

# RedIRIS Spectrum Reporting Tool

**Watch your Internet access through RedIRIS  
like never before**

Gerson Rodríguez de los Santos López  
gerson.rodriguez@rediris.es

Madrid, 28 de November 2017

# Why we wanted to offer monitoring

---

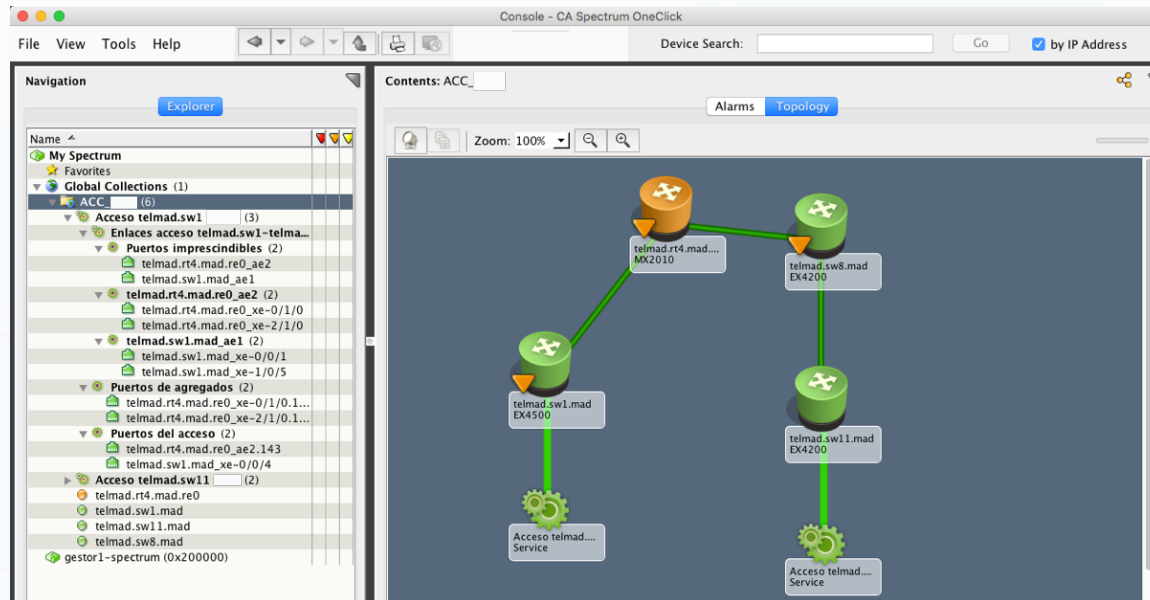
- We offer connectivity service to over 300 institutions in Spain
- IPv4 and IPv6
- DNS
- Addressing
- Peerings with other NRENs/providers and relevant ASes
- We want to offer tools linked to these services to provide not only a connectivity service, but a way to see how well the connection is doing:
  - Tool to solve performance problems
  - Speed test
  - Looking glass
  - Connection control and reporting tool

# The tools

---

- Three tools to provide information on different aspects of the network:
- OneClick: network monitoring
  - Show link status
  - Show alarms
- Performance Center: measure raw performance
  - Traffic through interfaces
  - Access node status
  - General Netflow information
  - Send monthly reports (email)
- Netflow Analysis: Protocol and host dissection
  - Access Netflow information for each interface
  - Monthly reports with Netflow information (email)

