Virtualizacion, Seguridad (UTM) y Alta Disponibilidad

Para mas informacion contactar con
Kamal Majaiti Twitter (@KamalMajaiti)

Virtualizacion - ¿Qué es?

- Es la division de los recursos físicos del hardware en otros lógicos que serán usados por un Software con capacidad de simular un hardware para la ejecución de varios sistemas operativos completos sobre un equipo físico.

Tipos de Virtualizacion

- Emulación.
- Virtualizacion completa.
- Virtualizacion nativa.
- ParaVirtualizacion.
- Virtualizacion a nivel del S.O

Emulación

- La maquina virtual simula un hardware completo ,para una CPU completamente diferente. Admitiendo el S.O sin modificar.

Destacan

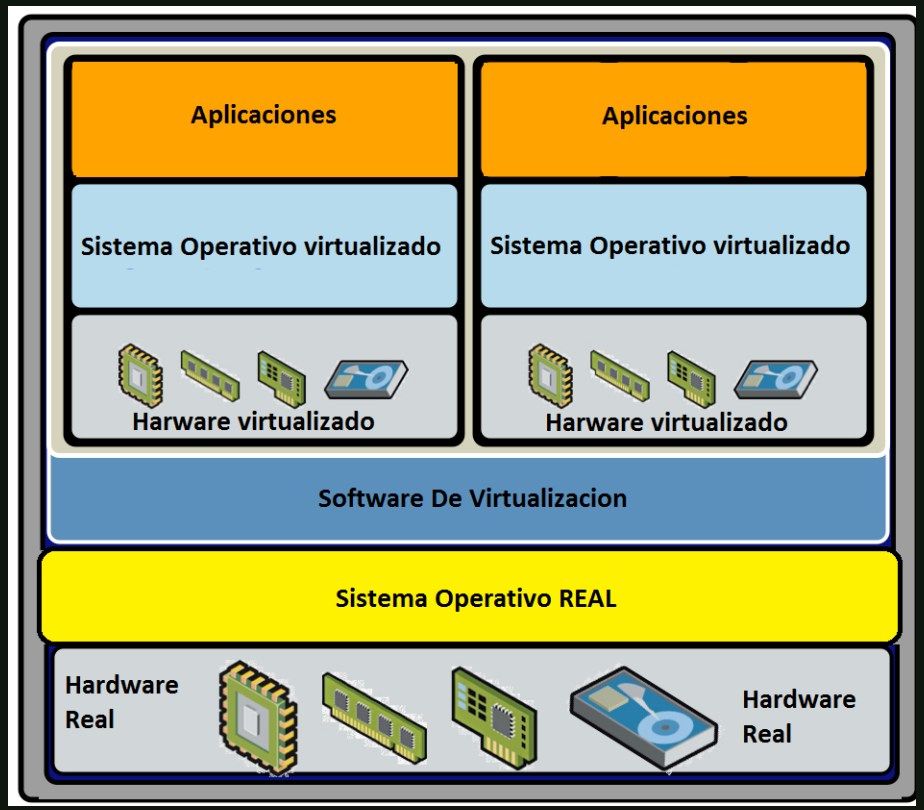
- Bochs y Qemu.
- Ambos son open source, pueden emular cualquier CPU y ejecutar cualquier S.O.
- Demasiado Lento para producción.

Ejemplo Emulación

Un ejemplo de un procesador PowerPC es capaz de ejecutar
un S.O diseñado para un procesador x86.

Virtualizacion Completa.

- El software de Virtualizacion emula todo el hardware y parchea el S.O virtualizado aun así sigue siendo Lenta.

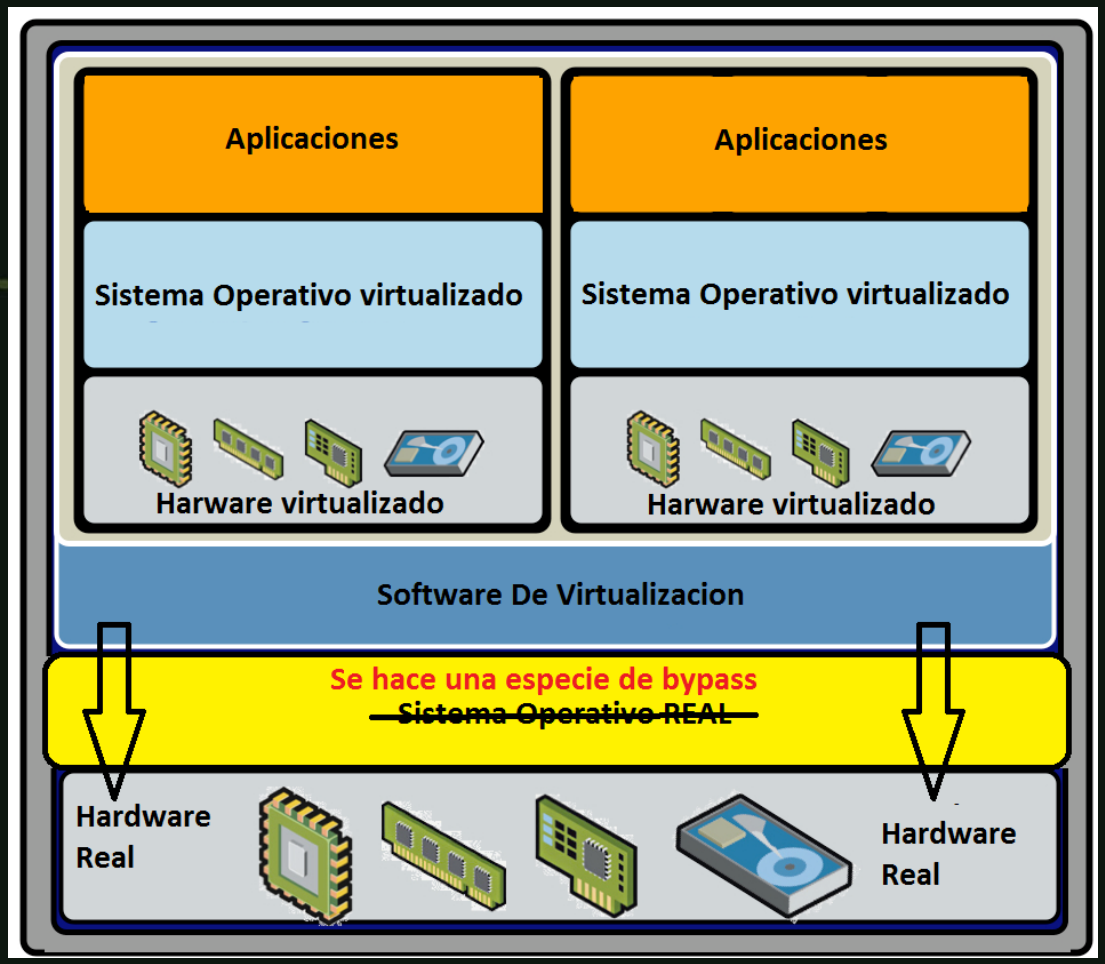


Virtualizacion nativa.

