Servicios en Tecnología y Telecomunicaciones

El camino más corto distratel S.R.L.

Network Management & Monitoring

Monitoreo de redes Mikrotik con SNMP

Freddy Bohorquez Quevedo

Sobre TecTel Bolivia

- Orígenes en Redes Inalámbricas Comunitarias
- 2004. Conectividad Rural e ISP Comunitarios
- Primeras Instalaciones basadas en WRAP
- Despliegue de Redes PtP y PtMP
- 2005. Encuentro con Mikrotik RB y ROS
- 2009. Inicio de Tectel como empresa especializada en Tecnología y Telecomunicaciones
- 2010. Distribuidor oficial de Mikrotik
- 2014 se crea DISTRATEL, incorporando soluciones en control y automatización.

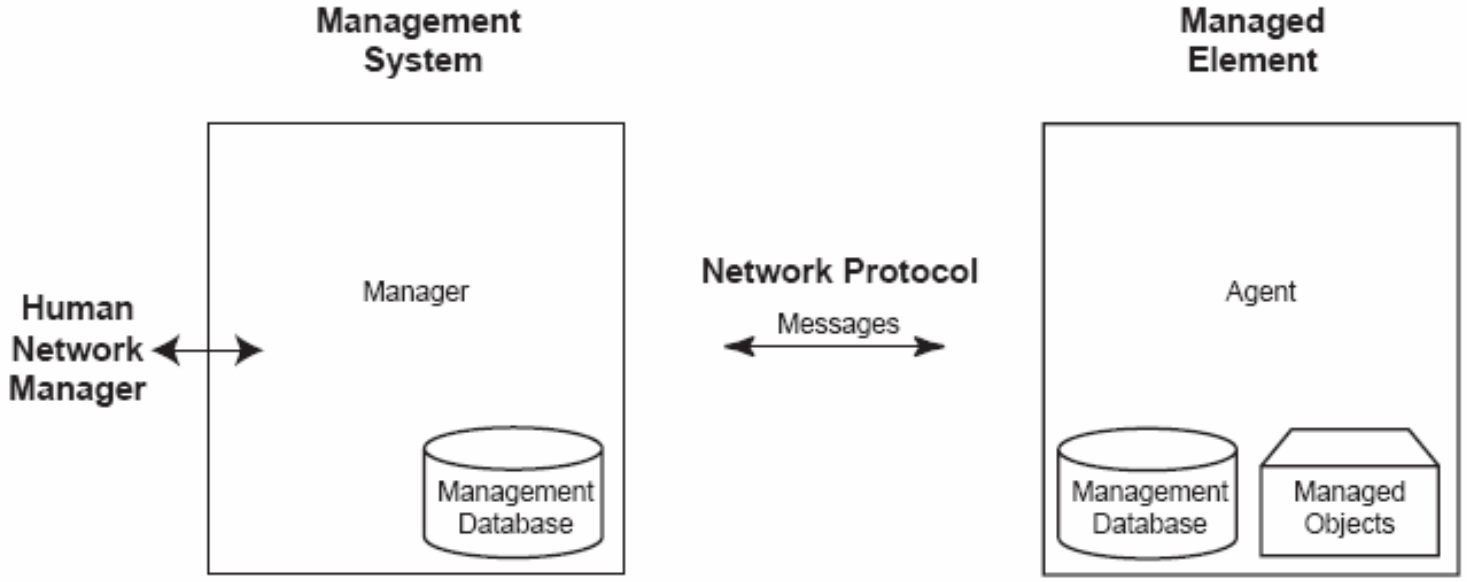
Contenido

- Qué es SNMP?
- Cómo funciona SNMP?
- OIDs y MIBs
- Polling, querying and Traps
- SNMP en Mikrotik
- Caso de Uso en Cacti

Qué es SNMP?

SNMP – Simple Network Management Protocol

- **Estándar abierto — existen cientos de herramientas para explotarla.**
- **Presente en cualquier equipo de red mínimamente decente.**



SNMP usa la arquitectura manager/agent.

Qué es SNMP?

Protocolo UDP, port 161, 162

Versiones:

- V1 (1988) – RFC1155, RFC1156, RFC1157
  - Especificaciones Iniciales originales
- v2 – RFC1901 ... RFC1908 + RFC2578
  - Mejoras a v1, tipos de datos nuevos, GETBULK
- v3 – RFC3411 ... RFC3418
  - seguridad y encriptación

Cómo funciona SNMP?

