



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERIA**

**“DISEÑO E IMPLEMENTACIÓN DE UN ENLACE
INALÁMBRICO PARA LA JUNTA LOCAL EJECUTIVA
DEL ESTADO DE DURANGO DEL IFE (ACTUAL INE)”**

TRABAJO PROFESIONAL
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN TELECOMUNICACIONES

PRESENTA:

CARLOS FERNANDO MENDOZA PÉREZ

ASESOR

DR. VÍCTOR GARCÍA GARDUÑO

CIUDAD UNIVERSITARIA

SEPTIEMBRE 2014

Agradecimientos.

Con todo mi cariño y mi amor para mis padres, que hicieron todo en la vida para que alcanzara mis sueños, nunca dejaron de motivarme y estrecharme la mano cuando creía que el camino se acababa, a ustedes por siempre mi corazón y agradecimiento.

A tu paciencia, comprensión y sobretodo amor, preferiste sacrificar una gran parte de tu tiempo para que pudiera cumplir con mi sueño. Con tu bondad y sacrificio, lograste inspirar y volverme una mejor persona. Este trabajo tiene mucho de ti, gracias por estar siempre a mi lado, Valeria.

ÍNDICE

INTRODUCCIÓN	8
--------------------	---

Capítulo I Instituto Federal Electoral

1.1 Misión	10
1.2 Historia	10
1.3 Estructura orgánica del IFE	11
1.3.1 Órganos Directivos.....	11
1.3.2 Órganos Técnico – Ejecutivos.....	12
1.3.3 Órganos de Vigilancia	13
1.4 Estructura Organizacional del Instituto Federal Electoral	13
1.4.1 Direcciones Ejecutivas	14
1.4.2 Unidades Técnicas.....	14
1.4.3 Organismos Desconcentrados	15
1.5. Unidad de Servicios de Informática (UNICOM)	15
1.5.1 Misión.....	17
1.5.2 Visión	17
1.5.3 Estructura de la Unidad de Servicios de Informática.....	18
1.5.4 Estructura Dirección de Operaciones.....	20
1.5.5 Estructura Subdirección de Comunicaciones.....	20
1.5.6 Departamento de Operación de la Red.....	21

Capítulo II Puesto de Trabajo y Proyectos

2.1 Descripción del Puesto de Trabajo.....	24
2.2 Proyectos, Participación y Logros Alcanzados dentro de la Institución.....	24
A. Monitoreo Proactivo (2008-2014)	24

B. Balanceo de tráfico en los enlaces primario y secundario de las Juntas Distritales (2014)	25
C. Diseño, Implementación, y Puesta en Operación de un Control de Acceso a la Red para la Macrosala de Prensa en las Elecciones Federales 2009 y 2012	25
D. Diseño, Implementación, y Puesta en Operación de un Radioenlace Punto a Multipunto para la Feria de Medios en el Proceso Electoral Federal 2012	26
E. Implementación de la tecnología WPA2 para la red inalámbrica del IFE en Oficinas Centrales y en sus respectivas Juntas Locales. (2014)	26
F. Diseño, Implementación, y Puesta en Operación de los servidores de autenticación para la Red Inalámbrica del IFE con esquema de alta disponibilidad y replicación automática. (2009)	27
G. Diseño e Implementación de un Sistema de Dominio Inalámbrico (<i>WDS, Wireless Domain System</i> , por sus siglas en inglés) en cada segmento de administración de los equipos de acceso inalámbrico. (2011)	28
H. Ampliación de cobertura de la Red Inalámbrica en las vocalías de Registro Federal de Electores en 11 Estados de la Republica (2013)	28
I. Separación de la Red Inalámbrica de Usuarios de las Juntas Locales Ejecutivas con la de usuarios de red cableada (2013)	29
J. Robustecimiento de la Red de los complejos “Quantum” y “CECYRD” en Distrito Federal y Pachuca respectivamente del Registro Federal de Electores (2013-2014)	30
K. Implementación de una herramienta para monitorear el servicio activo de <i>DHCP</i> en cada sitio de Oficinas Centrales y Registro Federal de Electores (2013)	30
L. Implementación de la herramienta de monitoreo <i>WLSE (Wireless LAN Solution Engine)</i> para los equipos de acceso inalámbrico (2010).....	31
M. Implementación de un nuevo SSID para el conjunto de equipos de acceso inalámbrico del Instituto Nacional Electoral (Actual)	31
2.3 Otros Proyectos y Actividades.....	32

Capítulo III

Redes Inalámbricas

3.1 Antecedentes	33
3.2 Transceptores	34
3.3 Topologías.....	34

3.3.1 Redes Ad-hoc	34
3.3.2 Redes Infraestructura.....	35
3.3.3 Radioenlaces o Enlace Inalámbrico	36
3.4 Modelo OSI	¡Error! Marcador no definido.
3.4.1 Capa de Física	¡Error! Marcador no definido.
3.4.1 Capa de Enlace.....	¡Error! Marcador no definido.
3.4.1 Capa de Red.....	¡Error! Marcador no definido.
3.4.1 Capa de Transporte	¡Error! Marcador no definido.
3.4.1 Capa de Sesión.....	¡Error! Marcador no definido.
3.4.1 Capa de Presentación.....	¡Error! Marcador no definido.
3.4.1 Capa de Aplicación	¡Error! Marcador no definido.
3.5 Espectro radioeléctrico y normatividad.....	39
3.6 Alianza Wi-Fi	40
3.7 Características de las señales RF.....	41
3.8 Modulación.....	42
3.8.1 Modulación por desplazamiento de frecuencia	42
3.8.2 Modulación por desplazamiento de fase	43
3.8.3 Modulación por amplitud de cuadratura	46
3.9 Espectro Disperso	47
3.9.1 Salto en Frecuencia (<i>Frequency Hopping</i>).....	48
3.9.2 Secuencia Directa (<i>Direct Sequence</i>)	48
3.9.2.1 Canales de Secuencia Directa y Dominio Regulatorio.....	49
3.10 Multiplexaje por División de Frecuencia Ortogonal	51
3.11 Acceso al Medio	52
3.11.1 FDMA (<i>Frequency Division Multiple Access</i>)	52
3.11.2 TDMA (<i>Time Division Multiple Access</i>)	53
3.11.3 CDMA (<i>Code Division Multiple Access</i>)	54
3.12 Potencia de una señal.....	54
3.12.1 Decibeles	555
3.12.2 Potencia nominal.....	56
3.13 Especificaciones 802.11.....	57

3.14 Seguridad para la red inalámbrica.....	59
3.14.1 SSID.....	59
3.14.2 Encriptación	59
3.14.3 Autenticación.....	60
3.14.3.1 Autenticación Usando Llave Criptográfica Pública.....	61
3.14.3.3 Tipos de autenticación	63
3.14.4 Asociación.....	63

Capítulo IV

Consideraciones para la Implementación del Enlace Inalámbrico

4.1 Antecedentes	65
4.2 Roles en el Radio de la Red Inalámbrica	65
4.3 VLANs.....	67
4.4 Antenas	68
4.4.1 Ganancia.....	68
4.4.2 Propiedades Direccionales.....	69
4.4.2.1 Antenas Omni-Direccionales	70
4.4.2.2 Antenas Direccionales	70
4.4.3 Polarización.....	71
4.4.4 Tipos de Antenas	71
4.4.4.1 Antena Parche	71
4.4.4.2 Antena Panel	72
4.4.4.3 Antena Yagi	73
4.4.4.4 Antenas Platillo	74
4.5 Consideraciones para la Trayectoria.....	75
4.5.1 Línea de Vista (LOS).....	75
4.5.2 Redondez de la Tierra.....	75
4.5.3 Zona de Fresnel	76
4.6 Consideraciones Ambientales	78
4.7 Consideraciones de Potencia.....	78

4.7.1 EIRP	79
------------------	----

Capítulo V

Implementación del Enlace Inalámbrico en la Junta Local Ejecutiva del Estado de Durango

5.1 Descripción del problema	80
5.2 Alternativas al Enlace Inalámbrico	80
5.3 Solución del problema	822
5.4 Punto de Acceso/Bridge Autónomo 1310G	82
5.4.1 Inyector de Potencia.....	¡Error! Marcador no definido.
5.4.2 Antena integrada.....	84
5.4.3 Puertos Ethernet	84
5.5 Diseño en sitio.....	85
5.5.1 Distancia entre las antenas o “bridges”	87
5.5.2 Utilidad para el cálculo de rango en bridges para exteriores.....	88
5.6 Configuraciones	91
5.6.1 Switch en sitio Principal.....	92
5.6.2 Switch en sitio Secundario	92
5.6.3 Bridge en sitio Principal.....	92
5.6.4 Bridge en sitio Secundario	100
5.7 Pruebas y Resultados	105
CONCLUSIONES.....	107
REFERENCIAS:.....	109
<i>Bibliográficas</i>	109
<i>Cibergráficas</i>	109
ANEXO	111
<i>Instalación física de los dispositivos inalámbricos</i>	111
GLOSARIO.....	115

INTRODUCCIÓN

A raíz de una serie de adecuaciones en la Junta Local del Estado de Durango, el Instituto Federal Electoral (IFE) se vio en la necesidad de rentar un espacio adicional con el fin de optimizar las actividades del personal, por lo que a partir de ese momento la Junta estaría constituida por dos inmuebles, mismos que se encontrarían separados, posteriormente la distancia se determina.

El edificio al que a partir de este momento llamaremos “Principal” ya contaba con la instalación de un servicio de enlace dedicado a través de un proveedor de servicios de red, el segundo inmueble al que denominaremos “Secundario” no contaba con dicho servicio, por lo que el IFE a través de la Unidad de Servicios de Informática (UNICOM), en su Departamento de Operación de Redes, trató de encontrar las posibilidades más viables para suministrar el servicio de voz y datos al edificio secundario.

Esta problemática ya se había presentado en la Junta Distrital II del Estado de Guanajuato (San Miguel de Allende) donde también existen dos inmuebles contiguos. Ahí se instauraron dos enlaces dedicados, pero esto representaba dos rentas mensuales, por lo que se empezó a realizar un análisis de alternativas para evitar duplicar el gasto en dos inmuebles cercanos del Instituto.

Ante las circunstancias, y derivado de un análisis costo-beneficio, el IFE optó por una nueva alternativa: la implementación del radioenlace o enlace inalámbrico que permitiera interconectar a los dos inmuebles a través de dispositivos que emitieran ondas electromagnéticas y transportaran la señal, sin necesidad de algún tipo de cableado. De esta manera, la institución tendría que realizar una inversión en

el costo de infraestructura (cableado, antenas y switch), pero a la larga se obtendría un ahorro considerable en la renta mensual del enlace dedicado para un sitio –más de 20 mil pesos mensuales–.

El presente trabajo tiene como finalidad realizar una descripción del procedimiento que se llevó a cabo para el diseño, implementación, configuración e instalación del enlace inalámbrico desde sus bases teóricas hasta su operación, pruebas y resultados. El trabajo se divide en cinco capítulos: El primero hace una descripción sobre el entorno donde se desarrolló el trabajo, el Instituto Federal Electoral, el segundo capítulo, se menciona un repaso sobre la trayectoria laboral que permitió que el presente tesista realizar el proyecto, en el tercer capítulo se exponen las bases teóricas de las redes inalámbricas; El cuarto se presenta el análisis del estudio de factibilidad y consideraciones; finalmente, en el quinto capítulo se desglosa el trabajo realizado en la Junta Local presentando el diseño, las configuraciones necesarias del enlace inalámbrico y las conclusiones.

CAPÍTULO I

INSTITUTO FEDERAL ELECTORAL

El Instituto Federal Electoral, ahora INE, es un organismo público, autónomo y permanente encargado de organizar las elecciones federales, es decir, las referentes a la elección del Presidente de la República y de los Diputados y Senadores que integran el Congreso de la Unión.

1.1 Misión

Contribuir al desarrollo de la vida democrática, garantizando el ejercicio de los derechos político-electorales de la sociedad a través de la promoción de la cultura democrática y la organización de comicios federales en un marco de certeza, legalidad, independencia, imparcialidad y objetividad.

1.2 Historia

Desde su constitución formal, el 11 de octubre de 1990, el Instituto Federal Electoral se ha distinguido como uno de los pilares en la construcción de la democracia en México. En más de dos décadas de existencia, el IFE ha experimentado importantes reformas relacionadas con su integración, atributos y funciones. Esto le ha permitido, perfeccionar la organización y celebración de los comicios electorales federales.

El 15 de agosto de 1990 se publicó el Código Federal de Instituciones y Procedimientos Electorales (COFIPE) previéndose la creación del Instituto Federal Electoral, en reemplazo de la CFE (Comisión Federal Electoral), autoridad que organizaba los comicios electorales antes de esta fecha. Se creó el Tribunal Federal Electoral, así como un nuevo padrón electoral y un formato diferente de credencial para votar.

A lo largo de más de 20 años de existencia, el Instituto Federal Electoral ha sufrido varias reformas constitucionales en cuanto a atribuciones y responsabilidades, la más reciente y significativa es del 10 de febrero de 2014 donde se publicó el decreto que reforma y adiciona varias disposiciones a la Constitución en materia política-electoral, entre ellas, la creación del Instituto Nacional Electoral (INE) en sustitución del IFE. Donde se ha incrementado el número de consejeros electorales; la reelección consecutiva de legisladores y legisladoras locales y federales; la aprobación de una Ley para regular la publicidad gubernamental; y, la anulación de una elección cuando se rebase el 5% al monto autorizado el tope de gastos de campaña, entre otros aspectos.

1.3 Estructura orgánica del IFE

Para la realización de sus actividades, el Instituto Federal Electoral cuenta con una sede central ubicada en el Distrito Federal, 32 delegaciones (una en cada entidad federativa) y 300 subdelegaciones (una en cada distrito electoral en que se divide el país).

El personal que labora en ellas se divide en dos cuerpos de funcionarios: Los integrados en el Servicio Profesional Electoral y la rama administrativa. Su estructura orgánica lo conforma lo siguiente:

- I. Órganos Directivos**
- II. Órganos Técnico – Ejecutivos**
- III. Órganos de Vigilancia**

La descripción y funciones de cada uno de estos órganos se detallan en la siguiente sección.

1.3.1 Órganos Directivos

Los Órganos Directivos están constituidos por el Consejo General y los Consejos Locales y Distritales que a continuación se explican más a detalle.

- **Consejo General**

Es el órgano superior de dirección de todo el Instituto, responsable de vigilar el cumplimiento con las disposiciones constitucionales y legales en materia electoral, y velar porque los principios de certeza, legalidad, independencia, imparcialidad y objetividad guíen todas las actividades de la institución.

- **Consejos Locales y Distritales**

A. Consejos Locales. Son los órganos de dirección constituidos en cada una de las 32 entidades federativas que, a diferencia del Consejo General, únicamente se instalan y sesionan durante los procesos electorales federales.

B. Consejos Distritales. Son los órganos de dirección constituidos en cada uno de los 300 distritos uninominales en que se divide el territorio nacional para efectos electorales. Al igual que los Consejos Locales, únicamente se instalan y sesionan durante los procesos electorales federales.

1.3.2 Órganos Técnico – Ejecutivos

Los Órganos Técnico – Ejecutivos están constituidos por la Junta General Ejecutiva, las Juntas Locales Ejecutivas y las Juntas Distritales Ejecutivas.

- **Junta General Ejecutiva**

Es el órgano ejecutivo y técnico de mayor jerarquía. Se encarga de instrumentar las políticas y programas generales del Instituto y cumplir con los acuerdos y resoluciones aprobados por el Consejo General.

- **Juntas Locales Ejecutivas**

Son los órganos permanentes de ejecución y soporte técnico de las actividades del Instituto en cada entidad federativa.

- **Juntas Distritales Ejecutivas**

Son los órganos permanentes de ejecución y soporte técnico de las actividades del Instituto en cada uno de los 300 distritos electorales uninominales, los cuales tienen sede en la cabecera de cada uno de los distritos.

1.3.2 Órganos de Vigilancia

Son órganos colegiados cuya finalidad es coadyuvar y supervisar los trabajos relacionados con la integración, depuración y actualización del Padrón Electoral. Aquí encontramos la Comisión Nacional de Vigilancia y las Comisiones Locales y Distritales de Vigilancia

1.4 Estructura Organizacional del Instituto Federal Electoral

Los órganos centrales del Instituto Federal Electoral son:

- A. Consejo General.** Lo integra 8 consejeros, un consejero presidente y un secretario ejecutivo.
- B. Presidencia del Consejo General.** Lo conforma el área del consejero presidente. Garantiza la unidad y cohesión de las actividades de los órganos del Instituto.
- C. Junta General Ejecutiva.** Está compuesto por un consejero presidente, un secretario, los directores de cada una de las direcciones ejecutivas y los coordinadores de las unidades técnicas.
- D. Secretaría Ejecutiva.** Lo conforma el área del secretario ejecutivo en turno. Entre sus funciones esta representar legalmente al Instituto y cumplir los acuerdos del Consejo General.

- E. Unidad de Fiscalización de los Recursos de los Partidos Políticos.** Audita con plena independencia técnica la documentación soporte, así como la contabilidad que presenten los partidos políticos en su caso, candidaturas independientes en cada uno de los informes que están obligados a presentar.
- F. Contraloría General.** Fijar los criterios para la realización de las auditorías, procedimientos, métodos y sistemas necesarios para la revisión y fiscalización de los recursos a cargo de las áreas y órganos del Instituto.

1.4.1 Direcciones Ejecutivas

Las Direcciones Ejecutivas del Instituto son creadas para el mejor funcionamiento de este. Al frente de cada una de estas direcciones habrá un Director Ejecutivo.

Las Direcciones Ejecutivas que actualmente se encuentran operando son:

- A.** Dirección Ejecutiva del Registro Federal de Electores (DERFE)
- B.** Dirección Ejecutiva de Prerrogativas y Partidos Políticos (DEPyPP)
- C.** Dirección Ejecutiva de Organización Electoral (DEOE)
- D.** Dirección Ejecutiva del Servicio Profesional Electoral (DESPE)
- E.** Dirección Ejecutiva de Capacitación Electoral y Educación Cívica (DECEyEC)
- F.** Dirección Ejecutiva de Administración (DEA)

1.4.2 Unidades Técnicas

Las Unidades Técnicas del Instituto son creadas para el mejor funcionamiento de este. El Secretario Ejecutivo presentará a consideración del presidente del Consejo General las propuestas para la creación de nuevos órganos técnicos, de acuerdo con la disponibilidad presupuestal.

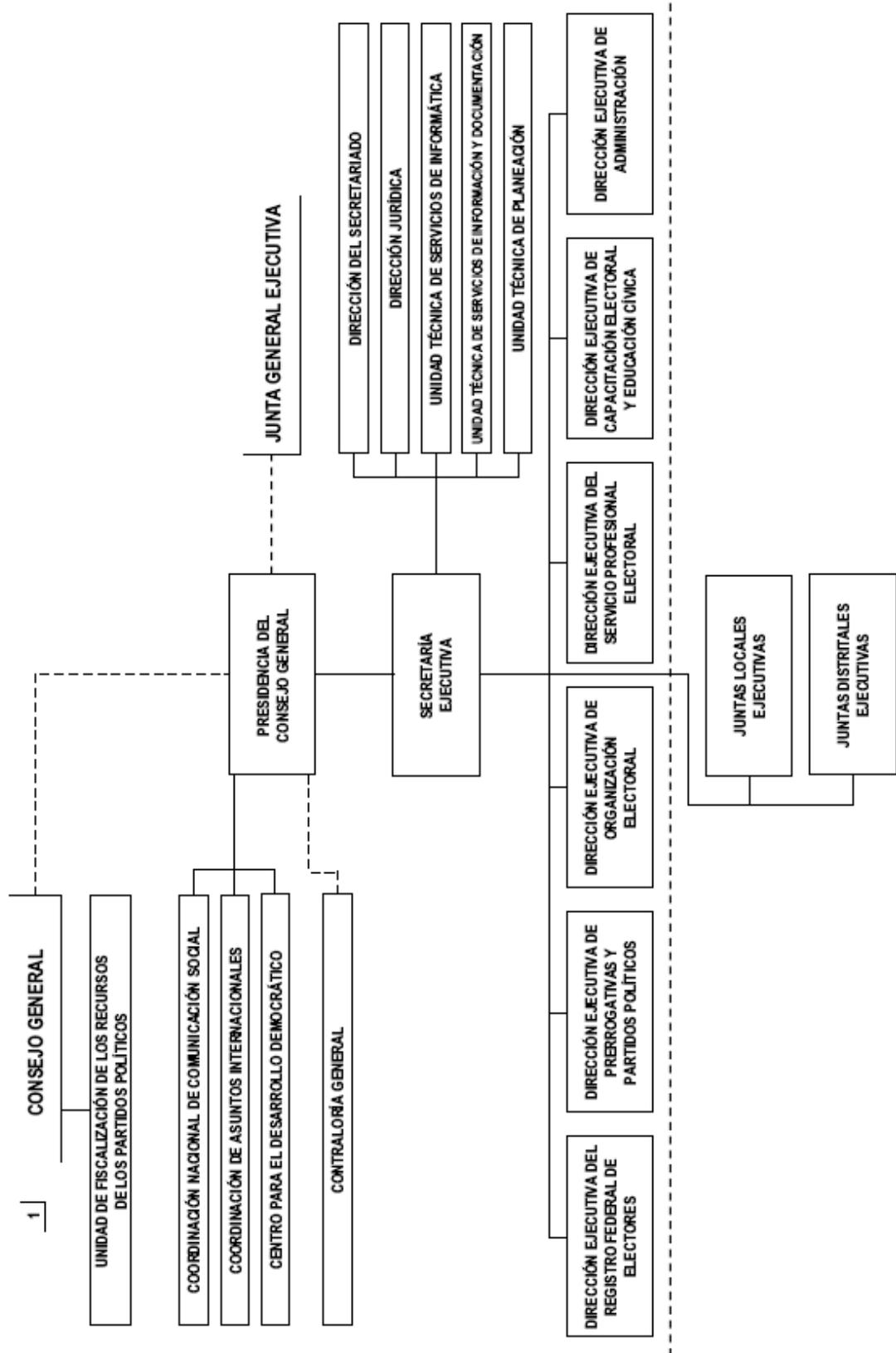
Las Unidades Técnicas que conforman al IFE son:

- A. Coordinación de Asuntos Internacionales
- B. Dirección del Secretariado
- C. Dirección Jurídica
- D. Centro para el Desarrollo Democrático
- E. Unidad Técnica de Servicios de Informática
- F. Coordinación Nacional de Comunicación Social
- G. Unidad Técnica de Servicios de Información y Documentación
- H. Unidad Técnica de Planeación

1.4.3 Organismos Desconcentrados

- a. Juntas Locales Ejecutivas
- b. Juntas Distritales Ejecutivas

→ Para mejor referencia de la estructura organizacional del Instituto Federal Electoral, consultar el *Organigrama 1.1*



Organigrama 1.1 Estructura Organizacional

1.5 Unidad de Servicios de Informática

La Unidad de Servicios de Informática llamada comúnmente **UNICOM** es una de las 8 unidades del Instituto y responde directamente al Secretario Ejecutivo. Brinda asesoría y soporte técnico en materia de informática y comunicaciones a las diversas áreas del Instituto.

