



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

# Infraestructura de red y servicios en el CIPFP Mislata

Ramón Onrubia Pérez  
[ronrubia@fpmislata.com](mailto:ronrubia@fpmislata.com)



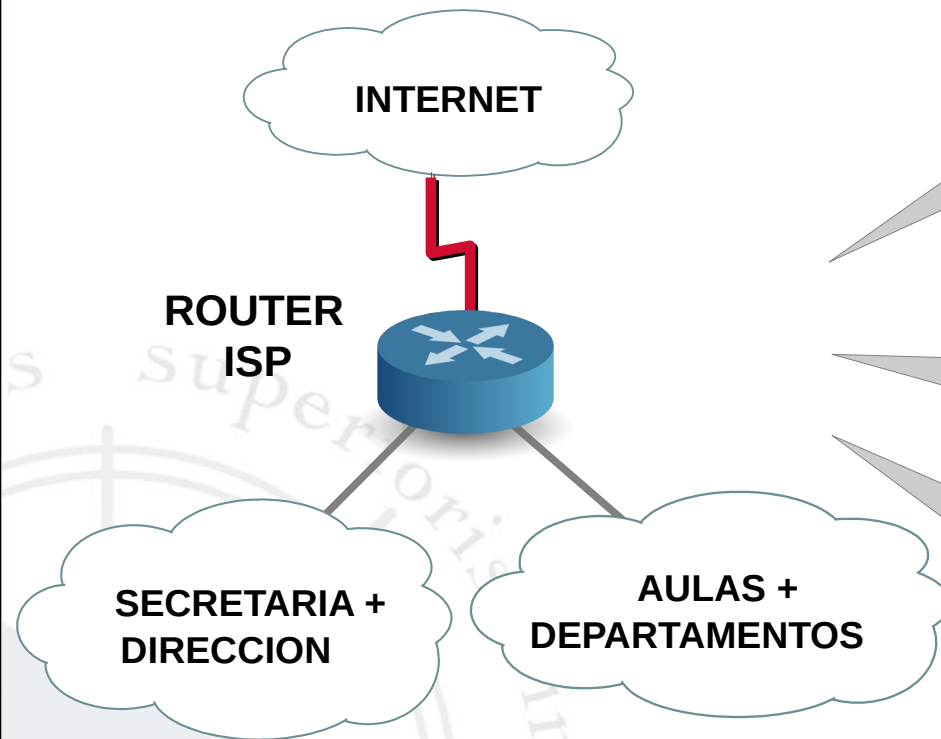
**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Situación de partida

# Modelo de red de centro de Conselleria



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



Modelo simple y sencillo  
de implantar en  
cientos de centros

Diseño **plano**: una subred para  
secretaría-dirección y  
otra para aulas-departamentos

Problemas en aulas/departamentos:

- **Rendimiento**
- **Seguridad**
- **Escalabilidad**

# Rendimiento



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

**Único dominio de broadcast para aulas/departamentos**

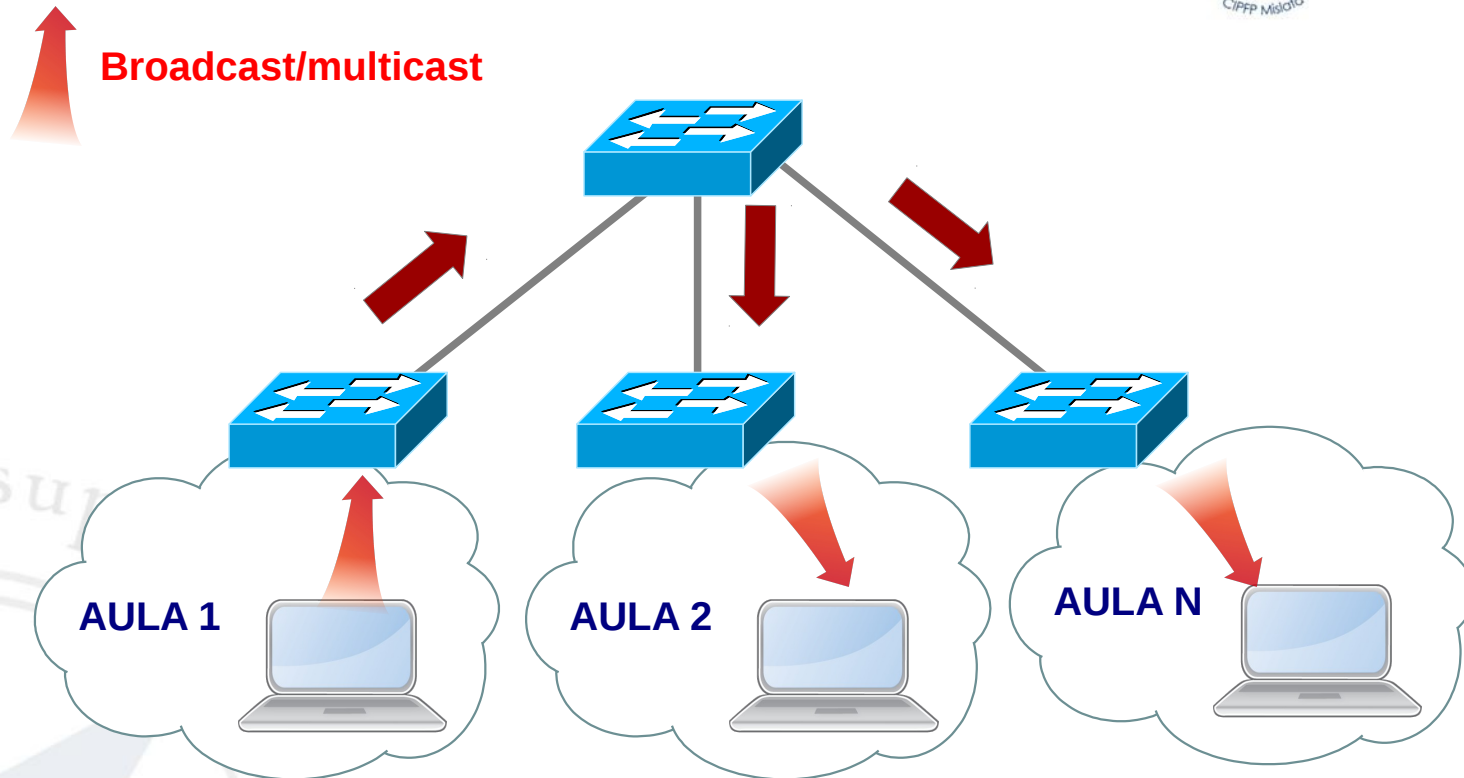
**Problemas en clonación multicast de aulas**

**Problemas en posibles tormentas de broadcast**

# Rendimiento



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



**!!!GRAVE PROBLEMA EN CLONACIÓN MULTICAST DE AULAS!!!**

**POSIBLE SOLUCIÓN: ACTIVAR IGMP SNOOPING/STORM CONTROL**

**→ NO SOLUCIONA EXCESO DE BROADCAST P.EJ.: WORMS**

**SOLUCIÓN ÓPTIMA: SEGMENTAR LA RED CON VLAN'S**

# Rendimiento



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



**Broadcast**

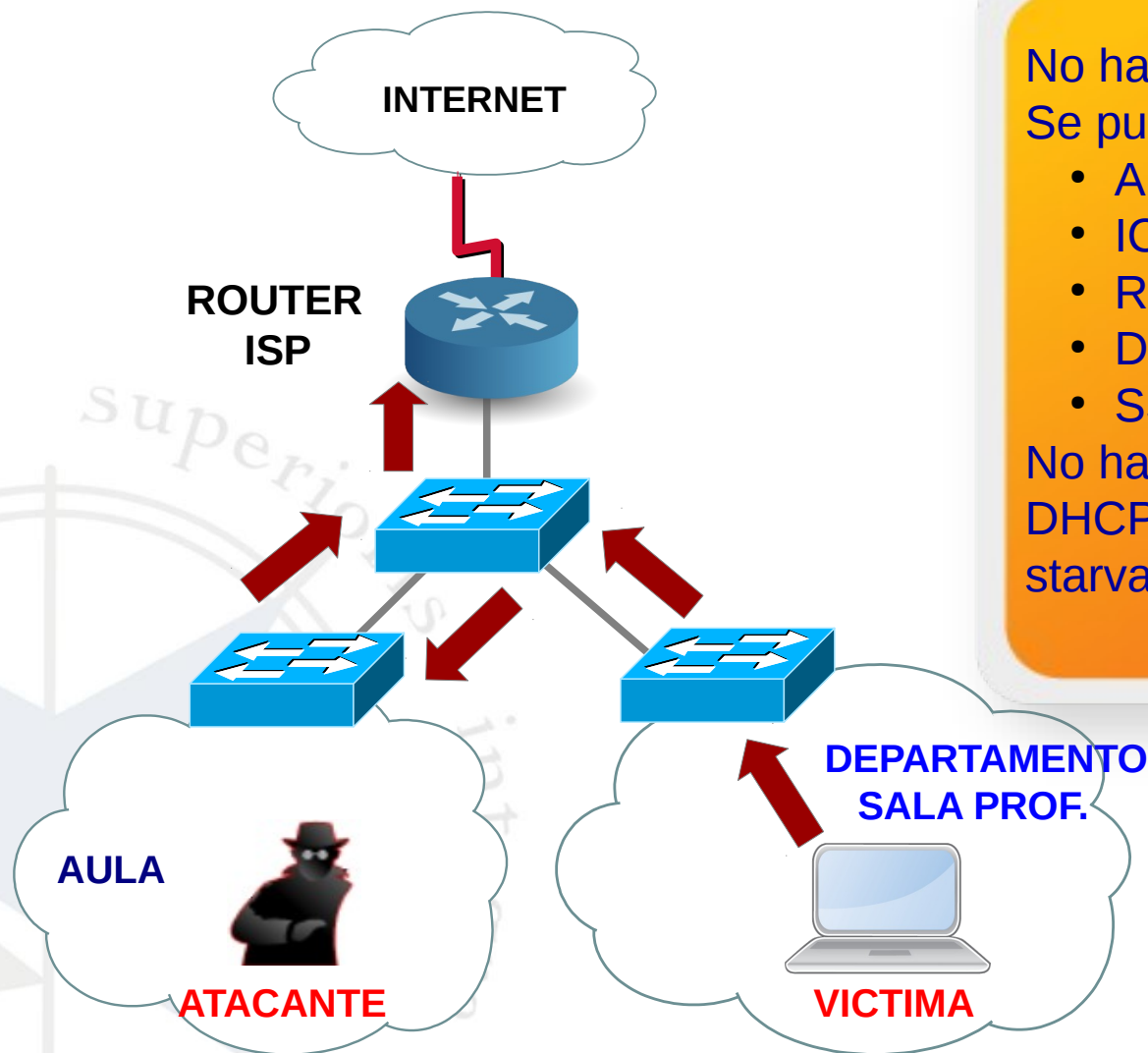


**En ausencia de switches gestionables con  
spanning tree activado se produce  
una tormenta de broadcast  
inutilizando TODA LA RED**

# Seguridad



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



No hay segmentación  
Se pueden hacer ataques MITM:

- Arp poison
- ICMP Redirect/IRDP
- Rogue DHCP/ACK Injection
- DNS Spoofing/Site Spoofing
- SSLStrip/WebMITM

No hay mecanismos de protección  
DHCP ante ataques DHCP  
starvation o rogue DHCP



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# **Necesidades y propuestas de mejora en el CIPFP Mislata**



**Rendimiento de la  
red**

**Servicios de red  
confiables**

**Plataforma  
para proyectos**

**Gestión wifi  
unificada**

**Seguridad  
informática**

**Monitorización  
de red y servicios**

**Control de acceso  
a Internet**

**¡¡¡Una solución  
quiero!!!**



# Rendimiento de la red

- Problemas con broadcast/multicast
- Crear dominios de broadcast reducidos
- Aumentar BW interno a 1GE/puesto
- Problema “Netsplit” → segmentos aislados
- Aumentar disponibilidad

# Servicios de red confiables

- Servicios críticos: DHCP, DNS, Proxy, RADIUS, etc
- Tolerancia a fallos
- Servicios en cluster de HA
- Modo activo/pasivo → un servicio está en standby esperando que falle en el nodo principal

# Gestión wifi unificada

- Problema wifi heterogénea, difícil gestión
- Configuración centralizada con controlador
- Soporte de múltiple SSID por AP
- Acceso con WPA2 Enterprise con RADIUS
- Detección de rogue AP's
- Mejora del roaming → BSSID virtual

# Monitorización red y servicios

- **Generar estadísticas de uso**
- **Monitorizar caídas en servicios**
- **Generar alertas ante fallos**
- **Diagnóstico de fallos y detección de problemas de rendimiento**

# Control de acceso a Internet

- No existía control en el aula por el profesor
- Desarrollar aplicación intuitiva para profesorado
- Interfaz web multiplataforma
- Bloquear aplicaciones de túneles para saltar filtros de contenidos (Ultrasurf, Tor, etc)

# Seguridad informática

- Separar los segmentos de red (VLAN) con seguridad perimetral
- Evitar o detectar ataques MITM
- Generar alertas ante ataques
- Evitar suplantaciones DHCP

# Plataforma para proyectos de alumnos

- **Infraestructura de virtualización para proyectos de alumnos**
- **Optimización del uso de recursos compartidos**
- **Ubicuidad: accesible desde Internet**





**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

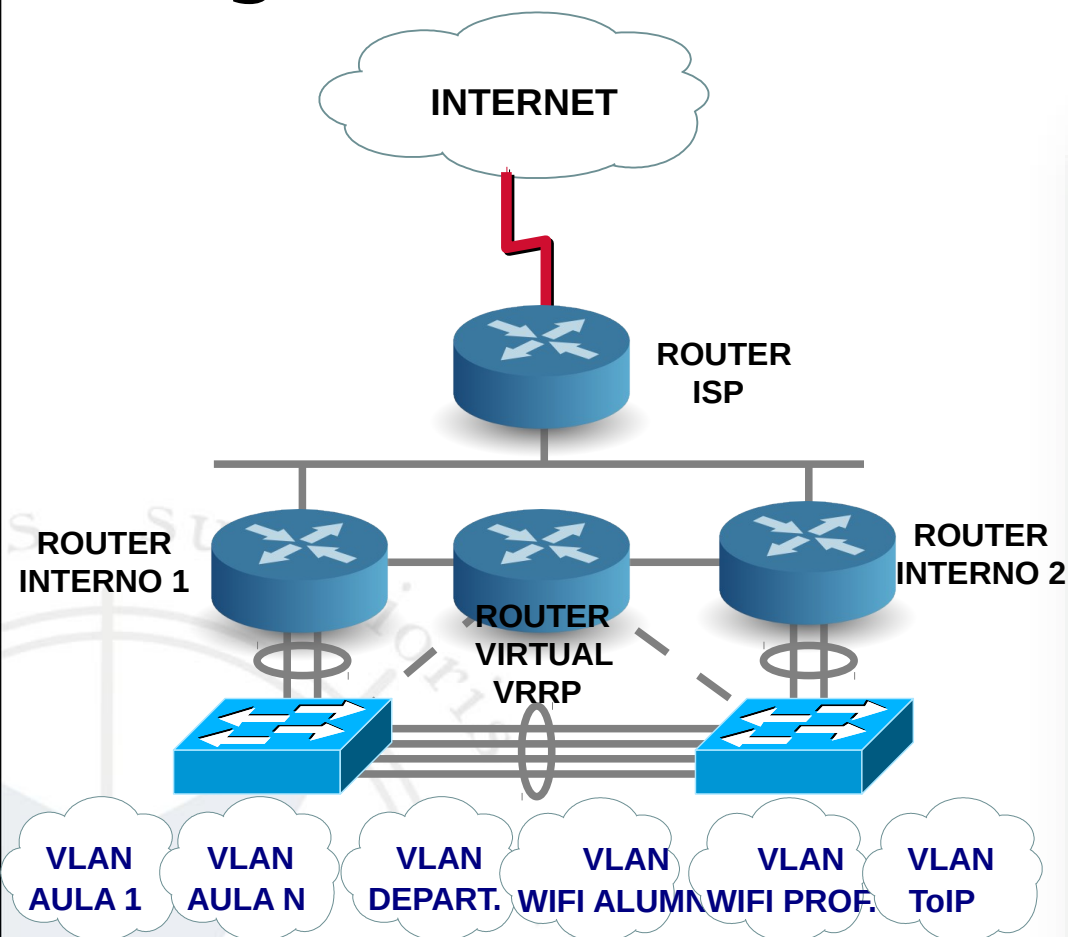
# Infraestructura de red



# Segmentación en VLAN's



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



- Segmentación en VLAN's con asignación de subredes a partir de 172.16.0.0/16
- Dominios de broadcast reducidos
- Contención de broadcast (STORM control)
- 35 VLAN/subredes actualmente
- Dos routers intermedios con NAT en alta disponibilidad (VRRP)
- Balanceo estático de VLAN's
- VLAN de ToIP en alta prioridad
- Conmutadores de GE con enlaces LACP en alta disponibilidad + RSTP + 802.1Q