- Debido a la perdida de rendimiento se crean unas instrucciones de procesamiento privilegiadas que tienen acceso directo al hardware.
- Permiten ejecutar instrucciones de ring 0 (Máximos Privilegios).
- Evitando la latencia causada por el S.O en procesar esas instrucciones.
- El S.O se modifica menos.

Virtualizacion nativa.

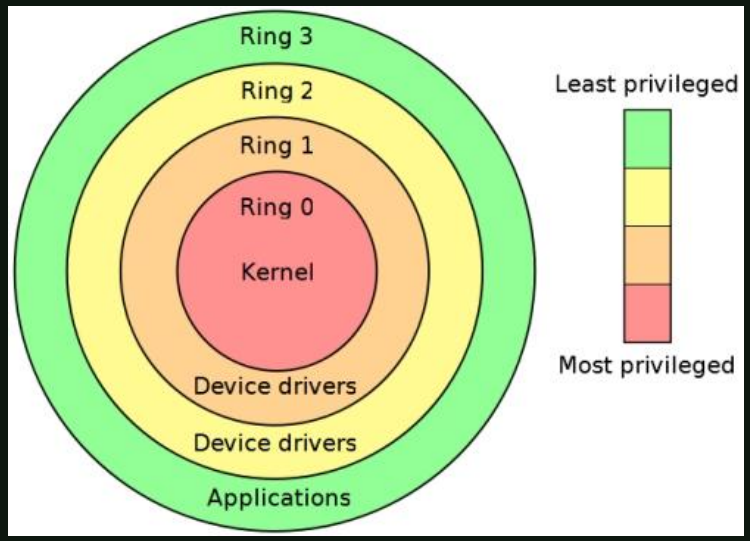
El software de Virtualizacion se comunica directamente con el hardware físico de la maquina real.



Repaso de los privilegios del Procesador.

- Indiferentemente del usuario que inicio sesión en el equipo cada proceso se ejecuta en un anillo de privilegios acorde a lo que necesita.

Cuando mas dentro mas cantidad de instrucciones se pueden ejecutar es decir, en Ring2 no se pueden ejecutar instrucciones de Ring 0. Pero en Ring0 están todas las instrucciones de los anillos anteriores.



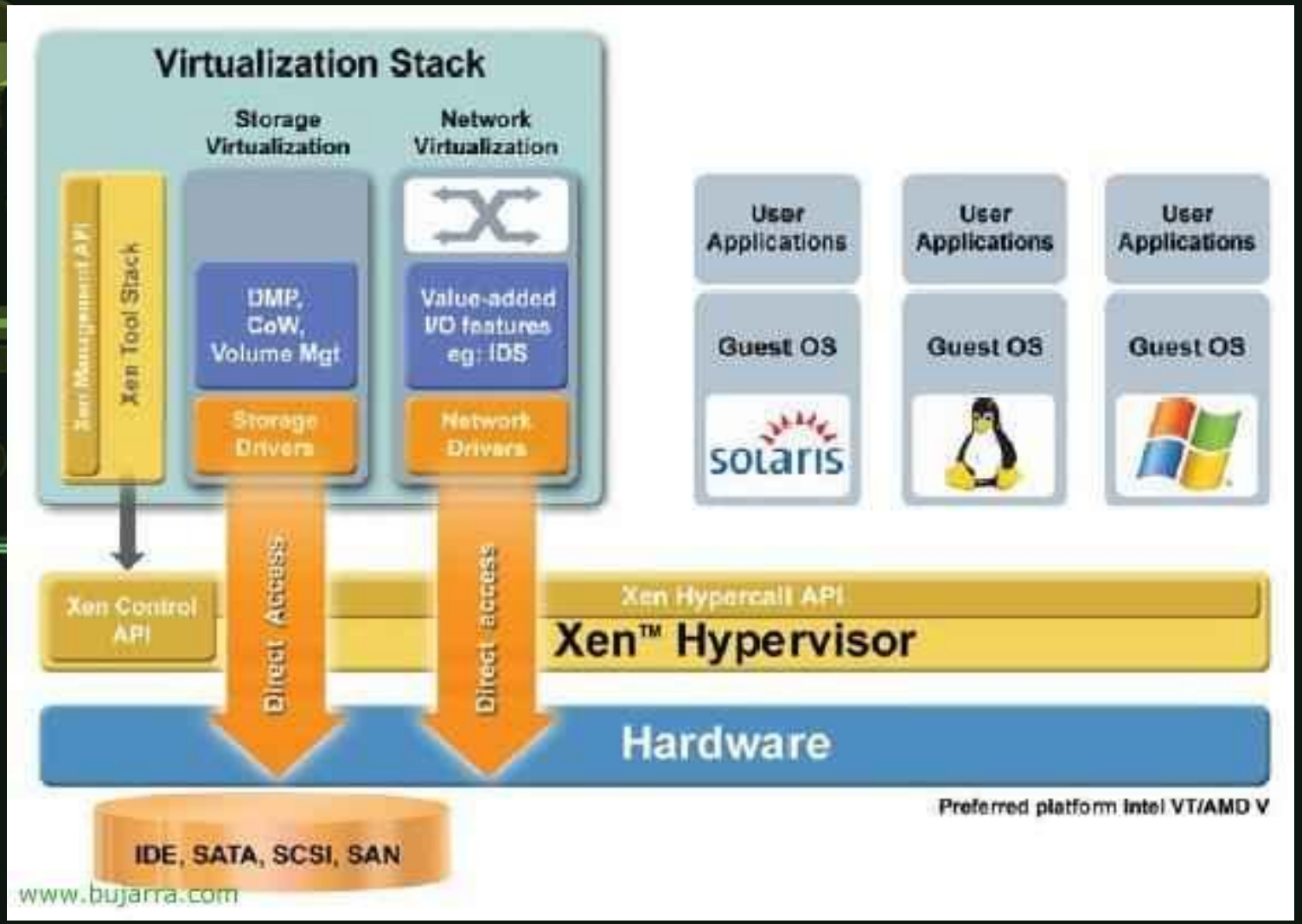
ParaVirtualizacion

- Es una técnica en la cual se crea una interface de acceso al KERNEL ejecutado en la maquina física. Por lo cual se modifica el KERNEL de la maquina virtual para que se comunique con núcleo real a través de la api (Llamada Hypervisor).