1.5.1 Misión

Administrar servicios en materia de Tecnologías de Información y Comunicaciones, así como establecer la dirección tecnológica que contribuya al cumplimiento de las atribuciones y objetivos del Instituto Federal Electoral.

1.5.2 Visión

Posicionar al Instituto Federal Electoral como un referente nacional e internacional en el aprovechamiento de tecnologías de información y comunicaciones en materia electoral, a través de una cultura orientada a procesos, calidad, seguridad, innovación y mejora continua.

Dentro de las actividades principales que realiza el personal de la Unidad de Servicios de Informática se pueden destacar las siguientes:

- a.** Automatizar procesos que permitan optimizar el desarrollo de las tareas que deben cumplir las diversas áreas del IFE, a través del desarrollo, implementación y actualización de sistemas y servicios informáticos.
- b.** Administrar y operar la infraestructura de cómputo y comunicaciones que soporta los servicios y sistemas que se encuentran disponibles a través de la Red Nacional de Informática, la cual permite comunicar a todo el personal que labora en el Instituto a nivel nacional, así como difundir información a la ciudadanía.
- c.** Coordinar y ejecutar el desarrollo y operación del Programa de Resultados Electorales Preliminares PREP, el cual permite difundir de forma inmediata a la ciudadanía, los resultados preliminares de las elecciones federales.

- d. Proporcionar capacitación, asesoría y soporte técnico a todo el personal del Instituto, en el uso de sistemas, servicios y equipos de cómputo.

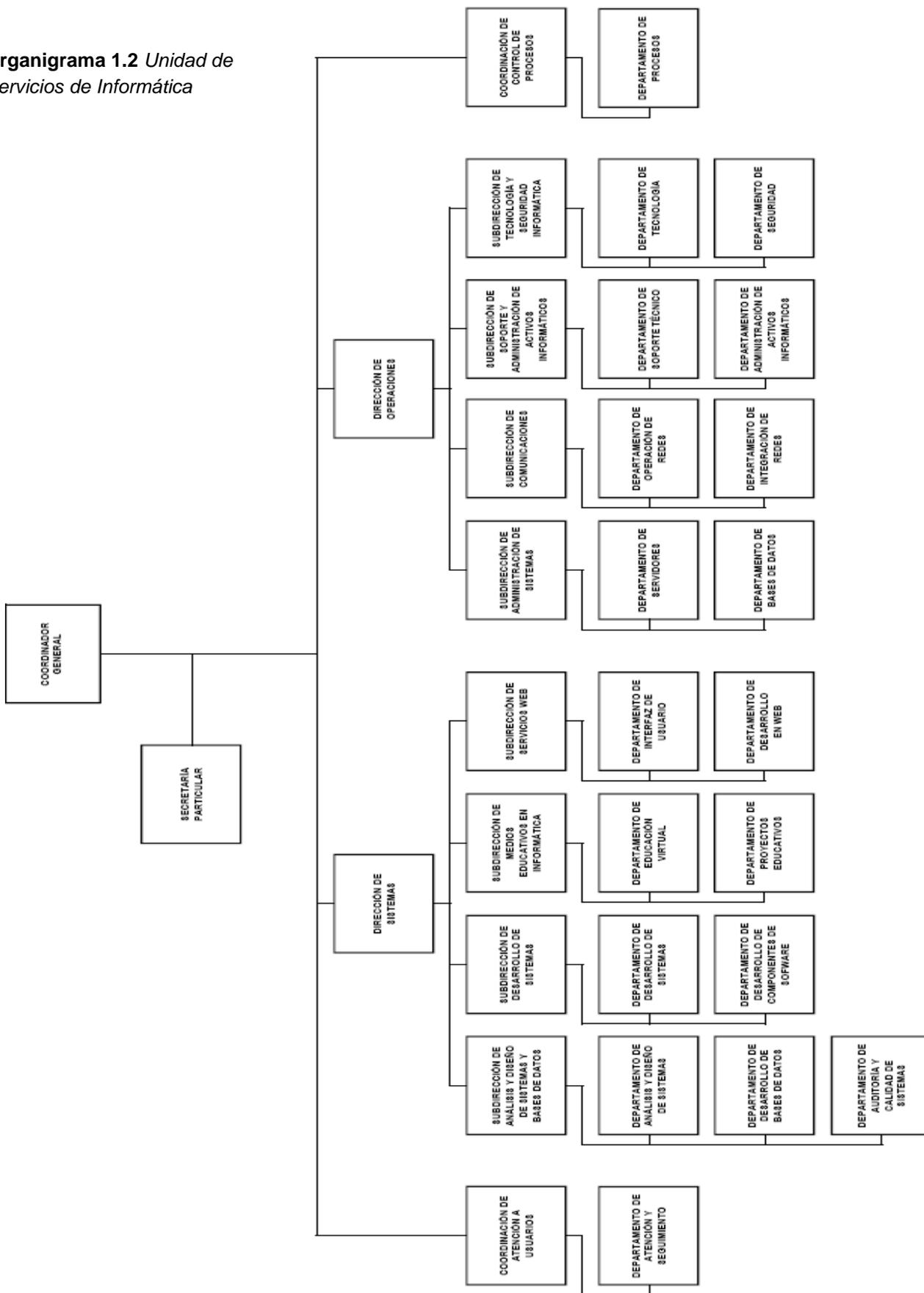
1.5.3 Estructura de la Unidad de Servicios de Informática

La Unidad de Servicios de Informática está compuesta por:

- I. **Coordinación General.** Coordina la modernización de la estructura informática del Instituto, agrupando integralmente la información generada por y para sus actividades, con la finalidad de producir, recolectar y difundir la información del Instituto con seguridad.
- II. **Secretaría Particular.** Llevar el seguimiento a los asuntos del titular, para organizar su agenda y atender los temas que determine.
- III. **Coordinación de Atención de Usuarios.** Coordina que la atención de solicitudes de servicio (reportes y consultas vía WEB, correo electrónico y vía telefónica) se realicen de acuerdo a tiempos y forma establecidos.
- IV. **Dirección de Sistemas.** Coordina el desarrollo, implementación y mantenimiento de los sistemas de cómputo necesarios para la consecución de los objetivos estratégicos del Instituto, así como brindar la capacitación en el uso y la operación de los sistemas de información.
- V. **Dirección de Operaciones.** Se encarga de coordinar la planeación, el diseño, la administración y la operación de la infraestructura informática, de telecomunicaciones y de soporte; de los sistemas y de los servicios informáticos y de telecomunicaciones; así como la atención de las solicitudes de servicio asociadas.
- VI. **Coordinación de Control de Procesos.** Supervisa el cumplimiento a los proyectos estratégicos, objetivos operativos de la unidad, la definición e implementación, de procesos y normatividad en materia de TIC.

→ Para mejor referencia para la estructura de la Unidad de servicios de Informática, consultar el *Organigrama 1.2*

Organigrama 1.2 Unidad de Servicios de Informática



1.5.4 Estructura Dirección de Operaciones

De acuerdo al organigrama 1.2 la Dirección de Operaciones está constituida por cuatro subdirecciones:

- **Subdirección de Administración de Sistemas (SAS).** Controla y supervisa la administración y operación de la infraestructura de procesamiento y almacenamiento, de las bases de datos, de los sistemas y de los servicios informáticos relacionados, así como la atención de las solicitudes de servicio asociadas.
- **Subdirección de Comunicaciones (SC)** se encarga de administrar y operar la Red Nacional de informática y telefonía IP del Instituto en materia de telecomunicaciones, de los sistemas y de los servicios informáticos relacionados, así como la atención de las solicitudes de servicio asociadas.
- **Subdirección de Soporte y Administración de Activos Informáticos (SSAAI).** Controla y supervisa la administración y operación de la infraestructura de ambiente físico, activos informáticos; así como la atención de las solicitudes de servicio asociadas.
- **Subdirección de Tecnología y Seguridad Informática (STSI).** Se encarga de controlar y supervisar la seguridad de la infraestructura, sistemas y servicios informáticos; así como las investigaciones y evaluaciones de nuevas tecnologías en la materia; así como la atención de las solicitudes de servicio asociadas.

1.5.5 Estructura Subdirección de Comunicaciones

Finalmente, la Subdirección de Comunicaciones tiene a su cargo dos departamentos:

- **Departamento de Integración de Redes (DIR).** Administrar y operar la Red Nacional de informática y telefonía IP del Instituto en materia de telecomunicaciones; de los sistemas y de los servicios informáticos relacionados; así como la atención de las solicitudes de servicio asociadas.

- **Departamento de Operación de Redes (DOR).** Instrumenta e implementa la administración y operación de los equipos y enlaces de telecomunicaciones, de los sistemas y servicios relacionados, así como la atención de las solicitudes de servicio asociadas.

1.5.6 Departamento de Operación de la Red

Las funciones del Departamento de Operación de Redes son:

- Elaborar e implementar las normas, políticas y estándares relacionados con la administración, operación, mantenimiento, soporte técnico y uso de la infraestructura de comunicaciones de la Red Nacional de cómputo y comunicaciones del Instituto.
- Implementar las políticas y programas del área para el adecuado funcionamiento de la infraestructura de comunicaciones.
- Facilitar el desarrollo de nuevos proyectos que contribuyan a mejorar la infraestructura de cómputo y comunicaciones del Instituto.
- Administrar la operación de la Red Nacional de Informática del Instituto garantizando la disponibilidad en los servicios.
- Facilitar el desarrollo de proyectos encaminados a mejorar la administración, operación, mantenimiento y soporte técnico de la infraestructura de comunicaciones del Instituto.
- Realizar el análisis, planeación y diseño de los esquemas de interconexión de las redes de comunicaciones del Instituto.
- Gestionar el servicio de nombres (DNS, *Domain Name System*) y asignación dinámica de direcciones IP (DHCP) de la Red Nacional de cómputo y de comunicaciones del Instituto.
- Gestionar el servicio de accesos remotos vía VPN a la Red Nacional de cómputo y de comunicaciones del Instituto.
- Gestionar el sistema de administración de red (NMS, *Network Management System*).

- Realizar los procedimientos específicos para las necesidades de conectividad a servicios de red de las áreas del Instituto.
- Implementar y dar seguimiento a las políticas de seguridad informática asociadas a la infraestructura de telecomunicaciones.
- Realizar el análisis del desempeño de la infraestructura de comunicaciones del Instituto.
- Implementar la normatividad establecida con relación a la administración, operación, mantenimiento, soporte técnico y uso de los equipos de comunicaciones del Instituto.
- Supervisar y llevar a cabo las actividades de mantenimiento preventivo y correctivo a la infraestructura de comunicaciones del Instituto.
- Aportar en la integración de los anexos técnicos de las licitaciones que se lleven a cabo para la adquisición de bienes y la contratación de servicios informáticos.
- Realizar los procedimientos específicos para la adecuada atención de las solicitudes de servicio referente a la infraestructura de comunicaciones de los usuarios.
- Realizar el estudio, análisis y evaluación de nuevas tecnologías de redes de comunicaciones.
- Implementar y operar los mecanismos e infraestructura de comunicaciones de la Red Nacional de cómputo necesarios para realizar el Programa de Resultados Electorales Preliminares.
- Supervisar las tareas asignadas al personal que integra el Departamento de Operación de Redes.
- Gestionar y operar el sistema de control de llamadas telefónicas del Centro de Atención a Usuarios y el Centro de Operaciones de la Red Nacional de cómputo y de comunicaciones del Instituto.
- Administrar la Red Nacional de telefonía IP del Instituto.
- Administrar la Red de acceso Inalámbrico Nacional del Instituto.

- Llevar a cabo las demás funciones necesarias para el cumplimiento de su objeto dentro del ámbito de su competencia, que le confieran las disposiciones jurídicas aplicables y sus superiores jerárquicos.
- Organizar y mantener permanentemente actualizada, clasificada y disponible la información, documentación, archivo documental o digital a su cargo, de conformidad con las disposiciones legales y administrativas aplicables.

CAPÍTULO II

PUESTO DE TRABAJO Y PROYECTOS

2.1 Descripción del Puesto de Trabajo

Durante seis años, el presente exponente ha colaborado dentro del Departamento de Operación de Redes, que forma parte de la Unidad Técnica de Servicios de Informática del Instituto Federal Electoral, con el puesto de Informático Especializado en Operación de Redes, labor que le ha permitido desarrollar las habilidades que se adquirieron durante la carrera de Ingeniería en Telecomunicaciones.

Este puesto está destinado a desarrollar e implementar nuevas tecnologías en la red de datos dentro del Instituto, así como apoyar otras áreas en la administración del *firewall* de Internet e Intranet, Balanceadores de Tráfico de Datos, entre otros. A continuación se enumeraran los proyectos más significativos en el que el exponente ha participado.

2.2 Proyectos, Actividades, Participación y Logros Alcanzados dentro de la Institución

A. Monitoreo Proactivo (2008-2014)

Esta actividad se realiza todos los días con la finalidad de mantener operando los enlaces de comunicaciones de la Red IFE que se rentan al proveedor de servicios Teléfonos de México (TELMEX)

Participación: Monitorear el correcto desempeño de cada uno de los enlaces, y en caso de presentarse alguna incidencia, se reporta con el proveedor para que se diagnostique y se solucione la falla.

Logros: Con esta actividad se ha logrado mantener una óptima comunicación y operación de la red.

Se ha logrado tener una disponibilidad de **99.72%**

B. Balanceo de tráfico en los enlaces primario y secundario de las Juntas Distritales (2014)

Este proyecto ha tenido como misión aprovechar y poner en operación dos enlaces de comunicaciones que se encuentran instalados en todas las juntas distritales del Instituto Federal Electoral, ya que actualmente se encuentra solo un enlace operando.

Participación: Verificar el comportamiento actual de tráfico de datos en los enlaces y diseñar los futuros parámetros con los cuales los *routers* instalados en cada Junta Distrital trabajarán para que ambos enlaces de comunicación instalados operen de manera balanceada.

Logros: En este proyecto, se logró la comprensión de varios protocolos de balanceo de tráfico de salida, así como el anuncio distribuido de las redes que operan la Junta Distrital para el tráfico de entrada.

Hasta el momento se ha logrado que en dos Juntas Distritales se tengan dos enlaces operando y balanceando tráfico tanto de entrada como de salida.

C. Diseño, Implementación, y Puesta en Operación de un Control de Acceso a la Red para la Macrosala de Prensa en las Elecciones Federales (2009,2012)

El objetivo de este proyecto era controlar el acceso a una red de usuarios por medio de un *hotspot*. Se pusieron en marcha diversos equipos de acceso inalámbrico para que los usuarios tuvieran la movilidad necesaria en el desempeño de su trabajo.

Participación: Se propuso un esquema de asignación de direccionamiento dinámico, configuración del *Appliance Cisco NAC* y equipos de acceso inalámbrico.

Logros: Se proporcionó Red Inalámbrica de la Macrosala a los dispositivos móviles a través de un usuario y contraseña, para evitar accesos no autorizados.

D. Diseño, Implementación, y Puesta en Operación de un Radioenlace Punto a Multipunto para la Feria de Medios en el Proceso Electoral Federal (2012)

Para evitar realizar un cableado temporal y proporcionar acceso a Internet a cada uno de los medios de comunicación y reporteros instalados en la explanada del Instituto Federal Electoral en el Proceso Electoral del 2012, se optó por utilizar radioenlaces de alcance corto con una antena *root* o maestra y 4 antenas *non-root* o esclavas.

Participación: Se propuso un esquema de asignación de direccionamiento dinámico, configuración de las antenas *root* y *non-root*, pruebas de conectividad y alcances, además del diseño de troncales sobre estos mismos enlaces, debido a que debían soportar una comunicación con múltiples *vlangs*.

Logros: Se permitió el acceso a Internet a los reporteros en las distintas instalaciones y carpas temporales, que los medios de comunicación utilizan para su respectiva transmisión del evento.

E. Implementación de la tecnología WPA2 para la red inalámbrica del IFE en Oficinas Centrales y en sus respectivas Juntas Locales (2014)

Hace algunos años el acceso inalámbrico en la Institución trabajaba con un nivel de seguridad WPA. Esto, debido a que la mayoría de los equipos inalámbricos de los usuarios no podrían soportar un acceso con seguridad más robusta, actualmente los dispositivos han evolucionado, por lo que se determinó la implementación de la tecnología WPA2.

Participación: Propuesta del WPA2 y configuración de equipos para acceso inalámbrico tipo infraestructura.

Logros: Se logró un esquema ambivalente de seguridad soportando WPA y WPA2 para anular el impacto que pudieran tener algunos usuarios que no soportaran WPA2, además se logró un robustecimiento en el cifrado de TKIP a AES.

F. Diseño, Implementación, y Puesta en Operación de los servidores de autenticación para la Red Inalámbrica del IFE con esquema de alta disponibilidad y replicación automática (2009)

Cada uno de los equipos de acceso inalámbricos distribuidos a lo largo de las Oficinas Centrales de la Institución y en cada uno de los estados de la República, realiza una consulta por medio un servidor *RADIUS* para determinar si se le da permiso de utilizar la red inalámbrica del IFE. El objetivo de este proyecto era sustituir dicho servidor con otros dos más actualizados.

Participación: Instalación y configuración de cada uno de los servidores *RADIUS Cisco ACS*, reconfiguración de los equipos de acceso inalámbrico, implementación de la alta disponibilidad, etapa de pruebas y operación final.

Logros: Se consiguió que trabajaran ambos servidores en alta disponibilidad activo-pasivo, es decir, si el servidor activo fallara, el servidor pasivo tomaría su lugar para anular una falla masiva en el acceso a la red inalámbrica. Además, se tiene una replicación en la configuración, esto es, si se realiza algún cambio en el servidor activo, la replicación de esta configuración al servidor pasivo se realiza todos los días a las 23 hrs. Está hora se determinó debido a que existe nula o poca demanda en el servicio de autenticación.

G. Diseño e Implementación de un Sistema de Dominio Inalámbrico (WDS, *Wireless Domain System*, por sus siglas en inglés) en cada segmento de administración de los equipos de acceso inalámbrico (2011)

Con el objetivo de minimizar la carga de número de peticiones de autenticación sobre los servidores de autenticación *RADIUS* del IFE se implementó un *WDS*, que permite a un equipo de acceso inalámbrico ser un intermediario con las solicitudes que se están realizando. Esto es, un grupo de equipos de acceso inalámbricos realizará una petición sobre su *WDS* al que le corresponde, este a su vez, realizará la petición a los servidores *RADIUS*. La ventaja de este “intermediario”, es que guarda nombres de usuarios y sus respectivas contraseñas de los clientes que se han asociado a la red por un determinado tiempo, evitando así, que una nueva petición de los mismos clientes ya asociados se realicen a los servidores *RADIUS* de forma repetida.

Participación: Diseño y configuración de cada uno de *WDS* para cada red de administración, etapa de pruebas y operación final. Ya que era varias redes en el que se debía configurar el sistema, se optó por diseñar un programa que automatizara esta serie de configuraciones, tanto para el *WDS*, como para cada uno de los equipos de acceso inalámbrico dentro del sistema de dominio para que pudieran ser parte del él.

Logros: Se colocó el Sistema de Dominio Inalámbrico a nivel nacional en Oficinas Centrales y Oficinas Delegacionales (Juntas Locales y Distritales) ya que cuentan con al menos un equipo de acceso inalámbrico, se determinó que en las Oficinas Centrales de Tlalpan se colocara un equipo de acceso inalámbrico dedicado exclusivamente a ser *WDS* ya que este sitio cuenta con una gran cantidad de puntos de acceso distribuidos en todos sus complejos y pertenecen a una misma red.

H. Ampliación de cobertura de la Red Inalámbrica en las vocalías de Registro Federal de Electores en 11 Estados de la Republica (2013)

A lo largo del país, existen sitios donde la Vocalía de Registro Estatal se encuentra fuera de la Junta Local Ejecutiva, por lo que no cuentan con acceso a la red de manera inalámbrica. Se determinó colocar red inalámbrica dentro de estos sitios.

Participación: Se realizaron las configuraciones necesarias en cada uno de los nuevos equipos de acceso inalámbrico, para que operara de la misma manera que los equipos ya instalados. Así como también se implementó un *DHCP* para asignación de direcciones *IP* a los clientes que se asocian a la red. En este punto se consideró un filtro o lista de acceso en la interfaz alámbrica del equipo, ya que el tráfico *DHCP* configurado en el mismo equipo podría proporcionar direccionamiento no deseado a la red cableada de la Vocalía de Registro.

Logros: Se instalaron correctamente los 11 equipos de acceso inalámbrico, y se validó correctamente su operación con cada una de las personas a cargo en sitio.

I. **Separación de la Red Inalámbrica de Usuarios de las Juntas Locales Ejecutivas con la de usuarios de red cableada (2013)**

Al implementarse la red inalámbrica en cada Junta Local de los 32 Estados de la República Mexicana, se determinó que su direccionamiento se compartiera con la red cableada de usuarios. Posteriormente se determinó tener un direccionamiento de red para la red cableada y otro direccionamiento para la inalámbrica.

Participación: Se propuso un esquema de direccionamiento para los usuarios inalámbricos para recordarlo con facilidad y evitar el traslape con alguna red ya existente.

Logros: Se separó la red de usuarios con infraestructura cableada con los usuarios que acceden a la red de manera inalámbrica, además de implementarse un *DHCP* local en cada equipo de acceso inalámbrico para facilitar el acceso a la red de los usuarios asociados.

J. Robustecimiento de la Red de los complejos “Quantum” y “CECYRD” en Distrito Federal y Pachuca respectivamente del Registro Federal de Electores (2013-2014)

Este proyecto tuvo como objetivo mejorar la red de los complejos del Registro Federal de Electores, separando la red de usuarios con la red de su Centro de Datos, así como poder tener una total administración de equipos críticos (*routers, switches, equipos de acceso inalámbrico*)

Participación: Se implementó un servidor *DHCP* para la asignación de direcciones IP, tanto a los clientes con red cableada como clientes inalámbricos. Se realizaron las configuraciones de los equipos de acceso inalámbrico, así como las pruebas y puesta en operación de los equipos con una nueva dirección IP separándose así, de la red de usuarios. Se amplió un sistema de administración de equipos para cada sitio con el anterior, para mejorar la gestión de los clientes que van formando parte de la red de datos y voz.

Logros: Se permitió la centralización del servidor *DHCP*, robusteciendo la administración y monitoreo. Se mejoró la administración de usuarios de ambos sitios permitiendo segmentar cada departamento en una sola red y una sola VLAN.

K. Implementación de una herramienta para monitorear el servicio activo de DHCP en cada sitio de Oficinas Centrales y Registro Federal de Electores (2013)

Para mejorar una respuesta rápida, a alguna posible contingencia en el servicio de asignación de direcciones IP, en las Oficinas Centrales y el Registro Federal de Electores del IFE, se implementó un programa sensor que monitorea el servicio de DHCP de distintos sitios del Instituto Nacional Electoral: Tlalpan, Acoxtla, Zafiro, DERFE Insurgentes, DERFE Quantum y DERFE CECYRD. Este programa es ejecutado desde el *NMS (Network Management System)*.

