

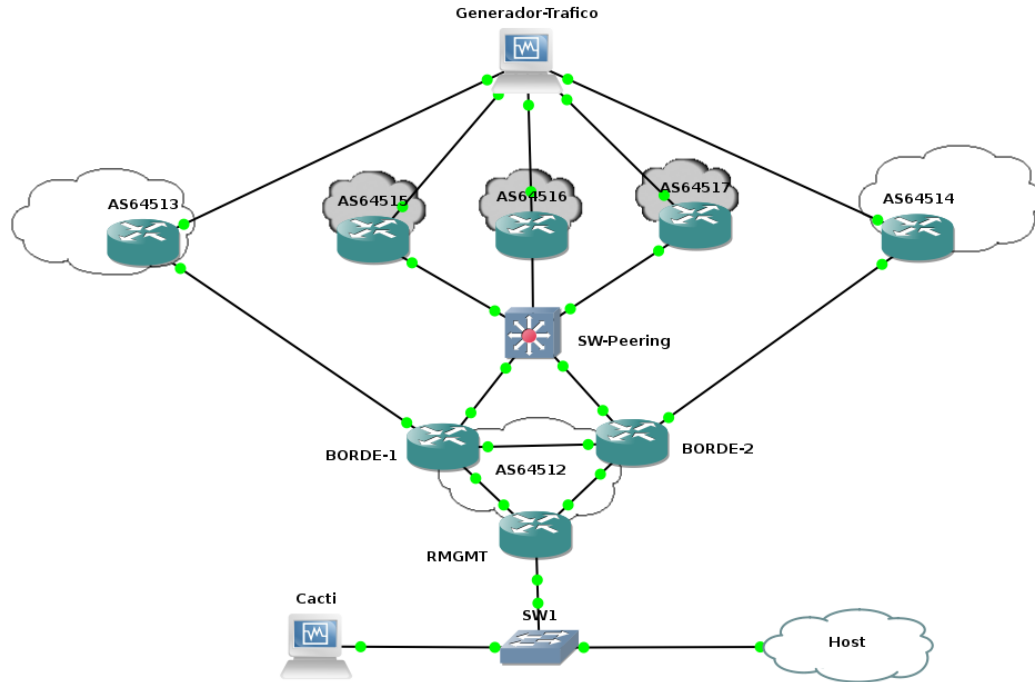
Cacti + PHP-Weathermap

Taller Monitoreo - Lacnog 2015

Monitoreo de enlaces de tránsito y peering

- Qué nos puede interesar monitorear de nuestros enlaces?
 - Utilización del CIR y el Burst (ej. percentil 95)
 - Tráfico por sistema autónomo.
 - Tráfico por zona geográfica por enlace.
 - Consumo de CDNs
 - Clientes BGP.
 - Tráfico por servicio/tecnología de acceso/usuario
 - Tráfico v4/v6, por aplicación, etc.
- Herramientas disponibles.
 - Comerciales (ej. Arbor).
 - Libres (NFCAPD, NFDUMP, NFSEN, CFLOWD, MRTG, CACTI, WEATHERMAPS, etc)
- Quienes requieren esta información?
 - Grupos de O&M, Planificación de red y Capacidad, Aseguramiento de Infraestructura, Gestión de Producto (planificación y costeo), Finanzas, etc, etc.

Maqueta de red y herramientas libres



- GNS3 para simular la red de la figura.
- Routers de borde con conexiones de tránsito (65536/65537) y peering.
- Agentes SNMP y NF v9 en routers.
- Generador de tráfico IPERF en VM Debian.
- Colector de tráfico (IPERF, NFCAPD) + Gestor (CACTI + Weathermap) en VM Debian.
- Conexión al host (via interface tap) para acceso a CACTI y Weathermap.

Cacti (www.cacti.net)

- Herramienta bajo licencia GNU-GPL.
- Brinda un front-end web completo para monitorizar hasta cientos de elementos. Basada en PHP, utiliza MySQL y RRDs para almacenar configuraciones y estadísticas.
- Administración de usuarios con permisos por áreas y funciones.
- Soporte SNMP (poller propio para manejar gran cantidad de dispositivos) y scripts externos para recolectar los datos.
- Genera, organiza y visualiza los gráficos creados.
- Creación de nuevos Templates para dispositivos y gráficos.
- Permite su modificación e integración de nuevas herramientas (add-ons).

Instalación de Cacti

- En distribuciones basadas en Debian

```
apt-get install cacti
```

- Esto instalará cacti y sus dependencias (apache, php, mysql, etc.)
- En el proceso de instalación se nos podrá consultar y solicitar:
 - Web Server a utilizar (si tenemos más de uno instalado)
 - Password de administración para mysql (si no lo teníamos previamente instalado).
 - Password de administración de mysql para crear la base de datos que usará Cacti.
 - Password de administración para Cacti en mysql si decidimos configurarlo desde allí (no tiene que ser el mismo password que para toda la base de datos).

