Tesis de Máster

Instalación y configuración de un supernodo de la red abierta Guifi.net en la U.P.V.

Autor: Vicente Javier Ortiz Gallart
Director: Pietro Manzoni

Máster en Ingeniería de Computadores
Depto. de Informática de Sistemas y Computadores

RESUMEN

En este trabajo se analizan uno a uno los pasos que han sido necesarios para crear un supernodo de la red ciudadana inalámbrica Guifi.net dentro de la Universidad Politécnica de Valencia.

Se hace, en primer lugar, una pequeña incursión por la filosofía e historia de la red abierta y sobre la tecnología Wifi, con una visión global de conceptos, técnicas, protocolos y materiales que van a ser utilizados.

A continuación se ejecuta prácticamente la instalación física del supernodo, del equipo servidor y del cliente con sus conexiones, y se realiza el estudio de dicha instalación desde un punto de vista técnico, analizando tanto la parte física (instalación hardware de las antenas, router, equipos…), como la parte de red (direccionamiento IP, encaminamiento…) y la de aplicación (instalación del servidor y los servicios ofrecidos).

También se desarrolla la gestión y configuración de los distintos elementos y aplicaciones de red, con las herramientas apropiadas para cada uno de ellos, y se realizan conexiones VPN con la UPV y el servidor Guifi.net de la Universidad Jaume I de Castellón.

Por último se analizan las prestaciones de throughput de la red, y se realiza un estudio comparativo de los valores obtenidos con las pruebas realizadas en los diferentes escenarios de red planteados.

AGRADECIMIENTOS

A muchas personas tengo que dedicar este apartado, ya que de una manera u otra muchos son los que han contribuido para que pudiera dedicar el tiempo necesario o me han ayudado con sus conocimientos a poder llevar a buen fin el máster y su tesis, desde mi familia a compañeros de la Universidad o la Escuela.

Pero sí que quiero destacar a mis compañeros del servicio de informática de la ETSINF, en especial a Juan Verdú y Emilio Bayo, por su continuo apoyo y colaboración.

A Miguel Pérez y Pablo Boronat, profesores de la Universidad Jaume I de Castellón e importantes miembros de Guifi.net en Castellón, sin cuya ayuda hubiera sido imposible la realización del nodo y, por consiguiente, de la tesis.

A Pietro Manzoni por su dirección en la tesis, porque siempre ha estado disponible y porque, en todo momento, sus ideas y consejos me han facilitado la realización de este proyecto.

INDICE GENERAL

A. Índice de tablas i

B. Índice de figuras y gráficos iii

INTRODUCCIÓN 1

I.1.-Justificación 1

I.2.-Objetivo 2

I.3.-Estructura del estudio 2

CAPÍTULO 1: REDES ABIERTAS Y LIBRES: GUIFI.NET 5

1.1.-Beneficios de la red abierta 6

1.2.-Diferencias con el modelo clásico 6

1.3.-Redes abiertas y libres en el mundo. 7

1.4.-La red Guifi.net: el principio "XOLN" 9

1.5.-Historia de Guifi.net 10

1.6.-Elementos de la red Guifi.net 12

1.6.1.-Nodos simples de los usuarios. 12

1.6.2.-Supernodos. 13

1.6.3.-Enlaces 13

1.6.4.-Troncal. 13

1.6.5.-Puntos de acceso. 13

1.6.6.-Trastos 13

1.6.7.-Proxys. 14

1.7.-Topología de la red 14

1.7.1.-Red Troncal 14

1.7.2.-Red de usuario 15

CAPÍTULO 2: CONCEPTOS Y TECNOLOGÍAS WIRELESS 17

2.1.-Redes Mesh: el estándar 802.11s 17

2.1.1.-Redes Mesh 17

2.1.2.-Estándar 802.11s 17

2.2.-La tecnología WIFI (802.11) 19

2.3.-Estandares WIFI 19

2.4.-Factores que influyen en la señal WIFI 20

2.4.1.-La claridad de la señal 20

2.4.1.1.-Potencia de la señal 20

2.4.1.2.-Distancia 20

2.4.1.3.-Interferencias 21

2.4.1.4.-Línea de visión 21

2.4.2.-Transmisión de la señal 21

2.4.3.-Enfocar la señal 22

2.4.4.-Línea de visión (LOS) 22

2.4.5.-Posición estable de la antena 23

2.5.-Protocolos de cifrado 23

2.6.-Bandas de frecuencia 24

2.7.-Canales de frecuencia 25

2.7.1.-Canales Wifi permitidos en España 25

2.7.1.1.-Banda de 2,4 GHz 25

2.7.1.2.-Banda de 5 GHz 25

2.8.-Modos de funcionamiento 26

2.8.1.-AD.HOC (IBSS) 26

2.8.2.-Infraestructure 26

2.8.2.1.-Basic Service Set (BSS) 26

2.8.2.2.-Extended Sevice Set (ESS) 26

2.9.-Protocolos de enrutamiento 27

2.9.1.-Enrutamiento estático 27

2.9.2.-Enrutamiento dinámico 27

2.9.2.1.-Proactivo (manejo por tablas) 27

2.9.2.2.-Reactivo (por demanda) 28

2.10.-Múltiple Input/múltiple Output (MIMO) 28

2.11.-Hardware Wireless 29

2.11.1.-Componentes para crear una red Wifi 29

2.11.1.1.-Punto de acceso (Access Point) 29

2.11.1.2.-Pasarela de enlace (Gateway) 29

2.11.1.3.-Router (Access Point + Gateway) 29

2.11.1.4.-Clientes inalámbricos 29

2.12.-Antenas 30

2.12.1.-Patrón de radiación 30

2.12.2.-Tipos de antenas por patrón de radiación 31

2.12.2.1.-Antenas direccionales 31

2.12.2.2.-Antenas omnidireccionales 32

2.12.2.3.-Antenas sectoriales 32

2.12.3.-Otras características de las antenas 32

2.12.3.1.-Polarización 32

2.12.3.2.-Ganancia 32

2.12.3.3.-Unidades de ganancia 33

2.12.3.4.-Ancho de haz 33

CAPÍTULO 3: INSTALACIÓN FÍSICA DEL SUPERNODO UPV 35

3.1.-Acciones Iniciales 35

3.2.-Componentes y material usado en la instalación 36

3.3.-Breve descripción de componentes 36

3.3.1.-Antena parabólica 36

3.3.2.-Router y radios de 5 GHz 37

3.3.3.-Antena sectorial 39

3.3.4.-Antena hotspot 39

3.3.5.-Caja estanca de aluminio 39

3.4.-Instalación del supernodo en el exterior..... 40

3.4.1.-Esquema de montaje 40

3.4.2.-Consideraciones de montaje 41

3.4.3.-La instalación paso a paso 41

3.4.3.1.-Preparación de la Routerboard en la caja estanca..... 41

3.4.3.2.-Preparación de la antena parabólica 43

3.4.3.3.-Instalación del cableado del armario a la terraza..... 44

3.4.3.4.-Traslado del material al punto de montaje..... 45

3.4.3.5.-Instalación de los soportes del mástil. 45

3.4.3.6.-Colocación caja del router y antenas en el mástil..... 45

3.4.3.7.-Cableado router y antenas..... 46

3.4.3.8.-Colocación del mástil en sus soportes y de los tensores..... 47

3.4.3.9.-Cableado y orientación de las antenas. 48

3.4.3.10.-Test de funcionamiento 49

CAPÍTULO 4: CONFIGURACIÓN DE LAS ANTENAS..... 51

4.1.-Dar de alta una nueva zona 51

4.1.1.-Crear un nodo multirradio..... 52

4.1.2.-Esquema de red y componentes del supernodo de la UPV..... 52

4.2.-Creamos el supernodo VLCUPVGRC (UPVone) 53

4.2.1.-Dar de alta usuario y trastos en Guifi.net..... 53

4.2.2.-Reserva de direcciones IP para conexiones de cable 55

4.2.3.-Añadir el routerboard para el nodo multirradio 55

4.2.3.1.-Modelo de dispositivo, firmware y dirección MAC 56

4.2.3.2.-Recomendaciones para los ESSID..... 56

4.2.4.-Configurar los radios y WLANs: rango de IP, orientación… 57

4.2.4.1.-Recomendaciones para los canales 57

4.2.4.2.-Configuración de los radios 57

4.3.-Con «unsolclic» preparar el archivo de configuración. 61

4.4.-Bajar y cargar el fichero de configuración del Mikrotik. (Winbox) 62

4.5.-Configurar el hotspot 63

CAPÍTULO 5: AÑADIR UN SERVIDOR Y SERVICIOS 67

5.1.-Añadir un servidor 67

5.1.1.-Elección del servidor y los servicios 67

5.1.2.-Dar de alta el servidor en Guifi.net 68

5.1.3.-Instalación del sistema operativo Ubuntu server 70

5.1.4.-Instalación de HERRAMIENTAS 72

5.1.4.1.-Instalación de Webmin 72

5.1.4.2.-Instalación de NX 72

5.1.4.3.-Instalación de Wine 73

5.1.4.4.-Instalación de Winbox 73

5.2.-Servicios 75

5.2.1.-Servidor Web (Apache2 + PHP5) 75

5.2.1.1.-Instalación de Apache2 en nuestro servidor Ubuntu 75

5.2.1.2.-Instalación de PHP5 77

5.2.1.3.-Dar de alta el servicio en la UPV para que salga a Internet 77

5.2.2.-Servidor DNS (dnsmasq) 78

5.2.2.1.-El servidor de nombres DNSmasq 78

5.2.2.2.-Instalación del servidor dnsmasq 78

5.2.2.3.-Configuración del servidor DNS 78

5.2.2.4.-Arranque y parada del servidor dnsmasq 80

5.2.3.-Servidor de Gráficas 80

5.2.3.1.-Para la web de guifi.net 81

5.2.3.2.-Para la web del servidor VLCUPVGRC 88

CAPÍTULO 6: NODO CLIENTE 97

6.1.-Instalación del nodo 97

6.2.-Conexión de la nanostation5. 98

6.3.-Crear cuenta usuario, nodo y radio 99

6.3.1.-Alta de usuario en la web guifi.net 99

6.3.2.-Alta del nodo en la web Guifi.net 101

6.3.3.-Añadimos un radio al nodo 102

6.4.-Configuración del nodo 104

6.4.1.-Preparamos el archivo de configuración de la Nanostation 104

6.4.2.-Configuramos la Nanostation (descarga del fichero) 106

6.5.-El cliente móvil: hotspot 107

6.5.1.-Conexión a la antena hotspot 107

CAPÍTULO 7: CONEXIONES VPN 109

7.1.-Salimos de la isla. 109

7.2.-Conexión VPN 109

7.2.1.-Usos de las VPNs 110

7.2.2.-Ventajas principales 110

7.2.3.-OpenVPN 110

7.3.-Túnel con Guifi.net Castellón 110

7.3.1.-Establecemos el túnel 111

7.4.-Túnel con la UPV 115

7.4.1.-VLAN 830 115

7.4.2.-Conexión al servidor VPN 117

7.4.3.-Configuración del servidor VPN 118

7.4.4.-Configuración del cliente VPN 120

CAPÍTULO 8: ESTUDIO DE PRESTACIONES 123

8.1.-Objetivos. 123

8.2.-Metodología. 125

8.2.1.- Parámetros a analizar 125

8.2.2.- Herramientas 127

8.2.2.1.-Iperf 127

8.2.2.2.-Jperf 128

8.2.3.- Procedimiento 130

8.2.4.- Acciones iniciales 132

8.3.- Resultados de las pruebas con Jperf. 133

8.3.1.-Sobre la red Guifi.net 133

8.3.1.1.-Prueba A (por tiempo) 133

8.3.1.2 -Prueba B (por bytes transmitidos) 138

8.3.2.-Sobre la red UPV 142

8.3.2.1.-Prueba C (por tiempo) 142

8.3.3.-Con conexión directa a Internet 147

8.3.3.1.-Con 1 stream y 1024 bytes de tamaño de paquete 147

8.3.3.2.-Con 10 streams y 1024 bytes de tamaño de paquete 147

8.4.-Resultado de las pruebas con Wget 148

8.4.1.-Desde la red Guifi.net 148

8.4.2.-Desde la red UPV 148

8.4.3.-Con conexión directa a Internet 149

8.5.-Evaluación y conclusiones de las pruebas. 149

8.5.1.- Con Jperf 149

8.5.1.1.- De la transmisión sobre la red Guifi.net 149

8.5.1.2.- Comparación de las redes Guifi.net y UPV (sobre VPN) 151

8.5.1.3.- Comparación de las redes Guifi.net y conexión directa Internet 152

8.5.2.- Con Wget 153

8.5.2.1.- Comparación de las redes Guifi.net y UPV (sobre VPN) 153

8.5.1.3.- Comparación con la conexión directa a Internet 153

CONCLUSIONES Y LINEAS FUTURAS DE TRABAJO 155

Conclusiones. 155

Líneas futuras de trabajo 156

ANEXO A: GLOSARIO DE TÉRMINOS 157

ANEXO B: COMPONENTES Y CARACTERÍSTICAS TÉCNICAS 161

B.1.- Routerboard 161

B.2.- Mikrotik R52N 162

B.3.- RocketDish (antena parabólica) 163

B.4.- Rocket M5 (antena parabólica) 164

B.5.- NanoStation2 (antena Hotspot) 165

B.6.- Interline INT-SEC-17/50 (antena Sectorial) 167

B.7.- Cable coaxial RF 5 GHZ. 168

B.8.- Pigtail 168

ANEXO C: SCRIPTS Y ARCHIVOS DE CONFIGURACIÓN 169

C.1.- Scripts de configuración "Unsoloclic" 169

C.1.1.-Configuración del Mikrotik (RouterOs) de UPVone 169

C.1.2.-Configuración del NanoStation (AirOs) de UPVdos 173

C.2.- Archivos de configuración de servicios 176

C.2.1.-Servidor de DNS (dnsmasq) 176

C.2.1.1.-/etc/dnsmasq.conf 176

C.2.1.2.-/etc/resolv.conf 176

C.2.1.3.-/etc/host 176

C.2.2.-Servidor de gráficas de la web de Guifi.net 176

C.2.2.1.-/etc/snpservices/config.php 176

C.2.2.2.-/var/www/snpservices/data/mrtg.cfg 178

C.2.3.-Servidor de gráficas de la web de VLCupvGRC 181

C.2.3.1.-/etc/mrtg.cfg 181

C.2.3.2.-/var/www/mrtg.html 185

BIBLIOGRAFÍA 189

Índice de tablas

Tabla 8.1. Bandwidth para un solo nodo
Tabla 8.2. Bandwidth para un solo nodo variando nº nodos
Tabla 8.3. Bandwidth para un solo nodo variando paquete
Tabla 8.4. Bandwidth para toda la transmisión
Tabla 8.4. Transferencia de un solo nodo
Tabla 8.5. Transferencia de toda la transmisión
Tabla 8.6. Diferencia de bandwidth entre nodos por tamaño paquete
Tabla 8.7. Diferencia de bandwidth por nodo
Tabla 8.8. Bandwidth para un solo nodo B
Tabla 8.9. Bandwidth para un solo nodo variando nº nodos B
Tabla 8.10. Bandwidth para toda la transmisión B
Tabla 8.11. Tiempo necesario para la transmisión B
Tabla 8.12. Diferencias de tiempo entre nodos por tamaño de paquete
Tabla 8.13. Diferencias de tiempo por nodo con tamaño de paquete fijo
Tabla 8.14. Bandwidth para un solo nodo C
Tabla 8.15. Bandwidth para un solo nodo variando nº nodos C
Tabla 8.16. Bandwidth para un solo nodo variando paquete C
Tabla 8.17. Bandwidth para toda la transmisión C
Tabla 8.18. Transferencia de un solo nodo C
Tabla 8.19. Transferencia de toda la transmisión C
Tabla 8.20. Diferencia de bandwidth por nodo C
Tabla 8.21. Bandwidth por nodo Guifi-UPV
Tabla 8.22. Bandwidth total en la transmisión Guifi-UPV
Tabla 8.23. Bandwidth por nodo Guifi-Rediris
Tabla 8.24. Bandwidth total en transmisión Guifi-Rediris

Índice de figuras y gráficos

Figura 1.1. Diferencias modelos de red cerrada y abierta
Figura 1.2. Curva de crecimiento Guifi.net
Figura 1.3. Cronología de red Guifi.net
Figura 1.4. Nodos y supernodos
Figura 1.5. Fotografía del supernodo
Figura 1.6. Fotografía de Punto acceso
Figura 1.7. Diagrama de conexiones troncales de una red mesh
Figura 1.8. Dibujo de la red de usuario
Figura 2.1. Red Mesh
Figura 2.2. Cronología del estándar 802.11
Figura 2.3. El estándar 802.11
Figura 2.4. La transmisión de la señal inalámbrica
Figura 2.5. La línea de visión (LOS)
Figura 2.6. La banda de frecuencia de 2,4 GHZ
Figura 2.7. La banda de frecuencia de 5 GHZ
Figura 2.8. Funcionamiento Ad-Hoc
Figura 2.9. Funcionamiento modo Infraestructura
Figura 2.10. Patrón de radiación
Figura 2.11. Patrón de radiación 3D
Figura 2.12. Antenas direccionales
Figura 2.13. Antenas omnidireccionales
Figura 2.14. Antenas sectoriales
Figura 2.15. Polarización
Figura 3.1. Fotografía de la antena parabólica
Figura 3.2. Fotografía Rocket M5 2x2 MIMO
Figura 3.3. Fotografías conexión Rocket M5
Figura 3.4. Fotografía Routerboard RB493AH
Figura 3.5. Fotografía Inyector POE
Figura 3.6. Fotografía Mikrotik R52n
Figura 3.7. Fotografía Routerboard con Mikrotik
Figura 3.8. Fotografía “pigtail”
Figura 3.9. Fotografías antena sectorial

Figura 3.10. Fotografía conexión pigtail-N.macho
Figura 3.11. Fotografía Nanostation M2 (Hotspot)
Figura 3.12. Fotografía caja estanca aluminio
Figura 3.13. Esquema de instalación del supernodo UPV
Figura 3.14. Fotografías preparación caja
Figura 3.15. Fotografía colocación radios en router
Figura 3.16. Fotografía colocación pigtails
Figura 3.17. Fotografía colocación conectores N-macho
Figura 3.18. Fotografías ensamblado antena parabólica
Figura 3.19. Fotografías ensamblado Rocket M5 en Rocket Dish Base
Figura 3.20. Fotografía roseta tejado
Figura 3.21. Fotografía cableado hasta armario red
Figura 3.22. Fotografías de vistas generales de la terraza
Figura 3.23. Fotografía y gráfico de los soportes del mástil
Figura 3.24. Fotografías de la colocación antenas y router en el mástil
Figura 3.25. Fotografías del cableado entre antenas y router
Figura 3.26. Fotografía de los tensores del mástil
Figura 3.27. Fotografía del cableado del nodo hacia la roseta
Figura 3.28. Fotografía de la roseta del tejado
Figura 3.29. Fotografía de los inyectores POE en el armario
Figura 3.30. Fotografía de las conexiones en el armario de red
Figura 3.31. Fotografía de las conexiones en el switch
Figura 3.32. Captura de las señales del test de funcionamiento
Figura 3.33. Fotografía de la instalación final con los que intervinieron en ella.
Figura 4.1. Página de inicio de la web de Guifi.net
Figura 4.2. Esquema de red del nodo UPVone de la UPV
Figura 4.3. Página web del nodo UPVone en Guifi.net
Figura 4.4. Vista detallada de la ubicación
Figura 5.1. Fotografía del servidor VLCupvGRC
Figura 5.2. Conexión del servidor de gráficas con el servidor Guifi.net
Figura 5.3. Tipos de gráficas que proporciona el servidor de gráficas
Figura 5.4. Gráfica de “ifspeed”
Figura 5.5. Gráfica general de todas las interfaces
Figura 5.6. Gráficas individuales de cada interface
Figura 6.1. Línea de visión de las antenas
Figura 6.2. Equipo del nodo cliente
Figura 6.3. Antena

Figura 6.4. Inyector POE
Figura 6.5. Vista detallada de ubicación del nodo cliente UPVdos
Figura 6.6. Antena hotspot
Figura 6.7. Gráfica de selección de la antena y tráfico de la conexión al hotspot
Figura 7.1. Esquema de conexiones VPN
Figura 7.2. Tabla de rutas del routerboard
Figura 7.3. Acceso a la Web de Castellón desde la red Guifi.net
Figura 7.4. Diagrama de conexiones de la VLAN 830
Figura 7.5. Puertos del switch configurados en la VLAN 830
Figura 7.6. Esquema de los elementos conectados a la VLAN 830
Figura 7.7. Nuestro túnel en el servidor de VPN de la UPV
Figura 7.8. Esquema de las redes VPN de la UPV
Figura 7.9. Web de configuración de VPN
Figura 8.1. Esquema del trayecto por la red Guifi.net
Figura 8.2. Esquema del trayecto por la red UPV
Figura 8.3. Esquema del trayecto directo a Internet
Figura 8.4. Esquema conexión Iperf cliente-servidor
Figura 8.5. Elementos de la pantalla de Jperf.
Figura 8.6. Ejemplo gráfico de resultado de Jperf
Figura 8.7. Bandwidth un solo nodo por tamaño de paquete
Figura 8.8. Bandwidth un solo nodo por nodos en paralelo
Figura 8.9. Bandwidth para un solo nodo variando nº nodos
Figura 8.10. Bandwidth para un solo nodo variando paquete
Figura 8.11. Bandwidth para toda transmisión por tamaño paquete
Figura 8.12. Bandwidth para toda transmisión por nodos en paralelo
Figura 8.13. Transferencia de un solo nodo por tamaño paquete
Figura 8.14. Transferencia de un solo nodo por nodos en paralelo
Figura 8.15. Transferencia de toda la transmisión por tamaño paquete
Figura 8.16. Transferencia de toda la transmisión por nodos en paralelo
Figura 8.17. Diferencia de bandwidth entre nodos por tamaño paquete
Figura 8.18. Diferencia de bandwidth por nodo
Figura 8.19. Bandwidth para un solo nodo por tamaño paquete B
Figura 8.20. Bandwidth para un solo nodo por nodos en paralelo B
Figura 8.21. Bandwidth para un solo nodo variando nº nodos B
Figura 8.22. Bandwidth para toda transmisión por tamaño paquete B
Figura 8.23. Bandwidth para toda transmisión por nodos en paralelo B
Figura 8.24. Tiempo necesario para la transmisión por tamaño paquete

Figura 8.25. Tiempo necesario para la transmisión por nodos en paralelo
Figura 8.26. Diferencias de tiempo entre nodos por tamaño de paquete por nodo
Figura 8.27. Diferencias de tiempo entre nodos por tamaño paquete
Figura 8.28. Diferencias de tiempo por nodo con tamaño de paquete fijo
Figura 8.29. Bandwidth para un solo nodo por tamaño paquete C
Figura 8.30. Bandwidth para un solo nodo por nodos en paralelo C
Figura 8.31. Bandwidth para un solo nodo variando nº nodos C
Figura 8.32. Bandwidth para un solo nodo variando paquete C
Figura 8.33. Bandwidth para toda transmisión por tamaño paquete C
Figura 8.34. Bandwidth para toda transmisión por nodos en paralelo C
Figura 8.35. Transferencia de un solo nodo por tamaño paquete C
Figura 8.36. Transferencia de un solo nodo por nodos en paralelo C
Figura 8.37. Transferencia de toda la transmisión por tamaño paquete C
Figura 8.38. Transferencia de toda la transmisión por nodos en paralelo C
Figura 8.39. Diferencia de bandwidth por nodo C
Figura 8.40. Conexión directa a Internet con 1 stream
Figura 8.41. Conexión directa a Internet con 10 streams
Figura 8.42. Bandwidth por nodo Guifi-UPV
Figura 8.43. Bandwidth total en la transmisión Guifi-UPV
Figura 8.41. Bandwidth por nodo Guifi-Rediris
Figura 8.42. Bandwidth total en transmisión Guifi-Rediris

INTRODUCCIÓN

La realidad, hoy por hoy, demuestra que las redes informáticas, se han vuelto indispensables, tanto para las personas como para las organizaciones ya que dan la oportunidad de interactuar con el resto del mundo, ya sea por motivos comerciales, personales o culturales.

Dentro de las redes, las posibilidades que ofrece la tecnología de comunicaciones de datos inalámbricos han facilitado que por todas partes se hayan construido múltiples comunidades independientes, con el objetivo principal de conectar usuarios distantes para así poder poner en común recursos y servicios.

Las comunidades "WiFi" proporcionan notables beneficios, puesto que hoy en día la tecnología crea excedentes en recursos que no siempre se aprovechan de forma particular, y que si se ponen en común proporcionan acceso a estos recursos al resto de la comunidad.

Un ejemplo claro de estas comunidades es la red Guifi.net que se puede definir como una red IP en expansión, a la cual se tienen que aplicar los mismos criterios de diseño y administración.

Esta tesis es un estudio técnico, con su materialización práctica, de un "supernodo" que conecte la red Guifi.net a la Universidad Politécnica de Valencia (UPV) y por ende al norte de la ciudad de Valencia.

I.1.-Justificación

La propuesta por hacer un modelo de red abierta en contraposición a las redes cerradas crea unas oportunidades que no se pueden potenciar con los modelos de redes cerradas. Creando una red abierta se favorece el desarrollo personal y social dentro del entorno donde se está desarrollando y es un ejemplo claro de inclusión digital, mucho más allá de la lucha contra la fractura digital.

La capacidad para gestionar infraestructuras de comunicaciones fuera de las operadoras tradicionales, favorece la aparición de otros grupos que realizan la gestión de tales infraestructuras basándose en modelos de "Xarxa Oberta Lliure i Neutral" (XOLN) lo que hace que el acceso a la tecnología y la comunicación sea cada vez más asequible en términos de costes y favorece su distribución para las personas interesadas.

La Universidad Politécnica de Valencia no puede quedarse fuera de este proyecto, participando en el desarrollo de esta red, por lo que supone una importante herramienta que aporta conocimientos

sobre las tecnologías y la sociedad de la información, la comunicación y la sensibilidad social hacia otros sectores, quizás no tan desarrollados. Además de facilitar con todo ello a la comunidad universitaria el acceso a los servicios que nos proporciona esta red inalámbrica de una manera deslocalizada, flexible y ubicua.

I.2.-Objetivo

La misión principal del proyecto es diseñar, implantar y configurar una infraestructura para el desarrollo de una red de telecomunicaciones libre, abierta y neutral integrada en la red guifi.net, que ayude a su implantación en Valencia y con ello, a que sus habitantes en general y los miembros de la Universidad Politécnica de Valencia en particular, puedan conocer y participar en la evolución de esta red y los servicios que ofrece.

Los objetivos que se plantean en el proyecto son los siguientes:

- Diseñar, instalar y explotar una red de telecomunicaciones abierta, libre y neutral que permita conectar entre sí, a la red libre y, en su caso, a la red de la universidad a los participantes en el proyecto.
- Favorecer el acceso a las Tecnologías de la Información y las Comunicaciones que la iniciativa proporciona y con ello permitir explotar el potencial de la red.
- Aprovechar las facilidades de red abierta para mejorar la formación en redes de los alumnos de informática del centro y de la universidad.
- Fomentar la innovación tecnológica por parte de las entidades que deseen participar en el proyecto, haciéndolos partícipes del desarrollo de esta red de telecomunicaciones.
- Ampliar la cobertura y el ámbito de aplicación de las redes propias de la universidad, haciendo llegar los servicios de red que ofrezcan hasta las casas de los miembros de la comunidad mediante el uso de la red guifi.net.
- Disponer de un servidor que ofrezca los servicios que proporciona esta red y que puedan ser explotados tanto desde las redes privadas de la Universidad como desde la red pública Guifi.net.

I.3.-Estructura del estudio

La tesis se ha estructurado en diferentes capítulos, intentando introducir en una primera parte los conceptos y tecnologías de la red abierta y libre Guifi.net para posteriormente centrarnos en la instalación, configuración y desarrollo del supernodo de la red en la UPV con sus servicios y, por

último, realizar un estudio de las prestaciones que ofrece la red.

La estructura de los capítulos es la siguiente:

- Lo primero que vemos es una introducción donde se motiva y justifica la realización del proyecto, así como los objetivos que se pretenden obtener.

- En un primer capítulo se presenta una pequeña visión de lo que es una red abierta con sus conceptos principales y los beneficios que proporciona, así como las más importantes que existen hoy en día. Seguidamente se da a conocer la comunidad GUIFI.NET con su historia, fundamentos, elementos de la red y su topología.

- En el capítulo dos, se introducen las tecnologías que son aplicables a este proyecto.

- En los capítulos tres y cuatro nos adentramos en lo que es el desarrollo de la instalación del supernodo de la Guifi.net en la UPV empezando por los contactos y permisos necesarios y compra del material, para continuar con la configuración del router y las antenas, dentro de la red Guifi.net, en el despacho y la instalación física de las antenas y resto de material en la azotea.

- En el quinto capítulo se describen los pasos de implementación del servidor y de los servicios necesarios para que los usuarios puedan conectarse a la red.

- El capítulo seis tratará de cómo se conecta un nodo cliente a la red Guifi.net.

- Para poder acceder a los servicios de la red Guifi.net y de la UPV se configuran dos VPNs (red privada virtual) lo que se desarrolla en el capítulo siete.

- El octavo capítulo se dedica a testear la red para valorar las prestaciones que puede proporcionar.

- Para finalizar, se presentan las conclusiones que se han obtenido, las líneas de trabajos futuros para la ampliación y mejora del nodo y la expansión de la red y, por último, en los anexos se recoge toda la información técnica y documentación que ha sido necesaria para implementar el estudio, así como los scripts y archivos de configuración más importantes en la instalación.

CAPÍTULO 1:

REDES ABIERTAS y LIBRES: GUIFI.NET

Una comunidad wireless consiste en grupos de voluntarios que pretenden construir redes informáticas libres y gratuitas alternativas a las redes personales gestionadas por empresas. Para este fin se utilizan tecnologías inalámbricas a través de frecuencias de radio de 2,4 o 5 GHz, ya que son libres y no requieren licencia para su uso. El objetivo de estas comunidades de usuarios no es sólo conectarse a Internet, sino que se trata de crear otra red que sea gestionada por los propios usuarios. También pretende acercar la tecnología a la sociedad, prestar servicios a los ciudadanos y crear nuevos canales gratuitos de comunicación entre personas.

Está basada en una red de área metropolitana (Wireless Metropolitan Area Network) pensada para crear un entorno de red entre ordenadores o terminales situados en un entorno definido y de una manera inalámbrica. Ponen la disposición de todo aquel que quiera participar, y disponga de infraestructura, la posibilidad de conectarse a ella, mediante un nodo propiedad del usuario, y obtener así todas las posibilidades que la red ofrece, generándose el concepto de "***Red Abierta (RA)"*** que en un sentido amplio se puede definir como toda infraestructura de telecomunicaciones que puede ser utilizada, estudiada y mejorada por todo el mundo sin discriminación de ningún tipo.

Mediante este sistema de conexión cada usuario crea su tramo de interconexión con la red responsabilizándose de ella. Por lo tanto la red tiene un crecimiento vírico aumentando con cada usuario, no existiendo, teóricamente, barreras ni fronteras de crecimiento y creando así una Intranet, similar a la que pueden utilizar las grandes corporaciones o entidades bancarias, para su transferencia de archivos personales, comunicación o gestión, pero de manera inalámbrica, libre y abierta.

Dichas conexiones se establecen bajo el concepto de autoprestación de servicios. En este modelo cada uno conserva la titularidad de los recursos que ha aportado a la red y es libre de retirarlos siempre que lo desee. El único compromiso que cada miembro contrae cuando se une a la infraestructura existente mediante los recursos que él aporta, es el de extender las condiciones de acceso y el uso de la infraestructura existente sobre sus recursos. Este modelo de organización es lo que comúnmente se designa en lengua inglesa como *"ownerless networks"*.

Este tipo de red dispone de infinidad de aplicaciones, como salida a Internet, videoconferencia,

VoIP, transferencia de archivos etc. La red no tiene restricciones de ningún usuario ya que es de todos, ni de su contenido ya que cada uno es responsable del uso que le da.

1.1.-Beneficios del modelo de Red Abierta

- Oportunidad de contribución al conocimiento general al no restringir el derecho de copia, aplicación, desarrollo, etc.).

- Proporciona un acceso general, en lugar de "sólo para aquellos que lo puedan pagar" de los modelos más comerciales.

- Es mucho más eficiente en términos económicos ya que con la misma inversión se puede hacer llegar la infraestructura a más gente ya que no está orientada a conseguir beneficios.

- La infraestructura que se desarrolla es única, y por lo tanto, se evita la multiplicidad de la misma, típica en muchos modelos actuales para el desarrollo de infraestructura de telecomunicaciones. Lo que implica una reducción de los recursos y, consecuentemente, una reducción de costes y del impacto ambiental.

Por lo tanto, tal y como se demuestra prácticamente, este entorno aumenta considerablemente la sostenibilidad tanto económica como tecnológica del modelo.

Un ejemplo de comunidad wireless es la red **Guifi.net** que cuenta con más de siete años de experiencia y miles de usuarios, recibiendo y generando servicios libres y gratuitos.

1.2.- Diferencias con el modelo clásico

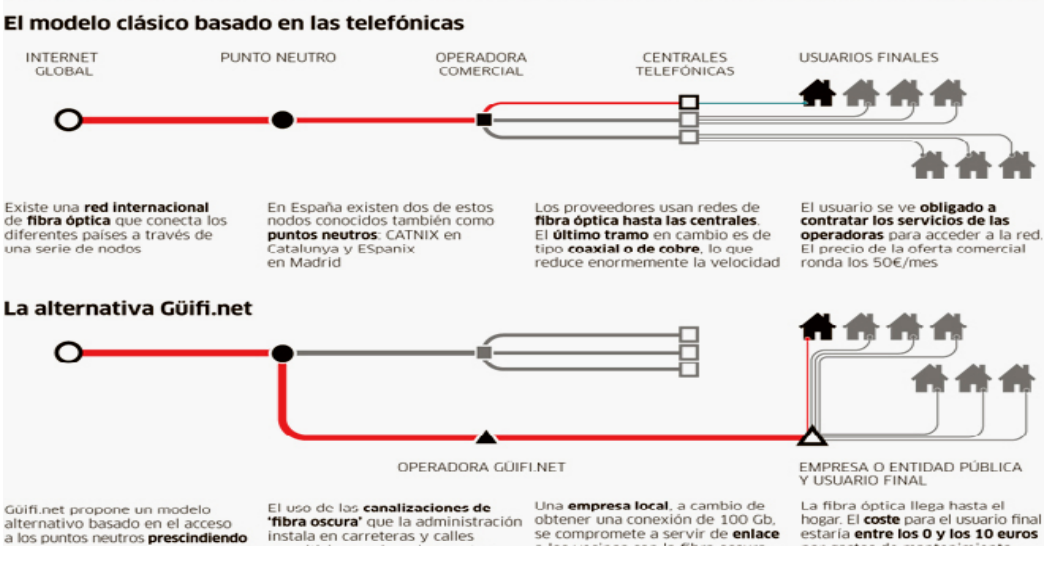


Figura 1.1. Diferencias modelos de red cerrada y abierta

1.3.- Redes abiertas y libres en el mundo

- **Awmn** (Athens Wireless Metropolitan Network): La red metropolitana de Atenas es la mayor red wireless de Europa y una de las mayores del mundo. Actualmente cuenta con más de 14.000 miembros y se extiende por varias islas griegas y de la costa de Turquía.

Iniciada en 2002 como una iniciativa social para proveer conectividad sin fines de lucro Opera en las bandas libres de 2,4 y 5GHz, utilizando varios protocolos entre los que se encuentran BGP (Border Gateway Protocol) y también OLSR. http://www.awmn.net/

- **Ninux.org:** Red italiana que nace en Roma y se extiende por varias decenas de kilómetros por las ciudades próximas contando con varios cientos de nodos. Utiliza el protocolo de encaminamiento OLSR. http://wiki.ninux.org/

- **PilsFree:** Una asociación cívica checa (Bohemia) que mantiene una de las redes más grandes con más de 10.000 asociados. Una característica es que se paga una cuota mensual a la asociación, pero no como una contrapartida a un compromiso de servicio de acceso a internet, sino como contribución a la asociación, lo que permite afrontar hasta cierto nivel algunas inversiones. La red da cobertura mediante una amplia red de fibra óptica y conexiones inalámbricas. http://www.pilsfree.net/

- **Freifunk:** Es una red mesh comunitaria basada en el protocolo OLSR que nació como una iniciativa para conectar ciertos sectores de Berlín. El crecimiento fue muy rápido y se desarrolló por otras ciudades europeas (Leipzig, Hannover, Dresden), que está utilizando un modelo de organización propio, con hardware y protocolos específicos. Cada usuario se compromete a darle servicio a otros mediante el contrato de "*picopeering*". Sus miembros han hecho importantes modificaciones al protocolo

OLSR para hacerlo más estable y escalable, denominándolo OLSRD (Optimizad Link State Router Daemon). http://start.freifunk.net/

NOTA: El acuerdo PicoPeering es un intento de conectar islas de redes comunitarias mediante un esqueleto mínimo de requerimientos de interconexión para un acuerdo equitativo entre usuarios.

- **CUWiN,** Red inalámbrica comunitaria (Illinois, EEUU). Es una iniciativa de desarrollo e investigación con una implementación de código abierto del protocolo de enrutamiento HSLS (Hazy Sighted Link State) desarrollado en MIT y el sistema operativo FreeBSD (variante de Unix de uso libre), apostando a una red AdHoc inalámbrica escalable y altamente robusta. http://cuwireless.net/

- **AirJaldi, Dharamsala Wireless,** (India). La red comunitaria de Dharamsala, se fundó después de la aprobación del uso del WiFi en exteriores en la India (28 de enero de 2005). Es una red comunitaria desplegada para el Tibetan Technology Center que conecta más de 2.000 PCs en terrenos montañosos alrededor de Dharamsala, una región al norte de la India y que, además, soporta la comunicación de la comunidad tibetana en el exilio.

- **Red MESH en el Instituto Meraka.** (Mpumalanga, Sudáfrica), La primera antena del Instituto Meraka fue hecha con una lata de metal y un trozo de rayo de bicicleta soldado a un conector especial que se puede conectar con una antena similar en otro punto a 5 kilómetros". http://www.meraka.org.za/

- **One Hundred Dollar Laptops.** (MIT, EEUU). Un proyecto del MIT que desarrolla "one hundred dollar laptops" para las escuelas en países en desarrollo. Planea utilizar el establecimiento de una red de malla para crear una infraestructura robusta y barata para los estudiantes que recibirán los ordenadores portátiles. Las conexiones instantáneas hechas por los ordenadores portátiles reducirían la necesidad de una infraestructura externa, como Internet, para alcanzar todas las áreas, porque un nodo conectado podría compartir la conexión con los nodos próximos. Actualmente sólo se ha implementado este sistema en un país entero en todo el mundo, Uruguay, a través del Plan Ceibal, Se basa en un programa originalmente pensado en Estados Unidos conocido como One Laptop Per Child (OLPC).

- **Doula,** (Camerún). Se instaló una red piloto por parte de una empresa comercial que despliega una red mallada inalámbrica utilizando postes de alumbrado público, donde la iluminación se provee mediante lámparas a LED (Light Emitting Diodes) que son más

eficientes y tienen menor impacto. La energía la obtienen de paneles fotovoltaicos montados en el mismo poste. www.starsightproject.com

- **Peebles Valley,** (Sudáfrica). Es un proyecto financiado por IDRC con el fin de explorar la factibilidad de la tecnología basada en 802.11 para aplicaciones rurales. Utiliza el protocolo OLSR y ofrece servicios de VoIP mediante un servidor Asterisk

http://www.fmfi.org.za/wiki/images/9/9d/FMFI_Mesh_PLC_FI_Brochure_Final.pdf

1.4.- La red Guifi.net: el principio "XOLN"

De forma coloquial se podría decir que Guifi.net es una "comunidad wireless", es decir, un grupo, cada vez más amplio, de personas con un gran interés por las telecomunicaciones en general y por las wifi (inalámbricas) en particular, que interconexionan entre sí sus ordenadores, servidores, y resto de dispositivos wifi para compartir archivos, aplicaciones e, incluso, la conexión a Internet y que se administra bajo unas condiciones comunes denominadas "el comuns sense fils" (2004) o los principios de la "Xarxa Oberta, Lliure i Neutral; XOLN" que definen lo que guifi.net es y realiza a un nivel más formal.

Es una red propiedad de todos los que la componen, que aceptan la licencia XOLN y que, a partir de los términos de este acuerdo de interconexión entre iguales, definen a Guifi.net como un proyecto tecnológico comunitario que tiene la finalidad de implementar una red de telecomunicaciones abierta, libre y neutral que se extiende con el tramo que incorpora cada participante al conectarse.

Es **abierta** porque los datos de configuración de la red se publican y se ofrece de forma universal a la participación de todos sin ningún tipo de exclusión o discriminación, y, por lo tanto, tienen la capacidad de mejorarla, mantenerla y ampliarla. La red no tiene una dependencia de ninguna empresa y los mismos usuarios pueden hacerse la conexión a la red.

Es **libre** porque no hay nadie que pueda poner restricciones y todos pueden hacer lo que quieran y disfrutar de las libertades independientemente de su nivel de participación en la red y sin imponer términos y condiciones que contradigan este acuerdo de forma unilateral.

Es **neutral** porque la red es independiente de los contenidos, no los condiciona y, así, pueden circular libremente. Dentro la red puede circular cualquier contenido que alguien necesite, de forma que los usuarios pueden acceder y producir contenidos independientemente de sus posibilidades financieras o condiciones sociales. Cuando se incorporan contenidos a la red en guifi.net se hace con el fin de estimular su aparición, gestionar mejor la red o simplemente como ejercicio de incorporar contenidos, pero en ningún caso con el objetivo de sustituir o bloquear otros contenidos

A nivel de usuario, se puede decir que se trata de que al conectar el ordenador a la red, en lugar de dar acceso sólo a Internet, se conecta con una serie de recursos y servicios compartidos y que, al conectarse, además participa en la propuesta de extender y hacer red.

Como se indica en el Principio básico final: ***El off-topic:*** **"**Guifi.net no es un foro de debate político, religioso, sexual o de actualidad. Guifi.net respeta todas las opiniones pero persigue un único objetivo: extender la red abierta. Para discutir sobre otros temas, existen otros foros en la red." (Fonts, 2009).

Con lo que en definitiva nos lleva a que el objetivo de Guifi.net es poner en común la infraestructura de red construida por múltiples iniciativas de redes inalámbricas, ya sean particulares, de comunidades, o de cualquier otra clase, y proporcionar los mecanismos de organización para que funcione y se gestione, además de ser un espacio de búsqueda y desarrollo para la adaptación de nuevas tecnologías a las finalidades que le son propias como red abierta.

1.5.-Historia de Guifi.net

En Cataluña, las primeras comunidades sin hilos aparecen hacia el año 2000 y presentan las mismas características de las que fueron pioneras como Seatlle Wireless, es decir, las primeras experiencias son de comunidades con pocos miembros, muy locales, y prácticamente sin comunicación entre ellas, con falta de recursos económicos y una tecnología aún incipiente.

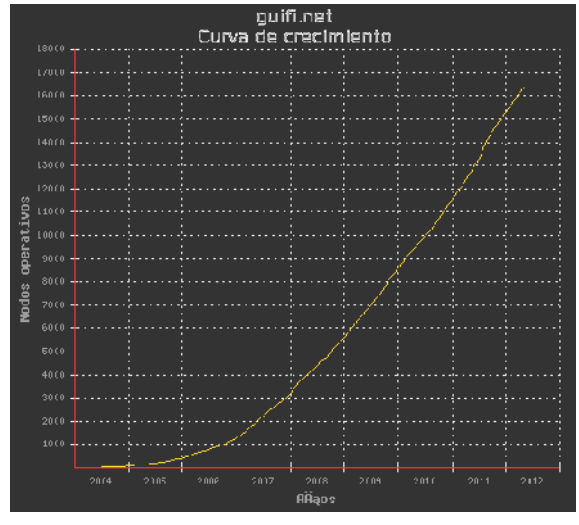


Figura 1.2. Curva de crecimiento Guifi.net

En abril de 2004 nace el proyecto guifi.net en el municipio de Gurb, comarca de Osona, para permitir el acceso a Internet de banda ancha en esta zona donde las operadoras no ofrecían este servicio. De ahí su nombre, Guifi, derivado de la contracción de las palabras "**Gu**rb" y "w**ifi**".

Una de sus características, desde su inicio, es que guifi.net no restringe su actuación al ámbito municipal sino que realiza enlaces con municipios vecinos. Otra característica propia es su capacidad de desarrollo de software, lo que le permite empezar a desarrollar aplicaciones.

En el plano legal, ya en el 2004 se redacta el acuerdo al que debería llegar cualquier usuario que quisiera entrar a la red; el *comuns sensefils (XOLN).*

En octubre de ese año recibían el Premio Vilaweb 2004.

En noviembre de 2006 el Consejo Nacional de Juventud de Catalunya le otorgó el premio al proyecto asociativo más innovador, por ser pionero en formas de participación en las que facilita recursos a comunidades e interconecta el mundo rural, a la vez que acerca a la juventud a las nuevas tecnologías da información y comunicación.

Guifi.net presenta unos resultados espectaculares a finales del 2006: más de 5.500 nodos declarados activos (dato que la convierte en la red más grande del mundo atendiendo a sus características).

En el mes de abril de 2007 fue finalista del Premio IGC (Ciudad del Conocimiento de Internet Global) Congreso 2007.

En verano, guifi.net celebraría en Vic el congreso internacional de referencia para las redes de telecomunicaciones libres; el World Summit for Free Information Infrastructures, con más de 140 inscritos.

En noviembre de ese año recibe el Premio Nacional de Telecomunicaciones de la Generalitat de Cataluña.

El 11 de julio de 2008 se crea la *Fundación privada para la red abierta, libre y neutral guifi.net*, que permitiría dotar de entidad jurídica a guifi logrando inscribirse así como un operador más de telecomunicaciones en el registro de la CMT conectado a CATNIX, el punto neutro de Internet en Cataluña. A su vez, la fundación también es una ONG de cooperación al desarrollo con diversos proyectos en África, Asia y América".

En el mismo 2008, la Unión Europea en la conferencia ITC2008 de Lion escoge a la fundación guifi.net como miembro de la European Network of Living Labs (EnoLL).

En abril de 2009 superan os 7000 nodos operativos, 10000 si se suman los no operativos.

En agosto en el marco de WiTFOR 2009 (World information Technology Forum) que organiza a IFIP con apoyo del gobierno de Vietnam y de la Unesco, guifi.net participó en una ponencia de la comisión "Construyendo infraestructuras".

Desde 2009 la Fundació guifi.net es miembro del RIPE (organización que gestiona los números de Internet en Euro-Asia por mandato de la IANA) y del CATNIX (punto neutro catalán) y desde 2010 están operativos los primeros tramos de fibra óptica para una conexión más eficiente al punto neutro.

Hoy, guifi.net es una referencia en las comunicaciones de libre acceso y una de las mayores y con más peso en Europa. Cuenta con más de 16.000 nodos operativos. La concentración más grande de nodos se da, lógicamente, en los municipios donde nació el proyecto y se está generalizando en toda Cataluña. Fuera de allí, también existen nodos de guifi.net en el País Valenciano, las islas Baleares, Madrid y resto de comunidades autónomas y también fuera de España como en los campos de refugiados del Sáhara y la India.

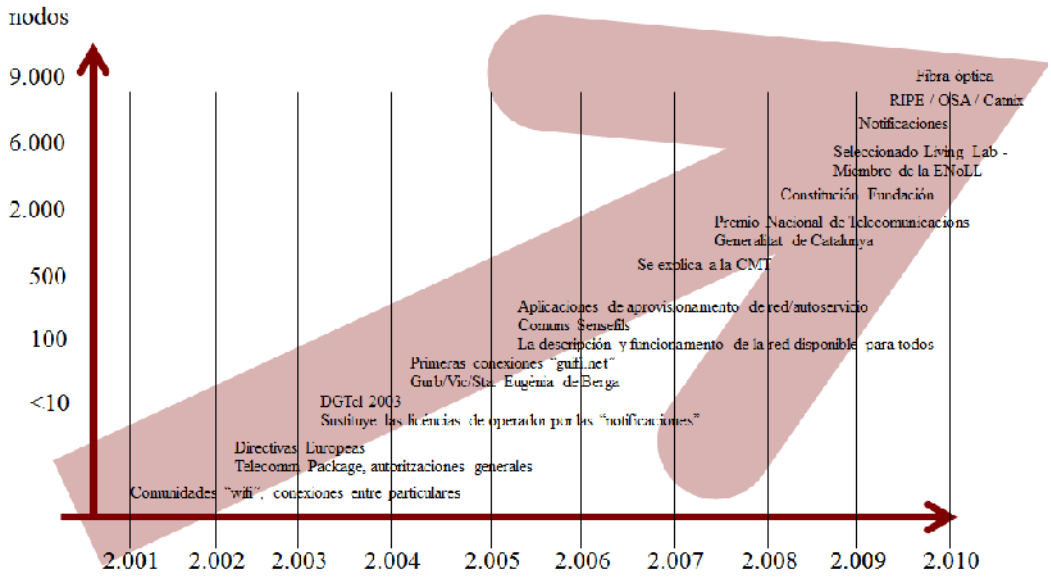


Figura 1.3. Cronología de red Guifi.net

1.6.-Elementos de la red Guifi.net

Como se ha indicado, la red se vertebra a partir de un acuerdo de `interconexión entre iguales donde cada uno al conectarse, extiende la red y obtiene conectividad con todos, y cuya finalidad es construir una red de Internet privada, donde se compartan recursos y servicios de forma autogestionada, sin la intervención de ningún organismo que lo quiera controlar o tenga intereses económicos.

La red de Guifi.net también está formada por una serie de puntos o nodos interconectados.

Simplificando, un nodo de Guifi.net tiene una radio con una antena y un router. La red de Guifi.net interconecta estos nodos.

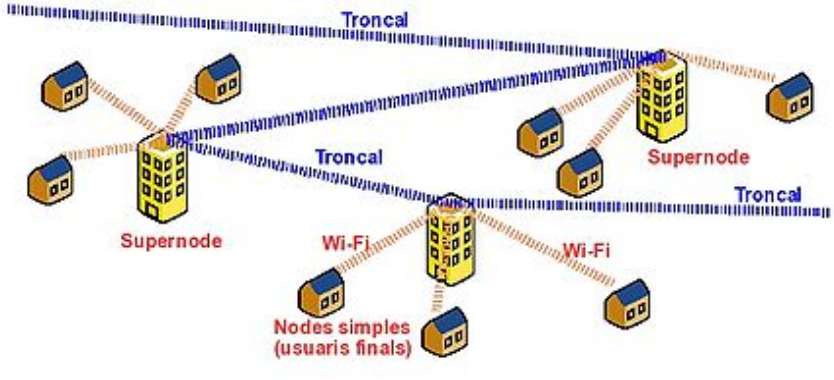


Figura 1.4. Nodos y supernodos

En la red de Guifi.net se pueden diferenciar:

1.6.1.-Nodos simples de los usuarios.

Es un punto final de la red donde está situado el usuario final que se conecta a la red. Tiene una única conexión hacia un punto de acceso de la red. El nodo tiene una radio y una antena que enlaza con el punto de acceso. Un nodo suele ser en sí mismo una subred, o "red local" donde se suele

crear redes locales para conectar los diferentes equipos en una casa para compartir archivos, impresoras y conexiones a Internet.

1.6.2.-Supernodos.

Figura 1.5. Fotografía del supernodo

Lugares donde simultáneamente se da cobertura a los usuarios de la zona y realizan un enlace entre dos puntos distantes de la red. Por tanto, es un punto que da cobertura a los usuarios (nodos finales) y / o une otros puntos de la red. Sus funciones básicas son:

- Extender geográficamente la red llevando la señal de un área geográfica a otra.
- Distribuir esta señal entre los usuarios finales (unos 30 por cada radio montada).

1.6.3.-Enlaces

Es la conexión entre dos nodos. En general utiliza la tecnología inalámbrica (mediante microondas), pero se pueden utilizar otros métodos como, por ejemplo, cable Ethernet o fibra óptica.

1.6.4.-Troncal.

Es la señal principal de la red que va de un supernodo a otro. El entrelazado de los diferentes tramos de la troncal forma la "malla" de la red. En la red de Guifi.net existen varias mallas, no necesariamente conectadas entre sí, situadas en regiones geográficamente distantes.

Figura 1.6. Fotografía Punto de acceso

1.6.5.-Puntos de acceso.

Es un lugar específico de la red donde se conectan, sin hilos, los nodos de los usuarios finales para poder acceder a la red (AP).

1.6.6.-Trastos

En Guifi.net se denomina “trastos” a los aparatos que realizan la conexión física del enlace. Los trastos mínimos para un nodo son:

- El router que sirve para mantener la conexión entre dos nodos y para dirigir y distribuir el tráfico de paquetes de información que pasan por el nodo.
- Una radio con su correspondiente antena que envía y recibe la señal de un nodo a otro.

En los nodos de los usuarios, existen trastos que llevan incorporado estos tres elementos (router, radio y antena) en una pequeña caja llamados CPEs (Customer Premisas Equipment o Equipo Local del Cliente).

1.6.7.-Proxys

Son puentes que hay entre la red de Guifi e Internet. Permiten que los usuarios de la red de Guifi.net puedan acceder a contenidos de Internet.

1.7.- Topología de la red

La topología de red de guifi.net tiene formato de malla («mesh») está formada por dos grandes pates: una la que forman los **supernodos** entre sí (**troncal**) y otra la que forman los **supernodos** con los nodos de usuario a los que sirven conexión.

1.7.1.- Red Troncal

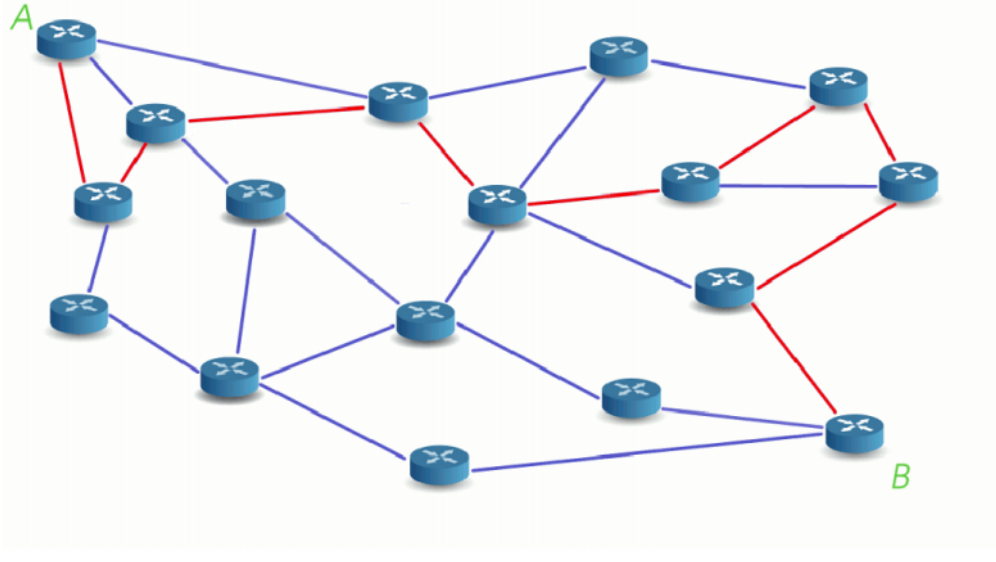


Figura 1.7. Diagrama de conexiones troncales de una red mesh

La parte «troncal» está formada por los llamados **supernodos,** una especie de centralitas de la red que mantienen varios enlaces con el resto de supernodos, cada uno de ellos del tipo **punto a punto**. Esta red que se obtendrá será de forma mallada con tantas conexiones entre supernodos como sea posible para maximizar tanto el ancho de banda como la tolerancia a fallos.

A diferencia de una red convencional en estrella, basada en troncales de alta capacidad, en las comunicaciones sin hilos la parte troncal no dispone de mucha más capacidad de ancho de banda, por tanto se procura el mismo resultado dispersando el tráfico a través de muchas troncales.

Carece de una organización centralizada o jerárquica, en su lugar los supernodos están dispersos por toda la red y se conectan de **igual a igual** con el máximo de alternativas posibles para evitar los pasos obligados dentro de la red.

Deberían ser los enlaces más estables y son gestionados con especial cuidado para orientarlos hacia la máxima disponibilidad, ancho de banda y seguridad. La idea es que esta parte de la red funcione con el máximo rendimiento según permita la tecnología sin hilos.

Al tratarse de conexiones punto a punto, están pensadas para aceptar conexiones de clientes «conocidos».

En un principio están pensados para hacer la función de enlaces de larga distancia, alcanzando más de 25km y es la red la que se encarga de posibilitar la comunicación entre las diferentes zonas

1.7.2.- Red usuario

Los supernodos mantienen otro tipo de conexiones **punto-multipunto** formadas por varias conexiones de usuario, es decir muchos usuarios se conectan a una mismo supernodo al mismo tiempo. Las «conexiones de usuarios» están formadas por los **nodos** normales que cada usuario monta en su casa.

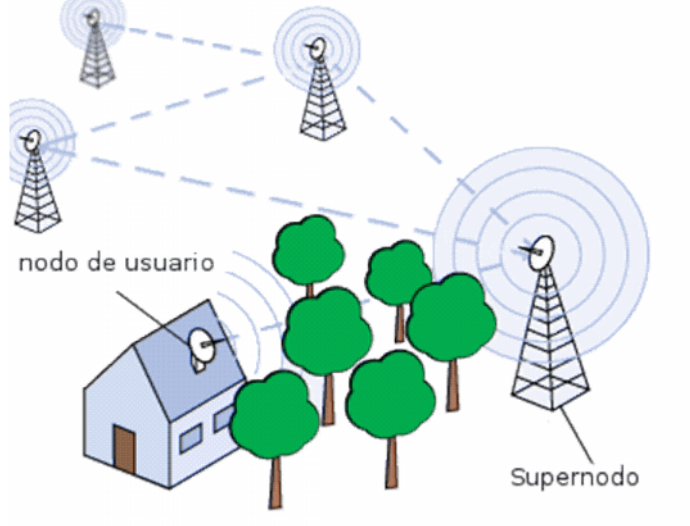


Figura 1.8. Dibujo de la red de usuario

Disponen también un hardware específico que integra todo lo necesario para realizar la conexión con el supernodo y tienen además un consumo bajo. Las conexiones de usuario pueden tener una distancia, dependiendo de las antenas utilizadas, de pocos metros a varios kilómetros (hasta ~ 10) entre la casa del usuario y el supernodo, siempre que exista visión directa entre ambos.

CAPÍTULO 2:

CONCEPTOS Y TECNOLOGÍAS WIRELESS

2.1.- Redes Mesh: estándar 802.11s

Una vez que se sabe, aunque de forma general y breve, en qué consiste la red wireless guifi.net, éste capítulo se centra en algunos conceptos teóricos básicos que son necesarios con el fin de conocer la base del funcionamiento de las herramientas que se van a utilizar en este estudio, así como presentar las tecnologías y enumerar los conocimientos mínimos necesarios para el buen entendimiento de los siguientes capítulos en cuanto al entorno tecnológico y a su utilización.

2.1.1.-Redes mesh

Actualmente, existe un elevado interés, tanto comercial como en investigación, sobre la aplicación de arquitecturas de redes malladas en las comunicaciones inalámbricas, conocidas como Wireless Mesh Networks (WMNs)

Se denomina Red Mallada (Mesh, en inglés), a aquella donde existen al menos 2 caminos a cada nodo**.** En ella se mezclan las 2 topologías: Redes de Infraestructura y Redes Ad-Hoc. Por un lado los Puntos de Acceso que configuran la red están conectados entre sí y por otro los ordenadores clientes pueden conectarse entre sí aunque no estén bajo la cobertura de un Access Point. En las redes malladas generalmente todos los nodos están conectados con los demás y, por lo tanto, hay múltiples caminos para enviar la información de un punto a otro. Este tipo de arquitecturas es tolerante a fallos pues si un punto se cae se podrá llegar a el por otras rutas.

En general utilizan protocolos de enrutamiento que son propietarios y también, a veces, hardware y software específicos.

Las redes mesh se basan en el nuevo estándar, el 802.11s.

2.1.2.- Estandar 802.11s

El estándar define como se conectan dispositivos inalámbricos para formar una WLAN (Wireless Local Area Network) mallada o mesh. Proporciona una arquitectura y protocolos que

permiten el reenvío de tramas y la selección de camino en el nivel 2 (enlace de datos) del modelo OSI.

Cubre diversos aspectos para redes mesh como seguridad, acceso al medio, sincronizacion, etc.

El objetivo del estándar 802.11s es crear la malla inalámbrica global a lo largo de todo el mundo, utilizando principalmente hardware de bajo coste y software libre y con la pretensión que estas redes sean autogestionables (proyecto llamado Open80211s).

Los componentes que define dicho estándar son:

- *Mesh Station (Mesh STA):* unidad básica de la red. Una mesh STA puede comunicarse con otras mesh STA de la red a través de varios saltos inalambricos, permitiendo alcanzar mesh STA que no estan dentro del rango propio de cobertura inalambrica.
- *Mesh Gate:* dispositivo encargado de integrar una red mesh con un sistema de distribución (Distribution System, DS) 802.11. De esta manera, la red puede conectarse con redes 802.11 cuyos puntos de acceso formen parte del DS.
- El conjunto de mesh STA y mesh gates conforman un *MBSS (Mesh Basic Service Set)*.
- *Mesh Access Point (MAP):* es una mesh STA con funcionalidades de punto de acceso. Es decir, además de las tareas propias de una mesh STA, un MAP tiene la capacidad de interconectar dispositivos inalámbricos 802.11, formando una WLAN, y añadirlos a la red mesh.
- *Mesh Portal (MPP):* permite conectar la red mesh con otras redes que no son 802.11 como, por ejemplo, una red Ethernet cableada.

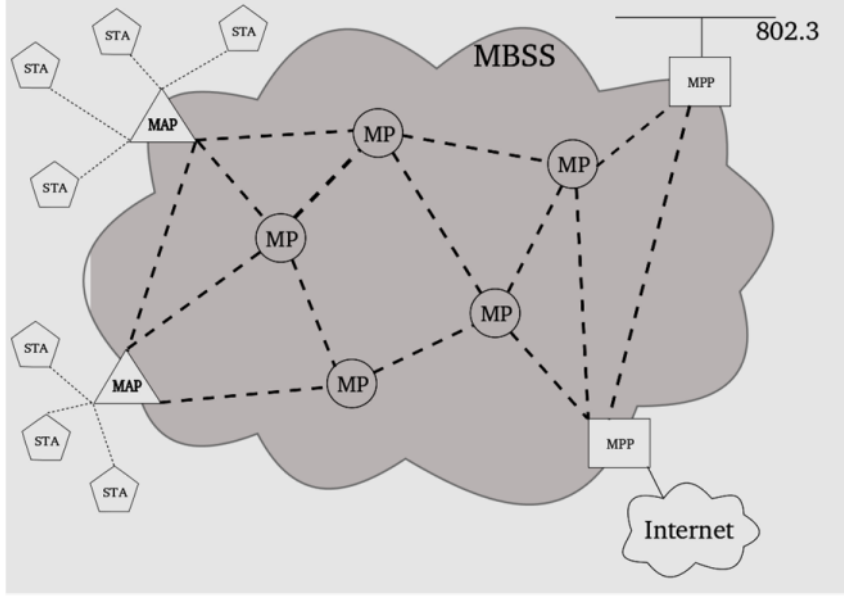


Figura 2.1. Red mesh

El punto clave en la operatividad de estas redes es el enrutamiento de paquetes. Es decir, decidir que ruta, serie consecutiva de nodos, debe atravesar un paquete para llegar de un origen a un destino. Además, estos protocolos deben ser capaces de descubrir cambios en la topología o en los enlaces entre nodos y actualizar la información correspondiente.

2.2.- La tecnología WIFI (802.11)

WI-FI es un sistema de envío de datos sobre redes de ordenadores de forma inalámbrica. Su funcionamiento es idéntico a la norma 802.3 (Ethernet), pero con la substitución de las capas física y MAC de la misma. La principal diferencia está en cómo se transmiten los paquetes de datos, por tanto una red 802.11 es completamente compatible con todos los servicios de las redes LAN de cable 802.3.

2.3.- Estándares WIFI

Existen diversos tipos de estándares WI-FI:

•IEEE 802.11b e IEEE802.11g, trabajan en la banda de 2.4 GHz que está universalmente disponible con velocidades teóricas de 11Mbps y 54Mbps respectivamente.

•IEEE802.11a opera a 5Ghz. Esta banda está mucho más limpia de interferencias, ya que no existen otras tecnologías como microondas o bluetooth que generan ruidos. Pero el alcance es menor debido a que la frecuencia es mayor, aproximadamente un 10%.

•IEEE802.11n. Este estándar hace uso simultáneo de ambas bandas, 2,4 GHz y 5,4 GHz. y puede alcanzar la velocidad teórica de 600Mbps (reales de 108Mbits).

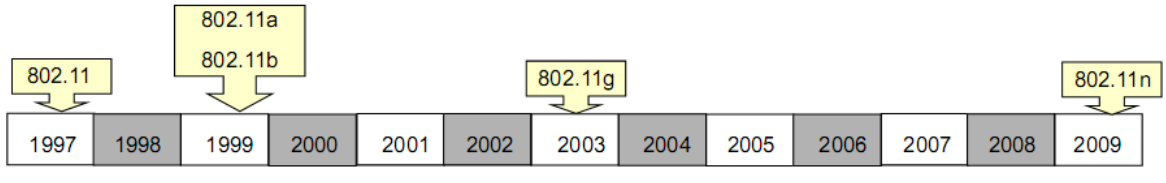


Figura 2.2. Cronología del estándar 802.11

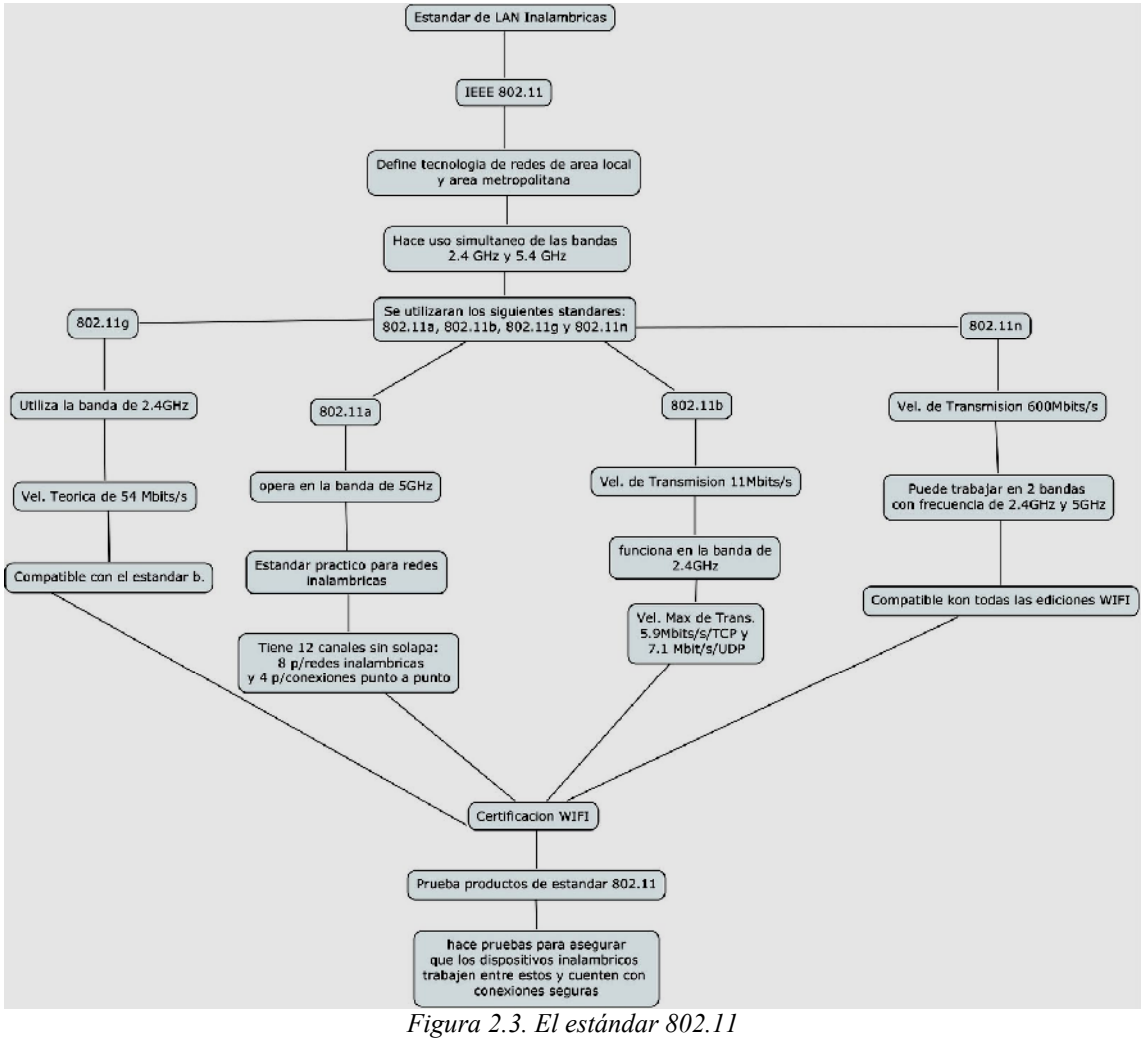


Figura 2.3. El estándar 802.11

2.4.- Factores que influyen en la señal WIFI

2.4.1.- La claridad de la señal

La claridad de señal es la clave para la realización de una comunicación Wireless. Algunos de los factores que afectan la claridad son:

2.4.1.1.-Potencia de la señal: Obviamente, una señal fuerte permite una mejor recepción en largas distancias. La normativa en España para el nivel de señal en transmisión Wireless es de 100mW para la frecuencia de 2'4GHz y de 1W para la frecuencia de 5'4GHz.