Participación: Se diseñó un programa que permite monitorear si el servicio se encuentra activo en cada sitio. Dicho programa se ejecuta cada 30 minutos, tiempo por debajo del promedio donde un cliente solicita la renovación de su dirección IP (desde 1 hora en el caso de la red inalámbrica, hasta 7 días, en el caso de la Telefonía IP).

Logros: Se mejoró el tiempo de respuesta para poder restablecer el servicio. En caso de alguna contingencia, el sistema manda un correo al personal del Departamento de Operación de la Red notificando que el servicio está detenido permitiendo al equipo de comunicaciones pueda solucionar a tiempo la incidencia y evitar que los usuarios perciban una falla *masiva en la red*.

L. Implementación de la herramienta de monitoreo WLSE (Wireless LAN Solution Engine) para los equipos de acceso inalámbrico (2010)

El *WLSE* es una herramienta de monitoreo para equipos de acceso inalámbrico autónomos. Esta herramienta puede realizar estadísticas y reportes de utilización, consumo de ancho de banda de cada equipo, número de usuarios asociados, entre otros.

Participación: Se instaló y se puso en operación un servidor de Cisco. En este procedimiento se configuró el envío automático de reportes cada cierto tiempo, para determinar si una zona requeriría algún dispositivo inalámbrico adicional y mejorar la cobertura y el servicio.

Logros: Se consiguió que el método de monitoreo para los equipos fuera con una versión más robusta de SNMP (*Simple Network Management Protocol*), en ese entonces se había utilizado la versión 2c, al implementar el WLSE se configuraron los equipos de acceso inalámbrico con versión 3 de SNMP.

M. Implementación de un nuevo SSID para el conjunto de equipos de acceso inalámbrico del Instituto Nacional Electoral (Actual)

Este proyecto aún se encuentra en etapa de pruebas. Debido al cambio de nombre de la institución, el actual SSID (Service Set Identifier) tiene incluido las iniciales del

Instituto Federal Electoral, ahora, se deberá actualizar este identificador en toda la infraestructura inalámbrica hacia las iniciales del Instituto Nacional Electoral (INE). Esto implica minimizar el impacto con los usuarios que utilizan la red inalámbrica con el SSID obsoleto

Participación: Se han realizado pruebas iniciales con un solo equipo de acceso inalámbrico para esta transición, se ha propuesto una red, direccionamiento y *VLAN* enteramente nuevos para el cambio. Se han determinado alcances e impactos a nivel usuario.

Logros: Han funcionado correctamente los dos *SSID* en el equipo de acceso inalámbrico de pruebas. Con la operación no ha habido algún tipo de interferencia que intervenga a nivel usuario.

2.3 Actividades y Proyectos

- Actualización de Sistema operativo *IOS* del *ASA (Adaptive Security Appliance)* Firewall de Internet del Instituto.
- Reemplazo de los *switches CORE* de complejo de Zafiro.
- Monitoreo de *pools* de *DHCP* Tlalpan en el módulo de *subcom* (interfaz web gráfica del NMS).
- Monitoreo de latencia de enlaces de Internet (enlaces tipo *STM1* y *E3*) en el módulo de *subcom*.
- Monitoreo de clientes asociados de equipos de acceso inalámbrico en módulo de *subcom* cada minuto.
- Balanceo de Tráfico en los enlaces *STM1* de Internet (en proceso).
- Implementación de una *VPN* entre las oficinas centrales del Instituto y el Banco Banamex.
- Apoyo en la instalación de teléfonos IP en cada Junta Distrital Ejecutiva (300 Distritos).
- Apoyo en la actualización de Sistema Operativo *IOS* en cada *switch* de las Juntas Distritales Ejecutivas del Instituto.

CAPÍTULO III

Redes Inalámbricas

3.1 Antecedentes

Las redes inalámbricas juegan un papel fundamental en la comodidad y facilidad del entorno social y laboral, representando grandes ventajas sobre las redes alámbricas convencionales. Una de ellas, y quizás la más importantes es el facilitamiento en la movilidad de las personas. Permite el acceso a la información, sin necesidad de cables que los obliguen a permanecer en un solo sitio. Las redes inalámbricas no solo permiten a la gente acceder a su correo electrónico, o navegar en el Internet, en una ubicación móvil de su preferencia, sino también les facilita compartir recursos de dos o más ubicaciones relativamente apartadas.

Otra de las ventajas es que, normalmente las redes inalámbricas tienen mucha flexibilidad en instalación y movilidad, que se traduce en una implementación rápida. Las redes inalámbricas utilizan varias estaciones base para enlazar a los usuarios a una red ya existente. Los puntos de acceso son las estaciones base en una red 802.11.

Un beneficio más que ofrecen es que son redes no cableadas. Cablear es una tarea que consume tiempo y recursos económicos y, además requiere de cierta infraestructura. Asimismo, con una red inalámbrica, no se requiere realizar el cableado de un edificio para ofrecer el acceso a los usuarios que lo requieran.

Finalmente, al igual que todas las redes, las redes inalámbricas utilizan un medio para transmitir los datos. A través del medio se propaga la energía electromagnética, éste debe cubrir cierta área para que los clientes puedan desplazarse a través del área de cobertura.

La enorme ventaja que ofrecen las ondas de radio a diferencia de la luz e infrarrojos es que pueden traspasar paredes con ciertas características, divisiones y/o distintos elementos de una casa u oficina, además tienen un rango de cobertura superior. Gran parte de los productos inalámbricos utilizan esta capa física.

3.2 Transceptores

Un transceptor consiste en un transmisor y un receptor. En un transmisor, el proceso conocido como *modulación* convierte las señales eléctricas de una computadora origen tanto a luz o a *RF* (Radio Frecuencia), las cuales son señales analógicas. Una vez modulada la señal, los amplificadores incrementan la magnitud de la señal antes de llegar a la antena. En el lugar destino, un receptor detecta las señales atenuadas, ingresa al amplificador para tratar de compensar las pérdidas del medio finalmente son demoduladas y convertidas en datos para la computadora o dispositivo destino.

3.3 Topologías

En una red *WLAN* se pueden distinguir tres tipos de configuraciones diferentes, en función de que se utilicen puntos de acceso o no. Se encuentran las redes Ad-hoc, las redes infraestructura y los radioenlaces o enlaces inalámbricos.

3.3.1 Redes Ad-hoc

Es de las configuraciones más sencillas, también conocidas como configuración *P2P* (*peer-to-peer*), en la que las terminales móviles se comunican directamente entre sí empleando una tarjeta adaptadora que soporte comunicación inalámbrica. La limitación más importante es que los dispositivos se encuentren dentro de sus áreas de cobertura. (Figura 3.1)

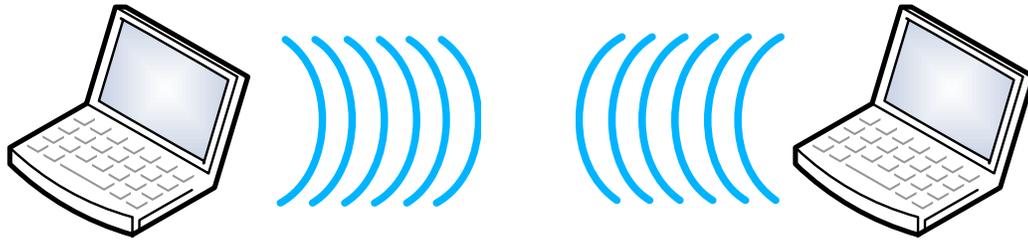


Figura 3.1: *Red ad-hoc*

3.3.2 Redes Infraestructura

Deriva de la extensión del concepto de cobertura celular (celdas) que es típico de las redes de telefonía móvil. A diferencia de una red ad-hoc, la estación base recibe el nombre de Punto de Acceso. Este tipo de redes, mucho más complejo, requiere de una planificación más elaborada, ya que los puntos de acceso deben distribuirse estratégicamente para evitar que algunas zonas se queden sin cobertura, exista algún traslape en la señal, asegurar un ancho de banda mínimo para cada usuario, entre otras. Un punto de acceso puede soportar un cierto número de usuarios conectados, y en función de las condiciones de propagación, alcanzar un rango comprendido entre los 30m y varios cientos de metros.

A pesar de ser más complejo su diseño, existe la gran ventaja de movilidad. Un usuario conectado a algún punto de acceso puede desplazarse libremente por la zona de cobertura de la red, de modo que, si en algún momento abandona la cobertura del punto de acceso original, y pasará a la cobertura de otro, y su conectividad se mantiene (*roaming*). (Figura 3.2)

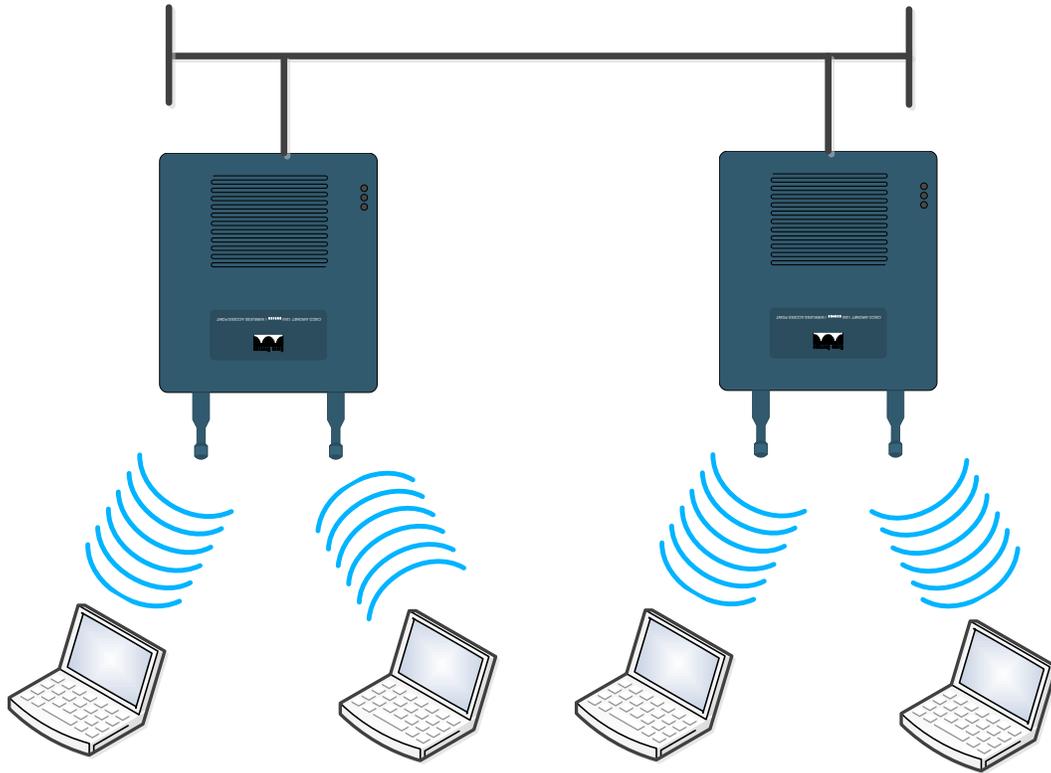


Figura 3.2: Red infraestructura

3.3.3 Radioenlace o Enlace Inalámbrico

Un radioenlace o enlace inalámbrico ofrece conectar varios segmentos de red de manera inalámbrica. Estos enlaces pueden ser punto a punto o punto a multipunto. En el primer caso, se utilizan antenas directivas que, bien en RF o bien en banda infrarroja, soportan el canal de comunicación entre los 2 extremos. En contraste, en los enlaces punto a multipunto, las antenas tienen un *beamwidth* mucho más amplio. (Figura 3.3)

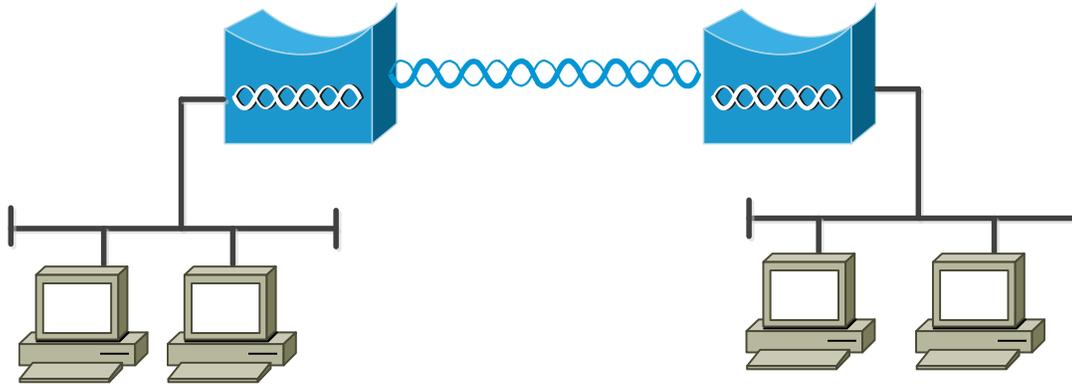


Figura 3.3. Radioenlace

3.4 Modelo OSI

Un estándar para ilustrar la arquitectura de una red y que pueda definir los protocolos y componentes necesarios para satisfacer los requerimientos de una aplicación es el modelo de referencia *OSI (Open System Interconnect)*, Sistema Abierto de Interconexión. Este sistema es creado en 1980 por la Organización Internacional de Estándares, que determina las diferentes etapas por la que deben atravesar los datos para viajar de un dispositivo a otro a través de una red de comunicaciones. Este modelo está dividido en siete capas:

3.4.1 Capa Física

Define las especificaciones eléctricas, mecánicas y funcionalidades para la activación, mantenimiento y desactivación del enlace físico para la transmisión de bits entre los dispositivos involucrados. Establece especificaciones tales como niveles de voltaje, tiempos de cambios de voltaje, velocidades de transmisión de datos, distancias máximas de transmisión, conectores físicos, y otros atributos similares. Para el caso de una red inalámbrica, ondas de radio y luz infrarroja.

3.4.2 Capa de Enlace.

Puntualiza cómo los datos se adecuan para su transmisión, y cómo es controlado el acceso al medio físico. Esta capa comúnmente incluye detención y corrección de errores para asegurar una entrega confiable de la información. Con las redes inalámbricas, más específicamente, regularmente se involucra la coordinación de acceso al medio (comúnmente el aire) y recuperación de errores que debe suceder en los datos como van propagándose desde el origen de las ondas hasta su destino.

3.4.3 Capa de Red

Proporciona conectividad y la selección de la ruta entre dos sistemas que puedan ser redes separadas geográficamente. El crecimiento de la Internet ha incrementado el número de usuarios que acceden a la información alrededor del mundo. La capa de red es aquella que administra la conectividad de estos usuarios, proporcionando un direccionamiento lógico. El protocolo IP (Internet Protocol) opera en este nivel.

3.4.4 Capa de Transporte

Define servicios para segmentar, transferir, y re ensamblar los datos para una comunicación individual entre dos dispositivos finales. El protocolo TCP (Transmission Control Protocol) trabaja en esta capa.

3.4.5 Capa de Sesión

Establece, administra y finaliza sesiones entre dos equipos que se están comunicando. Esta capa también sincroniza un dialogo entre las capas de presentación de dos equipos y administra su intercambio de datos.

3.4.6 Capa de Presentación

Asegura que la información que es enviada a la capa de aplicación de un sistema sea “legible” por la capa de aplicación de otro sistema. Por ejemplo, esta capa traduce el código que pueden tener los datos al comunicarse con un sistema remoto hecho por otro vendedor.

3.4.7 Capa de Aplicación

Es la capa del modelo OSI más cercana al usuario. Proporciona servicios de red a las aplicaciones del usuario, tales como correo electrónico (SMTP, Simple Mail Transfer Protocol), transferencia de archivos (FTP, File Transfer Protocol), visualizador de páginas web (HTTP HyperText Transfer Protocol), entre otros.

3.5 Espectro radioeléctrico y normatividad

El espectro radioeléctrico es un concepto en materia de telecomunicaciones, vinculado a las comunicaciones inalámbricas y se entiende como el medio por donde se transfieren o propagan las ondas electromagnéticas que son utilizadas en este tipo de comunicaciones para transmitir información como por ejemplo datos, imágenes, voz, entre otros.

Cada dispositivo inalámbrico requiere funcionar en cierta banda de frecuencia. Cada banda tiene una anchura asociada. La autoridad normativa de cada país controla rigurosamente la asignación del espectro del radio a través de los procesos de licencias. Otras tareas de asignación las lleva a cabo la ITU (International Telecommunications Union). En la tabla 3.1 se recopilan algunas bandas de frecuencia comunes que son utilizadas en Estados Unidos, y que ha sido adoptado asimismo por México.

Banda	Banda de frecuencia
UHF ISM	902 – 928 MHz
Banda S	2 – 4 GHz
Banda S para ISM	2.4 – 2.5 GHz
Banda C	4 – 8 GHz
Enlace de bajada de satélite banda C	3.7 – 4.2 GHz
Radar de banda C	5.25 – 5.925 GHz
Banda C para ISM	5.725 – 5.875 GHz
Enlace de subida de satélite banda C	5.925 – 6.425 GHz
Banda X	8 – 12 GHz
Radar de banda X	8.5 – 10.55 GHz
Banda Ku	12 – 18 GHz
Radar de banda Ku	15.7 – 17.7 GHz

Tabla 3.1 *Bandas de frecuencia*

En esta tabla aparecen tres bandas etiquetadas como ISM (*Industrial, Scientific, Medical*) Industrial, Científico y Médico, las cuales se han establecido para el equipamiento que está relacionado con los procesos industriales, científicos, o que utiliza un equipamiento médico; son particularmente importantes, ya que se permite su funcionalidad con un licenciamiento gratuito, siempre y cuando los dispositivos cumplan determinadas restricciones de potencia.

3.6 Alianza Wi-Fi

La Alianza de Fidelidad Inalámbrica (*Wireless Fidelity Alliance*) es una organización internacional creada en 1999 enfocada en el mercado e interoperabilidad de los productos inalámbricos 802.11. Esta organización empezó su trabajo y fue conocido como *Wireless Ethernet Compatibility Alliance (WECA)*.

La Alianza *Wi-Fi* tiene tres principales tareas:

1. Promover la certificación *Wi-Fi* alrededor del mundo alentando a los fabricantes a seguir los procesos de estandarización 802.11 en el desarrollo de sus productos inalámbricos.
2. Sellar/marcar los productos *Wi-Fi* certificados.
3. Probar y certificar la interoperabilidad de productos *Wi-Fi*

3.7 Características de las señales RF

Una señal *RF* se propaga entre las dos antenas de las estaciones emisora y receptora. Esta señal que alimenta la antena tiene una amplitud, frecuencia y fase. Estos atributos varían en tiempo con el fin de representar información.

La **amplitud** indica la intensidad de una señal RF. La medida de la amplitud es generalmente la potencia. En términos de las señales electromagnéticas, la potencia representa la cantidad de energía necesaria para transmitir la señal a través de una determinada distancia. A medida que la potencia se incrementa, el alcance de la señal también lo hará.

La **frecuencia** describe cuantas veces por segundo la señal se repetirá a sí misma. La unidad de la frecuencia es el Hertz (Hz), el cual es el número de ciclos ocurriendo por segundo.

La **fase** corresponde a qué tanto la señal está atrasada desde un punto de referencia. Cada ciclo de la señal se distribuye en 360 grados. Una variación en fase es regularmente útil para portar información. Por ejemplo, una señal puede representar el binario 1 cuando un desplazamiento de fase tiene 30 grados y el binario 0 cuando se tiene el desplazamiento de 60 grados. Una ventaja significativa de representar datos con la fase es que las deficiencias que suceden en la

propagación de la señal a través del medio no tienen mucho impacto. Estas deficiencias generalmente afectan la amplitud, no la fase de la señal.

3.8 Modulación

No es práctico transmitir las señales de información en su forma original. Las señales moduladas presentan una ventaja primordial. Si bien éstas pueden variar en amplitud, frecuencia y fase de una señal portadora, su amplificación no genera problemáticas en su transmisión, ya que las señales no son percibidas por el oído humano, encontrándose más allá del rango de percepción.

La modulación adecúa una señal de radio o una señal luminosa a partir de los datos de un dispositivo o de una red para su propagación a través del medio. Como parte de este proceso, la modulación superpone las señales de la información en una portadora, la cual es una señal con determinada frecuencia. Como consecuencia, la información viaja sobre la portadora. Con el fin de representar la información, las señales moduladas varían la frecuencia de su portadora de tal manera que representen datos.

Una moduladora mezcla señales de información origen, como la voz o los datos, con una señal portadora. El transceptor recibe la señal modulada y amplifica las señales hacia una antena. La señal modulada sale de la antena y se propaga a través del medio. La antena de la estación receptora manda la señal modulada hacia un demodulador, el cual filtra la señal portadora obteniendo las señales de información origen. A continuación se ejemplifican algunos tipos de modulación.

3.8.1 Modulación por desplazamiento de frecuencia

FSK (Frequency Shift-Keying) realiza ligeros cambios a la frecuencia de la señal portadora con el fin de representar información de tal manera que se adecúe a la

propagación sobre el medio. Por ejemplo, como se muestra en la Figura 3.4, este tipo de modulación puede representar un 1 o un 0 binario con un desplazamiento positivo o negativo en la frecuencia de la señal portadora. Si el desplazamiento en frecuencia es negativo, hay un desplazamiento de la portadora a una baja frecuencia; el resultado es un 0 Lógico. El receptor puede detectar este desplazamiento en frecuencia y demodular el resultado como un dato de bit 0.

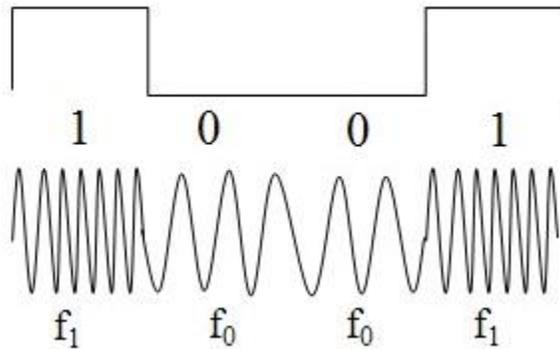


Figura 3.4. PSK, Modulación por desplazamiento de frecuencia

3.8.2 Modulación por desplazamiento de fase

Varios sistemas inalámbricos utilizan PSK (*Phase Shift-Keying*) para propósitos de modulación. Con PSK, los datos representados causan cambios en la fase de la señal mientras la frecuencia permanece constante. El desplazamiento de fase, como se muestra en la Figura 3.5, puede corresponder a un desplazamiento en fase positivo o negativo a partir de una referencia. Un receptor es capaz de detectar estos desplazamientos en fase y pueden interpretar los bits recibidos.

