MONITORIZANDO E INTERPRETANDO LA SALUD DE UNA RED CON SMOKEPING

Francisco J. Montilla

MUM MADRID
Septiembre 2016

FRANCISCO J MONTILLA

- Administrador de Sistemas desde 1998
- Primer contacto RouterOS en 2007
- MCC y TRAINER: MTCWE, MTCTCE, MTCRE, MTCINE
- Auditorías, Diseño, Despliegue, Diagnóstico, Training
- *Forum* nick: *pukkita*

EN ESTA PRESENTACIÓN:

MONITORIZANDO LA SALUD DE UNA RED

- Las partes del problema (y posibles soluciones)
- Claves para una Monitorización Eficaz, y Eficiente
- La Solucion: Smokeping
- Estrategias para una Implantación Efectiva (WISP)
- Interpretación de sus gráficas
- Conclusiones

Monitorización de Redes

Claves

- Visión tanto **global** como **puntual** de la salud de la red
- **Detectar** y **aislar** anomalías rápidamente
- Determinar **cuándo** empezó a producirse a anomalía
- Determinar **dónde** está la anomalía
- Cuantificar la **Calidad y Rendimiento** real de un segmento
- **Anticiparse** a futuros problemas

Monitorización de Redes

Beneficios: Tiempo = Dinero

- **Productividad:** menor tiempo dedicado a mantenimiento
- **Rapidez** solucionando incidencias
- **Organización:** Planificación Proactiva
- **Optimización** de recursos
- Proporcionar **Calidad** de servicio **constante** y **predecible**

Monitorización de Redes

Las Partes del Problema

- Obtención
- Almacenaje
- Correlación
- Análisis

} Multitud Datos Estadísticos:

Fecha y hora, Dispositivo o Servicio,
Latencia, Jitter, Pérdida de Paquetes...

Monitorización de Redes

Posibles Soluciones

- Obtención: Ping, SNMP...
- Almacenaje: BBDD relacionales, "planas"...
- Correlación: tabulación, SQL, gráficas...
- Análisis: **Nosotros**

Monitorización de Redes

El "Hardware Analítico": *Especificaciones*

Lóbulo Frontal

Procesado:

Logs, Datos tabulados

- Mucho más lento
- Esfuerzo (concentración)
- Mucho menos eficiente

Lóbulo Occipital

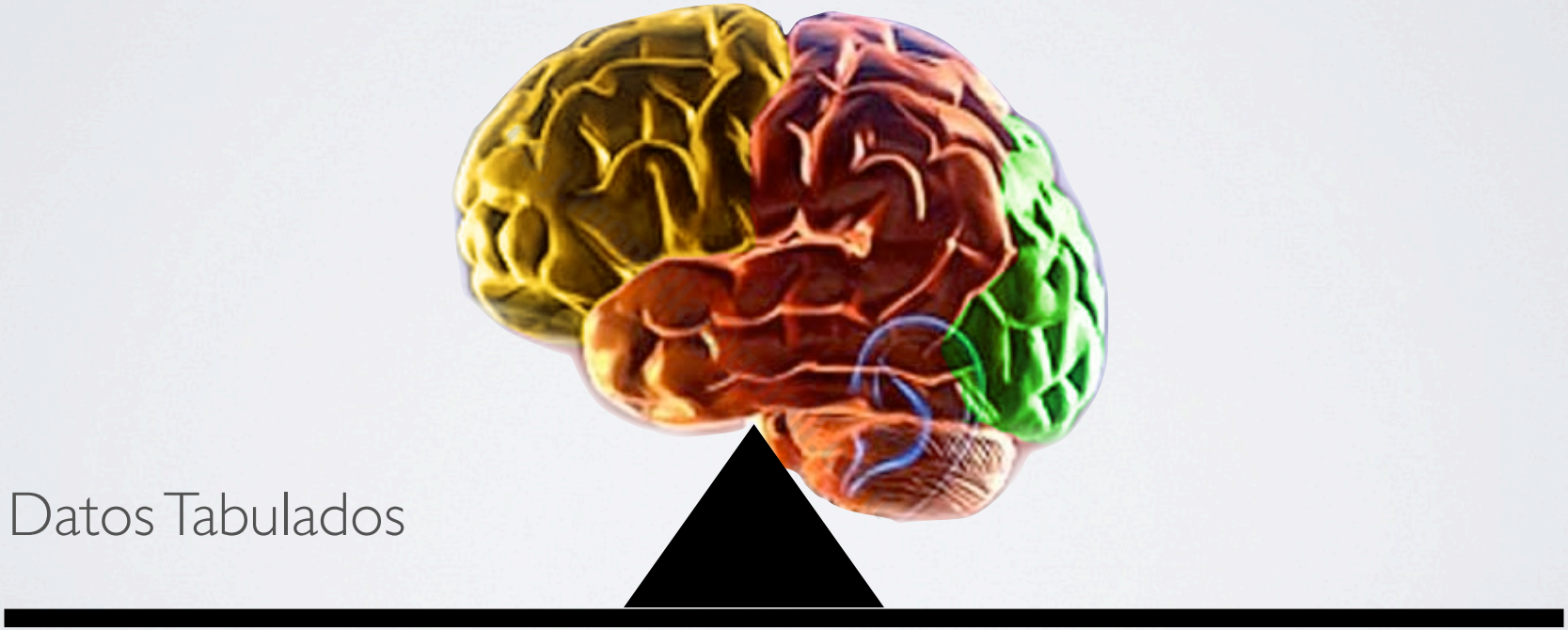
Percepción Visual:

Gráficos

- Extremadamente rápido
- Poco o nulo esfuerzo
- Alta Eficiencia

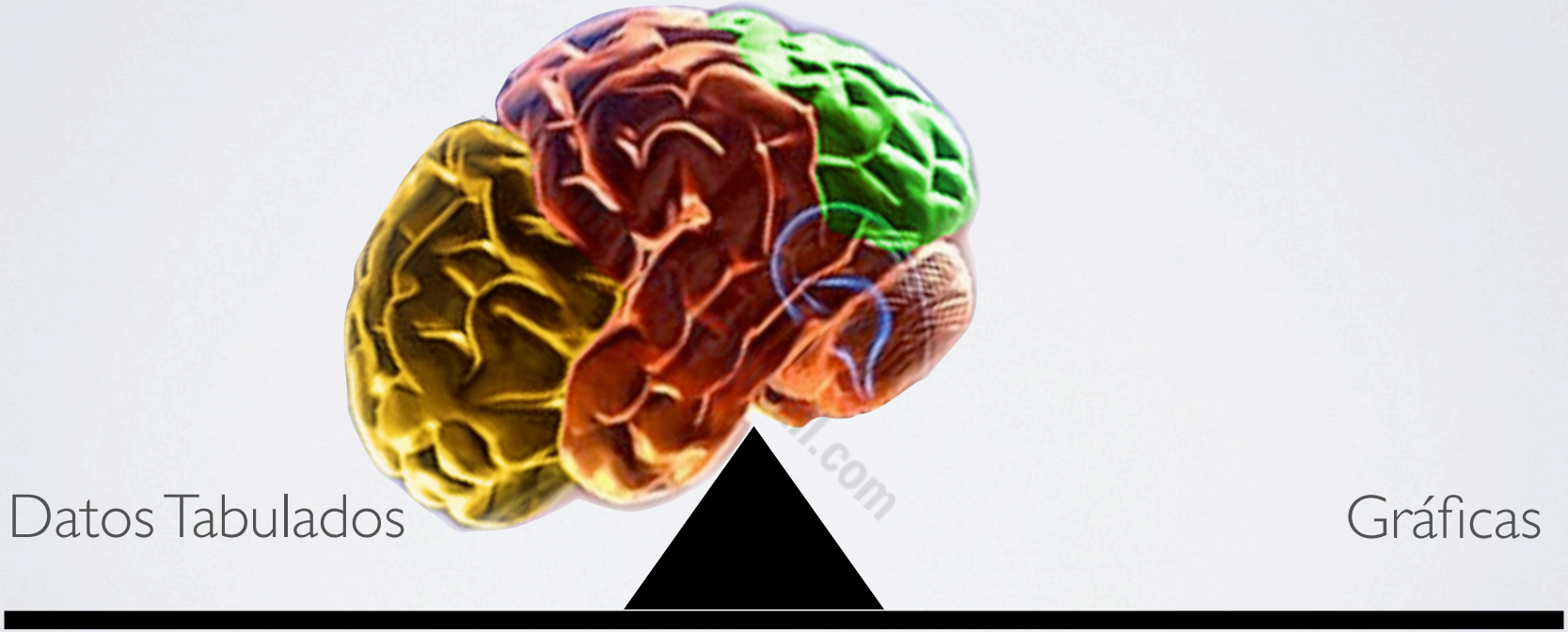
Monitorización de Redes

El "Hardware Analítico": *Optimizando*



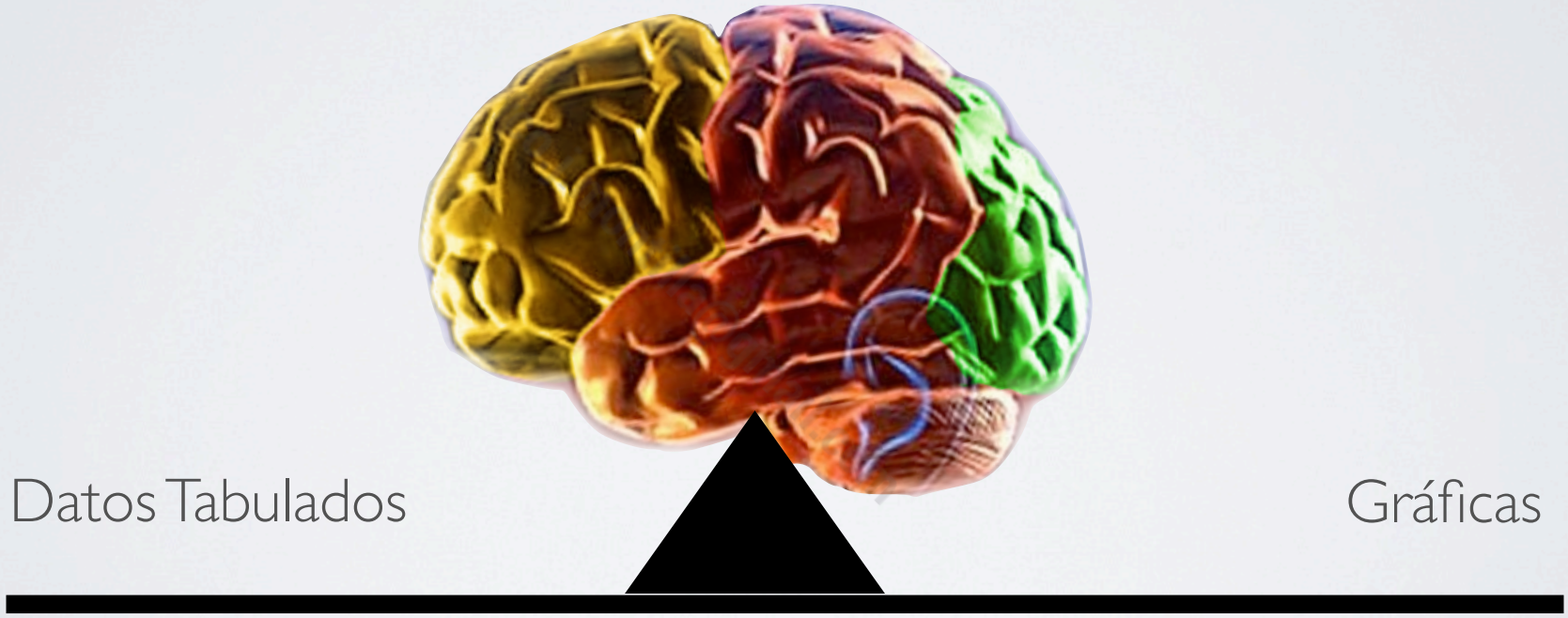
Monitorización de Redes

El "Hardware Analítico": *Optimizando*



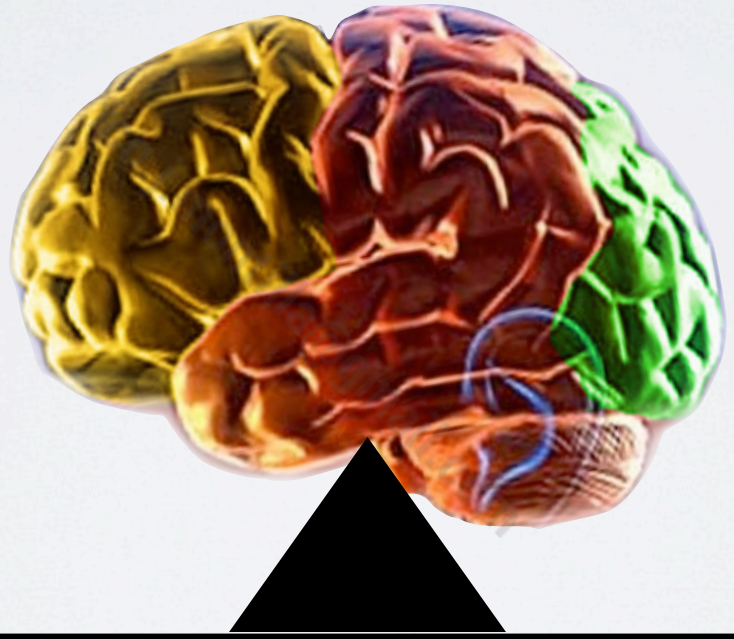
Monitorización de Redes

El "Hardware Analítico": *Optimizando*



Monitorización de Redes

El "Hardware Analítico": *Optimizando*



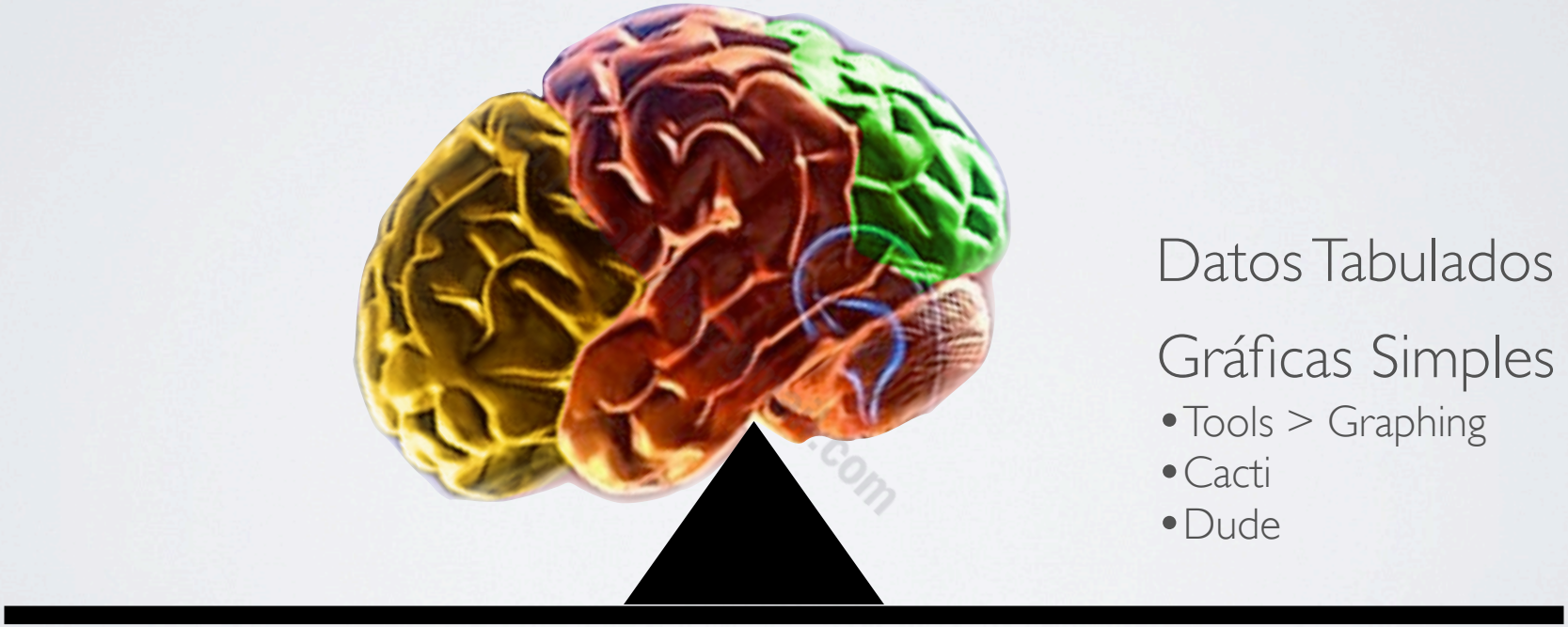
Datos Tabulados

Gráficas Simples

- Tools > Graphing
- Cacti (estandar)
- Dude

Monitorización de Redes

El "Hardware Analítico": *Optimizando*



Datos Tabulados

Gráficas Simples

- Tools > Graphing
- Cacti
- Dude

SMOKEPING

EN ESTA PRESENTACIÓN:

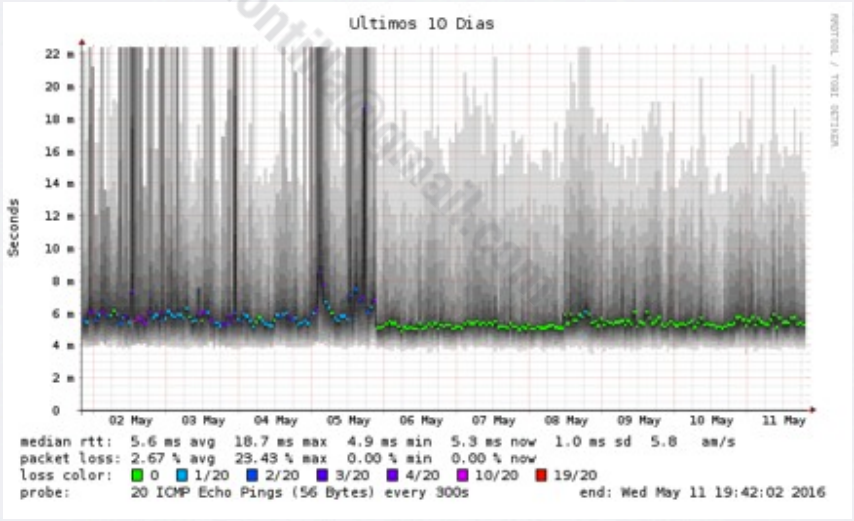
- Orígenes
- Requisitos Hardware y Software
- Instalación
- Estrategias de despliegue
- Anatomía de sus gráficas

SMOKEPING

ORIGENES

Autor: Tobias Oetiker

- MRTG: Multi Router Traffic Grapher (SNMP)
- RRDTool: Round Robin Database Tool
- Smokeping



SMOKEPING

REQUISITOS: HARDWARE

- CPU y RAM: acorde con despliegue
  - -FreeBSD/Celeron G1620 con 50+ sondas: 2Gb RAM, 0.19 top
- Interfaz de red: impacto en precisión y escalabilidad
  - -Realtek, tplink, etc... no óptimas
  - -Recomendable: Intel, Broadcom... ver recomendaciones SO
- Virtualización: impacto en precisión

SMOKEPING

Requisitos: Dependencias

- perl y módulos CPAN
- Servidor HTTP con fastcgi (UI)
- Librerías auxiliares (gráficas, sondas)
- Fping, RRDTool

SMOKEPING

Instalación

- FreeBSD: `pkg install smokeping`
- Debian/Ubuntu: `apt-get install smokeping`
- CentOS :

  http://www.wedebugyou.com/2012/11/how-to-install-and-configure-smokeping-on-centos-6/

SMOKEPING

CONFIGURACIÓN

- Edición fichero texto `/usr/local/etc/smokeping/config`
- Estructurado en secciones: obligatorias y opcionales
- Secciones Multinivel (árbol)

SMOKEPING

CONFIGURACIÓN: ESTRUCTURA SECCIONES OBLIGATORIAS

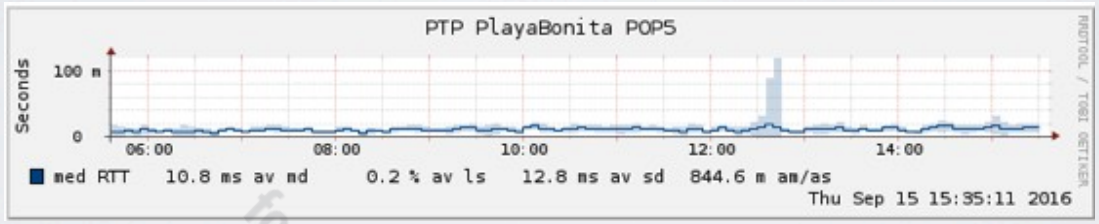
- **General:** paths, URLs, logging, permisos
- **Database:** propiedades BBDD
- **Presentation** UI. Multinivel: overview, detail
- **Probes:** Módulos sonda. Multinivel
- **Targets** (dispositivos a monitorizar) Multinivel.

