

**IMPACTO SOBRE EL *STREAMING* DE AUDIO Y VIDEO DEL ACCESO
PROTEGIDO WPA Y WPA 2 EN REDES IEEE 802.11b/g
DURANTE EL *ROAMING*.**



Trabajo de Grado

**Eduardo Enrique Álvarez Ortega
Rodrigo Andrés Arce Sánchez**

**Director
M.Sc. Guefry Agredo Méndez.**

**Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo I+D Nuevas Tecnologías en Telecomunicaciones - GNTT
Línea de investigación: Gestión Integrada de Redes, Servicios y
Arquitecturas de Telecomunicaciones
Popayán 2009**

**IMPACTO SOBRE EL STREAMING DE AUDIO Y VIDEO DEL ACCESO
PROTEGIDO WPA Y WPA 2 EN REDES IEEE 802.11b/g
DURANTE EL *ROAMING*.**



Trabajo de Grado

**Eduardo Enrique Álvarez Ortega
Rodrigo Andrés Arce Sánchez**

**Trabajo para optar por el título de Ingeniero en Electrónica y
Telecomunicaciones**

**Director
M.Sc. Guefry Agredo Méndez.**

**Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo I+D Nuevas Tecnologías en Telecomunicaciones - GNTT
Línea de investigación: Gestión Integrada de Redes, Servicios y
Arquitecturas de Telecomunicaciones
Popayán 2009**

AGRADECIMIENTOS

A familiares los cuales fueron fuente de apoyo y aliento para la constancia, inspiración y ganas de triunfar.

La culminación de éste proceso de vida es un paso más para el desarrollo de habilidades y análisis que se presentaran en el pasar de los días.

Al compañero de trabajo, el director del proyecto de grado - *Guefry Leider Agredo Méndez* - el cual entregó tiempo significativo, paciencia, conocimiento y estrategia para poder cumplir uno de los sueños esperado por mucho tiempo.

A todos los ingenieros que fueron más amigos que profesores durante el proceso de aprendizaje.

**Muchas gracias por creer
Andrés Arce y Enrique Álvarez**

TABLA DE CONTENIDO

	INTRODUCCIÓN.....	1
1.	COMPONENTES DEL ESTÁNDAR IEEE 802.11	3
1.1.	DESCRIPCIÓN GENERAL.....	3
1.2.	COMPONENTES IEEE 802.11	4
1.3.	SEGURIDAD EN 802.11.....	7
1.3.1.	Acceso protegido Wi-Fi (WPA)	8
1.3.2.	Acceso Protegido Wi-Fi versión 2 – WPA 2	9
1.3.2.1	Proceso de autenticación.....	10
1.3.2.2	Gestión de llaves de cifrado.....	11
1.3.2.3	Llave precompartida (PSK).....	12
1.4.	MOVILIDAD EN Wi-Fi (<i>Roaming</i>)	12
1.4.1.	Asociación con los APs.....	12
1.4.2.	Tipos de <i>roaming</i>	14
1.4.3	La naturaleza de <i>roaming</i> en 802.11.....	14
1.4.4	Funcionamiento del <i>roaming</i>	15
1.4.5	Dominio de <i>roaming</i>	15
1.4.6	Duración del <i>roaming</i>	16
1.4.7	Algoritmos de <i>roaming</i>	17
1.4.8	Búsqueda de AP.....	17
1.4.8.1	Descubrimiento de AP preventivo	18
1.4.8.2	Descubrimiento de AP en el momento del <i>roaming</i>	19
1.4.9	Proceso de <i>roaming</i> en la capa 2.	19
1.5.	<i>STREAMING</i>	22
1.5.1	<i>Streaming</i> con precarga de <i>buffer</i>	22
1.5.2	<i>Streaming</i> en tiempo real.....	23
1.5.3	Percepción humana.....	24
1.5.4	Medición del desfase	25
1.5.5	Acumulación de retrasos	26
1.6	Transmisión de audio	27
1.7	Formato fuente del vídeo	29
1.5.3	Transmisión de video.....	31
1.5.4	Recepción de audio.....	34
1.6	FACTORES QUE INFLUYEN EN EL DESEMPEÑO DEL <i>STREAMING</i>	35
1.6.1	Análisis de los factores influyentes	35
1.6.1.1	Ancho de banda	36
1.6.1.2	Movilidad	36
1.6.1.3	<i>Roaming</i>	36
2	IMPACTO DEL <i>ROAMING</i> EN REDES 802.11b/g.....	38
2.1	INTRODUCCIÓN A LAS PRUEBAS EXPERIMENTALES	38
2.1.1	Plan de trabajo para la actividad base	38
2.2	INICIO DE LAS PRUEBAS EXPERIMENTALES	38
2.2.1	Requisitos mínimos	38
2.2.2	Estudio del ambiente propicio para el montaje.....	39
2.3	MONTAJE Y COMPROBACIÓN DEL <i>ROAMING</i> PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS SIN SEGURIDAD NI <i>STREAMING</i>	51

2.3.1	Montaje y verificación de la topología ESS	51
2.3.1.1	Estructura física BSS.....	52
2.3.1.2	Estructura lógica: Direccionamiento.....	52
2.3.1.3	Montaje BSS.....	53
2.3.2.1	Estructura física cliente móvil.....	53
2.3.2.2	Estructura lógica del usuario móvil:	53
2.3.2.3	Estructura lógica de la topología ESS.....	54
2.3.2.4	SSID.....	54
2.3.2.5	Configuración del Servidor DHCP.....	54
2.3.2.6	Potencia de transmisión.....	55
2.3.2.7	Ganancia de la antena.....	55
2.3.2.8	Configuración de seguridad	55
2.3.2.9	Modo de la red inalámbrica.....	55
2.3.2.10	Dirección IP del AP	55
2.3.2.11	Nombre del AP	55
2.3.3	Búsqueda de variables críticas en el desempeño del <i>roaming</i>	57
2.3.4	Análisis de resultados y generación de conclusiones	57
2.4	CONFIGURACIÓN Y VERIFICACIÓN DEL <i>ROAMING</i> PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS CON SEGURIDAD Y SIN <i>STREAMING</i>	58
2.4.1	Montaje de la topología ESS con seguridad y sin <i>streaming</i>	58
2.4.2	Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con la funcionalidad de <i>roaming</i>	60
2.4.3	Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con la funcionalidad de <i>roaming</i>	61
2.4.4	Búsqueda de variables críticas que influyen en el desempeño cuando hay <i>roaming</i> y seguridad	62
2.4.5	Análisis de resultados y generación de conclusiones	63
2.5	CONFIGURACIÓN Y VERIFICACIÓN DEL <i>ROAMING</i> PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS SIN SEGURIDAD Y CON <i>STREAMING</i>	66
2.5.1	Montaje de la topología ESS sin seguridad y con servidor de <i>streaming</i>	66
2.5.2	Estudio de desempeño del servicio de <i>streaming</i> en tiempo real en redes 802.11b/g	67
2.5.3	Estudio del desempeño del servicio de <i>streaming</i> en tiempo real durante el <i>roaming</i> en 802.11b/g.....	69
2.5.4	Análisis de resultados y generación de conclusiones	69
2.6	CONFIGURACIÓN Y VERIFICACIÓN DEL <i>ROAMING</i> PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS CON SEGURIDAD WPA Y CON <i>STREAMING</i>	69
2.6.1	Montaje de la topología ESS con seguridad WPA y servidor de <i>streaming</i>	69
2.6.2	Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con el servicio de <i>streaming</i> de audio con mayor y menor desempeño.....	70
2.6.3	Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con el servicio de <i>streaming</i> de video con mayor y menor desempeño.....	71
2.6.4	Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con el servicio de <i>streaming</i> de audio y video con mayor y menor desempeño.....	71
2.6.5	Análisis de resultados y generación de conclusiones	72

