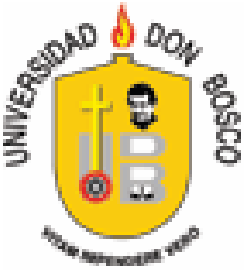
UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA

ESCUELA DE COMPUTACION



IMPLEMENTACION DE UNA INTRANET SEGURA PARA LA EMPRESA LEXINCORP S.A. DE C.V. CON TECNOLOGIA INALAMBRICA Y SEGURIDAD DE ACCESOS

Trabajo de graduación para optar al grado de

Ingeniero en Ciencias de la Computación

ASESOR:

ING. GILBERTO ANTONIO LARA SOSA

PRESENTADO POR:

CARLOS ALBERTO MEJÍA AGUILAR

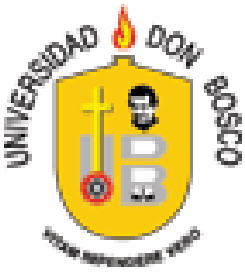
RAÚL AMILCAR MOLINA LÓPEZ

EDUARDO EULISES ORELLANA MULATO

CIUDADELA DON BOSCO, SEPTIEMBRE DE 2006

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA



RECTOR:

ING. FEDERICO MIGUEL HUGUET RIVERA

VICERRECTOR:

PADRE VICTOR BERMÚDEZ

SECRETARIO GENERAL:

LIC. MARIO RAFAEL OLMOS

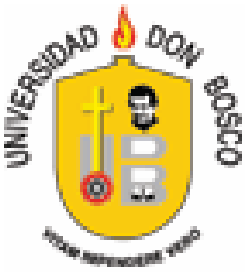
DECANO DE LA FACULTAD DE INGENIERIA:

ING. ERNESTO GODOFREDO GIRÓN

CIUDADELA DON BOSCO, SEPTIEMBRE 2006

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA



SUBCOMITE EVALUADOR DEL TRABAJO DE GRADUACIÓN

"IMPLEMENTACION DE UNA INTRANET SEGURA PARA LA EMPRESA LEXINCORP S.A. DE C.V. CON TECNOLOGIA INALAMBRICA Y SEGURIDAD DE ACCESOS"

ING. JULIO RIVERA
JURADO

ING. EDGARDO ROMERO
JURADO

ING. CARLOS LÓPEZ
JURADO

ING. GILBERTO ANTONIO LARA
ASESOR

ING. WALTER OVIDIO SÁNCHEZ
TUTOR

AGRADECIMIENTOS

La culminación de este trabajo esta dedicada a:

- A **Dios**, porque sin él no somos nada. Porque es mi padre creador que me cuida, me acompaña, me llena de bendiciones. Ha estado a mi lado durante toda mi vida, y seguirá estándolo.

- A mis **padres**, Bilha Eunice de Orellana y Eduardo Antonio Orellana por creer en mí, por cuidarme, por estar siempre apoyándome. Ellos me guiaron, me aconsejaron que si quiero tener éxito debo luchar duro para lograrlo. Por formarme, por hacerme una persona de bien.

- A mi **hermano**, Alejandro Eduardo Orellana por su cariño, por su apoyo en todo momento. Porque me daba fuerzas para continuar hasta la meta.

- A mis **abuelos**, Zoila América Mulato y Benjamín Hernández Porque siempre supo que lo lograría, confió en mí, me impulso a conseguir mis sueños.

- A mi **prima**, Zoila Hernández, por su ayuda, por su esfuerzo para que yo siguierá adelante.

- A la **familia Orantes Moreno** porque siempre creyeron que lo lograría. A Lourdes Orantes por su ayuda, apoyo, consejos, me ayudaron a llegar al objetivo, a soñar alto, a seguir aprendiendo.

- A los jóvenes de **eje Cristóbal**, por su preocupación, sus ánimos, por sus oraciones, por formarme en la fe cristiana.

- A mis compañeros de tesis, Amilcar Molina y Carlos Mejía por su ayuda, por su esfuerzo y esmero para terminar este trabajo de graduación.

- A mis **amigos**, Gonzalo Ernesto, Mario Calles, Fatima Orantes, Lourdes Orantes, Estelita Orantes, Victor, Juan Carlos Oseguera, Juan Carlos Chevez, Amilcar, Richard, Luzzy por su cariño, por su confianza, por su apoyo, porque estuvieron allí cuando los necesite.

- Al **asesor**, Ing. Gilberto Lara por su tiempo invertido, por sus consejos, su colaboración para que este trabajo fuera terminado.

- A los **jurados**, Ing. Julio Rivera, Ing. Edgardo Romero, Ing. Carlos López por su valiosa colaboración, consejos para este trabajo.

- Al **tutor**, Ing. Walter Sánchez por sus esfuerzos en los tramites durante todo el trabajo de graduación.

Eduardo Eulises Orellana Mulato

AGRADECIMIENTOS

A **Dios** por brindarme sabiduría y paciencia , mis **padres** Mariano Mejia y Amanda Aguilar por haberme apoyado incondicionalmente en mi formación académica desde mi infancia .

A mis **hermanos** :Noemí, Mario, Gerbert, Wilmer, Melvin y Yesenia , por haber estado siempre al expectativa de mi formación académica.

A tío Gregorio Aguilar, por ser generoso en recibirme en su hogar cuando inicie mi carrera universitaria, a mis primos por aceptarme como un miembro mas de su familia.

A mi novia Reina Landaverde, por comprenderme en mi proceso académico y apoyo emocional….

A mis compañeros de Universidad :Ricardo , Darwing, Miguel , Mario, Evelio ,Alfredo por crear siempre una motivación mutua y continua en todas circunstancias académicas.

A mis compañeros de Tesis : Amilcar Molina y Eduardo Orellana , por su apoyo equitativo el la búsqueda de un mismo objetivo académico.

A nuestro **comité evaluador** por la orientación importante y valiosa para finalizar nuestro trabajo de Graduación.

Carlos Alberto Mejia Aguilar.

AGRADECIMIENTOS

En primer lugar le doy gracias a **Dios** por darme la fuerza y la voluntad de terminar la universidad, a mis **padres** Amilcar Molina y Ana Luz de Molina ya que por ellos tengo todo en esta vida y sin ellos no seria la persona que soy, a mi **esposa Mayela de Molina** que amo tanto por darme esas palabras de aliento en los momentos difíciles, a **mis hijos** Amilcar Emanuel y Cristina Nicole que son mi tesoro más preciado los cuales son la razón de querer seguir adelante y superarme cada día más.

A todos aquellos que me ayudaron de alguna forma hacer esto posible, a mi **suegra** Ena López (C.G) y a Carlos Carcach, a mis **hermanos** Emerson Alejandro, Fernando José y Ana Gabriela, a mis amigos, compañeros de trabajo, gracias por todo.

"Mas buscad primeramente el reino de Dios y su justicia, y todas estas cosas os serán añadidas"

(Mateo 6:33)

Raúl Amilcar Molina López

INDICE

INTRODUCCIÓN 16
CAPITULO I. GENERALIDADES 18
1.1. OBJETIVOS 18
1.1.1. GENERAL 18
1.1.2 ESPECÍFICOS 18
1.2. ALCANCES 19
1.3. LIMITACIONES 20
1.4. DELIMITACIONES 20

CAPITULO II.FACTIBILIDAD 21
2.1.FACTIBILIDAD .OPERACIONAL 21
2.2.FACTIBILIDAD TÉCNICA. 23
2.3.FACTIBILIDAD ECONÓMICA 25

CAPITULO III.METODOLOGÍA DE LA INVESTIGACIÓN 27
3.1. INVESTIGACIÓN PRELIMINAR 27
3.2. ANÁLISIS DE LA INFORMACIÓN REQUISITOS DE HARDWARE Y SOFTWARE 28
3.2.1. HARDWARE. 28
3.2.2. SOFTWARE 28
3.3. DISEÑO 28
3.4. DEMOSTRACIÓN DE LA INTRANET INALAMBRICA 29
3.4.1. INSTALACIÓN DEL EQUIPO 29
3.4.2. CONFIGURACIÓN. 30
3.4.3. PRUEBAS Y CORRECCIONES DE ERRORES 30
3.5. DOCUMENTACIÓN 30

CAPITULO IV. SITUACION ACTUAL DE LA EMPRESA 32
4.1 DESCRIPCIÓN DE LA RED ACTUAL Y SU ENTORNO. 32
4.2 . CUADRO DE MAQUINAS ACTUALES POR DEPARTAMENTO Y SUS ESPECIFICACIONES. 33

4.3. ESQUEMA ACTUAL DE RED. 34

CAPITULO V. MARCO TEÓRICO 35
5.1. MARCO HISTÓRICO. 35
5.1.1. REFERENCIAS HISTÓRICAS 35
5.1.2. CAPAS DEL MODELO OSI. 36
5.2. MARCO CONCEPTUAL 39
5.2.1. REDES INALÁMBRICAS 39
5.2.1.1. DEFINICIÓN DE WLAN 41
5.2.1.2. CONFIGURACIONES DE WLAN 42
5.2.1.2.1. PEER TO PEER O AD-HOC 42
5.2.1.2.2. INFRAESTRUCTURA 43
5.2.1.2.3. INTERCONEXIÓN DE REDES 46
5.2.1.2.4. PUNTOS DE EXTENSIÓN 46
5.2.1.2.5. TOPOLOGÍA DE INFRAESTRUCTURA EXTENDIDA 47
5.2.1.2.6. TOPOLOGÍA DE ESTACIÓN BASE CON ACCESO A INTERNET POR LLAMADA 47
5.2.1.2.7. TOPOLOGÍA DE ESTACIÓN BASE CON ACCESO A INTERNET POR DSL O CABLE 48
5.2.1.2.8. TOPOLOGÍA DE REPETIDOR INALÁMBRICO 48
5.2.1.2.9. TOPOLOGÍA DE SISTEMA REDUNDANTE 49
5.2.1.2.10. TOPOLOGÍA DE EDIFICIO A EDIFICIO 49
5.2.1.3. MEDIOS INALÁMBRICOS 50
5.2.1.3.1. INFRAROJOS 50
5.2.1.3.1.1. CAPA FÍSICA EN INFRAROJOS 51
5.2.1.3.1.2. CAPA DE ENLACE EN INFRAROJOS 53
5.2.1.3.1.3. CAPA DE RED EN INFRAROJOS 53
5.2.1.3.1.4. CAPA DE TRANSPORTE EN INFRAROJOS 53
5.2.1.3.1.5. TOPOLOGÍAS PARA INFRAROJOS 54
5.2.1.3.2. RADIOFRECUENCIA 56

5.2.1.3.2.1. FACTORES QUE INFLUYEN EN LA COMUNICACIÓN POR RADIOFRECUENCIA 57
5.2.1.3.2.2. TECNOLOGÍAS DE TRANSMISIÓN PARA RADIOFRECUENCIA..... 59
5.2.1.3.3. MICROONDAS TERRESTRES 64
5.2.1.4. NIVEL DE ACCESO AL MEDIO DEL 802.11 66
5.2.1.4.1. DESCRIPCION FUNCIONAL DEL MAC. 66
5.2.1.4.1.1. FUNCIÓN DE COORDINACIÓN DISTRIBUIDA 67
5.2.1.4.1.1.1. PROTOCOLO DE ACCESO AL MEDIO CSMA/CA Y MACA 68
5.2.1.4.1.1.2. ESPACIADO ENTRE TRAMAS 70
5.2.1.4.1.1.3. CONOCIMIENTO DEL MEDIO.. 71
5.2.1.4.1.2. FUNCIÓN DE COORDINACIÓN PUNTUAL 72
5.2.1.4.2. FORMATO DE LAS TRAMAS MAC. 74
5.2.1.4.3. DIRECCIONAMIENTO EN MODO INFRAESTRUCTURA. 76
5.2.1.4.4. SERVICIOS DEL SISTEMA DE DISTRIBUCIÓN ASOCIACIÓN. 77
5.2.1.4.4.1. ALGORITMO DE ASOCIACIÓN ACTIVA..... 78
5.2.1.4.5. SUBNIVEL DE GESTIÓN MAC 79
5.2.1.4.5.1. SINCRONIZACIÓN 79
5.2.1.4.5.2. GESTIÓN DE POTENCIA..... 80
5.2.1.5. ESTÁNDARES INALÁMBRICOS 81
5.2.1.5.1. 802.11 LEGACY 81
5.2.1.5.2. 802.11a. 82
5.2.1.5.3 802.11b. 82
5.2.1.5.4. 802.11g. 83
5.2.1.5.5. 802.11n. 83
5.2.1.5.6. 802.11e. 84
5.2.1.5.7. 802.11SUPER G. 84
5.2.1.5.8. TECNOLOGÍA DE COMUNICACIONES WPAN..... 84

5.2.1.5.8.1 NIVELES DE ENERGÍA Y COBERTURA 85
5.2.1.5.8.2 CONTROL DEL MEDIO 86
5.2.1.5.8.3 TIEMPO DE VIDA DE LA RED 87
5.2.1.5.8.4 BLUETOOTH WPAN..... 88
5.2.1.5.8.5 TOPOLOGÍAS DE CONECTIVIDAD PARA BLUETOOTH WPAN..... 89
5.2.1.5.9. IEEE 802.16 WMAN. 90
5.2.1.5.10. IEEE 802.20..... 93
5.2.1.5.11. HIPERLAN/2. 94
5.2.1.5.11.1. ANTECEDENTES 94
5.2.1.5.11.2 LA RED HIPERLAN/2 95
5.2.1.5.11.3 CARACTERÍSTICAS DE HIPERLAN/2..... 96
5.2.1.5.11.4 ARQUITECTURA DEL PROTOCOLO Y LAS CAPAS..... 99
5.2.1.5.11.5 ASIGNACIÓN DEL ESPECTRO Y COBERTURA DEL ÁREA..... 101
5.2.1.6. DISPOSITIVOS PARA UNA RED INALÁMBRICA 101
5.2.1.6.1. DISPOSITIVOS BÁSICOS INALÁMBRICOS..... 101
5.2.1.6.2. TIPOS DE ANTENAS. 102
5.2.1.7. EL PROBLEMA DE LA SEGURIDAD INALÁMBRICA 109
5.2.1.8. TIPOS DE ATAQUES EN REDES INALÁMBRICAS..... 112
5.2.1.8.1. MÉTODOS DE ATAQUE..... 112
5.2.1.8.1.1. ATAQUES PASIVOS 112
5.2.1.8.1.2. ATAQUES ACTIVOS 113
5.2.1.9. PROTOCOLOS DE SEGURIDAD EN REDES INALÁMBRICAS 114
5.2.1.9.1. WEP(WIRED EQUIVALENT PROTOCOL)..... 115
5.2.1.9.2. OSA(OPEN SYSTEM AUTHENTICATION)..... 116
5.2.1.9.3. ACL(ACCESS LIST CONTROL)..... 117
5.2.1.9.4. CNAC(CLOSED NETWORK ACCESS CONTROL). 117
5.2.1.9.5. WPA(WI-FI PROTECTED ACCESS)..... 117
5.2.1.9.5.1 CARACTERISTICAS DE WAP..... 118

5.2.1.9.5.2 MEJORAS DE WPA RESPECTO A WEP... 118
5.2.1.9.5.3 MODOS DE FUNCIONAMIENTO DE WPA. 119
5.2.1.9.6. 802.11I. ... 119
5.2.1.9.7. WPA2(802.11I). ... 120
5.2.1.9.8. MÉTODOS DE AUTENTICACIÓN DE EAP. ... 120
5.2.1.9.8.1 EAP - TLS. ... 121
5.2.1.9.8.2 PEAP. ... 121
5.2.1.9.8.3 TTLS. ... 121
5.2.1.9.8.4 LEAP. ... 121
5.2.1.10. MÉTODOS DE ENRUTAMIENTO INALÁMBRICO ... 122
5.2.1.10.1. DESCUBRIMIENTO DE RUTAS. ... 123
5.2.1.10.2. MANTENIMIENTO DE RUTAS. ... 125
5.2.1.10.3. DEFINICIÓN DE RED AD-HOC. ... 126
5.2.2. TIPOS DE REDES ... 127
5.2.2.1. REDES DE AREA DE ALMACENAMIENTO (SAN) ... 127
5.2.2.2. REDE PRIVADA VIRTUAL (VPN) ... 128
5.2.2.3. REDES INTERNAS Y EXTERNAS ... 129
5.2.3. TECNOLOGÍAS DE CÓDIGO ABIERTO. ... 130
5.2.4. PLATAFORMA WEB. ... 131
5.2.5. GNU. ... 132
5.2.6. ¿QUÉ ES LA LICENCIA GPL?. ... 133
5.2.7. SERVIDOR APACHE. ... 134
5.2.7.1. ¿QUÉ ES APACHE?. ... 134
5.2.7.2. ¿DONDÉ OBTENERLO?. ... 134
5.2.7.3. ARQUITECTURA DEL SERVIDOR APACHE. ... 134
5.3. MARCO EXPERIMENTAL. ... 135
5.3.1. CASO PRÁCTICO. ... 135
5.3.2. APLICACIONES DE LAS WLAN. ... 137
5.3.2.1. BENEFICIOS ... 137
5.3.2.2. ESCENARIO 1 ... 138
5.3.2.3. ESCENARIO 2 ... 139
5.3.2.4. COORPORACIONES ... 140

5.3.2.5. EDUCACIÓN 140
5.3.2.6. FINANZAS 140
5.3.2.7. CUIDADO DE LA SALUD 140
5.3.2.8. RESTAURANTES Y VENTA AL POR MENOR 140
5.3.2.9. MANUFACTURACIÓN 141
5.3.2.10. ALMACENES 141

CAPITULO VI. IMPLEMENTACION DEL SISTEMA 142
6.1. IMPLEMENTACIÓN DEL SERVIDOR 143
6.1.1. SISTEMA OPERATIVO 143
6.1.2. SERVICIOS DEL SERVIDOR 144
6.1.3. INTERFACES DE RED 146
6.1.4. SEGURIDAD EN EL SERVIDOR 147
6.1.4.1. CONFIGURACIONES BÁSICAS EN LA INSTALACIÓN 147
6.1.4.2. INSTALACIÓN DE SERVICIOS Y PUERTOS 147
6.1.4.3. ESCANEO DE PUERTOS 148
6.1.4.4. IDENTIFICACIÓN DE SERVICIOS 149
6.1.4.5. PROTECCIÓN DE SERVICIOS INSTALADOS(MURO DE FUEGO) 150
6.2. IMPLEMENTACIÓN DE RED INALÁMBRICA 152
6.2.1. PRUEBAS DE SEÑAL Y COBERTURA 153
6.2.1.1. DWL-2000AP+ PRUEBAS DE SEÑAL 154
6.2.1.2. WIRELESS LAN ACCESS POINT 7250 PRUEBAS DE SEÑAL. 157
6.2.1.3. WIRELESS-G ACCESS POINT WAP54G PRUEBAS DE SEÑAL. 158
6.2.2. CONCLUSIONES DE LAS PRUEBAS 160
6.2.3. SEGURIDAD EN EL ACCESS POINT 161
6.2.4. DIAGRAMAS DE RADIACIÓN DEL ACCESS POINT 3COM 7250 162
6.2.5. DIAGRAMAS DE RADIACIÓN DE ANTENAS ADICIONALES DEL ACCESS POINT 3COM 7250 165
6.3. IMPLEMENTACIÓN DE LA INTRANET 173

6.3.1. AHORRAR TIEMPO 174
6.3.2. MEJORAR EL CLIMA ORGANIZACIONAL 175
6.3.3. REDUCIR COSTOS 175
6.3.4. REQUISITOS PARA LA IMPLEMENTACIÓN DE LA INTRANET 175
6.3.5. CUESTIONARIO INTRANET 176
6.3.5.1. ESTRUCTURA ORGANIZACIONAL 176
6.3.5.2. INTERCAMBIO DE INFORMACIÓN A NIVEL INTERNO 177
6.3.5.3. INTERCAMBIO DE INFORMACIÓN A NIVEL EXTERNO . .. 178
6.3.5.4. BARRERAS EN EL INTERCAMBIO DE INFORMACIÓN 179
6.3.5.5. RECURSOS DISPONIBLES 179
6.3.5.6. DEFINICIÓN DE OBJETIVOS GENERALES 180
6.3.5.7. DEFINICIÓN DE OBJETIVOS PUNTUALES 181
6.3.5.8. INFRAESTRUCTURA EN SISTEMAS DE LA ORGANIZACIÓN 182
6.3.6. CREACIÓN DE LA INTRANET 184
6.3.6.1. SELECCIÓN DE SOFTWARE PARA LA INTRANET 187
6.3.7. SEGURIDAD EN LA INTRANET 188
CONCLUSIONES..... 190
RECOMENDACIONES. 192
BIBLIOGRAFIA. 193
GLOSARIO..... 195
APENDICES..... 206
APENDICE A: MANUALES..... 207
1.1. MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE CHILI SPOT ... 207
1.2. MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE FREERADIUS 217
1.2.1. CONFIGURACIÓN DE FREERADIUS CON MYSQL 219
1.3. MANUAL DE CONFIGURACIÓN DE SERVIDOR 223
1.3.1. INSTALACIÓN Y CONFIGURACIÓN DE PROXY WEB SQUI 224
1.3.2. INSTALACIÓN DE MYSQL-SERVER 225
1.3.3. INSTALACIÓN Y CONFIGURACIÓN DE APACHE-SSL 227
1.3.4. CONFIGURACIÓN DE FIREWALL 231

1.4. MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE DE CONTABILIDAD DE ACCESOS – DIALUP ADMIN 233
1.5. MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE GPL INTRANE 235
1.6. MANUAL DE CONFIGURACIÓN DE ACCESS POINT 3COM 7250 … 247
1.7. MANUAL DE INSTALACIÓN DE SERVICIO PPTPD (VPN) 255
1.8. MANUAL DE POLITICAS DE SEGURIDAD RFC 2196 …..... 259

APENDICE B: DISPOSITIVOS DE REDES INALAMBRICAS..... 271
APENDICE C:ARTICULOS DE “LA SALUD EN LAS REDES INALÁMBRICAS”
.REDES INALAMBRICAS Y LA SALUD DEL CUERPO HUMANO 273
REDES INALÁMBRICAS Y LA SALUD DEL CUERPO HUMANO 273
LOS CAMPOS ELECTROMAGNÉTICOS Y LA SALUD PÚBLICA 276
APENDICE D:ANALISIS ECONÓMICO DE LAS REDES INALÁMBRICAS” 282
APENDICE E:ANÁLISIS COSTO-BENEFICIO REDES INALÁMBRICAS VRS ALAMBRICAS 320
APENDICE F:CARTA DE LA EMPRESA LEXINCORP S. A. DE C. V. 322

INTRODUCCIÓN

La disponibilidad de conexiones inalámbricas y redes LAN inalámbricas puede ampliar la libertad de los usuarios de la red a la hora de resolver varios problemas asociados a las redes con cableado fijo y, en algunos casos, incluso reducir los gastos de implementación de las redes. Sin embargo, a pesar de esta libertad, las redes LAN inalámbricas traen consigo un nuevo conjunto de desafíos.

La seguridad es un aspecto que cobra especial relevancia cuando se habla de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que se tienen para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Las expectativas de los usuarios finales de una Intranet son simplemente la facilidad de uso, la velocidad y la confiabilidad. Como con los demás sistemas de producción, los responsables de administración de la información necesitan asegurarse de que sus Intranets sean seguras, efectivas en relación a su costo y de fácil manejo. Como Internet, en un principio las Intranets fueron diseñadas pensando en la distribución de la información, pero con el tiempo permitieron ofrecer muchas otras posibilidades que permiten reducir costos.

Las empresas están interesadas en la Intranet para:

- Simplificar el control interno de la información y mejorar la comunicación dentro de las organizaciones, ofreciendo ayudas sumamente sencillas, pero poderosas, como las derivadas del uso de hipervínculos.

- Fomentar la colaboración real entre empleados, permitiendo el acceso generalizado a la información permanente por medio de herramientas de análisis fáciles de utilizar.
- Establecer líneas de acción para cada proceso de negocios y para las tareas administrativas, mediante la difusión de procedimientos en torno a las aplicaciones existentes referentes a los sistemas de producción.

La investigación pretende fusionar la Intranet con la tecnología inalámbrica como un medio de distribución de la información ya que las empresas de hoy en día, y muy especialmente en un futuro muy cercano, la Intranet va ha ser un recurso indispensable. Dada la gran cantidad de datos que genera cualquier empresa, se están quedando obsoletos los actuales métodos de inserción y consulta de datos.

Por tanto se implementara una WLAN bien diseñada, con el respaldo de políticas de seguridad proactivas, que pueden ofrecerle a los usuarios enormes beneficios de la información móvil, e incluso aumentar un tiempo real las ganancias de las actuales empresas, lo que se traduce en mayor productividad y flexibilidad a los trabajadores.

Finalmente se busca la investigación de los diferentes estándares y protocolos inalámbricos para la seguridad WLAN, topologías inalámbricas y los diferentes dispositivos disponibles en la actualidad para montar una red inalámbrica.

CAPITULO I GENERALIDADES

1.1. OBJETIVOS

1.1.1. OBJETIVO GENERAL

Implementar una Intranet segura para la empresa Lexincorp S.A. de C.V. con tecnología inalámbrica y seguridad de accesos para clientes Linux, Microsoft Windows y Macintosh OS X.

1.1.2. OBJETIVOS ESPECÍFICOS

a. Implementar una red inalámbrica segura con mecanismos de autorización, autenticación y auditoria de accesos por medio de FreeRadius.

b. Implementar ChilliSpot como portal cautivo para restringir el acceso a Internet a los usuarios no autorizados.

c. Implementar los estándares y políticas de acceso de una red inalámbrica.

d. Implementar un software de código abierto vía Web el cual sirva como Intranet para los usuarios de la red inalámbrica.

e. Implementar un software de código abierto vía Web para monitorear las sesiones y el tiempo de conexión de los usuarios autorizados.

f. Optimizar los recursos informáticos con los que actualmente cuenta la empresa a la que se implementará la Intranet.

1.2. ALCANCES

Se realizaran los siguientes alcances:

a. Se establecerán las políticas de seguridad y de acceso a los servicios que ofrecerá la Intranet por medio de la red inalámbrica y el servidor Linux.

b. Se establecerán los requerimientos de hardware y software para la implementación de una red inalámbrica.

c. Se realizará la respectiva configuración de los clientes Linux, Microsoft Windows y Macintosh OS X para una red inalámbrica segura.

d. Se realizará la siguiente documentación:
    a. Configuración de equipo inalámbrico a utilizar.
    b. Instalación y configuración de ChilliSpot.
    c. Instalación y configuración de FreeRadius.
    d. Configuración de FreeRadius con MySql.
    e. Configuración de software GPL para la Intranet.
    f. Configuración de servidor.
        - Interfaces de red.
        - Squid.
        - Apache, Apache-SSL
        - Mysql-Server.
        - Firewall
    g. Configuración de software de monitoreo de sesiones y accesos.
    h. Configuración de acceso al servidor por medio de una VPN.
    i. Manual de políticas RFC 2196.

1.3. LIMITACIONES

a. No sé desarrollará un software para la Intranet, ya que se utilizará un software de Código Abierto para brindar los servicios a los clientes.

b. La tecnología inalámbrica no está desarrollada para grandes volúmenes de información, por su limitado ancho de banda.

c. No se utilizara equipo inalámbrico especial para clientes del sistema operativo Macintosh OSX.

1.4. DELIMITACIONES

a. La Intranet utilizará una topología inalámbrica de Modalidad de Infraestructura.

b. El servidor de la Intranet utilizará un sistema operativo Linux.

c. Se protegerá únicamente al servidor y no a las estaciones de trabajo.

CAPITULO II FACTIBILIDAD

2.1. FACTIBILIDAD OPERACIONAL

Esta factibilidad se basa en el hecho que un sistema o proyecto se utilice o funcione como se había previsto. Para poder hacer un buen estudio se responderán las siguientes interrogantes:

a) ¿Son los servicios o programas de la Intranet demasiado complejos para los usuarios de la empresa o los operadores de estos?

No, para la Intranet se utilizara Group-Office que es un software de código abierto el cual fue diseñado para empresas o corporaciones que requieran compartir su información, esto a través de una interfaz Web amigable la cual permite al administrador de la Intranet agregar, quitar módulos, tales como Administrador de Archivos, Calendario, Libreta de Direcciones, Correo Electrónico, Project, entre otros.

b) ¿Existe apoyo suficiente para la implementación del proyecto por parte de la administración?, ¿Y por parte de los usuarios?

Si, luego de haber observado las operaciones de los programas de la empresa, se pudo llevar a la conclusión que éstos no están centralizados, lo cual dificulta la obtención de la información de manera inmediata, por esto, luego de hablar con la administración o encargados de la empresa se coincidió que es necesario una mejora en los servicios y en la seguridad al momento de acceder a la red y servicios.

Se decidió que se hará la implementación de un sistema centralizado basado en un servidor Linux en el cual se administrarán los servicios por medio de una Intranet, ésta podrá ser accedida por los usuarios ya sea en la red inalámbrica o alámbrica.

c) Los programas o software que actualmente se usan en la empresa, ¿son aceptados por los usuarios?

Si, los métodos o programas que utiliza la empresa a diario son Microsoft office, correo electrónico y programas para abogados estos para el manejo de datos e

información. Los usuarios opinan que estos programas son herramientas útiles para su trabajo y fáciles de usar para desarrollar ciertos procedimientos que realizan pero necesitan herramientas para compartir su información.

d) ¿Se perderá la facilidad de acceso a la información?

No, actualmente la información es compartida por medio de correos electrónicos o por disquetes. Para facilitar el acceso a la información se implementara una Intranet la cual tendrá un Administrador de Archivos con el cual los usuarios registrados podrán compartir y tener acceso a la información de la empresa. Además de eso se implementara una red inalámbrica la cual facilitara a los empleados movilidad en la empresa así mismo brindará mayor seguridad a la red al configurarle una tabla de direcciones MAC, con esto solo las computadoras de la empresa podrán tener acceso a la red, evitando así que un intruso externo pueda conectarse a la red.

Sin embargo, teniendo en cuenta que en un determinado momento el equipo puede ser robado, se hizo necesario incurrir en otra forma de autenticar el acceso. Por tanto, se utiliza un portal cautivo para brindar el acceso a la hora de entrar a Internet, pidiendo un usuario y una clave; una vez que la persona haya sido autenticada puede proceder a entrar en la Intranet. Con esto se hará un poco más difícil acceder a la información, pero de este modo la red estará bastante segura.

Al centralizar los servicios de la Intranet en un servidor Linux, los usuarios podrán obtener los datos e información requerida de forma más rápida y simple.

e) ¿La productividad de los empleados será menor después de la implementación del proyecto?

No, se espera que después de haber realizado la implementación de la Intranet y la red inalámbrica, los usuarios podrán desarrollar sus actividades y procedimientos de manera eficaz y eficiente, teniendo un alto grado de seguridad.

f) ¿Los usuarios se verán afectados por la implementación?

No, la implementación mejorara la productividad de la empresa.

2.2. FACTIBILIDAD TÉCNICA

La factibilidad técnica implica que si hay disponibilidad de equipo y software del proyecto a realizar. Por tanto, se recurre a responder las siguientes interrogantes:

g) ¿Existe o se puede adquirir la tecnología necesaria para realizar lo que se pide?

Si, hoy en día existen en el mercado una diversidad de equipos para este fin, para la implementación de la red inalámbrica se necesitará un equipo de buen precio, de buena calidad, que pueda satisfacer las exigencias que necesita la empresa siendo este cien por ciento escalable. En la siguiente tabla se detallan el hardware a utilizar:

Se escogerán tres de las mejores marcas de equipos inalámbricos en el mercado, las marcas que se han elegido son:

TABLA DE EQUIPO INALÁMBRICO				
Cant.	**Descripción**	**Marca**	**Modelo**	**Cobertura**
1	Access point	D-Link	2000-AP+	100 metros
1	Access point	3com	7250	100 metros
1	Access point	LynkSys	WAP54G	100 metros

Cuadro 1 tabla de Access Point mejor posicionados en el mercado

Para el caso de la Intranet se utilizará un software código abierto ya que la licencia es gratis y se pueden mejorar dependiendo de las exigencias que requiera la empresa. Se utilizará el software Group-Office para llevar un control de las actividades, fechas importantes, reuniones y otros de la empresa, también se utilizará un software para el monitoreo de las sesiones y actividades de los usuarios que acceden a Internet o a cualquiera de los otros programas de la Intranet.

h) ¿El equipo propuesto tiene la capacidad técnica para satisfacer los requerimientos de la empresa?

Si, para este propósito se realizaran pruebas con las diferentes marcas de equipos, por tanto, se puede asegurar que este equipo tendrá la capacidad de satisfacer las necesidades de la implementación.

i) ¿La implementación del proyecto ofrecerá respuestas adecuadas a las peticiones sin importar el número y ubicación de los usuarios?

Si, las pruebas determinaran que el equipo que se obtendrá sea el mejor y el más potente, al hacer esto se asegura que el equipo que se escoja podrá soportar un alto número de usuarios y podrá dar movilidad a los empleados que posean equipos inalámbricos en toda la empresa.

Con respecto a la Intranet se crearán los usuarios necesarios, los cuales podrán tener acceso a esta ya sea desde la red alambrica o inalámbrica.

j) Si se implementa el proyecto, ¿se puede crecer con facilidad?

Si, el crecimiento que ha tenido la empresa en estos últimos años nos lleva a implementar un sistema que tenga la capacidad de crecer fácilmente, el proyecto se enfocará en la proyección que tenga la empresa para así poder montar un sistema robusto y escalable.

El equipo inalámbrico que se obtendrá tendrá las características necesarias para realizar actualizaciones y mejoras en el camino como por ejemplo instalación de antenas que mejoren su potencial en la señal. Con respecto al equipo que tendrá la Intranet se instalara un servidor con sistema operativo Linux al cual se le pueden instalar otros programas en un futuro no muy lejano.

2.3. FACTIBILIDAD ECONÓMICA

a) ¿Es grande el costo de llevar a cabo la investigación completa del sistema?

No, la única inversión que se hará en este proyecto será la compra del equipo inalámbrico, esto se debe a que la empresa cuenta con el equipo necesario y sistema de red para poder realizarlo.

b) ¿Cuál es el costo del hardware y software para la aplicación?

El costo del hardware que se adquirirá dependerá de la expectativas que tiene la empresa y su crecimiento, con respecto al software para la aplicación se utilizara software de código abierto por tal motivo no habrá ningún costo, a continuación se presentara un cuadro de precios del equipo a utilizar:

COSTO DE EQUIPO INALÁMBRICO				
Cant.	**Descripción**	**Marca**	**Modelo**	**Precio**
1	Access point	D-Link	2000-AP+	$ 135.60
1	Access point	3com	7250	$ 450.00
1	Access point	LynkSys	WAP54G	$ 149.58

* Los precios incluyen IVA

Cuadro 2 Tabla de los precios de los Access Point seleccionados

c) ¿Cuales son los beneficios en la forma de reducción de costos o de menos errores costosos?

Los beneficios que se pueden mencionar en este caso son los siguientes:

a. Con respecto al software que se implementará no hay ningún costo ya se utilizará software con licencia GPL o de código abierto, el cual permite a la empresa hacer pruebas sin incurrir en gastos o compras de licencias o programas que no cumplen con sus expectativas, esto evita de gran manera errores costosos.
b. Con respecto a la implementación de la red inalámbrica esta permitirá a la empresa movilidad y evitará realizar nuevos cableados los cuales no están

previstos comprometiendo la capacidad en el equipo de red actual, esto reducirá en gran medida los costos.

c. La Intranet contribuirá a mejorar las labores diarias en la empresa ya que se compartirá información vital, la cual evitará y eliminara una gran cantidad de tiempo perdido y papeles que son impresos para verificación.

d) ¿El costo si nada sucede (si el proyecto no se lleva a cabo)?

El crecimiento de la empresa en estos últimos años es grande, este crecimiento lleva a pensar en adquirir nueva tecnología la cual permita reducir tiempo, esfuerzo y dinero. El costo si el proyecto no se lleva a cabo podría ser grande ya que la empresa quedaría en desventaja en relación a las demás empresas que cuentan con las herramientas necesarias para poder realizar sus tareas de una manera eficiente.

CAPITULO III METODOLOGÍA DE LA INVESTIGACIÓN

El proyecto se desarrollará de la siguiente manera:

a. Investigar el concepto de Intranet, así como sus ventajas y los servicios que brindan a los clientes.
b. Investigar estándares y políticas de seguridad para los dispositivos de la red.
c. Investigar protocolos de seguridad inalámbrica.
d. Investigación de dispositivos y topologías de redes para construir una Intranet inalámbrica.
e. Investigar la relación entre WLAN y alàmbricas.
f. Investigar acerca de redes VPN, SAN para la seguridad.
g. Investigar sobre un software con el que se pueda usar el método AAA (autenticación, autorización y contabilidad).
h. Investigar de un software que pueda brindar un portal cautivo para acceder a Internet.
i. Investigar sobre el posible software GPL para la Intranet.
j. Investigar acerca de la salud en cuanto a las redes inalámbricas.
k. Consultar a la empresa los requerimientos necesarios para llevar a cabo la implementación.
l. Implementación de una Intranet segura con tecnología WLAN.

En cuanto a la metodología a seguir para la realización del proyecto un ciclo de vida que consta de las siguientes actividades:

3.1 INVESTIGACIÓN PRELIMINAR

Para la recolección de datos se usarán diversidad de técnicas y herramientas, entre las cuales tenemos visitas a sitios Web, y bibliografía que contenga Información relacionada con el tema a investigar.

3.2. ANÁLISIS DE LA INFORMACIÓN, REQUISITOS DE HARDWARE Y SOFTWARE

Basándose en los datos recolectados en la investigación preliminar, se clasificará la información necesaria para la configuración en la Intranet, basándose en los requerimientos de la empresa, teniendo en cuenta la seguridad como punto indispensable en la Intranet.

3.2.1 HARDWARE

En cuanto al hardware se escogera una computadora como servidor Linux con memoria Ram y CPU capaz para procesar todos los programas y procedimientos que los clientes soliciten o utilicen.

También se seleccionará un Access Point que pueda brindar señal suficiente a todas las computadoras con tarjetas inalámbricas que se conectarán a la Intranet.

3.2.2 SOFTWARE

Se seleccionará un software GPL que brindará los servicios de la Intranet para los clientes de la empresa. Además se necesitará un software para poder brindar un método de AAA (autenticación, autorización, auditoria). También se utilizará un software para brindar un portal cauitvo para acceder a Internet. Finalmente, se instalará un software de contabilidad de accesos que mostrará las sesiones y tiempos de conexión de los usuarios autorizados.

Para brindar más seguridad para algunos usuarios de la empresa se configurará una red VPN, entre uno de los usuarios y el servidor Linux.

3.3. DISEÑO

Se procederá a realizar la definición de estándares y políticas de seguridad, pues con ellas se refuerza el aspecto de seguridad en la Intranet. Éstas políticas, son una serie de reglas o normas que se consideran en el momento de crear cierta tecnología ya que marcan los parámetros a seguir en cuanto a qué se debe proteger, cómo se debe proteger.

En la fase de recolección de información, se visitarán sitios Web con el fin de investigar información actualizada o más reciente con respecto a Tecnología Inalámbrica para posteriormente crear la Intranet segura y configurada.

3.4. DEMOSTRACIÓN DE LA INTRANET INALÁMBRICA

En la parte que concierne a demostración de WLAN, se han establecido una serie de métodos a incluir en el funcionamiento de la Intranet Inalámbrica con el objetivo de garantizar la seguridad del perímetro que se desea proteger.

Para esta etapa de manera general las técnicas pueden ser vistas como técnicas de estándares y políticas de seguridad, utilización de un software gratuito GPL que nos brindará seguridad por medio de perfiles de usuarios. Además se utilizará un software para brindar el método de AAA(autenticación, autorización y auditoria).

Siempre en la parte de demostración Inalámbrica serán necesarias las siguientes actividades:

3.4.1. INSTALACIÓN DEL EQUIPO

La instalación y configuración del equipo se realizará como se muestra en el siguiente diagrama.

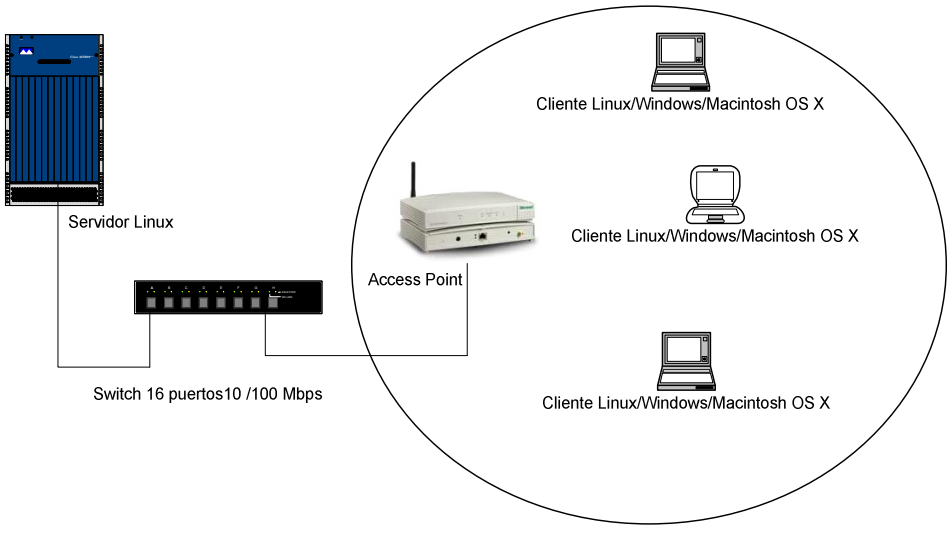


Figura 1 Diagrama de la implementación

Con libertad de ubicación para usuarios móviles dentro de las oficinas. Integración con la red cableada existente. Pero se debe de hacer pruebas de señal y cobertura del Access Point esto se comprobará en el Capitulo VI.

3.4.2. CONFIGURACIÓN

La configuración se realizará de la siguiente manera:

- Configuración del Access Point
- Configuración de servicios en el Servidor Linux.
- Configuración de software que brinda el portal cautivo para acceder a Internet.
- Configuración de software que brinda método AAA.
- Configuración de software de contabilidad de accesos.
- Instalación y configuración del software GPL de la Intranet
- Configuración de una red VPN.

3.4.3. PRUEBAS Y CORRECCIONES DE ERRORES

Luego de haber realizado las pruebas necesarias a la Intranet y observar el comportamiento de la misma, será necesario realizar las respectivas correcciones de las fallas que se presenten.

3.5. DOCUMENTACIÓN

Se mostrarán de manera detallada cada uno de los requerimientos necesarios para crear una Intranet segura con tecnología WLAN como son los estándares y políticas de seguridad, dispositivos inalámbricos, clientes, software.

La documentación a presentar es la siguiente:

1. Configuración de equipo inalámbrico – Access Point.
2. Instalación y configuración de software que brinda el portal cautivo para acceder a Internet.
3. Instalación y configuración de software que brinda el método AAA.
4. Configuración de software GPL – Intranet.
5. Configuración de servidor.
    a. Interfaces de red.
    b. DHCP
    c. Proxy.
    d. Firewall.

6. Instalación de software para servidor.
    a. Apache
    b. Apache-ssl
    c. Mysql-server
7. Configuración de software de contabilidad de accesos.
8. Instalación y configuración de una red VPN.
9. Manual de políticas

CAPITULO IV

SITUACIÓN ACTUAL DE LA EMPRESA

4.1. DESCRIPCIÓN DE LA RED ACTUAL Y SU ENTORNO

Lexincorp S.A. de C.V. es una firma de abogados que tiene oficinas en Centro América y el objetivo de esta es atender las necesidades integrales de los clientes en la región.

En la actualidad Lexincorp S.A. de C.V. maneja la mayoría de procesos de forma manual. Si bien es cierto que la utilización de herramientas tales como Microsoft Office, correos electrónicos y programas para abogados son de gran ayuda para la obtención de datos y de información, ésta no está centralizada y no puede ser obtenida de manera inmediata o en el momento que se requiera.

Además de esto cuenta con una maquina que realiza las funciones de un servidor la cual carece de las características necesarias para la demanda que tiene la empresa hoy en día, tiene como sistema operativo Windows 98 la cual provee de conectividad a las demás maquinas en la red por medio de un programa llamado WinProxy el cual es muy inestable y ocasiona muchos problemas.

La empresa cuenta con veintidós computadoras en total, el crecimiento de esta en los últimos años conlleva a realizar mejoras e implementaciones que agilicen, optimicen y den la seguridad al usuario al momento de utilizar los recursos con los que cuentan actualmente, es por esto que se hará la implementación de un sistema centralizado basado en un servidor Linux el cual administrara servicios por medio de una Intranet la cual a su vez podrá ser accedida a través de cualquier cliente en la red alambrica o inalámbrica por medio de un navegador.

Actualmente Lexincorp no posee red inalámbrica por lo cual se harán pruebas con los diferentes tipos de equipos inalámbricos que hay en el mercado para así determinar cual de estos ofrece todas aquellas características que cumplan con todos los requerimientos que tenga la empresa según la proyección y crecimiento que tenga esta.

4.2. CUADRO DE MAQUINAS ACTUALES POR DEPARTAMENTO Y SUS ESPECIFICACIONES

A continuación se muestra un cuadro de las maquinas que la empresa posee actualmente con su ubicación y el usuario que las utiliza.

CUADRO DE ESPECIFICACIONES TÉCNICAS							
Ubicación	**USUARIO**	**RAM**	**Sistema Operativo**	**Red**		**MARCA**	**MODELO**
				Alambrica	**Inalámbrica**		
Notariado	Cristina Urbano	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
	Carmen Morales	128 DDR	Windows Xp	Si	No	Clon	U8668-D
	Tathiana Villalta	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
	Ernesto Sanchez	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
	Lic Duarte	256 DDR	Windows Xp	Si	No	Clon	U8668-D
Cubículo	Pamela	256 DDR	Windows Xp	Si	No	Clon	U8668-D
	Francisco Barahona	384 DDR	Windows Xp	Si	No	Compaq	Presario 4400 LA
	Mónica Muñoz	256 DDR	Windows Xp	Si	No	Clon	U8668-D
	Karla Guzmán	256 DDR	Windows Xp	Si	No	Clon	U8668-D
	Cristobal	256 SDR	Windows Xp	Si	No	Dell	GX60
	Karen Carazo	512 DDR	Windows Xp	Si	No	Clon	P4M80-M4
	Karla Avilés	512 DDR	Windows Xp	Si	No	Clon	P4M80-M4
Contabilidad	Margarita Monterrosa	256 SDR	Windows Xp	Si	No	Dell	GX60
	Alexander Cubías	256 DDR	Windows Xp	Si	No	Clon	U8668-D
Recepción	Alberto	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
Oficinas Administrativas	Lic. Magaña	256 DDR	Windows Xp	Si	No	Clon	U8998
	Lic Nora Amaya	256 DDR	Windows Xp	Si	No	Dell	Dimension 2100
Oficinas 2do. Nivel.	Lic José Polanco	256 DDR	Windows Xp	Si	Si	Clon	U8668-D
	Lic. Escobar	512 DDR	MAC OSX	Si	Si	MAC	Laptop
	Lic. Giancarlo Angelucci	256 DDR	Windows Xp	Si	Si	Dell	Laptop
	Lic. Telles	512 DDR	MAC OSX	Si	Si	MAC	Laptop
Recepción 2do. Nivel	Josefina Hernández	256 DDR	Windows Xp	Si	No	Clon	M6VLR

Cuadro 3 computadoras de la empresa Lexicorp S. A. de C. V.

4.3. ESQUEMA ACTUAL DE RED

La empresa cuenta con un esquema básico de redes, tienen un enlace a Internet con un ancho de banda de 256 K, la topología que utiliza es en forma de estrella, como se muestra en la siguiente figura:

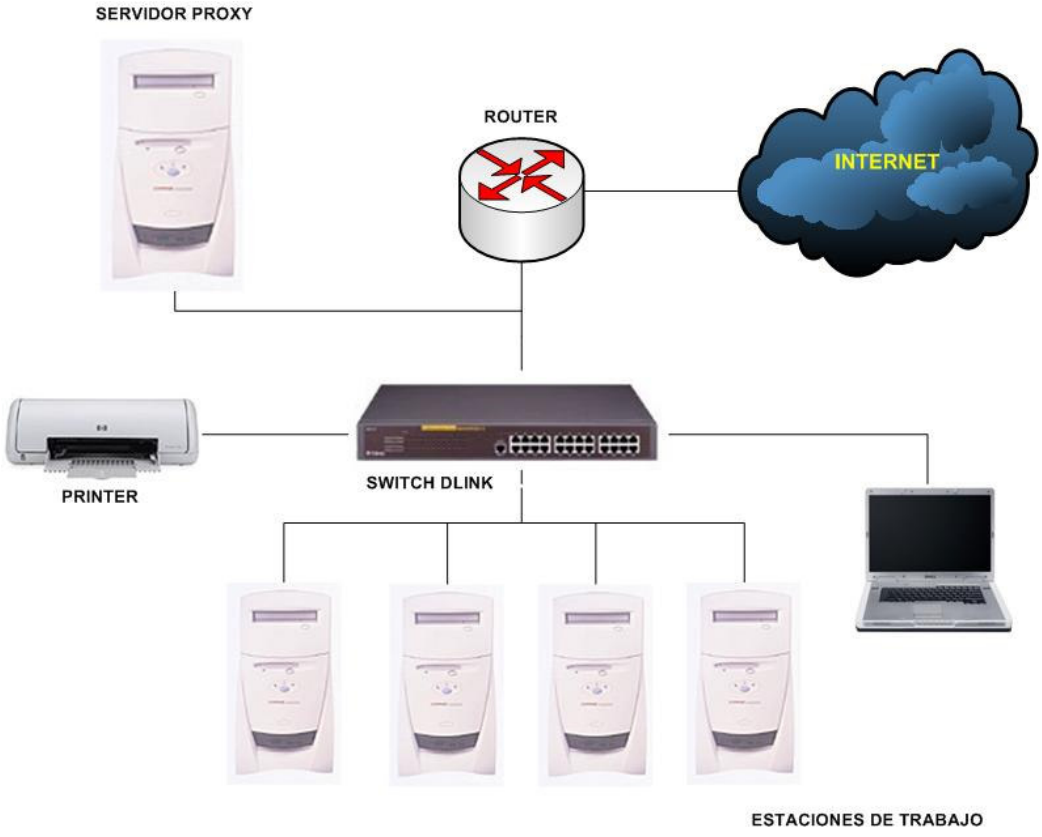


Figura 2 Esquema actual de red de la empresa Lexicorp S. A. de C. V.

CAPITULO V MARCO TEÓRICO

5.1. MARCO HISTORICO

5.1.1. REFERENCIAS HISTORICAS

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceding del IEEE, puede considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread- pectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.[1]

[1] *Esta información fue obtenida del sitio Web http://www.ubuntu-es.org/node/8184 - 18k*

5.1.2. CAPAS DEL MODELO OSI.

El modelo OSI (Open Systems Interconection) de telecomunicaciones esta basado en una propuesta desarrollada por la organización de estándares internacional (ISO), por lo que también se le conoce como modelo ISO - OSI.

Su función es la de definir la forma en que se comunican los sistemas abiertos de telecomunicaciones, es decir, los sistemas que se comunican con otros sistemas.

El modelo de referencia consiste en 7 capas. Estas capas se visualizan generalmente como un montón de bloques apilados o en ingles como un "stack of blocks", por lo que en ingles, a esto se le conoce como el "OSI Protocol Stack". La descripción de los 7 niveles es la siguiente:

1. **Nivel Físico:** Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:
    a. Definir conexiones físicas entre computadoras.
    b. Describir el aspecto mecánico de la interface física.
    c. Describir el aspecto eléctrico de la interface física.
    d. Describir el aspecto funcional de la interface física.
    e. Definir la Técnica de Transmisión.
    f. Definir el Tipo de Transmisión.
    g. Definir la Codificación de Línea.
    h. Definir la Velocidad de Transmisión.
    i. Definir el Modo de Operación de la Línea de Datos.
2. **Nivel Enlace de Datos:** Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:
    a. Detectar errores en el nivel físico.
    b. Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
    c. Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico.

d. Enviar bloques de datos con el control necesario para la sincronía.
e. En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

3. **Nivel de Red:** Este nivel define el enrutamiento y el envío de paquetes entre redes.
    a. Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
    b. Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
    c. Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
    d. Define el estado de los mensajes que se envían a nodos de la red.
4. **Nivel de Transporte:** Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información.
    a. Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).
    b. Este nivel define como direccionar la localidad física de los dispositivos de la red.
    c. Asigna una dirección única de transporte a cada usuario.
    d. Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
    e. Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
    f. Determina el protocolo que garantiza el envío del mensaje.
    g. Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.
5. **Nivel Sesión**: proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

a. Establece el inicio y termino de la sesión.
b. Recuperación de la sesión.
c. Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
d. Referencia a los dispositivos por nombre y no por dirección.
e. Permite escribir programas que correrán en cualquier instalación de red.

6. **Nivel Presentación:** Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.
    a. Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
    b. Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
    c. Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
    d. Opera el intercambio.
    e. Opera la visualización.
7. **Nivel Aplicación:** Proporciona servicios al usuario del Modelo OSI.
    a. Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
    b. Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), correo electrónico, telnet y otros.[2]

[2] *Esta información fue obtenida del sitio Web http://www.unincca.edu.co/boletin/indice.htm*

5.2. MARCO CONCEPTUAL

5.2.1. REDES INALAMBRICAS

Como ya se ha dicho, las redes de computadoras pueden estar constituidas por medios guiados o no guiados.

En este apartado se abordarán las redes que funcionan con medios no guiados. Esto debido a que se trata de una tecnología que está teniendo mucho auge en la actualidad debido a las características y ventajas que ofrece.

Aunque las técnicas que se utilizan para comunicar estas redes se han utilizado desde hace mucho tiempo, su aplicación en redes de computadoras es nueva. Debido a esto falta mucho por investigar y mejorar en este tipo de redes, ya que aun no alcanzan la misma eficiencia que las redes más comunes.

Las capacidades que ofrece la tecnología inalámbrica es proporcionar mayor movilidad y comodidad con total funcionamiento en cualquier lugar donde se encuentre. La funcionalidad debe garantizarse en cualquier plataforma y marca que los clientes prefieran para que esta tecnología tenga una buena aceptación. Para esto los fabricantes se están poniendo de acuerdo creando una serie de protocolos y estándares que regirán toda la tecnología inalámbrica.

La tecnología inalámbrica ha influido y se encuentra desde hace mucho tiempo en la vida cotidiana de todas las personas. Las ondas de radio, microondas, infrarrojos y ondas de sonido son algunas de las formas alguna vez ha utilizado una persona y a influido en su vida.

Cuando una persona a experimentado y se ha acostumbrado al uso del ordenador y los servicios de comunicación en su oficina o en casa, ahora espera disponer de los mismos servicios y capacidades pero mientras se encuentra en movimiento.

Con las redes inalámbricas se ha dado un paso más, al ofrecer conexiones de datos entre dispositivos informáticos en movimiento.

Una empresa moderna tiene cada vez más personal móvil. Ya no se trabaja detrás de un escritorio ocho horas diarias. Ahora los empleados están equipados con computadoras móviles y pasan más tiempo trabajando fuera de los lugares tradicionales de trabajo, obteniendo mayor productividad para su empresa que se obtiene en reuniones y fuera de la mesa de trabajo. El uso de Internet como fuente

de información y comunicación ha hecho que se demande el acceso 24 horas, 7 días a la semana, desde cualquier lugar donde este la persona, permitiendo a estas trabajar en hoteles, restaurantes, aviones, en el automóvil, etc.

Se estima que para el 2006 el 60% de los productos electrónicos más importantes serán portátiles y requerirán de una conexión a la red o a otros dispositivos. Esta tecnología "sin cables" nos permitirá no sólo obtener historiales financieros o médicos, si no que, se podrá hacer reservaciones de avión, programar el televisor o el horno de microondas desde cualquier lugar con solo dar un clic.

La tecnología inalámbrica esta revolucionando las telecomunicaciones, y junto con los nuevos dispositivos marcarán el futuro de una vida sin cables.[3]

Las redes WLAN se remontan a la primera publicación que se hizo en 1979 de los resultados obtenidos en un experimento hecho por ingenieros de la IBM en Suiza. Consistía en utilizar enlaces infrarrojos para crear una red local una fábrica. Estos resultados publicados en el volumen 67 de los Procedimientos de IEEE, puede considerarse como punto de partida de esta tecnología.

Las investigaciones continuaron con infrarrojos y microondas, donde se utilizaba el esquema "Spread-Spectrum" (Frecuencias Altas), en nivel laboratorio. En Mayo del 1985 y tras cuatro años de estudios, el FCC (*Federal Communications Comission*), la agencia federal del gobierno de Estados Unidos encargada de regular y administrar las telecomunicaciones, asignó las bandas ISM (*Industrial, Scientific and Medical*) 902 - 928 MHz., 2400 - 2485 GHz. y 5725, 5850 GHz. a las redes inalámbricas basadas en "Spread-Spectrum". ISM es una banda para uso comercial sin licencia, es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide quien debe transmitir en esa banda.

La asignación de una banda de frecuencia propicio una mayor actividad en las industrias.

Ese respaldo hizo que las WLAN dejaran de ser experimentos de laboratorio para comenzar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando en fase de desarrollo, hasta que en 1991 se publicaron los primeros

[3] *http://www.tecnotopia.com.mx/redes/redinalambricas.htm*

trabajos referentes a WLAN operativos que superaban la velocidad de 1Mbps, el mínimo establecido por la IEEE para que una red sea considerada una LAN.

Hasta ese momento las WLAN habían tenido muy poca aceptación en el mercado por dos razones fundamentales: falta de un estándar y los precios elevados para una solución inalámbrica.

Sin embargo en los últimos años se está produciendo un crecimiento explosivo de hasta un 100% anual. Lo anterior debido a las siguientes razones:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles.
- La conclusión de la norma IEEE 802.11 para redes de área local inalámbricas que ha establecido un punto de referencia y ha mejorado muchos aspectos de estas redes.[4]

5.2.1.1. DEFINICIÓN DE WLAN

WLAN (*Wireless Local Area Network*), Red Inalámbrica de Área Local, es una red de área local que utiliza medios no guiados para la comunicación entre los dispositivos conectados.

Los medios no guiados utilizan ondas electromagnéticas como medio de transmisión de datos.

Las microondas, el radio y los infrarrojos son los más utilizados. Esto da como resultado que los dispositivos puedan moverse dentro del radio de alcance de la red, cosa que con las redes cableadas resulta imposible.

Otra de las ventajas es que su instalación tiene bajo costo y se ahorra al no tener que cablear. Aun así, debido a que las prestaciones que ofrece en cuanto a velocidad es menor comparado con las redes alámbricas, estas son la mejor opción en situaciones donde no se puede utilizar cables como medio de transporte y generalmente se utilizan como un complemento en una LAN.[5]

---

[4] http://www.unincca.edu.co/boletin/indice.htm

[5] http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

5.2.1.2. CONFIGURACIONES DE WLAN

La complejidad de la configuración física de una WLAN puede ser muy variable, dependiendo de las necesidades que se presenten y requerimientos del sistema a implementar.

5.2.1.2.1. PEER TO PEER O AD-HOC

Es la configuración más básica y es llamada igual a igual o *Ad-Hoc* debido a que las terminales se conectan directamente entre si. Esta configuración es muy fácil de implementar y no requiere de algún tipo de administración. Para que exista una comunicación, las estaciones deben estar dentro del rango de alcance una de otra.

Muchas de las operaciones que controlaba el Access Point, como la señalización y la sincronización, son controladas por una estación. La red *Ad Hoc* no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

Las conexiones *Ad Hoc* son completamente privadas entre las máquinas en cuestión.

Dado que este tipo de conexiones sólo existen entre dos o más ordenadores, son útiles principalmente para transferir archivos en cualquier lugar sin necesidad de conectarse a la red alámbrica o a un Access Point.

El modo *Ad Hoc* es uno de los pocos aspectos de *Wi-Fi* que no forma parte del proceso de certificación de dispositivos fabricados antes de 2002. La *Wi-Fi Alliance* añadió un estándar

Ad-Hoc a finales de 2001, de modo que todo el equipamiento nuevo debe funcionar con esta configuración.[6]

[6] *Engst Adam, Fleishman, Introducción a las redes inalámbricas, Edit. Anaya.*

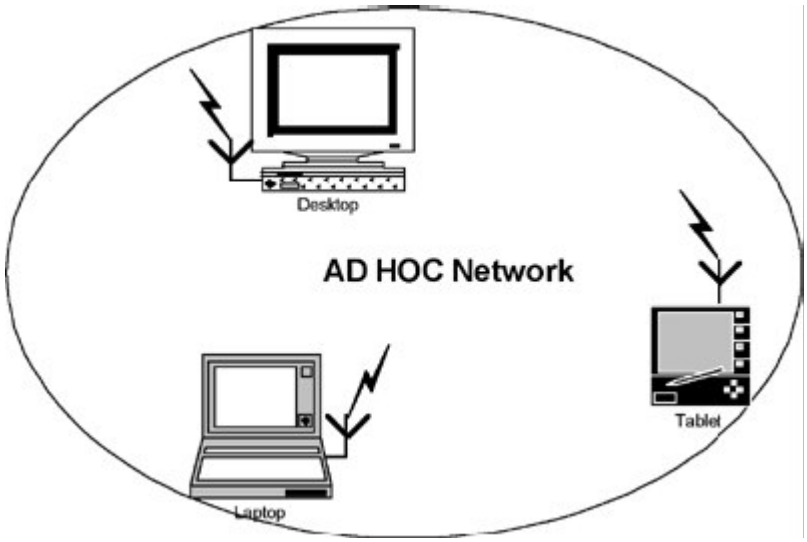


Figura 3 Conexión AD-HOC

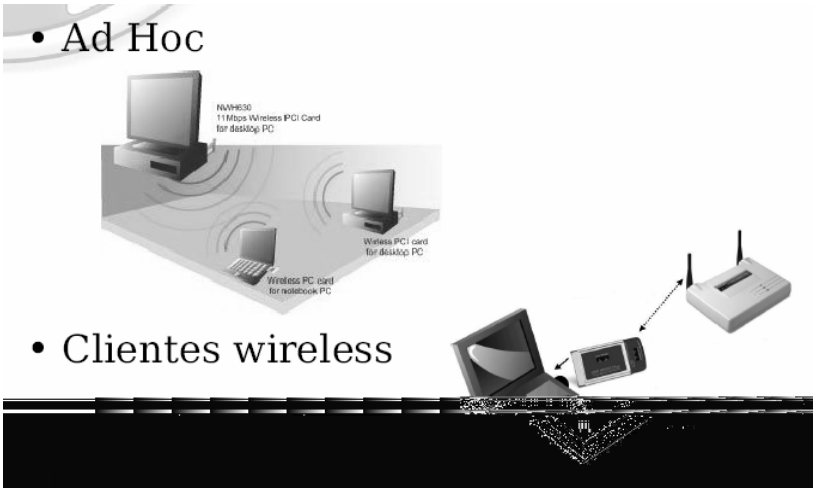


Figura 4 Conexión AD-HOC

5.2.1.2.2. INFRAESTRUCTURA

En este tipo de configuración se utiliza un Access Point. La ventaja de este dispositivo es que se agranda el radio de alcance de la red, se puede conectar a redes fijas y hace la función de administrador disminuyendo o evitando las colisiones entre las comunicaciones.

Para llevarse a cabo la comunicación del portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo

mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el Access Point. Una vez que el Access Point y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el Access Point y la estación intercambien información y datos de capacidad. El Access Point puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un Access Point para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del Access Point, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el Access Point y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un Access Point a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para

buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un Access Point diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el Access Point. Estas tramas contienen el valor de reloj del Access Point en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

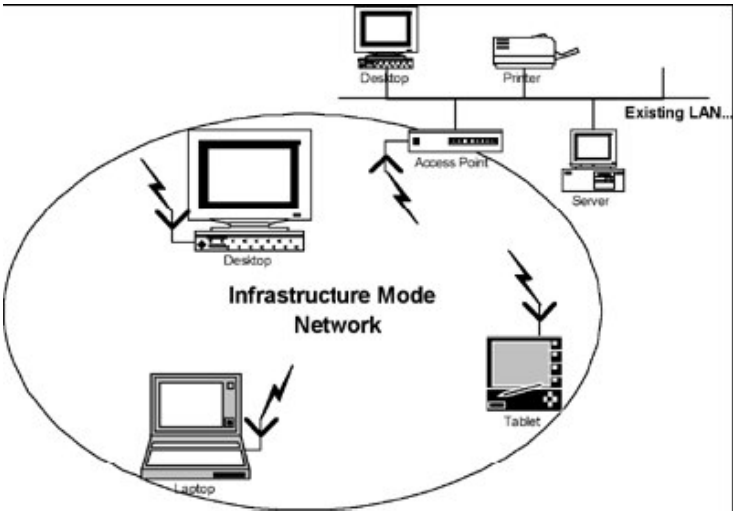


Figura 5 Configuración de Infraestructura

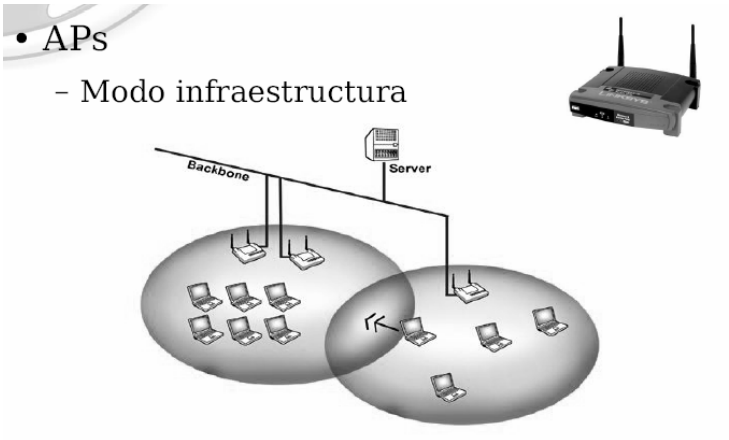


Figura 6 Configuración de Infraestructura

5.2.1.2.3. INTERCONEXIÓN DE REDES

Existe la posibilidad de que las redes inalámbricas se amplíen gracias a la posibilidad de las interconexiones con otras redes, sobre todo con redes no inalámbricas. De esta forma los recursos disponibles de ambas redes se amplían.

Mediante el uso de antenas, direccionales u omnidireccionales, es posible conectar dos redes separadas por varios cientos de metros, por ejemplo dos locales situados en diferentes edificios. De esta forma una red no inalámbrica se beneficia de la tecnología inalámbrica para interconectarse con otra, que de otra forma sería más costoso o simplemente imposible.

5.2.1.2.4. PUNTOS DE EXTENSIÓN

Si las anteriores configuraciones no son suficientes para resolver las necesidades más particulares y específicas, el diseñador de la red puede optar por usar un Punto de Extensión (EP), para aumentar el número de puntos de acceso a la red. Estas células de extensión funcionan como Access Point a Access Point, pero no están conectados a la red física como normalmente se encuentra un Access Point. Los puntos de extensión funcionan, como su nombre lo indica, extendiendo el alcance efectivo de la red mediante la retransmisión de las señales de un cliente hacia un Access Point o hacia otro cliente. Los EP pueden encadenarse para así servir como un puente entre dos estaciones situadas muy lejos una de la otra.[7]

[7] *http://www.microalcarria.com/descargas/documentos/Wireless/Redes_Inalambricas_802.11b.pdf*
http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf
http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp

5.2.1.2.5. TOPOLOGÍA DE INFRAESTRUCTURA EXTENDIDA

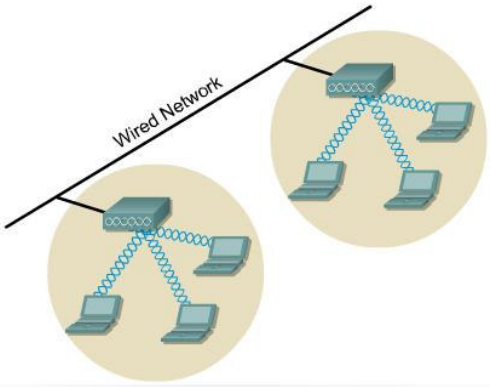


Figura 7 Configuración de infraestructura extendida

Servicio extendido (ESS) es definido como uno o dos BSSs que son conectados por un sistema de distribución común. Esto permite la creación de una red inalámbrica de un tamaño arbitral y complejo. Como con un BSS, todos los paquetes en un ESS deben atravesar uno de los Access Points.

5.2.1.2.6. TOPOLOGÍA DE ESTACIÓN BASE CON ACCESO A INTERNET POR LLAMADA.

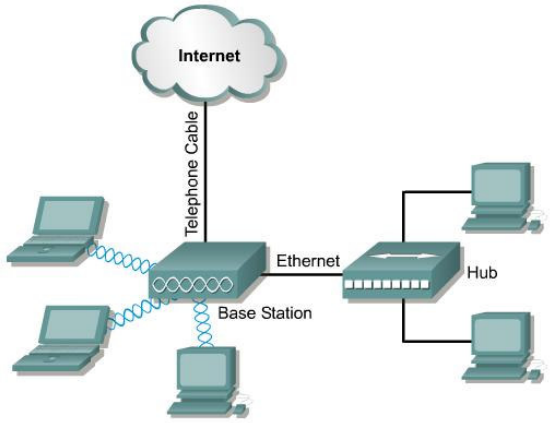


Figura 8 Configuración de estación base por llamada

Esta estación base fue diseñada para oficina de hogar y pequeñas oficinas (SOHO). Permite a los telecomunicadores, usuarios de oficinas, y usuarios desde su hogar la conveniencia de las redes inalámbricas. Conectividad por llamada permite a los equipos tanto alambricos como inalámbricos acceder al MODEM y al Internet. La estación base también va a funcionar como servidor DHCP para hasta 100 clientes alambricos e inalámbricos.

5.2.1.2.7. TOPOLOGÍA DE ESTACIÓN BASE CON ACCESO A INTERNET POR DSL O CABLE.

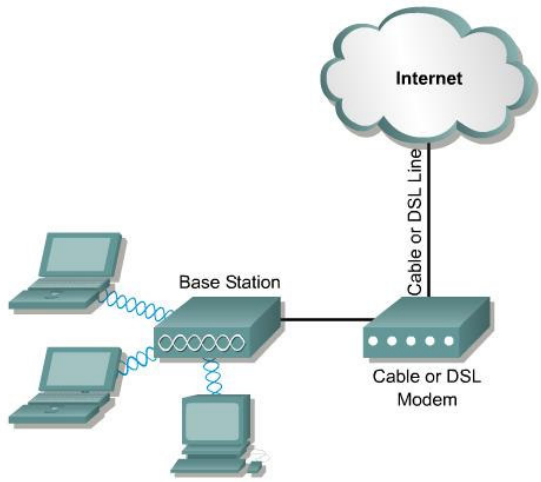


Figura 9Configuración de estación base con acceso por Dsl o cable

Esta estación de base ofrece soporte para cable o DSL modem, además solo soportará clientes inalámbricos. Aunque el servicio DHCP funciona, no se puede conectar al cable alambrico porque el puerto de ethernet esta debe ser usado para conectar el cable o DSL modem.

5.2.1.2.8. TOPOLOGÍA DE REPETIDOR INALAMBRICO

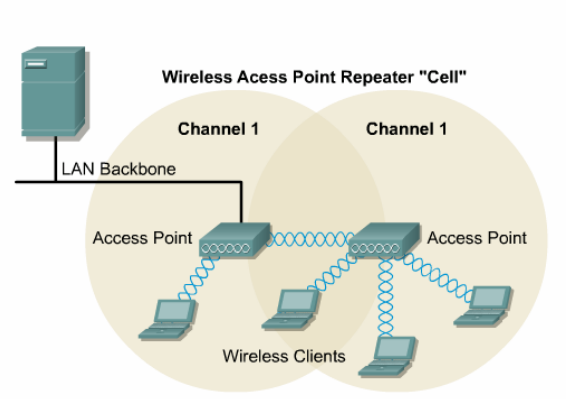


Figura 10 Configuración de repetidor inalámbrico

Un entorno donde extensa conectividad es necesaria pero el acceso al backbone no esta disponible, entonces se debe de usar un repetidor inalámbrico. Un repetidor inalámbrico es simplemente un Access Point que no esta conectado al backbone. Este método requiere de un 50 % de traslape entre el Access Point que esta conectado al backbone y el repetidor inalámbrico.

