# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE INGENIERÍA

**Reestructuración de las Redes**
**del Departamento de Ingeniería Biomédica**

**Reporte de actividades profesionales**

**QUE PARA OBTENER EL TÍTULO DE:**

**INGENIERO EN COMPUTACIÓN**

**P R E S E N T A :**
**Alejandro Baranda Vargas**


**Aval: M.C. María Jaquelina López Barrientos**

**2015**

# ÍNDICE

**Capítulo 1 Presentación de la Empresa ..... 1**

1.1. La Empresa ..... 2

1.2. Objetivo ..... 4

1.3. Visión ..... 4

1.4. Misión ..... 4

1.5. Valores ..... 4

1.6. Política de calidad ..... 4

1.7. Organigrama ..... 5

**Capítulo 2 Proyectos desarrollados ..... 9**

2.1. Rehabilitar el monitor espejo de UCIN Referidos de la Central de Monitoreo de la UCIN ..... 10

2.2. Cambio de direcciones IP en Monitores de Signos Vitales ..... 10

2.3. Videoteca ..... 11

2.4. Actualización de rutinas para mantenimiento preventivo ..... 11

2.5. Diseño, administración y mantenimiento del sitio web ..... 12

**Capítulo 3 Redes inalámbricas y sus seguridades ..... 13**

3.1. Fundamentos ..... 14

3.1.1. Redes de computadoras ..... 14

3.1.1.1. Clasificación de las redes de computadoras ..... 14

3.1.1.2. Topologías de red ..... 16

3.1.1.3. Modelo OSI ..... 17

3.1.1.4. Modelo TCP/IP ..... 18

3.1.2. Red inalámbrica ..... 19

3.1.3. Topología de una red inalámbrica ..... 22

3.1.4. Categorías de las redes inalámbricas ..... 24

3.1.5. Elementos de una red ..... 25

3.1.6. Aplicaciones de las Redes de Área Local Inalámbricas ..... 34

3.1.7. Requisitos de las redes inalámbricas ..... 35

3.1.8. Ventajas de las redes inalámbricas ..... 36

3.1.9. Desventajas de las redes inalámbricas ..... 37

3.1.10. Algunas vulnerabilidades de las redes inalámbricas ..... 38

3.1.10.1. Riesgos....38
3.1.11. Cifrado WEP....41
3.1.12. Cifrado WPA....42
3.1.13. Cifrado WPA2....44
3.1.14. Seguridad en las redes inalámbricas....48
3.1.15. Consejos de seguridad....48
3.1.16. Inseguridad en las redes inalámbricas....50
**Capítulo 4 Reestructuración de las redes....53**
4.1. Problemática actual....54
4.1.1. Existen intrusos en las redes del Departamento de Ingeniería Biomédica....55
4.1.2. Conflicto con las direcciones IP....56
4.1.3. Conflicto para la impresión a color....57
4.1.4. Conflicto para acceder a los ficheros del servidor desde las estaciones de trabajo....57
4.1.5. Tiempos de espera prolongados para hacer órdenes de servicio....58
4.2. Objetivo....59
4.3. Estrategia de gestión de redes....60
4.4. Desarrollo....60
4.4.1 Estrategia de solución....60
4.4.2. Implementación de la solución: Reestructuración de las redes....61
**Capítulo 5 Resultados....73**
**CONCLUSIONES DEL PROYECTO....75**
**GLOSARIO....77**
**REFERENCIAS....81**

# ÍNDICE DE IMÁGENES

Capítulo 1 Presentación de la Empresa

Imagen 1. 1 Organigrama de la Empresa a nivel Internacional .....2
Imagen 1. 2 Organigrama del Departamento de Ingeniería Biomédica .....5

Capítulo 3 Redes inalámbricas y sus seguridades

Imagen 3. 1 Cable de par trenzado conectado a un conector RJ-45.....15
Imagen 3. 2 Topologías de Red .....16
Imagen 3. 3 Comparativa entre los modelos OSI y TCP/IP .....19
Imagen 3. 4 Topología Ad-Hoc .....23
Imagen 3. 5 Topología Infraestructura .....23
Imagen 3. 6 Topología Red Mesh .....24
Imagen 3. 7 Denominación de una red a partir del área de cobertura .....24
Imagen 3. 8 Servidor .....25
Imagen 3. 9 Estaciones de trabajo.....26
Imagen 3. 10 Modem .....26
Imagen 3. 11 Repetidor.....27
Imagen 3. 12 Hub .....27
Imagen 3. 13 Switch .....28
Imagen 3. 14 Puente .....28
Imagen 3. 15 Router.....29
Imagen 3. 16 Puntos de Acceso.....30
Imagen 3. 17 Tarjetas de Red .....31
Imagen 3. 18 Antenas.....33
Imagen 3. 19 Usos fraudulentos de las redes inalámbricas.....40
Imagen 3. 20 Proceso de un EAP .....45

Capítulo 4 Reestructuración de las redes

Imagen 4. 1 Simulación del diseño de las redes en Departamento de Ingeniería Biomédica.....54
Imagen 4. 2 Simulación de las conexiones que tiene actualmente las redes .....54
Imagen 4. 3 Hosts no reconocidos “ISSMXLTHOSIXT12” y “COMPAQ-PC” .....56
Imagen 4. 4 Error de red .....56
Imagen 4. 5 Configuración DHCP Encendido .....57
Imagen 4. 6 Problema con el acceso directo .....58
Imagen 4. 7 Se muestra cómo está la configuración para la estación de trabajo asignada .....58
Imagen 4. 8 Estación de trabajo asignada e impresora conectada por USB .....59

Imagen 4. 9 Simulación de la redes sin conexión .....62
Imagen 4. 10 Simulación de la redes con conexión .....62
Imagen 4. 11 Red “H93H54Q3” .....63
Imagen 4. 12 Red “A01B03V13” .....63
Imagen 4. 13 Red “Q5QHQW89” .....64
Imagen 4. 14 “RICOH” con IP estática: 192.168.0.3 .....65
Imagen 4. 15 “KONICA” con IP estática: 192.168.0.4 .....65
Imagen 4. 16 “ETIQUETAS” con IP estática: 192.168.0.5 .....65
Imagen 4. 17 Ciclo de vida de una política de seguridad .....67
Imagen 4. 18 Clientes DHCP para la red “Q5QHQW89” .....71
Imagen 4. 19 Clientes de las redes “A01B03V13” y “H93H54Q3” .....72

# ÍNDICE DE TABLAS

Capítulo 3 Redes inalámbricas y sus seguridades

Tabla 3. 1Tipos de red con sus rangos y anchos de banda .....16

Capítulo 4 Reestructuración de las redes

Tabla 4. 1 Tabla de direcciones IP .....57
Tabla 4. 2 Criterios estratégicos para implementar una red de comunicación de datos .....60
Tabla 4. 3 Políticas para las redes del Departamento de Ingeniería Biomédica .....68

Capítulo 5 Resultados

Tabla 5. 1 Direcciones IP de la red “Q5QHQW89”.....74

# INTRODUCCIÓN

El presente documento es un informe que recoge la experiencia de mi primer empleo como egresado de la Facultad de Ingeniería de la carrera Ingeniería en Computación en el módulo terminal de Ingeniería Biomédica, estudié en la generación 2007-2011, culminé mis estudios profesionales en el mes de diciembre de 2011 con un promedio de 8.12, realicé mi servicio social en el Instituto de la Judicatura Federal en el periodo de marzo a septiembre de 2012. En febrero del 2013 se me ofreció la oportunidad de realizar prácticas profesionales en el área de Ingeniería Biomédica para la empresa Eductrade como inversionista proveedor del Hospital Regional de Alta Especialidad de Ixtapaluca por el periodo de marzo a septiembre de 2013, a partir del 01 de octubre de 2013 ingreso a las actividades laborales ya que obtengo mi primer contrato laboral. En este informe se reportan mis actividades profesionales, durante el primer año y medio que estoy laborando, en el cual desempeño el puesto de Ingeniero en Computación en el módulo de Ingeniería Biomédica.

En el primer capítulo se encuentra la presentación de Eductrade, en México Eductrade tiene el Departamento de Ingeniería Biomédica dedicada a facilitar la prestación y continuidad de los servicios médicos, reducir fallas, prolongar la vida útil y disminuir los costos de operación (Inspecciones, mantenimiento preventivo, reparaciones, capacitación, asistencias) lo anterior debe siempre realizarse bajo una estructura técnica bien establecida que incluye:

- Personal capacitado
- Herramientas especializadas
- Equipo de medición certificado (que garantice el correcto funcionamiento)

Garantizando que la calidad en los servicios de mantenimiento preventivo y correctivo coadyuve a la conservación y alargamiento de la vida útil del equipamiento médico, que será reflejada en un menor costo, continuidad en la operación y calidad en la atención para reintegrar al paciente a su vida cotidiana.

En el segundo capítulo, se muestra un compendio de los proyectos en los que he participado. Los proyectos fueron realizados con herramientas que tiene Eductrade, para áreas diversas. El formato en este capítulo para la redacción de los proyectos y actividades, contiene: una descripción de éstos, la propuesta solución, las actividades desarrolladas, resultados obtenidos y la inclusión del tiempo de su realización.

A lo largo del tercer capítulo se proporciona una breve descripción de lo que consisten las redes y en particular las redes inalámbricas explicando sus fundamentos, topologías, elementos, categorías, aplicaciones, ventajas, desventajas vulnerabilidades, tipos de encriptación, seguridad, consejos de seguridad.

Dentro de los diversos proyectos que se han llevado a cabo con mi participación, se eligió uno en específico para tomarlo como proyecto principal de este reporte. Tal proyecto es la reestructuración de la Red. Este tema se describe en el cuarto capítulo, presentando:

- Problemática actual
- Objetivo
- Antecedentes
- Estrategia de gestión de redes inalámbricas
- Metodología utilizada
- Desarrollo
- Políticas de redes inalámbricas

Además de capturas de pantalla para un mejor entendimiento.

Finalmente en el quinto capítulo se dan a conocer los resultados obtenidos en el proyecto, los beneficios de su creación y las tareas que se facilitaron para los usuarios.

En los apartados finales se menciona de igual forma, las conclusiones de la experiencia profesional obtenida durante mi desempeño laboral en Eductrade.

# Capítulo 1
# Presentación de la Empresa

La empresa Eductrade fue constituida en el año 1976 con el objetivo de exportar las soluciones y programas educativos, que ya se aplicaban en el sistema español, a los países latinoamericanos que conocían y seguían a distancia las experiencias educativas que se desarrollaban en España.

## 1.1. La Empresa

En los años posteriores, Eductrade pasó de ser una compañía exportadora de equipos educativos a una compañía proveedora de soluciones educativas integrales, que diseñadas a medida, contenían el refuerzo y fortalecimiento institucional, en consultoría, tecnología, equipos, programas, asistencia técnica, mantenimiento y formación; tanto de profesionales, como de formadores, que garantizaba la sostenibilidad de sus proyectos.

Eductrade detectó una demanda insatisfecha en otras áreas del sector social, e incorporó a su cartera, operaciones de salud y posteriormente operaciones de formación y consultoría aplicada a la salud y la educación.

Esta posición se ha visto reforzada con la incorporación de Eductrade al Grupo Essentium en 2010. La suma de las capacidades y experiencia propias con las del Grupo Essentium, permite a la compañía estar presente de forma activa en todos aquellos proyectos que requieren de una inversión y que su desarrollo se encuentra en sectores en los que Eductrade opera habitualmente: Proyectos Públicos Privados de Hospitales, Gestión de Centros Educativos, Culturales y Deportivos, proyectos de equipamiento integral cuya actividad es el diseño, gestión, ejecución y administración de contratos de suministros y servicios que suelen identificarse como llave en mano.

En la imagen 1.1 se muestra el organigrama a nivel internacional, cabe resaltar que en México la empresa Eductrade cuenta con los departamentos de Proyectos de Salud y las Concesiones Hospitalarias para proyectos nacionales. Dentro de las Concesiones Hospitalarias existe el Departamento de Ingeniería Biomédica en la cual laboro yo.

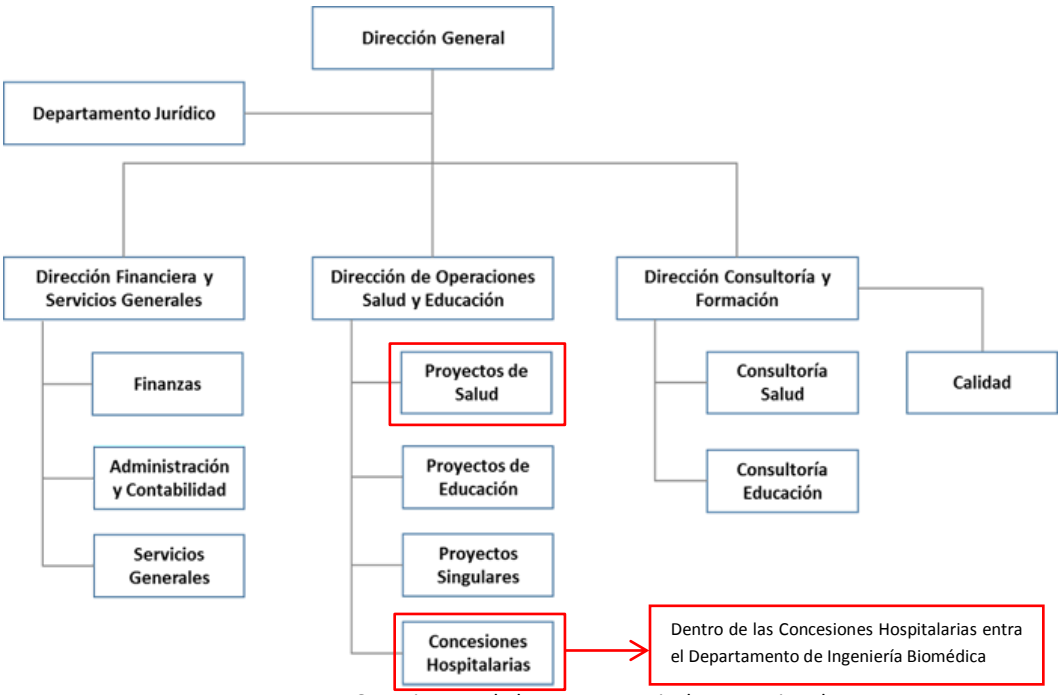


Imagen 1. 1 Organigrama de la Empresa a nivel Internacional

Entre las diversas participaciones de Eductrade en la industria, Eductrade en México tiene una oficina para los Proyectos de Salud ubicada en el Distrito Federal y para las Concesiones Hospitalarias Eductrade en México forma parte como inversionista proveedor del HRAEI (Hospital Regional de Alta Especialidad de Ixtapaluca) ubicado en el municipio de Ixtapaluca, Estado de México donde destaca el Departamento de Ingeniería Biomédica en el cual se hace el servicio de mantenimiento preventivo, correctivo y capacitación de equipamiento médico.

La Ingeniería Clínica es la rama de la Ingeniería Biomédica que se ocupa de la gestión tecnológica hospitalaria, cuyo objetivo fundamental es alcanzar una atención de excelencia a costos razonables, mediante el empleo óptimo y eficiente de la tecnología y la planeación, además, estudia, diseña y mantiene los sistemas que se emplean dentro de los edificios de las unidades de salud (equipo médico).

En Eductrade-Ixtapaluca el Departamento de Ingeniería Biomédica tiene como su principal objetivo garantizar el funcionamiento óptimo de los equipos médicos a través de la administración de los recursos tecnológicos planeando y realizando las actividades necesarias para minimizar las fallas que atenten con detener la prestación de los diversos servicios médicos y dando soluciones a las necesidades clínicas logrando así una adecuada atención a los pacientes.

En el desarrollo de la Ingeniería enfocada en los sistemas de salud es importante planificar las actividades. Planificar abarca definir objetivos, metas y establecer estrategias para alcanzarlas, además implica coordinar actividades que se deben plasmar por escrito y lograrse en un periodo establecido. Se debe planificar para proporcionar dirección, reducir repercusiones al cambio, reducir al mínimo desperdicios, identificar riesgos y minimizarlos, y que establezca normas que faciliten el control (políticas), en otras palabras, la planificación constituye un esfuerzo coordinado donde los miembros de la organización entienden hacia dónde se dirigen y qué deben aportar para alcanzar los objetivos, propiciando con ello trabajo en equipo.

Toda planificación debe llevar una etapa de control y medición por medio de la recolección de datos que permitan un análisis y toma de decisión para llevar a cabo mejoras o correcciones. Un indicador es una medida cuantitativa que puede usarse como guía para controlar y valorar la calidad de las actividades. En este caso en particular, se cuentan con indicadores que cuantifican el desempeño mediante la medición de mantenimientos preventivos, correctivos, tickets y asistencias al usuario.

A partir de este momento en la redacción nos enfocaremos al Departamento de Ingeniería Biomédica de la empresa Eductrade en México y para ser específicos en el municipio de Ixtapaluca en el Estado de México, se menciona en la redacción ya sea Eductrade-Ixtapaluca o Departamento de Ingeniería Biomédica.

## 1.2. Objetivo

Ofrecer un servicio de excelencia para la gestión y conservación del equipo médico, obteniendo resultados confiables y veraces mediante la alta especialización en su personal y el uso de herramientas tecnológicas, que ayude a la reintegración del paciente a la vida diaria.

## 1.3. Visión

Ser la empresa líder a nivel nacional en la prestación de Servicios de Gestión de Equipamiento Médico (Ingeniería Biomédica), reconocida a nivel internacional por su alta calidad y resultados confiables basados en la ciencia y tecnología.

## 1.4. Misión

Brindar un servicio de Gestión de Equipamiento Médico de excelencia que combine el trato humano, la alta capacidad de su personal y el uso de herramientas tecnológicas.

## 1.5. Valores

- Servicio: Tener la actitud y aptitud de atención al cliente, brindar ayuda cuando se requiere
- Responsabilidad: Responder satisfactoriamente a los desafíos o a las obligaciones contraídas que estén a nuestro alcance, ser consciente de que algunos equipos son de soporte de vida
- Ética: Decir y hacer lo correcto
- Profesionalismo: Aplicar los conocimientos en las problemáticas diarias para llegar soluciones satisfactorias
- Honestidad: Decir la verdad

## 1.6. Política de calidad

Ser una empresa que ofrece servicios de gestión de equipo médico de calidad, soportados por una infraestructura humana, instalaciones, equipamiento de vanguardia y procesos controlados que cumplan con estándares nacionales e internacionales, garantizando la confianza y satisfacción de nuestro cliente, buscando siempre la seguridad del paciente en la parte de equipamiento.

## 1.7. Organigrama

En la imagen 1.2 se muestra la Organización actual del Departamento de Ingeniería Biomédica, conformado por 14 personas.

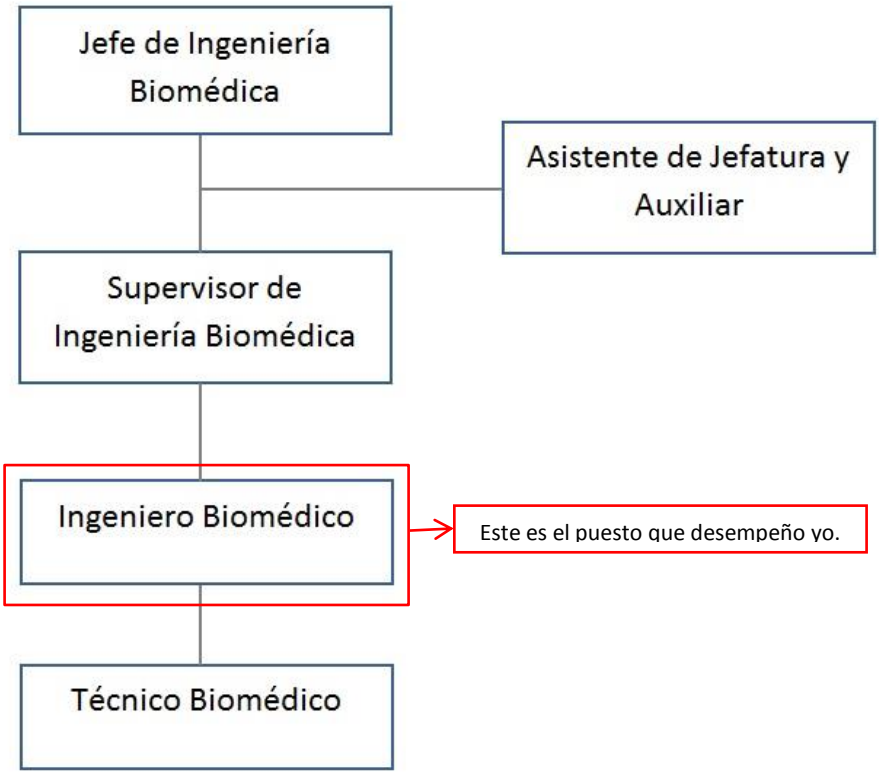


Imagen 1. 2 Organigrama del Departamento de Ingeniería Biomédica

El Jefe de Ingeniería Biomédica es el Ing. Atanasio López Vivero.

Sus asistentes de jefatura son:

- C. Karla Paola Urrutia Muñoz
- C. Ivonne Castañeda Rodríguez

Los Supervisores de Ingeniería Biomédica son dos:

- Ing. Marco Antonio Mejía Serratos, encargado de áreas quirúrgicas.
- Ing. Angélica Mireya Arzate Campos, encargado de áreas de diagnóstico.

Los Ingenieros Biomédicos somos ocho:

1. Ing. César Arturo Méndez Mosco, encargado de las siguientes áreas:
    - CEYE (Centro de Esterilización y Equipamiento)
    - Quirófano
    - Embarazo de alto riesgo
    - Sub CEYE

2. Ing. Oscar Villegas Granados, encargado de las siguientes áreas:
    - Imagenología
    - Hemodinamia
    - Radioterapia
    - Oncología
    - Farmacia
    - Medicina nuclear

3. Ing. Ever Rene Serrano Espíndola, encargado de las siguientes áreas:
    - Admisión continua
    - Terapia intensiva adulto
    - Terapia intermedia adulto
    - Endoscopia
    - Terapia intensiva neonatal

4. Ing. Noé Bonilla López, encargado de las siguientes áreas:
    - Inhaloterapia
    - Terapia intermedia pediátrica
    - Neumología
    - Hospitalización pediátrica
    - Anatomía patológica
    - Cirugía ambulatoria

5. Ing. Pedro Correa Juárez, encargado de las siguientes áreas:
    - Neonatología
    - Hospitalización cuarto piso
    - Aféresis
    - Clínica de la mujer

6. Ing. José Luis Sánchez Mejía, trabaja en el turno nocturno.

7. Ing. Sebastián Eduardo Olguín Ramírez, trabaja en el turno nocturno.

8. Ing. Alejandro Baranda Vargas, mis actividades son:
    A) Ser el encargado del turno vespertino y de las siguientes áreas: Terapia intensiva pediátrica, Hospitalización tercer piso, Clínica del dolor, Clínica del sueño, Terapia intermedia neonatal.
    B) Además realizo apoyo en áreas como: Endoscopias, Quirófano, Imagenología, Hemodinamia, Terapia intensiva adultos, Terapia intermedia adultos, Hospitalización

primer piso, Embarazo de alto riesgo, UCIN, CEYE, Terapia intensiva pediátrica, Hospitalización pediatría y Admisión continua.

C) Control de inventario
D) Revisiones de Áreas
E) Responsable del control y la mejora continua a rutinas de mantenimiento preventivo
F) Impartición de capacitaciones a usuario
G) Administrar las redes del Departamento de Ingeniería Biomédica
H) Responsable de la actualización y desarrollo de la videoteca
I) Apoyo en la instalación de software y configuración de red en impresoras
J) Apoyo en el desarrollo de páginas web
K) Mantenimiento preventivo, correctivo a equipos médicos

El Técnico Biomédico es Juan Antonio Camacho Gómez, encargado de las siguientes áreas:

- Hospitalización segundo piso
- Hospitalización primer piso
- Consulta externa
- Medicina física
- Unidades funcionales

# Capítulo 2
# Proyectos desarrollados

En el presente capítulo, se presentan algunos de los proyectos realizados durante el tiempo en el que he laborado en el Departamento de Ingeniería Biomédica, en el puesto de Ingeniero en Computación en el módulo de Ingeniero Biomédico.

## 2.1. Rehabilitar el monitor espejo de UCIN Referidos de la Central de Monitoreo de la UCIN

La primera tarea que me asignaron al entrar en el Departamento de Ingeniería Biomédica (octubre de 2013), fue:

Problema: revisar el por qué ya no funcionaba el monitor espejo de la central de monitoreo de la Unidad de Cuidados Intensivos Neonatales *(UCIN)*.

Propuesta de solución: revisar voltaje en los contactos, revisar las condiciones del cableado de red, verificar que los cables de red tengan la configuración adecuada y tengan continuidad.

Actividades desarrolladas: se verifica que los contactos tengan el voltaje requerido por lo tanto se descarta que el problema sea con el cable de corriente eléctrica, se revisa el cable de HDMI, se revisa el cableado estructurado y se comprueba con el probador de cables RJ45 que estén bien conectados, se etiquetan los cables.

Resultados obtenidos: se encontró que los problemas fueron:

- Un cable de red con configuración directa en vez de cruzada
- Cuatro de los conectores Jack RJ45 (hembra) en mal estado

Se corrigen problemas y se habilita el monitor espejo. Se sugiere que las conexiones no queden a nivel de piso, como actualmente se tienen ya que la tendencia es que vuelva a suceder lo mismo por los golpes que se tienen con los pies.

Período: octubre de 2013

## 2.2. Cambio de direcciones IP en Monitores de Signos Vitales

Problema: No se pueden ver los signos vitales de los pacientes en la central de monitoreo.

