SERVIDOR STREAMING EN PYMES usando técnicas de virtualización en entornos libres:

LINUX CONTAINERS

GRADO MULTIMEDIA
Área ingeniería

Autor: Juan Carrillo Foronda

Consultor: David Alcubierre Arenillas
Profesor: César Pablo Córcoles Briongos

Por qué este proyecto?

- *Diseño de redes.*
- *Software libre frente a privativo.*
- *Virtualización.*
- *Implementación servidores.*
- *Automatización tareas.*
- *Seguridad perimetral. Firewall*

Virtualización : ventajas

- *Ahorro energía , optimización hardware*
- *Seguridad, servicios separados, backups*
- *Protección contra errores hardware*
- *Flexibilidad y agilidad. Cubrir necesidades a demanda*
- *Portabilidad y migración rápida. Configuracion en ficheros de texto.*

Software Libre

Implantación software libre

- *Bajo coste económico*
- *Libertad de uso*
- *Adaptarlo a nuestras necesidades*
- *Soporte y compatibilidad a largo plazo*
- *Formatos estándar*
- *Seguridad. Acceso código fuente*

Virtualización : ventajas

- *Ahorro energía , optimización hardware*
- *Seguridad, servicios separados, backups*
- *Protección contra errores hardware*
- *Flexibilidad y agilidad. Cubrir necesidades a demanda*
- *Portabilidad y migración rápida. Configuracion en ficheros de texto.*

Entorno de virtualización

- Servidor físico Dell Poweredge
- Servidores virtuales Linux containers
- Segmentación red.
- Seguridad en firewall. Iptables
- Servidor ftp interno
- Servidor web , página corporativa empresa.
- Servidor streaming

DISEÑO RED
Simulación

- VM LXC
  - Server Web
  - Server ftp
  - Firewall
  - Server streaming
- SERVIDOR FÍSICO
  - 2 Ethernet físicas
  - Ip alias
- Red RRHH
  - 172.16.0.224
  - 255.255.255.224
- Red dirección
  - 172.16.0.128
  - 255.255.255.192
- Red Ventas
  - 172.16.0.64
  - 255.255.255.192
- Red Compras
  - 172.16.0.0
  - 255.255.255.192

HARDWARE

- *Servidor para rack Dell PowerEdge R730*
- *Intel Xeon E5 2600 v3*
- *64Gb Ram ECC*
- *SSD 256GB x 2 en RAID 1*
- *HDD 2T 24x7 x 4*

SOFTWARE

- *S.O Ubuntu Server 14.04*
- *Servidor web (Apache2)*
- *Servidor ftp (vsftpd)*
- *Seguridad (iptables)*
- *Servidor Icecast 2*

