

Fredys A. Simanca H.  
Fabián Blanco Garrido  
Eduardo Triana Moyano

# LAS REDES MESH



**UNIVERSIDAD  
LIBRE®**

Facultad de Ingeniería

**Las Redes MESH**

Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano. -- Bogotá : Universidad Libre, 2018.

165 p. : il. ; 24 cm.

Incluye referencias bibliográficas.

978-958-5466-19-7

1. Redes de computadores 2. Arquitectura de redes de computadores 3. Redes de computadores - Protocolos I. Blanco Garrido, Fabián II. Triana Moyano, Eduardo

004.6

SCDD 21

Catalogación en la fuente - Universidad Libre. Biblioteca.

*Comentarios y sugerencias:*

*Correo e-de los autores:*

fredysa.simanca@unilibre.edu.co

fabian.blancog@unilibre.edu.co

eduardo.trianam@unilibre.edu.co

© Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano, 2018

© Facultad de Ingeniería, 2018

© Universidad Libre Sede Principal, 2018

ISBN IMPRESO: 978-958-5466-19-7

ISBN DIGITAL: 978-958-5466-20-3

Queda hecho el depósito que ordena la ley.

Reservados todos los derechos. No se permite la reproducción total o parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin la autorización previa y por escrito de los titulares del copyright.

*Editorial:* Universidad Libre

*Coordinación de Publicaciones y Comunicaciones:* Luz Bibiana Piragauta Correa

*Correo-e:* comunicaciones@unilibre.edu.co

*Coordinación de edición:* Siby I. Garcés Polo

*Correo-e:* siby.garcés@unilibre.edu.co

Calle 8 No. 5-80, Tel.: 3821000, Bogotá D.C.

*Diseño y diagramación:* AFM Producción Gráfica S.A.S.

Esta obra está cofinanciada por el Fondo de Publicaciones de la Universidad Libre

Impreso en Colombia en los talleres gráficos  
de AF&M Producción Gráfica S.A.S.

Calle 63B No. 71E 45 of. 402

Tel.: +57(1) 5251938

afmproducciongrafica@gmail.com

Bogotá D.C., Colombia, 2018

*Printed in Colombia*

## **Directivas Universidad Libre**

<i>Presidente</i>	Jorge Alarcón Niño
<i>Vicepresidente</i>	Jorge Gaviria Liévano
<i>Rector Nacional</i>	Fernando Enrique Dejanón Rodríguez
<i>Secretario General</i>	Floro Hermes Gómez Pineda
<i>Censor Nacional</i>	Ricardo Zopó Méndez
<i>Director Nacional de Planeación (e)</i>	Alejandro Muñoz Ariza
<i>Directora Nacional de Investigaciones</i>	Elizabeth Villarreal Correcha
<i>Presidente Seccional</i>	Julio Roberto Galindo Hoyos
<i>Rector Seccional</i>	Jesús Hernando Álvarez Mora
<i>Decana Facultad de Ingeniería</i>	Martha Rubiano Granada
<i>Directora Centro de Investigación Facultad Ingeniería (CIFI)</i>	Siby Inés Garcés Polo
<i>Director Programa de Ingeniería de Sistemas</i>	Mauricio Alonso Moncada



Para nuestros alumnos,  
quienes a través de los años  
nos han enseñado tanto.

**Los autores**





# Contenido

Prólogo .....	13
Introducción.....	17

## (1) Esquematización teórica

Introducción.....	21
1.1. ¿Qué es una red en malla o MESH? .....	21
1.2 Ventajas de las redes MESH .....	23
1.3 Desventajas de las redes MESH.....	24
1.4 Generaciones de las redes MESH .....	25
1.5 Topologías de las redes MESH .....	27
1.7 Redes de infraestructura.....	34
1.8 Redes libres .....	38
1.9 Redes inalámbricas tipo malla.....	39
1.10 Arquitectura de las redes MESH .....	40
1.11 Protocolos de enrutamiento.....	42
1.12 Infraestructura para redes MESH.....	45
1.13 Plan Vive Digital.....	51
1.15 Ataques a Redes WLAN.....	56
1.16 Mecanismos de seguridad.....	59
1.17 El contexto de las redes MESH .....	63
1.18 Atributos de una red MESH.....	64
1.19 Rango y flujo de datos .....	65
1.20 Fuerzas electromagnéticas .....	69
1.21 Contexto social de las redes MESH.....	82
1.22 Manifiesto de las redes libres.....	85
Conclusión.....	88



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ( 2 ) Construcción de un esquema para las infraestructuras de Redes MESH en entornos comunitarios o rurales de Colombia

Introducción.....	89
2.1 Diseño del esquema de red .....	89
Conclusión.....	94

## ( 3 ) Construcción de un esquema tecnológico para protocolos de enrutamiento en Redes MESH

Introducción.....	95
3.1 Diseño de la red .....	95
3.2 Análisis de protocolos de enrutamiento.....	97
3.3 Métrica para evaluar los protocolos propuestos .....	104
Conclusión.....	104

## ( 4 ) Diseño de una arquitectura de seguridad para Redes MESH en entornos comunitarios o rurales de Colombia

Introducción.....	105
4.1 Diseño de la red .....	105
4.2 WEP ( <i>Wired Equivalent Privacy</i> - Privacidad Equivalente al Cable)...	105
4.3 WPA ( <i>Wi-Fi Protected Access</i> , Acceso Protegido Wi-Fi).....	109
4.4 WPA2 (802.11i).....	112
4.5 SSH ( <i>Secure Shell</i> ).....	115
4.6 SSL ( <i>Secure Sockets Layer</i> ).....	118
4.7 HTTPS (Protocolo seguro de transferencia de hipertexto) .....	121
4.8 PPTP (Protocolo de túnel punto a punto) .....	123
4.9 Resumen de los protocolos de seguridad.....	125
Conclusión.....	131

## ( 5 ) Valoración financiera para la implementación de sistemas de interconexión MESH

Introducción.....	133
5.1 Diseño ingenieril de la solución.....	133



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

5.2 Ruta de control del proyecto .....	133
5.3 Escenario de gestión financiera .....	135
5.4 Ruta crítica .....	140
5.5 Ponderación y análisis económico de inversión .....	144
Conclusión .....	149
Referencias bibliográficas .....	151



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## Índice de figuras

Figura 1.1.	Red MESH de primera generación.....	25
Figura 1.2.	Red MESH segunda generación.....	26
Figura 1.3.	Red MESH de tercera generación.....	27
Figura 1.4.	Escenario de red.....	27
Figura 1.5.	Topología Ad-hoc .....	28
Figura 1.6.	Topología de infraestructura.....	28
Figura 1.7.	Red en topología estrella.....	35
Figura 1.8.	Red punto a punto. ....	36
Figura 1.9.	Red con conexión por medio de repetidor.....	37
Figura 1.10.	Topología malla completa.....	38
Figura 1.11.	Topología de malla parcial. ....	38
Figura 1.12.	Infraestructura MESH.....	41
Figura 1.13.	Esquema de funcionamiento de una red MESH.....	45
Figura 1.14.	Red de infraestructura.....	45
Figura 1.15.	Red de clientes mallados.....	46
Figura 1.16.	Red híbrida. ....	46
Figura 1.17.	Mapas de conexión en Colombia.....	52
Figura 1.18.	Categorías de redes inalámbricas por su área de cobertura .	55
Figura 1.19.	Simbología.....	58
Figura 1.20.	Relación con la que se modifica las IP.....	58
Figura 1.21.	Validadores, Suplantantes mediante <i>Spoofing</i> .....	59
Figura 1.22.	Ilustración del ataque MITM.....	59
Figura 1.23.	Mecanismos de seguridad para la instalación de redes inalámbricas.....	61
Figura 1.24.	Diagrama del protocolo PPTP de Microsoft.....	63
Figura 1.25.	Inspiración de iniciativa de redes MESH.....	64
Figura 1.26.	Canales y frecuencias despejadas para 802.11b/g/n.....	72
Figura 1.27.	Representación de un patrón de radiación.....	81
Figura 1.28.	Colegio Rafael Uribe Uribe, sede secundaria. ....	83
Figura 1.29.	Universidad Libre, sede Bosque Popular.....	84
Figura 1.30.	Barrio Fátima, dirección Calle 51 A sur # 37-65. ....	85
Figura 2.1.	Modo de operación de una red MESH.....	90
Figura 2.2.	Diagrama de una red MESH Total Simple. ....	90
Figura 2.3.	Diagrama de una red MESH parcial.....	91
Figura 2.4.	Esquema básico de conexión PTP.....	92



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Figura 2.5. Esquema básico de enlace PMP.....	93
Figura 2.6. Esquema básico de una red en malla (MESH) multipunto a multipunto.....	94
Figura 3.1. ETX routing metric: OLSR-ETX.....	98
Figura 3.2. Propagación del paquete hello generado por OLSR. ....	98
Figura 3.3. Route Request. ....	100
Figura 3.4. Route Reply.....	100
Figura 3.5. Router Error.....	100
Figura 3.6. Formatos del paquete general BATMAN.....	102
Figura 5.1. Elementos parametrizados del control.....	134
Figura 5.2. Cuadrilátero de la confiabilidad.....	135
Figura 5.3. Relación operacional de factores de control del proyecto..	136
Figura 5.4. Rentabilidad sobre inversión (RSI).....	138
Figura 5.5. Comparación económica Empresa X y Y. ....	139
Figura 5.6. Asignación de tiempos red de actividades. ....	141
Figura 5.7. Ponderación de inicio rápido. ....	142
Figura 5.8. Cálculo de tiempos tardíos proyecto.....	143
Figura 5.9. Ruta crítica red de actividades.....	144
Figura 5.10. Configuración base de solución MESH. ....	145



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## Índice de tablas

Tabla 1.1.	Enrutamiento dinámico vs. enrutamiento estático.....	43
Tabla 1.2.	Barreras que impiden la masificación de Internet en Colombia .....	54
Tabla 1.3.	Rango de velocidades de los protocolos .....	65
Tabla 1.4.	Rango de velocidades 802.11a/b/g vs 802.11n.....	67
Tabla 1.5.	Pérdida de espacio libre en 2.4 GHZ. ....	76
Tabla 1.6.	Conversión de decibelios a vatios.....	80
Tabla 4.1.	WEP (Wired Equivalent Privacy, privacidad equivalente al cable). ....	126
Tabla 4.2.	WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi).....	127
Tabla 4.3.	WPA2 (802.11i). ....	128
Tabla 4.4.	SSH (Secure Shell). ....	129
Tabla 4.5.	SSL (Secure Sockets Layer).....	130
Tabla 4.6.	HTTPS (Protocolo Seguro de Transferencia de Hipertexto)...	131
Tabla 5.1.	Guía de control proyecto MESH.....	148
Tabla 5.2.	Matriz de pérdidas económicas.....	149



## Prólogo

La comunicación, como elemento fundamental de los sistemas, ha sido tema de investigación y de diferentes escritos en publicaciones diversas, desde trabajos como ensayos en la educación básica hasta libros que abordan asuntos de alta complejidad en el ámbito de los protocolos y los sistemas distribuidos. Difícil resulta abrir con un prólogo sobre las redes MESH sin abordar el acontecer histórico que, en nuestro país, le da el realce y la importancia que se merece este tipo de tecnología, la cual dirige la utilidad de su uso hacia espacios sociales menos favorecidos, y con la necesidad de contar con herramientas y elementos que coadyuven con su desarrollo, y sus oportunidades en el ámbito local o internacional. Abordemos entonces este escrito, desde el contexto histórico por el que ha atravesado el país, en estos marcos de la tecnología, la informática, las comunicaciones y la Ingeniería.

Colombia, como uno de los países que ha adoptado de otras regiones del orbe la tecnología de las comunicaciones, ha atravesado por diferentes estadios cronológicos en asuntos de las redes y los ambientes de cómputo, tanto de hardware como de software. Es así como desde finales de los años 70 del siglo pasado, existieron intentos de conectar e integrar los sistemas de software sobre estructuras de red que permitieran compartir la información, cumpliendo con métricas como la escalabilidad, la accesibilidad, la escalabilidad y la modularidad, donde las empresas del momento se comprometieron a probar los ambientes ofrecidos por otras que incursionaban en el ámbito de la informática.

Hacia mediados de los años 70, se inicia una era de mecanización y de automatización donde empresas bancarias, de servicios, de distribución y de fabricación buscaban un mejor rendimiento y control para sus operaciones, dados los objetivos de crecimiento tanto a nivel de rendimientos financieros como a nivel de la cobertura en espacios territoriales más amplios. Las inversiones extranjeras se hacían mayores y la tecnificación de los sistemas



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

informáticos era una necesidad creciente. Organizaciones como “Unión de Industrias Químicas”, hacían inversiones en empresas como PAAD (Productora Andina de ácidos y Derivados), Petroquímica Colombiana, Carboquímica o Poliquímicos y, el ofrecimiento de sus productos comenzaba a depender de canales de comunicación más efectivos.

Hacia inicios y mediados de los años 80, esta necesidad de hacer cada vez más efectivos los sistemas de comunicación se acrecientan y se buscan alternativas en los sistemas de red, utilizando los marcos de multilink o Novell en compañías de tamaño mediano. Redes que, a la postre, serían reemplazadas por otras que funcionaban con la filosofía de la red estrella, dejando de lado a las de tipo token ring o de bus exclusivamente. El surgimiento de compañías como Computone dio la posibilidad de interconectar terminales a los sistemas de red, que funcionaban con ambientes operativos como UNIX o XENIX, fortaleciendo el desarrollo de otras compañías como SCO (Santa Cruz Operation), la cual potenció considerablemente el desarrollo de los sistemas de microcomputador, especialmente en los equipos AT de IBM.

El universo de la computación, la informática y las comunicaciones, se vió ampliamente fortalecido cuando la OSF (Open Software Foundation) hacia inicios de los años 90 determina establecer un estándar de protocolos, y de sistemas de software de aplicación para los sistemas operativos basados en minicomputadores y en main frames, al mismo tiempo que Microsoft Corporation define sus estándares de programación basados en sus DLL's (Dynamic Link Library) y en su filosofía de operatividad bajo OLE (Object Linking Embedded). Esta situación hizo necesario el hecho de establecer estándares en los protocolos de comunicación ya que la OSF propendía por TCP/IP (Transmission Control Protocol/Internet Protocol), mientras que Microsoft lo hacía sobre NetBeui.

Lo anterior fue protagonista de un giro colectivo para mirar en la misma dirección y, evitar así que la discrepancia de opiniones y de versiones de productos de software dieran al traste, y los usuarios tuvieran que invertir esfuerzo y capital económico para utilizar los sistemas de la OSF y de Microsoft en caso de necesitarlo. Fue así como SCO (Santa Cruz Operation) dio los primeros pasos cuando ofreció el paquete de “Term Vision”, permitiendo que los usuarios de UNIX y de Microsoft pudieran ver sus sistemas de archivos como si se tratase de ambientes nativos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Este periplo de la historia de la comunicación en ambientes de cómputo ha señalado una directriz de interoperabilidad, donde el surgimiento de la Internet entra a jugar un papel importante, señalizando el derrotero hacia el cual las compañías de negocios y las instituciones educativas y del estado, formalizan su quehacer y lo ubican en un entramado informático para compartir recursos, tanto de hardware como de software, organizando verdaderos clusters de comunicación, donde ahora el costo y la cobertura son tan importantes como lo eran antes los primeros sistemas. Es aquí donde el presente libro contribuye de manera significativa, tratando el tema de las redes MESH como una alternativa de interconexión, de comunicación y de interoperabilidad menos costosa, donde el componente social y de cobertura se hace crucial, para que los entornos menos favorecidos económicamente puedan acceder a los servicios de la educación, y de los campos que las TIC, en general, presentan como herramientas de progreso.

PEDRO ALONSO FORERO SABOYA  
*Editor*





## Introducción

Gracias al avance tecnológico, en la actualidad, la mayoría de información transita en línea y en tiempo real, el siguiente paso cercano es lograr un acceso inalámbrico de acceso a servicios por parte de los usuarios. Así se destaca la presencia de redes MESH para la utilización de las redes inalámbricas en frecuencia de 2.4 GHz y 5 GHz.

El alto costo, la deficiencia en la prestación de servicios de las redes y la baja e intermitente conectividad, reflejan las debilidades de operación de los dispositivos WIFI, en sectores comunitarios y rurales del país. Por lo tanto, se plantea la posibilidad de potenciar las características de las redes MESH, como una alternativa que maximiza la interconectividad en la comunidad y áreas rurales.

Esta alternativa de configuración de redes con topología en malla da lugar a la formulación de una nueva metodología de diseño e implementación de una red MESH que, en prospectiva, reduciría esa brecha tecnológica entre las comunidades y las TIC, y que se diferencia sustancialmente de los proveedores comunes de internet.

Bajo este contexto se plantea la formulación y ejecución del proyecto de investigación que presenta como objetivo principal, el diseño e implementación de redes inalámbricas mediante la utilización de la topología en malla para realizar conectividad WiFi, en espacios geográficos específicos teniendo en cuenta las condiciones topográficas de Colombia, buscando reducir costos de implementación e inconvenientes de cobertura de WiFi.

Al trabajar bajo el supuesto que se puede diseñar e implementar redes inalámbricas mediante la utilización de la topología en malla, se dimensiona la infraestructura tecnológica requerida para garantizar la efectividad de la



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

solución planteada, además, de realizar la configuración de comunicación como medio de manejo de la información, utilizando protocolos abiertos y seguros de comunicación. Todo lo anterior se validad por medio de la aplicación a un caso de estudio.

La metodología de la presente investigación se realizó bajo el concepto de ingeniería didáctica, que consiste en la combinación de elementos didácticos aplicados directamente al planteamiento de la solución del problema planteado.

El presente libro esta comúestodo de cinco capítulos, en el primer capítulo se presenta la esquematización teórica de redes MESH, resaltando sus ventajas en areas rurales, sector al que va dirigido el presente estudio, se muestran las tres generaciones de la red y la topología. Para complementar la conceptualización, se presenta la definición de las topologías de estrella, el punto a punto, los repetidores, la topología en malla, la topologia en malla completa y la topología en malla parcial. El capitulo uno termina con las principales teorías de redes libres y redes inalambricas tipo malla.

El segundo capítulo trata de la construcción de un esquema para las infraestructuras de redes MESH en entornos comunitarios o rurales de Colombia, se presenta el esquema de la red, iniciando con el diagrama de una red MESH total simple y una parcial y el diseño, basado en el enlace punto a punto, punto a multipunto y multipunto a multipunto.

Para el tercer capitulo, se incluye la construcción de un esquema tecnológico para protocolos de enrutamiento en redes MESH, y se abordan lo siguientes: OLSR (*Optimized Link State Routing*) por estado de enlace; AODV (*Ad-Hoc On Demand Distance Vector*) por demanda, HSLS (*Hazy Sighted Link State Routing Protocol*) recomendado para redes de mas de mil nodos; BATMAN (*Mobile Ad-hoc Networks MANETs*) usan uno o multiples saltos, El PWRP (*Predictive Wireless Routing Protocol*) utiliza routers móviles y Babel (*A loop-free distance-vector routing protocol*) utiliza el vector de distancias.

El diseño de la arquitectura de seguridad se presenta en el capítulo cuatro, que determina la mejor alernativa y se presentan las características, ventajas y desventajas de los protocolos WEP (*Wired Equivalent Privacy - Privacidad Equivalente al Cable*) basado en el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC; WPA (*Wi-Fi Protected Access*,



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Acceso Protegido Wi-Fi) con base en claves dinámicas; WPA2 (802.11i) utiliza la encriptación; SSH (*Secure Shell*) usa información cifrada; SSL (*Secure Sockets Layer*) es criptográfico, HTTPS (Protocolo seguro de transferencia de hipertexto) basado en un esquema de petición respuesta y PPTP (Protocolo de túnel punto a punto) que utiliza la encriptación.

Para completar el libro, en el último capítulo se presenta la valoración financiera de la implementación de sistemas de interconexión MESH, que suministra información relativa a la viabilidad económica según los principios de gestión financiera, indicador de liquidez, prueba ácida, capacidad de endeudamiento, indicadores de rentabilidad, una ruta crítica para determinar tiempo de inicio y terminación de la implementación y la ponderación y análisis económico de inversión.





( 1 )

## Esquematización teórica

### • Introducción

El avance en TIC va mas allá del internet, como es el caso de la conexión por medio de redes MESH, cuya base es la conexión inalámbrica. Para el diseño de cualquier red, es necesario conocer su conceptualización teórica y su infraestructura. El presente capítulo esta enfocado en presentar la esquematización teórica de redes MESH, resaltando las ventajas que se visualizarían en áreas rurales, especialmente en la transmisión de datos. La primera, segunda y tercera generación demuestran el progreso de la red, que ya se encuentra en el nivel de emisión y recepción de datos. En cuanto a las topologías, se relacionan la de estrella, que utiliza un punto de conexión a Internet, la de punto a punto, en la que únicamente se comunican dos nodos, los repetidores o de retransmisión que pueden ser locales o remotos y las redes libres que tránsmiten la información por medio de una misma red.

### • 1.1. ¿Qué es una red en malla o MESH?

Una red en malla o MESH es un tipo de diseño de red más conocida como multipunto a multipunto, la cual está compuesta por nodos a través de los cuales se transporta el tráfico de los otros nodos, dado que estos se comunican directamente entre sí. Las llamadas *Wireless MESH Networks* son redes en las que la comunicación se puede hacer entre distintos puntos y no sólo entre punto y estación base. Por esta razón no son redes centralizadas, cada nodo es autodirigido y capaz de conectarse a otros nodos como sea necesario.

Una red de malla inalámbrica (WMN) se compone de nodos de la malla que forman la columna vertebral de la red. Los nodos son capaces de configurarse automáticamente y volver a configurarse de forma dinámica para mantener la conectividad de la malla. Esta relación de autosuficiencia entre los nodos de la malla elimina la necesidad de una gestión centralizada.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Formas inteligentes de enrutamiento permiten a los nodos de la malla, determinar la ruta necesaria para que los paquetes de datos que no pueden estar dentro del alcance inalámbrico directo (los unos del otro) logren llegar a sus destinos.

Así, la información se puede dirigir desde el origen al destino a través de múltiples saltos. Esto tiene una gran importancia y es una de las ventajas potenciales en términos de confiabilidad de la red con respecto a las redes tradicionales de salto único y especialmente para la comunicación de retorno (EcuRed, 2016).

Existen bastantes formas de lograr crear redes con topología en malla, las redes en general son una gran malla sobre la internet; aun así, no sólo la malla depende de la capa física sino también de la infraestructura que la acompaña, como lo son los protocolos de comunicación que permiten el flujo de datos entre los nodos de la red creada.

Entre los principales protocolos de redes con topología en malla se encuentran:

### ○ **Enrutamiento proactivo**

- HSLS – Visión Borrosa del Estado del Enlace.
- TBRPF – *Topology Broadcast base on Reverse*.
- OSLR – *Optimized Link State Routing*.
- Mobile MESH.

### ○ **Enrutamiento reactivo**

- AODV.
- Vector Distancia de Conexión de redes MESH Inalámbricas (WMNs), los enrutadores consisten en dos tipos de nodos.

Las redes solucionan los imprevistos y ayudan a incrementar el rendimiento de las redes *ad-hoc*. Debido a la posibilidad de generar conexiones a distintos *Access Point* se aumenta el ancho de banda que puede tener cada nodo y, siendo así, resulta mucho más estable, ya que puede funcionar aun cuando alguno de los nodos se vea interferido o con algún daño. Por el contrario, en las redes más comúnmente usadas, si cae



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

un Access Point los usuarios pertenecientes a este sector donde trabaja el punto de acceso se verán afectados por el fallo de la red.

## • 1.2 Ventajas de las redes MESH

El beneficio de este diseño de red es que, aun si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí.

### ○ Áreas municipales

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

- Seguridad ciudadana.
- Supervisión y control del tráfico.
- Servicios al ciudadano en materia de *Sociedad de la Información*: acceso a Internet en centros escolares y bibliotecas, así como información y orientación turística, entre otras, redes intranet.
- Uso corporativo, en las estaciones móviles (policía municipal, administración).

### ○ Áreas rurales

El diseño de red MESH permite introducir servicios de banda ancha en entornos rurales para implantar servicios sociales esenciales y promocionar la *Sociedad de la Información*. La instalación de las redes inalámbricas en estas zonas no requiere ninguna infraestructura previa de telecomunicaciones, con lo cual su implantación resulta rentable, ya que cada nodo presta:

- Cobertura a grandes extensiones.
- Enlaces directivos de *backhaul* entre nodos.

Entre otras ventajas se encuentran:

- **Autoformación:** la red inalámbrica se forma de manera automática, una vez que los nodos de la malla se han configurado y activado.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- **La tolerancia a fallos:** si existen rutas redundantes en la red, el flujo de información no se interrumpe en el resto de la red cuando un nodo falla. La red, de forma dinámica, redirige la información a través de la ruta disponible.
- **La autosanación:** una vez restaurado, un nodo vuelve a unirse a la red de malla sin problemas.
- **Propiedad de la comunidad:** la propiedad de la red se comparte, por lo tanto, la carga del soporte de la red no se apoya en una sola persona.
- **Bajo costo:** la infraestructura se puede construir a partir de nodos de bajo costo. Costo incremental de la red con la suma de un nodo adicional. El costo marginal de expansión es bajo para ese nodo, sin embargo, el alcance y el valor de la red es mayor.
- **Facilidad de implementación:** con la formación de miembros en la comunidad se pueden construir sus propios nodos, configurar e implementar la red en la comunidad.
- **Posibilidad de utilización de repetidores:** su empleo permite que resuelvan problemas de orografía e interconecten largas distancias (EcuRed, 2016).

### • 1.3 Desventajas de las redes MESH

- **Latencia:** retraso debido al número de saltos que puede llegar a dar un paquete hasta su destino. Problemas no permitidos en servicios de tiempo real, como la telefonía IP.
- **Compartiendo el medio:** puede haber interferencias entre usuarios debido al limitado número de frecuencias de las redes WLAN. Se podrían provocar problemas de direcciones duplicadas y conflictos de red (Solución IPv6).
- **Seguridad:** las redes *ad-hoc* necesitan hablar con sus clientes antes de autenticarlos, son vulnerables a ataques DoS y los datos pueden ser interceptados. Algunas empresas han desarrollado protocolos que utilizan técnicas de cifrado diferentes a las de Wifi y que no pueden ser interceptados con una tarjeta de red inalámbrica 802.11 común.
- **Rendimiento:** La disminución del rendimiento (*throughput*) se provoca por el número de saltos de acuerdo con XXXXX, donde (“n” es el número de saltos). MESH se ha implementado en equipos 802.11 con dos radios: uno en la banda 2,4 GHz y otro en la banda de 5 GHz. De esta manera, el



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

rendimiento no disminuye con el número de saltos (recibir y transmitir simultáneamente en bandas distintas) (Pérez & Granados, 2010).

#### • 1.4 Generaciones de las redes MESH

##### 1.4.1 Primera generación

En esta generación el sistema mallado tiene un sólo radio para hacer la interconexión entre nodos y dar servicio; los datos se retransmiten de un nodo a otro de una manera *store-and-forward*, es decir, un nodo primero recibe los datos y luego lo retransmite (Figura 1.1).

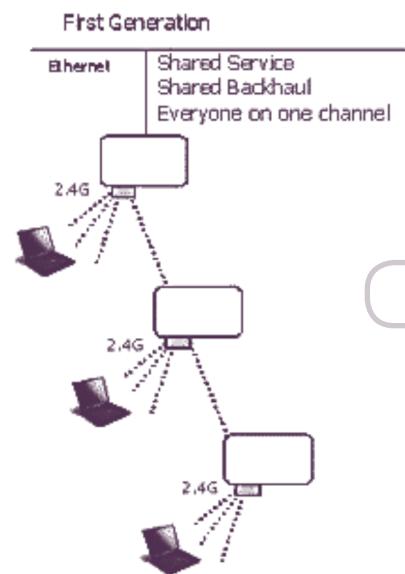


Figura 1.1. Red MESH de primera generación.

Fuente: Pérez y Granados (2010).

##### 1.4.2 Segunda generación

En esta generación se decidió combinar dos radios, uno para dar servicio con el estándar 802.11b/g y el otro para interconectar los nodos con el estándar 802.11a. Con este sistema se logró eliminar la interferencia en los nodos, ya que se trabaja con diversas bandas de frecuencia (entre 2.4GHz y 5.8GHz) para dar servicio a los usuarios e interconectar nodos. El problema surge cuando se aumenta la demanda de servicio por parte del usuario, ya que se presentan contenciones y congestiones significativas en la parte de la



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

radio que se usa para interconectar los nodos, lo cual hace que este sistema tenga una ligera desventaja (Figura 1.2).

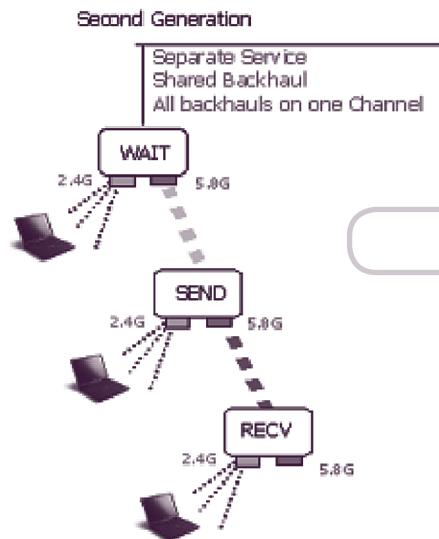


Figura 1.2. Red MESH segunda generación.

Fuente: Pérez y Granados (2010).

#### 1.4.3 Tercera generación

Los equipos de esta generación llevan una gran ventaja en comparación con las anteriores, ya que son considerados equipos inteligentes por utilizar una tecnología moderna. En esta generación cada nodo puede enviar y recibir datos de sus vecinos (Figura 1.3). Además, los canales disponibles se pueden reutilizar, haciendo que el espectro disponible sea más amplio y que el funcionamiento de la red aumente 50 o más veces.

Las empresas fabricantes de los equipos de esta generación se basan en productos multi-radios que soportan múltiples configuraciones de red. Un radio de los equipos de tercera generación se usa para crear un enlace hacia su nodo *upstream* (nodo más cerca al *gateway*) y otro radio se utiliza para un enlace *downstream* al nodo vecino siguiente. A diferencia de la generación anterior, estos radios pueden hacer uso de diversos canales (Pérez & Granados, 2010).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

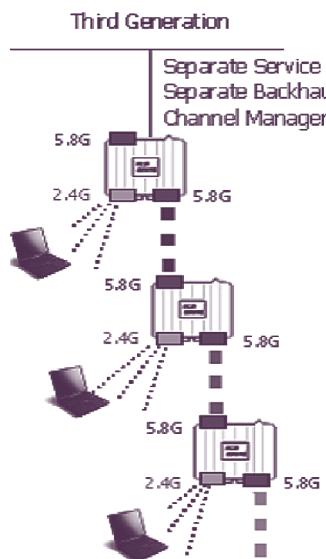


Figura 1.3. Red MESH de tercera generación.

Fuente: Pérez y Granados (2010).

## • 1.5 Topologías de las redes MESH

Las redes MESH se mezclan entre dos topologías de redes inalámbricas: la topología *ad-hoc* y la topología *infraestructura*, dada su necesidad de conexión y uso de la información que viaja a través de los nodos. Para conocer el escenario en el que trabaja una red MESH (Figura 1.4) (Bravo, 2008).

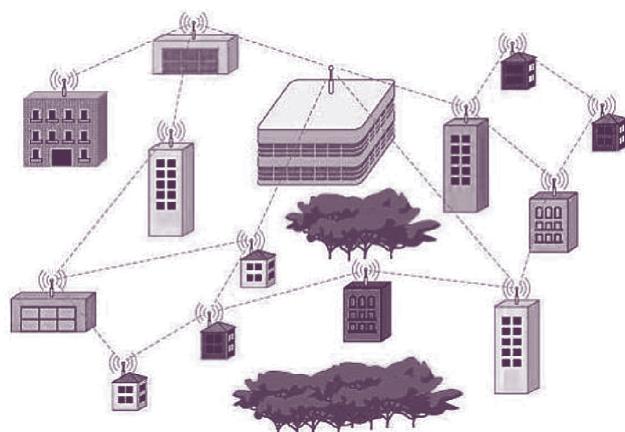


Figura 1.4. Escenario de red.

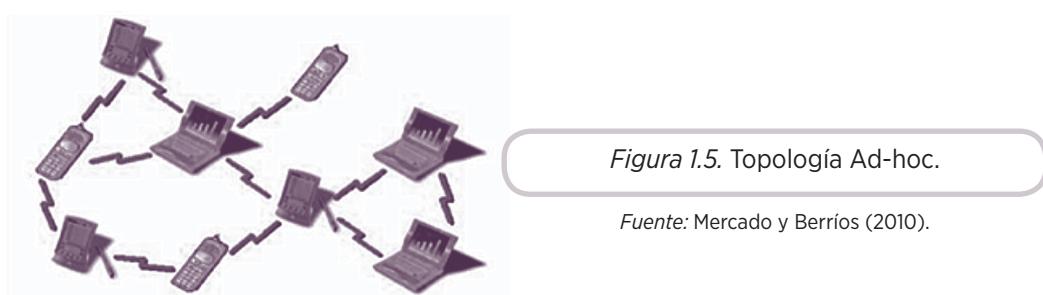
Fuente: Bravo (2008).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

### 1.5.1 Topología ad-hoc

*Ad-hoc* es una red formada sin ninguna administración central o sin existencia de un nodo central (Figura 1.5), sino que consta de nodos móviles que usan una interface inalámbrica para enviar paquetes de datos. Consiste en un grupo de ordenadores que se comunican, cada uno directamente con los otros, a través de las señales de radio sin usar un punto de acceso. Las configuraciones *ad hoc*, son comunicaciones de tipo punto a punto.



Solamente los ordenadores dentro de un rango de transmisión definido pueden comunicarse entre ellos. Esta tecnología es utilizada en varios campos como: ejército, celulares y juegos de video (Mercado & Berrios).

### 1.5.2 Topología infraestructura (BSS)

La topología de infraestructura es aquella en la que todos los ordenadores que tengan tarjetas de red inalámbrica trabajan en un orden jerárquico (Figura 1.6), dado que uno de los ordenadores es el punto de enlace para que los demás se conecten a la misma red.

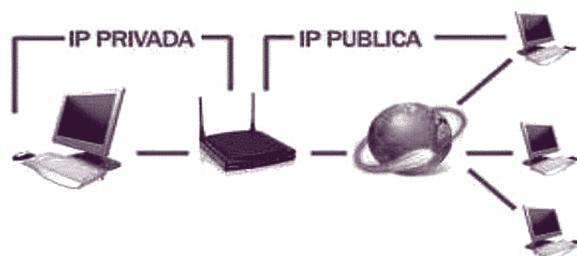


Figura 1.6. Topología de infraestructura.

Fuente: Tinajero (2011).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

En el modo infraestructura no hay un elemento central, sino que existe un elemento de coordinación, es decir, un punto de acceso o estación base; de esta manera si el punto de acceso se conecta a una red *Ethernet* cableada, los clientes inalámbricos pueden acceder a una red fija a través del punto de acceso.

Esta topología se encuentra compuesta por cuatro modos de conexión:

- Estrella
- Punto a Punto
- Repetidores
- Malla

Estos tipos de conexión son necesarios, dado que el sistema de distribución de la red se debe tener en cuenta para que la conexión entre los ordenadores sea óptima (Díaz & Castillo, 2013) (Tinajero, 2011).

### 1.5.3. Standard IEEE 802.X

**IEEE 802** es un estudio de estándares elaborado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que actúa sobre redes de ordenadores. Concretamente, y según su propia definición, sobre redes de área local (RAL, en inglés LAN) y redes de área metropolitana (en inglés, MAN). También se usa el nombre **IEEE 802** para referirse a los estándares que propone este instituto, algunos de los cuales son muy conocidos como: *Ethernet* (IEEE 802.3) o *Wi-Fi* (IEEE 802.11). Incluso, se encuentran intentando estandarizar *Bluetooth* en el 802.15 (IEEE 802.15).

- **IEEE 802.1 Protocolos superiores de redes de área local.** Esta parte del estándar de la IEEE apunta a la relación existente entre el contexto y el modelo de la interconexión de sistemas abiertos, así como toda la gestión para normas que se establece en el estándar para el funcionamiento de las redes.  
Define, además, cómo los formatos para la implementación de protocolos en fundamentos de la gestión de la red llegan a permitir un aumento normal en la seguridad y una agrupación por MAC que vendría unida a la gestión funcional de las redes LAN.
- **802.1D** Este apartado del estándar, se enfoca en ahondar en el tema de la interrelación funcional de la red con el mapeo fundamentado



de puente entre la red y la identificación del *host*. Para esto, en la red se implementó el trato de los puentes MAC, los cuales permiten la existencia de una sola ruta activa; gracias a un algoritmo que funciona como un *switch* disparado por el resultado de la existencia de un bucle en un algoritmo enfocado en la capa de datos, que audita la conexión entre dos dispositivos de la red. Ello beneficia el intercambio de mensajes sin problemas de redundancia e incoherencia.

Los bucles generalmente se presentan cuando la existencia de rutas activas en un mismo destino tiene propiedades alternativas, es decir, la muestra que se tiene para evidenciar el comportamiento de la interconexión a nivel de enlace entre los dispositivos y su red se ofrecerá con mayor fiabilidad y en caso de un fallo de enlace de la red, los dispositivos se activarán soportando así el tráfico de esta.