Propuesta de solución: Revisar la conexión de los cables al paciente y al monitor de signos vitales.

Actividades desarrolladas: Se acude al área, se revisan conexiones al paciente y al monitor de forma correcta. Se detecta que por logística se intercambiaron de área algunos monitores de signos vitales que son modelo: Infinity Vista por otros monitores modelo: Delta. Ya que los que son modelo: Infinity Vista. No cuentan con los módulos para revisar la presión arterial invasiva. Al detectar que no todos los monitores correspondían a su área original se realizó:

- Un mapeo de las direcciones IP asignadas por área de los monitores de signos vitales que tienen conexión a las centrales de monitoreo de las áreas (UCIN, Terapia Intensiva Pediátrica y Terapia Intensiva Adulto)
- Se identificaron los equipos que no correspondían al área asignada por guía de dotación y se configuraron con las IP correspondientes

Resultados obtenidos: Se capacitó al usuario para dar de alta al paciente colocando los datos personales en el monitor de signos vitales visualizando su información en el display. Con el propósito de identificar siempre al paciente por su nombre y no por ambiente de trabajo, además se demostró que se puede mandar una impresión de la información que presenta el paciente desde cada monitor de signos vitales o desde la central de monitoreo.

Período: octubre a noviembre de 2013

## 2.3. Videoteca

Problema: Discrepancia en la información que tiene el usuario para hacer pruebas a los equipos médicos.

Propuesta de solución: Con la finalidad de estandarizar la información que tenga el personal del Departamento de Ingeniería Biomédica se implementó una videoteca en la cual se puede ver el manual de usuario o de servicio en formato electrónico del equipo y videos para la capacitación de uso o servicio.

Actividades desarrolladas: Se trabajó con software (Dreamweaver, PHP, Movie Maker, Convertidor de Video Quick Media) y hardware (cámara de video). Se implementó una videoteca en el servidor para que desde las estaciones de trabajo los usuarios puedan acceder a la información necesaria y ver los videos o los manuales las veces que se requiera.

Resultados obtenidos: Información estandarizada para el Departamento de Ingeniería Biomédica y capacitación visual en cualquier momento.

Período: febrero de 2014 a la fecha

## 2.4. Actualización de rutinas para mantenimiento preventivo

Problema: No hay rutina de mantenimiento preventivo del equipo que tienen que hacer el técnico e ingenieros y tienen que esperar a que llegue el encargado de las rutinas de mantenimiento preventivo.

Propuesta de solución: Almacenar las rutinas en el servidor en formato PDF (Portable Document Format “formato de documento portátil”) y aplicarles contraseña para poder visualizarlos.

Actividades desarrolladas: Se realizó la revisión No. 3, esto es, actualizar la rutina de mantenimiento preventivo con base en el manual de servicio y en las necesidades que se tienen por ejemplo se anexa un apartado para saber si el equipo fue encontrado en su lugar original, en caso de no encontrarlo en su área asignada indicar su área externa y área interna. Lo anterior nos ayuda a mantener actualizado el inventario de equipo médico. Se guardó el archivo original y se guardó otro archivo con formato PDF, se le agregó una contraseña para visualizarlo, se

almacenaron las rutinas en formato electrónico en una carpeta compartida por el servidor y se les notificó al Departamento de Ingeniería Biomédica la contraseña para la revisión No.3.

Resultados obtenidos: El tiempo para realizar el mantenimiento preventivo disminuye ya que la información está disponible todo el tiempo, se hace la impresión de las rutinas y se guarda en una carpeta por si en algún momento no pueden visualizar las rutinas en formato electrónico.

Período: enero a marzo de 2015

## 2.5. Diseño, administración y mantenimiento del sitio web

Problema: Difundir lo que hace el Departamento de Ingeniería Biomédica para ofrecer servicios a otros hospitales.

Propuesta de solución: Desarrollo de un sitio web con dominio: www.eductrade.com.mx

Actividades desarrolladas: Se realiza la cotización para el alojamiento web por dos años y se verifica la disponibilidad del dominio, se realiza la propuesta y presentación del sitio web al Jefe de Ingeniería Biomédica, se me solicitó realizar algunas modificaciones las cuales ya fueron actualizadas, por lo que soy el responsable de administrar los contenidos dados de alta, modifico y organizo aquellos que tienen algunas fallas o bien, creo nuevas carpetas y temas que son solicitados. Actualmente ya está el diseño y la cotización. Estamos en espera de la aprobación por parte de Eductrade.

Resultados esperados: Difundir nuestros servicios para ampliar clientes.

Período: febrero 2015 a la fecha

# Capítulo 3 Redes inalámbricas y sus seguridades

En este capítulo se presenta lo que es una red inalámbrica, sus fundamentos, los diferentes tipos de topologías de una red inalámbrica sus ventajas y desventajas.

## 3.1. Fundamentos

Se establecen los conceptos básicos de redes de datos y redes inalámbricas los cuales facilitan la mejor comprensión de los capítulos posteriores. Es muy importante el desarrollo y entendimiento de estos fundamentos ya que aquí se acentúa la mayoría de la terminología necesaria para este informe.

### 3.1.1. Redes de computadoras

Conjunto de dispositivos electrónicos (equipos de cómputo) interrelacionados entre sí mediante vías o medios de transmisión, con la finalidad de compartir recursos (procesar, generar, almacenar y distribuir datos) y llevar a cabo la transferencia de información de manera segura, eficiente y confiable.

#### *3.1.1.1. Clasificación de las redes de computadoras*

En la actualidad existen muchos tipos de redes de computadoras cada una con sus características y objetivos diferentes, sin embargo, estas redes de computadoras pueden ser clasificadas de acuerdo a sus características principales. Una de las clasificaciones más comunes de las redes de computadoras son: las redes privadas dedicadas y las redes compartidas.

Las redes privadas dedicadas son aquellas en las que existe un único tipo de tráfico además de un determinado número de nodos que tienen como propósito asegurar la calidad, la seguridad y/o velocidad. Normalmente se utilizan para garantizar el servicio de transporte de datos en ciertas condiciones, a grandes grupos de usuarios de la red. Las tecnologías que soportan estas redes dedicadas dependen, en primer lugar, del tipo de información que manejan: voz, video o datos. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto. En una red punto a punto se permiten las conexiones en línea directa entre equipos y terminales. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión y la seguridad que presenta al no existir conexión con otros usuarios. En una red multipunto se permite la unión de varias terminales a su correspondiente computadora compartiendo una única línea de transmisión. La ventaja consiste en la disminución de costos, aunque pierde velocidad y seguridad.

Las redes compartidas son aquellas en las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con comunicaciones de otras naturalezas. Las redes más usuales de este tipo son las de conmutación de paquetes y las de conmutación de circuitos.

Otra forma de clasificar a las redes de computadoras es por su conexión y su alcance:

A) Redes de área personal (Personal Area Network, PAN): Las Redes de Área Personal son de alcance muy limitado (unos pocos metros), y se utilizan para interconectar dispositivos personales de marea inalámbrica (*Personal Computers PC's*, laptops, celulares, *Personal Digital Assistants PDA's*, impresoras, por mencionar algunos). Estas redes son de velocidad media (algunos MBps) y están teniendo creciente desarrollo en los últimos años.

B) Redes de área local (Local Area Network, LAN): Son las redes con una determinada área local, es decir las redes de pequeñas oficinas o empresas desean aplicar tecnología informática para compartir archivos, software, e impresoras de manera eficiente además de permitir las comunicaciones entre los equipos que estén conectados a esa red. Estas redes operan dentro de un área geográfica limitada, permiten el multi-acceso a medios con alto ancho de banda, controlan la red de forma privada con administración local, proporciona conectividad continua a los servicios locales y conectan dispositivos físicamente adyacentes. Existen redes LAN alámbricas e inalámbricas, ambos utilizan el estándar Ethernet. Una red de área local (LAN) es un grupo de ordenadores conectados a un área localizada para comunicarse entre sí y compartir recursos como, por ejemplo, impresoras. Los datos se envían en forma de paquetes, para cuya transmisión se pueden utilizar diversas tecnologías. La tecnología LAN más utilizada es la Ethernet y está especificada en la norma IEEE 802.3. El medio de transmisión físico para una LAN por cable implica cables, principalmente de par trenzado, o bien, fibra óptica. Un cable de par trenzado consiste en ocho cables que forman cuatro pares de cables de cobre trenzados, y se utiliza con conectores RJ-45 y sockets. La longitud máxima de un cable de par trenzado es de 100 m, 90 m para transmisión y 10 m para conexiones, mientras que para la fibra, el máximo varía entre 10 km y 70 km, dependiendo del tipo. En función del tipo de cables de par trenzado o de fibra óptica que se utilicen, actualmente las velocidades de datos pueden oscilar entre 100 Mbit/s y 10.000 Mbit/s. En la imagen 3.1 se muestra el cable de par trenzado que está formado por cuatro pares de cables trenzados que normalmente se conectan por el extremo a un conector RJ-45.

Imagen 3. 1 Cable de par trenzado conectado a un conector RJ-45

Existen diferentes tipos de redes Ethernet como son:

i. Fast Ethernet: Hace referencia a una red Ethernet que puede transferir datos a una velocidad de 100Mbit/s. Se puede basar en cable de par trenzado o de fibra óptica. El tipo de cable de par trenzado compatible con Fast Ethernet se denomina Cat-5e para las redes ya instaladas o Cat-6 para las nuevas instalaciones.
ii. Gigabit Ethernet: También se puede basar en cable de par trenzado o de fibra óptica, proporcionando una velocidad de transferencia de datos de 1.000 Mbit/s (1 Gbit/s) y es cada vez más frecuente.

C) Redes de área metropolitana (Metropolitan Area Network, MAN): Son las Redes de Área Metropolitana, un poco más extensas que las anteriores ya que permiten la conexión en un nivel más grande, como una población pequeña o una ciudad. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común.

D) Redes de área amplia (Wide Area Network, WAN): Son las Redes de Área Amplia, aquellas de grandes dimensiones que conectan países e incluso continentes. Las WAN son las que vinculan las redes LAN, que a su vez proporcionan acceso a las computadoras o a los servicios de archivos en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica, extensa, permiten que las organizaciones compartan información entre sí a través de grandes distancias. El software de colaboración brinda acceso a información en tiempo real y a recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona.

En la tabla 3.1 se muestra el ancho de banda y el rango de transmisión de los tipos de redes.

Tabla 3. 1Tipos de red con sus rangos y anchos de banda

| TIPO DE RED | RANGO | ANCHO DE BANDA |
|---|---|---|
| PAN | <10 [m] | 10 Mbps |
| LAN | 1-2 [km] | 10-1,000 Mbps |
| MAN | 2-50 [km] | 2-155 Mbps |
| WAN | 100-1000 [km] | 1 Mbps – 1 Gbps |

### *3.1.1.2. Topologías de red*

Existen diferentes maneras de conectar los dispositivos de una red, dependiendo de las necesidades que se tengan será la arquitectura que puede adoptar. Cada una de estas clasificaciones de alguna forma compartirá el medio de transmisión de datos. Las topologías básicas de las redes de datos se muestran en la imagen 3.2 y son las siguientes:

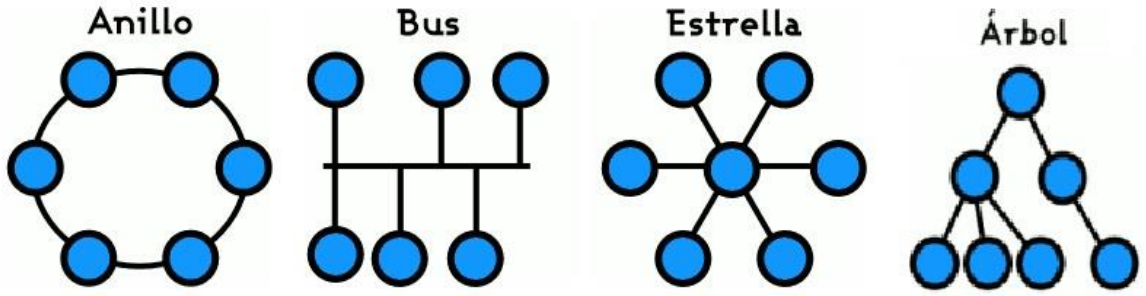


Imagen 3. 2 Topologías de Red

A) Topología de Anillo: Hace referencia a su nombre por la forma que toman los equipos conectados entre sí para formar un anillo físico del medio de transmisión. Los equipos que forman parte de la red se conectan uno a otro hasta llegar al último equipo que se conecta

al primero. La forma de comunicación entre dos equipos que forman este anillo es mandando un paquete de información que viaja a través del medio pasando por todas las computadoras hasta llegar al destino, haciendo énfasis en que el paquete y la información en general circulará en sólo un sentido.

B) Topología de Bus: Esta topología usa un solo cable como eje de la red al cual se conectan todos los equipos que termina en ambos extremos. Cuando los equipos quieren comunicarse se envían los paquetes por el medio de transmisión y todos los equipos pueden escuchar la señal, sin embargo este paquete lleva la información de la dirección a la cual va dirigido, por lo que si no son los destinatarios se ignora la información.

C) Topología de Estrella: Cada uno de los equipos que pertenecen a la red está conectado a un conmutador central. Aquí él envió de los paquetes de información viaja a través del medio de transmisión y llegan al punto central donde cada uno de los equipos puede ver la información, el nodo central o conmutador envía la información recibida a todos los demás nodos de la red.

D) Topología de Árbol: En esta topología de tipo jerárquica se compone de un punto raíz a partir del cual se conectan uno o más cables, en donde cada uno de ellos puede tener ramificaciones a cualquier otro punto, es decir que cada ramificación a partir del nodo central puede ramificarse, cabe señalar que en este tipo de topologías no se pueden formar ciclos.

#### *3.1.1.3. Modelo OSI*

El modelo de referencia de Interconexión de Sistemas Abiertos (*Open System Interconection, OSI*) creado por la Organización Internacional de Normalización como necesidad de establecer un estándar para el creciente desarrollo de las tecnologías de red y hacer que éstas tecnologías fueran compatibles además de aplicables a todas las redes existentes al momento, surgió en 1984. El modelo OSI ofrece muchas ventajas como por ejemplo reduce mucho la complejidad de los protocolos de interconexión de redes, asegura la interoperabilidad de la tecnología, estandariza interfaces que intervienen en el procesamiento de los paquetes de información, etcétera.

El modelo OSI permite hacer un análisis de cómo la información viaja en la red, de manera muy detallada va llevando paso a paso cómo un paquete de información pasa a través de diferentes capas de este modelo. Las capas del modelo OSI son 7, las cuales se describen a continuación:

1) Capa física: Transmisión de datos a nivel binario esto se logra mediante la transmisión física de las señales con niveles de voltajes diferentes, en esta capa interviene lo que son los elementos físicos como cables de red, conectores, voltajes, velocidades de transmisión de datos.
2) Capa de enlace de datos: Su objetivo es dar fiabilidad a la transmisión de las señales eléctricas, tener el control directo de enlaces, acceso a los medios, provee transferencia confiable de datos a través de los medios, conectividad y selección de ruta entre sistemas, direccionamiento lógico además de una tarea muy importante: el control de flujo.

3) Capa de red: La asignación de dirección de red y determinación de la mejor ruta es decir el direccionamiento, provee trasferencia confiable de datos a través de los medios. Conectividad y selección de rutas entre sistemas.
4) Capa de transporte: El objetivo principal de este nivel consiste en asegurar la calidad de transmisión de datos, ordenar la información, ajustar la velocidad de información. Se ocupa de aspectos de transporte entre dispositivos, además de establecer, mantener y terminar circuitos virtuales, detección de fallas y control de flujo de información de recuperación.
5) Capa de sesión: Comunicación entre los dispositivos; establece, administra y termina sesiones entre aplicaciones.
6) Capa de presentación: Representación de los datos, garantiza que los datos sean legibles para el sistema receptor, formato de los datos, estructuras de datos, negocia la sintaxis de transferencia de datos para la capa de aplicación.
7) Capa de aplicación: Procesos de red a aplicaciones, suministra servicios de red a los procesos de aplicaciones como lo son por ejemplo el correo electrónico, transferencia de archivos y emulación de terminales.

#### *3.1.1.4. Modelo TCP/IP*

El modelo TCP/IP creado por el Departamento de Defensa de los Estados Unidos como una necesidad de tener compatibilidad entre las redes y medios de transmisión en épocas de guerra, fue desarrollado como un estándar abierto es decir que cualquier persona podía usar el estándar. *Transfer Control Protocol (TCP),* proporciona mecanismos de control de flujo y errores entre los extremos que están llevando a cabo la comunicación, por otro lado *Internet Protocol (IP),* es un protocolo que proporciona mecanismos de interconexión entre redes de área local.

El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

El modelo TCP/IP está compuesto por 4 capas, a continuación se muestra la correspondencia que existe entre las capas del modelo OSI y las del modelo TCP/IP:

1) Capa de acceso a la red: Guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles de tecnología de red, y todos los detalles de la capa 2 (enlace de datos) y a la capa 1 (física) del modelo OSI.
2) Capa de Internet: El propósito de la capa es dividir los segmentos TCP en paquetes y enviarlos desde cualquier red. Los paquetes llegan a la red destino independientemente de la ruta que utilizaron para llegar allí. El protocolo específico que rige esta capa se denomina *Protocolo de Internet (IP),* En esta capa se produce la determinación de la mejor ruta y la comunicación de paquetes. La relación entre IP y TCP es importante. Se puede

pensar en IP como el que indica el camino a los paquetes, en tanto que TCP brinda el transporte seguro. Asimilable a la capa 3 (red) del modelo OSI.

3) Capa de transporte: Tiene como objetivo la calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. El protocolo para el control de transmisión (TCP) ofrece maneras flexibles de alta calidad para crear comunicaciones de red confiables sin problemas de flujo y con un nivel de error bajo. Orientado a conexión. Asimilable a la capa 4 (transporte) del modelo OSI.
4) Capa de aplicación: Maneja aspectos de presentación, codificación y control de diálogo Asimilable a las capas: 5(Sesión), 6 (presentación) y 7 (aplicación) del modelo OSI.

En la imagen 3.3. Se muestra una comparativa entre el modelo OSI y el modelo TCP/IP

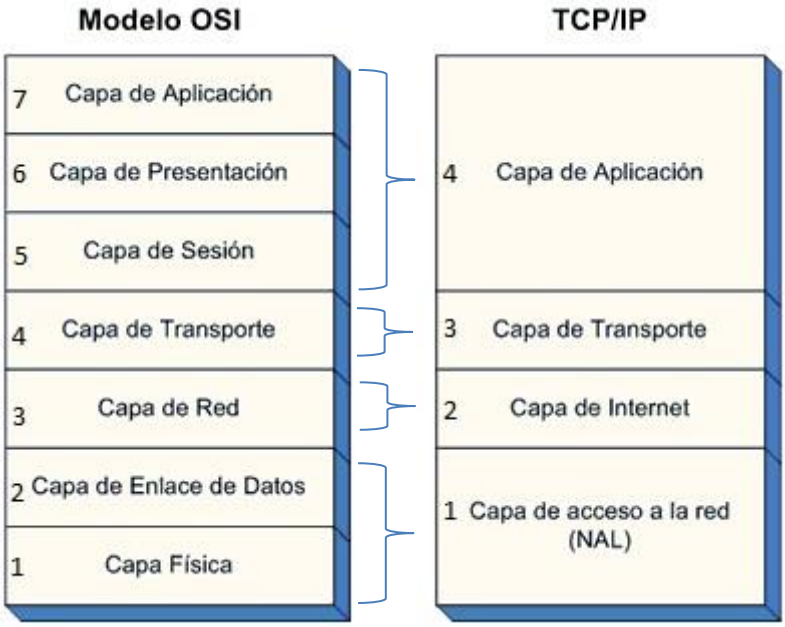


Imagen 3. 3 Comparativa entre los modelos OSI y TCP/IP

### 3.1.2. Red inalámbrica

Red inalámbrica o *WLAN (Wirless Local Area Network)* es un término nuevo que se ha formado en un tiempo relativamente corto, gracias al gran avance y popularidad de las comunicaciones móviles. En el mercado, se ha visto reflejado a este impacto como referente a la movilidad de las redes e Internet. Obviamente esto ha beneficiado al desarrollo de las redes inalámbricas locales, como por ejemplo en que la implementación de una red inalámbrica se ha simplificado, el bajo costo de los elementos que la conforman y flexibilidad para su uso. Las redes inalámbricas pueden ser conectadas a una red LAN cableada como una extensión del sistema o pueden operar de manera independiente para permitir conexiones de datos entre computadoras.

Las redes inalámbricas pueden proveer de casi todas las funciones y las altas tasas de transferencia ofrecidas por una red cableada LAN. Las velocidades en que una red inalámbrica opera típicamente son entre los 1 Mbps a 54 Mbps.

En la industria el estándar referente a las redes inalámbricas que describe las especificaciones inalámbricas es el 802.11, fue liberado en junio de 1977, en su primera versión.

Desde la perspectiva del usuario, sus funciones y uso son exactamente como una red alámbrica LAN, sin embargo el poder controlar el acceso en un medio de transmisión como el aire los métodos son más complejos que aquellos que se controlan por un medio cableado (Ethernet).

Hay diferentes versiones de redes inalámbricas WLAN, las diferencias de estas redes radican en la banda de frecuencia en que operan, el tipo de acceso inalámbrico y las velocidades máximas de transmisión.

El término red inalámbrica se utiliza para designar la conexión de nodos, sin necesidad de una conexión física (cables) del Punto de Acceso a las estaciones de trabajo, ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos y con las redes inalámbricas un usuario puede mantenerse conectado, cuando se desplaza dentro de una determinada área geográfica. Las redes inalámbricas tipo infraestructura requieren de un Punto de Acceso el cual está conectado al sistema de distribución por medio de un cable de par trenzado.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo), en lugar de cableado estándar. Hay muchas tecnologías que se diferencian por la frecuencia de transmisión que utilizan, el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad ya sea que se encuentren a unos metros de distancia o a varios kilómetros. Así mismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente, como pasa en las redes cableadas.

Por otro lado, existen cuestiones relacionadas con la regulación legal del espectro electromagnético, porque las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y aficionados), que son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica, restringida, por lo que un hacker puede con facilidad escuchar una red, si los datos que se transmiten no están codificados. Por lo tanto se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

La naturaleza de las redes Wireless hace que cualquier persona pueda tener acceso a los datos que son envidados, debido a que estos utilizan como medio de transmisión el aire (ondas electromagnéticas). Esto plantea un problema añadido con respecto al cable, pues para tener acceso a los datos transmitidos por cable, se ha de tener acceso al mismo o a los dispositivos asociados. Para las redes Wireless no es necesario, basta con que la señal viaje hasta nosotros. Por tanto, teniendo en cuenta esta perspectiva se han de implementar los mecanismos necesarios para mantener el nivel de seguridad que se requieren en muchos proyectos.

La revisión 802.11b del estándar original tiene una velocidad máxima de transmisión de 11 Mbps. El estándar 802.11b utiliza la frecuencia 2.4 Ghz que es la misma que ocupan otros dispositivos móviles, como GPS, Bluetooth y demás. Esto puede incidir, para mal, en la calidad de la señal.

Sin embargo, si se utiliza para implementar usuarios que trabajen con el estándar 802.11b, el rendimiento de la celda inalámbrica se ve afectado por ellos, permitiendo sólo una velocidad de transmisión de 22 Mbps.

El estándar 802.11i está dirigido para abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integras – Seguras – Temporales) y AES (Estándar de Cifrado Avanzado) que se implementa en WPA2.

Se debe tener en cuenta que a mayor distancia entre el emisor y el receptor menor velocidad de transmisión. Otro problema que se puede plantear son los elementos intermedios que pueden interferir en la señal, como pueden ser paredes, campos magnéticos o electrónicos. Un aspecto más y que puede producir reducción de la transmisión es la saturación del espectro debido al número de usuarios.

Por último, se puede comentar que existen dos tipos de antenas, omnidireccionales y direccionales. En las primeras, la emisión de la onda se produce en todas las direcciones a discreción, útil para entornos abiertos donde la ubicación de las estaciones no está definida o es susceptible de ocupar cualquier situación física. El segundo tipo dirige la señal a un punto determinado fuera del mismo la señal no es “audible”. Ideal para conectar dos puntos en particular.

En 2004 se comenzó a trabajar en una nueva revisión el 802.11n. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión son aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g y unas 40 veces más rápida que una red bajo el estándar 802.11b. Este estándar se viene implementando desde 2008, 802.11n puede trabajar en dos bandas de frecuencias: 2.4 GHz (la que emplean 802.11b y 802.11 g) y 5 GHz (la que usa 802.11a) Gracias a ello 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

Existen diferentes tipos de redes inalámbricas, algunas son:

A) ESSID/SSID: Toda Red Wireless tiene un *ESSID* (*Extended Service Set Identifier,* Servicio Extendido de Identificación) que la identifica. Este consta de como máximo 32 caracteres. Es necesario conocer el *ESSID* del *AP (Access Point)* para poder formar parte de la WLAN, es decir, el ESSID debe ser el mismo tanto en el *AP* como en el dispositivo móvil (cliente). Existen algunas variantes principales del *SSID*. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID *(Basic Service Set IDentifier)*;

mientras que en las redes en infraestructura que incorporan punto de acceso, se utiliza el ESSID. Se puede referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

B) BSSID: *(Basic Service Set IDentifier).* Utilizado en la red tipo ad-hoc. Se forma con la Dirección MAC (*Media Access Control*; Control de Acceso al Medio) del punto de acceso. Éstas las emplean las tarjetas Wireless para identificar y asociarse a redes inalámbricas.