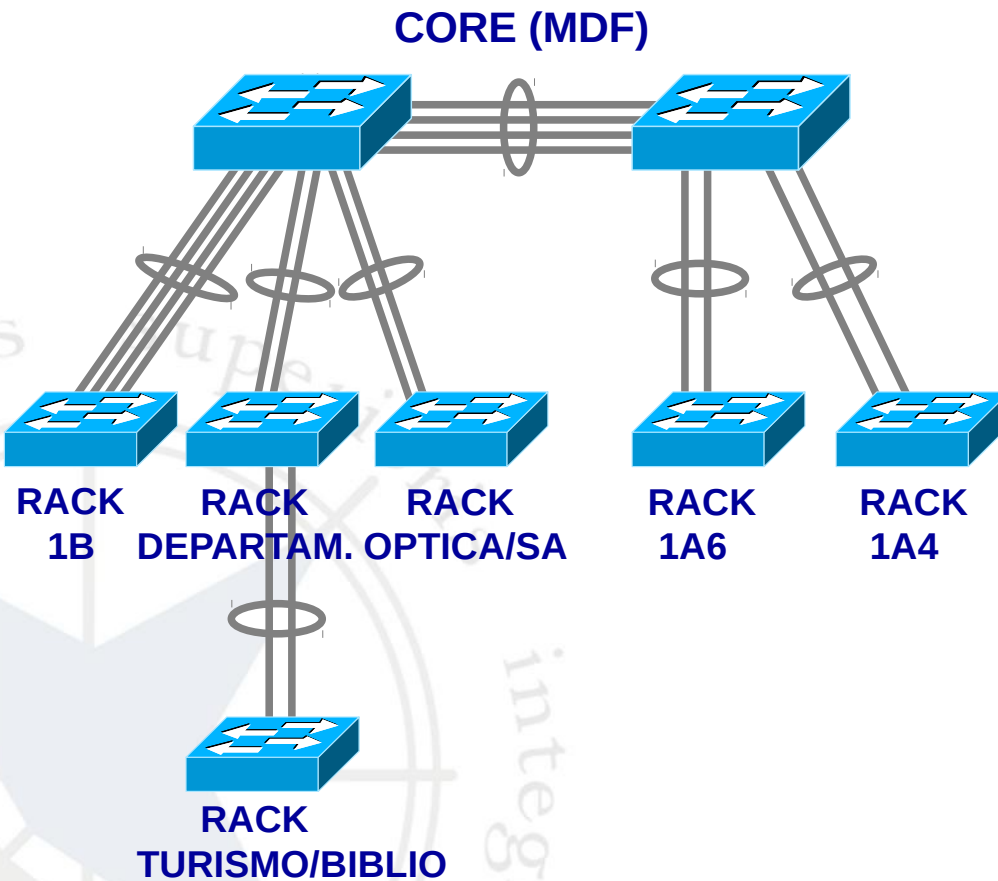
# Enlaces IDF con MDF

IDF: Rack intermedio

MDF: Rack principal



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



- No se han representado todos los racks por simplificar
- Los enlaces entre switches en los racks intermedios con el core de la red se hace con agregación de puertos (LACP 802.3ad)
- Las tramas se van balanceando por los miembros del LAG
- Aumenta BW disponible y la disponibilidad ante fallo de un cable o puerto



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Wifi Unificada



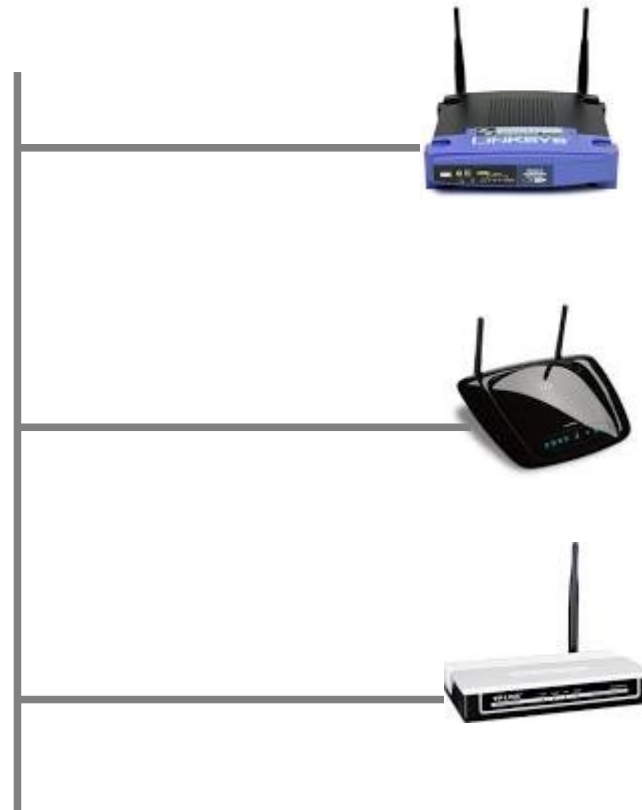
# Situación de partida



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- AP's standalone, con configuración distribuida e independiente
- Cada AP de distintos fabricantes
- Dificultad de gestión con muchos AP's
- No hay integración en el funcionamiento ni en la gestión de los AP
- Problemas para crear varios SSID
- No hay detección de rogue AP's, virtual BSSID, etc

## Extended Service Set (ESS)

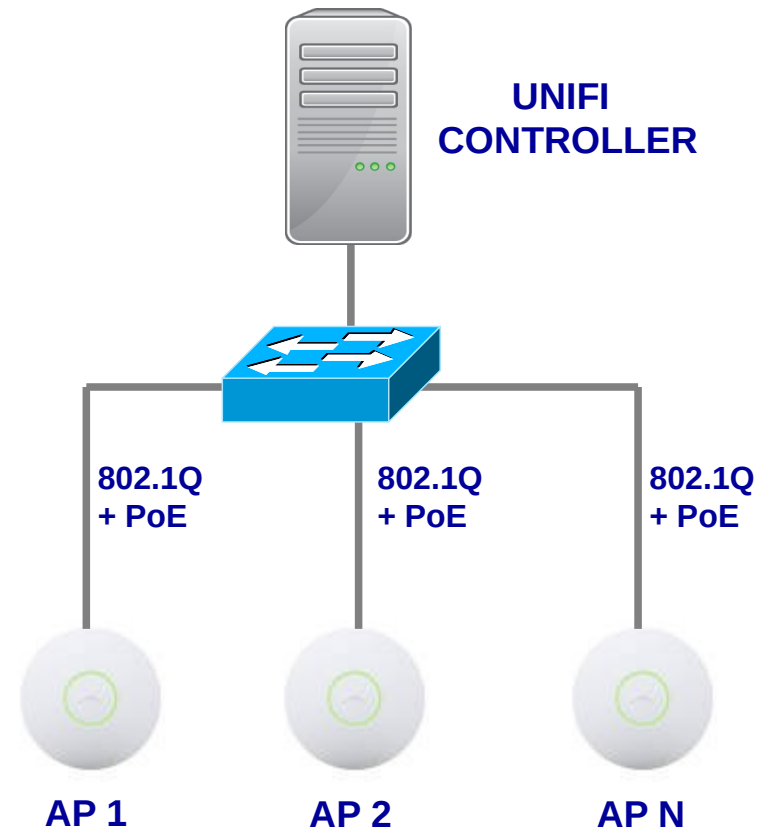


# Wifi Unificada



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- AP's ligeros, con configuración centralizada y gobernados por controlador
- Fabricante Ubiquiti, UAP LR
- Calidad/precio muy buena
- Alimentados por Ethernet (PoE)
- Facilidad de gestión y escalabilidad
- Despliegue de configuración a cientos o miles de AP's
- Múltiple SSID → VLAN por SSID
- Ajuste automático de canales
- Detección de rogue AP's, virtual BSSID, Zero Handoff, etc

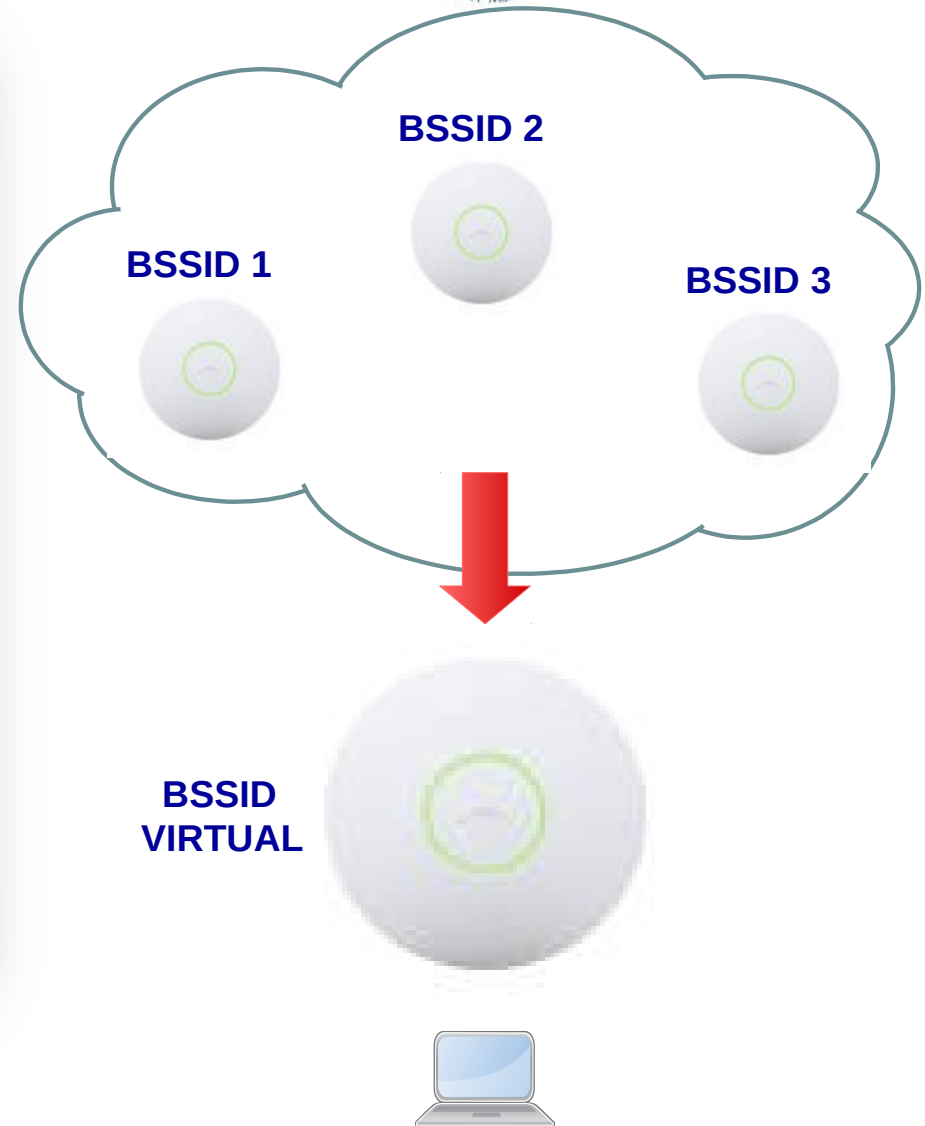


# Virtual BSSID o Virtual Cell



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

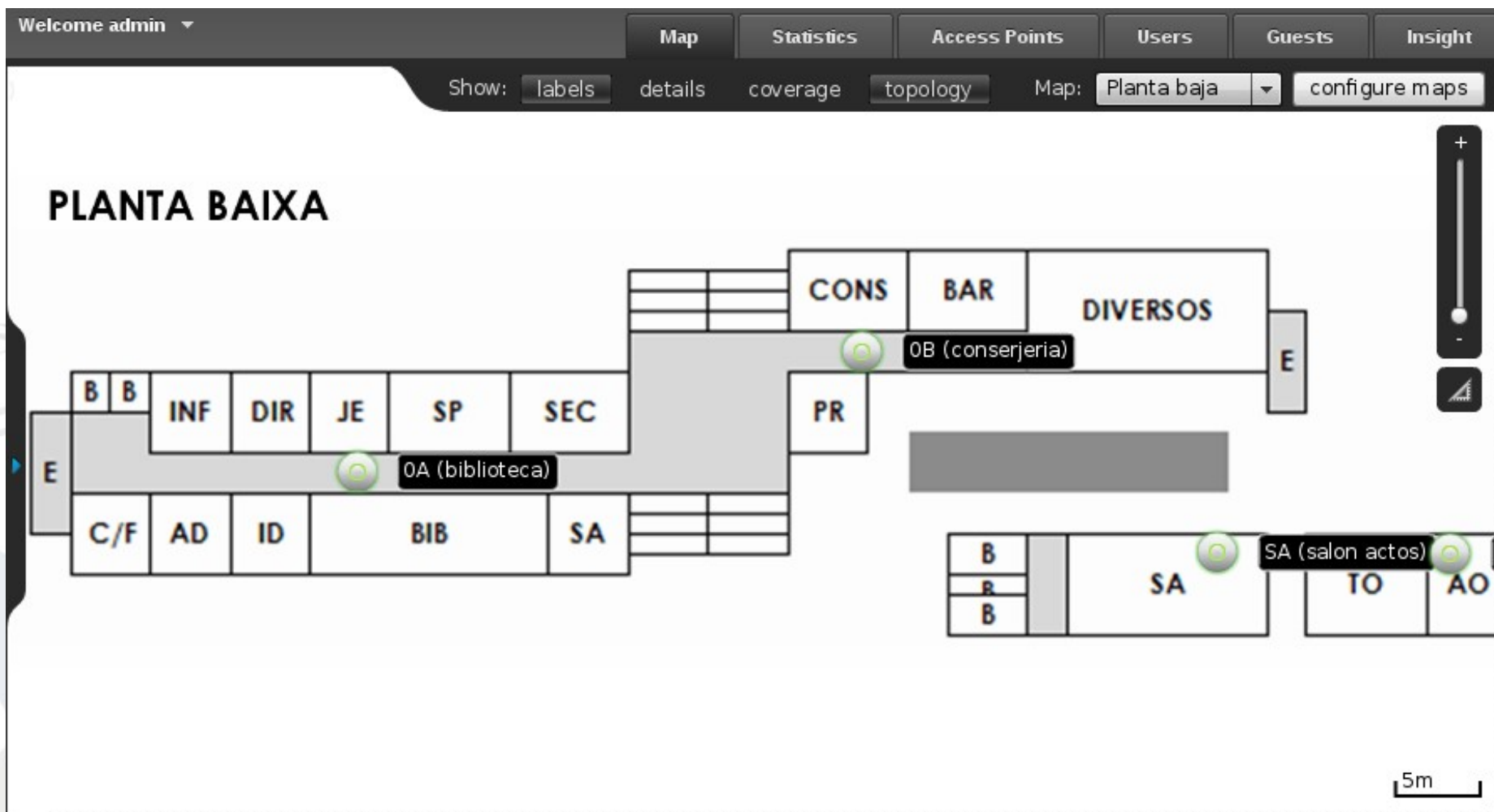
- Con la versión 3.X.X del firmware
- En vez de varios AP con diferentes BSSID, la red se presenta al cliente como un gran AP con un sólo BSSID y un gran radio de cobertura → Celda Virtual
- Ventaja: no hay roaming → Zero Handoff
- No hay cortes en sesiones VoIP, descargas, etc



# Controlador Wifi - Mapa



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

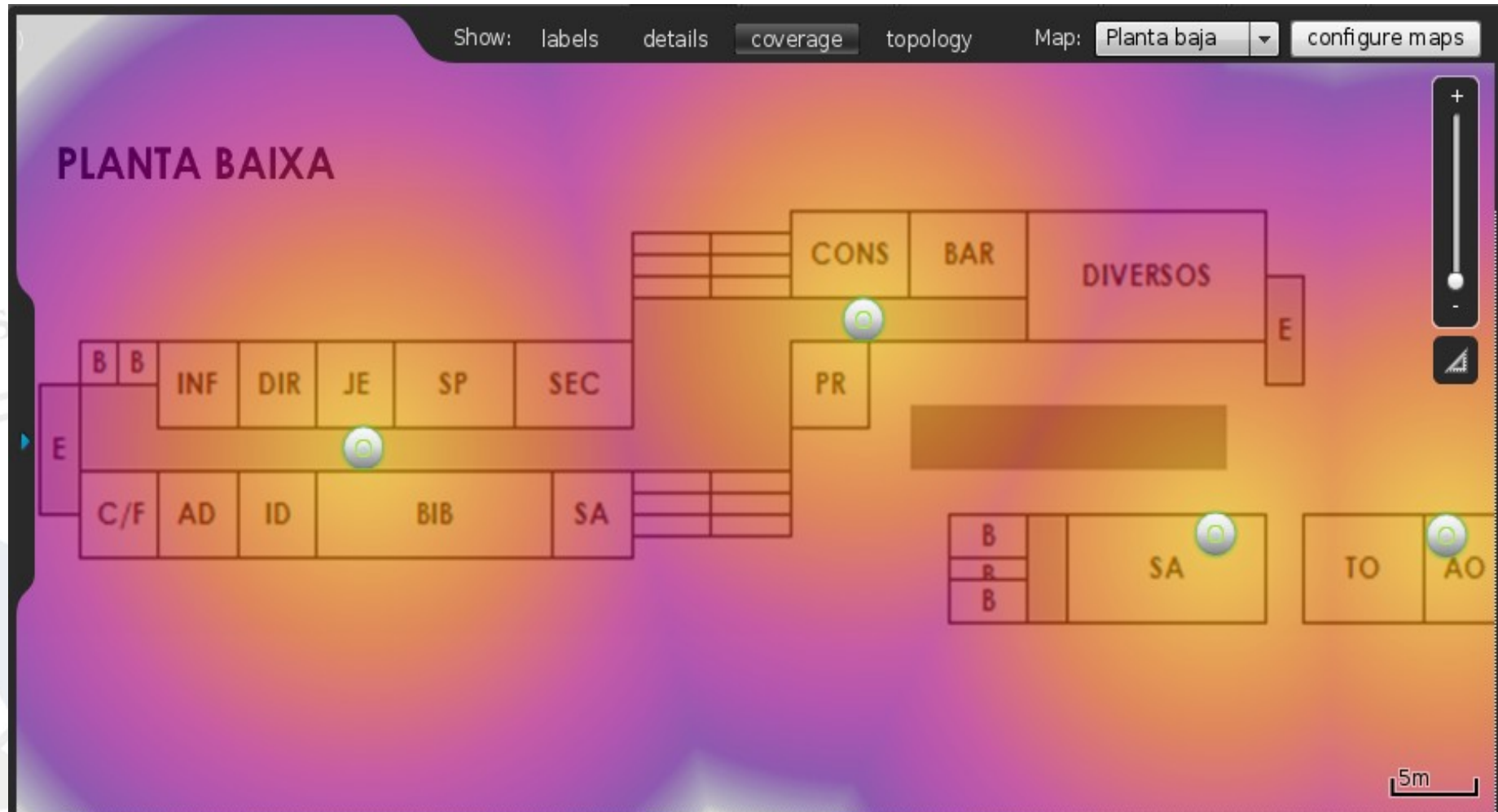




# Controlador Wifi - Cobertura



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Controlador Wifi - AP's



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Welcome admin ▾

Map Statistics Access Points Users Guests Insight

Managed Access Points Page Size 10 ▾

Search Overview Config Performance start rolling upgrade

◆	◆ Name/MAC Address	◆ IP Address	▼ Status	◆ Num Clients	◆ Download	◆ Upload	◆ Channel	Actions
🟢	SA (salon actos)	172.16.1.24	Connected	5	3.82G	350M	1 (ng)	<span>Restart</span> <span>Locate</span>
🟢	0A (biblioteca)	172.16.1.20	Connected	3	19.8G	2.41G	11 (ng)	<span>Restart</span> <span>Locate</span>
🟢	0B (conserjeria)	172.16.1.21	Connected	11	5.76G	1.15G	1 (ng)	<span>Restart</span> <span>Locate</span>
🟢	1A (aula 1A2)	172.16.1.22	Connected	14	28.0G	2.92G	1 (ng)	<span>Restart</span> <span>Locate</span>
🟢	TO (taller optica)	172.16.1.25	Connected	0	1.63G	949M	6 (ng)	<span>Restart</span> <span>Locate</span>
🟢	2B (aula 2B4)	172.16.1.23	Connected	10	35.8G	4.35G	11 (ng)	<span>Restart</span> <span>Locate</span>

