FACULTAD DE INGENIERÌA Y CIENCIAS AGROPECUARIAS

# DISEÑO DE SEGURIDAD EN LA RED DE TRANSPORTE DE UN SISTEMA DE MEDICION DE EFICIENCIA ENERGETICA PARA LA UDLA

Autor

Santiago Israel Jácome Vásconez

Año
2018

FACULTAD DE INGENIERÌA Y CIENCIAS AGROPECUARIAS

# DISEÑO DE SEGURIDAD EN LA RED DE TRANSPORTE DE UN SISTEMA DE MEDICION DE EFICIENCIA ENERGETICA PARA LA UDLA

Trabajo de titulación de presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones.


Profesor guía

Msc. Carlos Marcelo Molina Colcha

Autor

Santiago Israel Jácome Vásconez


Año

2018

## DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido el trabajo, **Diseño De Seguridad En La Red De Transporte De Un Sistema De Medición De Eficiencia Energética Para La UDLA**, a través de reuniones periódicas con el estudiante **Santiago Israel Jácome Vásconez**, en el semestre **2018-1**, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Carlos Marcelo Molina Colcha

Magister en Tecnologías de la información y comunicación (TIC)

CI: 170962421-5

**DECLARACIÓN DEL PROFESOR CORRECTOR**

"Declaro haber revisado este trabajo, **Diseño De Seguridad En La Red De Transporte De Un Sistema De Medición De Eficiencia Energética Para La UDLA**, de **Santiago Israel Jácome Vásconez**, en el semestre **2018-1**, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Jorge Wilson Granda Cantuña
Magister en Ingeniería Eléctrica
CI: 170859418-7

**DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE**

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Santiago Israel Jácome Vásconez

CI: 171796279-7

**DEDICATORIA**

Dedico este proyecto de tesis a una persona muy especial en mi vida, y aunque no se encuentre físicamente conmigo, estará siempre en mi corazón y en mi mente sus recuerdos, enseñanzas y ese don que tenía en guiarme para ser un profesional, estoy recordando a mi hermano que en paz descanse (Cristian †), también a mi familia que siempre estuvo y estará apoyándome.

## RESUMEN

Las seguridades en las redes garantizan el funcionamiento de la red y del flujo de la información, se plantea diseñar la seguridad de red para el proyecto "Análisis de Eficiencia Energética" el cual presenta una solución eficiente del consumo energético para la Universidad de las Américas en las sedes Queri, Granados y Udlapark, utilizando sensores de energía para la obtención de datos en tiempo real, que son transmitidos inalámbricamente a una base de datos, a la cual pueden acceder los usuarios de manera remota a través de un software de gestión.

El siguiente proyecto diseño de seguridad en la red de un sistema de medición de eficiencia energética en la Udla, tiene como objetivo la seguridad, la confidencialidad, la disponibilidad e integridad de los datos mediante la implementación de mecanismos y políticas de seguridad.

Capítulo 1.- En este capítulo se mencionará toda la información teórica, tecnologías actuales que nos permitan realizar un diseño relacionado con el proyecto

Capítulo 2.- En este capítulo se realizará el levantamiento de la información actual de la red

Capítulo 3.- En este capítulo se realizará el diseño de la solución para la red tomando como referencia una metodología estándar, de tal forma que el resultado sea una red segura y confiable.

## ABSTRACT

Security in networks guarantee the functioning of the network and the flow of information. This proposal recommends the design of the network security for the project “Energy Efficiency Analysis”, which presents a productive solution to the consumption of energy for Universidad de las Américas in the campuses of Queri, Granados and Udlapark, by using energy sensors to obtain data in real time, which are transmitted wirelessly to a data base that is at the reach of the users remotely through a management software.

This project is a network security design of a system to measure the productivity of energy at Udla. The objective is security, confidentiality, availability and integrity of data through the implementation of safety mechanisms and politics.

Chapter 1.- In this chapter theoretical information will be mentioned as well as current technologies that will allow us to create a design related to the project.

Chapter 2.- The next chapter will describe how the current information from the network is gathered.

Chapter 3.- In this final chapter we will design the solution for the network, taking a standard methodology as reference in order to obtain a safe and reliable network

# ÍNDICE

# 1. CAPITULO I. FUNDAMENTOS TEÓRICOS

## 1.1. Introducción

En el presente capítulo se describirá los fundamentos teóricos básicos que se requiere conocer para el desarrollo del proyecto, iniciando desde la definición de la seguridad de la información, redes inalámbricas su clasificación, componentes estándares y protocolos de seguridad.

## 1.2. Seguridad de la información.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma. (Isaca, 2016).

Recordemos que la **seguridad en cómputo** se limita a la protección de los sistemas y equipos que permiten el procesamiento de la información, mientras que la **seguridad informática** involucra los métodos, procesos o técnicas para el tratamiento automático de la información en formato digital, teniendo un alcance mayor, ya que incluye la protección de las redes e infraestructura tecnológica.

## 1.3. Seguridad en las redes

La conexión de las redes por cable o de manera inalámbrica constituye la carretera por donde fluye la información, tales como correo electrónico, información financiera y archivos en general.

Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo, los ataques a una red pueden ser

devastadores y pueden causar pérdida de tiempo y de dinero producto de las afectaciones a la información o de archivos importantes.

A los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se les denominan “Piratas Informáticos”. Una vez que un pirata tiene el acceso a una red pueden surgir 4 tipos de amenazas:

- Robo de información
- Robo de identidad
- Perdida y manipulación de datos  Interrupción del servicio.

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa.

**Amenazas externas**: Provienen de personas que no tienen autorización para acceder al sistema o a la red de computadoras. Logran introducirse principalmente desde Internet, enlaces inalámbricos o servidores de acceso por marcación o dial-.

**Amenazas internas**: Por lo general, conocen información valiosa y vulnerable o saben cómo acceder a esta. Sin embargo, no todos los ataques internos son intencionados.

Con la evolución de los tipos de amenazas, ataques y explotaciones se han acuñado varios términos para describir a las personas involucradas

- *Hacker*: un experto en programación. Recientemente este término se ha utilizado con frecuencia con un sentido negativo para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

- *Hacker* de sombrero blanco: una persona que busca vulnerabilidades en los sistemas o en las redes y a continuación informa a los propietarios del sistema para que lo arreglen.
- *Hacker* de sombrero negro: utilizan su conocimiento de las redes o los sistemas informáticos para beneficio personal o económico, un cracker es un ejemplo de hacker de sombrero negro.
- *Cracker*: es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- *Phrieaker*: persona que manipula la red telefónica para que realice una función que no está permitida. Por lo general, a través de un teléfono público para realizar llamadas de larga distancia gratuitas.
- *Spammer*: persona que envía grandes cantidades de mensajes de correo electrónico no deseado, por lo general, los *spammers* utilizan virus para tomar control de las computadoras domésticas y utilizarlas para enviar mensajes masivos.
- Estafador: utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial como número de cuenta o contraseñas. (Seguridad informática, *Wikispaces*)

### 1.4. Redes inalámbricas

La red inalámbrica *(wireless network*) son sistemas de comunicaciones entre nodos por medio de ondas electromagnéticas la transmisión y la recepción se realizan a través de puertos dentro de una misma área de cobertura (Interior y/o exterior), sin la necesidad de un medio físico de transmisión. (Huidobro Maya José Manuel, 2011).

Proporcionan movilidad e interconexión en lugares con accesos muy limitados
En la Figura 1, se presenta un diagrama general de una red inalámbrica

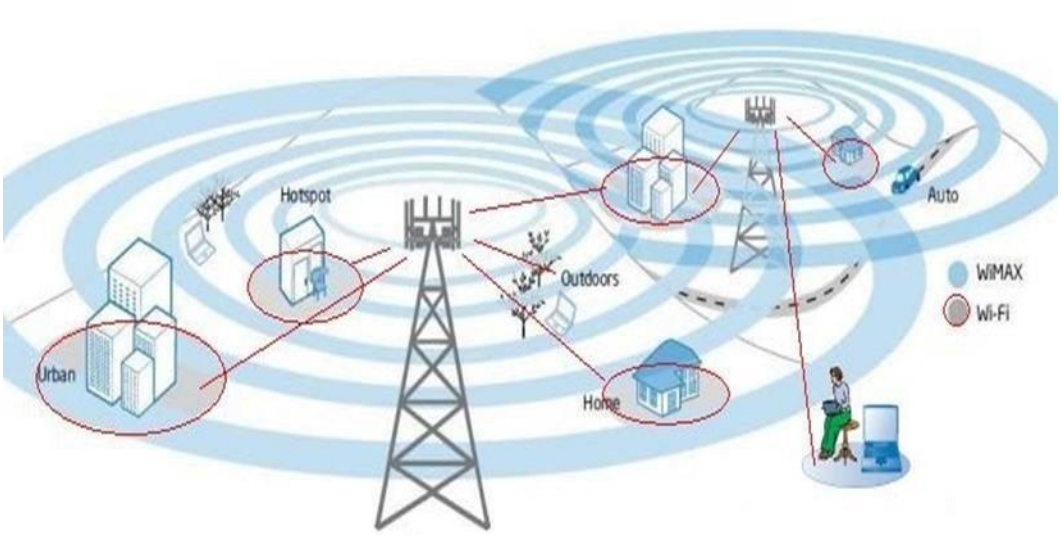



*Figura 1*. Redes inalámbricas.

Tomado de: Wiki Redes Inalámbricas (s.f.)

### 1.5. Componentes de un sistema inalámbrico

El sistema de comunicación inalámbrica es un conjunto de elementos que interactúan entre sí, son dispositivos de accesos al medio y dispositivos finales con el objetivo de intercambiar información sin la necesidad de la utilización de cables.

Los componentes en un modelo básico son:

Medio Aéreo

Es el componente principal en este tipo de sistemas que a pesar de no ser un medio tangible ese el medio por donde se propaga las señales inalámbricas.

Se radia energía electromagnética por medio de una antena esta se propaga por el medio aéreo y es recibida por otra antena, permitiendo de esta manera la intercomunicación de información sin la necesidad de un medio físico.

Dispositivos de Acceso al Medio

Una red inalámbrica requiere de una infraestructura tecnología adecuada que permita conectarse a la red e intercambiar información, este tipo comunicaciones son posibles con la integración de tarjetas inalámbricas o NIC (*Network Interface Card*) a los diferentes dispositivos finales de una red, que provee la interface y el radio que conecta el dispositivo de usuario final con la infraestructura de la red.

Las tarjetas inalámbricas pueden ser externas, internas, permanentes o desmontables, en la actualidad la mayoría de los dispositivos ya vienen incorporados de fábrica, como son en las computadoras portátiles*, Smartphone*, *tablets* etc. En la Figura 2. Se presentan los distintos tipos de tarjetas que existen en la actualidad.

*Figura 2*. Tarjetas inalámbricas.
Tomado de: Redes Inalámbricas (s.f.)

Estación Base:

Permite la comunicación de todos los dispositivos en un área determinada, tiene la capacidad de realizar las funciones de repetidor y amplificador de las señales inalámbricas, además de la interconectividad entre la red cableada. Procesa, direcciona y completa las llamadas generadas por los usuarios. En la Figura 3

se presenta una estación base más conocida como es el caso de *Acces Point*, encargada de interconectar equipos en un área determinada.

*Figura 3*. Estación Base
Tomado de: (*Wikispaces*, 2017 p. 171)

**1.6. Presupuesto de Potencia.**

El presupuesto de potencia no es más que el cálculo de toda la ganancia y pérdidas desde el transmisor hasta el receptor del enlace radioeléctrico. El cálculo debe constar desde la fuente de la señal de radio a través de los cables, conectores, y espacio libre hacia el receptor. (*Wireless Networking in the Developing World,* 2013) Este cálculo permite el correcto diseño de una red con una correcta elección de quipos.

Elementos del presupuesto de enlace.

Análisis en Transmisión

- **Potencia de transmisión**: Potencia generada en la salida del radio o antena (Estación base), Valor que se encuentra en las especificaciones técnicas del equipo. Sin embargo, los equipos que cumplen el estándar IEEE802.11 cuentan con una potencia que varía entre 15 – 26 dBm (30 - 40 mW). Cada país cuenta con su propia regularización vigente sobre los límites máximos de potencia a utilizar. (*Wireless Networking in the Developing World*, 2013)

- **Perdida de cable**: Es el valor medido en dBm que atenúa la potencia total producido por los cables que se conectan en el transmisor y el receptor que generan pérdidas variables dependiendo del tipo de cable, longitud y frecuencia de operación.
- **Perdida en conectores**: Se debe estimar por lo menos 0.25dB de pedida para cada conector en su cableado.
- **Amplificadores**: Son equipos de radio frecuencia que son implementados de manera opcional con el objetivo compensar las pérdidas o ampliar el área de cobertura de un enlace radioeléctrico, esta implementación puede resultar costosos, para lo cual el uso de las mismas debería considerar solo como última opción.
- **Ganancia de Antena**: Esta ganancia varía típicamente entre 2dBi (antena integrada simple) y 8dBi (omnidireccional) hasta 21-30 dBi (Parabólica).

Análisis de Propagación.

En el lado de propagación se debe tener en cuenta a la perdida de propagación que está relacionado con la atenuación que ocurre cuando la señal radioeléctrica sale de la antena de transmisión hasta que llega a la entena receptora.

- **Perdida en espacio libre:** Esta pérdida ocurre cuando el frente de onda de una señal producida por la potencia de un transmisor, sufre de ensanchamientos distribuyendo el frente de onda en áreas de mayor medida, efecto que se produce cada vez que la señal se aleja más del transmisor, consiguiendo que la densidad de potencia disminuya sin necesidad de que exista ningún tipo de obstáculo. (*Lightfoot*, 2013) La `FSL` o perdida de espacio libre se lo puede calcular mediante la siguiente formula:

  $$FSL(dB) = 20\log_{10}(d) + 20\log_{10}(f) - 187.5 \qquad \text{(Ecuación 1)}$$

  **D =**distancia (m)
  **F =** frecuencia (Hz)

**K =** Constante dependiente de d y f **187.5**

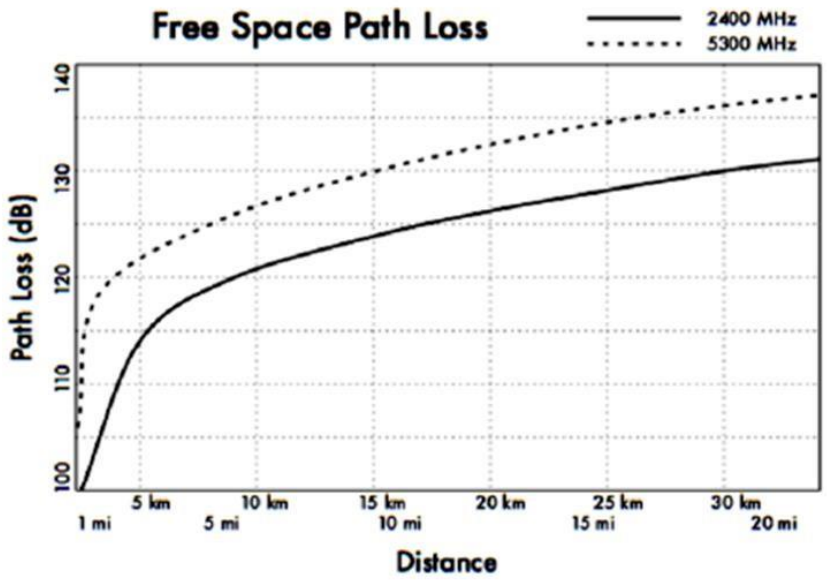



*Figura 4*. Perdida en dB en función de la distancia.
Tomado de: (*Wireless Networking in the Developing World*, 2013)

En la Figura 4, el gráfico muestra la pérdida en dB para 2.4 GHz y 5.4 GHz. Se puede observar que después de 1,5 km, las pérdidas son lineales.

Si se conoce las pérdidas de una señal a una frecuencia de 2.4 GHz, se puede calcular las pérdidas a 5Ghz añadiendo 8dB esto se evidencia mediante el cálculo de las perdidas con la formula dada. (*Lightfoot*, 2013). A continuación, la tabla 1, muestra las pérdidas de espacio libre tanto para las dos frecuencias con diferentes distancias.

Tabla 1.
*Perdidas en espacio Abierto*

| Distancia (Km) | 915 Mhz | 2.4 Ghz | 5.8 Ghz |
|---|---|---|---|
| 1 | 92 dB | 100 dB | 108 dB |
| 10 | 112 dB | 120 dB | 128 dB |

| | | | |
|---|---|---|---|
| 100 | 132 dB | 140 dB | 148 dB |

- **Zona de *Fresnel*:** La teoría exacta de las zonas de *Fresnel* (pronunciada "Fray-nell") es bastante complicada, pero en síntesis describe como una onda al propagarse interfiere consigo misma. Las zonas de *Fresnel* está compuesta por infinito número de capas como los de una cebolla, pero basta con despejar solo el 60% de la primera zona para la obtención de un enlace óptimo. La primera zona de *Fresnel* se limita a analizar el volumen elipsoidal alrededor de una línea recta entre el emisor y el receptor en un enlace radioeléctrico, con el objetivo de evitar que objetos como bosques, edificaciones o colinas, atenúen considerablemente la seña recibida aun cuando exista línea de vista directa entre dicho enlace.

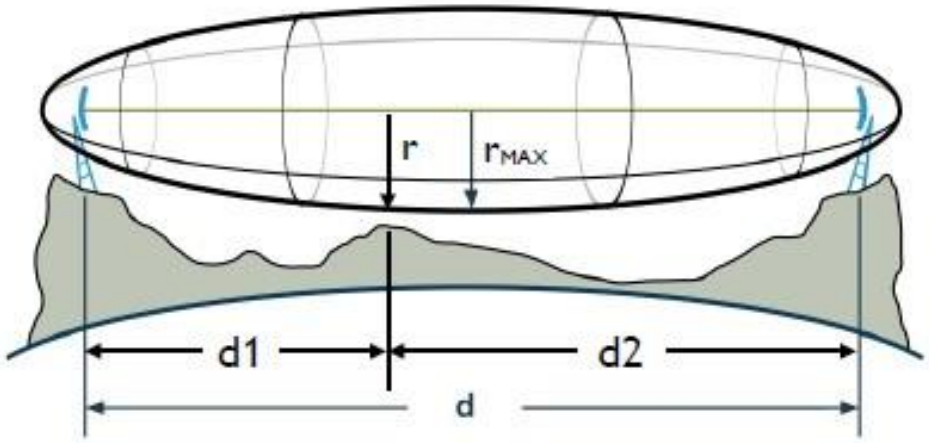



*Figura 2.* Zona de *Fresnel.*

Tomado de: (*Link Budget Calculation*, 2011)

En la figura 5 se ilustra los parámetros a considerar en el cálculo de la primera zona de *Fresnel* con el objetivo de que la potencia que alcance la antena receptora sea la máxima.

Para los cálculos la primera zona de *Fresnel* se utiliza la siguiente formula:

$$r = 17{,}32 * \sqrt{((d1 * d2)/(d * f))}$$ (Ecuación 2)

**d1=** distancia al obstáculo desde el transmisor (m)

**d2=** distancia al obstáculo desde el receptor (m)

**d=** distancia entre el transmisor y receptor (m) **f=** frecuencia (Mhz) **r=** radio (m)

Si el obstáculo está situado en el medio (d1=d2), la formula se simplifica:

$$r = 17{,}32 * \sqrt{(d/4\mathrm{f})}$$

Tomando el 60% nos queda

$$0{,}6r = 5{,}2 * \sqrt{d/f}$$

Lado Receptor

- **Potencia de Transmisión:** Cálculos idénticos al lado del transmisor.
- **Ganancia de antena Recepción:** Cálculo exacto de la Ganancia del transmisor.
- **Amplificador receptor:** Los cálculos y los principios son los mismos que el transmisor.
- **Sensibilidad del receptor:** Es el mínimo valor de potencia que se requiere para poder decodificar o extraer bits lógicos, cuando más baja es la sensibilidad mejor será la recepción del radio.

En la Figura 6. Se ilustra todos los componentes que integran para el cálculo del presupuesto de potencia para un enlace radioeléctrico.