Configuración de Cacti

- Luego de instalar Cacti debemos configurarlo.
- Para ello utilizamos el navegador visitando el siguiente URL y finalizamos la instalación: <http://IP-ADDRESS/cacti>

Cacti Installation Guide

Thanks for taking the time to download and install cacti, the complete graphing solution for your network. Before you can start making cool graphs, there are a few pieces of data that cacti needs to know.

Make sure you have read and followed the required steps needed to install cacti before continuing. Install information can be found for [Unix](#) and [Win32](#)-based operating systems.

Also, if this is an upgrade, be sure to reading the [Upgrade](#) information file.

Cacti is licensed under the GNU General Public License, you must agree to its provisions before continuing:

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

[Next >>](#)

Cacti Installation Guide

Please select the type of installation

The following information has been determined from Cacti's configuration file. If it is not correct, please edit 'include/config.php' before continuing.

Database User: cacti
Database Hostname: localhost
Database: cacti
Server operating System Type: unix

[Next >>](#)

Cacti Installation Guide

Make sure all of these values are correct before continuing.

[FOUND] RRDTool Binary Path: The path to the rrdtool binary.
/usr/bin/rrdtool
[OK: FILE FOUND]

[FOUND] PHP Binary Path: The path to your PHP binary file (may require a php recompile to get this file).
/usr/bin/php
[OK: FILE FOUND]

[FOUND] snmpwalk Binary Path: The path to your snmpwalk binary.
/usr/bin/snmpwalk
[OK: FILE FOUND]

[FOUND] snmpget Binary Path: The path to your snmpget binary.
/usr/bin/snmpget
[OK: FILE FOUND]

[FOUND] snmpbulkwalk Binary Path: The path to your snmpbulkwalk binary.
/usr/bin/snmpbulkwalk
[OK: FILE FOUND]

[FOUND] snmpgetnext Binary Path: The path to your snmpgetnext binary.
/usr/bin/snmpgetnext
[OK: FILE FOUND]

[FOUND] Cacti Log File Path: The path to your Cacti log file.
/var/log/cacti.log
[OK: FILE FOUND]

SNMP Utility Version: The type of SNMP you have installed. Required if you are using SNMP v2c or don't have embedded SNMP support in PHP.
NET-SNMP 5.x

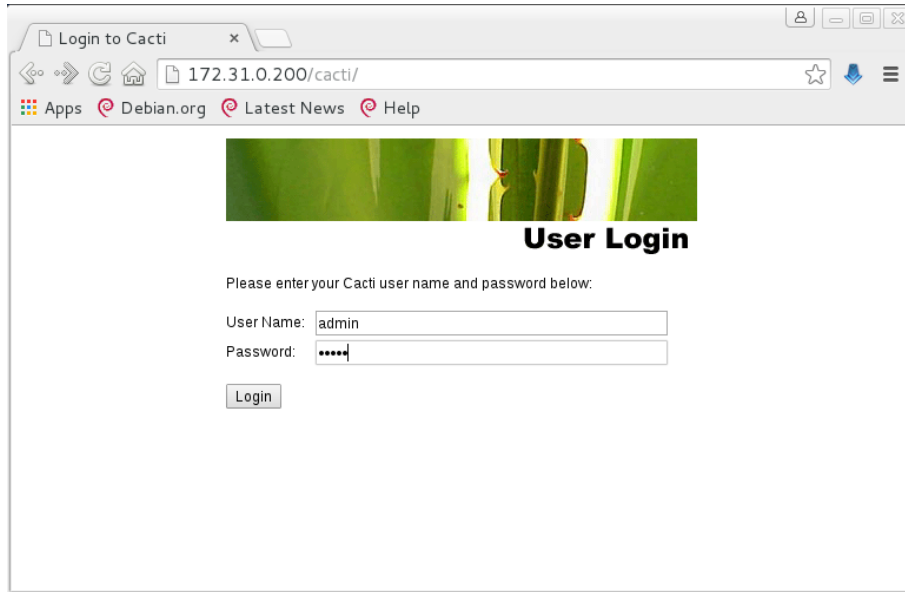
RRDTool Utility Version: The version of RRDTool that you have installed.
RRDTool 1.4.x

NOTE: Once you click "Finish", all of your settings will be saved and your database will be upgraded if this is an upgrade. You can change any of the settings on this screen at a later time by going to "Cacti Settings" from within Cacti.