1 - 6 / 6

# Controlador Wifi – Rendimiento



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Welcome admin ▾

Map

Statistics

Access Points

Users

Guests

Insight

## Managed Access Points

Page Size 10 ▾

Overview

Config

Performance

start rolling upgrade

↕	↕ Name/MAC Address	↕ IP Address	▼ Status	↕ 2G Clients	↕ 5G Clients	↕ TX	↕ RX	TX 2G	TX 5G	↕ Channel
🟡	SA (salon actos)	172.16.1.24	Connected	5	0	251K	56.2K	<div><div></div></div>	1 (ng)	
🟡	0A (biblioteca)	172.16.1.20	Connected	3	0	16.6K	746	<div><div></div></div>	11 (ng)	
🟡	0B (conserjeria)	172.16.1.21	Connected	11	0	125K	39.8K	<div><div></div></div>	1 (ng)	
🟡	1A (aula 1A2)	172.16.1.22	Connected	14	0	288K	95.5K	<div><div></div></div>	1 (ng)	
🟡	TO (taller optica)	172.16.1.25	Connected	0	0	10.3K	502	<div><div></div></div>	6 (ng)	
🟡	2B (aula 2B4)	172.16.1.23	Connected	10	0	156K	75.8K	<div><div></div></div>	11 (ng)	

1 - 6 / 6

Centre Integrat Públic  
Formació Professional Superior

21 - 30 / 90

# Controlador Wifi – Usuarios



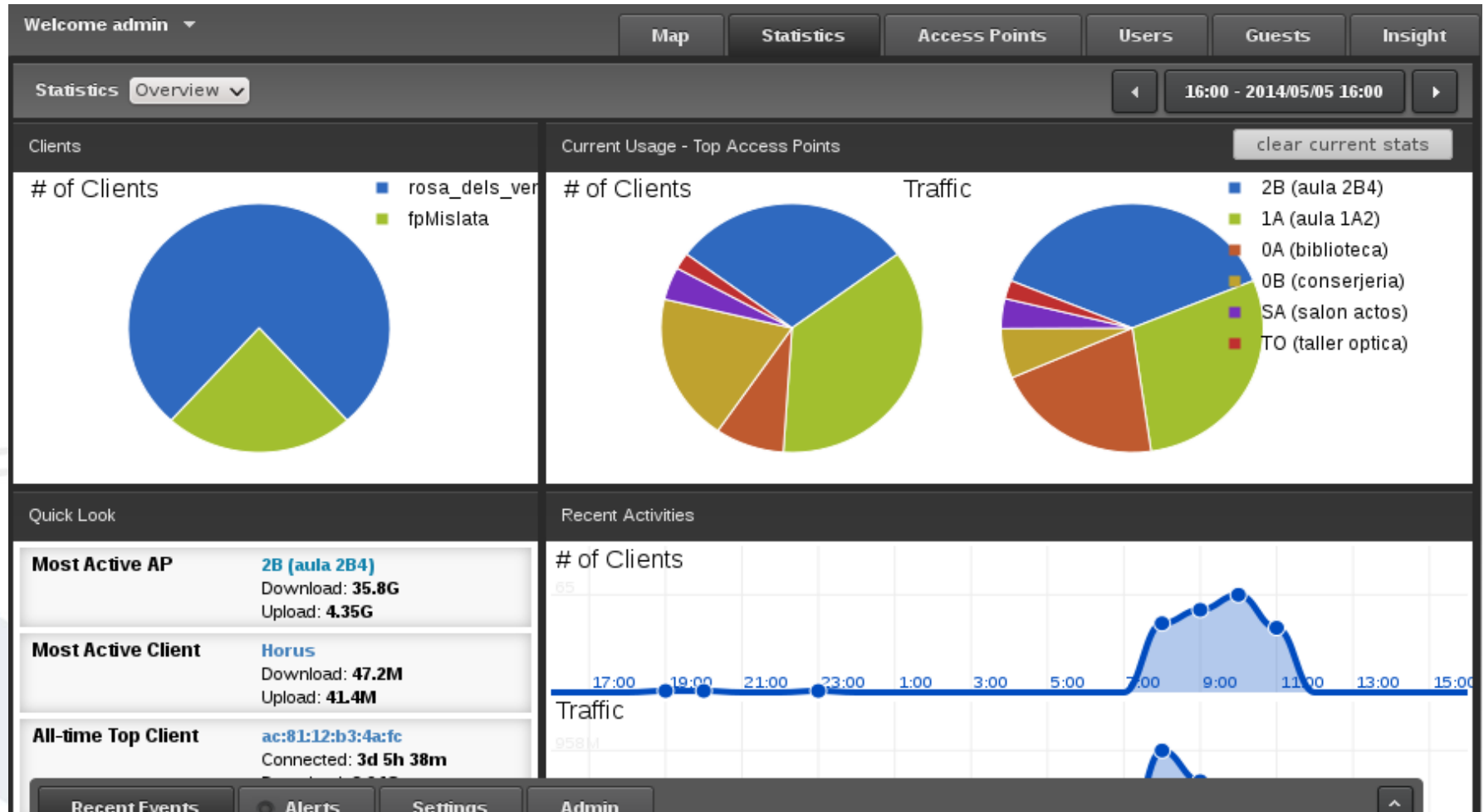
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Active Wireless Users										Page Size 10
Search		2G	5G	All	Filter by AP All					
↕ Name/MAC Address	↕ IP Address	↕ WLAN	↕ Access Point	↕ Signal	▼ Down	↕ Up	↕ Activity	↕ Uptime	Actions	
Nuria-PC	172.16.251.30	rosa_dels_vents	2B (aula 2B4)	59%	70.1M	7.08M		2h 27m 9s	block	reconnect
Sergio	172.16.251.98	rosa_dels_vents	1A (aula 1A2)	84%	49.8M	6.33M		2h 30m 43s	block	reconnect
Horus	172.16.251.77	rosa_dels_vents	1A (aula 1A2)	42%	47.2M	41.4M		2h 33m 28s	block	reconnect
iPad-de-Pedro	172.16.251.121	rosa_dels_vents	2B (aula 2B4)	22%	34.4M	31.1M		15m 12s	block	reconnect
alumno-PC	172.16.251.162	rosa_dels_vents	1A (aula 1A2)	27%	21.3M	6.44M		2h 33m 46s	block	reconnect
android-67e84167e0b9d023	172.16.251.130	rosa_dels_vents	1A (aula 1A2)	35%	20.7M	7.00M		45m 35s	block	reconnect
iPad-de-Jose	172.16.11.40	fpMislata	SA (salon actos)	27%	13.4M	5.73M		2h 18m 29s	block	reconnect
1A5PC01	172.16.11.137	fpMislata	1A (aula 1A2)	69%	13.2M	1.19M		2h 28m 20s	block	reconnect
android-fd5312ded59728a	172.16.251.85	rosa_dels_vents	0B (conserjeria)	15%	12.7M	1.38M		1h 19m 4s	block	reconnect
android-298aab3e64e489b4	172.16.251.163	rosa_dels_vents	0B (conserjeria)	5.0%	4.42M	859K		1h 33m 39s	block	reconnect
1 - 10 / 43										

# Controlador Wifi - Estadísticas



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Controlador Wifi - Alertas



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Recent Events

Alerts

Settings

Admin

Search

Unarchived

All

Archive All

↕ Date/Time	↕ Message	Actions
2014/04/30 14:10:13	AP[0A (biblioteca)] was disconnected	<div>Archive</div>
2014/04/29 10:24:23	AP[2B (aula 2B4)] was disconnected	<div>Archive</div>
2014/04/29 10:24:23	AP[0A (biblioteca)] was disconnected	<div>Archive</div>
2014/04/29 10:24:23	AP[SA (salon actos)] was disconnected	<div>Archive</div>
2014/04/29 10:24:23	AP[TO (taller optica)] was disconnected	<div>Archive</div>
2014/04/29 10:24:22	AP[0B (conserjeria)] was disconnected	<div>Archive</div>
2014/04/29 10:23:42	AP[1A (aula 1A2)] was disconnected	<div>Archive</div>

1 - 7 / 7

# Controlador Wifi – Notificaciones



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Gmail ▾



Mou a la Safata d'entrada



Més ▾

REDACTA

Safata d'entrada (3...

Destacats

Important

Enviats

Esborrany (239)

Correu brossa (44)

Paperera

Alta disponibilitat



[Inicia la sessió al xat](#)

Cerca persones...

[Mantenimiento IFPS Mislata] [UniFi] AP **Disconnected**



Paperera x



UniFi Controller

per a mantenimiento-. ▾

S'ha suprimit el missatge. [Restaura el missatge](#)

You have received a message generated by UniFi Controller

AP Name: OA (biblioteca)

Site: fpmislata (CIPFP Mislata)

Alarm: AP[00:27:22:50:db:48] **was disconnected**

Controller URL: <https://tifton:8443/manage/s/fpmislata>





# Redes Wifi independientes



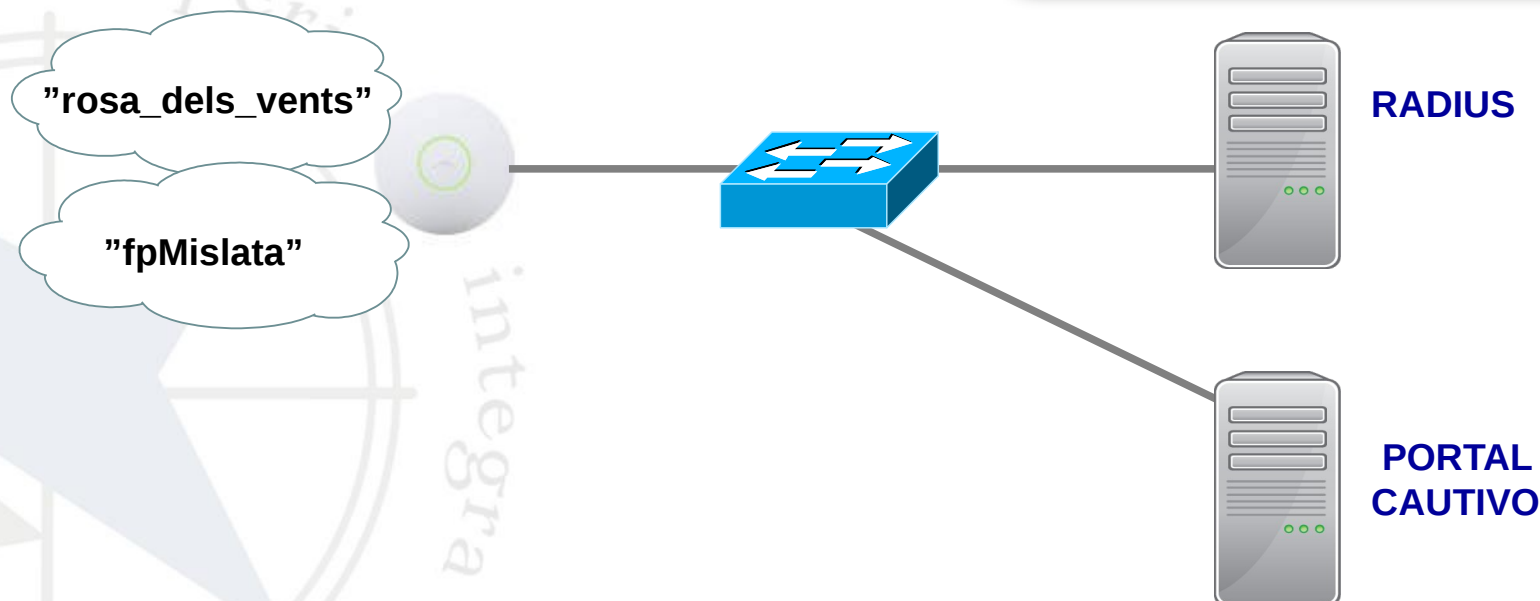
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

## “rosa\_dels\_vents”

- Red abierta con portal cautivo
- Acceso con cuentas del centro (Moodle)
- Acceso solo a Internet
- Sólo para alumnos e invitados

## “fpMislata”

- Protegida con WPA2 Enterprise
- Acceso con cuentas del centro (Moodle)
- Acceso a todos los recursos
- Sólo para profesores

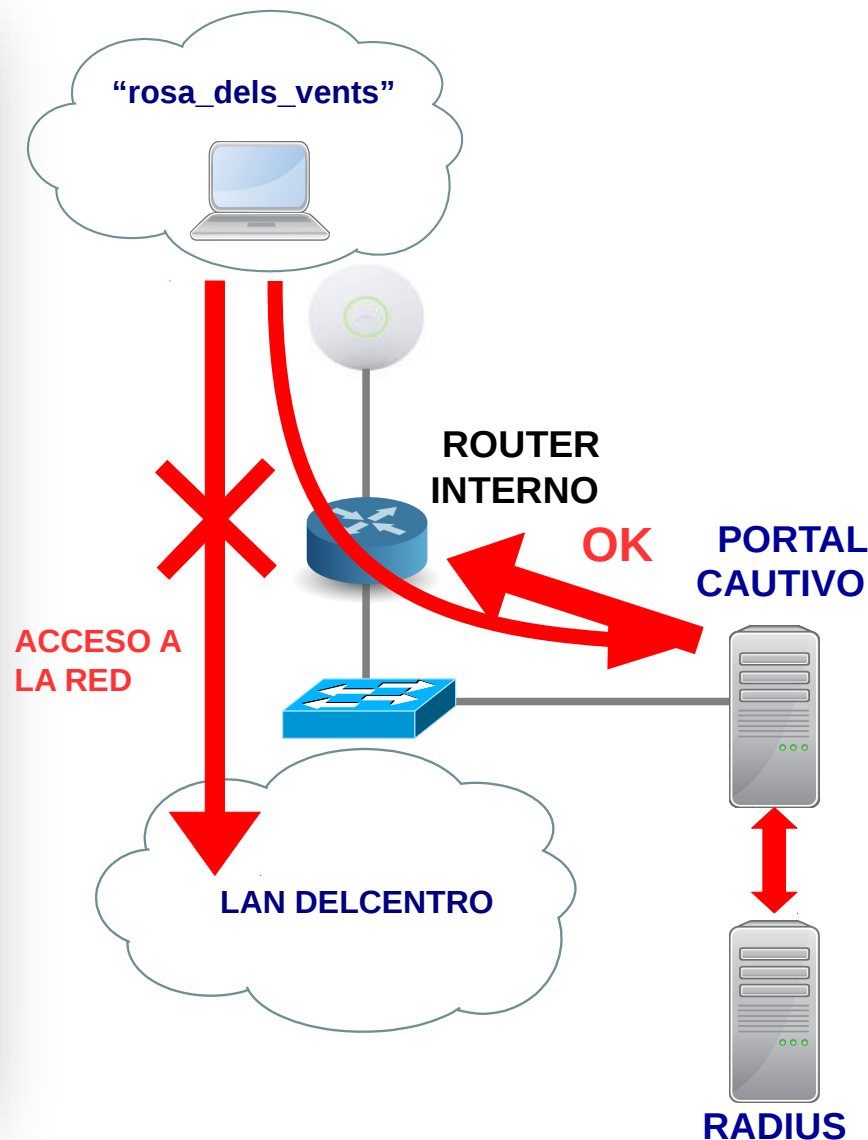


# Portal cautivo



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Sistema para el control de acceso a la wifi del centro
- Desarrollado íntegramente en el CIPFP Mislata con software libre
- Es un sistema como el implantado en hotspots en cafeterías, hoteles, aeropuertos, etc
- El usuario se identifica de forma sencilla a través un portal web, sin necesidad de hacer complicadas configuraciones en la tarjeta inalámbrica
- Sistema de autenticación contra RADIUS y la BBDD usuarios del centro
- Funciona en alta disponibilidad entre los dos servidores del centro



