Red de Gestión de Transmisores FM

Estudiante: Franco Joel Basalo Lagrange
Ingeniería Técnica en Telecomunicaciones, especialidad Telemática

Consultor: Antoni Morell Pérez
Fecha:12 de junio 2016

TRABAJO FINAL

Título del trabajo:	*Red de Gestión de Transmisores FM*
Nombre del autor:	*Franco Joel Basalo Lagrange*
Nombre del consultor:	Antoni Morell Pérez
Fecha del libramiento:	*06/2016*
Área del Trabajo Final:	*Integración redes telemáticas*
Titulación:	*Ingeniería Técnica de Telecomunicaciones, especialidad Telemática*

Resumen del Trabajo:

En este proyecto se implementa el diseño de una Red de Gestión de transmisores FM, de la marca Link serie Advancast 6K y 8K, basado en el protocolo SNMP.

Se realiza una introducción en donde se contextualiza y justifica la necesidad de llevar a cabo el proyecto (con la presentación de la topología de la red de gestión). Posteriormente, se realiza una descripción general de los conceptos y en el segundo ítem se marcan los objetivos a conseguir.

A partir del tercer punto, se inicia la explicación más exhaustiva del proyecto, haciendo referencia a la Arquitectura de la red a diseñar. Se realiza una descripción de las infraestructuras de telecomunicaciones y se nombran sus características principales. También se incluye un mapa que muestra la situación geográfica de los emplazamientos en donde se encuentran instalados los transmisores de FM.

Posteriormente, se dimensiona la solución de conectividad, con la utilización de la red celular de Colombia y se designa el hardware que dará salida a Internet en los emplazamientos. Se aborda también el estudio de infraestructuras de telecomunicaciones que existen en Colombia y se justifica la elección de la red celular como medio de transporte de la red. A continuación, se diseña la red IP y se presenta la tabla de direccionamiento.

Para finalizar este capítulo, se expone la conexión VPN (Virtual Private Network) y se presentan conceptos generales. Acto seguido, se comenta la herramienta OpenVPN y se muestra su configuración.

En el cuarto punto, se introducen conceptos del sistema de supervisión que se lleva a cabo con Zabbix. Posteriormente, se muestra la configuración de la interfaz web de Zabbix y se muestran los resultados obtenidos.

Para finalizar, se presenta el estudio económico del proyecto.

Abstract (in English, 250 words or less):

In this project the design of a Network Management FM transmitters, brand Advancast Link 6K and 8K series, based on the SNMP protocol is implemented.

An introduction where it is contextualized and justifies the need to carry out the project (with the presentation of the network topology management) is performed. Subsequently, an overview of the concepts is done, so that in the second item are marked objectives to be achieved.

From the third point, the most comprehensive explanation of the project begins, referring to the network architecture design. a description of the telecommunications infrastructure is performed and its main features are named. a map showing the location of the sites where they are installed FM transmitters also included.

Subsequently, the connectivity solution is dimensioned, with the use of the cellular network in Colombia and hardware that will output internet sites designated. the study of telecommunications infrastructures that exist in Colombia and the election of the cellular network is justified as a means of transport network it is also addressed. Then, the IP network is designed and the routing table is presented.

To end this chapter, the VPN (Virtual Private Network) connection is exposed and general concepts are presented. Then, the OpenVPN tool is discussed and its configuration.

In the fourth point, monitoring system concepts that are carried out with Zabbix are introduced. Subsequently, the configuration of Zabbix web interface shown and the results obtained are shown.

Economic study of the project is presented to end.

Palabras clave (entre 4 i 8):

SNMP, Zabbix, OpenVPN, Conectividad

Índice

Índice de Figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El Grupo Adtel, con sede central en Molins de Rei, provincia de Barcelona, es una empresa consolidada con más de 20 años de experiencia en el sector de las telecomunicaciones.

Link Comunicaciones es una empresa integrada en el grupo Adtel que se dedica al diseño, fabricación, distribución y mantenimiento de equipos de radiodifusión para profesionales.

En el último año, el Grupo Adtel ha realizado la venta de Transmisores FM del fabricante LINK a un radiodifusor colombiano. Los Transmisores FM Estéreo de la serie Advancast R-6K y Advancast R8-K se encuentran instalados por diferentes puntos de la geografía de Colombia y darán cobertura FM a las principales poblaciones del país.

Los emplazamientos, ubicados por lo general en el medio rural, no cuentan con presencia de personal técnico que pueda detectar in situ si se produce una incidencia que pueda generar una disfunción en el servicio.

Como consecuencia de la falta de personal presente en los sites, en caso de avería de un transmisor, la salida a antena de los diferentes programas de radio podría verse afectada durante un plazo de tiempo indeterminado.

Con el propósito de reducir el tiempo de afectación del servicio que puedan provocar las posibles incidencias, se ha propuesto al cliente implementar una red de monitorización de los Transmisores FM en tiempo real.

Con este sistema de gestión se tendría notificaciones vía correo electrónico y en caso de fallo de un transmisor, el personal técnico seria notificado, consiguiendo de esta manera disminuir el tiempo de respuesta en la actuación del correctivo. De esta manera, se busca ofrecer un mejor servicio de mantenimiento de las instalaciones.

El desarrollo de este sistema de monitorización se podría ofrecer, en un futuro, para otros servicios de este mismo cliente u otros nuevos que estén interesados en este tipo de gestión.

1.2 Descripción del proyecto

En el mundo de las telecomunicaciones, es cada vez más habitual utilizar redes de gestión, ya que aporta beneficios y mejora el rendimiento de una red de dispositivos. La monitorización eficaz de una red se basa en saber que datos son los que se deben recolectar, clasificarlos y gestionar esa información generando avisos de diferente nivel de importancia.

La red de gestión a implementar estará basada en el protocolo SNMP (Simple Network Management Protocol), que es ampliamente usado para la gestión y seguimiento de elementos dentro de una red. Actualmente, la gran mayoría de dispositivos disponen de un agente SNMP, configurado de tal forma que se pueda comunicar con el sistema de gestión de red (NMS; Network Management System).

Un NMS se encarga de la monitorización de la red mediante la toma de datos y, en caso de anomalía en el sistema, generará alarmas que serán enviadas por correo electrónico a los responsables de la gestión. El software elegido para cumplir la función de NMS será Zabbix

Zabbix es un software de código abierto (Open Source) que ofrece buenas prestaciones, como por ejemplo la posibilidad de personalizar la interfaz web. No requiere de un gran hardware en el servidor, trabaja sobre Linux (por lo que es bastante estable) y no necesita de licencias para su manejo.

La arquitectura de la red estará compuesta por el servidor NMS, instalado en Barcelona, y los Transmisores FM (Frecuencia Modulada), ubicados en Colombia. Estos Transmisores disponen de una lógica de control con un agente SNMP instalado. A través de este agente, el transmisor informará de los valores de potencia RF (Radio Frecuencia) de salida directa, potencia reflejada, temperatura, etc., que serán los datos a monitorizar.

La conexión entre los dos extremos requiere que se utilicen Proveedores de servicios de Internet (ISP), por lo tanto, los datos viajaran por la red pública. La solución de conectividad escogida ha sido la red celular 2G/3G de Colombia, de manera que se alquilará la red al operador local de telecomunicaciones “Claro”. En cuanto al extremo de Barcelona, ya se dispone de una conexión de Fibra Óptica para dar salida a Internet al servidor.

El Router 3G de la marca Teltonika, modelo RUT500, ha sido el elegido para dar conectividad a los Transmisores FM instalados en los emplazamientos. El router consta de 3 puertos LAN, un puerto WAN y conexión inalámbrica WiFi, que se deberá habilitar para posibilitar la conexión de un técnico con su ordenador portátil.

Se deberá realizar el diseño de la red IP acorde a las necesidades de los emplazamientos, teniendo en cuenta la posibilidad de crecimiento de equipos a monitorizar.

Las conexiones extremo a extremo por Internet se realizarán por túneles VPN (Virtual Private Network), que es una tecnología que permite compartir datos de manera segura utilizando una red pública como Internet. Se instalará un servidor OpenVPN también en Barcelona.

OpenVPN es también un software de código abierto (Open Source) muy extendido que ofrece una conectividad puno a punto y que utiliza el protocolo de seguridad por medio de encriptación de datos SSL (Secure Sockets Layer), lo que garantiza la seguridad en las conexiones.

Red de Gestión.

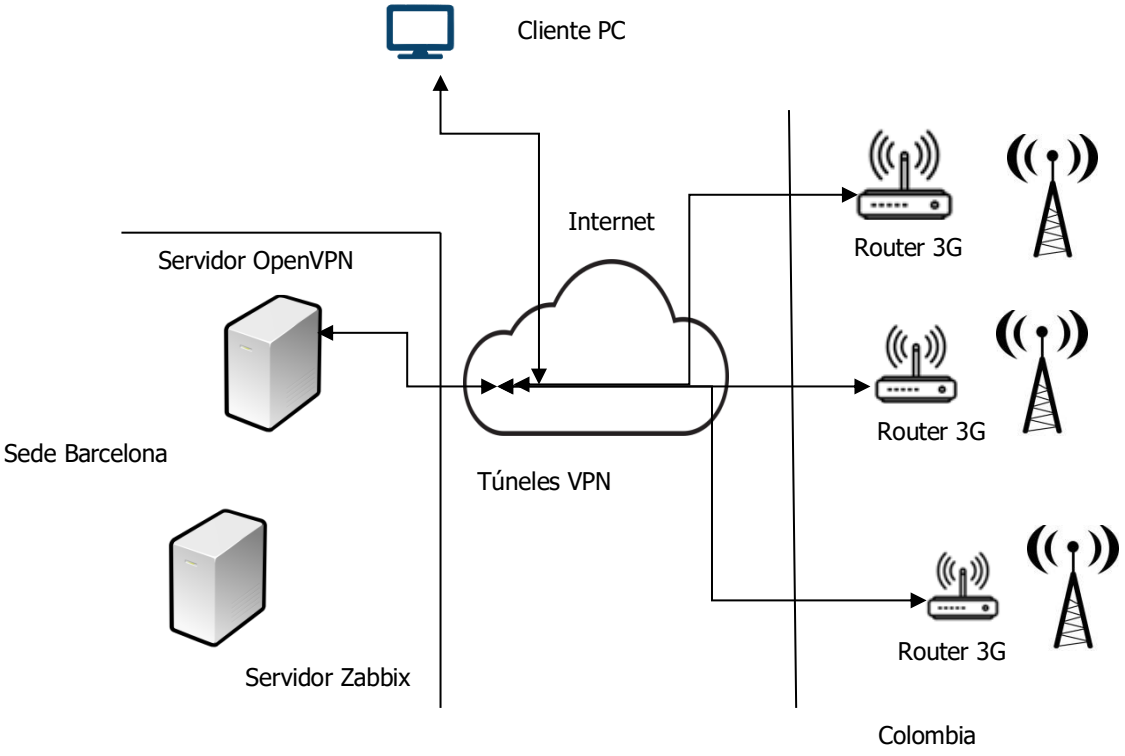


Figura 1 Red de gestión

2. Objetivos del Trabajo

2.1. General

Diseñar e implementar una red de gestión para Transmisores FM de la marca Link serie Advancast -sobre protocolo SNMP (Simple Network Management Protocol)- utilizando un servidor Zabbix.

Utilizar la red celular 2G/3G (GSM/UMTS) de Colombia para conectar los emplazamientos a Internet.

Realizar conexiones seguras punto a punto médiate conectividad VPN (Virtual Private Network).

2.2. Específicos

- Instalar y configurar el servidor Zabbix y personalizar la interfaz web.
- Diseñar la red LAN en los emplazamientos y realizar la tabla de direccionamiento IP.
- Configurar los Routers 3G Teltonika RUT500, asignados a cada emplazamiento.
- Instalar y configurar un servidor VPN con software de código abierto (OpenVPN).
- Configurar los clientes OpenVPN.
- Contratar un proveedor de servicios de Internet.

2.3. Planificación del Trabajo

En la figura 2 se muestra la planificación temporal del proyecto. La fecha de inicio es el 9 de marzo con la aceptación de la propuesta por parte del consultor. A partir de aquí, se desarrollarán los temas propuestos para la solución del proyecto. En la figura 2 aparecen todas las fechas de entrega. La fecha final del proyecto será el 10 de junio, con la entrega de la memoria final.

Debido a que en la entrega de la PAC2 no se cumplieron los objetivos marcados, se ha tenido que realizar una restructuración del proyecto. Este cambio ha afectado en el desarrollo de los temas. En primer lugar, se ha cambiado el planteamiento teórico con el objetivo de aportar una perspectiva más personal y no tan teórica. Se han añadido más gráficas que facilitan la lectura y comprensión del texto. Y finalmente, se han modificado los puntos para añadir diferentes tecnologías y compararlas entre ellas.

Se ha dedicado un mayor número de horas de trabajo para cumplir con los plazos de entrega. De esta manera, se ha conseguido no desviarse de los ítems marcados en la planificación temporal del trabajo.

	Nombre	Duración	Inicio	Fin
1	Pac1	1d?	09/03/2016	09/03/2016
2	Diseño de la solucion	54d?	10/03/2016	24/05/2016
3	5.1 Tx FM	6d?	11/03/2016	18/03/2016
4	5.1.1 Configuracion	2d?	11/03/2016	14/03/2016
5	5.1.2 SNMP	2d?	14/03/2016	15/03/2016
6	5.1.3 Gestor web	3d?	16/03/2016	18/03/2016
7	5.2 Conectividad	27d?	11/03/2016	18/04/2016
8	5.2.1a XDSL	4d?	15/03/2016	18/03/2016
9	5.2.1b Fibra/Coaxial	4d?	18/03/2016	23/03/2016
10	5.2.1c Satelite	4d?	23/03/2016	28/03/2016
11	5.2.1d Radio enlaces	4d	30/03/2016	04/04/2016
12	5.2.1e Wimax/Wi-fi	4d?	05/04/2016	08/04/2016
13	5.2.1f Red Celular	7d	08/04/2016	18/04/2016
14	5.2.2 Eleccion Tecnologia	2d?	19/04/2016	20/04/2016
15	Pac2	1d?	20/04/2016	20/04/2016
16	5.3 Networking	14d?	21/04/2016	10/05/2016
17	5.3.1Diseño Red IP	5d?	21/04/2016	27/04/2016
18	5.3.2 Tipo VPN	5d?	27/04/2016	03/05/2016
19	5.3.3 Solucion VPN	5d?	04/05/2016	10/05/2016
20	5.4 Sistema Supervision	10d?	12/05/2016	25/05/2016
21	5.4.1 Protocolo SNMP	4d?	12/05/2016	17/05/2016
22	5.4.2 Sistema NMS	6d?	18/05/2016	25/05/2016
23	PAC3	1d?	25/05/2016	25/05/2016
24	5.5 Configurciones	54d?	11/03/2016	25/05/2016
25	Memoria final	11d?	27/05/2016	10/06/2016
26	Entrega memoria	1d?	10/06/2016	10/06/2016

Figura 2.Planificación del trabajo

3. Arquitectura de Red

3.1. Infraestructuras

En este aparatado se realizará una breve descripción de las estaciones base en las que se encuentran instalados los equipos transmisores de FM. Los emplazamientos, que son propiedad del radiodifusor colombiano, se encuentran ubicados en gran parte en entornos rurales o de alta montaña de difícil acceso y otros en entorno urbano.

Los sites son del tipo no atendido, ya que las instalaciones no están adecuadas para la presencia de personal durante una jornada laboral, sino para albergar únicamente los equipos de radiodifusión. Tampoco se dispone en la actualidad de ningún sistema de monitorización, ni conexión a otras redes de telecomunicaciones, por lo que se realizara un estudio de viabilidad para tener acceso a proveedores de servicio de Internet (ISP).

3.2. Emplazamientos

Un emplazamiento, o site, es una infraestructura destinada al uso exclusivo de los equipos de telecomunicaciones. En función de su ubicación geográfica, los emplazamientos pueden ser rurales o urbanos.

Los emplazamientos ubicados en zonas rurales son recintos vallados en los que se construye una caseta de material y de una demisión reducida. El acceso a los emplazamientos se realiza, habitualmente, por pistas forestales que no están en buen estado y se hace necesario utilizar vehículos con tracción en las cuatro ruedas (4x4).

En el interior de la caseta se distribuyen por filas los armarios (Racks), en los que se encuentran los equipos. Las casetas están climatizadas mediante aire acondicionado, debido a que la temperatura en su interior puede llegar a ser elevada por el calor que disipan los equipos instalados.

El suministro eléctrico llega médiate postes que sujetan, de forma aérea, la acometida eléctrica. Dependiendo de las dimensión y de la zona de cobertura del site y de los servicios de los que dispone (Radio, Televisión, Telefonía Móvil), se suele instalar en una habitación contigua a la habitación de racks un grupo electrógeno que actuará en caso de falta de suministro eléctrico.

Dentro del recinto vallado, y lo más cerca a la caseta posible, se eleva la torre generalmente auto-soportada de entre 20 y 40 metros de altura, donde se instalan los sistemas radiantes (antenas).

Los emplazamientos urbanos se encuentran en las cubiertas de los edificios. También disponen de una caseta prefabricada de fibra de vidrio y de

dimensiones reducidas. Disponen de aire acondicionado para refrigeración y no necesitan de grupo electrógeno en su gran mayoría, ya que al estar en zonas urbanas tienen menos posibilidad de fallo eléctrico. Los sistemas radiantes se distribuyen en mástiles instalados en las cubiertas de los edificios y no tienen problemas de acceso.

Emplazamiento en medio rural

Emplazamiento medio urbano

Figura 3.Emplazamientos

En la figura 4 se muestra la ubicación geográfica de los emplazamientos y los equipos instalados con las potencias correspondientes.

Figura 4.Ubicación geografica de los Transmisores FM

3.3. Estudio de Conectividad

El objetivo es conectar la sede central, que se encuentra en Barcelona, con los distintos emplazamientos de Colombia. Para ello, se debe tener en cuenta:

- ¿Qué tipo de infraestructura de acceso utilizaremos?
- ¿Cuáles son los requisitos?
- ¿Qué tipo de tráfico circula por la red?
- El costo y rendimiento que ofrecen los diversos proveedores de servicio

Conceptualmente, una Red WAN es una red dispersa geográficamente. Esto se aplica al diseño que se busca en este proyecto, ya que se interconectaran distintas redes de área local (LAN). Una red LAN que estará compuesta por los servidores en Barcelona y las otras redes LAN estarán conformadas por los dispositivos instalados en los diferentes emplazamientos de Colombia.

El rendimiento en una red WAN está sujeto a diversas variables que se dan a nivel 2 del modelo OSI. Las variables incluyen aspectos como la latencia, los paquetes Broadcast u otros que se ven afectados por las distancias.

Topología de Red WAN

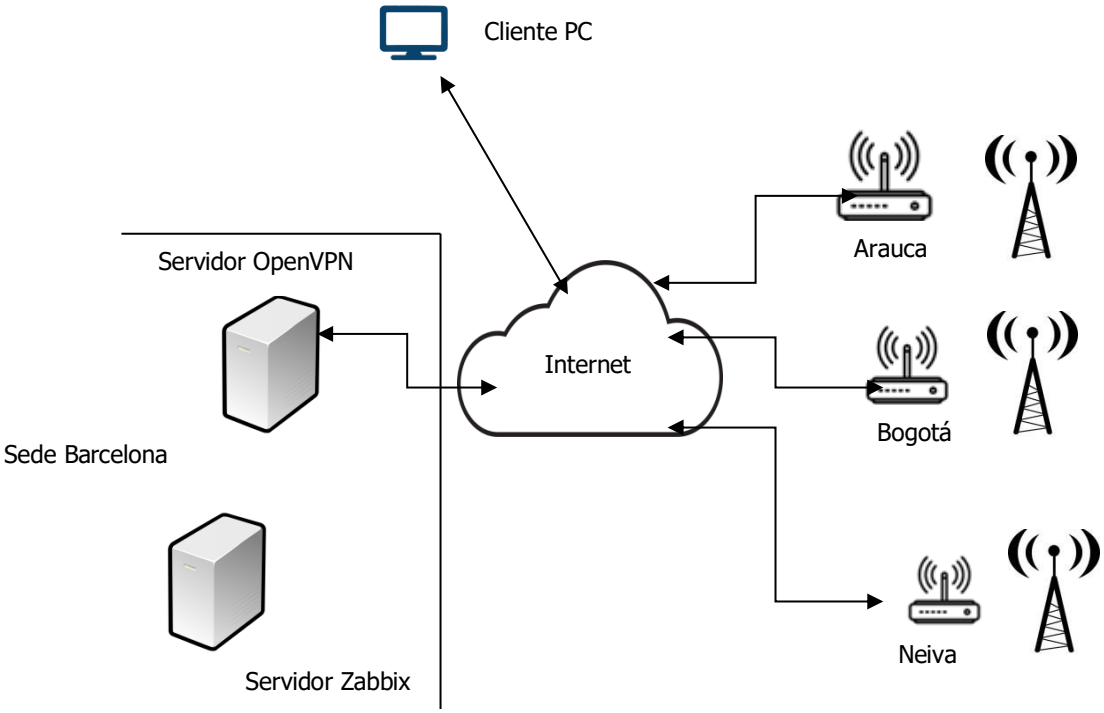


Figura 5. Topología red WAN

Barcelona:

Se decide que en la sede central de Molins de Rei estará instalado el servidor Zabbix, también llamado “gerente”, que realizará la gestión del grupo de host ubicados en Colombia.

Cada sistema gestionado ejecutará en todo momento un componente de software llamado “agente” que reportará la información a través de SNMP al gerente. Los agentes SNMP expondrán los datos de gestión en los sistemas administrativos como variables accesibles que están organizadas por jerarquías.

La conexión con el proveedor de Internet (ISP) en el extremo de Barcelona está solucionada, ya que la sede consta con una conexión banda ancha por fibra óptica, con un ancho de banda suficiente para cubrir las necesidades de tráfico que pueda generar la red.

Colombia:

La conexión con Internet se realizará a través de la red celular 3G. Después de realizar estudios de cobertura en diferentes emplazamientos sobre distintas tecnologías como cableadas e inalámbricas, se llega a la conclusión que la conectividad ofrecida por la red celular es la que mejor cobertura en medios rurales dispone actualmente en Colombia.

Actualmente, en Bogotá hay una delegación que hace de nexo entre el cliente y Barcelona, y se encarga también de dar soporte a los técnicos locales, en lo que a mantenimiento de los equipos se refiere. Los técnicos que trabajan en esta delegación han sido los encargados de realizar medidas de cobertura en distintos emplazamientos, en los cuales se podría prever que el nivel de recepción en el interior sería inferior a los límites deseados.

Los resultados indicaron que la red celular 3G (UMTS) que mejor cobertura ofrecía correspondía al del operador Claro. Los niveles de recepción en zonas urbanas, en el peor de los casos, era de -85dBm y en zonas con menor densidad de población o zonas rurales, los niveles oscilaron entre -90dBm y -98dBm.

Los estudios de cobertura también indicaron que en los emplazamientos ubicados en la zona sur de Colombia eran los que más deficiencia de cobertura tenían. El nivel de recepción en sites como Neiva, Popayán, Florencia y Pasto oscilaba entre los -90dBm los -100dBm.

Según el mapa de cobertura que facilita Claro en su página web, estos niveles de cobertura no son los óptimos para establecer una conexión 3G correcta.
Se propone realizar la instalación de antenas exteriores direccionales tipo Yagi en los emplazamientos con déficit de cobertura. De esta manera, se mejora el nivel de recepción en los sites y se consigue una buena señal 3G.

La frecuencia en la cual trabaja Claro para el servicio 3G (UMTS/HSDPA) es 850Mhz, por lo que la antena Yagi deberá estar adaptada para una banda que incluya esta frecuencia. Dado que en el peor nivel de recepción, éste cae hasta los -100dBm, se busca una antena que como mínimo tenga una ganancia de unos 10dBi aproximadamente.

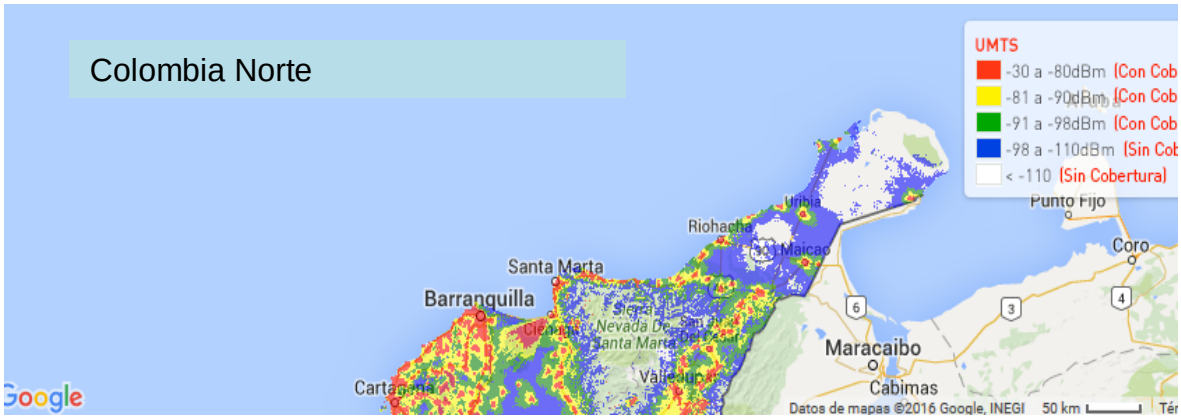
La solución escogida es una antena Yagi de 14 elementos de la marca TXPRO, modelo TX8001614.

Características de la Antena:

-Rango de frecuencia: 824-896 MHz.
-Ganancia: 16 dBi.
-Apertura (Horizontal / Vertical): 28° / 25°.
-Potencia: 100 W.
-Conector: N Hembra.
-Longitud: 151 cm.

Figura 6. Antena Yagi

Mapa de cobertura 3G Claro



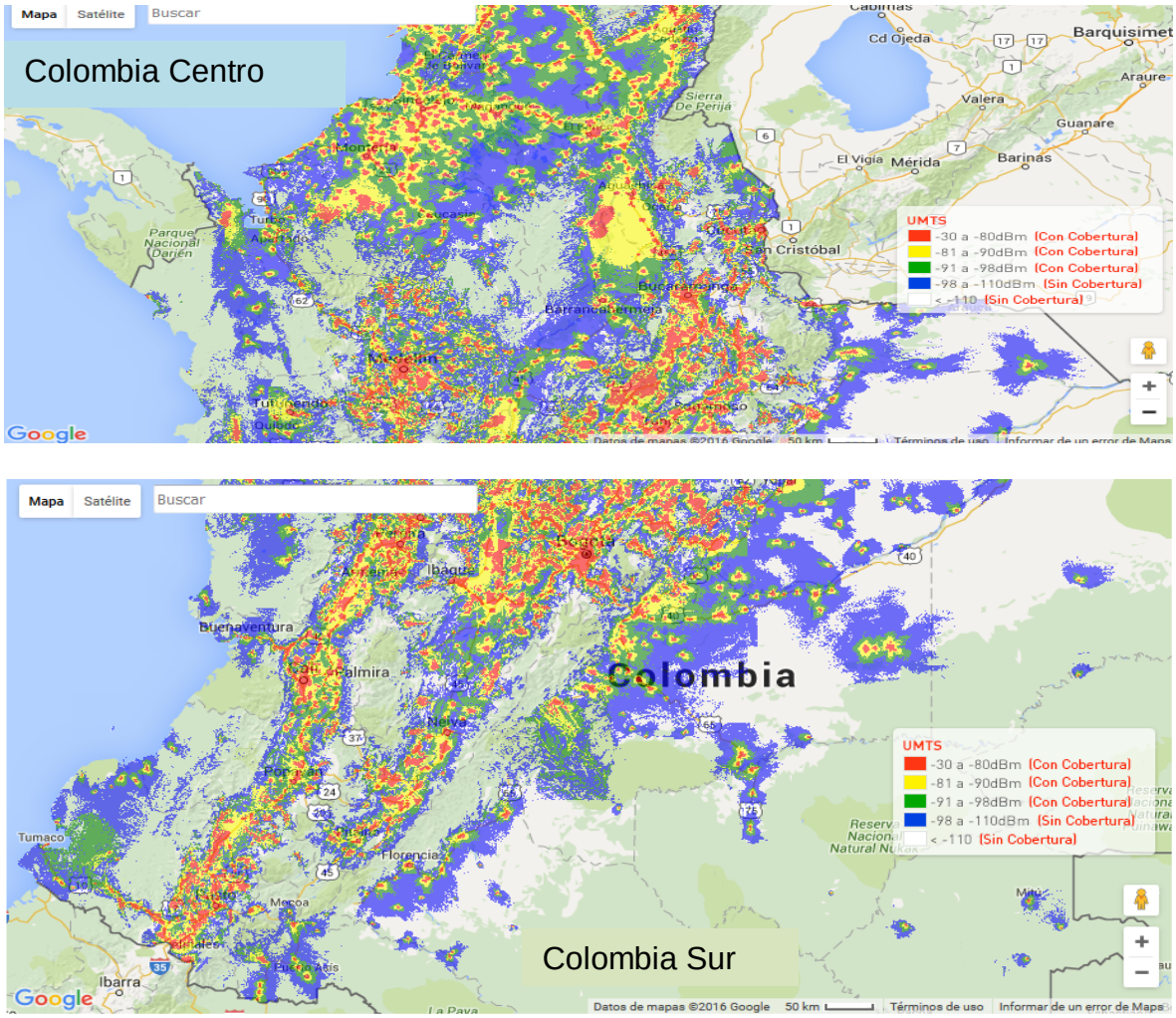


Figura 7.Cobertura Claro

3.4. Tránsito en Internet

El tránsito en una red, o en diferentes redes interconectadas, se puede dividir en dos categorías.

a. El tránsito que se adapta a cambios en el retardo y en el rendimiento de la red y aun así continua cubriendo las necesidades de las aplicaciones, que se denomina “Tránsito elástico”. Este es que normalmente circula a través de las redes basadas en TCP/IP. Algunas de estas aplicaciones son el correo electrónico, la transferencia de ficheros, la gestión de red, el acceso a web, etc.

b. El otro tipo de transito denominado “Tránsito inelástico” o tránsito en tiempo real, es el que no se adapta tan fácilmente a los cambios en el retardo y en el rendimiento de la red. Es un tipo de tránsito que necesita un rendimiento mínimo, no puede sufrir retardos ni variaciones de estos retardos.