- **802.1Q.** El protocolo IEEE 802.1Q, nació como un proyecto desarrollado para impedir la interferencia como problema y al que le fue planteado, el desarrollo de una herramienta que logre la unificación de múltiples redes en un mismo medio físico, sin embargo todo esto llegaría a hacerlo de forma transparente y así se definiría un protocolo de encapsulamiento que se usaría en la implementación del mecanismo en redes Ethernet, aunque en principio hubiese sido creado para soportar, la interconexión de todos los dispositivos en el funcionamiento y la administración en una VLAN.
- **802.1aq.** Es el estándar en el protocolo de la IEEE que se enfoca en el comportamiento simulado de un algoritmo, que busca el camino más corto en una ruta. Es así como reemplaza protocolos ya existentes, beneficiando la mejora en la utilización de las redes malladas, ya que al tratarse de multi-nodos le es necesario hacer uso de un paradigma que le permita invertir en la optimización de la red a partir del ancho de banda y de la mejor ruta, para que la distribución del tráfico se dé en un tiempo de re-convergencia menor, logrando así, aumentar de las posibilidades de generar varios caminos a un mismo costo y con los mejores beneficios.
- **IEEE 802.2 Control de enlace lógico.** El estándar IEEE 802.2 se encuentra en la parte superior de la capa de enlace y aunque ésta se implementa, depende de la configuración de la red usada, ya que fundamentalmente se enfoca en la definición en el control del enlace lógico (Baide, 2012). Presenta así, el posible envío de paquetes que añade etiquetas estándar de 8-bit; permite el uso de valores *EtherType* usados para especificar el protocolo transportado encima de IEEE 802.2; y también permite a los fabricantes definir sus propios espacios de valores del protocolo.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- IEEE 802.3 *Ethernet*. Se instanció un equipo de formación para la estandarización de la aplicación de *Ethernet*, presentándose grandes avances que cubrieron las necesidades de la implementación del estándar en un protocolo de la IEEE. Sin embargo, puntualidades como el formato de la trama, ampliaciones de red y algunos índices más, hicieron necesario todo un estudio de los medios requeridos y las especificaciones de la red que tendrían que enfocarse demasiado en la personalización, para que la implementación pudiese darse.  
Al final entonces se crearon una serie de subestándares desprendidos de este estándar, los cuales intentan dar un mapeo del campo de acción en la implementación de este.
- IEEE 802.11 Red local inalámbrica (*Wi-Fi*). El estándar original fue definido como el Protocolo de múltiple acceso por detección de portadora; evitando colisiones fue instanciado como método de acceso. El enfoque que se le dio fue parte fundamental que se le dio fue importante respecto a un ámbito de velocidad de transmisión teórica que se utiliza en los requerimientos de esta codificación para lograr una mejora progresiva de la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.
  - **802.11a.** Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2,4 GHz (hornos microondas, teléfonos digitales DECT, *BlueTooth*). Es aplicada a una LAN inalámbrica. La especificación está aplicada a los sistemas de ATM inalámbricos.
  - **802.11b.** Conocida como 802.11 *High Rate* o *Wi-Fi*. Es una extensión del 802.11 que se aplica a redes LAN y provee una transmisión de 11Mbps (con posibilidad de 5.5, 2 y 1Mbps) en la banda de 2.4GHz. 802.11b utiliza sólo DSSS. Fue una ratificación en 1999 al estándar 802.11 original, permitiendo funcionalidad comparable al *Ethernet*.
  - **802.11e.** Estándar encargado de diferenciar entre video-voz-datos. Su único inconveniente es el encarecimiento de los equipos. Los proveedores de servicio de banda ancha a la vista QoS y la casa multimedia son capaces de conectar una red de computadoras como un ingrediente esencial a ofrecer. Su acceso de Internet es de gran velocidad (*From NetworkWorldFusion*).



- ◎ **802.11g.** El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps, pero de 30 Mbps en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
- ◎ **802.11h.** Este estándar tiene como objetivo ser una modificación sobre el estándar 802.11 para WLAN, el cual pretende ser un precursor de la integración entre sistemas e intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de radar o satélite. Estándar que sobrepasa al 802.11a, al admitir la asignación dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además, define el TPC (*Transmit Power Control*) según el cual la potencia de transmisión se adecúa a la distancia a la que se encuentra el destinatario de la comunicación.
- ◎ **802.11n** (CISCO , 2016). Con la tecnología 802.11n, se puede obtener una fiabilidad sin precedentes y un aumento en el rendimiento que con las actuales redes 802.11a/b/g. La tecnología 802.11n puede proporcionar a los usuarios móviles con una red inalámbrica fiable y soportar una amplia gama de aplicaciones de movilidad sin comprometer el rendimiento total de la red. Se ofrece:
  - Acceso en cualquier momento a los recursos de red y aplicaciones.
  - El rendimiento óptimo para apoyar el creciente número de usuarios móviles BYOD.
  - La calidad del servicio, para voz consistente y video a través de la LAN inalámbrica.
  - Conexiones fiables para aplicaciones de misión crítica.
  - Cobertura predecible para entornos de RF difíciles.
- La adopción de la tecnología inalámbrica 802.11n hoy protege las inversiones a largo plazo y permite a las organizaciones a reducir su costo total de propiedad al ofrecer el rendimiento necesario para soportar nuevas aplicaciones y satisfacer las expectativas de los usuarios para la movilidad.
- **IEEE 802.15 Red de área personal inalámbrica (*Bluetooth*).** Según el estándar de la implementación del IEEE 802.15 se proponen dos categorías generales de 802.15, llamado TG4 (la proporción baja) y TG3 (la proporción alta). La versión de TG4 proporciona velocidades de los datos de 20 Kbps o 250 Kbps. La versión de TG3 apoya que los datos se aceleran yendo de 11 Mbps a 55 Mbps. Los rasgos adicionales incluyen el



uso de 254 dispositivos de la red, dirigiéndose al dispositivo dinámico, apoyado para aquéllos donde la latencia es el apretón de manos crítico, de forma que la seguridad aprovisiona y direcciona el poder. Habrá 16 cauces en la banda de 2.4-GHz, 10 cauces en la banda de 915-MHz, y un cauce en la banda de 868-MHz (Ramírez, 2014).

- **IEEE 802.16 Acceso inalámbrico de Banda Ancha (*WiMax*)**. Este estándar tiene un enfoque orientado al rendimiento y aprovechamiento de banda ancha, como norma de comunicaciones inalámbricas para las redes del área metropolitana desarrolladas en el estándar original del 802.16 específica por punto la banda ancha de sistemas inalámbricos que operan en los 10-66 GHz autorizaron el espectro. Una enmendadura, 802.16a, fue aceptada en enero del 2003, con las extensiones especificadas 2-11 GHz del espectro, entregando 70 Mbps distancias a 31 millas. Un grupo más temprano de normas de IEEE, las especificaciones 802.11, proporcionan una alternativa inalámbrica a *Ethernet LAN* (el área local conecta una red de computadoras); se espera que la norma 802.16 las complemente permitiendo una alternativa inalámbrica a T1, conectando las oficinas que nos unen a nosotros y a Internet. Aunque las primeras enmendaduras a la norma sólo son para las conexiones inalámbricas fijas, se espera que una enmendadura extensa, 802.16e, habilite las conexiones para los dispositivos móviles.
- **IEEE 802.17 Anillos de paquetes con recuperación**. El estándar IEEE 802.17 (RPR) es una solución competitiva para la gestión del tráfico en el núcleo de la red MAN-RPR, puesto que soporta el tráfico de tramas MAC *Ethernet*. A pesar de esto, RPR sufre de una pérdida de rendimiento a causa de problemas de congestión, pero se comprobó que es posible mejorar el desempeño del control de la congestión perfeccionando el algoritmo de equidad en modo *Agresivo* de este estándar (Gamez & Álvarez, 2010).
- **IEEE 802.20 Acceso inalámbrico de banda ancha móvil**. IEEE 802.20 o banda ancha móvil de acceso inalámbrico (MBWA) era una especificación estándar de la asociación del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para redes inalámbricas móviles de acceso a Internet. La principal norma fue publicada en 2008. El estándar IEEE 802.20, “también denominado Acceso Inalámbrico a Redes Móviles de Banda Ancha (*Mobile Broadband Wireless Access - MBWA*) fue iniciado en diciembre de 2002, con el propósito de estandarizar la creación de redes móviles de banda ancha, de bajo costo. Es considerada como la competencia de WIMAX Móvil.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Esta tecnología está soportada en las capas físicas y de enlace de datos; de esta última emplea la subcapa de control de acceso al medio (MAC) y la subcapa de control de enlace lógico (LLC). MBWA opera en bandas con licencia por debajo de 3.5 GHz y con velocidades máximas de un (1) Mbps por usuario; está enfocada a la transmisión hasta de datos, permitiendo el uso de antenas adaptativas, *roaming IP*, traspaso, movilidad hasta de 250 Km/h y bajos niveles de latencia (De la Hoz & De la Hoz, 2009).

- **IEEE 802.21 Interoperabilidad independiente del medio.** El estándar IEEE 802.21 *Media Independent Handoff* es un estándar que permite la entrega MIH independiente de los medios, la cual admite la entrega de paquetes entre redes del mismo tipo y de otros tipos. Se utiliza para las entregas a y desde el sistema celular GSM, GPRS, WiFi, Bluetooth, entre otros.
- **IEEE 802.22 Red inalámbrica de área regional.** El estándar IEEE 802.22 *Wireless Regional Área Network*, es un estándar inalámbrico que utiliza el espectro de las frecuencias de televisión análoga y digital, sin generar interferencia en estas señales, es decir que, utiliza técnicas de uso de radio que conoce cuáles son los límites de uso correcto del espectro electromagnético, lo que le permite llegar a lugares lejanos de las ciudades (IEEE 802 LAN/MAN, 2016) (Association, 2016).

### • 1.7 Redes de infraestructura

Las redes inalámbricas en modo infraestructura extienden una LAN de cable ya existente, normalmente *Ethernet*, de modo que sea accesible por otros dispositivos sin hilos a través de una estación base denominada punto de acceso inalámbrico (WAP). Este punto de acceso actúa como puente entre ambas redes (*Ethernet* y la inalámbrica), coordinando la transmisión y recepción de los diferentes dispositivos inalámbricos.

En el modo de infraestructura hay un elemento de “coordinación”: un punto de acceso o estación base. Si el punto de acceso se conecta a una red *Ethernet* cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID; y para asegurar que se maximice la capacidad total de la red, no se debe configurar el mismo canal en todos los puntos de acceso que se encuentran en la misma área física.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Los clientes descubrirán (a través del escaneo de la red) cuál canal está usando el punto de acceso, de manera que no se requiere que ellos conozcan de antemano el número de canal.

### 1.7.1 Caso 1. Topología de estrella

La topología de estrella es una de las más comunes en redes inalámbricas. Es aquella tecnología que usada para un *hostpot* (punto de conexión a Internet). Es una red en donde las estaciones se encuentran conectadas directamente a un punto central (Figura 1.7), en el cual todas las comunicaciones se realizan por medio de éste. Los diferentes dispositivos que se encuentren en la red no están directamente conectados entre sí, por lo que hay que tener en cuenta que posee una limitación de tráfico de información.

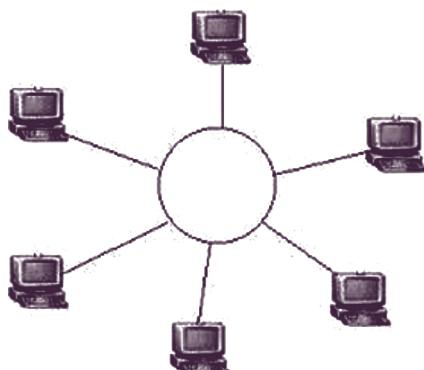


Figura 1.7. Red en topología estrella.

Fuente: Universidad Tecnológica Nacional (2016).

### 1.7.2 Caso 2. Punto a punto

Las redes punto a punto son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos (Figura 1.8), en clara oposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos. En una red punto a punto, los dispositivos actúan como socios iguales, o pares entre sí. Como pares, cada dispositivo puede tomar el rol de esclavo o la función de maestro. En un momento, el dispositivo A, por ejemplo, puede hacer una petición de un mensaje / dato del dispositivo B, y este es el que le responde enviando el mensaje / dato al dispositivo A. El dispositivo A funciona como esclavo, mientras que B funciona como maestro. Un momento después los dispositivos A y B pueden revertir los roles: B, como esclavo, hace una solicitud a A, y A, como maestro, responde



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

a la solicitud de B. Por tanto, A y B permanecen en una relación recíproca o par entre ellos.

Las redes punto a punto son relativamente fáciles de instalar y operar. A medida que las redes crecen, las relaciones punto a punto se vuelven más difíciles de coordinar y operar. Su eficiencia decrece rápidamente a medida que la cantidad de dispositivos en la red aumenta.

Los enlaces que interconectan los nodos de una red punto a punto se pueden clasificar en tres tipos según el sentido de las comunicaciones que transporta:

- **Simplex:** la transacción sólo se efectúa en un solo sentido.
- **Half-dúplex:** la transacción se realiza en ambos sentidos, pero de forma alternativa, es decir sólo uno puede transmitir en un momento dado, no pudiendo transmitir los dos al mismo tiempo.
- **Full-dúplex:** la transacción se puede llevar a cabo en ambos sentidos simultáneamente. Cuando la velocidad de los enlaces Semi-dúplex y dúplex es la misma en ambos sentidos se trata de un enlace simétrico, en caso contrario, se dice que es un enlace asimétrico.



Figura 1.8. Red punto a punto.

Fuente: Cika Electrónica (2016).

### 1.7.3 Caso 3. Repetidores

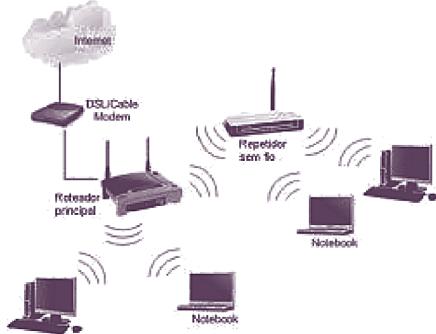
Es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alta, de tal modo que se pueda transmitir a distancias más largas sin distorsión o con una degradación tolerable. Cuando se habla de repetidores se sabe que se vuelve necesario su uso cuando existe obstrucción en la línea de vista directa o existe una distancia muy larga para un sólo enlace. Además, si las distancias entre los nodos de una red son muy elevadas los efectos de la atenuación resultan siendo intolerables, es necesario entonces utilizar dispositivos que restauren la señal a su estado original (Figura 1.9).

Existen dos tipos de repetidores:



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- **Locales:** son los que enlazan redes que se encuentran próximas o cercanas.
- **Remotos:** son los que se utilizan cuando las redes están alejadas y se necesita un puente intermedio de comunicación.



*Figura 1.9. Red con conexión por medio de repetidor.*

*Fuente: WIFIDEL (2016).*

#### 1.7.4 Caso 4. Topología en malla

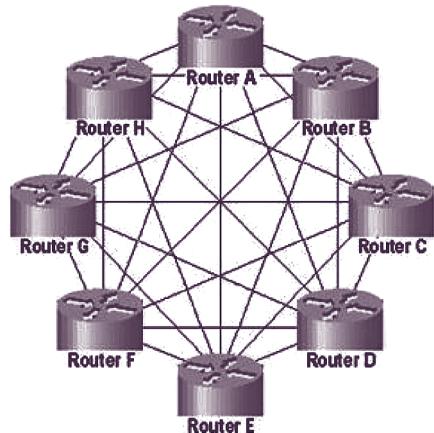
Esta tipología consiste en que cada nodo se encuentra conectado a uno o más nodos, de tal manera que se transmite la información por cualquier camino entre ellos. Cabe aclarar que, si la red en malla está completamente conectada, no puede existir ninguna interrupción en la comunicación entre nodos, dado que todos se encuentran conectados. Esta topología es la opción principal en los ambientes urbanos ya sean redes municipales, campus universitarios y vecindarios, empleando una de las dos distribuciones de conexión que se presentan a continuación.

#### 1.7.5 Caso 5. Topología de malla completa

Como se puede observar en la Figura 1.10, es en la que cada uno de los nodos se conecta directamente con todos los demás.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

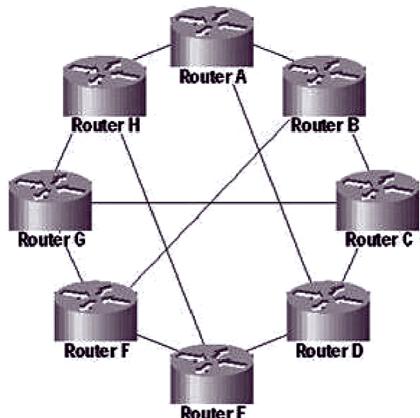


*Figura 1.10. Topología malla completa.*

*Fuente: Maya y Molina (2006).*

### 1.7.6 Caso 6. Topología de malla parcial

Como se puede observar en la Figura 1.11, es en la que los nodos se conectan únicamente a algunos de los otros nodos, no a todos (Gómez, 2016).



*Figura 1.11. Topología de malla parcial.*

*Fuente: Maya y Molina (2006).*

## • 1.8 Redes libres

Las redes libres son llamadas así porque permiten el libre tránsito de la información que fluye a través de la misma red. Es una red creada, administrada y gestionada por los propios usuarios al igual que su distribución, por lo que no pertenece a nadie en particular, pero les pertenece a todos. Una red libre ofrece acceso libre y gratuito a la propia red; por acceso libre se entiende que



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

cualquier persona puede acceder a la red en cualquier momento y puede llegar hasta cualquier parte de ella.

En esta red, todos están llamados a participar e interconectarse, defendiendo valores fundamentales como: el acceso universal a las tecnologías de la información, la libertad, igualdad de oportunidades, solidaridad o fraternidad. Una red que es:

- **Abierta:** porque se ofrece de forma universal a la participación de todos, sin ningún tipo de exclusión o discriminación, y porque se informa en todo momento acerca de cómo funciona la red y sus componentes, lo que permite que cualquiera pueda mejorarlala.
- **Libre:** porque todos pueden hacer lo que quieran y disfrutar de las libertades, tal y como se prevén en la referencia de los principios generales, todo esto independientemente de su nivel de participación en la red y sin imponer términos y condiciones que contradigan este acuerdo de forma unilateral.
- **Neutral:** porque la red es independiente de los contenidos, no los condiciona y, así, pueden circular libremente; los usuarios pueden acceder y producir contenidos independientemente de sus posibilidades financieras o condiciones sociales. Cuando se incorporan contenidos a la red abierta se hace con el fin de gestionar mejor la red o simplemente como ejercicio, pero en ningún caso con el objetivo de sustituir o bloquear otros contenidos (EcuRed, 2016), (Camino, García, & Criado, 2016).

### • 1.9 Redes inalámbricas tipo malla

Las redes tipo malla inalámbrica de infraestructura, unen las dos topologías de las redes inalámbricas: la topología *ad-hoc* y la topología infraestructura. Estas redes se autoorganizan y autoconfiguran dinámicamente con los nodos de la red, estableciendo automáticamente una red *ad-hoc* y manteniendo la conexión. Además, están formadas por dos tipos de nodos: los *routers* MESH y los clientes MESH.

Además de las funciones propias de un *router wireless* convencional, el *router* MESH contiene funciones adicionales para soportar la infraestructura MESH. Gracias al sistema de comunicaciones *multihop*, se puede conseguir la misma cobertura con menos energía de transmisión. Los *routers* MESH permiten



unir a la red dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso (PA), están dentro del rango de cobertura de alguna tarjeta de red que, directa o indirectamente, está dentro del rango de cobertura de un punto de acceso de la red. Para mejorar la flexibilidad de la red MESH, un *router* MESH contiene múltiples interfaces *Wireless*, basados en la propia tecnología inalámbrica. A pesar de estas pequeñas diferencias, los *routers* MESH están construidos sobre un *hardware* similar al de cualquier *router*.

Los *routers* MESH tienen una movilidad limitada y forman el esqueleto de la red. Los clientes MESH también pueden trabajar como un *router* para las redes malladas, sin embargo, su *hardware* y *software* son mucho más sencillos que los del *router*. Las tarjetas de red pueden comunicarse entre sí independientemente del punto de acceso; así pues, los dispositivos pueden no mandar directamente sus paquetes al punto de acceso, o *router* MESH, sino que pueden pasárselos a otras tarjetas de red para que lleguen a su destino. Para que esto sea posible, es necesario contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos o con un número que, aun no siendo el mínimo, sea suficientemente bueno. El IEEE está desarrollando un conjunto de estándares bajo el título 802.lls (*Wireless*), 802.16 (*WiMax*) y 802.155 (*Bluetooth*), para definir una arquitectura, y un protocolo de la red MESH ESS (*Extended Service Set*) necesario para reunir la interoperabilidad de fabricantes, ya que al no existir un estándar, cada uno de ellos ha realizado sus propias investigaciones aplicadas a sus productos (Gómez, Maimó, & Merideño, 2009-2010).

## • 1.10 Arquitectura de las redes MESH

La arquitectura de las redes MESH se clasifica en tres tipos:

### 1.10.1 Infraestructura

La infraestructura está formada por los *routers* MESH y es el esqueleto de la red. Dichos *routers* realizarán las funciones de *gateway*, *routing*, etc., y permitirán la conexión a Internet. Del mismo modo interconectan todo tipo de redes inalámbricas existentes, como puede ser *Wifi*, *WiMax* o telefonía móvil, tal como muestra la Figura 1.12. Aquellos dispositivos que tengan tecnología *Ethernet* se conectarán a los *routers* mediante la misma. Para aquellos dispositivos que utilicen la misma tecnología radio que dispongan



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

los *routers*, se conectarán directamente a ellos, y si es distinta podrán hacerlo mediante sus estaciones base, que a su vez utilizarán *Ethernet*.

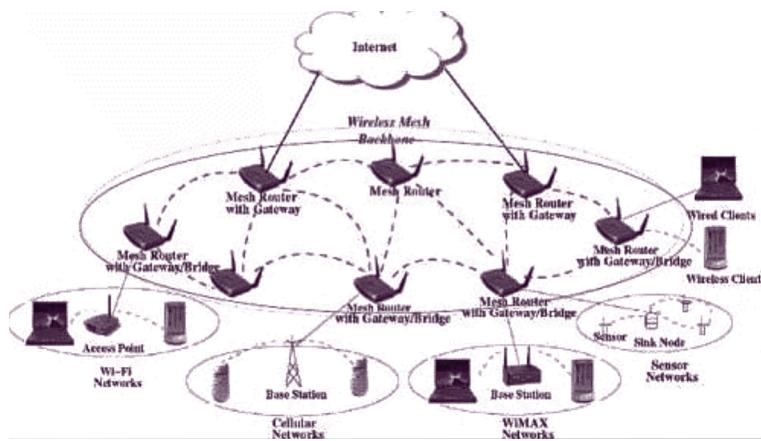


Figura 1.12. Infraestructura MESH.

Fuente: Gómez, Maimó y Merideño (2009-2010).

### 1.10.2 Clientes MESH

Los clientes MESH proporcionan una conexión punto a punto entre los dispositivos, además de realizar funciones básicas de red, como encaminamiento o configuración.

De este modo, no es necesario un *router* MESH. Estos clientes forman una red y sería similar a la conocida *ad-hoc*. Sin embargo, los clientes MESH disponen de una tecnología superior a los clientes habituales, puesto que su *software* y *hardware* han de ser capaces de soportar las funciones necesarias para la conexión.

### 1.10.3 MESH híbrido

Esta arquitectura combina la infraestructura con los clientes MESH. Éstos podrían acceder a la red a través de la red de *routers* o a través de otros clientes MESH, aumentando así la cobertura. Además de ello, se interconectan los otros tipos de redes ya existentes como pueden ser: *Wifi*, *WiMax*, redes móviles o radio. Los *routers* MESH tienen una movilidad reducida y están concentrados en realizar todas las tareas de encaminamiento y configuración, facilitando



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

la tarea de los clientes y otros nodos, reduciendo su trabajo. Se mantiene la tecnología *multihop*, gracias a la red de *routers* desde la que no es necesario que todos los nodos tengan completa visión de todos los nodos existentes, sino que tan sólo es necesario visualizar los nodos cercanos (Gómez, Maimó, & Merideño, 2009-2010).

### • 1.11 Protocolos de enrutamiento

Un protocolo de enrutamiento es un *software* complejo que se ejecuta de manera simultánea en un conjunto de *routers*, con el objetivo de completar y actualizar su tabla de enrutamiento con los mejores caminos para intercambiar información con otras redes. Así, se puede resumir que un protocolo de enrutamiento tiene como objetivos:

- Descubrir redes lejanas con las cuales intercambiar información.
- Mantener la información de enrutamiento actualizada de manera fiable.
- Elegir el mejor camino posible en cada momento hacia las redes de destino.
- Encontrar unas nuevas rutas para sustituir a aquellas que dejen de estar disponibles en los términos necesarios.

Frente al enrutamiento estático, el enrutamiento dinámico ofrece nuevas posibilidades (Tabla 1.1), ya que se adapta mejor a nuevas circunstancias, pero requiere una mayor complejidad en los sistemas y la gestión de éstos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 1.1. Enrutamiento dinámico vs. enrutamiento estático.

Característica	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Por lo general es independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Se requiere de un conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere la intervención del administrador
Escalamiento	Adecuado para las topologías simples y complejas	Adecuada para topologías simples
Seguridad	Es menos seguro	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

Fuente: Cisco System, inc (2016).

Los protocolos de enrutamiento dinámico se clasifican (en una primera instancia) según sean de aplicación a sistemas de *gateway* interior o exterior. Los primeros se agrupan según consideren como variable el vector distancia o el estado del enlace.

- **Babel:** Babel es un protocolo que se encuentra basado en el algoritmo vector de distancias, y diseñado para ser robusto y eficiente tanto en redes cableadas como en redes inalámbricas malladas. Emplea varias técnicas para asegurar ausencia de patologías de ruteo, tal como hacer bucles. Es proactivo, pero con características adaptativas. En su funcionamiento por defecto, Babel utiliza una medición de la calidad del enlace que está diseñado para redes que utilizan el estándar IEEE 802.11 MAC. En otras palabras, los caminos elegidos deben ser razonables en cualquier tipo de red, pero son particularmente adecuadas para las redes 802.11.
- **HSLS (Hazy Sighted Link Statin):** es un protocolo de enrutamiento, el cual elimina enlaces de baja calidad basado en el estado del enlace.



Éste protocolo es proactivo y reactivo dado que envía mensajes de actualización en un tiempo y espacio determinado.

- **PWRP (Predictive Wireless Routing Protocol):** es un protocolo que fue desarrollado específicamente para redes inalámbricas. Valida el estado del enlace además de la calidad de este. Este protocolo recalcula cuatro veces por segundo el estado de los enlaces de toda la red MESH y selecciona la ruta en función del estado de la red en cada momento. Este funcionamiento soporta redes dinámicas y proporciona la ruta óptima en cada momento (Universidad de Alcalá, 2011-2012) (Arias, Peña, & Chávez, 2015).
- **BATMAN (Better Approach to Mobile Ad-hoc Networks):** BATMAN es un protocolo de encaminamiento dinámico y proactivo para redes malladas *ad-hoc* que utiliza tablas de encaminamiento para las decisiones de éste mismo tipo. El protocolo no calcula rutas completas entre un nodo origen y destino, sino que selecciona un nodo de salto para utilizarlo como *gateway* hacia el destino. Su función es encontrar otros nodos BATMAN y definir el mejor vecino para llegar a ellos. Además, hace seguimiento de los nuevos nodos e informa a sus vecinos de su existencia (Benito, 2010).
- **BATMAN ADV (BATMAN advanced):** es un protocolo de enrutamiento *multi-hop ad-hoc* de redes en malla. Es una aplicación de este protocolo en la norma ISO/OSI Capa 2, permitiendo que las redes en malla sean usadas como conmutador virtual. Con este enfoque, las redes LAN y WAN se pueden integrar fácilmente.
- **AODV (Ad-hoc On-demand Distance Vector Routing):** es un protocolo que realiza un enrutamiento por demanda, eso quiere decir que establece una ruta y cuando un dispositivo de la red envíe un mensaje solicitando información, los dispositivos que conocen cómo llegar al destino enviarán el mensaje de respuesta al origen, con la finalidad de establecer la ruta que permanecerá activa mientras dure la comunicación origen-destino.
- **OLRS (Optimized Link State Routing Protocol):** es un protocolo de enrutamiento por optimización del estado de enlace en el que los dispositivos envían constantemente mensajes a los dispositivos vecinos con un intervalo determinado, con el fin de que los vecinos conozcan que aún se encuentra activo el dispositivo; éstos a su vez envían un mensaje de control para que toda la red conozca cuáles son los dispositivos que todavía siguen activos en la red y sean eliminados de las tablas de enrutamiento (gnuLinux, 2016).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## • 1.12 Infraestructura para redes MESH

Existen tres tipos de redes malladas inalámbricas, basadas en el funcionamiento de los nodos. Las redes malladas tienen dos tipos de nodos, los *routers* y los clientes mallados. Gracias a esto se debe encontrar una red en donde su funcionalidad resida en los *routers*, los clientes o una combinación de ambos nodos. El funcionamiento genérico de las redes MESH se pueden observar en la Figura 1.13.

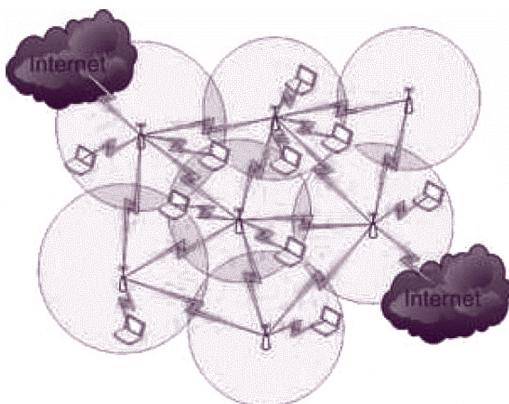


Figura 1.13. Esquema de funcionamiento de una red MESH.

Fuente: Benito (2010).

### 1.12.1 Red de infraestructura

En este tipo de red los *routers* mallados forman la infraestructura principal de la red y se conectan entre ellos de manera inalámbrica (Figura 1.14). Asimismo, permiten el acceso a clientes mallados y a clientes convencionales de otras redes; éstos últimos se pueden conectar a los *routers* mallados a través de cable Ethernet o de manera inalámbrica.

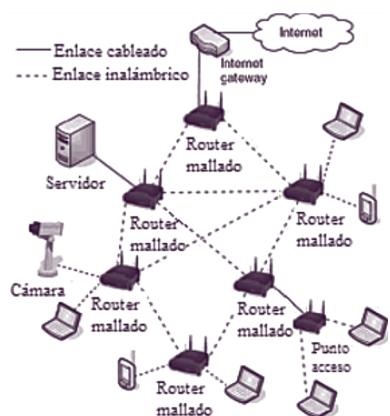


Figura 1.14. Red de infraestructura.

Fuente: Benito (2010).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

### 1.12.2 Red de clientes mallados

En las redes de clientes mallados no se utilizan los *routers* mallados. Los clientes mallados forman la infraestructura de la red y se conectan de manera inalámbrica (Figura 1.15). En este caso los clientes mallados actúan como cliente y *router* para el resto de los nodos.

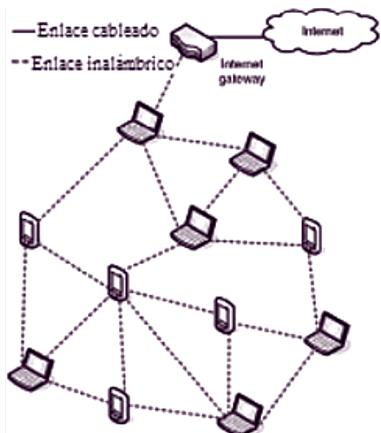


Figura 1.15. Red de clientes mallados.

Fuente: Benito (2010).

### 1.12.3 Red híbrida

Como su propio nombre indica, es una red que combina los dos conceptos anteriores. En las redes híbridas los *routers* y los clientes realizan las funciones de encaminamiento (Figura 1.16) (Benito, 2010).

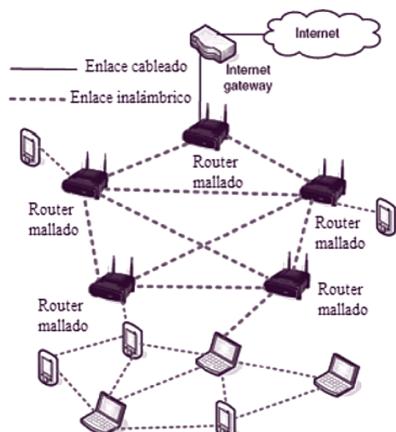


Figura 1.16. Red híbrida.

Fuente: Benito (2010).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Siguiendo las disposiciones del Reglamento de Radiocomunicaciones del Convenio de la Unión Internacional de Telecomunicaciones (UIT), las redes libres MESH siguen un protocolo de leyes, las cuales rigen los procedimientos científicos, administrativos, técnicos, jurídicos, económicos necesarios para garantizar el funcionamiento de este tipo de iniciativas; por ello es importante entender rápidamente las más importantes directivas que el Estado de la República de Colombia ha establecido a nivel nacional en el ámbito de las telecomunicaciones inalámbricas.

El espectro electromagnético es de propiedad exclusiva del Estado y como tal, constituye un bien de dominio público, inajenable e imprescriptible, cuya gestión, administración y control corresponde al Ministerio de Tecnologías de Información y Comunicaciones (Ministerio de las TIC) de conformidad con las leyes vigentes; con excepción del Espectro Electromagnético atribuido al servicio de TV, cuya administración corresponde a la Comisión Nacional de Televisión (CNTV)<sup>1</sup>, en coordinación con el Ministerio de Tecnologías de Información y Comunicaciones. Para ello, el Ministerio de las TIC concretamente ha declarado la gestión y control del espectro electromagnético a la Agencia Nacional del Espectro.

#### 1.12.4 La Agencia Nacional del Espectro y el Ministerio TIC

El objeto de la Agencia Nacional del Espectro es brindar el soporte técnico para la gestión y la planeación, la vigilancia y control del espectro radioeléctrico, en coordinación con las diferentes autoridades que tengan funciones o actividades relacionadas con el mismo.

La Agencia Nacional del Espectro tendrá, entre otras, las siguientes funciones:

- Asesorar al Ministerio de Tecnologías de la Información y Comunicaciones (TIC) en el diseño y formulación de políticas, planes y programas relacionados con el espectro radioeléctrico.

<sup>1</sup> Artículo 77 de La Carta Magna, la Constitución Política de Colombia estipula lo anterior en el mencionado artículo inicialmente, la televisión será regulada por una entidad autónoma del orden nacional, sujeta a un régimen propio.

Artículo 76: “La intervención estatal en el espectro electromagnético utilizado para los servicios de televisión, estará a cargo de un organismo de derecho público con personería jurídica, autonomía administrativa, patrimonial y técnica, sujeto a un régimen legal propio” (consultar la Constitución Política de Colombia para extender la visión de la normativa vigente).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Diseñar y formular políticas, planes y programas relacionados con la vigilancia y control del Espectro, en concordancia con las políticas nacionales y sectoriales y las propuestas por los organismos internacionales competentes (en este caso la UIT).
- Estudiar y proponer, acorde con las tendencias del sector y las evoluciones tecnológicas, esquemas óptimos de vigilancia y control del espectro electromagnético, incluyendo los satelitales, con excepción a lo dispuesto en el artículo de la Constitución Política para tales casos de uso.
- Ejercer la vigilancia y control del espectro electromagnético, con excepción de lo dispuesto en el artículo 76 de la Constitución Política de Colombia.
- Realizar la gestión técnica del espectro electromagnético.
- Investigar e identificar las nuevas tendencias nacionales e internacionales en cuanto a la administración, vigilancia y control del espectro.
- Estudiar y proponer los parámetros de valoración por el derecho al uso del espectro electromagnético y la estructura de contraprestaciones.
- Notificar ante los organismos internacionales las interferencias detectadas por señales originadas en otros países, previa coordinación con el Ministerio de Tecnologías de la Información y Comunicaciones (TIC).
- Apoyar al TIC en el establecimiento de estrategias para la participación en las diversas conferencias y grupos de estudio especializados en la Unión Internacional de Telecomunicaciones (UIT) y otros organismos internacionales.
- Adelantar las investigaciones a que haya lugar, por posibles infracciones al régimen del espectro definido por el TIC e las sanciones, con excepción de lo dispuesto en el artículo 76 de la Constitución Política de Colombia.
- Ordenar el cese de operaciones no autorizadas de redes, el decomiso provisional y definitivo de equipos y demás bienes utilizados para el efecto, y disponer su destino con arreglo a lo dispuesto en la ley, sin perjuicio de las competencias que tienen las autoridades militares y de policía para el decomiso de equipos<sup>2</sup>.
- Actualizar, mantener y garantizar la seguridad y confiabilidad de la información que se genere de los actos administrativos de su competencia.
- Las demás que por su naturaleza le sean asignadas o le correspondan por ley.

<sup>2</sup> Es muy importante por ello mismo tener en cuenta el marco legal del uso de una red libre, establecer una política de administración de recursos que no genere conflictos con la ley para evitar graves sanciones; como, por ejemplo, no establecer lucro para este tipo de redes, no utilizar material que afecte de forma grave los derechos de autor bajo ningún motivo, utilizar las bandas ISM (Industrial, Scientific and Medical Applications – ICM o aplicaciones industriales, científicas y mecánicas.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

### 1.12.5 ¿El uso de las frecuencias electromagnéticas requiere de licencia?

El uso de frecuencias radioeléctricas requiere de permiso previo otorgado por el Ministerio de Tecnologías de Información y Comunicaciones (TIC) y dará lugar al pago de los derechos que correspondan<sup>3</sup>. Cualquier ampliación, extensión, renovación o modificación de las condiciones, requiere de un nuevo permiso, previo y expreso<sup>4</sup>. El TIC ejerce las funciones de inspección y vigilancia sobre las redes y servicios de telecomunicaciones.

Acorde con el Decreto Ley 1900 de 1990 o “Estatuto de las Telecomunicaciones”, cualquier red o servicio de telecomunicaciones sin autorización previa será considerado como clandestino y el Ministerio de TIC y las autoridades militares y de policía procederán a suspenderlo y a decomisar los equipos, sin perjuicio de las sanciones de orden administrativo o penal a que hubiese lugar, conforme a las normas legales y reglamentarias vigentes. Los equipos decomisados serán depositados a órdenes del Ministerio de TIC, el cual les dará la destinación y el uso que fijen las normas pertinentes.

### 1.12.6 Infracciones al ordenamiento de las telecomunicaciones

Constituyen infracciones específicas al ordenamiento de las telecomunicaciones, entre otras:

- El ejercicio de actividades o la prestación de servicios, sin la correspondiente concesión o autorización; así como la utilización de frecuencias radioeléctricas sin permiso o en forma distinta de la permitida.
- La instalación, utilización o conexión a la red de telecomunicaciones del Estado de equipos que no se ajusten las normas fijadas por el ministerio de Tecnologías de Información y Comunicaciones (TIC).
- La producción de daños a la red de telecomunicaciones del Estado, como consecuencia de conexiones o instalaciones no autorizadas.

<sup>3</sup> Siempre y cuando requieran de un lucro para fines privados, el permiso de uso de licencias viene estipulado en el manifiesto de uso de redes libres, las cuales son analizadas más adelante.

<sup>4</sup> Si son diferentes a las bandas libres ISM o si se presentan intereses privados, para fines comunitarios es más permisivo, pues es una iniciativa transparente y abierta.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

### 1.12.7 Uso libre del espectro electromagnético

Se considera espectro de uso libre al uso sin necesidad de contraprestación o pago de algunas frecuencias o bandas de frecuencias del espectro radioeléctrico, atribuidas, permitidas y autorizadas de manera general y expresa por el Ministerio de Tecnologías de Información y Comunicación (TIC), definición contenida en la Resolución 689 de 2004. Esta resolución atribuyó unas bandas de frecuencias radioeléctricas para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local que utilicen tecnologías de espectro ensanchado y modulación digital (de banda ancha y baja potencia), en las condiciones establecidas por dicha resolución.