# Portal cautivo - login



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

WIFIportal 1.0

172.16.251.254/login/?gw\_address=172.16.251.253&gw

## WIFIportal 1.0

Identifíquese con su usuario de Moodle

Usuario:

Contraseña:

 Entrar

**El acceso a la red ROSA DELS VENTS está reservado únicamente para usuarios del CIPFP Mislata. Por favor, si usted no es un usuario autorizado, absténgase de entrar.**

Desarrollado por el equipo de mantenimiento de CIPFP Mislata



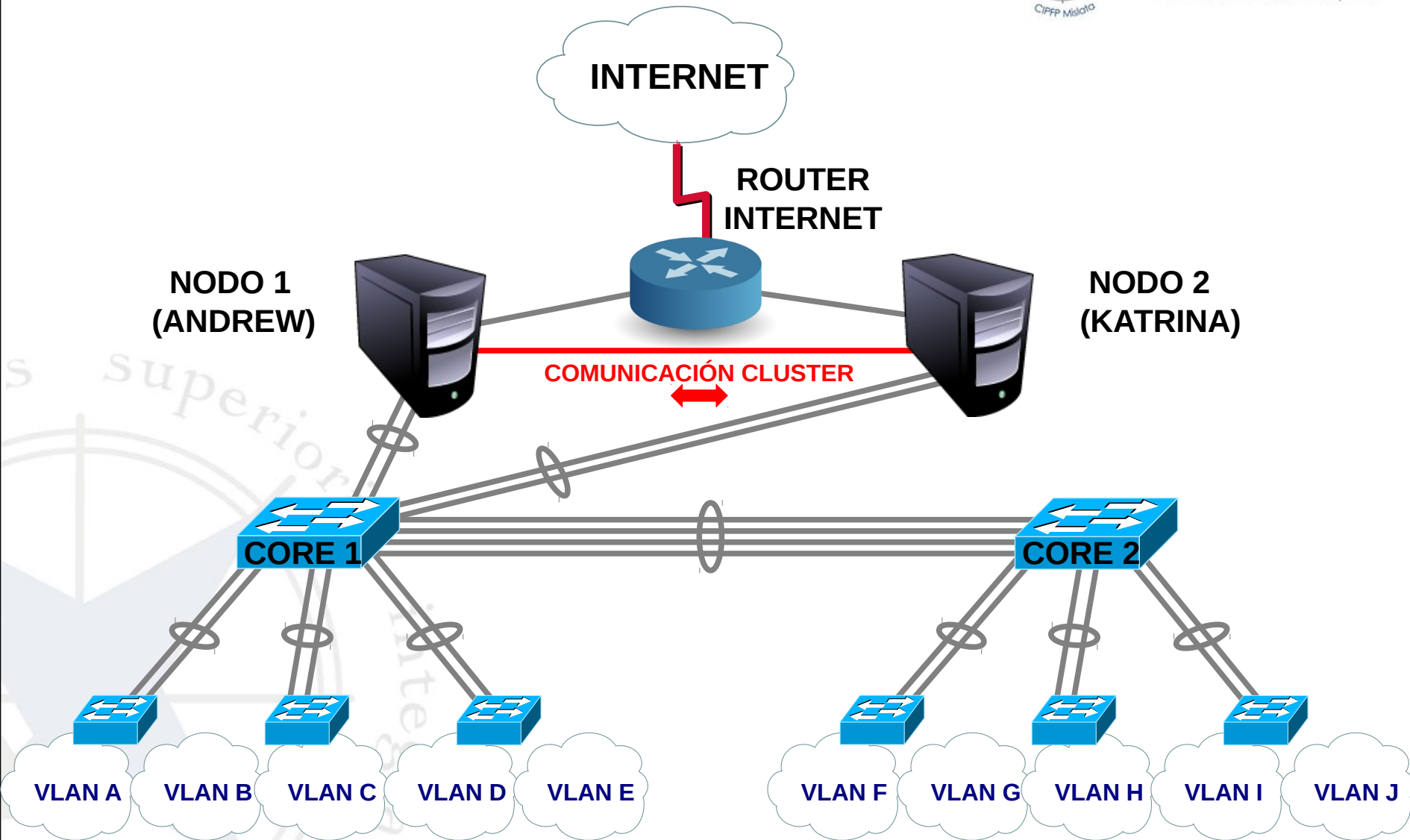
**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Cluster HA de servicios

# Arquitectura física actual



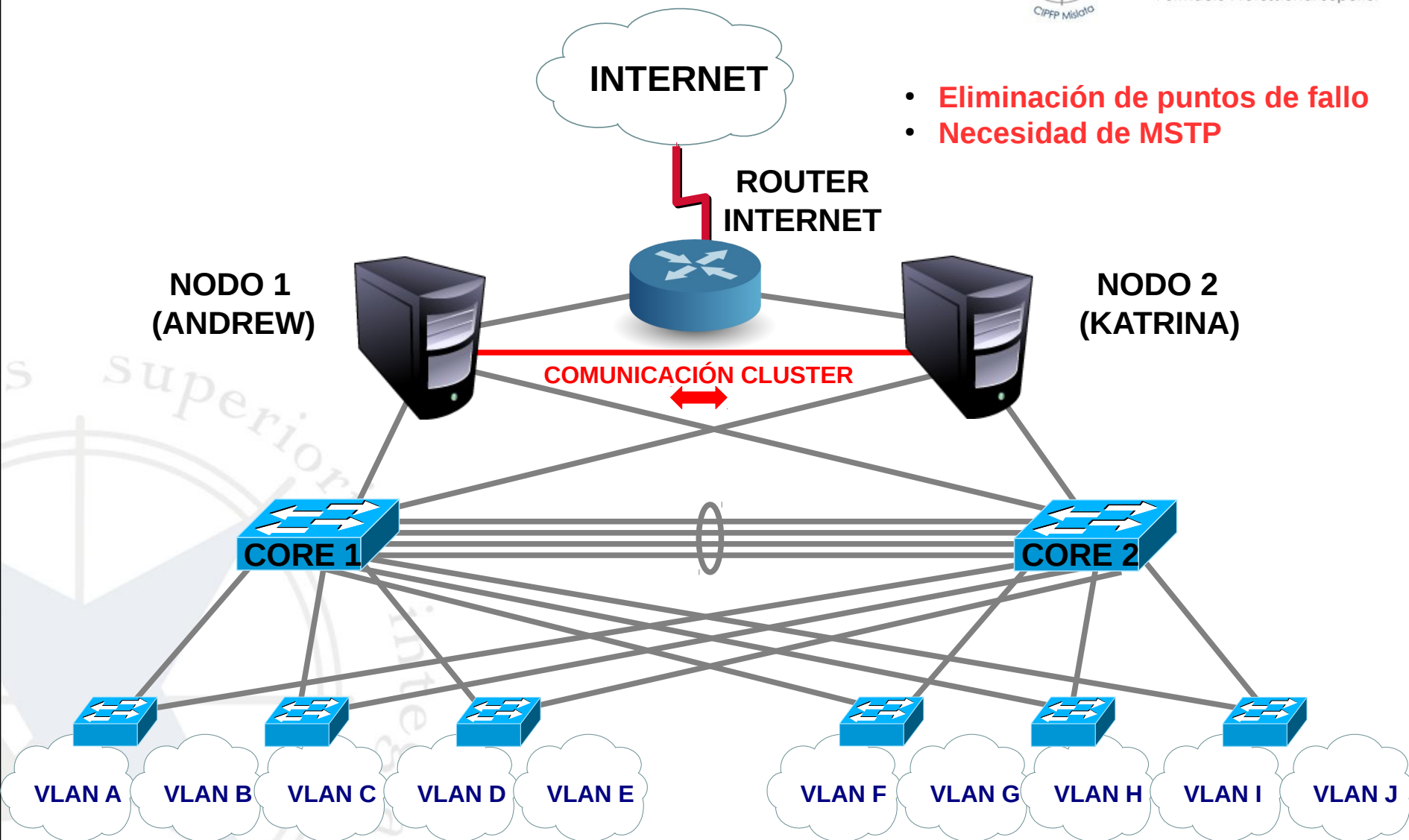
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Arquitectura física futura



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Servicios



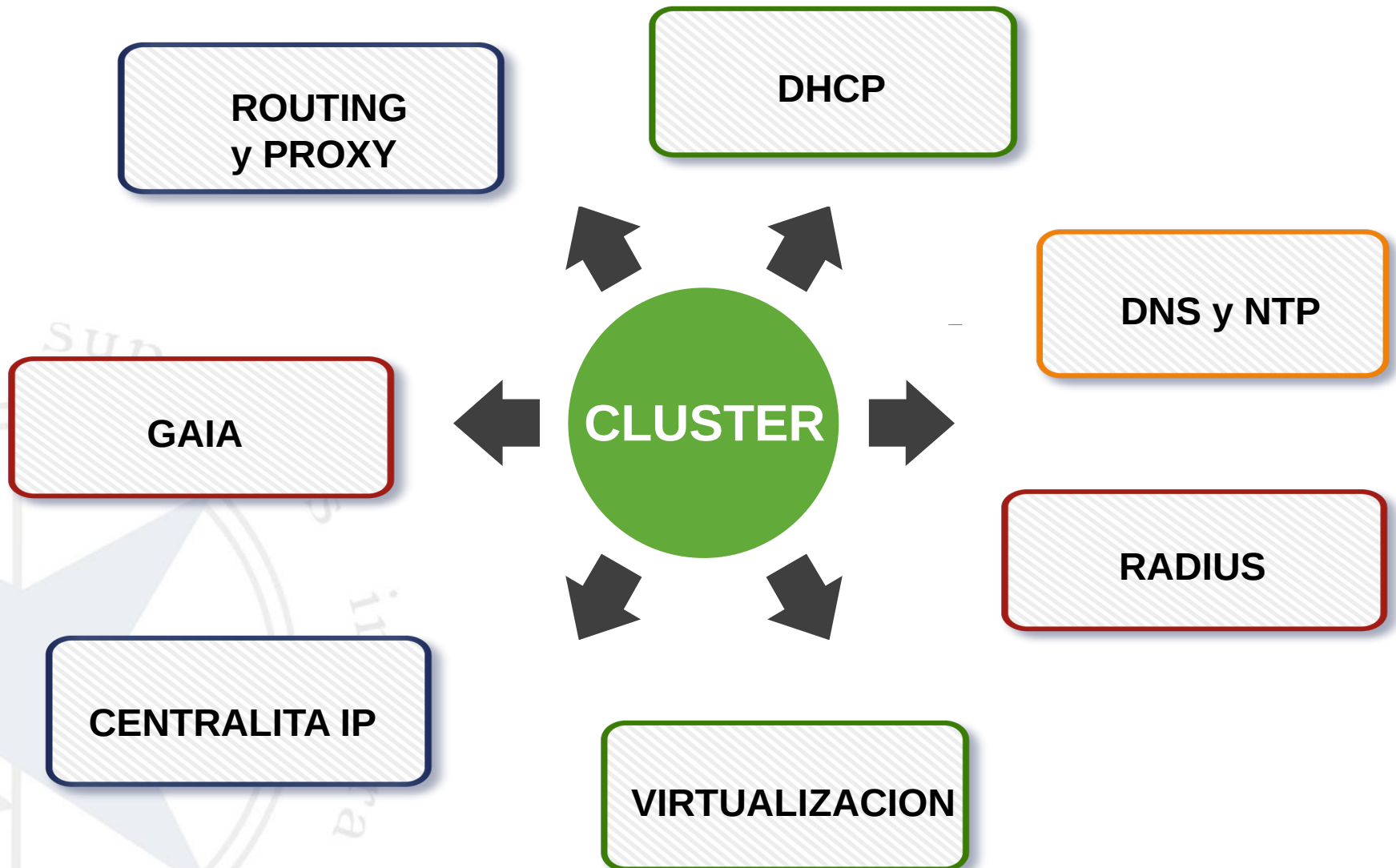
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Ambos servidores ofrecen servicios en **alta disponibilidad** (HA) tanto a aulas como a departamentos, haciendo un reparto de servicios inicial entre ambos
- Los dos servidores funcionan en **cluster activo-pasivo**: ambos funcionan como un único servidor mejorando la **disponibilidad** del conjunto:
  - ✓ Si un servicio falla en un servidor, el otro asume el servicio fallado
  - ✓ Si un servidor entero falla o se apaga el otro asume todas las funciones

# Servicios en HA



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior





# Fallo de un servicio



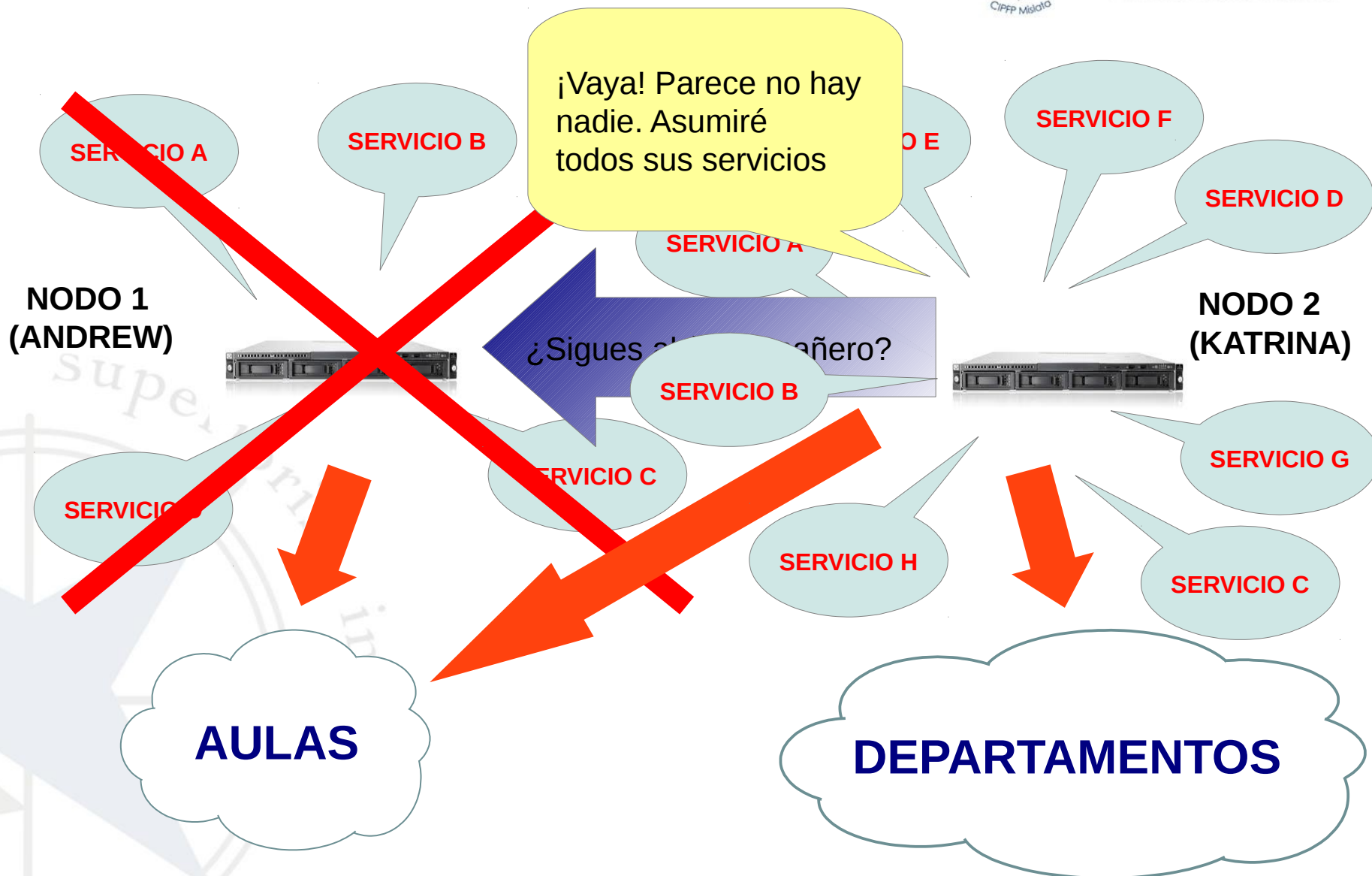
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Fallo de un servidor