SERVIDOR FÍSICO

Entornos de virtualización

- *VIRTUALIZACIÓN COMPLETA*
- *PARAVIRTUALIZACIÓN*
- *VIRTUALIZACIÓN a nivel SISTEMA OPERATIVO*

Tipos de virtualización

Virtualización completa

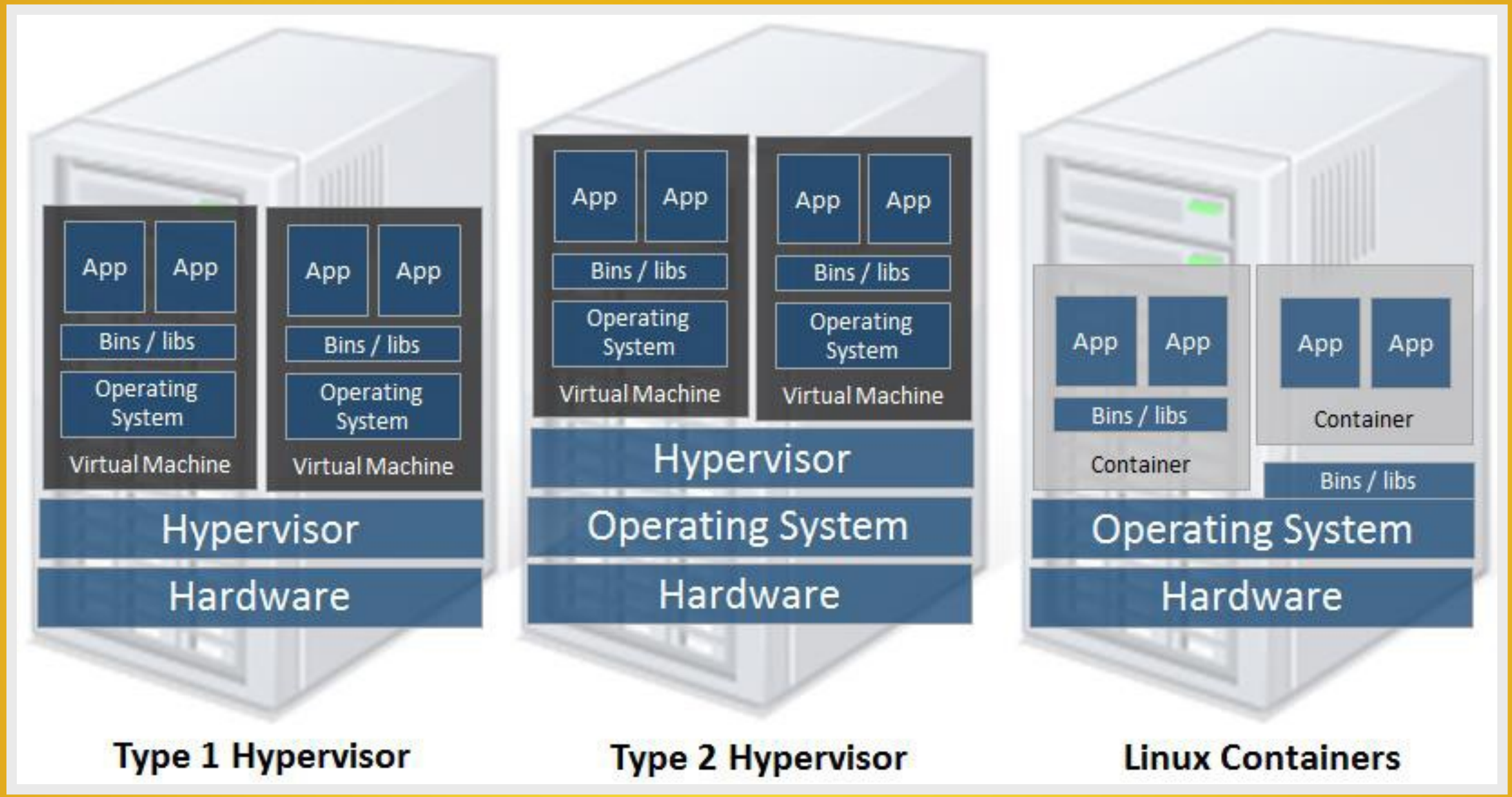
- *Hypervisor*
- *Intermediario Hw-S.O VM*
- *3 capas: Hardware, hypervisor e instancia S.O*
- *Alto Consumo de recursos*
- *NO modifica S.O virtuales*
- *VMWARE -VIRTUALBOX*

Paravirtualización

- *Hypervisor pero se introduce código consciente de la virtualización a los S.O*
- *Todo el sistema trabaja en una sola unidad*
- *Necesita modificar S.O*
- *XEN-UML*

Virtualización Sist. Operativo

- *No requiere hypervisor*
- *S.O hace de hypervisor*
- *Se aíslan servidores unos de otros*
- *Cada uno es una especie de Instancia diferente del espacio de usuario*
- *Rendimiento muy alto*
- *Cambios en kernel S.O*
- *Linux Containers-Openvz*



Type 1 Hypervisor **Type 2 Hypervisor** **Linux Containers**

Linux Containers : LXC

Características Básicas

Características básicas

Método de virtualización a nivel de sistema operativo.

Entornos virtuales denominados CONTENEDORES.

Modificación del kernel de Linux y un conjunto de herramientas en el espacio del usuario.