El artículo 5 de la norma atribuyó las siguientes bandas de frecuencias para la operación de dichos sistemas inalámbricos:

- Banda de 902 a 928 MHz.
- Banda de 2.400 a 2.483,5 MHz.
- Banda de 5.150 a 5.250 MHz.
- Banda de 5.250 a 5.350 MHz.
- Banda de 5.470 a 5.725 MHz.
- Banda de 5.725 a 5.850 MHz.

Igualmente, la Resolución 797 de 2001 atribuyó unas frecuencias y bandas de frecuencias radioeléctricas para su uso libre por parte del público general, en aplicaciones de: telemetría, tele-comando, tele-alarmas, telecontrol vehicular, dispositivos de operación momentánea, microfónica inalámbrica y transceptores de voz y datos que posean bajos niveles de potencia o de intensidad de campo, con las características técnicas particulares descritas en dicha resolución.

Por su parte, la Resolución 2190 de 2003 atribuyó unas frecuencias radioeléctricas para uso libre del público en general, en aplicaciones de radios de baja potencia y corto alcance de operación itinerante y definió las características técnicas de operación para la utilización de estos, en las condiciones que se establecen en esta norma.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

### • 1.13 Plan Vive Digital

Es el plan de tecnología para los próximos cuatro años en Colombia, desde el cual se busca que el país realice un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional.

El plan responde al reto del actual gobierno por alcanzar la prosperidad democrática gracias a la apropiación y el uso de la tecnología. *Vive Digital* le apuesta a la masificación de Internet. Está demostrado que hay una correlación directa entre la penetración de Internet, la apropiación de las Tecnologías de la Información y las Comunicaciones (TIC), la generación de empleo y la reducción de la pobreza. El plan *Vive Digital* conlleva entonces importantes beneficios sociales y económicos.

Según estudios de Raúl Katz, de la Universidad de Columbia, en el caso chileno al aumentar en 10% la penetración de Internet se generó una reducción en el desempleo del 2%. Según el UNCTAD, *Information Economy Report 2010*, en países en desarrollo como Filipinas e India, por cada empleo generado en la industria TIC se generan entre 2 y 3.5 empleos adicionales en la economía. Según el Banco Mundial y el reporte del Foro Económico Mundial, *The Global Information Technology Report 2010*, hay una correlación directa entre el *Network Readiness Index*, que mide el uso y desarrollo de las TIC, y su competitividad internacional.

Encontramos que Colombia debe superar diversas barreras para lograr la masificación de Internet. Tenemos barreras en todas las partes del ecosistema digital, es decir: en infraestructura, servicios, aplicaciones y usuarios. Aquí se propone analizar estas barreras y presentar diversas iniciativas para superarlas.

#### 1.13.1 Objetivos y aspiraciones del plan *Vive Digital*

El objetivo principal del plan *Vive Digital* es impulsar la masificación del uso de Internet, para dar un salto hacia la prosperidad democrática. A través de la masificación del uso de Internet, de la apropiación de tecnología y de la creación de empleos TIC directos e indirectos, se puede lograr la reducción del desempleo y la pobreza, así como aumentar la competitividad del país para dar un salto hacia la prosperidad democrática.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

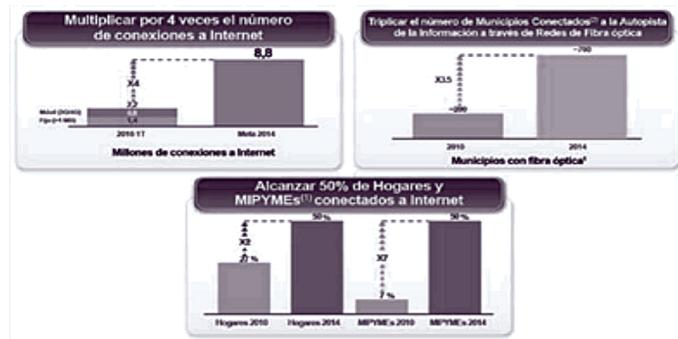


Figura 1.17. Mapas de conexión en Colombia.

Fuente: MinTic (2010-2014).

Para lograr la masificación del uso de Internet, el equipo del plan *Vive Digital* ha fijado algunas metas concretas para el año 2014 (MinTic, 2010-2014) (Figura 1.17):

- Triplicar el número de municipios conectados a la autopista de la información. Queremos expandir esta infraestructura para llegar al menos a 700 municipios del país.
- Conectar a Internet al 50% de las MIPYMES y al 50% de los hogares. Queremos en el 2014 llegar al 50% tanto de hogares como de MiPyMes.
- Multiplicar por 4 el número de conexiones a Internet. Queremos llegar en el 2014 a 8.8 millones.

Para alcanzar estas metas, el plan *Vive Digital* desarrollará el ecosistema digital del país.

### 1.13.2 Principios básicos del Plan *Vive Digital*

Para asegurar que las intervenciones estatales sean adecuadas e integrales y logren optimizar el uso de los recursos, el plan sigue cinco principios básicos:

- “El mercado hasta donde sea posible, el Estado hasta donde sea necesario” (La Tercera Vía, 1999, Dr. Juan Manuel Santos. Promover el desarrollo del sector privado para expandir infraestructura y ofrecer servicios.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Incentivar de forma integral la oferta y la demanda de servicios digitales para alcanzar una masa crítica.
- Reducir barreras normativas e impositivas para facilitar el despliegue de infraestructura y oferta de servicios de telecomunicaciones.
- Priorizar los recursos del Estado en inversiones de capital.
- El Gobierno va a dar ejemplo.

### 1.13.3 Barreras que impiden la masificación de Internet en Colombia

A partir del análisis que se ha hecho, hemos encontrado que en Colombia existen cuatro grandes barreras que dificultan la masificación del uso de Internet (Tabla 1.2).

- **Ciudadanos y microempresas no ven la utilidad.** Como muestran las encuestas, una de las grandes razones para no tener Internet, tanto para los ciudadanos como para las microempresas, es que no encuentran la necesidad o utilidad de este servicio. Ello se debe, en parte, a la falta de contenidos y aplicaciones locales útiles para el ciudadano o microempresa nacional, así como a la falta de apropiación de la tecnología.
- **Bajo poder adquisitivo del ciudadano.** El costo de los terminales y el servicio de Internet sigue siendo relativamente alto para los ingresos de la mayoría de los ciudadanos, por lo que muchos de éstos no tienen posibilidad económica de acceder a ellos.
- **Altos costos de desplegar infraestructura.** En el país, actualmente sólo alrededor de 200 municipios de los 1.102 están conectados a través de la red de fibra óptica. Las características geográficas y de dispersión, han limitado el despliegue de las redes de telecomunicaciones. También, existen dificultades administrativas tanto en los territorios como en la última milla, para el despliegue de infraestructura.
- **Recursos.** La realidad colombiana hace que los recursos con los que cuenta el Estado para invertir en infraestructura sean limitados, por lo que es importante encontrar la mejor manera de invertirlos.



Tabla 1.2. Barreras que impiden la masificación de Internet en Colombia.

Ciudadanos y microempresas no ven utilidad	Bajo poder adquisitivo del ciudadano	Alto costo para desplegar infraestructura	Recursos
<ul style="list-style-type: none"><li>Insuficientes aplicaciones</li></ul>	<ul style="list-style-type: none"><li>Terminales</li><li>Servicio</li></ul>	<ul style="list-style-type: none"><li>Dispersión y complejidad geográfica</li><li>Alrededor de 200 municipios conectados con fibra óptica</li><li>Complejidad administrativa última milla</li></ul>	<ul style="list-style-type: none"><li>Presupuestos limitados de inversión del gobierno</li></ul>

Fuente: MinTic (2010-2014).

#### 1.13.4 Iniciativas para superar barreras de masificación de Internet

- **Inversión para la ejecución del Plan Vive Digital.** La cifra que se estimó en octubre de 2010 para la implementación de las iniciativas fue de 5.5 billones de pesos, de los cuales 3.2 billones resultan de las decisiones del Ministerio de Tecnologías de la Información y las Comunicaciones y 2.3 billones hacen parte de las iniciativas de los demás ministerios.
- **Tiempo de duración.** El Plan Vive Digital será la política de gobierno en materia TIC durante los próximos cuatro años (2014-2018).
- **Metas del Plan Vive Digital.** Metas específicas para la masificación de Internet en 2014:
  - Pasar de 27 a 50% de hogares y del 7% al 50% de MiPymes conectados a Internet.
  - Multiplicar por cuatro las conexiones a Internet, pasando de 2.2 a 8.8 millones.
  - Triplicar el número de municipios conectados a la autopista de la información, a través de redes de fibra óptica (alrededor de 200 hasta llegar a 700 municipios).
  - ¿Qué busca el Plan Vive Digital en cuanto a servicios?
    - Reducir el IVA para Internet.
    - Masificar los terminales para Internet.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Crear un esquema de subsidios para Internet para Estratos 1 y 2.
- Crear un Marco Legal y Regulatorio para la Convergencia.
- Reducir el impacto de las TIC en el Medio Ambiente (MinTic, 2010-2014).

### 1.13.5 Redes WLAN

Antes de entender el porqué de una red WLAN, es necesario entender que una red inalámbrica, como su nombre lo dice, es aquella en la que dos o más terminales obtienen comunicación sin la existencia de conexiones por medio de cables. Entre éstas existen varias categorías que dependen del área de cobertura (Figura 1.18).

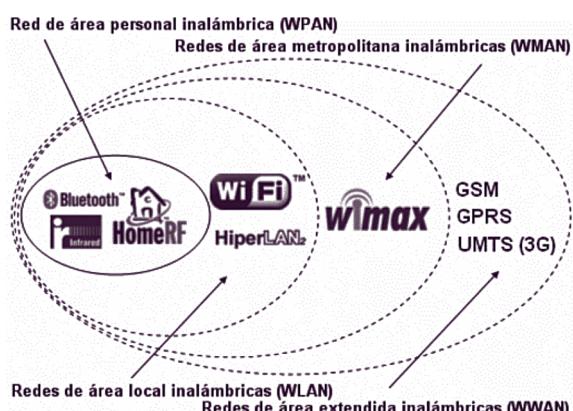


Figura 1.18. Categorías de redes inalámbricas por su área de cobertura.

Fuente: CCM Benchmark Group (2016).

Las redes WLAN según la empresa CISCO System, reconocida por su fabricación, mantenimiento, venta y consultoría de todo aquello relacionado con equipos de telecomunicaciones, hace referencia de la siguiente manera: "Una red WLAN usa ondas de radio para transmitir datos y conectar dispositivos tanto a Internet como a la red y aplicaciones de su empresa" (CISCO, 2016). Sin embargo, si se desglosa su abreviatura se encuentra WLAN (*Wireless Local Area Network*) lo cual, traducido al español, significa: Red de Área Local, dicho concepto se asocia a toda aquella comunicación existente entre datos de manera inalámbrica y flexible; alternativa de mayor uso que las conocidas redes LAN, las cuales son enfocadas a dicha comunicación.

Así que en la actualidad los almacenes, los hogares, las comunidades, usan las redes WLAN para la comunicación de datos en un tiempo real y hacia una terminal central, inclusive, cuando se habla de internet compartido para varios equipos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Existen más conceptos para entender las funciones de las redes WLAN, donde intervienen características como movilidad, flexibilidad y facilidad de instalación, ya que se transmite información en tiempo real en cualquier lugar de utilización para el usuario. Su facilidad de instalación (gracias al método inalámbrico) evita toda clase de uso de cables, y su flexibilidad, supera el mayor número de obstáculos, sin importar las paredes que existan desde el punto de partida o inicio hasta el punto de llegada a los equipos necesarios.

Se observa un concepto interesante sobre dichas redes en la siguiente descripción: "Sistema de comunicaciones de datos que transmite y recibe datos inalámbricos flexibles utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica, utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (*peer to peer*), dentro de un edificio, de una pequeña área residencial/ urbana o de un campus universitario" (QWERTY, 2010) o porqué no, un campo rural. Razones que motivan a usar estas redes para zonas rurales de Colombia, siendo algo elemental en la actualidad para la educación, el trabajo y el comercio entre otras áreas.

### • 1.15 Ataques a Redes WLAN

Una de las características poco mencionadas al hablar de las redes inalámbricas WLAN, es la inseguridad que estas pueden contener, pues son vulnerables a ataques en el transcurso de la información, debido a la propagación que se presenta en la señal, ya que esta se genera hacia todas las direcciones.

Para poder brindar seguridad en redes es importante reconocer primero cuáles son los posibles ataques que pueden sufrir las redes WLAN. Dichos ataques se dividen en dos grandes grupos: ataques pasivos y ataques activos.

#### 1.15.1 Ataques pasivos

Su principal objetivo para atacar las redes es lograr obtener información, suponiendo un primer paso para poder atacar posteriormente, por ejemplo, monitorizaciones y escuchas de la red (Andreu, Pellejero, & Lesta, 2006).

Dentro de este grupo se pueden encontrar ataques como los siguientes:



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- **Espionaje o *surveillance*.** Consiste en observar el entorno en el que se relaciona dicha red para así recopilar información relacionada con la topología de la red. Datos que se usan para un próximo ataque, sin necesidad de un *hardware* o un *software* específico, simplemente se genera ataque teniendo acceso a la instalación. Información usada para su favor, con motivos de daño al usuario principal.
- **Escuchas o *sniffing*.** Su objetivo final es monitorizar la red para así poder tener el acceso a información sensible como la dirección IP de origen y destino, contraseñas, clave WEP (IEEE, 1999), con el modo de inyectar o modificar los mensajes.  
Al obtener información comprometida son considerables los ataques de gran impacto y peligro, difícilmente detectables.
  - Las herramientas que permiten obtener estos datos son los *sniffers* y los analizadores de protocolos.
  - Un *sniffer* o rastreador de red es un proceso que olfatea el tráfico que se genera en la red a nivel de enlace; de este modo puede leer toda la información que circule por el tramo (segmento) de red en el que se encuentre.
- Un analizador de protocolos es un *sniffer* que ha extendido su funcionalidad para comprender ciertos protocolos y permite analizar la información contenida en los paquetes enviados por la red.  
Un ordenador conectado a una red mediante un *hub* puede ver el tráfico de toda la red poniendo su tarjeta en modo promiscuo y analizarlo con programas como tcpdump, dsniff, wireshark, ettercap (ac.usc.es, 2016).
- **Warchalking:** Este ataque hace referencia al lenguaje de símbolos normalmente utilizados para señalar el sitio donde se encuentra la red inalámbrica, de forma que aquella persona que pase por allí pueda utilizarla. La simbología es sencilla y clara (Figura 1.19 ); el objetivo es identificar si la red es cerrada con clave de acceso o si es abierta sin clave de acceso, claro está que se debe especificar que la misma indica el nombre de la red SSID, además indicando qué velocidad es manejada para dicha red.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid 
CLOSED NODE	ssid 
WEP NODE	ssid access contact 

blackbeltjones.com/warchalking

Figura 1.19. Simbología.

Fuente: McGarvey (2002).

### 1.15.2 Ataques activos

Este ataque hace referencia a la modificación en el flujo de datos o la creación de falsos flujos en la transmisión de datos. Teniendo dos objetivos generales: uno, suplantar al usuario para así obtener información ajena o dos, colapsar la red para así bajar la funcionalidad de los servicios que este mismo puede prestar.

- **Spoofing.** Consiste en la creación de trampas TCP/IP utilizando una dirección IP falsa para así suplantar la red y obtener información (Figura 1.20). Para esto, entran en juego tres máquinas: un atacante, un atacado y un sistema suplantado con que se relaciona con el atacado (Princeton University, 1997).

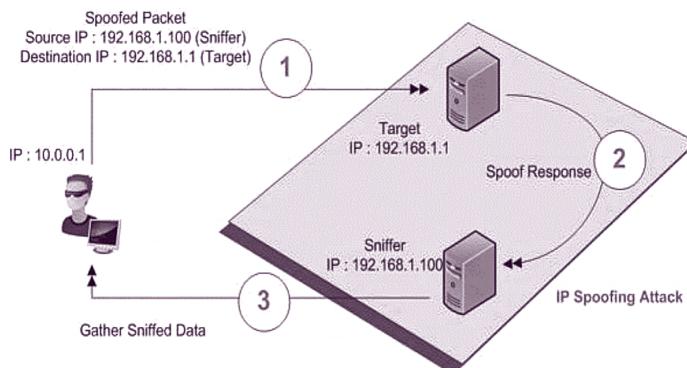


Figura 1.20. Relación con la que se modifica las IP.

Fuente: Phatak (2011).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

En la Figura 1.21 se observa la información con la que la red se vuelve vulnerable y que los atacantes pueden llegar a modificar, para así tener el acceso a la red que desean suplantar.



Figura 1.21. Validadores, Suplantantes mediante *Spoofing*.

Fuente: Libro Virtual Redes WLAN (2013).

- **Man in the Middle (MITM).** Como su nombre lo indica “hombre en el medio” es un tipo de amenaza que se aprovecha de un intermediario. El atacante, en este caso, tiene la habilidad de desviar o controlar las comunicaciones entre dos partes. Por ejemplo, si se tratase de un ataque MITM a algún correo electrónico, el perpetrador podría desviar todos los e-mails a una dirección alterna para leer o alterar toda la información antes de enviarla al destinatario correcto (González, 2014) con el fin, en general, de obtener información y a su vez modificarla para algún mal en específico (Figura 1.22).

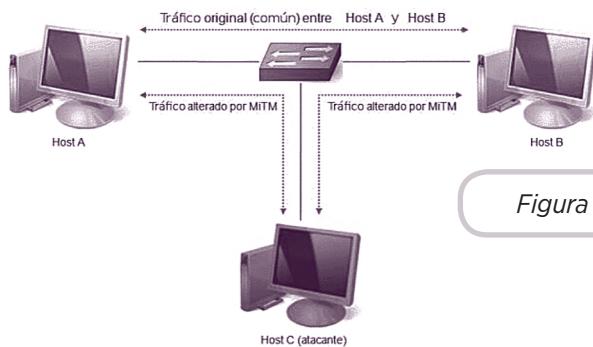


Figura 1.22. Ilustración del ataque MITM.

Fuente: Infyseg (2013).

## • 1.16 Mecanismos de seguridad

Al hablar de seguridad en estas redes se trata de abarcar dos elementos importantes: el acceso a la red (autenticación) y la protección de los datos a trasmisir (encriptación). Las violaciones que se presentan en las redes WLAN son aquellas que generalmente vienen desde los puntos de acceso no autorizados o por terceros quienes modifican la trasmisión (Figura 1.23). A continuación, se nombran algunos mecanismos de seguridad para las redes WLAN.



### 1.16.1 Especificación original 802.1

Esta especificación utiliza tres mecanismos así:

- **SSID (Identificador de servicio):** contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía.
- **Filtrado con dirección MAC (Control de acceso al medio):** restringe el acceso a computadoras cuya dirección MAC del adaptador está presente en una lista, creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico.
- **WEP (Privacidad equivalente a cable):** es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema, cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de estas se dificulta con el incremento en el número de estaciones (Ruiz, 2004).

### 1.16.2 Mecanismo 802.1X

Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas, usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes (RADIUS<sup>5</sup>, Servicio Remoto de Autenticación de Usuarios Entrantes).

<sup>5</sup> "El Servidor de directivas de redes (NPS) se puede usar como un servidor de servicio de autenticación remota telefónica de usuario (RADIUS) para llevar a cabo la autenticación, la



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

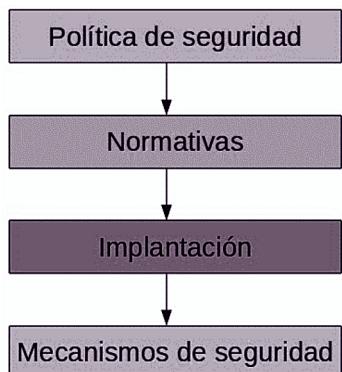


Figura 1.23. Mecanismos de seguridad para la instalación de redes inalámbricas.

Fuente: Wordpress (2013).

### 1.16.3 Otros mecanismos de seguridad (Romero, 2003/2004)

#### ○ De prevención:

- Mecanismos de autenticación e identificación.
- Mecanismos de control de acceso.
- Mecanismos de separación (física, temporal, lógica, criptográfica y fragmentación).
- Mecanismos de seguridad en las comunicaciones (cifrado de la información).

#### ○ De detección:

- IDS (*Intruder Detected System*).

#### ○ De recuperación:

- Copias de seguridad (*Backup*).
- Mecanismos de análisis forense: averiguar alcance, las actividades del intruso en el sistema y cómo ingresó.

### 1.16.4 SLL (Secure Sockets Layer)

Es un protocolo diseñado para permitir que las aplicaciones transmitan información de ida, y de manera segura hacia atrás. Las aplicaciones que utilizan el protocolo *Secure Sockets Layer* sí saben cómo dar y recibir claves

autorización y las cuentas para clientes RADIUS. Un cliente RADIUS puede ser un servidor de acceso, como un servidor de acceso telefónico o punto de acceso inalámbrico, o un proxy RADIUS" (Microsoft Corp., 2003).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos.

Algunas aplicaciones que están configuradas para ejecutarse incluyen navegadores *Web* como Internet Explorer y Firefox, programas de correo como Outlook, Mozilla Thunderbird, Mail.app de Apple, y SFTP (*Secure File Transfer Protocol*), etc. Estos programas son capaces de recibir de forma automática conexiones SSL.

Para establecer una conexión segura SSL, sin embargo, la aplicación debe tener una clave de cifrado que le asigna una autoridad de certificación en la forma de un certificado. Una vez que haya una única clave de la cuenta, se puede establecer una conexión segura utilizando el protocolo SSL (DigiCert, 2003-2016).

#### 1.16.5 HTTPS (Protocolo seguro de transferencia de hipertexto)

El protocolo de transferencia de hiper-texto (HTTPS) es la versión segura del HTTP (*Hyper Text Transfer Protocol*), siendo la más conocida y usada diariamente en Internet. La diferencia es que, con HTTPS se logra desarrollar *e-commerce*, ya que permite realizar transacciones de forma segura; siendo esto un modelo de negocio confiable para la economía.

Este protocolo crea un canal de transferencia cifrado con el que obviamente aumenta la seguridad en el tráfico de información, en comparación con el protocolo HTTP común (Interlab, 2010).

#### 1.16.6 PPTP (Protocolo de túnel punto a punto)

Puede tener acceso a una red privada a través de Internet o de otra red pública, mediante una conexión de red privada virtual (VPN, *Virtual Private Network*) con el Protocolo de túnel punto a punto (PPTP, *Point-to-Point Tunneling Protocol*).

PPTP permite la transferencia segura de datos desde un equipo remoto a un servidor privado, al crear una conexión de red privada virtual por medio de redes de datos basadas en IP. PPTP acepta redes privadas virtuales bajo demanda y multiprotocolo a través de redes públicas, como Internet.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Desarrollado como una extensión del Protocolo Punto a Punto (PPP), PPTP agrega un nuevo nivel de seguridad mejorada y comunicaciones multiprotocolo a través de Internet (Figura 1.24). Si se utiliza el nuevo protocolo de autenticación extensible (EAP, *Extensible Authentication Protocol*) con métodos de autenticación seguros como los certificados, la transferencia de datos a través de una conexión VPN con PPTP es tan segura como en una LAN de un sitio corporativo.

PPTP encapsula los protocolos IP o IPX en datagramas PPP. Esto significa que puede ejecutar de forma remota aplicaciones que dependen de protocolos de red específicos. El servidor de túnel ejecuta todas las comprobaciones y validaciones de seguridad, y activa el cifrado de los datos, lo que hace mucho más seguro el envío de información a través de redes no seguras. También se puede utilizar PPTP para establecer conexiones de LAN a LAN privadas (Microsoft Corp., 2003).

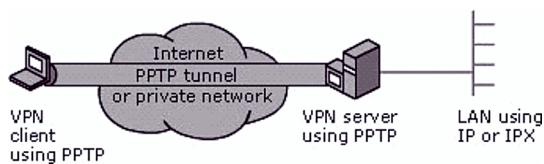


Figura 1.24. Diagrama del protocolo PPTP de Microsoft.

Fuente: Microsoft Corp. (2003).

### • 1.17 El contexto de las redes MESH

Hoy en día, las redes inalámbricas han facilitado el acceso a la información por diferentes medios y hacia muchas personas, de manera que el aporte de la tecnología inalámbrica prácticamente ha cambiado al mundo, impulsando nuevos paradigmas de uso que hace unas décadas se pensaban como una fantasía. Actualmente, es una realidad gratamente materializada, y justo en estos momentos, su capacidad evoluciona hasta niveles insospechadas e inimaginables, mientras que su costo disminuye o al menos, se ajusta a las capacidades financieras de una persona común, lo cual posibilita diversos factores para la estimulación de investigaciones sobre el funcionamiento de las redes MESH, pues son recursos que se consideran de fácil acceso, al alcance de todos y a un costo razonable.

Partiendo del principio básico en que el ser humano vive para su sociedad, un rasgo noble que muchas personas comparten como vivir en una comunidad



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

estable, satisfecha y en constante evolución, este proyecto busca que el usuario sea capaz de aprovechar lo que se ofrece en una red MESH para poder compartirlo con su comunidad, formando así, la cultura de una sociedad libre.

### • 1.18 Atributos de una red MESH

En la Figura 1.25 se puede observar un planteamiento ideológico de cómo se genera la cultura de la sociedad libre, que hoy en día ha permitido la creación de diversos tipos de culturas y paradigmas que han traído increíbles regalos para la sociedad.



Figura 1.25. Inspiración de iniciativa de redes MESH.

Fuente: elaboración propia.

Uno de los principales puntos de una red MESH es la comunidad: en la medida en que ésta crezca, mayor será la red. Ello significa más nodos, mayor alcance, mayores recursos para compartir y aprovechar, así como más fuentes desde donde compartir, ya que habrá más personas interesadas en estos ámbitos. Comparado con lo que pueden llegar a proveer otros medios informativos como la radio, la televisión y el teléfono, las redes MESH pueden lograr un contacto directo con una comunidad completa en tiempo real, las 24 horas al día, 7 días a la semana, lo que la hace una red moldeable y en constante evolución, si así lo desea la comunidad.

Esto mismo es lo que la hace tan importante a la hora de compararla con Internet, la cantidad de servicios y el tipo de función que realiza depende de su



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

creatividad y empeño, por poner un pequeño ejemplo: comunicaciones de voz, el correo electrónico y otros datos, pueden ser intercambiados a un bajo costo. Mientras un usuario comparte dichos servicios, otro fácilmente puede colocar un servicio de documentación para aprender a hacer videojuegos en una determinada plataforma bajo un perfil diferente, y mejor aún, si dichos recursos son de fuente abierta, podría compartir absolutamente toda la fuente sin temor a repercusiones por parte de infracción de licencias ni situaciones similares, que tanto abundan en la red de redes, gobernada bajo ese tipo de ley marcial *online*.

Cuando se habla de redes MESH se trata de algo muy importante, el estándar 802.11, la cual abarca todo lo relacionado con la tecnología inalámbrica, pero en este caso en particular, se analizará el patrón dedicado a la transmisión de datos.

### • 1.19 Rango y flujo de datos

Los estándares 802.11a, 802.11b, 802.11g y 802.11n, llamados “estándares físicos” (Hackerfriendly, 2008), son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Tabla 1.3. Rango de velocidades de los protocolos

Estándar	Frecuencia	Velocidad	Rango
Wifi a (802.11a)	5 GHz	54 Mbit/s	10 m
Wifi b (802.11b)	2,4 GHz	11 Mbit/s	100 m
Wifi g (802.11g)	2,4 GHz	54 Mbit/s	100 m
Wifi n (802.11n)	2,4 GHz y 5 GHz	300 Mbit/s	150 m

Fuente: elaboración propia.

- **Estándar 802.11a:** el estándar 802.11 tiene en teoría en flujo de datos máximo de 54 Mbps, cinco veces el del 802.11b y sólo a un rango de 30 metros aproximadamente. El estándar se basa en la tecnología ODFM (multiplicación por división de frecuencias ortogonales) (Tanenbaum, 2012) Transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no superpuestos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Es por esto por lo que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de “banda dual”.

- **Estándar 802.11b:** el estándar 802.11b permite un máximo de transferencia de datos de 11 Mbps en un rango de 100 metros aproximadamente, en ambientes cerrados, y de más de 200 metros al aire libre, incluso más que eso, con el uso de antenas direccionales.
- **802.11g:** el estándar 802.11g permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los 802.11b. Además, y debido a que el estándar 802.11g utiliza el rango de frecuencia de 2,4 GHz con codificación ODFM, es compatible con los dispositivos 802.11b, con excepción de algunos más antiguos.
- **802.11n:** el estándar WiFi IEEE 802.11n es la próxima generación de tecnología inalámbrica que entrega espectaculares mejoras en confiabilidad, velocidad y rango en comunicaciones 802.11. Cuenta con una velocidad de modulación cerca de seis veces más rápida y una tasa de transferencia de datos de 2 a 5 veces mayor que una antena WiFi 802.11 a/g, mejoras sustanciales en cobertura y calidad de conexión. El WiFi 802.11n fue diseñado para reemplazar por completo la actual tecnología alámbrica (*Ethernet*) y convertirse en la tecnología dominante en redes de área local.  
Las antenas WiFi 802.11n introducen varias mejoras a las capas 802.11 PHY (radio) y MAC, que resultan en mejor *throughput* y confiabilidad para redes inalámbricas.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 1.4. Rango de velocidades 802.11a/b/g vs 802.11n

Una cadena de datos (MCS0-7)			Dos cadenas de datos (MSC8-15)			
Velocidades 802.11a/g	Velocidades 802.11n Requeridas (canal de 20 MHz)	Velocidades 802.11n Requeridas (canal de 40 MHz)	Intervalo de Guarda Corta Habilitado	Dos Cadenas	802.11n Velocidad Requerida (canal de 40 MHz)	Intervalo de Guarda Corta Habilitado
6	6.5	13.5	15	13	27	30
9	13	27	30	26	54	60
12	19.5	40.5	45	39	81	90
18	26	54	60	52	108	120
24	39	81	90	78	162	180
36	52	108	120	104	216	240
48	58.5	121.5	135	117	243	270
54	65	135	150	130	270	300

Fuente. elaboración propia.

En el estándar 802.11, la banda de frecuencia 2.400 - 2.4835 GHz (83.5 MHz de ancho) se ha dividido en 14 canales distintos de 5 MHz cada uno. Sólo los primeros 11 se pueden usar en Estados Unidos y Canadá; en el Reino Unido se pueden usar los canales del 1 al 13 solamente<sup>6</sup>.

Sin embargo, para una correcta transmisión de 11 Mbps se debe transmitir en una banda de MHz porque, de acuerdo con el teorema de Shannon<sup>7</sup>:

$$C = B \log_2 (1+S/N) \text{ bps}$$

La frecuencia de muestreo debe ser al menos el doble de la señal para que se digitalice. Algunos canales se superponen con canales cercanos. Es

<sup>6</sup> Debe consultarse cada regulación del espectro de cada país, para saber cuáles son los parámetros que pueden usarse.

<sup>7</sup> Claude Elwood Shannon (30 de abril de 1916 – 24 de febrero de 2001), fue un matemático, ingeniero eléctrico y criptógrafo. Es considerado como “el padre de la teoría de la información”, después de la investigación de Nyquist estudió acerca de cómo el ruido afecta a la transmisión de datos. Shannon tomó en cuenta la razón señal-a-ruido del canal de transmisión (medido en decibeles o dB) y derivó el Teorema de Capacidad de Shannon.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

por ello que generalmente se utilizan canales aislados (1, 6 y 11) que están a 25 MHz de distancia.

Por lo tanto, cuando dos puntos de acceso que usan los mismos canales tienen áreas de transmisión que se superponen, las distorsiones de señal pueden afectar las transmisiones. Para evitar cualquiera de estas interferencias, se recomienda distribuir los puntos de acceso y seleccionar canales, de tal manera que dos puntos de acceso que usen el mismo canal nunca se encuentren cerca.

Las comunicaciones inalámbricas hacen uso de las ondas electromagnéticas para enviar señales a través de largas distancias. Desde la perspectiva del usuario, las conexiones inalámbricas no son particularmente diferentes de cualquier otra conexión. Generalmente, al usuario no le importa cuál es la mejor alternativa de conexión y qué parámetros debe usar para que funcione correctamente su navegador, su correo y demás aplicaciones que espera que trabajen como es debido.

En una red MESH, aunque no es vital su comprensión, se espera que el usuario conozca su implementación, y para ello, es necesario que su administrador entienda las nociones básicas de las telecomunicaciones por vía inalámbrica, de la manera más estable y con mayor velocidad. Por lo cual, es importante entender las propiedades físicas que son las que hacen posible el enlace y la comunicación inalámbrica con conceptos tales como una onda de radio, y todo lo que se relaciona con ello.

## ¿Qué es una onda de radio?

El concepto de onda viene relacionado con el movimiento ondulatorio o vibración en muchas formas: puede ser un péndulo, un árbol meciéndose con el viento, las cuerdas de una guitarra, una piedra chocando con un río, entre otros.

Todos estos casos son ejemplos perfectos de onda de radio, desarrollándose en un medio determinado, vibrando de forma periódica, con un cierto número de ciclos por unidad de tiempo. Se desarrolla un movimiento denominado onda mecánica, que es definida por el medio de propagación (Hackerfriendly, 2008). Medios conocidos en los que las oscilaciones de una onda de radio mecánica se propagan, pueden ser tanto el aire, el agua, un objeto sólido en particular como edificios, metales y papel, hasta el mismo vacío.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Una onda tiene cierta velocidad, frecuencia y longitud de onda. Las mismas están conectadas en la siguiente relación:

$$\text{Velocidad} = \text{Frecuencia} * \text{Longitud de onda}$$

La longitud de onda (denominada como lambda,  $\lambda$ ) es la distancia medida desde un punto en una onda hasta la parte equivalente de la siguiente, por ejemplo, desde la cima de un pico, hasta la siguiente.

La frecuencia es el número de ondas enteras que pasan por un punto fijo en un segundo.

La velocidad se mide en metros/segundos; la frecuencia, en ciclos por segundos (denominado Hertz Hz); y la longitud de onda en metros. Por ejemplo, si una onda en el agua viaja a un metro por segundo y oscila cinco veces por segundo entonces cada onda tendrá veinte centímetros de largo:

$$1 \text{ metro/segundo} = 5 \text{ ciclos/segundos} * \lambda \\ \lambda = 1 / 5 \text{ metros} \lambda = 0.2 \text{ metros} = 20 \text{ centímetros}$$

Las ondas también tienen una propiedad denominada **amplitud**. Esta es la distancia desde el centro de la onda hasta el extremo de uno de sus picos, y puede ser asimilada a la altura de una onda de agua.

Realmente no hace falta saber mucho para ver una onda, simplemente tirando una piedra en un lago o tocando una cuerda de una guitarra es posible visualizar el movimiento ondulatorio, pero para entender qué es lo que está oscilando y todo su proceso, es necesario entender el concepto de fuerza electromagnética.

## • 1.20 Fuerzas electromagnéticas

Las fuerzas electromagnéticas son fuerzas entre cargas y corrientes eléctricas. Por ejemplo, se percata de ellas cuando se toca la manija de una puerta después de haber caminado en una alfombra sintética o cuando se está rozando una cerca eléctrica. Los relámpagos de plasma generados durante las tormentas eléctricas son un perfecto ejemplo (Hackerfriendly, 2008).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

La fuerza eléctrica es la fuerza entre las cargas eléctricas. La fuerza magnética es la fuerza entre corrientes eléctricas.

Los electrones son partículas que tienen carga eléctrica negativa. También hay otras partículas, pero los electrones son responsables de la mayor parte de las cosas relacionadas con el funcionamiento de un radio, por poner un ejemplo.

## ○ **Ganancia**

Esto viene a ser la potencia de amplificación de la señal, la ganancia representa la relación entre la intensidad de campo que produce una antena en un punto determinado, y la intensidad de campo que produce una antena omnidireccional (llamada isotrópica) en el mismo punto y en las mismas condiciones. Cuanto mayor es la ganancia, mejor es la antena (Delgado, 2009).

La ganancia de la antena se proporciona habitualmente en dB isotrópicos (dBi), es decir, la ganancia de potencia con respecto a un modelo teórico de antena isotrópica que radia la misma energía en todas las direcciones del espacio. En algunos casos la ganancia se expresa en dBi con respecto a una antena de tipo dipolo. En este caso, se tiene la siguiente fórmula de conversión:

$$G \text{ (dBi)} = G \text{ (dBm)} + 2,14$$

Las ganancias típicas de las antenas varían entre 2 dBi (antena integrada sencilla) a 5 dBi (omnidireccional estándar), 15 dBi (antena omnidireccional para exteriores, que se implementara a modo práctico) hasta 25 – 30 dBi (parabólica).

## ○ **Relación señal - ruido (Delgado, 2009)**

Siempre que se emite o se recibe una señal de radio, lleva acoplada una señal de ruido (*Ruido Termal*, ruido industrial debido por ejemplo a microondas o ruido de interferencia debido a otra WLAN en la misma banda de frecuencia). Obviamente, cuanto menor sea la relación de ruido con respecto a la señal óptima se considerará la señal válida. Incluso en las transmisiones digitales, se tienen que usar métodos de modulación que reduzcan el ruido y amplifiquen la señal de radio.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

El resultado de dividir el valor de la señal de datos, entre la señal de ruido es lo que se conoce como relación señal/ruido. Cuanto mayor es, mejor es la comunicación. Se expresa en decibelios (dB) y en escala exponencial, lo que quiere decir que una relación señal/ruido de 10 dB, indica que la señal es 10 veces mayor que la de ruido, mientras que 20 dB indica 100 veces más potencia.

Si el nivel de ruido es alto se necesitará más energía recibida. En condiciones normales sin ninguna otra WLAN en la frecuencia y sin ruido industrial, el nivel de ruido será de alrededor de -100dBm.

## ○ El espectro electromagnético

Las ondas electromagnéticas abarcan un amplio rango de frecuencias (y, correspondientemente, de longitudes de onda). Este rango de frecuencias y longitudes de onda es denominado espectro electromagnético. La parte del espectro más familiar a los seres humanos es probablemente la luz, la porción visible del espectro electromagnético. La luz se ubica aproximadamente entre las frecuencias de  $7,5 \times 10^{14}$  Hz y  $3,8 \times 10^{14}$  Hz, correspondientes a longitudes de onda desde cerca de 400 nm (violeta/azul) a 800 nm (rojo).

