



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL
DESARROLLO**

**CARRERA DE INGENIERÍA EN TELECOMUNICACION
CON MENCIÓN EN GESTIÓN EMPRESARIAL**

TÍTULO:

**“Análisis y Diseño de redes MESH para aumentar
cobertura de internet en la Facultad Técnica para el
Desarrollo”**

AUTOR:

Andrés Josué Villacreses Tobar

**Trabajo de Investigación, Análisis y Diseño previo a la
obtención del título de:
INGENIERO EN TELECOMUNICACION CON MENCIÓN EN
GESTIÓN EMPRESARIAL**

TUTOR:

Ing. Efraín Suárez Murillo

**Guayaquil, Ecuador
2013**



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACION CON
MENCION EN GESTION EMPRESARIAL**

CERTIFICACIÓN

Certifico que el desarrollo del presente trabajo ha sido realizado en su totalidad por **Andrés Josué Villacreses Tobar**, como requerimiento parcial para la obtención del Título de **Ingeniero en Telecomunicación con mención en Gestión Empresarial**.

TUTOR

Ing. Efraín Suárez Murillo

REVISORES

Ing. Washington Medina

Ing. Juan González

DIRECTOR DE CARRERA

Ing. Armando Heras

Guayaquil, a los 14 días del mes de noviembre del año 2013



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACION CON
MENCION EN GESTION EMPRESARIAL**

DECLARACIÓN DE RESPONSABILIDAD

Yo **Andrés Villacreses Tobar**, DECLARO que el Trabajo titulado “**Análisis y Diseño de redes MESH para aumentar cobertura de internet en la Facultad Técnica para el Desarrollo**” previo a la obtención del Título de **Ingeniero en Telecomunicación con mención en Gestión Empresarial**, se desarrolló a través de una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 14 días del mes de noviembre del año 2013

EL AUTOR

Andrés Josué Villacreses Tobar



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACION CON
MENCION EN GESTION EMPRESARIAL**

AUTORIZACIÓN

Yo, **Andrés Villacreses Tobar**, Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **“Análisis y Diseño de redes MESH para aumentar cobertura de internet en la Facultad Técnica para el Desarrollo”**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 14 días del mes de noviembre del año 2013

EL AUTOR

Andrés Josué Villacreses Tobar

AGRADECIMIENTO

Primeramente me gustaría agradecer a Dios por bendecirme para llegar hasta donde he llegado, porque gracias a él pude hacer realidad este sueño tan anhelado.

A la UNIVERSIDAD CATOLICA DE SANTIAGO DE GUAYAQUIL por darme la oportunidad de estudiar y ser un profesional.

A mi director de tesis, ING. EFRAIN SUAREZ MURILLO por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

También me gustaría agradecer a mis profesores durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación.

Andrés Josué Villacreses Tobar

DEDICATORIA

Esta tesis se la dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin desfallecer en el intento.

A mi familia quienes por ellos soy lo que soy.

A mis padres por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar, quienes me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

Andrés Josué Villacreses Tobar

ÍNDICE GENERAL

Contenido	Pag.
Certificación	II
Declaración de Responsabilidad	III
Autorización	IV
Agradecimiento	V
Dedicatoria	VI
Índice General	VII
Índice de Tablas	XIV
Índice de Figuras	XV
Resumen	XXI
Abstract	XXII

CAPITULO:

1.	GENERALIDADES	
1.1	Introducción	1
1.2	Justificación	2
1.3	Hipótesis	2
1.4	Descripción del problema	3
1.5	Objetivos	3
1.5.1	Objetivo general	3
1.5.2	Objetivos específicos	4
2.	MARCO TEORICO	5
2.1	Arquitecturas y protocolos de las redes inalámbricas MESH (WMNs)	5
2.1.1	Redes inalámbricas E IEEE 802.11	5
2.2	Selección Dinámica de Frecuencias y Control de Potencia del Transmisor	9

2.3	Otros estándares	10
2.3.1	Estándar IEEE 802.16 (Wi-Max)	10
2.4	Características generales de las redes inalámbricas MESH	13
2.5	Topología MESH o en malla	14
2.6	Relación entre redes inalámbricas AD HOC y redes MESH	15
2.6.1	Retos en redes Mesh	16
2.6.2	Confianza y robustez	17
2.6.3	Servicio de recursos	17
2.6.4	Arquitecturas en redes Mesh	18
2.7	Particularidades específicas de las redes MESH	20
2.8	Ambientes de aplicación	20
2.9	Metodologías de funcionamiento	22
2.10	Topología de control de la red	23
2.11	Recursos multiradio en capa de enlace	24
2.12	Regla de unificación multiradio [MUP]	24
2.13	Reglas de control de acceso al medio para MR-WMNs	27
2.14	Reglas de enrutamiento multiradio para redes Mesh	30
2.15	Niveles o capas de las redes MESH	30
2.16	Redes MESH multiradio y multicanal	34
2.17	Arquitectura MESH en 802.11	36
2.18	Capacidad de expansión	37
2.19	Redes Mesh Multiradio	39
2.20	Redes MESH basadas en IEEE 802.11	42
2.21	Problemas de rendimiento y sus causas	43
2.22	Redes MESH multicanal	45
2.23	Asignación del canal basado en la topología	46
2.24	Interferencia inter-canal	47
2.25	Protocolos en las redes MESH	48
2.26	Requisitos de enrutamiento en las redes WMNs	49
2.27	Enrutamiento multicamino para balanceo de carga y tolerancia a fallos	49

2.28	Estrategia de selección de ruta	53
2.29	Generación de peticiones de rutas	54
2.30	Seguridad	57
2.30.1	Métodos en seguridad	57
3.	ANÁLISIS PREVIO PARA EL DISEÑO DE LA RED	61
3.1	Introducción	61
3.2	Estado actual de las comunicaciones en la Facultad Técnica para el Desarrollo	61
3.3	Latencia	63
3.4	Ancho de banda	64
3.5	Selección de canales	65
3.6	Planeación de la capacidad de la red	67
3.7	Estudio de cobertura	68
3.8	Infraestructura	71
4.	DISEÑO DE LA RED MESH APLICADA A LA FACULTAD TECNICA PARA EL DESARROLLO	74
4.1	Introducción	74
4.2	Visión general de la propuesta del diseño de la red WMNS	74
4.3	Características de diseño para redes inalámbricas	76
4.4	Requisitos para el diseño de la red mesh	79
4.4.1	Requisitos generales	79
4.4.2	Requisitos específicos	79
4.4.3	Requisitos de funcionamiento	80
4.5	Características de funcionamiento	80
4.6	Ganancia de las antenas	82

4.7	El mínimo nivel de señal recibida	82
4.8	Pérdidas en los cables	82
4.9	Pérdidas en los conectores	83
4.10	Software mikrotik mesh	84
4.11	Características principales	85
4.12	Calidad de servicio (QoS)	86
4.13	Interfaces del RouterOS	87
4.14	Herramientas de manejo de red	87
4.15	Instalación de mikrotik routers	88
4.15.6	Asignación de nombres a las interfaces	97
4.15.7	Definición de Vlans	102
4.15.8	Asignación de direcciones IP´Salas interfaces	105
4.15.9	Configuración POOLS de direcciones de IP	109
4.15.10	Definir DNS	110
4.15.11	Nat Masquerade para todas las redes	111
4.15.12	Configuración servidor DHCP	112
4.15.13	Asignación de direcciones de IP fijas a partir de direcciones MAC	114
4.15.14	Configuración servidor - CLIENTE NTP	115
4.15.15	Servidor web PROXY	117
4.15.16	Bloqueo de pornografía	122
4.15.17	Bloqueo de páginas que brinden el servicio de web Messenger	124
4.15.18	Bloqueo del Skype a través del Proxy	125
4.15.19	Bloqueo de descarga directa de archivos MP3 y AVI	126
4.15.20	Balanceo de carga	128
4.15.21	Control de ancho de banda	132
4.15.22	Configuración RF y HOTSPOT	138
4.15.23	Sistema HOTSPOT	157
4.15.24	Antenas	160
4.16	Presupuesto y estimación de costos	162

5.	CONCLUSIONES Y RECOMENDACIONES	163
5.1	Conclusiones	163
5.2	Recomendaciones	165
	BIBLIOGRAFÍA	166

ÍNDICE DE TABLAS

Tabla		Pag.
2.1	Comparación de las redes AD HOC y MESH	16
4.1	Características de las redes Mesh	81
4.2	Características del Software	81
4.3	Valores típicos de pérdida en cables para 2.4 Ghz y 5.8 Ghz	83

ÍNDICE DE FIGURAS

Figura	Pag.
2.1 Aplicación de redes Mesh en la UCSG	14
2.2 Funcionamiento de los nodos en una red MESH	23
2.3 Representación de la arquitectura MUP	25
2.4 Protocolo IC SMA	29
2.5 Representación esquemática de los dos tipos de nodos Mesh: Aps y puntos Mesh	36
2.6 Dos niveles de arquitectura de red Mesh	37
2.7 Redes Mesh Multicanal de un solo radio	38
2.8 Malla de red inalámbrica	42
2.9 Balanceo de carga cuando una ruta falla en la Facultad Técnica de la UCSG	50
2.9 Ejemplo de búsqueda de un nuevo nodo	57
2.10 Acceso a WLAN basada en EAP	60
3.1 Páginas de contenido social	63
3.2 Tiempos de respuesta hacia la Ip 200.93.195.21	64
3.3 Tiempos de respuesta hacia la Ip 200.93.195.21	64
3.4 Tiempos de respuesta hacia la Ip 200.93.195.21	65
3.5 Tiempos de respuesta hacia la Ip 200.93.195.21	66
3.6 Canales de bandas otorgadas para Wi.Fi	66
3.7 Canales de bandas divididas otorgada para Wi.Fi	67
3.8 Distribución de los nodos de una red inalámbrica	68
3.9 Internet intermitente en pasillos de la Facultad (Laboratorios)	68
3.10 Comprobación de la ausencia de Internet dentro de las Aulas	69
3.11 Comprobación de la ausencia de internet fuera del Aula FT-14 a pesar de estar asociado al Ssid: _ wifiucsg	69
3.12 Comprobación de la ausencia de internet dentro del Aula FT-14, se observan niveles de -84dbm	70

3.13	Internet intermitente en los alrededores de la Facultad	70
3.14	Ausencia de internet dentro del Aula FT-15, no se puede asociar al Wifi	71
3.15	Torre de 6mts de Altura ubicada en la parte superior de la Secretaría de la Facultad Técnica para el Desarrollo	72
3.16	Torre de 9mts de altura ubicada en la parte superior del laboratorio de computación	72
3.17	Sitio para distribuir Wifi en la Facultad de Agronomía	73
4.1	Arquitectura a implementar para el diseño de la red WMNs	75
4.2	Simulación de 2 antenas sectorial en la torre de 6 mts. (Secretaría)	77
4.3	Simulación de instalación de 2 antenas sectorial en la torre de 12 mts.(Laboratorio de computación)	77
4.4	Simulación de instalación de equipos de radio (Facultad de Agronomía)	78
4.5	Diseño de una Red Mesh en la Facultad Técnica para el Desarrollo	78
4.6	Paquetes de configuración	88
4.7	Proceso de instalación	89
4.8	Instalación de paquetes seleccionados	90
4.9	Proceso de instalación (usuario y contraseña)	90
4.10	Licencia de instalación	91
4.11	Consola para la configuración del Mikrotik	91
4.12	Winbox para loguearse al Mikrotik	92
4.13	Descarga de los plugins instalados en Mikrotik	93
4.14	Configuración del Mikrotik	93
4.15	Backup de la configuración	94
4.16	Almacenamiento del archivo de configuración en Windows	95
4.17	Recuperación del archivo de configuración del Mikrotik	96
4.18	Recuperación del archivo de configuración del Mikrotik	96
4.19	Pestaña general del interface (Administración)	98

4.20	Pestaña Ethernet del interface (Administración)	98
4.21	Pestaña status del interface (Administración)	99
4.22	Pestaña Traffic del interface (Administración)	99
4.23	Pestaña general del interface (Agronomía)	100
4.24	Pestaña Ethernet del interface (Agronomía)	101
4.25	Pestaña General del interface (Laboratorio)	101
4.26	Pestaña Ethernet del interface (Laboratorio)	102
4.27	Pestaña General del Vlan (Administración)	103
4.28	Pestaña Traffic del Vlan (Administración)	104
4.29	Pestaña de la lista de interface del Vlan (Administración)	105
4.30	Pestaña de asignación de IP a las interfaces	105
4.30	Pestaña de asignación de IP a la interface Administración	106
4.31	Pestaña de asignación de IP a la interface Laboratorio	106
4.32	Pestaña de asignación de IP a la interface Agronomía	107
4.33	Pestaña de asignación de IP a la interface Hot Spot	107
4.34	Pestaña de configuración interna o externa de IP de las interfaces	108
4.35	Pestaña de anulación de opción	108
4.36	Pestaña de configuración del Pool Servers	109
4.37	Pestaña de configuración del Pool Administración	109
4.38	Pestaña de inicio de los rangos	110
4.39	Pestaña para definir DNS	110
4.40	Pestaña general para configurar políticas de NAT	111
4.41	Pestaña action para configurar políticas de NAT	111
4.42	Pestaña de configuración DHCP	112
4.43	Pestaña de configuración de las redes	113
4.44	Pestaña de configuración de la red de Administración	113
4.45	Pestaña de asignación de direcciones IP	114
4.46	Pestaña de asignación de direcciones IP fijas	114
4.47	Pestaña de configuración de Servidor NTP	115
4.48	Pestaña de configuración de cliente NTP	116
4.49	Pestaña de configuración de datos	116

4.50	Pestaña del servidor web Proxy	117
4.51	Pestaña de configuración del servidor web Proxy	118
4.52	Pestaña de redireccionamiento del NAT Rule	119
4.53	Pestaña de Action de redireccionamiento del NAT Rule	119
4.54	Pestaña general del NAT Rule	120
4.55	Pestaña de Action del NAT Rule	120
4.56	Pestaña de Firewall del NAT	120
4.57	Pestaña general de Firewall Rule	121
4.58	Pestaña Action de Firewall Rule	121
4.59	Pestaña de filtrado del Firewall	122
4.60	Pestaña de bloqueo de pornografía	123
4.61	Política 2 para el bloqueo de pornografía	123
4.62	Política 3 para el bloqueo de pornografía	124
4.63	Pestaña de bloqueo del Messenger	125
4.64	Pestaña de bloqueo del Skype	125
4.65	Pestaña de bloqueo del Mp3	126
4.66	Pestaña de bloqueo de archivos Avi	127
4.67	Pestaña de políticas del servidor web Proxy	127
4.68	Pestaña general del balanceo de cargas	128
4.69	Pestaña extra del balanceo de cargas	129
4.70	Pestaña action del balanceo de cargas	129
4.71	Pestaña general del balanceo de cargas (política 2)	130
4.72	Pestaña action del balanceo de cargas (política 2)	130
4.73	Pestaña de política de mangle del balanceo de cargas	131
4.74	Política de ruteo del balanceo de cargas	131
4.75	Pestaña de control de ancho de banda	133
4.76	Pestaña general de control de ancho de banda	133
4.77	Pestaña de colas configuradas de ancho de banda	134
4.78	Pestaña de colas del ancho de banda habilitadas entre horarios	135
4.79	Pestaña de colas del ancho de banda habilitadas entre horarios	135
4.80	Pestaña de configuración de la lista de scripts	137

4.81	Pestaña de configuración del primer evento	137
4.82	Pestaña de configuración del segundo evento	138
4.83	Pestaña de configuración de eventos del ancho de banda	138
4.84	Pestaña de configuración de RF y HOTSPOT	139
4.85	Pestaña general de configuración de RF y HOTSPOT	139
4.86	Pestaña wireless de configuración de RF y HOTSPOT	140
4.87	Pestaña data rates de configuración de RF y HOTSPOT	141
4.88	Pestaña advanced de configuración de RF y HOTSPOT	142
4.89	Pestaña WDS de configuración de RF y HOTSPOT	142
4.90	Pestaña NSTREME de configuración de RF y HOTSPOT	143
4.91	Pestaña TX power de configuración de RF y HOTSPOT	143
4.92	Pestaña status de configuración de RF y HOTSPOT	144
4.93	Pestaña comprensión status de configuración de RF y HOTSPOT	144
4.94	Pestaña traffic de configuración de RF y HOTSPOT	145
4.95	Pestaña de configuración de HOTSPOT	146
4.96	Pestaña de configuración de ip (HOTSPOT)	146
4.97	Pestaña de asignación de pool de ip	147
4.98	Pestaña de selección de certificado	147
4.99	Pestaña de asignación del servidor STMP	147
4.100	Pestaña de asignación de los DNS	148
4.101	Pestaña de comprobación delos DNS	148
4.102	Pestaña de usuario	148
4.103	Pestaña de configuración de parámetros	149
4.104	Pestaña general de configuración del profile hspof1	150
4.105	Pestaña login del profile hspof1	150
4.106	Pestaña radius del profile hspof1	151
4.107	Pestaña generación de users	152
4.108	Pestaña de desactivación de advertencias	152
4.109	Pestaña Script del hotspot	153
4.110	Pestaña general de seguridad del Profilewireless	154
4.111	Pestaña EAPde seguridad del Profilewireless	154

4.112 Pestaña static keys del security Profile	155
4.113 Pestaña de asignación de perfil de seguridad al wlan 1	155
4.114 Pestaña final de configuración	156
4.115 Sistema HOTSPOT (Ethernet Interface)	157
4.116 Ventana prueba de ingreso al sistema Hotspot	157
4.117 Ventana de acceso a internet	158
4.118 Acceso a internet por medio de la interface Hotspot	159
4.119 Antenas externas sectorial	160
4.120 Antenas externas vertical y horizontal	161

RESUMEN

Este proyecto tiene como propósito ofrecer una solución tecnológica para dotar de servicios de comunicación inalámbrica a todas las áreas correspondientes a la Facultad Técnica para el desarrollo de la UCSG, definiendo todos los parámetros técnicos que se deben cumplir y la normativa a seguir para operar redes inalámbricas con tecnología MESH (WMNs).

Esta tesis tiene como objetivo principal brindar el servicio de conexión a través de una red WiFi en cualquier sitio de la facultad donde se encuentren tanto estudiantes como maestros y visitantes, además se presenta un estudio de los protocolos para estas redes, software y hardware a utilizar para el buen funcionamiento de la red.

En el capítulo III, se aborda el estudio realizado en RF según el área de cobertura para cubrir todas las áreas.

En el capítulo IV, se realiza el diseño de la red inalámbrica Mesh en base a los resultados obtenidos en capítulo III, aquí se determina el número de enlaces, tipo de enlaces, puntos de acceso, cobertura, así como las características técnicas de los equipos necesarios para la implementación de la red.

En este capítulo, se da un presupuesto referencial para la implementación de la red con referencia a los precios reales en el mercado, en la que se incluye costos de los equipos, infraestructura, mantenimiento y operación, además se presentan las conclusiones y recomendaciones que se han obtenido en la elaboración del proyecto.

ABSTRACT

This project aims to provide a technological solution to provide wireless communication services to all areas relevant to the Technical Faculty of the UCSG development, defining all technical parameters that must be met and the rules to follow to operate wireless networks MESH technology (WMNS).

This thesis aims to provide the service main connection through a WiFi network anywhere in the faculty where they are both students and teachers, and visitors also presents a study of protocols for these networks, software and hardware to use for the proper functioning of the network.

In capitulated III study addresses the RF as the coverage area to cover all areas.

In capitulated IV, are designing wireless mesh network based on the results obtained in Chapter III, this determines the number of links, types of links, access points, coverage as well as the technical characteristics of the equipment necessary for the implementation of the network.

In this chapter, there is a reference budget for network implementation with reference to the actual market price, which includes equipment costs, infrastructure, maintenance and operation, and presents conclusions and recommendations been obtained in the development of the project.

CAPITULO I

GENERALIDADES

1.1 INTRODUCCIÓN

La evolución del Internet ha propiciado recursos y herramientas necesarias para las acciones sociales, económicas y didácticas. Este proyecto propone realizar el análisis e implementación de una Red Mesh para el acceso inalámbrico (WiFi) a internet en la Facultad Técnica para el Desarrollo en la Universidad Católica de Santiago de Guayaquil mediante el uso de computadoras portátiles y teléfonos inteligentes, así como cualquier otro dispositivo WIFI, con el propósito de brindar el acceso de esta tecnología a todos los estudiantes y visitantes que se encuentren en el área comunitaria de la Facultad para que puedan incrementar sus niveles de productividad y competitividad en el campo educativo; además como también su proyección profesional.

Las redes inalámbricas de malla son el siguiente paso a la evolución de la arquitectura inalámbrica, la prestación de servicios para una gran variedad de aplicaciones tanto personal, campos educativos y áreas metropolitanas. A diferencia de las redes WLAN, las redes Mesh son sistemas auto- configurables en la que cada Punto de Acceso (AP) puede transmitir mensajes en nombre de los demás, lo que aumenta el rango de operación y el ancho de banda disponible. Las principales ventajas de las redes de malla inalámbricas incluyen la facilidad de instalación, sin costo alguno por cable, conexión automática entre los nodos, la flexibilidad de la red, descubrimiento de nuevos nodos agregados, la redundancia y facilidad de auto-repararse.

Las redes Mesh han atraído la atención de muchos técnicos interesados en implementar redes comunales, debido a los valores implícitos que éstas tienen. Este documento contiene información teórica sobre los protocolos y arquitecturas de las redes Mesh que ayudarán a comprender de mejor forma el

funcionamiento de este tipo de redes, así como la metodología de trabajo seguida para el diseño de la red. Un aporte importante que se hace en este proyecto consiste en la aplicación de estándares IEEE802.11 en largas distancias lo que reduce aún más los costos de implementación de la red, pues los equipos con estándar IEEE802.11 son relativamente baratos comparados con otras soluciones tecnológicas, como por ejemplo Wi-Max, otra ventaja al usar esta tecnología es el uso de bandas de frecuencias libres lo que reduce el problema de adquirir una banda licenciada para que opere la red.

1.2 JUSTIFICACIÓN

La Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil en su plan de expansión y mejoramiento de servicios para sus estudiantes me ha motivado a realizar esta tesis para la implementación de una solución inalámbrica de acceso a internet y servicios convergentes basada en una infraestructura de Red Mesh aplicada en el área comunitaria y salones de clase de la facultad. El acceso mediante el uso de dispositivos WiFi le garantiza una alta confiabilidad de conectividad y un ancho de banda adecuado con el cual podrán navegar a internet a gran velocidad.

Se formula el esquema de una red inalámbrica Mesh que tiene mejoras técnicas específicas sobre el resto de redes inalámbricas, ya que son factibles de realizar y demandan de poco mantenimiento.

1.3 HIPÓTESIS

Mediante esta investigación se analizará y diseñará una red Mesh, que permita la conexión de dispositivos inalámbricos para la navegación en internet, realizado como una ayuda para la formación académica de los estudiantes de la

Facultad de Educación Técnica Para el Desarrollo de la “Universidad Católica de Santiago de Guayaquil”,

1.4 DESCRIPCIÓN DEL PROBLEMA

Después de haber realizado el estudio técnico a nivel de cobertura de internet inalámbrico, se observó algunos problemas que se mencionan a continuación:

- Falta de implementación de una red inalámbrica en toda la Facultad Técnica
- Internet limitado
- Se ocupan Wifi caseros
- Falta de seguridad en páginas de internet
- Escaso niveles de señal dentro de los laboratorios y aulas de la Facultad

Una vez observado y analizado estos problemas se considera que a través de esta red se logre la comunicación sin necesidad de extender cables, y así lograr la comunicación en cualquier lugar de la Facultad; haciendo posible la compartición de recursos, información de los usuarios y contar con el acceso a Internet en cualquier lugar donde se encuentren tanto los alumnos como el personal docente.

1.5 OBJETIVOS

1.5.1 Objetivo General

Diseñar una red Inalámbrica Mesh o Mallada para ser utilizada sobre la banda 2.4GHZ y 5 GHZ liberada; a través de nodos montados en diferentes

sitios ubicados estratégicamente en toda la Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil.

1.5.2 Objetivos Específicos

- Permitir a los alumnos un intercambio más rápido y eficaz de información y acceso a internet por medio de señales de transmisión inalámbrica dentro de todo el entorno de la Facultad Técnica para el Desarrollo.
- Permitir el acceso a la red o internet con equipos móviles portátiles, en lugares en los que no se dispone normalmente de red cableada.

CAPITULO II

MARCO TEÓRICO

2.1 Arquitecturas y protocolos de redes MESH (WMNs)

2.1.1 Redes inalámbricas IEEE 802.11

El estándar IEEE 802.11, delimita el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

Según el trabajo académico de (Chiluisa & Ulcuango, 2009) destacan el uso de frecuencias radioeléctricas gratuitas, que están en la denominada bandas ISM de 2,4 GHz y 5,8 GHz, lo que abarata considerablemente su costo operativo.

A continuación se describen los distintos estándares que componen la familia IEEE 802.11.

2.1.1.1 IEEE 802.11a

La revisión 802.11a fue aprobada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 sub-portadoras OFDM (*orthogonal frequency-division multiplexing*) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales sin solapamiento, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar

con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

2.1.1.2 IEEE 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbits sobre TCP y 7,1 Mbit/s sobre UDP.

2.1.1.3 IEEE 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del nuevo estándar lo tomó el hacer compatibles ambos modelos. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados.

Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

2.1.1.4 IEEE 802.11n

En enero del 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 300 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (3).

Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado, y se viene implantando desde 2008. A principios de 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo estuviera implantado). Ha sufrido una serie de retrasos y el último lo lleva hasta noviembre de 2009. Habiéndose aprobado en enero de 2009 el proyecto 7.0 y que va por buen camino para cumplir las fechas señaladas.¹ A diferencia de las otras versiones de Wi-Fi, 802.11n puede

trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a).

Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.²³

En la actualidad la mayoría de productos son de la especificación b o g , sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 300 Mbps (80-100 estables).

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es objeto de promociones por parte de los distintos ISP, de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador WiFi integrado, para poder conectarse a la red.

Sin duda esta es la principal ventaja que diferencia WiFi de otras tecnologías propietarias, como LTE, UMTS y Wimax, las tres tecnologías mencionadas, únicamente están accesibles a los usuarios mediante la suscripción a los servicios de un operador que está autorizado para uso de espectro radioeléctrico, mediante concesión de ámbito nacional.

La mayor parte de los fabricantes ya incorpora a sus líneas de producción equipos WiFi 802.11n, por este motivo la oferta ADSL, ya suele

venir acompañada de WiFi 802.11n, como novedad en el mercado de usuario doméstico.

Se conoce que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1 Gb/s.⁴

2.1.1.5 IEEE 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08).

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.**[1]**

2.2 Selección Dinámica de Frecuencias y Control de Potencia del Transmisor

DFS (DynamicFrequencySelection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (TransmitterPower Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

2.3 Otros estándares

El trabajo de (Chiluisa & Ulcuango, 2009) recoge los siguientes estándares:

- 802.11c**: Define características de Acces Point como Bridges.
- 802.11d**: Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).
- 802.11e**: Calidad de servicio (QoS)2.
- 802.11f**: Protocolo de conexión entre puntos de acceso de distintos fabricantes, protocolo IAPP (Inter Access PointProtocol)
- 802.11i**: Seguridad.
- 802.11m**: Mantenimiento de redes inalámbricas.

2.3.1 Estándar IEEE 802.16 (Wi-Max)

IEEE 802.16 es una serie de estándares inalámbricos de banda ancha publicados por el Institute of Electrical and ElectronicsEngineers IEEE (Instituto de Ingenieros Eléctricos y Electrónicos). Se trata de una especificación para las redes de acceso metropolitanas inalámbricas de banda ancha fijas (no móvil) publicada inicialmente el 8 de abril de 2002. En esencia recoge el estándar de facto WiMAX.

La junta de normas del IEEE (IEEE StandardsBoard) estableció un grupo de trabajo en 1999 para el desarrollo económico de las normas para la banda ancha inalámbrica para redes de área metropolitana. El grupo de trabajo es una unidad de la red de área local IEEE 802 y el comité metropolitano red de área estándares.

Aunque la familia de estándares 802.16 se nomina oficialmente como WirelessMAN en el ámbito del IEEE, ha sido comercializado bajo el nombre de "WiMAX" que son las siglas de "WorldwideInteroperabilityforMicrowave Access" (del inglés, Interoperabilidad Mundial para Acceso por Microondas) . El WiMAXForum promueve y certifica la interoperabilidad de los productos basados en los estándares IEEE 802.16.

Por ejemplo, Wi-MAX se constituye como alternativa a ser el Backbone para Redes de Distribución Wi-Fi y la segunda para acceso a móviles. Wi-Max, es un estándar de banda ancha elaborado por el comité IEEE 802.16. Suelen llamarlo también, WMAN ya que con esta tecnología se puede alcanzar teóricamente enlaces de hasta unos 50 Km.

2.3.2 IEEE 802.16-2001, Primera versión del estándar

La primera versión del estándar fue completada en el 2001. Esta versión de Wi-Max considera un rango de espectro mayor a 10GHz (especialmente de 10 a 66 GHz), siendo la línea de vista necesaria, y el direccionamiento utiliza técnicas de ción ortogonal por división de frecuencia (OFDM). Así se soportan canales con un ancho de banda mayor a 10MHz Este primer estándar consideró la prestación del servicio con las autorizaciones correspondientes (licencias), aunque se utilice un espectro libre de licencia. Además este primer estándar fue diseñado para conexiones punto a punto.

2.3.3 IEEE 802.16a

La actualización de 802.16a, completada en enero del 2003, consideró el rango del espectro de frecuencia de 2 a 11 GHz, utiliza rangos de frecuencia tanto licenciados como no licenciados, además incorpora la capacidad de no línea de vista (NLOS) y características de calidad de servicio (QoS).

Esta versión da mayores capacidades a la capa de control de acceso al medio o MAC (medium access control). Son soportados protocolos como Ethernet, ATM e IP.

2.3.4 IEEE 802.16c

Este estándar se ocupó sobretodo del rango de 10 a 66 GHz, además desarrolla otros aspectos como la evolución de la prueba y ensayo de los posibles perfiles del sistema. Esto último es un elemento crucial en el juego de herramientas de Wi-Max, porque pasa a constituir un gran acuerdo de opciones disponibles con 802.16 en general. El intento era definir a los fabricantes los elementos obligatorios que se deben considerar para asegurar la interoperabilidad. Los elementos opcionales tales como diversos niveles de los protocolos de la seguridad incorporados permiten que los fabricantes distingan sus productos por precio, funcionalidad y el sector de mercado [1].

2.3.5 IEEE 802.16d

Las principales características de los protocolos para Wi-Max fijos, mencionados en los puntos anteriores, se han incorporado en 802.16d-2004. Por lo que éste es el reemplazo del estándar IEEE 802.16a. Teóricamente podría transmitir hasta un rango de datos de 70Mbps en condiciones ideales, aunque el rendimiento real podría ser superior a 40Mbps.

Debe tenerse presente que para este estándar se tiene tres tipos de modulación para la capa PHY: modulación con una sola portadora, modulación con OFDM de 256 portadoras y de 2048 portadoras, pero el elegido es OFDM

de 256 portadoras, debido a que en el proceso de cálculo para la sincronización se tiene menor complejidad respecto a la utilización del esquema de 2048 portadoras [1].

2.3.6 IEEE 802.16e

Wi-Max, a las cuales se agrega un soporte robusto para una banda ancha móvil.

Mientras no esté completamente fija, la tecnología está basada sobre la tecnología de OFDM. Esta técnica OFDM soporta 2K, 1K, 512 y 128 portadoras.

De manera interesante, ambos estándares soportan el esquema de 256-portadoras elegido para IEEE 802.16-2004 [1].

2.4 Características generales de las redes inalámbricas MESH

Las redes inalámbricas Mesh (WMNs) es un tipo de red radical que marca la diferencia en relación con las tradicionales y centralizadas sistemas inalámbricos, tales como las redes celulares y las redes de área local (LAN).

Unas de las características de las redes Mesh es su inherente tolerancia a fallos cuando existe algún problema en la red, incluso cuando varios nodos fallan, la facilidad de implementación de este tipo de red, y una gran capacidad de ancho de banda.

Aunque las redes inalámbricas Ad Hoc son similares a WMNs, los protocolos y arquitecturas diseñados para las redes inalámbricas Ad Hoc funcionan mal cuando se aplican en redes WMNs. Además los criterios de diseño son diferentes para ambas redes. Estas diferencias de diseño se originan principalmente debido a los tipos de aplicación para cada red. Por ejemplo, una red Ad Hoc es generalmente diseñada para ambientes de alta movilidad, por otro lado una red WMNs está diseñada para ambientes de baja movilidad.

Factores como la ineficacia de los protocolos, las interferencias de fuentes externas, compartir el espectro electromagnético y su escasez reducen aún más la capacidad que pueden alcanzar las redes inalámbricas que funcionan en base a sistemas monoradio. Con el fin de mejorar la capacidad de las redes Mesh y poder cubrir la cada vez más alta demanda de tráfico planteadas por las nuevas aplicaciones, las redes Meshmultiradio (MR-WMNs) están bajo intensa investigación. Los recientes avances en redes Mesh se basan principalmente en un enfoque multiradio. Aunque MR-WMNs proveen de mayor capacidad en comparación con redes Meshmonoradio existen todavía inconvenientes y retos que resolver. Las siguientes secciones se enfocan en el estudio, para los dos tipos de redes Mesh.

Las redes inalámbricas de malla son el siguiente paso a la evolución de la arquitectura inalámbrica, la prestación de servicios para una gran variedad de aplicaciones tanto personal, campos educativos y áreas metropolitanas. A diferencia de las redes WLAN, las redes Mesh son sistemas auto- configurables en la que cada Punto de Acceso (AP) puede transmitir mensajes en nombre de los demás, lo que aumenta el rango de operación y el ancho de banda disponible. Las principales ventajas de las redes de malla inalámbricas incluyen la facilidad de instalación, sin costo alguno por cable, conexión automática entre los nodos, la flexibilidad de la red, descubrimiento de nuevos nodos agregados, la redundancia y facilidad de auto-repararse [12].



Fig. 2.1: Aplicación de redes Mesh en la UCSG
Fuente: Autor

2.5 Topología MESH o en malla

La topología en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible transmitir y recibir datos de un nodo a otro por diferentes caminos.

Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con los otros servidores.

En una topología Mesh o en malla, cada equipo está conectado a todos los demás equipos. Aunque la facilidad de solución de problemas y el aumento de la facilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. Por ello cobran mayor importancia en el uso de las redes inalámbricas, ya que no hay necesidad de cableado. En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar topologías híbridas.

Nada es necesariamente dinámico en una Red Topología Mesh o en Malla. Sin embargo en años recientes y en redes de conexión inalámbrica el término "Mesh" es a menudo usado como un sinónimo de "AD HOC" o red móvil. Obviamente combinando las dos características de la topología MESH y las capacidades de Ad Hoc, es una proposición muy atractiva.

Mientras algunas de las grandes ventajas en entornos dinámicos, la mayoría de las implementaciones más relevantes y exitosas que han surgido hasta ahora son completamente estáticas. Como por ejemplo con Nodos/Antenas colocados en techo o Torres.

2.6 Comparación entre redes inalámbricas AD HOC y redes MESH

Entre las redes Ad Hoc y las redes Mesh. Las principales diferencias entre estos dos tipos de redes son la movilidad de los nodos y topología de la red.

Las redes Ad Hoc son redes de alta movilidad, donde la topología de la red cambia dinámicamente. Por otra parte una red WMNs tiene una topología relativamente estable con la mayoría de los nodos fijos. Por lo tanto la movilidad en redes Mesh es muy baja en comparación con las redes Ad Hoc.

CARACTERISTICAS	RED AD HOC	RED MESH
TOPOLOGIA DE RED	Altamente dinámica	Relativamente estática
MOVILIDAD DE LOS NODOS	De media y alta	Baja
TIEMPO DE SERVICIO	Temporal	Semi permanente o permanente
TIPO DE TRAFICO	Tráfico de usuario	Típicamente tráfico de usuario y tráfico de control de red
AMBIENTES DE APLICACIÓN	Comunicaciones internas	Comunicaciones internas y externas
IMPLEMENTACION	Fácil	Requiere algo de planificación

Tabla 2.1: Comparación de las redes AD HOC y MESH
Fuente: Autor

Como se puede apreciar en la tabla otra gran diferencia entre estos dos tipos de redes es el escenario de aplicación ya que las redes Mesh son diseñadas para proveer servicios de comunicaciones a bajos costos como son: servicios de internet en zonas relativamente extensas como pueden ser ciudades, barrios, etc., mientras que las redes Ad Hoc se utilizan en ambientes pequeños [3], [10].

2.6.1 Desafíos en redes Mesh

Comúnmente las redes inalámbricas Ad Hoc y las redes Mesh se basan en un solo canal o en un solo interfaz de radio. Las redes Mesh con independencia de su sencillez y alta tolerancia a fallos, se enfrentan a una limitación en cuanto a la capacidad de la red. Un enfoque para mejorar la capacidad de una red Mesh es usar múltiples interfaces de radio. Aunque el límite superior teórico de capacidad no se ve afectada ya que al utilizar

múltiples interfaces de radios el ancho de banda se divide para el número de interfaces de radio MR-WMNs provee varias ventajas como el aumento de la capacidad de la red, pero también este tipo de red se enfrenta a varios problemas y desafíos que se mencionan a continuación:

2.6.2 Confiabilidad y robustez

Una característica importante que motiva el uso de redes Mesh y sobre todo de las redes MR-WMNs se debe a que mejora la confiabilidad y la robustez de las comunicaciones.