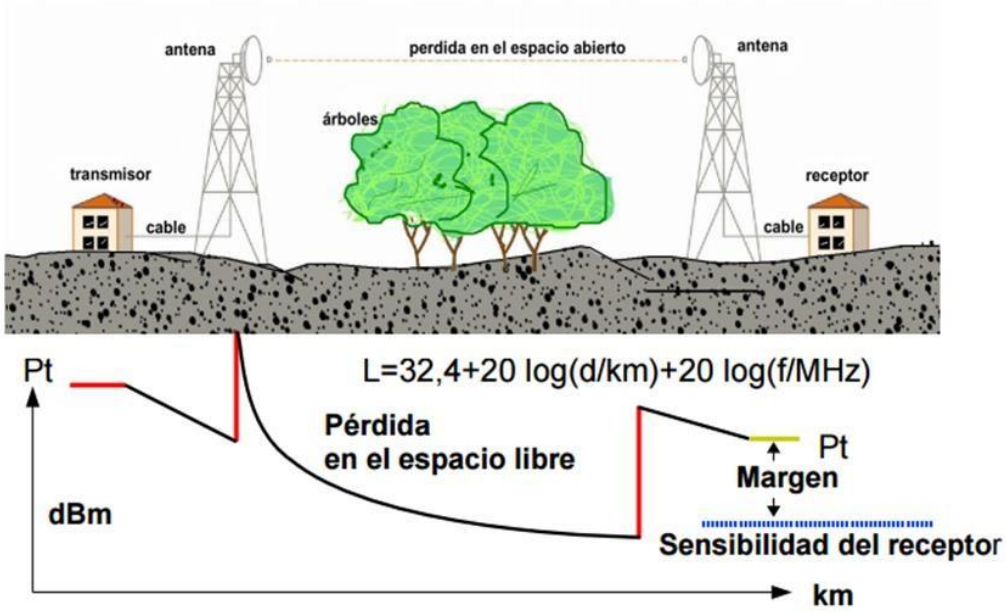



*Figura 6.* Elementos de un Radioenlace.
Tomado de: (Calculo de Radio enlace, 2007)

La ecuación del presupuesto de enlace se expresa mediante la siguiente formula en decibeles:

$$\mathbf{S(dBm) = Pt - A_T + Gt - Lfs + Gr - A_R} \qquad \text{(Ecuación 3)}$$

**Pt =** Potencia del Transmisor [dBm]
**$A_T$ =** Pérdidas en el Cable TX [dB]
**Gt =** Ganancia de Antena TX [dBi]
**Lfs =** Pérdidas en la trayectoria en el espacio libre [dB]
**Gr =** Ganancia de Antena RX [dBi]
**$A_R$ =** Pérdidas en el Cable RX [dB]
**S =** Margen – Sensibilidad del receptor [dBm]

En la figura 7 se observa los componentes lógicos para el cálculo de potencia en función de la distancia

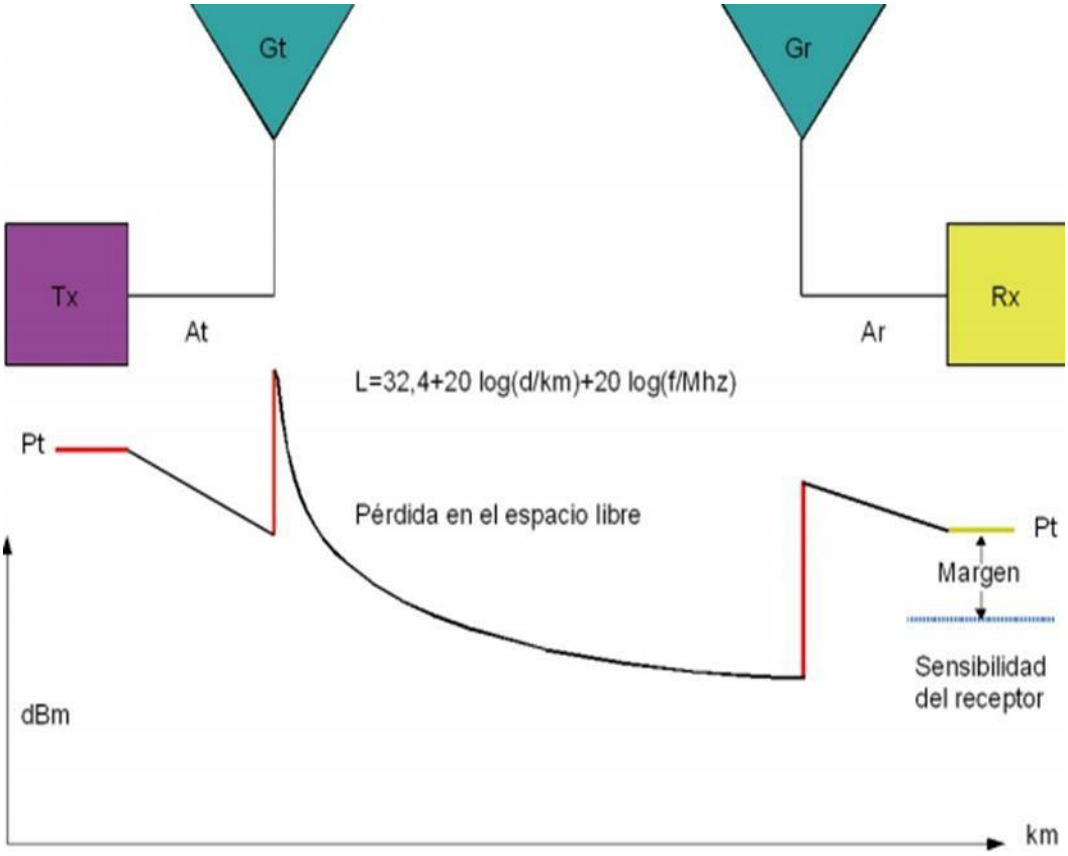
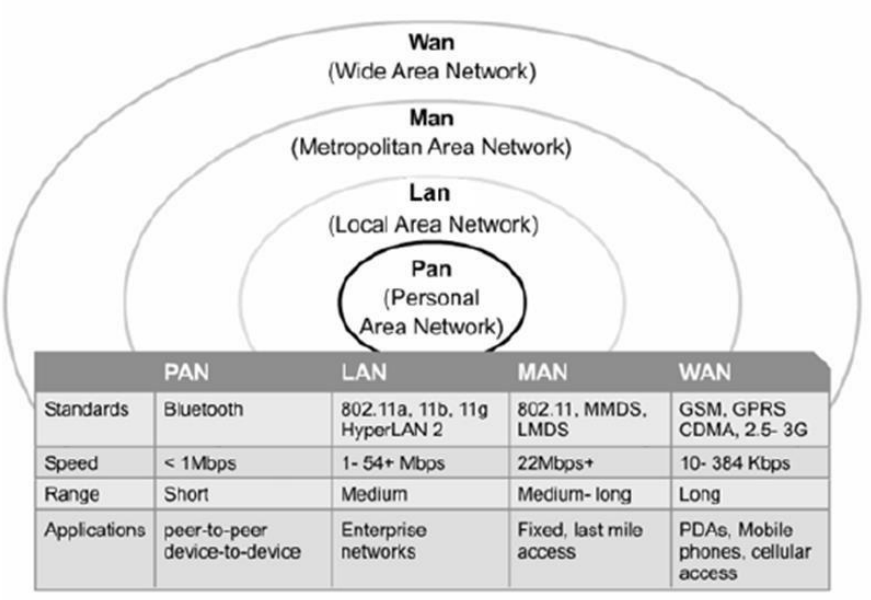



*Figura 7*. Diagrama Potencia en dB en función de la distancia.
Tomado de: (*Lightfoot,* 2013)

### 1.7. Clasificación de redes inalámbricas

Los sistemas inalámbricos se pueden clasificar dependiendo del área física que cubren, satisfaciendo así los diferentes tipos de aplicaciones de cada una de ellos. Figura 8 muestra dicha clasificación de una manera ilustrativa.




| | PAN | LAN | MAN | WAN |
|---|---|---|---|---|
| Standards | Bluetooth | 802.11a, 11b, 11g HyperLAN 2 | 802.11, MMDS, LMDS | GSM, GPRS CDMA, 2.5- 3G |
| Speed | < 1Mbps | 1- 54+ Mbps | 22Mbps+ | 10- 384 Kbps |
| Range | Short | Medium | Medium- long | Long |
| Applications | peer-to-peer device-to-device | Enterprise networks | Fixed, last mile access | PDAs, Mobile phones, cellular access |

*Figura 8*. Clasificación de las redes inalámbricas
Tomado de: (Curriculum Cisco WLAN, s.f)

**Redes Inalámbricas de Área Personal (WPAN**)

Las WPAN son redes una conexión inalámbrica de corto alcance, el rango de cobertura no excede más de 15m y cuenta con una velocidad de transferencias de información de 1 Mbps como máximo es decir su rendimiento es muy limitado. Los dispositivos que permiten este tipo de conexiones son como se muestra en la Figura 9 los que poseen los estándares Bluetooth, o Wifi directo habilitado ya sea PC, teléfonos móviles o PDA. (Seguridad informática, *Wikispaces)*

*Figura 9*. Redes inalámbricas de área personal

Redes Inalámbricas de Área Local (WLAN)

Este tipo de redes proporcionan un alto desempeño, tiene un alcance de alrededor de 30m y cuenta con una tasa de transmisión cercana a los 54Mbps, el cual permite conectar una red de computadores en una determinada localidad geográfica. La figura 10 presenta una arquitectura típica de una conexión inalámbrica de área local. *(Wikispaces)*


*Figura 10*. Diagrama de una red Inalámbrica

Tomado de: Informaticahoy (s.f.)

Redes Inalámbricas de Área Metropolitana (WMAN)

Las redes inalámbricas de área metropolitana, tiene un alcance de kilómetros cuenta con jerarquía de datos móviles y su aplicación más común es la interconexión de ciudades mediante transmisiones de microondas. El desempeño de las WMAN de la distancia a las que interconecta al igual que los componentes que se utilicen. (*Wikispaces)* La figura 11 tiene como objetivo de ilustrar una de las posibles arquitecturas de una red WMAN.

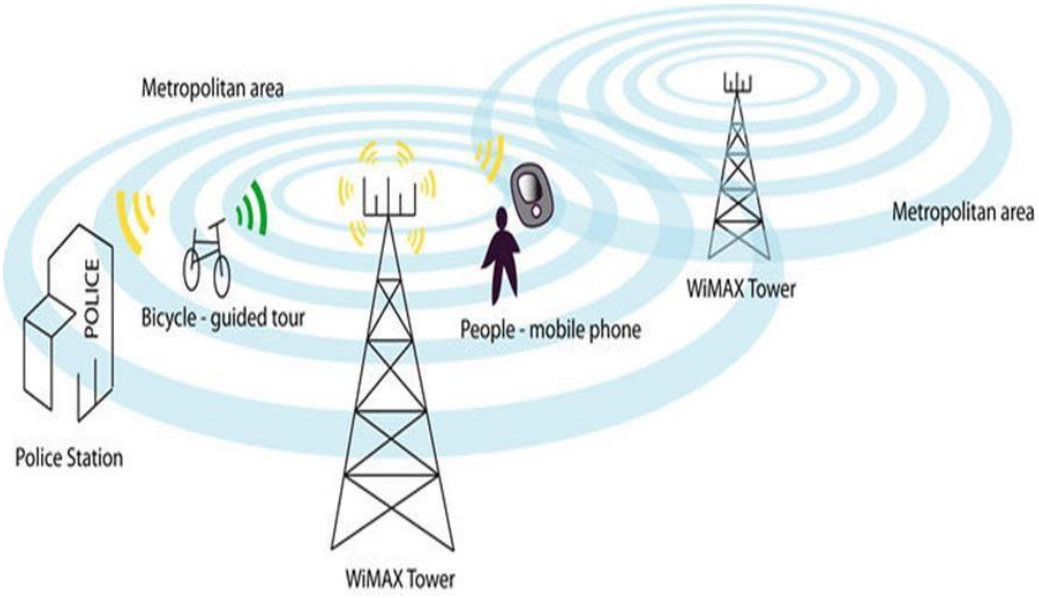



*Figura 11.* Redes inalámbricas de área metropolitana
Tomado de: (*The Industrial Desing Engineering wiki*, 2012)

Redes Inalámbricas de Área Extensa (WWAN)

Este tipo de redes cuentan con una cobertura en áreas extremadamente grandes, su alcance sobrepasa a todas las otras redes inalámbricas antes mencionadas, típicamente permiten a múltiples organismos como oficinas de gobierno, universidades y otras instituciones conectarse en una misma red. Este tipo de infraestructura son considerablemente costosas, generalmente los gastos son compartidos por todos los usuarios que utilizan la red. Las WWAN tradicionales hacen estas conexiones generalmente por medio de líneas telefónicas, o líneas estáticas. En la actualidad la principal aplicación de este tipo de redes es, en redes satelitales y redes de telefonía celular, ya que es posible abarcar un ámbito global que interconectan diferentes redes de varias empresas proveedoras del servicio utilizando itinerancia comúnmente conocido como *Roaming (Wikispaces).*

En la figura 12 se puede evidenciar claramente el área de cobertura que cuenta cada una de tipos de redes mencionadas en esta clasificación.

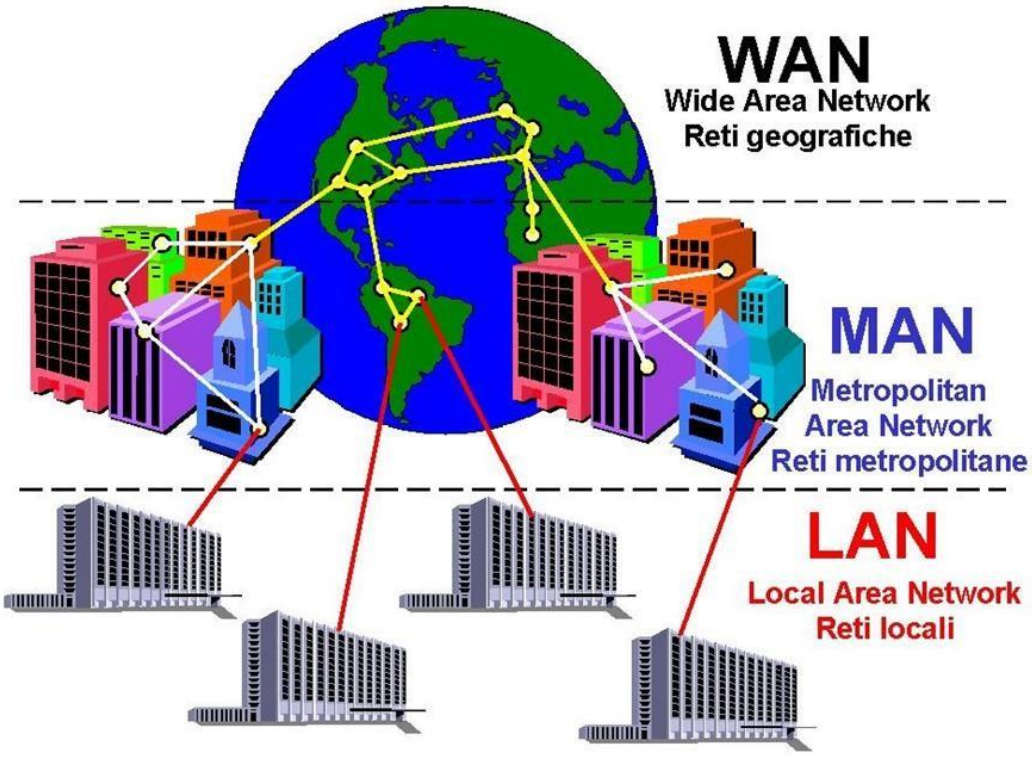



*Figura 12.* Área de cobertura delas redes inalámbricas.
Tomado de: vyiri. (s.f.)

Otros tipos de redes inalámbricas

Red Inalámbrica Punto a Punto.

Si se dispone de un bajo número de equipos distribuidos en un espacio reducido, hay dispositivos idóneos para poner en marcha una red inalámbrica independiente. En esta red se puede conectar un pequeño número de ordenadores de sobremesa, portátiles, PDAs, impresoras.

Red Inalámbrica con Punto de Acceso

El diseño e instalación de la red inalámbrica es adecuada en caso de que disponga de un alto número de equipos, o bien éstos se encuentren distribuidos en un edificio o en un espacio amplio. La red inalámbrica dispondrá de un Punto de Acceso que controlará el tráfico entre los dispositivos inalámbricos.

En la Figura 13 se ilustra el tipo de conexión punto a punto, así como punto multipunto.

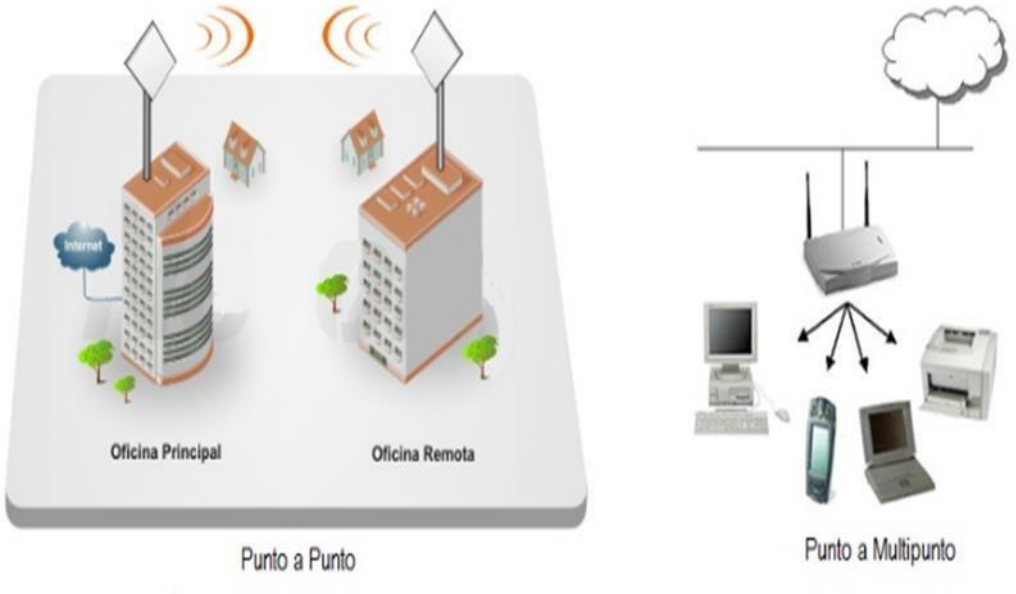



*Figura 13.* Conexión punto a punto y punto multipunto

Tomado de: Redes Inalámbricas (s.f.)

### 1.8. Estándares Inalámbricos IEEE.

Los Estándares son especificaciones desarrollados desde febrero de 1980 con el fin de integrar los diferentes tipos de tecnologías inalámbricas y lograr un trabajo conjunto, especialmente está enfocado en regularizar la fabricación de los componentes inalámbricos permitiendo y de esa manera la interoperabilidad de los mismos. La figura 14 se muestra los diferentes estándares creados de acuerdo a su clasificación.

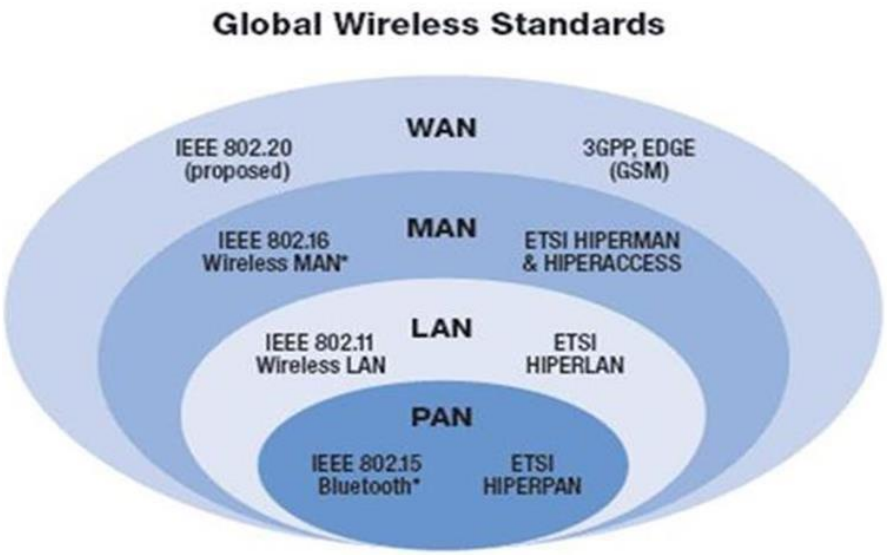



*Figura 14.* Estándares Inalámbricos IEEE.
Tomado de: (IEEE, 2016)

Estándar 802.15

Este estándar se presenta en una red inalámbrica de área personal (WPAN) con tecnología Bluetooth, es un estándar global que permite la comunicación inalámbrica entre varios dispositivos para transmisión de voz mediante un enlace por radio frecuencia segura. Esta tecnología que utiliza un rango de frecuencias de los 2,4 GHz a los 2,4835 GHz que interconecta a una distancia de 15 metros con una velocidad máxima de 5Mbps, especificaciones que fueron definidas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). (Bluetooth, 2016). La figura 11 se ilustra el logo característico de la tecnología Bluetooth.


*Figura 15.* Logo- Tecnología Bluetooth
Tomado de: *Androidpit* (s.f.)

Estándar 802.16.

Estándar nominado oficialmente como *Wireless* MAN o "*WiMAX" (Worldwide Interoperability for Microwave Access*), también conocido como tecnología de última milla. Especificaciones definidas por la IEEE para las redes de acceso metropolitanas inalámbricas de banda ancha fija, que permite la trasferencia de información por enlaces microondas (IEEE 802.20 -*Workshop*, 2011). Este tipo de tecnología resultan ser muy atractivas ya que permiten altas tasas de transmisión en coberturas extensas, posibilita las implementaciones movilidad y calidad de servicio, cuenta con las siguientes características:

- Las tecnologías *WiMAX* operan en bandas licenciadas (2.3GHz y 3.5 GHz) para enlaces radioeléctricos con larga distancia y en bandas no licenciadas entre 5.8 GHz, 8 GHz y 10 GHz, tomando en cuenta las asignaciones del espectro cada región o país cuente. (Facultad de Ingeniería UNAM , 2011, pág. 57).
- Se basa en OFDM14, puede cubrir distancias muy amplias que abracan campus enteros incluso ciudades pues el rango está en el orden de 50 km, con la utilización de antenas direccionales y de alta ganancia, tiene eficiencia espectral de 5 bps/Hz y tasa de transmisión de hasta 128 Mbps. (Facultad de Ingeniería UNAM , 2011, pág. 57)
- Maneja velocidades de hasta 70 Mbps, 35+35 Mbps, siempre que el espectro este completamente limpio.
- Permite la interoperabilidad con aplicaciones de video y voz en el mismo canal, apto para el uso de tecnologías de VoIP, videoconferencias y otras tecnologías de comunicación.