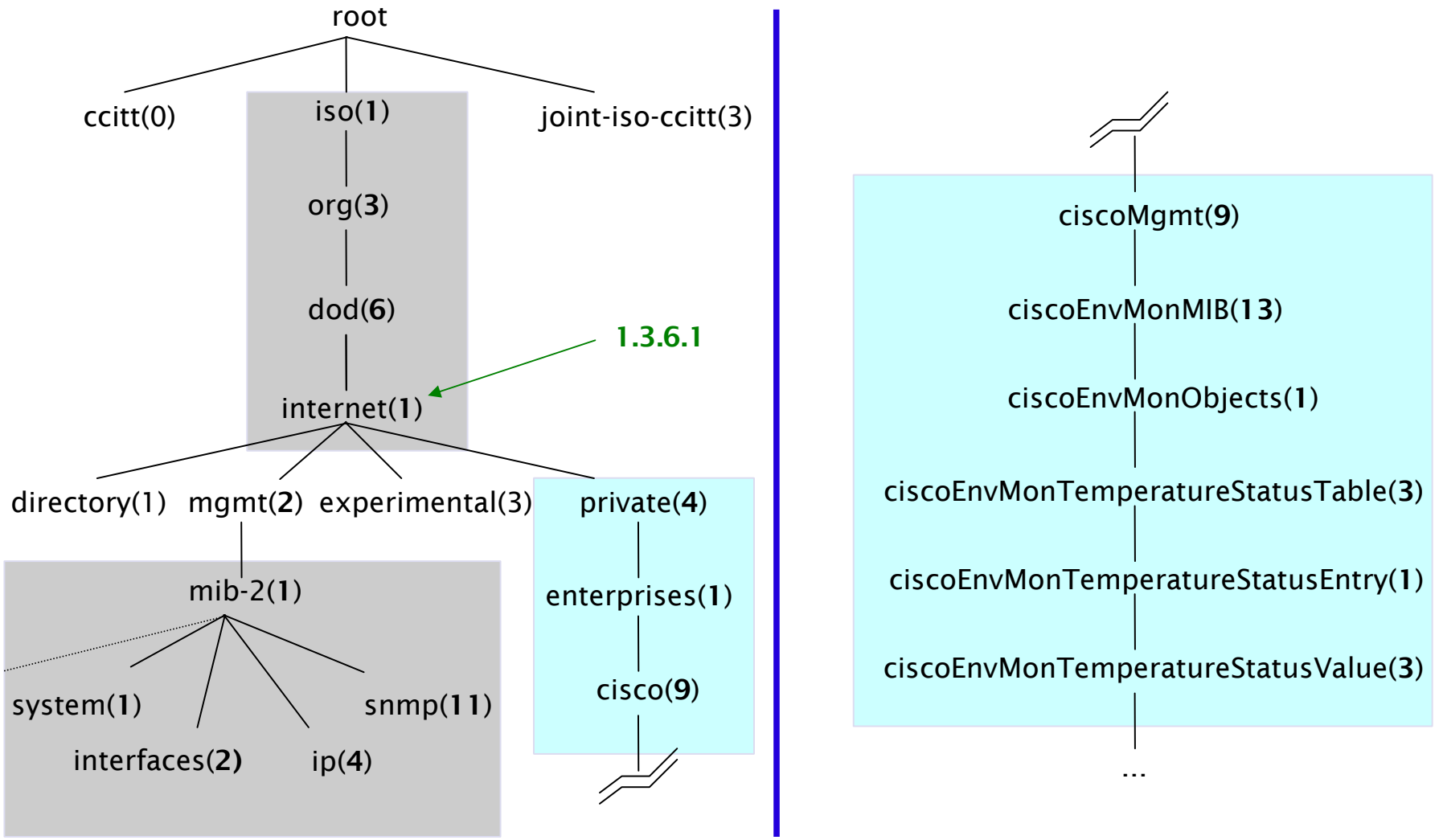
Comandos básicos o primitivas

- GET (manager -> agent)
- GET-NEXT (manager -> agent)
- GET-RESPONSE (agent -> manager)
- SET (manager -> agent)
- TRAP (agent -> manager)

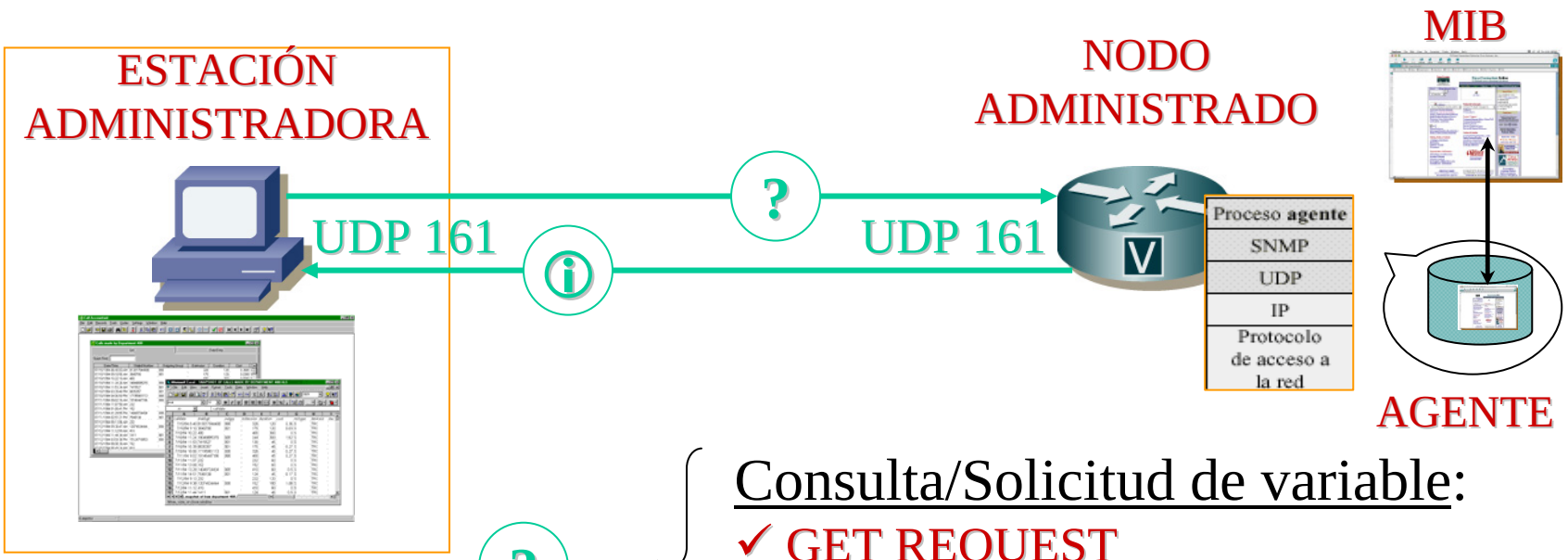
MIB: Base de Información de Administración