La topología en malla en una red Mesh proporciona una alta confiabilidad, en los sistemas de acceso inalámbrico los errores en el canal pueden ser muy elevados en comparación con las redes cableadas, por lo tanto se necesita una alta calidad de comunicación durante la transmisión cuando se utiliza un canal inalámbrico.

Esto es muy importante en una red Mesh que utiliza frecuencias sin licencia, para mejorar la confiabilidad de la comunicación se puede emplear la diversidad de frecuencia mediante el uso de múltiples interfaces de radio, lo cual es difícil de lograr en sistemas mono radio. Mientras que en redes MR-WMNs puede lograr mayor tolerancia a fallos en la comunicación, ya sea por cambio de las radios, los canales, o mediante el uso de radios múltiples simultáneamente.

2.6.3 Gestión de recursos

La gestión de los recursos se refiere a la gestión eficiente de los recursos de la red como son: la energía, el ancho de banda, interfaces, etc. Por ejemplo, el balanceo de carga a través de múltiples interfaces podría ayudar a prevenir que cualquier canal en particular que esté muy saturado pueda convertirse en un cuello de botella esto también podría ayudar para obtener una alta velocidad de transmisión de datos. Una importante ventaja de utilizar un sistema multiradio en

una red Mesh es la posibilidad de tener calidad de servicio a través de la diferenciación de servicio [12].

2.6.4 Arquitecturas en redes Mesh

La Arquitectura de las redes Mesh se apoyan sobre una infraestructura modular que permite realizar un diseño escalable con tanta precisión como requiera casa aplicación individualizada.

Los nodos son utilizados tanto para los dispositivos de los clientes (red de acceso) como para la propia comunicación entre nodos.

Gracias a la tecnología empleada en las redes Mesh se consigue mayor capacidad de transmisión con menor latencia (suma de retardos temporales dentro de una red). De este modo, los usuarios pueden disponer de diferentes aplicaciones en tiempo real.

Una red inalámbrica Mesh (WMNs) puede ser diseñada basadas en tres diferentes arquitecturas de red:

- Arquitectura plana

- Arquitectura jerárquica

- Arquitectura híbrida

2.6.4.1 Arquitectura plana

En una red plana WMNs, la red está formada por los equipos cliente que actúan como host4 y router. En este caso, todos los nodos están al mismo nivel. Los nodos de los clientes inalámbricos coordinan entre sí para proporcionar enrutamiento, configuración de la red, provisión de servicios, y algún otro tipo de solicitud. Esta arquitectura es la más parecida a una red Ad Hoc y es el caso más simple entre los tres tipos de arquitecturas WMNs. La principal ventaja de

esta Arquitectura es su sencillez, y sus desventajas incluyen la falta de escalabilidad y limitaciones de recursos. Los principales problemas a resolver en el diseño de esta arquitectura WMNs son: esquema de direccionamiento, enrutamiento, servicios. En una red plana, el direccionamiento es uno de los problemas que llegan a impedir la estabilidad.

2.6.4.2 Arquitectura jerárquica

En una arquitectura jerárquica, la red tiene múltiples niveles jerárquicos en la que los nodos del cliente forma el nivel más bajo dentro de la arquitectura.

Estos nodos del cliente pueden comunicarse con la red que está formada por router. En la mayoría de los casos, los nodos WMNs se dedican a formar un Backbone de una red troncal WMNs. Esto significa que los nodos que forman el Backbone no pueden originar o terminar el tráfico de datos como los nodos del cliente. La responsabilidad de auto-organizar y mantener la red troncal está a cargo de los routerWMNs, algunos de los cuales pueden tener interfaz externa a Internet y a esos nodos se los llama nodos pasarela.

2.6.4.3 Arquitectura híbrida

Este es un caso especial de redes jerárquicas WMNs, donde la red WMNs utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de otras infraestructuras tales como las redes celulares, redes Wi-Max, o las redes satelitales.

Criterios de diseño en redes inalámbricas Meshmultiradio MR-WMNs

Las principales ventajas de utilizar redes MR-WMNs son el aumento de la capacidad, escalabilidad, fiabilidad, robustez, y flexibilidad de implementación. A pesar de las ventajas de utilizar un sistema de multiradio para WMNs, existen muchos desafíos para el diseño de un sistema eficiente MR-WMNs. En esta sección se examinan las cuestiones a tener en cuenta para el diseño de una MR-WMNs. Las principales cuestiones pueden clasificarse en:

diseño de la arquitectura, diseño MAC, diseño de protocolos de enrutamiento y diseño de métricas, que se explican a continuación.

2.7 Características específicas de las redes MESH

La tecnología de las redes inalámbricas tipo Mesh está creciendo enormemente de manera gradual a un punto donde no puede ser ignorada por la sociedad tecnológica, cuando se considera el despliegue de las tecnologías de redes inalámbricas en la actualidad.

El primer despliegue de una comunidad Mesh es gran escala han demostrado suficientes ventajas para motivar futuros experimentos. Esto hace que las redes Mesh sean una de las tecnologías más prometedoras en los próximos años, y este a la vanguardia respecto a los demás [3].

2.8 Entornos de aplicación

Hasta ahora, las redes Mesh han sido mayormente propuestas para redes urbanas y redes municipales. Sin embargo, hay una gran potencial para redes MESH en zonas de conectividades rurales o lejanas donde las redes convencionales son muy costosas, o simplemente de muy difícil acceso para redes alambradas.

Para zonas rurales la combinación de enlaces WIFI de larga distancia con redes MESH representan indudablemente la forma más económica de ofrecer conectividad , y constituyen tecnologías que pueden ser instaladas por las propias comunidades sin necesariamente depender de las empresas tradicionales de comunicaciones , que a menudo son renuentes a hacer las inversiones necesarias para ofrecer servicio de zonas de baja densidad de población o habitadas por gentes de escasos recursos económicos por temor a no recuperar las ingentes inversiones requeridas para dar servicios con los métodos tradicionales.

2.8.1 Áreas Rurales

Permiten introducir servicios de banda ancha en entornos rurales para implantar servicios sociales esenciales y promocionar la sociedad de la información.

La Instalación en esta zona de las redes inalámbricas malladas ofrece innumerables ventajas:

- No requiere ninguna infraestructura precia de telecomunicaciones
- Su implantación resulta rentable
- Cada nodo presta cobertura a grandes extensiones
- Enlaces directos de “ Backhaul” entre nodos
- Posibilidad de utilización de repetidores que resuelven problemas de orografía y salvan largas distancias

2.8.2 Áreas Metropolitanas

La aplicación de esta tecnología en grandes ciudades presenta notables ventajas en su instalación y uso:

- Facilidad de implantación : se utiliza el mobiliarios urbano como soporte para su instalación y elimina necesidad de realizar obra civil
- Ajuste preciso de las zonas de cobertura al entramado de la calle y avenidas de las grandes ciudades
- Uso de nodos repetidores
- Uso de antena directivas
- Flexibilidad de interconexión
- Aprovechamiento de infraestructura existente
- Utilización de Backbone propio.

2.8.3 Áreas Municipales

Las redes inalámbricas Mesh son una solución natural para la implantación de nuevas tecnologías en entornos municipales. Su utilización puede destinarse a servicios como:

- Seguridad ciudadana
- Supervisión y control del tráfico
- Servicios al ciudadano en materias de sociedad de la información :
Acceso a internet en centros escolares y bibliotecas, así como información y orientación turísticas entre nodos.

2.9 Técnicas de funcionamiento

En las redes Mesh, cada nodo de radio múltiple soporta una cobertura en todas direcciones, esto es según su tipo de antena.

Para logra la disponibilidad del sistema de red, se combinan diferentes técnicas:

- ✓ Tanto la potencia como la velocidad de transmisión cambian dinámicamente en cada uno de los enlaces para compensar efectos como “Fading”o “shadowing”(Desvanecimiento o sombreado).
- ✓ Los algoritmos de enrutamiento tiene en cuenta el estado de las conexiones de radio y seleccionan la mejor ruta basándose en la capacidad disponible, la latencia y el rendimiento del enlace.
- ✓ Para incrementar el tiempo de operación de los equipos y minimizar los cortes de comunicaciones, el tráfico de cada equipo puede ser equilibrado encaminándolo a través de dos o más rutas minimizando, además posibles problemas por saturación de enlaces u otros fallos.
- ✓ Los equipos calculan continuamente los posibles caminos alternativos de modo que es posible enrutar el tráfico minimizando la pérdida de información debido a posibles fallos en el enlace.

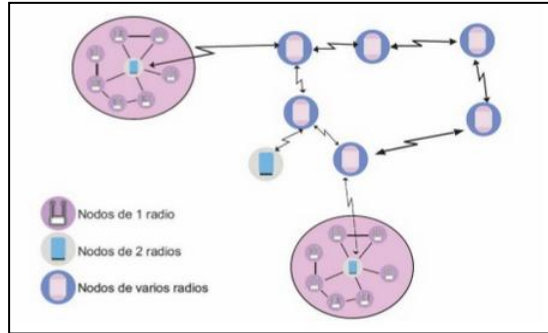


Fig. 2.2:Funcionamiento de los nodos en una red MESH

Fuente: http://wn.com/redes_mesh

2.10 Topología de control de la red

Topología de control se define como la capacidad de manipular tanto los parámetros de la red como la ubicación de los nodos, la movilidad de los nodos, la energía, las propiedades de la antena, y las interfaces de red. La topología de control tiene la capacidad de modificar ya sea una sola vez los parámetros durante la actividad de la red, en la fase de inicialización o como una actividad periódica durante el tiempo de funcionamiento de la red. El uso eficaz de la topología de control de la red puede ayudar a mejorar la capacidad. Los objetivos de los mecanismos de topología de control son la conectividad, la capacidad, fiabilidad, tolerancia a fallos y la cobertura de la red.

2.11 Soluciones multiradio para la capa de enlace

La escalabilidad de la red es el más importante problema que afecta en gran escala a una red WMNs. Las razones principales detrás de la falta de escalabilidad en una red WMNs son las siguientes:

- ✓ El carácter half-duplex de los radios WLAN
- ✓ Las colisiones debido al problema del terminal oculto
- ✓ La pérdida de recursos debido a problemas del nodo expuesto
- ✓ Las dificultades en el manejo de un sistema multicanal.

Algunos de los problemas antes mencionados pueden ser resueltos por una MR-WMN. Existen varias soluciones de capa de enlace tales como protocolo de unificación multiradio (MUP) que se analizan a continuación.

2.12 Protocolo de unificación multiradio [MUP]

El MUP es una solución de capa de enlace para proporcionar una capa virtual que controla múltiples interfaces de radio a fin de optimizar el uso del espectro en una red MR-WMNs.

Los principales objetivos de diseño del protocolo MUP son los siguientes:

- ✓ Reducir al mínimo las modificaciones de hardware
- ✓ Evitar hacer cambios en los protocolos de capa superior.

El MUP proporciona una única interfaz virtual a las capas superiores ocultando las múltiples interfaces físicas y canalizar mecanismos de selección para escoger un canal adecuado para la comunicación entre nodos. MUP es implementado en la capa enlace y por tanto las capas superiores no necesitan experimentar ningún cambio para utilizar de forma eficiente múltiples interfaces de radio.

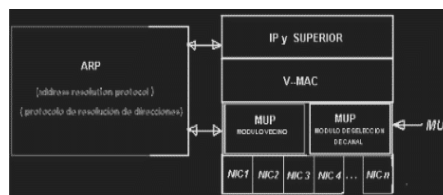


Fig. 2.3: Representación de la arquitectura MUP
Fuente: www.wikipedia.org/wiki/IEEE_802.11 [20]

Una de las principales tareas que hace la capa MUP es vigilar la calidad del canal entre un nodo y sus vecinos de tal manera que el nodo puede elegir la mejor interfaz para comunicarse con un nodo vecino. Con el fin de virtualizar múltiples interfaces de radio con una dirección MAC diferente, MUP utiliza una dirección MAC virtual que oculta eficazmente las múltiples direcciones físicas

que tiene cada tarjeta de red inalámbrica. Esto hace que la capa física aparezca para las capas más alta como una única interfaz.

MUP emplea dos diferentes esquemas para la selección de interfaces de radio, estos esquemas son llamados MUP-Random y MUP-Channel-quality.

De acuerdo con el esquema MUP-Random que es el esquema básico, un nodo al azar elige una interfaz para la transmisión de un paquete hacia un nodo destino. El esquema MUP-channel-quality está diseñado para mantener la información del estado del canal (conocida también como calidad métrica del canal) este esquema escoge entre algunos nodos y elige el mejor canal basado en mensajes de sondeo de información del estado del canal. El uso de mensajes de sondeo permite a la capa MUP obtener información sobre el estado del canal.

MUP consta de dos módulos:

- ✓ Módulo vecino
- ✓ Módulo de selección de canal.

El módulo vecino proporciona tablas y el estado de los canales de nodos vecinos.

El módulo MUP de selección de canal elige el canal más adecuado.

Cada nodo elige y mantiene la información de calidad del canal para todas las interfaces mediante el intercambio de mensajes de sondeo.

El retardo del viaje de ida y vuelta experimentado por el mensaje de sondeo es utilizado como canal de observación de la calidad de la métrica. Este retardo de viaje de ida y vuelta incluye el retardo debido al protocolo MAC de contención, la carga de tráfico, las interferencias en el canal, las colisiones de paquetes, y el retardo de procesamiento entre los nodos finales. Con el fin de reducir el retardo, que en general podría ser muy alto en un nodo que tiene gran

carga, MUP proporciona una alta prioridad para los paquetes de sondeo ya sea colocando el paquete a la cabeza de los demás paquetes mediante el uso de mecanismos de prioridad definidos en los protocolos MAC tales como IEEE 802.11e.

Las ventajas de MUP son las siguientes:

- ✓ Puede trabajar con nodos que tengan una interfaz única o múltiples interfaces
- ✓ aísla a las capas superiores de 17 conocer los protocolos que manejan múltiples interfaces de radio
- ✓ Mejora la eficiencia del espectro y el rendimiento del sistema.

Algunas de las desventajas son las siguientes:

- ✓ La asignación de canales es ordinaria y, por lo tanto MUP no podrá hacer uso de los mejores canales disponibles
- ✓ La exigencia de prioridad para los paquetes de sondeo, hace a MUP inutilizable en redes WMNs basadas en estándares IEEE 802.11a, IEEE 802.11b, IEEE802.11g, debido a que el protocolo MAC utilizado en estos estándares no permite el uso adecuado de múltiples interfaces
- ✓ MUP decide cual canal utilizar en un nodo local y este canal a veces puede que no sea el más óptimo sobre los otros canales disponibles, esto afecta en la utilización adecuada de los recursos globales de la red.

Otra cuestión con MUP es la asignación de canales para nuevos nodos que entran en funcionamiento en la red, para una red que tiene múltiples canales, se hace necesario el reinicio de todo el sistema, para determinar cuáles son los canales que se asignarán a las interfaces de los nuevos nodos con el fin que estos puedan comunicarse con el resto de la red.

2.13 Protocolos de control de acceso al medio para MR-WMNs

El diseño de protocolos MAC es importante en una red MR-WMNs en comparación con redes WMNs de un solo radio a causa de problemas adicionales que esta enfrenta. Aquí se presenta algunas de las recientes propuestas para protocolos MAC en redes MR-WMNs. Estos protocolos son los MCSMA, ICSMA.

2.13.1 Acceso múltiple por detección de portadora multicanal (MCSMA)

El protocolo MAC MCSMA es similar al sistema FDMA (Acceso múltiple por división de frecuencia). En este protocolo el ancho de banda disponible se divide en anchos de banda más pequeños para tener $n+1$ canales, es decir, n canales de datos y un canal de control. Esta división es independiente del número de nodos en el sistema. Un nodo que tiene paquetes para ser transmitidos selecciona un canal óptimo de datos para su transmisión.

Cuando un nodo está inactivo, es decir, no transmite paquetes de información, monitorea todos los n canales de datos y todos los canales por los cuales a recibido el TRSS (total received signals trength = total de intensidad de la señal recibida), el TRSS se estima por la suma de componentes individuales de señal de múltiples rutas, los 18 canales que tienen un TRSS por debajo de ST (sensing threshold = sensibilidad del umbral) son marcados como canales inactivos.

Cuando un canal está inactivo durante un determinado tiempo, se añadirá a la lista de canales libres. El mecanismo de transmisión de paquetes con el protocolo MCSMA es el siguiente.

Cuando un nodo potencial está en la capacidad de enviar y recibir paquetes de datos, comprueba en su lista de canales, si existe algún canal libre, el transmisor comprueba si el canal por el cual transmitió con éxito el último paquete está incluido en la lista de canales libres, se iniciará la

transmisión por este canal. Si la lista de canales libres está vacía, espera a que un canal esté inactivo. Tras detectar un canal inactivo, el transmisor espera por un LIFS (longinter frames pace= gran espacio interframe), seguido por un acceso aleatorio back-off.

Después del período de back-off el transmisor comprueba nuevamente el canal, y si el canal está aún inactivo, se inicia la transmisión por ese canal. En el caso que el último canal utilizado para la transmisión no esté presente en la lista de canales libres, el transmisor elige al azar un canal entre los canales inactivos, incluso en estos casos, el transmisor espera a que el canal siga inactivo durante el tiempo LIFS más el período de back-off, si después de este tiempo el TRSS del canal supera al ST, entonces el proceso de back-off se cancela, cuando el TRSS del canal va por debajo de ST se inicia la transmisión. Si un canal está siendo ocupado para una transmisión exitosa, se da prioridad a otro canal para poder entablar la transmisión, siempre y cuando $n > N$, donde n es el número de canales de datos y N es el número de nodos de la red [10].

2.13.2 Acceso múltiple por detección de portadora intercalado (IC SMA)

El IC SMA es un nuevo protocolo multicanal de acceso al medio. Está diseñado para superar el problema del terminal expuesto, que está presente en los sistemas de un solo canal, basados en sensor portadoras de los protocolo MAC.

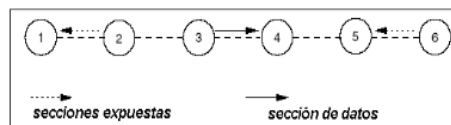


Fig. 2.4:Protocolo IC SMA

Fuente:www.wikipedia.org/wiki/IEEE_802.11[20]

Cuando existe una transmisión en curso entre los nodos 3 y 4, los otros nodos en la red es decir los nodos 2 y 6 no están autorizados a transmitir a los nodos 1 y 5 respectivamente. Esto se debe a dos razones:

- ✓ Ninguna transmisión simultánea del nodo 2 es posible por su propio mecanismo de sensor portadora
- ✓ El reconocimiento de los paquetes recibidos por el nodo 3 también puede colisionar por la transmisión del nodo 2.

Del mismo modo el nodo 6 es impedido para la transmisión porque el reconocimiento de los paquetes originados por el nodo 5 que podrían colisionar con la recepción de los paquetes de datos del nodo 4.

Por lo tanto, los nodos 2 y 6 son designados como transmisor-receptor respectivamente.

ICSMA es un sistema de dos canales de intercambio de paquetes. En comparación con el esquema CSMA/CA, el protocolo de proceso es intercalado entre los dos canales[10].

2.14 Protocolos de enrutamiento multiradio para redes Mesh

Además del diseño de la arquitectura y del diseño del protocolo MAC, el rendimiento de una red WMNs y de una red MR-WMNs se ven afectadas por el diseño del protocolo de enrutamiento y las métricas de enrutamiento.

2.15 Niveles o capas de las redes MESH

Se han diseñado varias herramientas para ayudar a los diseñadores de los protocolos a entender las partes del problema de comunicación y planear la familia de protocolos, una de estas herramientas y la más importante es el modelo de capas esto es solo una manera de dividir el problema de la comunicación en partes llamadas capas.

La familia de protocolos puede diseñarse especificando un protocolo que corresponda a cada capa.

La organización internacional de estandarización (OSI) definió uno de los modelos más importantes y el más utilizado, el modelo de siete capas, en este tema se hablara de las diferentes capas de las cuales se componen las redes MESH [1].

2.15.1 Capa o nivel físico

Esta capa se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.

La carga de un canal de radio depende del nivel de interferencias recibido o mejor dicho de su SNR (Señal ruido).

Al tener una mayor densidad de nodos en este tipo de redes, y siendo el espectro radioeléctrico limitado, es necesario optimizar al máximo la utilización del canal minimizando la interferencia, son la selección dinámica de frecuencia (DFS) y el control de potencia (TPC) aunque para ser aplicados en estas arquitecturas necesitan un control por parte de los protocolos de capas superiores.

La utilización de antenas inteligente, de antenas adaptivas o de antenas auto configurables y reprogramables vía software (radios cognitivas) son algunos de los tópicos actuales de investigación que pueden ayudar a mejorar y aumenta la capacidad ofrecida por las redes inalámbricas tipo MESH. También la utilización de técnicas MIMO (*Multiple Output , Multiple Input*).

Según (Chiluisa & Ulcuango, 2009) mejoran la eficiencia espectral permitirán el estándar 802.11n el cual la velocidad real de transmisión podría llegar a los 108Mbps (lo que significa que las velocidades teóricas de transmisión seria aún mayores) y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g , cerca de 40 veces más rápida que una red bajo el estándar 802.11b.

En un futuro próximo, se espera que los distintos clientes dispongan de varias interfaces de red, empleando en cada momento la más adecuada según las necesidades del usuario de las redes inalámbricas tipo Mesh [1].

2.15.2 Capa de enlace o capa MAC

Esta capa se encarga de asegurar con confiabilidad el medio de transmisión, ya que realizan la verificación de errores, retransmisión, control fuera de flujo y la secuencia de las capacidades que se utiliza en la capa de red.

El acceso al medio de la redes inalámbricas tipo Mesh, debe proporcionar mecanismos que solventan las limitaciones de los estándares actuales, como IEEE 802.11, que se basa en CSMA /CA (Acceso múltiple por detección de portadora con evasión de colisiones que es un protocolo del control de redes de bajo nivel que permiten múltiples estaciones utilicen un mismo medio de transmisión) con serias limitaciones en las redes multisaltos debido a los problemas del nodo oculto y del nodo expuesto.

Mecanismo deterministas de acceso al medio , basados en TDMA (time división múltiple Access) que es una técnica de multiplexación que distribuye las unidades de información en ranuras (slots)alternas de tiempo , proveyendo acceso múltiple a un reducido número de frecuencias , la cual puede ser bastante útil si existe una buena sincronización , mientras que la opción de emplear CDMA (Code división múltiple acces) lo cual es un término genérico para varios métodos de multiplexación o control de acceso al medio basados en la tecnología de espectro ensanchado , este puede disminuir los efectos de interferencia , ya que dos nodos pueden ocupar simultáneamente el canal empleado códigos distintos .

Hay que recordar que los equipos basados en la familia de estándares IEEE802.11 presentan un bajo costo y una gran aceptación en el mercado, por lo que son la solución más atractiva para implementar redes multisalto.

Debido a esta razón , existe multitud de propuestas de nuevos protocolos MAC para las redes 802.11 basados en distintos objetivos de diseño y , además el IEEE se encuentra trabajando en el estándar 802.11s , el cual incluirá en su capa MAC mecanismos para el encaminamiento a nivel 2 y un acceso al medio más eficiente.

Pero la capa MAC no solo se centra en el acceso al medio, la utilización de varios canales simultáneamente también puede ser encontrada por la capa MAC o por alguna capa de enlace superior, tal y como muestra las propuestas de MMAC (multichannel MAC) y HMCP (Irbid Multichannel protocol) ya que está demostrado que la utilización de varios canales simultáneos correctamente coordinados pueden mejorar la capacidad de Red.

En la primera, se emplean varios canales empleando una sola interfaz radio, por lo que se requiere señalización y coordinación para que todos los nodos escuchen el canal adecuado en cada momento [1].

2.15.3 Capa de red

A nivel de red, los protocolos de encadenamiento deberán proporcionar distintos mecanismo para el encubrimiento de caídas de enlace, balanceo de cargas proporcionando QoS (Quality of service) y además, en función del tipo de red inalámbrica tipo Mesh que se desee implementar, los parámetros de diseño de los protocolos diferirán (movilidad nivel de baterías). En resumen muchas de las propiedades de auto-configuración y auto-reparación de las redes inalámbricas Mesh son, en parte proporcionadas por los distintos protocolos de encaminamiento.

Debido a su flexibilidad y operación en redes sin infraestructura, el punto de partida en este punto son los protocolos de encaminamiento desarrollados por el grupo de trabajo MANET (mobile Ad-Hoc Networks) de IETF [1].

2.15.4 Capa de transporte

Esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario y representa el corazón de la jerarquía de los protocolos que permiten realizar el transporte de los datos en forma segura y económica.

El protocolo TCP (transport control protocol) es la base de la mayoría de las aplicaciones existentes hoy en día en las redes de datos basadas en IP. Sin embargo su eficiencia en las redes inalámbricas se ve seriamente afectada debido a que TCP supone que las pérdidas se produce que un RTT (round – tripdelaytime) no es muy viable (Típico de redes cableadas).

Estos factores no se dan en las redes inalámbricas y, mucho menos en las redes inalámbricas Mesh donde los paquetes pueden atravesar múltiples enlaces antes de llegar a su destino.

Por lo tanto para optimizar el transporte en las redes inalámbricas tipo Mesh es necesario o bien modificar el TCP para distinguir entre los motivos de las pérdidas o retardos (retransmisiones etc.) o proponer totalmente nuevos protocolos de transporte. A pesar de que la segunda opción sea más óptima o permite aplicar protocolos con mayor rendimiento en las redes inalámbricas tipo Mesh, la gran aceptación y asentamiento de TCP hace que la mayoría de propuestas que pueden ser utilizadas en el mundo real sean variaciones de TCP. [1].

2.16 Redes MESH multiradio y multicanal

La relación costo-beneficio de las tecnologías de acceso inalámbrico tales como IEEE 802.11 ha cambiado las comunicaciones y la informática de manera importante. Su éxito es debido a su despliegue en el hogar y en la pequeña empresa, donde se tiene cobertura limitada y sirve a sólo unos pocos usuarios a la vez. Actualmente existe un considerable interés en la ampliación

de redes IEEE802.11 a gran escala empresarial, para proporcionar una cobertura amplia y de banda ancha para el acceso a un número significativo de usuarios. Esto requiere de una proliferación de puntos de acceso (AP) en el área de cobertura deseada, bajo el estándar IEEE 802.11 con conjuntos de servicios básicos (BSSs). Para aumentar el alcance de la red (por ejemplo, entre un cliente y AP) se basa en reutilizar el espacio de frecuencias, asignándoles un conjunto de canales ortogonales de manera sistemática. El valor de la señal de interferencia y ruido (SINR)(signal to interferencenoise ratio) en el extremo del BSS, junto con las propiedades inherentes del protocolo de la función de coordinación distribuida (DCF), determinan esencialmente el rendimiento obtenido en el BSSs.

La expansión de la red y el rendimiento global sobre el de área de cobertura se pueden lograr mediante una combinación de enfoques como el uso de antenas directivas; con esto lo más evidente que se logra es el aumento de la disponibilidad de ancho de banda en los sistemas (esto es equivalente a más canales ortogonales). Actualmente, sólo un número limitado de este tipo de canales ortogonales están disponibles: 3 en IEEE 802.11b(2,4 GHz) y 12 en IEEE 802.11a (5 GHz), está claro que el aumento de ancho de banda para la ampliación no es una opción viable. Por consiguiente para aumentar el rendimiento de la red se requiere necesariamente de mejorar toda la pila de protocolos.

Una opción prometedora para ampliar la capacidad de una red de acceso inalámbrico es configurar la capa 2, que actualmente está previsto dentro del grupo de trabajo IEEE 802.11s. Esto implica una directa interconexión inalámbrica de un conjunto de nodos en malla para formar una red multihop.

Estos nodos forman parte de los APs que permiten el acceso directo de los clientes, así como "routers" los cuales retransmiten solo paquetes entre otros elementos de malla similar a una red Ad Hoc.

Para el diseño de redes de mayor cobertura se debe modificar los mecanismos de topología, entre ellos el control de la energía y asignación de canales (CAs).

Tradicionalmente las redes inalámbricas multihop (históricamente denominado redes de paquete de radio) están compuestos casi exclusivamente de un solo radio, estas redes no están en condiciones de escala efectiva para explotar los crecientes sistemas de ancho de banda disponible. En consecuencia, el uso de nodos de múltiples radios en una red Mesh, parece ser una de las vías más prometedoras para la expansión de la red. Varios radios aumentan en gran medida el potencial para mejorar la selección del canal y la información de ruta, mientras la malla controla la interferencia y la topología de control permite controlar la potencia.

2.17 Arquitectura MESH en 802.11

Se puede construir redes WMNs utilizando productos básicos de hardware IEEE 802.11. Sin embargo, antes de que esas redes pueden llegar a ser parte de los principales despliegues, se deben resolver algunas cuestiones como son: seguridad, QoS y gestión de redes.

Muchos de estos problemas son propios de cualquier red WMNs y no sólo de redes WMNs en base a IEEE 802.11.

La creciente disponibilidad de radios multimodo, integrados en las tarjetas 802.11a/b/g, de los clientes y dispositivos de infraestructura, permitirá implementar nuevas arquitecturas en malla. Los nodos en una malla para una red de acceso constan de dos tipos, un ligero predominio de puntos Mesh cuya única función es el enrutamiento de los paquetes de forma inalámbrica a los nodos vecinos y a otros subconjuntos de nodos MeshAPs que permiten la conexión directa con el cliente. Una pequeña fracción de estos nodos MeshAPs estarán conectados por el cable del backbone y sirven como puertas de entrada o de enlace para el tráfico de ingreso / salida.

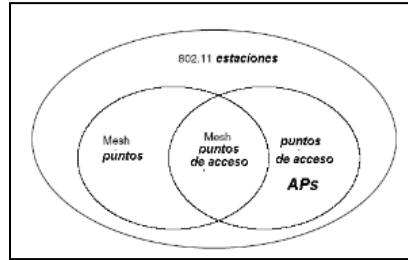


Fig. 2.5: Representación esquemática de los dos tipos de nodos Mesh: Aps y puntos Mesh
Fuente: www.wikipedia.org/wiki/IEEE_802.11

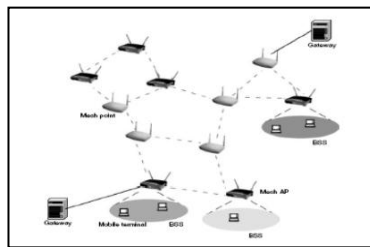


Fig. 2.6: Dos niveles de arquitectura de red Mesh
Fuente: www.wikipedia.org/wiki/IEEE_802.11

2.18 Capacidad de expansión

El aumento del rendimiento de extremo a extremo está relacionado con un aumento de los saltos, que a su vez depende del número de transmisiones simultáneas por canal, esto se puede conseguir a través de muchos factores, como puede ser la topología de red y varios atributos de los protocolos de pila de las capas 1, 2 y 3. Los atributos de la capa 1 incluyen el tipo de radio, requisitos del SINR en el receptor para la detección fiable y la propagación de la señal en medio ambiente. Los atributos de la capa 2 incluyen control de acceso al medio MAC, atributos para controlar las interferencias y los atributos de la capa 3 incluyen la elección de las métricas de enrutamiento para determinar la mejor ruta.

De este modo, la optimización global de la red requiere de un enfoque multidimensional, propuesta en el siguiente enfoque. En orden aparece la capa IP como una simple red de área local, una red Mesh puede aplicar su propia

funcionalidad de enrutamiento y otros servicios a la capa “2.5”, es decir, como una capa intermedia entre el estándar IEEE 802.11 MAC (o bajo MAC) y la capa IP.

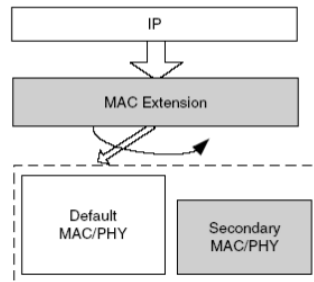


Fig. 2.7:Redes Mesh Multicanal de un solo radio
Fuente:www.wikipedia.org/wiki/IEEE_802.11

Cualquier ruta de extremo a extremo en una red multihop deben utilizarse todos los canales ortogonales disponibles, una manera de mejorar el rendimiento de la red es maximizar la reutilización espacial, es decir, maximiza el número de transmisiones simultáneas en el área de la red.

Desafortunadamente existe una limitación en los dispositivos inalámbricos de un solo radio y es que operarán solamente en modo half-duplex, y por lo tanto no puede transmitir y recibir simultáneamente, incluso si múltiples canales está disponible.

Un posible enfoque multihop es la formación de rutas para todos los nodos que utilizan el mismo canal, aunque varios canales están disponibles, sin embargo, evita el inconveniente de los grandes retardos de extremo a extremo cuando los nodos adyacentes utilizan diferentes canales de comunicación.

Esta última requiere el escaneo de canales para realizar la conmutación y una radio activa tal que dos nodos adyacentes comparten un mismo canal, lo que retarda la conmutación por nodo. Por ejemplo, el retardo de conmutación varía para el hardware en IEEE 802.11 desde unos pocos milisegundos a unos cientos de microsegundos. Esta frecuencia de conmutación de canales puede

considerarse como una vía eficaz debido a que el retardo de conmutación se manifiesta como un salto virtual a lo largo de la ruta. De ahí que, aprovechando los múltiples canales ortogonales claramente se mejora el rendimiento global con respecto a la hipótesis de un solo canal, pero a costa de aumentar el retardo de extremo a extremo.

Por todas estas razones las red Meshmultiradio introducen varios y nuevos grados de libertad con respecto a la limitación de dispositivos inalámbricos de un solo radio, se espera que los dispositivos multiradio sean un componente clave en lograr escalabilidad y adaptabilidad (como un software definido para las múltiples radios) para las futuras redes inalámbricas.

2.19 Redes MeshMultiradio

Los nodos con múltiples radios son efectivamente full dúplex, es decir, que puedan recibir en el canal C1 en una interfaz mientras simultáneamente se transmite en el canal C2 en otra interfaz, con lo que se duplica el rendimiento en el nodo.

La asignación de canales tiene una gran influencia en el rendimiento de extremo a extremo, al igual que la elección de métricas de enrutamiento para la formación de ruta. En resumen con buen diseño de las capas 1, 2, 3, aumenta el rendimiento de redes Meshmultiradio así como su tamaño.

2.19.1 Asignación de canales y enrutamiento

En una topología típica, algunos de los nodos Mesh sirven como puertas de enlace, y el tráfico desde o hacia estos portales pueden ser mucho más elevado que en otros lugares en la red. La carga de tráfico en cada enlace se ve afectada por la elección de los protocolos de enrutamiento, así como por las métricas de enrutamiento. En una red WMNs, cuando un flujo se dirige por un determinado enlace, no sólo reduce la capacidad disponible de ese enlace, sino también la capacidad disponible en otros canales. Esto se debe a que todos los

enlaces dentro del canal comparten el mismo ancho de banda total para sus transmisiones.

La discusión anterior pone en manifiesto que existe una estrecha relación entre CAs y el enrutamiento en redes de malla. Por lo tanto, con el fin de maximizar el rendimiento. Los dos problemas deben ser tratados conjuntamente. Sin embargo, en la práctica el problema común es generalmente difícil de resolver óptimamente.

Un enfoque para el problema común es resolver la asignación de canales y los problemas de enrutamiento e iterar sobre las dos fases para mejorar el rendimiento global.

2.19.2 Asignación básica de canal

El problema básico de CAs se puede plantear en términos de asignación de canales, garantizando al mismo tiempo que dos nodos vecinos tienen por lo menos un canal común (lo que asegura que los nodos vecinos puedan comunicarse).

Un método de asignación aleatorio de canales para radios puede que no sea factible. Consideremos, por ejemplo, una red en la que todos los nodos tienen dos radios y asignar uno de los cuatro canales a cada una al azar. Si algún nodo está asignado los canales 1 y 2, y su vecino se le asigna canales 3 y 4 esto lleva a que los dos nodos no tienen un canal en común, y la sesión no es factible.

El objetivo de varios algoritmos CAs es la posibilidad de elegir un canal que mejor optimice el rendimiento, a continuación presentamos uno de estos algoritmos.

2.19.3 Programación lineal entera

Un enfoque para la obtención de un óptimo CAs es plantear el problema como una programación lineal entera (ILP) (integer linear program). El objetivo es maximizar el número de transmisiones simultáneas. La solución resultante maximiza el rendimiento alcanzable en forma instantánea. Si bien una ILP a base de la formulación puede dar soluciones óptimas usando software estándar ILP, el necesario tiempo de ejecución para encontrar la solución óptima puede ser muy alto, incluso para un modesto tamaño de redes. Sin embargo, se da por concluida la búsqueda después de un cierto tiempo.

2.19.4 Métricas de enrutamiento

La métrica más simple de enrutamiento, cuenta los saltos (el camino más corto), y ha sido ampliamente utilizado en los actuales protocolos de enrutamiento Ad Hoc.