2.7	CONFIGURACIÓN Y VERIFICACIÓN DEL <i>ROAMING</i> PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS CON SEGURIDAD WPA 2 Y CON <i>STREAMING</i>	72
2.7.1	Montaje de la topología ESS con seguridad WPA 2 y servidor de <i>streaming</i>	72
2.7.2	Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con el servicio de <i>streaming</i> de audio con mayor y menor desempeño.....	73
2.7.3	Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con el servicio de <i>streaming</i> de video con mayor y menor desempeño.....	73
2.7.4	Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con el servicio de <i>streaming</i> de audio y video con mayor y menor desempeño.....	74
2.7.5	Análisis de resultados y generación de conclusiones	74
3	ANÁLISIS DEL ESTÁNDAR IEEE 802.11r	76
3.1	COMPARACIÓN DE LOS PROCESOS DE <i>ROAMING</i> CON Y SIN 802.11r.....	77
4	RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE UNA RED SEGURA Y DE CALIDAD PARA EL <i>STREAMING</i>	82
4.1	RECOMENDACIONES DE DISEÑO PARA LA TOPOLOGÍAS ESS EN REDES 802.11b/g	82
4.1.1	Análisis previo	82
4.1.2	Pruebas y verificación.....	84
4.2	RECOMENDACIONES PARA EQUILIBRAR LA IMPLEMENTACIÓN ENTRE SEGURIDAD Y <i>STREAMING</i> EN UNA TOPOLOGÍA ESS PARA REDES 802.11b/g	85
4.2.1	Implementación de seguridad.....	85
4.2.2	Implementación de <i>streaming</i> de audio y video soportada por VLC; Error! Marcador no definido	
4.2.3	Implementación de <i>roaming</i>	90
	CONCLUSIONES Y RECOMENDACIONES	91
	REFERENCIAS BIBLIOGRÁFICAS.....	95

LISTA DE FIGURAS

Figura 1-1 Componentes de IEEE 802.11.....	4
Figura 1-2 Conjunto de servicio básico.....	6
Figura 1-3 Conjunto de servicio extendido.....	7
Figura 1-4 Funcionamiento de 802.1x.....	10
Figura 1-5 Gestión y derivación de llaves en 802.11i.....	11
Figura 1-6 <i>Roaming</i> dentro de un dominio en la capa 2.....	15
Figura 1-7 <i>Roaming</i> a través de los diferentes dominios.....	16
Figura 1-8 Descubrimiento de AP preventivo.....	18
Figura 1-9 Descubrimiento de AP en el momento del <i>roaming</i>	19
Figura 1-10 Solicitud de envío de datos a una estación móvil.....	20
Figura 1-11 Pérdida de datos después de realizar el <i>roaming</i>	21
Figura 1-12 Actualización de las tablas de direcciones MAC.....	22
Figura 1-13 Capas de OSI para multimedia y 802.11.....	24
Figura 1-14 Recepción de los flujos sin sincronización.....	26
Figura 1-15 Acumulación del desfase de audio y vídeo.....	27
Figura 1-16 Procesamiento de fuente de audio y vídeo.....	27
Figura 1-17 Retrasos de audio.....	29
Figura 1-18 Secuencia vídeo entrelazado.....	30
Figura 1-19 Buffer de captura de vídeo.....	31
Figura 1-20 Retrasos en la captura y codificación del vídeo.....	31
Figura 1-21 Proceso para codificar 30 FPS vídeo.....	32
Figura 1-22 Procesamiento en el receptor.....	34
Figura 1-23 Acumulación de retardos en el proceso de recepción de audio.....	35
Figura 2-1 Escenario ESS.....	40
Figura 2-2 Estructura de traslape de los BSSs.....	41
Figura 2-3 Estructura con 0% de cobertura continua.....	42
Figura 2-4 Estructura con 5% de cobertura continua.....	42
Figura 2-5 Estructura con 50% de cobertura continua.....	43
Figura 2-6 Estructura con 65% de cobertura continua.....	43
Figura 2-7 Comparación de ancho de banda en 802.11g.....	44
Figura 2-8 Comparación de señal RSSI en 802.11g.....	44
Figura 2-9 Comparación de ancho de banda en 802.11b.....	45
Figura 2-10 Comparación de señal RSSI en 802.11b.....	45
Figura 2-11 Referencia de calidad de movilidad y calidad de <i>roaming</i>	48
Figura 2-12 Comparación de señal RSSI.....	49
Figura 2-13 Comparación de porcentaje de paquetes perdidos.....	50
Figura 2-14 Comparación de retardo.....	50
Figura 2-15 Distancia efectiva de <i>roaming</i> en 802.11b/g.....	51
Figura 2-16 Comparación de calidad de movilidad.....	52
Figura 2-17 Estructura de servicio extendido ESS.....	54
Figura 2-18 Configuración de la intensidad de movilidad.....	56
Figura 2-19 Verificación de <i>roaming</i> en 802.11g.....	56
Figura 2-20 Verificación de <i>roaming</i> en 802.11b.....	58
Figura 2-21 Topología ESS con seguridad y sin <i>streaming</i>	59
Figura 2-22 Paquetes básicos de conexión.....	62
Figura 2-23 Procesos de autenticación en redes inalámbricas.....	63
Figura 2-24 Diferencias del proceso de autenticación.....	64
Figura 2-25 Autenticación TLS en <i>roaming</i> con AP desconocido.....	64
Figura 2-26 Autenticación PEAP- MSCHAPV2 en <i>roaming</i> con AP desconocido.....	64