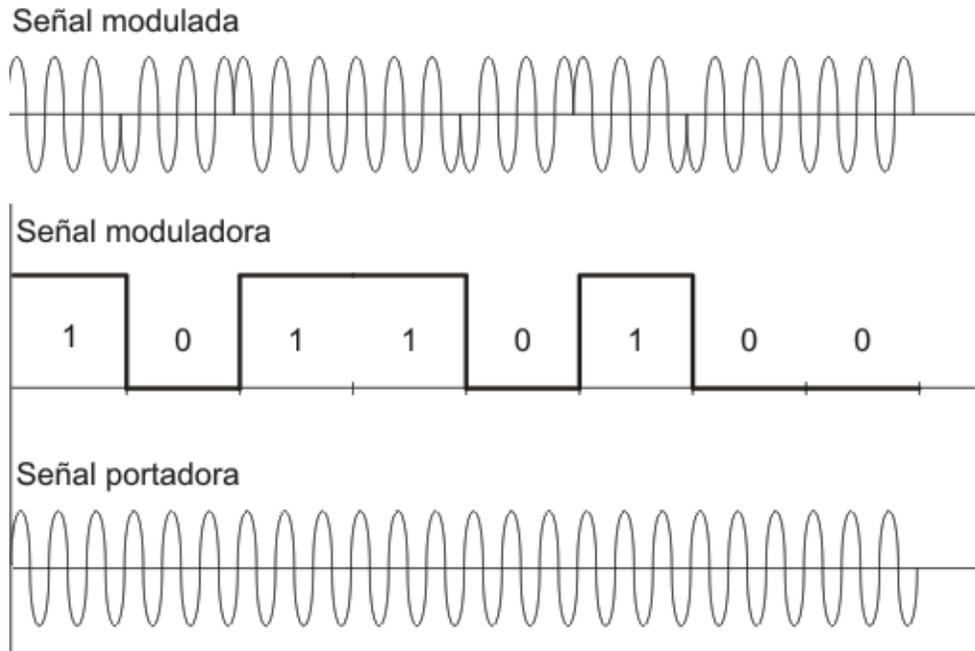


Figura 3.5. PSK, Modulación por desplazamiento en fase

La modulación PSK más sencilla es la BPSK (*Binary PSK*), en la que únicamente existen dos símbolos posibles (1 y 0), donde la figura anterior representa esta modulación y su constelación es mostrada en la Figura 3.6. La constelación es el conjunto de símbolos que representa la información.

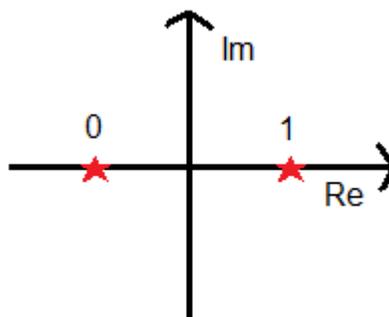


Figura 3.6. Constelación para BPSK

Otro tipo de modulación en fase es la *QPSK* (*Quaternary PSK*) donde su constelación puede apreciarse en la Figura 3.7. Su característica principal es la alta eficiencia espectral y la capacidad para aumentar la velocidad de transmisión gracias a que emplea más *bits* para codificar los símbolos. Sin embargo, la desventaja es que cuanto mayor sea esta velocidad, será mayor la susceptibilidad al ruido.

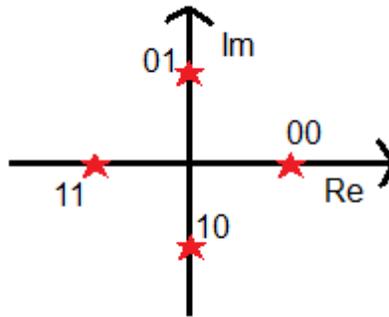


Figura 3.7. Constelación para QPSK

En la modulación *8PSK* se utilizan 3 bits para representar los símbolos, por tanto entre cada símbolo habrá un desfase de 45° (Figura 3.8). Este es el esquema de modulación empleado por *EDGE*.

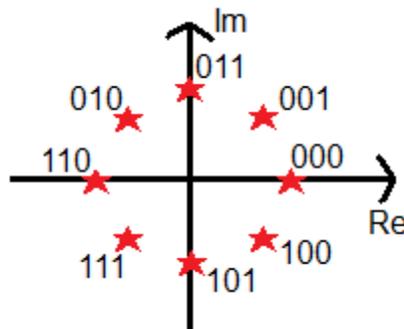


Figura 3.8. Constelación para 8PSK

Otro tipo de modulación en fase es la modulación *GMSK* (*Gaussian Minimum Shift Keying*), utilizado cuando la técnica de acceso es *TDMA*. Se trata de una modulación

binaria en la que la señal se pasa por un filtro gaussiano antes de su modulación. Es utilizada en redes *GSM*.

3.8.3 Modulación por amplitud de cuadratura

QAM (*Quadrature Amplitude Modulation*) provoca que tanto la amplitud como la fase de una señal portadora cambien con el fin de representar los símbolos (Figura 3.9). La ventaja de *QAM* es su capacidad de representar varios grupos de bits como una combinación de amplitud y una fase determinadas. De hecho, algunos sistemas basados en *QAM* hacen uso de 64 combinaciones de fase y amplitud, esto da como resultado la representación de 6 bits de datos por símbolo. Esto hace posible en estándares como 802.11a y 802.11g soportar tasas de velocidad más altas.

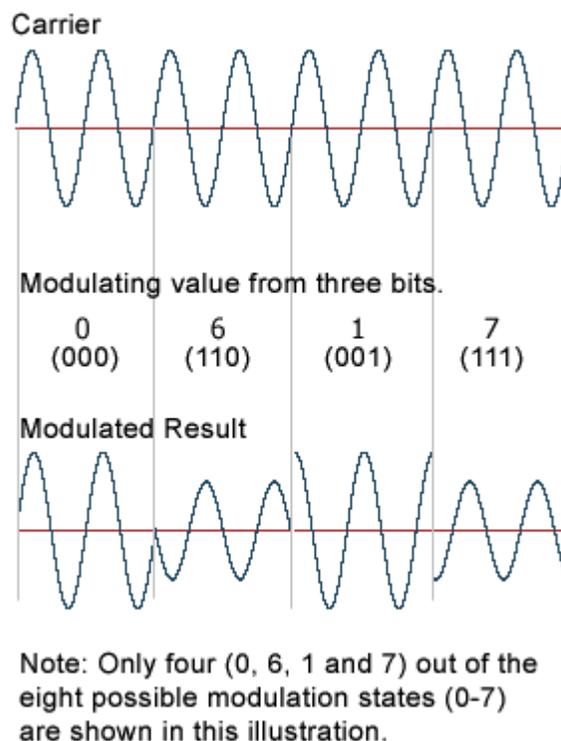


Figura 3.9. *QAM. Modulación de Amplitud en Cuadratura de 8 combinaciones (símbolos)*

3.9 Espectro Disperso

El espectro disperso, desarrollado por la milicia, distribuye la potencia de una señal sobre una banda amplia de frecuencias, ver Figura 3.10.

Además de modular la señal digital en una señal portadora analógica utilizando *FSK*, *PSK* o *QAM*, algunas redes inalámbricas también distribuyen la portadora modulada sobre un espectro más amplio con el fin de cumplir reglas en regulación y normatividad. Este proceso es llamado *espectro disperso* (*spread spectrum*), el cual significativamente reduce la posibilidad de mandar y/o recibir interferencia a la señal. Esto representa una herramienta eficaz para la supresión de ruido.



Figura 3.10 Espectro disperso

Los componentes de radio del espectro disperso pueden utilizar **salto de frecuencia** o **secuencia directa** para distribuir la señal.

3.9.1 Salto en Frecuencia (*Frequency Hopping*)

Como su nombre lo implica, los dispositivos móviles, coordinados van saltando simultáneamente de frecuencia en frecuencia, utilizando un patrón fijo. El receptor puede recibir datos del espectro disperso por salto de frecuencia si tanto el emisor como el receptor utilizan el mismo patrón de saltos que es controlado por un algoritmo de secuencialización que se establece durante una sesión de encuentro o negociación inicial. En la figura 3.11 se muestra una gráfica de tiempo contra frecuencia para el salto en frecuencia.

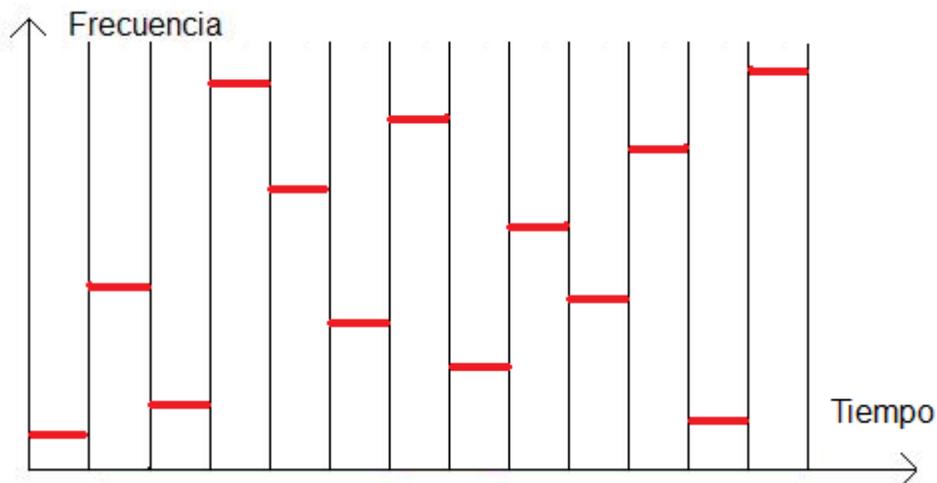


Figura 3.11 Salto de frecuencia

3.9.2 Secuencia Directa (*Direct Sequence*)

Este método de dispersión de espectro modula una portadora de radio por un código digital a una velocidad de transmisión mucho más alta que con el ancho de banda de la señal y su información. La Tabla 3.2 ejemplifica la secuencia directa.

Si los bits de los datos son: 1001
 El código de trozo es: 1=00110011011 0=11001100100
 Los datos transmitidos serían:
 110011011 11001100100 11001100100 110011011
 1 0 0 1

Tabla 3.2 *Secuencia Directa*

3.9.2.1 Canales de Secuencia Directa y Dominio Regulatorio

Cada país tiene sus propios organismos reguladores y algunos de ellos pueden permitir tener hasta 14 canales disponibles. En algunos países (incluidos México), reducen su posibilidad de utilizar 11 canales. En la tabla 3.3 se ilustra qué dominios regulatorios (conjunto de países) están disponibles cada frecuencia central para su utilización.

Identificador de canal	Frecuencia Central [MHz]	Dominio Regulatorio			
		Américas	Europa, Europa Oriental y Asia	Japón	Israel
1	2412	X	X	X	
2	2417	X	X	X	
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	
11	2462	X	X	X	
12	2467		X	X	
13	2472		X	X	
14	2484			X	

Tabla 3.3. *Dominios Regulatorios*

Nota: México está incluido en el Dominio Regulatorio de las Américas; sin embargo, es posible solo tener en uso interno (*indoor*) todo el rango de canales del dominio (1 al 11), pero únicamente de los canales 8 al 11 para uso externo (*outdoor*).

Con la secuencia directa, la energía es distribuida sobre un área y cada canal tiene un ancho de banda de 22 MHz. Esto permite 3 canales sin traslapes y sin interferencias con otros para poder ser utilizados en la misma área. Esto es también el esquema de canal 802.11. En la Figura 3.12 se puede apreciar que los 3 canales sin traslapes son los canales 1,6 y 11 (en rojo) para el dominio regulatorio de las Américas.



Figura 3.12 *Canales en DSSS para las Américas*

Por otra parte, la Figura 3.13 ilustra el dominio regulatorio de Japón donde utilizan 1 canal extra sin traslape (en morado), adicionalmente los canales 12 y 13.

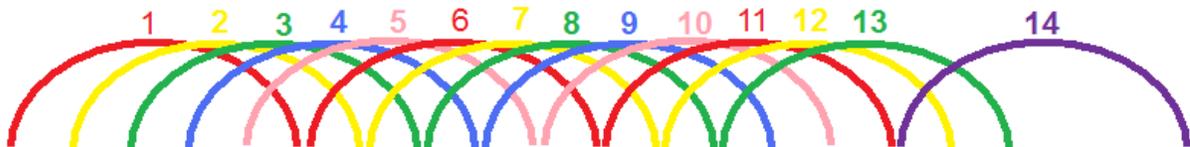


Figura 3.13 *Canales en DSSS para Japón*

3.10 Multiplexaje por División de Frecuencia Ortogonal

En lugar de usar espectro disperso, algunos sistemas inalámbricos hacen uso de *OFDM* (*Orthogonal Frequency Division Multiplexing*). Este procedimiento divide una portadora de datos de alta velocidad, dividiéndolas en varias sub-portadoras las cuales transmiten información en paralelo, ver Figura 3.14. Cada portadora de alta velocidad tiene un ancho de banda de 20 MHz y es dividida en hasta en 52 subcanales de datos, cada una en aproximadamente de 300kHz de ancho de banda. *OFDM* utiliza 48 de estos canales para datos, mientras los restantes 4 son usados para corrección de errores. El Código de Multiplexaje por División de Frecuencia Ortogonal (*COFDM*) entrega velocidades más altas de transmisión y un alto grado de recuperación de errores por la reflexión por multitrayectoria, gracias a su esquema de codificación y corrección de errores.

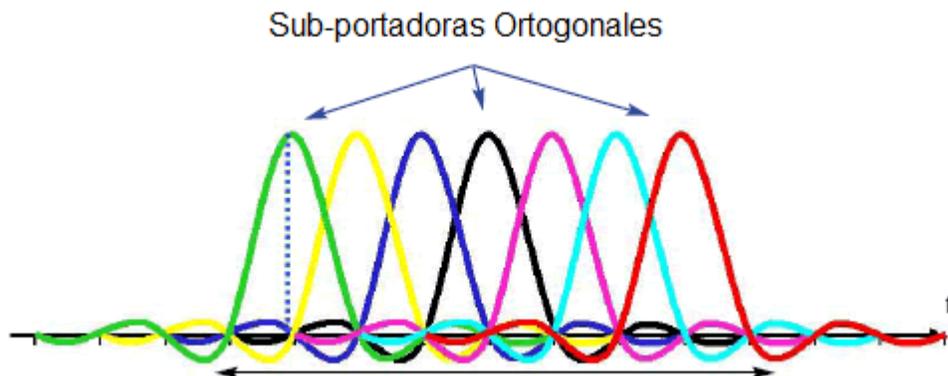


Figura 3.14 OFDM

Cada subportadora tiene 300kHz, en el extremo inferior del gradiente de velocidad. La Modulación por Desplazamiento de Fase Binaria (*BPSK*) es utilizada para decodificar 125 kbps de datos por canal, dando como resultado 6,000 Kbps, o 6 Mbps de velocidad de transmisión. Utilizando la Modulación por Desplazamiento de Cuadratura de Fase (*QPSK*), se puede duplicar la cantidad de datos codificados a 250 Kbps por canal, obteniendo una tasa de velocidad de trasmisión de 12 Mbps. Y

al utilizar la Modulación por Cuadratura de Amplitud a un nivel 16 (16-QAM) codificando 4 bits por Hertz, se logra una tasa de transmisión de 24 Mbps. Las velocidades de 54 Mbps son alcanzadas al utilizar un nivel 64 de Modulación por Cuadratura de Amplitud (64-QAM), en el cual se tienen 8 bits por ciclo o 10 bits por ciclo, por un total de hasta 1.125 Mbps por canal (300 kHz). Con 48 canales, dan como resultado velocidades de 54 Mbps. Se debe tener en cuenta que entre más bits por ciclo son codificados, existe mayor susceptibilidad de contraer mayor interferencia y existirá también atenuación en la señal. (Tabla 3.4)

Modulación con subportadoras	Tasa de Transmisión por subcanal [kbps]	Tasa Total de Transmisión[Mbps]
BPSK	125	6
BPSK	187.5	9
QPSK	250	12
QPSK	375	18
16QAM	500	24
16QAM	750	36
64QAM	1,000	48
64QAM	1,125	54

Tabla 3.4 Velocidades de transmisión para OFDM

3.11 Acceso al Medio

Para evitar que los datos de los usuarios interfieran entre sí, se utiliza la técnica de acceso al medio.

3.11.1 FDMA (*Frequency Division Multiple Access*)

En esta técnica de acceso al medio, el ancho de banda del canal se divide en porciones de menor ancho de banda y se asigna cada porción a un usuario para su uso exclusivo durante todo el tiempo que requiera. Tiene el inconveniente de que se

requieren bandas de guarda en las que no se envíe información para evitar así las interferencias. (Figura 3.15)

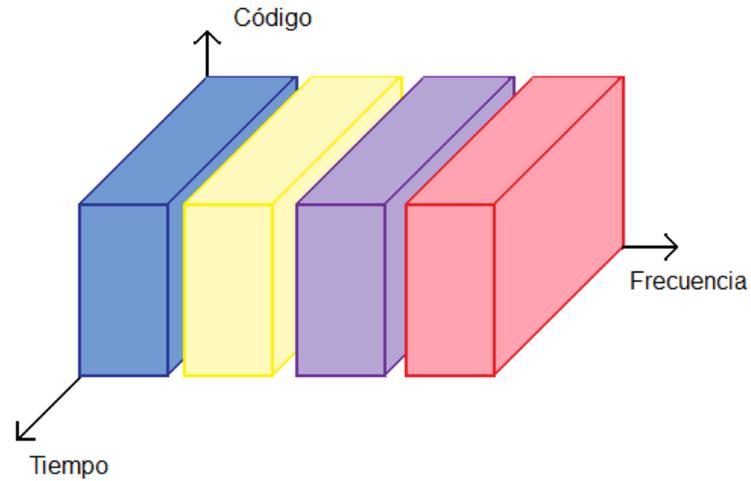


Figura 3.15. Acceso al medio FDMA

3.11.2 TDMA (Time Division Multiple Access)

Con *TDMA*, el ancho de banda se asigna completamente a cada usuario durante ranuras de tiempo ya que lo que se divide es el tiempo de acceso al canal. (Figura 3.20)

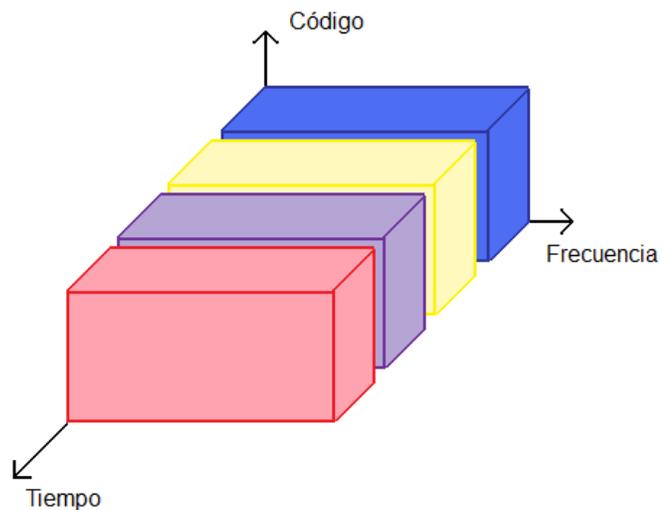


Figura 3.16. Acceso al medio TDMA

3.11.3 CDMA (Code Division Multiple Access)

La técnica más empleada en las redes inalámbricas es *CDMA*. A cada usuario se le asigna un código distinto de manera que todos los usuarios pueden ocupar la misma frecuencia. Para identificar la señal procedente de cada uno se realiza una correlación, con su código tras la que se obtendrá la señal deseada. Este tipo de acceso al medio es en el que se basan las técnicas de espectro disperso. (Figura 3.17)

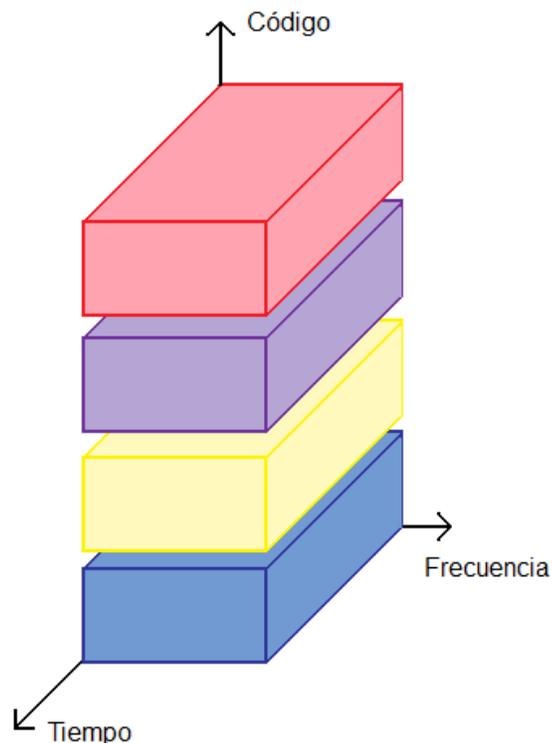


Figura 3.17. Acceso al medio CDMA

3.12 Potencia de una señal

Otra característica que debe ser incluida es la potencia de una señal de Radio Frecuencia. La intensidad de una señal puede ser definida como el rango de una señal. Así como una señal RF se va desplazando, interactúa con sus alrededores (moléculas de aire, muros, humedad, etc.) y pierde parte de su energía provocando atenuaciones. El dispositivo receptor tiene un límite inferior, llamado umbral de

recepción, que define la cantidad de energía mínima que se necesita para recibir la señal y poder interpretar de forma adecuada la información que contiene.

Si la potencia de la señal está por debajo del umbral de recepción, la información contenida en la señal no puede ser apropiadamente decodificada y se vuelve inservible. Es necesario mantener cierto nivel de la potencia de la señal por encima del umbral de recepción.

Las señales de RF son objeto de varias pérdidas e incrementos de energía cuando van pasando desde el transmisor hasta la antena, atravesando también el cable, y, finalmente a la antena receptora. La mayoría de todos estos factores que provocan estas pérdidas se pueden utilizar en el proceso de diseño para determinar si un sistema RF, como por ejemplo, una WLAN, funcionará. Para entender cómo evaluar estos sistemas, se deben saber cuantificar estos parámetros.

3.12.1 Decibeles

La escala decibel es una escala logarítmica usada para expresar la relación de dos magnitudes: la magnitud que se estudia y la magnitud de referencia:

$$\text{dB} = 10 \log_{10} (\text{Potencia A} / \text{Potencia B})$$

Un incremento de 3dB indica una duplicación (2x) de potencia. Un incremento de 6dB indica una cuadruplicación (4x) de potencia. De la misma manera, un decremento de 3dB significa que la potencia ha disminuido la mitad (1/2), y un decremento de 6dB indica que ha disminuido a una cuarta parte (1/4). En la Tabla 3.5 se muestran más ejemplos.