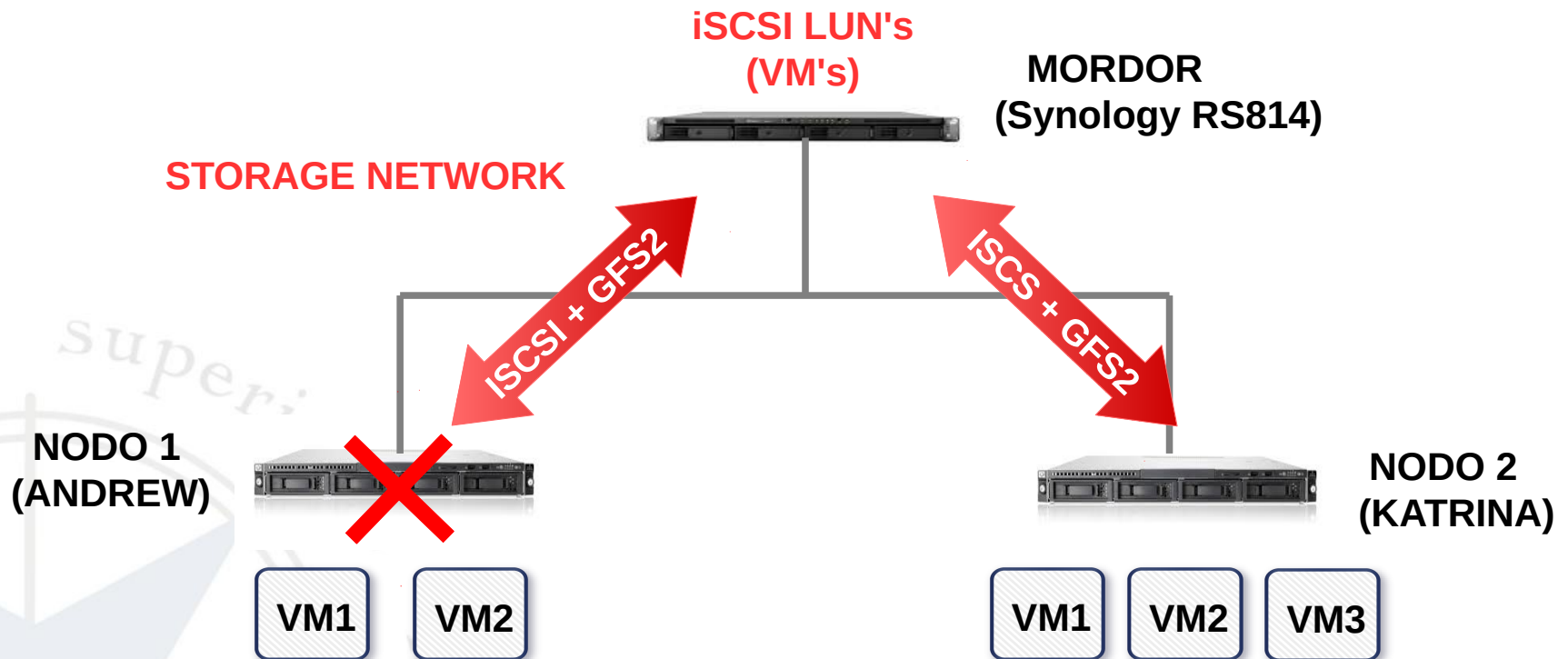
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Virtualización



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Software utilizado



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- **CentOS 6.5:** S.O. compatible binariamente con **RHEL**
- **Keepalived:** paquete para implementar VRRP y LVS (balanceadores) → permite llevar seguimiento de fallos de interfaces y servicios en el cluster y actuar en consecuencia
- **Csync2:** paquete para mantener archivos sincronizados en un cluster. Es un rsync para clusters
- **GFS2** y **CMAN:** gestión de los sistemas de archivos en cluster, montados por ambos con iSCSI
- **VirtualBox** y **KVM:** virtualización. Actualmente Vbox pero en un futuro únicamente KVM para **live migration** de VM's entre nodos almacenadas en iSCSI



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Seguridad



# Seguridad perimetral

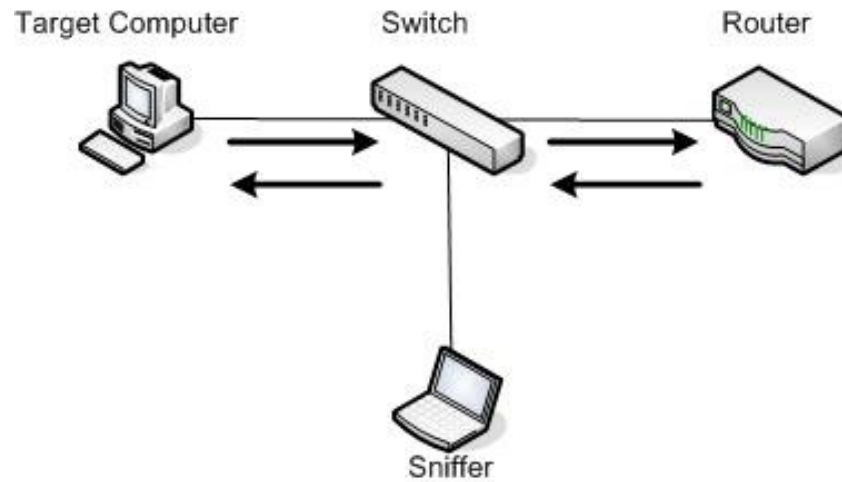


CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

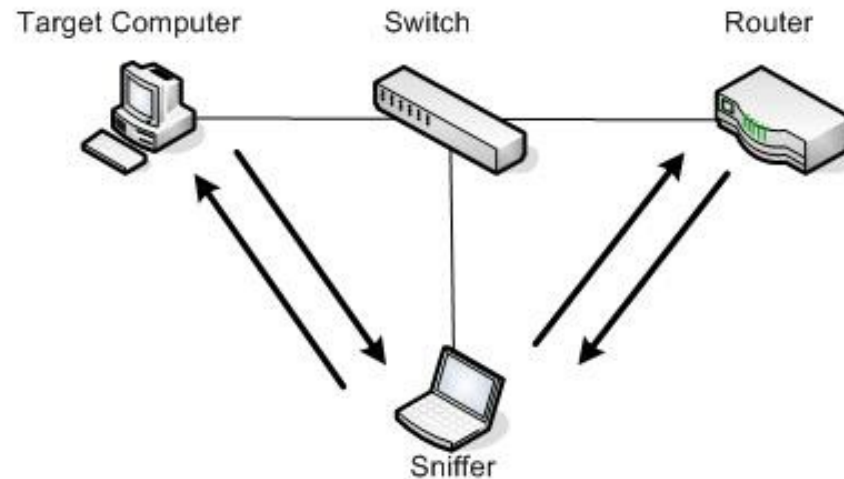
- **Política restrictiva** en las aulas: sólo se permite el tráfico y aplicaciones explícitamente habilitados
- Se utiliza **iptables** en un archivo de configuración sincronizado en el cluster
- **Seguimiento de conexiones**: utilización de **conntrackd** para sincronizar seguimiento de conexiones en el cluster
- **TODO**: implantar un NIDS (Suricata) o HIDS (OSSEC) para detección de ataques internos

# Envenenamiento ARP

Normal Traffic Pattern



Poisoned ARP Cache



# Detección ARP poison



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- **ARP poison** es la base de muchos ataques **MITM**
- Disponible en muchas herramientas al alcance de cualquiera sin ser experto → hemos **sufrido** ataques de este tipo en el centro (ARP Poison, DNS Spoofing, Site spoofing)
- Se detecta con el software **arpalert** instalado en el cluster
- Genera BBDD de **asociaciones MAC-IP** y ante cambios reacciona como se le indique
- En nuestro caso generamos **alerta por email**
- **TODO:** implementar **ARP inspection** en los conmutadores del centro → próxima actualización del firmware



# Alerta ARP poison



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

**Gmail**     **Mou a la Safata d'entrada**  **Més**

**REDACTA**  
**Safata d'entrada (3....)**  
Destacats  
Important  
Enviats  
**Esborrany (239)**  
**Correu brosa (44)**  
Paperera  
**Alta disponibilitat...**


    
[Inicia la sessió al xat](#)

**Mensaje de arpalert: Cambio de mac (posible MITM)**    
 Safata d'entrada x

 **arpalert** 2/5/13   

per a usuari 

Se ha producido la siguiente alerta en la red local  
Cambio de mac (posible MITM): mac=08:00:27:d3:db:28, ip=192.168.0.100, valor anterior al cambio=, NIC=CADMUS COMPUTER SYSTEMS



Feu clic aquí per [Respon](#) o per [Reenvia](#)

# Bloqueo de túneles



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Existen multitud de herramientas para realizar **túneles** SSL/TLS para navegar sin restricciones saltándose los filtros de contenidos de Conselleria: **Ultrasurf**, **Tor**, **SoftEther**, **stunnel**, etc
- No es necesario ser un experto, algunas de ellas no se instalan (ultrasurf)
- Se estudió su comportamiento con analizador de redes
- **Patrón común**: conexiones 443/tcp a IP (no usan nombre dns)

# Posibles soluciones



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- **Listas negras** de IP's → cambian constantemente
- **Lista blanca** de IP's → inviable
- **Inspección HTTPS** → requiere muchos recursos para cifrado/descifrado, generación de “falsos” certificados al vuelo y es un MITM que debe ser consentido por el usuario (derecho fundamental Constitución: secreto comunicaciones)
- **Solución adoptada** → forzar a usar proxy explícito para todo. El proxy deniega conexiones CONNECT 443 a IP

# Proxy explícito



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

## PROS

- Se **fuerza** a que las peticiones https pasen por el proxy, inviable con proxy transparente
- Se guarda en los **logs** los accesos https (ip origen, destino, bytes transferidos, etc)
- **Menos recursos** que https inspection → el proxy no cifra/descifra el tráfico
- Respetamos los **derechos fundamentales** al no interceptar tráfico cifrado

## CONTRAS

- **Todas** las aplicaciones deben soportar proxy explícito → si no soportan, se **deshabilita** temporalmente en el aula con **G.A.I.A.**
- **Configuración manual** de proxy en equipos → solución: descubrimiento automático (WPAD)
- Si **cae** el proxy, no funciona https → solución: proxy en HA en el cluster

# Protección DHCP



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Para **evitar** ataques intencionados o no, es necesario proteger la red de servidores DHCP no legítimos (Rogue DHCP)
- P.ej: típico problema de realización de prácticas DHCP en la red del aula → deben realizarse en redes virtualizadas host-only
- Cisco → **DHCP Snooping**
- DLINK, Netgear → **DHCP Server Screening**
- En ambas soluciones se marcan los puertos a los que se conectan el servidor o servidores DHCP legítimos de la red como confiables y el resto no confiables



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# G.A.I.A.



- Sistema para la **Gestión del Acceso a Internet en Aulas**
- Desarrollado íntegramente en el CIPFP Mislata con **software libre** (coste cero)
- Permite a un profesor desde **cualquier ordenador** del centro controlar el acceso a Internet de un aula
- Se accede **fácilmente** desde el navegador: <http://gaia>
- Sistema de identificación **integrado** con Moodle: el profesor se identifica con el usuario y contraseña de Moodle → no es necesario aprender un usuario y contraseña nuevos

- El ordenador del profesor **siempre** tiene acceso a Internet, no le afecta el estado del aula
- Queda **registrado** en el panel de la aplicación, la última persona que ha modificado el estado de un aula, desde donde y a qué hora
- GAIA funciona en **alta disponibilidad** → el estado de las aulas se sincroniza entre ambos servidores del centro
- **Permite** al profesor:
  - Abrir Internet (con las restricciones de Conselleria)
  - Cortar Internet
  - Dejar acceso sólo al Moodle cortando el resto
  - Dejar acceso a los dominios que el profesor decida: p.ej. un periódico online, la wikipedia, el servef, etc
  - Permitir el proxy transparente para aplicaciones que no soportan proxy



# G.A.I.A. - login



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

## G.A.I.A.

### Gestión de Acceso a Internet para Aulas

**Identifíquese, por favor**

Utilice su nombre y contraseña de Moodle

Nombre de usuario

Contraseña

**El acceso a este sistema está reservado únicamente para profesores. Cualquier intento de acceso con un usuario no autorizado, quedará registrado en el sistema.**

# G.A.I.A. - panel de control



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Ud. está en el sistema como **ronrubia** (Salir)

## G.A.I.A.

### Gestión de Acceso a Internet para Aulas

Usted está en el aula 2A3

Aula	Descripción	Cambiado por	IP	Fecha	Dominios permitidos	Estado aula ?	Ultrasurf/Tor
2A3	1º ASIR	ronrubia	172.16.203.1	29-04-2014 13:06:10	todos	abierto ▼	aplicar desbloquear

### Resto de aulas

Aula	Descripción	Cambiado por	IP	Fecha	Dominios permitidos	Estado aula ?	Ultrasurf/Tor
1A2	Multiusos	jhayA	172.16.102.1	30-04-2014 12:02:56	todos	abierto ▼	aplicar desbloquear
1A3	Multiusos	adelrio	172.16.103.1	02-12-2013 17:28:02	todos	abierto ▼	aplicar desbloquear
1A4	1º GEA y 1º CAE				todos	abierto ▼	aplicar desbloquear
1A5	1º AiF				todos	abierto ▼	aplicar desbloquear
1A6	2º GEA	jmartin	172.16.106.1	18-12-2013 16:43:56	todos	abierto ▼	aplicar desbloquear
2A1	1º DAI	mabellver	172.16.201.101	16-04-2014 12:19:49	todos	abierto ▼	aplicar desbloquear
2A2	2º SMR	isanz	172.16.202.103	15-04-2014 15:28:12	todos	abierto ▼	aplicar desbloquear
2A4	2º ASIR	ronrubia	172.16.204.1	27-03-2014 11:15:00	todos	abierto ▼	aplicar desbloquear

# Alternativas a GAIA



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- En muchos centros, el profesor que quiere cortar Internet tiene que usar **métodos físicos**:
  - ✓ apagar el cuadro eléctrico del aula → nadie puede usar el ordenador
  - ✓ apagar el switch del aula → nadie puede usar la red local ni Internet
  - ✓ desconectar el cable de red del switch → nadie puede usar Internet
- GAIA gestiona el acceso a Internet del aula de forma **lógica**, no **física**
- Las alternativas basadas en un servidor de aula que controla el acceso a Internet presentan un punto de fallo en ese equipo → **GAIA es centralizado** y en **HA** y permite cualquier diseño de red físico



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Monitorización



# Necesidades monitorización

- Generar estadísticas de uso
- Monitorizar caídas en servicios
- Generar alertas ante fallos
- Diagnóstico de fallos y detección de problemas de rendimiento

# NAGIOS Core



- Estandar de facto en monitorización TIC
- Software libre bajo licencia GPLv2
- Existen varias licencias, incluyendo comercial (Nagios XI)
- Monitoriza servicios de red así como servidores, impresoras, infraestructura de red, etc
- Genera informes y alertas ante fallos
- Alternativas: Icinga (fork), Shinken, PandoraFMS, Zabbix, etc

# Sistemas monitorizados

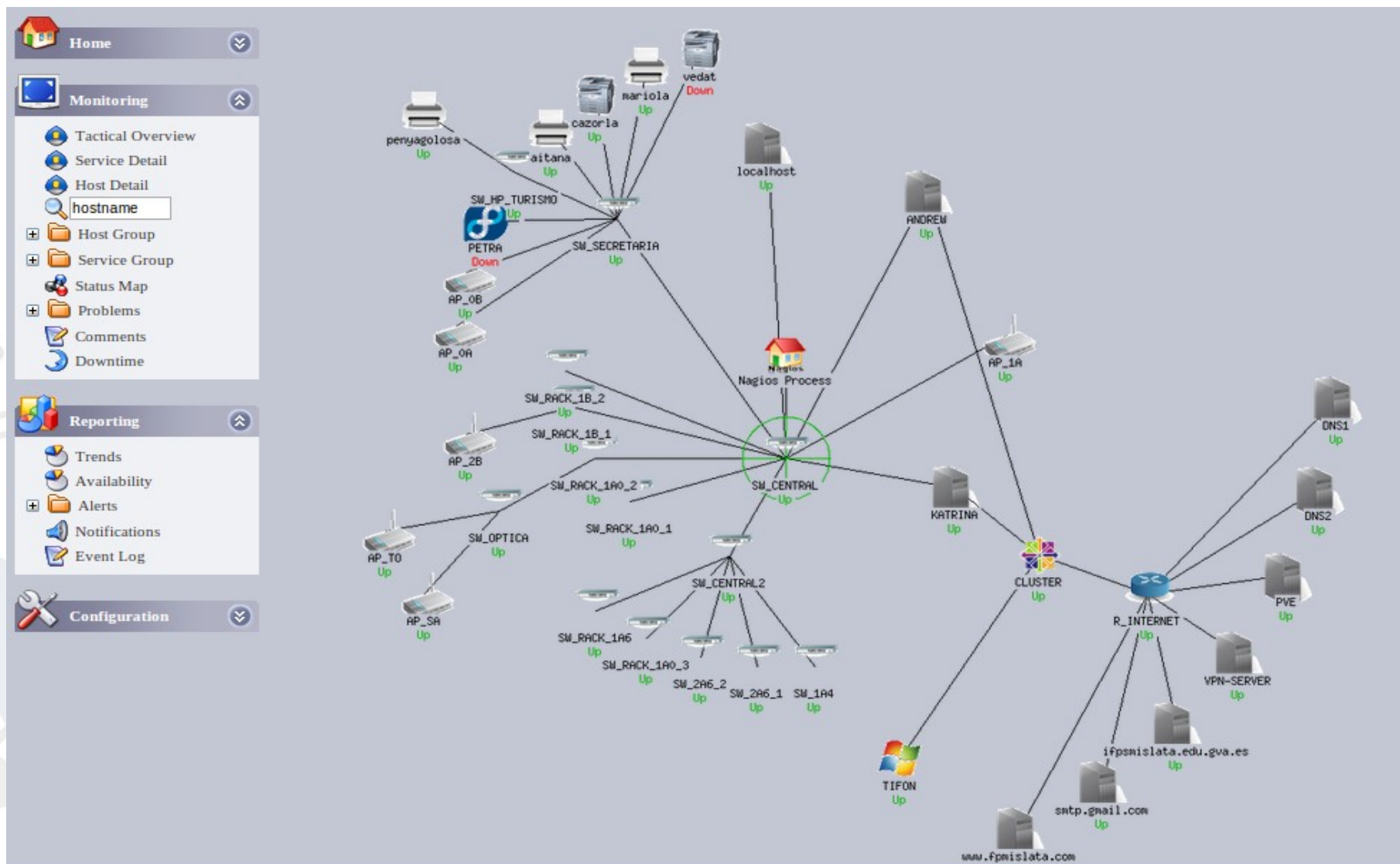


- **Infraestructura:**
  - Conmutadores
  - Routers (Macrolan, internos)
  - AP's (monitorizados también por Unifi Controller)
- **Servicios:**
  - Internos (proxy, dhcp, dns, ntp, radius, gaia, asterisk, etc)
  - Externos (dns conselleria, web del centro, servidor proyectos)
- **Hosts:** Servidores físicos y virtualizados, NAS e impresoras