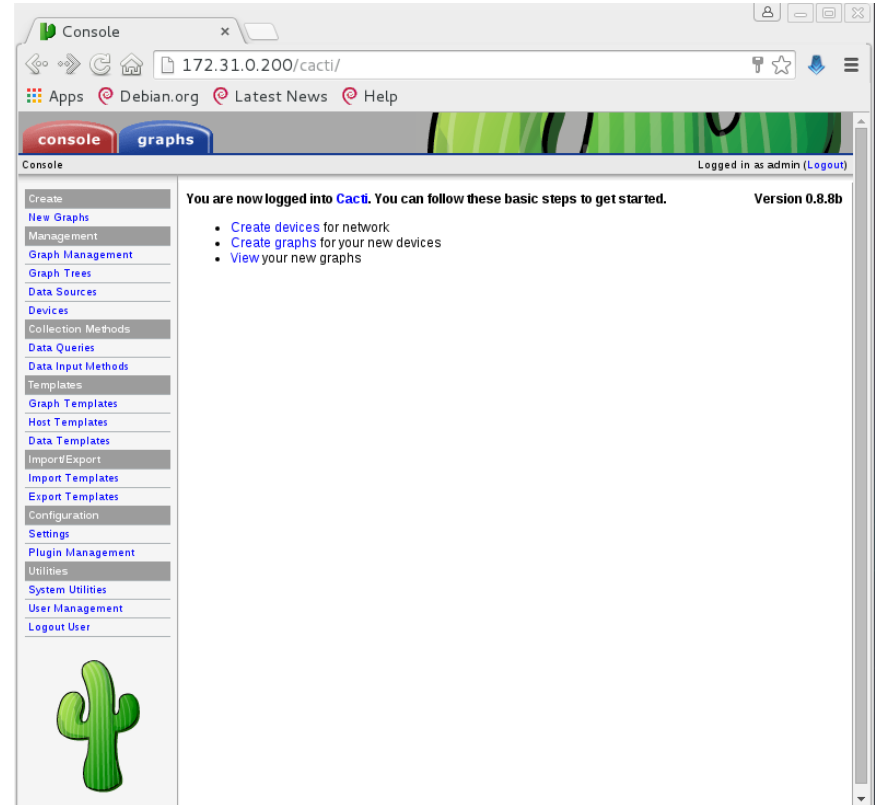
[Finish](#)

Iniciamos sesión y agregamos los dispositivos

- Usuario por defecto admin/cacti



The screenshot shows the 'Login to Cacti' page in a web browser. The address bar shows '172.31.0.200/cacti/'. The page features a green banner with a cactus image and the text 'User Login'. Below the banner, there is a prompt: 'Please enter your Cacti user name and password below:'. There are two input fields: 'User Name:' with 'admin' entered, and 'Password:' with '****' entered. A 'Login' button is located below the password field.



The screenshot shows the Cacti Console dashboard after a successful login. The browser address bar shows '172.31.0.200/cacti/'. The page title is 'Console' and the user is logged in as 'admin'. The dashboard includes a navigation menu on the left with categories like 'Create', 'Management', 'Data Sources', 'Devs', 'Collection Methods', 'Data Queries', 'Data Input Methods', 'Templates', 'Import/Export', 'Configuration', 'Settings', 'Plugin Management', 'Utilities', 'System Utilities', and 'User Management'. The main content area displays a welcome message: 'You are now logged into Cacti. You can follow these basic steps to get started.' followed by three bullet points: 'Create devices for network', 'Create graphs for your new devices', and 'View your new graphs'. The version '0.8.8b' is shown in the top right corner. A green cactus icon is visible in the bottom left corner of the dashboard.

Network-Weathermap (network-weathermap.com)

- Herramienta open source para visualizar elementos y datos en un mapa.
- Colecta información con plugins: soporte de RRDs, MRTG, archivos de texto, SNMP, fping, datos desde CACTI y scripts externos.
- Los mapas se crean “a mano” a partir de la documentación o utilizando un editor web (con funcionalidades acotadas).
- La integración con Cacti permite además brindar control de acceso a los mapas.

Instalación de Cacti Plugin.

- Requiere la instalación de la “Cacti Plugin-Architecture” (PIA) en versiones anteriores a Cacti 0.8.8.
- Obtengo el zip para la instalación:

```
wget network-weathermap.com/files/php-weathermap-0.97c.zip
```

- Descomprimir el contenido en `/usr/share/cacti/site/plugins/`. y dar permiso al usuario web para escribir los mapas.

```
chown www-data /usr/share/cacti/site/plugins/weathermap/output
```

- Desde Cacti se instala el plugin visitando Configuration-> Plugin Management y haciendo click en “Actions” (Install).
- Este proceso tiene bastante más pasos en versiones anteriores de Cacti.

Instalación de Cacti Editor.