2.4.1.2.-Distancia: La potencia de la señal de radiofrecuencia (RF) disminuye con la distancia. Además se pueden sumar interferencias no deseadas con lo que se consiguen distancias menores. La señal, como se verá más adelante, puede ser modificada de diferentes formas para adecuarla a la distancia que tenga que recorrer (tipos de antenas).

2.4.1.3.-Interferencias: Los factores atmosféricos, como la nieve, la lluvia o el

granizo, pueden interferir en la señal. Es un dato a tener en cuenta cuando se quieren realizar enlaces wireless en exteriores. Normalmente las interferencias de RF son causadas por aparatos que están emitiendo cerca, en la misma banda y mismo canal. También se consideran interferencias a las transmisiones wifi que estén en el mismo canal que una señal, por lo que siempre es conveniente utilizar el canal menos utilizado. Incluso otros sistemas de RF como puede ser microondas o cualquier otro sistema también puede interferir y degradar el nivel de la señal.

***2.4.1.4.-Línea de visión*:** La señal necesita *visión directa* para realizar bien la comunicación. Si hay obstáculos en la línea de visión, no se podrá realizar la conexión. La transmisión Wifi es sólo válida para enlaces con visión directa.

2.4.2.-Transmisión de la señal

Las ondas de señal de radio viajan como las vibraciones del agua de una piscina cuando se lanza un objeto. La potencia de la señal disminuye a medida que la señal se aleja de la primera onda.

Una antena direccional refleja la señal en una dirección y crea un foco en forma de cono con gran potencia. La señal no se propagada a partes iguales por todo el foco.

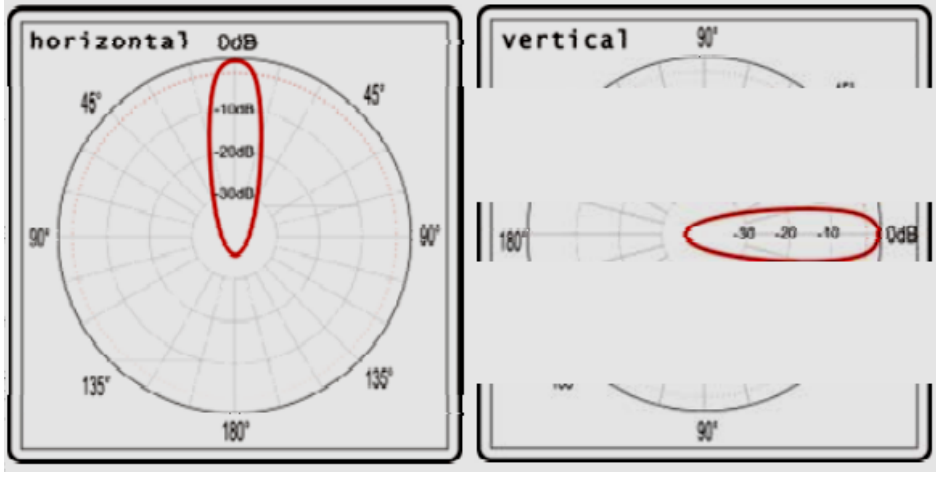


Figura 2.4. La transmisión de la señal inalámbrica

Igual que la luz es enfocada con más intensidad con una lupa, la señal de RF es más fuerte con un área más estrecha y central. Se refiere al área donde la señal es más fuerte como el centro del lóbulo. Siempre siendo más débil en los extremos.

El ancho del haz de la señal de RF depende de cómo la antena forma la señal (tipo de antena) y la distancia de la fuente de la señal. La señal se atenúa gradualmente en el borde del cono y no es aconsejable medir la señal desde el borde. La amplitud del haz (no el nivel de potencia) de señal aumenta con la distancia, si se desea medir la anchura de la señal en metros, no se podrá determinar hasta que no se sepa a que distancia estará. La potencia de la señal se mide en decibelios (dB). El

número de decibelios indica la distancia de la señal respecto a su punto central, es decir el alcance de esta.

Las ondas pueden rebotar en algunos objetos que encuentren por su camino, en este caso las ondas se desfasan con mayor o menor grado en función del material en el que reboten y su ángulo de incisión. Una vez una señal es rebotada/desfasada puede ser recuperada o no en función del desfase de la misma. Normalmente si los desfases son muy pequeños, casi despreciables se puede recuperar la señal. Existen tipos de antenas que emiten con una polarización concreta, horizontal, vertical, circular o con multipolaridad que recupera las señales desfasadas. Se ha de resaltar que si se utiliza en un emisor una antena con polarización horizontal, es lógico, que en la recepción se utilice una antena con la misma polarización, ya que en caso contrario no se recuperaría la señal debido al desfase natural que hay entre las dos antenas (90 grados).

2.4.3.- Enfocar la señal

Si la distancia de transmisión aumenta, es necesario compensar la distancia seleccionando una antena con una transmisión más enfocada y un foco más estrecho, es decir una antena direccional.

Algunos de los beneficios de utilizar antenas direccionales es que al tener un foco más estrecho, las señales que interfieren se minimizan.

Para conseguir un enlace entre dos puntos, lo más conveniente es que los dos lóbulos principales del emisor y el receptor coincidan en al menos un punto, no es necesario que el lóbulo de cada uno de los extremos este superpuesto con el otro. Pero cuanta más superposición exista entre los lóbulos del emisor y el receptor mejor será la señal

2.4.4.- Línea de visión (LOS)

El éxito de un enlace de RF depende de la línea de visión. Una línea de visión sin obstáculos se llama “free space path” (camino con espacio libre). Sin línea de visión directa, tal y como se ha comentado con anterioridad, no es posible realizar un enlace vía Wifi.

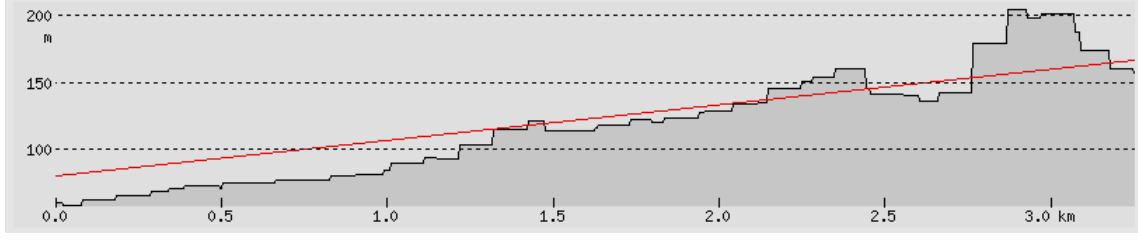


Figura 2.5. La línea de visión (LOS)

Un obstáculo en la línea de visión del enlace reduce o elimina totalmente la señal. La desviación de la señal al pasar alrededor de un obstáculo se llama *difracción*. Una reducción de la potencia de la

señal es conocida como *atenuación*.

También se ha de comentar, que no siempre es suficiente una visión directa entre dos puntos para realizar un enlace wireless. Ya que ha de tener un campo de visión lo suficientemente ancho como para que pase un cierto porcentaje del haz del emisor y el receptor. Existen las zonas de Fresnel que definen las anchuras y alturas necesarias para tener una línea de visión suficiente para realizar los enlaces.

2.4.5.- Posición estable de la antena

Para obtener un óptimo rendimiento, se debe ajustar las antenas con la máxima precisión posible. Para asegurar un buen alineamiento de las antenas, es preciso mantenerlas en una posición estable y rígida. Hay que asegurarse que el mástil donde se instala sea rígido. Para instalaciones interiores este fenómeno es despreciable.

En resumen para conseguir una buena señal en distancias largas, se debe mantener el enlace RF libre de obstáculos, transmitir en los canales menos utilizados y utilizar antenas lo más direccionales posibles para obtener menores interferencias.

2.5.-Protocolos de cifrado

El crecimiento de las redes y su gran aceptación obligó a la creación de métodos para proteger la información de los usuarios mediante cifrados. Manteniendo así una confidencialidad de toda la información que circula por la red.

Cuando las redes están instaladas sin ningún tipo de seguridad se convierten en redes abiertas, no protegiendo la información que circula por ellas. Existen múltiples protocolos de cifrado para la información que se transmite. Los más utilizados son:

•WEP: (Wired Equivalent Privacy). WEP es un sistema de cifrado para el estándar IEEE 802.11 como protocolo para redes Wi-Fi. Fue lanzado 1997, en un intento de proveer confidencialidad en las redes inalámbricas. Pero a partir de 2001, se encontraron múltiples debilidades en el protocolo, como resultado, es posible romper una conexión con seguridad WEP con facilidad. Por lo tanto se incorporó una solución temporal llamada TKIP para mejorar las vulnerabilidades del WEP.

Permite cifrado de nivel dos y está basado en el algoritmo RC4, utilizando claves de 64 bits o 128 bits. Emplea suma de comprobación CRC-32 para la integridad. Cifra los datos de la red mediante cifrados de 64 o 128 bits.

•WPA: (WiFi Protected Access). Fue creado en respuesta a los serios problemas y debilidades encontrados en el sistema de seguridad anterior WEP. WPA se implementa en la mayoría de los estándares 802.11i, y fue diseñado para trabajar con todas las tarjetas de redes inalámbricas, pero no

necesariamente podrán trabajar con la primera generación de puntos de accesos inalámbricos. WPA fue creado por la WiFi Alliance, dueños de la marca WiFi, y diseñado para usarse en servidores de autenticación IEEE 802.11X, el cual distribuye diferentes claves para cada usuario (aunque puede ser utilizado de forma menos segura y darle a cada usuario la misma clave). presenta mejoras como la creación de una clave dinámica como clave de acceso, no teniendo restricción de caracteres.

•WPA2: o WiFi Protected Access 2, también conocido como IEEE 802.11i, es una enmienda en la seguridad del estándar 802.11 (WPA). Establece medidas estándares de seguridad para redes inalámbricas. Remplaza el WPA e introduce el CCMP, una nueva forma de encriptación basada en cifrado por bloques AES con gran seguridad.

Mejora el IEEE 802.11-1999, proveyendo un RSN (Robust Security Network) con dos nuevos protocolos: el 4-Way Handshake y el Group Key Handshake. Estos utilizan los servicios de autenticación y control de acceso a puertos descritos en IEEE 802.1X para establecer y cambiar las claves criptográficas apropiadas. El RSN es una red de seguridad que solo permite la creación de asociaciones de red de seguridad robustas (RSNAs), que son un tipo de asociación usada por un par de estaciones (STAs) si el procedimiento de establecer la autenticación o asociación entre éstas incluye el 4-Way Handshake. También provee dos protocolos de confidencialidad e integridad de datos: TKIP y CCMP, con la implementación de CCMP obligatoria.

2.6.- Bandas de frecuencia

La tecnología de redes inalámbricas ha tenido una particular explosión, gracias a la adopción de las bandas de frecuencias ICM.

Las bandas ICM son bandas definidas por la Unión Internacional de Telecomunicaciones (UIT) reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industriales, científicas y médicas, concretamente son tres bandas de frecuencias: 902 a 928 MHz, 2.400 a 2.483 y de 5.000 a 5.725 MHz. En España no es preciso contratar una licencia de uso o concesión administrativa de ningún tipo para su uso. Razón por la cual se conocen como bandas de frecuencia libres.

Estas dos últimas bandas de 2,4 y 5 GHz son las utilizadas por la tecnología Wifi. Guifi.net, para aprovechar el máximo de posibilidades, utiliza ambas bandas simultáneamente, la de 2,4 GHz, para los enlaces de nodo a supernodo y la banda de 5 GHz para los enlaces supernodo a supernodo.

La banda de los 5GHz, más amplia y menos saturada, se reserva para los enlaces troncales haciendo un uso más eficiente de la totalidad de los canales y frecuencias de libre disposición.

2.7.- Canales de frecuencia

Cuando se definió el estándar IEEE 802.11, que regula las redes locales inalámbricas, se especificó también los tres rangos de frecuencia disponibles para los dispositivos que desearan emitir de esta forma: 2.4 GHz, 3.6 GHz y 5 GHz. La mayoría de dispositivos actuales operan, en las franjas de frecuencia de 2.4 y 5 GHz. Cada rango de frecuencias fue subdividido, a su vez, en multitud de **canales**.

2.7.1.- Canales Wi-Fi permitidos en España

En España las referencias sobre la regulación del espectro electromagnético se establecen en el CNAF (Cuadro Nacional de Atribución de Frecuencias). La tecnología Wi-Fi utiliza una banda de frecuencias u otra según el estándar al que nos refiramos:

- **2,4 GHz**: 802.11b, 802.11g y 802.11n
- **5 GHz**: 802.11a y 802.11n

2.7.1.1.-Banda 2,4 GHz

Para 2.4 GHz, el espectro de frecuencias se divide en **14 canales**, separados por 5 MHz. Cada país y zona geográfica aplica sus propias restricciones al número de canales disponibles. En España se pueden utilizar los canales 1-13; el canal 14 es el único prohibido. Al igual que el resto de Europa.

El problema de esta distribución es que cada canal necesita 22MHz de ancho de banda para operar, por lo que se produce un **solapamiento de varios canales contiguos**.

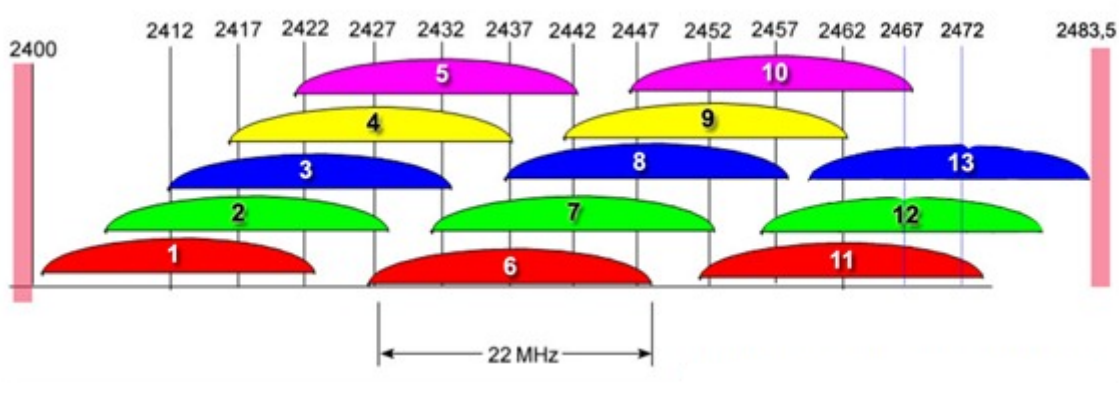


Figura 2.6. La banda de frecuencia de 2,4 GHZ

2.7.1.2.- Banda 5 GHz

La principal ventaja de esta frecuencia es que dispone de un rango de frecuencias limpio y por ello menos susceptible de interferencias por parte de otras redes.

En España se permite el uso de los canales 34-64 y 100-140, al igual que en el resto de Europa. Son canales de unos 20 MHz cada uno y que están separados entre sí 20 MHz, por lo que el solape es mucho menor que en la banda de 2,4 GHz.

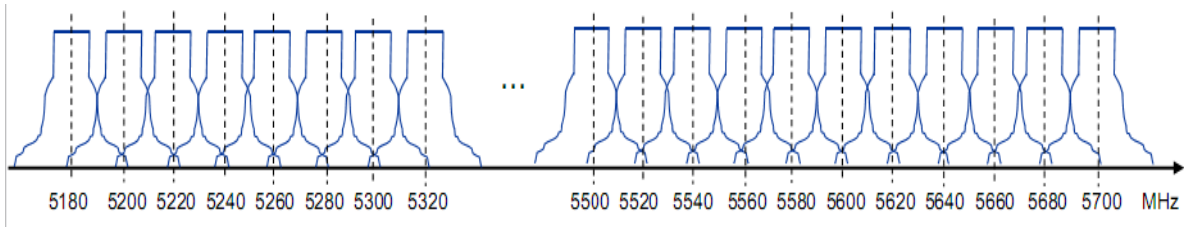


Figura 2.7. La banda de frecuencia de 5 GHZ

2.8.- Modos de funcionamiento

2.8.1.- "AD-HOC": los clientes se comunican directamente entre ellos. Solamente los clientes dentro de un rango de transmisión definido pueden comunicarse entre ellos. El modo ad-hoc se denomina **Independent Basic Service Set (IBSS).**

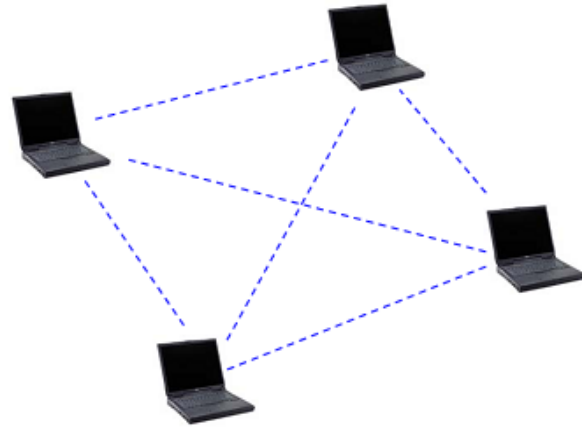


Figura 2.8. Funcionamiento Ad-Hoc

2.8.2.-"Infrastucture":

Cada cliente envía todas sus comunicaciones a una estación central o punto de acceso (Access Point–AP).

Este AP actúa como un bridge Ethernet y reenvía las comunicaciones a la red apropiada, ya sea una red cableada u otra red inalámbrica.

El modo infraestructura permite dos posibles topologías:

2.8.2.1.-Basic Servicie Set (BSS). Existe una única célula servida por un punto de acceso.

2.8.2.2.-Extended Service Set (ESS). Se compone de varios BSS's (cada uno con su AP) conectándolos a través de un sistema de distribución, que suele ser una red Ethernet. En esta arquitectura, las estaciones pueden desplazarse y conectarse a otro AP (roaming).

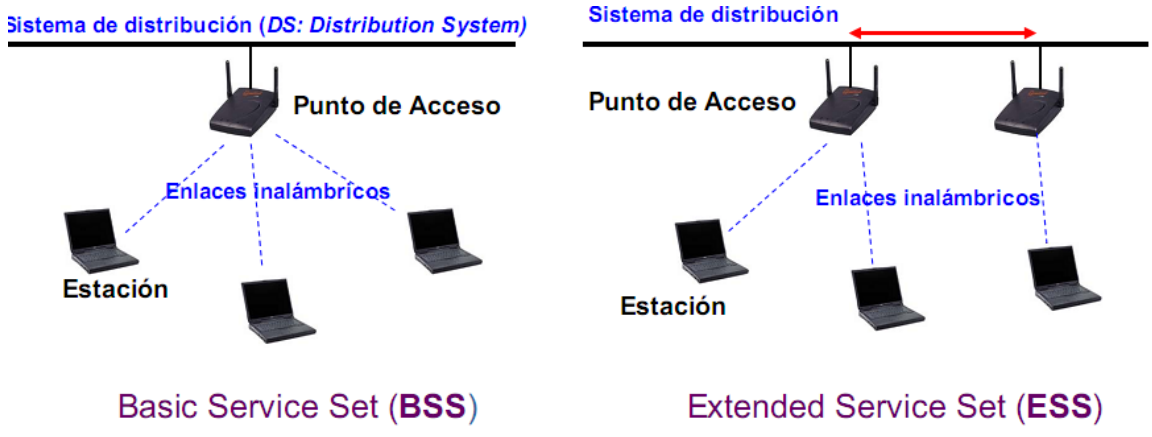


Figura 2.9. Funcionamiento modo Infraestructura

2.9.- Protocolos de enrutamiento.

El trabajo del enrutamiento es determinar la mejor ruta al destino, y crear una tabla de enrutamiento que liste el mejor camino para todos los diferentes destinos.

2.9.1.-Enrutamiento estático.- Es el término utilizado cuando la tabla de enrutamiento es creada por configuración manual. Algunas veces esto es conveniente para redes pequeñas, pero puede transformarse rápidamente en algo muy dificultoso y propenso al error en redes grandes. Peor aún, si la mejor ruta para una red se torna inutilizable por un fallo en el equipo u otras razones, el enrutamiento estático no podrá hacer uso de otro camino.

2.9.2.-Enrutamiento dinámico.- Es un método en el cual los elementos de la red, en particular los enrutadores, intercambian información acerca de su estado y el estado de sus vecinos en la red, y luego utilizan esta información para automáticamente tomar la mejor ruta y crear la tabla de enrutamiento. Si algo cambia, como que un router que falla, o uno nuevo que se pone en servicio, los protocolos de enrutamiento dinámico realizan los ajustes a la tabla de enrutamiento. El sistema de intercambio de paquetes y toma de decisiones es conocido como protocolo de enrutamiento.

Dependiendo de la manera en la cual el protocolo controla los enlaces y sus estados, distinguimos dos tipos principales: proactivo y reactivo.

2.9.2.1.-Proactivo (manejo por tablas)

Están caracterizados por chequeos proactivos del estado del enlace y actualización de tablas de enrutamiento, la cual lleva a una alta complejidad y carga de CPU, pero también a un alto rendimiento.

- *OLSR,* Optimized Link State Routing Protocol (protocolo de enrutamiento por enlaces optimizados), OLSREXT, QOLSR.
- *TBRP,* Topology Broadcast based on Reverse Path.

- *Forwarding routing protocol*, (protocolo de transmisión basado en el reenvío por camino invertido).
- *HSLS,* Hazy Sighted, Link State routing protocol (protocolo de enrutamiento basado en desechar los enlaces de baja calidad).
- *MMRP,* Mobile Mesh Routing Protocol.
- *OSPF,* Open Shortest Path First

2.9.2.2.-Reactivo (por demanda)

Reacción pasiva en detección de problemas (rutas que no trabajan), tiende a ser menos efectiva, pero también es menos exigente con la CPU.

Las líneas entre estos dos tipos no son estrictas, existen mezclas y formas diferentes como el **AODV (**Ad hoc On Demand Distance Vector) Protocolo de demanda de vectores de distancia, diseñado para redes móviles

El protocolo de enrutamiento más relevante en redes MESH inalámbricas es el OSPF **(**Open Shortest Path First) que opera sobre la ruta más corta, desarrollado por Interior Gateway Protocol (IGP) un grupo trabajador de la IETF, y está basado en algoritmo SPF:

- La especificación OSPF envía llamadas, verifica el estado de los enlaces y se lo notifica a todos los enrutadores de la misma área jerárquica.
- OSPF además funciona como un LSAs (Link – state advertsement) y avisa las interfaces presentes, informa el tipo de medición usada y otras variables.
- Los enrutadores con este protocolo almacenan información y usando el algoritmo SPF calculan el camino más corto.
- Este protocolo compite con RIP y IGRP, los cuales son protocolos de enrutamiento de vectores de distancia. Estos envían toda o una porción de sus tablas de enrutamiento a todos los enrutadores vecinos refrescando la información continuamente.

2.10.- Multiple Input / Multiple Output (MIMO)

Hasta el año 2004, solo se usaba una antena para transmitir y otra para recibir. Algunos dispositivos usaban varias antenas, pero simplemente se elegía por cual se transmitía, siendo la elegida la que mejor ganancia presentaba en ese momento.

El siguiente paso a esto era tener varias antenas de transmisión, de forma que se podía dividir el paquete a transmitir entre las antenas. Seguidamente en el receptor se unían de nuevo y se entregaban de forma correcta. Esta es la tecnología conocida como MIMO y en teoría permite multiplicar la

tasa de transmisión por el número de antenas que se usen. En el estándar 802.11n están definidas hasta 4 antenas de transmisión y recepción, por lo que la velocidad puede multiplicarse por 4.

2.11.-Hardware Wireless

Guifi.net se basa en un equipamiento común para formar la parte troncal y en equipamiento propio para el usuario final. Debido a esto cada usuario puede utilizar el equipamiento que considere mejor.

En el nivel básico, se necesitan dos piezas de hardware para cualquier red inalámbrica: un punto de acceso central y un adaptador de red. Los puntos de acceso suelen ser dispositivos independientes. Por el contrario, las tarjetas de red se suelen instalar dentro de un ordenador en bahías PC Card, ranuras PCI y ranuras adaptadas. También hay disponibles adaptadores externos que se conectan a puertos USB o Ethernet. Por último, aunque tanto los puntos de acceso como las tarjetas de red tienen antenas integradas, hay antenas externas que pueden ampliar el alcance de ciertas redes.

2.11.1.- Componentes para crear una red WiFi (Wireless):

2.11.1.1.-Punto de acceso. (Access Point):

Se suele abreviar como AP Los puntos de acceso son meras "emisoras" de señales WiFi y se utilizan para crear una red wíreless. El punto de acceso también debe estar conectado a una red Ethernet mediante un cable de red.

Actúan como un HUB o SWITCH de red normal cableada. Es un dispositivo que 'gestiona' los paquetes lanzados por otras estaciones inalámbricas, haciéndolas llegar a su destino. Además al estar conectado a una red cableada, hace que la red inalámbrica puede acceder a otros equipos de esta red.

2.11.1.2.-Pasarela de Enlace (Gateway):

Un Gateway o pasarela en su definición estricta, es un dispositivo que conecta entre sí redes con diferentes protocolos, aunque su significado se ha ampliado y podría aplicarse simplemente a equipos que conectan redes con diferentes rangos IP, básicamente lo mismo que hace un router, pero con algunas pequeñas diferencias.

2.11.1.3.-Router (Acces Point + Gateway):

Es simplemente la combinación de ambos: Acces Point + Gateway

2.11.1.4.-Clientes inalámbricos (Tarjetas de conexión):

Son todas aquellas tarjetas que proporcionan conectividad inalámbrica. Las más conocidas son las que vienen en formato PCI, en Compact Flash, Smart Card, USB y similares. Tanto si son

internas como si son externas estas tarjetas sirven para conectar a un PC a un punto de acceso inalámbrico.

Su configuración a nivel de IP es exactamente igual que una tarjeta Ethernet, pero existen diferencias más importantes entre una WIFI y una Ethernet, como son: El cifrado de datos, el ESSID, el Canal, y el ajuste de velocidad.

2.12.-Antenas

Todos los puntos de acceso y tarjetas inalámbricas tienen antenas que están conectadas con ellos o integradas y, como es evidente, suponen un elemento imprescindible de una red inalámbrica.

Una antena es un elemento que permite la emisión y recepción de ondas electromagnéticas. En los términos más simples, una antena aumenta la potencia de un transceptor. Un transceptor combina un transmisor y un receptor, de modo que, enfocando mejor la energía electromagnética que entra o sale, la antena aumenta tanto la fuerza de la señal transmitida como la sensibilidad de la recepción. La potencia de una antena se expresa en decibelios, o dB, y cada antena tiene un rango de potencias en decibelios, generalmente conocido como ganancia. Los decibelios aumentan en escala logarítmica: un pequeño aumento de los decibelios provoca un gran aumento de la sensibilidad.

Por tanto, una misma antena puede usarse tanto para recibir como para transmitir y además las antenas están diseñadas para funcionar cada una en una frecuencia o conjunto de frecuencias (banda).

No es necesariamente cierto que cuanto más larga o grande sea la antena nota mejor la señal. La forma, composición y varios otros factores se combinan para determinar la ganancia. Las antenas de mayor ganancia, por ejemplo, también enfocan su energía en estrechos haces adecuados sólo para intercambios punto a punto.

2.12.1.-Patrón de radiación

En primer lugar, las antenas se agrupan en dos grandes tipos, según la forma en que irradian la señal: las **omnidireccionales** y las **direccionales**.

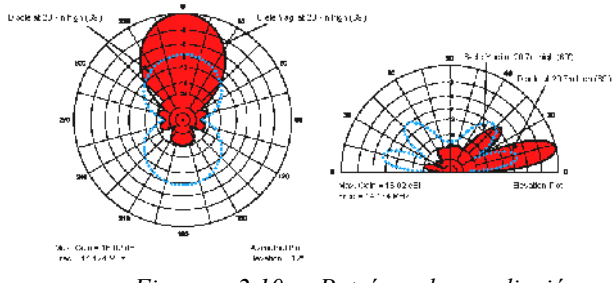


Figura 2.10. Patrón de radiación

La primera irradia en todas direcciones y la segunda en una dirección en particular. Aunque existe un tercer tipo de antenas (sectoriales), las consideraremos direccionales. El patrón de radiación es un gráfico en el que se representa la fuerza y forma de los campos radioeléctricos radiados por una antena. Normalmente los patrones de radiación de las antenas suelen venir entre las características técnicas de las mismas y se representan normalmente o bien en dos planos perpendiculares conocidos como azimut y elevación o bien en un

modelo 3D, que nos da la misma información que el grafico anterior pero en 3 dimensiones.

2.12.2.- Tipos de antenas por patrón de radiación

Existen tres grupos principales de antenas según sus patrones de radiación que se utilizan para diferentes cometidos dentro de la red, la utilización de cada tipo de antena para el uso concreto mejora ampliamente la capacidad de transmisión y alcance de la tecnología wifi.

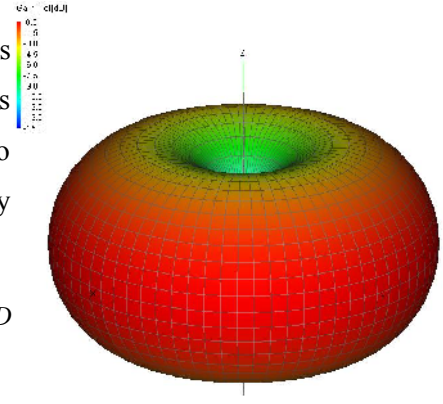


Figura 2.11. Patrón de radiación 3D

2.12.2.1.-Antenas direccionales

Estas antenas se usan porque principalmente orientan las señales un una sola dirección con un haz muy delgado o estrecho pero con un alcance muy largo. Esta antena se asemeja a una linterna que envía luz en un haz limitado pero también más focalizado, esto permite por un lado que la emisión de la antena no manche todo el espectro radioeléctrico y por otro evita que la antena reciba interferencias de otras fuentes.

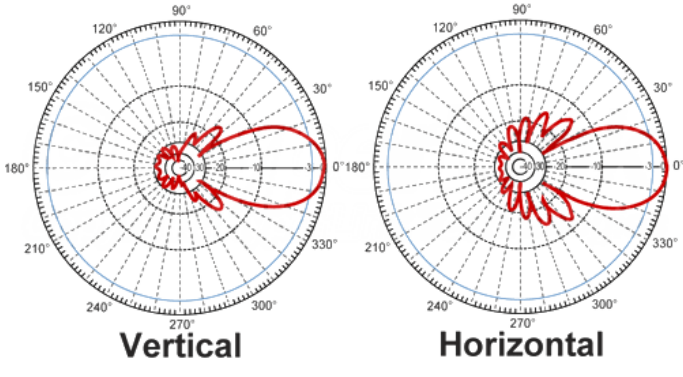


Figura 2.12. Antenas direccionales

Este tipo de antenas en la banda de 5GHz son las utilizadas para los llamados enlaces troncales de la red, que son los enlaces entre distintos supernodos y que por tanto soportan mayor cantidad de tráfico de toda la red.

2.12.2.2.-Antenas omnidireccionales

Estas antenas envían la señal a todos los lados a un alcance muy corto. Esta antena se asemeja a un foco que envía luz a todos lados con baja intensidad y alcance mucho menor que las antenas direccionales. Son 360 grados teóricos.

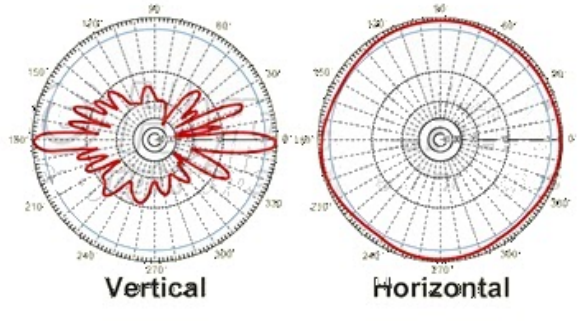


Figura 2.13. Antenas omnidireccionales

Este tipo de antenas en 2.4 GHz se usan normalmente para "servir" conexión a los clientes de un supernodo y tienen un alcance limitado de 1 a 2km. Para distancias mayores es recomendable usar antenas sectoriales.

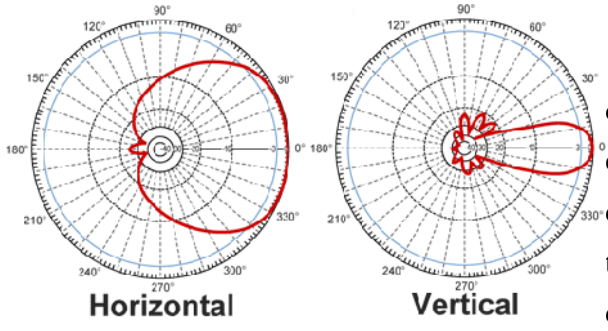


Figura 2.14. Antenas sectoriales

2.12.2.3.-Antenas sectoriales

Es la conjunción de ambas antenas, omnidireccionales y direccionales. Estas antenas emiten su radiación con un ángulo mayor al direccional pero no tanto como los 360 grados teóricos de una omnidireccional, sería como un foco de gran apertura con intensidad media-alta. Sumando 3 o 4 antenas sectoriales se puede dar cobertura a 360º como con una omnidireccional pero con un alcance que puede llegar a los 10 km.

2.12.3.- Otras características de las antenas

2.12.3.1.-Polarización,

Las que tienen polarización vertical y las de polarización horizontal son las más comunes. Una antena de polarización vertical es aquella cuyo campo eléctrico es perpendicular a la tierra. En las del tipo horizontal el campo eléctrico es paralelo a la tierra. Para que un enlace funcione correctamente, todas las antenas deben tener la misma polarización, en caso contrario, se producirán importantes interferencias en el enlace.

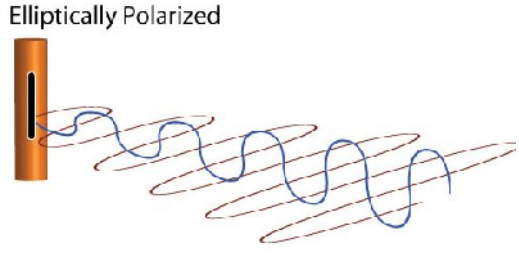


Figura 2.15. Polarización

2.12.3.2.-Ganancia.

Cualidad que tiene una antena para concentrar la energía en un área dada. Existe una antena teórica, llamada isotrópica, que irradia uniformemente su energía en todas direcciones. Si representáramos gráficamente esa energía radiada, veríamos una figura similar a una esfera. En la práctica y dependiendo del tipo de antena, la figura que se generaría seria una deformación de la esfera, cuya forma dependerá del tipo de antena. A mayor concentración de la energía hacia una dirección, mayor será la ganancia de una antena y por lo tanto se concentrará la potencia que se le

aplica, hacia el área que interesa. Esa área de concentración principal se llama lóbulo de radiación principal.

2.12.3.3.-*Unidades de Ganancia:*

+Dbm**:** es una unidad relativa a decibel (db) comparada con miliwatts, y nos indica la energía o potencia de un transmisor. A modo de ejemplo si un transmisor nos dice que tiene una potencia de 15 miliwatts entonces expresado en db seria: 10 x log10 (15) = 11.76 db pero como se compara con miliwatt quedaría expresado como 11.76 dbm .

+Dbi: también es una unidad relativa a decibel (db) y expresa la ganancia de energía de una antena en comparación con una antena isotrópica (antena que difunde energía en todas las direcciones con la misma potencia).

A modo de ejemplo una antena que tenga 3 veces la ganancia de una antena isotrópica significa que tiene una ganancia de 10 x log10 (3) = 4.77 db y quedaría expresado como 4.77 dbi,

Como resumen en wifi el dbm se utiliza tanto para saber la potencia de transmisión como la sensibilidad de recepción de un equipo (tarjetas wifi, Access Points etc.), y si se conoce además la ganancia de la antena en dbi permite realizar distintos cálculos como por ej. saber si es factible hacer una conexión entre 2 o más equipos a determinadas distancias...

+Pire**:** en la práctica es un dato de un emisor en el punto donde mayor potencia tenga de emisión. Se tiene en cuenta la potencia de la emisión (dbm) y la ganancia de la antena (la capacidad de concentrar la emisión, dbi). El cálculo se hace sumando los decibelios del dispositivo emisor y los decibelios de ganancia de la antena.

Ejemplo de cálculo de potencia PIRE. Una antena con 16 dbi de ganancia y emitiendo a 16dbm tendría una potencia PIRE de 32 decibelios (valores que pueden corresponder a una nanostation M5). Para convertir 32 decibelios en watios salen 1,58 watios.

2.12.3.4.-Ancho de haz.- A grandes rasgos, el ancho del haz es el ángulo que se forma entre dos líneas imaginarias entre las que "encajaría" el lóbulo de radiación principal. Cuanta más ganancia tenga la antena más concentrada estará la radiación, más alargado será el lóbulo principal y, por lo tanto, más estrecho será el haz. Todas las antenas tienen un ancho de haz vertical y un ancho de haz horizontal.

CAPÍTULO 3:

INSTALACIÓN FÍSICA DEL SUPERNODO UPV

3.1.- Acciones iniciales

En este capítulo se describe tanto los componentes como el material necesario para crear el supernodo para la nueva zona en la UPV de la red Guifi.net y, con él, distribuir la señal en toda la zona para la conexión de nuevos usuarios de la red por medio de varios puntos de acceso. Una vez descritos los componentes utilizados se explica, paso a paso, el proceso de instalación física del mástil con todos los componentes y cableado del nodo.

Pero antes de empezar con esta descripción, voy a enumerar brevemente las solicitudes y acciones que ha sido necesario realizar para conseguir el permiso para el establecimiento del nodo de Guifi.net

- Una vez planteada la posibilidad de constituir el nodo se estableció contacto con los profesores de la UJI (Universidad Jaume I de Castellón) Miguel Pérez y Pablo Boronat, que son administradores de Guifi.net Castellón y cuya inestimable ayuda ha sido fundamental para llevar a buen fin el proyecto.
- Lo siguiente que se realizó fue solicitar a la Comisión Permanente de la ETSINF permiso para la colocación del mástil con sus antenas inalámbricas en la azotea del edificio de la Escuela.
- De esta Comisión se obtuvo la aceptación condicionada a un informe que se tuvo que solicitar al Servicio Integrado de Prevención y Salud Laboral de la universidad sobre la existencia de posibles problemas de radiación.
- Con el informe favorable del servicio de Prevención y el consiguiente permiso del Centro, el último paso para conseguir la acreditación y resto de permisos fue, siguiendo el protocolo de acceso a cubiertas aplicado en la UPV, recibir un seminario sobre los riesgos y medidas preventivas a adoptar en el acceso a la cubierta del edificio 1H, así como de las instrucciones a aplicar y medidas de emergencia
- Una vez conseguida la acreditación se planteó que componentes iban a constituir el nodo y se solicitó presupuesto del material.

3.2.- Componentes y material usado en la instalación.

Básicamente los componentes que se van a instalar son:

• 1 Antena parabólica para poder enlazar con otra antena parabólica, que de momento no está instalada y que unirá nuestra zona a la red por el norte.

• 3 Antenas sectoriales para repartir la señal entre los usuarios con nodo fijo.

• 1 Antena hotspot para repartir la señal entre los usuarios con equipos móviles (portátiles, PDA…) que se conecten a ella.

• 1 Router que organice el tránsito de la señal y la encamine al lugar adecuado.

• 1 Caja estanca de aluminio.

• 1 Mástil para ubicar las antenas.

• Cables y conectores para la interconexión de todos los elementos en la red.

Las herramientas que se necesitan para construirlo son:

• Tenazas para cables, de corriente y de red.

• Llaves inglesas, fijas y de tubo

• Destornilladores planos y de estrella.

• Bridas y cables para sujetar y tensar.

• Una escalera

• Un portátil para probar que todo funciona bien, tanto por red cableada como por wifi.

NOTA: Las radios deben estar previamente configuradas y probadas con el script "unsolclic" como se ve en el capítulo siguiente.

La documentación técnica de los componentes utilizados se encuentra en el anexo correspondiente de documentación técnica del material.

3.3.- Breve descripción de componentes

Se presenta a continuación una breve descripción de los componentes empleados con fotografías de los mismos.

3.3.1.- Antena parabólica

En guifi.net se utilizan fundamentalmente antenas parabólicas para conexiones entre supernodos cuando las

Figura 3.1. Fotografía de la antena parabólica

distancias son muy grandes, aunque son más complicadas de encarar. La ventaja principal es que emiten en un ángulo pequeño y, por lo tanto, la señal pierde menos intensidad con la distancia que con otros tipos de antenas.

La antena parabólica utilizada es una Rocket M5 2x2 MINO de 650 mm de diámetro que trabaja en 5 GHz, con una ganancia (potencia de emisión relativa) de 30 dBi y polarización horizontal o vertical. En teoría permite hacer conexiones de más de 30 km.

A la antena se le conecta la estación base Rocket M5-5GHz 2XRSMA 2x2 MIMO AIRMAX con 2x2 radios MIMO que se caracteriza por su gran alcance (+50km) y rendimiento (+150Mbps real TCPI/IP) y que está específicamente diseñado para realizar enlaces en exterior Punto a Punto y trabajar como Estación Base AirMax Punto Multipunto.

Figura 3.2. Fotografía Rocket M5 2x2 MIMO

Figura 3.3. Fotografías conexión Rocket M5

La instalación del Rocket M5 como estación base AirMax a la antena Rocket no requiere ninguna herramienta especial, es muy sencillo, simplemente hay que deslizarlo en el kit de montaje suministrado junto con las antenas.

3.3.2.- Router y radios de 5 GHz

Utilizamos un router de placa de la casa Mikrotik, modelo Routerboard RB493AH.

Este router permite tener tres radios y dispone de:

• Nueve conectores Ethernet 10/100.

• Tres ranuras del tipo miniPCI para poner hasta 3 radios.

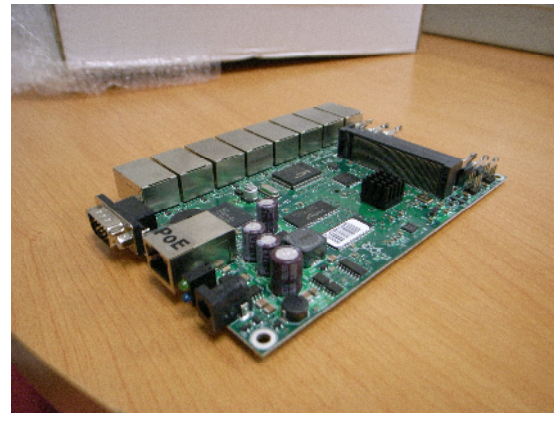


Figura 3.4. Fotografía Routerboard RB493AH

• Alimentación eléctrica de 12-28V que se puede realizar directamente con un conector jack o a través de un cable Ethernet, que suministra con un solo cable la señal de la red y la corriente eléctrica, tecnología denominada PoE (Power over Ethernet). El otro extremo del cable Ethernet PoE se conecta a un transformador inyector que dispone de tres conexiones:

Figura 3.5. Fotografía Inyector POE

• Una conexión para la fuente de alimentación.

• Una enchufe Ethernet que se conecta a algún dispositivo (switch) que permita repartir la señal de red hacia uno o más ordenadores.

• Un enchufe PoE Ethernet que llega del routerboard que está conectado a las antenas.

Se utilizan radios Mikrotik mini-PCI Mikrotik R52-n. que emiten en la banda de 5 GHz y tienen una potencia media de 25 dBm.

Figura 3.6. Fotografía Mikrotik R52n

Figura 3.7. Fotografía Routerboard con Mikrotik

Las radios se introducen en las ranuras mini-PCI que tiene el routerboard.

Figura 3.8. Fotografía "pigtail"

Las radios que están en las ranuras del routerboard tienen unos conectores para la antena muy pequeños, y no se suelen conectar directamente al cable coaxial que viene de la antena. Por eso, entre la radio y el cable coaxial que viene de la antena se intercala otro cable coaxial pequeño llamado "pigtail", que es recomendable que sean cortos para minimizar la pérdida de señal.

Una vez preparados el router y las radios se colocan en una caja hermética donde la corriente eléctrica le llegará la caja a través del mismo cable Ethernet por el que circula la señal de red.

3.3.3.- Antena sectorial

Estas antenas son ampliamente utilizadas para estaciones base, ya que sectorizan la cobertura, aumentando por tanto la capacidad del canal. La estación base está compuesta por tres (con anchura del haz de 90º) o por cuatro (ancho del haz de 60º) de este tipo de antenas. El modelo utilizado es el Interline INT-SEC-17/50-V sector VP Maxi 5 GHz, que dispone de una ganancia de 17 dBi con

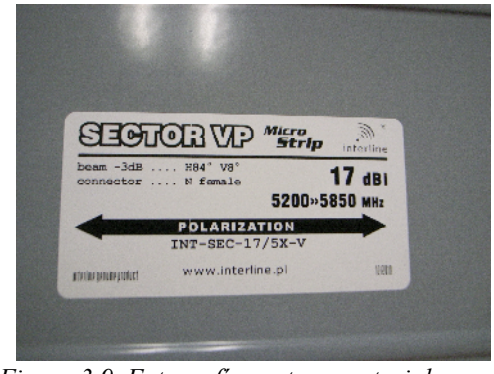


Figura 3.9. Fotografías antena sectorial

polarización vertical.

Se conecta a la caja del router (al pigtail) mediante un cable coaxial RF 5 GHz de 3 metros con conectores N-Macho/N-Macho.

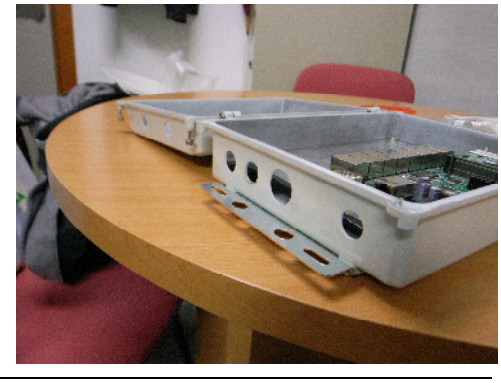
Figura 3.10. Fotografía conexión pigtail-Nmacho

3.3.4.- Antena hotspot

Para la instalación de una antena hotspot a la que se puedan conectar usuarios con equipos portátiles a 2.4 GHz se ha elegido una UBIQUITI NANOSTATION M2 2.4GHZ MIMO, con tecnología AirMAX de Ubiquiti, que permite modular en TDMA. Puede alcanzar los 150 Mbps de rendimiento real en exterior y más de 5 km de distancia. Cuenta con tecnología MIMO 2x2 que permite que la comunicación sea mucho más rápida y de mucho más alcance. Dispone de 2 conectores RJ45 (uno PoE) y una ganancia de 11dBi.

Figura 3.11. Fotografía Nanostation M2 (Hotspot)

3.3.5.- Caja estanca de aluminio



El routerboard tiene que estar muy cerca de las antenas. Por lo tanto a menudo tiene que estár a la intemperie y en principio no dispone de ningún tipo de

Figura 3.12. Fotografía caja estanca aluminio

protección. Por lo tanto se tiene que colocar en una caja para protegerlo. Hay cajas más o menos adaptadas para ello, pero en muchos casos, como en el nuestro, hay que realizar algunas modificaciones para que se adapte perfectamente a nuestro sistema.

3.4.- Instalación del supernodo en el exterior

3.4.1.- Esquema de montaje

Una vez se tiene todo el material, se configura y se da de alta en Guifi.net el routerboard con sus radios, lo que se desarrolla en el tema siguiente, y a continuación, una vez obtenidos todos los permisos necesarios, se plantea el lugar exacto de la terraza donde se va a instalar el mastil y se realiza, sobre papel, el montaje de los componentes en el mástil. La antena parabólica se situa en la parte más baja orientada hacia el norte ya que es, por su forma y dimensiones la más susceptible a moverse por el viento y, al ser direccional, sufrir perdidas de señal más importantes. Encima de la parabólica se coloca la caja estanca con el router y las radios, A continuación la antena hotspot con orientación suroeste (hacia la biblioteca del centro) y seguidamente las 3 antenas sectoriales con orientaciones oeste, sur y este respectivamente.

El esquema de la instalación es:

Encabezado

GUIFINET - UPV		
Conexión de antenas		
Símbolo	Total	Descripción
	3	Interline INT-SEC-17/50-V Sector VP Maxi 5 GHz (Antena Sectorial)
	1	Nanostation M2-2,4GHz
	1	Switch del armaric de red
	1	Rocket M5-5GHz 30 dBi 2x2 MIMO (Antena Parabólica)
	2	Routerboard RB493AH + 3 Mikrotik R52N (Caja con placa)

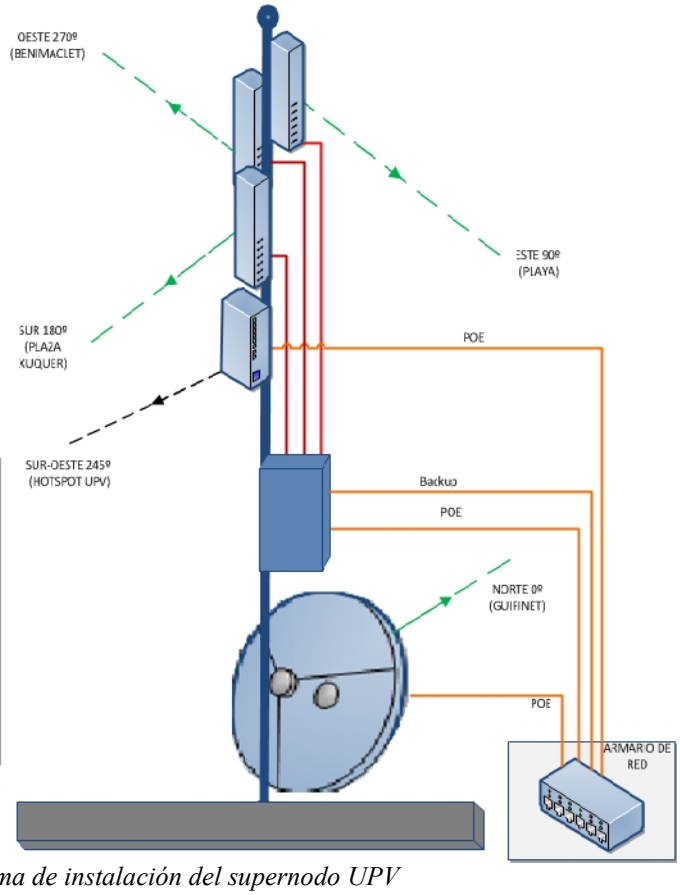


Figura 3.13. Esquema de instalación del supernodo UPV

3.4.2.- Consideraciones de montaje

Antes de empezar a instalar equipamiento electrónico en exteriores se deben tener en cuenta algunas consideraciones prácticas. Hay que observar cosas tan obvias como que debe protegerse de la lluvia, el viento y el sol, que se debe proveer energía o que la antena tiene que estar montada a una altura suficiente. Se deberá tener en cuenta:

- Como hemos visto, para la protección de los elementos electrónicos más sensibles, los hemos situado dentro de una caja metálica hermética, prestando especial atención en sellar los agujeros, sobre todo los que hemos tenido que perforar nosotros para evitar que pueda entrar el agua de lluvia o insectos.

- El suministro eléctrico a cada elemento se realiza mediante los cables de red Ethernet con el sistema llamado PoE (Power of Ethernet) según el estándar 802.3af que define un método para proveer energía, aproximadamente 13 vatios de forma segura y sin interferir con la transmisión de datos, a los dispositivos usando los pares que no se utilizan en un cable Ethernet estándar.

- Cuando colocamos antenas en mástiles o torres, es muy importante utilizar soportes separadores, y no adosarlas directamente ya que nos ayudarán en muchas funciones incluyendo separación, alineación y protección de la antena. Los soportes deben ser lo suficientemente fuertes para aguantar el peso de las antenas, y también mantenerlas en su lugar en días de mucho viento.

- El tubo del mástil que soporta las antenas debe ser circular, para que se puedan girar para alinearlas.

- Hay que tener en cuenta que, como el equipamiento va a estar en exteriores durante toda su vida de servicio, es importante asegurarse de que el material utilizado no sea fácil de oxidar.

Y una vez conocidas todas estas consideraciones, en el siguiente apartado se muestra el proceso de instalación de todo este material para la construcción física del supernodo, desde la colocación de la caja con la placa del routerboard y las radios, de las antenas y resto del material en el mástil con su cableado, hasta la colocación del mástil en la terraza de la Escuela y su conexión al armario de red del edificio.

3.4.3.- La instalación paso a paso

3.4.3.1.-Preparación de la Routerboard en la caja estanca.

La instalación completa de la routerboard, las radios con los conectores de las antenas y del puerto Ethernet en la caja estanca se realiza en el despacho. A continuación se muestra el proceso de montaje.

- Adaptación de la caja estanca

Habitualmente las cajas para la colocación de la placa del router y las radios no están diseñadas especialmente para una placa y hay que adaptarlas. La adaptación depende de la caja utilizada y de los elementos que se tengan que poner. En nuestro caso en la caja había que meter:

- La placa del routerboard modelo Mikrotik RB933.
- Las radios Mikrotik R52-n.
- Los conectores pigtail con los cables que conectan las radios con las antenas).
- Conector Ethernet POE y para conectar la antena hotspot.

Dentro de la caja hay una plancha de aluminio que se fija a la misma con unos separadores metálicos (studs). La placa del router va atornillada a esta plancha de aluminio.

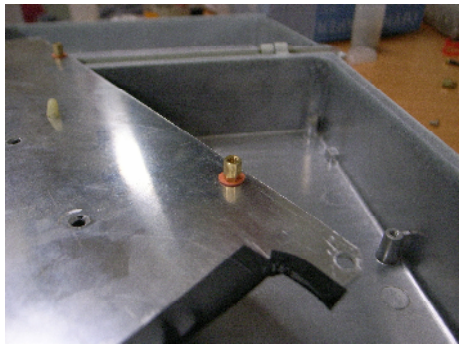
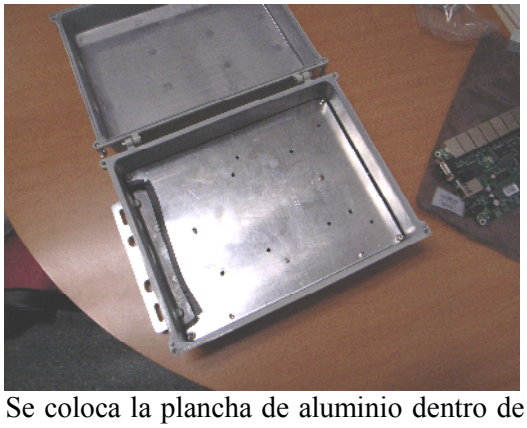


Figura 3.14. Fotografías preparación caja

Como los agujeros que tiene la caja no son suficientes para los conectores de los cables coaxiales se tiene que hacer uno nuevo. Además con la plancha de aluminio metida a la caja, no hay bastante espacio para colocar los conectores hay que limar 5 o 6 cm esta plancha en los lugares donde irán los agujeros por estos conectores.



- Colocación de la routerboard y los radios en la caja

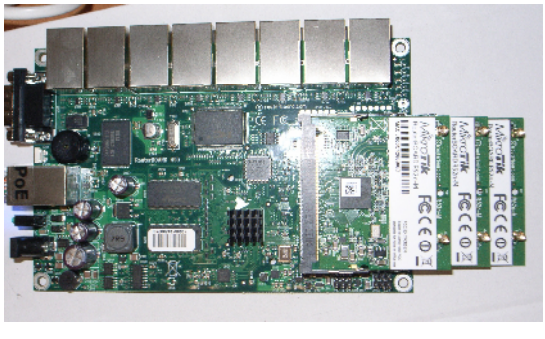


Figura 3.15. Fotografía colocación radios en router

Se coloca la plancha de aluminio dentro de la caja y sobre ella el routerboard. Se conectan las radios a la placa del router en las tres ranuras mini-PCI. Antes de meter las radios en su ranura, es recomendable apuntar el número MAC de cada una de ellas, puesto que este número es necesario para después poderlas configurar.

- Conexión de las radios a las antenas.

Se hace con dos tipos de cable:

• Los pigtails que van de la radio a la pared de la caja donde finaliza con un conector adecuado para el cable que viene de la antena

• Los coaxiales que va de la caja (concretamente del conector de los pigtails) a la antena.

Figura 3.16. Fotografía colocación pigtails

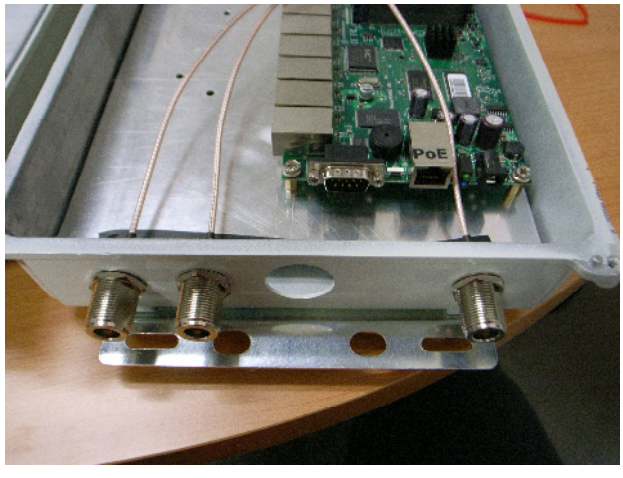


Figura 3.17. Fotografía colocación conectores N-macho

Primero se han de enroscar los conectores de los pigtails al agujero correspondiente de la caja, de forma que el conector quede fuera y poder así conectar el cable coaxial que viene de la antena

Después se tiene que conectar el otro extremo del pigtail a las radios. Cada tarjeta de radio tiene 2 sitios donde conectar el pigtail. Hay que colocarlo en el conector de la izquierda pues el otro no amplifica la señal.

3.4.3.2.- Preparación de la antena parabólica.

La antena parabólica también se monta antes de colocarla en el mástil.

Figura 3.18. Fotografías ensamblado antena parabólica

Se trata de una antena parabólica de plato solido desarrollada por Ubiquiti para lograr enlaces punto a punto superiores a 30 Kms.

El Radio Rocket M5 y la antena Rocket Dish Base AIRMAX han sido diseñados para trabajar juntos sin ningún problema. La instalación no requiere herramientas especiales, solo basta con afirmar el radio Rocket M5 en los soportes instalados en la parte posterior de la antena y conectar los pigtails.

Figura 3.19. Fotografías ensamblado Rocket M5 en Rocket Dish Base

3.4.3.3.- Instalación del cableado desde el armario de red a la terraza.

Para la instalación del mástil del nodo con sus antenas se tuvo en cuenta tanto la altura y visibilidad que debía tener, como la cercanía de un armario con electrónica de red de la universidad al que se pudiera conectar el cableado del router y antenas y así, en cierta forma, integrar a nivel físico nuestro nodo en la red de la UPV como veremos en capítulos posteriores. *Figura 3.20.Fotografía roseta tejado*

El lugar elegido, la terrada del edificio 1H de la Escuela (ETSINF) dispone, justo debajo, en el 3º piso de un armario de red, en el cual se conectó un nuevo cableado, formado por 4 cables de par trenzado, que por las bajantes del edificio, se deslizó hasta la terraza donde se instaló una caja con 4 rosetas para la conexión de los cables del nodo.

Figura 3.21. Fotografía cableado hasta armario red

3.4.3.4.- Traslado del material al punto de montaje (terraza)

Se traslada todo el material necesario para la instalación al punto donde se va a montar el nodo, es decir, a la terraza del edificio 1H de la Escuela. Desde los componentes que formarán el nodo (router, antenas, etc.) hasta el tubo del mástil, la escalera o las herramientas.

Figura 3.22. Fotografías de vistas generales de la terraza

3.4.3.5.- Instalación de los soportes del mástil.

Este soporte se fija a los lados de la pared.

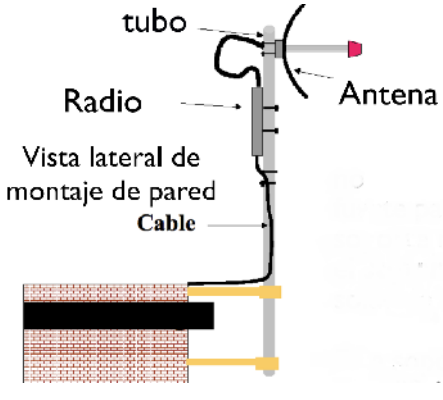


Figura 3.23. Fotografía y gráfico de los soportes del mástil

3.4.3.6.- Colocación de la caja del router y de las antenas en el mástil.

Antes de colocar el mástil en sus soportes, en el suelo, se colocan todos los elementos que deben ir sujetos a él.

En la parte inferior se coloca, orientada al norte, la antena parabólica, ya que por su tamaño y forma, como ya se ha indicado, va a tener más problemas los días de viento y al ser direccional cualquier variación en la orientación producirá fallos en la comunicación.

Encima de la antena parabólica colocamos la caja estanca con el router al que se conectará los cables procedentes del hotspot y las antenas sectoriales.

A continuación, y por este orden, se colocan en el mástil la antena de 2,4 GHz (hotspot) y las 3 antenas sectoriales de 5 GHz. El orden de las antenas sectoriales se decidió teniendo en cuenta la visibilidad, colocando más abajo las orientadas a oeste y sur cuya zona de cobertura está bastante despejada y con amplia visibilidad y en la parte más alta del mástil la antena orientada al este donde los edificios altos de la universidad obstaculizan en mayor medida la visión.

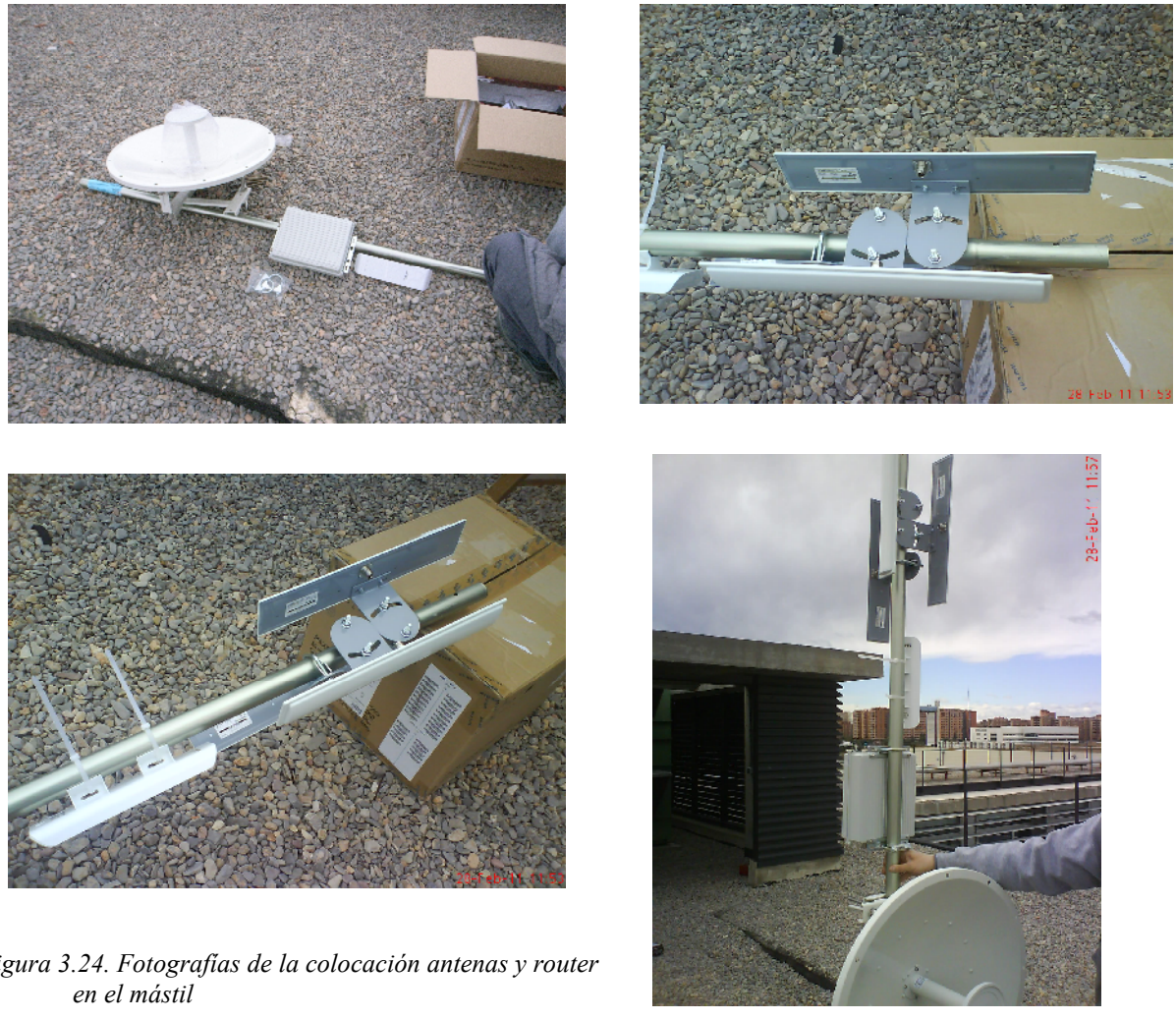


Figura 3.24. Fotografías de la colocación antenas y router en el mástil

3.4.3.7.- Cableado router y antenas

Una vez colocados los elementos en el mástil realizamos el cableado entre ellos.

En el routerboard tenemos 3 tarjetas de radios que con 3 pigtails se conectan a la caja estanca y cada conector por medio de cable coaxial se conecta a una antena sectorial. Además del segundo puerto Ethernet (eth2) se sacará un cable de par trenzado que se conectará al segundo puerto del hotspot y del primer puerto Ethernet (eth1) que es POE saldrá otro cabe de par trenzado que se conectará a las rosetas preparadas en la terraza.