Figura 2-27 Autenticación TTLS en <i>roaming</i> con AP desconocido.....	65
Figura 2-28 Autenticación PSK en <i>roaming</i> con AP desconocido.....	65
Figura 2-29 Autenticación PEAP-GTC en <i>roaming</i> con AP desconocido.....	73
Figura 2-30 Configuración de seguridad WPA 2 en AP.....	70
Figura 3-1 Proceso de <i>roaming</i> en 802.11i (WPA 2)	78
Figura 3-2 Proceso de <i>roaming</i> con 802.11r.....	79
Figura 4-1 Referencia entre distancia y cobertura continua.....	83
Figura 4-2 Estructura de canales para el diseño.....	83
Figura 4-3 Verificación de conectividad.....	85
Figura 4-4 Campos de información para configuración de 802.11b/g.....	88
Figura 4-5 Proceso de <i>roaming</i> en la experimentación.....	89

ÍNDICE DE TABLAS

Tabla 1-1 Comparación ente WEP y WPA.....	9
Tabla 2-1 Requisitos básicos hardware.....	39
Tabla 2-2 Requisitos básicos <i>software</i>	39
Tabla 2-3 Selección de edificación.....	40
Tabla 2-4 Promedios del estudio de <i>roaming</i> en 802.11b.....	47
Tabla 2-5 Promedios del estudio de <i>roaming</i> en 802.11g.....	47
Tabla 2-6 Configuración del direccionamiento.....	52
Tabla 2-7 Calidad de movilidad y <i>roaming</i> en 802.11b.....	57
Tabla 2-8 Calidad de movilidad y <i>roaming</i> en 802.11g.....	57
Tabla 2-9 Composición de las pruebas de WPA con <i>roaming</i>	60
Tabla 2-10 Composición de las pruebas de WPA 2 con <i>roaming</i>	61
Tabla 2-11 Tiempo de reconexión de <i>streaming</i> para WPA.....	72
Tabla 2-12 Tiempo de reconexión de <i>streaming</i> para WPA 2.....	75
Tabla 3-1 Tiempos de <i>roaming</i> sin <i>streaming</i> en 802.11g.....	80
Tabla 3-2 Tiempos de <i>roaming</i> con <i>streaming</i> en 802.11g.....	80
Tabla 3-3 Tiempos de <i>roaming</i> sin <i>streaming</i> en 802.11b.....	80
Tabla 3-4 Tiempos de <i>roaming</i> con <i>streaming</i> en 802.11b.....	81
Tabla 3-5 Comparación de diferentes aspectos de 802.11 con 802.11r.....	81
Tabla 4-1 Combinaciones óptimas de seguridad.....	86
Tabla 4-2 Tolerancia a retardo y pérdida de paquetes para 802.11b/g.....	86
Tabla 4-3 Tiempo promedio de autenticación sin <i>roaming</i> para 802.11b/g.....	86
Tabla 4-4 Tiempo promedio de autenticación con <i>roaming</i> para 802.11b/g.....	87
Tabla 4-5 Pérdidas en <i>streaming</i> durante el <i>roaming</i> para 802.11b/g.....	90

LISTA DE APÉNDICES

- Apéndice A Herramientas de evaluación
- Apéndice B Estudio de movilidad
- Apéndice C Estudio de *roaming*
- Apéndice D Instalación y configuración de servidor RADIUS
- Apéndice E Estudio de seguridad y *roaming*
- Apéndice F Instalación y configuración de *streaming*
- Apéndice G Estudio de *roaming* con seguridad y *streaming*
- Apéndice H Actualización de *Firmware* para D-link (DIR 300)
- Apéndice I Propuestas de optimización de *streaming* en *roaming* para 802.11b/g

LISTA DE ANEXOS

- Anexo A Estándar IEEE 802.11r

ACRÓNIMOS

ACK	: Acknowledgement, Reconocimiento
AES	: Advanced Encryption Standard, Estándar de Cifrado Avanzado
AP	: Access Point, Punto de Acceso
ATSC	: Advanced Television Systems Committee, Comité de Sistemas Avanzados de Televisión.
BSS	: Basic Service Set, Conjunto de Servicio básico
BSSID	: Basic Service Set Identifier, Identificador de Conjunto de Servicio básico
BW	: Band Width, Ancho de banda
CCD	: Charge - Coupled Device, Dispositivo de Cargamentos Adyacentes
CCK	: Complementary Code Keying, Código Complementario
CCMP	: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, Protocolo
CRC	: Cyclic Redundancy Check, Comprobación de Redundancia Cíclica
CSMA/CA	: Carrier Sense Multiple Access/Collision Avoidance, Acceso Múltiple por Detección de Portadora con Evasión de Colisiones
DHCP	: Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de host
DS	: Distribution System, Sistema de Distribución
DSSS	: Direct Sequence Spread Spectrum, Espectro Ensanchado por Secuencia Directa
EAP	: Extensible Authentication Protocol, Protocolo de Autenticación Extensible
EAPOL	: Extensible Authentication Protocol over LAN, Protocolo de Autenticación Extensible sobre LAN
ESS	: Extended Service Set, Conjunto de Servicio Extendido.
FHSS	: Frequency Hopping Spread Spectrum, Espectro Ensanchado por Salto de Frecuencia
FIPS	: Federal Information Processing Standard, Estándar Federal de Procesamiento de información
FPS	: Frames Per Second, Cuadros por Segundo
FT	: Fast BSS Transition, Transición Rápida BSS.
FTC	: Fast BSS Transition Confirmation Frame, Trama de Confirmación FT.
FTIE	: Fast BSS Transition Information Element, Elemento de información FT
FTR	: Fast BSS Transition Request Frame, Trama de Petición FT
FTRR	: Fast Transition Resource Request, Petición de recursos FT
FTRES	: Fast BSS Transition Response Frame, Trama de respuesta FT
FTRRP	: FT Resource Request Protocol, Protocolo de petición de recursos FT
GOB	: Group Of Blocks, Grupo de Bloques
GSM	: Global System for Mobile Communications, Sistema Global para Comunicaciones Móviles.
GTC	: Generic Token Card, Tarjeta de Testigo Genérico
GTK	: Group Temporal Key, Llave Temporal de Grupo
HTTP	: Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto
IAPP	: Inter Access Point Protocol, Protocolo Inter Puntos de Acceso
IE	: Information Element, Elemento de Información
IR	: Infra Red, Infra Roja
IEEE	: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos.
IETF	: Internet Engineering Task Force, Grupo de Trabajo en Ingeniería de Internet