- No tiene integración con el gestor de usuarios de Cacti (restringir con apache Deny, Allow o usar y luego cambiar permisos).
- Requiere la instalación de la biblioteca GD para manipular imágenes.

```
apt-get install php5-gd && /etc/init.d/apache2 reload
```

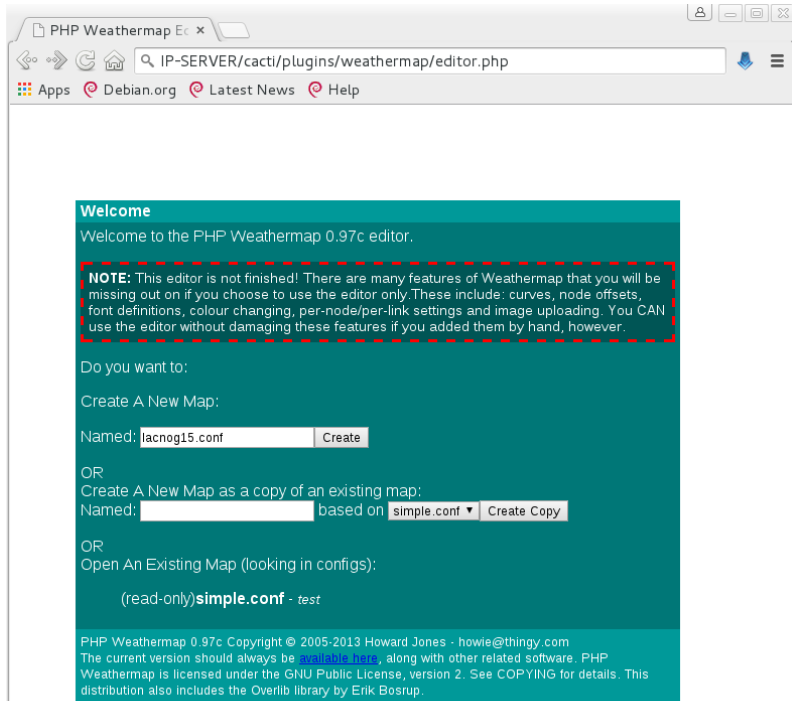
- Modifico los permisos de la carpeta donde se almacenan las configuraciones.

```
chown www-data /usr/share/cacti/site/plugins/weathermap/configs
```

Chequeo en: <http://IP-SERVER/cacti/plugins/weathermap/editor.php>

Weathermap Editor

- Elegir un nombre.conf para el mapa, crear y diseñarlo.



PHP Weathermap Editor

IP-SERVER/cacti/plugins/weathermap/editor.php

Apps Debian.org Latest News Help

Welcome

Welcome to the PHP Weathermap 0.97c editor.

NOTE: This editor is not finished! There are many features of Weathermap that you will be missing out on if you choose to use the editor only. These include: curves, node offsets, font definitions, colour changing, per-node/per-link settings and image uploading. You CAN use the editor without damaging these features if you added them by hand, however.

Do you want to:

Create A New Map:

Named: Create

OR

Create A New Map as a copy of an existing map:

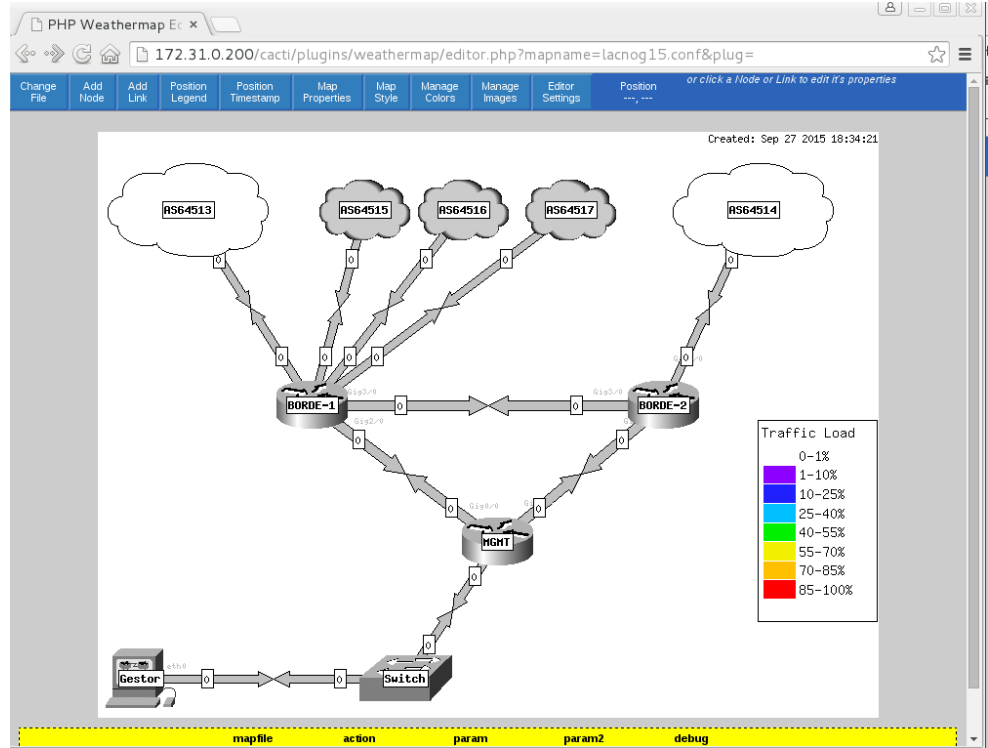
Named: based on Create Copy

OR

Open An Existing Map (looking in configs):

(read-only) - test

PHP Weathermap 0.97c Copyright © 2005-2013 Howard Jones - howie@thingy.com
The current version should always be [available here](#), along with other related software. PHP Weathermap is licensed under the GNU Public License, version 2. See COPYING for details. This distribution also includes the Overlib library by Enik Bostrup.



PHP Weathermap Editor

172.31.0.200/cacti/plugins/weathermap/editor.php?mapname=lacnog15.conf&plug=

Change File Add Node Add Link Position Legend Position Timestamp Map Properties Map Style Manage Colors Manage Images Editor Settings Position ...

Created: Sep 27 2015 18:34:21

or click a Node or Link to edit it's properties

Traffic Load

0-1%
1-10%
10-25%
25-40%
40-55%
55-70%
70-85%
85-100%

mapfile action param param2 debug

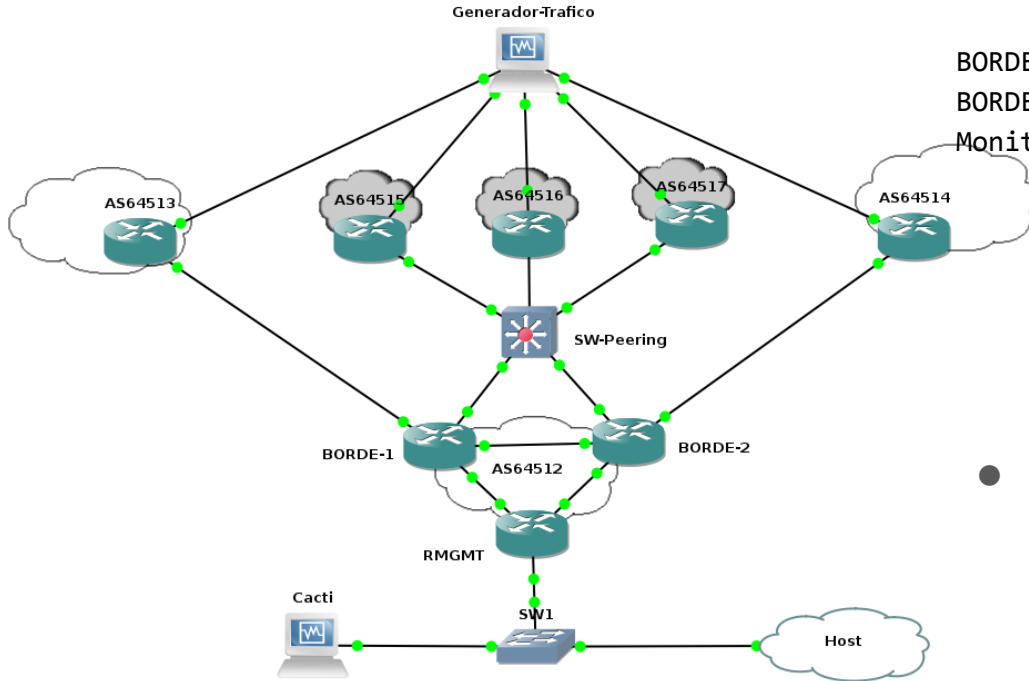
The screenshot shows a network diagram with nodes labeled RS64513, RS64515, RS64516, RS64517, RS64514, BORDE-1, BORDE-2, MGMT, Gestor, and Switch. The diagram is a tree structure with BORDE-1 and BORDE-2 as central nodes. A legend on the right indicates traffic load percentages with corresponding colors. The bottom of the page has a yellow bar with labels: mapfile, action, param, param2, debug.