# One Click console

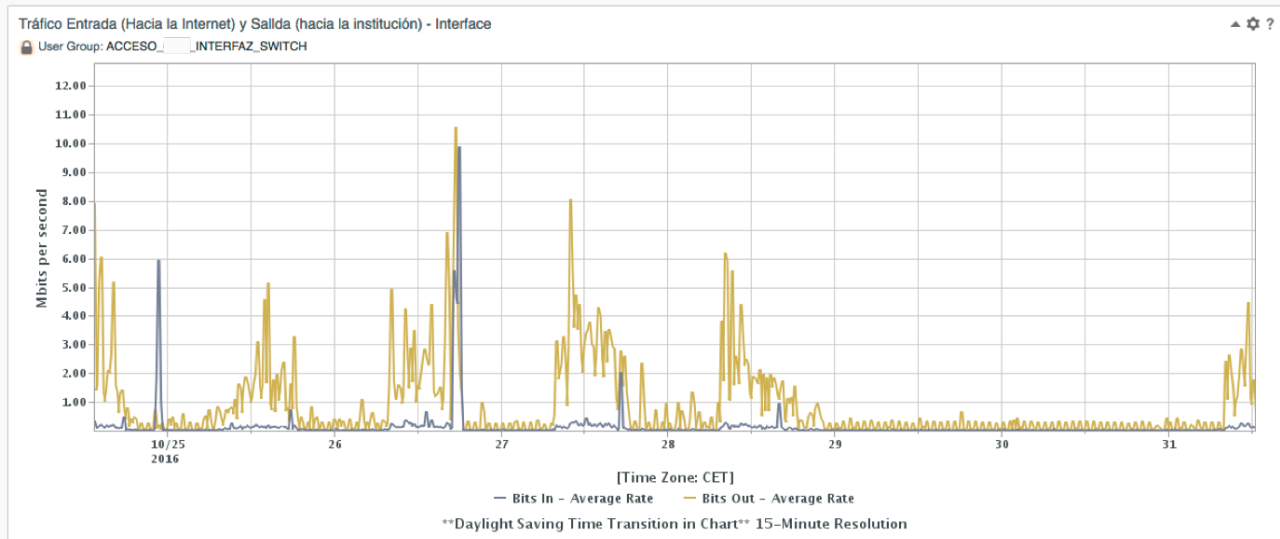


- Link down alarms
- Send alarm details to your mail account\*
- Topology view

\*Manual process, does not automatically send every alarm that is triggered

- Raw Network usage:
  - In/Out traffic
  - Discarded packets
  - Errors
  - Access switch CPU utilisation and memory occupation
- Select custom time ranges
- Zoom in on each graph separately
- Receive a monthly report through email
- Email a report for a custom time range

# Performance Center



Errores y descartes en enlace de acceso - Interface

User Group: ACCESO\_...INTERFAZ\_SWITCH

Resolution: Hourly Roll-up (Default)

Device Name	Name	Description	Errors In - Total	Errors Out - Total	Discards In - Total	Discards Out - Total
telmad.sw11.mad.red.rediris.es	ge-1/0/7 -- Línea de acceso ...	ge-1/0/7	0 pkts	0 pkts	0 pkts	0 pkts

Search

Page 1 of 1

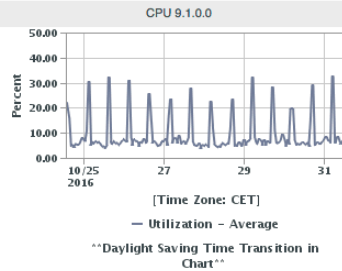
Displaying 1 - 1 of 1

Max Per Page 10

## Uso de CPU en switch de acceso - CPU - Utilization - Average



User Group: ACCESOS\_TELMAD\_SW11\_COMUNES



Device Name	Name	Utilization - Average
telmad.sw11.mad.red.rediris.es	CPU 9.1.0.0	8.32%
telmad.sw11.mad.red.rediris.es	CPU 9.2.0.0	3.71%