C) Beacom Frames: Los AP mandan continuamente "anuncios" de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red Wireless. Estos anuncios son conocidos como "Beacom Frames". Esta propiedad puede ser deshabilitada en la mayoría de los AP actuales.

D) OSA (Open System Authentication): Es un proceso de autenticación nulo, las tramas se envían en texto plano aun teniendo activado cualquier cifrado.

E) SKA (Shared Key Authentication): Este método utiliza una clave compartida entre el Punto de Acceso y el cliente. El cliente envía un Authentication Request, mientras que el Punto de Acceso responde con un Authentication Challenge. El cliente a su vez, responde con un Autentication Response (cifrado) y finalmente el Punto de Acceso responde con Authentication Result. Es dentro del SKA donde se pueden utilizar los diferentes sistemas de cifrados existente para redes Wireless.

### 3.1.3. Topología de una red inalámbrica

La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (por ejemplo: impresoras, switches, hubs, servidores, computadoras, enrutadores, entre otros) se interconectan entre sí sobre un medio de comunicación.

- Topología física: Se refiere al diseño actual del medio de transmisión de la red.
- Topología lógica: Se refiere a la trayectoria lógica de una señal a su paso por los nodos de la red.

Existen varias topologías de red inalámbrica (ad-hoc, tipo infraestructura y demás), pero también existen redes híbridas que combinan una o más de las topologías anteriores en una misma red. A continuación se explican algunas de ellas:

A) Modo Ad-Hoc (Redes Independientes IBSS, Independent Basic Service Sets): Esta topología se caracteriza porque no hay Punto de Acceso (AP), las estaciones se comunican directamente entre sí *P2P (peer to peer)*, de esta manera el área de cobertura está limitada por el alcance de cada estación individual. Como se aprecia la interconexión de dispositivos con el modo Ad-Hoc en la imagen 3.4.

No hay un punto de acceso determinado y todos los equipos se comunican entre sí. La naturaleza descentralizada de las redes ad hoc, hace de ellas las más adecuadas en aquellas situaciones en las que no puede confiarse en un nodo central y mejora su escalabilidad comparada con las redes inalámbricas tradicionales, desde el punto de vista teórico y práctico.

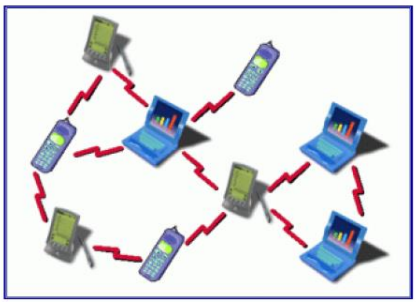

Imagen 3. 4 Topología Ad-Hoc

B) Modo Infraestructura: En el modo infraestructura se dispone como mínimo de un Punto de Acceso (AP) y las estaciones Wireless no se pueden comunicar directamente, todos los datos deben pasar a través del AP. Todas las estaciones deben ser capaces de ver y establecer conexión con el AP, como se aprecia en la imagen 3.5. En está topología debe existir forzosamente un punto de acceso y todos los equipos se conectan a través de él.

La mayoría de las redes inalámbricas se pueden encontrar en las empresas. Utilizan el Modo Infraestructura con uno o más puntos de acceso. El AP actúa como un *Hub* en una red cableada y redistribuye los datos hacia todas las estaciones.

Si el AP se conecta a una red cableada, los clientes inalámbricos pueden acceder a la red fija a través del AP. Para interconectar muchos AP y clientes inalámbricos, todos deben configurarse con el mismo SSID. Es importante resaltar que, a diferencia del modo ad-hoc, los equipos inalámbricos no se comunican directamente entre sí, sino que lo hacen a través de la unidad base, lo que ofrece más seguridad (gracias a la gestión ofrecida por la unidad base) y conectividad con las terminales situados en la red con cables.

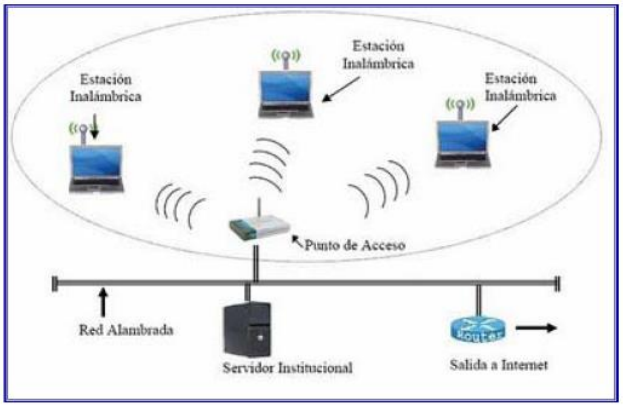


Imagen 3. 5 Topología Infraestructura

C) Redes Mesh (Áreas de servicio extendidas ESS Extended Service Sets): Las redes inalámbricas Mesh, redes acopladas o redes de árbol inalámbricas de infraestructura, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas: la topología Ad-hoc y la topología modo infraestructura. Básicamente son redes con topología de infraestructura que permiten unirse a la red a dispositivos, que están fuera

del rango de cobertura de los AP como se aprecia en la imagen 3.6. Esta topología no es más que una mezcla de las topologías Ad-Hoc e Infraestructura.

Por tanto, se utiliza una topología en árbol (de ahí que se denominen redes acopladas) por la que los mensajes son transmitidos directamente entre las estaciones, aunque éstas no estén gestionadas por el mismo AP.

Imagen 3. 6 Topología Red Mesh

### 3.1.4. Categorías de las redes inalámbricas

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (denominada área de cobertura), como se puede apreciar en la imagen 3.7.

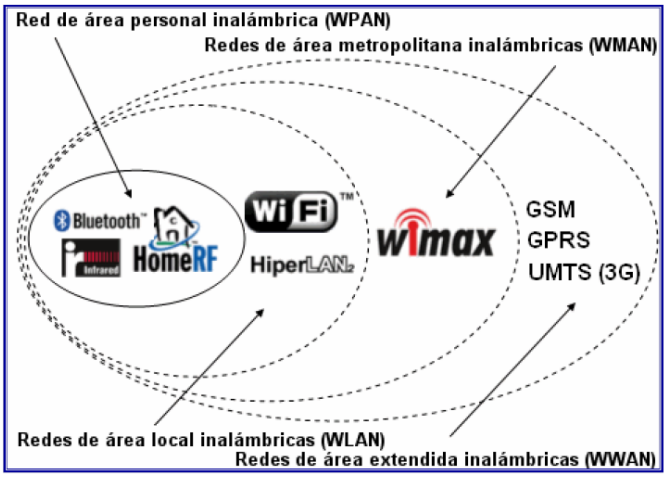


Imagen 3. 7 Denominación de una red a partir del área de cobertura

En el tipo de red de área personal inalámbrica WPAN, existen tecnologías basadas en las radiofrecuencias caseras (protocolo que sigue la especificación IEEE 802.15.1) y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías.

### 3.1.5. Elementos de una red

Los componentes básicos que forman parte de una red son:

- Servidores: la función de los nodos de la red la determina la manera como la configura cada uno cuando se instala por primera vez en la red. A nivel más elemental, un nodo de red puede configurarse como servidor o como estación de trabajo. Servidor es el dispositivo electrónico que proporciona servicio a las estaciones de trabajo. Hay dos tipos de servidores los dedicados y los no dedicados. La cantidad y tipos de servidores de una red depende de la flexibilidad del NOS (Network Operating System) que haya seleccionado y de la manera en que se haya escogido la configuración de las computadoras de la red.
    - Servidor no dedicado: un servidor no dedicado también opera como estación de trabajo. Es posible operar un servidor no dedicado y usarlo como estación de trabajo compartiendo al mismo tiempo sus recursos con otras computadoras.
    - Servidor dedicado: Es un servidor que no puede ejecutar ningún otro trabajo aparte del requerido para compartir sus recursos con los nodos de la red. A diferencia de los servidores no dedicados, los servidores dedicados no pueden usarse como estaciones de trabajo. Un servidor dedicado por lo general maneja un versión del NOS que optimiza la velocidad a la que se intercambian los datos entre el servidor y los nodos de la red. En la imagen 3.8 se muestra un servidor.

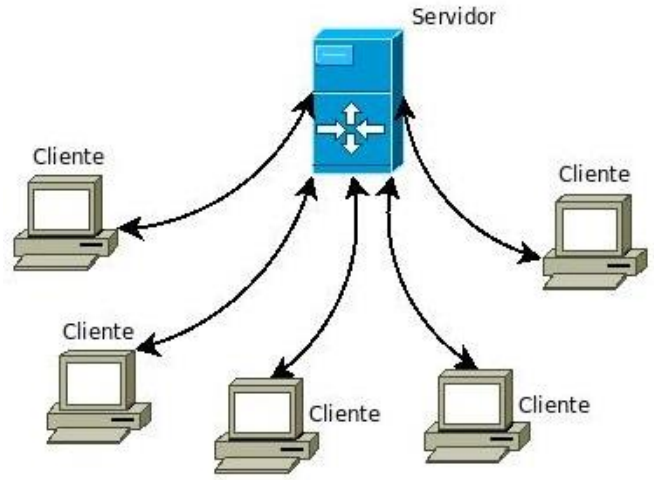


Imagen 3. 8 Servidor

- Terminales o estaciones de trabajo: la estación de trabajo es la computadora ante la cual opera el usuario, capaz de aprovechar los recursos, comunidades de disco e impresoras de otras computadoras (servidores). Una estación de trabajo no comparte sus propios recursos con otras computadoras y por lo tanto los demás nodos no pueden utilizar ningún recurso de ella. En muchas redes en lo particular aquellas que son de tipo servidor no dedicado, cierta computadora puede funcionar como servidor y estación de trabajo.
  Cuando se trata de estaciones de trabajo en un ambiente de red, el significado es el mismo, salvo por un punto adicional, que se tiene la capacidad de utilizar los recursos compartidos de otras computadoras. Las otras computadoras a las que se puede acceder

son las que han sido configuradas como servidores. En la imagen 3.9 se muestran algunas estaciones de trabajo.

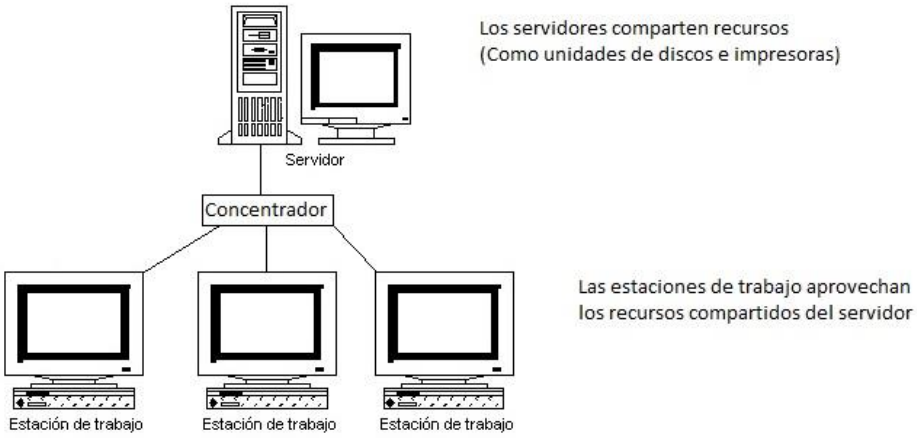


Imagen 3. 9 Estaciones de trabajo

- Sistema operativo de red (NOS): es el software de red instalado en cada computadora o nodo, que permite que la computadora se comunique con las demás. El NOS determina las características de red disponibles y la capacidad de la red; también permite que se configuren los nodos de la red para que se ejecuten las funciones que se desean. Por ejemplo, el NOS permite configurar una o más computadoras de la red para que compartan recursos como las unidades de disco y las impresoras con otras computadoras.
- Módem: Modulador Demodulador. Es un dispositivo que convierte señales digitales en analógicas y viceversa. En el nodo origen, un módem convierte las señales digitales en forma apropiada para su transmisión a través de dispositivos de comunicación analógica. En el destino, las señales analógicas retoman su forma digital. Los módems permiten la transmisión de datos a través de líneas telefónicas de voz. En la imagen 3.10 se muestra un modem, el cual permite conectar una línea telefónica al equipo y acceder a distintas redes, como internet. Los datos transferidos desde una línea telefónica llegan en forma analógica. El módem se encarga de “demodular” para convertir esos datos en digitales, también permiten hacer el proceso inverso, “modular” los datos digitales hacia analógicos, para poder ser transferidos por la línea telefónica.

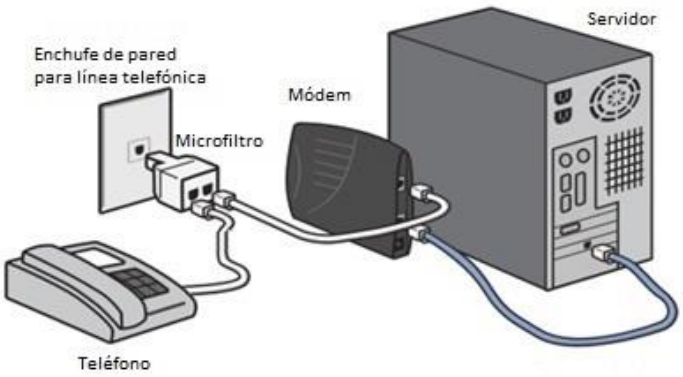


Imagen 3. 10 Modem

- Repetidores: un repetidor se muestra en la imagen 3.11. Es un dispositivo que permite extender la longitud de una red, amplifica y retransmite la señal de red.

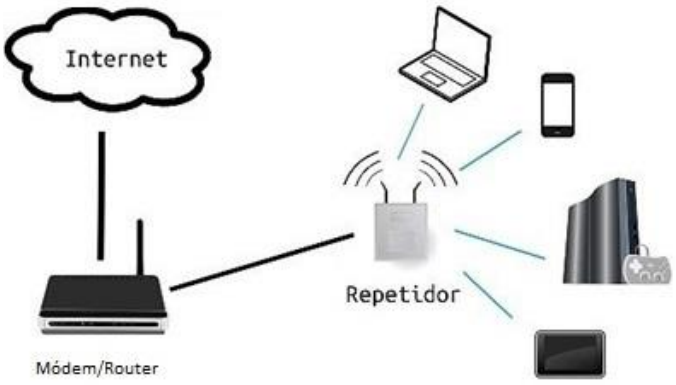


Imagen 3. 11 Repetidor

- Concentradores (Hub): En la imagen 3.12 se muestra el Hub, trabaja en la capa física (capa 1) del modelo OSI o la capa de acceso a la red (capa1) del modelo TCP/IP. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos. La deficiencia que presenta un Hub es que divide la señal que recibe entre el número de nodos que tiene conectados, por ejemplo; si recibe 100Mb/s a la entrada y tiene cinco estaciones de trabajo, cada estación de trabajo tendrá una velocidad de conexión de 20 Mb/s ya que la señal se replica simultáneamente a todos los equipos conectados al Hub.

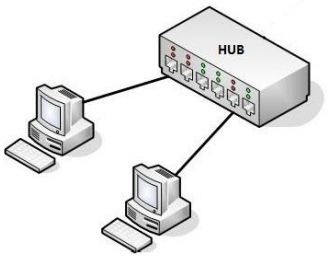


Imagen 3. 12 Hub

- Conmutadores (Switch): En la imagen 3.13 se muestra un conmutador. El conmutador es un dispositivo digital de interconexión de redes de computadoras, trabaja en la capa de enlace de datos (capa 2) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta. Los conmutadores se utilizan para conectar múltiples redes, haciendo que funcione como si fuera una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes LAN. Su ventaja que presenta es que tiene la capacidad de mantener la misma velocidad de transmisión en cada una de sus estaciones de trabajo conectadas. Por ejemplo; si recibe 100Mb/s a la entrada y tiene cinco estaciones de trabajo, cada estación de trabajo tendrá una velocidad de conexión de 100 Mb/s. Otra de sus cualidades es que poseen la capacidad de aprender

y almacenar las direcciones de red (direcciones MAC) de los dispositivos conectados a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que la información dirigida a un dispositivo vaya desde el puerto origen al puerto destino sin replicarse hacia el resto de los dispositivos conectados al Switch.

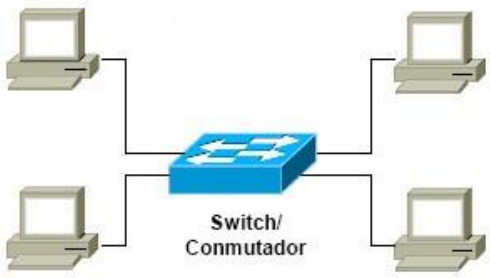


Imagen 3. 13 Switch

- Puentes (Bridges): un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparente ser una sola LAN. Los puentes revisan la dirección asociada con cada paquete de información. Sin embargo también permiten segmentar redes grandes en varias subredes más manejables, si la dirección es la correspondiente al otro segmento de red, el puente pasará el paquete al segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del segmento de red actual no pasará el paquete al otro lado. En la imagen 3.14 se muestra un puente de red. Opera en la capa de enlace de datos (capa 2) del modelo OSI.

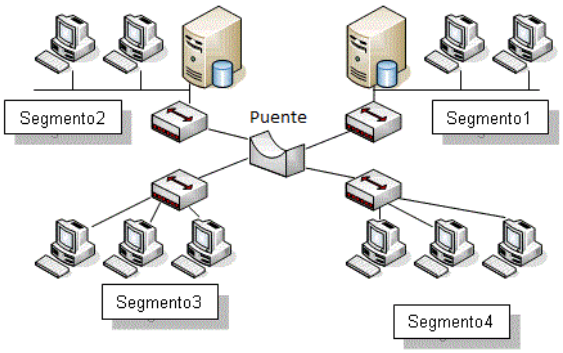


Imagen 3. 14 Puente

- Ruteadores (Routers): Los ruteadores no requieren por lo general que cada red tenga el mismo NOS. Con un NOS común el ruteador puede ejecutar funciones más avanzadas de las que podría permitir un puente, como conectar redes basadas en topologías lógicas completamente diferentes. Los ruteadores también suelen ser lo suficientemente inteligentes para determinar la ruta más eficiente para el envío de datos, en caso de haber más de una ruta. Es un dispositivo que proporciona conectividad en la capa de red (capa 3) del modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir interconectar subredes, entendiendo por subred un conjunto de

máquinas con direcciones IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos. En la imagen 3.15 se aprecia un Router.

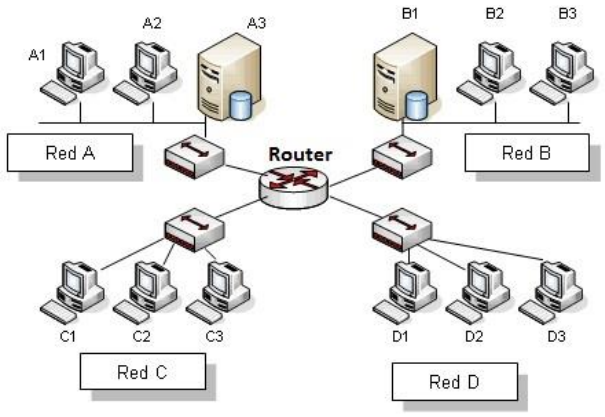


Imagen 3. 15 Router

- Puntos de Acceso (AP): Un punto de acceso es el dispositivo que se utiliza para conectar los diferentes equipos con las redes inalámbricas que poseen una arquitectura en modo infraestructura. El punto de acceso es el componente que ofrece cobertura inalámbrica a todos los equipos conectados a la red. Por lo tanto el punto de acceso es el elemento fundamental que debe existir en una red inalámbrica, y su objetivo básico consiste en gestionar de manera centralizada la comunicación entre los dispositivos de la red.
  El punto de acceso consiste básicamente en un equipo de radio que dispone de una o varias antenas que se usan para transmitir y recibir información, con varios conectores de red RJ-45 que sirven de enlace físico a la red cableada. Los puertos RJ-45 se pueden usar para conectar la red inalámbrica a una red cableada o a Internet. Los puntos de acceso incorporan en su interior un switch, y a veces incluso incorporan puertos paralelos o USB para compartir impresoras sin necesidad de conectarlas a un ordenador. Un punto de acceso, al igual que un switch, incorpora una serie de LED que indican en cada momento la actividad del enlace.

  Los puntos de acceso suelen ofrecer múltiples servicios entre los que se muestran: DHCP, firewall, filtrado de direcciones MAC, cifrado WEP, cifrado WPA2, entre otros. Actualmente casi todos los puntos de acceso del mercado suelen incorporar un servidor web que permite configurar el punto de acceso de forma fácil y cómoda. Para configurar el punto de acceso debe abrir el navegador y escribir la dirección IP que tiene por defecto. Cabe mencionar aunque las estaciones de trabajo se conectan de forma inalámbrica, el Punto de Acceso se conecta al Sistema de Distribución por medio de cable de red.

  Los parámetros de configuración más importantes de un punto de acceso son:
  - Nombre de la red (SSID): es el nombre que identifica la red inalámbrica.

- Canal de trabajo: existen hasta 11 canales de funcionamiento y puede configurar el punto de acceso para que trabaje en un canal determinado o que lo seleccione de forma automática.
- Protocolo de cifrado: existen tres protocolos de cifrado: el WEP, WPA y el WPA2. Por su seguridad se aconseja utilizar el protocolo WPA2 ya que el protocolo WEP se puede vulnerar en pocos minutos.

En la imagen 3.16 se muestran varios Puntos de Acceso, algunos con una, dos o más antenas, esto se debe a las diferentes configuraciones MIMO (Múltiple entrada múltiple salida) los cuales permiten una cobertura mayor en zonas de difícil acceso eliminando en lo posible la pérdida de paquetes de datos vía inalámbrica, también nos proporciona mayor velocidad inalámbrica por usar varias antenas de forma simultánea, la tecnología MIMO tiene las configuraciones 3T3R (3 antenas para transmitir, 3 antenas para recibir) que permiten alcanzar velocidades de hasta 450 Mb/s teóricos y la configuración 2T2R (2 antenas para transmitir, 2 antenas para recibir) que permiten alcanzar 300 Mb/s teóricos.

Imagen 3. 16 Puntos de Acceso

Los paquetes de información en las redes 802.11 necesitan ser convertidos a otro tipo de paquetes para ser entregados a Internet, los dispositivos encargados de esta tarea de transformación de la información de la red inalámbrica a información que se transmite por redes cableadas son los Puntos de Acceso (AP), no sólo realizan esta función, sin embargo es la que se considera la más importante.

Un punto de acceso puede gestionar diferentes tipos de datos mediante operaciones como “puentear” (Conectar redes – Puente), retransmitir (Repetidor), distribuir (Concentrador), direccionar paquetes de información (*switching o ruteo*) o para adaptar los formatos de los paquetes de información para otras redes *(Gateway)*. Una característica más es que por ejemplo un conjunto de AP pueden dar la función de *roaming*, en donde los usuarios se conecten al punto de acceso más cercano para hacer uso de la red, y si el usuario se mueve a otra área de cobertura donde esté al alcance de otro AP, el dispositivo automáticamente se conecta al nuevo AP sin perder la comunicación.

Un punto de acceso puede soportar dos tipos de topología, la de punto-punto y la de punto-multipunto. En un sistema donde se tiene una configuración del AP como punto-punto son permitidas las comunicaciones entre punto de acceso a punto de acceso o a una

computadora directamente. En la otra disposición, los puntos de acceso son capaces de comunicarse con más de un cliente u otro punto de acceso.

- Tarjetas de red NIC (Network Interface Controller): Un adaptador de red inalámbrico es un componente de hardware que permite a un ordenador conectarse a una red inalámbrica o alámbrica. Existen en el mercado numerosos modelos de adaptadores de red inalámbricos que se diferencian dependiendo del bus de expansión que utilizan (PCMCIA, PCI, USB, entre otros) y la normativa 802.11 que utilizan (802.11b, 802.11g o 802.11n). El precio de los adaptadores depende dependen de la normativa que utilizan y del bus de conexión. Los adaptadores más baratos son aquellos que utilizan bus USB y PCI, y los más caros son aquellos que utilizan bus PCMCIA o SD, Respecto a la normativa, lógicamente los adaptadores más caros son aquellos que utilizan una normativa más rápida. Por ejemplo, los adaptadores 802.11g son más caros que los 802.11b.

  En la imagen 3.17 se pueden ver diferentes tipos de tarjetas de red. A continuación se van a analizar los diferentes adaptadores dependiendo del bus de expansión que utilizan:


Imagen 3. 17 Tarjetas de Red

  - Adaptadores PCMCIA. Suelen utilizarse sobre todo en los ordenadores portátiles, para expandir su funcionalidad en aspectos muy variados, como puede ser por ejemplo añadirles una tarjeta de red, un nuevo disco duro o más memoria. La conexión PCMCIA se ha aplicado a todo tipo de componentes del mercado, y por supuesto existen numerosos modelos de adaptadores de red inalámbricos disponibles en este formato.
  - Adaptadores PCI e ISA. Los dispositivos PCI (Peripheral Component Interconnect) son componentes hardware que se conectan directamente a la placa base del ordenador, por lo tanto es necesario abrir el equipo para instalar un adaptador inalámbrico PCI en el sistema. También hay tarjetas de red inalámbricas ISA, sin embargo este tipo de conectores no es tan eficiente como el PCI, ya que los dispositivos PCI se configuran automáticamente al arrancar el sistema y en los adaptadores ISA hay que configurar algunos parámetros, utilizando para ellos jumpers externos. Además, actualmente el bus ISA se está quedando obsoleto ya que no suele incorporar en las nuevas placas base.
  - Adaptador USB. El conector USB (Universal Serial Bus) se aplica actualmente a casi todos los dispositivos que pueden comunicarse con un ordenador, ya que se trata de un estándar que se ha extendido por todo el mundo y que garantiza la compatibilidad entre dispositivos que usan este tipo de conector. Las características de este tipo de dispositivos USB son muy parecidas a las de los

adaptadores inalámbricos PCMCIA, excepto el precio, ya que los adaptadores USB suelen ser bastante más económicos.