Configuración SNMP

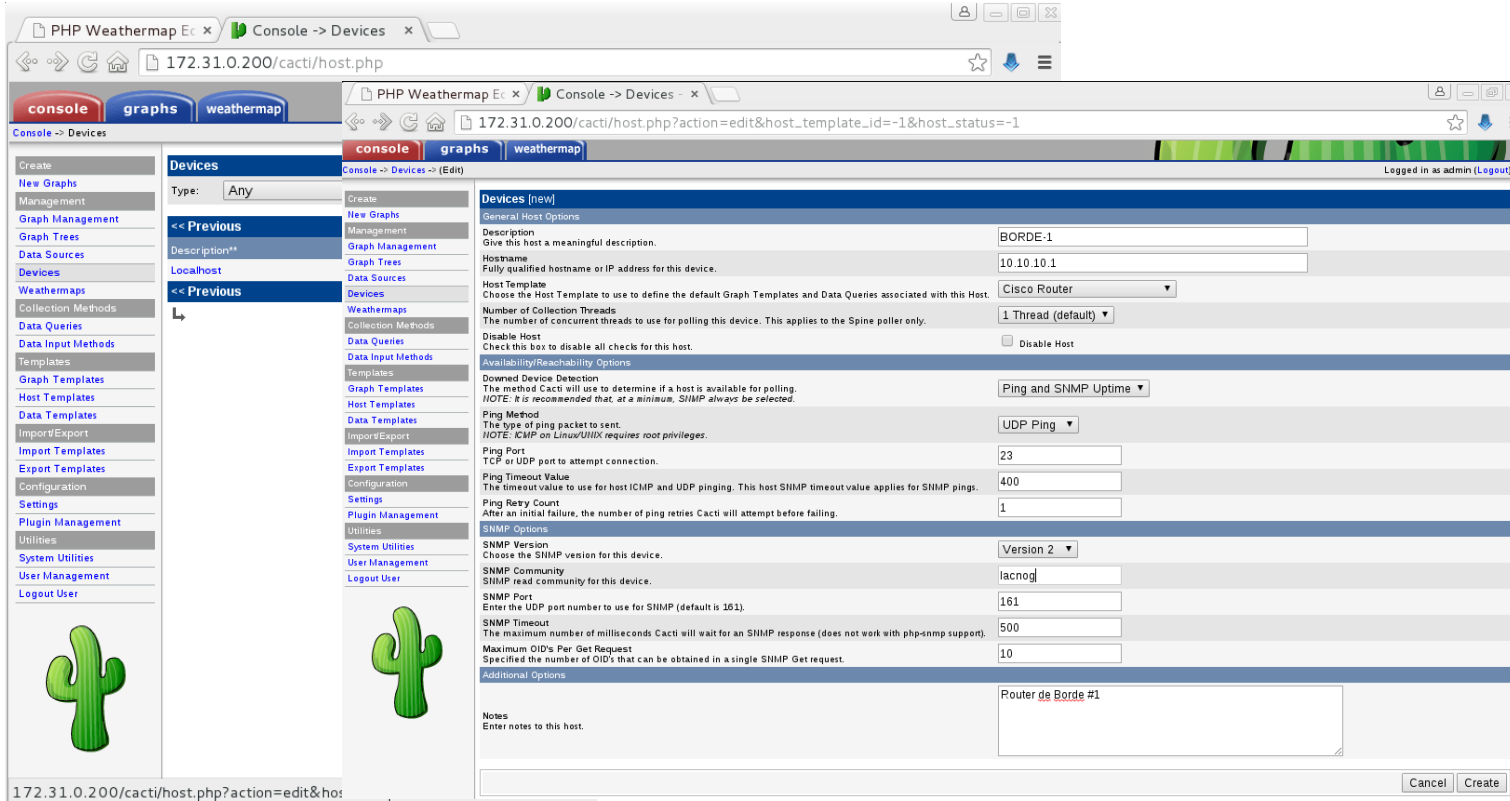
- Configuramos BORDE-1

```
BORDE-1(config)#snmp-server community lacnog R0  
BORDE-1(config)#snmp-server location "Taller  
Monitoreo Lacnog15"
```

- Otras opciones (datos contacto, vistas, trap-managers, etc)



Cacti: Management>Devices>Add



The screenshot displays the Cacti web interface for adding a new device. The browser address bar shows the URL `172.31.0.200/cacti/host.php`. The page title is `Console -> Devices`. The interface includes a navigation menu on the left with categories like Management, Templates, Configuration, and Utilities. The main content area is titled `Devices [new]` and contains the following fields:

- Description:** BORDE-1
- Hostname:** 10.10.10.1
- Host Template:** Cisco Router
- Number of Collection Threads:** 1 Thread (default)
- Disable Host:** Disable Host
- Availability/Reachability Options:**
 - Downed Device Detection:** Ping and SNMP Uptime
 - Ping Method:** UDP Ping
 - Ping Port:** 23
 - Ping Timeout Value:** 400
 - Ping Retry Count:** 1
- SNMP Options:**
 - SNMP Version:** Version 2
 - SNMP Community:** lacnogl
 - SNMP Port:** 161
 - SNMP Timeout:** 500
 - Maximum OID's Per Get Request:** 10
- Additional Options:** Router de Borde #1
- Notes:** Router de Borde #1

At the bottom right, there are `Cancel` and `Create` buttons. The page footer shows the URL `172.31.0.200/cacti/host.php?action=edit&ho`.