La red de gestión se basa en el protocolo SNMP y el servidor Zabbix utiliza una interfaz web sobre protocolo HTTP (Hypertext Transfer Protocol), por lo que el tráfico que se genere en la red será de tipo elástico, descartando así que por la red circule tráfico en tiempo real, que necesita un mayor ancho de banda.

Teniendo en cuenta esto, se realizará una breve estimación de ancho de banda que será necesario contratar para las conexiones con Internet de los emplazamientos de Colombia.

La RFC 3416 [2] define la versión 2 del protocolo de operaciones para el Protocolo simple de administración de redes (SNMP). En el apartado 2.3 “Size Mensage”, se define el tamaño de un mensaje SNMP:

“El tamaño máximo de un mensaje SNMP se limita al mínimo de:

(1) el tamaño máximo de mensaje que la entidad puede destino SNMP puede aceptar, y,

(2) el tamaño máximo de mensaje que la fuente de SNMP entidad puede generar.”

La definición no determina claramente el tamaño de un paquete SNMP, pero en este apartado recomienda evitar la fragmentación para que no se produzca perdida de información. La norma indica que el tamaño medio que una entidad SNMP debe aceptar se de 484 bytes., también recomienda que debe aceptar hasta un máximo de 1472 bytes, que corresponde al tamaño de mensaje más grande que puede ser encapsulado en una trama Ethernet

La RFC 3416 también aconseja ser más bien conservador en el envío de mensajes, cita textual:

“Quien envía una PDU GetBulkRequest debe tener cuidado en ajustar sus parámetros. En consecuencia, a fin de reducir el riesgo de fragmentación, y en particular, en condiciones de estrés de la red, sólo deben utilizarse pequeños valores con un máximo de repeticiones.”

Teniendo en cuenta estos parámetros, se ha configurado el servidor para realizar una consulta por minuto y los cálculos se realizarán con la recomendación de 484 bytes.

De esta forma, en un mes se realizarán 43200 consultas. Esta cifra multiplicada por el tamaño de mensaje resulta 20908800 bytes, que son 19.94MBytes de consumo, si se le suma el tamaño de la página del servidor que es de 14.42KB.

Si se realizan cuatro consultas a la página diarias durante treinta días, se obtiene un consumo de 1730.4KB. Esta cifra sumada a la anterior resulta 21.63MB consumo/mes.

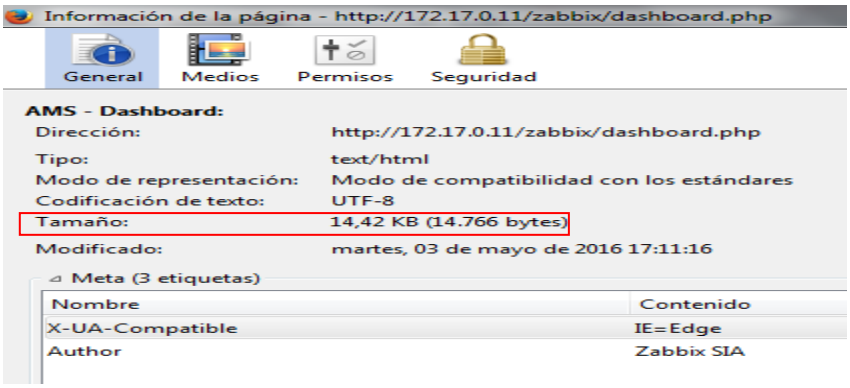


Figura 8. Tamaño página http

Se decide contratar la tarifa Plan 1000MB [3] que ofrece el operador Claro, con una capacidad de datos de 1024MB (1GB) y con un coste mensual de 30900 $ Peso Colombiano, que equivalen a 10,76US$ Dólar Americano.

Esta tarifa es la de mínima capacidad que se puede contratar y aunque está sobredimensionada para el consumo anteriormente calculado, hay que tener en cuenta una posible ampliación de servicios en el futuro.

En lo que al mantenimiento se refiere, un técnico que esté utilizando la conexión WiFi en un emplazamiento puede necesitar que se lo asesore y de esta forma podrá realizar llamadas VoIP (mediante Skype, por ejemplo) a la sede de Barcelona, enviar correos electrónicos o consultar documentación a través de Internet. Con lo cual, es posible que se realice un uso completo de la capacidad contratada.

Plan	Capacidad de Datos Incluida	CFM con IVA*	Aplicación a la que puede continuar accediendo una vez consumida la capacidad del plan
Plan 1000 MB 2016	1024 MB (1GB)	$ 30.900	Facebook, Twitter y Chat de WhatsApp
Plan 1500 MB 2016	1536MB (1,5GB)	$ 36.900	
Plan 2000 MB 2016	2048 MB (2GB)	$ 42.900	
Plan 2500 MB 2016	2560 MB (2,5 GB)	$ 48.900	
Plan 3000 MB 2016	3072 MB (3GB)	$ 53.900	
Plan 3500 MB 2016	3584 MB (3,5GB)	$ 57.900	
Plan 5000 MB 2016	5120 MB (5GB)	$ 64.900	
Plan 6000 MB 2016	6144 MB (6GB)	$ 69.900	
Plan 7000 MB 2016	7168 MB (7GB)	$ 74.900	
Plan 8000 MB 2016	8192 MB (8GB)	$ 80.900	
Plan 10000 MB 2016	10240 MB (10GB)	$ 107.900	

Figura 9.Tarifa Claro

3.5. Router sobre redes celulares

La estructura de la red de gestión está compuesta por distintas redes LAN, en diferentes zonas geográficas, esto hace necesario la presencia de un dispositivo hardware que sea capaz de interconectar dichas redes a través de Internet.

El dispositivo capaz de realizar la interconexión entre redes y rutear los paquetes, desde el origen hasta destino, es un Router. Este equipo desempeña su trabajo en el nivel de red del modelo OSI y realiza la interconexión de redes a través de Internet.

En el extremo de Barcelona hay instalado un Router que da servicio a la red local y dará salida a Internet a los servidores. En cada uno de los emplazamientos es necesaria la instalación de un Router que deberá cumplir con una serie de requisitos.

Las características que debe reunir el Router a seleccionar serán:

- El Router deberá ser de tipo industrial y que se pueda utilizar en la red celular de Colombia, ya que la conexión con Internet, como se explica anteriormente, se realizará con el operador local “Claro” de telefonía móvil a través de su red 3G.

- Deberá disponer, como mínimo, de tres puertos LAN para conectar los equipos que se encuentra instalados en los emplazamientos (un Combinador y dos Excitadores).

- La conexión extremo a extremo se realizará médiate túneles VPN. En el extremo de Barcelona se instalará un servidor OpenVPN, por lo que deberá ser configurable como cliente OpenVPN.

- Dado que se ha pensado en la posibilidad de que un técnico se pueda conectar en el emplazamiento con su ordenador portátil mediante conexión Wi-Fi, deberá tener opción Wireless compatible con los estándares actuales de conexión, IEEE 802.11n, IEEE 802.11g, IEEE 802.11b.

El mercado ofrece una gran variedad de productos que cumplen con los requisitos. A continuación se muestran algunos:

DLink modelo DWR-921:

- 4 10/100 Ethernet LAN ports
- WAN (RJ-45) port
- Two detachable 4G LTE / 3G antenas
- 802.11n, compatible with 802.11g/b;
- L2TP/PPTP/IPSEC VPN pass-through
- Precio: 138€

[4]

Figura 10.DLink DWR-921

TP-LINK modelo Archer MR200:

- 3 10/100Mbps LAN Ports, 1 10/100Mbps LAN/WAN Port, 1 SIM Card Slot
- IPSec VPN: Supports up to 10 IPSec VPN tunnels
- Port Forwarding: Virtual Server, Port Triggering, UPnP, DMZ
- IEEE 802.11ac/n/a 5GHz, IEEE 802.11b/g/n 2.4GHz
- Precio: 137€

[5]

Figura 11.TP-LINK MR200

Teltonika modelo RUT500:

- 3 10/100Mbps LAN Ports
- 1x WAN 10/100Mbps Ethernet port
- Complies with IEEE 802.11n, IEEE 802.11g,
  IEEE 802.11b wireless standards
- OpenVPN
- Monitoring by SNMP
- NAT: Virtual server
- Precio: 105€

[6]

Figura 12.Teltonika RUT500

A la hora de escoger Router, la opción del RUT500 de la marca Teltonika es la escogida para instalar en los emplazamientos. Si bien la comparativa entre precios y prestaciones son similares, el router modelo RUT500 de Teltonika brinda la oportunidad de trabajar con OpenVPN, que era uno de los requisitos anteriormente mencionados. Además, se sabe por experiencia de anteriores proyectos que es un dispositivo fiable y de fácil configuración.

Sus características principales se detallan en la página web de la marca www.teltonika.it

Se describe como: "Un router compacto con HSPA + 3G de alta velocidad, conexiones wi-fi y Ethernet"

3.6. Justificación de Conectividad

- **Tipos de Redes de Acceso**

XDSL: Es una red de conmutación de paquetes que proporciona acceso a Internet con alta velocidad sobre la línea telefónica a los hogares. Existe una familia de módems conocidos como xDSL (x-type subscriber line) que operan de nexo entre las redes LAN e Internet. Los más populares son los denominados ADSL.

ADSL (Línea de abonado digital asimétrica): Es un tipo de línea perteneciente al grupo de la línea DSL, que realiza una transmisión analógica de datos digitales a través del par trenzado de cobre. Como su nombre indica, el término asimétrico está asociado al hecho que proporciona más capacidad de ancho de banda al enlace de bajada que al de subida. Se define una tasa de transferencia estándar que son de 12 Mbps de bajada con 1.8 Mbps en subida [ITU1999]; y 24Mbps de bajada con 2.5Mbps de subida [ITU 2003]. Dependerá de la longitud del enlace de par trenzado, de la calidad del cable, de las interferencias, etc.

Internet de acceso por cable (HFC): Es otra forma de acceso a Internet mediante la infraestructura de cable coaxial. Esta forma requiere módems especiales denominados cable-módems. El modo de trabajo es similar a la red DSL, el cable-modem divide la red HFC en dos canales, un canal de bajada y otro de subida. También es de acceso asimétrico. La DOCSIS 2.0 es el estándar que define la velocidad de tasa de transferencia, que es para el canal de bajada 42,8Mbps y el canal de subida 30,7Mbps.

El inconveniente de este sistema es la compartición de los enlaces, por lo que se comparte también ancho de banda con diferentes usuarios, lo que puede generar faltas de seguridad en las comunicaciones.

Fibra Óptica (FTTH): También conocida como fibra hasta casa. Esta red de distribución óptica hace llegar un enlace óptico directamente, desde el nodo hasta el usuario en el que se encuentra el terminador de red óptico (ONT). La

velocidad de tasa de transferencia en el enlace de bajada es aproximadamente de 20 Mbps [FTTH Council 2011b].

Satélite: En lugares a los que no llegan DSL, cable o FTTH, por ejemplo en zonas rurales, se puede usar la conexión satélite para dar servicio de Internet a los domicilios con velocidades de 1Mbps.

Red Celular 3G UMTS: UMTS es el estándar Europeo para tercera generación de redes de gran alcance sin hilos. Se realizan actualizaciones de las versiones de UMTS a cargo de 3GPP (3rd generation partnership project), que es un grupo de trabajo del ETSI. En la actualización de 1999 (R99), la red troncal de UMTS era la de GPRS. En diversas actualizaciones posteriores, se realizaron cambios, hasta que en la reléase 6 se consigue la arquitectura básica de UMTS. Las especificaciones de UMTS son 5MHz de ancho de banda por canal. Con respecto a la velocidad, dependerá de la celda que da el servicio, con baja movilidad (10km/h) se llega hasta 2Mbps.

- **Estado actual de Colombia**

La intención es conocer el estado actual de la banda ancha en Colombia y de algunos elementos de las tecnologías de la Información y las comunicaciones en el país.

La información se recoge a través de diferentes informes nacionales e internacionales del sector, estadísticas y datos recopilados de diferentes reportes. Se resume los principales objetivos del actual plan de desarrollo de las TIC “Plan Vive Digital” [11], además de sus campos de acción y alcances.

Por las características geográficas de Colombia, el despliegue en infraestructuras de redes acceso, ya sean sobre Par de cobre trenzado, Fibra Óptica o Cable Coaxial, se dificulta por los altos costos que conllevan construcción, por lo que la penetración de Adsl cableado en el país no es muy extensa.

Las principales operadoras del país como Movistar, Claro, ETB o Tigo ofrecen unas velocidades de conexión que van desde los 2Mbps hasta los 15Mbps, por lo general, con capacidad ilimitada, por un precio promedio de US$ 40 (Dólares Americanos).

La figura 16[12] muestra un mapa que indica la de penetración de internet fijo a nivel nacional.

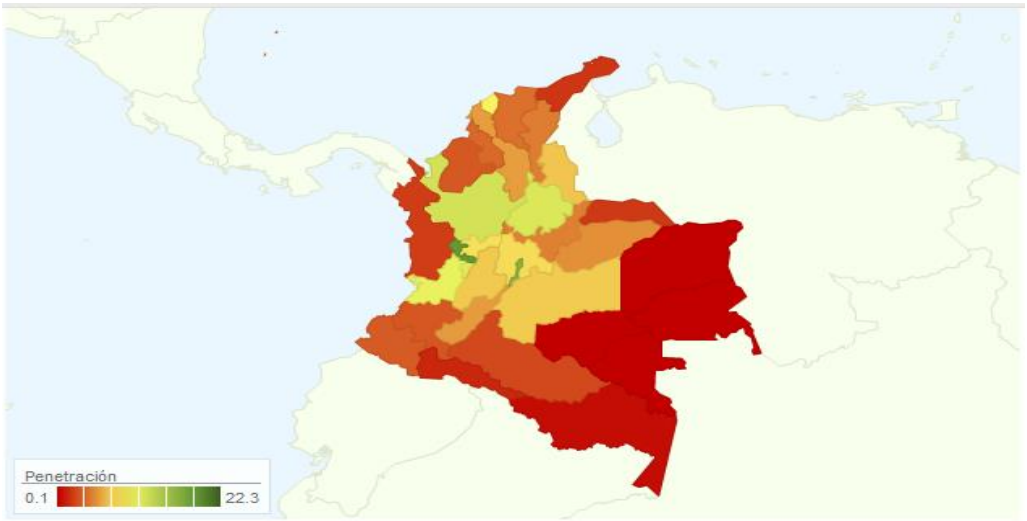


Figura 13. Cobertura ADSL

- **Satélite**

La Conexión a Internet Vía Satélite es la solución para acceder a la red a gran velocidad desde lugares donde no existe cobertura ADSL.

Existen dos formas de implementar la Conexión a Internet Vía Satélite:

Sistema Una Vía: Esta forma de conexión utiliza el satélite sólo para recibir datos. Por tanto, es necesario disponer de otra conexión a Internet, aunque sea de baja velocidad (vía módem, Móvil GSM o GPRS, RDSI, ADSL, TRAC...).
Este sistema realiza las peticiones a través de la conexión terrestre y recibe los datos por satélite, lo que nos permitirá acceder a Internet con un mayor ancho de banda, proporcionándonos mayor velocidad de navegación y descarga de ficheros. Actualmente, se pueden contratar conexiones de 256 Kbps, 512 Kbps y 1 Mbps.

Sistema de Doble Vía: Esta forma de conexión utiliza el satélite para enviar y recibir datos. No necesitaremos otra conexión adicional y tendremos acceso a Internet desde cualquier zona de cobertura del satélite. Normalmente, este tipo de conexiones son asimétricas, es decir, tendremos diferente velocidad de envío y de recepción. Las velocidades de subida irán entre los 64 Kbps y los 2.048 Kbps. Las velocidades de bajada irán desde 256 Kbps a 38 Mbps.

La posibilidad de internet por satélite es un mercado nuevo en el país. En busca de información de operadoras que desarrollen esta tecnología, se ha encontrado una empresa llamada BanSAT.

En su página web http://www.bansat.co/ dan información sobre la cobertura geográfica que ofrecen.

Imagen de cobertura:

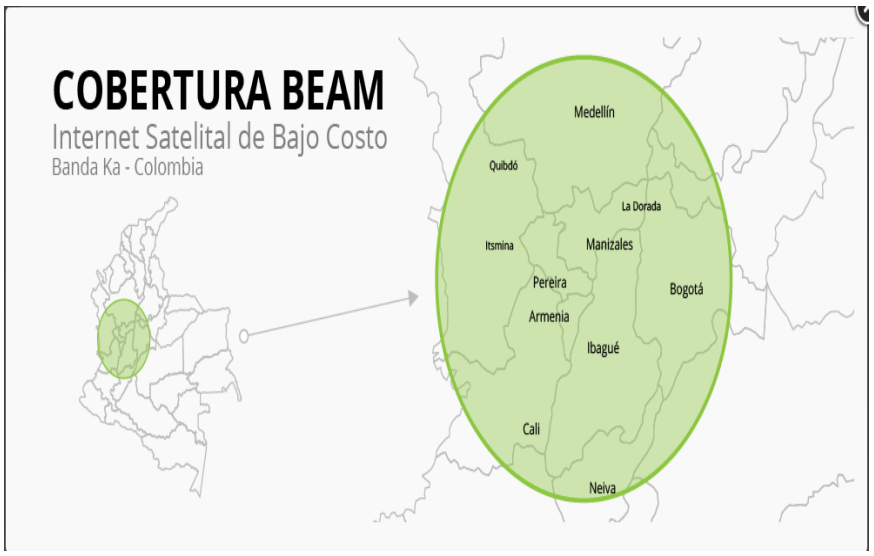


Figura 14. Cobertura Satélite

- **Radio Enlaces RF**

Una red de transporte con enlaces de radiofrecuencia podría ser una solución práctica que prestaría la misma utilidad que el ADSL o internet móvil. El cliente no dispone de esta infraestructura para comunicar los emplazamientos y así poder utilizarla para la red de gestión.

- **Red Celular 3G**

En Colombia se está llevando a cabo la implementación, por parte del gobierno, del “Plan Vive Digital”. La intención del plan es favorecer el acceso a Internet a la población, ya sea mediante conexiones fijas de más de 1024kbps e inalámbricas de 3G/4G.

Es por esto que dentro de las iniciativas planteadas para aumentar la cobertura se encuentra la asignación de más espectro radioeléctrico para este tipo de servicios, el aumento de la conectividad internacional y de la cobertura de la red de fibra óptica nacional a más de 700 municipios en el país.

Los avances tecnológicos en materia de banda ancha de redes inalámbricas se están dando en tecnologías denominadas genéricamente como 3G o 4G que ofrecen servicios de datos y acceso a Internet a velocidades que en teoría pueden superar los 300 Mbps, aunque típicamente la oferta comercial inicia en los 20 Mbps de velocidad, lo cual resulta superior al promedio de las velocidad de conexiones fijas, de cable o xDSL.

La opción de internet móvil es la más viable para las necesidades del proyecto, por el despliegue en infraestructura realizado en el país en los últimos años.

Un inconveniente a la hora de contratar servicios de internet móvil, es el de saber la capacidad que debemos contratar. Esto podría afectar al servicio ya

que si contratamos poca capacidad y luego la demanda es mayor podría verse afectada la calidad del servicio.

La siguiente tabla muestra una comparativa de precios de internet móvil.

Producto	Cargo Mensual	Capacidad	Costo por Mb	Costos Adicionales	Velocidad
Limitado Control Mes 1Gb tigo	$ 29.900	1,0 Gb	$ 29,20	Pospago	4.0 Mbps (min:128 kbps)
Plan Navegación 2Gb Claro	$ 42.900	2,0 Gb	$ 20,95	Pospago	5.0 Mbps
Limitado Control Mes 2Gb tigo	$ 39.900	2,0 Gb	$ 19,48	Pospago	4.0 Mbps (min:128 kbps)
Plan Navegación 3Gb Claro	$ 53.900	3,0 Gb	$ 17,55	Pospago	5.0 Mbps
Limitado Control Mes 3Gb tigo	$ 52.900	3,0 Gb	$ 17,22	Pospago	4.0 Mbps (min:128 kbps)
Promoción : $ 35.000 por 2 meses					

Figura 15. Tarifas Internet móvil

- **Comparativa tecnologías Conectividad**

Tecnología	Ventajas	Desventajas	Coste Aproximado
ADSL (Cable de cobre, fibra óptica Cable Coaxial)	Aprovecha cableado de voz. La señal luminosa en fibra óptica está libre de interferencias. La velocidad es mayor.	EL ancho de banda puede ser reducido según la localización del usuario. Poca penetración en zonas rurales.	Alquiler de la red entre 30 a 50 US$.
Satélite	Cobertura en medios rurales.	Necesidad de instalar parábolas en cada emplazamiento. Alta latencia.	Alquiler de la red entre 40 a 60 US$ mes. Suministro e instalación antenas 200 US$ unidad
Radio Enlaces Microondas en banda licenciada	Sistema privado punto a punto.	El despliegue de una red de este tipo tiene un coste muy elevado.	Suministro e instalación antenas 10000 US$ unidad.
Red Celular 3G	Crecimiento a nivel de infraestructuras en el país.	Se deberá tener en cuenta la capacidad contratada.	Alquiler de la red entre 25 a 50 US$

[13]

- **Conclusión**

De los datos obtenidos en la comparativa anterior, se observa que la principal desventaja de la tecnología ADSL es que no existe garantía por parte de ninguna de la operadoras que trabajan en Colombia de ofrecer cobertura a los emplazamientos.

La solución ofrecida por satélite es viable y el precio que ofrece la operadora por el alquiler de la red es competitivo. Pero se ha sopesado el coste que conllevaría el suministro e instalación de antenas parabólicas para la recepción satelital y se concluye que sobrepasaría el presupuesto marcado para el proyecto. Lo mismo ocurre con los Radio Enlaces de microondas. El proyecto se encuentra actualmente en vías de desarrollo y no es posible la elección de esta tecnología por costes.

La opción de trabajar con la red celular es la más viable de las vistas anteriormente. A nivel de infraestructuras, Colombia se encuentra enmarcada en un plan de inversión por parte del gobierno, con lo cual las operadoras invierten en este aspecto. El alquiler de la red es moderado y ofrecen distintos precios según la tarifa que se contrate. En el aspecto de coberturas en el interior de los emplazamientos, se realizaron mediciones en distintas visitas realizadas.

3.7. Direccionamiento IP

La interconexión entre distintas redes LAN a través de Internet la realizará un router 3G de la marca Teltonika. Estos routers disponen de un puerto WAN, que será el interfaz 3G conectado a la red celular, y al que el operador asignará una IP pública dinámica y tres puertos LAN, que serán los que se conectarán a los equipos existentes para crear la red local, y que es la que se pretende dimensionar.

La arquitectura de la red local en los emplazamientos está compuesta por: el router y un transmisor de FM. Éste está equipado con tres puertos LAN, uno para el combinador, y otros dos para cada uno de los excitadores (más adelante se explica con más detalle los diferentes elementos que forman un transmisor FM).

Para la asignación eficiente del direccionamiento, se tiene que conocer el número de Host que van a existir, y dejar prevista una reserva de direccionamiento para futuros despliegues de más equipamientos a gestionar.

Si se parte de la convergencia a un mundo en el que cada vez hay más dispositivos conectados a las redes IP, surge la necesidad de realizar una reserva amplia de direcciones para prever futuros crecimientos de las redes locales.

Dicho esto, la necesidad actual de direcciones de host por emplazamiento es únicamente de 4, más 1 o 2 para la conexión de un ordenador de mantenimiento, cuando se desplace un técnico a ejecutar estas tareas.

En la delegación de Barcelona, en la que se acogerán los servidores, ya hay un direccionamiento impuesto por el departamento de sistemas, que reserva la red 172.17.0.0/16 para el despliegue de este proyecto.

El direccionamiento cedido es de clase B y se traduce en una única red de 254*254 hosts, lo que suma un total de 64516 hosts.

El despliegue de la gestión se va a realizar en 18 emplazamientos, por lo que de partida, es necesario disponer de 18 redes diferentes, pero solo se ha cedido una única red. La solución pasa por segmentar esa red en redes más pequeñas. Esta técnica de segmentación de redes es conocida con el anglicismo *subnetting*.

La solución de establecer una red por emplazamiento, en lugar de hacer que los equipos de los diferentes emplazamientos remotos pertenezcan a una única red, se argumenta en la necesidad de reducir los dominios de *broadcast* al máximo, para ahorrar en tráfico, ya que trabajando en capa 3 se elimina la propagación de tráfico *broadcast* en la red, y por lo tanto se puede reducir la tarifa de datos contratada con el operador de la red celular.

Una vez argumentada la necesidad de practicar el subnetting, se establece convertir la red de clase B asignada en 254 redes de clase C, estableciendo una reserva de 254 hosts por emplazamiento. Si se tiene en cuenta que 4 se reservan para los equipos, quedarán 250 direcciones libres en los emplazamientos para asignar un pool de 10 direcciones IP para la interfaz Wifi habilitada para el mantenimiento y 240 para futuras ampliaciones.

Las direcciones IP (Internet Protocol) son utilizadas para identificar cada uno de los ordenadores u otros dispositivos que están conectados a una red, ya sea una red de trabajo privada (LAN, Local Area Network) o una red de área ancha, (WAN, Wide Area Network) que es una suma de redes LAN interconectadas mediante Routers que disponen de acceso a Internet.

Direcciones públicas y privadas

Hay dos espacios de direcciones IP: las públicas y las privadas. Las direcciones privadas están reservadas y únicamente se pueden utilizar dentro de la red interna, pero no en Internet. De manera que estas direcciones deben ser mapeadas por direcciones públicas cuando quieren salir a Internet.

La RFC 1918 (address allocation for private Internet) define los siguientes rangos de direcciones privadas:

- **Clase A**: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts). Esta clase es para las redes muy grandes, tales como las de una gran compañía internacional.

- **Clase B**: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas. Uso en universidades y grandes compañías.

- **Clase C**: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C continuas. Uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

IP estáticas y dinámicas

IP Estáticas: Se asignarán a los dispositivos, ya que las conexiones se realizan mediante túneles VPN.

IP Dinámicas: El Router consta con un servidor DHCP, al cual se le asigna un rango de direcciones IP que estarán disponibles para la conexión Wi-Fi.

Máscara de subred

La máscara de red [7] (netmask) se encarga de marcar el número de host que pertenece a la red interior.