- Adaptadores para PDA. Puede encontrar en el mercado adaptadores de red inalámbricos SD que permiten conectar, por ejemplo una PDA a una red inalámbrica. Los adaptadores SD más usuales son los basados en IEEE 802.11b, que además disponen de encriptación WEP de 64/128-bit para proteger la información que se transmite durante la comunicación.
- Adaptadores COM y LPT. También puede encontrar en el mercado, adaptadores inalámbricos que se conectan al equipo a través del puerto serie (COM) o el puerto (LPT). Las prestaciones que ofrecen los adaptadores en este formato son muy parecidas a las que ofrecen las tarjetas de red, aunque su precio suele dispararse.
- Portátiles WIFI. Actualmente casi todos los ordenadores portátiles que se deben en el mercado incorporar de serie un adaptador de red inalámbrico para poder conectarse a una red WIFI, sin necesidad de añadir ningún dispositivo adicional. La incorporación de dichos adaptadores a los portátiles ha surgido como la consecuencia de la enorme repercusión social y tecnológica que ha supuesto la posibilidad de formar redes de ordenadores sin necesidad de crear para ellos una instalación cableada.
- Las tarjetas de red (NIC's) proveen la comunicación entre la computadora y la red inalámbrica. Las tarjetas de red se encuentran dentro de los dispositivos de los clientes, sin embargo existen adaptadores para poner tarjetas de red externas. El estándar 802.11 define cómo deben operar estas tarjetas de red, por ejemplo una tarjeta de red inalámbrica puede tener soporte para el protocolo IEEE 802.11b, en donde sólo funcionará para redes que tengan implementado ese protocolo.

  Una tarjeta de red es un transductor (envío y recepción) que convierte las señales de radiofrecuencia a señales digitales que pueden ser procesadas por las computadoras. Por medio de estas tarjetas de red inalámbricas los dispositivos acceden al AP que recibe y envía paquetes de información hacia otros dispositivos o hacia otras redes.

  Las tarjetas de red que son conectadas a los dispositivos como laptops requieren del software necesario para controlar el dispositivo y para comunicarlas con el sistema operativo. Parte de la configuración del software que controla la tarjeta de red, puede implicar realizar configuraciones como fijar el SSID de la red, la clave de cifrado WEP, o el canal que ocupará.

  Pueden ser conectados con cable o sin cable de red. Las velocidades de transmisión varían.

- Antenas: permiten ampliar la cobertura de una red inalámbrica, llegando a alcanzar distancias de incluso 20 Km. Existen muchos modelos en el mercado y además también se pueden fabricar de manera casera.

Aunque todos los dispositivos inalámbricos, tanto los puntos de acceso como los adaptadores de red, ya incorporan su antena propia, en muchas ocasiones es necesario ampliar el tamaño de la red para ofrecer una mayor cobertura.

Una clasificación básica de las antenas consiste en agruparlas, según su patrón de radiación, como omnidireccionales o direccionales. Las antenas omnidireccionales se utilizan para conexiones punto a multipunto y las direccionales para conexiones punto a punto. En la imagen 3.18 se muestran antenas omnidireccionales y direccionales.


Imagen 3. 18 Antenas

Un aspecto importante es que la ganancia de las antenas omnidireccionales es algo menor que la de las antenas direccionales.

Dentro de las antenas omnidireccionales y direccionales, puede encontrar otros tipos como lo que se muestra a continuación.

- Antena de sector. Son antenas direccionales que se utilizan para las conexiones punto a multipunto. Con este tipo de antenas se consigue mejorar la ganancia de las antenas omnidireccionales.
- Antena de panel. Con este tipo de antenas se consiguen conexiones punto a punto con una ganancia comparable a las antenas de sector.
- Antenas parabólicas. Estas antenas tienen una garantía muy elevada ya que son las más potentes que pueden adquirirse en el mercado.
- Antena yagui. Son antenas direccionales con forma de tubo y con una buena ganancia.
- Antena omnidireccional. Son antenas que tienen poca potencia, por lo que están indicadas para comunicar dispositivos cercanos.
- Antenas caseras. Aunque parezca un trabajo artesanal, para construir este tipo de dispositivos es necesario no solo disponer de los conocimientos técnicos apropiados, sino también cumplir la regulación de emisiones electromagnéticas, es decir emitir y recibir señales en la banda de frecuencia correcta para evitar interferencias con otros dispositivos, pues este sería ilegal.

  Algunas de estas antenas caseras no tienen mucha ganancia, unos 4dB, en cambio otros ofrecen una ganancia de hasta 20dB, con lo cual si se construyen adecuadamente pueden ofrecer unas prestaciones similares a las antenas comerciales, que suelen ofrecer una ganancia en torno a los 20dB.

Uno de los elementos más importantes de las redes inalámbricas son las antenas, ya que se encargan de hacer la transformación de las señales electromagnéticas en señales eléctricas y viceversa. Existen de dos tipos, las antenas direccionales y omnidireccionales reciben y envían señales desde cualquier dirección del espacio en donde se encuentra.

Los diferentes tipos de antenas tienen diferentes coberturas de área en dirección horizontal y vertical, por ejemplo las antenas omnidireccionales tienen una cobertura horizontal de 360° y de manera vertical de 7° a 80° de cobertura.

Dentro de las antenas omnidireccionales podemos encontrar dos tipos de antenas que tienen patrones de radiación basándose en las omnidireccionales, las antenas multitrayectoria que son como su nombre lo dice, irradian señales en todas direcciones; por otro lado existen las antenas semidireccionales que son las que irradian señales a media trayectoria. Una antena de este tipo puede tener al menos el doble de alcance que una antena de tipo omnidireccional. De manera efectiva una antena semidireccional puede tener un aumento de 10 veces la amplitud de la señal.

Las antenas direccionales tienen una cobertura muy estrecha pero con un alcance de cobertura muy largo. Para alcanzar este grado de direccionalidad, se necesita usar antenas de plato que enfocan la emisión de las ondas de radio mayoritariamente en una sola dirección, este tipo de antenas son caras comparadas con las antenas omnidireccionales.

### 3.1.6. Aplicaciones de las Redes de Área Local Inalámbricas

A continuación se describen tres áreas principales de aplicación:

1) Ampliación: Los primeros productos de LAN inalámbricas, aparecidos a finales de los años ochenta, eran ofrecidos como sustitutos de las Redes de Área Local cableadas tradicionales. “Una red LAN inalámbrica evita el coste de la instalación del cableado y facilita las tareas de traslado y otras modificaciones en la estructura de la red. Sin embargo, esta motivación de las LAN inalámbricas fue superada por los acontecimientos. En primer lugar, a medida de que las Redes de Área Local se hizo cada vez más necesaria, los arquitectos incluyeron en el diseño de los nuevos edificios un extenso cableado para aplicaciones de datos.”[1] Además, con los avances en la tecnología de transmisión de datos se ha incrementado la dependencia con los pares trenzados para las Redes de área Local, especialmente con los *UTP* de categoría 5e y 6. Así, dado que la mayor parte de los edificios viejos estaban ya cableados con par trenzado de categoría 5, resulta escaso el uso de LAN inalámbricas como sustituto de las LAN cableadas. Sin embargo el papel de una LAN inalámbrica como alternativa a las LAN cableadas es importante en un gran número de entornos.

[1]Julio Gómez López, “Guía de Campo Wi-Fi” RA-MA 2008 Pag. 559

Algunos ejemplos son edificios que poseen una gran superficie, como plantas de fabricación, plantas comerciales y almacenes, edificios históricos con insuficiente cable de par trenzado y en los que está prohibido hacer más agujeros para introducir nuevo cableado, y en pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan rentables. En todos estos casos, una Red de Área Local inalámbrica ofrece una alternativa efectiva y más atractiva. En la mayor parte de estas situaciones, una organización dispondrá también de una LAN cableada con servidores y algunas estaciones de trabajo estacionarias. Por ejemplo, una planta de manufacturación dispone, generalmente, de una oficina independiente de la propia planta, pero que debe estar interconectada con ella con el fin de proporcionar trabajo en red. Por tanto, una LAN inalámbrica está conectada en muchas ocasiones con una LAN cableada en el mismo recinto, denominándose este campo de aplicación ampliación o extensión de Redes de Área Local.

2) Interconexión de edificios: Otra aplicación de las LAN de tecnología inalámbrica es la conexión de Redes de Área Local situadas en edificios vecinos ya sean cableadas o inalámbricas. En este caso se usa un enlace punto a punto inalámbrico entre los dos edificios. Los dispositivos así conectados son, generalmente, puentes o dispositivos de encaminamiento. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de esta aplicación en el contexto de redes LAN inalámbricas.
3) Acceso nómada: El acceso nómada proporciona un enlace inalámbrico entre un concentrador de una LAN y un terminal de datos móvil equipado con una antena, como un computador portátil. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de un viaje la transferencia de datos desde un computador personal portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio, como un campus o un centro financiero situado lejos de un grupo de edificios. En ambos casos, los usuarios se pueden desplazar con sus computadores portátiles y pueden conectarse con los servidores de una LAN inalámbrica desde distintos lugares.

### 3.1.7. Requisitos de las redes inalámbricas

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total entre las estaciones pertenecientes a la red y capacidad de difusión. Además de las mencionadas existe un conjunto de necesidades específicas para entornos de LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- Rendimiento: el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio inalámbrico para maximizar la capacidad.
- Número de nodos: las LAN inalámbricas pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas.

- Conexión a la LAN troncal: en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbricas con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que conectan con ambos tipos de LAN. Puede ser también necesario dar soporte a usuarios móviles y redes inalámbricas *ad-hoc.*
- Área de servicio: Una zona de cobertura para una red LAN inalámbrica tiene un diámetro de entre 100 y 300 metros.
- Consumo de energía: los usuarios móviles utilizan estaciones de trabajo con batería que necesitan tener una larga vida cuando se usan con adaptadores sin cable. Las implementaciones típicas de LAN inalámbricas poseen características propias para reducir el consumo de potencia mientras no se esté usando la red, como un nodo de descanso *(sleep mode)*.
- Robustez en la transmisión y seguridad: a menos de que exista un diseño apropiado, una LAN inalámbrica puede ser propensa a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- Funcionamiento de redes adyacentes: a medida que las LAN inalámbricas se están haciendo más populares, es probable que dos o más de estas redes operen en la misma zona o alguna en la que sea posible la interferencia entre ellas. Estas interferencias pueden recurrir negativamente en el funcionamiento normal del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.
- Traspasos (*Handoff*) / Itinerancia (*Roaming*): el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.
- Configuración dinámica: los aspectos de direccionamiento MAC y gestión de la red LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

### 3.1.8. Ventajas de las redes inalámbricas

El uso de las redes inalámbricas es hoy en día una alternativa con la que se cuenta, en organizaciones de todo tipo, para poder ser competitivos. A pesar de presentar algunos inconvenientes, en este reporte se hace énfasis en que el uso de esta tecnología ofrece una gran cantidad de ventajas que repercuten en la economía, eficiencia, imagen y competitividad de quienes la implementan. Las ventajas de las redes inalámbricas con respecto a las redes cableadas son:

- Cableado más económico. La instalación de una infraestructura completa de cableado representa una fuerte inversión, el número de conexiones previsto implica, en la mayoría de los casos, el triple de estaciones instaladas al principio a fin de simplificar las extensiones y cambios futuros. Las redes de área local inalámbricas existentes, en realidad necesitan algunos cables, sobre todo entre la salida de la computadora y un dispositivo de transmisión.

- Instalación simplificada. Entre menos cableado se realice la instalación se hará de manera más rápida. Si la red solo consta de una docena de estaciones, agrupadas en un radio de unos 20 metros, el alcance puede realizarse por radio en su totalidad. Un día es suficiente para instalar las tarjetas de comunicación y realizar las pruebas de transmisión. De igual forma, en caso de que se requiera alguna modificación, también será una tarea fácil.
- Escalabilidad. Permite expandir la red con efectividad en costos, al instalar tarjetas de red inalámbricas en computadoras adicionales e impresoras que tengan tarjetas de red inalámbrica.
- Facilidad de uso. Si el usuario planea conectar múltiples puntos de acceso a una red cableada existente, debe considerar una solución que ofrezca conexiones automáticas a la red. Como resultado, los usuarios podrán movilizarse libremente dentro de sus instalaciones y más allá, permitiéndoles seguir conectados a la red.
- Servidor Web. Para una administración más fácil. El administrador de la red podrá habilitar el uso de configuración por medio del servidor Web si es que el punto de acceso tiene esta opción. Esto le permite acceder y definir los parámetros de configuración, monitorear el rendimiento y hacer diagnósticos desde un navegador Web.
- Seguridad. Se puede incrementar la seguridad incluyendo encriptación y autenticación de usuarios.
- Facilidad de configuración para el usuario. La persona que se va a conectar a la red sólo tiene que escribir la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está abierta no será necesario configurar, pues la tarjeta de red inalámbrica detecta la red automáticamente.
- Esta flexibilidad de instalación se opone a la ardua instalación del cableado clásico: redacción de un manual que precise la posición de cada una de las conexiones, consultas a las compañías, sin olvidar que la tarea requiere de dos a tres meses para concluirse y que incomoda a gran medida a los ocupantes de los locales. En lo sucesivo si las redes de área local inalámbricas permiten reducir el tiempo de instalación en algunas semanas sin incrementar los costos, el éxito está asegurado.

### 3.1.9. Desventajas de las redes inalámbricas

Los inconvenientes o desventajas que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un período transitorio de introducción, donde faltan estándares que permitan transmisiones más rápidas, por otro lado hay dudas de que algunos sistemas puedan llegar a afectar a la salud de los usuarios, sin embargo, se ha estado trabajando en ello, logrando hasta el momento un gran avance que ha permitido la implementación cada vez más de este tipo de comunicación. Algunas de las desventajas que se derivan por la implementación de redes inalámbricas con respecto a las redes cableadas, son las que se mencionan a continuación:

- Interferencias. Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, también pueden ser por redes inalámbricas cercanas.

- Velocidad. Las redes cableadas alcanzan la velocidad de 1000Mb/s, mientras que las redes inalámbricas alcanzan cuando mucho 54 Mb/s.
- Seguridad. En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire.
- Calidad de la transmisión ligada a la distancia entre los emisores y receptores. Las pruebas efectuadas al momento de la instalación permiten establecer los límites del área de cobertura. La estructura del edificio, la naturaleza de los tabiques o el acondicionamiento de los espacios influyen en el radio de acción. En los espacios libres, como se sabe, predomina el uso de los tabiques metálicos. Los riesgos de interferencia entre las celdas, por lo general se eliminan por medio de canales de diferentes frecuencias.
- Reglamentación. Los contratiempos técnicos no son el único obstáculo en el desarrollo de las redes inalámbricas. También es necesario considerar la aglomeración del espectro de frecuencias. La regulación puede ser demasiado restrictiva según el país en que usted se encuentre en cuyo caso no está permitido construir verdaderas redes de área local inalámbricas.
- Sin embargo, el verdadero obstáculo en las redes inalámbricas es el desempeño, el cual por lo general se considera bajo en relación con el de las redes cableadas. Además, se debe vigilar la distribución inteligente de las estaciones de trabajo en la arquitectura a fin de no sobrecargar algunas celdas de radio.

### 3.1.10. Algunas vulnerabilidades de las redes inalámbricas

Las comunicaciones inalámbricas tienen un inconveniente adicional: carecen de barreras físicas. Por tanto, cualquier persona, con conocimientos sobre seguridad y con una tarjeta de *Wi-Fi* instalada en su ordenador puede, potencialmente, acceder a un punto de acceso de una red inalámbrica (siempre que se encuentre en su área de cobertura). No obstante, fundamentalmente, lo que hace esto sea cierto es que muy pocos usuarios se toman en serio las medidas de seguridad. Por ejemplo, suele ser común que un usuario instale una red WI-Fi sin modificar la configuración que trae el sistema por defecto. Si un intruso desea entrar en un sistema, lo primero que comprobará es si todavía tiene la configuración inicial.

Desde un punto de vista técnico, las redes Wi-Fi incorporan unos sistemas de seguridad suficientes como para poder garantizar la confidencialidad, integridad y autenticidad de toda la información. El inconveniente es que estos sistemas no funcionan si sus usuarios no los utilizan. Por tato, el punto débil de la seguridad Wi-Fi son sus usuarios. Las redes Wi-Fi requieren una autenticación en materia de seguridad algo mayor que las redes cableadas y muchos de sus usuarios no son todavía conscientes de ello.

#### *3.1.10.1. Riesgos*

La seguridad es un riesgo tanto para las redes inalámbricas como para las cableadas. Hasta la fecha, todas las tecnologías informáticas que han ido apareciendo en el mercado (desde el

ordenador personal hasta las redes de cualquier tipo) han sido susceptibles, de una u otra forma, de ser violadas en la integridad, confidencialidad o autenticidad de los datos que contiene.

Ciertamente, a diferencia de las redes cableadas, las redes inalámbricas emiten señales que pueden ser fácilmente recogidas en el exterior del recinto vigilado de la red (la oficina o el hogar particular). Desde ese punto de vista, las redes inalámbricas tienen un riesgo añadido. Pero este riesgo es controlable. De la misma forma que es controlable el riesgo que tiene una red cableada de que un usuario remoto y desconocido pueda entrar en ella a través de su conexión a Internet. El riesgo siempre es mayor cuantas menos medidas se tomen para atajarlo.

Las cuatro categorías de riesgos que preocupan en el uso de cualquier tecnología de red son las siguientes:

1) Pérdida del equipo: Es sorprendente la cantidad de información que se puede llegar a almacenar en un ordenador, información no sólo profesional, sino, incluso, personal: el listado de clientes, las cuentas de la empresa, las descripciones de productos, la correspondencia con proveedores y clientes, la agenda de direcciones y teléfonos, números de tarjetas de crédito o las fotos de las últimas vacaciones. Perder un ordenador puede convertirse en un gran problema si cae en las manos equivocadas. No obstante, aparte del problema que supone el exponer determinada información a ojos indiscretos, existe un problema adicional y es que dicho ordenador podría ser utilizado para acceder a la red de la propia empresa. Este problema existe tanto si el ordenador está conectado a una red cableada como si lo hace a una red inalámbrica.
   Si la red es cableada y dispone de acceso remoto, cualquiera podría acceder desde cualquier parte del mundo vía Internet (si tiene las claves grabadas). En este caso, este riesgo puede eliminarse fácilmente deshabilitando las cuentas de acceso del usuario en cuestión. Si la red es inalámbrica, el acceso se tendría que hacer necesariamente desde una zona de cobertura. En este caso, pueden cambiarse también todos los códigos de acceso. No obstante, es cierto que, administrativamente, es mucho más sencillo eliminar una cuenta de acceso de una red cableada que cambiar manualmente las configuraciones de acceso de todos los usuarios de la red inalámbrica. Sin embargo, también es cierto que, a menos que exista algún tipo de etiqueta identificativa, la persona que consiga dicho equipo no dispondrá de ninguna pista para saber dónde se encuentra la red inalámbrica a la que se accede desde el equipo.
2) Infección de un virus: Los virus son pequeños programas informativos que se instalan en el ordenador para causarle algún tipo de daño directo o utilizarlo como plataforma para conseguir otros objetivos. Los virus afectan tanto a redes cableadas como inalámbricas. Hasta la fecha no existe ningún virus que sea específico de redes inalámbricas.
   Esto quiere decir que las medidas antivirus son idénticas, independientemente del tipo de red al que se encuentre conectado el ordenador: mantener el programa antivirus actualizado y disponer de un cortafuegos (firewall).
3) Mal uso por personas autorizadas: El que personas autorizadas hagan un mal uso del sistema (intencionado o accidental) es una amenaza de la que resulta difícil protegerse.

Una vez que el usuario ha pasado todos los niveles de seguridad y se encuentra dentro del sistema, es complicado controlar en detalle el uso que cada usuario hace de él.

Ciertamente, existen historias de empleados que han robado información de su empresa, borrando archivos, modificando información sensible o hecho cualquier otro uso malintencionado de la información, pero, existen todavía más historias de empleados que de una forma no intencionada producen el mismo daño compartiendo sus claves de acceso abiertamente, introduciendo datos equivocados, imprimiendo en la impresora equivocada, enviando un correo con información confidencial a personas equivocadas o copiando datos confidenciales a su disco duro o flexible sin las medidas de seguridad adecuadas.

Como se puede ver, estos riesgos son equivalentes tanto para las redes cableadas como para las inalámbricas. El único sistema que existe para protegerse de este riesgo es implementar una política de seguridad adecuada en la empresa.

4) Uso fraudulento por personas no autorizadas: Si hay un punto en el que las redes inalámbricas Wi-Fi tienen desventaja frente a las redes cableadas, es el riesgo por uso fraudulento por personas no autorizadas. La desventaja viene por lo que es su ventaja fundamental: cualquier usuario puede conectarse a la red desde cualquier sitio sin necesidad de conectarse físicamente a ningún medio. Los usos fraudulentos pueden venir por cualquiera de los siguientes caminos como se muestra en la imagen 3.19:

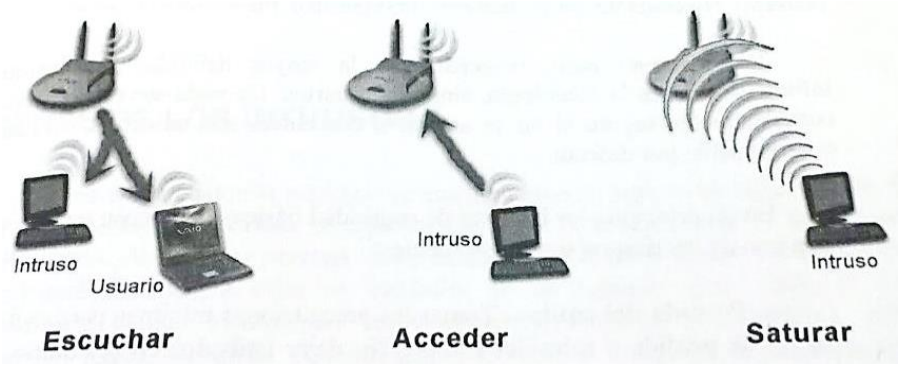


Imagen 3. 19 Usos fraudulentos de las redes inalámbricas

- Escuchar: con un receptor adecuado, los datos emitidos por un usuario pueden ser recogidos por terceras personas. De hecho, existen programas como Airopeek, Airsnort, NetStrumbler o Webcrack que facilitan esta labor. Estos programas descubren datos como el SSID, la dirección MAC o si el sistema WEP está o no habilitado.
- Acceder: se trata de configurar un dispositivo para acceder a una red para la que no se tiene autorización. Esto se puede hacer de dos formas: configurando un ordenador para que acceda a un punto de acceso existente o instalando un nuevo punto de acceso y, a través de él, conectar fraudulentamente todos los ordenadores externos que se deseen.

- Saturar: en este caso no se trata de intentar acceder fraudulentamente a una red, sino de dejarla fuera de servicio. El resultado es que la red no puede ser utilizada por sus propios usuarios, por lo que es un ataque a la seguridad. Para dejar inhabilitada una red inalámbrica, bastará simplemente con saturar el medio radioelectrónico con el suficiente ruido como para que sea imposible llevar a cabo cualquier comunicación. A este tipo de ataques se le conoce también como negación del servicio, *DOS (Denial of Service) o jamming (literalmente "atasco").*

### 3.1.11. Cifrado WEP

Es el sistema de cifrado incluido en el estándar *IEEE* 802.11 como un protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits o de 128 bits.

Su historia del cifrado WEP se remonta cuando apareció la tecnología inalámbrica WI-Fi, el único sistema de seguridad que incluía era el cifrado *WEP (Wired Equivalency Protocol "protocolo de equivalencia con red cableada")*. Este sistema cifra todos los datos que se intercambian entre los usuarios y el punto de acceso utilizado en el algoritmo de cifrado RC4.

*RC4* fue diseñado en 1987 por Ron Rivest de la empresa RSA Segurity. El nombre *RC4* es un acrónimo de *Rivest Cipher 4*, aunque también se dice que su significado es el *Ron's Code 4*.

Este algoritmo RC4 se basa en generar una clave de forma pseudoaleatoria (conocida como *keystream*) que tiene la misma longitud que el texto original. A esta clave y al texto original se le aplica la operación lógica *XOR (OR exclusiva)*, dado como resultado un texto cifrado.

En el caso WEP, la clave pseudoaleatoria se genera utilizando la clave secreta que define el propio usuario y un vector de inicialización *(IV, Initialization Vector)* que lo genera aleatoriamente el sistema para cada trama (bueno, ésta es la teoría, la realidad es que no se cambia). La clave secreta se concatena con el IV creado lo que se conoce como semilla (*seed*), a partir de la cual se genera la clave pseudoaleatoria de la longitud deseada utilizando el algoritmo *PRNG (Pseudorandom Number Generation, "Generación de números pseudoaleatorios")*.

Para garantizar la integridad del texto original se envía junto con lo que se conoce como *ICV (Integrity Check Value, valor de comprobación de integridad)*. Se trata de 32 bits de comprobación de integridad que se calcula con el algoritmo *CRC-32 (Cyclic Redundacncy Chek o Codigo de redundancia cíclica de 32 bits)*.

Por tanto, en el caso de WEP, la operación XOR se realiza entre la clave pseudoaleatoria y el texto original con su ICV. El resultado es el texto cifrado que se emite finalmente junto con el valor IV sin cifrar.