Sin embargo estos protocolos funcionan mal en las redes de malla. Una perfeccionada métrica es la métrica ETX (contar con la expectativa de transmisión). La métrica ETX asigna un peso a cada uno de los enlaces que corresponden, con el número esperado de transmisiones requeridas por el 802.11MAC, para transmitir con éxito un paquete sobre el enlace. Estas ETX asignan un peso superior a los enlaces que están sujetos a una alta pérdida de paquetes.

Esta es una mejora con respecto al enfoque de contar saltos, sin embargo, no cuenta el hecho de que los diferentes enlaces pueden usar diferentes anchos de banda o la reutilización del mismo canal a lo largo de un camino lo que reduce la capacidad disponible. La métrica ETT (expectativa de tiempo de transmisión).

Aborda el problema de multiplexación de ETX por el tiempo que necesita para cada transmisión.

2.20 Redes MESH basadas en IEEE 802.11

IEEE 802.11 se ha convertido en el estándar de facto para el hogar, empresa y el despliegue de redes de área local inalámbricas (WLANs).

La mayoría de estos despliegues operarán en el modo de infraestructura, donde un conjunto de puntos de acceso (AP) sirven de centros de comunicación para estaciones móviles y proporcionan puntos de acceso a Internet. El papel actual de IEEE802.11 se limita a los clientes móviles que se comunican a través de AP. Las economías de escala hacen que IEEE 802.11 sea una alternativa deseable incluso para interconectar estos APs en forma de una malla de red inalámbrica (WMN) como se muestra en la Figura.

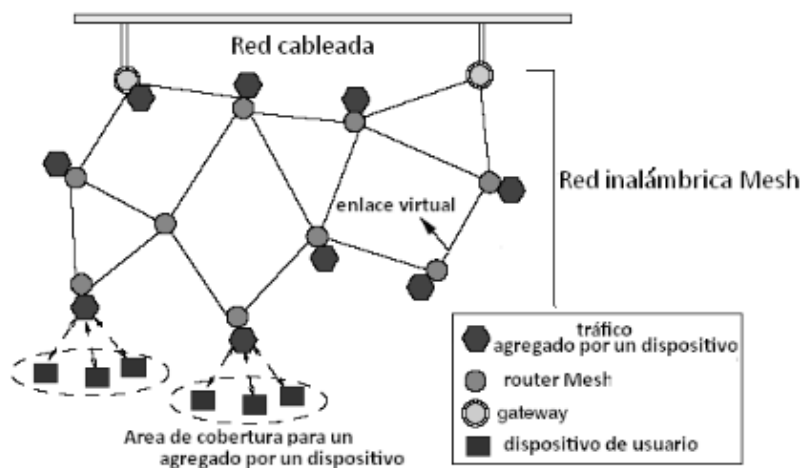


Fig. 2.8: Malla de red inalámbrica

Fuente: www.wikipedia.org/wiki/IEEE_802.11

En el núcleo de una red Mesh, al cual está conectada una red cableada a través de un conjunto de Gateway. Cada nodo WMNs tiene un radio interface que es usado para comunicarse con otros nodos WMNs a través de enlaces como se muestra en la fig.

Un nodo WMNs es equipado con un dispositivo (similar a un Access point) que interactúa con las estaciones móviles individuales. Las estaciones

móviles retransmisoras WMNs agrega tráfico de datos hacia y desde la red cableada.

Para satisfacer aplicaciones, IEEE 802.11 soporta dos modos de funcionamiento: el modo Ad Hoc que con un solo salto en la red los nodos Ad Hoc se comunican entre sí directamente, sin la utilización de un AP. EL segundo modo es el sistema de distribución inalámbrica (WDS), modalidad para la formación de transmisión punto a punto donde cada AP no sólo actúa como una estación base, sino también como un nodo retransmisor inalámbrico. Sin embargo, una red IEEE 802.11 pueden utilizarse para formar una eficaz red WMNs.

El rendimiento, la seguridad y la gestión son cuestiones que deben ser abordadas. Desde el punto de vista de rendimiento, el rendimiento bajo de extremo a extremo es un problema común en redes WMNs basados IEEE 802.11.

2.21 Problemas de rendimiento y sus causas

2.21.1 Capacidad limitada

A pesar de los muchos avances de la tecnología para la capa física (inalámbrica), la limitada capacidad sigue siendo una cuestión apremiante, incluso para redes WLAN de un solo salto. La publicidad de 54 Mbps de ancho de banda para el hardware IEEE 802.11a/g es el pico de velocidad de transmisión de datos.

Además, la máxima velocidad de transmisión en la capa enlace decrece rápidamente al aumentar la distancia entre el transmisor y el receptor.

2.21.2 Selección efectiva de ruta

La más simple métrica de enrutamiento para redes WMNs, es la métrica de contar los saltos. Sin embargo, el uso de esta métrica de contar los saltos

conduce a una selección no fiable de ruta. En primer lugar, contar los pequeños saltos se traduce en más tiempo y por tanto tendencia a más errores de salto individual. En segundo lugar esta métrica no hace nada para equilibrar la carga de tráfico a través de la red. Esto reduce la capacidad efectiva de la red WMNs.

2.21.3 El problema de compartir el canal

Los protocolos de transporte existentes hacen el mejor intento de asignar un canal de radio con un ancho de banda específico, entre los flujos de un solo nodo, en lugar de entre todos los flujos de todos los nodos que comparten el canal de radio.

Como resultado, un flujo emana de un nodo con menos densidad y con un ancho de banda de canal grande.

La equidad de TCP depende en gran medida del tiempo de ida y vuelta (RTT) de los flujos involucrados, cuando dos flujos multi salto TCP comparten el mismo enlace inalámbrico, los flujos que atraviesa un número de saltos, tiende a adquirir más de ancho de banda. Si bien esto es cierto incluso para las operaciones de TCP en la internet por cable, el problema es mucho más frecuente en una red WMNs.

En una red WMNs la mayor parte del tráfico se dirige hacia y desde los nodos gateway (nodos de puertas de enlace) que conectan una red WMN al Internet por cable.

2.21.4 Alto rendimiento de enrutamiento

El enrutamiento gobierna y regula el flujo de paquetes a través de la red WMNs.

Mientras más rutas cortas de enrutamiento, reduce al mínimo la cantidad de ancho de banda utilizado en la red para transferir los paquetes, no considera factores importantes, tales como errores de enlace (enlaces críticos), la

inteligente selección de las rutas en base de estos factores pueden no sólo mejorar la calidad de la ruta elegida para el actual flujo de paquetes, sino también permitir la admisión de paquetes con más carga en la red.

Existen diferentes técnicas de enrutamiento que están todavía en estudio como son:

- Enrutamiento vigilante de la calidad del enlace
- Enrutamiento vigilante de la interferencia
- Enrutamiento multicamino
- Enrutamiento vigilante de la diversidad
- Enrutamiento oportuno

2.22 Redes MESH multicanal

El estándar IEEE 802.11b/g y el estándar IEEE 802.11a proporcionan 3 y 11 canales, respectivamente, que podrían ser utilizados simultáneamente con un nodo adyacente. La posibilidad de utilizar múltiples canales aumenta sustancialmente la eficacia del ancho de banda disponible para los nodos de la red inalámbrica. Sin embargo, una arquitectura convencional WMNs equipa cada nodo con una sola interfaz, que siempre está sintonizada a un canal único con el fin de preservar la conectividad. Para utilizar múltiples canales dentro de la misma red, cada nodo necesita tener capacidad de conmutación de canal o estas necesitan múltiples interfaces, cada uno sintonizado, para operar en un canal diferente. La conmutación de canal requiere de una eficaz sincronización entre los nodos en el momento en que cualquier nodo transmite o recibe en un canal en particular.

Un posible esquema es tener a todos los nodos de conmutación entre todos los canales disponibles en algún orden predeterminado. Aquí una interfaz

cambia entre los canales disponibles en diferentes slots de tiempo, de forma aleatoria.

Los nodos que deseen comunicarse esperan una ranura de tiempo donde sus interfaces están en el mismo canal.

Estas secuencias no son fijas y pueden alterarse. La ventaja de este sistema es que el tráfico de carga es equilibrada en todos los canales disponibles en general logra la reducción de interferencias. Sin embargo, dicha sincronización es difícil de conseguir sin modificar la capa MAC 802.11. Por lo tanto, utilizar routers WMNs multiradio es un enfoque más prometedor para formar redes WMNs multicanal basadas en IEEE 802.11.

La asignación de canales para interfaces de radio juega un papel importante en el aprovechamiento de la capacidad de ancho de banda de esta arquitectura multiradio. Por ejemplo, una idéntica asignación de canal para todos los nodos limita sustancialmente el rendimiento que es posible alcanzar para arquitecturas de un solo radio.

El objetivo de canalizar la asignación del canal es reducir las interferencias mediante la utilización de tantos canales como sea posible, manteniendo al mismo tiempo la conexión entre nodos. En esta sección, se discuten las diferentes técnicas propuestas para llevar a cabo la asignación inteligente de canal [10].

2.23 Asignación del canal basado en la topología

La asignación del canal puede hacerse exclusivamente sobre la base de la topología de la red, con el objetivo de reducir al mínimo la interferencia en el enlace. El problema es computacionalmente difícil de conseguir, por lo que las soluciones propuestas son aproximadas.

Una de las soluciones se revisa a continuación. El algoritmo denominado, conexión de baja interferencia de asignación de canal (CIICA) revisa todos los

nodos en el orden de calidad del canal, los nodos de menor calidad son visitados primero.

Al visitar un nodo los canales se eligen y se escoge el nodo local con el canal óptimo, el objetivo es reducir al mínimo la interferencia que se ejerce entre enlaces.

Existen otras soluciones para asignación de canal en redes Mesh basadas en IEEE 802.11

- Asignación de canales mediante vigilancia de tráfico
- Asignación dinámica de canal

2.24 Interferencia inter-canal

En experimentos que se han realizado con hardware 802.11, se analiza la interferencia entre dos tarjetas en la misma máquina. El grado de interferencia depende de las posiciones relativas de las tarjetas. La colocación de tarjetas en la parte superior derecha de cada uno lleva al máximo de la interferencia, y sólo alcanza un máximo del 20% de ganancia, la pérdida del rendimiento debido a la interferencia inter-canal se encontró independencia de bandas, es decir, la degradación es casi la misma cuando el canal 1 y 6 se utiliza a la vez.

Se sospecha que esta interferencia surge debido a los filtros imperfectos presentes en las tarjetas.

Este resultado tiene implicaciones sobre la colocación de varias tarjetas en la misma máquina. Las fugas electromagnéticas de las tarjetas es necesario tener en cuenta, y una posición adecuada de la tarjeta debe encontrarse para reducir al máximo la interferencia entre tarjetas.

Una posible forma de lograrlo es usar tarjetas USB con antenas externas en vez de tarjetas PCI/PCMCIA **[10]**.

2.25 Protocolos en las redes MESH

Según los modelos de la capa OSI y TCP/IP, la funcionalidad de la asignación de ruta está localizada en la capa 3, la capa de gestión de redes que normalmente usa el protocolo de Internet (IP). Hay esfuerzos para desarrollar protocolos de asignación de ruta para las redes Mesh en la capa 2.

Aunque esto “viola” el concepto de la capa red actual, se espera obtener los siguientes beneficios:

- ✓ acceso más rápido y a más información del estado de la capa2 y de la capa física.

El enrutamiento en capa 2 es más difícil de llevar a cabo, la información adicional sobre la estructura de la red, las direcciones IP no están disponibles en las direcciones MAC, y es más difícil de hacer entre redes heterogéneas.

No obstante, las ventajas del acceso a las capas más bajas aumentarán la fiabilidad de las redes Mesh inalámbricas debido a las reacciones más rápidas y apropiadas a los cambios del ambiente de los radio canales.

Los conceptos para la selección de la ruta son los mismos, tanto para la capa 3 o la capa 2. El último sólo usa las direcciones MAC. También significa que algunos mecanismos, hasta ahora desconocidos en capa 2, tengan que ser introducidos al tiempo de vida útil (TTL), dirección de la fuente y destino como los saltos a través de la ruta inalámbrica multihop.

2.26 Requisitos de enrutamiento en las redes WMNs

Un protocolo de asignación de ruta óptimo para redes WMNs debe cumplir con lo siguiente:

- ✓ Tolerancia a fallos: un problema importante en las redes es la supervivencia, que es la capacidad de la red para funcionar en caso de

que un nodo falle. De la misma manera los protocolos de enrutamiento también deberían permitir una nueva selección de ruta en caso de fallas.

- ✓ Balanceo de carga: los routers inalámbricos Mesh son recomendados en el balanceo de carga porque ellos pueden escoger la ruta más eficaz para los datos.
- ✓ La reducción del Enrutamiento overhead: la conservación del ancho de banda es indispensable en el éxito de cualquier red inalámbrica. Es importante reducir la asignación de ruta overhead, sobre todo el causado por la retransmisión.
- ✓ Escalabilidad: una red mallada es escalable y puede ocuparse miles de nodos, ya que el funcionamiento de la red no depende de un punto mando central.
- ✓ QoS: debido a la limitada capacidad del canal, la interferencia es un factor muy importante, el gran número de usuarios y las aplicaciones multimedia en tiempo real, apoyada por la calidad de servicio (QoS) se ha vuelto un requisito indispensable en redes de computadoras.

2.27 Enrutamiento multicamino para balanceo de carga y tolerancia a fallos

Una red mallada se basa en caminos múltiples entre los nodos de la red ya que es más robusta contra alguna falla de un nodo o varios nodos. Pueden agregarse más nodos a la malla para aumentar la redundancia.

La selección de caminos múltiples entre el nodo fuente y el nodo destino, ayuda, por ejemplo, cuando un enlace está roto y la información que cruzaba por este enlace puede atravesar por otra ruta sin esperar un nuevo enrutamiento esto reduce notablemente retardo de extremo a extremo y aumenta el rendimiento.

También ayuda equilibrar la carga para prevenir la congestión y el tráfico alrededor de los nodos congestionados.

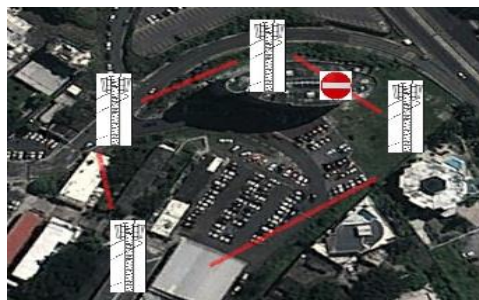


Fig. 2.9: Balanceo de carga cuando una ruta falla en la Facultad Técnica de la UCSG
Fuente:Autor

2.27.1 Enrutamiento con QoS

El enrutamiento de las redes inalámbricas multihop con QoS, necesita mantener un ancho de banda que garantice los requerimientos de la conexión y sin que la ruta se sienta afectada por la interferencia de otras rutas en la red.

Hay dos tipos diferentes de interferencia en una red multihop inalámbrica: la interferencia interflujo y la interferencia intraflujo. Para una ruta P, la interferencia interflujo ocurre cuando un enlace de P usa el mismo canal con otro enlace que no es de P dentro de su rango de interferencia; y la interferencia intraflujo ocurre cuando dos enlaces de P dentro de su rango de interferencia utilizan el mismo canal [9].

2.27.2 Canal único/multicanal

Esta es una propiedad de capa 2, hay protocolos en los que todos los nodos comparten el mismo canal de comunicación lo que significa que todas las comunicaciones pasan por el mismo canal disminuyendo la velocidad de la red. El control acceso al medio en IEEE802.11 utiliza el protocolo CSMA/CA con reconocimiento y un tiempo de back off aleatorio que sigue una condición demedio ocupado.

El protocolo CSMA/CA de 802.11 se diseñó para reducir la probabilidad de colisión entre los múltiples intentos de acceso al medio. Las múltiples estaciones están esperando que el medio este libre y cuando lo está todas las

estaciones intentan acceder al mismo tiempo. Por lo tanto se utiliza una distribución back off aleatoria para poder minimizar los conflictos en el medio. Hay protocolos que especifican el canal de comunicación como: AODV, OLSR.

En cambio, otros protocolos utilizan CDMA, FDMA o TDMA para poder especificar el canal. En este caso la comunicación es mucho más eficiente porque se puede trabajar con velocidades más altas pero en contra se tiene que controlar mediante las estaciones la asignación de canales [9].

2.27.3 Topología jerárquica/Enrutamiento con Clúster

La idea de utilizar clúster en las redes es para intentar dar una estructura a este tipo de redes. Estos clúster habitualmente tienen un nodo principal dedicado, que es el encargado de indicar a los nodos cercanos a qué clúster pertenecen y de este modo estructurar la red. Estos nodos principales aparte de ser informados de la conexión y desconexión de nodos también se encargan de ser las puertas de unión entre los diferentes clúster. Se debe mencionar que en muchos casos los clúster tienen diferentes capas jerárquicas, en este tipo de protocolos se envía información más frecuentemente a los nodos que se mueven rápidamente o a los que están más cerca.

El problema de los clúster es que el nodo principal y el gateway tienen que trabajar con mucha información y se pueden convertir en el cuello de botella de la red, ya que si todos los nodos de la red pretenden enviar información a otro nodo, toda esta información tratará de salir por el mismo nodo. Además de reanudar la comunicación, estos nodos también gastarán mucha más energía que los otros, lo que puede suponer un problema en nodos que trabajen con fuentes autónomas de alimentación.

2.27.4 Proactivo/Enrutamiento bajo demanda

Un protocolo de enrutamiento puede mantener la información bajo demanda (reactiva), es decir, actualiza su información de enrutamiento a

medida que es necesaria. Este tipo de protocolo no necesita que todos los nodos tengan la información de enrutamiento en todo momento, sino que la actualizará a medida que la necesita. Lo que se pretende conseguir es que la red inalámbrica no tenga una gran carga de señalización innecesaria. Se puede considerar muy útil cuando la información viaja a menudo por rutas muy parecidas.

Estos protocolos necesitan saber al menos el primer salto que deben hacer, si no lo conocen se debe hacer un broadcast hacia todos los nodos vecinos, esta estrategia sólo se puede utilizar en los primeros saltos, si se utilizara en exceso se inundaría la red, lo que no es conveniente. Los paquetes no se empiezan a enviar hasta que la ruta no está especificada, esto supone un retraso en el envío de los primeros paquetes.

Una vez la ruta está finalizada, se debe guardar en caché la tabla de enrutamiento durante un período de tiempo, una vez que pasa este tiempo la ruta se invalida.

Los protocolos proactivos, al contrario que los reactivos (bajo demanda), intentan mantener toda la información de enrutamiento correcta en todos los nodos de la red en cada momento. Estos protocolos también se pueden dividir en dos clases:

- ✓ Los que tratan eventos y los que se actualizan de manera regular.
- ✓ Los que trabajan con eventos no envían paquetes de actualización hasta que no hay un cambio en la topología de la red.

En cambio, en el caso de actualización regular, la información se retransmite cada cierto tiempo. La ventaja de este tipo de protocolos es que no necesitan un tiempo para crear la ruta, por el contrario añaden mucha más carga a la red **[9]**.

2.28 Estrategia de selección de ruta

Este es uno de los aspectos más importantes de los protocolos de enrutamiento obviamente, hay que tener en cuenta que puede haber muchas maneras de elegir la estrategia. Las más conocidas y utilizadas son las siguientes:

- Intensidad de señal: encamina los paquetes a través de la conexión siguiendo los que tienen la señal más fuerte.
- Estabilidad de conexión: Los paquetes viajan por los nodos que parecen más estables durante un período de tiempo.
- Camino más corto/Estado de la conexión: Selecciona el camino más corto siguiendo algunas métricas como la calidad del enlace.
- Vector de distancia: Método de vector de distancia común, normalmente basado en la cuenta de saltos.
- Encaminamiento direccional: Encamina hacia la dirección geográfica del destinatario, usado en los protocolos de localización.

2.29 Generación de peticiones de rutas

Un nodo envía un mensaje RREQ cuando determina que necesita saber la ruta hacia un destino y no lo tiene en su tabla de enrutamiento o es una entrada no válida. En ese momento se envía un mensaje RREQ con el valor del número de secuencia de destino igual al último número conocido para este destino. El valor del número de secuencia de origen en el mensaje RREQ es el número de secuencia del nodo que es incrementado antes del envío del mensaje.

Al tener en cuenta que las comunicaciones son bidireccionales, además de la ruta para llegar al destino también es necesario saber una ruta de vuelta. Para este cometido cualquier nodo intermedio que genere un mensaje de respuesta (RREP) debe también realizar una acción que notifique al nodo destino una ruta de vuelta hacia el nodo origen.

Para no crear congestión en la red ni hacer que los mensajes circulen indefinidamente por ella, el nodo que origina peticiones debe indicar un TTL máximo a los mensajes y además seleccionar un timeout para esperar una respuesta. Tanto el timeout como el TTL son calculados de manera periódica y tiene en cuenta el tamaño de la red y el tiempo que tarda un paquete en cruzarla [9].

2.29.1 Procesamiento y retransmisión de peticiones de ruta

Cuando un nodo recibe un RREQ, crea o actualiza una ruta hacia el salto anterior.

Posteriormente comprueba que no haya recibido un mensaje con el mismo ID y origen y si lo ha recibido descarta este nuevo mensaje. En este apartado se explicará las acciones que se realizan cuando este mensaje no se descarta.

Lo primero que se hace es aumentar el valor del contador de saltos en uno.

Después, el nodo busca una ruta hacia la IP origen del mensaje. Si no existe se debe crear una nueva ruta de vuelta. Una vez que se ha creado esta ruta de vuelta se siguen las siguientes acciones:

- ✓ El número de secuencia origen se compara con el número de secuencia hacia el destino que se tiene en la tabla, y si es mayor se copia en ella.
- ✓ Se valida el campo de número de secuencia.
- ✓ El siguiente salto en la tabla de enrutamiento se procesa en el nodo a donde ha llegado el mensaje de información.
- ✓ Se copia el número de saltos en la tabla de enrutamiento.

2.29.2 Generación de respuesta de ruta

Un nodo genera un mensaje RREP si él mismo es el destino, o tiene una ruta activa hacia el destino y el número de secuencia de la entrada de la tabla

es mayor que el del mensaje RREQ. Una vez que se genera el RREP el nodo descarta el mensaje RREQ.

Si un nodo no genera un RREP y el valor del TTL es mayor a uno, entonces actualiza y envía el mensaje RREQ a una dirección broadcast.

Si el nodo que genera el mensaje RREP no es el nodo destino sino que es un nodo intermedio, copia su propio número de secuencia para el destino en el campo de número de secuencia de destino del mensaje RREP.

Entonces este nodo intermedio actualiza la ruta de retransmisión poniéndose a él como último nodo en la lista de precursores [9].

2.29.3 Recepción y retransmisión de respuesta de ruta

Cuando un nodo recibe un mensaje RREP busca una ruta hacia el salto anterior, si es necesario se crea esta ruta. Posteriormente el nodo incrementa el contador de saltos en el mensaje. Entonces se crea una ruta para llegar al destino si no existe. De otra manera, el nodo compara el número de secuencia de destino del mensaje con el que tiene guardado. Después de la comparación la ruta existente se actualiza en los siguientes casos:

- ✓ El número de secuencia en la tabla de enrutamiento está marcado como inválido.
- ✓ El número de secuencia de destino en el mensaje es mayor al que el nodo tiene guardado y el valor es válido.
- ✓ Los números de secuencia son iguales pero la ruta está marcada como inactiva.
- ✓ Los números de secuencia son los mismos, y el nuevo valor del contador de saltos es menor.

Cuando se actualiza una entrada en la tabla la ruta se marca como activa, el número de secuencia de destino también se marca como válido y en el siguiente salto en la entrada de la tabla se asigna el nodo del que ha llegado

el mensaje RREP. También se debe actualizar el nuevo valor del contador de saltos, el tiempo de expiración de la ruta y el número de secuencia de destino, se debe actualizar por el número de secuencia del mensaje RREP.

2.29.4 Mensajes de error (RERR)

Normalmente una ruta errónea o el corte de un enlace necesitan un procedimiento similar. Primero se debe invalidar las rutas existentes, determinar los destinos afectados, determinar los nodos vecinos afectados y enviar un mensaje apropiado RERR a estos nodos vecinos.

Un nodo inicia el procesamiento de un mensaje RERR en tres situaciones:

- ✓ Si detecta la caída de un enlace para el siguiente salto de una ruta activa en su tabla de enrutamiento mientras envía datos.
- ✓ Si recibe un paquete de datos desde un nodo del que no tiene ninguna ruta activa.
- ✓ Si recibe un mensaje RERR desde un nodo vecino por una o más rutas activas[9].

2.29.5 Ejemplo de utilización

En la figura se puede ver como un nodo (A) busca la ruta hacia otro nodo (J) del que no conoce el camino. Lo primero que hace el nodo A es enviar un mensaje broadcast RREQ hacia todos los nodos, preguntando por el nodo J, con el que se quiere comunicar. Cuando el mensaje RREQ llega al nodo J este genera un mensaje RREP de respuesta. Este mensaje se envía como unicast de vuelta hacia el nodo A utilizando las entradas en memoria de los nodos H, G y D.

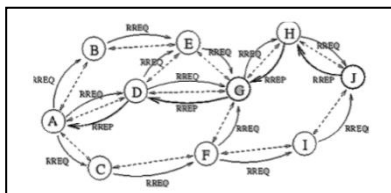


Fig. 2.9: Ejemplo de búsqueda de un nuevo nodo
Fuente: www.wikipedia.org/wiki/IEEE_802.11

2.30 Seguridad

2.30.1 Tecnologías en seguridad

El potencial de una red WMNs no puede ser explotada sin considerar la seguridad.

Las WMN se exponen a las mismas amenazas básicas comunes de las redes cableadas e inalámbricas: los mensajes pueden ser interceptados, modificados, duplicados, etc. Una red que posee recursos importantes, se podría acceder sin autorización.

Los servicios de seguridad que por lo general tratan de combatir estas amenazas son:

- ✓ Confidencialidad: Los datos se revelan solamente en las entidades o personas interesadas.
- ✓ Autenticación: Una entidad tiene de hecho la identidad que demanda tener, es decir, reconocimiento de los usuarios dueños del servicio.
- ✓ Control de acceso: Se asegura de que solamente las acciones autorizadas puedan ser realizadas.
- ✓ No negación: Protege las entidades que participan en un intercambio de la comunicación puede negar más adelante algo falso que ocurrió el intercambio.
- ✓ Disponibilidad: Se asegura de que las acciones autorizadas puedan tomar lugar.

Los Servicios de seguridad en el futuro serán mucho más restringidos buscando para el usuario privacidad y la confidencialidad del tráfico. La protección del tráfico de datos implica: la confidencialidad (cifrado), la autenticación de los socios de la comunicación, así como la protección de la integridad y de la autenticidad de mensajes intercambiados. La protección de la integridad se refiere no sólo a la integridad del mensaje, sino también al orden

correcto de los mensajes relacionados (reenvío, el reordenamiento, o cancelación de mensajes).

Esta sección describe los mecanismos utilizados para la protección del tráfico de la comunicación. Estas tecnologías pueden también ser utilizadas dentro de una red mesh para autenticar los nodos Mesh (MNs) y para establecer las claves de la sesión que protegen la confidencialidad y la integridad del tráfico intercambiado entre MNs.

Los datos pueden ser protegidos por diversas capas (capa de enlace, capa de red, capa de transporte y capa de aplicación): especialmente en sistemas inalámbricos, (IEEE 802.11WLAN, Bluetooth, 802.16 WiMax), que incluye medios de proteger el enlace inalámbrico. Éstos utilizan diversos esquemas de encapsulación de tramas, diversos protocolos de autenticación, y diversos algoritmos criptográficos. Ya sea una llave compartida es configurada en los dispositivos WLAN (la llave pre-compartida PSK) Las Redes de área local inalámbricas (WLAN) basada en IEEE 802.11i (WPA, WPA2) soporta dos modos de seguridad: puede ser *sharedkey* (clave compartida) que es configurada en los dispositivos WLAN ([PSK = *pressharedkey*] claves pre-compartidas), que es de uso frecuente en las redes domésticas, los usuarios pueden ser autenticados con un servidor autenticador (servidor AAA).

Para este propósito, se utiliza el protocolo extensible de autenticación (*extensible authentication protocol*) (EAP). La autenticación real ocurre entre la estación móvil (MS) y el servidor AAA. Usando EAP como lo muestra la Figura.

El EAP es transportado entre el MS y el punto de acceso (AP) que usan EAPOL (encapsulación EAP sobre LAN), y entre el AP y el servidor AAA por el protocolo RADIUS.

Si es habilitado el nodo, una sesión maestra de claves (MSK) es utilizada, el cual se envía desde el servidor de la autenticación (AS) al WLAN AP y se utiliza como entrada al WLAN.

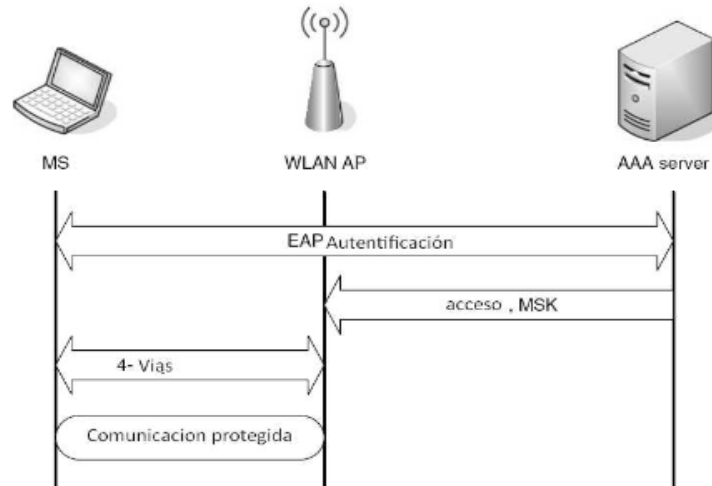


Fig. 2.10: Acceso a WLAN basada en EAP
Fuente: www.wikipedia.org/wiki/IEEE_802.11

Hay 4 maneras de establecer una sesión de clave temporal para proteger el enlace inalámbrico. Esta clave se utiliza realmente para proteger el tráfico del usuario, usando cualquier protocolo de integridad de clave temporal (TKIP), que es parte de WPA) o AES-basado en CCMP (CTR con el protocolo de CBC-MAC, parte de WPA2). Los varios métodos de EAP existen para una autenticación basada en los certificados digitales, las contraseñas, o los protocolos móviles reusing de la autenticación de la red (EAP-SIM, EAP-AKA).

El acceso EAP-basado en WLAN se utiliza particularmente para las redes de la empresa y los hot-spots públicos donde está disponible una base de datos del usuario. El tráfico de la comunicación se puede también proteger en la capa enlace. IPsec protege tráfico IP en la capa de la red (IP) [9].

CAPÍTULO III

ANÁLISIS PREVIO PARA EL DISEÑO DE LA RED

3.1 Introducción

En este capítulo abordamos la situación actual de las comunicaciones inalámbricas en la Facultad Técnica para el desarrollo después de realizar un estudio de cobertura a nivel de WIFI; se observó la necesidad de investigar esta tecnología, tomando como referencia el Wifi actual con ssid: **wifiucsg** debido al fallo de errores en la Tx/Rx el cual el servicio es demasiado intermitente ocasionando que los estudiantes de la Facultad no tenga esta herramienta tan importante para ampliar sus conocimientos en el ámbito educativo.

3.2 Estado actual de las comunicaciones en la Facultad Técnica para el Desarrollo

Para realizar este análisis se tomó en cuenta requerimientos físicos, operativos y funcionales,

Los físicos que comprenden la parte del hardware de este proyecto, conformado por los enrutadores inalámbricos, el servidor, y los computadores portátiles, así como estudiantes y docentes que nos permitirán realizar las pruebas correspondientes.

Los operativos corresponden al protocolo de enrutamiento que utilizaremos, la topología de red tanto física como lógica, el enrutador inalámbrico como para el servidor.

Los funcionales son las características mínimas necesarias para el correcto funcionamiento de este proyecto, entre los cuales tenemos que nuestra red debe brindar completa movilidad a los usuarios, además el valor mínimo del indicador de la potencia de la señal recibida (RSSI) debe ser de -55dBm en los

clientes de la red; todos los enrutadores deben ser capaces de comunicarse entre sí, así también debe existir una redundancia en la red, para que en caso de la pérdida de un nodo la red no se vea afectada.

Se ha realizado un análisis de espectro en todo el entorno de la Facultad para poder diagnosticar cuales son los fallos de errores en la TX del wifi que posee la UCSG como ssid: **wifiucsg**, hemos realizado el estudio de RF con un software llamado **inSSIDer** el cual es una aplicación para visualizar todas las redes Wifi existentes en la zona, que hay alrededor de una PC, señalando el nombre y la calidad, así como el listado en pantalla de todos los detalles relativos a SSID, dirección MAC, canal, RSSI, tipo de red y seguridad, velocidad e intensidad de la señal.

Concretamente, con inSSIDer detectamos todas las redes inalámbricas que tiene cobertura en la UCSG. Esta herramienta funciona como auditoria de redes inalámbricas, a través de un sistema de descompresión y ejecución del sistema.

Además, mediante una gráfica, inSSIDer nos permite monitorizar la calidad de la señal utilizando como parámetro de control el indicador que refleja la fuerza o intensidad de la señal de radio recibida (RSSI). La ejecución se realiza en instantes junto con todos estos detalles.

Con es de conocimiento este programa realiza un estudio de rf en todos los punto donde los estudiantes se conectan a la red Wifi, observamos que los niveles de RX son la mayoría en -85dbm esto significa que con estos niveles no se puede lograr una comunicación estable y de esto va a depender que el BW (ancho de banda) sea limitado, para un correcto funcionamiento de la red.

Existen algunos factores que influyen en el buen transporte de la información tales como latencia libre de errores, Ancho de Banda circulando en la red y selección de canales para evitar interferencia entre otros equipos utilizados dentro de la Universidad.

Otro de los factores importantes para el buen uso del WiFi es la seguridad en la Web, en el Wifi de la Universidad se ha encontrado que se puede acceder a algunas páginas como por ejemplo **Facebook**, en el diseño que se está presentando se bloquearan todas estas páginas de contenido social y solo se permitirá el acceso a información educativa.

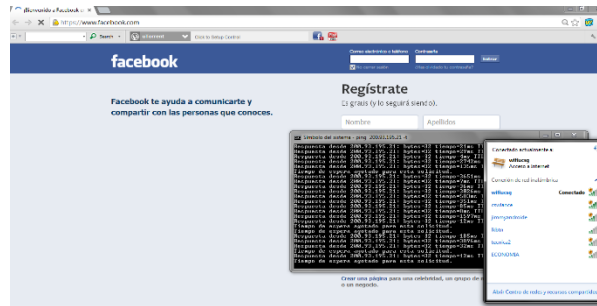


Fig. 3.1: Páginas de contenido social
Fuente:www.facebook.com

3.3 Latencia

Observamos que existe un alto tiempo de respuesta (latencia) con un máximo de 800ms y en ciertos sectores como por ejemplo Secretaria de la Facultad donde se pierden paquetes en la Última milla, esto provoca un corte en la comunicación y que el internet se vuelva lento, también existen sectores donde no existe comunicación; es decir se escanea la red en -89dbm pero al momento de autenticar no se enlaza al ruteador es decir no da Ip de destino para poderse asociar a la red.

Para un óptimo transporte de paquetes no debe existir un retraso que es la demora del tiempo de emisión y recepción de un paquete, existen varios parámetros que influyen en el aumento o disminución del mismo, tales como la distancia por lo que los datos deben viajar, el tamaño del paquete y el número de redes que existen entre los terminales.

```

cmd. Símbolo del sistema - ping 200.93.195.21 -t
Respuesta desde 200.93.195.21: bytes=32 tiempo=503ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=536ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=12ms TTL=250
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 200.93.195.21: bytes=32 tiempo=606ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=1249ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=1090ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=182ms TTL=250
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.16.24.247: Host de destino inaccesible.
Respuesta desde 200.93.195.21: bytes=32 tiempo=67ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=760ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=607ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=874ms TTL=250
Respuesta desde 200.93.195.21: bytes=32 tiempo=56ms TTL=250
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.16.24.247: Host de destino inaccesible.
Respuesta desde 172.16.24.247: Host de destino inaccesible.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.16.24.247: Host de destino inaccesible.

```

Fig. 3.2: Tiempos de respuesta hacia la Ip 200.93.195.21
Fuente: Autor(Servidor DNS Ro Acceso proveedor de servicios de Internet Ecuador)

3.4 Ancho de banda

Es la cantidad de información o paquetes de datos que pueden ser enviados a través de la red en un período de tiempo dado, y se mide en bits por segundo (Kbps, Mbps, Gbps). La cantidad de ancho de banda requerida para una Red Mesh depende de muchos factores, incluyendo el número simultáneo de conexiones, códec empleado, tamaño de la trama, entre otros, si existe un retardo en el tiempo de respuesta hacia el servidor esto va a reducir el BW, en el SSID: **_wifiucsg** tenemos varias capturadas de los tiempos de respuesta donde el servicio en ciertos sectores es Irregular.