5.2.1.2.9. TOPOLOGÍA DE SISTEMA REDUNDANTE

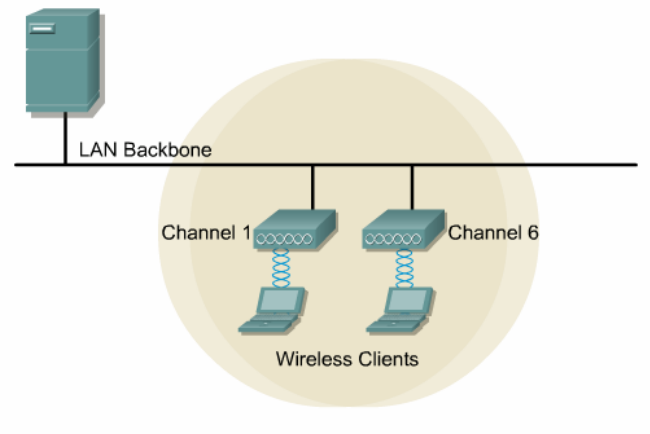


Figura 11Configuración de sistema redundante

En una LAN donde es esencial tener comunicación, se debe de usar redundancia. Con el Espectro de Dispersión de Secuencia Directa (DSSS) producido de diferentes fuentes, ambos Puntos de Acceso serán enviados a la misma frecuencia. Como estas unidades comparten la frecuencia solo pueden comunicarse una a la vez, si por alguna razón un Access Point cae abajo o deja de funcionar, todos los clientes de este seguirían comunicados por medio del otro Access Point. Con esto podemos afirmar que se posee un sistema redundante, con tolerancia a fallos.

5.2.1.2.10. TOPOLOGÍA DE EDIFICIO A EDIFICIO

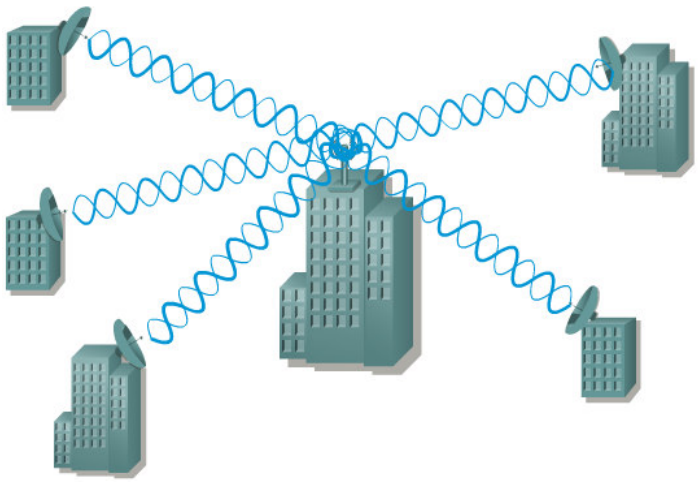


Figura 12 Configuración de edificio a edificio

Con un puente inalámbrico, redes localizadas en edificios a muchas millas de distancia pueden ser integradas en una sola. Sin la ayuda de las redes inalámbricas, organizaciones frecuentemente recurren a la ayuda de redes de área amplia (WAN) para unir sucursales que están a muchas millas de distancia. Estas tecnologías WAN representas ciertas desventajas:

- La instalación es típicamente cara y no es inmediata
- Las cuotas mensuales por el uso de ancho de bando son bastantes altas.

Las redes inalámbricas pueden ser compradas e instaladas en pocos días. Una vez hecha la inversión no hay cargos adicionales a uso de este equipo.[8]

5.2.1.3. MEDIOS INALÁMBRICOS

Lo interesante de las redes inalámbricas no es que funcionen sin cables, sino que, funcionan sin necesidad de que esté visible el Access Point al que se conecta. Hoy en día esto se ve con normalidad pero al inicio no fue así.

5.2.1.3.1. INFRARROJOS

Las primeras redes inalámbricas utilizaban la radiación infrarroja. Las redes infrarrojas tienen una limitación: se necesita una visión directa entre un transceptor infrarrojo y otro, lo que dificultaba trabajar con este tipo de dispositivos dentro de una oficina con muchos cubículos, ya que había que colocar los transceptores lo suficientemente alto para que no existiera algún obstáculo que interfiriera con la señal.

Los infrarrojos se siguen utilizando actualmente en las agendas electrónicas basadas en Palm OS, aparatos PocketPC, teléfonos móviles y algunas computadoras portátiles donde su uso está reservado para conexiones *Ad Hoc* cortas especiales.

Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos no pueden pasar a través de objetos opacos pero se pueden reflejar en determinadas

[8] *Esta Información fue obtenida de Curriculum Cisco Wireless Version 1.0 Module 4 Wireless Topologies*

superficies lo que limita su capacidad de difusión. En contraparte esta limitación supone un seguro contra receptores indeseados.

También, debido a la alta frecuencia, presentan una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por otros dispositivos, pudiendo, además, alcanzar grandes velocidades de transmisión; de hecho, se han desarrollado sistemas que alcanzan velocidades de hasta 100Mbps.

Otras ventajas son: que no existen restricciones de uso, la transmisión de rayos infrarrojos no requiere autorización especial de ningún país, excepto por los organismos de salud que limitan la potencia de la señal transmitida y que los componentes utilizados son sumamente económicos y de bajo consumo energético, importantes ventajas a considerar en equipos móviles portátiles.

En cuanto a las señales de infrarrojos las modulaciones son de 16-PPM (Modulación Por Posición de Impulsos) y 4-PPM que permiten 1 y 2 Mbps de transmisión; las longitudes de onda de operación se sitúan alrededor de los 850-950 manómetros de rango, es decir, a unas frecuencias de emisión que se sitúan entre los 3,15 · 10e14 Hz y los 3,52 · 10e14 Hz.

5.2.1.3.1.1. CAPA FÍSICA EN INFRARROJOS

Para describir la capa física se tomarán las especificaciones de IRDA (*Infrared Data Assosciation*), organismo que ha desarrollado estándares para conexiones basadas en infrarrojos.

Para la capa infrarroja se tienen las siguientes velocidades de transmisión:

- 1 y 2 Mbps, infrarrojos de modulación directa.
- 4 Mbps, mediante infrarrojos portadora modulada.
- 10 Mbps, infrarrojos con modulación de múltiples portadoras

CLASIFICACIÓN

De acuerdo con el ángulo de apertura con el que se emite la información del transmisor, los sistemas infrarrojos pueden clasificarse en sistema de corta apertura,

también llamados de rayo dirigido o de línea de vista LOS (*Line Of Sight*), y en sistemas de gran apertura, reflejados o difusos.

Sistemas de corta apertura, de haz dirigido o de visibilidad directa que funcionan de manera similar a los mandos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información. Este sistema solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico pero no móvil, o sea que está más orientado a la portabilidad pero no la movilidad.

Sistemas de gran apertura, reflejados o de difusión que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio. La norma IEEE 802.11 especifica dos modulaciones para esta tecnología: la modulación 16-PPM y la modulación 4-PPM proporcionando unas velocidades de transmisión de 1 y 2 Mbps respectivamente. Esta tecnología se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance o redes locales en entornos muy localizados como puede ser una aula concreta o un laboratorio.

La dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria reflejada llega con un retraso al receptor). Esta es una de las dificultades que han retrasado el desarrollo del sistema infrarrojo en la norma 802.11.

Las velocidades de transmisión de datos no son elevadas y sólo se han conseguido en enlaces punto a punto. Este tipo de redes están lejos de competir con las LAN de radiofrecuencia, sus uso esta orientado al apoyo y complemento de las LAN ya instaladas, ya sean cableadas o por radio, cuando la aplicación requiera de un enlace de corta distancia punto a punto que, mediante tecnología de infrarrojos, se consigue menor coste y potencia que con las convencionales.

El principio de funcionamiento en la capa física es muy simple y proviene del ámbito de las comunicaciones ópticas por cable. Un LED (*Light Emitting Diode*), que constituye el dispositivo emisor, emite luz que se propaga en el espacio libre en lugar de hacerlo en una fibra óptica, como ocurre en una red cableada. En el otro extremo,

el receptor, un fotodiodo PIN recibe los pulsos de luz y los convierte en señales eléctricas que, tras su manipulación (amplificación, conversión a formato Bit –mediante un comprador- y retemporización), pasan ala UART (*Universal Asynchronous Receiver Transmitter*) del ordenador, de forma que para la CPU todo el proceso luminoso es transparente. En el proceso de transmisión los bits viajan mediante haces de pulsos, donde el cero lógico se representa por existencia de luz y el uno lógico por su ausencia. Debido a que el enlace es punto a punto, el cono de apertura visual es de 30 grados y la transmisión es *Half Duplex*, esto es, cada extremo del enlace emite por separado.

5.2.1.3.1.2. CAPA DE ENLACE EN INFRARROJOS

Tras la capa física se encuentra la capa de enlace, conocida como IrLAP (*Infrared Link Access Protocol*), que se encarga de gestionar las tareas relacionadas con el establecimiento, mantenimiento y finalización del enlace entre los dos dispositivos que se comunican. IrLAP constituye una variante del protocolo de transmisiones asíncronas HDLC (*Half Duplex Line Control*) adaptada para resolver los problemas que plantea el entorno de radio. El enlace establece dos tipos de estaciones participantes, una actúa como maestro y otra como esclavo. El enlace puede ser punto a punto o punto a multipunto, pero en cualquier caso la responsabilidad del enlace recae en el maestro, todas las transmisiones van a el o vienen desde el.

5.2.1.3.1.3. CAPA DE RED EN INFRARROJOS

Está definida por el protocolo IrLMP (*Infrared Link Management Protocol*), la capa inmediata superior a la IrLAP, se encarga del seguimiento de los servicios (impresiones, fax y módem), así como de los recursos disponibles por otros equipos, es decir, disponibles para el enlace.

5.2.1.3.1.4. CAPA DE TRANSPORTE EN INFRARROJOS

IrTP (*Infrared Transport Protocol*), se ocupa de permitir que un dispositivo pueda establecer múltiples haces de datos en un solo enlace, cada uno con su

propio flujo de control. Se trata de multiplexar el flujo de datos, lo cual permite, por ejemplo, poner en cola un documento a la impresora mientras se carga el correo electrónico del servidor. Este software, de carácter opcional –dado que no es necesario para la transferencia básica de ficheros- resulta útil cuando se establece un enlace entre una PDA (*Personal Digital Assistant*) y la LAN.

En las aplicaciones de LAN inalámbricas, el modo operativo consiste en modular la intensidad de la luz producida por el emisor mediante una señal modulada eléctricamente. El detector percibe las variaciones de intensidad de la señal infrarroja y las convierte directamente en una señal eléctrica equivalente. Este modo de operación se llama IMDD (*Modulación* de Intensidad Con Detección Directa) y se emplean en diversos métodos de modulación, incluida la modulación en banda base.

En las aplicaciones de LAN inalámbricas como la luz no necesita propagarse dentro de una fibra óptica, es preciso hacerla más difusa para que no cause daños en los ojos de las personas. Pero el LED produce una luz que comprende una banda de frecuencia que, con los bajos niveles de potencia de salida empleados, es totalmente segura. El ancho de banda disponible para la modulación de los LED es de 20 MHz, lo que limita a menos de 10 Mbps la tasa de bits máxima que es posible usar. Por su bajo costo, lo normal es utilizar LED en los casos en que se requiere tasas de bits de este nivel o menores.

Si se quiere una tasa de bits mayor a 10Mbps es necesario utilizar diodos de láser. El ancho de banda de modulación disponible para estos dispositivos es de varios cientos de MHz. La amplia banda de frecuencias asociados a los LED obliga a usar en el receptor un filtro óptico con un pasa banda ancho que permita detectar toda la señal transmitida. No obstante, esto incrementa la señal de ruido en el receptor, y esto a su vez dificulta el diseño del receptor cuando la tasa de bits es alta.

5.2.1.3.1.5. TOPOLOGÍAS PARA INFRARROJOS

En los enlaces con tecnología de infrarrojos se pueden utilizar uno de los dos modos: *punto a punto* o *difuso*. En el modo punto a punto en emisor apunta directamente hacia el detector (que en la práctica es un fotodiodo), y esto permite usar emisores de menor potencia y detectores menos sensibles. Este modo de

funcionamiento es más apropiado para establecer un enlace inalámbrico entre dos equipos.

En las aplicaciones de LAN inalámbricas se requiere un modo de operación de uno a muchos (difusión). Para lograr esto, la salida de la fuente de infrarrojo se difunde ópticamente de modo que la luz se distribuya por un área angular amplia. Este es el modo difuso y tiene tres modos de operación alternativos:

1. Con el modo básico cada computador tiene asociado un emisor óptico de ángulo grande y detector. La señal de infrarrojo producida por cualquier emisor se recibe en todos los detectores después de múltiples reflexiones dentro del recinto. El efecto de este modo operativo es que varias copias de la misma señal fuente a cada detector con distintos retardos de propagación, determinados por el camino físico que haya seguido cada señal. Esto es lo que se denomina *Dispersión Multicamino* y su efecto es una dispersión de retardo, ya que los pulsos que representan a los bits individuales dentro del flujo de bits transmitidos se extienden o ensanchan. Esto hace que las señales asociadas a un bit/símbolo previo interfieran las señales asociadas al siguiente bit/símbolo, a esto se le llama: ISI (interferencias entre símbolos). Como con las ondas de radio, la amplitud de las diversas señales reflejadas varían respecto a la de la señal más directa en función del camino seguido y la atenuación en que hayan incurrido. En una oficina ordinaria, es posible recibir señales significativas con atenuaciones de retardo tan altas como 100 nanosegundos. Este modo de operación sólo es satisfactorio con tasas de bits hasta 1Mbps, ya que con tasas mayores los efectos de ISI se incrementan considerablemente.
2. Con infrarrojos y radio, además de la ecualización, se puede reducir los efectos de la dispersión de retardo empleando múltiples emisores y detectores direccionales. Cuando se sigue esta estrategia todos los emisores y detectores se orientan de modo que apunten a la dirección general de una cúpula reflectora fija en el techo, denominada satélite. A fin de maximizar la potencia de la señal recibida y minimizar las reflexiones, la señal de origen se enfoca. ópticamente para formar un haz relativamente angosto. La forma de la cúpula reflectora se escoge de modo que asegure que todas las señales

transmitidas serán recibidas en todos los detectores. Para reducir los efectos de multicamino, la abertura de los detectores se reduce de modo que sólo reciban la señal directa del satélite.

3. El satélite anterior sólo actúa como reflector de la luz. Por tanto, si se quiere obtener una potencia de señal aceptable en el detector, la potencia de la señal emitida tendrá que ser relativamente alta. En el caso de dispositivos portátiles que obtienen su potencia de baterías, esta es una desventaja que hace necesario refinar el esquema básico para utilizar un satélite activo. En este esquema se distribuye una serie de detectores alrededor de la cúpula, junto con un conjunto de emisores de infrarrojo. Todas las señales recibidas por uno o más conjuntos de detectores sarán repetidas después por los emisores. Esto significa que la potencia de la señal emitida por cada dispositivo portátil puede ser mucho más baja, ya que sólo necesita lo suficiente para formar un camino directo hacia el satélite.

5.2.1.3.2. RADIOFRECUENCIA

El medio que es más usado en la actualidad son las señales de Radiofrecuencia, las cuales tienen un amplio campo de aplicación; entre ellos la difusión de radio y televisión y las redes de telefonía celular. Este tipo de ondas no tienen el inconveniente de que los transceptores deben tener una línea de visibilidad para transmitir entre ellos información, además, se alcanzan mayores velocidades y se pueden implementar en modo infraestructura.

Por otro lado, debido al gran número de aplicaciones existentes en la actualidad, se hace necesaria una asignación oficial de bandas de frecuencia específica para cada una de ellas. Históricamente, esta asignación se hacia a nivel nacional, pero cada vez se están firmando más convenios internacionales que determinan bandas de frecuencia concretas para las aplicaciones que tienen alcance internacional.

Los requisitos para que las emisiones de radio a una banda de frecuencia específica y para que los receptores correspondientes sólo seleccionen las señales que caigan en dicha banda implican que, en general, los circuitos asociados a los sistemas basados en radio sean más complejos que los empleados en los sistemas

ópticos de infrarrojos. No obstante, el uso tan difundido de radio implica que es imposible llevar a la práctica diseños de sistemas de radio muy complejos con costos razonables.

5.2.1.3.2.1. FACTORES QUE INFLUYEN EN LA COMUNICACIÓN POR RADIOFRECUENCIA

Perdida de camino. En el diseño de todos los receptores de radio se contempla que operen con una relación señal-ruido SNR (*Signal to Noise Ratio*) específica; es decir, la razón entre la señal recibida y la potencia de la señal de ruido del receptor no debe ser menor que cierto valor especificado. En general, la complejidad (y en consecuencia el costo) del receptor aumentará conforme disminuya el SNR. Por lo tanto, la disminución en el costo de los ordenadores portátiles implica que el costo aceptable de la unidad de interfaz con la red de radio debe ser comparable con el costo de los computadores portátiles. Esto significa que la SNR del receptor de radio se debe fijar en más alto posible.

La potencia en la señal en el receptor es una función no sólo de la potencia de la señal transmitida, sino también de la distancia entre el transmisor y el receptor. En el espacio libre, la potencia de una señal de radio decae en proporción inversa al cuadrado de la distancia del origen.

En interiores, el decaimiento se incrementa más debido, en primer lugar, a la presencia de objetos como muebles y personas y, en segundo lugar, a la interferencia destructiva de la señal transmitida que causan las señales reflejadas en dichos objetos. Todo esto se combina para producir lo que se llama *pérdida de camino* del canal de radio.

Para que un receptor de radio pueda operar con una SRN aceptable, debe trabajar con un nivel de potencia de transmisión tan alto como sea posible o con un alcance de cobertura limitado, o las dos cosas. En la práctica con los computadores portátiles, la potencia de la señal transmitida está limitada por el consumo de potencia de unidad de interfaz con la red de radio, que significa un aumento en la carga sobre la batería del computador. Es por estas razones que el alcance de la cobertura de una LAN *ad hoc* suele ser más limitado que la de una LAN de *infraestructura*.

Interferencia del canal adyacente. Las ondas de radio se propagan a través de casi cualquier objeto sin mucha atenuación, es posible que sufra alguna interferencia de otros transmisores que estén operando en la misma banda de frecuencias y están situados en una habitación adyacente dentro del mismo edificio o en otros edificios.

En el caso de las redes *ad hoc*, como es posible establecer varias de estas LAN en recintos adyacentes, es preciso adoptar técnicas que permitan la coexistencia de varios usuarios de la misma banda de frecuencia.

En el modo *infraestructura*, como la topología es conocida y el área total de cobertura de la red inalámbrica es mucho más amplia que el ancho de banda disponible se puede dividir en varias sub-bandas de modo tal que las áreas de cobertura de sub-bandas adyacentes utilicen frecuencias distintas. El esquema general se conoce como patrón de repetición de tres celdas, aunque es posible formar patrones más grandes. La proporción de ancho de banda disponible en cada celda se escoge de modo tal que suministre un nivel de servicio aceptable para el número de usuarios activos que se esperan estarán dentro de esa área. Con esto se aprovecha mejor el ancho de banda disponible y, al asegurar que cualquier celda adyacente utilice una frecuencia distinta, también reducirá considerablemente el nivel de interferencia del canal adyacente.

Multicamino. Las señales de radio, al igual que las ópticas, sufren el efecto multicamino; es decir, en cualquier instante dado el receptor recibe múltiples señales que se originan en el mismo transmisor.

Existe también un problema llamado *desvanecimiento selectivo de frecuencias* causado por la variación de las longitudes de camino de las diferentes señales recibidas. Esto produce cambios de fase relativos que pueden hacer que las diversas señales reflejadas atenúen significativamente la señal de camino directo y, en el límite, se cancelan entre si. Esto se denomina *desvanecimiento de Rayleigh.* En la práctica, la amplitud de la onda reflejada es una fracción de la onda directa, y el grado de atenuación dependerá de la naturaleza del material reflejante. Una solución a este problema aprovecha el hecho de que la longitud de onda asociada a las señales de radiofrecuencia es muy corta, y por tanto es sensible a pequeñas variaciones en la posición de la antena. Para evitar el desvanecimiento, es común

usar dos antenas con una separación física entre ellas igual a una cuarta parte de la longitud de la onda. Las señales recibidas de ambas antenas se combinan para formar la señal recibida compuesta. A esta técnica se le conoce como *diversidad espacial*.

Otra solución consiste en valerse de la técnica llamada *ecualización*. Las imágenes retardadas y atenuadas de la señal directa se restan de la señal recibida real. Puesto que las señales reflejadas variarán dependiendo de las ubicaciones del transmisor y del receptor, el proceso tendrá que ser adaptativo. Por ello el circuito empleado se denomina *ecualizador adaptativo*. El emplear estos circuitos eleva el costo del receptor.

5.2.1.3.2.2. TECNOLOGÍAS DE TRANSMISIÓN PARA RADIOFRECUENCIA

Para este medio inalámbrico, existe la tecnología de espectro ensanchado que consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta lo que se hace es repartirla por toda la banda disponible. Este ancho de banda total se comparte con el resto de usuarios que trabajan en la misma banda frecuencial. Tiene muchas características que le hacen sobresalir sobre otras tecnologías de radiofrecuencias (como las de banda estrecha, que utiliza microondas), ya que, posee excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación. Esta tecnología es necesaria porque, para poder coexistir las redes inalámbricas (mediante radiofrecuencia), con distintos dispositivos que utilizan la misma banda para transmitir, se necesita tener un alto nivel de rechazo de interferencia de co-canal. Esta, como muchas otras tecnologías, proviene del sector militar.

Existen dos tipos de tecnologías de espectro ensanchado:

- DSSS (*Direct Sequence Spread Spectrum* / Espectro Ensanchado por Secuencia Directa)
- FHSS (*Frequency Hopping Spread Spectrum* / Espectro Ensanchado por Salto en Frecuencia)

El Espectro Ensanchado por Secuencia Directa (DSSS) es una técnica que consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de RF. En recepción es necesario realizar el proceso inverso para obtener la señal de información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barrer (también llamado código de dispersión o *PseudoNoise*). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de secuencia sería:

+1-1+1+1-1+1+1+1-1-1-1-1

La secuencia binaria pseudoaleatoria se conoce también como *secuencia de dispersión*, en la que cada bit se conoce como un *chip*, la tasa de bits de transmisión resultante como la *tasa de chips* y el número de bits de la secuencia como el *factor de dispersión*.

Todos los miembros de la misma LAN inalámbrica conocen la secuencia binaria pseudoaleatorio que se está utilizando. Todas las tramas de datos transmitidas van precedidas por una secuencia de preámbulo seguida de un delimitador de principio de trama. Una vez que han remodulado la señal transmitida, todos los receptores buscan primero la secuencia de preámbulo conocida y, una vez que lo encuentran, comienzan a interpretar el flujo de bits recibido según los límites de bits correctos de los datos de origen. A continuación, los receptores esperan la llegada del delimitador de principio de trama y luego proceden a recibir el contenido de la trama. El o los destinatarios están determinados por l dirección de destino en la cabecera de la trama, igual que siempre.

Sólo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Las estaciones que pertenecen a la misma LAN inalámbrica ocupan la misma banda defrecuencia asignada y utilizan la misma secuencia binaria pseudoaleatoria.

Por ello es necesario usar un método de MAC apropiado que asegure que sólo se realizará una transmisión en cualquier momento dado.

El gran ancho de banda que se requiere para las LAN inalámbricas hace poco recomendables los esquemas de modulación que implican variaciones en la amplitud, ya que los amplificadores de potencia que son lineales dentro de anchos de banda amplios tienen un costo elevado y además consumen una cantidad importante de potencia. Por ello se emplean esquemas de modulación basados en variaciones en una fase de una sola portadora de amplitud constante.

Se tienen definidos dos tipos de modulaciones para la señal de información una vez que se sobrepone la señal de chip tal y como especifica el estándar IEEE 802.11: la modulación DBPSK, (Modulación de cambio de fase binario diferencial, *Differential Binary Phase Shift Keying*) y la modulación DQPSK, (Modulación de cambio de fase en cuadratura diferencial, *Differential Quadrature Phase Shift Keying*), proporcionando unas velocidades de transferencia de 1 y 2 Mbps respectivamente.

La modulación para la banda de los 5 GHz utiliza otro tipo de modulación: OFDM (*Ortogonal Frecuency Division Multiplexing*).

Este tipo de modulación utiliza múltiples portadoras. El principio de funcionamiento consiste en dividir primero la señal binaria de altas tasas de bits que se va a transmitir en varios flujos de menor tasa de bits. Después cada uno de estos flujos modula una subportadora distinta – de la banda de frecuencias asignada- como el esquema de portadora única. La diferencia es que, dada la relativa baja tasas de bits por portadora, el nivel de ISI se reduce bastante, lo que hace innecesario el empleo de ecualizadores. Aunque no desaparece la posibilidad que haya desvanecimiento selectivo de frecuencias, es probable que sólo una (o un número pequeño) de las subportadoras resulte afectada. En la práctica las subportadoras empleadas son múltiplos enteros de la primera subportadora y por ello a este esquema de le denomina *Multiplexión por división ortogonal de frecuencias* (OFDM).

En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa, DSSS, opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en un total de 14 canales con un ancho de

banda por canal de 5 MHz de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular.

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema, si la separación entre las frecuencias centrales es como mínimo de 30 MHz. Esto significa que de los 83.5 MHz de ancho de banda total disponible se puede obtener un total de 3 canales independientes que pueden operar simultáneamente en una determinada zona geográfica sin que aparezcan interferencias en un canal procedentes de los otros dos canales. Esta independencia entre canales permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales

CANAL	FREC U.S.A.	FREC EUROPA	FREC JAPON
1	2412 Mhz	N/A	N/A
2	2417 Mhz	N/A	N/A
3	2422 Mhz	2422 Mhz	N/A
4	2427 Mhz	2427 Mhz	N/A
5	2432 Mhz	2432 Mhz	N/A
6	2437 Mhz	2437 Mhz	N/A
7	2442 Mhz	2442 Mhz	N/A
8	2447 Mhz	2447 Mhz	N/A
9	2452 Mhz	2452 Mhz	N/A
10	2457 Mhz	2457 Mhz	N/A
11	2462 Mhz	2462 Mhz	N/A
12	N/A	N/A	N/A

Cuadro 4 Tabla de Frecuencias DSSS

El Espectro Ensanchado por Salto en Frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada *dwell time* e inferior a 400ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo. La banda de frecuencia asignada se divide

en varias sub-bandas de menor frecuencia llamadas *canales*. Cada canal tiene el mismo ancho de banda, que esta determinado por la tasa de bits de datos y el método de modulación empleado.

Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer. La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología se puede tener más de un Access Point en la misma zona geográfica sin que existan interferencias si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

El patrón de uso de canal es pseudoaleatorio y se denomina *secuencia de salto*; el tiempo que se transmite por cada canal es el periodo de *chip* y la tasa de salto es la *tasa de chip*.

Existen dos métodos de operación por salto de frecuencia que están determinados por la razón entre la tasa de chip y la tasa de datos de origen.

Cuando la tasa de chip es más alta que la tasa de datos, el modo operativo se conoce como *salto de frecuencia rápido*, mientras que si la tasa de chip es más baja que la tasa de datos se conoce como *salto de frecuencia lento*. En ambos casos se utiliza una frecuencia portadora en el centro de cada canal.

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación el efecto global es que, aunque vamos cambiando de canal físico con el tiempo se mantiene un único canal lógico a través del cual se desarrolla la comunicación. Para un usuario externo a la comunicación, la recepción de una señal FHSSS equivale a la recepción de ruido impulsivo de corta duración. El estándar IEEE 802.11 describe esta tecnología mediante la modulación en frecuencia FSK (*Frequency Shift Keying*) y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps bajo condiciones de operación óptimas.

El salto de frecuencia tiene una ventaja sobre la frecuencia directa: tiene la capacidad de evitar el empleo de canales seleccionados dentro de la banda de

frecuencia global asignada. Ello ofrece una especial utilidad en el caso de las bandas ISM (bandas de 920 a 928 MHZ, 2400 a 2483.5 MHz y 5725 a 5850 MHZ), debido a que una o más fuentes de interferencia de banda angosta de alta potencia pueden estar presentes dentro del campo de cobertura de la LAN. Con la secuencia directa la señal de interferencia queda dispersa sobre la banda de frecuencias asignada, con fuentes de interferencia de alta potencia ésta puede alcanzar de todos modos un nivel de interferencia significativo que, en el límite, puede imposibilitar el uso de ciertas bandas.[9]

5.2.1.3.3. MICROONDAS TERRESTRES

La antena más común para microondas es la parabólica. El tamaño normal es de 3 metros de diámetro. Esta se debe fijar rígidamente en la parte más alta del edificio y apuntando hacia otra antena receptora. Lo anterior con el fin de conseguir mayores separaciones entre ellas y evitar posibles obstáculos en la transmisión.

Para hacer transmisiones a larga distancia, se utiliza la concatenación de enlaces punto a punto entre las antenas situadas en torres adyacentes, hasta cubrir la distancia requerida.

El uso principal de los sistemas por microondas son los servicios de telecomunicaciones de larga distancia, como una alternativa del cable coaxial o las fibras ópticas. Para determinadas distancias, las microondas necesitan menos repetidores o amplificadores que el cable coaxial, pero las antenas deben estar perfectamente alineadas.

Un uso cada vez más frecuente es en enlaces punto a punto entre edificios. Y las aplicaciones típicas son circuitos cerrados de TV o la interconexión de redes locales. Además también son utilizadas en aplicaciones denominadas "*by-pass*", con las que una compañía puede establecer enlaces privados hasta el centro proveedor de transmisiones a larga distancia, evitando la contratación del servicio de telefonía local.

El rango de las microondas cubre gran parte del espectro electromagnético. La banda de frecuencias esta entre los 2 y 40 GHz. Cuanto mayor sea la frecuencia

[9] *http://www.microalcarria.com/descargas/documentos/Wireless/Redes_Inalambricas_802.11b.pdf*
http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

utilizada, mayor es el ancho de banda disponible, y con esto, mayor velocidad de transmisión.

Los sistemas que utilizan microondas, amplificadores y/o repetidores se pueden distanciar de 10 a 100 Km. Con el aumento creciente del uso de las microondas, las áreas de cobertura se pueden solapar, haciendo que las interferencias sean un peligro potencial. Por eso la asignación de bandas tiene que realizarse apegado a una regularización estricta.

Las bandas más utilizadas para transmisiones a largas distancias están entre 4 GHz y 6 GHz. Pero la banda de 11 GHz esta empezando a ser más utilizada debido a la saturación que están sufriendo las otras bandas. Para enlaces cortos punto a punto son utilizadas las altas frecuencias como es la banda de 22 GHz. Las bandas de frecuencias altas son menos recomendables para largas distancias debido a la mayor atenuación que sufrirían, pero son bastante adecuadas para distancias cortas y con la ventaja que a mayor frecuencia las antenas utilizadas son más pequeñas y baratas.

A continuación se presenta una tabla con la comparación de diferentes frecuencias de bandas utilizadas comúnmente para microondas y la velocidad de transmisión que se tienen con ellas.

Banda (GHZ)	Velocidad transmision de (Mbps)
2	12
6	90
11	135
18	274

Cuadro 5 Tabla de Frecuencias y Velocidades de Transmisión Utilizadas Comúnmente en Microondas

5.2.1.4. NIVEL DE ACCESO AL MEDIO DEL 802.11

Los diferentes métodos de acceso de IEEE802 están diseñados según el modelo OSI y se encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC.

Además, la capa de gestión MAC controlará aspectos como sincronización y los algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura. Por último, veremos el aspecto y los tipos de tramas MAC.

5.2.1.4.1. DESCRIPCIÓN FUNCIONAL MAC

La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades básicas: la función de coordinación puntual (PCF) y la función de coordinación distribuida (DCF).

DCF

Es el estándar básico del mecanismo de acceso CSMA/CA. Al igual que Ethernet, primeramente verifica que el enlace radial esta libre para transmitir. Para evitar colisiones, las estaciones utilizan un backoff al azar después de cada trama.

En algunas circunstancias el DCF utilizará las técnicas de CTS/RTS para reducir las posibilidades de colisión.

PCF

La función de coordinación provee servicios libres de contiendas. Estaciones especiales llamadas Puntos Coordinadores son usadas para asegurar que el medio es proveído sin contienda. Los Puntos Coordinadores residen en los Access Point , por lo tanto, son usados en las redes de Infraestructura. Para ganar prioridad sobre servicios basados en contienda, el PCF permite a las estaciones transmitir tramas después de un corto período.

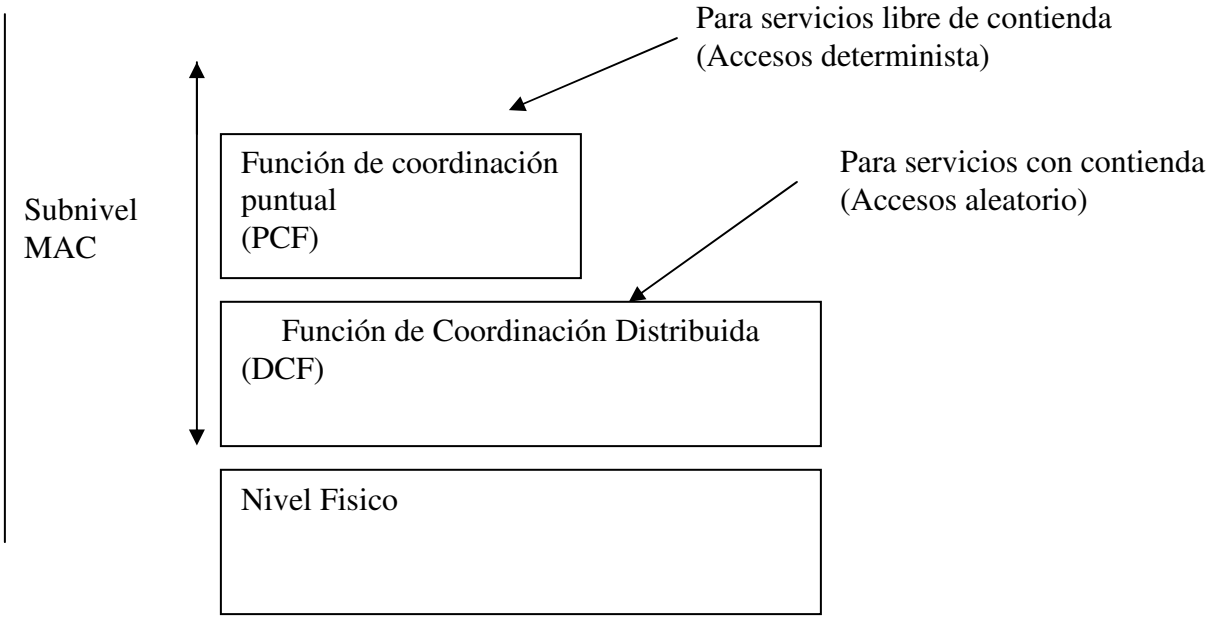


Figura 13 Diagrama del Acceso al medio 802.11

5.2.1.4.1.1. FUNCIÓN DE COORDINACIÓN DISTRIBUIDA

Definimos *función de coordinación* como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio.

El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos.

Las características de DFC las podemos resumir en estos puntos:

- Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio
- Necesario reconocimientos ACKs, provocando retransmisiones si no se recibe
- Usa campo Duration/ID que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán al escuchar cuando el canal volverá a quedar libre

- Implementa fragmentación de datos
- Concede prioridad a tramas mediante el espaciado entre tramas (IFS)
- Soporta Broadcast y Multicast sin ACKs

5.2.1.4.1.1.1. PROTOCOLO DE ACCESO AL MEDIO CSMA/CA Y MACA

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA (Carrier Sense Multiple Access / Collision Advoidance). Este algoritmo funciona tal y como describimos a continuación:

- Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).
- Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).
- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
- Una vez finaliza esta espera debida a la ocupación del medio la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado *ventana de contienda* (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.
- Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo. Por otra parte, el valor del slot time es 20µseg.

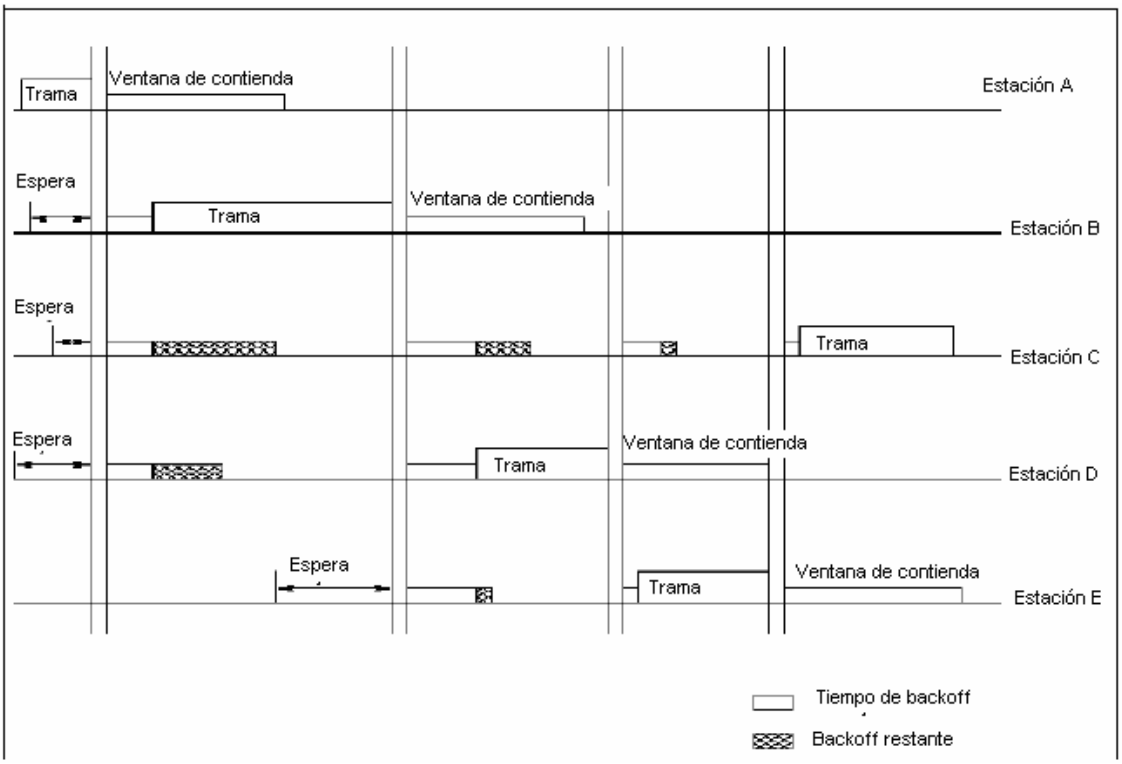


Figura 14 Método de acceso al medio

Sin embargo, CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas que intentaremos resolver con alguna modificación. Los dos principales problemas que podemos detectar son:

- Nodos ocultos. Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye
- Nodos expuestos. Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone 802.11 es MACA o MultiAccess Collision Avoidance. Según este protocolo, antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con

una trama CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS
- Al escuchar un CTS, hay que esperar según la longitud

La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

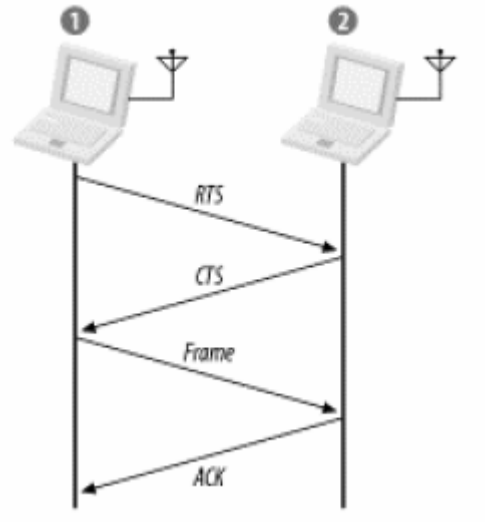


Figura 15 MACA o MultiAccess Collision Avoidance

5.2.1.4.1.1.2. ESPACIADO ENTRE TRAMAS IFS

El tiempo de intervalo entre tramas se llama IFS. Durante este periodo mínimo, una estación STA estará escuchando el medio antes de transmitir. Se definen cuatro espaciados para dar prioridad de acceso al medio inalámbrico. Veámoslos de más cortos a más largos:

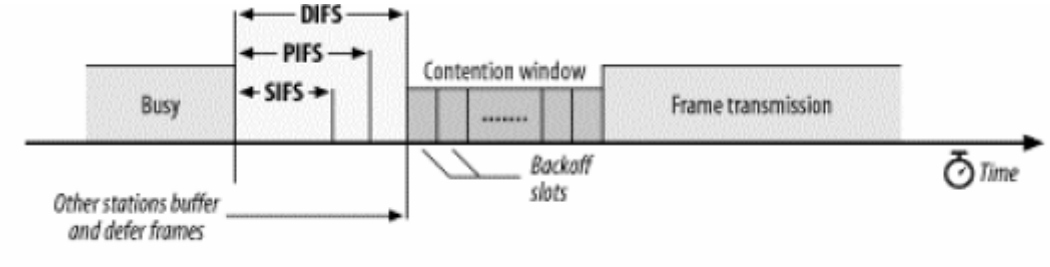


Figura 16 Espaciado entre tramas IFS

- SIFS (Short IFS). Este es el periodo más corto. Se utiliza fundamentalmente para las transmisiones de alta prioridad como RTS/CTS y los reconocimientos. Las transmisiones de alta prioridad pueden comenzar una vez que el SIFS haya concluido. Una vez que estas transmisiones comienzan, el medio se pone en ocupado, por tanto, tramas transmitidas después de que el SIFS termine, tienen myor prioridad sobre tramas que pueden ser transmitidas después de intervalos grandes.
- PIFS (PCF). Es utilizado por STAs para ganar prioridad de acceso en los periodos libres de contienda. Lo utiliza el PC para ganar la contienda normal, que se produce al esperar DIFS.
- DIFS (DCF). Es el tiempo de espera habitual en las contiendas con mecanismo MACA. Se utiliza pues para el envío de tramas MAC MPDUs y tramas de gestión MMPDUs.
- EIFS (Extended IFS). Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución.

5.2.1.4.1.1.3 CONOCIMIENTO DEL MEDIO

Las estaciones tienen un conocimiento específico de cuando la estación, que en estos momentos tiene el control del medio porque está transmitiendo o recibiendo, va a finalizar su periodo de reserva del canal.

Esto se hace a través de una variable llamada NAV (Network Allocation Vector) que mantendrá una predicción de cuando el medio quedará liberado.

Tanto al enviar un RTS como al recibir un CTS, se envía el campo Duration/ID con el valor reservado para la transmisión y el subsiguiente reconocimiento. Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo Duration/ID. En realidad, hay una serie de normas para modificar el NAV, una de ellas es que el NAV siempre se situará al valor más alto de entre los que se disponga.

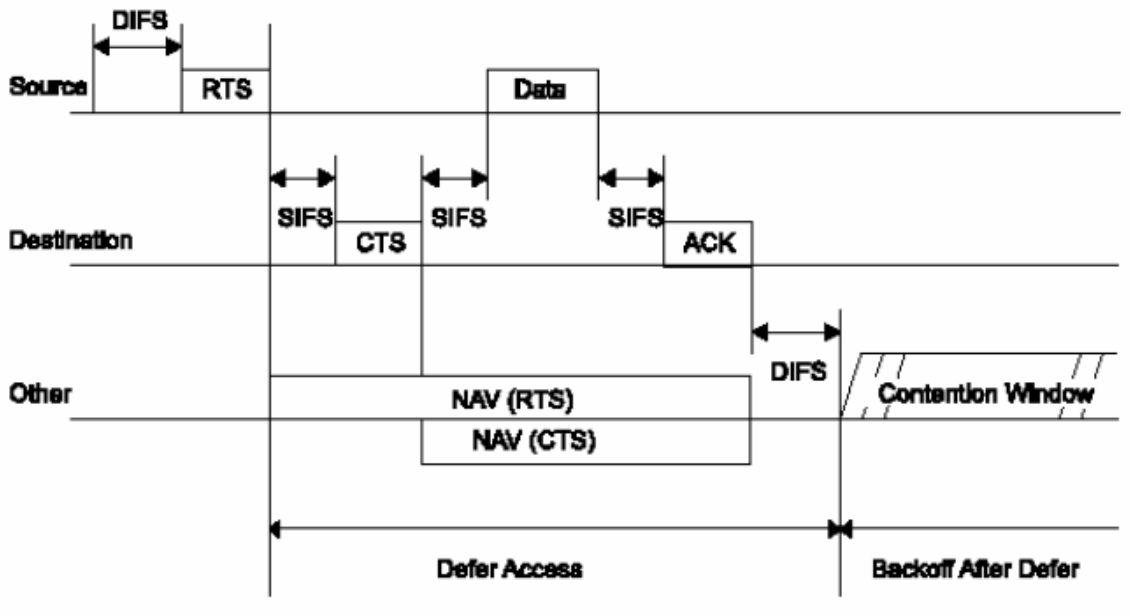


Figura 17 Conocimiento del medio

5.2.1.4.1.2. FUNCIÓN DE COORDINACIÓN PUNTUAL

Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual, PCF, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. El estándar IEEE 802.11, en concreto, define una técnica de interrogación circular desde el Access Point para este nivel.

Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio. En la figura 8 mostramos la relación entre estos dos modos de operación.

Estos dos métodos de acceso pueden operar conjuntamente dentro de una misma celda o conjunto básico de servicios dentro de una estructura llamada *supertrama*. Un parte de esta *supertrama* se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finaliza este periodo el Access Point toma el medio y se inicia un periodo libre de contienda n el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas.

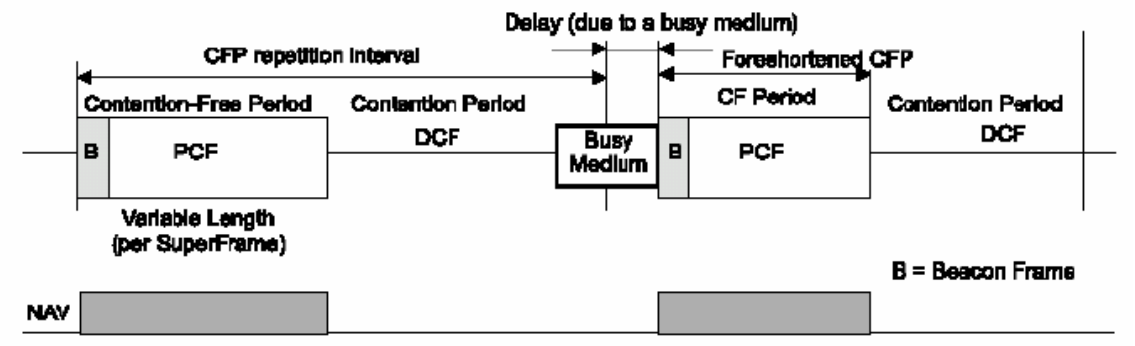


Figura 18Función de coordinación puntual

Un aspecto previo a comentar el funcionamiento de PFC es que es totalmente compatible con el modo DFC, observándose que el funcionamiento es transparente para las estaciones. De esta manera, una estación se asociará (se dará de alta en un modo infraestrucutra) de modo que pueda actuar en el periodo CFP, declarándose como CFPollable, o por el contrario, se situará su NAV según las indicaciones del punto de coordinación.

Existe un nodo organizador o director, llamado punto de coordinación o PC. Este nodo tomará el control mediante el método PIFS, y enviará un CF-Poll a cada estación que pueda transmitir en CFP, concediéndole poder transmitir una trama MPDU. El PC mantendrá una lista Pollable donde tendrá todos los datos de las estaciones que se han asociado al modo CF-Pollable. La concesión de transmisiones será por riguroso listado y no permitirá que se envíen dos tramas hasta que la lista se haya completado.

El nodo utilizará una trama para la configuración de la supertrama, llamada Beacon, donde establecerá una CFRate o tasa de periodos de contienda. Pese a que el periodo de contienda se puede retrasar por estar el medio ocupado, la tasa se mantendrá en el siguiente periodo con medio libre.

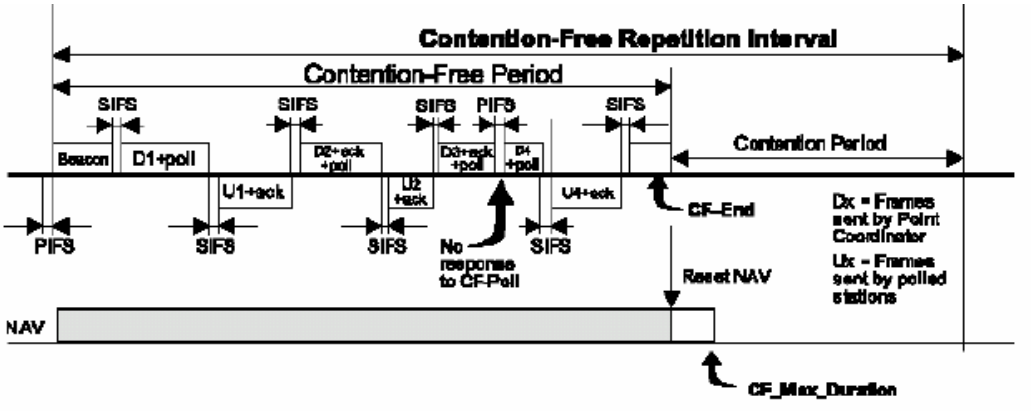


Figura 19

Como podemos observar, la transmisión de CF-Polls espera un tiempo SIFS.También podemos ver que si una estación no aprovecha su CF-Poll se transmite a la siguiente en el listado Pollable.

Las estaciones que no usen el CF, situarán su NAV al valor del final del CF y luego lo resetearán para poder modificarlo en el periodo de contienda en igualdad de condiciones.

Un problema importante que podemos encontrarnos en solapamiento de redes, ocurrirá cuando varios sistemas con coordinación puntual compartan una tasa semejante. Una solución suele ser establecer un periodo de contienda entre PCs para ganar el medio esperando un tiempo DIFS+ BackOff (1-Cwmin). Sin embargo, podemos encontrarnos con mayores dificultades que exigirían un estudio diferenciado.

5.2.1.4.2. FORMATO DE LAS TRAMAS MAC

Las tramas MAC contienen los siguientes componentes básicos:

- Una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia
- Un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama
- Un secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits

Las tramas MAC se pueden clasificar según tres tipos:

- Tramas de datos.
- Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda
- Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el Access Point.

El formato de la trama MC genérica tiene el siguiente aspecto:

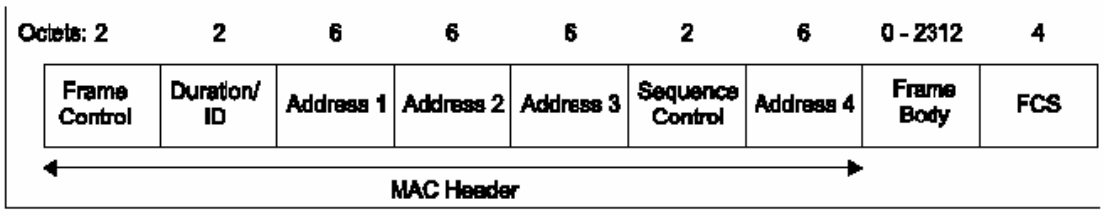


Figura 20 Formato de la trama

Los campos que componen esta trama son:

- Campo de control. Merece examinar aparte. Lo haremos más abajo.
- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.
- Campos address1-4. Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el Access Point origen y el Access Point destino.
- Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.
- FCS. Contiene el checksum.

Los campos de control de trama tienen el formato siguiente:

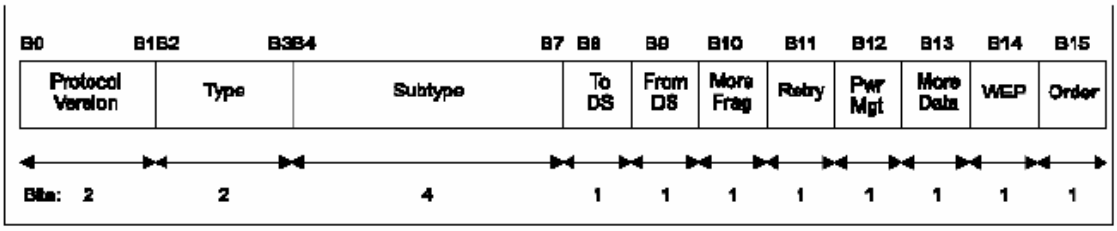


Figura 21

- Versión.
- Type/Subtype. Mientras tipo identifica si la trama es del tipo de datos, control o gestión, el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.
- ToDS/FromDS. Identifica si la trama si envía o se recibe al/del sistema de distribución.
- En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS.
- Más fragmentos. Se activa si se usa fragmentación.
- Retry. Se activa si la trama es una retransmisión.
- Power Management. Se activa si la estación utiliza el modo de economía de potencia.
- More Data. Se activa si la estación tiene tramas pendientes en un Access Point.
- WEP. Se activa si se usa el mecanismo de autenticación y encriptado.
- Order. Se utiliza con el servicio de ordenamiento estricto, en el cual no nos detendremos.

5.2.1.4.3. DIRECCIONAMIENTO EN MODO INFRAESTRUCTURA

Veamos de manera específica como funciona el direccionamiento en modo infraestructura. Como hemos comentado con anterioridad, el caso más complejo de direccionamiento se produce cuando una estación quiere transmitir a otra ubicada en otro BSS o sistema de servicios básicos.

En este caso los campos ToDS=FromDS=1 y las direcciones de cada uno de los componentes por los que pasa la trama toman el siguiente valor en la trama MAC, quedando la dirección 1 como el nodo destino, la dirección 2 será la del Access Point final, la dirección 3 sería la del Access Point origen y por último, la dirección 4 sería la del nodo origen.

En la figura podemos ver un ejemplo de transmisión del nodo A al nodo E.

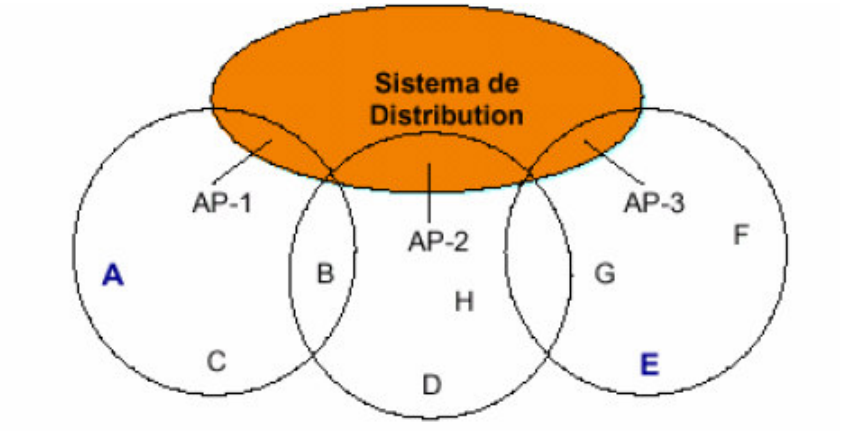


Figura 22

5.2.1.4.4. SERVICIOS DEL SISTEMA DE DISTRIBUCIÓN ASOCIACIÓN.

La especificación IEEE802.11 define el sistema de distribución como la arquitectura encargada de interconectar diferentes IBSS o redes inalámbricas independientes.

El componente fundamental de este sistema de distribución es el Access Point, y además la especificación define lo que llama los servicios de distribución que facilitan y posibilitan el funcionamiento en modo infraestructura. Se definirán servicios diferentes para cada componente, según se tratase de Access Point o estación.

Enumeraremos los servicios y expondremos el servicio de asociación, por su carácter básico. Los cinco primeros los implementa el Access Point y los cuatro últimos la estación. La especificación añade en algunos servicios la información necesaria para implementarlo pero no se detiene en esta implementación.

- Distribución. Se encarga de llevar un paquete del Access Point de origen al de destino.
- Integración. Se encarga de la función de pasarela con otros sistemas IEEE802.x. En concreto, define el componente portal que se encargará de aspectos necesarios como redireccionamiento.
- Asociación. Servicio necesario para que una estación pueda adherirse al modo infraestructura y utilizar sus servicios.
- Reasociación. Consiste en el campo de Access Point al que se asocia la estación para adherirse al modo infraestructura. También se utiliza para modificar las características de la asociación.
- Autenticación y Deautenticación. Proceso necesario para que la estación se pueda conectar a la wireless LAN y consiste en la identificación de la estación.El proceso pues de conexión, pasa por la autenticación previamente a la asociación.
- Privacidad. Este servicio utilizará WEP para el encriptado de los datos en el medio.
- Reparto de MSDUs entre STAs. Este es el servicio básico de intercambio.

5.2.1.4.4.1. ALGORITMO DE ASOCIACIÓN ACTIVA.

Veremos como ejemplo como funciona el sencillo algoritmo de asociación activa, según la cual la estación utilizará las tramas de prueba y respuesta para mantenerse asociada a un Access Point que puede variar si tiene la condición de móvil.

El algoritmo consiste en los siguientes pasos:

- El nodo envía una trama de prueba (Probe)
- Los puntos de acceso alcanzados responden con una trama de respuesta.
- El nodo seleccionará generalmente por nivel de señal recibida el Access Point al que desea asociarse, enviándole una trama de requerimiento de asociación
- El Access Point responderá con una respuesta de asociación afirmativa o negativa

La asociación activa implica que la estación continuará enviando este tipo de tramas y podrá provocar una reasociación en función de los parámetros de selección que él mismo utilice y defina.

5.2.1.4.5. SUBNIVEL DE GESTION MAC

La subcapa de gestión MAC implementa las siguientes funcionalidades:

- Sincronización.
- Gestión de potencia
- Asociación-Reasociación
- Utiliza el MIB o Management Information Base

Se describirán los primeros dos puntos.

5.2.1.4.5.1. SINCRONIZACIÓN

La sincronización se consigue mediante una función de sincronización (TSF) que mantendrá los relojes de las estaciones sincronizados. Según el modo de operación, distinguiremos el modo de funcionamiento.

En el modo infraestructura, la función de sincronización recaerá en el Access Point, de tal manera que el Access Point enviará la sincronización en la trama portadora o Beacon y todas las estaciones se sincronizarán según su valor.

En el modo ad-hoc, el funcionamiento es más complejo. Por una parte, la estación que instancie la red establecerá un intervalo de beacon, esto es, una tasa de transferencia de portadoras que permitan la sincronización.

Sin embargo, en este caso, el control está distribuido y entre todas las estaciones se intentará mantener la sincronización. Para ello, toda esta estación que no detecte en un determinado tiempo de BackOff una trama de sincronización, enviará ella misma una trama de portadora para intentar que no se desincronice la red.

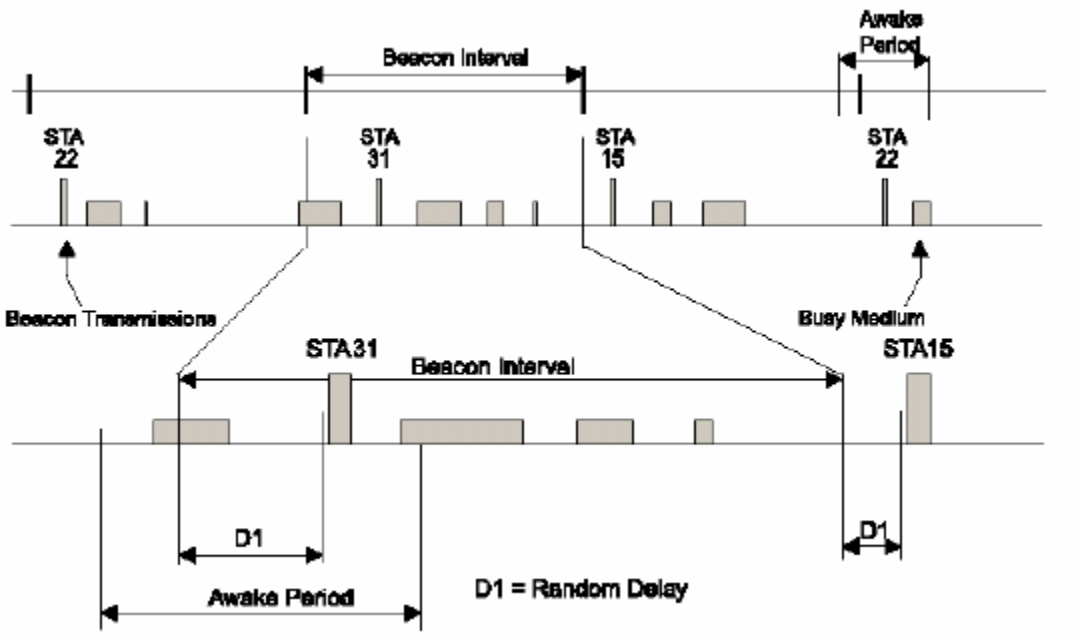


Figura 23

5.2.1.4.5.2. GESTIÓN DE POTENCIA

Las estaciones en la red pueden adoptar un modo limitado de potencia. Este modo de funcionamiento implicará que la estación se "despertará" sólo en determinados momentos para conectarse a la red.

Estas estaciones se denominan PS-STAs (Power Save Station) y estarán a la escucha de determinadas tramas como la de portadora y poco más. El control de este tipo de estaciones lo llevará el Access Point, que tendrá conocimiento de qué estación se ha asociado en este modo.

El Access Point mantendrá almacenados los paquetes que le lleguen con destino a los nodos limitados de potencia. Por tanto, el Access Point mantendrá un mapa de paquetes almacenados y los destinos a quienes tendrá que repartirlos o enviarlos.

Cuando el Access Point decida enviarle el paquete lo hará enviándole una trama TIM o Traffic Indication Map a la estación para que despierte en el próximo intervalo de portadora. De esta manera, estas estaciones recibirán la información con un desgaste mínimo de potencia.

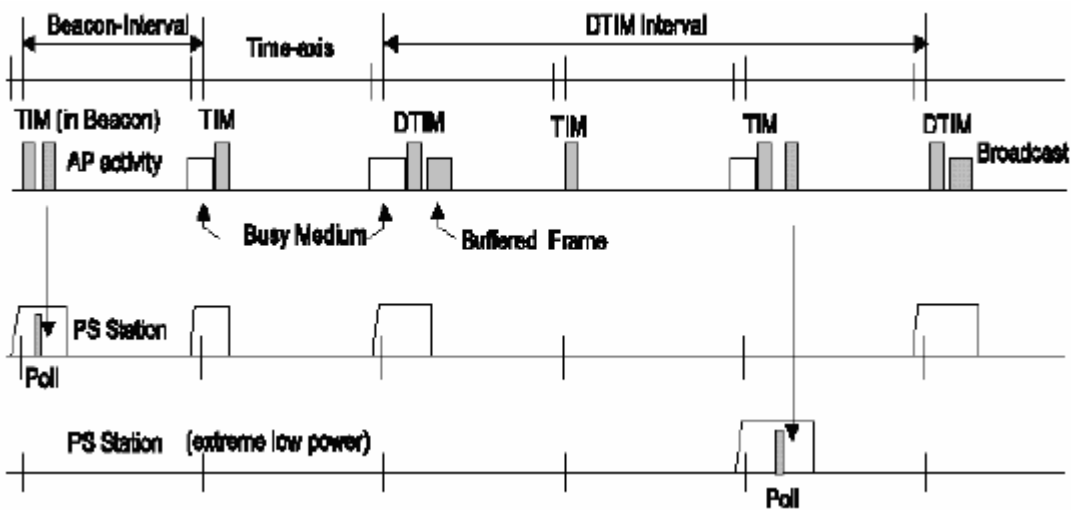


Figura 24

5.2.1.5. ESTANDARES INALAMBRICOS

Existen multitud de estándares definidos o en proceso de definición que es necesario conocer para una correcta interpretación de las redes Inalámbricas.

5.2.1.5.1. 802.11 LEGACY

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

5.2.1.5.2. 802.11a

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps. En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b. En 2001 hizo su aparición en el mercado los productos del estándar 802.11a.

La revisión 802.11a al estándar original fue ratificada 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 subportadoras orthogonal frequency-division multiplexing (OFDM) 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 no solapados, 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.

Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

Transmisión Exteriores Valor Máximo A 30 metros 54 Mbps Valor Mínimo A 300 metros 6 Mbps Interiores Valor Máximo A 12 metros 54 Mbps Valor Mínimo A 90 metros 6 Mbps

5.2.1.5.3. 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de

acceso CSMA/CA definido en el estándar original. El estandar 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 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

5.2.1.5.4. 802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 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 estándar lo tomó el hacer compatibles los dos estándares. 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. 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 hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

5.2.1.5.5. 802.11n

En enero de 2004, la 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 500 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 cerca de 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. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar

que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto. No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo esté implantado)

5.2.1.5.6. 802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access y
- (HCCA) Controlled Channel Access.

5.2.1.5.7. 802.11 SUPER G

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz y 5 Ghz, con una velocidad de transferencia de 108 Mbps.[10]

5.2.1.5.8. TECNOLOGÍA DE COMUNICACIONES WPAN (IEEE 802.15)

Los dispositivos electrónicos personales están llegando a ser más inteligentes e interactivos. Muchos dispositivos han aumentado capacidades de los datos. Esta capacidad permite conservar, utilizar, procesar e intercambiar información. Por ejemplo, estos dispositivos personales tienen una base de datos personal de gerencia PIM (*Personal Information Management*), calendarios personales, libros de dirección, etc. Las bases de datos de un dispositivo personal deben seguir sincronizadas con las bases de datos de otros dispositivos personales.

[10] Esta información fue obtenida de http://en.wikipedia.org/wiki/IEEE_802.11#802.11a

Tradicionalmente, los cables se han utilizado para interconectar los dispositivos personales. Sin embargo, muchos usuarios encuentran en estos cables frustración e improductividad.

A primera vista la operación y los objetivos de WPAN pueden aparecer semejantes a WLAN. Las tecnologías WLAN y WPAN permiten que un dispositivo se conecte con el ambiente circundante e intercambien datos entre ellos. Sin embargo, WLAN se ha diseñado y se optimiza para el uso de los dispositivos transportables, por ejemplo computadoras portátiles. Los dispositivos de WPAN son aún más móviles.

Las dos tecnologías se diferencian de tres maneras fundamentales:

- Niveles de energía y cobertura
- Control del medio
- Tiempo de vida de la red

5.2.1.5.8.1. NIVELES DE ENERGÍA Y COBERTURA

Para ampliar WLAN tanto como sea posible, mientras que reduce al mínimo la carga de redes multipunto, una instalación de WLAN se optimiza a menudo para la cobertura. Las distancias típicas de cobertura son de 100 m y se ponen en ejecución a expensas del consumo de energía. El consumo de energía agregado para distancias más grandes de cubierta tiene un impacto en los dispositivos que participan en la WLAN. Tienden a ser conectados en tomacorrientes de pared o utilizan el acoplamiento inalámbrico por un tiempo relativamente corto mientras que están desconectados.

WLAN se han diseñado para servir como substituto de los cables físicos en una infraestructura cableada (LAN). Mientras que la conectividad inalámbrica permite la portabilidad de los dispositivos, WLAN es semi-estático. Un dispositivo cliente en una WLAN está conectado típicamente con una estación base fija, y en ocasiones puede moverse entre las estaciones base fijas. Mientras que WLAN es mucho más fácil de desplegar con respecto a sus contrapartes, todavía necesita ser desplegada y ser instalada. Su orientación primaria es aumentar la posibilidad de conexión de los dispositivos portátiles en una infraestructura establecida, alámbrica o no alámbrica.

WPAN se orienta a interconectar los múltiples dispositivos móviles, personales. La distinción entre dispositivo "móvil" y dispositivo "portátil" en este caso es que los dispositivos móviles funcionan típicamente mediante baterías y tienen una interconexión breve con otros dispositivos; los dispositivos portátiles por su parte, se mueven con menos frecuencia, tienen períodos más largos de conexión y funcionan generalmente de energía provista por tomacorrientes de pared. Un dispositivo personal no necesariamente debe tener acceso a servicios de datos de nivel LAN, pero no se excluye.

En contraste con un WLAN, un WPAN negocia la cobertura para el consumo de energía. Con área pequeña de cobertura (cerca de 10 m), consumo de energía reducido, y modo de operación bajo de energía, un WPAN pueden alcanzar rangos suficientemente pequeños de consumo de energía para permitir la portabilidad. Varios dispositivos personales simples, pueden por lo tanto, utilizar una tecnología de WPAN, compartir datos, y ser verdaderos móviles.

5.2.1.5.8.2. CONTROL DEL MEDIO

Dado la gran variedad de dispositivos personales que pueden participar en una WPAN, la tecnología WPAN debe de soportar aplicaciones con rigurosos requisitos del ancho de banda, así como requisitos más flexibles de ancho de banda. Para proporcionar las garantías necesarias de ancho de banda, WPAN emplea un mecanismo que controla que regula las transmisiones de los dispositivos en WPAN.

WLAN emplea como opción funciones de coordinación similares a las anteriores, pero sobre distancias grandes, puede no ser recomendable tener un control terminante y absoluto de los medios. Cuando se tiene un nivel del control de este tipo, se dice que hay un "período contención-libre," pero no significa un ambiente libre de interferencia. Otras redes funcionando independientemente (de varias tecnologías), pueden interferir de vez en cuando con las transmisiones durante un período de contención-libre. Sin embargo, no se emplea ningún mecanismo de resolución de contención para recuperar las transmisiones perturbadas durante un período de contención-libre. Por lo anterior, en IEEE 802.15 WPAN, todo el tiempo existe contención libre. Este nivel de control es alcanzado creando una relación (en IEEE 802.15.WPAN, una relación maestro-esclavo) entre los dispositivos y un solo

sistema funcionando, tiempo-multiplexado y el sistema ranurado. Usar ranuras de tiempo pequeñas controla eficientemente la inquietud en las transmisiones experimentadas por el tráfico de alta calidad. Además, el empleo de un esquema de frecuencia-esperada con las pequeñas ranuras proporciona resistencia al ruido de interferencia que pueda ocurrir proveniente de otras redes.

Los dispositivos personales que participan en una WPAN se diseñan para funcionalidad personal. No se diseñan para ser miembros de una infraestructura establecida, pero incluso se pueden conectar a ella cuando es necesario. Un dispositivo típico de WPAN no necesita mantener un estado red-observable y red-controlable. En una WLAN se requiere, por ejemplo, mantener un administrador de información base, MIB (Management Information Base).

5.2.1.5.8.3. TIEMPO DE VIDA DE LA RED

WLAN no tiene un tiempo de vida inherente. Tienen "existencia" independiente de sus dispositivos constitutivos. Si todos los dispositivos emigraran del área de cobertura de una WLAN y llegara unidades de reemplazo, se podría decir que la WLAN tiene existencia ininterrumpida. Este concepto no aplicable para IEEE 802.15 WPAN. Si no participa el maestro, la red deja de existir.

En una WPAN un dispositivo crea una conexión que dura solamente el tiempo necesario y tiene una esperanza de vida finita. Por ejemplo, para la transferencia de archivo se puede hacer una conexión con bastante tiempo para lograr su meta. Cuando termina la transferencia, la conexión entre los dos dispositivos puede ser terminada. Las conexiones que un dispositivo móvil cliente crea en un WPAN son Ad Hoc y de naturaleza temporal. Los dispositivos con los cuales un dispositivo personal está conectado en un WPAN en determinado momento pueden no tener semejanza alguna con los dispositivos a los cuales fue conectada previamente o será conectado en el futuro. Por ejemplo, una computadora portátil se puede conectar con un PDA en un momento, con una cámara fotográfica digital en otro momento, y con un teléfono en otro momento.

Ocasionalmente, la computadora portátil se puede conectar con cualquiera de estos dispositivos. La tecnología de WPAN debe apoyar la rápida conectividad Ad Hoc sin la necesidad de un despliegue previo de cualquier tipo.

5.2.1.5.8.4 BLUETOOTH WPAN

La tecnología Bluetooth (Su nombre se deriva del antiguo héroe de las sagas vikingas, Diente Azul), utiliza un acoplamiento de radio de alcance corto que se ha optimizado para dispositivos personales ligeros, operados con pilas y pequeños. Un Bluetooth WPAN soporta los canales de comunicaciones síncronos para la comunicación de voz de telefonía y los canales de comunicaciones asincrónicas para las comunicaciones de datos. Esta facilidad permite a un gran número de dispositivos y aplicaciones participar en Bluetooth WPAN. Por ejemplo, en un teléfono celular se puede mantener una conferencia de audio mientras intercambia datos con una computadora portátil.

Un Bluetooth WPAN no se crea a priori y tiene una vida limitada. Se crea de una manera punto a punto siempre que un dispositivo desee intercambiar datos con otros dispositivos. El Bluetooth WPAN puede dejar de existir cuando los usos implicados han terminado sus tareas y no existe necesidad de continuar intercambiando datos.

El Bluetooth WPAN funciona en la banda de 2,4 GHz. Un transmisor-receptor rápido de salto de frecuencia se utiliza para combatir interferencia y descolorarse en esta banda (es decir, reduzca la probabilidad que toda la transmisión sea interrumpida por la interferencia). Se utiliza un canal ranurado, que tiene una duración de ranura de 625 µs. En el canal, la información se intercambia a través de los paquetes. Cada paquete se transmite a diversas frecuencias en salto de secuencia. Un paquete cubre una sola ranura, pero se puede extender hasta tres o cinco ranuras.

Para la transferencia de datos, una canal unidireccional con un máximo de 723,2 kb/s es posible entre dos dispositivos. Un canal bidireccional de 64 kb/s soporta tráfico de voz entre dos dispositivos.

5.2.1.5.8.5. TOPOLOGÍAS DE CONECTIVIDAD PARA BLUETOOTH WPAN

Piconet.- Un piconet es una WPAN formado por dispositivos de Bluetooth sirviendo como maestros en el piconet y unos o más dispositivos de Bluetooth que sirven como esclavos.