Comparte el kernel con cada una de las instancias.

Las apps/sistemas se ejecutan dentro de un contenedor usando los recursos asignados a ese contenedor.

Fácil acceso a los archivos en ambos sentidos.

Limitación: Debe de ejecutarse contenedores sobre que soporten el mismo kernel.

Funciona aprovechando dos características muy importantes del nucleo de Linux: CGROUPS y NAMESPACES

USOS y VENTAJAS

- *Actualizar o mover servidores rápidamente.*
- *Distribuir cargas de trabajo sin ataduras de hardware.*
- *Probar cambios mediante clones o snapshots.*
- *No hay tiempos de inactividad*
- *Copias rápidas y seguras de trabajos. Backups fáciles*
- *Movilidad en la nube con poco esfuerzo*
- *Facilidad de realizar pruebas con diferentes versiones de aplicaciones*

CGROUPS y NAMESPACES

CGROUPS

- *Sirven para medir y limitar el uso de los recursos para un grupo de procesos.*
- *Permite controlar CPU, RAM, HDD …de un grupo de procesos.*
- *Cada contenedor tiene su cgroup al que pertenecen los procesos del contenedor*
- *Se organizan jerárquicamente*

NAMESPACES

- *Proporcionan y garantizan aislamiento entre los procesos*
- *Permite aislar a un identificador de una serie de recursos del resto de sistema*
- *Particionan estructuras esenciales del kernel para crear entornos virtuales*
- *Permite usarlos de forma independiente.*
- *Diferentes tipos de namespaces: PID,NET,MNT,USER,UTS,IPC*

Ambos características nativas del kernel

CONFIGURACIÓN GLOBAL

CONFIGURACIÓN GLOBAL

RUTA : /etc/lxc

- *lxc.conf : ajustes lxc, path, cgroups, backend*
- *default.conf : configuración contenedor*
- *lxc.usernet.conf : usuarios sin privilegios*
- *Configuración básica /etc/lxc/default.conf*

CONFIGURACIÓN GENERAL Sistema

RUTA : /etc/lxc/lxc.conf

- *Configuración del path*
- *LVM*
- *ZFS*

Ubicación del Contenedor	/var/lib/nom_contenedor
Configuración de cada contenedor	/var/lib/nom_contenedor/config
Sistema raíz contenedor	/var/lib/nom_contenedor/rootfs
Archivo fstab de los contenedores individuales	/var/lib/lxc/nom_contenedor/fstab
Diversas variables ,como un directorio lxc alternativo	/etc/lxc/lxc.conf
lxc.network por defecto y los ajustes utilizados al crear contenedores	/etc/lxc/default.conf
Configurar Dnsmasq para asignar direcciones IP estáticas a los contenedores	/etc/lxc/dnsmasq.conf
Define si por defecto lxc bridge se utiliza	/etc/default/lxc
Iniciar automáticamente contenedores LXC según ajustes de los contenedores individuales.	/etc/init.d/lxc
Comienza el puente de red lxcbr0 defecto	/etc/init.d/lxc-net
Donde se almacenan las plantillas de SO contenedor	/usr/share/lxc/templates
Donde las diversas configuraciones de contenedores por defecto	/usr/share/lxc/config
Donde cgroup está montado	/etc/fstab

Tipos de almacenamiento

Lxc soporta varios backends para los sistemas de archivos raíz de contenedores.

Sistemas soportados :Overlays, BTRFS, LVM y ZFS

Acciones contenedores

- *Crearlos*
- *Iniciarlos*
- *Snapshots*
- *Congelarlos*
- *Pararlos*
- *Eliminarlos*

Acceso contenedores

- *Consola*
- *Prompt*
- *ssh*

Información contenedores

- *Listarlos*
- *Información*
- *Estado*

Tipos de almacenamiento

Lxc soporta varios backends para los sistemas de archivos raíz de contenedores.

