante etiquetas VLAN.

1º. Crea una Zona VLAN (recordar que las SDN se configuran a nivel de Centro de datos:

SDN	Nodo	Estado
localnet...	vm-prox...	ok
ZonaVL...	vm-prox...	pending

Registro del cluster					
Hora de inicio ↓	Hora final	Nodo	Nombre de usuario	Descripción	Estado
May 09 12:52:36	May 09 12:52:42	vm-proxm...	root@pam	SRV networking - Recargar	OK
May 09 12:52:33	May 09 12:52:42	vm-proxm...	root@pam	reloadnetworkall	OK

Imagen de elaboración propia: *Crear una VLAN* ([CC BY-NC-SA](#))

Llamaremos a la Zona como "ZonaVLAN" y la conectaremos al Bridge "vibr0":



Agregar: VLAN

ID:

Bridge:

MTU:

Nodos:

IPAM:

Servidor de DNS:

Servidor de DNS inverso:

Zona de DNS:

Avanzado

Imagen de elaboración propia: Creación de la Zona SDN del tipo VLAN (CC BY-NC-SA)

Crema una VNet denominada "SwVLAN10" con la etiqueta VLAN 10 en la Zona creada anteriormente:

Centro de datos

Permisos

- Usuarios
- Tokens de API
- Dos factores
- Grupos
- Conjuntos
- Roles
- Dominios
- HA
- SDN
- Zonas
- VNETs**
- Opciones
- IPAM
- ACME

VNETs

ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
------	-------	------	----------	-----------	--------

Crear: VNet

Nombre:

Alias:

Zona:

Etiqueta:

Consciente de VLAN:

Imagen de elaboración propia: Creación de la VNet "SwVLAN10" (CC BY-NC-SA)

Aplica la configuración a través del panel principal de SDN:

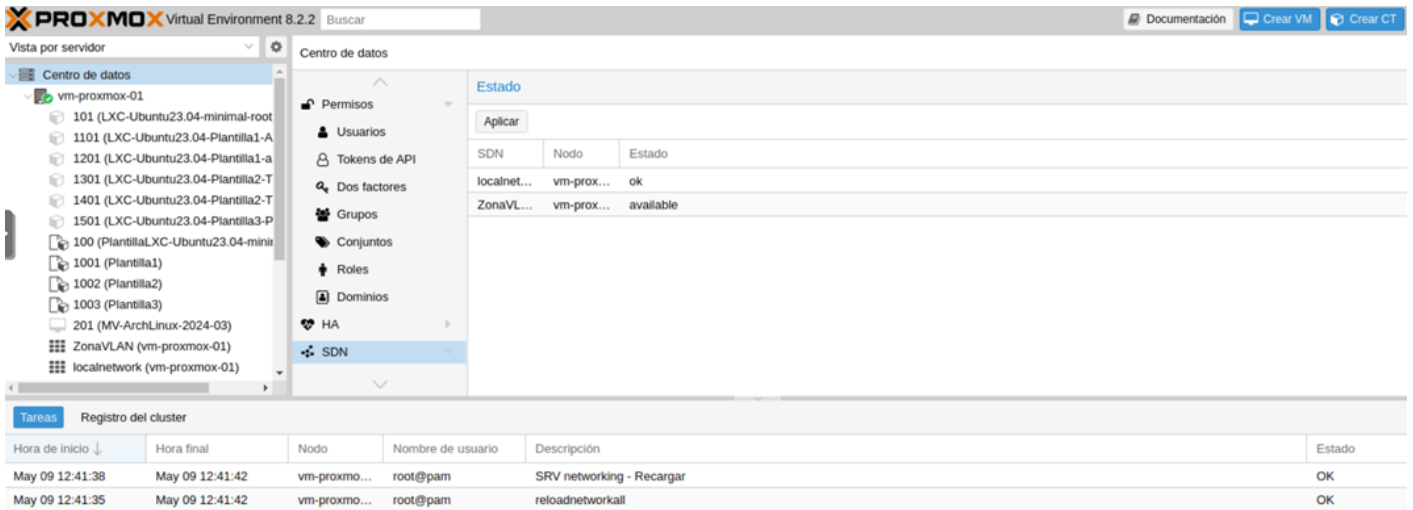


Imagen de elaboración propia: *Aplicar cambios en las SDN* (CC BY-NC-SA)