IP	: Internet Protocol, Protocolo Internet
IPTV	: Internet Protocol Television, Televisión IP
KCK	: Key Confirmation Key, Llave de Confirmación de Llave
KDF	: Key Derivation Function, Función de Derivación de Llave
KH	: Key Holder, Portador de Llave
L2	: Layer 2, Capa 2
L3	: Layer 3, Capa 3
MAC	: Medium Access Control, Control de Acceso al Medio
Mbps	: Mega bits per second, Un millón de bits por segundo
MD	: Mobility Domain, Dominio de Movilidad
MDID	: Mobility Domain Identifier, Identificador de Dominio de Movilidad
MDIE	: Mobility Domain Information Element, Elemento de Información de Dominio de Movilidad.
MIC	: Message Integrity Code, Código de Integridad de Mensaje
MK	: Master Key, Llave maestra
MMS	: Multimedia Streaming, Flujo de Multimedia
NIC	: Network Interface Card, Tarjeta de Interfaz de Red
NTSC	: National Television System Committee, Comité Nacional de Sistemas de Televisión
ODS	: Over the Distribution System, Sobre el Sistema de Distribución
ODSFTP	: Over the DS FT Protocol, Protocolo de Transición Rápida inter BSSs sobre el Sistema de Distribución
ODSFT	: Over the DS Fast BSS Transition, Transición Rápida inter BSSs sobre el Sistema de Distribución
OFDM	: Orthogonal Frequency Division Multiplexing, Multiplexación por División de Frecuencias Ortogonales.
OSI	: Open System Interconnection, Interconexión de Sistemas Abiertos
OTA	: Over the Air, Sobre el Aire
OTAFTP	: Over the Air FT Protocol, Protocolo de Transición Rápida inter BSSs sobre el Aire
OTAFT	: Over the Air Fast BSS Transition, Transición Rápida inter BSSs sobre el Aire
OTDS	: Over The Distribution System, Sobre el Sistema de Distribución
PAL	: Phase Alternating Line, Línea de Fase Alternada
PBCC	: Packet Binary Convolutional Coding, Codificación Convolutiva Binaria de Paquetes
PDA	: Personal Digital Assistant, Asistente Digital Personal
PEAP	: Protected Extensible Authentication Protocol, Protocolo Protegido de Autenticación Extensible.
PMK	: Pairwise Master Key, Llave Maestra de Pareja
PP	: Porcentaje de Pérdida de Paquetes
PPP	: Point to Point Protocol, Protocolo Punto a punto
PPR	: Pérdida de Paquetes en Roaming
PSK	: Pre Shared Key, Llave Pre Compartida
PTK	: Pairwise Transient Key, Llave Transiente de Pareja
PTKSA	: Pairwise Transient Key Security Association, Asociación de Seguridad PTK
QM	: Calidad de Movilidad
QoS	: Quality of Service
QR	: Calidad de Roaming
R	: Retardo
RF	: Radio Frequency, Radio Frecuencia

R0KH : PMK-R0 Key Holder, Portador de Llave PMK-R0
 R1KH : PMK-R1 Key Holder, Portador de Llave PMK-R1
 RADIUS : Remote Authentication Dial-In User Server, Servidor de Autenticación Remota Telefónico de Usuario.
 RC4 : Rivest Cipher 4, Cifrado Rivest 4
 RFC : Request For Comments, Petición de Comentarios
 RIC : Resource Information Container, Contenedor de Información de Recursos
 RSN : Robust Security Network, Red de Seguridad Robusta
 RSNIE : Robust Security Network Information Element, Elemento de Información RSN
 RSSI : Received Signal Strength Indicator, Indicador de Fuerza de Señal Recibida
 RTCP : Real-Time Control Transport Protocol, Protocolo de Control de Transporte de Tiempo Real
 RTMP : Real Time Messaging Protocol, Protocolo de Mensajería en Tiempo Real
 RTP : Real-time Transport Protocol, Protocolo de Transporte en Tiempo Real
 SA : Security Association, Asociación de Seguridad
 SECAM : Séquentiel Couleur à Mémoire, Color Secuencial con Memoria
 SSID : Service Set Identifier, Identificador de Conjunto de Servicio
 STA : Station, Estación
 STP : Spanning Tree Protocol, Protocolo de Apertura de Árbol
 TCP : Transmission Control Protocol, Protocolo de Control de Transmisión
 TDMA : Time Division Multiple Access, Acceso Múltiple por División de Tiempo
 TK : Temporal Key, Llave Temporal
 TKIP : Temporal Key Integrity Protocol, Protocolo de Integridad de Llave Temporal
 TLS : Transport Layer Security, Seguridad de Capa de Transporte
 TSN : Transitional Security Network, Red Segura Transicional
 TTLS : Tunneled Transport Layer Security, Seguridad de Capa de Transporte Tunelada
 UDP : User Datagram Protocol, Protocolo de Datagramas de Usuario
 U-NII : Unlicensed National Information Infrastructure, Infraestructura Nacional de Información Sin Licenciar
 UTP : Unshielded Twisted Pair, Cable de Par Trenzado Apantallado
 VLC : Video Lan Client, Cliente de Video Lan
 VoIP : Voice over IP, Voz sobre IP
 WEP : Wired Equivalent Privacy, Privacidad Equivalente a Cableado
 Wi-Fi : Wireless Fidelity, Fidelidad Inalámbrica
 WPA : Wi-Fi Protected Access , Acceso Protegido Wi-Fi

RESUMEN

El nacimiento de la tecnología inalámbrica incorporó al diario vivir posibilidades que facilitan muchas actividades. Abriendo la necesidad de comunicación a través de la transmisión de *streaming* de video y *streaming* de audio, surgiendo el inconveniente entre seguridad y el *roaming* en los dispositivos móviles. Los progresos mundiales por reducir la pérdida de paquetes durante las transmisiones multimedia en tiempo real son indispensables para brindar un nuevo servicio de uso cotidiano, capaz de competir con los servicios tradicionales existentes los cuales se brindan dentro de empresas, universidades y grandes ciudades.

La movilidad es una característica indispensable que combinada con nuevos servicios crea necesidades y problemas que deben ser minimizados o controlados, buscando las variables críticas que cambian la calidad deseada por los clientes móviles. La experimentación se enfoca en encontrar el grado de impacto de la seguridad sobre el *streaming* de audio y video en el momento del *roaming*.