Incremento	Factor	Decremento	Factor
0dB	1x (igual)	0dB	1x (igual)
1dB	1.25x	-1dB	0.8x
3dB	2x	-3dB	0.5x
6dB	4x	-6dB	0.25x
10dB	10x	-10dB	0.10x
12dB	16x	-12dB	0.06x
20dB	100x	-20dB	0.01x
30dB	1,000x	-30dB	0.001x
40dB	10,000x	-40dB	0.0001x

Tabla 3.5: Valores en decibeles y su correspondiente factor

3.12.2 Potencia nominal

La potencia nominal del transmisor de la mayoría del equipo inalámbrico está regularmente detallada en decibeles en comparación con los conocidos valores de mW (miliWatts) o W (watts).

La sensibilidad de la potencia de transmisión y recepción se especifican en dBm, donde *m* significa 1 miliWatt (1mW). Un valor de 0 simboliza una cantidad igual a 1 mW, y basándonos de la tabla 3.5, se puede calcular que 3 dBm son iguales a 2mW, así como 6dBm equivalen a 4mW, etcétera. Por ejemplo, un sistema que irradia 100 mW de potencia de transmisión, es similar que si estuviera irradiando 20-dBm de potencia.

dBm	mW	dBm	mW
0	1	0	1
1	1.25	-1	0.8
3	2	-3	0.5
6	4	-6	0.25
7	5	-7	0.2
10	10	-10	0.1
12	16	-12	0.06
13	20	-13	0.05
15	32	-15	0.03

17	50	-17	0.02
20	100	-20	0.01
30	1000	-30	0.001
40	10000	-40	0.0001

Tabla 3.6: *Valores entre dBm y mW*

3.13 Especificaciones 802.11

El estándar 802.11 es, en realidad, un conjunto de especificaciones que abarcan todos los aspectos de una red WLAN. Las especificaciones de nivel físico (802.11a, 802.11b, 802.11g y 802.11n) definen las técnicas de modulación y el procesamiento de la señal a bajo nivel. En 1997 se ratificó el estándar inicial 802.11, que utilizaba FHSS (Frequency Hopping Spread Spectrum) en la banda de 2.4 GHz a una tasa de transmisión de 2Mbps. Posteriormente surgieron estándares más rápidos. A continuación se enumeran algunos de los estándares 802.11 más importantes.

802.11a Esta variante, a 5GHz, emplea una modulación 64-QAM y codificación OFDM. Alcanza una tasa de transmisión nominal de hasta 54 Mbps aunque con un alcance limitado a 50 m, algo que complica la infraestructura de red al ser requeridos más puntos de acceso, con el costo adicional que ello supone. (Tabla 3.7)

802.11b. El estándar 802.11b, más conocido como WiFi, nació como una versión del 802.11 original para WLAN corporativas. Ofrece tasas de transmisión normalizadas de 11Mbps, 5.5 Mbps, 2 Mbps y 1 Mbps y un alcance se 100 m. Trabaja en la banda libre de 2.4 GHz pero utiliza DSSS, una modulación lineal compleja. (Tabla 3.7)

802.11g. Alcanza tasas de transmisión de hasta 54 Mbps en la banda de los 2.4 GHz. Una de sus ventajas es que puede coexistir con los equipos 802.11b ya instalados, aunque los equipos 802.11g se verán obligados a trabajar a 11 Mbps. Utiliza OFDM. (Tabla 3.7)

802.11i. Uno de los puntos críticos de las redes WLAN es la seguridad. Al ser comunicaciones tipo radio, cualquiera con los dispositivos adecuados puede acceder a la información que se transmite por el medio. Los mecanismos de seguridad definidos en el estándar original no son suficientes y, por esta razón, se ha ampliado para garantizar la autenticación de usuarios y el cifrado de la información.

802.11n. Los estándares anteriores ofrecen tasas de transmisión teóricas de 11Mbps (802.11b) y 54 Mbps (802.11a/g). Sin embargo, en la práctica, el usuario ve reducida esta tasa drásticamente (5Mbps y 20Mbps, respectivamente). Estas tasas de transmisión resultan poco comparables con los 100 Mbps o 1 Gbps que soportan las redes locales convencionales.

El estándar 802.11n pone a disposición del usuario tasas reales cercanas a los 100Mbps. Todos los dispositivos 802.11n son totalmente compatibles con equipos 802.11a, 802.11b y 802.11g.

	802.11b	802.11a	802.11g
Banda de frecuencia	2.4 GHz	5GHz	2.4GHz
Canales	3	Hasta 23	3
Transmisión	Espectro Disperso por Secuencia Directa (DSSS)	Multiplexaje por División de Frecuencia Ortogonal (OFDM)	DSSS / OFDM
Tasa de transmisión (Mb/s)	1,2,5.5,11	6,9,12,18,24,36,48,54	1,2,6,5.5,9,11,12,18,24,36,48,54

Tabla 3.7 Bandas, canales y trasmisiones para 802.11b, a y g

3.14 Seguridad para la red inalámbrica

La seguridad es de vital importancia en las redes inalámbricas, principalmente porque las señales están completamente disponibles y abiertas en el medio. Las compañías e individuos que utilizan frecuentemente las redes inalámbricas deben tener la precaución de los problemas potenciales y la manera de combatirlas.

3.14.1 SSID

La Identidad de Conjunto de Servicio (*Service Set Identifier*) es el nombre de una red para permitir a los usuarios identificar una red inalámbrica. Este por lo general se relaciona con una VLAN de la red.

3.14.2 Encriptación

Es el proceso para volver ilegible la información. Es una medida para transferir información y que no pueda ser accesible a terceros.

La encriptación altera los bits de cada paquete de datos. Antes de la encriptación, los datos son llamados “textos planos”, los cuales son fáciles de decodificar usando determinadas herramientas (*sniffers*). La encriptación convierte el texto plano en texto cifrado, el cual se puede decodificar solo con el uso de una llave secreta apropiada. El proceso se ilustra en la figura 3.18.

Existen muchos métodos de encriptación tal como el método 802.11 *Wired Equivalent Privacy* (WEP), el cual es simétrico, esto es que la llave que realiza la encriptación, también realiza la desencriptación.

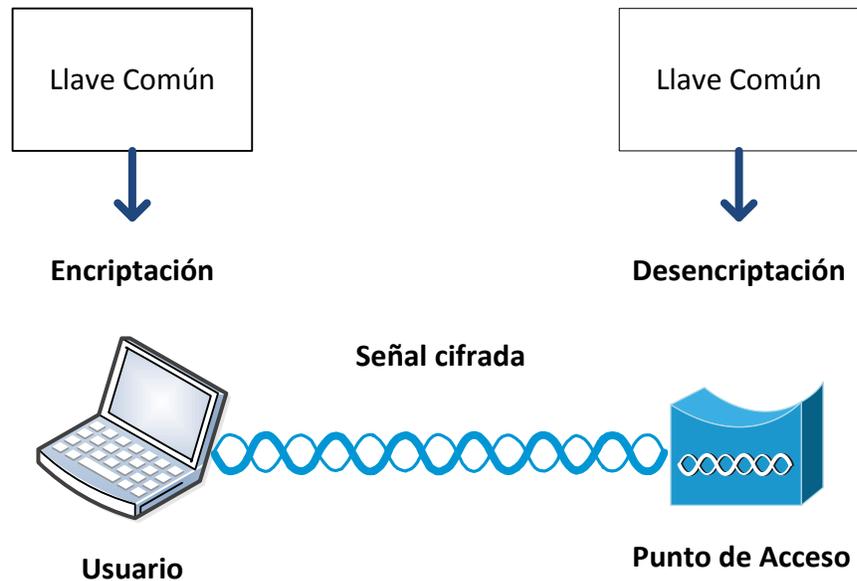


Figura 3.18 *Encriptación*

3.14.3 Autenticación

Es el proceso de comprobar una identidad, y el estándar 802.11 especifica dos maneras:

- a. Un sistema de autenticación abierta
- b. Una autenticación de llave compartida.

El sistema de autenticación abierta se da en dos procesos. Un cliente inicializa el proceso mandando una trama de solicitud de autenticación al Punto de Acceso o equipo de acceso inalámbrico. Este responderá con una trama de respuesta de la autenticación aprobando o no la petición.

La autenticación de llave compartida se da en cuatro pasos que basa su autenticación si el dispositivo tiene una llave WEP correcta. El cliente empieza enviando una trama de solicitud de autenticación al equipo de acceso inalámbrico. Este a su vez, coloca un *texto identificador* en el cuerpo de la trama que responderá

y la envía de regreso al equipo que inicia la comunicación, así utilizará la llave WEP para encriptar el *texto identificador* y mandarlo de regreso una vez más al punto de acceso inalámbrico en otra trama. El punto de acceso finalmente desencripta el “texto desafío” y lo compara con su texto inicial. Si el texto es igual, el punto de acceso asume que el usuario tiene la llave correcta, y finaliza su secuencia mandando una trama que autoriza su acceso.

Este proceso puede utilizar un servidor de autenticación, como por ejemplo RADIUS (*Remote Authentication Dial-In User Service*), para ejecutar la autenticación.

3.14.3.1 Autenticación Usando Llave Criptográfica Pública

Además de proteger la información de los *hackers*, las estaciones pueden usar una llave criptográfica pública para autenticarse a ellos mismos o con otras estaciones o puntos de acceso. Esto es necesario antes de que un punto de acceso o controlador permita a una estación en particular interferir con una zona protegida de la red. De la misma manera, el cliente puede autenticarse al punto de acceso.

Una estación se autentica a si misma encriptando una cadena de texto dentro de un paquete usando su llave privada. La estación receptora desencripta el texto con la llave publica de la estación emisora. Si el texto desencriptado coincide al texto predeterminado, tal como el nombre de la estación, la estación receptora sabe que la estación emisora es válida. La encriptación de una cadena en particular de texto en este caso actúa como una firma digital. La figura 3.19 ilustra el proceso anterior.

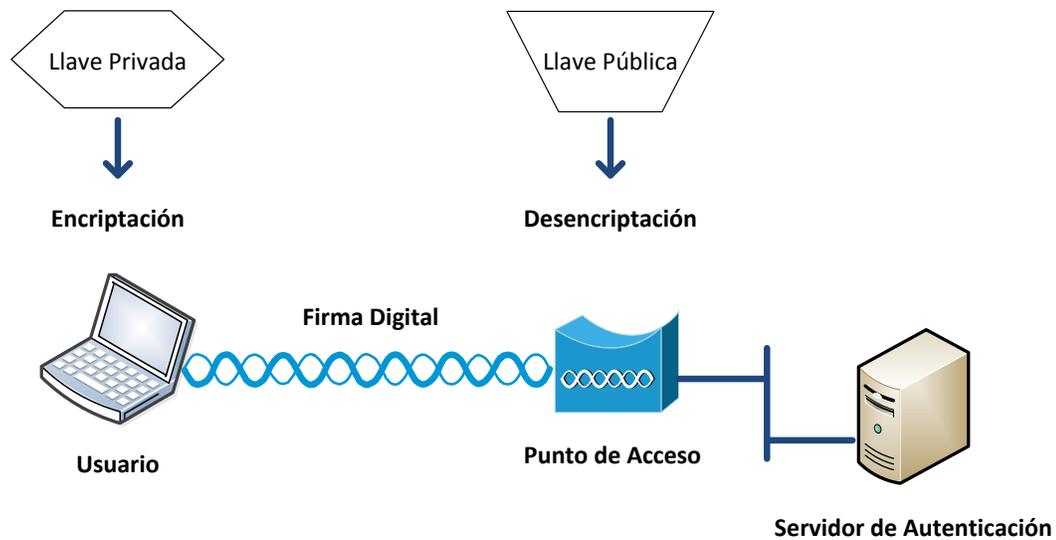


Figura 3.19 *Encriptación con llave pública y privada*

➤ 802.1x

Es un mecanismo de autenticación a nivel puerto. La especificación describe la interacción de tres entidades que forma cualquier sistema de autenticación:

- La parte que se debe autenticar (*suplicant*)
- La que debe aprobar o denegar el acceso (*authenticator*)
- Un servidor de autenticación ubicado en un equipo separado o junto al *authenticator*.

El uso de IEEE 802.1x ofrece un marco efectivo para autenticar y controlar el tráfico a una red protegida de manera automática, como también la rotación dinámica de llaves de encriptación. 802.1x liga un protocolo llamado Protocolo Extensible de Autenticación (*EAP Extensible Authentication Protocol*) a los medios alámbrico e inalámbrico y el soporte de múltiples métodos de autenticación, tales como las “*token cards*”, *Kerberos*, certificados, y llaves de autenticación públicas.

➤ Operación 802.1x

La comunicación inicial de 802.1x inicia con el *suplicant* sin autenticar (dispositivo cliente inalámbrico) tratando de conectar con un *authenticator* (estación base inalámbrica o punto de acceso). La estación base responde activando un puerto para dejar pasar sólo los paquetes EAP del cliente hacia el servidor de autenticación ubicado en la zona cableada de la red. La estación base bloquea todos los puertos del tráfico restante, tales como paquetes de HTTP, DHCP, POP, etcétera, hasta que la estación base pueda verificar la identidad del cliente usando un servidor de autenticación, como RADIUS. Una vez autenticado, la estación base abre el resto de los puertos para otro tipo de tráfico basado en los derechos de acceso que concede el servidor de autenticación.

3.14.3.2 Tipos de autenticación

Es importante resaltar que 802.1x no proporciona los mecanismos actuales de autenticación. Cuando se utiliza 802.1x, se necesita escoger un tipo de EAP (tal como *EAP TLS*, Protocolo Extensible de Autenticación con Seguridad de Capa de Transporte, o *LEAP*, Protocolo Ligero Extensible de Autenticación de Cisco), el cual define como toma lugar la autenticación. De acuerdo a cada software, puede soportar o no los distintos tipos de EAP en el servidor de autenticación y dentro del sistema operativo o el software de aplicación de cada dispositivo cliente.

3.14.4 Asociación

Cuando se finaliza el proceso de autenticación, el cliente debe asociarse con el punto de acceso inalámbrico, antes de mandar tramas de datos. La asociación es necesaria para sincronizar el usuario o cliente con el punto de acceso con información importante, tal como velocidades de transmisión soportadas. El cliente inicia la asociación mandando una trama de solicitud de asociación, esta contiene elementos importantes como *SSID* y velocidades de transmisión soportadas. El

punto de acceso responde mandando una trama de respuesta en la que contiene un identificador de asociación e información referente al punto de acceso. Una vez que el cliente y el punto de acceso terminan el proceso de asociación, ellos pueden intercambiar tramas de datos entre ellos.

Capítulo IV

CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE UN ENLACE INALÁMBRICO

4.1 Antecedentes

Los enlaces inalámbricos son utilizados para conectar dos o más LAN's, usualmente localizadas en distintos edificios y dentro de un área relativamente cercana, creando así una gran LAN. Los enlaces inalámbricos proporcionan velocidades de transmisión, en muchas ocasiones, más altas que una línea E1/T1. De esta manera, los enlaces inalámbricos eliminan la necesidad de rentar servicios alternativos para satisfacer la misma necesidad.

4.2 Roles en el Radio de la Red Inalámbrica

Existen dos tipos de topología de enlace inalámbrico que son normalmente implementados. Estos tipos son:

- Punto a punto
- Punto a multipunto

En el primer caso se extiende la red a un solo lugar a diferencia del segundo caso, donde se extiende a dos o más lugares. La figura 4.1 ilustra este concepto.

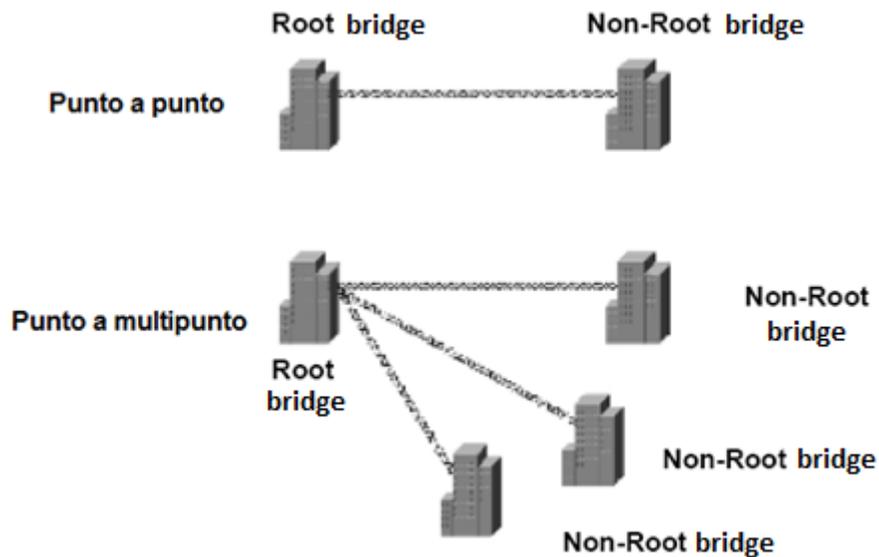


Figura 4.1 Tipos de Topología en un enlace inalámbrico

Como se muestra en la figura 4.1, tenemos dos roles en la red:

- *Root bridge* y
- *Non-root bridge*

El *Root bridge* es el rol para el equipo inalámbrico principal, en otras palabras, es el equipo que se conecta a la LAN principal para otros clientes alámbricos o inalámbricos. El *Non-root bridge*, en cambio, es para el o los equipos inalámbricos que se encuentra en las redes “satélite” de la red principal, y que requieren de algún modo para tener conectividad.

Para que estos equipos de acceso inalámbricos puedan iniciar su comunicación uno al otro, deben establecer una relación padre-hijo. Un equipo de acceso inalámbrico que es configurado como “*root bridge*” es considerado el equipo padre, mientras que el que es configurado como “*non-root bridge*” es el equipo hijo. El equipo hijo aprenderá varios de los parámetros configurables del equipo padre ya que podrá comunicarse con él.

Un solo equipo padre puede soportar varios equipos hijo. La cantidad de equipos hijo conectados al equipo padre será determinado por las necesidades de uso y cargas. Se tiene una excepción: Un equipo “*non-root*”, puede comunicarse con otro equipo “*non-root*” siempre y cuando exista un equipo “*root*” de por medio.

En algunos casos, los dispositivos que despliegan el enlace inalámbrico, pueden actuar también como Puntos de Acceso permitiendo clientes inalámbricos asociarse a dichos dispositivos.

4.3 VLANs

Una VLAN es un grupo de estaciones finales con un grupo de requerimientos comunes, independientemente de su ubicación. Una VLAN tiene los mismos atributos que una LAN física, pero permite agrupar estas estaciones aún cuando no están ubicadas físicamente en la misma subred.

El protocolo 802.1Q permite transportar sobre un solo enlace alámbrico o inalámbrico un conjunto de VLANs sin tener que utilizar un enlace para cada VLAN. (Figura 4.2)

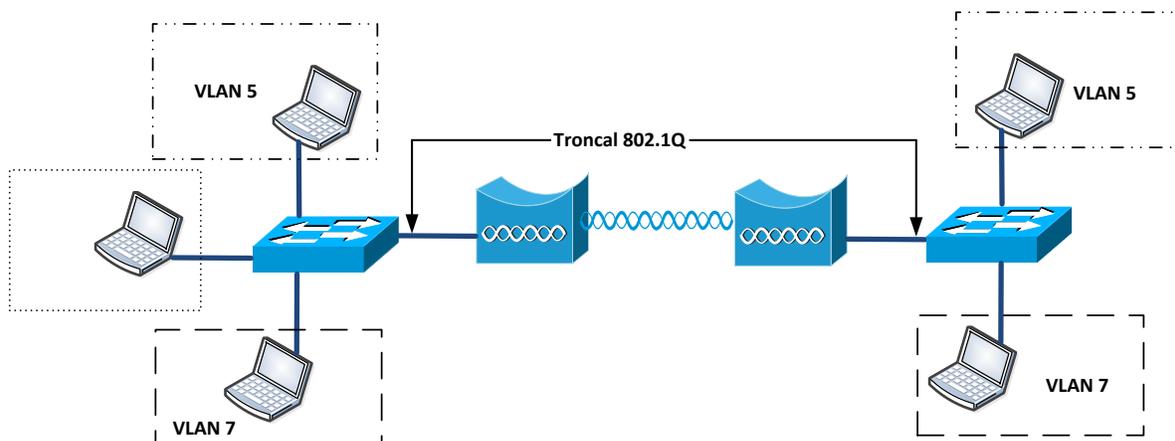


Figura 4.2 Topología del Enlace utilizando VLANs

4.4 Antenas

El correcto uso de las antenas puede mejorar el desempeño de una WLAN dramáticamente. De hecho, las antenas son probablemente la única manera más fácil de refinar el desempeño de la red inalámbrica. Toda antena tiene tres propiedades fundamentales:

- Ganancia
- Dirección
- Polarización

4.4.1 Ganancia

Es la cantidad de incremento en energía que una antena parece agregar a una señal RF. La ganancia de una antena es medida en comparación de una antena isotrópica o una antena tipo dipolo. Una antena isotrópica es una antena teórica con un patrón de radiación uniforme en todas direcciones. La medida dBi se utiliza para comparar el nivel de potencia de cualquier antena al de una antena isotrópica (por eso el uso de la *i* en dBi). Muchos organismos regulatorios hacen uso del dBi para definir los niveles de potencia en las políticas y regulaciones de las coberturas de las antenas. Una antena isotrópica tiene un nivel de potencia de 0 dBi (esto es, sin ganancias y sin pérdidas cuando se compara a si misma).

A diferencia de las antenas isotrópicas, las antenas dipolo son antenas físicas que son un estándar en varios productos inalámbricos. Las antenas dipolo tienen un patrón de radiación diferente comparadas con las isotrópicas. El patrón de radiación es de 360° sobre el plano horizontal y usualmente como 75° en el plano vertical (asumiendo que la antena está colocada verticalmente). Ver figura 4.3. Debido a que el haz de radiación está ligeramente concentrado, las antenas dipolo tienen una ganancia sobre las antenas isotrópicas en el plano horizontal. Las antenas dipolo tienen una ganancia de 2.14 dBi (en comparación de una isotrópica).

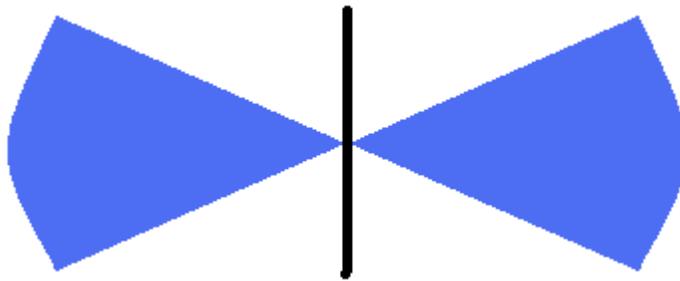


Figura 4.3 Vista Lateral del Patrón de Radiación de una Antena Dipolo

Algunas antenas son medidas en comparación con las antenas dipolo. Esto es denotado por el sufijo dBd. Debido a esto, las antenas dipolo tienen una ganancia de 0 dBd (0 dBd = 2.14 dBi).