El receptor recibe el texto cifrado y el valor IV. Como el receptor conoce la clave, al disponer del valor IV puede generar la semilla con la que se crea la clave pseudoaleatoria. Al aplicarle la

operación XOR a esta clave y al texto cifrado se obtiene el texto original y el valor *ICV* generado en origen. Para comprobar la integridad de este texto se le calcula localmente el valor *ICV* y se comprueba con el *ICV* generado en origen. Si no coincide indica que el texto ha sido modificado por el camino.

Las debilidades de WEP: A continuación se hace mención de cuatro tipos de ataques posibles contra WEP:

1. El primero hacía posible descifrar un mensaje basado en la fragilidad del *IV* (*vector de inicialización de sólo 24 bits)* y en la utilización de códigos estáticos.
2. El segundo ataque posibilitaría crear mensajes utilizando los mensajes existentes.
3. El tercer ataque permitiría descifrar la información contenida en las cabeceras de los paquetes. Con esto se podrían reenviar los paquetes a otra estación para descifrar allí su contenido.
4. El último ataque permitiría crear una tabla de *IV (vectores de inicialización)* y claves permitiendo descifrar fácilmente todos los mensajes interceptados.

*WECA (la asociación de fabricantes de productos y servicios inalámbricos que certifica los equipos WI-Fi)* siempre ha respondido a estos informes diciendo que los ataques descritos siempre utilizan sistemas sofisticados que necesitan un esfuerzo y tiempo considerable para llevarlos a cabo. Manifiesta que WEP sigue siendo un sistema suficientemente seguro como para estar protegidos de la inmensa mayoría de los posibles intrusos. Por otro lado, WEP nunca fue diseñado para ser un sistema de seguridad total.

En cualquier caso, tanto *WECA* como *IEEE* han trabajado para ofrecer una alternativa a WEP que ofrezca unos mayores niveles de seguridad. Los resultados han sido WPA y WPA2 *(IEEE 802.11i).*

### 3.1.12. Cifrado WPA

Es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP. Se han encontrado varias debilidades en el algoritmo WEP, como la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros. Nació para corregir las deficiencias de seguridad de WEP. Implementa el estándar 802.11i.

Dadas las debilidades evidentes de WEP, había que hacer algo para resolver el problema. La solución ideal era que el IEEE emitiera un nuevo estándar complementario a 802.11b/g/a que definiera unos nuevos mecanismos de seguridad completamente fiables. Sin embargo, definir un estándar con todas sus garantías lleva su tiempo, y la alianza WI-FI, WECA, veía que este problema tenía que resolverse en breve. Hay que tener en cuenta que WEP es de 1999 y que sus principales debilidades se descubrieron en 2001.

Cuando el IEEE se puso a trabajar en su nueva recomendación, la 802.11i, se dio cuenta que no iba a ser compatible con el hardware existente. Este hecho, junto con la urgencia en tener una

alternativa fiable a WEP, llevó a WECA a emitir su protocolo *WPA (Wi-Fi Protected Access, "Acceso Wi-Fi protegido")*. Posteriormente, el IEEE publicaría el estándar 802.11i, al que WECA bautizaría con el nombre de WPA2. Por tanto tenemos dos protocolos WPA:

- WPA. Publicado por WECA a principios de 2003 y que tiene la ventaja de ser compatible con el hardware existente (actualizando su firmware).
- WPA2 o 802.11i. Publicado por IEEE en junio de 2004. Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser más seguro. Este estándar también conoce como RSN (Robust Security Network, "Red de seguridad robusta").

WPA es un subconjunto de 802.11i. Incorpora las características *TKIP (Temporal Key Integrity Protocol, "Protocolo de integridad de clave temporal")* y 802.1x, mientras que deja fuera otras como la desautenticación segura, la desasociación, IBSS segura, cambio seguro de puntos de acceso, así como protocolos mejorados de cifrado como AES. Algunas de estas características (no incluidas en WPA) requieren cambios en el hardware de los equipos Wi-Fi anteriores. Por el contrario, todas las características que incluye WPA pueden ser actualizadas en los equipos anteriores mediante una actualización del firmware.

TKIP ofrece características tan interesantes como:

- Incluye cuatro nuevos algoritmos para mejorar la seguridad
- Utiliza IV más largas
- Impide la reutilización de claves estáticas
- Hace uso de claves de sesión para facilitar el cambio frecuente de las claves criptográficas.
- Permite la construcción de claves por paquete
- Ofrece la integridad criptográfica
- Ofrece derivación y distribución de claves

El estándar 802.1x, aprobado en junio de 2001, incluye un nuevo protocolo de seguridad conocido como *EAP (Extensible Authentication Protocol, "Protocolo extensible de autenticación").* Este protocolo se utiliza para controlar el acceso de los usuarios a los puntos de acceso y autenticar sus comunicaciones. 802.1x está siendo cada vez más aceptado por la industria. De hecho, tanto los sistemas operativos como los fabricantes de puntos de acceso ya lo incorporan.

En definitiva, WPA ofrece soluciones para las principales deficiencias de WEP; mejora el cifrado de datos mediante TKIP, utiliza claves dinámicas (con WEP son estáticas) y permite la distribución automática de las claves (con WEP es manual), así mismo proporciona una autentificación fuerte (según lo aconsejado por el estándar 802.1x).

En cuanto a WPA2, la principal diferencia con los sistemas de cifrado anteriores es que utiliza el cifrado de bloques AES (Advanced Encryption Standard, "Estandar de cifrado avanzado"), WEP y WPA utilizan el sistema de cifrado de flujo *RC4*.

Los componentes principales de la arquitectura 802.11i son los siguientes:

- Define la autenticación utilizado EAP y servidores de autenticación.
- Utiliza RSN para mantener un registro un registro de asociaciones
- Utiliza CCMP basado en AES para garantizar la confidencialidad, integridad y autentificación del origen. AES soporta claves de 128, 192 y 256 bits.
- Utiliza un proceso de negociación a cuatro bandas para la autenticación

### 3.1.13. Cifrado WPA2

Sistema de cifrado creado a partir del WPA, que corrige vulnerabilidades del anterior. WPA y WPA2 se diferencian poco conceptualmente y difieren principalmente en el algoritmo que emplean. Mientras WPA basa el cifrado de las comunicaciones en el uso del algoritmo *TKIP (Temporary Key Integrity Protocol)*, que está basado en RC4 al igual que WEP, WPA2 utiliza *CCMP (Counter-mode/CBC-MAC Protocol)*, basado en *AES (Advanced Encryption System)*.

La segunda diferencia notable se encuentra en el algoritmo utilizado para controlar la integridad del mensaje. Mientras WPA usa una versión menos elaborada para la generación del código *MIC (Message Integrity Code)* o código "Michael", WPA2 implementa una versión mejorada de MIC.

Una vez finalizado el estándar 802.11ie se crea el WPA2 basado en éste. WPA se podría considerar de migración, mientras que WPA2 es la versión certificada del estándar de la IEEE. El estándar 802.11i fue ratificado en junio de 2004.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de acceso apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA – FIPS140-2. "WPA2 está idealmente pensado tanto para empresas del sector privado como del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI (Tecnologías de la Información) la seguridad de que la tecnología cumple con estándares de inter-operatividad", declaró Frank Hazlik Managing, Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES, es importante resaltar que los productos certificados para WPA siguen siendo seguros, de acuerdo a lo establecido en el estándar 802.11i.

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en las redes WLAN. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

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

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

Características y funcionamiento: El estándar WPA2 tiene la función principal del protocolo 802.1x que es encapsular los protocolos de autenticación, sobre los protocolos de la capa de enlace de datos (capa 2 del modelo OSI) que describe el modo de autenticación basado en EAP (Extensible Authentication Protocol) el cual se aprecia en la imagen 3.20.

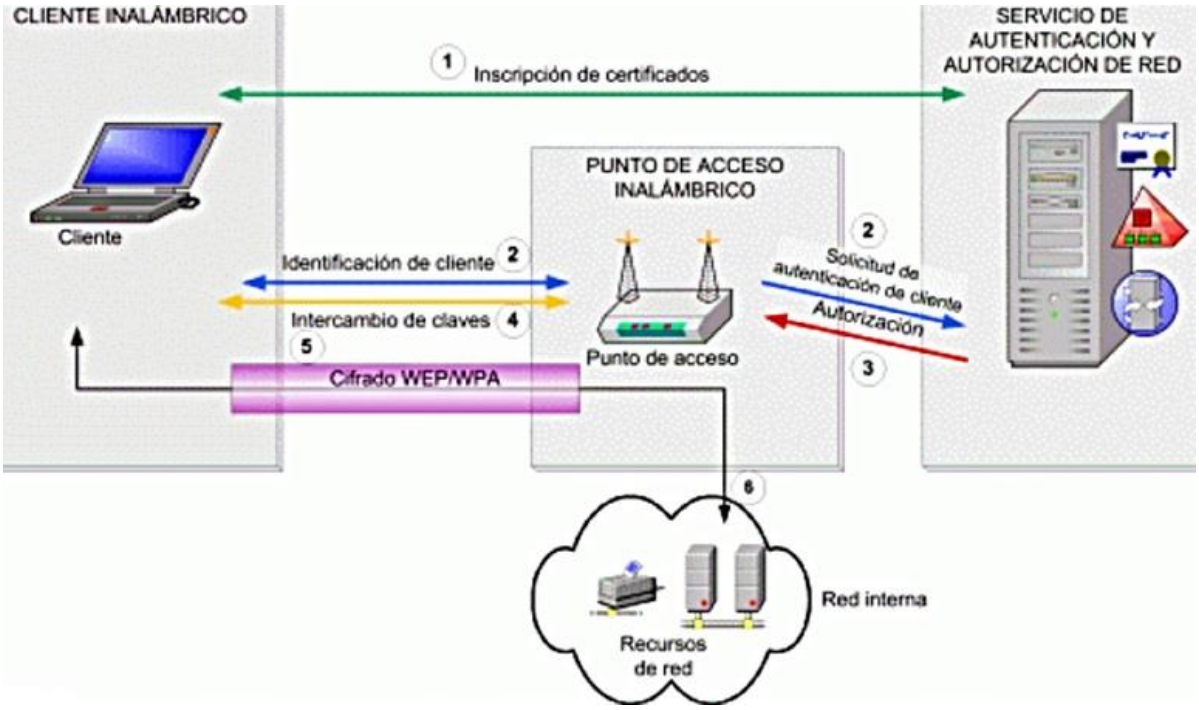


Imagen 3. 20 Proceso de un EAP

Define tres elementos:

1. Solicitante o suplicante: es el elemento que solicita la autenticación. Generalmente el Cliente.
2. Autenticador: elemento al que se conectará el suplicante. Pasa la información al servidor de autenticación, generalmente el Punto de Acceso.
3. Servidor de autenticación: elemento que evalúa la autenticación del suplicante enviando una respuesta al autenticador.

EAP es una estructura de soporte, no un mecanismo específico de autenticación. Puede transportar diferentes protocolos de autenticación: TLS (Transport Layer Security), TTLS (Tunnel Transport Layer Security), ND5 (Message Digest 5), PEAP (Protected EAP), LEAP (Lightweight EAP).

EAP-TLS está basado en el uso de certificados digitales X.509 para autenticación del cliente y del servidor. En el protocolo TTLS, sólo se autentica el cliente. El mayor inconveniente de EAP-TLS es

que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número de clientes puede ser costosa y difícil. Por este motivo se creó PEAP y EAP que sólo requieren certificados en el servidor.

EAP-TTLS añade a las características de seguridad de EAP-TLS un canal de comunicación seguro para intercambiar credenciales con el usuario, incrementando la seguridad contra ataques de Sniffing. Por otro lado, elimina la necesidad de contar con certificados en todos los clientes.

Definición de los tipos de mensajes de intercambio:

- Request: petición desde el Punto de Acceso al cliente
- Resposnse: mensaje del cliente al Punto de Acceso
- Success: autorización del acceso
- Failure: denegación del acceso

El transporte de los mensajes se realiza a través del protocolo EAPoL (EAP over LAN), protocolo desarrollado para entornos Ethernet. En dicho protocolo se pueden encontrar cinco tipos de mensajes:

- Start: el cliente envía, a la dirección MAC multicast, a la espera de que el Punto de Acceso responda
- Key: una vez obteniendo el acceso, el AP usa este mensaje para enviar las claves al cliente
- Packet: los mensajes EAP que son transmitidos se encapsulan en este mensaje EAPoL
- Logoff: Mensaje de desconexión enviado por el cliente

El funcionamiento estándar de 802.11x se enfoca en la denegación de todo tráfico que no sea hacia el servidor de autenticación, hasta que el cliente no se haya autenticado. El autenticador crea un puerto por el cliente creando 2 posibilidades: uno autorizado, el otro no, este último lo mantiene cerrado hasta que el servidor de autenticación le comunique que el cliente acceso.

Cuando el solicitante pasa a estar activo, selecciona y se asocia a un AP, el autenticador (que está en el AP) al detectar la asociación del cliente le habilita un puerto permitiendo sólo tráfico 802.1x, el resto lo bloquea.

El cliente envía un mensaje “EAP Start”, el autenticador responde con mensaje “EAP Request Identity” para obtener la identidad del cliente, la respuesta del solicitante “EAP Response” contiene su identificador y es retransmitido por el autenticador hacia el servidor de autenticación. A partir de este momento el solicitante y el servidor de autenticación se comunicarán directamente.

Modos de funcionamiento de WPA2. WPA2 tiene dos modos de funcionamiento:

1. WPA2-ENTERPRISE: basado en el protocolo 802.1x explicado anteriormente, que utiliza los tres elementos ya descritos (suplicante, autenticador, servidor de autenticación).

2. WPA2-PSK (Pre-Share Key): pensado para entornos personales, evita el uso de dispositivos externos de autenticación. Se han descrito ataques off-line contra los mismos basados en ataques de diccionarios o contraseñas débiles.

Tanto el servidor de autenticación como el suplicante generan dos claves aleatorias denominadas PMK (Pairwise Master Key) durante la fase de autorización y autenticación de 802.1x. Una vez finalizada la fase de autenticación, el servidor de autenticación y el cliente tienen PMK idénticas, pero el AP no, por lo tanto a través del uso RADIUS copia la clave del servidor de autenticación al AP. El protocolo no especifica el método de envío de la clave entre ambos dispositivos.

Llegados hasta este punto aún no se permite la comunicación si no que deben generar nuevas claves, en función de la PMK, para ser usadas en relación al cifrado y a la integridad, formando un grupo de cuatro claves llamado PTK (Pairwise Transient Key) con una longitud de 512 bits.

Para asegurar el tráfico broadcast, se crean claves de grupos de 256 bits llamadas GMK (Group Master Key) usado para crear la GEK (Group Encryption Key) y la GIK (Group Integrity Key) de 128 bits de longitud cada una. Las cuatro claves forman GTK (Group Transent Key).

La última parte es demostrar que el AP tiene PMK idéntico, para ello lo valida el servidor de autenticación.

Este proceso se realiza cada vez que es asociado un cliente con AP.

Vulnerabilidades: Aunque se han descubierto algunas pequeñas debilidades en WPA/WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2.

Ya se ha comentado del proceso de asociación de un cliente a una red Wireless; si el AP está emitiendo *Beacon Frames*, el proceso se realiza en dos fases, una de autenticación que podrá ser abierta o con la clave compartida y una segunda fase de asociación. En el supuesto caso de que el AP no esté emitiendo "*Beacon Frames"* existe una Fase de Prueba inicial donde el cliente envía el ESSID de la red Wireless a la que quiere conectarse, esperando que el AP responda y así iniciar las fases de Autenticación y Asociación.

Pues bien, conociendo todo el proceso o modo de funcionamiento que realiza WPA2 y el intercambio de números aleatorios que llevan a cabo entre un cliente y el AP para la autenticación y asociación, un atacante que quiera vulnerar una red WPA2-PSK va a tratar de capturar ese intercambio de números, para que una vez conocidos éstos, junto con el SSID, las direcciones MAC del cliente y el AP de la red, obtener la frase o secreto compartido que se utilizó. Una vez que el atacante tenga la clave compartida se podrá conectar a la red.

### 3.1.14. Seguridad en las redes inalámbricas

Un intruso es cualquier persona que entra en nuestro espacio sin autorización. En el caso de las redes inalámbricas, el espacio a proteger es la utilización de los equipos de red. Por tanto, cuando una persona ajena se conecta a nuestro equipo de red (punto de acceso) está llevando a cabo una intrusión en un espacio ajeno (esto es lo que anteriormente hemos identificado como acceder). También se considera intrusión cuando, sin establecer dicha comunicación, escucha e interpreta la información que intercambian los usuarios (escuchar). Así como, cuando, sin acceder ni escuchar, impide el uso normal de la red (saturar).

De estas tres formas de intrusión (acceso, escucha y saturación), las dos primeras se pueden evitar, simplemente, cifrando las comunicaciones. Aunque se pueden tomar también otra serie de medidas adicionales que refuerzan la protección. El conjunto de medidas disponibles son las siguientes:

- Utilizar una clave WEP, WPA oWPA2
- Utilizar un filtro MAC
- No publicar la identificación SSID
- No habilitar DHCP
- Utilizar un firewall

Por último para reforzar la importancia de adoptar medidas de seguridad se recomienda que:

- Nunca decirle a nadie la clave y, en el caso de las empresas, asegurarse que todos los trabajadores sigan esta regla.
- Evitar en lo posible el uso de claves estáticas. Las claves hay que modificarlas periódicamente, aunque sea una molestia.

### 3.1.15. Consejos de seguridad

a) Utilizar un filtro MAC: Como se ha visto, las siglas MAC (Media Access Control, “control de acceso al medio”) pueden hacer referencia a dos cosas: se emplea en la familia de estándares IEEE 802 para definir la subcapa de control de acceso al medio y a un número de identificación globalmente único que identifica a cada dispositivo de comunicación (cada tarjeta de red). En este caso se hace referencia a este último significado, también conocido como dirección MAC.

   El hecho es que existe un número que identifica a cada una de las tarjetas de comunicaciones que se fabrican. Este número es único y fue creado para facilitar las comunicaciones del protocolo Ethernet. La ventaja de la dirección MAC frente a la dirección IP es que la primera es única para cada equipo, mientras que la segunda la asigna a cada red y puede ser modificada por sus usuarios. Por tanto, un número de dirección MAC identifica a cada terminal de forma inequívoca.

   Pues bien, aprovechando este hecho, algunos puntos de acceso ofrecen la posibilidad de definir una lista de números MAC permitidos. Esto quiere decir que el punto de acceso

sólo permitirá la comunicación a los equipos (ordenadores) cuyo número MAC se encuentre en la lista. Al resto de equipos, entre ellos al de los intrusos, no se les permitirá el acceso.

El filtro MAC es una buena barrera de acceso, no obstante, tiene una debilidad: un pirata experimentad puede descubrir los números MAC autorizados, modificar este número en su equipo y entrar en la red. Ciertamente, un usuario normal no puede modificar su número MAC, pero existen procedimientos que lo permiten hacer. Por tanto, este sistema supone una buena barrera, pero no es definitivo.

Los números MAC están formados por 48 bits o, lo que es lo mismo, por 12 caracteres hexadecimales que suelen representarse como una cadena de seis grupos de dos cifras separados por dos puntos (por ejemplo, 12:AB:56:78:90:FE). Este número lo asigna cada fabricante a cada una de las tarjetas de comunicación (también conocida como NIC o Network Interface Card, "tarjeta interfaz de red") que produce y tiene la particularidad de ser único. Quiere decir que no existen dos tarjetas con números iguales.

b) No publicar la identificación SSID: Como se sabe, los puntos de acceso se identifican por un nombre que le otorga arbitrariamente su administrador y que se conoce como SSID o nombre de red. El punto de acceso puede anunciar este nombre, emitir esta información, o mantenerlo oculto. Cuando lo anuncia, cualquier usuario en su área de cobertura que explore las redes disponibles lo encontrará y podrá intentar conectarse a ella con un simple clic. Si el punto de acceso no publica su SSID, su nombre no aparecerá en la lista de redes disponibles, y por tanto, no invitará a su conexión.

   Ocultar el SSID es una barrera para los intrusos, pero también para los usuarios autorizados, a los que obligará a conocer e introducir el nombre específico de la red cuando deseen conectarse. Para esto tenemos dos noticias: la buena es que el ordenador del usuario suele guardar los perfiles con los que se conecta a cada red, por lo que, una vez establecida la conexión la primera vez, las siguientes se realizarán de forma automática, sin más intervención. La mala noticia es que existen herramientas para descubrir el SSID aunque el punto de acceso no lo publique, por tanto, un pirata experimentado no tendrá problemas en saltarse esta barrera.

   Por otro lado, dado que el identificador SSID se puede elegir, es mejor utilizar un nombre que no tenga ninguna relación con los propietarios ni con los usuarios de la red. Esto complicará, al menos, la identificación de la red. Por ejemplo, si la empresa Ferrox le asignase a su red el nombre FerroxWIFI, cualquiera que detectase este SSID podría fácilmente a quién pertenece. Un pirata especialmente interesado en entrar en esta red tendría sencillo su identificación. Por el contrario, si se eligiese el nombre N2J3X, el pirata la detectará igualmente, pero no podrá deducir fácilmente a quién pertenece.

c) No habilitar DHCP. Para que un equipo se conecte a una red IP necesita disponer de un número IP de identificación (su dirección IP). Este número puede introducirse manualmente en cada equipo o puede configurarse para que lo obtenga automáticamente en el momento de su conexión. Quien asigna los número IP de forma automática es un

servicio del punto de acceso conocido como *DHCP (Dynamic Host Control Protocol, "Protocolo de control dinámico del Host")*.

El servicio *DHCP* puede habilitarse o no. Si se habilita, cualquier usuario puede conectarse a la red simplemente configurando la opción "Obtener IP de forma automática". Si no se habilita, a cada equipo de usuario hay que configurarle manualmente una dirección IP válida. Esto significa que cada número IP tiene que estar dentro del rango de números de la red y no estar siendo utilizado por otro ususario.

Por tanto, tener deshabilitado el servicio DHCP supone una barrera, aunque obliga al administrador de la red a gestionar de forma manual la asignación de números IP. De nuevo tenemos dos noticias: la buena es que esta asignación sólo habría que hacerla una vez. El ordenador se encargaría de guardar dicha asignación en el perfil de la red para que no sea necesario definirla en las futuras conexiones. La mala noticia es que las redes privadas disponen de unos rangos de numeración específicos que son conocidos por todos. Por tanto, descubrir un número IP válido es solo cuestión de paciencia. En cualquier caso, para intrusos sin experiencia puede suponer un gran impedimento.

### 3.1.16. Inseguridad en las redes inalámbricas

La única manera de conseguir seguridad en cualquier sistema informático es manteniendo unas técnicas de protección adecuadas. Hay que ser conscientes de que ninguna técnica de protección es eficaz al cien por cien, siempre existe riesgo, aunque sea pequeño. No obstante, a más barreras de seguridad, menor será el riesgo.

En cualquier caso, recuerde que la mayor debilidad de cualquier sistema informático no es la tecnología, sino sus usuarios. De nada sirve un sistema de cifrado completamente seguro si no se activa, si sus claves son evidentes o si se deja con la configuración por defecto.

En un principio, las barreras de seguridad básicas que se deben tener en cuenta para cada uno de los riesgos son las siguientes:

- Pérdida del equipo. Tomar las precauciones mínimas para evitar en lo posible la pérdida o robo del equipo. No dejar grabados en el equipo los nombres de usuario y contraseña, ni tampoco dejar estos datos escritos en papeles que estén permanentemente con el equipo o en documentos fácilmente identificables.

- Infección por un virus. Utilizar software antivirus, Los ataques exteriores se pueden presentar bajo tres formas: virus, gusanos y caballos de Troya. Un virus es un programa diseñado para autorreplicarse y ejecutarse sin el conocimiento del usuario. Un gusano es un programa que está pensado para autorreplicarse y difundirse por el mayor número de equipos posibles. Un caballo de Troya es un programa que aparenta ser un programa útil, pero que, se dedica a recoger información o a facilitar que el intruso tenga acceso a ese ordenador o a la red en la que se encuentra. Es importante ser conscientes de que el mundo de la piratería está siempre evolucionando; por este motivo, conviene mantener actualizado el software antivirus.

- Mal uso por personas autorizadas (intencionado o accidental). Este problema suele aparecer en los entornos corporativos, por lo que su solución se basa en implantar una política de seguridad donde se defina cuáles son los puntos importantes que deben tener en cuenta los empleados (uso de las claves, copias de seguridad, por mencionar algunos). Es importante plasmar estos puntos en un documento y difundirlo adecuadamente, además de ofrecer formación sobre el uso de los ordenadores, las posibles amenazas a la seguridad y cómo evitarlas.

- Uso fraudulento por personas no autorizadas (intrusos). A pesar de que la mayoría de los usuarios tiene en mente el problema de la seguridad, lo cierto es que no se le suele dedicar mucha atención. Por ejemplo, es habitual dejar los productos con su configuración por defecto de los equipos. Por ello, es recomendable cambiar las claves de acceso y activar las medidas de seguridad no configuradas por defecto (*WEP o WAP*). También son recomendables otras medidas como ocultar la identificación *SSID*, no habilitar *DHCP* o utilizar *firewall*.

Todas las medidas anteriores son necesarias si se busca la seguridad de los sistemas informáticos, pero, desde el punto de vista de las redes inalámbricas, quizás, el problema que más preocupa sea el del último punto: la protección frente a intrusos.