El *roaming* involucra un algoritmo que evalúa el nivel de señal y el estado de la cobertura para la toma de decisiones, inmediatamente después de realizar la asociación al nuevo AP, el cliente solicita la autenticación generando pérdidas causadas por el tiempo que lleva la reautenticación 802.1x/EAP. Sólo sabiendo el efecto de las pérdidas y el retardo en el *streaming* se podrá encontrar un equilibrio configurable entre seguridad y *roaming*.

El estándar IEEE 802.11r estudia y sugiere una posible solución para aplicaciones que necesitan una transición transparente entre puntos de acceso. A partir de la comparación de lo obtenido en la experimentación frente a la propuesta establecida en el estándar 802.11r se generó una serie de recomendaciones de diseño, implementación y uso de la topología ESS con la posibilidad de transmisión de *streaming* enfocado a mantener el equilibrio entre seguridad, *streaming* y *roaming*.

INTRODUCCIÓN

Wi-Fi en sus inicios surgió como una tecnología meramente para servicios muy básicos, así que no había un requerimiento muy grande o exigente en las velocidades de transmisión. Pero con el paso de los años y los nuevos desarrollos de la tecnología inalámbrica, se ha llegado a unos niveles muy superiores de transmisión, que con el mejoramiento en velocidad y creación de elementos de seguridad más robustos han hecho que esta tecnología pueda ser usada de una manera confiable por sectores en los cuales se puede aprovechar más estas nuevas capacidades pasando a niveles mucho más críticos y complejos que una simple red casera.

Dentro de los servicios multimedia que se ofrecen hoy en día están los de *streaming* de audio y video en tiempo real, en el proyecto se trabajó con una emisora de transmisión en vivo y un dispositivo de captura de video también en tiempo real, ya que, en la transmisión de contenido pregrabado es más factible que se soporten cortes abruptos y más largos de la información, más de lo que soportaría, por motivos de calidad una transmisión en vivo de audio o video. Al unirse el *streaming* con la tecnología de transmisión de datos inalámbrica, y a su vez con la movilidad de usuario se ofrece comodidad y flexibilidad para el usuario final, pero no es totalmente transparente como se desea, debido al problema asociado al retardo y la pérdida de paquetes cuando se realiza una transición de una celda a otra (*roaming*), más aun cuando se tienen procesos de autenticación de los modernos esquemas de seguridad que deben volverse a realizar debido a la nueva asociación con el nuevo punto de acceso (AP, *Access Point*). El problema anterior de movilidad y seguridad es al que se quiere aportar mediante el desarrollo del presente proyecto.

En las redes Wi-Fi actuales existe el problema de la pérdida de conexión durante el proceso de *roaming* entre celdas adyacentes, debido, entre otras cosas, a la reautenticación que debe hacer el usuario móvil en la nueva celda. Hasta la fecha, en lo consultado, no existe un estudio sólido del impacto real de los mecanismos de seguridad de acceso protegido Wi-Fi (WPA, *Wi-Fi Protected Access*) y WPA 2 en el proceso de *roaming*, ni en la forma como la red maneja el proceso de *roaming* para evitar estas desconexiones. Debido a lo anteriormente expuesto, este proyecto evaluó el impacto sufrido en cuanto a retardo y pérdida de paquetes en los servicios de *streaming* de audio y video en un cliente inalámbrico alternando la implementación de los mecanismos de autenticación (WPA y WPA 2 – Personal y Empresa) y enfocado en la transición entre puntos de acceso. Más específicamente, se observó un flujo de información desde una fuente fija en la red cableada, hacia clientes inalámbricos dentro de un área específica de cobertura, mientras estos se mueven de un AP a otro.

Adicionalmente, con el desarrollo del proyecto se buscó generar recomendaciones para alcanzar un adecuado equilibrio entre seguridad y desempeño de la red, así como también analizar los mecanismos propuestos por el estándar 802.11r, para analizar teóricamente si éste da solución o no al problema planteado, dado que 802.11r es un estándar encaminado a reducir los tiempos de transición entre APs.

La abundancia en el mercado actual de dispositivos que hacen uso de Wi-Fi como por ejemplo: teléfonos celulares, *Palms*, *PDA*s, *Laptops* (computadores portátiles), dispositivos de juego, *Wi-Fi Phones*, etc., hacen necesario que el cliente tenga disponible “a cualquier hora y en cualquier lugar” los servicios que dichos dispositivos soportan, y

adicional a estos servicios se debe brindar movilidad, lo cual es una característica inherente a la tecnología inalámbrica. Así, con el fin de lograr coberturas grandes para los dispositivos, se hace necesario implementar infraestructuras de red que deben tener más de un punto de acceso, así pues, se logra ampliar la cobertura, pero se genera un problema adicional, el cual es debido a los retardos que se generan en el paso de la cobertura de un AP hacia la de otro AP, los servicios en tiempo real como el *streaming* de audio y video son más sensibles a estos retardos que las transmisiones de datos normales.

Toda la experimentación que se realizó durante el desarrollo del proyecto arrojó resultados que sirvieron en la planeación e implementación más eficaz de *streaming* de audio y/o video a través de Wi-Fi y con movilidad, ya sea en el sector empresarial o educativo. En estos momentos es de gran importancia analizar este tipo de servicios multimedia, ya que la popularidad de que gozan en el mundo es muy grande, existiendo este servicio inclusive a través de Internet, con una calidad aceptable.

El capítulo uno concentra toda la información necesaria para comprender la situación y desarrollar propuestas en los siguientes capítulos, además de concluir con los posibles factores que influyen en el mal funcionamiento del *streaming* de audio y de video en *roaming* con implementación de seguridad (WPA y WPA 2).

Las pruebas y resultados de toda la experimentación se encuentra en el capítulo dos, el estudio se hace de forma incremental iniciando con movilidad, *streaming* y seguridad por separado, luego se evalúa estos tres elementos en conjunto para encontrar el posible problema o variables críticas.

En los capítulos tres y cuatro se identifican los mecanismos propuestos por el estándar IEEE 802.11r y se compara con los resultados obtenidos en el capítulo anterior, además de describir los resultados logrados teniendo en cuenta los aspectos más influyentes en su desarrollo representados en una serie de recomendaciones.