http://oss.oetiker.ch/smokeping/doc/smokeping_config.en.html

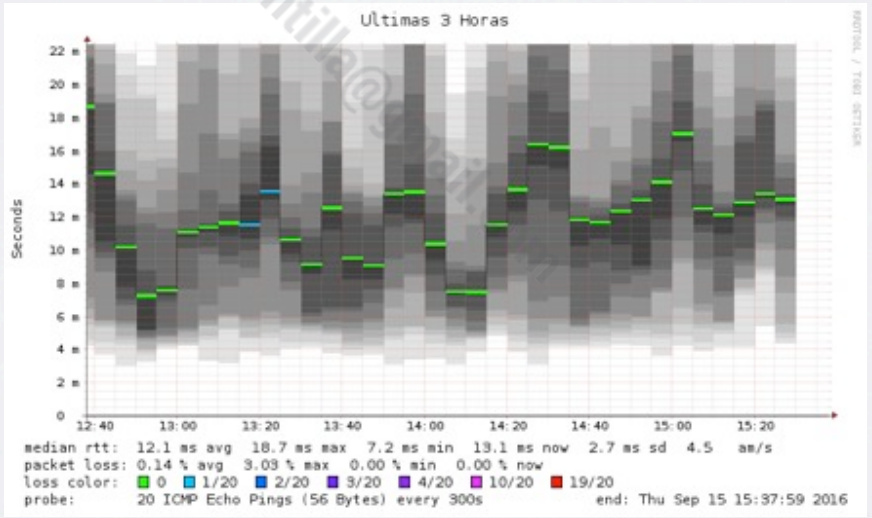
SMOKEPING

TIPOS DE GRÁFICAS: SEGÚN VISTA

General:



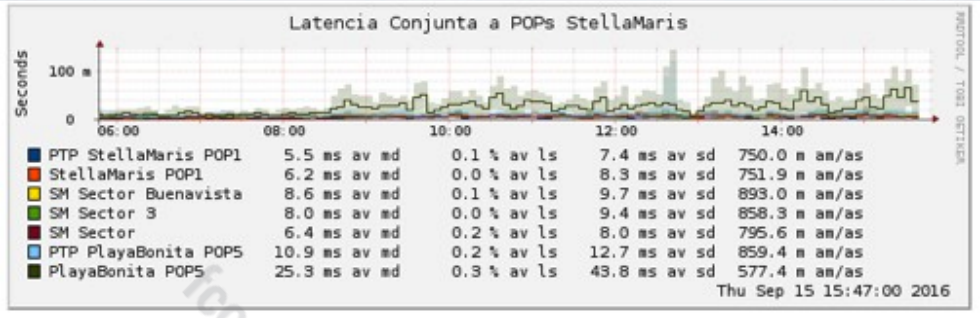
Detalle: (3h, 30h, 10d, 400d, Dinámica)



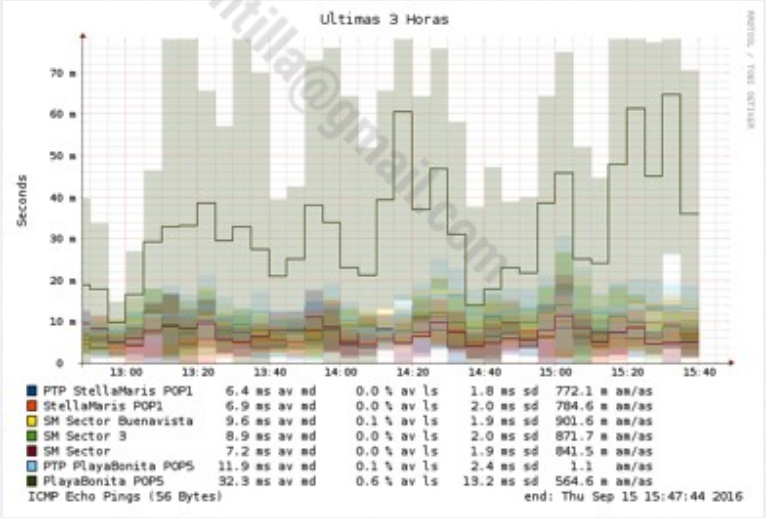
SMOKEPING

GRÁFICAS: COMPUESTAS

General:



Detalle: (3h, 30h, 10d, 400d, Dinámica)