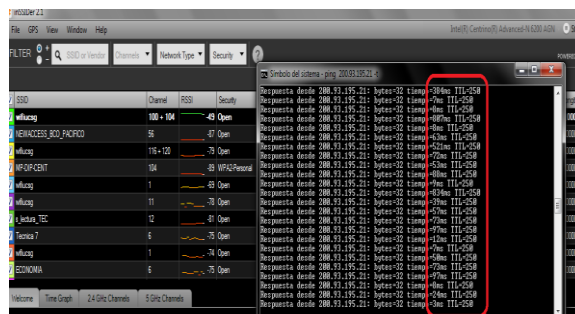


Fig. 3.3: Tiempos de respuesta hacia la Ip 200.93.195.21
Fuente: Autor(Servidor DNS Ro Acceso proveedor de servicios de Internet en Ecuador)

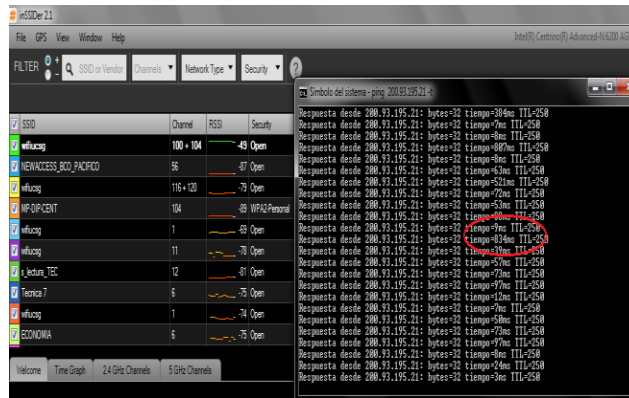


Fig. 3.4: Tiempos de respuesta hacia la Ip 200.93.195.21
Fuente:Autor (Servidor DNS Ro Acceso proveedor de servicios de Internet en Ecuador)

3.5 Selección de canales

Realizando un análisis de espectro observamos que el SSID: **_ wifiucsg** posee los mismos canales en algunos equipos tales como por ejemplo el canal 1, esto provoca interferencia entre el mismo nodo ocasionando que el canal de transmisión no es la correcta y baje su rendimiento.

Una de las opciones que se da en este estudio sería modificar los diferentes canales en cada uno de los enlaces que se van a configurar en todas las interfaces con el objetivo de no causar interferencia entre ellos tras agrupar los nodos en diferentes sectores de la facultad como lo vamos analizar en el capítulo IV.

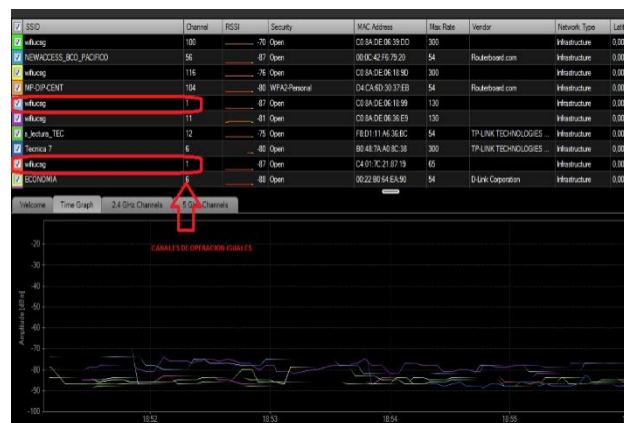


Fig. 3.5: Tiempos de respuesta hacia la Ip 200.93.195.21
Fuente:Autor(Servidor DNS Ro Acceso proveedor de servicios de Internet en Ecuador)

Para poder selección el mejor canal se debe conocer cómo se reparte la banda libre de frecuencias situada alrededor de los 2,4 GHz que emplean este tipo de redes. Con 802.11g, una antena emplea un ancho de banda de **22 MHz para transmitir sus datos**, mientras que **los trece canales** en los que se divide la banda otorgada para Wi-Fi, **se separan 5 MHz entre ellos**.

En efecto, cuando usamos un canal para emitir **estamos relleno con nuestros datos los adyacentes**.

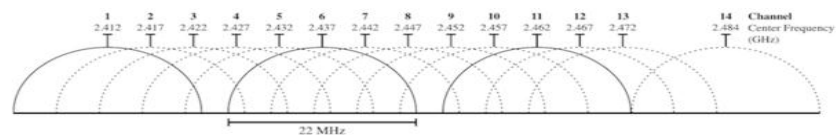


Fig. 3.6: Canales de bandas otorgada para Wi-Fi
Fuente: http://wn.com/redes_mesh

De hecho, este estudio planifica una red inalámbrica estable y no las que se suelen emplear con canales que no se solapan entre sí, como por ejemplo la tripleta conformada por el canal 1, 7 y 13, tal y como podemos ver en la gráfica de a continuación. Otra opción es usar los canales 1, 6 y 11.

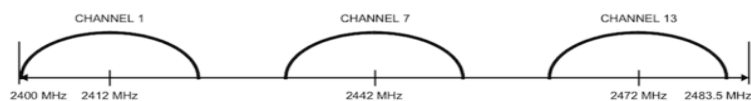


Fig. 3.7: Canales de bandas divididas otorgada para Wi-Fi
Fuente: http://wn.com/redes_mesh

3.6 Planeación de la capacidad de la red

El objetivo de este proyecto es brindar a los usuarios de la red un servicio con parámetros de QoS (calidad de servicio). Para cumplir con este propósito, es necesario saber los tipos de aplicaciones que correrán en la red y tener una idea general de cuantos posibles usuarios se tendrá. Todo esto será de mucha ayuda para el correcto dimensionamiento de la capacidad de la red.

Para analizar la capacidad de la red, es necesario determinar el ancho de banda promedio que consume y las distintas aplicaciones como son: bajar información, e-mail, música, chat etc. En base al análisis de las aplicaciones anteriores, se pretende tener una idea general de la capacidad de ancho de banda que se necesitaría contratar al proveedor de servicios de Internet (ISP) y además poder hacer un correcto dimensionamiento de nuestra red y una correcta división del BW en cada nodo que se va a distribuir la red, con esto evitamos cuellos de botella provocando lentitud en la red.

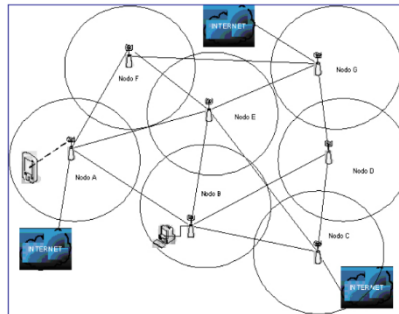


Fig. 3.8: Distribución de los nodos de una red inalámbrica
Fuente: http://wn.com/redes_mesh

3.7 Estudio de cobertura

Se ha realizado un estudio de análisis de espectro en todo el entorno de la Facultad viendo los puntos críticos donde la señal es débil o donde no hay

internet, para poder cubrir estas zonas y tener una visión más clara de cuáles son las deficiencias actuales, a continuación se detalla capturas de los estudios:

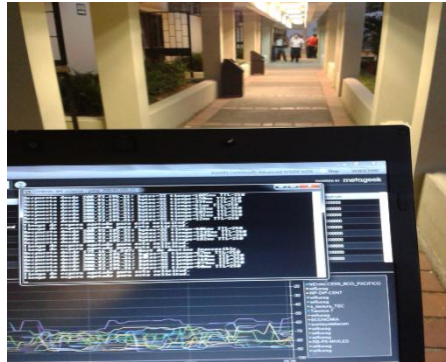


Fig. 3.9: Internet intermitente en pasillos de la Facultad (Laboratorios)
Fuente: Autor



Fig. 3.10: Comprobación de la ausencia de Internet dentro de las Aulas
Fuente: Autor

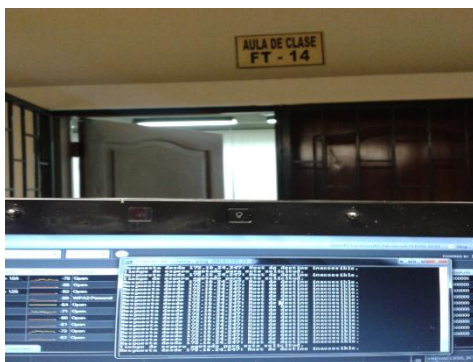


Fig. 3.11: Comprobación de la ausencia de internet fuera del Aula FT-14 a pesar de estar asociado al Ssid: _wifiucsg
Fuente: Autor

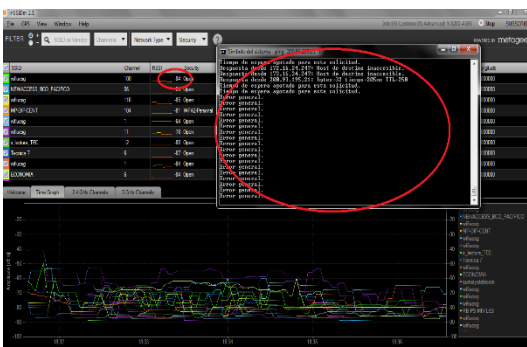


Fig. 3.12: Comprobación de la ausencia de internet dentro del Aula FT-14, se observan niveles de -84dbm
Fuente: Autor



Fig. 3.13: Internet intermitente en los alrededores de la Facultad
Fuente: Autor

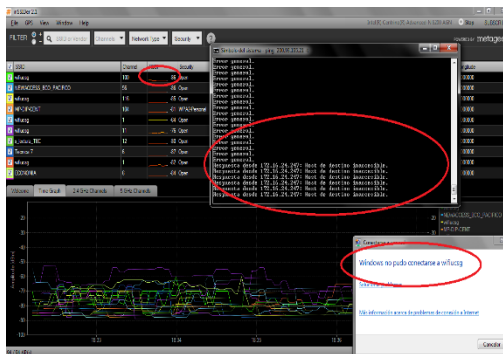


Fig. 3.14: Ausencia de internet dentro del Aula FT-15, no se puede asociar al wifi
Fuente: Autor

3.8 Infraestructura

Para poder implementar este proyecto de Redes Malladas en la Facultad y después de realizar el estudio de cobertura viendo los puntos críticos donde se necesita llegar con Internet y contando con la infraestructura (Torres) que posee la Facultad Técnica se ha tomado como referencia ocupar los puntos más altos y las dos torres que se tiene una de 6mts de Altura (como se muestra

en la figura) ubicada en la parte superior de la Secretaría y otra 9 mts de altura (como se muestra en la figura) ubicada en el laboratorio de informática, el otro punto que se ocupará sería en la parte superior de la facultad de Agronomía (como se muestra en la Figura) donde se instalará un mástil galvanizado de aproximadamente 3 mts.de altura, en estos sitios se Instalarán las Antenas Sectoriales, Equipos, cables y cajas de interperie para la implementación.



Fig. 3.15: Torre de 6mts de Altura ubicada en la parte superior de la Secretaría de la Facultad Técnica para el Desarrollo
Fuente: Autor



Fig. 3.16: Torre de 9mts de altura ubicada en la parte superior del laboratorio de computación
Fuente: Autor



Fig. 3.17: Sitio para distribuir Wifi en la Facultad de Agronomía
Fuente: Autor

CAPÍTULO IV

DISEÑO DE LA RED MESH APLICADA A LA FACULTAD TECNICA PARA EL DESARROLLO

4.3 Introducción

Este capítulo aborda el diseño de una Red WMNs para las áreas seleccionadas, tomando en cuenta o identificando los diferentes requisitos tecnológicos y necesidades de la Facultad que conlleva a diseñar dicha red. Se hace mención sobre los equipos WMNs que en la actualidad están disponibles en el mercado con el fin de seleccionar los productos que mejor se adapten a las necesidades específicas así mismo como los precios de los equipos y el software a operar con todas las especificaciones técnicas requeridas .

4.2 Visión general de la propuesta del diseño de la red WMNS

De los resultados obtenidos en el capítulo anterior, se resume un conjunto de características sobre la situación actual de las comunicaciones Inalámbricas en la UCSG.

Nos centraremos exclusivamente en Analizar y diseñar una red WMNs para dar servicios de internet a la Facultad Técnica para el Desarrollo.

Uno de los retos para el diseño será describir y justificarla arquitectura de la red.

La idea principal es construir una red troncal en malla que constituye la columna vertebral de la red a ser diseñada y que garantice la conectividad en las zonas críticas, el estándar empleado para los enlaces de la red será IEEE 802.11.

La siguiente figura muestra la arquitectura que implementaremos para el diseño de la red WMNs en la Facultad Técnica para el desarrollo aquí se ven todos los 3 puntos donde se instalarán los equipos de Radios.

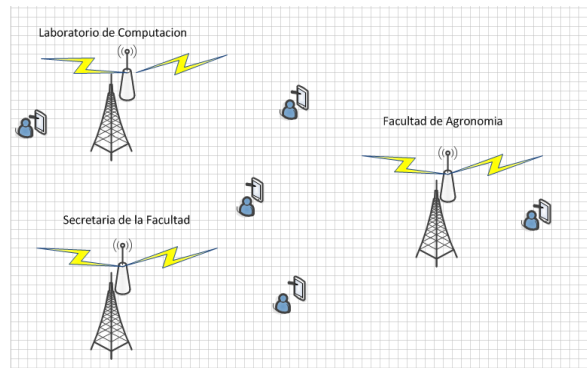


Fig. 4.1: Arquitectura a implementar para el diseño de la red WMNs
Fuente: Autor

Las Redes Inalámbricas Mesh (WMNs) consisten en dos tipos de nodos: los repetidores y los clientes, donde los repetidores tienen movilidad mínima y forman la red transporte de la red WMNs.

Estas redes pueden integrarse a otras como Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. El servicio con que se conectarán los alumnos puede ser estático o móvil y pueden crear una red mallada entre ellos mismos o con los repetidores. Estas redes solucionan las limitaciones y mejoran el rendimiento de las redes ad hoc.

Gracias a la posibilidad de conectarse a distintos puntos de acceso en lugar de uno sólo, se aumenta el ancho de banda que puede tener cada Alumno, también resulta mucho más estable, ya que puede seguir funcionando

Aunque caiga un nodo, en cambio en las redes habituales si cae un punto de acceso los usuarios de ese punto de acceso se quedan sin servicio.

De los resultados obtenidos en el capítulo anterior, se resume un conjunto de características sobre la situación actual de las comunicaciones.

4.3 Características de diseño para redes inalámbricas

La UCSG cuenta con un gran número de Alumnos matriculados en diferentes Facultades, todo esto conlleva que la mayor parte del estudiantado ocupe el internet, como hemos manifestado en los previos estudios que realizamos donde el internet es limitado puesto a que la mayor parte de los alumnos ocupan el internet en Horas picos de clases, pese a esto se generaliza en la carencia de infraestructuras de comunicación y acceso a la información.

El reto es dotar a todas las zonas con conectividad a redes de información y en especial a la Facultad Técnica para el Desarrollo.

Frente a este panorama la red que se pretende aplicar de manera sostenible, esta red que se está estudiando que debe que ser robusta y sencilla de usar, y en lo posible tendrá que requerir del menor número de personal especializado para dar el mantenimiento respectivo, para ello en la figura que presentamos indicamos la distribución de los enlaces y la ubicación:

- El primer punto va a estar ubicado en la parte superior de la Secretaría de la Facultad Técnica que funcionará como Administrador de la Red, en ella como ya hemos indicado en el capítulo III cuenta con una torre de 6 mts. de altura aquí se Instalará un Radio de Marca Mikrotik ideal para Redes Mesh , 2 Antenas Sectorial de 15 dbi de 2.4GHZ/5GHZ y 1 Splitter para dividir el servicio y direccionar las dos antenas sectoriales.



Fig. 4.2: Simulación de 2 antenas sectorial en la torre de 6 mts. (Secretaría)
Fuente: Autor

- El segundo punto donde se instalarán los equipos antes mencionados con las mismas características es en la torre de 12 mts ubicada en el centro de cómputo de la facultad como se muestra en la figura la simulación de 2 Antenas sectoriales, previo al estudio donde que se analizó en el capítulo III, las antenas van a estar direccionadas en los puntos críticos donde el internet es intermitente o no es escaso, las Antenas que se instalaron tienen 90° grados de cobertura.



Fig. 4.3: Simulación de instalación de 2 antenas sectorial en la torre de 12 mts.
(Laboratorio de computación)
Fuente: Autor

- El siguiente punto donde se instalarán los equipos de Radio es en la Facultad de Agronomía, se ha buscado estratégicamente este punto y debido a no tener infraestructura para poder instalar los equipos se pondrá un Mastil de aproximadamente 6 mts. de Altura.



Fig. 4.4: Simulación de instalación de equipos de radio (Facultad de Agronomía)

Fuente: Autor

- El siguiente diagrama muestra el diseño de una Red Mesh en la Facultad Técnica para el Desarrollo, aquí se detallan los 3 puntos antes mencionados.

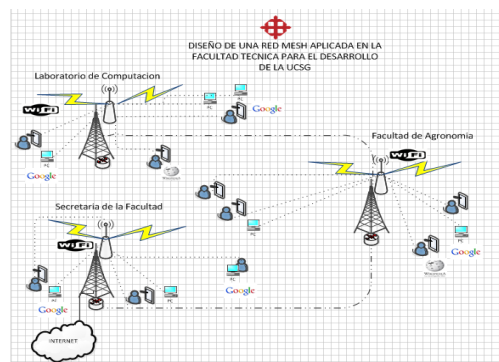


Fig. 4.5: Diseño de una Red Mesh en la Facultad Técnica para el Desarrollo

Fuente: Autor

4.4 Requisitos para el diseño de la red mesh

4.4.1 Requisitos generales

Se identificarán los siguientes requisitos generales para la Red Mesh:

- **Fácil despliegue:** Los nodos de la red deben ser de fácil instalación y configuración.
- **Robustez:** La red debe ser sólida y ofrecer suficiente redundancia de rutas, también debe ser de auto detección y corrección de problemas que existan dentro de la red.
- **Banda ancha:** Calidad de servicio (QoS), priorización de tráfico con el fin de ajustar la red a las necesidades de estos servicios.
- **El uso del protocolo estándar:** Protocolos de comunicación estándar son preferibles con el fin de facilitar la interoperabilidad entre los dispositivos de comunicación.
- **Hospot:** Publicidad al momento de asociarse al Wifi de la Facultad, es decir aparecer un Usuario y Password que tendrán los alumnos para registrarse a la Red.

4.4.2 Requisitos específicos

- Requisitos de radio y topología de la red
- **Múltiples interfaces de radio:** El uso de múltiples interfaces de radio y diferentes canales, podrá maximizar la capacidad de la red, con múltiples canales de radio disponibles, mientras que los otros canales disponibles pueden ser utilizadas para la comunicación entre los nodos de la red troncal y clientes. Además, lo que permite evitar el uso de una frecuencia con interferencia, está característica hace que el WMNs sea más robusta.
- **Tecnología de interfaz de radio:** La banda de 2,4 GHz y 5.8 GHz son útiles para conectar ordenadores portátiles a una red WMNs, la

conectividad inalámbrica de los dispositivos de este tipo se basa actualmente en el estándar IEEE 802.11b/g.

4.4.3 Requisitos de funcionamiento

- **Latencia de extremo a extremo:** El retardo de extremo a extremo debe mantenerse en valores aceptables, ya que afecta el rendimiento de las comunicaciones de datos, sobre todo en tiempo real de servicios tales como las comunicaciones de voz. Por ejemplo para los servicios de VoIP el retardo de extremo a extremo debe ser menor a 150 ms.
- **El ancho de banda de extremo a extremo:** Nos referimos al ancho de banda disponible en una ruta sin enlaces rotos, debe estar disponible para permitir el uso de varios servicios como voz, video etc. Para las comunicaciones se recomienda un mínimo de 5 Megas por cada Acess Point.
- **Retardos a los cambios de Ruta:** La conectividad de nuevas rutas deberá reducirse al mínimo, maximizando así la disponibilidad del servicio.

4.5 Características de funcionamiento

Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado.

Una de las principales características para el buen funcionamiento de la Red son los diferentes equipos y programas a utilizar son:

- Software
- Hardware
- Tasa de Transferencia
- Seguridades
- Ganancia de las Antenas
- RSL
- Perdidas de cables
- Perdidas en los conectores.

Características	IEEE 802.11
Tasas de Transferencia	54Mbps
Escalabilidad	20Mhz
Cobertura	200mts
TX	Full Duplex
Seguridad	WPA-AES/WEP

Tabla4.1: Características de las redes Mesh

Fuente: www.wikipedia.org/wiki/Red_inalámbrica_Mesh

Características	Descripción
Compatibilidad	XP-Linux
Conexiones	LAN/WAN
Servicio de Red	ping / Sntp
TX	Full Duplex
Seguridad	WPA-AES/WEP
Polarización	Dual
Ancho de Canal	5/10/20/40 MHZ
Potencia	21db
Monitoreo	Tiempo Real

Tabla4.2: Características del Software

Fuente: www.wikipedia.org/wiki/Red_inalámbrica_Mesh

4.6 Ganancia de las antenas

Las antenas son dispositivos pasivos que crean el efecto de amplificación debido a su forma física. Las antenas tienen las mismas características cuando reciben que cuando transmiten. Por lo tanto, una antena de 12 dBi simplemente es una antena de 12 dBi, sin especificar si esto es en el modo de transmisión o de recepción. Las antenas parabólicas tienen una ganancia de 19-24 dBi, las antenas omnidireccionales de 5-12 dBi, y las antenas sectoriales de 12-15 dBi.

4.7 El mínimo nivel de señal recibida

Conocido como sensibilidad del receptor (RSL) y se expresa siempre como dBm negativos (- dBm) y es el nivel más bajo de señal que la red inalámbrica puede distinguir. El RSL mínimo depende de la tasa de transmisión, y como regla general la tasa más baja (1 Mbps) tiene la mayor sensibilidad. El mínimo va a ser generalmente en el rango de -75 a -95 dBm. Al igual que la potencia TX, las especificaciones RSL deben ser provistas por el fabricante del equipo.

4.8 Pérdidas en los cables

Las pérdidas en la señal de radio se pueden producir en los cables que conectan el transmisor y el receptor a las antenas. Las pérdidas dependen del tipo de cable y la frecuencia de operación y normalmente se miden en dB/m o dB/pies.

Independientemente de lo bueno que sea el cable, siempre tendrá pérdidas. Por eso, hay que recordar que el cable de la antena debe ser lo más corto posible. La pérdida típica en los cables está entre 0,1 dB/m y 1 dB/m. En general, mientras más grueso y más rígido sea el cable menor atenuación presentará. Para darle una idea de cuán grande puede ser la pérdida en un cable, considere que está usando un cable RG58 que tiene una pérdida de

aproximadamente 1 dB/m, para conectar un transmisor con una antena. Usando 3 m de cable RG58 es suficiente para perder el 50% de la potencia (3 dB).

Tipo de cable	Atenuación dB/metro	
	2.4GHz	5.8GHz
RG174	1.20	1.85
RG316	1.10	1.70
RG58	0.83	1.40
RG58U	0.57	0.89
LMR195	0.56	0.88
RF213U	0.39	0.51
C2FP	0.23	0.36
LMR400	0.23	0.35
LDF4/50A	0.13	0.21

Tabla4.3: Valores típicos de pérdida en cables para 2.4 Ghz y 5.8 Ghz
Fuente: www.wikipedia.org/wiki/Red_inalámbrica_Mesh

4.9 Pérdidas en los conectores

Hay que estimar por lo menos 0.25 dB de pérdida para cada conector en su cableado. Estos valores son para conectores bien hechos mientras que los conectores mal soldados pueden implicar pérdidas mayores.

Para las pérdidas en su rango de frecuencia y el tipo de conector que usará.

Si se usan cables largos, la suma de las pérdidas en los conectores está incluida en una parte de la ecuación de “Pérdidas en los cables”. Pero para estar seguro, hay que considerar un promedio de pérdidas de 0.3 a 0.5 dB por conector como regla general.

Además, protectores contra descargas eléctricas que se usan entre las antenas y el radio debe ser presupuestado hasta con 1 dB de pérdida, dependiendo del tipo.

Revise los valores suministrados por el fabricante (los de buena calidad sólo introducen 0.2 dB).

4.10 Software mikrotik mesh

El Software Mikrotik tanto como sus procedimientos de configuración como sus equipos son las que se implementaran en la red de Faculta Técnica para el Desarrollo, esta red se implementara con Mikrotik RouterOS que es el sistema operativo y software del router, el cual convierte a una PC Intel ó un Mikrotik Router BOARD en un router dedicado.

Se toma esta decisión ya que estos equipos brindan seguridad, flexibilidad y son muy económicos, lo cual es un gran beneficio para la UCSG ya que la red es de un tamaño considerable.

El Router OS es un sistema operativo y software que convierte a una PC en un ruteador dedicado, bridge, firewall, controlador de ancho de banda, punto de acceso inalámbrico, por lo tanto puede hacer casi cualquier cosa que tenga que ver con las necesidades de red, además de ciertas funcionalidad como servidor.

El software Router OS puede ejecutarse desde un disco IDE memoria tipo FLASH. Este dispositivo se conecta como un disco rígido común y permite acceder a las avanzadas características de este sistema operativo

Los pasos y procedimientos para la implementación del Mikrotik, son tomados de un trabajo de titulación denominado; Implementación red con Mikrotik, cuyo autor es (Arias, 2011) y de un manual de configuración a equipo Mikrotik, disponible en la página; <http://www.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>, se debe ejecutar los siguientes aspectos:

- Instalación Mikrotik
- Acceso al Mikrotik
- Declaración de interfaces
- Definición Vlan´s
- Asignación de dirección ip por interfaces

- Asignación de pools de direcciones ip's
- Configuración servidor DHCP
- Instalación del servidor y cliente NTP.
- Servidor VPN
- Balanceo de carga
- Control de ancho de banda
- Instalación servidor SNMP
- Instalación servidor RADIUS
- Instalación servidor JABBER
- Instalación servidor PROXY
- Configuración Hotspot.

El trabajo de (Pica, Roche, & Di Rienzo, 2008) toma también información del manual Mikrotik.

4.11 Características principales

El Sistema Operativo es basado en el Kernel de Linux y es muy estable.

Puede ejecutarse desde discos IDE o módulos de memoria flash.

- Diseño modular
- Módulos actualizables
- Interfaz gráfica amigable.

4.11.1 Características de ruteo

- Políticas de enrutamiento. Ruteo estático o dinámico.
- Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en el bridge.
- Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
- Cache: web-proxy, DNS.

- Gateway de HotSpot.
- Lenguaje interno de scripts.

4.11.2 Características del RouterOS

Filtrado de paquetes por:

- Origen, IP de destino.
- Protocolos, puertos.
- Contenidos (seguimiento de conexiones P2P).
- Puede detectar ataques de denegación de servicio (DoS)
- Permite solamente cierto número de paquetes por periodo de tiempo.

4.12 Calidad de servicio (QoS)

4.12.1 Tipos de colas

- RED
- BFIFO
- PFIFO
- PCQ

4.12.2 Colas simples

- Por origen/destino de red.
- Dirección IP de cliente.
- Interface

4.12.3 Árboles de colas

- Por protocolo.
- Por puerto.
- Por tipo de conexión.

4.13 Interfaces del RouterOS

- Ethernet 10/100/1000 Mbit.
- Inalámbrica (Atheros, Prism, CISCO/Airones)
- Punto de acceso o modo estación/cliente, WDS.
- Síncronas: V35, E1, FrameRelay.
- Asíncronas: Onboard serial, 8-port PCI.
- ISDN
- xDSL
- Virtual LAN (VLAN)

4.14 Herramientas de manejo de red

- Ping, traceroute.
- Medidor de ancho de banda.
- Contabilización de tráfico.
- SNMP.
- Torch.
- Sniffer de paquetes.

Estas son las principales características del sistema operativo y software Mikrotik RouterOS elegido para la implementación de la red.

4.15 Instalación de Mikrotik routers

A continuación vamos a mostrar paso por paso como se realiza la instalación de Mikrotik sobre una plataforma x86. La plataforma cuenta con 2 placas de red PCI que poseen 4 bocas de red gigabyte Ethernet. Utilizaremos 2 bocas para conectarnos al proveedor de Internet. El resto de las placas se utilizaran para la distribución de nuestra red interna. Utilizaremos la versión 2.9.27 Nivel 6 del software Mikrotik Router Os.

Se “botea” con un CD que contenga la imagen del Mikrotik RouterOs ya quemada. Luego nos aparecerá el menú de instalación que nos preguntará que paquetes deseamos instalar.

Para desplazarnos por el menú utilizamos las tecla ‘P’ o ‘N’ o sino las flechas del teclado. Para seleccionar o deseleccionar los paquetes a instalar utilizamos la Barra Espaciadora. Luego presionamos la tecla ‘I’ para comenzar la instalación local en nuestra plataforma

```
Welcome to MikroTik Router Software Installation
Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'n'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

[X] system          [ ] lcd             [X] telephony
[X] ppp             [ ] ntp             [X] ups
[X] dhcp            [ ] radiolan        [X] user-manager
[X] advanced-tools [X] routerboard     [X] web-proxy
[ ] arlan           [X] routing         [X] webproxy-test
[ ] gps             [ ] routing-test    [ ] wireless
[X] hotspot         [X] rstp-bridge-test [X] wireless-legacy
[X] hotspot-fix    [X] security
[ ] isdn            [ ] synchronous
```

Fig. 4.6: Paquetes de configuración

Fuente: <http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>

- System: Paquete principal que posee los servicios básicos al igual que los drivers básicos.
- Ppp: Provee de soporte para PPP, PPTP, L2TP, PPPoE e ISDN PPP.
- Dhcp: Servidor y cliente DHCP.

El manual Mikrotik, además indica;

- Hotspot: provee de un hot spot.
- Hotspot-fix: Provee el parche para actualizar el modulo hot spot que tiene problemas en las versión 2.9.27.
- Ntp: Servidor y cliente NTP.
- Routerboard: provee de las utilidades para el router board.
- Routing: Provee soporte para RIP, OSPF y BGP4.
- Rstp-bridge-test: Provee soporte para Rapid Spanning Tree Protocol.

- Security: Provee soporte para IPSEC, SSH y conectividad segura con Winbox.
- Telephony: Provee soporte para H.323.
- Ups: provee soporte para UPS APC.
- User-manager: Servicio de usuario del RouterOs
- Web-Proxy: Paquete para realizar un Web Proxy.
- wireless-legacy: Provee soporte para placas Cisco Aironet, PrismII, Atheros entre otras.

Luego la instalación nos pregunta si deseamos quedarnos con la configuración anterior, contestamos que no 'N'.

La siguiente pregunta hace referencia a que perderemos todos los datos que se encuentran en el disco fijo le contestamos que si 'Y'.

```
Do you want to keep old configuration? [y/n]:n
Warning: all data on the disk will be erased!
Continue? [y/n]:
```

Fig. 4.7: Proceso de instalación

Fuente: <http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>

A continuación comienza el proceso de particionado y formateado del disco fijo que es automático y no nos hace ningún tipo de preguntas. Luego indica que se presione; 'Enter' para que el sistema se reinicie.

Seguidamente que se reinicia el sistema, nos pregunta si deseamos chequear la superficie del disco fijo le contestamos que si 'Y'.

Luego comienza la instalación de los paquetes seleccionados con anterioridad. Al finalizar dicho proceso se pide presionar: 'Enter' nuevamente para reiniciar el sistema.

```
installed hotspot-2.9.27
installed ppp-2.9.27
installed routing-test-2.9.27
installed advanced-tools-2.9.27
installed dhcp-2.9.27
installed ntp-2.9.27
installed routerboard-2.9.27
disabled routing-test-2.9.27
installed routing-2.9.27
installed rstp-bridge-test-2.9.27
installed security-2.9.27
installed telephony-2.9.27
installed ups-2.9.27
installed user-manager-2.9.27
installed web-proxy-2.9.27
installed (disabled) webproxy-test-2.9.27
installed wireless-legacy-2.9.27
disabled wireless-legacy-2.9.27
installed wireless-2.9.27

Software installed.
Press ENTER to reboot
```

Fig. 4.8: Instalación de paquetes seleccionados

Fuente: <http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>

Con el sistema reiniciado e instalado, la consola solicita el usuario y contraseña. Por defecto dicho nombre de usuario es: admin y para la contraseña se deja el casillero en blanco y se presiona enter.

```
MikroTik 2.9.27
MikroTik Login:
```

Fig. 4.9: Proceso de instalación (usuario y contraseña)

Fuente: <http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>

A continuación nos da la bienvenida y nos pregunta si deseamos leer la licencia lo cual contestamos que si 'Y'.

```
MikroTik 2.9.27
MikroTik Login: admin
Password:

MMM  MMM  KKK                      TTTTTTTTTT  KKK
MMMM  MMMM  KKK                      TTTTTTTTTT  KKK
MMM  MMMM  MMM  III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
MMM  MM  MMM  III  KKKKKK  RRR  RRR  000  000  TTT  III  KKKKKK
MMM  MMM  III  KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK
MMM  MMM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 2.9.27 (c) 1999-2006      http://www.mikrotik.com/

Do you want to see the software license? [Y/n]: _
```

Fig. 4.10: Licencia de instalación

Fuente: <http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>

Luego de haber leído la licencia ya nos queda la consola para comenzar a configurar nuestro Mikrotik.

```
MIKROTIK ROUTEROS V2.9 SOFTWARE ROUTER SYSTEM

This End-User License Agreement ("License Agreement") is a binding
agreement between you (either an individual or a single entity) and
MikroTikls SIA ("MikroTikls" or "MikroTik"), which is the manufacturer
of the SOFTWARE PRODUCT ("SOFTWARE PRODUCT" or "SOFTWARE") identified
above. HARDWARE refers as the computer, which the Software Product is
installed on. Any software provided along with the SOFTWARE PRODUCT
that is associated with a separate end-user License Agreement is
licensed to you under the terms of that License Agreement. The term
SOFTWARE or SOFTWARE PRODUCT does not include the software listed
after point 12 of this document that is under the GNU General Public
License or other free software licenses listed after point 12 of this
document.

By opening or installing SOFTWARE PRODUCT MikroTik RouterOS V2 you
indicate that you agree with terms of this agreement, if you do not
agree with the terms of this agreement, do not open the diskette
package and do not install or use the software, instead, return the
unopened package of the SOFTWARE including manuals, documentation, or
written materials that are associated with this program to the place
```

Fig. 4.11: Consola para la configuración del Mikrotik

Fuente: <http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>

4.15.1 Logueo al MIKROTIK

Hay varias maneras para acceder a la administración del Mikrotik sin haber configurado nada en un principio.

La primera es directamente desde la consola finalizada la instalación, otro método es utilizando una consola Telnet a través del el puerto serie o Ethernet por MAC o IP, sino mediante la utilización del software winbox, el cual lo brinda los desarrolladores de Mikrotik.

Debido a la flexibilidad, rapidez y ventajas que presenta la utilización de winbox respecto a los otros métodos, éste será la manera con la cual realizaremos la configuración de la red.

Desde una PC remota con Windows xp instalado. Conectados mediante un cable cruzado al Mikrotik al puerto Ethernet. Hacemos correr el softWinbox, el cual nos brindará una ventana para loguearse al Mikrotik.



Fig. 4.12: Winbox para loguearse al Mikrotik
Fuente:<http://www.mikrotik.com>[29]

En esta ventana nos deja introducir las direcciones Mac o IP de la placa del Mikrotik a la cual estamos conectados. Debido a que no hemos configurado el Mikrotik desde la consola. Hacemos clic en (...) esto hará que el software nos devuelva las direcciones Mac de las interfaces de red que posean un Mikrotik instalado y corriendo. Seleccionamos la interface y luego utilizaremos de Login: admin y como Password: (nada). Al finalizar esta carga de datos hacemos clic en Connect.

Cuando el software se conecta al Mikrotik automáticamente empieza a descargar los plugins instalados en el Mikrotik para poder administrarlos remotamente.



Fig. 4.13: Descarga de los plugins instalados en Mikrotik
Fuente:<http://www.mikrotik.com>[29]

Al finalizar la descarga de los plugins nos aparece la pantalla de configuración del Mikrotik. En la cual a mano izquierda se encuentra el menú de configuración de cada uno de los módulos instalados.

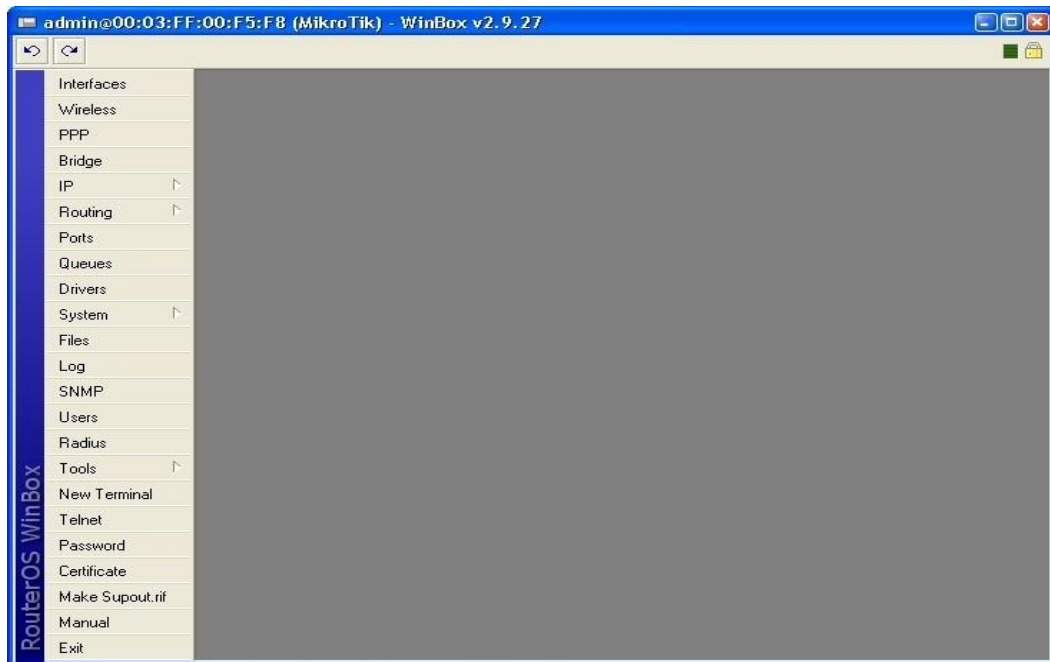


Fig. 4.14: Configuración del Mikrotik
Fuente: <http://www.mikrotik.com>[29]

En la barra superior del software nos encontramos con la barra de herramienta. En la misma sobre mano izquierda posee las opciones de undo y redo. Sobre mano derecha podemos encontrar dos iconos, el primero muestra la utilización del Mikrotik y el segundo nos indica si la conexión que estamos realizando es segura o no.