Crearemos otra VNet llamada "SwVLAN30" para comprobar que el tráfico de red se encuentra aislado entre distintas VLAN:

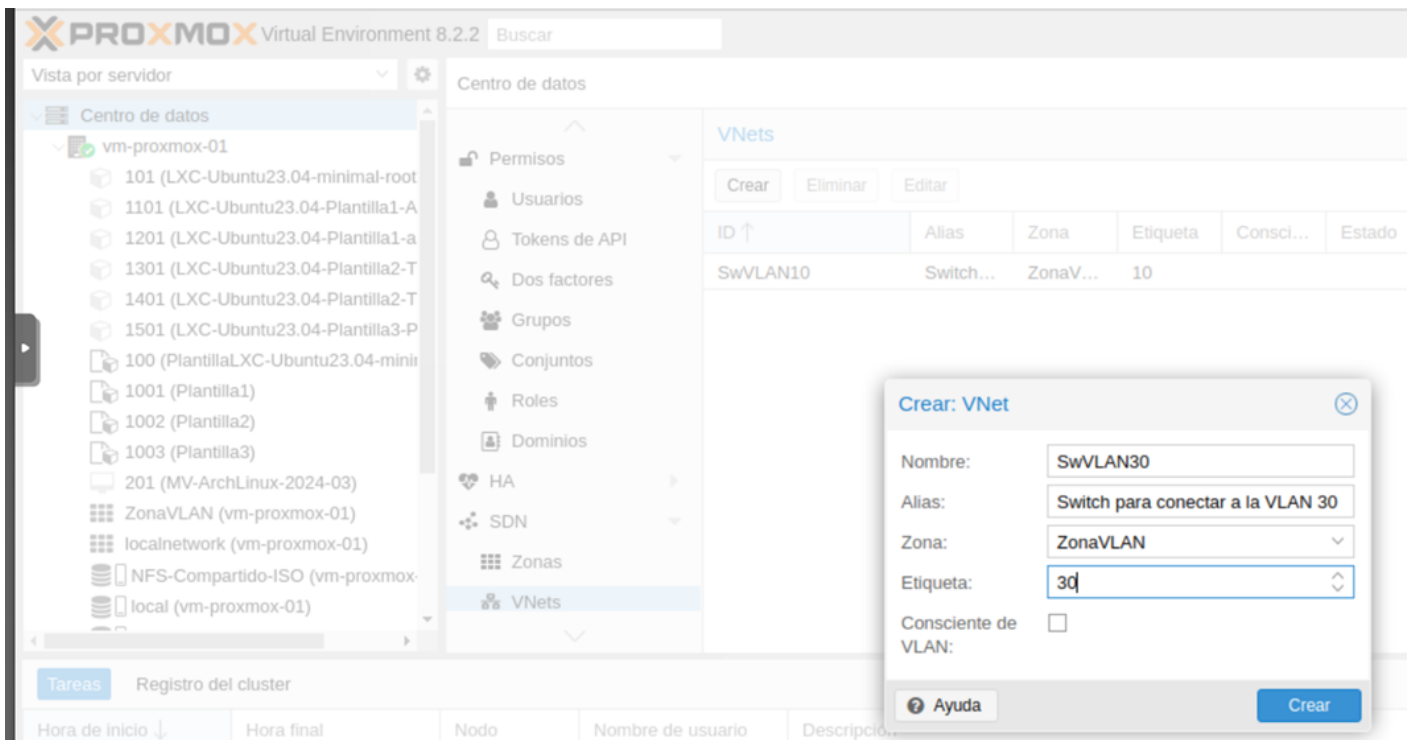


Imagen de elaboración propia: *Creación de otro Switch virtual para hacer otra VLAN distinta a la anterior* (CC BY-NC-SA)

Aplicamos nuevamente los cambios en la SDN.