Estándar 802.20

Es un nuevo estándar desarrollado por MBWA (*Mobile Broadband Wireless Acces*) y patrocinado por el grupo IEE 802 y el comité de Normas y Redes del Área Metropolitana, estándar orientado específicamente a las comunicaciones de acceso móvil inalámbrico de banda ancha, mejor conocido como *MobileFi* el

estándar 802.11 proporciona mayor eficiencia en el transporte de paquetes basados en el protocolo IP.

Permite el despliegue rápido en todo el mundo, brindando un servicio rentable y asequible en todas partes del mundo, interoperable con múltiples proveedores móviles de redes de acceso inalámbrico de banda ancha, cuyo principal objetivo es satisfacer las necesidades de los usuarios finales, residenciales y comerciales. (IEEE 802.20 -*Workshop*, 2011). El estándar 802.20 cuenta con las siguientes características:

- Especificación de interfaz aérea PHY y en la capa de MAC, permitiendo inter-operar en sistemas móviles de acceso inalámbrico de banda ancha.
- Opera en bandas licenciadas por debajo de 3.5 Ghz.
- Optimizado para el transporte de datos IP.
- Permite la interoperabilidad con aplicaciones como VoIP, transferencias de video, correo electrónico y juegos *multiplayer*.

En la tabla 2, se detalla los valores típicos de las características técnicas estándar como velocidades de subida y bajada, y los valores con los diferentes tipos de duplexación que la estándar cuenta.

Tabla 2.
*Características de redes MBWA*

| CARACTERISTICAS | VALOR |
|---|---|
| Velocidad Vehicular en movimiento | sobre 250 Km/h |
| Eficiencia espectral | Mayor a 1 b/s/Hz/celda |
| Máxima tasa de transmisión de datos DL | Mayor a 1Mbps |
| Máxima tasa de transmisión de datos UL | Mayor a 1 300 Kbps |

| | |
|---|---|
| Máxima Tasa de DL por celda | Mayos a 4Mbs |
| Máxima Tasa de UL por celda | Mayos a 800 Kb/d |
| Ancho de banda | 1,25 MHZ hasta 5 MHZ |
| Tamaño de celdas | Debe ser apropiado para lograr ubicación MANS y capaz de recurso de la infraestructura |
| Espectro máximo de operación de frecuencia | Menor a 3,5 GHZ |
| Espectro (arreglos de frecuencia) | Soporta arreglos de frecuencia en FDD |
| Espectro de asignación | Espectro de asignación licenciado para el servicio móvil. |
| Seguridad | AES (Estándar de encriptación ) |

Estándar 802.11

El estándar denominado así por la IEEE opera en las bandas de frecuencia ISM sin licencia. Implementada para brindar acceso a la red a usuarios domésticos y empresariales, que permiten incluir tráfico de datos, voz y video a distancias de hasta 300m (*Wikispaces*).

Con el fin de contar con mejores anchos de banda el estándar IEEE ha venido definiendo ciertas variantes que operan en diferentes frecuencias y variedad de ancho de banda. Estas especificaciones se realizaron basándose en tecnologías de microondas y con técnicas de *Spread Spectrum*, que a continuación se detalla las características de cada una de las variantes del estándar:

- **IEEE 802.11:** Estándar no vigente al momento, creado en 1997, es la especificación de WLAN original, definía el uso de la capa física y la capa

de enlaces de datos del modelo OSI. Manejaba velocidades de hasta 2Mbps bajo la banda de 2,4 GHz. (IEEE 802 LAN/MAN *Standards*, 2016)

- **IEEE 802.11a:** Estándar aprobado en 1999 por la IEEE, funciona en la banda de frecuencia de 5 GHz y velocidades de hasta 54 Mb/s. Utiliza como técnica de modulación la Multiplicación por división ortogonal de Frecuencia (OFDM). Todos los dispositivos que operan en este estándar no son compatibles para operar conforme los estándares 802.11b y 802.11g.
- **IEEE 802.11b**: Estándar aprobado en 1993 por la IEEE, utiliza la banda de frecuencia de 2,4 GHz y ofrece velocidades de hasta 11 Mb/s. Maneja Espectro Amplio mediante Secuencia Directa (DSSS) como técnica de modulación.
- **IEEE 802.11g:** Estándar ratificado en el 2003 cuenta con una velocidad de 54Mbps sobre la banda de los 2.4 Ghz, su técnica de modulación es OFDM, el estándar es compatible con el estándar 802.11b.
- **IEEE 802.11n**: Estándar aprobado en el 2009, operan en las bandas de frecuencia de 2,4 GHz y 5 GHz, y se conoce como “dispositivo de doble banda”. Cuenta con velocidades de operación que van desde150 Mb/s hasta 600 Mb/s, tienen un alcance de hasta 70 m (0,5 mi). Este estándar es compatible con dispositivos 802.11a/b/g anteriores, su limitante al aplicar en un entorno mixto es que sus velocidades de datos serán menores a las previstas. (*Wikispaces*)
- **IEEE 802.11ac**: Estándar aprobado en el 2013, operan en la banda de frecuencia de 5 GHz y cuenta velocidades de datos que van desde 450 Mb/s hasta 1,3 Gb/s (1300 Mb/s). Utiliza la tecnología MIMO para optimizar el rendimiento de la comunicación. Cuenta con la capacidad de incorporar hasta ocho antenas. Este estándar es compatible con dispositivos 802.11a/n anteriores, su limitante al aplicar en un entorno mixto es que sus velocidades de datos serán menores a las previstas. (*Wikispaces*)

- **IEEE 802.11ad:** Estándar aprobado en el 2013 y también conocido como "*WiGig",* utiliza una solución de *Wi-Fi* de triple banda con 2,4 GHz, 5 GHz y 60 GHz, y cuenta con velocidades de hasta 7 Gb/s. este estándar está diseñado para comunicaciones directas de corto alcance a gran velocidad, Hace el uso de la banda de 60 GHz que requiere necesariamente línea de visión directa, por lo tanto, no puede penetrar
  las paredes o techos. Compatible con bandas de 2.4 y 5 GHz, su limitante al aplicar en un entorno mixto es que sus velocidades de datos serán menores a las previstas. (*Wikispaces*).

En la tabla 3 se presenta un cuadro comparativo resumido, realizado en base a las características detalladas en la clasificación ya anteriormente mencionado.

Tabla 3.

Tabla comparativa de los estándares 802.11

| **Estándar IEEE** | **Velocidad Máxima** | **Frecuencia** | **Comparación con versiones anteriores** |
|---|---|---|---|
| 802.11 | 2 Mb/s | 2.4 GHz | |
| 802.11a | 54 Mb/s | 5 GHz | |
| 802.11b | 11 Mb/s | 2.4 GHz | |
| 802.11g | 54 Mb/s | 2.4 GHz | 802.11b |
| 802.11n | 600 Mb/s | 2.4 GHz y 5 GHz | 802.11a/b/g |
| 802.11ac | 1.3 Gb/s | 5 GHz | 802.11a/n |
| 802.11ad | 7 Gb/s | 2.4 GHz, 5 GHz, 60 GHz | |

## 1.9. Protocolos de Seguridades en Redes Inalámbricas

Protocolo de seguridad WEP

*Wired Equivalent Privacy* o Privacidad Equivalente al cable, protocolo implementado por la IEEE 802.11 para dotar de seguridad a las redes inalámbricas. Su principal objetivo es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalentes a las redes cableadas, además de impedir que usuarios no autorizados intenten acceder a la red.
Proporciona un cifrado a nivel 2, basado en algoritmo de cifrado CR4.

Lamentablemente el protocolo contaba con unas serias vulnerabilidades que a lo largo del tiempo fueron eliminando por completo la utilización de este tipo de protocolos de seguridad.

La Tabla 4 muestra de forma breve y cronológica las vulnerabilidades que presentaba este protocolo y que lo llevo a la extinción de la misma.

Tabla 4.
Descripción cronológica delas vulnerabilidades de WEP

| Fecha | Descripción |
|---|---|
| Septiembre 1995 | Vulnerabilidad RC4 potencial (Wagner) |
| Octubre 2000 | Primera publicación sobre las debilidades de WEP: Insegura para cualquier tamaño de clave; Análisis de la encapsulación WEP (Walker) |
| Mayo 2001 | Ataque contra WEP/WEP2 de *Arbaugh* |
| Julio 2001 | Ataque CRC *bit flipping* – *Intercepting Mobile Communications: The Insecurity* of 802.11 (Borisov, Goldberg, Wagner) |
| Agosto 2001 | Ataques FMS – Debilidades en el algoritmo de programación de RC4 (Fluhrer, Mantin, Shamir) |

| | |
|---|---|
| Agosto 2001 | Publicación de *AirSnort* |
| Febrero 2002 | Ataques FMS optimizados por h1kari |
| Agosto 2004 | Ataques KoreK (IVs únicos) – publicación de chopchop y chopper |
| Julio/agosto 2004 | Publicación de *Aircrack* (Devine) y *WepLab* (Sánchez), poniendo en práctica los ataques KoreK. |

Tomado de: (Guillaume Lehembre, 2005)

PROTOCOLO DE SEGURIDAD WAP

La arquitectura WAP o Acceso Protegido a *WiF*i surge después del deceso de WEP, este protocolo fue diseñado para ser usado junto a un servidor AAA, de esta forma se asignaba diferentes claves a cada uno de los posibles usuarios conectados a la red, sin embargo, para el uso doméstico también se tiene la configuración WAP-PSK, es menos segura, pero permite la conexión con una única clave compartida (*Pre-shared key*- PSK). WAP utiliza TIK (*Temporal Key Integry Protocol)*, protocolo que permitió la destitución de WEP cuyo propósito fue la de no sustituir el hardware existente y que solo se requería actualización del firmware para su funcionamiento. (Análisis entre WEP y WAP, 2008)

PROTOCOLO DE SEGURIDAD WAP 2

El protocolo WAP 2 es la versión certificada de WAP y que es parte del estándar IEEE 802.11i lanzado en septiembre del 2004 provee un ambiente escalable y extensible para el desarrollo de aplicaciones para dispositivos de comunicaciones móviles. Esto se logró a través de un diseño de capas de la pirámide completa del protocolo, es decir que cada capa de la arquitectura es accesible por las capas superiores, así como por otros servicios y aplicaciones. Utiliza un protocolo de cifrado AES, su utilización requirió cambio de hardware a uno más actual. (Análisis entre WEP y WAP, 2008).

# 2. CAPITULO II. LÍNEA BASE ESTADO DEL ARTE REDES WSN

Este Capítulo describe el estado del arte de las Redes Inalámbricas de Sensores (WSN), en el cual convergen componentes de (*hardware, software* y de ingeniería de redes), cada uno realizando sus funciones propias y diferentes entre estos. Por consiguiente, en este Capítulo resume cada uno de los aspectos fundamentales que caracterizan a los sistemas basados en redes de sensores.

## 2.1. Introducción

Las redes de sensores inalámbricas difieren con respecto a sensores autónomos, ya que de manera implícita asumen diferentes puntos de observación y la necesidad de organizarse en red para poder ejecutar tareas funcionales básicas (comunicación hacia el centro de control, por ejemplo) o tareas cooperativas de nivel aplicación.

Estas redes se basan en el concepto de nodo sensor autónomo de bajo coste que dispone de recursos limitados en términos de cálculo y capacidad de almacenamiento de información, baja potencia de transmisión y recursos sensores variados. Se caracterizan por un tamaño extremadamente reducido y una ingeniería orientada a la eficiencia energética (normalmente las plataformas se gestionan según un paradigma orientado a eventos que supone que el dispositivo está en un estado de bajo consumo durante gran parte de su ciclo de vida) y al entorno de red. La transmisión (y la recepción) suelen considerarse operaciones críticas en términos de recursos energéticos y, por lo tanto, aconsejan la utilización de estándares de comunicación de baja potencia expresamente diseñados para soportar eficientemente el tráfico a ráfagas de pequeñas cantidades de datos en entornos de comunicación multi-salto. Aunque no sea habitual, se pueden encontrar diferentes plataformas que difieren de forma importante respecto al modelo de bajo coste por una o más características (comunicación de largo alcance, por ejemplo). Las redes inalámbricas de

sensores de bajo coste contienen implícitamente una (o más) estación base también denominadas sumideros (*sink*). Una estación base suele ser un dispositivo caracterizado por recursos más potentes respecto a los de un dispositivo sensor y suele actuar, respecto a la red circundante, como el punto de destino de toda la información generada y retransmitida por los nodos sensores. Una estación base que también proporciona funciones de pasarela para la información hacia centros de control o de mando remoto asume el rol de *Gateway*, cuando este dispositivo tiene interconexión a dos redes de comunicación diferentes. También existen otros actores con funciones específicas que pueden ser parte activa de la red: se consideran actores de interés todos aquellos dispositivos que pueden actuar o modificar su comportamiento a consecuencia de observaciones, medidas o comportamiento de componentes sensores. El campo de aplicación de las redes de sensores inalámbricos es muy variado y extendido (Figura 16): tanto en el sector civil como el militar, para aplicaciones orientadas a: la adquisición de datos; monitorización y control de procesos; aplicaciones médicas y cuidado de salud; aplicaciones para seguridad; vigilancia y seguimiento; aplicaciones para agricultura y ganadería; automoción; control de tráfico; monitorización ambiental; de estructuras y de fenómenos naturales; entre otras muchas.

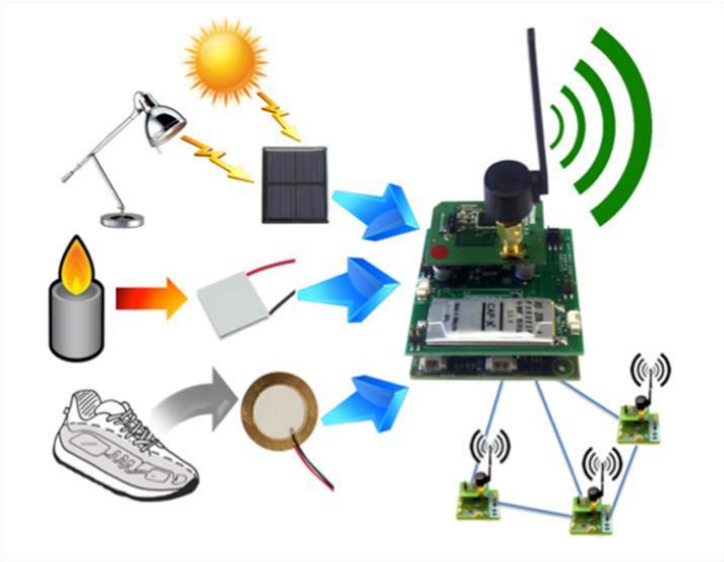


*Figura 16.* Esquema de funcionamiento redes WSN
Tomado de: *Cairn Wireless Sensor Network* (s.f.)

## 2.2 Ámbitos de Aplicación.

El uso de redes de sensores inalámbricos no solo puede observar sino también reaccionar para activar funciones de otros sistemas, estas tienen distintos usos como vemos a continuación:

- **Eficiencia Energética:** Red de sensores se utilizan para controlar el uso eficaz de la electricidad, como el caso de Japón y España.
- **Entornos de Alta Seguridad:** Existen lugares que requieren altos niveles de seguridad para evitar ataques terroristas, tales como centrales nucleares, aeropuertos, edificios del gobierno de paso restringido. Aquí gracias a una red de sensores se pueden detectar situaciones que con una simple cámara sería imposible.
- **Sensores ambientales:** El control ambiental de extensas áreas de bosque o de océano, sería imposible sin las redes de sensores. El control de múltiples variables, como temperatura, humedad, fuego, actividad sísmica, así como otras. También ayudan a expertos a diagnosticar o prevenir un problema o urgencia y además minimiza el impacto ambiental de la presencia humana.
- **Sensores industriales:** Dentro de fábricas existen complejos sistemas de control de calidad, el tamaño de estos sensores les permite estar allí donde se requiera.
- **Automoción:** Las redes de sensores son el complemento ideal a las cámaras de tráfico, ya que pueden informar de la situación del tráfico en ángulos muertos que no cubren las cámaras y también pueden informar a conductores de la situación, en caso de atasco o accidente, con lo que estos tienen capacidad de reacción para tomar rutas alternativas.
- **Medicina:** Es otro campo bastante prometedor. Con la reducción de tamaño que están sufriendo los nodos sensores, la calidad de vida de pacientes que tengan que tener controlada sus constantes vitales (pulsaciones, presión, nivel de azúcar en sangre, etc.), podrá mejorar sustancialmente.

- **Domótica:** Su tamaño, economía y velocidad de despliegue, lo hacen una tecnología ideal para domotizar el hogar a un precio asequible.
- **Internet de las Cosas:** Con el advenimiento de IoT, el ámbito de aplicación de las redes de sensores inalámbricos es prácticamente ilimitado.

## 2.3 Tecnología Básica

La tecnología básica hace referencia a la ingeniería de los nodos inalámbricos en todos sus componentes: (hardware, específicamente a procesadores de bajo consumo, tamaño y memorias), tecnología inalámbrica de baja potencia (orientada a soportar eficientemente el tráfico, periódico o a ráfagas, de pequeñas cantidades de datos), componentes sensores y soluciones para la alimentación de los nodos (baterías).
Los avances en los componentes sensóricos es clave para la utilización masiva de redes de sensores inalámbricas. Existe una gama de componentes de medida avanzados (temperatura, humedad, acústico, magnetómetro, acelerómetro, presencia, detectores químicos/biológicos, biomédicos, GPS y cámaras).

En las redes inalámbricas las baterías se consideran un elemento crítico en los nodos sensores como para las estaciones base.

### 2.3.1 *Hardware*

Los nodos se caracterizan por procesadores (FPGA, micro- controladores, micro-procesadores) de bajo consumo orientados a la máxima eficiencia energética. El concepto fundamental es la gestión del ciclo de vida del sensor que suele asumir una gestión orientada a eventos y que fuerza al dispositivo a trabajar durante la mayor parte del tiempo en un estado de consumo energético mínimo.

Las memorias utilizadas son integradas (volátiles) y flash (no volátiles); el tamaño de ambas se incluye en un rango de pocos *Kbytes* a unos *Mbytes*; las memorias no se suelen considerar componentes críticos en términos de coste de los nodos utilizados en este tipo de redes.

Las fuentes de alimentación portátiles actualmente se están proponiendo soluciones extremadamente avanzadas (alimentación mecánica o solar, por ejemplo) como alternativa a las baterías tradicionales (siempre más avanzadas).

#### 2.3.1.1. Arquitectura tipo MOTE

La empresa *Crossbow* es el mayor fabricante de nodos sensores y para aplicaciones reales desplegadas, estas plataformas se caracterizan por una ingeniería básica de tipo “MOTE”, diseñada y desarrollada por la Universidad de Berkeley, así como la plataforma software de gestión TinyOS. *Crossbow* también comercializa un conjunto completo de módulos sensores y dispositivos avanzados (GPS, Cámara) compatibles con los módulos inalámbricos proporcionados según una política orientada a favorecer el diseño y desarrollo de prototipos sin tener que recurrir al costoso hardware a medida que suele caracterizar productos finales.

La Arquitectura tipo MOTE incluye tres clases de dispositivos: nodos inalámbricos de bajo coste, nodos para control, nodos para aplicaciones avanzadas con requerimientos de recursos.

Nodos de bajo coste (Mica2, MicaZ, Iris), se caracteriza por componentes de base en línea con el concepto típico de nodo sensor (memorias del orden de los kbytes, etc.).

Nodos para control (TelosB), su peculiaridad es disponer de interfaces especiales (USB normalmente) para favorecer la comunicación directa con otros dispositivos electrónicos

Nodos avanzados (IMOTE2), se caracteriza por su memoria en *Mbytes* y plataformas de gestión (TinyOS o .Net Micro Framework), utiliza un procesador con características superiores respecto a lo de los demás dispositivos de la familia, este tipo de nodos está diseñada para soportar aplicaciones avanzadas (multimedia) que requieren alta capacidad de procesamiento local.

En la Figura 17 se representan las plataformas comerciales más relevantes proporcionadas por diferentes fabricantes.


*Figura 17.* Plataforma de Hardware
Tomado de: *Slideshare* Redes de Sensores Inalámbricos (s.f.)

2.3.1.2. Otras Soluciones de Hardware

Existen otras empresas que han proporcionado plataformas similares a los MOTEs o, bien, con características diferentes, ya que no existe una arquitectura estándar y todos los sistemas son propietarios. Las principales soluciones son:

**SENTILLA** (MoteIV) debe su popularidad principalmente a la comercialización de los nodos TMote, diseñados de acuerdo a la arquitectura tipo MOTE.

**SHOCKFISH** se sitúa como puente ideal entre mundo científico/académico y mundo real. Su mayor campo de acción es el entorno industrial por el cual ha diseñado y desarrollado la plataforma *TinyNode*, actualmente considera una de las pocas alternativas válidas a los nodos de tipo MOTE.

**BTNode** fabrica nodos sensores desarrollados por ETH *Zurich*; actualmente, dichos componentes son a la base de varios experimentos y proyectos de notable interés científico y comercial.

***Ember*** es una de las mayores promotoras de ZigBee Alliance; la tecnología desarrollada, basada en comunicación ZigBee, es ideal para soluciones escalables de bajo consumo que requieren topologías en mallas.

***Sun*** propone una interesante solución (*Sun* SPOT [Sun2]) basada en el estándar físico IEEE 802.15.4 operativa sobre máquina virtual *JAVA Squawk.*

**Nano-RK** ha desarrollado recientemente una solución de bajo coste y consumo (FireFly) con el objetivo primario de proporcionar pleno y eficiente soporte para servicios y aplicaciones de tiempo real.