# NAGIOS - Mapa



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior





# NAGIOS – Tactical Overview



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Home

Monitoring

Tactical Overview

Service Detail

Host Detail

hostname

Host Group

Service Group

Status Map

Problems

Comments

Downtime

Reporting

Trends

Availability

Alerts

Notifications

Event Log

Configuration

Tactical Monitoring Overview

Last Updated: Tue May 6 01:03:53 CEST 2014  
Updated every 90 seconds  
Nagios® Core™ 3.5.1 - www.nagios.org  
Logged in as admin

Network Outages

0 Outages

Hosts

2 Down	0 Unreachable	37 Up	0 Pending
--------	---------------	-------	-----------

2 Unhandled Problems

Services

3 Critical	0 Warning	0 Unknown	87 Ok	0 Pending
------------	-----------	-----------	-------	-----------

1 Unhandled Problems  
2 on Problem Hosts

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Disabled N/A	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled

Monitoring Performance

Service Check Execution Time: 0.01 / 10.02 / 1.722 sec  
Service Check Latency: 0.00 / 0.25 / 0.121 sec  
Host Check Execution Time: 0.13 / 4.08 / 3.619 sec  
Host Check Latency: 0.00 / 0.25 / 0.135 sec  
# Active Host / Service Checks: 39 / 90  
# Passive Host / Service Checks: 0 / 0

Network Health

Host Health:

Service Health:

# NAGIOS – Service Detail



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

**Home**

**Monitoring**

- Tactical Overview
- Service Detail
- Host Detail
- hostname
- Host Group
- Service Group
- Status Map
- Problems
- Comments
- Downtime

**Reporting**

- Trends
- Availability
- Alerts
- Notifications
- Event Log

**Configuration**

**Current Network Status**

Last Updated: Tue May 6 01:04:45 CEST 2014  
Updated every 90 seconds  
Nagios® Core™ 3.5.1 - www.nagios.org  
Logged in as admin

View History For all hosts  
View Notifications For All Hosts  
View Host Status Detail For All Hosts

**Host Status Totals**

Up	Down	Unreachable	Pending
37	2	0	0
<b>All Problems</b>		<b>All Types</b>	
2		39	

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
87	0	0	3	0
<b>All Problems</b>		<b>All Types</b>		
3		90		

**Service Status Details For All Hosts**

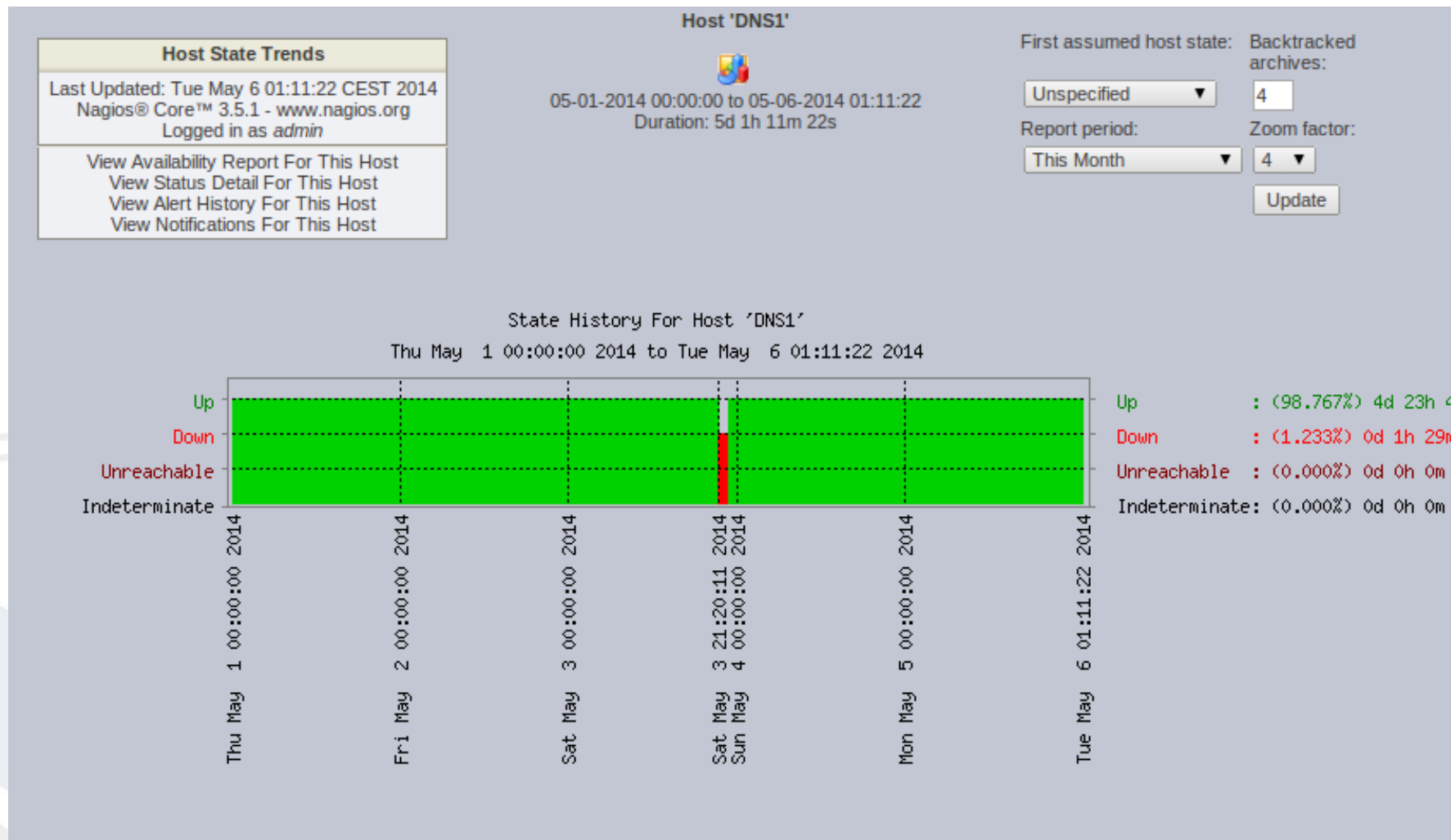
Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ANDREW	PING	OK	05-06-2014 01:03:42 30d 15h 51m 37s	1/3	PING OK - Packet loss = 0%, RTA = 0.60 ms	
	PROXY	OK	05-06-2014 00:56:21 30d 13h 25m 4s	1/3	OK: Proxy server accessible. Run completed in .59 seconds (.32 direct access, .26 proxied)...	
AP_0A	PING	OK	05-06-2014 01:00:01 0d 16h 14m 44s	1/3	PING OK - Packet loss = 0%, RTA = 0.53 ms	
	SSH	OK	05-06-2014 01:03:46 39d 2h 18m 23s	1/3	SSH OK - dropbear_2013.59 (protocol 2.0)	
AP_0B	PING	OK	05-06-2014 01:02:26 0d 8h 12m 19s	1/3	PING OK - Packet loss = 0%, RTA = 0.55 ms	
	SSH	OK	05-06-2014 00:59:06 39d 1h 9m 37s	1/3	SSH OK - dropbear_2013.59 (protocol 2.0)	
AP_1A	PING	OK	05-06-2014 01:03:51 39d 1h 7m 15s	1/3	PING OK - Packet loss = 0%, RTA = 0.97 ms	
	SSH	OK	05-06-2014 00:56:31 39d 1h 11m 50s	1/3	SSH OK - dropbear_2013.59 (protocol 2.0)	
AP_2B	PING	OK	05-06-2014 01:04:11 39d 1h 9m 28s	1/3	PING OK - Packet loss = 0%, RTA = 0.92 ms	
	SSH	OK	05-06-2014 01:03:57 39d 1h 7m 7s	1/3	SSH OK - dropbear_2013.59 (protocol 2.0)	
AP_SA	PING	OK	05-06-2014 01:01:37 39d 1h 11m 41s	1/3	PING OK - Packet loss = 0%, RTA = 0.49 ms	
	SSH	OK	05-06-2014 00:59:17 39d 1h 9m 19s	1/3	SSH OK - dropbear_2013.59 (protocol 2.0)	
AP_TO	PING	OK	05-06-2014 01:04:02 39d 1h 6m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.46 ms	
	SSH	OK	05-06-2014 00:56:42 39d 1h 11m 32s	1/3	SSH OK - dropbear_2013.59 (protocol 2.0)	
CLUSTER	CENTRALITA	OK	05-06-2014 00:59:22 30d 14h 9m 14s	1/3	SIP/2.0 404 Not Found, 0.000946 seconds response time, cnt=1	
	DNS	OK	05-06-2014 01:04:07 30d 14h 55m 15s	1/3	DNS OK: 0.026 seconds response time. www.google.es returns 173.194.41.23 173.194.41.24 173.194.41.31	

# NAGIOS – Reports



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# NAGIOS – Availability Report



**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

## Hostgroup 'electronica'



First assumed host state:   
First assumed service state:   
Report period:   
Backtracked archives:

**Hostgroup Availability Report**  
Last Updated: Tue May 6 01:14:14 CEST 2014  
Nagios® Core™ 3.5.1 - www.nagios.org  
Logged in as admin

05-01-2014 00:00:00 to 05-06-2014 01:14:14  
Duration: 5d 1h 14m 14s

[ Availability report completed in 0 min 0 sec ]

### Hostgroup 'electronica' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
R_INTERNET	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_1A4	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_2A6_1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_2A6_2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_CENTRAL	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_CENTRAL2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_HP_TURISMO	19.767% (19.767%)	80.233% (80.233%)	0.000% (0.000%)	0.000%
SW_OPTICA	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_RACK_1A0_1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_RACK_1A0_2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_RACK_1A0_3	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_RACK_1A6	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_RACK_1B_1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_RACK_1B_2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SW_SECRETARIA	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	94.651% (94.651%)	5.349% (5.349%)	0.000% (0.000%)	0.000%

# NAGIOS – Alertas



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

Gmail ▾



Mou a la Safata d'entrada



Més ▾

REDACTA

Safata d'entrada (3...)

Destacats

Important

Enviats

Esborranys (239)

Correu brossa (47)

Paperera

Alta disponibilitat...



[Inicia la sessió al xat](#)

Cerca persones...

[Mantenimiento IFPS Mislata] \*\* RECOVERY Alerta: SW\_HP\_TURISMO esta UP \*\*



nms.fpmislata@gmail.com

per a mantenimiento-. ▾

S'ha suprimit el missatge. [Restaura el missatge](#)

\*\*\*\*\* Servicio de monitorizacion Nagios de CIPFP Mislata \*\*\*\*\*

Tipo de notificacion: RECOVERY

Anfitrión: SW\_HP\_TURISMO

Estado: UP

Dirección: 172.16.1.12

Info: PING OK - Packet loss = 0%, RTA = 14.29 ms

Fecha/Hora: Mon May 5 08:20:11 CEST 2014



# CACTI



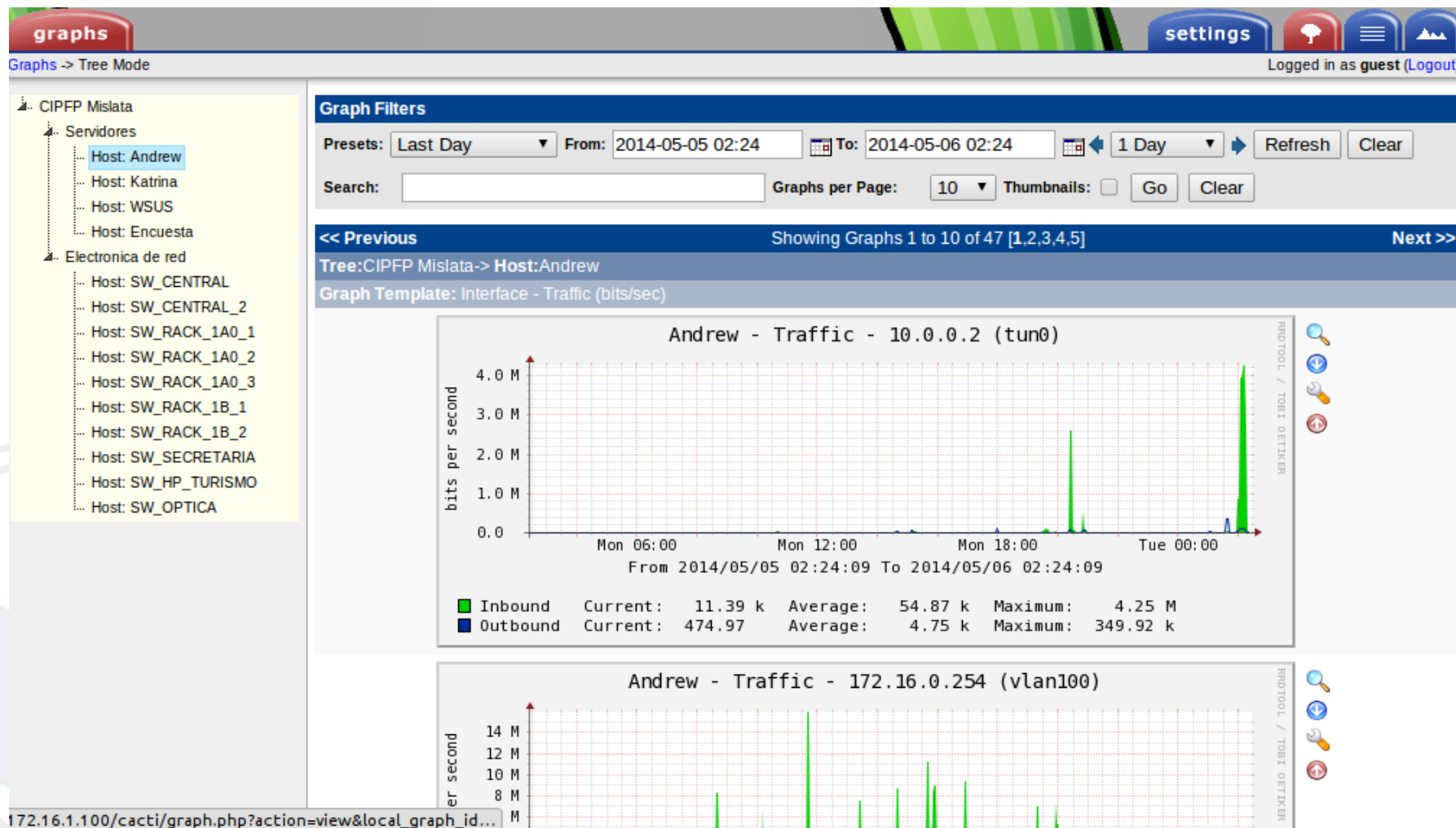
- Software libre bajo licencia GPL
- Es un frontend web de RRDTool, para generar gráficos con datos y estadísticas de red
- Utiliza RRDTool, estándar para almacenar datos de gráficas
- Muestra datos diarios, semanales, mensuales y anuales
- Utiliza SNMP, para interrogar a los dispositivos monitorizados y obtener datos (tráfico de red, CPU, disco, memoria, procesos, etc)
- Es intuitivo de usar, con múltiples plantillas de dispositivos