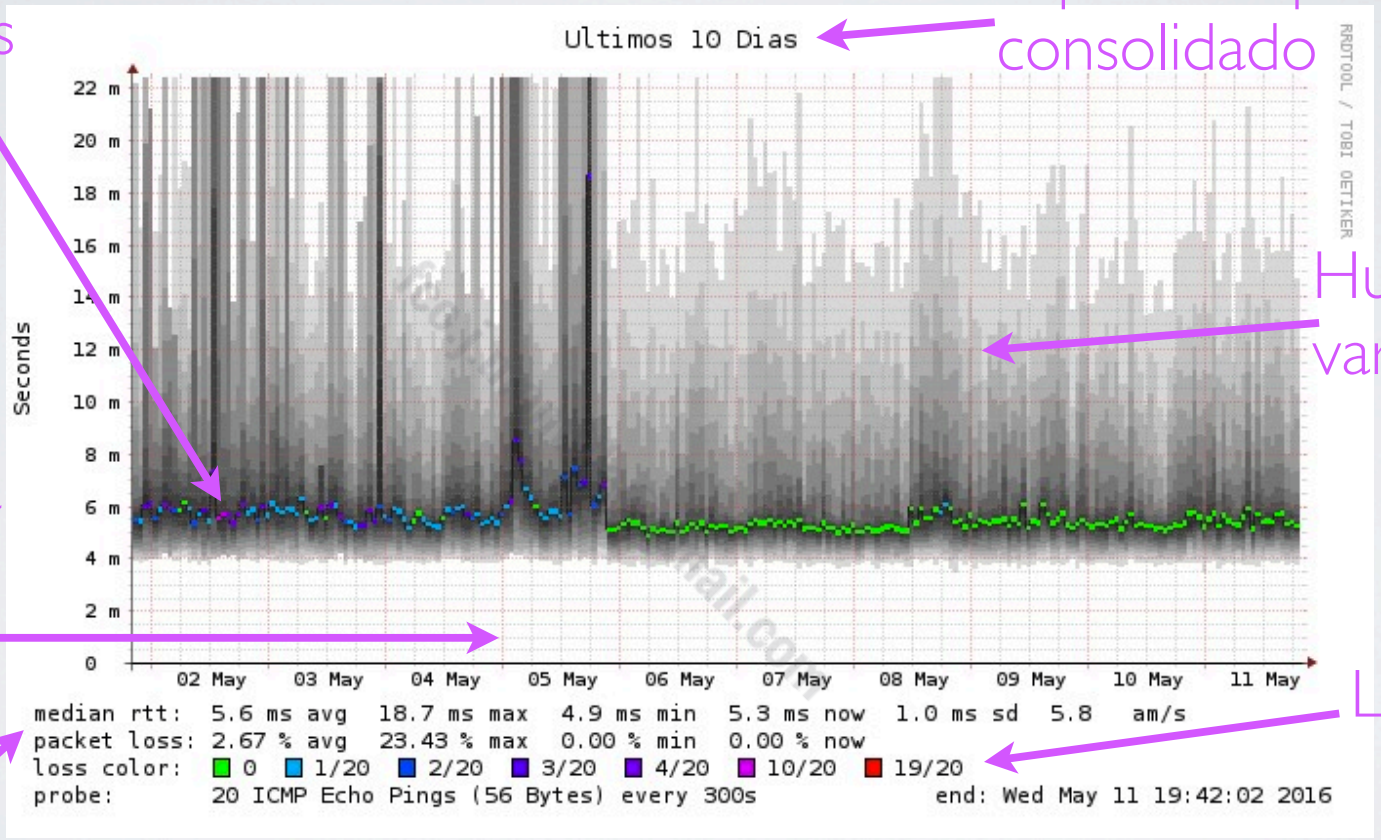


SMOKEPING

ANATOMÍA DE UNA GRÁFICA

Pérdida paquetes

Lapso tiempo consolidado



Humo: varianza jitter

Latencia vs Tiempo

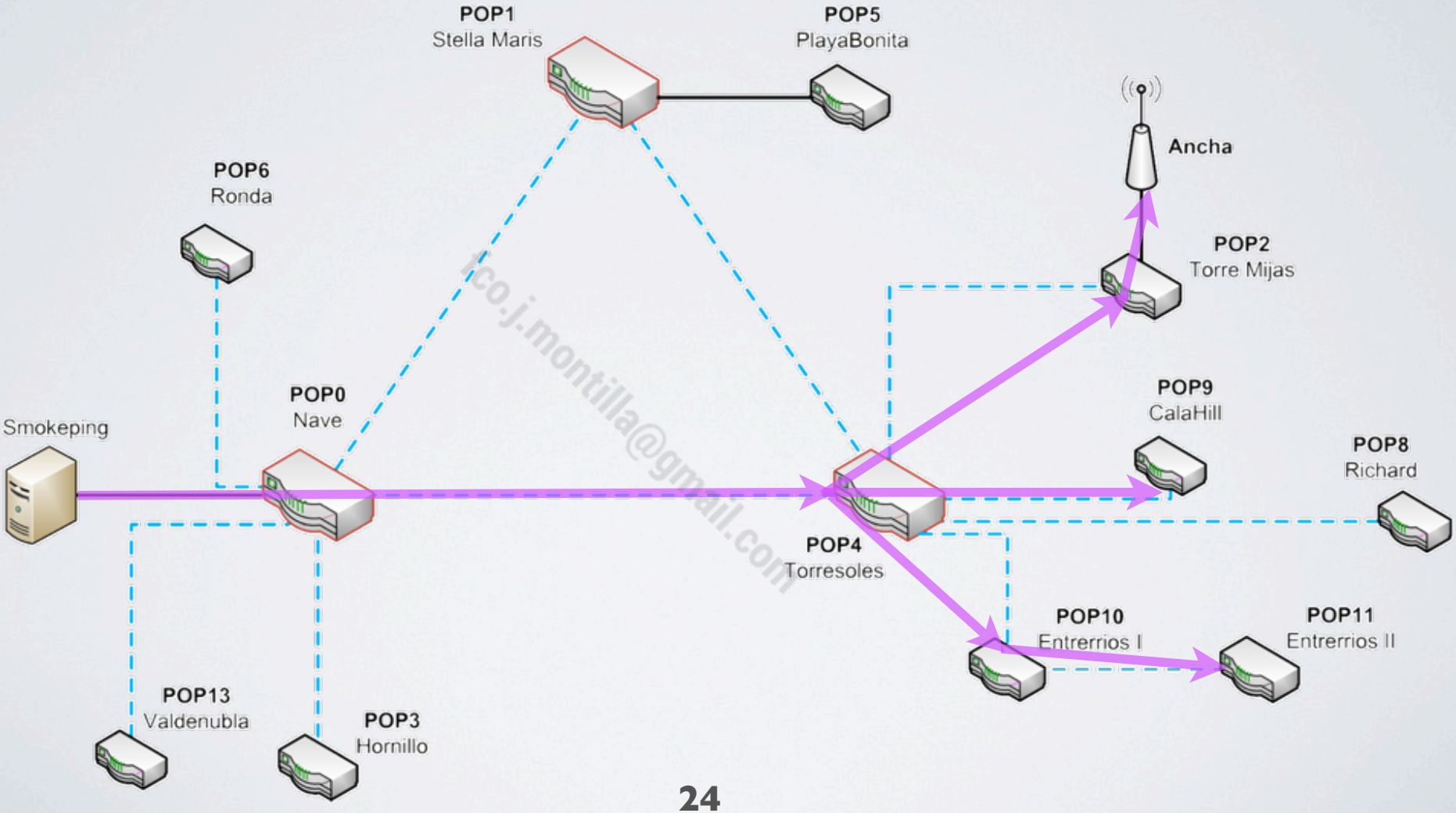
Leyenda

Datos Estadísticos

http://oss.oetiker.ch/smokeping/doc/reading.en.html

SMOKEPING

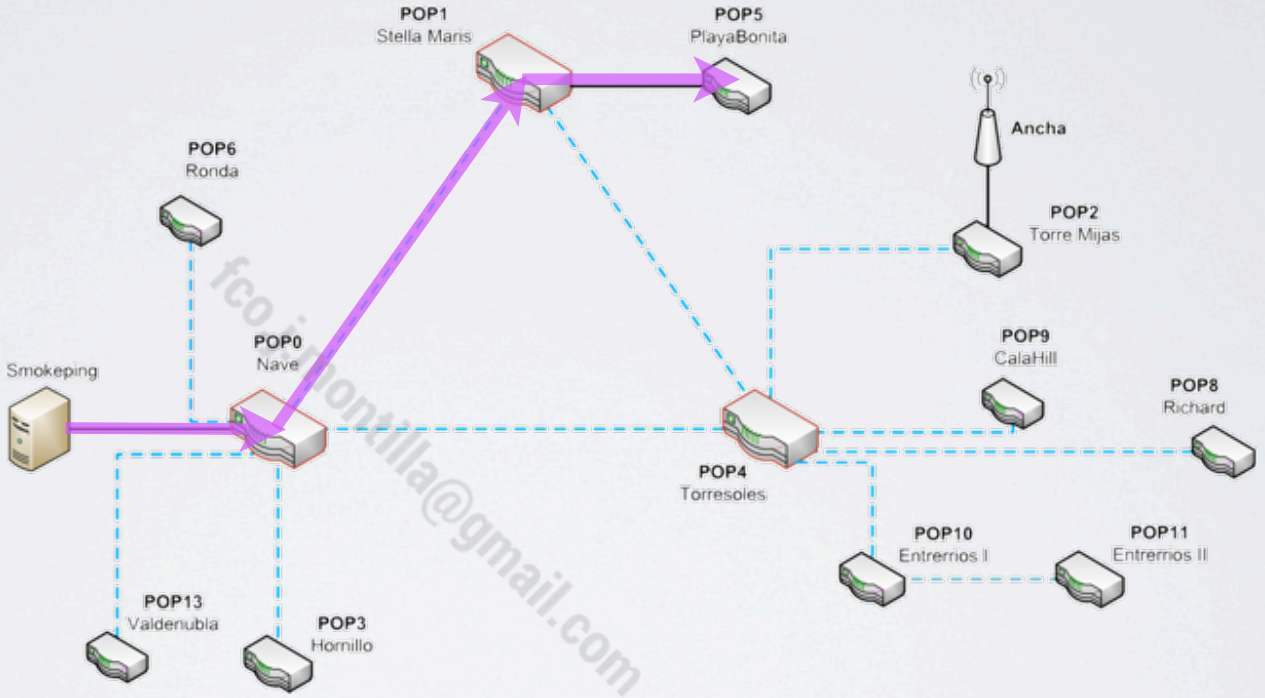
ESTRATEGIA DE DESPLIEGUE: DIAGRAMA RED



SMOKEPING

ESTRATEGIA DE DESPLIEGUE: CONFIGURACIÓN

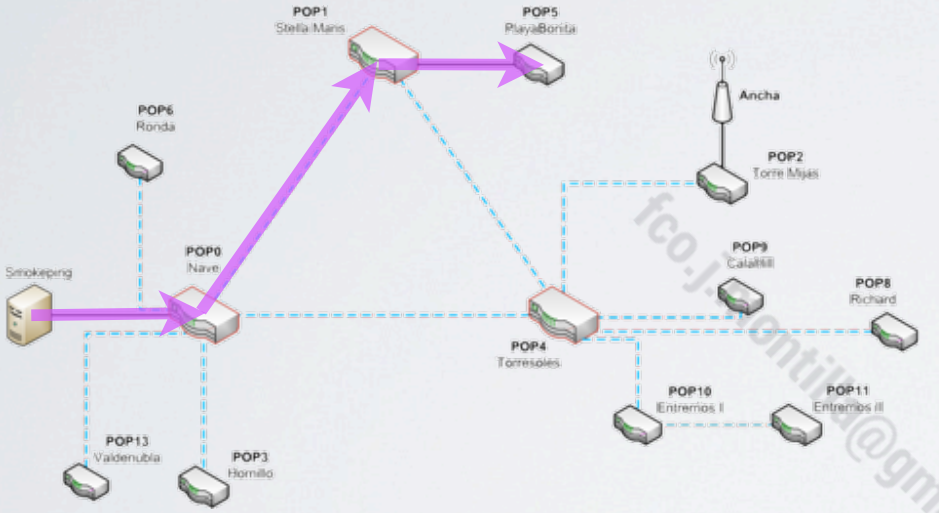
```
+ StellaMaris
menu = StellaMaris
title = StellaMaris

++ PTPStellaMaris
menu = PTP StellaMaris POP1
title = PTP StellaMaris POP1
host = 10.0.100.44

++ POP1StellaMaris
menu = StellaMaris POP1
title = StellaMaris POP1
host = 10.0.101.1

++ SMSectorBuenavista
menu = SM Sector Buenavista
title = SM Sector Buenavista
host = 10.0.101.82

++ SMSector3
menu = SM Sector 3
title = SM Sector 3
host = 10.0.101.83

++ SMSector
menu = SM Sector
title = SM Sector
host = 10.0.101.85

++ PTPPlayaBonita
menu = PTP PlayaBonita POP5
title = PTP PlayaBonita POP5
host = 10.0.101.20

++ POP5PlayaBonita
menu = PlayaBonita POP5
title = PlayaBonita POP5
host = 10.0.105.1
```

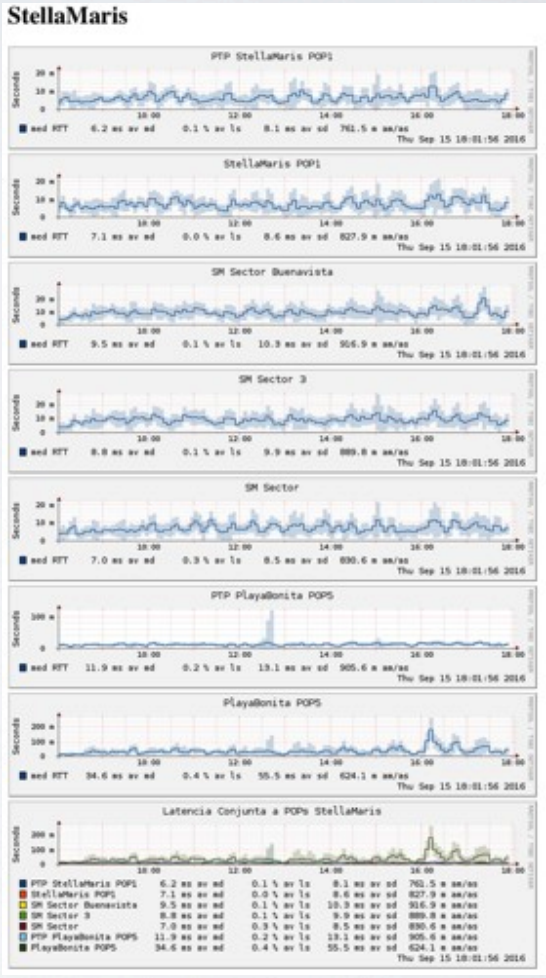



```
++ SMPOPs
menu = Latencia Conjunta a POPs StellaMaris
title = Latencia Conjunta a POPs StellaMaris
host = /StellaMaris/PTPStellaMaris /StellaMaris/POP1StellaMaris /StellaMaris/SMSectorBuenavista /StellaMaris/SMSector3 /StellaMaris/SMSector \
/StellaMaris/PTPPlayaBonita/StellaMaris/POP5PlayaBonita
```