Clase	Bits	IP Subred	IP Broadcast	Máscara en decimal	CIDR
A	0	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255	sin definir	sin definir
E	1111	240.0.0.0	255.255.255.254	sin definir	sin definir

Figura 16.Clase de máscaras de subred

Se ha decidido realizar una asignación de IP clase B y el prefijo de la red será 172.17.x.x. Al ser un IP clase B le corresponde un máscara 255.255.0.0 (/16), según las normas de IETF (Internet Engineering Task Force), organismo que integra varios grupos de trabajo que se preocupan por la evolución de la arquitectura de Internet y su buen funcionamiento.

Las IP de clase B tipo 172.17.x.x/16 asignan, 16bits para la parte de red y 16 bits para la parte de host.

172.17.0.0/16 → 10101100.00010001.00000000.00000000
16 bits red 16 bits host

Esta configuración deja 2^{16}-2=65534 direcciones IP para asignar a distintos hosts.

De momento, cada emplazamiento necesita únicamente 4 +10 direcciones IP, por lo que se segmentará la red mediante el protocolo de enrutamiento classless que soporta la solución de máscara de subred de tamaño variable (VLSM), que es el proceso de dividir una subred en subredes. La utilización de VLSM tiene como ventaja el mejor aprovechamiento de las direcciones IP.
Para realizar la división en subredes de la IP 172.17.0.0/16, se toman prestados 8 bits más, con lo que se generan 256 subredes con una máscara /24. Esta mascara (/24) permite 2^8-2=254 direcciones IP disponibles para hosts por subred. El rango de subredes irá de 172.17.0.0/24 hasta 172.17.255.0/24.

Así, ante un posible crecimiento de las redes LAN de cada emplazamiento, se tendría direcciones suficientes y en caso de no cubrir las necesidades en un momento dado se podría volver a fragmentar las subredes mediante VLSM.

En la figura 17 se muestra un ejemplo de topología de la red LAN diseñada para cada emplazamiento.

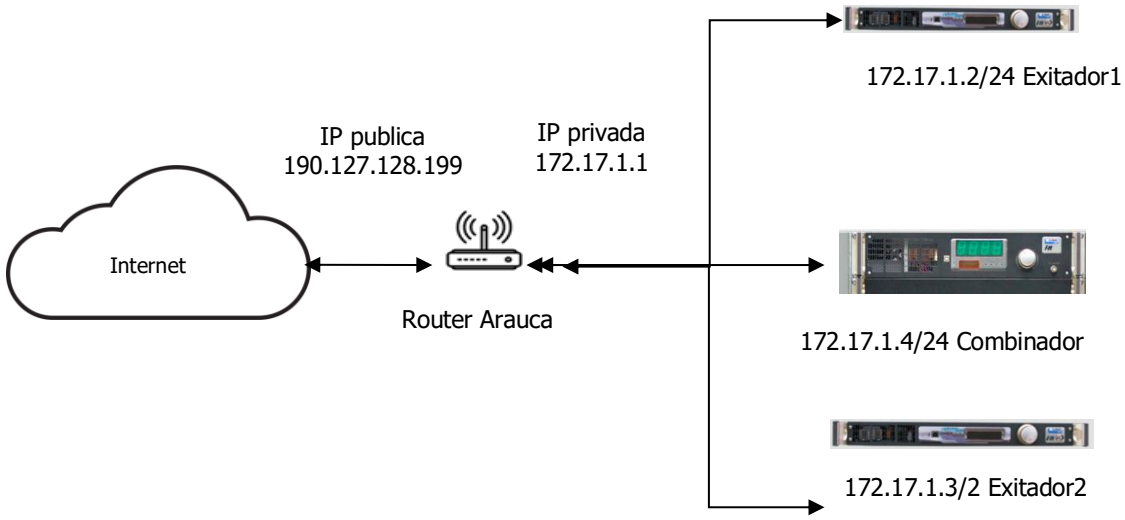


Figura 17.Topología red LAN

Además del rango de las redes LAN, anteriormente mencionado, al trabajar con un servidor OpenVPN, éste necesitará un rango de IP que utilizará cuando un cliente inicie una conexión. El servidor estará configurado para realizar conexiones en modo TUN y este tipo de conexiones crea una interfaz virtual para cada túnel a la que le asigna una IP, que será del rango 172.29.90.0 255.255.255.0. En el apartado de OpenVPN se explicará la configuración del servidor.

Tabla de direccionamiento IP

Barcelona	AMS-Zabbix	172.17.0.11
Barcelona	OpenVPN	172.17.0.5
Cliente	Pool acceso	172.10.128.1-172.10.128.255
Arauca	Router Arauca	172.17.1.1
	Excitador 1 Arauca	172.17.1.2
	Excitador 2 Arauca	172.17.1.3
	Combinador Arauca	172.17.1.4
	Pool Wireless Arauca	172.17.1.50-172.17.1.60
Barranquilla	Router Barranquilla	172.17.2.1
	Excitador 1 Barranquilla	172.17.2.2
	Excitador 2 Barranquilla	172.17.2.3
	Combinador Barranquilla	172.17.2.4
	Pool Wireless Barranquilla	172.17.2.50-172.17.2.60

Bogotá	Router Bogotá	172.17.3.1
	Excitador 1 Bogotá	172.17.3.2
	Excitador 2 Bogotá	172.17.3.3
	Combinador Bogotá	172.17.3.4
	Pool Wireless Bogotá	172.17.3.50-172.17.3.60
Cali	Router Cali	172.17.4.1
	Excitador 1 Cali	172.17.4.2
	Excitador 2 Cali	172.17.4.3
	Combinador Cali	172.17.4.4
	Pool Wireless Cali	172.17.4.50-172.17.4.60
Cartagena	Router Cartagena	172.17.5.1
	Excitador 1 Cartagena	172.17.5.2
	Excitador 2 Cartagena	172.17.5.3
	Combinador Cartagena	172.17.5.4
	Pool Wireless Cartagena	172.17.5.50-172.17.5.60
Cúcuta	Router Cúcuta	172.17.6.1
	Excitador 1 Cúcuta	172.17.6.2
	Excitador 2 Cúcuta	172.17.6.3
	Combinador Cúcuta	172.17.6.4
	Pool Wireless Cúcuta	172.17.6.50-172.17.6.60
Florencia	Router Florencia	172.17.7.1
	Excitador 1 Florencia	172.17.7.2
	Excitador 2 Florencia	172.17.7.3
	Combinador Florencia	172.17.7.4
	Pool Wireless Florencia	172.17.7.50-172.17.7.60
Manizales	Router Manizales	172.17.8.1
	Excitador 1 Manizales	172.17.8.2
	Excitador 2 Manizales	172.17.8.3
	Combinador Manizales	172.17.8.4
	Pool Wireless Manizales	172.17.8.50-172.17.8.60
Montería	Router Montería	172.17.9.1
	Excitador 1 Montería	172.17.9.2
	Excitador 2 Montería	172.17.9.3
	Combinador Montería	172.17.9.4
	Pool Wireless Montería	172.17.9.50-172.17.9.60
Pasto	Router Pasto	172.17.10.1
	Excitador 1 Pasto	172.17.10.2
	Excitador 2 Pasto	172.17.10.3
	Combinador Pasto	172.17.10.4
	Pool Wireless Pasto	172.17.10.50-172.17.10.60
Pereira	Router Pereira	172.17.11.1
	Excitador 1 Pereira	172.17.11.2
	Excitador 2 Pereira	172.17.11.3
	Combinador Pereira	172.17.11.4
	Pool Wireless Pereira	172.17.11.50-172.17.11.60
Popayán	Router Popayán	172.17.12.1
	Excitador 1 Popayán	172.17.12.2
	Excitador 2 Popayán	172.17.12.3
	Combinador Popayán	172.17.12.4
	Pool Wireless Popayán	172.17.12.50-172.17.12.60
Riohacha	Router Riohacha	172.17.13.1
	Excitador 1 Riohacha	172.17.13.2
	Excitador 2 Riohacha	172.17.13.3
	Combinador Riohacha	172.17.13.4
	Pool Wireless Riohacha	172.17.13.50-172.17.13.60
Santa Marta	Router Santa Marta	172.17.14.1
	Excitador 1 Santa Marta	172.17.14.2
	Excitador 2 Santa Marta	172.17.14.3
	Combinador Santa Marta	172.17.14.4
	Pool Wireless Santa Marta	172.17.14.50-172.17.14.60

Tunja	Router Tunja	172.17.15.1
	Excitador 1 Tunja	172.17.15.2
	Excitador 2 Tunja	172.17.15.3
	Combinador Tunja	172.17.15.4
	Pool Wireless Tunja	172.17.15.50-172.17.15.60
Valledupar	Router Valledupar	172.17.16.1
	Excitador 1 Valledupar	172.17.16.2
	Excitador 2 Valledupar	172.17.16.3
	Combinador Valledupar	172.17.16.4
	Pool Wireless Valledupar	172.17.16.50-172.17.16.60
Neiva	Router Neiva	172.17.17.1
	Excitador 1 Neiva	172.17.17.2
	Excitador 2 Neiva	172.17.17.3
	Combinador Neiva	172.17.17.4
	Pool Wireless Neiva	172.17.17.50-172.17.17.60
Bucaramanga	Router Bucaramanga	172.17.18.1
	Excitador 1 Bucaramanga	172.17.18.2
	Excitador 2 Bucaramanga	172.17.18.3
	Combinador Bucaramanga	172.17.18.4
	Pool Wireless Bucaramanga	172.17.18.50-172.17.18.60

Figura 18. Tabla IP

3.8. OpenVPN (Red Privada Virtual)

De la necesidad de utilizar una red pública como Internet para con conectar los host de la red de gestión con el servidor Zabbix, surge la idea de realizar túnel VPN por medio del software libre OpenVPN.

Una VPN (Red Privada Virtual) se utiliza principalmente para conectar dos redes privadas a través de una red pública de datos, mediante túneles encriptados.

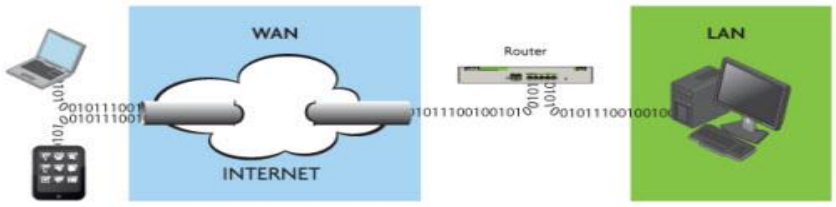


Figura 19. Túnel VPN

Las VPN deben proporcionar: confidencialidad, integridad y autenticación.

Autenticación y autorización: Identificar quien está al otro lado y que nivel de acceso debe tener.

Integridad: Los datos que han sido enviados no han sido alterados, para esto utiliza funciones Hash.

Confidencialidad: Dado que únicamente puede ser interpretada por los destinatarios de la misma, se hace uso de algoritmos de cifrado como DES, 3DES y AES.

La conexión VPN que se llevará a cabo será del tipo punto-multipunto y es normalmente utilizada en topologías cliente/servidor. En este caso, el servidor con acceso a Internet estará instalado en Barcelona y los clientes serán los routers instalados en los emplazamientos del extremo de Colombia, con acceso a Internet por medio de un operador local.

Se barajó también la posibilidad de llevar a cabo conexiones con re direccionamiento de puerto (Port Forwarding).

La redirección de puertos, a veces llamado tunelado de puertos, es la acción de redirigir un puerto de red de un nodo de red a otro. Esta técnica permite que un usuario externo tenga acceso a un puerto en una dirección IP privada (dentro de una LAN) desde el exterior vía un router con NAT activado.

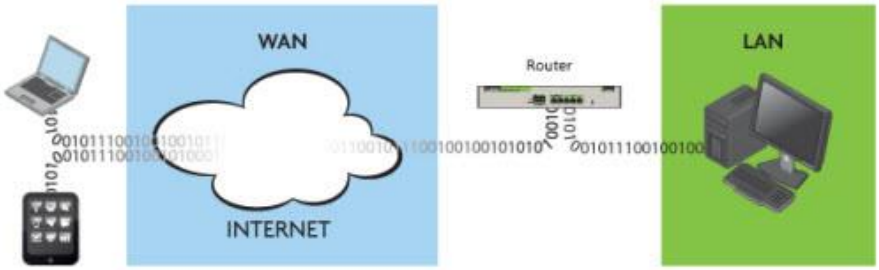


Figura 20. Port Fordwarding

Pero la opción de re direccionado de puertos se descartó finalmente, debido a que la conexión con túneles VPN ofrece más seguridad al encriptar los mensajes. Se aprovechará también el hecho que los routers disponen de la posibilidad ser configurados como clientes, al ser compatibles con OpenVPN.

"OpenVPN [10] es un producto de software creado por James Yonan en el año 2001 y que ha ido mejorando desde entonces. Ofrece una combinación de seguridad a nivel empresarial, facilidad de uso y riqueza de características".

OpenVPN utiliza protocolo de seguridad SSL/TLS para sus túneles, utiliza certificados como métodos de autentificación de clientes y permite la conexión de varios clientes al servidor.

Esta aplicación se adapta a la necesidad de la red y ofrece conexiones seguras extremo a extremo, dando la sensación de que los equipos se encontrarán en la misma red LAN. El software se instalará en el firewall que se encuentra en Barcelona, desde donde cumplirá la función de servidor.

Las VPN se usan generalmente para:

- Conexión entre diversos puntos de una organización a través de Internet.

- Conexiones de trabajadores domésticos o de campo con IP dinámicas.

- Soluciones extranet para clientes u organizaciones asociadas, con los cuales se necesita intercambiar cierta información en forma privada, pero que no se les debe dar acceso al resto de la red interna.

- Brinda una excelente fiabilidad en la comunicación de usuarios móviles, así como también al unir dos puntos distantes, como agencias de una empresa dentro de una sola red unificada.

OpenVPN ofrece dos formas de crear el túnel, VPN Bridging (TAP) y Routed (TUN). Ambas son funcionalmente muy similares. La principal diferencia es que una Routed VPN no pasará Broadcast IP VPN, mientras que una Bridged lo hará. Por este motivo, se utilizará la opción Routed TUN

Capa de implementación del túnel

OpenVPN puede establecer el túnel entre cliente y servidor en la capa 2 o en la capa 3 del modelo OSI. Si el túnel es en capa 2, se realiza la unión de la red local y la remota de modo que el encargado es un switch, es decir, se tendrá un mismo dominio de Broadcast y ambos segmentos pertenecerán a la misma red. En cambio, si el túnel se estableciera en la capa 3, los dos segmentos (local y remoto) pertenecerán a redes distintas y sólo viajará el protocolo IP.

Al realizar un túnel VPN entre cliente y servidor, en ambos extremos se crean sendas interfaces virtuales, que son las que logran vincular un equipo con el otro. Si el enlace es de nivel 2, las interfaces virtuales serán interfaces tap, es decir, interfaces virtuales Ethernet; si es de nivel 3, las interfaces virtuales serán tun, es decir, interfaces virtuales punto a punto que admiten paquetes ip.

Bridging vs. Routing

- Se utiliza TAP para transportar tráfico basado no IP.

- Se utiliza TUN para que los clientes LAN y VPN estén en el mismo dominio Broadcast.

	Ventajas	Inconvenientes
Modo TUN	• Una sobrecarga de tráfico inferior transporta sólo el tráfico que está destinado para el cliente VPN. • Transporta solamente los paquetes IP de capa 3.	• El tráfico Broadcast no se transporta normalmente. • Sólo se puede transportar IPv4 (OpenVPN 2.3 añade IPv6). • No puede ser utilizado en Bridges.
Modo TAP	• Se comporta como un adaptador de red real (excepto que es un adaptador de red virtual). • Puede transportar a cualquier protocolo de red (IPv4, IPv6, Netalk, IPX, etc.) • Trabaja en la capa 2, es decir, las tramas Ethernet son pasadas a través del túnel VPN. • Puede ser utilizado en Bridges.	• Consume muchos recursos de difusión en el túnel VPN. • Agrega la sobrecarga de las cabeceras de Ethernet en todos los paquetes transportados por el túnel VPN. • Redimensiona. • No se puede utilizar con dispositivos Android o IOS.

Figura 21.Modo TUN/TAP

Seguridad en VPN

OpenVPN tiene dos modos de autenticación:

- Clave estática – Utiliza una clave estática pre-compartida.
- TLS - Utiliza SSL/TLS certificados para la autenticación y el intercambio de claves.

C**lave estática**: se genera una clave pre-compartida y compartida entre los dos pares de OpenVPN antes de que se inicie el túnel. Esta clave estática contiene 4 claves independientes:

- HMAC enviar
- HMAC recibir
- cifrar
- descifrar

Por defecto, en el modo de clave estática ambos anfitriones utilizan la misma clave HMAC y la misma clave de cifrar/descifrar.

- **HMAC**

Un MAC (Message Authentication Code) es una porción de información utilizada para autenticar un mensaje. Si hay dos extremos, A y B, que comparten una única clave secreta, la combinación de esta clave de longitud fija y el mensaje de longitud arbitraria da como resultado un código MAC de longitud fija.

De esta manera, A envía el mensaje en claro y el mensaje MAC a B. Con esto, el receptor B garantiza la integridad y autenticación porque utilizará la clave secreta para descifrar el mensaje.

Por otro lado, las funciones Hash (MD5, SHA-1) no han sido diseñadas para la autentificación dado que carecen de clave secreta. No obstante, son interesantes puesto que su velocidad es mayor que muchas encriptaciones de bloque, su código fuente es abierto y sus propiedades y funcionamiento son muy conocidos.

La RFC 2104 propone el uso de una autenticación en entornos seguros, como SSL, mediante una operación MAC en la que intervenga una función hash, su nombre es HMAC.

HMAC utiliza la función de hash y clave secreta para su implementación. Esto ofrece menos vulnerabilidad que solo encriptación o hash.

Cuando ambos lados usan la misma clave para cifrar y descifrar los datos, se está utilizando el mecanismo conocido como “clave simétrica” y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN.

Cualquiera que posea la clave podrá descifrar el tráfico, por lo que si un atacante la obtuviese comprometería el tráfico completo de la organización, ya que tomaría parte como un integrante más de la VPN.

Modo SSL/TLS: una sesión SSL se establece con la autenticación bidireccional (cada lado de la conexión debe presentar su propio certificado). Si la autenticación SSL/TLS tiene éxito, el cifrado/descifrado y el material fuente clave HMAC se generan entonces al azar por la función RAND_bytes de OpenSSL y se intercambian a través de la conexión SSL/TLS.

SSL/TLS usa una de las mejores tecnologías de cifrado para asegurar la identidad de los integrantes de la VPN. Cada integrante tiene dos claves, una pública y otra privada

La clave pública es distribuida y usada por cualquiera para cifrar los datos que serán enviados a la contraparte, quien conoce la clave privada que es imprescindible para descifrar los datos.

El par de clave pública/privada es generado a partir de algoritmos matemáticos que aseguran que solo con la clave privada es posible leer los datos originales.

Si se encontrase un modo de quebrar la seguridad que estos algoritmos proporcionan, todas las conexiones cuya integridad depende de ellos se verían potencialmente comprometidas

Es de destacar que la clave privada debe permanecer secreta, mientras que la clave pública debe ser intercambiada para que nos puedan enviar mensajes.

Las bibliotecas SSL/TLS son parte del software OpenSSL que viene instalado en cualquier sistema moderno e implementa mecanismos de cifrado y autenticación basados en certificados.

Los certificados generalmente son emitidos por entidades de reconocida confiabilidad, aunque también podemos emitirlos nosotros mismos y usarlos en nuestra propia VPN. Con un certificado firmado, el dueño del mismo es capaz de demostrar su identidad a todos aquellos que confíen en la autoridad certificadora que lo emitió.

Configuración del servidor OpenVPN sobre Linux principales parámetros

Se utilizará la opción de Ruting (TUN) para la configuración del servidor VPN. Esta opción trabaja en capa 3, como ya se explica anteriormente, y es totalmente compatible con el modelo de Router escogido para realizar la función de cliente. Otra de las ventajas que proporciona este modo de trabajo es la no sobrecarga en el túnel con tráfico innecesario.

En el aspecto de seguridad, el modo SSL/TLS obliga a cifrar las comunicaciones siendo necesaria la creación de una autoridad certificadora. También, se deberán crear certificados para cada uno de los clientes que se quieran conectar al servidor a través del túnel.

El servidor OpenVPN está instalado sobre un sistema operativo CentOS 6.7 x86_64. Se realiza la instalación de las librerías necesarias mediante las siguientes líneas de comandos en el terminal.

```
cd /home/
mkdir openvpn
cd openvpn/

yum install epel-release bison bison-devel ncurses-devel zlib-devel opensslels
op

wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm

wget http://openvpn.net/release/lzo-1.08.rf.src.rpm

wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-
2.el5.rf.i386.rpm

rpmbuild –rebuild lzo-1.08-4-rf-src-rpm

rpm –Uvh lzo-*.rpm

rpm –Uvh rpmforge-release*
```

Una vez instaladas las librerías, se prosigue a instalar el servidor OpenVPN. El primer paso a realizar es la creación de una autoridad certificadora que es la que posibilita la emisión y revocación de certificados.

Se dispondrá de un certificado raíz ca.ctr y una clave ca.key para poder crear y firmar las claves de los clientes y del servidor. Para realizar este paso, y el resto de pasos, se ejecutarán los scripts que OpenVPN trae incorporados de serie. Se crea una carpeta con nombre **easy-rsa** dentro de la ubicación **/etc/openvpn**.

yum install openvpn

wget https://github.com/downloads/Openvpn/easy-rsa/easy-rsa-2.2.0_master.tar.gz

tar –zxvf easy-rsa-2.2.0_master.tar.gz

cp –R easy-rsa-2.2.0_master/easy-rsa/ /etc/openvpn

cd /etc/openvpn/easy-rsa/2.0

chmod 755*

Se debe modificar una serie de parámetros en el fichero **vars** antes de ejecutar los scrips. En el terminal se ingresa el comando **nano vars**.

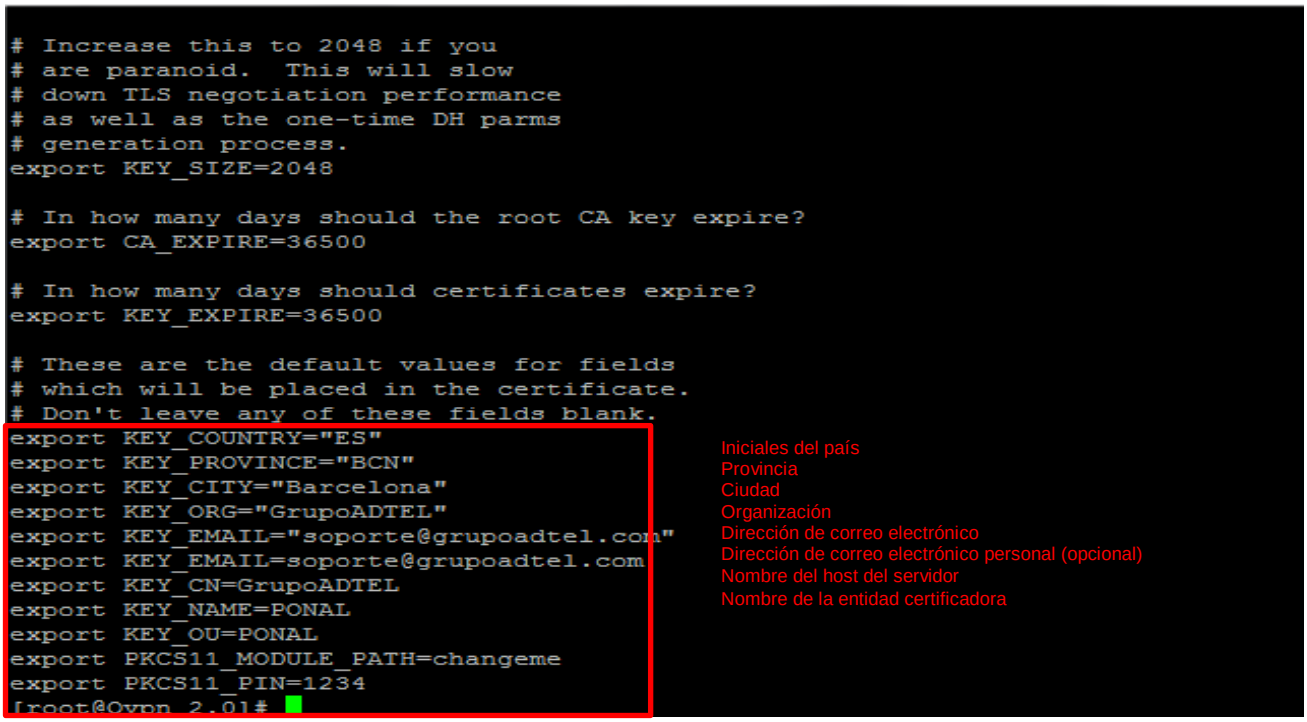
Una vez abierto el editor de texto, se deberá localizar y modificar las siguientes líneas.

export_KEY_SIZE=1024

Una vez encontrada, la sustituyen por la siguiente línea:

export_KEY_SIZE=2048

Con esta modificación se incrementa el tamaño de las claves privadas (.key) que se generan. Se incrementa también el parámetro de Diffie Hellman y las claves de 1024 bits a 2048 bits. Este parámetro no tiene porqué penalizar en exceso el rendimiento del servidor. Únicamente penalizará el proceso autentificación Handshake de SSL/TLS. Se ingresan los datos de la entidad emisora de los certificados.



Una vez modificados los campos del archivo **vars,** se salvan los cambios realizados. Luego se exportan sus variables con el siguiente comando.

- source ./vars

El script clean-all borrará la totalidad de claves que podrían existir en la ubicación **/etc/openvpn/easy-rsa/keys**.

- ./clean-all

Con el siguiente comando se generan los paramentos Diffie Hellman, que se utilizarán para poder intercambiar de manera segura las claves entre cliente y servidor.

- ./build-dh

Por último, se creará el certificado y la calve privada de la autoridad certificadora con el siguiente comando.

- ./build-ca

Se realizarán una serie de preguntas durante el proceso de creación, a las cuales se aceptará el valor por defecto.

Al terminar el proceso dentro de la ubicación **/etc/openvpn/easy-rsa/keys** se ha creado **ca.crt** y **ca.key**:

- **ca.crt:** Es el certificado raíz público de la autoridad de certificación (CA)

- **ca.key:** Este fichero contiene la clave privada de la autoridad de certificación (CA). Este archivo debe mantenerse protegido y no debe estar al alcance de terceros.

Ahora es turno de crear el certificado y la clave del servidor. Se introduce el siguiente comando en la terminal:

- ./build-key-server server

Se realizarán una serie de preguntas durante el proceso de creación a las cuales se aceptará el valor por defecto.

Al finalizar el proceso dentro de la ubicación **/etc/openvpn/easy-rsa/keys,** se habrán creado los siguientes archivos:

server.key: Fichero que contiene la clave privada del servidor.

server.crt: Fichero corresponde al certificado público del servidor.

server.csr: Este archivo es la petición de certificado que se envía a la autoridad de certificación. Mediante la información que contiene el archivo .csr, la autoridad de certificación podrá realizar el certificado del servidor una vez hayan realizado las comprobaciones de seguridad pertinentes.

A continuación, se crean los certificados y las claves de los clientes que se podrán conectar al servidor VPN. Se tiene que teclear el siguiente comando en la terminal:

- ./build-key grupoadtel.[nombre de usuario]
  Ejemplo: ./build-key grupoadtel.arauca

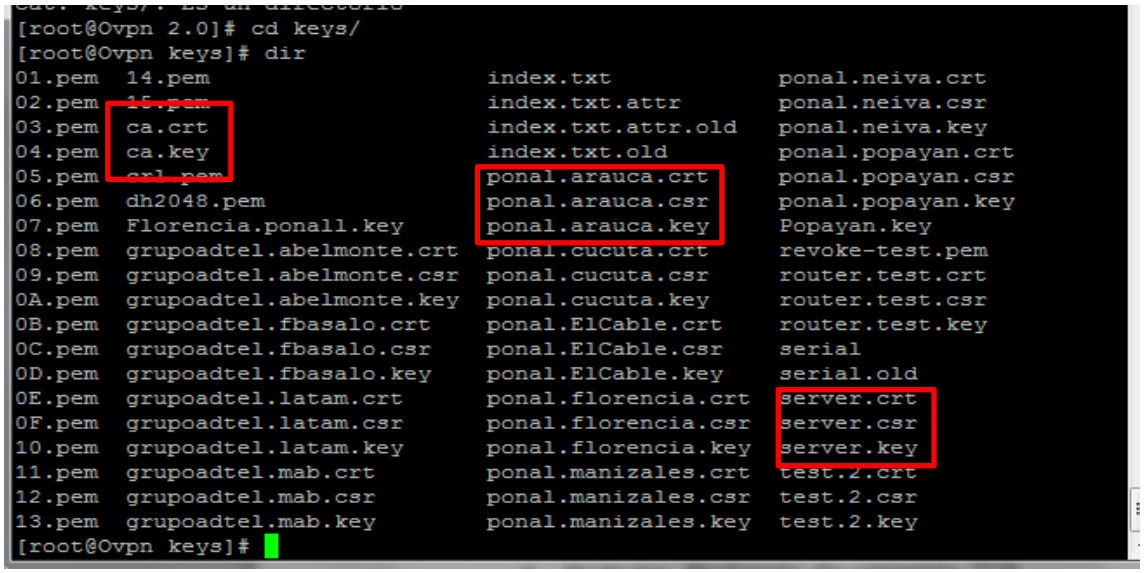
Se realizarán una serie de preguntas durante el proceso de creación a las cuales se aceptara el valor por defecto.