### 2.3.2 Tecnología Inalámbrica

La tecnología inalámbrica es fundamental para el desarrollo de nodos sensores avanzados aptos al funcionamiento en el mundo real. El entorno de comunicación para nodos sensores inalámbricos de bajo coste se puede caracterizar como un medio orientado a soportar la transmisión de pequeñas cantidades de datos, transmitidos de manera periódica o impulsiva, utilizando transmisores de muy baja potencia en el contexto de redes *data-centric*. Estos requisitos orientan la tecnología inalámbrica de referencia hacia tecnologías inalámbricas para redes de área personal (PAN).

Anteriormente se utilizó transmisores con frecuencia entre 400 y 900Mhz. actualmente la tendencia propone frecuencias más altas (2.4Ghz). Una excepción significativa es representada por dispositivos que trabajan bajo el agua que suelen comunicar a través de tecnologías con frecuencias notablemente inferiores. Hay dos soluciones concretas, en términos de tecnología inalámbrica, actualmente en el mercado para aplicaciones en redes PAN: *Bluetooth* y ZigBee. El primero se caracteriza por un mayor ancho de banda y consumo energético, el segundo por una mayor cobertura y menor tasa de transmisión. Evidentemente las soluciones tipo ZigBee se adapta con más naturalidad que Bluetooth a las redes de sensores inalámbricas, posiblemente más indicado para redes personales de pequeña escala a soporte de aplicaciones *user-centric*

Una de las extensiones de las redes de sensores es para soporte de aplicaciones multimedia (Visual Sensor Networks) (nodos equipados con cámara, micrófono y/o otros sensores) que, posiblemente, podrían necesitar mayores capacidades, en términos de ancho de banda superiores a las proporcionadas por ZigBee. Esta clase de redes, aunque emergente, tiene gran importancia científica y de gran potencial comercial.

Tecnologías inalámbricas orientadas a proporcionar comunicación optimizada en entornos concretos (industriales) algunos ejemplos son *Wireless HART* e ISA100.

Independientemente de la tecnología considerada, se debe tomar en cuenta que un número importante de plataformas tan solo cumplen con una parte de los estándares de referencia, normalmente la capa física.

#### 2.3.2.1. Tecnología basada en 802.15.4: ZigBee y Xbee ZigBee

ZigBee se basa en el estándar físico IEEE 802.15.4 y propone la integración del estándar que se amplía con capas de niveles superiores (acceso al medio especialmente) de la pila de protocolos de comunicación.

IEEE 802.15.4 trabaja con frecuencia a 2.4Ghz, velocidad de 250Kbps y modulación DSSS. El estándar trabaja, por lo tanto, sobre las bandas ISM de uso no regulado. Se definen hasta 16 canales en el rango de 2,4 GHz, cada uno de ellos con un ancho de banda de 5 MHz. Zigbee está principalmente diseñado para el soporte de transmisión a baja potencia de pequeñas cantidades de datos siendo, por lo tanto, un estándar de gran perspectiva y potencialidad en diferentes campos de aplicación como WPAN, redes demóticas y redes de sensores inalámbricos. Es probablemente el estándar que mejor se adapta a las *Personal Area Networks* (PANs) y, por tanto, a las redes inalámbricas de sensores en cuanto ZigBee privilegia el bajo consumo respecto al ancho de banda, aunque proporcionando rangos de operación interesantes (hasta 75 metros). Otro punto fuerte de ZigBee, como se puede apreciar en Figura 18, es la robustez bastante superior a la garantizada por otros estándares. ZigBee propone dos posibles versiones de protocolo de acceso al medio para ampliar ulteriormente su campo potencial de aplicación: RFD (*Reduced Function Device*) *and* FFD (*Full Function Device*). El primero proporciona funcionalidades mínimas, el segundo pleno soporte para acceso al medio como en otros estándares.

La mayoría de los dispositivos sensores inalámbricos suelen hacer referencia a la solución básica (RFD) lo que proporciona al desarrollador la posibilidad de diseñar soluciones a medida (normalmente implementadas vía software como complemento de los protocolos de enrutamiento).

De esta forma se consigue optimizar la comunicación en entornos específicos, aunque limitando el nivel de abstracción en el desarrollo de los sistemas de comunicación. En su versión integral (que también incluye el nivel de red), ZigBee permite conectar un elevado número de nodos eventualmente distribuidos en subredes. No obstante, el nivel de red no es compatible entre las diferentes versiones de ZigBee, al no poder combinarse *routers* de versiones distintas. Un *router* ZigBee (ZR, *Zigbee Router*) es un tipo de dispositivo que básicamente interconecta nodos separados en la topología de red.

Estos nodos pueden ser o bien nodos finales (ZED, *ZigBee End Device*) o bien coordinadores (ZC, *ZigBee Coordinator*). *Xbee* es una variante de *ZigBee* a nivel físico y nivel de enlace de datos. A nivel físico, la diferencia fundamental es la variación progresiva del control de potencia para alcanzar

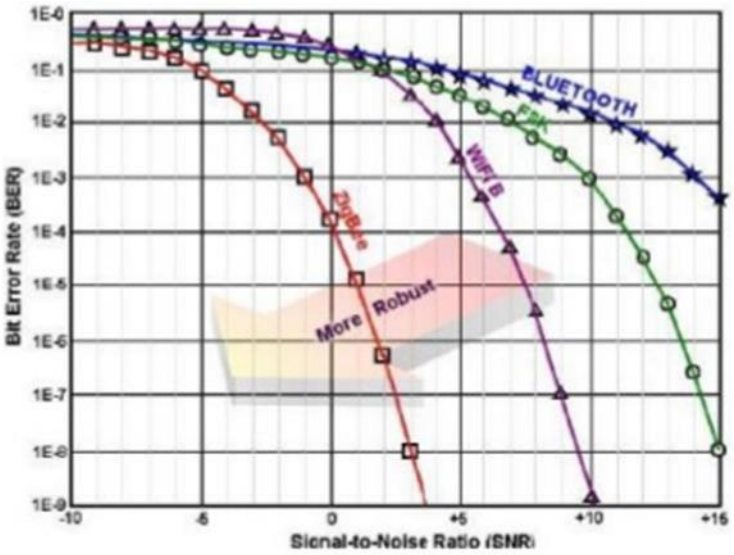



*Figura 18.* Relación señal a ruido (SNR) v/s tasa de errores por Bit
Tomado de: Wikipedia (s.f.)

2.3.2.2 Soluciones basadas en 802.15.1: *Bluetooth*

Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal normalmente empleado para posibilitar la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y

en banda ISM (2,4 GHz). Compatible con el estándar físico IEEE 802.15.1, proporciona, respecto a ZigBee, un mayor ancho de banda y un radio de comunicación inferior (en su versión de bajo consumo), normalmente a coste de un mayor gasto energético. La cobertura alcanzada por un dispositivo *Bluetooth* depende de la potencia de transmisión, criterio que clasifica a estos. Otra clasificación puede efectuarse respecto a la velocidad de transmisión (BT 1.0, con una velocidad de hasta 1 Mbps, y BT 2.0 con una velocidad de 3Mbps; los futuros dispositivos, UWB *Bluetooth*, con velocidades entre 50 y 480 Mbps). El estándar Bluetooth, análogamente a WiFi, emplea la técnica FHSS (*Frequency Hopping Spread Spectrum*), que divide la banda de frecuencia de 2.402 - 2.480 GHz en 79 canales (saltos) de 1 MHz y transmite la señal utilizando una secuencia de canales conocida tanto para la estación emisora como para la receptora.

Al cambiar de canal con una frecuencia de 1600 veces por segundo, el estándar Bluetooth puede evitar la interferencia con otras señales de radio. El estándar Bluetooth define un cierto número de perfiles de aplicación (denominados perfiles *Bluetooth*) para definir qué tipos de servicios ofrece un dispositivo Bluetooth. Por lo tanto, cada dispositivo puede admitir múltiples perfiles. Algunos de ellos son: Perfil de distribución de audio avanzado (A2DP), Perfil de control remoto de audio y vídeo (AVRCP), Perfil básico de imagen (BIP), Perfil básico de impresión (BPP), Perfil de telefonía inalámbrica (CTP) y Perfil de fax (FAX).

*Bluetooth* garantiza una conectividad notablemente inferior respecto a *ZigBee* a causa de su reducido radio de comunicación; el ancho de banda proporcionado se quedaría prácticamente desaprovechado visto el típico entorno de trabajo del tipo de redes que lo utilizan.

*Bluetooth* puede ser un válido antagonista de *ZigBee* o, incluso, proporcionar mejores prestaciones especialmente en un contexto de comunicación multimodo.

#### 2.3.2.3. Wireless HART

El estándar *WirelessHART* se basa en el estándar HART de amplia difusión, se concibió originalmente como una ampliación del bucle de corriente 4 a 20 mA común, con el fin de proporcionar dispositivos de campo con mayor funcionalidad. *WirelessHART* es la combinación entre la ampliamente difundida y probada tecnología *HART* y la nueva tecnología de radio (por lo menos, nueva en la tecnología de proceso). Además de la conocida aplicación HART para la parametrización de dispositivos, HART ya se ha utilizado ampliamente para: (i) Supervisión de valores de instrumentos y medioambientales; (ii) Gestión y optimización de activos; (iii) Mantenimiento preventivo; (iv) Supervisión del rendimiento y (v) Gestión de energía. *WirelessHART* utiliza la banda ISM como medio de transferencia como varias tecnologías de radio, incluido WLAN, *Bluetooth y ZigBee*. Con el fin de evitar colisiones en la banda de frecuencia de 2,4 GHz, *WirelessHART* lleva a cabo una búsqueda especial de los canales no utilizados en esta banda de frecuencia y comprueba las interferencias mutuas de las tecnologías de radio. Se considera, actualmente, una de las referencias para comunicación inalámbrica en entornos industriales.

#### 2.3.2.4. Wifi

Wifi es un sistema de envío de datos inalámbrico estandarizado en IEEE 802.11. Básicamente se trata de portar la flexibilidad de las redes Ethernet a un entorno radio, con las consiguientes adaptaciones de un medio inalámbrico. Existen varios estándares de 802.11. El primero de ellos, 802.11b permite velocidades de hasta 11 Mbps en la banda libre de 2.4 GHz. Nótese que, en un entorno radio donde la recepción de la señal es altamente variable, se emplean diferentes modulaciones para garantizar la robustez de la comunicación, a costa de sacrificar velocidad. Es por ello por lo que 802.11b permite descender hasta 2 Mpps si es necesario. El siguiente estándar, 802.11g permite velocidades de hasta 54 Mbps, opera en la banda libre de 2.4 GHz y es actualmente el más

utilizado en la actualidad, al permitir sesiones multimedia debido a su capacidad de transmisión y ser retro-compatible con 802.11b.

El estándar 802.11a opera hasta 54 Mpbs en la banda de 5 GHz, por lo que se pierde retrocompatibilidad en este aspecto, si bien esta banda está más libre de interferencias al no coexistir con otras tecnologías como BT, *Zigbee* y microondas. El último estándar recientemente aprobado es 802.11n, que permite velocidades de hasta 300 Mbps empleando modulaciones más robustas y sistemas MIMO.

La seguridad en redes Wifi es aportada a través de diferentes alternativas o protocolos de cifrado, como son WEP, WPA y WPA2, éste último el más seguro de todos. Otras mejoras relativas a la seguridad son el filtrado por MAC y el uso de túneles IP en VPNs.

Desde el punto de vista de la arquitectura, la conexión mediante Wifi requiere básicamente un punto de acceso (AP) que permite y coordina el acceso inalámbrico y el acceso a una red cableada (ya sea una LAN o directamente Internet).

Los clientes Wifi simplemente deben asociarse (y registrarse, si la autenticación lo requiere) a un punto de acceso Wifi para empezar a transmitir información. También es posible la comunicación entre dos clientes Wifi sin punto de acceso, mediante una configuración ad-hoc.

## 2.4 Arquitectura de protocolos

La arquitectura de protocolos que constituye el *software*, ejecutado por un nodo sensor inalámbrico, puede variar en función de los requisitos funcionales y no funcionales de la aplicación considerada; puede incluir tan solo funcionalidades extremadamente básicas, extender/integrar estas últimas o proporcionar un conjunto complejo de mecanismos avanzados. Aunque no exista, de momento,

un modelo de referencia universalmente reconocido para la pila de protocolos de una red inalámbrica de sensores, en el presente capitulo se hace referencia al modelo representado en Figura 1.5 A continuación se propone una clasificación esquemática de los principales protocolos que suelen componer el comportamiento de un nodo sensor inalámbrico

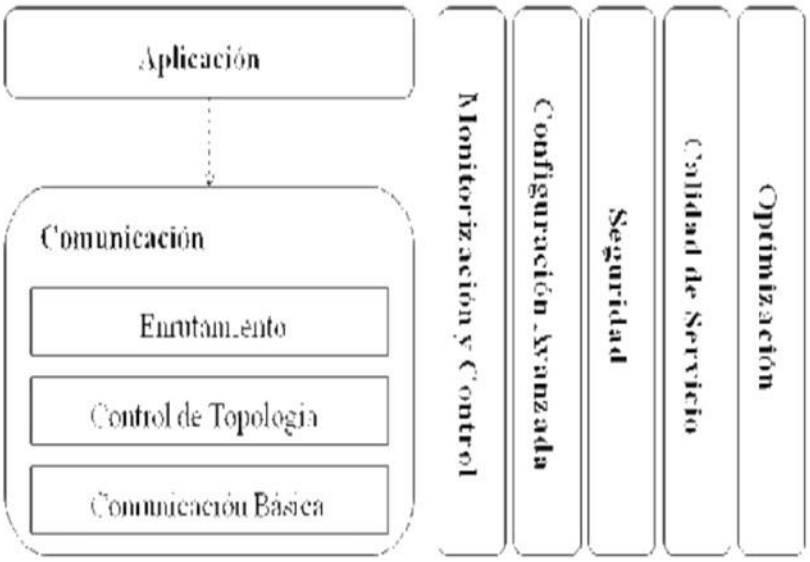



*Figura 19.* Modelo de referencia para la pila de protocolos de una red de sensores inalámbricos.

Tomado de: bibing (s.f.)

### 2.4.1 Funcionalidades de comunicación básicas

La mayoría de los nodos inalámbricos se comunica de acuerdo con la versión de funciones reducidas de *ZigBee* que, de hecho, no proporciona ninguna funcionalidad de acceso al medio.

Esta forma de funcionar aparentemente ineficiente e incómoda para el programador proporciona, realmente, un grado de libertad añadido al programador que puede, en función del dominio aplicativo considerado (y la relativa densidad de nodos), extender las funcionalidades de base para maximizar las prestaciones.

Considerando una tecnología inalámbrica de referencia extremadamente limitada a nivel de acceso al medio, cualquier red de una cierta densidad requiere una extensión de dichas funcionalidades básicas de comunicación para garantizar prestaciones aceptables. En un contexto de comunicación mono-salto, las funcionalidades de comunicación básica suelen constituir el único protocolo de comunicación.

La mayoría de las soluciones más eficientes se basan en TDMA; los protocolos de tipo TDMA suelen ser bastante más sencillos de los correspondientes para redes ad-hoc. La solución más lógica parece ser TDMA con *ack* que proporciona un protocolo de acceso al medio conforme a los adoptados en redes tradicionales; considerando las características peculiares de comunicación de los nodos sensores inalámbricos, en presencia de alta densidad, se prefiere replicar la información a través de múltiples rutas más que comunicación bidireccional (mensaje y confirmación).

Soluciones tipo TDMA suelen ser poco funcionales en el contexto de aplicaciones extremadamente impulsivas que requieren una comunicación extremadamente reactiva; un ejemplo clásico son las redes que detectan actividad sísmica. Para esta clase de aplicaciones suelen adoptarse soluciones de enrutamiento orientadas a privilegiar flujos impulsivos de datos que se caracterizan por intentar garantizar un cierto porcentaje de información correctamente trasmitido (y recibido); por lo tanto, resulta difícil considerar soluciones de acceso al medio estándar

### 2.4.2 Configuración básica o control de topología

Es un conjunto de protocolos orientados a proporcionar a la red la configuración mínima para garantizar sus funciones básicas, normalmente de enrutamiento. Por esta razón, en muchos casos esta clase de protocolo suele considerarse parte integrante del protocolo de enrutamiento, aunque soluciones altamente

flexibles multi-dominio y/o caracterizadas por múltiples modos de funcionamientos aconsejan una ingeniería altamente modular de acuerdo con los fundamentos de la ingeniería del software moderna. Normalmente el protocolo de configuración básica proporciona a cada nodo sus parámetros de configuración (normalmente resultado de operaciones de descubrimiento) junto con su visión del entorno (normalmente tabla de vecinos y características relacionadas). Eventualmente puede también proporcionar el conocimiento de ciertos parámetros (lógicos o físicos) relacionados con una parte restringida de nodos (normalmente de los vecinos) o de todos los nodos (configuración centralizada). Ejemplos típicos de información adicional, relacionada con los nodos de entorno, pueden ser la posición física (soporte de soluciones de enrutamiento *location-aware*) o la energía (soporte de protocolos de enrutamiento *energy-aware*). Otras funciones típicas se consideran la estimación de la estabilidad de las rutas (a soporte de los protocolos de enrutamiento que la requieren) y la diseminación dinámica de parámetros (por ejemplo, identificadores dinámicos de nodos o grupos).

### 2.4.3 Enrutamiento

El enrutamiento es la funcionalidad más relevante de una red de sensores inalámbricos; las prestaciones de la red completa dependen, en gran parte, de la eficacia del mecanismo de enrutamiento que suele tener una estricta dependencia de la configuración básica y avanzada (*clustering* por ejemplo) de la misma. Los protocolos de enrutamiento para redes de sensores inalámbricos han sido y siguen siendo objeto de gran interés para la comunidad científica. Desde el punto de vista del enrutamiento, una red de sensores inalámbricos se caracteriza por su topología (números de bases, números de nodos, densidad de nodos), por el patrón de comportamiento de los nodos (estático, semiestático, móvil) y por las características específicas de las aplicaciones (pasivas, *on-demand*, reactivas, etc.). La mayoría de las redes tan solo necesitan de comunicación convergente (desde los nodos sensores hacia la estación base); de todos modos, muchos algoritmos también proporcionan soporte para

comunicación divergente (desde la base a todos o unos cuantos nodos) y/o nodo a nodo. La clasificación más elemental para protocolos de comunicación suele diferenciar soluciones centralizadas y distribuidas. Un contexto distribuido proporciona a los nodos una visión muy limitada de la red: un nodo suele disponer de información relacionada con los nodos a su alrededor y, eventualmente, de la información relacionada con los mismos (parámetros lógicos y/o físicos); a la hora de tener que encaminar un paquete (Figura 1.6, izquierda), el nodo en cuestión elige la ruta en función de la información que dispone; su entorno de conocimiento al salto i se limita, por lo tanto, al paso i+1. Al contrario, un algoritmo centralizado proporciona a cada nodo una visión completa de la red. Con esta información global un nodo está capacitado para elegir la ruta óptima. No siempre un algoritmo distribuido configura rutas óptimas. En Figura 1.6 a la derecha, se propone, a título de ejemplo, una sencilla topología en el cual cada salto se caracteriza por un cierto factor de coste que tiene que minimizarse; en presencia de dos posibles rutas formadas por el mismo número de saltos, un nodo operante con algoritmo distribuido elige la ruta marcada por línea continua disponiendo tan solo de información de coste directamente relacionada con sus vecinos; contrariamente, una solución centralizada optaría por la ruta de coste mínimo (marcada con línea discontinua). Evidentemente los algoritmos centralizados proporcionan prestaciones mejores, aunque tan solo en un contexto teórico. De hecho, a causa de la necesidad de diseminar por la red cantidad relevantes de información sujeta a continuos cambios, las soluciones centralizadas son poco difusas porque costosas en términos de recursos y difícilmente escalables. Redes complejas caracterizadas por pequeña/medianas escalas pueden trabajar en un contexto distribuido extendido (semi-centralizado) en el cual el entorno de conocimiento de un nodo se extiende a un conjunto de nodos superior a lo de sus vecinos, aunque no a toda la red. Dicha extensión del entorno de conocimiento implica un mayor gasto de recursos en las tareas de configuración/reconfiguración. Este tipo de solución, por ejemplo, extendida a dos saltos, puede configurar rutas optimas en topologías como la propuesta en Figura 1.6 aunque requiriendo mayores recursos para las tereas de configuración/reconfiguración.

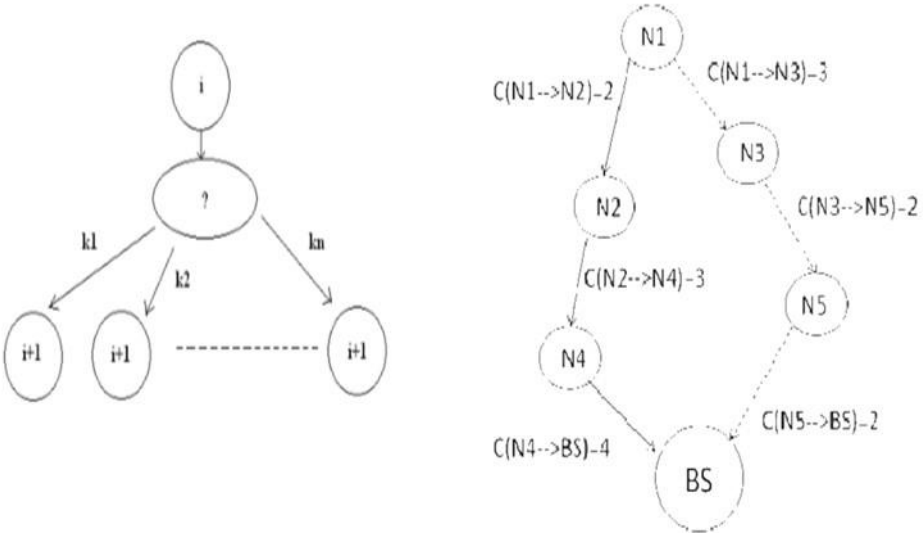



*Figura 20.* Ejemplo de protocolo de enrutamiento distribuido y centralizado
Tomado de: wikimedia.org (s.f.)