- MIB, colección de información que está organizada jerárquicamente, incluye:
  - Identificador del Objeto (OID)
  - Nombre del Objecto
  - Descripción del Objecto
  - Tipo de Dato (integer, text, list)
- MIB se describe usando ASN.1
- MIB estandar incluye:
  - MIB-II – (RFC1213) – a group of sub-MIBs
  - HOST-RESOURCES-MIB (RFC2790)

MIB Tree


root
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
system(1)
snmp(11)
cisco(9)
interfaces(2)
ip(4)
ciscoMgmt(9)
ciscoEnvMonMIB(13)
ciscoEnvMonObjects(1)
ciscoEnvMonTemperatureStatusTable(3)
ciscoEnvMonTemperatureStatusEntry(1)
ciscoEnvMonTemperatureStatusValue(3)
...

Obtención de Información



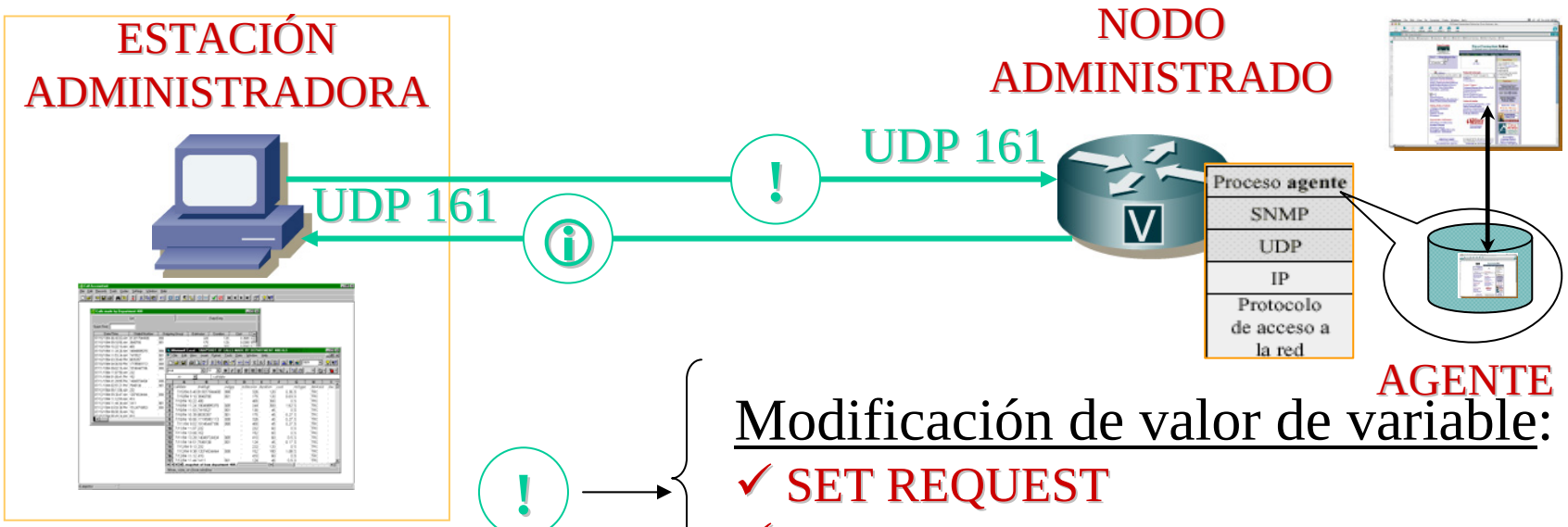
Consulta/Solicitud de variable:

- ✓ GET REQUEST
- ✓ GET NEXT REQUEST
- ✓ GET BULK (SNMP v.2)

Respuesta a solicitud:

- ✓ GET RESPONSE

Modificación de Información



Modificación de valor de variable:

- ✓ SET REQUEST
- ✓ SET NEXT REQUEST

Respuesta a solicitud:

- ✓ GET RESPONSE

EJEMPLO: Se puede usar para resetear el valor de los contadores, como el número de paquetes procesados.

Traps - Interrupciones

Un Agente informa de un evento:

✓ TRAP

EJEMPLO: El Agente de un router informa de que un enlace ha caído.

SNMP en Mikrotik

Management information base (MIB)

Puede descargarse de
http://mikrotik.com/download/Mikrotik.mib

Object identifiers (OID)

```
[admin@Mikrotik] > /system resource print oid
         uptime: .1.3.6.1.2.1.1.3.0
   total-memory: .1.3.6.1.2.1.25.2.3.1.5.65536
    used-memory: .1.3.6.1.2.1.25.2.3.1.6.65536
  cpu-frequency: .1.3.6.1.4.1.14988.1.1.3.14.0
     build-time: .1.3.6.1.4.1.14988.1.1.7.6.0
[admin@Mikrotik] >
```