4.15.2 Backup y restore de configuración

Debido a los problemas que pueden producirse en los equipamientos, siempre es buena política tener back up de todas las configuraciones de los sistemas. Ahora mostraremos como se realizar un backup de la configuración y como se recupera.

4.15.3 BACKUP de la configuración

Primero se da clic al menú FILES allí se nos abrirá una ventana y nos mostrará los archivos que se encuentran almacenados. Debemos hacer clic sobre el botón de BACKUP para realizar nuestro backup.

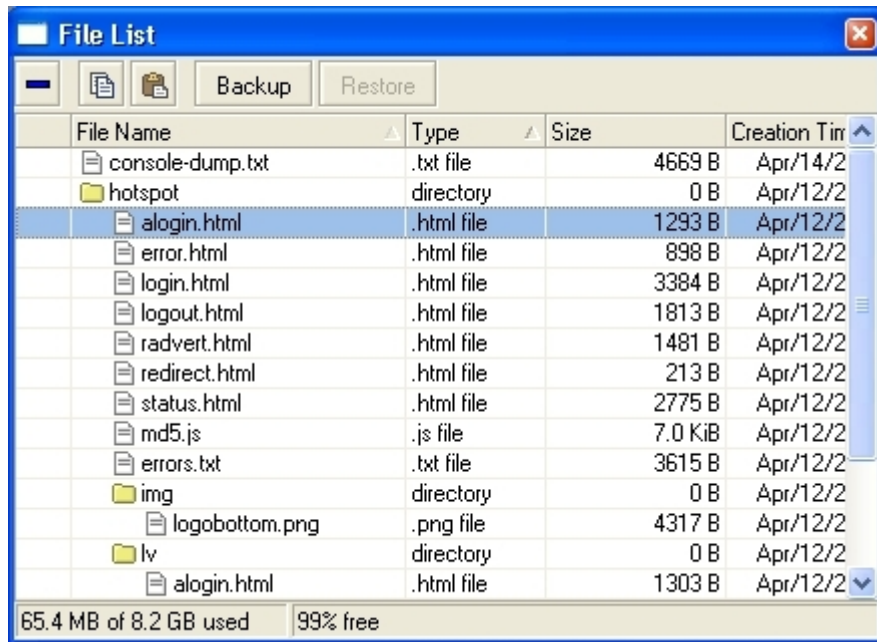


Fig. 4.15: Backup de la configuración

Fuente: <http://www.mikrotik.com>

Luego de haber hecho clic nos aparece un nuevo archivo en la lista que poseíamos, que es nuestro backup de toda la configuración del Mikrotik.

Sabiendo que el almacenamiento puede fallar, siempre es bueno tener una copia de resguardo en otro sitio. Para ello debemos hacer lo siguiente.

E selecciona el archivo de backup que deseamos y luego hacemos clic sobre el icono de COPY. Esto hará que nuestro archivo de configuración quede almacenado en el porta papeles de Windows. A continuación creamos una carpeta en el disco fijo de la PC y pegamos el archivo. Nos aparecerá y ya tendremos el backup de nuestro archivo de configuración en nuestra PC

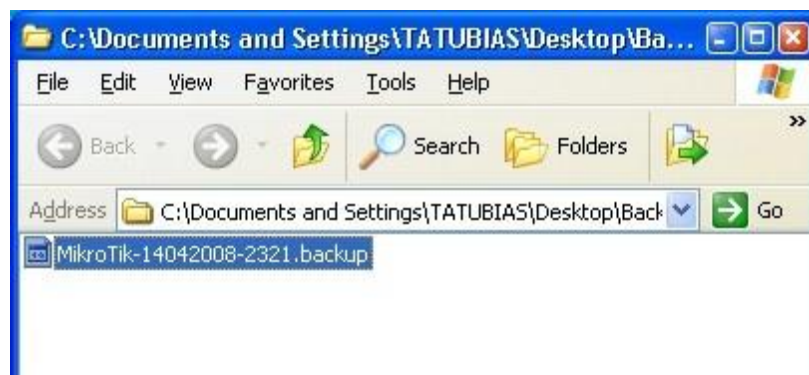


Fig. 4.16: Almacenamiento del archivo de configuración en Windows
Fuente: <http://www.mikrotik.com>

4.15.4 Restore de la configuración

Si estamos recuperando el archivo de configuración que está dentro del Mikrotik. Simplemente debemos ir al menú FILES. En la ventana que nos aparece debemos seleccionar la versión del backup que deseamos recuperar y hacer clic sobre el botón de RESTORE.

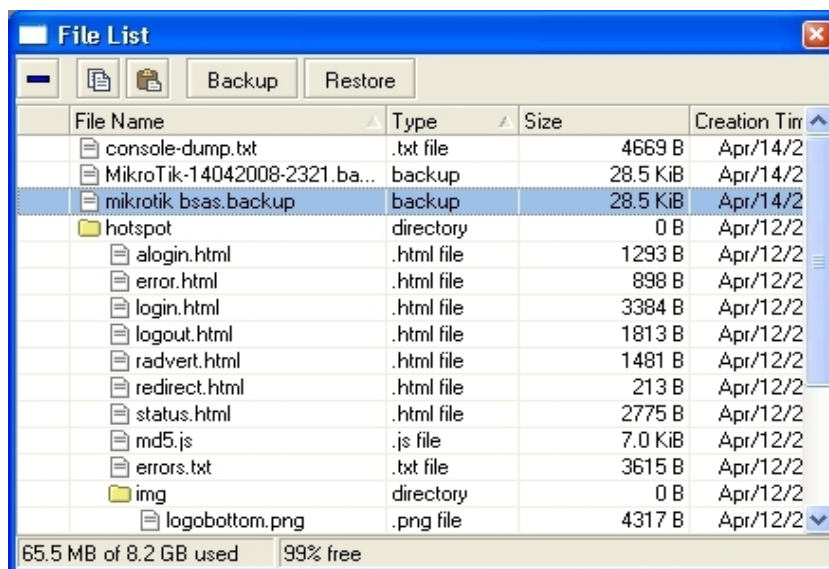


Fig. 4.17: Recuperación del archivo de configuración del Mikrotik
Fuente: <http://www.mikrotik.com>

Para el caso que el archivo de back up se encuentre en nuestro disco fijo. Seleccionamos el archivo de backup, luego hacemos clic con el botón derecho del mouse y seleccionamos copiar. Luego en el winbox, simplemente debemos ir al menú FILES. En la ventana que nos aparece, debemos hacerle

clic en el icono de pegar y nos aparecerá nuestra nueva configuración. A continuación seleccionamos nuestra nueva configuración y apretamos el botón de restore. Se nos abrirá una nueva ventana que nos aplicara la nueva configuración y nos hará reiniciar nuestro Mikrotik.

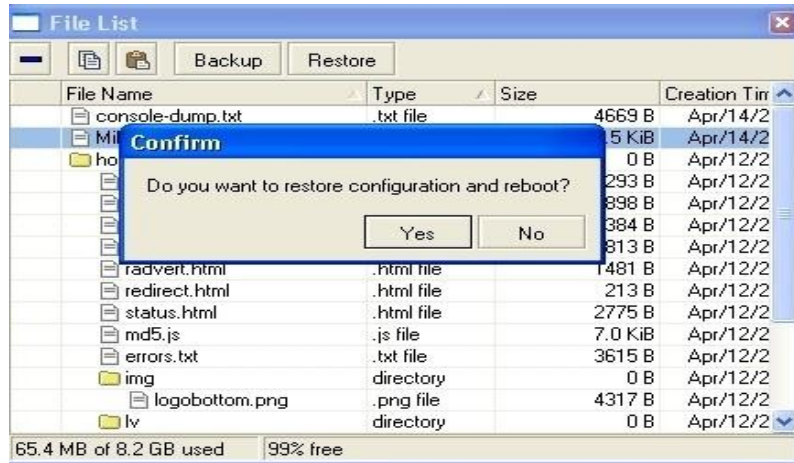


Fig. 4.18: Recuperación del archivo de configuración del Mikrotik
Fuente: <http://www.mikrotik.com/software.html>[30]

4.15.5 Definición y configuración de interfaces

Actualmente las placas de red están funcionando pero les falta la configuración básica para que se pueda acceder a ellas. Para esto deberemos asignarles los IP a cada una de las interfaces.

4.15.6 Asignación de nombres a las interfaces

En el menú se escoge INTERFACES. A continuación aparece la lista de interfaces que posee nuestro sistema. Se hace doble clics sobre las interfaces y se procede a cambiar el nombre asignándole los nombres correspondientes a cada una. En nuestro caso utilizaremos:

- ADMINISTRACION:_Será la interface exclusiva de Administración ubicada en Secretaría.
- AGRONOMIA: _Para nuestra conexión dedicada con IP fijo.
- LABORATORIO: _Para nuestra conexión dedicada con IP fijo.

4.15.6.1 Interface: ADMINISTRACIÓN

Ubicada en Secretaría de la Facultad Técnica

PESTAÑA GENERAL:

- Name: Administración
- MTU: 1500
- ARP: Enable

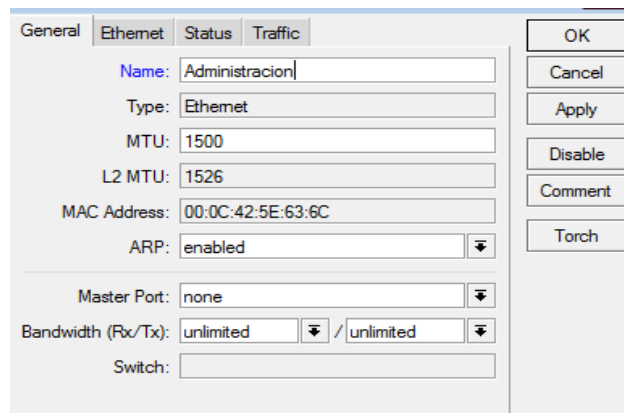


Fig. 4.19: Pestaña general del interface (Administración)
Fuente: <http://www.mikrotik.com/software.html>[30]

PESTAÑA ETHERNET:

- 100Mbps: Seleccionado
- Auto negotiation: seleccionado
- Full duplex: seleccionado.

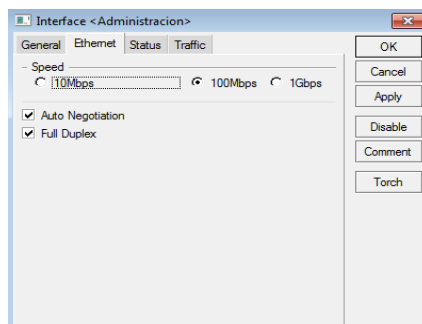


Fig. 4.20: Pestaña Ethernet del interface (Administración)
Fuente: <http://www.mikrotik.com/software.html>[30]

PESTAÑA STATUS:

En esta ventana podemos ver el estatus la interface actual.

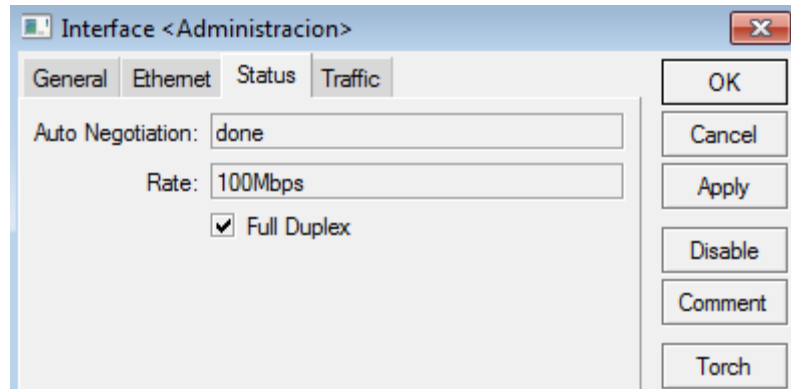


Fig. 4.21: Pestaña status del interface (Administración)

Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA TRAFFIC:

1. Vemos la gráfica de kbps enviados y recibidos por dicha interface.
2. Vemos la gráfica de p/s enviados y recibidos por la interface.

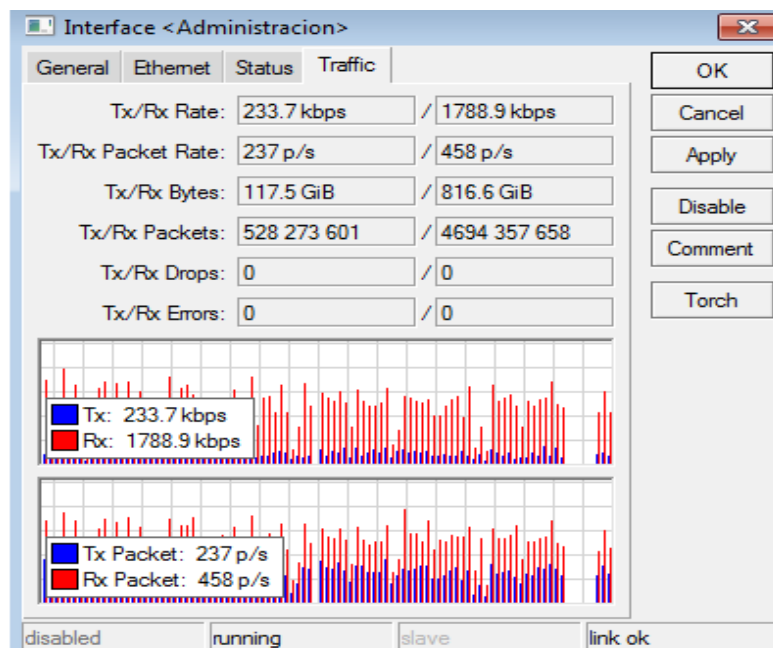


Fig. 4.22: Pestaña Traffic del interface (Administración)

Fuente: <http://www.mikrotik.com/software.html>

4.15.6.2 Interface: AGRONOMÍA

Ubicada en la Facultad de Agronomía

PESTAÑA GENERAL:

- Name: Agronomía
- MTU: 1500
- ARP: Enable

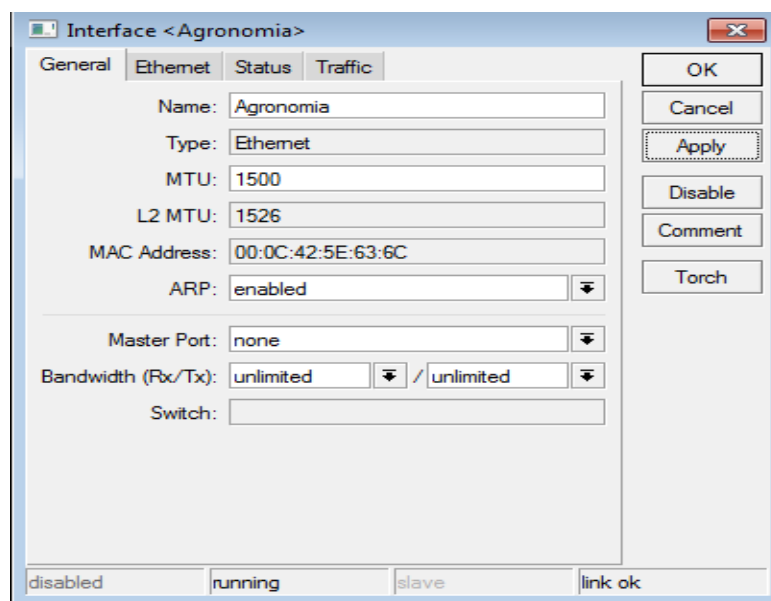


Fig. 4.23: Pestaña general del interface (Agronomía)

Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ETHERNET:

- 100Mbps: Seleccionado
- Auto negotiation: seleccionado
- Full duplex: seleccionado

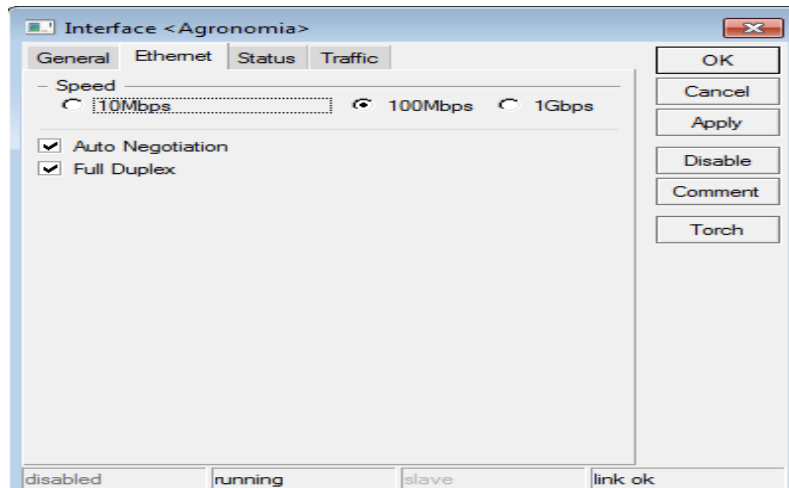


Fig. 4.24: Pestaña Ethernet del interface (Agronomía)
Fuente: <http://www.mikrotik.com/software.html>

4.15.6.3 Interface: LABORATORIO

Ubicada en el Laboratorio de Computación

PESTAÑA GENERAL:

- Name: Laboratorio
- MTU: 1500
- ARP: Enable

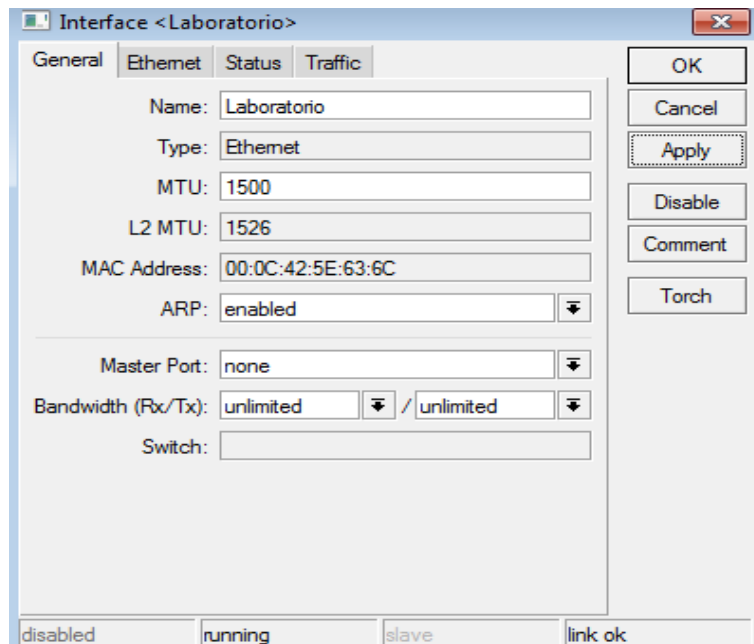


Fig. 4.25: Pestaña General del interface (Laboratorio)
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ETHERNET:

- 100Mbps: Seleccionado
- Auto negotiation: seleccionado
- Full duplex: seleccionado

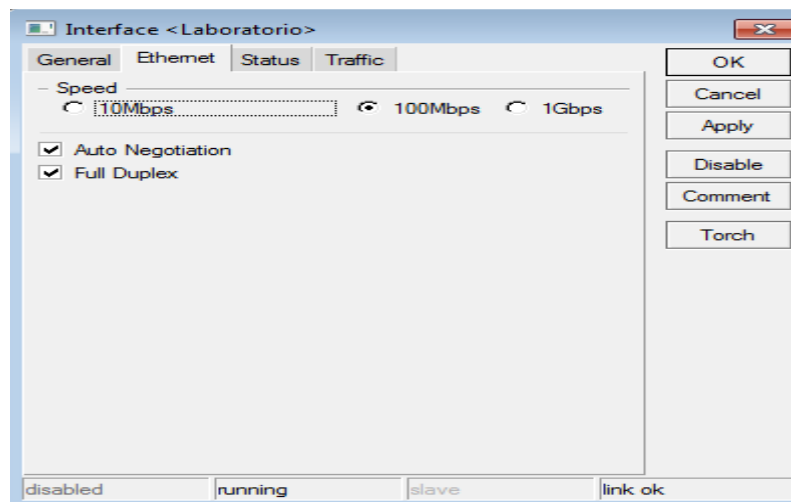


Fig. 4.26: Pestaña Ethernet del interface (Laboratorio)

Fuente: <http://www.mikrotik.com/software.html>

4.15.7 Definición de Vlans

Debido a las características departamentales de la empresa debemos realizar 3 vlans para separar las áreas de:

- Administración
- Agronomía
- Laboratorio de Computación

Para configurar las Vlans debemos ir al menú Interfaces, se nos abrirá la ventana de configuración de interfaces. Hacemos clic sobre el icono (+) y se nos desplegará un menú, elegimos la opción Vlan y entramos a la ventana de configuración de las mismas.

4.15.7.1 Vlan ADMINISTRACIÓN

PESTAÑA GENERAL:

- Name: Vlan_Administración
- Type: Vlan
- MTU: 1500
- MAC:00:0C:42:5E:63:6C
- ARP: Enable
- Vlan ID:1
- Interface: Administración

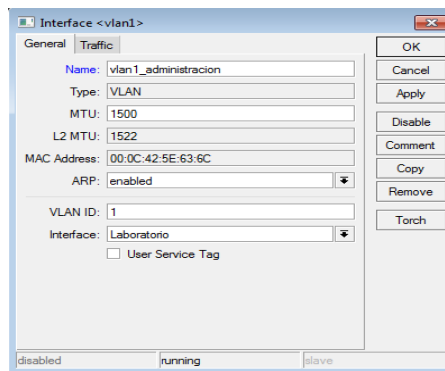


Fig. 4.27: Pestaña General del Vlan (Administración)

Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA TRAFFIC:

- Ver la gráfica de kbps enviados y recibidos por dicha vlan
- Ver la gráfica de p/s enviados y recibidos por la vlan

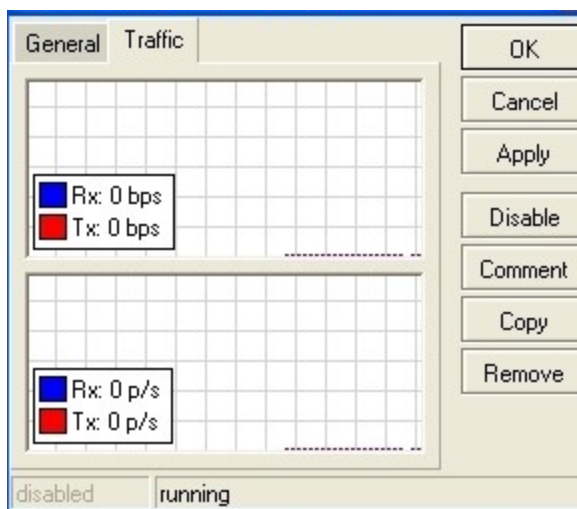


Fig. 4.28: Pestaña Traffic del Vlan (Administración)
Fuente: <http://www.mikrotik.com/software.html>

Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP	Bonding
R	↔ Laboratorio	Ethernet				
R	↔ vlan1	VLAN				
R	↔ bridge100	Bridge				
X	↔ ether2	Ethernet				
X	↔ ether3	Ethernet				
R	↔ wlan_	Wireless (Atheros AR5...				
DRA	↔ wds1	WDS				

Fig. 4.29: Pestaña de la lista de interface del Vlan (Administración)
Fuente: <http://www.mikrotik.com/software.html>

4.15.8 Asignación de direcciones IP Salas interfaces

Con los nombres asignados a las interfaces, debemos asignarle el IP a las mismas. Para ello debemos ir al menú IP / Addresses.

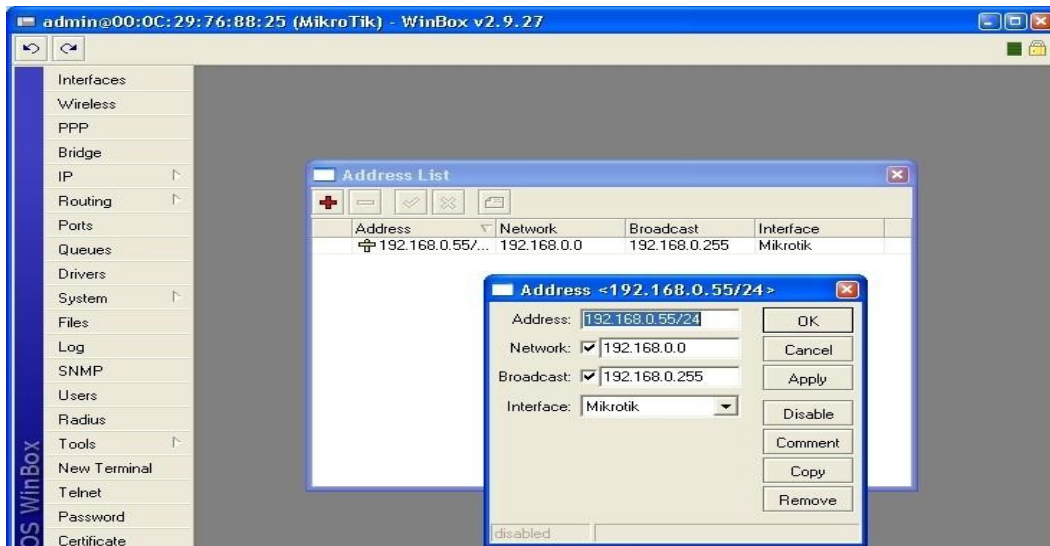


Fig. 4.30: Pestaña de asignación de IP a las interfaces

Fuente: <http://www.mikrotik.com/software.html>

Haciendo clic sobre el icono (+) nos abre una ventana que nos deja introducir los datos necesarios para nuestras interfaces.

INTERFAcE ADMINISTRACIÓN:

- Address: 172.16.1.199/24
- Network 172.16.1.0
- Broadcast: 172.16.1.255
- Interface: Administracion

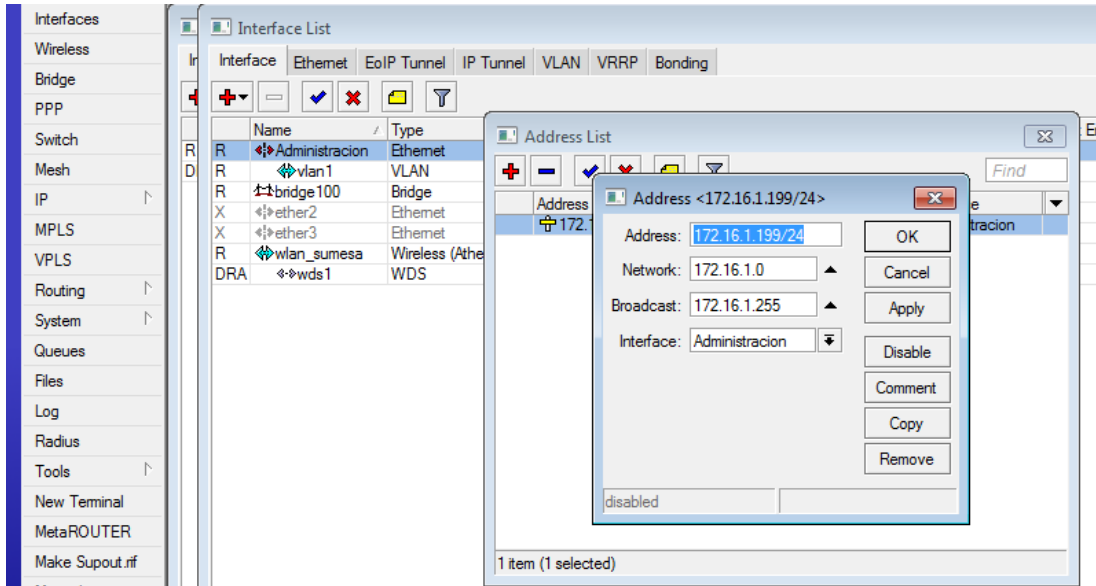


Fig. 4.30: Pestaña de asignación de IP a la interface Administracion

Fuente: <http://www.mikrotik.com/software.html>

INTERFACE LABORATORIO:

- Address: 172.16.1.200/24
- Network 172.16.1.0
- Broadcast: 172.16.1.255
- Interface: Laboratorio

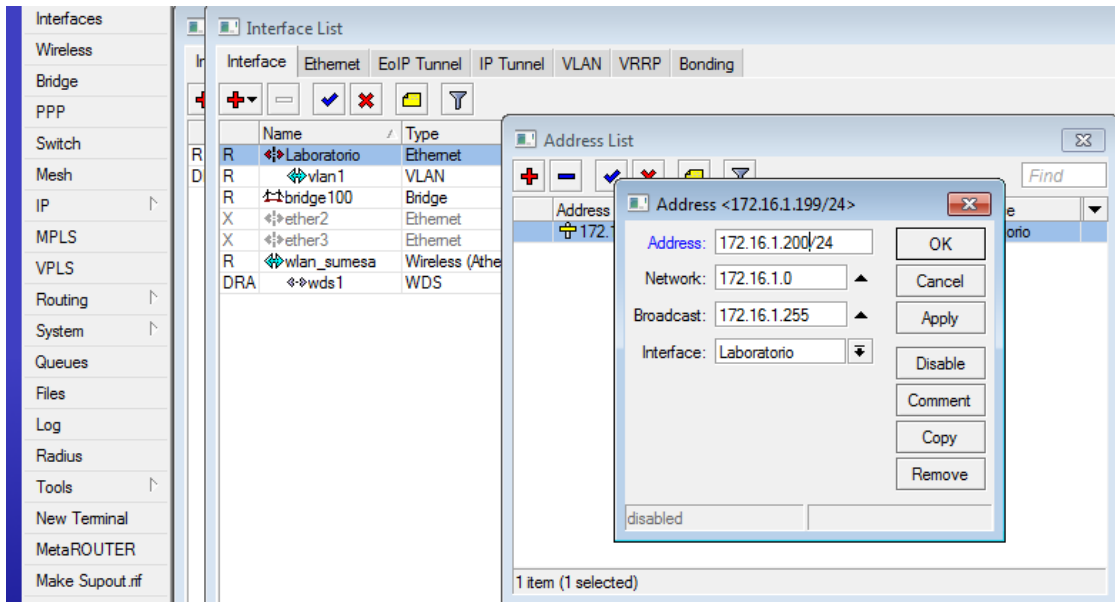


Fig. 4.31: Pestaña de asignación de IP a la interface Laboratorio

Fuente: <http://www.mikrotik.com/software.html>

INTERFACE AGRONOMIA:

- Address: 172.16.1.201/24
- Network 172.16.1.0
- Broadcast: 172.16.1.255
- Interface: Agronomía

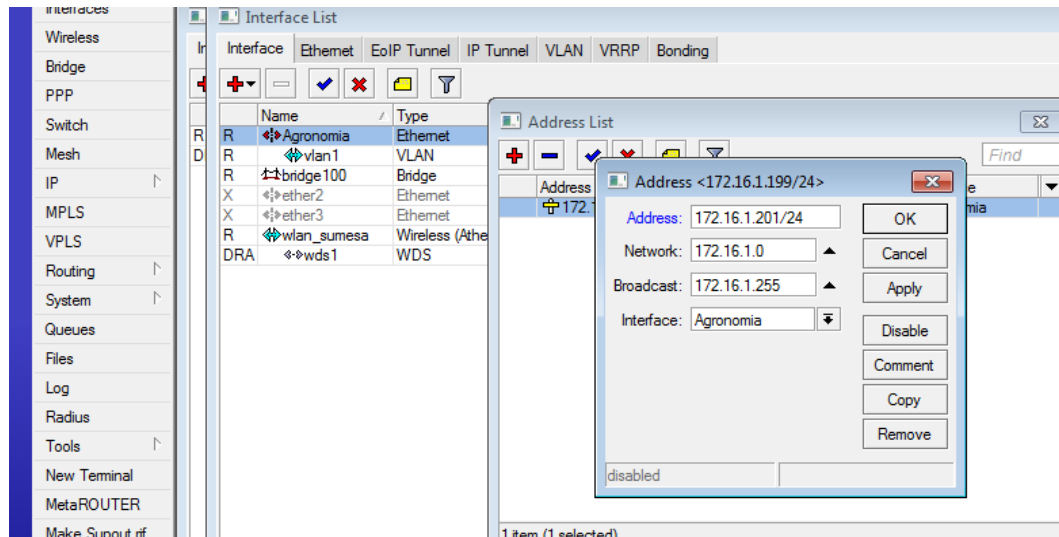


Fig. 4.32: Pestaña de asignación de IP a la interface Agronomía
Fuente: <http://www.mikrotik.com/software.html>

INTERFACE HOT SPOT:

- Address: 192.168.5.1/24
- Network: 192.168.5.0
- Broadcast: 192.168.5.255
- Interface: Hot spot



Fig. 4.33: Pestaña de asignación de IP a la interface Hot Spot
Fuente: <http://www.mikrotik.com/software.html>

Para realizar dicha configuración debemos ir en el menú a: IP / UNPnP. Hacemos clic sobre el icono (+) y asignamos a cada una de las interfaces si es interna o externa.

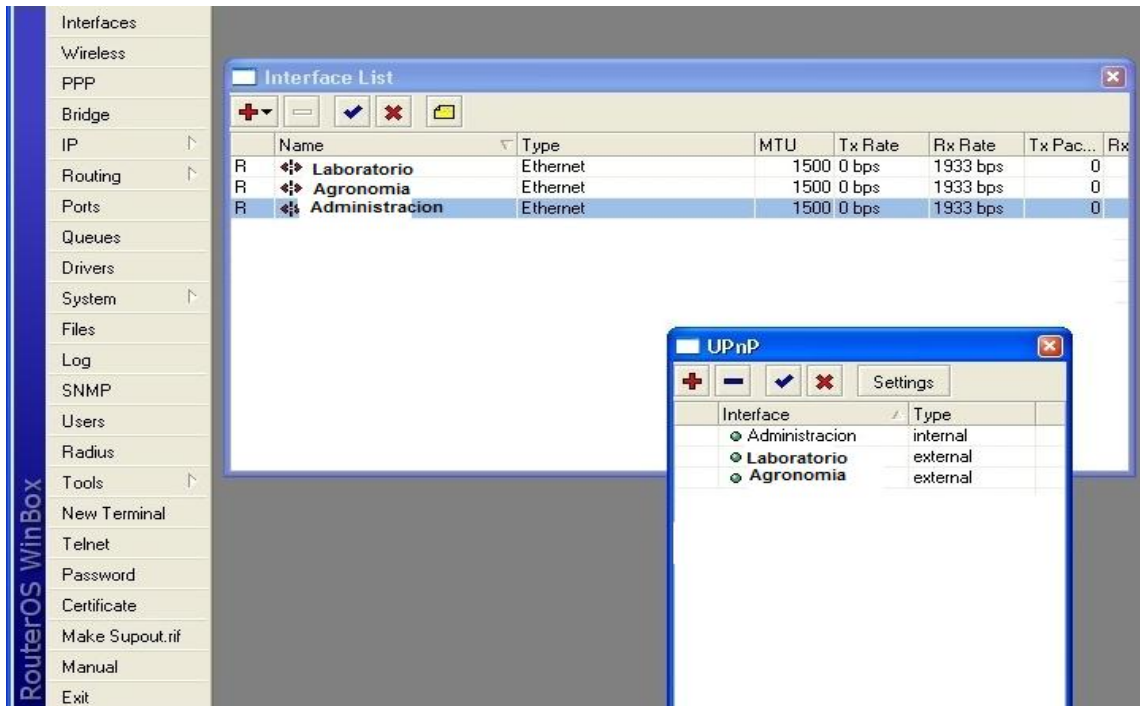


Fig. 4.34: Pestaña de configuración interna o externa de IP de las interfaces
Fuente: <http://www.mikrotik.com/software.html>

Luego de haber asignado los tipos de interface debemos configurar un último detalle en settings. Le deseleccionamos la opción “allow to disableExternal Interface”



Fig. 4.35: Pestaña de anulación de opción
Fuente: <http://www.mikrotik.com/software.html>

4.15.9 Configuración POOLS de direcciones de IP

En una primera instancia hay que crear los pool's de ip's que van a poseer los grupos de administración, ventas y producción y servers.

Para ello Vamos al menú IP / POOL. Se nos abre la ventana de configuración de pool y hacemos clic en el icono (+). En la nueva ventana creamos cada pool para cada una de los grupos. La configuración de los mismos es:

- Nombre: Pool Servers
- Rango de ip: 192.168.1.5 a 192.168.1.254



Fig. 4.36: Pestaña de configuración del Pool Servers
Fuente: <http://www.mikrotik.com/software.html>

- Nombre: Pool Administración
- Rango de ip: 192.168.2.5 a 192.168.2.254



Fig. 4.37: Pestaña de configuración del Pool Administración
Fuente: <http://www.mikrotik.com/software.html>

Se ha elegido comenzar todos los rangos a partir del ip x.x.x.5 para reservar números de ip en el caso que se necesite instalar algún tipo de servidor en cada grupo.