Durante los últimos años se han propuesto una gran variedad de soluciones avanzadas caracterizadas por eficiencia, robustez y fiabilidad para entornos estáticos y nomádicos, dichas soluciones se caracterizan por principios básicos y diferentes y suelen optimizar la comunicación configurando rutas con un número mínimo de saltos y/o balanceando el tráfico entre las rutas de forma de maximizar el tiempo de vida real.

Las soluciones más sencillas se basan simplemente en el balanceo de tráfico o, bien, sobre la configuración aleatoria de las rutas. Todas y cada una de las soluciones disponibles pueden, en ciertos entornos aplicativos, necesitar de mayor robustez y fiabilidad que suele proporcionarse a través de información redundante o, bien, a través de la utilización de protocolos de enlace de datos más robustos a coste, obviamente, de un mayor gasto de recursos.

A continuación, se describen las dos clases de soluciones más relevantes: enrutamiento *energy-aware* y enrutamiento posición *aware* (*o location-aware*); finalmente se describen brevemente las peculiaridades del entorno móvil.

#### 2.4.3.1. Soluciones *Energy-aware*

Soluciones basadas en C asumen que en cada nodo conozcan el nivel de carga de la batería de sus vecinos  y Position Soluciones basadas en *energy* conozca el nivel de carga de la batería de sus vecinos (*energy* toda o gran parte de la red (*energy-aware*-local) o, incluso de toda o gran parte de la red *(energy-awareness*-centralizado), aprovechando esta comunicación  las rutas de comunicación pueden configurarse de forma tal que se intente la comunicación entre nodos con mayores cargas de baterías maximizando el tiempo de vida global de la red. Obviamente, en el caso de soluciones distribuidas, quedan las limitaciones descriptas en la sección anterior.  Evidentemente esta clase caracterizadas por tráfico de información altamente irregular que puede generar consumos energéticos bastante diferentes entre los nodos; es prácticamente inútil en el caso contrario especialmente considerando que el estimador de energía no suele ser extremadamente preciso en dispositivo de bajo coste y, por lo tanto, se considera fiable solo por diferencias notables de energías.

Evidentemente esta clase de solución garantiza altas prestaciones en aplicaciones caracterizadas por tráfico de información altamente irregular que puede generar consumos energéticos bastante diferentes entre los nodos; es prácticamente inútil en el caso contrario especialmente considerando que el estimador de energía no suele ser extremadamente preciso en dispositivo de bajo coste y, por lo tanto, se considera fiable solo por diferencias notables de energías.

Contrariamente el coste de diseminación de la información suele ser poco relevante en un contexto distribuido, aunque, evidentemente, tiene que ser periódico siendo el nivel de carga de la batería un valor variable en el tiempo en función de la actividad de la red.

Otra solución de altas prestaciones se basa en *location* o *position-aware*, en este caso el factor guía para determinar las rutas de comunicación es la posición física de los nodos y es concretamente aplicable gracias a la disponibilidad de dispositivos para localización (GPS) de bajo coste. Evidentemente el enrutamiento geográfico podría, por lo menos en teoría, ser funcional tanto en contestos estáticos como nomádicos/móviles. En general las soluciones de enrutamiento geográfico garantizan altas prestaciones para la comunicación divergente o nodo a nodo.

En un contexto estático esta clase de solución proporciona buenas prestaciones especialmente considerando que, si la posición no varía, no se requiere diseminación continua de información. La limitación más grande, en este sentido, es representada por el mismo dispositivo GPS que implica un hardware bastante más avanzado a lo usual; además su utilizo se limita a contextos *outdoor*. Otras soluciones [Rao1] *position-aware* se basan en la estima de la posición de los nodos en función de las potencias detectada en la recepción de los mensajes; aparecen poco interesantes en contextos generales, posiblemente funcionales en unos entornos aplicativos específicos. La aplicación de soluciones position-*aware* en entornos móviles y *outdoor* con posicionamiento GPS esta, de momento, limitada a causa de las propias características de los dispositivos GPS que están diseñados para georreferenciar la información más que a soporte de mecanismos básicos.

#### 2.4.3.2. Enrutamiento en redes móviles

Mención particular merece el entorno móvil que, también gracias a la disponibilidad de dispositivos de posicionamiento integrados en los nodos inalámbricos y, por lo tanto, de generar información geo-referenciada, es objeto de particular atención en el contexto científico-comercial. Una red de sensores se considera móvil si la posición de los nodos que la componen puede cambiar en el tiempo de vida de la aplicación. Realmente la movilidad de los nodos puede

generar diferentes escenarios: *sinks* móviles y nodos sensores estáticos, *sinks* estáticos y nodos sensores móviles, *sinks* y nodos sensores móviles o, finalmente, soluciones hibridas caracterizadas por coexistencia de nodos móviles y fijos. Evidentemente la tecnología de referencia por excelencia es MANET (*Mobile* Ad-hoc *NETwork* [Jey1][Dha1]), con la cual hay muchos puntos en común y unas diferencias sustanciales. Aunque ambos entornos requieren soluciones diferentes respecto a redes con topologías predefinidas y presentan muchos elementos de convergencia, no sería del todo correcto considerar las redes móviles de sensores inalámbricos simplemente como caso particular de MANET. En primer lugar, las redes de sensores, móviles o estáticas, suelen ser sistemas data-*centric* [Hon1] al contrario de las redes ad-hoc que proponen un enfoque id-*centric* o, eventualmente, *user-centric* con fuerte interacción entre usuario y nodo. Además, la presencia de las estaciones base implícitamente centraliza las redes de sensores, al contrario de las *MANETs* que, propone un entorno distribuido potencialmente peer-to-peer. Finalmente, el *hardware* de los nodos en *MANET* se asume potencialmente limitado solamente en términos de alimentación y suele diseñarse para soportar aplicaciones avanzadas de alta capacidad; al contrario, el contexto aplicativo de los nodos sensores es bastante más limitado (normalmente a la interacción con el ambiente circundante) así como su hardware.

Las soluciones diseñadas para redes de sensores móviles sueles ser simplificaciones de las equivalentes diseñadas para MANET o bien, especializaciones de las soluciones diseñadas para entornos de redes de sensores estáticos con diferente gestión del estado relativo a las rutas de comunicación. Estas últimas soluciones se basan, en función del entorno de aplicación, sobre configuración *soft-state* o *stateless (on-demand*) de las rutas de comunicación: en el primer caso las rutas se consideran validas tan solo por un cierto periodo de tiempo (al contrario de las soluciones con estado que asumen rutas estables entre dos tareas de configuración) requiriendo, por lo tanto, continuos refrescos; soluciones *ondemad* (normalmente iniciadas por la

estación base) suelen basarse en la configuración de las rutas en tiempo real asumiendo las mismas validas tan solamente para la comunicación corriente.

El entorno nomádico asume movimientos limitados de los nodos debidos a fenómenos naturales o accidentales y/o cambios de posicionamiento puntuales; redes nomádicas de sensores suelen trabajar con protocolos diseñados para redes estáticas; así como para redes estáticas que trabajan en entornos de comunicaciones hostiles (interferencias temporales, obstáculos, etc.), los mecanismos de monitorización y gestión suelen garantizar la fiabilidad necesaria. En el contexto de las redes de sensores móviles hay un siempre creciente interés en las aplicaciones *"group-based*", especialmente en entornos militares y en aplicaciones vehiculares. En este último campo de aplicación, las redes de sensores inalámbricos proporcionan una interesante alternativa de bajo coste para el soporte de aplicaciones innovadoras para monitorización de grandes áreas aprovechando la movilidad de los vehículos.

### 2.4.4 Monitorización y Control

Arquitecturas caracterizadas por tráfico de datos periódico y continuo se monitorizan implícitamente. (ejemplo aplicaciones reactivas a eventos) requieren mecanismos específicos para monitorización. Es difícil identificar patrones generales para los mecanismos de monitorización; normalmente suelen comprobar la operatividad de la red a través de la diseminación de paquetes de test con espera de notificación por parte de los nodos interesados; visto el coste implícito de la diseminación de dichos paquetes (test y notificaciones), unas soluciones prefieren reconfigurar la red periódicamente sin monitorizar explícitamente la misma. De hecho, otro de los parámetros comerciales más comunes es la robustez que impone que la red se reconfigure, periódicamente o de forma reactiva, para asegurar funcionalidad en presencia de interferencias, obstáculos y otros factores que pueden limitar, de forma temporánea o permanente, la operatividad de la red. Considerando la intervención humana

como extremadamente costosa (imposible en unos casos), la auto-gestión de la red es uno de los requisitos principales de muchas arquitecturas reales. Todos los aspectos relacionados con monitorización y control tienen importancia en presencia de despliegue aleatorio de los nodos

(muy común), donde diferentes

despliegues pueden presentar prestaciones significativamente diferentes entre ellas y, tal vez, lejanas de las esperadas.

El entorno móvil representa, una vez más, una excepción en cuanto los mecanismos de monitorización y control son implícitamente parte del proprio mecanismo de enrutamiento de base.

### 2.4.5 Calidad de servicio y Seguridad

En campo de redes de sensores el concepto de calidad de servicio puede ser bastante ambiguo. A parte de los ya mencionados requisitos no funcionales (fiabilidad, robustez, eficiencia energética, todos directamente gestionados por los mecanismos de comunicación, monitorización y gestión), los requisitos de las aplicaciones reales suelen referirse a calidad de servicio especialmente en términos de tolerancia de fallos. En otras palabras, aunque existan ciertos parámetros de calidad de servicio unánimemente reconocidos, requisitos reales de calidad de servicio no suelen definirse de acuerdo con métricas estándares como en otros tipos de red. Una técnica bastante utilizada es medir el “beneficio” introducido por un cierto mecanismo de calidad de servicio en función de los recursos utilizados. La capacidad de garantizar una cierta calidad de servicio (como definida en el entorno considerado) puede ser una de las claves para el éxito comercial de las redes de sensores inalámbricos.

Como en otros entornos, la tolerancia a fallos en redes de sensores se caracteriza por dos fases (detección del fallo y reacción al mismo). Unos fallos

simplemente son indetectables, ciertas arquitecturas auto detectan los fallos, otras necesitan mecanismos específicos de monitorización. Asimismo, en unos casos las arquitecturas son implícitamente tolerantes a los fallos en otros necesitan mecanismos reactivos. En el caso específicos de las redes de sensores, el concepto de fallo hardware/software de un nodo puede integrarse con el “fallo” debido al acabarse de la batería. Tanto los mecanismos de detección como de reacción a fallos suelen ser característica de sistemas concretos; es, por lo tanto, difícil identificar patrones. El caso más crítico es, seguramente, representado por las tareas cooperativas que, a frente de fallos no detectados, podrían producir resultados erróneos o indeseados. Los aspectos relacionados con la seguridad de los sistemas informáticos han representado siempre un punto fijo de interés para la comunidad científica y, además, uno de los elementos clave para la difusión comercial de determinados productos.

Históricamente se han propuesto diferentes modelos teóricos de ataque *(Denial of Service, Sybil Attack, Blackhole/Sinkhole Attack, Hello Flood Attack, Wormhole attack*, etc.); una manera moderna y sugestiva de relacionarse al problema de la seguridad es plantearlo de acuerdo con la teoría de juegos en el cual un jugador propone un ataque y el otro se defiende.

Inevitablemente, el problema de la seguridad se representa sobre redes inalámbricas de sensores tanto a nivel de acceso a los recursos como a nivel de protección de los datos. Problemas de mayor relevancia se consideran el propio entorno (inalámbrico), la posibilidad de capturar uno o más nodos e intentar de comprometer el entero sistema y el entorno a recursos limitados que impone el uso de mecanismos de seguridad más sencillo y, por lo tanto, más vulnerables. De hecho, la gran mayoría de los mecanismos de seguridad para redes de sensores suelen ser simplificaciones de las correspondientes para redes ad-hoc. El objetivo básico de un sistema de seguridad sobre redes inalámbricas de sensores es de proporcionar un buen nivel de defensa (acceso seguro y encriptación de datos) y, al mismo tiempo, en el caso de ataque físico de un sensor evitar comprometer todo el sistema; el mecanismo diseñado tiene que ser

evaluado en función de los recursos que requiere y, por tanto, proporcionar un compromiso entre nivel de seguridad proporcionado y recursos utilizados. Técnicas típicas de seguridad usan llaves para habilitar un enlace; dependiendo del nivel de seguridad deseado y de los recursos disponibles se pueden diseñar mecanismos basados en la compartición de claves globales, en claves de grupo o, incluso, de pareja. La generación de las claves puede ser un punto relevante y puede basarse en varias asunciones (generación casual o de acuerdo con determinados modelos matemáticos). En general, la organización jerárquica de la red puede aconsejar una política de distribuciones de las claves basadas sobre principios de localidad de la información.

### 2.4.6 Configuración avanzada y Optimización

Los protocolos de configuración avanzada suelen proporcionar un nivel lógico adicional que complemente y se integre con el nivel lógico básico. Pueden necesitarse para garantizar altas prestaciones (o parámetros non funcionales) al crecer de la escala a través de arquitecturas multi-base que requieren *clustering* dinámico o para soporte de soluciones avanzadas (por ejemplo, arquitecturas orientadas a roles) o para solucionar problemas específicos. El más relevante es, seguramente, el *clustering* dinámico que será objeto explícito de la sección siguiente; entre los otros protocolos de configuración dinámica de relevancia se citan:

- Protocolos para asignación de roles: las arquitecturas orientadas a roles se basan sobre la definición de unos cuantos roles de base que tienen que cumplir con unos cuantos requisitos lógicos (ciertas propiedades de configuración básica), topológicos (por ejemplo, un cierto número de vecinos) y/o físicos (cierto *hardware* en el caso de redes heterogéneas). Para que estas arquitecturas puedan trabajar correctamente se necesita evaluar las condiciones de configuración básica y de la red y asignar (eventualmente de forma optimizada) los roles en función de las condiciones detectadas. Evidentemente

se trata, en la mayoría de los casos, de algoritmos centralizados, aunque existan variantes distribuidas. Un ejemplo típico de rol, muy utilizado para optimizar aplicaciones de adquisición periódica de datos, es el *data-collector*; su función es de actuar como *"hole*" para los nodos circunstantes que envían datos; el *data-collector* se preocupa de comunicar con la estación base optimizando el *throughput* a nivel de aplicación.

• Distribución aleatoria de parámetros: ciertas aplicaciones requieren la diseminación de ciertos parámetros de forma aleatoria, tal vez con unos vínculos o condiciones. Un ejemplo típico es la diseminación dinámica de los identificadores que no tiene que repetirse. Otros parámetros podrían relacionarse con aspectos de seguridad o de prioridad en la comunicación o de prioridad en la asignación de recursos. • Diseminación y configuración de tareas: non siempre los nodos sensores actúan de forma aislada en la red; ciertas aplicaciones requieren tareas cooperativas entre sensores; dichas tareas necesitan configuración, dinámica normalmente, especialmente en presencia de hardware homogéneo. De la misma forma, ciertas aplicaciones, en función de ciertos eventos externos (control por parte del usuario) o internos (condiciones detectadas), necesitan la configuración del comportamiento de los nodos sensores; estos últimos pueden actuar todos de acuerdo a un mismo patrón o actuar de forma diferente; en ambos casos necesitan de configuración dinámica. La diseminación de tareas suele ser un mecanismo centralizado, aunque soluciones distribuidas puedan ser funcionales a ciertos entornos aplicativos.

• Otros protocolos: otros protocolos orientados a proporcionar funcionalidades añadidas. Dichos mecanismos también pueden tener el objetivo de configurar parámetros complejos, así como de garantizar alguna propiedad o a solucionar algún problema específico (de cálculo por ejemplo). Un ejemplo de protocolos que añaden funcionalidades en función de la aplicación a soportar son los protocolos de nivel de transporte (encargados de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red). Por sus propias

características (transmisión de pequeñas cantidades de datos en modalidad convergente), las redes inalámbricas de sensores suelen asumir funcionalidades de transporte extremadamente reducidas o ausentes. Sin embargo, arquitecturas a soporte de aplicaciones caracterizadas por transferencia de flujos de datos importantes (redes de sensores multimediales por ejemplo) pueden presentar capas de transporte extendidas.

Independientemente de la presencia o menos de protocolos de configuración avanzadas, arquitecturas de protocolos complejas que incluyen varios mecanismos operantes simultáneamente suelen proponer una capa de optimización; el objetivo de esta capa es optimizar la comunicación (minimizando el número de mensajes intercambiados) multiplexando la información de los varios protocolos y mecanismos en mensajes optimizados. Esta última capa lógica no es de confundirse con la optimización a nivel de aplicación, aunque, en muchos casos, puede coincidir especialmente en el contexto de aplicaciones que trabajan con ciclos periódicos.

### 2.4.7 *Clustering*

Una arquitectura orientada a *clusters* supone la división o partición del sistema principal en unos cuantos subsistemas que *interoperan* entre sí. Un *cluster* clásico se compone de una cabeza o *header*, normalmente con funciones de gestión y representación del entero *cluster* cara al sistema global, y por el contexto de los actores componentes el *cluster* que suelen organizarse de forma jerárquica. En el modelo más común la interacción entre *clusters* (o con el sistema de gestión centralizado) es gestionada por las cabeceras de los *clusters*. En un sistema general la configuración mediante *clusters* puede aplicarse por varios motivos con objetivo la optimización de factores relacionados con la arquitectura, las infraestructuras o la información.

En el caso de las redes inalámbricas de sensores se presentan, básicamente, dos posibles aplicaciones de técnicas de clusterizacion:

- La cabecera de los *cluster* es representada por una Estación Base (Figura 17): es el caso más relevante en cuanto, en presencia de nodos sensores con recursos limitados, permite una mayor escalabilidad del sistema dividiendo un sistema formado por n nodos sensores en m subsistemas (*clusters*) compuestos medianamente por n/m nodos. La gestión de cada *cluster* es autónoma respecto a su cabecera por lo cual las rutas de comunicación resultan reducidas de un factor proporcional a m así como el *energy-hole.* Por el contrario, tanto las prestaciones (tiempo de vida de la red) como los típicos parámetros no funcionales (fiabilidad y robustez) resultan beneficiarse de dicha organización lógica. La organización en *clusters* suele introducir una complejidad añadida a las infraestructuras de *control* así como, en el caso de configuración dinámica, la necesidad de configuración avanzada. Los aspectos positivos de la organización en *clusters* se consideran bastante más relevantes que los aspectos negativos así que esta técnica esta progresivamente ganando importancia en el seno de las aplicaciones reales siendo, de hecho, la única técnica válida para garantizar ciertas prestaciones, en un contexto de fiabilidad y robusteza, para arquitecturas operantes sobre larga escala.

- La cabecera de los *clusters* está representada por un nodo sensor: es un caso realmente menos relevante del anterior; su aplicación, tal vez solamente teórica, se enfoca básicamente dentro de las arquitecturas orientadas a roles o, más en general, en un contexto de cálculo distribuido sobre redes de sensores. Su aplicación real resulta, por lo tanto, muy limitada.

Con referencia a *clusters* caracterizados por cabeceras representadas por Estaciones Base, se distinguen, básicamente, dos posibilidades en términos de configuración:

- Configuración Estática: cada nodo sensor se asocia a un cierto *cluster* a priori; este tipo de configuración puede aplicarse a contextos con topologías más o

menos predefinidas o despliegues aleatorios controlados. Evidentemente no implica ningún mecanismo de configuración avanzado.

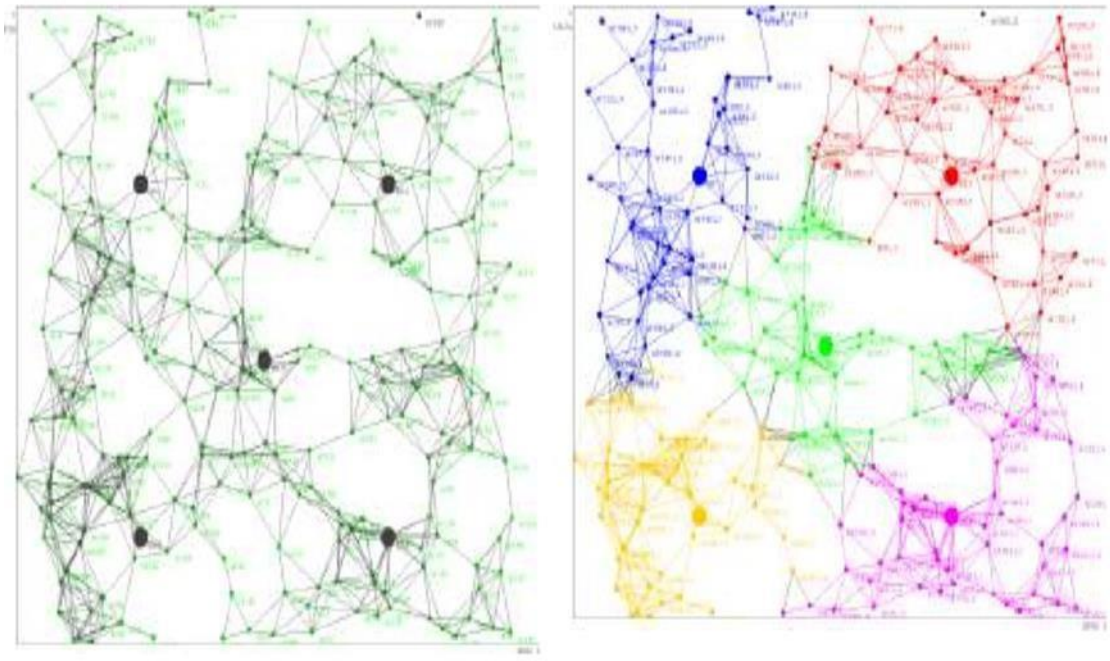


*Figura 21.* Ejemplo de configuración de *clusters*
Tomado de: procordoba (s.f.)