Un canal de salto frecuencia basado en la dirección del maestro define cada piconet. Todos los dispositivos que participan en la comunicación en un piconet son sincronizados al canal de salto de frecuencia por el piconet, usando el reloj del maestro del piconet. Los esclavos se comunican sólo con su maestro punto a punto bajo control del maestro. Las transmisiones del maestro pueden ser de cualquiera de estas formas: punto a punto o punto a multipunto. Los escenarios de uso pueden decidir que ciertos dispositivos actúan siempre como maestro o como esclavos. Sin embargo, este estándar no distingue entre los dispositivos con designaciones maestro y designaciones esclavo permanentes. Un dispositivo esclavo durante una sesión de comunicación puede ser maestro en otra y viceversa.

Scatternet.- Un scatternet es un conjunto de piconets operacionales de Bluetooth que se traslapan en tiempo y espacio. Un dispositivo de Bluetooth puede participar en varios piconets al mismo tiempo, permitiendo así la posibilidad de que fluya la información más allá del área de la cobertura de un sólo piconet. Un dispositivo en un scatternet podía ser un esclavo en varios piconets, pero maestro en uno de ellos Integración con LAN.- Un Bluetooth WPAN se puede unir y participar en comunicaciones con otra LAN de la familia IEEE 802 haciendo uso de un accesorio LAN IEEE 802, AG (Attachment Gateway). Un AG de IEEE 802 es un componente arquitectónico lógico que se puede o no poner en ejecución directamente en un dispositivo de Bluetooth. Con un AG de IEEE 802, las unidades de servicio de datos del MAC (MSDUs) se pueden ser condicionadas para el transporte sobre un Bluetooth WPAN.[11]

[11] *http://standards.ieee.org/getieee802/download/802.15.1-2002.pdf*

5.2.1.5.9. IEEE 802.16 WMAN

El estándar IEEE 802.16, terminado en octubre de 2001 y publicado el 8 de abril de 2002, define la especificación de interfaz Wireless MAN para las redes inalámbricas de área metropolitana.

Según lo definido actualmente el estándar IEEE 802.16, una MAN inalámbrica proporciona el acceso de red a los edificios, a través de antenas exteriores que se comunican con las estaciones base de radio. La MAN inalámbrica ofrece una alternativa a las redes de acceso cablegrafiadas, tales como: acoplamientos ópticos de fibra, sistemas coaxiales usando los módems de cable y acoplamientos de suscriptor de línea digital DSL (Digital Subscriber Line).

Ya que los sistemas inalámbricos tienen la capacidad de cubrir amplias áreas geográficas sin la costosa infraestructura requerida en cable, la tecnología puede ofrecer menos costo por despliegue y un acceso de banda ancha. Con la tecnología de Wireless MAN llevando la red a un edificio, los usuarios dentro del edificio se conectarán con las redes convencionales ya construidas, por ejemplo: para los datos, Ethernet o WLAN de IEEE 802,11. Sin embargo, el diseño fundamental del estándar puede permitir la eventual extensión de los protocolos de una red Wireless MAN directamente al usuario individual. Por ejemplo: una base central puede, mediante el protocolo de control de acceso al medio, intercambiar información con una computadora portátil que se encuentra en un hogar. Los acoplamientos de la base central al receptor casero y del receptor casero a la computadora portátil utilizarían probablemente capas físicas diversas, pero el diseño del MAC de Wireless MAN podría brindar tal conexión con calidad de servicio QoS (Quality of Service), que garantiza la calidad de una red en cuanto a velocidad, rendimiento, etc. Con la tecnología ampliándose en esta dirección, es probable que el estándar se desarrolle para apoyar a usuarios nómadas y cada vez más móviles.

El estándar IEEE 802.16 fue diseñado para desarrollarse como un sistema de interfaces de aire basados en un protocolo común de MAC pero con las especificaciones de la capa física dependientes en el espectro del uso y de las regulaciones asociadas. El estándar, según lo aprobado en 2001, trata frecuencias desde 10 hasta 66 GHz, donde el espectro extendido está disponible mundialmente pero las longitudes de onda cortas introducen desafíos significativos de despliegue.

Un nuevo proyecto, actualmente en la etapa de votación, extenderá la ayuda para frecuencias desde 2 hasta 11 GHz, incluyendo espectros con y sin licencia. Comparado a las frecuencias más altas, tales espectros ofrecen la oportunidad de alcanzar a muchos más clientes con menos costo, aunque en tasas de transferencia de datos generalmente más bajas. Esto sugiere que tales servicios sean orientados hacia hogares individuales o pequeñas empresas.

Los servicios requeridos por los usuarios finales son variados en su naturaleza e incluyen voz y datos, conectividad con el protocolo de Internet IP (Internet Protocol) y voz sobre IP. Para soportar esta variedad de servicios, la MAC de 802.16 debe de alojar tanto tráfico continuo como tráfico exigente. 802.16 proporciona una amplia gama de servicios a los clásicos servicios de tipo asíncrono y a nuevas categorías de servicio.

El protocolo 802.16 también debe soportar una variedad de requerimientos de soporte como: el modo de transferencia asíncrono ATM (Asynchronous Transfer Mode), y protocolos basados en paquetes. Las subcapas convergentes son utilizadas como capas de transporte específico hacia una MAC que es flexible para transportar cualquier tipo de tráfico. A través de características como: la supresión de carga de encabezado, el empaquetado y la fragmentación, las subcapas convergentes y la MAC trabajan para llevar el tráfico de forma más eficiente que el mecanismo original de transporte.

La eficiencia de las aplicaciones de transporte también se tratan en la interfaz que esta entre la MAC y capa física. Por ejemplo, la modulación y los esquemas de codificación se especifican en un perfil de explosión que se pueda ajustar a cada estación del suscriptor. El MAC puede hacer uso de anchura de banda eficiente bajo condiciones favorables de enlace.

El mecanismo Solicitud-Concesión esta diseñado para ser escalable, eficiente y autocorregible. El sistema de acceso 802.16 no pierde eficacia cuando está frente a conexiones de múltiples terminales, múltiples niveles de QoS por terminal o una gran cantidad de usuarios. Se vale de una gran variedad de mecanismos de petición, balanceando la estabilidad del acceso con la eficacia del acceso orientado a la contención.

Junto con la tarea fundamental de asignar anchura de banda y transportar datos, la MAC incluye una subcapa de aislamiento que proporciona la autentificación en el establecimiento del acceso y de la conexión de red para evitar el hurto del servicio y proporciona el intercambio y el cifrado dominantes para el aislamiento de datos.

Para adaptarse al ambiente físico más exigente y a los diversos requisitos de servicio en las frecuencias de entre 2 y 11 GHz, el proyecto 802.16 está aumentando la MAC para proporcionar la petición automática de repetición ARQ (Automatic Repeat-reQuest), y la ayuda para el acoplamiento, en arquitecturas de red punto a multipunto.

Puede resultar adecuado para unir puntos calientes Wi-Fi a las redes de los operadores, sin necesidad de establecer un enlace fijo. El equipamiento Wi-Fi es relativamente barato pero un enlace E1 o DSL resulta caro y a veces no se puede desplegar, por lo que la alternativa del radio parece buena. 802.16 extiende el alcance de Wi-Fi y provee una alternativa o complemento a las redes 3G (Tercera Generación de Telefonía Móvil). Para las empresas, es una alternativa a contemplar, ya que el coste puede ser hasta 10 veces menor que en el caso de emplear un enlace E1 (Es una Interfaz digital homologada en Europa y América Latina que lleva datos a 2Mbits/s, E3 para 34Mbit/s y E4 para 134Mbit/s) o T1 (Conexión por medio de línea telefónica que transporta datos con velocidades de hasta 1.544.000 bps). De momento no esta disponible para el acceso residencial, pero en un futuro podría ser una realidad, sustituyendo a las conexiones ADSL o de cable y haciendo que la banda ancha llegue a todos los hogares. Otra de sus aplicaciones es ofrecer servicios a zonas rurales de difícil acceso, a las que no llegan las redes cableadas. Es una tecnología muy adecuada para establecer radio enlaces, dado su gran alcance y alta capacidad, a un coste muy competitivo frente a otras alternativas. En los países en desarrollo resulta una buena alternativa para el despliegue rápido de servicios, compitiendo directamente con las infraestructuras basadas en redes de satélites, que son muy costosas[12]

[12] *http://www.coitt.es/antena/pdf/157/17_Internet_WIMAX.pdf*
http://grouper.ieee.org/groups/802/16/docs/02/C80216-02_05.pdf

5.2.1.5.10. IEEE 802.20

- Trabaja en bandas licenciadas debajo de los 3.5 GHz
- Soporta velocidades de hasta 1Mbps por usuario
- Soporta vehículos en movimiento arriba de 250Km/h
- Cubre áreas de igual tamaño a las de una red metropolitana MAN (Metropolitan Area Network)
- Posee eficiencia espectral, índices de datos sostenidos de usuario y número de
- Usuarios activos perceptiblemente más arriba que el alcanzado por los sistemas móviles existentes

Permite el despliegue mundial rentable, un espectro eficiente, y esta siempre disponible y acceso a los sistemas inalámbricos de banda ancha móviles interoperable para tratar las necesidades del usuario como:

- Acceso a Internet móvil
- Soporte transparente para aplicaciones de Internet
- Acceso a todos los servicios de Intranet
- Acceso transparente a la información y localización de servicios

Esta especificación llena el hueco de funcionamiento entre los servicios de transferencia alta con poca movilidad, desarrollados actualmente en 802 y las redes celulares de alta movilidad.

La capacidad del medio inalámbrico para apoyar la movilidad, es una característica incomparable de las capacidades de las redes de acceso de banda ancha cableadas. La capacidad móvil ha probado ser acertado en muchos dispositivos móviles de banda ancha. El acceso inalámbrico de banda ancha móvil, basado en movilidad IP, abre todo el contenido de Internet al público en general. El mercado potencial son todos los usuarios de IP, estos incluyen:

- Servicios de redes virtuales e Intranet
- Juegos y entretenimiento
- Internet y servicios locales

IEEE 802 no tiene actualmente proyectos para soportar la movilidad de vehículos. El estándar móvil BWA (Broadband Wireless Access) esta diseñado para prever al público el acceso las redes móviles operadas por terceros, donde el usuario típicamente hace uso de una red de acceso amplio a través de una red de acceso móvil. Diferencia con una LAN inalámbrica es que funciona sobre distancias más pequeñas.

El proyecto propuesto especificará una solución única al PHY y a la capa del MAC de la interfaz aérea que funciona en el espectro asignado al servicio móvil. Se prevé que el estándar será flexible y apoyará eficientemente una variedad de servicios, algunos de los cuales pueden estar limitados a rigurosos requisitos. Esta solución incorporará la ayuda para la ingeniería del tráfico y QoS para el tráfico de datos en tiempo real y tráfico en no-tiempo real.

La factibilidad técnica del sistema ha sido demostrada junto a otros sistemas propietarios que están en uso o están en etapa de prueba. Estos sistemas utilizan componentes tecnológicos actuales como: módems, radio, antenas y protocolos PHY/MAC.

Esta solución puede ser operada en tecnologías que operan bajo espectro extendido, tecnologías de radio, técnicas de proceso avanzado de señal y arquitecturas celulares. Todas estas tecnologías han sido probadas, se están extendiendo exitosamente y han encontrado un creciente uso de las LAN y MAN, así como de ambientes celulares.[13]

5.2.1.5.11. HIPERLAN/2

5.2.1.5.11.1. ANTECEDENTES

El establecimiento de una red inalámbrica ha sido más o menos sinónimo de redes celulares de área amplia basadas en diversos estándares. Se han hecho con

[13] http://www.ieee802.org/20/P_Docs/IEEE%20802.20%20PD-04.pdf

el propósito principal de la transferencia de voz, aunque algunos también ofrecen servicios de Datacom a velocidad muy baja (~10 kbits/s).

El servicio inalámbrico del Datacom ofrece rendimiento de procesamiento necesario para satisfacer necesidades reales en el acceso a Internet y al Intranet y es una manera de competir en el mercado a una escala más amplia. En el ambiente del LAN, los productos inalámbricos del

WLAN basados en los diversos tipos de 802.11 están disponibles con una gran gama de vendedores. Dependiendo del esquema de la transmisión, los productos pueden ofrecer bandas que se extienden desde 1 Mbps hasta 11 Mbps. Se espera que los precios bajen, haciendo de WLAN más y más una alternativa seria al acceso fijo de Ethernet. En el área amplia, los servicios generales de radio celulares aumentaron la anchura de banda disponible a un usuario hasta cerca de 64 kbit/s a partir del año 2000, haciendo este servicio del Datacom comparable a dial-in.

Para reunir los requisitos de una red para el futuro, una nueva generación de WLAN y tecnologías de red celular está en desarrollo. Estos requisitos incluyen calidad de servicio (QoS), seguridad, capacidad de moverse entre el área local y áreas amplias así como entre los ambientes corporativos y públicos y rendimiento de procesamiento.

5.2.1.5.11.2. LA RED HIPERLAN/2

Las estaciones móviles se comunican con los puntos de acceso sobre un interfaz de aire según lo definido por el estándar HiperLAN/2. Hay también la posibilidad de comunicación directa entre dos estaciones móviles, que sigue estando en etapa de prueba. El usuario de la estación móvil puede moverse libremente alrededor de la red HiperLAN/2, que asegurará que el usuario y la estación móvil consigan el mejor funcionamiento de transmisión posible. Una estación móvil, después de que se haya realizado la asociación (para ser visto como conexión), sólo se comunica con un Access Point en cada punto en tiempo. El Access Point que ve a esa estación móvil configura la red de radio automáticamente, es decir no hay necesidad del planeamiento manual de frecuencia.

5.2.1.5.11.3. CARACTERÍSTICAS DE HIPERLAN/2

Las características generales de la tecnología HiperLAN/2 son las siguientes:

- Transmisión rápida
- Conexión-orientada
- Soporte de calidad-de-servicio (QoS)
- Asignación automática de frecuencia
- Soporte de seguridad
- Soporte de movilidad
- Red y aplicación independientes
- Ahorro de energía

TRANSMISIÓN RÁPIDA

HiperLAN/2 tiene una banda alta de transmisión, llega hasta 54 Mbps. Para alcanzar esto, HiperLAN/2 hace uso del método de modularización llamado Orthogonal Frequency Digital Multiplexing (OFDM) para transmitir las señales análogas. OFDM es muy eficiente en ambientes dispersivos y dentro de las oficinas, en donde las señales de radio transmitidas se reflejan de muchos puntos.

Sobre la capa física, el protocolo de control de acceso al medio (MAC) pone en ejecución la división de tiempo dinámico duplex para permitir un eficiente uso de los recursos de radio.

CONEXIÓN-ORIENTADA

En una red HiperLAN/2, los datos se transmiten en conexiones entre la estación móvil y el Access Point que se han establecido previamente usando funciones señalización del plano de control HiperLAN/2. Hay dos tipos de conexiones, punto a punto y punto a multipunto. Las conexiones punto a punto son bidireccionales mientras que las de punto a multipunto son unidireccionales en dirección hacia la estación móvil. Además, hay también un canal dedicado de la difusión a través de el cual el tráfico alcanza todas las terminales a partir de un Access Point.

SOPORTE DE CALIDAD-DE-SERVICIO (QOS)

La naturaleza de la conexión orientada de HiperLAN/2 hace fácil la ejecución del soporte para la calidad de servicio (QoS). A cada conexión se le puede asignar un QoS específico, por ejemplo: anchura de banda, retraso, tasa de error de bits, etc. También a una conexión se le puede asignar niveles de prioridad en relación a otras conexiones. El soporte QoS combinado con la alta tasa de transmisión, facilita la transmisión simultánea de diversos tipos de secuencias de datos, voz, video, etc.

ASIGNACIÓN AUTOMÁTICA DE FRECUENCIA

En una red HiperLAN/2, no hay necesidad de la asignación manual de frecuencia como en redes celulares, en el caso de GSM (Global System for Mobile communications). Los puntos de acceso en HiperLAN/2, tienen una ayuda incorporada para seleccionar automáticamente un canal de radio apropiado para la transmisión, dentro de cada área de cobertura del Access Point. Un Access Point escucha al Access Point vecino, así como a otras fuentes de radio en el ambiente, y selecciona un canal de radio apropiado basado en otros canales de radio que están siendo utilizados por otros puntos de acceso y así reducir al mínimo la interferencia con el ambiente.

SOPORTE DE SEGURIDAD

La red HiperLAN/2 tiene ayuda para la autenticación y el cifrado. Con la autenticación entre el Access Point y la estación móvil se asegura el acceso autorizado a la red (desde el punto de vista del Access Point) o para asegurar el acceso a un operador de red válido (desde el punto de vista de la estación móvil). La autenticación confía en la existencia de una función de soporte, tal como un servicio del directorio, pero que está fuera del alcance de HiperLAN/2.

El tráfico del usuario en conexiones establecidas se puede cifrar para protegerse contra espías y ataques.

SOPORTE DE MOVILIDAD

La estación móvil considerará al Access Point "más cercano", o con mejor transmisión para establecer una conexión. Así, una estación móvil en movimiento puede detectar que hay una alternativa de Access Point con un mejor funcionamiento de transmisión de radio que el Access Point al cual está asociado actualmente. La estación móvil pedirá unirse a este Access Point. Todas las conexiones establecidas serán movidas al nuevo Access Point dando por resultado que la estación móvil siga asociada a la red HiperLAN/2 y que pueda continuar su comunicación. Durante el cambio entre puntos de acceso puede ocurrir una pérdida de paquetes.

Si una estación móvil se sale de la cobertura de radio por cierto tiempo, la estación móvil puede soltar su asociación a la red HiperLAN/2 dando por resultado la interrupción de todas las conexiones.

RED Y APLICACIÓN INDEPENDIENTE

El protocolo HiperLAN/2 tiene una arquitectura flexible para la fácil adaptación y la integración con una gran variedad de redes fijas. Todos los usos que funcionan hoy sobre una infraestructura fija pueden también funcionar sobre una red HiperLAN/2.

AHORRO DE ENERGÍA

En HiperLAN/2, el mecanismo a tener en cuenta para que una estación móvil ahorre energía se basa en la negociación de los períodos de sueño. La estación móvil puede solicitar en cualquier momento al Access Point incorporar un estado energía baja (específico por la estación móvil), y pedir un período específico de sueño. En la expiración del período negociado de sueño, la estación móvil busca la presencia de cualquier indicación “despertar” del Access Point. En ausencia de la indicación “despertar” la estación móvil regresa de nuevo a su estado de energía baja para el período próximo de sueño, y así sucesivamente. Un Access Point retrazará cualquier dato pendiente a una estación móvil hasta que expira el período correspondiente de sueño.

5.2.1.5.11.4. ARQUITECTURA DEL PROTOCOLO Y LAS CAPAS

El protocolo se divide en dos partes: una parte en el plano de control y otra en el plano de usuario. El plano de usuario incluye las funciones para transmisión de tráfico bajo conexiones establecidas y el plano de control incluye las funciones para el control del establecimiento, del lanzamiento, y de la supervisión de la conexión. El protocolo HiperLAN/2 tiene tres capas básicas: Capa física (PHY), capa de control de transmisión de datos DLC (Data Link Control), y la capa de la convergencia.

CAPA FÍSICA (PHY)

El formato de la transmisión en la capa física es una explosión, que consiste en una parte del preámbulo y una parte de datos, donde el último podría originarse desde cada uno de los canales del transporte del DLC. (OFDM) ha sido elegida debido a su funcionamiento excelente en los canales altamente dispersivos. El espaciamiento de canal es 20 megaciclos, que permite altos índices binarios por canal pero todavía tiene un número razonable de canales en el espectro asignado 19 canales en Europa. 52 subcanales se utilizan por canal, donde 48 subcanales llevan datos reales y 4 subcanales son los pilotos que facilitan la fase que sigue para la desmodulación coherente. La duración del intervalo protector es igual a 800 ns, con los cuales es suficiente para permitir el buen funcionamiento en los canales, hasta con 250 ns de extensión de retraso. Un intervalo más corto opcional de protección es de 400 ns que se puede utilizar en ambientes interiores pequeños.

CAPA DE CONTROL DE ENLACE DE DATOS (DLC)

La capa de control de enlace de datos (DLC) constituye el acoplamiento lógico entre un Access Point y la estación móvil. El DLC incluye las funciones para el acceso al medio y la transmisión (plano del usuario) así como terminal/usuario y la dirección de la conexión (plano de control). Así, la capa de DLC consiste en un sistema de subcapas:

- Protocolo de control de acceso al medio (MAC)
- Protocolo de control de error (EC)

- Protocolo de enlace de radio (RCL) con entidades de señalización: control de conexión DLC (DCC), el control de recursos de radio (RRC) y la función de control de asociación (ACF).

PROTOCOLO MAC

El protocolo del MAC es el protocolo usado para el acceso al medio (enlace de radio) con la transmisión resultante de datos sobre ese medio. El control se centraliza en el Access Point que informa a las estaciones móviles el momento en que el marco del MAC permite transmitir sus datos, de acuerdo al pedido de recursos de cada una de las estaciones móviles.

PROTOCOLO DE CONTROL DE ERROR

La repetición selectiva (SR) y Solicitud de repetición automática (ARQ) es el mecanismo del control de error (EC) que se utiliza para aumentar la confiabilidad sobre el enlace de radio. La EC detecta los errores de bits y los retransmite si ocurren tales errores.

SEÑALIZACIÓN Y CONTROL

El protocolo de control de enlace de radio otorga un servicio de transporte para las entidades de señalización: función de control de asociación (ACF), función de control de recursos de radio (RRC) y la función control de conexión de usuarios DLC (DCC). Estas cuatro entidades conforman el plano de control de DLC para el intercambio de mensajes de señalización entre la estación móvil y el Access Point.

CAPA DE CONVERGENCIA (CL)

La capa de la convergencia (CL) tiene dos funciones principales: adaptar la petición del servicio de capas más altas al servicio ofrecido por el DLC y convertir los paquetes más altos de la capa SDU (Service Data Unit) con tamaño variable o fijó en un tamaño fijo que se utiliza dentro de DLC. La función del acolchado, de la segmentación y del nuevo ensamble del tamaño fijo DLC SDUs es una cuestión clave que permite estandardizar y poner un DLC y un PHY en ejecución que es

independiente de la red fija con la cual la red HiperLAN/2 está conectada. La arquitectura genérica del CL hace a HiperLAN/2 conveniente como red de acceso de radio para una diversidad de redes fijas, Ethernet, IP, UMTS, etc.

5.2.1.4.11.5 ASIGNACIÓN DEL ESPECTRO Y COBERTURA DEL ÁREA

En Europa, 455 megaciclos se sugieren para ser asignados para los sistemas de HiperLAN. Las diversas partes de las bandas tienen diversas condiciones operacionales fijadas por La Conferencia Europea de Administraciones de Correos y Telecomunicaciones CEPT (Conference of European Post and Telecommunications) para permitir coexistencia con otros servicios.

En los E.U., 300 megaciclos se asignan a WLAN. En Japón, 100 megaciclos se asignan para WLAN, y más asignación del espectro está bajo investigación. La Unión Internacional de Telecomunicaciones - Sector Radiocomunicaciones, ITU-R (International Telecommunication Union – Radiocommunication Sector), también ha comenzado actividades para recomendar una asignación global para WLAN.

Una Access Point de HiperLAN/2 tiene un radio de cobertura de aproximadamente 30 metros en el interior de una oficina y 150 metros en el exterior.

5.2.1.6. DISPOSITIVOS PARA UNA RED INALAMBRICA

5.2.1.6.1. DISPOSITIVOS BASICOS INALÁMBRICOS

Los Puntos de Acceso son el 'centro de datos' de una red inalámbrica. Se trata de unas pequeñas unidades que extienden la conectividad inalámbrica a aquellas computadoras de escritorio o portátiles que dispongan de tarjetas inalámbricas (los clientes inalámbricos pueden compartir archivos, recursos y una conexión a Internet). Los puntos de acceso, que se instalan en paredes para mejorar la recepción, envían y reciben datos de red hacia y desde los clientes inalámbricos mediante ondas de radio en el margen de frecuencias de 2,4 GHz.

Las tarjetas Inalámbricas cuentan con unas pequeñas antenas que sobresalen ligeramente de la ranura de la tarjeta y que, en el caso de las computadoras portátiles o agendas, se pliegan durante los desplazamientos para evitar daños.

Los Gateways son dispositivos que permiten compartir conexiones por Cable o DSL a Internet entre múltiples dispositivos en red. Para poder conectar la LAN a Internet, este dispositivo ha de ofrecer funciones integradas de router. Existen diferentes tipos de pasarelas Ethernet disponibles: de cable e inalámbricas, con distintos grados de seguridad.

Los Bridges Ethernet se pueden acoplar a cualquier dispositivo Ethernet para ampliar la conectividad inalámbrica. Por ejemplo, una impresora preparada para Ethernet puede carecer de ranura de expansión para añadirle capacidad inalámbrica nativa, pero se puede conectar a la red inalámbrica mediante un puente Ethernet.[14]

5.2.1.6.2. TIPOS DE ANTENAS

Una clasificación de las antenas puede basarse en:

Frecuencia y tamaño. Las antenas utilizadas para HF son diferentes de las antenas utilizadas para VHF, las cuales son diferentes de las antenas para microondas. La longitud de onda es diferente a diferentes frecuencias, por lo tanto las antenas deben ser diferentes en tamaño para radiar señales a la correcta longitud de onda. En este caso estamos particularmente interesados en las antenas que trabajan en el rango de microondas, especialmente en las frecuencias de los 2,4 GHz y 5 GHz. A los 2400 MHz la longitud de onda es 12,5cm, mientras que a los 5000 MHz es de 6cm.

Directividad. Las antenas pueden ser omnidireccionales, sectoriales o directivas. Las antenas omnidireccionales irradian aproximadamente con la misma intensidad en todas las direcciones del plano horizontal, es decir en los 360°. Los tipos más populares de antenas omnidireccionales son los dipolos y las de plano de tierra. Las antenas sectoriales irradian principalmente en un área específica. El haz puede ser tan amplio como 180 grados, o tan angosto como 60 grados. Las direccionales o directivas son antenas en las cuales el ancho del haz es mucho más angosto que en las antenas sectoriales. Tienen la ganancia más alta y por lo tanto se utilizan para enlaces a larga distancia. Tipos de antenas directivas son las Yagi, las biquad, las de bocina, las helicoidales, las antenas patch, los platos parabólicos, y muchas otras.

[14] *Esta información fue obtenida del sitio Web http://www.idatelnetworks.com*

Construcción física. Las antenas pueden construirse de muchas formas diferentes, desde simples mallas, platos parabólicos, o latas de café. Cuando consideramos antenas adecuadas para el uso en WLAN de 2,4GHz, se pueden utilizar otras clasificaciones:

Aplicaciones. Los puntos de acceso tienden a hacer redes punto a multipunto, mientras que los enlaces remotos son punto a punto. Esto implica diferentes tipos de antenas para el propósito. Los nodos utilizados para accesos multipunto pueden utilizar tanto antenas omni, las cuales irradian igualmente en todas direcciones, como antenas sectoriales que se enfocan en un área limitada. En el caso de los enlaces punto a punto, las antenas se usan para conectar dos lugares. Las antenas directivas son la elección principal para esta aplicación.

Ahora le presentamos una breve lista de tipos comunes de antenas para la frecuencia de 2,4GHz, con una corta descripción de la información básica acerca de sus características.

ANTENA DE 1/4 DE LONGITUD CON PLANO DE TIERRA

Esta antena es muy simple en su construcción y es útil para las comunicaciones cuando el tamaño, el costo y la facilidad de construcción son importantes. Esta antena se diseñó para transmitir una señal polarizada verticalmente. Consiste en un elemento de 1⁄4 de longitud onda como medio dipolo, y tres o cuatro elementos de un 1⁄4 de longitud de onda inclinados de 30 a 45 grados hacia abajo.

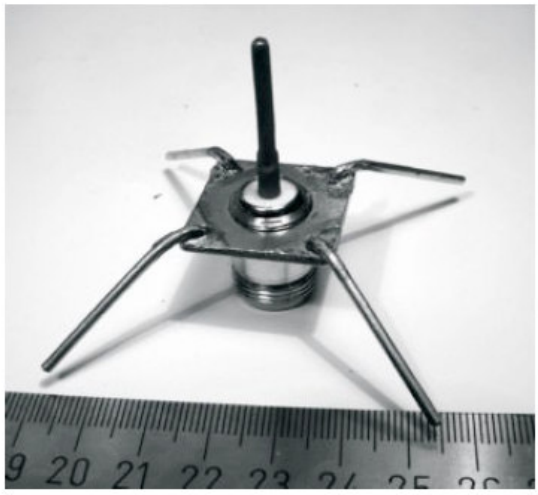


Figura 25 muestra una Antena de un cuarto de longitud de onda con plano de tierra

Este conjunto de elementos, denominados radiales, constituyen el plano de tierra. Esta es una antena simple y efectiva que puede capturar una señal con igual facilidad en todas las direcciones. Para incrementar la ganancia, la señal puede hacerse más achatada para concentrar la radiación en el plano horizontal. El ancho del haz vertical representa el grado de achatamiento en el foco. Esto es útil en una situación de punto a multipunto, si todas las otras antenas se encuentran a la misma altura. La ganancia de esta antena está en el orden de 2 a 4 dBi.

ANTENA YAGI

La antena Yagi básica consiste en un cierto número de elementos rectos que miden cada uno aproximadamente la mitad de la longitud de onda. El elemento excitado o activo de una Yagi es el equivalente a una antena dipolo de media onda con alimentación central. En paralelo al elemento activo, y a una distancia que va de 0,2 a 0,5 longitudes de onda en cada lado, hay varillas rectas o alambres llamados reflectores y directores, o simplemente elementos pasivos. Un reflector se ubica detrás del elemento activo y es ligeramente más largo que media longitud de onda; un director se coloca en frente del elemento activo y es ligeramente más corto que media longitud de onda. Una Yagi típica tiene un reflector y uno o más directores. La antena propaga la energía del campo electromagnético en la dirección que va desde el elemento activo hacia los directores, y es más sensible a la energía electromagnética entrante en esta misma dirección. Cuantos más directores tiene

una Yagi, mayor la ganancia. Cuantos más directores se agreguen a una Yagi, la misma va a ser más larga. La siguiente es una foto de una antena Yagi con 6 directores y 1 reflector.

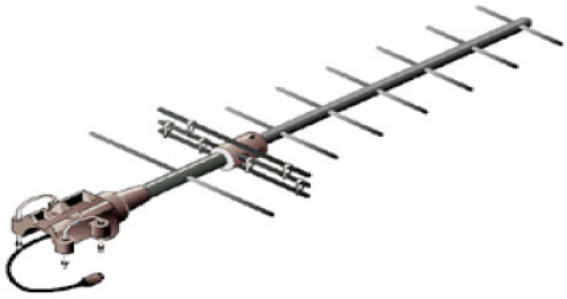


Figura 26 muestra una antena Yagi

Las antenas Yagi son utilizadas principalmente por los enlaces Punto a Punto; tienen una ganancia desde 10 a 20 dBi y un ancho de haz horizontal de 10 a 20 grados.

BOCINA

El nombre de la antena bocina deriva de su apariencia característica acampanada o de cuerno. La porción acampanada puede ser cuadrada, rectangular, cilíndrica o cónica. La dirección de máxima radiación se corresponde con el eje de la campana. Se puede alimentar sencillamente con una guía de onda, pero también puede hacerse con un cable coaxial y la transición apropiada. Las antenas bocina se utilizan comúnmente como el elemento activo en una antena de plato. La antena bocina se coloca hacia el centro del plato reflector. El uso de una bocina, en lugar de una antena dipolo o cualquier otro tipo de antena en el punto focal del plato, minimiza la pérdida de energía alrededor de los bordes del plato reflector. A 2,4GHz, una antena bocina simple hecha con una lata tiene una ganancia del orden de 10 a 15 dBi.

Figura 27 muestra una Antena bocina hecha con una lata de comida.

PLATO PARABÓLICO

Las antenas basadas en reflectores parabólicos son el tipo más común de antenas directivas cuando se requiere una gran ganancia. La ventaja principal es que pueden construirse para tener una ganancia y una directividad tan grande como sea requerido. La desventaja principal es que los platos grandes son difíciles de montar y están predispuestos a sufrir los efectos del viento.

Los platos de más de un metro generalmente están hechos de material sólido. Frecuentemente se utiliza el aluminio por una ventaja de peso, su durabilidad y sus buenas características eléctricas. El efecto del viento se incrementa rápidamente con el tamaño del plato y se convierte en un problema severo. A menudo se utilizan platos que tienen una superficie reflectora constituida por una malla abierta. Éstos tienen un a relación de ganancia adelante/atrás más pobre pero son seguros de utilizar y sencillos de construir. Materiales como el cobre, aluminio, bronce (latón), acero galvanizado y hierro son apropiados para una malla.

Figura 28 muestra una Una antena plato sólida.

BIQUAD

La antena BiQuad es fácil de armar y ofrece buena directividad y ganancia para las comunicaciones punto a punto. Consiste en dos cuadrados iguales de 1⁄4 de longitud de onda como elemento de radiación y un plato metálico o malla como reflector. Esta antena tiene un ancho del haz de aproximadamente 70 grados y una ganancia en el orden de 10-12 dBi. Puede ser utilizada como una antena única o como un alimentador para un Plato Parabólico.

Para encontrar la polarización, debemos observar el frente de la antena, con los cuadrados colocados lado a lado; en esa posición la polarización es vertical.

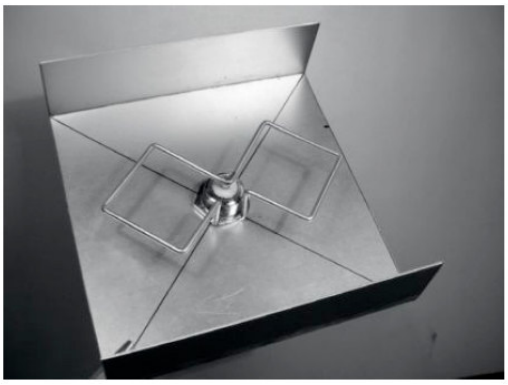


Figura 29 muestra una Antena BiQuad.

OTRAS ANTENAS

Existen muchos otros tipos de antenas y se crean nuevas siguiendo los avances tecnológicos.

Antenas de Sector o Sectoriales: son muy usadas en la infraestructura de telefonía celular y en general se construyen agregando una cara reflectora a uno o más dipolos alimentados en fase. Su ancho de haz horizontal puede ser tan amplio como 180 grados, o tan angosto como 60 grados, mientras que el vertical generalmente es mucho más angosto. Las antenas compuestas pueden armarse con varios sectores para cubrir un rango horizontal más ancho (antena multisectorial).

Antenas Panel o Patch: son paneles planos sólidos utilizados para cobertura interior, con una ganancia de hasta 20 dB.[15]

[15] *Información obtenida de http://wndw.net/pdf/wndw-es-ebook.pdf*

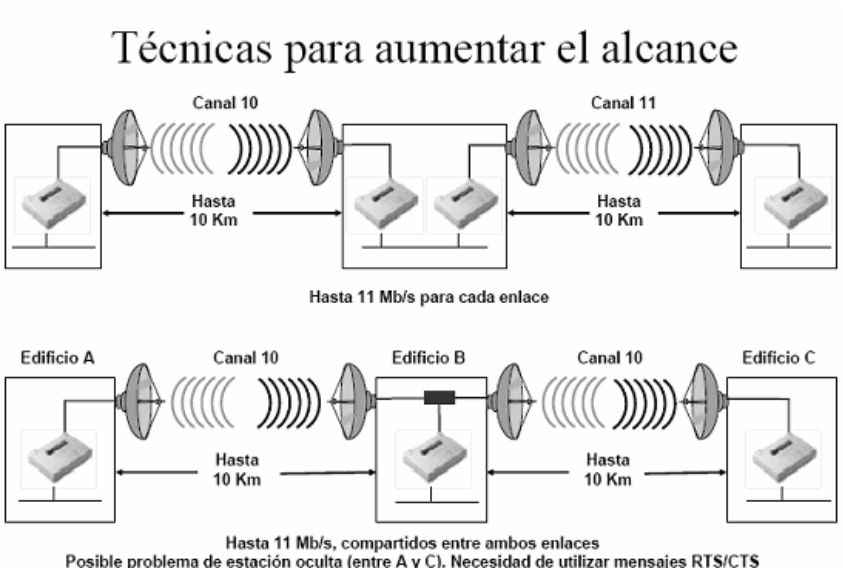


Figura 30 Muestra técnicas para aumentar el alcance

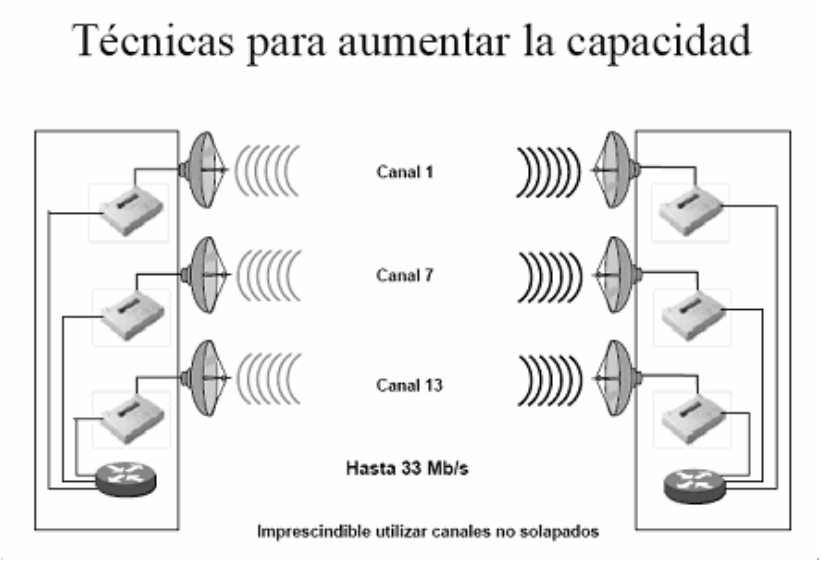


Figura 31 Muestra técnicas para aumentar la capacidad

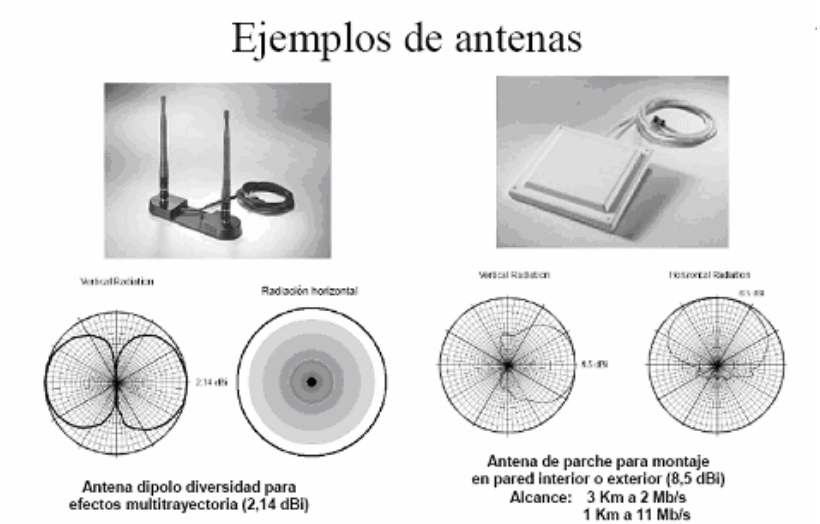


Figura 32 Muestra ejemplos de antenas

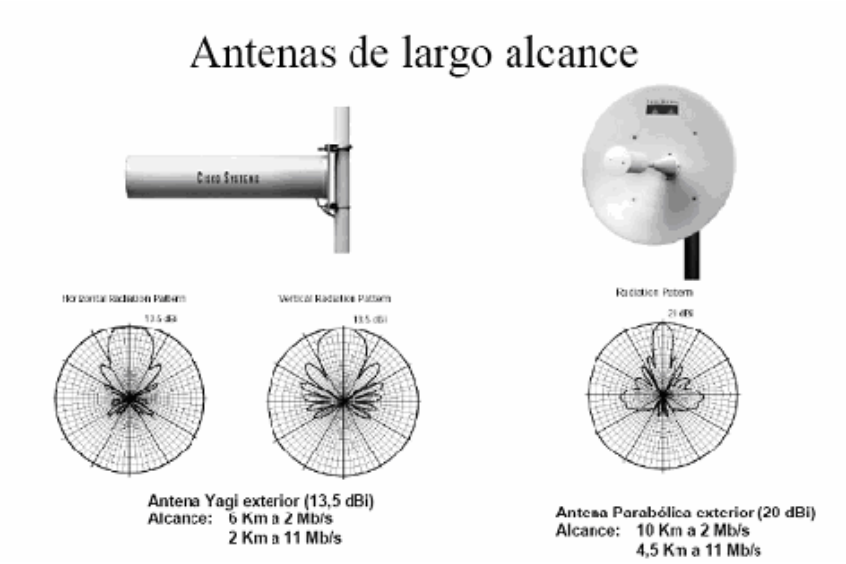


Figura 33 Muestra antenas de largo alcance

5.2.1.7. EL PROBLEMA DE LA SEGURIDAD INALAMBRICA

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere.

Cualquier equipo que se encuentre a 100 metros o menos de un Access Point, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o

más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya. Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.[16]

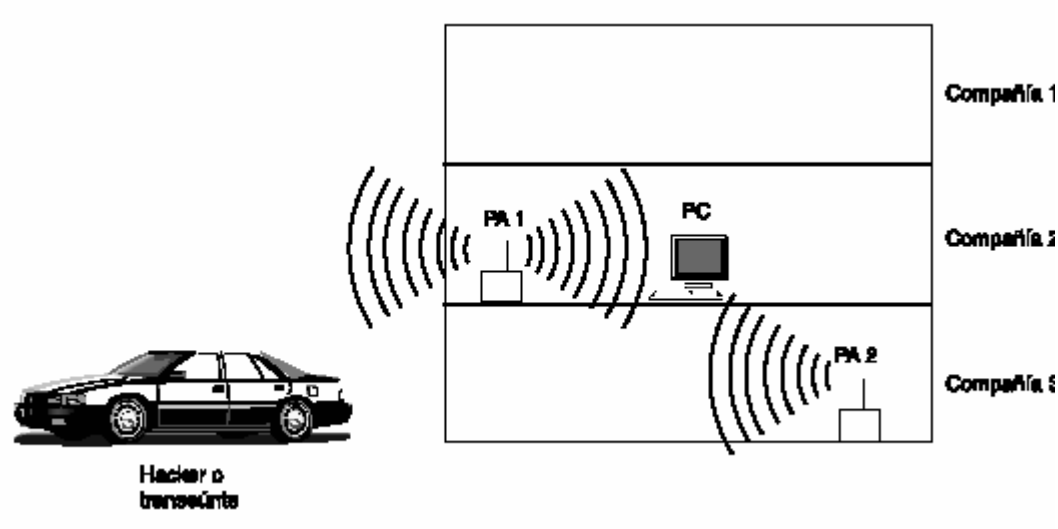


Figura 34 Acceso no autorizado a una red inalámbrica.

Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la red de una empresa. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio.

Cualquier persona que desde el exterior capte la señal del Access Point, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en la Internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas. Un Access Point inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

[16] *Esta información fue obtenida del sitio Web http://www.microsoft.com/windowsxp*

La mala configuración de un acceso inalámbrico es, desgraciadamente, una cosa muy común. Un estudio publicado en 2003 por RSA Security Inc. encontró que de 328 puntos de acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP (Wired Equivalent Protocol).

Además, cien de estos puntos de acceso estaban divulgando información que permitía identificar la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica.

Existen dos prácticas bien conocidas para localizar redes inalámbricas:

El warchalking, que consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del Access Point y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

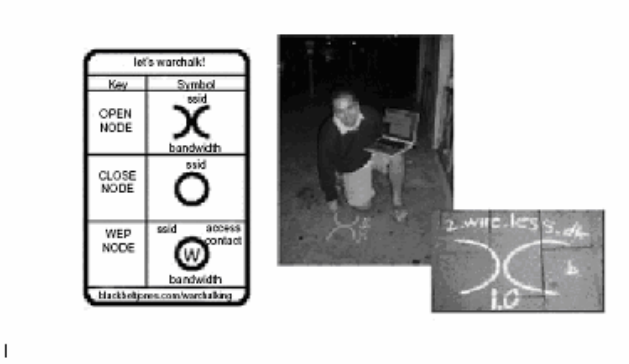


Figura 35. Warchalking y su Simbología.

El wardriving, propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en la Internet.

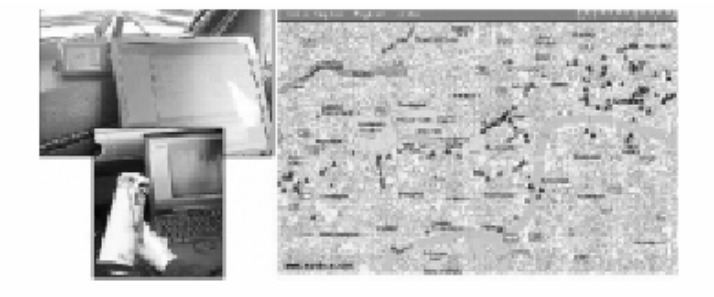


Figura 36. Wardriving.

A la izquierda puede observarse el equipo necesario (computador, GPS y antena); a la derecha, los triángulos indican sobre el mapa la posición de redes inalámbricas.

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un Access Point propio, orientando la antena de tal modo que los computadores que son clientes legítimos de la red atacada se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichos computadores, instalarles software maligno o dañar la información.

5.2.1.8. TIPOS DE ATAQUES EN REDES INALAMBRICAS

5.2.1.8.1. MÉTODOS DE ATAQUE

Los métodos de ataque pueden diferenciarse entre ataques pasivos y ataques activos.

5.2.1.8.1.1. ATAQUES PASIVOS

En los ataques pasivos no se ataca la red, sino que discretamente se accede a la red y se analiza la circulación de datos. Este tipo de ataques sirven para espiar información como Direcciones IP, contraseñas, etc, y en muchas ocasiones sirven como preparación para un ataque activo.

Los ataques más peligrosos se pueden dividir de la siguiente manera:

Port Scanning: (escaneo de puertos) como todos los protocolos TCP (Protocolo de control de transmisión) y UDP (Protocolo de datagramas de usuario) que ofrece el computador los ofrece por, es muy útil para espiar el número de puerto usado. Así se puede a través de un número de puerto evitar la función del Firewall para atacar más tarde de forma activa. El Port Scanning (Escaneado de puertos) funciona de tal manera que el atacante envía datos con distintos números de puerto a la computadora "escaneada". Como con cada TCP se responde a cada petición de acceso, si es necesario se responderá con un mensaje de error y el atacante puede espiar los puertos.

Sniffing: Aquí el atacante necesita una entrada a la red. Por medio de un analizador de protocolos (ej. Ethherreal, Sniffer…) se graban y analizan todos los datos. Estos ataques son muy difíciles de llevar a cabo en redes convencionales, ya que se necesita o bien un acceso directo o una red interna (Ataque de colaborador), o grabar y analizar todos los datos de un segmento a través de conexión a Internet. En las redes LAN inalámbricas este acceso es más sencillo, ya que las ondas electromagnéticas también pueden recibirse desde el exterior del edificio. Si los datos no están codificados el "fisgón" puede escuchar y grabarlos fácilmente los datos.

5.2.1.8.1.2. ATAQUES ACTIVOS

Si el hacker ya ha obtenido suficiente información a través de los ataques pasivos puede atacar la red de forma directa y cambiar los datos, y parar el sistema.

Estos ataques tienen como objetivo dañar la integridad y la disponibilidad del sistema:

Spoofing (engaño): IP Spoofing (engaño de IP): Muchos privilegios en la red se gestionan por medio de direcciones IP inequívocas. El atacante puede acceder a los datos si ha encontrado las direcciones. DNS Spoofing (engaño de DNS):

El *Domain Name System,* sistema de referencia/información en Internet, que se encarga de trasladar las direcciones que se detectan fácilmente (ej. www.fh-stpoelten.ac.at) a las direcciones IP correspondientes (198.15.13.12). Cuando el usuario introduce una dirección de este tipo en el navegador origina en un segundo plano una petición en el servidor DNS.

Este servidor DNS, a su vez, memoriza las direcciones por servidores superiores, es decir, por peticiones anteriores. Ya que el servidor DNS no comprobó la veracidad de los datos, también graba la información falsa que le proporciona un atacante. El usuario es enviado a un servidor falso, y no se da cuenta del ataque, ya que casi nunca conoce la dirección IP correspondiente. MAC Spoofing (de engaño de MAC): Al igual que con IP Spoofing, aquí se utiliza una dirección MAC conocida de un usuario para poder fingir una identidad falsa.

Ataques Jamming (ataque denegación de servicio): El atacante intenta parar la red o una sola computadora, mediante un número elevado de peticiones. Para hacerlo utiliza fallos de protocolo. (Ej.: TCP SYN Flooding)

Ataques Man-in-the.middle (ataque de intercepción): El atacante se interpone y finge ser usuario y servidor al mismo tiempo. Estos ataques son especialmente peligrosos ya que el atacante obtiene toda la información necesaria sobre los certificados de seguridad, etc. Este peligro es muy elevado sobre todo en redes LAN inalámbricas. El cliente siempre intenta conectarse desde el Access Point (Access Point, AP) que disponga de la señal más fuerte, por eso resulta normal que se cambie al AP que disponga de la emisión más potente. Por tanto, si se acepta un AP "falso", quizás incluso con una potencia de emisión demasiado alta, todos los clientes se cambiarán a la señal del atacante y transferirán todos sus datos a través de esta nueva vía. Para el atacante se vuelve muy sencillo filtrar los datos que le interesan. Por supuesto el AP tiene que estar configurado (SSID,…) de antemano en el AP "correcto".

Perturbación de la banda de frecuencia a través de un interferente: Las redes LAN inalámbricas se pueden interrumpir muy fácilmente activando un emisor con una mayor potencia. Estos ataques suelen afectar sobre todo a la disponibilidad de las redes.

5.2.1.9. PROTOCOLOS DE SEGURIDAD EN REDES INALAMBRICAS

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito.

Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar. Para poder entender la forma de implementar mejor la seguridad en una red Inalámbrica, existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas.
Entre los protocolos de seguridad tenemos:

5.2.1.9.1.WEP (WIRED EQUIVALENT PROTOCOL):

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un Access Point o una estación cliente es la encargada de desencriptar la trama.

Como parte del proceso de encriptación, WEP prepara una estructura denominada 'seed' obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generada aleatoriamente. La estación cambia el IV para cada trama transmitida.

A continuación, WEP utiliza el 'seed' en un generador de números pseudoaleatorio que produce una llave de longitud igual a el payload (cuerpo más CRC) de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud.

El ICV es un checksum que utiliza la estación receptora para recalcularla y compararla con la enviada por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma.

WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica.

Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que producirá el texto cifrado. Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama.

La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación receptora para desencriptar la parte del payload del cuerpo de la trama.

Cuando se transmiten mensajes con el mismo encabezado, por ejemplo el FROM de un correo, el principio de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el principio de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación. Esto se soluciona utilizando un IV diferente para cada trama.

La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo. Si utilizamos solamente 24 bits, WEP utilizará el mismo IV para paquetes diferentes, pudiéndose repetir a partir de un cierto tiempo de transmisión continua. Es a partir de entonces cuando un intruso puede, una vez recogido suficientes tramas, determinar incluso la llave compartida.

En cambio, 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistemas y los usuarios utilizan las mismas llaves durante días o incluso meses. Algunos vendedores han desarrollado soluciones de llaves dinámicas distribuidas.

A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

5.2.1.9.2. OSA (OPEN SYSTEM AUTHENTICATION)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

5.2.1.9.3. ACL (ACCESS CONTROL LIST)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

5.2.1.9.4. CNAC (CLOSED NETWORK ACCESS CONTROL)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

5.2.1.9.5. WPA (WI-FI PROTECTED ACCESS, ACCESO PROTEGIDO WI-FI)

Es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

5.2.1.9.5.1. CARACTERÍSTICAS DE WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un Access Point con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del Access Point. El Access Point mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el Access Point abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el Access Point (como priorizar ciertos tráficos o descartar otros).

EAP, definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).

TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.

MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

5.2.1.9.5.2. MEJORAS DE WPA RESPECTO A WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2

elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un Access Point con esta funcionalidad.

5.2.1.9.5.3. MODOS DE FUNCIONAMIENTO DE WPA

WPA puede funcionar en dos modos:

Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y Access Point. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

5.2.1.9.6. 802.11i.

El instituto IEEE aprobó recientemente (julio 2004) la norma 4002.11i, una extensión de la 802.11 para mejorar la seguridad.

5.2.1.9.7. WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

También podemos mencionar que WPA2 es la segunda generación de WPA. Proporciona encriptación con AES (Seguridad de Encriptación Avanzada), un alto nivel de seguridad en autentificación de usuarios y esta basado en la norma IEEE 802.11i.

Además proporciona administración de red con alto nivel de seguridad de forma que solamente los usuarios autorizados puedan acceder a la red, esta tecnología de cifrado WPA2 pone la seguridad de redes inalámbricas dos generaciones más avanzadas que la WEP.[17]

5.2.1.9.8. MÉTODOS DE AUTENTICACIÓN DE EAP

EAP soporta muchos métodos de autenticación. Estos métodos pueden usar diferentes protocolos de autenticación como por ejemplo el protocolo de

[17] *Esta información fue obtenida del sitio Web http://www.jamdrid-seguridad- redes- inalambricas*

autenticación Kerberos versión 5, el protocolo TLS (Seguridad en la capa de transporte), y el protocolo MS-CHAP.

Los métodos principales para el uso de WLANs son EAP –TLS, EAP protegido (PEAP), TLS por tunel (TTLS), EAP liviano (LEAP).

5.2.1.9.8.1. EAP –TLS

Definido en la RFC 2716 y es probablemente el método de autenticación más ampliamente soportado en clientes inalámbricos y en servidores RADIUS. Este método utiliza claves publicas certificadas para autentificar tanto al cliente como al servidor mediante el establecimiento de una sesión encriptada entre ellos.

5.2.1.9.8.2. PEAP

Este es un método de autenticación de dos pasos. Primeramente, establece una sesión TLS con el servidor y permite al cliente autentificar al servidor usando la certificación digital del servidor. Luego, se requiere un segundo método EAP haciendo un túnel dentro de la sesión PEAP para autenticar al cliente hacia el servidor RADIUS.

5.2.1.9.8.3. TTLS

Es un método de 2 pasos similar a PEAP, el cual usa una sesión TLS para proteger la autenticación por medio de túnel del cliente. Además de los métodos de túnel de EAP, TTLS puede usar versiones de protocolos de autenticación que no sean EAP tales como CHAP, MS-CHAP, y otros.

5.2.1.9.8.4. LEAP

Es un método EAP propietario de Cisco que utiliza claves para autenticar los clientes. LEAP solo trabaja con software y hardware de Cisco y otros pocos proveedores. Tiene muchas vulnerabilidades tales como la susceptibilidad a ataques para descubrir las claves de usuarios, también que solo puede autenticar a los

usuarios para entrar a la WLAN no a la computadora, sin esto las políticas de la maquina no se ejecutaran debidamente ni tampoco las instalaciones de programas.[18]

5.2.1.10. MÉTODOS DE ENRUTAMIENTO INALÁMBRICO

Cuando se trata de construir una red inalámbrica de área extensa, es muy conveniente disponer de más de un punto de acceso a Internet pues ello nos permite disminuir los problemas de interferencia ya que podemos trabajar con menores potencia de transmisión y también permite mejorar el ancho de banda disponibles por cada usuario. Además es muy conveniente disponer de un sistema que automáticamente reenrute las señales en caso de falla de uno de los puntos de acceso a Internet. Se han propuesto numerosas soluciones para este fin y nosotros nos enfocaremos en una de dominio público conocida como AODV (Ad Hoc Distance Vector).

Una de las características que define a AODV es el uso de tablas de enrutamiento en cada nodo para evitar transportar rutas en los paquetes. Cada destino de la tabla de enrutamiento lleva asociado un número de secuencia y un temporizador o lifetime. Este número permite distinguir entre información nueva e información antigua, de tal manera que se evita la formación de lazos y la transmisión de rutas caducadas. La función del temporizador es evitar usar enlaces de los que no se conoce su estado desde hace mucho tiempo.

AODV no mantiene rutas para cada nodo de la red. Estas rutas son descubiertas según se vayan necesitando bien sea que se activen o desactiven nodos en la red. AODV es capaz de proveer transmisión unicast, multicast y broadcast. La transmisión unicast consiste en enviar datos de un nodo a otro, la trasmisión multicast consiste en enviar información de un nodo a un grupo de nodos y la transmisión broadcast consiste en enviar datos de un nodo a los demás nodos de la red. Los descubrimientos de rutas son siempre bajo demanda y siguen un ciclo de petición/respuesta de ruta.

Las peticiones son enviadas usando un paquete especial denominado RREQ (Route Request). A su vez, las respuestas son enviadas en un paquete denominado

[18] *Esta información fue obtenida de www.securitywireless.info*

RREP (Route Reply). A continuación se resume la secuencia de pasos para descubrir una ruta:

- Cuando un nodo desea conocer una ruta hacia un nodo destino, envía por broadcast un RREQ.
- Cualquier nodo que conozca una ruta hacia el destino solicitado (incluído el propio destino) puede contestar enviando un RREP.
- Esta información viaja de vuelta hasta el nodo que originó el RREQ y sirve para actualizar las rutas de los nodos que lo necesiten.
- La información recibida por el nodo destino del RREP se almacena en su tabla de enrutamiento.

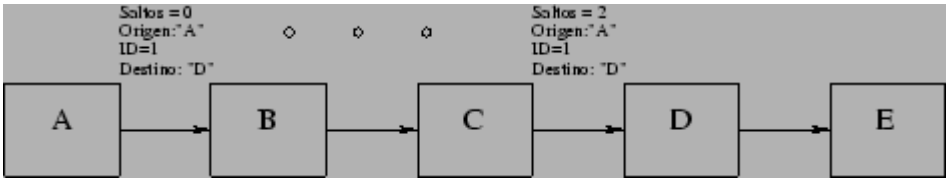
Ahora, el nodo ya podría enrutar su paquete de datos, pues ya conoce un camino hacia su destino.

5.2.1.10.1. DESCUBRIMIENTO DE RUTAS

Antes de descubrir las rutas, los nodos deben estar debidamente configurados, bajo la modalidad requerida (Ad-Hoc).

Cuando un nodo desea enviar datos a otro, primero comprueba si tiene alguna entrada en su cache de rutas para dicho destino. Si tiene alguna entrada activa, enruta los datos por el vecino que le indica la tabla. Sin embargo, si el origen no dispone de una entrada activa, bien porque es la primera vez que se va a comunicar con él, o bien porque el plazo para esa destino ha expirado (al comprobar el campo lifetime y la fecha de última modificación), se inicia un descubrimiento de ruta. Para ello se debe crear un paquete RREQ que contiene información relativa al nodo destino e información propia. Cada paquete RREQ es identificado unívocamente con un identificador propio, unido al originador del mensaje. Este identificador se incrementa cada vez que se genere un nuevo RREQ y lo utilizan los nodos intermedios para saber si deben retransmitir el paquete o, por el contrario, descartarlo porque ya lo retransmitieron con anterioridad. Dichos nodos, aún no siendo los destinatarios del RREQ mantienen una entrada para ese destino en su tabla de enrutamiento, y contestarán al origen para evitar la propagación innecesaria

de RREQ a través de la red. Aquí es donde entran en juego los números de secuencia. Cuando un nodo reenvía un RREQ, añade una ruta inversa en su tabla, que apunta al origen del RREQ (suponiendo enlaces simétricos). Si este paquete llega al destinatario, éste devolverá un RREP al origen, a través del camino inverso por el que le llegó la petición. Por ejemplo, observando la figura supongamos que el nodo A quiere descubrir una ruta hacia el nodo D:



Ejemplo de descubrimiento de ruta entre A y D.

Para iniciar un descubrimiento de ruta el nodo A transmite un RREQ enviando un único paquete en modo broadcast, el cual es recibido por todos los nodos que están en el rango de transmisión de A (en nuestro ejemplo, incluiría el nodo B). Cada Route Request incluye el origen y el destino del descubrimiento de ruta, además del identificador único (en nuestro ejemplo el 1) otorgado por el iniciador de la petición. Cada Route Request contiene, además, datos del origen para que los nodos intermedios puedan actualizar sus tablas con esta información. Por último también se añade un campo con información del número de saltos que da el paquete. Cuando otro nodo reciba esta petición (el nodo B en el ejemplo), si él fuera el destinatario del descubrimiento de ruta, devolvería al origen un RREP. Cuando el origen recibiera esta Route Reply, almacenaría en su cache este camino para los futuros envíos al mismo destino. En nuestro ejemplo, el nodo B que recibe el Route Request, comprueba que no le ha llegado con anterioridad otra petición con mismo origen y mismo identificador. Después de esto, verifica que no es el destinatario del RREQ y tampoco dispone de una ruta hacia el nodo D. A continuación, reenvía por broadcast la petición incrementando en una unidad el número de saltos. Como también viaja la información del nodo que originó la petición, podría añadir una ruta en su tabla para llegar hacia dicho nodo. El vecino por el que le ha llegado el RREQ, sería el nodo escogido para enrutar los paquetes hacia el nodo origen del RREQ. Esta última petición es recibida por el nodo C, que hace lo mismo, y por el nodo A, que descarta el paquete debido a que él fue quién lo inició. Por último, la petición lega al nodo D

que es el destino. Este último, mandará el Route Reply correspondiente al nodo A con la ruta obtenida por Route Request. Para enviar este paquete al nodo A, mirará en su caché para obtener algún camino o iniciará otro Route Discovery si fuera necesario. No hay que olvidar que debido a la omnidireccionalidad de los envíos, el nodo B también obtendría una copia del último mensaje, descartándolo por haberlo reenviado con anterioridad.

5.2.1.10.2. MANTENIMIENTO DE RUTAS

Cuando se establece una ruta entre dos nodos, la ruta se considera válida durante un periodo de tiempo. Esto es debido a que los nodos son móviles y un camino que antes era óptimo, pasado un tiempo puede que ni siquiera sea válido porque es posible que el nodo no sea visible por obstrucciones o desvanecimiento de las ondas. Para defenderse de estas situaciones, AODV utiliza el mantenimiento de rutas. Si el nodo origen de un envío se mueve (y altera la topología de la red), él debe reiniciar un nuevo descubrimiento de ruta hacia el destino. Sin embargo, si ha sido el nodo destino de los datos el que se ha movido o algún nodo intermedio, y hay algún mensaje dirigido hacia él, un mensaje especial de error en ruta (RERR) será enviado al nodo que originó el envío, por el nodo que advierta el cambio en la topología de la red. Es importante resaltar que no todos los cambios de los nodos ocasionan operaciones en el protocolo, recordemos que AODV enruta bajo demanda. Todos los nodos por los que atraviese este paquete (RERR), cancelarán las rutas que pasaran por el nodo que se ha vuelto inaccesible. En el momento que el RERR llegue a su destino, éste puede decidir dar por terminado el envío o iniciar un nuevo RREQ si aún necesitase establecer la comunicación. Es preciso mantener información actualizada de quiénes son los vecinos de cada nodo cada cierto tiempo. Cada vez que un nodo recibe un paquete de algún vecino, la entrada para ese vecino en la tabla de rutas se renueva, pues se sabe con seguridad que sigue en su lugar. Si no hubiera entrada todavía para el vecino, se crearía una nueva en la tabla de enrutamiento. Además, cada cierto intervalo de tiempo, se mandan paquetes HELLO a los vecinos para informarles que el propio nodo sigue activo. Esta información es usada por los vecinos para actualizar los temporizadores asociados a dicho nodo o

en su defecto, para deshabilitar las entradas que se encaminen por el nodo que no responde.

5.2.1.10.3. DEFINICIÓN DE RED AD-HOC

Las redes de computadores inalámbricas (Wireless Networks) pueden clasificarse en dos grandes grupos:

Redes con infraestructura:

Constan de un número fijo de enlaces cableados entre sí. Cada host móvil debe comunicar con uno de estos enlaces dentro de su radio de acción. El nodo puede moverse libremente pero si sale fuera del rango de cobertura de la radio base, debe conectar con otra radio base para asegurar que la información llegue a su destino. Un ejemplo de este tipo de redes es la red de telefonía móvil formada por numerosas estaciones bases y antenas dispersas por todas las ciudades.

Redes sin infraestructura (Ad-Hoc):

Formadas por hosts móviles y que pueden estar conectados entre sí arbitrariamente y de manera dinámica. Es decir, no hay ningún elemento fijo y la topología de la red puede adoptar múltiples formas siendo igual de funcional. En este tipo de redes, todos los nodos funcionan como enrutadores (routers) y se ven involucrados tanto en el descubrimiento como en el mantenimiento de rutas.

Los algoritmos de enrutamiento usados en las redes Ad-Hoc se pueden clasificar en dos grupos:

Basados en tablas de enrutamiento:

Estos algoritmos tratan de mantener la información necesaria para el enrutamiento continuamente actualizada. Cada nodo mantiene una o más tablas con los datos para encaminar hacia cualquier otro nodo de la red. Los cambios en la topología de la red propician el envío masivo de paquetes para mantener las tablas actualizadas. Los siguientes algoritmos se encuadran dentro de esta categoría: DSDV (The Destination-Sequenced Distance-Vector Routing Protocol), CGSR(Clusterhead Gateway Switch Routing) y WRP (The Wireless Routing Protocol). Los protocolos anteriores difieren en el número de tablas utilizadas y en la política de envío de paquetes para mantener las tablas actualizadas.

Basados en enrutamiento bajo demanda:

En contraste con los algoritmos basados en tablas, las rutas son creadas sólo cuando se requieren. Cuando un nodo requiere una ruta hacia un destino concreto se inicia un proceso de descubrimiento de ruta. Este proceso termina cuando se encuentra un camino hacia el destino o cuando se examinan todas las alternativas y ninguna lleva al destino final. Cuando la ruta es descubierta, es necesario mantenerla (mantenimiento de ruta) hasta que el destino se vuelva inalcanzable o la ruta deje de ser necesaria. Algunos ejemplos de este tipo de protocolos son: AODV (Ad Hoc On-Demand Distance Vector Routing), DSR (Dynamic Source Routing), LMR (Lightweight Mobile Routing), TORA (Temporary Ordered Routing Algorithm), ABR (Associative-Based Routing) y SSR (Signal Stability Routing).

5.2.2. TIPOS DE REDES

5.2.2.1. REDES DE AREA DE ALMACENAMIENTO (SAN)

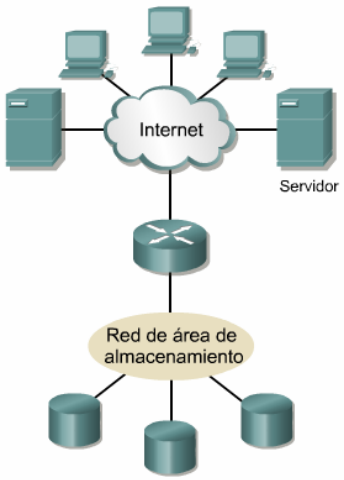


Figura 37 Ejemplo Red de area de almacenamiento

Una SAN es una red dedicada, de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada, evita todo conflicto de tráfico entre clientes y servidores.

La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor. Este

método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

Las SAN poseen las siguientes características:

- Rendimiento: Las SAN permiten el acceso concurrente de matrices de disco o cinta por dos o más servidores a alta velocidad, proporcionando un mejor rendimiento del sistema.
- Disponibilidad: Las SAN tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de10 kilómetros (km) o 6,2 millas.
- Escalabilidad: Al igual que una LAN/WAN, puede usar una amplia gama de tecnologías. Esto permite la fácil reubicación de datos de copia de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas.

5.2.2.2. RED PRIVADA VIRTUAL (VPN)

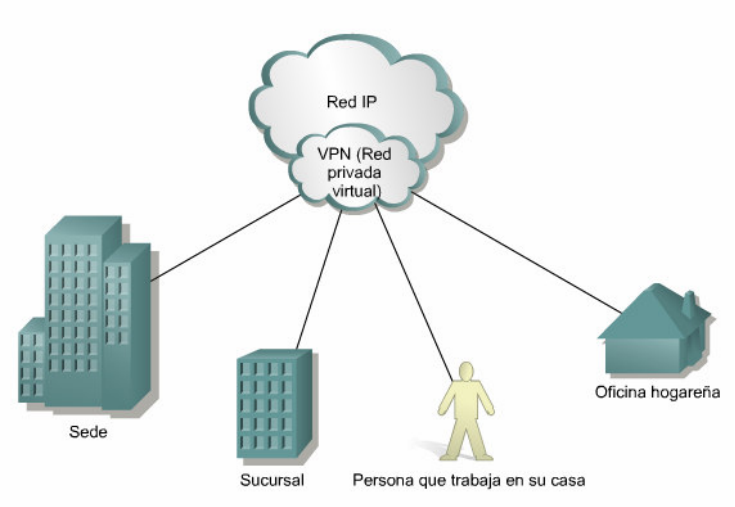


Figura 38 Ejemplo de red rrivada virtual

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

Los productos Cisco admiten la más reciente tecnología de VPN. La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como la Internet. Las VPN conservan las mismas políticas de

seguridad y administración que una red privada. Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa.

A continuación se describen los tres principales tipos de VPN:

- VPN de acceso: Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.
- Redes internas VPN: Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.
- Redes externas VPN: Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

5.2.2.3. REDES INTERNAS Y EXTERNAS

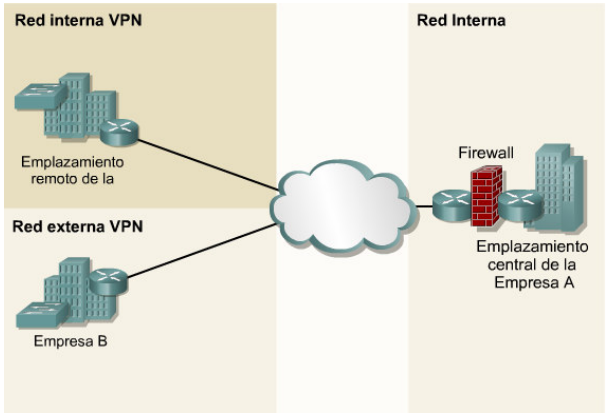


Figura 39 Ejemplo de redes internas y externas

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "Intranet". Los servidores de Web de red interna son distintos de los servidores de Web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización. Dentro de una red interna, los servidores de Web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.

Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.[19]

5.2.3. TECNOLOGÍAS DE CÓDIGO ABIERTO

Cada vez son más las empresas que apuestan por software Open Source (Código Abierto), y cada vez son más las que repiten la experiencia después de los buenos resultados que obtienen. Software Open Source es el software que permite ver abiertamente su código fuente y disponer de él, de manera que se puedan hacer modificaciones, revisiones o adaptaciones. Las ventajas del Open Source para una empresa son numerosas:

Bajo costo: las aplicaciones Open Source tienen un costo muy bajo o incluso nulo en muchos casos, lo cual repercute directamente en el costo de su proyecto : permite ahorrar una gran cantidad de dinero en licencias comerciales de Gestores de Base de Datos, Servidores Web, Servidores de Correo, Servidores de Aplicaciones, Intranet, etc.

A modo de ejemplo, destacar que Amazon.com cambió en el año 2000 todo su servicio a Linux, ahorrando así 17 millones de dólares (similar cantidad en euros).

[19] *Esta Información fue obtenida de Currículo Cisco CCNA Semestre 1version 3.1 en Español módulo 2 Aspectos básicos de Networking*

Mayor seguridad: de forma contraria a como piensa mucha gente, el hecho que el código de un programa no se pueda ver no indica que sea más seguro. Al contrario, si aparece un fallo de seguridad en ese código, al tratarse de algo cerrado, únicamente puede ser arreglado por la empresa o persona que lo haya desarrollado. Por lo tanto, permanecerá inseguro hasta el momento que los responsables de ese programa solucionen el problema. Sin embargo el código Open Source puede ser visto por todo el mundo y cualquier persona puede verificar y encontrar problemas de seguridad en el código.

Como ejemplo, podemos ver el famoso fallo de 'Ping of Death' en 1997, el cual afectaba prácticamente a la totalidad de los sistemas operativos presentes en el momento. Mientras que Linux solucionó el problema en unas cuantas horas, los sistemas operativos comerciales tardaron meses en solucionarlo.

Menor riesgo para su empresa: al poseer el código fuente, su empresa no liga la inversión hecha en el software a la empresa que lo realizó. Se han visto muchos casos de programas de código cerrado, que las empresas que los desarrollaron han abandonado, o han quebrado, quedando el cliente adquiriente del software sin posibilidades de mantener o actualizar sus sistemas. Esto no ocurre con el Open Source, ya que teniendo el código fuente, cualquier otra empresa podrá realizar las adaptaciones que a usted le sean necesarias. *

5.2.4. PLATAFORMA WEB

Normalmente en los sistemas basados en WEB se usa la arquitectura cliente-servidor.