ParaVirtualizacion

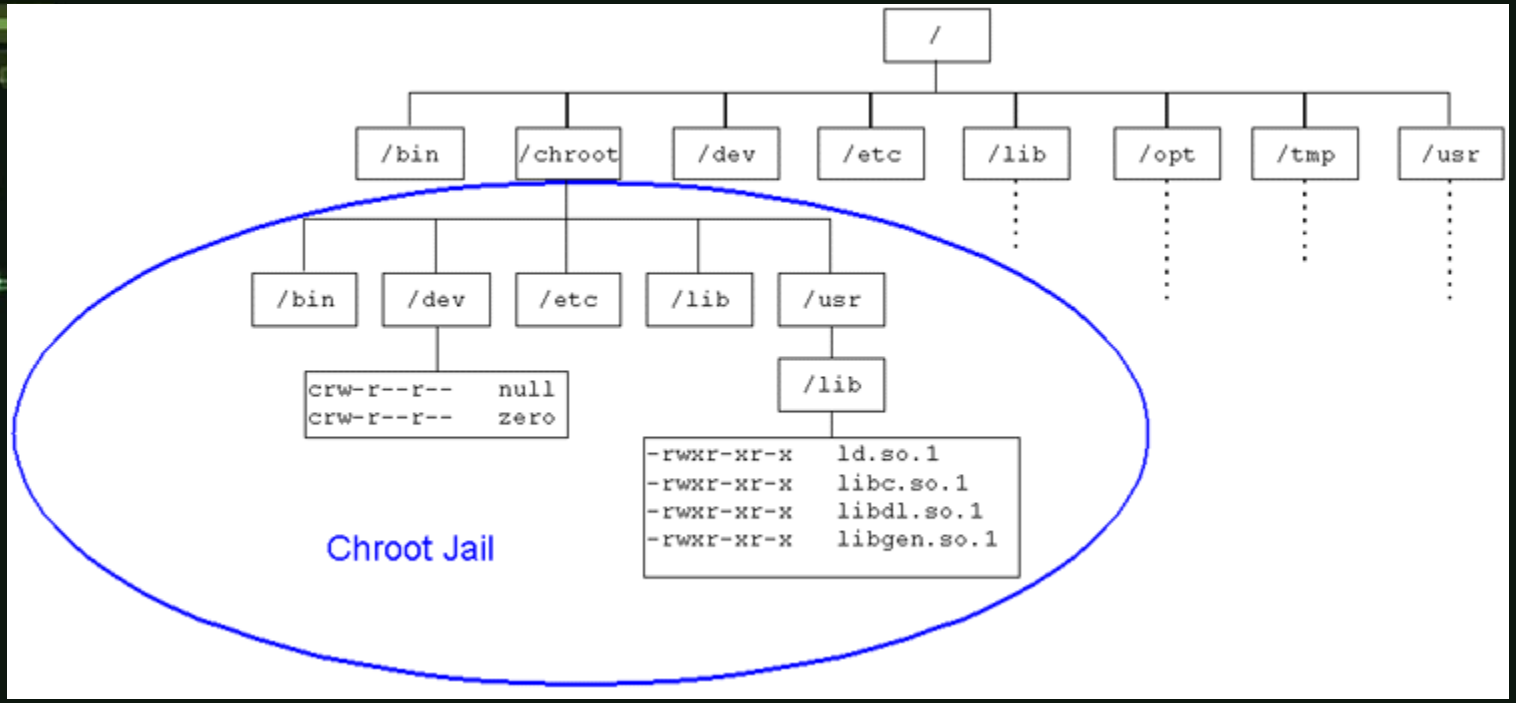
- Al modificarse el sistema operativo, se consigue ejecutar las maquinas virtuales con un alto rendimiento (Tan solo un 2% al 8% de perdida) ,esta técnica es la que se esta utilizando para producción en servidores VPS.

ParaVirtualizacion

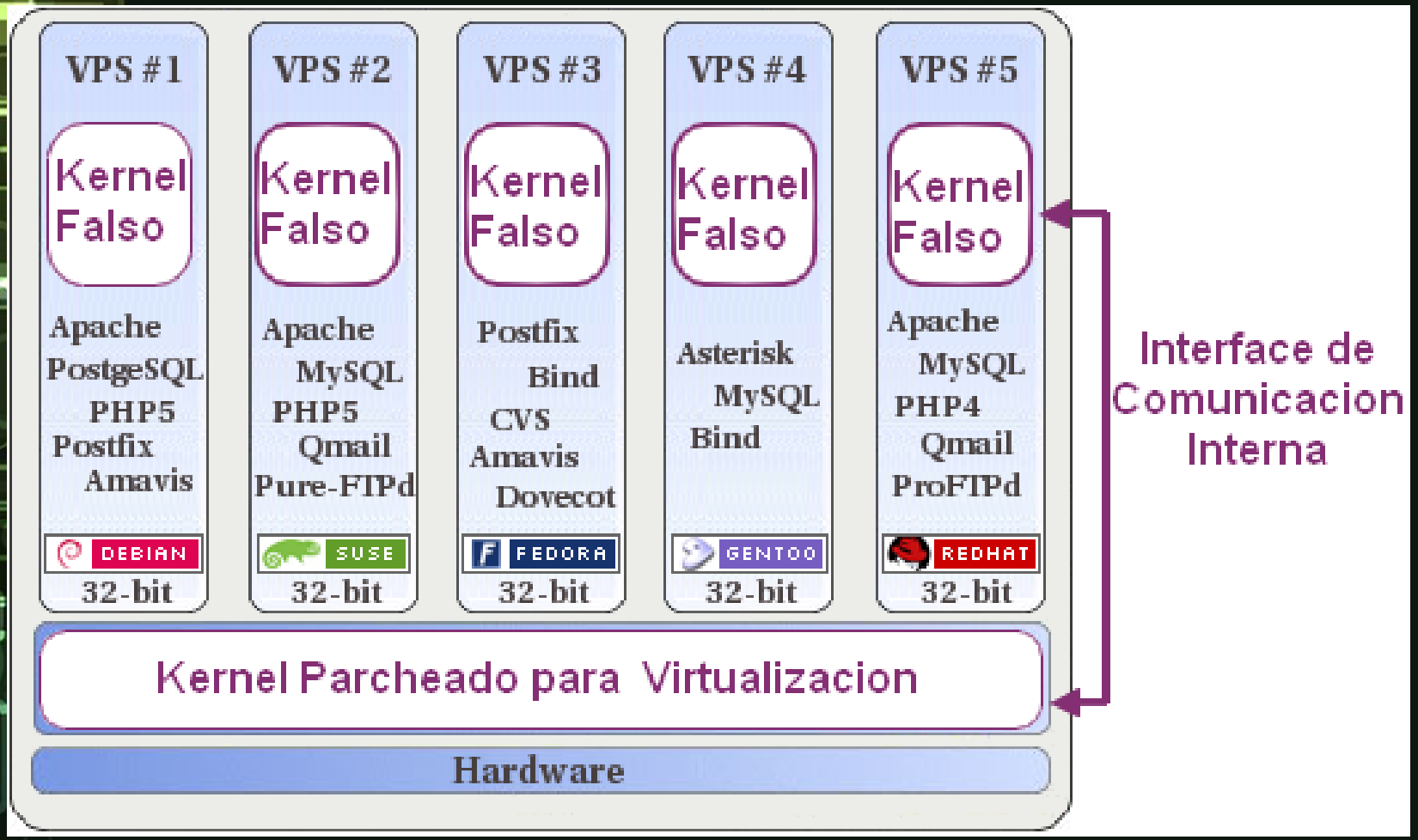


Virtualizacion a nivel del S.O

- Las maquinas virtuales y la maquina real comparten el mismo núcleo. Únicamente se aíslan entre ellos