- Configuración Dinámica: al contrario del caso anterior, cada sensor se asocia dinámicamente a un *cluster* más que a otro; a lo largo del tiempo de vida de la aplicación el mismo sensor puede, por lo tanto, asociarse a *cluster* diferentes en función de las condiciones de entorno, de vínculos y restricciones.

Potencialmente un nodo sensor puede asociarse a más que un *cluster* contemporáneamente. Evidentemente esta clase de solución (que requiere mecanismos de configuración avanzada) proporciona soluciones mucho más complejas y dinámicas que mejor se adaptan a despliegues completamente aleatorios y a cambios significativos de topologías y condiciones de entorno. Un mecanismo dinámico de configuración avanzada en *clusters* se caracteriza por la política según el cual asocia los nodos a un *cluster* más que a otro; se distinguen, normalmente, dos tendencias de base: una orientada a las prestaciones y otras orientada al balanceo de las dimensiones. La primera, con

diferencia la más difusa, configura el *cluster* intentando minimizar las rutas en términos de saltos; evidentemente aspectos relacionados con la comunicación y con la optimización de los recursos suelen ser beneficiados, aunque los diferentes *clusters* que componen el sistema puedan resultar bastante desequilibrados respecto al tamaño. Soluciones orientadas al balanceo, al contrario, intentan configurar los *clusters* de forma que el tamaño medio sea lo más parecido posible; esta clase de solución puede causar una cierta ineficiencia en términos de comunicación y, por lo tanto, se suele asociar a entornos de aplicación muy específicos. De todos modos, las dos soluciones descriptas suelen converger al disminuir de la escala del sistema a paridad de densidad de nodos sensores y números de bases.

### 2.4.8 Aplicación

Exactamente como en las arquitecturas de protocolos tradicionales, los protocolos de nivel de aplicación suelen implementar las funcionalidades de la aplicación considerada apoyándose en las funcionalidades proporcionadas por las capas inferiores. En el contexto de las redes inalámbricas de sensores, el nivel de aplicación suele implementar el software para la adquisición y la interpretación de la información proporcionada por los transductores o, bien, la implementación del algoritmo distribuido que define el comportamiento del nodo en la red. Así como visto para capas inferiores, también el nivel de aplicación puede incluir una capa virtual de optimización; el objetivo es el mismo de lo relativo a protocolos más básicos: se pretende, básicamente, optimizar las tareas de comunicación consideradas notablemente más dispendiosas respecto a la elaboración local de datos. Las técnicas más comunes actúan, por lo tanto, para optimizar el *throughput*: técnicas basadas en *data-fusion* intentan privilegiar, donde posible, la elaboración local de los datos generados (por ejemplo enviando tan solo la media sobre unos valores más que cada singulo valor); técnicas basadas en *data-aggregation* intentan, visto el pequeño tamaño de los datos

generados, de agrupar más tramas informativas (collación de datos) en cada mensaje de aplicación para minimizar el número de mensajes transmitidos.

## 2.5 Tecnología para *Middleware*

Un número importante de arquitecturas reales suelen basarse en topologías formadas por más de una estación base, algunas veces organizadas de forma jerárquicas. La funcionalidad básica de este tipo de infraestructura es recoger la información, eventualmente integrarla y/o procesarla, y finalmente transmitirla hacia un centro de control remoto. Un número creciente de redes de sensores inalámbricos se integra en sistemas complejos como sistemas empotrados. Más recientemente, también el modelo de explotación de las redes de sensores se ha complicado progresivamente y los servicios proporcionados por dichas redes se manejan dentro de Comunidades Virtuales siempre más complejas y articuladas que requieren políticas de acceso y manejo de la información y de los servicios extremadamente complejas (normalmente *context-aware* o *content-aware*). Todos estos aspectos imponen (o aconsejan) la utilización de un modelo middleware extremadamente flexible que pueda soportar eficientemente tanto sistemas propietarios como sistemas embebidos o interoperables, eventualmente integrando políticas de acceso y gestión compleja. El middleware es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas. Funciona como una capa de abstracción de software distribuida, que se sitúa entre las capas de aplicaciones y las capas inferiores (sistema operativo y red). El middleware abstrae de la complejidad y heterogeneidad de las redes de comunicaciones subyacentes, así como de los sistemas operativos y lenguajes de programación, proporcionando una API para la fácil programación y manejo de aplicaciones distribuidas. En el contexto tecnológico actual, el modelo tecnológico de referencia al respecto es, sin duda, el modelo Web-*service* especificado por W3C. El concepto clave de un *webservice* es la clara división entre interfaz (definida según un modelo de datos interoperable) del

servicio e implementación del mismo con el objetivo de enfatizar la interoperabilidad y el modularidad de los sistemas distribuidos de acuerdo con los más relevantes principios de la ingeniería del software.

Más recientemente, modelos avanzados de *web-services* se han diseñado con el intento de incrementar las prestaciones en el contexto del cálculo paralelo y distribuido o bien, la flexibilidad en entornos virtuales extremadamente complejos y articulados. Es el caso de *Grid Computing* que se caracteriza por un modelo de servicio con gestión compleja de su estado: un *web-service* tradicional es sin estado por definición. El entorno *Grid* proporciona, en su última versión, un modelo mucho más complejo en el cual un servicio puede ser sin estado (y por lo tanto compatible con el estándar W3C) o, bien, con estado manejable de forma estática (un servicio se instancia y se destruye explícitamente) o según políticas de gestión dinámicas (instancias temporizadas o relacionadas con eventos). Recientemente se han propuesto varias soluciones middleware para redes inalámbricas de sensores que se basan en tecnología *Grid*. Una de las últimas tendencias en redes de sensores es su progresiva evolución conceptual hacia el modelo lógico-computacional conocido como "*Internet-of-things*".

El concepto básico es la consideración de cada nodo sensor como un objeto lógico siempre conectado y la información asociada (o generada) como la base para construir modelos de conocimientos más avanzados y abiertos de los proporcionados por servicios propietarios. Evidentemente, vista la imposibilidad (o el elevado conste) de conectar cada sensor a la Red como unidad independiente, este modelo implica un middleware de virtualización extremadamente eficiente y flexible que asocie una instancia de servicio a cada nodo. La solución *Grid*, en este sentido, aparece especialmente eficaz. Temas de investigación relacionados se consideran el modelo de datos para garantizar la interoperabilidad de la información en sistemas heterogéneos y la semántica asociadas para garantizar soporte para interacciones complejas. Una posible alternativa en el desarrollo de componentes middleware es el modelo de computación multi-agente. Respecto al modelo a servicios, los Sistemas

MultiAgente son meno modulares, medianamente menos interoperables a causa de su modalidad de funcionamiento que, normalmente, requiere un acuerdo entre las partes para garantizar entornos seguros. Las principales opciones son:

- Arquitecturas orientadas a servicios: *Web Services*
  Entornos empotrados
- Organizaciones Virtuales y *Grid-Computing Open Grid Service Architecture* (OGSA)
  *Frameworks* para desarrollo en tecnología *Grid*
- Sistemas Multi-Agente
  Negociación en Sistemas Multi-Agente
  Plataformas Multi-Agentes

## 2.6 Vulnerabilidades

Las redes de sensores en la actualidad son una realidad emergente, con muchas expectativas de cara al futuro, para entornos empresariales o públicos, apostando servicios a los usuarios para permitir una comunicación fiable y segura en este tipo de redes. Estas redes de sensores al igual que la mayoría de redes inalámbricas, no están exentas de potenciales peligros que pueden ponerlas en un serio riesgo de compromiso de seguridad.

- **Denegación de servicio (*Denial of Service*-DOS):** De difícil mitigación, colocando un nodo que controle las comunicaciones permanentemente.
- **Escucha de la red (*eavesdropping*):** Un dispositivo escucha la red a la espera de recibir la información que se transmite. Con cifrado se hace más difícil la escucha.
- **Usurpación de identidad (*spoofing*):** Hacerse pasar por otro nodo de la red para recibir y enviar datos de terceros. Si es encaminador podrá capturar todo el tráfico que pase por él.
- **Reenvió de paquetes (*replay*):** Consiste en el reenvío, o no, de paquetes capturados anteriormente para desestabilizar la red o el nodo que los

recibe y que únicamente espera un dato. El control de secuencia ayudará a la mitigación de este ataque.

# 3 CAPITULO III: DISEÑO Y PROPUESTA DE LA SOLUCIÓN

## 3.1 Introducción

Este Capítulo describe un esquema de la **seguridad en redes** de sensores inalámbricos (**WSN**), partiendo desde la normativa hasta la aplicación de un esquema de seguridad a nivel técnico, considerando que la plataforma de redes de la Universidad de las Américas es CISCO, es necesario seguir en la misma línea de equipamiento por temas de compatibilidad, además que existe el conocimiento necesario, pues la UDLA es Academia CISCO.

## 3.2 Esquema de seguridad de red

### 3.2.1 Normativa ISO27001

La norma ISO 27001 define activo de información como los conocimientos o datos que tienen valor para una organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.

El propósito de la seguridad en todos sus ámbitos de aplicación es reducir riesgos hasta un nivel que sea aceptable para los interesados en mitigar amenazas latentes y que la información se maneje bajo un marceo de:

***Confidencialidad (Confidentiality)***, se enfoca que la información sólo puede ser accedida por la persona y/o sistema con las credenciales pertinentes. Igualmente, nadie sin credenciales puede tener acceso a ningún tipo de información dentro de la red. En la práctica, la confidencialidad se logra a través

de la implementación del cifrado de la información. Debemos de cifrar tanto la información guardada en disco como la que viaja a través de la red.

**Integridad *(Integrity)***, establece que la información NO puede ser modificada sin los permisos correspondientes, de lo contrario, la información es corrupta. La integridad de la información es lo que garantiza la validez de la información. En la práctica, para garantizar la integridad de la información se implementa algoritmos de *Hashing*.

**El término Disponibilidad *(Availability)***, establece que la información debe de estar disponible a los usuarios de la red en el momento que se precise, de lo contrario, la red no cumple su cometido principal. Las redes pueden en algún momento no ofrecer servicio producto de un ataque informático, donde las peticiones de los usuarios legítimos NO son procesadas como consecuencia de una avalancha de acceso de manera simultánea proveniente desde el exterior. A esto se le llama Ataque de Negación de Servicios (*Denial of Service Attack*).

#### 3.2.1.1. Ciberseguridad

Ciberseguridad, Según ISACA se define como, “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

Concluyendo que la ciberseguridad se enfoca en la protección de la información digital que “vive” en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

### 3.2.2 Seguridad en los Dispositivos de Red

Las topologías de las redes de sensores inalámbricos establecen que los nodos se encuentran esparcidos en ambientes abiertos inclusive en la intemperie, dependiendo de la aplicación y uso de la red, debido a esta particularidad las redes WSN son propensas a diferentes tipos de ataques, entre los más relevantes se puede mencionar:

- **Denegación de Servicio DoS. -** Busca dejar inoperativo el servicio, es decir, este ataque afecta a la disponibilidad.
- **Equipamiento no autorizado. -** Introducción en la topología de red de nodos no autorizados, lo cual compromete la integridad de la información.
- **Ataque de hombre en el medio. -** Se realiza escucha de la información que circula por la red.
- **Daños a la infraestructura física. -** Puede entenderse como vandalismo o sabotaje, los daños que se causan a los nodos de la red.
- ***SinkHole*. -** Instalación de un nodo espía en las inmediaciones del nodo central, a fin de apoderarse de información.

En el análisis de seguridades de cualquier tipo de red, es necesario considerar las amenazas, para el caso de las WSN, podemos identificar:

- **Intercepción. -** El atacante intercepta la información, podríamos decir, que saca una copia de los datos que se están transmitiendo.
- **Fabricación. -** El atacante genera o introduce información ilegitima en la red, la cual fluye como si fuese real o legitima.
- **Modificación. -** El atacante utilizando herramientas de hacking modifica partes o toda la data transmitida.
- **Interrupción. -** El atacante interrumpe el servicio, es decir, la disponibilidad de la red es comprometida.

#### 3.2.2.1 Mecanismos de Seguridad

Es de vital importancia resaltar que previo la implementación de cualquier mecanismo de seguridad para una red, se debe disponer de la Política de Seguridad de la Información, que abarca de extremo a extremo la operación de una empresa o institución, pues establece los lineamientos y procedimientos de acceso a la información, mecanismos de protección y sanciones para el personal que incumpla lo establecido en dicho documento.

Para el presente proyecto nos basamos en la política de seguridad de la información de la UDLA, en lo referente a los accesos inalámbricos.

#### 3.2.2.2 Servicios Tres A

Existen tres pilares para asegurar una red, los cuales son conocidos como servicios AAA (Autenticación, Autorización y Auditoría), los cuales se encaminan a cubrir los ámbitos de la Confidencialidad, Integridad y
Disponibilidad (por sus siglas en inglés).

Se puede implementar soluciones de varios niveles para cubrir las tres A´s, a nivel corporativo se puede utilizar los protocolos TACACS+ o RADIUS.

**TACACS+. -** Protocolo propietario de CISCO que implementa los servicios de las tres A, por separado lo que permite que esta solución sea más escalable. Otro aspecto importante a resaltar es que éste protocolo utiliza conexiones TCP, lo que garantiza la entrega de información, así como todas las comunicaciones entre el transmisor y el receptor son encriptadas.
**RADIUS. -** Protocolo de aplicación genérica que implementa los servicios tres A, en dos pasos: al momento de autenticar también realiza la autorización y luego se efectúa la auditoria.

Con la implementación de éste protocolo se puede utilizar el protocolo IEEE802.1X, que permite autenticación a nivel de infraestructura.

#### 3.2.2.3 Autenticación

La autenticación es quizá el punto más crítico a considerar en el aseguramiento de una red, pues la mayoría de los ataques a las redes WSN son la inserción de nodos maliciosos para alterar el flujo normal de datos, por lo que disponer de un mecanismo que permita reconocer la procedencia de la información, es decir, autenticar al transmisor, entre los mecanismos más comunes en ésta línea es la autenticación mediante MAC.

**Autenticación de múltiples saltos**

Éste tipo de autenticación es usual emplearla en la verificación de las identidades de los nodos nuevos en la topología de la red, esto con el objetivo de garantizar la procedencia del sensor.

Este mecanismo se basa en la utilización del protocolo de autenticación con *broadcast uTESLA*, que tiene como principio que únicamente la estación central o base puede generar *broadcast*.

El nodo que transmite crea dos secuencias de claves aleatorias a las cuales les aplica una función Hash a fin de generar otras claves, con lo cual queda conformada la cadena de clave primaria y secundaria, la primera clave de la cadena principal se denomina compromiso de clave y permite la autenticación de las otras claves, mientras que la primera clave de la cadena secundaria permite la actualización de compromiso de clave cuando termine su periodo de vida.

El proceso de autenticación inicia cuando el nodo transmisor envía las dos primeras claves de cada cadena, así como el intervalo de tiempo de inicio, por el

lado del nodo receptor, éste se asegura que el tiempo de transmisión del paquete no sobrepase el tamaño del intervalo, si esto se cumple la clave queda verificada.

**Autenticación por *Broadcast***

La operación de éste mecanismo que es el de mayor despliegue en red de sensores, tiene su centro de operación en la función *Hash*.

El nodo transmisor genera una cadena con una clave inicial y la remite a todos los nodos de la red, la autenticación se basa en la utilización de un rompecabezas que contiene la concatenación de un mensaje, la secuencia de comprobación de que el mensaje no se ha utilizado previamente y una clave previamente generada. Al rompecabezas se le agrega la solución y el número de clave empleada, a éste conjunto se la aplica la función Hash y se envía el *broadcast*. El nodo receptor verifica la clave inicial y si es correcta comprueba la solución del rompecabezas.

#### 3.2.2.4 Detección de Intrusos

Los sensores o nodos de la red se despliegan en un ambiente al aire libre, por lo que la presencia de intrusos es común en éste tipo de redes, para prevenir este tipo de eventos se debe realizar el monitoreo de los nodos, para lo cual existen dos algoritmos:

**PIA** (Activación Independiente Preprogramada). - Cada sensor tiene una lista predefinida de activación, a la cual se acogen sin tener ningún conocimiento del comportamiento de otros sensores. De esta forma, cuando expira el reloj de un nodo, se activa el sensor con una probabilidad P y reinicia su reloj. Al activarse, busca nodos activos para enlazarse y compartir información de posibles eventos sospechosos, pero si no encuentra, vuelve a un estado de reposo. Sin embargo, si ha conformado de manera premeditada, un par de comunicación con otro nodo, ambos se activan en el mismo instante.

**NC** (Cooperación de Vecinos). - Los nodos poseen una lista de activación distribuida, es decir los nodos se activan teniendo en cuenta el comportamiento de sus vecinos.

3.2.2.4.1 Sistema de detección de intrusos

En la línea de sensores de red, existen dos corrientes una activa y una pasiva, las cuales tienen que ver con la actuación en línea para prevenir y la otra es de monitoreo.

Los sistemas de detección de intrusos (IDS), son soluciones que verifican los patrones de tráfico de la red fuera de línea, es decir, previamente se saca una copia del tráfico para comprobar si hace match con alguna de las firmas habilitadas.

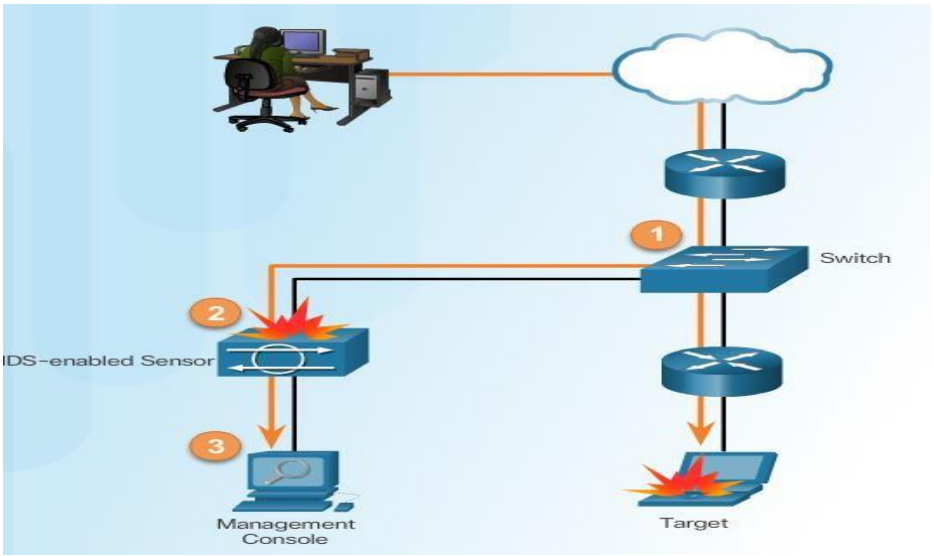



*Figura 22*. Detección de Intrusos IDS.
Tomado de: elprocus (s.f.)

Los sistemas de prevención de intrusos (IPS), trabajan en línea es decir que el tráfico antes de ingresar a la red es verificado con las firmas habilitadas, si hace match el tráfico es eliminado en ese instante.

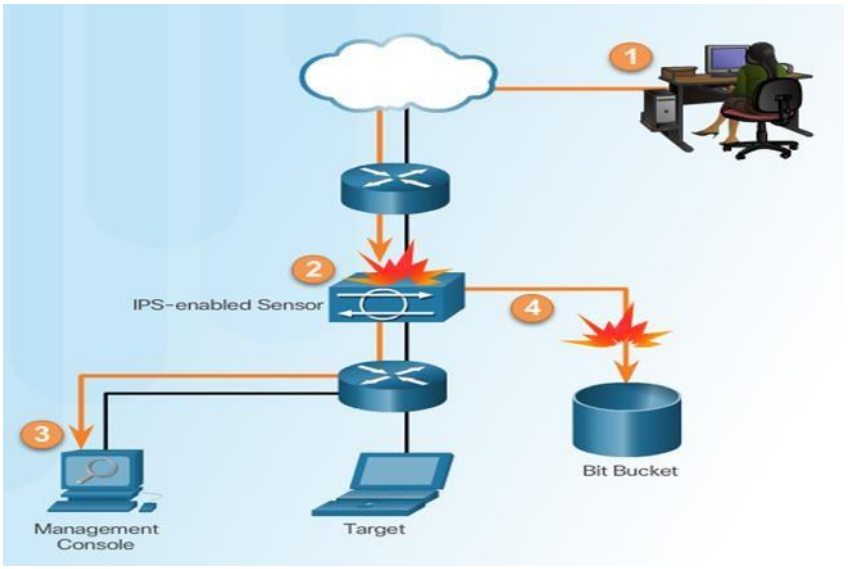



*Figura 23.* Detección de Intrusos IPS.

Tomado de: elprocus (s.f.)

### 3.2.2.5 IEEE802.1X – Autenticación Basada en Puerto

El estándar IEEE802.1X define el control de acceso y autenticación, a fin de evitar que estaciones no autorizadas utilicen la infraestructura de red.