Este tipo de organización se basa en que entre todos las Computadoras que están en la red, unos ofrecen servicios (los llamados servidores) y otros usan esos servicios (los denominados clientes). Como ejemplo, cuando están visualizando estas páginas, están accediendo a un servicio (pidiendo una página WEB concreta) que les ofrece nuestro servidor de páginas WEB (sirviéndole la página solicitada). Por lo tanto, su Computadora es un cliente y el que hospeda estas páginas es un Servidor.

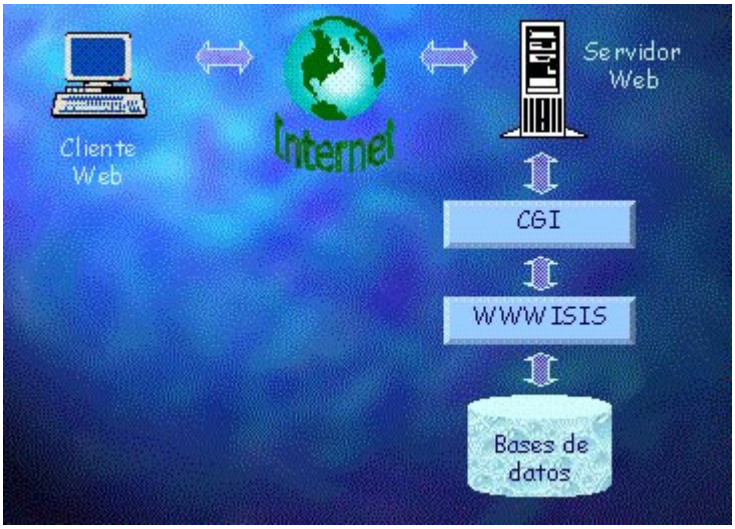


Figura 40 Ejemplo de funcionamiento de plataforma Web

Una red puede tener un servidor que distribuya datos a múltiples clientes a la vez. Un cliente también podría tener múltiples servidores enviando datos simultáneamente.

En el entorno de computación actual, Una Computadora Windows, Macintosh, UNIX o una computadora grande, puede ser un cliente. Cualquiera de estas plataformas puede actuar como servidor e incluso puede actuar como cliente y servidor simultáneamente. Esta doble función es posible debido a las capacidades multitarea de los modernos sistemas operativos.

5.2.5. GNU

El proyecto GNU fue iniciado por el hacker estadounidense Richard Stallman con el objetivo de crear un sistema operativo completo totalmente libre: el sistema GNU . Se anunció públicamente el proyecto el 27 de septiembre, de 1983, en el grupo de noticias net.unix-wizards. Al anuncio original, siguieron otros ensayos escritos por Richard Stallman como el “Manifiesto GNU“, que establecieron sus motivaciones para realizar el proyecto GNU, entre los que destacamos “retornar al espíritu de cooperación que prevaleció en los tiempos iniciales de la comunidad de usuarios de computadoras”.

GNU es un acrónimo recursivo que significa “GNU No es Unix”. Stallman sugiere que se pronuncie Ñu (se puede observar que el logo es un ñu) para evitar confusión con “new” (nuevo). UNIX es un sistema operativo propietario muy popular,

porque está basado en una arquitectura que ha demostrado ser técnicamente estable. El sistema GNU fue diseñado para ser totalmente compatible con UNIX. El hecho de ser compatible con la arquitectura de UNIX implica que GNU esté compuesto de pequeñas piezas individuales de software, muchos de los cuales ya estaban disponibles, como el sistema de edición de textos TeX y el sistema gráfico X Window, que pudieron ser adaptados y reutilizados; otros en cambio tuvieron que ser reescritos.

Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en inglés como copyleft (en clara oposición a copyright, derecho de copia), y está contenida en la Licencia General Pública de GNU (GPL).

5.2.6. ¿QUÉ ES LA LICENCIA GPL?

Los programas de Computadora suelen distribuirse con licencias propietarias o cerradas.

Estas licencias son intransferibles y no exclusivas, es decir, no eres propietario del programa, sólo tienes derecho a usarlo en una computadora o tantas como permita expresamente la licencia y no puedes modificar el programa ni distribuirlo.

La licencia GPL o General Public License, desarrollada por la FSF o Free Software Foundation, es completamente diferente. Puedes instalar y usar un programa GPL en una computadora o en tantas como te apetezca, sin limitación. También puedes modificar el programa para adaptarlo a lo que tú quieras que haga. Además, podrás distribuir el programa GPL tal cual o después de haberlo modificado.

Puedes hacer esto, regalando el programa o vendiéndolo, tu única obligación, es facilitar siempre con el programa binario el código fuente, es decir, el programa de forma que pueda ser leído por un programador.

Los programas propietarios o cerrados, solo se distribuyen en binario, listos para ejecutarse en la Computadora.

Los programas GPL no tienen garantía, igual que casi todos los programas propietarios, no obstante, ofrecen más derechos a sus usuarios y su sistema abierto

hace que los defectos sean detectados y depurados a gran velocidad con la ayuda de cientos de programadores a través de Internet. Por otro lado, nada impide a una empresa garantizar el Software Libre junto a otros servicios que oferte.

5.2.7. SERVIDOR APACHE

5. 2.7.1. ¿QUÉ ES APACHE?

Apache es un servidor Web, que permite el alojamiento de páginas Web en una máquina específica.

Esta herramienta tiene varias funciones tales como: permitir a los usuarios tener sus propias páginas Web, restricción a determinados sitios Web, conexiones seguras a través de SSL, configuración de módulos de programación.

5. 2.7.2. ¿DÓNDE OBTENERLO?

El software lo puedes obtener del sitio oficial http://www.apache.org, la UNAM cuenta ya con un sitio espejo de este sitio en apache.unam.mx.

Para instalar Apache se requiere:

- Aproximadamente 12 MB durante la instalación, y 3MB para alojamiento.
- Compilador ANSI-C, es recomendable GCC se obtiene de http://www.gnu.org/

  Para IRIX, se puede obtener gcc de http://freeware.sgi.com/ y seguir las instrucciones de instalación en IRIX.

5. 2.7.3. ARQUITECTURA DEL SERVIDOR APACHE

El servidor Apache es un software que esta estructurado en módulos. La configuración de cada módulo se hace mediante la configuración de las directivas que están contenidas dentro del módulo. Los módulos del Apache se pueden clasificar en tres categorías:

- **Módulos Base:** Módulo con las funciones básicas del Apache.

- **Módulos Multiproceso:** son los responsables de la unión con los puertos de la máquina, aceptando las peticiones y enviando a los hijos a atender estas peticiones

- **Módulos Adicionales:** Cualquier otro módulo que le añada una funcionalidad al servidor.

Las funcionalidades más elementales se encuentran en el módulo base, siendo necesario un módulo multiproceso para manejar las peticiones. Se han diseñado varios módulos multiproceso para cada uno de los sistemas operativos sobre los que se ejecuta el Apache, optimizando el rendimiento y rapidez del código.

El resto de funcionalidades del servidor se consiguen por medio de módulos adicionales que se pueden cargar. Para añadir un conjunto de utilidades al servidor, simplemente hay que añadirle un módulo, de forma que no es necesario volver a instalar el software.[20]

5.3. MARCO EXPERIMENTAL

5.3.1. CASO PRÁCTICO

Escenario en el que vamos a compartir recursos, impresoras, servidores, espacios de almacenamiento, y además vamos a tener un acceso a Internet.

Tendremos una infraestructura de sistemas internos muy grande, a la cual se dirigirá la mayoría de las comunicaciones. El acceso a Internet no será muy amplio, basándose sobre todo en el uso del correo electrónico.

Vamos a suponer una empresa en la que disponemos de por ejemplo 50 computadoras repartidas por diferentes plantas y con un área física grande. La seguridad dentro de las comunicaciones será un aspecto crítico. Se aconsejará el uso de VPNs (Redes Privadas Virtuales).

Dispondremos de una infraestructura básica de comunicaciones tradicional mediante el uso de una red Ethernet 100, a la que conectaremos PA Routers 802.11g.

[20] *Esta Información fue obtenida del sitio Web http://www.inetsys.es/open.html*

Aunque aún no está estandarizada por el IEEE, la especificación 802.11g parece que va a ser el futuro de este tipo de redes. En este caso el coste de los PAs y TRs no va a ser un punto crítico, por lo que se recomienda fuertemente la compra de los mismos a marcas de reconocido prestigio como por ejemplo CISCO.

Hay que tener en cuenta que tratándose de una empresa, podríamos llegar a tener puntos con una gran demanda de ancho de banda y otros con muy poca. Hay que investigar cuáles pueden ser los puntos donde haya más concentración de máquinas, como pueden ser las zonas de reuniones, zonas de gran concentración de trabajadores. De esta forma después de hacer esta investigación decidiremos cuáles son las mejores zonas para montar el AP.

Desde el punto de vista de la seguridad y después de comentar el punto anterior, hay que pensar también que las antenas es mejor colocarlas en lugares ¿centrales? del edificio, donde el radio de alcance de la señal no exceda demasiado del edificio físico en el que se encuentre.

En cualquier caso, siempre o casi siempre tendremos cobertura inalámbrica fuera de nuestro edificio. Por ello hay que seguir las normas de seguridad escrupulosamente.[21]

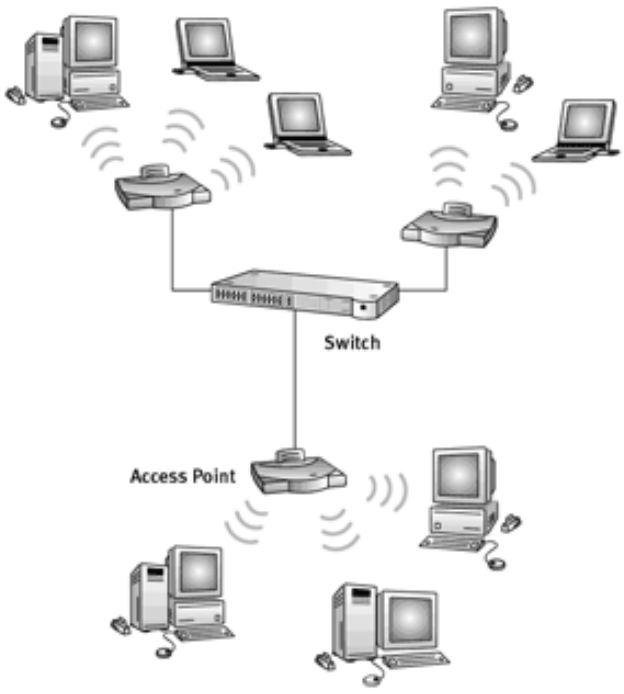


Figura 41. Representación gráfica de una red inalámbrica

[21] *Esta información fue obtenida del sitio Web http://www.el202.homeip.net/schedule.htm*

5.3.2. APLICACIÓN DE LAS WLAN

Las redes inalámbricas permiten a las empresas la conectividad en red de sus empleados en todo momento y sin necesidad de cables.

Una empresa en muchos casos necesita una serie de computadoras comunicadas entre ellas, situadas en el mismo o en varios locales diferentes. No siempre resulta cómodo y sencillo hacer el cableado de una red para unir estas computadoras, y en muchas ocasiones necesitan no estar situadas siempre sobre la misma mesa.

Ahora se tiene la posibilidad de disponer de comunicación entre diferentes computadoras olvidándose de la necesidad de llevar cable entre ellas. Las soluciones inalámbricas permiten disfrutar de las ventajas de una red de computadoras, sin tener que realizar importantes cambios en la estructura de los locales.

5.3.2.1. BENEFICIOS

- Acceso inalámbrico en toda la empresa.
- Aumentar la eficiencia y efectividad de los empleados.
- Reducir tiempo y problemas en la correcta actualización de información.
- Facilitar el acceso a la información.
- Conectar locales remotos y temporales al edificio principal.
- Facilitar conexiones portátiles a los empleados.
- Incrementar la movilidad y la flexibilidad de los empleados.

Las redes inalámbricas son totalmente compatibles con las redes cableadas tradicionales. Así que, si se tiene pensado una ampliación de la red actual, entonces es momento para instalar una red inalámbrica en la empresa: realizar la ampliación con una red inalámbrica resulta más sencillo, y se tiene una solución más flexible para el futuro.

Una red inalámbrica es la solución ideal para una empresa que cuente con trabajadores dotados de computadoras portátiles o de PDA. Con una WLAN no es necesario de canalizaciones para cable de red, rosetas con conexión activada a la

red, posibles variaciones en la configuración de los equipos portátiles según dónde se conecten, etc. Este tipo de usuarios podrán conectarse a la red desde cualquier lugar de la empresa y sin necesidad de modificar la configuración de su equipo.

Incluso aunque los empleados vayan a residir en un lugar fijo del local, con una computadora, se evitará el tener que llevar el cable hasta ese lugar, preparar la conexión, etc. La instalación y configuración del equipo en red será mucho más rápida y sencilla que si se conectara directamente a una red cableada tradicional.

Si se va a ampliar la distribución física de la empresa con un nuevo local o las características concretas del edificio en el que se encuentra situado el negocio impiden la realización de las obras necesarias para dotar de una red cableada de computadoras, una red inalámbrica evita cualquier tipo de obra o canalización para llevar el cable de red hasta las computadoras de los trabajadores y con un impacto visual mínimo en las distintas dependencias del edificio.

Ahora que, si la empresa dispone de dos o más locales, una solución consistente y más económica para conectar los sistemas informáticos es la realización de un enlace inalámbrico entre cada uno de los edificios. Aparte de las ventajas habituales de las redes inalámbricas, se añade la no existencia de cuotas mensuales por este tipo de comunicación.

La conexión mediante un enlace inalámbrico exterior de dos edificios está supeditada a la existencia de visión directa entre ambos edificios.

A continuación se plantean dos escenarios comunes en una empresa y de la cual se valen de una red inalámbrica para lleva a cabo esta actividades.

5.3.2.2. ESCENARIO 1

Entra un empleado a su oficina por la mañana y necesita pasar algunos archivos a la Intranet corporativa. Mientras va andando por el vestíbulo del edificio puede transferir los archivos en los que ha trabajado la noche anterior desde su computadora portátil a la LAN corporativa sin necesidad de cables y antes incluso de llegar a su despacho.

Una vez que ha llegado a su despacho decide enviar un correo electrónico a un compañero. Como ya ha establecido una conexión inalámbrica desde su

computadora portátil a la LAN corporativa podrá escribir y enviar el correo rápidamente.

A la hora de la comida lleva su computadora portátil a la cafetería de la empresa desde donde puede acceder a Internet o a la red corporativa a través de un Access Point inalámbrico.

Mientras está comiendo envía un correo electrónico a su hermano, que se encuentra en el otro extremo del país.

Después, envía otro mensaje a un compañero que está sentado al otro lado de la cafetería. Establecen contacto entre sus computadoras portátiles y juegan una partida rápida antes de volver a la oficina.

Por la tarde, antes de irse de la oficina, decide descargar en su computadora portátil una copia de un documento de la LAN corporativa. Con Bluetooth, no necesita intercambiar disquetes o CDs. Se establece la conexión y el archivo de la LAN se copia en su computadora portátil sin esfuerzo y en cuestión de segundos.

5.3.2.3. ESCENARIO 2

Se encuentra una persona de viaje de negocios y pasa mucho tiempo en los aeropuertos y hoteles. Le gustaría seguir en contacto con sus compañeros a través del correo electrónico y también tener acceso a Internet y a sus archivos almacenados en el servidor de red de su compañía.

Mientras está en el aeropuerto esperando a que salga su vuelo retrasado, enciende su computadora portátil y entra en el servicio de acceso inalámbrico a Internet situado en la Terminal, descarga los correos electrónicos que no ha leído y comprueba su carpeta de inversiones.

Dentro del avión responde a su correo y lo deja listo para enviarlo una vez en tierra. Una vez en el hotel, enciende su ordenador y accede al servicio de acceso a Internet inalámbrico, bien en su habitación o bien el vestíbulo, envía el correo que tenía preparado y descarga utilizando la VPN (*Virtual Private Network* / Red Privada Virtual) una presentación que había olvidado en la oficina.[22]

---

[22] *http://www.e-advento.com/soluciones/wlan.php*
http://www.tecnotopia.com.mx/redes/redinalambricas.htm

5.3.2.4. COORPORACIONES

Con WLAN los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartición de archivos, y visualización de web's, independientemente de dónde se ubiquen en la oficina.

5.3.2.5. EDUCACIÓN

Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios con computadoras conectarse a la red de la universidad para intercambio de opiniones en las clases, para acceso a Internet, etc.

5.3.2.6. FINANZAS

Mediante una PC portátil y un adaptador a la red WLAN, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios. Los grupos de auditorias contables incrementan su productividad con una rápida puesta a punto de una red.

5.3.2.7. CUIDADO DE LA SALUD

WLAN permite obtener información en tiempo real, por lo que proporciona un incremento de la productividad y calidad del cuidado del paciente eliminando el retardo en el tratamiento del paciente, los papeles redundantes, los posibles errores de trascripción, etc.

5.3.2.8. RESTAURANTES Y VENTA AL POR MENOR

Los servicios de restaurantes pueden utilizar WLAN para directamente entrar y enviar los pedidos de comida a la mesa. En los almacenes de ventas al por menor un WLAN se puede usar para actualizar temporalmente registros para eventos especiales.

5.3.2.9. MANUFACTURACIÓN

WLAN ayuda al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.

5.3.2.10. ALMACENES

En los almacenes, terminales de datos con lectores de código de barras y enlaces con redes WLAN, son usados para introducir datos y mantener la posición de las paletas y cajas. WLAN mejora el seguimiento del inventario y reduce los costos del escrutinio de un inventario físico.

CAPITULO VI IMPLEMENTACION DEL SISTEMA

El proyecto consiste en Implementar una Intranet para la empresa Lexincorp S.A. de C.V. con tecnología inalámbrica y seguridad de accesos para clientes Linux, Microsoft Windows y Macintosh OS X.

Esto se lograra a través de mecanismos de control y seguridad los cuales nos garanticen que la información que transita en nuestro sistema sea segura. Para esto ocuparemos ChilliSpot como portal cautivo para nuestra red el cual restringirá el acceso al Internet y a la Intranet a todo aquel usuario que no este registrado y FreeRadius como servidor AAA (Autenticación, Autorización y Auditoria) el cual nos monitoreara las sesiones y el tiempo de conexión de los usuarios autorizados. El esquema de red final planteado es el siguiente:

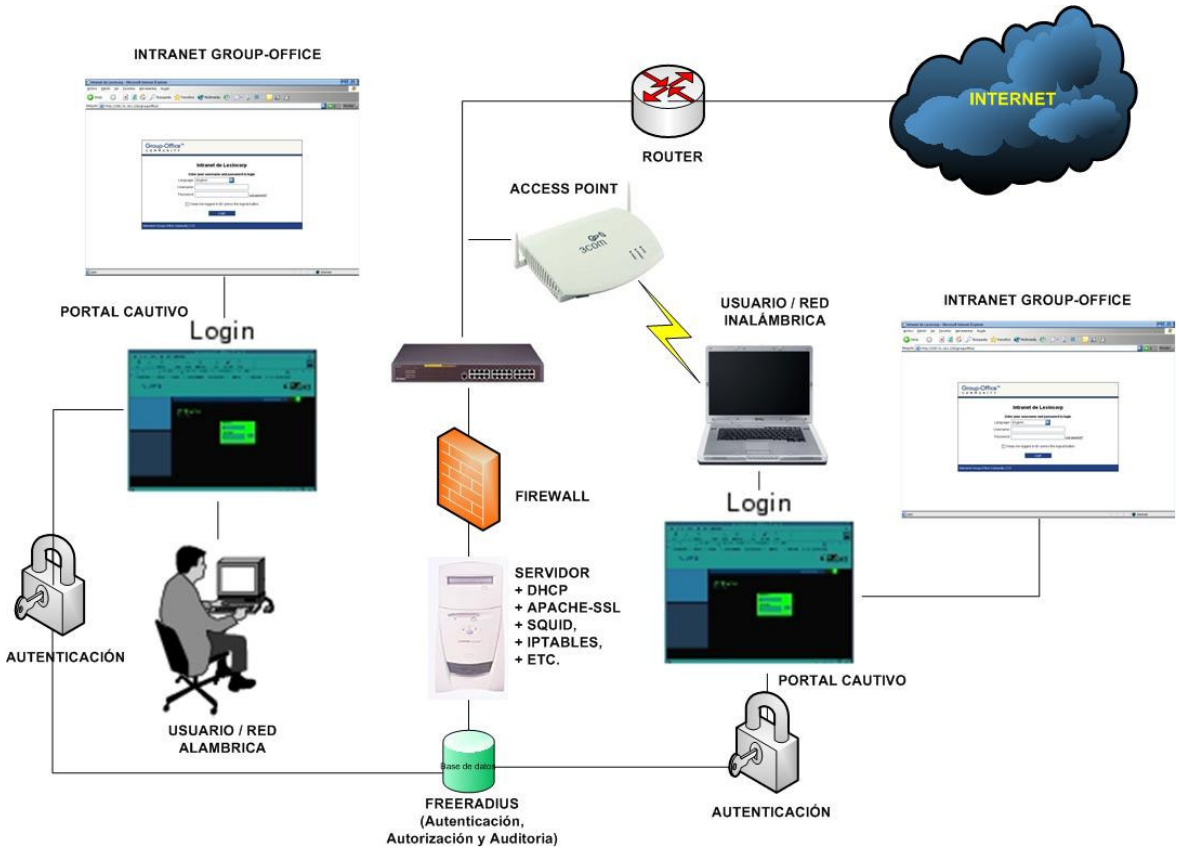


Figura 42 Muestra la implementación de la red

La implementación del sistema consiste en tres partes estas son:

a. Implementación del servidor:
    I. Sistema Operativo.
    II. Servicios.
    III. Interfaces de Red.
    IV. Seguridad en el servidor.
b. Implementación de la red inalámbrica.
    I. Pruebas de cobertura.
    II. Conclusiones para adquirir el equipo.
    III. Seguridad en el Access Point.
c. Implementación de la Intranet.
    I. Requerimientos de servicios.
    II. Pruebas del Software seleccionado.

6.1. IMPLEMENTACIÓN DEL SERVIDOR

6.1.1. SISTEMA OPERATIVO

Para el proyecto sea elegido software de código abierto por tal razón se ha elegido Linux distribución Debían Sarge 3.1 como sistema operativo, ya que este ofrece las siguientes ventajas:

- En Linux pueden correr varios procesos a la vez de forma ininterrumpida como un servidor de red.
- Seguridad porque es un sistema operacional diseñado con la idea de Cliente - Servidor con permisos de acceso y ejecución a cada usuario. Esto quiere decir que varios usuarios pueden utilizar una misma maquina al tiempo sin interferir en cada proceso.
- Linux es software libre, casi gratuito. Linux es popular entre programadores y desarrolladores e implica un espíritu de colaboración.
- Linux integra una implementación completa de los diferentes protocolos y estándares de red, con los que se puede conectar fácilmente a Internet y acceder a todo tipo de información disponible.

- Su filosofía y sus programas están dictados por el movimiento ”Open Source" que ha venido crecido en los últimos años y ha adquirido el suficiente fortaleza para hacer frente a los gigantes de la industria del software.
- Linux puede ser utilizado como una estación personal pero también como un potente servidor de red.
- Linux incorpora una gama de sistemas de interfaz gráfica (ventanas) de igual o mejor calidad que otras ofrecidas en muchos paquetes comerciales.
- Posee el apoyo de miles de programadores a nivel mundial.
- El paquete incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades del usuario.
- Utiliza varios formatos de archivo que son compatibles con casi todos los sistemas operacionales utilizados en la actualidad.[23]

6.1.2. SERVICIOS DEL SERVIDOR

Linux es un sistema operacional diseñado con la idea de Cliente - Servidor con permisos de acceso y ejecución, para esta implementación se ocuparán la mayoría de servicios en el servidor, a continuación se detalla cada uno de estos:

- Portal Cautivo: ChilliSpot es un programa o máquina de una red LAN o WLAN que restringe el tráfico HTTP:// y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. A veces esto se hace para pedir una autenticación válida, o para informar de las condiciones de uso de un servicio de una red alambrica o de una red inalámbrica. (Que es donde más se encuentran).
- Software AAA: FreeRadius es un sistema cliente/servidor usado para Autenticación, Autorización y Auditoria para asegurar la red contra accesos no autorizados, normalmente el router tiene el rol de cliente del servidor Radius, en este caso se utilizara en el servidor Linux.

[23] *Información obtenida de: http://www.maginvent.org/articles/linuxmm/Ventajas_Linux.html*

- Mysql-Server: es un Sistema de Gestión de Base de Datos, se utilizara para manejar las bases de datos del sistema de auditoria y para la Intranet.
- Apache: es un servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etcétera).
- Apache SSL: Apache-SSL es un servidor seguro de WWW, basado en Apache y SSLeay/OpenSSL, libre para uso comercial y no comercial, encriptación de 128 bit en cualquier sitio del mundo, Autenticación de clientes. Se utilizará en este caso para publicar un cgi el cual nos dará el acceso al portal cautivo.
- Proxy Web Squid: es un programa que sirve de Proxy-Cache de Internet
- Firewall Iptables: nos servirá como muro de fuegos el cual detendrá los ataques e intrusiones a la red.
- Samba: es una implementación libre del sistema de redes SMB de Microsoft. La versión 3 de Samba brinda servicios de archivos e impresión para varios clientes de Microsoft Windows y además puede integrarse a un dominio de Windows Server, como PDC o como Miembro del dominio. También puede ser parte de un dominio Active Directory.
- Software GPL Group Office para Intranet: Es una Intranet para Empresas o corporaciones que requieran compartir su información, esto a través de una interfaz Web amigable la cual Permite al administrador de la Intranet agregar, quitar módulos, tales como File Manager, Calendario, Address Book, Correo Electrónico, Project, entre otros. Además ofrece seguridad por medio de perfiles de usuarios.Los requisitos son: PHP, Mysql, Apache y para los módulos es necesario configurar samba (File Manager), módulos de Imap, mysql para Apache, entre otros. *http://sourceforge.net/projects/group-office/*
- Software GPL Dial-up admin: Software para el monitoreo y control de sesiones y tiempo de conexión de usuarios autorizados.

La instalación y configuración de cada uno de estos servicios se encuentran en los apéndices de este documento, para la instalación de Debían entrar al sitio http://www.debian.org/releases/stable/i386/.

6.1.3. INTERFACES DE RED

Para la implementación se ocuparan dos interfaces de red en el servidor, por lo cual se ocuparan en este caso dos tarjetas de red en las cuales se configuraran la red externa, la red interna y una interfaz virtual la cual es la encargada de asignar direcciones IP a los usuarios de la red, a continuación se detalla cada una de ellas:

Red Externa: La red externa es típicamente el Internet la cual dará acceso a la navegación. Esta es proporcionada por el servidor del servicio.

Red Interna: La red interna está conectada a los puntos de acceso con el servidor que contendrá el ChilliSpot, como por ejemplo el Switch, Access Point, etc. A estos puntos de conexión se les asignaran direcciones IP del rango 10.0.0.0 /24.

Red Virtual: ChilliSpot crea una interfaz virtual la cual asigna direcciones IP del rango 192.168.182.0/24 a los clientes que estén conectados a los puntos de acceso, en este caso son para la red alambrica e inalámbrica.

Red Inalámbrica: Los clientes inalámbricos están conectados con la red inalámbrica, y el Access Point sirve como puente entre la red interna y la red inalámbrica. Estos habilitan el direccionamiento entre la interfaz Ethernet y el servidor ChilliSpot, los clientes que tengan acceso a la red inalámbrica se les asignaran direcciones IP del rango 192.168.182.0 /24.

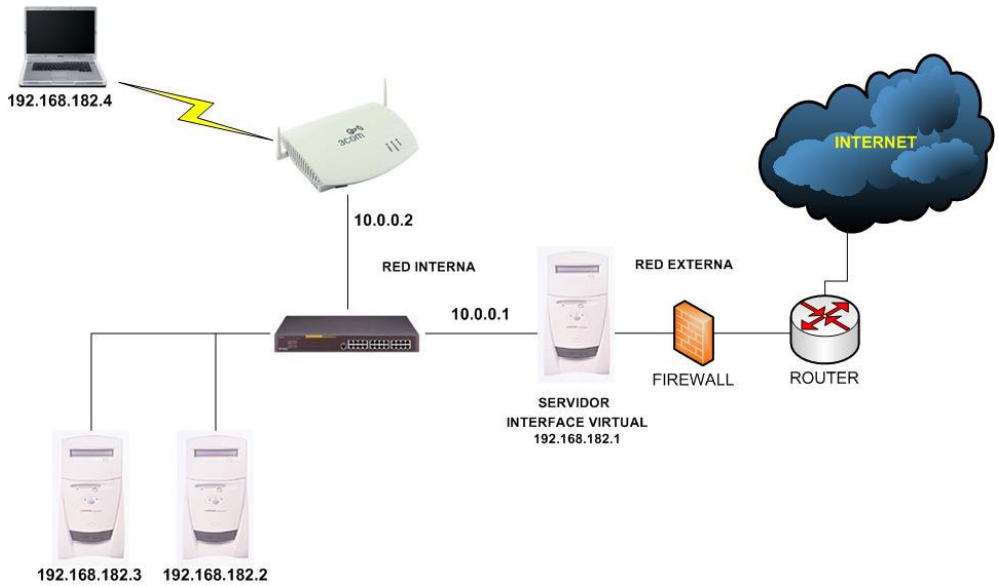


Figura 43 Esquema con interfaces de red

6.1.4. SEGURIDAD EN EL SERVIDOR

Para la seguridad en el servidor nos basaremos en lo siguiente:

6.1.4.1. CONFIGURACIONES BÁSICAS EN LA INSTALACIÓN

La instalación es parte fundamental de la seguridad en el servidor evitando gran parte de los problemas al momento de proteger un sistema operativo como linux, muchos administradores de redes hacen una instalación completa de linux dejando así muchos puertos abiertos y programas que no son utilizados, muchos de estos programas traen consigo vulnerabilidades que pueden ocacionar perdida total de la información por medio de ataques ya sea internos o externos.

Para la implementación del sistema operativo se realizara una instalación básica, esta tendrá únicamente el sistema base y la paqueteria necesaria para arrancar nuestro sistema, luego esta nos permitirá instalar unicamente aquellos programas o paquetes que sean necesarios para la implementación de los diferentes programas o servicios que utilicemos, estos paquetes serán a su vez los más actualizados permitiendolos así proteger nuestro sistema de ataques.

6.1.4.2. INSTALACIÓN DE SERVICIOS Y PUERTOS

Una vez instalado el sistema base se instalaran los siguientes servicios:

1. ChilliSpot.
2. FreeRadius.
3. Mysql-Server.
4. Apache.
5. Apache SSL.
6. Proxy Web Squid.
7. Samba.
8. FTP.

6.1.4.3. ESCANEO DE PUERTOS

Para el escaneo de puertos que se realizará se utilizara el comando nmap, nmap es un programa open source que sirve para efectuar escaneos de puertos. Está orientado a la identificación de puertos abiertos en una computadora objetivo, determinando que servicios está ejecutando la misma, e intenta determinar qué sistema operativo utiliza dicha computadora, (esta técnica es también conocida como fingerprinting). Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.Una vez instalado el sistema base nos conectaremos por medio de una herramienta la cual nos permita tener acceso a servidor, en nuestro caso ocuparemos un cliente de Secure Shell llamado "SSH Secure Shell Client".

El siguiente comando ejecutado desde la consola, determina cuáles puertos están escuchando por conexiones TCP desde la red: **nmap –sT –O localhost**

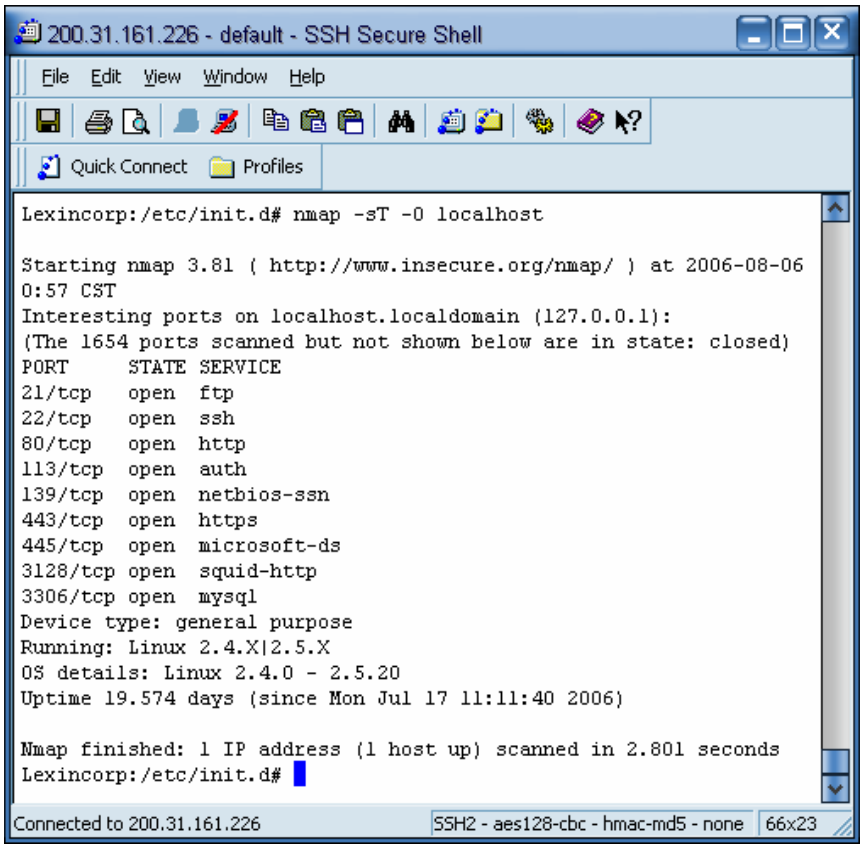


Figura 44 Muestra un ejemplo de escaneo de puertos

Esta salida muestra que en el sistema se está ejecutando los siguientes servicios:

1. Ftp, puerto 21. (Conocido)
2. SSH, puerto 22. (Conocido)
3. Apache, Puerto 80. (Conocido)
4. AUTH, Puerto 113. (Desconocido)
5. Netbios-ssn, Puerto 139. (Desconocido)
6. Apache-SSL, Puerto 443. (Conocido)
7. Microsoft-ds, Puerto 445. (Desconocido)
8. Squid-http, Puerto 3128. (Conocido)
9. Mysql, Puerto 3306. (Conocido)

Como se muestra en la salida del comando son varios los servicios que se están ejecutando en nuestro sistema, se han clasificado como conocidos y como desconocidos, nos enfocaremos en los desconocidos, para identificar estos servicios y saber si son realmente necesarios utilizaremos herramientas tales como, lsof y netstat.

6.1.4.4. IDENTIFICACION DE SERVICIOS

Para cada uno de los servicios desconocidos ejecutaremos el siguiente comando:

lsof –i | grep “puerto o nombre del comando”, o
netstat -anp | grep “puerto”

Se identificaron cada uno de los servicios los cuales mostraremos a continuación:

1. AUTH (ident, Identifica el usuario que origina una peticion hacia un servicio o socket), Puerto 113.
2. Netbios-ssn (Samba), Puerto 139.
3. Microsoft-ds (Samba), Puerto 445.

Se identificaron los servicios los cuales son necesarios para el sistema, no se quitaran y no se realizaran cambios.

6.1.4.5. PROTECCION DE SERVICIOS INSTALADOS (MURO DE FUEGO)

Para proteger los servicios que hemos instalado ocuparemos iptables, se crearan reglas las cuales nos permitiran bloquear o restringir el acceso a todas aquellas redes que nosotros nos queremos que tengan acceso.

Para esto se creará un script llamado S99rules el cual será colocado en la carpeta /etc/rc2.d con los permisos necesarios de lectura y escritura para que cada vez que arranque el sistema operativo se ejecute y carge así las reglas que se pondrán.

Los servicios que se protegerán son los siguientes: FTP, SSH, SAMBA, SQUID, MYSQL. Estos servicios se ocuparan por el momento solo por la red interna por lo cual se bloqueara el acceso a la red externa, así:

Script “S99rules”:

```
#Bloqueo a FTP
#Acceso a FTP por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 21 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 21 -j ACCEPT

#Bloqueo de FTP a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 21 -j DROP

#Bloqueo a SSH
#Acceso a SSH por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 22 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 22 -j ACCEPT
```

```
#Bloqueo de SSH a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 22 -j DROP
#Bloqueo a Samba
#Acceso a Samba por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 445 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 445 -j ACCEPT
#Bloqueo de Samba a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 445 -j DROP

#Bloqueo a SQUID
#Acceso a SQUID por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 3128 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 3128 -j ACCEPT

#Bloqueo de SQUID a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 3128 -j DROP

#Bloqueo a MYSQL
#Acceso a MYSQL por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 3306 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 3306 -j ACCEPT

#Bloqueo de MYSQL a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 3306 -j DROP
```

6.2. IMPLEMENTACIÓN DE RED INALAMBRICA

Para la implementación de la red inalámbrica se escogerán tres de las mejores marcas de equipos inalámbricos en el mercado, las marcas que se han elegido son:

1. 3Com.
2. D-Link.
3. LynkSys.

Para la adquisición del equipo nos basaremos en dos fases las cuales determinarán la compra del equipo, estas son:

1. Pruebas de Señal o Cobertura.
2. Conclusiones de las pruebas para la adquisición del Equipo.

El Access Point estará ubicado en la recepción de la segunda planta del edificio debido a que la mayoría de usuarios que tendrán acceso a la conectividad inalámbrica se encuentran ahí.

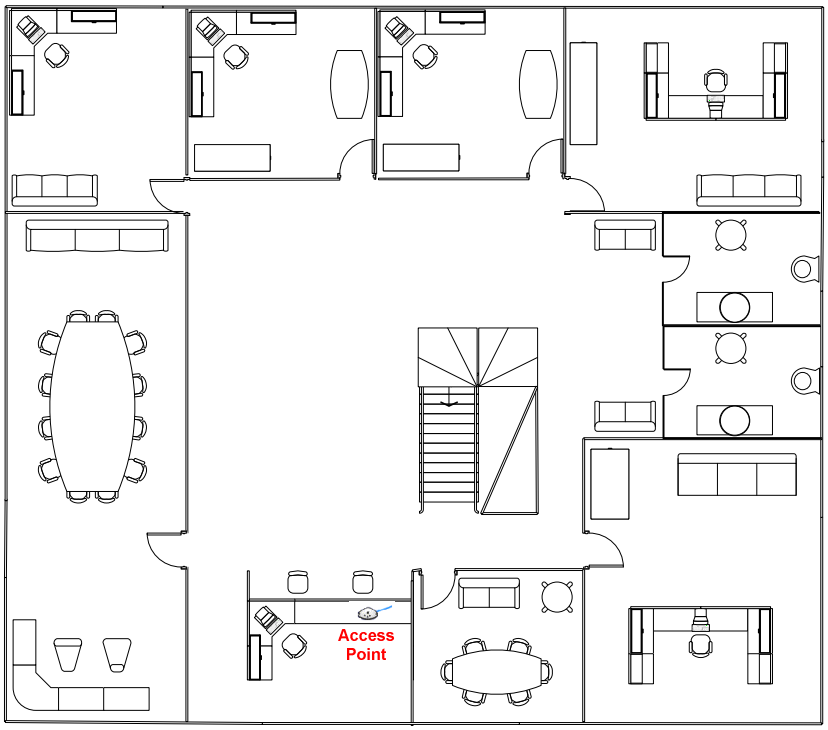


Figura 45 Ubicación de Access Point en la empresa

6.2.1. PRUEBAS DE SEÑAL Y COBERTURA

Las pruebas consistirán en 2 fases, cobertura y movilidad de usuarios.
Se realizaran las pruebas con las diferentes marcas de equipo inalámbrico siguiendo el orden siguiente:

1. D-Link
2. 3Com
3. LynkSys

Se clasificaron los niveles de señal en tres colores, estos se mostraran en cada una de las plantas según al Access Point que sea probado:

Verde: Señal alta
Amarillo: Señal baja
Rojo: No hay señal

EQUIPO INALÁMBRICO D-LINK

Modelo: D-LINK DWL-2000AP+

Descripción: Es Access Point Inalámbrico potenciado, perteneciente a la nueva línea AirPlus G+ de D-Link, que responde al estándar 802.11g, operando a 54Mbps de velocidad y gracias al nuevo Chip de Texas Instruments (tm), puede alcanzar en througput comparable a los 100Mbps en una red FastEthernet.
El modo de operación 8x exclusivo de D-Link le permite alcanzar una velocidad de operación ocho veces más rápida que una red Wireless tradicional de 11Mbps, con un througput real de 36Mbps aproximadamente.

Características:

- Velocidad de Transmisión de hasta 54Mbps, en 2.4GHz.
- Compatible con productos que operen bajo el estándar 802.11b y 802.11g, y la serie b+ de D-Link.

- Cuatro modos de operación. Access Point, Bridge PtP, Bridge PtMP y AP Cliente.
- Seguridad Avanzada, WPA y 802.1x.
- Antena desmontable con conector RSMA.
- DHCP Server.
- Fácil Instalación.
- Alto Rendimiento.
- Fácil integración en red.

6.2.1.1. DWL-2000AP+ PRUEBAS DE SEÑAL

Se coloco el Access Point en la recepción de la segunda planta y se realizaron pruebas. El rango de cobertura de este equipo es de 100 metros en interiores, el siguiente diagrama presentará los niveles de cobertura del D-LINK DWL-2000 AP +:

Primera Planta:

Figura 46 Cobertura del Access Point Dwl-2000 ap +

Como se observa en la figura la señal en la primera planta es muy mala, el rango de cobertura del Access Point se ve disminuido por paredes que dividen las diferentes áreas.

Segunda Planta:

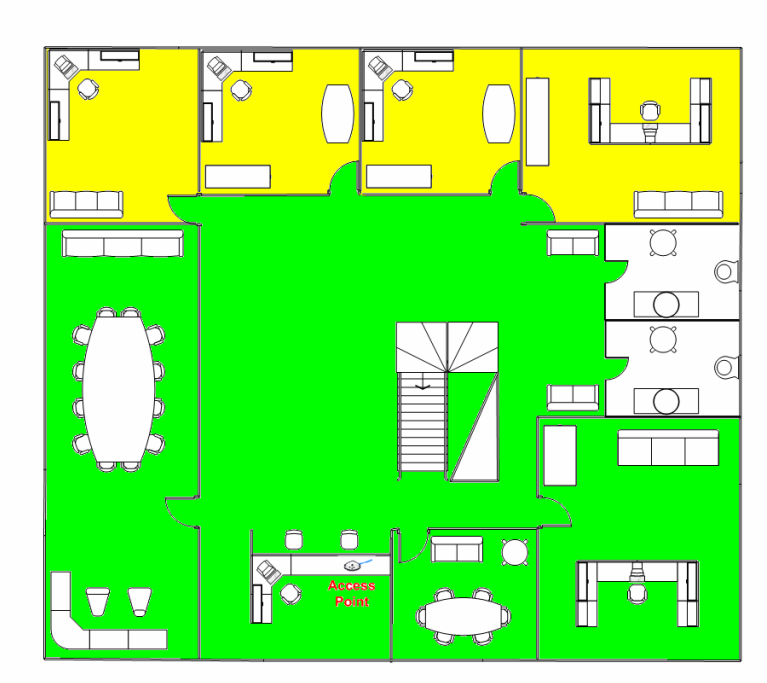


Figura 47 Cobertura del Access Point Dwl-2000 ap +

Como se observa en la figura en la segunda planta el rango de cobertura es un poco mejor pero no es el deseado, ya que existen muchos puntos donde la señal es baja.

EQUIPO INALÁMBRICO 3COM

MODELO: WIRELESS LAN ACCESS POINT 7250

Descripción: Soporta a hasta 253 usuarios simultáneos a velocidades de hasta 54 Mbps en un radio de hasta 100 metros. Selecciona el canal menos ocupado para unas conexiones sin problemas. Mantienen las conexiones de red constantemente disponibles al cambiar automáticamente la velocidad de las conexiones a medida que cambian las condiciones y que los usuarios móviles se desplazan por el área de cobertura de la red. Encriptación WEP de 40/64 y 128/154 bits; encriptación WPA AES de 256 bits; encriptación Dynamic Security Link de 128 bits; 802.11x con autenticación de servidor RADIUS; autenticación EAP-MD5, EAP-TLS, EAP-TTLS y PEAP; control de difusión ESSID; autenticación MAC local; listas de control de

acceso de servidor, administración de Clave de Sesión Dinámica y TKPI, asignación dinámica de VLAN, filtrado de cliente a cliente y de uplink.

Características:

- Soporta a hasta 253 usuarios simultáneos a velocidades de hasta 54 Mbps en un radio de hasta 100 metros.
- Clear Channel Select.
- Seguridad: Encriptación WEP, WPA AES de 256 bits, Dynamic Security Link de 128 bits; 802.11x con autenticación de servidor RADIUS.
- Autenticación EAP-MD5, EAP-TLS, EAP-TTLS, y PEAP.
- Control de difusión ESSID.
- Filtrado de cliente a cliente y de uplink.
- Dynamic Security Link asigna automáticamente claves específicas de encriptación de 128 bits para las sesiones inalámbricas.
- La autenticación basada en servidor RADIUS 802.11x controla el acceso a la red inalámbrica y centraliza la autorización de usuario para toda la red.
- La administración dinámica de clave de sesión y la asignación dinámica de claves TKIP mejoran la seguridad y simplifican el despliegue.
- Las listas de control de acceso de las direcciones MAC controlan el acceso a los recursos de red.
- El filtrado de cliente a cliente y de uplink bloquean las comunicaciones directas entre otros usuarios inalámbricos asociados a los puntos de acceso.
- La asignación dinámica de VLAN, usada con la autenticación RADIUS, asigna una VLAN apropiada a los usuarios, protegiendo aún más el acceso a los recursos de red.
- La antena de radio con diversidad ofrece un rendimiento y una cobertura excelentes en contextos con elevado multipath, como por ejemplo oficinas, almacenes y otras instalaciones de interior.
- Las opciones de antena externa amplían el alcance de las conexiones inalámbricas 802.11g a hasta 305 metros.

6.2.1.2. WIRELESS LAN ACCESS POINT 7250 PRUEBAS DE SEÑAL

Se coloco el Access Point en la recepción de la segunda planta y se realizaron pruebas. El rango de cobertura de este equipo es de 100 metros en interiores, el siguiente diagrama presentará los niveles de cobertura del LAN Access Point 7250:

Segunda Planta:

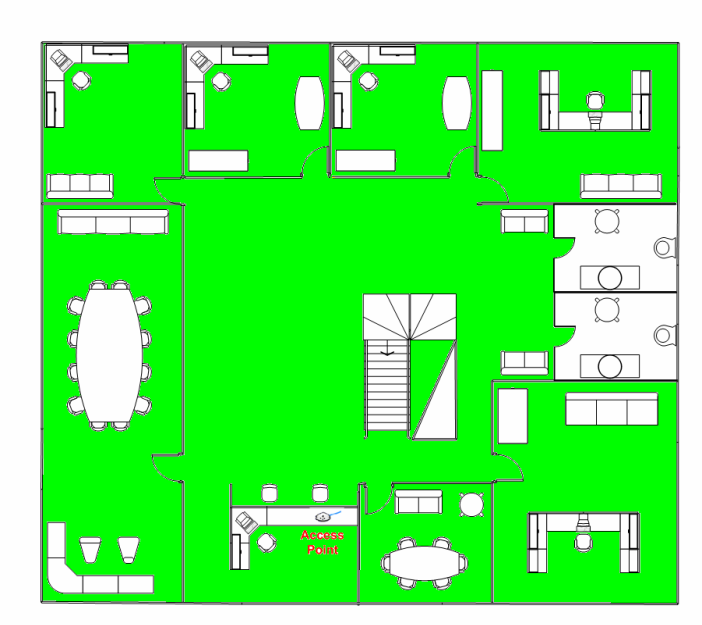


Figura 48 Cobertura Access Point 7250

Como se observa en la figura 32 en la segunda planta el rango de cobertura es total y en cada de los lugares la señal es alta.

Primera Planta:

Figura 49 Cobertura Access Point 7250

Como se observa en la figura en la primera planta el rango de cobertura es total y en cada de los lugares la señal es alta.

EQUIPO INALÁMBRICO LINKSYS

Modelo: Wireless-G Access Point WAP54G

Descripción: Wireless-G es el novedoso estándar de red inalámbrica de 54 Mbps que proporciona una velocidad casi 5 veces superior que los populares productos Wireless-B (802.11b) para el hogar, la oficina y establecimientos públicos con conexiones inalámbricas. Los dispositivos Wireless-G comparten una banda de radio común de 2,4 GHz, por lo que también funcionan con equipos Wireless-B de 11 Mbps existentes. El Access Point Wireless-G de Linksys permite conectar dispositivos Wireless-G o Wireless-B a la red. Ya que ambos estándares son incorporados, puede aprovechar la inversión realizada en infraestructura 802.11b y migrar los clientes de red al novedoso y velocísimo estándar Wireless-G a medida que aumentan sus necesidades.

Características:

- Configurar una red Wireless-G (802.11g) de alta velocidad en el hogar o la oficina.
- Velocidades de transferencia de datos de hasta 54 Mbps: 5 veces más rápido que Wireless-B (802.11b).
- También es compatible con redes Wireless-B (a 11 Mbps).
- Seguridad inalámbrica avanzada con encriptación WEP de 128 bits y filtro de MAC.

6.2.1.3. WIRELESS-G ACCESS POINT WAP54G PRUEBAS DE SEÑAL

Se coloco el Access Point en la recepción de la segunda planta y se realizaron pruebas. El rango de cobertura de este equipo es de 100 metros en interiores, el siguiente diagrama presentará los niveles de cobertura del LAN Wireless-G Access Point WAP54G:

Segunda Planta:

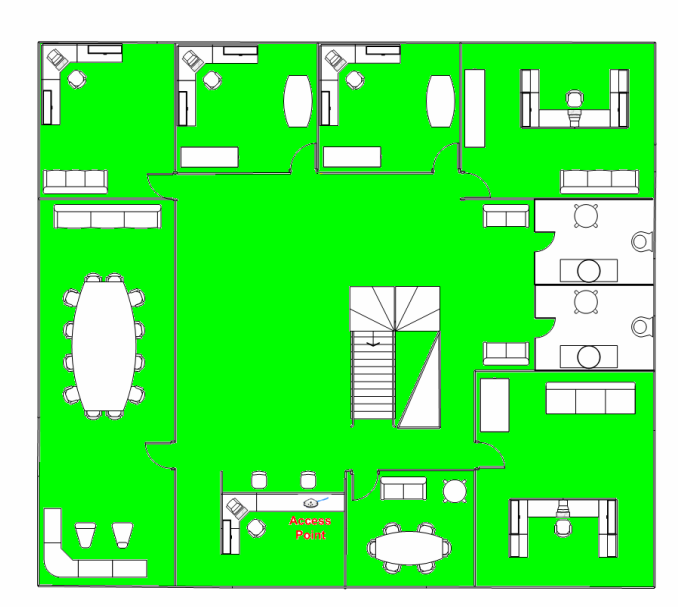


Figura 50 Cobertura Access Point WAP54G

Como se observa en la figura en la segunda planta el rango de cobertura es total y en cada de los lugares la señal es alta.

Primera Planta:

Figura 51 Cobertura Access Point WAP54G

Como se observa en la figura en la primera planta el rango de cobertura no es total y abarca un noventa y cinco por ciento del área total del la primera planta.

6.2.2. CONCLUSIONES DE LAS PRUEBAS

Después de haber realizado las pruebas con cada uno de los equipos inalámbricos el resultado es el siguiente:

			RANGO DE COBERTURA	
MARCA	MODELO	COBERTURA	PRIMERA PLANTA	SEGUNDA PLANTA
D-LINK	DWL-2000AP +	100 mt	Parcial	Parcial
3COM	Wireless Lan Access point 7250	100 mt	Total	Total
LYNKSYS	Wireless-G Access Point WAP54G	100 mt	Parcial	Total

Cuadro 6 Comparación de las coberturas de los Access Point

El Access Point de 3Com tiene una cobertura total en el edificio por tal motivo se recomienda adquirirlo.

Caracteristicas	D-LINK DWL-2000AP+	3COM ACCESS POINT7250	LINKSYS Access Point WAP54G
Seguridad WPA	SI	SI	NO
802.1x.	SI	SI	NO
WEP	SI	SI	SI
Velocidad 54Mbps	SI	SI	SI
Estándar 802.11g	SI	SI	SI

Cuadro 7 comparativo de especificaciones de los access point.

6.2.3. SEGURIDAD EN EL ACCESS POINT

A parte de las medidas que se hayan tomado en el diseño de la red inalámbrica, debemos aplicar ciertas normas y políticas de seguridad que nos ayudarían a mantener una red más segura:

- Utilizar WEP, aunque sea rompible con herramientas como AirSnort o WebCrack, como mínimo de seguridad.
- Inhabilitar el DHCP del Access Point. Las IPs serán distribuidas por el Chilli Spot.
- Actualizar el firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones wireless.
- Proporcionar un entorno físicamente seguro a los puntos de acceso y desctivarlos cuando se pretenda un periodo de inactividad largo (ej. Ausencia por vacaciones).
- Cambiar el SSID (Server Set ID) por defecto del Access Point, conocidos por todos. El SSID es una identificación configurable que permite la comunicación de los clientes entre la estración cliente con un determinado Access Point. Actúa como un password compartido entra la estación cliente y el punto de accesso. Ejemplos de SSID por defecto son “tsumani” para Cisco, “101 o default” para 3com, “default” para D-link, etc.
- Inhabilitar la emisión broadcast del SSID.
- Reducir la propagación de las ondas de radio fuera del edicio.
- Utilizar firewalls y monitorizar los accesos a los puntos de acceso.

6.2.4. DIAGRAMAS DE RADIACIÓN DEL ACCESS POINT 3COM 7250

Las antenas del Access Point que hemos elegido se comportan como antenas omnidireccionales. Una antena omnidireccional recive las señales de todas direcciones, lo que significa que cubren 360 º alrededor de la antena. Estas antenas son recomendables para oficinas, facilidades públicas donde el grupo de trabajo requiere trabajar eficientemente y eficazmente.

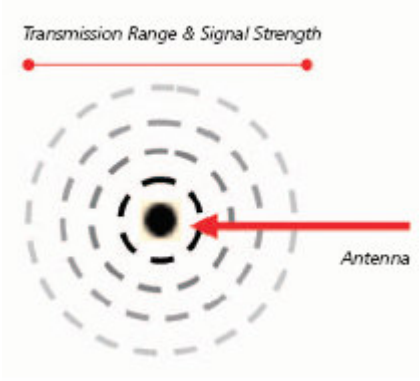


Figura 52 Forma de onda de antena omnidireccional

Los diagramas de radiación de las antenas son frecuentemente usados para desplegar las características y capacidades de una antena particular. Un parámetro de radiación indica como las ondas electromagneticas se propagan hacia fuera de la antena. El parámetro de radiación depende de la polarización entre la antena transmisora y la antena receptora. La polarización de las antenas pueden ser horizontales, verticales o circulares, sabiendo cual de esa es la correcta y como aplicarla a tu medio es lo más importante para el desempeño óptimo de la antena.

Antenas verticalmente polarizadas tienen sus campos electricos perperndiculares a la superficie de la tierra, mientras que las antenas horizontalmente polarizadas tienen sus campos electricos paralelos a la superficie de la tierra. Una antena que esta circularmente polarizada radia tanto en horizontal como en vertical y cualquier parte entre ellos.

En la figura se puede apreciar las cuatro formas de configurar una antena para transmitir o recibir, conocido como acoplamiento cruzado. Para muchas aplicaciones, el sistema de la antena debe de usar escenario 1. La mejor señal ocurre cuando los dos dispositivos usan el mismo método de polarización.

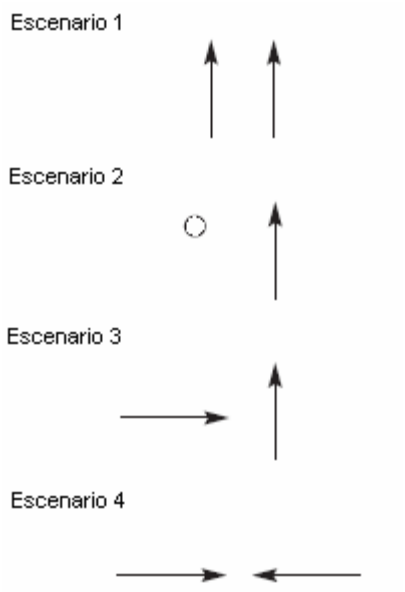


Figura 53Las cuatro formas de configurar una antena

Un diagrama de radiación tipico para una antena omnidireccional es la que se muestra en la figura. La linea circundante del esquema muestra la intensidad de la señal relativa hacia la localización radial en una area de 360 º.

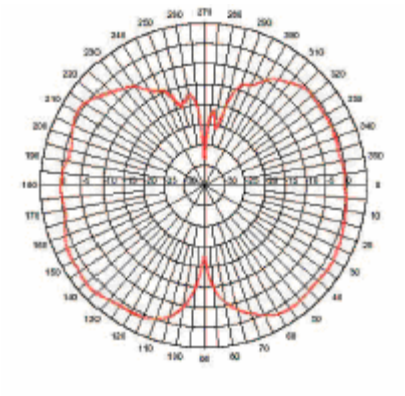


Figura 54Diagrama de radiación de una antena omnidireccional

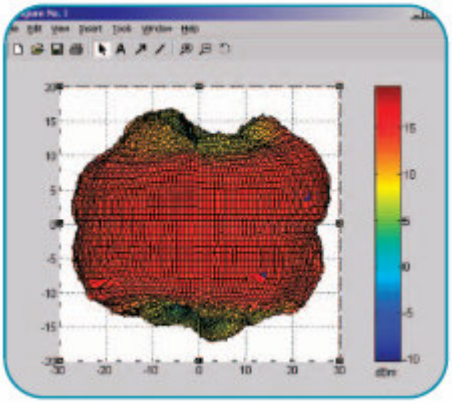


Figura 55 muestra una vista detallada en tres dimensiones de una antena omnidireccional con intesidad de señal relativa en relación a la antena de en medio.

Al elegir la antena apropiada para su aplicación de red inalámbrica, se debe de entender los parámetros de rendimiento de la antena. En muchos parámetros se observarán los lóbulos, estos identifican donde la area más intensa de la señal es relativa a la antena. Los nulos identifican donde la señal es débil.

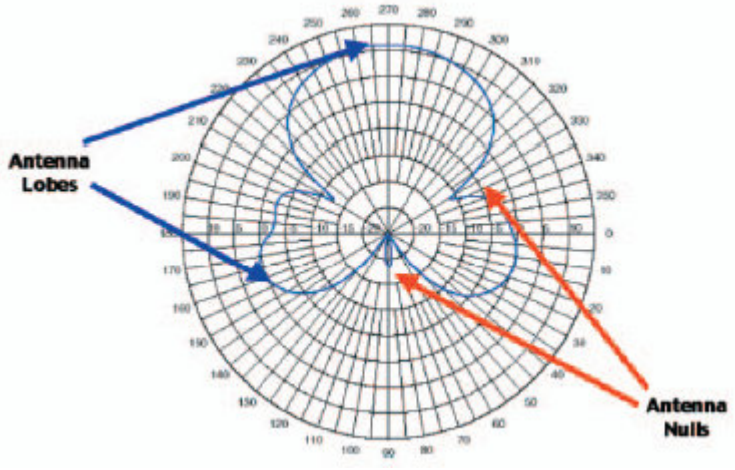


Figura 56 muestra un diagrama de radiación con sus lóbulos y nulos.

El Access Point 3com 7250 que hemos elegido viene con dos antenas separadas por una corta distancia. Estas antenas son conocidas como *diversity antenna*, son diseñadas para cubrir el mismo espacio geográfico, para mejorar el rendimiento al recibir la mejor señal en una región determinada. En el 802.11b o 802.11g, la distancia que separa a las antenas es aproximadamente de 3 cm, un cuarto de la longitud de onda de 2.4 Ghz.

Figura 57 Ejemplos de Access Point 3COM

6.2.5. DIAGRAMAS DE RADIACIÓN DE ANTENAS ADICIONALES DEL ACCESS POINT 3COM 7250

Si se desea tener un mejor alcance de la señal del Access Point, se recomienda el uso de una antena adicional para mejorar el rendimiento de la señal hacia otro edificio.

Las antenas que se pueden escoger son 5, se detallan a continuación:

ANTENA DE BANDA DUAL OMNI 3COM 6/8 DBI (3CWE591)

Figura 58 Antena de banda dual 3COM 6/8

Esta antena provee cobertura uniforme hacia todas direcciones, diseñada para la variedad de estandares 802.11 para ambientes no tan flexibles. La antena funciona bien para conexiones inalámbricas estaticas y de edificio a edificio.

Proporciona conexiones de punto a multipunto con Access Point 3com en modo bridge de edificio a edificio.

Especificaciones generales:

- Polarización: Vertical
- Impedancia nominal: 50 Ohms
- Banda VSWR: 100 MHz
- 2.4 GHz ancho de la emisión vertical (50% de poder): 30 degrees
- 5 GHz ancho de la emisión vertical(50% power): 20 degrees
- 125 mph
- Conector: N Hembra
- Método de montado: paredl o en el cielo, techo
- Ganancia: 2.4 GHz: 6 dBi; 5 GHz: 8 dBi

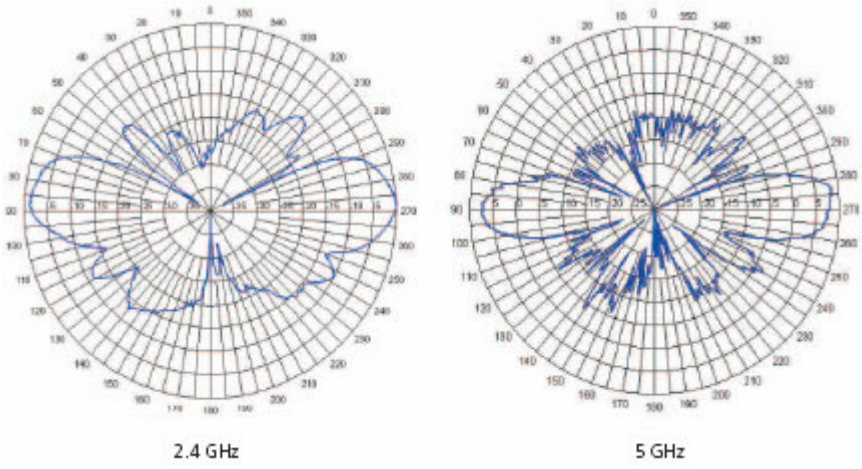


Figura 59 Diagramas de radiación de la Antena de banda dual 3COM 6/8

ANTENA DE BANDA DUAL OMNI 3COM 3/4 DBI PARA MONTAR EN EL TECHO (3CWE592)

Figura 60 Antena de banda dual ovni 3com 3/4

Esta antena ofrece una cobertura uniforme en todas las direcciones en areas abiertas como lobbies o salas de conferencias

Especificaciones generales:

- Polarización: Vertical, linear
- Impedancia nominal: 50 Ohms
- Conector: N Hembra
- Cable: 12-pulgadas (30.5 cm) Plenum RG58/U
- Ganancia: 2.4 GHz: 3 dBi; 5 GHz: 4 dBi

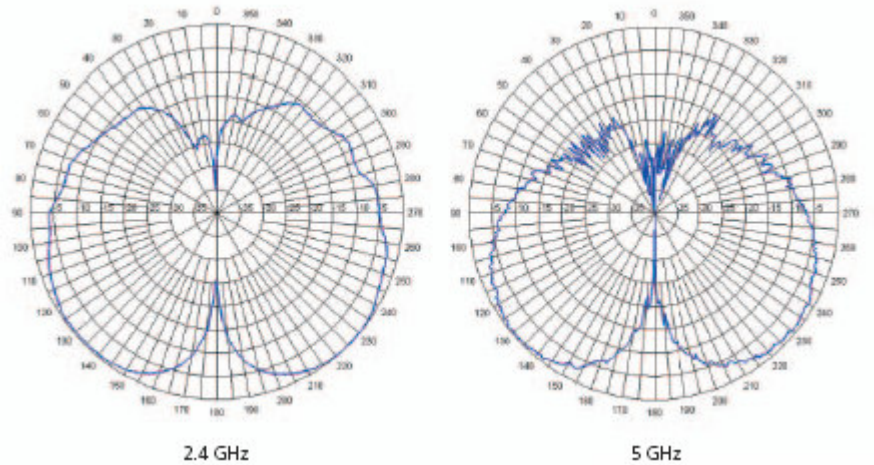


Figura 61Diagrama de radiación de la Antena de banda dual ovni 3com 3/4

ANTENA DE BANDA DUAL HALLWAY 3COM 4/6 DBI (3CWE597)

Figura 62 Antena de banda dual hallway 3com 4/6

Esta antena diminuta es perfecta para alcanzar tu red inalámbrica en espacios estrechos y pasillos. Es ideal para largos corredores donde radiación intensa es necesaria para alcanzar una buena señal.

Especificaciones generales:

- Polarización: Vertical
- Impedancia nominal: 50 Ohms
- 2.4 GHz ancho de emisión vertical: 100 grados
- 5 GHz ancho de emisión vertical: 75 grados
- Conector: N Hembra
- Cable: 12-pulgadas (30.5 cm) Plenum RG58/U
- Método de montaje: Pared o techo
- Ganancia: 2.4 GHz: 4 dBi; 5 GHz: 6 dBi

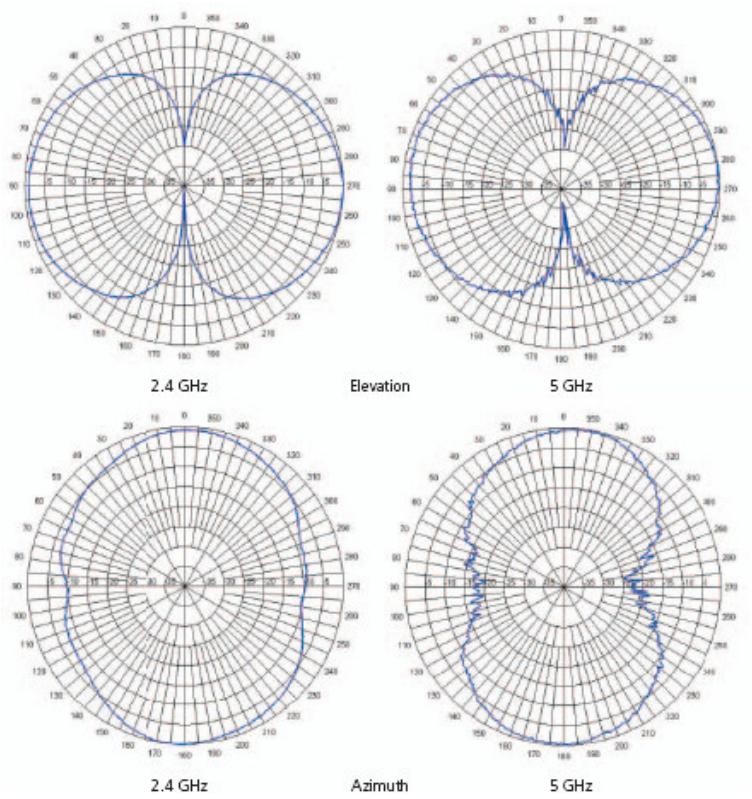


Figura 63Diagramas de radiación Antena de banda dual hallway 3com 4/6

ANTENA DE BADA DUAL PANEL 3COM 18/20 DBI (3CWE596)

Figura 64 Antena de banda dual panel 3com 18/20

Esta antena permite enlaces de largo alcance para interiores. La antena puede ser montado donde sea en cualquier orientación proporcionando cobertura directa tanto en exteriores como en interiores. Es ideal para conexiones punto a punto las cuales requieren cables largos para correr entre la antena y el puente.

Especificaciones generales:

- Polarización: Lineal, vertical u horizontal
- Impedancia nominal: 50 Ohms
- 3dB ancho de emisión horizontal: 18 degrees
- 3dB ancho de emisión vertical: 19 degrees
    - 25 dB
- Conector: N Hembra
- Cable: 12-pulgadas (30.5 cm) Plenum RG58/U
- Método de montaje: exterior e interior
- Ganancia: 2.4 GHz: 18 dBi; 5 GHz: 20 dBi

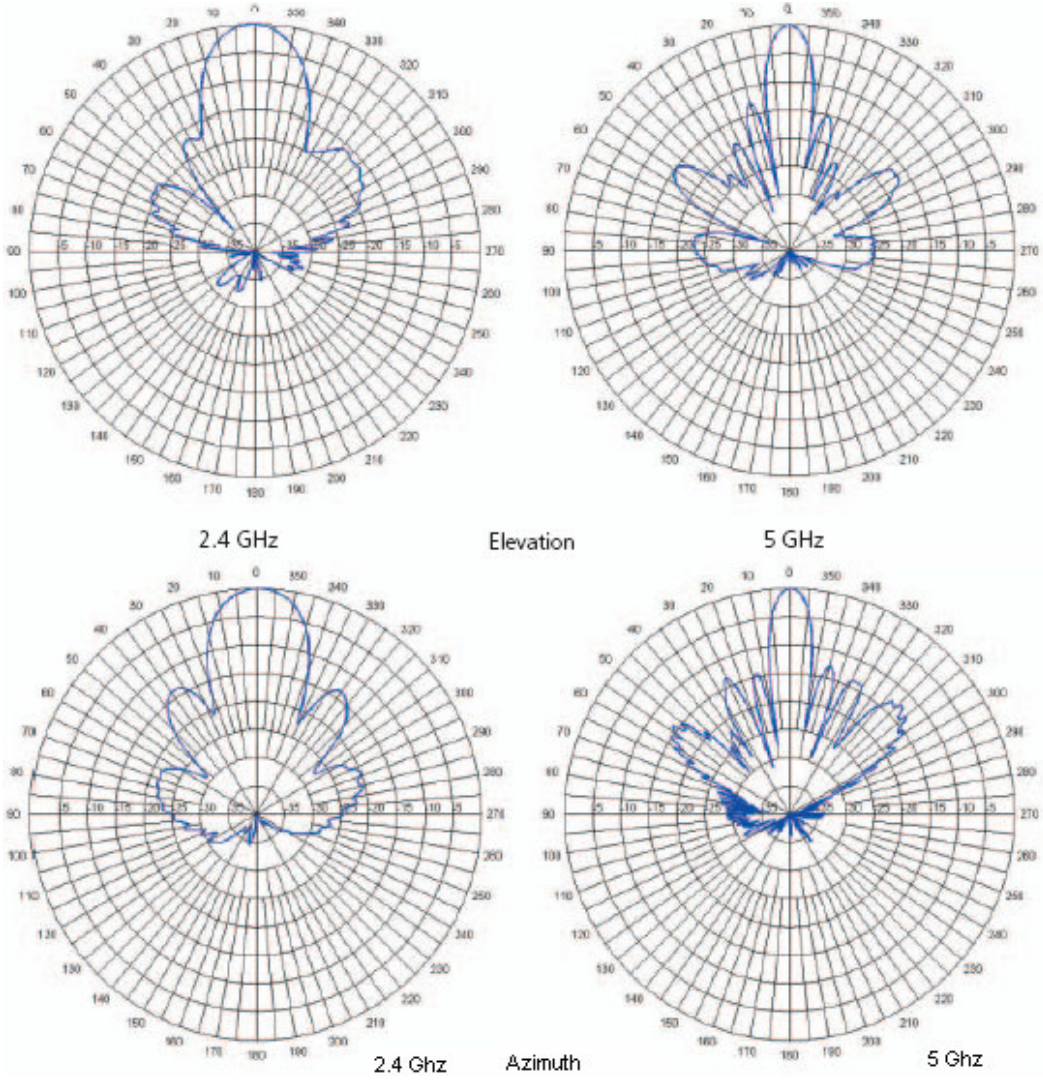


Figura65 Diagramas de radiación de Antena de banda dual panel 3com 18/20

ANTENA DE BANDA DUAL PANEL 3COM 8/10 DBI (3CWE598)

Figura 66 Antena de banda dual panel 3com 8/10

Esta antenna permite enlaces de corto alcance para interiores. Es versátil puede ser montada donde sea y en cualquier dirección proporcionando cobertura directa en ambos ambientes exteriores e interiores. Es ideal para conexiones de punto a punto o para partir la cobertura de un Access Point en un área especifica.