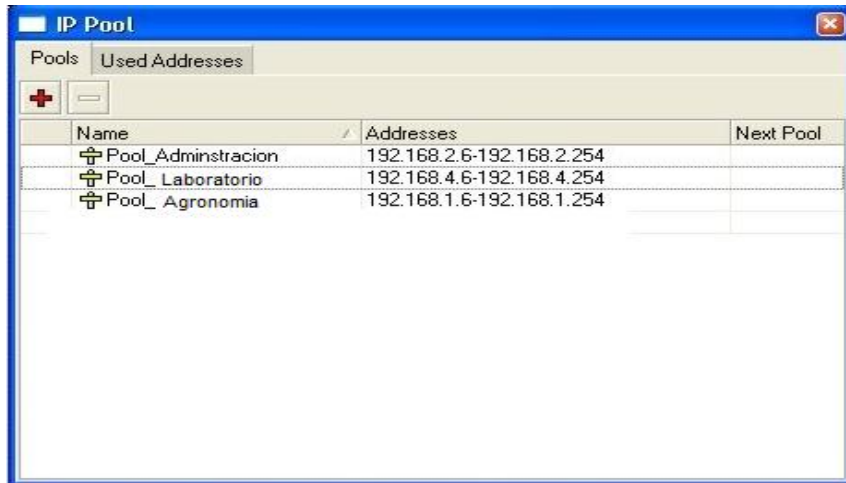


Fig. 4.38: Pestaña de inicio de los rangos

Fuente: <http://www.mikrotik.com/software.html>

4.15.10 Definir DNS

Para definir los DNS simplemente hay que ir al menú IP / DNS. Se nos abre una ventana de configuración. Hacemos clic en Settings y escribimos los DNS del proveedor de Internet.

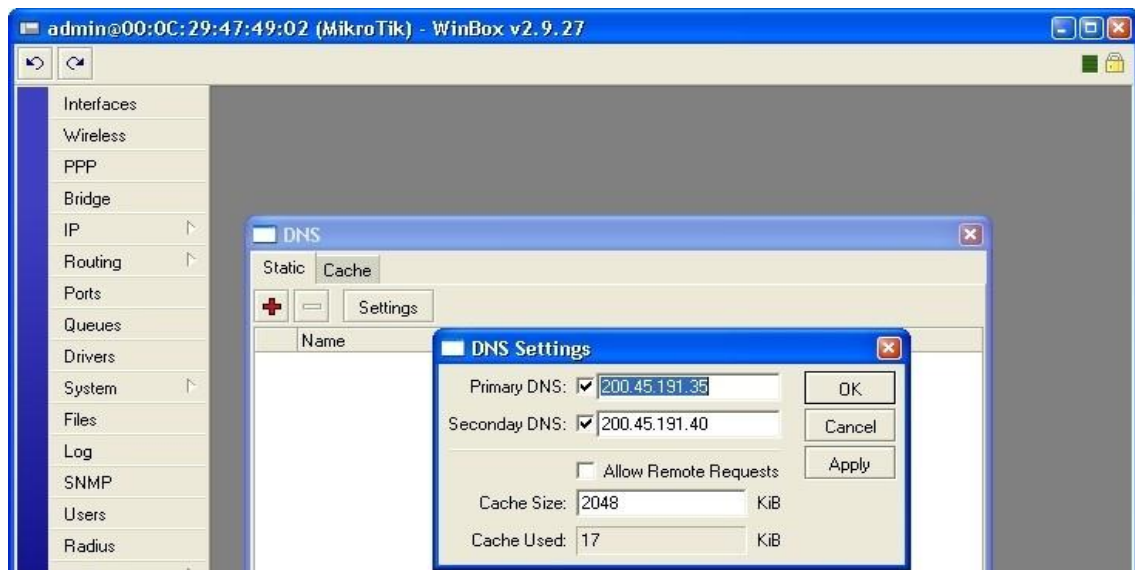


Fig. 4.39: Pestaña para definir DNS

Fuente: <http://www.mikrotik.com/software.html>

Los datos que ingresamos son:

- ✓ Primary DNS: 200.45.191.35
- ✓ Secondary DNS: 200.45.191.40

4.15.11 Nat Masquerade para todas las redes

Para realizar el **NAT** transparente entre todas las redes debemos ir al menú IP/FIREWALL. Ahí en la nueva ventana nos dirigimos a la pestaña NAT y hacemos clic sobre el icono (+). A continuación aparece una ventana nueva de configuración para políticas de NAT y la configuramos de la siguiente manera:

PESTAÑA GENERAL:

- ✓ Chan: srcnat

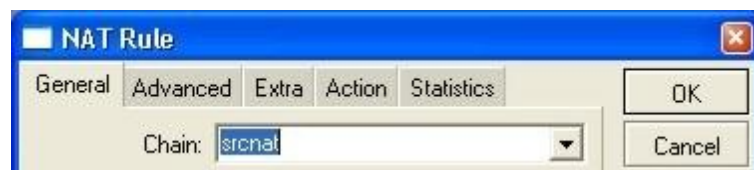


Fig. 4.40: Pestaña general para configurar políticas de NAT

Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ACTION:

- ✓ Action: masquerade

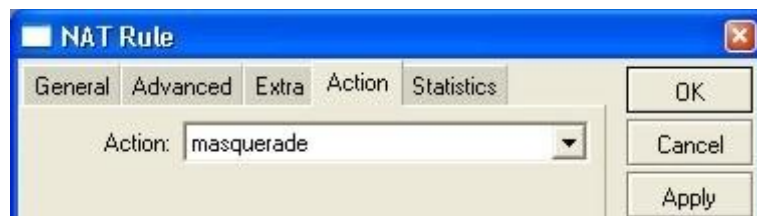


Fig. 4.41: Pestaña action para configurar políticas de NAT

Fuente: <http://www.mikrotik.com/software.html>

4.15.12 Configuración servidor DHCP

A continuación daremos de alta el servidor de DHCP en si. Para ello debemos ir al menú IP / DHCP Server. Se nos abrirá una ventana de configuración de servidores dhcp. Hacemos clic en el icono (+) y creamos nuestros servidores de dhcp para cada una de las áreas ya mencionadas.

4.15.12.1 Ventana de configuración DHCP:

En esta ventana iremos introduciendo todos los requisitos necesario para ir levantado los servidores de dhcp. La configuración para cada uno de los servidores dhcp fue la siguiente:

DHCP Administración y así iremos realizando estos cambios en todos nuestros equipos:

- ✓ Nombre: DHCP Administración
- ✓ Interface: administración
- ✓ Address Pool: Pool administración



Fig. 4.42: Pestaña de configuración DHCP

Fuente: <http://www.mikrotik.com/software.html>

No obstante los servidores de dhcp están configurados, necesitamos configurar las ´redes´. Para ello en la ventana de DHCP Server hacemos clic en la pestaña Network. Luego hacemos clic en el icono (+) y cargamos los datos de la red.

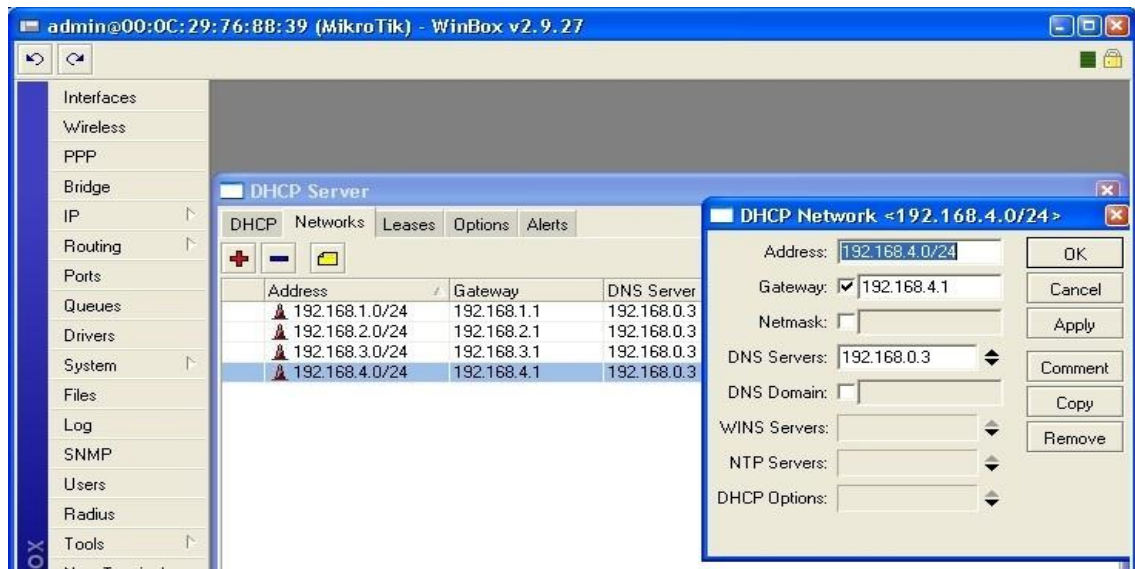


Fig. 4.43: Pestaña de configuración de las redes
Fuente: <http://www.mikrotik.com/software.html>

Configuración:Red Administración:

Address: 192.168.2.0/24

Gateway: 192.168.2.1

Dns Server: 192.168.0.3

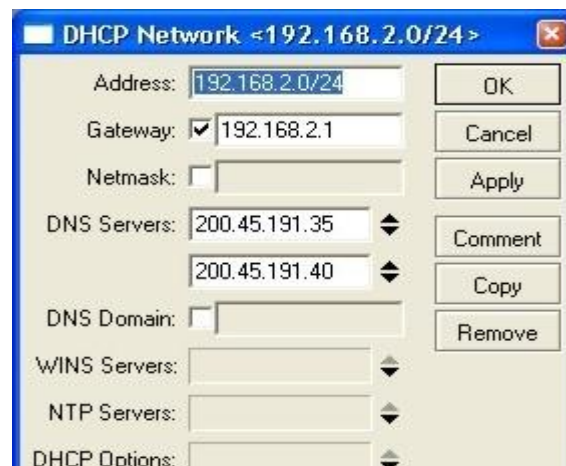


Fig. 4.44: Pestaña de configuración de la red de Administración
Fuente: <http://www.mikrotik.com/software.html>

4.15.13 Asignación de direcciones de IP fijas a partir de direcciones MAC

Debemos asignarle ip fijo a nuestros servidores para que sea más simple nuestra configuración del sistema. Para ello la asignación de ip fijo la hacemos mediante el servidor de dhcp, asignando una dirección de ip fija a una Mac.

Los pasos de configuración son los siguientes. Nos dirigimos al menú IP / DHCP Server. En la ventana que nos aparece hacemos clic en la pestaña LEASES. En mencionada pestaña hacemos clic en el icono (+). La configuración de la ventana es:

Server de snmp, jabber:

- Address: 192.168.1.2
- MAC Address: 00:0C:29:64:45:9E (MAC del servidor snmp, jabber)
- Servers: all

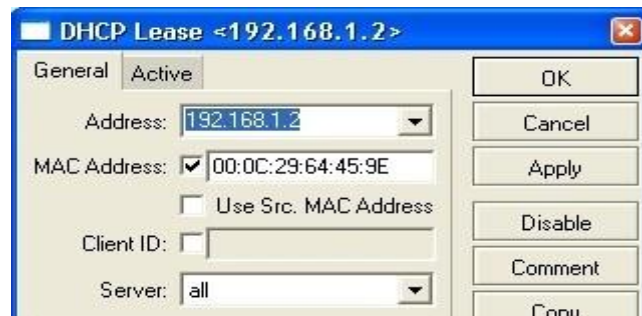


Fig. 4.45: Pestaña de asignación de direcciones IP
Fuente: <http://www.mikrotik.com/software.html>

Luego para que esta asignación quede estática debemos hacer clic en el botón de MAKE STATIC. De la pestaña LEASES.

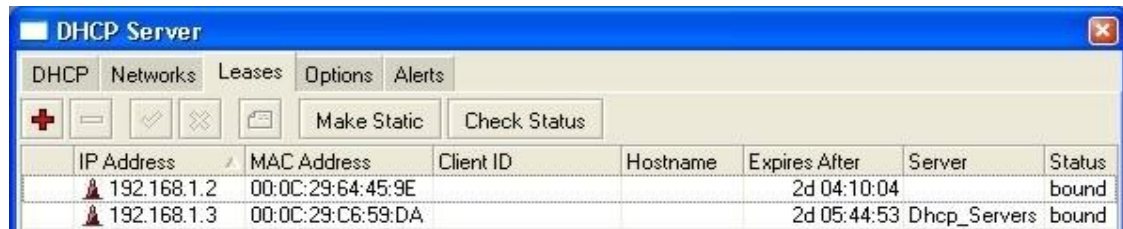


Fig. 4.46: Pestaña de asignación de direcciones IP fijas
Fuente: <http://www.mikrotik.com/software.html>

4.15.14 Configuración servidor - CLIENTE NTP

Debido a que utilizaremos políticas referenciadas a tiempo debemos ser precisos con el mismo. Para ello debemos instalar un cliente en nuestro Mikrotik para tener la hora precisa y un servidor para brindarles dicha hora a los clientes. Consecuentemente debemos seguir los siguientes pasos.

4.15.14.1 Servidor NTP

Para el servidor nos dirigimos al menú SYSTEM / NTP SERVER. En la nueva ventana Seleccionamos solamente la opción MANYCAST y hacemos clic en el botón de ENABLE

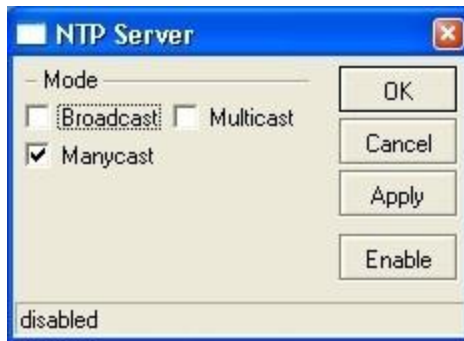


Fig. 4.47: Pestaña de configuración de Servidor NTP

Fuente: <http://www.mikrotik.com/software.html>

Ahora Con esta configuración del servidor podemos hacer que todas las computadoras de la red estén sincronizadas con nuestro servidor de tiempo.

4.15.14.2 Cliente NTP

Para configurar nuestro cliente NTP, para que nos sincronice nuestra hora del Mikrotik conjuntamente con la de un reloj nuclear. Debemos ir al menú SYSTEM / NTP CLIENT. Se nos abrirá la ventana de configuración del cliente NTP y le asignamos los valores siguientes:

- Mode: Unicast
- Primary NTP Server: 129.6.15.28

- Secondary NTP Server: 129.6.15.29

Luego hacemos clic en ENABLE. Dichos servidores son:

- time-a.nist.gov 129.6.15.28
- NIST, Gaithersburg, Maryland
- time-b.nist.gov 129.6.15.29
- NIST, Gaithersburg, Maryland

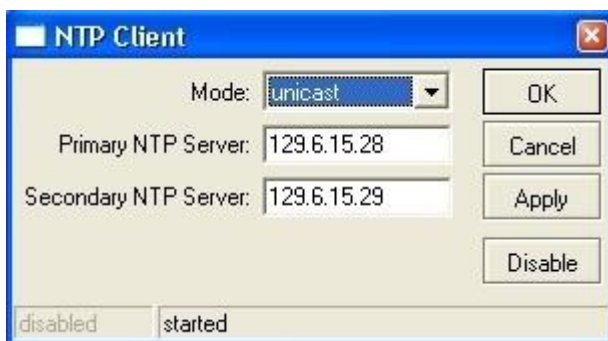


Fig. 4.48: Pestaña de configuración de cliente NTP

Fuente: <http://www.mikrotik.com/software.html>

A continuación nos dirigimos al menú SYSTEM / CLOCK. En la nueva ventana le cargamos los datos de fecha, hora, y uso horario. Para nuestro caso los mismos son:

- Date: Sept/07/2013
- Time: 16:17:00
- Time Zone: Manual

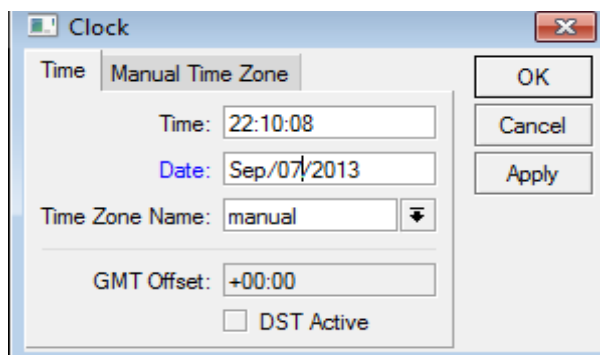


Fig. 4.49: Pestaña de configuración de datos

Fuente: <http://www.mikrotik.com/software.html>

4.15.15 Servidor web PROXY

Se decidió utilizar un servidor Web Proxy para ahorrar ancho de banda utilizado por los usuarios en Internet. Para ello nos dirigimos al menú IP / WEB-PROXY.

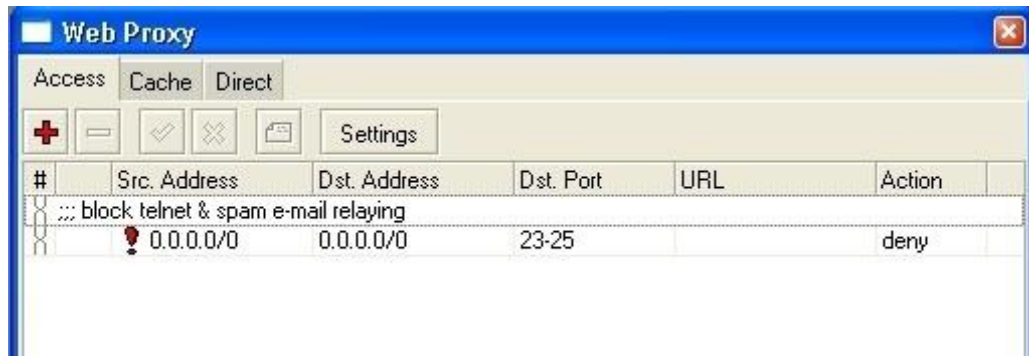


Fig. 4.50: Pestaña del servidor web Proxy
Fuente: <http://www.mikrotik.com/software.html>

En nuestra ventana de configuración hacemos clic en SETTINGS. De esta manera entramos a la ventana de configuración del servidor Proxy. Dicha ventana la configuraremos de la siguiente manera.

- Src. Address: La dejamos en blanco
- Port: 3128
- Hostname: Proxy
- Transparent Proxy: Seleccionado.
- Parent Proxy: lo dejamos en blanco
- Parent Proxy Port: lo dejamos en blanco
- Cache Administrator: administrador@ucsg.com
- Maximum Object size: 4096
- Cache Drive: system
- Maximum cache Size : 2000000
- Maximum Ram Cache Size 128000

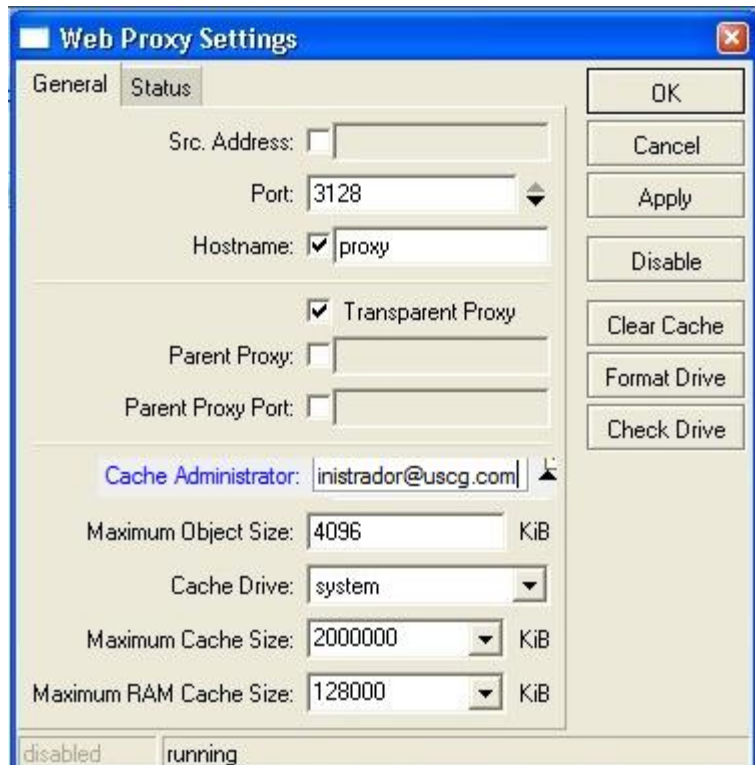


Fig. 4.51: Pestaña de configuración del servidor web Proxy
Fuente: <http://www.mikrotik.com/software.html>

A continuación hacemos clic en ENABLE. Se nos abre una ventanita y le hacemos clic en ok.

Como segundo paso debemos generar un una regla en el firewall para que haga un redireccionamiento al servidor Proxy. Para ello nos dirigimos al menú IP / FIREWALL en nuestra ventana de configuración hacemos clic en la pestaña NAT, luego clic en el botón (+). La ventana la configuramos de la siguiente manera.

INTERFACE ADMINISTRADOR:

- Chain: dstnat
- Protocol: 6 (tcp)
- Interface producción.

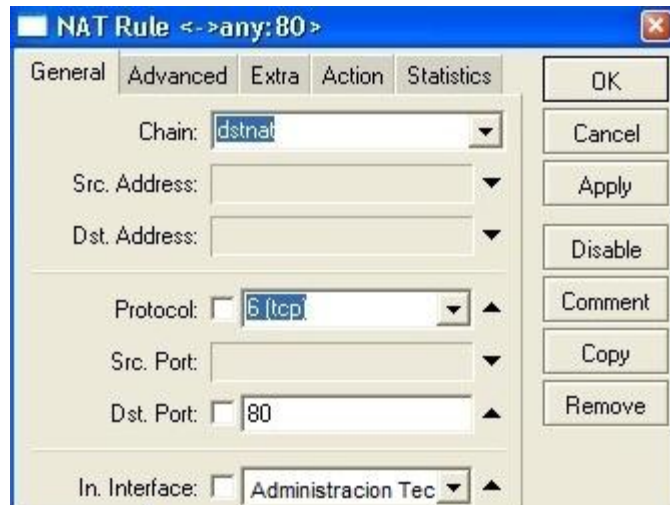


Fig. 4.52: Pestaña de redireccionamiento del NAT Rule
Fuente: <http://www.mikrotik.com/software.html>

Luego hacemos clic sobre la pestaña ACTION y la configuramos de la siguiente manera:

- ✓ Action: Redirect
- ✓ To ports: 3128



Fig. 4.53: Pestaña de Action de redireccionamiento del NAT Rule
Fuente: <http://www.mikrotik.com/software.html>

Realizamos esta misma configuración para cada una de las interfaces de nuestra red.

Por último configuraremos el NAT para el ruteo entre todas las subredes de la Facultad. Para ello nos dirigimos al menú IP / FIREWALL en nuestra ventana de configuración hacemos clic en la pestaña NAT, luego clic en el botón (+). La ventana la configuramos de la siguiente manera.

PESTAÑA GENERAL:

- Chain: srcnat

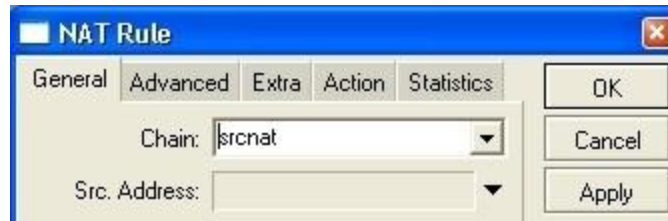


Fig. 4.54: Pestaña general del NAT Rule
Fuente: <http://www.mikrotik.com/software.html>

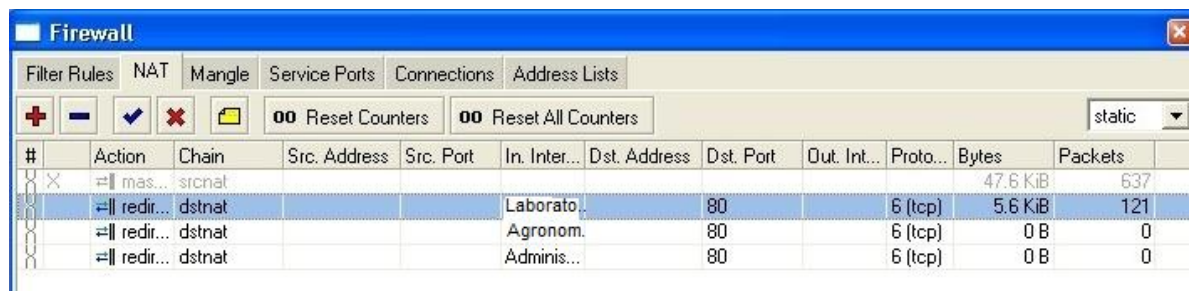
PESTAÑA ACTION:

- Action: Masquerade



Fig. 4.55: Pestaña de Action del NAT Rule
Fuente: <http://www.mikrotik.com/software.html>

Nuestra configuración de políticas de NAT se ven de la siguiente manera:

The image shows a "Firewall" window with several tabs: "Filter Rules", "NAT", "Mangle", "Service Ports", "Connections", and "Address Lists". The "NAT" tab is selected. Below the tabs, there are buttons for adding (+), deleting (-), enabling (checkmark), and disabling (cross) rules, along with "Reset Counters" and "Reset All Counters" buttons. A dropdown menu is set to "static". Below this is a table with columns: "#", "Action", "Chain", "Src. Address", "Src. Port", "In. Inter...", "Dst. Address", "Dst. Port", "Out. Int...", "Proto...", "Bytes", and "Packets".

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
	mas...	srcnat								47.6 KiB	637
	redir...	dstnat			Laborato...		80		6 (tcp)	5.6 KiB	121
	redir...	dstnat			Agronom.		80		6 (tcp)	0 B	0
	redir...	dstnat			Adminis...		80		6 (tcp)	0 B	0

Fig. 4.56: Pestaña de Firewall del NAT
Fuente: <http://www.mikrotik.com/software.html>

A continuación debemos proteger nuestro servidor de cualquier utilización desde el exterior de la red. Para ello nos dirigimos al menú IP / FIREWALL. En la ventana nueva hacemos clic en la pestaña FILTER RULES, a continuación hacemos clic en el icono (+). Nuestra nueva política de filtrado de paquetes la configuramos así:

PESTAÑA: GENERAL:

- Chain: input
- Protocol: 6 (tcp)
- Dst. Port.: 3128
- In. Interface: administración Técnica

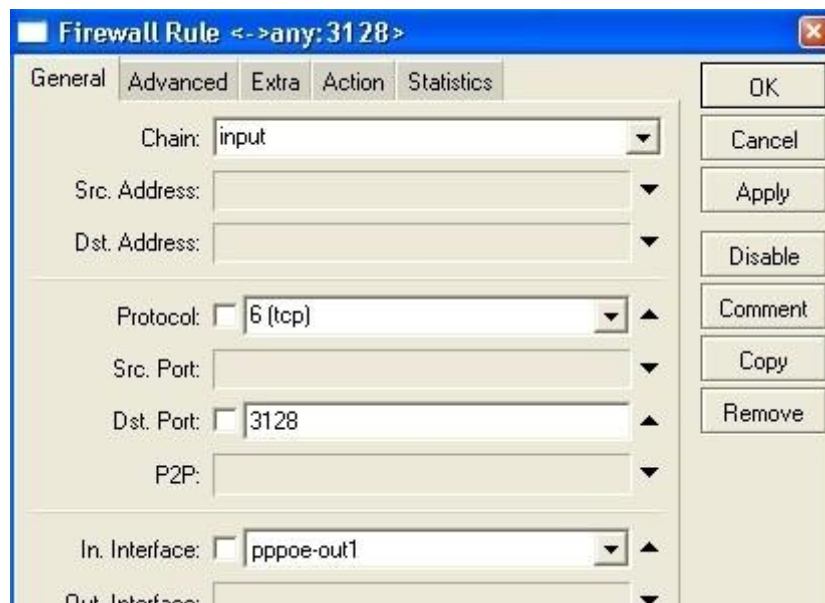


Fig. 4.57: Pestaña general de Firewall Rule
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ACTION:

- Action: Drop



Fig. 4.58: Pestaña Action de Firewall Rule
Fuente: <http://www.mikrotik.com/software.html>

Nuestras políticas de filtrado se ven de la siguiente manera:

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
...	drop	forward					1863		6 (tcp)	0 B	0
...	drop	forward				207.46.107...			6 (tcp)	0 B	0
...	drop	forward					5190		6 (tcp)	0 B	0
...	drop	forward					6901		6 (tcp)	0 B	0
...	drop	forward					6891-6900		6 (tcp)	0 B	0
...	drop	forward						Agrono..		0 B	0
...	drop	forward						Laborat..		0 B	0
...	drop	input			pppoe:...		3128		6 (tcp)	0 B	0

Fig. 4.59: Pestaña de filtrado del Firewall
Fuente: <http://www.mikrotik.com/software.html>

Bloquearemos algunas páginas con la utilización del Web Proxy. Para ello se definió que no se podrá ingresar a sitios pornográficos desde la red ni la utilización de páginas que tengan el servicio de Web Messenger al igual que Yahoo u otros.

4.15.16 Bloqueo de pornografía

Nos dirigimos al menú IP / Web Proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *porn*
- Method: any
- Action: deny

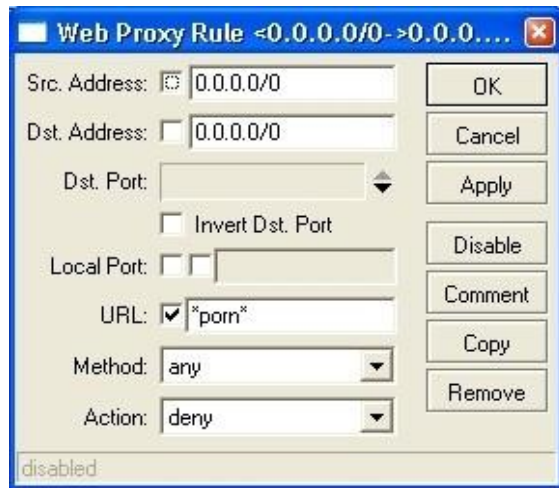


Fig. 4.60: Pestaña de bloqueo de pornografía
Fuente: <http://www.mikrotik.com/software.html>

Este filtro nos bloqueara cualquier site que posea la palabra *porn* en su nombre. También nos sirve debido a que si el usuario busca algo con la palabra porn en Google o cualquier otro buscador también nos bloquee la búsqueda.

Política 2

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *sex*
- Method: any
- Action: deny

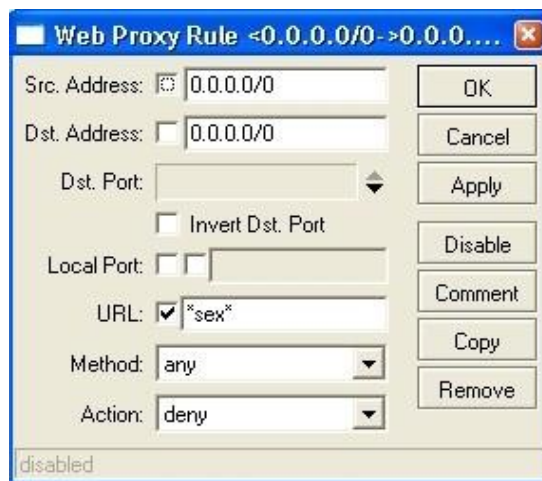


Fig. 4.61: Política 2 para el bloqueo de pornografía
Fuente: <http://www.mikrotik.com/software.html>

Política 3

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *xxx*
- Method: any
- Action: deny

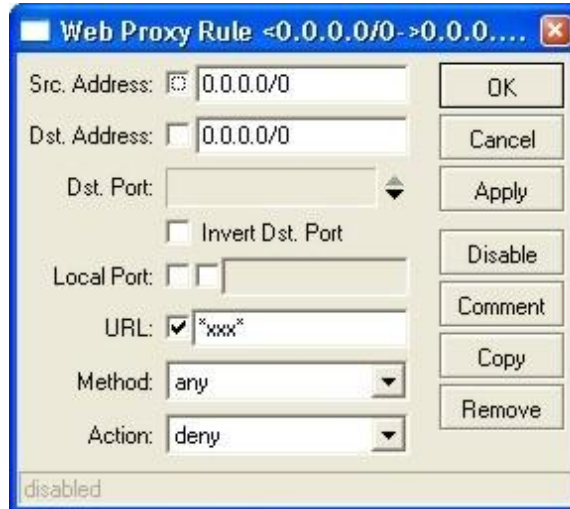


Fig. 4.62: Política 3 para el bloqueo de pornografía
Fuente: <http://www.mikrotik.com/software.html>

4.15.17 Bloqueo de páginas que brinden el servicio de web Messenger

El Bloqueo de las páginas que brindan el servicio de Web Messenger también será bloqueado. Para dicha configuración realizamos los siguientes pasos. Nos dirigimos al menú IP / Web Proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *webmessenger.yahoo.com*
- Method: any
- Action: deny

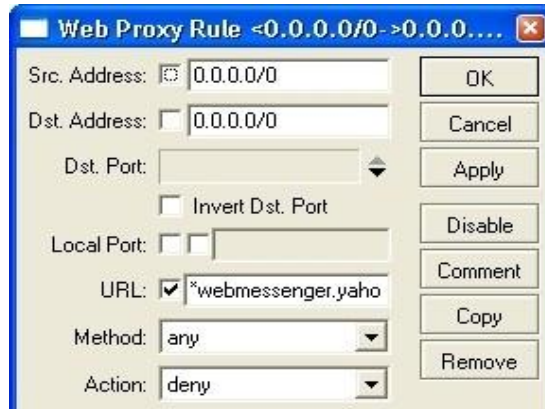


Fig. 4.63: Pestaña de bloqueo del Messenger
Fuente: <http://www.mikrotik.com/software.html>

4.15.18 Bloqueo del Skype a través del Proxy

Para el bloqueo de Skype utilizamos la siguiente política en el Web Proxy para bloquearlo. Para ello realizamos los siguientes pasos. Nos dirigimos al menú IP / Web Proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

BloqueoSkype

- Src.Address:0.0.0.0/0
- Dst. Address:0.0.0.0/0
- URL:*Gateway.skype.*
- Method:any
- Action:deny



Fig. 4.64: Pestaña de bloqueo del Skype
Fuente: <http://www.mikrotik.com/software.html>

4.15.19 Bloqueo de descarga directa de archivos MP3 y AVI

Para el bloqueo de descarga directa de archivos MP3 y avi debemos utilizar la siguiente política en el Web Proxy para bloquearlo. Para ello realizamos los siguientes pasos. Nos dirigimos al menú IP / Web Proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

4.15.19.1 Bloqueo de archivos Mp3

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.mp3
- Method: any
- Action: deny

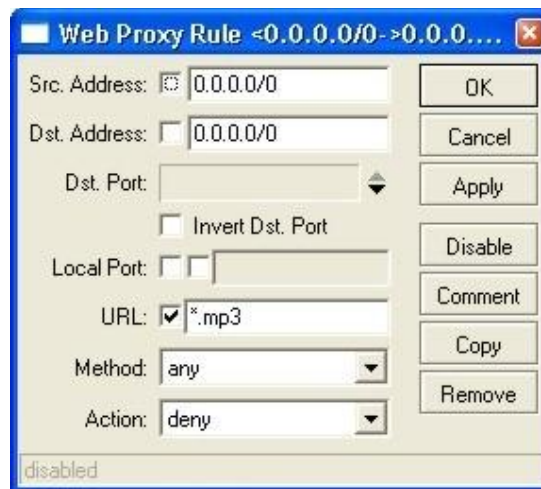


Fig. 4.65: Pestaña de bloqueo del Mp3

Fuente: <http://www.mikrotik.com/software.html>

4.15.19.2 Bloqueo de Archivos Avi

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.avi*
- Method: any
- Action: deny

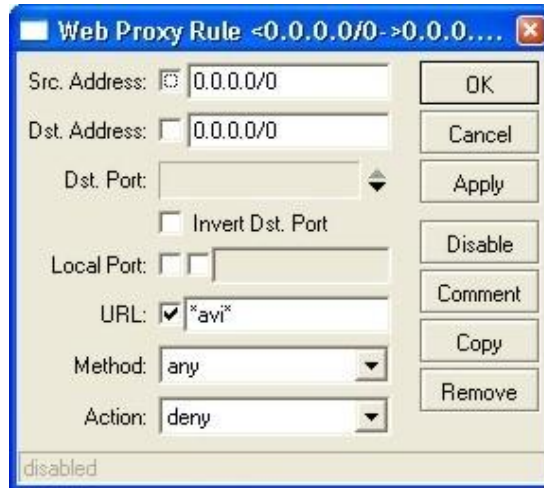


Fig. 4.66: Pestaña de bloqueo de archivos Avi
Fuente: <http://www.mikrotik.com/software.html>

Las políticas del servidor web Proxy se ven de la siguiente manera:

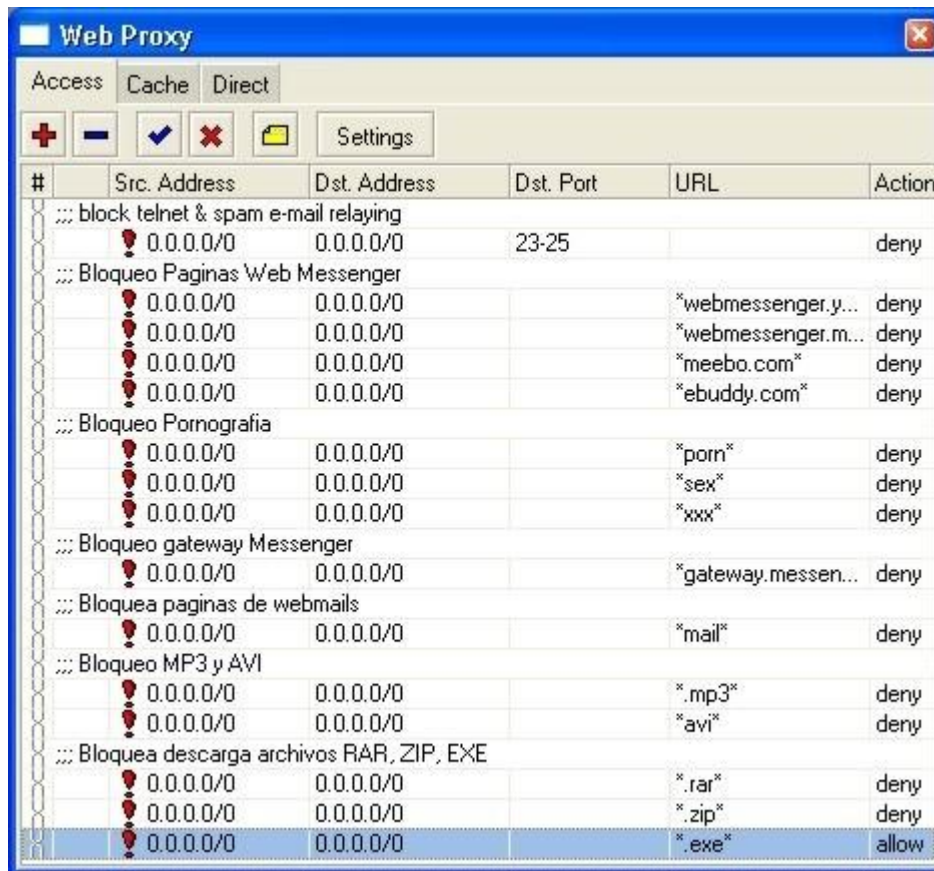


Fig. 4.67: Pestaña de políticas del servidor web Proxy
Fuente: <http://www.mikrotik.com/software.html>

4.15.20 Balanceo de carga

Utilizaremos el balanceo de carga para optimizar el tráfico en la red. Debido a que la sub red Administración Técnica generara grandes volúmenes de tráfico hacia Internet por estar en la parte Central de la Red el balanceo de carga será aplicado a ella.