# CACTI – Tree Mode



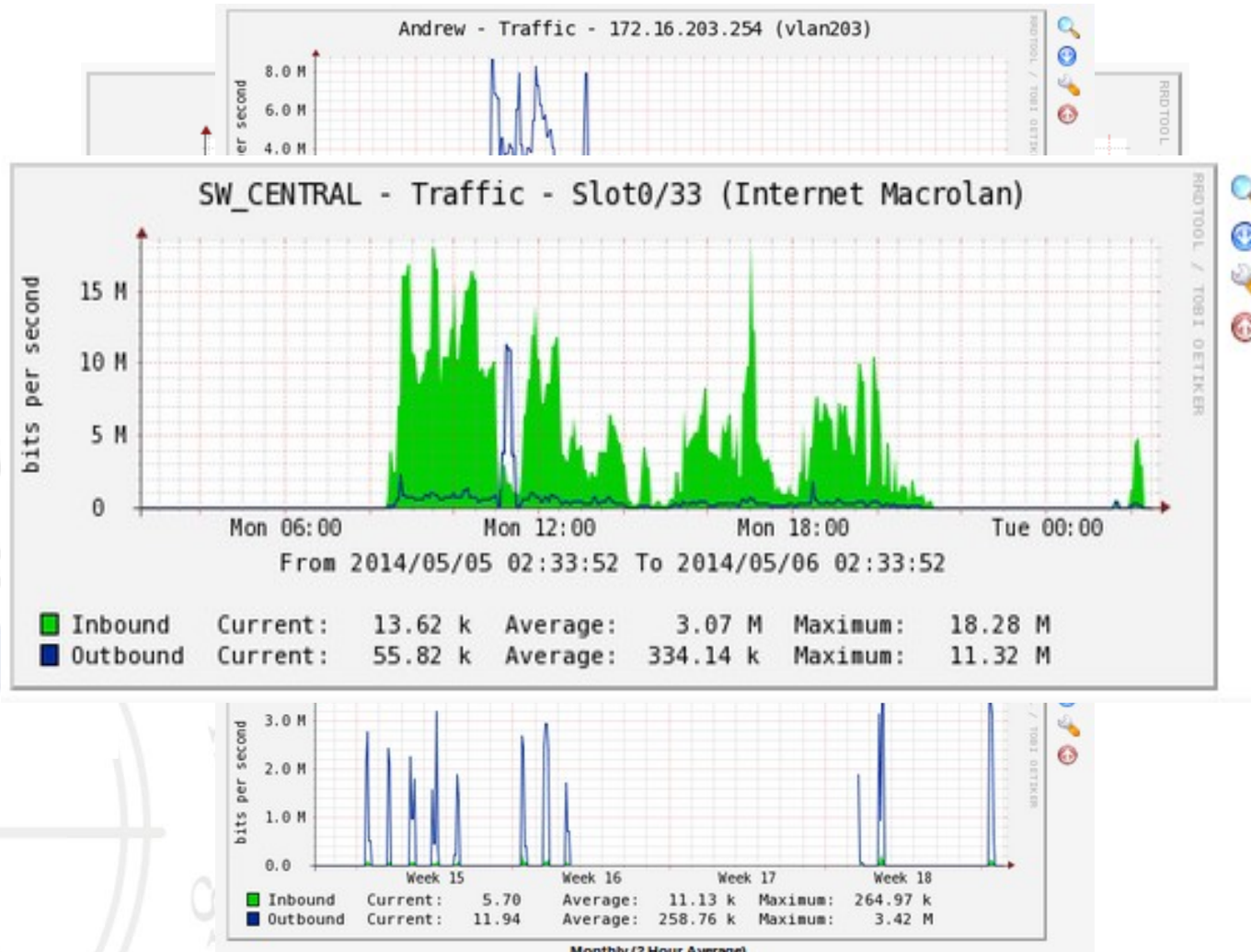
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# CACTI – Tráfico de aulas



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

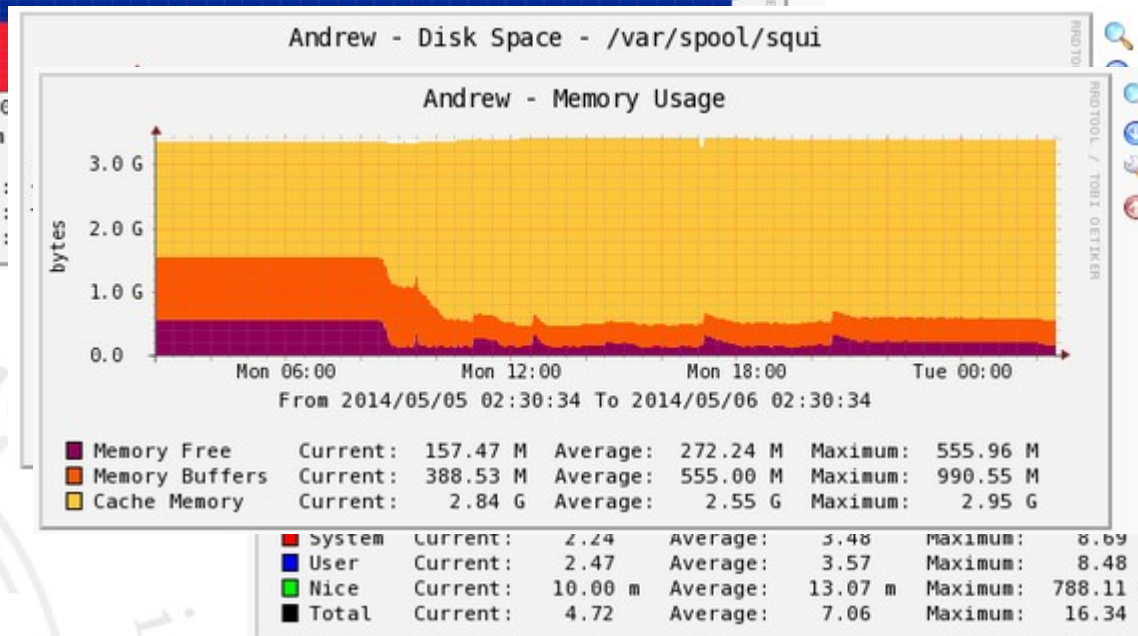
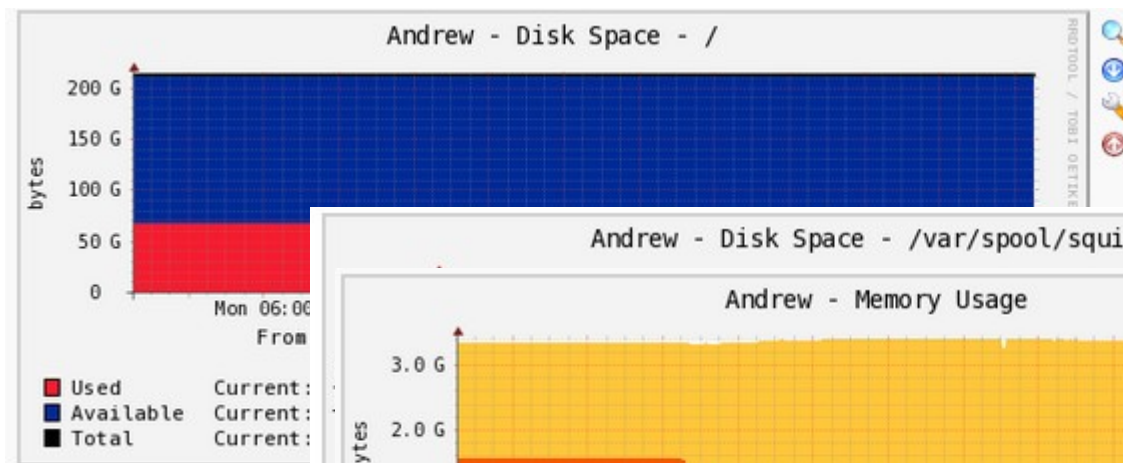




# CACTI – Servidores



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior





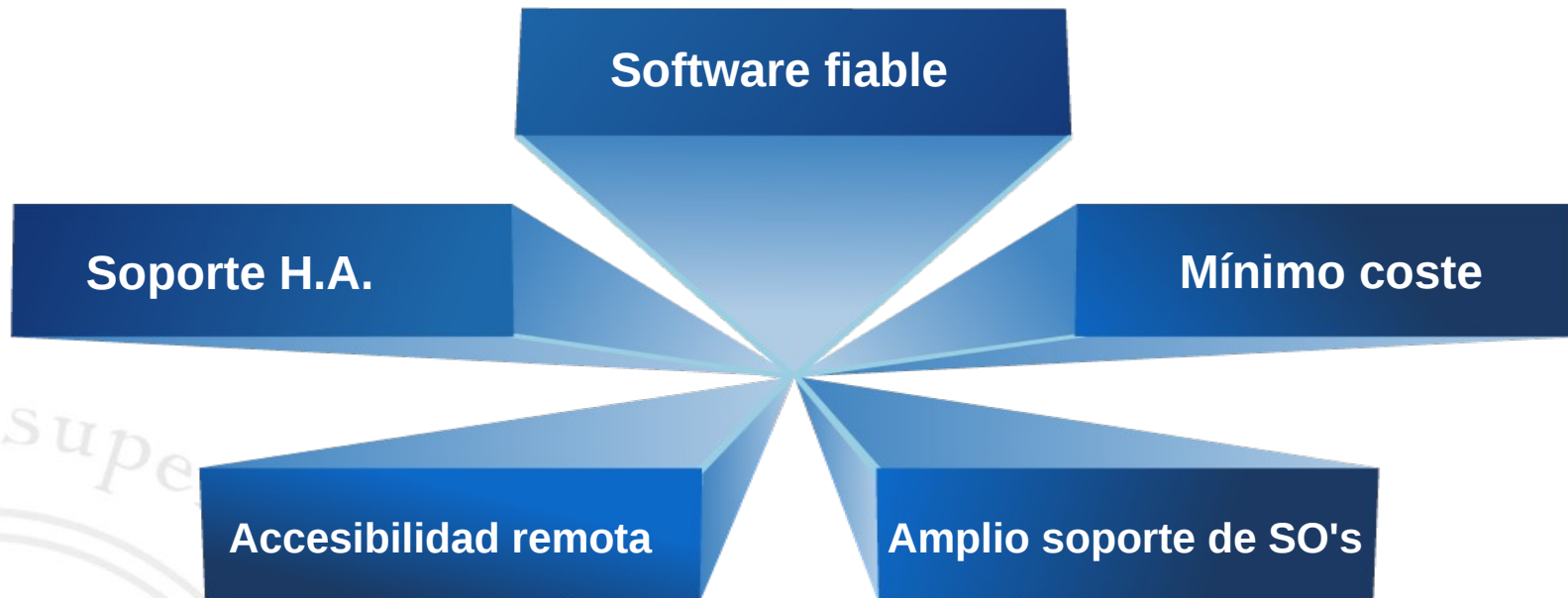
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

# Plataforma para proyectos de alumnos

# Requisitos de la plataforma



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# PROXMOX VE

# ¿Porqué PROXMOX VE?



- Solución libre (AGPLv3) para virtualización
- Basado en Debian 6 (Squeeze)
- Soporta virtualización completa con KVM
- Soporta VPS con contenedores Openvz
- Poderosa interfaz web
- Estable, fiable y seguro
- Muy implantado en entornos profesionales

# Virtual Machines



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Las **VM** son una tecnología conocida por todos → utiliza **full virtualization**
- Todos los dispositivos son **emulados**
- Soporta cualquier SO invitado sin modificación, pero **reserva toda la RAM** asignada
- PROXMOX utiliza **KVM** como tecnología de virtualización completa
- KVM (Kernel-based Virtual Machine) está integrada en el kernel Linux (kvm.ko) desde la versión 2.6.20
- Utiliza una variante de **QEMU** como **frontend**

# Containers



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Los **VPS** (Virtual Private Server), **VE** (Virtual Environment) o **Contenedores** son una tecnología habitual en los hostings
- Utiliza **virtualización de SO**, de forma que todas los VPS comparten el kernel, módulos del kernel, etc → eficiencia en el uso de recursos
- PROXMOX utiliza **OpenVZ**, que permite a un servidor físico correr múltiples instancias de un SO (en este caso, GNU/Linux)
- Todos los VPS usan por tanto el **mismo kernel** pero pueden ser distribuciones diferentes (debian, fedora, red hat, ubuntu, centos, etc)
- Un VPS puesto en marcha puede ocupar inicialmente entre 20 o 30 MB de RAM → ¡podemos tener **decenas** o **cientos** de VPS en marcha!

# VM's vs Containers



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

VM	VPS
Virtualización completa	Virtualización de SO
Cualquier SO	Mismo kernel que anfitrión
Con 4GB: pocos VM (3 ó 4)	Decenas o cientos de servidores
Peor rendimiento	Mejor rendimiento
No hay paravirtualización	Soporta dispositivos paravirtualizados
VMWare, VirtualBox, KVM, etc	Virtuozzo, OpenVZ, BSD jails, Solaris zones, etc

# Servidor dedicado



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- PROXMOX VE se encuentra instalado en un servidor **externo** dedicado contratado con un **proveedor de hosting**
- Permite que los alumnos **accedan desde casa** a sus proyectos
- **Características** servidor dedicado:
  - S.O. Debian 6.0.7 + PROXMOX VE 2.3
  - 16 GB de RAM
  - Intel QuadCore i5-2400 CPU @ 3.10GHz
  - RAID 1 de 2TB (2TB+ 2TB)
  - Conexión a Internet de 100 Mbps SIMÉTRICA
  - Tráfico ilimitado



# PROXMOX – Panel de control



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

**PROXMOX** Proxmox Virtual Environment  
Version: 2.3-12/ad9c5c05

You are logged in as 'ronrubia@pam' [Logout](#) [Create VM](#) [Create CT](#)

Server View **Container 104 ('jproduccion.pve.fpmislata.com') on node 'pve'** [Start](#) [Shutdown](#) [Stop](#) [Remove](#) [Migrate](#) [Console](#)

[Summary](#) [Resources](#) [Network](#) [DNS](#) [Options](#) [Task History](#) [UBC](#) [Backup](#) [Permissions](#)

Hour (average)

**Network traffic**

netin netout

**Tasks** [Cluster log](#)

Start Time	End Time	Node	User name	Description	Status
Apr 03 20:30:40	Apr 03 20:30:40	pve	jnmurgui@pam	CT 225 - Start	OK
Apr 03 20:29:49	Apr 03 20:29:50	pve	jnmurgui@pam	CT 225 - Start	Error: command 'vzctl start 225' faile...
Apr 03 20:29:11	Apr 03 20:29:13	pve	jnmurgui@pam	CT 225 - Start	Error: command 'vzctl start 225' faile...
Apr 03 20:27:35	Apr 03 20:28:00	pve	jnmurgui@pam	CT 225 - Restore	OK
Apr 03 20:26:56	Apr 03 20:27:20	pve	jnmurgui@pam	CT 225 - Shutdown	OK
Apr 03 20:22:57	Apr 03 20:22:58	pve	jnmurgui@pam	CT 223 - Start	OK
Apr 03 09:39:07	Apr 03 09:39:11	pve	jnmurgui@pam	CT 223 - Shutdown	OK

# Panel de control



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Gestión de VM's y contenedores
- Gestión de almacenamiento local y externo (S.A.N, N.A.S)
- Gestión del cluster y HA
- Gestión del networking virtual
- **Migración en vivo** de VM's y contenedores entre servidores físicos
- Gestión de usuarios, roles y permisos a las VM's y contenedores
- Consola remota vía Java

# Acceso panel de control



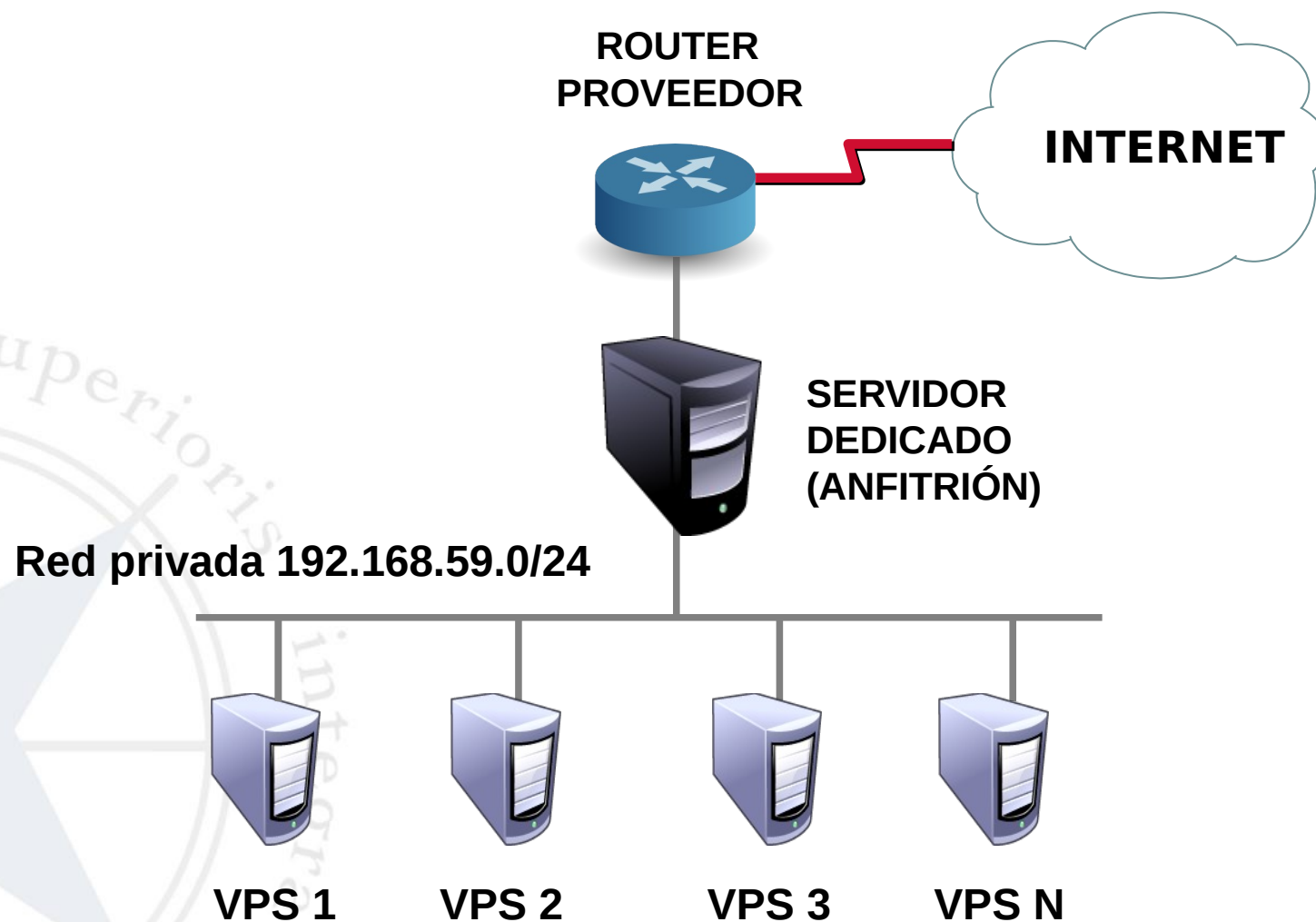
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Desde un navegador web con soporte Java
- Autenticación PAM sobre RADIUS
- Se utilizan las credenciales de Moodle
- Cada alumno pertenece a un grupo de proyecto con acceso sólo a sus VM y contenedores
- Los profesores están en un grupo con permiso total a las VM y contenedores de alumnos

# Arquitectura de red



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Funciones de red del anfitrión



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Puerta de enlace para las VM
- NAT (Traducción de direcciones)
- Servidor DNS
- Cortafuegos + IDS/IPS (OSSEC)
- Concentrador VPN
- Proxy inverso HTTP, HTTPS y FTP

# Características IDS/IPS



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- **OSSEC** → HIDS licencia GPLv2
- Funciona en muchas plataformas
- Detecta **ataques** de red conocidos mediante patrones
- Detecta **anomalías** (excesivos puertos abiertos, errores de aplicaciones en logs, etc)
- Detecta **rootkits**
- Verifica **integridad** de archivos así como cambio en permisos
- Antes posibles ataques DDoS o excesivos errores en aplicaciones, **banea** la dirección del presunto atacante

# Alertas OSSEC



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

REDACTA

--END OF NOTIFICATION

**Safata d'entrada (3....**

Destacats

Important

Enviats

**Esborrany (239)**

**Correu brossa (49)**

Paperera

**Alta disponibilitat...**



[Inicia la sessió al  
xat](#)

OSSEC HIDS Notification.