Cacti: generar gráficos (Create Graphs for this Host)

Save Successful.

BORDE-1 (10.10.10.1)

SNMP Information
System: Cisco IOS Software, 7200 Software (C7200-ADVSRVICESK9-M), Version 15.2(4)M3
/cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 24-Mar-11 15:26 by prod_re_team
Uptime: 204745 (0 days, 0 hours, 34 minutes)
Hostname: BORDE-1
Location: TA'LER Monitoro Lacrogis
Contact:

Ping Results
UDP Ping Success (30 ms)

Devices [edit BORDE-1]

General Host Options

Description: Give this host a meaningful description.

Hostname: Fully qualified hostname or IP address for this device.

Host Template: Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

Number of Collection Threads:

- *Create Graphs for this Host
- *Data Source List
- *Graph List

- Seleccionamos los recursos a graficar y creamos los gráficos.

weathermap

- Created graph: BORDE-1 - CPU Usage
- Created graph: BORDE-1 - Traffic - Gi0/0
- Created graph: BORDE-1 - Traffic - Gi1/0
- Created graph: BORDE-1 - Traffic - Gi2/0
- Created graph: BORDE-1 - Traffic - Gi3/0

PHP Weathermap Ec x Console -> Create N x

172.31.0.200/cacti/graphs_new.php?graph_type=-2&host_id=2&filter=

console graphs weathermap

Console -> Create New Graphs

Logged in as admin (Logout)

BORDE-1 (10.10.10.1) Cisco Router

Host: Graph Types:

Graph Templates

Graph Template Name:


Create: Cisco - CPU Usage

Create:

Data Query [SNMP - Interface Statistics]

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address	
1	Down	Ethernet0/0	E0/0		6	1000000000	100	CA:01:13:48:00:06		<input type="checkbox"/>
2	Up	GigabitEthernet0/0	Gi0/0		6	10000000000	1000	CA:01:13:48:00:08	192.168.0.1	<input checked="" type="checkbox"/>
3	Up	GigabitEthernet1/0	Gi1/0		6	10000000000	1000	CA:01:13:48:00:1C	10.0.0.1	<input checked="" type="checkbox"/>
4	Up	GigabitEthernet2/0	Gi2/0		6	10000000000	1000	CA:01:13:48:00:38	192.10.2.1	<input checked="" type="checkbox"/>
5	Up	GigabitEthernet3/0	Gi3/0		6	10000000000	1000	CA:01:13:48:00:54	192.10.2.9	<input checked="" type="checkbox"/>
6	Down	GigabitEthernet4/0	Gi4/0		6	10000000000	1000	CA:01:13:48:00:70		<input type="checkbox"/>
7	Down	GigabitEthernet5/0	Gi5/0		6	10000000000	1000	CA:01:13:48:00:8C		<input type="checkbox"/>
8	Down	GigabitEthernet6/0	Gi6/0		6	10000000000	1000	CA:01:13:48:00:A8		<input type="checkbox"/>
9	Up	VoiP-Null0	Vo0		1	4294967295	10000			<input type="checkbox"/>
10	Up	Null0	Hu0		1	4294967295	10000			<input type="checkbox"/>
11	Up	Loopback0	Lo0		24	4294967295	8000		10.10.10.1	<input type="checkbox"/>

Select a graph type:



Cacti: visualización de gráficos.

- Debo agregar luego el host al “Default Tree” o crear un grupo nuevo (ej. “Routers”): Management > Graph Trees > Add.
- Luego se agrega el equipo al tree: Add > ”Tree Item Type=Host”, “Host=BORDE-1” > Create.
- En la pestaña “graphs” selecciono “Routers” y visualizo los gráficos.

Iperf para generar tráfico.

- Primero en el Colector (Cacti) ejecuto el iperf como “server” para escuchar en IPv4 y en IPv6 en diferentes puertos UDP.

```
root@Cacti:~/iperf -s -u -p 12345 &  
root@Cacti:~/iperf -V -s -u -p 12345 &  
root@Cacti:~/iperf -s -u -p 23451 &  
root@Cacti:~/iperf -V -s -u -p 23451 &
```

- En el Generador ejecuto el iperf como cliente enviando flujos UDP (controlando el throughput) hacia el server usando v4 y v6 hacia los puertos previamente configurados desde diferentes IPs de origen.

```
root@Cacti:~/iperf -B 198.51.100.254 -c 172.31.0.200 -u -p 12345 -t 3600 -b 2M&  
root@Cacti:~/iperf -V -B 2001:db8:2000::fe -c 2001:db8:1000::200 -u -p 12345 -t 3600 -b 1M&  
root@Cacti:~/iperf -B 172.16.0.254 -c 172.31.0.200 -u -p 23451 -t 3600 -b 3M&  
root@Cacti:~/iperf -V -B 2001:db8:4000::fe -c 2001:db8:1000::200 -u -p 23451 -t 3600 -b 1M&
```


WeatherMap: asociar source a links.