Especificaciones generales:

- Polarización: Lineal, vertical u horizontal
- Impedancia nominal: 50 Ohms
- 3dB ancho de emisión horizontal: 60 degrees
- 3dB ancho de emisión vertical: 60 degrees
    - 15 dB
- Conector: N Hembra
- Cable: 12-pulgadas (30.5 cm) Plenum RG58/U
- Método de montaje: externo e interno
- Ganancia: 2.4 GHz: 8 dBi; 5 GHz: 10 dBi

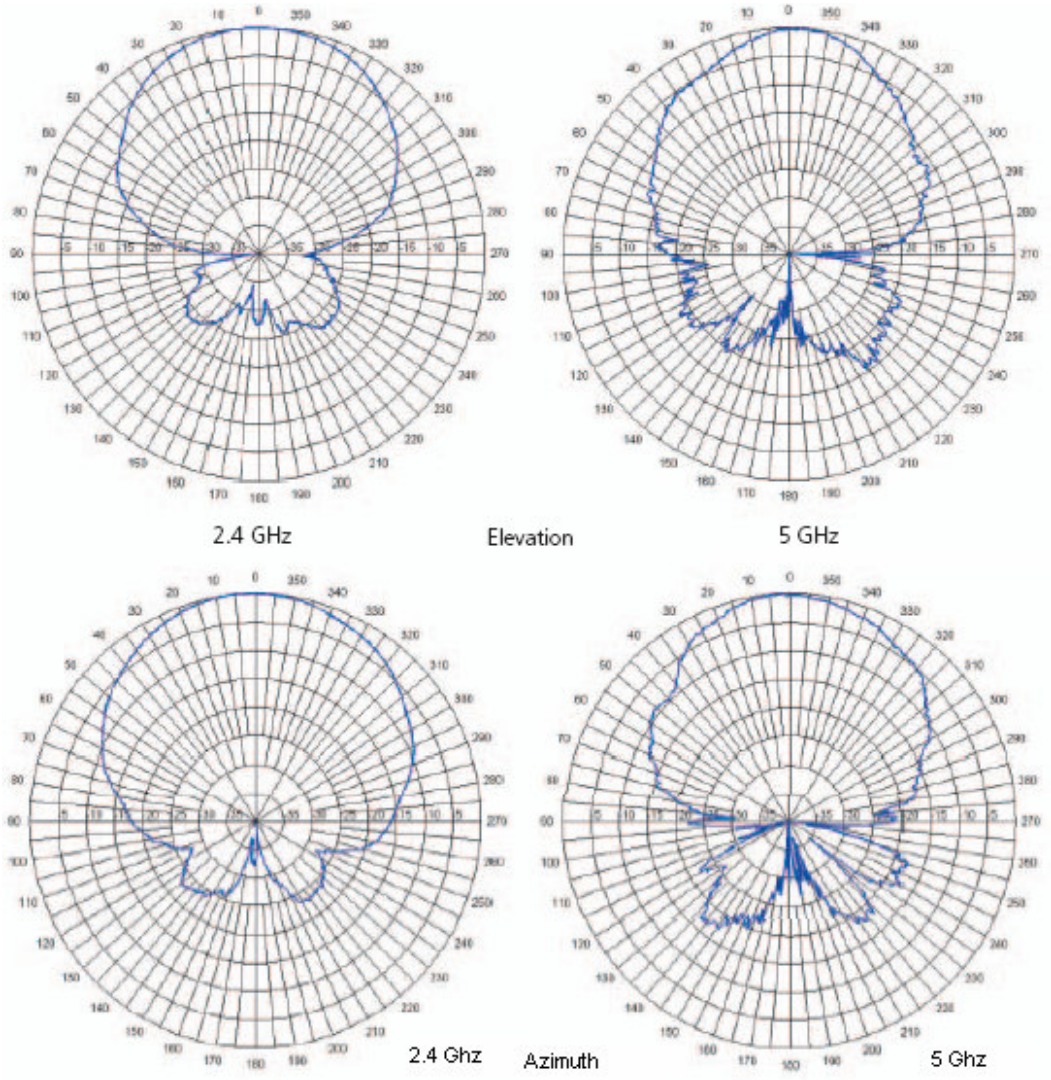


Figura 67 Diagramas de radiación de la Antena de banda dual panel 3com 8/10

6.3. IMPLEMENTACIÓN DE LA INTRANET

Antes de comenzar con la implementación de la Intranet conoceremos un concepto de esta, una Intranet es una red de computadoras de una red de área local (LAN) privada empresarial o educativa que proporciona herramientas de Internet, las cuales tienen como función principal proveer lógica de negocios para aplicaciones de captura, reportes, consultas, etc. con el fin de auxiliar la producción de dichos grupos de trabajo; es también un importante medio de difusión de información interna a nivel de grupo de trabajo. No necesariamente proporciona Internet a la organización; normalmente, tiene como base el protocolo TCP/IP de Internet y, por ser privada, puede emplear mecanismos de restricción de acceso a nivel de programación como lo son usuarios y contraseñas de acceso o incluso a nivel de hardware como un sistema firewall (muro de fuegos) que pueda restringir el acceso a la red organizacional.

Para la implementación de la Intranet que se realizara sea han elegido tres software de código abierto, los cuales nos permitirán hacer pruebas sin ningún costo, el software que se han elegido para la implementación son los siguientes:

1. Group-Office.
2. Simple-Groupware.
3. XenIntranet.

Para la implementación y funcionamiento del software nos basaremos en tres poderosas razones que justifican el esfuerzo:

1. Para ahorrar tiempo en los procesos.
2. Mejorar el clima organizacional.
3. Para reducir costos.

6.3.1. AHORRAR TIEMPO

La empresa Lexincorp es una organización que trabaja con información en forma conjunta, comunicándose entre si utilizando el teléfono, el fax, el correo electrónico, enviando y recibiendo papel y en reuniones persona a persona.

Una Intranet puede reducir el tiempo que los colaboradores de la empresa utilizan para tareas de procesamiento de información y comunicación rutinaria. En la mayoría de los casos utilizan el correo electrónico rutinariamente, ya se conocen las ventajas de este medio sobre el teléfono por ejemplo. El problema con el correo electrónico es que no toda la información es entregada en la primera comunicación, siendo entonces necesaria una cadena de correos para lograr que la contraparte entienda completamente de que se trata el tema.

Como se puede medir el ahorro que se tendría, se responderán a las siguientes preguntas:

¿Cuanto tiempo pierden sus colaboradores, o los jefes, contestando rutinariamente las mismas preguntas?

Se colocara información en la Intranet y se ahorrara tiempo el cual se convertirá en resultados

¿Parte del trabajo de sus colaboradores consiste el tramitar documentos elaborados dentro de la empresa misma?

Se publicaran para que los encuentren en la Intranet.

¿Su organización depende de procesos y procedimientos claramente establecidos que son necesarios tener a la mano?

Se publicaran para que los usuarios los encuentren en la Intranet. Ahorrándoles tiempo para que se dediquen a labores que producen valor agregado y dinero

6.3.2. MEJORAR EL CLIMA ORGANIZACIONAL

Muchas de las empresas hoy en día no tiene un medio oficial de distribución de su información, por lo cual muchos de sus departamentos o empleados no la comparten, quedando información valiosa oculta y sin el conocimiento de los demás que podrían hacer uso de esta, un ejemplo sería toda aquellas estadísticas que generan los departamentos de informática accesos a portales o servicios que puede ser útil para los departamentos de mercadeo o ventas, esta información puede ser usada para saber que tanto acceso han tenido a determinado servicio.

¿Su empresa es un conjunto de islas dispersas aunque compartan un solo edificio?

Publique temas de interés personal que ayude a la integración de las personas y mejore el ambiente de trabajo

6.3.3. REDUCIR COSTOS

Con una solución basada en la Intranet se puede compartir información, publicar toda clase de documentos además del directorio como por ejemplo el boletín mensual, la información de carteleras, noticias, etc.

Esto en gran medida ayudará a la empresa en el ahorro de tiempo y generara productividad, para la implementación se ha pensado además en software de código abierto el cual no tiene ningún costo, el cual además puede ser escalable según los requerimientos de la empresa.

6.3.4. REQUISITOS PARA LA IMPLEMENTACION DE LA INTRANET

A la hora de construir cualquier red de computadoras, y, en especial, una Intranet, necesitaremos unos elementos básicos:

En primer lugar, es necesario disponer de un hardware o soporte físico adecuado para la Intranet, que incluye:

- Servidores de Web, bajo el modelo Cliente-Servidor.

- PC de los empleados, que actúan como Clientes, y sus correspondientes periféricos.
- Un sistema de cableado que conecte el Servidor con los equipos Cliente (En nuestro caso la red alambrica por cable UPT y red inalámbrica por medio de Access Point)
- Elementos de hardware que configuran el concepto tradicional de red: tarjetas de conexión o NIC (Network Interface Card), o Switch, etc.
- Máquinas que actúan como firewalls, y su correspondiente software, se utilizara el servidor Linux como firewall.

En segundo lugar, necesitaremos una serie de elementos de software que hagan posible configurar la red como una Intranet. Destacan:

- Un sistema operativo de red, que soporta el intercambio de información y, que, como tal, reside tanto en clientes como en servidores. Hoy en día, existen varios sistemas operativos disponibles en el mercado: Unix, Linux, Windows NT, Novell Netware, y otros. Se utilizara LINUX como sistema Operativo.
- Aplicaciones de red, que en este caso, se refieren a la utilización de navegadores de Internet, residentes en los equipos clientes, así como de programas específicos de correo electrónico, FTP, etc.
- Un sistema de gestión de red, que permite el control de prestaciones, problemas, seguridad o configuración.
- Protocolos de comunicación Web estándares.

6.3.5. CUESTIONARIO INTRANET

Responder el siguiente cuestionario nos permitirá aclarar ciertos puntos y conocer más de cerca las necesidades de la empresa. En consecuencia, estaremos en capacidad de optar por una solución que se adapte a la realidad de la empresa.

6.3.5.1. ESTRUCTURA ORGANIZACIONAL

Es necesario comprender como funciona la empresa, ya que un buen entendimiento de la estructura de ésta ayuda a determinar la utilidad de la Intranet en

general. Del mismo modo, es importante definir que funciones específicas pueden generar valores agregados.

¿Tiene la empresa oficinas en diferentes sitios?

No, si bien es cierto que la empresa esta ubicada en toda Centro América en El Salvador excité únicamente una.

¿Existen personas del mismo departamento en diferentes oficinas?

No, todos los empleados están en sus respectivas oficinas con sus respectivos departamentos.

¿Es una organización jerárquica, Centralizada o Descentralizada?

Somos una organización centratilizada.

6.3.5.2. INTERCAMBIO DE INFORMACIÓN A NIVEL INTERNO

Entender y visualizar como la organización intercambia información internamente ayuda a identificar los obstáculos que una Intranet puede ayudar a superar.

¿Cuales son los principales recursos de información a nivel interno y externo?

Los principales medios o recursos de información actualmente son el correo electrónico,

¿Cómo se reparte usualmente la información (teléfono, memorandos, reuniones, e-mail, otras formas)

La información se reparte de forma manual, medios de almacenamientos como disquetes o cds o por correo electrónico.

¿Cómo se toman usualmente las decisiones? (Por Jerarquía, Consenso, otra forma).

Por medio de la junta directiva, estos se reúnen una vez a la semana para tomar decisiones en la empresa.

¿Cómo se realizan y dan a conocer los proyectos, decisiones, e investigaciones?

Se comunica al personal por memos y por correos electrónicos de la actividades a realizar que la junta a decidido.

6.3.5.3. INTERCAMBIO DE INFORMACIÓN A NIVEL EXTERNO

Conocer como interactúa la empresa con factores externos (proveedores, clientes, asociados) facilita el proceso de adaptación a sus necesidades.

¿Cuales son las personas y/o entidades con las cuales la empresa se comunica con frecuencia?

Se relacionan con juzgados, con el centro nacional de registro, diarios oficiales, bancos, clientes internacionales o bufetes de la región centro americana.

¿Cómo se comunica normalmente la empresa con estas personas y/o organizaciones?

Por correo electrónico, por teléfono y contacto personal.

¿Que información se necesita, Quiere, Espera y que Requiere?

La información que se necesita y se requiere es únicamente de trabajo.

¿Cómo recibe y procesa la información que se recibe de ellos?

Por correo electrónico.

6.3.5.4. BARRERAS EN EL INTERCAMBIO DE INFORMACIÓN

La identificación objetiva de las principales barreras que impiden una comunicación eficiente ayuda a definir las prioridades en el desarrollo de la Intranet.

¿Cuáles son los principales obstáculos para el intercambio efectivo de información?

El mal uso de las herramientas que actualmente poseen un ejemplo es el correo electrónico muchas veces no es efectivo para el intercambio de información, por que muchas veces este es usado para otros fines y no para trabajo generando así una saturación de los servidores de correos.

¿Son estos obstáculos Técnicos? Logísticos? Culturales?

Son técnico-culturales, técnicamente son porque no existen las políticas necesarias para restringir el uso de los servicios que les son brindados, culturales por que no hay una concientisación del uso de los recursos que poseen y para que se usan cada uno de ellos.

¿Cuál es el impacto de estos obstáculos?

Perdida de tiempo ya que no se puede tener una comunicación fluida con los empleados o clientes en la empresa, la cual genera una crisis ya que muchas veces no se cumplen con los tiempos esperados.

6.3.5.5. RECURSOS DISPONIBLES

La evaluación de recursos disponibles ayuda a establecer un punto de partida realista para un proyecto Intranet.

¿Cuál es el nivel actual de sistematización de la empresa?

No hay sistematización todo se hace manual.

¿Que recursos internos se necesitan para implementar y administrar la Intranet?

Los recursos internos son, contar con el hardware y software necesario para la Intranet, lo cual se ha descrito en el capitulo VI, y con la persona necesaria para administrar la Intranet.

¿Qué recursos financieros, técnicos y demás están disponibles en este momento?

Con lo que cuenta la empresa es una infraestructura de red básica, con veintidós computadoras para usuarios, financieramente no habrá costo en la implementación de la Intranet ya que se usara software de código abierto.

6.3.5.6. DEFINICIÓN DE OBJETIVOS GENERALES

El objetivo general al que se quiere llegar es a que la información este centralizada y que sea de fácil acceso a los empleados de la empresa, esto con las medidas de seguridad necesarias para que la información que transitará en ella esta protegida de ataques ya sean internos o externos.

Sin importar que tipo de metas se tenga, es necesario definirlas y tenerlas muy claras antes de iniciar el proyecto. En particular es importante tener en cuenta los siguientes puntos:

¿Qué queremos lograr?

Nos ayuda a entender el objetivo general del proyecto, de esta forma podremos definir prioridades y enfocarnos en los aspectos importantes de la Intranet.

¿Por qué queremos lograrlo?

Esta pregunta nos fuerza a considerar la Intranet en el contexto general de nuestra estrategia y que queremos lograr con ella. Esta respuesta es clave para asegurar que la productivaza en la empresa sea la proyectada.

¿Cómo vamos a monitorear el progreso?

Las Intranets tienden a evolucionar con el tiempo. Por esta razón es importante contar con mecanismos que nos permitan determinar el progreso del proyecto y compararlo con las expectativas.

¿Cómo vamos a medir el éxito del proyecto?

Como en muchos otros casos, el éxito de este tipo de proyecto se mide por medio de la relación costo beneficio de la inversión.

6.3.5.7. DEFINICIÓN DE OBJETIVOS PUNTUALES

A un nivel más especifico, la empresa que va a desarrollar la Intranet debe definir los siguientes puntos:

¿A quién está dirigida la Intranet?

La Intranet estará dirigida a todos los empleados y socios de la empresa, los cuales harán uso de esta para realizar sus actividades de una manera más eficiente. Lo importante es tener muy claro que se espera de cada grupo de usuarios de la Intranet y cuales son los beneficios mutuos por su implementación y uso.

¿Cómo esperamos que los usuarios utilicen la Intranet?

La interacción de los usuarios con una Intranet varia permanentemente, dependiendo de las funciones de cada grupo de usuarios. Para cada grupo se debe definir los usos específicos, y los beneficios asociados, para que el diseño de la Intranet se adapte a las necesidades y expectativas de todos sus usuarios.

¿Qué necesitan los usuarios potenciales para utilizar la Intranet?

Los servicios necesarios para poder realizar tareas diarias específicas y poder compartir información valiosa con los demás departamentos.

6.3.5.8. INFRAESTRUCTURA EN SISTEMAS DE LA ORGANIZACIÓN

Ahora es necesario analizar la infraestructura actual de la organización. Teniendo en cuenta los criterios ya establecidos.

¿Quién es responsable del contenido?

La actualización de la información será responsabilidad del departamento de sistemas de la empresa o encargado de los sistemas de cómputo. El contenido de la información será responsabilidad de cada área.

¿Qué tan escalable es su servidor?

El servidor que actualmente se posee la empresa es básico pero escalable ya que se le puede incrementar memoria, discos, etc, para que cuando el proyecto de Intranet se extienda el servidor pueda soportar este crecimiento.

Adicionalmente deberíamos tener en cuenta los siguientes puntos:

¿Cuenta su empresa con cableado estructurado?

Si, la empresa cuenta con cableado estructurado.

¿De ser así, que tipo de cableado utilizan?

Actualmente se utiliza cableado UTP categoría cinco y la topologia es en forma de estrella.

¿Cuantos puntos de red tiene su empresa?

De 1 a 15	16 a 30	**31 a 50**	50 a 100	Mas de 100 puntos

Cuadro 8 Puntos de red que posee la empresa

¿Que tipo de servidor(es) utiliza su organización (todos los que apliquen)?

Actualmente se cuenta con un servidor con Windows 98 el cual sirve como Proxy, con la implementación se instalara un sevidor Linux el cual dará todos los servicios de la Intranet.

¿Que tipo de estaciones de trabajo utilizan sus trabajadores. Para cada sistema operativo cuente cuantos que tipo de equipos (386, 486 o Pentium) utiliza y el total de equipos corriendo cada sistema operativo?

CUADRO DE ESPECIFICACIONES TÉCNICAS							
Ubicación	USUARIO	RAM	Sistema Operativo	Red		MARCA	MODELO
				Alambrica	Inalámbrica		
Notariado	Cristina Urbano	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
	Carmen Morales	128 DDR	Windows Xp	Si	No	Clon	U8668-D
	Tathiana Villalta	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
	Ernesto Sanchez	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
	Lic Duarte	256 DDR	Windows Xp	Si	No	Clon	U8668-D
Cubículo	Pamela	256 DDR	Windows Xp	Si	No	Clon	U8668-D
	Francisco Barahona	384 DDR	Windows Xp	Si	No	Compaq	Presario 4400 LA
	Mónica Muñoz	256 DDR	Windows Xp	Si	No	Clon	U8668-D
	Karla Guzmán	256 DDR	Windows Xp	Si	No	Clon	U8668-D
	Cristobal	256 SDR	Windows Xp	Si	No	Dell	GX60
	Karen Carazo	512 DDR	Windows Xp	Si	No	Clon	P4M80-M4
	Karla Avilés	512 DDR	Windows Xp	Si	No	Clon	P4M80-M4
Contabilidad	Margarita Monterrosa	256 SDR	Windows Xp	Si	No	Dell	GX60
	Alexander Cubías	256 DDR	Windows Xp	Si	No	Clon	U8668-D
Recepción	Alberto	128 SDR	Windows Xp	Si	No	Compaq	Presario 5000
Oficinas Administrativas	Lic. Magaña	256 DDR	Windows Xp	Si	No	Clon	U8998
	Lic Nora Amaya	256 DDR	Windows Xp	Si	No	Dell	Dimension 2100
Oficinas 2do. Nivel.	Lic José Polanco	256 DDR	Windows Xp	Si	Si	Clon	U8668-D
	Lic. Escobar	512 DDR	MAC OSX	Si	Si	MAC	Laptop
	Lic. Giancarlo Angelucci	256 DDR	Windows Xp	Si	Si	Dell	Laptop
	Lic. Telles	512 DDR	MAC OSX	Si	Si	MAC	Laptop
Recepción 2do. Nivel	Josefina Hernández	256 DDR	Windows Xp	Si	No	Clon	M6VLR

Cuadro 9 Cuadro de especificaciones técnicas

¿Cual es el nivel técnico promedio de sus empleados en las siguientes áreas, siendo 5 excelente?

Windows	1 | 2 | **3** | 4 | 5
Redes	1 | **2** | 3 | 4 | 5
Internet	1 | 2 | 3 | **4** | 5
Procesador de palabras	1 | 2 | 3 | 4 | **5**
Hoja de cálculo	1 | 2 | 3 | 4 | **5**
Desarrollo de páginas Web	**1** | 2 | 3 | 4 | 5
Diseño Gráfico	**1** | 2 | 3 | 4 | 5

Cuadro 10 promedio de nivel técnico de la empresa

Aunque no existen dos Intranets iguales, todos los proyectos Intranet exitosos tienen en común el hecho de tener una definición y entendimiento muy claros y lo mejor es tener una metodología para llegar a buen término.

6.3.6. CREACIÓN DE LA INTRANET

Para la creación de la Intranet se utilizara software de código abierto, este proveerá los servicios necesarios para los usuarios, tales como: Calendario, Notas, Directorio telefónico, Administrador de Archivos, Administrador de Proyectos, Etc. El software a utilizar son: Group-Office, Simple-Groupware y XenIntranet. A continuación se detallara cada uno de ellos:

GROUP-OFFICE

Group-Office es un software de código abierto con licencia GNU GPL diseñado para implementar una Intranet para empresas o corporaciones que requieran compartir su información, esto a través de una interfaz Web amigable la cual permite al administrador de la Intranet agregar, quitar módulos, tales como File Manager, Calendario, Address Book, Correo Electrónico, Project, entre otros. Ofrece además ofrece seguridad por medio de perfiles de usuarios. Los requisitos para montar esta aplicación son: PHP, Mysql, Apache y para los módulos es necesario configurar samba (Administrador de Archivos), módulos de Imap, mysql para Apache, entre otros.

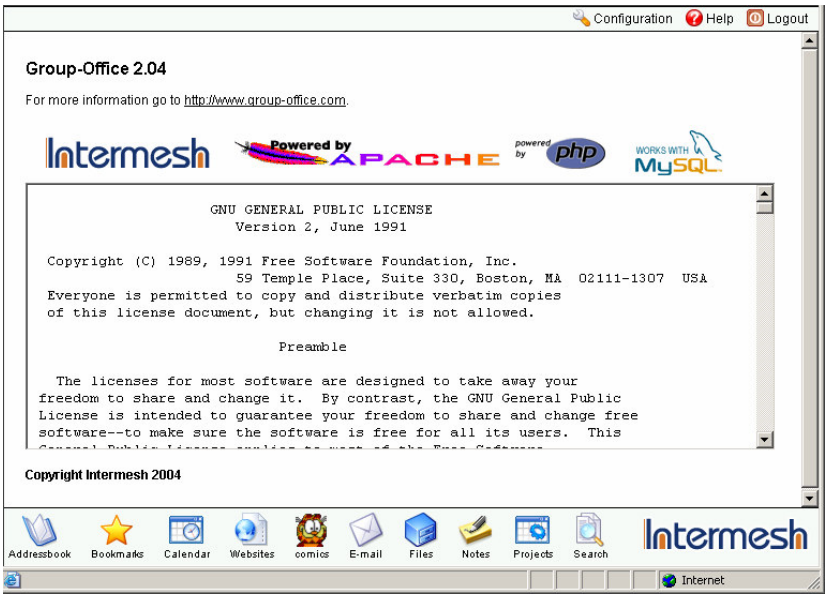


Figura 68 Interface Web del software Group-Office

SIMPLE-GROUPWARE

Simple_Groupware es un software de código abierto con licencia GNU GPL diseñado para implementar una Intranet, en general Simple Groupware ofrece:

- Una aplicación 100% basada en Web.
- Una completa seguridad de comunicación usando
- SSLComplete.
- Interfase Amigable.
- Plataforma de Administración, control y seguimiento de procesos de negocios.
- Autonomía: Simple Groupware es 100% código Abierto.
- Individualidad.
- Notificaciones: Unicode: Simple Groupware soporta Unicode usando UTF-8

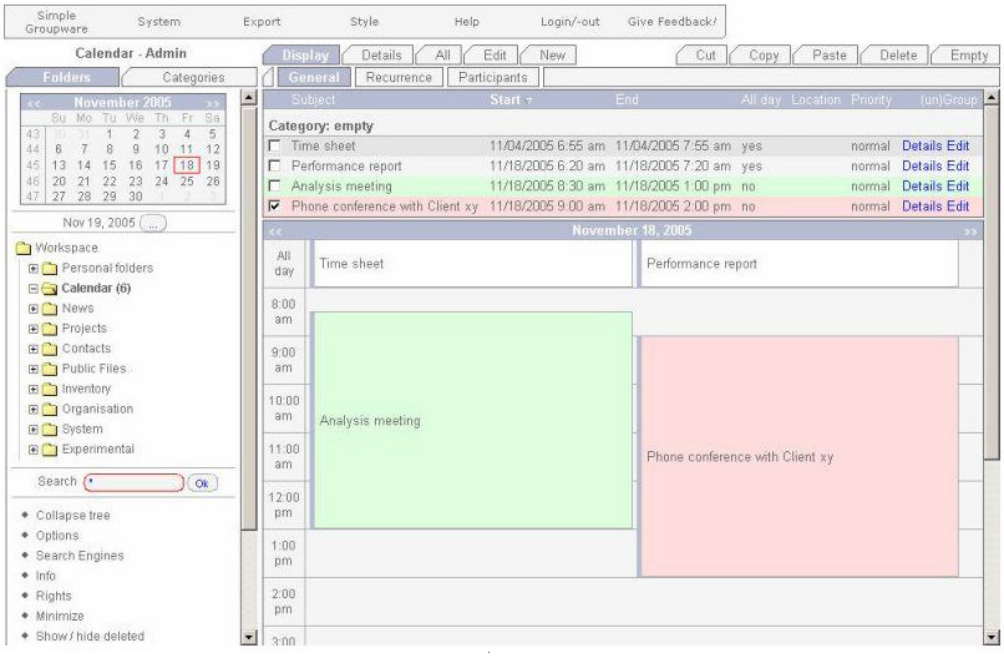


Figura 69 Interface Web del software Simple-Groupware

XENINTRANET

XenIntranet es una Intranet modular basada en una plataforma Web y PHP la cual brinda muchas herramientas tales como:

Características Generales

- Estructura Modular.
- Permisos (Privados, Públicos, Limitados por una lista de acceso).
- Grupos.
- Temas para las interfaces.
- Reportes.
- Calendario
- Directorio.
- Notas.

Figura 70 Interface Web del software XenIntranet

6.3.6.1. SELECCIÓN DE SOFTWARE PARA LA INTRANET

Para la selección del software se realizará un cuadro comparativo para decidir que software es el más adecuado para la implementación, el cuadro se basará en la seguridad y los servicios que estos poseen y aquellos que la empresa necesita, a continuación se detallan las características de cada uno del software elegido:

SERVICIOS	GROUP-OFFICE	SIMPLE-GROUPWARE	XENINTRANET
Libreta de Direcciones	Si	No	Si
Sitios Web Favoritos	Si	No	No
Correo Electrónico	Si	Si	No
Noticias	Si	Si	Si
Buscador	Si	Si	No
Separador de Libros (BookMarks)	Si	Si	No
Caricaturas	Si	No	Si
Libreta de Notas	Si	Si	SI
Calendarios	Si	Si	Si
Administrador de Archivos	Si	Si	No
Administrador de Proyectos	Si	Si	No
Interfase Web amigable	Si	No	Si

SEGURIDAD	GROUP-OFFICE	SIMPLE-GROUPWARE	XENINTRANET
Admnistrador de Perfiles	SI	No	Si
Admnistrador de Grupos	SI	Si	Si
Admnistrador de Usuarios	SI	Si	Si
Administrador de Servicios	SI	No	No

Cuadro11 comparativo de software para la Intranet

Después de haber analizado el cuadro comparativo se observa que el programa Group-Office es el programa más completo ya que cumple con los requerimientos de seguridad y de servicios que la empresa necesita, como a continuación se muestra:

SERVICIOS	GROUP-OFFICE	SIMPLE-GROUPWARE	XENINTRANET
Libreta de Direcciones	Si	No	Si
Sitios Web Favoritos	Si	No	No
Correo Electrónico	Si	Si	No
Noticias	Si	Si	Si
Buscador	Si	Si	No
Separador de Libros (BookMarks)	Si	Si	No
Caricaturas	Si	No	Si
Libreta de Notas	Si	Si	SI
Calendarios	Si	Si	Si
Administrador de Archivos	Si	Si	No
Administrador de Proyectos	Si	Si	No
Interfase Web amigable	Si	No	Si

SEGURIDAD	GROUP-OFFICE	SIMPLE-GROUPWARE	XENINTRANET
Admnistrador de Perfiles	SI	No	Si
Admnistrador de Grupos	SI	Si	Si
Admnistrador de Usuarios	SI	Si	Si
Administrador de Servicios	SI	No	No

Cuadro 12 comparativo de software para la Intranet

DIAGRAMA DE LA INTRANET

El diagrama en el cual la Intranet estará montada será el siguiente:

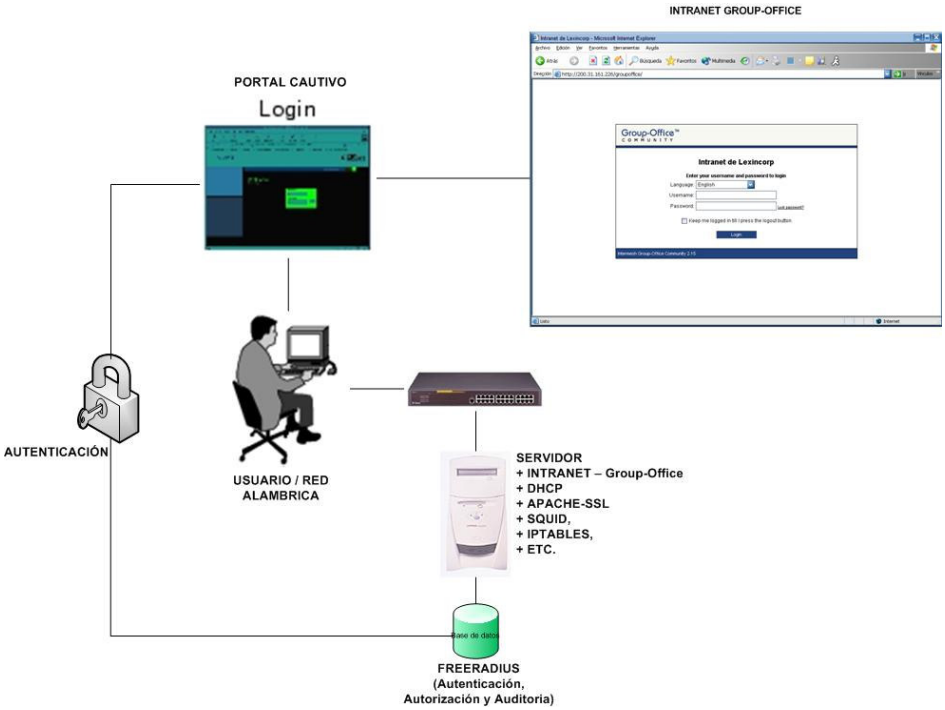


Figura 71 Diagrama de la Intranet

EXPLICACIÓN:

Un usuario de la red ya sea alambrica o inalámbrica entra a su maquina y utiliza un navegador, todas las transacciones que hace por el navegador son interceptadas por el portal cautivo, el cual muestra una pantalla de logeo.

Si el usuario posee una cuenta registrada podrá autenticarse en el servidor de freeradius el cual desde ese momento llevara estadísticas de logeo y monitoreara las sesiones que han habido en el, todo esto se almacenara en una base de datos la cual guardara la información de una manera efectiva y segura.

6.3.7. SEGURIDAD EN LA INTRANET

La seguridad estará compuesta básicamente por los mecanismos de control que el programa Group-Office posee, el programa Group-Office cuenta con una serie de ventajas de seguridad que son:

- **Administración de Perfiles:** se establecerán perfiles para todos los usuarios de la empresa, ejemplo, administrador del sistema, gerentes de área, usuarios normales, etc.
- **Administración de Grupos:** se crearan grupos por departamento los cuales tendrán registrados únicamente a los empleados que pertenecen a ellos.
- **Administración de Usuarios:** se crearan todos los usuarios conforme a la lista de empleados que tiene la empresa, estos formaran parte de grupos y tendrán perfiles los cuales delimitaran su uso en la Intranet.
- **Administración de Servicios:** se administraran los servicios según las necesidades de cada departamento, quitando o sumando a estos la que sea necesario.

Estas características de seguridad se integraran con la seguridad de las diferentes partes que constituyen el proyecto como lo son, la seguridad en el servidor y la seguridad en la red inalámbrica.

CONCLUSIONES Y RECOMENDACIONES:

CONCLUSIONES:

- Crear una Intranet segura con accesos desde una red inalámbrica protegida es un proceso desafiante y permanente respecto a la seguridad, la movilidad y la configuración.
- Una red inalámbrica bien diseñada, con el respaldo de políticas de seguridad proactivas, puede ofrecerle a los usuarios enormes beneficios de la información móvil, e incluso aumentar un tiempo real las ganancias de las actuales empresas, lo que se traduce en mayor productividad y flexibilidad a los trabajadores.
- Para casi cualquier empresa de hoy en día, y muy especialmente en un futuro muy cercano, la Intranet va ha ser un recurso indispensable. Dada la gran cantidad de datos que genera cualquier empresa, se están quedando obsoletos los actuales métodos de inserción y consulta de datos. Una Intranet puede resolver estos y otros problemas. Una Intranet puede resolver, por ejemplo, el problema de la distribución de información para todos los empleados, así pues se pueden publicar manuales, planes de acción, procedimientos, material de formación, folletos de marketing y productos, listas de precios, información comercial, anuncios, promociones etc. Y son accesibles para el empleado o cliente de forma inmediata, y con un ahorro considerable respecto a los métodos clásicos, panfletos, circulares, notas informativas, etc. Además cualquier actualización de datos es inmediata y no supone ninguna carga para la empresa como los métodos tradicionales.
- Se aprovechará también la potencia de una Intranet para tener acceso rápido a cualquier documento de la empresa, siempre que se tenga el nivel de privilegios adecuado.
- Las tecnología Intranet, también permiten compartir información y conocimientos independientemente de la ubicación.

- La tecnología Intranet es la habilidad de entregar información actualizada de manera rápida y costo eficiente a toda la base de usuarios. Una Intranet pone información vital al alcance de todos los empleados con acceso a ella.
- Cualquier actualización de datos es inmediata y no supone ninguna carga para la empresa como los métodos tradicionales manteniendo la consistencia porque la información es la misma a lo largo y ancho de la empresa.
- Los grupos multidisciplinarios y multi-departamentales, pueden aprovechar grandemente los grupos de discusión virtuales y boletines informativos para preparar reuniones o mejorar la toma de decisiones.
- Con el apoderamiento que da la Intranet, viene la capacidad (muy deseable por cierto) que los usuarios mismos publiquen por su cuenta información de interés de su grupo de trabajo o de la empresa entera. Esto incrementa la complejidad de la Intranet y sus requerimientos.

RECOMENDACIONES:

- La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.
- También es importante que al crear una red inalámbrica se tomen protocolos de seguridad que no requieran de actualizaciones de hardware en los equipos a corto plazo.
- Las WLAN tienen un alcance limitado que debe nivelarse en función de la seguridad de la red.
- Cubrir solo las áreas requeridas; las zonas para estacionar vehículos pueden no necesitar cobertura.
- Colocar los puntos de acceso más cerca del centro de las unidades. Evitar las paredes o ventanas quedan hacia la calle.
- Deben elegirse equipos que cumplan las últimas especificaciones de seguridad, tales como (WPA, 802.11i, WPA2, etc.).
- Activar el mayor nivel de seguridad que soporta el Hardware. Incluso si tiene un equipo de un modelo anterior que soporta únicamente WEP.
- Instalar cortafuegos personales y protección antivirus en todos los dispositivos móviles.
- Tanto el sistema operativo Linux como el resto de aplicaciones GPL deben ser tomados en cuenta como una verdadera competencia respecto a los sistemas operativos y aplicaciones propietarias, ya que su calidad, costo y herramientas son argumentos muy fuertes para su consideración y uso.

- El uso de herramientas de software gratuitos, es una forma de ahorrar costos a diversas cantidades de todo tipo y de mantener la eficiencia y calidad de las labores en las que estas se utilicen.

BIBLIOGRAFIA

a) Libros

- Hernández Sampieri, Roberto and Pilar Baptista Lucio. Metodología de la Investigación. : McGraw Hill/ Interamericana Editores S.A. de C.V. Tercera Edición, 2003.

b) Sitios de Internet

- Estándares Wireless. 5 Jul. 2006. IEEE. 12 Jul 2006. <http://standards.ieee.org/wireless/>.

- Articulos de redes inalámbricas. 6 Mar. 2006. IDATEL NETWORKS. 28 Apr. 2006. <http://www.idatelnetworks.com/publicaciones/articulos/>.

- 10 Jun. 2006. IEEE 802 Wireless World. 23 Jul. 2006. <http://www.802wirelessworld.com/index.jsp>.

- Dispositivos inalámbricos. 15 Feb. 2006. Alcalawireless. 24 Mar. 2006. <http://www.alcalawireless.com>.

- Comunidades Wireless. 24 Aug. 2006. Pucela Wireless. 28 Aug. 2006. <http://www.pucelawireless.net>.

- Articulos de redes inalámbricas. 29 May 2006. Red Libre. 16 Jun. 2006. <http://www.redlibre.net>.

- Dispositivos de redes inalámbricas. Wireless Router. 21 Jun. 2006. <http://www.scqwireless.com>.

- Asociación Wireless. Sevilla Wireless. 8 Apr. 2006. <http://www.scqwireless.com>.

- Redes Inalámbricas en los países en desarrollo. Jan. 2006. Limehouse Book Sprint Team. 20 Apr. 2006. <http://wndw.net/pdf/wndw-es-ebook.pdf>.

- Análisis Económico. Wi-fi. 20 Aug. 2006. <http://www.dgroups.org/groups/ica/wifipublico/docs/wireless%20Fidelity%20Costos.rtf>.

- Security Handbook. RFC. 7 Jun. 2006. <//ftp.rfc-editor.org/in-notes/rfc2196.txt>.

- Radiación de antenas. 3COM. 11 Sep. 2006. <http://www.3com.com/other/pdfs/products/en_US/101900.pdf#search=%223com%20Omni%20antennas%20radiation%22>.

GLOSARIO

A

AAA

- **Autenticación** es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.
- **Autorización** es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.
- **Accounting** es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeamiento de capacidad, billing, auditoría y costallocation.

A menudo los servicios **AAA** requieren un servidor dedicado. RADIUS es un ejemplo de un servicio AAA.

Access Point: Son Puntos de Acceso son el 'centro de datos' de una red inalámbrica. Se trata de unas pequeñas unidades que extienden la conectividad inalámbrica a aquellos computadores de escritorio o portátiles que dispongan de NICs inalámbricas (los clientes inalámbricos pueden compartir archivos, recursos y una conexión a Internet.

ACL (Access Control List): Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la

dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

Ad Hoc: Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un Access Point. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

AES - Estándar de Cifrado Avanzado: También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.

B

Bridge: Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.Se pueden acoplar a cualquier dispositivo Ethernet para ampliar la conectividad inalámbrica.

C

ChilliSpot: Es un programa o máquina de una red LAN o WLAN que restringe el tráfico HTTP:// y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. A veces esto se hace para pedir una autenticación válida, o para informar de las condiciones de uso de un servicio de una red alambrica o de una red inalámbrica. (Que es donde más se encuentran).

Cortafuegos (**Firewall**): Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de

seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc...

D

DES: Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

3DES: Basado en 3 iteraciones sucesivas del algoritmo DES consiguiendo con ello una clave de 128 bits. Además es compatible con DES simple.

Dial-up admin: Software para el monitoreo y control de sesiones y tiempo de conexión de usuarios autorizados.

E

EAP - Protocolo de Autenticación Extensible: Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virutla (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP

EAP –TLS: Definido en la RFC 2716 y es probablemente el método de autenticación más ampliamente soportado en clientes inalámbricos y en servidores RADIUS. Este método utiliza claves publicas certificadas para autentificar tanto al cliente como al servidor mediante el establecimiento de una sesión encriptada entre ellos.

F

Firewall Iptables: Sirve como muro de fuegos el cual detendrá los ataques e intrusiones a la red.

FreeRadius: Es un sistema cliente/servidor usado para Autenticación, Autorización y Auditoria para asegurar la red contra accesos no autorizados.

G

Gateway: Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas.

Group-Office: Es una Intranet para Empresas o corporaciones que requieran compartir su información, esto a través de una interfaz Web amigable la cual Permite al administrador de la Intranet agregar, quitar módulos, tales como File Manager, Calendario, Address Book, Correo Electrónico, Project, entre otros. Además ofrece seguridad por medio de perfiles de usuarios. Los requisitos son: PHP, Mysql, Apache y para los módulos es necesario configurar samba (File Manager), módulos de Imap, mysql para Apache, entre otros. *http://sourceforge.net/projects/group-office/*

I

IEEE - Instituto de Ingenieros Eléctricos y Electrónicos : Formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo (http://www.ieee.org/).

> **802.11**: Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas (wireless). Permite la conexión de dispositivos móviles (lap-top, PDA, teléfonos celulares a una red cableada, por medio de un Access Point (Access Point). La conexión se realiza a través de ondas de Radio Frecuencia. Originalmente ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de 2.4 GHz. Se le conoce popularmente como WIFI. Tiene un área de cobertura aproximada de 100 ms.

802.11g: Estándar de conexión wireless que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz. Se basa en la tecnología OFDM, al igual que el estándar

802.1x: Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

802.16: Estándar de transmisión wireless conocido como WIMAX (Worldwide Interoperability for Microwave Access). Es compatible con WIFI. Se originó en Abril de 2002 con la finalidad de cubrir inalámbricamente distancias de hasta 50 Km. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz.. La interoperatividad es certificada por el WIMAX FORUM *(http://www.wimaxforum.org/).*

802.11n: Estándar en elaboración desde Enero 2004. Tiene como objetivo conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps. Hay 2 propuestas distintas. En 2006 se aprobará una de las dos. La de TGn Sync o la WWiSE.

802.11i: Estándar de seguridad para redes wifi aprobado a mediados de 2004. En el se define al protocolo de encriptación WPA2 basado en el algoritmo AES.

802.16d: Estándar de transmisión wireless (WIMAX*) que suministra una velocidad de entre 300 K y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Ratificado a finales de 2004. Se utiliza para el cubrimiento de la "primer milla".

802.16e: El cual se prevee su publicacion a finales del 2005, en el cual permitira conectividad semejante al Wi-Fi en dispositivos moviles pero con mayor ancho de banda, a lo cual, Intel planea sacar un chip listo para WiMAX como parte de su chip Centrino al momento de la publicación del estandar.

Intranet: Intranet es un Internet interno diseñado para ser utilizado en el interior de una empresa, universidad, u organización. Lo que distingue a un Intranet del Internet de libre acceso es el hecho de que el Intranet es privado. Gracias a los Intranets, la comunicación y la colaboración interna son más fáciles.

IPX: Conectan una red de computadoras utiliza Protocolos de capa 3

L

LEAP (Lightweight Extensible Authentication Protocol): Es un método EAP propietario de Cisco que utiliza claves para autenticar los clientes. LEAP solo trabaja con software y hardware de Cisco y otros pocos proveedores. Tiene muchas vulnerabilidades tales como la susceptibilidad a ataques para descubrir las claves de usuarios, también que solo puede autenticar a los usuarios para entrar a la WLAN no a la computadora, sin esto las políticas de la maquina no se ejecutaran debidamente ni tampoco las instalaciones de programas

M

MIC (Message Integrity Code) o Michael: Código que verifica la integridad de los datos de las tramas.

O

OSA (OPEN SYSTEM AUTHENTICATION): Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

P

PAP: Password Authentication Protocol. Protocolo de Autentificación por Password. Permite al sistema verificar la identidad del otro punto de la conexión mediante password.

PEAP: Este es un método de autenticación de dos pasos. Primeramente, establece una sesión TLS con el servidor y permite al cliente autentificar al servidor usando la certificación digital del servidor. Luego, se requiere un segundo método EAP haciendo un túnel dentro de la sesión PEAP para autenticar al cliente hacia el servidor RADIUS.

PIX: (Private Internet Exchange/ Intercambio de Internet Privado): Es una solución de seguridad de hardware/software especializada que entrega la seguridad de alto nivel sin impactar la actuación de la red. Es un sistema híbrido porque usa los rasgos de ambos el paquete que se filtra y tecnologías de servidor de apoderado.

Politica de Seguridad Informatica (PSI): Es una herramienta organizacional creada con el fin de concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento

POP: Protocolo de Oficina de Correos (Post Office Protocol) Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita la entre de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

PPP: Protocolo Punto a Punto (Point to Point Protocol). Implementación de TCP/IP por líneas seriales (como en el caso del módem). Es más reciente y complejo que SLIP.

R

RADIUS - Remote Authentication Dial-In User Service: Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un

servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

Redes externas: Hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas. Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

Red inalámbrica: Una Red Inalámbrica Es una red que permite a los usuarios conectarse a una red local o a Internet sin estar conectado físicamente, no hace falta tener una toma de red o de teléfono. La comunicación se realiza a través de ondas que viajan por el aire, sin necesidad de cables

Redes internas: Están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización. Dentro de una red interna, los servidores de Web se instalan en la red.

RFC (Request For Comments). En esta serie de documentos se detalla prácticamemnte todo lo relacionado con la tecnología de la que se sirve **Internet**: protocolos, recomendaciones, comunicaciones...

RFC 2196 (Manuel de Seguridad): Este es una guía para desarrollar políticas y procedimientos. El propósito es proveer una guía práctica a los administradores que tratan de darle seguridad a su información y servicios. Los temas cubiertos incluyen políticas, un rango amplio de sistemas técnicos y temas de seguridad en redes, y incidentes de seguridad.

Roaming (Itinerancia): En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Access Point a otra sin interrumpir el servicio o pérdida de conectividad

Router: (Direccionador) Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza basándose en información de nivel de red y tablas de direccionamiento.

S

Servidor de Autenticación: Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.

SMTP (Simple Mail Transfer Protocol / Protocolo Simple de Transferencia de Correo): Protocolo estándar de Internet para intercambiar mensajes de correo electrónico.

SPAM: También conocido como *junk-mail o correo basura*, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

Switch: Es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconection*).

T

TKIP - Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS - Transport Layer Security: Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet.

TTLS: Es un método de 2 pasos similar a PEAP, el cual usa una sesión TLS para proteger la autenticación por medio de túnel del cliente. Además de los métodos de túnel de EAP, TTLS puede usar versiones de protocolos de autenticación que no sean EAP tales como CHAP, MS-CHAP, y otros.

V

VPN - Red Privada Virtual: Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (*LAN*).

W

WAN (Wide Area Network / Red de Area Amplia): Red en que los componentes se encuentran físicamente distantes unos de otros.

WEP - Wired Equivalent Privacy: Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

Wi-Fi : Abreviatura de Wireless Fidelity. Es el nombre “comercial” conque se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.

WIMAX: Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM

divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

WLAN - Red de Área Local Inalámbrica: También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA - Acceso Wi-Fi Protegido: Protocolo de aplicación de tecnología inalámbrica que posibilita el acceso a páginas web especialmente diseñadas para este lenguaje y está disponible en versiones 1.1 y 2.0. Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WPA2 - Protocolo de Aplicación Inalámbrica: Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.

APENDICES

APENDICE A: MANUALES

1.1. MANUAL DE INSTALACION Y CONFIGURACION DE CHILLI SPOT

INSTALACION

Paso 1: Bajar el programa del sitio http://www.chillispot.org
wget http://www.chillispot.org/download/chillispot-1.0.tar.gz

Paso 2: Descomprimir el archivo chillispot-1.0.tar.gz.
tar -xzvf chillispot-1.0.tar.gz

Paso 3: Entrar al directorio que se ha descomprimido.
cd chillispot-1.0

Paso 4: Ejecutar el comando configure, “configure” es una herramienta GNU que sirve para detectar las configuraciones del sistema y crea los archivos Makefile.
./configure

Paso 5: Ejecutar el comando make, “make” lee los archivos makefile y compila todo. Este además reporta si le hace falta algo al sistema para seguir compilándolo.
make

Paso 6: Ejecutar el comando
make install

Paso 7: Copiar archivo de configuración al directorio “/etc” este se encuentra en la siguiente dirección /usr/share/doc/chillispot.
cp /usr/share/doc/chillispot/chilli.conf /etc

Paso 8: Crear Directorio para la interfaz tun.
mkdir /dev/net

Paso 9: Crear Ficheros especiales para la interfaz tun, esto lo haremos con mknod.
mknod /dev/net/tun c 10 200

Paso 10: Levantar el modulo de tun
modprobe tun

Paso 11: El directorio en el cual se ha instalado el programa es el siguiente:
/etc, acá podrá hacer las configuraciones necesarias para hacer funcionar el programa.

CONFIGURACION

Paso 1: Editar archivo chilli.conf en el directorio /etc.
nano /etc/chilli.conf

Paso 2: Habilitación de Chilli Spot en modo debug, buscaremos la sección siguiente TAG: debug y quitaremos el signo "#" a debug, esto nos ayudara a resolver problemas al momento de correr el servicio:

```
# TAG: debug
# Include this flag to include debug information.
debug
```

Paso 3: parámetros de la interfaz TUN, dejar los valores por defecto.

Paso 4: parámetro de conexión a servidor Radius.

a. Servidor Radius 1: este será el primer servidor radius al cual se conectara, como estamos trabajando con localhost dejaremos 127.0.0.1 así:

```
# TAG: radiusserver1
# IP address of radius server 1
# For most installations you need to modify this tag.

radiusserver1 127.0.0.1
```

b. Servidor Radius 2: al igual que el 1 este lo colocaremos en localhost, este es un respaldo del primero, si el primer servidor no esta disponible entra este.

```
# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set
# radiusserver2 to the same value as radiusserver1.
# For most installations you need to modify this tag.

radiusserver2 127.0.0.1
```

c. Contraseña de conexión entre Chilli Spot y Freeradius: colocar la contraseña que utilizara para conectar ambos servicios:

TAG: radiussecret
Radius shared secret for both servers
For all installations you should modify this tag.

radiussecret lexincorp123

Paso 5: Parámetros del Proxy: dejar los valores por defecto.

Paso 6: Parámetros del dhcp:

a. Interfaz dhcp: esta será la interfaz Ethernet que estará conectada con las pc y con la cual el chilli spot dará direcciones IP dinámicas del rango 192.168.0.182/24. Utilizaremos para este objetivo la Interfaz eth0

TAG: dhcpif
Ethernet interface to listen to.
This is the network interface which is connected to the access points.
In a typical configuration this tag should be set to eth1.

dhcpif eth0

Paso 7: Parámetros UAM (Método de Acceso Universal)

b. Servidor uamserver: este se encargará de autenticar y autorizar a todo aquel usario que tenga la autorización para poder logearse en el sistema esto a través de un cgi llamado hotspotlogin.cgi.

TAG: uamserver
URL of web server handling authentication.

uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi

c. Servidor uamhomepage: este se encargará de redireccionar todas las peticiones que las maquinas de usuario hagan al puerto 80 y las enviará a un portal cautivo o algún portal que se configure para este objetivo.

TAG: uamhomepage
URL of welcome homepage.
Unauthenticated users will be redirected to this URL. If not specified
users will be redirected to the uamserver instead.
Normally you do not need to uncomment this tag.

uamhomepage https://192.168.182.1/index.html

d. Dirección Autenticación: esta será la dirección por la cual todas las maquinas de usuario que tengan acceso a la red podrán autenticarse.
TAG: uamlisten
IP address to listen to for authentication requests
Do not uncomment this tag unless you are an experienced user!

uamlisten 192.168.182.1

Paso 8: parámetros de autenticación por MAC: dejar los valores por defecto.

Paso 9: Guardar Cambios.

Paso 10: ejecutar chilli spot
Chilli&

ARCHIVO DE CONFIGURACION

TAG: fg
Include this flag if process is to run in the foreground
fg
TAG: debug
Include this flag to include debug information.
debug

TAG: interval
Re-read configuration file at this interval. Will also cause new domain
name lookups to be performed. Value is given in seconds.
#interval 3600

TAG: pidfile
File to store information about the process id of the program.
The program must have write access to this file/directory.
#pidfile /var/run/chilli.pid

TAG: statedir
Directory to use for nonvolatile storage.

```
# The program must have write access to this directory.
# This tag is currently ignored
#statedir ./
# TUN parameters

# TAG: net
# IP network address of external packet data network
# Used to allocate dynamic IP addresses and set up routing.
# Normally you do not need to uncomment this tag.
#net 192.168.182.0/24

# TAG: dynip
# Dynamic IP address pool
# Used to allocate dynamic IP addresses to clients.
# If not set it defaults to the net tag.
# Do not uncomment this tag unless you are an experienced user!
#dynip 192.168.182.0/24

# TAG: statip
# Static IP address pool
# Used to allocate static IP addresses to clients.
# Do not uncomment this tag unless you are an experienced user!
#statip 192.168.182.0/24

# TAG: dns1
# Primary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns1 172.16.0.5

# TAG: dns2
# Secondary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns2 172.16.0.6
# TAG: domain
```

```
# Domain name
# Will be suggested to the client.
# Normally you do not need to uncomment this tag.
domain salnet.net

# TAG: ipup
# Script executed after network interface has been brought up.
# Executed with the following parameters: <devicename> <ip address>
# <mask>
# Normally you do not need to uncomment this tag.
#ipup /etc/chilli.ipup

# TAG: ipdown
# Script executed after network interface has been taken down.
# Executed with the following parameters: <devicename> <ip address>
# <mask>
# Normally you do not need to uncomment this tag.
#ipdown /etc/chilli.ipdown

# Radius parameters

# TAG: radiuslisten
# IP address to listen to
# Normally you do not need to uncomment this tag.
#radiuslisten 127.0.0.1

# TAG: radiusserver1
# IP address of radius server 1
# For most installations you need to modify this tag.
radiusserver1 127.0.0.1

# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set radiusserver2 to the
# same value as radiusserver1.
# For most installations you need to modify this tag.
radiusserver2 127.0.0.1
# TAG: radiusauthport
```

```
# Radius authentication port
# The UDP port number to use for radius authentication requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
#radiusauthport 1812

# TAG: radiusacctport
# Radius accounting port
# The UDP port number to use for radius accounting requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
#radiusacctport 1813

# TAG: radiussecret
# Radius shared secret for both servers
# For all installations you should modify this tag.
radiussecret testing123

# TAG: radiusnasid
# Radius NAS-Identifier
# Normally you do not need to uncomment this tag.
#radiusnasid nas01

# TAG: radiuslocationid
# WISPr Location ID. Should be in the format: isocc=<ISO_Country_Code>,
# cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<ssid/ZONE>
# Normally you do not need to uncomment this tag.
#radiuslocationid isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport

# TAG: radiuslocationname
# WISPr Location Name. Should be in the format:
# <HOTSPOT_OPERATOR_NAME>,<LOCATION>
# Normally you do not need to uncomment this tag.
#radiuslocationname ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport


# Radius proxy parameters
# TAG: proxylisten
```

```
# IP address to listen to
# Normally you do not need to uncomment this tag.
#proxylisten 10.0.0.1

# TAG: proxyport
# UDP port to listen to.
# If not specified a port will be selected by the system
# Normally you do not need to uncomment this tag.
#proxyport 1645

# TAG: proxyclient
# Client(s) from which we accept radius requests
# Normally you do not need to uncomment this tag.
#proxyclient 10.0.0.1/24

# TAG: proxysecret
# Radius proxy shared secret for all clients
# If not specified defaults to radiussecret
# Normally you do not need to uncomment this tag.
#proxysecret testing123


# DHCP Parameters

# TAG: dhcpif
# Ethernet interface to listen to.
# This is the network interface which is connected to the access points.
# In a typical configuration this tag should be set to eth1.
dhcpif eth0

# TAG: dhcpmac
# Use specified MAC address.
# An address in the range  00:00:5E:00:02:00 - 00:00:5E:FF:FF:FF falls
# within the IANA range of addresses and is not allocated for other
# purposes.
# Normally you do not need to uncomment this tag.
#dhcpmac 00:00:5E:00:02:00
# TAG: lease
```

```
# Time before DHCP lease expires
# Normally you do not need to uncomment this tag.
#lease 600

# Universal access method (UAM) parameters

# TAG: uamserver
# URL of web server handling authentication.
uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi

# TAG: uamhomepage
# URL of welcome homepage.
# Unauthenticated users will be redirected to this URL. If not specified
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.
uamhomepage https://192.168.182.1/index.html

# TAG: uamsecret
# Shared between chilli and authentication web server
#uamsecret ht2eb8ej6s4et3rg1ulp

# TAG: uamlisten
# IP address to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
uamlisten 192.168.182.1

# TAG: uamport
# TCP port to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
#uamport 3990

# TAG: uamallowed
# Comma separated list of domain names, IP addresses or network segments
# the client can access without first authenticating.
# It is possible to specify this tag multiple times.
# Normally you do not need to uncomment this tag.
#uamallowed 192.168.182.0/24
# TAG: uamanydns
```

```
# If this flag is given unauthenticated users are allowed to use
# any DNS server.
# Normally you do not need to uncomment this tag.
#uamanydns

# MAC authentication

# TAG: macauth
# If this flag is given users will be authenticated only on their MAC
# address.
# Normally you do not need to uncomment this tag.
#macauth

# TAG: macallowed
# List of MAC addresses.
# The MAC addresses specified in this list will be authenticated only # on their MAC address.
# This tag is ignored if the macauth tag is given.
# It is possible to specify this tag multiple times.
# Normally you do not need to uncomment this tag.
#macallowed 00-0A-5E-AC-BE-51,00-30-1B-3C-32-E9

# TAG: macpasswd
# Password to use for MAC authentication.
# Normally you do not need to uncomment this tag.
#macpasswd password

# TAG: macsuffix
# Suffix to add to MAC address in order to form the username.
# Normally you do not need to uncomment this tag.
#macsuffix suffix
```

1.2. MANUAL DE INSTALACION Y CONFIGURACION DE FREERADIUS

INSTALACION

Dependiencias: Instalar los siguientes paquetes antes de la instalación

1. libmysqlclient10-dev.
2. libmysqlclient10.
3. libperl-dev.
4. libdb3.
5. gcc.
6. libdb3-dev.

Paso 1: bajar el programa del sitio http://www.freeradius.org
wget ftp://ftp.freeradius.org/pub/radius/old/freeradius-1.1.1.tar.gz

Paso 2: Descomprimir el archivo freeradius-1.1.1.tar.gz.
tar -xzvf freeradius-1.1.1.tar.gz

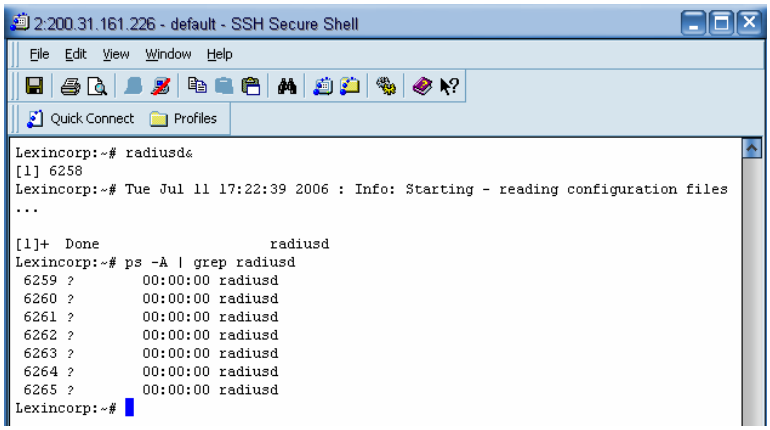
Paso 3: Entrar al directorio que ha descomprimido.
cd freeradius-1.1.1

Paso 4: Ejecutar el comando configure, “configure” es una herramienta GNU que sirve para detectar las configuraciones del sistema y crea los archivos Makefile.
./configure

Paso 5: Ejecutar el comando make, “make” lee los archivos makefile y compila todo. Este además reporta si le hace falta algo al sistema para seguir compilándolo.
make

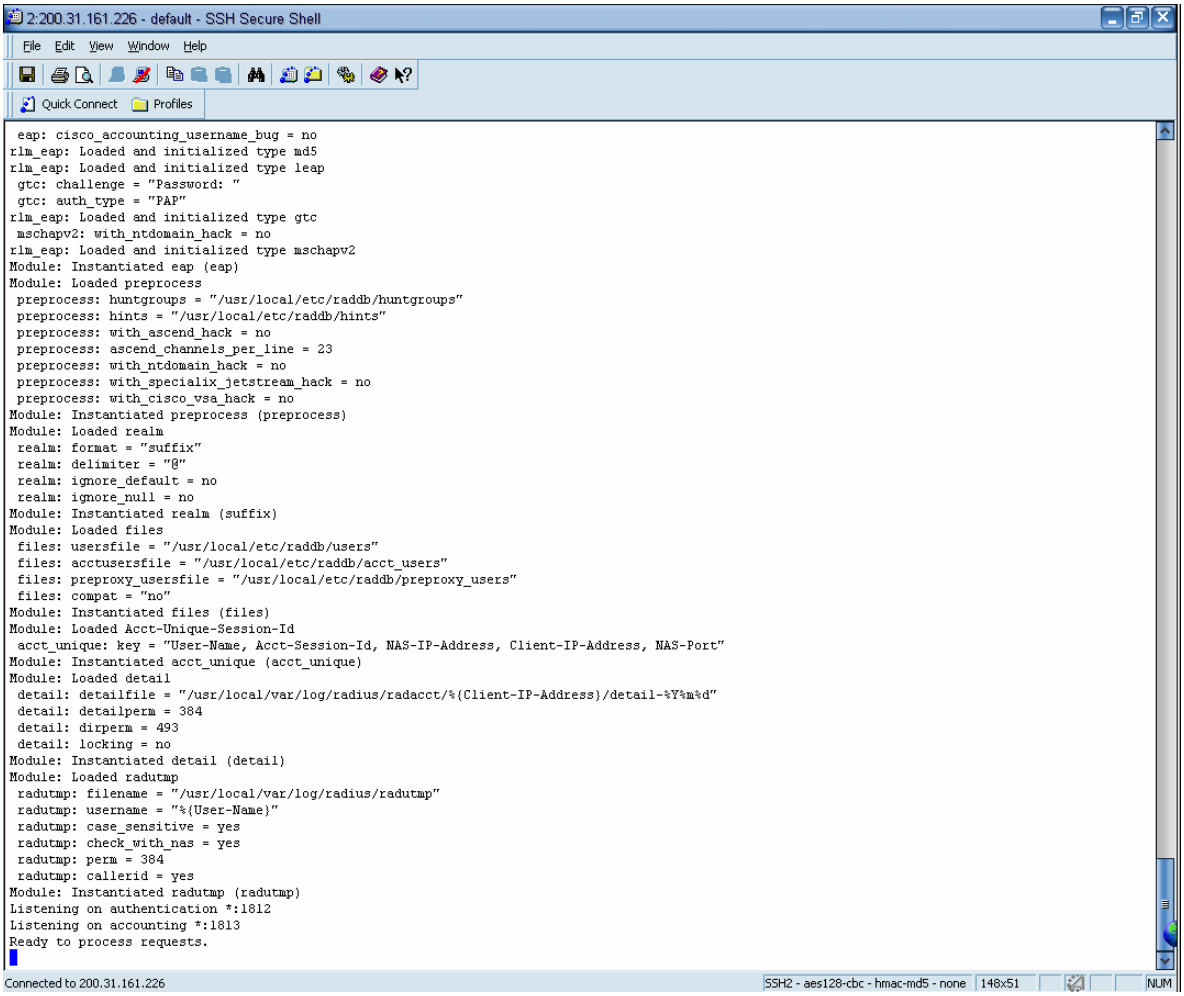
Paso 6: Ejecutar el comando
make install

Paso 7: Ejecutar radius: para la ejecución de radius se puede hacer de dos forma, la primera corriendo como servicio sin depuración y la segunda con depuración así:
Correrlo sin depuración: este correra como un servicio más del sistema
radiusd&



Paso 8: Correrlo con depuración: este te informara de errores de conexión a la base de datos y de los módulos que fueron cargados

radiusd -X



Paso 9: El directorio en el cual se ha instalado el programa es el siguiente:

/usr/local/etc/raddb, acá podrá hacer las configuraciones necesarias para hacer funcionar el programa.

CONFIGURACION

Paso 1: Editar el archivo de configuración /usr/local/etc/raddb/clients.conf, en este archivo de configuración se modificara únicamente el password “secret” para unir el freeradius y el Chilli Spot, así:
secret: lexincorp123

Paso 2: el archivo de configuración /usr/local/etc/raddb/users no se modificará ya que utilizaremos mysql para la autenticación de los usuarios.

Paso 3: el archivo de configuración /usr/local/etc/raddb/realms no se modificará ya no utilizaremos nombre con la opción realms.

1.2.1. CONFIGURACION DE FREERADIUS CON MYSQL

CONFIGURACIÓN DE BASE DE DATOS

Paso 1: entrar al directorio de freeradius
cd freeradius-1.1.1

Paso 2: entrar a la carpeta que contiene el scritp de sql que crea las tablas de la base de datos.
cd doc/examples

Paso 3: Crear una base de datos con nombre “freeradius”.
mysqladmin create freeradius

Paso 4: ejecutar el scritp que contiene las tablas de la base de datos
mysql freeradius < mysql.sql

Paso 5: Agregar usuario para manejar la base de datos
mysql -u root -p -e "GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP ON freeradius.* TO freeradius@localhost IDENTIFIED BY 'radius'" mysql

CONFIGURACION DE FREERADIUS PARA USAR MYSQL

Paso 1: Editar el archivo de configuración sql.conf ubicado en el directorio /usr/local/etc/raddb, buscar en el archivo de configuración las líneas donde se encuentra la información del servidor, base de datos, usuario y contraseña, configurarlo con los datos que usted a creado, con estos datos se podrá conectara a la base de datos así:

Ejecutar el comando, el cual editara el archivo: nano sql.conf

```
sql {
 # Database type
# Current supported are: rlm_sql_mysql, rlm_sql_postgresql,
# rlm_sql_iodbc, rlm_sql_oracle, rlm_sql_unixodbc, rlm_sql_freetds
driver = "rlm_sql_mysql" # Driver que se utilizará, en este caso utilizaremos mysql.

# Connect info
server = "localhost" # Servidor al cual se conectará freeradius.
login = "freeradius" # Usuario para conectarse a la base de datos.
password = “radius" # Contraseña del usuario.

# Database table configuration
radius_db = "freeradius" # Base de datos donde se guardará la información.
```

Paso 2: Si piensas utilizar usuarios para autentificarse solamente con un nombre como por ejemplo “amolina” tienes que editar la línea “sql_user_name”, en nuestro caso se utilizaran usuarios con nombres sencillos.

```
sql_user_name = "%{User-Name}"
#sql_user_name = "%{Stripped-User-Name}"
```

Paso 3: editar el archivo de configuración radiusd.conf ubicado en el directorio /usr/local/etc/raddb, busca la sección “authorize{}” la cual autoriza a los usuarios, en este caso la configuraremos para que autoricé a los usuarios que tenemos en nuestra base de datos, al final quedará configurado así:

```
authorize {
        preprocess
        chap
        mschap
        #counter
        #attr_filter
        #eap
        suffix                                  sql
```

```
        #files
        #etc_smbpasswd
}
```

Paso 4: editar el archivo de configuración radiusd.conf ubicado en el directorio /usr/local/etc/raddb, busca la sección “authenticate {}” la cual autentica a los usuarios con un método de autenticación como por ejemplo PAP, CHAP, MS-CHAP, al final quedará configurado así:

```
authenticate {
        authtype PAP {
                pap
        }
        authtype CHAP {
                chap
        }
        authtype MS-CHAP{
                mschap
        }
        #pam
        #unix
        #authtype LDAP {
                #       ldap
        #}
}
```

Paso 5: editar el archivo de configuración radiusd.conf ubicado en el directorio /usr/local/etc/raddb, busca la sección “preacct {}” el cual es una pre-contabilidad este decide que tipo de contabilidad se utilizará, al final quedará configurado así:

```
preacct {
        preprocess
        suffix
        #files
}
```

Paso 6: editar el archivo de configuración radiusd.conf ubicado en el directorio /usr/local/etc/raddb, busca la sección “accounting {}” crea un registro detallado de los paquetes. Observa las peticiones de la contabilidad que son proxiadas y las guarda en un archivo de log, al final quedará configurado así:

```
accounting {
        acct_unique
        detail
```

```
        #counter
        unix
        sql
        radutmp
        #sradutmp
}
```

Paso 7: editar el archivo de configuración radiusd.conf ubicado en el directorio /usr/local/etc/raddb, busca la sección “session {}” esta sección se usa para chequear multiples sesiones la cual usa los modulos radutmp o rlm_sql los cuales son sumamente rapidos, al final quedará configurado así:

```
session {
        radutmp
}
```

1.3. MANUAL DE CONFIGURACION DEL SERVIDOR

INTERFACES DE RED

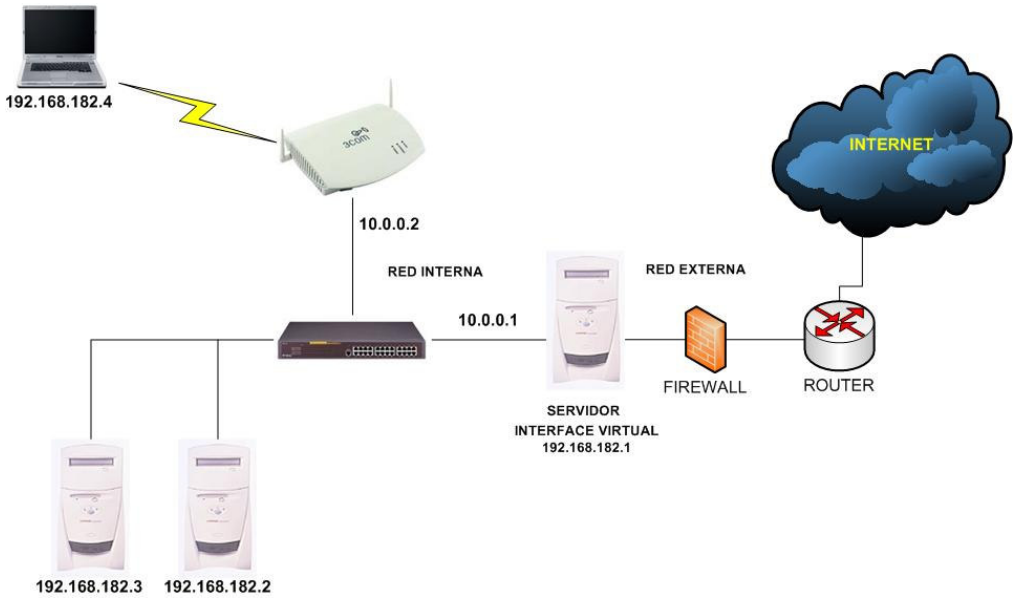
Para la implementación se ocuparan dos interfaces de red en el servidor, por lo cual se ocuparan en este caso dos tarjetas de red en las cuales se configuraran la red externa, la red interna y una interfaz virtual la cual es la encargada de asignar direcciones IP a los usuarios de la red, a continuación se detalla cada una de ellas:

Red Externa: La red externa es típicamente el Internet la cual dará acceso a la navegación. Esta es proporcionada por el servidor del servicio.

Red Interna: La red interna está conectada a los puntos de acceso con el servidor que contendrá el ChilliSpot, como por ejemplo el Switch, Access Point, etc. A estos puntos de conexión se les asignaran direcciones IP del rango 10.0.0.0 /24.

Red Virtual: ChilliSpot crea una interfaz virtual la cual asigna direcciones IP del rango 192.168.182.0/24 a los clientes que estén conectados a los puntos de acceso, en este caso son para la red alambrica e inalámbrica.

Red Inalámbrica: Los clientes inalámbricos están conectados con la red inalámbrica, y el Access Point sirve como puente entre la red interna y la red inalámbrica. Estos habilitan el direccionamiento entre la interfaz Ethernet y el servidor ChilliSpot, los clientes que tengan acceso a la red inalámbrica se les asignaran direcciones IP del rango 192.168.182.0 /24.



Esquema con interfaces de red

La configuración de las interfaces de red quedará de la siguiente manera:

* Editar archivo /etc/network/interfaces

This file describes the network interfaces available on your system

and how to activate them. For more information, see interfaces(5).
Red loopback
auto lo
iface lo inet loopback

Red Externa
auto eth1

iface eth1 inet static

address 200.31.161.226

netmask 255.255.255.252

gateway 200.31.161.225

Red Interna

auto eth0

iface eth0 inet static

address 10.0.0.1

netmask 255.255.255.0

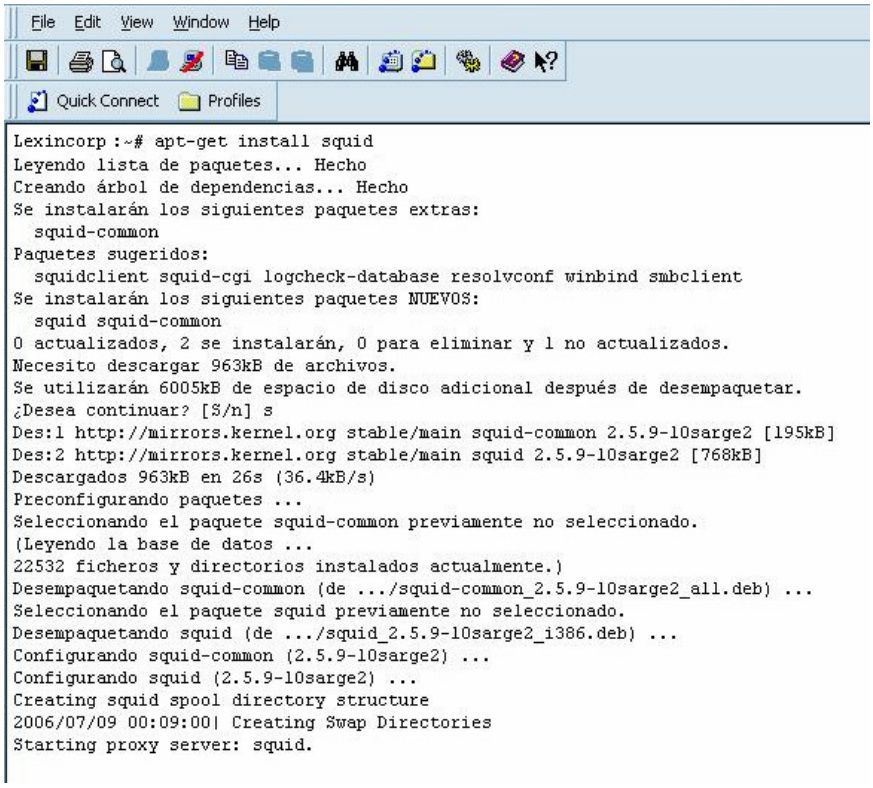
network 10.0.0.0

Esta configuración estará programada para que cada vez que el servidor inicie levante las interfaces.