SMOKEPING

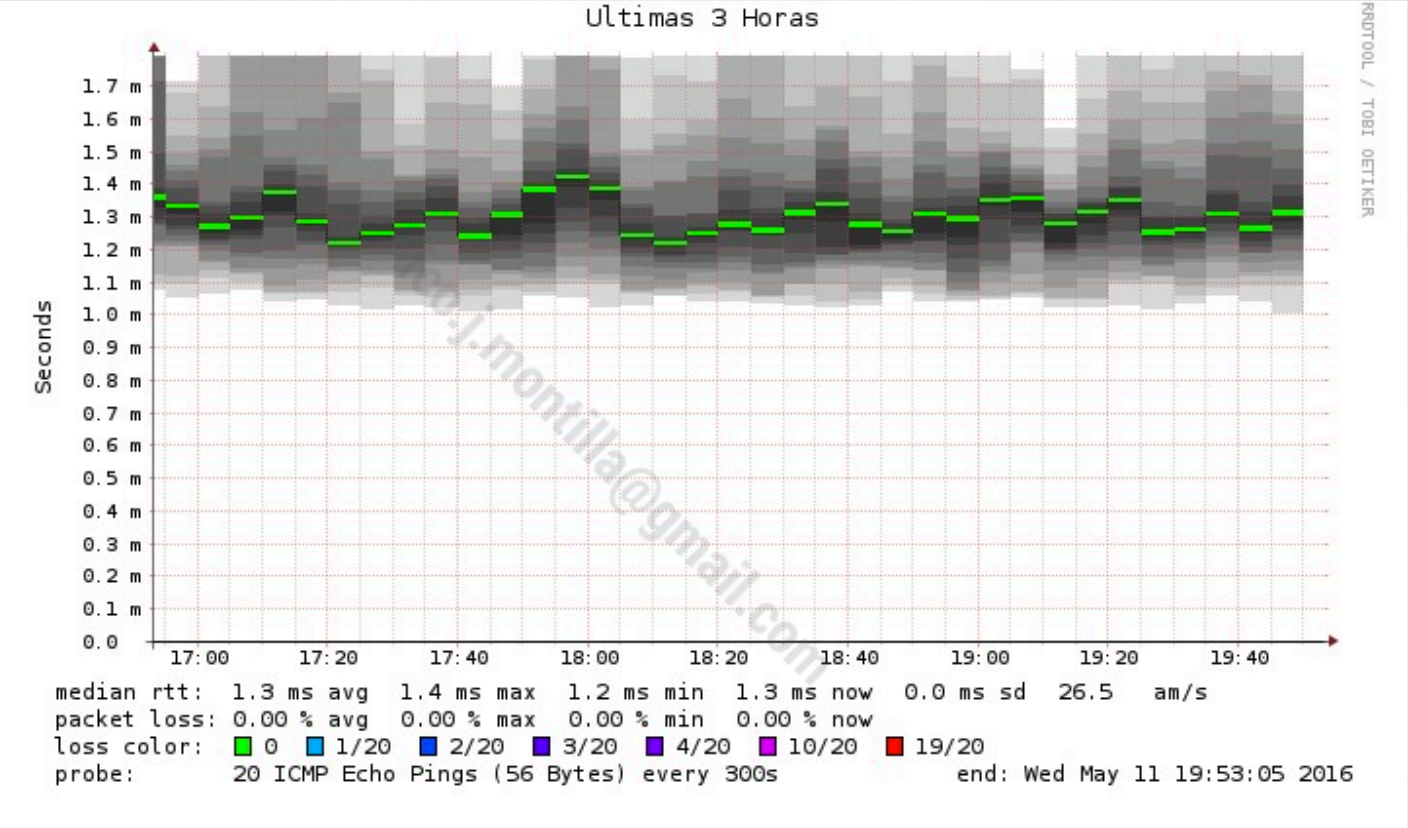
ESTRATEGIA DE DESPLIEGUE: DISTRIBUCIÓN





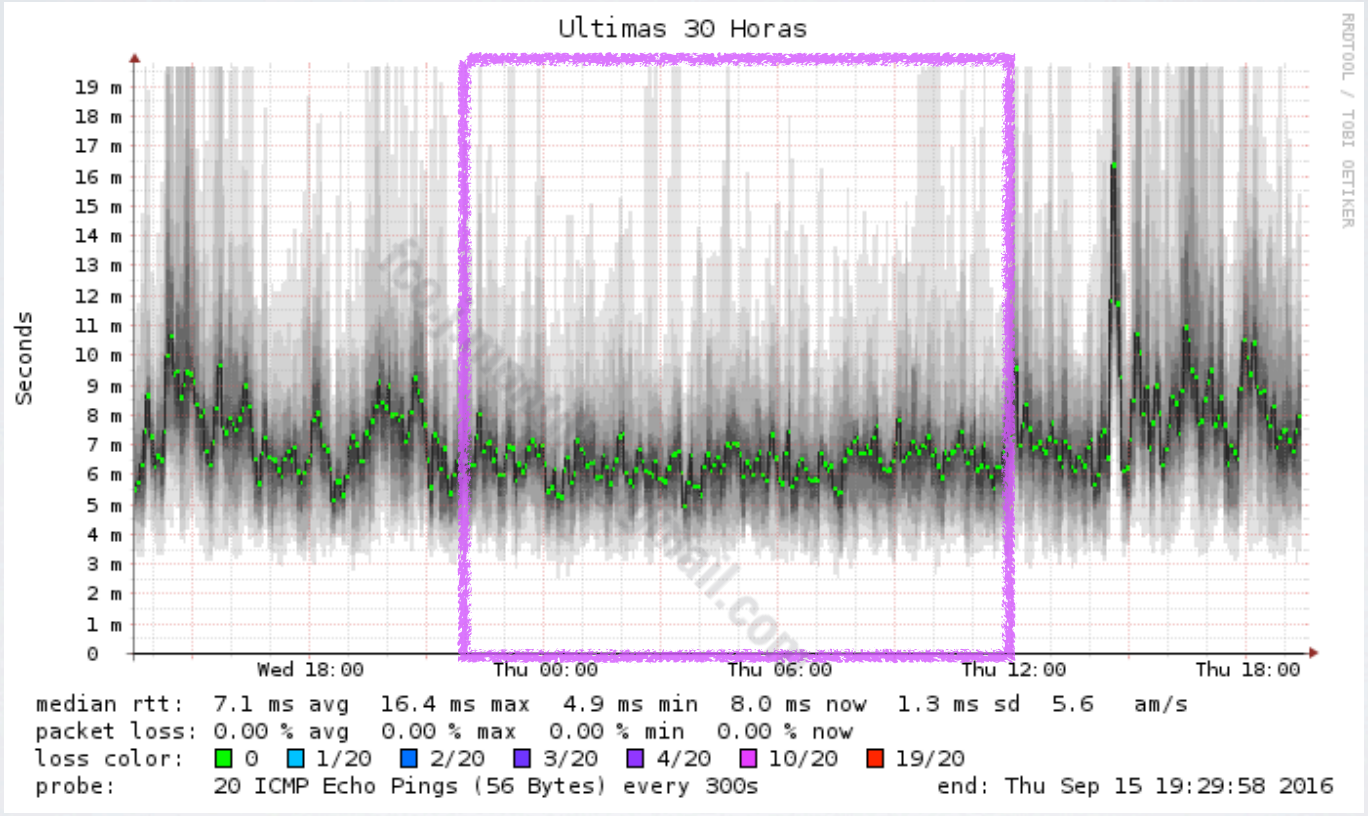
SMOKEPING

ENTRENANDO OJO Y MENTE: ENLACE ÓPTIMO



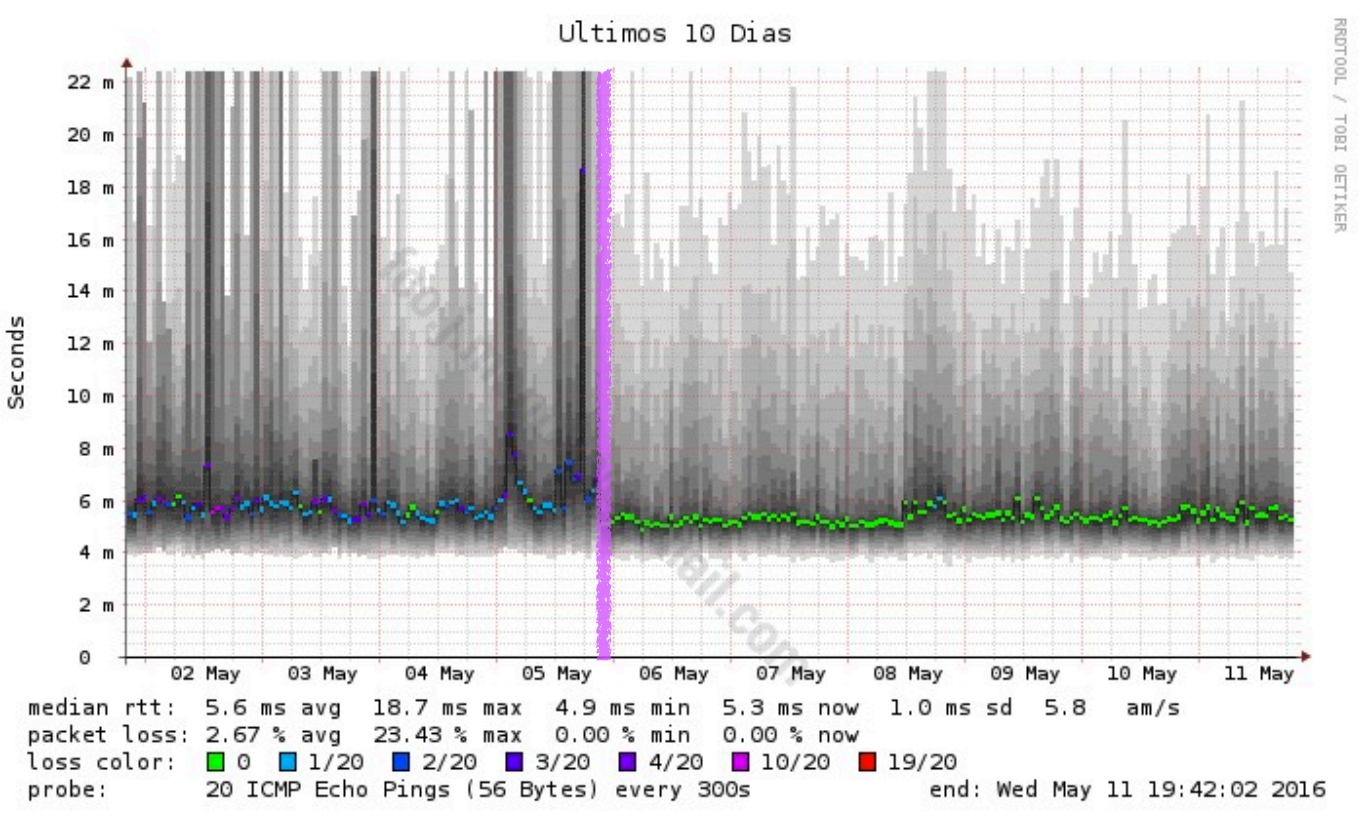
SMOKEPING