SNMP en Mikrotik

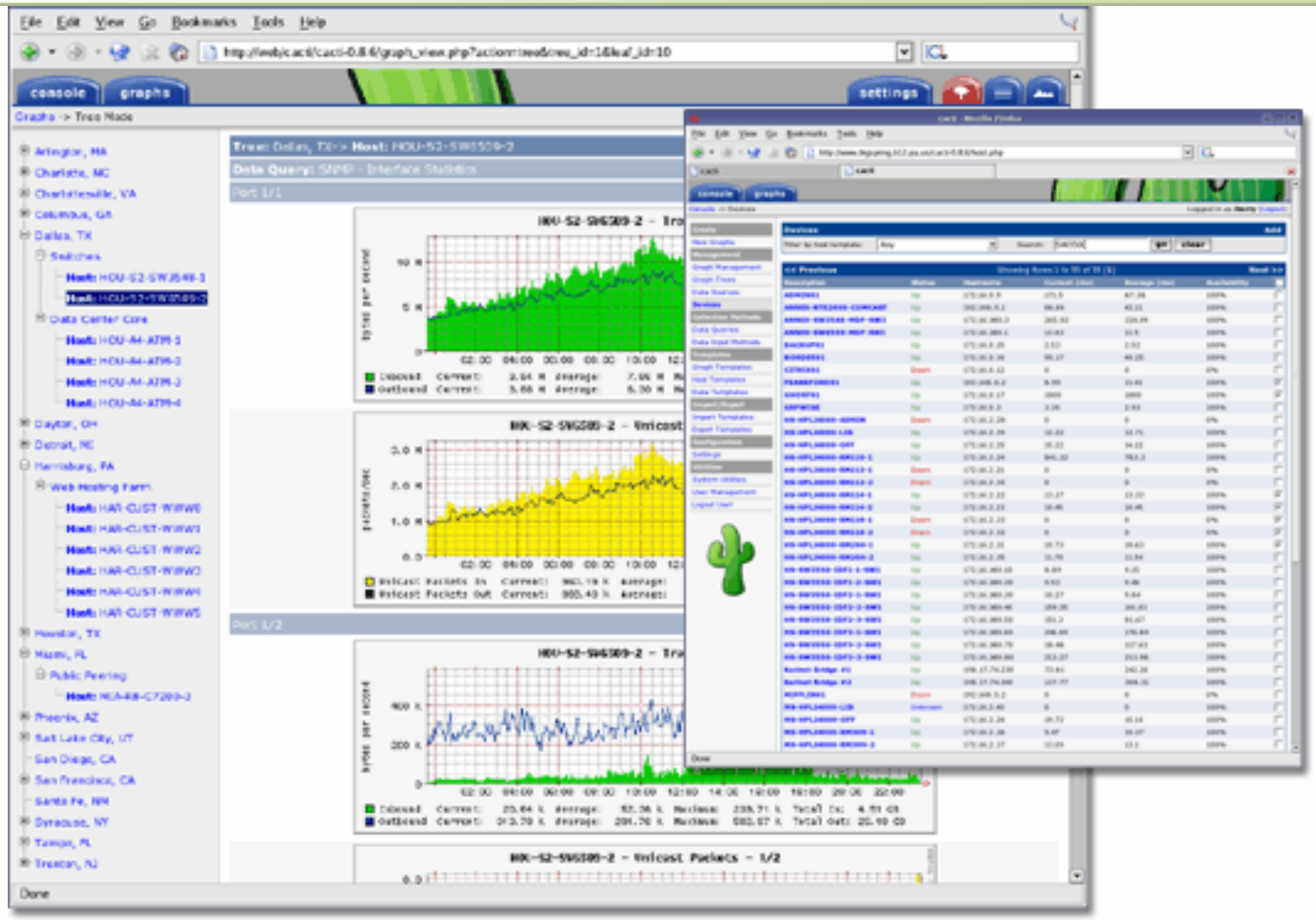
Object identifiers (OID)

```
root@debian:~# snmpwalk -v 1 -c freddybq -On 192.168.14.126 | more
.1.3.6.1.2.1.1.1.0 = STRING: "RouterOS RB751U-2HnD"
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.14988.1
.1.3.6.1.2.1.1.3.0 = Timeticks: (8310000) 23:05:00.00
.1.3.6.1.2.1.1.4.0 = STRING: "fbq"
.1.3.6.1.2.1.1.5.0 = STRING: "MikroTik"
.1.3.6.1.2.1.1.6.0 = STRING: "tectel"
.1.3.6.1.2.1.1.7.0 = INTEGER: 78
.1.3.6.1.2.1.2.1.0 = INTEGER: 8
```