Se identifican tres roles en la implementación de IEEE802.1X:

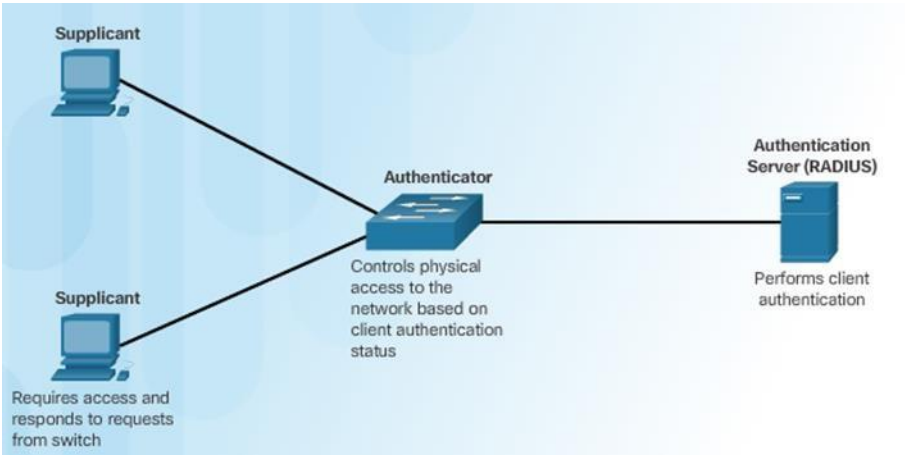



*Figura 24.* Implementación IEEE802.1X.

Tomado de: networkjutsu(s.f.)

- **Suplicante (Cliente)**. - Equipo que requiere ingresar a utilizar los recursos de red, para lo cual debe superar el proceso de autenticación. El sistema operativo de la estación debe soportar el cliente de IEEE802.1X.
- **Autenticador (*Switch* - AP). -** Controla el acceso físico a la red, sin embargo, su función es actuar como proxy entre el cliente y el servidor de autenticación. El *switch* utiliza el agente de RADIUS, el cual es responsable de encapsular y desencapsular EAP (Protocolo Extensible de Autenticación).
- **Servidor de Autenticación.** - Realiza la autenticación de los clientes, validando su identidad y comunicando el resultado al *switch*.

Hasta que la estación es autenticada, el acceso al puerto únicamente soporta EAPOL (Protocolo Extensible de Autenticación sobre LAN). Cuando un puerto está configurado con 802.1X, inicia con el estado no autorizado, lo que implica que no se permite el ingreso ni el egreso de tráfico, excepto los paquetes del protocolo 802.1X. Una vez el cliente es autenticado el puerto va al estado de autorizado y con ello se permite todo el tráfico de usuario.
La negociación de 802.1X se muestra a continuación.

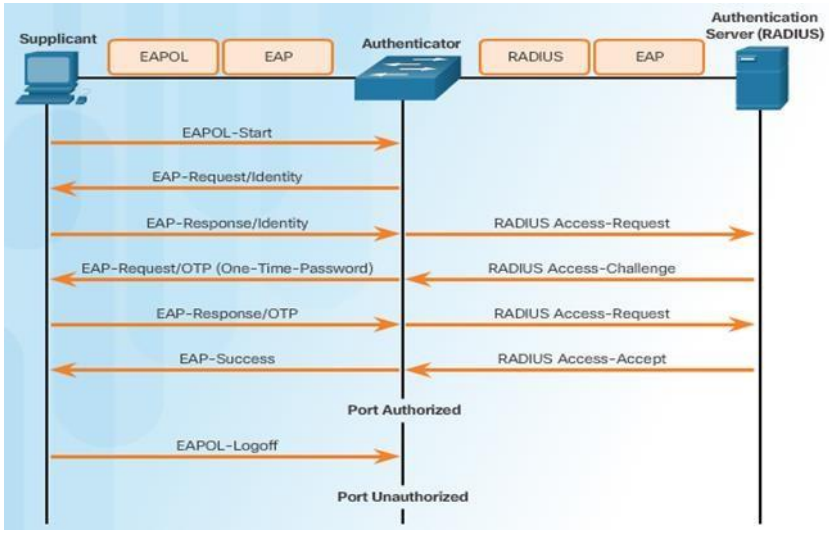



*Figura 25.* Ejemplo de Negociación 802.1X.
Tomado de: wlan-peap (s.f.)

### 3.2.2.6 Formato de Trama

Al referirnos al formato de la trama 802.11 referente a las comunicaciones inalámbricas aplicable a las WSN, se muestra a continuación:

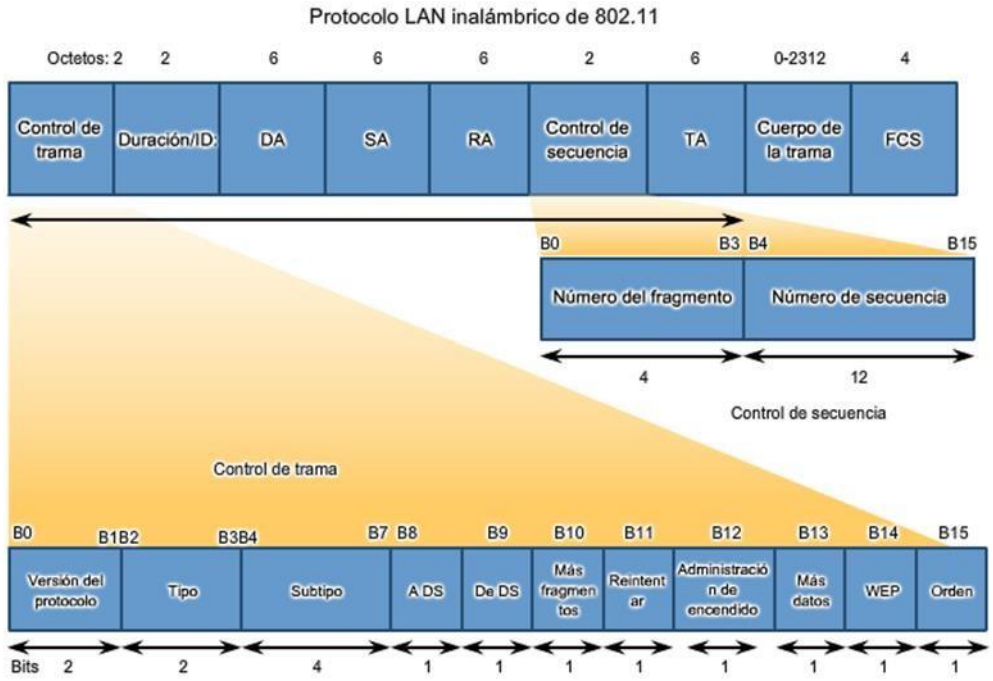



*Figura 26.* Formato de trama.
Tomado de: wlan-peap. (s.f.)

- **Control de trama:** identifica el tipo de trama inalámbrica y contiene subcampos para la versión del protocolo, el tipo de trama, el tipo de dirección, la administración de energía y la configuración de seguridad.
- **Duración:** en general, se usa para indicar la duración restante necesaria para recibir la siguiente transmisión de tramas.
- **Dirección 1:** normalmente, contiene la dirección MAC del dispositivo o AP receptor inalámbrico.
- **Dirección 2:** normalmente, contiene la dirección MAC del dispositivo o AP transmisor inalámbrico.

- **Dirección 3:** en ocasiones, contiene la dirección MAC del destino, como la interfaz del *router* (*gateway* predeterminado) a la que se conecta el AP.
- **Control de secuencia:** contiene los subcampos Número de secuencia y Número de fragmento. El Número de secuencia indica el número de secuencia de cada trama. El Número de fragmento indica el número de cada trama que se envió de una trama fragmentada.
- **Dirección 4:** suele faltar, ya que se usa solo en el modo ad hoc.
- **Contenido:** contiene los datos para la transmisión.
- **FCS:** es la Secuencia de verificación de trama, usada para el control de errores de capa 2.

#### 3.2.2.7 Mecanismos de encriptación

La encriptación es transformar los datos que se encuentran en texto plano a un formato no legible, para lo cual requiere de algoritmos de encriptación, mismos que se clasifican en:

**Simétricos:**

- Conocido como algoritmo de clave compartida
- Usualmente tiene una longitud entre 80 y 256 bits **Asimétricos:**
- Conocido como algoritmo de llave pública
- Usualmente tiene una longitud entre 512 y 4.096 bits

**El cifrado puede ser realizado utilizando dos mecanismos:**

**Cifrado simétrico por bloque. -** Al texto plano se lo agrupa en bloques de 64 bits, mismos que luego son cifrados.

**Cifrado de flujo. -** Cada uno de los bits del texto plano es cifrado en línea, por lo que es más rápido que el anterior.

A nivel de redes inalámbricas el estándar a seguir es el establecido en la IEEE802.11i, para el caso de la mayoría de los fabricantes la implementación del 802.11i es WPA2 (*Wireless Protected Access*), el cual utiliza como mecanismo de encriptación el algoritmo AES.

El AES, encripta el contenido de capa dos utilizando información del encabezado de la MAC que les permite a los hosts de destino reconocer si se alteraron los bits no encriptados. Además, agrega un número de secuencia al encabezado de información encriptada.

En los puntos de acceso o *routers* inalámbricos, es posible que no exista WPA o WPA2; en su lugar aparece (PSK: Clave precompartida).

- PSK o PSK2 con TKIP es el mismo que WPA
- PSK o PSK2 con AES es el mismo que WPA2
- PSK2, sin un método de encriptación especificado, es el mismo que WPA2.

### 3.2.3 Seguridad en los Dispositivos de Red

La seguridad el tráfico que sale de la red y escrutar el tráfico ingresante son aspectos críticos de la seguridad en redes. La seguridad del *router* de borde, que se conecta con la red externa, es un primer paso importante al asegurar la red. El *hardening* de dispositivos es una tarea esencial que nunca debe ser pasada por alto. Significa implementar métodos probados para asegurar el *router* físicamente y proteger el acceso administrativo utilizando la interfaz de línea de comandos (*command-line interface* - CLI) del IOS *Cisco,* así como también el Administrador de Routers y Dispositivos de Seguridad de Cisco (*Cisco Router and Security Device Manager* - SDM). Algunos de estos métodos comprenden la seguridad del acceso administrativo, incluyendo mantener contraseñas, configurar funciones de identificación virtual mejoradas e implementar *Secure* Shell (SSH). Como no todo el personal de la tecnología de la información debería tener el mismo nivel de acceso a los dispositivos de infraestructura, definir roles administrativos de acceso es otro aspecto importante de la seguridad los dispositivos de infraestructura. La seguridad de las funciones de administración y reportes del IOS de los dispositivos de Cisco también es importante. Las prácticas recomendadas para asegurar el *syslog*, utilizando el Protocolo de

Administración de Redes Simple (*Simple Network Management Protocol* - SNMP), y configurando el Protocolo de Tiempo de Red (*Network Time Protocol* - NTP) son examinadas. Muchos servicios del *router* están habilitados por defecto. Muchas de estas funciones están habilitadas por razones históricas pero ya no son necesarias.

#### 3.2.3.1. Seguridad en el *router* de *border*

La seguridad en la infraestructura de la red es crítica para toda la red. Considerando como parte de esta infraestructura de la red incluye *routers*, *switches*, servidores, estaciones de trabajo y otros dispositivos.

***Shoulder surfing*** es una manera sorprendentemente fácil para un atacante de ganar acceso no autorizado. Si un atacante obtiene acceso a un *router*, la seguridad y la administración de toda la red pueden ser comprometidas, dejando a los servidores y las estaciones de trabajo bajo riesgo. Es crítico que las políticas y controles de seguridad apropiados puedan ser implementados para prevenir el acceso no autorizado a todos los dispositivos de la infraestructura. Aunque todos los dispositivos de una infraestructura están en riesgo, los *routers* generalmente son el objetivo principal para los atacantes de redes. Esto ocurre porque los *routers* actúan como la policía del tránsito, dirigiendo el tráfico hacia, desde y entre redes. El *router* de borde es el último *router* entre la red interna y una red de confianza como Internet. Todo el tráfico a Internet de una organización pasa por este *router* de borde; por lo tanto, generalmente funciona como la primera y última línea de defensa de una red. A través del filtrado inicial y final, el *router* de borde ayuda a asegurar el perímetro de una red protegida. También es responsable de implementar las acciones de seguridad que están basadas en las políticas de seguridad de la organización.
Por estas razones, es imperativo asegurar los *routers* de la red.

**Enfoque de un solo *router***

Todas las políticas de seguridad están configuradas en este dispositivo. Generalmente se utiliza este esquema en implementaciones de sitios pequeños como sitios de sucursales y SOHO. En las redes más pequeñas, las funciones de seguridad requeridas pueden ser soportadas por ISRs sin comprometer el rendimiento del *router*.

**Enfoque de defensa profunda**

Es más seguro que el de un solo *router*. En este enfoque, el *router* de borde actúa como la primera línea de defensa y se lo conoce como *screening router*. Envía al firewall todas las conexiones dirigidas a la LAN interna.

La segunda línea de defensa es el firewall. El firewall básicamente retoma donde dejó el *router* y realiza filtrado adicional. Provee control de acceso adicional ya que monitorea el estado de las conexiones, actuando como un dispositivo de control.

El *router* de borde tiene un conjunto de reglas que especifican qué tráfico permitir y qué tráfico denegar. Por defecto, el firewall deniega la iniciación de conexiones desde las redes externas (no confiables) para la red interna (confiable). Sin embargo, permite a los usuarios internos conectarse a las redes no confiables y permite que las respuestas vuelvan a través del firewall. También puede realizar autenticación de usuario (proxy de autenticación) para que los usuarios tengan que estar autenticados para ganar acceso a los recursos de la red.

**Enfoque DMZ**

Una variante del enfoque de defensa profunda es ofrecer un área intermedia llamada zona desmilitarizada (*demilitarized zone* - DMZ). La DMZ puede ser utilizada para los servidores que tienen que ser accesibles desde Internet o alguna otra red externa. La DMZ puede ser establecida entre dos *routers*, con un *router* interno conectado a la red protegida y un *router* externo conectado a la red no protegida, o ser simplemente un puerto adicional de un solo *router*. El *firewall*,

ubicado entre las redes protegida y no protegida, se instala para permitir las conexiones requeridas (por ejemplo, HTTP) de las redes externas (no confiables) a los servidores públicos en la DMZ. EL firewall sirve como protección primaria para todos los dispositivos en la DMZ. En el enfoque DMZ, el *router* provee protección filtrando algún tráfico, pero deja la mayoría de la protección a cargo del *firewall*.

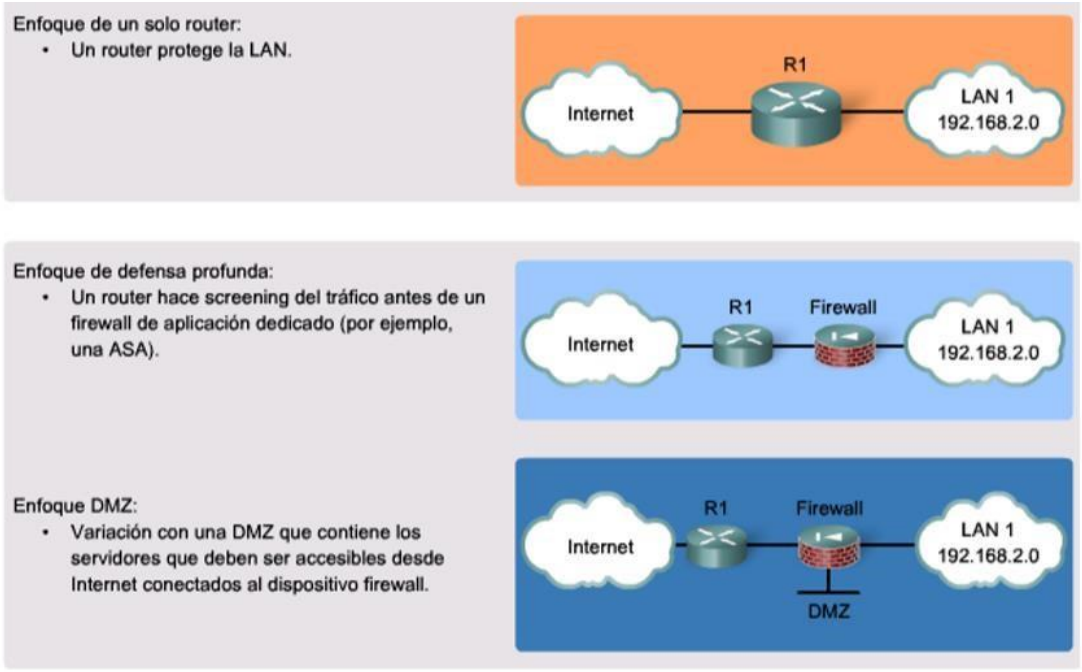



*Figura 27*. Gráfica respectiva *router* de borde

Tomado de: Cisco (s.f.)

Asegurar el *router* de borde es un primer paso crítico en la seguridad de la red. Si hay otros *routers* internos, también deben estar configurados con seguridad. Deben mantenerse tres áreas de seguridad de *routers*.

- Seguridad física
- Seguridad de los Sistemas Operativos
- Seguridad de las funciones y rendimiento de los sistemas operativos del *router*:

**Hardening del router**

Se debe eliminar potenciales abusos de puertos y servicios no utilizados:

- Asegure el control administrativo. Asegúrese de que solo personal autorizado tenga acceso y su nivel de acceso sea controlado.
- Deshabilite puertos e interfaces no utilizadas.
- Reduzca la cantidad de maneras por las que puede accederse a un dispositivo.
- Deshabilitar servicios innecesarios.
- El *router* tiene servicios habilitados por defecto. Algunos de estos servicios son innecesarios y pueden ser utilizados por un atacante para reunir información o para efectuar explotaciones.

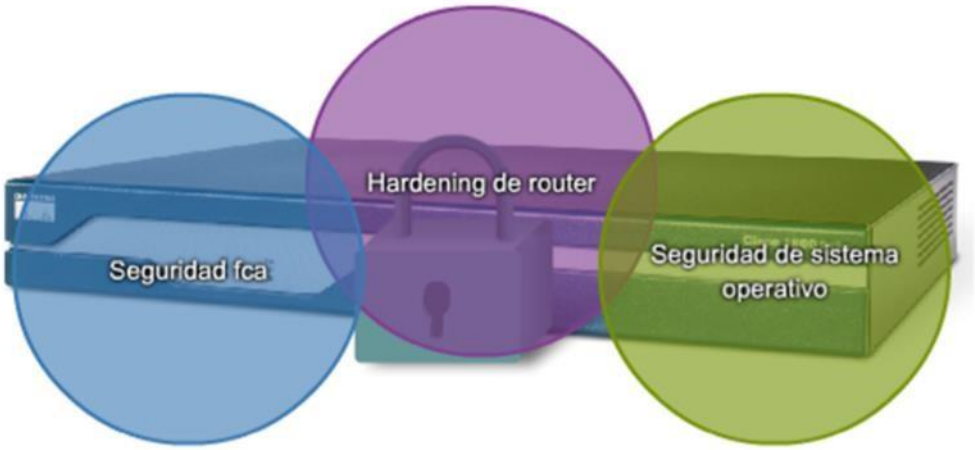



*Figura 28.* Gráfica áreas de seguridad de un *router* de borde
Tomado de: Cisco (s.f.)

**Seguridad física**

Para la ubicación del *router* y los dispositivos físicos que se conectan a él, su accesibilidad solo para personal autorizado, por buenas prácticas dentro de un Data Center el cual tiene el ambiente adecuado para el objetivo, reduciendo la posibilidad de un ataque de DoS a causa de pérdida de electricidad.

**Seguridad de los Sistemas Operativos**

Se debe aplicar en las funciones y rendimiento de los sistemas operativos del *router*, la configuración del *router* se la debe realizar con la máxima cantidad de memoria posible, ya que la disponibilidad de la memoria puede ayudar a proteger la red de ataques de DoS,

Considerar la vulnerabilidad de los datos en tránsito sobre un canal de comunicación expuestos a *sniffing*, secuestros de sesión y ataques *man* in *the middle* (MITM). Hay dos maneras de acceder a un dispositivo para propósitos administrativos: local y remotamente.

**Local**, todos los dispositivos de la infraestructura de la red puede ser accedidos localmente. El acceso local a un *router* usualmente requiere una conexión directa a un puerto de consola en el *router* utilizando una computadora que esté ejecutando software de emulación de terminal.

**Remotamente**, El acceso remoto típicamente requiere permitir conexiones *Telnet*, *Secure Shell* (SSH), HTTP, HTTPS o *Simple Network Management Protocol* (SNMP) al *router* desde una computadora. Esta computadora puede estar en la misma subred o en una diferente.

Algunos protocolos de acceso remoto envían al *router* los datos en texto plano, incluyendo nombres de usuario y contraseñas. Si un atacante logra reunir tráfico de red mientras un administrador está autenticado remotamente a un *router*, el atacante podrá capturar las contraseñas o información de configuración del *router*. Por esta razón, se prefiere permitir solo acceso local al *router*. Sin embargo, el acceso remoto puede ser necesario de cualquier forma.

3.2.2.2. Precauciones: Acceso a la red remotamente

**Cifrar todo el tráfico** que entre hacia el equipo del administrador y el *router*.

- En lugar de usar Telnet, usar SSH.