Virtualizacion a nivel del S.O



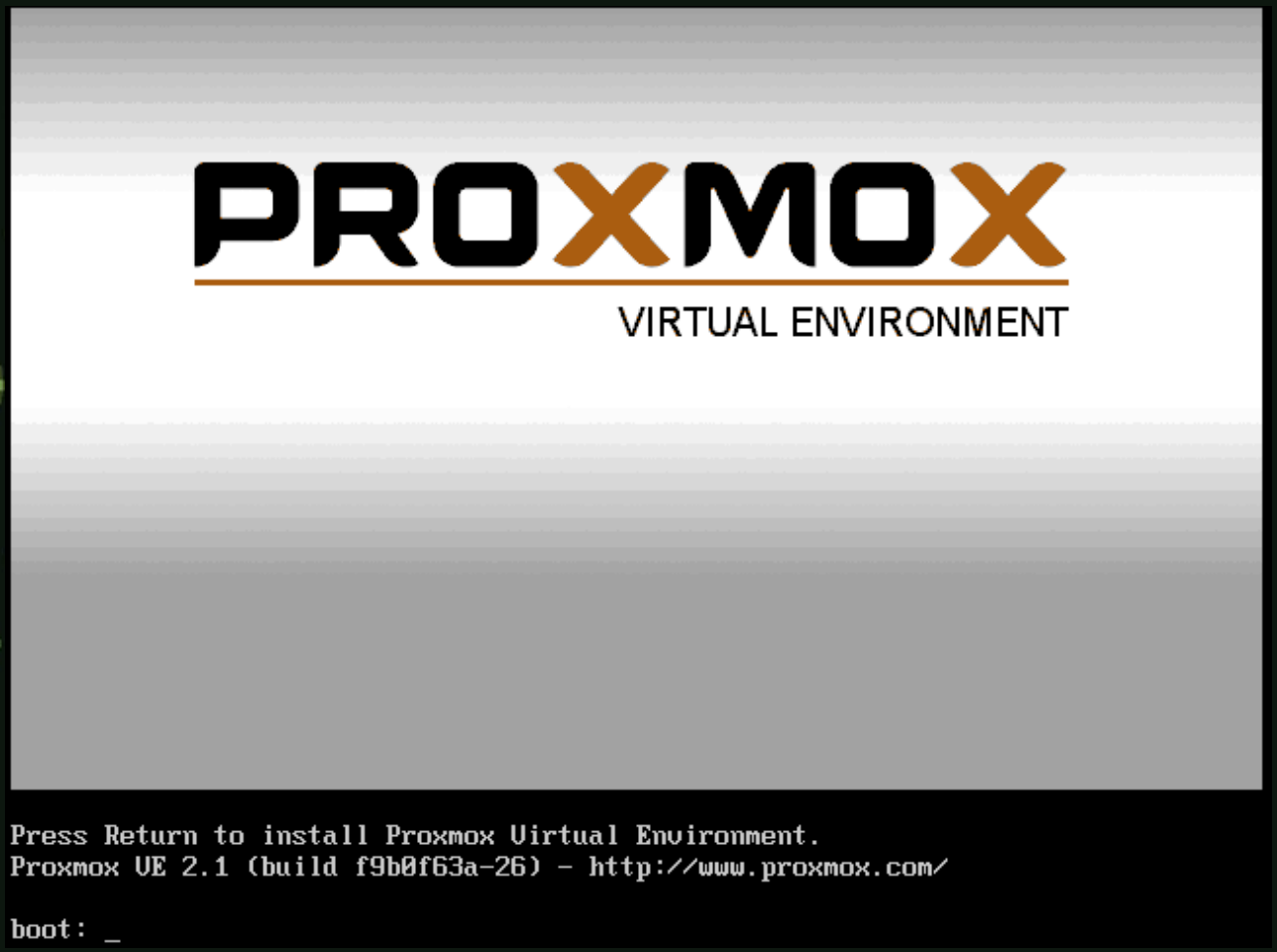
Virtualizacion a nivel del S.O

- En esta técnica de Virtualizacion no existe perdida de rendimiento es la mas usada en servidores.

Ventajas de la Virtualizacion.

- Mejor aprovechamiento de los recursos.
- Administración mas sencilla.
- Alta Escalabilidad.
- Alta Disponibilidad.
- Reducción de costes y consumo.
- Balanceo de carga Dinámico.
- Copias de Seguridad mas sencillas.

Vista rápida de ProxMox



ProxMox VPS Server

- Basado en debían.
- Interface web de administración.
- Automatización de VPS.
- Capacidad de funcionar en Clúster
- Soporta KVM y OpenVZ

Vmware vSphere / esxi

- Utiliza un núcleo modificado de Red Hat Enterprise Linux.
- Soporta Administración por web
- Soporta Administración por consola.
- Soporta infraestructuras complejas.
- Tiene una Consola grafica muy completa.

Xen Server

- **Era libre hasta que fue comprado por Citrix .**
- **Usa Xen como tecnología de Virtualizacion (Buen rendimiento).**
- **Soporta mover maquinas virtuales entre diferentes servidores VPS.**
- **No soporta administración compartida.**

Características de un UTM

- VPN
- Proxy
- Antispam
- Antiphishing
- AntiMalware
- Filtro de contenidos
- IDS
- Cortafuegos.

Ventajas de un UTM.

- Gestión Centralizada.
- Despliegue Rápido.
- Mejor Administración y control de la red.
- Facilita las tareas de monitorización.
- Auto Actualización desatendida. (Algunos).

Desventajas de un UTM.

- Problemas de rendimiento.
- Soporte del fabricante (Adecuado).
- Dependemos de un fabricante en la seguridad de la empresa.
- Cuellos de botella en la red.
- Muy vulnerable a ataques dirigidos.
- Solo filtramos lo que pasa entre la LAN y la WAN.

UTM Algo estamos haciendo mal.

- La mayoría de las desventajas se pueden eliminar.
  - –Usando mas UTM en la empresa y descentralizados.
  - –Usando UTM basado en Open Source (No son nada malos).