Las frecuencias más interesantes para trabajar este proyecto son 2400 - 2484 MHz, que son utilizadas por los estándares de radio 802.11b y 802.11g (correspondientes a longitudes de onda de alrededor de 12,5 cm). Otro equipamiento disponible comúnmente, utiliza el estándar 802.11a, que opera a 5150 - 5850 MHz (correspondiente a longitudes de onda de alrededor de 5 a 6 cm).

## ○ Ancho de banda

Un término que se encontrará a menudo en la física de radio es ancho de banda, éste es simplemente una medida de rango de frecuencia. Si un rango de 2400 MHz a 2480 MHz es usado por un dispositivo, entonces el ancho de banda sería 0,08 GHz (o más comúnmente 80MHz).

Se puede ver fácilmente que el ancho de banda definido aquí está muy relacionado con la cantidad de datos que se pueden trasmisitir dentro de él: a más lugar en el espacio de frecuencia, más datos caben en un momento dado.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

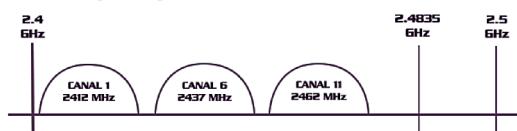
El término ancho de banda es a menudo utilizado por algo que se denomina tasa de transmisión de datos, como cuando se dice: "mi conexión a Internet tiene 1 Mbps de ancho de banda", lo cual significa que ésta puede trasmitir datos a 1 megabit por segundo.

## ○ Frecuencias y canales

En este apartado se verá un poco más de cerca cómo se utiliza la banda 2,4 GHz en el estándar 802.11b. El espectro está dividido en partes iguales, distribuidas sobre la banda en canales individuales, note que los canales son de un ancho de 22 MHz, pero están separados sólo por 5 MHz. Esto significa que los canales adyacentes se superponen, y pueden interferir unos con otros (Figura 1.26).

### Canales despejados para WLAN

#### 802.11b (DSSS) Ancho de Banda 22 MHz



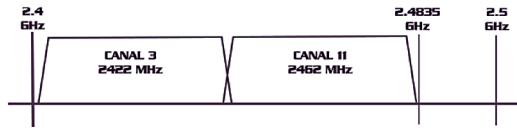
#### 802.11g/n (OFDM) Ancho de Banda 20 MHz



Figura 1.26. Canales y frecuencias despejadas para 802.11b/g/n.

Fuente: elaboración propia.

#### 802.11n (OFDM) Ancho de Banda 40 MHz



## ○ Comportamiento de las ondas de radio

A continuación, se presentan algunas reglas simples que pueden ser de mucha ayuda cuando se elaboran los primeros planes para una red inalámbrica:

- Cuanto más larga la longitud de onda, más lejos llega.
- Cuanto más larga la longitud de onda, mejor viaja a través y alrededor de obstáculos.
- Cuanto más corta la longitud de onda, puede transportar más datos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ Propagación de ondas de radio (Hackerfriendly, 2008)

Las ondas de radio (RF por *Radio Frequency*) se propagan en línea recta en varias direcciones al mismo tiempo y en el vacío se propagan a 3.108 m/s. Las ondas presentan propiedades de propagación como son: absorción, difracción, reflexión y refracción.

- **Absorción:** cuando las ondas electromagnéticas atraviesan algún material, generalmente se debilitan o atenuan. La cantidad de potencia perdida va a depender de su frecuencia y, por supuesto, del material. El vidrio de una ventana es transparente para la luz, mientras que el vidrio utilizado en los lentes de sol filtra una porción de la intensidad de la luz y bloquea la radiación ultravioleta.
- **Difracción:** es el comportamiento de las ondas cuando, al incidir en un objeto, dan la impresión de doblarse. Es el efecto de “ondas doblando las esquinas”. Desde esta abertura va a comenzar una onda circular, y por supuesto va a alcanzar puntos que están en una línea directa detrás de esa abertura, pero también a ambos lados de ella. Si se mira este frente de onda (y pudiera ser también una onda electromagnética) como un haz de luz, sería difícil explicar cómo logra alcanzar puntos que están ocultos por una barrera. Cuando se modela como un frente de onda, el fenómeno tiene sentido.
- **Reflexión:** cuando una onda de radio choca con un obstáculo, parte o la totalidad de la onda se refleja y se observa una pérdida de la intensidad. La reflexión es tal que el ángulo de incidencia equivale al ángulo de reflexión. Por definición, una onda de radio es susceptible de propagarse en varias direcciones. Después de reflejarse varias veces, una señal de origen puede llegar a una estación o punto de acceso después de tomar muchas rutas diferentes (llamadas multirutas). Puede usarse la reflexión en ventaja para la construcción de las antenas: por ejemplo, colocando grandes paráolas detrás del transmisor/receptor para recoger las ondas de radio y concentrarlas en un punto.
- **Refracción:** es el cambio de dirección de una onda cuando cruza el límite entre dos medios en los cuales la onda viaja con diferente rapidez. El fenómeno de la refracción supone un cambio en la velocidad de propagación de la onda, cambio asociado al paso de un medio a otro de diferente naturaleza o de diferentes propiedades. Este cambio de velocidad da lugar a un cambio en la dirección del movimiento



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

ondulatorio. Como consecuencia, la onda refractada se desvía un cierto ángulo respecto del incidente.

## ○ Interferencia

Cuando se trabaja con ondas, uno más uno no es necesariamente igual a dos. Incluso puede resultar cero.

Esto es sencillo de entender cuando se dibujan dos ondas senoidales y se suman las amplitudes. Cuando un pico coincide con el otro pico, se tendrá un resultado máximo ( $1 + 1 = 2$ ). Esto es denominado interferencia constructiva. Cuando un pico coincide con un valle, dará una completa aniquilación ( $1 + (-1) = 0$ ), y se denomina interferencia destructiva.

Puede probar esto creando dos ondas circulares en el agua mediante dos varitas, verá que cuando dos olas se cruzan, hay áreas con picos de onda más grandes y otras que permanecen casi planas y en calma.

Para que los trenes de ondas se sumen o se cancelen perfectamente, tienen que tener exactamente la misma longitud de onda y una relación de fase fija; esto significa posiciones fijas desde el pico de una onda hasta las otras.

En la tecnología inalámbrica, la palabra *interferencia* es usada comúnmente en un sentido amplio, para disturbios desde otras fuentes RF (radio frecuencia), por ejemplo, canales adyacentes. Entonces, cuando los constructores de redes inalámbricas hablan de interferencia, generalmente se refieren a todos los tipos de alteraciones generadas por otras redes y otras fuentes de microondas. La interferencia es una de las principales fuentes de dificultad en el despliegue de enlaces inalámbricos, especialmente en ambientes urbanos, o en espacios cerrados (como en un local para conferencias) donde muchas redes pueden competir por el uso del espectro.

Siempre que las ondas de igual amplitud y fases opuestas se crucen en el camino, son eliminadas y no se pueden recibir señales. El caso más común es que las ondas se combinen y generen una nueva forma de onda que no puede ser utilizada efectivamente para la comunicación. Las técnicas de modulación y el uso de canales múltiples ayudan a manejar el problema de la interferencia, pero no lo eliminan completamente.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ Sensibilidad del receptor

Siempre que las ondas de igual amplitud y fases opuestas se crucen en el camino, son eliminadas y no se pueden recibir señales. El caso más común es que las ondas se combinen y generen una nueva forma de onda que no puede ser utilizada efectivamente para la comunicación. Las técnicas de modulación y el uso de canales múltiples ayudan a manejar el problema de la interferencia, pero no lo eliminan completamente.

Para ello se tienen una serie de parámetros que se emplean en el análisis de diseño para una red inalámbrica, se habla del receptor.

El equipo necesita un mínimo nivel de señal para conseguir un funcionamiento aceptable (denominado nivel de calidad), lo que se conoce habitualmente como sensibilidad. Esta suele expresarse en términos de potencia o tensión de acuerdo con la siguiente fórmula de conversión.

$$S (\text{dBm}) = (\text{dBmV}) - 10 \log_{10} R(\Omega) - 30$$

Cuanto menor sea la sensibilidad, mejor es el receptor de radio. Un valor típico es -82 dBm para un enlace de 11 Mbps y -94 dBm para un enlace de 1 Mbps.

Una diferencia de 10 dB (la cual puede encontrarse fácilmente entre diferentes tarjetas) es tan importante como 10 dB de ganancia que se puedan obtener mediante el uso de amplificadores o antenas más altas.

## ○ Pérdidas de propagación en espacio libre

Se trata de pérdidas de propagación que sufre la señal radioeléctrica en condiciones de espacio libre: sin ningún obstáculo en el camino, es decir, visión directa entre las antenas. En esta magnitud no suelen incluirse otras pérdidas adicionales debidas a lluvia, absorción atmosférica, etc. Las pérdidas mencionadas inicialmente están relacionadas directamente con la distancia del enlace y la frecuencia de funcionamiento de este mediante la expresión (Hackerfriendly, 2008):

$$L_{\text{bas}} (\text{dB}) = 92,44 + 20 \log_{10} f(\text{GHz}) + 20 \log_{10} d(\text{Km})$$



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ Pérdidas adicionales de propagación

Las señales sufren pérdidas adicionales durante su propagación que realmente no pueden atribuirse ni catalogarse hacia el grupo de espacio libre, fenómenos climáticos, difracciones, reflexión, obstáculos naturales o construcciones que entran en este tipo de categoría, y son imposibles de clasificar, pues su variación depende del entorno en donde está instalado el enlace.

## ○ Pérdida de espacio libre en 2.4 GHz

Es la pérdida de energía de recorrido de onda en espacio libre (sin obstáculos). Corresponde a una pérdida entre ganancia de espacio libre en dB y distancia en kilómetros, la Tabla 1.5 muestra tal información para una frecuencia de 2.45 GHz.

Tabla 1.5. Pérdida de espacio libre en 2.4 GHZ.

Pérdida en dB (valor negativo)	Km
-100.399	1
-114.379	5
-120.4	10
-128.358	25
-134.379	50
-137.901	75
-140.4	100

Fuente. elaboración propia.

## ○ Línea visual

El término línea visual, a menudo abreviada como LOS (por su sigla en inglés, *Line of Sight*), es fácil de comprender cuando se habla acerca de la luz visible: si es posible ver un punto B desde un punto A, aparece una línea visual. Dibujando simplemente una línea desde A hasta B, y si no hay nada en el camino, parecerá una línea visual (Hackerfriendly, 2008).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Las cosas se ponen un poco más complicadas cuando se está tratando con microondas. Recuerde que la mayoría de las características de propagación de las ondas electromagnéticas son proporcionales a la longitud de onda. Este es el caso del ensanchamiento de las ondas a medida que avanzan. La luz tiene una longitud de onda de aproximadamente 0,5 micrómetros, las microondas usadas en las redes inalámbricas tienen una longitud de onda de unos pocos centímetros. Por consiguiente, los haces de microondas son más anchos, necesitan más espacio.

Los haces de luz visibles también se ensanchan, y si viajaran lo suficiente, se verían los resultados a pesar de su pequeña longitud de onda. Cuando se usa un láser bien enfocado a la luna, el haz se extenderá abarcando más de 100 metros de radio cuando alcance su superficie. Puede observarse éste utilizando un apuntador láser económico y un par de binoculares en una noche clara. En lugar de apuntar a la luna, se puede apuntar hacia una montaña distante o una estructura desocupada (como una torre de agua).

El radio de su haz va a incrementarse con la distancia. La línea visual que se necesita para tener una conexión inalámbrica óptima desde A hasta B es más que simplemente una línea delgada, su forma es más bien la de una elipse y su ancho puede ser descrito por medio del concepto de zonas de Fresnel.

## ○ Zona de Fresnel

El proceso de propagación de radio entre dos puntos se puede considerar como un “tubo” virtual donde la mayoría de la energía viaja entre el transmisor y receptor. Por lo que, para evitar pérdidas NO debería haber obstáculos dentro de una zona (región prohibida), porque un obstáculo alterará “el flujo de energía” (Hackerfriendly, 2008).

Por ejemplo, si la mitad de la zona prohibida está en mascarada (antena en el límite de la Línea de Vista (LoV o *Line of Sight LoS*), habrá una pérdida de energía de señal de 6 dB (pérdida de poder de 75%).

En la práctica en redes inalámbricas, un resultado aceptable debe ser mayor al 60% de la primera zona de Fresnel que esté libre. Aquí hay una fórmula para calcular la primera zona de Fresnel:

$$r = 17,31 * \sqrt{((d1*d2) / (f*d))}$$



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

$r$  es el radio de la primera zona en metros,  $d_1$  y  $d_2$  son las distancias desde el obstáculo a los extremos del enlace en metros,  $d$  es la distancia total del enlace en metros, y  $f$  es la frecuencia en MHz. Note que esta fórmula calcula el radio de la zona. Para calcular la altura sobre el terreno, se debe sustraer este resultado de una línea trazada directamente entre la cima de las dos torres.

Por ejemplo, calculando el tamaño de la primera zona de Fresnel en el medio de un enlace de 2 Km, transmitiendo a 2437 MHz (802.11b canal 6):

$$r = 17,31 \sqrt{((1000 * 1000) / (2437 * 2000))}$$
$$r = 17,31 \sqrt{1000000 / 4874000} r = 7,84 \text{ metros.}$$

Suponiendo que ambas torres tienen 10 metros de altura, la primera zona de Fresnel va a pasar justo a 2,16 metros sobre el nivel del suelo en medio del enlace. Pero ¿cuán alta puede ser una estructura en este punto para despejar el 60% de la primera zona?

$$r = 0,6 * 17,31 \sqrt{((1000 * 1000) / (2437 * 2000))}$$
$$r = 4,70 \text{ metros}$$

Restando el resultado de los 10 metros, se puede ver que una estructura de 5,30 metros de alto en el centro del enlace aún permite despejar el 60% de la primera zona de Fresnel. Esto es normalmente aceptable, pero en el caso de que hubiera una estructura más alta, habría que levantar más nuestras antenas o cambiar la dirección del enlace para evitar el obstáculo.

## ○ Potencia

Cualquier onda electromagnética contiene energía, o potencia, por ello se puede sentir cuando se disfruta del calor del sol. La potencia  $P$  es de una importancia clave para lograr que los enlaces inalámbricos funcionen: se necesita cierto mínimo de potencia para que el receptor le dé sentido a la señal.

El campo eléctrico se mide en V/m (diferencia de potencial por metro) y la potencia contenida en él es proporcional al campo eléctrico al cuadrado:

$$P \sim E^2$$

En la práctica, se mide la potencia por medio de algún tipo de receptor, por ejemplo, una antena y un voltímetro, un medidor de potencia, un



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

osciloscopio, o inclusive una tarjeta inalámbrica y una computadora portátil. La potencia es proporcional al cuadrado del voltaje de la señal.

## ○ Cálculo en dB

La técnica, sin duda, más importante para calcular la potencia es por decibeles (dB). No hay física nueva en esto, es solamente un método conveniente que hace que los cálculos sean muy simples.

El decibel es una unidad sin dimensión, esto es, que define la relación entre dos medidas de potencia. Se define como:

$$\text{dB} = 10 * \text{Log} (\text{P1} / \text{P0}) \text{ (Hackerfriendly, 2008)}$$

Donde P1 y P0 pueden ser dos valores cualesquiera que se van a comparar, normalmente, en este caso, se tratará de potencia. ¿Por qué es tan práctico el uso de decibeles? Muchos fenómenos de la naturaleza se comportan de una manera que se ha denominado exponencial. Por ejemplo, el oído humano escucha un sonido dos veces más fuerte que otro, si el primero tiene diez veces la intensidad física del segundo.

Otro ejemplo, muy relacionado con nuestro campo de interés, es el de la absorción. Por ejemplo, una pared en el camino de nuestro enlace inalámbrico, y cada metro de esa pared absorbe la mitad de la señal disponible. El resultado va a ser:

- metros = 1 (señal completa)
- metros = 1/2
- metros = 1/4
- metros = 1/8
- metros = 1/16 n metros =  $1/2^n = 2^{-n}$

Pero una vez que se ha aprendido cómo aplicar el logaritmo (log), las cosas son mucho más sencillas: en lugar de elevar un valor a la potencia n-ésima, se multiplica por n. En lugar de multiplicar valores, se pueden sumar. Aquí hay algunos valores utilizados comúnmente que es importante recordar:

- +3 dB = doble potencia
- -3 dB = potencia media



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- +10 dB = orden de magnitud (10 veces la potencia)
- -10 dB = un décimo de potencia

Además de los dBs adimensionales, hay cierto número de definiciones relacionadas que están basadas en una referencia P0 fija. Las más relevantes para el caso de las redes MESH son:

**dBm relativo a P0 = 1 mW dBi relativo a una antena isotrópica ideal**

Una antena isotrópica es una antena hipotética que distribuye uniformemente la potencia en todas direcciones. La antena que más se aproxima a este concepto es el dipolo, pero una antena isotrópica perfecta no puede ser construida en la realidad. El modelo isotrópico es útil para describir la ganancia de potencia relativa de una antena real.

Otra forma común (aunque menos conveniente) de expresar la potencia es en milivatios (miliwatts). En la Tabla 1.6 hay algunas equivalencias de niveles de potencia expresadas en miliwatts y dBm.

*Tabla 1.6. Conversión de decibelios a vatios.*

<b>dBm</b>	<b>Vatios</b>	<b>dBm</b>	<b>Vatios</b>	<b>dBm</b>	<b>Vatios</b>
1.	1.0 mW	17.	40 mW	33.	1.6 W
2.	1.3 mW	18.	50 mW	34.	2.0 W
3.	1.6 mW	19.	63 mW	35.	2.5 W
4.	2.0 mW	20.	79 mW	36.	3.2 W
5.	2.5 mW	21.	100 mW	37.	4.0 W
6.	3.2 mW	22.	126 mW	38.	5.0 W
7.	4 mW	23.	158 mW	39.	6.3 W
8.	5 mW	24.	200 mW	40.	8.0 W
9.	6 mW	25.	250 mW	41.	10 W
10.	8 mW	26.	316 mW	42.	13 W
11.	10 mW	27.	398 mW	43.	16 W
12.	13 mW	28.	500 mW	44.	20 W
13.	16 mW	29.	630 mW	45.	25 W
14.	20 mW	30.	800 mW	46.	32 W
15.	25 mW	31.	1.0 W	47.	40 W
16.	32 mW	32.	1.3 W	48.	50 W

*Fuente. elaboración propia.*



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ Patrón de radiación

El patrón de radiación es un gráfico o diagrama polar sobre el que se representa la fuerza de los campos electromagnéticos por una antena. Este patrón varía en función del modelo de antena. Las antenas direccionales representan un mayor alcance que las omnidireccionales.

Es la representación gráfica de la energía emitida o radiada de una antena, dicho de otra forma, es un gráfico que representa las propiedades direccionales de radiación de una antena en el espacio, y para representarla se usan generalmente dos formas, mostrando el patrón o modelo de elevación de la antena y mostrando el modelo de azimut, de la misma.

Ambos son gráficos que representan la energía radiada o emitida por la antena, sin embargo, el modelo de elevación (horizontal) nos muestra esta misma, pero de perfil; en cambio el patrón o modelo de azimut (vertical), muestra una vista directa desde arriba. La combinación de estas dos gráficas crea una representación tridimensional de cómo es realmente la energía emitida desde la antena (Figura 1.27)<sup>8</sup>.

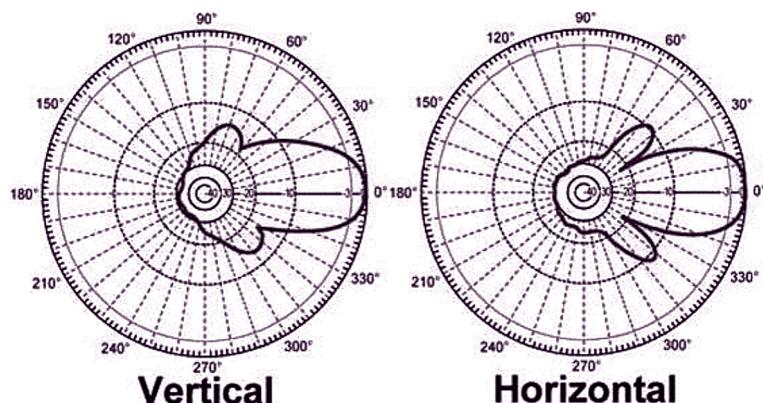


Figura 1.27. Representación de un patrón de radiación.

Fuente: Hoy, Diario Electrónico (2001-2016).

<sup>8</sup> Puede consultar el anexo D para más información sobre el patrón de radiación del nodo Fátima (Delgado, 2009).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## • 1.21 Contexto social de las redes MESH

Aunque no deja de ser un proyecto experimental, hoy en día es posible implementar tecnologías MESH para proporcionar servicios útiles a más de una persona, con el fin de que pueda aprovecharse un nodo en beneficio de un cualquier grupo interesado para este proyecto. Se resalta la capacidad de proporcionar ciertos elementos en común que permitan el desarrollo cultural e integral de las personas, por medio de conocimientos que pueden ser aprovechados vía inalámbrica.

Entre estos conocimientos se encuentra Wikipedia, un servidor *web* que contiene documentación y en lo posible, un servidor de archivos de video con contenido variado; este material, puede ser estudiado y analizado libremente gracias a las licencias libres de uso que permiten su manipulación e intercambio, para que todos puedan beneficiarse y aprender “libremente”.

### 1.21.1 Escenarios apropiados para un nodo MESH

Se tienen pensados tres escenarios inicialmente como modelos de aplicación:

#### ○ Colegio

En un colegio con bajos recursos, puede adquirirse la infraestructura necesaria para poner mínimo un nodo para dictar un cronograma de actividades que aprovechen sus recursos, siendo el mismo análisis de los recursos del nodo y el nodo en sí, propiedades útiles de estudio.

Mientras que niños de grados menores, pensado en cursos desde tercero de primaria hasta octavo de secundaria, podrían simplemente utilizar Wikipedia, documentos del servidor del nodo a modo de consulta rápida, entre otras cosas; alumnos de grados superiores pueden aprender recursos valiosos de capacitación como podría ser la implementación de servicios en red, diseño de una página *web*, programación en diversos lenguajes de programación como JavaScript, HTML, CSS entre otros, y aprender la capacidad de otros sistemas operativos aparte de Windows, como Linux y las diversas filosofías que rodean su administración, que dicho sea de paso, es aprender la utilidad de usar alternativas de manejo de sistemas.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano



Figura 1.28. Colegio Rafael Uribe Uribe, sede secundaria.

Fuente: elaboración propia.

Un trabajo muy interesante es el proyecto Edubuntu, una línea de aprendizaje basada en el proyecto Ubuntu, que provee conocimientos en pro de la educación de pequeños siendo una plataforma de manejo simple, pero muy eficaz para el desarrollo de nuevas sinergias de conocimiento.

Podría darse un ejemplo, albergando los archivos de instalación sin que tenga que reemplazarse el sistema inicial (recordando que un nodo puede manejarse y consultarse desde Windows o Linux o cualquier sistema, pero se sugiere Linux, al menos para el único servidor de trabajo para el nodo), usando un entorno rápido de virtualización como VirtualBox o VMware (como experiencia personal, el *software* de Oracle VirtualBox es mucho más eficaz y más cómodo para prácticas) con Edubuntu o cualquier *software* para aprender.

Es fundamental entender que todos estos documentos pueden ser implementados dependiendo de la capacidad del administrador, y que básicamente es un material introductorio para no representar una asignatura pesada de aprender, sino simplemente una lúdica agradable para disfrutar.

## ○ Universidad

Continuando rápidamente con la línea de aprendizaje sobre el entorno de redes MESH, podría implementarse un cronograma de estudios



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

mucho más elaborado, siendo importante resaltar las siguientes pautas, no necesariamente en el siguiente orden:

- Política de redes MESH.
- Infraestructura e Instalación.
- Introducción de redes.
- Introducción a servidores.
- Virtualización.
- Resolución de problemas.
- Programación, diseño y desarrollo web.
- Seguridad de recursos.
- Linux y BSD.
- Monitoreo y auditoría.

Estas son sólo sugerencias para guiar apropiadamente a futuros profesionales, quienes deben tener un manejo más allá del básico sobre diversos paradigmas y ser capaces de afrontar cualquier desafío en sus trabajos.

Si la universidad lo permite, sería ideal y muy apropiado establecer laboratorios prácticos de trabajo, implementando diferentes antenas con conexiones variadas y enlaces punto a punto, punto a multipunto y multipunto a multipunto; y proporcionando materiales como *routers*, cableado, antenas y obviamente equipos para trabajar apropiadamente los servicios.



Figura 1.29. Universidad Libre, sede Bosque Popular.

Fuente: elaboración propia.

## ○ Barrio

Al ser un entorno más personalizado en el barrio pueden compartirse determinados recursos, ya sea desde un ambiente casero o ir más



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

allá con recursos comunitarios, como puede ser una biblioteca o un salón comunal. En estos espacios, al ser de acceso libre para todas las personas que forman parte de la comunidad, pueden aprovecharse apropiadamente los recursos mencionados anteriormente, como Wikipedia, el cual es un sitio muy apropiado para aquellas personas que deseen realizar una consulta rápida sin tener que implementar, pagar o piratear innecesariamente en busca del derecho al conocimiento.



Figura 1.30. Barrio Fátima, dirección Calle 51 A sur # 37-65.

Fuente: elaboración propia.

## • 1.22 Manifiesto de las redes libres

Dado el estado actual de la red de redes, Internet, que es principalmente operada y controlada a nivel mundial por un pequeño número de corporaciones internacionales cuya motivación principal es meramente económica; y considerando las implicaciones que esto tiene en el curso que está tomando el desarrollo de la red de redes, los miembros y activistas de las redes libres manifiestan que una red libre es aquella red informática construida y administrada colaborativamente por sus propios usuarios y presenta como mínimo estas características:

- Garantiza la descentralización y evita la monopolización de recursos, la coerción o la opresión.
- Respeta la neutralidad de la red.
- Garantiza el acceso público y libre.
- Su estructura es de red distribuida; el crecimiento es posible desde cualquier punto existente.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- La interconexión se realiza entre pares que pueden publicar o recibir servicios y contenidos en igualdad de condiciones.
- Promueve la creación de otras redes libres, su interconexión e interoperabilidad.

### ○ **Estrategias y acciones comunes**

Priorizar la interacción con otros actores de la sociedad que promuevan el bien común. Por ejemplo, pero no limitándose a:

- Instituciones del sistema educativo y de salud.
- Organizaciones sociales formales o informales.
- Promover el intercambio de saberes necesarios para la apropiación social de las tecnologías que hacen posible la existencia de las redes libres.
- Utilizar *software* libre para la implementación de los diferentes componentes de la red. Cuando no existan alternativas libres, se promoverá su desarrollo.
- Promover el uso de licencias libres no sólo en materia de *software* sino también de cualquier producción amparada por el derecho de autor; tanto la documentación sobre el funcionamiento y administración de la red como la información que circule por ella debería poseer licencias que permitan su libre circulación.
- Defender el derecho a la libre circulación y acceso a la información y el conocimiento.
- Trabajar por conseguir la participación de las redes libres en los puntos neutros de las zonas donde se despliegan como estrategia para: ampliar su alcance, mejorar las posibilidades de interconexión entre redes libres y defender los principios de libertad, neutralidad y bien común dentro de la infraestructura de comunicaciones de su región.
- Llevar adelante acciones tendientes a lograr que los estados reconozcan la existencia de las redes libres y modifiquen las normativas pertinentes para facilitar su creación y expansión.
- Para facilitar la creación de redes libres, las legislaciones nacionales deberían contemplarlas como un actor de primer orden en la estructura de comunicaciones del país, considerando la importancia que su desarrollo representa para el bien común. La experiencia demuestra que las redes libres:



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Aumentan, en su área de cobertura, el nivel de acceso a las nuevas tecnologías, independientemente de la condición socioeconómica de la población.
- Representan una oportunidad única en áreas donde el despliegue de las redes de operadores tradicionales es económicamente inviable.
- En complemento con políticas de Estado de “inclusión digital”, las redes libres pueden proveer la capilaridad necesaria para que las acciones lleguen realmente a la población que más las necesita.

## ○ Lineamientos técnicos

Para mantener la estructura de red distribuida, deberá intentarse siempre mantener rutas redundantes entre los nodos que componen la red. Por lo que, es deseable que:

- Las redes provean números de IP fijos y un servicio interno de resolución de nombres de dominio.
- El ancho de banda sea simétrico.

## ○ Licencia - Localización del Pico - Peer Agreement

- *Tránsito libre*: el propietario acepta permitir el tránsito libre a través de su red libre. El propietario acuerda no modificar ni interferir con la información que circula por su red libre.
- *Comunicación abierta*. El propietario acuerda publicar la información necesaria para que la interconexión sea posible. La información deberá ser publicada bajo una licencia libre; y el propietario acepta estar disponible para ser contactado y proveerá al menos una dirección de correo electrónico.
- *Sin garantías no hay niveles de servicio garantizados*. El servicio es provisto “tal cual”, sin garantía o responsabilidad de ningún tipo. El servicio puede reducirse o desaparecer en cualquier momento sin notificación.
- *Términos de uso*. el propietario tiene derecho a formular una “política de uso aceptable”. Esta puede contener o no información sobre servicios adicionales provistos (aparte del acceso básico). El propietario es libre de formular esta política mientras no contradiga los puntos 1 a 3 de este acuerdo.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## • Conclusión

La fundamentación teórica de la red MESH vía conexión inalámbrica permite comprender el funcionamiento de los sistemas wifi y dimensionar la tendencia de transmisión de información en aquellas zonas comunitarias y rurales desprovistas de una infraestructura robusta en TIC.

( 2 )



## Construcción de un esquema para las infraestructuras de Redes MESH en entornos comunitarios o rurales de Colombia

### Introducción

Una vez conceptualizada la red MESH, se avanza con la presentación del esquema para la infraestructura que soporta la demanda de recursos de base tecnológica entre emisores y receptores, dirigiéndose a usuarios lejanos de centros o puntos de conexión a internet. Para este caso se muestra el diagrama de una red MESH total simple y una parcial. La total simple consiste en la conexión de un nodo con los demás y, la parcial, en conexión de algunos nodos. En cuanto al diseño, se aprecia el enlace punto a punto, punto a multipunto y multipunto a multipunto.

#### • 2.1 Diseño del esquema de red

El diseño se aborda en las características netamente físicas, congruentes con los requerimientos para su implementación dentro del funcionamiento integral de la red MESH como un esquema de aplicación regular en ambientes comunales.

##### ○ Diagrama de una red MESH

En la Figura 2.1 se puede observar cómo es el funcionamiento del envío de información entre la Fuente y el Destino, donde se escoge el mejor canal de comunicación para que la información se trasmite correctamente.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

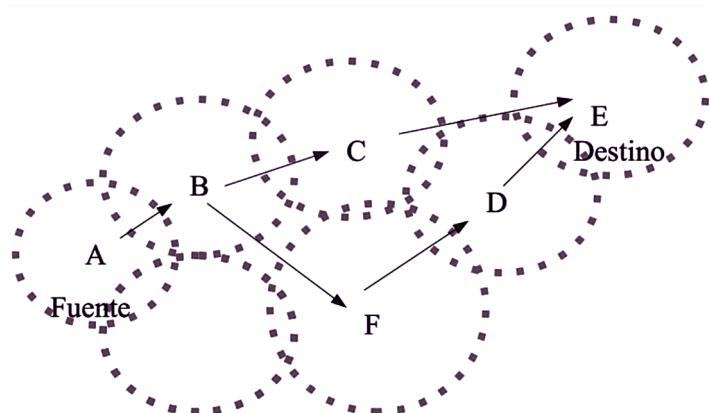


Figura 2.1. Modo de operación de una red MESH.

Fuente: Pérez (2010).

### ○ Diagrama de una red MESH total simple

Como se puede observar en la Figura 2.2, una red MESH total simple es aquella en la cual cada uno de los nodos se encuentran conectados con los demás nodos.

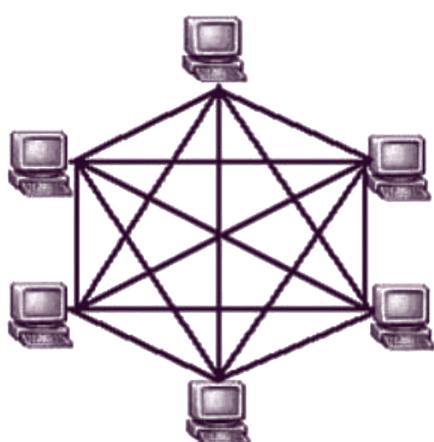


Figura 2.2. Diagrama de una red MESH Total Simple.

Fuente: Pérez (2011).

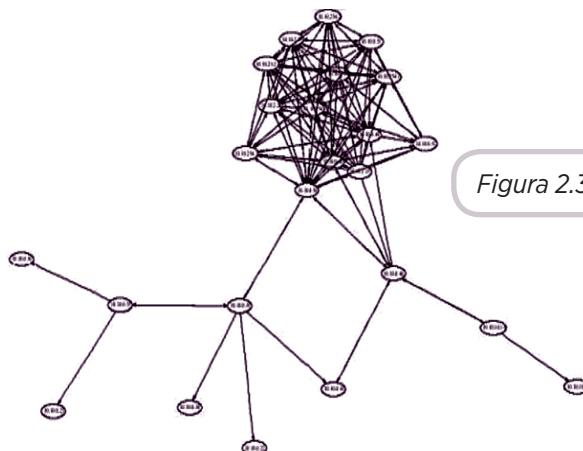
### ○ Diagrama de una red MESH Parcial

Como se puede observar en la Figura 2.3, una red MESH parcial es en la que los nodos no se encuentran conectados con todos los demás, sino



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

que por el contrario, algunos nodos se conectan a muchos y otros que se encuentran en los extremos, se conectan con pocos o realizan una única conexión.



Fuente: Pérez (2011).

## ○ Diseño de la red

El diseño de la red se encuentra clasificada en tres tipos:

- **Punto a punto:** los enlaces punto a punto generalmente se usan para conectarse a Internet donde dicho acceso no está disponible de otra forma (Figura 2.4). Uno de los lados del enlace punto a punto estará conectado a Internet, mientras que el otro utiliza el enlace para acceder al mismo.

El enlace punto a punto proporciona soluciones de conectividad para centros de trabajo múltiples que necesiten de una gran coordinación y trabajo compartido. Este enlace proporciona un entorno de intercambio de información con un coste periódico de cero, tan sólo la información. Es el complemento exterior perfecto a una instalación interior de red local estándar o inalámbrica.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

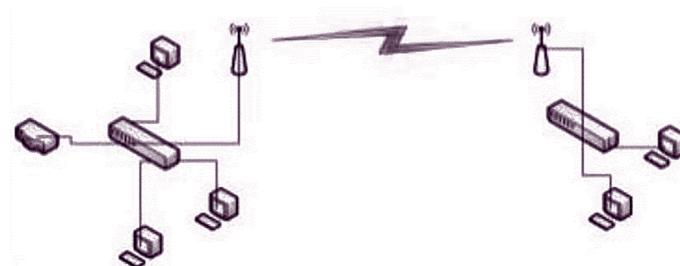


Figura 2.4. Esquema básico de conexión PTP.

Fuente: Pérez (2010).

Gracias a la potente antena o parrilla de emisión/recepción que utiliza un protocolo similar al de la red local inalámbrica, pero con un alcance extendido, pueden unirse mediante el enlace punto a punto centros situados hasta a 15 kilómetros. Esto proporciona los beneficios que supone compartir una red local con una velocidad de transferencia de 10 MB (megabytes) por segundo, sin ninguno de los costes ni problemas asociados a una interconexión estándar, que pueden ser la diferencia entre una instalación eficiente y con beneficios y una instalación caótica y en números rojos. Es la gran alternativa a las costosas y problemáticas líneas dedicadas de alta velocidad entre centros.

Existen tres tipos de enlaces que interconectan los nodos basándose en el sentido en que se transportan:

- *Simplex*: es la transacción que se realiza en un sólo sentido.
  - *Half-dúplex*: es la transacción que se realiza en ambos sentidos desde alguno de los nodos, siempre y cuando el emisor y el receptor no estén realizando funciones iguales.
  - *Full-dúplex*: es la transacción en la que se puede emitir y receptar simultáneamente.
- ◎ **Punto a multipunto:** el enlace punto a multipunto es la versión del punto a punto para la conexión rápida y fiable de más de dos instalaciones, donde varios nodos están hablando con un punto de acceso central (Figura 2.5).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

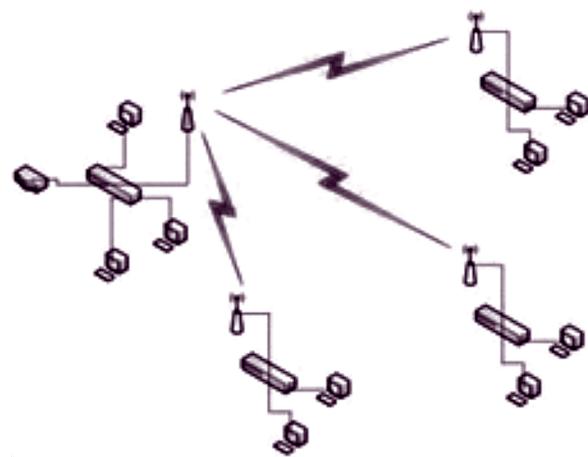


Figura 2.5. Esquema básico de enlace PMP.

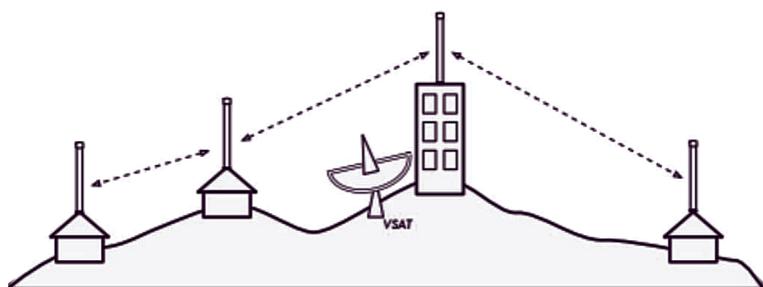
Fuente: Pérez (2011).

Para reducir costes, este sistema consta de una instalación central dotada de una antena multidireccional a la que apuntan las antenas direccionales del resto de centros. Esto brinda una capacidad igual a la del punto a punto, pero extensible hasta a 16 centros (incluso más, con instalaciones replicadas).

- **Multipunto a multipunto:** el tercer tipo de diseño de red es el multipunto a multipunto, el cual también es denominado red *ad hoc* o en malla (MESH). En una red multipunto a multipunto, no hay una autoridad central, cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí. El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí (Figura 2.6). Las buenas implementaciones de redes MESH son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red MESH es tan sencillo como agregar más nodos; si uno de los nodos en la “nube” tiene acceso a Internet, esa conexión puede ser compartida por todos los clientes.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano



*Figura 2.6. Esquema básico de una red en malla (MESH) multipunto a multipunto.*

*Fuente:* Pérez (201).