- en lugar de usar HTTP, usar HTTPS.
- Establecer una red de administración dedicada.
- La red de administración deberá incluir solo hosts de administración identificados y conexiones a una interfaz dedicada en el *router*.
- Configurar un filtro de paquetes para permitir que solo los hosts de administración identificados y protocolos de preferencia accedan al *router*.
- Por ejemplo, permitir solo solicitudes SSH de la dirección IP del host de administración para iniciar una conexión a los *routers* en la red.

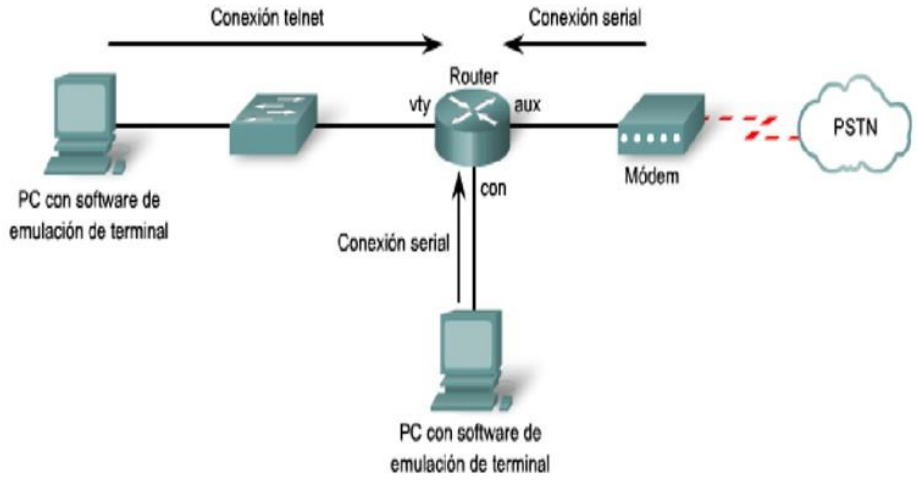



*Figura 29.* Métodos de acceso al *router* de borde
Tomado de: Cisco (s.f.)

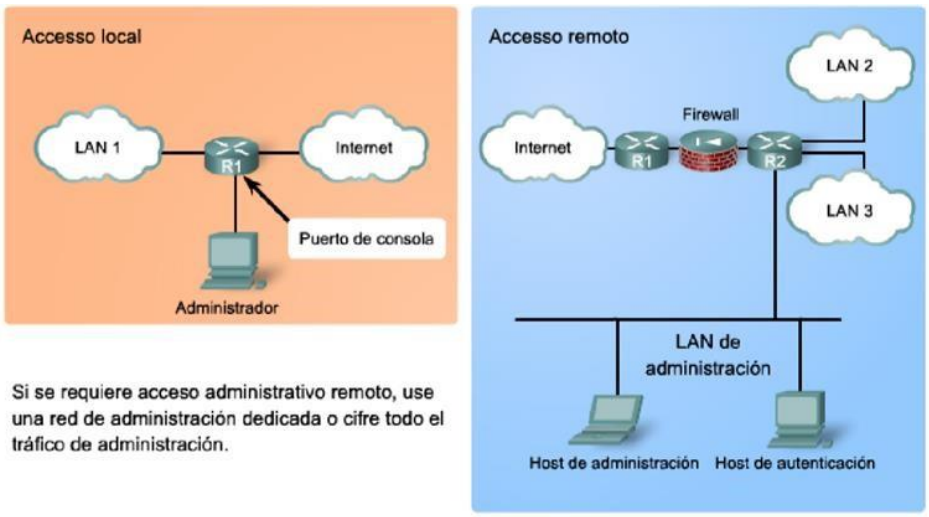



*Figura 30.* Métodos de acceso local y remoto al *router* de borde
Tomado de: Cisco (s.f.)

3.2.3.3. Configuración de acceso administrativo seguro[4]

Para contrarrestar los ataques se usan varios métodos de descubrimiento de contraseñas administrativas.

***Shoulder surfing***, intentar adivinar las contraseñas basándose en la información personal del usuario

***Sniffing* de los paquetes TFTP**, que contienen archivos de configuración en texto plano.

**Herramientas como *L0phtCrack* y Cain & Abel**, para efectuar ataques de fuerza bruta para adivinar las contraseñas.

**Gestión de Contraseñas**

En cuanto a la protección de *routers* y *switches*, se debe seguir estos parámetros para elegir contraseñas fuertes y no sean descubiertas por medio de herramientas de cracking y de adivinación inteligente:

**Políticas**

- Utilice una contraseña de 10 o más caracteres de longitud (Cuanto más larga, mejor)
- Contraseña compleja (Incluya una mezcla de letras mayúsculas y minúsculas, símbolos y espacios).
- Evite contraseñas basadas en repeticiones, palabras de diccionario, secuencias de letras o números, nombres de usuario, nombres de mascotas o parientes, información biográfica (como cumpleaños, número de pasaporte o documento, nombres de ancestros) u otros tipos de información fácilmente identificable.
- Cambie las contraseñas seguido.

- No escriba las contraseñas en papel o las deje en lugares obvios como el escritorio o el monitor.

Los administradores deben asegurarse de que se usen contraseñas fuertes en toda la red. Una manera de lograr esto es usando las mismas herramientas de ataques de fuerza bruta y cracking que usaría un atacante para verificar la solidez de las contraseñas.

Varios puertos de acceso requieren contraseñas en un *router*, incluyendo el puerto de consola, el puerto auxiliar y las conexiones de terminal virtual. La administración de las contraseñas en una red grande debería mantenerse por medio de un servidor de autenticación central TACACS+ o RADIUS como el Servidor de Control de Acceso Seguro de Cisco (ACS). Todos los *routers* deben ser configurados con las contraseñas de usuario y de EXEC privilegiado. También se recomienda el uso de una base de datos de nombres de usuario local como copia de resguardo si el acceso a un servidor de autenticación, autorización y registro de auditoría (*authentication*, *authorization*, *and accounting* - AAA) se encuentra comprometido. El uso de una contraseña y la asignación de niveles de privilegios son maneras simples de proporcionar control de acceso terminal en una red. Deben establecerse contraseñas para el modo de acceso EXEC privilegiado y líneas individuales como las líneas de consola y auxiliar.

**Contraseña *enable secret***

El comando de configuración *enable secret* contraseña restringe el acceso al modo EXEC privilegiado. La contraseña *enable secret* siempre está dispersa (*hashed*) dentro de la configuración del *router* usando un algoritmo *Message Digest* 5 (MD5). Si la contraseña *enable secret* se pierde o se olvida, debe ser reemplazada utilizando el procedimiento de recuperación de contraseñas de los *routers* Cisco.

**Línea de consola**

Por defecto, el puerto de línea de consola no requiere una contraseña para el acceso administrativo de la consola; sin embargo, siempre debe ser configurado con una contraseña a nivel de línea de puerto de consola. Use el comando line *console* 0 seguido de los subcomandos *login* y *password* para solicitar el ingreso y establecer una contraseña de ingreso en la línea de consola.

**Líneas de terminal virtual**

Por defecto, los *routers* de Cisco soportan hasta cinco sesiones simultáneas de terminal virtual vty (Telnet o SSH). En el *router*, los puertos vty se numeran del 0 al 4. Use el comando line vty 0 4 seguido por los subcomandos *login* y *password* para solicitar ingreso y establecer una contraseña de ingreso a las sesiones Telnet entrantes.

**Línea auxiliar**

Por defecto, los puertos auxiliares del *router* no requieren una contraseña para acceso administrativo remoto. Los administradores algunas veces usan este puerto para configurar y monitorear remotamente el *router* usando una conexión de módem *dialup*.

Para acceder a la línea auxiliar, use el comando *line aux* 0. Use los subcomandos *login* y *password* para solicitar ingreso y establecer una contraseña de ingreso a las conexiones entrantes.

Por defecto, con excepción de la contraseña *enable secret*, todas las contraseñas de *router* de Cisco están almacenadas en texto plano dentro de la configuración del *router*. Estas contraseñas pueden ser visualizadas con el comando *show running-config*. Los *sniffers* también pueden ver estas contraseñas si los archivos de configuración de servidor TFTP atraviesan una conexión no asegurada de intranet o Internet. Si un intruso gana acceso al servidor TFTP donde están almacenados los archivos de configuración del *router*, podrá obtener estas contraseñas

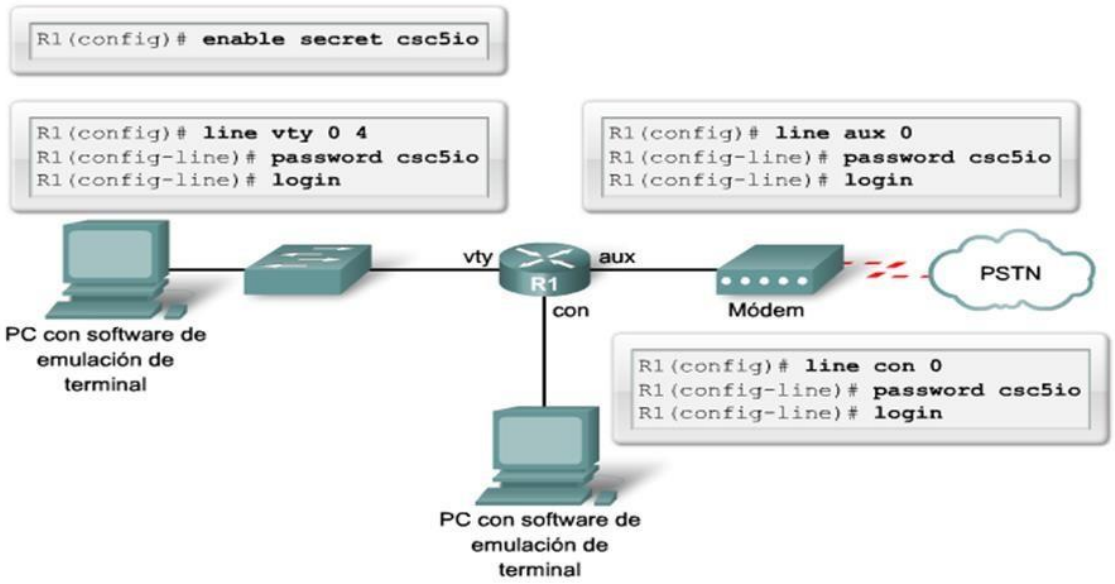



*Figura 31*. Métodos de acceso al *router* de borde
Tomado de: Cisco (s.f.)

**Cifrar todas las contraseñas**

Por defecto, algunas contraseñas se muestran en texto plano, o sea, sin cifrar, en la configuración del software IOS de Cisco. Con excepción de la contraseña *enable secret*, todas las otras contraseñas en texto plano en el archivo de configuración pueden ser cifradas con el comando *service passwordencryption*. Este comando dispersa contraseñas en texto plano actuales y futuras en el archivo de configuración a un texto cifrado. Solo las contraseñas creadas luego de que se emita el comando no serán no cifradas. Las contraseñas ya existentes que estén cifradas permanecerán de esa manera.

El comando *service password-encryption* es útil principalmente para evitar que individuos no autorizados puedan ver contraseñas en el archivo de configuración. El algoritmo utilizado por el comando *service passwordencryption* es simple y fácilmente reversible por alguien que tenga acceso al texto cifrado y una aplicación de cracking de contraseñas. Por esta razón, el comando no deberá ser utilizado con la intención de proteger los archivos de configuración contra ataques serios.

El comando *enable secret* es mucho más seguro, ya que cifra la contraseña utilizando MD5, un algoritmo mucho más fuerte.

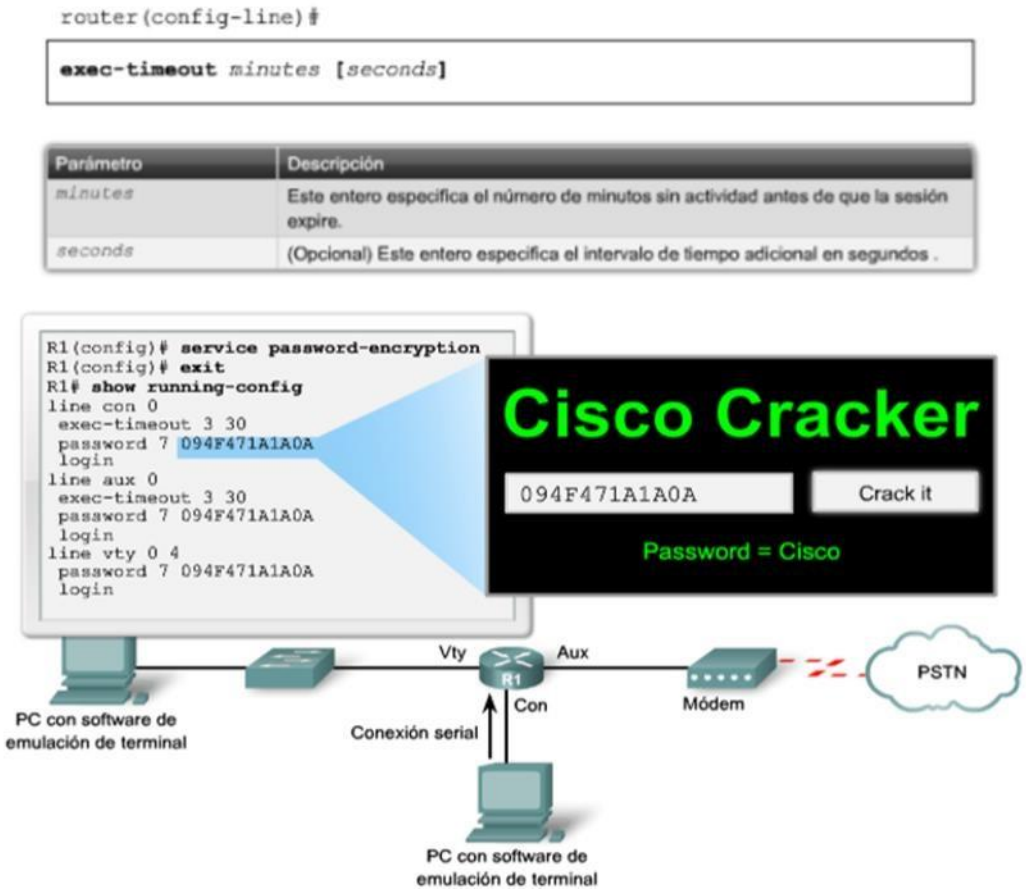



*Figura 32*. Cifrado de contraseñas

Tomado de: Cisco (s.f.)

**Configuración de SSH**

En el acceso remoto, también es importante considerar las implicancias de seguridad al enviar información a través de la red. Básicamente, el acceso remoto en los *routers* era configurado usando Telnet sobre el puerto 23 de TCP. Sin embargo, Telnet fue desarrollado cuando la seguridad no era un problema, por lo tanto, todo el tráfico de Telnet se envía en texto plano. Al usar este protocolo, los datos críticos, como configuraciones del *router*, son de fácil acceso para los atacantes. Los hackers pueden capturar paquetes reenviados por la computadora de un administrador usando un analizador de protocolos como

*Wireshark*. Si el atacante captura el flujo Telnet inicial, podrá aprender el nombre de usuario y la contraseña del administrador.

No obstante, el acceso remoto puede ahorrarle tiempo y dinero a una organización a la hora de hacer cambios necesarios en la configuración.
SSH ha reemplazado a Telnet como práctica recomendada para proveer administración de *router* remota con conexiones que soportan confidencialidad e integridad de la sesión.

Provee una funcionalidad similar a una conexión Telnet de salida, con la excepción de que la conexión está cifrada y opera en el puerto 22. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura.

Necesariamente deben completarse cuatro pasos antes de configurar un *router* para el protocolo SSH:

**Paso 1**. Asegurarse de que los *routers* destino estén ejecutando una imagen del IOS de Cisco *release* 12.1(1) T o posterior, para que soporten SSH. Solo las imágenes criptográficas del IOS de Cisco que contienen el grupo de funciones *IPsec soportan* SSH. Específicamente, las imágenes criptográficas del IOS de Cisco 12.1 o la posterior *IPsec* DES o el *Triple Data Encryption Standard* (3DES) soportan SSH. Estas imágenes generalmente tienen el ID k8 o k9 en su nombre de imagen. Por ejemplo, c1841- *advipservicesk9-mz*.124-10b.*bin* es una imagen que soporta SSH.

**Paso 2.** Asegurarse de que cada uno de los *routers* destino tenga un nombre de host único.
**Paso 3**. Asegurarse de que cada *router* destino esté usando el nombre de dominio correcto para la red.

**Paso 4.** Asegurarse de que los *routers* destino estén configurados para autenticación local o servicios AAA para autenticación de usuario y contraseña. Esto es obligatorio para una conexión SSH de *router* a *router*.

**Configuración de un *router* para que soporte SSH:**

En la figura 33, demuestra la configuración de SSH en un simulador de diseño de red.

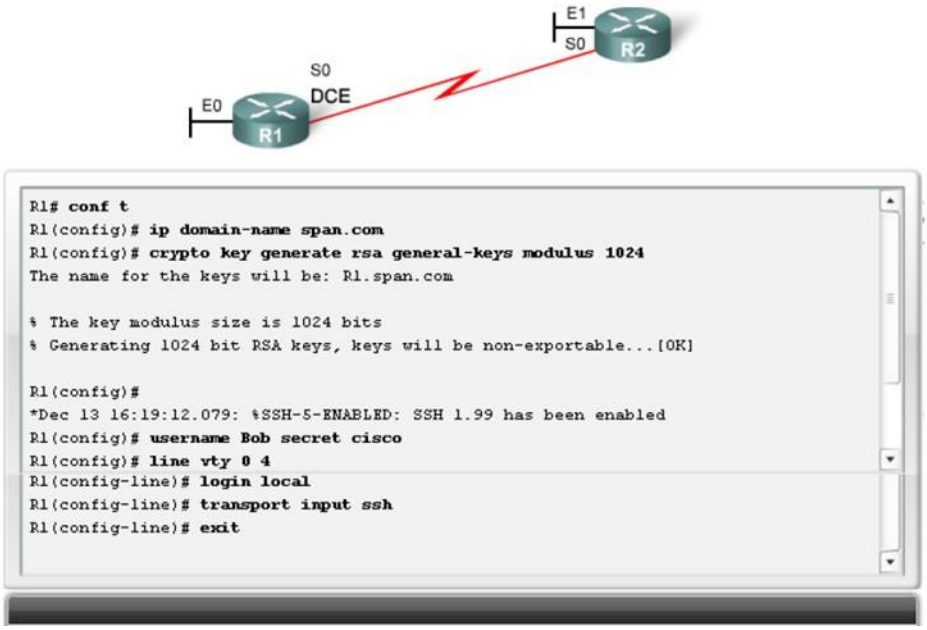



*Figura 33.* Configuración de SSH en un *router*

Tomado de: Cisco (s.f.)

- Configurar el nombre del dominio IP
- Generar claves secretas de una sola vía
- Verificar o crear una entrada en la base de datos local
- Habilitar sesiones SSH VTY de entrada

# 4. CONCLUSIONES Y RECOMENDACIONES

## 4.1 Conclusiones

La seguridad de la información brinda prestaciones de confidencialidad, disponibilidad e integridad de datos, en la red en base al esquema general de seguridad propuesto, tomando como guía referencial la Política de Seguridad de la Información y capitulo 6 Gestión de Comunicaciones y Operaciones ítem 6.14 seguridad de los servicios de la red de la norma ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Se presenta un esquema general de seguridad de redes basada en la seguridad de los dispositivos de red puntualmente en los *router* de borde, puerta de ingreso y salida de la información.

En este esquema de seguridad propuesta se puntualiza la seguridad en el acceso, donde se propone precauciones al acceso remoto y se configura el esquema de acceso administrativo para resguardar las prestaciones que la información debe tener al ser transmitida y recibida.

## 4.2 Recomendaciones

En base al estudio de este proyecto sobre seguridad de redes, se recomienda establecer una capacitación sobre políticas de seguridad en el uso y acceso a la red.

Se recomienda fortalecer al esquema de seguridad de red en el *router* de borde ya que este constituye la puerta de ingreso y salida de la información.

Se recomienda fortalecer y precautelar al acceso remoto y acceso administrativo para resguardar las prestaciones que la información debe tener al ser transmitida y recibida.

Asignar autorizaciones sólo a los usuarios que las necesiten para que sean usadas adecuadamente.

## REFERENCIAS

Acssi. (2015). Seguridad informática. Barcelona: Ediciones ENI

Areitio, J. (2008). Seguridad de la Información. Redes, Informática y Sistemas de Información. Universidad de Deusto

Calder, A., Watkins, S. (2010). *Information Security Risk Management for ISO27001/ ISO27002.* IT *Governance Publishing.*

Carpentier, J. (2016). La seguridad informática en la pyme. Barcelona: Ediciones ENI.

Chicano, E. (2014). Auditoria de seguridad informática. Málaga: IC Editorial.

Del Pozo, H. (2013). Esquema gubernamental de seguridad de la información. Ecuador: Editora Nacional.

Dordoigne, J. (2015). Redes informáticas. Barcelona: Ediciones ENI.

ISO27000.ES. (2012). El portal de ISO 27001 en español. Recuperado el 09 de septiembre del 2017 de http://www.iso27000.es/

Rivera, J. (2016). Fundamentos de redes informáticas. Estados Unidos: *CreateSpace.*

Santos, J., Gónzalez, L. (2010). Seguridad Informática. RA-MA S.A. Editorial y Publicaciones

Stallings, W., González Rodríguez, M. and Joyanes Aguilar, L. (2010). Fundamentos de seguridad en redes. Madrid: Pearson Prentice Hal.

# ANEXOS

# 1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## 1.1. Documento de la Política de la Seguridad de la Información

a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (*)[1].

b) Se difundirá la siguiente política de seguridad de la información como referencia (*):

"Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.