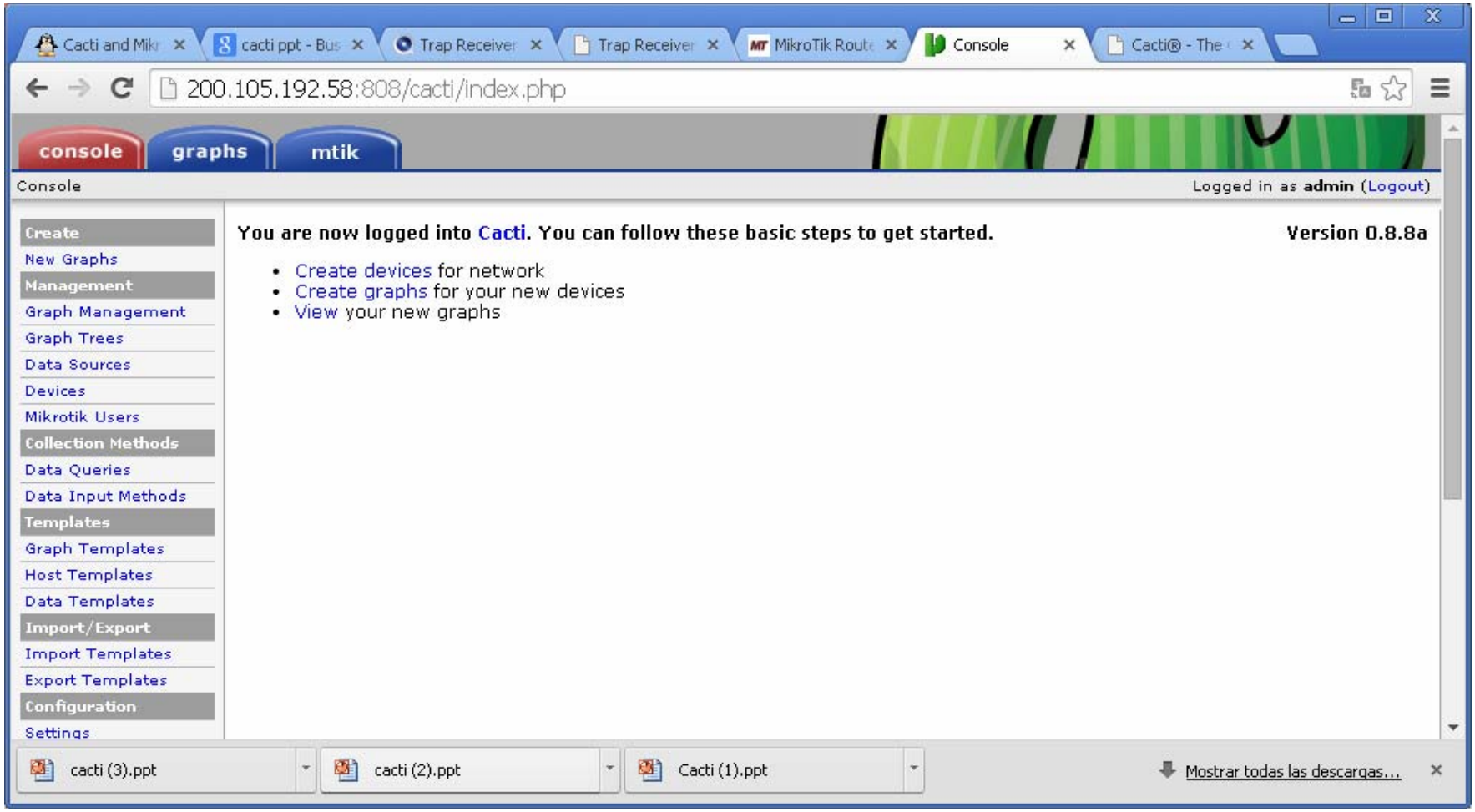
CACTI

- Herramienta para sensar (poolling), almacenar y presentar estadísticas de red y sistemas.
- Está diseñada en base a RRDTool, con especial énfasis en la interfaz gráfica
- Casi todas las funcionalidades pueden configurarse a través de interface web.

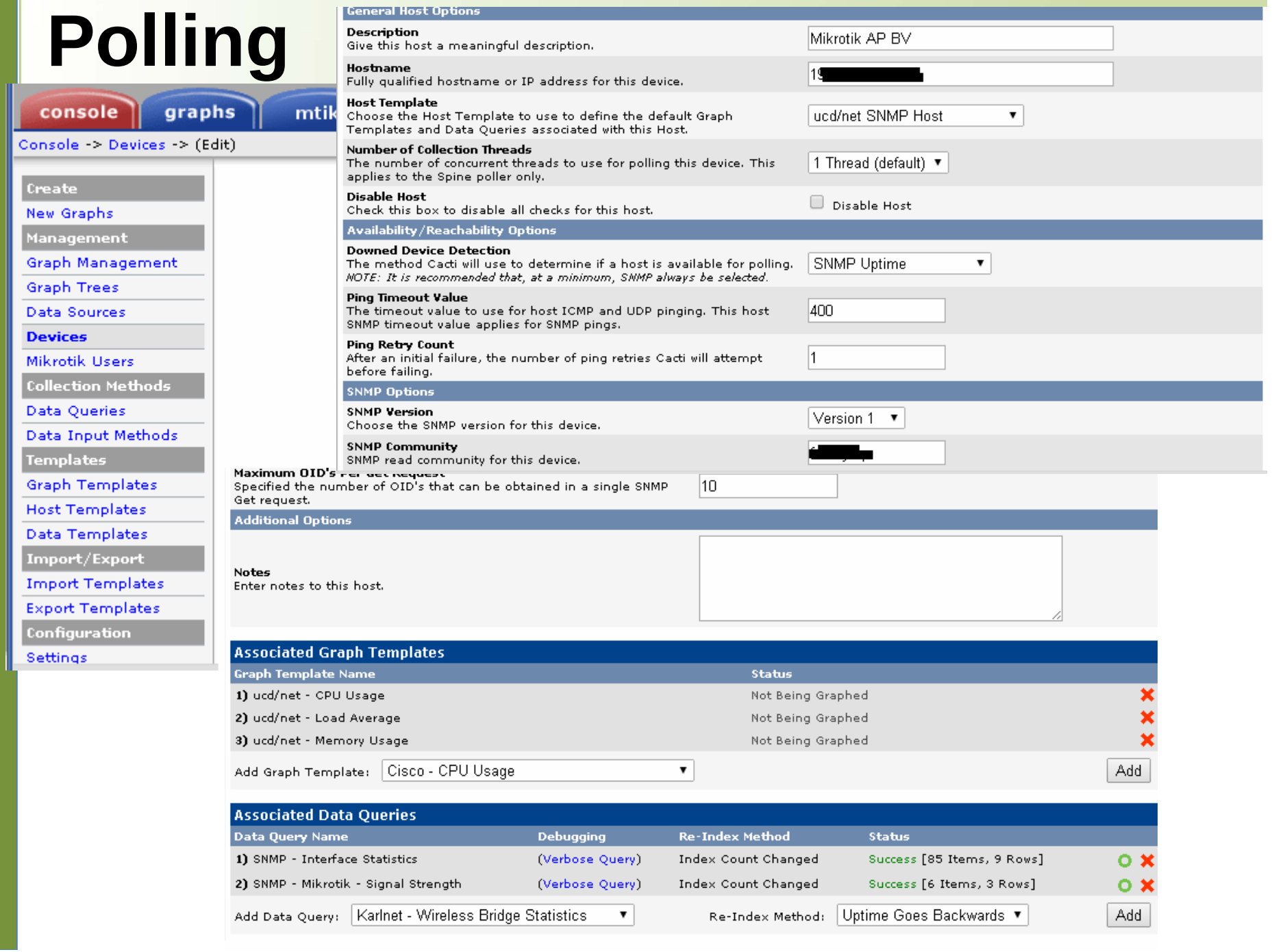
CACTI


File Edit View Go Bookmarks Tools Help
console
graphs
settings
Graphs -> Tree Mode
Done