- Luego de haber agregado el dispositivo al Cacti puedo asociar las fuentes de tráfico para visualizarlas en el mapa (ej. Links).
- Volviendo al editor selecciono el link y en “Data Source” selecciono “Pick from Cacti”
- Selecciono la interfaz de interés y se completan los datos, incluyendo el URL y el “Hover” Graph URL que me permitirán visualizar el gráfico de cacti al hacer “click” en el link y cuando me posiciono sobre él.
- Puedo además agregar comentarios para el link y agregar/modificar otras opciones no disponibles en el editor haciendo “Edit” y trabajando directamente sobre el texto del archivo.

WeatherMap: visualización en Cacti.

- Previo a visualizarlo en la pestaña “weathermap” debo agregarlo en Cacti.
- Management>Weathermaps>Add, selecciono el archivo de configuración y lo agrego.
- En el siguiente período de polling lo podré visualizar.

Separando tráfico en peering

- Todo el tráfico proviene de la misma interfaz.
- No tengo una separación lógica (ej. VLANs) para poder monitorizar via SNMP.
- Habilito Netflow para identificar el tráfico de cada AS Peer (o AS origen) en los routers de borde.
- Debo capturar las trazas (nfcapd), procesarlas y almacenar los octetos que provienen de cada AS de interes.
- Luego puedo utilizar CACTI + Weathermaps para su visualización.

Instalación de nfcapd

- En distribuciones basadas en Debian

```
1 apt-get install gcc flex librrd-dev make
2 cd /usr/local/src/
3 wget http://sourceforge.net/projects/nfdump/files/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
4 gzip -dc nfdump-1.6.13.tar.gz | tar -xf -
5 cd nfdump-1.6.13
6 ./configure --enable-nfprofile
7 make && make install
```

Configuración router BORDE-1

- Configuro netflow en router de borde:

```
BORDE-1(config)#ip flow-export source Loopback0
```

```
BORDE-1(config)#ip flow-export version 9 peer-as (origin-as)
```

```
BORDE-1(config)#ip flow-export destination 172.31.0.200 16001
```

```
BORDE-1(config)#interface GigabitEthernet1/0
```

```
BORDE-1(config-if)#ip flow ingress
```

```
BORDE-1(config-if)#ip flow egress
```

Configuración del Colector netflow

- Lanzo la captura

```
root@Cacti:~/nfcapd -w -D -l /var/cache/flows/borde-1 -p 16001
```

- Verifico agregando por sistema autónomo de origen:

```
root@Cacti:/var/cache/flows/borde-1# nfdump -A srcas -r ./nfcapd.201509271855
```

Date first seen	Duration	Src AS	Packets	Bytes	bps	Bpp	Flows
2015-09-27 15:58:14.904	144.724	0	22	1070	59	48	16
2015-09-27 15:57:21.964	182.028	64513	15555	23.3 M1.0 M	1498	3	
2015-09-27 15:57:21.964	182.028	64515	15558	23.3 M1.0 M	1498	3	

Configuración CACTI

- Defino un nuevo **Data Input Method** que utiliza un script para obtener en dos variables “in” y “out” los octetos con origen y destino un número de sistema autónomo que se le pasa como entrada.
- Defino un nuevo **Data Template** que define la base de datos (RRD) y asocia el *Data Input Method* anterior. En esta RRD se almacenará cada 5 minutos los valores que devuelve el script.
- Defino un nuevo **Graph Template** para generar las gráficas a partir de la RRD. Teniendo en cuenta que deben pasarse los datos a bits y promediarse durante el período de medición (nueva CDEF).
- A partir de allí puedo instanciar las **Data Sources** y asociarles nuevos gráficos. Estos quedarán disponibles para ser usados en el Weathermap.

Otros posibles usos

- Estadísticas de tráfico IPv6 (en equipos cuyos agentes no soportan el objeto IP-MIB::ipIfStatsInOctets.ipv6).
- Tráfico hacia subredes que alojan CDNs.
- Tráfico desde/hacia distintos países o regiones con información de RIRs (ej. <ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-latest>)
- Segmentación de tráfico por servicio (usando BD propias de IPs).
- Tráfico por bloques publicados por enlace (balanceo de tráfico entrante).

PREGUNTAS