De los puertos POE del hotspot y de la antena parabólica también salen cables de par trenzado (un cable de cada uno) que asimismo se conectarán a las rosetas

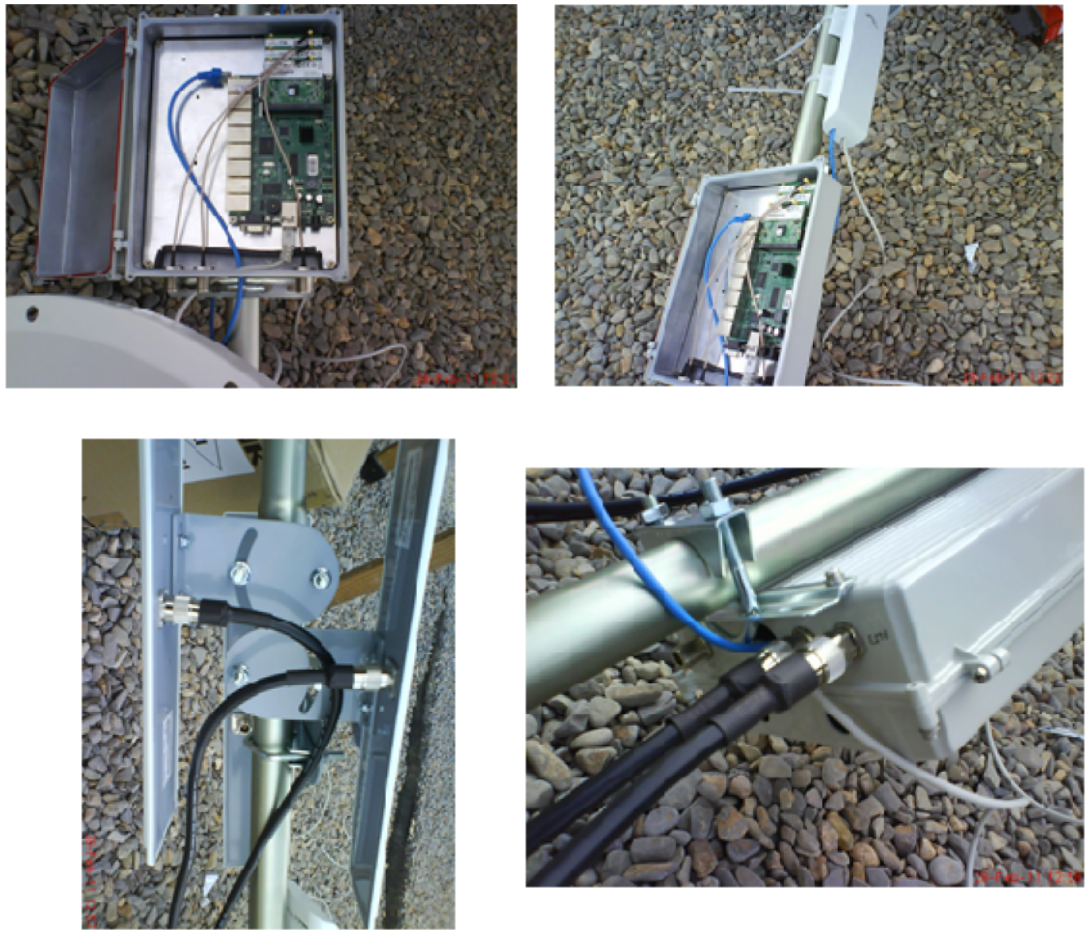


Figura 3.25. Fotografías del cableado entre antenas y router

3.4.3.8.- Colocación del mástil en sus soportes y de los tensores.

Una vez realizada la instalación y fijación de todos los componentes en el mástil y el cableado entre ellos, se procede a la colocación del conjunto en el soporte preparado para el mástil.

También se colocan 3 tensores de acero, en ángulos de 120º, desde la parte superior del mástil a distintas partes de la terraza para evitar lo máximo posible que el viento mueva las antenas.

Figura 3.26. Fotografía de los tensores del mástil

3.4.3.9.- Cableado y orientación de las antenas

Con todas las antenas situadas en el mástil, y antes de apretar definitivamente todas las sujeciones, se vuelve a comprobar la orientación de las antenas.

A continuación se conectan en la roseta los 3 cables de par trenzado POE procedentes del router, hotspot y antena parabólica y que por el cableado del edificio bajan hasta el armario de red del 3º piso de la Escuela.

Figura 3.27. Fotografía del cableado del nodo hacia la roseta

Figura 3.28. Fotografía de la roseta del tejado

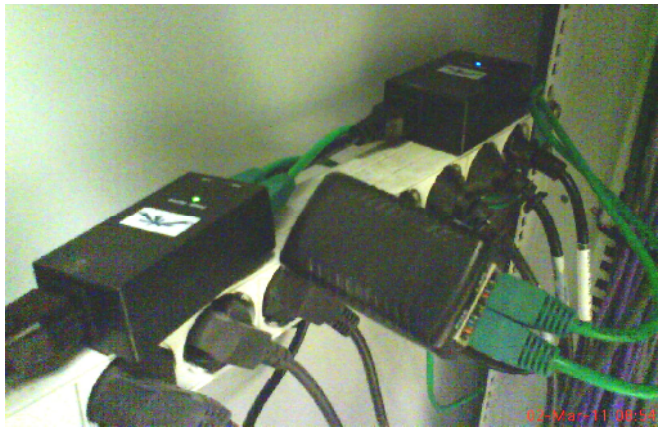


Figura 3.29. Fotografía de los inyectores POE en el armario

Allí se pincha un cable en cada uno de los 3 conectores del armario, con cableado procedente del mástil, que seconectará a un "inyector" del que se sacan 2 cables: uno de alimentación que se conectará a la regleta eléctrica y otro Ethernet que conectamos a la electrónica de red (switch).

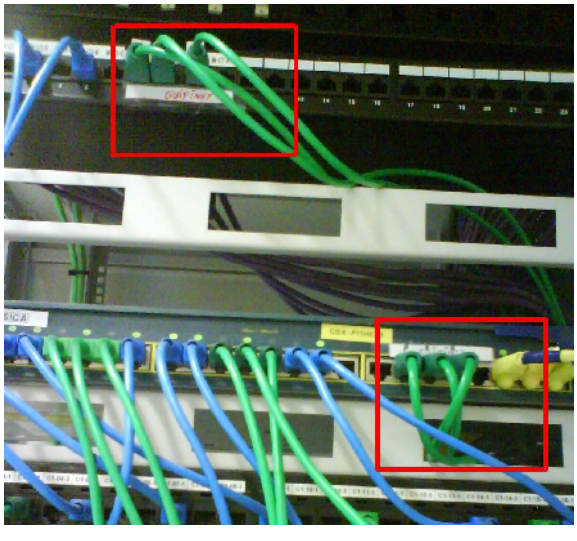


Figura 3.30 Fotografía de las conexiones en el armario de red

Figura 3.31. Fotografía de las conexiones en el switch

3.4.3.10.- Test de funcionamiento.

Una vez realizada toda la instalación comprobamos, conectando un portátil con una aplicación que detecta conexiones inalámbricas de un amplio rango de frecuencias, que las antenas se visualizan con su ESSID, frecuencia y canal indicados.

Y con todo ello damos por finalizada la instalación física del supernodo Guifi.net de la UPV (UPVone)

Figura 3.32. Captura de las señales del test de funcionamiento

Figura 3.33. Fotografía de la instalación final con los que intervinieron en ella.

CAPÍTULO 4:

CONFIGURACIÓN DE LAS ANTENAS

4.1.- Dar de alta una nueva zona

Guifi.net se estructura en zonas. Cada zona puede tener unos servicios por omisión (servidor de gráficas, DNS, proxy, estadísticas) que suele heredar de la zona superior de la que cuelga. A las zonas se pueden añadir subzonas.

Normalmente se crean zonas por cada provincia, y dentro de éstas por cada población. Un nodo puede estar geográficamente en una zona y conectarse a una radio de cobertura de otra zona si tiene mejor visión. La división es puramente organizativa, sin tener otro significado.

A las zonas se les asignan bloques de direcciones IP con el interés fundamental de facilitar la sumarización de rutas y reducir la tabla de encaminamiento de los routers

Para crear una zona se accede a la web http://Guifi.net

Figura 4.1. Página de inicio de la web de Guifi.net

4.1.1.- Crear un nodo multirradio

En la jerga guifi le llaman supernodo cuando un nodo tiene más de una radio. El supernodo se establece cuando, además de recibir señal como cliente, propagamos la señal hacia otras ubicaciones ampliando así la cobertura y el alcance de la red libre.

Elementos comunes de un nodo multirradio:

- Antenas de cobertura. Normalmente abren 90 ó 120º y tienen la ganancia a partir de 14dbi. Las omnidireccionales se usan poco.
- Antenas para enlazar con otros nodos. Normalmente direccionales, menos de 30º de apertura y la ganancia a partir de 19dbi.
- Un router que participe en el encaminamiento dinámico.

Dar de alta nodos multirradio sigue un proceso similar al de crear nodos cliente. Se sitúa la ubicación, se añade el router (el *trasto*) y se añaden radios.

Las radios pueden ser de los siguientes tipos:

- Una radio de cobertura. Por omisión recibe una IP de red 10.x.y.z/27 (para 30 direcciones). La primera IP la asigna a esa radio (y quedan 29 direcciones para nodos cliente). Estas direcciones son públicas en guifi.net.
- Un enlace troncal. Sirve para enlazar nodos multirradio. Por omisión recibe una IP de red 172.x.y.z/30 (para dos direcciones). Estas direcciones no se activan en guifi.net. Solo sirven para hacer los enlaces.
- Una radio para un *hotspot*. Los hotspot son puntos de acceso para conectarse directamente con ordenadores o teléfonos. Por omisión reciben una 192.168.x.y/24. Estas direcciones son para hacer redes privadas en guifi.net. Estas IPs no se deben publicar y propagar en el encaminamiento dinámico.

En ocasiones a una radio se le puede dar más de una función. Por ejemplo, una antena de cobertura se puede aprovechar para hacer un enlace punto a punto con otro nodo multirradio. Esto se hace para abaratar el precio del nodo o porque no hay espacio disponible en la ubicación. Si es posible siempre es mejor separar las radios.

4.1.2.- Esquema de red y componentes del supernodo de la UPV

Antes de empezar a dar de alta cada componente en la web de Guifi.net, de configurar el router y las radios y del montaje físico de las antenas se realizó un esquema de conexiones, tanto inalámbrico como cableado cuyos valores se fueron concretando conforme se iban obteniendo las direcciones

desde Guifi.net, cuando se creó la VLAN y cuando se conectó con el servidor de VPN de la UPV. El resultado final es el siguiente esquema de red del Nodo UPVone de la UPV.

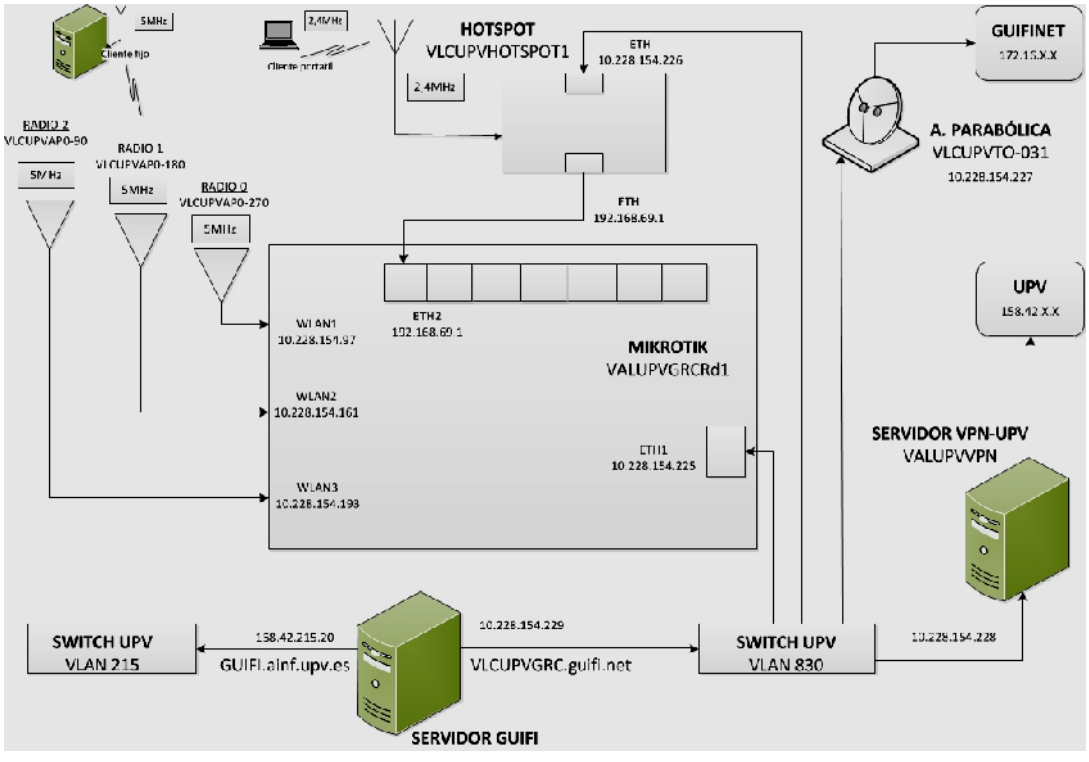


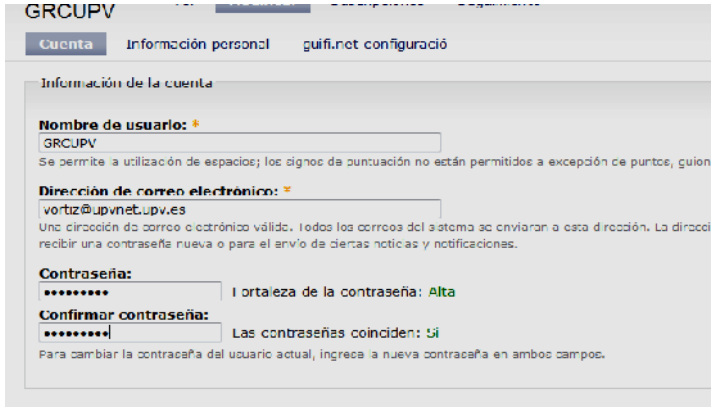
Figura 4.2. Esquema de red del nodo UPVone de la UPV

4.2.- Creamos el Supernodo VLCupvGRC (UPVone)

4.2.1.-Dar de alta usuario y trastos en Guifi.net

La configuración de las antenas se debe realizar también desde la Web de la Guifi (http://www.guifi.net).

En primer lugar nos damos de alta (registramos) en la página de Guifi.net en "Crear nueva cuenta" situado a la parte superior derecha de la página. Se pide un nombre de usuario (GRCUPV), una dirección de correo electrónico y después nos pide una contraseña.



A continuación se accede a la página web de Guifi.net con el usuario registrado introduciendo el nombre de usuario (GRCUPV) y la "contraseña" en la parte superior de la página. Luego, una vez identificado, accedemos a la url de mapas "/guifinet/Valencia/mapas" e indicamos la situación física donde se colocara el mástil con las antenas. Para ello, nos situamos arriba en la página, justo encima de "Iberian Peninsula", y navegamos hasta la zona donde queremos plantar nuestro nodo. Una vez encontrada la ubicación pulsamos sobre ella, aparece un globo y pulsamos en "Add new node here".

Una vez situada la ubicación de las antenas se rellenan el resto de campos solicitados en el alta:

- nombre de red: Será el nombre del nuevo nodo. Se recomienda nombre de institución, población con calle… **(UPVone)**
- nombre corto: nombre abreviado del nodo. Será el que aparecerá en los dispositivos. Se inicia con las siglas de la zona geográfica. **(VALUPVGRC)**
- Aceptamos la licencia XOLN.
- Contactar: Dirección de correo electrónico de quien va a gestionar el nodo. Pongo la mía de la universidad.
- Zona: donde se encuentra nuestro nodo **(Barrio)**
- Altura de la antena: respeto el suelo **(12 metros)**

Figura 4.3. Página web del nodo UPVone en Guifi.net

Vista más detallada de la ubicación en la terraza del edificio 1H de la Escuela Técnica Superior de Ingeniería Informática de la UPV.

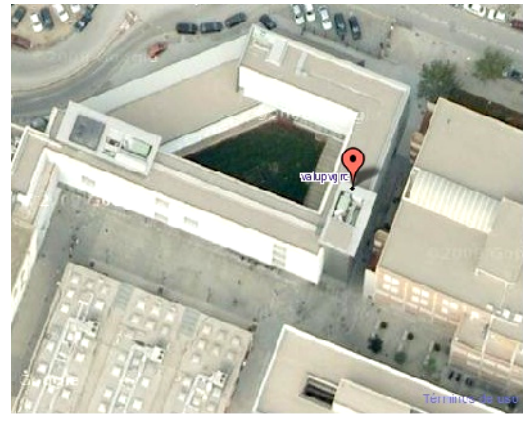
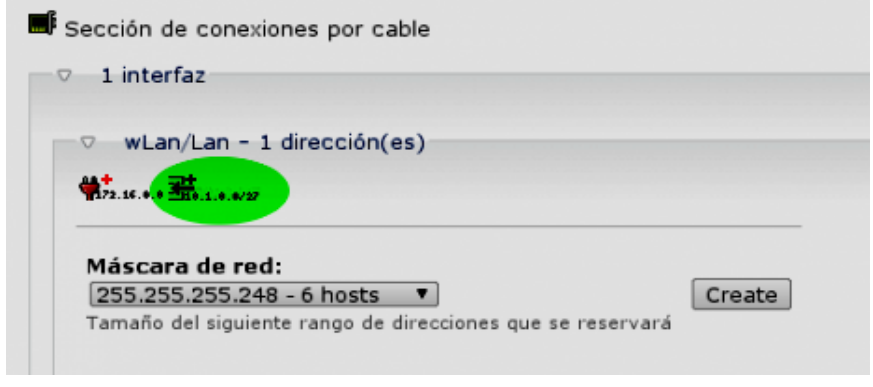


Figura 4.4. Vista detallada de la ubicación

4.2.2.- Reserva de direcciones IP para conexiones de cable

Una vez introducidos los datos solicitados se procede a reservar un paquete de direcciones IP para poder crear una red cableada que asocie los distintos elementos que van a intervenir en el supernodo, como nuestro servidor, el router o la conexión con el servidor VPN de la UPV y para ello se accede a la sección de conexiones por cable y le pedimos a la web un rango de 6 IPs.



Se reserva un rango de direcciones de la red 10.228.154.224 con máscara 225.225.225.248 que asignaremos a:

Mikrotik (Routerboard) → 10.228.154.225

Hotspot → 10.228.154.226

Antena parabólica → 10.228.154.227

Servidor VPN-UPV → 10.228.154.228

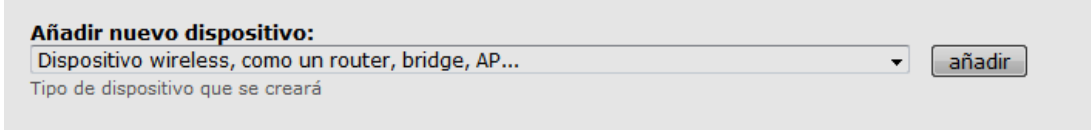
Servidor Guifi.net UPV → 10.228.154.229

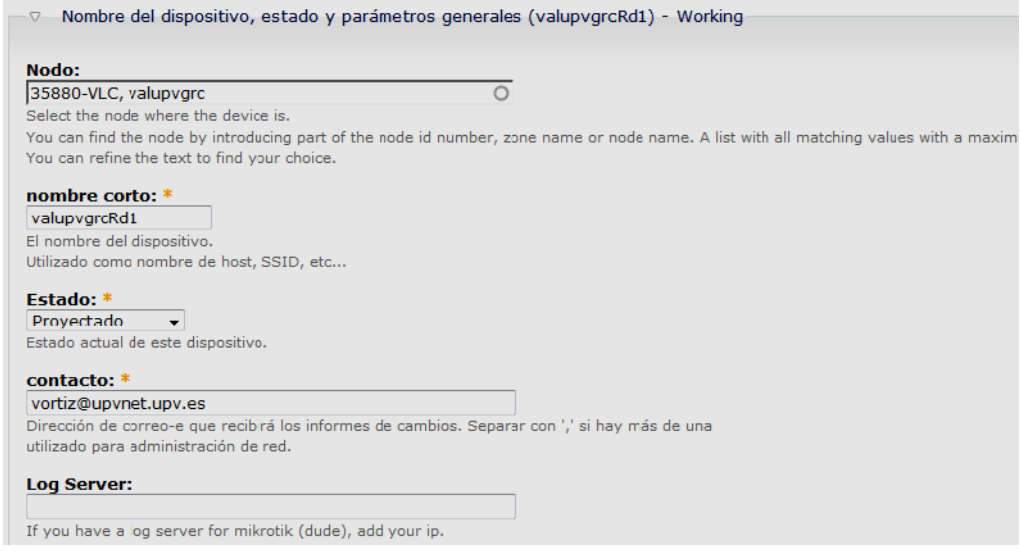
4.2.3.- Añadir el Routerboard para el nodo multirradio

Cuando se empiezan a añadir los elementos para crear el supernodo en la web se debe tener claro todos sus parámetros y el objetivo que debe cumplir cada uno.

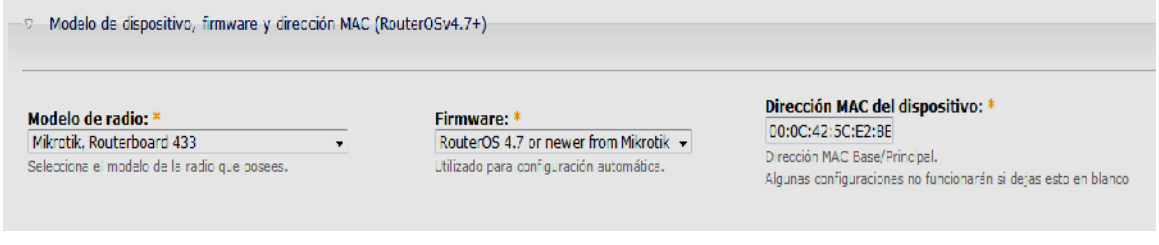
El primer dispositivo que se añade es el Mikrotik, Routerboard 433 (debemos poner éste, que es el más parecido, ya que el nuestro, routerboard RB493AH, no está en la base de datos).

Para añadirlo, accedemos por añadir nuevo dispositivo, Dispositivo wireless, como un router, bridge… pulsamos en "añadir" y rellenamos el formulario.





4.2.3.1.- Modelo del dispositivo, firmware y dirección MAC (RouterOSv4.7+)



4.2.3.2.- Recomendaciones para los ESSID

Los ESSID (o *Extended* SSID *Service Set IDentifier*), son los nombres de las radios o puntos de acceso wifi. La web de guifi propondrá nombres para las radios a partir del nombre que genera para el router. Recomendamos modificar esos nombres para hacerlos más claros:

- Dejar el nombre corto. La web siempre añade «guifi.net-» delante.
- Añadir detrás: AP (si es una antena de cobertura) o T (troncal).
- Añadir detrás: un número empezando por 0 para numerar cada tipo de antena.
- Añadir detrás: -xyz indicando la orientación de la antena (el azimut). Si la antena es una omnidireccional, poner -OMNI en vez del azimut.

Esta forma de poner los nombres para las radios facilita tanto el trabajo de campo como seleccionar los enlaces en la web. Si los ESSID de las antenas no coinciden con los de guifi.net,

herramientas como el *unsolclic* no sirven y tampoco se puede hacer una preconfiguración de los nodos cliente.

4.2.4.-Configurar los radios y WLANs: rango de IPs, orientación…

El siguiente paso es el configurar los radios. Se van a instalar un total de 5 antenas, 3 del rango de 5 GHz (802.11 a) para punto de acceso a la red de los usuarios de guifi.net, 1 antena parabólica, también 802.11 a, completamente direccional, para la conexión punto a punto con otro supernodo y que haga, por lo tanto, de backbone enlace y por último, otra del rango de 2,4 GHz (802.11 g) que haga de hotspot. Para cada radio se reservan 30 direcciones IP. Las 2 últimas antenas (parabólica y hotspot) no es necesario darlas de alta en la Web, pero lo hacemos, para que se reserven direcciones IP también para ellas.

4.2.4.1.- Recomendaciones para los canales

Se volverá sobre este tema más adelante. La banda de frecuencia pensada para exterior es la de 5GHz. La de 2,4GHz es para redes dentro de edificios. En la banda de 5GHz hay más canales disponibles. En general es mejor poner canales más bajos para antenas de cobertura y canales altos para enlaces de troncal. En 5GHz se puede usar más potencia (hasta 1 watio pire) que en 2,4GHz (0.1 watio pire).

La razón de recomendar los canales bajos para antenas de cobertura es que la potencia de 1 watio no es para todos los canales, es para unos cuantos de los de frecuencia más alta y parece razonable dejar estos canales para los enlaces punto a punto.

En cualquier caso, para elegir el canal, conviene hacer un scan para ver los canales ya ocupados. En el caso de un enlace punto a punto, hay que hacerlo necesariamente en los dos extremos para asegurarnos de que el canal está libre en las dos ubicaciones a enlazar.

Para diferenciar si es una antena de cobertura o para enlaces de troncal hay que usar las opciones de la radio. Si ponemos un rango de direcciones públicas, normalmente será de cobertura. Por defecto será para 29 nodos cliente. Al crear la radio podemos seleccionar una máscara diferente para aumentar el número de nodos cliente. Se desaconseja más de 60 nodos cliente para una misma radio.

4.2.4.2.- Configuración de los radios

Los nombres de los 3 primeros radios, correspondientes a los puntos de acceso para conexiones de 5 GHz, estarán estructurados de la siguiente forma:

Ciudad – Universidad -Punto Acceso Nº - Orientación en grados.

De está forma cuando veamos el nombre de la antena sabremos perfectamente a que antena se van a conectar. Se siguen los pasos de creación de la radio (ESSID, permite clientes, etc.) y en la misma

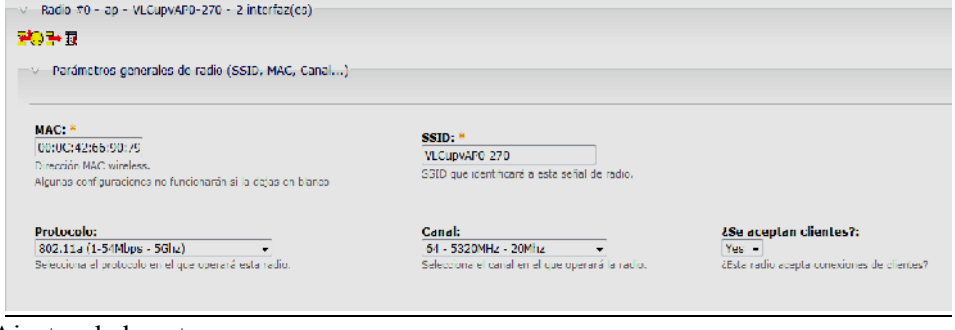
radio se pide el rango de direcciones IP (10.x.x.x) para lo clientes que por defecto se asignaran para 30 hosts.

El primer radio (Radio 0) se va a configurar para la antena con orientación Oeste (270º) y se realizara una conexión en bridge que nos servirá al mismo tiempo para configurar la conexión IPV4 del Routerboard.

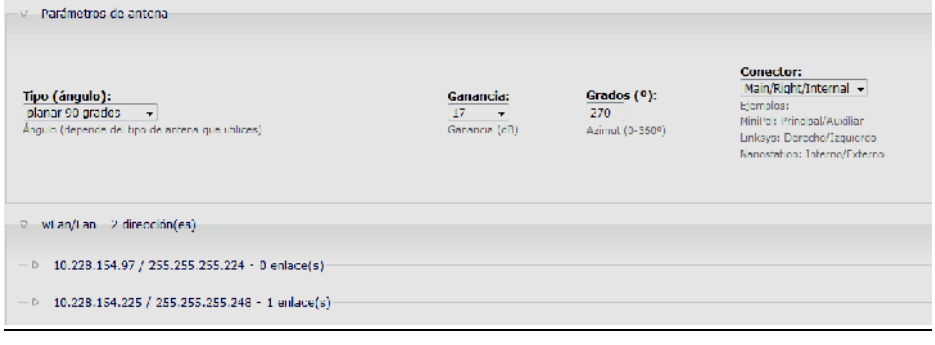
Una vez rellenado el formulario, la configuración del radio 0 quedará:

- *Radio #0 - ap - VLCupvAP0-270 - 2 interfaces*

  Ajustes principales de Radio (ESSID, MAC, Canal...)



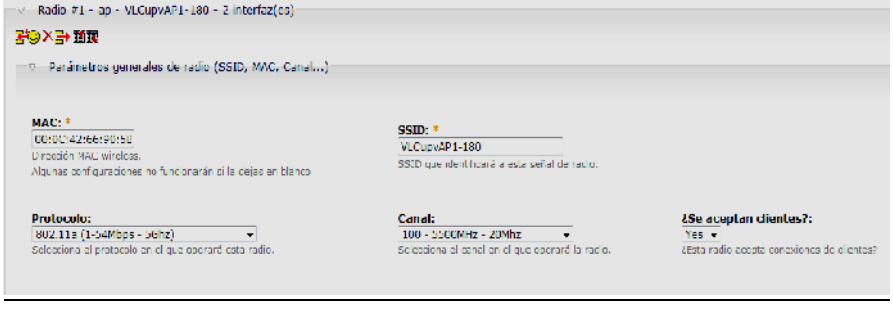
  Ajustes de la antena



La configuración de los radios 1 y 2 es equivalente con las orientaciones Sur (180º) y Este (90º) respectivamente. La única diferencia es que para estás 2 antenas no se indica automáticamente el rango de IPs de cada una y hay que darlo manualmente.

- *Radio #1 - ap - VLCupvAP1-180 - 2 interfaces*

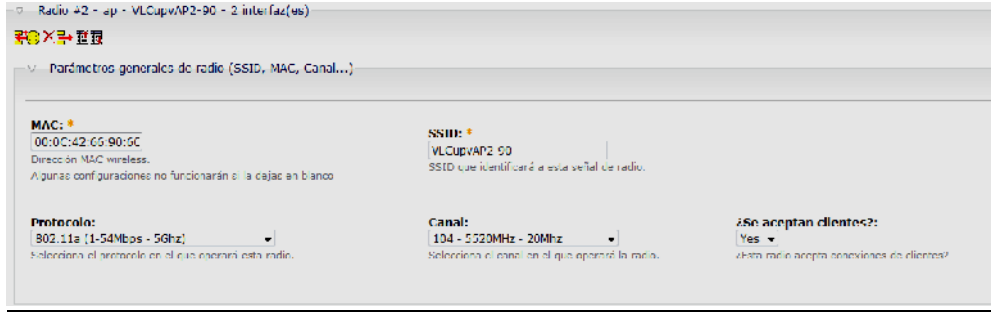
  Ajustes principales de la Radio (SSID, MAC, Canal...)



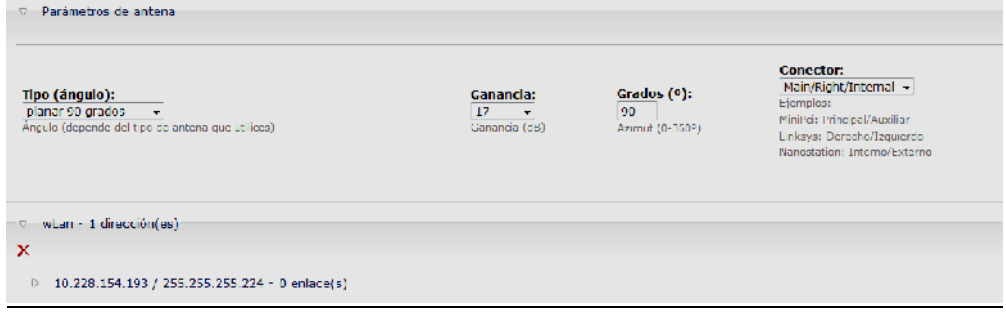
Ajustes de la antena

- *Radio #2 - ap - VLCupvAP2-90 - 2 interfaces*

Ajustes principales de la Radio (SSID, MAC, Canal...)



Ajustes de la antena



El hotspot y la antena parabólica, como se ha indicado, no es necesario inscribirlas como radios, pero se hace para reservar direcciones IP. Los inscribimos como radios 3 y 4 respectivamente y su configuración es equivalente a los radios anteriores con pequeños matices como en el nombre que en el caso del hotspot se coloca en lugar del nº de ap y los grados la palabra HOTSPOT y el nº que es por si hay más de 1. En el caso de la antena parabólica se sustituye por T0 (indicativo de Troncal) y los grados de orientación.

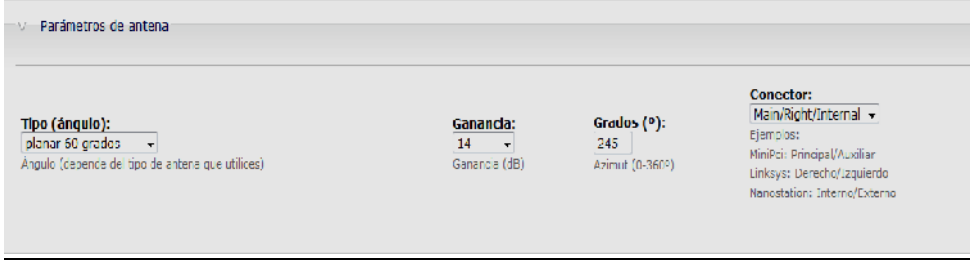
Respecto a los grados, para poder orientar estas antenas hacia el destino elegido se visualiza el mapa de perfiles que nos suministra la propia Web de Guifi.net y se calcula la curvatura del nodo.

La configuración de los dos radios quedará:

- *Radio #3 - ap - VLCupvHOTSPOT1 - 1 interface*

  Ajustes principales de la Radio (SSID, MAC, Canal...)

  Ajustes de la antena

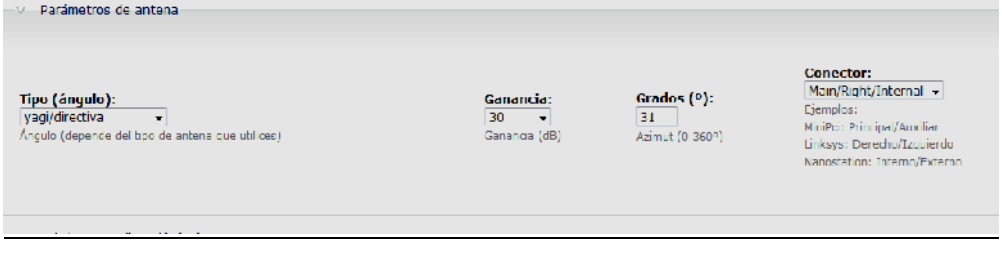


Se le da manualmente la dirección IP para su red privada (192.168.69.254)

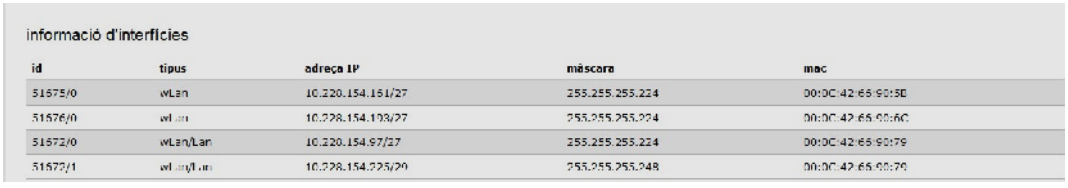
- *Radio #4 - ap - VLCupvT0-031 - 1 interface*

  Ajustes principales de la Radio (SSID, MAC, Canal...)

  Ajustes de la antena



El resumen de las interfaces de las antenas sectoriales y del Routerboard es:



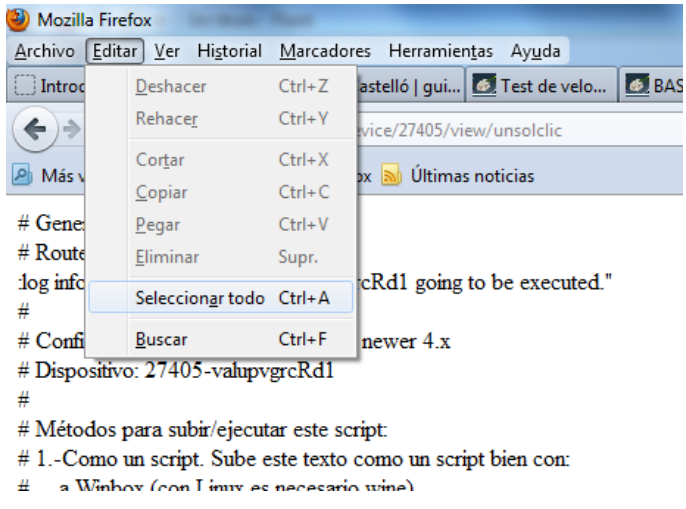
4.3.- Con «unsolclic» preparar el archivo de configuración.

El siguiente paso será introducir la configuración de los interfaces en el Mikrotik, para lo que se utilizará un script que nos suministra la Web de Guifi.net.

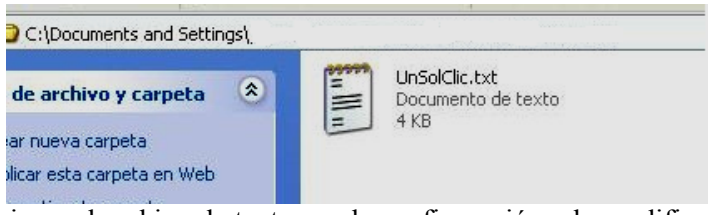
Se configurará el router y sus interfaces con los parámetros que hemos introducido en la Web de Guifi.net para poder conectarnos al punto de acceso que anteriormente hemos seleccionado.

Para ello utilizaremos la opción "unsolclic". Accedemos a la página de nuestro dispositivo (http://guifi.net/es/guifi/device/27405) y clicamos en el enlace "unsolclic".

Nos aparecerá una pantalla con el texto del fichero de configuración del Routerboard, (el fichero de configuración completo se encuentra en el anexo C) y en nuestro navegador pinchamos en "EDITAR-SELECCIONAR TODO"

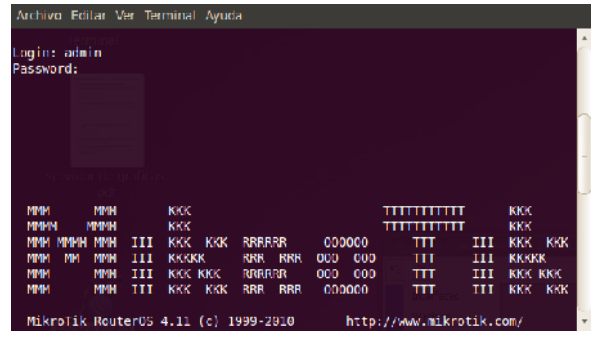


Y una vez lo tenemos todo seleccionado "EDITAR-COPIAR" y guardamos el fichero de configuración en un archivo de texto plano.



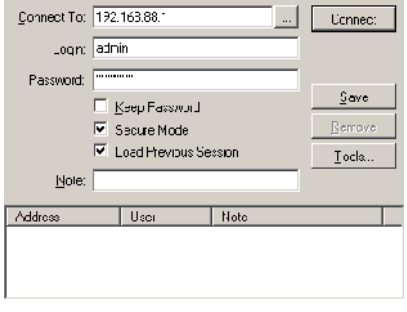
A continuación, abrimos el archivo de texto con la configuración y lo modificamos eliminando los bloques que hacen referencia al hotspot y la antena parabólica (radios 3 y 4 respectivamente) y se vuelve a guardar.

4.4.-Bajar y cargar el fichero de configuración del Mikrotik. (Winbox)



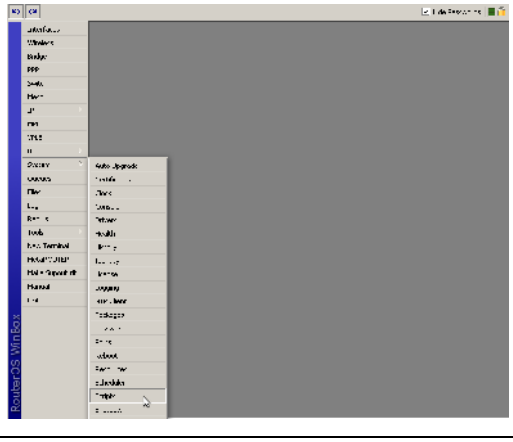
Lo siguiente consiste en copiar la configuración que contiene el archivo de texto en el Mikrotik (routerboard). Lo primero que haremos pues será conectar el RouterBoard, con sus tarjetas miniPCI ya conectadas, a un portátil, con sistema operativo XP por el puerto 2 de la RB (conectamos el Mikrotik, por su conector POE a la alimentación y al portátil) y asignamos al portátil una IP del rango 192.168.88.0/24 (192.168.88.10), teniendo en cuenta que la IP por defecto de la RB es la 192.168.88.1.

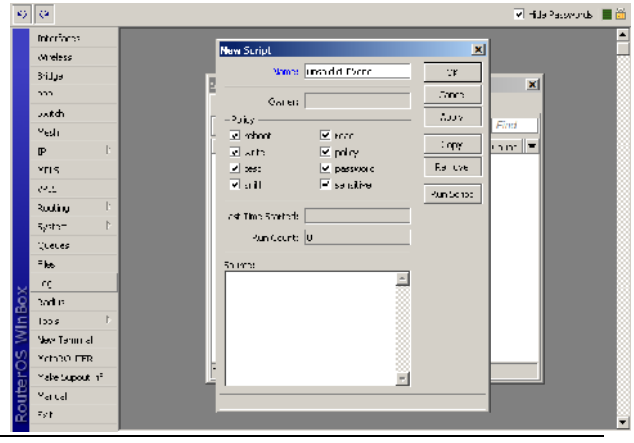
Accedemos al RB por medio de telnet a la IP 192.168.88.1, con el login: *admin* y sin password.



Para configurar el Mikrotik necesitamos Winbox, un programa de gestión del routerOS, para windows, pero con el wine es posible hacerlo funcionar en Linux. Descargamos el programa winbox.exe de la página de Mikrotik: *http://www.mikrotik.com/download.html*.

Se ejecuta el programa y pulsar en el botón de los tres puntos [...]. Al cabo de un rato aparecerá nuestro routerboard. "Se le da al botón de conectar.

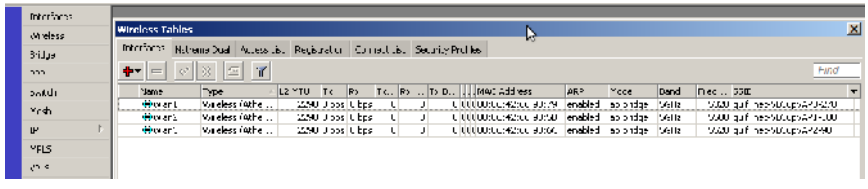




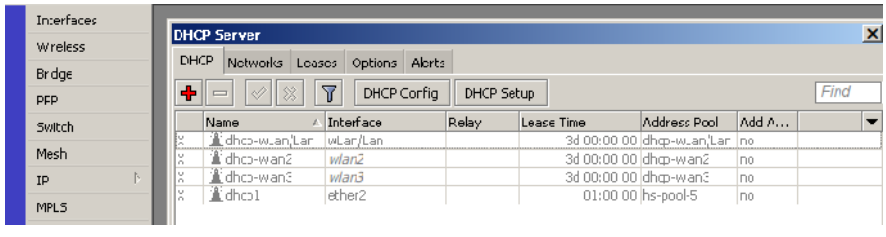
Dentro de winbox ir a "Sistema - Scripts"

y añadir uno nuevo copiando el texto de configuración que hemos seleccionado y editado en el archivo de texto.

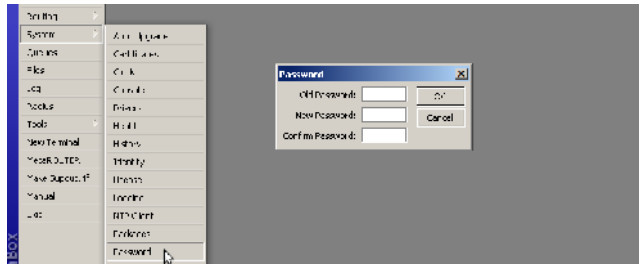
Tras ejecutarlo las radios están deshabilitados. Se deben activar desde wireless/interfaces.



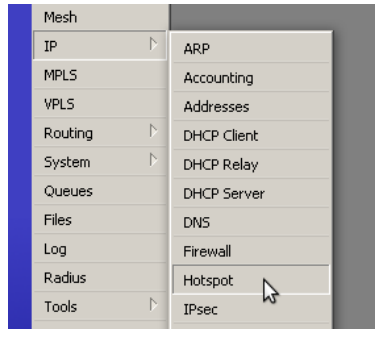
Los 2 últimos pasos serán desactivar el DHCP desde IP/DHCP server



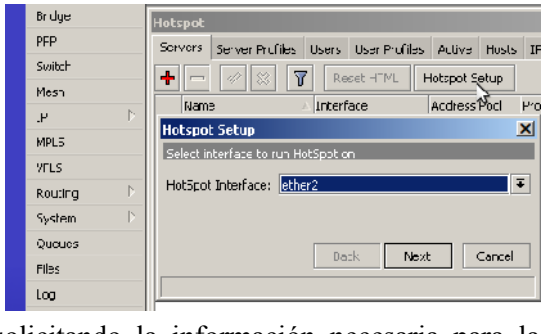
y ponerle password al Routerboard desde system/password



4.5.- Configurar el hotspot



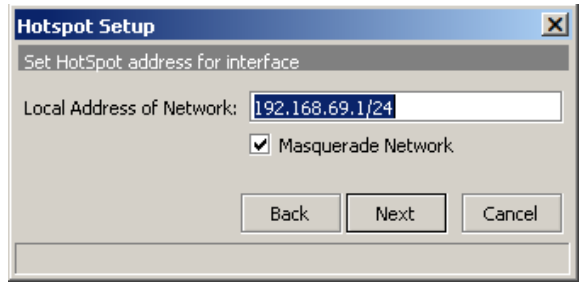
El último elemento que nos queda por configurar es el hotspot. Físicamente tiene 2 conexiones de red, una conexión POE que irá conectada a la alimentación y a la red Guifi.net y la otra que se conecta un puerto Ethernet del routerboard (Mikrotik).



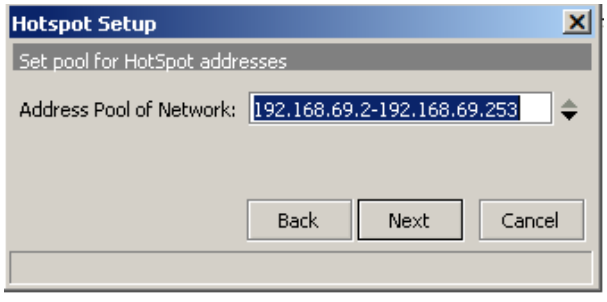
La primera parte de la configuración se realiza en el Mikrotik por medio de la aplicación Winbox. Para ello, accedemos a IP/Hotspot:

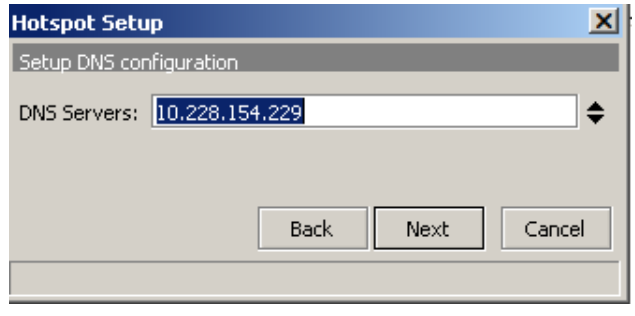
Una vez en la pantalla del hotspot se pulsa sobre el botón Hotspot Setup y un asistente nos va solicitando la información necesaria para la configuración del hotspot en el Mikrotik como que conexión del hotspot al routerboard se hará por el 1º puerto Ethernet de la tarjeta (Ether2).

La dirección IP y la máscara de la red interna del hotspot

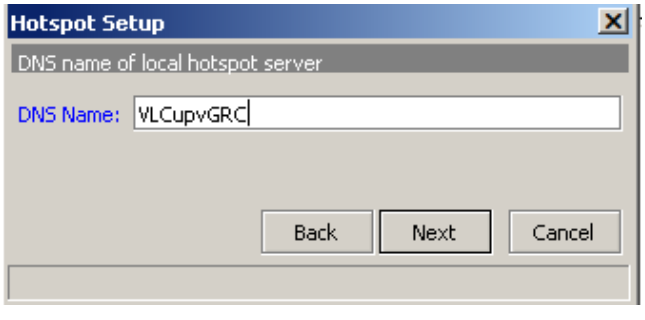


El rango de direcciones IP que dará el hotspot por DHCP, que será del 192.168.69.2 a la 192.168.69.253 dejando la 192.168.69. 254 para ponérselo a mano a la nanostation (aunque, en principio, no hace falta).



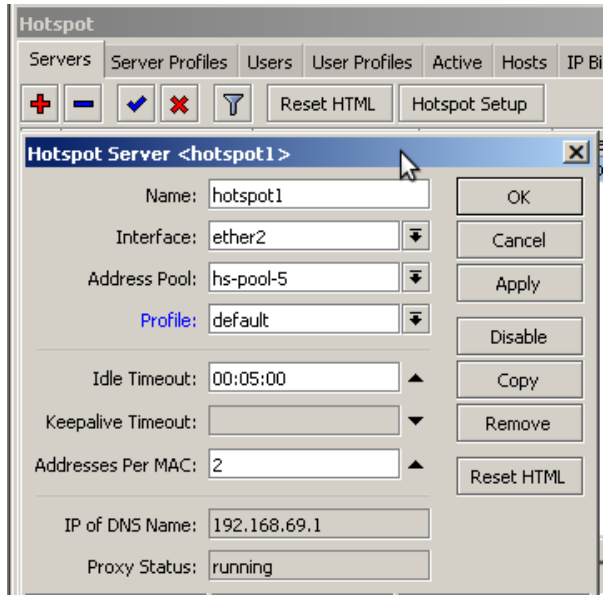


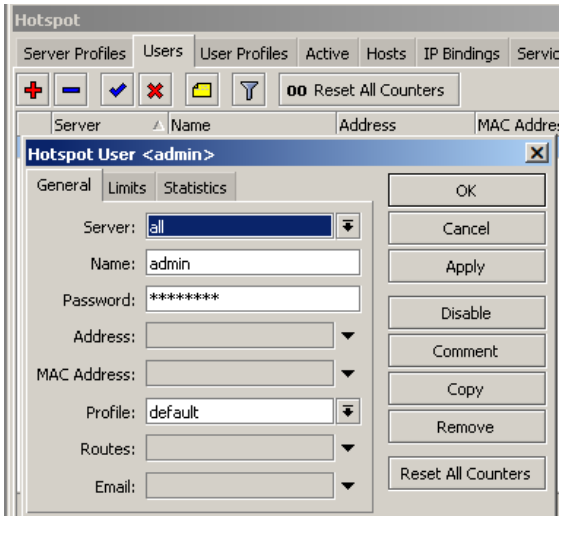
Le diremos que no queremos certificado y nos pedirá la dirección IP del equipo que va a hacer de servidor de DNS dentro de nuestra VLAN de la red Guifi.net (10.228.154.229)



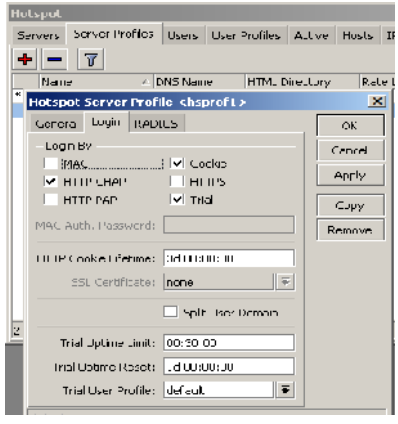
El nombre que tiene (o va a tener) este servidor DNS (VLCUPVGRC).

Una vez acabado el asistente, solo nos quedará indicarle cual es la IP del servidor DNS para la red interna del hotspot, que debe ser su IP.



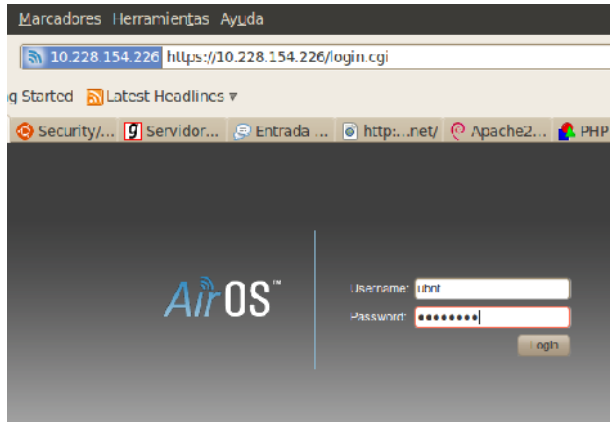


Dentro de la pestaña Users/General indicar el password del administrador (admin), para acceder al hotspot.



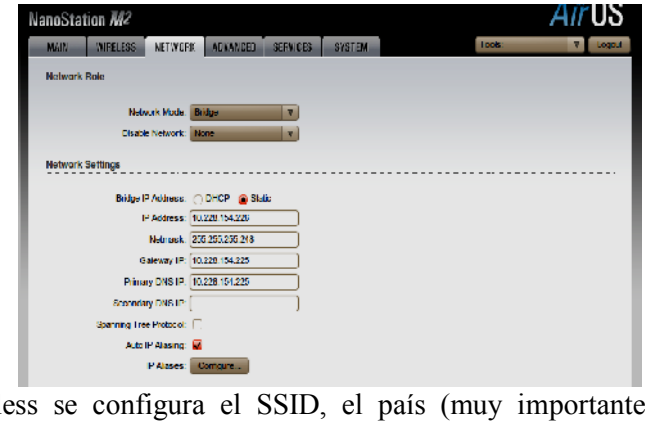
Y dentro de la pestaña Server Profile/login quien se puede logear y el tiempo de conexión.

La segunda y última parte de la configuración del hotspot se realiza en la propia nanostation. Para ello se utiliza su propio programa de configuración, el AirOS, al que se accede por Web, poniendo como URL la dirección IP del nano, en nuestro caso la 10.228.154.226.

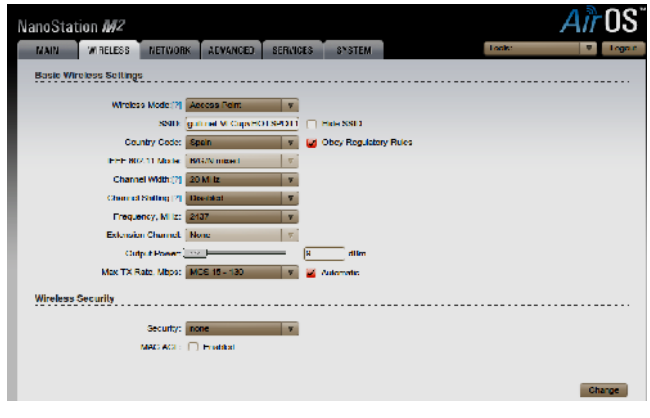


Lo primero que nos solicita es el login (ubnt) y el password que hemos puesto para él desde el Mikrotik.

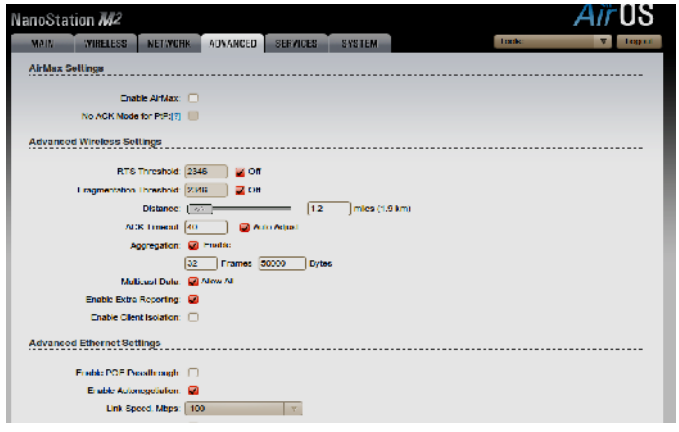
Una vez dentro del programa, accedemos a la pestaña Network, donde lo configuraremos en modo bridge, y le daremos de forma estática sus valores de red: IP, mascara, Gateway DNS. No activamos el protocolo spanning tree pero si que se activa el auto IP Aliassing.



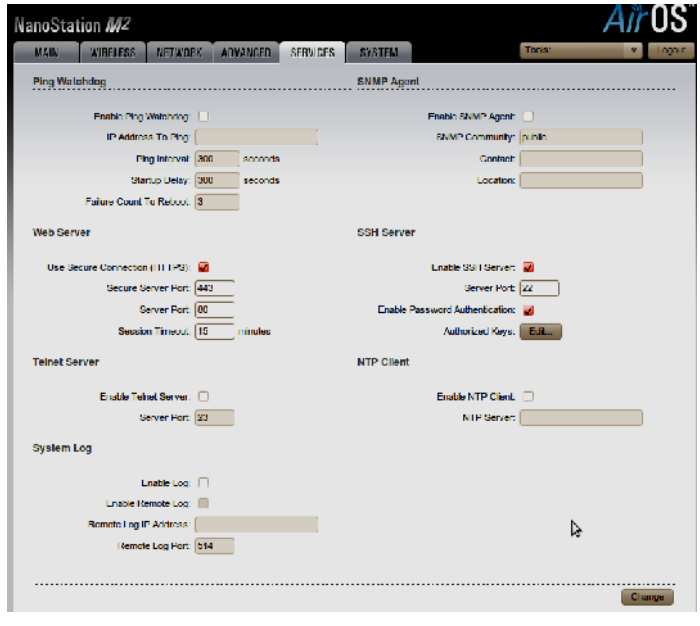
En la pestaña Wireless se configura el SSID, el país (muy importante por la diferencia de frecuencias entre Europa y EEUU dentro de la norma 803.11a del rango de 5 GHz), canal, frecuencia, etc…y deberá quedar:



En la pestaña ADVANCED se indicara NO en Enable AirMax y que la distancia es de 1,2 millas.



Por último en la pestaña SERVICES se activarán solo el HTTPS y el SSH.



Finalmente se aplican los cambios y finaliza la configuración.

CAPÍTULO 5:

AÑADIR EL SERVIDOR Y LOS SERVICIOS

5.1.- Añadir un servidor

5.1.1.- Elección del servidor y los servicios

Una vez realizada la instalación física y la configuración del routerboard y las radios de las antenas, la siguiente acción será añadir un servidor al nodo multirradio. Siguiendo las instrucciones y recomendaciones de la web de guifi.net se plantea la instalación de un servidor GNU/Linux que proporcione diversos servicios y funciones para los usuarios y para la red. Los servicios elegidos son:

- Servidor web para poner documentación, noticias, gráficas, etc. del supernodo.
- Servicio DNS. para resolver los nombres de los dispositivos por su nombre y no su IP
- Servidor de gráficas para graficar el estado de los nodos y supernodos. (las gráficas se verán tanto en las páginas de los nodos de Guifi.net como en el propio servidor).
- Servidor de Reloj. Para que todos los dispositivos dispongan de la misma hora, lo que facilita la identificación de problemas en los logs y la sincronización de los mismos
- Servidor de vpn para la conexión con los servidores de Guifi UJI-Castellón y con la UPV.

Para realizar todas estas funcionalidades se ha hecho uso completamente de software libre, por lo que no se ha tenido que adquirir ninguna licencia. A continuación se lista el software utilizado. En los apartados sucesivos se detallará la instalación y la configuración de los mismos.

- El sistema operativo utilizado ha sido **Ubuntu 10.04 server LTS**, que es un sistema operativo Linux basado en Debian.
- Como servidor web se ha elegido **Apache HTTP Server** que es un servidor web de código abierto para sistemas Unix/Linux, Microsoft Windows y otros.
- El servidor de nombres utilizado ha sido **dnsmasq** que es un ligero servidor DNS, TFTP y DHCP.

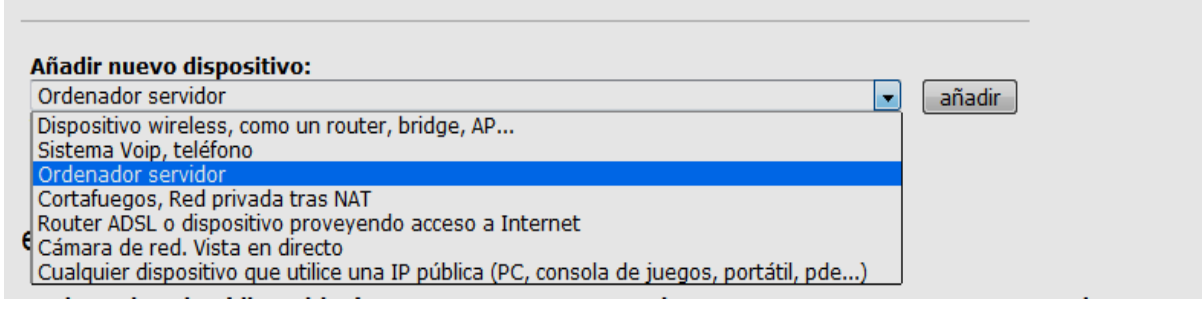
- Para el servidor de gráficas se utiliza el **SNPServices**, herramienta de monitorización/graficado de nodos y el **MRTG** que consulta a los dispositivos de red por SNMP, y almacena la información.
- Como servidor de VPN se utiliza OpenVPN que es una aplicación de tunneling robusta y flexible.
- Y por último para la implementación del servidor de reloj se utiliza el servicio NTP propio del sistema Ubuntu.

Respecto al ordenador, se eligió un equipo que aunque no era nuevo, dispone de prestaciones suficientes para las funciones que se debe realizar. Sus especificaciones técnicas son Pentium Core2 Duo a 3 GHz con 2 GB de memoria RAM y disco duro SATA de 160 GB., con tarjeta de red integrada conectada a la red pública y se le añade una nueva tarjeta de red Ethernet 3Com para la VLAN que corresponde a la red Guifi.net.

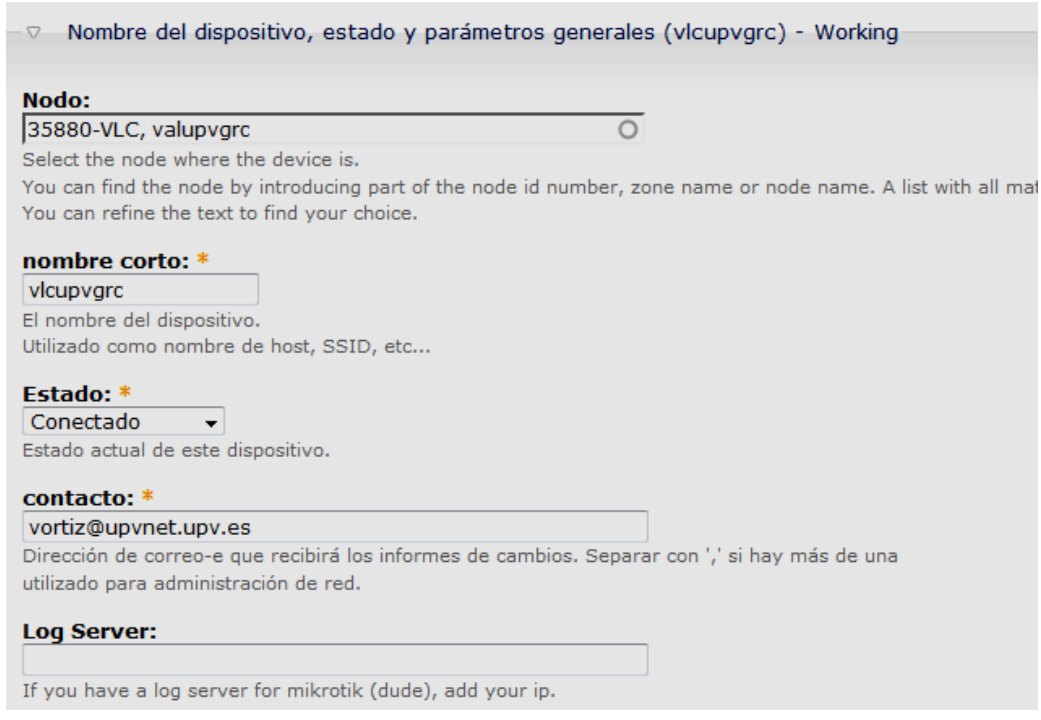
Figura 5.1. Fotografía del servidor VLCupvGRC

5.1.2.- Dar de alta el servidor en Guifi.net

El primer paso consiste en acceder a nuestro nodo (UPVone) en la web de Guifi.net e iniciar sesión con nuestro usuario GRCUPV. A continuación nos situamos en el centro de la página en *Añadir nuevo dispositivo* y en el despegable elegimos *Ordenador servidor*.



Al pulsar el botón "*añadir*" nos aparece un formulario donde ya nos aparece el nodo al que se le va a añadir el servidor y su nombre (valupvgrc), el estado en el que ponemos *conectado,* el correo de contacto, etc.



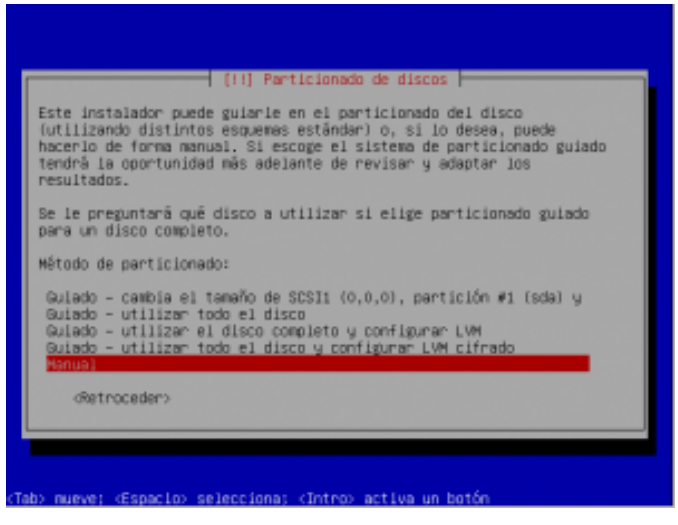
Por último, entrando en la sección de conexiones por cable, enlazar el servidor con el nodo, para lo que le asignamos la IP, de la misma forma que le hemos asignado las IPs a las antenas, pero del grupo de 6 IPs que hemos reservado antes de conexiones por cable (10.228.154.229)

5.1.3.- Instalación del sistema operativo Ubuntu server

Para la instalación del sistema operativo del servidor elegimos Ubuntu 10.04 server de 32 bits y descargamos una imagen .iso desde la web de la distribución http://www.ubuntu.com/server/get-ubuntu/download.forma

Vemos de forma breve los pasos de la instalación:

- Iniciamos con el cd de instalación dentro del servidor.
- Arranca el asistente para la instalación y solicita seleccionar el idioma que queremos usar en la instalación y el predeterminado del sistema final (Español)
- Después tenemos dos opciones Probar Ubuntu 10.04 o Instalar Ubuntu 10.04. Pulsamos sobre Instalar Ubuntu 10.04.
- Establecemos la zona horaria [España (Madrid)].
- Seleccionamos la distribución del teclado y se empiezan a cargar los datos iniciales de instalación
- Le damos el nombre a la maquina **(vlcupvgrc)**
- Particionado de los discos. Elegimos **utilizar todo el disco**. Se crearan 2 particiones



1. Partición raíz (/): que contendrá todos los directorios y archivos del sistema operativo y los datos de los usuarios.
2. Partición de intercambio (swap).

- Escogemos como sistema de ficheros etx4, el que usa Ubuntu 10.04 por defecto.
- Punto de montaje: / (raíz).
- Comienza la instalación del sistema, durante la cual pregunta:

- Nombre de usuario para la cuenta: **Guifi**
- Password:********
- Actualización manual o *automática.*

- Se cargan e instalan los paquetes y escogemos los servicios, entre los que activamos el ssh y desactivamos Bind9 porque vamos a utilizar otro servidor de nombres (dns).
- Al finalizar la instalación quitamos el CD de instalación y reiniciamos la máquina.