Para el entendimiento lógico de toda la información encontrada en los capítulos de éste proyecto; los Apéndices son de vital importancia debido a que concentran estudios independientes que fueron realizados necesariamente para la continuidad de todas las actividades de experimentación basándose en la metodología investigativa cíclica propuesta, cada capítulo y Apéndice presenta datos que pueden ser utilizados para posteriores proyectos, por esto se sugiere tener en cuenta los Apéndices, porque sin ellos no se podrá mantener una idea de lo que se hizo.

Debido al dimensionamiento de este proyecto y la limitación del espacio para su explicación, fue seccionado en estudios llamados Apéndices ya que son información adicional desarrollada en el mismo contexto de experimentación perteneciendo totalmente a el cuerpo de este trabajo; de igual manera fue importante el uso de un Anexo, el cual es un documento extra correspondiente al estándar IEEE 802.11r.

1. COMPONENTES DEL ESTÁNDAR IEEE 802.11

En este capítulo se tratan los conceptos básicos del estándar IEEE 802.11 y se definen cada uno de los componentes del estándar por separado para dar una mejor idea al lector acerca de lo que el estándar es y de lo que éste abarca, para de ésta manera entrar a trabajar con los temas más específicos del proyecto como lo son: seguridad, *roaming* en IEEE 802.11 y *streaming* de audio y video. Luego de reunir la información requerida se analizaron los factores que influyen en el desempeño del *streaming* de audio y video cuando se hace *roaming* en redes IEEE 802.11 b/g y se utiliza WPA y WPA 2 (personal y empresa).

1.1. DESCRIPCIÓN GENERAL

El estándar salió en 1997 [1] [2], éste define la subcapa de control de acceso al medio (MAC, *Medium Access Control*), la capa física, servicios y protocolos para manejar esta subcapa MAC. En un comienzo se definió en la parte física la tecnología IR, luego se usó radio frecuencia con espectro ensanchado por salto de frecuencia (FHSS, *Frequency Hopping Spread Spectrum*), luego el espectro ensanchado por secuencia directa (DSSS, *Direct Sequence Spread Spectrum*), estos dos últimos trabajan en la banda de 2.4 GH con velocidades de 1 y 2 Mbps. En 1999 se crea el suplemento 802.11a el cual utiliza la multiplexación por división de frecuencias ortogonales (OFDM, *Orthogonal Frequency Division Multiplexing*) y trabaja en la banda de infraestructura de información nacional sin licencia (U-NII, *Unlicensed National Information Infrastructure*), la cual opera en los 5 GH y tiene una velocidad de 54 Mbps. En 1999 se crea un nuevo suplemento denominado el 802.11b, el cual trabaja en la frecuencia 2.4 GH con DSSS, alcanzando 11 Mbps. Luego en 2002 sale el suplemento 802.11g, el cual desarrolla toda la potencialidad de OFDM en la banda de 2.4 GH también alcanzando 54 Mbps. En noviembre del año 2008 se ratificó la versión 7.0 del borrador del estándar 802.11n y se está en los lineamientos finales del estándar el cual alcanza hasta 200 Mbps[3].

El estándar IEEE 802.11 fue desarrollado para establecer especificaciones técnicas de la subcapa MAC y de la capa física de la arquitectura de interconexión de sistemas abiertos (OSI, *Open System Interconnection*), para estaciones inalámbricas portables, fijas y móviles dentro de un área local determinada. El estándar busca específicamente describir las funciones y servicios de los dispositivos que son compatibles con 802.11 que son necesarios para operar dentro de una red de infraestructura o una red ad-hoc, así como también los aspectos de movilidad dentro de estas redes (transición entre celdas o *roaming*). Así mismo, describe todos los procedimientos necesarios para proveer al usuario final con privacidad de los datos que se están enviando a través de estas redes inalámbricas así como de la autenticación que deben realizar los dispositivos que cumplen con la norma. El estándar también provee servicios de nivel superior que sean transparentes para los usuarios de tal manera que no noten la diferencia de estar en una red inalámbrica, o en una red cableada común y corriente. Las redes inalámbricas tienen diferencias sustanciales de las redes cableadas comunes, inclusive algunos países imponen características específicas de transmisión física para los dispositivos de radio además de las impuestas por el estándar 802.11.

En las redes cableadas una dirección IP es casi siempre asociada o asignada de manera física a algún lugar o locación, a diferencia de esto, en redes inalámbricas una estación es el destino de un mensaje más no es algún lugar físico específico.

La capa física de una red cableada es diferente de la de una red inalámbrica, entre las diferencias están: los límites de la cobertura de red son muy difusos, los dispositivos están desprotegidos contra señales externas, el medio por el que se realiza la comunicación es mucho menos confiable que el cableado, las topologías son dinámicas, no hay una conectividad total o 100% asegurada todo el tiempo y las propiedades de propagación de la señal radio-eléctrica son muy variables.

Es importante resaltar que esta tecnología debe soportar tanto estaciones móviles como portátiles, la diferencia está en que las estaciones portátiles son inalámbricas pero normalmente no están en movimiento, más bien se trasladan de un sitio a otro y son usadas cuando están en un sitio fijo. También otro aspecto a tratar con las estaciones móviles, es que éstas normalmente se alimentan por energía almacenada en baterías, con lo cual no se puede especular con que siempre estarán encendidas debido a los mecanismos de ahorro de energía que implementan estos dispositivos.

1.2. COMPONENTES IEEE 802.11

De acuerdo con [1] [2] la arquitectura de IEEE 802.11 consta de múltiples componentes que permiten la conectividad y movilidad de las estaciones de una manera transparente para el resto de capas superiores de la arquitectura OSI. En la Figura 1-1 [2] se observan los componentes de una red IEEE 802.11.

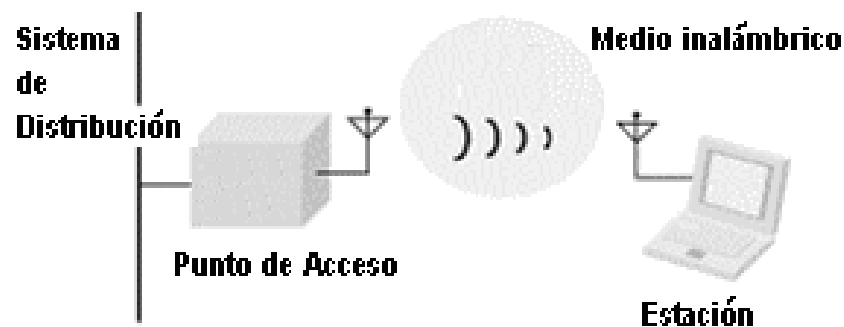


Figura 1-1 Componentes de IEEE 802.11

⊕ Estación

La estación es el componente que realmente se conecta (asocia) a un punto de acceso. Muchas personas pueden pensar que la estación es el dispositivo en sí, por ejemplo: un computador portátil, un teléfono celular, un punto de venta, etc, pero en realidad la estación es la tarjeta de interfaz de red (NIC, *Network Interface Card*), inalámbrica en éste caso, la cual es la encargada de todos los procesos de conectividad. Cada estación es la que da soporte a los servicios claves de autenticación, desautenticación, privacidad y entrega. Los servicios de una estación mediante los cuales se brinda la capacidad de conexión inalámbrica son cuatro [2]:

1. **Autenticación:** Este es el servicio mediante el cual una estación se identifica con otras estaciones y puede intercambiar ciertos tipos de paquetes o información.
2. **Desautenticación:** Es el servicio contrario al anterior, cuando se invoca este servicio la estación que se desautentica ya no puede intercambiar ningún tipo de paquetes con la red.