Al finalizar el proceso dentro de la ubicación /etc/openvpn/easy-rsa/keys se habrán creado los siguientes archivos:

[nombre de usuario].key: Fichero que contiene la clave privada del servidor.

[nombre de usrario].crt: Fichero corresponde al certificado público del servidor.

[nombre de usuario].csr: Este archivo es la petición de certificado que se envía a la autoridad de certificación. Mediante la información que contiene el archivo .csr, la autoridad de certificación podrá realizar el certificado del servidor una vez hayan realizado las comprobaciones de seguridad pertinentes.



Para realizar la configuración del servidor, existen ficheros de ejemplo que se pueden utilizar y que se encuentran disponibles en la siguiente ubicación.

/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz

Se copia el ejemplo de un archivo de configuración.

- Cp –R /usr/share/doc/openvpn-2.3.8/sample/sample-config-files/server.conf /etc/openvpn/

Y después se accede a la ubicación en donde se ha copiado.

- cd /etc/openvpn/

Se abre el archivo mediante un editor de texto para su configuración. Los parámetros a modificar se marcan en rojo.

- nano server.conf

```
#################################################
#                                               #
#        Configuración OpenVPN para PONAL       #
#                                               #
#                - Creado:        GrupoADTEL     #
#                - Version:       1              #
#                - Fecha:         29/09/2015     #
#                                               #
#################################################


# Port OpenVPN

port 1194

# TCP or UDP server?

proto tcp
;proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.

;dev tap
dev tun

# root certificate (ca), certificate(cert), and private key (key)
```

port 1194, TCP/UDP de escucha del servicio.

Proto tcp, Protocolo de conexión TCP.

dev tun, dispositivo virtual en que se creara el túnel

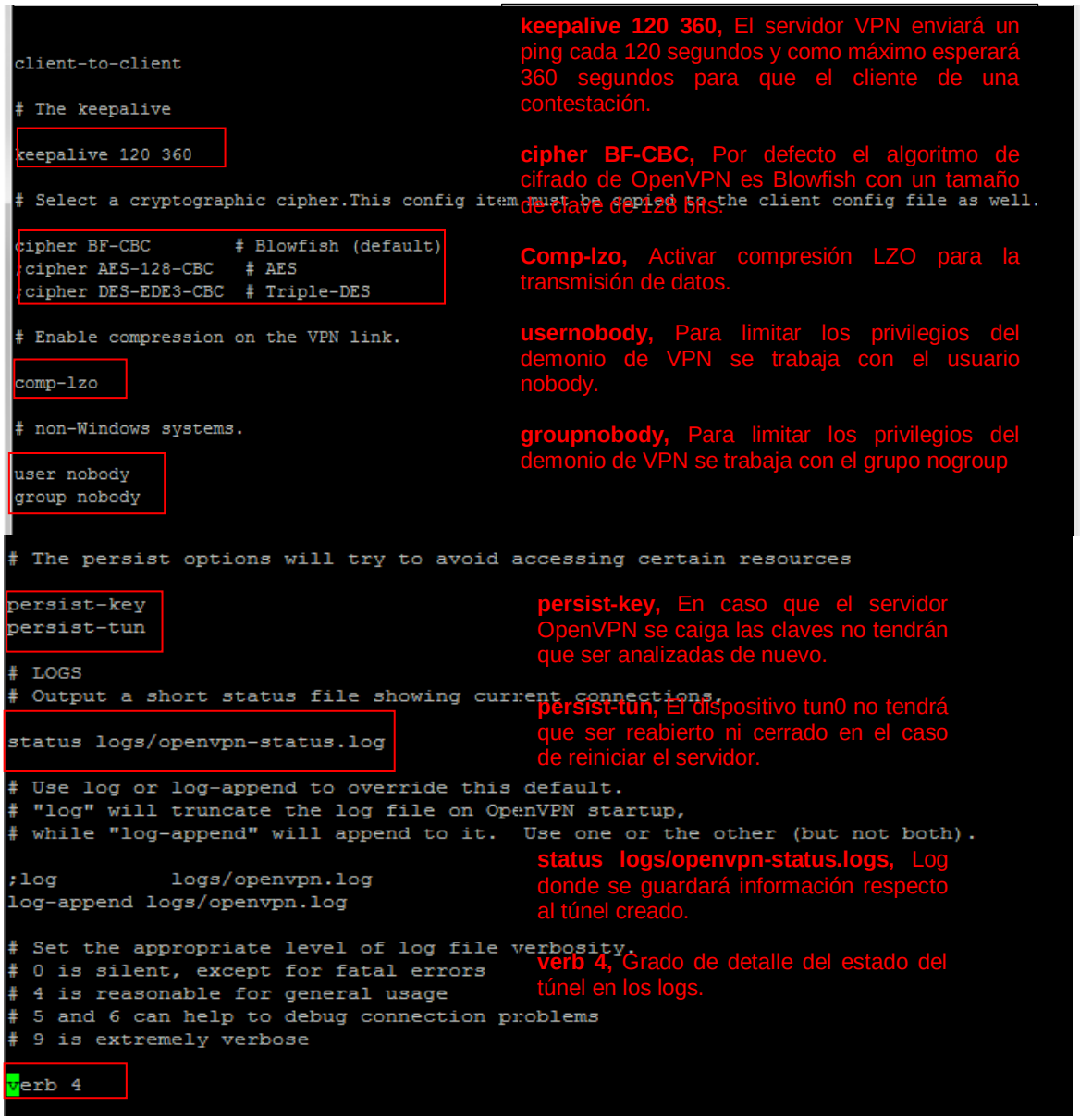
```
ca easy-rsa/2.0/keys/ca.crt
cert easy-rsa/2.0/keys/server.crt
key easy-rsa/2.0/keys/server.key

#Diffie hellman parameters.

dh easy-rsa/2.0/keys/dh2048.pem

# VPN subnet for OpenVPN

server 172.29.90.0 255.255.255.0

# Si queremos mantener las IP proporcionadas dentro de la VPN

;ifconfig-pool-persist ipp.txt

# Push routes to the client to allow it to reach other private subnets behind the server.

push "route 172.17.0.0 255.255.255.0"
route 172.17.0.0 255.255.255.0

# Router ponal.arauca
push "route 172.17.1.0 255.255.255.0"
route 172.17.1.0 255.255.255.0

# Router ponal.barranquilla
push "route 172.17.2.0 255.255.255.0"
route 172.17.2.0 255.255.255.0

# Router ponal.ElCable
push "route 172.17.3.0 255.255.255.0"
route 172.17.3.0 255.255.255.0

# Router ponal.cartagena
push "route 172.17.5.0 255.255.255.0"
route 172.17.5.0 255.255.255.0

# Router ponal.cucuta
push "route 172.17.6.0 255.255.255.0"
route 172.17.6.0 255.255.255.0


# Router ponal.florencia
push "route 172.17.7.0 255.255.255.0"
route 172.17.7.0 255.255.255.0
```

ca.crt, Certificado de la autoridad certificadora que se ha generado.
server.crt, Certificado del servidor que se ha creado.
server.key, Clave privada del servidor que se ha generado.
dh2048.pem, Carga de los parámetros de Diffie Hellman.
server 172.29.90.0 255.255.255.0, Se indica que a los clientes del VPN se les asignará IP del tipo 172.29.90.0/24

ifconfig-pool-persist ipp.txt, Se crea un fichero ipp.txt en el que se registran las IP de los clientes que se conectan al servidor VPN.

push "route 172.17.0.0 255.255.255.0", Con esta línea se consigue que los paquetes que tengan como destino la red

172.17.0.0 viajen por la interfaz del túnel (tun0). De esta forma el cliente VPN se podrá comunicar con cualquier máquina de la red 172.17.0.0



Cuando el servidor OpenVPN reciba las peticiones de los clientes, se deberán enrutar adecuadamente, y además se deberá configurar el firewall para que permita el tráfico a través del túnel que se ha creado ente el cliente y el servidor.

- iptables –I INPUT –p tcp –m tcp –dport 1194 –j ACCEPT
- iptables –I INPUT –p tcp –m udp –dport 1194 –j ACCEPT
- service iptables save
- Check:
- Iptables –L

Se deberá habilitar el IP Forwaring mediante el editor de texto.

- nano /etc/sysctl.conf

Se modificará la siguiente línea que se encuentra comentada.

- sysctl –w net.ipv4.ip_forward=1

Guardar y Ejecutar

Una vez habilitado IP Forwaring, se ha de permitir el tráfico por el túnel VPN mediante nano /etc/rc.local

- iptables –A FORWARD –o eth0 –j ACCEPT
- iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
- service iptables save

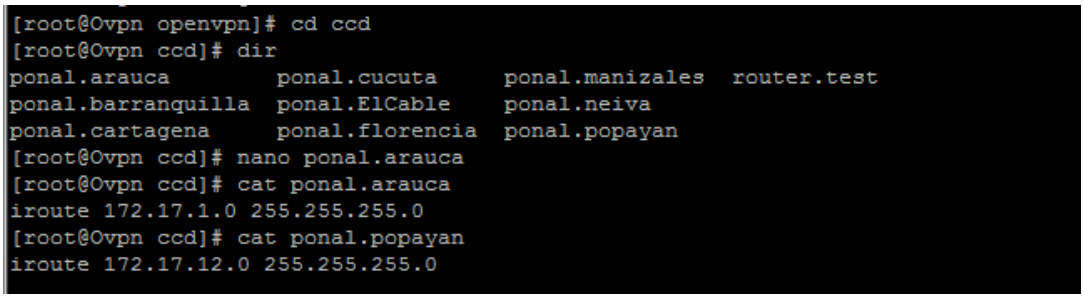
Y ya se tendrá el servidor configurado.

Para que finalmente se pueda tener acceso a la red de detrás del los routers, se deberá crear en el directorio ccd, un archivo para cada router.

- nano ponal.arauca
- iroute 172.17.1.0 255.255.255.0

Se establece la red de cada router.

En el archivo ccd muestra las rutas de cada cliente.



Configuración de cliente en PC con Windows

Se debe descargar e instalar el cliente para Windows de OpenVPN. El software se puede descargar desde la página:
https://openvpn.net/index.php/open-source/downloads.html

Después de instalarlo, hay que dirigirse al directorio de instalación donde se encuentrabel directorio “sample-config”. Una vez dentro, seleccionar el archivo “client.ovpn” y copiar. Salir de este directorio, buscar el directorio “config” y pegar el archivo anteriormente copiado. A continuación, se debe editar este archivo. Se editarán parámetros como los certificados y la dirección del servidor.

ca.crt: Certificado de la autoridad certificadora
grupoadtel.fbasalo.crt: Certificado del cliente

grupoadtel.fbasalo.key: Parte privada del certificado del cliente (clave)
client

dev tun200
proto tcp
;proto udp
remote ponalvpn.grupoadtel.com 1194
resolv-retry infinite
nobind

persist-key
persist-tun

ca ca.crt
cert grupoadtel.fbasalo.crt
key grupoadtel.fbasalo.key

ns-cert-type server
comp-lzo
verb 3

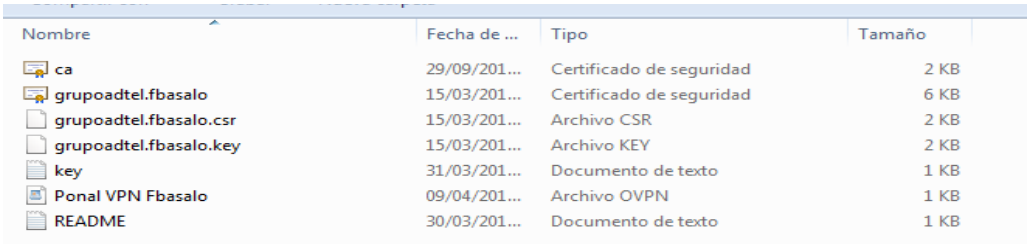
En dicha configuración se ajustan adecuadamente las siguientes opciones:

remote: Indica el servidor al que conectar y el puerto que sea, por defecto el 1194

cert: Indica el certificado del cliente

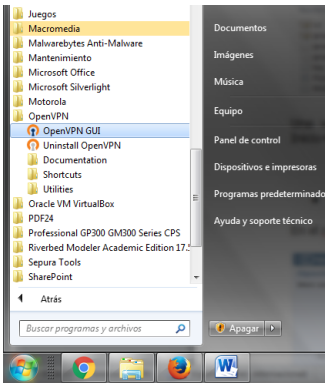
key: Indica la clave privada del cliente

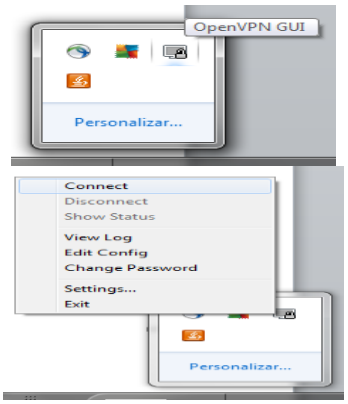
Certificados de configuración de OpenVPN GUI



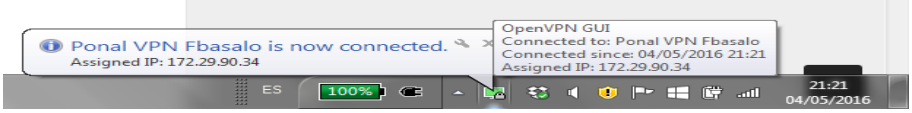
Nombre	Fecha de ...	Tipo	Tamaño
ca	29/09/201...	Certificado de seguridad	2 KB
grupoadtel.fbasalo	15/03/201...	Certificado de seguridad	6 KB
grupoadtel.fbasalo.csr	15/03/201...	Archivo CSR	2 KB
grupoadtel.fbasalo.key	15/03/201...	Archivo KEY	2 KB
key	31/03/201...	Documento de texto	1 KB
Ponal VPN Fbasalo	09/04/201...	Archivo OVPN	1 KB
README	30/03/201...	Documento de texto	1 KB

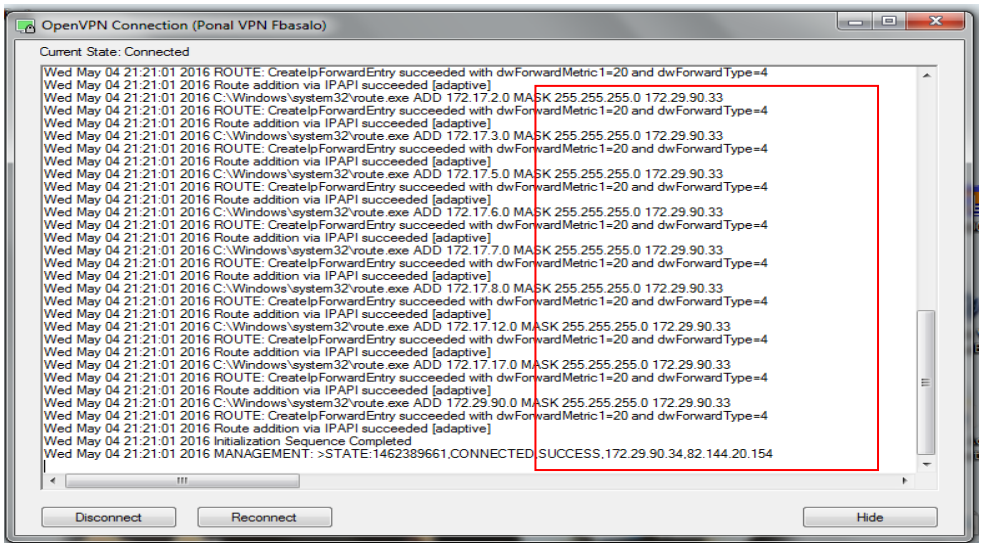
Una vez realizados estos pasos de puede comprobar la conexión del cliente, desde Inicio→ Todos los programas → OpenVPN→OPenVPN GUI
Sobre el Icono de OpenVPN GUI click derecho y Connect





Establecimiento de la conexión:





La opción de Show Status muestra las direcciones IP de las redes a la cuales se tiene acceso y en la última línea muestra que el estado es CONNECTED y la dirección IP asignada al cliente

4. Diseño de la solución de gestión

4.1. Introducción

Los sistemas de supervisión/gestión se encuentran cada vez más presentes en la vida cotidiana. Su uso se extiende desde el control de las instalaciones de una vivienda (como las luces, caldera, apertura y cierre de puertas), hasta la gestión en grandes industrias de cadenas de montajes.

Estos tipos de sistemas, que se utilizan comúnmente en la industria y en las viviendas, son sistemas de Telecontrol que funcionan mediante sensores que envían señales eléctricas a estaciones remotas. Las comunicaciones entre los sensores y la estación remota local se realizan mediante el protocolo RS485.

El protocolo RS485 es un sistema de bus que llega a buenas velocidades de transmisión para distancias cortas (hasta 500mts a 125kbps) y es utilizado para controlar remotamente sistemas de iluminación, por ejemplo, pero siempre desde la misma red LAN.

Cuando es necesario realizar un control remoto (exterior de la red LAN), se necesita un conversor que encapsule el protocolo RS485 en tramas Ethernet TCP/IP, para que estas puedan viajar normalmente a través de un modem GSM o Adsl.

El protocolo SNMP (Simple Network Managment Protocol) es una herramienta de gestión que trabajar sobre TCP/IP. Su uso se estandarizó a principio de los 90 y actualmente se utiliza universalmente en todo tipo de redes.

La arquitectura básica de una red basada en SNMP está compuesta por:

- **Una estación de gestión:** serán aplicaciones para el análisis de datos, interfaz de usuario, control de los elementos remotos y base de datos con información de las MIBs.
- **Agentes de gestión:** tendrán una MIB local y atenderán solicitudes de la estación de gestión.
- **Base de información de gestión (MIB):** la MIB local de cada agente mantiene información sobre objetos del recurso que gestiona. Cada tipo de objeto dispone de un identificador único que sirve para nombrarlo. Además, cada valor que se asocian al identificador es jerárquico, en consecuencia estos identificadores dan forma de árbol a la estructura MIB.

Los agentes SNMP, instalados en los transmisores FM, tienen un MIB. En la figura 22 se muestra su estructura de árbol y el Objet ID asociado a la petición

SET de potencia directa (ControlSetFotwardPower). Se denomina “potencia directa” a la potencia en Watts que es entregada a la antena por el transmisor de FM y a través del SET se le indica al transmisor la potencia que debe transmitir.

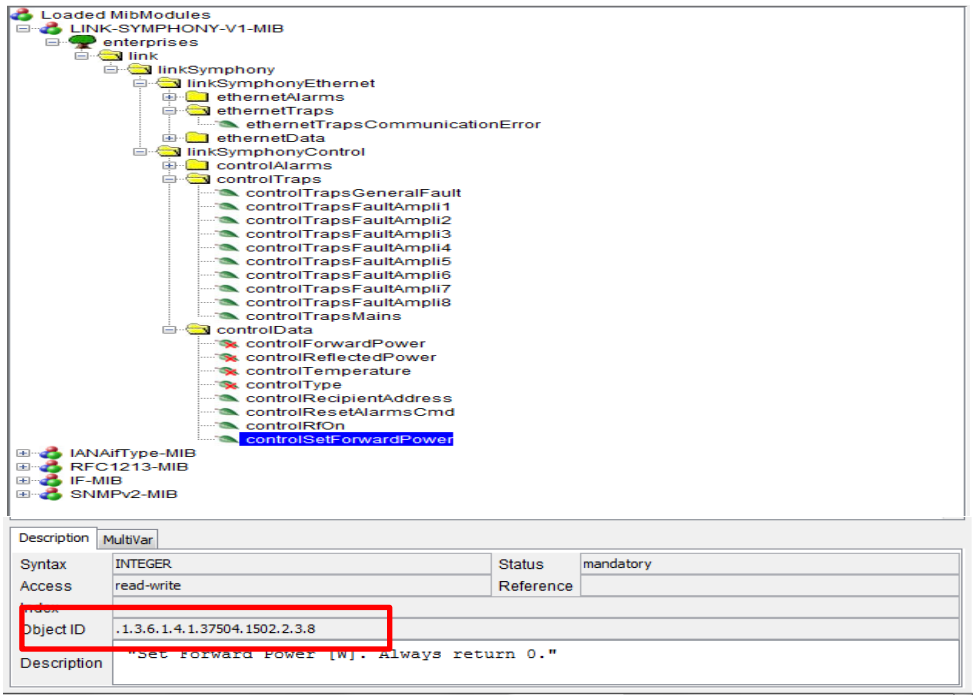


Figura 22. Árbol MIB transmisor FM

Protocolo de gestión de red (SNMP): es el encargado de enlazar la estación de gestión con los agentes mediante tres tipos de peticiones.

- GET: permite la obtención de valores de los agentes a la estación gestora.
- SET: permite modificar valores del agente a la estación gestora.
- TRAP: permite a un agente enviar una notificación de manera asíncrona a la estación gestora.

El protocolo SNMP opera en la capa de aplicación, ignorando el hardware sobre el que trabaja, ya que utiliza el protocolo de transporte TCP/IP. La gestión se lleva acabo de nivel IP, por lo que se puede controlar dispositivos que estén conectados a Internet y no únicamente a los que estén en su red local. En la figura 23 se muestra el entorno de gestión por niveles.

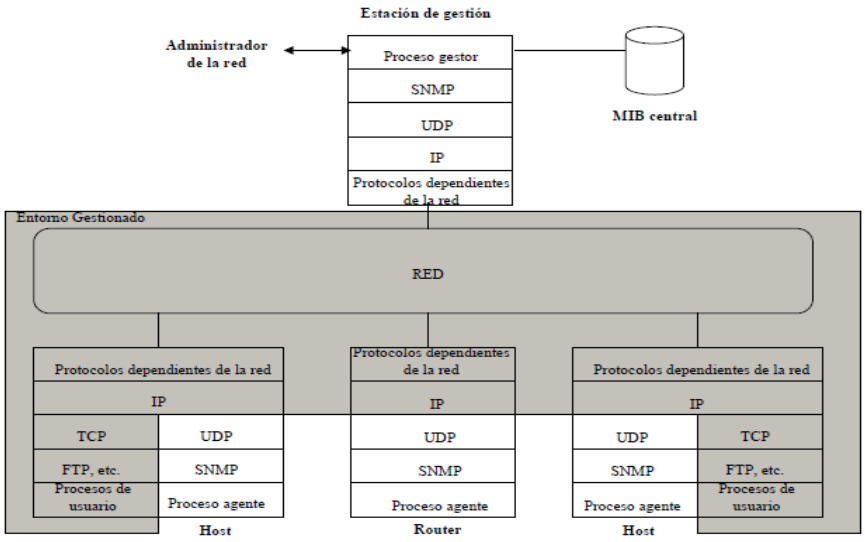


Figura 23. Entorno de Gestión

4.2. Transmisores FM

Introducción

El Transmisor de FM JR 6kW trabaja en la Banda II de la FM, con el rango de frecuencias de 87,5 a 108 MHz y con el modo de Modulación en Frecuencia FM. Es capaz de entregar hasta 6 kW de potencia de RF en la salida.

Composición Mecánica y Diseño

El Transmisor está compuesto por un bastidor principal que alberga los siguientes componentes:

- 1 Excitador ADVANCAST 30 DDS – Excitador FM de 30 W (principal).
- 1 Excitador ADVANCAST 30 DDS – Excitador FM de 30 W (reserva) .
- 1 Changeover ACOM-150 – Unidad de cambio automático de excitadores.
- Amplificadores FM ADVANCAST 2 kW – Módulo amplificador de 2.000 W.
- Combinador ADVANCAST PDC03/6K – Módulo Combinador de 3 vías para 6 kW.
- 1 A.C. unit. – Unidad de distribución de alimentación de Red.

La estructura modular del equipo Transmisor de FM, de la serie Advancast, permite el fácil y rápido servicio del equipo, reduciendo los tiempos de mantenimiento y permitiendo la total actuación del técnico sin interrupciones, con tan solo una simple degradación de la potencia.

Vista Frontal Vista Posterior

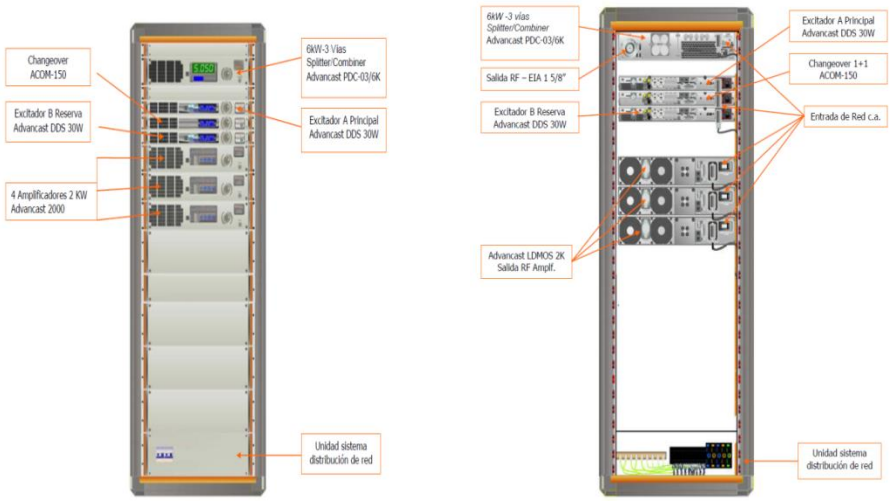


Figura 24.Transmisor FM Link serie Advancast

Lógica de Control

La placa del micro-controlador controla todo el transmisor en modo Master y administra todos los módulos amplificadores. Sus principales funciones son:

- Adquirir y mostrar todos los parámetros de trabajo (potencia de salida de RF, directa y reflejada, potencia de RF en resistencias de equilibrio, temperatura, etc.).

- Adquirir y mostrar el estado de las alarmas (excesivo ROE, sobre temperatura, ventiladores, etc.).

- Paro de la RF.

- Comunicación vía red RS485 con los otros equipos.

- Supervisión (contactos) también web-server y/o SNMP.

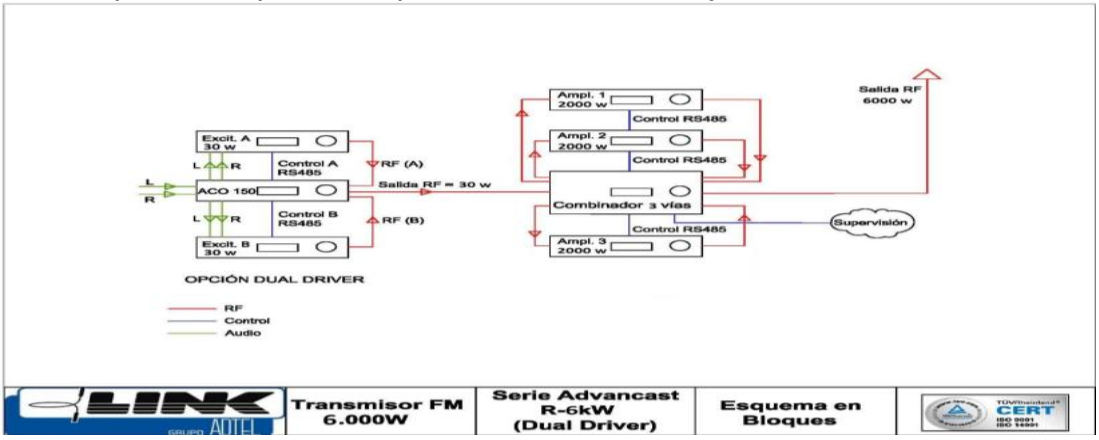


Figura 25.Esquema en Bloques ADVANCAST JR 6KW

4.3. Herramienta NMS (Network Management System)

El uso de una herramienta de monitorización tiene como objetivo disponer de un informe continúo del estado de la red y de los elementos que la componen. De esta forma, se tiene un control de manera remota que facilita el mantenimiento y ahorra en coste de recursos.