## • Conclusión

La infraestructura tecnológica mallada no requiere necesariamente de una conexión para su funcionamiento, precisamente, se contemplan las distancias de las comunidades y de la población rural como instrumento que ayuda a disminuir la brecha digital.

( 3 )



## Construcción de un esquema tecnológico para protocolos de enrutamiento en Redes MESH

### • Introducción

Los protocolos de enrutamiento determinan la transmisión de información, pueden ser reactivos o proactivos. Los reactivos se movilizan en tanto haya un estímulo, los proactivos, se mantienen y actualizan periódicamente según eventos basados en vectores de distancia y de estado en fase enlace. También se distinguen los híbridos que toman características de los dos anteriores.

### • 3.1 Diseño de la red

En este capítulo se presentará la comparación de los protocolos de enrutamiento: BABEL, HSLS, PWRP, BATMAN, BATMAN ADV, AODV y OLRS. Se tendrán en cuenta los siguientes parámetros: métrica de ruteo, alcance de transmisiones, tipo de protocolo y si es de uso libre o si tiene propietario.

#### ○ Métrica de ruteo

Teniendo en cuenta que un protocolo de enrutamiento aprende acerca de más de una ruta para llegar a un mismo destino, debe diferenciarlas y a través de la métrica se busca evaluar la ruta más conveniente para ello, con base en parámetros propios de cada protocolo. Así se observa si la métrica no es comparable y varía entre protocolos, de este modo se puede llegar a un mismo destino a través de dos rutas distintas.

Una métrica es una forma de evaluar cuál ruta es la óptima, teniendo en cuenta uno o varios parámetros como:



- OLSR usa el conteo entre saltos, prefiriendo rutas que impliquen menos saltos entre *routers*.
- AODV usa una combinación de ancho de banda y conteo de saltos.
- PWRP selecciona el camino óptimo, calculando los enlaces dinámicamente.
- BATMAN busca el próximo mejor vecino para cada destino.
- Babel y HWMP permiten combinar métricas y configurar, ya que no tienen determinadas.
- HSLS elimina los enlaces de baja calidad.

## ○ **Alcance de transmisiones**

Es importante identificar si se trata de un protocolo Unicast o Multicast:

- **Protocolo Unicast:** el envío de los datos se realiza en un sólo sentido a la vez (emisor - receptor), es decir que un nodo envía y puede recibir cuando ya ha terminado la transmisión. Ejemplo: AODV, OLSR y PWRP.
- **Protocolo Multicast:** el envío de datos se realiza de muchos a muchos, es decir, los datos se pueden enviar a múltiples destinos simultáneamente. Aquí podemos encontrar el protocolo GPSR, que entrega la información a un grupo de destinos en una red identificada por sus ubicaciones geográficas. Al determinar el método de transmisión, es posible que se utilicen simultáneamente los dos protocolos, y en ese sentido el Unicast y el Multicast, se combinen en un sistema de acceso múltiple, en el cual sería necesario establecer una primera de trasmisión de mensajes diferentes, y otra de mensaje idéntico. (Largo, Chen , & Qiang, 2017)

## ○ **Tipo de protocolo**

En los protocolos es importante determinar si se trata de un protocolo proactivo, reactivo o basado en la posición, para ello es importante tener en cuenta sus principales características:

- **Protocolos reactivos:** obtienen información de enrutamiento sólo cuando es necesario, el tiempo en establecer las conexiones es mayor que los protocolos proactivos, pero la sobrecarga de red es menor. Por ejemplo: AODV Ad-hoc On demand distance vector routing, apropiado para ajustarse a la necesidad del entorno, que opera bajo demanda, encamina salto a salto y usa horas lógicas para diferenciar información nueva de la antigua. (Perkins & Royer, 1999)



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- **Protocolos proactivos:** conocen exhaustivamente el estado de la red, así cuando necesitan una ruta esta ya se conoce y se encuentra lista para ser usada inmediatamente. En escenarios cambiantes el envío constante de mensajes para actualizar las tablas de enrutamiento sobrecarga la red. Por ejemplo: Babel, BATMAN, OLSR, OSPF y PWRP.
- **Protocolos híbridos:** utilizan las ventajas de cada uno de los protocolos anteriores, haciendo uso del encaminamiento proactivo cuando los nodos están cerca y el encaminamiento reactivo cuando los nodos están lejos, y cuando los caminos son utilizados en pocas ocasiones. Son los recomendados por el estándar 802.11s.  
En todo caso, el protocolo seleccionado debe contribuir no solo a mejorar el tráfico de la red, ya sea por un aumento de la demanda o por deficiencias de la movilidad (Peng & Sy, 2003)

## ○ **Tipos de licencias**

Las licencias de TORA y PWRP son propietarias, las otras son de uso libre.

### • **3.2 Análisis de protocolos de enrutamiento**

## ○ **OLSR (*Optimized Link State Routing*)**

- Son protocolos para redes *ad-hoc*.
- Protocolo de enrutamiento por estado de enlace.
- Utiliza la capa tres del modelo OSI (enlace de datos) para encontrar las rutas a través de toda la malla.
- Cada nodo envía un mensaje de saludo (*Hello*) en intervalos establecidos.
- Los nodos adyacentes reciben el mensaje (*Hello*), comparan el mapa de red con el mensaje para detectar un cambio en la ruta, si dicho cambio existe se procede a transmitir a los vecinos un mensaje TC (cambio de topología).
- Cada vez que llega un mensaje TC se debe volver a calcular toda la topología de la red; así cada nodo sabrá enrutar cada paquete, usando su nueva tabla de enrutamiento actualizada.
- Se basa en el algoritmo de Dijkstra usando una métrica ETX (*Expected Transmission Count*) para establecer los caminos.
- Opera en modo distribuido, la carga del tráfico se reparte en varios nodos inalámbricos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

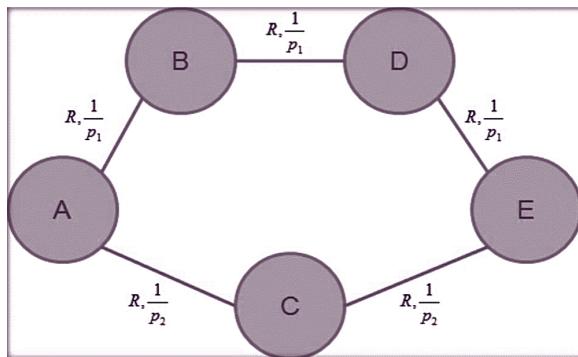


Figura 3.1. ETX routing metric: OLSR-ETX.

Fuente: Hussein (2010).

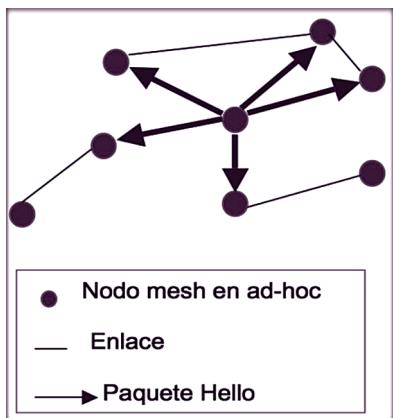


Figura 3.2. Propagación del paquete hello generado por OLSR.

Fuente: elaboración propia.

El OLSR es un protocolo proactivo, debido a ello utiliza la red para el envío de los mensajes; lo cual, a medida que se incrementan los números de nodos cambia la topología y, por ende, aumenta el tráfico de mensajes cogestionando la red y originando la pérdida de paquetes.

Como en cada nodo se hace el cálculo total de la ruta hacia otros nodos, debido al conocimiento de la topología de la red, el funcionamiento es descentralizado, lo cual trae un alto procesamiento en cada nodo.

## ○ AODV (Ad-Hoc On Demand Distance Vector)

- Protocolo de enrutamiento IP, el cual consiste en que los nodos pueden encontrar y almacenar rutas hacia otros nodos en la red.



- Es *on-demand*, o reactivo, es decir las rutas son por demandas, se establecen sólo cuando se requieren.
- Las decisiones de enrutamiento se establecen utilizando vectores de distancia, las cuales se miden en saltos entre los *routers* de la red.
- En el nodo se tiene un número de secuencia (*timestamp*), el cual se utiliza para determinar las rutas actuales; se determina por el número mayor y se descartan los más antiguos en la tabla de enrutamiento.
- Cada ruta activa tiene un tiempo de disponibilidad en la tabla de enrutamiento, cuando este tiempo se termina se elimina de la tabla la ruta.
- Tiene un procedimiento de descubrimiento de rutas, si el nodo origen requiere la ruta de un nodo destino, envía por *broadcast* un mensaje, y de esta manera se establecen las rutas entre nodos.
- Otro procedimiento es el de mantenimiento de rutas, el cual proporciona una retroalimentación al requerimiento de una ruta, en caso de que un enlace o un *router* se dañe o pierda, de esta forma la ruta se modifica o se redescubre.
- El uso de tablas de enrutamiento en cada nodo evita que los paquetes lleven dichas rutas.
- En cada nodo no se mantienen rutas, las rutas se obtienen de acuerdo a la necesidad, ya sea porque se activen o se desactiven.
- Este protocolo puede realizar tres tipos de transmisión: Unicast: envía datos de un nodo a otro. Multicast: envía datos de un nodo a un grupo de nodos. Broadcast: envía datos de un nodo a los demás nodos de la red.
- Para encontrar una ruta se realiza bajo demanda y se hace utilizando un ciclo de petición/respuesta de ruta, estas peticiones son enviadas por medio de un paquete llamado RREQ (*Route Request*) y las respuestas por medio del paquete RREP (*Route Reply*), el resumen de las secuencias para encontrar una ruta son las siguientes:
  - Para conocer la ruta de un nodo origen hacia un nodo destino, se utiliza vía *broadcast* un RREQ.
  - Los nodos que conocen unas rutas hacia un destino solicitado contestan enviando un RREP, la información retorna hasta el nodo origen del RREQ y actualiza las rutas de los nodos que lo necesiten.
  - La información que se reciben en el nodo del RREP, se almacena en la tabla de enrutamiento del nodo.

Una de las ventajas de este protocolo es la disminución del tiempo para el enrutamiento de los paquetes y que trabaja bajo demanda.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

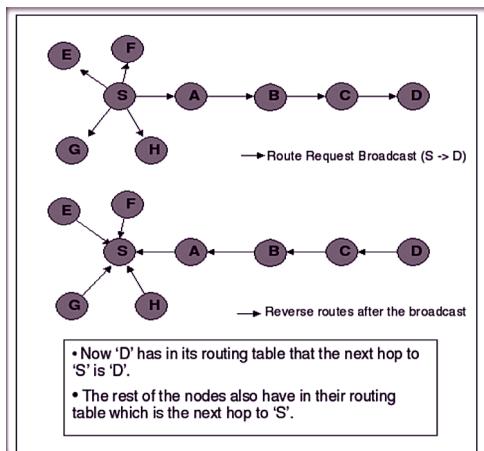


Figura 3.3. Route Request.

Fuente: Paulus (2013).

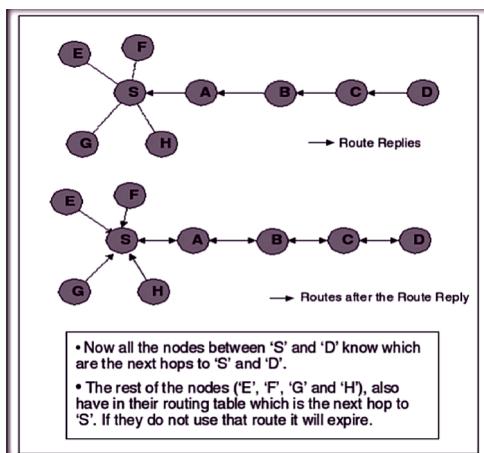


Figura 3.4. Route Reply.

Fuente: Paulus (2013).

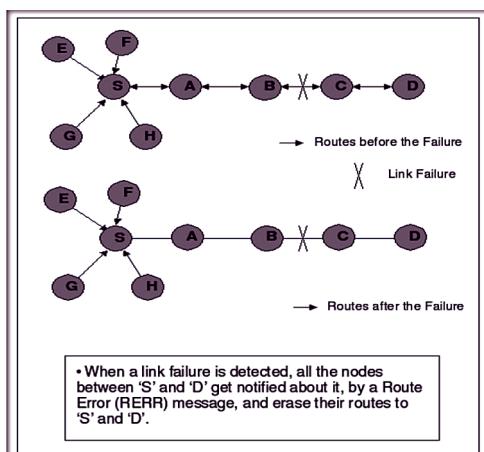


Figura 3.5. Router Error.

Fuente: Paulus (2013).



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ HSLS (*Hazy Sighted Link State Routing Protocol*)

Este protocolo de enrutamiento trabaja con vista confusa del estado de enlace, es decir que los enlaces de baja calidad los elimina. Es tanto proactivo como reactivo, ya que envía los mensajes de actualización en un determinado tiempo y espacio.

Se recomienda el uso del protocolo para redes que estén compuestos por más de mil nodos.

## ○ BATMAN (*Mobile Ad-hoc Networks MANETs*)

Este es un protocolo de enrutamiento proactivo para Redes MESH *Ad-Hoc*. Mantiene proactivamente la información sobre la existencia de todos los nodos en la red MESH, que son accesibles con unas comunicaciones de un solo salto o de múltiples saltos.

Determina para cada nodo destino un único salto vecino, el cual será usado como la mejor puerta de enlace para comunicarse con el nodo destino y no requiere calcular la ruta completa, por ello la comunicación es rápida y eficiente. Además, realiza el análisis estadístico de la pérdida de paquetes del protocolo y la velocidad de propagación y no depende del estado o topología de la información de otros dispositivos.

Las decisiones de enrutamiento son basadas en el conocimiento de la existencia o la falta de información. Los paquetes contienen una cantidad limitada de información, es por ello por lo que son pequeños.

Este protocolo fue diseñado en función de medios poco fiables que, si bien experimentan altos niveles de inestabilidad y de pérdida de datos, fue concebido para contrarrestar los efectos de las fluctuaciones de una red y compensar su inestabilidad, permitiendo así un alto nivel de robustez.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano



Figura 3.6. Formatos del paquete general BATMAN.

Fuente: Tiwari (2013).

## ○ PWRP (*Predictive Wireless Routing Protocol*)

Protocolo de enrutamiento inalámbrico y dinámico que permite que los *routers* de malla realicen mediciones de extremo a extremo de la calidad de la ruta y las utilicen para tomar decisiones de enrutamiento cuyo resultado es un rendimiento máximo. Se basa en algoritmos patentados de enrutamiento que maximizan el rendimiento y la resistencia de las redes inalámbricas de malla.

La red se puede ampliar con rapidez mediante *routers* móviles de la misma línea de productos. Utiliza algoritmos patentados para optimizar de forma continua y dinámica el uso del espectro disponible como:

- **PowerCurve™:** este algoritmo distribuido aumenta o disminuye dinámicamente los niveles de potencia de transmisión y adapta las tasas de datos de enlace para mantener la fiabilidad de cada enlace inalámbrico y maximizar el número de enlaces simultáneos. Evita, por ejemplo, que los *routers* “fuertes” ahoguen las “conversaciones” cercanas.
- **Airtime Congestion Control™ (ACC):** ACC se ha diseñado para facilitar un rendimiento uniforme a un gran número de usuarios, especialmente en redes muy saturadas, superando de este modo una deficiencia conocida de 802.11 MAC.
- **Inmunidad al ruido adaptativa (ANI):** ajusta los parámetros de detección de paquetes a nivel de chip en tiempo real, para minimizar los sucesos de detección en falso y maximizar la sensibilidad del receptor.
- **PWRP:** fue creado para enrutamiento a través de redes de malla, los nodos de la red se pueden mover o se apaga. Esta es la razón por la cual PWRP abandona la base de datos de enrutamiento, generalmente utilizado por los protocolos de enrutamiento.



## ○ **Babel (A loop-free distance-vector routing protocol)**

Está basado en el algoritmo vector de distancias y diseñado para ser robusto y eficiente tanto en redes cableadas como en redes inalámbricas malladas.

Se origina sobre las ideas de *Destination-Sequenced Distance Vector routing* (DSDV) y *Ad hoc On-Demand Distance Vector Routing* (AODV). Funciona con IPv4 e IPv6 y fue diseñado, en un principio, para redes inalámbricas *ad-hoc*, por lo que es un protocolo muy robusto en presencia de nodos móviles, impidiendo la formación de bucles sin fin y ofreciendo una rápida convergencia.

Está basado en el algoritmo de Bellman-Ford, al que incorpora ciertos refinamientos que previenen la formación de bucles o, al menos, aseguran que un bucle desaparecerá después de un cierto tiempo y no volverá a aparecer.

El funcionamiento y formatos de los paquetes de Babel se dividen en cinco tipos:

- **Nodos e interfaces:** igual que BATMAN, Babel distingue entre nodos e interfaces. Un nodo puede tener más de una interfaz formando parte de la red.
- **Métrica:** Babel se basa en la calidad de los enlaces entre nodos para calcular la métrica de una ruta. Se define el coste de un enlace entre A y B como C(A, B) y la métrica de A hacia un destino S como D(A). Para determinar estas métricas se utilizan dos tipos de paquetes: Hello y IHU (I Heard yoU).
- **Algoritmo de Bellman-Ford:** este algoritmo calcula la ruta más corta entre dos nodos en un grafo dirigido y ponderado. Babel se basa en él para el cálculo de rutas. El algoritmo se ejecuta en paralelo para cada nodo, calculando las distancias a los demás nodos de la red. Para la explicación teórica que sigue, se define un nodo destino S de referencia para el que se calculará la distancia mínima.
- **Condición de viabilidad:** cuando el enlace entre dos nodos vecinos se rompe, pueden crearse bucles en la actualización de rutas. Para evitar esto, se define la condición de viabilidad como aquella que permite a un nodo rechazar un anuncio de ruta por parte de otro nodo, si dicho anuncio puede crear un bucle sin fin. Las condiciones de viabilidad pueden ser muy diversas.



- Números de secuencia: Babel utiliza números de secuencia para las rutas, una solución introducida por DSDV y AODV. Además de la métrica, cada ruta transporta un número de secuencia, un número entero no decreciente que se propaga inalterado por toda la red. El único que puede incrementar el número de secuencia es el nodo origen. El par (métrica, númer. secuencia) se conoce como distancia. De esta forma, se puede saber si la información recibida sobre una ruta es nueva o antigua.

### • 3.3 Métrica para evaluar los protocolos propuestos

De acuerdo con las comparaciones realizadas en los protocolos de enrutamiento, se propone como esquema de evaluación basada en los siguientes elementos:

#### ○ Cálculo de rutas

- Métrica de ruteo:
  - Número de saltos.
  - Tráfico enviado y recibido.
  - Tiempo requerido para describir una ruta.
  - Número total solicitudes de rutas enviadas.
  - Número total solicitudes de rutas recibidas.
  - Tráfico de control recibido y enviado.
  - Tráfico de datos recibido y enviado.
  - Intentos de retransmisión.
  - Potencia promedio.
  - RTT (Round-Trip Time): tiempo de ida y vuelta.
  - Rendimiento (*Throughput*).
  - Alcance de transmisiones o tipo de protocolo.
  - Si es de uso libre o si es propietario.

#### • Conclusión

Cada protocolo de enrutamiento presenta ventajas y desventajas que se tienen en cuenta en el diseño e implementación de una red MESH. Este determinará la transmisión de información de origen a destino con el menor número de saltos entre dispositivos.

( 4 )



## Diseño de una arquitectura de seguridad para Redes MESH en entornos comunitarios o rurales de Colombia

### • Introducción

Los protocolos de seguridad están presentes en el diseño e implementación de redes MESH. Es por esto por lo que se presentan numerosas alternativas que minimicen los riesgos pasivos y activos que se pueden presentar en una red inalámbrica y ofrecer a los usuarios la confianza y tranquilidad de un entorno seguro.

### • 4.1 Diseño de la red

Al momento de reconocer la mejor alternativa para brindar seguridad a las redes MESH, es necesario conocer las características, ventajas y desventajas de los protocolos de seguridad en redes MESH.

### • 4.2 WEP (*Wired Equivalent Privacy - Privacidad Equivalente al Cable*)

#### ○ Características

- WEP cifra los datos en su red, de forma que sólo el destinatario deseado pueda acceder a ellos.
- Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP.
- WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.



- Cuanto más larga sea la clave, más fuerte será el cifrado.
- WEP utiliza RC4 como algoritmo de cifrado.
- En WEP se usan claves de 64 o 128 bits (40+24 o 104+24).
- Cada paquete cifrado, contiene un IV sin cifrar y el bloque de datos cifrado, el cual, a su vez, contiene un CRC32 (cifrado) para comprobar integridad.
- El algoritmo WEP forma parte de la especificación 802.11 y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado.
- WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia se unifica con el mensaje mediante una operación XOR, para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial, a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo).

El algoritmo WEP10 forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

Este algoritmo cifra de la siguiente manera:

Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red, lo cual genera



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de las ocasiones, que la clave se cambie poco o nunca.

Este algoritmo está diseñado para proveer autenticación de usuarios, privacidad de datos e integridad de datos en una forma equivalente a una red cableada LAN. Se encarga de cifrar la información que se va a transmitir entre dos puntos, de forma que sólo le sea posible tener acceso a los nodos e interpretarlos a aquellos puntos que tengan la misma clave, mediante tres tipos de clave:

- Clave WEP de 64 bits: 5 caracteres o 10 dígitos hexadecimales (0-9 A-F, precedidos por la cadena ox).
- Clave WP 128 Bits: 13 caracteres o 26 dígitos hexadecimales.
- Clave WEP 256: 29 caracteres o 58 dígitos hexadecimales.

## ○ Ventajas

- La activación del cifrado WEP de 128 bits evitara que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad.
- WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.
- Compatibilidad entre distintos fabricantes.
- Pueden proporcionar niveles de seguridad todavía más altos. La implantación de éstos y de otros métodos de autorización y encriptación garantizan que la seguridad en las redes WLAN sea igual o incluso, superior a la de las tecnologías LAN convencionales.
- Es uno de los algoritmos más empleados, ya que viene como medida de seguridad básica en las tarjetas inalámbricas.
- Tiene la ventaja de que todos los dispositivos lo pueden implementar.
- Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autenticación y control de acceso en redes WLAN.
- Protege las comunicaciones inalámbricas contra ataques de intrusos y previene de acceso no autorizado a una red inalámbrica.
- Para descifrar la clave es necesario un tráfico interrumpido de datos durante un tiempo determinado (por cierto, bastantes datos y bastante tiempo).



## ○ Desventajas

- Sistemas de clave.
- Sistema de integridad.
- *Sniffing*.
- Identificación de estaciones.
- Vector inicial (IV).
- Las claves de cifrado estáticas son pocas veces cambiadas permitiendo que el atacante obtenga varias veces el mismo texto de cifrado.
- No ofrece servicio de autenticación.
- Existen varias herramientas que pueden permitir romper la clave secreta.
- Es probable que el IV que se asigna se repita aproximadamente 5 horas en redes de alto tráfico.
- Nuestro ICV viaja en texto plano hasta el momento en que se realiza el cifrado completo, tiempo suficiente como capturar los paquetes necesarios y atacar la red.
- Permitiendo mediante *software* ‘piratear’ la clave.
- El principal problema con la implementación del algoritmo anteriormente descrito es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto, es inseguro debido a su implementación.
- Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.
- Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros).
- WEP no ofrece servicio de autenticación.
- El cliente no puede autenticar a la red o al contrario; basta con que el equipo móvil y el punto de acceso comparten la clave WEP para que la comunicación pueda llevarse a cabo.
- Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP.
- El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl, diseñados para analizar un archivo de captura de paquetes de un *sniffer*.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- La herramienta AirSnort hace lo mismo, pero integra las funciones de *sniffer* y rompedor de clave y, por lo tanto, es más fácil de usar.
- Se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (*Integrity Check Value*) un algoritmo diseñado para tal fin como SHA1-HMAC.
- WEP no incluye autentificación de usuarios. Lo máximo que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso se tendría una autentificación de sistema abierto.
- El algoritmo RC4 es susceptible a ataques de fuerza bruta.
- El manejo de las llaves no está especificado y sin un manejo de llaves, estas permanecen útiles durante mucho tiempo. La mayoría de los usuarios del WEP tienen una sola llave compartida con cada nodo de la red; el punto de acceso y los clientes deben estar programados con la misma llave.
- El vector de inicialización es muy pequeño.
- La encriptación WEP de 256 bits no es soportada por muchos dispositivos, aunque una clave de encriptación se puede descifrar (existen programas para ello).

#### • 4.3 WPA (*Wi-Fi Protected Access, Acceso Protegido Wi-Fi*)

##### ○ Características

- WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP, mientras 802.11i era finalizado.
- Sistemas operativos: Windows 98/ME/2000/XP y Linux.
- Utiliza los protocolos: EAP-TLS, PEAP, EAP-TTLS para autenticar al usuario.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- ◎ Método de trabajo: claves dinámicas.
- ◎ Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autenticación.
- ◎ WPA propone un nuevo protocolo para cifrado, conocido como TKIP (*Temporary Key Integrity Protocol*). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente, se mejoraron los algoritmos de cifrado de trama, con respecto a WEP.
- ◎ WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP.
- ◎ Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autenticación.

## ○ **Tecnologías**

- ◎ IEEE 802.1X: estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un *switch*, pero también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).
- ◎ EAP: EAP, definido en la RFC 2284, es el protocolo de autenticación extensible para llevar a cabo las tareas de autenticación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X, bajo el nombre de EAPOL (*EAP over LAN*). TKIP (*Temporal Key Integrity Protocol*), según indica Wi-Fi, es el protocolo



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

encargado de la generación de la clave para cada trama. MIC (*Message Integrity Code*) o Michael, es el código que verifica la integridad de los datos de las tramas.

Basada en servidores de autenticación (normalmente servidores Radius (*Remote Authentication Dial-In User Server*), en la que es el servidor de autenticación es el encargado de distribuir claves diferentes entre los usuarios. Usa un protocolo TKIP (*Temporal Key Integrity Protocol*) que cambia la clave de encriptación dinámicamente, a medida que se utiliza dicha conexión.

## ○ Ventajas

- Busca subsanar los problemas de la encriptación WEP.
- Establece nuevos protocolos para cambiar clave compartida entre AP y cliente cada cierto tiempo.
- Permite trabajar en dos modalidades caseras y corporativas.
- La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la *Wi-Fi Alliance* a partir de finales de 2003. Según la *Wi-Fi Alliance*, todo equipo de red inalámbrica que posea el sello *Wi-Fi Certified* podrá ser actualizado por software para que cumpla con la especificación WPA.
- WPA es considerado uno de los más altos niveles de seguridad inalámbrica para red, es el método recomendado si el dispositivo es compatible con este tipo de cifrado.
- No se necesita ningún conocimiento ni experiencia técnica y no es necesario introducir manualmente una contraseña, ni clave asociada con una configuración de seguridad tradicional inalámbrica.
- WPA soluciona la debilidad del vector de inicialización (IV) de WEP, mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar  $2^{48}$  combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).
- Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Las claves ahora son generadas dinámicamente y distribuidas de forma automática, por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.
- Para la autenticación, se sustituye el mecanismo de autenticación de secreto compartido de WEP, así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.
- Las claves dinámicas o las autenticaciones las hace mediante claves generadas por el sistema, que además no se repiten.

## ○ **Desventajas**

- Resulta que si las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque de diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red. Esta debilidad se resuelve fácilmente, empleando claves largas.
- No todos los dispositivos son capaces de implementarlo.
- No todas las tarjetas inalámbricas son compatibles con este estándar.
- Su manejo aún no es altamente conocido.
- WPA se considera una solución provisional y no cumple la norma IEEE 802.11i.
- El mayor inconveniente es que no son muchos los dispositivos WIFI que la soportan.

## • **4.4 WPA2 (802.11i)**

## ○ **Características**

- WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de “migración”, no incluye todas las características del IEEE 802.11i, mientras que WPA2, se puede inferir que es la versión certificada del estándar 802.11i.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Sistemas operativos: Windows 98/ME/2000/XP y Linux.
- Método de Autenticación: utiliza el estándar de encriptación AES.
- WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requiere un *hardware* potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.
- Una vez se ha verificado la autenticidad del usuario, el servidor de autentificación crea una pareja de claves maestras (PMK) que se distribuyen entre el punto de acceso y el cliente, y éstas se utilizarán durante la sesión del usuario. La distribución de las claves se realizará mediante los algoritmos de encriptación correspondientes TKIP o AES con las que se protegerá el tráfico entre el cliente y el punto de acceso.
- WPA2 utiliza el modo de Contador con *Cipher Block Chaining* Mensaje Protocolo de Autenticación de Código (CCMP) y *Advanced Encryption Standard* (AES). CCMP también utiliza cifrado por paquete, sino que utiliza el AES con un máximo de una clave de cifrado de 256 bits, que es considerablemente más seguro que RC4.
- Una estación inalámbrica solicita abrir una sesión con el punto de acceso, entre ambos extremos se establece una clave denominada *Pairwise Master Key* (PMK). Para ello, se utiliza típicamente el estándar LAN y WLAN 802.1x, que permite al responsable de seguridad aplicar un método de autenticación tan potente como desee, desde las simples combinaciones usuario/contraseña hasta certificados digitales.

## ○ Ventajas

- WPA2 está idealmente pensado para empresas, tanto del sector privado como del público.
- Los productos que son certificados para WPA2 les dan a los gerentes de TI la seguridad que la tecnología cumple con estándares de interoperabilidad" declaró Frank Hazlik Managing director de la Wi-Fi Alliance.
- Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo con lo establecido en el estándar 802.11i



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.
- Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes *ad-hoc*).
- Para la encriptación se utiliza un algoritmo mejor que el TKIP, concretamente el AES. En el modo Enterprise el sistema trabaja gestionada mente asignando a cada usuario una única clave de identificación, lo que proporciona un alto nivel de seguridad.
- Permite equipos más antiguos utilizar el cifrado por paquete la red utiliza una clave de 40 bits o 128 bits que sólo cambió cuando el usuario cambia el código de acceso.
- Introdujo cifrado por paquetes, lo que significa que cada paquete utiliza una clave generada especialmente para ese paquete.
- Reduce considerablemente la complejidad y el tiempo de *roaming* de los usuarios de un punto de acceso a otro.
- El estándar 802.11i elimina muchas de las debilidades de sus predecesores tanto en el lo que autenticación de usuarios como a robustez de los métodos de encriptación se refiere. Y lo consigue en el primer caso gracias a su capacidad para trabajar en colaboración con 802.1x y en el segundo, mediante la incorporación de encriptación *Advanced Encryption Standard* (AES).

## ○ Desventajas

- Los dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.
- Una de las vulnerabilidades más conocidas es el ataque a la clave PSK, ya que toda la información da la red va en formato texto y se transmite cuando un usuario se autentifica en el conocido 4-handshake. Esta vulnerabilidad se puede explotar con ataques por diccionarios o por fuerza bruta, donde el procedimiento es básicamente el mismo, se va comparando múltiples claves con la suma de chequeo del handshake, una vez que la coincidencia se logra, la red está al descubierto.
- Con contraseñas sencillas se puede obtener clave por ataque de diccionario Con una gran potencia de cálculo de CPU, se puede obtener por fuerza bruta.
- No se puede controlar el área de cobertura de una conexión.
- No todos los dispositivos WIFI admiten este tipo de encriptación, que además presenta una serie de inconvenientes.



## • 4.5 SSH (**Secure Shell**)

### ○ Características

- Disponibilidad en la mayor parte de los servidores (pero, si no estuviera disponible, además es sencillo habilitarlo). Por otro lado, SSH es el único protocolo de red con el que se puede fácilmente tanto leer como escribir.
- Los datos que circulan entre el cliente y el servidor están cifrados y esto garantiza su confidencialidad (nadie más que el servidor y el cliente pueden leer la información que se envía a través de la red). Como resultado, no es posible controlar la red con un rastreador.
- El cliente y el servidor se autentifican uno a otro para asegurarse que las dos máquinas que se comunican son, de hecho, aquellas que las partes creen que son. El *hacker* ya no puede adoptar la identidad del cliente o de su servidor (falsificación).
- Una conexión SSH se establece en varias fases: En primera instancia, se determina la identidad entre el servidor y el cliente para establecer un canal seguro (capa segura de transporte). En segunda instancia, el cliente inicia sesión en el servidor.
- SSH es un protocolo para iniciar sesiones en máquinas remotas que ofrecen autenticación, confidencialidad e integridad.
- SSH es una herramienta que permite realizar conexiones seguras entre equipos unidos mediante una red insegura, como puede ser Internet. Utiliza el puerto 22 y sigue el modelo cliente-servidor.
- La seguridad de SSH se basa en la utilización de mecanismo de criptografía, de forma que toda transmisión de información es cifrada y el mecanismo de autenticación es transparente al usuario.
- Protocolo utilizado para *login* y ejecución de procesos remotos.
- Es una herramienta de administración remota que permite la conexión segura entre equipos unidos mediante una red insegura como por ejemplo Internet. Utiliza el puerto 22 y sigue el modelo cliente-servidor. La aportación más importante es que da soporte seguro a cualquier protocolo que funcione sobre TCP. Dicha seguridad se basa en la utilización de mecanismo de criptografía. Se suele utilizar como medida de seguridad para sustituir las típicas ordenes de comunicaciones como telnet, login, rsh, rcp o ftp. Funciona sobre la mayoría de las distribuciones Unix/Linux, y hay versiones para Windows y MacOs.



- ◎ Soporta una variedad más amplia:
  - *Public-key* (RSA only) de clave pública (RSA solamente) *RhostsRSA*.
  - *Password/contraseña*.
  - *Rhosts* (*rsh-style*)/ *Rhosts* (*rsh-estilo*).
  - TIS Kerberos103.
- ◎ El cliente puede verificar que se está conectado a un mismo servidor por:
  - Información de autenticación encriptada con 128 bits.
  - Datos enviados y recibidos encriptados con 128 bits.
- ◎ Posibilidad de enviar aplicaciones lanzadas desde el intérprete de comandos (reenvío por X11).
- ◎ Sirve para el inicio de sesión remoto seguro y otros servicios de red seguros a través de una red no segura. Proporciona soporte para el inicio de sesión remoto seguro, la transferencia segura de archivos o el reenvío seguro de tráfico de sistemas TCP/IP y X Windows.

## ○ Ventajas

- ◎ SSH es el mecanismo de autenticación, sencillo de habilitar y de usar.
- ◎ El uso de SSH tiene múltiples ventajas. En primer lugar, se necesita usarlo si se quiere un acceso de escritura autenticado a su repositorio. En segundo lugar, SSH es sencillo de habilitar. Los demonios (*daemons*) SSH son de uso común, muchos administradores de red tienen experiencia con ellos y muchas distribuciones del SO los traen predefinidos o tienen herramientas para gestionarlos. Además, el acceso a través de SSH es seguro, estando todas las transferencias encriptadas y autenticadas. Y, por último, al igual que los protocolos Git y Local, SSH es eficiente, comprimiendo los datos lo más posible antes de transferirlos.
- ◎ Es un protocolo que hace posible que un cliente (un usuario o incluso un equipo) abra una sesión interactiva en una máquina remota (servidor) para enviar comandos o archivos a través de un canal seguro.
- ◎ Posibilita a sus usuarios (o servicios TCP/IP) acceder a un equipo a través de una comunicación cifrada (llamada túnel).
- ◎ Todos los datos que se envían y se reciben durante la conexión son cifrados.
- ◎ El cliente puede ejecutar aplicaciones gráficas desde el Shell.
- ◎ Iniciar sesiones *login* en servidores remotos, ejecutar comandos remotamente, copiar archivos entre distintos *hosts*, ejecutar aplicaciones



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

remotamente, realizar túneles IP cifrados. Brinda comunicaciones seguras (cifradas) entre el cliente y el servidor.

- Después de la primera conexión, el cliente puede saber que está conectando al mismo servidor en futuras sesiones.
- El cliente puede transmitir al servidor usuario y contraseña en formato cifrado.
- Todos los datos que se envían o reciben en la conexión son cifrados. El cliente puede ejecutar aplicaciones gráficas desde el Shell (intérprete de órdenes) de forma segura (reenvió por X11).
- Es posible la interceptación de la comunicación entre dos sistemas por parte de una tercera máquina.
- Interceptación de la comunicación entre dos sistemas: un tercero en algún lugar de la red entre entidades en comunicación hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información, o puede modificar la información y luego enviarla al recipiente al cual estaba destinada.
- Personificación de un determinado *host*: un sistema interceptor finge ser el receptor a quien está destinado un mensaje. Si funciona la estrategia, el cliente no se da cuenta del engaño y continúa la comunicación con el interceptor como si su mensaje hubiese llegado a su destino satisfactoriamente.
- Puede cifrar, autenticar y comprimir de forma automática los datos trasmisidos.

## ○ Desventajas

- El aspecto negativo de SSH es su imposibilidad para dar acceso anónimo al repositorio. Todos han de tener configurado un acceso SSH al servidor, incluso aunque sea con permisos de sólo lectura; lo que no lo hace recomendable para soportar proyectos abiertos. Si se usa únicamente dentro de su red corporativa, posiblemente sea SSH el único protocolo que tenga que emplear. Pero si se quiere también habilitar accesos anónimos de sólo lectura, se tendrá que reservar SSH para sus envíos (*push*) y habilitar algún otro protocolo para las recuperaciones (*pull*) de los demás.
- La gran desventaja de transmitir el intercambio de información en texto plano en la red, en particular, el nombre de acceso y la contraseña para acceder a equipos remotos. Tal es así, que un *hacker* que se encuentre ubicado en una red entre el usuario y un equipo



remoto puede controlar el tráfico, es decir, utilizar una herramienta llamada rastreador que puede capturar paquetes que circulan en la red y obtener el nombre de acceso y la contraseña para acceder al equipo remoto.

- ◉ La transmisión entre cliente y el servidor se realiza completamente en texto plano (sin cifrar), por lo que con cualquier *sniffer* es posible capturar tramas y obtener de ellas *login* y la contraseña del usuario.
- ◉ No soporta cambio de contraseña.
- ◉ No soporta los certificados de clave pública.
- ◉ No presenta sustitución periódica de claves de sesión.
- ◉ CRC-32 tiene débil control de integridad; admite un ataque de inserción en relación con algunas cifras a granel.
- ◉ Fija la codificación, se opone interoperables adiciones.