3. **Privacidad:** Este es el servicio mediante el cual se logra tener un nivel de privacidad de los datos enviados en radio frecuencia, similar al de una red cableada. Lo que busca es asegurar los datos desde que salen de la estación emisora pasando por el medio físico hasta que llegan a la estación receptora.
4. **Entrega:** Este es el servicio fundamental de todo el estándar, y busca entregar los datos de manera confiable desde la MAC de una estación hasta la MAC de otra estación con la menor duplicación y reordenamiento de tramas como sea posible.

⊕ Sistema de distribución

Un Sistema de distribución (DS, *Distribution System*), es un componente lógico el cual es usado para comunicar diferentes APs cuando estos se unen con el fin de formar un área de servicio más grande, se puede decir entonces, que es el encargado de unir físicamente varios puntos de acceso a través de una infraestructura de red, cabe resaltar que la tecnología de red que comúnmente se usa como *backbone*¹ en un sistema de distribución es la IEEE 802.3 o *Ethernet*. Además, mediante el DS se logra la intercomunicación de los puntos de acceso² lo cual es fundamental para que estos dispositivos intercambien información de las estaciones que se encuentran asociadas a ellos y así saber cuáles estaciones están en determinado conjunto de servicio básico (BSS, *Basic Service Set* con el fin de dirigir de una manera ágil y óptima los paquetes que le corresponden a cada estación. El DS se basa en la prestación de 5 servicios básicos con los cuales puede interactuar con las estaciones, estos servicios son [2]:

1. **Asociación:** Permite crear el enlace entre una estación y un punto de acceso, con este se logra enviar datos a la estación desde el DS y enviar datos desde la estación.
2. **Reasociación:** Es muy similar a la asociación, adicionalmente incluye información acerca del AP con el que estaba asociado anteriormente. Este servicio se invoca en cada transición entre APs cuando una estación viaja a través del ESS.
3. **Desasociación:** Este servicio puede ser invocado tanto por el AP como por la estación. En el caso de ser usado por un AP, éste lo puede usar para forzar a una estación a asociarse a otro AP, o puede ser usado por una estación para poder asociarse a otro AP cuando detecta que la recepción es mejor en este nuevo AP.
4. **Distribución:** Este servicio es necesario para saber en cuál BSS se encuentra una estación y por ende enviarle los respectivos paquetes de datos.
5. **Integración:** Mediante este servicio se logra intercambiar mensajes que vienen o salen hacia una red cableada desde y hacia una red inalámbrica IEEE 802.11.

⊕ Punto de acceso

Las tramas que usa o maneja IEEE 802.11 tienen al igual que todo protocolo de comunicación un formato específico; para que los paquetes lleguen al resto de las redes o Internet deben pasar al sistema de distribución en un formato que éste pueda manejar. Para esta tarea específica se crearon los puntos de acceso (AP), ellos son los encargados de servir de *gateway*³ o puerta de salida para las tramas desde el medio inalámbrico al

¹ *Backbone* es la red núcleo o red central de una infraestructura de redes de datos.

² Se tratan más adelante en esta misma sección.

³ *Gateway*: Es la parte física por donde una red se comunica hacia otra red (no necesariamente del mismo tipo que la anterior).

medio cableado. Esta tarea de puenteo no es la única que realizan los puntos de acceso pero si la más importante. Otro punto a resaltar de los APs, es que usan el protocolo inter punto de acceso (IAPP, *Inter Access Point Protocol*) para comunicarse entre ellos cuando se forma un conjunto de servicio extendido (ESS, *Extended Service Set*) y en conjunto con un servidor de autenticación remota telefónica de usuario (RADIUS, *Remote Authentication Dial-In User Server*) para lograr un mejor funcionamiento de las estaciones cuando pasan de un AP a otro, esto se llama *roaming*, se busca que este *roaming* sea lo más transparente para el usuario final.

⊕ Medio inalámbrico

El medio inalámbrico (aire) es el medio físico que usa IEEE 802.11 para el envío de las tramas. Se han definido varias capas físicas para que sean soportadas por la subcapa MAC de 802.11, en un comienzo se establecieron 2 tipos de transmisión o capas físicas, una de RF y una física IR, ahora solo se usan las de radio frecuencia.

⊕ Conjunto de servicio básico (BSS)

Un BSS es la reunión de los componentes mínimos que conforman un conjunto de 802.11, en la Figura 1-2 [2] se pueden observar los componentes de un BSS. Dentro de este conjunto las estaciones que se encuentran allí como por ejemplo STA1 y STA2 en el BSS1 tienen conectividad una con otra luego de haber pasado por los procesos de autenticarse y asociarse con el AP del BSS1 o por ejemplo la STA3 con la STA4 en el BSS2. Se suele pensar indistintamente en un BSS como en el área de servicio de una red 802.11, es así, como una estación fuera de un BSS o del área de servicio de la red 802.11 no puede comunicarse con otras estaciones en este BSS.