Sistemas soportados :Overlays, BTRFS, LVM y ZFS

Instalar	Confirmar	Crear contenedores	Listar contenedores	Iniciar contenedores
apt-get install lxc	lxc-checkconfig	lxc-create –n nom –t template	lxc-ls -f	lxc-start –n nom -d
Snapshots contenedores	**Listar Snapshot contenedores**	**Deshacer Snapshot**	**Restaurar Snapshot**	**Acceso consola**
lxc-snapshot –n nom -c	lxc-snapshot –n nom -LC	lxc-snapshot -n -r	lxc-snapshot -n nom -r	lxc-console -n nom
Acceso Prompt	**Acceso SSH**	**Parar contenedores**	**Info contenedores**	**Estado contenedores**
lxc-attach -n nom	ssh user@ip	lxc-stop -n nom	lxc-info –n nom	lxc-monitor -n nom
Congelar contenedores	**Eliminar contenedores**	**Clonar contenedores**		
lxc-freeze -n nom lxc-unfreeze -n nom	lxc-destroy -n nom	lxc-clone –o -n nom		

Configuración interfaces

Posibles tipos de interfaces:

- *EMPTY*
- *VETH*
- *PHYS*
- *MACVLAN*
- *VLAN*

MODO Empty

- *Modo empty:*
- *Vacío, sin dispositivos de red. Sólo se crea por defecto el loopback.*
- *El contenedor no tiene dirección ip.*
- *Útil sobre todo para diagnósticos de pruebas o cuando no queremos exponer el contenedor a la red.*

MODO VETH

- *Modo bridge:*
- *Es el creado por defecto.*
- *Enlace bridge con el servidor físico.*
- *Unimos el lado del contenedor con el lado del servidor.*
- *Útil sobre todo para crear redes virtuales entre contenedores, emular redes para configuraciones de red local, probar topologías de red.*

MODO PHYS

- *Modo PHYS:*
- *Asignamos una interfaz física a un contenedor.*
- *La interfaz no es compartida con el servidor. Este deja de tener el dispositivo para él.*
- *Normalmente capturamos la interface que sale al exterior.*
- *Útil sobre todo para poder filtrar el trafico que sale de nuestra red.*

MODO VLAN

- *Modo VLAN:*
- *Asignamos una interfaz de un contenedor a una VLAN específica.*
- *Simplemente debemos especificar el ID de la VLAN.*
- *Útil sobre todo para unir VLANs.*