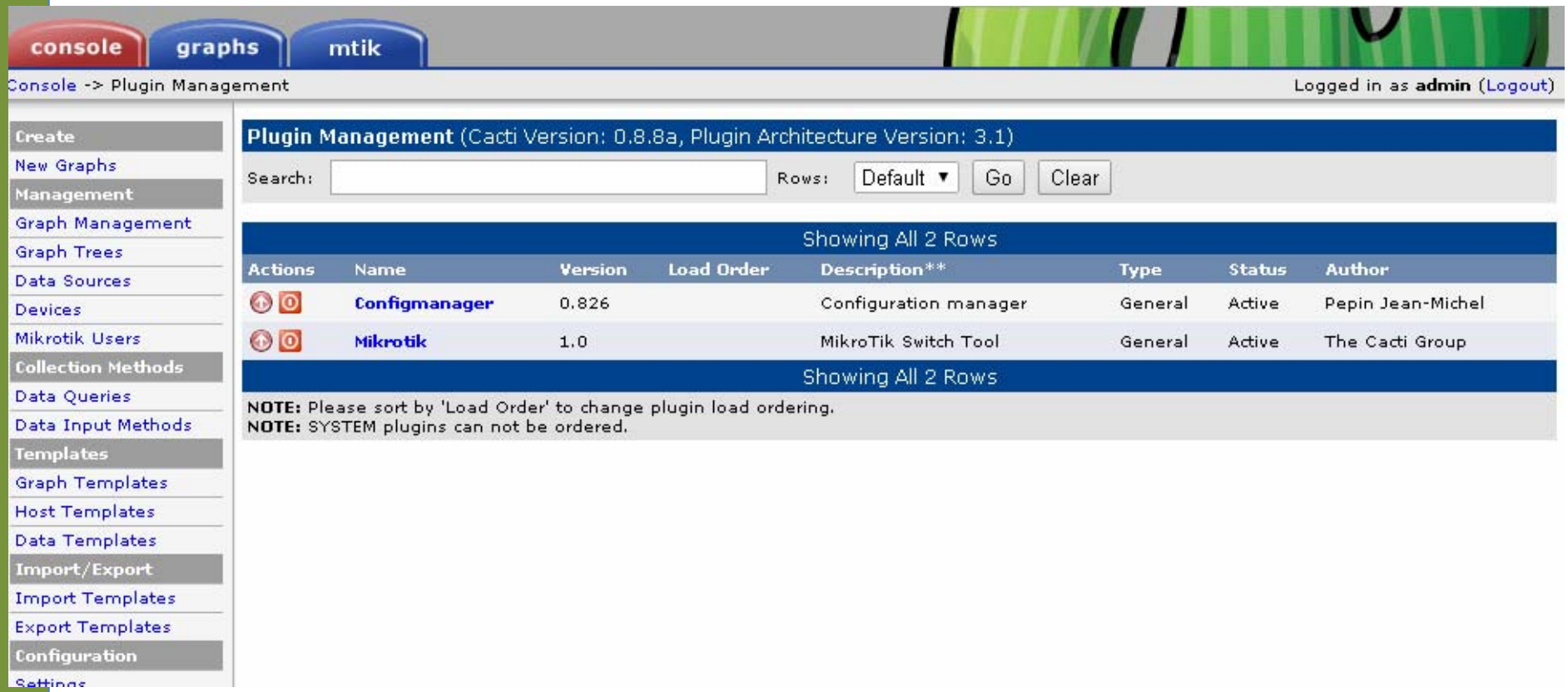
CACTI - Interface



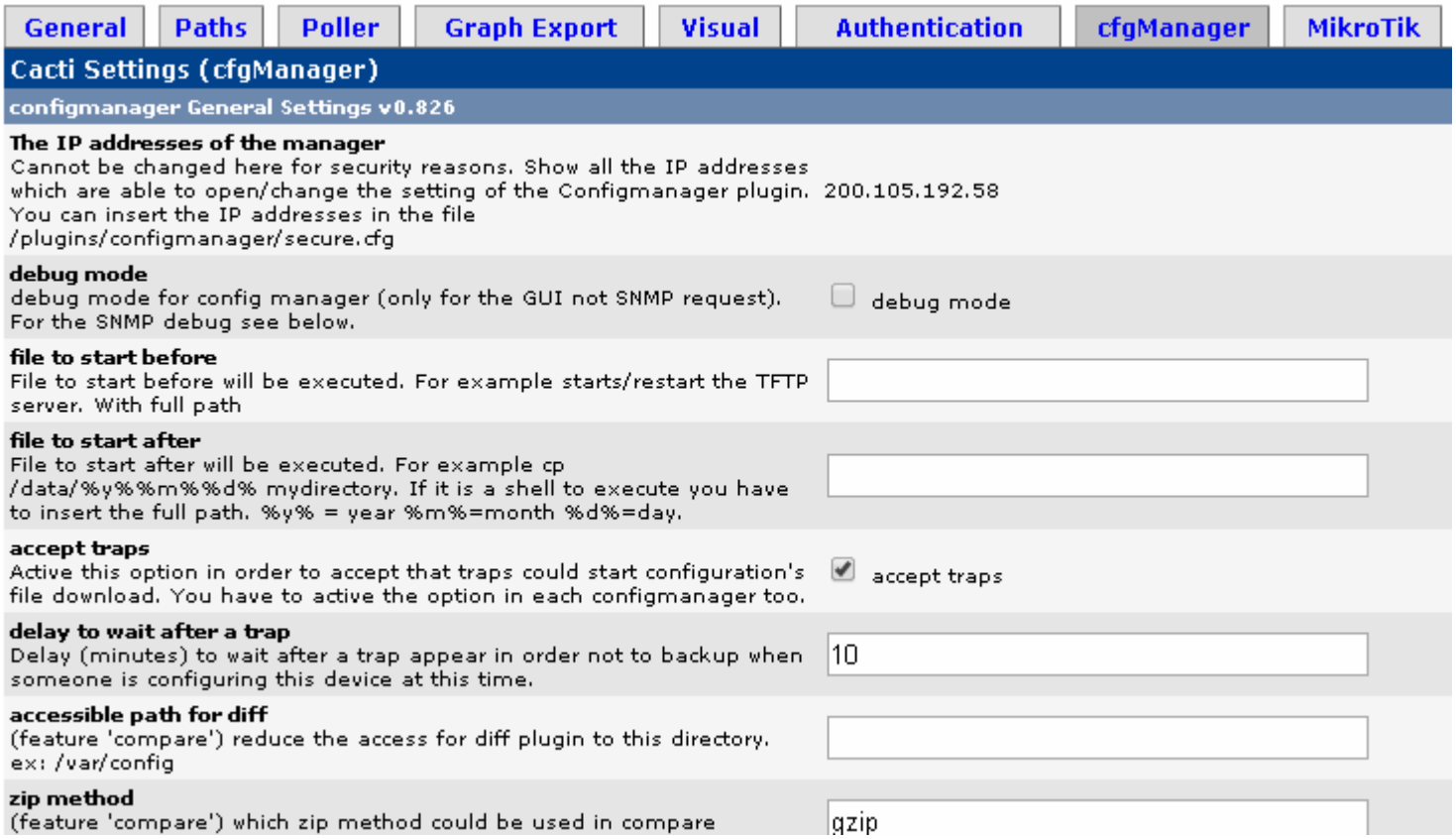
Polling


console
graphs
mtik
Console -> Devices -> (Edit)
Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Mikrotik Users
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Import/Export
Import Templates
Export Templates
Configuration
Settings
General Host Options
Description
Give this host a meaningful description.
Mikrotik AP BV
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.
ucd/net SNMP Host
Number of Collection Threads
The number of concurrent threads to use for polling this device. This applies to the Spine poller only.
1 Thread (default)
Disable Host
Check this box to disable all checks for this host.
Disable Host
Availability/Reachability Options
Downed Device Detection
The method Cacti will use to determine if a host is available for polling.
NOTE: It is recommended that, at a minimum, SNMP always be selected.
SNMP Uptime
Ping Timeout Value
The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.
400
Ping Retry Count
After an initial failure, the number of ping retries Cacti will attempt before failing.
1
SNMP Options
SNMP Version
Choose the SNMP version for this device.
Version 1
SNMP Community
SNMP read community for this device.
Maximum OID's
Specified the number of OID's that can be obtained in a single SNMP Get request.
10
Additional Options
Notes
Enter notes to this host.
Associated Graph Templates
Graph Template Name
Status
1) ucd/net - CPU Usage
Not Being Graphed
2) ucd/net - Load Average
Not Being Graphed
3) ucd/net - Memory Usage
Not Being Graphed
Add Graph Template:
Cisco - CPU Usage
Add
Associated Data Queries
Data Query Name
Debugging
Re-Index Method
Status
1) SNMP - Interface Statistics
(Verbose Query)
Index Count Changed
Success [85 Items, 9 Rows]
2) SNMP - Mikrotik - Signal Strength
(Verbose Query)
Index Count Changed
Success [6 Items, 3 Rows]
Add Data Query:
Karlnet - Wireless Bridge Statistics
Re-Index Method:
Uptime Goes Backwards
Add