UTM Propietario

- Cisco (ASA Firewalls).
- Junniper (SSG security platforms)
- Fortinet (Especializada en Seguridad).
- CheckPoint (Security Gateway).
- IBM (ISS - Internet Security Systems)

IBM (ISS)

CheckPoint (Security Gateway)

Cisco (ASA Firewalls)

Junniper (SSG platforms)

Varios UTM de Cerca

UTM - Pfsense

- Basado en FreeBSD.
- Es Modular.
- Cortafuegos.
- IDS, Antivirus, Proxy, VPN etc..
- Servidor WEB ,Radius ,HTTP…
- Balanceado de carga.
- Monitorización SNMP.
- Y muchísimo mas….

UTM - Endian

- Basado en Linux.
- Firewall Bidireccional.
- AntiMalware,AntiSpam,IDS,proxy.
- Balanceador de carga.
- NTP,DHCP,Syslog,
- Estadisticas Reales de Red.
- Voip, Radius ,Wireless AP

UTM - Vyatta

- Es modular, basado en debían.
- Enrutamiento OSPF/RIP/BGP.
- Monitoreo de Redes SNMP.
- IDS,IPS,Firewall,L2TP,IPSEC,SSH,
- Balanceo de carga , Redundancia VRRP.
- VPN,QOS,DHCP,Sniffer,**Clustering**
- VLAN,HDLC,PPP,PPPoE,Frame Relay.
- 3G,Web Cache, Filtrado HTTP.

UTM - ClearOS

- Basado en CentOS.
- Firewall , IDS, VPN, Proxy.
- Antimalware.
- Reportes Automatizados.
- Balanceo de Carga y MultiWAN.
- Servidor Samba ,Ftp ,Cups ,Email.
- Servidor LAMP.

UTM - untangle

- AntiSpam ,AntiMalware ,AntiPhising.
- Servidor Web Cache ,Proxy.
- Control del Ancho de Banda.
- Análisis de Paquetes TCP/UDP.
- Firewall ,IDS ,VPN, Mitigador de Ataques.
- Bloqueador de publicidad/contenido.
- Avisos automáticos ,Balanceador de Carga.

UTM open source NetCop

- Filtrado de contenidos.
- Proxy ,Web cache.
- Firewall.
- Antimalware.
- Balanceador de Carga.
- Soporta VLAN.
- Control del Ancho de banda.
- Punto de Acceso ,Servidor Radius.

Alta Disponibilidad - ¿Qué es?

- Mas bien conocida como HA, es una implantación de un sistema de forma que nos garantiza una gran tolerancia a fallos y una continuidad de funcionamiento durante un tiempo prolongado.

Alta Disponibilidad - Técnicas

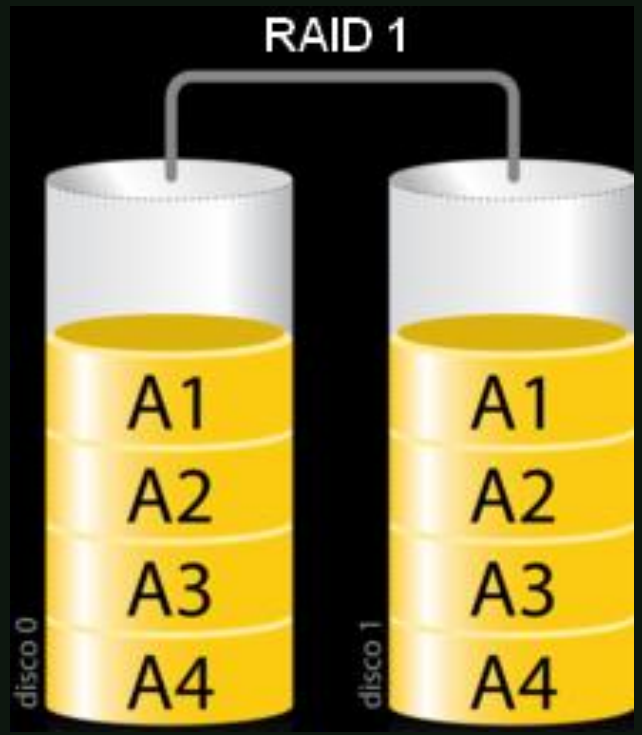
- Redundancia del Hardware.
- Redundancia del suministro eléctrico.
- Redundancia de las Conexiones.
- Clustering.
- Balanceado de Carga.
- Evasión inteligente de Ataques.
- Detección de anomalías.

HA -Redundancia del Hardware.

- Fuentes de alimentación redundantes.

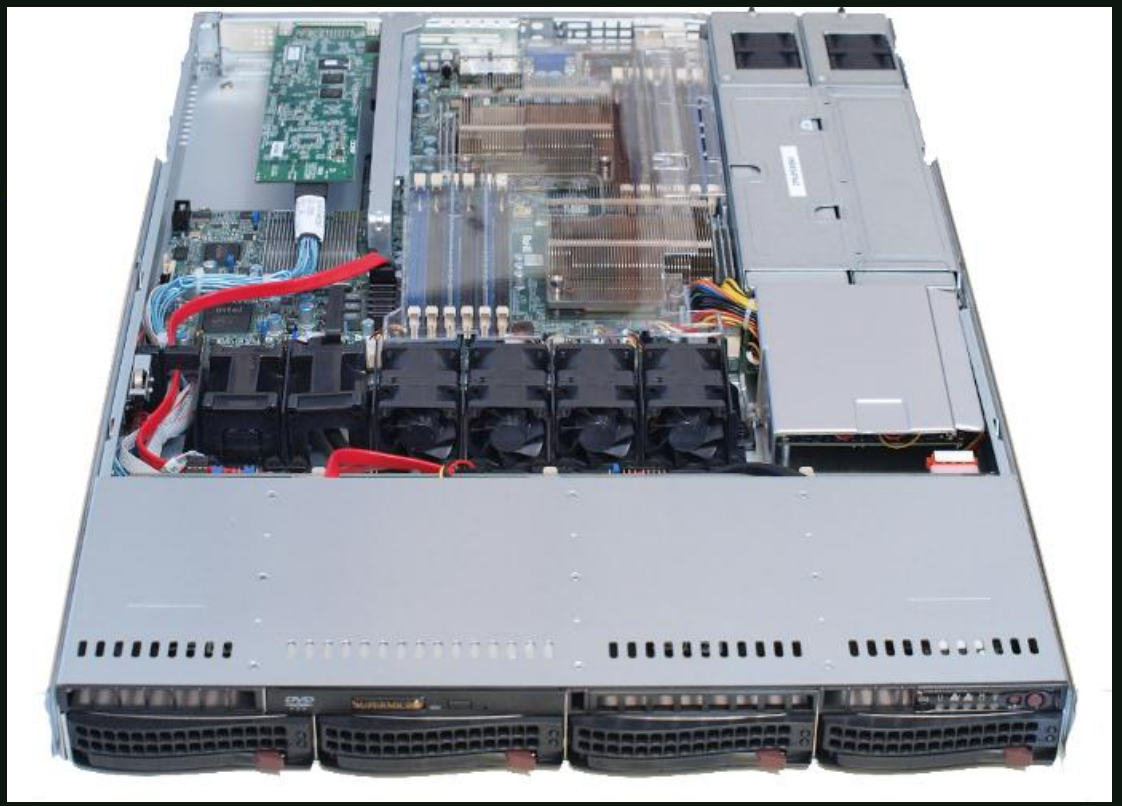
HA -Redundancia del Hardware.