Hay herramientas NMS de código abierto que son las encargadas de realizar la monitorización del sistema, enviando periódicamente peticiones a los agentes remotos. En caso de que alguno de los valores devueltos no cumplieran con los mínimos requeridos, la herramienta genera alertas que son enviadas por correo electrónico a los responsables de la infraestructura que se está gestionando.

En el mercado actual existen herramientas de software libre (OpenSource) que ofrecen muy buenas prestaciones, como por ejemplo Nagios, Zabbix, Pandora FMS, etc. Software abierto significa que son de distribución libre y generalmente gratuita, aunque no siempre esto último es así. Su principal ventaja es su bajo coste de adquisición y la innovación y corrección de errores por parte de cualquier usuario.

Nagios [14]**:** es una de las herramientas de código abierto más utilizadas. Dispone de interfaz web y soporta gran cantidad de host.

Algunas de sus características son:

- Permite definir políticas de notificaciones según contactos, listas de contactos; dispositivos y grupos de dispositivos; servicios y grupo de servicios.
- Los usuarios pueden realizar comentarios sobre eventos
- Estadísticas de disponibilidad.
- Permite diferentes métodos de notificación (SMS, e-mail, audio, etc.).
- Definir niveles de escalado de notificaciones.
- Permite diferenciar entre host caídos e inaccesibles.

Como inconveniente, podemos presentar que la instalación, configuración y los complementos (pugins) se basa en código, lo cual implica una dificultad media si no se tiene un cierto grado de conocimiento.

Pandora FMS [15]**:** es una herramienta de código abierto que se distribuye bajo licencia GPL v2. También dispone de una licencia comercial Pandora FMS Enterprise que proporciona numerosas características adicionales. Esta aplicación es usada para vigilar y analizar de forma visual todo tipo de sistemas utilizando un entorno web.

Algunas de sus características son:

- Reconocimiento automático del mapa de red.
- Diferentes tipos de usuario según nivel de acceso.
- Control total con interfaz web.
- Mide rendimientos, compara valores y establece límites sobre lindantes.
- Soporta SNMP.
- Notificación mediante correo electrónico o SMS.
- Gracias a la base de datos (MySQL), genera gráficas y estadísticas.
- La versión comercial genera informes que pueden ser enviados a un correo electrónico determinado.

El inconveniente de esta herramienta es que hay opciones interesantes, como gestión remota de agentes o envío de informes por correo electrónico, que solo se encuentran disponibles en la versión comercial.

Zabbix [8]**:** se distribuye bajo licencia GPLv2. Es una herramienta que permite monitorizar el estado de una red y realizar controles simples que comprueben la disponibilidad del servicio o más complejos mediante la instalación de agentes.

Algunas de sus características son:

- Permite monitorizar dispositivos SNMP.
- Las notificaciones o alertas permiten configurar nivel de escalado, se pueden enviar alertas por correo electrónico y SMS.
- Interfaz basada en web control total.
- Permite la personalización de la interfaz gráfica (Mapas).
- Detección automática de dispositivos de red.

Las diferencias entre estas herramientas, en lo que a aspectos técnicos se refiere, son casi inexistentes, ya que las características de cada una son muy similares entre sí.

Tabla comparativa

	Nagios	*Zabbix*	*Pandora FMS*
Graficas	✓ Si	✓ Si	✓ Si
Informes	✓ Si	✓ Si	✗ Bajo GPL comercial
Estadísticas	✓ Si	✓ Si	✓ Si
Autodescubrimiento	✓ Si	✓ Si	✓ Si
SNMP	✗ Necesario plugin	✓ Si	✓ Si
Agentes	✓ Si	✓ Si	✓ Si
Alertas	✓ Vía e-mail y SMS	✓ Vía e-mail y SMS	✓ Vía e-mail y SMS
Aplicación web	✓ Solo visualización	✓ Control total	✓ Control total
Licencia	✓ GPL v2	✓ GPL v2	✗ GPL v2 más GPL comercial
Mapas	✗ Necesario instalar frotend	✓ Permite personalización	✓ Permite personalización

Información recopilada de [14]; [15]; [8]

En la elección del sistema de monitorización, uno de los principales requerimientos que se buscan en el aplicativo es la posibilidad de personalizar del entorno visual, para dar una imagen de marca. Desde el punto de vista comercial, se pretende integrar esta solución de monitorado como un servicio adicional vendible a futuros clientes, junto con la venta de los transmisores de FM.

Por eso es relevante poder personalizar al máximo el sistema. De todas las soluciones antes mencionadas, Zabbix es la que posibilita mayor grado de personalización, permite la integración de logos, el desarrollo de “screens” y “mapas” personalizados, y una serie de características adicionales en este sentido.

El proyectista ha realizado un estudio sobre campo captando el grado de satisfacción de los diferentes clientes que disponen de sistemas NMS. En todos los casos en que en los clientes disponían de Zabbix, todos han mostrado su acuerdo en que es una herramienta fiable, estable, y muy escalable. Esta transferencia de satisfacción también ha supuesto un parámetro de decisión a la hora de escoger esta herramienta.

4.4. Zabbix

"Zabbix es una solución de monitorización de código abierto que fue creado por Alexei Vladishev. Supervisa numerosos parámetros de una red y utiliza mecanismos de notificación que permite a los usuarios configurar alertas en función de correo electrónico para prácticamente cualquier evento. A la configuración de parámetros se accede mediante una interfaz web." [8]

El funcionamiento de servidor con base Zabbix se divide en tres funciones que son:

- Servidor Zabbix
- Interfaz web
- Almacenamiento de base de datos

El servidor Zabbix [9] es el que se encarga de realizar la captura de datos (traps). Tiene en cuenta los disparadores (Triggers) y envía las notificaciones a los usuarios. En el servidor se encuentra la configuración y se almacenan los datos estadísticos.

4.4.1. Requisitos Zabbix

Zabbix necesita unos mínimos requisitos de Hardware para funcionar, estos vienen especificados en la documentación que se encuentra en su página web. Recomienda que al menos se disponga de 128MB de memoria física y 256MB de espacio libre en el disco. Aunque la cantidad de espacio requerido depende de los dispositivos a monitorizar.

En su página [8] se encuentra la siguiente tabla, que especifica los requisitos en función de la cantidad de host que ha de tener una máquina para funcionar como servidor Zabbix.

Tamaño de la red	*Plataforma*	*CPU/Memoria*	*Base de datos*	*Num. Host*
Pequeña	Ubuntu Linux	PII 3500Mhz 256MB	MySQL MyISAM	20
Media	Ubuntu Linux	AMD Athlon 3200 +2G	MySQL InnoDB	500
Grande	Ubuntu Linux	Intel Dual Core6400 4GB	RAID10 MySQL InnoDB or PostgraeSQL	>1000
Muy Grande	RedHat Enterprise	Intel Xeon 2xCPU 8GB	FASTRAID10 MySQL InnoDB or PostgraeSQL	>10000

Como plataforma de apoyo, Zabbix recomienda UNIX como sistema operativo debido a la estabilidad, tolerancia a los fallos y capacidad de recuperación. Teniendo en cuenta el tamaño de la red se instalado Zabbix sobre un procesador AMD Athlon 64 X2 6400 con sistema operativo Ubuntu 14.04 LTS (64bits).

4.4.2. Configuración web Zabbix

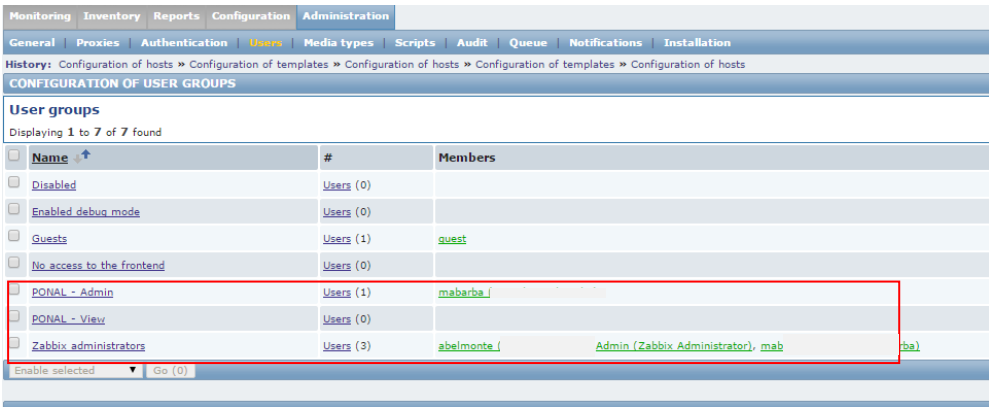
La administración de todas las tareas de monitorización se realiza desde el panel frontal, este es una interfaz web que permite gestionar las actividades de monitorización, se pueden agregar dispositivos, configurar todas las opciones del Zabbix, generar reportes, graficas, alarmas y crear cuentas.

Zabbix [9] ofrece la posibilidad de crear varios perfiles de usuarios agrupados que tendrán distintos tipos de permisos. Inicialmente, hay dos usuarios creados por defecto: el usuario “Admin” (que consta con permisos de lectura/escritura) y el usuario “Invitado” (que solo tiene permiso de lectura).

Para este proyecto, se han definido tres grupos de usuarios con diferentes permisos según su función (Administradores, Operadores y Operarios de mantenimiento).

- Zabbix Administrators: Dispone de permisos R/W sobre el host Zabbix.
- PONAL – Admin: Dispone de permisos R/W de los hosts de PONAL.
- PONAL – View: Dispone de permiso de R de los hosts de PONAL.

En la pestaña Administration → Users; es posible ver los grupos y a su izquierda en verde los usuarios que pertenecen a ese grupo.

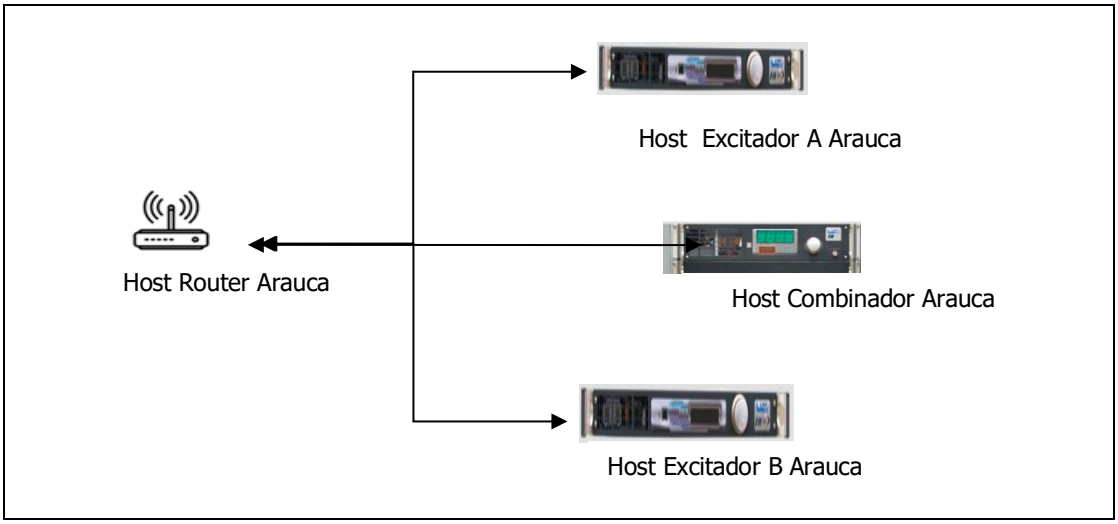


Zabbix tiene la opción de crear distintos “host” (dispositivo) para después poder agruparlos y conformar un “host group” (grupo de dispositivos).

Teniendo en cuenta esto, se ha decidido que el grupo de dispositivos del emplazamiento de Arauca conformen un host group -por ejemplo- y así sucesivamente con todos los emplazamientos. Se ha decidido también, realizar la agrupación de todos los transmisores FM por potencias (host group 6KW, host group 8KW), los Routers se agruparán en el grupo Teltonika y también un grupo para los Excitadores.

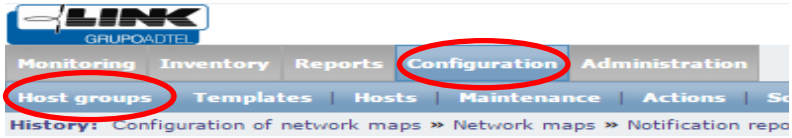
Además, mediante la inserción de un mapa de Colombia y la configuración de distinto iconos distribuidos sobre el mapa se ha personalizado la pantalla (screen). Cada icono representa un emplazamiento o host group y a través de un click el usuario podrá acceder a los distintos host que lo conforman.

Host Group Arauca



- **Crear un Host Group**

Una vez en la interfaz web, para crear un grupo de host se ha de dirigir a la pestaña Configuration y posteriormente Host Groups. Luego, realizar click en Create Group e ingresar los parámetros identificativos del grupo (Nombre)

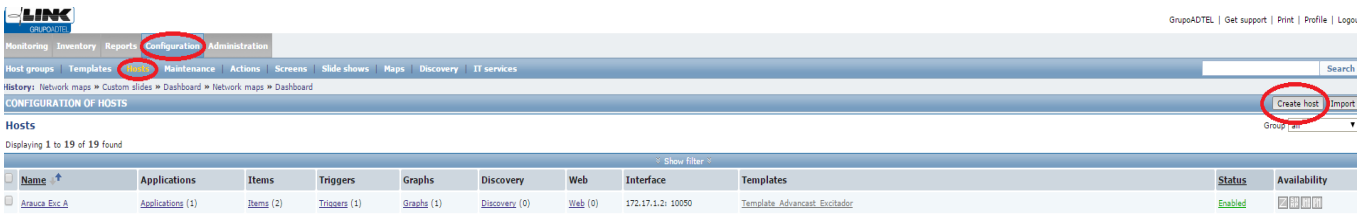


- **Creación de un Host**

El sistema dispone de plantillas para crear un nuevo host y disponer de los checks, de esta manera en cuatro pasos se dispone de un host monitorizado.

Pasos a seguir para la creación de un host. En este ejemplo, se crea el host Router del emplazamiento de Cúcuta.

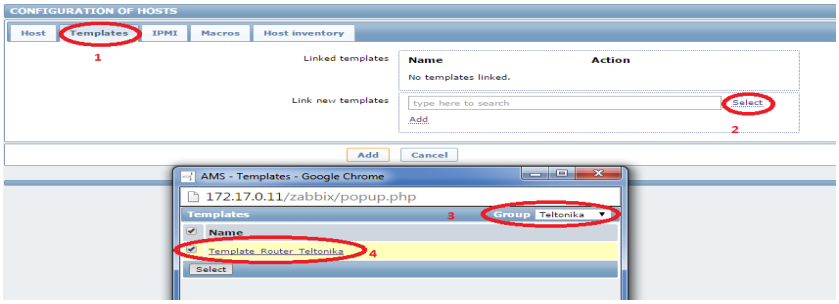
Configuration → Hosts → Create Host



Se introducen los datos del nuevo host, será necesario añadir el Router en el grupo Teltonika y crear un nuevo grupo que será el nombre del emplazamiento, en este caso Cúcuta. Para el Router se utiliza la interfaz SNMP, por lo que la interfaz Agent se puede eliminar.

Una vez completado, se pasa a la pestaña Templates. Plantilla (Templates) definida como un conjunto de entidades (items, triggers, graphs, reglas de detección de bajo nivel) que se pueden aplicar a varios host. Al existir host iguales, se crean plantillas con parámetros definidos y luego se aplica una misma plantilla a todos los host de la misma familia.

En la pestaña Templates, se selecciona la plantilla que se desea aplicar al host, en este caso la Teltonika.



- **Añadir imagen**

La personalización de la interfaz web mediante la inserción de imágenes posibilita que la visualización de la herramienta de gestión sea más gráfica e intuitiva para el usuario.

Los mapas en Zabbix consisten en arreglos gráficos de hosts que permiten visualizar en una misma pantalla o gráfica, el estado básico, las alarmas y los triggers de un grupo, o varios grupos de hosts.

Aprovechando esta prestación, se ha decidido insertar el mapa de Colombia y para disponer de una mejor visibilidad se ha dividido en tres zonas: Norte, Centro y Sur.

Para añadir la imagen de un equipo o de un mapa, hay que ir a la sección General de Administration. ***Administration → General***

Una vez en el menú General, seleccionar en el desplegable la opción Images, donde se mostrará un segundo desplegable y se podrá elegir entre Icon o Background. Una vez realizada en la sección, se podrá hacer un click en Create y añadir la imagen o Mapa.

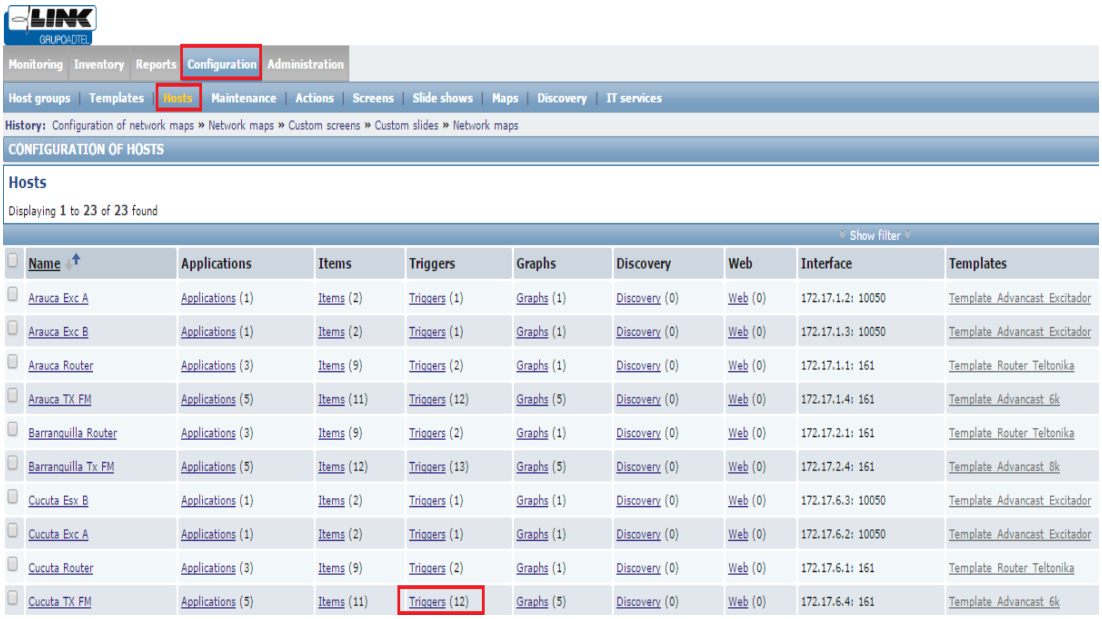
- **Triggers**

Los Triggers son expresiones lógicas que evalúan el estado del sistema. Se añaden dependencias a triggers de los hosts creados para evitar recibir un número elevado de avisos, cuando no se tenga acceso a los equipos.

Se dispondrá que los checks ICMP de los EXCA, EXCB y TX FM dependan del Router, de tal manera que, en caso de perder la conectividad, solo se recibirá un aviso en vez de cuatro.

Esta actuación es necesaria realizarla manualmente y después de tener los cuatro hosts creados no es posible hacerlo desde la propia plantilla.

Acceder al menú de configuración de host. **Confguration → Hosts**



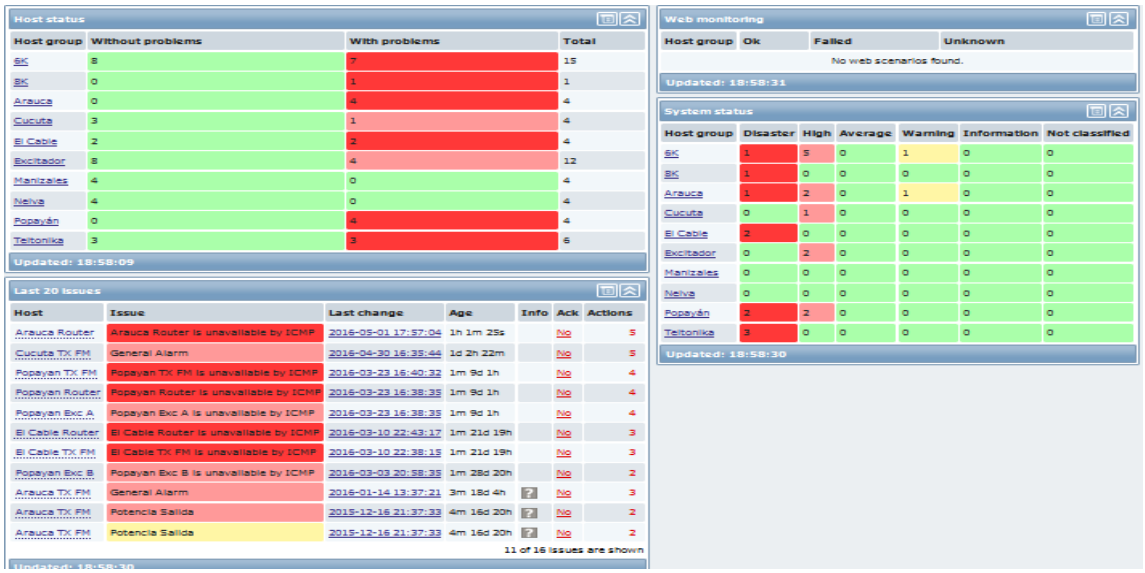
4.4.3. Resultados de la Personalización

En este apartado se verá el resultado obtenido tras realizar la personalización de la herramienta Zabbix.

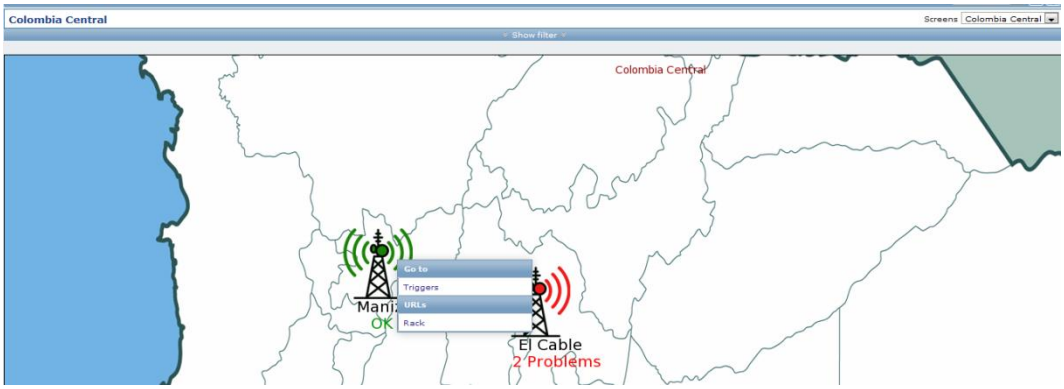
La interfaz web está compuesta por cinco secciones frontend. Como actualmente el proyecto se encuentra en fase de desarrollo, se muestran las opciones configuradas hasta el día de hoy, no obstante son las mínimas indispensables para un correcto funcionamiento del sistema.

Monitoring (Monitoreo)

Dashboard: muestra en resumen la información del sistema por host group.



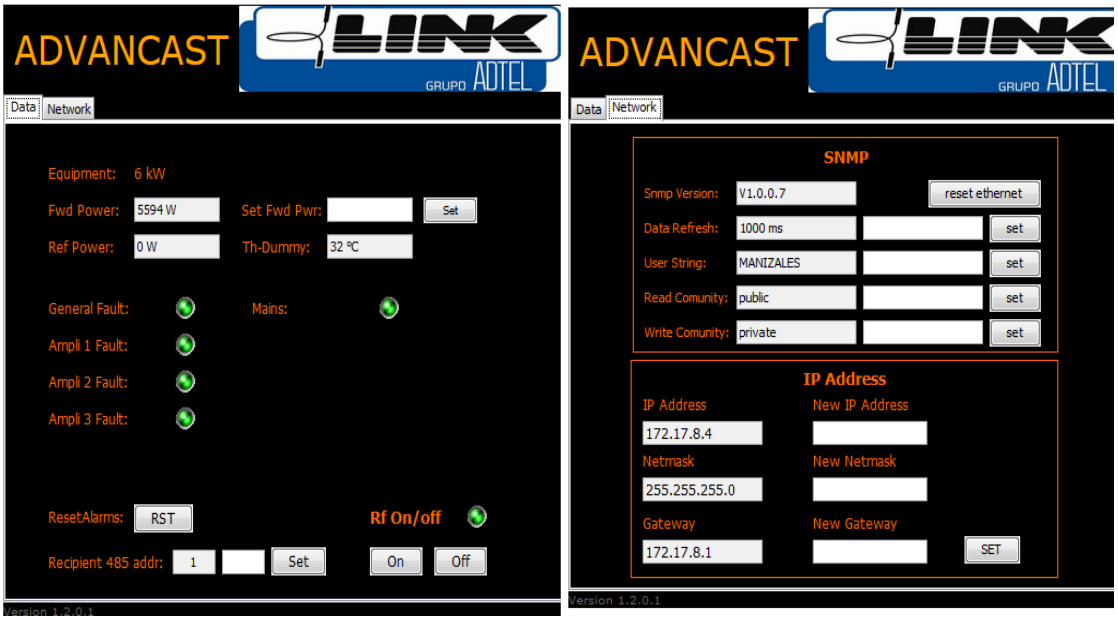
Screens (Pantallas) muestra las pantallas que han sido personalizadas con el mapa de Colombia y los iconos sobre plano representan cada emplazamiento.



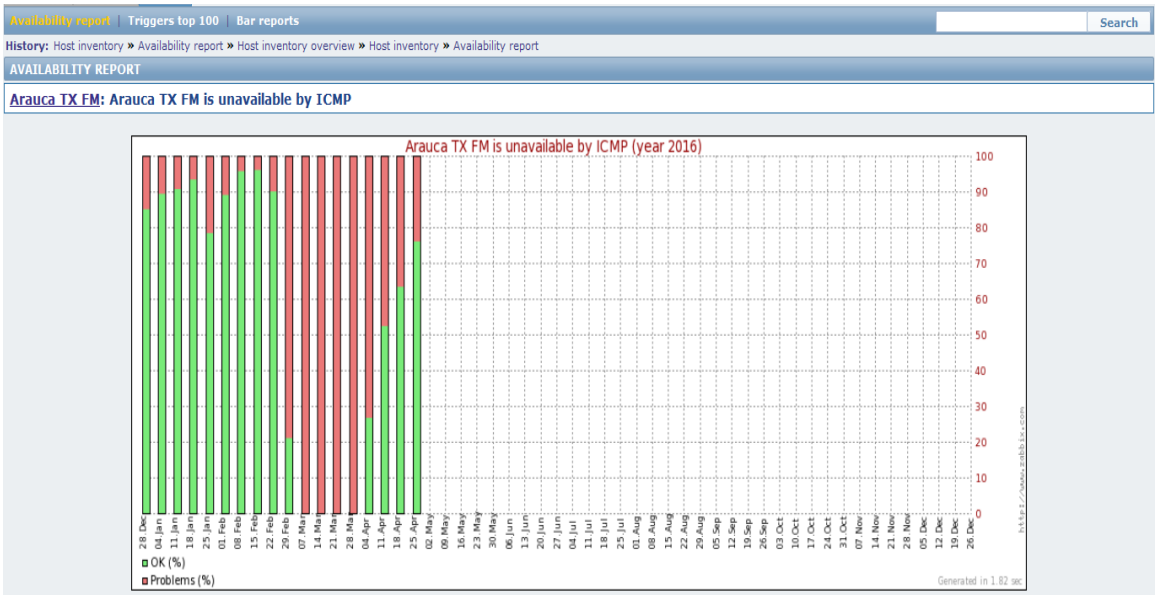
Es posible seleccionar la opción de visualizarse, como Slide Shows (diapositivas) que se irán alternando las tres pantallas configuradas (Colombia Norte, Centro y Sur). Con un click sobre el icono de Manizales, se abre una ventana que da opción a ir a ver los triggers o tener una vista del rack que se ofrece también en la pestaña Maps.

Se ve una imagen del transmisor FM y se muestra el estado de cado uno de los equipos que lo conforman. También muestra el estado del Router, el nivel de RSSI de la red 3G, la potencia directa que sale hacia antena y la potencia reflejada (parámetro que indica perdida de potencia en antena). La opción de Gestión posibilita entrar a la gestión de los Excitadores o el Combinador, Home se vuelve a la página inicial.