ENTRENANDO OJO Y MENTE: NIVELES DETALLE



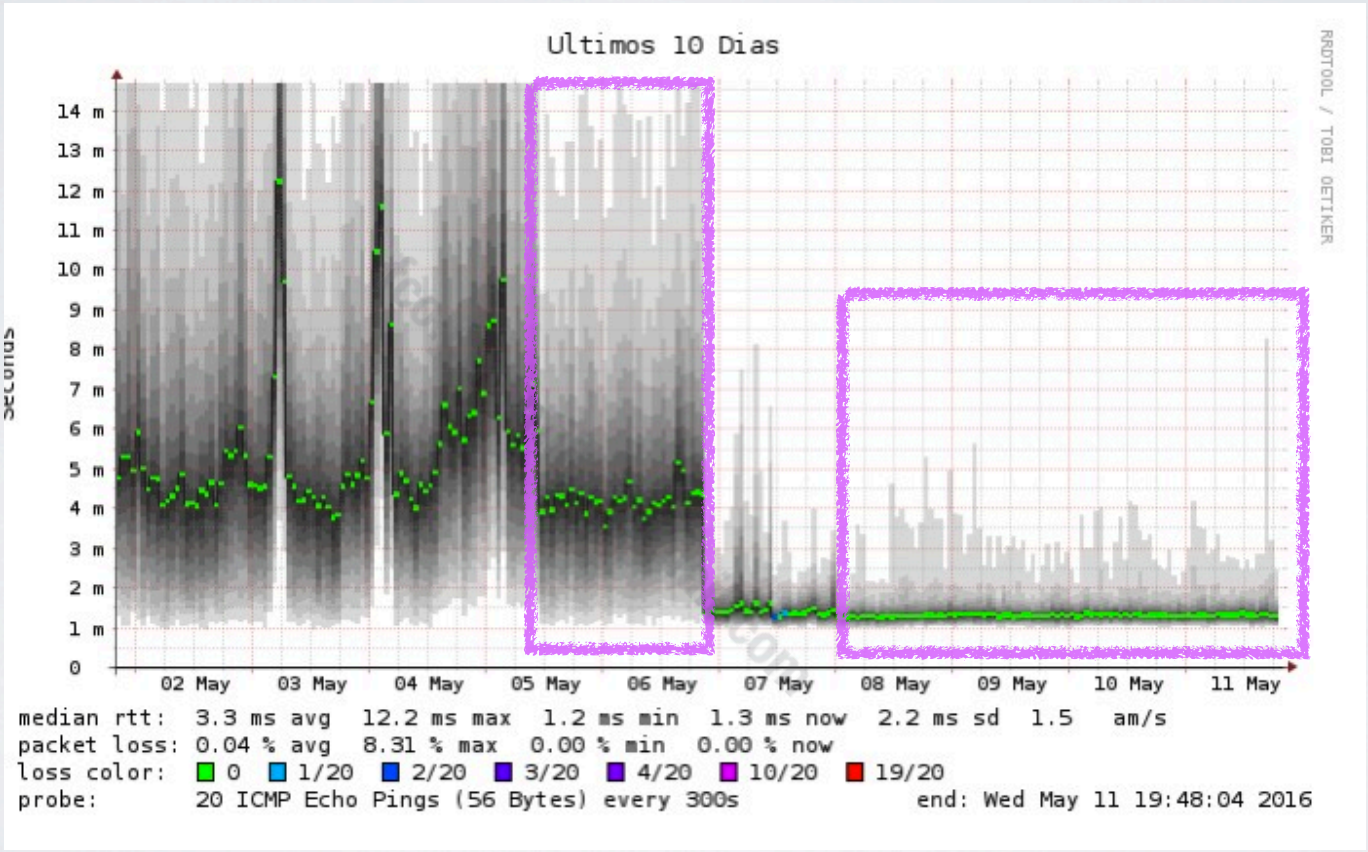
SMOKEPING

ENTRENANDO OJO Y MENTE: PATRONES



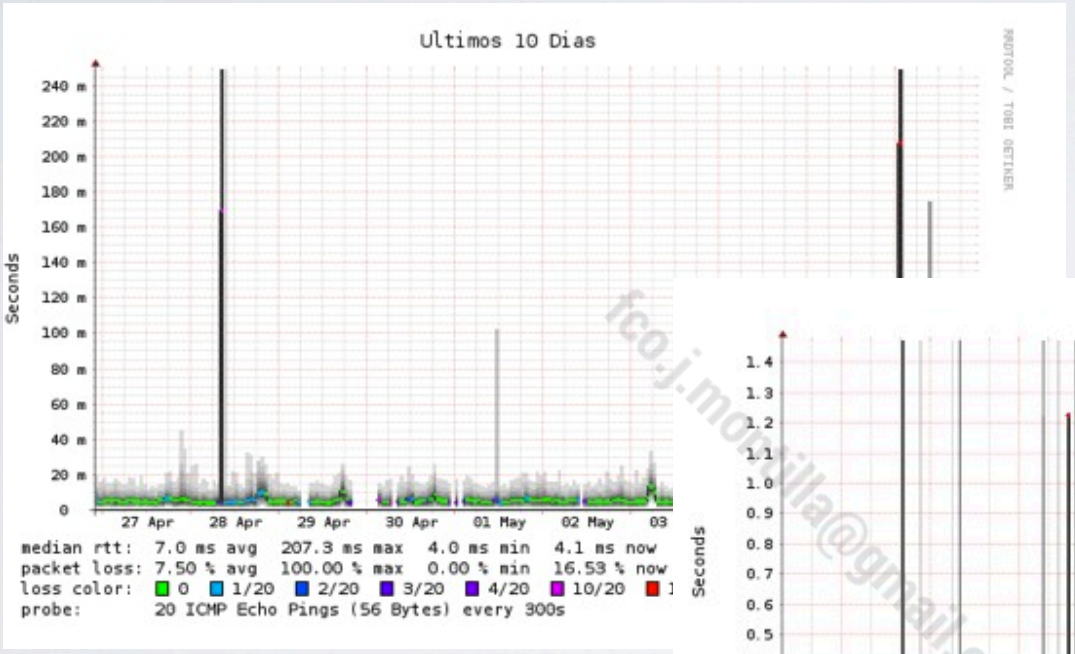
SMOKEPING

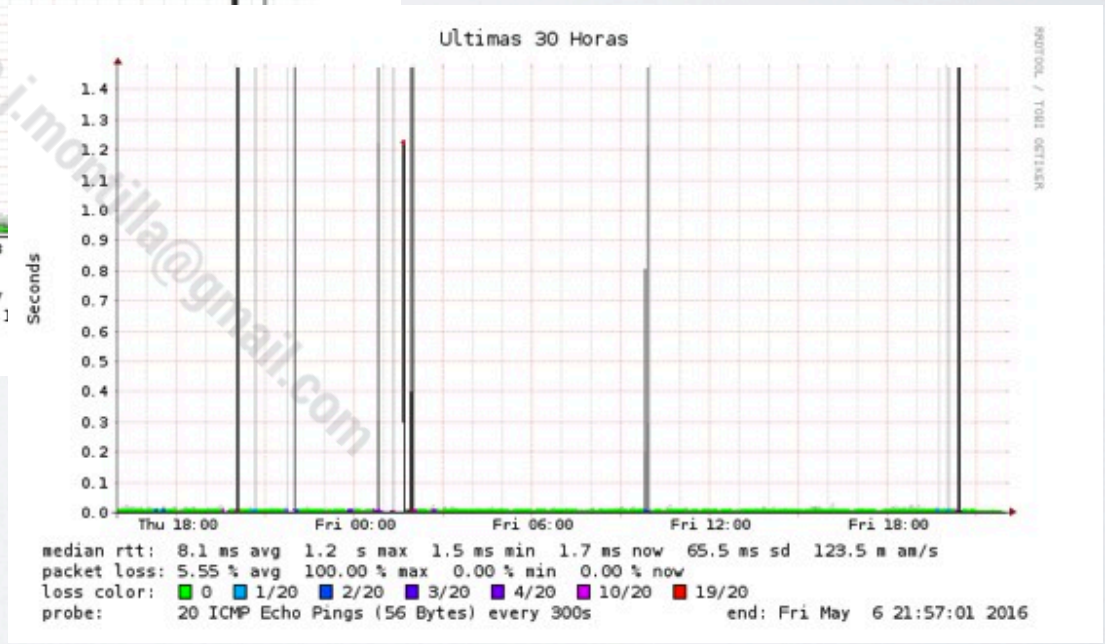
ENTRENANDO OJO Y MENTE: CAMBIOS DE PATRÓN