Page 1 of 1 | Displaying 1 - 2 of 2

## Uso de memoria en nodo de acceso - Memory

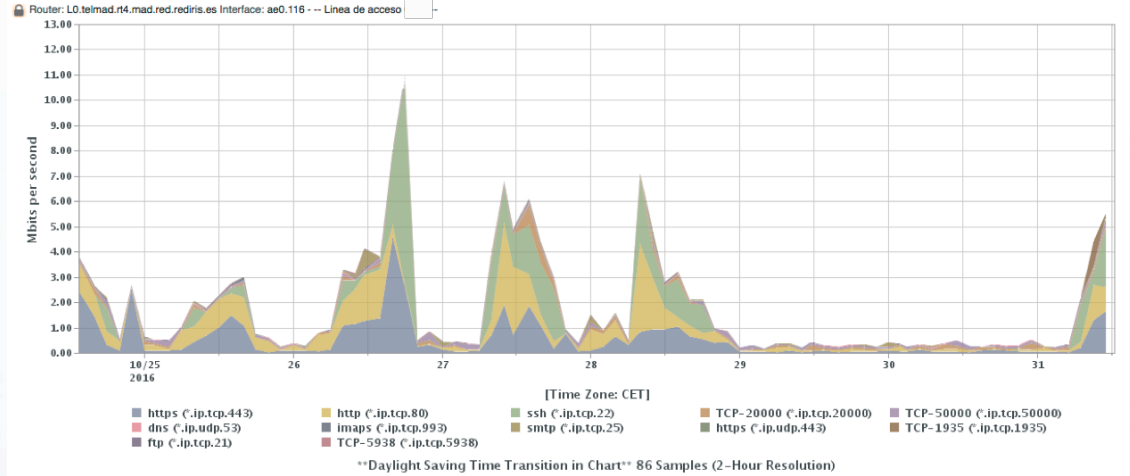


User Group: ACCESOS\_TELMAD\_SW11\_COMUNES

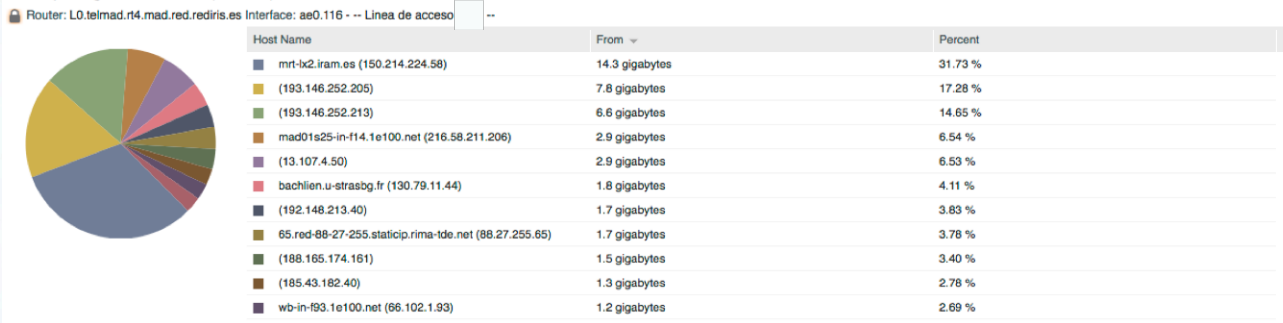
Resolution: Hourly Roll-up (Default)

Device Name	Name	Description	Utilization - Average
telmad.sw11.mad.red.rediris.es	Memory 9.1.0.0	Juniper Memory Statistics 9.1.0.0	56%
telmad.sw11.mad.red.rediris.es	Memory 9.2.0.0	Juniper Memory Statistics 9.2.0.0	48%

## Protocolos que generan más tráfico (ambas direcciones, tendencia en el tiempo) - Total - Rate



## Hosts que originan más tráfico (sectorial) - From





# Netflow Analysis

---

- View Netflow information concerning your access live
  - Hosts
  - Protocols
  - AS
  - Send an email with the selected time range
- Monthly reports
  - Which hosts do you exchange more information with?
  - Which hosts do generate the largest traffic volume?