## • 4.6 SSL (*Secure Sockets Layer*)

### ○ Características

- ◉ Protocolos criptográficos que proporcionan confidencialidad e integridad a las comunicaciones en redes TCP/IP.
- ◉ Protegen del nivel de transporte hacia arriba.
- ◉ Protegen la comunicación *end-to-end*.
- ◉ Son la base de las comunicaciones seguras con navegadores web.
- ◉ El objetivo principal de SSL es mantener la información en secreto, ya que sólo se envía al dispositivo correcto y la persona. Esto es vital ya que la información que he dado es enviada desde un ordenador a otro.
- ◉ Integridad de mensajes. (MD5, SHA) Autenticación tanto del servidor de destino, como del cliente (opcional). (RSA).
- ◉ SSL es un protocolo que se instala entre los niveles de transporte y de aplicación, con aplicación local puede ser utilizado con pequeñas modificaciones en los programas que utilizan protocolos de red.
- ◉ SSL fue diseñado como un protocolo seguro de propósito general y no teniendo en mente las necesidades específicas del comercio electrónico.
- ◉ SSL trabaja sobre el protocolo TCP, por debajo de protocolos como HTTP, IMAP, LDAP, etc., y puede ser usado por todos ellos de forma transparente para el usuario. Opera entre la capa de transporte y la de sesión del modelo OSI (o entre la capa de transporte y la de aplicación)



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

del modelo TCP) y está formado, a su vez, por dos capas y cuatro componentes bien diferenciados.

- SSL supone una serie de fases básicas: negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales. Encriptación del tráfico basado en cifrado simétrico.

## ○ Ventajas

- Una de las ventajas del SSL es que es independiente del protocolo de aplicación, ya que es posible ubicarlo por encima del mismo en forma transparente.
- SSL encripta los datos por toda la ruta desde el cliente al servidor de destino.
- Proporciona a una comunicación:
  - Confidencialidad (cifrado).
  - Integridad (mediante HMAC).
  - Autenticidad de servidor (y en algunos casos, de cliente, mediante certificados).
- Protocolo base de la seguridad en el comercio electrónico.
- Hay una tendencia a que uno de estos equipos puede pretender ser su sitio y que engañaría a sus clientes para que pudieran enviar información. Esto sólo se puede evitar cuando hay un uso de PKI o la infraestructura de clave pública y certificada SSL de un proveedor de SSL fiables.
- Proporciona seguridad durante la transmisión. Es transparente para el usuario. No son necesarias muchas modificaciones en los programas que lo utilizan.
- Aumenta la seguridad del negocio, ya que la información privada que vaya de un ordenador a otro se encuentra encriptada.
- Aumenta la confianza de los clientes; los certificados SSL hacen ver que en la empresa se pueden depositar datos sin problema de posibles robos, ya que van a ser cifrados.
- Aumenta el número de ventas gracias a la confianza: a mayor confianza, mayor número de ventas; la repetición y el boca a boca de lo seguro que es, ayudarán a subir las cifras de ventas.
- Certifica la personalidad de la empresa, ya que demuestra que se trata de esa empresa, hecho difícil ante el gran número de *webs phishing* legítimas que existen su *web*, porque consigue que una entidad independiente respalde el visto bueno.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Elimina *malware* de su web, ya que los certificados SSL escanean el sitio buscando programas dañinos.
- Aumenta el tráfico de su *web*, porque sin virus la página se posiciona orgánicamente mejor en Google, consiguiendo más visitas sin pagar ni un sólo peso.
- Evita que los usuarios se vayan cuando van a comprar y tienen que introducir claves privadas, ya que está demostrado que las personas salen del sitio cuando tienen que poner datos privados, si no están seguros de que va a haber seguridad.
- No da problemas con los navegadores, ya que funciona perfectamente con el 99% de los navegadores.
- Convierte la Internet en una red más segura, porque la seguridad la formamos todos, y si su *web* es insegura la incertidumbre entre los usuarios es mayor. Por el contrario, si hay más seguridad, el comercio electrónico aumentará, beneficiando a todo el mundo.
- Los servicios de seguridad son transparentes al usuario y a la aplicación y puede ser usado por otros protocolos aparte del HTTP. S-HTTP.
- SSL puede establecer múltiples conexiones dentro de una misma sesión o reanudar una sesión previamente interrumpida.
- SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet, mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor, comunicarse de una forma diseñada para prevenir ataques.

## ○ Desventajas

- Costoso en recursos (10x). Uso de SSL es muy costoso. Debe crearla con el servidor correcto y su identidad debe estar autenticado. Algunos de los proveedores de SSL son populares y por eso tienen precios altos. La segunda desventaja es el rendimiento. Se requiere más recursos del servidor cuando se envía la información cifrada. La diferencia en el rendimiento se verá en los sitios *web* que reciben gran cantidad de tráfico.
- Incrementa notablemente la carga del procesador tanto al encriptar como al desencriptar, en relación a una comunicación no encriptada.
- Cada conexión necesita una configuración diferente.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Los certificados pueden expirar y son complicados para el usuario final.
- Debido a las fuertes restricciones que tenían los EEUU hasta hace poco, las versiones de exportación tanto de Netscape como del otro navegador utilizaban claves de sesión de 40 bits. Estas longitudes de clave garantizan la seguridad durante la transmisión, pero no después de ella, ya que estos datos pueden ser almacenados y cripto-analizados con éxito al tener una clave de 40 bits. Compruebe su navegador preferido y desactive todas las opciones para utilizar algoritmos simétricos con claves menores de 128 bits y claves menores de 1,024 bits con algoritmos asimétricos.
- Se definió como una extensión de HTTP y sus servicios sólo están disponibles para este protocolo.

#### • 4.7 HTTPS (Protocolo seguro de transferencia de hipertexto)

##### ○ Características

- Para actualizar un archivo en un sitio web, todo lo que el usuario necesita es un navegador de Internet moderno. Sin embargo, en el servidor del sitio web, un programador de sitios debe implementar un sistema que pueda manejar la carga de un archivo. El programador tiene varias opciones para hacer esto, desde cargar un HTML simple hasta formularios más avanzados con lenguajes como PHP y ASP, para usar en un foro o blog. Con la descarga, todo lo que el usuario tiene que hacer es cliquear un enlace.
- Protocolo de comunicaciones estándar que comunica servidores, proxys y clientes. Permite la transferencia de documentos web, sin importar cuál es el cliente o cual es el servidor.
- Es un protocolo basado en el esquema petición/respuesta.
- El cliente envía un mensaje de petición y el servidor contesta con un mensaje de respuesta, cuyo contenido es función de la petición hecha por el cliente.

##### ○ Ventajas

- La mejor parte del protocolo HTTP es su sencillez de preparación. Simplemente lanzando unos cuantos comandos, se dispone de un



método sencillo de dar al mundo entero acceso a tu repositorio Git, en tan sólo unos minutos. Además, el protocolo HTTP no requiere de grandes recursos en el servidor. Por utilizar normalmente un servidor HTTP estático, un servidor Apache estándar puede con un tráfico de miles de archivos por segundo; siendo difícil de sobrecargar, incluso con el más pequeño de los servidores.

- ◉ Se pueden también servir los repositorios de sólo lectura a través de HTTPS, teniendo así las transferencias encriptadas. O se puede ir más lejos aún, requiriendo el uso de certificados SSL, específicos para cada cliente. Aunque, si se pretende ir tan lejos, es más sencillo utilizar claves públicas SSH, pero está la posibilidad por si en algún caso llega a ser mejor solución el uso de certificados SSL u otros medios de autenticación HTTP para el acceso de sólo-lectura a través de HTTPS.
- ◉ Otro detalle muy útil al emplear HTTP es que, al ser un protocolo de uso común, la mayoría de los cortafuegos corporativos suelen tener habilitado el tráfico a través de este puerto.
- ◉ Las cargas HTTP proporcionan un método increíblemente simple para subir archivos a un servidor, con un mínimo de conocimiento sobre transferencias de archivos. Descargar un archivo también es increíblemente fácil.
- ◉ El protocolo HTTP está basado en mensajes, ya que es un texto plano que permite que sea legible y fácil de depurar.
- ◉ La dirección IP no distingue usuarios, sólo máquinas.
- ◉ Los controles HTML ocultos y las URL infladas se vuelven más complicados de mantener, cuando la información persistente crece en tamaño.
- ◉ Las URL infladas funcionan si el acceso de las páginas se realiza activando enlaces (es decir, si no se introduce la URL directamente). Las *cookies* pueden ser leídas por terceros.
- ◉ Es una técnica de autenticación sencilla que utiliza la cabecera del protocolo HTTP. Con sus variables globales, \$PHP\_AUTH\_USER, \$PHP\_AUTH\_PW, para controlar el acceso restringido a una zona de nuestra aplicación web.
- ◉ Lo que hace esta restricción es mostrar una ventana *pop up* que solicita el ingreso de un usuario y su respectivo *password* y lo almacena en las variables globales: \$PHP\_AUTH\_USER, \$PHP\_AUTH\_PW, respectivamente, y estas las compara con los *logins* almacenados, ya sea en un archivo plano de texto (.txt) o en una base datos como mysql.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ Desventajas

- La pega de servir un repositorio a través de HTTP es su relativa ineeficiencia para el cliente. Suele requerir mucho más tiempo el clonar o el recuperar (*fetch*), debido a la mayor carga de procesamiento y al mayor volumen de transferencia que se da sobre HTTP, respecto de otros protocolos de red. Y precisamente por esto, porque no es tan inteligente y no transfiere solamente los datos imprescindibles (no hay un trabajo dinámico por parte del servidor), el protocolo HTTP suele ser conocido como el protocolo estúpido.
- Las desventajas radican en la carencia de potencia HTTP cuando se trata de cargar archivos. Además, un programador necesita tener el conocimiento requerido para crear el formulario en HTML, con el fin de cargar el archivo en cuestión.
- El protocolo HTTP está basado en mensajes, el cual es un texto plano con desventaja de ser un mensaje más largo.
- Se debe utilizar exclusivamente *cookies* de sesión.
- Algunos usuarios no aceptan *cookies* de ningún tipo.
- La dirección IP está oculta si hay un proxy de por medio.
- Si su aplicación web la van a usar en lugares públicos como cibercafés, la universidad o entro de un lugar a su aplicación web.
- Si no se utiliza con algún tipo de encriptación donde tengan activado algún *firewall* o bloqueados los *pop up*, no podría autenticarse para ingresar.
- Dificultad en la administración de permisos.

## • 4.8 PPTP (Protocolo de túnel punto a punto)

## ○ Características

- El protocolo PPTP fue desarrollado por Microsoft para permitir a las personas acceder a las redes de forma remota y segura a través de Internet, a través de una red privada virtual. Los datos se encapsulan en datagramas IP y cifrados utilizando *Microsoft Point -to -Point Encryption* antes de su transporte, a través de IP a través de Internet. PPTP se basa en el protocolo de encapsulación de enrutamiento genérico y el Protocolo *Point-to-Point*.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- PPTP es un protocolo basado en PPP y GRE (*Generic Routing Encapsulation*) que se usa para establecer túneles a nivel IP, permitiendo armar redes privadas virtuales (VPNs).
- Este protocolo ofrece una conexión básica, rápida y securizada. Es posible utilizarlo en un ordenador, en un teléfono móvil o en una tableta. Realiza una encriptación máxima de 128 bits.

## ○ **Ventajas**

- Es más fácil de configurar y usar que L2TP. Los datos se encriptan sin IPsec, lo que significa que no es necesaria la instalación de certificados de equipo o una infraestructura de clave pública (PKI). Los ordenadores que utilizan los sistemas operativos de Microsoft son compatibles con PPTP de forma predeterminada.
- La ventaja del protocolo PPTP es que es ampliamente soportado por plataformas Windows, pudiendo Linux trabajar como servidor PPTP y Windows (95 en adelante) conectarse como clientes, o en el caso de Windows NT, 2000 y XP se daría el caso inverso.
- Es fácil, simple y rápido de utilizar.
- No se necesita instalar un *software*.
- Reconocido por la mayoría de los *software* y operadores.

## ○ **Desventajas**

- El principal inconveniente de PPTP es la seguridad más pobre en comparación con L2TP. No proporciona integridad de datos o datos de verificación de origen, lo que significa que no puede confirmar los datos no se alteró en tránsito o verificar que fue enviado por una fuente autorizada. Esto también significa PPTP puede tener problemas de rendimiento en redes inestables.
- La gran desventaja de este protocolo reside en su diseño, que no es del todo seguro: antes que el túnel GRE se establezca, parte del inicio de sesión, autenticación y demás, se hace por protocolo TCP en forma de texto claro, parte de la información que pasa de este modo es el IP del cliente y el servidor, el nombre de usuario, la contraseña cifrada, etc., datos que cualquiera que esté en el medio puede llegar a usar para intentar entrar. Además, la implementación de Microsoft agrega un poco más de fallas a su implementación del protocolo, usando un sistema de clave simétrico para la autenticación: RC4 de



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

40 y 128 bits. La versión de 40 bits es demasiado débil para poder ser considerada segura, pero además de todo, la clave se basa en la contraseña del usuario (de esta manera el usuario puede tener múltiples sesiones con su propia clave). El problema de esto es que la clave debería cambiarse cada tanto (más aún cuando las sesiones PPTP son prolongadas) y esto realmente no sucede casi nunca.

- ◎ Menos securizado que los otros dos protocolos.
- ◎ Más bloqueado a menudo por los proveedores de servicios de Internet.

#### • 4.9 Resumen de los protocolos de seguridad

A continuación, se presenta un resumen de lo mencionado anteriormente para poder localizar con mayor facilidad, el objetivo principal, reconociendo la mejor alternativa de seguridad para las redes MESH.

En la Tabla 4.1 se da a conocer un resumen de los beneficios y desventajas del protocolo WEP.



Tabla 4.1. WEP (Wired Equivalent Privacy, privacidad equivalente al cable).

Características	Ventajas	Desventajas
<ul style="list-style-type: none"><li>• Cifra los datos de red de forma que sólo el destinatario pueda acceder.</li><li>• Cuenta con dos niveles de seguridad, clave de 64 (5 caracteres o 10 dígitos hexadecimales) y 128 bits (13 caracteres o 26 dígitos hexadecimales).</li><li>• Codifica los datos mediante una clave de cifrado antes de ser enviado a su destinatario.</li><li>• Utiliza el algoritmo de flujo RC4 y el algoritmo de chequeo de integridad CRC. Junto una llave secreta y un vector de iniciación.</li><li>• Forma parte de la especificación 802.11.</li><li>• Opera al nivel 2 del modelo OSI.</li><li>• Los dos puntos de acceso deben tener la misma clave.</li></ul>	<ul style="list-style-type: none"><li>• El cifrado de 128 bits evita que el intruso informático acceda a sus archivos y conexión de alta velocidad. Bloqueando sus accesos por el alto consumo de este cifrado.</li><li>• Compatibilidad entre distintos fabricantes.</li><li>• Superior a la seguridad en redes LAN.</li><li>• Existe tráfico interrumpido de datos durante un tiempo determinado al momento de cifrar la clave.</li></ul>	<ul style="list-style-type: none"><li>• Vector inicial.</li><li>• Sistema de integridad.</li><li>• Claves de cifrado estáticas, el atacante accede varias veces con el mismo texto cifrado.</li><li>• No brinda servicio de autenticación.</li><li>• Existen varias herramientas (Software) para romper la clave secreta.</li><li>• Es probable que el vector inicial se repita a las 5 horas en redes de alto tráfico. Reutilización del vector.</li><li>• El cliente no puede autenticar a la red.</li><li>• Su algoritmo permite la modificación de datos sin ser notado.</li><li>• El punto de acceso y los clientes deben estar programados con la misma llave, hecho que debilita la red.</li></ul>

Fuente: elaboración propia.

En la Tabla 4.2 se da a conocer un resumen de los beneficios y desventajas del protocolo WPA.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 4.2. WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi).

Características	Ventajas	Desventajas
<ul style="list-style-type: none"><li>• Implementa la mayoría del estándar IEEE 802.11i.</li><li>• Resiste Sistemas operativos desde Windows 98 – XP y Linux.</li><li>• Distribución Dinámica de claves, utilización más robusta en el vector inicial.</li><li>• Propone un nuevo protocolo para cifrado TKIP (<i>Temporary Key Integrity Protocol</i>) el cual se encarga de cambiar la clave compartida entre el punto de acceso y cliente cada cierto tiempo.</li><li>• Basada en servidores de autenticación (<i>Radius Remote Authentication Dial-In User Server</i>) distribuye claves el cual diferentes entre los usuarios.</li></ul>	<ul style="list-style-type: none"><li>• Subsana los problemas de WEP.</li><li>• Establece nuevos protocolos para cambiar clave compartida.</li><li>• Trabaja en dos modalidades caseras y corporativas.</li><li>• No es necesario el conocimiento técnico, sin introducir manualmente una contraseña ni clave asociada.</li><li>• Claves dinámicas, autenticaciones mediante claves generadas por el sistema.</li><li>• Se genera autenticación evitando la verificación de las direcciones MAC. De las estaciones por la terna.</li></ul>	<ul style="list-style-type: none"><li>• No todos los dispositivos son capaces de implementarlo.</li><li>• No todas las tarjetas inalámbricas son compatibles con este estándar.</li><li>• No cumple la norma IEEE 802.11i.</li><li>• Vulnerable ante claves cortas.</li><li>• Preestablecidas utilizan palabras presentes en el diccionario y longitud menor a 20 caracteres, lo cual permite un ataque más fácilmente.</li></ul>

Fuente: elaboración propia.

En la Tabla 4.3 se despliega un resumen de los beneficios y desventajas del protocolo WPA2 (802.11i).



Tabla 4.3. WPA2 (802.11i).

Características	Ventajas	Desventajas
<ul style="list-style-type: none"><li>• Versión de migración de WPA, pues esta es la segunda generación y es la versión certificada del estándar 802.11i</li><li>• Incluye el algoritmo de cifrado AES (<i>Advanced Encryption Standard</i>) el cual es un algoritmo cifrado de bloque con claves de 128 bits, con un máximo de 256 bits.</li><li>• Luego de la autenticación del usuario el servidor crea una pareja de claves maestras PMK, las cuales se distribuyen entre el punto de acceso y cliente. Así se protegerá el tráfico entre éstos.</li></ul>	<ul style="list-style-type: none"><li>• Ideal para sector privado y público.</li><li>• Utiliza protocolos para el aseguramiento de la integridad y autenticidad de los mensajes.</li><li>• Asigna a cada usuario una clave única de identificación.</li><li>• Cifrado por paquete, así que cada paquete utiliza una clave generada específicamente para ese mismo.</li><li>• Reduce la complejidad y el tiempo de los usuarios de un punto de acceso a otro.</li></ul>	<ul style="list-style-type: none"><li>• Es necesario de equipos potentes pues no todos podrán soportar el protocolo.</li><li>• Vulnerabilidad en la información pues esta va en formato de texto, hecho que permite ser más fácil su manipulación.</li><li>• No se puede controlar el área de cobertura de una conexión.</li><li>• No todos los dispositivos pueden adquirir el protocolo.</li></ul>

Fuente: elaboración propia.

En la Tabla 4.4 se dará a conocer un resumen de los beneficios y desventajas del protocolo SSH.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 4.4. SSH (Secure Shell).

Características	Ventajas	Desventajas
<ul style="list-style-type: none"><li>• Su conexión se establece en una primera instancia donde se determina la identidad entre el servidor y el cliente para así tener un canal seguro. Y como segunda instancia, el cliente inicia sesión en el servidor.</li><li>• El cliente y el servidor se autentica uno a otro para asegurar que las dos máquinas que se comunican se identifiquen y así adquirir información.</li><li>• Su objetivo es iniciar sesiones en máquinas remotas que ofrecen autenticación, confidencialidad e integridad.</li><li>• Utiliza el puerto 22 y sigue el modelo cliente-servidor.</li><li>• Usa el mecanismo de criptografía.</li><li>• Por medio de <i>login</i> y ejecución de procesos remotos genera seguridad.</li><li>• El cliente puede verificar que se está conectado a un mismo servidor.</li><li>• Soporta la transferencia segura de archivos y el reenvío seguro de tráfico de sistemas TCP/IP y X Windows.</li></ul>	<ul style="list-style-type: none"><li>• Sencillo de usar y habilitar.</li><li>• Comprime los datos lo más posible antes de ser transferidos.</li><li>• Permite que un cliente abra sesión interactiva en una máquina remota y lograr el envío de comandos o archivos.</li><li>• Comunicación cifrada en todos sus componentes sean datos, archivos o comandos. Entre cliente servidor.</li><li>• Inicia sesiones <i>login</i> en servidores remotos, ejecutar aplicaciones graficas desde Shell. Realizar túneles IP.</li><li>• La interceptación de la comunicación entre dos sistemas por parte de una tercera maquina generando una copia.</li><li>• Puede cifrar, autenticar y comprimir de forma automática los datos trasmítidos.</li></ul>	<ul style="list-style-type: none"><li>• Imposibilidad para dar acceso anónimo al repositorio.</li><li>• Trasmite la información en texto plano, lo que deja que esté vulnerable sin ser notado ante cualquier intruso.</li><li>• Por medio de una herramienta rastreadora logra capturar paquetes, obteniendo el nombre de acceso y la contraseña para acceder remotamente.</li><li>• No soporta cambio de contraseña.</li><li>• No soporta certificados de clave pública.</li><li>• No sustitución periódica de claves de sesión.</li><li>• Débil control de integridad.</li></ul>

Fuente: elaboración propia.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

En la Tabla 4.5 se da a conocer un resumen de los beneficios y desventajas del protocolo SSL.

Tabla 4.5. SSL (Secure Sockets Layer).

Características	Ventajas	Desventajas
<ul style="list-style-type: none"><li>• Protegen del nivel de transporte hacia arriba</li><li>• Base de las comunicaciones seguras con navegadores web.</li><li>• Integridad de mensajes, autenticando tanto del servidor de destino como del cliente.</li><li>• Instala entre los niveles de transporte y de aplicación.</li><li>• Trabaja sobre el protocolo TCP y por debajo de protocolos como HTTP, IMAP.</li><li>• Intercambio de claves públicas y autenticación basada en certificados digitales.</li><li>• Encriptación del tráfico basado en cifrado simétrico.</li></ul>	<ul style="list-style-type: none"><li>• Es independiente del protocolo de aplicación, pues es posible ubicarlo por encima del mismo en forma transparente.</li><li>• Encripta los datos por toda la ruta desde el cliente al servidor.</li><li>• Confidencialidad (cifrado) en todo su ámbito.</li><li>• Protocolo base de seguridad en el comercio electrónico.</li><li>• Es transparente para el usuario. No necesita de muchas modificaciones en los programas que lo utilizan.</li><li>• Elimina <i>malware</i> de la web, pues escanea el sitio para detectar programas dañinos.</li><li>• Funcionalidad 99% con todos los navegadores.</li><li>• Establece múltiples conexiones dentro de la misma sesión o reanudar una sesión previamente interrumpida.</li><li>• Sólo el servidor es autenticado, garantizando así la identidad.</li></ul>	<ul style="list-style-type: none"><li>• Costoso en recursos.</li><li>• Incrementa la carga del procesador en cualquier momento, en comparación a la comunicación sin autenticación.</li><li>• Cada conexión necesita una configuración diferente.</li><li>• Claves de sesión de 40 bits, lo cual desprotege después de la transmisión.</li><li>• Sólo disponibles sus servicios para protocolo HTTP.</li></ul>

Fuente: elaboración propia.

En la Tabla 4.6 se da a conocer un resumen de los beneficios y desventajas del protocolo HTTPS.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 4.6. HTTPS (Protocolo Seguro de Transferencia de Hipertexto).

Características	Ventajas	Desventajas
<ul style="list-style-type: none"><li>• La carga de documentos y archivos en la <i>web</i> se torna más rápido, facilitando al usuario gracias a su lenguaje PHP y ASP.</li><li>• Comunica servidores, <i>proxies</i> y clientes, permitiendo la transferencia de documentos <i>web</i>, sin importar cuál es el cliente o cuál es el servidor.</li><li>• Basado en esquema petición/respuesta.</li><li>• El cliente envía un mensaje de petición y el servidor contesta con un mensaje de respuesta, con el cual fue dado a petición del cliente.</li><li>• Solicita usuario y <i>password</i> (confianza).</li><li>• Texto plano legible y fácil de depurar.</li></ul>	<ul style="list-style-type: none"><li>• Sencillez de preparación.</li><li>• No requiere de grandes recursos en el servidor.</li><li>• Los repositorios de sólo lectura para así lograr transferencias encriptadas.</li><li>• Proporciona un método increíblemente simple para subir archivos al servidor, con un mínimo de conocimiento sobre la transferencia de archivos.</li><li>• El acceso a las páginas se realiza activando enlaces, sin necesidad de copiar todo el URL.</li><li>• Con variables globales permite restringir zonas de la aplicación <i>web</i>.</li></ul>	<ul style="list-style-type: none"><li>• No hay un trabajo dinámico por parte del servidor.</li><li>• Carece de potencia en el momento de carga.</li><li>• La dirección IP está oculta, si hay un <i>proxy</i> de por medio.</li><li>• Dificultad en la administración de permisos.</li></ul>

Fuente: elaboración propia.

## • Conclusión

Como todos los proyectos tecnológicos, la seguridad ocupa un lugar importante. Es necesario conocer bondades y debilidades de los diferentes protocolos de seguridad para implementar uno o varios, de acuerdo con el entorno de conexión y los riesgos asociados al manejo de información.





( 5 )

## Valoración financiera para la implementación de sistemas de interconexión MESH

### • Introducción

La planeación de un proyecto tecnológico debe contar con una valoración financiera. En materia de redes MESH, se tiene en cuenta información de tipo financiero, como el indicador de liquidez, la prueba ácida, la capacidad de endeudamiento, e indicadores de rentabilidad. En cuanto a la temporalidad, se traza una ruta crítica para identificar punto de inicio y terminación. En general, se presenta ponderación y análisis económico de inversión de un proyecto de redes MESH.

### • 5.1 Diseño ingenieril de la solución

Se describe en este capítulo, la base operacional de la solución que soporta el análisis y la valoración de los costos demandados para implementar la solución MESH en donde esta sea requerida. La consideración económica por contemplar y estructurar, integra el análisis y direccionamiento de los factores citados:

- Ruta de control del proyecto.
- Escenario de gestión financiera.
- Ruta crítica.
- Segmentación tecnológica.

### • 5.2 Ruta de control del proyecto

El manejo, gestión y gerenciamiento de un proyecto de base tecnológica, como lo es la entidad representativa de la implementación de una solución



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

MESH, exige la consideración de una estricta ruta de control cuya significancia fue expresada por autores como George Terry (Memphis, 2010), quien afirma que el control es el proceso que determina lo que se está llevando a cabo, evaluando y calificando para, según el caso, aplicar medidas correctivas que garantizan que la ejecución del mismo se ajuste a lo planeado.

La implementación de una solución teleinformática soportada en redes MESH, demanda que el grupo realizador del proyecto valore los discriminantes siguientes:

- Relación de lo realizado con lo planeado.
- Medición de resultados.
- Detección de desviaciones.
- Establecimiento de medidas correctivas.

Estos discriminantes, contribuyen al direccionamiento paramétrico de los elementos que se señalan en la Figura 5.1.

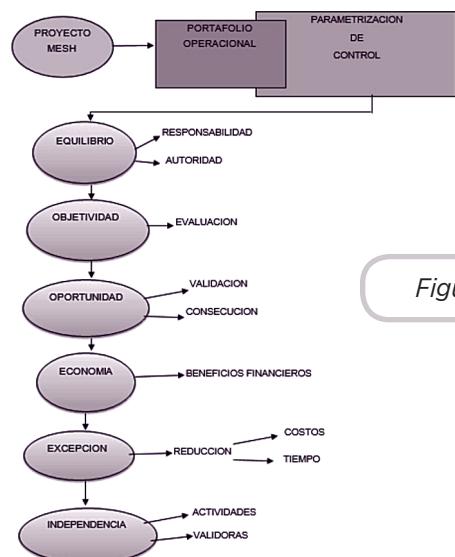


Figura 5.1. Elementos parametrizados del control.

Fuente: elaboración propia.

Los proyectos teleinformáticos en su desarrollo, demandan de la integración de los vértices o modos de acción funcional que se listan a continuación:

- Definición de objetivos y estándares técnicamente estructurados.
- Difusión entre el campo desarrollador de los controles establecidos.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

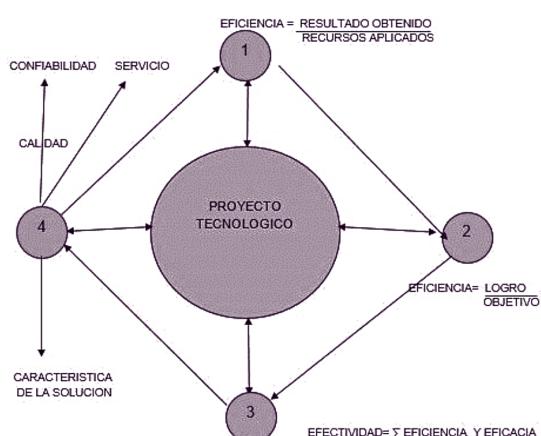
- Relación de objetivos del proyecto con los resultados de cada actividad.
- Evaluación de efectividad de los controles.
- Espejo operacional del grupo o empresa realizadora.
- Oportunidad como valoradora de utilidad.
- Accesibilidad.
- Ubicación estratégica.

Al implementar la solución MESH, debe tenerse presente que el logro de los resultados y la confiabilidad de su funcionalidad depende de la aplicación de los tipos de control señalados:

- Control previo: anterior a la realización de la actividad.
- Control en proceso: seguimiento de actividad realizado.
- Control posterior: comparación del resultado contenido con el esperado o presupuestado.

### • 5.3 Escenario de gestión financiera

La definición y estructuración de una solución teleinformática con tecnología MESH exige la consideración de la plataforma de indicadores de gestión, que integran como significantes funcionales la base del denominado *cuadrilátero de la confiabilidad* (Miranda, 2000), que se presentan en la Figura 5.2.



*Figura 5.2. Cuadrilátero de la confiabilidad.*

Fuente: elaboración propia.

La formulación de un indicador implica la consideración y aplicación de las unidades descriptivas que se listan:



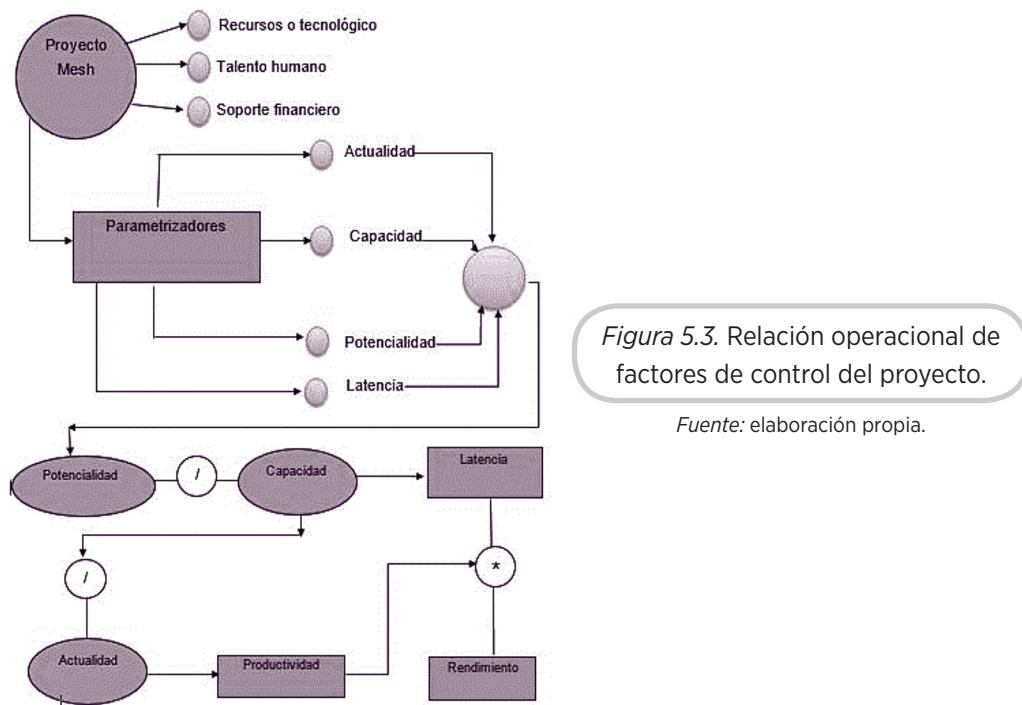
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Denominación o nombres del indicador.
- Propósito.
- Instrumentos.
- Responsables.
- Estándar de referencia.
- Patrón de comparación.

Los desarrollos de base tecnológica presuponen que el grupo realizador maneja e instrumenta estos valoradores operacionales (Memphis, 2010), a saber:

- **Actualidad:** que se puede construir o implementar con los recursos que se posee en el momento.
- **Capacidad:** que se puede producir o construir con los recursos del proyecto, si se aumenta el esfuerzo del talento que actúa.
- **Potencialidad:** se implementaría aumentando los recursos en el proyecto.
- **Latencia:** cómo se relaciona la potencialidad y la capacidad.

Gráficamente, se puede validar esta relación al observar la Figura 5.3:



*Figura 5.3. Relación operacional de factores de control del proyecto.*

Fuente: elaboración propia.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Cuando se realiza un proyecto telemático es importante tener presente los indicadores de gestión financiera (Miranda, 2000), estos son:

## ○ Indicadores de liquidez

Señala la potencialidad de efectuar para sostener económicamente el proyecto, sus elementos de análisis son:

*Disponibilidad de efectivo*

$$D.E = \frac{\text{Activo Corriente}}{\text{Pasivo Corriente}}$$

Señala el respaldo económico que se tiene para pagar cada peso que se adeuda por motivo de ejecución del proyecto.

*Prueba ácida*

$$PA = \frac{AC - INV - GPA}{PC}$$

AC = Ácido corriente  
INV = Inventarios  
GPA = Gastos pagados por anticipado  
PC = Pasivo Corriente

Mide la capacidad de la organización que ejecuta el proyecto, para poder atender las obligaciones asociadas con la implementación de la solución.

*Capacidad de endeudamiento*

$$CE = \frac{PT}{AT}$$

CE = Capacidad de endeudamiento  
PT = Pasivo Total  
AT = Activo Total

Señala, el índice real de endeudamiento que puede cubrirse al realizar el proyecto.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

## ○ Indicadores de rentabilidad

Señalan la base que califica el poder de gestión gerencial en la realización del proyecto, al medir la rentabilidad sobre la inversión realizada (Memphis, 2010).

La Figura 5.4 ilustra la generación y la estructuración del RSI (Rentabilidad Sobre Inversión).

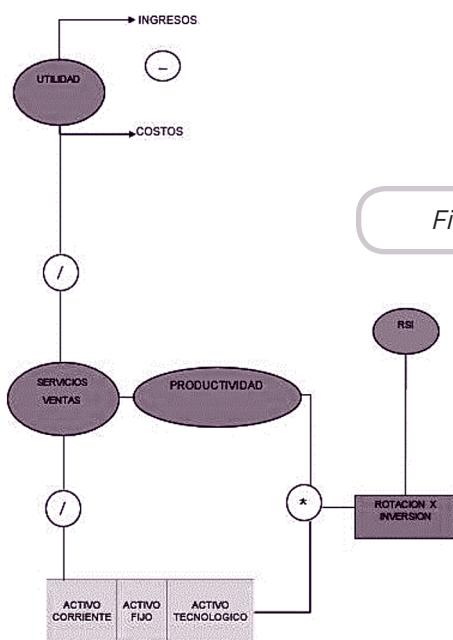


Figura 5.4. Rentabilidad sobre inversión (RSI).

Fuente: elaboración propia.

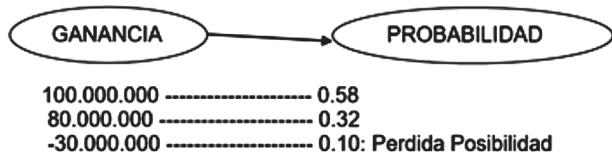
Junto con el RSI, se hace importante el evaluar en el proyecto telemático, la función de unidad, construir a partir de la cualificación de los resultados con la tendencia probabilística, para de esta manera valorar las consecuencias financieras que tendría el proyecto (Rheault, 2002).

Por ejemplo, si se quiere implementar una solución MESH, en el municipio de Yacopí, en Cundinamarca y se negocia con dos empresas oferentes, la Alcaldía valorará los esquemas de análisis que se listan, a saber:

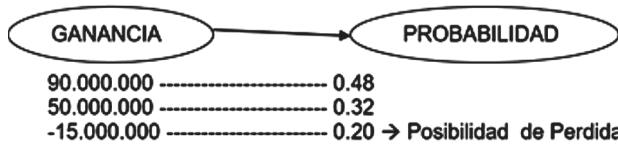


Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

❖ Empresa X



❖ Empresa Y



*Figura 5.5. Comparación económica Empresa X y Y.*

*Fuente.* elaboración propia.

La alcaldía valorará los estados, al configurar una lotería que definirá el valor monetario esperado, tal como se escribe aquí:

$$V_{ME} = L(\mu_1, \varepsilon_1, (1 - \mu, \varepsilon_2))$$

Que para cada caso genera:

Proyecto X:

$$V_{ME}(X) = \frac{100.000.000}{\emptyset.58 + 80.000.000 \cdot 0.32 + -30.000.000 (\emptyset.10)}$$

$$V_{ME}(X) = 100 \times 10^6 \times 0.58 + 80 \times 10^6 \times 0.32 - 30 \times 10^6 \times 0.10$$

$$V_{ME}(X) = 58.000.000 + 25.600.000 - 3.000.000$$

$$V_{ME}(X) = 80.600.000$$

Proyecto Y:

$$V_{ME}(Y) = 90.000.000 (0.48) + 50.000.000 (0.32) - 15.000.000 (0.20)$$

$$= 43.200.000 + 16.000.000 - 3.000.000$$

$$= 56.200.000$$



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Señalando, que la alcaldía optará por negociar con la empresa X, pues garantiza la obtención de mejores dividendos.

#### • 5.4 Ruta crítica

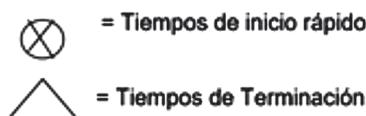
Conocer los tiempos de inicio y de terminación rápida en un proyecto de tecnología, es de vital importancia para quien pretende construir el andamiaje de solución, pues la gerencia del proyecto puede conocer cuál valor económico deberá ser añadido, en caso de una demora en el desarrollo o una tardanza en la entrega de un equipo (Prawda, 2004).

Por ejemplo, si se valora el proyecto para configurar la solución MESH, para el municipio de Yacopí y se identifican las siguientes actividades:

Compra de equipos	<A>
Obtención del sostén financiero	<B>
Establecimiento de nodos de operación	<C>
Estructuración de servicios	<D>
Configuración de equipos	<E>
Prueba de servicios	<F>
Capacitación de personal	<G>
Valoración de concurrencia y efectividad de la MESH	<H>

A dichas actividades, al pasarse al esquema de red, se les asignan tiempos programados de duración, tal como se observa en la *Figura 5.6. Asignación de tiempos red de actividades*.