2014 May 07 17:56:36

Received From: pve->/var/log/dpkg.log

Rule: 2902 fired (level 7) -> "New dpkg (Debian Package) installed."

Portion of the log(s):

2014-05-07 17:56:35 status installed lshw 02.14-1

--END OF NOTIFICATION

# Alertas OSSEC



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

REDACTA

Safata d'entrada (3....

Destacats

Important

Enviats

Esborrany (239)

Correu brossa (49)

Paperera

Alta disponibilitat...



[Inicia la sessió al xat](#)

Cerca persones...

OSSEC HIDS Notification.  
2014 Feb 18 16:16:52

Received From: pve->**netstat** -tan |grep LISTEN |grep -v 127.0.0.1 | sort  
Rule: 533 fired (level 7) -> "Listened ports status (**netstat**) changed (new port opened or closed)."  
Portion of the log(s):

ossec: output: '**netstat** -tan |grep LISTEN |grep -v 127.0.0.1 | sort':

tcp	0	0	<a href="#">0.0.0.0:10022</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:110</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:110</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:110</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:110</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:111</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:111</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:111</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:12320</a>	0.0.0.0:*	LISTEN

Previous output:

ossec: output: '**netstat** -tan |grep LISTEN |grep -v 127.0.0.1 | sort':

tcp	0	0	<a href="#">0.0.0.0:10022</a>	0.0.0.0:*	LISTEN
tcp	0	0	<a href="#">0.0.0.0:110</a>	0.0.0.0:*	LISTEN



# Alertas OSSEC



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

REDACTA

Safata d'entrada (3...)

Destacats

Important

Enviats

Esborrany (239)

Correu brosa (49)

Paperera

Alta disponibilitat...



Inicia la sessió al



OSSEC HIDS

per a ronrubia ▾



anglès ▾



espanyol ▾

[Tradueix el missatge](#)

OSSEC HIDS Notification.

2014 Mar 02 07:39:59

Received From: pve->rootcheck

Rule: 510 fired (level 7) -> "Host-based anomaly detection event (rootcheck)."

Portion of the log(s):

File '/var/lib/vz/private/214/var/log/httpd/error\_log-20140302' is owned by root and has written permissions to anyone.

# Alertas OSSEC



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

REDACTA

Safata d'entrada (3....

Destacats

Important

Enviats

Esborrany (239)

Correu brosa (49)

Paperera

Alta disponibilitat...



[Inicia la sessió al xat](#)

Cerca persones...

antoni Bagur

Diana Exposito

## OSSEC Notification - pve - Alert level 8



Paperera x

 **OSSEC HIDS** <pve.fpmislata@gmail.com>  
per a ronrubia ▾

 anglès ▾ > espanyol ▾ [Tradueix el missatge](#)

S'ha suprimit el missatge. [Restaura el missatge](#)

**OSSEC HIDS** Notification.  
2014 May 06 10:00:57

Received From: pve->/var/log/messages  
Rule: 5104 fired (level 8) -> "Interface entered in **promiscuous**(sniffing) mode."  
Portion of the log(s):

May 6 10:00:55 pve kernel: device vmbr0 entered **promiscuous** mode

# Alerta OSSEC - DoS



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

REDACTA

## OSSEC Notification - pve - Alert level 2

Safata d'entrada x

Safata d'entrada (3....

Destacats

Important

Enviats

Esborrany (239)

Correu brossa (49)

Paperera


Alta disponibilitat...



[Inicia la sessió al xat](#)

Cerca persones...

 **OSSEC HIDS** <pve.fpmislata@gmail.com>  
per a ronrubia ▾

 anglès ▾ > espanyol ▾ [Tradueix el missatge](#)

OSSEC HIDS Notification.

2014 Feb 25 03:39:06

Received From: pve->/var/log/syslog

Rule: 1002 fired (level 2) -> "Unknown problem somewhere in the system."

Portion of the log(s):

Feb 25 03:39:04 pve mod\_evasive[757862]: Blacklisting address [188.165.212.171](#): possible DoS attack.

# Acceso a los servicios



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Servicios que ofrecen los VPS de los proyectos: HTTP, HTTPS y FTP
- Posible solución: redirigir puertos en el anfitrión
- Problema: una **sola IP pública** para todos → sólo se puede redirigir un puerto
- Solución cara: contratar un rango IP público a RIPE y hacer NAT estático
- Solución elegida: proxy inverso para los servicios indicados

# Proxy inverso



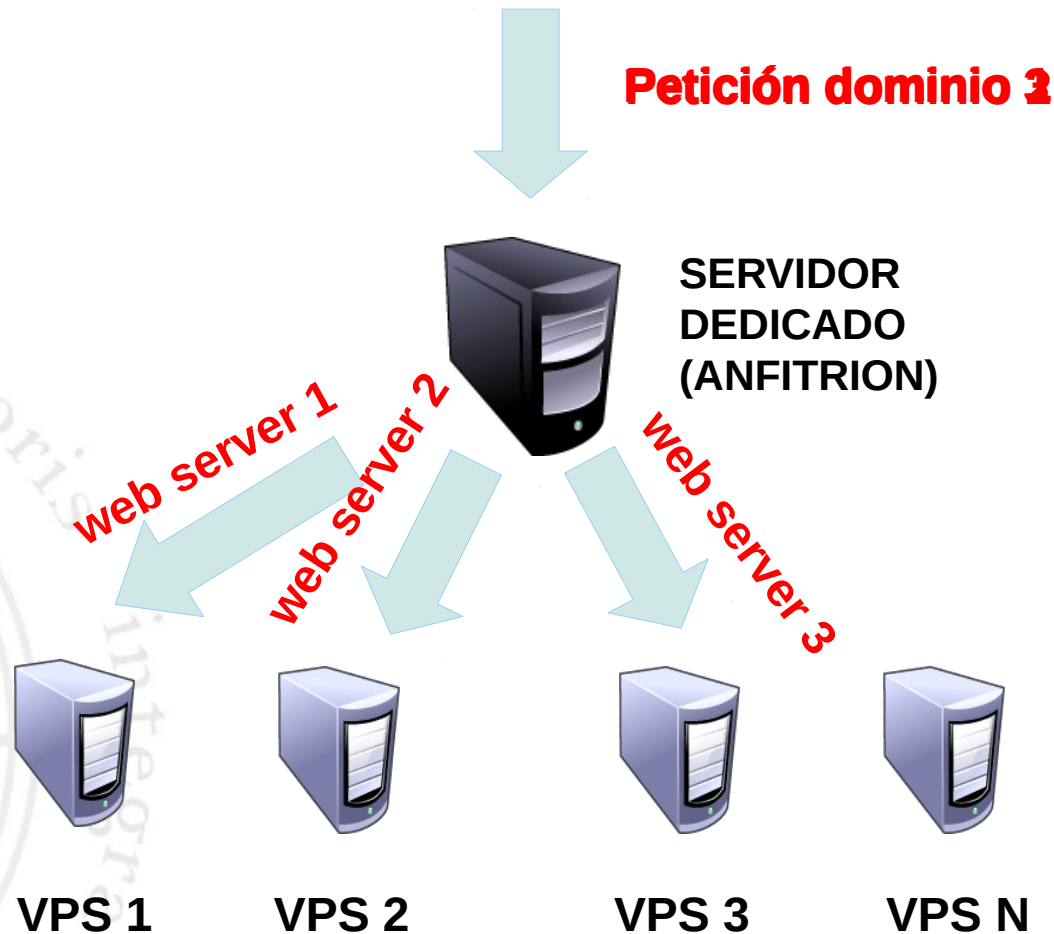
CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

- Uso contrario al habitual: para entrar desde Internet en vez de para salir hacia Internet
- Características:
  - **Seguridad:** protege a los servidores
  - **Aceleración SSL:** puede liberar a los servidores del cifrado/descifrado SSL/TLS
  - **Balanceo** de carga entre servidores
  - **Caché** de contenido estático

# Funcionamiento proxy inverso



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior



# Administración de servidores



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

**Acceso directo por consola Java desde panel web de PVE**

**Acceso local a los servidores desde el propio centro**

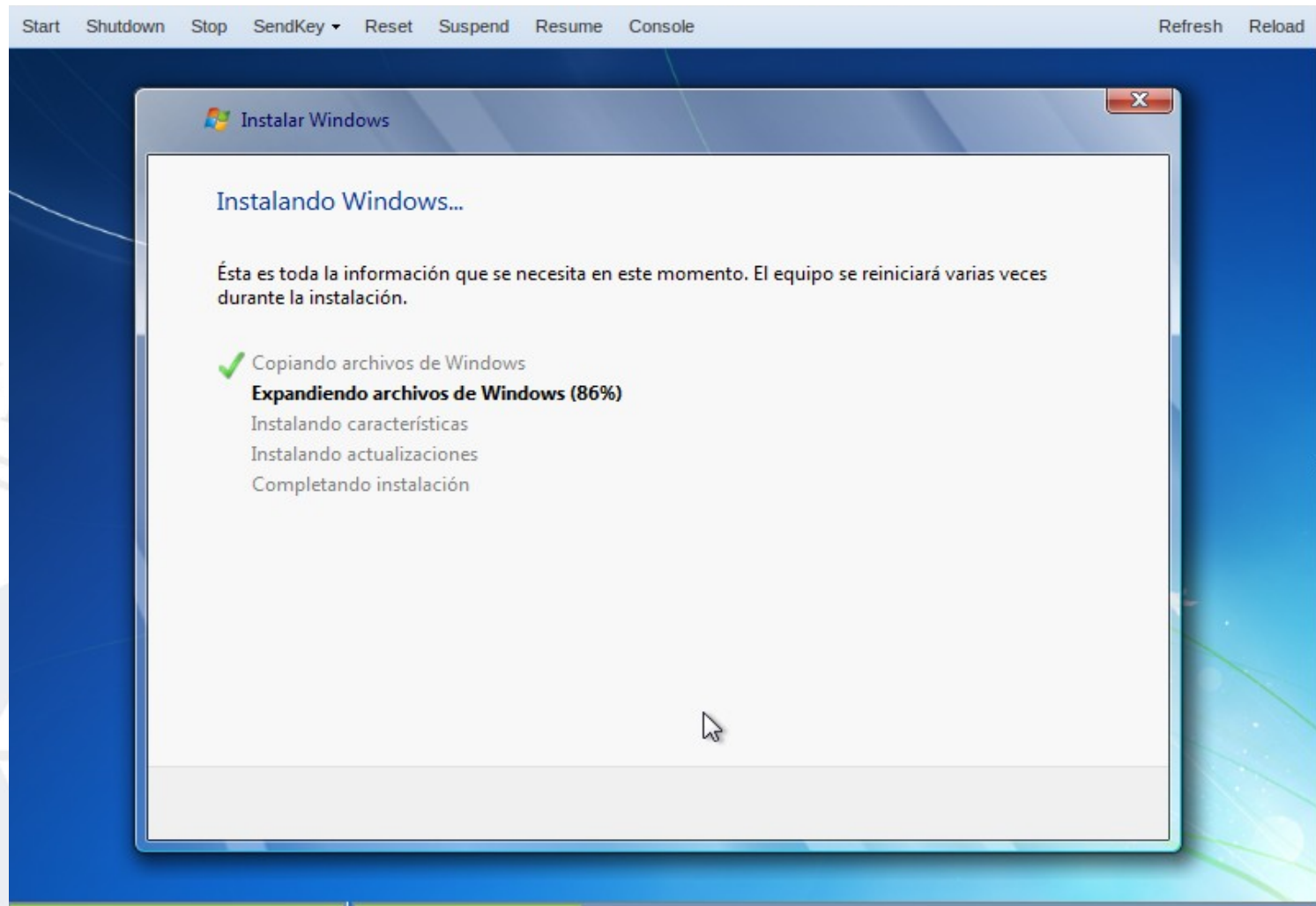
**Acceso remoto a los servidores por VPN desde fuera**



# Consola Java



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior

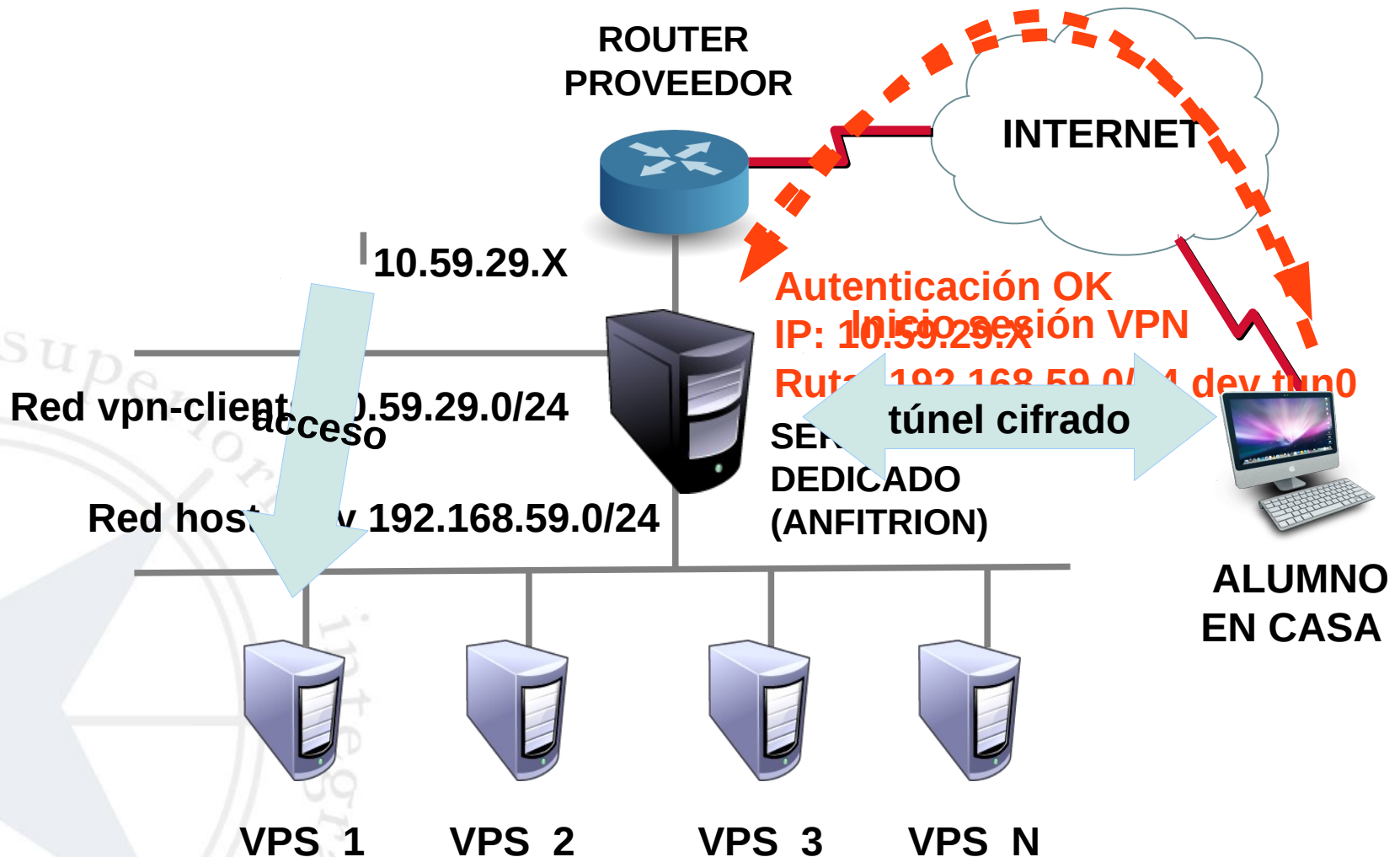




# Acceso por VPN



CIPFP Mislata  
Centre Integrat Públic  
Formació Professional Superior





**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Conclusiones





**CIPFP Mislata**  
Centre Integrat Públic  
Formació Professional Superior

# Muchas gracias por la atención