# Capítulo 4
# Reestructuración de las redes

Las redes de comunicación de datos permiten a varias compañías ser viables a largo plazo. Cuando se pretende utilizar la red para un uso en particular es necesario fijar un objetivo y los beneficios deben ser palpables para justificar su implementación.

En este capítulo se presentan los problemas de comunicación de las redes “Intinitum0898” y “EDUCTRADE2014”. Se propone que los usuarios desde su estación de trabajo puedan acceder a los ficheros del servidor para hacer su órden de servicio e impriman su etiqueta sin estar esperando a que se desocupe la estación de trabajo asignada.

## 4.1. Problemática actual

A continuación en la imagen 4.1 se muestra como fueron diseñadas las redes “Infinitum0898” y “EDUCTRADE2014”:

Existen dos router, los cuales también funcionan como puntos de acceso, en los cuales se encuentran conexiones de más de 45 dispositivos móviles, 4 tablet’s, 2 estaciones de trabajo como intrusos, 3 estaciones de trabajo como invitados, 14 estaciones de trabajo del Departamento de Ingeniería Biomédica y 2 impresoras en red y una por conexión USB y 2 Switch. En la imagen 4.2 se simulan las conexiones que tienen actualmente las redes mencionadas.

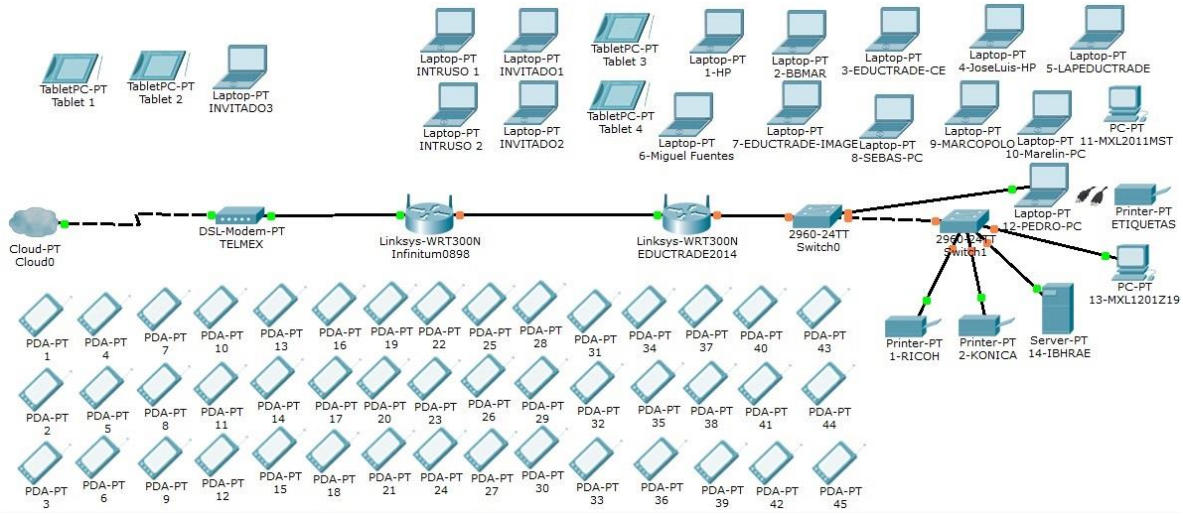


Imagen 4. 1 Simulación del diseño de las redes en Departamento de Ingeniería Biomédica

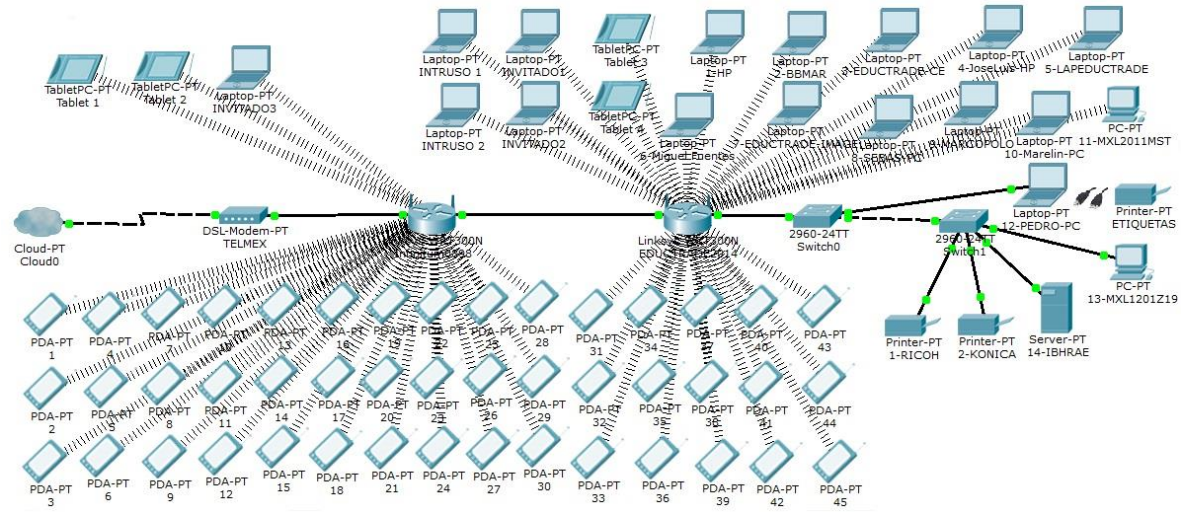


Imagen 4. 2 Simulación de las conexiones que tiene actualmente las redes

Algunas estaciones de trabajo están conectadas al punto de acceso con SSID “Infinitum0898” y otros al punto de acceso con SSID “EDUCTRADE2014”.

En el Departamento de Ingeniería Biomédica existen problemas de comunicación y administración con las redes “Infinitum0898” y “EDUCTRADE2014” descritas a continuación:

- Intrusos en la red
- Duplicidad en las direcciones IP
- No se puede imprimir en la impresora de color
- No se puede acceder a los ficheros del servidor desde las estaciones de trabajo
- Tiempos de espera muy prolongados para hacer órdenes de servicio

### 4.1.1. Existen intrusos en las redes del Departamento de Ingeniería Biomédica

Los clientes no reconocidos o intrusos dentro de las redes del Departamento de Ingeniería Biomédica pueden:

- Escuchar: con un receptor adecuado, los datos emitidos por un usuario pueden ser recogidos por terceras personas. De hecho, existen programas como Airopeek, Airsnort, NetStrumbler o Webcrack que facilitan esta labor. Estos programas descubren datos como el SSID, la dirección MAC o si el sistema WEP está o no habilitado.

- Acceder: se trata de configurar un dispositivo para acceder a una red para la que no se tiene autorización. Esto se puede hacer de dos formas: configurando un ordenador para que acceda a un punto de acceso existente o instalando un nuevo punto de acceso y, a través de él, conectar fraudulentamente todos los ordenadores externos que se deseen.

- Saturar: en este caso no se trata de intentar acceder fraudulentamente a una red, sino de dejarla fuera de servicio. El resultado es que la red no puede ser utilizada por sus propios usuarios, por lo que es un ataque a la seguridad. Para dejar inhabilitada una red inalámbrica, bastará simplemente con saturar el medio radioelectrónico con el suficiente ruido como para que sea imposible llevar a cabo cualquier comunicación. A este tipo de ataques se le conoce también como negación del servicio, DOS (Denial of Service) o jamming (literalmente “atasco”).

- Realizar: robo de identidad, pérdida de información, denegación de acceso o fuga de información.

La imagen 4.3 muestra los clientes no reconocidos en la red “EDUCTRADE2014” del Departamento de Ingeniería Biomédica.

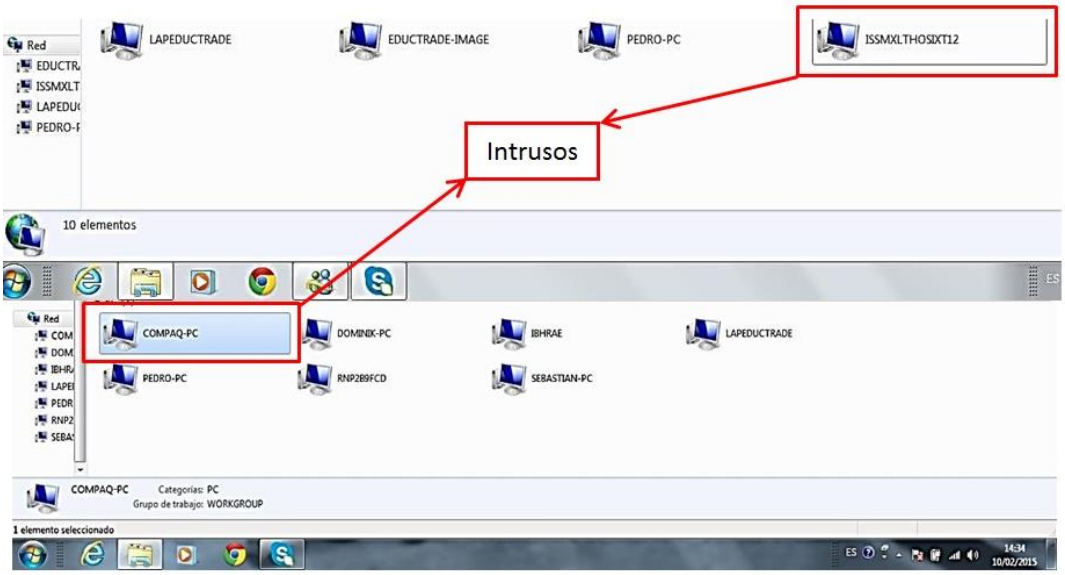


Imagen 4. 3 Hosts no reconocidos “ISSMXLTHOSIXT12” y “COMPAQ-PC”

### 4.1.2. Conflicto con las direcciones IP

Las estaciones de trabajo cuando están conectadas por medio de la red inalámbrica “EDUCTRADE2014”, al encender las estaciones de trabajo en ocasiones aparece el mensaje: Windows detectó un conflicto en la dirección IP (Otro equipo de esta red tiene la misma dirección IP de este equipo. Póngase en contacto con el administrador de red para que le ayude a resolver este problema. Puede tener más detalles en el registro de eventos de sistema de Windows). En la imagen 4.4 se muestra el error.

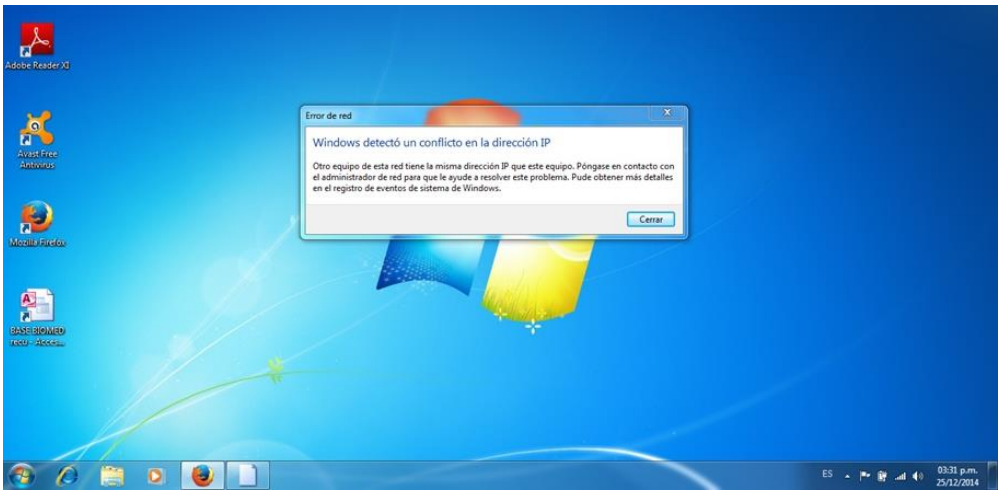


Imagen 4. 4 Error de red

La tabla 4.1 muestra las direcciones IP que tenían las estaciones de trabajo.

Tabla 4. 1 Tabla de direcciones IP

| RED DE TRABAJO DE EDUCTRADE-IXTAPALUCA | | | | | | | |
|---|---|---|---|---|---|---|---|
| USUARIO | HOST | IP | | | | | CONEXIÓN |
| TELMEX | MÓDEM | 192 | 168 | 1 | 254 | | ETHERNET |
| D'LINK | DIR 400 -- ROUTER-LAN | 192 | 168 | 0 | 1 | | ETHERNET |
| ETIQUETAS | ETIQUETAS | Sin habilitar | | | | | ETHERNET |
| KONICA | KONICA | DHCP Dinámico | | | | | ETHERNET |
| RICOH | RICOH | 192 | 168 | 0 | 198 | | ETHERNET |
| PEDRO 1 | PEDRO-PC | 192 | 168 | 0 | 201 | | ETHERNET |
| OSCAR | EDUCTRADE-IMAGE | 192 | 168 | 0 | 51 | | ETHERNET |
| EVER | MARCOPOLO | 192 | 168 | 0 | 123 | | WI-FI |
| SEBASTIAN | SEBAS-PC | 192 | 168 | 0 | 76 | | WI-FI |
| BARANDA TRABAJO | LAPEDUCTRADE | 192 | 168 | 0 | 9 | | WI-FI |
| DESCONOCIDO 1 | ISSMXLTHOSIXT12 | 192 | 168 | 0 | 156 | | WI-FI |
| IVONNE | MXL1201Z19 | 192 | 168 | 0 | 56 | | WI-FI |
| SERVIDOR | IBHRAE | 192 | 168 | 0 | 57 | | ETHERNET |
| PEDRO 2 | PEDRO-PC | 192 | 168 | 0 | 32 | | WI-FI |
| MARCO ANTONIO | BBMAR | 192 | 168 | 0 | 98 | | WI-FI |
| ATANASIO | HP | 192 | 168 | 0 | 63 | | WI-FI |
| ANGÉLICA | Miguel Fuentes | 192 | 168 | 0 | 71 | | WI-FI |
| MARELIN | Marelin-PC | 192 | 168 | 0 | 90 | | WI-FI |
| CESAR | EDUCTRADE-CE | 192 | 168 | 0 | 159 | | WI-FI |
| JOSÉ LUIS | JoseLuis-HP1 | 192 | 168 | 0 | 64 | | WI-FI |
| DESCONOCIDO 2 | COMPAQ-PC | 192 | 168 | 0 | 192 | | WI-FI |

### 4.1.3. Conflicto para la impresión a color

La impresora a color tiene un direccionamiento dinámico provocando que al apagar y encender el equipo adquiera una dirección IP diferente, por lo que cada vez que enciende hay que revisar qué IP tiene y volver a configurarla. En la imagen 4.5 se puede apreciar que la impresora a color tiene la configuración DHCP encendido.

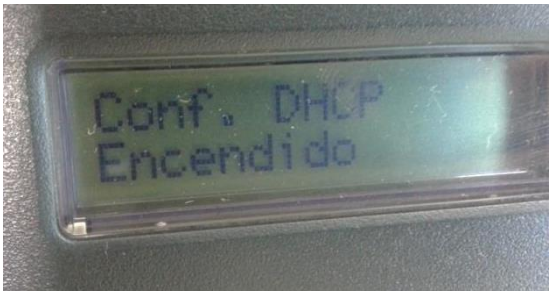


Imagen 4. 5 Configuración DHCP Encendido

### 4.1.4. Conflicto para acceder a los ficheros del servidor desde las estaciones de trabajo

Problema con el acceso directo

La unidad o conexión de red a la que se refiere el acceso directo “FICHEROS – Acceso directo.lnk” no está disponible. Asegúrese de haber insertado el disco correctamente o de la disponibilidad del

recurso de red e inténtelo de nuevo. En la imagen 4.6 se muestra el problema con el acceso directo.

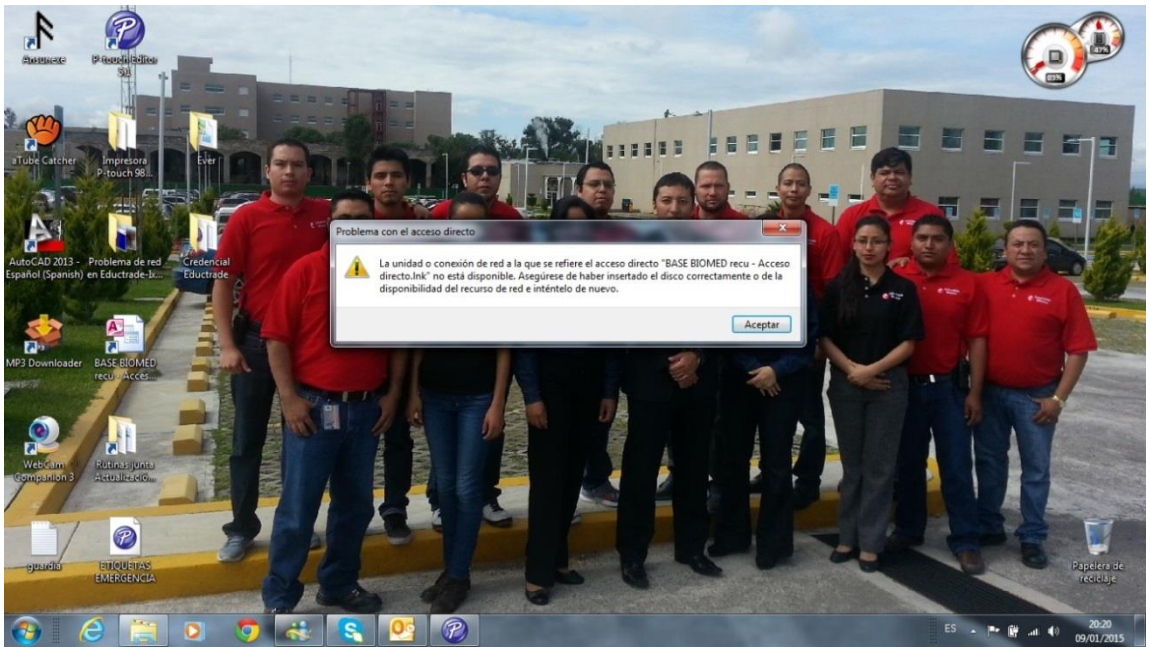


Imagen 4. 6 Problema con el acceso directo

### 4.1.5. Tiempos de espera prolongados para hacer órdenes de servicio

En el Departamento de Ingeniería Biomédica los usuarios realizan órdenes de servicio (mantenimiento preventivo, correctivo, asistencia, ticket, entrada o salida de equipo) e impresión de etiquetas en una estación de trabajo asignada "PEDRO-PC" (conectada por cable USB a la impresora) mostrado en la imagen 4.7, debido a que solo existe un equipo para esta actividad (imagen 4.8) el tiempo de espera puede llegar a ser de 30 minutos entre un usuario y otro.

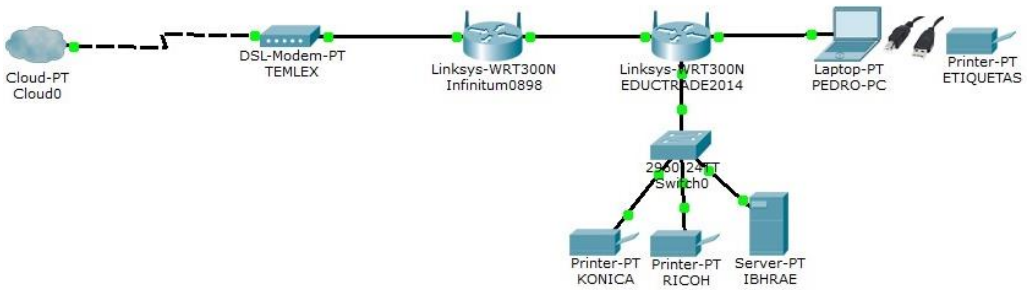


Imagen 4. 7 Se muestra cómo está la configuración para la estación de trabajo asignada

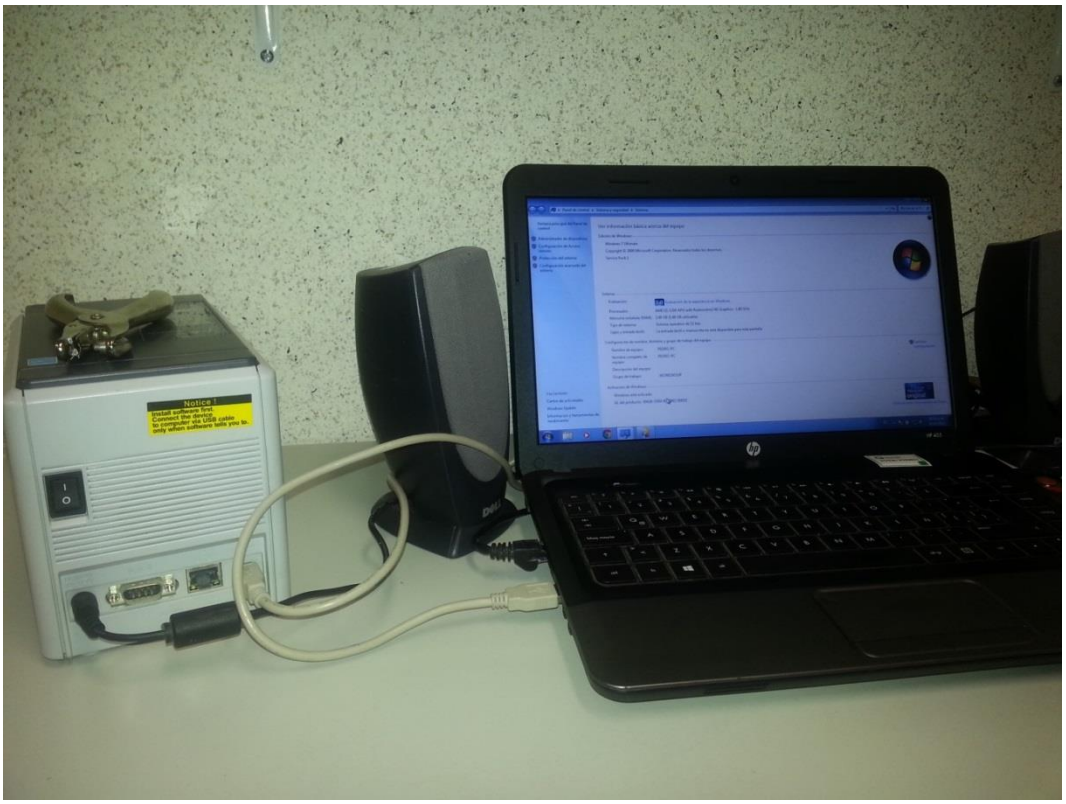

Imagen 4. 8 Estación de trabajo asignada e impresora conectada por USB

## 4.2. Objetivo

Analizar, diseñar, implementar y administrar una red de datos. Así como descentralizar el uso de la impresora de etiquetas en el Departamento de Ingeniería Biomédica.

Para alcanzar el objetivo general planteado, se consideran los siguientes objetivos particulares:

- Diseñar y administrar una red de datos para la empresa, implementar políticas de seguridad internas para el Departamento de Ingeniería Biomédica, en la cual no esté centralizado el servicio para las labores de los trabajadores.
- Tener identificadas las estaciones de trabajo que están dentro de la empresa, generar una red en la cual las direcciones IP de las estaciones de trabajo no sean repetidas ni ocupen la IP asignada al servidor o de las impresoras.
- Configurar el punto de acceso para que filtre las direcciones MAC de las estaciones de trabajo, se pretende acceder a los ficheros del servidor y hacer que la impresión de etiquetas no sea centralizada.

## 4.3. Estrategia de gestión de redes

La tabla 4.2 presenta un conjunto de criterios que deben ser considerados al momento de instalar una red de comunicación de datos para proporcionar excelentes resultados prácticos.

Tabla 4. 2 Criterios estratégicos para implementar una red de comunicación de datos

| | |
|---|---|
| Integración y flexibilidad | Integración de servicios disponibles de comunicación. |
| Conectividad | Acceso fácil y conexión eficaz a la red de comunicación. |
| Compartimiento de recursos | Uso de la red para compartir hardware, software y recursos entre los sistemas de información empresariales. |
| Disponibilidad | Hardware, software y servicios de comunicación que satisfagan los estándares de comunicación utilizados de manera permanente por la compañía. |
| Confiabilidad y seguridad | Red de comunicación de datos confiable y segura para garantizar las operaciones y los servicios vitales de la empresa. |
| Facilidad de manejo | Administradores experimentados y capacitados para mantener las redes en óptimas condiciones. |

Para las empresas una red de comunicación debe estar disponible las 24 horas del día a fin de mantener comunicación continua. Además la confiabilidad es una característica importante que considera la frecuencia y duración de las fallas. Una red debe ser flexible a fin de permitir al usuario realizar cambios a un costo mínimo. La flexibilidad también significa que el crecimiento tenga efectos mínimos en las instalaciones existentes: posibilidad de aumentar la potencia de los procesadores, la velocidad de transmisión, el número de terminales de comunicación, entre otros. Es recomendable utilizar las arquitecturas y estándares de la industria para facilitar los cambios ocasionales que se deben hacer a la red garantizando la seguridad de la misma.

## 4.4. Desarrollo

Se requiere plantear una estrategia integral que permite mejorar la situación actual en la cual está inmerso el Departamento de Ingeniería Biomédica con relación a la omisión de la gestión de redes inalámbricas. Esta estrategia cubre aspectos de carácter administrativos y técnicos, de manera que se finquen responsabilidades a la persona encargada de estos recursos en caso de alguna contingencia.

### 4.4.1 Estrategia de solución

La estrategia que se pretende seguir y que se desarrolla en este reporte cubre los siguientes aspectos:

1) Configuraciones adecuadas y buenas prácticas. Otra parte importante de la gestión de redes inalámbricas son las configuraciones adecuadas y buenas prácticas que son procedimientos y recomendaciones que se emiten para hacer una red inalámbrica más

segura y eficiente, esta parte resulta muy importante ya que si los recursos de las Tecnologías de Información del Departamento de Ingeniería Biomédica siguen este tipo de prácticas el número de incidentes de seguridad en cómputo disminuyen.