Por defecto, las versiones server de Ubuntu vienen sin entorno gráfico, por lo que el equipo se inicia en línea de comandos, y lo primero que hacemos es actualizar el sistema:

guifi@VLCupvGRC:~$ sudo apt-get update

guifi@VLCupvGRC:~$ sudo apt-get upgrade

Instalamos el servidor ssh para poder conectarse remotamente.

guifi@VLCupvGRC:~$ sudo apt-get install openssh-server

Como nuestro el servidor tiene que actuar como router hay que activar el forwarding permanente. Para ello editamos el fichero /etc/sysctl.conf y la línea *net.ipv4.ip_forward = 1* que normalmente está comentada, hay que descomentarla. Lo que hace que el forwarding se active al arrancar

A continuación se plantea la posibilidad de disponer de un entorno gráfico e instalamos:

guifi@VLCupvGRC:~$ *sudo apt-get install Ubuntu-desktop*

así tenemos una versión limitada del entorno gráfico a la que le añadimos algunas aplicaciones:

- El gestor de paquetes gráfico (synaptic):

  guifi@VLCupvGRC:~$ sudo apt-get install synaptic

- Gestor gráfico para controlar qué servicios se inician cuando el sistema arranca o se reinicia. (Rcconf)

  guifi@VLCupvGRC:~$ sudo apt-get install rcconf

- Administrador y monitor de tareas del sistema (GKrellM)

  guifi@VLCupvGRC:~$ sudo apt-get install gkrellm

5.1.4.- Instalación de HERRAMIENTAS

Se instalan en el servidor una serie de herramientas que ayudan a la gestión y control remoto de todo el nodo, desde el servidor al routerboard, como son Webmin, NXserver, Wine y Winbox.

5.1.4.1.- Instalación de Webmin

Webmin no está integrado en Ubuntu por lo que tenemos que ir a descargarlo desde su sitio web (http://www.webmin.com/download.html). Bajamos el paquete:

guifi@VLCupvGRC:~$ sudo wget http://prdownloads.sourceforge.net/webadmin/webmin_1.580_all.deb

y lo instalamos

guifi@VLCupvGRC:~$ sudo dpkg --install webmin_1.580_all.deb

Si nos aparecen fallos de dependencias habrá que ejecutar:

guifi@VLCupvGRC:~$ sudo apt-get -f install

Ahora ya se puede acceder a webmin con un navegador en la dirección http://localhost:10000/ o por internet o guifi.net en la dirección del servidor.

Se puede configurar el idioma de la interfaz de webmin en Webmin –> Cambio de Idioma y Tema

También se puede limitar el acceso en Webmin –> Configuración de Webmin –> Control de Acceso a IP

Si se ha puesto en marcha el cortafuegos y si se quiere dar acceso desde fuera, hay que abrir el puerto 10000:

guifi@VLCupvGRC:~$ sudo IPTABLES -A INPUT -m state --state NEW -p tcp --dport 10000 -j ACCEPT

5.1.4.2.- Instalación de NX

X11 hace referencia al sistema gráfico estándar de Unix, y permite realizar conexiones remotas con los escritorios de Unix o Linux. Para poder establecer estas conexiones remotas es necesario tener instaladas cada una de las partes (cliente y servidor) que componen un software como NX.

Es de la empresa NoMachine. El servidor es gratuito pero limitado a 2 usuarios como máximo y 2 conexiones simultaneas. Existen también versiones de pago sin limitaciones. Todos los clientes NX de NoMachine son gratuitos.

NX es seguro ya que utiliza ssh y utiliza los usuarios y contraseñas declarados en el sistema. La descarga se realiza desde la web http://www.nomachine.com/. El sistema servidor **NX Server** está formado por 3 paquetes NX Client, NX Node y NX Free Edition que hay que descargarlos e instalarlos en este orden haciendo doble clic en "Instalar el paquete".

NX Client es la aplicación que realiza las peticiones para lograr realizar la conexión remota al equipo en el que se encuentra instalado NX Server, el programa servidor.

La instalación en Windows es:

- Se descarga el cliente para Windows de http://www.nomachine.com/download.php
- Se ejecuta la aplicación y se van completando los pasos del asistente.
- El primer paso nos pide un nombre para la sesión (Guifi), el servidor remoto al que deseamos conectarnos (VLCupvGRC o su IP) y la velocidad de la conexión.

- En la siguiente pantalla pregunta a qué tipo de sistema nos vamos a conectar (Unix), y con qué escritorio (GNOME).
- A continuación pulsamos Terminar, y ya se puede introducir el nombre del usuario (Guifi) y la contraseña:

Y una vez autenticado aparece la pantalla de nuestro servidor Ubuntu:

5.1.4.3.- Instalación de Wine

Winbox es una utilidad para windows que permite la administración del sistema RouterOS utilizando una interfaz gráfica sencilla. Aunque es una aplicación diseñada para windows, se puede ejecutar en ordenadores con GNU/Linux como nuestro servidor Ubuntu utilizando **wine** que es una aplicación que permite ejecutar programas de windows en entornos /Linux.

Instalamos Wine desde la consola del servidor:

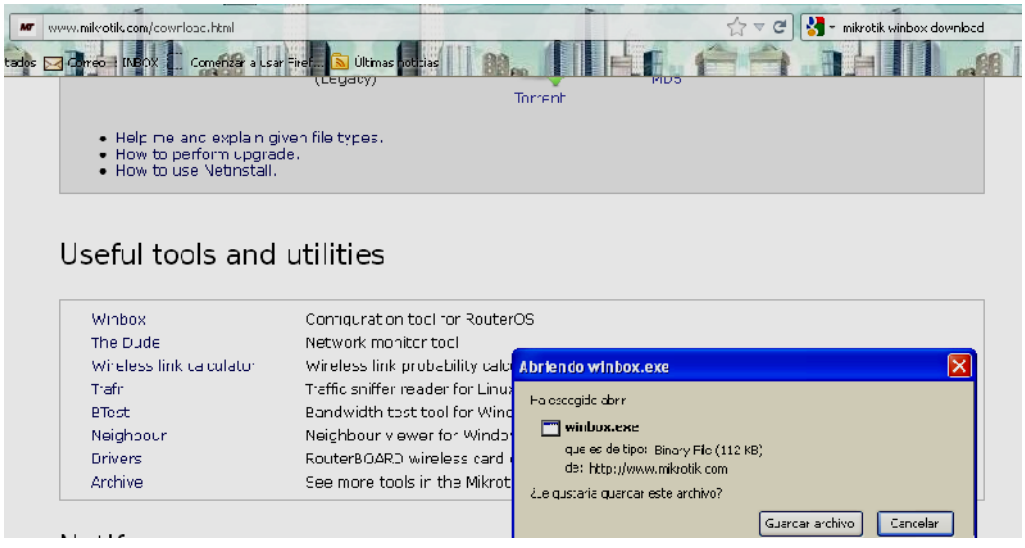
guifi@VLCupvGRC:~$ sudo apt-get install wine

5.1.4.4.- Instalación de Winbox

Como hemos indicado, la consola Winbox se utiliza para acceder a la configuración del router Mikrotik mediante la interfaz gráfica de usuario (GUI).

La consola de Winbox, es decir, el programa winbox.exe, puede ser descargado desde la propia web del router Mikrotik, en la dirección URL http://www.mikrotik.com/download.html.

Se puede descargar desde el mismo interface de la web de Mikrotik con "*Guardar archivo*"



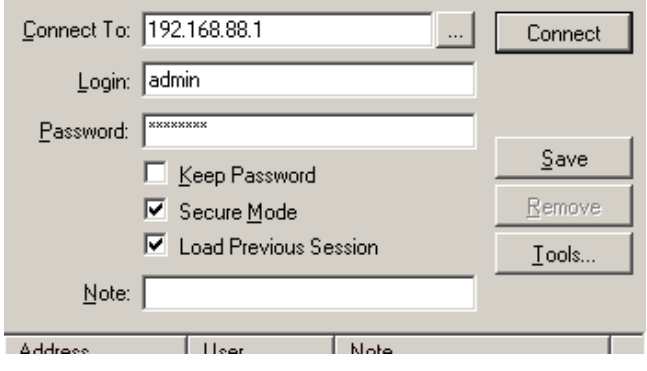
O bien desde la consola con wget:

guifi@VLCupvGRC:~$ sudo wget http://www.mikrotik.com/download/winbox.exe

Para ejecutarlo en nuestro servidor Ubuntu, se lanza desde la consola con el comando wine:

guifi@VLCupvGRC:~$ sudo wine ./winbox.exe

O bien desde el entorno gráfico pulsando el botón derecho del ratón sobre el link de Winbox e indicando "*abrir con Wine*"



Lo primero que nos aparece es una ventana para loguearse al Mikrotik que permite introducir las direcciones Mac o IP de la placa del Mikrotik.

Cuando se conecta al Mikrotik, de forma automática, empieza a descargar los plugins instalados en el Mikrotik para poder administrarlo remotamente. Y al finalizar la descarga de los plugins nos aparece la pantalla de configuración del Mikrotik, en la que a mano izquierda se encuentra el menú de configuración de cada uno de los módulos instalados.

En el capitulo anterior, cuando se ha configurado el Mikrotik con la opción "*unsoloclic*" de Guifi.net, se ve alguno de los módulos que se han utilizado.

5.2.- Servicios

Para crear una zona Guifi, se necesita como mínimo un supernodo (para que se conecten los nodos) y al menos un servidor con varios servicios imprescindibles: un servidor de gráficas, para que el supernodo y los nodos grafiquen en la web de guifi y un servidor de nombres de dominio, para poder resolver los nombres de dominios de los dispositivos de la red. Hay otros servicios importantes pero no estrictamente necesarios como son un servidor de reloj, para que todos los dispositivos de la red estén a la hora, un servidor proxy, que ofrece una puerta de salida a Internet desde la propia red o un servidor de ficheros por FTP para que se pueda intercambiar ficheros entre los usuarios de la red.

Al iniciar el proyecto se planteó qué servicios se iban a ofrecer desde nuestro supernodo y, en principio, se decidió a instalar los servicios básicos, el servidor web, el de graficas y el DNS, y, aunque no podíamos instalar el servidor proxy, si que se podía crear un túnel con el servidor VPN de la universidad y ofrecer acceso a la red de la universidad e Internet a la comunidad universitaria unicamente creando un nodo y conectandose a las antenas de nuestro supernodo.

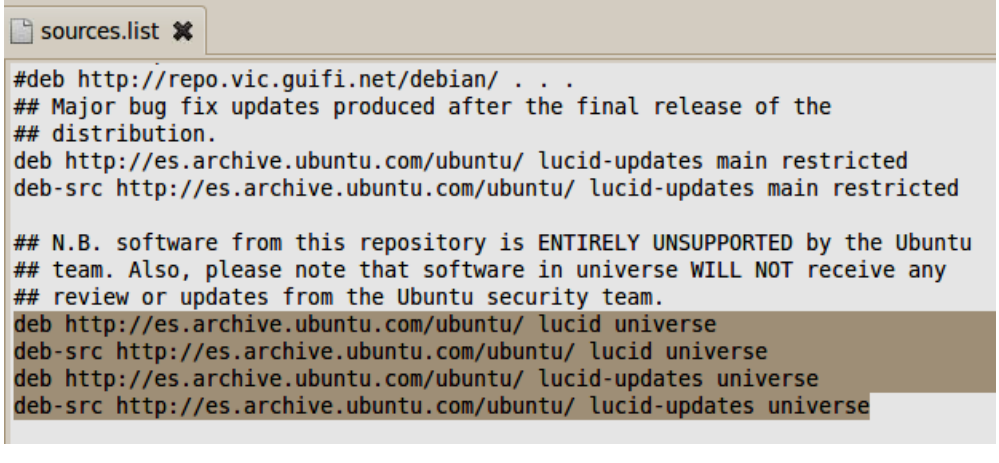
Vamos a ver a continuación la instalación de los servicios básicos indicados, web (apache y php), DNS (dnsmasq) y gráficas (para la web de Guifi.net y otro para nuestro servidor) y en el capitulo siguiente se desarrollarán las conexiones VPN.

5.2.1.- Servidor Web (Apache2 + PHP5)

Para crear nuestro servidor Web elegimos “Apache HTTP Server” ya que es un software libre de código abierto tanto para sistemas Linux como Windows.

5.2.1.1.- Instalación de Apache2 en nuestro servidor Ubuntu

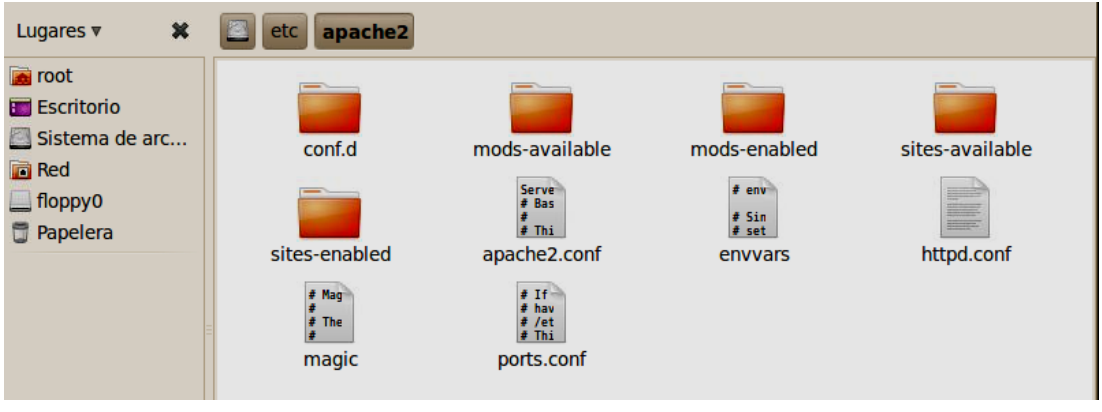
Antes de realizar la instalación desde una consola de nuestro servidor, comprobamos y actualizamos todos los repositorios de software de nuestra distribución, fundamentalmente el repositorio de origen universe en el archivo /etc/apt/*sources.list*



En la orden de descarga no solo le indicamos el paquete de apache2 que queremos instalar sino también el resto de paquetes que son necesarios. Si la instalación la hiciéramos desde el gestor de paquetes Synaptic al marcar el paquete de apache2 a instalar nos indicaría directamente todas las dependencias.

guifi@VLCupvGRC:~$ sudo *apt-get install apache2 apache2-common apache2-mpm-prefork apache2-utils ssl-cert*

Con esta orden se completará la instalación del servidor web apache2 y a continuación se comprueban los archivos de configuración y la raíz de documentos del servidor web Apache. Por defecto, todos los archivos de configuración se encuentran en /etc/apache2



Y la raíz por defecto para documentos es /var/www.

El archivo de configuración principal se encuentra en / etc/apache2/apache2.conf. y el puerto de escucha, por defecto, es el 80.

Cada vez que se realiza un cambio es necesario reiniciar el servidor apache.

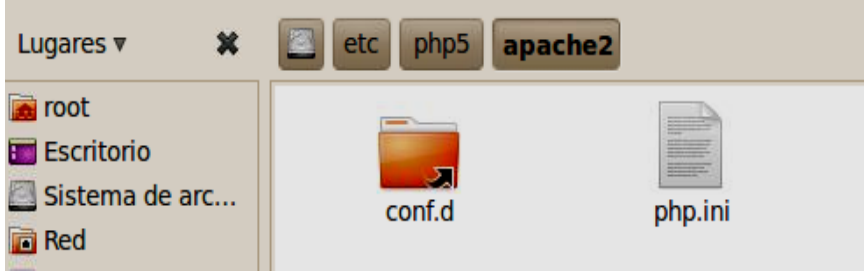
guifi@VLCupvGRC:~$ sudo / etc/init.d/apache2 restart

5.2.1.2.- Instalación de PHP5

La instalación del php5, para que este enlazado con apache, y el resto de módulos que necesitamos la hacemos también desde la consola de órdenes:

guifi@VLCupvGRC:~$ sudo apt-get install libapache2-mod-php5 php5-cli php5-common php5-cgi

El archivo de configuración es el php.ini que se encuentra en /etc/php5/apache2/php.ini

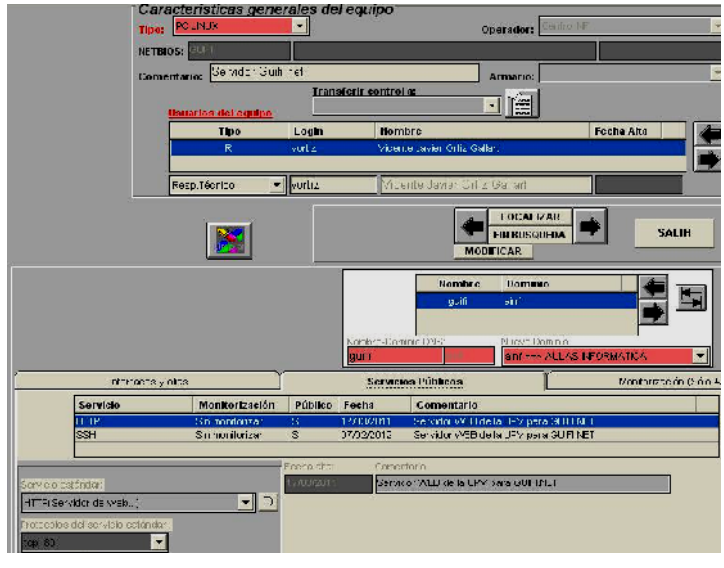


5.2.1.3.- Dar de alta el servicio en la UPV para que salga a Internet

Una vez instalado el servicio WEB en nuestro servidor nos planteamos que es necesario que la información que introduzcamos en nuestras páginas pueda ser vista no solo desde la red de Guifi.net sino también desde Internet.

Para ello la universidad tiene una aplicación de gestión para asociar una tarjeta de red a una dirección IP real y fija para la MAC de dicha tarjeta y en la que se puede indicar que servicios tiene instalados el equipo y que solo pueden ser vistos localmente, dentro de la red de la universidad, o si se publican para que puedan ser visualizados desde cualquier sitio de Internet.

Finalmente se publican 2 servicios del servidor: el servicio web (HTTP) por el puerto 80 y el servicio SSH por el puerto 22.



5.2.2.- **Servidor DNS (dnsmasq)**

5.2.2.1.- El servidor de nombres DNSmasq

La instalación de un servidor de nombres en el servidor del supernodo es considerado imprescindible para la creación del nodo de Guifi.net. Para el alta del nodo en la universidad no se consideró necesario dar de alta el servicio en la red Guifi.net, sino que, en principio, únicamente tuviera como radio de acción la propia red del supernodo, por lo que se eligió el software dnsmasq para servidor de nombres.

El paquete dnsmasq permite poner en marcha un servidor DNS de una forma muy sencilla, ya que simplemente instalando y arrancando el servicio dnsmasq, sin realizar ningún tipo de configuración adicional, nuestro equipo se convierte en un servidor caché DNS. y además, resolverá los nombres que tengamos configurados en el archivo /etc/hosts de nuestro servidor. La resolución funcionará tanto en sentido directo como en sentido inverso, es decir, resolverá la IP dado un nombre de PC y el nombre del equipo dada la IP. Aunque en nuestro caso no es necesario, dnsmasq también dispone de servidor DHCP y permite resolver los nombres de los PCs a los que les ha asignado dirección IP dinámica.

DNSmasq actúa como DNS forwarder, cacheando las peticiones DNS que se realizan y por tanto acelerando la resolución de nombres para una red local.

5.2.2.2.- Instalación del servidor dnsmasq

Para instalar la última versión de dnsmasq en Ubuntu o en cualquier otra distribución de Linux basada en Debian únicamente debemos actualizar los paquetes del repositorio e instalarlos con apt-get desde una consola:

```
guifi@VLCupvGRC:~$ sudo apt-get install  dnsmasq
```

5.2.2.3.-Configuración del servidor DNS

Ahora que ya está el servidor DNS instalado, el siguiente paso será editar los archivos de configuración /etc/dnsmasq.conf, /etc/resolv y /etc/hosts de nuestro servidor, para que resuelva los nombres y las IPs de nuestra red.

- /etc/dnsmasq.conf

En el fichero /etc/dnsmasq.conf hay que modificar las siguientes líneas:

- Descomentamos *strict-order* para que se realicen las peticiones DNS a los servidores que aparecen en el fichero /etc/resolv.conf en el orden en el aparecen.

- Descomentamos *address* y ponemos el dominio de nuestra red local para que la petición no tenga que salir de él:

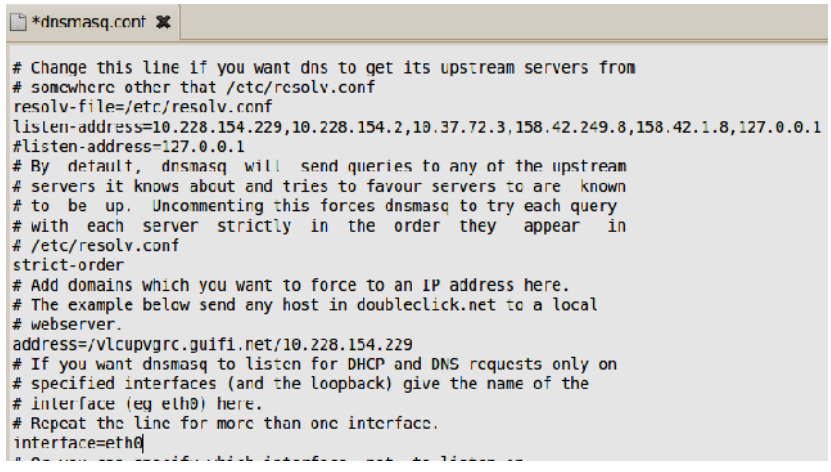
  address=/vlcupvgrc.guifi.net/10.228.154.229

- . Incluimos las interfaces de red que deben aceptar peticiones DNS:

  interface=eth0

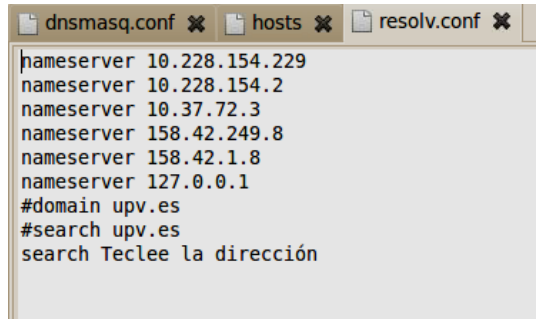
- Incluimos las direcciones IP que aceptan peticiones DNS:

  listen-address=10.228.154.229,10.228.154.2,10.37.72.3,158.42.249.8.....



- /etc/resolv.conf

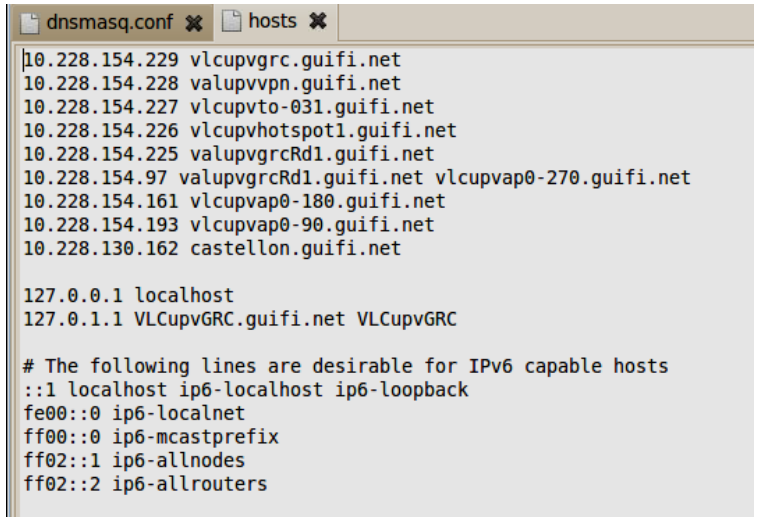
El archivo /etc/resolv.conf guarda la información sobre los servidores recursivos que se utilizan para resolver las consultas de DNS. En él se especifican los servidores DNS que utiliza el sistema para la resolución de nombres. Normalmente se ponen varios jerárquicos para que en caso de que el principal falle el siguiente tome el control.



- /etc/hosts

Para que dnsmasq resuelva los nombres e IPs de todos los equipos (servidor, router, hotspot…) de nuestra red que disponen de IP fija solo hay que añadir sus nombres e IPs en el archivo hosts del servidor.

De esta manera, tan solo editando el archivo /etc/hosts del servidor, se dispone de un sencillo servidor DNS para nuestra red.



5.2.2.4.- Arranque y parada del servidor dnsmasq

El servicio dnsmasq, al igual que todos los servicios, dispone de scripts de arranque y parada en la carpeta /etc/init.d. que se deben ejecutar desde una consola de root. (o con sudo)

// Arrancar o reiniciar el servidor dnsmasq

guifi@VLCupvGRC:~$ sudo /etc/init.d/dnsmasq restart

// Parar el servidor dnsmasq

guifi@VLCupvGRC:~$ sudo /etc/init.d/dnsmasq stop

// Arrancar el servidor dnsmasq

guifi@VLCupvGRC:~$ sudo /etc/init.d/dnsmasq start

Cada vez que se modifique cualquiera de los archivos del servidor que hemos visto, deberemos reiniciar el servicio dnsmasq y recargar la información contenida en dicho archivo.

5.2.3.- **Servidor de Gráficas**

El servidor de gráficas es totalmente necesario para la plataforma de gestión de guifi.net, de manera que se puedan mostrar gráficas y estadísticas de tráfico de la red en su interfaz. Es una herramienta esencial para llevar a cabo un seguimiento de la evolución de la red y detectar en qué momento y lugar es necesario ampliarla.

5.2.3.1.- Para la web de guifi.net

Lo primero que se necesita para poder dar de alta e instalar el servicio de gráficas en Guifi.net es que nuestro servidor tenga acceso al servidor de guifi.net para poder consultar los componentes de nuestra red cuya actividad ha de graficar y además también debe tener acceso a Internet para poder mostrar los datos del nodo cuando desde ésta se consulten. Como no podemos acceder al servidor guifi.net por la propia guifi.net, utilizamos para todo la tarjeta de red conectada a la UPV y que proporciona al servidor conectividad a Internet.

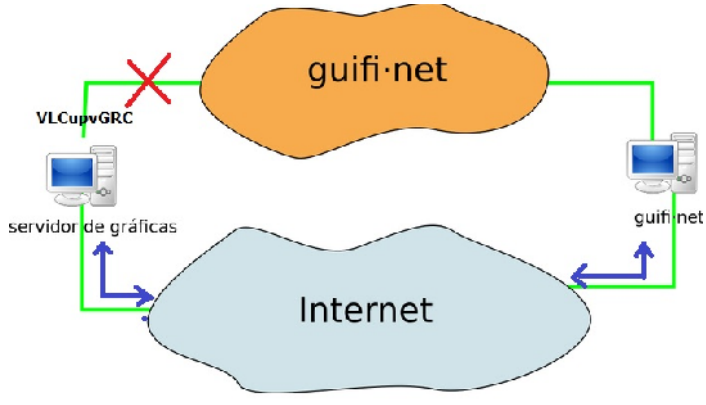
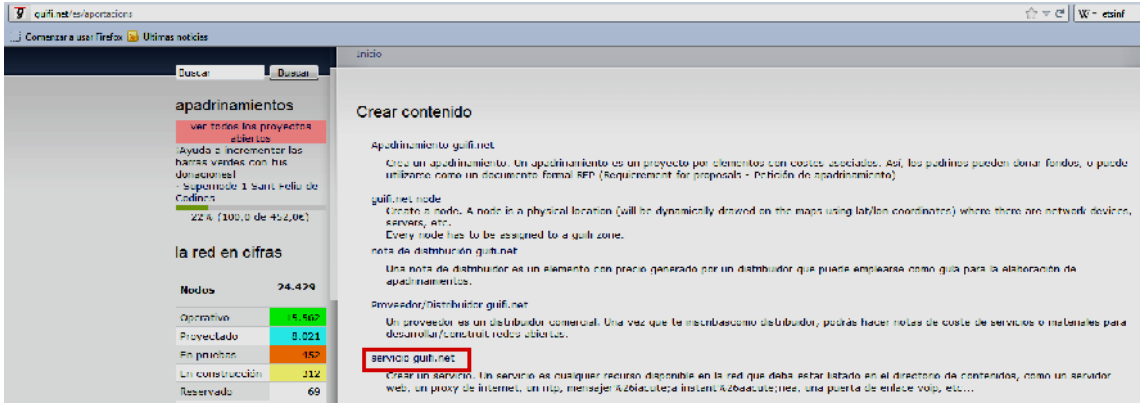


Figura 5.2. Conexión del servidor de gráficas con el servidor Guifi.net

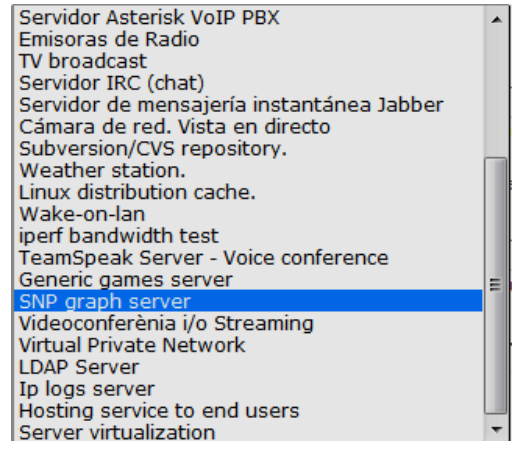
El servidor de gráficas, por medio de un cron, consulta cada 30 minutos al servidor de guifi.net de qué elementos debe realizar las gráficas y cada 5 minutos mira el SNP para ver si hay cambios y si los hay, obtiene una lista, en un formato comprimido, y genera el data/mrtg.cfg. El contenido de este fichero indica si el servicio está funcionando adecuadamente (si está vacío es que algo no está funcionando adecuadamente).

- <u>Dar de alta el servicio en guifi.net</u>

Para dar de alta en la web de guifi.net al servidor de gráficas accedemos a la página http://guifi.net/es/aportacions al apartado *crear contenido* --> servicio guifi.net



Aparecerá un formulario que debemos rellenar



- En Servicio hay que elegir «*SNP Graph Server*».
- En el nombre del servicio ponemos "*Servidor de gráficas UPV*"
- Nombre corto "*upvgraf*"
- En Dispositivo se pone el identificador del servidor en guifi.net. Para averiguarlo hay que empezar a teclear el nombre del nodo y la aplicación lo mostrará.

Después de crear el servicio, hay que editarlo y comprobar la versión (2.0), y poner en la URL del servidor en internet que sirve las gráficas con el servicio snpservices: *http://guifi.inf.upv.es/snpservices/graphs/graphs.php.*

En la zona donde se va a utilizar el servidor de gráficas indicamos que como Servidor predeterminado de gráficas no tome de las zonas superiores si no que utilice el que acabamos de crear.

- <u>Instalación del software</u>

Para la creación de un servidor de gráficos en Guifi.net hay que instalar el paquete SNPServices que es la herramienta de monitorización/graficado del estado/tráfico de los nodos. Está basado totalmente en software open-source. Es una utilidad de diagnóstico rápido y el proceso de monitorización de nuevos nodos es automático. Se basa en el protocolo SNMP

- Funciones del servidor de gráficas

a) Obtener los datos de los dispositivos que ha de monitorizar: Estos datos se obtienen a través de un servicio web que proporciona un fichero de texto en formato CSV.

b) Monitorizar: El servidor periódicamente se pone en contacto con los dispositivos utilizando pings y SNMP con tal de comprobar la disponibilidad y obtener les datos de las interfaces de red respectivamente.

c) Almacenar los datos de monitorización: los datos obtenidos al monitorizar se guardan en una base de datos Round Robin utilizando la herramienta *RRDTool*

d) Mostrar gráficas: Finalmente se utiliza *MRTG* para mostrar los datos a través de Internet (en página web HTML).

NOTA: SNPServices utiliza MRTG pero no en el formato original (utilizando archivos de log) sino utilizando RRD como LogFormat (LogFormat: rrdtool)

- Requerimientos

Para montar el servicio SNPServices tiene varios requerimientos.

a) Un servidor preferiblemente basado en GNU/Linux con acceso a la red a monitorizar (Guifi.net), y a Internet.

b) Un servidor web que se encargará de publicar las gráficas en Internet, para que se muestren en la web de guifi.net.

c) Unas herramientas de monitorización que extraerán la información de guifi.net

d) Dar de alta el servicio en la web de Guifi.net

Además, el paquete SNPServices tiene las siguientes dependencias:

a) Debconf: Para poder hacer las preguntas de configuración del servidor de gráficas durante la instalación del servidor.

b) Apache2: Servidor web.

c) PHP5: Para mostrar las gráficas vía web

d) RRDTool: Para la generación de gráficas y bases de datos Round Robin

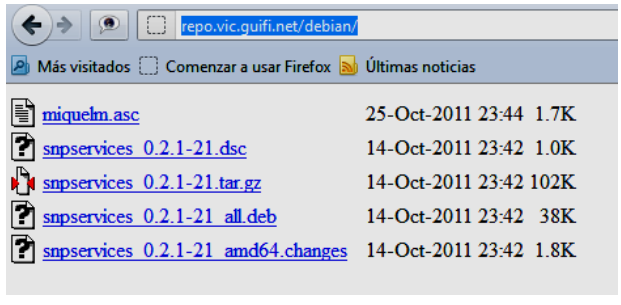
e) MRTG: Para monitorizar dispositivos de red mediante SNMP .

- Instalación de SNPServices

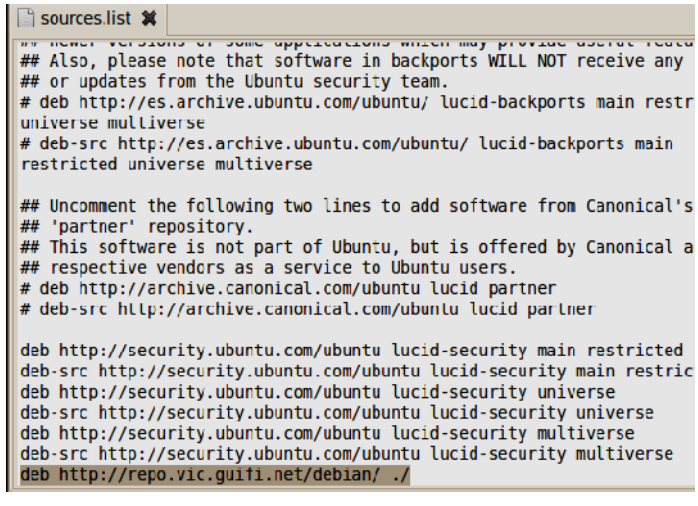
Para instalar SNPServices hay que bajar el paquete de un repositorio oficial, instalarlo con todas sus dependencias y personalizar la instalación editando y modificando varios archivos de configuración bastante complejos.

apt-get install rrdtool librrdp-perl librrds-perl mrtg mrtg-rrd subversion php5-cli

Además hay que tener en cuenta, que algunos repositorios pueden estar obsoletos y contendrán versiones de SNPServices obsoletos. En el nodo de Vic de Guifi.net existe un repositorio donde han creado un paquete de SNPServices ya preparado para generar el servidor de gráficas para la web de Guifi.net. Por lo que es el que utilizamos. http://repo.vic.guifi.net/debian/



Podemos descargarlo directamente de la web o bien añadir el repositorio al fichero /etc/apt/sources.list y actualizar los repositorios.



guifi@VLCupvGRC:~$ sudo vi /etc/apt/sources.list

deb http://repo.vic.guifi.net/debian/ ./

guifi@VLCupvGRC:~$ sudo apt-get update

y finalmente, en ambos casos instalamos el paquete snpservices

guifi@VLCupvGRC:~$ sudo apt-get install snpservices

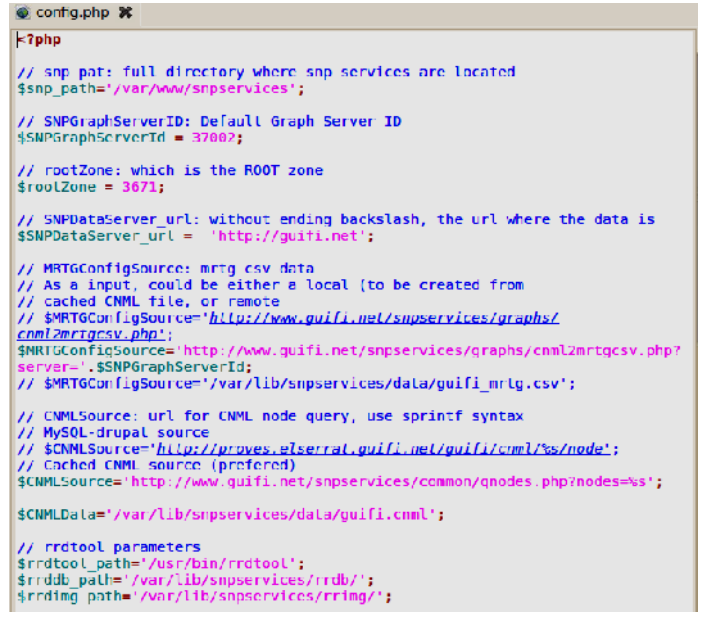
El apt resuelve todas las dependencias del paquete snpservices y muestra todos los paquetes que se instalan. Al empezar la instalación aparecerá el configurador (*debconf*), primero el de MRTG (si no está instalado) y después el de snpservices. El instalador pregunta el ID del servidor de gráficas, y hay que poner el número que se le ha asignado al dar de alta el servidor (37002). Con esto, el servidor de gráficas estará accesible mediante la URL http://guifi.net/node/37002. y la URL desde Internet será: http://guifi.inf.upv.es/snpservices/graphs/graphs.php

- Configuración del servidor de gráficas

Ahora hay que proceder a comprobar y/o configurar el servidor de gráficas. Primero obtenemos una copia de la plantilla del archivo de configuración:

guifi@VLCupvGRC:~$ sudo cp /var/www/snpservices/common/config.php.template /var/www/snpservices/common/config.php

El fichero */var/www/snpservices/common/config.php es un enlace al que* encontramos en la carpeta principal de configuración /etc/snpservices donde encontraremos los dos ficheros: *config.php y config.php.template*. El primero, /etc/snpservices/config.php es el archivo principal de configuración y el segundo es una plantilla de ejemplo.



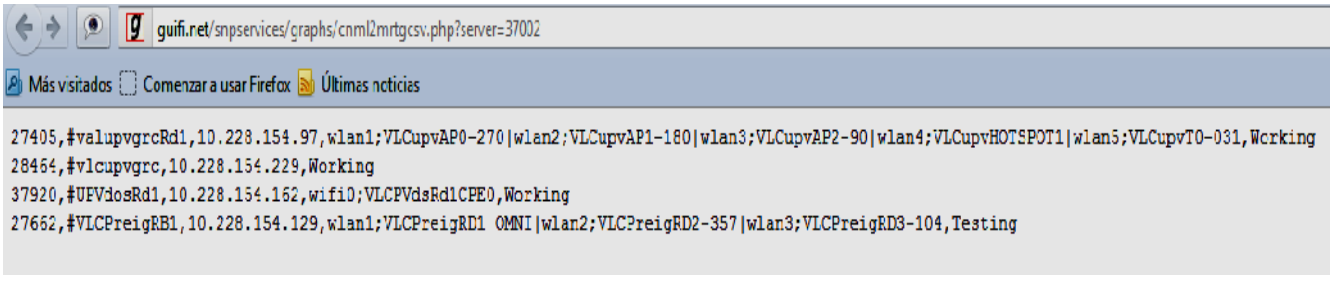
En este fichero php se ajustan los parámetros necesarios a los que correspondan para nuestro servidor, como el ID del servidor de gráficas:

Las variables más importantes son:

- *$SNPGraphServerId*: es el identificador del servidor de gráficas en la web de Guifi.net. El id 37002 corresponde a nuestro servidor: *http://guifi.net/es/node/37002*
- *$rootZone*: Su valor suele ser 3671 y no se cambia ya que corresponde a la zona raíz de guifi.net: *http://guifi.net/ca/node/3671*
- *$SNPDataServer_url*: es la URL de la web Guifi.net: *'http://guifi.net'*;
- El resto de variables son variables de configuración de la herramienta MRTG o de las fuentes de datos para crear las gráficas:

- $*MRTGConfigSource* = Ejecuta un PHP de la web de guifi para obtener los datos de un servidor de gráficas. Se obtiene un archivo CSV con la lista de nodos gestionados por el servidor de gráficas:

http://guifi.net/snpservices/graphs/cnml2mrtgcsv.php?server=37002



Variables que configuran el CNML:

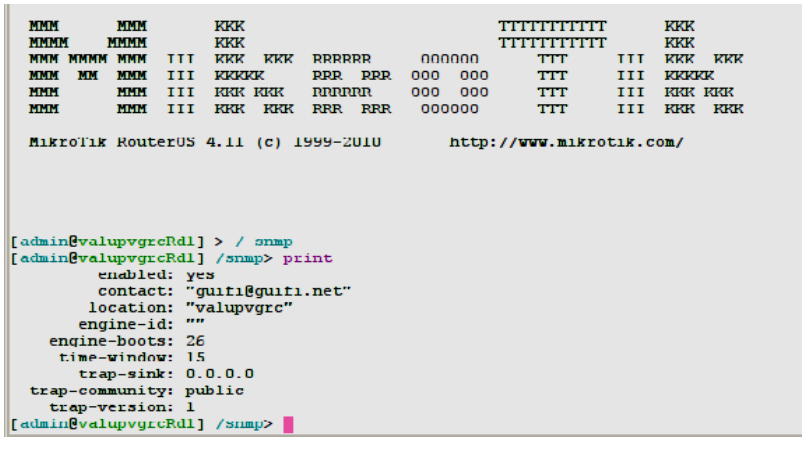
- $*CNMLSource: http://www.guifi.net/snpservices/common/qnodes.php?nodes=%s*
- *$CNMLData:* /var/lib/snpservices/data/guifi.cnml

Variables que configuran RRDTool y MRTG

- ***$****rrdtool_path*: ='/usr/bin/rrdtool';
- ***$****rrddb_path*: Carpeta donde se guardan los archivos y las Base de datos de gráficas RRD. Por defecto /var/lib/snpservices/rrdb
- ***$****rrdimg_path*: Carpeta donde se guardan las imágenes de las gráficas RRD. Por defecto /var/lib/snpservices/rrimg

  - Activar clientes snmp

A nivel de cliente, en los dispositivos de los que hay que obtener gráficas, se debe activar el servicio snmp que responda a las consultas que haga nuestro servidor de gráficas. En la configuración hay que poner como comunidad «public». En nuestro Mikrotik queda así:

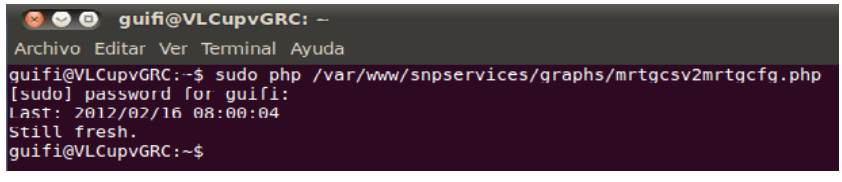


- Primeros gráficos y comprobación

Una vez finalizada la puesta en marcha del servidor de gráficas, podemos esperar a que actúe el cron para que se haga la primera descarga de los dispositivos a graficar desde guifi.net o podemos forzarla ejecutando un fichero php de snpservices que, además nos sirve para comprobar si se ejecuta bien el script php (y si no es así nos indica con mensajes de error la línea que es errónea). Para ello desde una consola, con permisos de root, escribimos

guifi@VLCupvGRC:~$ sudo php /var/www/snpservices/graphs/mrtgcsv2mrtgcfg.php

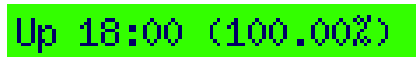
y nos debe dar una respuesta corta de 2 líneas con fecha y hora y si ha habido cambios para que todo esté correcto

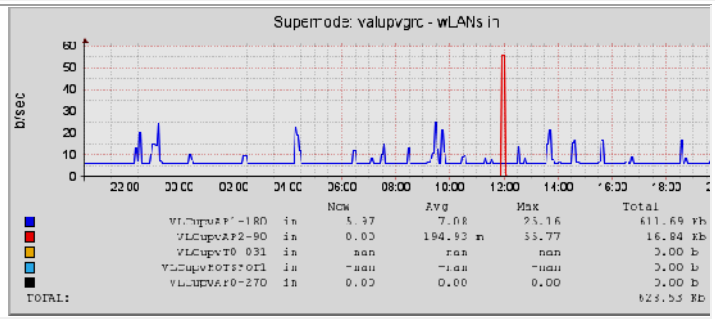


- Gráficas que proporciona

Las gráficas nos proporcionan la siguiente información:

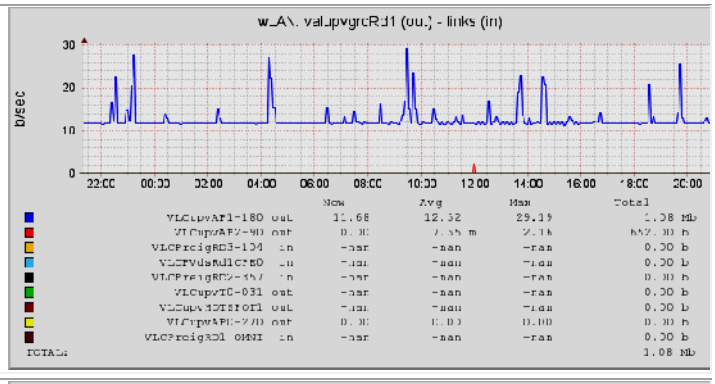
- A nivel de supernodo, nos mostrará una gráfica de la evolución del tráfico de cada uno de los interfaces de red instalados.
- Dentro de cada radio, podremos visualizar el tráfico de esa radio en cada uno de sus enlaces.
- Además, visualizaremos unas gráficas de la latencia del ping hacia esa radio (desde el servidor de gráficas).

Gráfico	Descripción/Parámetros
	Gráfica de disponibilidad del supernodo en formato corto. **Up** (verde) o Down (rojo). • **Type**=availability • **device**=guifi_device_ID • **format**=short
	Gráfica de disponibilidad del supernodo en formato corto largo. Muestra también la última hora en que se ha consultado el estado. • **Type**=availability • **device**=guifi_device_ID • **format**=long



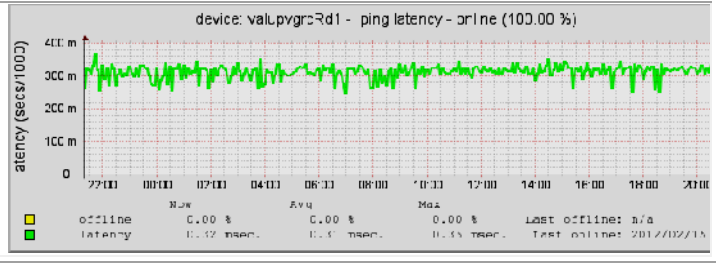
Muestra el tráfico de datos de los APs de un supernodo (AP/cliente o WDS). Tanto de entrada (in) como de salida (out).

- **Type**=supernode
- **node**=guifi_device_ID
- **direction**=in|out



Muestra los Ap que tienen diversos clientes.

- **Type**=clients
- **node**=guifi_supernode_ID
- **radio**=guifi_device_ID
- **direction**=in|out



Muestran el resultado del ping y la latencia de cada elemento de un supernodo.

- **Type**=pings
- **node**=guifi_supernode_ID
- **device**=guifi_device_ID

Figura 5.3. Tipos de gráficas que proporciona el servidor de gráficas

5.2.3.2.- Para la web del servidor VLCUPVGRC

En el punto anterior se desarrolla como se ha instalado y configurado un servidor de gráficas que presente en una página de la web de Guifi.net las gráficas de disponibilidad y tráfico del supernodo con sus radios y los nodos clientes que se van uniendo a él. Para la filosofía de esta red libre, como ya se ha indicado, constituye una herramienta esencial que le sirve para llevar a cabo un seguimiento de su evolución y detectar en qué momento y lugar es necesario ampliarla.

Pero al mismo tiempo, como administrador del supernodo, también es importante saber cómo se comporta mi red a través de un histórico que engloba tanto el momento actual como las horas o días pasados. La administración de red es necesaria para poder asegurar que se brindan correctamente los servicios para los que está diseñada, además de asegurar que cumple con un nivel aceptable de seguridad y es en estas ocasiones cuando el empleo de una utilidad de monitorización es útil

Por todo ello, se plantea instalar otro servidor de gráficas que nos grafique el tráfico que se mueve por los radios del nodo en distintas vistas temporales (por horas, días, semanas y meses), pero al

contrario que en el caso anterior donde la misma red Guifi.net dirige la instalación para particularizarla según su interés y propósito, en éste caso realizamos la instalación típica de cada protocolo.

- Protocolos necesarios para crear el servidor de gráficas

Lógicamente para el nuevo servidor de gráficas se utilizarán los mismos protocolos, aunque tratados de forma diferente. Para la medición del tráfico se utiliza el Protocolo Simple de Administración de Red (Simple Network Manager Protocol SNMP) y el Graficador de Trafico para Routers (Multi Router Traffic Grapher, MRTG).

MRTG es una herramienta utilizada para supervisar la carga de tráfico de interfaces de red generando un informe que es interpretado en gráficas en una página de HTML, por lo que también es necesario instalar un servidor Web (en nuestro caso Apache2). Para obtener esta información pide los datos requeridos o que se desean monitorizar al servidor SNMP cada cierto tiempo constante controlado por un cron.

El SNMP es un protocolo que permite una estructura de mensajes para el intercambio de información entre el administrador y el agente SNMP. Un administrador SNMP, es un sistema empleado para controlar la actividad de los componentes de la red, regularmente denominado NMS, Sistema de Administración de Red (Network Management System). ·Un agente SNMP, es el componente software dentro del dispositivo administrado que mantiene los datos del mismo e informa al administrador acerca de ellos, cuando se requiere. Contiene variables de la MIB (colección de objetos de información de administración) cuyos valores pueden ser solicitados o modificados por el administrador SNMP, mediante operaciones get y set.

SNMP manda peticiones con objetos (OIDs) al equipo.

- *ifInOctets:* Indica el número total de bytes recibidos en el enlace.
- *ifOutOctets:* El número total de octetos transmitidos fuera del enlace.
- *ifSpeed*: Nos da una estimación del ancho de banda actual del que dispone el enlace en bits por segundo. En aquellos enlaces en los que el ancho de banda no varíe o en los que no sea posible hacer una aproximación exacta, este objeto suele contener el ancho de banda nominal.

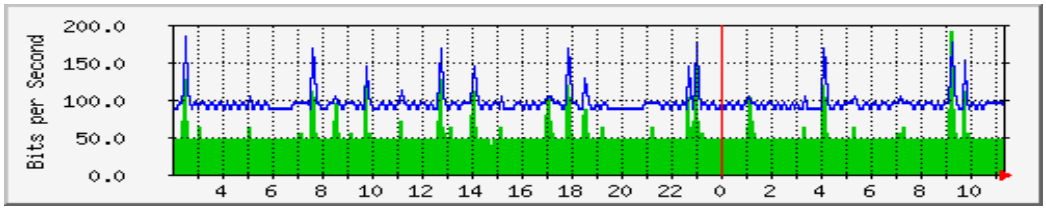


Figura 5.4. Gráfica de "ifspeed"

	Max	Average	Current
In	192.0 b/s (0.0%)	56.0 b/s (0.0%)	48.0 b/s (0.0%)
Out	184.0 b/s (0.0%)	96.0 b/s (0.0%)	88.0 b/s (0.0%)

- Instalación y Configuración de SNMP

Los pasos de preparar el Mikrotik habilitando el agente SNMP (Enable SNMP Agent) e indicando que la Comunidad (Community), que es una especie de contraseña para acceder al dispositivo SNMP sea *public,* no se explica al ya estar descrita en el apartado de Guifi.net.

Considerando preparado el router se instala el SNMP en el servidor

guifi@VLCupvGRC:~$ sudo apt-get install snmp snmpd

y una vez instalado vemos el archivo de configuración en "/etc/snmp/snmpd.conf" y, para configurarlo, se utiliza el comando snmpconf.

guifi@VLCupvGRC:~$ sudo /etc/snmp/snmpconf

Le indicamos snmp.conf cuando pregunta qué tipo de archivo de configuración se desea crear

En la siguiente pantalla nos da una lista de los parámetros que pueden ser configurados, y le indicamos:

- Extending the Agent: *agentx*
- System Information Setup: *localización física y datos de contacto del administrador*
- Agent Operating Mode: *puerto y protocolo que utiliza (udp:161)*
- Access Control Setup: *com2sec readonly default public*

Tecleamos quit y se sobreescribe el archivo y se reinicia el servicio

guifi@VLCupvGRC:~$ sudo /etc/init.d/snmpd restart

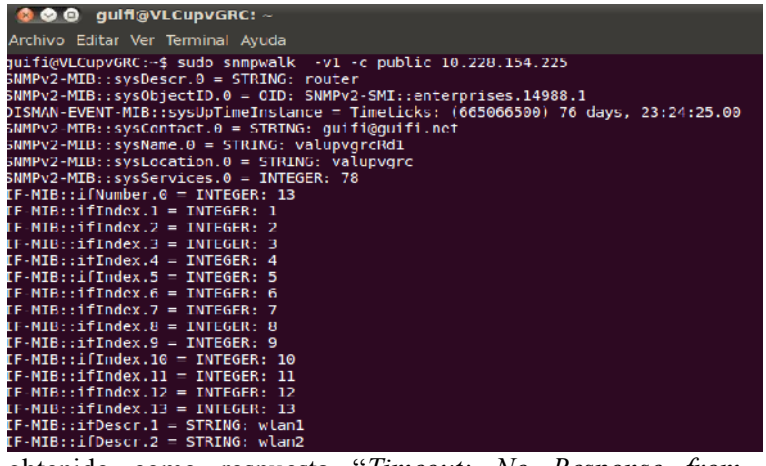
A continuación verificarnos que el puerto 161 este abierto con el comando:

guifi@VLCupvGRC:~$ sudo netstat -natup | grep 161

```
guifi@VLCupvGRC:~$ sudo netstat -natup | grep 161
[sudo] password for guifi:
udp        0      0 127.0.0.1:161           0.0.0.0:*                           3784/snmpd
guifi@VLCupvGRC:~$
```

Ahora ejecutamos el comando "snmpwalk" que nos ayuda a comprobar si el agente que queremos monitorizar está respondiendo a las peticiones SNMP.

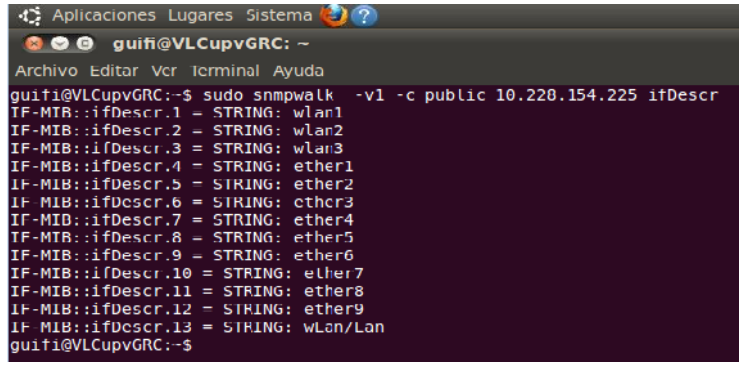
guifi@VLCupvGRC:~$ sudo snmpwalk –v1 -c public 10.228.154.225



Si hubiéramos obtenido como respuesta "*Timeout: No Response from 10.228.154.225*" deberíamos verificar el SNMP Community y/o la dirección IP del dispositivo Mikrotik.

Al obtener respuesta correcta, comprobamos qué interfaces usa nuestro dispositivo:

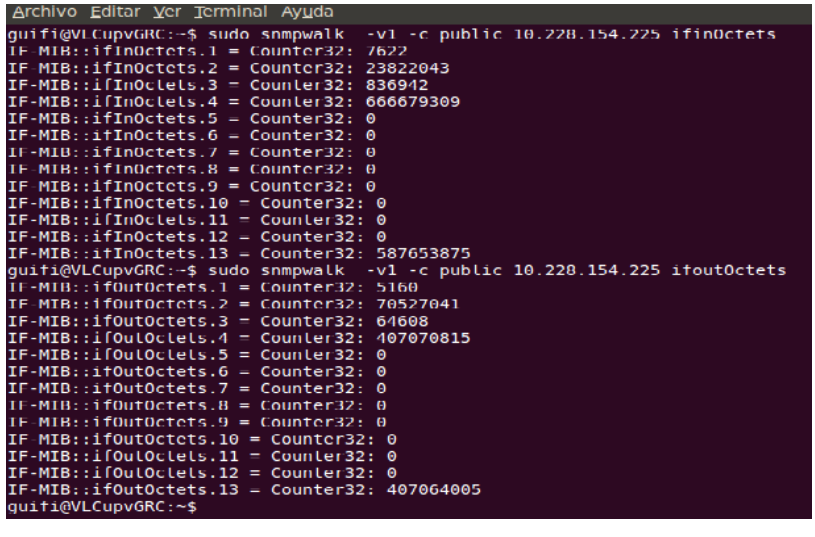
guifi@VLCupvGRC:~$ sudo snmpwalk –v1 -c public 10.228.154.225 ifDescr



También podemos ver cuántos bytes ha recibido (ifinOctets) y transmitido (inoutOctets) nuestro dispositivo desde el último reinicio.

guifi@VLCupvGRC:~$ sudo snmpwalk –v1 -c public 10.228.154.225 ifinOctets

guifi@VLCupvGRC:~$ sudo snmpwalk –v1 -c public 10.228.154.225 ifoutOctets



- Instalación y Configuración de MRTG

Para instalar MRTG ponemos en una consola el siguiente comando:

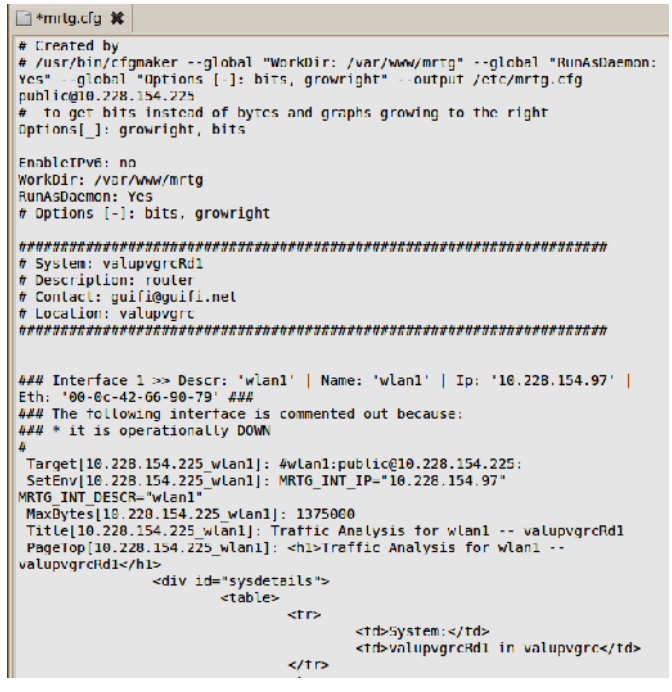
guifi@VLCupvGRC:~$ sudo apt-get install mrtg

Una vez instalado pasamos a realizar la configuración para la que se utilizan los programas *cfgmaker e indexmaker*, cgkmaker nos establece la configuración que debemos de tener en /etc/mrtg.cfg e indexmaker nos construye la página de índice para el directorio de trabajo de mrtg (en /var /www /mrtg)

Para obtener el archivo de configuración para mrtg primero creamos la carpeta mrtg en /var/www y a continuación se ejecuta el comando

guifi@VLCupvGRC:~$ sudo cfgmaker public@127.0.0.1

Esto nos va ha crear una configuración automática y básica de mrtg. Pero se puede editar el fichero para cambiar cosas que no nos interesen.



Ahora lanzamos la aplicación:

guifi@VLCupvGRC:~$ sudo env LANG=c /usr/bin/mrtg /etc/mrtg.cfg

guifi@VLCupvGRC:~$ sudo mrtg /etc/mrtg.cfg

Si hay que parar MRTG debemos matar el proceso, para ello buscamos el id del proceso:

guifi@VLCupvGRC:~$ sudo more /etc/mrtg.pid

guifi@VLCupvGRC:~$ sudo kill -9 "id proceso"

Ahora ya tenemos una primera configuración, creamos los archivos html para publicar nuestros gráficos y poder acceder a las páginas HTML, para ello antes incluimos con indexmaker una página principal que indexa los interfaces que se monitorizan.

guifi@VLCupvGRC:~$ sudo indexmaker --columns=1 --output /var/www/mrtg/mrtg.html /etc/mrtg.cfg

El comando indexmaker hay que ejecutarlo cada vez que realizamos un cambio en la configuración de mrtg.cfg.

*mrtg.html

```
<style type="text/css">
/* commandline was: /usr/bin/indexmaker --columns=1 --output /var/www/mrtg/
mrtg.html /etc/mrtg.cfg */
</style>
</HEAD>

<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000"
alink="#000000">


<H1>MRTG Index Page</H1>

<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
<tr>
<td><DIV><B>Traffic Analysis for wlan2 -- valupvgrcRd1</B></DIV>
<DIV><A HREF="10.228.154.225_wlan2.html"><IMG BORDER=1
ALT="10.228.154.225_wlan2 Traffic Graph" SRC="10.228.154.225_wlan2-
day.png"></A><BR>
<SMALL><!--#flastmod file="10.228.154.225_wlan2.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Traffic Analysis for ether1 -- valupvgrcRd1</B></DIV>
```

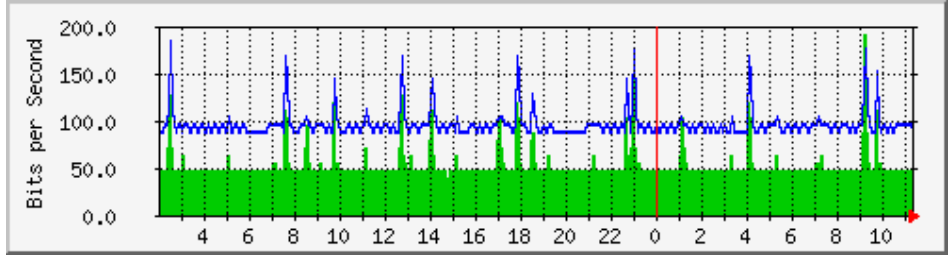
Los gráficos no se actualizan en tiempo real, cuando hemos instalado el mrtg también se ha creado un cron que se ejecuta cada 5 minutos y obtiene los datos, por eso los gráficos no aparecen al instante de ejecutar el comando indexmaker.

Vemos los gráficos obtenidos:

GENERALES (TODAS LAS INTERFACES)

MRTG Index Page

Traffic Analysis for wlan2 -- valupvgrcRd1



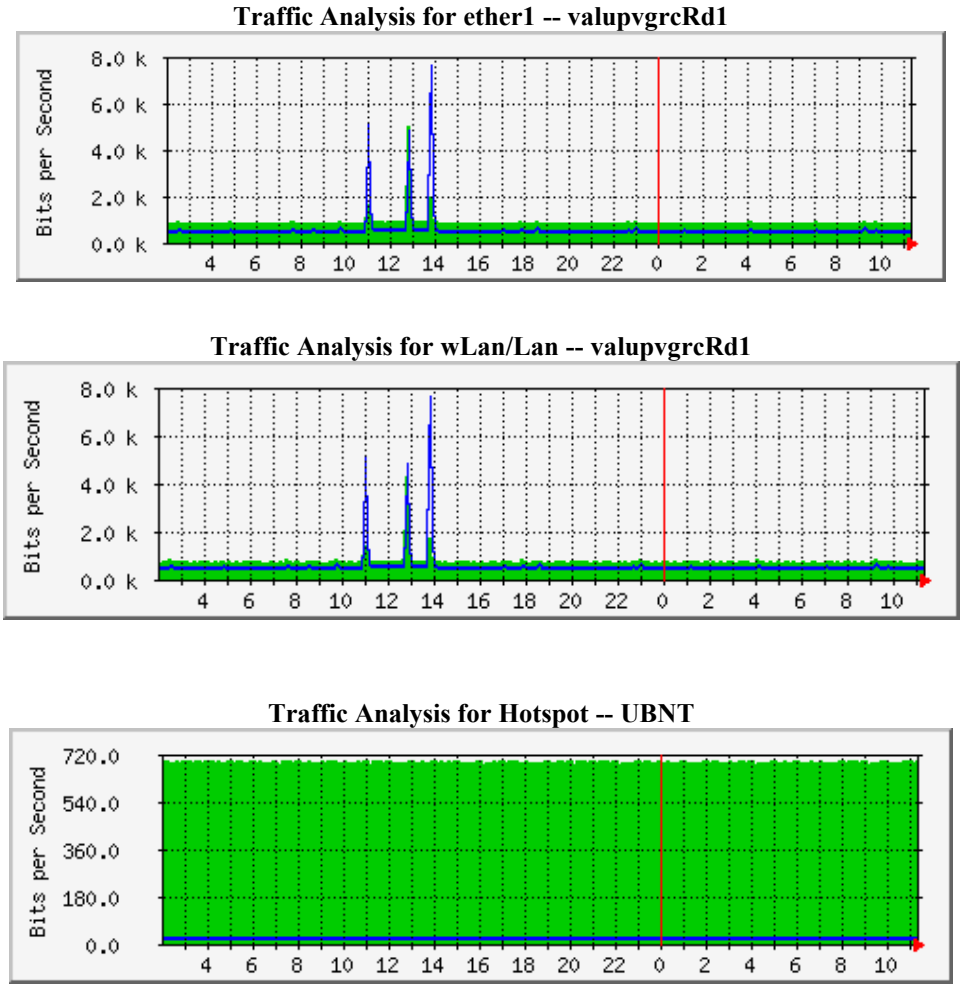


Figura 5.5. Gráfica general de todas las interfaces

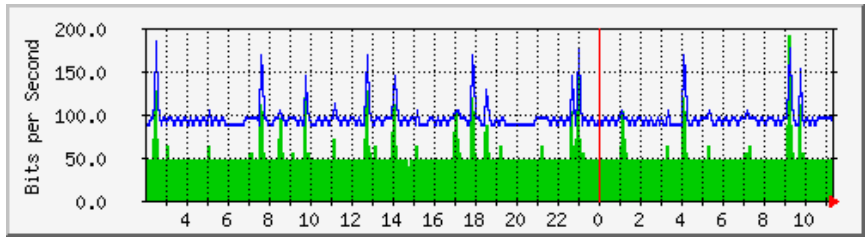
DE UNA SOLA INTERFACE

Traffic Analysis for wlan2 -- valupvgrcRd1

System:	valupvgrcRd1 in valupvgrc
Maintainer:	guifi@guifi.net
Description:	wlan2
ifType:	Radio Spread Spectrum (802.11) (71)
ifName:	wlan2
Max Speed:	1375.0 kBytes/s
Ip:	10.228.154.161 (vlcupvap0- 180.guifi.net)

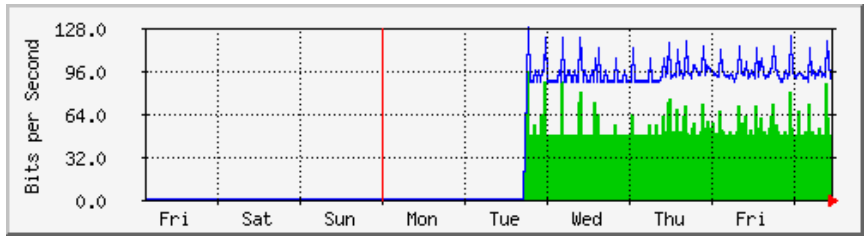
The statistics were last updated **Saturday, 18 February 2012 at 11:20**,
at which time **'valupvgrcRd1'** had been up for **77 days, 21:58:19**.