- Almacenamiento Redundante..



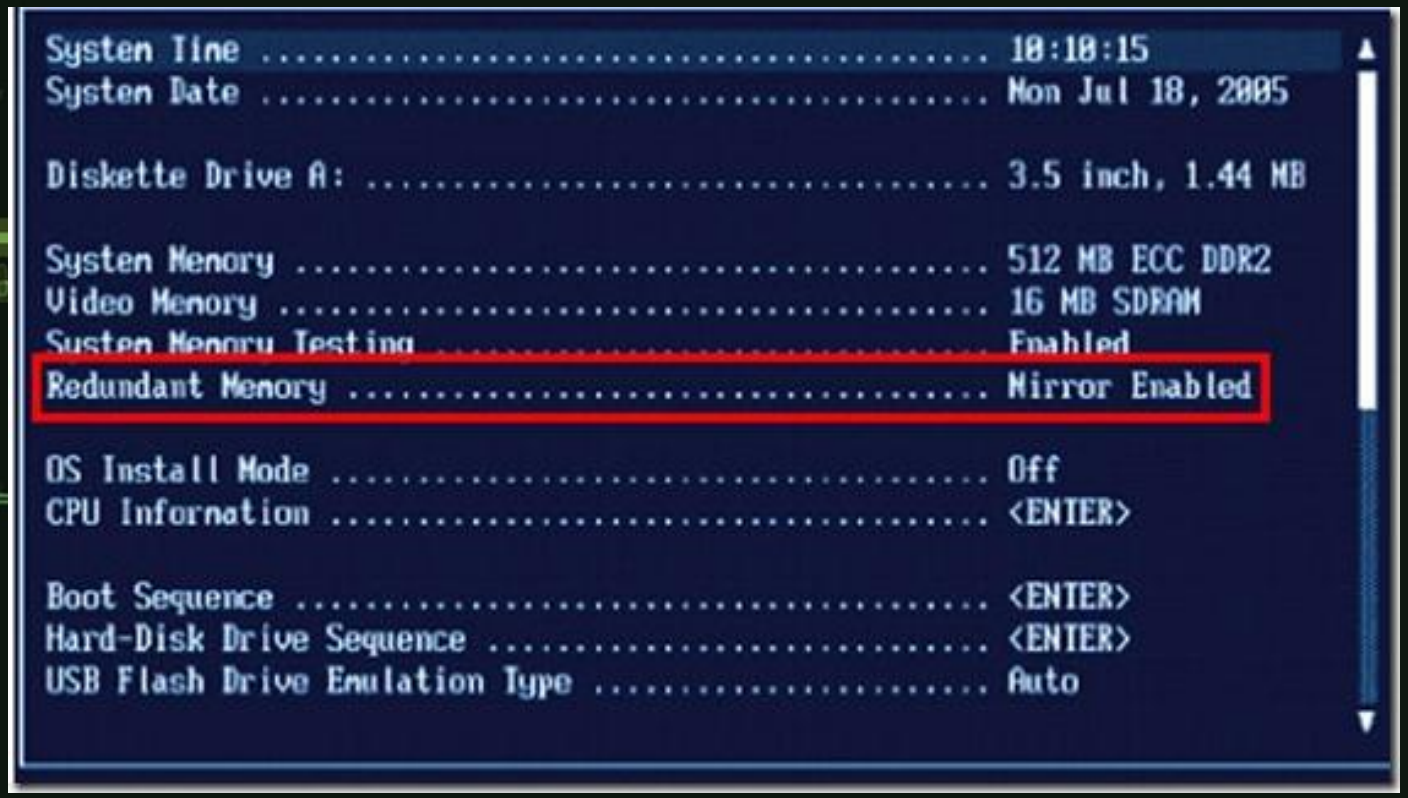
HA -Redundancia del Hardware.

- Ventilación Redundante..



HA -Redundancia del Hardware.

Memoria RAM Redundante..



HA -Redundancia del Hardware.

Memoria RAM con corrección.

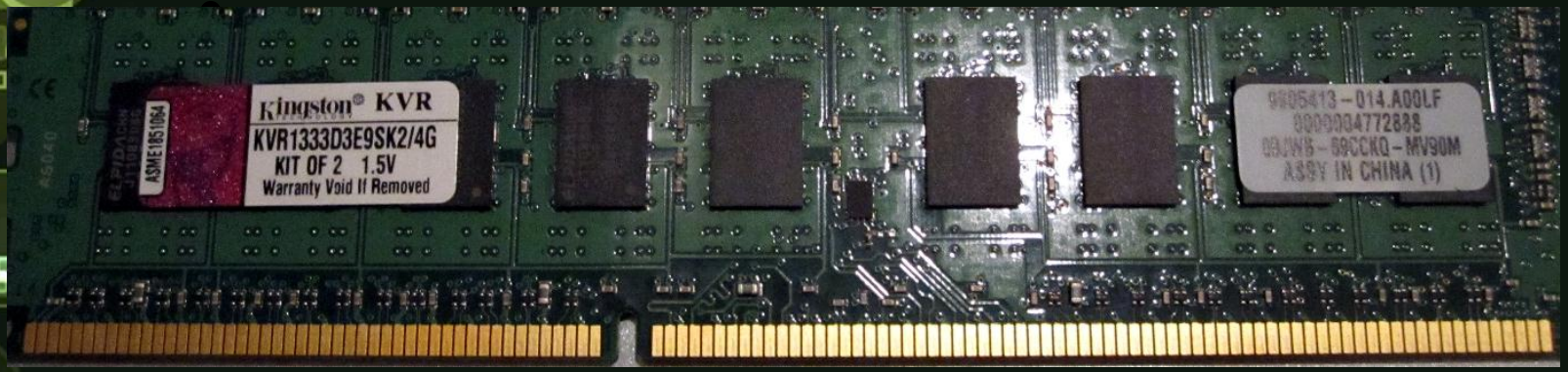
- **Técnicas empleadas**

Paridad del bit consiste en guardar un bit adicional por cada byte de datos, y en la lectura se comprueba si el número de unos es par (paridad par) o impar (paridad impar), detectándose así el error.