2) Políticas para las redes. Parte fundamental de esta estrategia de gestión de redes inalámbricas es contar con políticas de seguridad de las redes del Departamento de Ingeniería Biomédica. Como se mencionó anteriormente la falta de normatividad en los servicios de red inalámbricos dentro del departamento puede ser razón de un mal uso de las Tecnologías de Información del Departamento de Ingeniería Biomédica.
   Cabe mencionar que las redes inalámbricas son una extensión de las redes cableadas y complementan todo sistema de comunicaciones, por lo que se hace necesario contemplar en estas políticas también las necesarias para todo el sistema.
   Las políticas de las redes inalámbricas para el Departamento de Ingeniería Biomédica que se proponen están sustentadas, se aplica la mejora continua a la problemática presentada y cubrirán aspectos tales como políticas de uso, seguridad, confidencialidad, control de acceso, disponibilidad e integridad, seguridad física de la infraestructura de red, e interferencia.

3) Monitoreo de redes inalámbricas. En las redes de datos de manera general, el monitoreo es una actividad que representa el saber cómo se está comportando la red, además de que permite identificar a posibles intrusos y sus actividades que intenten sobre la red, las redes inalámbricas que son una extensión de las redes cableadas y en el Departamento de Ingeniería Biomédica complementan el sistema de comunicación por lo tanto el monitoreo resulta una tarea elemental para un óptimo rendimiento.

Mediante estas estrategias se pretende gestionar las redes inalámbricas del Departamento de Ingeniería Biomédica y resulta importante señalar que esta tarea es un trabajo en conjunto en donde las responsabilidades sobre las redes inalámbricas recaigan no sólo en una persona encargada de la administración de la red sino, desde las personas encargadas de la instalación y configuración de los puntos de acceso hasta los usuarios de las mimas.

### 4.4.2. Implementación de la solución: Reestructuración de las redes

Fase 1: Configuraciones adecuadas y buenas prácticas.

A continuación se muestra en la imagen 4.9 la propuesta de reestructuración de las redes y la imagen 4.10 simula las conexiones, esto permite dar solución a los problemas (1, 2, 3 y 4) presentados:

1. Existen intrusos en las redes del Departamento de Ingeniería Biomédica
2. Conflicto con las direcciones IP

3. Conflicto para la impresión a color
4. Conflicto para acceder a los ficheros del servidor desde las estaciones de trabajo

En los cuales estaba inmerso el Departamento de Ingeniería Biomédica.

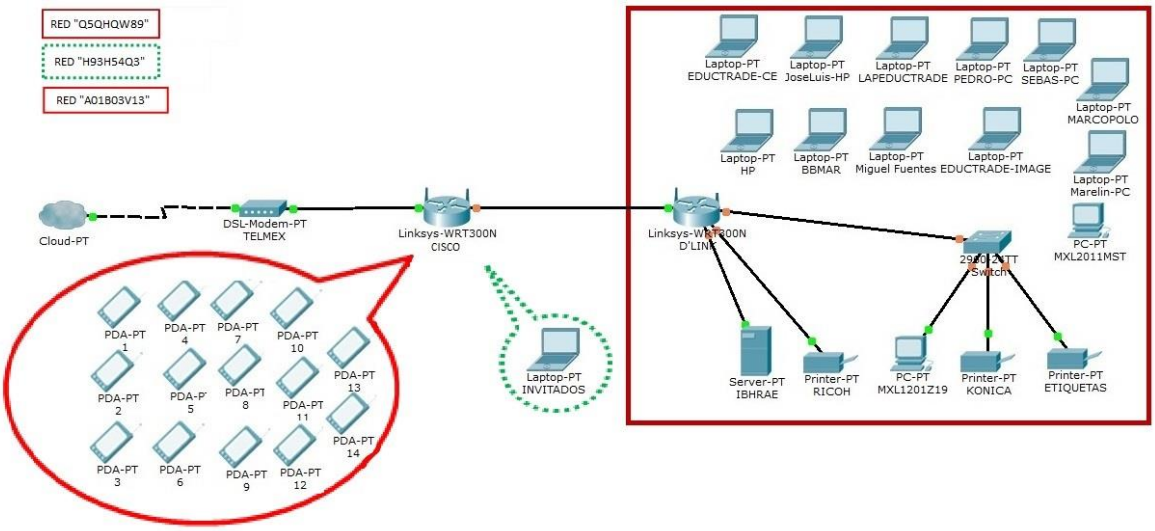


Imagen 4. 9 Simulación de la redes sin conexión

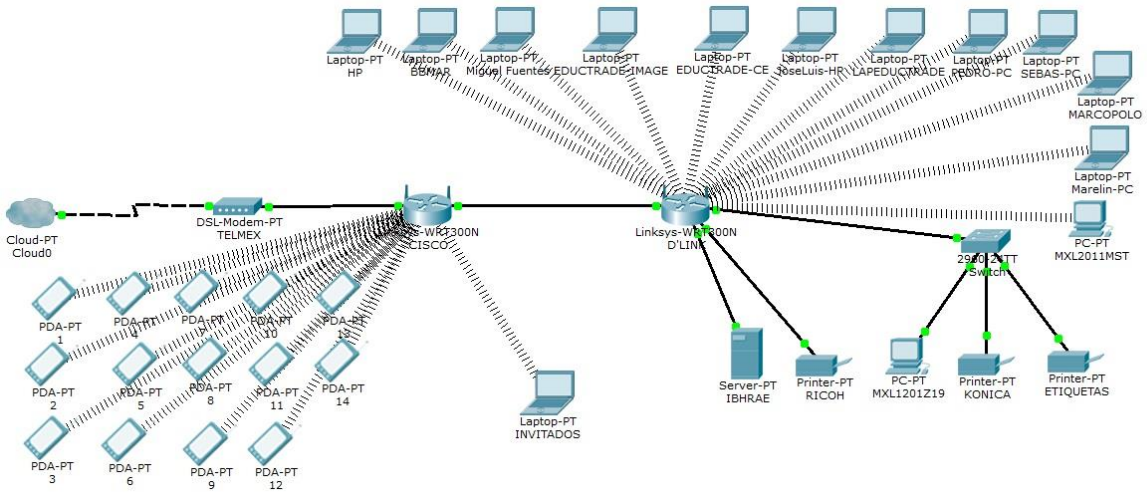


Imagen 4. 10 Simulación de la redes con conexión

Por cuestiones del servicio en el Departamento de Ingeniería Biomédica. Se configuraron dos puntos de acceso uno que es marca: Cisco, modelo: N300 y otro marca: D'Link, modelo: DIR400.

En el AP Cisco se configuró el SSID "H93H54Q3" para que sea visible (red 192.168.33.0/24). Esta red se configuró para que en aquellas ocasiones cuando llegue al Departamento algún proveedor externo o invitado y requiera conexión a internet, lo haga sin afectar las redes "A01B03V13" y "Q5QHQW89".

Adicionalmente se limita a cinco el número de invitados permitidos como se observa en la imagen 4.11.

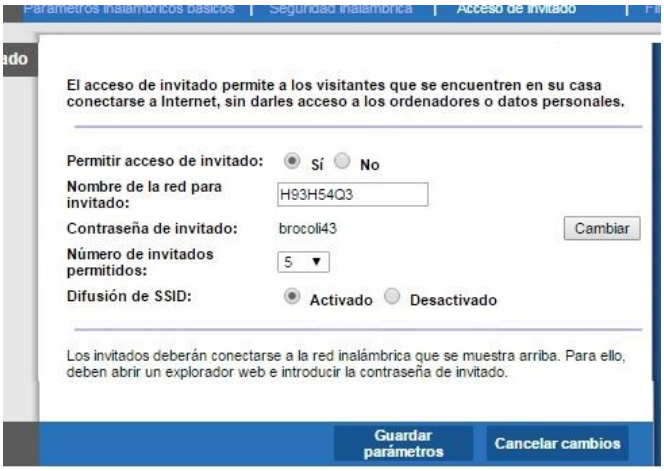


Imagen 4. 11 Red "H93H54Q3"

El mismo AP Cisco también tiene la opción de incluir una red privada con un SSID "A01B03V13" no visible, en la cual se conectaron dispositivos móviles y computadoras portátiles de uso personal. Se activó el rango de direcciones DHCP (red 192.168.0.0/24) y se habilitó el filtrado de direcciones MAC. Se configuró un cifrado de seguridad WPA2 con una encriptación AES-Personal. En la imagen 4.12 se muestra la configuración de la red "A01B03V13" configurado en el canal de transmisión 5.

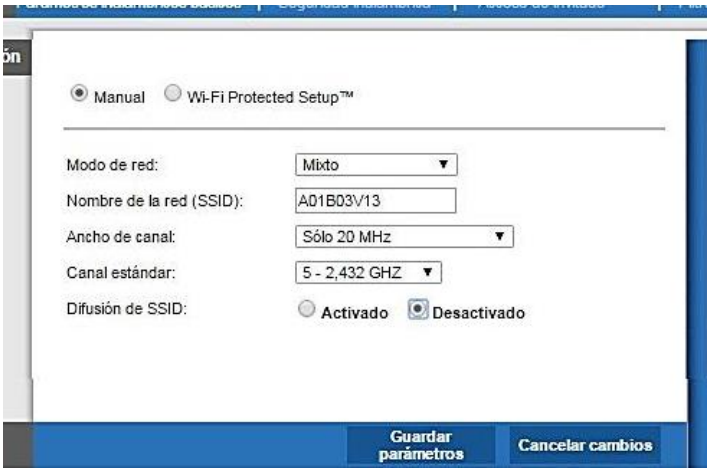


Imagen 4. 12 Red "A01B03V13"

Para el SSID “Q5QHQW89” no visible (red 192.168.1.0/24) en el AP D’Link. Se configuró el cifrado de seguridad WPA2 con encriptación AES-Personal, para mayor seguridad se habilitó el filtrado de direcciones MAC y se estableció el canal 2 para esta red como se muestra en la imagen 4.13.

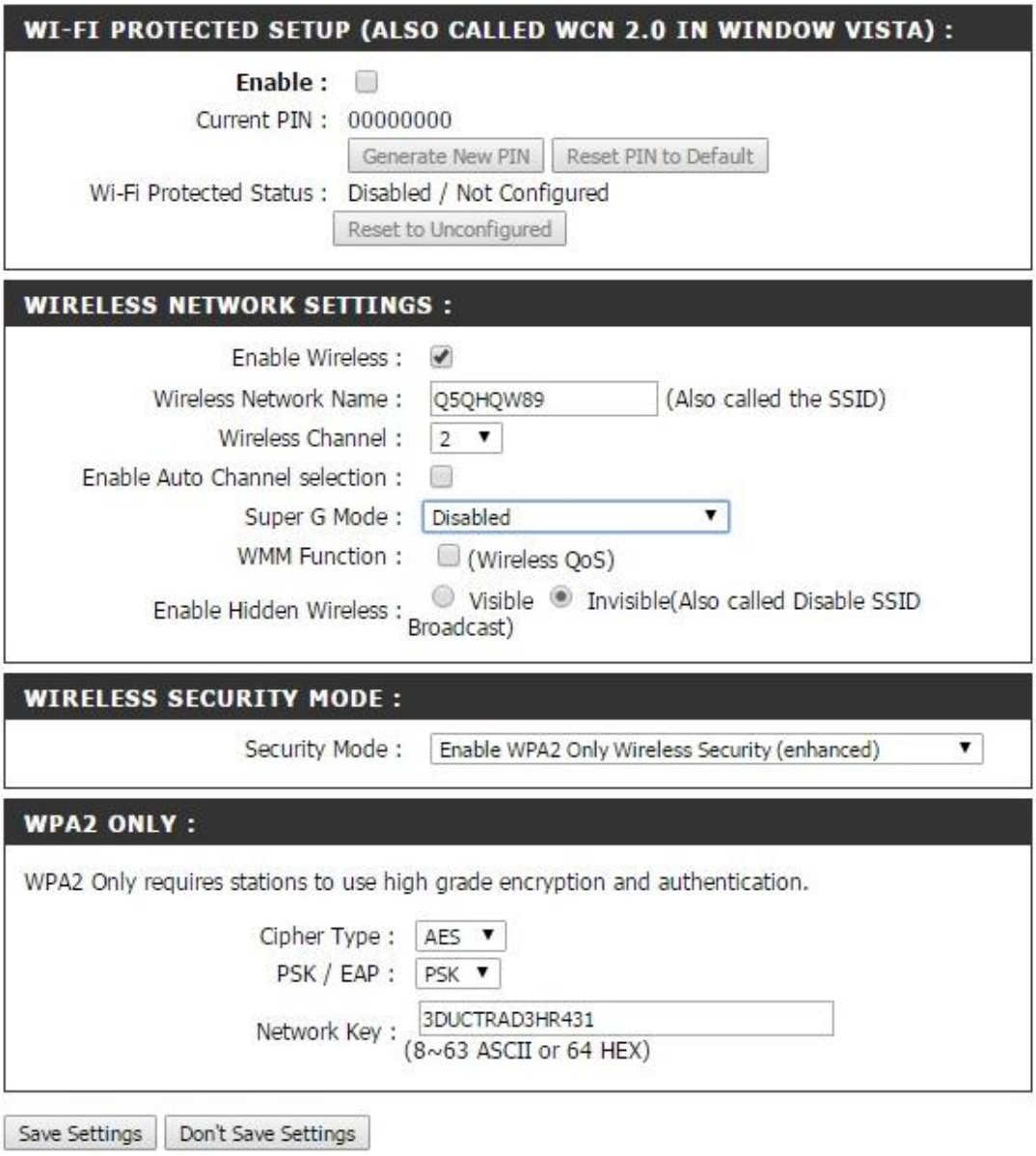


Imagen 4. 13 Red “Q5QHQW89”

Para dar solución al problema 5 (Tiempos de espera prolongados para hacer órdenes de servicio) del Departamento de Ingeniería Biomédica se realizó la configuración de los equipos de impresión. Se les asignaron IP estática. Para “RICOH” (192.168.0.3), “KONICA” (192.168.0.4) y “ETIQUETAS” (192.168.0.5) como se muestra en las imágenes 4.14, 4.15, 4.16:

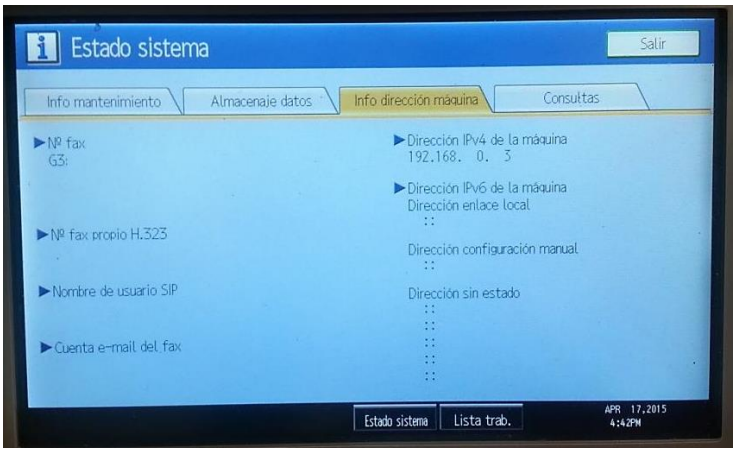


Imagen 4. 14 “RICOH” con IP estática: 192.168.0.3


Imagen 4. 15 “KONICA” con IP estática: 192.168.0.4

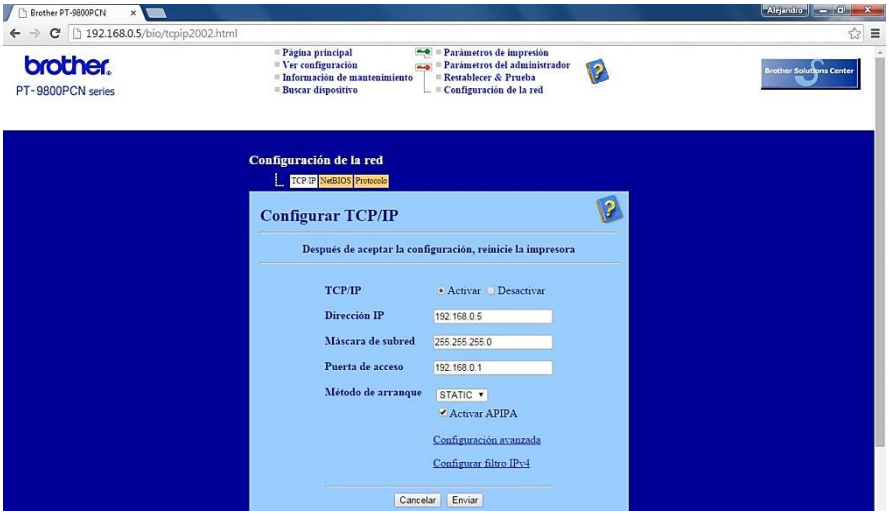


Imagen 4. 16 “ETIQUETAS” con IP estática: 192.168.0.5

Fase 2: Políticas para las redes.

De manera general una norma es un conjunto de especificaciones de carácter administrativo y técnico que dictan el comportamiento adecuado del proceso tecnológico en este caso, son de aplicación voluntaria y están elaboradas por las partes interesadas que participan en el proceso al cual se esté aplicando, estas normas deben de ser de conocimiento público.

Hablando de las redes inalámbricas se ha mencionado de su problemática y peligros que afectan el rendimiento, la seguridad, la calidad en el servicio, entre otros, cuando no se tienen correctamente gestionadas. Es por ello necesario crear un conjunto de normas que eviten el acceso no controlado a los recursos tecnológicos.

La inexistencia de normatividad en cuestión de redes inalámbricas es causa de problemas como la falta de asignación de responsabilidades en asuntos de administración, configuración y control de los dispositivos de la red como los son los puntos de acceso. También como consecuencia de esta carencia de normatividad, surge la creación de redes inalámbricas sin justificar su uso ni su localización.

En una organización en donde se requiere tener controlado el uso de sus tecnologías de información es necesario establecer principios que declaren su buen uso y sus posibles penalizaciones en caso de no seguir con estos principios. Para ello es necesario crear un conjunto de reglas o políticas de seguridad y divulgarlas como herramienta de control de la infraestructura tecnológica, en este caso del Departamento de Ingeniería Biomédica.

Una política de seguridad es un conjunto de documentos en donde se detallan las reglas de seguridad en cómputo para una organización. Tienen como objetivo informar al personal de la organización (generalmente todas las áreas) las normas y mecanismos que se deben cumplir y poner en práctica para proteger los recursos tecnológicos y la información de la organización.

Las necesidades de la organización y el análisis de riesgos son las principales directrices en la creación de las políticas de seguridad. El documento general que especifique las políticas de seguridad debe estar formado por tres documentos diferentes:

- Políticas. Elemento esencial de las políticas de seguridad y que generalmente no son tecnológicamente específicas y tienen repercusiones más amplias sobre los aspectos relacionados con la red.
- Guías de uso. Mejores prácticas de la organización.
- Procedimientos. El conjunto mínimo de criterios de operaciones de ciertas tecnologías o activos.

Las políticas de seguridad tienen un ciclo de vida en donde se desarrollan varias etapas como lo son de investigación, elaboración, aprobación, divulgación, aceptación por parte de los usuarios finales, darles seguimiento, actualización y como etapa final la eliminación cuando haya quedado obsoleta. Cuando alguna de estas etapas no se lleva a cabo queda la posibilidad de que no se

tomen como válidas estas políticas. En la imagen 4.17 se muestra el ciclo de vida de una política de seguridad de red.

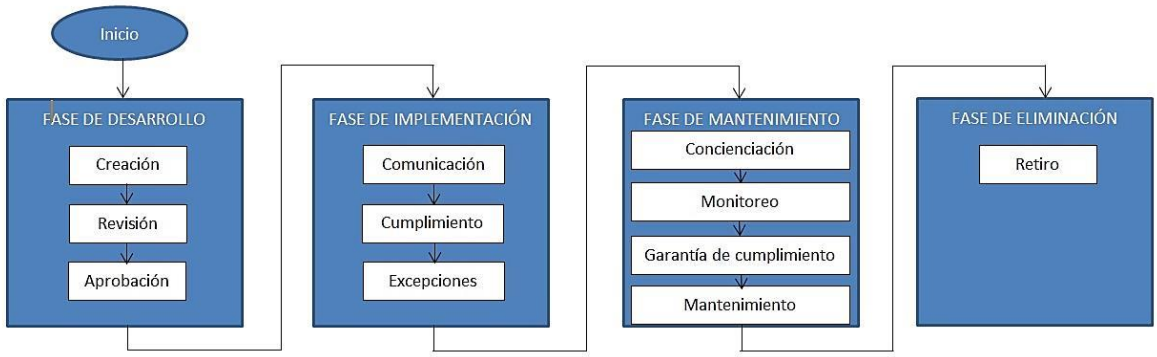


Imagen 4. 17 Ciclo de vida de una política de seguridad

Como ya se mencionó, las necesidades de la organización son una de las dos directrices en el desarrollo de las políticas de seguridad, el impacto de estas necesidades que tienen sobre las políticas de seguridad recaen en los objetivos de la empresa.

Políticas de seguridad para las redes de comunicación del Departamento de Ingeniería Biomédica.

A continuación se hace la propuesta de las Políticas de Seguridad para las redes del Departamento de Ingeniería Biomédica.

Objetivo

Definir las políticas relacionadas para instalar equipos inalámbricos y alámbricos a las redes del Departamento de Ingeniería Biomédica y establecer los procedimientos para su instalación y configuración.

Metas

- Mantener la integridad y confidencialidad de la información y de la infraestructura de la red.
- Prevenir la interferencia con otros usuarios que utilicen el mismo espectro de frecuencias.

El mantenimiento de la seguridad e integridad de las redes del Departamento de Ingeniería Biomédica requiere de medios adecuados para asegurar que solamente los usuarios autorizados puedan hacer uso de ella. Los dispositivos de red inalámbricos que utilizan la infraestructura de la red, deben de cumplir con ciertas normas para que solamente usuarios autorizados y autenticados puedan conectarse y que dichos dispositivos no queden expuestos.

Plantear la normatividad para regular el buen uso, disponibilidad y nivel de servicio de los recursos de redes inalámbricas de la empresa. El uso de estos recursos inalámbricos debe respetar los fines con los que fue instalado, evitar interferir los servicios que ofrece o de otros equipos que forman

parte de la infraestructura de red, así mismo evitar situaciones que afectan la seguridad de la información y de los usuarios.

El administrador de la red, junto con el jefe de Ingeniería Biomédica pueden modificar estas políticas de seguridad y uso de las redes inalámbricas en cualquier momento cuando se considere necesario y es responsabilidad de los usuarios asegurarse del conocimiento de tales cambios. Estas políticas por tal motivo están impresas en la oficina para consulta en cualquier momento.

Aquellas personas que ignoren esta normativa de forma reiterada, deliberada, por negligencia o las infrinjan están sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) o disciplinarias que se estimen oportunas.