`Daily' Graph (5 Minute Average)



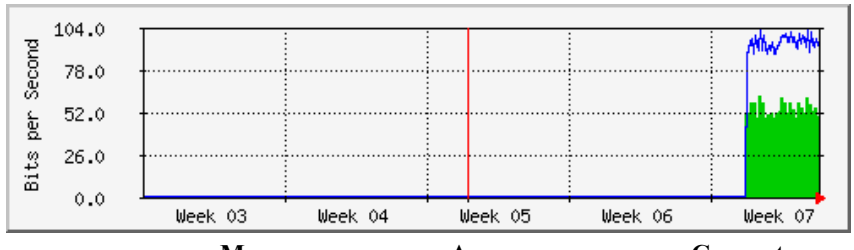
	Max	Average	Current
In	192.0 b/s (0.0%)	56.0 b/s (0.0%)	48.0 b/s (0.0%)
Out	184.0 b/s (0.0%)	96.0 b/s (0.0%)	88.0 b/s (0.0%)

`Weekly' Graph (30 Minute Average)



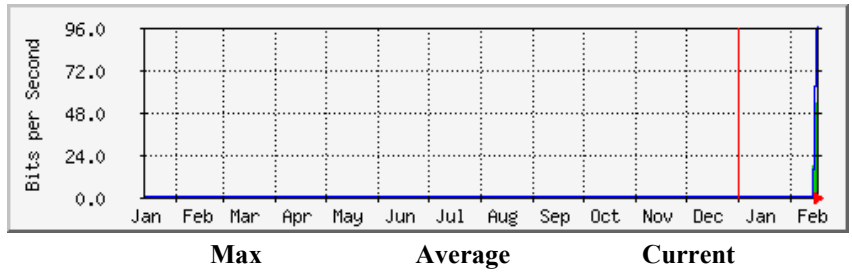
	Max	Average	Current
In	96.0 b/s (0.0%)	56.0 b/s (0.0%)	48.0 b/s (0.0%)
Out	128.0 b/s (0.0%)	96.0 b/s (0.0%)	96.0 b/s (0.0%)

`Monthly' Graph (2 Hour Average)



	Max	Average	Current
In	56.0 b/s (0.0%)	56.0 b/s (0.0%)	48.0 b/s (0.0%)
Out	96.0 b/s (0.0%)	96.0 b/s (0.0%)	96.0 b/s (0.0%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	48.0 b/s (0.0%)	40.0 b/s (0.0%)	56.0 b/s (0.0%)
Out	96.0 b/s (0.0%)	72.0 b/s (0.0%)	96.0 b/s (0.0%)

GREEN ### Incoming Traffic in Bits per Second

BLUE ### Outgoing Traffic in Bits per Second

Figura 5.6. Gráficas individuales de cada interface

CAPÍTULO 6:

CONEXIÓN NODO CLIENTE A GUIFI.NET

6.1. Instalación del nodo

Para completar la red inalámbrica, ejecutar las pruebas finales de funcionalidad y realizar la última parte del estudio con el análisis de las prestaciones que nos proporciona la red, hemos instalado un nodo cliente en un despacho del edificio de la Escuela que dispone de visión directa con las antenas de supernodo.

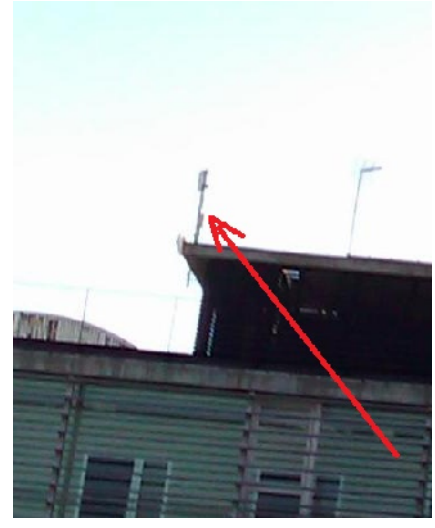


Figura 6.1. Línea de visión de las antenas

Para ello instalamos un ordenador (Probanano) con una antena conectada a su tarjeta de red Ethernet. La elección del hardware del ordenador no tiene gran influencia en la configuración del equipo cliente. El equipo que se ha colocado es un Pentium Dual Core a 3 GHz con 2GB de memoria RAM. El sistema operativo que se ha instalado es un Windows XP. Si hubiéramos elegido otro sistema operativo los pasos a seguir serían los mismos ya que son independientes del sistema operativo, aunque la configuración de la dirección IP variará. Lo que si tiene mucha más relevancia es la elección de la antena, tanto por sus características de ganancia y alcance como por la forma de configurarla. Para el cliente la antena elegida es una Ubiquiti Nanostation5 de 5 GHz.

Figura 6.2. Equipo del nodo cliente

A continuación se desarrollan los pasos a seguir para conectar el equipo cliente a la red Guifi.net. De forma resumida los pasos son:

- Averiguar el ESSID de la antena del supernodo a la que nos conectamos.
- Dar de alta al usuario en Guifi.net.
- Creación del nodo en Guifi.net
- Dar de alta el radio (antena) en Guifi.net
- Configurar la antena/router.

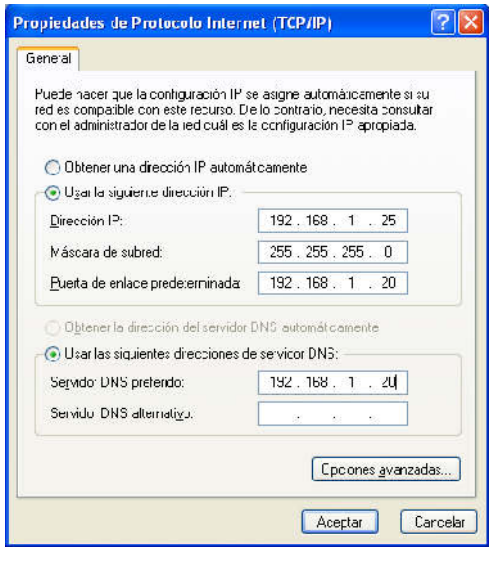
6.2. Conexión de la Nanostation5 .

Figura 6.4. Inyector POE

El primer paso será conectar la antena para averiguar el ESSID de la antena del supernodo a la que nos vamos a conectar. Para la conexión de la antena conectamos un extremo de un cable Ethernet a la antena (conector POE), el otro extremo al inyector del que sacamos otro cable Ethernet que se conecta a la tarjeta de red del ordenador.

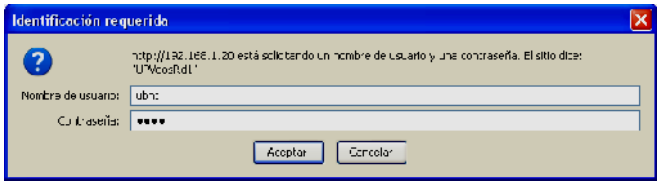
Figura 6.3. Antena

A continuación desde el sistema operativo XP cambiamos las opciones de la tarjeta de red del ordenador para poder conectarnos a la antena/router.



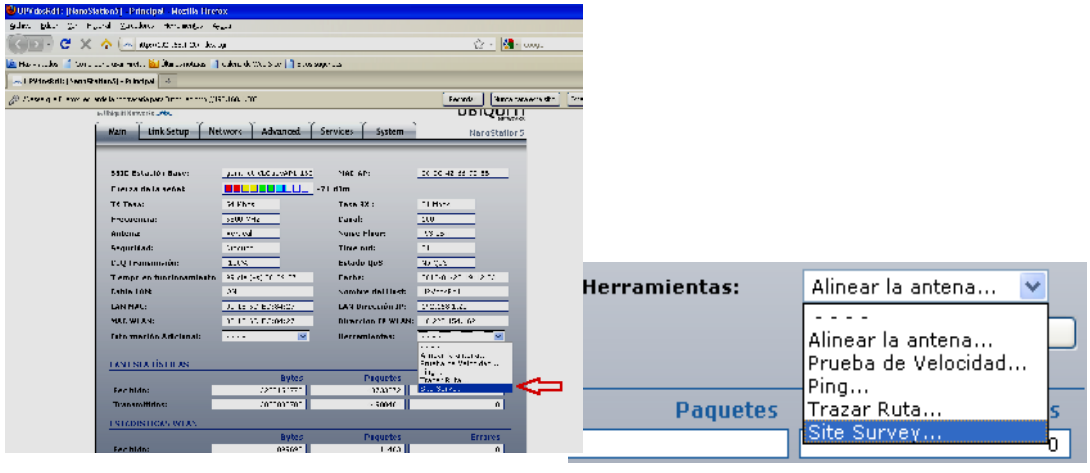
La Nanostation tiene prefijada la dirección IP privada 192.168.1.20 por lo que, como vemos en la imagen le ponemos al PC una dirección de la misma subred (192.168.1.25) para poder conectarnos.

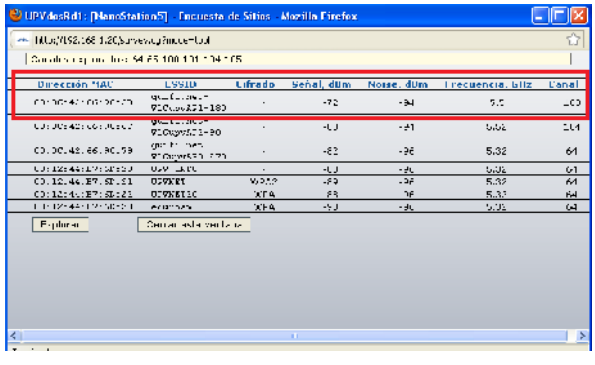
Una vez configurada la tarjeta de red accedemos a la Nanostation para buscar la antena del supernodo al que hemos de conectarnos. Para ello abrimos un navegador y escribimos la dirección de la Nanostation http://192.168.1.20.



Nos solicita identificarnos y ponemos tanto en Usuario como en contraseña: **ubnt** y accedemos a la aplicación de configuración de la antena.

En la pestaña **Main** desplegamos **Herramientas** y nos aparecerán diversas opciones, entre las que escogemos **Site Survey** y se abrirà una nueva ventana donde podremos ver todos los puntos de acceso a los que podemos conectarnos.





De las que corresponden a nuestro supernodo de Guifi.net elegimos la que tenga una mayor ganancia, es decir, una señal dBm más pequeña y guardaremos su ESSID (guifi.net- VLCupvAP1-180)

6.3. Crear cuenta usuario, nodo y radio

6.3.1. Alta de usuario en la web guifi.net

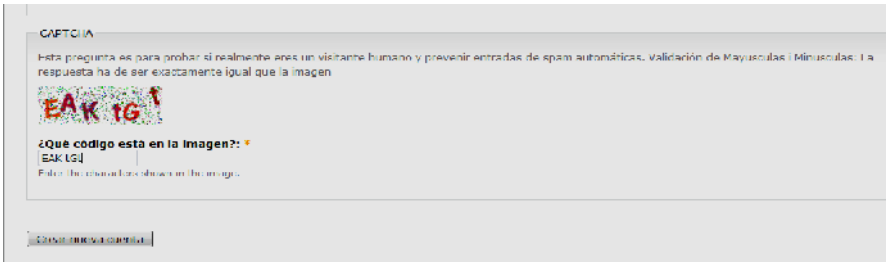
Para darnos de alta en la web es necesario un ordenador que tenga conexión a internet para acceder a la página http://www.guifi.net.

Accedemos a la parte superior de la página a "*Crear nueva cuenta*":

Donde se rellena un formulario que nos pide:

- Nombre de usuario: javiero
- Dirección correo electrónico: vjaviero09@gmail.com
- Ciudad y Provincia: Valencia
- El resto de los datos son opcionales.

En la parte inferior introducimos el código de verificación del gráfico (Captcha) y se pulsa en "Crear nueva cuenta"



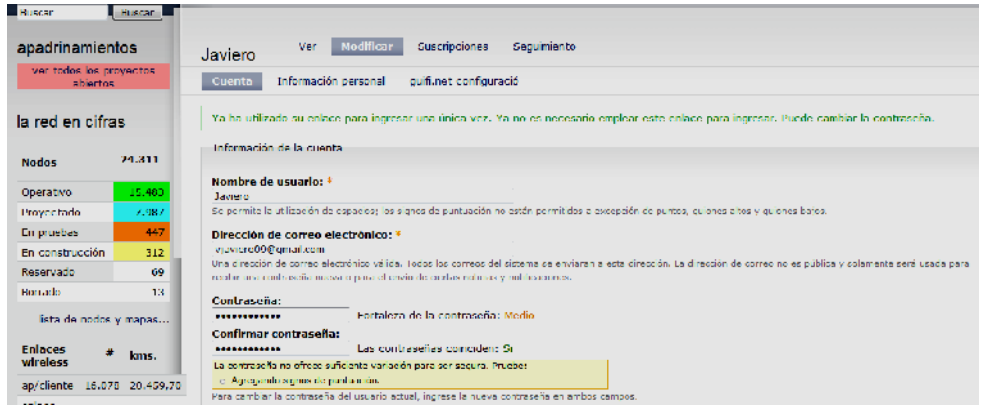
Recibimos un correo electrónico en la dirección que se ha indicado en el que nos indica cual es nuestra contraseña de acceso inicial.

"Javiero, Gracias por registrarte en guifi.net. Ya puedes iniciar sesión en http://guifi.net/ca/user utilizando el siguiente nombre de usuario y contraseña:"

Nombre de usuario: Javiero

Contraseña: Q5qBkheHpR

Y ahora ya se puede acceder con el usuario y cambiar la contraseña desde nuestra zona de usuario.



6.3.2. Alta del nodo en la web Guifi.net

Para crear nuestro nodo cliente accedemos a la página http://guifi.net/guifi.dir/mapa/mapa.html Donde aparece el mapa de la Península Ibérica y donde buscamos nuestra ubicación que marcamos en el mapa.

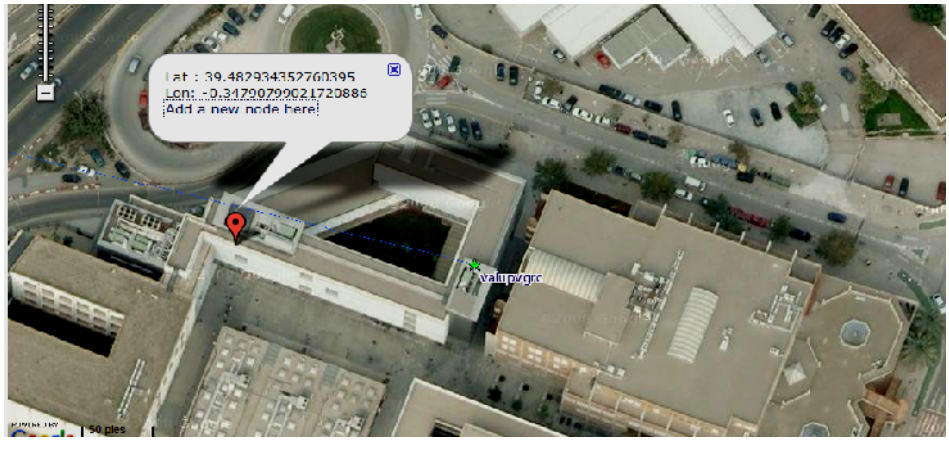
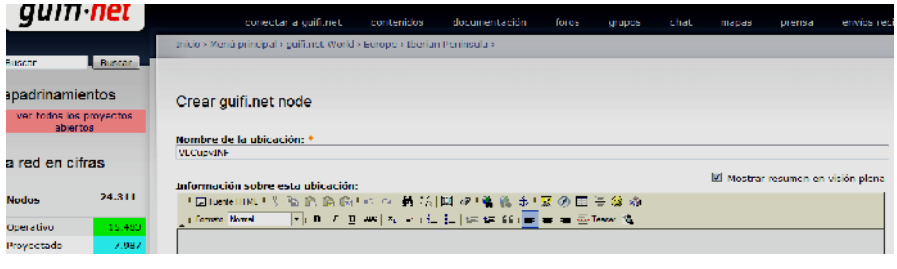


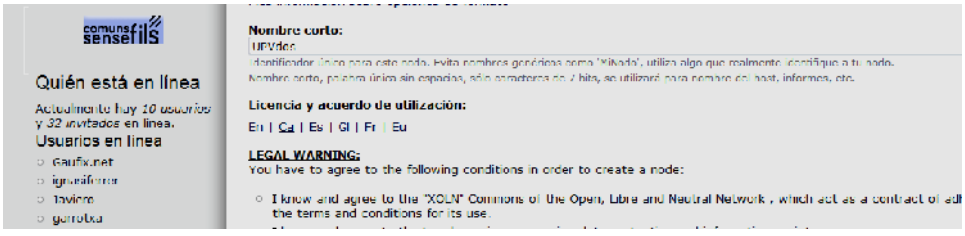
Figura 6.5 Vista detallada de ubicación del nodo cliente UPVdos

Aparecerá una ventana con las coordenadas y pulsamos sobre "*Add a new node here*"

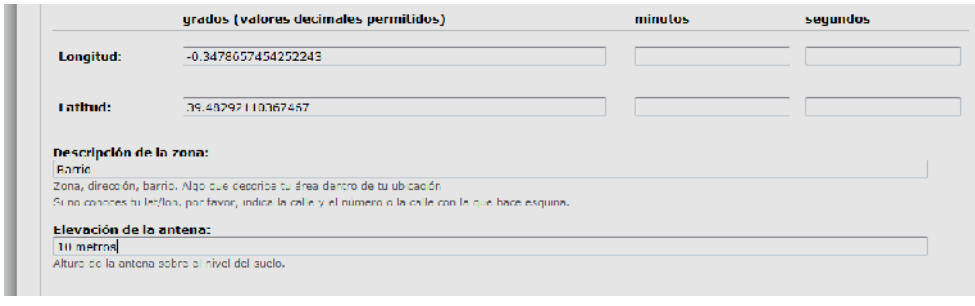
Y aparece la siguiente página donde ponemos el nombre de la ubicación: *VLCupvINF*



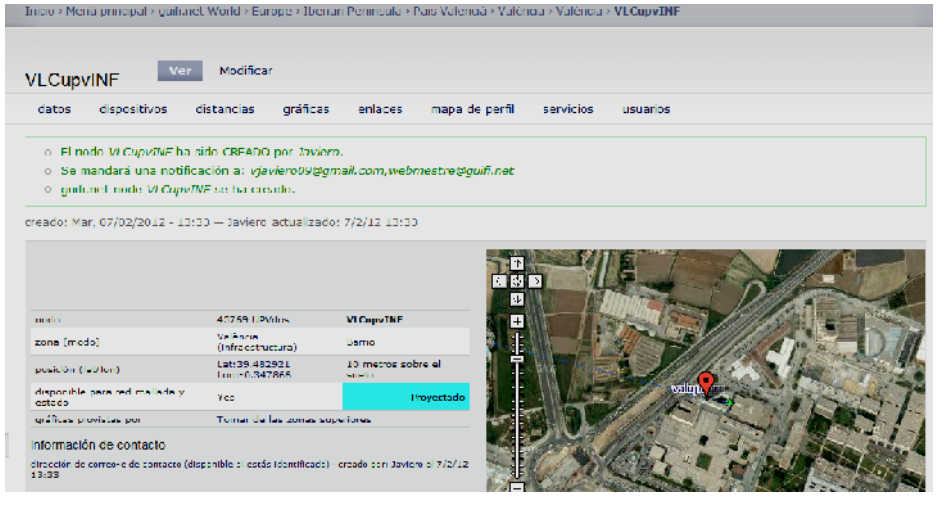
Colocamos el nombre corto de nuestro nodo (UPVdos). Y marcamos la casilla "**LEGAL WARNING**"



Se ajustan las coordenadas, se describe la zona, "*Barrio",* y se indica la que altura está la antena del suelo: 10 metros.



Y con esto se ha dado de alta el nodo que en principio aparecerá como *Proyectado* aunque después lo pondremos como *Operativo*.

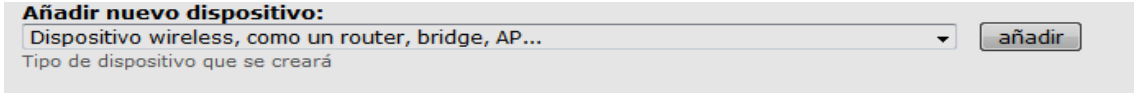


6.3.3. Añadimos un radio al nodo

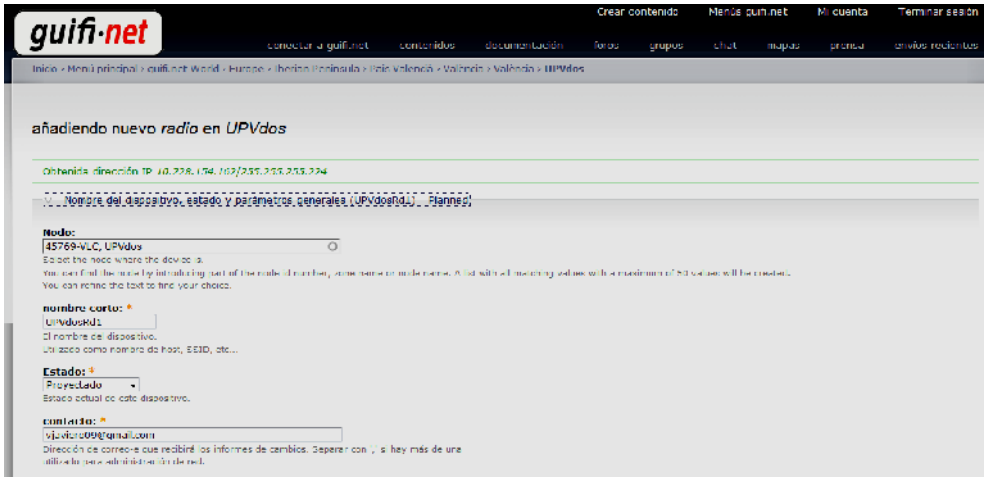
Para que nuestra Nanostation pueda funcionar dentro de la red Guifi.net es necesario que demos de alta un radio en la web.

En la página de nuestro nodo e identificándonos con Javiero, tenemos la opción de agregar un nuevo radio, lo que nos permitirá indicar a Guifi la antena que utilizamos pera conectarnos y poder descargar el fichero de configuración.

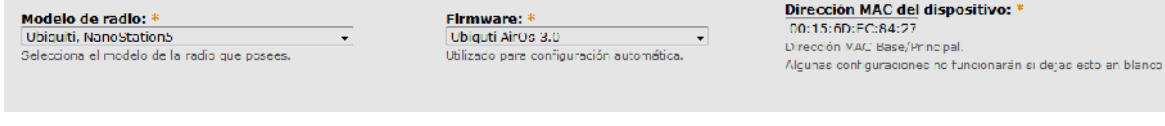
Primero abrimos el desplegable y seleccionamos la opción **"***Dispositivo wireless, como un router, bridge, AP,…"*



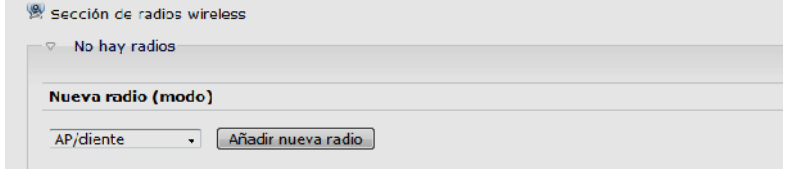
y nos aparece un formulario relleno con los nombres de radio UPVdosRd1 y la dirección de correo del usuario Javiero.



En modelo de radio escogemos del desplegable el modelo de antena: "Ubiquiti Nanostation 5. En Firmware elegimos "Ubiquiti AirOs 3.0" (sistema operativo de la Nanostation) y en Dirección MAC la de nuestra nanostation que encontraremos en la tapa, donde está el conector RJ45, escrita en una pegatina, o en la caja de la Nanostation:



Por último para agregar la radio. Pulsamos en *"No hay radios"* y lo dejamos en la opción *"Wireless Client"* pulsando en "*Añadir nueva radio"*.



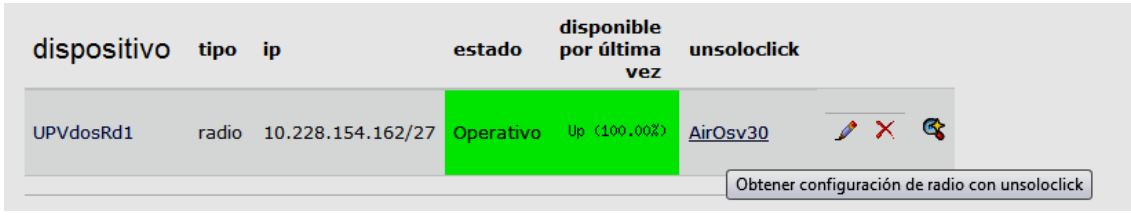
Aparecerá una nueva página donde ajustamos, el tipo (ángulo): *planar 90º*, ganancia: *14* y Grados: *100.*

Y para acabar se crea el enlace con la antena del supernodo cuyo ESSID hemos seleccionado con el *"survey"* antes (guifi.net- VLCupvAP1-180). Para ello pulsamos en la "*casa*" de *"Conexión al AP..." y* aparecerá una lista con los Supernodos ordenados, de los que escogemos el que nos interesa y volvemos a la página principal donde ya tenemos asignada una IP del rango de la antena del supernodo a la que nos hemos enlazado.

6.4. Configuración del nodo

6.4.1. Preparamos el archivo de configuración de la Nanostation

Una vez introducidos todos los datos y dado de alta el nodo en la web de Guifi.net tenemos que pasar la configuración que hemos creado a la Nanostation. Para ello la web de Guifi.net dispone de una utilidad en la página principal de nuestro nodo llamada **Unsoloclic**.



Pulsamos en el enlace de unsoloclick (AirOSv30) y nos aparecerá el fichero, en formato texto, de configuración

:

```
#Generado por:
#AirOsv30

Click here to download configuration file for: UPVdosRd1
Put the mouse cursor over the link. Right click the link and select "Save Link/Target As..." to save to
your Desktop.

#Configuration for AirOs> Unsolclic version:1.1 !! WARNING: Beta version !!
#Device: UPVdosRd1
#
#Methods to upload/execute the file:
#1.- As a file. Upload this through web managment:
#a.System->Configuratuion Managment->Locate file
#b.Upload
#2.- Telnet: Open a terminal session, create new /tmp/system.cfg file and cut&paste
#the contents of the file. Save it an execute the command:
#
#/usr/etc/rc.d/rc.softrestart save
#
#Notes:
#-Web access method is recommended
#(the script reconfigures some IP addresses, so communication can be lost.
# 192.168.1.1 will be the new one)
#-Changes are done in user passwords on the device, default user and password are
#changed to root/guifi.
#-The ACK is set to 45 for 802.11b mode, and to 25 for 802.11a (600 meters aprox,)
#
## Link to AP info
Ap SSID = guifi.net-VLCupvAP1-180
WAN Ip address = 10.228.154.162
WAN Netmask = 255.255.255.224
WAN Gateway = 10.228.154.161
Primary DNS Server = 10.228.154.2
Secondary DNS Server = 10.37.72.3
Device HostName = UPVdosRd1
IEEE 802.11 Mode: = A (5Ghz)
Antenna Selection or/and Polarization: = Main/Internal - Vertical
```

Ahora tenemos 2 opciones:

- Introducir de forma manual, en el programa del sistema operativo de Ubiquiti AirOs de la Nanostation, accediendo por la URL http://192.168.1.20 desde el ordenador cliente, la configuración de red que nos indica.
- Cargar de forma automática, utilizando también el mismo método de acceso, el fichero de configuración que nos ofrece unsoloclick y que se encarga de configurar todo el nodo sin nuestra intervención.

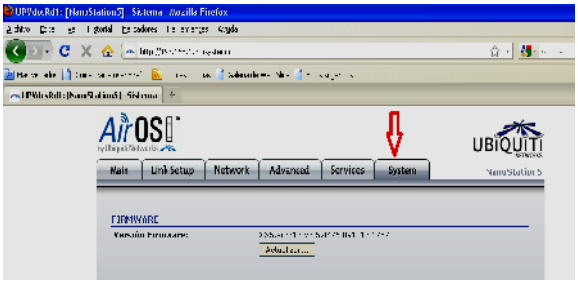
En principio he hecho la configuración de forma manual, pero la forma automática es más fácil de realizar y evita cometer algún error u olvido en la introducción de los datos.

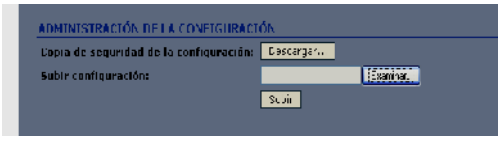
Para obtener el archivo de configuración necesario para realizar el proceso automáticamente hay que pulsar sobre el enlace *"Click here to download configuration file for: UPVdosRd1"* lo que abre otra página con el código a introducir en la Nanostation.

Lo siguiente es abrir el "bloc de notas", seleccionar todo el código, pegarlo al bloc y guardarlo con el nombre que queramos pero con la extensión .conf (le he puesto *UPVdos.conf*)

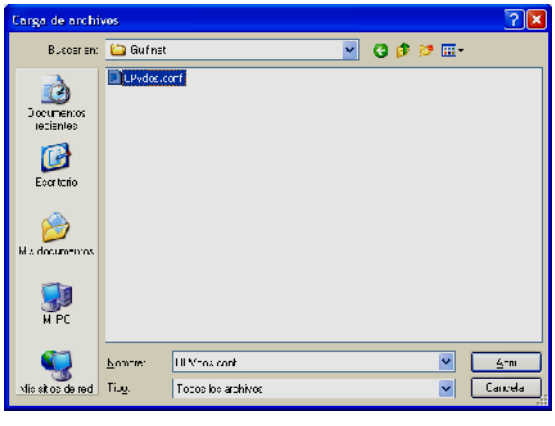
6.4.2. Configuramos la Nanostation (descarga del fichero de configuración)

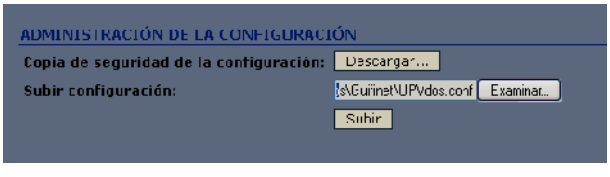
Con la Nanostation conectada al PC cliente, como se ha descrito antes, volvemos a abrir el navegador con la URL de la Nanostation http://192.168.1.20 e introducimos usuario y password (ubnt) accedemos a la aplicación de configuración de la antena a la pestaña *System* y al final de ella al apartado *Administración de la configuración*:



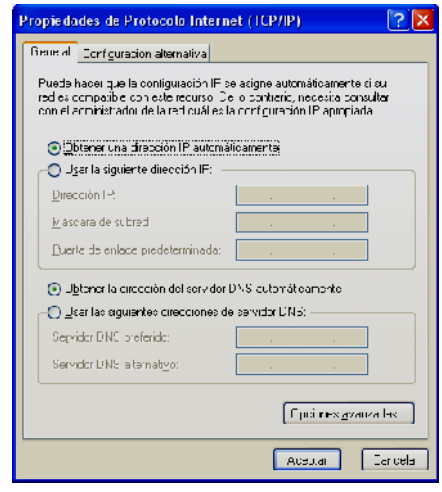


Pulsamos en "*Examinar*" y aparece la siguiente ventana de seleccionamos el fichero de configuración creado (*UPVdos.conf*). Pulsamos *Abrir* y a continuación *Subir*.



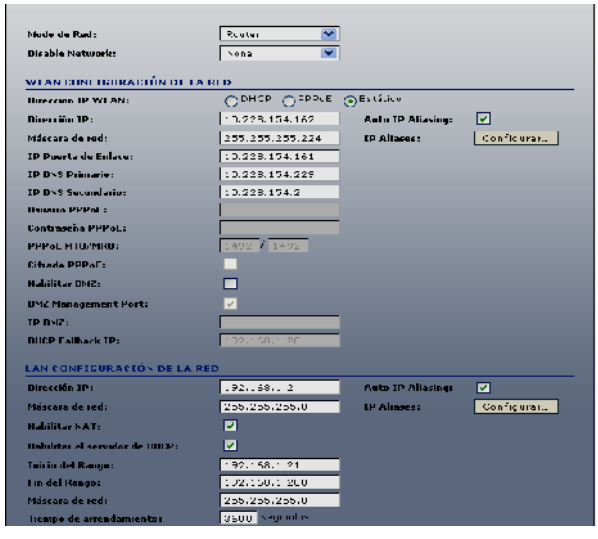


Y después de dar la conformidad en la parte superior de la página con *Aplicar* se reinicia la Nanostation y ya está configurada.



Ahora, en primer lugar, cambiamos la configuración de TCP/IP de la tarjeta de red de nuestro ordenador e indicamos que obtenga todos sus datos de red por DHCP.

A continuación accedemos de nuevo a la Nanostation para comprobar su configuración final y para ello ahora debemos poner la URL *http:///192.168.1.2* que abre la ventana de solicitud del nuevo usuario y password que será *root y guifi* respectivamente, y finalmente accedemos a la configuración de la antena cuya pestaña de Network ha quedado así:



6.5 El cliente móvil: Hotspot

Aunque la filosofía de la red Guifi.net se basa en que existan nodos y supernodos estáticos gestionados, tanto a nivel de usuario, como de equipo (nodo) y servicios desde la propia web de Guifi.net, al realizar la instalación del supernodo de la UPV incluimos la instalación de una antena Nanostation2 que trabaja a 2,4 GHz para que hiciera de punto de acceso (hotspot) de modo que equipos móviles (PC portátiles, PDAs, teléfonos móviles…) pudieran acceder a la red de Guifi.net y, como veremos en el capítulo correspondiente, mediante VPN, a la red de la UPV.

La instalación y configuración del hotspot ya se ha descrito anteriormente. Aquí solo se va a ver como se conecta un portátil a la antena hotspot.

6.5.1. Conexión a la antena hotspot

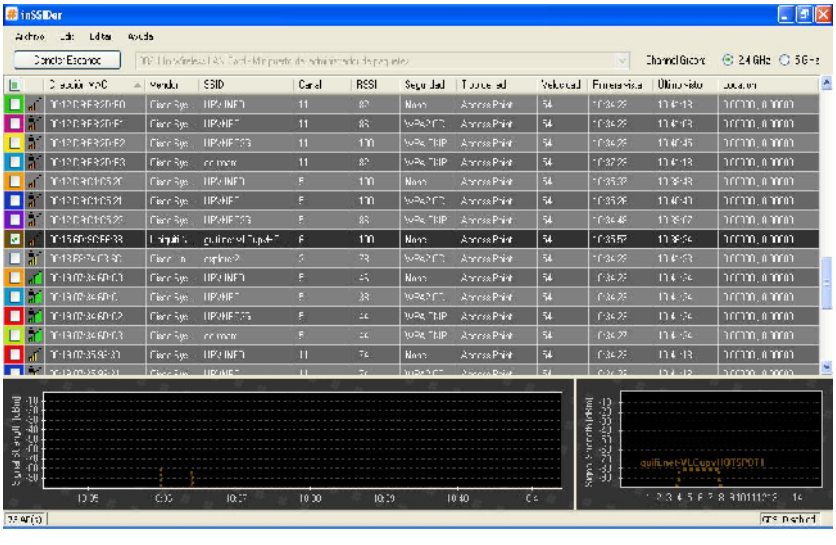
Para realizar esta prueba utilizamos un portátil con sistema operativo Windows XP que lleva incorporada y activa una interface inalámbrica de tipo “g” a 2,4 GHz.

Le instalamos la aplicación InSSIDer que es una utilidad open source que busca redes Wi-Fi cercanas y muestra la potencia de su señal. Este escáner WiFi de red solo funciona para Windows Vista y Windows XP.

Utiliza la antena Wifi de cada portátil para escanear las redes cercanas y determinar la información necesaria: SSID, dirección MAC, potencia, seguridad...

Nos situamos, con el portátil, en una zona de la Escuela con visión directa a la antena hotspot. Arrancamos el sistema operativo y lanzamos la aplicación InSSIDer. Aparece en pantalla su interface dividida en tres zonas. En la parte superior el programa lista las redes que hay en nuestro entorno con la información del número de canal que usan, así como la potencia de señal que recibimos de dicha red, la protección que usa y la velocidad a la que trabajan. En la parte de abajo a la izquierda, se ve un histórico de la potencia de la señal recibida en cada red, y en la parte derecha el estado actual de las redes, observando qué espectro utilizan, y cómo se solapan entre sí. En nuestro caso, para esta última zona seleccionamos nuestra antena guifi.net-VLCupvHOTSPOT1

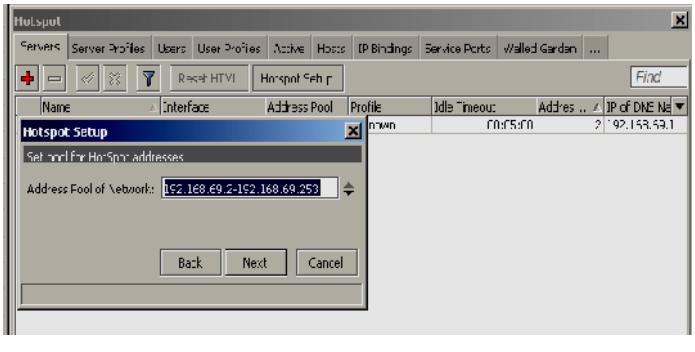
Figura 6.6 Antena hotspot



Una vez detectada la antena y después de comprobar el canal, ganancia y resto de datos, nos conectamos a ella. El Mikrotik, con su servicio de DHCP nos proporciona la dirección IP 192.168.69.2 con la que tenemos comunicación con la antena por su interface con IP 192.168.69.1.

Figura 6.7 Gráfica de selección de la antena y tráfico de la conexión al hotspot

Cuando queremos comunicarnos con equipos de la red Guifi.net el router hace NAT y saca la información por el Gateway por defecto 10.228.154.225 y así ya se puede acceder, tanto a la red Guifi.net, como a la red de la UPV si se realiza una conexión por VPN.



CAPÍTULO 7:

CONEXIONES VPN

7.1. Salimos de la isla.

Una vez instalado y configurado nuestro nodo con sus radios y nuestro servidor con sus servicios solo nos queda establecer la conexión con la red Guifi.net. En el momento de escribir esta memoria no existe posibilidad de establecer una comunicación inalámbrica con ningún "supernodo" que nos dé acceso al resto de la red de Guifi.net. Existen diferentes nodos aislados en la zona de Valencia que como nosotros son islas esperando que la red, en su expansión, sea accesible. La antena parabólica Ubiquiti Rocket5 direccional que tenemos en el nodo está orientada al norte pendiente de establecer conexión con un nodo de, esperemos, próxima instalación en la zona de Sagunto.

Mientras llega el momento de establecer esta comunicación, decidimos realizar la conexión con la zona de Guifi.net Castellón por la red cableada, estableciendo para ello un túnel VPN entre nuestro nodo y el servidor de Guifi.net de la Universidad Jaume I de Castellón.

También planteamos dar un servicio adicional para los usuarios que den de alta sus nodos cliente en Guifi.net, se conecten a nuestro supernodo y además pertenezcan a la comunidad universitaria de la UPV, consistente en poder acceder a la red UPVNET y desde allí tener acceso a Internet. Para ello aprovechamos, igualmente, la existencia de un servidor VPN en la UPV y creamos un túnel con él desde nuestro nodo.

7.2. Conexión VPN

VPN (Virtual Private Network) o Red Privada Virtual (RPV) es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Las siglas de VPN nos indican que son redes "Virtuales" y "Privadas". Virtuales porque no son redes directas reales entre partes, sino solo conexiones virtuales provistas mediante software sobre la red Internet. Además son privadas porque solo la gente debidamente autorizada puede leer los datos transferidos por este tipo de red logrando la seguridad mediante la utilización de modernos mecanismos de criptografía.

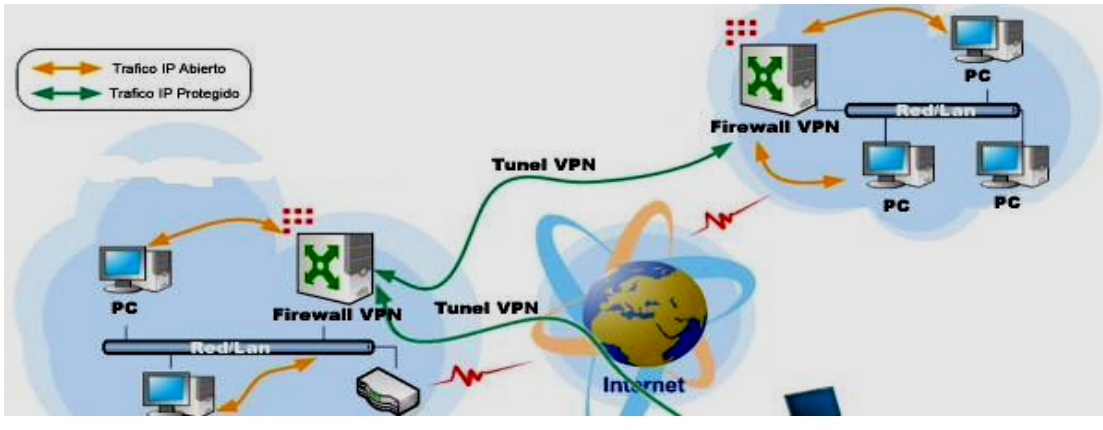


Figura 7.1 Esquema de conexiones VPN

7.2.1. Usos de las VPNs

Las VPN's se usan generalmente para:

- Conexión entre diversos puntos de una organización a través de Internet
- Conexiones de trabajadores domésticos o de campo con IP's dinámicas
- Soluciones extranet para clientes u organizaciones asociadas con los cuales se necesita intercambiar cierta información en forma privada pero no se les debe dar acceso al resto de la red interna.

7.2.2. Ventajas principales

- Se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).
- Las conexiones VPN pueden ser realizadas a través de casi cualquier firewall.
- Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y como servidor.
- Alta flexibilidad y posibilidades de extensión mediante scripting.
- Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.
- Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.

7.2.3. OpenVPN

Para la implementación del túnel entre nuestro nodo y el servidor de Guifi.net Castellón se ha elegido OpenVPN.

OpenVPN es una solución de conectividad de software libre bajo la licencia GPL, basada en software SSL (Secure Sockets Layer) que ofrece conectividad punto a punto con validación jerárquica de usuarios y host conectados remotamente.

7.3. Túnel con Guifi.net Castellón

Para establecer la conexión con la zona Guifi.net de Castellón se crea un túnel encriptado entre dos máquinas, servidor en la UJI y cliente en nuestro equipo servidor del supernodo, utilizando una clave estática. Ambos cliente y servidor tienen una IP fija de la red Guifi.net y de Internet. El cliente debe mantener siempre el túnel abierto.

7.3.1. Establecemos el túnel

En este caso el servidor del túnel ya está en funcionamiento en la UJI y tiene la IP pública 150.128.97.38. En él ya está instalado el paquete openvpn con todas sus dependencias.

En nuestro ordenador (VLCupvGRC) que actúa como **cliente** del servidor VPN se instala también el openvpn. Para ello solo es necesario escribir en la consola:

guifi@VLCupvGRC:~$ sudo apt-get install openvpn

Se lee la lista de paquetes. Se construye el árbol de dependencias y se instalan los paquetes auxiliares: liblzo2-2 libpkcs11-helper1 openvpn-blacklist

Preparamos el archivo de configuración:

guifi@VLCupvGRC:~$ sudo cp -a /usr/share/doc/openvpn/examples/easy-rsa/2.0/ /etc/openvpn/2.0

guifi@VLCupvGRC:~$ sudo cd /etc/openvpn/2.0/

guifi@VLCupvGRC:~$ sudo gedit vars

Personalizamos el fichero:

```
# Don't leave any of these fields blank.
export KEY_COUNTRY="ES"
export KEY_PROVINCE="VLC"
export KEY_CITY="Valencia"
export KEY_ORG="UJI-UPV"
export KEY_EMAIL="micorreo@gmail.com"
```

Lo guardamos e inicializamos las variables:

guifi@VLCupvGRC:~$ sudo source ./vars

guifi@VLCupvGRC:~$ sudo ./clean-all

Ahora se crea la *clave estática* en el **servidor**, lo que se realiza con el administrador del servidor Guifi.net de la UJI:

root@Castellon: ~# cd /etc/openvpn/

root@Castellon: ~#:/etc/openvpn# openvpn --genkey --secret staticUJI-UPV.key

root@Castellon: ~# etc/openvpn# ls -l

total 3

-rw------- 1 root root 636 feb 18 19:48 staticUJI-UPV.key

-rwxr-xr-x 1 root root 1352 sep 18 2008 update-resolv-conf

root@Castellon: ~# /etc/openvpn#

y a continuación mediante ssh se copia el fichero de clave al cliente en la misma carpeta /etc/openvnc.

En el servidor, se crea el fichero */etc/openvpn/tunUJI-UPV.conf* con el siguiente contenido:

dev tunUJI-UPV

ifconfig 10.228.170.5 10.228.170.6

secret static.key

Donde *10.228.170.5* es la IP del servidor en el túnel y *10.228.170.6* la IP del cliente en el túnel.

En el cliente creamos también el fichero */etc/openvpn/tunUJI-UPV.conf* con el siguiente contenido:

tunUJI-UPV.conf

```
remote 150.128.97.38
dev tunUJI-UPV
ifconfig 10.228.170.6 10.228.170.5
secret staticUJI-UPV.key
#keepalive 10 60
log /var/log/openvpn
```

donde 150.128.97.38 es la IP pública del servidor.

Podíamos haber puesto también la instrucción port 1194 donde se le indica el puerto que utiliza pero no es necesario ya que este es el puerto por defecto. Lo que si que hay que tener en cuenta es que si lo cambiamos hay que poner el mismo tanto en el servidor como en el cliente. Los puertos hay que abrirlos en el cortafuegos.

keepalive 10 60 Es para que automáticamente vuelva a abrir el túnel si no está funcionando. Pero al instalar openvpn ya se pone en el arranque de la máquina por lo que no es necesario añadirlo. También le indicamos donde debe dejar el fichero de logs.

Si no queremos que el túnel esté encriptado hay que añadir en el fichero de opciones o en la línea de órdenes al ejecutar el túnel: *cipher none*

Con esto, en principio, el túnel ya funciona y está configurado en /etc/openvpn/tunUJI-UPV.conf, y únicamente falta establecer que haga forwarding y poner en los ficheros de configuración 2 rutas estáticas, ya que si se reinicia el ordenador dejará de funcionar, la 10.228.0.0/16 y la 10.229.0.0/16.

Le agregamos las 2 rutas al final del fichero */etc/openvpn/tunUJI-UPV.conf*

tunUJI-UPV.conf

```
remote 150.128.97.38
dev tunUJI-UPV
ifconfig 10.228.170.6 10.228.170.5
secret staticUJI-UPV.key
#keepalive 10 60
log /var/log/openvpn
route-up "route add -net 10.228.0.0 netmask 255.255.0.0 gw 10.228.170.5"
route-up "route add -net 10.229.0.0 netmask 255.255.0.0 gw 10.228.170.5"
```

Y la tabla de rutas de nuestro servidor quedará:

```
guifi@VLCupvGRC: ~
Archivo  Editar  Ver  Terminal  Ayuda
guifi@VLCupvGRC:~$ route
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
10.228.170.5    *               255.255.255.255 UH    0      0        0 tunUJI-UPV
10.228.154.224  *               255.255.255.248 U     0      0        0 eth0
10.228.154.0    valupvgrcRd1.gu 255.255.255.0   UG    0      0        0 eth0
158.42.214.0    *               255.255.254.0   U     0      0        0 eth1
10.229.0.0      10.228.170.5    255.255.0.0     UG    0      0        0 tunUJI-UPV
10.228.0.0      10.228.170.5    255.255.0.0     UG    0      0        0 tunUJI-UPV
link-local      *               255.255.0.0     U     1000   0        0 eth1
172.16.0.0      10.228.170.5    255.240.0.0     UG    0      0        0 tunUJI-UPV
10.0.0.0        valupvgrcRd1.gu 255.0.0.0       UG    0      0        0 eth0
default         rou-afi.net2.up 0.0.0.0         UG    100    0        0 eth1
guifi@VLCupvGRC:~$
```

Donde aparece el túnel y las rutas estáticas pero se comprueba que si se para el servicio, al volver a arrancarlo o al restaurarlo desaparecen las rutas estáticas y el túnel no funciona por lo que para solucionarlo introducimos las 2 rutas en el script */etc/init.d/openvpn*, tanto en el start como en el restart, para forzar así que se instalen cada reinicio.

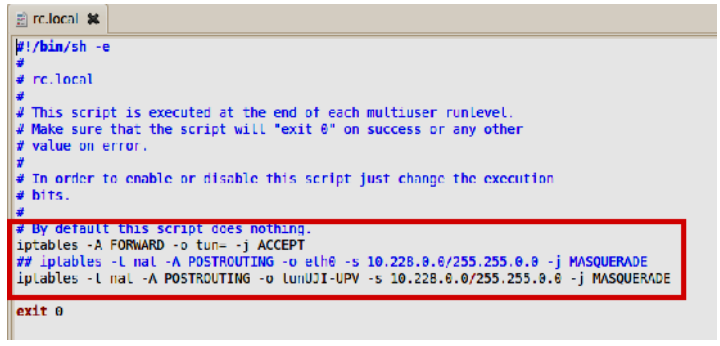
```
openvpn
    fi
  #start VPNs from command line
  else
    while shift ; do
      [ -z "$1" ] && break
      NAME=$1
      if test -e $CONFIG_DIR/$NAME.conf ; then
        log_daemon_msg "  Starting VPN '$NAME'"
        start_vpn
      else
        log_failure_msg "  Starting VPN '$NAME': missing $CONFIG_DIR/$NAME.conf file !"
        STATUS=1
      fi
    done
  fi

route add -net 10.228.0.0/16 gw 10.228.170.5
route add -net 10.229.0.0/16 gw 10.228.170.5
```

En el fichero */etc/network/interfaces* vemos que ya aparecen en el interface de red (eth0) las rutas estáticas del túnel

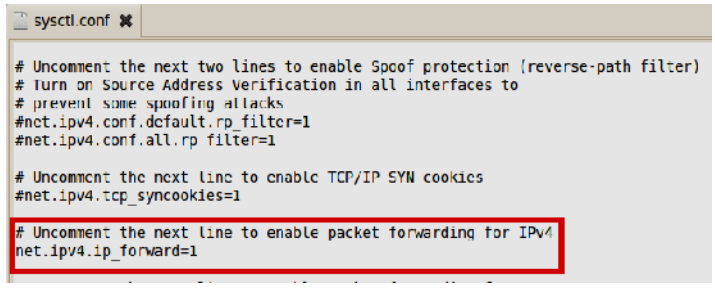
```
*interfaces
auto eth0
iface eth0 inet static
        address 10.228.154.229
        netmask 255.255.255.248
        network 10.228.154.224
        #broadcast 10.228.138.162
        #gateway 10.1.1.201
        #post-up route add -net 10.228.0.0 netmask 255.255.0.0 gw 10.228.138.161
        #pre-down route del -net 10.228.0.0 netmask 255.255.0.0 gw 10.228.138.161
        #dns-nameservers 158.128.98.10 150.128.16.10
        #dns-search castello.guifi.net

up route add -net 10.228.154.0/24 gw 10.228.154.225
up route add -net 10.228.0.0/16 gw 10.228.170.5
up route add -net 10.229.0.0/16 gw 10.228.170.5
up route add -net 10.0.0.0/8 gw 10.228.154.225
```

Para activar el forwarding realizamos 2 acciones:

- Modificamos el iptables editando el fichero /etc/rc.local y añadiendo al final las filas siguientes:



Editamos el fichero /etc/sysctl.conf y descomentamos la línea: #net.ipv4.ip_forward=1



Reiniciamos el servidor openvnc:

guifi@VLCupvGRC:~$ sudo /etc/init.d openvpn restart

Comprobamos la tabla de router del Mikrotik para comprobar que todas las direcciones que no tengan un destino con Gateway expresamente indicado se direccionen al servidor de nuestro nodo (10.228.154.229) donde está la entrada del túnel.

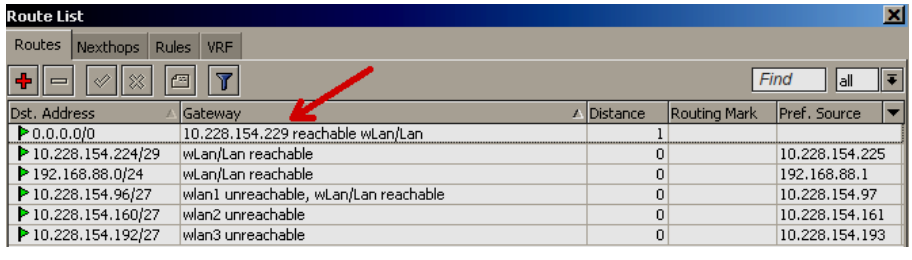
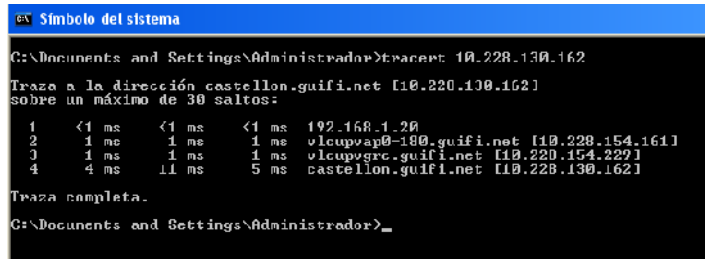


Figura 7.2 Tabla de rutas del routerboard

Por último realizamos la prueba desde el equipo cliente Windows XP. Primero ejecutando un tracert a la dirección 10,228.130.162 (servidor de Guifi-Castellón).



Y después accediendo a su web Castello.guifi.net desde la red de Guifi.net (10.228.130.162)

Figura 7.3 Acceso a la Web de Castellón desde la red Guifi.net

7.4. Túnel con la UPV

Muchos fueron los motivos por los que nos planteamos la idea de instalar un supernodo de Guifi.net dentro de la Universidad Politécnica de Valencia, y entre ellos los más importantes fueron:

- Apoyar la extensión y promoción de la red libre en la provincia de Valencia y, por ende, entre la comunidad universitaria.
- Proporcionar los servicios de la red a aquellos usuarios que quisieran participar en su desarrollo.
- La oportunidad de ofrecer a los usuarios de Guifi.net, que al mismo tiempo fueran miembros de la universidad, la posibilidad de conectarse a la red de la universidad y desde ella a Internet.

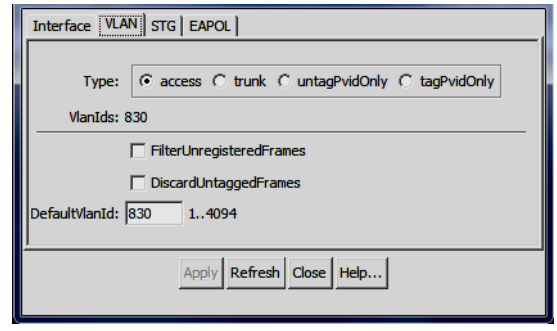
Para ello se solicitó al ASIC (Área de Sistemas de Información y Comunicaciones) de la UPV la creación de una VLAN (red de área local virtual) para los accesos de Guifi.net y desde ella una conexión VPN (red privada virtual) con el servidor VPN de la universidad.

7.4.1. VLAN 830

Para la interconexión de todos los componentes del nodo y su funcionamiento, solamente sería necesario utilizar un equipo electrónico, generalmente un switch, y después, si se desea establecer una conexión con la UPV se hubiera hecho la conexión de un puerto de dicho switch al servidor VPN de la UPV.

Pero, aprovechando la existencia de electrónica de red y de un cableado estructurado con rosetas que interconexionan los equipos de la red de la UPV y teniendo la posibilidad de conectar los elementos del nodo Guifi.net a esta electrónica, surge la necesidad de independizar a nivel de enlace la subred de Guifi.net del resto de la red UPV permitiendo que los elementos puedan convivir a nivel físico conectados en el mismo switch.

Por ello es necesario crear una VLAN que permita a los distintos elementos del nodo estar integrados en la electrónica de red de la universidad y que así podamos posteriormente conectarlos al terminador de túneles.



Una VLAN (Virtual LAN) es una subred IP separada de manera lógica que permite que redes IP y subredes existan en la misma red conmutada. Son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local que no deben intercambiar datos usando la red local.

Cada ordenador de una VLAN debe tener una dirección IP y una máscara de subred correspondiente a dicha subred.

Para nuestra red Guifi.net dentro de la red de la UPV se crea la VLAN 830. Para que todos los equipos de esta subred (10.228.154.224/29) puedan comunicarse se configura cada puerto de switch al que estén conectados en la VLAN de Guifi.net 830

Con la configuración de los puertos de los switches donde están conectados todos nuestros equipos del nodo, router (10.228.154.225), hotspot (10.228.154.226), antena parabólica (10.228.154.227) y servidor (10.228.154.229) a la VLAN 830 ya tenemos finalizada la instalación física de la red de nuestro nodo en lo que respecta a la conectividad con guifi.net.

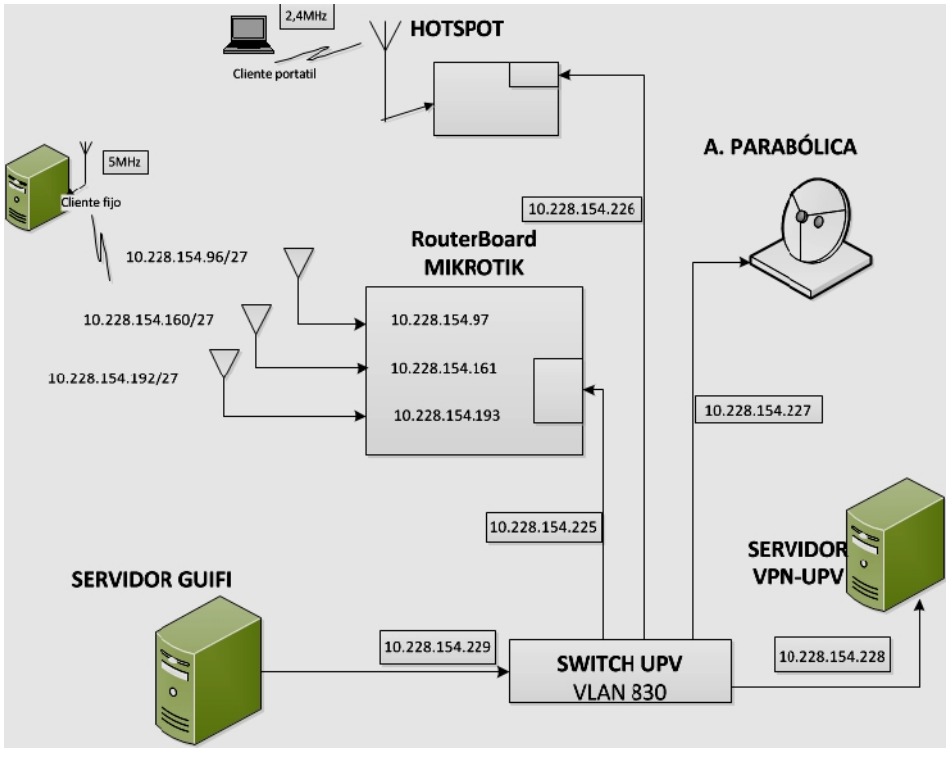


Figura 7.4 Diagrama de conexiones de la VLAN 830

Puerto	802.1Q Tagged	VLAN por defecto	VLANs	Color	Auto negociación	Velocidad	Full Duplex
01	SI	990	236, 820, 822, 829, 990		SI		
02	SI	990	236, 820, 822, 829, 990		SI	-	-
03	SI	990	236, 820, 822, 829, 990		SI	-	-
04	NO	830	830		SI	-	-
05	NO	830	830		SI	-	-
06	NO	830	830		SI	-	-
07	NO	830	830		SI	-	-
08	NO	46	46		SI	-	-
09	NO	46	46		SI	-	-

Figura 7.5 Puertos del switch configurados en la VLAN 830

Pero como se quiere tener acceso a la red de la UPV también se debe conectar una interface de red del servidor VPN de la UPV a un puerto de un switch que este configurado en la VLAN 830 (10.228.154.228)

7.4.2. Conexión al servidor VPN

Aunque en el punto anterior se ha visto como nuestro nodo Guifi está integrado a nivel 1 y 2 (físico y enlace de datos) en la red de la universidad a nivel 3 (de red) la red Guifi.net es una red "externa" a la red de la UPV.

Es por esto que para poder acceder a la red de la UPV es necesario crear el túnel ya que los nodos de la red Guifi disponen, en dicha red de direcciones privadas (10.X.X.X) y, el servidor de VPN, después de autenticarse, hace que adquieran las direcciones publicas 158.42.X.X con las que pueden "navegar" por la red de la UPV.

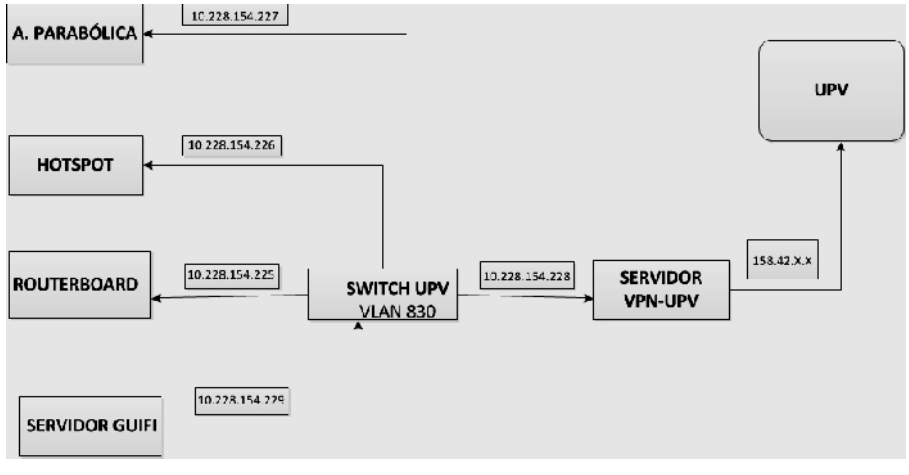


Figura 7.6 Esquema de los elementos conectados a la VLAN 830

El servidor de túneles, a nivel físico, tiene tres interfaces: uno en la red privada (parte interior de nuestra red de la UPV con IPs públicas), una pública (la que está en el "exterior", con IP pública del mismo rango que la anterior pero en una VLAN externa al cortafuegos) y una tercera privada que corresponde a la subred de Guifi.net. Estas conexiones se llevan mediante latiguillos a los switches

que tienen configuradas las VLANs correspondientes para la adecuada comunicación con el resto de la red. En la siguiente imagen vemos la configuración del interfaz correspondiente a Guifi.net y la parte de conexiones del terminador de túneles (Cisco VPN 3030) con sus tres interfaces Ethernet.

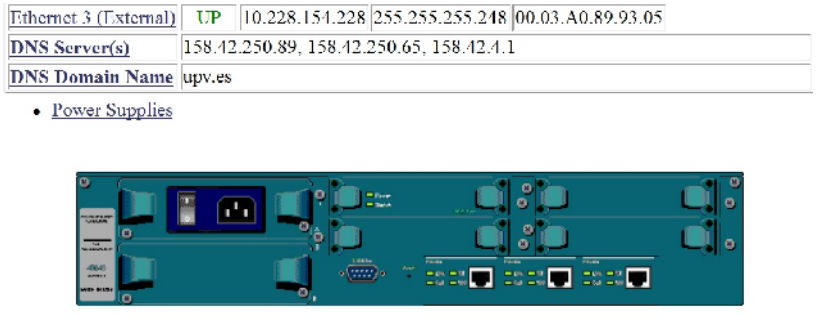


Figura 7.7 Nuestro túnel en el servidor de VPN de la UPV

Un diagrama, aproximado, de las conexiones entre la UPV y el "mundo exterior" sería:

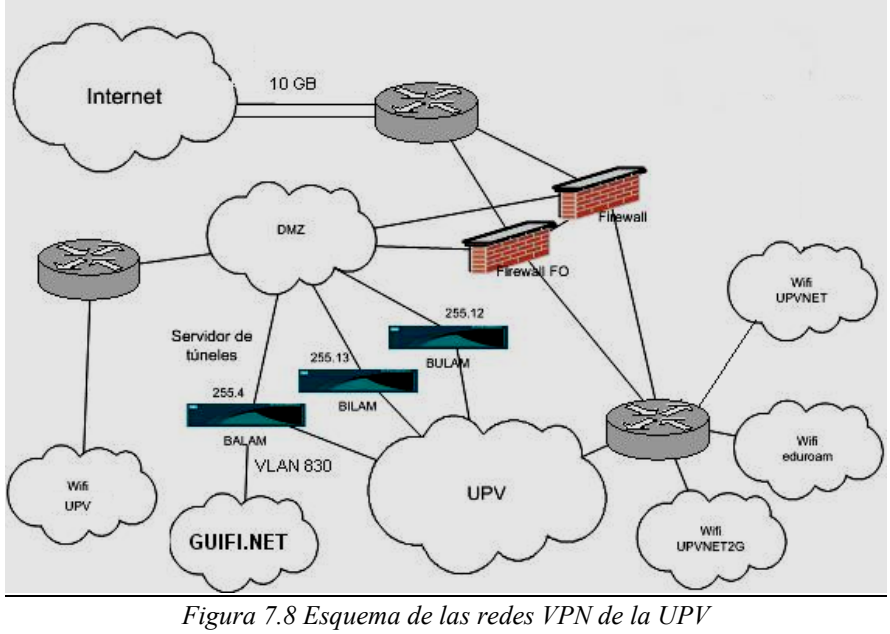


Figura 7.8 Esquema de las redes VPN de la UPV

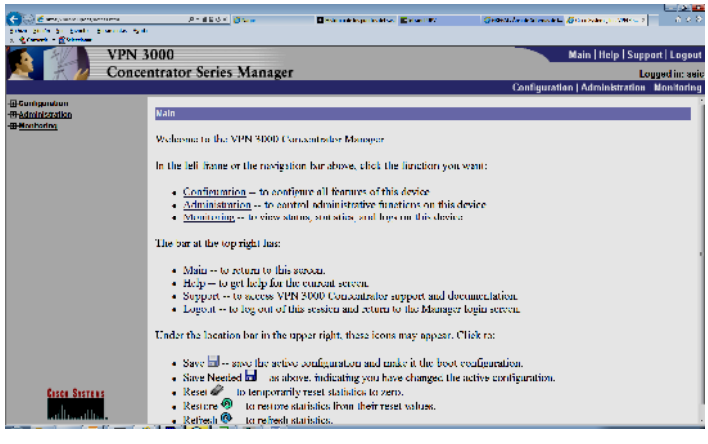
7.4.3. Configuración del servidor VPN

Una vez realizadas las conexiones necesarias para crear un túnel que conecte los nodos cliente de la red Guifi.net con la red de la UPV hay que configurar el servidor de VPN de la UPV.

Para ello, accedemos vía web al servidor VPN con su aplicación de configuración VPN3000

Figura 7.9 Web de configuración de VPN

Una vez autenticado se accede al panel



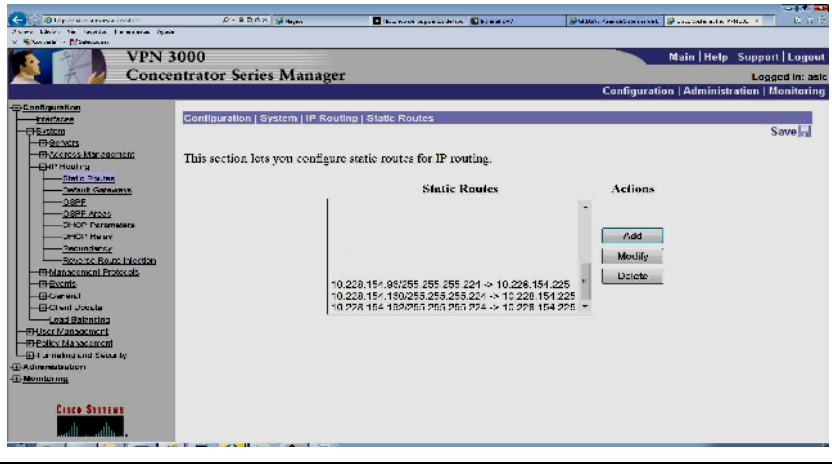
Y al desplegar el menú de *Configuración*, tenemos las pestañas *System, IP routing y Static Routes*

En Static Routes se dan de alta de forma estática las rutas de las subredes que corresponden a cada radio del nodo y que todas deben tener por Gateway el puerto LAN del router Mikrotik.

10.228.154.96 / 255.255.255.224 -→ 10.228.154.225

10.228.154.160 / 255.255.255.224 -→ 10.228.154.225

10.228.154.192 / 255.255.255.224 -→ 10.228.154.225



Y por último se configura la tercera interface del servidor VPN (Balam) dándole la IP que le corresponde de la red Guifi.net (10.228.154.228), la máscara. Nombre, etc.