Después de realizar un clik sobre el icono de Gestión, se accede a través de web server al Comobinador de Manizales en este caso.



Availability Reports muestra la disponibilidad. Se puede ver qué periodo de tiempo ha estado un trigger activo y el tiempo en que ha estado funcionando correctamente. En Gaph, se puede ver el estado en función del tiempo en una gráfica de barras.



5. **Reporte económico**

La siguiente tabla muestra los costes de hardware, su instalación y configuración. En la configuración del servidor Zabbix se destina un técnico programador durante dos semanas (diez días), con dedicación exclusiva. En la configuración del servidor OpenVPN se destina un técnico programador durante una semana (cinco días), con dedicación exclusiva. Los routers Teltonika RUT500 necesitan ser configurados para cada uno de los 18 emplazamientos. Se destina un técnico dos días (16 horas).

	Precio € unidad	*Recursos destinados*	*Precio €*
Servidor OpenVPN	1.000	1 unidades	1.000
Licencia GPL OpenVPN	0	1 unidades	0
Servidor Zabbix	1.000	1 unidades	1.000
Licencia GPLv2 Zabbix	0	1 unidades	0
Router Teltonika RUT 500	105	18 unidades	1.890
Técnico OpenVPN config.	35/hora	80 horas	2.800
Técnico Zabbix config.	35/hora	40 horas	1.400
Técnico Teltonika config.	35/hora	16 horas	560
Subtotal 1ª partida			**8.650,00**

Algunos emplazamientos requieren de la instalación de antenas tipo Yagi externas para mejorar los niveles de cobertura 3G. Se realiza un presupuesto de la mano de obra de un técnico de campo cuyo precio hora es de 25€ y coste de material de cableado necesario.

	Precio € Unidad	*Recurso destinados*	*Precio €*
Técnico Campo	25/hora	16 horas	400
Cable RG214	7,63	25 mts.	247,97
Conectores varios	4	2 unidades	10,40
Herraje sujeción antena	30	1 unidad	39
Antena Yagi	48	1 unidad	62,40
Subtotal 2ª partida			**759,77**

El subtotal de la segunda partida se ha de multiplicar por cuatro, ya que es el número de emplazamientos con problemas de cobertura; al material (conectores, herrajes, Antena Yagi, Cable RG214), se le ha sumado un 30% al coste de compra, en concepto de gasto por suministro. Se deberá tener en cuenta también el gasto fijo mensual ocasionado por el alquiler de la red celular del operador colombiano Claro que es de 10€/mes. Los gastos de la conexión Internet del extremo de Barcelona no se tienen en cuenta para este proyecto.

- Presupuesto total

	Recursos destinados	*Precio €*
Subtotal 1ª partida	1	8,650
Subtotal 2ª partida	4 emplazamientos	3.039,08
Conexión Internet Colombia anual	(10€ x 18 emplazamientos) x 12 meses	2.160
Total presupuesto		**13.849,08**

Bibliografía

[1], En línea, http://www.syscom.mx/principal/verproductoazul/tx8001614-txpro-14251.html, [Fecha de consulta: 5/5/2016]

[2], En línea, https://www.ietf.org/rfc/rfc3416.txt, [Fecha de consulta: 14/4/2016]

[3], En línea, http://www.claro.com.co/wps/portal/co/pc/personas/internet/internet-movil/Internet-movil-con-consumo-incluido/contenidos, [Fecha de consulta: 10/4/2016]

[4], En línea, http://www.dlink.com/es/es/home-solutions/connect/routers/dwr-921-4g-lte-router, [Fecha de consulta: 19/3/2016]

[5], En línea, http://www.tp-link.com/en/products/details/Archer-MR200.html#specifications, [Fecha de consulta: 19/3/2016]

[6], En línea, http://www.teltonika.lt/en/pages/view/?id=1031, [Fecha de consulta: 19/3/2016]

[7], En línea, https://es.wikipedia.org/wiki/M%C3%A1scara_de_red#Tabla_de_m.C3.A1scaras_de_red, [Fecha de consulta: 22/3/2016]

[8], En línea, www.zabbix.com/documentation/2.4/manual/introduction/about, [Fecha de consulta: 25/4/2016]

[9], En línea, https://www.zabbix.com/documentation/2.4/manual/concepts/server, [Fecha de consulta: 25/4/2016]

[10], En línea, https://es.wikipedia.org/wiki/OpenVPN, [Fecha de consulta: 30/4/2016]

[11], En línea, http://www.mintic.gov.co/portal/604/w3-channel.html, [Fecha de consulta: 10/4/2016]

[12], En línea, http://estrategiaticolombia.co/estadisticas/stats.php?id=51&pres=map&jer=1&cod=, [Fecha de consulta: 10/4/2016]

[13], En línea, https://comparabien.com.co/internet/result, [Fecha de consulta: 12/4/2016]

[14], En línea, https://www.nagios.com/, [Fecha de consulta: 26/4/2016]

[15], En línea, http://pandorafms.com/es/, [Fecha de consulta: 26/4/2016]

[16] Libro: James F. Kurose, Keith W. Ross, Computer Networking A top-Down Approach, Sixth Edition, Pearson, 2013.

[17] Material UOC: Pere Barberán Agut, Enric Lopez i Rocafiguera, Xarxes i Serveis, Primera Edicion, Editorial UOC, 9/2011.

[18], En línea, https://openvpn.net/index.php/open-source/documentation/howto.html#dynamic, [Fecha de consulta: 2/5/2016]

6. Anexo

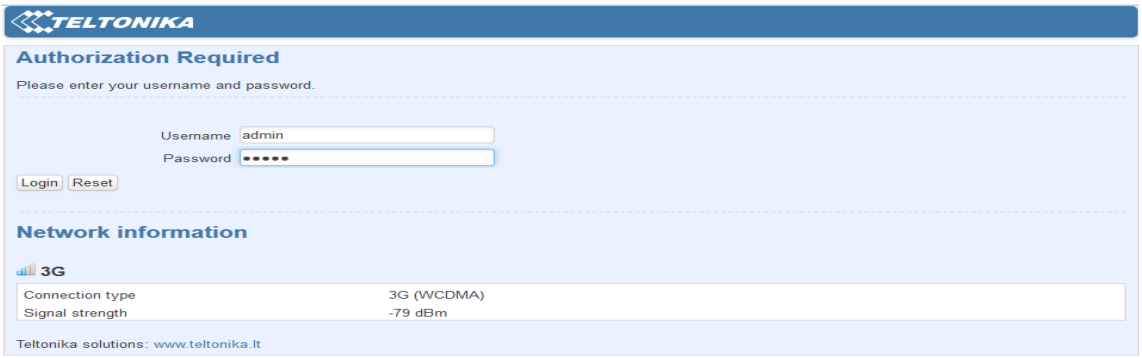
6.1. Configuración Router Teltonika RUT500

Después de haber realizado la elección de conectividad, haber elegido la tecnología hardware adecuado y disponer de la tabla de direccionamiento IP, se procede a la configuración del router Teltonika RU500. Para ello, se deberá conectar la tarjeta de red del ordenador a un puerto LAN1-3 del Router y se deberá configurar la conexión en DHCP.

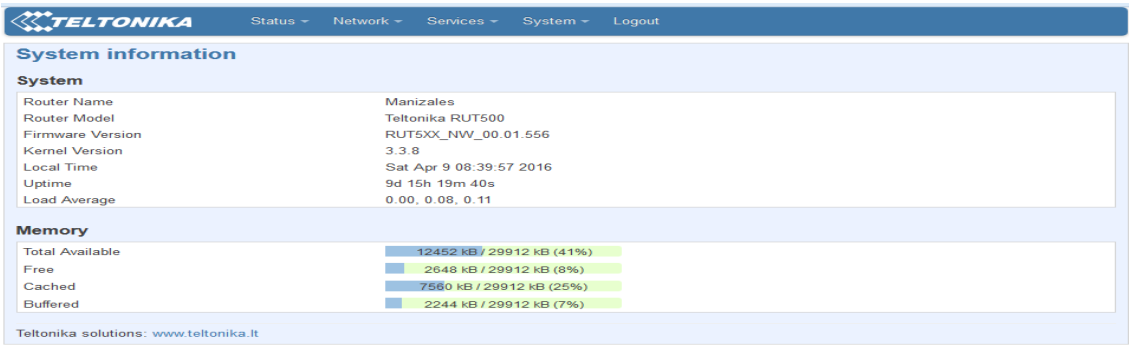
Cuando se asigne IP, se cargará el navegador Explorer, por ejemplo, y en la barra de direcciones se introducirá la siguiente dirección IP: 192.168.1.1

El Router es configurable por web-server. Para acceder, solicita un usuario (admin) y una contraseña (admin01 por defecto).

La siguiente captura de pantalla muestra que está conectado a la red 3G y el nivel RSSI es -79dBm



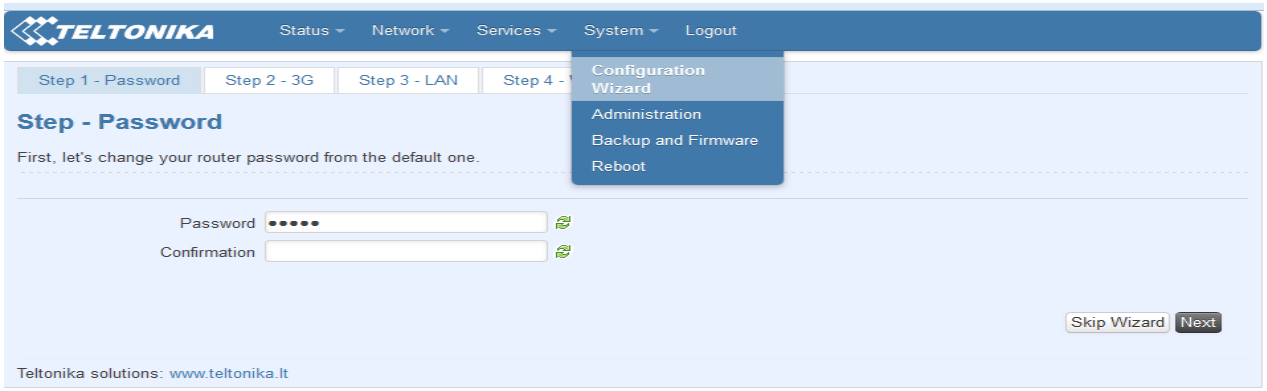
En la página de inicio se muestra la informacion general del Router.



System-> Configuration Wizard

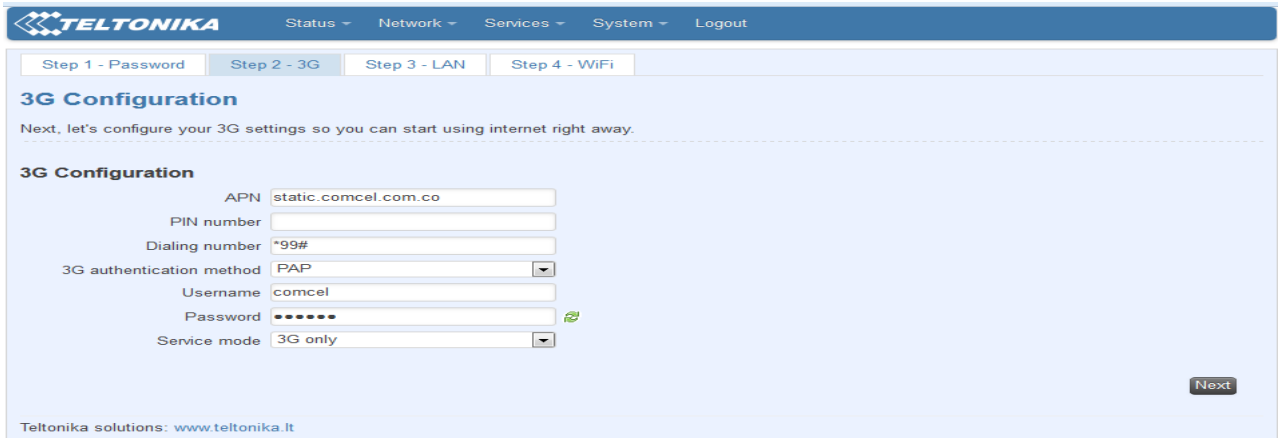
Paso 1

Password y confirmar para cambiar la que viene por defecto



Paso 2

Configuración red 3G



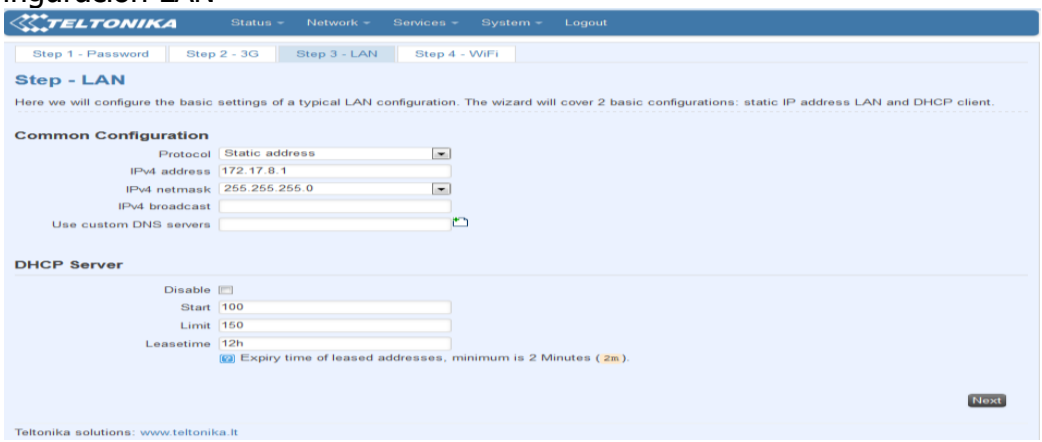
APN: configurar el APN según el operador móvil

PIN Number: se recomienda quitar el PIN a la SIM para evitar 3 intentos y bloqueo de la SIM(desbloque por PUK)

- Dialing number: dejar *99#.
- 3G authenticacion method: consultar con el operador móvil.
- Username y Password: consultar con el operador móvil.
- Service mode: forzar 3G (da opción de auto).

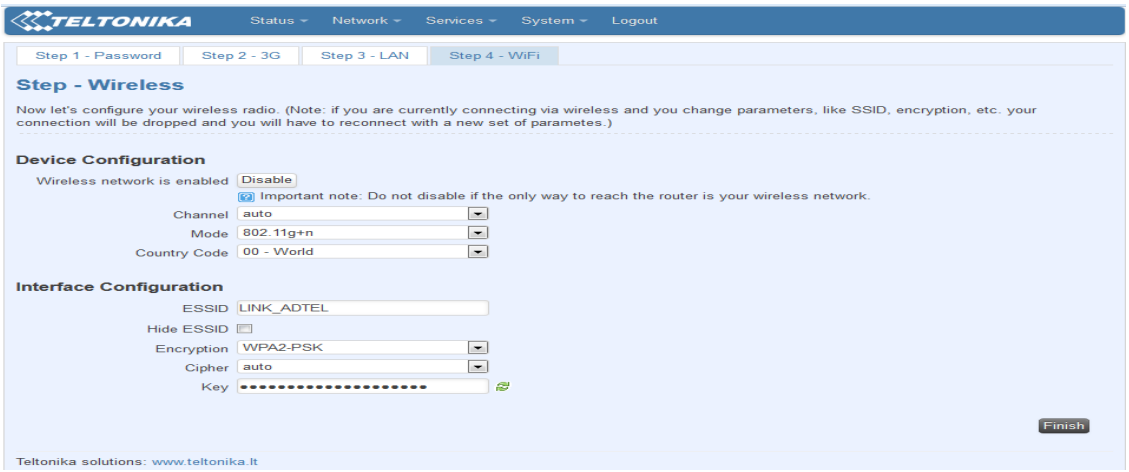
Paso 3

Configuración LAN



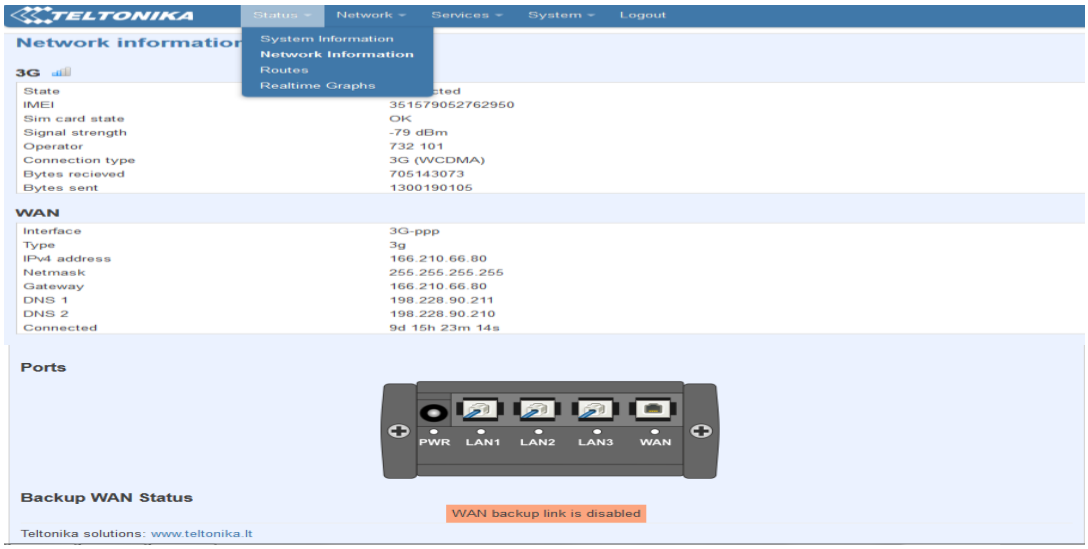
- Protocol: dejar static address, salvo que se utilice el router como cliente DHCP de un Router ADSL/cable.
- IPv4 address: dirección IP de gestión del Router, será la Gateway de cualquier máquina conectada a la LAN del equipo.
- Use Custom DNS servers: dejar en blanco para usar los que provee el operador móvil.
- DHCP Server: deshabilitado si se quiere que las máquinas tengan IP fija.

Paso 4
Configuración WiFi



- Por defecto el AP WiFi está deshabilitado, si se habilita recordar montar la antena WiFi.
- Chanel: canal de frecuencia en auto.
- Mode: seleccionar 802.11g+n.
- Country code: código del país por defecto.
- ESSID: configuración identificador del AP
- Encryption: configurar modo de encriptación wireless.

En Status->Network Information



- State: informa estado de conexión.
- IMEI de la tarjeta.
- Sim card State: debe estar en Ok si no hay problemas de PIN.
- Signal strength: nivel de señal.
- Operator: código identificativo del operador móvil.
- Connection Type: tipo de conexión 2G, GPRS o 3G (WCDMA).
- Bytes recieved/sent: contadores deben ir incrementando.
- WAN IPv4address: es la dirección pública del Router.

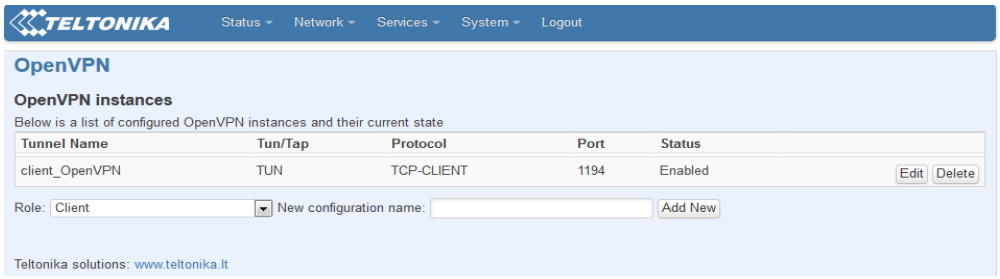
Configuración de cliente en Router Teltonika RUT500 cliente OpenVPN

En el router en la pestaña Services-> OpenVPN configuramos los parámetros:

- Enable: habilitado con check.
- Tun/Tap: modo Tun.
- Protocolo: el escogido en el servidor es TCP.
- Port: el puerto de comunicación 1194.
- LZO: utilizamos compresión LZO.

- Authetication: Tls.

- Remote host/IP address: la dirección IP del servidor.
- El recuadro muestra que se han cargado los certificados y la key del cliente.



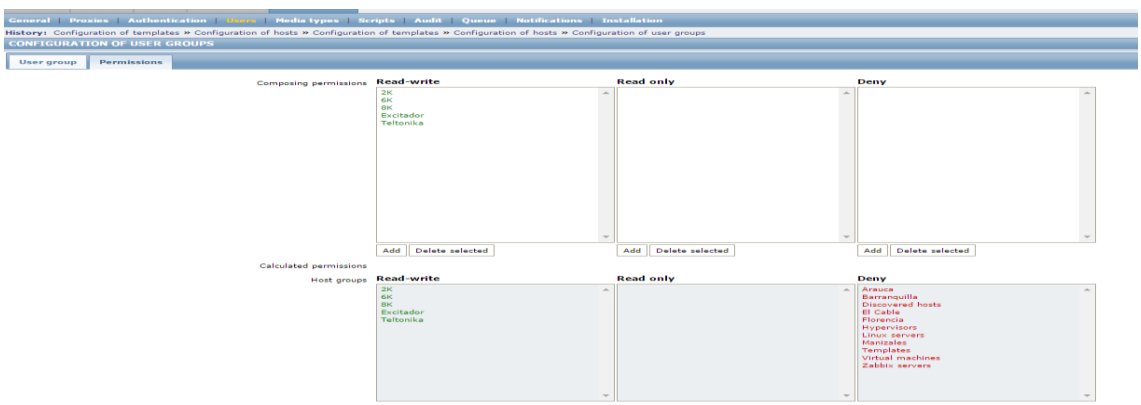
Confirmación de que se ha habilitado la conexión VPN.

6.2. Detalle configuración Zabbix

- **Usuarios**

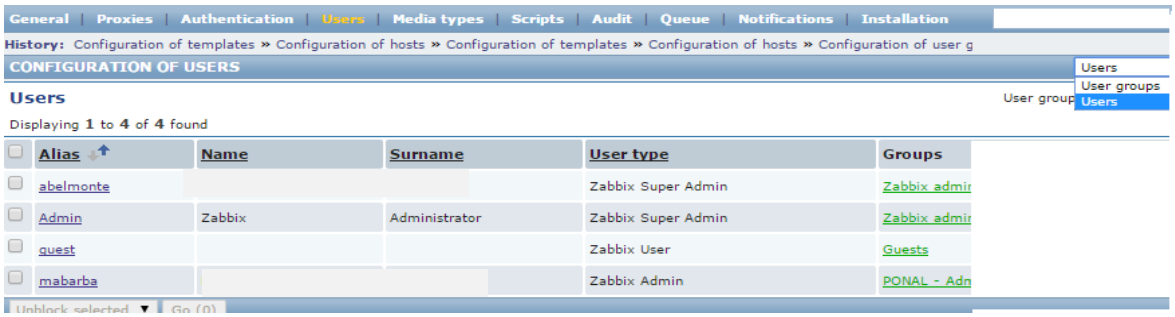
En la pestaña Administration → Users; es posible ver los grupos y los usuarios que pertenecen a ese grupo.

Si se selecciona un grupo, se podrá ver los permisos que tiene.

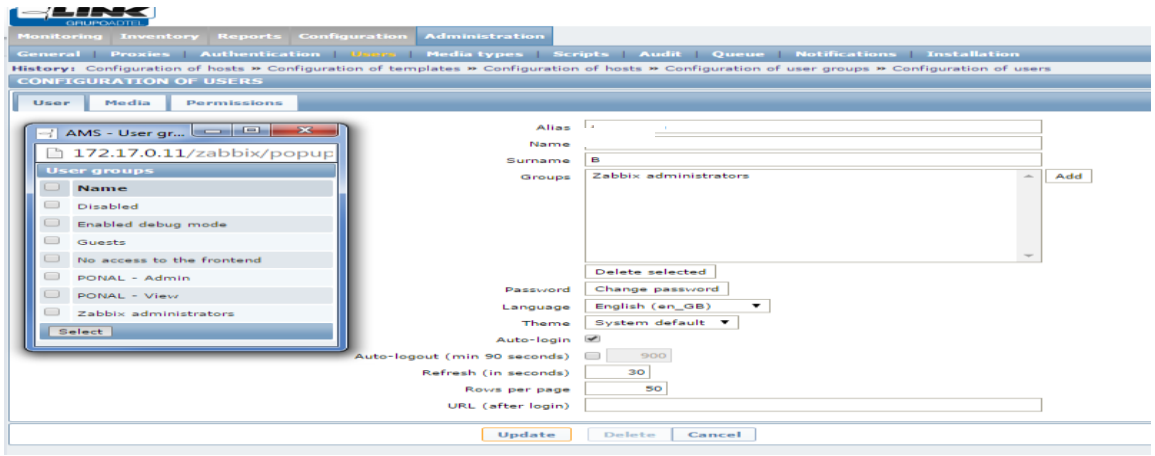


Se puede ver que el grupo seleccionado dispone de R/W en diferentes Host Groups. Los usuarios que pertenezcan a este Grupo dispondrán de permisos de R/W sobre los hosts que estén asociados a esos Host Group.

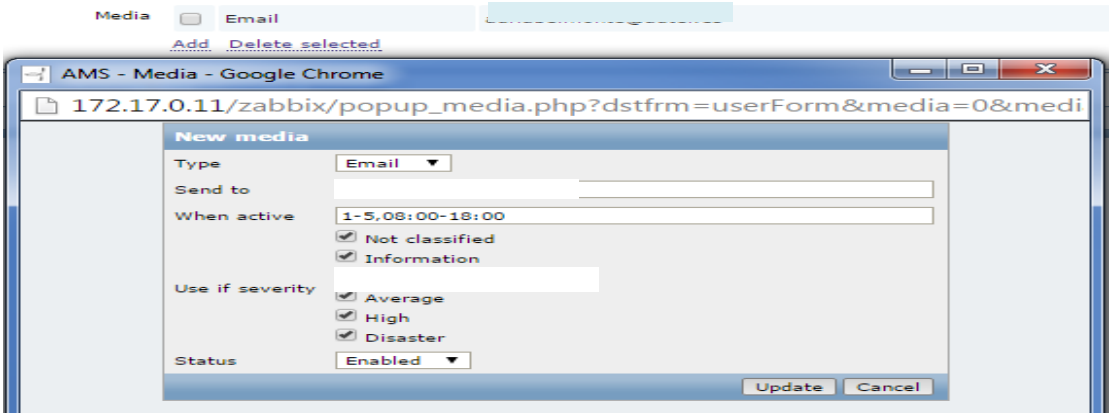
Para añadir/eliminar usuarios, se realiza desde el mismo panel que los grupos, pero seleccionando en el desplegable Users.



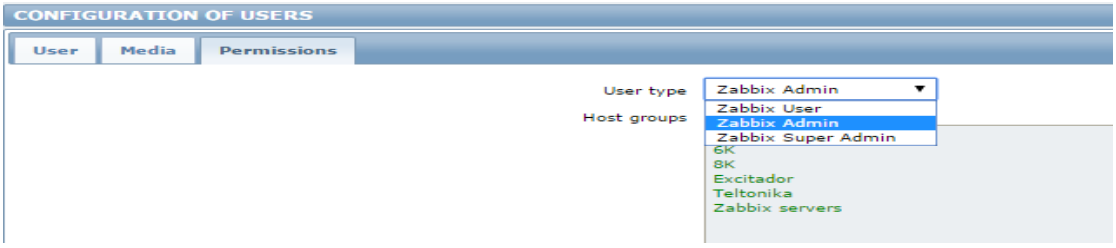
Si se ingresa en un usuario, se podrán cambiar el grupo al que pertenece, contraseña y cuenta de correo electrónico.



En la pestaña Media es posible añadir la cuenta o las cuentas de correo, seleccionando el horario y el tipo de avisos.

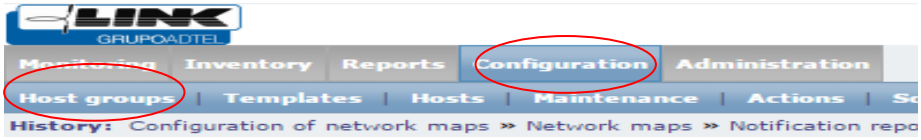


En la pestaña Permissions se define el tipo de usuario al seleccionar la opción de Zabbix User, son solo los permisos genéricos para navegar por Zabbix.