1.3.1. INSTALACION DE PROXY WEB (SQUID)

Paso 1: instalación con apt

apt-get install squid



Paso 2: Configuración, entra al directorio donde esta el archivo de configuración de squid.
cd /etc/squid

Paso 3: Hacer una copia de seguridad del archivo
cp squid.conf squid.conf.old

CONFIGURACIÓN BÁSICA

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf, y podrá trabajar sobre este utilizando su editor de texto simple preferido. Existen un gran número de parámetros, de los cuales recomendamos configurar los siguientes:

- http_port: se utilizara el puerto 3128.
- cache_dir: se utilizara el siguiente directorio para el cache del squid cache_dir ufs /var/spool/squid 700 16 256
- Al menos una Lista de Control de Acceso: No se ocuparan listas de acceso.
- Al menos una Regla de Control de Acceso: se agregara una línea en esta sección la cual permitirá a la red 192.168.182.0/24 para que puede navegar:
  acl redlocal src 192.168.182.0/255.255.255.0
- httpd_accel_host: se habilitara en esta sección lo siguiente:
  httpd_accel_host virtual
- httpd_accel_port: Se utilizara el puerto 80
  httpd_accel_port 80
- httpd_accel_with_proxy: Se habilitara el aceleramiento con el Proxy y se dejara en on.
  httpd_accel_with_proxy on

Reiniciar el servicio en /etc/init.d:
./squid restart

Si desea mayor información de cómo configurar este servicio puede entrar a la página http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=19-0-como-squid-general

1.3.2. INSTALACION DE MYSQL-SERVER

Paso 1: instalación con apt
apt-get install mysql-server

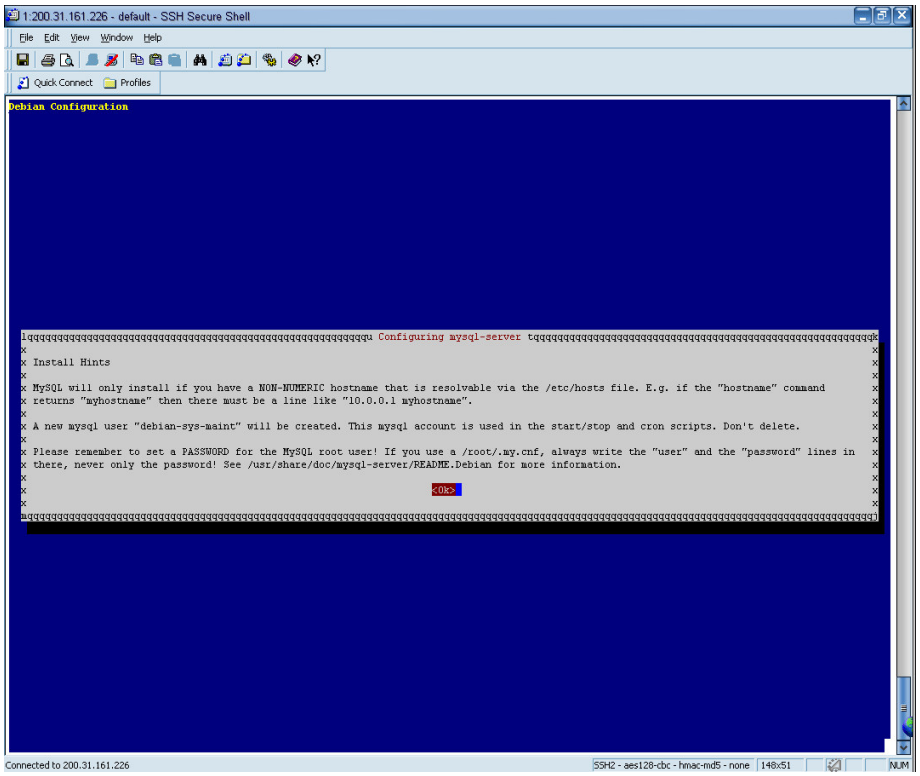
* En la instalación de mysql-server se instalaran los siguientes paquetes:

a. libdbd-mysql-perl
b. libdbi-perl
c. libmysqlclient12
d. libnet-daemon-perl
e. libplrpc-perl
f. mysql-client
g. mysql-common

Se sugiere instalara los siguientes:

a. dbishell
b. libcompress-zlib-perl
c. mysql-doc

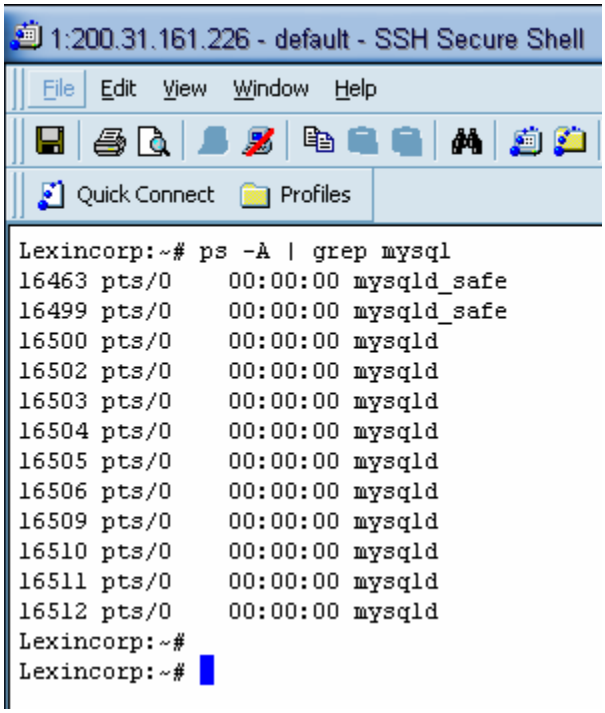
Paso 2: Aparecerá una pantalla a la que daremos OK, esta realizará las configuraciones necesarias para que mysql-server se ejecute.



Paso 3: Revisar si esta corriendo Mysql-Server

ps –A | grep mysql

Aparecerá si la configuración fue exitosa lo siguiente:

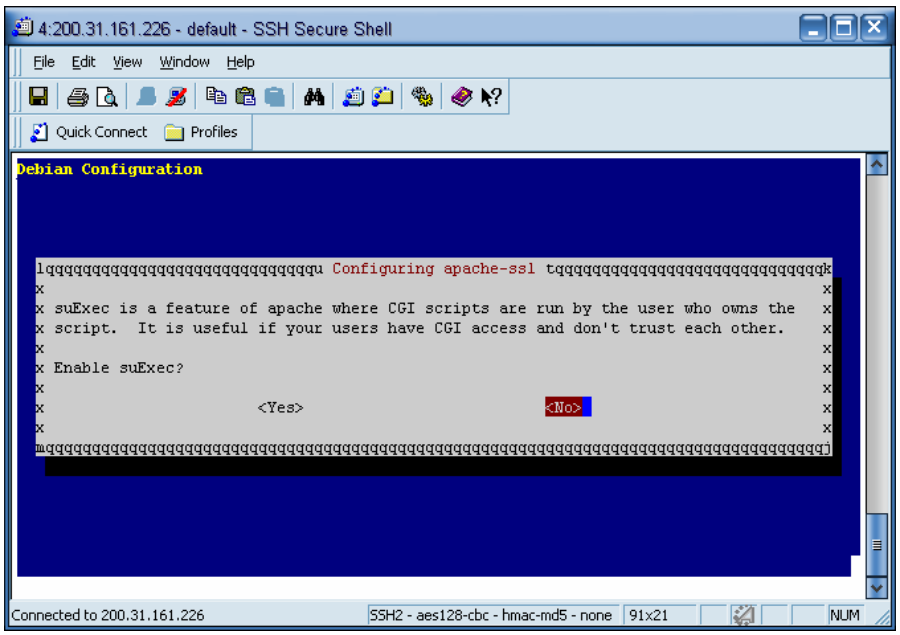


1.3.3. INSTALACION Y CONFIGURACION DE APACHE-SSL

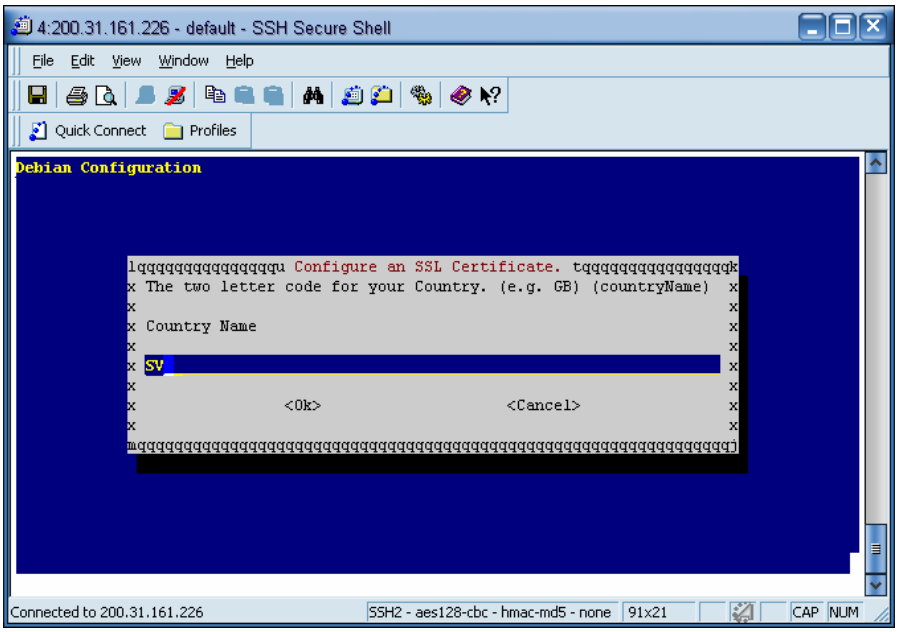
INSTALACION:

Paso 1: Se ejecuta el siguiente comando
apt-get install apache-ssl

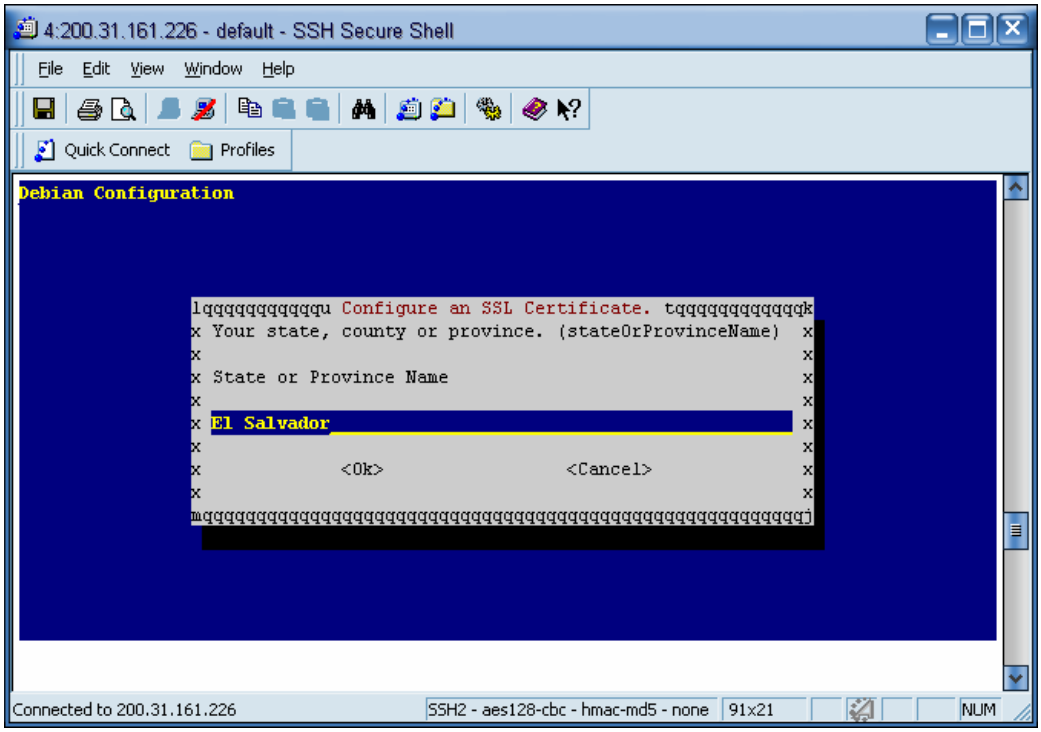
CONFIGURACION:



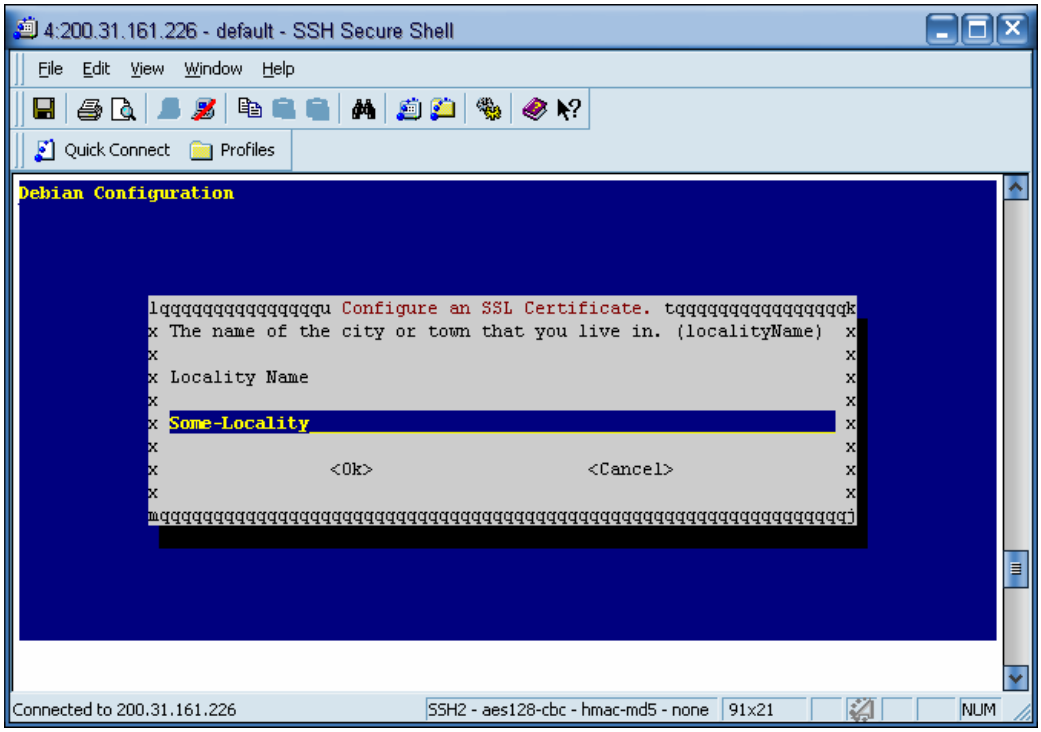
Paso 2: Dar clic en No ya no utilizaremos esa opción



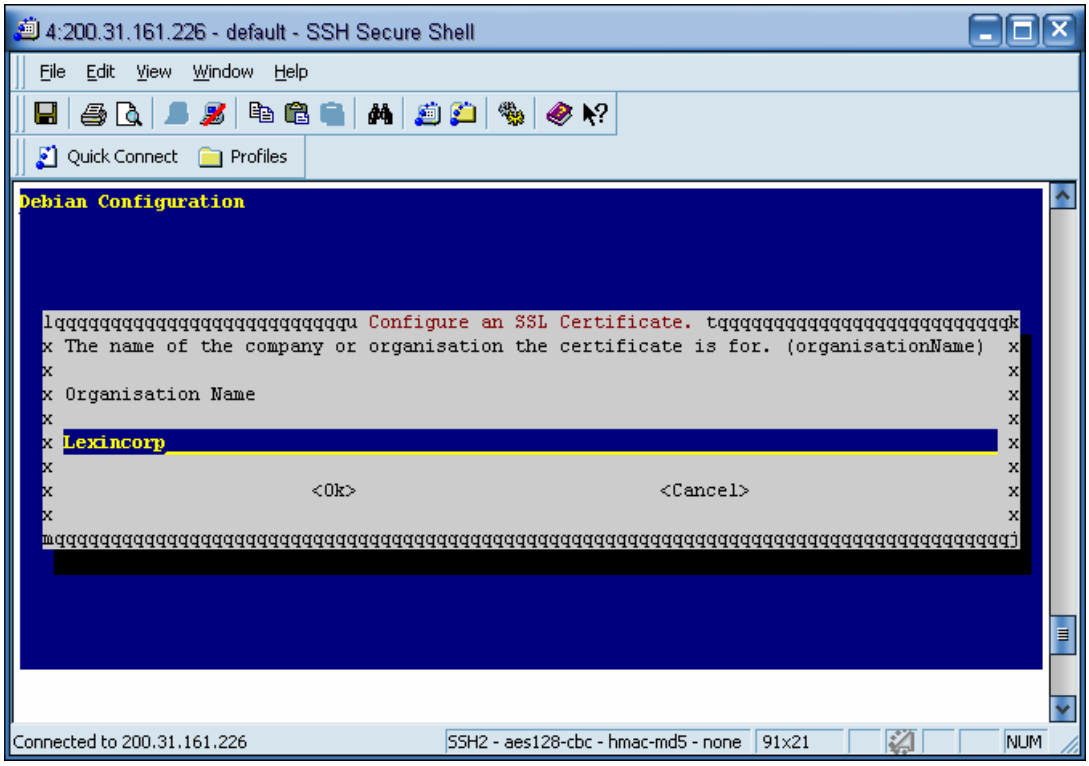
Paso 3: En Country Name escribiremos: SV



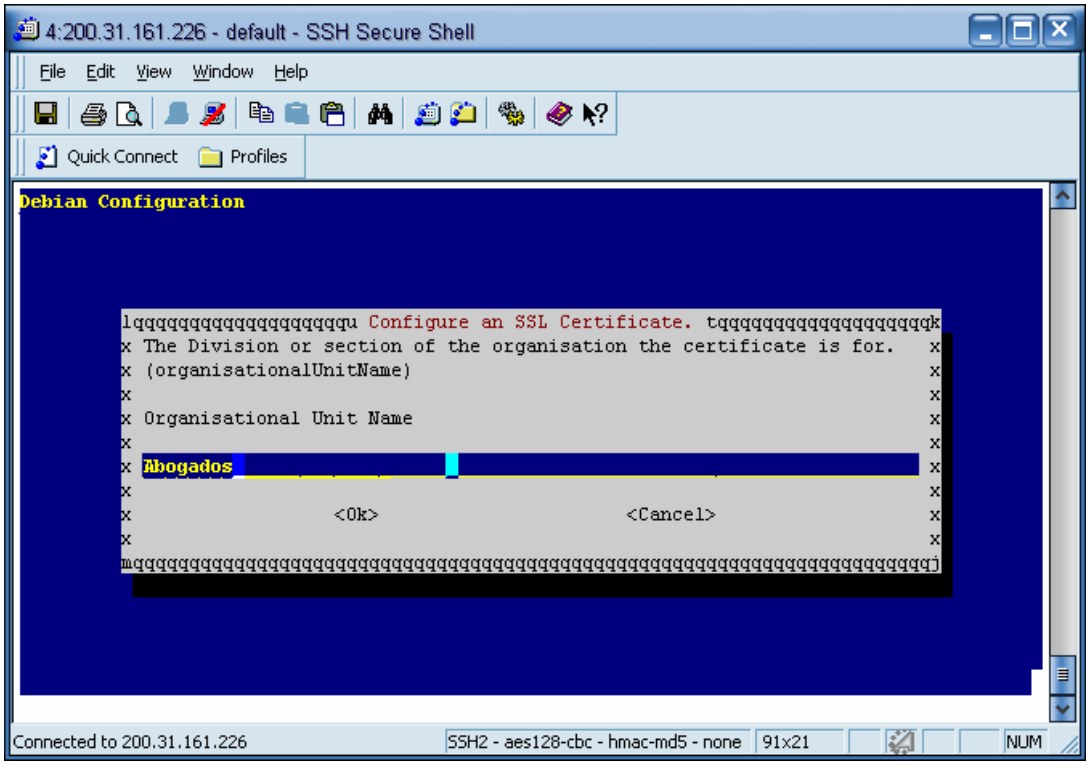
Paso 4: En State o Province escribiremos: El Salvador



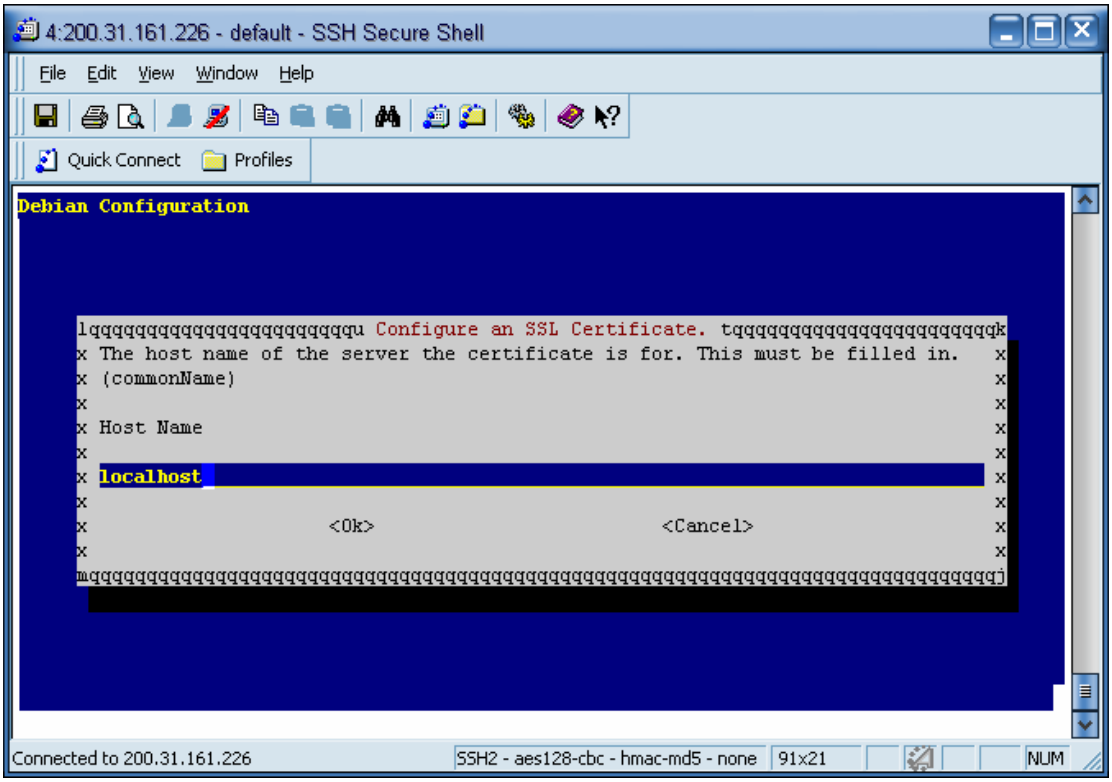
Paso 5: En Locality Name escribiremos: San Salvador



Paso 6: En Organiation Name escribiremos: Lexincorp.



Paso 7: En Organisational Unit Name escribiremos: Abogados.

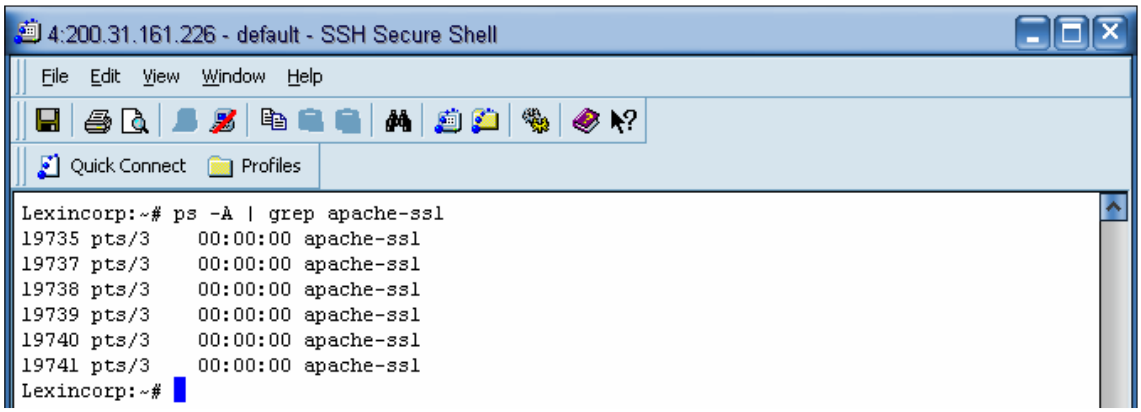


Paso 8: Nombre del Host Name: localhost

Paso 9: Para finalizar con la configuración ejecutar el siguiente comando:

ps –A | grep apache-ssl

Si la instalación fue buena nos aparecerá lo siguiente:



1.3.4. CONFIGURACIÓN DE FIREWALL

Para proteger los servicios que hemos instalado ocuparemos iptables, se crearan reglas las cuales nos permitiran bloquear o restringir el acceso a todas aquellas redes que nosotros nos queremos que tengan acceso.

Para esto se creará un script llamado S99rules el cual será colocado en la carpeta /etc/rc2.d con los permisos necesarios de lectura y escritura para que cada vez que arranque el sistema operativo se ejecute y carge así las reglas que se pondrán.

Los servicios que se protegerán son los siguientes: FTP, SSH, SAMBA, SQUID, MYSQL. Estos servicios se ocuparan por el momento solo por la red interna por lo cual se bloqueara el acceso a la red externa, así:

Script “S99rules”:

#Bloqueo a FTP

#Acceso a FTP por la red Interna

/sbin/iptables -A INPUT -p TCP -d localhost --dport 21 -j ACCEPT

/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 21 -j ACCEPT

#Bloqueo de FTP a todas las redes

/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 21 -j DROP

#Bloqueo a SSH

#Acceso a SSH por la red Interna

/sbin/iptables -A INPUT -p TCP -d localhost --dport 22 -j ACCEPT

```
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 22 -j ACCEPT
#Bloqueo de SSH a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 22 -j DROP

#Bloqueo a Samba
#Acceso a Samba por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 445 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 445 -j ACCEPT
#Bloqueo de Samba a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 445 -j DROP

#Bloqueo a SQUID
#Acceso a SQUID por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 3128 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 3128 -j ACCEPT

#Bloqueo de SQUID a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 3128 -j DROP

#Bloqueo a MYSQL
#Acceso a MYSQL por la red Interna
/sbin/iptables -A INPUT -p TCP -d localhost --dport 3306 -j ACCEPT
/sbin/iptables -A INPUT -p TCP -d 192.168.182.0/24 --dport 3306 -j ACCEPT

#Bloqueo de MYSQL a todas las redes
/sbin/iptables -A INPUT -p TCP -d 0.0.0.0/0 --dport 3306 -j DROP
```

1.4. MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE DE CONTABILIDAD DE ACCESOS – DIALUP ADMIN

INSTALACION

Paso 1: entrar al directorio:
cd freeradius-1.1.1

Paso 2: copiar directorio dialup_admin al directorio de publicación del Apache:
cp –fr dialup_admin /var/www

Paso 3: Una ves copiado entrar al directorio de publicación del Apache y renombrar el directorio a freeradius.
cd /var/www
mv dialup_admin freeradius

Paso 4: entrar al directorio freeradius.
cd freeradius

CONFIGURACION

Paso 1: entrar al directorio conf y editar el archivo con tu editor preferido admin.conf.
cd conf
nano admin.conf

Paso 2: configuración de directorios.

a. Buscar opción general_base_dir y colocar el directorio donde copiastes el dialup_admin, este hará referencias a los archivos de configuración en sus diferentes directorios:
   general_base_dir: /var/www/freeradius

b. Buscar opción general_radiusd_base_dir y colocar el directorio donde fue instalado freeradius, esta buscará los archivos de configuración:
   general_radiusd_base_dir: /usr/local/etc/raddb

Paso 3: Habilitar modo debug para sql, si quieres que el programa tenga un debug para sql deja habilitada la opción sql_debug de lo contrario coméntala:
sql_debug: trae

Paso 4: conexión a la base de datos, modifica los valores siguientes según tus configuraciones:
sql_type: mysql
sql_server: localhost
sql_port: 3306
sql_username: apache #usuario con permisos de conexión
sql_password: groupoffice
sql_database: freeradius #Base de datos.

Paso 5: Como el programa dialup_admin esta hecho con extensiones de php3 modificaremos el archivo de configuración del Apache ubicado en /etc/apache2 y buscaremos la opción “AddType application” y agregaremos la extensión:

nano /etc/apache2/apache2.conf

Agregar la extensión .php3 al final de AddType application
AddType application/x-httpd-php .php .php3
AddType application/x-httpd-php-source .phps

Paso 6: abrir un navegador y colocar, este nos mostrará el programa con el cual vamos a crear y administrar a los usuarios que sean registrado en la base de datos, también este nos dará reportes detallados de logeos, horas de inicio y finalización, etc.
http://200.31.161.226/freeradius/htdocs/

1.5. MANUAL DE INSTALACION Y CONFIGURACIÓN DE SOFTWARE GPL – INTRANET

INSTALACION

Dependencias:

1. apt-get install php4-mysql
2. apt-get install libapache2-mod-php4
3. apt-get install php4-imap

Paso 1: Bajar programa del sitio http://prdownloads.sourceforge.net/group-office/
wget http://prdownloads.sourceforge.net/group-office/groupoffice-com-2.15.tar.gz?use_mirror=optusnet

Paso 2: descomprimir el archivo:
tar -xzvf groupoffice-com-2.15.tar.gz

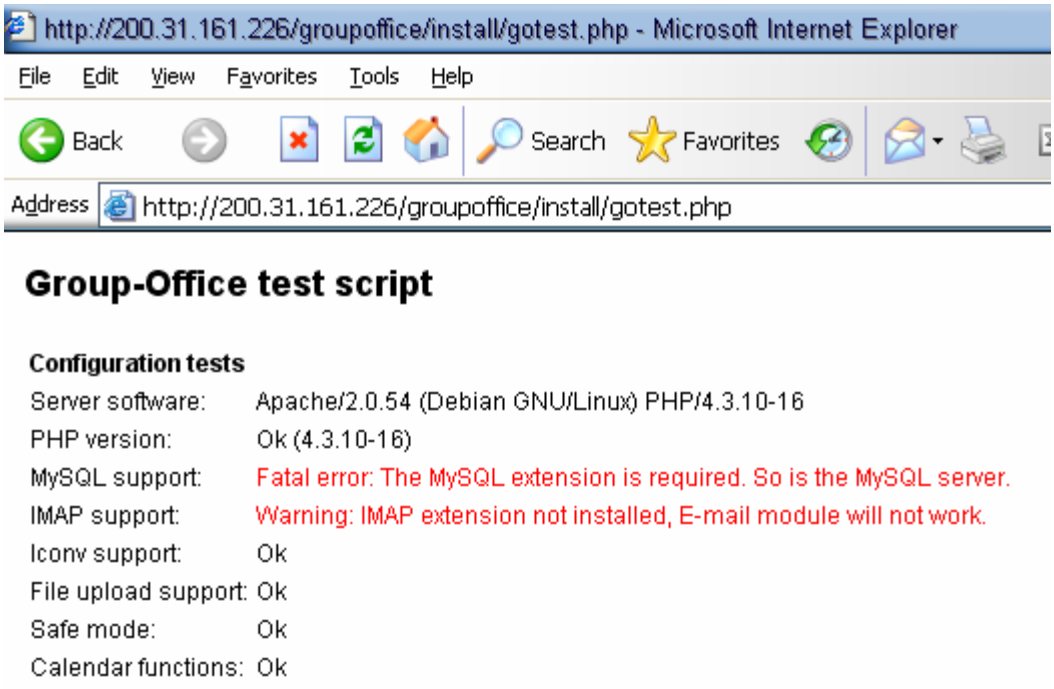
Paso 3: Renombrar el directorio a groupoffice
mv groupoffice-com-2.15 groupoffice

Paso 4: Copiar el directorio groupoffice al directorio de publicación del Apache.
cp -fr groupoffice /var/www

CONFIGURACION

Paso 1: entrar a la siguiente dirección para realizar un test para revisar lo que necesitamos para la instalación

http://200.31.161.226/groupoffice/install/gotest.php



El test nos da un reporte el cual nos indica de color rojo que nos hacen falta esos paquetes para la instalación.

Paso 2: Instalación de paquetes.

a. Instalación de php4-imap

apt-get install php4-imap

Se instalaran adicionalmente los siguientes paquetes:

1. libc-client2002edebian
2. mlock

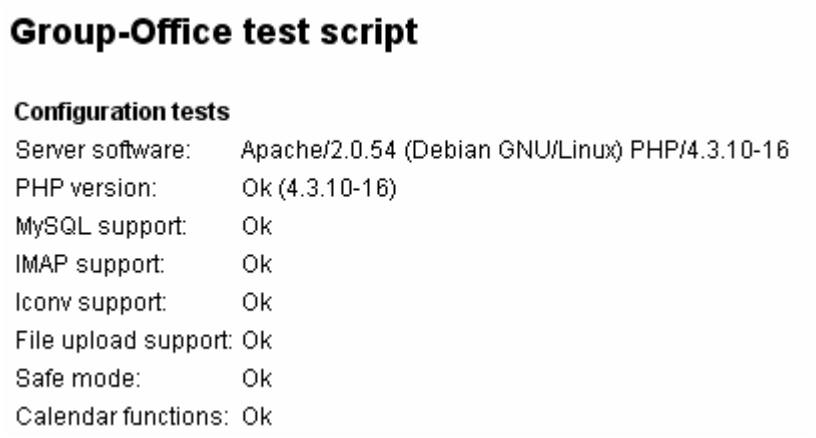
b. instalación de php4-mysql

apt-get install php4-mysql

Paso 3: Reiniciar el servidor Web, en este caso utilizaremos Apache2

/etc/init.d/apache2 restart

Paso 4: Revisar el test nuevamente:



Group-Office test script

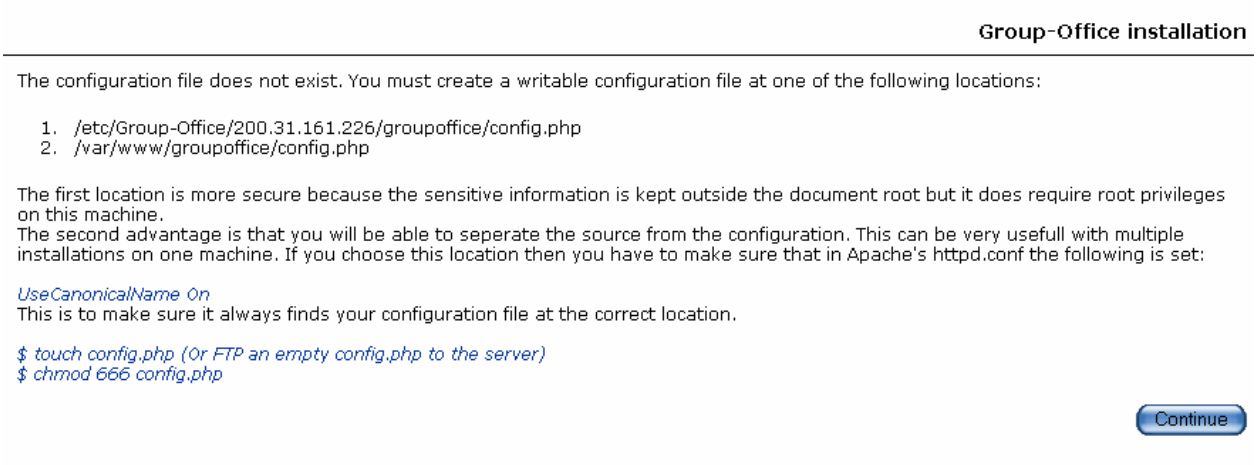
Configuration tests

Server software:	Apache/2.0.54 (Debian GNU/Linux) PHP/4.3.10-16
PHP version:	Ok (4.3.10-16)
MySQL support:	Ok
IMAP support:	Ok
Iconv support:	Ok
File upload support:	Ok
Safe mode:	Ok
Calendar functions:	Ok

Todos los paquetes que nos piden están instalados.

Paso 5: entrar a la dirección de instalación, esta ejecutará un script el cual nos guíara paso a paso en la configuración.

http://200.31.161.226/groupoffice/install/install.php



Group-Office installation

The configuration file does not exist. You must create a writable configuration file at one of the following locations:

1. /etc/Group-Office/200.31.161.226/groupoffice/config.php
2. /var/www/groupoffice/config.php

The first location is more secure because the sensitive information is kept outside the document root but it does require root privileges on this machine.
The second advantage is that you will be able to seperate the source from the configuration. This can be very usefull with multiple installations on one machine. If you choose this location then you have to make sure that in Apache's httpd.conf the following is set:

UseCanonicalName On
This is to make sure it always finds your configuration file at the correct location.

$ touch config.php (Or FTP an empty config.php to the server)
$ chmod 666 config.php

Continue

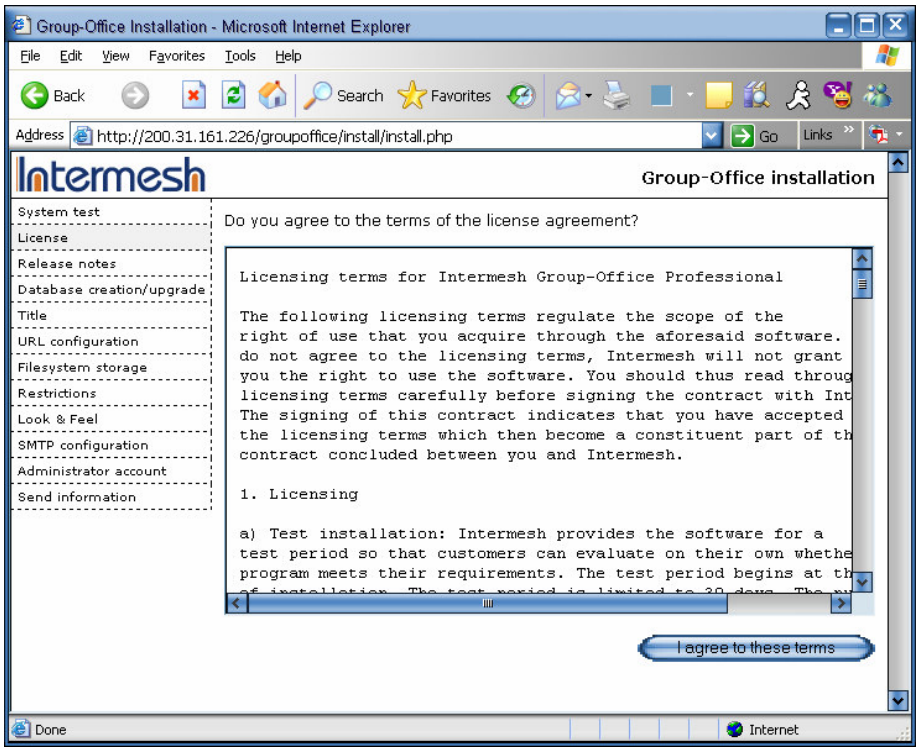
Paso 6: desde una ventana de comandos crear el archivo de configuración “config.php” y dar permisos de escritura y lectura, para esto nos colocaremos en el directorio de Group Office /var/www/groupoffice

touch config.php

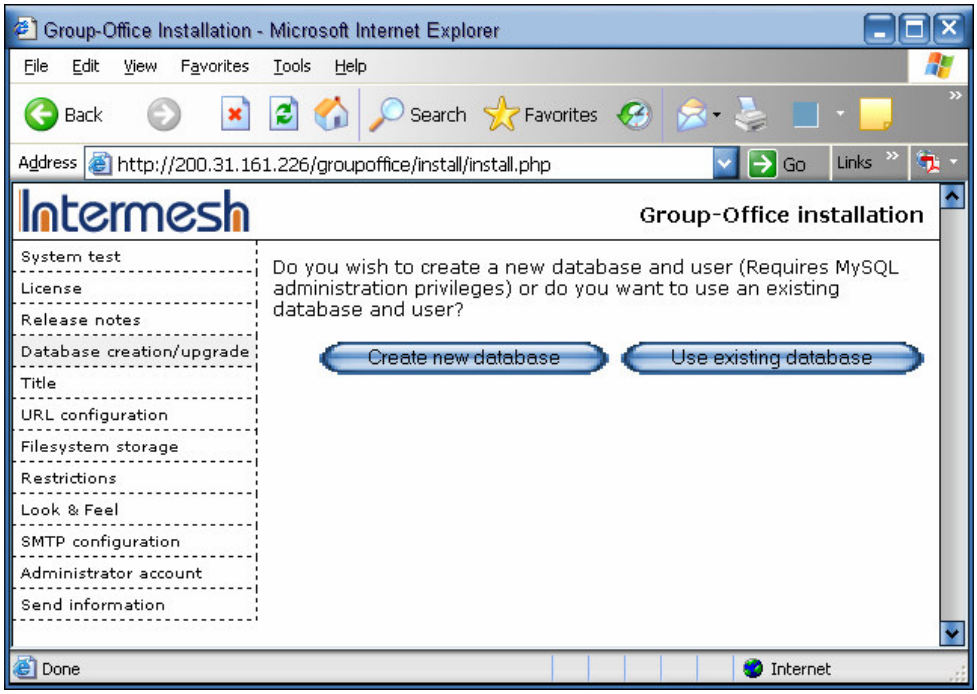
chmod 666 config.php

Paso 7: Después de haber creado el archivo volvemos a la página web y daremos clic en continue.

Paso 8: Dar clic en “I Agree to these terms”



Paso 9: Creación de la base de datos, esta nos servirá para guardar los usuarios que tendrán acceso a la Intranet y también para guardar perfiles, etc. Clic en Create new database.



Paso 10: Introducir el usuario que tendrá el control de sistema, el nombre de la base de datos, servidor, usuario y password para la base de datos.

Host: localhost

User Name: apache

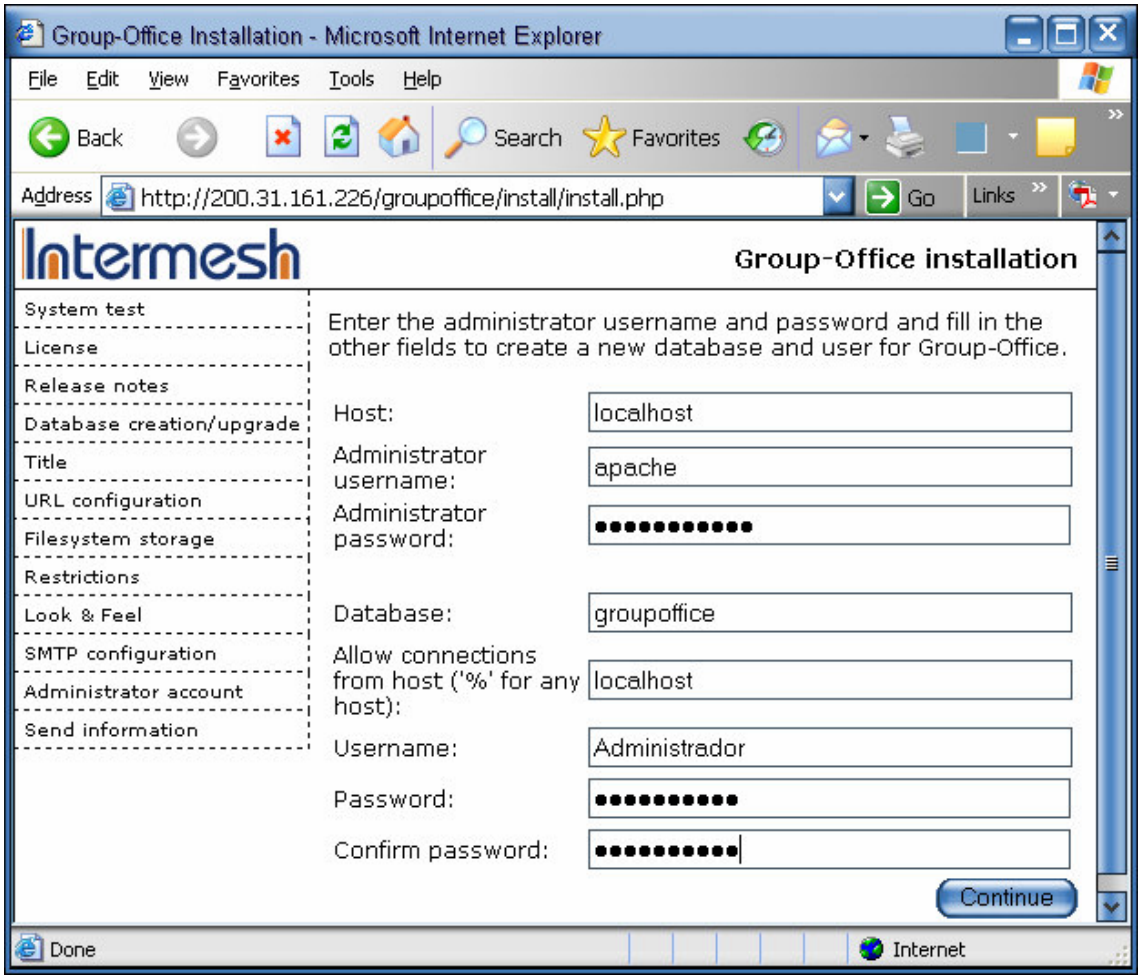
Password: groupoffice

Nombre de Base de datos: groupoffice

Servidor: localhost

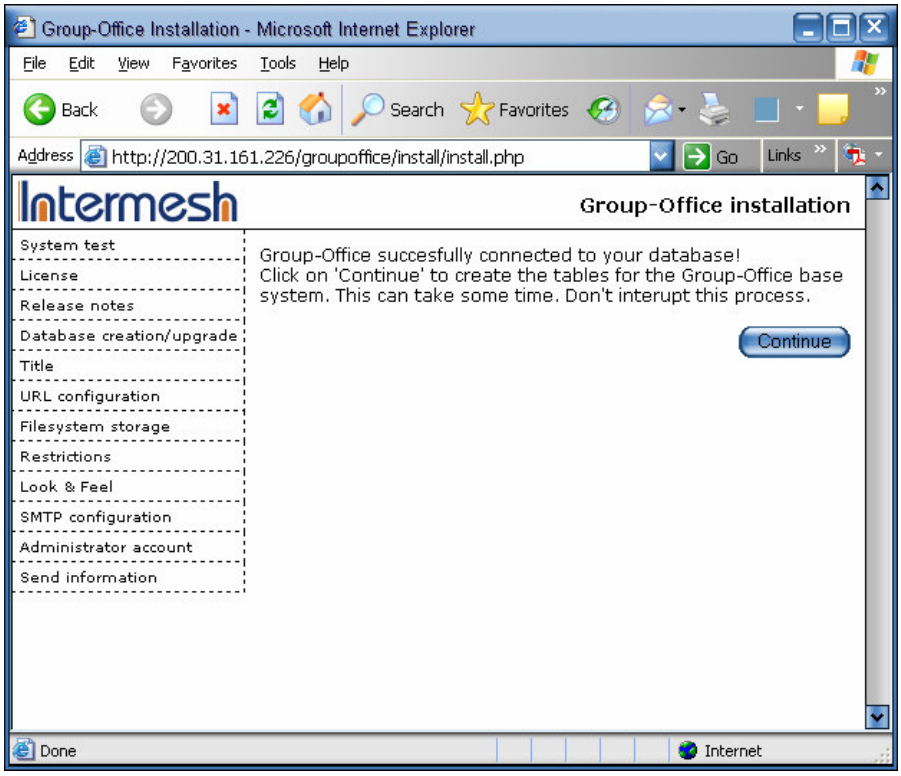
Usuario: Administrador

Password: lexincorp7

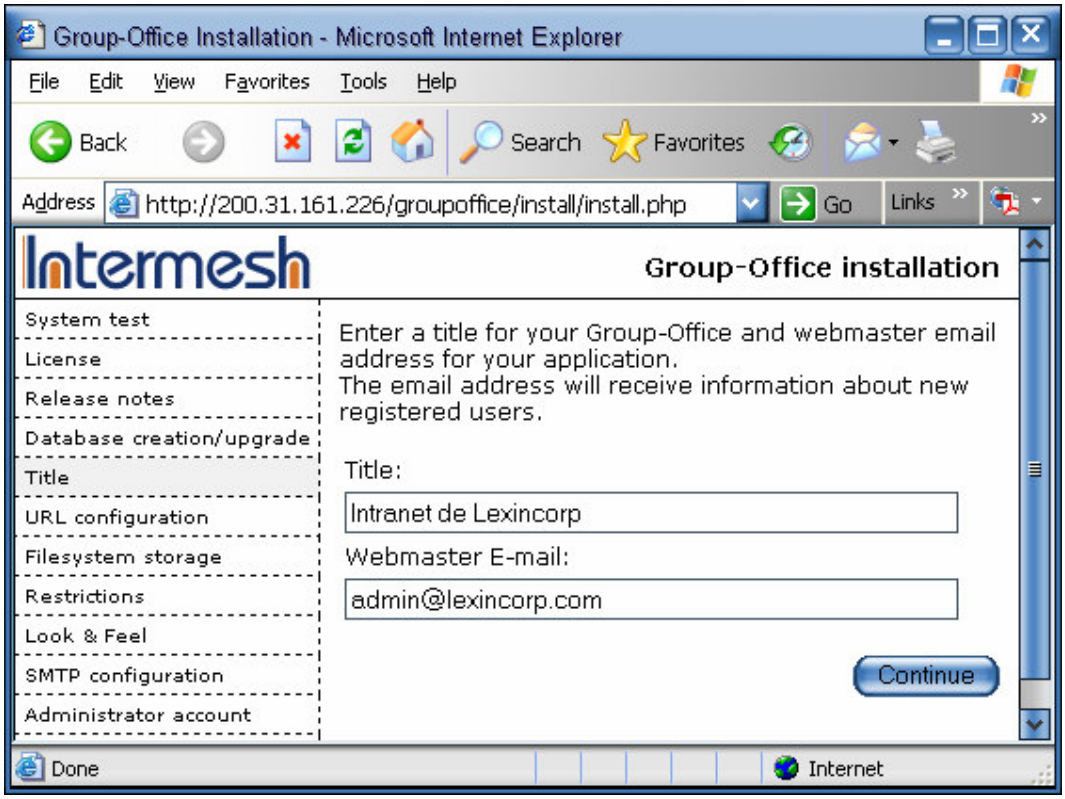


Paso 11: Dar clic en Continue

Paso 12: Nos lanzara un mensaje al cual le daremos Continue, este creara las tablas para la base de datos de Group Office.

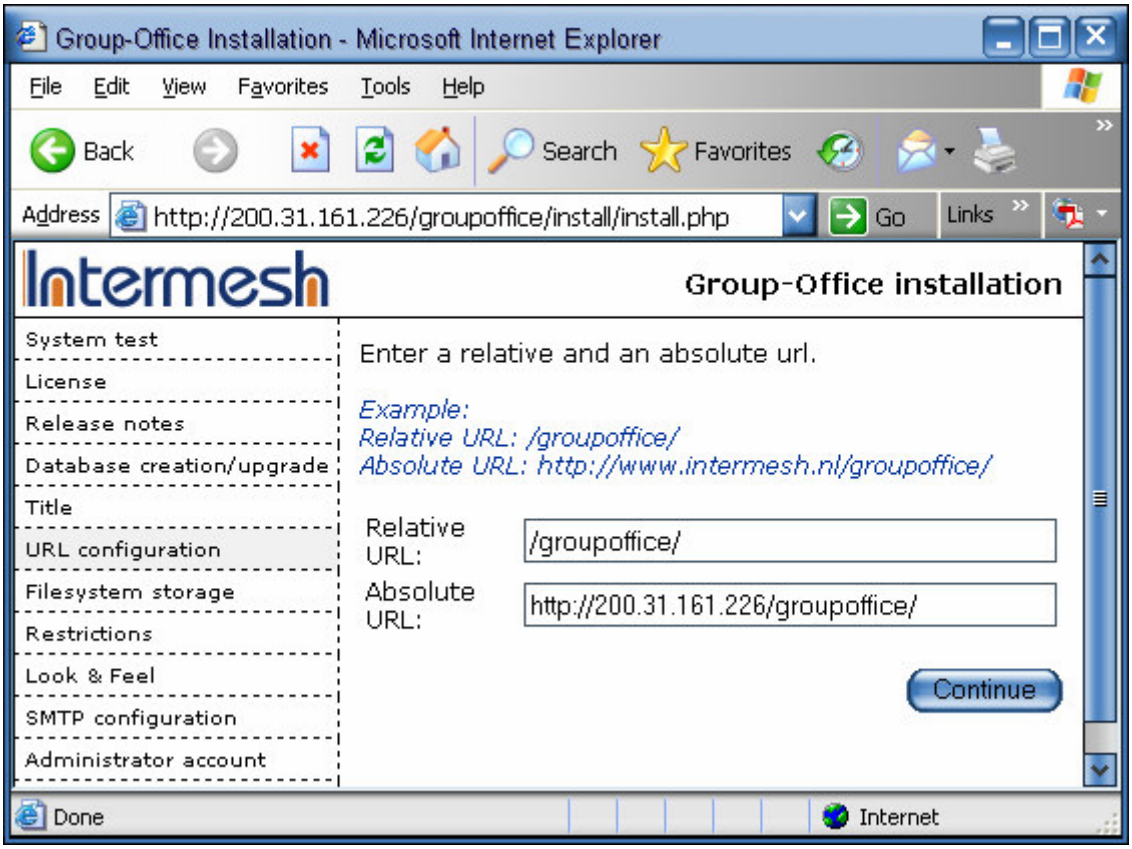


Paso 13: Creación de titulo a la cual le pondremos “Intranet de Lexincorp”

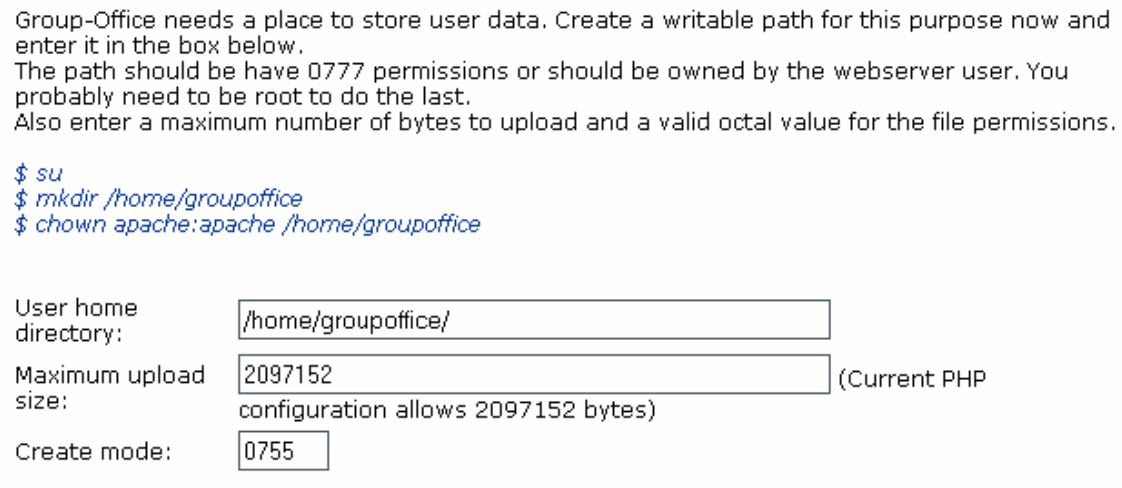


Paso 14: Clic en Continue →

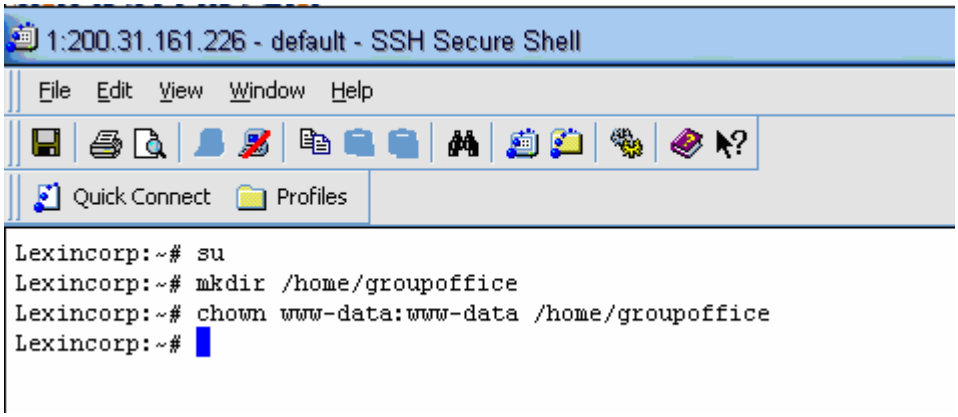
Paso 15: Configuración de URL de acceso a la Intranet. En la cual le pondremos según la figura mostrada. Clic en Continue.



Paso 16: Configuración de directorios, para esto ocuparemos un cliente de Secure Shell para tener acceso al servidor y seguiremos las instrucciones mostradas.

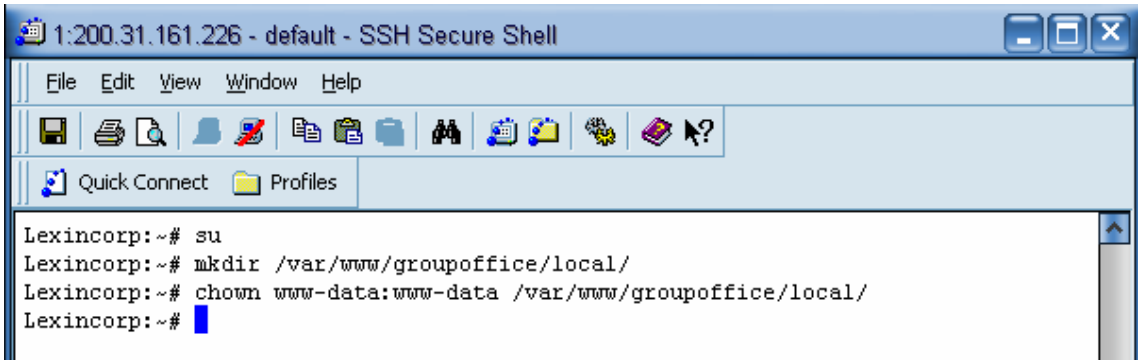


Paso 17: En nuestro caso ocuparemos el usuario www-data en lugar de Apache así:



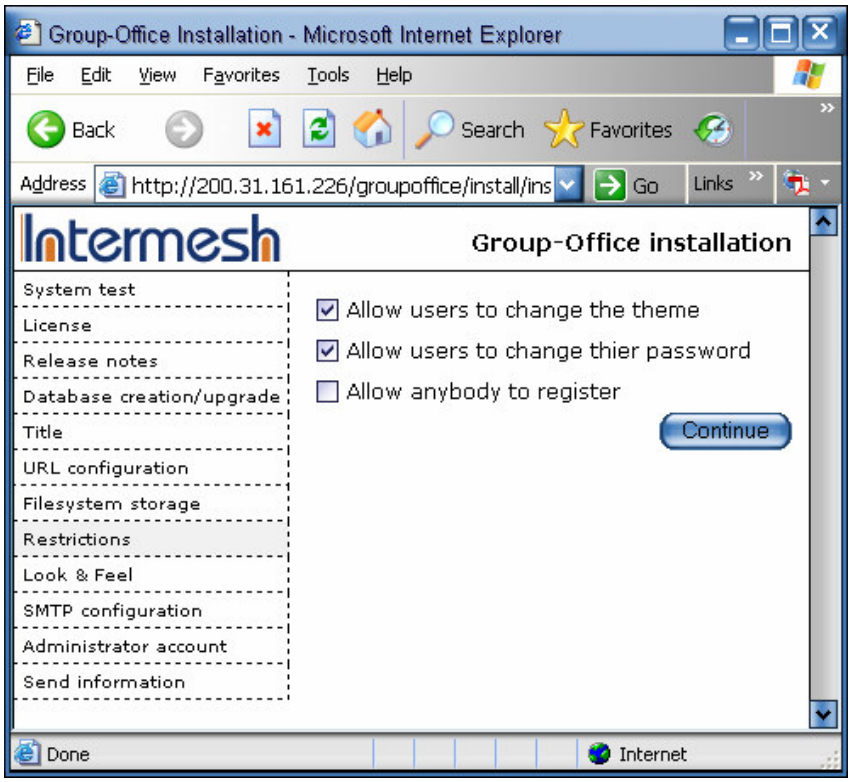
Paso 18: Además de esa configuración realizaremos otra según las instrucciones mostradas, por lo cual ocuparemos el mismo cliente de Secure Shell:

Paso 19: En nuestro caso ocuparemos el usuario www-data en lugar de apache así



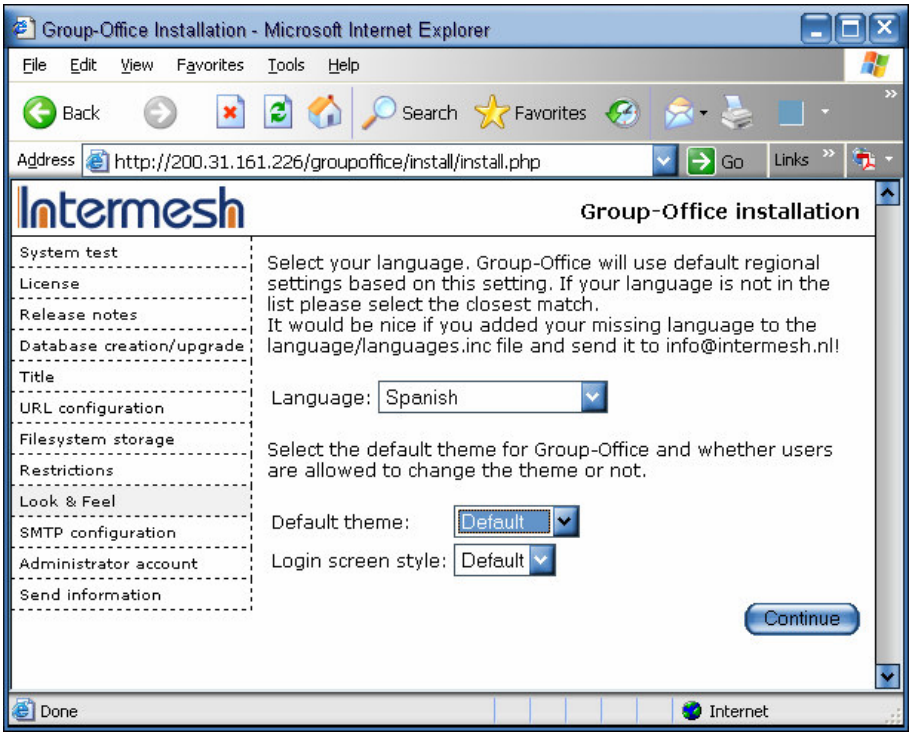
Paso 20: Clic en Continue.

Paso 21: Crear Permisos a usuario:

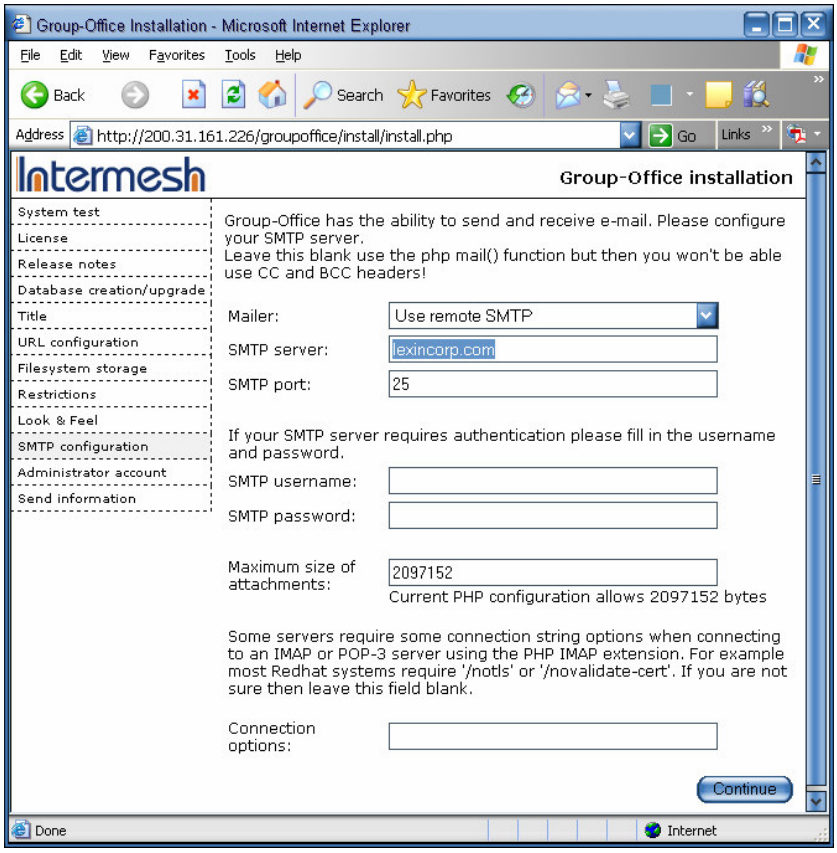


Acá permitiremos a los usuarios cambiar de tema y password. No permitiremos que cualquiera se pueda registrar.

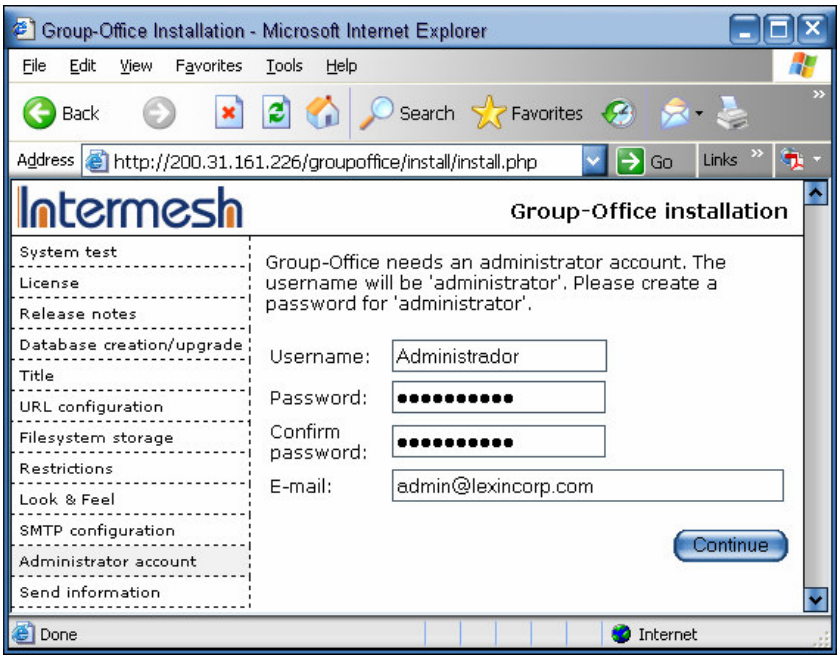
Paso 22: Idioma o Visualizaciones: Elegiremos Español como idioma y los demás en Default.



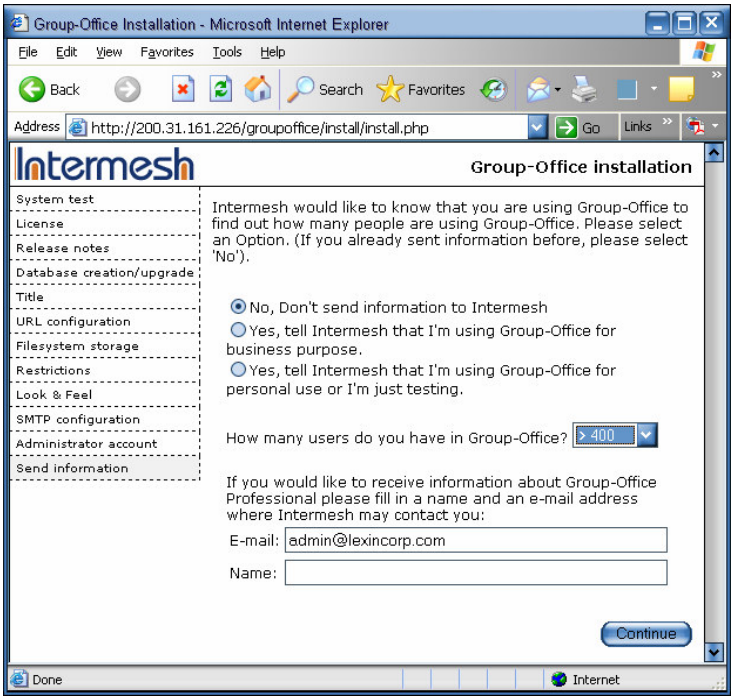
Paso 23: Configuración de SMTP. En nuestro caso utilizaremos un SMTP Remoto, el SMTP Server será lexincorp.com y el puerto que por default es el 25, lo demás queda igual.



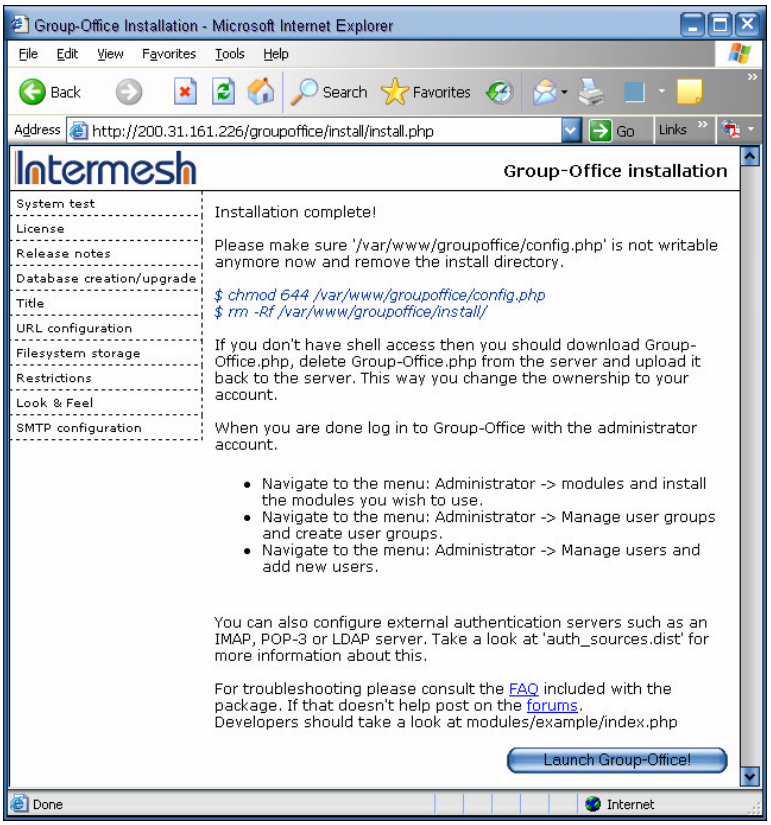
Paso 24: Creación de cuenta de administrador



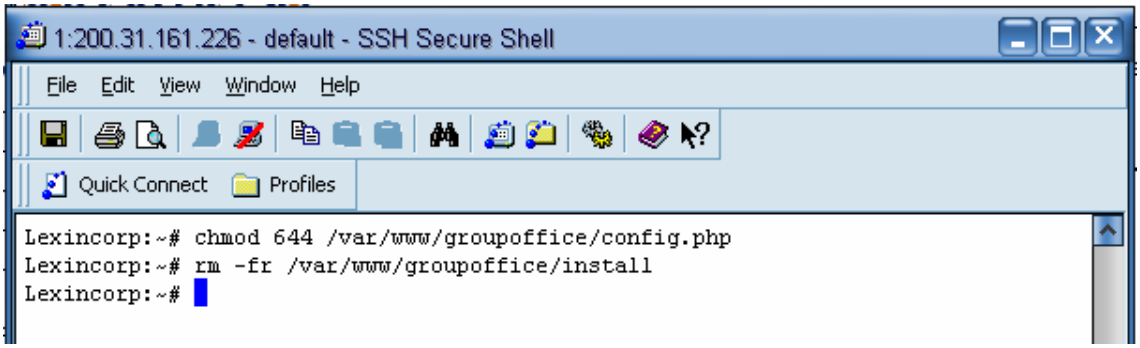
Paso 25: Mandar Información. Acá en esta ventana elegiremos que no nos mande información del producto y le pondremos la máxima cantidad de usuarios que utilizaran la aplicación en este caso más de 400. Clic en Continue.