SMOKEPING

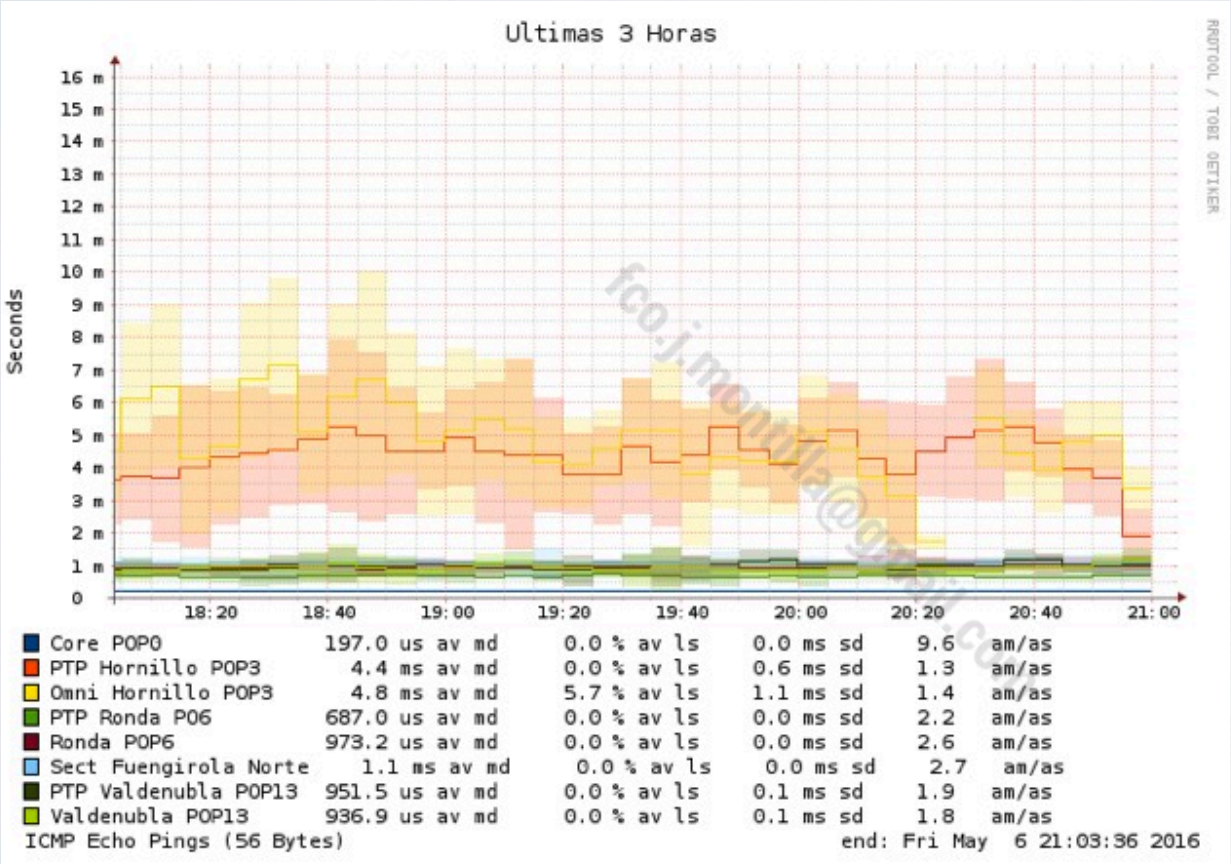
ENTRENANDO OJO Y MENTE: ANOMALÍAS

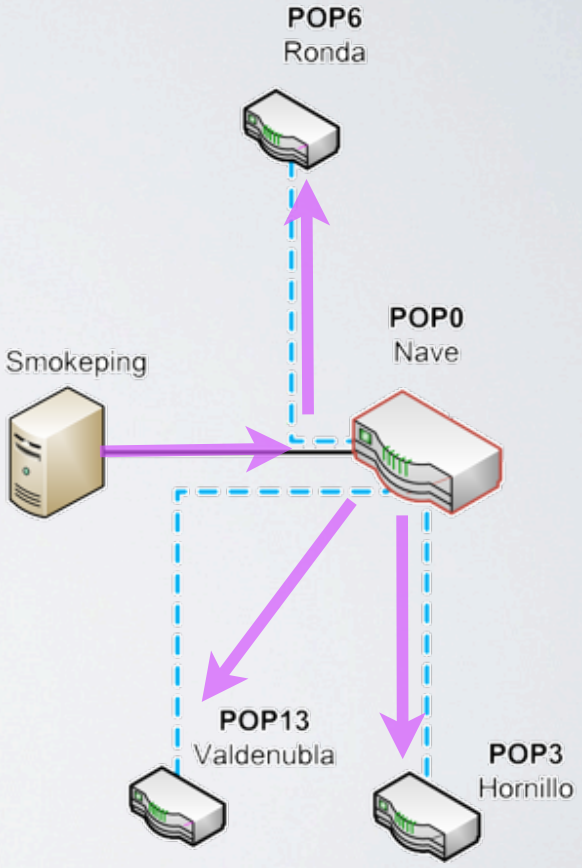




SMOKEPING

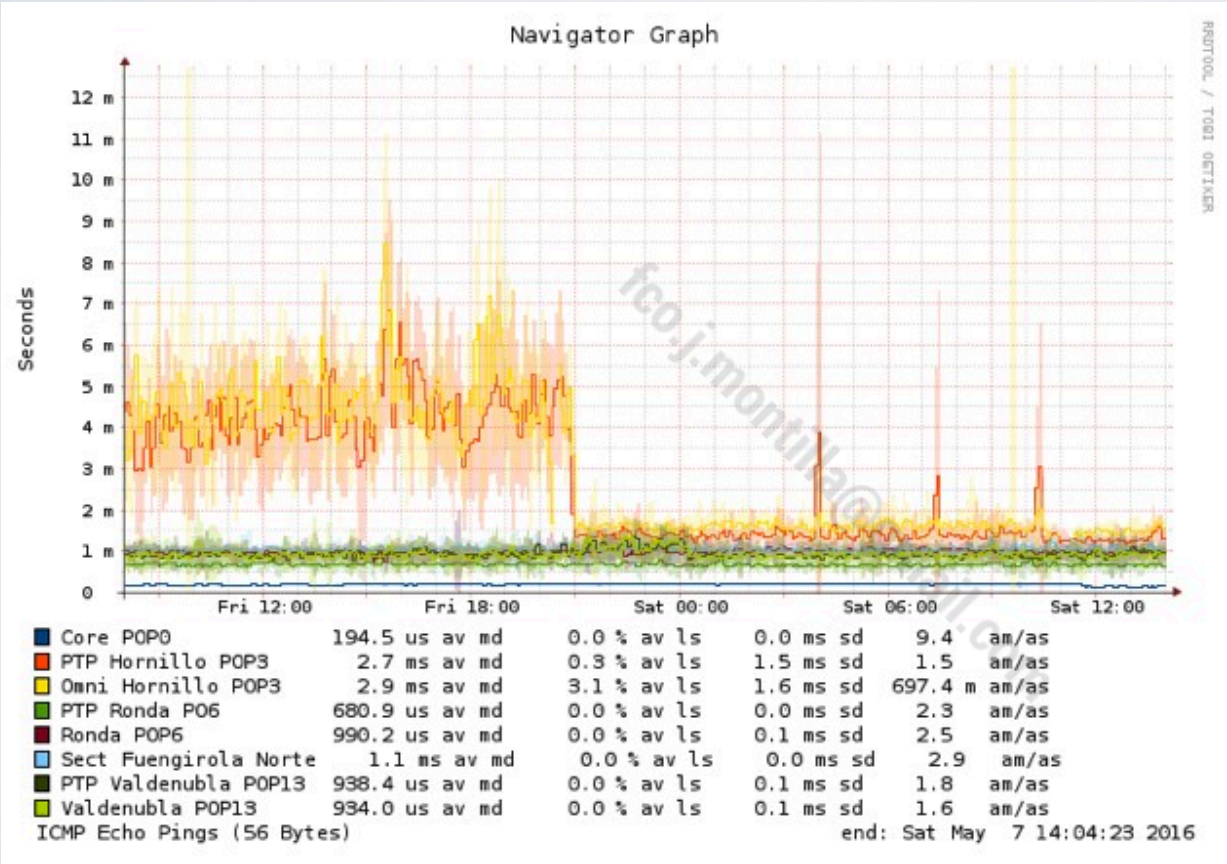
GRÁFICAS CONJUNTAS: IDENTIFICANDO Y AISLANDO

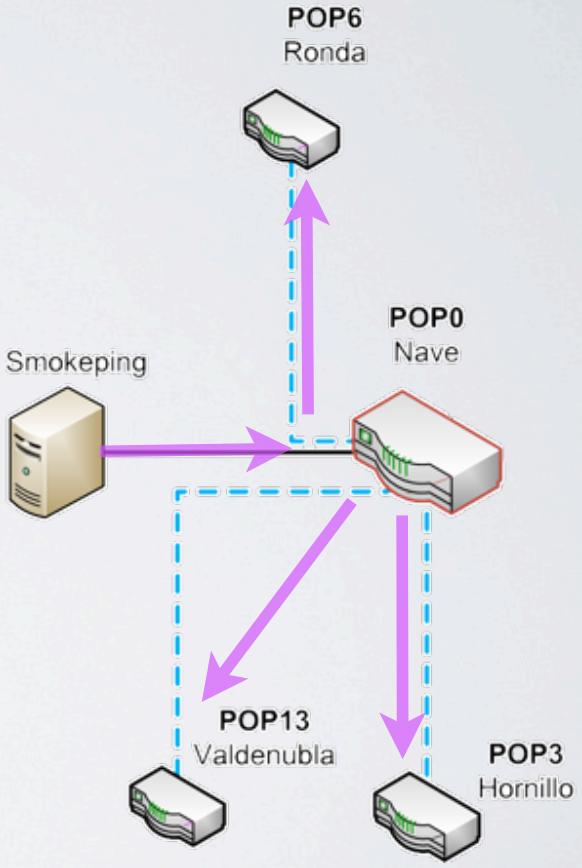




SMOKEPING

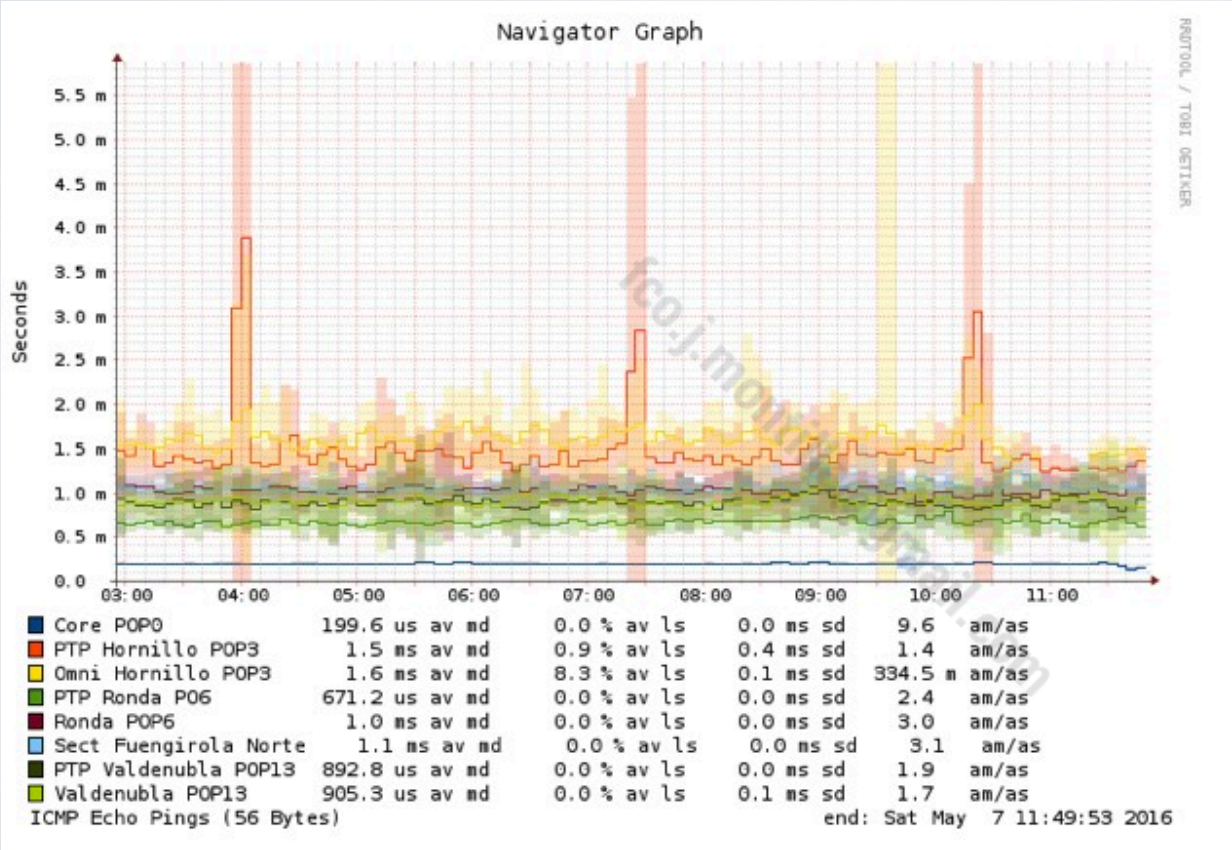
GRÁFICAS CONJUNTAS: IDENTIFICANDO Y AISLANDO