Muchos proveedores de equipos inalámbricos han estandarizado sobre dBi para especificar medidas de ganancia. Sin embargo, algunos otros vendedores aun catalogan sus productos en dBd, en lugar de dBi, como punto de referencia. Para convertir cualquier número de dBd a dBi, simplemente hay que agregar 2.14 a la cantidad en dBd. Por ejemplo se tiene una antena de 3 dBd, al realizar la conversión, se tendrán 5.14 dBi, o si se redondea superiormente (práctica comúnmente utilizada), se tiene una ganancia de 5.2 dBi.

4.4.2 Propiedades Direccionales

Cualquier antena, excepto la antena isotrópica (teóricamente una antena perfecta que irradia igualmente en todas direcciones), tiene cierto patrón de radiación. Esto significa que irradia una mayor cantidad de energía en ciertas direcciones que en otras. Una analogía aplica cuando se tiene un reflector. Éste concentra e intensifica el haz de luz en una dirección en particular. Esto es muy similar a lo que las antenas parabólicas hacen con la señal RF.

La ganancia de la antena se forma con el área de cobertura o con lo que es conocido como *beamwidth* (ancho de haz). Cuando se va incrementando la ganancia de una antena, el ancho de haz, usualmente, disminuye. La energía total irradiada de una antena no se incrementa, solo se redirige.

4.4.2.1 Antenas Omni-Direccionales

Una antena omni-direccional está diseñada para proporcionar un patrón de radiación de 360° sobre el plano horizontal. Este tipo de antena es usada cuando se quiere tener una cobertura en todas las direcciones. La antena Rubber Duck de 2.14 dBi es una de las antenas omni-direccionales más comunes. Cuando una antena *omni* es diseñada para tener mayor ganancia, resulta tener pérdidas de cobertura en ciertas áreas.

4.4.2.2 Antenas Direccionales

Las antenas direccionales pueden ser utilizadas para proporcionar un rango más lejano en ciertas direcciones y aislar los radios de otras señales. Se pueden escoger de una gran diversidad de antenas direccionales, desde antenas que proporcionen rangos cortos y coberturas amplias hasta antenas que ofrezcan áreas de cobertura estrecha y sumamente específica. Como se mencionó antes, una antena no agrega ninguna potencia adicional a la señal, en lugar de esto, redirige la energía desde una dirección y la enfoca otra dirección en particular. Esto da como resultado mayor energía en ciertas direcciones y menor en otras, Así como va incrementándose la ganancia de una antena direccional, va disminuyendo su área de cobertura total. Ejemplos de antenas direccionales son las antenas parabólicas o de tipo platillo, antenas tipo parche y antenas Yagi.

4.4.3 Polarización

Son dos planos los que se usan para radiaciones RF: el plano E y el plano H. El plano E (campo eléctrico) define la orientación de las ondas de radio que van siendo irradiadas por la antena. Si el plano E es perpendicular a la superficie de la Tierra, se dice que tiene una polarización vertical. En sistemas inalámbricos por ejemplo, una antena omni-direccional es usualmente una antena verticalmente polarizada. El plano H (campo magnético) se propaga perpendicularmente al plano E.

Las antenas horizontalmente polarizadas (lineales) tienen su campo eléctrico paralelo a la superficie de la Tierra. Los equipos WLAN rara vez utilizan antenas horizontalmente polarizadas, excepto en ciertos sistemas para exteriores punto a punto.

4.4.4 Tipos de Antenas

Existen varios tipos de antenas que se puede escoger para aplicarlo en sistemas WLAN. A continuación se explicarán cuatro tipos de antenas principales.

4.4.4.1 Antena Parche

Esta antena es típicamente pequeña y plana y está usualmente diseñada para montarse en contra de un muro o de un soporte pequeño. Tiene un ancho de haz menor de 180° , y es a veces conocida como antena hemisférica. (Figura 4.4)



Figura 4.4 Antena parche

4.4.4.2 Antena Panel

Esta antena (a veces mencionada como antena sectorizada) es similar a la antena tipo parche, pero es generalmente de mayor ganancia y físicamente es más larga. La mayoría de las veces la antena tipo panel tiene un reflector trasero ajustable que es usado para cambiar el ancho de haz.

Son antenas que usualmente son usadas para exteriores y puede tener rangos de ganancias entre 5dBi hasta más de 20 dBi. Puede ser usada como una sola antena o se instalan varias para cubrir una extensa área. (Figura 4.5)



Figura 4.5 Antena panel

4.4.4.3 Antena Yagi

Una antena Yagi tiene una serie de pequeños elementos, conocidos como *reflectores* o *directores*, y un elemento activo. Estos son colocados sobre una línea y dirige la energía sobre una dirección dada. Las antenas Yagi generalmente tienen una ganancia bastante alta. Entre más reflectores y directores tenga la antena, mayor será la ganancia. (Figura 4.6)

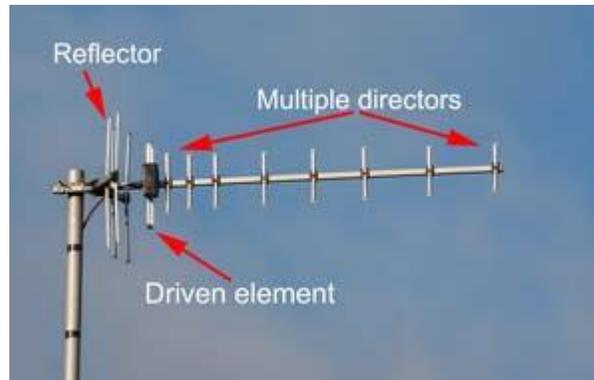


Figura 4.6 Antena Yagi

Debido a la longitud de onda de la frecuencia de los sistemas WLAN, los elementos son bastante pequeños, y la mayoría de las antenas Yagi usadas para frecuencias de 2.4GHz o 5 GHz tienen un tipo de cubierta para proteger los componentes de la antena del clima y para proporcionar mayor fortaleza estructural. Estas antenas tienen un rango en ganancia desde 5 dBi hasta ganancias de 17dBi o más. (Figura 4.7)



Figura 4.7 Antena Yagi para frecuencias 2.4 GHz

4.4.4.4 Antenas Platillo

Hay dos tipos de antenas tipo platillo: las parabólicas y las de malla (*grid dish*). La antena tipo parabólica tiene un reflector sólido y un elemento activo soportado en el centro del reflector. Estas son similares a las antenas comunes utilizadas para televisión restringida, excepto por la colocación del elemento activo que está centralizado sobre la antena de la WLAN. (Figura 4.8)



Figura 4.8 Antena platillo o antena parabólica

La antena platillo con malla (*grid dish*), es muy similar a la antena parabólica, excepto de que el reflector no es sólido. Este está hecho de una estructura tipo malla que permite al agua y viento atravesarlo. Esto proporciona menos resistencia al viento y por lo tanto requiere de una estructura de montaje más pequeña. (Figura 4.9)



Figura 4.9 Antena platillo en malla

4.5 Consideraciones para la Trayectoria

Para tener un óptimo desempeño del enlace inalámbrico entre ambos dispositivos, se debe considerar lo siguiente:

- a. Línea de Vista (LOS)
- b. Redondez de la Tierra
- c. Zona de Fresnel
- d. Antena y cableado
- e. Velocidad de transmisión

4.5.1 Línea de Vista (LOS: Line of Sight)

Para un enlace inalámbrico adecuando se debe tener una trayectoria clara y visible entre las dos antenas. No deben existir obstrucciones entre las antenas. Además, se deben tomar en cuenta otros factores de línea de vista como la curvatura de la tierra y la zona de Fresnel.

4.5.2 Redondez de la Tierra

Otro de los aspectos que se debe tomar en cuenta es la curvatura de la Tierra y la refracción atmosférica. Típicamente, con distancias menores a 11.26 km, la redondez de la Tierra puede ser omitida. (Figura 4.10)

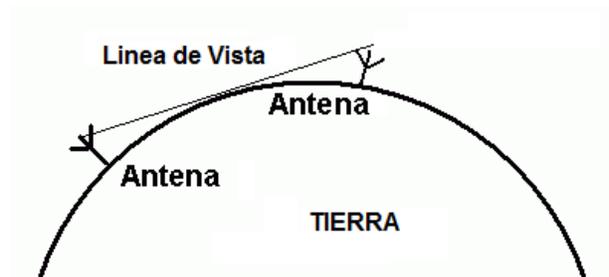


Figura 4.10 Curvatura de la Tierra

4.5.3 Zona de Fresnel

La zona de Fresnel es un volumen elíptico que rodea la trayectoria visual entre las antenas. Este se va modificando dependiendo de longitud de la trayectoria de la señal así como la frecuencia de operación. La zona de Fresnel puede ser calculada, y debe ser tomada en cuenta para cuando se diseña un enlace inalámbrico. Si la zona de Fresnel es obstruida entonces, no habrá una clara línea de vista necesaria para que el enlace sea confiable. Si las ondas de radio (incluso ondas de luz) encuentran obstáculos en el área de Fresnel cuando van atravesando el espacio libre hacia su destino, pueden ser atenuados severamente. El mejor rango y desempeño es alcanzado cuando no existe obstrucción en el área de Fresnel. Aunque esto no es siempre completamente inevitable, se debe mantener la mayor parte de la zona de Fresnel despejada.

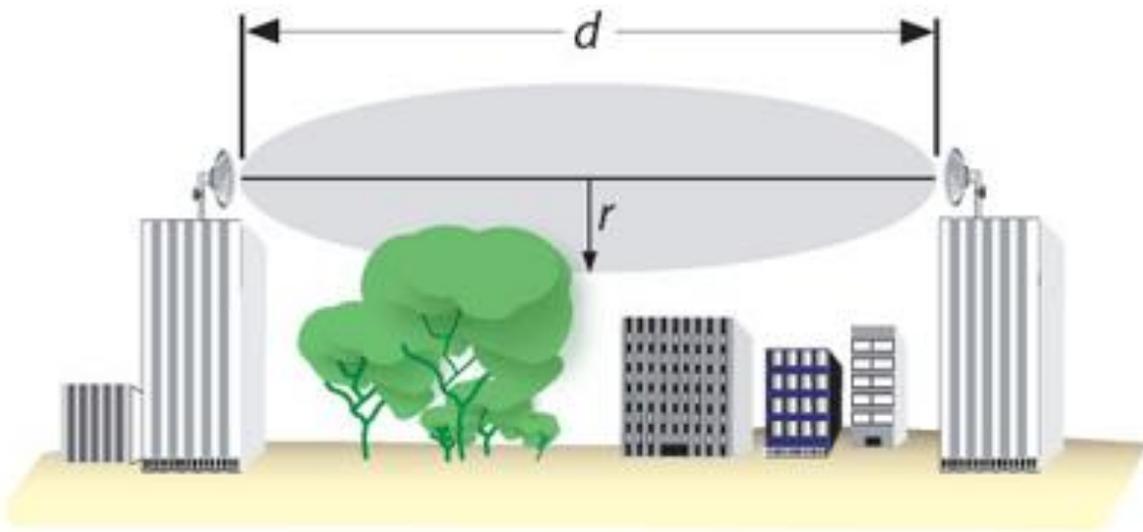


Figura 4.11 Zona de Fresnel entre un enlace inalámbrico

Para poder calcular el radio de la zona de Fresnel en cualquier distancia a lo largo de la trayectoria, se ha utilizado la siguiente ecuación:

$$r = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$

dónde:

- r = radio de la enésima zona de Fresnel (n = 1, 2, 3...)
- d₁ = distancia desde el transmisor al obstáculo en metros
- d₂ = distancia desde el obstáculo al receptor en metros.
- d = distancia total del enlace d = d₁ + d₂
- λ = longitud de onda en metros.

Debemos tomarnos en cuenta la definición de longitud de onda:

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8 [m \cdot s^{-1}]}{f [Hz(s^{-1})]}$$

Primero, ajustamos la ecuación para la primera zona de Fresnel **n = 1**, ya que aquí se concentra el 50% de la potencia de la señal. Segundo asumimos que d₁ = d₂, por lo tanto d = 2d₁.

$$r = \sqrt{\frac{c d_1 d_2}{f d}} [m] = \sqrt{3 \times 10^8} \cdot \sqrt{\frac{d_1 d_1}{2d_1}} [m] = 17320.51 \sqrt{\frac{d_1}{2}} [m]$$

Y considerando que d₁ = d / 2, queda al final la siguiente ecuación:

$$r = 17,320.51 \sqrt{\frac{d(m)}{4f(Hz)}} [m]$$

Ahora bien, si se aplica esta ecuación, el alcance varía dependiendo de cuan libre estén las zonas de Fresnel, además también depende de la frecuencia de operación. Esta ecuación nos puede dar una idea de que distancia debe encontrarse la antena

del suelo para mantener lo más libre posible la zona de Fresnel y mantener un enlace estable.

Para mantener la zona de Fresnel despejada, se pueden realizar las siguientes acciones:

- ✓ Elevar el punto de montaje de la antena en una estructura existente.
- ✓ Erigir una nueva estructura, por ejemplo una torre de radio suficientemente alta para montar la antena.
- ✓ Localizar diferentes puntos de montaje para la antena.
- ✓ Derribar los árboles que pudieran ser un problema.

4.6 Consideraciones Ambientales

Se ha oído que la lluvia, nieve, neblina y otras condiciones climáticas donde se tenga un alto porcentaje de humedad puede obstruir o afectar la Línea de Vista (LOS), introduciendo una pequeña pérdida (a veces conocida como *atenuación de lluvia o margen de atenuación*). Generalmente, estas condiciones climatológicas tienen un mínimo efecto en enlaces inalámbricos, cuando las frecuencias se encuentran por debajo de los 10GHz. Si se ha establecido una buena conexión, además de ser estable, el clima casi nunca es un problema; sin embargo, si el enlace fue pobre desde un principio, el mal clima podría degradar el desempeño, o causar pérdidas en el enlace.

4.7 Consideraciones de Potencia

Cuando se definen reglas y regulaciones con lo que respecta a la potencia de transmisión, varios métodos se usan para definir estos métodos. En primera, hay una potencia de transmisión de salida directa, la cual es la cantidad de energía de

radiofrecuencia enviada desde el amplificador de potencia del transmisor al conector de la antena. En segunda, varias limitaciones como el tipo de antena, la potencia y el umbral de recepción afectan a la ganancia de la antena que pudieran ser utilizadas.

4.7.1 EIRP

Los requerimientos de regulación para los niveles de potencia de salida son a veces evaluados en la potencia actual de transmisión, o en muchos casos en la potencia efectiva basada en los valores de transmisión y en los de la antena. Éste método es conocido como Potencia Radiada Isotrópica Efectiva (*EIRP: Effective Isotropic Radiated Power*). Este valor es un valor calculado, no sólo se usa la potencia de transmisión, sino también el valor de la ganancia isotrópica de una antena. Este valor también incluye cualquier pérdida del cable, supresores, o cualquier otro dispositivo colocado entre la antena y el conector de transmisión. Esta es la potencia efectiva que es irradiada de una antena.

Para obtener el valor EIRP, se puede tomar la potencia de transmisión (en dBm), agregar la ganancia de la antena (en dBi), y sustraer las pérdidas del cable o de los dispositivos intermedios (en dB). Por ejemplo:

Transmisión con una potencia de salida de 100mW (+20 dBm)
Antena Yaggi con una ganancia de 13.5 dBi
50 pies de cable con pérdidas de 2.2 dB
Potencia TX + Ganancia de la antena – Pérdidas del cable = EIRP
 $+20 \text{ dBm} + 13.5 \text{ dBi} - 2.2 \text{ dB} = 31.3 \text{ dBm EIRP}$

CAPÍTULO V

IMPLEMENTACIÓN DEL ENLACE INALÁMBRICO EN LA JUNTA LOCAL EJECUTIVA DEL ESTADO DE DURANGO

5.1 Descripción del problema

Como se mencionó con anterioridad, existía la necesidad de mudar al personal que labora en la Junta Local de Durango (Edificio Principal) de manera temporal a otro edificio (Edificio Secundario). Dentro de la configuración del *ruteador* de borde de la Junta Local se tienen dos *VLANs* que deben ser transportadas en el enlace:

- VLAN de la Junta Local de Durango (10.10.0.0/24)
- VLAN del Centro de Verificación y Monitoreo de Durango (10.50.100.0/24)

Ambos direccionamientos deben ser contemplados para la migración del personal al Edificio Secundario, por lo que se debe tener en cuenta para la configuración los equipos para el enlace inalámbrico.

5.2 Alternativas al Enlace Inalámbrico

Existen varias alternativas a la implementación del enlace inalámbrico. A continuación se ha analizado los precios

El precio de una renta mensual de un E1 está en \$21,421.57 sin *Puerto Extendido* (suministro del enruteador) y con servicio de Puerto Extendido \$22,004.63 (Precios actuales de Telmex). Si se contempla que la conexión entre ambos sitios

durará alrededor de un año. Se tiene un precio entre \$257,058.83 y \$264,055.58. Ver Tabla 5.1.

RENTA MENSUAL							
Velocidad de transmisión	Enlace para transporte de datos [A]	Puerto PVN [B]	Puerto Extendido Ruteador para MPLS [C]	Subtotal	IEPS (3%)	IVA (16%)	Total
2,048	\$5,321.00	\$10,560.00	\$488.00	\$18,417.00	\$552.51	\$3,035.12	\$22,004.63

Tabla 5.1 Precio de renta mensual para un enlace MPLS

Otra opción popular sería una conexión a través de un modem DSL. Esta solución a veces ofrece una conexión de descarga rápida, pero es más lenta para velocidades de carga.

El uso de microondas es una solución para algunos sitios donde la distancia es cercana (entre 1 y 25 kilometros de distancia) y si el recurso monetario no es problema. Se requiere un licenciamiento especial para el uso de la frecuencia de operación. El costo de equipamiento es elevado, alrededor de \$150 mil por sitio, sin incluir costos de instalación. En caso de lluvia, neblina o nieve, el desempeño es cuestionable. Las conexiones multipunto usualmente no son posibles.

Los radioenlaces o enlaces inalámbricos se han vuelto uno de los usos más populares de las redes inalámbricas. Esto es en parte debido a la instalación y configuración de suma facilidad, pero también a la variedad de mercados emergentes donde el enlace inalámbrico puede ser colocado. Algunos de estos mercados son:

- Ambientes de campus, como hospitales, universidades y corporaciones.
- Áreas donde la geografía complicaría otras soluciones

- Instalaciones temporales de la red
- Proveedores de servicio de Internet
- Alternativas de conexiones de respaldo
- Países en desarrollo donde no hay disponibilidad de otras alternativas para su solución.

5.3 Solución del problema

Se contempló contratar un enlace dedicado adicional, pero proyectando que al menos un año estuvieran en estas condiciones, económicamente no era opción ya que como anteriormente se mencionó, la renta mensual de dicho enlace es de \$21,421.57, a un año: \$257,058.83 (sin *Puerto Extendido*).

Esta cantidad resultaba un gasto bastante adicional, por lo que se determinó la implementación de un enlace inalámbrico con dos equipos Cisco Aironet AIR-BR1310G. Uno instalado en el edificio Principal y el otro instalado en el edificio Secundario para acoplar ambas redes de la Junta Local.

5.4 Punto de Acceso/Bridge Autónomo 1310G

El punto de acceso/bridge autónomo (modelo: AIR-BR1310G Cisco), soporta un sistema de administración basado en el software Cisco IOS. Este dispositivo es un transceptor inalámbrico certificado por la Alianza Wi-Fi. El punto de acceso/bridge autónomo utiliza un solo mini-PCI que cumple con los estándares IEEE 802.11b y 802.11g que puede ser actualizado a futuras tecnologías de radio. (Figura 5.1)

El punto de acceso/*bridge* autónomo sirve como un punto de conexión entre una red alámbrica y otra inalámbrica. En el interior de grandes instalaciones, dentro de un rango de radio de un punto de acceso, los usuarios inalámbricos pueden

itinerarse (roam) a lo largo de un complejo manteniendo el acceso a la red de manera ininterrumpida.

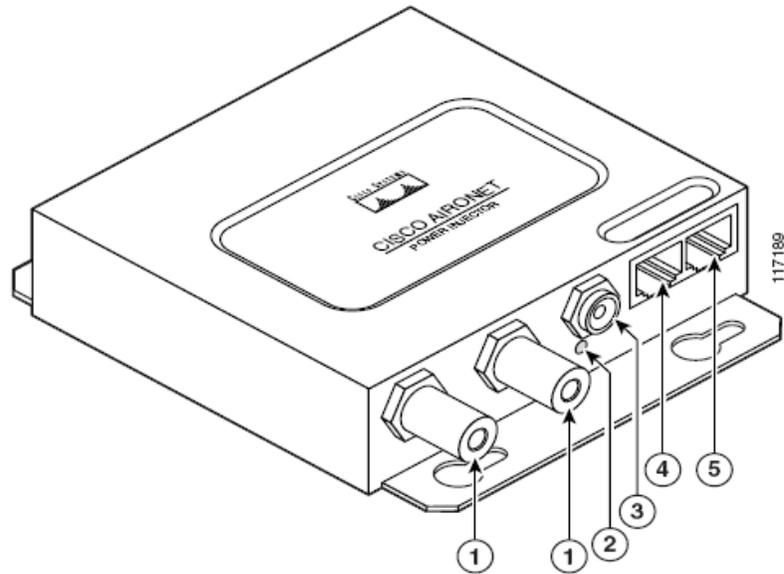


Figura 5.1 Cisco Aironet Modelo 1310G

Se puede configurar y monitorear este dispositivo utilizando la interfaz de comando de línea (*CLI*), el sistema de administración basado en navegador, o por medio del Protocolo Simple de Administración de Red (*SNMP*).

5.4.1 Inyector de Potencia

El punto de acceso/*bridge* recibe potencia en línea desde el inyector de potencia (*Power Injector*) a través de cable coaxial dual donde también se proporcionan los datos al punto de acceso/*bridge*. El inyector de potencia es una unidad externa diseñada para operar en ambientes internos, por ejemplo, dentro de un edificio o de un vehículo. El inyector de potencia también tiene una interfaz donde se conecta a la red a través de un cable Categoría 5 funcionando como repetidor. (Figura 5.2)



1	Puertos Ethernet Coaxial dual (Conectores tipo F)	4	Puerto Ethernet LAN (Conector RJ-45)
2	LED de estado de potencia	5	Puerto de Consola (Conector RJ-45)
3	Jack de potencia		

Figura 5.2 Inyector de Potencia para el bridge modelo 1310G

5.4.2 Antena integrada

Este modelo de punto de acceso/bridge tiene una antena de tipo parche integrada con una ganancia de 13 dBi. La antena está cubierta por una cúpula para protegerla de las condiciones ambientales exteriores. Dicha antena está verticalmente polarizada.

5.4.3 Puertos Ethernet

Los puertos Ethernet de cable coaxial dual del punto de acceso/bridge consisten de un par de conectores tipo F de 75 ohms. El cable coaxial dual se usa para enviar y recibir datos y para proporcionar una potencia de 48 VDC desde el inyector de potencia hasta el punto de acceso/bridge

5.5 Diseño en sitio

Como se mencionó con anterioridad, se requiere extender las VLANs de la Junta Local de Durango y del Centro de Verificación y Monitoreo hacia un inmueble remoto. Por lo que se debe considerar que el enlace inalámbrico debe ser implementado como una troncal donde se transporten estas VLANs. En la figura 5.3 se ilustra la interconexión de los elementos involucrados para la implementación del enlace inalámbrico.