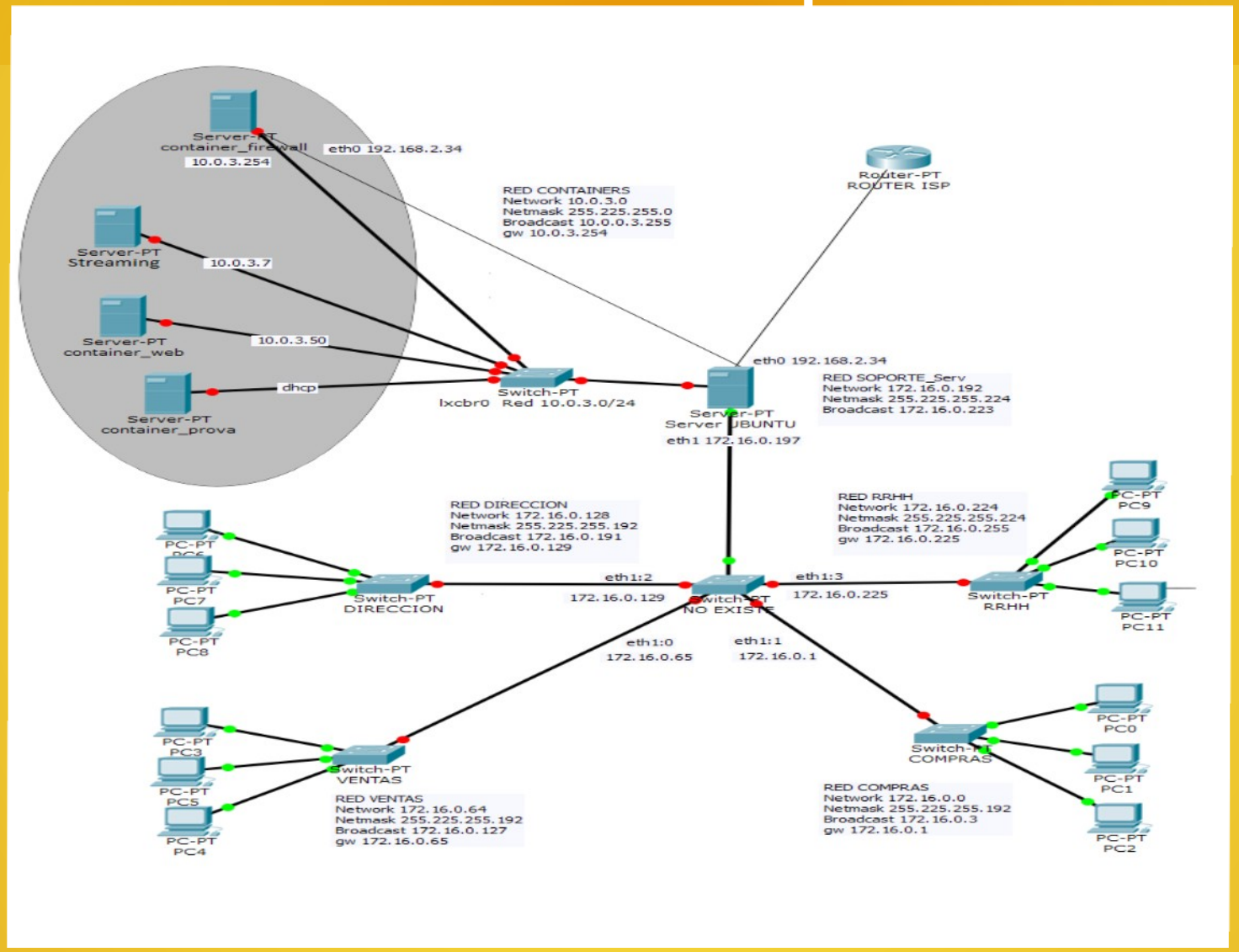
MODO MACVLAN

- *Modo MACVLAN:*
- *Como vlan pero con mac distintas. Una interface macvlan está vinculada con una interface del servidor físico y asignada al contenedor.*
- *Nos permite asociar multiples mac-addres(multiples ips) a una única interface fisica.*
- *Cada interface puede estar asociada a una subred distinta.*
- *Aislamiento seguro de red*
- *Uso DMZ*

MODO MACVLAN

- *3 modos de comunicación entre diferentes macvlans en el mismo dispositivo:*
  - *private: el dispositivo no se comunica por defecto con ningún otro dispositivo al que están conectadas las macvlan*
  - *vepa : se genera el trafico que es local al puerto de macvlan. Como viejo hub, tráfico a todas interfaces*
  - *Bridge: se comporta como un puente entre macvlan*

Solución Propuesta



PRESUPUESTO Projecte LXC			
HARDWARE			
Modelo	**Cantidad**		**Total**
Servidor rack PowerEdge R730	**1**		**1.690€**
Cisco SMB SRW2024-K9-EU SG 300-28 28-port Gigabit Managed Switch	**4 x 439**		**1.756€**
Cisco SMB RV325-K9-G5 Cisco RV325 Dual Gigabit WAN VPN Router	**1**		**262€**
SOFTWARE			
S.O Ubuntu 14.0.4.1 LTS trusty	**1**		**0**
Firewall Iptables v1.4.21	**1**		**0**
Servidor Apache Versión 2.4.7	**1**		**0**
Servidor Ftp Versión 3.0.2	**1**		**0**
INSTALACIÓN y CONFIGURACION	**HORAS**	**PRECIO**	
Hora técnico	**46**	**20**	920 €
Total Presupuesto			4.628 Euros

Futuras ampliaciones

- Openswitch
- Virtualización en la nube
- Diseño plantillas personalizadas