Paso 26: Completar instalación.

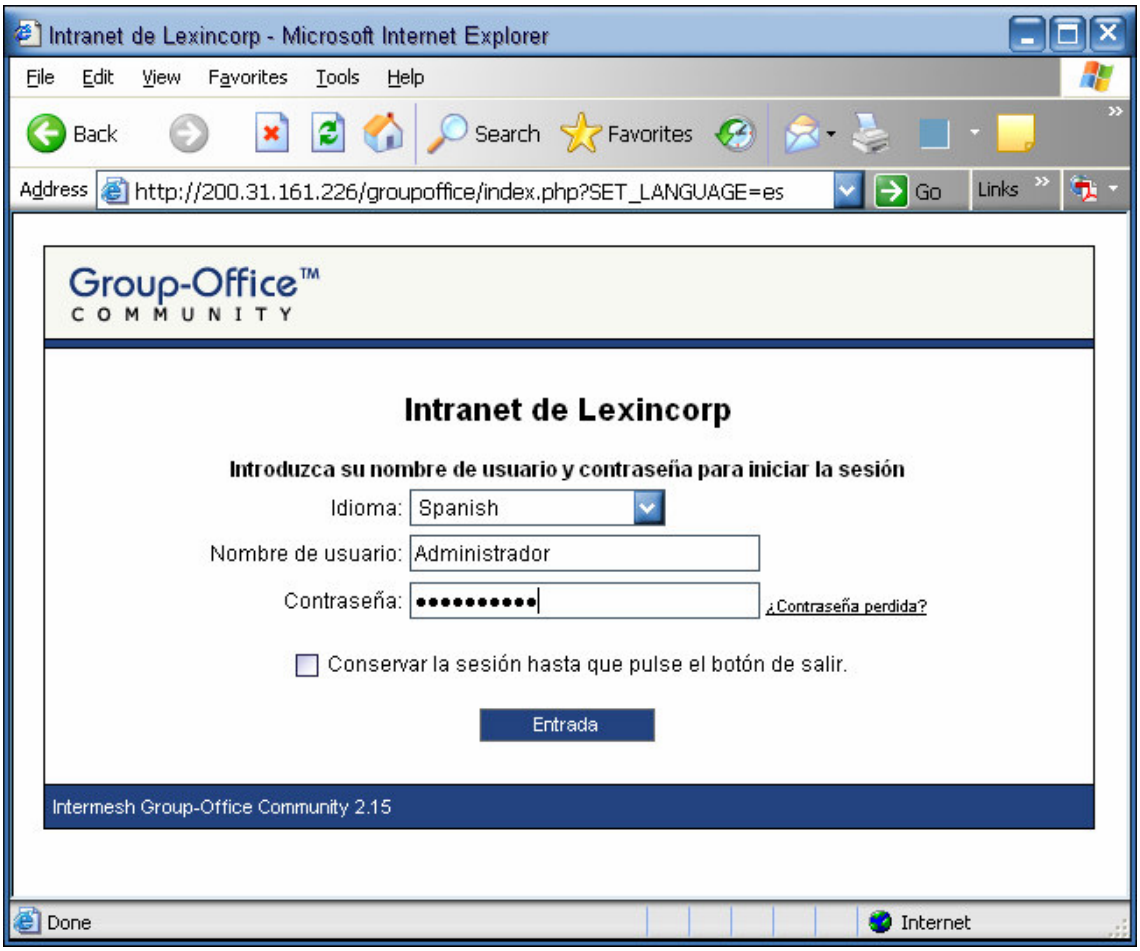


Paso 27: Nuevamente utilizaremos un cliente de Secure Shell y seguiremos las instrucciones mostradas en azul. Aquí cambiamos los permisos del archivo “config.php” y eliminamos la carpeta install. Clic en “Launch Group-Office”.



Paso 28: Acceso a Intranet con cuenta administrativa.

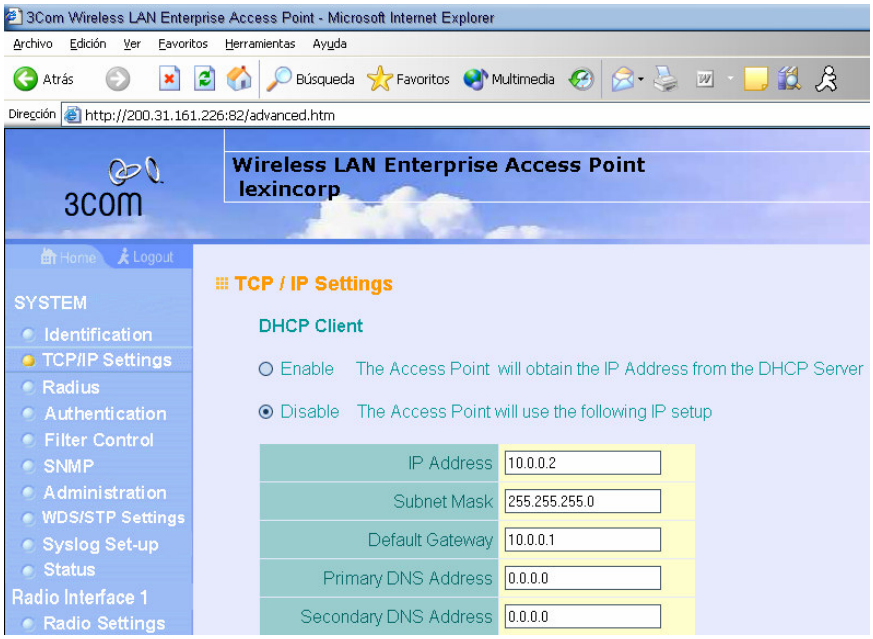
Link: http://200.31.161.226/groupoffice/



1.6. MANUAL DE CONFIGURACION DE ACCESS POINT 3COM 7250

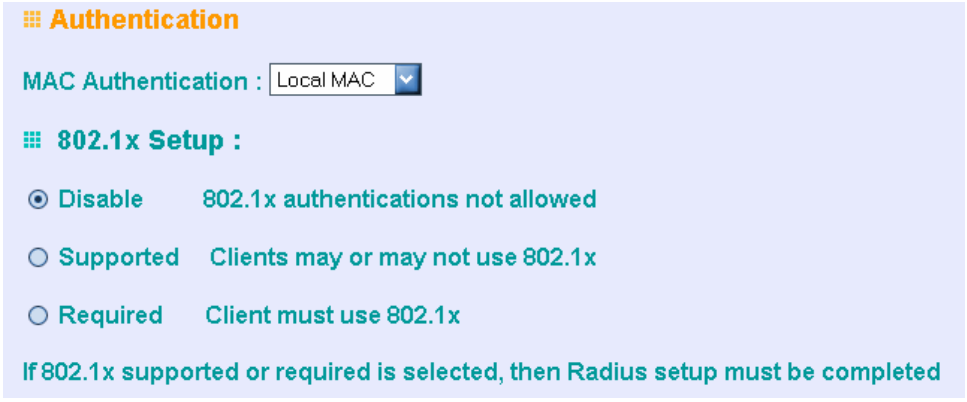
Paso 1: IDENTIFICACIÓN: sirve para identificar el dispositivo únicamente. El nombre de nuestro AP (Access Point) será "Lexincorp". Los cambios son reflejados hasta que aplicas los cambios y se actualice el navegador.

Paso 2: Configuración TCP/IP: en la configuración del TCP / IP se colocará la IP con la cual se conectara al servidor, esta será del rango 10.0.0.0 / 24 la cual es de la red interna del servidor. La IP que se le pondrá al AP es fija:

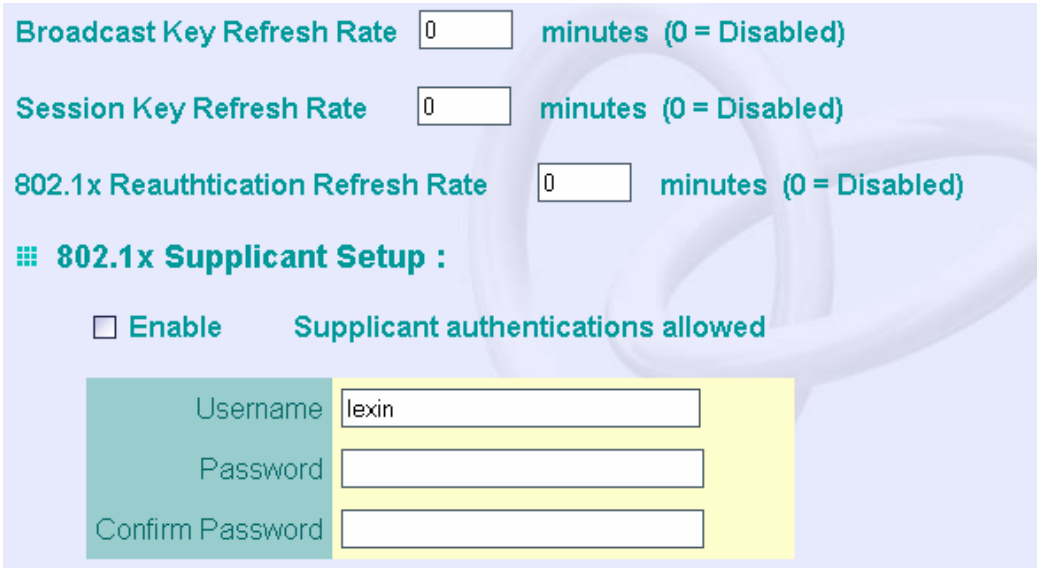


Paso 3: Radius: No se tocará la configuración en este apartado ya que se utilizara freeradius en el servidor y no se ocupara el del AP.

Paso 4: Autenticación: las opciones de autenticación de esta parte son dos, por medio de direcciones MAC y por medio del protocolo 802.1x. Nos enfocaremos en la autenticación por medio de direcciones físicas MAC ya que el protocolo 802.1x no es compatible con la mayoría de los sistemas operativos, y trae problemas al momento de la implementación. Se deshabilitara el 802.1x y quedara habilitada la autenticación por medio de direcciones MAC, así:



Paso 5: No se utilizara una llave por lo cual quedará también deshabilitado.



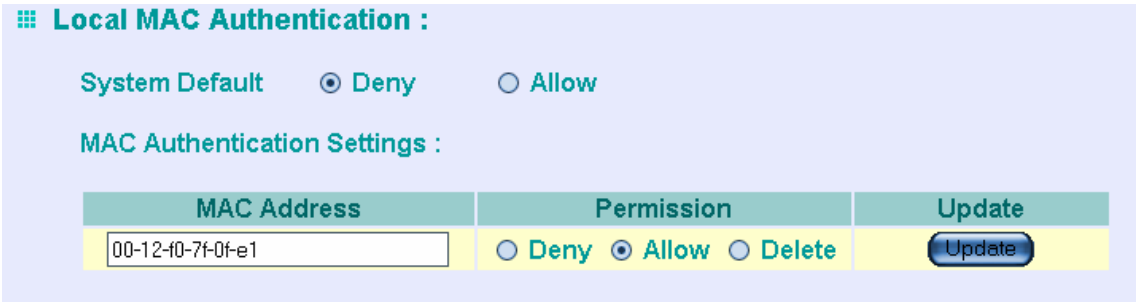
Paso 6: Se levantará un inventario de las computadoras que tengan tarjetas de red inalámbricas las cuales tendrán acceso al AP, luego se introducirán a la tabla del de computadoras permitidas, únicamente aquellas PC que estén en esta tabla podrán conectarse al AP. El valor por defecto del AP es negar cualquiera maquina.

TABLA DE DIRECCIONES MAC PERMITIDAS EN LEXINCORP

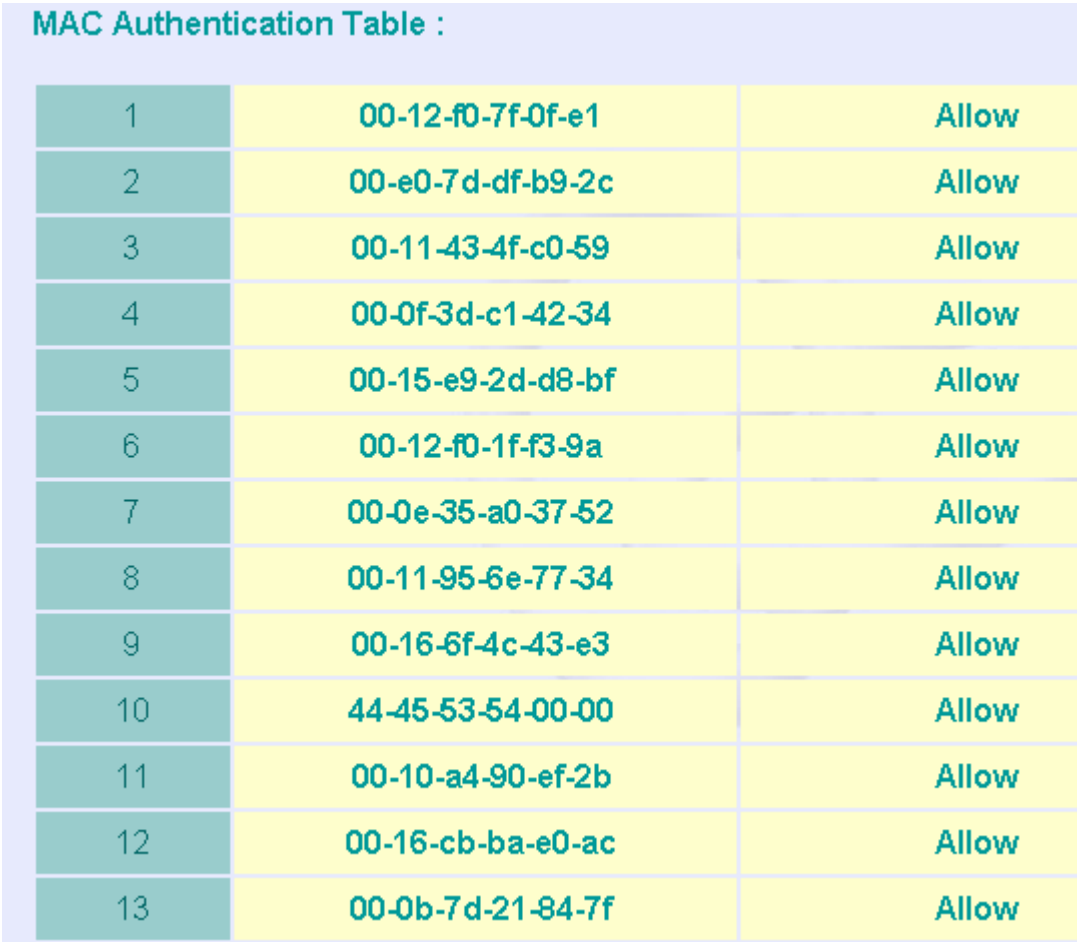
No.	Dirección Fisica MAC	Estado
1	00-12-f0-7f-0f-e1	Allow
2	00-e0-7d-df-b9-2c	Allow
3	00-11-43-4f-c0-59	Allow
4	00-0f-3d-c1-42-34	Allow
5	00-15-e9-2d-d8-bf	Allow
6	00-12-f0-1f-f3-9a	Allow
7	00-0e-35-a0-37-52	Allow
8	00-11-95-6e-77-34	Allow
9	00-16-6f-4c-43-e3	Allow
10	44-45-53-54-00-00	Allow
11	00-10-a4-90-ef-2b	Allow
12	00-16-cb-ba-e0-ac	Allow
13	00-0b-7d-21-84-7f	Allow
14	00-16-6f-4b-09-1b	Allow
15	00-0c-f6-09-aa-09	Allow
16	00-16-cb-bf-94-87	Allow
17	00-16-6f-2c-6f-14	Allow

Paso 7: Las direcciones MAC se introducirán de la siguiente manera:

- Se digitara la dirección física en el cuadro donde dice MAC Address y se le dará la instrucción “Deny” o “Allow”, en este caso daremos Allow. Como se muestra en la siguiente figura, luego se dará clic en Update.



Una vez introducida las direcciones físicas quedara una tabla como se muestra en la siguiente figura:



MAC Authentication Table :

1	00-12-f0-7f-0f-e1	Allow
2	00-e0-7d-df-b9-2c	Allow
3	00-11-43-4f-c0-59	Allow
4	00-0f-3d-c1-42-34	Allow
5	00-15-e9-2d-d8-bf	Allow
6	00-12-f0-1f-f3-9a	Allow
7	00-0e-35-a0-37-52	Allow
8	00-11-95-6e-77-34	Allow
9	00-16-6f-4c-43-e3	Allow
10	44-45-53-54-00-00	Allow
11	00-10-a4-90-ef-2b	Allow
12	00-16-cb-ba-e0-ac	Allow
13	00-0b-7d-21-84-7f	Allow

Paso 8: Filter Control: Esta parte del AP no se tocara ya que no se utilizaran los filtros que aquí nos da, esta parte quedará con los valores por defecto.

Paso 9: SNMP (Simple Network Management Protocol): El Protocolo SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. No utilizaremos este protocolo por lo tanto esta parte quedará con los valores por defecto.

Paso 10: Administración: en esta sección se podrá cambiar el password del AP, así como otros servicios tales como:

- Configuración de Acceso a Telnet y SSH. Se dejara deshabilitado el telnet y se activara el SSH.
- Actualización del software del AP (Firmware) por medio de:
    i. FTP.
    ii. TFTP.

- Respaldo y Restauración de la configuración del AP.
- Resetear el Access Point.
- Restaurar los valores de Fábrica.

Paso 11: Configuración WDS/STP: en esta sección se configurara el AP como Access Point, así:

* El spanning Tree Protocol, es usado como puente (Bridge) entre Access point si se ponen en esa modalidad. En este caso quedará deshabilitado.

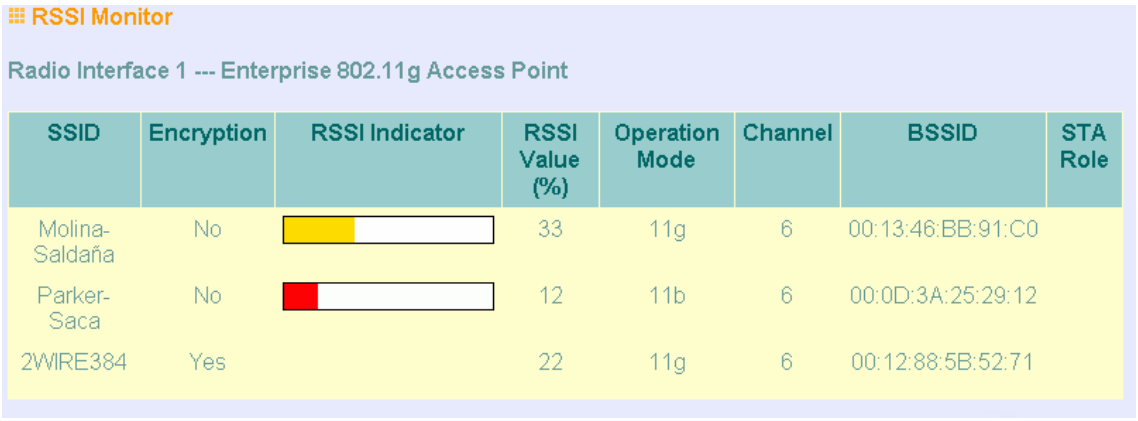
Paso 12: System Log: en esta sección se configurara lo siguiente:

- Habilitación de Log del sistema.
- Habilitación del SNTP (Simple Network Time Protocol)
- Configuración de la Hora del sistema

La configuración quedara de la siguiente manera:

Paso 13: Status del Access point: esta sección comprende de la siguiente información (No requiere Configuración):

- Estatus de las Estaciones: da un estatus de las estaciones conectadas.
- Log de los Eventos: da un reporte de las conexiones que ha sucedido como de las conexiones fallidas, etc.
- Monitor RSSI: escanea redes inalámbricas cerca del AP



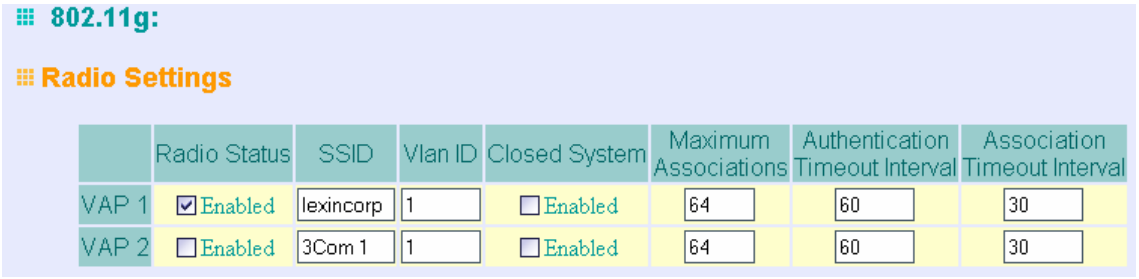
Paso 14: Radio Interfaces: esta se divide en:

- Configuraciones de Radio.
- Seguridad.

Estas quedarán configuradas de la siguiente manera:

Configuración de Radio:

a) Se habilitara el VAP1 el cual pertenece a red inalámbrica de Lexincorp



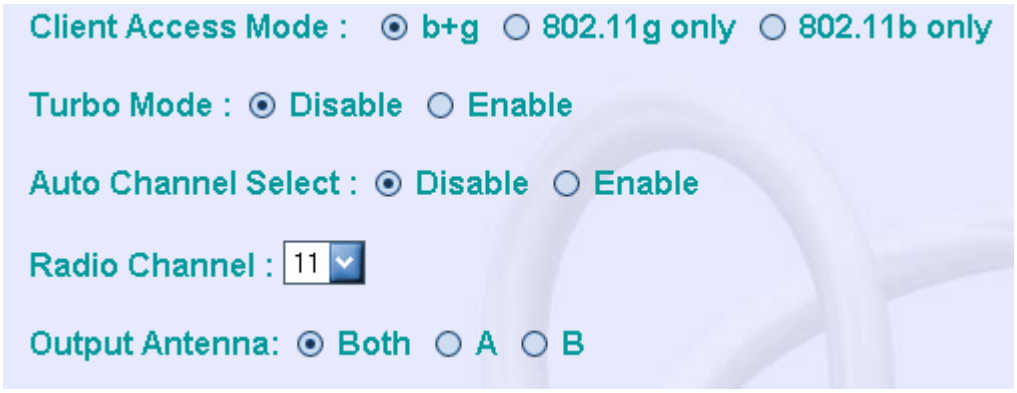
b) Se configurara el AP para que se puedan conectar a el los estándares 802.11 b y 802.11. g.

c) Se deshabilitara el Turbo Mode.

d) Se deshabilitara el Auto Channel Select.

e) Se elegirá el canal 11.

f) Y se utilizaran ambas antenas para transmitir la señal



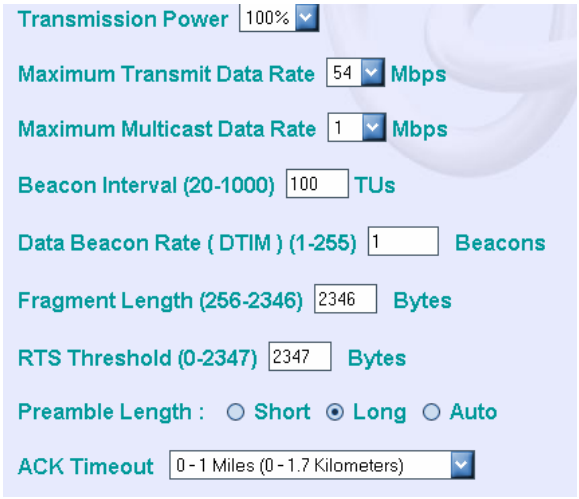
g) Se utilizara el 100% de poder de transmisión del AP.

h) Se utilizaran los valores por defecto de:

   a. Maximun Transmit Data Rate.
   b. Maximum Multicast Data Rate
   c. Beacon Interval (20-1000)
   d. Data Beacon Rate (DTIM) (1-255)
   e. Fragment Length (256-2346)
   f. RTS Threshold (0-2347)

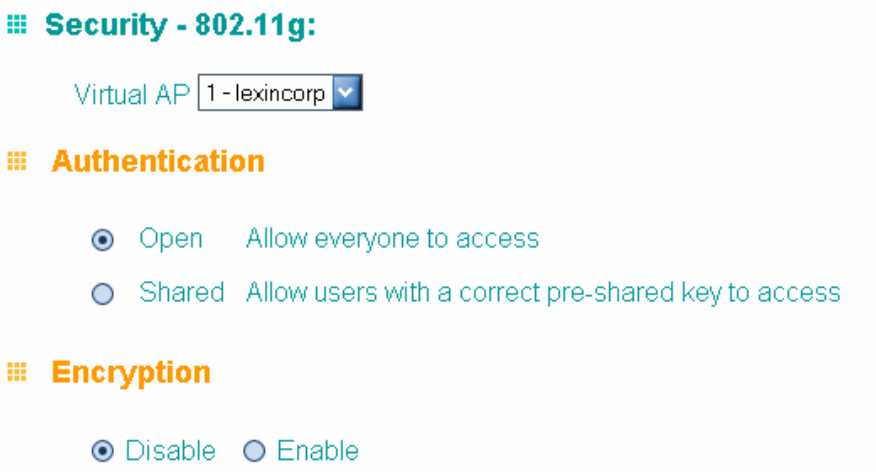
i) Se utilizara Preamble length en LONG.

j) El tiempo de espera ACK se utilizara de 0 a 1 Miles.



Seguridad:

En esta parte se utilizará los valores por defecto que el AP trae, así:



1.7. MANUAL DE INSTALACIÓN DEL SERVICIO PPTPD (VPN)

SERVIDOR

Paso 1: instalar servicio en servidor

apt-get install pptpd

Paso 2: Identificar el Kernel del Sistema Operativo:

uname –a

Linux Lexincorp 2.4.27-2-386 #1 Thu Jan 20 10:55:08 JST 2005 i686 GNU/Linux

Paso 3: Agregar encabezados del Kernel para poder agregarle módulos

apt-get install kernel-headers-2.4.27-2-386

Paso 4: Actualizar paquetes:

apt-get install dkms patch make gcc

Paso 5: Instalar las Fuentes del modulo de encriptación

apt-get install kernel-ppp-mppe

Paso 6: Compilar y agregar los módulos al Kernel, habilitando el servicio de cifrado para ppp.

dkms add -m kernel_ppp_mppe -v 1.0.2

dkms build -m kernel_ppp_mppe -v 1.0.2

dkms install -m kernel_ppp_mppe -v 1.0.2

CONFIGURACIÓN

Paso 1: Editar archivos de configuración: (Ver archivos de configuración en http://poptop.sourceforge.net/dox/)

1. /etc/ppp/options.pptp
2. /etc/ppp/chap-secrets
    a. Crear usuario de conexión según formato de archivo.

Paso 2: Crear archivo de conexión en /etc/ppp/pears, con las siguientes instrucciones:

Nombre: “conexion”

Contenido:

pty "pptp $SERVER --nolaunchpppd"

name $DOMAIN\\$USERNAME

remotename PPTP

require-mppe-128

file /etc/ppp/options.pptp

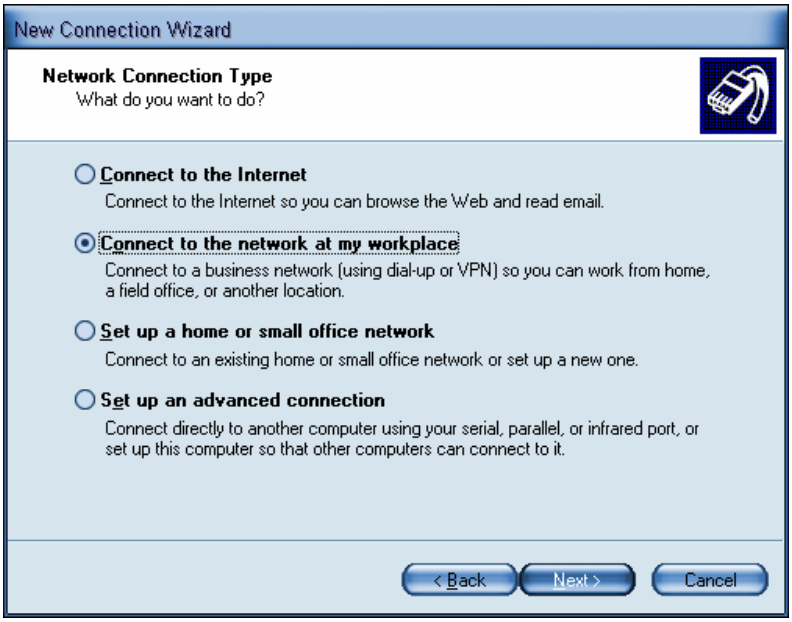
ipparam $TUNNEL

CLIENTE

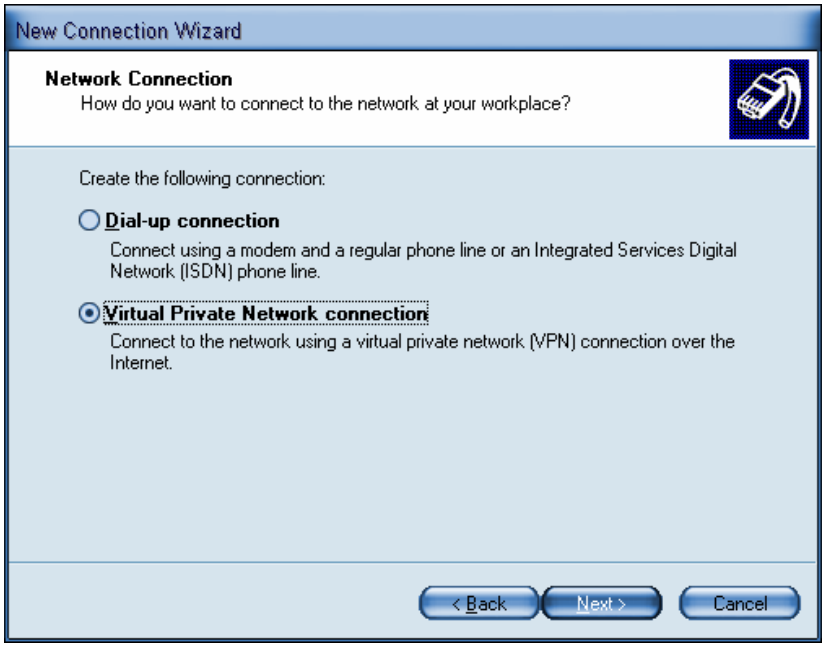
Paso 1: Clic derecho en entorno de red.

Paso 2: Crear una nueva conexión. Siguiente.

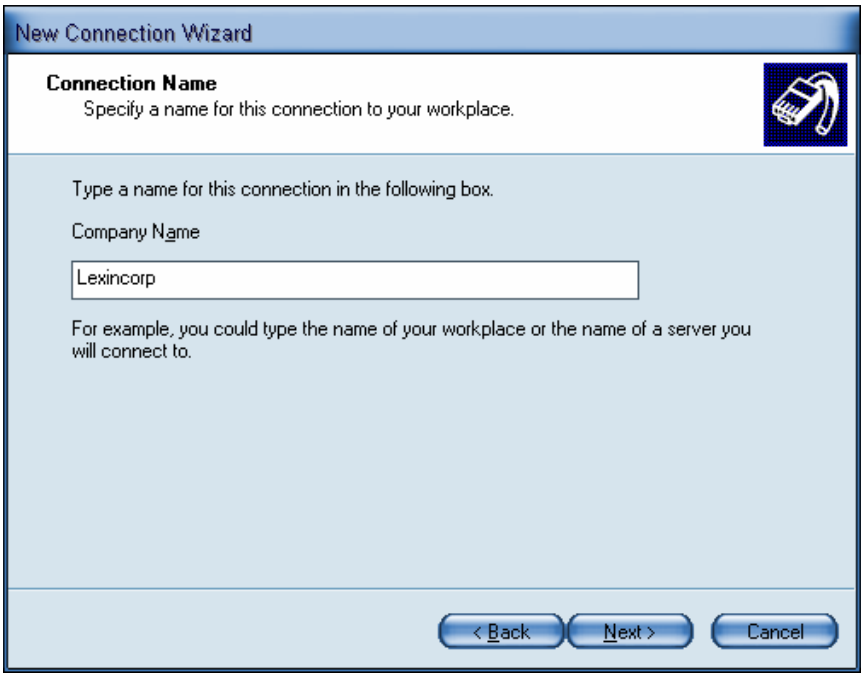
Paso 3: Elegir la Opción, “Conectar a una red en el trabajo”, siguiente.



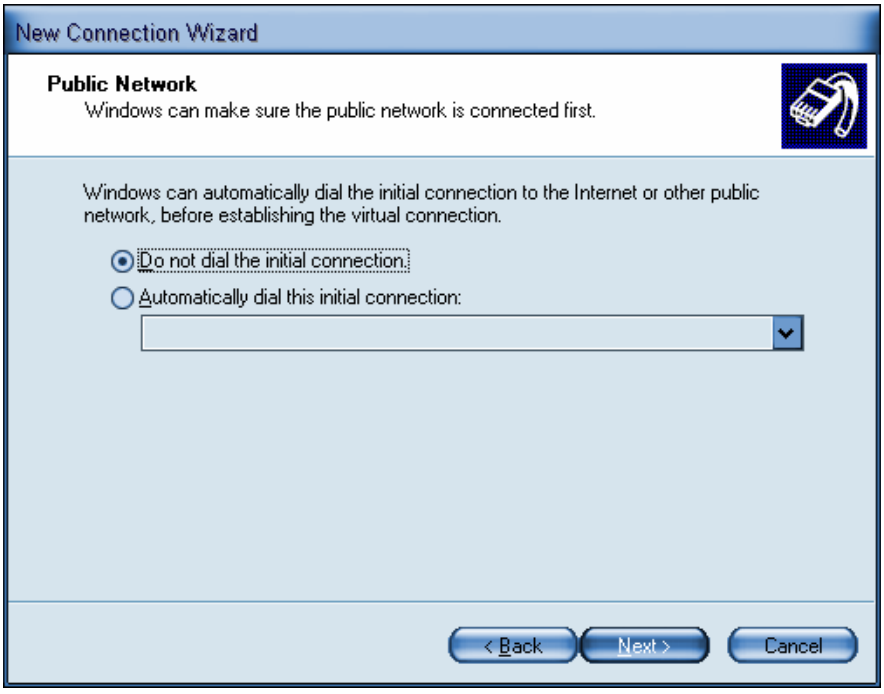
Paso 4: Elegir Opción, “Conectarme a una VPN”. Siguiente



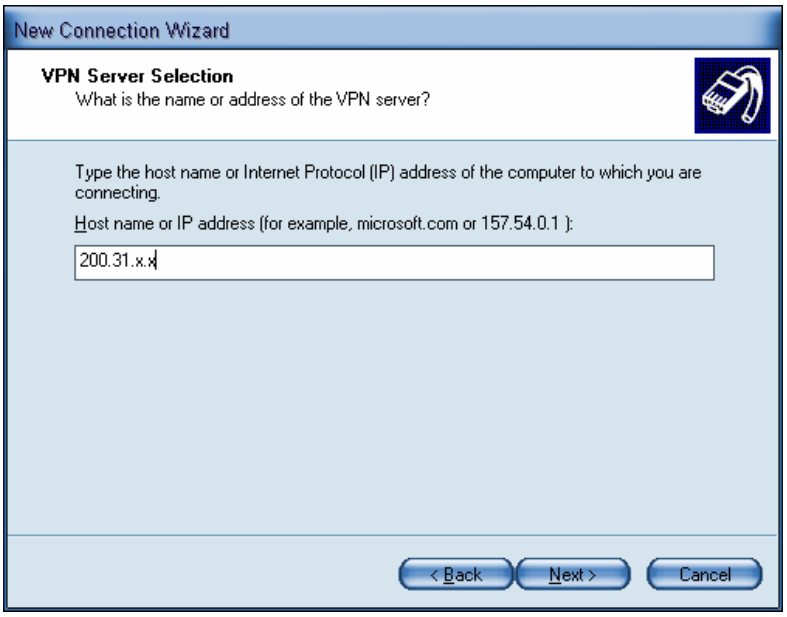
Paso 5: Escribir el nombre de la conexión.



Paso 6: Elegir la siguiente opción.



Paso 7: Colocar la IP a la que se conectaran, Siguiente.



Paso 8: Agregar un acceso directo en el escritorio. Introducir usuario y password creado en chap-secrets y conectarse.

Paso 9: Verificar que se efectué la conexión

1.8. MANUAL DE POLITICAS DE SEGURIDAD UTILIZANDO RFC 2196

POLITICAS DE SEGURIDAD

1.8.1. ¿QUÉ ES UNA POLÍTICA DE SEGURIDAD Y POR QUÉ TENER UNA?

Las decisiones de seguridad que hagas siendo un administrador pueden afectar tu red, determinando si es segura o insegura, que tan bien se puede acceder a los servicios que esta brinda, y la operabilidad de estos.

Sin embargo, no se pueden hacer buenas decisiones sin antes saber que objetivos de seguridad se necesitan o se desean, de esa manera poder elegir que herramientas o dispositivos se utilizarán para lograr esos objetivos.

Para poder determinar los objetivos de seguridad se emplearán los siguientes determinantes:

SERVICIOS OFRECIDOS VERSUS SEGURIDAD PROVEÍDA

Cada servicio proporciona a los usuarios a asumir ciertos riesgos de seguridad. Pero si algunos servicios ofrecen un riesgo mayor a los beneficios de éste, el administrador deberá decidir detener el servicio en lugar de asegurarlo.

Para la empresa Lexicorp S. A. de C. V., que realizan sus actividades con programas básicos como por ejemplo Office y Magic (programa para abogados), con estos programas se maneja mucha información importante que hoy en día no tiene las medidas de seguridad necesarias y que puede ser victima de ataques de cualquier extraño o de alguien mal intencionado a dentro de la empresa, por tanto, se ha decidido que se proporcionarán las medidas necesarias de seguridad.

FACILIDAD DE USO VERSUS SEGURIDAD

Los sistemas que son fáciles de usar muchas veces no proveen la seguridad necesaria a la información que manejan, el sistema más fácil de usar permitirá acceso a cualquier persona sin que este requiera de una clave para ingresar. Al

utilizar perfiles de usuarios los sistemas estarán menos vulnerables a ataques de seguridad, haciéndolos menos accesibles.

Para la Intranet se utilizara un software de código el cual manejara perfiles de usuarios, grupos y habrá un administrador del sistema el cual tendrá los permisos necesarios para crearlos, este dará la seguridad necesaria para que únicamente los usuarios registrados puedan tener acceso a ella.

Para la seguridad en el Access Point se utilizará el método de direcciones MAC, el cual consiste en introducir una tabla de direcciones físicas en el permitiendo así que solo las computadoras ya sean Desktop o Laptop que están en esa tabla puedan conectarse a la red.

Para la seguridad en el servidor se creara un script el cual se cargara al inicio del sistema, estas reglas estarán creadas con Iptables, que es un muro de fuego de código abierto que trae el sistema este dará al seguridad necesaria a todos los servios que habrán en él.

COSTOS DE SEGURIDAD VERSUS RIESGO A PÉRDIDAS

Hay diferentes costos de seguridad:

- **Monetario:** Incluye los costos de comprar hardware o software para brindar seguridad a tu red, como: firewalls, y generadores de claves.
- **Rendimiento:** La forma como la red responde a peticiones de los usuarios; el rendimiento puede ser reducido al utilizar métodos de encriptación porque consumen recursos de memoria y CPU.
- **Facilidad de uso:** si el sistema esta excedido de mecanismos de seguridad este se vuelve inoperable, con lo que baja la productividad a la empresa.

Hay diferentes niveles de riegos

- **Perdida de privacidad:** Cuando un usuario no autorizado lee información valiosa.
- **Perdida de datos:** Ocurre cuando información es corrompida o borrada de la base de datos.

- **Perdida de servicio:** Al no haber espacio suficiente para guardar la información, al no haber suficiente disponibilidad de recursos, al negar el acceso a ciertos usuarios.

1.8.2. OBJETIVO

Implementar las políticas de seguridad al sistema conforme al RFC 2196.

1.8.2.1. PLAN DE SEGURIDAD

La implementación del sistema se divide en tres grandes partes, la Intranet, la red inalámbrica, el servidor y sus servicios. Las tres partes requieren seguridad y políticas que nos digan como poder realizarlo por lo cual utilizaremos el RFC 2196 (Request For Comments) para este objetivo, este nos dará los lineamientos necesarios para poder dar seguridad a todos los sistemas que se implementaran, a continuación se detallan los lineamientos según el RFC escogido:

- Separación de servicios.
- Denegar todos / Permitir todos.
- Configuración de la red y los servicios.
- Protegiendo la Infraestructura.
- Protegiendo la red.
- Protegiendo los servicios.
- Servicios de seguridad y procedimientos.
- Autenticación.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autorización, Acceso y Auditoria.
- Asegurar los respaldos
- Manejando incidentes de seguridad.
- Preparando y planeando incidentes de seguridad.
    - Notificación y puntos de contactos.

- Identificación de incidentes.
- Manejando un incidente.
- Documentación de un incidente.
- Responsabilidades.
- Actividades en Curso o Cambiantes.

A continuación de detallan cada uno de ellos:

1.8.2.2. SEPARACIÓN DE SERVICIOS

Hay muchos servicios, algunos de estos pueden ser internos o públicos, los cuales por muchas razones de seguridad deben mantenerse aislados el uno del otro en segmentos de redes distintos, esto además provee un incremento del desempeño generalizado en la prestación de dichos servicios.

En el caso de la implementación nos concentraremos en los servicios internos ya que se bloqueara el acceso a las redes publicas e Internet desde la empresa, por tanto se ha decidido que tanto los servicios del software GPL Group-Office que servirá como Intranet, Magic (software para abogados), estarán ubicados en el Servidor Linux, así como también el Software del portal cautivo ChilliSpot y el software AAA (Autenticación, Autorización y Auditoria) FreeRadius porque todos están basados bajo la misma tecnología.

1.8.2.3. DENEGAR TODOS / PERMITIR TODOS

Con el objetivo de tener mayor seguridad en los servicios se ha decidido implementar el método de “Denegar todos”, en lo cual todo lo que no esta explícitamente permitido estará bloqueado.

En primer lugar, se hará una instalación básica del sistema operativo, el cual tendrá únicamente aquellos programas para arrancar el sistema.

Luego selectivamente se instalaran y configurarán los servicios necesarios para el buffet según las necesidades de la plataforma de seguridad a instalar, una vez que el sistema operativo este preparado se procederá a instalar aquellos programas que nos servirán específicamente para la implementación de los servicios, como los son FreeRadius incluyendo todos los paquetes necesarios para

su perfecto desempeño, MySQL, Apache, Apache SSL y otros. Seguidamente, se pondrá en marcha ChilliSpot y todos los servicios para que este proporcione el portal cautivo para el acceso a Internet o Intranet. Finalmente, se procederá a instalar el software GPL Group-Office.

1.8.2.4. CONFIGURACIÓN DE LA RED Y LOS SERVICIOS.

1.8.2.4.1. PROTEGIENDO LA INFRAESTRUCTURA

Se protegerá la red de acceso no autorizados provenientes de cualquier red pública por medio de un muro de fuego (firewall) y además de otros incidentes comunes como son:

- Catástrofes Naturales.
- Accesos no Autorizados.
- Condiciones climáticas inapropiadas.
- Falla en la alimentación eléctrica.

1.8.2.4.2. PROTEGIENDO LA RED

Debido a que en la actualidad no todas las entidades disponen de métodos efectivos para garantizar su seguridad interna y además tienen poca o nula experiencia en el área de redes informáticas, es por ello que los problemas de seguridad que existen en su entorno suelen volverse más complejos.

Al estudiar los problemas de seguridad que puede tener la red o Intranet, se ha decidido utilizar métodos de que garanticen que la esta estará protegida de ataques como los son muros de fuego (firewall), autenticación por medio de un portal cautivo Chilli Spot, con el cual se pedirá un usuario y una clave para los usuarios que intenten acceder a Internet Explorer. La clave y el usuario que se introduzcan serán comparados en la base de datos del servidor Linux con la asistencia de FreeRadius, si la comparación es exitosa, el usuario podrá acceder a los servicios de la Intranet.

1.8.2.4.3 PROTEGIENDO LOS SERVICIOS

Hay diferentes tipos de servicio y cada uno tiene que ser protegido. Estos requerimientos podrían variar según la intensidad de uso del servicio.

Para proteger los servicios se utilizara un muro de fuego (Firewall) el cual esta basado en iptables, se creará un script el cual se cargará cada vez que el servidor arranque, este bloqueará el acceso a los servicios a todas las redes menos a la red interna.

1.8.3. SERVICIOS DE SEGURIDAD Y PROCEDIMIENTOS.

1.8.3.1 AUTENTICACIÓN

Para la autenticación de los usuario se utilizará un portal cautivo el cual interceptara todas las transacciones que el usuario haga a través de su navegador, el portal cautivo trabajara en conjunto con freeradius el cual estará conectado a su vez a una base de datos la cual tendrá los usuarios que podrán tener acceso al sistema.

1.8.3.2 CONFIDENCIALIDAD

La información debe ser manipulada de tal forma que ningún atacante pueda leerla o usuario no autorizado esto también incluye anonimicidad, lo se leerá, las páginas que visitarán es información que a la mayoría de las personas no les gusta dar a conocer.

1.8.3.3. INTEGRIDAD / AUTENTICACIÓN

La autenticación valida la integridad del flujo de información garantizando que no ha sido modificado en el tránsito emisor-receptor y además confirma el origen/destino de la información -corrobora que los interlocutores son quienes dicen ser.

1.8.3.4. AUTORIZACIÓN

La autorización se da normalmente en un contexto de autenticación previa. Se trata un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.

1.8.3.5. ACCESO

Restringir el acceso físico a los host únicamente permitiendo a las personas que estarán autorizadas a utilizarlos.

1.8.3.6. AUDITORIA

Para la autidoria del servidor y del Access Point se habilitaran los logs de los diferentes servios con el objetivo de mantener una bitácora de todos los eventos registrados por cada uno de ellos, también se implementará un software llamado dialup admin el cual registrara todas las sesiones y tiempos de conexión de los usuarios que estén registrados en el sistema.

1.8.3.7. ASEGURAR LOS RESPALDOS

Se Implementara una tarea programa (CRON) la cual se ejecutará todos días a las 12:00 a.m. este será un Script el cual hará un respaldo de la información más importante como los archivos de configuración e información vital de la empresa residente en la Intranet y la copiara a otro disco que se encuentra en el servidor.

1.8.4. MANEJANDO INCIDENTES DE SEGURIDAD

1.8.4.1. PREPARANDO Y PLANEANDO INCIDENTES DE SEGURIDAD

La preparación y el planeamiento de incidentes de seguridad en las empresas comprenden un grupo de etapas que las organizaciones deben cumplir cuando un evento de seguridad ocurra. Un proceso de respuesta a incidentes ayudaría a manejar correcta y eficientemente un evento inusual determinado.

Asimismo, el diseño de un proceso para el monitoreo y respuesta a incidentes podría ayudar a identificar la necesidad de recursos y asignación de roles y responsabilidades. A continuación se detallara los procesos recomendados para el monitoreo y respuesta a incidentes de manera efectiva:

- Notificación y Puntos de Contactos.
- Identificación de incidentes.
- Manejar el Incidente.
- Documentación del Incidente.
- Responsabilidades.
- Actividades en Curso o Cambiantes

.

1.8.4.2. NOTIFICACIÓN Y PUNTOS DE CONTACTOS

Cuando un incidente ha sido identificado, el nivel de severidad determinará las personas apropiadas que deben ser notificadas de la ocurrencia de dicho incidente, con el fin de que realicen las acciones adecuadas de acuerdo con sus roles y responsabilidades.

1.8.4.3. IDENTIFICACIÓN DE INCIDENTES

La organización debe determinar si el incidente es un ataque real o una falsa alarma, y de ser un ataque real, debe identificar el tipo específico de ataque. Algunos tipos comunes de incidentes incluyen:

- Ataques a Website.
- Ataques de denegación de servicio.
- Barrido de puertos (Scan).
- Sniffing.
- Ingeniería social.
- Acceso no autorizado.
- Infección de virus.

Categorizar el incidente por tipo, contribuye a hacer seguimiento y entender el riesgo al que se encuentra sometida la organización.

Una vez que se ha determinado las causas del ataque se debe proceder a eliminar los rastros del ataque y configurar el equipo para que no se vuelvan a producir estos ataques. Si la versión del sistema operativo es algo antigua es un buen momento para instalar una versión mas actualizada del equipo. Igualmente si se disponen de copias de seguridad anteriores al ataque se puede restaurar las copias (aunque convendría comprobar si los ficheros de la copia de seguridad no han sido modificados). o proceder a reinstalar solamente los ficheros o paquetes modificados.

Una vez que se tiene el sistema operativo “limpio” proceder a instalar los parches de seguridad que hayan salido para esta versión del equipo, eliminar los

servicios de red que no sean precisos, etc. Existen diversas guías de configuración en este sentido.

1.8.4.4. MANEJANDO UN INCIDENTE

Una vez que el administrador se ha enterado del problema, en líneas generales los pasos a seguir serian:

1. Desconexión de la red o apagado del equipo, para evitar que el atacante pueda seguir accediendo al equipo, impidiendo que recupere la información que haya podido obtener sobre otras redes o intente borrar sus huellas, o inutilice (borrado o formateo) el equipo atacado. Dado que el apagado del equipo pude provocar la perdida de información sobre el ataque (procesos que se están ejecutando, sesiones abiertas, etc.) muchas veces es preferible el filtrado completo/desconexión del equipo de la red, para así proceder al análisis de estos datos. No sólo esto, el sistema puede haber sido modificado para que un apagado no esperado (o una desconexión de la red) borre todo el sistema de forma completa
2. Realizar una copia de seguridad a bajo nivel. Siempre que sea posible es conveniente realizar una copia de los datos del equipo a bajo nivel, de forma que se tenga la información completa del estado del sistema cuando se detecto el ataque. Si es posible el análisis posterior de los datos se debería realizar sobre la copia (con el equipo apagado/desconectado). La copia debe hacerse siempre que sea posible empleando binarios compilados estáticamente en otro equipo “fiable”, para evitar que se empleen programas modificados por el atacante. Estos datos se pueden enviar a los responsables de seguridad de la organización para que procedan a su análisis si el administrador no puede realizarlos.
3. Averiguar, examinando los datos disponibles, toda la información posible sobre el ataque: vulnerabilidad empleada por el atacante, logs que muestren los ataques, escaneos y conexiones del atacante, programas instalados, logs y datos que las herramientas que el atacante ha instalado, etc. Estos datos deben ser después analizados para poder avisar a otros equipos que se han podido ver involucrados.

4. Proceder a restaurar el equipo. Volver a configurar el equipo, reinstalando el Sistema Operativo si es preciso, y aplicando los parches y configuraciones adecuadas para evitar que el ataque se vuelva a producir. En caso de existir cuentas de usuarios en el equipo es conveniente que se avise a todos los usuarios y que estos cambien sus cuentas, ya que el atacante puede haberse copiado el fichero de claves y proceder después en su equipo a buscar claves débiles para volver a entrar.
5. Avisar a los responsables de los equipos atacados o fuente del ataque, así mismo notificar toda la información a los responsables de la organización (servicio de informática, centro de cálculo, etc.) En la actualidad los ataques son "aleatorios" ya que éstos se producen buscando equipos que presenten una determinada vulnerabilidad, por lo tanto el atacante puede haber conseguido entrar en otros equipos situados en la misma red. Suele ser conveniente además contactar con los responsables de la red desde donde se produjo el ataque, ya que muchas veces se trata de equipos "trampolín", si estos equipos son "limpiados" se consigue que la red sea "un equipo" más segura.

1.8.4.5. DOCUMENTACIÓN DE UN INCIDENTE

Cuando se produce un incidente de seguridad en un equipo es siempre conveniente realizar un análisis del equipo o equipos atacados, siguiendo los pasos que se han comentado anteriormente, para así intentar averiguar desde donde se produjo el ataque, que vulnerabilidad empleo para acceder al equipo, que acciones realizó en el equipo, nivel de destreza del atacante, etc.

De esta forma se debe intentar determinar los motivos por los que el ataque tuvo éxito, de forma que se puedan tomar las medidas oportunas para que no se vulva a producir.

1.8.4.6. RESPONSABILIDADES

Muchas veces los equipos atacados son empleados para lanzar ataques a otros sistemas, por lo que no necesariamente el equipo origen de un ataque es

“culpable”, muchas veces este equipo ha sido a su vez atacado y si se avisa al administrador se puede conseguir que este también corrija los problemas de seguridad que hay en este equipo.

Los atacantes muchas veces han realizado inicialmente un barrido buscando equipos vulnerables, por lo que una notificación a los administradores de la red en la organización del ataque puede ayudar a descubrir problemas de seguridad a nivel global. Este es uno de los motivos por los cuales desde los grupos de seguridad de diversos organismos, se solicita que se envié notificación de todos los incidentes de seguridad “sufridos” por los equipos, de forma que se pueda tener una visión global de los ataques que se están produciendo.

El procedimiento de actuación, en general, de los grupos de seguridad es intentar contactar con los responsables de las organizaciones origen del ataque, para avisarles de que hay un equipo que ha podido ser atacado, de esta forma se intenta evitar que existan equipos “trampolin” empleados para atacar impunemente otros equipos.

1.8.5. ACTIVIDADES EN CURSO O CAMBIANTES

En este punto, existe una política completa de la seguridad y se han desarrollado procedimientos para poder asistir a los diferentes problemas que pueden ocasionarse, con el apoyo de esas políticas.

Sería agradable pensar que los problemas de seguridad en el trabajo se acabaron. Desafortunadamente, eso no es posible. Los sistemas y redes no son un ambiente estático, existe la necesidad de actualizar las políticas y procedimientos sobre una base regular.

Existen medidas que se pueden tomar encuenta para ayudar a los administradores o encargados de centro de cómputo a continuar con los cambios que surgen alrededor de ellos de modo que puedan emprender acciones correspondientes a la dirección de esos cambios. Los siguientes pasos pueden dar la ayuda necesaria para tener actualizado las políticas de seguridad de tus sistemas:

1. Suscribirse a los boletines son publicados por las empresas que se dedican a la seguridad en redes o de información, como por ejemplo el centro de

coordinación, que ponen al día tus sistemas contra esas amenazas que se apliquen a la tecnología de tu sitio.

2. Estar pendientes de los parches de seguridad que son producidos por los vendedores de tu equipo, obtenerlos e instalar todos los que se apliquen.
3. Vigilar activamente las configuraciones de tus sistemas para identificar cualquier cambio que pudo haber ocurrido, e investigar todas las anomalías.
4. Repasar todas las políticas y procedimientos de seguridad anualmente (como mínimo).
5. Estar pendiente de los foros o revistas para mantenerse actualizado con la última información que es compartida por los administradores de las diferentes redes.
6. Tener un agente externo que compruebe regularmente los sistemas para saber si hay conformidad con las políticas y procedimientos implementados. Esta intervención se debe realizarse por alguien que no tenga nada que ver con la empresa esta puede ser un auditor de sistemas.

APENDICE B: DISPOSITIVOS DE REDES INALAMBRICAS.

Access Point Inalámbrico LAN con Bridge

SP912 V3/SP912 V3H

CARACTERISTICAS PRINCIPALES

- Cumple con los standards industriales IEEE 802.11 & 802.11b
- Bridge LAN-a-LAN de conexión punto-a-multipunto
- Alto poder para largas distancias de bridge (SP912V3H)
- Adaptable a varias antenas de diferentes ganancias
- Seguridad Mejorada para cumplir con el □icrones IEEE 802.1x
- Control de Banda Ancha
- Control de administración SNMP

Access Point Inalámbrico LAN

SP912G

CARACTERISTICAS PRINCIPALES

- Cumple con los standards IEEE 802.11, 802.11b, 802.11g and 802.11d
- Provee 1 puerto RJ-45 LAN de 10/100M
- Soporta auto rango de datos selección a 54, 48, 36, 24, 18, 12, 9 y 6M para IEEE802.11g
- Opera en 2.4GHz de frecuencia
- Soporta modulación con Multiplexación De División De Frecuencia Orthogonal (OFDM) para IEEE 802.11g y tecnología de Espectro Directo De la Extensión De la Secuencia (DSSS) para IEEE 802.11b

AP/Bridge Inalámbrico LAN para exteriores

SP915

CARACTERISTICAS PRINCIPALES

- Su sólida cubierta proporciona rigurosa protección contra condiciones climáticas
- Cumple con los standards IEEE 802.11 y 802.11b
- Provee 1 puerto RJ-45 LAN de 10/100M
- Soporta selección automática de rango de datos a 11, 5.5, 2 y 1M para IEEE802.11b

Tarjetas Inalámbricas.

NIC

Adaptador Inalámbrico LAN PCMCIA

SP905BD

CARACTERISTICAS PRINCIPALES

- Soporta □icrones IEEE802.11(b)
- Interfase PCMCIA tipo-II
- Módulo de antena desmontable
- Trabaja sobre Win95/98/NT4/2000/ME/XP

Adaptador Inalámbrico LAN

SP906G

CARACTERISTICAS PRINCIPALES

- Cumple con los standards inalámbricos IEEE802.11g y IEEE802.11b
- Puede dconectarse a una antena externa de mayor ganancia
- Soporta 64(40)/128 bit WEP para seguridad en la red
- Soporta Windows 98SE/ME/2000/XP

APENDICE C: ARTICULOS DE "LA SALUD EN LAS REDES INALAMBRICAS"

REDES INALÁMBRICAS Y LA SALUD DEL CUERPO HUMANO.

En primer lugar diremos que los efectos de las ondas electromagnéticas dependen en gran medida de su frecuencia. Los primitivos móviles analógicos (el servicio Móvil de Telefónica) trabajaban en la banda de 450 MHz. Los primeros móviles GSM trabajaban en la banda de 900 MHz, y en la actualidad se ha habilitado una banda más en 1.800 MHz. La telefonía móvil de tercera generación (UMTS) funcionará inicialmente en la banda de 2.100 MHz. Y la wi-fi 802.11b funciona con una banda de 2.400 MHz

La profundidad a la que penetran las ondas en el cuerpo humano depende de la frecuencia. Las señales de frecuencia más baja (del orden de kilohercios) atraviesan el cuerpo humano como si éste fuera transparente, de forma que no hay energía que se disipe en el cuerpo y los efectos de la radiación son despreciables.

A frecuencias más altas, la radiación comienza a ser absorbida por los tejidos, y a la frecuencia de trabajo de los móviles, casi la totalidad de la energía es absorbida en unos pocos centímetros de profundidad a partir de la piel.

La energía absorbida se convierte en calor, produciendo el calentamiento de los tejidos expuestos. Cuanta mayor sea la potencia de la señal incidente, tanto mayor será el calentamiento de los tejidos.

Hay que tener en cuenta que los tejidos son extremadamente sensibles a los incrementos de temperatura, y las células comienzan a morir a partir de los 42ºC, y se produce un gran índice de mortandad a partir de los 45ºC. Sin embargo, es conocida la enorme capacidad reguladora del cuerpo humano, y es muy difícil conseguir un calentamiento de los tejidos a estas temperaturas.

Si se calienta un cuerpo humano por entero, la sudoración y otros fenómenos fisiológicos se encargarán de mantener la temperatura dentro de los límites tolerables.

Si se calienta una zona concreta del cuerpo, el riego sanguíneo funciona como un refrigerante efectivo, que extrae el calor de la zona afectada para distribuirlo sobre todo el cuerpo, que a su vez tiene la temperatura regulada por los procesos fisiológicos antes citados.

En la actualidad, los límites de radiación recomendados por distintos organismos oficiales han sido establecidos teniendo en cuenta únicamente los efectos térmicos de las radiaciones electromagnéticas, que son los únicos que han sido demostrados con evidencia en la actualidad.

Por debajo de los límites de radiación establecidos, los efectos térmicos de la radiación electromagnética son contrarrestados sobradamente por los mecanismos de regulación de la temperatura del cuerpo humano.

Sin embargo, hoy en día la controversia está centrada en posibles efectos no térmicos de los campos electromagnéticos. A menudo se considera que dado que la telefonía móvil tiene escasos años de existencia, los efectos médicos de los campos electromagnéticos no han sido estudiados hasta hace poco tiempo.

Nada más lejos de la realidad. La primera aplicación de un campo eléctrico para el tratamiento del cáncer se produjo tan solo cuatro décadas después de que Volta, en el año 1.800, describiera la pila eléctrica.

Quizás sea destacable el hecho de que al contrario de los pioneros de la radioactividad y las radiaciones ionizantes, que vieron su salud y su vida seriamente afectadas por los experimentos, d´Arsonval (1851-1940), Tesal (1856-1943) y otros pioneros de la radiofrecuencia, como Eli Thomson (1853-1937), vivieron todos más de ochenta años. Estos pioneros realizaron muchas experiencias sobre sí mismos en busca de efectos médicos de los campos electromagnéticos.

Desde entonces, han sido muy numerosos los estudios científicos que se han llevado a cabo en busca de efectos no térmicos de los campos electromagnéticos, pero ninguno de ellos ha podido establecer una relación causa-efecto.

En la década de los años cincuenta, se generó alrededor de la utilización de los hornos microondas una polémica bastante similar a la que se ha suscitado en la actualidad con las antenas de telefonía móvil. En realidad, la radiación que existe en el interior de un microondas es muy similar a la generada por las antenas de telefonía celular, salvo que la potencia en el interior del horno es muy superior.

En 1953, Schwan recomendó que se adoptara una radiación de 10mW/cm2 como límite de las dosis electromagnéticas tolerables. Sin embargo, cinco años más tarde, la Unión Soviética promulgó un límite estándar de tan solo 10mW/cm2. Pasado algún tiempo, tras revisar todos los datos experimentales sobre animales de que se disponía entonces, varios investigadores norteamericanos llegaron a la conclusión de que eran necesarios más de 100 mW/cm2 para producir algún efecto biológico de relevancia. Sobre esta base, adoptando un factor de seguridad de 10, el United States of America Standards Institute (USASI, ANSI en la actualidad) recomendó un nivel máximo de seguridad de 10mW/cm2.

Llegados a este punto, la polémica se desató, e incluso desde el Gobierno de los Estados Unidos se temió por la posibilidad de que a largo plazo pudiesen aparecer problemas de salud pública que afectaran a millones de ciudadanos. Sin embargo, estos problemas jamás aparecieron y en la actualidad, el horno microondas es aceptado en la mayoría de los hogares como un electrodoméstico más.

En la actualidad, los límites generalmente aceptados para la exposición a los campos electromagnéticos son del orden 900 mW/cm2 para GSM 1800 y la mitad para GSM 900.

Estos límites están algo por encima de los límites conservadores impuestos por las autoridades Soviéticas, pero están bien por debajo del umbral recomendado por el ANSI en su día. En 1992 David Reynard disparó la alarma al anunciar en la televisión de Estados Unidos que el uso del teléfono móvil había causado el tumor cerebral de su esposa.

En 1995 la demanda interpuesta contra las compañías de telefonía móvil fue desestimada por falta de evidencia, pero desde entonces, se han realizado numerosos estudios a lo largo de todo el mundo, con la intención de demostrar o refutar los efectos de los campos electromagnéticos sobre la salud humana. Estos estudios han puesto un mayor énfasis en determinar la relación entre el cáncer y la exposición a las radiaciones electromagnéticas.

Hacer un estudio epidemiológico completo no es una tarea sencilla, cuando lo que se busca no es una relación causa-efecto directa. Al igual que en el caso del tabaco, no hay una relación directa entre el consumo de tabaco y, por ejemplo, el

cáncer de pulmón. Existe gente que contrae cáncer de pulmón y no ha fumado jamás, y por el contrario, existen grandes consumidores de tabaco que conservan su salud hasta edades muy avanzadas. Sin embargo, el efecto del tabaco se hace manifiesto cuando se analizan los datos de forma estadística.

Es decir, el efecto del tabaco se puede medir como el incremento de la probabilidad de contraer cáncer de pulmón en la población fumadora, respecto de la que no lo es.

Este tipo de respuestas es el que se ha buscado en los estudios epidemiológicos realizados para analizar los efectos de las radiaciones electromagnéticas.

Diversos estudios han cruzado datos correspondientes a cientos de miles de personas y no se han encontrado ninguna causa de enfermedad que se correlacione con la utilización del teléfono móvil o la residencia en las proximidades de una estación base.

¿Quiere decir esto que no existe una incidencia de los campos electromagnéticos sobre la posibilidad de contraer alguna enfermedad? Para muchos esto es así, pero sin embargo, esto no puede afirmarse de forma categórica.

LOS CAMPOS ELECTROMAGNÉTICOS Y LA SALUD PÚBLICA

ESTACIONES DE BASE Y TECNOLOGÍAS INALÁMBRICAS

Hoy día la telefonía móvil es algo corriente en todo el mundo. Esa tecnología inalámbrica se basa en una amplia red de antenas fijas o estaciones de base que transmiten información mediante señales de radiofrecuencia (RF). Hay más de 1,4 millones de estaciones de base en todo el mundo, y la cifra está aumentando de forma considerable con la aparición de las tecnologías de tercera generación.

Hay otras redes inalámbricas que permiten obtener servicios y acceso a Internet de alta velocidad, como las redes de área local inalámbricas (WLAN), cuya presencia también es cada vez más frecuente en los hogares, las oficinas y muchos lugares públicos (aeropuertos, escuelas y zonas residenciales y urbanas).

A medida que crece el número de estaciones de base y de redes locales inalámbricas, aumenta también la exposición de la población a radiofrecuencias. Según estudios recientes, la exposición a RF de estaciones de base oscila entre el 0,002% y el 2% de los niveles establecidos en las directrices internacionales sobre los límites de exposición, en función de una serie de factores, como la proximidad de las antenas y su entorno. Esos valores son inferiores o comparables a la exposición a las RF de los transmisores de radio o de televisión.

Las posibles consecuencias para la salud de la exposición a campos de RF producidos por las tecnologías inalámbricas han causado preocupación. En la presente nota descriptiva se examinan las pruebas científicas disponibles sobre los efectos en la salud humana de una exposición continua de bajo nivel a estaciones de base y otras redes locales inalámbricas. Para obtener información detallada sobre un taller de la OMS dedicado a este tema.

PREOCUPACIONES SANITARIAS

Un motivo de inquietud común en relación con las antenas de las estaciones de base y de las redes locales inalámbricas es el relativo a los efectos a largo plazo que podría tener en la salud la exposición de todo el cuerpo a señales de RF. Hasta la fecha, el único efecto de los campos de RF en la salud que se ha señalado en los estudios científicos se refería al aumento de la temperatura corporal (> 1º C) por la exposición a una intensidad de campo muy elevada que sólo se produce en determinadas instalaciones industriales, como los calentadores de RF. Los niveles de exposición a RF de las estaciones de base y las redes inalámbricas son tan bajos que los aumentos de temperatura son insignificantes y no afectan a la salud de las personas.

La potencia de los campos de RF alcanza su grado máximo en el origen y disminuye rápidamente con la distancia. El acceso a lugares cercanos a las antenas de las estaciones de base se restringe cuando las señales de RF pueden sobrepasar los límites de exposición internacionales. Una serie de estudios recientes ha puesto de manifiesto que la exposición a RF de las estaciones de base y tecnologías inalámbricas en lugares de acceso público (incluidos hospitales y escuelas) suele ser miles de veces inferior a los límites establecidos por las normas internacionales.

De hecho, debido a su menor frecuencia, a niveles similares de exposición a RF, el cuerpo absorbe hasta cinco veces más señal a partir de la radio de FM y la televisión que de las estaciones de base. Ello se debe a que las frecuencias utilizadas en las emisiones de radio de FM (unos 100 MHz) y de televisión (entre 300 y 400 MHz) son inferiores a las empleadas en la telefonía móvil (900 y 1800 MHz), y a que la estatura de las personas convierte el cuerpo en una eficaz antena receptora. Además, las estaciones de emisión de radio y televisión funcionan desde hace por lo menos 50 años sin que se haya observado ningún efecto perjudicial para la salud.

Aunque la mayoría de las tecnologías de radio utilizaban señales analógicas, las telecomunicaciones inalámbricas modernas usan señales digitales. Los detallados estudios realizados hasta el momento no han revelado ningún peligro específico derivado de las diferentes modulaciones de RF.

Cáncer: las noticias publicadas por los medios informativos sobre conglomerados de casos de cáncer en torno a estaciones de base de telefonía móvil han puesto en alerta a la opinión pública. Cabe señalar que, desde el punto de vista geográfico, el cáncer se distribuye de forma irregular en cualquier población. Dada la presencia generalizada de estaciones de base en el entorno, pueden producirse conglomerados de casos de cáncer cerca de estaciones de base simplemente por casualidad. Además, los casos de cáncer notificados en esos conglomerados suelen ser de distinto tipo, sin características comunes, por lo que no es probable que se deban a una misma causa.

Se pueden obtener pruebas científicas sobre la distribución de los casos de cáncer entre la población mediante estudios epidemiológicos bien planificados y ejecutados. En los últimos 15 años, se han publicado estudios en los que se examinaba la posible relación entre los transmisores de RF y el cáncer. En esos estudios no se han encontrado pruebas de que la exposición a RF de los transmisores aumente el riesgo de cáncer. Del mismo modo, los estudios a largo plazo en animales tampoco han detectado un aumento del riesgo de cáncer por exposición a campos de RF, incluso en niveles muy superiores a los que producen las estaciones de base y las redes inalámbricas.

Otros efectos: se han realizado pocos estudios sobre los efectos generales en la salud humana de la exposición a campos de RF de las estaciones de base. Ello se debe a la dificultad para distinguir los posibles efectos en la salud de las señales muy bajas que emiten las estaciones de base de otras señales de RF de mayor potencia existentes en el entorno. La mayoría de los estudios se han centrado en la exposición a RF de los usuarios de teléfonos móviles. Los estudios con seres humanos y animales en los que se han examinado las ondas cerebrales, las funciones intelectuales y el comportamiento tras la exposición a campos de RF, como los generados por los teléfonos móviles, no han detectado efectos adversos. El nivel de exposición a RF utilizado en esos estudios era unas 1000 veces superior al de exposición del público en general a RF de estaciones de base o de redes inalámbricas. No hay pruebas de que se produzcan alteraciones del sueño o de la función cardiovascular.

Algunas personas han señalado síntomas inespecíficos tras la exposición a campos de RF de estaciones de base y otros dispositivos de campos electromagnéticos. Como se indica en una nota descriptiva recientemente publicada por la OMS sobre la «hipersensibilidad electromagnética», no se ha demostrado que los campos electromagnéticos provoquen esos síntomas. Sin embargo, es importante tener en cuenta la difícil situación de las personas que sufren esos síntomas.

De todos los datos acumulados hasta el momento, ninguno ha demostrado que las señales de RF producidas por las estaciones de base tengan efectos adversos a corto o largo plazo en la salud. Dado que las redes inalámbricas suelen producir señales de RF más bajas que las estaciones de base, no cabe temer que la exposición a dichas redes sea perjudicial para la salud.

NORMAS DE PROTECCIÓN

La Comisión Internacional de Protección contra las Radiaciones No Ionizantes (ICNIRP, 1998) y el Instituto de Ingenieros Electricistas y Electrónicos (IEEE, 2005) han elaborado directrices internacionales sobre los límites de exposición para ofrecer protección contra los efectos reconocidos de los campos de RF.

Las autoridades nacionales deberían adoptar normas internacionales para proteger a los ciudadanos de los niveles perjudiciales de RF. Además, deberían restringir el acceso a las zonas en que puedan rebasarse los límites de exposición.

PERCEPCIÓN PÚBLICA DEL RIESGO

Algunas personas consideran probable que la exposición a RF entrañe riesgos y que éstos puedan ser incluso graves. Ese temor se debe, entre otras cosas, a las noticias que publican los medios de comunicación sobre estudios científicos recientes y no confirmados, que provocan un sentimiento de inseguridad y la sensación de que puede haber riesgos desconocidos o no descubiertos. Otros factores son las molestias estéticas y la sensación de falta de control y participación en las decisiones de ubicación de las nuevas estaciones de base. La experiencia demuestra que los programas educativos, así como una comunicación eficaz y la participación del público y otras partes interesadas en las fases oportunas del proceso de decisión previo a la instalación de fuentes de RF, pueden aumentar la confianza y la aceptación del público. La OMS ha destacado la necesidad de ese diálogo en una publicación disponible en nueve idiomas.

CONCLUSIONES

Teniendo en cuenta los muy bajos niveles de exposición y los resultados de investigaciones reunidos hasta el momento, no hay ninguna prueba científica convincente de que las débiles señales de RF procedentes de las estaciones de base y de las redes inalámbricas tengan efectos adversos en la salud.

Iniciativas de la OMS

A través del Proyecto Internacional CEM, la OMS ha establecido un programa para supervisar las publicaciones científicas sobre los campos electromagnéticos, evaluar los efectos en la salud de la exposición a frecuencias de 0 a 300 GHz, ofrecer asesoramiento sobre los posibles peligros de los campos electromagnéticos y determinar las medidas de mitigación más idóneas. Basándose en amplios estudios internacionales, el Proyecto ha promovido investigaciones para subsanar la falta de conocimientos. En respuesta a ello, en los 10 últimos años, diversos gobiernos e

institutos de investigación nacionales han destinado más de US$ 250 millones al estudio de los campos electromagnéticos.