El cálculo de la ruta crítica conlleva a la identificación de:





Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

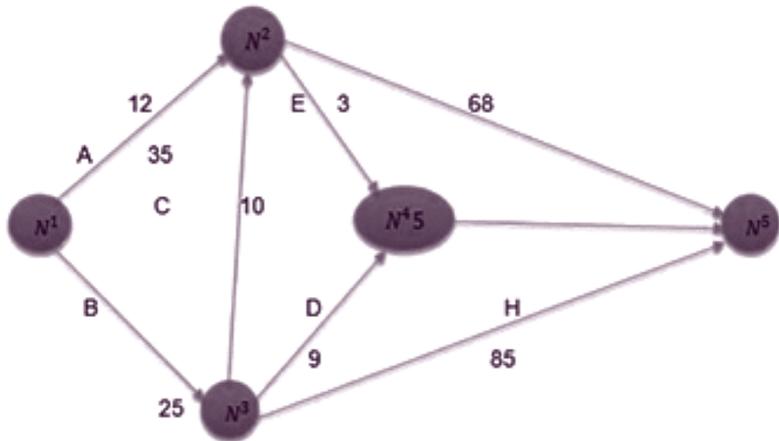


Figura 5.6. Asignación de tiempos red de actividades.

Fuente: elaboración propia.

## ○ Cálculo de $\emptyset$

$$IR_1 = \emptyset < \text{COMIENZO PROYECTO}$$

$$IR_3 = 0 + 25 = 25$$

$$IR_2 = \text{Max } 0 + 12, 25 + 35 = \text{Max } 12, 60 = 60$$

$$IR_4 = \text{Max } 60 + 3, 25 + 9 = \text{Max } 63, 34 = 63$$

$$IR_5 = \text{Max } 60 + 8, 63 + 10, 25 + 85$$

$$\begin{aligned} &= \text{Max } 68, 73, 110 \\ &= 110 \end{aligned}$$

Cuya valoración, se presenta en la Figura 5.7:

## ○ Cálculo de $\Delta$ (estos valores se incluyen en la figura 5.7)

$$TT_5 = 110$$

$$TT_4 = 110 - 10 = 100$$

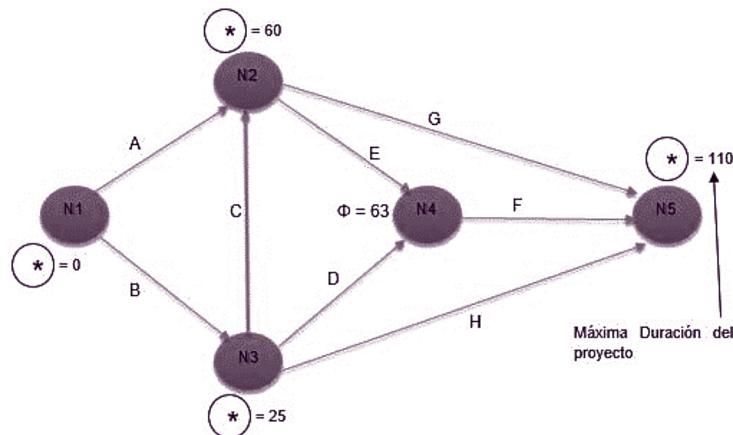
$$TT_2 = \text{Min } 110 - 8, 100 - 3 = 97$$

$$\begin{aligned} TT_3 &= \text{Min } 110 - 85, 100 - 9, 97 - 35 = \\ &= \text{Min } 25, 91, 62 = 25 \end{aligned}$$

$$\begin{aligned} TT_1 &= \text{Min } 25 - 25, 97 - 12 \\ &= \text{Min } \emptyset, 85 = \emptyset \end{aligned}$$



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano



*Figura 5.7. Ponderación de inicio rápido.*

*Fuente:* elaboración propia.

## ○ Cálculo de holgura

La holgura, que, como parámetro básico, generará la ruta crítica, es la diferencia entre los tiempos de terminación tardíos y los tiempos de inicio rápido ( $TT_i - IR_i$ ),  $i=1, 2, 3, 4, 5$ , la holgura  $H_i$ , será definida como:

$$\begin{aligned}
 H_i &= \diamond \\
 H_1 &= 0 - 0 = 0 \\
 H_2 &= 97 - 20 = 77 \\
 H_3 &= 25 - 25 = 0 \\
 H_4 &= 100 - 63 = 37 \\
 H_5 &= 110 - 110 = 0
 \end{aligned}$$

Estos valores se incluyen en la Figura 5.8:



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

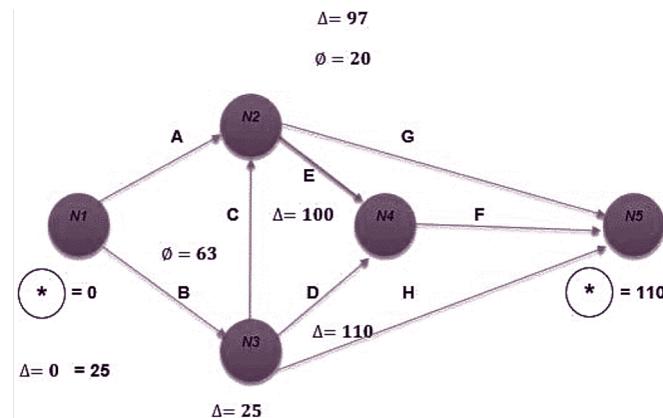


Figura 5.8. Cálculo de tiempos tardíos proyecto.

Fuente: elaboración propia.

En aquellos modos donde  $x\Delta = 0$ , se presenta la realización de una actividad crítica que, para el caso, será  $x\Delta = H_1, H_3$  y  $H_5$ , como nodos que conforman la ruta crítica, que se muestra en la Figura 5.9.

En la realización de proyectos telemáticos, puede trabajarse con tiempos de asignación por actividad, de forma no determinística, en cuyo caso se recurre al PERT (*Project Evaluation Review Technique*), que implica la catalogación de los factores listados:

**Tiempo optimista :**

$A_{ij}$  = Tiempo esperado en forma óptima de realización.

**Tiempo pesimista :**

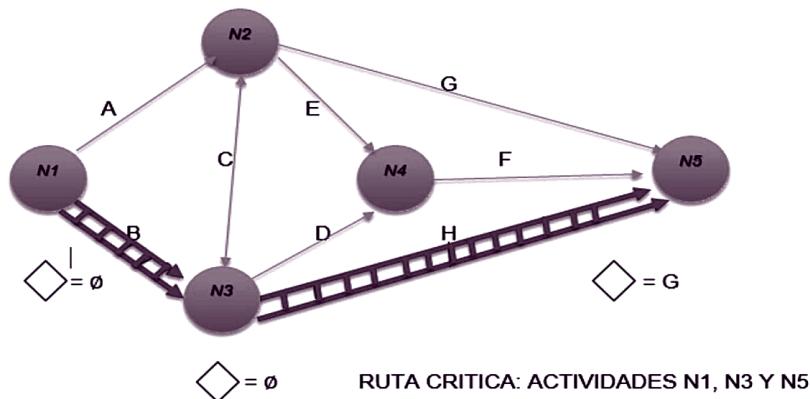
$\beta_{ij}$  = Tiempo asociado duraciones, modificación por eventos de previstos.

**Tiempo Real :**

$M_{ij}$  = Tiempo definido en condición normal de ejecución.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano



*Figura 5.9.* Ruta crítica red de actividades.

Fuente: elaboración propia.

El tiempo ponderado  $T_{ij}$  de trabajo se define como:

$$T_{ij} = \frac{1}{6} (A_{ij} + 4 M_{ij} + \beta_{ij})$$

Sus factores de duración esperada y varianza son:

$$\begin{aligned} \bar{T}(Y) &= \frac{n}{i=j=1} T_{ij} \\ \theta^2 Y &= \frac{1}{36} (\beta_{ij} - A_{ij}) 2 \end{aligned}$$

## • 5.5 Ponderación y análisis económico de inversión

La configuración de una solución MESH, demanda para las autoridades de la Junta Administradora Local o de los responsables delegados por el Concejo o Alcaldía Municipal, para: soportar el proyecto de adquisición de tecnología y supervisar el diseño, construcción e implantación de los entregables contratados, conocer con propiedad, los costos operacionales asociados con el *hardware*, los valores de los procesos de ajuste y los costos propios del montaje y alineamiento de la antena.

Previa valoración del costo de inversión para la solución MESH, es indispensable que se consideren y dominen completamente las especifica-



ciones del modelo Guifi.net<sup>9</sup>, que parametriza el transporte de la señal por acción de *routers* troncales que la impulsan a *routers* de distribución local o comunitaria, para entonces poder establecer la carta básica de instalación, según referente que se observa en la Figura 5.10.

La configuración lógica debe garantizar:

- Compatibilidad integral con protocolos dinámicos como BATMAN.
- Distribución funcional interactiva con el sistema Openwrt (distribución de Linux, basada en la catalogación segmentada de Fireware, para operar routers convencionales como linksys wrt54g).

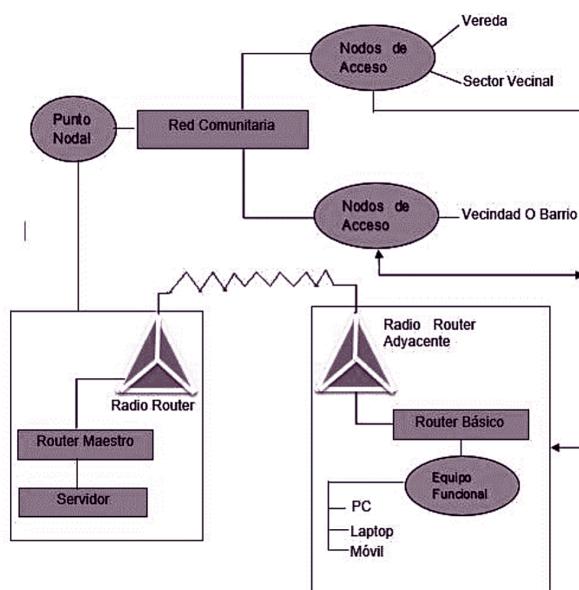


Figura 5.10. Configuración base de solución MESH.

Fuente: elaboración propia.

Para poseer un alto nivel de confiabilidad en la realización de la inversión, se debe tener como agente regulador de tecnología, el conjunto de parámetros que se listan a continuación:

- Frecuencia nominal de CPU = 680 MHz.
- Core count de CPU = 1.
- Arquitectura = mips-B2.
- Espacio Ram = 256 Mb.

<sup>9</sup> Red de telecomunicaciones, red abierta, libre y neutral, <https://guifi.net/es>



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Configuración de puertos
- 10/100 Ethernet = 0.
- 10/100/1000 Ethernet = 9.
- Condicionadores lógicos
- Slots miniPCI = 1.
- Factor POE/In-Out.
- Voltaje de alimentación = 8-28V.
- Controlador de voltaje.
- Monitor de temperatura = PBC/CPU.
- Patronato complementario de especificación o dimensiones.
- Temperatura de operación.
- Ganancia de antena.
- Referencia CPU.
- Puerto serial.
- Banda Dual IEEE802.11 /a /b /g /n.
- Potencia de salida.
- Chipset o Atheros.
- Conector de antena = mmcx.
- Tipo de modulación
- OFDM
- BPSK
- QPSK
- 16 QAM
- 64 QAM DSSS
- DBPSK
- DQPSK
- CCK

Técnicamente, es recomendable que en los costos del proyecto de implantación de la solución MESH, se considere como requisito fundamental que los equipos troncales estén basados en el procesador Atheros Mips 42 kc de 32 Mbytes y 400 Mhz, con equipamiento inalámbrico y con enlace directo a la interface de operación de configuración UCI (*Unified Configuration Interface*), a lo que se debe sumar y valorar estos parámetros, a saber:

- Tipo de red.
- Alineamiento OPENWRT o IPTABLES-MOD-EXTRA.
- IPTABLES-MOD-IPOPT.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- KMOD-IPT-NAT.
- LIPTHREAD.
- WIFIDOG.
- IPTABLES-MOD-WAT-EXTRA.

Debe recordarse que un costo a tener en cuenta en el asociado con la planta de pruebas de conectividad implica (Martinez, 2014):

- Búsqueda de nodos adyacentes.
- Conexión con nodos adyacentes.
- Verificación de tasa mínima de transferencia como medida de la calidad de conexión.

Debido a la naturaleza operacional de la construcción de la solución MESH, se requiere incluir en el presupuesto de la inversión, estos diferenciadores económicos:

- Afinamiento de interface de red.
- Catalogación a modo de prueba de error.
- Iniciación de consola TFTP.
- Reiniciación vía telnet del dispositivo.
- Instalación de paquetes.
- Asignación de contraseñas.
- Ajustes de configuración.
- Implementación *Fireware*.
- Implementación *Wifidog*.
- Implementación de servidores.

El control económico de la inversión deberá hacerse mediante programación entera y heurística, considerando los distractores señalados en la Tabla 5.1.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 5.1. Guía de control proyecto MESH.

Componentes	Recursos				
	Identificación	Costos de instalación	Tiempo de instalación	Probabilidad de fallas	Retorno de inversión
A	A1	X1	D1	P1	TRI 1
	A2	X2	D2	P2	TRI 2
	A3	X3	D3	P2	TRI 3
B	B4	X4	D4	P4	TRI 4
	A5	X5	D5	P5	TRI 5
	A6	X6	D6	P6	TRI 6
C	A7	X7	D7	P7	TRI 7
	A8	X8	D8	P8	TRI 8
	A9	X9	D9	P9	TRI 9

Fuente: elaboración propia.

Así mismo, es recomendable valorar el costo de una póliza de seguro para el punto nodal de operación central, para lo cual hay que tener en cuenta, estos valores:

- Valor prima anual.
- Valor de cobertura de la póliza.
- Valor asegurable (equipos de seguridad y soporte computacional).
- Índice probabilístico de tendencia al desastre o robo.

Esto con el fin ponderar el valor de salvamento de la inversión y de cuantificar el valor de inversión adicional, por ejemplo, si el costo de la arquitectura computacional del punto nodal de operación central es de 14 millones de pesos, el valor de prima anual de aseguramiento es de dos millones de pesos y si la aseguradora se compromete el valor de 17 millones de pesos, sabiendo que la ocurrencia probabilística de desastre es de 0.20, según historial a nivel nacional (robo, incendio, terremoto), el grupo responsable del proyecto, deberá entonces saber que la pérdida esperada será de:

$$\begin{aligned} PE &= (14.000.000) (0.20) + 0(0.80) \\ PE &= \$2.800.000 \end{aligned}$$

Lo que presupone la obligación de apartar como índice de inversión adicional los dos millones de pesos que vale la prima de aseguramiento, tal como lo registra la Tabla 5.2.



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Tabla 5.2. Matriz de pérdidas económicas.

Cursos de acción	Espacio decisional	
	Existe desastre	No hay desastre
Se asegura proyecto	\$ 2'000.000	\$ 2'000.000
	<Gana 17.000.000>	<No obtiene nada>
No se asegura proyecto	\$ 14'000.000	\$ 0
	<Pierde todo>	<No pierde nada>

Fuente: elaboración propia.

Nota: si la vecindad local o regional, no cuenta con la participación directa del grupo consultor en tecnología que dedique la universidad para desarrollar el proyecto, es necesario presupuestar el valor de ocho horas hombre, el cual se liquida según estándar de cobro ingenieril a \$100.000 hora.

En resumen, la valoración económica del proyecto MESH, incluye:

- Equipo computacional
- Servidores.
- Unidades de acceso.
- Routers.
- Antena.
- Talento humano
- Instalación.
- Afinamiento.
- Pruebas.
- Póliza de seguro
- Obras civiles.

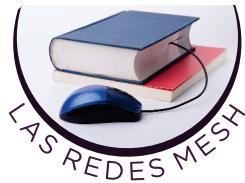
## • Conclusión

Las redes MESH se caracterizan por presentar un bajo costo de diseño e implementación, ideal para comunidades distantes o de bajos recursos. Sin embargo, es necesario, realizar toda la ponderación económica y financiera que soporte técnicamente los proyectos.



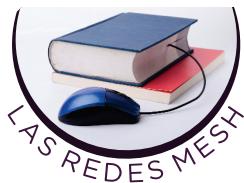


## Referencias bibliográficas



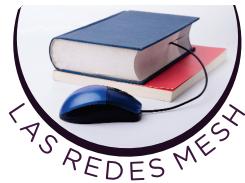
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Andreu, F., Pellejero, I., & Lesta, A. (2006). <https://books.google.com.co/>. (Marcombo, Ed.) Recuperado el Agosto de 2016, de Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica.
- Arias, A., Peña, R., & Chávez, P. (Agosto de 2015). *Repositorio de la Escuela Superior Politécnica del Litoral Artículo Tesis Grado*. Recuperado el 2016, de Análisis comparativo en términos de capacidad y calidad de servicio de una PBX en código abierto instalada en un enrutador inalámbrico y en un servidor tradicional usando Redes Inalámbricas MESH.: [https://www.researchgate.net/publication/277786852\\_Analisis\\_comparativo\\_en\\_terminos\\_de\\_capacidad\\_y\\_calidad\\_de\\_servicio\\_de\\_una\\_pbx\\_en\\_codigo\\_abierto\\_instalada\\_en\\_un\\_enrutador\\_inalambrico\\_y\\_en\\_un\\_servidor\\_tradicional\\_usando\\_redes\\_inalambricas\\_MESH](https://www.researchgate.net/publication/277786852_Analisis_comparativo_en_terminos_de_capacidad_y_calidad_de_servicio_de_una_pbx_en_codigo_abierto_instalada_en_un_enrutador_inalambrico_y_en_un_servidor_tradicional_usando_redes_inalambricas_MESH)
- Arroyo Miguel. (Mayo de 2011). *Un ataque a la infiltracion*. Recuperado el 2016, de [http://hacking-etico.com/wpcontent/uploads/2012/05/diagrama\\_arp\\_dns\\_spoof.png](http://hacking-etico.com/wpcontent/uploads/2012/05/diagrama_arp_dns_spoof.png)
- Artman, J. (2014). *eHow Español*. Recuperado el Agosto de 2016, de Qué es una red ad hoc: [http://www.ehowenespanol.com/red-hoc-sobre\\_498728/](http://www.ehowenespanol.com/red-hoc-sobre_498728/)
- Association, I.-S. (2016). *IEEE Standards*. Recuperado el 2016, de 802: <http://odysseus.ieee.org/query.html?qt=802&charset=iso-88591&style=standard&col=sa>
- Baide, b. (Junio de 2012). *Normas IEEE 802*?Qué es? Recuperado el 2016, de <http://es.slideshare.net/sirenita2/ieee-802-brenda-baide>
- Barajas, S. (2014). *Universidad Carlos III de Madrid*. Recuperado el Agosto de 2016, de Protocolos de seguridad en redes inalámbricas: <http://www.saulo.net/pub/inv/SegWiFi-art.htm>
- Barcayola, L. R. (5 de Diciembre de 2012). *Estandar IEEE 802.X*. Recuperado el Agosto de 2016, de Protocolos de Red I: <http://es.slideshare.net/LarryRuiz/estndar-ieee-802-15502942bdat>. (s.f.). *Seguridad en redes Inalámbricas: Una guía básica. WPA*. Recuperado el Mayo de 2015, de [http://www.bdat.net/seguridad\\_en\\_redes\\_inalambricas/x59.html](http://www.bdat.net/seguridad_en_redes_inalambricas/x59.html)
- Beatriz Gómez Suárez, J. M. (2010). *Universitat de les Illes Balears* . Recuperado el 2016 de Agosto, de Wireless MESH Networks : [http://ibdigital.uib.es/greenstone/collect/enginy/index/assoc/Enginy\\_2/010v02p0/09.dir/Enginy\\_2010v02p009.pdf](http://ibdigital.uib.es/greenstone/collect/enginy/index/assoc/Enginy_2/010v02p0/09.dir/Enginy_2010v02p009.pdf)
- Benito, M. (5 de Julio de 2010). *Evaluación experimental de redes malladas basadas en el protocolo B.A.T.M.A.N*. Recuperado el 2016, de <http://e-archivo.uc3m.es/handle/10016/11159>
- Betsy Beltrán, Nicolas Sepuñlveda. (Abril de 2012). *Antena Biguad*. Recuperado el 2016, de <http://sistemascomunicacionales.blogspot.com.co/2012/04/primero-debemos-saber-losconocimientos.html>
- Bolivariana, U. P. (2014). *Topologia Redes MESH*. Recuperado el Agosto de 2016, de <http://eav.upb.edu.co/banco/sites/default/files/files/04CAPITULOS.pdf>
- Bravo González, Alberto G. (2008 de Julio). *Universidad* . Recuperado el Febrero de 2015, de Estudio de conocimiento en las Redes inalámbricas MESH: <http://cdigital.uv.mx/bitstream/123456789/29463/1/Bravo%20Gonzalez.pdf>
- Bravo, A. (Julio de 2008). *Estudio de Conocimiento en las Redes Inhalámbricas*. Recuperado el 2016, de Universidad Vercruzana: <http://cdigital.uv.mx/bitstream/123456789/29463/1/Bravo%20Gonzalez.pdf>



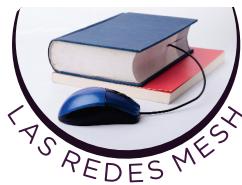
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Bravo, W. G. (Julio de 2008). *Universidad de Veracruz*. Recuperado el Agosto de 2016, de Estudio del Conocimiento en las Redes Inalambricas: <http://cdigital.uv.mx/bitstream/123456789/29463/1/Bravo%20Gonzalez.pdf>
- Brown Andrew. (Febrero de 2003). *IEEE 802.17 Resilient Packet Ring (RPR) Standards Update*, . Recuperado el Enero de 2015, de Cisco Systems, NANOG: <https://www.nanog.org/meetings/nanog27/presentations/brown.pdf>
- Buettrich, S. (Octubre de 2007). *Redes MESH*. Recuperado el 2016, de Unidad 13: [http://www.itrainonline.org/itrainonline/mmtk/wireless\\_es/files/13\\_es\\_redes\\_MESH\\_presentacion\\_v02.pdf](http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/13_es_redes_MESH_presentacion_v02.pdf)
- Bustamante Sánchez, R. (s.f.). *Universidad Autónoma del Estado de Hidalgo*. Recuperado el Abril de 2015, de Ataques en la seguridad en redes. Seguridad en Redes Capítulo 2,: <http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf>
- C, M. G. (s.f.). *Significado de rutear*. Obtenido de <http://www.significadode.org/rutar.htm>
- Camilo Astudillo, J. A. (2012). *Estudio preliminar para un sistema MESH*. Recuperado el Agosto de 2016, de Topologia de Malla en Red: [http://wiki.ead.pucv.cl/index.php/Red\\_MESH](http://wiki.ead.pucv.cl/index.php/Red_MESH)
- Camino, A., García, B., & Criado, S. (2016). *Redes Libres, Abiertas y Comunitarias*. Recuperado el 2016, de [http://www.lugro-MESH.org.ar/w/images/d/d4/Redes\\_libres\\_abiertas\\_y\\_comunitarias.pdf](http://www.lugro-MESH.org.ar/w/images/d/d4/Redes_libres_abiertas_y_comunitarias.pdf)
- Canchi Radhakrishna. (Marzo de 2011). *IEEE Standard 802.20 MBWA MobileBroadband Wireless Access Systems Supporting Vehicular Mobility*, . Recuperado el 2 de Febrero de 2015, de IEEE 802 Standards Workshop: [http://www.ieee802.org/minutes/2011-March/802%20workshop/IEEE\\_March2011-Workshop-IEEE80220](http://www.ieee802.org/minutes/2011-March/802%20workshop/IEEE_March2011-Workshop-IEEE80220)
- Carrillo Arellano Carlos Ernesto, Ramos Ramos Víctor Manuel. (s.f.). *Límites de la capacidad de redes inalámbricas multi-hop*. Recuperado el Abril de 2015
- CCM. (Julio de 2016). *WiMAX - 802.16 - Interoperabilidad mundial para acceso por micro*. Recuperado el 2016, de <http://es.ccm.net/contents/795-wimax-802-16-interoperabilidad-mundial-para-acceso-por-micro>
- CCM Benchmark Group. (Agosto de 2016). *kioskea. Categorías de redes*. Obtenido de Redes por cobertura: <http://es.ccm.net/contents/818-redes-inalámbricas>
- CETECOM. (2014 de Julio). *Frequencybandsfor medical data transmission*. Recuperado el 5 de Enero de 2015, de [http://www.cetecom.com/fileadmin/files/images/NEWSLETTER/NEWSLETTER\\_2014/Frequency\\_Bands\\_for\\_medical\\_data\\_transmission.pdf](http://www.cetecom.com/fileadmin/files/images/NEWSLETTER/NEWSLETTER_2014/Frequency_Bands_for_medical_data_transmission.pdf)
- ChowdhuryRahulSingha. (2013). *Journal of Mobile Network Communicacitons&Telematics*. Recuperado el Enero de 2015, de SourangsuBanerji, On IEE 802.11: Wireless LAN Technology: <http://arxiv.org/ftp/arxiv/papers/1307/1307.2661.pdf>
- Cika Electronica. (2016). *Productos Destacados*. Recuperado el 2016, de <http://www.cika.com/>
- CISCO (2016). *802.11N*. Recuperado el 2016, de <http://www.cisco.com/c/en/us/solutions/enterprise-networks/802-11n/index.html>
- CISCO. (2016). *CISCO*. Recuperado el Agosto de 2016, de WLAN: [http://www.cisco.com/c/es\\_es/solutions/mobility/wlan.html](http://www.cisco.com/c/es_es/solutions/mobility/wlan.html)
- CISCO. (2016). *Mobile Ad Hoc Networking*. Recuperado el 2016 de Agosto, de CISCO IOS IP MOBILITY: <http://www.cisco.com/c/en/us/products/ios-nx-os-software/mobile-ad-hoc-networking/index.html>



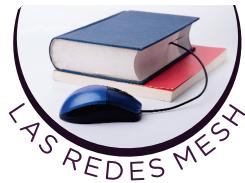
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Clausen T., Jacquet P., (Octubre de 2003). *Proyecto Hipercor, INRIA*. Recuperado el 2015, de <https://www.ietf.org/rfc/rfc3626.txt>
- Cloud Security Alliance,. (Diciembre de 2009). *CSA security Alliance, Security Guidance*. Recuperado el Abril de 2015, de <https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>
- Colemanres, J. (3 de Febrero de 2008). *estandaresieee802redes.blogspot*. Recuperado el Agosto de 2016, de Estándares IEEE 802: <http://estandaresieee802redes.blogspot.com.co/>
- Colnodo. (1993-2016). *Colnodo Uso estratégico de Internet para el desarrollo*. Recuperado el 22 de Septiembre de 2015, de <http://colnodo.org.co/apropiacionTecnologias.shtml>
- commentcamarche. (Julio de 2013). *Redes de Area Local*. Recuperado el 2016, de <http://static.commentcamarche.net/es.kioskea.net/pictures/wireless-imageswpan-wlan-wman-wwan.png>
- cs.nccu. (s.f.). *Hop-by-hop\_TCP*. Recuperado el 2015, de <http://www.cs.nccu.edu.tw/-lien/TALK/WiMoN/sensor1.gif>
- David J. Horat. (s.f.). *Secure Shell*. Recuperado el Mayo de 2015, de Ampliación de Sistemas Operativos - U.L.P.G.C. : <http://es.davidhorat.com/publicaciones/descarga/ssh-documento.pdf>
- De la Hoz, E., & De la Hoz, E. (2009). *IEEE802.20*. Recuperado el 2016
- decaWave. (2016). *IEEE802.15.4-2011 Standard*. Recuperado el 2016, de <http://www.decawave.com/technology/ieee802154a-standard>
- Delgado, H. (2009). *Redes Inalámbricas*. Macro.
- Díaz, R., & Castillo, L. (7 de Marzo de 2013). *Topologías de infraestructura de redes inalámbricas*. Recuperado el 2016, de <http://es.slideshare.net/dcesmas/topologas-de-infraestructura-de-redes-inalmbricas>
- DigiCert. (2003-2016). *Capa de conexión segura SSL*. Recuperado el Agosto de 2016, de ¿Qué es SSL?: <https://www.digicert.com/es/ssl.htm>
- Dignani Jorgue Pablo. (2011). *Análisis del protocolo ZigBee*. Recuperado el 2015 de Enero, de Universidad Nacional de la Plata: [http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes\\_y\\_Seguridad/Trabajos\\_Finales/Dignanni\\_docente.ucol.mx](http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Dignanni_docente.ucol.mx). (Septiembre de 2014). *CÓDIGO HDB3*. Recuperado el 2016, de [http://docente.ucol.mx/al000408/public\\_html/HDB3.html](http://docente.ucol.mx/al000408/public_html/HDB3.html)
- ecma International. (2008). *Standard ECMA-368*. Recuperado el 2016, de High Rate Ultra Wideband PHY and MAC Standard: <http://www.ecma-international.org/publications/standards/Ecma-368.htm>
- EcuRed. (2016). *Red inalámbrica MESH*. Recuperado el Agosto de 2016, de [http://www.ecured.cu/index.php/Red\\_inal%C3%A1lmbrica\\_MESH](http://www.ecured.cu/index.php/Red_inal%C3%A1lmbrica_MESH)
- EcuRed. (2016). *Red inalámbrica MESH*. Obtenido de [https://www.ecured.cu/index.php/Red\\_inal%C3%A1lmbrica\\_MESH](https://www.ecured.cu/index.php/Red_inal%C3%A1lmbrica_MESH)
- EcuRed. (2016). *Red inalámbrica MESH*. Recuperado el Agosto de 2016, de [https://www.ecured.cu/index.php/Red\\_inal%C3%A1lmbrica\\_MESH](https://www.ecured.cu/index.php/Red_inal%C3%A1lmbrica_MESH)
- edgaracredes. (Diciembre de 2013). *Mecanismos para la Seguridad*. Recuperado el 2016, de <https://edgaracredes.wordpress.com/2013/02/16/mecanismo-de-seguridad-de-lainstalacion-de-una-red/>

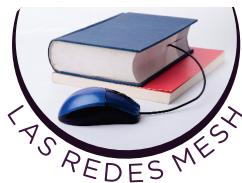


Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- ehusfera. (2010). *Identificación automática en SSH usando claves RSA*. Obtenido de <http://www.ehu.eus/ehusfera/ghym/2010/10/15/identificacion-automatica-en-ssh-usando-claves-rsa/>
- Emilio Monachesi, A. M. (2011). *Conceptos generales de Antenas*. Tucumán, Argentina: Editorial de la Universidad Tecnológica Nacional - edUTecNe .
- FACCE (13 de Diciembre de 1901). *Zona Virus*. Recuperado el Abril de 2015, de Que es Spoofing: <http://www.zonavirus.com/articulos/que-es-el-spoofing.asp>
- Felipe Muñoz, J. P. (Julio 28 de 2014). *REDES AD HOC*. UNIVERSIDAD TECNICA FEDERICO SANTA MARIA, Departamento de Electronica.
- ffmpeg.org. (s.f.). *About FFmpeg*. Recuperado el Agosto de 2016, de <https://ffmpeg.org/about.html>
- Flickenger, R. (s.f.). *Antenna on the Cheap (er, Chip)*. Recuperado el 2016, de [http://archive.oreilly.com/pub/post/antenna\\_on\\_theCheap\\_er\\_chip.html](http://archive.oreilly.com/pub/post/antenna_on_theCheap_er_chip.html)
- Flor, R. F. (Julio de 2007). *Universidad de San Carlos de Guatemala*. Recuperado el 7 de Enero de 2015, de Redes de área metropolitana inalámbricas como una alternativa para enlaces de última milla según el estándar IEEE 802.16: [http://biblioteca.usac.edu.gt/tesis/08/08\\_0199\\_EO.pdf](http://biblioteca.usac.edu.gt/tesis/08/08_0199_EO.pdf)
- Gabo, K. (10 de Junio de 2015). *gabogaby13*. Recuperado el Agosto de 2016, de Elementos de una red: <http://gabogaby13.blogspot.com.co/>
- Gálvez Serra, J. A., & Hincapié, R. C. (s.f.). *Las Redes Inalámbricas Ad-Hoc en la comunicación vehicular*. Medellin: Universidad Pontificia Bolivariana.
- Gamez, E., & Álvarez, F. (2010). Control de la Congestión en el IEEE 802.17. Nexo, *Revista Científica*, 1.
- gnuLinux. (2016). *Package: batman-adv-dkms (0.2-5)*. Recuperado el 2016, de DKMS Source for the batman-advanced kernel module: <http://packages.trisquel.info/es/taranis/batman-adv-dkms>
- Gómez, B., Maimó, J., & Merideño, J. (2009-2010). *Wireless MESH Networks*. Universitat de les Illes Balears.
- Gómez, J. (2016). *Administrador de Sistemas Operativos*. Recuperado el 2016, de Redes Inalambricas en modo Infraestructura: [http://www.adminso.es/index.php/1.1.\\_Redes\\_inal%C3%A1mbricas\\_en\\_modo\\_infraestructura](http://www.adminso.es/index.php/1.1._Redes_inal%C3%A1mbricas_en_modo_infraestructura)
- GONCALVES, M. (1997). Firewalls Complete. Beta Book. En [https://www.segu-info.com.ar/ataques/ataques\\_monitorizacion.htm](https://www.segu-info.com.ar/ataques/ataques_monitorizacion.htm). EE.UU.: McGraw Hill.
- González Valiñas Manuel. (5 de Mayo de 2006). *Seguridad en Redes 802.11x*. Recuperado el 4 de Enero de 2015, de [http://www.atc.uniovi.es/inf\\_med\\_gijon/3iccp/2006/trabajos/wifi/](http://www.atc.uniovi.es/inf_med_gijon/3iccp/2006/trabajos/wifi/)
- González, G. (5 de Junio de 2014). *Qué es un ataque Man in The Middle*. Recuperado el Agosto de 2016, de <http://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/>
- Granada, U. d. (s.f.). *Redes de área local, Transmisión de datos y redes de ordenadores*. Recuperado el Enero de 2015, de Departamento de Ciencias de la computación e I.A: <http://elvex.ugr.es/decsai/internet/pdf/5%20LAN.pdf>
- Gregorio Prieto. (Noviembre de 2012). *Ataques y contramedidas en sistemas personales* diapositiva 6. Recuperado el 2016, de <https://vicentesanchez90.files.wordpress.com/2012/12/ataques-y-contramedidas-ensistemas-personales.pptx>

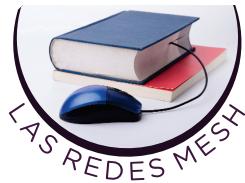


- Gregorio Prieto. (Noviembre de 2012). *Ataques y contramedidas en sistemas personales* diapositiva 6. Recuperado el 2016, de <https://vicentesanchez90.files.wordpress.com/2012/12/ataques-y-contramedidas-ensistemas-personales.pptx>
- Grupo IEEE 802.22. (2015). *Standards for spectrum Sharing and White Spaces to Bridge Digital Divide*. Recuperado el 2015, de [http://www.itu.int/dms\\_pub/itu-r/oth/0c/06/ROC060000560010PDFE.pdf](http://www.itu.int/dms_pub/itu-r/oth/0c/06/ROC060000560010PDFE.pdf)
- gsyc-profes (arroba). (Noviembre de 2013). *Encaminamiento en Redes Ad-Hoc*. Recuperado el 2015, de Departamento de Sistemas Telemáticos y Computación (GSyC): [https://gsyc.urjc.es/~mortuno/rom/06-encaminamiento\\_adhoc.pdf](https://gsyc.urjc.es/~mortuno/rom/06-encaminamiento_adhoc.pdf)
- H. Katz, Frank. (s.f.). *Armstrong Atlantic State University. Department of Information, Computing, and .* Recuperado el Mayo de 2015
- Hackerfriendly. (2008). *Redes Inalámbricas en los Países en Desarrollo*. <http://hackerfriendly.com/>
- Hernandez, J. P. (2014). *Prototipo De Una Red MESH Con Protocolo De Enrutamiento Olsr*. Obtenido de Pontificia Bolivariana Seccional Bucaramanga: [https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiogbre8\\_rOAhVLSS YKHReNAjgQFggaMAA&url=http%3A%2F%2Fdocplayer.es%2F2302665-Prototipo-de-una-red-MESH-con-protocolo-de-enrutamiento-olsr-para-la-universidad-pontifi](https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiogbre8_rOAhVLSS YKHReNAjgQFggaMAA&url=http%3A%2F%2Fdocplayer.es%2F2302665-Prototipo-de-una-red-MESH-con-protocolo-de-enrutamiento-olsr-para-la-universidad-pontifi)
- howstuffworks. (2016). *Streaming Video*. Obtenido de <http://computer.howstuffworks.com/internet/basics/streaming-video%20and-audio4.htm>
- Hoy, Diario Electrónico (2001-2016). *Patron de Radiacion*. Recuperado el 2016, de <http://www.diarioelectronicohoy.com/>
- <http://wiki.bogota-MESH.org/>. (6 de Julio de 2016). *Página principal*. Recuperado el Agosto de 2016, de ¿QUÉ ES BOGOTA-MESH? : [http://wiki.bogota-MESH.org/index.php?title=P%C3%A1gina\\_principal](http://wiki.bogota-MESH.org/index.php?title=P%C3%A1gina_principal)
- ICECAST. (2011). */icecast-2.4.12*. Obtenido de Config: <http://icecast.org/docs/icecast-2.4.0/config-file.html>
- IEEE. (Septiembre de 1999). IEEE 802.11. *WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable)*.
- IEEE. (2016). *Institute of Electrical and Electronics Engineers*. Recuperado el Agosto de 2016, de About IEEE: <https://www.ieee.org/about/index.html>
- IEEE 802. (Febrero de 2008). *IEEE 802 Redes*. Obtenido de <http://estandaresieee802redes.blogspot.com/>
- IEEE 802. (s.f.). *ieee802*. Recuperado el Enero de 2015, de <http://www.ieee802.org/18/>
- IEEE Computer Society. (Mayo de 1998). *IEEE Standard for Information technology. Recuperado el 2015, de Part 2: Logical Link Control*: <http://www.signallake.com/publications/1998802.2LogicalLinkControl.pdf>
- Infyseg. (Noviembre de 2013). Obtenido de Ataque Man in the Middle: <http://infyseg.blogspot.com/2013/11/ataque-man-in-middle>
- Interlab. (2010). *¿Qué significa el protocolo HTTPS y cómo funciona?* Recuperado el Agosto de 2016, de [http://www.internetlab.es/post/888/que-significa-el-protocolo-https-y-IT46. \(2011\). Redes MESH. Recuperado el Agosto de 2016, de Redes MESH Presentacion: http://www.it46.se/courses/wireless/materials/es/13\\_RedesMESH/13\\_es\\_redes\\_MESH\\_presentacion\\_v01.pdf](http://www.internetlab.es/post/888/que-significa-el-protocolo-https-y-IT46. (2011). Redes MESH. Recuperado el Agosto de 2016, de Redes MESH Presentacion: http://www.it46.se/courses/wireless/materials/es/13_RedesMESH/13_es_redes_MESH_presentacion_v01.pdf)