ECC consiste en un sistema trabaja en conjunción con el controlador de memoria, y anexa a los bits de datos los bits ECC, son almacenados junto con los de datos. Estos bits extras, junto con la decodificación correspondiente, sirven para realizar la comprobación en el momento de la lectura.

HA -Redundancia del Hardware.

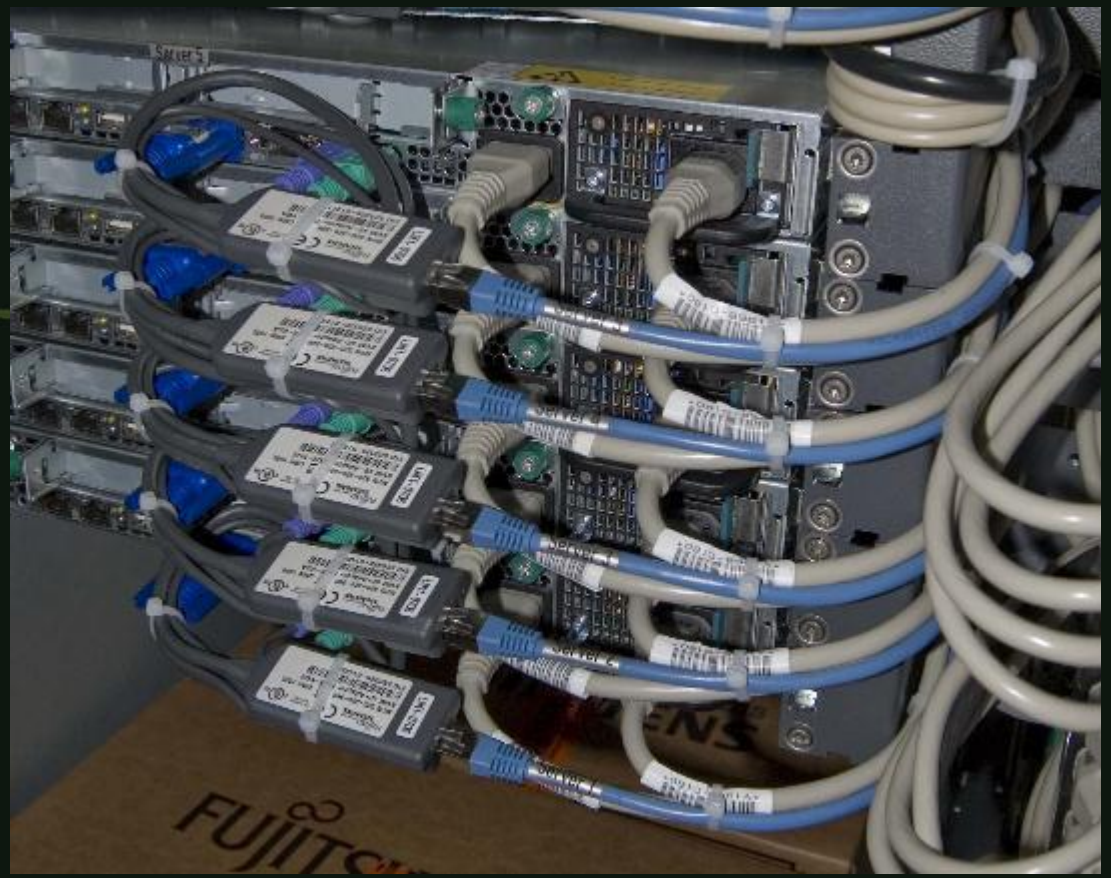
- **Memoria RAM con ECC.**



DESCRIPTION

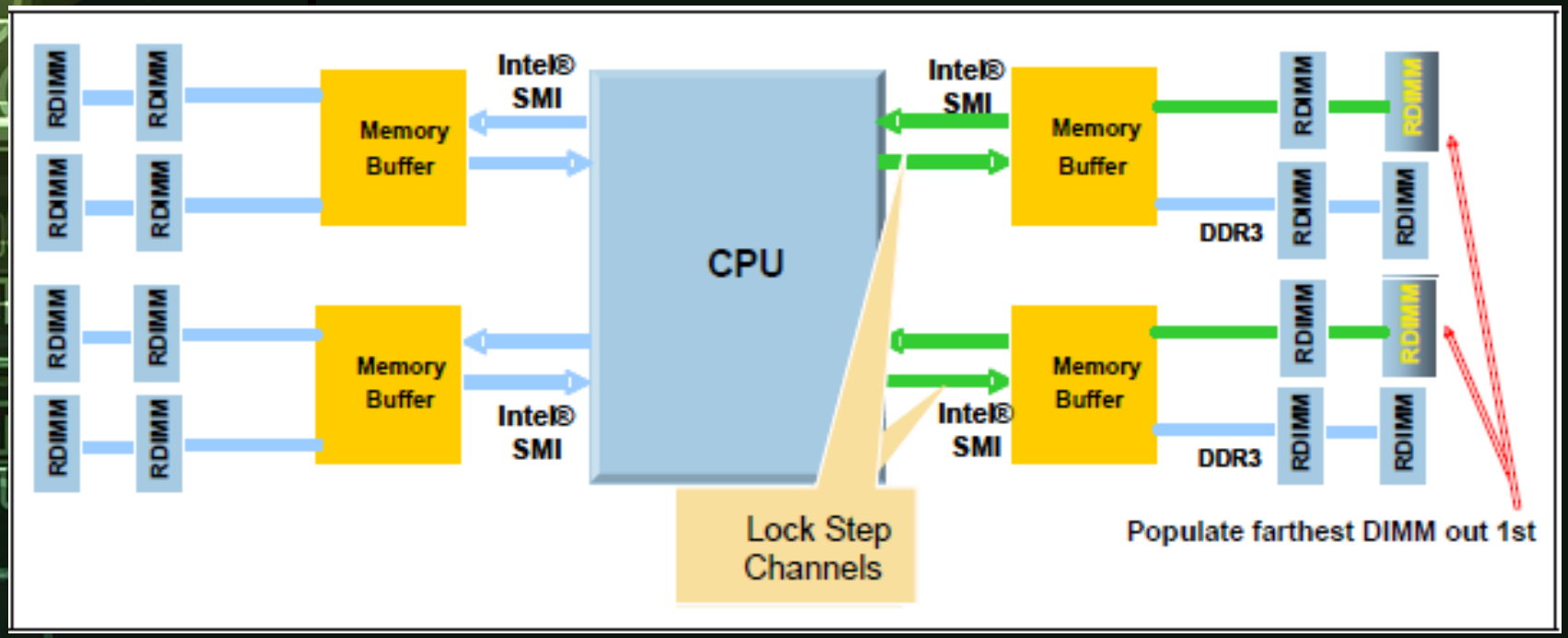
ValueRAM's KVR1333D3E9SK2/8G is a kit of two 512M x 72-bit (4GB) DDR3-1333 CL9 SDRAM (Synchronous DRAM), 2Rx8 ECC memory modules, based on eighteen 256M x 8-bit FBGA components per module. Total kit capacity is 8GB. The SPD's are programmed to JEDEC standard latency DDR3-1333 timing of 9-9-9 at 1.5V. Each 240-pin DIMM uses gold contact fingers. The electrical and mechanical specifications are as follows:

HA -Redundancia del Hardware.