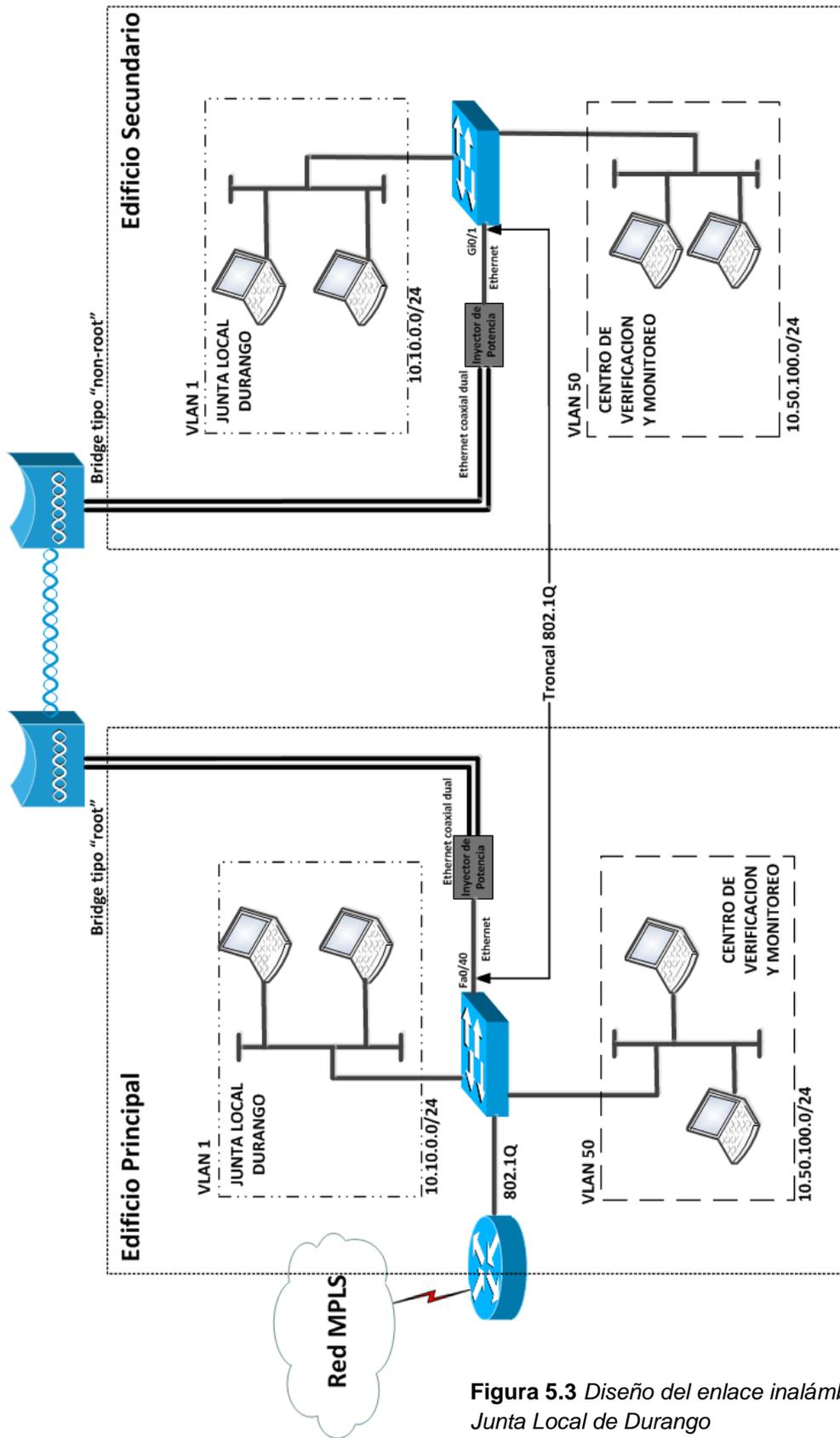


Figura 5.3 Diseño del enlace inalámbrico en la Junta Local de Durango

5.5.1 Distancia entre las antenas o “bridges”

Para el cálculo de la distancia entre los “bridges” inalámbricos se utilizó la herramienta en línea “free map tools”

<http://www.freemaptools.com/measure-distance.htm>

La cual calcula de manera aproximada la distancia entre dos puntos de cualquier lugar del globo terráqueo.

La distancia entre ambos dispositivos fue de 60 metros aproximadamente. Ver Figura 5.4.

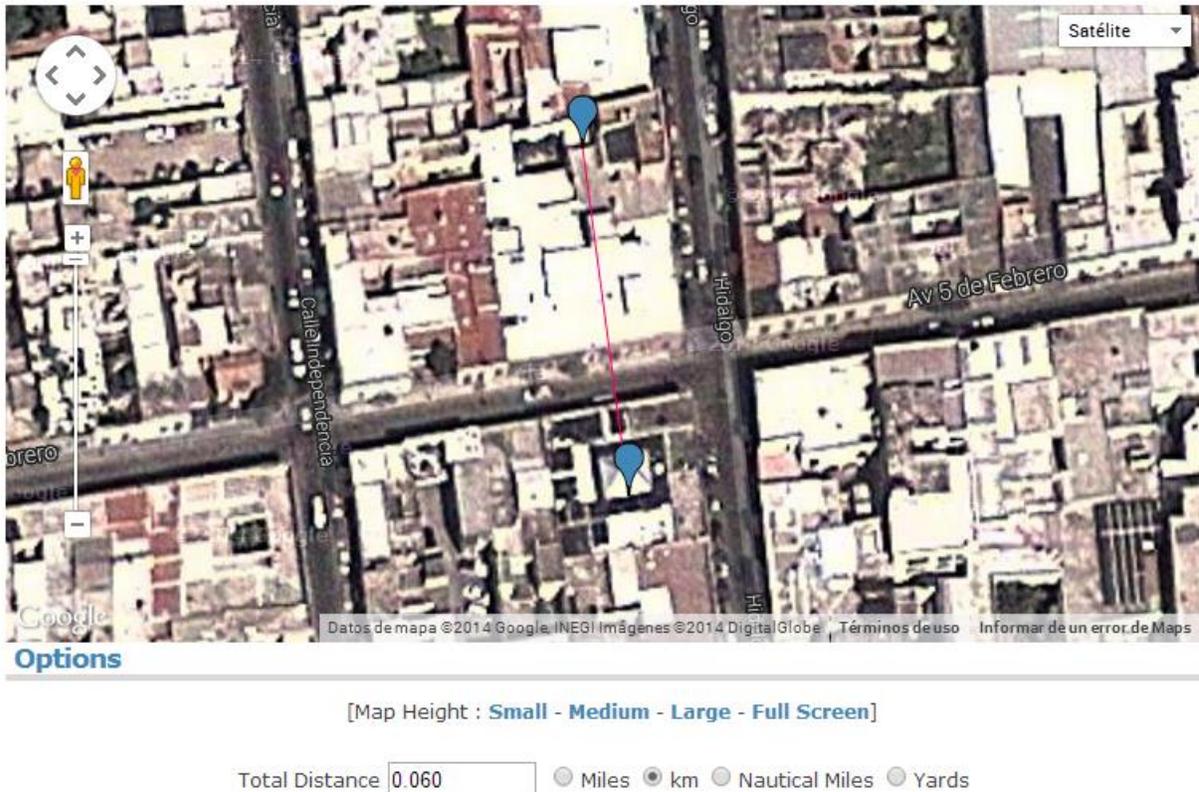


Figura 5.4 Distancia entre “bridges” por medio de free map tools

5.5.2 Utilidad para el cálculo de rango en bridges para exteriores

A través de la página en línea del fabricante se proporciona una utilidad para proporcionar los rangos máximos en distancia para los “*bridges*”.

A continuación se mencionan los puntos importantes para su uso:

- a. Elegir la frecuencia de operación (2.4 o 5 GHz)
- b. Optar el dominio regulatorio.
- c. Escoger el producto (dispositivo) en ambas locaciones (Modelo).
- d. Seleccionar la velocidad de transmisión en Mbps.
- e. Elegir la antena que se utilizaría (solo aplica para antenas no integradas del bridge) y si es en caso de tener otra antena, se deberá ingresar el factor de ganancia en dBi.
- f. Optar el nivel de potencia suministrada a la antena en ambos extremos
- g. Elegir los cables utilizados en cada extremo (para el cálculo del factor de pérdidas en acoplamientos en antenas no integradas)
- h. Escoger las condiciones regulares ambientales.
- i. Es necesaria la Línea de Vista.
- j. Tener en cuenta que estos son valores teóricos.

En la figura 5.5 se muestran los valores introducidos:

1. Cálculo para: 2.4 GHz
2. Dominio regulatorio: Estados Unidos / Canadá (Américas)
3. Dispositivo: AIR-BR1310G Antena Integrada
4. Velocidad de transmisión: 54 Mbps
5. Antena: tipo parche de 13 dBi
6. Potencia suministrada: 1 mW
7. Seleccionar cable: sin cable (es antena integrada)
8. Terreno y atmósfera (sin influencia en los resultados)

Figura 5.5 Utilidad para el cálculo del rango en bridges para exteriores

Cisco Systems
For Cisco Aironet 2.4Ghz Outdoor Links ONLY!

Regulatory Domain.....>	United States/Canada >	Site 1	Site 2
Select Device.....>	AIR-BR1310G w/Integrated antenna >	Select Device.....>	AIR-BR1310G w/Integrated antenna >
Select Datarate.....>	54 >		
Modulation Type.....>	OFDM >		
Select Antenna 1 here.....>	Integrated 13dBi Patch >	Select Antenna 2 Here.....>	Integrated 13dBi Patch >
For other Antenna- Enter Gain Here.....>	0.00	For other Antenna- Enter Gain Here.....>	0.00
Power levels permitted are based on antenna gain, modulation mode (based on datarate) and regulatory domain			
Select Power level.....>	1mW >	Select Power level.....>	1mW >
Select Cable 1.....>	other cable >	Select Cable 2.....>	other cable >
For 'OTHER' Cable		For 'OTHER' Cable	
Enter Cable Loss dB/100 ft here.....>	0.00	Enter Cable Loss dB/100 ft here.....>	0.00
Enter in Length Here.....>	0	Enter in Length Here.....>	0
Note: When using Integrated antennas, cable is not used in calculations			
Effective Isotropic Radiated Power (dBm).....>	13	Effective Isotropic Radiated Power (dBm).....>	13

Figura 5.6 Utilidad para el cálculo del rango en bridges para exteriores (resultados)

Terrain.....→	Very smooth terrain over water or flat desert; →	
Atmosphere.....→	Normal, interior continent temperate or sub-arctic →	
Max Distance (w/ min 5dB Link Margin).....→	0.22 Miles	0.36 Kilometers
Earth Bulge at above distance.....→	3 Feet	0.9 Meters
Fresnel Zone clearance for above distance.....→	7 Feet	2.0 Meters
Required antenna height above obstructions.....→	10 Feet	2.9 Meters
Recommended Fade Margin (factor of distance).....→	5 dB	

Con los datos introducidos, se obtiene los siguientes datos calculados que se muestran en la figura 5.6:

- A. EIRP = 13 dBi
- B. Distancia máxima: 360 metros
- C. Altura para superar la curvatura de la Tierra: 90 cm
- D. Altura para superar la zona de Fresnel: 2 metros

Una vez obtenidos los valores necesarios para configurar los equipos para el enlace inalámbrico, se deberá aplicar las siguientes configuraciones. En la tabla 5.2 se muestran las características para dichos dispositivo:

Edificio	Rol de Bridge	Dirección IP	Distancia entre antenas	Potencia	Ganancia antena	EIRP	Velocidad deseada	Altura para despejar Zona de Fresnel
Principal	root	10.10.0.21	60 m	1 mW	13 dBi	13 dBm	54Mbps	1.37 m
Secundario	non-root	10.10.0.22		1 mW	13 dBi	13 dBm		

Tabla 5.2 Valores de diseño

5.6 Configuraciones

A continuación se muestran las configuraciones para los equipos involucrados:

1. Switch en sitio Principal
2. Switch en sitio Secundario
3. Bridge en sitio Principal
4. Bridge en sitio Secundario

5.6.1 Switch en sitio Principal

```
interface FastEthernet0/40
description Conexion Antena
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
end
```

5.6.2 Switch en sitio Secundario

```
interface GigabitEthernet0/1
description Conexion Antena
switchport mode trunk
switchport nonegotiate
end
```

Las configuraciones de los equipos inalámbricos se realizaron a través de una interfaz web donde se determinaron todos sus parámetros.

5.6.3 Bridge en sitio Principal

- Configuración de la Dirección IP, Mascara de red y puerta de enlace predeterminada:

The screenshot shows the Cisco Aironet 1300 Series Wireless Bridge configuration interface. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "ant-ji-dgo-rb" and the time is "21:15:51 Mon Jun 30 2014". The left sidebar contains a navigation menu with items like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, IP Address, FastEthernet, Radio0-802.11G, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Network Interfaces: IP Address" and shows the configuration for the IP Address. The "Configuration Server Protocol" is set to "Static IP". The "IP Address" is "10.10.0.21", the "IP Subnet Mask" is "255.255.255.0", and the "Default Gateway IP Address" is "10.10.0.254". There are checkboxes for "Disable DHCP Address Binding" and "Override DHCP Default Gateway".

➤ Rol en el enlace inalámbrico (*Root Bridge*)

The screenshot displays the configuration page for the Radio0-802.11G interface. The top navigation bar includes 'RADIO0-802.11G STATUS', 'DETAILED STATUS', 'SETTINGS', and 'CARRIER BUSY TEST'. The hostname is 'ant-ji-dgo-rb' and the date is '21:20:55 Mon Jun 30 2014'. The 'Role in Radio Network' section is expanded, showing radio roles such as Access Point, Repeater, and Root Bridge. The 'Root Bridge' option is selected.

➤ Determinación de la potencia de la señal y su canal

The configuration page shows power and channel settings. The 'CCK Transmitter Power (mW)' is set to 1 mW. The 'OFDM Transmitter Power (mW)' is set to 1 mW. The 'Client Power Local' is set to Disable. The 'Limit Client Power (mW)' is set to 1 mW. The 'Default Radio Channel' is set to Channel 8 - 2447 MHz. The 'Least Congested Channel Search' dropdown menu is open, showing a list of channels from 1 to 11.

- Distancia del enlace, se deberá colocar 1 km ya que el enlace no es mayor a esto.

Concatenation: Enable Disable

Max Length of Concatenation: (1600-4000)

Distance (Km): (0-99)

Reliable Multicast to WGB: Disable Enable

Public Secure Packet Forwarding: [PSPF must be set per VLAN. See VLAN page](#)

- Se configura un servidor tipo RADIUS para implementar una autenticación EAP en el enlace inalámbrico, en este caso el servidor se coloca en el mismo root-bridge inalámbrico, y se coloca una “*shared secret*” o contraseña.

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

RADIUS ▾

< NEW >
10.10.0.21

Delete

Server: (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): (0-65536)

Accounting Port (optional): (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: <input type="text" value="10.10.0.21"/>	Priority 1: <input type="text" value="< NONE >"/>	Priority 1: <input type="text" value="< NONE >"/>

- Se determinan las VLANs que el sitio contiene, la VLAN 1 será la VLAN nativa de la troncal

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 1

Assigned VLANs

Current VLAN List

Create VLAN

Define SSIDs

< NEW >
VLAN 1
VLAN 50

Delete

VLAN ID: 1 (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

STP: Enable Disable

- Asimismo, se configura la VLAN 50, en este caso no es nativa.

Current Native VLAN: VLAN 1

Assigned VLANs

Current VLAN List

Create VLAN

Define SSIDs

< NEW >
VLAN 1
VLAN 50

Delete

VLAN ID: 50 (1-4094)

VLAN Name (optional):

Native VLAN

Enable Public Secure Packet Forwarding

STP: Enable Disable

Para ambos casos no es necesario activar STP (*Spanning Tree Protocol*) ya que no existe una redundancia en el enlace inalámbrico.

- Administrador de encriptación: La encriptación WEP será obligatoria en la VLAN 1, y como llave de encriptación se colocara una cadena de 26 caracteres hexadecimales. Esta misma cadena deberá ser configurada en el otro equipo inalámbrico.

The screenshot shows the configuration page for the Cisco Aironet 1300 Series Wireless Bridge. The browser address bar shows the URL: https://10.10.0.21/ap_sec_ap-key-security.shtml. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "ant-ji-dgo-rb" and the time is "21:31:07 Mon Jun 30 2014".

The left sidebar contains a navigation menu with the following items: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (highlighted), Admin Access, Encryption Manager (highlighted), SSID Manager, Server Manager, AP Authentication, Intrusion Detection, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.

The main content area is titled "Security: Encryption Manager". It shows the "Set Encryption Mode and Keys for VLAN:" section with a dropdown menu set to "1" and a "Define VLANs" link. Below this is the "Encryption Modes" section, which has three radio buttons: "None", "WEP Encryption" (selected), and "Cipher". The "WEP Encryption" option has a "Mandatory" dropdown. Underneath, there are two checkboxes for "Cisco Compliant TKIP Features": "Enable Message Integrity Check (MIC)" and "Enable Per Packet Keying (PPK)". The "Cipher" option has a dropdown menu set to "WEP 128 bit".

The "Encryption Keys" section is partially visible at the bottom, showing a table with columns: "Transmit Key", "Encryption Key (Hexadecimal)", and "Key Size". The "Encryption Key 1:" row shows a radio button selected for "Transmit Key", a text input field for the hexadecimal key, and a dropdown menu set to "128 bit".

- De igual forma para la VLAN 50 se configuran los mismos parámetros de encriptación WEP con la misma cadena.

The screenshot shows the configuration page for WEP encryption on a Cisco device. The left sidebar contains a navigation menu with items like HOME, EXPRESS SET-UP, SECURITY, and SERVICES. The main content area is titled "Security: Encryption Manager" and shows the configuration for VLAN 50. Under "Encryption Modes", "WEP Encryption" is selected with "Mandatory" as the mode. Under "Encryption Keys", "Transmit Key" is selected, and "Encryption Key 1" is set to a hexadecimal string. The key size is set to 128 bit.

Hostname ant-ji-dgo-rb 21:34:17 Mon Jun 30 2014

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 50 [Define VLANs](#)

Encryption Modes

- None
- WEP Encryption Mandatory
- Cipher WEP 128 bit

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC) Enable Per Packet Keying (PPK)

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	128 bit

- Se configura un SSID para identificación del enlace, además se colocará como una red EAP el tipo de autenticación que deberá contar el enlace.

HOME Hostname ant-jl-dgo-rb 21:36:14 Mon Jun 30 2014

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

AP Authentication

Intrusion Detection

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
JL-DGO-LINK

SSID: JL-DGO-LINK

VLAN: < NONE > [Define VLANs](#)

Backup 1:

Backup 2:

Backup 3:

Interface: Radio0-802.11G

Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

Open Authentication: < NO ADDITION >

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID: JL-DGO-LINK

Multiple BSSID

Set Infrastructure SSID: JL-DGO-LINK Force Infrastructure Devices to associate only to this SSID

Apply Cancel

- Administrador de Servidor RADIUS: Se activan o desactivan que protocolo será necesario para la autenticación, en este caso solo es LEAP.

The screenshot shows the configuration page for the Local RADIUS Server. The left sidebar contains navigation options like HOME, EXPRESS SET-UP, SECURITY, and SERVICES. The main content area is titled 'Security: Local RADIUS Server - General Set-Up' and includes sections for 'Local Radius Server Authentication Settings' and 'Network Access Servers (AAA Clients)'. In the authentication settings, 'LEAP' is selected. Under network access servers, one server is listed with IP 10.10.0.21 and a shared secret.

- Se crea un usuario en el servidor RADIUS para la autenticación remota del otro dispositivo inalámbrico.

The screenshot shows the 'Individual Users' configuration page. It features a 'Current Users' list with 'user_omg' selected. To the right, there are input fields for 'Username' (filled with 'user_omg'), 'Password' (masked with dots), 'Confirm Password', and 'Group Name' (set to '< NONE >'). There are radio buttons for 'Text' and 'NT Hash' password types, and a checkbox for 'MAC Authentication Only'. 'Apply' and 'Cancel' buttons are at the bottom right.

5.6.4 Bridge en sitio Secundario

- Configuración de la Dirección IP, Mascara de red y puerta de enlace predeterminada:

The screenshot shows the configuration page for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "ant-jl-dgo-nrb" and the time is "21:15:32 Mon Jun 30 2014". The "Express Set-Up" section is active, showing the following configuration:

Host Name:	ant-jl-dgo-nrb
MAC Address:	5057.a81b.ccf8
Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address:	10.10.0.22
IP Subnet Mask:	255.255.255.0
Default Gateway:	10.10.0.254

- Se determinan las VLANs que el sitio secundario contiene, la vlan 1 será la VLAN nativa de la troncal.

The screenshot shows the "Services: VLAN" configuration page. The "Global VLAN Properties" section shows "Current Native VLAN: VLAN 1". The "Assigned VLANs" section shows a "Current VLAN List" with "VLAN 1" selected. The "Create VLAN" section shows "VLAN ID: 1" and "VLAN Name (optional):". The "Native VLAN" checkbox is checked, and the "STP" radio buttons are set to "Disable".

- Se configura la VLAN 50, en este caso no es nativa.

Current Native VLAN: VLAN 1

Assigned VLANs

Current VLAN List

- < NEW >
- VLAN 1
- VLAN 50

Delete

Create VLAN

VLAN ID: 50 (1-4094)

VLAN Name (optional): _____

Native VLAN

Enable Public Secure Packet Forwarding

STP: Enable Disable

- Como en el equipo anterior se configura un SSID para identificación del enlace, y se colocará como una red EAP el tipo de autenticación que deberá contar el enlace.

Homepage ant-jl-dgo-nrb 21:53:26 Mon Jun 30 2014

Security: Global SSID Manager

SSID Properties

Current SSID List

- < NEW >
- JL-DGO-LINK

Delete

SSID: JL-DGO-LINK

VLAN: 1 Define VLANs

Backup 1: _____

Backup 2: _____

Backup 3: _____

Interface: Radio0-802.11G

Client Authentication Settings

Methods Accepted:

- Open Authentication: < NO ADDITION >
- Shared Authentication: < NO ADDITION >
- Network EAP: < NO ADDITION >

- En este mismo apartado se colocará el usuario y contraseña del usuario RADIUS que se configuró en el equipo root-bridge.