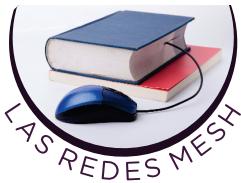
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- IT46. (s.f.). *Redes MESH*. Recuperado el Agosto de 2016, de Redes MESH Presentacion: [http://www.it46.se/courses/wireless/materials/es/13\\_RedesMESH/13\\_es\\_redes\\_MESH\\_presentacion\\_v01.pdf](http://www.it46.se/courses/wireless/materials/es/13_RedesMESH/13_es_redes_MESH_presentacion_v01.pdf)
- itpn.mx. (s.f.). *UnidadVI: Tecnologías inalámbricas*. Recuperado el Mayo de 2015, de [http://itpn.mx/recursosisc/7semestre/conmutaciony\(enrutamiento en redes de datos\)/Unidad%20III.pdf](http://itpn.mx/recursosisc/7semestre/conmutaciony(enrutamiento en redes de datos)/Unidad%20III.pdf)
- itrainonline.org. (2016). *Red MESH*. Recuperado el 2016, de <http://www.itrainonline.org/itrainonline/english/index.shtml>
- Jahangir, K. (Octubre de 2010). *Handover managemeth in GSM celularesystem*. Recuperado el 3 de Febrero de 2015, de <http://www.ijcaonline.org/volume8/number12/pxc3871763.pdf>
- Kharagpur. (s.f.). *TokenPassingc LANs*. Recuperado el 8 de Enero de 2015, de tomado de <http://nptel.ac.in/courses/117105076/pdf/5.4%20Lesson%2018%20.pdf>
- Kotsev, M. (2011). *Networks & Communications*. Recuperado el Enero de 2015, de <http://network-communications.blogspot.com/2011/06/802standards-ieee-8022-8023-8025-80211.html>
- Lara, R. (2015). *Evaluación de Protocolos de Enrutamiento usados en las Redes Móviles AdHoc (MANET), utilizando el software Network Simulator ns-2*. Recuperado el 2015, de [http://www.academia.edu/4734203/Evaluaci%C3%B3n\\_de\\_Protoxolos\\_de\\_Enrutamiento\\_usados\\_en\\_las\\_Redes\\_M%C3%BAviles\\_AdHoc\\_MANET\\_utilizando\\_el\\_software\\_Network\\_Simulator\\_ns-2](http://www.academia.edu/4734203/Evaluaci%C3%B3n_de_Protoxolos_de_Enrutamiento_usados_en_las_Redes_M%C3%BAviles_AdHoc_MANET_utilizando_el_software_Network_Simulator_ns-2)
- Largo, Y., Chen , J., & Qiang, N. (2017). NOMA- Enabled Cooperative Unicast- Multicast:Design and Outage Analysis. *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*(99), 1-20. doi: DOI 10.1109/TWC.2017.2754261
- Law David. (Marzo de 2001). *IEEE 802.3 Ethernet*. Recuperado el 8 de Enero de 2015, de [http://www.ieee802.org/minutes/2011March/802%20workshop/IEEE\\_802d3\\_Law\\_V1p1.pdf](http://www.ieee802.org/minutes/2011March/802%20workshop/IEEE_802d3_Law_V1p1.pdf)
- Lehembre Guillaume. (2006). *Seguridad Wi-fi-WEP, WPA y WPA 2*. Recuperado el Abril de 2015, de [http://www.hsc.fr/ressources/articles/hakin9\\_wifi/hakin9\\_wifi\\_ES.pdf](http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf)
- Leonardo Uzcátegu. (2012). *Seguridad en Redes Inalámbricas*. Recuperado el 2015, de <http://www.eslared.org.ve/walc2012/material/track4/Wireless/9-WLAN-Security.pdf>
- Lerones Fernández, L. (Enero de 2006). *Desarrollo de un analizador de red (Sniffer)*. Recuperado el 7 de Abril de 2015, de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/454/1/38443tfc.pdf>
- Lesta, F. A. (2006). <https://books.google.com.co/>. (Marcombo, Ed.) Recuperado el Agosto de 2016
- Maria, O. N. (23 de Enero de 2012). *Universidad del Valle de Guatemala*. Recuperado el Agosto de 2016, de Personal Area Network (PAN): <http://streaming.uvg.edu.gt/mediawiki/images/3/3f/PAN.pdf>
- Marks, Roger. (Abril de 2003). *The IEEE 802.16 WirelessMAN Standard for Broadband Wireless Metropolitan Area Networks*. Recuperado el 2015, de [https://www.ieee.li/pdf/viewgraphs/wireless\\_802\\_16.pdf](https://www.ieee.li/pdf/viewgraphs/wireless_802_16.pdf)
- Marleny Guzman C.. (2011). Obtenido de <http://www.significadode.org/rutear.htm>
- Marrone Luis. (2009 de Junio). *Facultad de Inforática Universidad Nacional de la Plata*. Recuperado el Enero de 2015, de Especialidad en Redes: [http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes\\_y\\_Seguridad/Trabajos\\_Finales/Luques.pdf](http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Luques.pdf)



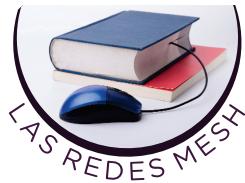
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Martinez, J. A. (2014). *Implementación modelo de red abierta tipo*. Cataluña: Universidad de Cataluña.
- Martinez, M. C. (2014). *Diseño e implementación de una red MESH como alternativa de solución para redes*. Bogota D.C.: Universidad Libre.
- Mas WIFI. (Mayo de 2012). *Redes MESH. ¿Qué son y cómo funcionan?* Obtenido de <http://www.maswifi.com/blog/2012/05/redes-MESH-que-son-y-como-funcionan/>
- Maya, I., & Molina, J. L. (2006). *Redes*. Recuperado el 2016, de Topología Malla Completa: <http://revista-redes.rediris.es/>
- McGarvey, J. (Julio de 12 de 2002). *What is it Good For?* Obtenido de War(chalking):: <http://www.wi-fiplanet.com/columns/article.php/1402401>.
- McKinnonBettye, Schultz Michael, Watson Josh, . (12 de Junio de 2006). *Wireless Network Security*. Recuperado el 9 de Enero de 2015, de [http://www.cs.fsu.edu/~burmeste/CIS4360/Fall2006/projectPresentations/wireless\\_security.pdf](http://www.cs.fsu.edu/~burmeste/CIS4360/Fall2006/projectPresentations/wireless_security.pdf)
- Memphis, L. (2010). *Principios de Administracion*. Publicaciones Universidad Autónoma de Colombia.
- Mendoza Acevedo, E. (Abril de 2005). *Universidad Tecnológica de la Mixteca*. Recuperado el Enero de 2015, de Implementación de un sistema de captura de paquetes en redes inalámbricas 802.11 y Bluetooth: [http://mixteco.utm.mx/~resdi/historial/Tesis/Tesis\\_Emanuel.pdf](http://mixteco.utm.mx/~resdi/historial/Tesis/Tesis_Emanuel.pdf)
- Mercado, A., & Berriós, R. (s.f.). *Redes inalámbricas ad hoc*. Recuperado el 2016, de <http://facultad.bayamon.inter.edu/cgonzalezr/elen4618/adhoc.pdf>
- MESHDynamic. (2010). *Performance Analysis of three MESH Networking* . Recuperado el Agosto de 2016, de MESH Dynamics: <http://MESHdynamics.com/%20performance-analysis.html>
- Microsoft Corp. (2003). *Windows Server 2003*. Obtenido de [http://msdn.microsoft.com/es-es/library/cc739465\(v=ws.10\).aspx](http://msdn.microsoft.com/es-es/library/cc739465(v=ws.10).aspx)
- Microsoft. (s.f.). *Microsoft TechNet*. Recuperado el Enero de 2015, de <http://technet.microsoft.com/es-es/co/library/cc755248.aspxconsultado>
- Miguel Ángel Landero Rodríguez. (2005). *Protocolo de Ruteo Híbrido para Redes Móviles Ad Hoc*. Instituto Politécnico Nacional.
- Ministerio de Educación, P. S. (2008). *¿Qué es el streaming?* Recuperado el Agosto de 2016, de <http://www.ite.educacion.es/formacion/materiales/107/cd/video/video0103.html>
- MinTic. (2010). *El Plan Vive Digital*. Recuperado el Agosto de 2016, de <http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html>
- MinTic. (2010-2014). *El Plan Vive Digital*. Recuperado el Agosto de 2016, de <http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html>
- Miranda, G. (2000). Como valorar proyectos de Tecnología Blanda. *Conferencia Universidad central de Caracas*. Caracas.
- Miranda, G. (2000). Como valorar proyectos de Tecnología Blanda. *Conferencia Universidad central de Caracas*. Caracas.
- MISO, ". I. (Abril de 2010). *Antena BCT*. Recuperado el 2016, de <http://misomantenimiento.blogspot.com.co/2010/04/lo-prometido-esdeudaantena-wi-fi.html>
- mitre Software Corporation. (2014). *Welcoma*. Obtenido de <http://www.mitresoftware.com/>



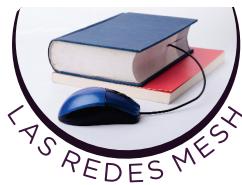
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Monachesi, E. (2011). *Conceptos generales de Antenas*. Tucumán Argentina: Editorial de la Universidad Tecnológica Nacional - edUTecNe.
- Navarro Gavira, Sara. (2006). *Algoritmos cross-layer para la optimización de las prestaciones del tcp en redes wireless ad-hoc*. Recuperado el 2016, de <http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F07++Capitulo+2.pdf>
- Nodalis.es. (2008). *Nodalis.es*. Recuperado el Agosto de 2016, de ¿Por qué una red MESH?: <http://www.nodalis.es/sobre-nodalismesh-o-mallada.htm>
- Opennet. (1996-2006). *Interworking Technology*. Recuperado el 2015, de [http://www.opennet.ru/docs/RUS/Cisco\\_ITO/6.html](http://www.opennet.ru/docs/RUS/Cisco_ITO/6.html)
- Pablo Jara Werchau, Patricia Nazar. (2009). *Estándar IEEE 802.11X de las WLAN*. Recuperado el 2016, de [http://www.edutecne.utn.edu.ar/monografias/standard\\_802\\_11.pdf](http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf)
- Pascua, A. E. (Octubre de 2007). *Unidad 02: Estándares en Tecnologías Inalámbricas*. Recuperado el Agosto de 2016, de [http://www.itrainonline.org/itrainonline/mmtk/wireless\\_es/files/02\\_es\\_estandares-inalambricos\\_guia\\_v02.pdf](http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf)
- Pascual Esudero Alberto. (Octubre de 2007). Recuperado el Enero de 2015, de *Estándares en tecnologías Inalámbricas*: [http://www.itrainonline.org/itrainonline/mmtk/wireless\\_es/files/02\\_es\\_estandares-inalambricos\\_guia\\_v02.pdf](http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf)
- Pellejero I., A. F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica*. Recuperado el 17 de Agosto de 2016, de <https://books.google.com.co/>.
- Peng, S., & Sy, S. (2003). A general simulation environment for IP mobility. *IEEE SIMULATION CONFERENCE*. doi:10.1109 / WSC.2002.1166505
- Pérez González Tania, Granados Bayona Ginés, . (s.f.). *Redes MESH*. Obtenido de Universidad de Almería: [http://www.adminso.es/recursos/Proyectos/PFM/2010\\_11/PFM\\_MESH\\_presentacion.pdf](http://www.adminso.es/recursos/Proyectos/PFM/2010_11/PFM_MESH_presentacion.pdf)
- Pérez, T., & Granados, I. (Noviembre de 2010). *Universidad de Almería*. Recuperado el 2016, de Redes MESH: [http://www.adminso.es/recursos/Proyectos/PFM/2010\\_11/PFM\\_MESH.pdf](http://www.adminso.es/recursos/Proyectos/PFM/2010_11/PFM_MESH.pdf)
- Perkins, C. E., & Royer, E. M. (25 de Febrero de 1999). Ad hoc On-Demand distance vector routing. *IEEE Computer Society Washington*, 1991-1997. Recuperado el 5 de octubre de 2017
- Phatak, P. (28 de Diciembre de 2011). *Cyber Attacks Explained: Packet Spoofing*. Obtenido de <http://www.opensourceforu.com/2011/12/cyber-attacks-explainedhttp://www.opensourceforu.com/2011/12/cyber-attacks-explained-packet-spoofing/packet-spoofing/>
- Pietrosemoli, E. (2011). *Redes en MESH* . Recuperado el Agosto de 2016, de (Topología de Malla) : [http://eslared.net/walcs/walc2011/material/track1/redes\\_MESH\\_presentacion\\_es.pdf](http://eslared.net/walcs/walc2011/material/track1/redes_MESH_presentacion_es.pdf)
- PietrosemoliErmanno. (Octubre de 2011). *Redes en MESH (Topología de Malla)*. Recuperado el Febrero de 2015, de [http://www.eslared.org.ve/walcs/walc2011/material/track1/redes\\_MESH\\_presentacion\\_es.pdf](http://www.eslared.org.ve/walcs/walc2011/material/track1/redes_MESH_presentacion_es.pdf)
- Prawda, J. (2004). *Investigación de Operaciones Volumen I*. Addison Wesley.
- Princeton University, D. o. (Febrero de 1997). <http://www.zonavirus.com/>. Recuperado el 2016 de Agosto, de <http://www.zonavirus.com/articulos/que-es-el-spoofing.asp>



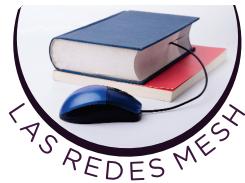
Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- QWERTY, U. (7 de Enero de 2010). <http://es.slideshare.net/>. Recuperado el Agosto de 2016, de <http://es.slideshare.net/DavlcHoJD/redes-inalambricas-wlan>
- Ramírez, A. (2014). *NORMA IEEE 802*. Recuperado el 2016, de <http://andersonramirez.tripod.com/ieee802.htm>
- RedesZone. (s.f.). QoS. Recuperado el 2016, de Calidad de Servicio: <http://www.redeszone.net/redes/qos-y-control-de-ancho-de-banda-como-funciona-deforma-interna/>
- Rheault, H. (2002). *Toma de decisiones Administrativas*. Editorial Limusa.
- Rizo, A.-A. P. (Marzo de 2011). *Modulación delta*. Recuperado el 2016, de <http://es.slideshare.net/AvalloAvalonPichardoRizo/modulacion-delta>
- Roberto Vignoni José. (2007). *Bluetooth, Instrumentación y Comunicaciones Industriales*. Recuperado el 14 de Enero de 2015, de <http://www.ing.unlp.edu.ar/electrotecnia/procesos/transparencia/Bluetooth.pdf>
- Rodríguez Eduardo; Deco Claudia; Burzacca Luciana; Petinari Mauro, . (2000). *Protocolos de encaminamiento para Redes malladas Inalámbricas*. Recuperado el 2015, de [http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento\\_completo.pdf?sequence=1](http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento_completo.pdf?sequence=1)
- Romero, M. C. (2003/2004). *Seguridad en Redes y Protocolos Asociados*. Recuperado el Agosto de 2016, de <http://www.dte.us.es/>: <http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf>
- Ruiz, J. C. (Agosto de 2004). *Redes Inalámbricas. Estándares y mecanismos de seguridad*. Recuperado el Agosto de 2016, de Enterate en Linea: <http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm>
- Sanmiguel, O. J. (2015). *Universidad Nacional de Rosario Facultad de Ciencias Exactas, Ingeniería y Agrimensura*. Recuperado el Agosto de 2016, de Redes Móviles Ad-Hoc.
- Schneier Bruce. (s.f.). *Cryptanalysis of Microsoft's Point-to-Point TunnelingProtocol (PPTP)*. Recuperado el Mayo de 2015, de <https://www.schneier.com/paper-pptp.pdf>
- Seguridad. Rinuex. (s.f.). *Laboratorio WiFi*. Recuperado el 2016, de <https://rinuex.unex.es/modules.php?op=modload&name=Textos&file=index&serid=39>
- Sevilla MESH. (Julio de 2010). *sevillaMESH.wordpress.com*. Obtenido de esquema de una red Ad-HOC: <http://sevillaMESH.wordpress.com/2011/02/22/origenes-de-las-redesMESH-i-las-primeras-redes-ad-hoc/>
- Sevilla MESH. (22 de Febrero de 2011). *Red inalámbrica abierta y libre de Sevilla*. Recuperado el Agosto de 2016, de Origenes de las redes MESH y las primeras redes ad hoc: <https://sevillaMESH.wordpress.com/2011/02/22/origenes-de-las-redes-MESH-i-las-primerasredes-ad-hoc/>
- Sevilla MESH. (5 de Febrero de 2014). *Orígenes de las redes MESH I: las primeras redes ad-hoc*. Recuperado el 22 de Mayo de 2015, de Red inalámbrica abierta y libre de Sevilla: <https://sevillaMESH.wordpress.com/2011/02/22/origenes-de-las-redes-MESH-i-las-primeras-redes-ad-hoc/>
- Sistemas Informaticos S.A.S. (s.f.). *Redes MESH*. Obtenido de <http://www.grssistemas.com.ar/productos-servicios.htm>
- Smaldone, Javier. . (Enero de 2004). *Introducción a Secure Shell*. Recuperado el Mayo de 2015, de [http://es.tldp.org/Tutoriales/doc-ssh-intro/introduccion\\_ssh-0.2.pdf](http://es.tldp.org/Tutoriales/doc-ssh-intro/introduccion_ssh-0.2.pdf)

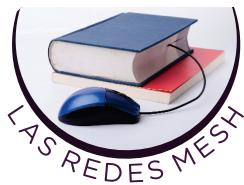


Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- SniferL4bs. (2015). *WEP para Cifrar y Desifrar*. Obtenido de <http://www.sniferl4bs.com/2012/09/seguridad-en-redes-inalambricas>
- Solutek Informática. (2016). *Redes Inalámbricas*. Recuperado el Agosto de 2016, de Servicio de Instalación Redes Inalámbricas: [http://www.solutekcolombia.com/redes\\_inalambricas.htm](http://www.solutekcolombia.com/redes_inalambricas.htm)
- Soy Periodista. (2014). Recuperado el Agosto de 2016, de Redes MESH: <http://www.soyperiodista.com/tecnologia/nota592-redes-MESH>
- Suarez Gomez Beatriz, Quetglas Maimó Javier, Medireño Garcia Juan,. (2010). *Universitat de les Illes Balears.*, Obtenido de WirelessMESH Networks: <http://enginy.uib.es/index.php/enginy/article/download/48/30>
- surfability. (04 de 2015). *surfability.com*. Obtenido de Estructura de una red: <http://www.surfability.com/images/MESHAP.gif>
- Tanenbaum, A. S. (2012). *Redes de Computadoras*. Mexico: Pearson.
- techopedia. (2016). *Pulse Code Modulation (PCM)*. Recuperado el 2016, de <https://www.techopedia.com/definition/24128/pulse-code-modulation-pcm>
- Tecno Empresarial. (2009-2010). *Redes MESH*. Recuperado el Abril de 2015, de [http://tecnoempresarial.com.mx/ri\\_certified.html](http://tecnoempresarial.com.mx/ri_certified.html)
- Tejedor, R. J. (2004). *UWB (Ultra Wide-Band)*. Recuperado el 2016, de <http://www.ramonmillan.com/tutoriales/ultrawideband.php>
- Teleco. (2016). *Red Inalámbrica Metropolitana*. Recuperado el 2016, de [http://www.teleco.com.br/imagens/tutoriais/tutorialmercwimax\\_figura4.gif](http://www.teleco.com.br/imagens/tutoriais/tutorialmercwimax_figura4.gif)
- Thaler Patricia. (10 de Marzo de 2013). *IEEE 802.1Q Media Access Control Bridges and Virtual Bridged Local Areanebowrks*. Recuperado el 7 de Enero de 2015, de <https://www.ietf.org/meeting/86/tutorials/86-IEEE-8021-Thaler.pdf>
- ThatcherJonatha. (s.f.). *Standards and Tecnology, World Wide Packets*. Recuperado el Enero de 2015, de Ethernet Tutorial: <http://bkarak.wizhut.com/www/lectures/networks-07/ethernet.pdf>
- the office network. (s.f.). *Red WPAN*. Recuperado el 2016, de <http://www.theofficenetwork.co.uk/wp-content/uploads/2014/08/pan.jpg>
- Tinajero, L. (22 de Febrero de 2011). *Topologías inalámbricas Ad-hoc e Infraestructura*. Recuperado el 2016, de <http://manejoredes.blogspot.com.co/2011/02/topologias-inalambricas-ad-hoc-e.html>
- Tomasi, W. (2003). *sistemas de comunicaciones*. Pearson.
- Toshiba. (s.f.). *Conozca la banda ancha WWAN ¿Qué supone para el profesional móvil?* Recuperado el 7 de Enero de 2015, de [http://escomputers.toshiba-europe.com/Contents/Toshiba\\_es/ES/WHITEPAPER/files/2006-09-WWAN-forbusiness-ES.pdf](http://escomputers.toshiba-europe.com/Contents/Toshiba_es/ES/WHITEPAPER/files/2006-09-WWAN-forbusiness-ES.pdf)
- Uivers-spb. (s.f.). *Distribucion de Canales Normas IEEE 802.11*. Recuperado el 2015, de [http://www.univers-spb.ru/images/cisco/antennas/ccmigration\\_09186a008008883b\\_09186a0080722f45-110.jpg](http://www.univers-spb.ru/images/cisco/antennas/ccmigration_09186a008008883b_09186a0080722f45-110.jpg)
- Unipamplona. (s.f.). *Unipamplona*. Recuperado el 2016 de Agosto, de Revista: [http://plataforma4.unipamplona.edu.co/unipamplona/portallG/home\\_40/recursos/01\\_general/revista\\_3/13102011/08.pdf](http://plataforma4.unipamplona.edu.co/unipamplona/portallG/home_40/recursos/01_general/revista_3/13102011/08.pdf)



- Universidad Abierta y a Distancia. (s.f.). *Topología Red Ad-HOC*. Recuperado el 2015, de [http://dataoteca.unad.edu.co/contenidos/2150509/Contenido\\_en\\_linea/53696e5f74c3ad74756c6f11.png](http://dataoteca.unad.edu.co/contenidos/2150509/Contenido_en_linea/53696e5f74c3ad74756c6f11.png)
- Universidad de Alcalá. (2011-2012). *REDES DE COMPUTADORES*. Recuperado el 2016, de Protocolos de enrutamiento dinámico RIP y OSPF: [http://atc2.aut.uah.es/~jmruiz/Descarga\\_LE/Prac\\_3.ProtocolosEnrutamientoDinamico\\_RIP\\_y OSPF.pdf](http://atc2.aut.uah.es/~jmruiz/Descarga_LE/Prac_3.ProtocolosEnrutamientoDinamico_RIP_y OSPF.pdf)
- Universidad de Málaga. (2009). *FDDI: FIBER DISTRIBUTED DATA INTERFACE*. Recuperado el 2016, de <http://www.lcc.uma.es/~eat/services/fddi/fddi.htm>
- Universidad Nacional Abierta y a Distancia. (2014). *Lección 26: Características del protocolo SSL/TLS*. Recuperado el Mayo de 2015, de [http://dataoteca.unad.edu.co/contenidos/233011/233011Exe/leccin\\_26\\_caractersticas\\_del\\_protocolo\\_ssllts.html](http://dataoteca.unad.edu.co/contenidos/233011/233011Exe/leccin_26_caractersticas_del_protocolo_ssllts.html) consultado el día 30 de abril de 2015
- Universidad Pontificia Bolivariana. (2015). *Topología de Redes MESH*. Obtenido de <http://eav.upb.edu.co/banco/sites/default/files/files/04CAPITULOS.pdf>
- Universidad tecnológica de Pereira. (2008). *El Presente de las redes IP*. Recuperado el 9 de Enero de 2015, de <http://repositorio.utp.edu.co/dspace/bitstream/11059/1311/1/0046T172.pdf>
- Universidad Tecnológica Nacional. (2016). *Red en Topología*. Recuperado el 2016, de <http://www1.frm.uthn.edu.ar/menu/>
- valonso. (15 de noviembre de 2008). *el blog del informático*. Recuperado el Agosto de 2016, de LAS REDES INALAMBRICAS MESH: <http://blog-del-linformatico.blogspot.com.co/2008/11/las-redes-inalambricas-MESH.html>
- Villacañas, J. (Abril de 2015). *Así apagaron los Hackers la TV Pública Francesa*. Recuperado el Abril de 2015, de [www.cope.es/detalle/Asi-apagaron-los-Hackers-la-TV-ublica Francesa.html](http://www.cope.es/detalle/Asi-apagaron-los-Hackers-la-TV-ublica Francesa.html)
- Virginia. (Septiembre de 2010). *“INSEGURIDAD” INFORMÁTICA*. Recuperado el 2016, de <http://revolucioninformatica2010.blogspot.com.co/>
- Virtual Labs. (2014). *Red ad hoc Movil*. Obtenido de <http://virtual-labs.ac.in/cse28/ant/ant/7/theory/>
- web.mit.edu/. (s.f.). *Red Hat Enterprise Linux 4: Manual de referencia*. Recuperado el Agosto de 2016, de Capítulo 20. Protocolo SSH: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rh-es-4/ch-ssh.html>
- webopedia. (2014). *webopedia*. Obtenido de red MESH: <http://www.webopedia.com/TERM/I/iBGP.html>
- Werchau Jara Pablo, N. P. (s.f.). *Estándar IEEE 802.11X de las WLAN* Departamento de Ingeniería en . Recuperado el 4 de Enero de 2015, de Universidad Tecnológica Nacional - U.T.N: [http://www.edutecne.utm.edu.ar/monografias/standard\\_802\\_11.pdf](http://www.edutecne.utm.edu.ar/monografias/standard_802_11.pdf)
- WIFIDEL. (2016). *Red de Conexión por medio de Repetidor*. Recuperado el 2016, de [www.wifidel.com](http://www.wifidel.com)
- Wikipedia. (11 de Mayo de 2012). *MAS WIFI*. Recuperado el Agosto de 2016, de Redes MESH. ¿Qué son y cómo funcionan?: <http://www.maswifi.com/blog/2012/05/redes-MESH-que-son-y-como-funcionan/>
- Wikipedia, the free encyclopedia. (Septiembre de 2014). *Hybrid Wireless MESH Protocol*. Recuperado el Agosto de 2016, de [https://en.wikipedia.org/wiki/Hybrid\\_Wireless\\_MESH\\_Protocol](https://en.wikipedia.org/wiki/Hybrid_Wireless_MESH_Protocol)



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

Wikipedia.org. (25 de Diciembre de 2012). *¿Qué sabes sobre Anonymous?* Recuperado el 7 de Enero de 2015, de Principales ataques de Anonymous: <https://quesabesobreanonymous.wordpress.com/actividad-deanonymous/principales-ataques-de-anonymous/>

Wordpress. (16 de 02 de 2013). edgaracredes. Obtenido de mecanismos de seguridad para la instalacion de redes: <http://edgaracredes.wordpress.com/2013/02/16/mecanismo-de>

Xiph.Org. (2004-2014). *Icecast 2.4.0 Docs — Config File*. Recuperado el Agosto de 2016, de <http://icecast.org/docs/icecast-2.4.0/config-file.html>

Xiph.Org. (2014-2016). *About Icecast 2*. Recuperado el Agosto de 2016, de Icecast Release 2.4.3: <http://icecast.org/>

zero13wireless.(2002-2016).AntenaFrisko.Recuperadoel2016,dehttp://www.zero13wireless.net/showthread.php?501-Antena-Fisko-9-dBi-s-%28-tipo-MiniYagui-%29

ac.usc.es. (3 de septiembre de 2016). Recuperado en agosto de 2016 de [http://www.ac.usc.es/docencia/ASRII/Tema\\_3html/node3.html](http://www.ac.usc.es/docencia/ASRII/Tema_3html/node3.html)

Andreu, F., Pellejero, I. y Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica*. Recuperado en agosto de 2016 de <https://books.google.com.co/>.

Arias, A., Peña, R. y Chávez, P. (Agosto de 2015). *Análisis comparativo en términos de capacidad y calidad de servicio de una PBX en código abierto, instalada en un enrutador inalámbrico y en un servidor tradicional usando Redes Inalámbricas MESH*. Repositorio de la Escuela Superior Politécnica del Litoral (Tesis Grado). Recuperado en 2016, de [https://www.researchgate.net/publication/277786852\\_Analisis\\_comparativo\\_en\\_términos\\_de\\_capacidad\\_y\\_calidad\\_de\\_servicio\\_de\\_una\\_pbx\\_en\\_codigo\\_abierto\\_instalada\\_en\\_un\\_enrutador\\_inalambrico\\_y\\_en\\_un\\_servidor\\_tradicional\\_usando\\_redes\\_inalambricas\\_MESH](https://www.researchgate.net/publication/277786852_Analisis_comparativo_en_términos_de_capacidad_y_calidad_de_servicio_de_una_pbx_en_codigo_abierto_instalada_en_un_enrutador_inalambrico_y_en_un_servidor_tradicional_usando_redes_inalambricas_MESH)

Association, I.-S. (2016). *IEEE Standards*. Recuperado en 2016 de <http://odysseus.ieee.org/query.html?qt=802&charset=iso-88591&style=standard&col=sa>

Baide, B. (Junio de 2012). *Normas IEEE 802 ¿Qué es?* Recuperado en 2016 de <http://es.slideshare.net/sirenita2/ieee-802-brenda-baide>

Benito, M. (5 de Julio de 2010). *Evaluación experimental de redes malladas basadas en el protocolo B.A.T.M.A.N.* Recuperado en 2016 de <http://e-archivo.uc3m.es/handle/10016/11159>

Bravo, A. (Julio de 2008). *Estudio del Conocimiento en las Redes Inalámbricas MESH*. (Monografía). Recuperado en agosto de 2016 de <http://cdigital.uv.mx/bitstream/123456789/29463/1/Bravo%20Gonzalez.pdf>

Camino, A., García, B. y Criado, S. (2016). *Redes Libres, Abiertas y Comunitarias*. Recuperado en 2016 de [http://www.lugro-MESH.org.ar/w/images/d/d4/Redes\\_libres\\_abiertas\\_y\\_comunitarias.pdf](http://www.lugro-MESH.org.ar/w/images/d/d4/Redes_libres_abiertas_y_comunitarias.pdf)

CCM Benchmark Group. (Agosto de 2016). *Kioskea. Categorías de redes*. Recuperado de: <http://es.ccm.net/contents/818-redes-inalambricas>

Cika Electrónica. (2016). *Productos Destacados*. Recuperado en 2016 de <http://www.cika.com/>



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- CISCO. (2016). *802.11N*. Recuperado en 2016 de <http://www.cisco.com/c/en/us/solutions/enterprise-networks/802-11n/index.html>
- De la Hoz, E. y De la Hoz, E. (2009). *IEEE802.20*. Recuperado en 2016 de
- Delgado, H. (2009). *Redes Inalámbricas*. Lima: Editorial Macro.
- Diario Electrónico Hoy. (2001-2016). *Patrón de Radiación*. Recuperado en 2016 de <http://www.diarioelectronicohoy.com/>
- Diaz, R. y Castillo, L.. (7 de Marzo de 2013). *Topologías de infraestructura de redes inalámbricas*. Recuperado en 2016 de <http://es.slideshare.net/dcesmas/topologas-de-infraestructura-de-redes-inalambricas>
- DigiCert. (2003-2016). *Capa de conexión segura SSL*. Recuperado en agosto de 2016 de <https://www.digicert.com/es/ssl.htm>
- EcuRed. (2016). *Red inalámbrica MESH*. Recuperado en agosto de 2016 de [http://www.ecured.cu/index.php/Red\\_inal%C3%A1mbrica\\_MESH](http://www.ecured.cu/index.php/Red_inal%C3%A1mbrica_MESH)
- Gamez, E. y Álvarez, F. (2010). Control de la Congestión en el IEEE 802.17. *Nexo, Revista Científica 1*.
- gnuLinux. (2016). *Package: batman-adv-dkms (0.2-5)*. DKMS Source for the batman-advanced kernel module. Recuperado en 2016 de <http://packages.trisquel.info/es/taranis/batman-adv-dkms>
- Gómez, B., Maimó, J. y Medireño, J. (2010). *Wireless MESH Networks*. Recuperado de <http://enginy.uib.es/index.php/enginy/article/download/48/30>
- Gómez, J. (2016). *Administrador de Sistemas Operativos. Redes Inalámbricas en modo Infraestructura*. Recuperado en 2016 de [http://www.adminso.es/index.php/1.1.\\_Redes\\_inal%C3%A1mbricas\\_en\\_modo\\_infraestructura](http://www.adminso.es/index.php/1.1._Redes_inal%C3%A1mbricas_en_modo_infraestructura)
- González, G. (5 de junio de 2014). *Qué es un ataque Man in The Middle*. Recuperado en agosto de 2016 de <http://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/>
- Hackerfriendly. (2008). *Redes Inalámbricas en los Países en Desarrollo*. Recuperado de <http://hackerfriendly.com/>
- Hussein, H. (2010). *Implementation and Performance Measurement and Analysis of OLSR Protocol*. (Tesis de grado). Recuperado de <https://ir.library.oregonstate.edu/xmlui/bitstream/handle/1957/15012/sinkyh.fi%20nal.ms.thesis.pdf?sequence=1>
- IEEE (Institute of Electrical and Electronics Engineers) . (Septiembre de 1999). *IEEE 802.11 WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable)*.
- IEEE 802 LAN/MAN. (Julio de 2016). *IEEE 802 LAN/MAN Standards Committee*. Recuperado en 2016 de <http://www.ieee802.org/>
- Infyseg. (Noviembre de 2013). *Ataque Man in the Middle*. Recuperado de <http://infyseg.blogspot.com/2013/11/ataque-man-in-middle>
- Interlab. (2010). *¿Qué significa el protocolo HTTPS y cómo funciona?* Recuperado en agosto de 2016 de <http://www.internetlab.es/post/888/que-significa-el-protocolo-https-y>
- Maya, I. y Molina, J. (2006). *Redes. Topología Malla Completa*. Recuperado en 2016 de <http://revista-redes.rediris.es/>
- McGarvey, J. (Julio de 12 de 2002). *What is it Good For? War(chalking)*. Recuperado de <http://www.wi-fiplanet.com/columns/article.php/1402401>
- Mercado, A., Berríos, R. (s.f.). *Redes inalámbricas ad hoc*. Recuperado en 2016 de <http://facultad.bayamon.inter.edu/cgonzalezr/elen4618/adhoc.pdf>



Fredys A. Simanca H. • Fabián Blanco Garrido • Eduardo Triana Moyano

- Microsoft Corp. (2003). *Windows Server 2003*. Recuperado de [http://msdn.microsoft.com/es-es/library/cc739465\(v=ws.10\).aspx](http://msdn.microsoft.com/es-es/library/cc739465(v=ws.10).aspx)
- MinTic. (2010-2014). *El Plan Vive Digital*. Recuperado en agosto de 2016 de <http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html>
- Pérez, T., Granados I. (2010). *Redes MESH*. Universidad de Almería. Recuperado de [http://www.adminso.es/recursos/Proyectos/PFM/2010\\_11/PFM\\_MESH\\_presentation.pdf](http://www.adminso.es/recursos/Proyectos/PFM/2010_11/PFM_MESH_presentation.pdf)
- Phatak, P. (28 de diciembre de 2011). *Cyber Attacks Explained: Packet Spoofing*. Princeton University, Department of Computer Science. (Febrero de 1997). *Qué es el spoofing*. Recuperado en agosto de 2016 de <http://www.zonavirus.com/articulos/que-es-el-spoofing.asp>
- Qwerty, U. (7 de Enero de 2010). *Redes inalámbricas WLAN*. Recuperado en agosto de 2016 de <http://es.slideshare.net/DavlcHoJD/redes-inalambricas-wlan>
- Ramírez, A. (2014). *Norma IEEE 802*. Recuperado en 2016 de <http://andersonramirez.tripod.com/ieee802.htm>
- Romero, M. C. (2003/2004). *Seguridad en Redes y Protocolos Asociados*. Recuperado en agosto de 2016 de <http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf>
- Ruiz, J. C. (Agosto de 2004). *Redes Inalámbricas. Estándares y mecanismos de seguridad*. Recuperado en agosto de 2016 de <http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm>
- Sentencia C-189 de 1194.
- Tanenbaum, A. S. (2012). *Redes de Computadoras*. Mexico: Pearson.
- Tinajero, L. (22 de febrero de 2011). *Topologías inalámbricas Ad-hoc e Infraestructura*. Recuperado en 2016 de <http://manejoredes.blogspot.com.co/2011/02/topologias-inalambricas-ad-hoc-e.html>
- Universidad de Alcalá. (2011-2012). *Redes de computadores. Protocolos de enrutamiento dinámico RIP y OSPF*. Recuperado en 2016 de [http://atc2.aut.uah.es/~jmruiz/Descarga\\_LE/Prac\\_3.ProtocolosEnrutamientoDinamico\\_RIP\\_y OSPF.pdf](http://atc2.aut.uah.es/~jmruiz/Descarga_LE/Prac_3.ProtocolosEnrutamientoDinamico_RIP_y OSPF.pdf)
- Universidad Tecnológica Nacional. (2016). *Red en Topología*. Recuperado en 2016 de <http://www1.frm.utn.edu.ar/menu/>
- WIFIDEL. (2016). *Red de Conexión por medio de Repetidor*. Recuperado en 2016 de [www.wifidel.com](http://www.wifidel.com)
- Wndw.net. (2006). Redes inalámbricas en los países en desarrollo. Recuperado de <http://wndw.net/pdf/wndw2-es/wndw2-es-ebook.pdf>
- Wordpress. (16 de febrero de 2013). *Edgaracredes. Mecanismos de seguridad para la instalación de redes*. Recuperado de <http://edgaracredes.w>

## Las Redes MESH

Se terminó de imprimir en junio de 2018.

Para su elaboración se utilizó papel bond blanco de 75 g en páginas interiores  
y papel esmaltado de 160 g para la carátula.

Las fuentes tipográficas empleadas son de la familia Gotham, en 12 puntos  
en texto corrido y 20 puntos en títulos.