TICAR 2013 UNC
Implementación de Vyatta en la Universidad Nacional de Quilmes
(UNQ)

Cesar Luis Zaccagnini
Jefe de Departamento de
Infraestructura Tecnológica y Telecomunicaciones
cesar@unq.edu.ar

Alejandro Del Brocco
Director de Servicios Informático
alejandro@unq.edu.ar

Universidad Nacional de Quilmes

Exposición

Explicaremos el proceso que determinó la exitosa implementación del Router/Firewall basada en Software Libre.

Las características de esta distribución que llevo a su elección.

Exposición

- Identificación de la necesidad.
- Contexto de la Universidad
- Evaluación de alternativas
- Características del Vyatta
- Implementación Actual
- Implementaciones Futuras
- Ventajas y Desventajas

Identificación de la necesidad

La Universidad contaba con un router encargado de brindar la conectividad interna y dar acceso a Internet a dichas redes.

Funciones asignadas

- NAT
- Vlan 802.1q
- ACL (Access List)
- Enlace RIU

Identificación de la necesidad

- El Router era un Cisco 3620 adquirido en 1999, este en su momento remplazo al 2501 que originalmente vino con el enlace de la RIU.
- En el 2005 se intento contratar los servicios de mantenimiento y soporte de cisco, pero la mayoría de los equipos que poseíamos se encontraban fuera de la linea de vida para Cisco, y no era admitido por el servicio de mantenimiento que cisco ofrece.
- Esto nos ponía en una situación delicada, en caso de que el router falle nos dejaba sin conectividad Interna/Externa.

Identificación de la necesidad

- Con el incremento de nuestra red interna empezó a quedar chico el equipo para las funcionalidades asignadas. Comenzamos a tener problemas con el procesamiento del equipo (CPU 100%).

- Todo su hardware y software estaba discontinuado y sin soporte quedando fuera de línea para la empresa fabricante y representantes oficiales.

Contexto de la Universidad

- Crecimiento de puestos de trabajo
- Segmentación en redes mas pequeñas.

Evaluación de alternativas

- Actualizar un router Cisco o comparable
- Implementar el router con un equipo x86 y GNU/Linux
- Utilizar una distribución de GNU/Linux con este objetivo

Evaluación de alternativas

Actualizar un router Cisco o comparable

-Costosa

-En un tiempo estaríamos nuevamente fuera de la linea de vida del producto (con hardware sin soporte)

-Cada elemento adicional es propietario y costoso (ETH, Memoria)

Evaluación de alternativas

Implementar el router con un equipo x86 y GNU/Linux o BSD

-Se puede utilizar hardware estándar

-Existen multiples aplicaciones para implementarlo (Squid, Snort, OpenVPN, IPSec y de ruteo XORP, Zebra, Quagga, Iptables, y mas..)

-Es Libre

-Pero... Cada aplicación posee una configuración individual que lo hace complejo de mantener y propenso a errores humanos

Evaluación de alternativas

Utilizar una distribución de GNU/Linux con este objetivo

-Se evaluaron varias distribuciones desde el IPCOP al Zeroshell pasando por monowall y sus derivados, pero no nos resultaron para lo que queríamos (Remplazar el Router Cisco)

-Dentro de estas pruebas le toco el turno a Vyatta que cumplió con nuestros requerimientos y mas

Características del Vyatta

Características por cual se eligió

-Es GPL

-Resuelve todas las necesidades que teníamos

-La configuración del mismo se guarda en un único archivo

-Posee una comunidad activa y tiene actualizaciones periódicas (2 por año)

Características del Vyatta

Características: Protocolos de Ruteo y IP

- IPv4 y Ipv6
- Rutas Estáticas
- RIPv2
- OSPFv2
- BGPv4

Características del Vyatta

Características: Administración de direccionamiento IP

- Estático
- DHCP: Relay / Server / Client
- DNS: Forwarding / Dynamic DNS

Características del Vyatta

Características: Encapsulamiento

- Ethernet
- Frame Relay
- 802.1Q VLANs
- PPP
- MLPPP
- HDLC
- PPPoE
- GRE
- IP in IP

Características del Vyatta

Características: Performance y Optimización

- Balanceo de carga de WAN
- Qos Priorizar y clasificar de trafico
- Ethernet Bonding
- Control de Ancho de Banda
- Web Cache y filtrado de URL por categoría