Aunque nada hace pensar que la exposición a campos de RF de estaciones de base y redes inalámbricas tenga efectos en la salud, la OMS sigue fomentando las investigaciones para determinar si la exposición a la mayor RF de los teléfonos móviles puede repercutir en la salud. Para consultar las investigaciones más recientes dedicadas fundamentalmente a la telefonía móvil (véase enlaces relacionados al final de la página).

Está previsto que en 2006-2007 el Centro Internacional de Investigaciones sobre el Cáncer (CIIC), un organismo especializado de la OMS, lleve a cabo un estudio sobre el riesgo de cáncer provocado por los campos de radiofrecuencia, y que en 2007-2008 el Proyecto Internacional CEM realice una evaluación general de los riesgos para la salud de los campos de RF.[24]

[24] OMS (Organización Mundial de la Salud) http://www.who.int/mediacentre/factsheets/fs304/es/index.html

APENDICE D: ANALISIS ECONOMICO DE LAS REDES INALAMBRICAS

Versión Preliminar para discusión

ICAWF "WIRELESS FIDELITY. LA CLAVE PARA LA INCLUSION DIGITAL?"

17 de Noviembre a 4 de Diciembre de 2003

Fecha de presentación: 11-10-2003

Título: **WIRELESS FIDELITY. LA CLAVE PARA LA INCLUSION DIGITAL?** - ANALISIS ECONOMICO

Autor/a: Ing. Oscar Manuel Guarin Figueroa
Consultor de Redes y Telecomunicaciones
Escuela de Ingenierías Eléctrica y Electrónica
Universidad del Valle
Cali (Colombia)
Email: omguarin@hotmail.com

Formatos disponibles: 1

Idioma original: Español

Traducciones disponibles: 1

Este trabajo fue realizado con fondos otorgados por el International Development Research Center (IDRC) en nombre del Instituto para la Conectividad en las Américas (ICA). ICA es un proyecto administrado por el International Development Research Center (IDRC), Canadá.

WIRELESS FIDELITY: LA CLAVE PARA LA INCLUSION DIGITAL?

Un análisis de costos para un tipo de tecnología como WiFi implica realizar un estudio comparativo desde el punto de vista global de todas las variables implicadas, tomando como punto de partida los lineamientos establecidos por un estándar global de comunicaciones, procesos de regulación espectral de frecuencias, características mismas del mercado en cuanto a fabricantes, integradores y desarrolladores de sistemas inalámbricos, convergencia de servicios y visión futura dentro de un marco de apertura hacia tecnologías de segunda o tercera generación.

Si bien ya existen procesos bien definidos para su implementación dentro del concepto que manejamos sobre una red de telecomunicaciones digital totalmente integrada a los servicios de una red como la Internet, debemos considerar otro tipo de aspectos como la seguridad de la información, servicios y aplicaciones en banda ancha que hacen uso de redes Wan/IP, protocolos de comunicación, roaming con operadores móbiles, implementación de tecnologías picocecular (PAN) y convivencia con otros sistemas que hacen uso del espectro de frecuencias UHF.

Todo ello, implica hacer un estudio pormenorizado del tipo de implementación que se ha venido imponiendo dentro de las redes inalámbricas a lo largo de estos años, de tal manera que podamos analizar las diferentes alternativas de conexión wireless LAN que existen en nuestro medio. Aplicaciones y desarrollo de sistemas operativos en equipos móbiles como un pocket PC, una PDA o dispositivos empotrados en la carrocería de un automóvil nos hacen vislumbrar un futuro cercano en donde los servicios de una red podrán ser ofrecidos independientemente del lugar donde se encuentre un usuario. La tecnología establecida a través de un estándar de comunicaciones como Wi-Fi ya está desempeñando un papel importante en las soluciones de conectividad en el hogar, en las empresas, en la industria, en el gobierno, en la educación y, en general, en todas aquellas aplicaciones enmarcadas dentro de un ambiente que opere en un campus de amplia cobertura mediante

puntos de acceso remotos o haciendo uso de antenas especiales para una solución out-door punto a punto o punto-multipunto.

En el presente documento se hará un análisis económico desde la perspectiva general de un proyecto para la implementación de un sistema de red inalámbrica Wi-Fi que haga uso de la tecnología de radiofrecuencia en las bandas ya establecidas por los organismos de estandarización y regulación (2.4 y 5 GHz), mostrando las diferentes alternativas de solución desde el punto de vista costo vs beneficio/eficiencia y su incidencia en el proceso de conectividad WAN hacia la web.

Ello implica hacer un muestreo general a nivel del estado del arte, características de implementación, nivel de estandarización, integración e interoperabilidad con otras plataformas, capacidad de transmisión, valores agregados, etc, que de alguna manera tienen algún tipo de incidencia en el costo total de la solución, vistos desde la perspectiva de los diversos tipos de fabricantes que podemos encontrar en el mercado a nivel mundial y que hacen uso del estándar y homologados por la Wi-Fi Alliance (www.wi-fi.org) y su organismo asociado el Weca.

Para nuestro análisis hemos tomado una muestra significativa de los fabricantes de dispositivos, tarjetas, chipsets, equipos de conectividad, laptops, sistemas de entretenimiento, accesorios, integradores con tecnologías inalámbricas como bluetooth o protocolos como el WAP, etc, más reconocidos del mercado dentro de la industria de las telecomunicaciones inalámbricas, con el ánimo de establecer unos puntos de referencia que nos permitan vislumbrar las ventajas y desventajas de cada solución, sus tendencias futuras en el mercado y todo desde la perpectiva general de aplicaciones para redes ethernet LAN inalámbricas que ofrece la industria.

Hemos analizado los diferentes escenarios posibles en los cuales se puede llegar a implementar una solución wireless con los estándares y protocolos ya definidos (IEEE 802.11a, 802.11b, 802.11g). Sin embargo, cada escenario de

solución conlleva a analizar otro tipo de variables que están, de alguna manera, correlacionadas con el uso de este tipo de tecnologías y su implicación en el desarrollo de aplicaciones particularizadas de acuerdo a los requerimientos de cada usuario en la red.

Haremos un análisis general de los efectos en el costo total de un proyecto de redes wireless LAN a nivel de estándares, modos de operación, características integradas como valor agregado de una solución como es el caso del nivel de seguridad requerido, interoperabilidad con otras plataformas y, por supuesto, las tendencias futuras del mercado y su impacto en la implementación de redes Lan/wan para accesos a la Internet en banda ancha mediante equipos gateways o routers.

ESTANDARES DE COMUNICACIÓN Wi-Fi

Un análisis de costos para la implementación de una solución o proyecto wireless LAN requiere de un análisis comparativo de los diferentes estándares de comunicación WiFi que se han ratificado actualmente en el mercado. Aunque el estándar 802.11g todavía se encuentra en su fase borrador, se espera que a finales del 2003 esté ratificado por la IEEE.

Si bien el costo total de una solución con equipos Access Points 802.11a es más alto que el de una solución con equipos que manejen dispositivos 802.11b (25-30%), hay que analizar ciertas ventajas a nivel del uso de más canales no sobrelapados disponibles (8 ch), un nivel mayor de seguridad por el uso de una banda de frecuencia no muy común y sobre todo, la disponibilidad de unos equipos que no tienen problemas de interferencia con otros tipos de tecnologías inalámbricas como son los teléfonos cordless, dispositivos que hace uso de la tecnología bluetooth, equipos de microondas, etc, los cuales operan en un espectro cercano a la banda de los 2.4 GHz.

En la Tabla 1 se muestra un listado general de los principales fabricantes (a nivel de muestra representativa) de equipos Access Points que cumplen con el estándar 802.11b. De hecho, siendo el 802.11b la primera norma ratificada por el

grupo de la IEEE, la mayoría de los fabricantes de hoy en día cumplen con todas las especificaciones establecidas por dicho organismo y han sido certificadas por la Wi-Fi Alliance a través de su grupo Weca (www.weca.org).

EQUIPOS ACCESS POINTs IEEE 802.11b			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
3Com	3CRWE80096A	Wireless Lan Access Point 8000 802.11b	**354.16**
Adaptec	2012500	Wireless 802.11b AP Extends Wireless Ethernet Networks	**98.62**
Buffalo	WLMRL11G	AirStation Wireless 802.11b LAN Access Point/Bridge	**85.20**
Cisco	AIRBR350EK9	Cisco Aironet 350 Series Access Point 802.11b	**760.0**
D-Link	DWL1000AP	Wireless Access Point 802.11b 11 Mbps	**205.00**
Enterasys Networks	CSIWS-AB	Roamabout 2000 Access Point 802.11b	**647.00**
Hawking Technology	HWR258	Wireless Access Point 11 Mbps AP 802.11b	**79.35**
Intel Corp.	APWE1120NA	Wireless ENET Access Point 802.11b	**199.0**
Linksys	WAP11CA	Wireless Network Access Point 802.11b	**71.05**
NetGear	ME102	ME102NA Wireless Access Point 802.11b	**70.64**
Proxim	700017505	Orinoco AP-200 Low Cost AP for Home or SOHO Office	**139.99**

SMC	SMC2455W	2.4 GHz 11/22 Mbps autosensing Wireless Access Point	**95.00**
U.S. Robotics	USR2249	802.11b Wireless Access Point 22 Mbps	**75.0**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 1. *Access Points IEEE 802.11b.*

Una de las características más interesantes a tener en cuenta desde el punto de vista económico es la compatibilidad de las nuevas tecnologías emergentes con la plataforma o recursos ya instalados. Desde este marco de referencia, el protocolo Wi-Fi que se impone es el IEEE 802.11g debido a que utiliza la misma interfaz de radio en la banda de los 2.4 GHz y puede soportar la comunicación con tarjetas que cumplan con el estándar 802.11b (en modo dual). En el mercado, muchos fabricantes ya comercializan este tipo de dispositivos a nivel de Access Points, tarjetas de red NICs (PC Cards o Adaptadores PCI) o chipsets que cumplan con la multifuncionalidad requerida, de tal forma que se consiga el mismo alcance a nivel de radio que es una de las ventajas de la norma 802.11b y con velocidades de transmisión de 54 Mbps (en teoría, el troughput real es del orden de unos 20 a 25 Mbps) que es una de las ventajas principales obtenidas con la norma 802.11a. El efecto inmediato a nivel de costos es la posibilidad de hacer uso de una misma interfaz de radio y permite obtener el mismo nivel de alcance o cobertura.

Dentro de un proyecto de redes inalámbricas, la diferencia entre cada uno de estos fabricantes se establece en los diferentes valores agregados de cada dispositivo como su compatibilidad a nivel de equipos y tarjetas con otros fabricantes (lo cual ya ha sido homologado a nivel mundial), cumplimiento con otros estándares como el 802.11i para proveer niveles de seguridad (una norma que todavía se encuentra en proceso de certificación), el 802.11e que permite definir características a nivel de Calidad del Servicio (QoS) para otro tipo de señalización sensible al retardo como el audio y el video, enlace con operadores Wlan, procesos de fabricación especiales para equipos portátiles y PDAs, posibilidad de diseño e implementación de redes virtuales (VPNs), conexión a la Web, realizando funciones

de un gateway externo, u otro tipo de redes a través de los servicios como routers inalámbricos, etc.

La diferencia de precios de algunos fabricantes se debe a que ofrecen equipos con características mínimas o sirven como adaptadores de equipos switches para redes cableadas. El precio que hemos tomado como referencia para este análisis es el precio de lista del fabricante al cual tendríamos que incluirle los costos de compra, importación, envío, etc (ello incrementa el valor en un rango de unos 20 a 40%). Dependiendo del País, estos costos varían en menor o mayor proporción. Hemos hecho énfasis en los principales fabricantes y distribuidores con presencia en los países de Latinoamérica y el Caribe.

A nivel de tarjetas, el estándar 802.11b es el más difundido a nivel mundial por todos los fabricantes y empresas comercializadoras de redes inalámbricas. Podemos ver este tipo de tarjetas en múltiples equipos móviles como desktops, laptops, PDAs, equipos adaptadores que operan con el estándar bluetooth, etc. En la Tabla 2 se muestra un listado general de este tipo de tarjetas tanto para PCs con adaptadores PCI o PC Cards (por lo general tipo II) para equipos portátiles. Hay que destacar que muchos fabricantes ya han implementado características de encripción en sus tarjetas (128+) y cumplen con los estándares 802.1x.

Muchos de los fabricantes ofrecen un precio especial por la compra de un paquete (pack) o grupo de tarjetas. Es de anotar que el costo de las tarjetas adaptadoras PCI es mayor en comparación con las tarjetas para equipos portátiles. En el mercado se pueden encontrar todavía tarjetas adaptadoras para conexión con radios 802.11b tipo ISA o bien, ya hay fabricantes que integran tecnología WiFi en sus Mainboards.

TARJETAS Y ADAPTADORES IEEE 802.11b			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***

3Com	3CRWWE62092B	3Com 11 Mbps Wireless LAN PC Card with Xjack Antenna	**69.68**
	3CRDW696	3Com 11 Mbps Wireless LAN PCI Adapter	**88.75**
Adaptec	2012400	Wireless 802.11b PC CardKit Connectivity for Notebooks	**52.99**
Apple	M7600LLE	Airport Card for Notebooks	**78.53**
Avaya	700016777	Intl Wireless 11 Mbps Silver WiFi Single Pack 64 bit Encryption	**89.0**
Buffalo	WLPIPCML11GP	AirStation 802.11b 11 Mbps Wireless PCMCIA	**42.37**
	WLIPCIOP10B	AirStation PCI Adapter	**21.47**
D-Link	DWL650+	Wireless 22 Mbps CardBus Adapter	**29.50**
	DWL520+	Wireless 22 Mbps PCI Adapter	**39.83**
Enterasys Networks	CSIBDAB128	Roamabout 128 bit PC Card	**76.48**
Hawking Technology	WE110P	Wireless 11M Network PC Card PCMCIA Type II 802.11b	**33.0**
IBM	31P8301	IBM Cisco AIRNET WL Adapter 802.11b mini PCI	**94.00**
NetGear	MA401NA	Wireless PC Card 802.11b	**39.90**
	MA311NA	MA311 802.11b Integrated PCI	**56.00**
Proxim	848441481	Orinoco Turbo 11M PCCard-Gold	**76.95**
SMC	SMC2532WB	2.4 GHz 802.11b High Power Wireless PC Card	**51.83**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 2. *Tarjetas PC-Cards y adaptadores 802.11b*

Algunos equipos y tarjetas adaptadoras vienen equipados para trabajar en modo “Turbo” el cual permite optimizar el rendimiento a 22 Mbps (en realidad el performance obtenido es menor) mediante un algoritmo de compresión, sobre todo

en dispositivos que trabajan en modo dual. Estos modos de operación y algoritmos de compresión han sido trabajados por varios fabricantes y ahora se están trabajando en tecnologías 802.11g a 54 Mbps.

EQUIPOS Y TARJETAS 802.11A.

El estándar IEEE 802.11a se ha destacado por su amplia capacidad de operar con un número mayor de canales sin sobrelapamiento (8 ch) y trabajar en una banda de frecuencias que no genera interferencia con otro tipo de tecnologías. En la Tabla 3 se muestra un listado del costo de los equipos Access Points que cumplen con la especificación 802.11a en la que podemos ver ciertos fabricantes que establecen características de ampliación y compatibilidad con tecnologías anteriores como la b. Otros fabricantes venden un Kit de actualización con una tarjeta de radio 802.11a sobre el chasís en el que venía la tarjeta de radio de 2.4 GHz.

EQUIPOS ACCESS POINTs IEEE 802.11a			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
3Com	3CRWE825075AUS	Wireless Access Point 8250 802.11a	**579.55**
Apple	M8930LLA	AirPort Extreme Base Station	**190.88**
Cisco	AIRAP1230AAK9	802.11a IOS AP w/AVAIL MPCI Slot ENET	**798.59**
Compaq	216709001	WL 510 Enterprise Access Point LAN (802.11b,a)	**540.0**
D-Link	DWL5000AP	AirPro Wireless Access Point IEEE 802.11a	**177.19**
Enterasys Networks	RBTBFAX	Roamabout R2 Wireless AP + 54 Mbps Radio Card 802.11a	**785.4**
Intel Corp.	WDAP5000M	Pro Wireles 5000 LAN dual	**645.4**
Linksys	WAP54A	Wireless Access Point 802.11a	**239.0**
NetGear	HE102	HE102NA 802.11a Wireless	**59.00**

		Access Point	
Proxim	857105	Harmony 802.11a Connectorised Access Point	**98.0**
SMC	SMC2755W	EZ Connect 802.11a Wireless Access Point	**58.95**
Sony	PCWAA500	Sony VAIO Wireless LAN Pro Access Point 5 GHz	**319.41**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 3. *Access Points IEEE 802.11a*

Las tarjetas que cumplen con el estándar 802.11a tienen un costo mayor dependiendo del tipo de solución y nicho de mercado para el cual están orientadas, es conveniente establecer pruebas de compatibilidad entre los diferentes fabricantes. En la Tabla 4 hacemos un análisis comparativo de costos para este tipo de tarjetas tanto para PCCards como Adaptadores PCI. En la mayoría de las tarjetas que encontramos en el mercado, el modo que prevalece para este estándar es el dual (802.11a y b) como veremos en la siguiente sección.

Algunos fabricantes de tarjetas adaptadoras ofrecen versiones en tecnologías anteriores con su interfaz de radio y antena acopladas a los chipsets del dispositivo, mientras que empresas como Enterasys o D-Links ofrecen tarjetas con slots para la conexión de PC-Cards que son los radios que permiten establecer la comunicación con el equipo Access Point.

TARJETAS Y ADAPTADORES IEEE 802.11ª			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
3Com	3CRPAG175	Wireless 802.11 a/b/g LAN PC Card with Xjack antenna	**102.99**
Cisco	AIRPCM35240	Cisco Aironet 340 Series PC Card Adapter w/128 bit WEP	**106.25**
D-Link	DWLA650	WRLS Air Pro PC Card Adapter IEEE 802.11a up to 72 Mbps	**73.95**

IBM	31P9101	Wireless 11 a/b/g 54 Mbps Cardbus Adapter	**96.95**
Linksys	WPC54A	Wireless Card bus Adapter 802.11a 54 Mbps	**65.00**
NetGear	HA311NA	HA311 802.11a Integrated PCI Adapter	**117.25**
Proxim	846005	Orinoco GOLD Combocard 802.11a/b	**76.13**
SMC	SMC2735W	EZ Connect 802.11a Wireless Cardbus Adapter	**25.95**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 4. *Tarjetas PC-Cards y adaptadores PCI 802.11a.*

MODOS DUALES DE OPERACIÓN.

Otra de las características interesantes dentro de un proyecto de redes LAN inalámbricas lo constituye el hecho de que algunos equipos puedan cumplir con más de un estándar de comunicaciones Wi-Fi. Es el caso de algunos fabricantes de dispositivos los cuales pueden ser ensamblados con dos tipos de radio; básicamente que cumplan con la norma IEEE 802.11a y, a su vez, compatibles con la interfaz de radio 802.11b o g.

Por otro lado, ya vimos una de las ventajas de los equipos que cumplen con el estándar 802.11g debido a que opera en la misma banda de frecuencia o espectro del 802.11b, razón por la cual, se pueden describir como si operaran en modo dual aunque en realidad, sólo utilizan una misma interfaz de radio.

Este tipo de proyectos se pueden establecer dentro de escenarios especiales donde prevalezca una determinada norma o estándar de comunicaciones o donde ya se haya realizado una inversión considerable de equipos o elementos a nivel de tarjetas PC Cards, adaptadores PCI en equipos desktops, dispositivos Palms con chipsets 802.11b, etc. Este es el caso, por ejemplo de una Universidad, organismo gubernamental o grupo de departamentos dentro de una corporación y que a su vez, se requiera de algunos grupos de trabajo o usuarios móviles (en el caso de laptops,

PDAs, etc) que necesiten de un mayor ancho de banda para establecer acceso a aplicaciones multimedia, videoconferencia, internet (caso por ejemplo de un departamento de ventas móviles dentro de algún área asignada dentro del campus de la red local), etc.

En estos casos, es conveniente analizar diferentes tipos de alternativas:

Por un lado podríamos utilizar tecnologías de equipos en modo dual que cumplan con las especificaciones de los estándares 802.11b y 802.11a siendo este último el utilizado para incrementar la velocidad de acceso y capacidad de canal de un determinado grupo de usuarios. La desventaja en este caso sería el costo inherente del uso de access Points 802.11a , los cuales representan un incremento en el costo total del proyecto y hay que tener en cuenta ciertas restricciones en cuanto a la distancia que pueden llegar a cubrir (15% menor). Este tipo de implementaciones han sido probadas desde que se ratificaron ambos estándares de comunicación y teniendo en cuenta que sólo se dispone de una versión borrador (draft compliant) del estándar IEEE 802.11g. En la Tabla 5 se muestra un listado de los principales fabricantes que ofrecen equipos Access Points en modo dual 802.11a+b.

EQUIPOS ACCESS POINTs IEEE 802.11a+b

Fabricante	***Referencia***	**Modelo**	**Precio (US)***
Cisco	AIRBR1200BZK	Cisco Aironet 1200 Mode Dual 802.11a/b Access Point	**689.50**
D-Link	DWL7000AP	Wireless Access Point 802.11a/g 54 Mbps	**199.99**
Enterasys Networks	RTB2AB + RBTBFAX	Roamabout Access Point 802.11b + Radio 802.11a	**867.65**
Intel Corp.	WDAP5000AM	Pro Wireless 5000 Lan Dual Access Point	**685.50**

Linksys	WAP51AB	Instant Wireless Dual band Access Point (802.11a + b)	**109.00**
NetGear	WAB102NA	NetGear 802.11a+b dual Band Wireless Access Point	**66.88**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 5*. Access Points Modo Dual IEEE 802.11a+b.*

Otra de las alternativas y que se ha venido imponiendo últimamente con la ratificación del estándar es el uso de dispositivos Access Point 802.11g en modo dual, los cuales operan a 54 Mbps (el troughput real es del orden de 18 Mbps alcanzando velocidades mayores en equipos que operan en modo dual) y que son compatibles con los dispositivos y tarjetas de radio anteriores y que cumplen con el estándar 802.11b certificados por el grupo WiFi. Esta es la tecnología que prevalece y se va imponiendo en el mercado de fabricantes e integradores de tecnologías inalámbricas, puesto que se consigue las ventajas de las normas anteriores (802.11a y 802.11b). En la Tabla 6 se muestra un listado de equipos Access Points que cumplen con el estándar en modo dual 802.11b/g y 802.11a/g.

EQUIPOS ACCESS POINTs IEEE 802.11a+g			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
Apple	M8799LLA	AirPort Extreme Base StationNW 56K and External Connector	**239.88**
Belkin	F5D7130	54G Wireless Network Access Point 802.11 a+g	**174.60**
D-Link	DWL810	Wireless Adapter Access Point 802.11a+g	**149.00**
Linksys	WAP55AG	Wireless A+G Access Point 802.11a/b/g	**211.00**
NetGear	WGT624NA	WGT624 Wireless 802.11g/b 108 Mbps Firewall Router	**111.00**
	WG602NA	NetGear WG602 54 Mbps Access Point (802.11b backward	**87.81**

		compatible).	
Proxim	857005	Proxim Access Point 54 Mbps Harmony	**69.00**
	8658FC	Wireless Ap-600 802.11b/g Upgrade Kit	**99.63**
SMC	SMC2700KIT	SMC EZ Connect 5 GHz 54 Mbps Wireless Networking Starter Kit	**176.99**
Sony	PCWAA500	Sony VAIO 5 GHz Wireless Lan Access Point	**319.41**
TRENDware	TEW411BRP	Wireless 802.11g 54 Mbps Router Access Point	**88.21**
U.S. Robotics	USR8054	US Robotics 802.11g/b 54 Mbps Turbo Router	**94.50**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante*

Tabla 6. *Access Points IEEE 802.11g y 802.11a/g.*

En la evaluación total del proyecto, cada estándar presenta ciertas ventajas y desventajas. No obstante, se deben considerar ciertos parámetros generales y específicos dependiendo del tipo de aplicación, características de implementación en los usuarios (móviles con laptops, PDAs, etc o equipos Desktops con tarjetas PCI Cards para wireless), nivel de escalabilidad en la solución, nivel de eficiencia y rendimiento, alcance o rango de cobertura del equipo (el cual a su vez depende de las características mismas del tipo de solución: in-door o out-door con antenas bien sea direccionales u omnidireccionales con ganancias desde 5 a 8 dBi en adelante), etc.

Otros parámetros de igual importancia son el nivel de seguridad requerido el cual depende a su vez del tipo de emplazamiento y solución que se quiera obtener, el nivel de compatibilidad con otro tipo de redes LAN o el establecimiento de gateways con enlaces MAN/WAN para accesos en banda ancha o el nivel mismo de gestión y adminitración que se requiera conseguir. Cada tipo de solución tiene su mercado cautivo, si bien para el sector de pymes y SOHO ya se encuentran equipos

Access Points con las mismas características robustas de un equipo previsto para el sector corporativo o industrial.

Por ejemplo, en la Tabla 7 se muestra un listado de las soluciones de equipos Access Points de clase empresarial que cumplen con el estándar IEEE 802.11b y que han ganado reputación en el mercado por sus características de operación, funcionalidad y esquemas de seguridad robustos.

EQUIPOS ACCESS POINTs IEEE 802.11b Enterprise-Class			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
Proxim	700001114	Agere Orinoco AP-2000 802.11b Access Point	**900.00**
Cisco Systems	AIRAP350EK9	Cisco Aironet 350 Series 802.11b Access Point	**760.00**
Enterasys Networks	RBTR2-AZ	Roamabout R2 w/MEZANNINE Access Point 802.11b	**793.52**
Intel Corp.	WEAP2011BAK	Intel Pro/Wireless 2011B Lan Access Point 802.11b	**700.00**
Nokia		Nokia A032 Wireless LAN Access Point	**800.00**
Symbol	AP41311050ZIWW	Symbol Espectrum24 High Rate 4131 Access Point	**1099.00**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 7. *Equipos Access Points 802.11b de clase Empresarial.*

Un aspecto interesante a tener en cuenta cuando se analiza determinado estándar de comunicaciones es su capacidad de actualización (upgrade) bien sea por hardware como es el caso de algunos fabricantes que disponen de un slot para el uso de otra tarjeta de radio o bien por software o firmware, tanto en los equipos Access Points como en el cliente (para el caso de tarjetas de radio compatibles). La mayoría de los fabricantes que hemos analizado en el presente documento cuentan

con este tipo de facilidades lo cual respalda la inversión del cliente y asegura un proceso de migración sin mayor impacto en el usuario. Algunas soluciones establecen parámetros como el costo total de propiedad o TCO dependiendo del número de valores agregados con los que cuente un determinado equipo o dispositivo dentro del diseño de la red WiFi.

A nivel de tarjetas PCCards, PCMCIA o adaptadores PCI para desktops, lo que más se ofrece en el mercado son los dispositivos que operan en modo dual a/b o b/g. En el momento, prevalece una tendencia a ofrecer un tipo de tarjeta que cumpla con los tres estándares Wi-Fi de la IEEE, tanto en modo normal como en modo turbo (el cual optimiza el rendimiento y la velocidad de transmisión en la red inalámbrica). En la Tabla 8 se muestra un listado de tarjetas que operan en el modo dual o con las tres interfaces de radio.

TARJETAS Y ADAPTADORES IEEE 802.11ª			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
3Com	3CRWE154G72	OfficeConnect Wireless 802.11g PC Card	**55.22**
Buffalo	WLICBG54A	AirStation 802.11g/b 54 Mbps Wireless Cardbus Card with Ant interface	**57.95**
Cisco	AIRLMC35240	Aironet 350 Series PCI Adapter with 128+ bit	**189.00**
Compaq	191808002	WL 110 Wlan PC Card iPaq Networking 54 Mbps	**90.00**
D-Link	DWLG650	54 Mbps Cardbus 802.11g/b PC Card AirPlus Xtreme G	**49.73**
	DWLAG520	Wireless PCI Adapter 802.11a/g 54 Mbps	**67.00**
IBM	31P9101	Wireless 802.11a/b/g Cardbus Adapter 54 Mbps	**96.95**

Linksys	WMP54G	Wireless PCI G Adapter 2.4 GHz	**57.71**
NetGear	WAG511NA	WAG511 Wireless PC Card 802.11a/b/g	**65.00**
Proxim	8482WD	Wireless 802.11a/b/g PCI Card Gold World	**99.63**
SMC	SMC2336WAG	Universal 2.4/5 GHz Wireless Cardbus Adapter	**74.91**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 8. *Tarjetas PC-Cards y adaptadores en modo dual.*

Para la implementación de un tipo determinado de tecnología o estándar de comunicaciones, cada solución es muy particularizada de acuerdo a los requerimientos del usuario, tipo de aplicación y modo de operación. Para una solución, por ejemplo, que requiera acceso a equipos Macintosh, el Airport Extreme Base Station de Apple o el Belkin 54G Wireless Network Access Point serían los dispositivos adecuados, toda vez que pueden interactuar con este tipo de clientes (sistema operativo). Si se requiere optimizar el enlace de 11 Mbps de las interfaces que operan con tarjetas 802.11b, el Access Point USR2249 de US Robotics presenta un desempeño inmejorable en modo "Turbo" a 22 Mbps aún para distancias del orden de unos 150 m.

Es indudable que el estándar que va a prevalecer es el 802.11g en modo dual y aquí los requerimientos que diferencian una solución de otra tienen que ver con el nivel de compatibilidad con el estándar 802.11a, nivel de seguridad requerido en cuanto a tipo de autenticación de usuarios, filtraje de direcciones IP y direcciones MAC como veremos en el siguiente segmento.

De las tablas anteriores podemos ver diferencias apreciables en precios de algunos fabricantes que presentan soluciones muy robustas para el área corporativa, industrial y para campus de universidades grandes. Es el caso de Cisco, Enterasys Networks, Proxim o el mismo Linksys.

La solución que ofrecen algunos fabricantes como Cisco System o Enterasys Networks para el sector corporativo, es muy modular y podemos adquirir el chasis y los radios 802.11b y 802.11a de manera independiente. De igual forma, también podemos incluir una tarjeta para la encriptación de los datos que cumpla con los estándares WAP (Roamabout 128bit ENCRYPT PC Radio Card US$ 45.00 List Price).

Para el mercado SOHO (Small Office – Home Office), los fabricantes que más destacan son Linksys, Netgear o SMC con una línea bien completa de equipos Access Points y tarjetas; Linksys y U.S. Robotics para equipos de la línea 802.11b. En este tipo de sectores prevalece la inclusión de estándares en modo simple ya que se trata de un número menor de equipos o usuarios móviles. En lo que respecta a las soluciones para el hogar y el Home Office, la idea es poder garantizar la movilidad del usuario a lo largo de toda el área de cobertura sin que esto afecte la seguridad de su información. Aún en estos casos se deben tener en cuenta ciertas reglas para la protección del acceso a su red privada. En este caso también se deben tener en cuenta los equipos gateways que permiten el acceso a redes públicas de datos como la Internet. Fabricantes como NetGear ya han venido posicionando algunos productos muy robustos para este nicho de mercado como el WG602 Access Point 802.11g el cual presenta un throughput de 25 Mbps a una distancia de prueba de 200 m y cuenta con características de seguridad muy buenas para el usuario final.

Para el mercado Pyme se debe considerar como un parámetro a tener en cuenta (aunque no es tan importante) la base instalada de radios en los equipos (tanto portátiles como desktops). El tipo de tarjeta estará determinada por la capacidad de acceso de la red cableada (por lo regular, Fast-Ethernet a 100 Mbps), así que no es tan necesario migrar hacia plataformas de 54 Mbps cuando el backbone de la red todavía opera a 10BaseT. Algunos fabricantes como Belkin, D-Link o el mismo Linksys ofrecen soluciones muy variadas dentro del estándar b a 11 Mbps o en modo turbo a 22 Mbps.

LA SEGURIDAD: REDES WIRELESSLAN CONFIABLES.

Es uno de los aspectos más importantes a tener en cuenta dentro del proceso de aceptación de las nuevas tecnologías inalámbricas en las aplicaciones donde se requiere control dentro de los procesos de conexión y autenticación de los usuarios en la red.

Muchas de las soluciones más robustas que presentan fabricantes de equipos y dispositivos inalámbricos para el sector industrial y corporativo (Enterasys, Cisco, Proxim, Avaya, Linksys, etc), hacen énfasis en el establecimiento de unas políticas adecuadas de seguridad y protección de la información, tanto para soluciones in-door dentro de una oficina como en soluciones out-door para un campus universitario o bloque de edificios.

Las redes inalámbricas son muy vulnerables a los ataques informáticos de un Hacker o pueden ser empleadas de manera maliciosa para obtener permiso a ciertos servicios de la red LAN como es el caso del acceso a la web o a bases de datos, etc.

Con el desarrollo de las últimas técnicas de monitoreo en redes cableadas como el sniffing para el chequeo del tráfico en la red, procesos de spoofing que permiten simular una sesión autorizada de comunicación con el dispositivo activo o bien el empleo de herramientas para hackear un determinado equipo servidor, en el mundo inalámbrico se ha venido generando toda una filosofía de diseño para afianzar aún más el nivel de seguridad dentro de un segmento de red o grupo de usuarios móviles.

Todos los dispositivos WiFi analizados cumplen con protocolos como el WEP (Wired Equivalent Protocol), que permite a través de un algoritmo (40 a 128 bits) establecer una sesión de comunicación segura. Sin embargo, existen herramientas como el Webcrack o el Airsnort que ofrecen un mecanimo de captura de cientos de millones de paquetes con el ánimo de descifrar la información pertinente a una sesión de usuario o login-in. Desde la inclusión del estándar 802.11b en adelante, los principales fabricantes, consorcios y organismos de estandarización han venido

desarrollando algoritmos y técnicas de cifrado más potentes como el filtraje de direcciones MAC, asignación de direcciones IP estáticas para un grupo de usuarios móviles establecidos dentro de una zona desmilitarizada, protocolos como el 3DES o AES de 128, 192 o 256 bits de cifrado, técnicas para el establecimiento de múltiples conexiones encriptadas, etc.

En el mercado se encuentran productos que cumplen con estas especificaciones tanto en los equipos Access Points como en los clientes por medio de un software de configuración de la tarjeta. Muchas de estas políticas de seguridad se pueden implementar directamente en las interfaces de configuración (por lo regular en formato browser http o Java) del equipo Access Point o bien, se hace uso de una conexión a un dispositivo que hace las veces de Gateway o Router para la interconexión entre la red LAN y el equipo de acceso a la Wan (DSL o cable módem).

WEP es un protocolo exigente que limita un poco la velocidad de transferencia de la información debido a sus características de encriptación. Por estas y otras razones, ya se utiliza un nuevo protocolo de encripción como el WAP (WiFi Protected Access) disponible ya con equipos Access Point 802.11g más robusto, eficiente y fácil de inicializar dentro de las aplicaciones del cliente.

Debido a que WEP no es un protocolo lo suficientemente robusto ya que solo permite la autenticación de los clientes y técnicas de cifrado de flujo tipo RC4 que ya han sido vulneradas, este tipo de encriptación y técnicas de autenticación de usuarios se utilizan en equipos Access Points para el hogar y la pequeña oficina donde el nivel de exigencia en cuanto a seguridad no es una prioridad. En este caso el costo de los equipos es menor ya que no se trata de una solución bien robusta que garantice la confidencialidad de la información.

En entornos más exigentes como el campus de una universidad, el área de cobertura de una corporación o empresa con altos estándares de seguridad y protección de la información, en áreas públicas de acceso (hotspots) hacia los

servicios de la web o Intranets que operan con redes virtuales VPNs, se deben contar con equipos y tarjetas que cumplan con otros estándares y servicios adicionales de seguridad como es el caso del manejo de algoritmos de encriptación más robustos como el 802.1x establecido por la IEEE el cual permite hacer un proceso de encripción dinámico por usuario y por sesión, al igual que el establecimiento de políticas para la autenticación mutua entre el equipo Access Point y el cliente.

El IEEE está en proceso de estandarizar un nuevo protocolo conocido como el 802.11i para redes inalámbricas el cual hace uso de asignación de llaves públicas temporal (TKIP) y la idea es afianzar como mecanismo de encripción el nuevo protocolo AES para sus procesos de autenticación y verificación de la integridad de la información. Los nuevos equipos Access Point cumplirían con este estándar y ya hay fabricantes que lo incluyen en sus hojas de especificaciones.

Ya podemos ver en el mercado retail para pequeñas y medianas empresas y aún para el hogar (SOHO) equipos como el Access Point FVM318 Prosafe VPN Security Firewall de NetGear (US $ 1049) el cual provee al usuario de un medio seguro para la encriptación de su información (utiliza protocolo AES de 256 bits) y le permite crear redes privadas al igual que puede utilizarse como router ya que hace uso de un coprocesador diseñado exclusivamente para manejar los procesos de encriptación de los datos.

INTEROPERABILIDAD: COMUNICACIONES WLAN-WIFI INTEGRALES.

Para la conexión de los usuarios a la web, se cuentan actualmente con dispositivos que sirven como gateways entre redes Wireless LAN compatibles, tanto en modo dual como en modo simple y redes de acceso en banda ancha para conexión Wan con redes públicas de datos o enlaces establecidos por proveedores de acceso a Internet ISP como es el caso de interfaces ADSL o Cable módems.

Dentro de los dispositivos para la interconexión de redes hay que destacar tres tipos: a través de un Bridge para la conexión entre la red de cableado estructurado y la red Wireless o para la interconexión entre dos redes inalámbricas WiFi, los gateways que permiten el acceso a la wan mediante interfaces con dispositivos de comunicación y los routers que posibilitan la conexión entre varios dominios de difusión y la creación de redes privadas VPNs tanto para la conexión con redes cableadas como el establecimiento de sesiones entre redes inalámbricas. En la Tabla 9 se muestra un listado de algunos fabricantes que se han destacado en la implementación de equipos inalámbricos que hacen las veces de bridge para la interconexión de redes en un mismo campus o a nivel de Area Metropolitana MAN por medio de soluciones Outdoor. También aquí se debe tener muy en cuenta el nivel de seguridad y estrategia a emplear para el acceso y autenticación de los usuarios y el tipo de estándar con el cual se debe cumplir (IEEE 802.11a,b o g).

En la Tabla 9 hemos destacado las principales soluciones Indoor como Outdoor de los fabricantes más representativos. Existen otro tipo de soluciones que hacen uso de gateways o interfaces con soluciones wlan, es el caso por ejemplo del Aironet 1410 Wireless Bridge de Cisco (AIRBR1410AAK9) el cual tiene un precio de US$ 3408.64 y hace uso de una antena de 22.5 dBi y puede ser interconectado a equipos Access Points por medio de una interfaz.

EQUIPOS WiFi BRIDGE WIRELESS 802.x			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
3Com	3CWE91096A	3Com Wireless LAN Building to Building Bridge	**442.00**
	3CRWE83096A	3Com 11 Mbps Wireless LAN Workgroup Bridge	**209.79**
BreezCOM	872403	BreezCOM SA-10D Wireless Bridge Outdoor	**750.00**

	811501	BB-DS.11D Wireless Remote Bridge 11 Mbps use w/BU-DS.11	**1057.82**
Buffalo	WLAG54	AirStation 802.11g 54 Mbps Wireless Bridge Access Point	**92.77**
	WLAAWCG	AirStation Pro 802.11b 11 Mbps Wireless Bridge Access Point	**116.64**
Cisco	AIRBR350AK9	Cisco 350 Series Bridge 11 Mbps DSSS w/128 bit WEP	**874.37**
D-Link	DWL1750	Outdoor Wireless Bridge/Router 802.11b 11 Mbps	**836.93**
Hawking Technology	WB320	Wireless Bridge 20 usr Workgroup 802.11b	**89.00**
Linksys	WET54G	Wireless-G Ethernet Bridge 802.11g Interface	**134.51**
SMC	SMC2582WB	EliteConnect 2.4 GHz 802.11b Wireless Bridge	**504.00**
Zoom	41300200	ZoomAir Wireless Bridge Kit 11 Mbps Lan to Lan Bridging Syst	**1013.71**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 9. *Equipos WiFi Bridge 802.1x.*

Existen en el mercado otras soluciones Outdoor como el BreezCOM 811501 o el Zoom 413002200 que pueden ser enlazadas a redes Wireless por medio de un equipo gateway o interfaz en un equipo Access Point con tales prestaciones. En un proyecto outdoor de este tipo hay que considerar el rango de cubrimiento y la velocidad de acceso requerida para brindar un adecuado nivel de calidad y servicio.

En cuanto a los equipos Access Points que hemos analizado, un equipo como el Cisco 350 Series cumple con todas las especificaciones de seguridad en cuanto a compatibilidad con protocolos como el WAP/LDAP, IPSec, etc. Este equipo permite hacer filtraje de direcciones IP y filtraje de direcciones MAC, cumple con el estándar 802.1x y permite la creación de redes VPNs.

Hoy en día es muy frecuente ver en los web sites de los fabricantes que se ofrece todo tipo de equipos para la interconexión con redes LAN inalámbricas, bridges para la comunicación con otras redes (cableadas o inalámbricas) y dispositivos de acceso a redes de banda ancha para la conexión con redes públicas de datos o proveedores de acceso a Internet ISP.

La conectividad y la interoperabilidad son dos parámetros bien importantes dentro de las redes LAN que cuentan con un acceso a una red pública de datos como la Internet o que realizan todos sus procesos de conexión con una red privada de conmutación de paquetes tipo X.25, xDSL o RDSI a través de un proveedor de servicios. El costo total de un proyecto Wireless debería tener en consideración el tipo de compatibilidad a nivel de acceso con este tipo de redes de banda ancha. Algunos equipos Access Points cuentan con una interfaz o gateway de acceso para la conexión de una red pública (o privada) de datos. Otros fabricantes ofrecen equipos Routers y bridges con acceso a redes de banda ancha cableadas o a redes totalmente inalámbricas mediante la conexión de antenas especiales con línea de vista.

Hay algunas consideraciones que se deben tener en cuenta a la hora de elegir entre un equipo Wireless Bridge o un Router que sirva como pasarela entre la red WiFi y el equipo de acceso WAN. La recomendación es utilizar gateways/routers con funciones inalámbricas que cumplan con el estándar 802.11g por su mayor compatibilidad con los otros estándares. El equipo Belkin 802.11g DSL/Router, por ejemplo, viene equipado igualmente con 4 puertos Fast-Ethernet y permite una configuración fácil. Por otro lado, en una red wireless 802.11a se requiere que el gateway o el router opere en modo dual o sea compatible con los tres estándares. Un equipo como el Linksys WRT55 a+b Router es catalogado como genérico para ser implementado en cualquier tipo de red WiFi.

Dentro de los aspectos que se deben considerar en un adecuado proceso de compra para equipos Gateways/Routers o aún Wireless Bridge, tenemos el de poder contar con un proceso de detección automática de los clientes y métodos de

conexión Wan. Los equipos de altas prestaciones cuentan con un Firewall interno y servicios de traslación de direcciones NAT, se debe proveer Stateful Packet Inspection (SPI) y características de filtraje URL de contenido a la Web.
Un aspecto interesante lo consituye el nivel de respaldo, servicio y tiempo de garantía. La mayoría de los equipos analizados ofrecen una garantía de tres años lo cual protege el nivel de inversión, sobre todo en ambientes operativos bastante exigentes o con conexión Outdoor a una red de área metropolitana.

En la Tabla 10 se muestra un listado de equipos que hacen las veces de Gateways o Routers tanto para soluciones Indoor como Outdoor y que pueden estar integrados directamente en un dispositivo Access Point. Muchas veces, ambos tipos de equipos realizan funciones similares por lo que esto se presta para confusión dentro del proceso de integración con plataformas de acceso Wlan. No hay que olvidar que el costo depende del tipo de funcionalidad que tengan, por ejemplo, si se utiliza un equipo bridge para conectar a un servidor de impresión o establecer conexión con una red cableada.

EQUIPOS WiFi GATEWAY/ROUTERS WIRELESS 802.x			
Fabricante	***Referencia***	**Modelo**	**Precio (US)***
3Com	3CRWE554G72US	OfficeConnect Wireless 802.11g Cable/DSL Gateway	**85.94**
Adaptec	2012600	Adaptec Wireless 802.11b Cable/DSL Router 4 Ptos Kit	**98.83**
	WLMRL11G	AirStation Pro Plus 802.11b 11 Mbps Wireless Router AP	**213.74**
Cisco	AIRBR1410AAK9	Aironet 1410 Series Wireless Bridge	**1399.0**
D-Link	DI774	Router 802.11a/802.11g	**199.99**
	DWL1750	Outdoor Wireless Bridge/Router 802.11b 11 Mbps	**836.93**
Hawking	WR304S	Wireless Broadband Router/AP	**129.75**

Technology		4 Ptos 10/100 Switch IEEE 802.11b	
Linksys	BEFW11P1	Ethernet Wireless AP Plus Cable/DSL Router with Print Server	**205.00**
NetGear	FWAG114NA	FWAG114 ProSafe Dual Band Wireless VPN Firewall	**250.09**
Proxim	700002486	Orinoco or-500 Remote Outdoor Router	**456.95**
SMC	SMC7004WFW	Wireless Cable/DSL Broadband Router Access Point 802.11g	**164.41**
U.S. Robotics	USR8011	USR Wireless Cable & DSL Router	**75.00**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 10. *Equipos Gateway/Routers Wireless 802.1x.*

La diferencia de precios con respecto a un router depende de las características mismas de la solución bien sea como gateway de acceso a redes de área amplia o como elemento de interconexión entre dos segmentos de red totalmente independientes. Avaya, por ejemplo, ofrece un equipo Access Point como el 300 Router (2) 10/100 ISDN S/T (AP-300-ST) por US$ 2.389,oo único en su clase ya que ofrece conexión a redes RDSI y sirve como pasarela para redes wireless LAN.

SOLUCIONES: VALOR AGREGADO DE LAS TECNOLOGIAS WiFi

En el ámbito corporativo se habla de soluciones de valor agregado teniendo en cuenta las diferentes prestaciones que puede tener un determinado equipo o elemento de conexión a una red. En el mundo wireless LAN se cuentan con diversos tipos de solución de acuerdo a las características mismas de los usuarios, tipo de acceso, costo vs beneficio y grado de confiabilidad.

Algunos fabricantes e integradores se han especializado en la implementación de equipos y dispositivos complementarios que permiten obtener un mayor nivel de

prestación dentro de los parámetros establecidos por un determinado estándar de comunicaciones. Empresas como Hawking Technologies ofrecen antenas de largo alcance (1.5 millas o más), Cisco ha integrado toda su estrategia wireless con su sistema operativo de red IOS y ofrece la gestión de toda la red inalámbrica dentro de los servicios del paquete CiscoWorks, U.S. Robotics ha implementado equipos Access Points que permiten ofrecer una velocidad de transmisión cercana a los 100 Mbps que es la capacidad establecida para redes cableadas Fast-Ethernet, algunas otras empresas como Proxim ofrecen dispositivos especiales para la conexión de redes de acceso WAN o redes de Area Metropolitana en donde los equipos no tienen que tener necesariamente línea de vista.

En la Tabla 11 se muestra un listado general de las diferentes tipos de antenas que podemos encontrar en el mercado WiFi tanto para soluciones Indoor como antenas especiales de alta ganancia (15 dBi en adelante) para la interconexión con dispositivos gateways en soluciones Outdoor punto-punto o punto-multipunto. En este tipo de soluciones hay que considerar el nivel de potencia y características del arreglo de antenas para conseguir el área de cobertura deseada.

En el análisis de los tipos de soluciones tenemos un parámetro importante como es la diversidad de la antena, ganancia y tipo de cobertura (direccional, omnidireccional, patrón de arreglo, etc). La mayoría de los equipos Access Points utilizan antenas de 2.2 dBi y pueden hacer uso de un procedimiento de ampliación para la conexión con un equipo que haga las veces de gateway.

Una característica interesante de algunos routers y Bridges wireless es el disponer de un conector adicional para la conexión de una antena externa, lo que permite incrementar el alcance de cobertura o calidad de la señal (70% aprox). Es el caso, por ejemplo del equipo Buffalo AirStation WBR-G54 el cual dispone de un conector auxiliar para antena externa de mayor ganancia tanto direccional como omnidireccional.

ANTENAS PARA EQUIPOS WiFi			
Fabricante	**Referencia**	**Modelo**	**Precio (US)***
BreezCOM	901916	16 dBi Directional Antenna with 3 ft Cable type N	**85.79**
	811938	8 dBi Omnidirectional High Performance Antenna (Outdoor)	**104.76**
Buffalo	WLENDR	AirStation 2.4 GHz Indoor Omnidirectional Antenna	**48.64**
Cisco	AIRANT5959	Cisco Aironet Antenna 2.0 dBi diversity OmniCeiling Mount	**187.91**
D-Link	ANT241400	D-Link 14 dBi Directional Outdoor Ant	**119.00**
Hawking Technology	H-AI6SIP	Omnidirectional 6 dBi Antenna 2.4 GHz wlan SMA connector	**29.00**
Intel	WLANT2139WW	Intel YAGI Antenna kit for 802.11b 13.9 dBi 2.4 GHz	**404.22**
Proxim	5054PA18	18 dBi Panel Antenna 5.25-5.875 GHz	**81.50**
SMC	SMCANTCEILINGBOX	2.4 GHz High Gain Antenna Ceiling EZ connect Box kit (outdoor)	**811.95**
TRENDware	TEWIA06D	TRENDnet 6 dBi wireless directional Indoor Antenna	**29.00**

* *El valor que se tomó como referencia es el precio de Lista del Fabricante.*

Tabla 11. *Dispositivos de Antenas para equipos WiFi (Indoor y Outdoor)*

Algunos dispositivos se comportan mejor con el uso de tarjetas PCCards y adaptadores del mismo fabricante y estándar IEEE, aunque esto no es una regla general y se aprecian algunos dispositivos compatibles con fabricantes no regulares en el mundo wireless. Esto es un factor bien importante a tener en cuenta sobre todo por el tipo de software de configuración (se ofrecen kits o bundles de conexión que

permiten cubrir todo el diseño o solución específica de acuerdo a los requerimientos del usuario).

Uno de los inconvenientes en el caso de tarjetas adaptadoras es su ubicación en el PC por lo que algunos fabricantes han optado por ofrecer soluciones de antenas externas en adaptadores Wireless-USB de alta ganancia (del orden de unos US$ 90) el cual no es más que un adaptador de red USB-WiFi al que se le ha añadido una antena direccional. Uno de estos equipos es el NetGear MA101 que cuenta con un adaptador de este tipo.

Uno de los fabricantes que destacan en la implementación de soluciones de ampliación para antenas es Hawking Technologies el cual dispone de equipos como el H-AO14SD que cuenta con una solución de antena de alta ganancia (14 dBi) direccional para un emplazamiento Outdoor con un lóbulo de cobertura de 30 grados.

Este tipo de soluciones vienen equipados con un kit que cuenta con un cable del orden de unos 3 m de tal manera que en la parte del servidor, conectamos la antena con un equipo Access Point de altas prestaciones y del lado del cliente conectamos la antena direccional de alta ganancia con un equipo que hace las veces de bridge el cual viene equipado con puertos de conexión Fast-Ethernet.

Hay que tener en cuenta el tipo de conectores utilizados para el emplazamiento de tales antenas. Cisco y Linksys ofrecen soluciones con conectores tipo RP-TNC mientras que otros fabricantes ofrecen conexiones con interfaces tipo RP-SMA . No obstante, también se encuentran adaptadores TNC – SMA.

Dependiendo del tipo de proyecto hay que analizar el nivel de potencia y ganancia de la antena, tipo de conexión a un Access Point o Router de acceso a la Wan, características de las tarjetas instaladas, tipo de emplazamiento o nivel de alcance requerido y, por supuesto, compatibilidad entre los equipos considerados.

Hawking Technologies cuenta también con soluciones como el H-A16SI que es una antena omnidireccional de 6 dBi de ganancia, la cual se utiliza para mejorar el

nivel de alcance y evitar zonas muertas de recepción de acuerdo al tipo de instalación. En aquellos casos que se requiere una solución punto a punto direccional, Hawking ofrece el H-A16SD (US $ 30.oo), la cual cuenta con un patrón de radiación del lóbulo de 80 grados.

SOLUCIONES PUNTO-PUNTO Y PUNTO-MULTIPUNTO.

Las soluciones punto-punto o punto-multipunto pertenecen al mundo wlan y si bien se pueden catalogar como soluciones WiFi, estamos hablando también de otro rango de frecuencias no estandarizado. En materia de conectividad, se han venido imponiendo dos tipos de estándares para conexión punto-punto o punto-multipunto, las cuales hacen uso de antenas de alta ganancia y directividad. Este tipo de emplazamiento se utilizan para zonas públicas de servicio o puntos de acceso (Hot Spots) como Aeropuertos, Coffee Shops, parques públicos, etc.

Ya hay en el mercado varios fabricantes que proveen soluciones inalámbricas de banda ancha (11-960 Mbps) para transmisión de datos, voz (con conexión a centrales telefónicas PBX) y video multimedia. La idea central es expandir la capacidad de transmisión de redes tradicionales interconectadas por enlaces de alta velocidad E1/T1 o mediante fibra óptica (OC-3).

Una gran aplicación de este tipo de soluciones es proveer acceso de última milla mediante puntos de presencia o acceso a los servicios que ofrece un ISP tradicional o los servicios que puede llegar a prestar un proveedor de red inalámbrica con conexión a redes inalámbricas WiFi. Lo que se requiere es poder captar nuevas oportunidades de negocio haciendo uso de una red totalmente inalámbrica Wireless LAN/WAN de fácil y rápida implementación con respecto a las redes cableadas, con posibilidades de administración remota de tal forma que haya una verdadera reducción en los costos de operación.

Las aplicaciones son muy variadas y van desde sistemas de vigilancia y seguridad a nivel de red de área metropolitana, backbones de enlace entre campus de edificios, acceso en banda ancha a la web por parte de los operadores, etc. Este

tipo de redes tienen la ventaja de proveer control de ancho de banda tanto simétrico como asimétrico, lo cual permite implementar soluciones bastante robustas y flexibles al mismo tiempo.

En la Figura 1 se muestra un enlace de conexión punto a punto entre varias localidades los cuales hacen uso de equipos especiales para la interconexión de redes wireless LAN. Muchos proveedores de acceso inalámbrico WISPs utilizan este tipo de conexiones.

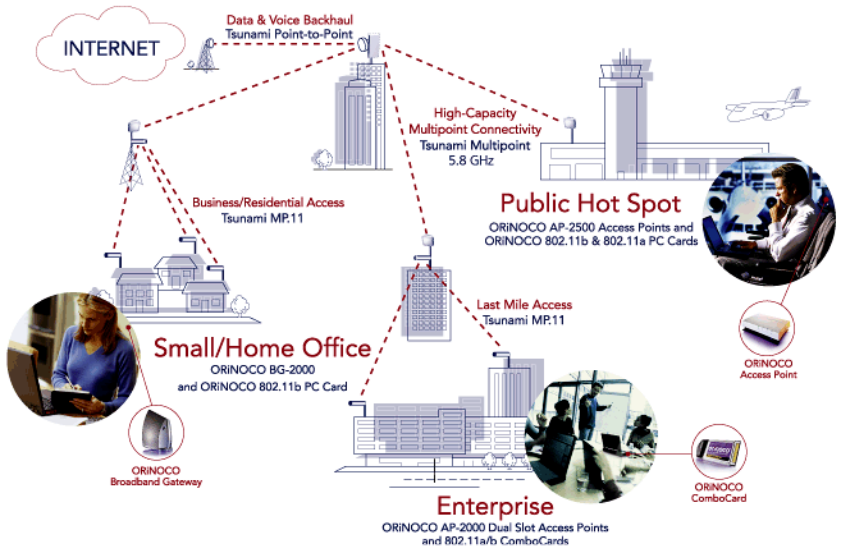


Figura 1. *Conexión Punto a punto entre redes Wlan (Cortesía de Proxim Corp).*

Este tipo de soluciones son provistas para enlaces de amplia cobertura y cumplen con estándares ya establecidos. Algunos equipos cumplen con nuevos protocolos como el Wireless Outdoor Router Protocol (WORP) que garantiza un mejor desempeño en ambientes con altos requerimientos de ancho de banda.

Hay que tener en cuenta el grado de movilidad conseguido con este tipo de implementaciones dentro de la red wireless mediante técnicas de roaming entre las redes inalámbricas o mediante el uso de gateways o routers de banda ancha.

Para el mercado SOHO y Home Office se hace uso de soluciones puntuales de este tipo o conexiones con Gateways de acceso a redes públicas como la Web. En la Figura 2 se muestra un diseño básico de conexión para un grupo de usuarios que requieren del servicio wireless con conexión punto –multipunto.

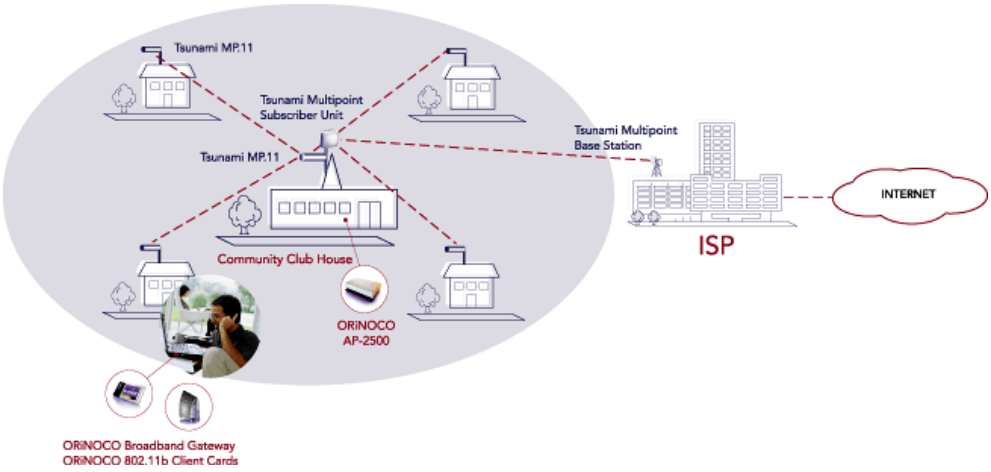


Figura 2. *Conexión Wireless Punto-Multipunto SOHO y Home Office (Cortesía de Proxim Corp).*

Para la conexión a la web se puede hacer uso de este tipo de redes como solución de última milla a un centro de servicio u oficina ISP. Empresas como Proxim con equipos como el **Tsunami MP.11A Base Station** (US $809.11) ofrecen este tipo de soluciones, si bien ya están apareciendo equipos de este tipo con otros fabricantes. En este sentido, los equipos Wireless Bridge desempeñan un papel muy importante en la interconexión de redes y acceso compartido a la Internet, por lo regular mediante enlaces tipo Cable-módem o dispositivos Routers xDSL.

A nivel de soluciones Outdoor, fabricantes de nivel corporativo como Cisco con su equipo Aironet 1400 Series Wireless Bridge soporta aplicaciones punto-punto o punto-multipunto y se utilizan para brindar servicios de amplia cobertura y troughput con enlace wireless 802.11a de 54 Mbps. Este tipo de equipos utiliza mecanismos de seguridad mejorados y servicios basados en los estándares 802.1x y WAP.

También hay fabricantes que utilizan sus equipos Access Points con antenas especiales de alta ganancia para brindar soluciones Outdoor de amplia cobertura. Por ejemplo, Enterasys Networks hace uso de su equipo Roamabout 1200 AP y

antenas de alta ganancia para cubrir un amplio sector dentro de un campus de edificios o bien, utiliza lo que denomina su “Plataforma de Acceso” Roamabout R2 con diversos tipos de radios (802.11a y b) y diversidad de antenas para cubrir zonas más distantes dentro de un área metropolitana.

La idea central en este tipo de proyectos es permitir soluciones flexibles con antenas internas o externas de alta ganancia y directividad (las cuales pueden provenir de otros fabricantes). Se pueden utilizar para proveer enlaces redundantes con conexión a líneas de alta velocidad tipo E1/T1. Equipos como el Cisco Aironet 1400 o el Proxim Tsunami MPA.11 pueden proveer soluciones de backup para enlaces cableados primarios con conexión por fibra óptica.

Dentro de las aplicaciones que hacen uso de estos tipos de equipos tenemos:

Gobierno. Los cuales se utilizan como backbone para redes municipales metropolitanas.

Educación. Para la interconexión de edificios y escuelas a Centros de Servicios, capacitación o bibliotecas.

Salud. Para ofrecer un amplio cubrimiento entre redes de hospitales, clínicas y Centros de Salud en áreas metropolitanas.

Corporativo. Para la interconexión de redes entre edificios.

Hoteles y Aeropuertos. Se utiliza hoy en día la palabra “hot spot” para definir un área de servicio pública que implementa una red inalámbrica con conexión a redes de banda ancha. En el caso de los hoteles y aeropuertos esto puede ser un valor agregado dentro de los servicios que se ofrecen para la conexión a la web o a bases de datos propias como reserva automatizada de tiquetes, confirmación, sitios turísticos dentro de una ciudad, etc. Hay una necesidad bastante grande en materia de soluciones por software y aplicaciones para este tipo de mercados.

Los equipos Wireless Bridge se pueden requerir dentro de un proyecto que requiera de los servicios de distribución de alta velocidad y acceso a redes de área amplia y gran ancho de banda o bien, se pueden utilizar como gateways para la conexión con proveedores de Servicios y aplicaciones.

Los servicios de interconexión punto a punto o punto-multipunto ofrecen un alto rendimiento y disminuyen el costo total de propiedad TCO, al igual que desempeñan un importante papel en el retorno de inversión dentro de un proyecto de interconexión de redes en comparación con las redes dedicadas. Hacen uso de la banda no regulada de los 5.8 GHz con radios de 24 dBm (250 mW) y conexión con redes wireless 802.11x. El nivel de alcance en estos sistemas es de 7.5 millas para redes punto a punto y de 2 millas para redes punto-multipunto, si bien con el uso de sistemas de antenas de alta ganancia se puede extender el rango de alcance a áreas que cubran los 35 Km equivalentes a un área de cobertura celular.

Una característica importante dentro del costo total de un sistema multipunto es que podemos incrementar el ancho de banda y troughput requerido con el uso de múltiples Wireless Bridges mediante el empleo de canales Ethernet Fast, protocolos para la agregación de puertos (Pag-P) o protocolos de enrutamiento. Igualmente los servicios de red se pueden segmentar basados en los requerimientos del usuario final.

Hay que tener en cuenta un adecuado diseño para el montaje de las antenas de acuerdo a su ganancia y tipo de polarización. Este tipo de dispositivos cuentan con arreglos de montaje multifuncionales para poder hacer un diseño basado en la polarización (vertical u horizontal) de la antena. El costo de un instalado experto es representativo dentro de un proyecto Wireless para una solución Outdoor de amplia cobertura.

EL FUTURO DE LAS REDES WIFI: LA INTEGRACIÓN DE SERVICIOS.

Con la implementación de nuevos estándares de comunicación para redes de área amplia como el UWB (Ultrawide Band) o más conocido como IEEE 802.15 e integración de las redes wirelessLAN con los servicios que ofrecen las redes wlan de celulares GSM/GPRS o CDMA 1xRTT y equipos de tercera y cuarta generación, el futuro de la movilidad en red dependerá del tipo de convergencia que se logre con estas tecnologías.

Las soluciones de acceso a la web y los servicios de interconexión de última milla que ofrecen algunas compañías proveedoras u operadores de redes inalámbricas, han generado un incremento en los puntos de acceso (hotspots) provistos por los integradores WiFi y las compañías proveedoras de redes celulares. Tenemos el caso, por ejemplo, de empresas como Nokia y Ericsson las cuales ofrecen PC Cards y módems con doble funcionalidad: proveen servicios WiFi en redes 802.11x y sirven para conexión con redes WANs GPRS/CDMA tanto para dial-up o como acceso a la web.

El costo de estas soluciones depende del tipo de integración que se logre entre múltiples tecnologías inalámbricas, incluyendo bluetooth y UWB para el caso de redes PAN (Personal Area Network). La inclusión de varias tecnologías en un solo dispositivo le permitiría al usuario móvil estar siempre conectado a la red, bien sea mediante un proveedor de acceso Wan a través de una red privada virtual o VPN o bien, mediante un proceso de roaming en el cliente, estableciendo una sesión de comunicaciones WiFi wireless con equipos de red 802.11x.

Algunos fabricantes ya han empezado a implementar este tipo de dispositivos como el Wireless Any-network Digital Assistant (WANDA) de Texas Instruments que es un handheld que opera en redes 802.11b, bluetooth y con redes GSM/GPRS; de tal manera que el usuario pueda surfear en la web mientras atiende una llamada celular de algún operador GSM.

Por ahora la tendencia es a manejar dos tipos de redes que puedan trabajar en paralelo e integradas dentro de un dispositivo multifuncional que pueda operar con los protocolos respectivos. La idea central de todo esto es tener equipos PDAs y laptops con tarjetas PC-Cards especiales capaces de detectar la mejor red (Wlan/WiFi) en términos de velocidad (troughput) y rango de cubrimiento.

En términos de servicio y cobertura a nivel de operadores o agentes de servicio, estaríamos hablando de una verdadera convergencia entre las redes celulares de amplia cobertura pero ancho de banda limitado (384 Kbps en redes 2.5G), las redes de área amplia con anchos de banda muy superiores y las redes de área metropolitanas MAN que operan a través de puntos de acceso para la comunicación con redes locales interconectadas con equipos Access Points. Es indudable el crecimiento exponencial que han tenido los hotspots o puntos de acceso a redes móviles de área metropolitana al igual que las diferentes soluciones punto-multipunto de operadores o Proveedores de Acceso a la Web inalámbricos WISP, tanto en Norteamérica como en algunos países de Europa y Asia. Es el caso del operador T-Mobile que provee una cadena de hotspots para Starbucks Coffe el cual ofrece los servicios de Wlan y WiFi por una tarifa única mensual para voz y datos.

Otro ejemplo es el de Cometa Networks que es una compañía creada por un consorcio de empresas como AT&T, IBM e Intel, la cual tiene como meta construir 20.000 hotspots para finales de 2004 en los 50 mercados más grandes de los EEUU o está el caso de la cadena de hoteles Marriot International con 400 hotspots en los EEUU, Reino Unido y Alemania. Todos estos operadores ofrecen servicios de acceso de alta velocidad a la web, y hacen uso de partners con otros operadores de redes WiFi, concepto que ya se conoce con el nombre de Agregadores (Aggregators).

En América Latina se cuentan con muy pocos proveedores y operadores de servicios Wlan para puntos de acceso, es el caso por ejemplo de Hotspot International o de algunos operadores de telefonía móvil celular que han venido

integrando servicios WiFi en sus redes. Tal vez esta sea la tendencia futura del mercado.

En la Tabla 12 se muestra una lista sobre la tarifa mensual que cobran en promedio los operadores de redes Hotspots por la utilización de las redes, por parte de los usuarios que accesan los servicios ofrecidos. Se destacan los planes combinados de acuerdo a los requerimientos de los clientes móviles.

PROVEEDOR DE ACCESO WiFi PARA REDES HOSTPOTS	
Operador	**Tarifa Mensual (Plan de Costos)**
AT&T Wireless	US$ 9.99 por día para uso ilimitado; US$ 69.00 por mes para uso ilimitado desde cualquier lugar que opere la red.
Boingo	US$ 7.95 por dos días para uso ilimitado desde una localidad específica; US$ 7.95 por cada día adicional; US$ 39.00 por mes para uso ilimitado desde cualquier lugar (US$ 29.00 para los primero doce meses)
Ipass	Variable de acuerdo al plan de cada compañía o lugar donde se ofrezca el Access Point.
T-Mobile	US$ 0.10 por minuto para un mínimo de 60 min desde cualquier sitio; US$ 29.00 por mes para uso ilimitado desde cualquier Access Point (se debe realizar un contrato a un año).
Telia HomeRun	US$ 12.00 por día para uso ilimitado desde cualquier Access Point; US$ 19.00 por mes más US$ 0.29 por minuto desde cualquier punto (contrato a un año).
WayPort	US$ 6.95 para uso ilimitado hasta medianoche desde cualquier aeropuerto donde haya cubrimiento; US$ 29.00 por mes para uso ilimitado desde cualquier Access Point (contrato a un año).

Tabla 12. *Tarifa Mensual que cobran los Operadores Wireless WAN.*

Ya se han venido integrando otro tipo de tecnologías a los servicios que ofrece una red WiFi tanto para el sector del entretenimiento como el sector industrial. Desde dispositivos manos libres, equipos de video y audio con tecnología bluetooth interconectados a la red del hogar mediante sistemas wlans, hasta sensores de temperatura controlados por control remoto, el campo de aplicaciones que está por desarrollarse es ilimitado.

APENDICE E: ANALISIS COSTO – BENEFICIO REDES ALAMBRICAS VRS INALAMBRICAS

PRESUPUESTO PARA IMPLEMENTAR UNA RED CABLEADA O INALÁMBRICA CON UNA CANTIDAD DE 22 COMPUTADORAS.

PRESUPUESTO PARA UNA RED CABLEADA.

Cantidad	Dispositivo	Precio unitaro	Total
1	Switch 24 puertos	$ 80.00	$ 80.00
22	Tarjetas 10/100	$ 25.00	$ 550.00
100	Conectores macho rj 45	$ 0.40	$ 40.00
22	Conectores hembra rj 45	$6.00	$ 132.00
22	Cañuela con adhesivo	$10.00	$ 220.00
3	Bobina cable UTP categoría 5 ó 6	$60.00	$ 180.00
40	Patch cord de 6''	$3.00	$ 120.00
1	Rack patch panel	$ 180.00	$ 180.00
1	Mano de obra	$500.00	$ 500.00
		Costo Total	$ 2002.00

** Los precios incluyen iva*

PRESUPUESTO PARA UNA RED INALÁMBRICA.

Cantidad	Dispositivo	Precio unitario	Total
1	Access Point	$ 450.00	$ 450.00
22	Tarjetas	$45.00	$ 990.00
1	Mano de Obra	$300.00	$300.00
		Costo Total	$1740.00

** Los precios incluyen iva*

COSTO - BENEFICIO

COSTO

Como se observa en los cuadros anteriores la implementación de la red alambrica es un trece porciento más caro que la red inalámbrica incluyendo mano de obra, esto con relación al costo.

BENEFICIO

Los beneficios de la red inalámbrica con respecto a la alambrica es la movilidad de los usuarios en la empresa y la escalabilidad de la red misma, esta posibilidad de desplazamiento físico puede conducir a un incremento de productividad.

Esta tambien ocupa un espacio menor ya que se utilizan menos materiales en su implementación.

Otro beneficio es al momento de crecimiento de la empresa, dichos crecimientos ocacionan que la empresa busque mayores espacios fisicos o una mayor infraestructura, lo cual es una ventaja para las WLAN ya que se pueden mover sin ningún problema o sin desperdiciar materiales tales como cañuelas, cableados, puntos de red en la pared, etc.

En conclusión se puede afirmar que el analisis de costo – beneficio hoy en día es mucho más favorable al implementar una red inalámbrica que una alambrica.

LEXINCORP
SERVICIOS LEGALES INTERNACIONALES
WWW.LEXINCORP.COM

San Salvador 20 de Septiembre de 2006

Señores
Universidad Don Bosco
Presente

Por este medio hacemos constar que el grupo de alumnos comprendido por **CARLOS ALBERTO MEJÍA AGUILAR, RAÚL AMILCAR MOLINA LÓPEZ y EDUARDO EULISES ORELLANA MULATO** quienes trabajaron en esta empresa en el proyecto de tesis llamado **"IMPLEMENTACION DE UNA INTRANET SEGURA PARA LA EMPRESA LEXINCORP S.A. DE C.V. CON TECNOLOGIA INALAMBRICA Y SEGURIDAD DE ACCESOS"** han cumplido satisfactoriamente con los objetivos estipulados y con las necesidades que la empresa tenía, por lo cual se extiende esta constancia de satisfacción a los veinte días del mes de septiembre de 2006.

LEXINCORP, S.A. DE C.V.

Lic. Aida de Magaña
Gerente Administrativo

GUATEMALA
Tel.: (502) 2337-1819
Fax: (502) 2333-5334
15 calle 1-85 zona 10
Ciudad de Guatemala

EL SALVADOR
Tel.: (503) 2263-0503
Fax: (503) 2263-0601
71 Av. Norte y 3a. Calle Pte.
No. 3698, Col. Escalón
San Salvador

HONDURAS
Tel.: (504) 553-0578
Fax: (504) 553-2411
Plaza Cibeles #14 y 15
6 calle, 17 avenida S.O
San Pedro Sula

NICARAGUA
Telefax: (505) 278-7935
Del Restaurante La Marsellesa
1½ Cuadra al Norte No. 57,
Managua

COSTA RICA
Tel.: (506) 232-4000
Fax: (506) 232-2569
Barrio Nara, de la CNFL
300 oeste, 150 sur, Sabana S.O.
San Jose

UNA REGIÓN, UNA FIRMA