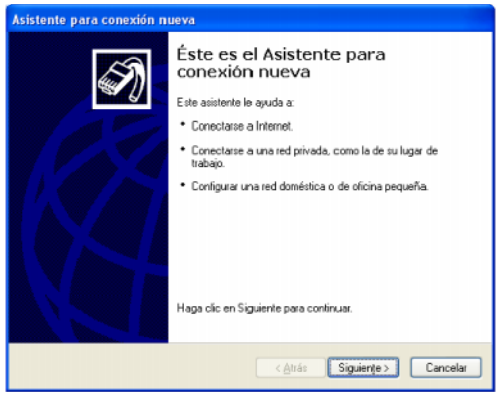
7.4.4. Configuración del cliente VPN

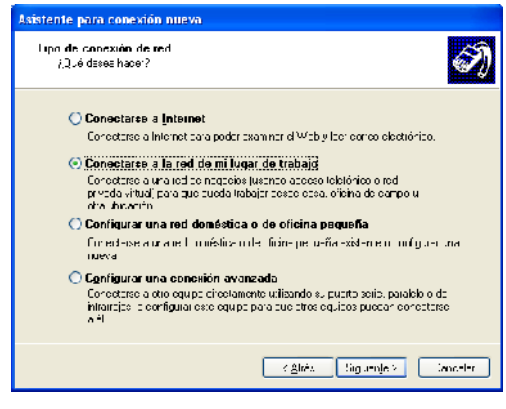
Realizamos, desde nuestro equipo nodo cliente de guifi.net con el equipo Probanano que dispone de Windows XP, la conexión por VPN a la red de la universidad.

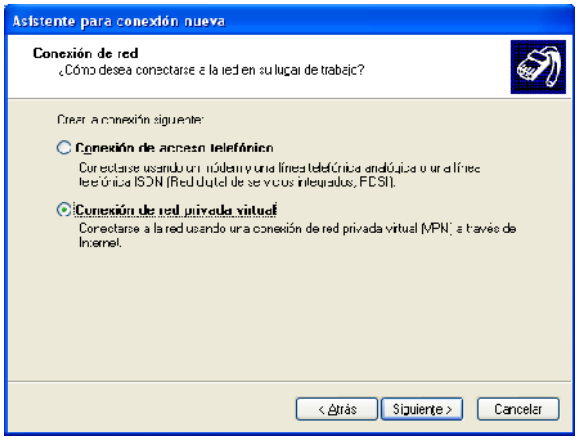
El equipo conectado a la red de Guifi.net tiene una dirección IP 10.228.154.162 y no dispone de acceso a Internet.

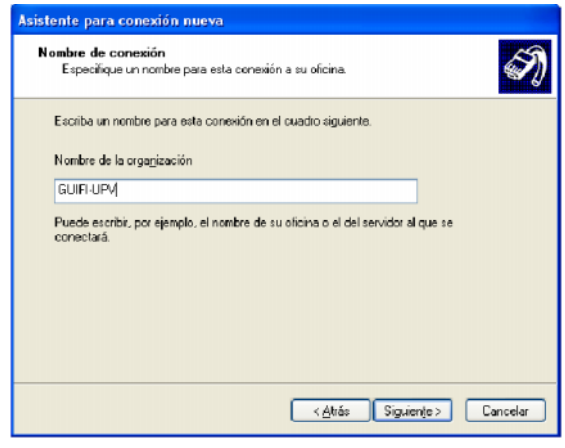
Los pasos para configurar una conexión VPN con la UPV son:

Pulsamos sobre Inicio → Configuración → Panel de Control → Conexiones de red → "Crear una conexión nueva" lo que nos abrirá un asistente, pulsamos siguiente y en la siguiente pantalla marcamos en "Conectarse a la red de mi lugar de trabajo". Siguiente

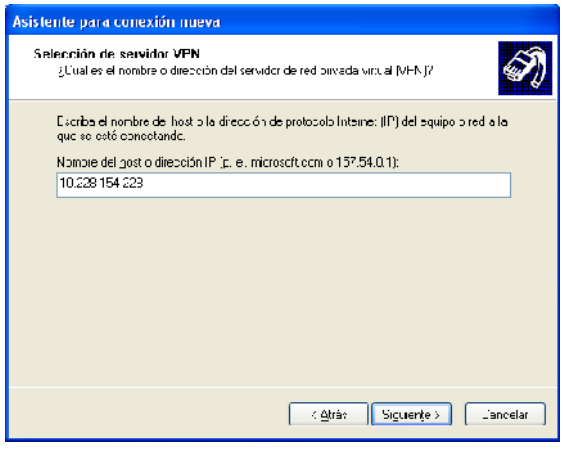


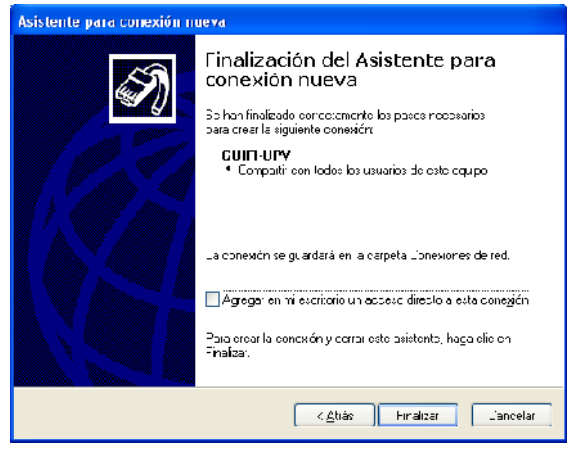




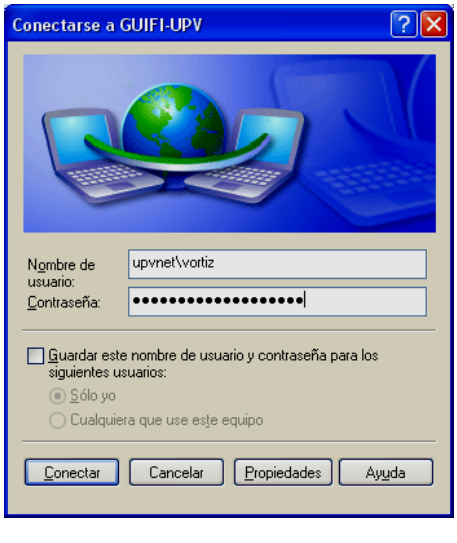


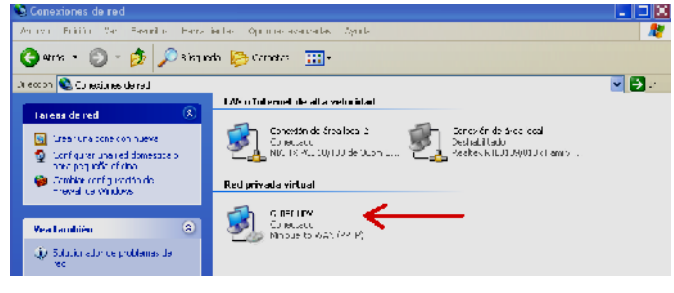
Seleccionamos "Conexión de red privada virtual" y le ponemos el nombre Guifi-UPV. Siguiente. Le ponemos la dirección IP, de nuestra red, del servidor VPN al que nos queremos conectar "10.228.154.228" (al tener el servidor DNS, también le podíamos haber puesto el nombre VLCupvvpn.guifi.net) y finaliza el asistente.





Para conectarnos a la UPV por la VPN accedemos a Inicio → Configuración → Conexiones de red y pulsamos en GUIFI-UPV (para posteriores conexiones hacemos un acceso directo en el escritorio)

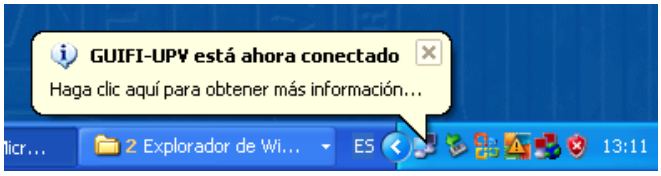




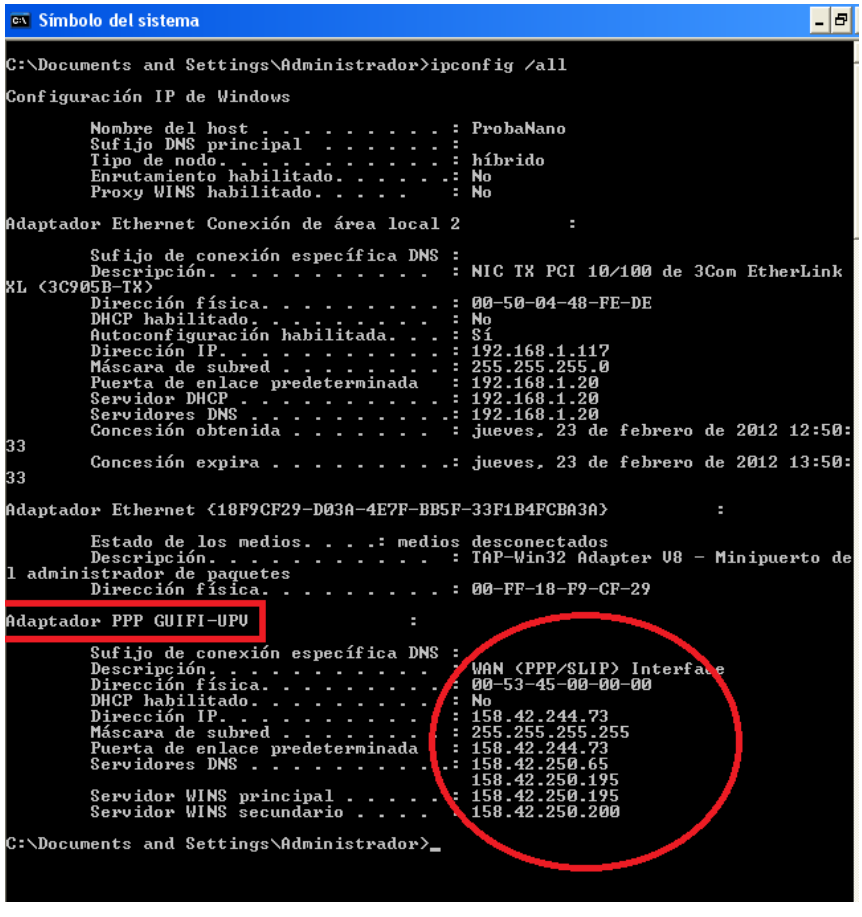
Nos pide los datos para autenticarnos (pulsando en propiedades se puede configurar la conexión respecto al TCP/IP, seguridad, etc)

Y como tenemos un usuario autenticado en el dominio

UPVNET (vale cualquier dominio de la UPV que permita validar) nos permite realizar la conexión.



Cuando estamos conectados a la red de la UPV nuestro equipo tiene una dirección IP, Gateway, servidores DNS, etc… de esa red, lo que comprobamos ejecutando desde la línea de comandos la orden "ipconfig /all,



CAPÍTULO 8:

ESTUDIO DE PRESTACIONES

8.1. Objetivos.

Una vez que hemos montado nuestro supernodo, que tenemos nodos clientes conectados a él y que gracias, en este momento a la creación de un túnel entre la UJI y nuestro servidor del supernodo estamos conectados a guifi.net (Castellón), lo último que queda para finalizar este proyecto es realizar un estudio de prestaciones de esta red, que incluya un test de velocidad que nos ayude a saber la calidad de la conexión y como está rindiendo la red en unas condiciones determinadas.

El objetivo que se persigue con este estudio es, al calcular el ancho de banda de la red en distintos escenarios, poder comparar y evaluar el Throughput que nos proporciona la red Guifi.net, con direccionamiento IP privado, respecto al que se tiene desde el mismo cliente inalambrico con conexión VPN a la red de la UPV y respecto a un equipo, con dirección IP pública, conectado directamente a Internet.

Ante la imposibilidad de realizar la conexión a la red Guifi.net de forma completanete inalámbrica, con nuestra antena parabólica Rocket M5, al no existir ningún otro supernodo dentro de nuestro alcance que hiciera posible acceder al servidor de la red Guifi en la UJI de Castellón, la conexión se realiza en forma inalámbrica entre el cliente y el radio sur del router y desde éste a nuestro servidor por cable y hasta el servidor de Castellón por medio de un túnel (red privada virtual VPN), también por cable, como vimos en el capítulo anterior.

```
C:\Documents and Settings\Administrador>tracert 10.228.130.162

Traza a la dirección castellon.guifi.net [10.228.130.162]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.1.20
  2     1 ms     1 ms     1 ms  vlcupvap0-180.guifi.net [10.228.154.161]
  3     1 ms     1 ms     1 ms  vlcupvgrc.guifi.net [10.228.154.229]
  4     4 ms    11 ms     5 ms  castellon.guifi.net [10.228.130.162]

Traza completa.
```

Por tanto, para realizar el análisis experimental se van a realizar pruebas con 3 escenarios distintos:

- El primero va a consistir en conectar el equipo cliente al servidor de Castellón.guifi.net por la red privada Guifi.net.

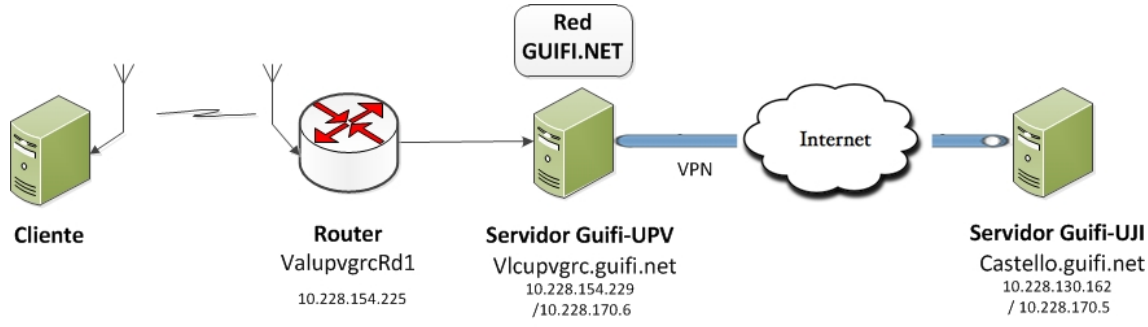


Figura 8.1. Esquema del trayecto por la red Guifi.net

- El segundo consistirá en realizar la conexión por VPN a la red de la UPV y así obtener una IP global con la que acceder al servidor de Castellón desde la red pública.

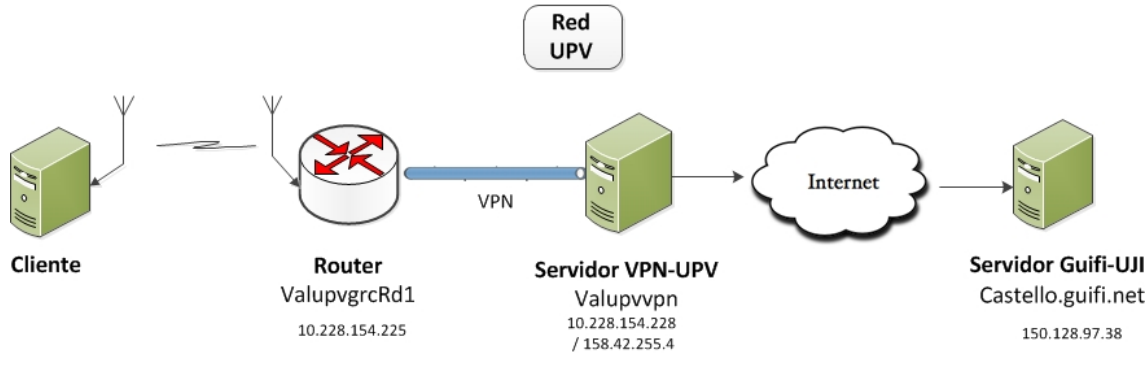


Figura 8.2. Esquema del trayecto por la red UPV

- El tercer escenario consistirá en conectarse al mismo servidor de Castellón desde un equipo con una IP pública de la red UPV con acceso directo a Internet por Rediris

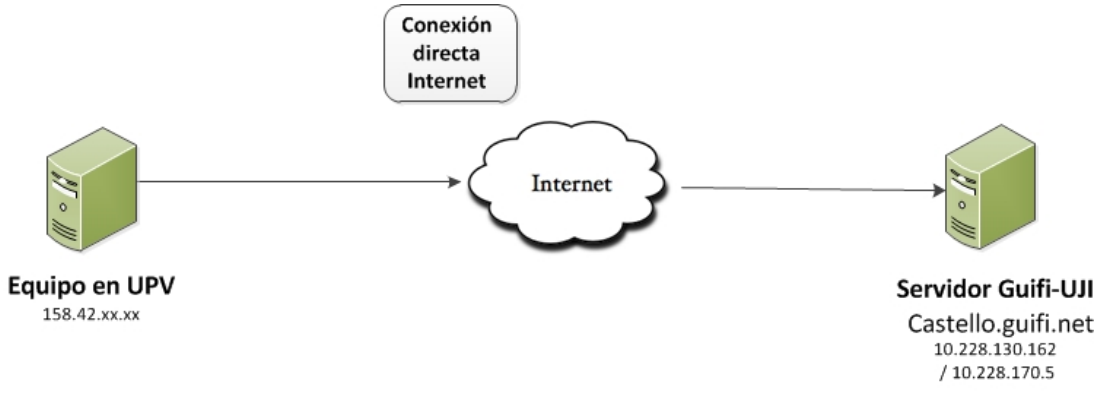


Figura 8.3. Esquema del trayecto directo a Internet

Las pruebas se realizan utilizando 2 herramientas nos permiten conocer el ancho de banda de la red. La mayor parte del análisis se ejecuta con **Jperf** generando tráfico desde el cliente hacia el servidor acorde con una configuración de parámetros tales como: tipo de paquete, tamaño del paquete y número de estaciones a simular desde el nodo terminal y cuyo funcionamiento e instalación se explica posteriormente

La segunda herramienta utilizada será **Wget** con la que, en cada uno de los escenarios indicados, se realizarán varias pruebas de descarga de un archivo de la web de guifi.net de Castellón.

Finalmente, con los resultados obtenidos, se procederá a realizar un análisis comparativo del throughput ofrecido por cada red y determinar que repercusión tiene la instalación Guifi.net de la UPV en el throughput.

8.2. Metodología.

8.2.1. Parámetros a analizar.

Todos los parámetros que analizan el comportamiento de la red miden la fiabilidad, disponibilidad y velocidad del sistema.

La fiabilidad se puede medir en tiempo medio de retardo, y la disponibilidad en el número de horas al año que no está disponible debido a un fallo.

La velocidad de la red depende directamente de la calidad del enlace y de la cantidad de saltos que tiene que hacer hasta llegar al destino. Esto quiere decir que si se está conectado con un enlace muy bueno y rápido la velocidad que permitirá ese enlace será la velocidad que se pueda alcanzar dentro de la red, pero si para llegar al destino hay que pasar por otros enlaces de peor calidad la velocidad se verá reducida al pasar por dichos enlaces. También se debe tener en cuenta que la red troncal y los puntos de acceso para clientes son compartidos por otros muchos usuarios y no siempre se puede disponer del total de la capacidad de los enlaces.

El rendimiento es sin duda uno de los aspectos de mayor interés dentro del análisis global en las redes debido al efecto que éste produce sobre el usuario final. El rendimiento puede ser definido según diversos puntos de vista permitiendo con ello incorporar otras formas de evaluación dependiendo del objeto de interés en particular. Básicamente, el parámetro más común para evaluar el rendimiento de una red es el Throughput, es decir, la capacidad de un enlace de transportar información útil. Representa a la cantidad de información útil que puede transmitirse por unidad de tiempo. Este puede variar en una misma conexión de red dependiendo del protocolo usado para la transmisión (TCP o UDP) y el tipo de datos de tráfico (HTTP, FTP, etc.).

Lo primero que hay que tener claro es la diferencia entre la tasa de transferencia del enlace (habitualmente denominada "data rate") y la tasa de transferencia efectiva (denominada "throughtput).

- El *data rate* se refiere a la capacidad absoluta de un enlace y es función directa de la manera en que modula y codifica la portadora sobre ese enlace. Habitualmente suele medirse en bits/segundo (Mbps, Gbps, etc.).

El data rate establece un límite absoluto para la transmisión: no pudiendo transmitir mayor cantidad de datos que la definida en el data rate.

- El *througput* en cambio, es la capacidad efectiva de transferencia de datos sobre el enlace. Esta capacidad siempre es menor al data rate ya que en los enlaces, junto con los datos, hay tráfico de negociación, mantenimiento y control del enlace. Esto en sistemas TCP/IP además depende del protocolo de capa de transporte que utiliza la aplicación, que puede ser TCP o UDP.

Normalmente suele medirse el throughput en Bytes/segundo (KBps, MBps).

Otros parámetros que se pueden analizar son el retardo, la variación de retardo (jitter) y la pérdida de paquetes.

- El *retardo o latencia* es la cantidad de tiempo requerida para transmitir y recibir una señal, es decir, es el tiempo transcurrido entre un evento y el instante en el que el sitio remoto lo escucha u observa.

- La *variación del retardo o Jitter* es la variación aleatoria de la latencia, cuyo origen puede estar en el equipo terminal, en el tráfico que temporalmente reduce las capacidades de la red a lo largo de toda la ruta, o con cambios en el camino que siguen los paquetes (saltando de un router a otro)

En consecuencia, el *Jitter* incrementa la latencia y sus efectos.

- La pérdida de paquetes significa que los paquetes de datos no llegan a su destino. El problema puede tener su origen en el ancho de banda o en errores de transmisión.

La variación del retardo en la red (Jitter) puede causar perdida de paquetes.

Lo que generalmente interesa es la medición de *throughput* y para esto lo que se necesita es generar tráfico sobre el enlace para medir efectivamente cuál es su capacidad.

En la actualidad existen diferentes herramientas software que permiten realizar mediciones sobre una red y analizar el tráfico que van desde productos propietarios que incluyen hardware y software, hasta soluciones gratuitas y de código abierto.

8.2.2. Herramientas.

La mayoría de herramientas operan mediante configuraciones cliente/servidor, enviando paquetes de un host a otro, generando situaciones de tráfico controladas y aleatorias, permitiendo variar el tipo de protocolo de transmisión, TCP o UDP, el tamaño del paquete, y en algunas ocasiones la tasa de transferencia.

Los métodos empleados para las mediciones se caracterizan por hacer evaluaciones de la conexión entre hosts enviando algún patrón de tráfico para luego realizar su evaluación; obviamente dichas mediciones, se repiten varias veces y luego se promedian para mejorar su aproximación.

Teniendo en cuenta las características y su uso constante en situaciones que requieren evaluar el rendimiento de una red vamos a utilizar la aplicación cliente/servidor "Iperf/Jperf" que se encarga de testear el canal de comunicaciones para la medición de Throughput.

8.2.2.1. Iperf

Iperf es una herramienta de libre distribución, capaz de medir el ancho de banda, el retardo, el Jitter e incluso la pérdida de paquetes de un enlace entre dos PCs.

Como hemos indicado, Iperf trabaja bajo el modelo de cliente-servidor, donde el PC cliente inventa cualquier tipo de información y se la manda al otro PC que actúa como servidor durante un tiempo determinado, para ello es necesario que el cliente sepa la dirección IP del PC servidor. Básicamente el cliente es el que envía la información y el servidor es el que registra los datos que obtiene cuando le llegan los paquetes y los muestra.

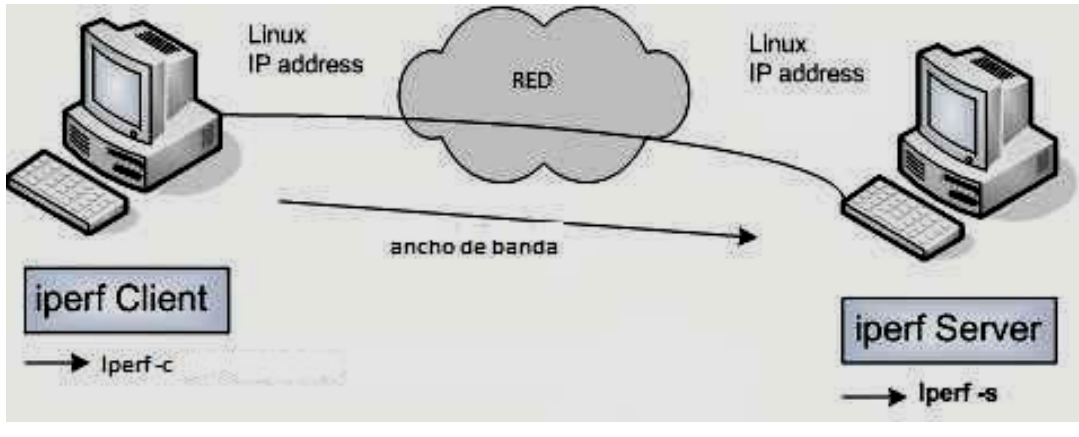


Figura 8.4. . Esquema conexión Iperf cliente-servidor.

Sus principales característica recaen en la facilidad con la que permite configurar sus diferentes parámetros, y en la capacidad de poder enviar datos que usan tanto el protocolo TCP, como el protocolo UDP.

La manera más fácil de hacer uso de Iperf es utilizándolo en modo cliente en línea de comandos.

```
guifi@VLCupvGRC:~$ sudo iperf -c 10.228.130.162 -i 1
------------------------------------------------------------
Client connecting to 10.228.130.162, TCP port 5001
TCP window size: 1.87 MByte (default)
------------------------------------------------------------
[  3] local 10.228.130.162 port 40470 connected with 10.228.130.162 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec  50.5 MBytes  424 Mbits/sec
[  3]  1.0- 2.0 sec  46.2 MBytes  388 Mbits/sec
[  3]  2.0- 3.0 sec  49.2 MBytes  413 Mbits/sec
[  3]  3.0- 4.0 sec  56.7 MBytes  476 Mbits/sec
[  3]  4.0- 5.0 sec  58.0 MBytes  486 Mbits/sec
```

Si se quiere ver de manera más gráfica los resultados de Iperf, se debe utilizar una aplicación creada explícitamente para ello, se llama Jperf.

8.2.2.2. Jperf

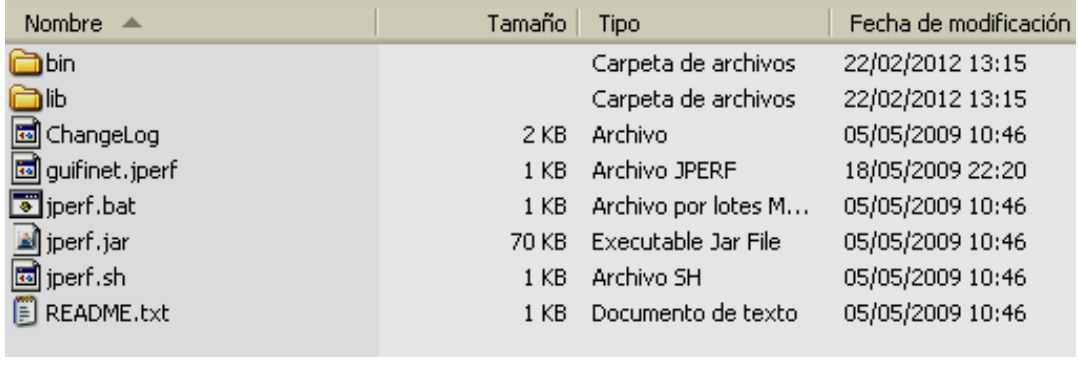
Como acabamos de indicar, JPerf es una GUI para IPerf, es decir, Jperf es una interface gráfica para Iperf. Al estar basado en Java, será necesario tener instalado el VM de Java.

La filosofía de uso es la misma que Iperf. Al tratarse de una herramienta *cliente-servidor*, se debe ejecutar Jperf en dos máquinas, una hará de Servidor y otra de Cliente. Tanto en una como en otra se puede ejecutar indistintamente Jperf o Iperf. En nuestro caso como ya tenemos funcionando un servidor iperf solo habrá que ejecutar jperf como cliente y herramienta de análisis.

- Instalación

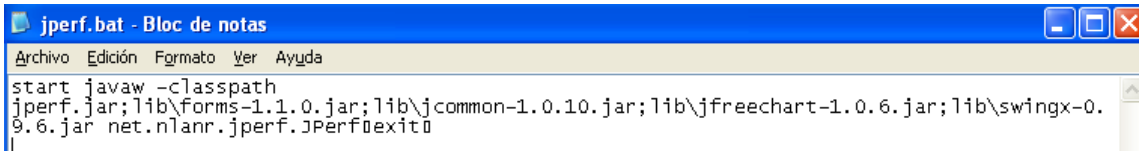
La última versión de Jperf es la 2.0.2 Se puede descargar de distintos repositorios y páginas web como la página oficial del proyecto Jperf http://code.google.com/p/xjperf/. Nosotros la descargamos directamente desde la página web de Guifi-Castellón http://castello.guifi.net/sites/default/files/jperf-2.0.2.zip.

Una vez descargado el paquete de instalación se descomprime el archivo.zip.



Nombre	Tamaño	Tipo	Fecha de modificación
bin		Carpeta de archivos	22/02/2012 13:15
lib		Carpeta de archivos	22/02/2012 13:15
ChangeLog	2 KB	Archivo	05/05/2009 10:46
guifinet.jperf	1 KB	Archivo JPERF	18/05/2009 22:20
jperf.bat	1 KB	Archivo por lotes M...	05/05/2009 10:46
jperf.jar	70 KB	Executable Jar File	05/05/2009 10:46
jperf.sh	1 KB	Archivo SH	05/05/2009 10:46
README.txt	1 KB	Documento de texto	05/05/2009 10:46

.Como nuestro sistema operativo es un Windows XP, ejecutamos, haciendo clic con el botón derecho del ratón y pulsando Ejecutar, el archivo jperf.bat



- Interface gráfica

Y nos aparecerá la interfaz java de Jperf, que se organiza en los siguientes campos u opciones importantes:

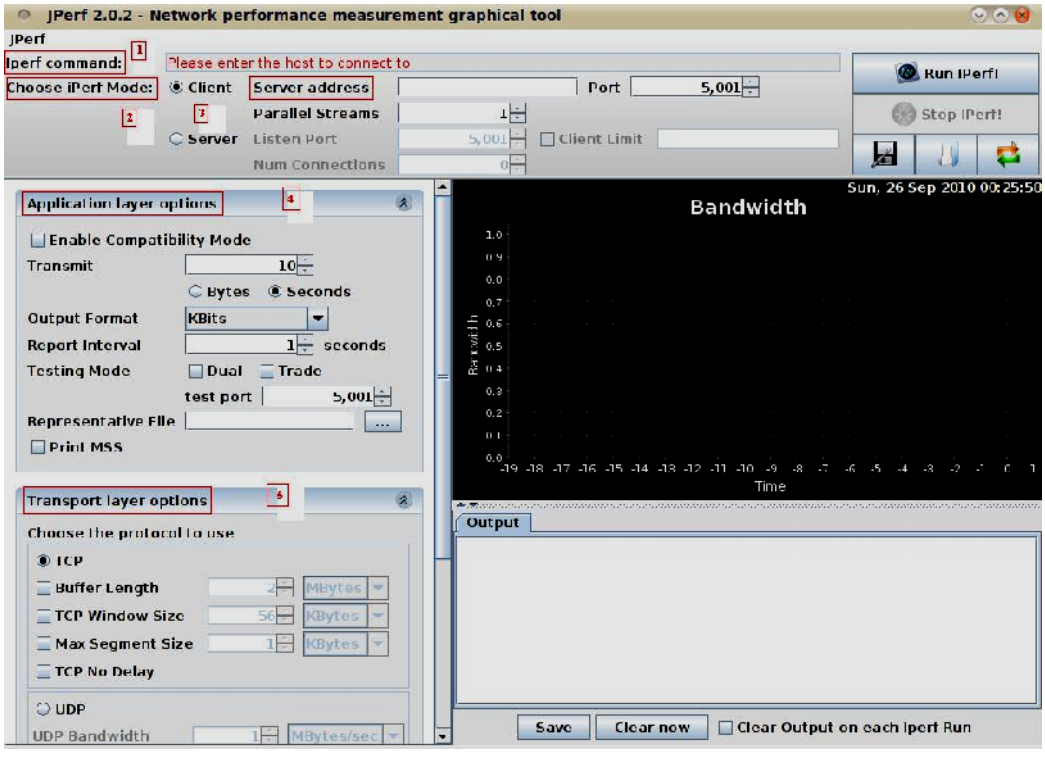


Figura 8.5. Elementos de la pantalla de Jperf.

1. **iperf command**: se rellenará automáticamente al introducir la **IP** del host remoto en el campo *server address*

2. **Server address** *(dirección del host remoto)*. Aquí se introduce la IP del host remoto. Automáticamente se rellenará el campo *iperf command* con unas opciones por defecto que irán cambiando a medida que se rellenen los cuadros *Aplication layer options y Transport layer options*.

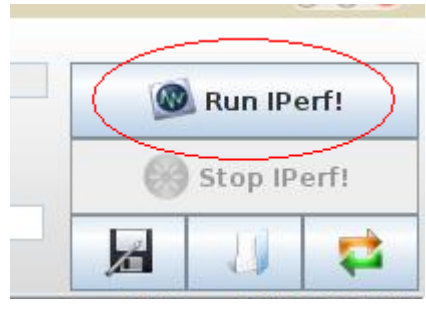
3. **Choose iPerf Mode**: Se indica si se está usando jperf en modo cliente o servidor. En este análisis se usará siempre como cliente.

4. **Application layer options.** Aquí hay que destacar las opciones para *cantidad de transmisión* en Bytes o segundos de muestreo, el *Formato de Salida*, el *valor de intervalos de tiempo* y el *puerto* al que se dirigirá y en el que escucha el host remoto (por defecto 5001).

5. **Transport layer options.** Aquí se indicará el protocolo TCP o UDP. Se podrán ajustar valores como el *Tamaño de la ventana*, *Longitud de buffer* y el *MSS* (Maximum Segment Size) o cantidad de datos enviados en cada paquete, para encontrar los valores óptimos para el mejor rendimiento de la red.

- Ejecutar Jperf

Una vez que ya están introducidos todos los valores deseados en los campos correspondientes, solo es necesario pulsar el botón **Run Iperf.**



8.2.3. Procedimiento

Para realizar el estudio de prestaciones aprovechamos el servidor Iperf que ofrece Guifi-Castellón en su servidor (10.228.130.162) y que permanece continuamente activo a la espera que el cliente realice una petición.

Como se ha indicado para el análisis se utiliza la herramienta Iperf que aunque puede realizar mediciones de throughput, retardo (delay), jitter (variación del retardo) y pérdidas de datagramas, permitiendo para ello manipular diversos parámetros del tráfico generado, desde el cliente, solo se puede analizar el throughput, que es lo que estudiamos, al no tener acceso al servidor.

Con el objetivo de realizar mediciones suficientes para cada una de las configuraciones requeridas se han considerado un total de 10 tomas de muestras realizadas en distintos días unas por la mañana y las otras por la tarde, prestableciéndose, de las 2 variables utilizadas, una con valor fijo y la otra variable en cada uno de los casos.

El procedimiento consistirá en enviar un número determinado de tramas en un tiempo específico o un tamaño de bytes fijo. En el caso transmisión durante un tiempo fijo cada una de las ráfagas enviadas dura 10 segundos y si es por tamaño de transmisión fijo éste será de 20.000.000 bytes. Las transmisiones se realizan utilizando datagramas bajo el protocolo UDP y en todas el cliente será el encargado de enviar los paquetes de datos.

Se elige usar el **protocolo UDP** en las pruebas de Throughput debido a que no implementa ventanas que otorgan control de flujo a la transmisión de bytes, de forma que no se limita el ancho de banda de la red que está disponible. Además, UDP tampoco realiza retransmisiones de bytes, ya que no espera un reconocimiento afirmativo (ACK) por parte del receptor de cada byte que envía, para

enviar el siguiente. El tamaño de los datagramas UDP considera que cada datagrama involucrado en la prueba se encapsula en un sólo paquete IP, de modo que se pueden obtener resultados en paquete por segundo (pps).

Por otro lado, para el análisis no se puede utilizar un iperf unidireccional ya que, en este caso, se deberían de mirar los resultados que reporta el servidor, ya que quien inyecta tráfico a la red (el cliente en nuestro caso) no es capaz de conocer con tanta exactitud lo que ha llegado con éxito al otro extremo y como ya se ha indicado no se puede acceder a los resultados en el servidor.

Por lo tanto se utilizará el **iperf dual** y así al mirar los resultados que nos da el cliente se conocerá el throughput real en el enlace servidor->cliente.

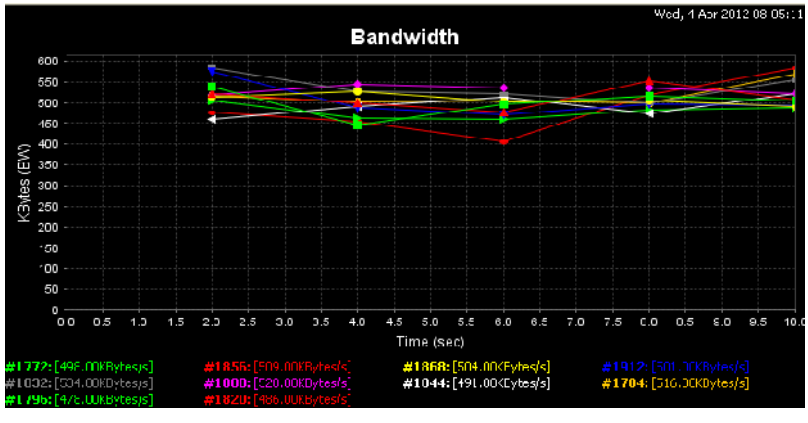
Respecto a las variables, en el análisis se consideran fundamentalmente dos, aunque para ampliar las conclusiones se considerará algún otro parámetro, el **tamaño del paquete** y **número de streams** en la red (conexiones virtuales).

El utilizar como una de las variables el tamaño de paquetes que cruzarán la red es porque teóricamente el throughput deberá ser completamente dependiente de éste tamaño y se deberá demostrar que a tamaños de paquete menores, más overheading y por tanto menos throughput, y a tamaños superiores mayor posibilidad de jitter superior.

Para la variable del número de streams aprovechamos una de las principales ventajas que ofrece IPERF, como es el hecho de permitir desde una misma estación cliente emular "n" terminales o nodos clientes, generando el tráfico correspondiente acorde con los parámetros establecidos para UDP a través de diferentes puertos, presentándonos el comportamiento del canal en relación al ancho de banda.

Los valores establecidos para cada una de las variables son:

- Tamaño del Paquete: 64, 128, 256, 512, 1024, 1470 (longitudes de tramas recomendadas en la RFC 2544)
- Número de PCs activos en la red: 1, 2, 4, 6, 8, 10



Un ejemplo gráfico que nos proporciona Jperf para una transmisión con 10 nodos simunltaneos y un tamaño de paquete fijo de 64 Bytes es:

Figura 8.6. Ejemplo gráfico de resultado de Jperf.

8.2.4. Acciones iniciales

Al descomprimir el archivo jperf-2.0.2.zip que se había descargado directamente desde la página web de Guifi-Castellón, encontramos el archivo "*guifinet.jperf*" con la configuración básica necesaria para iniciar el testeo, es decir, dirección IP del servidor, segundos de monitorización, medida de los resultados, etc. Esta configuración es sencilla y basándonos en ella se crean 2 archivos con una configuración más especifica para los testeos que se van a realizar.

El primero, "*CastellonGuifi.jperf*", tendrá la configuración para ejecutar en las pruebas en la red privada Guifi.net y el segundo "*CastellonUPV.jperf*" se utiliza cuando se realizan las pruebas en la red pública de la UPV.

El contenido de los archivos es el siguiente:

CastellonGuifi.jperf

```
#Thu Apr 19 08:45:52 CEST 2012
print-mss-enabled=false
transmit-unit=seconds
tcp-mss-enabled=false
tos=NONE
mode=client
client-limit-enabled=false
compatibility-mode-enabled=false
tcp-no-delay-enabled=false
test-mode-port=5001
test-mode-trade-enabled=false
udp-bandwidth-unit=MEGABYTES_PERSEC
output-format=KBYTES
udp-bandwidth=40.0
tcp-buffer-length-unit=MBYTES
listen-port=5001
server-port=5001
clientside-parallel-streams=0
udp-buffer-size-unit=KBYTES
tcp-window-size-enabled=false
server-address=10.228.130.162
ttl=1
udp-buffer-size-enabled=false
transmit-value=10
ipv6-enabled=false
udp-buffer-size=41.0
transport-protocol=udp
test-mode-dual-enabled=true
tcp-buffer-length-enabled=false
tcp-buffer-length=2.0
tcp-mss-unit=KBYTES
report-interval=2
udp-packet-size-enabled=true
udp-packet-size=64.0
tcp-mss=1.0
serverside-parallel-streams=1
client-limit=
tcp-window-size-unit=KBYTES
tcp-window-size=56.0
udp-packet-size-unit=BYTES
bind-to-host=
```

CastellonUPV.jperf

```
#Thu Apr 19 08:18:46 CEST 2012
print-mss-enabled=false
transmit-unit=seconds
tcp-mss-enabled=false
tos=NONE
mode=client
client-limit-enabled=false
compatibility-mode-enabled=false
tcp-no-delay-enabled=false
test-mode-port=5001
test-mode-trade-enabled=false
udp-bandwidth-unit=MEGABYTES_PERSEC
output-format=KBYTES
udp-bandwidth=40.0
tcp-buffer-length-unit=MBYTES
listen-port=5001
server-port=5001
clientside-parallel-streams=0
udp-buffer-size-unit=KBYTES
tcp-window-size-enabled=false
server-address=150.128.97.38
ttl=1
udp-buffer-size-enabled=false
transmit-value=10
ipv6-enabled=false
udp-buffer-size=41.0
transport-protocol=udp
test-mode-dual-enabled=true
tcp-buffer-length-enabled=false
tcp-buffer-length=2.0
tcp-mss-unit=KBYTES
report-interval=2
udp-packet-size-enabled=true
udp-packet-size=64.0
tcp-mss=1.0
serverside-parallel-streams=1
client-limit=
tcp-window-size-unit=KBYTES
tcp-window-size=56.0
udp-packet-size-unit=BYTES
bind-to-host=
```

Como se puede comprobar, para que los resultados de las pruebas puedan ser comparados, los parámetros de los dos archivos son iguales excepto el que indica la dirección IP de cada una de las redes (**server-address**), 10.228.130.162 para la Guifi.net y 150.128.97.38 para la red de Internet del servidor.

Las variables que irán variando para la realización de las distintas pruebas, como se ha indicado, son **upd-packet-size** (entre 64 y 1470 bytes) y **serverside-parallel-streams** (entre 1 y 10).

Además, las pruebas se realizarán, por un lado, con ráfagas de un tiempo fijo de duración y por otro con una cantidad fija de bytes a transmitir, por lo que para cada uno hay que modificar 2 parametros: **transmit-unit** (seconds y bytes en cada caso) y **transmit-value** (10 y 20000000 respectivamente).

8.3. Resultados de las pruebas con Jperf

8.3.1. Sobre la red Guifinet

8.3.1.1. Prueba A (por tiempo):

Las mediciones se realizan por la mañana, utilizando transmisión UTP dual, con mediciones durante un tiempo de 10 segundos en intervalos de 2 segundos.

Partiendo de estas opciones se irán haciendo mediciones variando en cada caso una de las variable manteniendo la otra fija. Como se ha indicado los tamaños utilizados para la generación de Datagramas son: 64, 128, 256, 512, 1.024, 1470 bytes y .el número de nodos clientes son 1, 2, 4, 8 y 10.

```
bin/iperf.exe -c 10.228.130.162 -u -P 2 -i 2 -p 5001 -l 64.0B -f K -b 40.0M -t 10 -d -L 5001 -T 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 64 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
Client connecting to 10.228.130.162, UDP port 5001
Sending 64 byte datagrams
UDP buffer size: 8.00 KByte (default)

[1868] local 192.168.1.117 port 2191 connected with 10.228.130.162 port 5001
[1848] local 192.168.1.117 port 2192 connected with 10.228.130.162 port 5001
[ ID] Interval       Transfer     Bandwidth
[1868]  0.0- 2.0 sec  5131 KBytes  2566 KBytes/sec
[1848]  0.0- 2.0 sec  4520 KBytes  2260 KBytes/sec
[SUM]  0.0- 2.0 sec  9651 KBytes  4826 KBytes/sec
[1848]  2.0- 4.0 sec  4360 KBytes  2180 KBytes/sec
[1868]  2.0- 4.0 sec  5050 KBytes  2525 KBytes/sec
[SUM]  2.0- 4.0 sec  9409 KBytes  4705 KBytes/sec
[1868]  4.0- 6.0 sec  5050 KBytes  2525 KBytes/sec
[1848]  4.0- 6.0 sec  4123 KBytes  2062 KBytes/sec
[SUM]  4.0- 6.0 sec  9173 KBytes  4586 KBytes/sec
[1868]  6.0- 8.0 sec  5098 KBytes  2549 KBytes/sec
[1848]  6.0- 8.0 sec  4099 KBytes  2050 KBytes/sec
[SUM]  6.0- 8.0 sec  9197 KBytes  4599 KBytes/sec
[1848]  8.0-10.0 sec  4080 KBytes  2040 KBytes/sec
[1868]  8.0 10.0 sec  5002 KBytes  2501 KBytes/sec
[SUM]  8.0-10.0 sec  9082 KBytes  4541 KBytes/sec
[1848]  0.0-10.0 sec  21182 KBytes  2115 KBytes/sec
[1868]  0.0-10.0 sec  25330 KBytes  2529 KBytes/sec
[1848] Sent 338918 datagrams
[1868] Sent 405276 datagrams
[SUM]  0.0-10.0 sec  46512 KBytes  4644 KBytes/sec
```

Cada uno ensayos realizados nos dará como resultado un conjunto de datos como los que se indican arriba, que variará según el valor de P, es decir, el número de transmisiones en paralelo, pero que en cualquier caso nos presentan 3 valores correspondientes a las columnas Interval – Transfer – Bandwidth, que indican tiempo (sec), cantidad de información transferida (KBytes) y ancho de banda efectivo (KBytes/sec) respectivamente.

Con los resultados promedio de Transfer y Bandwidth de cada una de las muestras realizadas en cada prueba, a nivel de nodo individual y de la suma de todos los nodos implicados se construyen las tablas y las gráficas correspondientes que posteriormente permitirán analizar los resultados.

- BANDWIDTH (Kbytes/sec) para un solo nodo

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	2559	2500	4414	4879	4869	4860
	2	2529	2087	2440	3155	4774	4606
	4	1234	1552	1658	1887	2071	2080
	6	841	1174	1291	1316	1397	1381
	8	611	863	1051	1087	1109	1013
	10	462	705	840	921	940	837

Tabla 8.1. Bandwidth para un solo nodo

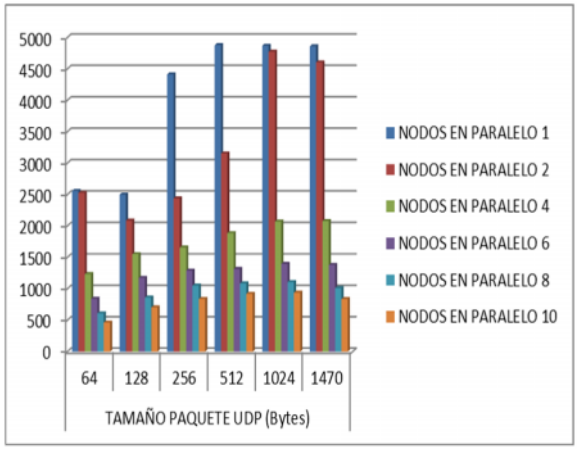


Figura 8.7. Bandwidth un solo nodo por tamaño de paquete

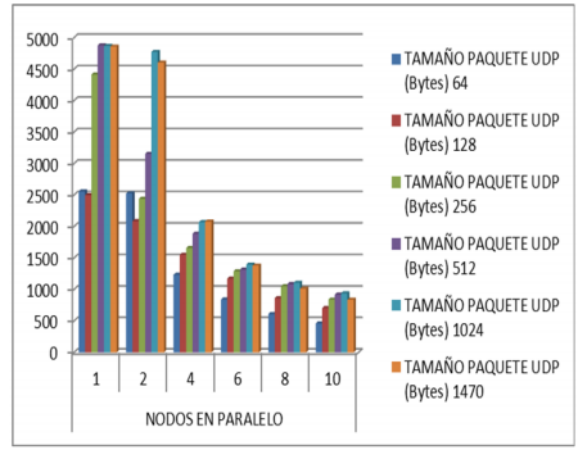


Figura 8.8. Bandwidth un solo nodo por nodos en paralelo

- BANDWIDTH (kbytes/sec) para un solo nodo variando el nº de nodos en paralelo

		TAMAÑO PAQUETE FIJO
		512
NODOS EN PARALELO	1	4879
	2	3155
	4	1887
	6	1316
	8	1087
	10	921

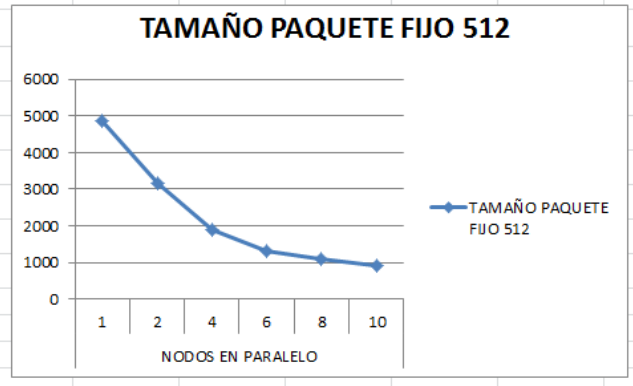


Figura 8.9. Bandwidth para un solo nodo variando nº nodos

Tabla 8.2. Bandwidth para un solo nodo variando nº nodos

- BANDWIDTH (kbytes/sec) para un solo nodo variando el tamaño del paquete

		TAMAÑO PAQUETE UDP (Bytes)					
		64	128	256	512	1024	1470
NODOS EN PARALELO	4	1234	1552	1658	1387	2071	2080

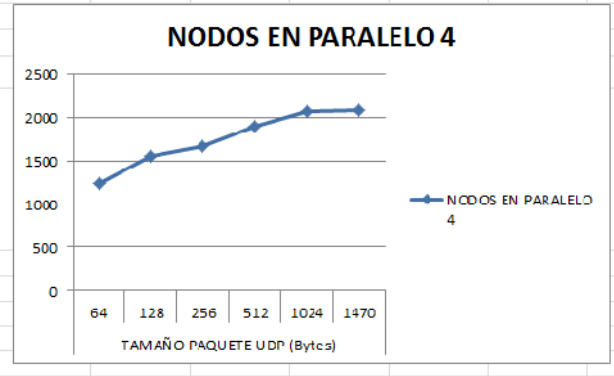


Tabla 8.3. Bandwidth para un solo nodo variando paquete

Figura 8.10. Bandwidth para un solo nodo variando paquete

- BANDWIDTH (Kbytes/sec) para toda la transmisión

		TAMAÑO PAQUETE UDP (Bytes)					
		64	128	256	512	1024	1470
NODOS EN PARALELO	1	2559	2500	4414	4879	4869	4860
	2	4644	4073	4872	6298	9578	9160
	4	4874	6250	6707	7330	8332	8246
	6	5001	6914	7674	7701	8381	8225
	8	4825	6892	8217	8607	8686	8092
	10	4902	6943	8350	9211	9351	8341

Tabla 8.4. Bandwidth para toda la transmisión

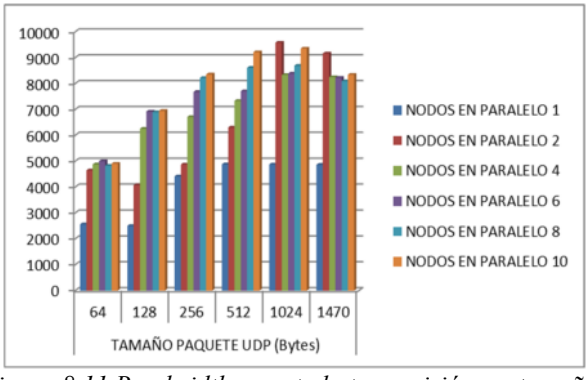


Figura 8.11 Bandwidth para toda transmisión portamaño paquete

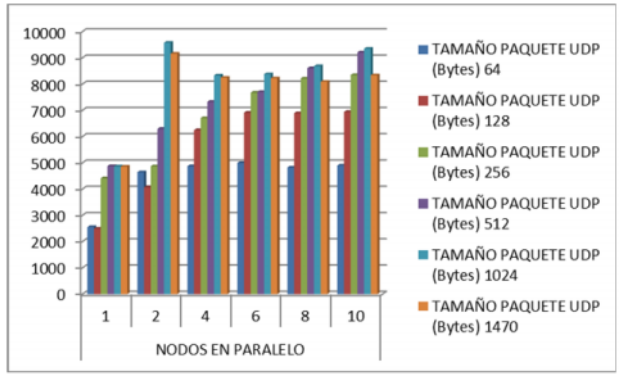


Figura 8.12. Bandwidth para toda transmisión por nodos en paralelo

- TRANFERENCIA (KBytes) de un solo nodo

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	25633	25040	44211	48868	48767	48681
	2	25330	20906	24438	31595	47812	46136
	4	12400	15545	16608	18926	20741	20831
	6	8465	11758	12930	13181	14012	13831
	8	6158	8666	10531	10884	11108	10142
	10	4633	7119	8430	9226	9448	8386

Tabla 8.4. Transferencia de un solo nodo

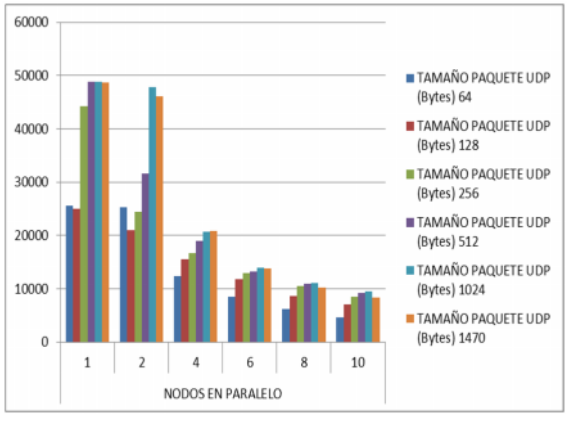


Figura 8.13. Transferencia de un solo nodo portamaño paquete

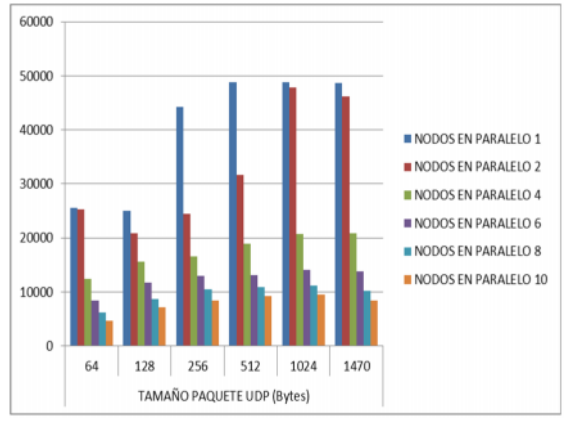


Figura 8.14. Transferencia de un solo nodo por nodos en paralelo

- TRANFERENCIA (KBytes) de toda la transmisión

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	25633	25040	44211	48868	48767	48681
	2	46512	40793	48799	63172	95926	91882
	4	48971	62789	67275	73648	83310	82721
	6	50400	69576	77103	77488	84200	82504
	8	49231	69674	82816	86746	87538	81555
	10	50625	70627	84546	92971	94386	83672

Tabla 8.5. Transferencia de toda la transmisión

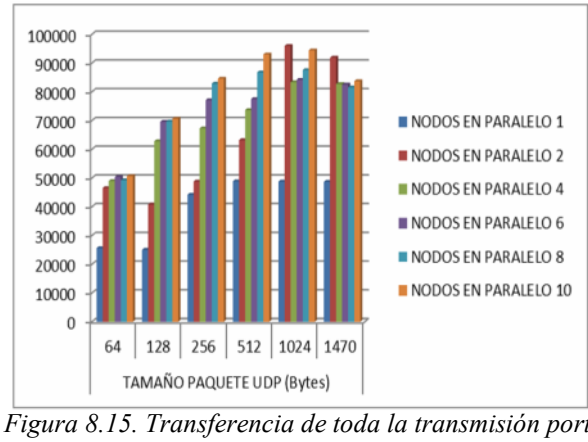


Figura 8.15. Transferencia de toda la transmisión portamaño paquete

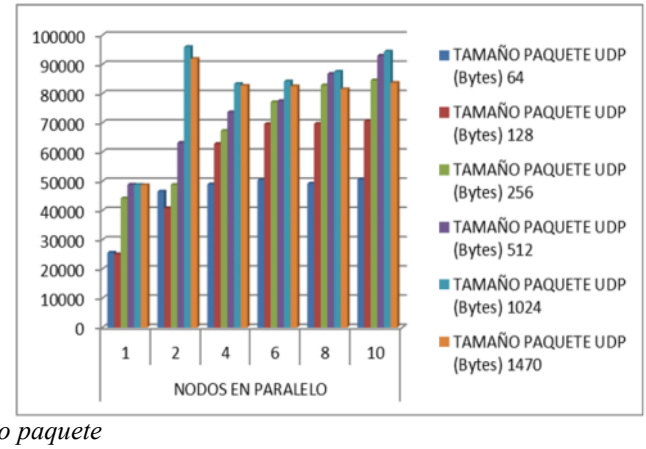


Figura 8.16. Transferencia de toda la transmisión por nodos en paralelo

- DIFERENCIAS DE BANDWIDTH (Kbytes/sec) entre nodos por tamaño de paquete

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS	**[1752]**	530	693	855	950	962	832
	[1764]	474	697	841	919	919	842
	[1776]	546	708	852	925	952	830
	[1788]	507	699	827	913	930	846
	[1800]	523	708	856	940	946	834
	[1812]	478	709	846	926	939	832
	[1824]	505	701	831	932	953	835
	[1836]	502	713	827	920	928	828
	[1848]	523	704	861	934	948	837
	[1868]	462	705	840	921	940	837

Tabla 8.6. Diferencia de bandwidth entre nodos por tamaño paquete

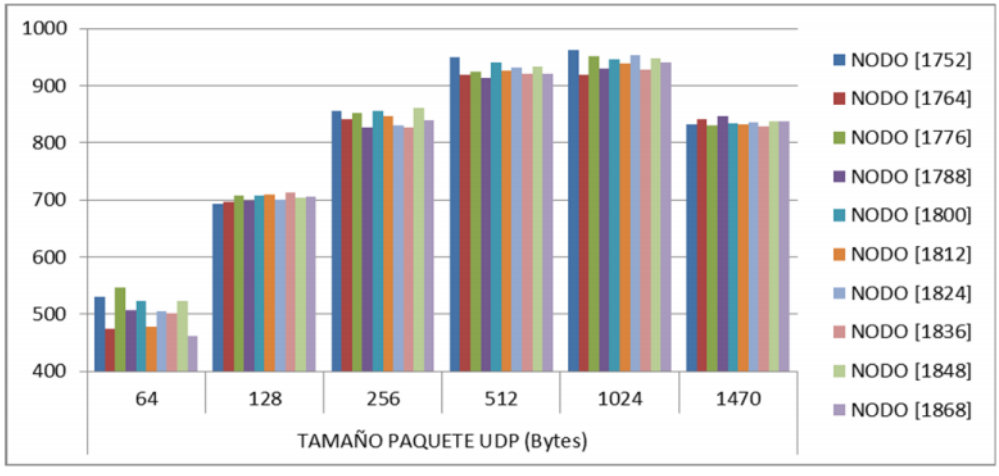


Figura 8.17. Diferencia de bandwidth entre nodos por tamaño paquete

- DIFERENCIAS DE BANDWIDTH (Kbytes/sec) por nodo con tamaño de paquete fijo

		TAMAÑO PAQUETE UDP (Bytes)	
		64	1024
NODO	[1752]	530	962
	[1764]	474	919
	[1776]	546	952
	[1788]	507	930
	[1800]	523	946
	[1812]	478	939
	[1824]	505	953
	[1836]	502	928
	[1848]	523	948
	[1868]	462	940

Tabla 8.7. Diferencia de bandwidth por nodo

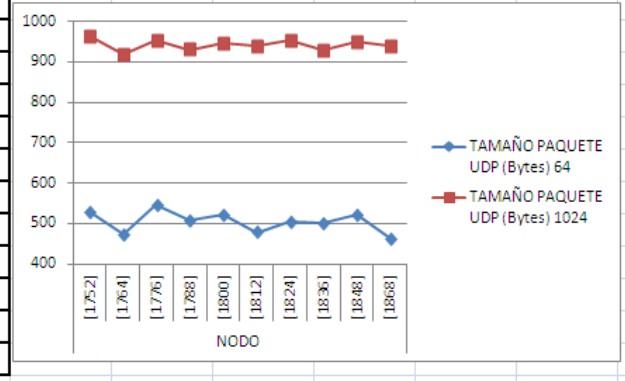


Figura 8.18. Diferencia de bandwidth por nodo

8.3.1.2. Prueba B (por bytes transmitidos):

Las mediciones en la prueba B se realizan para los mismos valores de las variables, utilizando transmisión UTP dual, manteniendo fijo el UDP Bandwidth pero con la diferencia que se realizan por la tarde y que en lugar de medir durante un tiempo fijo de 10 segundos se realizaran mediciones hasta que se transmita un total de 20.000.000 bytes por nodo en intervalos de 2 segundos.

Como en la prueba anterior, se realizan 6 bloques de mediciones, uno para cada valor de nodos conectados (1, 2, 4, 6, 8, 10), variando en cada bloque los tamaños de paquete para los valores utilizados (64, 128, 256, 512, 1024 y 1470 bytes).

Vemos también una muestra de la línea de comando de Iperf con los parámetros que se han utilizado y los valores obtenidos para esta prueba:

```
bin/iperf.exe -c 10.228.130.162 -u -P 2 -i 2 -p 5001 -l 64.0B -f K -b 40.0M -n 20000000 -d -L 5001 -T 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 64 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
Client connecting to 10.228.130.162, UDP port 5001
Sending 64 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1848] local 192.168.1.117 port 2782 connected with 10.228.130.162 port 5001
[1868] local 192.168.1.117 port 2781 connected with 10.228.130.162 port 5001
[ ID] Interval       Transfer     Bandwidth
[1848]  0.0- 2.0 sec  4968 KBytes  2484 KBytes/sec
[1868]  0.0- 2.0 sec  4725 KBytes  2362 KBytes/sec
[SUM]  0.0- 2.0 sec  9693 KBytes  4846 KBytes/sec
[1848]  2.0- 4.0 sec  5098 KBytes  2549 KBytes/sec
[1868]  2.0- 4.0 sec  4318 KBytes  2159 KBytes/sec
[SUM]  2.0- 4.0 sec  9416 KBytes  4708 KBytes/sec
[1848]  4.0- 6.0 sec  5070 KBytes  2535 KBytes/sec
[1868]  4.0- 6.0 sec  4295 KBytes  2148 KBytes/sec
[SUM]  4.0- 6.0 sec  9365 KBytes  4683 KBytes/sec
[1848]  0.0- 7.7 sec  19531 KBytes  2525 KBytes/sec
[1868]  6.0- 8.0 sec  4231 KBytes  2115 KBytes/sec
[1868] Sent 312500 datagrams
[SUM]  0.0- 8.8 sec  39063 KBytes  4448 KBytes/sec
```

En este caso de cada una de las muestras realizadas en cada ensayo se tomarán los resultados promedio de Interval y Bandwidth, viendo, por un lado, si el momento del día influye en el ancho de banda y, por otro, si varian los resultadosel hecho de que las mediciones se realicen en lugar de con un intervalo fijo de tiempo, cuando lo que se geja fijo es la cantidad de bytes a transmitir.