Características del Vyatta

Características: Logging, Monitoreo y Seguridad

- Stateful Inspection Firewall
- Network Address Translation
- SSL-based OpenVPN
- Site to Site VPN (IPSec)
- Remote VPN (PPTP, L2TP, IPSec)
- Intrusion Prevention
- Syslog
- SNMPv2c

La implementación

Hardware Remplazado

CPU 80 Mhz IDT RISC R4700
Memoria 8 MB DRAM
Memoria Flash 4MB

Conectividad
1 Ethernet100
1 Ethernet10
2 Serial

La implementación

Hardware utilizado

CPU
Intel(R) Xeon(TM) CPU 2.80GHz 2 nucleos

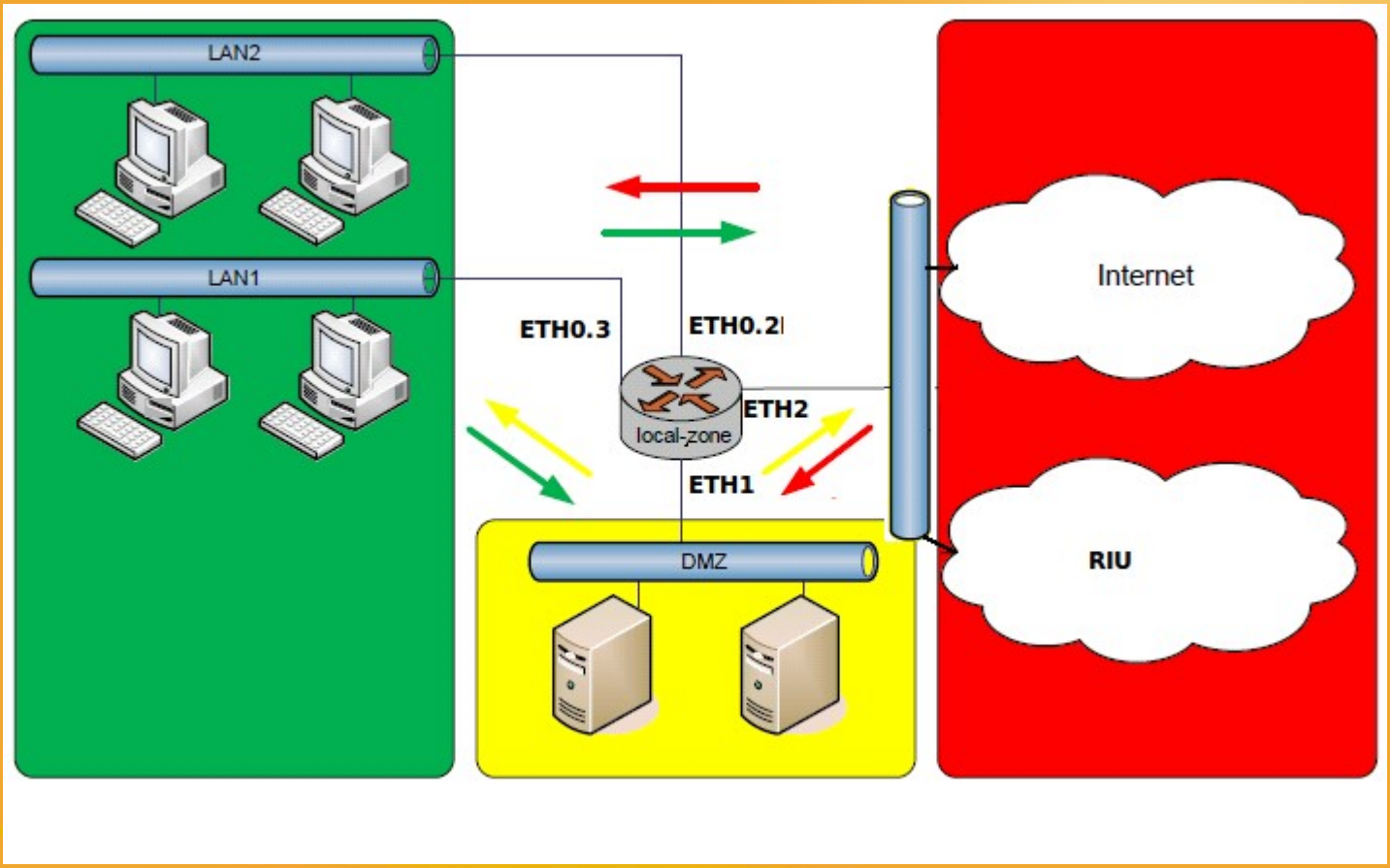
Memoria
2Gb DDR ECC

Conectividad
2 Intel e100
1 Intel e1000

La implementación

Vyatta 6.2 Core Edition
Instalación basada en imagen
Firewall por zonas
Nat
802.1Q
Proxy transparente
SquidGuard
IDS