# Netflow Analysis

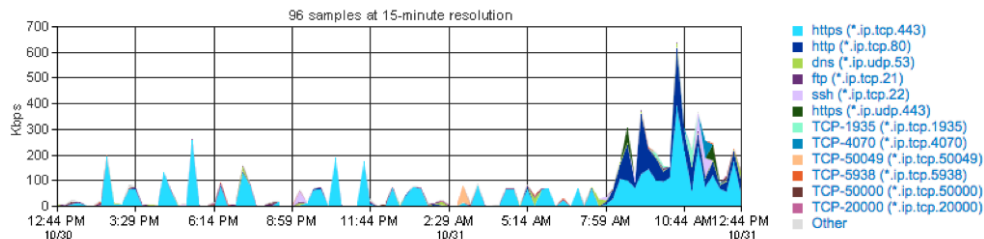
## Flow Forensics

### Stacked Protocol Trend - In

October 30, 2016 12:52:00 PM - October 31, 2016 12:52:00 PM CET

telmad.rt4.mad.re0 (130.206.206.250)::ae0.116 -- Linea de acceso

20.00 Gbps

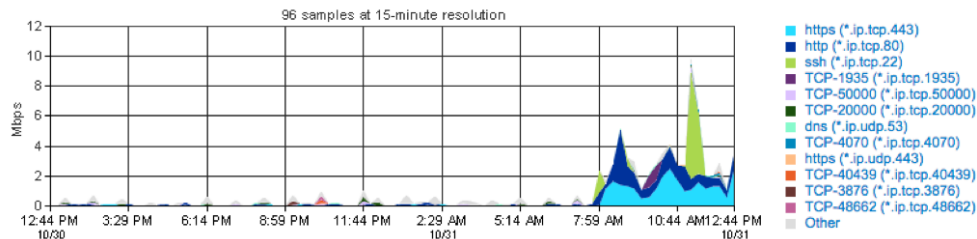


### Stacked Protocol Trend - Out

October 30, 2016 12:52:00 PM - October 31, 2016 12:52:00 PM CET

telmad.rt4.mad.re0 (130.206.206.250)::ae0.116 -- Linea de acceso

20.00 Gbps



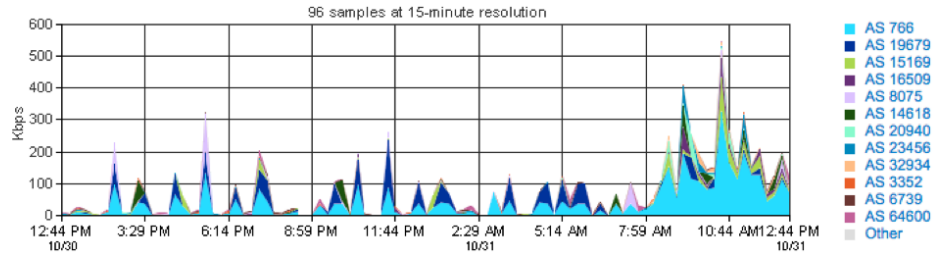
# Netflow Analysis

## Stacked AS Trend - In

October 30, 2016 12:53:00 PM - October 31, 2016 12:53:00 PM CET

telmad.r4.mad.re0 (130.206.206.250):ae0.116 -- Linea de acceso

20.00 Gbps

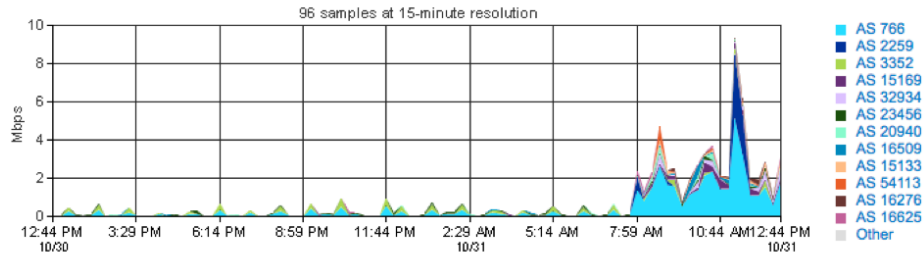


## Stacked AS Trend - Out

October 30, 2016 12:53:00 PM - October 31, 2016 12:53:00 PM CET

telmad.r4.mad.re0 (130.206.206.250):ae0.116 -- Linea de acceso

20.00 Gbps



# Netflow Analysis

## Host Summary Pie Chart - To

September 19, 2016 12:15:00 PM - October 19, 2016 12:15:00 PM CEST

Informe Acceso  con filtro (incluye rango)