- .BANDWIDTH (Kbytes/sec) para un solo nodo

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	2593	2505	4664	4883	4883	4864
	2	2525	2056	2451	3102	4717	4630
	4	1261	1576	1793	1926	2076	2056
	6	869	1175	1314	1294	1434	1417
	8	623	873	1028	1097	1104	1080
	10	502	706	845	938	938	846

Tabla 8.8. Bandwidth para un solo nodo B

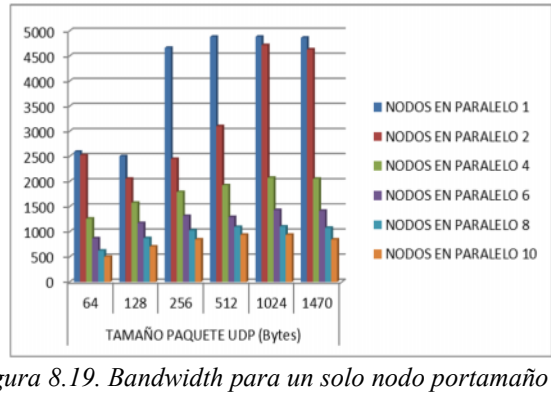


Figura 8.19. Bandwidth para un solo nodo portamaño paquete B

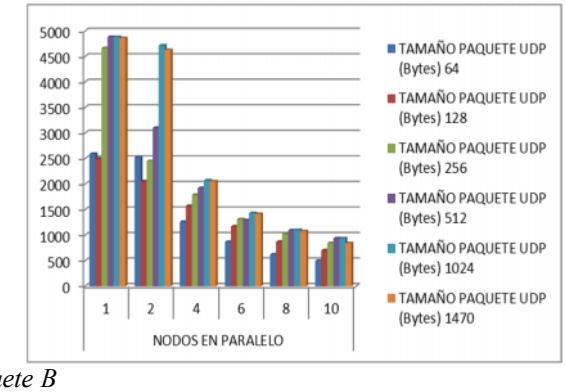


Figura 8.20. Bandwidth para un solo nodo por nodos en paralelo B

- BANDWIDTH de un nodo con tamaño de paquete fijo variando el nº de nodos en paralelo

		TAMAÑO PAQUETE UDP (Bytes)
		512
NODOS EN PARALELO	1	4883
	2	3102
	4	1926
	6	1294
	8	1097
	10	938

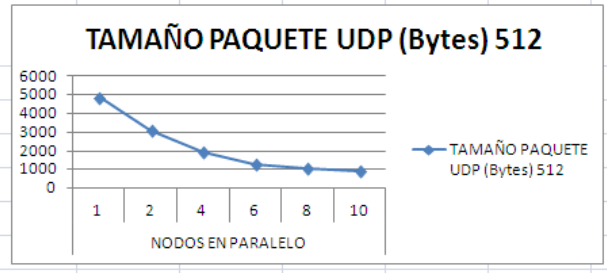


Figura 8.21. Bandwidth para un solo nodo variando nº nodos B

Tabla 8.9. Bandwidth para un solo nodo variando nº nodos B

- BANDWIDTH (Kbytes/sec) para toda la transmisión

		TAMAÑO PAQUETE UDP (Bytes)					
		64	128	256	512	1024	1470
NODOS EN PARALELO	1	2593	2505	4664	4883	4883	4864
	2	4448	4032	4892	6204	9399	9260
	4	4916	6188	6868	7278	8210	8157
	6	4980	6912	7845	7545	8552	8475
	8	4983	6983	8197	8613	8734	8555
	10	4980	7015	8339	9118	9343	8429

Tabla 8.10. Bandwidth para toda la transmisión B

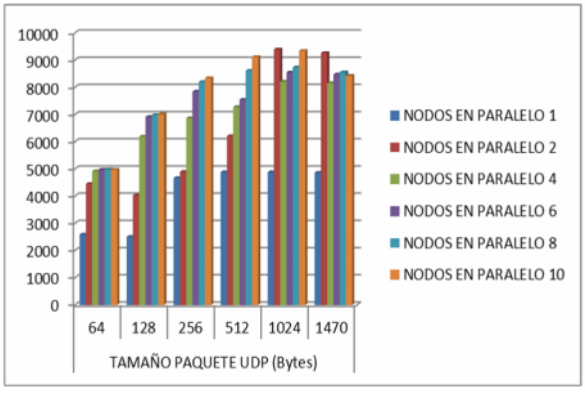


Figura 8.22. Bandwidth para toda transmisión portamaño paquete B

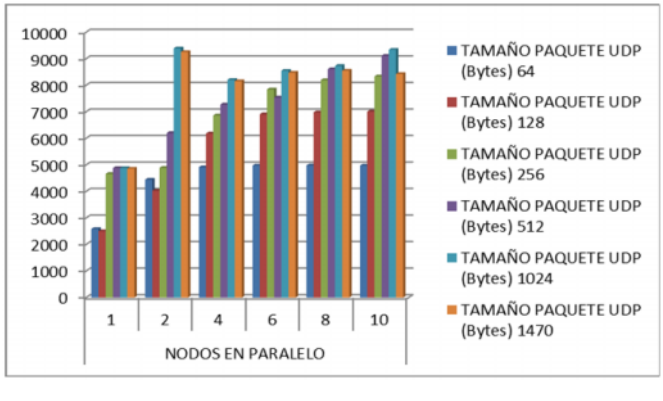


Figura 8.23. Bandwidth para toda transmisión por nodos en paralelo B

- TIEMPO (sec) necesario para la transmisión

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	7,5	7,8	4,2	4,0	4,0	4,0
	2	8,8	9,7	8,0	6,3	4,2	4,2
	4	15,9	12,6	11,4	10,7	9,5	9,6
	6	23,5	17,0	14,9	15,5	13,7	13,8
	8	31,4	22,4	19,1	18,1	17,9	18,3
	10	39,2	27,8	23,4	21,4	20,9	23,2

Tabla 8.11. Tiempo necesario para la transmisión B

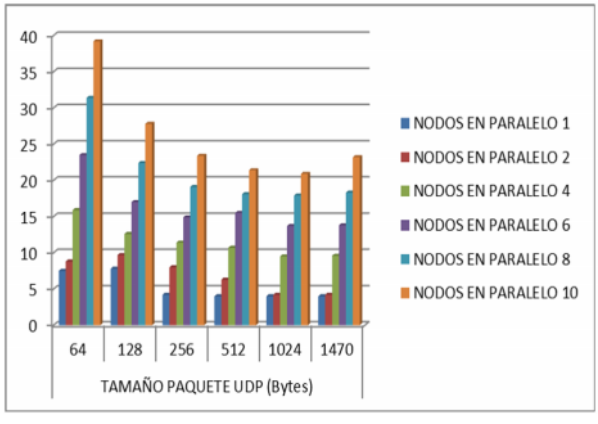


Figura 8.24. Tiempo necesario para la transmisión por tamaño paquete

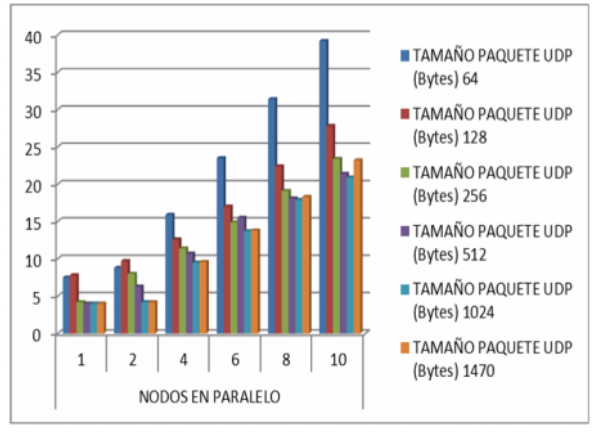


Figura 8.25. Tiempo necesario para la transmisión por nodos en paralelo

- DIFERENCIAS DE TIEMPO (sec) entre nodos por tamaño de paquete

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS	**[1752]**	37,2	27,8	23,3	21,3	20,3	22,9
	[1764]	39,0	27,5	23,2	21,0	20,8	23,1
	[1776]	38,5	27,7	23,2	21,4	20,4	23,1
	[1788]	39,0	27,6	23,3	21,3	20,9	23,2
	[1800]	38,4	27,8	23,3	21,4	20,5	23,0
	[1812]	38,9	27,8	23,4	21,0	20,8	23,1
	[1824]	37,5	27,6	23,2	21,4	20,5	23,0
	[1836]	39,1	27,8	23,4	21,2	20,9	23,1
	[1848]	38,5	27,7	23,3	21,4	20,4	23,1
	[1868]	38,9	27,7	23,1	20,8	20,8	23,1

Tabla 8.12. Diferencias de tiempo entre nodos por tamaño de paquete

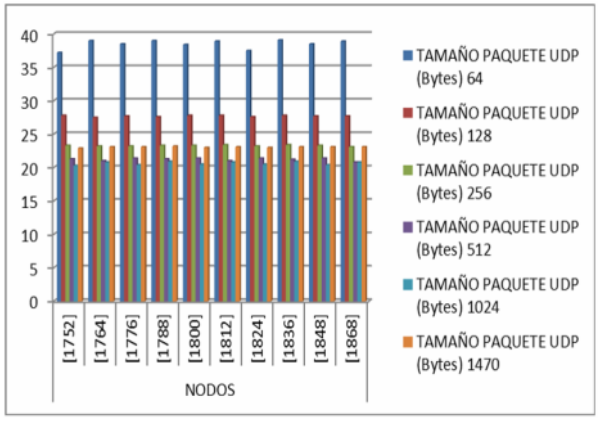


Figura 8.26. Diferencias de tiempo entre nodos por tamaño de paquete por nodo

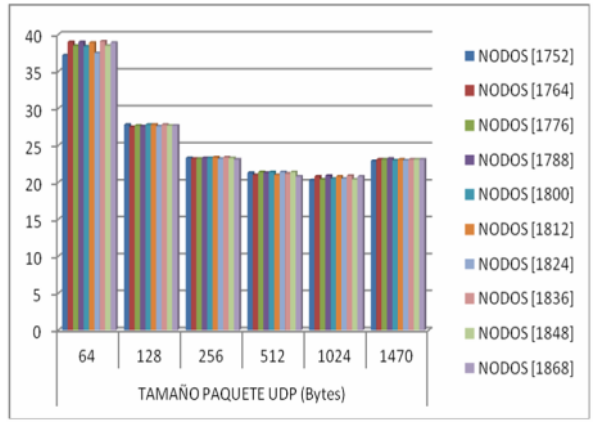


Figura 8.27. Diferencias de tiempo entre nodos por tamaño paquete

- DIFERENCIAS DE TIEMPO (sec) por nodo con tamaño de paquete fijo

		TAMAÑO PAQUETE UDP (Bytes)	
		64	1024
NODOS	[1752]	37,2	20,3
	[1764]	39	20,8
	[1776]	38,5	20,4
	[1788]	39	20,9
	[1800]	38,4	20,5
	[1812]	38,9	20,8
	[1824]	37,5	20,5
	[1836]	39,1	20,9
	[1848]	38,5	20,4
	[1868]	38,9	20,8

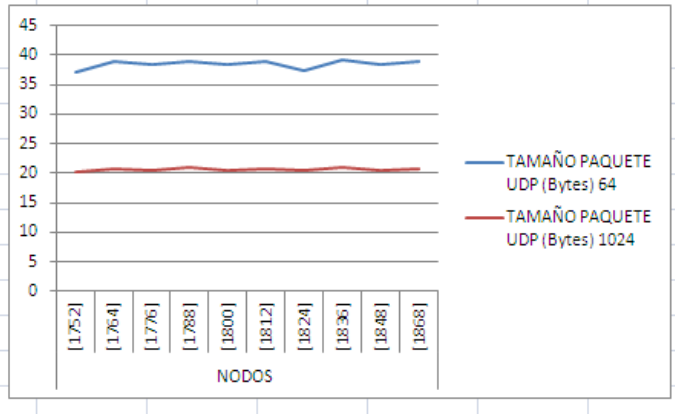


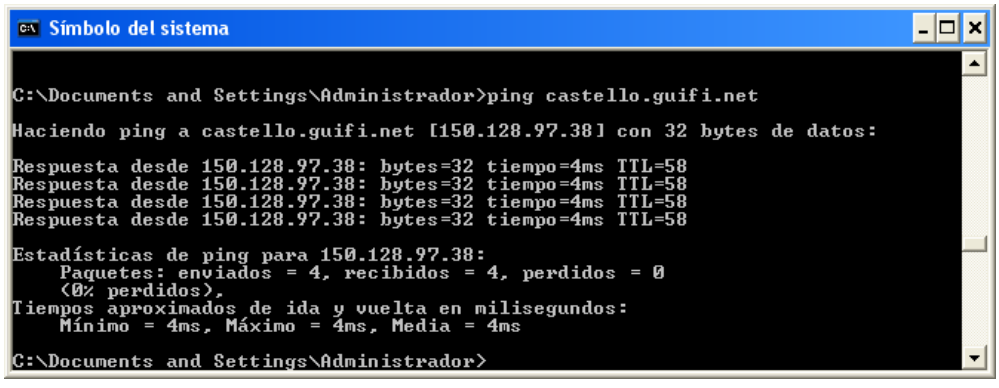
Tabla 8.13. Diferencias de tiempo por nodo con tamaño de paquete fijo

Figura 8.28. Diferencias de tiempo por nodo con tamaño de paquete fijo

8.3.2. Sobre la red UPV

8.3.2.1. Prueba C (por tiempo)

Esta prueba va a consistir en repetir alguno de los ensayos anteriores pero accediendo al servidor de Castellón desde Internet, por su dirección IP pública. Para ello desde el cliente se hace una conexión VPN con la red de la UPV y con esto el cliente obtiene una dirección IP de esta red y acceder a Internet.



Vemos la línea de comando y los valores obtenidos al ejecutar Iperf desde esta red:
bin/iperf.exe -c **150.128.97.38** -u -**P 2** -i 2 -p 5001 -l **64.0B** -f K -b 40.0M -**t 10** -d -L 5001 -T 1

```
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 64 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
Client connecting to 150.128.97.38, UDP port 5001
Sending 64 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1868] local 192.168.1.117 port 3805 connected with 150.128.97.38 port 5001
[1912] local 192.168.1.117 port 3808 connected with 150.128.97.38 port 5001
[ ID] Interval       Transfer     Bandwidth
[1868]  0.0- 2.0 sec  4524 KBytes  2262 KBytes/sec
[1912]  0.0- 2.0 sec  5131 KBytes  2566 KBytes/sec
[SUM]  0.0- 2.0 sec  9656 KBytes  4828 KBytes/sec
[1868]  2.0- 4.0 sec  4270 KBytes  2135 KBytes/sec
[1912]  2.0- 4.0 sec  5131 KBytes  2565 KBytes/sec
[SUM]  2.0- 4.0 sec  9401 KBytes  4701 KBytes/sec
[1868]  4.0- 6.0 sec  4159 KBytes  2079 KBytes/sec
[1912]  4.0- 6.0 sec  5093 KBytes  2546 KBytes/sec
[SUM]  4.0- 6.0 sec  9252 KBytes  4626 KBytes/sec
[1868]  6.0- 8.0 sec  4062 KBytes  2031 KBytes/sec
[1912]  6.0- 8.0 sec  5129 KBytes  2565 KBytes/sec
[SUM]  6.0- 8.0 sec  9192 KBytes  4596 KBytes/sec
[1868]  8.0-10.0 sec  4004 KBytes  2002 KBytes/sec
[1868]  0.0-10.0 sec  21020 KBytes  2099 KBytes/sec
[1912]  8.0-10.0 sec  5064 KBytes  2532 KBytes/sec
[SUM]  8.0-10.0 sec  9068 KBytes  4534 KBytes/sec
[1912]  0.0-10.0 sec  25548 KBytes  2551 KBytes/sec
[1868] Sent 336318 datagrams
[1912] Sent 408774 datagrams
[SUM]  0.0-10.0 sec  46568 KBytes  4642 KBytes/sec
```

- BANDWIDTH (Kbytes/sec) para un solo nodo

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	2602	2500	4483	4872	4887	4860
	2	2551	2046	2447	3056	4766	4681
	4	1268	1589	1639	1863	2103	2075
	6	868	1168	1291	1335	1399	1398
	8	656	874	1047	1098	1113	1037
	10	491	707	834	904	943	840

Tabla 8.14. Bandwidth para un solo nodo C

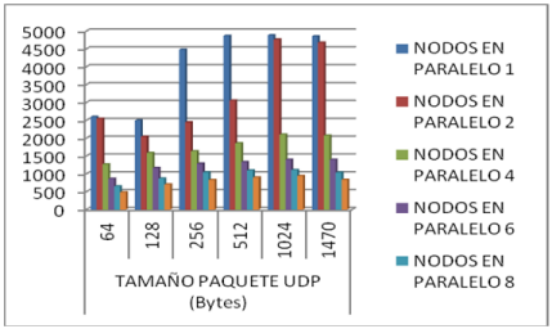


Figura 8.29. Bandwidth para un solo nodo portamaño paquete C

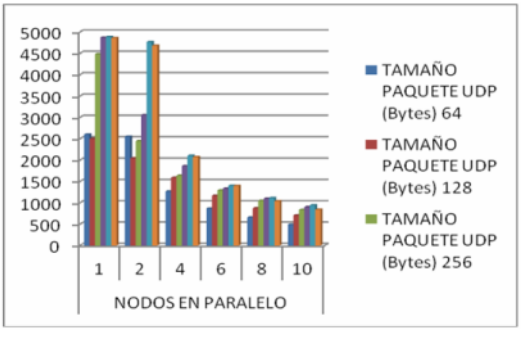


Figura 8.30. Bandwidth para un solo nodo por nodos en paralelo C

- BANDWIDTH (kbytes/sec) para un solo nodo variando el nº de nodos en paralelo

		TAMAÑO PAQUETE FIJO
		512
NODOS EN PARALELO	1	4872
	2	3056
	4	1863
	6	1335
	8	1098
	10	904

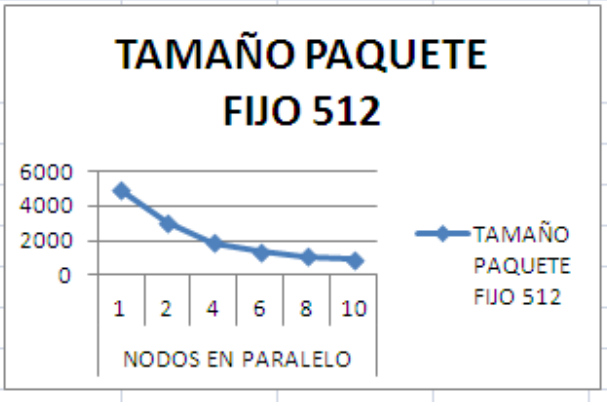


Figura 8.31. Bandwidth para un solo nodo variando nº nodos C

Tabla 8.15 Bandwidth para un solo nodo variando nº nodos C

- BANDWIDTH (kbytes/sec) para un solo nodo variando el tamaño del paquete

		TAMAÑO PAQUETE UDP (Bytes)					
		64	128	256	512	1024	1470
NODOS EN PARALELO	4	1268	1589	1639	1863	2103	2075

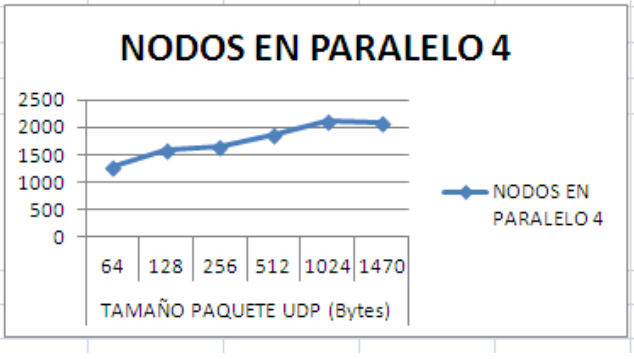


Tabla 8.16. Bandwidth para un solo nodo variando paquete C

Figura 8.32. Bandwidth para un solo nodo variando paquete C

- BANDWIDTH (Kbytes/sec) para toda la transmisión

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	2602	2500	4483	4872	4887	4860
	2	4642	4169	4892	6089	9540	9392
	4	4908	6287	6737	7122	8242	8180
	6	4991	6884	7835	7925	8414	8399
	8	4929	6965	8165	8588	8729	8440
	10	4903	6986	8386	9000	9393	8246

Tabla 9.17. Bandwidth para toda la transmisión C

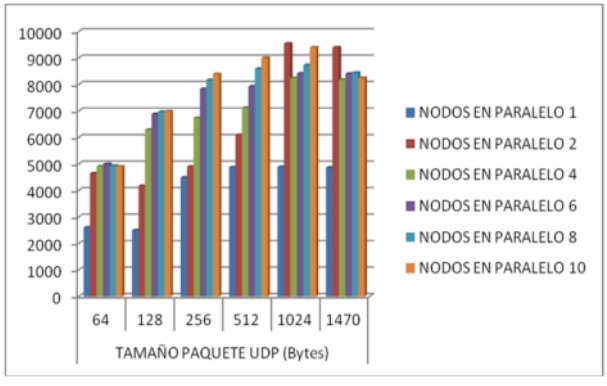


Figura 8.33. Bandwidth para toda transmisión por tamaño paquete C

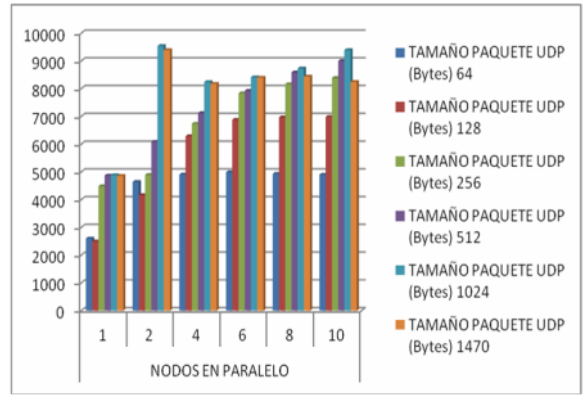
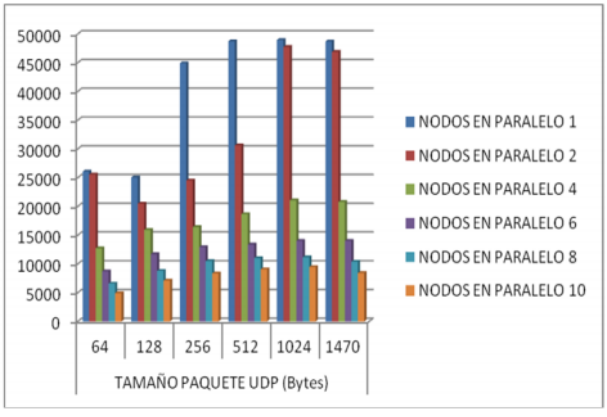


Figura 8.34. Bandwidth para toda transmisión por nodos en paralelo C

- TRANFERENCIA (KBytes) DE UN SOLO NODO

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	26062	25040	44898	48716	48946	48681
	2	25548	20489	24504	30606	47734	46884
	4	12717	15914	16419	18657	21059	20778
	6	8722	11701	12932	13368	14015	14022
	8	6576	8784	10487	11001	11151	10386
	10	4915	7103	8354	9059	9463	8418

Tabla 8.18. Transferencia de un solo nodo C



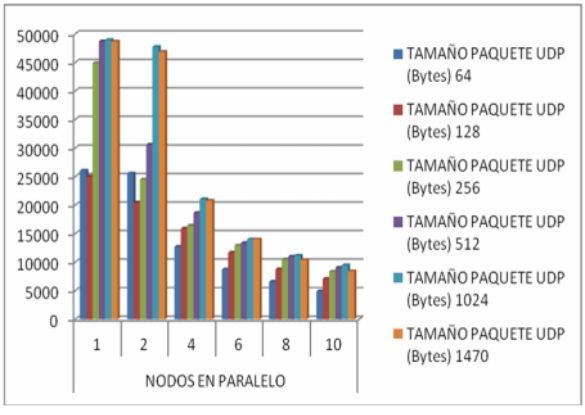


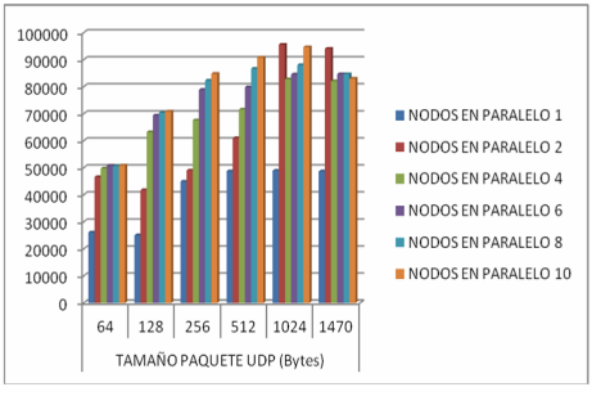
Figura 8.35. Transferencia de un solo nodo por tamaño paquete C

Figura 8.36. Transferencia de un solo nodo por nodos en paralelo C

- TRANFERENCIA (KBytes) de toda la transmisión

		TAMAÑO PAQUETE UDP (Bytes)					
		64	**128**	**256**	**512**	**1024**	**1470**
NODOS EN PARALELO	**1**	26062	25040	44898	48716	48946	48681
	2	46568	41759	49000	60984	95546	94067
	4	49766	63167	67585	71553	82805	82060
	6	50842	69375	78841	79846	84537	84641
	8	50677	70411	82291	86685	87976	84660
	10	50864	70838	84773	90842	94659	82976

Tabla 8.19. Transferencia de toda la transmisión C



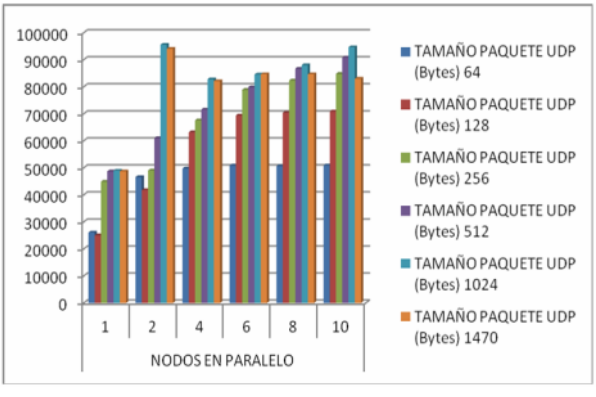


Figura 8.37. Transferencia de toda la transmisión po rtamaño paquete C

Figura 8.38. Transferencia de toda la transmisión por nodos en paralelo C

- DIFERENCIAS DE BANDWIDTH (Kbytes/sec) por nodo con tamaño de paquete fijo

		TAMAÑO PAQUETE UDP (Bytes)	
		64	1024
NODO	[1752]	472	982
	[1764]	517	922
	[1776]	491	963
	[1788]	521	914
	[1800]	487	958
	[1812]	540	919
	[1824]	491	964
	[1836]	517	911
	[1848]	503	963
	[1868]	522	943

Tabla 8.20. Diferencia de bandwidth por nodo C

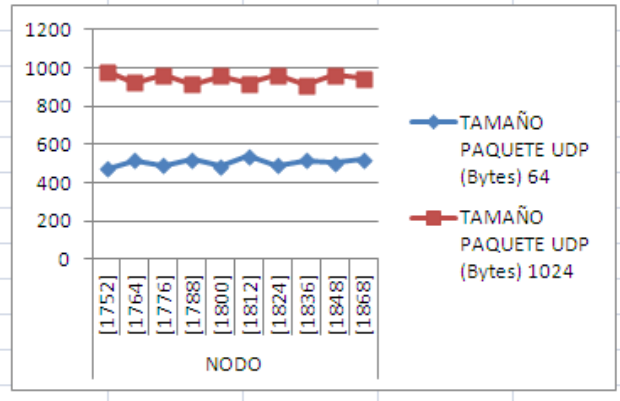


Figura 8.39. Diferencia de bandwidth por nodo C

8.3.3. Con conexión directa a Internet

8.3.3.1.-Con 1 stream y 1024 bytes de tamaño de paquete

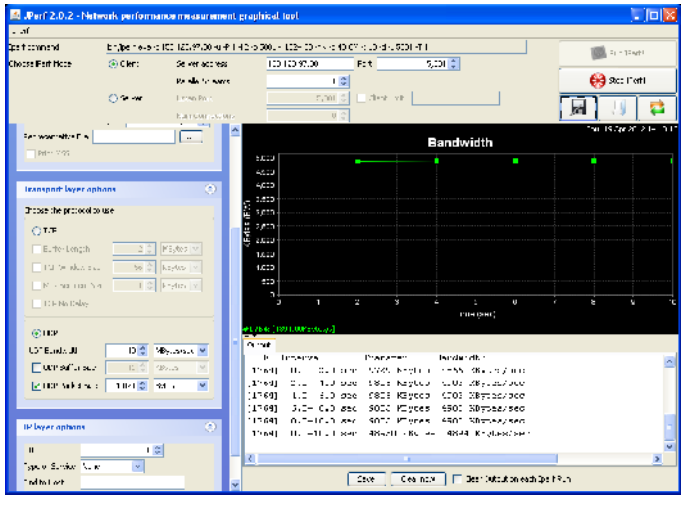


Figura 8.40. Conexión directa a Internet con 1 stream

8.3.3.2.-Con 10 streams y 1024 bytes de tamaño de paquete

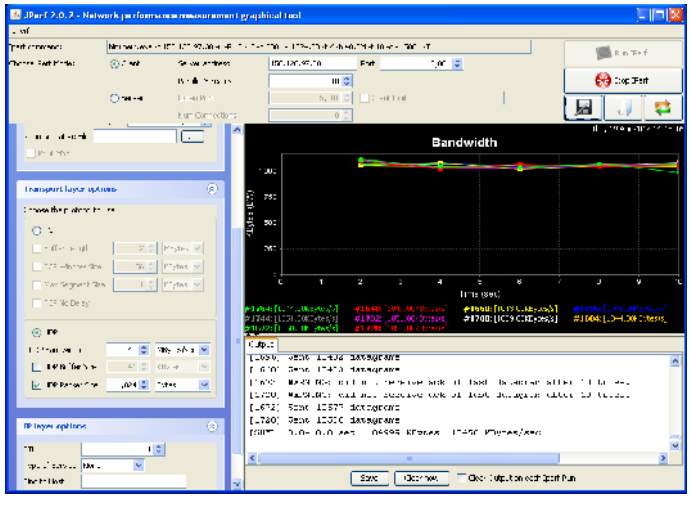
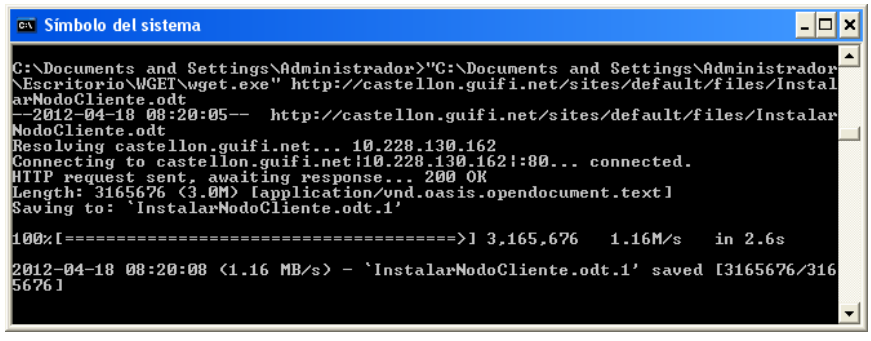


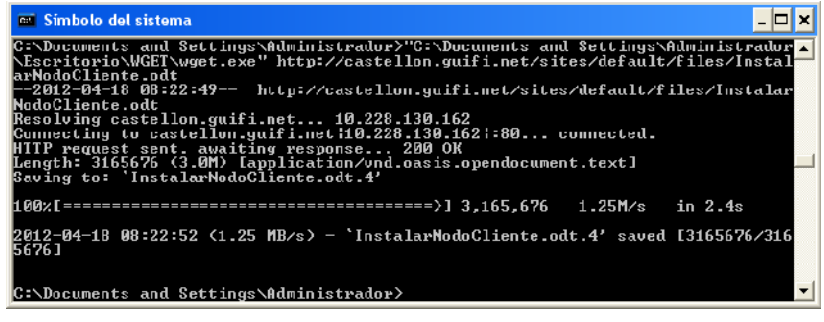
Figura 8.41. Conexión directa a Internet con 10 streams

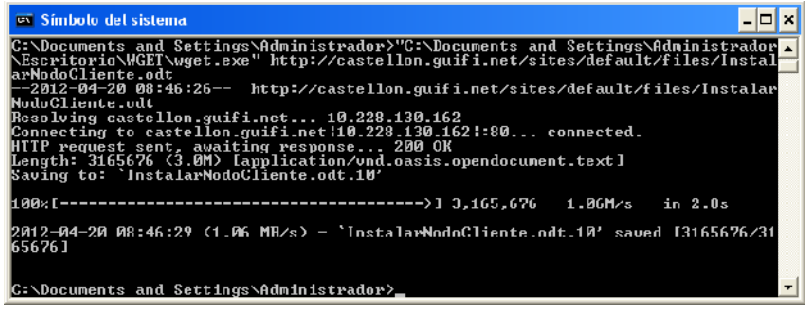
8.4. Resultado de las pruebas con Wget

Se procede a descargar, en todos los casos el fichero el fichero “InstalarNodoCliente.odt de 3,1 Mbytes desde la URL http://castellon.guifi.net

8.4.1. Desde la red Guifi.net

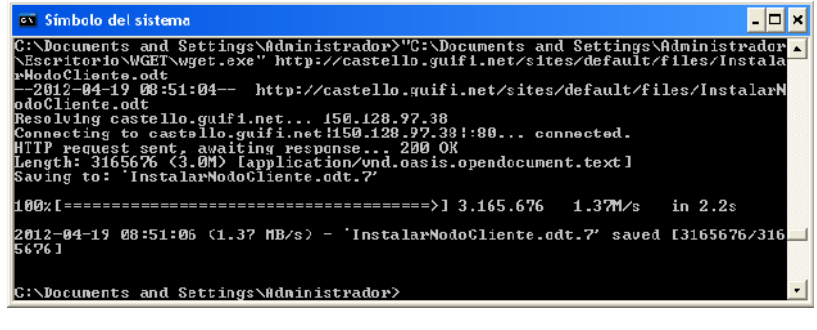


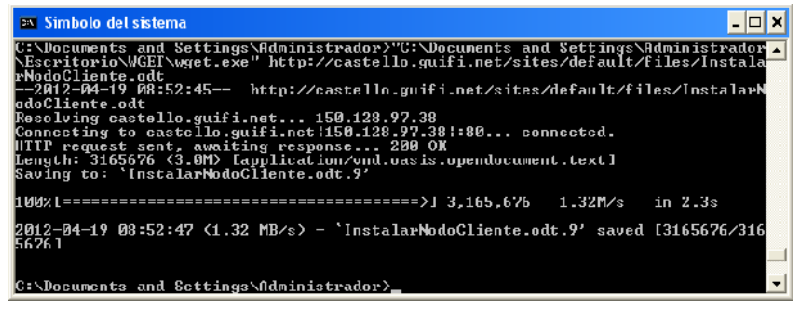


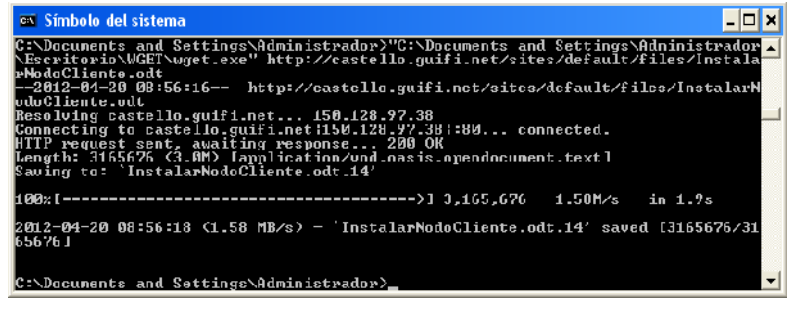


8.4.2. Desde la red UPV

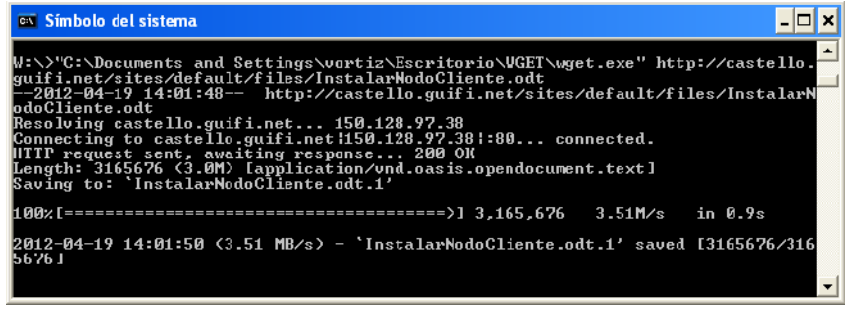
La URL en este caso, siendo el mismo servidor, es http://castello.guifi.net

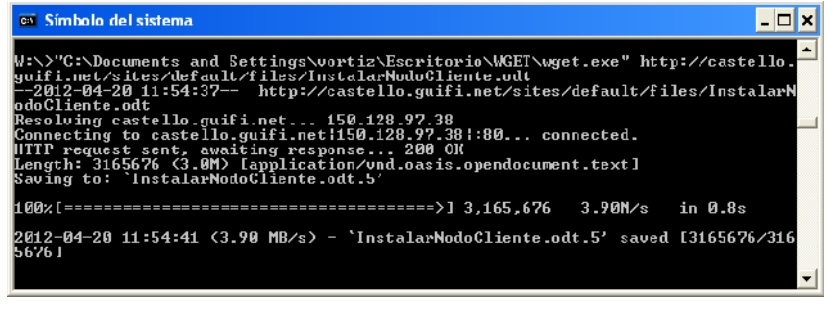






8.4.3. Con conexión directa a Internet





8.5. -Evaluación y conclusiones de las pruebas

8.5.1.- Con Jperf

8.5.1.1.-De la transmisión sobre la red Guifi.net

Comparando las tablas y gráficos en las 2 pruebas realizadas sobre la red Guifi.net se puede concluir que **no existen diferencias a considerar respecto a la hora en que se realice el ensayo**,

obteniéndose prácticamente los mismos valores cuando las medidas son realizadas por la mañana o cuando se hacen por la tarde.

Tampoco tiene influencia en el throughput el hecho de configurar Iperf para **que las muestras se tomen** durante un periodo de **tiempo fijo o** con la transmisión de una **cantidad de bytes constante**.

En cambio, en cualquiera de las 2 pruebas, los resultados obtenidos en la medición de throughput si que permiten observar que éste varía de forma importante, al variar algún parámetro, a lo largo del estudio siendo una de las conclusiones más importantes que se obtienen es que se evidencia un **aumento del throughput a medida que el tamaño del paquete aumenta** (prácticamente se duplica entre los valores extremos) alcanzando, en todos los casos, su mayor valor con un tamaño de paquete de 1024 bytes, aunque se mantiene bastante estable a partir de 512 bytes y disminuye ligeramente cerca del tamaño máximo que puede yener el paquete (1470 bytes)

El throughput máximo, unos 9.5000 Kbytes/sec, se alcanza, con la transmisión de 10 streams en paralelo y un tamaño de paquete de 1024 bytes, al sumarse el bandwidth utilizado por todos los streams.

Igualmente se observa que **a medida que aumenta la cantidad de nodos activos en la red, el throughput de cada nodo disminuye** considerablemente indicando que éste parámetro regula de una forma muy relevante el comportamiento del throughput en relación al rendimiento de una red.

A nivel de cantidad de bytes totales transmitidos, la variación no es proporcional a la variación de las variables. Al pasar de 1 a 2 streams si que se duplican prácticamente los bytes transmitidos, pero al seguir aumentando el número de nodos la cantidad de bytes transmitidos se mantiene en valores cercanos al doble de un solo nodo con pocas variaciones. Al analizarlo respecto a la variación del tamaño de paquete, se observa que si que produce un aumento más continuo de bytes en la transferencia, alcanzandose un aumento aproximado del 75% con tamaños de paquete superiores a 512 bytes.

Respecto al tiempo necesario para que en cada stream se transmita una cantidad fija de información se compueba que al ir incrementando el tamaño del paquete va disminuyendo el tiempo proporcionalmente hasta el tamaño de 1024 bytes donde se estabiliza en aproximadamente la mitad del tiempo que con paquetes de 64 bytes. Por otro lado, al aumentar el número de streams se observa que, a partir de 4 streams el valor del tiempo de transmitisión necesario se puede aproximar al obtenido con la fórmula:

Tiempo de transmisión ≈ (nº streams / 2) * tiempo utilizado por 1 stream

Tambien se puede observar que cuando la transmisión se realiza con 10 streams en paralelo**, no existen grandes diferencias en los valores que se obtienen por cada nodo (stream)**, tanto en bandwidth como en el tiempo necesario para la transmisión, obteniendose un porcentaje de variación

estre el menor y el mayor valor entre 7 y 12% en el peor caso (tamaño de paquete de 64 bytes) y entre 3 y 5% en el mejor (1024 bytes).

8.5.1.2. Comparación de las redes Guifi.net y UPV (sobre VPN)

En la comparación de cada una de las tablas que se han generado con los resultados obtenidos al hacer las pruebas de transferencia de datos con Jperf desde el cliente hasta el servidor Guifi, tanto por la red Guifi.net como por la red pública desde la red UPV podemos sacar como conclusión que no hay prácticamente ninguna diferencia significativa ya que se obtienen valores de throughput similares en todas y cada una de las pruebas variando tanto los valores de tamaño de paquete como de número de streams en paralelo en la transmisión.

Visualmente se comprueba esta igualdad en las siguientes muestras de las comparaciones realizadas donde vemos como las gráficas resultantes se solapan:

- Bandwidth por nodo

		RED GUIFINET	RED UPV
NODOS EN PARALELO	1	4883	4872
	2	3102	3056
	4	1926	1863
	6	1294	1335
	8	1097	1098
	10	938	904

Tabla 8.21. Bandwidth por nodo Guifi-UPV

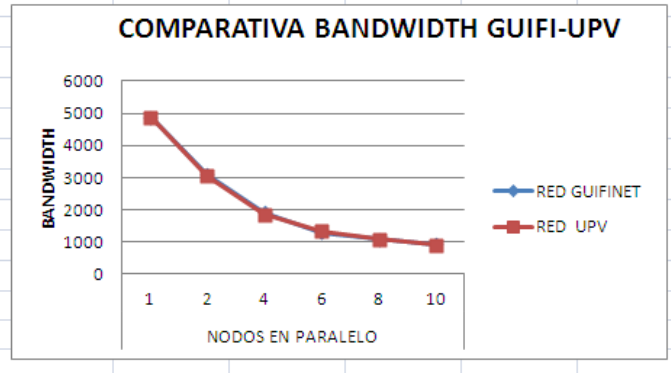


Figura 8.42. Bandwidth por nodo Guifi-UPV

- Bandwidth total en la transmisión

		Red Guifi	Red UPV
NODOS EN PARALELO	1	4883	4872
	2	6204	6089
	4	7278	7122
	6	7545	7925
	8	8613	8588
	10	9118	9000

Tabla 8.22. Bandwidth total en la transmisión Guifi-UPV

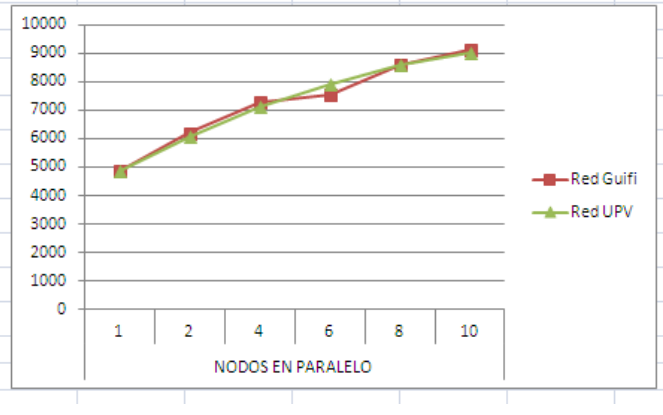


Figura 8.43. Bandwidth total en la transmisión Guifi-UPV

La igualdad de throughput que se observa en las dos redes al hacer los ensayos está dentro de la lógica ya que los paquetes UDP en la transmisión transitan básicamente por el mismo camino y atraviesan los mismos routes aunque uno sea utilizando direcciones privadas y el otro direcciones publicas.

8.5.1.3. Comparación de las redes Guifi.net y conexión directa a Internet

Simplemente con las 2 muestras que se han tomado en la conexión directa con Internet se obtienen valores que se pueden comparar con los resultados de las pruebas anteriores;

- Bandwidth por nodo

		Red Guifi	Rediris
NODOS EN PARALELO	1	4883	4894
	10	938	1044

Tabla 8.23. Bandwidth por nodo Guifi-Rediris

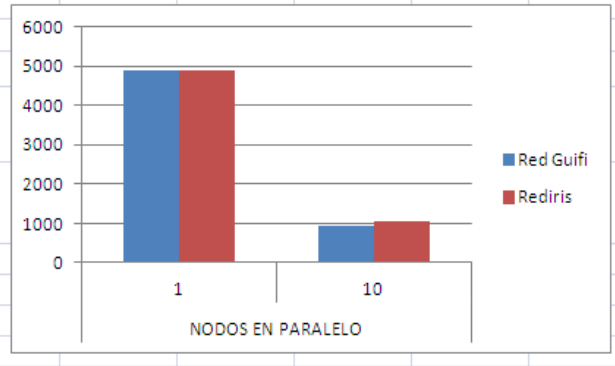


Figura 8.44. Bandwidth por nodo Guifi-Rediris

- Bandwidth total de la transmisión

		Red Guifi	Rediris
NODOS EN PARALELO	1	4883	4894
	10	9118	10405

Tabla 8.24. Bandwidth total en transmisión Guifi-Rediris

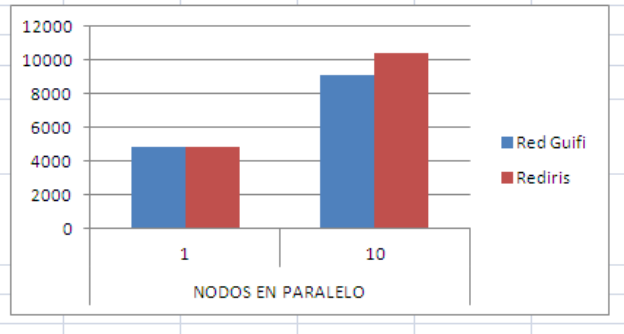


Figura 8.45. Bandwidth total en transmisión Guifi-Rediris

De la comparación efectuada de los resultados de las mediciones efectuadas con Jperf se deduce que el ancho de banda resultante para los mismos valores de las variables no presenta una gran diferencia, ya que la red que no incorpora la parte inalambrica de Guifi.net, en el caso de 10 streams en paralelo que es cuando la diferencia es mayor, presenta un bandwidth mayor en, aproximadamente un 10%.

8.5.2.-Wget

8.5.2.1. Comparación de las redes Guifi.net y UPV (sobre VPN)

Las muestras, obtenidas en distintos días, nos dan distintos valores de los que podemos deducir que el ancho de banda medio aproximado en la descarga desde el servidor web sobre la red Guifi.net está 1,15 MB/s y sobre la red UPV de 1,40 MB/s. lo que nos indica que en la descarga de archivos si que se aprecia una diferencia de throughput, siendo mayor en un 20% aproximadamente sobre la red UPV.

8.5.1.3. Comparación con la conexión directa a Internet

De nuevo la prueba de descarga con wget ofrece valores mucho más significativos del ancho de banda que se dispone en la descarga. El valor promedio en el caso de conexión directa a internet es aproximadamente de 3,70 MB/s que es 3 y 2,5 veces superior a las obtenidas anteriormente en las pruebas de descarga desde Guifi.et (1,15 MB/s) y desde UPV (1,40 MB/s) respectivamente.

CONCLUSIONES Y LÍNEAS FUTURAS DE TRABAJO

- **Conclusiones**

La instalación física del supernodo de la red Guifinet, principal objetivo al plantear este trabajo, así como la instalación del servidor Ubuntu con sus servicios, la programación del router, la creación de las redes privadas virtuales o las pruebas de prestaciones con la aplicación Jperf, han posibilitado el plasmar de forma práctica una parte importante de los temas teóricos desarrollados en el máster, tanto a nivel de redes inalámbricas, como de sistemas operativos o monitorización y estudio de las prestaciones de la red.

Por otra parte, el diseño del nodo y su inclusión en la red inalámbrica comunitaria, ha creado nuevas posibilidades de expansión de la red abierta Guifi.net y, el dotar de conectividad a Internet a través de la implementación de esta nueva red inalámbrica, han abierto nuevas iniciativas para incrementar la conectividad de la red de la universidad y de sus usuarios.

Además, una vez que la red estuvo operativa, se midieron los parámetros de rendimiento obteniendo los valores promedio de throughput de una transmisión con un solo nodo de unos 4500 Kbytes/s y de 8300 Kbytes/s con una transmisión de 10 streams en paralelo y una tasa de transmisión máxima de 4879 Kbytes/s y 9351 Kbytes/s respectivamente. Al ser comparados, obviando la inexistencia del enlace troncal inalámbrico, con las medidas obtenidas en otros escenarios ya establecidos, se comprobó que la nueva red ofrece un rendimiento similar.

En conclusión, teniendo claro que aún faltan muchas acciones para que éste proyecto se considere finalizado y que conforman las líneas futuras de este estudio, se puede decir que se han cumplido las expectativas propuestas y todos aquellos objetivos que fueron especificados en el tema introductorio.

- **Líneas futuras de trabajo**

La realización de este proyecto, con la implantación de un supernodo de la red Guifi.net, puede ser muy ventajosa por el valor añadido de un entorno inalámbrico nuevo que puede servir de base a otros futuros proyectos sobre redes y telecomunicaciones

A nivel del nodo UPV de la red Guifi.net, en este momento, ya se han creado nuevas conexiones con otros nodos cercanos y, por tanto, ya se ha iniciado con el continuo proceso del seguir expandiendo la red mesh como una clara apuesta de futuro. Para ello, una tarea pendiente, que inexorablemente depende de la creación de nuevos nodos troncales en el norte de la provincia de Valencia, es la configuración y activación de la antena parabólica para la conexión inalámbrica con el núcleo de la red.

Otra línea de trabajo sería, aunque ya están instalados los servicios imprescindibles, estudiar la implantación en el servidor UPVone de Guifi.net de nuevos servicios, como el de FTP, Proxys federados o Voz sobre IP.

Una acción a seguir, importante para difundir el conocimiento de la red y su implantación, sería la inclusión del nodo y de la red Guifi.net en el conjunto de la red inalámbrica de la UPV, y así garantizar la conexión a ésta red desde cualquier punto de acceso inalámbrico (AP) dentro de la Universidad.

También se puede indicar como tarea a realizar el mejorar el acceso desde la red Guifi.net, tanto de clientes fijos como móviles, instalando un sistema de autenticación, un portal cautivo para la conexión inicial web e integrar la gestión de usuarios y permisos, así como desarrollar la web del sitio.

Y, por último, dentro de la red Guifi.net se podría colaborar en los proyectos y estudios que proporcionan las líneas futuras de desarrollo de esta red como la implantación de Ipv6 en Guifi.net, mecanismos de calidad de servicio (QoS) o la optimización del encaminamiento.

ANEXO A:

GLOSARIO DE TÉRMINOS

802.11. Se usa frecuentemente para referirse a una familia de protocolos utilizados principalmente para redes inalámbricas de área local que incluyen 802.11a, 802.11b, 803.11g y 802.11n. También se le denomina Wi-Fi.

Access Point (AP). *Punto de Acceso*. Un dispositivo que crea una red inalámbrica que usualmente está conectado a una rede Ethernet cableada.

Ancho De Banda. (Bandwidth) Gama de frecuencias ocupada por una señal. En comunicaciones digitales se usa comúnmente para indicar la capacidad o tasa de transmisión. T*ambién: channel, throughput.*

Antena Direccional. Antena que radia más energía en una dirección particular.

Antena Omnidireccional. Tipo de antena que irradia con igual intensidad en todas las direcciones del plano horizontal.

Antena sectorial. Antena que radia principalmente en un área específica. El haz puede ser tan amplio como de 180 grados, o tan estrecho como 60 grados.

Azimut. Ángulo que especifica la desviación con respecto al meridiano. Normalmente se mide en sentido de las agujas del reloj desde el norte.

Canal (Channel) Un rango de frecuencias bien definidas usadas para comunicaciones. En 802.11 cada canal tiene un ancho de banda de 22 MHz, pero la separación de canales es de 5 MHz.

CATNIX. Punto neutro de conexión a Internet, situado en Cataluña y del que Guifi.net es miembro.

CMT. Comisión del Mercado de las Telecomunicaciones de España

CNML. Estándar abierto basado en XML y usado para describir redes libres.

Conector N. Robusto conector de microondas utilizado en componentes para exteriores, como antenas y puntos de acceso (AP).

Decibel (dB). Unidad de medida logarítmica que expresa la magnitud de potencia con respecto a un nivel de referencia. Sus derivadas más comunes son el dBi y dBm

Direct Sequence Spread Spectrum (DSSS). Espectro Ensanchado por secuencia directa. Método de modulación utilizado en los radios 802.11b

Enrutable Globalmente. Direcciones suministradas por un ISP, o por el RIR (Regional Internet Registry) que son alcanzables desde cualquier punto de la Internet. En IPv4 hay unos cuatro mil millones de direcciones IP posibles, aunque no todas son enrutables globalmente.

eXO - Expansió de la Xarxa Oberta. Asociación que trabaja expandiendo la red Guifi.net.

Filtrado por MAC. Método de control de acceso basado en la dirección MAC de los dispositivos que se comunican.

Firewall (Cortafuegos) Enrutador que acepta o rechaza tráfico con base en algún criterio. Constituye una herramienta básica utilizada para proteger toda la red de tráfico no deseado.

Ganancia. La capacidad de un dispositivo (tal como una antena o un amplificador) de aumentar la potencia de una señal.

Ganancia de Antena. Cantidad en la que se concentra la potencia de una antena en la dirección de su radiación máxima, usualmente expresada en dBi. La ganancia de una antena es recíproca, lo que significa que el incremento de potencia se presenta tanto en transmisión como en recepción.

gLIR (guifi Local Internet Registry) Grupo de trabajo encargado de llevar el LIR de guifi: organizar y coordinar todo lo relacionado con la presencia en Catnix y otros centros de datos, la fibra y la conectividad a internet a través de dichos CPDs, las relaciones con RIPE (NCC), el etiquetado y la monitorización de todos los dispositivos, y varias otras funciones.]

ICM. (Banda Industrial, Científica y Médica) Bandas del espectro radioeléctrico reservadas para uso no comercial. No tienen necesidad de licencia, pero está regulado el nivel de potencia al que se puede transmitir. En esta banda funcionan tecnologías como Wi-Fi o Bluetooth.

IFIP. (International Federation for Information Processing) es una organización no gubernamental internacional, cuya creación auspició Unesco en 1960. El núcleo principal de la actividad de IFIP lo gestionan los Comités Técnicos (TCs). En ellos coordinan su actividad y sus trabajos técnicos informáticos de Universidades y Centros de investigación.

IANA (Internet Assigned Numbers Authority). La organización que administra partes críticas de la infraestructura de Internet incluyendo la adjudicación de las direcciones IP.

ISM (Industrial, Scientific and Medical band). Ver ICM

Latencia. Tiempo que tarda un paquete en atravesar una conexión de red. A menudo se utiliza (incorrectamente) para designar el Round Trip Time (RTT), puesto que es mucho más fácil medir este último parámetro en una conexión de área extendida que la verdadera latencia.

Line Of Sight (LOS). Línea De Vista. Si una persona desde un punto A logra ver un punto B, se dice que existe línea de vista entre ambos puntos.

MARCo. El Servicio Mayorista de Acceso a Registros y Conductos (MARCo) constituye en su conjunto la oferta de Telefónica de España para permitir a los operadores acceder al uso compartido de infraestructuras de obra civil de Telefónica de España. De esta forma, los operadores podrán realizar sus propios despliegues de redes de acceso de nueva generación.

Mesh. *Malla.* Red carente de organización jerárquica, donde cada nodo puede transportar el tráfico de otros nodos. Las buenas implementaciones de redes en malla detectan y resuelven automáticamente los problemas de enrutamiento en forma dinámica.

MMCX. Conector de microondas muy pequeño utilizado en equipos Cisco.

NAT (Network Address Translation). NAT es una tecnología de red que permite que muchos ordenadores compartan una misma dirección de red válida (enrutable globalmente). Aunque esto es muy útil para resolver el problema del número limitado de direcciones IP disponibles, crea un problema técnico para servicios bidireccionales, como Voz sobre IP.

Octocefal. Servidor que aloja la web de Guifi.net.

OpenFPnet . Proyecto de implantación de una red integrada en Guifi.net para interconectar centros de Formación Profesional, empresas e instituciones.

OFDM. (Orthogonal Frequency Division Multiplexing) Técnica de modulación que consiste en descomponer una señal de banda ancha en muchas componentes de banda estrecha, cada una de las cuales es modulada en frecuencia por una subportadora.

Pasarela Por Defecto. Cuando un enrutador recibe un paquete destinado a una red para la cual no tiene una ruta específica, lo envía a la pasarela por defecto. La pasarela por defecto repite entonces el proceso, posiblemente enviando el paquete a su propia pasarela por defecto, hasta que el paquete alcanza su destino final.

Pigtail. *Latiguillo.* Cable corto y flexible usado en microondas para convertir un conector no estándar en algo más robusto y común. Sirve también para disminuir el esfuerzo mecánico aplicado al conector del radio.

PoE. (Power Over Ethernet) Técnica utilizada para suministrar corriente continúa a un dispositivo utilizando el cableado Ethernet.

Proxy. Programa o dispositivo que realiza una acción en representación de otro. Muy comunes los servidores proxy que almacenan localmente las páginas web más frecuentadas para disminuir el tráfico del enlace a Internet.

RFC. (Request For Comments). Los RFC son una serie de documentos numerados publicados por la Internet Socierty que describen las ideas y conceptos de las tecnologías de Internet. No todos los RFC son estándares, pero muchos son aprobados explícitamente por el IETF, o en algún

momento se convierten en estándares de facto. Los RFC están disponibles en línea en http://rfc.net/.

RIR. (Regional Internet Registrars)**.** Los 4 mil millones de posibles direcciones IP son administrados por IANA. El espacio ha sido dividido entre grandes subredes, cuya administración ha sido delegada a alguna de las 5 entidades regionales llamadas Registrars, cada una con autoridad sobre una gran área geográfica. Por ejemplo, en América Latina y el Caribe es LACNIC.

Router. *Enrutador,* Dispositivo que reenvía paquetes entre diferentes redes. El proceso de reenviar paquetes hacia el próximo salto es llamado enrutamiento, ruteo o encaminamiento.

RP-TNC. Versión modificada del popular conector de microondas TNC con el género invertido, utilizado por los equipos fabricados por Linksys.

RTT. (Round Trip Time)**.** Tiempo de ida y vuelta. Cantidad de tiempo que le toma a un paquete para que la confirmación de su recepción llegue al transmisor. No confundir con la latencia.

Squid. Un web proxy cache muy popular. Es flexible, robusto, con muchas funcionalidades y puede adaptarse a redes de cualquier tamaño. http://www.squid-cache.org/.

SSL. (Secure Sockets Layer)**.** Tecnología de cifrado de extremo a extremo incorporada prácticamente en todos los navegadores de red (web browsers). SSL usa public key cryptography y una public key infrastructure para permitir comunicaciones seguras en la web.

Switch. Conmutador. Dispositivo de red que provee una conexión temporal dedicada entre nodos que se comunican.

TNC Connector. Un popular conector de rosca utilizado en microondas.

Traceroute / Tracert. Herramienta de diagnóstico ubicua usada a menudo en conjunción con ping para determinar la ubicación de un problema en la red. La versión Unix se llama traceroute, mientras que la versión Windows es tracert. Ambas usan paquetes ICMP de solicitud de eco que van incrementando el valor del TTL para determinar cuáles enrutadores se están usando para conectar al anfitrión remoto y también muestra las estadísticas de latencia.

TTL. (Time To Live). Tiempo de vida. En redes TCP/IP el TTL es un contador que empieza con cierto valor (tal como 64), y se decrementa en cada salto. Si el TTL llega a 0, el paquete se descarta.

U.FL. Diminuto conector de microondas utilizado por muchas tarjetas de radio mini-PCI.

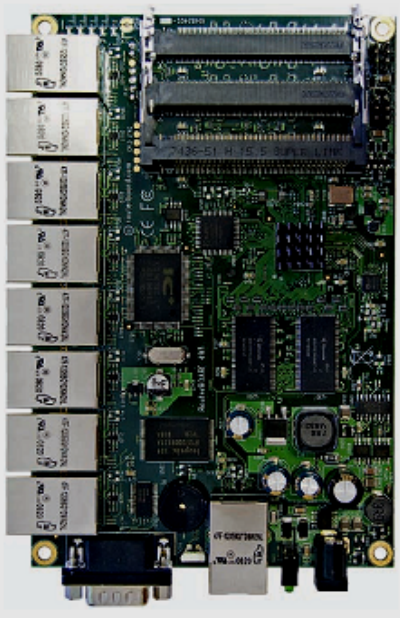
Wi-Fi. Marca comercial de propiedad de la WiFi Alliance usada para referirse a las tecnologías 802.11a, 802.11b, 802.11g y 802.11n. Wi-Fi es la abreviación de Wireless Fidelity.

WITFOR: Congreso bianual internacional que se orienta a la aplicación de las nuevas tecnologías para el desarrollo,

ANEXO B:
COMPONENTES Y CARACTERÍSTICAS TÉCNICAS

B.1.-RouterBoard (493AH)

RouterBOARD 493AH



The RB493AH has nine ethernet ports and three miniPCI slots, it also has a switch chip, so the ethernet ports of your choice can be grouped together to make it act as a switch.

The heart of this device is a new generation high performance Atheros CPU, much faster than the one found on the regular RB493.

RB493 includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/ **firewall or bandwidth manager.**

One small device - with all the power of RouterOS. At a very special price.

routerboard.com

CPU	Atheros AR7161 680MHz
Memory	128MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	Nine 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X
miniPCI	Three miniPCI slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC
Dimensions	105mm x 160mm, 189 grams
Power consumption	~3W without extension cards, maximum – 16 W
Operating System	MikroTik RouterOS v3, Level5 license

B.2.-Mikrotik R52N

Mikrotik R52N 802.11AGBN 65/100 mW 300 Mb/s

El adaptador MiniPCI RouterBOARD R52n ofrece el rendimiento líder en el estándar 802.11a/b/g/n tanto en la banda de 2.4 GHz como en 5GHz, soportando 300Mbps de velocidad y hasta 200Mbps de flujo real tanto en subida como en bajada. Añadiendo Wireless N a su dispositivo Wireless, aumenta la eficiencia en las aplicaciones diarias como la transferencia de ficheros, navegación en Internet y media streaming.

Características y Beneficios

- Doble banda IEEE 802.11a/b/g/n standard
- Potencia de salida de 25dBm @ Banda b/g/n
- Soporta hasta 2x2 MIMO con multiplexación espacial
- Hasta 4 veces más rápido que las opciones 802.11a/g
- Atheros AR9220, chipset
- Alto rendimiento (hasta 300Mbps en flujo de datos físico y 200Mbps de flujo real con un consumo realmente bajo.
- 2 X conectores de antena U.FL
- Modulaciones: OFDM: BPSK, QPSK, 16 QAM, 64QAM
DSSS: DBPSK, DQPSK, CCK
- Temperaturas de operación: 0ºC a 60ºC
- Consumo de energía: MAX 2.4W
- Protección ESD contra descargas en el puerto de antena de +/-10kV

Especificaciones

802.11a	RX Sensibilidad	TX Potencia
6Mbit	-97/-95	21
54Mbit	-80/-79	19
802.11n 5 GHz		
MCS0 MHz	-97/-95	21/19
MCS0 MHz	-93/-91	19
MCS7 MHz	-78/-76	16
MCS7 MHz	-75/-73	13

802.11b	RX Sensibilidad	TX Pot.
1Mbit	-95/-94	23
11Mbit	-92	23
802.11g		
6Mbit	-95/-94	25
54Mbit	-80	21
802.11n 2.4GHz		
MCS0 MHz	-95/-94	23
MCS0 MHz	-91	21
MCS7 MHz	-77	20

Velocidades

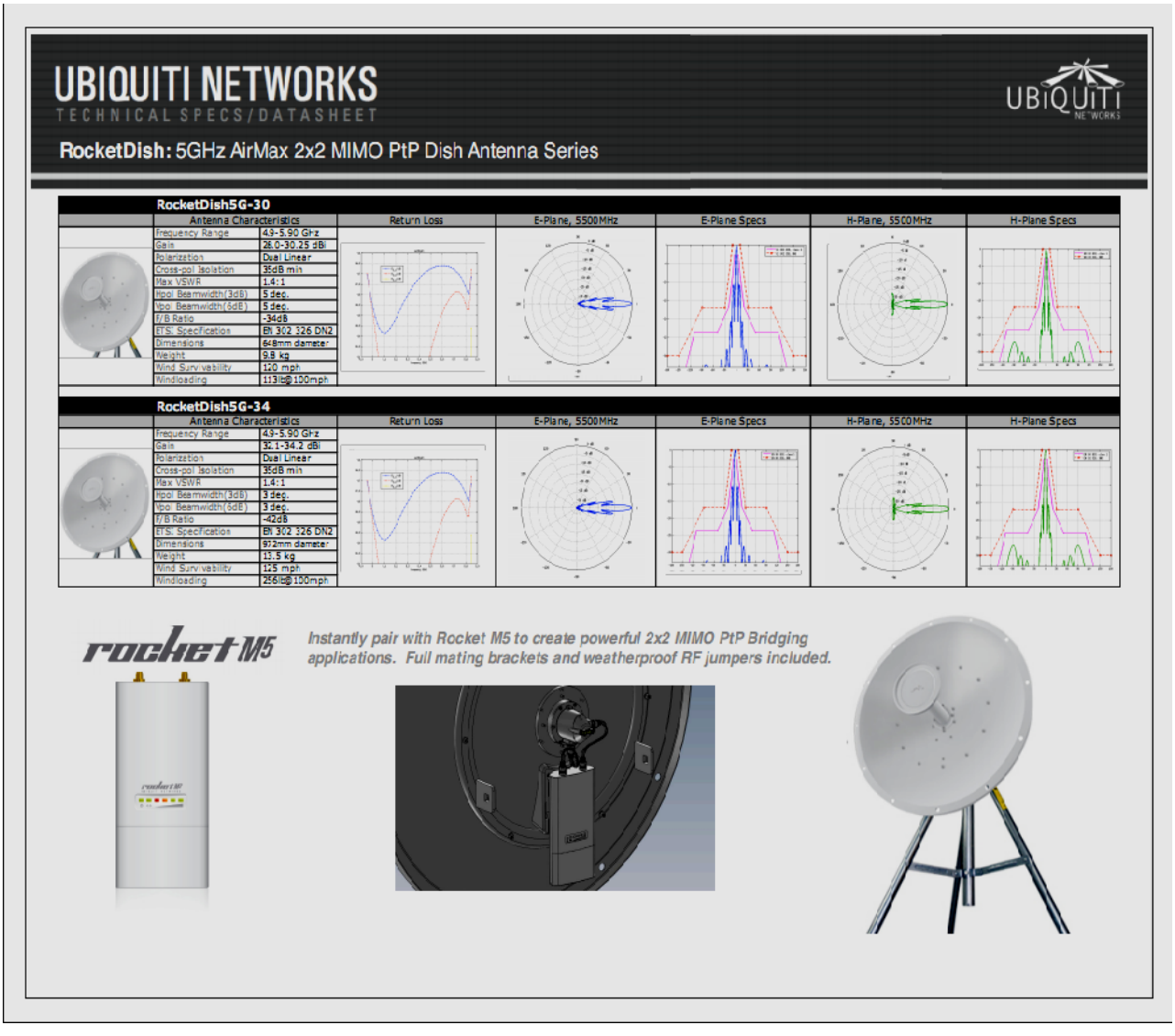
802.11B: 11Mbps; 5.5Mbps; 2Mbps; 1Mbps

802.11A/G: 54Mbps; 48Mbps; 36Mbps; 24Mbps; 18Mbps; 12Mbps; 9Mbps; 6Mbps

20MHz 1Nss: 65Mbps @ 800GI, 72.2Mbps @ 400GI (Max.)
2Nss: 130Mbps @ 800GI, 144.4Mbps @ 400GI (Max.)

40MHz 1Nss: 135Mbps @ 800GI, 150Mbps @ 400GI (Max.)
2Nss: 270Mbps @ 800GI, 300Mbps @ 400GI (Max.)

B.3.- Antena Parabólica (RocketDish)



UBIQUITI NETWORKS

TECHNICAL SPECS/DATASHEET

RocketDish: 5GHz AirMax 2x2 MIMO PtP Dish Antenna Series

RocketDish5G-30

Antenna Characteristics	
Frequency Range	4.9-5.90 Ghz
Gain	28.0-30.25 dBi
Polarization	Dual Linear
Cross-pol Isolation	35dB min
Max VSWR	1.4:1
Hpol Beamwidth(3dB)	5 deg.
Vpol Beamwidth(3dB)	5 deg.
F/B Ratio	-34dB
ETS Specification	EN 302 326 DN2
Dimensions	648mm diameter
Weight	9.8 kg
Wind Survivability	120 mph
Windloading	113lb@100mph

Return Loss | E-Plane, 5500MHz | E-Plane Specs | H-Plane, 5500MHz | H-Plane Specs

RocketDish5G-34

Antenna Characteristics	
Frequency Range	4.9-5.90 Ghz
Gain	32.1-34.2 dBi
Polarization	Dual Linear
Cross-pol Isolation	35dB min
Max VSWR	1.4:1
Hpol Beamwidth(3dB)	3 deg.
Vpol Beamwidth(3dB)	3 deg.
F/B Ratio	-42dB
ETS Specification	EN 302 326 DN2
Dimensions	972mm diameter
Weight	15.5 kg
Wind Survivability	125 mph
Windloading	256lb@100mph

Return Loss | E-Plane, 5500MHz | E-Plane Specs | H-Plane, 5500MHz | H-Plane Specs

rocket M5

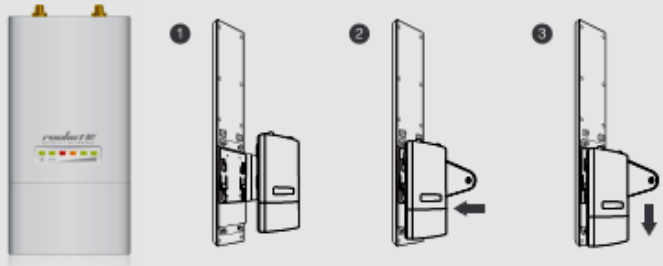
Instantly pair with Rocket M5 to create powerful 2x2 MIMO PtP Bridging applications. Full mating brackets and weatherproof RF jumpers included.