La implementación



Implementaciones Futuras

- Implementación de HA
  - Wan Balanceo de carga
  - Routers redundantes
- Control de AB
- Virtualizacion de los routers redundantes

Ventajas

- Posibilidad de instalar aplicaciones por ser un Linux (ej. NTOP)

- Proyecto muy activo (2 versiones por año)

- Comunidad importante, y muchos sitios con información

Desventajas

-Funcionalidades que venían el la versión Core ahora solo esta en la SE

Ejemplo de instalación Vyatta

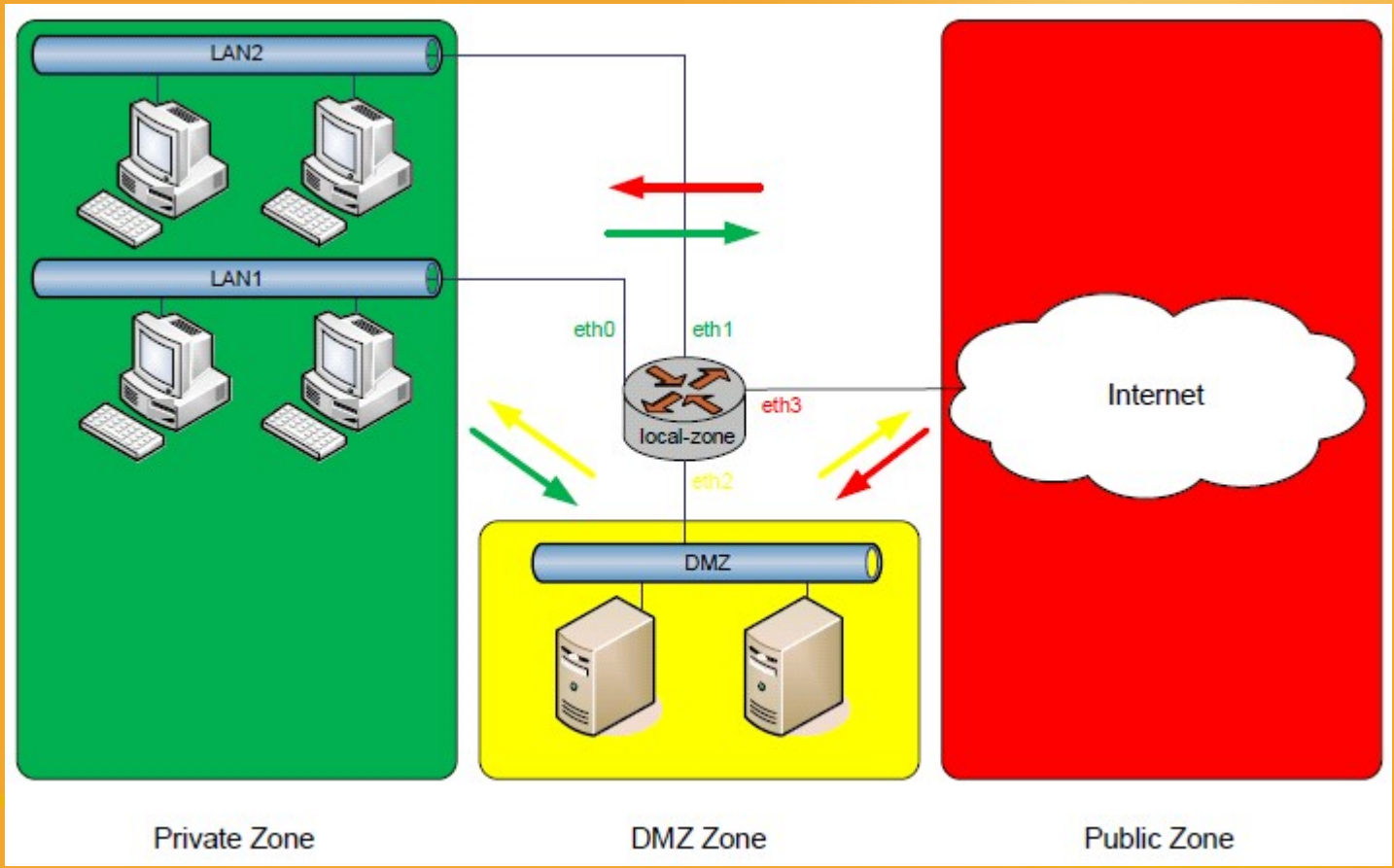
Objetivo:

-Instalar un router/Firewall VYATTA

Topología simple de 4 redes

- Internet
- DMZ
- 2 redes Internas.

Esquema lógico de la red

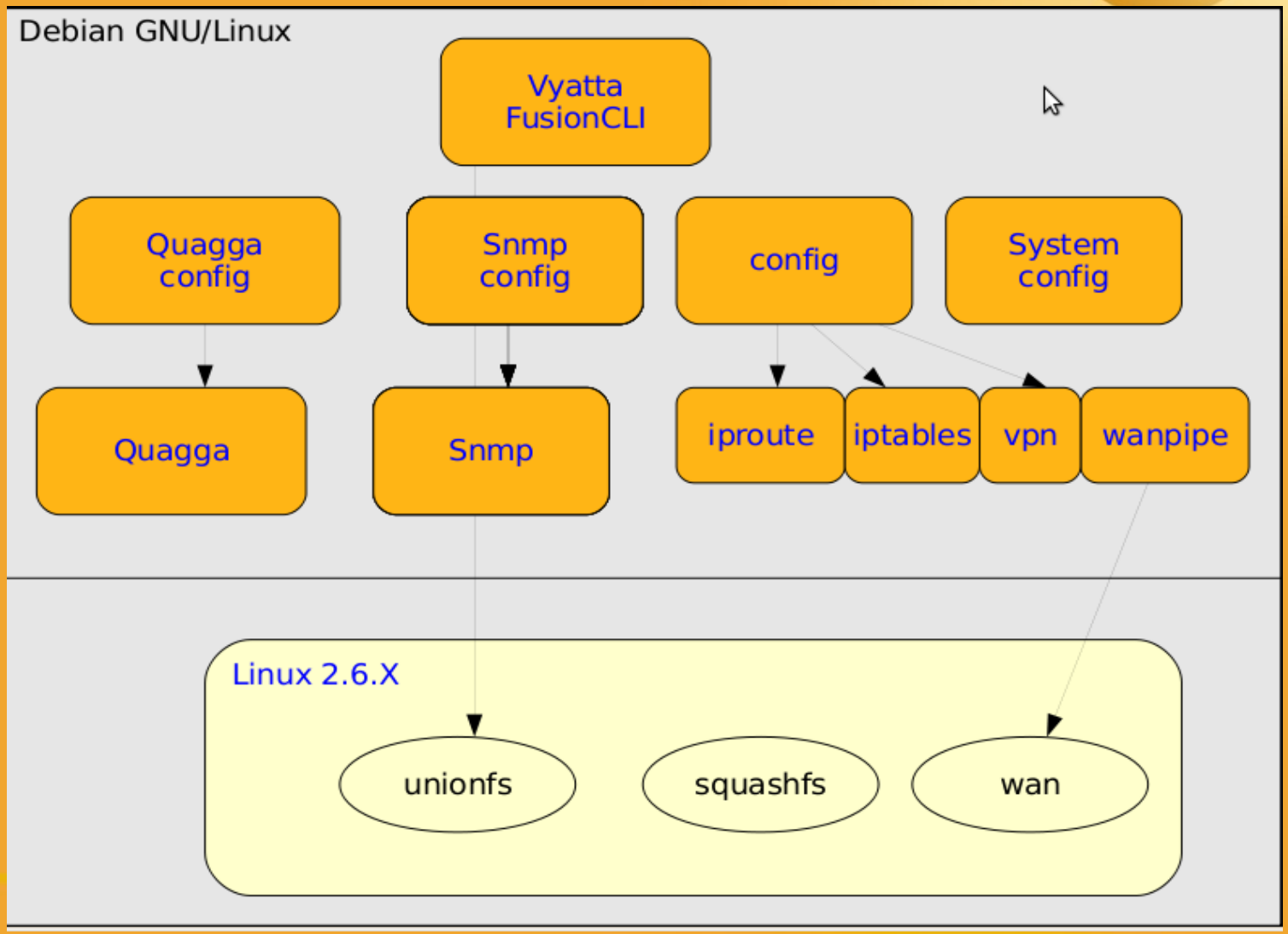


Instalación

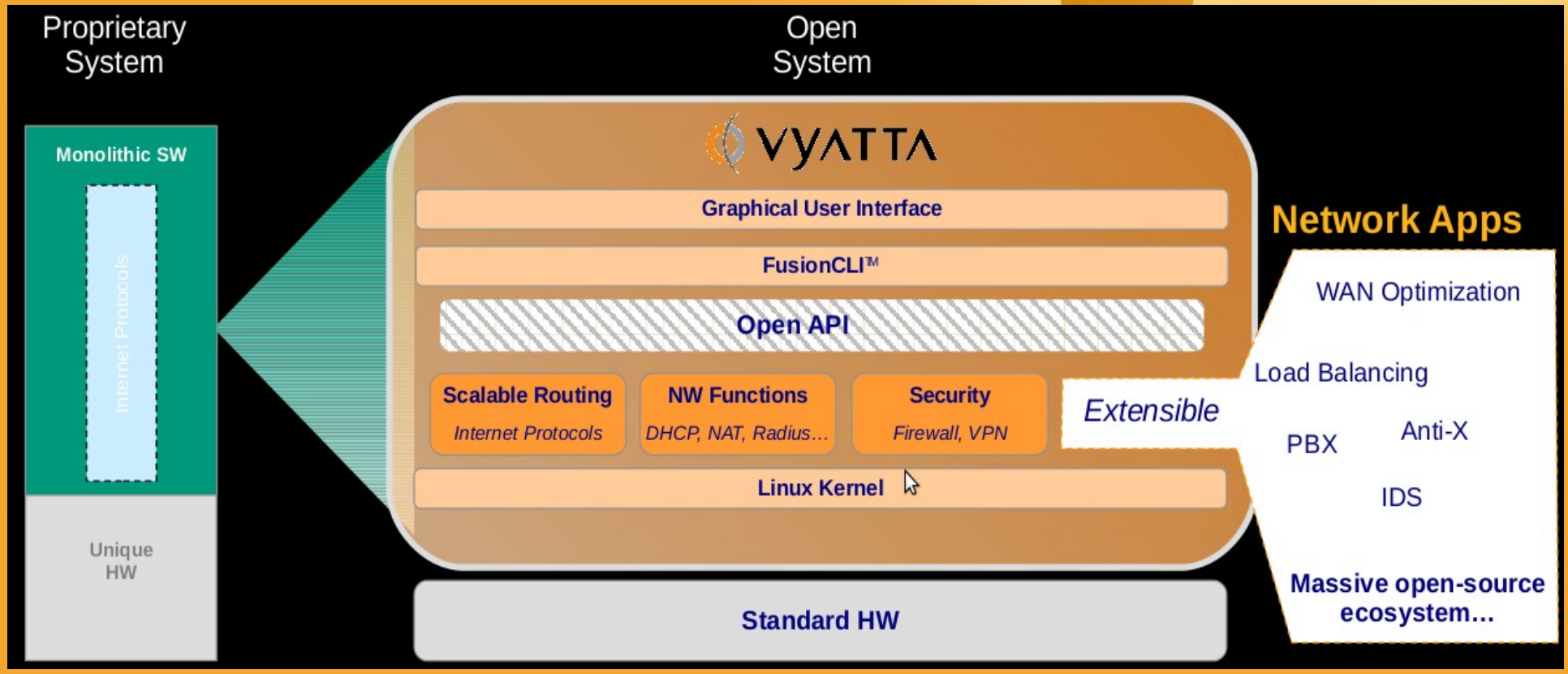
-Inicio de Live CD, ISO de x86 o virtualizadas