CACTI - Plugins



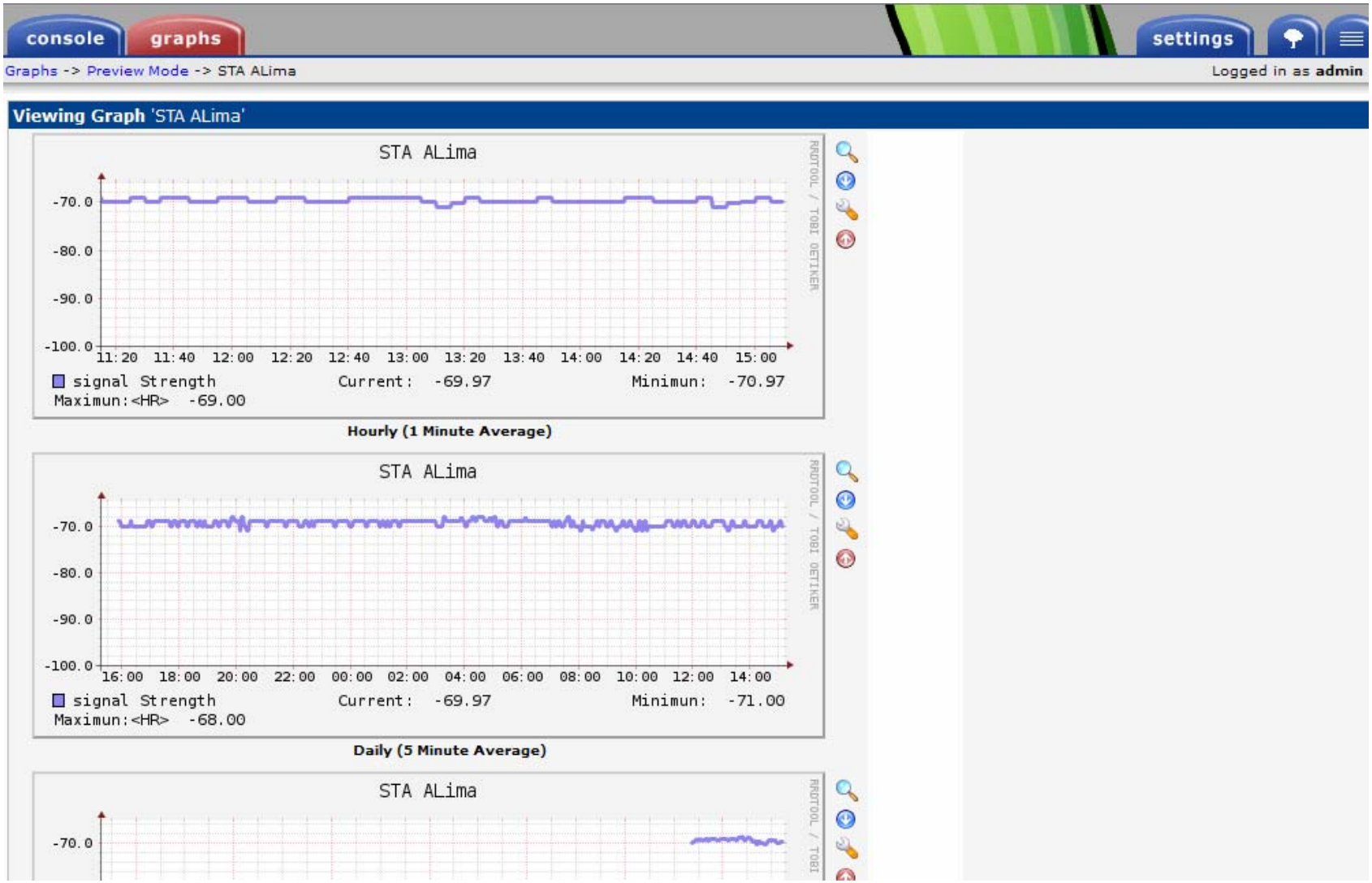
CACTI - Trap


General
Paths
Poller
Graph Export
Visual
Authentication
cfgManager
MikroTik
Cacti Settings (cfgManager)
configmanager General Settings v0.826
The IP addresses of the manager
Cannot be changed here for security reasons. Show all the IP addresses which are able to open/change the setting of the Configmanager plugin. You can insert the IP addresses in the file /plugins/configmanager/secure.cfg
200.105.192.58
debug mode
debug mode for config manager (only for the GUI not SNMP request). For the SNMP debug see below.
debug mode
file to start before
File to start before will be executed. For example starts/restart the TFTP server. With full path
file to start after
File to start after will be executed. For example cp /data/%y%%m%%d% mydirectory. If it is a shell to execute you have to insert the full path. %y% = year %m%=month %d%=day.
accept traps
Active this option in order to accept that traps could start configuration's file download. You have to active the option in each configmanager too.
accept traps
delay to wait after a trap
Delay (minutes) to wait after a trap appear in order not to backup when someone is configuring this device at this time.
10
accessible path for diff
(feature 'compare') reduce the access for diff plugin to this directory. ex: /var/config
zip method
(feature 'compare') which zip method could be used in compare
gzip

CACTI - snmp-query

```
<interface>
  <name>Mikrotik - Get signal strength</name>
    <description>Get signal strength</description>
      <index_order>signalStrengthIndex</index_order>
      <index_order_type>alphabetic</index_order_type>
      <oid_index>.1.3.6.1.4.1.14988.1.1.1.2.1.1</oid_index>
      <oid_index_parse>OID/REGEXP:^.{30}(.*)</oid_index_parse>
      <fields>
        <signalStrengthIndex>
          <name>Index</name>
          <source>index</source>
          <direction>input</direction>
        </signalStrengthIndex>
        <signalStrengthDevice>
          <name>Device</name>
          <method>get</method>
          <source>value</source>
          <direction>input</direction>
          <oid>.1.3.6.1.4.1.14988.1.1.1.2.1.1</oid>
        </signalStrengthDevice>
        <signalStrengthValue>
          <name>Value</name>
          <method>get</method>
          <source>value</source>
          <direction>output</direction>
          <oid>.1.3.6.1.4.1.14988.1.1.1.2.1.3</oid>
        </signalStrengthValue>
      </fields>
</interface>
```

CACTI - Mikrotik Nivel de señal



Referencias

- *Essential SNMP* (O'Reilly Books) Douglas Mauro, Kevin Schmi
- Wikipedia: http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
- SNMP: http://informatica.uv.es/iiguia/R/apuntes/snmp.ppt. Rogelio Montañana, Universidad de Valencia, Departamento de Informática
- SNMP Link – collection of SNMP resources http://www.snmplink.org/
- Net-SNMP Open Source SNMP tools http://net-snmp.sourceforge.net/
- Cacti and Mikrotik - How to graph signal strength without hassle: Cacti and Mikrotik - How to graph signal strength without hassle
- Manual SNMP Mikrotik: http://wiki.mikrotik.com/wiki/Manual:SNMP
- Integration with Nagios http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html