B.4.- Antena Parabólica (Rocket M5)

UBIQUITI NETWORKS

TECHNICAL SPECS/DATASHEET

ROCKET M5: 5GHz Hi Power 2x2 MIMO AirMax TDMA BaseStation



airMAX
MIMO TDMA Protocol

COMPATIBLE ANTENNAS

- AirMax Sector 5G-17-90
- AirMax Sector 5G-16-120
- AirMax Sector 5G-20-90
- AirMax Sector 5G-19-120
- Rocket Dish 5G-30

SYSTEM INFORMATION	
Processor Specs	Atheros MIPS 24KC, 400MHz
Memory Information	64MB SDRAM, 8MB Flash
Networking Interface	1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface

REGULATORY / COMPLIANCE INFORMATION	
Wireless Approvals	FCC Part 15.247, IC RS210, CE
RoHS Compliance	YES

OPERATING FREQUENCY 5470MHz-5825MHz

5GHz TX POWER SPECIFICATIONS

	DataRate	Avg. TX	Tolerance
11a	6-24Mbps	27 dBm	+/-2dB
	36Mbps	25 dBm	+/-2dB
	48Mbps	23 dBm	+/-2dB
	54Mbps	22 dBm	+/-2dB
5GHz 11n	MCS0	27 dBm	+/-2dB
	MCS1	27 dBm	+/-2dB
	MCS2	27 dBm	+/-2dB
	MCS3	27 dBm	+/-2dB
	MCS4	26 dBm	+/-2dB
	MCS5	24 dBm	+/-2dB
	MCS6	22 dBm	+/-2dB
	MCS7	21 dBm	+/-2dB
	MCS8	27 dBm	+/-2dB
	MCS9	27 dBm	+/-2dB
	MCS10	27 dBm	+/-2dB
	MCS11	27 dBm	+/-2dB
	MCS12	26 dBm	+/-2dB
	MCS13	24 dBm	+/-2dB
	MCS14	22 dBm	+/-2dB
	MCS15	21 dBm	+/-2dB

5GHz RX SPECIFICATIONS

	DataRate	Sensitivity	Tolerance
11a	6-24Mbps	-94 dBm min	+/-2dB
	36Mbps	-80 dBm	+/-2dB
	48Mbps	-77 dBm	+/-2dB
	54Mbps	-75 dBm	+/-2dB
5GHz 11n	MCS0	-96 dBm	+/-2dB
	MCS1	-95 dBm	+/-2dB
	MCS2	-92 dBm	+/-2dB
	MCS3	-90 dBm	+/-2dB
	MCS4	-86 dBm	+/-2dB
	MCS5	-83 dBm	+/-2dB
	MCS6	-77 dBm	+/-2dB
	MCS7	-74 dBm	+/-2dB
	MCS8	-95 dBm	+/-2dB
	MCS9	-93 dBm	+/-2dB
	MCS10	-90 dBm	+/-2dB
	MCS11	-87 dBm	+/-2dB
	MCS12	-84 dBm	+/-2dB
	MCS13	-79 dBm	+/-2dB
	MCS14	-78 dBm	+/-2dB
	MCS15	-75 dBm	+/-2dB

PHYSICAL / ELECTRICAL / ENVIRONMENTAL	
Enclosure Size	16cm length x 8cm width x 3cm height
Weight	0.5 kg
RF Connector	2x RPSMA (Waterproof)
Enclosure Characteristics	Outdoor UV Stabalized Plastic
Mounting Kit	Pole Mounting Kit included
Max Power Consumption	8 Watts
Power Supply	24V, 1A POE Supply Included
Power Method	Passive Power over Ethernet (pairs 4,5+; 7,8 return)
Operating Temperature	-30C to 75C
Operating Humidity	5 to 95% Condensing
Shock and Vibration	ETSI300-019-1.4

802.11n / Airmax Support Only at this Time. 802.11a support expected with AirOS 5.1 Release by end of Year

Ubiquiti Networks Inc., 91 E. Tasman Dr., San Jose, CA 95134 www.ubnt.com

B.5.-Antena Hotspot (NanoStation2)

UBIQUITI NETWORKS

NanoStation2

Datasheet

GLOBAL WISP ROI INITIATIVE

SYSTEM INFORMATION	
Processor Specs	Atheros AR2315 SOC, MIPS 4KC, 180MHz
Memory Information	16MB SDRAM, 4MB Flash
Networking Interface	1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface

REGULATORY / COMPLIANCE INFORMATION	
Wireless Approvals	FCC Part 15.247, IC RS210, CE
RoHS Compliance	YES

RADIO OPERATING FREQUENCY 2412-2462 MHz

TX SPECIFICATIONS

	DataRate	TX Power	Tolerance
802.11b	1Mbps	26 dBm	+/-1dB
	2Mbps	26 dBm	+/-1dB
	5.5Mbps	26 dBm	+/-1dB
	11Mbps	26 dBm	+/-1dB
802.11g OFDM	6Mbps	26 dBm	+/-1dB
	9Mbps	26 dBm	+/-1dB
	12Mbps	26 dBm	+/-1dB
	18Mbps	26 dBm	+/-1dB
	24Mbps	26 dBm	+/-1dB
	36Mbps	24 dBm	+/-1dB
	48Mbps	23 dBm	+/-1dB
	54Mbps	22 dBm	+/-1dB

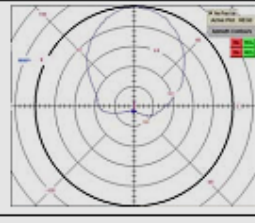
RX SPECIFICATIONS

	DataRate	Sensitivity	Tolerance
802.11b	1Mbps	-97 dBm	+/-1dB
	2Mbps	-96 dBm	+/-1dB
	5.5Mbps	-95 dBm	+/-1dB
	11Mbps	-92 dBm	+/-1dB
802.11g OFDM	6Mbps	-94 dBm	+/-1dB
	9Mbps	-93 dBm	+/-1dB
	12Mbps	-91 dBm	+/-1dB
	18Mbps	-90 dBm	+/-1dB
	24Mbps	-86 dBm	+/-1dB
	36Mbps	-83 dBm	+/-1dB
	48Mbps	-77 dBm	+/-1dB
	54Mbps	-74 dBm	+/-1dB

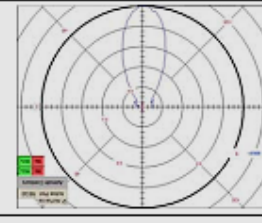
RANGE PERFORMANCE	
Outdoor (BaseStation Antenna Dependent):	Over 15km

INTEGRATED ADAPTIVE ANTENNA POLARITY + EXTERNAL ANTENNA SUPPORT (4 OPTIONS TOTAL)

Gain	10dBi (2400-2483.5MHz)	External Connector	RP-SMA
Polarization	Multi-Polarized	3dB Beamwidth Elevation	30 degrees
Polarization Selection	Software Controlled	3dB Beamwidth Azimuth	60 degrees



Azimuth



Elevation

PHYSICAL / ELECTRICAL / ENVIRONMENTAL	
Enclosure Size	26.4 cm x 8 cm x 3cm
Weight	0.4kg
Enclosure Characteristics	Outdoor UV Stabalized Plastic
Mounting Kit	Pole Mounting Kit included
Max Power Consumption	4 Watts
Power Supply	12V, 1A (12 Watts). Supply and injector included
Power Method	Passive Power over Ethernet (pairs 4,5+; 7,8 return)
Operating Temperature	-20C to +70C
Operating Humidity	5 to 95% Condensing
Shock and Vibration	ETSI300-019-1.4

SOFTWARE

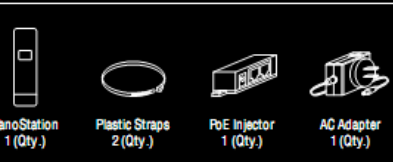
AirOS™ by Ubiquiti Networks

visit www.ubnt.com/airos

UBIQUITI NETWORKS
www.ubnt.com

UBIQUITI NETWORKS

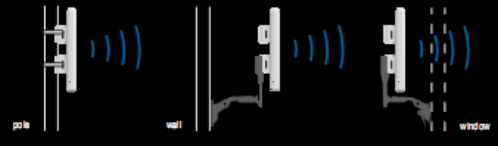
Package Contents

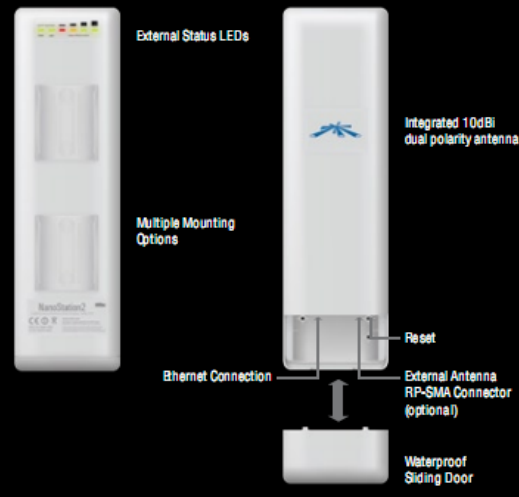


NanoStation 1 (Qty.) | Plastic Straps 2 (Qty.) | PoE Injector 1 (Qty.) | AC Adapter 1 (Qty.)

Mounting Options

1. Pole Mount (Standard) 2. Wall Mount (optional) 3. Window Mount (optional)





CPU	Atheros 180MHz MIPS
RAM	16MB RAM
Flash	4MB FLASH
Wireless	2.4GHz, 802.11b/g
Channel width	5/10/20MHz
Antenna Gain	10dBi x2
Polarity	Adaptive Vertical/Horizontal
Ext. Ant. Option	Yes, RP-SMA Connector
Range	15km+ (100km using ext ant.)
Throughput	25Mbps+ TCP/IP
Mounting	Pole Mount (straps included)
Accessories	Ubiquiti Window/Wall Mount (sold seperately)
Size	26.4cm x 8cm x 3cm
Weight	0.4 kg
Power Supply	12V, 1A POE (included)
Approvals	FCC 15.247, IC, CE

AirOS™ by Ubiquiti Networks

Air OS is an intuitive, versatile, highly developed Ubiquiti firmware technology that is included with NanoStation.

It is exceptionally intuitive and was designed to require no training to operate. Behind the user interface is a powerful firmware architecture which enables hi-performance outdoor multipoint networking.

AAP TECHNOLOGY

NanoStation utilizes Adaptive Antenna Polarity technology, which can statically or dynamically software switch antenna polarities to optimize your connections.

NanoStation2
www.ubnt.com

B.6.- Antena Sectorial (Interline INT-SEC-17/50)

Interline INT-SEC-17/50-V SECTOR VP MAXI 5Ghz - Base Station Ant

technical specification

Electrical

Gain.....17 dBi
Frequency.....5150 - 5850 MHz
Polarization.....vertical
Polarization isolation.....>13 dB
Front/Back ratio.....>30 dB
(-3dB) horizontal.....(-5dB)90°
(-3dB) vertical.....8°
VSWR.....1.5:1
Impedance.....50 OHm

Mechanical

Connector.....N female
Dimension.....428 x 85 x 10 mm
Weight.....0,5 kg
Mounting.....fi 38÷51

B.7.- Cable coaxial (RF 5 GHz)

Cable 3 m. RF 5 GHz. N-Macho/N-Macho [WRL-CBL-53NN]

Atenuación :

MHz - db/100m
50 – 2.9
100 – 3.9
200 – 5.7
400 – 7.5
900 – 13.0
1000 - 13.6
1500 – 17.0
2000 – 20.1
2500 – 23.2
5800 – 38.0

Conductor AWG(mm): 2.74 mm Solid Copper Clad Aluminum
Insulation Nominal O.D. mm: 7.24 mm Gas Injected Foam PE
Funda estándar O.D. mm: 10.3 mm Black PE
Material de protección y cubierta: Bonded Aluminum Foil + 95% Tinned Copper Braid
Impedancia Ohm: 50
Velocidad de propagación : 85%
Atenuación PF/m: 80

B.8.- Pigtail

Pigtail U.FL a N-Hembra Bulkhead, 30 cm LMR178

- Pigtail U.FL a N-Hembra Bulkhead, 30cms
- Mini-PCI Compatible (EMP-8602, EMP-8602PLUS-S, R52N, R52Hn, etc..)
- U.FL/iPax/Hirose Conector mini-PCI Compatible
- Longitud: 12" (30cm)

ANEXO C:
SCRIPTS Y ARCHIVOS DE CONFIGURACIÓN

C.1.- Scripts de configuración "Unsolclic"

C.1.1. Configuración del Mikrotik (RouterOS) de UPVone

```
      # Generat per a:
# RouterOSv4.7+
:log info "Unsolclic for 27405-valupvgrcRd1 going to be executed."
#
# Configuration for RouterOS 4.7 and newer
# Trasto: 27405-valupvgrcRd1
#
# ATENCIÓ: Versió Beta
#
# Methods to upload/execute this script:
# 1.-As a script. Upload this output as a script either with:
#    a.Winbox (with Linux, wine required)
#    b.Terminal (telnet, ssh...)
#   Then execute the script with:
#    > /system script run script_name
# 2.-Fitxer importat:
#    Desa aquesta "sortida" a un fitxer, després puja'l al router
#    fent servir FTP amb un nom de l'estil "script_name.rsc".
#    (note, l'extensió ".rsc" es un requisit)
#    Executa el fitxer importat amb la comanda:
#    > /import script_name
# 3.-Telnet copia i enganxar:
#    Open a terminal session, and cut&paste this output
#    directly on the terminal input.
#
# Notes:
# -routing-test package is required, be sure you have it enabled at system packages
# -wlans should be enabled manually, be sure to set the correct antenna (a or b)
#   according in how did you connect the cable to the miniPCI. Keep the
#   power at the minimum possible and check the channel.
# -The script doesn't reset the router, you might have to do it manually
# -You must have write access to the router
# -MAC access (winbox, MAC telnet...) method is recommended
#   (the script reconfigures some IP addresses, so communication can be lost)
# -No changes are done in user passwords on the device
# -A Read Only guest account with no password will be created to allow guest access
#   to the router with no danger of damage but able to see the config.
# -Be sure that all packages are activated.
# -Don't run the script from telnet and being connected through an IP connection at
#   the wLan/Lan interface: This interface will be destroyed during the script.
#
/ system identity set name=valupvgrcRd1
#
# DNS (client & server cache) zone: 20145
:delay 1
#
# NTP (client & server cache) zone: 20145
:delay 1
#
# Bandwidth-server
/ tool bandwidth-server set enabled=yes authenticate=no allocate-udp-ports-from=2000
#
```

```
# SNMP
/snmp set contact="guifi@guifi.net" enabled=yes location="valupvgrc"
#
# Guest user
/user
:foreach i in [find group=read] do={/user remove $i;}
add name="guest" group=read address=0.0.0.0/0 comment="" disabled=no
      #
# Graphing
/tool graphing interface add
# Remove current wLan/Lan bridge if exists
:foreach i in [/interface bridge find name=wLan/Lan] \
do={:foreach i in [/interface bridge port find bridge=wLan/Lan] \
do={/interface bridge port remove $i; \
:foreach i in [/ip address find interface=wLan/Lan] \
do={/ip address remove $i;};};
/interface bridge remove $i;}
# Construct main bridge on wlan1 & ether1
/ interface bridge
add name="wLan/Lan"
/ interface bridge port
add interface=ether1 bridge=wLan/Lan
add interface=wlan1 bridge=wLan/Lan
:delay 1
#
# Radio#: 0 VLCupvAP0-270
/interface wireless set wlan1 name="wlan1" \
radio-name="VLCupvAP0-270" mode=ap-bridge ssid="guifi.net-VLCupvAP0-270" \
band="5ghz" \
frequency-mode=regulatory-domain country=spain antenna-gain=17 \
frequency=5320 \
dfs-mode=none \
antenna-mode=ant-a wds-mode=static wds-default-bridge=none wds-default-cost=100 \
wds-cost-range=50-150 wds-ignore-ssid=yes hide-ssid=no
:delay 1
# Type: wLan/Lan
/ip address
:foreach i in [find address="10.228.154.97/27"] do={remove $i}
/ ip address add address=10.228.154.97/27 network=10.228.154.96 broadcast=10.228.154.127 interface=wLan/Lan
disabled=no
/ routing ospf interface
:foreach i in [/routing ospf interface find interface=wLan/Lan] do={/routing ospf interface remove $i;}
add interface=wLan/Lan
/ routing ospf network
:foreach i in [/routing ospf network find network=10.228.154.96/27] do={/routing ospf network remove $i;}
add network=10.228.154.96/27 area=backbone disabled=no
/ip address
:foreach i in [find address="10.228.154.225/29"] do={remove $i}
/ ip address add address=10.228.154.225/29 network=10.228.154.224 broadcast=10.228.154.231 interface=wLan/Lan
disabled=no
/ routing ospf interface
:foreach i in [/routing ospf interface find interface=wLan/Lan] do={/routing ospf interface remove $i;}
add interface=wLan/Lan
/ routing ospf network
:foreach i in [/routing ospf network find network=10.228.154.224/29] do={/routing ospf network remove $i;}
add network=10.228.154.224/29 area=backbone disabled=no
:delay 1
#
# DHCP
:foreach i in [/ip pool find name=dhcp-wLan/Lan] do={/ip pool remove $i;}
/ip pool add name=dhcp-wLan/Lan ranges=10.228.154.230-10.228.154.230
:foreach i in [/ip dhcp-server find name=dhcp-wLan/Lan] do={/ip dhcp-server remove $i;}
/ip dhcp-server add name=dhcp-wLan/Lan interface=wLan/Lan address-pool=dhcp-wLan/Lan disabled=yes
:foreach i in [/ip dhcp-server network find address="10.228.154.224/29"] do={/ip dhcp-server network remove $i;}
/ip dhcp-server network add address=10.228.154.224/29 gateway=10.228.154.225 domain=guifi.net comment=dhcp-
wLan/Lan
/ip dhcp-server lease
```

```
:foreach i in [find comment=""] do={remove $i;}
:delay 1
#
:delay 1
# Type: wds/p2p
# Remove all existing wds interfaces
:foreach i in [/interface wireless wds find master-interface=wlan1] \
do={:foreach n in [/interface wireless wds get $i name] \
do={:foreach inum in [/ip address find interface=$n] \
do={/ip address remove $inum;};}; \
/interface wireless wds remove $i;}
#
:delay 1
#
# Radio#: 1 VLCupvAP1-180
/interface wireless set wlan2 name="wlan2" \
radio-name="VLCupvAP1-180" mode=ap-bridge ssid="guifi.net-VLCupvAP1-180" \
band="5ghz" \
frequency-mode=regulatory-domain country=spain antenna-gain=17 \
frequency=5500 \
dfs-mode=none \
antenna-mode=ant-a wds-mode=static wds-default-bridge=none wds-default-cost=100 \
wds-cost-range=50-150 wds-ignore-ssid=yes hide-ssid=no
:delay 1
# Type: wLan
/ip address
:foreach i in [find address="10.228.154.161/27"] do={remove $i}
/ ip address add address=10.228.154.161/27 network=10.228.154.160 broadcast=10.228.154.191 interface=wlan2
disabled=no
/ routing ospf interface
:foreach i in [/routing ospf interface find interface=wlan2] do={/routing ospf interface remove $i;}
add interface=wlan2
/ routing ospf network
:foreach i in [/routing ospf network find network=10.228.154.160/27] do={/routing ospf network remove $i;}
add network=10.228.154.160/27 area=backbone disabled=no
:delay 1
#
# DHCP
:foreach i in [/ip pool find name=dhcp-wlan2] do={/ip pool remove $i;}
/ip pool add name=dhcp-wlan2 ranges=10.228.154.167-10.228.154.190
:foreach i in [/ip dhcp-server find name=dhcp-wlan2] do={/ip dhcp-server remove $i;}
/ip dhcp-server add name=dhcp-wlan2 interface=wlan2 address-pool=dhcp-wlan2 disabled=no
:foreach i in [/ip dhcp-server network find address="10.228.154.160/27"] do={/ip dhcp-server network remove $i;}
/ip dhcp-server network add address=10.228.154.160/27 gateway=10.228.154.161 domain=guifi.net comment=dhcp-wlan2
/ip dhcp-server lease
:foreach i in [find comment=""] do={remove $i;}
:delay 1
#
:delay 1
# Type: wds/p2p
# Remove all existing wds interfaces
:foreach i in [/interface wireless wds find master-interface=wlan2] \
do={:foreach n in [/interface wireless wds get $i name] \
do={:foreach inum in [/ip address find interface=$n] \
do={/ip address remove $inum;};}; \
/interface wireless wds remove $i;}
#
:delay 1
#
# Radio#: 2 VLCupvAP2-90
/interface wireless set wlan3 name="wlan3" \
radio-name="VLCupvAP2-90" mode=ap-bridge ssid="guifi.net-VLCupvAP2-90" \
band="5ghz" \
frequency-mode=regulatory-domain country=spain antenna-gain=17 \
frequency=5520 \
dfs-mode=none \
```

```
antenna-mode=ant-a wds-mode=static wds-default-bridge=none wds-default-cost=100 \
wds-cost-range=50-150 wds-ignore-ssid=yes hide-ssid=no
:delay 1
# Type: wLan
/ip address
:foreach i in [find address="10.228.154.193/27"] do={remove $i}
/ ip address add address=10.228.154.193/27 network=10.228.154.192 broadcast=10.228.154.223 interface=wlan3
disabled=no
/ routing ospf interface
:foreach i in [/routing ospf interface find interface=wlan3] do={/routing ospf interface remove $i;}
add interface=wlan3
/ routing ospf network
:foreach i in [/routing ospf network find network=10.228.154.192/27] do={/routing ospf network remove $i;}
add network=10.228.154.192/27 area=backbone disabled=no
:delay 1
#
# DHCP
:foreach i in [/ip pool find name=dhcp-wlan3] do={/ip pool remove $i;}
/ip pool add name=dhcp-wlan3 ranges=10.228.154.199-10.228.154.222
:foreach i in [/ip dhcp-server find name=dhcp-wlan3] do={/ip dhcp-server remove $i;}
/ip dhcp-server add name=dhcp-wlan3 interface=wlan3 address-pool=dhcp-wlan3 disabled=no
:foreach i in [/ip dhcp-server network find address="10.228.154.192/27"] do={/ip dhcp-server network remove $i;}
/ip dhcp-server network add address=10.228.154.192/27 gateway=10.228.154.193 domain=guifi.net comment=dhcp-wlan3
/ip dhcp-server lease
:foreach i in [find comment=""] do={remove $i;}
:delay 1
#
:delay 1
# Type: wds/p2p
# Remove all existing wds interfaces
:foreach i in [/interface wireless wds find master-interface=wlan3] \
do={:foreach n in [/interface wireless wds get $i name] \
do={:foreach inum in [/ip address find interface=$n] \
do={/ip address remove $inum;};}; \
/interface wireless wds remove $i;}
#
:delay 1
#
# Radio#: 3 VLCupvHOTSPOT1
/interface wireless set wlan4 name="wlan4" \
radio-name="VLCupvHOTSPOT1" mode=ap-bridge ssid="guifi.net-VLCupvHOTSPOT1" \
band="2.4ghz-b" \
frequency-mode=regulatory-domain country=spain antenna-gain=14 \
frequency=2437 \
dfs-mode=none \
antenna-mode=ant-a wds-mode=static wds-default-bridge=none wds-default-cost=100 \
wds-cost-range=50-150 wds-ignore-ssid=yes hide-ssid=no
:delay 1
# Type: wds/p2p
# Remove all existing wds interfaces
:foreach i in [/interface wireless wds find master-interface=wlan4] \
do={:foreach n in [/interface wireless wds get $i name] \
do={:foreach inum in [/ip address find interface=$n] \
do={/ip address remove $inum;};}; \
/interface wireless wds remove $i;}
#
:delay 1
#
# Radio#: 4 VLCupvT0-031
/interface wireless set wlan5 name="wlan5" \
radio-name="VLCupvT0-031" mode=ap-bridge ssid="guifi.net-VLCupvT0-031" \
band="5ghz" \
frequency-mode=regulatory-domain country=spain antenna-gain=30 \
frequency=5700 \
dfs-mode=none \
antenna-mode=ant-a wds-mode=static wds-default-bridge=none wds-default-cost=100 \
wds-cost-range=50-150 wds-ignore-ssid=yes hide-ssid=no
```

```
:delay 1
# Type: wds/p2p
# Remove all existing wds interfaces
:foreach i in [/interface wireless wds find master-interface=wlan5] \
do={:foreach n in [/interface wireless wds get $i name] \
do={:foreach inum in [/ip address find interface=$n] \
do={/ip address remove $inum;};}; \
/interface wireless wds remove $i;}
#
:delay 1
#
# Routed device
#
# Altres connexions de cable
#
# Internal addresses NAT
:foreach i in [/ip firewall nat find src-address="172.16.0.0/12"] do={/ip firewall nat remove $i;}
:foreach i in [/ip firewall nat find src-address="192.168.0.0/16"] do={/ip firewall nat remove $i;}
/ip firewall nat
add chain=srcnat src-address="192.168.0.0/16" dst-address=!192.168.0.0/16 action=src-nat to-addresses=10.228.154.225
comment="" disabled=no
add chain=srcnat src-address="172.16.0.0/12" dst-address=!172.16.0.0/12 protocol=!ospf action=src-nat to-
addresses=10.228.154.225 comment="" disabled=no
#
# Enrutament BGP
# Filtres BGP i OSPF
:foreach i in [/routing filter find chain=ospf-in] do={/routing filter remove $i;}
:foreach i in [/routing filter find chain=ospf-out] do={/routing filter remove $i;}
/ routing filter
add chain=ospf-out prefix=10.0.0.0/8 prefix-length=8-32 invert-match=no action=accept comment="" disabled=no
add chain=ospf-out invert-match=no action=discard comment="" disabled=no
add chain=ospf-in prefix=10.0.0.0/8 prefix-length=8-32 invert-match=no action=accept comment="" disabled=no
add chain=ospf-in invert-match=no action=reject comment="" disabled=no
#
# Instància BGP
/ routing bgp instance
set default name="default" as=27405 router-id=10.228.154.225 redistribute-static=yes \
redistribute-connected=yes redistribute-rip=yes redistribute-ospf=yes \
redistribute-other-bgp=yes out-filter=ospf-out \
client-to-client-reflection=yes comment="" disabled=no
#
# Enrutament OSPF
/routing ospf instance set default name=default router-id=10.228.154.225 comment="" disabled=no distribute-default=never
redistribute-bgp=as-type-1 redistribute-connected=no redistribute-other-ospf=no redistribute-rip=no redistribute-static=no in-
filter=ospf-in out-filter=ospf-out
#
:log info "Unsolclic for 27405-valupvgrcRd1 executed."

/
```

C.1.2. Configuración del NanoStation (AirOS) de UPVdos

```
aaa.1.status=disabled
aaa.status=disabled
bridge.1.devname=br0
bridge.1.fd=1
bridge.1.port.1.devname=eth0
bridge.1.port.2.devname=ath0
bridge.status=disabled
dhcpc.1.devname=br0
dhcpc.1.status=disabled
dhcpc.status=disabled
dhcpd.1.devname=eth0
dhcpd.1.end=192.168.1.254
dhcpd.1.lease_time=3600
```

```
dhcpd.1.netmask=255.255.255.0
dhcpd.1.start=192.168.1.33
dhcpd.1.status=enabled
dhcpd.status=enabled
ebtables.1.cmd=-t nat -A PREROUTING --in-interface ath0 -j arpnat --arpnat-target ACCEPT
ebtables.1.status=enabled
ebtables.2.cmd=-t nat -A POSTROUTING --out-interface ath0 -j arpnat --arpnat-target ACCEPT
ebtables.2.status=enabled
ebtables.3.cmd=-t broute -A BROUTING --protocol 0x888e --in-interface ath0 -j DROP
ebtables.3.status=enabled
ebtables.status=disabled
httpd.https.status=enabled
httpd.port.http=80
httpd.status=enabled
iptables.1.status=enabled
iptables.1.cmd=-t nat -I POSTROUTING -o ath0 -j MASQUERADE
iptables.2.status=disabled
iptables.status=enabled
netconf.1.devname=eth0
netconf.1.ip=192.168.1.1
netconf.1.netmask=255.255.255.0
netconf.1.promisc=enabled
netconf.1.status=enabled
netconf.1.up=enabled
netconf.2.allmulti=enabled
netconf.2.devname=ath0
netconf.2.status=enabled
netconf.2.up=enabled
netconf.3.devname=br0
netconf.3.ip=192.168.1.20
netconf.3.netmask=255.255.255.0
netconf.3.status=disabled
netconf.3.up=enabled
netconf.status=enabled
netmode=router
ppp.1.password=
ppp.1.status=disabled
ppp.status=disabled
radio.1.ack.auto=enabled
radio.1.ackdistance=450
radio.1.ani.status=enabled
radio.1.chanshift=0
radio.1.clksel=0
radio.1.countrycode=724
radio.1.devname=ath0
radio.1.frag=off
radio.1.mode=managed
radio.1.rate.auto=enabled
radio.1.rts=off
radio.1.tx_antenna_diversity=disabled
radio.1.rx_antenna_diversity=disabled
radio.1.status=enabled
radio.1.thresh62a=28
radio.1.thresh62b=28
radio.1.thresh62g=28
radio.ratemodule=ath_rate_minstrel
radio.countrycode=724
radio.status=enabled
```

resolv.host.1.status=enabled
resolv.nameserver.1.status=enabled
resolv.nameserver.2.status=enabled
resolv.status=enabled
route.1.devname=ath0
route.1.ip=0.0.0.0
route.1.netmask=0
route.1.status=enabled
route.status=enabled
snmp.community=public
snmp.contact=guifi@guifi.net
snmp.status=enabled
telnetd.status=enabled
sshd.status=enabled
tshaper.status=disabled
users.1.name=root
users.1.password=JjYNUu92yMZd.
users.1.status=enabled
users.status=enabled
wireless.1.ap=
wireless.1.authmode=1
wireless.1.compression=0
wireless.1.devname=ath0
wireless.1.fastframes=0
wireless.1.frameburst=0
wireless.1.hide_ssid=disabled
wireless.1.l2_isolation=enabled
wireless.1.macclone=disabled
wireless.1.rssi_led1=1
wireless.1.rssi_led2=15
wireless.1.rssi_led3=22
wireless.1.rssi_led4=30
wireless.1.security=none
wireless.1.status=enabled
wireless.1.wds=disabled
wireless.1.wmm=disabled
wireless.1.wmmlevel=-1
wireless.status=enabled
wpasupplicant.device.1.status=disabled
wpasupplicant.status=disabled
wireless.1.ssid=guifi.net-VLCupvAP1-180
netconf.2.ip=10.228.154.162
netconf.2.netmask=255.255.255.224
route.1.gateway=10.228.154.161
resolv.nameserver.1.ip=10.228.154.2
resolv.nameserver.2.ip=10.37.72.3
resolv.host.1.name=UPVdosRd1
snmp.location=UPVdos
radio.1.ieee_mode=a
radio.1.rate.max=54M
radio.1.txpower=6
radio.1.acktimeout=25
radio.1.rx_antenna=2
radio.1.tx_antenna=2
radio.1.ext_antenna=disabled
radio.1.mcastrate=54

C.2.- Archivos de configuración de servicios

C.2.1. Servidor de DNS (Dnsmasq)

C.2.1.1. */etc/dnsmasq.conf* (solo líneas importantes no comentadas)

```
# Change this line if you want dns to get its upstream servers from
# somewhere other that /etc/resolv.conf
resolv-file=/etc/resolv.conf
listen-address=10.228.154.229,10.228.154.2,10.37.72.3,158.42.215.20,127.0.0.1
strict-order
# The example below send any host in doubleclick.net to a local
# webserver.
address=/guifi.net/10.228.154.229
address=/upv.es/158.42.215.20
```

C.2.1.2. /etc/resolv.conf

```
nameserver 10.228.154.229
nameserver 10.228.154.2
nameserver 10.37.72.3
nameserver 158.42.249.8
nameserver 158.42.1.8
nameserver 127.0.0.1
#domain upv.es
#search upv.es
search Teclee la dirección
```

C.2.1.3. /etc/host

```
10.228.154.229 vlcupvgrc.guifi.net
10.228.154.228 valupvvpn.guifi.net
10.228.154.227 vlcupvto-031.guifi.net
10.228.154.226 vlcupvhotspot1.guifi.net
10.228.154.225 valupvgrcRd1.guifi.net
10.228.154.97 valupvgrcRd1.guifi.net vlcupvap0-270.guifi.net
10.228.154.161 vlcupvap0-180.guifi.net
10.228.154.193 vlcupvap0-90.guifi.net
10.228.130.162 castellon.guifi.net

127.0.0.1 localhost
127.0.1.1 VLCupvGRC.guifi.net VLCupvGRC

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

C.2.2 Servidor de gráficas para la web de Guifi.net

C.2.2.1. /etc/snpservices/config.php

```
<?php
// snp_pat: full directory where snp services are located
$snp_path='/var/www/snpservices';
```

```
// SNPGraphServerID: Default Graph Server ID
$SNPGraphServerId = 37002;
// rootZone: which is the ROOT zone
$rootZone = 3671;
// SNPDataServer_url: without ending backslash, the url where the data is
$SNPDataServer_url =  'http://guifi.net';
// MRTGConfigSource: mrtg csv data
// As a input, could be either a local (to be created from
// cached CNML file, or remote
// $MRTGConfigSource='http://www.guifi.net/snpservices/graphs/cnml2mrtgcsv.php';
$MRTGConfigSource='http://www.guifi.net/snpservices/graphs/cnml2mrtgcsv.php?server='.$SNPGraphServerId;
// $MRTGConfigSource='/var/lib/snpservices/data/guifi_mrtg.csv';
// CNMLSource: url for CNML node query, use sprintf syntax
// MySQL-drupal source
// $CNMLSource='http://proves.elserrat.guifi.net/guifi/cnml/%s/node';
// Cached CNML source (prefered)
$CNMLSource='http://www.guifi.net/snpservices/common/qnodes.php?nodes=%s';
$CNMLData='/var/lib/snpservices/data/guifi.cnml';
// rrdtool parameters
$rrdtool_path='/usr/bin/rrdtool';
$rrddb_path='/var/lib/snpservices/rrdb/';
$rrdimg_path='/var/lib/snpservices/rrimg/';
// which version does have this server?
// currently supported versions are:
// 1.2
// 1.3
$rrdtool_version = '1.3';
// mrtg local header
$rrdtool_header='# PathAdd: /usr/local/rrdtool-1.2.12/bin
# LibAdd: /usr/local/rrdtool-1.2.12/lib/perl/5.8.8/i386-linux-thread-multi
HtmlDir: %s
ImageDir: %s
LogDir: %s
LogFormat: rrdtool
ThreshDir: %s
Forks: 25
';
// mrtg ping template
$mrtg_ping_template ='Title[%s_ping]: Temps del ping de %s
PageTop[%s_ping]: <H1>Lat&egrave;ncia %s</H1>
    <TABLE
    <TR><TD>System:</TD>     <TD>%s</TD></TR>
    <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
    <TR><TD>Description:</TD><TD>ping</TD></TR>
    <TR><TD>IP:</TD>         <TD>%s</TD></TR>
    </TABLE>
Target[%s_ping]: `/usr/share/snpservices/common/ping.sh %s`
MaxBytes[%s_ping]: 2000
Options[%s_ping]: growright,unknaszero,nopercent,gauge
LegendI[%s_ping]: Perduts %
LegendO[%s_ping]: Temps mig
Legend1[%s_ping]: Temps max. en ms
Legend2[%s_ping]: Temps min. en ms
YLegend[%s_ping]: RTT (ms)
';
$mrtg_traffic_template='Target[%s_traf]: %s:public@%s:
SetEnv[%s_traf]: MRTG_INT_IP="%s" MRTG_INT_DESCR="%s"
MaxBytes[%s_traf]: 3000000
Title[%s_traf]: Trafic a %s de %s
PageTop[%s_traf]: <H1>Tr&agrave;fic a %s de %s</H1>
    <TABLE>
    <TR><TD>System:</TD>     <TD>%s</TD></TR>
    <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
    <TR><TD>Description:</TD><TD>%s</TD></TR>
    <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
    </TABLE>
```

';
?>

C.2.2.2. /var/www/snpservices/data/mrtg.cfg

```
# PathAdd: /usr/local/rrdtool-1.2.12/bin
# LibAdd: /usr/local/rrdtool-1.2.12/lib/perl/5.8.8/i386-linux-thread-multi
HtmlDir: /var/lib/snpservices/rrimg/
ImageDir: /var/lib/snpservices/rrimg/
LogDir: /var/lib/snpservices/rrdb/
LogFormat: rrdtool
ThreshDir: /var/lib/snpservices/rrdb/
Forks: 25
Title[27405_ping]: Temps del ping de #valupvgrcRd1
PageTop[27405_ping]: <H1>Lat&egrave;ncia #valupvgrcRd1</H1>
    <TABLE
    <TR><TD>System:</TD>     <TD>#valupvgrcRd1</TD></TR>
    <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
    <TR><TD>Description:</TD><TD>ping</TD></TR>
    <TR><TD>IP:</TD>         <TD>10.228.154.97</TD></TR>
    </TABLE>
Target[27405_ping]: `/usr/share/snpservices/common/ping.sh 10.228.154.97`
MaxBytes[27405_ping]: 2000
Options[27405_ping]: growright,unknaszero,nopercent,gauge
LegendI[27405_ping]: Perduts LegendO[27405_ping]: Temps mig
Legend1[27405_ping]: Temps max. en ms
Legend2[27405_ping]: Temps min. en ms
YLegend[27405_ping]: RTT (ms)
Target[27405-0_traf]: \wlan1:public@10.228.154.97:
SetEnv[27405-0_traf]: MRTG_INT_IP="10.228.154.97" MRTG_INT_DESCR="#valupvgrcRd1"
MaxBytes[27405-0_traf]: 3000000
Title[27405-0_traf]: Trafic a VLCupvAP0-270 de #valupvgrcRd1
PageTop[27405-0_traf]: <H1>Tr&agrave;fic a VLCupvAP0-270 de #valupvgrcRd1</H1>
    <TABLE>
    <TR><TD>System:</TD>     <TD>#valupvgrcRd1</TD></TR>
    <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
    <TR><TD>Description:</TD><TD>VLCupvAP0-270</TD></TR>
    <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
    </TABLE>
Target[27405-1_traf]: \wlan2:public@10.228.154.97:
SetEnv[27405-1_traf]: MRTG_INT_IP="10.228.154.97" MRTG_INT_DESCR="#valupvgrcRd1"
MaxBytes[27405-1_traf]: 3000000
Title[27405-1_traf]: Trafic a VLCupvAP1-180 de #valupvgrcRd1
PageTop[27405-1_traf]: <H1>Tr&agrave;fic a VLCupvAP1-180 de #valupvgrcRd1</H1>
    <TABLE>
    <TR><TD>System:</TD>     <TD>#valupvgrcRd1</TD></TR>
    <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
    <TR><TD>Description:</TD><TD>VLCupvAP1-180</TD></TR>
    <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
    </TABLE>
Target[27405-2_traf]: \wlan3:public@10.228.154.97:
SetEnv[27405-2_traf]: MRTG_INT_IP="10.228.154.97" MRTG_INT_DESCR="#valupvgrcRd1"
MaxBytes[27405-2_traf]: 3000000
Title[27405-2_traf]: Trafic a VLCupvAP2-90 de #valupvgrcRd1
PageTop[27405-2_traf]: <H1>Tr&agrave;fic a VLCupvAP2-90 de #valupvgrcRd1</H1>
    <TABLE>
    <TR><TD>System:</TD>     <TD>#valupvgrcRd1</TD></TR>
    <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
    <TR><TD>Description:</TD><TD>VLCupvAP2-90</TD></TR>
```

```
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Target[27405-3_traf]: \wlan4:public@10.228.154.97:
SetEnv[27405-3_traf]: MRTG_INT_IP="10.228.154.97" MRTG_INT_DESCR="#valupvgrcRd1"
MaxBytes[27405-3_traf]: 3000000
Title[27405-3_traf]: Trafic a VLCupvHOTSPOT1 de #valupvgrcRd1
PageTop[27405-3_traf]: <H1>Tr&agrave;fic a VLCupvHOTSPOT1 de #valupvgrcRd1</H1>
   <TABLE>
   <TR><TD>System:</TD>     <TD>#valupvgrcRd1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>VLCupvHOTSPOT1</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Target[27405-4_traf]: \wlan5:public@10.228.154.97:
SetEnv[27405-4_traf]: MRTG_INT_IP="10.228.154.97" MRTG_INT_DESCR="#valupvgrcRd1"
MaxBytes[27405-4_traf]: 3000000
Title[27405-4_traf]: Trafic a VLCupvT0-031 de #valupvgrcRd1
PageTop[27405-4_traf]: <H1>Tr&agrave;fic a VLCupvT0-031 de #valupvgrcRd1</H1>
   <TABLE>
   <TR><TD>System:</TD>     <TD>#valupvgrcRd1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>VLCupvT0-031</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Title[28464_ping]: Temps del ping de #vlcupvgrc
PageTop[28464_ping]: <H1>Lat&egrave;ncia #vlcupvgrc</H1>
   <TABLE
   <TR><TD>System:</TD>     <TD>#vlcupvgrc</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>ping</TD></TR>
   <TR><TD>IP:</TD>         <TD>10.228.154.229</TD></TR>
   </TABLE>
Target[28464_ping]: `/usr/share/snpservices/common/ping.sh 10.228.154.229`
MaxBytes[28464_ping]: 2000
Options[28464_ping]: growright,unknaszero,nopercent,gauge
LegendI[28464_ping]: Perduts LegendO[28464_ping]: Temps mig
Legend1[28464_ping]: Temps max. en ms
Legend2[28464_ping]: Temps min. en ms
YLegend[28464_ping]: RTT (ms)
Target[28464-0_traf]: \eth0:public@10.228.154.229:
SetEnv[28464-0_traf]: MRTG_INT_IP="10.228.154.229" MRTG_INT_DESCR="#vlcupvgrc"
MaxBytes[28464-0_traf]: 3000000
Title[28464-0_traf]: Trafic a  de #vlcupvgrc
PageTop[28464-0_traf]: <H1>Tr&agrave;fic a  de #vlcupvgrc</H1>
   <TABLE>
   <TR><TD>System:</TD>     <TD>#vlcupvgrc</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD></TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Title[37920_ping]: Temps del ping de #UPVdosRd1
PageTop[37920_ping]: <H1>Lat&egrave;ncia #UPVdosRd1</H1>
   <TABLE
   <TR><TD>System:</TD>     <TD>#UPVdosRd1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>ping</TD></TR>
   <TR><TD>IP:</TD>         <TD>10.228.154.162</TD></TR>
   </TABLE>
```

```
Target[37920_ping]: `/usr/share/snpservices/common/ping.sh 10.228.154.162`
MaxBytes[37920_ping]: 2000
Options[37920_ping]: growright,unknaszero,nopercent,gauge
LegendI[37920_ping]: Perduts LegendO[37920_ping]: Temps mig
Legend1[37920_ping]: Temps max. en ms
Legend2[37920_ping]: Temps min. en ms
YLegend[37920_ping]: RTT (ms)
Target[37920-0_traf]: \wifi0:public@10.228.154.162:
SetEnv[37920-0_traf]: MRTG_INT_IP="10.228.154.162" MRTG_INT_DESCR="#UPVdosRd1"
MaxBytes[37920-0_traf]: 3000000
Title[37920-0_traf]: Trafic a VLCPVdsRd1CPE0 de #UPVdosRd1
PageTop[37920-0_traf]: <H1>Tr&agrave;fic a VLCPVdsRd1CPE0 de #UPVdosRd1</H1>
   <TABLE>
   <TR><TD>System:</TD>     <TD>#UPVdosRd1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>VLCPVdsRd1CPE0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Title[27662_ping]: Temps del ping de #VLCPreigRB1
PageTop[27662_ping]: <H1>Lat&egrave;ncia #VLCPreigRB1</H1>
   <TABLE
   <TR><TD>System:</TD>     <TD>#VLCPreigRB1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>ping</TD></TR>
   <TR><TD>IP:</TD>         <TD>10.228.154.129</TD></TR>
   </TABLE>
Target[27662_ping]: `/usr/share/snpservices/common/ping.sh 10.228.154.129`
MaxBytes[27662_ping]: 2000
Options[27662_ping]: growright,unknaszero,nopercent,gauge
LegendI[27662_ping]: Perduts LegendO[27662_ping]: Temps mig
Legend1[27662_ping]: Temps max. en ms
Legend2[27662_ping]: Temps min. en ms
YLegend[27662_ping]: RTT (ms)
Target[27662-0_traf]: \wlan1:public@10.228.154.129:
SetEnv[27662-0_traf]: MRTG_INT_IP="10.228.154.129" MRTG_INT_DESCR="#VLCPreigRB1"
MaxBytes[27662-0_traf]: 3000000
Title[27662-0_traf]: Trafic a VLCPreigRD1 OMNI de #VLCPreigRB1
PageTop[27662-0_traf]: <H1>Tr&agrave;fic a VLCPreigRD1 OMNI de #VLCPreigRB1</H1>
   <TABLE>
   <TR><TD>System:</TD>     <TD>#VLCPreigRB1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>VLCPreigRD1 OMNI</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Target[27662-1_traf]: \wlan2:public@10.228.154.129:
SetEnv[27662-1_traf]: MRTG_INT_IP="10.228.154.129" MRTG_INT_DESCR="#VLCPreigRB1"
MaxBytes[27662-1_traf]: 3000000
Title[27662-1_traf]: Trafic a VLCPreigRD2-357 de #VLCPreigRB1
PageTop[27662-1_traf]: <H1>Tr&agrave;fic a VLCPreigRD2-357 de #VLCPreigRB1</H1>
   <TABLE>
   <TR><TD>System:</TD>     <TD>#VLCPreigRB1</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
   <TR><TD>Description:</TD><TD>VLCPreigRD2-357</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
   </TABLE>
Target[27662-2_traf]: \wlan3:public@10.228.154.129:
SetEnv[27662-2_traf]: MRTG_INT_IP="10.228.154.129" MRTG_INT_DESCR="#VLCPreigRB1"
MaxBytes[27662-2_traf]: 3000000
```

```
Title[27662-2_traf]: Trafic a VLCPreigRD3-104 de #VLCPreigRB1
PageTop[27662-2_traf]: <H1>Tr&agrave;fic a VLCPreigRD3-104 de #VLCPreigRB1</H1>
  <TABLE>
  <TR><TD>System:</TD>     <TD>#VLCPreigRB1</TD></TR>
  <TR><TD>Maintainer:</TD> <TD>guifi@guifi.net</TD></TR>
  <TR><TD>Description:</TD><TD>VLCPreigRD3-104</TD></TR>
  <TR><TD>Max Speed:</TD>  <TD>30.0 Mbits/s</TD></TR>
  </TABLE>
```

C.2.3. Servidor de gráficas para la web de VLCupvGRC

C.2.3.1. /etc/mrtg.cfg

```
# Created by
# /usr/bin/cfgmaker --global "WorkDir: /var/www/mrtg" --global "RunAsDaemon: Yes" --global "Options [-]: bits,
growright" --output /etc/mrtg.cfg public@10.228.154.225

### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  for Debian
# WorkDir: /var/www/mrtg

#  or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
Options[_]: growright, bits

EnableIPv6: no
WorkDir: /var/www/mrtg
RunAsDaemon: Yes
# Options [-]: bits, growright

######################################################################
# System: valupvgrcRd1
# Description: router
# Contact: guifi@guifi.net
# Location: valupvgrc
######################################################################

### Interface 1 >> Descr: 'wlan1' | Name: 'wlan1' | Ip: '10.228.154.97' | Eth: '00-0c-42-66-90-79' ###
### The following interface is commented out because:
### * it is operationally DOWN
#
 Target[10.228.154.225_wlan1]: #wlan1:public@10.228.154.225:
 SetEnv[10.228.154.225_wlan1]: MRTG_INT_IP="10.228.154.97" MRTG_INT_DESCR="wlan1"
 MaxBytes[10.228.154.225_wlan1]: 1375000
 Title[10.228.154.225_wlan1]: Traffic Analysis for wlan1 -- valupvgrcRd1
 PageTop[10.228.154.225_wlan1]: <h1>Traffic Analysis for wlan1 -- valupvgrcRd1</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>System:</td>
                                        <td>valupvgrcRd1 in valupvgrc</td>
                                </tr>
                                <tr>
                                        <td>Maintainer:</td>
                                        <td>guifi@guifi.net</td>
                                </tr>
```

```
                                <tr>
                                        <td>Description:</td>
                                        <td>wlan1  </td>
                                </tr>
                                <tr>
                                        <td>ifType:</td>
                                        <td>Radio Spread Spectrum (802.11) (71)</td>
                                </tr>
                                <tr>
                                        <td>ifName:</td>
                                        <td>wlan1</td>
                                </tr>
                                <tr>
                                        <td>Max Speed:</td>
                                        <td>1375.0 kBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>10.228.154.97 (valupvgrcRd1.guifi.net)</td>
                                </tr>
                        </table>
                </div>

### Interface 2 >> Descr: 'wlan2' | Name: 'wlan2' | Ip: '10.228.154.161' | Eth: '00-0c-42-66-90-5b' ###

Target[10.228.154.225_wlan2]: #wlan2:public@10.228.154.225:
SetEnv[10.228.154.225_wlan2]: MRTG_INT_IP="10.228.154.161" MRTG_INT_DESCR="wlan2"
MaxBytes[10.228.154.225_wlan2]: 1375000
Title[10.228.154.225_wlan2]: Traffic Analysis for wlan2 -- valupvgrcRd1
PageTop[10.228.154.225_wlan2]: <h1>Traffic Analysis for wlan2 -- valupvgrcRd1</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>System:</td>
                                        <td>valupvgrcRd1 in valupvgrc</td>
                                </tr>
                                <tr>
                                        <td>Maintainer:</td>
                                        <td>guifi@guifi.net</td>
                                </tr>
                                <tr>
                                        <td>Description:</td>
                                        <td>wlan2  </td>
                                </tr>
                                <tr>
                                        <td>ifType:</td>
                                        <td>Radio Spread Spectrum (802.11) (71)</td>
                                </tr>
                                <tr>
                                        <td>ifName:</td>
                                        <td>wlan2</td>
                                </tr>
                                <tr>
                                        <td>Max Speed:</td>
                                        <td>1375.0 kBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>10.228.154.161 (vlcupvap0-180.guifi.net)</td>
                                </tr>
                        </table>
                </div>

### Interface 3 >> Descr: 'wlan3' | Name: 'wlan3' | Ip: '10.228.154.193' | Eth: '00-0c-42-66-90-6c' ###
### The following interface is commented out because:
### * it is operationally DOWN
#
```

```
Target[10.228.154.225_wlan3]: #wlan3:public@10.228.154.225:
SetEnv[10.228.154.225_wlan3]: MRTG_INT_IP="10.228.154.193" MRTG_INT_DESCR="wlan3"
MaxBytes[10.228.154.225_wlan3]: 1375000
Title[10.228.154.225_wlan3]: Traffic Analysis for wlan3 -- valupvgrcRd1
PageTop[10.228.154.225_wlan3]: <h1>Traffic Analysis for wlan3 -- valupvgrcRd1</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>System:</td>
                                <td>valupvgrcRd1 in valupvgrc</td>
                        </tr>
                        <tr>
                                <td>Maintainer:</td>
                                <td>guifi@guifi.net</td>
                        </tr>
                        <tr>
                                <td>Description:</td>
                                <td>wlan3  </td>
                        </tr>
                        <tr>
                                <td>ifType:</td>
                                <td>Radio Spread Spectrum (802.11) (71)</td>
                        </tr>
                        <tr>
                                <td>ifName:</td>
                                <td>wlan3</td>
                        </tr>
                        <tr>
                                <td>Max Speed:</td>
                                <td>1375.0 kBytes/s</td>
                        </tr>
                        <tr>
                                <td>Ip:</td>
                                <td>10.228.154.193 (vlcupvap0-90.guifi.net)</td>
                        </tr>
                </table>
        </div>

### Interface 4 >> Descr: 'ether1' | Name: 'ether1' | Ip: '10.228.154.225' | Eth: '' ###

Target[10.228.154.225_ether1]: #ether1:public@10.228.154.225:
SetEnv[10.228.154.225_ether1]: MRTG_INT_IP="" MRTG_INT_DESCR="ether1"
MaxBytes[10.228.154.225_ether1]: 12500000
Title[10.228.154.225_ether1]: Traffic Analysis for ether1 -- valupvgrcRd1
PageTop[10.228.154.225_ether1]: <h1>Traffic Analysis for ether1 -- valupvgrcRd1</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>System:</td>
                                <td>valupvgrcRd1 in valupvgrc</td>
                        </tr>
                        <tr>
                                <td>Maintainer:</td>
                                <td>guifi@guifi.net</td>
                        </tr>
                        <tr>
                                <td>Description:</td>
                                <td>ether1  </td>
                        </tr>
                        <tr>
                                <td>ifType:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>ifName:</td>
                                <td>ether1</td>
```

```
                                        </tr>
                                        <tr>
                                                <td>Max Speed:</td>
                                                <td>12.5 MBytes/s</td>
                                        </tr>
                                </table>
                        </div>

### Interface 5 >> Descr: 'ether2' | Name: 'ether2' | Ip: '' | Eth: '00-0c-42-5c-e2-bf' ###
### The following interface is commented out because:
### * it is administratively DOWN
### * it is operationally DOWN
#
# Target[10.228.154.225_ether2]: #ether2:public@10.228.154.225:
# SetEnv[10.228.154.225_ether2]: MRTG_INT_IP="" MRTG_INT_DESCR="ether2"
# MaxBytes[10.228.154.225_ether2]: 12500000
# Title[10.228.154.225_ether2]: Traffic Analysis for ether2 -- valupvgrcRd1
# PageTop[10.228.154.225_ether2]: <h1>Traffic Analysis for ether2 -- valupvgrcRd1</h1>
#                       <div id="sysdetails">
#                               <table>
#                                       <tr>
#                                               <td>System:</td>
#                                               <td>valupvgrcRd1 in valupvgrc</td>
#                                       </tr>
#                                       <tr>
#                                               <td>Maintainer:</td>
#                                               <td>guifi@guifi.net</td>
#                                       </tr>
#                                       <tr>
#                                               <td>Description:</td>
#                                               <td>ether2  </td>
#                                       </tr>
#                                       <tr>
#                                               <td>ifType:</td>
#                                               <td>ethernetCsmacd (6)</td>
#                                       </tr>
#                                       <tr>
#                                               <td>ifName:</td>
#                                               <td>ether2</td>
#                                       </tr>
#                                       <tr>
#                                               <td>Max Speed:</td>
#                                               <td>12.5 MBytes/s</td>
#                                       </tr>
#                               </table>
#                       </div>


### Interface 13 >> Descr: 'wLan/Lan' | Name: 'wLan/Lan' | Ip: '10.228.154.225' | Eth: '' ###

Target[10.228.154.225_wLan_Lan]: #wLan/Lan:public@10.228.154.225:
SetEnv[10.228.154.225_wLan_Lan]: MRTG_INT_IP="10.228.154.225" MRTG_INT_DESCR="wLan/Lan"
MaxBytes[10.228.154.225_wLan_Lan]: 12500000
Title[10.228.154.225_wLan_Lan]: Traffic Analysis for wLan/Lan -- valupvgrcRd1
PageTop[10.228.154.225_wLan_Lan]: <h1>Traffic Analysis for wLan/Lan -- valupvgrcRd1</h1>
                        <div id="sysdetails">
                                <table>
                                        <tr>
                                                <td>System:</td>
                                                <td>valupvgrcRd1 in valupvgrc</td>
                                        </tr>
                                        <tr>
                                                <td>Maintainer:</td>
                                                <td>guifi@guifi.net</td>
                                        </tr>
                                        <tr>
                                                <td>Description:</td>
```

```
                                        <td>wLan/Lan  </td>
                                </tr>
                                <tr>
                                        <td>ifType:</td>
                                        <td> (209)</td>
                                </tr>
                                <tr>
                                        <td>ifName:</td>
                                        <td>wLan/Lan</td>
                                </tr>
                                <tr>
                                        <td>Max Speed:</td>
                                        <td>12.5 MBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>10.228.154.225 (valupvgrcRd1.guifi.net)</td>
                                </tr>
                        </table>
                </div>

    ### Interface Hotspot >> Descr: 'eth0_real' | Name: '' | Ip: '10.228.154.226' | Eth: '' ###

    Target[10.228.154.226_3]: 3:public@10.228.154.226:
    SetEnv[10.228.154.226_3]: MRTG_INT_IP="" MRTG_INT_DESCR="eth0_real"
    MaxBytes[10.228.154.226_3]: 12500000
    Title[10.228.154.226_3]: Traffic Analysis for 3 -- UBNT
    PageTop[10.228.154.226_3]: <h1>Traffic Analysis for Hotspot -- UBNT</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>System:</td>
                                        <td>UBNT in Valupvgrc</td>
                                </tr>
                                <tr>
                                        <td>Maintainer:</td>
                                        <td>guifi@guifi.net</td>
                                </tr>
                                <tr>
                                        <td>Description:</td>
                                        <td>eth0_real  </td>
                                </tr>
                                <tr>
                                        <td>ifType:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>ifName:</td>
                                        <td></td>
                                </tr>
                                <tr>
                                        <td>Max Speed:</td>
                                        <td>12.5 MBytes/s</td>
                                </tr>
                        </table>
                </div>
```

C.2.3.2. /var/www/mrtg.html

```
    /VAR/WWW/MRTG.HTML
    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
    <HTML>
    <HEAD>
```

```
        <TITLE>MRTG Index Page</TITLE>
        <!-- Command line is easier to read using "View Page Properties" of your browser -->
        <!-- But not all browsers show that information. :-(                          -->
        <meta http-equiv="content-type" content="text/html; charset=iso-8859-15" >
        <META NAME="Command-Line" CONTENT="/usr/bin/indexmaker --columns=1 --output /var/www/mrtg.html
/etc/mrtg.cfg" >
        <META HTTP-EQUIV="Refresh" CONTENT="300" >
        <META HTTP-EQUIV="Cache-Control" content="no-cache" >
        <META HTTP-EQUIV="Pragma" CONTENT="no-cache" >
        <META HTTP-EQUIV="Expires" CONTENT="Thu, 24 Nov 2011 15:14:59 GMT" >
        <LINK HREF="favicon.ico" rel="shortcut icon" >

      <style type="text/css">
      /* commandline was: /usr/bin/indexmaker --columns=1 --output /var/www/mrtg.html /etc/mrtg.cfg */
      /* sorry, no style, just abusing this to place the commandline and pass validation */
      </style>
      </HEAD>

      <BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000" alink="#000000">

      <H1>MRTG Index Page</H1>

      <TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
      <tr>
      <td><DIV><B>Traffic Analysis for wlan2 -- valupvgrcRd1</B></DIV>
      <DIV><A HREF="10.228.154.225_wlan2.html"><IMG BORDER=1 ALT="10.228.154.225_wlan2 Traffic Graph"
SRC="10.228.154.225_wlan2-day.png"></A><BR>
      <SMALL><!--#flastmod file="10.228.154.225_wlan2.html" --></SMALL></DIV>
      </td></tr>
      <tr>
      <td><DIV><B>Traffic Analysis for ether1 -- valupvgrcRd1</B></DIV>
      <DIV><A HREF="10.228.154.225_ether1.html"><IMG BORDER=1 ALT="10.228.154.225_ether1 Traffic Graph"
SRC="10.228.154.225_ether1-day.png"></A><BR>
      <SMALL><!--#flastmod file="10.228.154.225_ether1.html" --></SMALL></DIV>
      </td></tr>
      <tr>
      <td><DIV><B>Traffic Analysis for wLan/Lan -- valupvgrcRd1</B></DIV>
      <DIV><A HREF="10.228.154.225_wlan_lan.html"><IMG BORDER=1 ALT="10.228.154.225_wlan_lan Traffic
Graph" SRC="10.228.154.225_wlan_lan-day.png"></A><BR>
      <SMALL><!--#flastmod file="10.228.154.225_wlan_lan.html" --></SMALL></DIV>
      </td></tr>
      <tr>
      <td><DIV><B>Traffic Analysis for Hotspot -- UBNT</B></DIV>
      <DIV><A HREF="10.228.154.226_3.html"><IMG BORDER=1 ALT="10.228.154.226_3 Traffic Graph"
SRC="10.228.154.226_3-day.png"></A><BR>
      <SMALL><!--#flastmod file="10.228.154.226_3.html" --></SMALL></DIV>
      </td></tr>
      <tr>
      <td></td>
      </tr>
      </TABLE>

      <BR>
      <TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
        <TR>
          <TD WIDTH=63><A
          HREF="http://oss.oetiker.ch/mrtg/"><IMG
          BORDER=0 SRC="mrtg-l.png" WIDTH=63 HEIGHT=25 ALT="MRTG"></A></TD>
          <TD WIDTH=25><A
          HREF="http://oss.oetiker.ch/mrtg/"><IMG
          BORDER=0 SRC="mrtg-m.png" WIDTH=25 HEIGHT=25 ALT=""></A></TD>
          <TD WIDTH=388><A
          HREF="http://oss.oetiker.ch/mrtg/"><IMG
          BORDER=0 SRC="mrtg-r.png" WIDTH=388 HEIGHT=25
          ALT="Multi Router Traffic Grapher"></A></TD>
        </TR>
      </TABLE>
```

```
      <TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
        <TR VALIGN=top>
        <TD WIDTH=88 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
        version 2.16.2</FONT></TD>
        <TD WIDTH=388 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
        <A HREF="http://tobi.oetiker.ch/">Tobias Oetiker</A>
        <A HREF="mailto:tobi+mrtglink@oetiker.ch">&lt;tobi@oetiker.ch&gt;</A>
        and <A HREF="http://www.bungi.com/">Dave Rand</A> <A
HREF="mailto:dlr@bungi.com">&lt;dlr@bungi.com&gt;</A></FONT>
        </TD>
      </TR>
      </TABLE>
      </BODY>
      </HTML>
```

BIBLIOGRAFÍA:

GENERAL

- CREATIVE COMMONS "Creative Commons Reconocimiento-compartirigual License España" *http://creativecommons.org/licenses/by-sa/3.0/es/* (En línea, consultado en mayo 2012)

- ROCA, R. "Licencia Procomún Inalámbrica". Agosto 2010. (En línea, consultado en mayo 2012). *http://guifi.net/es/ProcomunInalambrica*

CAPÍTULO 1: REDES ABIERTAS y LIBRES

- TIC. "La red abierta como modelo sostenible para el desarrollo de la sociedad". I Jornadas Internacionales de Investigación en TIC para el Desarrollo Humano. Fuenlabrada, Madrid Mayo 2.010
- FLICKENGER, R. "Redes Inalámbricas en los Países en Desarrollo". 3ª edición (2008) (En línea, consultado en mayo 2012) *http://wndw.net/*
- DALMAU, Lluis. "Guifi.net – des dels inicis fins avui" (2006) (En línea, consultado en mayo 2012) *http://guifi.net/es/node/5551*
- FONTS, Oscar. "Análisis de la red ciudadana Guifi.net". Diciembre 2009.
- ROCA. R. "Els inicis a Gurb" (2004) (En línea, consultado en mayo 2012) *http://guifi.net/es/node/649*
- GARCÍA FERNÁNDEZ, Victor "Scalability study of Guifi.net and mesh networks". Universitat Politècnica de Catalunya. Marzo 2011.

CAPÍTULO 2: CONCEPTOS Y TECNOLOGÍAS WIRELESS

- AKYILDIZ Ian F, WANG Xudong y WANG Weilin. "Wireless mesh networks: a survey". Computer Networks. 2005.
- CNAF. "Cuadro nacional de atribución de frecuencias". Ministerio de industria, energía y turismo. (En línea, consultado en mayo 2012) *http://www.minetur.gob.es/telecomunicaciones/Espectro/Paginas/CNAF.aspx*

- BUETTRICH, Sebastian. " Redes MESH"., wireless.dk 2006
- CONNER W. S., KRUYS J., ZUNIGA J: C. "IEEE 802.11s Tutorial. Overview of the Amendment for Wireless Local Area Mesh Networking". Dallas. Nov. 2006.
- LEE, M. "Emerging Standards for Wireless Mesh Technology", IEEE Wireless Communications, Abril 2006.
- RIGGIO Roberto, MIORANDI Daniele, CHLAMTAC Imrich et al. "Hardware and Software Solutions for Wireless Mesh Network Testbeds". IEEE Communications Magazine 2008.
- SIMAL, Tomás. "Monográfico: Redes Wifi" Instituto Nacional de Tecnologías Educativas y Formación del Profesorado. Ministerio de Educación, Cultura y Deporte. Febrero 2011 (En línea, consultado en mayo 2012) *http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi*

CAPÍTULO 3: INSTALACIÓN FÍSICA DEL SUPERNODO UPV

- PÉREZ, Miguel, BORONAT, Pablo, RUBERT, David. " Curso de instaladores Guifi2011", Universitat Jaume I, septiembre 2011 (En línea, consultado en mayo 2012) https://roure.act.uji.es/wiki/public/guifinet/cursoinstaladoresguifi2011/start
- RUBERT, David. "Guifi.net, Materiales, combinaciones y precios para diferentes tipos de nodos" Julio 2010. Universidad Jaime I. (En línea, consultado en mayo 2012) *http://enruta.me/*
- MIKROTIK. "Manual de Usuario" Mayo 2011 (En línea, consultado en mayo 2012) *http://wiki.mikrotik.com/wiki/Manual:License_levels* .
- UBIQUITI, "Manual de configuración del Ubiquiti Nanostation 2 y 5 (AirOS 3.1.1) Cómo hacer un enlace punto-a-punto" – Enero 2009
- UBIQUITI **"**Manual de Ubiquiti AirOS"**.** Traducido por Salvador Bertenbreiter Febrero 2011 (En línea, consultado en mayo 2012) *http://wiki.ubnt.com/wiki/index.php/airos_manual_spanish*

CAPÍTULO 4: CONFIGURACIÓN DE LAS ANTENAS

- SALA, Jaume. "La guia d'instal·lació de Guifi.net" (En línea, consultado en mayo 2012) *http://www.jaumesala.net/guiaguifi/*

- VIQUILLIBRES. "Guifi.net. Tutorial/Afegir els trastos". Febrero 2010) *http://ca.wikibooks.org/wiki/Guifi.net._Tutorial/Afegir_els_trastos*

CAPÍTULO 5: AÑADIR UN SERVIDOR Y SERVICIOS

- BORONAT, Pablo. " Cómo Instalar y configurar un servidor completo guifi.net" (enero 2012) (En línea, consultado en mayo 2012) *https://roure.act.uji.es/wiki/public/guifinet/doc/recetas/guifinetservidorcompleto*
- BORONAT, Pablo. "Instalar y configurar un servidor de gráficas en guifi". (marzo 2011) (En línea, consultado en mayo 2012) *https://roure.act.uji.es/wiki/public /guifinet/doc/recetas/guifinetservidorgraficas*
- KELLEY, Simon. "Manual DNSmasq". Ubuntu manuals. (2010) (En línea, consultado en mayo 2012) *http://manpages.ubuntu.com/manpages/hardy/es/man8/dnsmasq.8.html*
- PRUNOIU, Florin. "MRTG Implementation Manual" Rev. 11260301. Enterastream Communications Inc. (En línea, consultado en mayo 2012) http://www.enterastream.com/whitepapers/mrtg/mrtg-manual.html
- RUÍZ GÓMEZ, Alberto " Redes de área local Aplicaciones y Servicios Linux". Instituto de Tecnologías Educativas. Ministerio de Educación. Madrid (En línea, consultado en mayo 2012) *http://www.ite.educacion.es/formacion/ materiales/85/cd/REDES_LINUX/indice.htm*

CAPÍTULO 6: NODO CLIENTE

- DALMAU, Lluis. "Instrucciones de conexión a Guifi.net" (En línea, consultado en mayo 2012) *http://castello.guifi.net/content/instrucciones-de-conexion-guifinet #elementos*
- LINKSYSDS "Unirse a guifi.net, en tres pasos".(2011) (En línea, consultado en mayo 2012) http://guifi.net/es/trespasos

CAPÍTULO 7: CONEXIONES VPN

- BORONAT, Pablo. "Cómo crear un túnel cifrado entre dos máquinas con clave estática". Marzo 2011 (En línea, consultado en mayo 2012) *https://roure.act.uji.es/wiki/howtos/linuxcreartunelencriptado?Do=backlink*
- INFOACCESO. "Acceso inalámbrico a la UPV por VPN" (En línea, consultado en mayo 2012) *http://www.upv.es/contenidos/INFOACCESO/indexc.html*

CAPÍTULO 8: ESTUDIO DE PRESTACIONES

- GARZÓN ALCALDE, Joaquín "Monitorización gráfica del tráfico de red y otros parámetros del sistema". (En línea, consultado en mayo 2012) *http://beta.redes-linux.com/manuales/Monitorizacion_redes/mrtg.pdf*
- GATES, Mark, "Iperf Version 2.0.0", Universidad de Illinois, Mayo 2004. (En línea, consultado en mayo 2012) *http://www.onl.wustl.edu/restricted/iperf.html*
- IPERF. "Documentación Iperf " Agosto 2011 (En línea, consultado en mayo 2012) *http://dast.nlanr.net/Projects/Iperf/*

Instalación y configuración de un supernodo de la red abierta Guifi.net en la U.P.V.

Autor: Vicente Javier Ortiz Gallart

Director: Pietro Manzoni

Tesis del máster en Ingeniería de Computadores

Departamento de Informática de Sistemas y Computadores

Universidad Politécnica de Valencia

15 de junio de 2012