Repetiremos el proceso en otro nodo Proxmox:

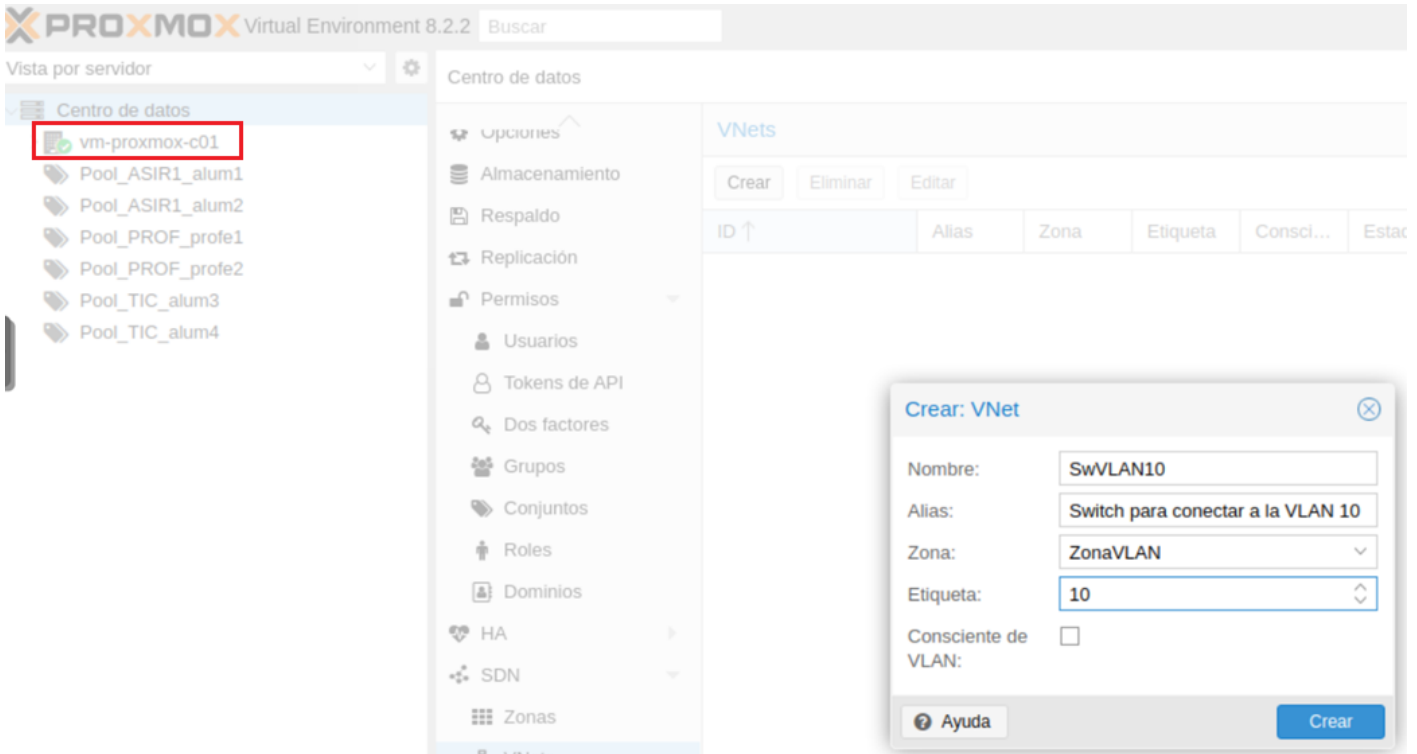


Imagen de elaboración propia: Repetir el proceso de creación de la Zona VLAN y VNet en otro nodo de Proxmox distinto al anterior (CC BY-NC-SA)

Aplicamos cambios en el SDN de nuevo nodo Proxmox:

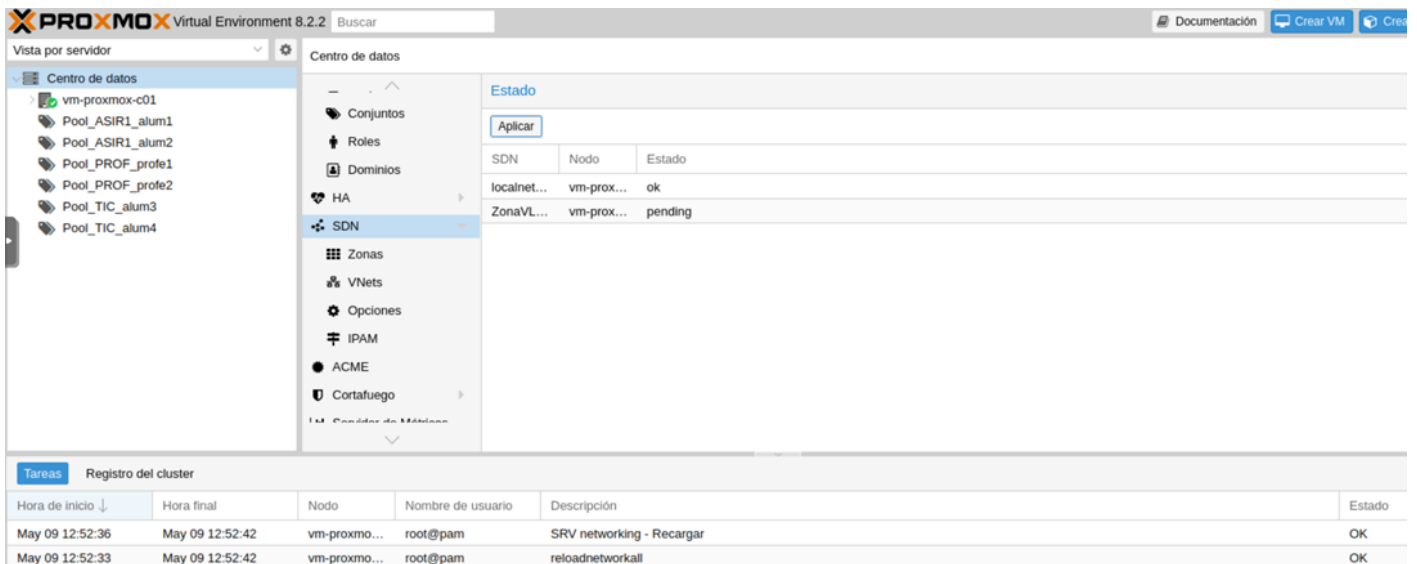


Imagen de elaboración propia: Aplicar cambios en el SDN (CC BY-NC-SA)



Creamos contenedores para hacer las pruebas y le asignamos la IP de forma estática, ya que Proxmox no nos facilita un servidor DHCP para Zonas del tipo VLAN. Configuraremos un contenedor en cada nodo de Proxmox y asociaremos su interfaz de red a la VNet "SwVLAN10":