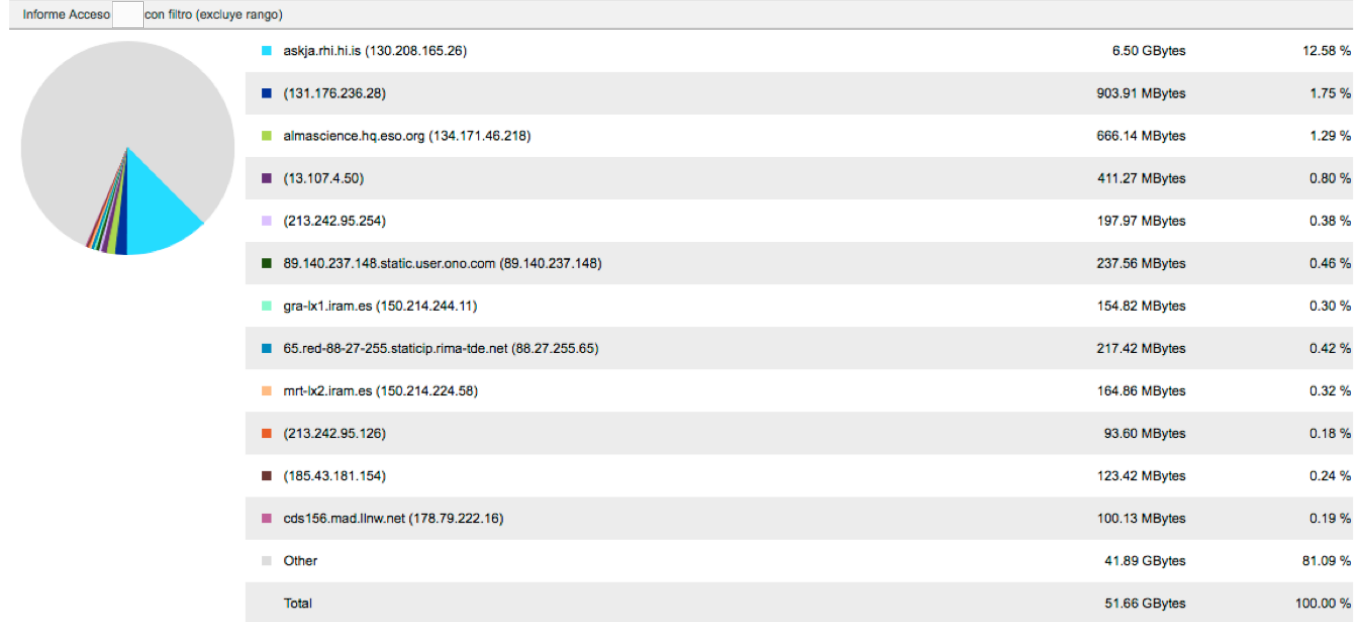


(193.146.252.205)	973.51 GBytes	95.89 %
(193.146.252.213)	29.25 GBytes	2.88 %
remote0.oan.es (193.146.252.210)	7.04 GBytes	0.69 %
mercurio.oan.es (193.146.252.206)	3.41 GBytes	0.34 %
(193.146.252.197)	612.79 MBytes	0.06 %
remote1.oan.es (193.146.252.211)	546.29 MBytes	0.05 %
(193.146.252.196)	421.49 MBytes	0.04 %
(193.146.252.227)	17.58 MBytes	0.00 %
(193.146.252.200)	12.84 MBytes	0.00 %
(193.146.252.224)	12.08 MBytes	0.00 %
(193.146.252.202)	12.07 MBytes	0.00 %
(193.146.252.194)	11.58 MBytes	0.00 %
Other	334.50 MBytes	0.03 %
Total	1.02 TBytes	100.00 %

# Netflow Analysis

## Host Summary Pie Chart - To

September 19, 2016 12:15:00 PM - October 19, 2016 12:15:00 PM CEST



# Deployment

---

- Deployment started: May 2017
  - [https://www.rediris.es/servicios/soporte\\_instituciones/herr-monitor/monitorizacion.html.es](https://www.rediris.es/servicios/soporte_instituciones/herr-monitor/monitorizacion.html.es)
- Service enabled for 78 institutions as of today
  - 46 with direct access to RedIRIS (direct IP delivery)
  - 32 with indirect access (through regional network)
- Integration with SIR authentication (work in progress)
  - We are solving the issue with the developers
  - Some tools do not still support it (but it is in the roadmap)

- Platform is shared with RedIRIS
- Different levels of access according to the type of user
  - Full access for RedIRIS's own staff
  - Partial access for institutions
- Give each user vision of its own part of the network
- Dashboard and report design and scheduling

## Technical issues (2): One Click

---

- Setting roles and privileges associated
- Controlling what part of the network the user sees
- Alarm filtering
- Cannot offer monitoring if the institution connects through a regional network



## Technical issues (3) Performance Center

---

- Creating roles in Performance center
- Define a template for dashboards and adapt it to each special case
- Special cases (eg: directly connected to router or aggregated interfaces): needs consideration
- Map resources to users
- Copying dashboards and changing each field
- Creating users
- Work in progress: automation process through scripting
- Cannot provide Performance Center access if the institution is indirectly connected

## Technical issues (4) Netflow Analysis

---

- Showing all relevant information in the reports
- Lack of granularity
- Direct access vs regional networks: restrictions in reports apply
- Some options not available in custom reports for Netflow (eg: show ASes)
- Sending reports with enough spacing: table with schedules
- Work in progress: “Ghost traffic”, Small institutions get hidden if they do not move enough traffic

# Feedback from users

---

- IPv6 support
- Reports for specific ranges (eg: WiFi access)
- BGP alarms
- Ability to define filters by IP address and time in Netflow reports
- Higher sampling rates for Netflow
- Monitoring other connections apart from the IP access connections. As of now, only the Internet connection associated with the institution is included.
  - Eg: One institution has an IP connection different from the main IP connection used to access the Internet. This second IP connection is used to join a worldwide collaboration network

**Thank you for  
your attention!  
Any questions?**