Con base en las actividades del Departamento de Ingeniería Biomédica y sus usuarios así como los requerimientos de uso y mantenimiento se configuraron tres redes:

A) Red “H93H54Q3” - configurada para proveedores de servicios e invitados
B) Red “A01B03V13” - configurada para dispositivos personales
C) Red “Q5QHQW89” – configurada para uso Institucional

En la tabla 4.3 se muestran las políticas que se desarrollaron en 10 rubros distintos:

Tabla 4. 3 Políticas para las redes del Departamento de Ingeniería Biomédica

| | Red “H93H54Q3” - configurada para proveedores de servicios e invitados | Red “A01B03V13” - configurada para dispositivos personales | Red “Q5QHQW89” - configurada para uso Institucional |
|---|---|---|---|
| 1) Políticas de Uso | ✣ Los proveedores de servicios e invitados que necesiten conexión a Internet deben solicitar la clave al personal que labora en el Departamento de Ingeniería Biomédica.<br>✣ Se deberá registrar en la bitácora de uso de la Red “H93H54Q3” el nombre de la persona, nombre de la empresa, equipo que usa para navegar, hora de entrada y hora de salida. | ✣ Ningún usuario está autorizado a conectar dispositivos inalámbricos a la red, sin el visto bueno del administrador y previa autorización del jefe de ingeniería biomédica.<br>✣ Cuando se detecte un equipo instalado sin cumplir lo anterior se procede a deshabilitar el acceso del mismo en la red.<br>✣ La interferencia de los canales de comunicación inalámbrica con otras actividades que no sean las establecidas es una violación al uso aceptable. | |
| 2) Políticas sobre la Seguridad Lógica | ✣ Se deberá modificar los parámetros configurados de fábrica a los Puntos de Acceso, con base en las políticas de seguridad lógica definidas para cada red a fin de evitar que cualquier individuo tenga acceso a los mismos.<br>✣ Los puntos de acceso a las redes inalámbricas deben contar con las más recientes actualizaciones de su firmware antes de ser puestos en operación.<br>✣ Una vez que hayan iniciado su uso los Puntos de Acceso, se deberá | | |

<table>
<tr><td></td><td colspan="2">actualizar de manera constante su firmware.<br>- Los Puntos de Acceso deberán de tener canales de comunicación diferentes de manera que minimice la interferencia con otros equipos de radiofrecuencia.<br>- Las contraseñas son definidas por el administrador de la red.</td></tr>
<tr><td></td><td>- La contraseña al Punto de Acceso debe ser por lo menos de 8 caracteres alfanuméricos.<br>- La contraseña se debe cambiar los días lunes.</td><td>- La contraseña a los puntos de acceso deben ser de por lo menos 8 caracteres en una combinación de caracteres alfanuméricos y especiales.<br>- Las contraseñas deben ser cambiadas como mínimo cada dos meses.</td></tr>
<tr><td>3) Sobre la Confidencialidad</td><td colspan="2">- Las comunicaciones inalámbricas no proveen un mecanismo de codificación de los datos transmitidos confiable al cien por ciento por lo tanto la protección de los datos es responsabilidad del usuario y de la aplicación que utilice para transmitir los datos.<br>- Las redes inalámbricas no deben de ser utilizadas como medio de transmisión de datos para información sensible ya que esta puede ser monitoreada por intrusos.<br>- Las redes inalámbricas existentes en el Departamento de Ingeniería Biomédica deben implementar como mínimo el método de cifrado de datos WPA.</td></tr>
<tr><td></td><td>- La clave de acceso será enviada por correo electrónico al personal que labora en el Departamento de Ingeniería Biomédica.</td><td>- Las claves deben de ser conocidas únicamente por el administrador de sistemas.<br>- Las claves de acceso deben ser cambiadas como mínimo cada dos meses y en caso de que un usuario no permitido tenga acceso a esta llave debe cambiarse inmediatamente para asegurar que sólo el administrador de sistemas la conozca.</td></tr>
<tr><td>4) Sobre el Control de Acceso</td><td>- El SSID debe ser visible para los usuarios.<br>- La clave de acceso se solicita al momento de abrir el navegador preferido de internet.</td><td>- Una manera de minimizar riesgos de conexión no autorizado a la red, es mediante el uso del control de acceso a los Puntos de Acceso, estos dispositivos deben implementar filtros de direcciones MAC de los usuarios que tengan permitido el uso de la red inalámbrica, la implementación de este método presenta vulnerabilidades, no obstante representa un control administrativo de los clientes que utilizan la red.<br>- No deben de ser redes inalámbricas tipo abiertas, es decir que no tengan un mecanismo de autenticación.<br>- El SSID de las redes inalámbricas debe de estar oculto al conocimiento público</td></tr>
</table>

| | | |
|---|---|---|
| | | (No Broadcast), en caso de ser necesaria la publicación del SSID de red, se informará durante el procedimiento de registro de la red inalámbrica. |
| 5) Sobre la Disponibilidad | ➢ La disponibilidad de esta red dependerá del número de clientes que estén haciendo uso de la misma (máximo cinco). | ➢ La disponibilidad de los servicios inalámbricos ofrecidos a la comunidad es responsabilidad del administrador de red. |
| 6) Sobre la Seguridad Física de la Infraestructura de Red | ➢ El mantenimiento de la seguridad de la infraestructura de redes inalámbricas del Departamento de Ingeniería Biomédica requiere que sólo el administrador de red pueda tener acceso al mismo. De esta manera, se evita el robo o acceso no autorizado a los dispositivos y en consecuencia que se vean afectados los servicios.<br>➢ Los equipos (servidores y módem) deben ser resguardados dentro del site.<br>➢ En el site solo el administrador de la red tiene acceso.<br>➢ Los Puntos de Acceso deben estar localizados en un área accesible en donde se les pueda dar mantenimiento y ser configurados sin impedimentos.<br>➢ Los Puntos de Acceso deberán colocarse alejados de fuentes de interferencias como lo son hornos de microondas, tarjas de desinfección, antenas de radiofrecuencia, entre otros.<br>➢ Cuando se coloquen al aire libre los Puntos de Acceso deben contar con una protección contra agua, radiación solar, etcétera.<br>➢ La instalación y configuración de los Puntos de Acceso deben ser realizados por el administrador de la red. | |
| 7) Sobre la Interferencia | ➢ El funcionamiento correcto de una instalación inalámbrica que cubre la oficina del Departamento de Ingeniería Biomédica, requiere que todo el equipo esté correctamente instalado y configurado para evitar interferencias entre los componentes de otros segmentos de red o entre otros equipos.<br>➢ El administrador de la red de es el encargado de regular y administrar la configuración de frecuencias.<br>➢ El administrador de la red responderá a reportes de equipos que puedan estar causando interferencia y de no resolverse la situación, el uso del equipo sospechoso debe ser restringido o retirado. | |
| 8) Sobre el Monitoreo | ➢ Como medida de seguridad y rendimiento de las redes el administrador debe monitorear de manera periódica la red inalámbrica.<br>➢ El Administrador de la Red debe monitorear las redes cuando se tengan indicios de incidentes o reportes de actividad anormal.<br>➢ En las redes existentes en donde se asigne IP mediante el protocolo DHCP se deberán de almacenar bitácoras de las direcciones asignadas. | |
| 9) Sobre la Responsabilidad del Administrador de Red | ➢ Debe llevar un registro de direcciones MAC de los dispositivos que se utilicen en las redes inalámbricas.<br>➢ Resolver los problemas de interferencia en la comunicación.<br>➢ Informar a los usuarios de la red sobre las políticas de confidencialidad y seguridad relacionados con el uso de las comunicaciones.<br>➢ Crear, mantener y actualizar las políticas y las buenas prácticas de | |

| | |
|---|---|
| | seguridad.<br>- Verificar el cumplimiento de la presente normatividad a través de revisiones periódicas.<br>- Dar solución a cualquier evento de falla que se presente.<br>- Toda situación que se presente y no esté contemplada en este documento, deberá ser atendida por el administrador de la red y avalada por el jefe del departamento de Ingeniería Biomédica. |
| 10) Sobre el mal uso de los recursos | - El administrador de red podrá suspender o desconectar los servicios de red inalámbrica de manera temporal o definitiva según la falta que se haya cometido. |

Fase 3: Monitoreo de redes inalámbricas.

El monitoreo que se realiza permite visualizar los host's conectados, en la imagen 4.18 se observan los clientes de la red "Q5QHQW89", también nos muestra el nombre del cliente conectado, su dirección IP privada así como su dirección MAC y el tiempo en el que expirará su dirección IP, esta información nos permite estar corroborando de forma continua los clientes de la red versus los registros que tiene el Administrador de la Red.

**DHCP CLIENT LIST :**

| Host Name | IP Address | MAC Address | Expired Time |
|---|---|---|---|
| EDUCTRADE-CE | 192.168.0.100 | 54:27:1e:45:46:b8 | Sun Feb 22 03:30:19 2015 |
| MiguelFuentes | 192.168.0.101 | cc:52:af:5e:f9:68 | Sun Feb 22 20:29:46 2015 |
| Marelin-PC | 192.168.0.102 | 5c:ac:4c:75:0a:b5 | Mon Feb 23 02:29:56 2015 |
| JoseLuis-HP1 | 192.168.0.103 | cc:52:af:8d:c9:ad | Sun Feb 22 19:39:52 2015 |
| PEDRO-PC | 192.168.0.104 | d8:9d:67:80:3e:ba | Sat Feb 21 12:15:57 2015 |
| SEBASTIAN-PC | 192.168.0.106 | f4:b7:e2:5b:de:91 | Mon Feb 23 07:51:41 2015 |
| LAPEDUCTRADE | 192.168.0.107 | c0:f8:da:89:a9:27 | Mon Feb 23 09:22:37 2015 |
| BBMAR | 192.168.0.108 | d0:df:9a:19:4a:43 | Sun Feb 22 19:24:41 2015 |
| HP | 192.168.0.109 | 20:68:9d:e1:14:49 | Mon Feb 23 02:02:16 2015 |
| MXL2011MST | 192.168.0.110 | 90:f6:52:15:8c:15 | Mon Feb 23 06:18:59 2015 |
| DOMINIK-PC | 192.168.0.111 | 00:13:e8:e6:7a:59 | Mon Feb 23 09:29:57 2015 |

Imagen 4. 18 Clientes DHCP para la red "Q5QHQW89"

En la imagen 4.19 se muestran los clientes de las redes “A01B03V13” y “H93H54Q3”.

Esta tabla nos permite ver los clientes conectados versus los clientes que se tienen registrados en la bitácora y registros que tiene el Administrador de las Redes.

Imagen 4. 19 Clientes de las redes “A01B03V13” y “H93H54Q3”

# Capítulo 5
# Resultados

En este capítulo se dan a conocer los resultados obtenidos en el proyecto, los beneficios de su creación y las tareas que se facilitaron para los usuarios.

Con la misma infraestructura que se tenía se reestructuraron las redes del Departamento de Ingeniería Biomédica.

Se eliminaron los intrusos que se tenían dentro de las redes de trabajo, se configuraron los canales de frecuencias y los puntos de acceso para que sean ocultos los SSID, se generó un filtrado de direcciones MAC para mantener la seguridad, se realizó una reasignación de direcciones IP y se habilitó el DHCP.

Se configuraron las impresoras para que tengan IP estática y se descentralizó el uso de la estación de trabajo para no perder tiempo en realizar órdenes de servicio.

Se generaron las políticas de red que requiere el Departamento de Ingeniería Biomédica.

Se solucionó el problema de impresión.

Se actualizó la tabla de direcciones IP y se verificaron las MAC de los equipos.

A continuación se muestra la tabla 5.1 con las direcciones IP, las cuales han sido modificadas para el presente reporte y que conforman la red “Q5QHQW89”.

Tabla 5. 1 Direcciones IP de la red “Q5QHQW89”

| RED DE TRABAJO DEL DEPARTAMENTO DE INGENIERÍA BIOMÉDICA | | | | | | | |
|---|---|---|---|---|---|---|---|
| USUARIO | HOST | IP | | | | CONEXIÓN | ASIGNACIÓN |
| CISCO | MÓDEM-ROUTER-AP | 192 | 168 | 1 | 254 | ETHERNET | IP-ESTÁTICA |
| D'LINK | DIR 400 - ROUTER-LAN | 192 | 168 | 0 | 1 | ETHERNET | IP-ESTÁTICA |
| SERVIDOR | IBHRAE | 192 | 168 | 0 | 2 | ETHERNET | IP-ESTÁTICA |
| RICOH | RICOH | 192 | 168 | 0 | 3 | ETHERNET | IP-ESTÁTICA |
| KONICA | KONICA | 192 | 168 | 0 | 4 | ETHERNET | IP-ESTÁTICA |
| ETIQUETAS | ETIQUETAS | 192 | 168 | 0 | 5 | ETHERNET | IP-ESTÁTICA |
| | | 192 | 168 | 0 | 6 | RANGO DE | |
| | | 192 | 168 | 0 | 7 | DIRECCIONES | |
| RANGO DE DIRECCIONES DISPONIBLES POR CRECIMIENTO LABORAL | | 192 | 168 | 0 | 8 | DISPONIBLES POR | |
| | | 192 | 168 | 0 | 9 | CRECIMIENTO | |
| | | 192 | 168 | 0 | 10 | LABORAL | |
| IVET | MXL1201Z19 | 192 | 168 | 0 | 11 | ETHERNET | IP-ESTÁTICA |
| PABLO | PABLO-PC | 192 | 168 | 0 | 12 | ETHERNET | IP-ESTÁTICA |
| | | 192 | 168 | 0 | 13 | | |
| | | 192 | 168 | 0 | 14 | RANGO DE | |
| | | 192 | 168 | 0 | 15 | DIRECCIONES | |
| RANGO DE DIRECCIONES DISPONIBLES POR CRECIMIENTO LABORAL | | 192 | 168 | 0 | 16 | DISPONIBLES POR | |
| | | 192 | 168 | 0 | 17 | CRECIMIENTO | |
| | | 192 | 168 | 0 | 18 | LABORAL | |
| | | 192 | 168 | 0 | 19 | | |
| ARTURO | HP | 192 | 168 | 0 | 20 | WI-FI | IP-DINÁMICA |
| MARIO | BBMAR | 192 | 168 | 0 | 21 | WI-FI | IP-DINÁMICA |
| ALMA | Miguel Fuentes | 192 | 168 | 0 | 22 | WI-FI | IP-DINÁMICA |
| OSORIO | EDUCTRADE-IMAGE | 192 | 168 | 0 | 23 | WI-FI | IP-DINÁMICA |
| CARLOS | EDUCTRADE-CE | 192 | 168 | 0 | 24 | WI-FI | IP-DINÁMICA |
| NAPOLEON | NAPOLEON-HP1 | 192 | 168 | 0 | 25 | WI-FI | IP-DINÁMICA |
| JORGE | LAPEDUCTRADE | 192 | 168 | 0 | 26 | WI-FI | IP-DINÁMICA |
| ERNESTO | PEDRO-PC | 192 | 168 | 0 | 27 | WI-FI | IP-DINÁMICA |
| IGNACIO | SEBAS-PC | 192 | 168 | 0 | 28 | WI-FI | IP-DINÁMICA |
| KAREN | MXL2011MST | 192 | 168 | 0 | 29 | WI-FI | IP-DINÁMICA |
| MARIA | MARIA-PC | 192 | 168 | 0 | 30 | WI-FI | IP-DINÁMICA |
| EMIGDIO | MARCOPOLO | 192 | 168 | 0 | 31 | WI-FI | IP-DINÁMICA |

# CONCLUSIONES DEL PROYECTO

Se visualizó que las arquitecturas de las redes empleadas no era la mejor en ese momento, y gracias al proyecto realizado se restructuraron las redes permitiendo que el trabajo del Departamento de Ingeniería Biomédica se agilice.

Al inicio de este trabajo, la seguridad en las redes era de nivel bajo, ahora la seguridad de las redes es de nivel medio y permite tener un control sobre los equipos que están dentro de la red de trabajo, con el control de las direcciones IP se mejoró el rendimiento del tráfico de red.

Se realizó la propuesta del rediseño, la administración y el monitoreo de las redes del Departamento de Ingeniería Biomédica. Se separaron los cables de red de los cables de corriente eléctrica, se descentralizó el uso exclusivo de una estación de trabajo.

Se identificaron las estaciones de trabajo y los clientes de las redes del Departamento de Ingeniería Biomédica, se logró que las direcciones IP no se dupliquen, se configuraron los puntos de acceso para filtrar las direcciones MAC de las estaciones de trabajo, se accede a los ficheros del servidor y se hacen las impresiones de hojas a color cuando es requerido, de etiquetas y órdenes de servicio sin problemas.

Por medio de la simulación de la red se pudo visualizar y determinar cuál era la mejor configuración de las estaciones de trabajo, se resolvieron los problemas que presentaba el Departamento de Ingeniería Biomédica.

Actualmente se cuenta con conectividad, disponibilidad, confiabilidad y seguridad con la implementación de las redes "Q5QHQW89", "A01B03V13" Y "H93H54Q3".

Para la red "Q5QHQW89" se utilizó una red híbrida entre una WLAN con topología tipo Infraestructura y una red con topología de árbol permitiendo administrar y monitorear la red de manera segura y confiable. La red "A01B03V13" permite tener un acceso a los dispositivos personales sin que cause conflicto en la red institucional y la red "H93H54Q3" permite que tanto invitados como proveedores de servicios trabajen de forma independiente.

Con base en la estrategia de solución propuesta se cubrieron tres aspectos sobresalientes y atendiendo a cada uno de ellos se logra contar con un sistema de comunicaciones, así, de esta forma se identifican los problemas puntuales y se propone implementar el conjunto de políticas de redes acorde a lo que requiere el Departamento de Ingeniería Biomédica.

En la estructura organizacional se tienen diferentes puestos o roles, los cuales son igualmente valiosos para el trabajo diario, ya que cada uno representa parte de la cadena del proceso, por lo que es importante que estos funcionen de tal forma que se tenga un cumplimiento eficiente y efectivo de las tareas solo de esta manera se podrá llegar al objetivo y a las metas planteadas.

Es importante mencionar que en el camino todo proceso es perfectible, por lo que se debe trabajar de la forma más eficiente, siempre y cuando la perfección no sea un obstáculo al cumplimiento de las metas.

Los beneficios adicionales son:

- Activar el control parental para bloquear el acceso a sitios web
- Monitorear la tabla de clientes
- Disponibilidad de direcciones IP para el crecimiento laboral

Las perspectivas a futuro con esta propuesta son mantener un control de las redes, dar de alta nuevos equipos cuando se requiere, minimizar los problemas de acceso a los ficheros del servidor.

Como tal mi experiencia en el área de Ingeniería Biomédica presenta problemas que se han podido resolver gracias a los conocimientos adquiridos en la carrera de Ingeniería en Computación en el módulo de Ingeniería Biomédica.

# GLOSARIO

***AES*** *(Advanced Encryption Standard).* Esquema de cifrado por bloque de tamaño fijo de 128 bits, con llaves de 128,192 o 256 bits respectivamente.

**AP** *(Access Point)* Puntos de Acceso. Es un dispositivo que sirve para crear una WLAN, ofreciendo cobertura inalámbrica a través de una o varias antenas que tiene incorporadas.

**BSSID** *(Basic Service Set IDentifier).* Utilzado en la red tipo ad-hoc.

***CCM*** *(Counter Mode with CBC-MAC).* Un modo de código con bloque definido, se puede utilizar con cualquier código de bloque de 128 bits pero normalmente se utiliza con AES.

***CCMP*** *(Counter-Mode with CBC-MAC Protocol)* 802.11i define el uso de AES con el método de operación CCM como CCMP. Es el protocolo de cifrado más fuerte para su uso en las redes inalámbricas de área local.

***EAP*** (*Extensible Authentication Protocol),* protocolo de autenticación extensible. Es un framework de autenticación usado habitualmente en redes WLAN Point-to-Point Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuente su uso en las primeras. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

***EAP-TLS*** El protocolo sólo autentica al cliente.

***EAPoL*** El Protocolo de Autenticación Extensible sobre Red.

***ESSID*** (*Extended Service Set Identifier)* Servicio Extendido de Identificación. Utilizado en la red tipo infraestructura.

***GPS*** *(Global Positioning System)* Sistema de Posicionamiento Global es un objeto que permite a una persona determinar en todo el mundo la posición de un objeto, una persona o un vehículo con una precisión hasta de centímetros.

***HOST*** (*Hardware Oriented Security and Trust)* anfitrión. Es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red. En general, los anfitriones son computadores monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, entre otros. Los usuarios que hacen uso de los anfitriones pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red. De forma general un anfitrión es todo equipo informático que posee una dirección IP y que se encuentra interconectado con uno o más equipos.

***IEEE*** *(Intitute of Electrical and Electronics Engineers).* Organización profesional que ha estandarizado las redes IEE 802.

***IP*** *(Internet Protocol)* Protocolo de Internet. Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

***MAC*** *(Medium Access Control)* control de acceso al medio. Función en las redes IEEE que arbitran el uso de la capacidad de la red y determina las estaciones a las que les permite utilizar el medio para la transmisión.

***MIC*** *(Message Integrity Code)*. Código de integridad del mensaje. Un valor calculado sobre un conjunto de datos protegidos para protegerlos frente al sabotaje. En la mayoría de los sistemas criptográficos, este valor se denomina código de autenticación de mensaje. 802.11 utiliza el algoritmo MIC para evitar la confusión con la capa de control de acceso al medio.

***OSI*** *(Open Systems Interconection)* Interconexión de sistemas abiertos. Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicación.

***PC*** *(Personal Computer)* Computadora personal, es un tipo de microcomputadora diseñada en principio para ser utilizada por una solo persona a la vez (aunque hay sistemas operativos que permiten varios usuarios simultáneamente, lo que es conocido como multiusuario)

***PCI*** *(Peripheral Component Interconnect)*, Interconexión de Componentes Periféricos es un bus de ordenador estándar para conectar dispositivos periféricos directamente a su placa base. Estos dispositivos pueden ser circuitos integrados ajustados en ésta o tarjetas de expansión que se ajustan en conectores.

***PCMCIA*** *(Personal Computer Memory Card International Association),* asociación internacional de tarjetas de memoria para computadoras personales.

***PDA*** *(Personal Digital Assistant)* es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

***P2P*** *(peer to peer)* Red de pares. Es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

***RADIUS*** (*Remote Authentication Dial-In User Service*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

***RC4*** Algoritmo de código propietario desarrollado por RSA Data Security y cuya licencia es muy cara. También se utiliza como base para WEP y evitar la existencia de implantaciones WEP de código libre debido a la amenaza de litigios por parte de RSA.

***RSN*** (Robust Security Network) Red de seguridad robusta.

***SITE*** Los Cuartos de Equipos, comúnmente llamados SITE de comunicaciones, proveen el espacio para albergar el equipo de telecomunicaciones y cómputo de una organización. El espacio del Cuarto de Equipos no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. Y debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de Cuartos de Equipos debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de comunicaciones.

***SSID*** *(Service Set Identtity)* Identificador del conjunto de servicio. Una cadena utilizada para identificar un conjunto de servicios extendido. Normalmente el SSID es una cadena de caracteres reconocibles. A menudo al SSID se le conoce como "nombre de la red"

***TCP*** *(Transmision Control Protocol)* Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina.

***TKIP*** *(Temporary Key Integrity Protocol)*. Protocolo de integridad de clave temporal. Uno de los protocolos de cifrado mejorados en 802.11i que utiliza las operaciones fundamentales de WEP con los nuevos mecanismos de comprobación e integridad y cifrado WEP para ofrecer una seguridad adicional.

***UCIN*** *(Unidad de Cuidados Intensivos Neonatales)* A menudo, los recién nacidos que necesitan cuidados médicos intensivos ingresan en un área especial del hospital denominada Unidad de Cuidados Intensivos Neonatales (UCIN). La UCIN combina tecnología avanzada y profesionales de la salud capacitados para brindarles cuidados especializados a los pacientes más pequeños. Las unidades de este tipo a veces cuentan con áreas de cuidados intermedios o continuos para los bebés que no se encuentran graves, pero que necesitan cuidados de enfermería especializada. Algunos hospitales carecen de este personal especializado o de una UCIN, y los bebés deben ser trasladados a otro hospital.

***UCINR*** *(Unidad de Cuidados Intensivos Neonatales) Referidos*

***USB*** (*Universal Serial Bus),* Bus Universal en Serie, es un bus estándar industrial que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.

***WEP*** *(Wired Equivalent Privacy).* Privacidad equivalente al cableado. Estándar para codificación individual de las tramas de datos. Se diseñó para proporcionar una privacidad mínima.

***Wi-Fi*** La Wi-Fi Alliance inicio el programa de certificación Wi-Fi (Fidelidad Inalámbrica) para aprobar la interoperatividad de la implantación 802.11. Originalmente el término se aplicaba a dispositivos que cumplían con 802.11b, ahora incluye la interoperatividad 802.11g y 802.11ª así como la seguridad WPA. La similitud con el término "Hi-Fi", del inglés *High Fidelity*, usado frecuentemente en la grabación de sonido, ha hecho creer erróneamente que el término "Wi-Fi" es una abreviatura de *Wireless Fidelity (*Fidelidad inalámbrica) en inglés.

***WLAN*** *(Wirless Local Area Network)*. Es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

***WPA y WPA2*** Acceso Wi-Fi protegido. Estándar de seguridad basado en el borrador 3 de 802.11i. Wi-Fi Alliance tomo el borrador 3 de 802.11i y empezó a certificar la conformidad con las primeras implantaciones TKIP para acelerar la adopción de los protocolos de seguridad de 802.11. WPA2 se basa en la versión totalmente ratificada de 802.11i.

**802.1X** es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 2284). El RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software *suplicante*. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad de WEP.

# REFERENCIAS


Armand St-Pierre, William Stéphanos *"Redes locales e internet"*

2001, Ed. Trillas pag. 74-78

Alberto León-García, Indra Widjaja *"Redes de comunicación conceptos fundamentales y arquitecturas básicas"*

Michael A. Gallo, *"Comunicación entre computadoras y tecnologías de redes"*

Thomson

William Stallings, *"Comunicaciones y Redes de Computadores"*

2008, 7ª Edición, Perarson Prentice Hall

Julio Gómez López*, "Guía de Campo Wi-Fi"*

RA-MA 2008

José A. Carballar, *"Wi-Fi Instalación, Seguridad y Aplicaciones"*

Alfaomega, 2007

José M. Huidobro Moya, David Roldán Martínez, *"Comunicaciones en redes WLAN"*

Limusa, 2006

Edson Armando Guerrero Martínez "Gestión de redes inalámbricas en la Facultad de Ingeniería"

Tesis, 2009

http://www.ieee802.org/11 Junio 2015

http://techterms.com/definition/p2p Abril 2015

http://standards.ieee.org/about/get/802/802.11.html Abril 2015

http://www.inegi.org.mx/geo/contenidos/geodesia/gps.aspx?dv=c1 Abril 2015

http://www.terra.com/salud/articulo/html/sal8078.htm Abril 2015

http://www.nlm.nih.gov/medlineplus/spanish/ency/patientinstructions/000590.htm Abril 2015

http://systemadmin.es/2011/01/que-diferencia-hay-entre-bssid-y-essid Abril 2015

http://searchwindowsserver.techtarget.com/definition/PCI-Peripheral-Component-Interconnect Abril 2015

www.informaticamoderna.com/Tarjetas_PCMCIA_inalam.htm Abril 2015

http://www.intel.com/content/www/us/en/io/universal-serial-bus/universal-serial-bus.html Abril 2015

http://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=e&word=eap-extensible-authentication-protocol Abril 2015

https://technet.microsoft.com/es-es/magazine/2008.02.cableguy.aspx Abril 2015

https://technet.microsoft.com/es-es/library/cc755248.aspx Abril 2015

http://www.redeszone.net/2012/09/10/mimo-que-es-para-que-sirve-todo-lo-que-necesitas-saber/ Mayo 2015

http://www.iret-telecom.net/Site.php Junio 2015

http://www.mastermagazine.info/termino/5270.php Junio 2015

Apuntes de la materia Redes de Datos Impartida por la Prof. M.C. Ma. Jaquelina López Barrientos

Apuntes de la materia Administración de Redes Impartida por el Prof. Ing. Juan José García Romero