Para configurar nuestro balanceo debemos realizar los siguientes pasos. Nos dirigimos al menú IP / FIREWALL. De ahí vamos a la pestaña Mangle. Hacemos clic en el icono (+) y comenzamos nuestra configuración de las políticas para el balaceo de cargas. A la nueva ventana la configuramos de la siguiente manera.

PESTAÑA GENERAL:

- Chain: prerouting
- In. Interface Ventas
- Connection State: new

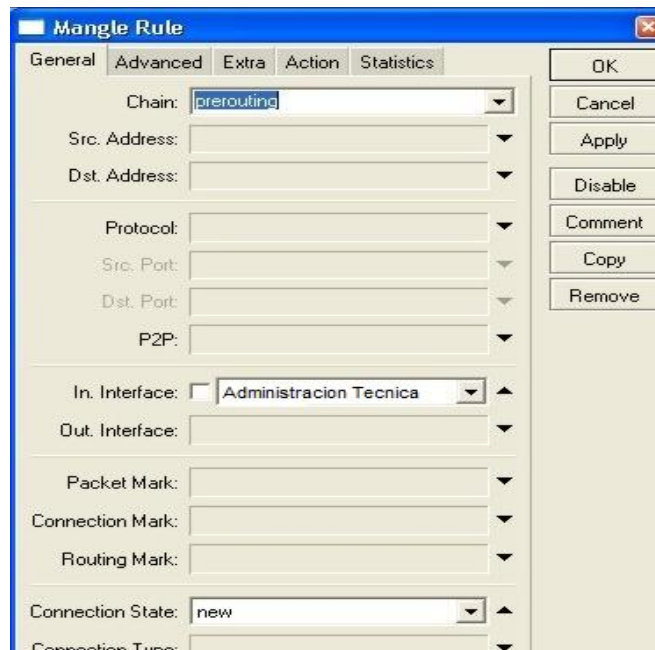


Fig. 4.68: Pestaña general del balanceo de cargas

Fuente: <http://www.mikrotik.com/software.html>

Pestaña Extra:

- Every: 1
- Counter: 1
- Packet:0

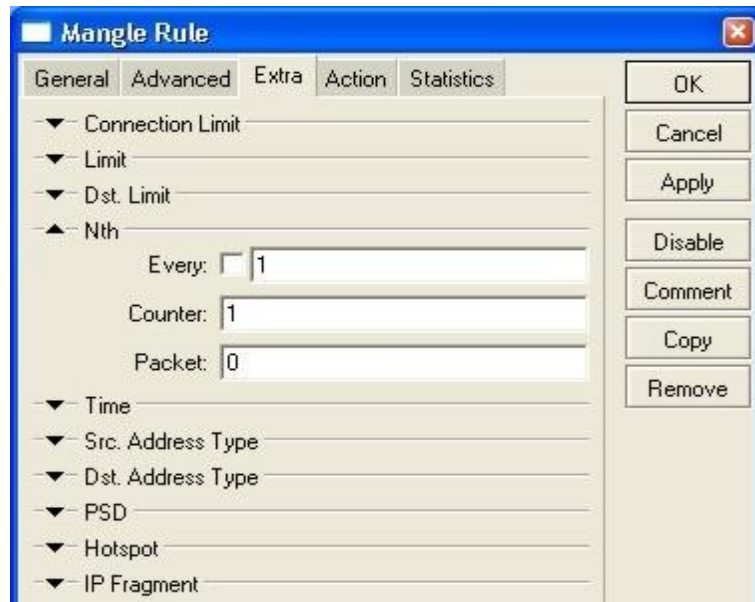


Fig. 4.69: Pestaña extra del balanceo de cargas
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ACTION:

- Action: mark connection
- New Connection Mark: Salida_Agronomía
- Pass thought: seleccionado

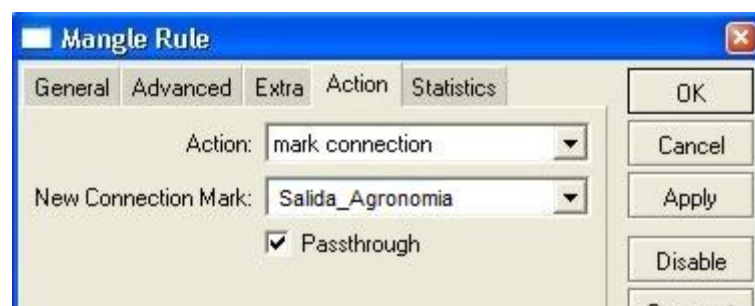


Fig. 4.70: Pestaña action del balanceo de cargas
Fuente: <http://www.mikrotik.com/software.html>

Creamos una segunda política y la configuramos así:

PESTAÑA GENERAL:

- Chain: prerouting
- In.Interface: Laboratorio
- Connection mark: Salida_Agronomía

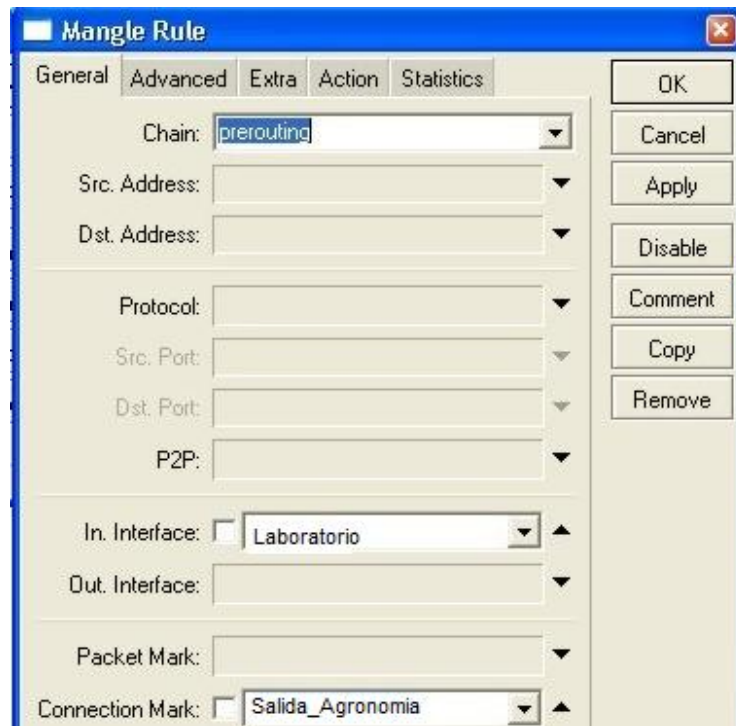


Fig. 4.71: Pestaña general del balanceo de cargas (política 2)
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ACTION:

- Action: mark routing
- New Routing Mark: Marca_Salida_Agronomia

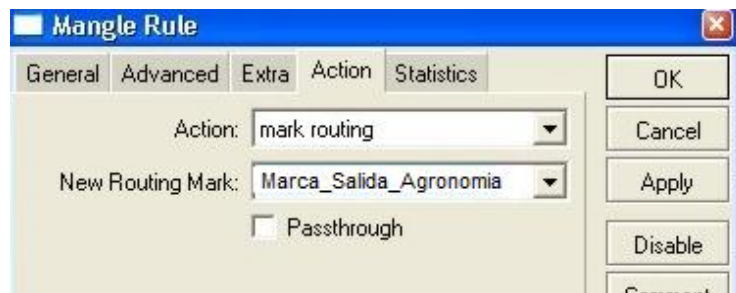


Fig. 4.72: Pestaña action del balanceo de cargas (política 2)
Fuente: <http://www.mikrotik.com/software.html>

Nuestras políticas de Mangle se ven así:

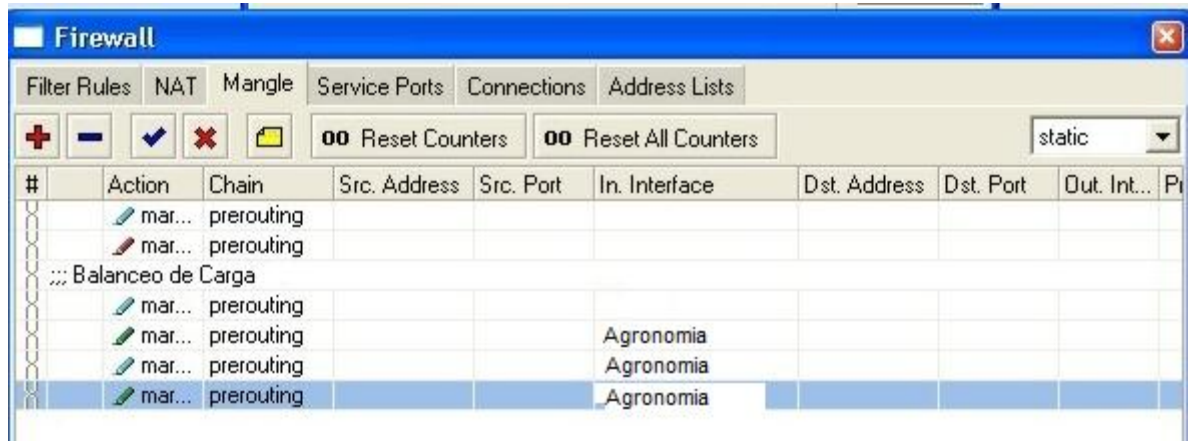


Fig. 4.73: Pestaña de política de mangle del balanceo de cargas
Fuente: <http://www.mikrotik.com/software.html>

Por ultimo para finalizar la configuración debemos realizar unas últimas políticas de ruteo. Para ello entramos en el menú *NEW TERMINAL*. En la terminal que nos aparece escribimos lo siguiente:

```
/ip route add dst-address=0.0.0.0/0 gateway=200.45.3.1 scope=255 t
arget-scope=10 routing-mark=Marca_Salida_Agronomia comment=""
disabled=no

/ip route add dst-address=0.0.0.0/0 gateway=200.45.4.1 scope=255 t
arget-scope=10 routing-mark=Marca_Salida_Agronomia comment=""
disabled=no

/ip route add dst-address=0.0.0.0/0 gateway=200.45.4.1 scope=255 t
arget-scope=10 comment="Gateway por Defecto" disabled=no
```

Fig. 4.74: Política de ruteo del balanceo de cargas
Fuente: <http://www.mikrotik.com/software.html>

4.15.21 Control de ancho de banda

4.15.21.1 Asignación de ancho de banda por sub red

Debido a que muchas veces los usuarios realizan malos usos de los anchos de banda, hemos decidido agregarle políticas al router para poder controlar dicho problema.

Para los distintos grupos de usuarios les asignaremos distinto ancho de banda:

Administración Técnica: _

Subida: _ 1M/Bits

Bajada: _ 3M/Bits

Agronomía: _

Subida: _ 1M/Bits

Bajada: _ 3M/Bits

Laboratorio: _

Subida: _ 1M/Bits

Bajada: _ 3M/Bits

Para el control del ancho de banda debemos ir al menú *QUEUES*. Allí se nos abrirá una ventana de configuración.

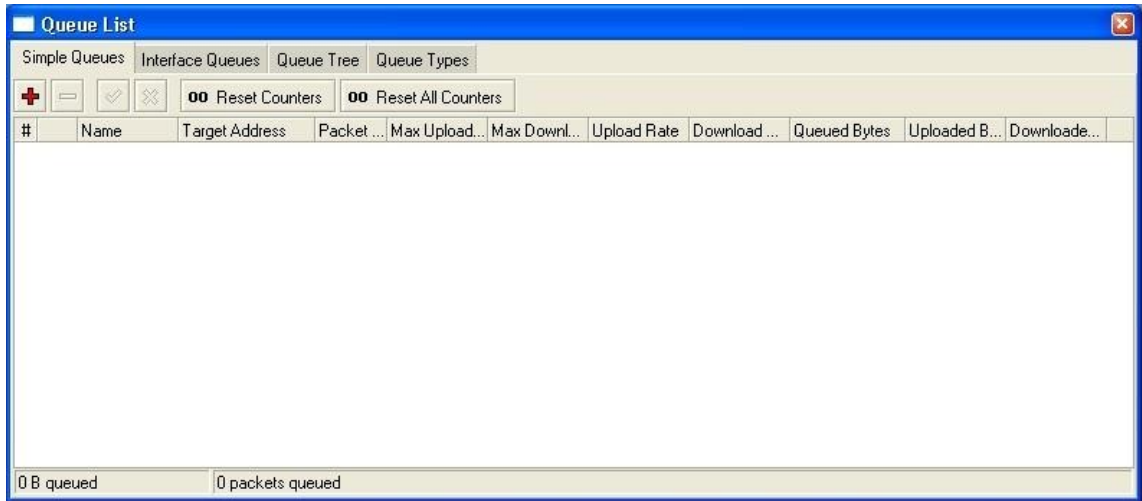


Fig. 4.75: Pestaña de control de ancho de banda
Fuente: <http://www.mikrotik.com/software.html>

Hacemos clic en el icono (+) de la pestaña *Simple Queues*. Se nos abre la nueva para configurar la nueva cola.

Cola Administración:

PESTAÑA GENERAL:

- Name: Queue_Administración
- Target Address:192.168.2.0/24
- Max Limit:1M(upload), 3M (download)

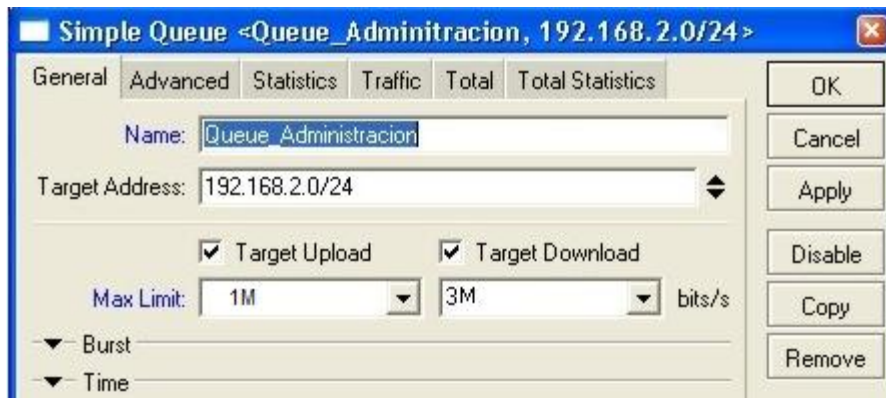
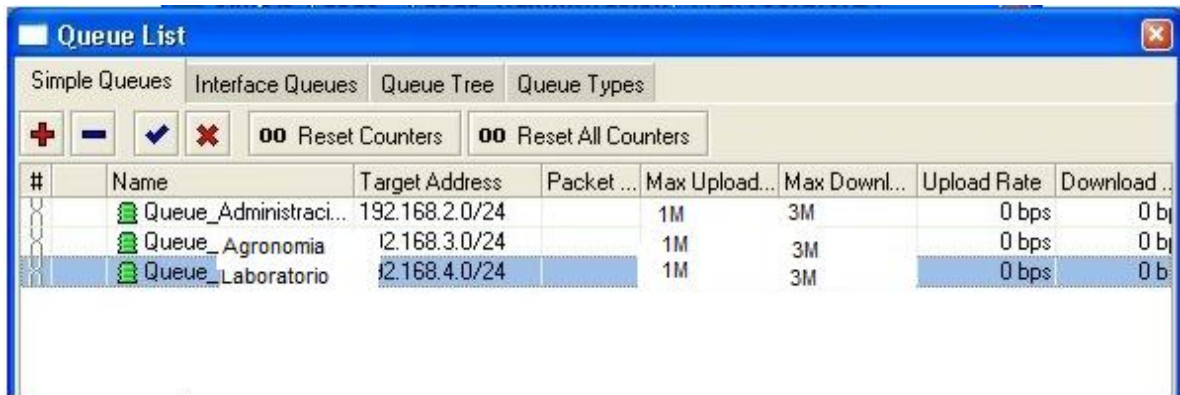


Fig. 4.76: Pestaña general de control de ancho de banda
Fuente: <http://www.mikrotik.com/software.html>

Las colas configuradas se verán de la siguiente manera:



#	Name	Target Address	Packet ...	Max Upload...	Max Downl...	Upload Rate	Download ..
	Queue_Administraci...	192.168.2.0/24		1M	3M	0 bps	0 b
	Queue_Agronomia	12.168.3.0/24		1M	3M	0 bps	0 b
	Queue_Laboratorio	12.168.4.0/24		1M	3M	0 bps	0 b

Fig. 4.77: Pestaña de colas configuradas de ancho de banda

Fuente: <http://www.mikrotik.com/software.html>

4.15.21.2 Liberación del ancho de banda fuera del horario de clases

Debido a que la Facultad Técnica no trabaja las 24hs al día y debido a que existen dos jornadas de estudio, se dispuso la posibilidad de liberar el ancho de banda para la red de Administración Técnica, en un rango horario determinado.

Para ello lo primero que debemos hacer es una nueva cola que la habilitaremos en los horarios de 14:00hs a 18:00hs. Ir al menú *QUEUES* en la pestaña *Queues Tree*, hacemos clic en el icono (+). Se nos abre la ventana de configuración. La configuración de la misma es:

- Name: Queue_in_Global_P2P_libre
- Parent: global-in
- Packet Mark: p2p
- Queue Type: Default
- Priority: 8

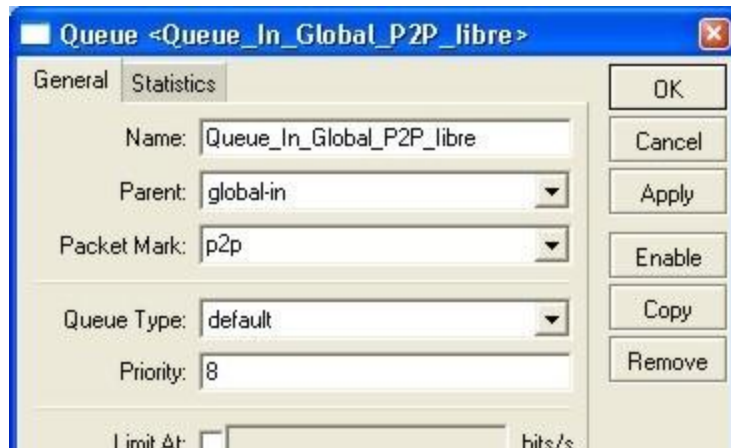


Fig. 4.78: Pestaña de colas del ancho de banda habilitadas entre horarios
Fuente: <http://www.mikrotik.com/software.html>

Antes de hacer clic sobre aceptar, hacemos clic en DISABLE y luego hacemos clic en aceptar. La segunda cola que debemos realizares de la siguiente manera:

- Name: Queue_out_Global_P2P_Libre
- Parent: global-out
- Packet Mark: p2p
- Queue Type: Default
- Priority: 8

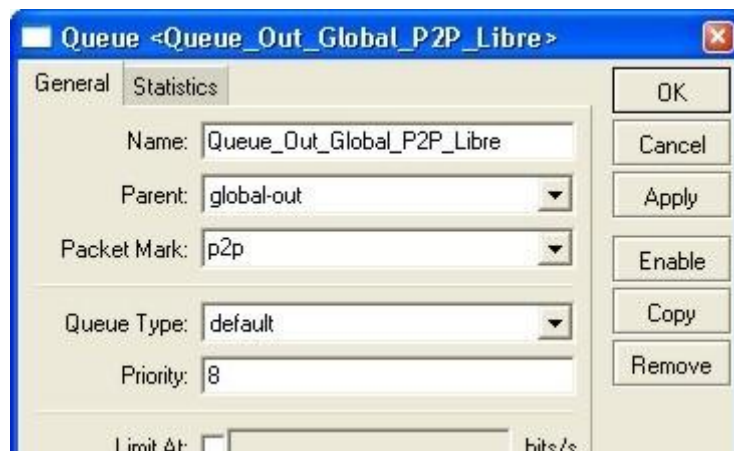


Fig. 4.79: Pestaña de colas del ancho de banda habilitadas entre horarios
Fuente: <http://www.mikrotik.com/software.html>

Antes de hacer clic sobre aceptar hacemos clic en DISABLE y luego hacemos clic en aceptar.

Vamos al menú *SYSTEM / SCRIPTS*. Se nos abre la ventana de administración de scripts. Hacemos clic en el icono (+) y configuramos la ventana nueva con los siguientes datos:

- Name: Bloquea_Bw
- Policy: Write y Read
- Source:

```
/queue tree enable Queue_In_Global_P2P_Limitado
```

```
/queue tree disable Queue_In_Global_P2P_Libre
```

```
/queue tree enable Queue_Out_Global_P2P_Limitado
```

```
/queue tree disable Queue_Out_Global_P2P_Libre
```

Ahora con nuestro segundo script. Vamos al menú *SYSTEM / SCRIPTS*. Se nos abre la ventana de administración de scripts. Hacemos clic en el icono (+) y configuramos la ventana nueva con los siguientes datos:

- Name: Libera_Bw
- Policy: Write y Read
- Source:

```
/queue tree disable Queue_In_Global_P2P_Limitado
```

```
/queue tree enable Queue_In_Global_P2P_Libre
```

```
/queue tree disable Queue_Out_Global_P2P_Limitado
```

```
/queue tree enable Queue_Out_Global_P2P_Libre
```


De la siguiente manera se ve como queda configurada nuestra lista de scripts:

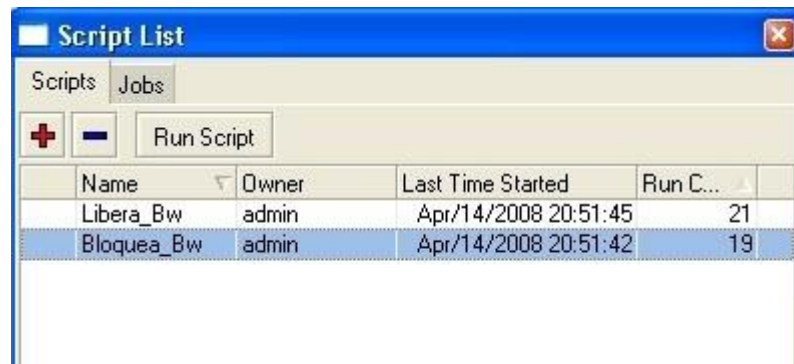


Fig. 4.80: Pestaña de configuración de la lista de scripts

Fuente: <http://www.mikrotik.com/software.html>

Siguiendo con la configuración vamos al menú *SYSTEM / SCHEDULER*. En la ventana nueva que se nos abre, comenzaremos con la configuración de nuestros eventos.

Hacemos clic sobre el botón (+). La configuración del primer evento es:

- Name: Bloquea_Bw
- State Date: Apr/16/2008
- Start Time: 06:00:00
- Interval: 1d00:00:00
- On Event: Bloquea_Bw



Fig. 4.81: Pestaña de configuración del primer evento

Fuente: <http://www.mikrotik.com/software.html>

Luego hacemos clic nuevamente en el icono (+) y creamos nuestro segundo evento, cuyas configuraciones:

- Name: Libera_Bw
- State Date: Apr/16/2008
- Start Time: 20:00:00
- Interval: 1d00:00:00
- On Event: Libera_Bw

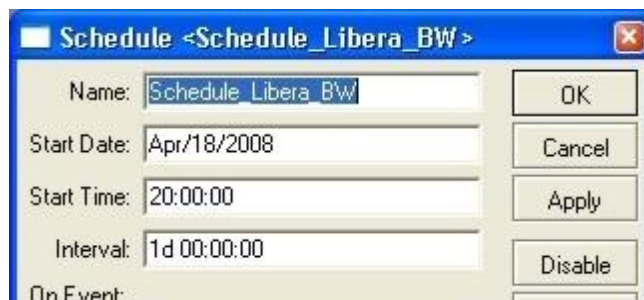


Fig. 4.82: Pestaña de configuración del segundo evento
Fuente: <http://www.mikrotik.com/software.html>

Así es como se ve configurada nuestra lista de scripts:

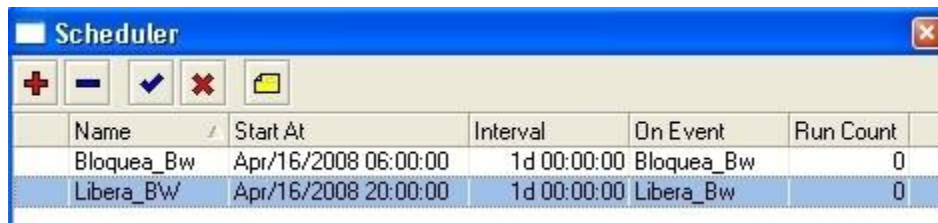


Fig. 4.83: Pestaña de configuración de eventos del ancho de banda
Fuente: <http://www.mikrotik.com/software.html>

4.15.22 Configuración RF y HOTSPOT

Debido a que nuestra área de esparcimiento no está cercana al router principal. Se ha decidido instalar una red Wireless. Para ello se utilizará un router AP Mikrotik RB600.

Logueados al Mikrotik mediante Winbox. Nos dirigimos al menú *INTERFACES*. En la ventana que nos aparece hacemos clic sobre la interface *wlan1* y la habilitamos apretando el botón derecho del Mouse y elegimos la opción *Enable*

	Name	Type	MTU	Tx Rate	Rx Rate	Tx Pac...	Rx Pac...
R	ether1	Ethernet	1500	5.7 kbps	1457 bps	4	2
R	ether2	Ethernet	1500	0 bps	0 bps	0	0
R	ether3	Ethernet	1500	0 bps	0 bps	0	0
	wlan1	Wireless (Atheros AR5413)	1500	0 bps	0 bps	0	0

Fig. 4.84: Pestaña de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA GENERAL

A continuación le hacemos doble clic a la interface y comenzamos la configuración de la misma. La pestaña General se configura de la siguiente manera:

- Name: wlan1
- MTU: 1500
- MAC Address: 00:0C:42:05:A9:A3
- Arp: enabled



Fig. 4.85: Pestaña general de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA WIRELESS:

- ✓ Radio Name: AP Facultad Tecnica
- ✓ Mode: AP bridge
- ✓ SSID: Wifi_Tecnica
- ✓ Band: 2.4Ghz
- ✓ Frequency: 2.412mhz
- ✓ Security Profile: default
- ✓ Frequency Mode: manual Txpower
- ✓ County: Uzbekistan
- ✓ DFS Mode: none
- ✓ Proprietary Extensions: post-2.9.25
- ✓ Default Authenticate: Seleccionado
- ✓ Default forward: Seleccionado

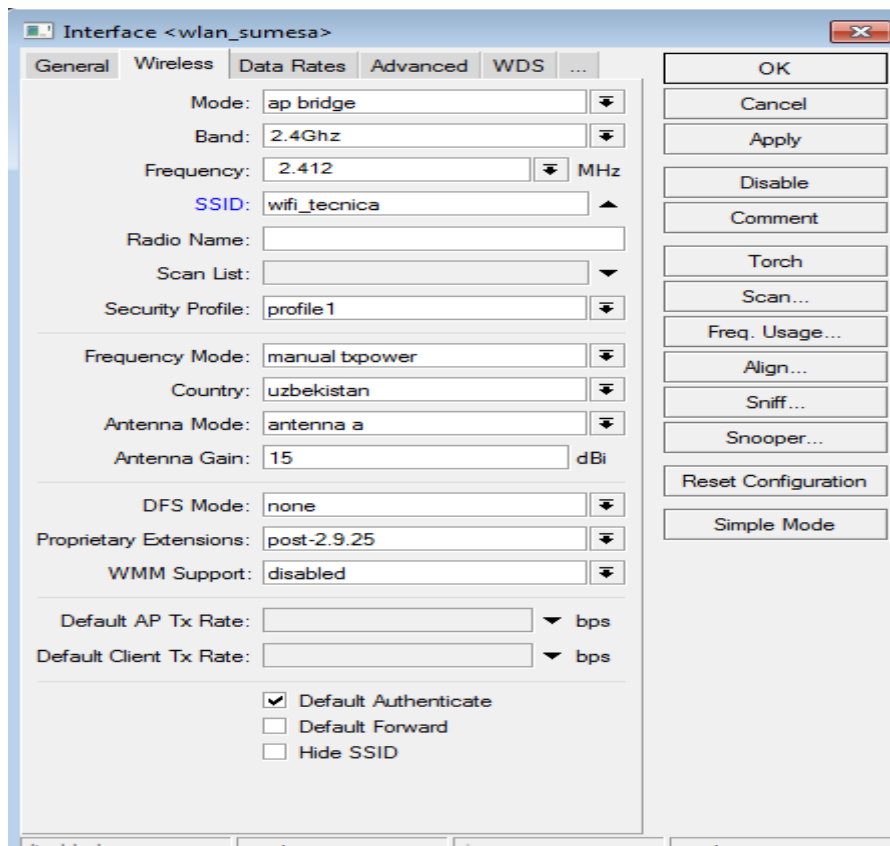


Fig. 4.86: Pestaña wireless de configuración de RF y HOTSPOT

Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA DATA RATES:

No se le modificara la configuración Standard.

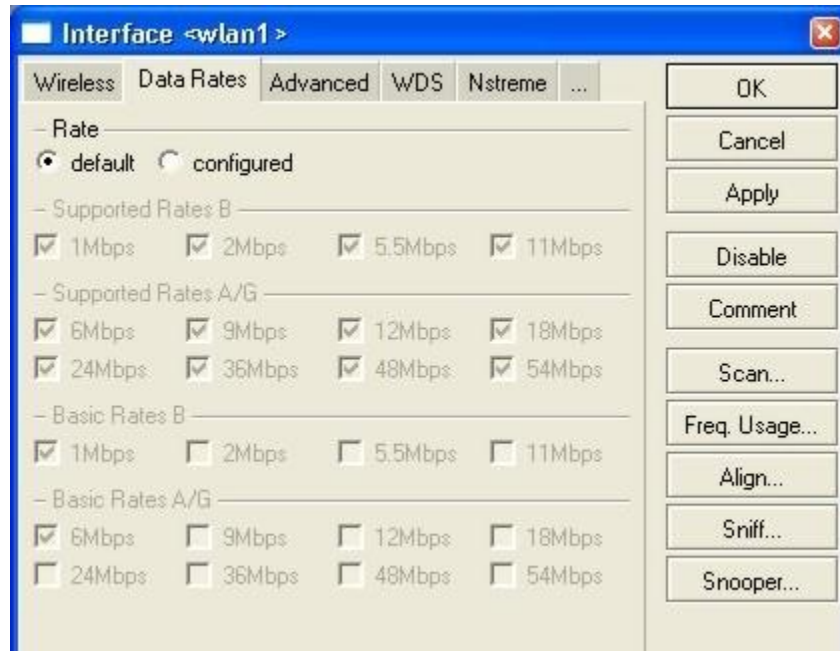


Fig. 4.87: Pestaña data rates de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ADVANCED:

- Max Station Count: 2007
- Act Timeout: dynamic
- Periodic Calibration: Default
- Calibration level: 00:01:00
- Antenna mode: antenna a
- Preamble mode: both
- Disconnect time out: 00:00:03
- On Fail Retry Time: 100

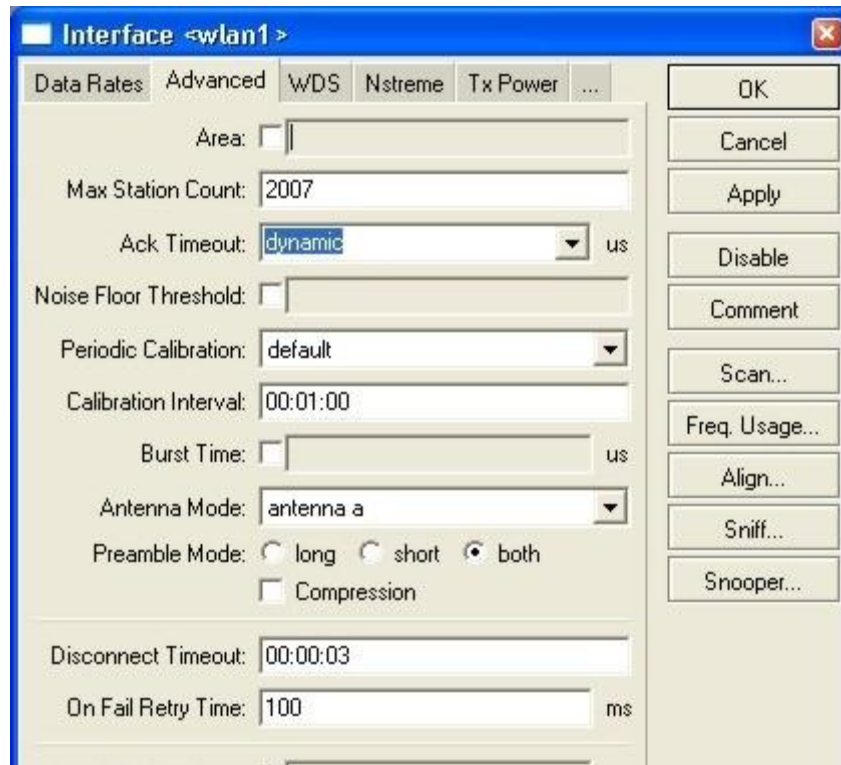


Fig. 4.88: Pestaña advanced de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA WDS:

- ✓ WDS Mode: Disable
- ✓ WDS default Bridge: none
- ✓ WDS Default Cost: 100
- ✓ WDS Cost Range: 50-100



Fig. 4.89: Pestaña WDS de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA NSTREME:

- Enable Ntreme: Deseleccionado
- Enable Polling: Seleccionado
- Framers Policy: none
- Framers Limit: 3200

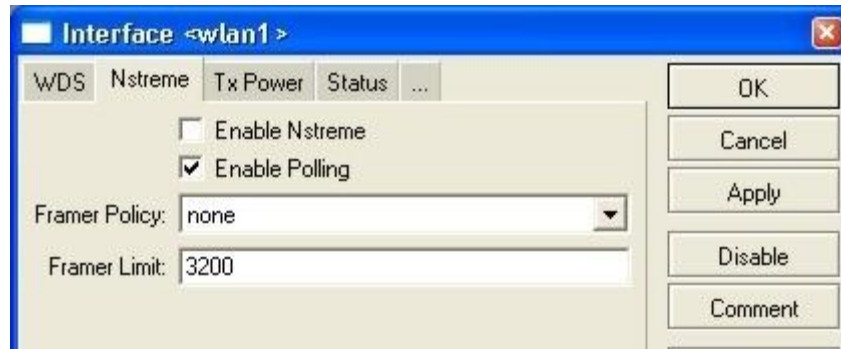


Fig. 4.90: Pestaña NSTREME de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA TX POWER:

- TX Power Mode: default

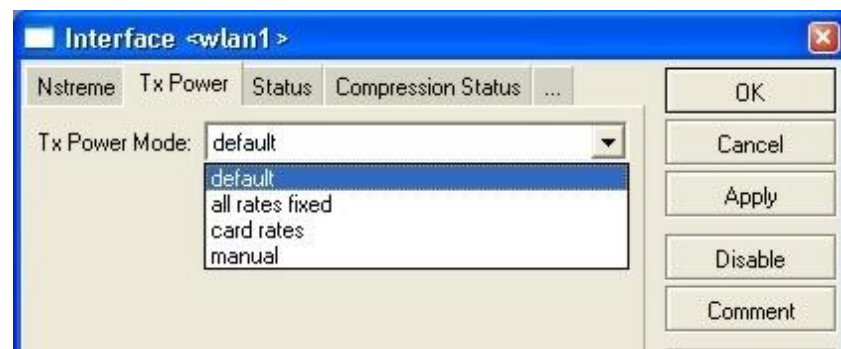


Fig. 4.91: Pestaña TX power de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA STATUS:

Esta pestaña nos muestra el Status de la interface Wireless.