- Tarjeta de Red Redundante
- 

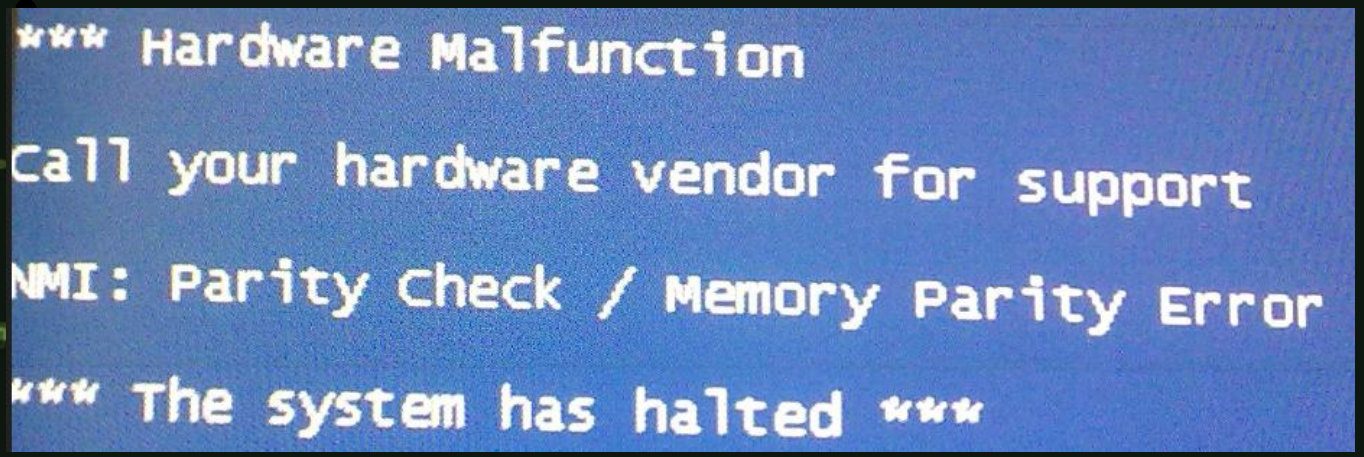
HA -Redundancia del Hardware.

- Procesamiento en paralelo con paridad. (Lock stepped)
-



HA -Redundancia del Hardware.

- Paridad del bus de datos de la CPU.

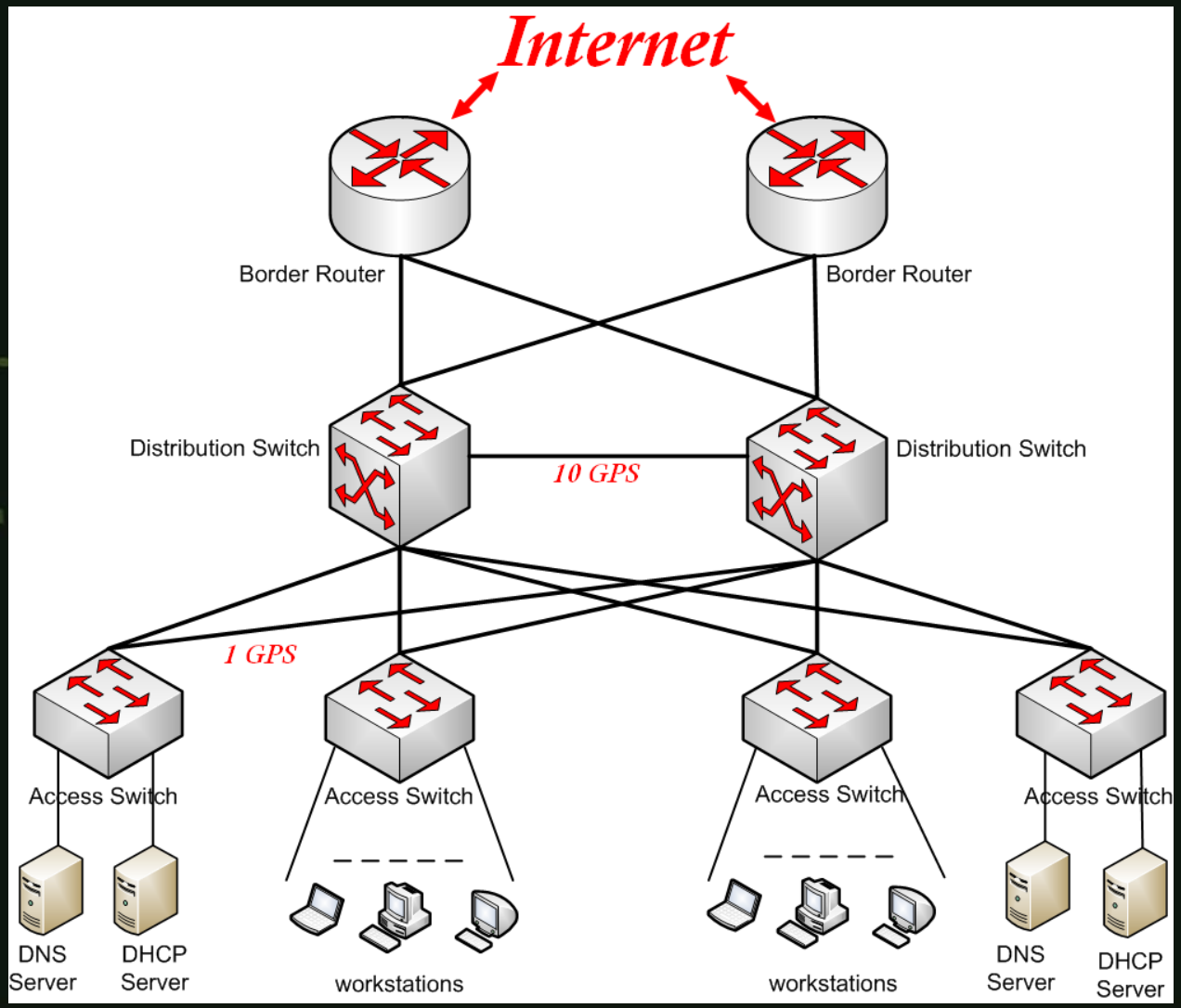


HA -Redundancia del suministro eléctrico.

Contratos con varias eléctricas, sistemas SAI, Cuarto de Baterías ,Generadores eléctricos

HA -Redundancia de la red.

Conexiones Redundantes y con gran ancho de banda.



Fin