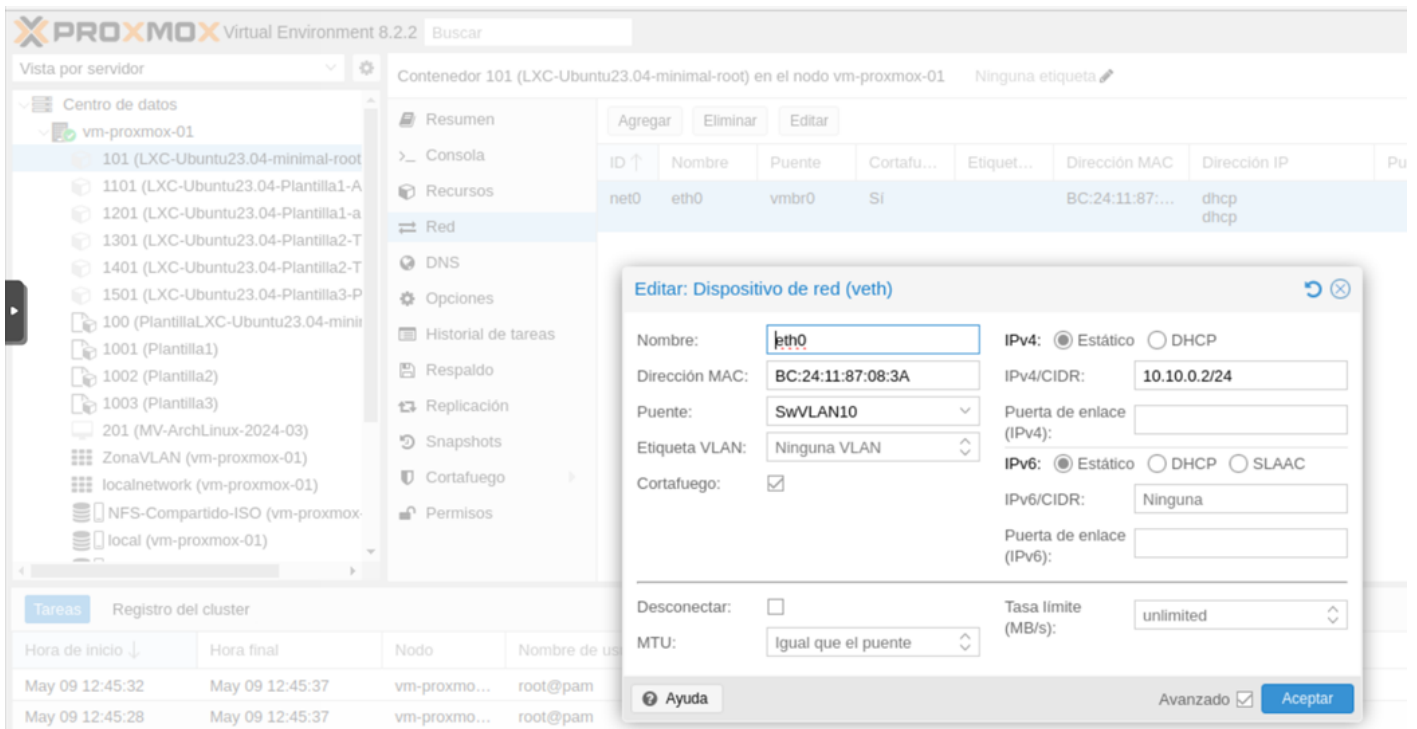


Imagen de elaboración propia: *Asignación de IP estáticas y conexión a la VNet "SwVLAN" de los contenedores* (CC BY-NC-SA)

Haremos otro contenedor y le asociaremos su interfaz de red al "SwVLAN30"

Comprobaremos el resultado haciendo ping entre los contenedores de la mismo VLAN 10:



```
root@LXC-Ubuntu23:~# ping 10.10.0.2
PING 10.10.0.2 (10.10.0.2) 56(84) bytes of data:
64 bytes from 10.10.0.2: icmp_seq=1 ttl=64 time=3.07 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=64 time=0.964 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=64 time=1.13 ms
64 bytes from 10.10.0.2: icmp_seq=5 ttl=64 time=0.987 ms
^C
--- 10.10.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.964/1.439/3.066/0.815 ms
root@LXC-Ubuntu23:~#
```

```
PING 10.10.0.22 (10.10.0.22) 56(84) bytes of data:
64 bytes from 10.10.0.22: icmp_seq=1 ttl=64 time=5.90 ms
64 bytes from 10.10.0.22: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 10.10.0.22: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.10.0.22: icmp_seq=4 ttl=64 time=1.11 ms
64 bytes from 10.10.0.22: icmp_seq=5 ttl=64 time=1.04 ms
64 bytes from 10.10.0.22: icmp_seq=6 ttl=64 time=1.14 ms
^C
--- 10.10.0.22 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.035/1.898/5.900/1.789 ms
root@LXC-Ubuntu23-VLAN10:~#
```

Imagen de elaboración propia: *Comprobación de la interconexión de 2 contenedores en la misma VLAN pero en distintos nodos Proxmox* (CC BY-NC-SA)

Ahora configuraremos la IP estática del tercer contenedor pero estará conectado a la VLAN 30:



Contenedor 1602 (LXC-Ubuntu23-VLAN30) en el nodo vm-proxmox-01

ID ↑	Nombre	Puente	Cortafu...	Etiquet...	Dirección MAC	Dirección IP
net0	eth0	SwVLAN...	Si		BC:24:11:1B:...	10.10.0.2/24

Editar: Dispositivo de red (veth)

Nombre: IPv4: Estático DHCP

Dirección MAC: IPv4/CIDR:

Puente: Puerta de enlace (IPv4):

Etiqueta VLAN: IPv6: Estático DHCP SLAAC

Cortafuego: IPv6/CIDR:

Desconectar: Puerta de enlace (IPv6):

MTU: Tasa límite (MB/s):

Avanzado

Imagen de elaboración propia: Configuración del tercer contenedor conectado a la VLAN30 (CC BY-NC-SA)

Podemos observar como el contenedor en la VLAN30 se encuentra aislado del tráfico de red de los contenedores que se encuentran el VLAN10:

Contenedor 101 (LXC-Ubuntu23.04-NodoC01-01) en el nodo vm-proxmox-c01

```

root@LXC-Ubuntu23:~# ping 10.10.0.2
PING 10.10.0.2 (10.10.0.2) 56(84) bytes of data:
64 bytes from 10.10.0.2: icmp_seq=1 ttl=64 time=3.07 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=64 time=0.964 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=64 time=1.13 ms
64 bytes from 10.10.0.2: icmp_seq=5 ttl=64 time=0.987 ms
^C
--- 10.10.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.964/1.439/3.066/0.815 ms
root@LXC-Ubuntu23:~#

```

Contenedor 1602 (LXC-Ubuntu23-VLAN30) en el nodo vm-proxmox-01

```

root@LXC-Ubuntu23-VLAN30:~# ping 10.10.0.2
ping: connect: Network is unreachable
root@LXC-Ubuntu23-VLAN30:~# ping 10.10.0.2
ping: connect: Network is unreachable
root@LXC-Ubuntu23-VLAN30:~#

```



Salida a Internet de los contenedores

Supongamos que ahora queremos tener acceso a Internet en algún contenedor. Para ello tendremos que hacer una nueva Zona SDN Simple.

¡ATENCIÓN! esto solo funciona con la configuración de red del nodo Proxmox con Linux Bridge. No funciona para la versión de Proxmox actual (8.2.2) con OVS Bridge.

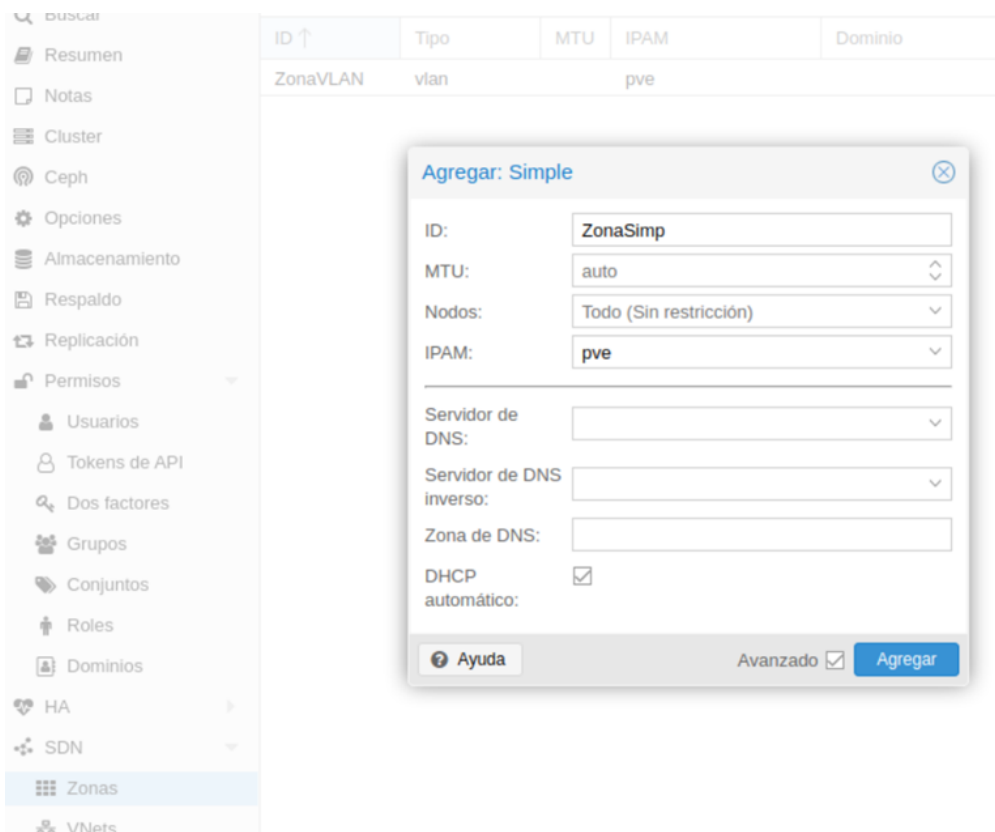


Imagen de elaboración propia: *Creación de una Zona Simple para proporcionar acceso hacia fuera de Proxmox a los contenedores y MV* ([CC BY-NC-SA](#))