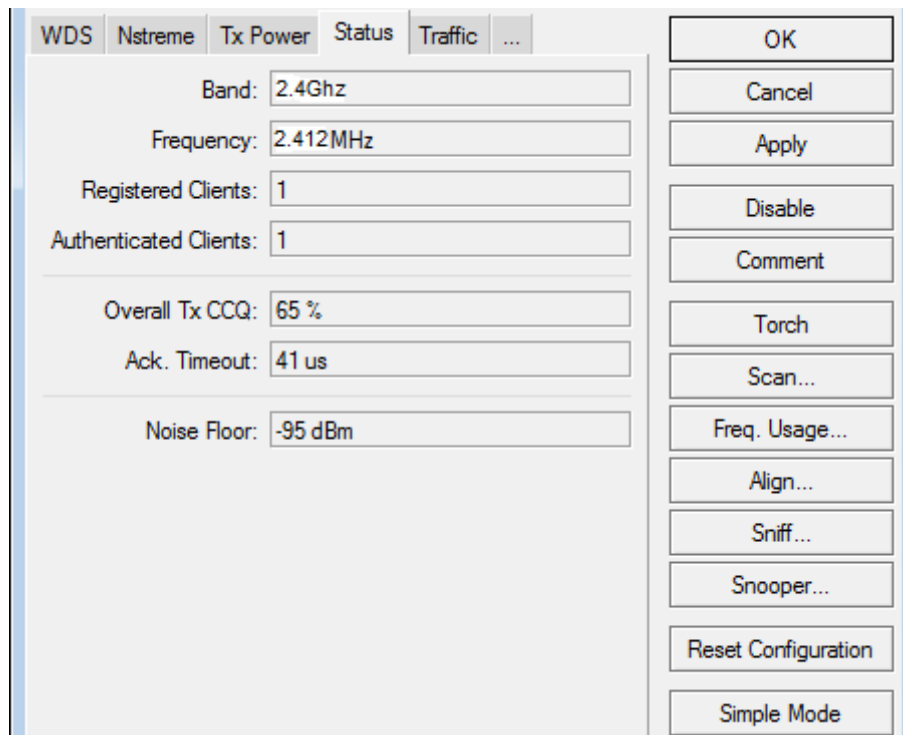


Fig. 4.92: Pestaña status de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA COMPRESSION STATUS:

Esta pestaña nos muestra el estado de la compresión de datos.

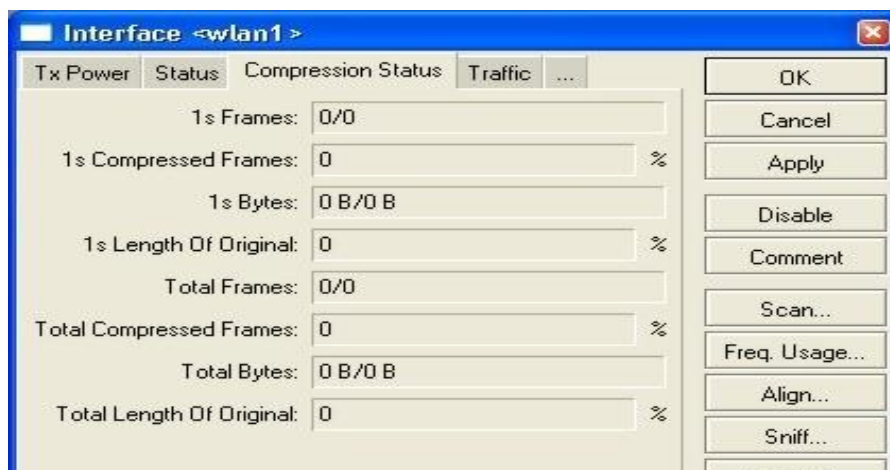


Fig. 4.93: Pestaña compresión status de configuración de RF y HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA TRAFFIC:

Nos muestra el tráfico actual de la interface en paquetes enviados y recibidos al igual que bits por segundo

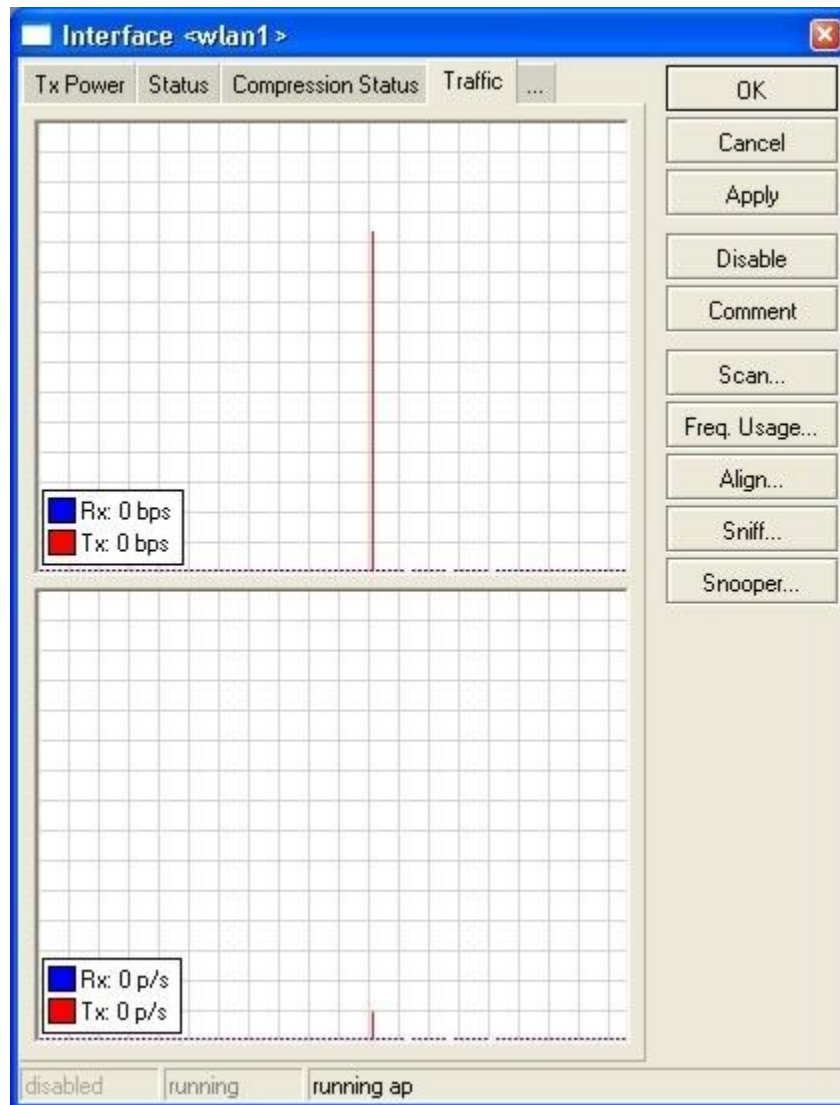


Fig. 4.94: Pestaña traffic de configuración de RF y HOTSPOT

Fuente: <http://www.mikrotik.com/software.html>

A continuación deberemos configurar nuestro HotSpot. Para ello nos dirigimos al menú *IP / Hotspot*. En la nueva ventana dentro de la pestaña Servers, hacemos clic sobre el botón *SETUP*.

En la ventana que nos aparece la configuramos de la siguiente manera.

- HotSpot interface: wlan1



Fig. 4.95: Pestaña de configuración de HOTSPOT
Fuente: <http://www.mikrotik.com/software.html>

En la ventana siguiente elegimos la dirección de ip para la interface de hotspot.
La configuración es:

- Local Address of Network 192.168.10.1/24
- Masquerade Network: Seleccionado



Fig. 4.96: Pestaña de configuración de ip (HOTSPOT)
Fuente: <http://www.mikrotik.com/software.html>

A continuación le asignamos el pool de ip que nos interesa que dicha interface nos brinde a los clientes. La configuración es:

- Address Pool of Network: 192.168.10.2-192.168.10.254



Fig. 4.97: Pestaña de asignación de pool de ip
Fuente: <http://www.mikrotik.com/software.html>

Luego no le seleccionamos ningún certificado SSL



Fig. 4.98: Pestaña de selección de certificado
Fuente: <http://www.mikrotik.com/software.html>

Siguiendo nos pide la dirección del servidor SMTP de nuestra red locales:

IP Address of SMTP Server: 192.168.1.1

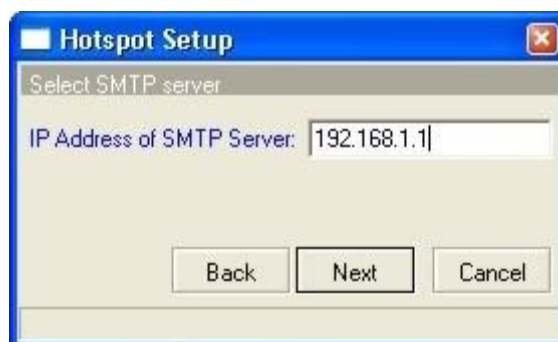


Fig. 4.99: Pestaña de asignación del servidor SMTP
Fuente: <http://www.mikrotik.com/software.html>

Luego le asignamos los DNS correspondientes.

DNS Servers: 192.168.0.3
200.45.191.35

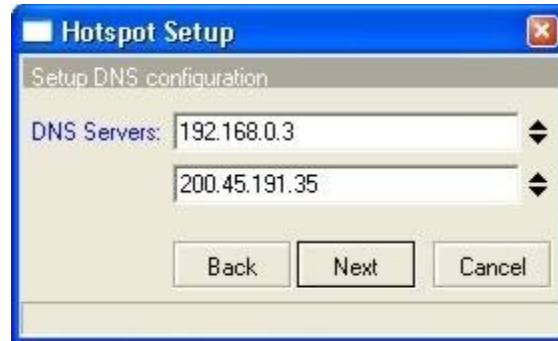


Fig. 4.100: Pestaña de asignación de los DNS
Fuente: <http://www.mikrotik.com/software.html>

Seguimos con el nombre de nuestro servidor DNS el cual es:

✓ DNS Name: hotspot.ucsg.edu.ec



Fig. 4.101: Pestaña de comprobación de los DNS
Fuente: <http://www.mikrotik.com/software.html>

Finalizando creamos nuestro usuario administrador. Nuestro hotspot configurado se ve de la siguiente manera.

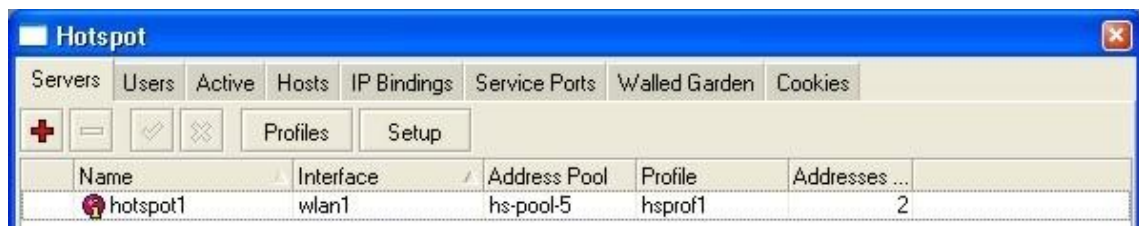


Fig. 4.102: Pestaña de usuario
Fuente: <http://www.mikrotik.com/software.html>

Le hacemos doble clic al hotspot1 para configurar sus parámetros. La configuración de los mismos son:

- Name: hotspot
- Interface: wlan1
- Hs-pool-5
- Profile hspof1
- Idle Time out: 00:05:00
- Addresses per Mac: 2



Fig. 4.103: Pestaña de configuración de parámetros
Fuente: <http://www.mikrotik.com/software.html>

Luego dentro de la pestaña Servers hacemos clic en profiles. Y luego editamos la configuración del profile *hspof1*. La configuración del mismo es:

PESTAÑA GENERAL:

- Name: hspof1
- Hotspot Address: 192.168.10.1
- DNS Name: Hotspot.ucsg.edu.ec
- HTML Directory: hotspot
- SMTP: 192.168.1.1



Fig. 4.104: Pestaña general de configuración del profile hspof1
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA LOGIN:

- HTTP CHAP y Cookie: Seleccionado
- MAC, HTTP PAP, HTTPS y Trial: deseleccionado.
- HTTP Cookie Lifetime: 01:00:00



Fig. 4.105: Pestaña login del profile hspof1
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA RADIUS:

- Use RADIUS: (seleccionado)
- Default Domain: 192.168.1.3
- NAS PORT Type 19 (Wireless-802.11)



Fig. 4.106: Pestaña radius del profile hsprof1
Fuente: <http://www.mikrotik.com/software.html>

Luego hacemos clic sobre la pestaña Users hacemos clic en el botón Profile y generamos uno. La configuración del mismo es:

Name Profile_Hotspot

- Address Pool:hs-pool-5
- Idle Timeout. None
- Keekalive Timeout: 00:02:00
- Shared Users: 1
- Rate limit: 128k/256k



Fig. 4.107: Pestaña generación de users
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA ADVERTISE:

- ✓ Advertise: deseleccionado



Fig. 4.108: Pestaña de desactivación de advertencias
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA SCRIPT:

No se genera ningún script y queda configurada por default.



Fig. 4.109: Pestaña Script del hotspot
Fuente: <http://www.mikrotik.com/software.html>

Finalmente generaremos un perfil de seguridad para las conexiones Wireless. Para ello debemos ir al menú *WIRELESS*, luego hacemos clic en la pestaña *Security Profiles*. Y creamos un profile nuevo haciendo clic en el icono (+).

PESTAÑA GENERAL:

- ✓ Name: Facultadtecnica-Secure
- ✓ Mode: dynamic keys
- ✓ WPA PSK, WPA2 PSK: Seleccionados
- ✓ Unicast ciphers
 - Tkip: Seleccionado
 - Aes ccm: Seleccionado
- ✓ GroupCiphers
 - Tkip: Seleccionado
 - Aes ccm: Seleccionado
- ✓ WPA Pre-Shared Key: tecnica

- ✓ WPA2 Preshared Key: ucsg_tecnica
- ✓ RADIUS MAC Authentication (deseleccionado)



Fig. 4.110: Pestaña general de seguridad del Profilewireless
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA EAP:

- EAP Methods:
- TLS Mode: no certificate
- TLS certificate: none

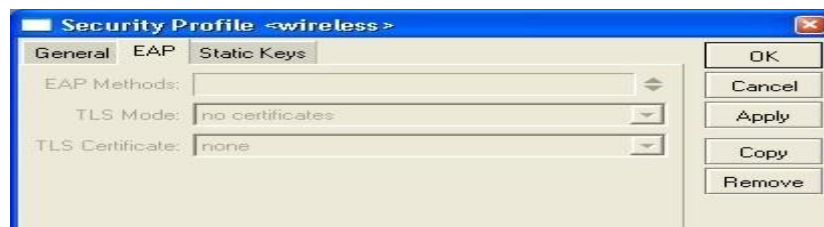


Fig. 4.111: Pestaña EAPde seguridad del Profilewireless
Fuente: <http://www.mikrotik.com/software.html>

PESTAÑA STATIC KEYS:

No utilizaremos llaves estáticas



Fig. 4.112: Pestaña static keys del security Profile
Fuente: <http://www.mikrotik.com/software.html>

A continuación debemos asignarle este perfil de seguridad a nuestra interface wlan1. Para ello nos dirigimos al menú *WIRELESS*. Dentro de la pestaña *Interfaces*. Le hacemos doble clic a nuestra interface wlan1 modificamos el siguiente valor.

✓ Security Profile: Facultad técnica-Secure

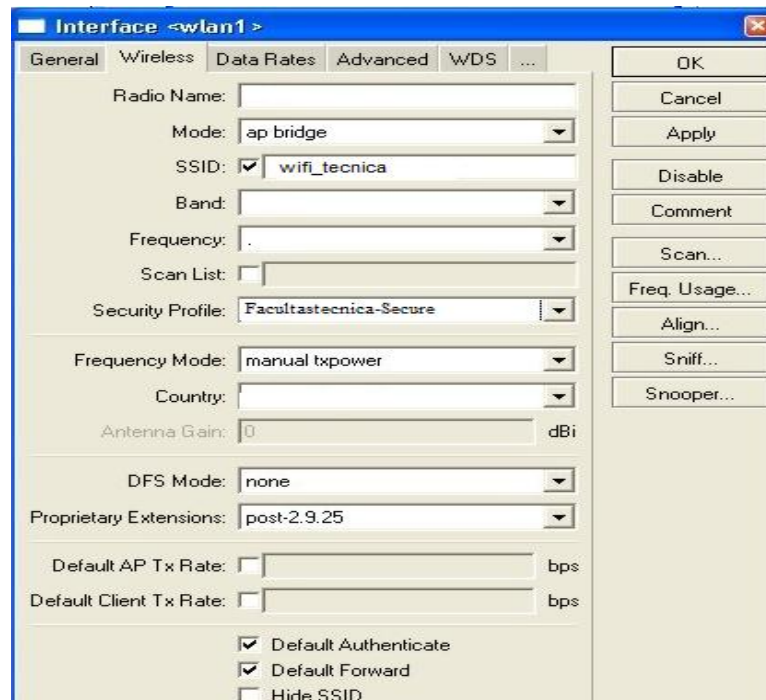


Fig. 4.113: Pestaña de asignación de perfil de seguridad al wlan 1
Fuente: <http://www.mikrotik.com/software.html>

Finalmente Vamos al menú *RADIUS*. En la ventana nueva que se nos abre le hacemos clic en el icono (+). La nueva ventana la configuramos de la siguiente manera:

- ✓ Ppp, hotspot, login, wireless, telephony, dhcp: Seleccionados
- ✓ Address: 192.168.0.3

Secret: Radius

- Authentication port: 1812
- Accounting: 1813
- Time out: 600

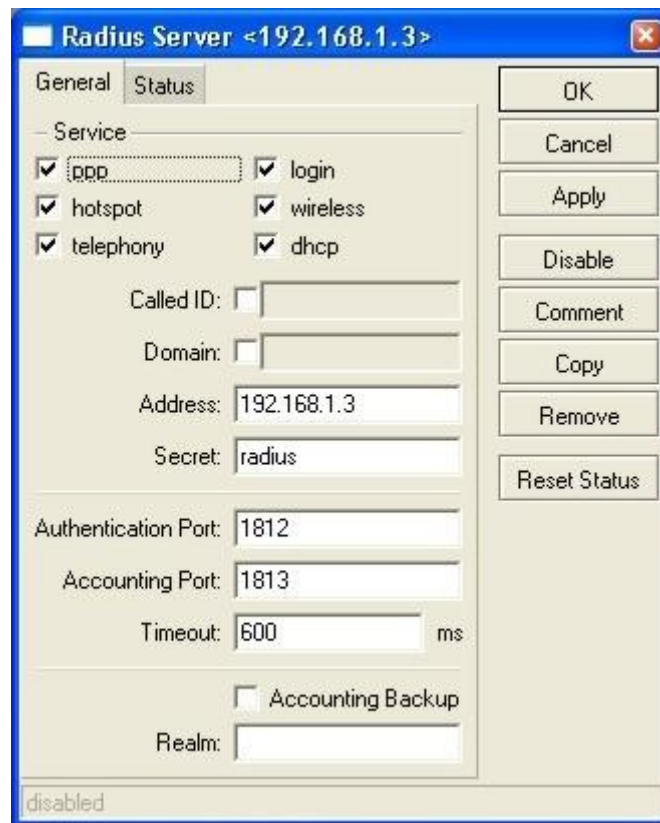


Fig. 4.114: Pestaña final de configuración
Fuente: <http://www.mikrotik.com/software.html>

4.15.23 Sistema HOTSPOT

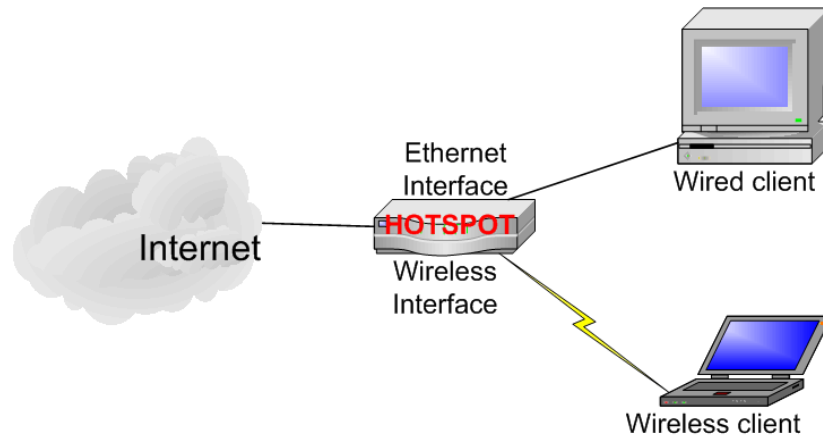


Fig. 4.115: Sistema HOTSPOT (Ethernet Interface)

Fuente: <http://www.mikrotik.com/software.html>

- Usuario trata de abrir una página Web
- El ruteador checa si el usuario esta autenticado por el sistema hotspot, si no es así lo redirige a la página de autenticación.
- El usuario provee la información de login y password para tener acceso

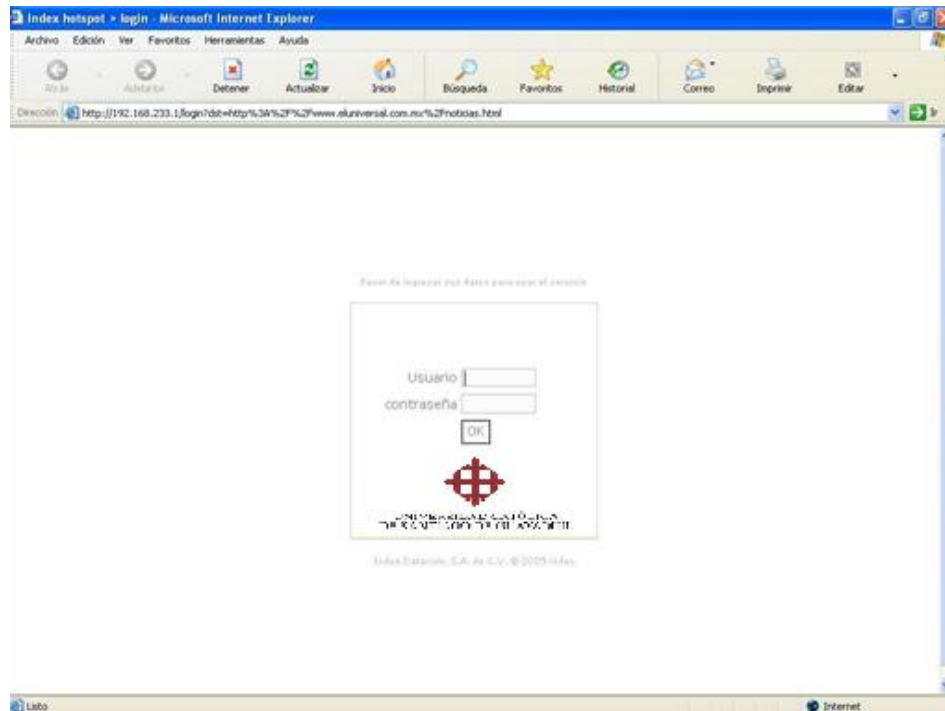


Fig. 4.116: Ventana prueba de ingreso al sistema Hotspot

Fuente: <http://www.mikrotik.com/software.html>

- Si la información de login y password fue correcta, el ruteador autentifica al cliente en el sistema HotSpot y abre la página solicitada así como una ventana de status popup
- Este usuario puede acceder al Internet



Fig. 4.117: Ventana de acceso a internet
Fuente: <http://www.mikrotik.com/software.html>

4.15.23.1 Funcionalidades de Hotspot

- Autenticación de usuarios
- Contabilización por usuario por tiempo, datos transferidos/recibidos
- Limitación de datos
 - Por velocidad
 - Por cantidad
- Limitación por tiempo
- Soporte de RADIUS
- Zona de navegación libre

4.15.23.2 Uso de Hotspot

- HotSpot es una tecnología de autenticación que puede ser usada para proveer acceso público a Internet:
 - Aeropuertos, barcos, hoteles, Universidades, oficinas, salones de conferencia, hospitales
 - EN redes alámbricas o inalámbricas
 - Tarifa por autenticar o acceso libre

4.15.23.3 Método de registro en Hotspot

- Direcciones habilitadas:
 - Al usuario se le asigna una dirección IP, puede ser por el método de DHCP
 - HotSpot autentica al usuario
 - HotSpot permite al tráfico del usuario pasar a través del firewall

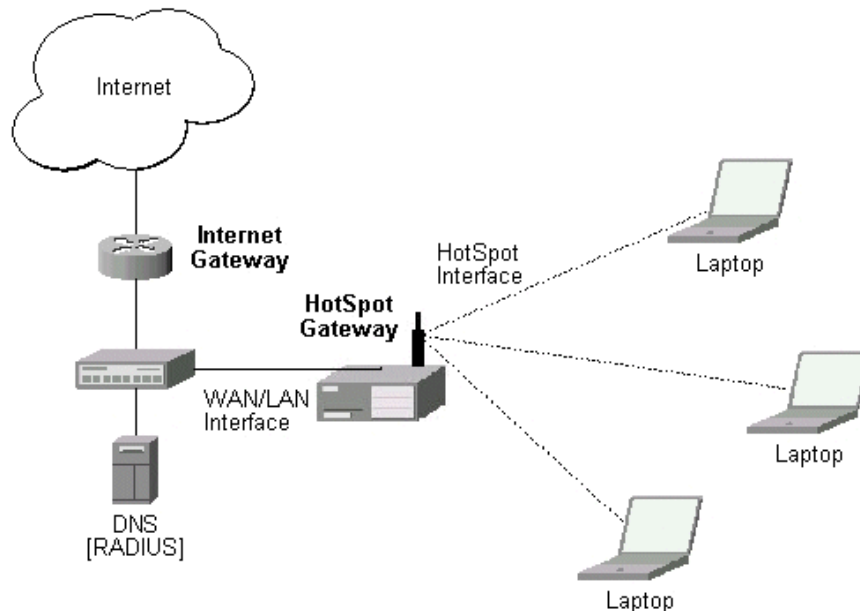


Fig. 4.118: Acceso a internet por medio de la interface Hotspot
Fuente: <http://www.mikrotik.com/software.html>

4.15.24 Antenas

Se puede adaptar a los enrutadores Mikrotik Antenas Externas sectorial para este caso se eligió el modelo de antena Hyperlink L-com Modelo HG2414SP-090 que opera a una frecuencia de 2.4GHz puesto que tiene un gran ángulo de radiación lo que lo hace ideal para cubrir los sectores críticos.

Estas antenas están fabricadas para exteriores donde se conecta a través de un cable coaxial, un protector de línea y un pigtail

Dentro de esta marca y dado que las antenas siempre se instalan a la intemperie, se eligen los modelos específicos para exteriores. A partir de aquí la elección de la antena depende de la ganancia necesaria de la misma para poder realizar el enlace y de la frecuencia en que se va a trabajar.



Fig. 4.119: Antenas externas sectorial

Fuente: <http://www.l-com.com/wireless-antenna-24-49-58-ghz-dual-feed-dual-band-90-degree-sector-panel-antenna>[31].

Frequency	2400 - 2500 MHz
Gain	14 dBi
Polarization	Vertical
Horizontal Beam Width	90°
Vertical Beam Width	12.5° to 15°
Impedance	50 Ohm
VSWR	< 1.5:1 avg.
Front to Back Ratio	> 23 dB
Max. Input Power	300 Watts
Lightning Protection	DC Ground
Weight	4.4 lbs. (2 kg)
Dimensions	20 x 7 x 3.5 inch (500 x 180 x 90 mm)
Radome Material	UV-inhibited Plastic
Mounting	2 inch (50 mm) dia. mast max.
Operating Temperature	-40° C to 85° C (-40° F to 185° F)
Rated Wind	>130 MPH (210 Km/h)
Compliant	ANATEL® Brazil and RoHS

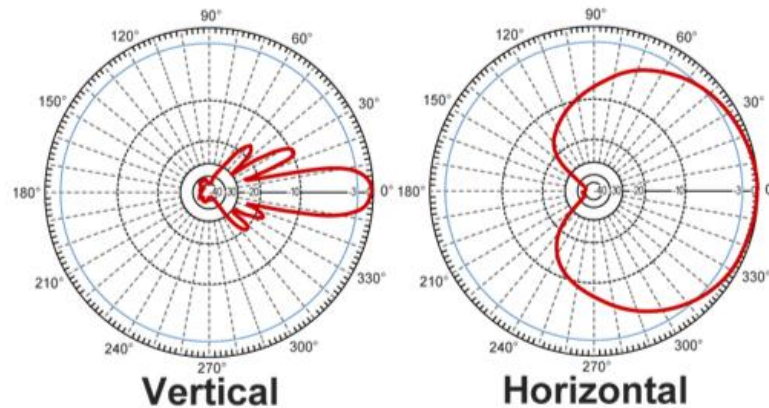


Fig. 4.120: Antenas externas vertical y horizontal
Fuente: <http://www.l-com.com/wireless-antenna-24-49-58-ghz-dual-feed-dual-band-90-degree-sector-panel-antenna>[31].

4.16 Presupuesto y estimación de costos

A continuación se detalla el presupuesto económico y la estimación de los equipos a ocuparse, así como también la mano de Obra de la Instalación, cabe indicar que estos precios son reales y están sujetos a cambios sin previo aviso.

Item	Descripción	Cantidad	Valor Unitario	Total
	Licencia MikroTikRouterOSLevel 6	1	\$ 1.000,00	\$ 1.000,00
HG2458-14P-090	2.4/ 4.9-5.8 GHz Dual Feed Dual Band 90 Degree Sector Panel Antenna	6	\$ 400,00	\$ 2.400,00
RB600	AP Mikrotik RB600	3	\$ 700,00	\$ 2.100,00
	Cable Diamond RG8 / N-Male	6	\$ 50,00	\$ 300,00
	Caja de cable Utp Cat6 marca NEXXT	1	\$ 240,00	\$ 240,00
	Funda De 10 Conectores Rj-45 Blindados Categoría 6 Qpcom	2	\$ 15,00	\$ 30,00
	Caja de Interperie	3	\$ 150,00	\$ 450,00
	CPU Servidor Linux	1	\$ 200,00	\$ 200,00
	Mastil de 6mts	1	\$ 200,00	\$ 200,00
	Mano de Obra: _Instalación de Antenas, Cableado estructurado, Configuración de MikrotikRouterOs, Configuración de Hospot Básico.	1	\$ 1.700,00	\$ 1.700,00
	Soporte Técnico , Mantenimiento Preventivo y Correctivo por 1 Año	1	\$ 1.000,00	\$ 1.000,00
		Subtotal		\$ 9.620,00
		Iva:(12%)		\$ 1.154,40
		Total		\$ 10.774,40

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Del análisis de los resultados se concluye que se debería re-estructurar la red informática del Wifi de la Universidad Católica de Santiago de Guayaquil, debido a que es ineficiente el aprovechamiento al máximo de esta herramienta.

En esta propuesta de Tesis se ha dado esta alternativa para que la Facultad Técnica para el Desarrollo tenga su propia Red de WiFi; independiente de las que existen en la comunidad Universitaria.

- Para la implementación de la red se utilizará el sistema operativo Mikrotik RouterOS basado en Linux. El mismo convierte un PC Standard en un router de alto rendimiento.
- Se define la configuración de los interfaces asignando nombres, direcciones de IP a las mismas y definición de las Vlan.
- Se configuró el servidor de DHCP para cada una de las sub redes. En el cual se definieron los pools de ip para cada una. También la asignación de direcciones de IP fijas a partir de direcciones MAC de los servidores.
- Se configuró un servidor NTP para sincronizar la hora dentro de toda la red.

- También se configuró un equipo cliente NTP para sincronizar la hora de la red con otros servidores de tiempo.

- Se configuró un servidor de Web Proxy para optimizar la utilización de los recursos hacia Internet. En el mismo se configuró políticas de bloqueo de tráfico hacia ciertas páginas al igual que el bloqueo de descarga de ciertos archivos.

- Se realizó un balanceo de carga entre todos los 3 Aps para la optimización del recurso.

- Se realizaron políticas de control de ancho de banda para los clientes P2P.

- Se implementó políticas de firewall como bloqueo de p2p, bloqueo del Msn Messenger, redireccionamiento de puertos y bloqueo de paquetes no deseados.

- Se configuró un Hot Spot en la cual los usuarios se autentican mediante un servidorRadius.

5.2 Recomendaciones

- Es importante mencionar que el proyecto únicamente refleja el análisis y diseño de la red, se realiza este estudio en base a las Tecnologías que existen actualmente en toda la comunidad Universitaria; sería óptimo que se llegue a plasmar todo el estudio realizado para demostrar de manera tangible que si es posible brindar este servicio.
- Incentivar a los estudiantes de la Universidad para que desarrollen investigaciones de campo y de implementación de proyectos existentes sobre todo en este tipo ya que favorecen el ámbito social y humano que a la larga se transforma en el valor agregado que nuestro país necesita.
- De llegar a implementar este proyecto sería imprescindible crear políticas de seguridad de acceso ya que la señal está destinada únicamente para la Facultad Técnica para el Desarrollo, más no para las Facultades aledañas, por lo tanto además de las seguridades que puede tener Mesh y todos sus componentes es necesario proveer seguridades adicionales que permitan controlar el acceso al canal.

BIBLIOGRAFÍA

- Arias, M. (Octubre de 2011). *Implementacion red con mikrotik*. Obtenido de www.slideshare.net:
<http://www.slideshare.net/ariasmarco1979/implementacion-red-con-mikrotik>
- Chiluisa, M., & Ulcuango, J. (Marzo de 2009). *Diseño de una red inalambrica Mesh (WMNs) para las parroquias rurales del canton Latacunga de la provincia de Cotopaxi*. Obtenido de Dspace EPN:
<http://www.readbag.com/dspace-epn-ec-bitstream-15000-9228-1-t11160>
- Pica, G., Roche, E., & Di Rienzo, V. (Diciembre de 2013 de 2008). *Implementación de una red para la empresa Royal Tech*. Obtenido de <http://www.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>
- STALLINGS, WILLIAM. (2002) “*Comunicaciones y Redes DE Computadoras*”, Sexta Edición, Prentice Hall, España.
- GRUPO FIRETIDE. (2008) “*Designing and Deploying Mesh Network Planning and Installing your Wireless Mesh*”
- SCOTT KEAGY (2001) “*Integración de redes de voz y datos*”, Editorial: Cisco Press, Madrid-España
- CREATIVE COMMONS (2008) “*Redes Inalámbricas en los Países en Desarrollo*”, Tercera Edición
- ACUÑA M. y RONCALLO, R. (2007)“*Redes Inalámbricas Malladas Metropolitanas*”: Colombia
- HIDROBO j. (2009) ”*Redes y servicios de Telecomunicaciones*”, Segunda Edición, Editorial: Paraninfo, Madrid-España
- CARBALLAR JOSÉ, “*Wi-Fi Como construir una red inalámbrica*”, Segunda Edición, España 2004
- D. GARCIA, J. PARADELLS, (2005) “*Improving Performance of a Real Ad-Hoc Network by Tuning OLSR Parameters*”, Colombia
- Comer Douglas E., (2008). *Redes de Computadoras, internet e interredes*, México: Prentice Hall.

Gilbert Held, (2007), *Wireless Mesh Networks*, Taylor & Francis Group (144 pag).

Izaskun Pellejero, Fernando Andreu y Amaia Lesta, (2006). *Fundamentos y aplicaciones de seguridad en redes Wlan*. Barcelona:España: Marcombo S.A.

OTRAS REFERENCIAS

- [1].Mikrotik. (2006), "MikrotikRouterOS y Referencia Manual", 1era Edición, Estados unidos.
- [2].http://www.it46.se/courses/wireless/materials/es/13_RedesModule/13_es_redes_mesh_presentacion_v01.pdf
- [3].http://www.adminso.es/index.php/PFM_RedesModule
- [4].<http://sistemas.itlp.edu.mx/tutoriales/comadmva/t24.htm>
- [5].<http://es.scribd.com/doc/16020012/23/Logueo-al-Mikrotik>
- [6].<http://www.mikrotik.com/>
- [7].<http://www.mikrotik.com/software.html>
- [8].<http://www.l-com.com/wireless-antenna-24-49-58-ghz-dual-feed-dual-band-90-degree-sector-panel-antenna>