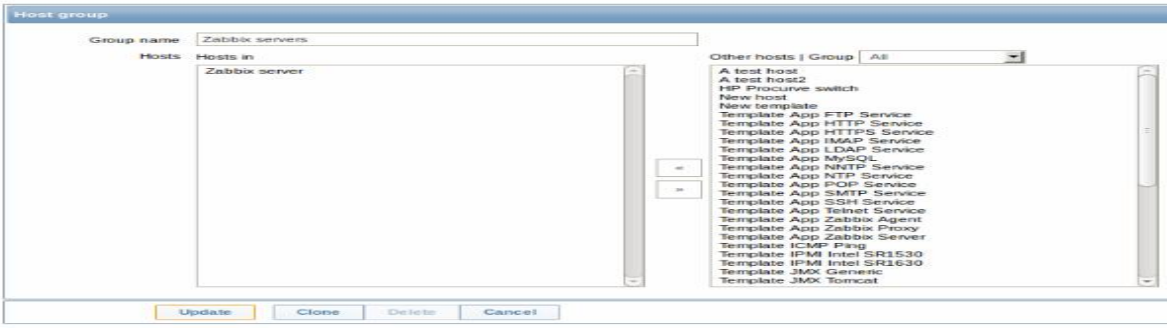


- **Crear un Host Group**

Una vez en la interfaz web, para crear un grupo de host se ha de dirigir a la pestaña Configuration y posteriormente Group Host



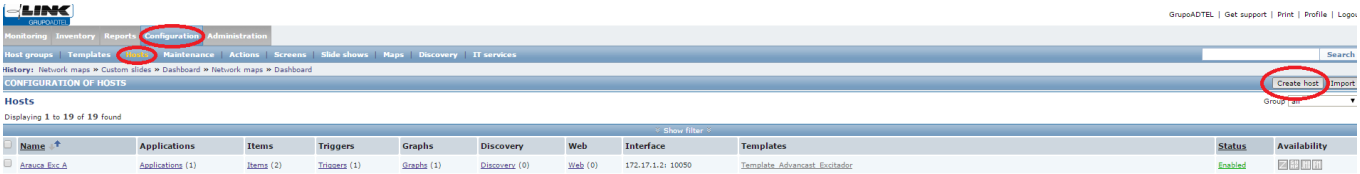
Posteriorment, realizar click en Create Group e ingresar los parámetros identificativos del grupo (Nombre) .



- **Creación de un Host**

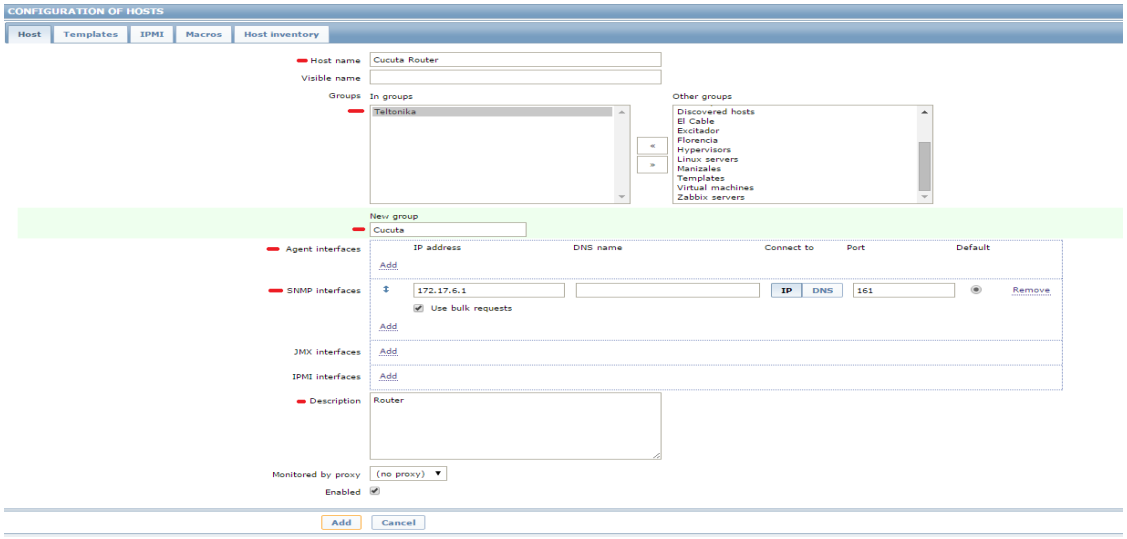
Paso a seguir para la creación de un host. En este ejemplo se crea el host Router del emplazamiento de Cúcuta.

Configuration → Hosts → Create Host



Se introducen los datos del nuevo host. Será necesario añadir el Router en el grupo Teltonika y crear un nuevo grupo que será el nombre del emplazamiento, en este caso Cúcuta.

Para el Router se utiliza la interfaz SNMP, por lo que la interfaz Agent se puede eliminar.

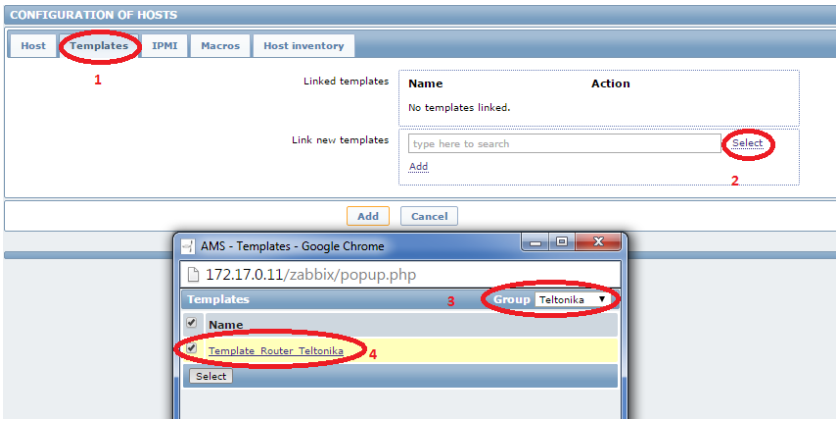


- Seleccionar el grupo o los grupos que pertenece.
- Eliminar la interfaz agente "**Agent Interfaces**".
- Añadir la interfaz SNMP "**SNMP Interfaces**" y la IP del cliente.
- Se puede añadir una breve descripción.

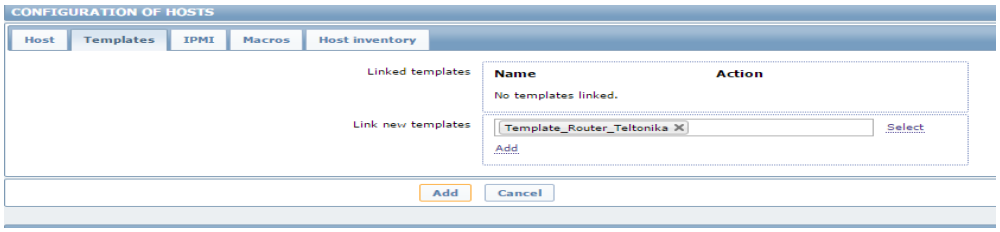
Una vez completado, se pasa a la pestaña Templates.

Plantilla (Templates): definidas como un conjunto de entidades (items, triggers, graphs y reglas de detección de bajo nivel) que se pueden aplicar a varios host. Al existir host iguales, se crean plantillas con parámetros predefinidos y luego se aplica una misma plantilla a todos los host de la misma familia.

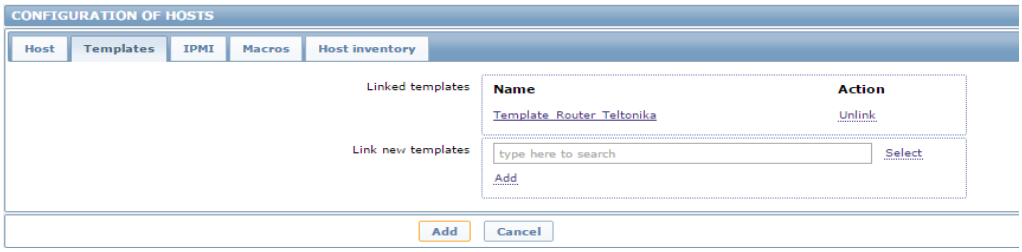
En la pestaña de Templates se tiene que buscar la plantilla que se quiere aplicar al host, en este caso la Teltonika.



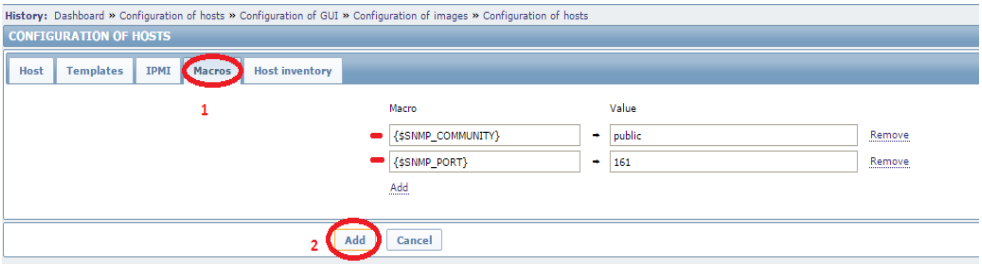
Realizada la selección, será necesario realizar un click en ADD para utilizar la plantilla.



Una vez añadida, se verá como en la siguiente captura.



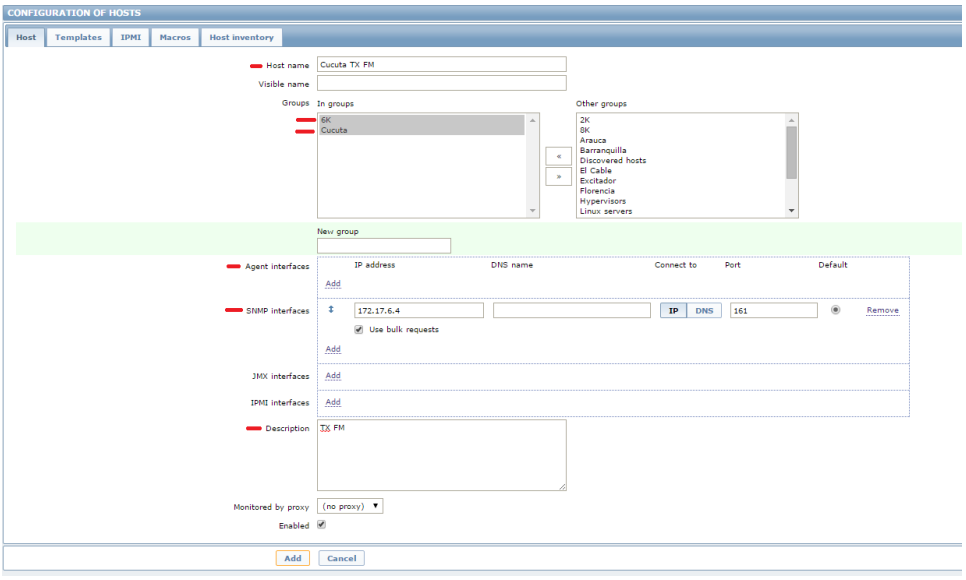
En la pestaña Macros, se deben introducir las siguientes variables o macros que servirán para los triggers.



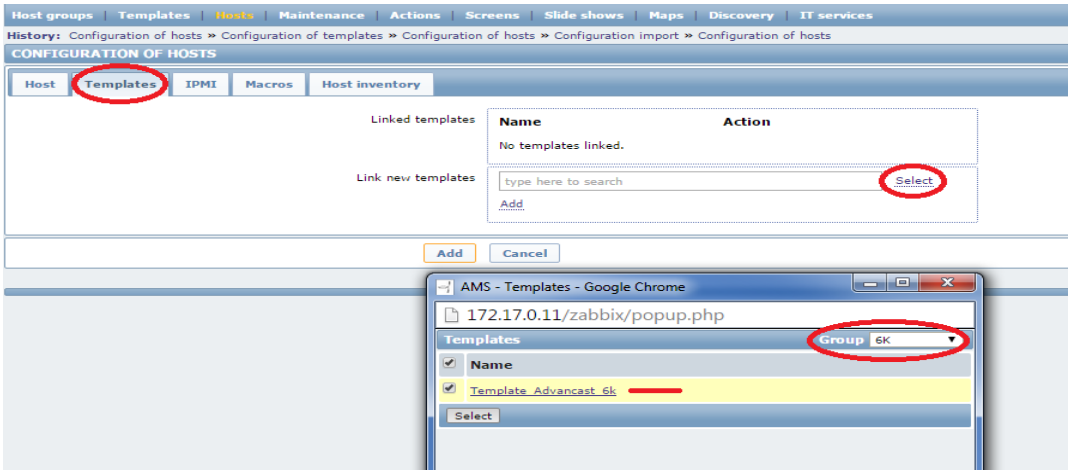
Con los datos ya introducidos, se finaliza la creación del host con el botón ADD.

Paso a seguir para la creación de un host. En este ejemplo se crea el host Transmisor FM de 6Kdel emplazamiento de Cúcuta.

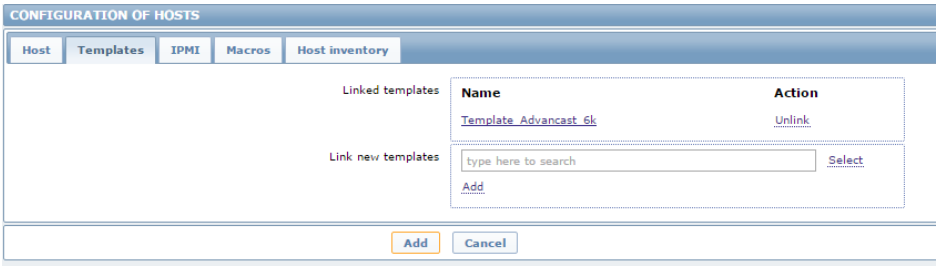
Configuration → Hosts → Create Host



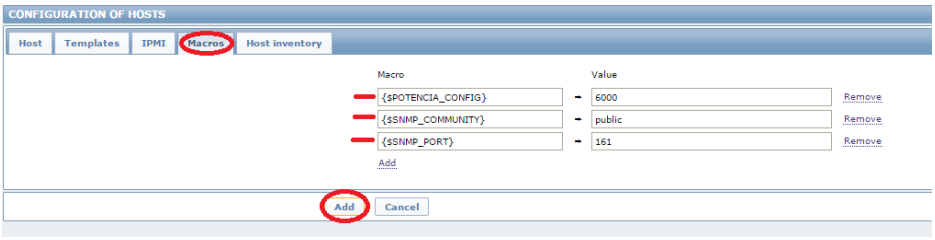
No será necesaria la creación del grupo porque en el desplegable ya aparecerá. Una vez creados los datos, se pasa a la plantilla.



Seleccionar la plantilla que aplica, en este caso es la de 6k, y realizar los mismos pasos que en el router.



En los equipos transmisores se añade una nueva macro/variable.



Una vez introducidas, se finaliza la creación del host con el botón ADD.

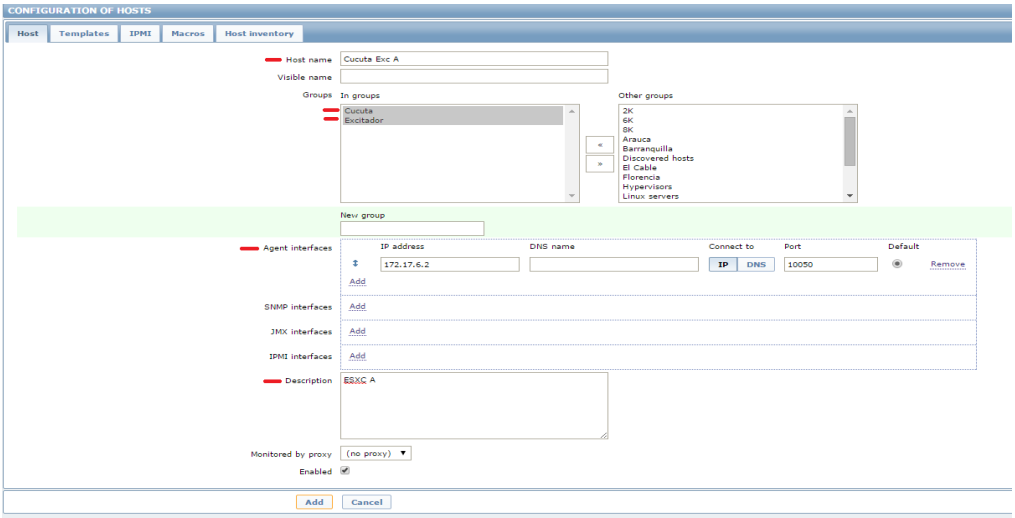
Paso a seguir para la creación de un host. En este ejemplo se crea el host excitador (EXC A) del emplazamiento de Cúcuta.

Configuration → Hosts → Create Host

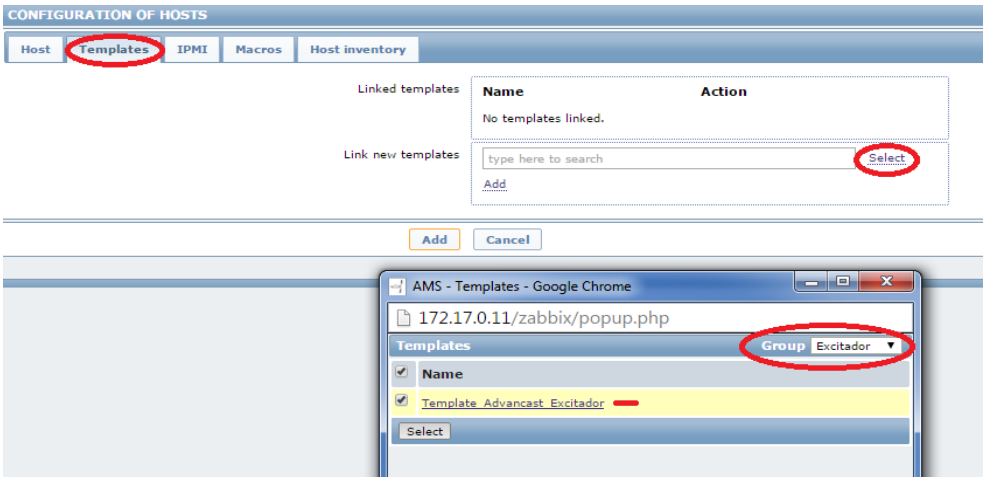
Estos pasos se deberán realizar por duplicado, ya que se dispone de dos excitadores (A y B).

Se introducen los datos igual que en las anteriores ocasiones, pero con la diferencia que el Excitador no utiliza una interfaz SNMP, sino que utiliza la interfaz Agent.

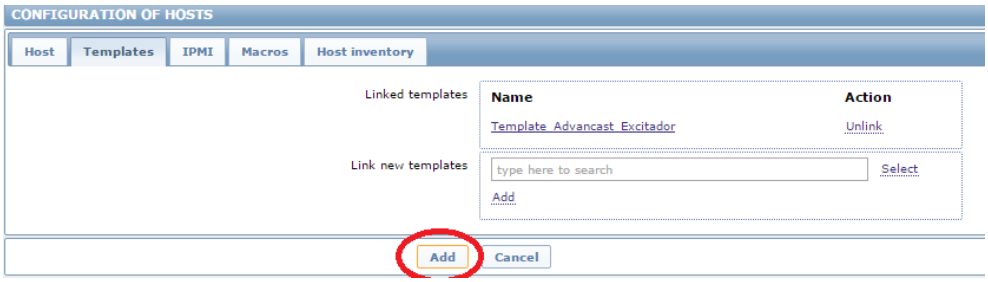
Igual que en los anteriores, se selecciona el grupo de la zona (Cúcuta) y el grupo de los equipos (Excitador).



Introducido los datos, se dirige a la pestaña de Templates.

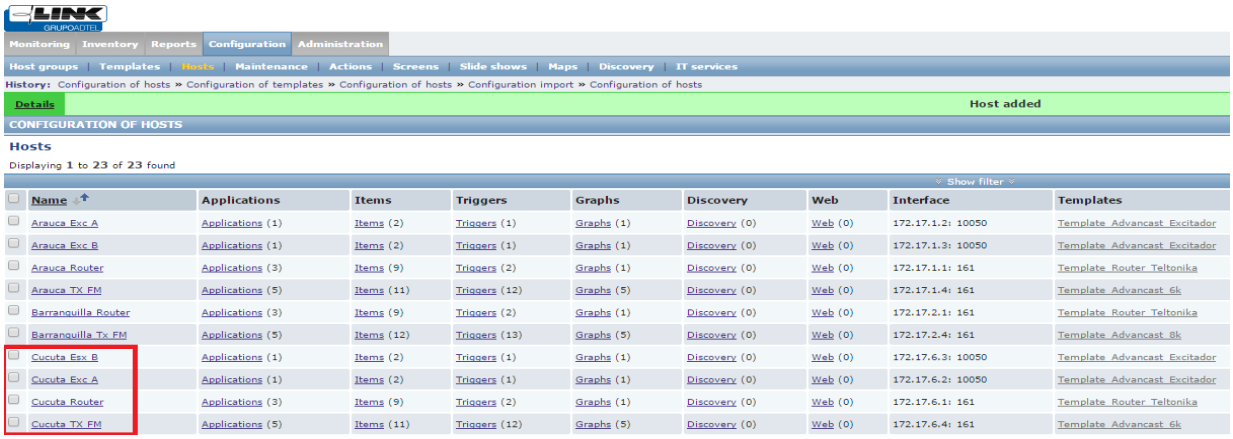


Seleccionar la plantilla que aplica, en este caso es la de Excitador.



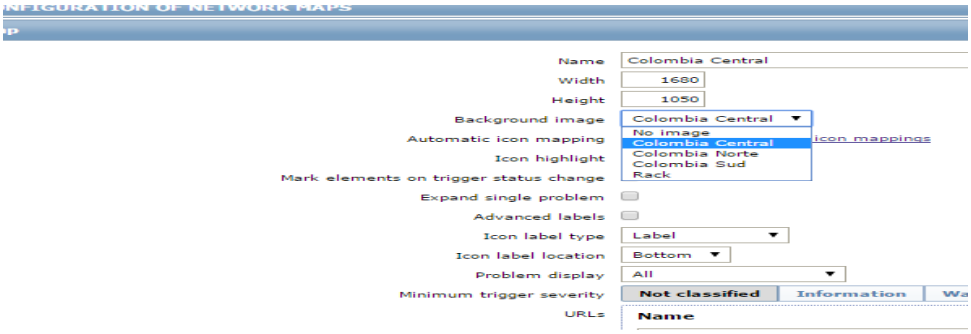
Cuando se tiene la plantilla seleccionada, añadir el host. En los excitadores no es necesario crear macros/variables.

Una vez se crea el EXC A, se deben reptir los mismos pasos para el EXC B y ya se dispondrá de los cuatro equipos.



- **Añadir imagen**

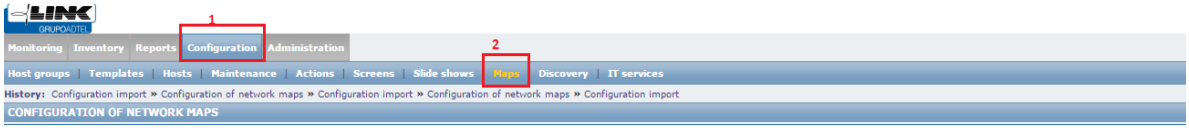
Para modificar el fondo de algún mapa ya existente, se debe seleccionar la opción EDIT del mapa y en el desplegable seleccionar el nuevo fondo.



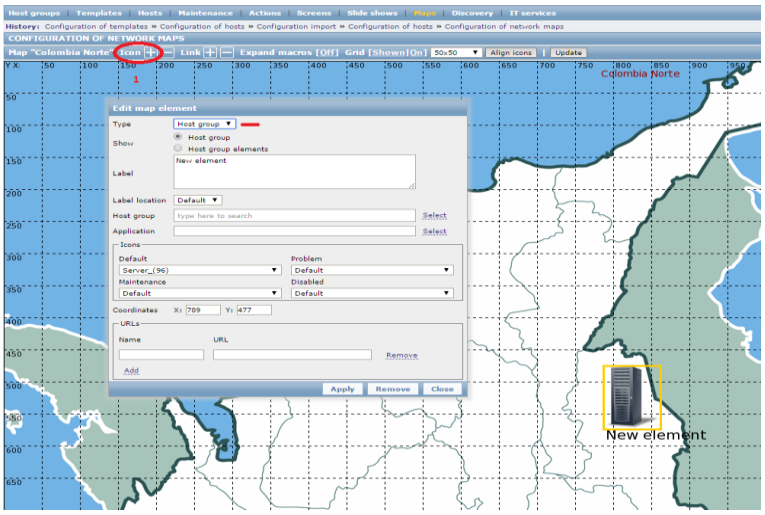
- **Mapa de Colombia**

Una vez creados los host, se añade el icono en el mapa de Colombia en el siguiente menú.

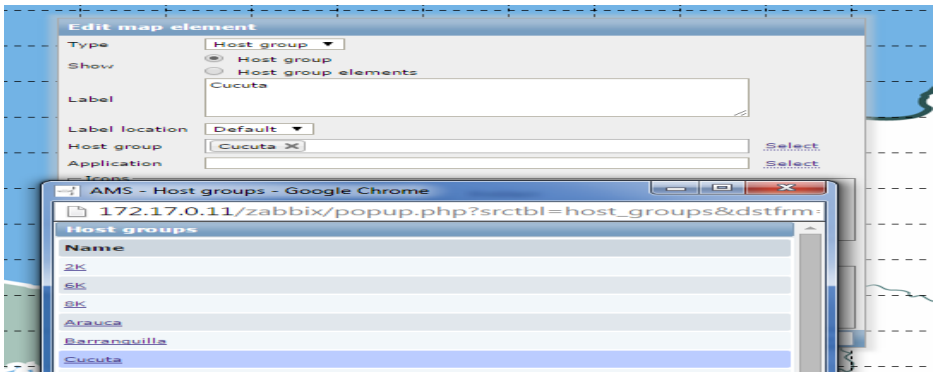
Configuration → Maps → Create map



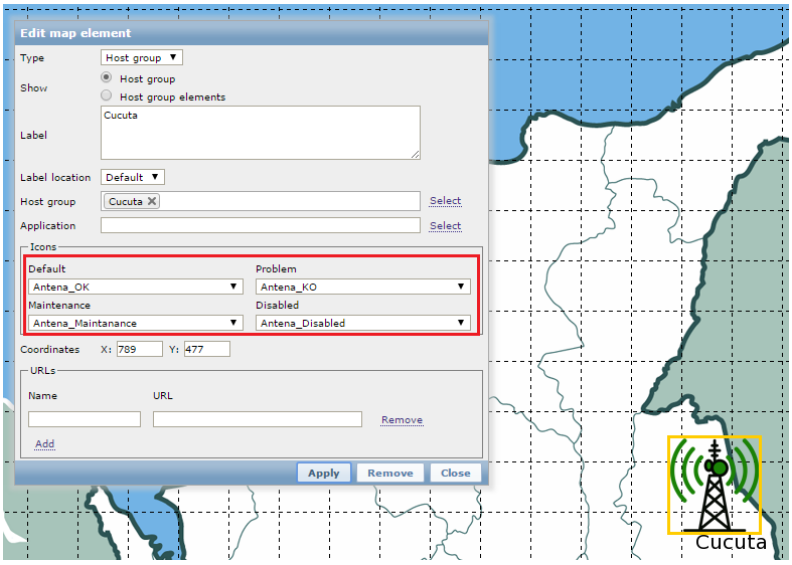
Una vez situados dentro del mapa, añadiremos el icono. Para ello, clickar en el botón de Icon, que está en la barra superior, una vez clickado se abre una ventana en la que se debe seleccionar la opción Host Group.



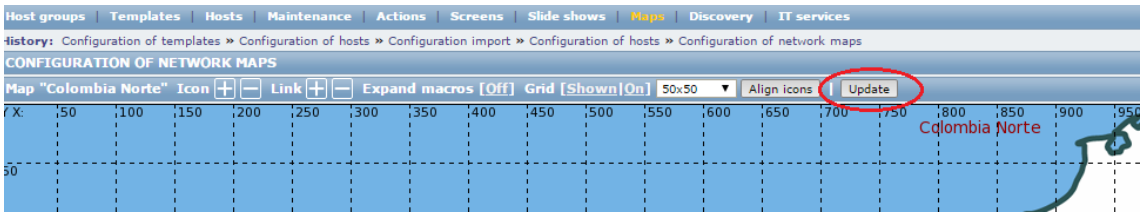
Con la opción seleccionada, se debe buscar el grupo del host, donde se muestra un desplegable con el listado de grupos, en el que se debe seleccionar el nombre del nuevo centro.