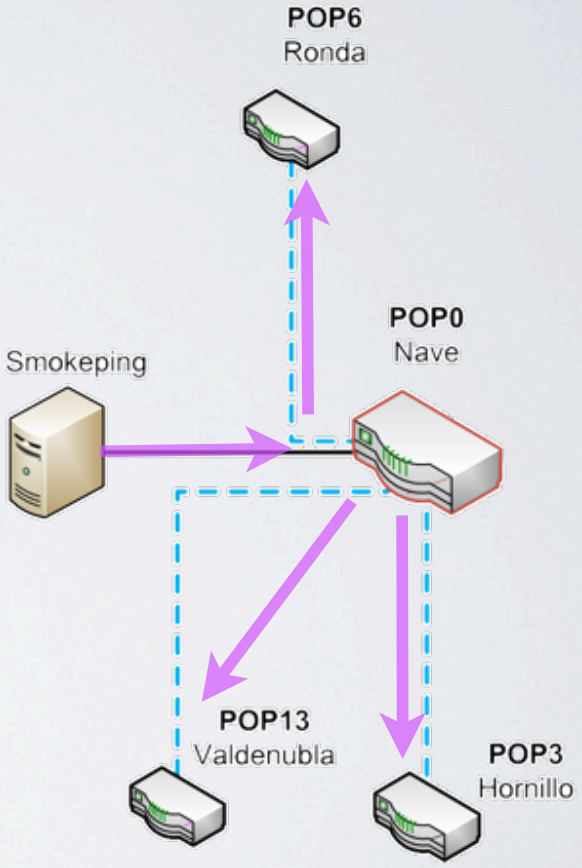




SMOKEPING

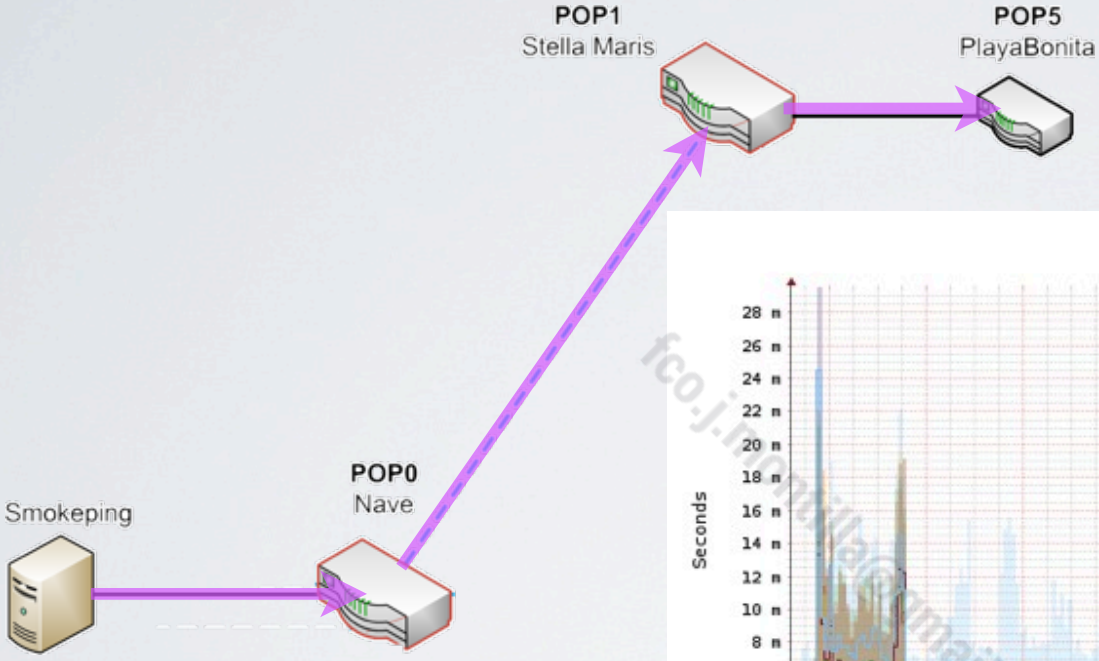
GRÁFICAS CONJUNTAS: IDENTIFICANDO Y AISLANDO

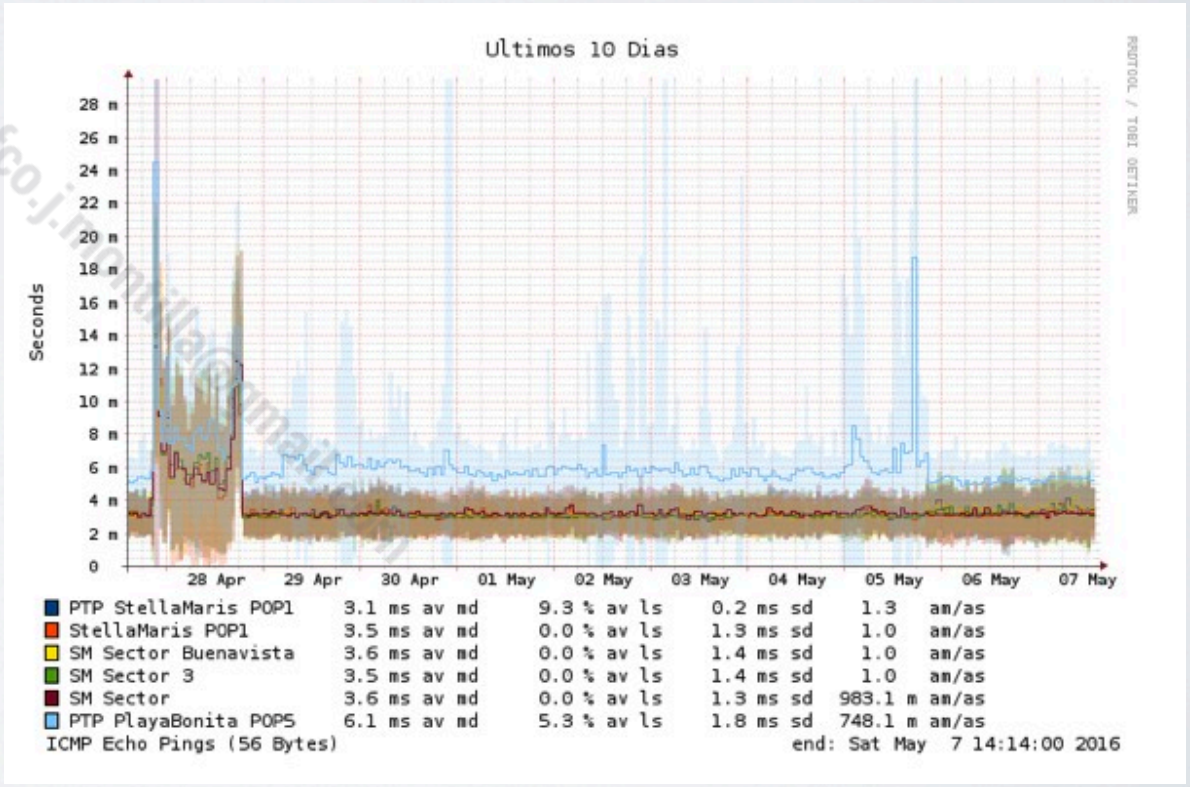




SMOKEPING

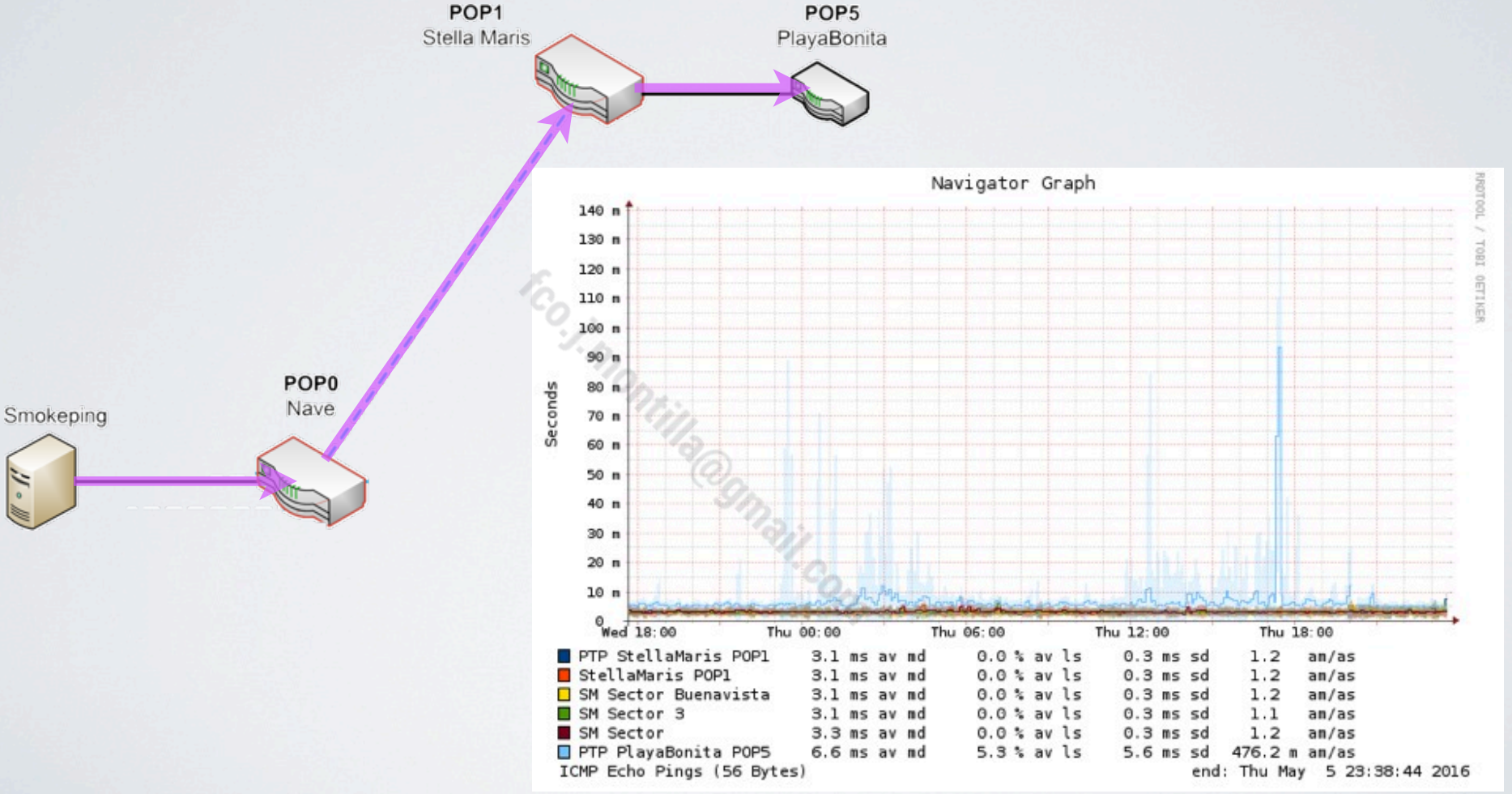
GRÁFICAS CONJUNTAS: IDENTIFICANDO Y AISLANDO





SMOKEPING

GRÁFICAS CONJUNTAS: IDENTIFICANDO Y AISLANDO



SMOKEPING

ADEMÁS...

- Modo maestro: gestión o esclavo: sondas remotas
- Multitud de sondas: DNS, HTTP, VoIP, (SipSak) Radius...
- Extopus: Agregador de Monitorización

http://oss.oetiker.ch/extopus/

SMOKEPING

RECAPITULANDO: CONCLUSIONES

- Porqué gráficos "complejos": aprovechando nuestra ***GPU***
- Smokeping es la herramienta concebida **específicamente** para ello
- Abierta, Flexible, Mínimo Mantenimiento, Cómoda, Eficaz y "coste óptimo"
- Requisitos, Configuración, Estrategias de Despliegue
- Cómo nos permite **Radiografiar** las ***constantes vitales*** de nuestra red:
  - ✓ Detectar problemas de "un vistazo" (Anomalías, Patrones no coincidentes)
  - ✓ Identificar y Aislar problemas, tanto en el ramal como en el tiempo
  - ✓ Análisis cualitativo, precisión al microsegundo (Fping)
  - ✓ Correlacionar saltos (ramales) y eventos en el tiempo

SMOKEPING: PREGUNTAS

- email: **fco.j.montilla@gmail.com**
- PDF actualizado: **https://goo.gl/MLNOZI**
- Próximamente: MTCNA en Sevilla (Oct-Nov)

¡Gracias!