The screenshot shows the Proxmox VE interface. On the left is a sidebar with a tree view of resources under 'Centro de datos' and 'vm-proxmox-01'. A central menu contains options like 'Buscar', 'Resumen', 'Notas', 'Cluster', 'Ceph', 'Opciones', 'Almacenamiento', 'Respaldo', 'Replicación', 'Permisos', 'Usuarios', 'Tokens de API', 'Dos factores', 'Grupos', and 'Conjuntos'. The main area displays a table of VNETs:

ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
SwVLAN10	Switch...	ZonaV...	10		
SwVLAN30	Switch...	ZonaV...	30		

A 'Crear: VNet' dialog box is open, with the following fields:

- Nombre: SwSALIDA
- Alias: Switch para tener acceso a Internet
- Zona: ZonaSimp
- Etiqueta: (empty)
- Consciente de VLAN:

Buttons for 'Ayuda' and 'Crear' are at the bottom of the dialog.

Imagen de elaboración propia: Creación de la VNet "SwSALIDA" para proporcionar salida hacia Internet (CC BY-NC-SA)

The screenshot shows the Proxmox VE interface. The VNET table now includes 'SwSALIDA':

ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
SwSALIDA	Switch...	ZonaSi...			new
SwVLAN10	Switch...	ZonaV...	10		
SwVLAN30	Switch...	ZonaV...	30		

A 'Crear: Subred' dialog box is open, with the 'Rangos de DHCP' tab selected. The fields are:

- Subred: 10.0.0.0/24
- Puerta de enlace: 10.0.0.1
- SNAT:
- Prefijo de zona de DNS: (empty)

A 'Crear' button is at the bottom right of the dialog.

Imagen de elaboración propia: Configuración de la Subnet para proporcionar IP por DHCP y hacer SNAT (CC BY-NC-SA)



ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
SwSALIDA	Switch...	ZonaSi...			new
SwVLAN10	Switch...	ZonaV...	10		
SwVLAN30	Switch...	ZonaV...	30		

Editar: Subred

General **Rangos de DHCP**

Dirección de inicio	Dirección final	
10.0.0.2	10.0.0.100	

Agregar

Aceptar

Imagen de elaboración propia. *Configuración del DHCP* ([CC BY-NC-SA](#))

Actualizamos los cambios en la SDN.

Añadimos una nueva interfaz de red al contenedor que queremos que tenga acceso a Internet mediante Source NAT:

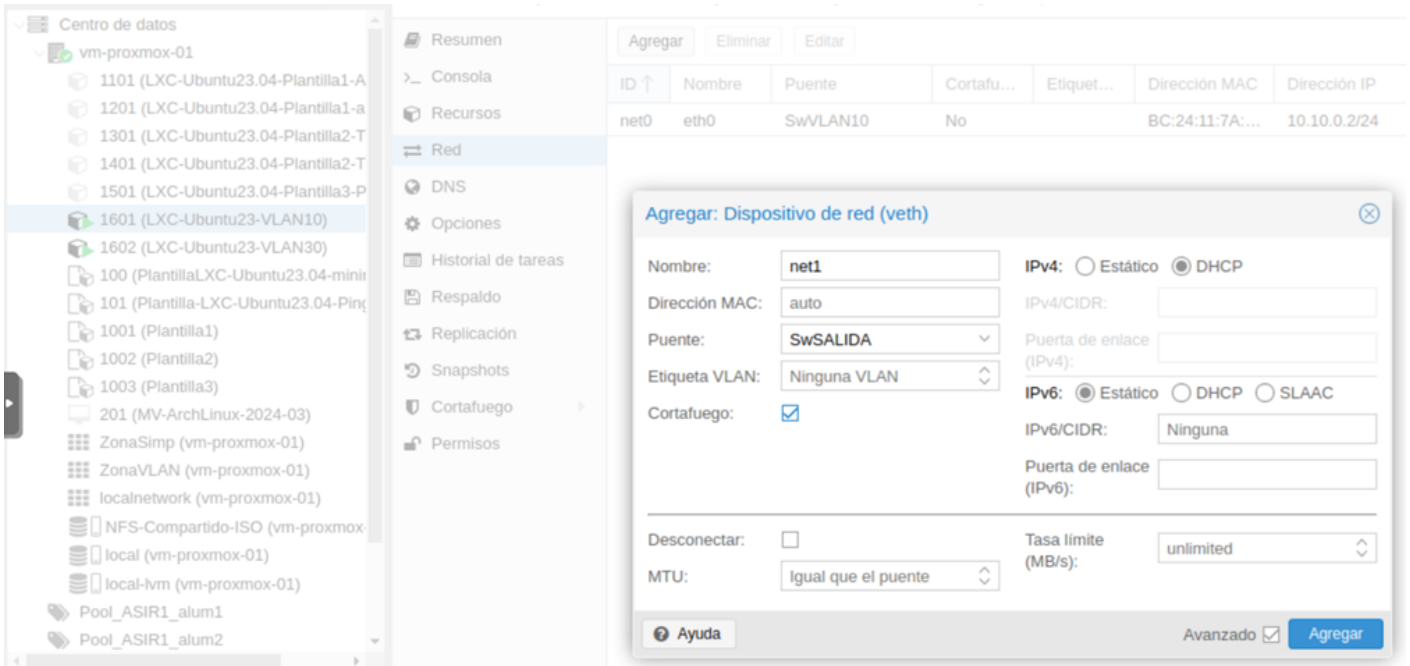


Imagen de elaboración propia: Conexión una nueva interfaz de red al "SwSALIDA" (CC BY-NC-SA)

Reiniciamos el contenedor para una correcta instalación de la tabla de enrutamiento y comprobamos las conexiones haciendo ping tanto a la zona VLAN y a google.es:

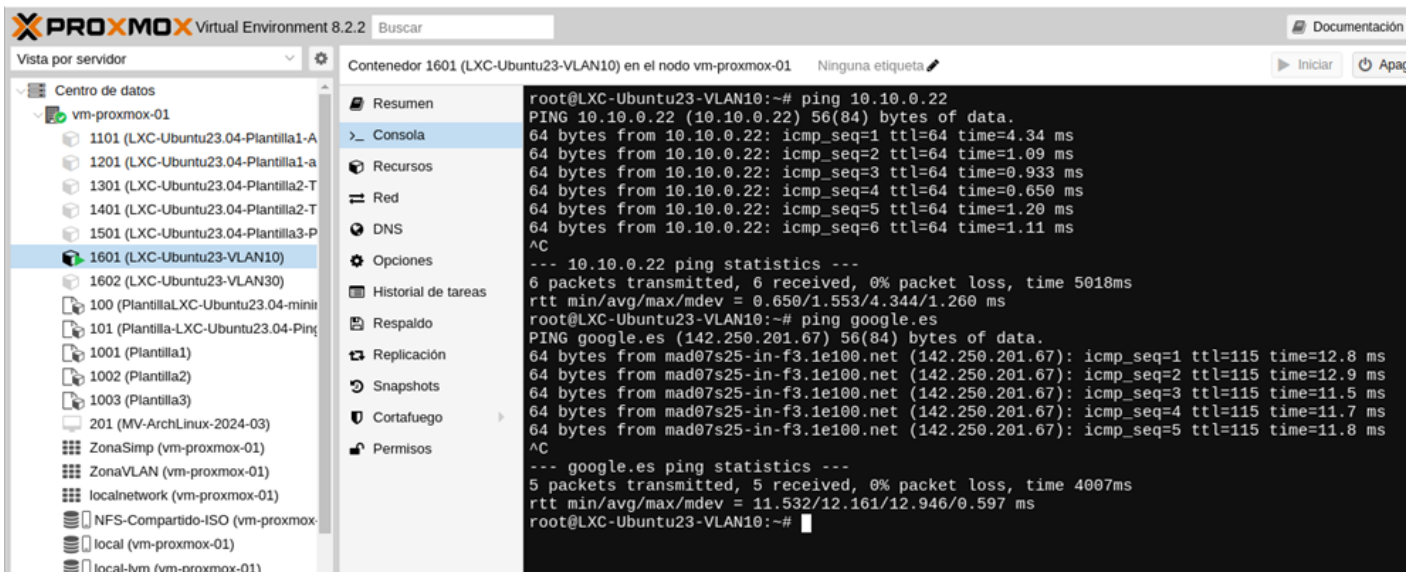


Imagen de elaboración propia: Ping al otro contenedor en la misma VLAN10 y ping a google.es (CC BY-NC-SA)

Revisión #1

Creado 11 mayo 2024 15:01:04 por Daniel Cano Verdú

Actualizado 12 mayo 2024 16:53:02 por Daniel Cano Verdú