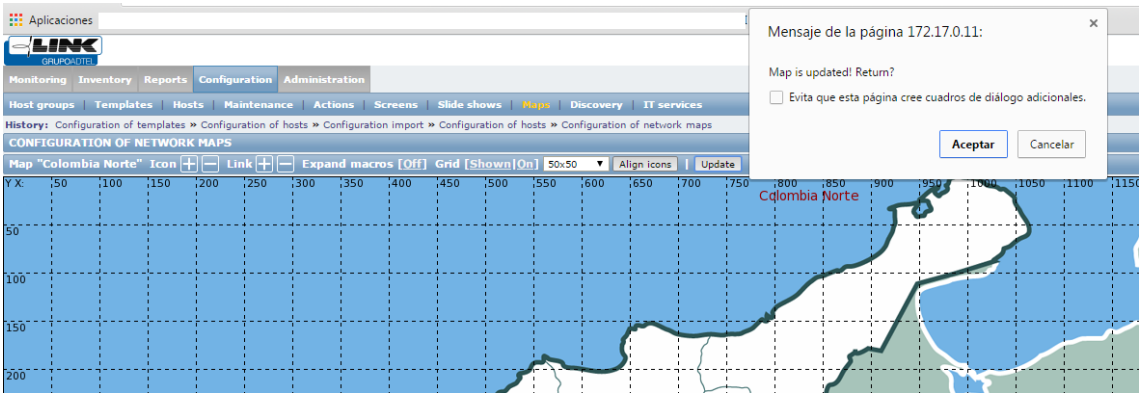
Una vez seleccionado el grupo, solo faltará modificar el nombre dentro del LABEL y seleccionar los iconos.



Con los iconos cambiados, solo se debe guardar la ventana, **Apply → Close**
La ventana, después de darle al botón de Apply, no se cerrará.
Para finalizar, se guardan los cambios en el mapa con el botón Update.

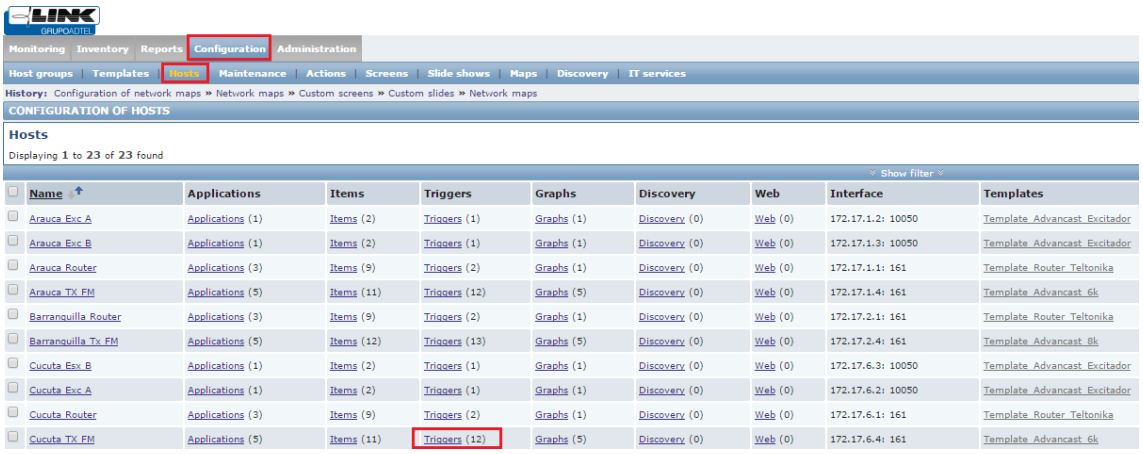


En este botón sí que se mostrará una ventana emergente que se debe aceptar.

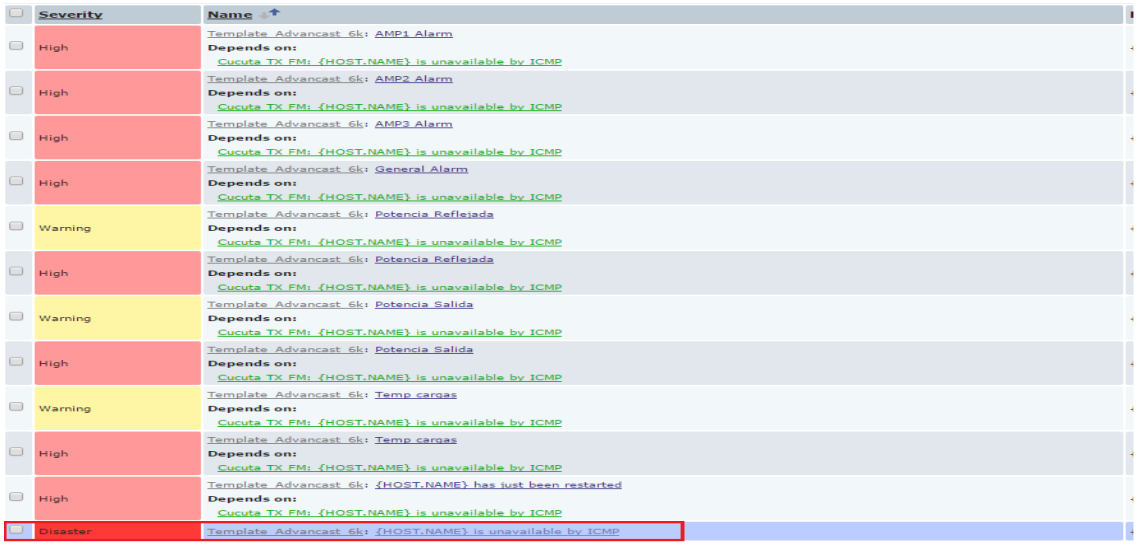


- **Triggers**

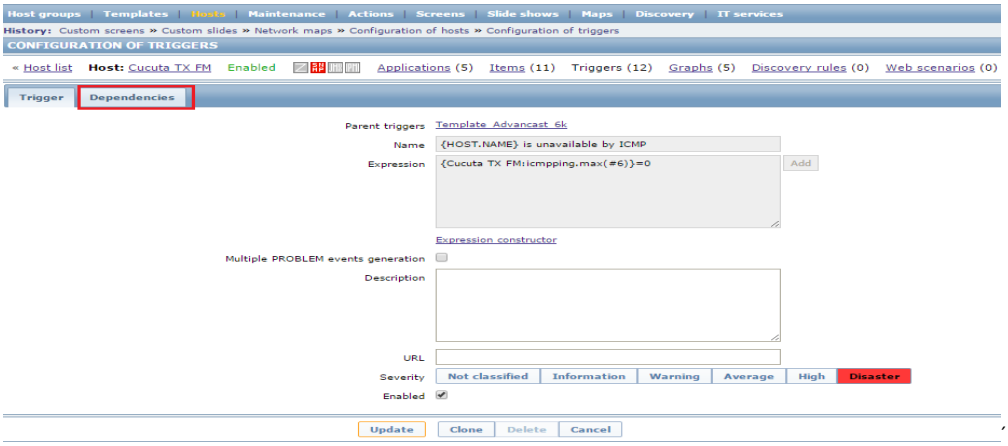
Acceder al menú de configuración de host. **Confguration → Hosts**



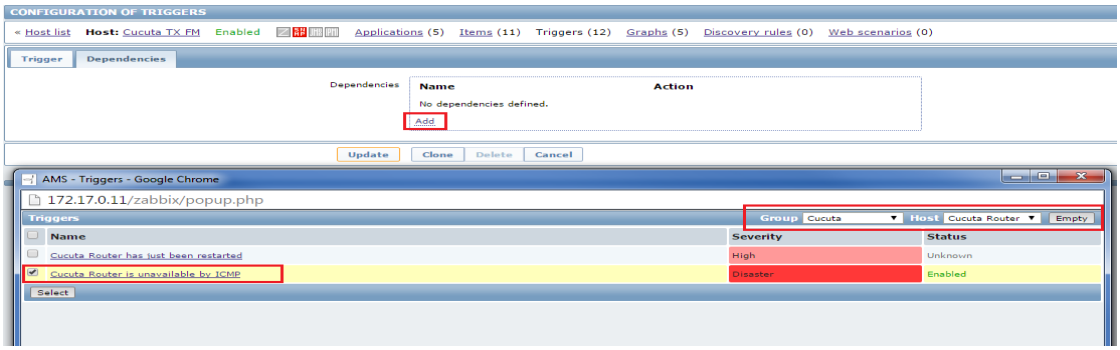
Seleccionar el menú Triggers de un host, en este caso del TX FM.
Se mostrarán los distintos triggers que dispone este host, buscar el ICMP y seleccionar.



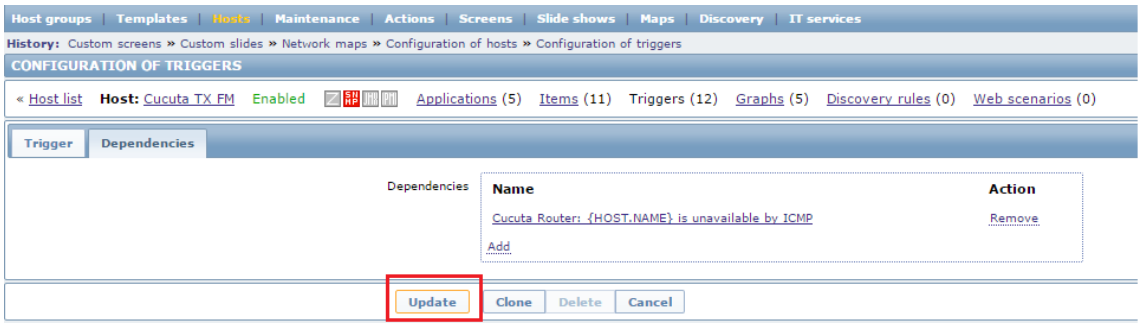
Una vez seleccionado, ir al menú DEPENDENCIES.



En el Menú Dependencies, seleccionar que el trigger tenga dependencia del trigger del Router.



Cuando tengamos seleccionado el Trigger, se verá el resultado y se actualizará el host con UPDATE.

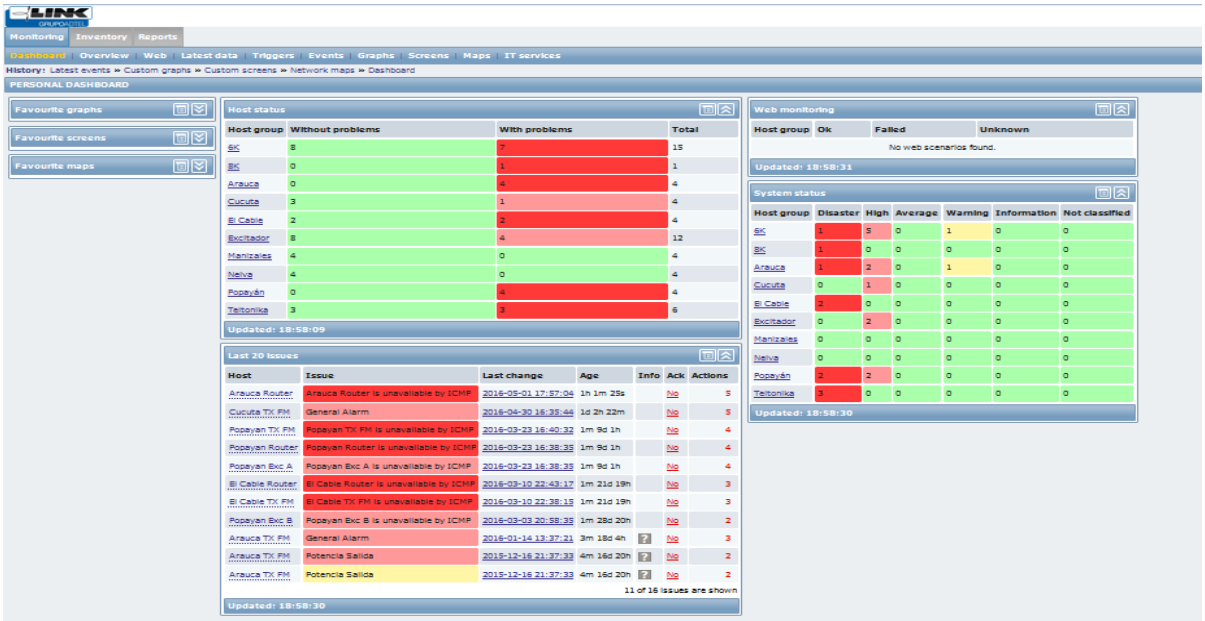


Este paso se repite con los otros dos host (EXC A y EXC B).
Con estos pasos se tiene el host del nuevo centro creado correctamente.

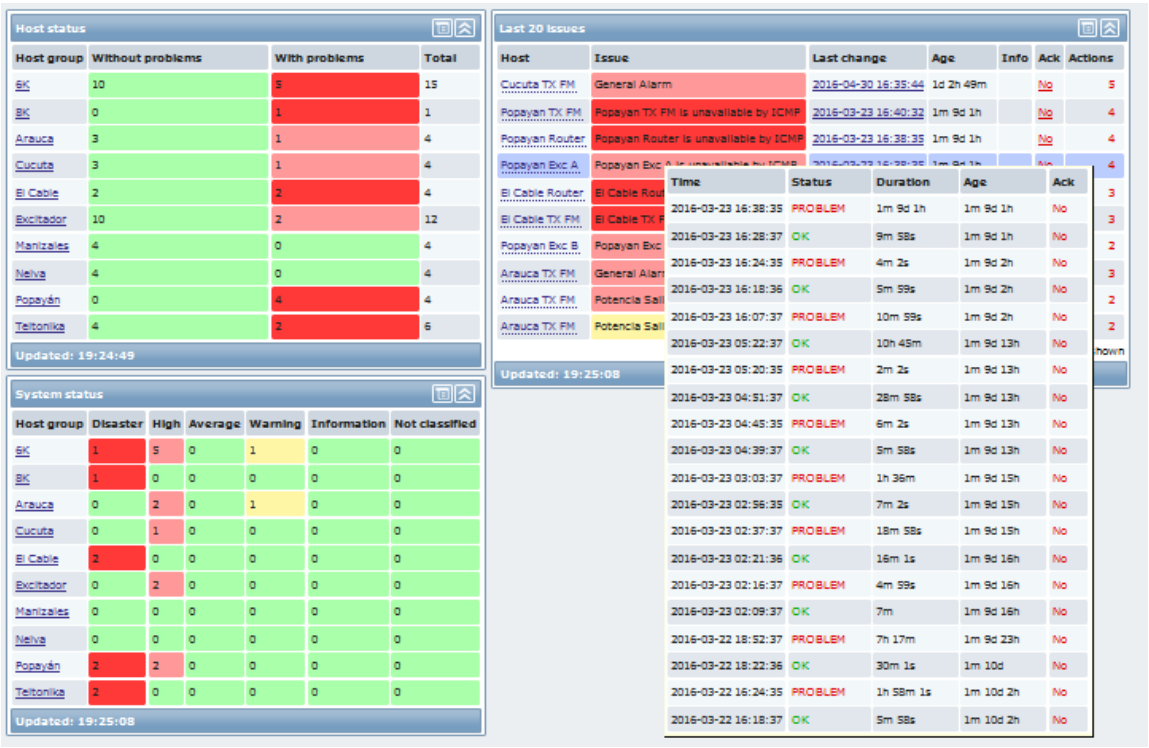
6.3. Resultados de la personalización

Monitoring (Monitoreo)

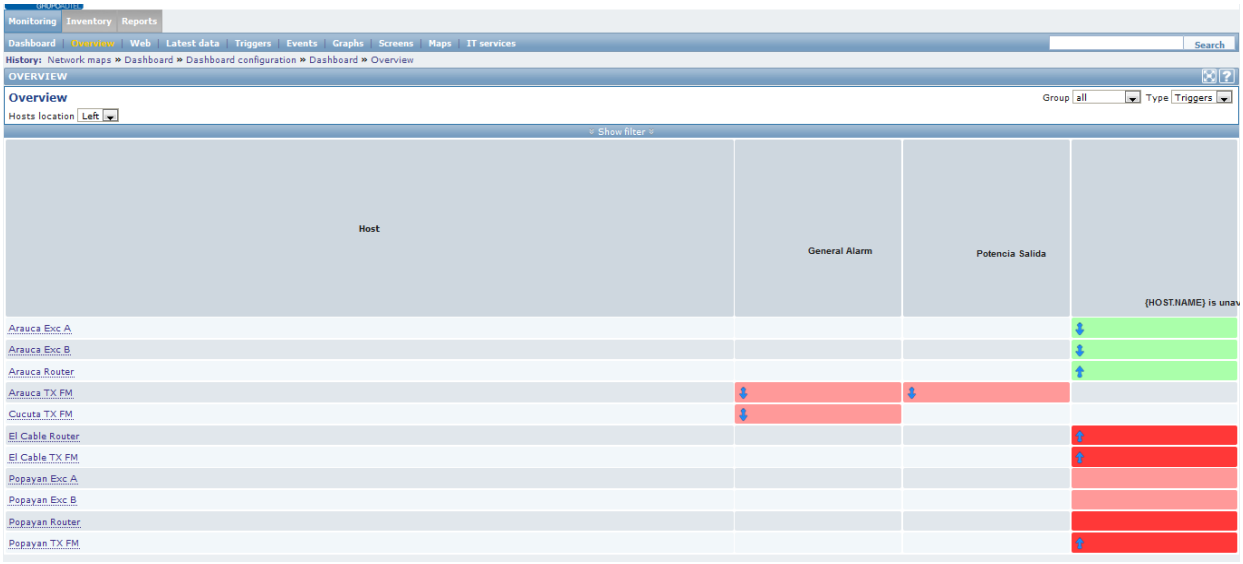
Dashboard: muestra, en resumen, la información del sistema.



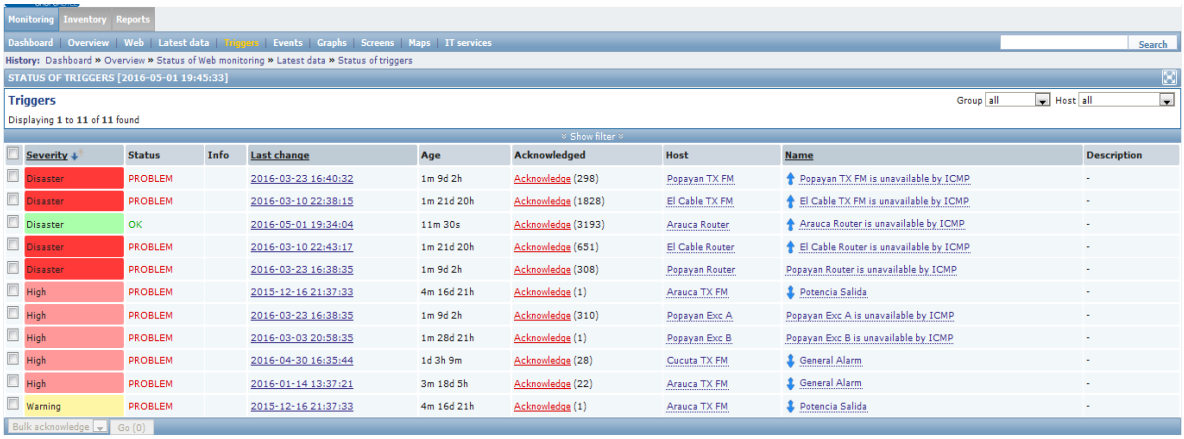
Status widgets: muestra el estado de los hosts, del sistema y de los últimos 20 estados.



Overview: visión general del estado de los triggers de varios hosts a la vez.

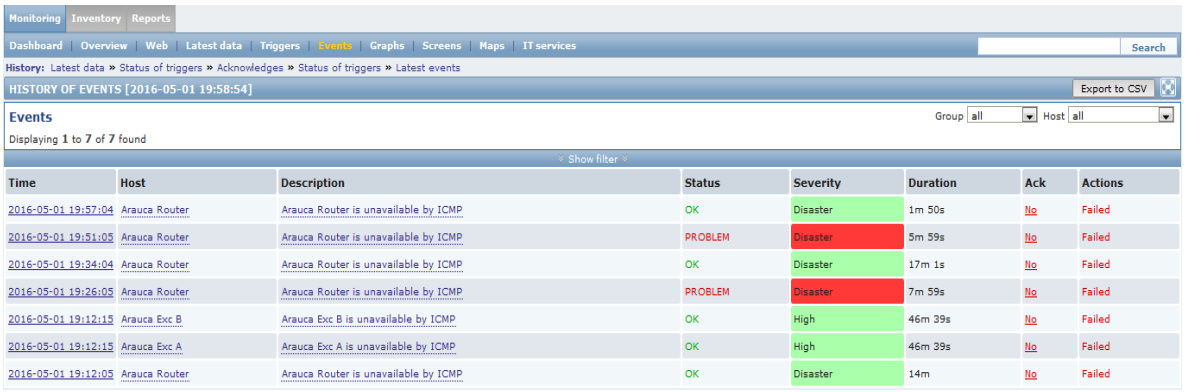


Triggers (disparadores): muestra el estado de los disparadores por columnas.



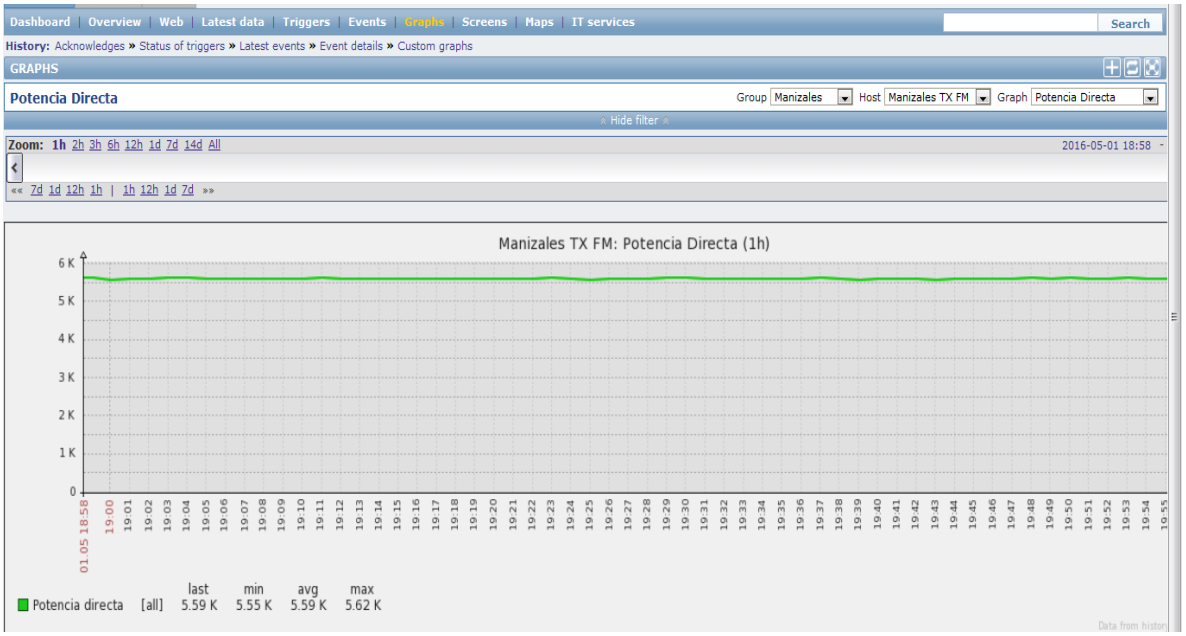
Severity: muestra el grado de severidad High, Warning, etc.
Status: muestra el estado Problem u Ok.
Last change: muestra cuando se ha realizado el último cambio de estado del trigger.
Acknowledged: indicador de trigger reconocido.
Host: Indica el nombre del host a donde está el trigger.
Name: nombre del Trigger.

Events: muestra los últimos eventos ocurridos

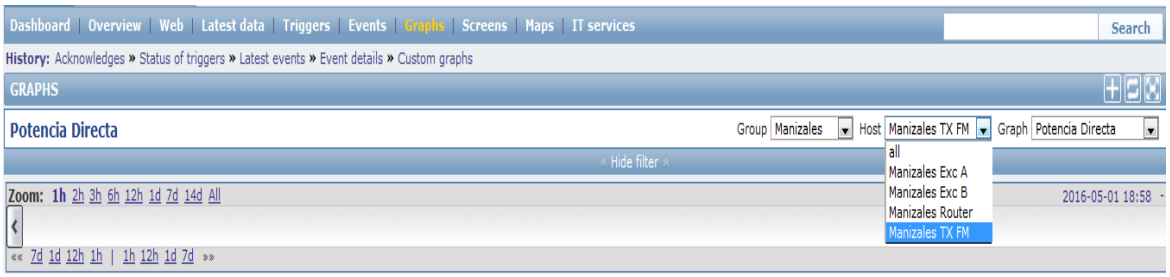


Time	Host	Description	Status	Severity	Duration	Ack	Actions
2016-05-01 19:57:04	Arauca Router	Arauca Router is unavailable by ICMP	OK	Disaster	1m 50s	No	Failed
2016-05-01 19:51:05	Arauca Router	Arauca Router is unavailable by ICMP	PROBLEM	Disaster	5m 59s	No	Failed
2016-05-01 19:34:04	Arauca Router	Arauca Router is unavailable by ICMP	OK	Disaster	17m 1s	No	Failed
2016-05-01 19:26:05	Arauca Router	Arauca Router is unavailable by ICMP	PROBLEM	Disaster	7m 59s	No	Failed
2016-05-01 19:12:15	Arauca Exc B	Arauca Exc B is unavailable by ICMP	OK	High	46m 39s	No	Failed
2016-05-01 19:12:15	Arauca Exc A	Arauca Exc A is unavailable by ICMP	OK	High	46m 39s	No	Failed
2016-05-01 19:12:05	Arauca Router	Arauca Router is unavailable by ICMP	OK	Disaster	14m	No	Failed

Graphs(gráficos): muestra los gráficos que se han configurado.



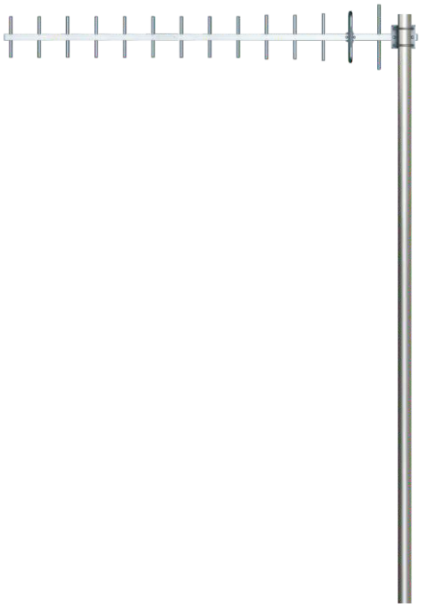
Para visualizar la gráfica anterior, se escoge el grupo de hosts, el host y la gráfica que esté configurada. En el ejemplo anterior, se ve Potencia Directa en función del tiempo en horas: minutos del transmisor FM de Manizales perteneciente al grupo Manizales.



6.4. Antena Yagi

Electrical Data

Frequency:	824-896 MHz
Gain:	16 dBi
VSWR:	<1.5:1
Polarization:	Horizontal Or Vertical
Horizontal Beamwidth :	28°
Vertical Beamwidth:	25°
Nominal Impedance:	50 Ohms
F/B Ratio:	>20 dB
Max Input Power:	100 W
Lightning Protection:	DC Ground

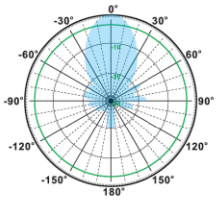


Mechanical Data

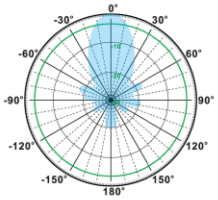
Connector :	N Female
Dimension:	1510mm/59.45in
Weight:	0.6kg/1.32lb
Cable Length:	360mm/14.17in
Reflector Material:	Aluminum Alloy
Antenna Material:	Mast
Mast Size:	Ø40-Ø60mm
Rated Wind Velocity:	210km/h
Operating temperature:	-40~+65℃

Shipment Data

Packing Qty:	10pcs/Carton
Carton Size:	980*440*365mm
(length*width*height)	38.6*17.3*14.4in
Packing Weight:	8.2kg/18.06lb



H-Plane



V-Plane