EAP Client (optional):

Username: Password:

Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

- Se determina el rol del dispositivo inalámbrico (non-root bridge)

<ul style="list-style-type: none"> HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION + NETWORK INTERFACES IP Address FastEthernet Radio0-802.11G SECURITY + SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + 	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc;"> RADIO0-802.11G STATUS DETAILED STATUS SETTINGS CARRIER BUSY TEST </div> <p>Hostname ant-jl-dgo-nrb 21:58:56 M</p> <hr/> <p>Network Interfaces: Radio0-802.11G Settings</p> <p>Enable Radio: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Current Status (Software/Hardware): Enabled ↑ Up ↑</p> <p>Role in Radio Network:</p> <ul style="list-style-type: none"> <input type="radio"/> Access Point <input type="radio"/> Access Point (Fallback to Radio Shutdown) <input type="radio"/> Access Point (Fallback to Repeater) <input type="radio"/> Repeater <input type="radio"/> Root Bridge <input checked="" type="radio"/> Non-Root Bridge <input type="radio"/> Root Bridge with Wireless Clients <input type="radio"/> Non-Root Bridge with Wireless Clients <input type="radio"/> Install Automatic <input type="radio"/> Install Root Bridge <input type="radio"/> Install Non-Root Bridge
---	--

- La misma potencia y el mismo canal que se colocó en el equipo del Sitio Principal, así como la misma distancia.

CCK Transmitter Power (mW): 1 5 10 20 30 50 100 Max

OFDM Transmitter Power (mW): 1 5 10 20 30 Max

[Power Translation Table \(mW/dBm\)](#)

Client Power Local: Enable Disable

Limit Client Power (mW): 1 5 10 20 30 50 100 Max

Default Radio Channel: Channel 8 - 2447 MHz ▾

Least Congested Channel Search:
(Use Only Selected Channels)

- Channel 1 - 2412 MHz ▲
- Channel 2 - 2417 MHz
- Channel 3 - 2422 MHz
- Channel 4 - 2427 MHz
- Channel 5 - 2432 MHz
- Channel 6 - 2437 MHz
- Channel 7 - 2442 MHz
- Channel 8 - 2447 MHz
- Channel 9 - 2452 MHz
- Channel 10 - 2457 MHz
- Channel 11 - 2462 MHz ▼

Concatenation: Enable Disable

Max Length of Concatenation: DISABLED (1600-4000)

Distance (Km): 1 (0-99)

Reliable Multicast to WGB: Disable Enable

Public Secure Packet Forwarding: [PSPF must be set per VLAN. See VLAN page](#)

- En este administrador se determina una encriptación WEP, y la llave de encriptación deberá ser la cadena de 26 caracteres hexadecimales que en el equipo root-bridge se configuró, tanto para la VLAN 1 como para la VLAN 50.

HOME Hostname ant-ji-dgo-nrb 22:03:08 Mon Jun 30 2014

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

AP Authentication

Intrusion Detection

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 1 [Define VLANs](#)

Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)

Enable Per Packet Keying (PPK)

Cipher WEP 128 bit

Encryption Keys

Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1: <input checked="" type="radio"/>	128 bit

HOME Hostname ant-ji-dgo-nrb 22:03:08 Mon Jun 30 2014

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

AP Authentication

Intrusion Detection

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 50 [Define VLANs](#)

Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)

Enable Per Packet Keying (PPK)

Cipher WEP 128 bit

Encryption Keys

Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1: <input checked="" type="radio"/>	128 bit

5.7 Pruebas y Resultados

El enlace se estableció con éxito a partir de estas configuraciones. Se realizó una prueba de *ping* por cada punta hacia el otro extremo respectivo del enlace.

```
ant-jl-dgo-nrb#ping 10.10.0.21 repeat 100
```

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to 10.10.0.21, timeout is 2 seconds:

!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/3 ms

```
ant-jl-dgo-rb#ping 10.10.0.22 repeat 100
```

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to 10.10.0.22, timeout is 2 seconds:

!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms

No se registraron pérdidas de paquetes ICMP para esta prueba.

Posteriormente se censaron algunos parámetros para encontrar la estabilidad en el enlace. En la tabla 5.3 se contemplan las pruebas realizadas en el enlace inalámbrico y los resultados en cuanto a velocidad de transmisión en Mbps, Indicador de Fuerza de la Señal Recibida (*RSSI*) y Relación Señal a Ruido (*SNR*), con los equipos ya instalados en sitio.

Potencia [mW]	Velocidad de Transmisión [Mbps]	RSSI [dbm]	SNR [dbm]
1	18	-77	15
1	12	-76	14
1	24	-76	15
1	9	-76	12
5	36	-73	18
5	24	-72	18
5	48	-72	17
10	48	-71	20
10	54	-70	21

Tabla 5.3 Resultados de pruebas

Existió una mayor estabilidad en el enlace cuando se aplicaba una potencia de 10mW, se mantuvo el enlace a 48 y 54 Mbps con el RSSI y SNR aceptables, esto debido a la gran cantidad de cables, antenas, rejillas, entre otros objetos, que se encuentran en los techos de los inmuebles contiguos y provocan ciertas degradaciones en la señal, por los efectos de absorción, reflexión y multirayectorias, a pesar de que se mantiene una línea de vista y una zona de Fresnel despejada.

CONCLUSIONES

El enlace inalámbrico entre los dos inmuebles se estableció con una potencia de 10 mW debido a la estabilidad en velocidad y RSSI que se obtuvieron. A pesar de existir cercanía, línea de vista, zona de Fresnel sin obstáculos, se tuvo que aumentar la potencia en los dispositivos de la calculada previamente, esto a causa de los diferentes fenómenos de absorción, multitrayectoria, dispersión, entre otros, que provocan una atenuación en la señal irradiada. La cantidad de antenas, enrejados, cables, postes que se encuentran en los techos de las viviendas en el sitio contribuyen a que estos fenómenos se acentúen en la transmisión de las señales inalámbricas por lo que fue necesario inyectar mayor potencia y mantener una velocidad de transmisión alta estable.

Un punto de mejora en el enlace inalámbrico muy evidente es la seguridad implementada: *WEP*. A pesar de aumentar su seguridad con el protocolo *801.1X* a través de un servidor *RADIUS* instalado de manera local en un *bridge* y una autenticación *PEAP*, la encriptación de *WEP (RC4)* debe ser reemplazada con una más robusta como *TKIP* o *AES*, protocolos de encriptación para *WPA* y *WPA2* respectivamente. Recordemos que se está utilizando una encriptación de 128 bits (la cadena ingresada era de 26 números hexadecimales, 4 bits que tiene cada número, esto da un total de 104 bits, nuestra *clave secreta*, más 24 bits que representa el vector de inicialización *IV*).

Otro punto de mejora para este proyecto es la implementación de Calidad de Servicio (QoS) sobre el enlace inalámbrico. Esto hace que las aplicaciones corran mejor y la utilización del ancho de banda sea más efectiva. Al usar las cualidades de QoS, se puede priorizar los tipos de tráfico en lugar de mandar paquetes de la forma *FIFO* (First In, First Out), el paquete que llegue primero, es el primero que va a

mandarse. Los datos sensibles al retardo son voz y video, por lo que sería conveniente colocar éstos datos como prioritarios. El protocolo inalámbrico encargado de realizar esta labor es *802.11e*.

Actualmente ya se ha comercializado la tecnología *802.11n*, por lo que ya sería una realidad desplazar *802.11g* con la que se implementó el enlace inalámbrico. A pesar de que tiene tasas de transmisión más altas, se tendrían que reemplazar los equipos actuales, eso implicaría más tiempo e inversión. Las tasas de transmisión con la que se opera son suficientes por el momento para este enlace.

Finalmente, y con el objetivo de disminuir la potencia irradiada en las antenas, es necesario despejar de objetos metálicos la zona donde operan las antenas para mantener lo más estable posible el enlace implementado.

REFERENCIAS:

Bibliográficas

- Ahmad, A. (2005) *Wireless Mobile Data Networks*. Estados Unidos: Wiley
- Alexander B. (2005) *802.11 Wireless Network Site Surveying and Installation*. Estados Unidos: Cisco Press
- Anderson R. (2008) *Security Engineering*. Estados Unidos: Wiley
- Black, U. (2010) *Redes*. España: Anaya.
- Cisco Systems. (2003) *Aironet Wireless LAN Fundamentals Volume 1*. Estados Unidos: Cisco Press.
- Cisco Systems. (2013) *Interconnecting Cisco Networking Devices Part 1*. Estados Unidos: Cisco Press.
- Cisco Systems. (2013) *Interconnecting Cisco Networking Devices Part 2*. Estados Unidos: Cisco Press.
- Gast. M. (2006) *Redes Wireless 802.11*. España: Anaya.
- Geier, J. (2005) *Wireless Networks first-step*. Estados Unidos: Cisco Press.
- Olifer N. / Olifer V (2009). *Redes de Computadoras: principios, tecnología y protocolos para el diseño de redes*. México: McGraw Hill /Interamericana de México
- Roldan, D. (2005) *Comunicaciones Inalámbricas*. México: Alfaomega Ra-Ma.
- Roshan P. / Leary J. (2004) *802.11 Wireless LAN Fundamentals* Estados Unidos: Cisco Press.

Cibergráficas

- http://normateca.ife.org.mx/internet/files_disp/18/78/CREACIONUNICOM.pdf
- https://normateca.ife.org.mx/normateca/files_disp/52/239/MOG_JGE186-2013_normaife%20version%20final.pdf (Manual de Organización General, Instituto Federal Electoral, 2013, NormalFE)

- http://www.ine.mx/portal/site/ifev2/Que_es/
- <http://elprojects.blogspot.mx/2011/10/digital-modulation.html>
- http://www.ecured.cu/index.php/Modulaci%C3%B3n_QAM
- http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps458/prod_technical_reference09186a00800a912a.xls
- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/product_data_sheet09186a00802252e1.pdf
- <http://www.youblisher.com/p/163794-Zonas-de-Fresnel-en-redes-inalambricas/>
- <http://www.freemaptools.com/measure-distance.htm>
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1300/installation/guide/1300hig6.pdf
- http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_5-1/ieee.html
- <http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html>
- <https://www.cisco.com/web/ES/publicaciones/04-Cisco-aironet-swan.pdf>
- http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
- http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/08_es_antenas-y-cables_presentacion_v02.pdf
- <http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/gsm>
- <http://tools.ietf.org/html/rfc2616>
- <http://www.ecured.cu/index.php/Hertz>
- <http://www.itu.int/es/about/Pages/default.aspx>
- <http://www.gnu.org/software/radius/>
- <https://www.ietf.org/rfc/rfc793.txt>
- <http://www.alegsa.com.ar/Dic/tkip.php>

ANEXO

Instalación física de los dispositivos inalámbricos

➤ *Antena tipo Root*





➤ **Antena tipo Non-Root**





GLOSARIO

802.11

Estándar de la IEEE (Institute of Electrical and Electronics Engineers), introducido en 1997 para regir las redes locales inalámbricas. A lo largo de varios años ha sufrido varias modificaciones en sub-estándares donde se especifican las especificaciones para la utilización de las redes inalámbricas (802.11a, 802.11b, etcétera). La versión inicial especificaba dos velocidades de transmisión: 1 y 2 Mbps transmitidas en señales infrarrojas.

802.1Q

Protocolo que permite el mecanismo para compartir múltiples redes de forma transparente en el mismo medio físico. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de VLANs.

Access Point, Punto de Acceso o Equipo de Acceso Inalámbrico

Es el dispositivo que comúnmente interconecta la zona cableada de la red con la no cableada o región inalámbrica por donde los clientes, también inalámbricos, acceden a la red.

AES

Advanced Encryption Standard. Algoritmo de encriptación para el Sistema WPA2 adoptado como estándar de cifrado por el gobierno de los Estados Unidos como necesidad de mejorar la encriptación del sistema WPA.

Aironet

Familia de puntos de acceso inalámbrico de la marca Cisco Systems ©. Inicialmente fue una reconocida empresa que posteriormente fue incorporada a Cisco en febrero de 2000 dedicada al mercado de la infraestructura inalámbrica.

Antena

Dispositivo físico compuesto generalmente por un conductor metálico para enviar y recibir ondas electromagnéticas hacia el espacio libre. Las antenas transmisoras transforman la energía eléctrica recibida a ondas electromagnéticas. Las antenas receptoras realizan la función inversa.

Beamwidth

Angulo subtendido por la radiación emitida entre los puntos en que la potencia disminuye a la mitad (3 dB)

Bluetooth

Estándar de comunicaciones que utiliza ondas de radio, a corta distancia, en la banda de los 2.4GHz, que permite la comunicación entre dos dispositivos y que no requiere licencia.

CCK

Complementary Code Keying. *Cifrado de Código Complementario.* Un estándar de modulación que codifica los bits como desfases se puede seleccionar uno de cada dos desfases para codificar un solo bit.

CLI

Command Line Interface. Es el medio de interacción con un sistema operativo donde el usuario ejecuta comandos al programa en un modo de líneas sucesivas de texto. En el caso de Cisco Systems ©, define su propio conjunto de reglas y sintaxis para conformar comandos específicos.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidence. Acceso múltiple con escucha de portadora y evitación de colisión. Un método CSMA que intenta evitar un

acceso simultáneo (colisiones) aplazando el acceso al medio. 802.11 y LocalTalk de AppleTalk son dos protocolos que utilizan CSMA/CA.

dBm

Unidad de medida de potencia expresada en decibeles y relativo a un miliWatt.

DHCP

Dynamic Host Configuration Protocol. *Protocolo de Configuración de Host Dinámico.* Protocolo de red de tipo *cliente/servidor* que permite a los clientes de una red IP obtener sus parámetros de configuración de manera automática por lo que las direcciones pueden ser reutilizadas cuando los clientes ya no las requieran.

DSL

Digital Subscriber Line. *Línea Digital de Abonado.* Tecnología que proporciona acceso a Internet mediante la transmisión de datos a través de la infraestructura de la red telefónica local a distancias limitadas. Existen cuatro tipos: ADSL, HDSL, SDSL y VDSL.

E1

Formato de transmisión digital inicialmente para interconectar troncales entre centrales telefónicas y posteriormente fue teniendo otras aplicaciones. Consiste en 32 *time slots* de 64kbps cada una, lo cual conforma un total de 30 líneas telefónicas normales y 2 canales de señalización. Su ancho de banda total es de 2048 kbps.

EAP

Extensible Authentication Protocol. *Protocolo de Autenticación Extensible.* Protocolo de autenticación de estructura utilizado por 802.11X para proporcionar autenticación de red. La propia autenticación se delega a subprotocolos denominados métodos. Los métodos modernos de EAP proporcionan un mecanismo seguro de autenticación negociando un PMK entre el *supplicant* y el *servidor de*

autenticación. En esta situación, el PMK puede ser usado para abrir una sesión inalámbrica cifrada TKIP o AES.

EDGE

Enhanced Data Rates for Global Evolution. Tasa de Datos Mejorada para la Evolución Mundial de GSM. Técnica mejorada de modulación de radio para GSM y TDMA (ANSI-136) que amplía los intervalos de tiempo (*timeslots*) de radio hasta 48 kbps. Cuando se combina con GPRS, proporciona un ancho de banda máximo de 384 kbps por abonado.

Ethernet

Red de área local con topologías de bus y velocidades que van desde 10Mbps a 10Gbps sobre cable coaxial, de pares o fibra óptica, que sigue la norma IEEE 802.3 y utiliza el protocolo CSMA/CD.

FIFO

First In, First Out. Concepto utilizado en estructura de datos para implementar colas. En comunicaciones es común el uso de este concepto donde los primeros datos que ingresan en un extremo de un equipo (interfaz de entrada), serán los primeros que serán mandados por otro extremo (interfaz de salida).

FTP

File Transfer Protocol. Protocolo de aplicación, parte de la pila de protocolos TCP/IP, utilizado para transferir archivos entre nodos de red. FTP está definido en el RFC 959.

GSM

Global System for Mobile communications / Groupe Spécial Mobile. Estándar en telecomunicaciones móviles. A pesar de ser diseñado originalmente para operar en la banda de 900MHz, pronto adoptó la banda de 1800MHz. La introducción en Norte America requirió contemplar adaptarla a las bandas 800 y 1900 MHz.

GPRS

General Packet Radio Service. Servicio General de Radio por Paquetes, una mejora sobre GSM que permite la transmisión de paquetes de datos a una velocidad de hasta 115 kbps.

HTTP

Hyper Text Transfer Protocol. Protocolo de aplicación utilizado en las transacciones de la WWW.

Hotspot

Son los lugares que ofrecen acceso Wi-Fi, y que pueden ser aprovechados por dispositivos móviles tales como laptops, PDAs, entre otros.

Hz

Hertz. Unidad de medida de frecuencia del Sistema Internacional de Unidades, su símbolo es Hz, debe su nombre al alemán Heinrich Rudolf Hertz. Un Hertz representa un ciclo por cada segundo, entendiendo ciclo como la repetición de un suceso. Por ejemplo, un hertz se aplica en física a la medición de la cantidad de veces por un segundo que se repite una onda (ya sea sonora o electromagnética), magnitud denominada frecuencia y que es, en este sentido, la inversa del período. Un hertz es la frecuencia de una partícula en un período de un segundo.

IOS

Internetwork Operating System. Software utilizado en la gran mayoría de los equipos de comunicaciones de Cisco Systems®, que engloba un paquete de funciones integrándose estrechamente con un sistema operativo multitarea.

IEEE

Institute of Electrical and Electronic Engineers. Organismo americano, fundado en 1884, responsable de determinados estándares en el campo de las

telecomunicaciones; los más importantes son la definición de los niveles 1 y 2 para LAN.

IP

Internet Protocol. Protocolo en la capa de red que contiene información de dirección y control para el encaminamiento de los paquetes a través de la red. Suele asociarse con TCP y está documentado en RFC 791, RFC 1009 y MIL STD 1777.

ISM

Industrial. Scientific and Medical. Bandas de frecuencias internacionalmente reservadas para uso no comercial de radiofrecuencia electromagnética. Está abierto a todo el mundo sin necesidad de un licenciamiento, pero deben cumplir las regulaciones para limitar los niveles de potencia transmitida.

ITU

International Telecommunications Union. Organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación. Atribuye el espectro radioeléctrico y las órbitas de satélite a escala mundial además de elaborar normas técnicas que garantizan la interconexión continua de las redes y las tecnologías.

Jitter

Fluctuación del retardo que sufre la información al atravesar la red.

Kerberos

Protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.

LAN

Local Area Network. Redes de altas velocidades, tasa de errores bajos que cubre áreas geográficas relativamente pequeñas. Las LANs interconectan estaciones de trabajo, periféricos, terminales, y otros dispositivos de un área limitada permitiendo que se compartan recursos entre sí. Los estándares de la LAN especifican el cableado y la señalización en las capas física y de enlace del modelo OSI. Ethernet, FDDI, y Token Ring son ampliamente utilizados en las tecnologías LAN.

MPLS

Multi-Protocol Label Switching. Estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. El protocolo MPLS es el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP y pretende ser el sustituto de la conocida arquitectura IP sobre ATM.

P2P

Peer-to-peer. Red de computadoras en la que todos o algunos clientes actúan como clientes y/o servidores frente a los demás. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Ping

Packet Internet Groper. Herramienta de administración y diagnóstico de redes más conocida. Su función es mandar paquetes para verificar si un equipo remoto está respondiendo y, por ende, es accesible a través de la red.

POP

Post Office Protocol. Protocolo de aplicación utilizado para obtener los mensajes de correo electrónico almacenados en un servidor. POP no necesita una conexión permanente a internet, puesto que es en el momento de la conexión cuando solicita al servidor el envío de la correspondencia almacenada en el servidor para dicho usuario.

QoS

Quality of Service. *Calidad de Servicio.* Prestaciones exigidas a la red en función de parámetros tales como el retardo, el *jitter*, la tasa de pérdidas, etc. Se emplea para la clasificación del tráfico en diferentes tipos.

RADIUS

Remote Authentication Dial-In User Service. *Servicio de Autenticación de Conexión Telefónica Remota Autenticada.* Protocolo utilizado para autenticar usuarios de conexión telefónica que se ha utilizado más ampliamente debido a la autenticación 802.1X. Es el tipo más común de servidor de autenticación utilizado en sistemas 802.1X.

RJ-45

Registered-Jack 45. Interfaz física comúnmente usada para conectar redes de cableado estructurado. Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

Roaming o itinerancia

Concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra.

Router, ruteador o enrutador.

Dispositivo a nivel de capa de red que utiliza una o más métricas para determinar la trayectoria óptima en la red y establece por donde mandará su tráfico.

RSSI

Received Signal Strength Indicator. Escala de referencia en relación a 1 mW para medir el nivel de potencia de las señales recibidas por un dispositivo inalámbrico.

SMTP

Simple Mail Transfer Protocol. Protocolo de internet que proporciona servicios de correo electrónico.

Sniffer

Analizador de paquetes que captura las tramas de una red de área local.

SNMP

Simple Network Management Protocol. Protocolo de administración de la red que facilita el intercambio de información de gestión entre los dispositivos de red. Es útil para la administración de configuraciones, desempeño y seguridad.

SNR

Signal to Noise Ratio. Medida de proporción de los niveles de ruido relativos en sistemas analógicos y de la distorsión introducida por el proceso de cuantificación en sistemas digitales.

Switch

Dispositivo de interconexión de equipos que opera en la capa de enlace de datos del modelo de referencia OSI. El switch construye una tabla llamada MAC, que relaciona la dirección MAC con el puerto utilizado para conectar un nodo.

T1

Provee transmisiones de datos a velocidades de 1.544Mbps y pueden llevar tanto voz como datos. Un T1 está dividido en 24 canales de 64kbps cada uno. Esto es debido a que cada circuito de voz requiere ese ancho de banda, así cuando los T1 son divididos en canales de 64kbps, la voz y los datos pueden ser llevados sobre el mismo servicio de T1.

TCP

Transmission Control Protocol. Protocolo de capa de transporte usado por aplicaciones que requieran que se garantice su entrega. *TCP* agrega funciones necesarias para prestar un servicio que permita que la comunicación entre dos clientes o sistemas se efectúe sin errores ni pérdidas. Es un protocolo orientado a conexión, es decir, permite que dos máquinas que se están comunicando controlen el estado de la transmisión.

TKIP

Temporal Key Integrity Protocol. *Protocolo de Integridad de Llave Temporal.* En criptografía, es un protocolo de seguridad usado en *WPA* para mejorar el cifrado de datos en redes inalámbricas para corregir las deficiencias de *WEP*. La principal diferencia entre *WEP* y *TKIP*, es que *WEP* utiliza periódicamente la misma clave para cifrar los datos; en cambio *TKIP* comienza con una clave temporal de 128 bits que comparte entre los clientes y puntos de accesos. *TKIP* combina la clave temporal con la dirección *MAC* del cliente. Luego añade un valor de inicialización relativamente largo (de 16 octetos) para producir la clave final con la cual se cifrarán los datos. Tanto *WEP* como *TKIP* utilizan el *RC4* para hacer el cifrado.

WLAN

Wireless Local Area Network. Red que cubre un área equivalente a la red local, con un alcance inalámbrico de aproximadamente cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí.

WPA/WPA2

Wireless Protected Access. *WPA* fue una implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación *TKIP*. Posteriormente en junio del 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial de *WPA2*. Introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. Utiliza el algoritmo de cifrado *AES*.