-Opciones del modo de instalación Imagen/system

Implementación de Vyatta en la UNQ



Implementación de Vyatta en la UNQ



Modos de configuración

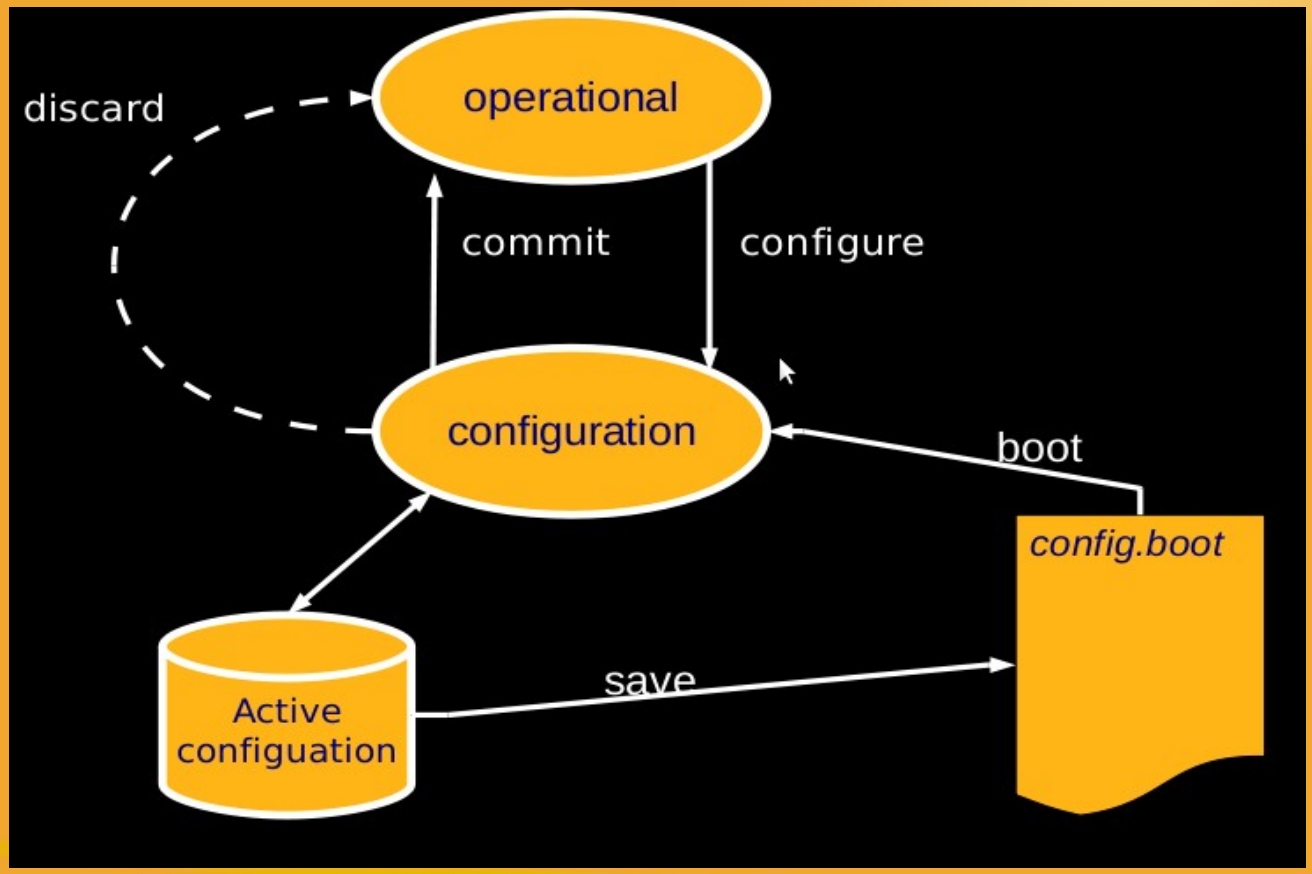
-Acceso CLI y GUI (a partir de v6.3 SE)

-Modo Operacional

-Modo Configuración

-Se configura y luego se aplica (commit)

Lógica de funcionamiento



Implementación de Vyatta en la UNQ

```
set system host-name FW-Bernal
set system gateway-address 10.253.253.253
set system name-server 8.8.8.8
set system ntp server 170.210.73.14
set system time-zone America/Argentina/Buenos_Aires
set interfaces ethernet eth0 address 10.253.253.200/24
```

Muchas Gracias

FIN

Cesar Luis Zaccagnini

Jefe de Departamento de Infraestructura Tecnológica y Telecomunicaciones

cesar@unq.edu.ar

Universidad Nacional de Quilmes