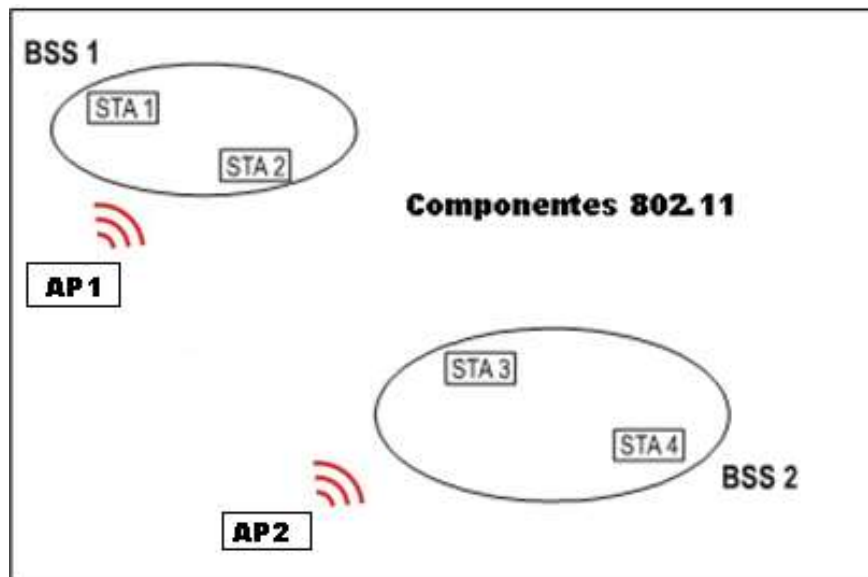


Figura 1-2 Conjunto de servicio básico.

⊕ Conjunto de servicio extendido (ESS)

Un ESS es la unión de varios BSS a través de un sistema de distribución, se pueden observar los componentes de un ESS en la Figura 1-3 [2]. Un BSS tiene un identificador único, cuando se forma un ESS, todos y cada uno de los BSS componentes de este ESS tienen el mismo identificador, este identificador se conoce comúnmente como identificador de conjunto de servicio (SSID, *Service Set Identifier*). Un ESS provee un marco de referencia mediante el cual las estaciones pueden moverse de un BSS a otro BSS, tratando de hacerlo de manera transparente para el usuario final.

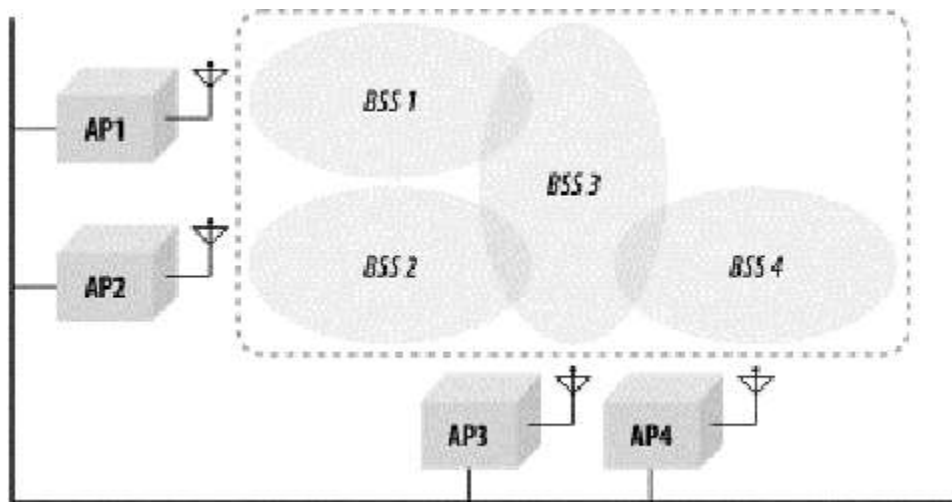


Figura 1-3 Conjunto de servicio extendido.

1.3. SEGURIDAD EN 802.11

La seguridad en el caso de las redes inalámbricas significa tener confianza y privacidad en los datos que se envían o intercambian a través de ésta. Uno de los problemas más grandes que enfrentan los administradores de redes inalámbricas, es el hecho de que todos los datos que se envían en este tipo de redes están siempre en el medio inalámbrico y este medio no tiene ningún tipo de protección o seguridad a nivel físico ya que cualquier dispositivo puede tener acceso a él, caso diferente en las redes cableadas, ya que estas pueden tener protección por medio de armarios y lugares cerrados bajo llave. Cuando se habla de seguridad en redes inalámbricas existen 3 tipos de seguridad que se implementan hasta la fecha, estos son: Privacidad equivalente a cableado (WEP, *Wired Equivalent Privacy*), acceso protegido Wi-Fi o WPA y la versión 2 o WPA 2 [2].

WEP fue una tecnología que nació con el estándar IEEE 802.11b, este es el método de seguridad que se creó inicialmente para proteger todos los entornos IEEE 802.11 pero debido a la gran cantidad de fallas que presenta surgió la necesidad de mejorarlo para que fuera más seguro. Entre las fallas que presenta WEP se tiene la utilización de una misma clave o llave⁴ entre el AP y todas las estaciones, el cifrado que se usa es el cifrado rivest 4 (RC4, *Rivest Cipher 4*) el cual es muy débil, se usa la comprobación de redundancia cíclica (CRC, *Cyclic Redundance Check*) para la integridad de los datos el

⁴ En este documento se trata indistintamente el término clave y llave, en lo referente a cifrado y seguridad.

cual es muy vulnerable. Otro factor es que WEP no tiene autenticación ya que se hace por llave compartida lo cual no garantiza seguridad, sin mencionar que obtener la llave usada por WEP es un proceso muy sencillo[2].

Debido a lo anterior, la alianza Wi-Fi desarrolló, basándose en el trabajo del grupo de trabajo 802.11i de la IEEE, una nueva técnica denominada acceso protegido Wi-Fi. WPA viene a aportar un nivel intermedio de seguridad en la aplicación total del estándar IEEE 802.11i que fue ratificado en 2004 y el cual busca implementar una seguridad e integridad total a los datos que viajan en las redes 802.11 a través de métodos que se verán más adelante.

1.3.1. Acceso protegido Wi-Fi (WPA)

WPA fue desarrollado para la seguridad de redes Wi-Fi y lanzado por la alianza Wi-Fi como un punto intermedio en la implementación de 802.11i, de aquí que se le llame red segura transicional (TSN, *Transicional Security Network*). WPA fue diseñado en su versión empresa (WPA *Enterprise*) para trabajar con un servidor de autenticación 802.11x y el protocolo de autenticación extensible (EAP, *Extensible Authentication Protocol*), pero en hogares y pequeñas empresas puede ser usado con el sistema de llave precompartida (PSK, *Pre Shared Key*), a éste WPA se le conoce con el nombre de versión personal (WPA *personal*). WPA usa el mismo algoritmo de cifrado que usa WEP el cual es el RC4 ya que WPA lo fortalece a través del uso del protocolo de integridad de llave temporal (TKIP, *Temporal Key Integrity Protocol*), no lo cambia. Otra característica que se mejora sustancialmente con WPA es la integridad de la información cifrada, normalmente WEP utiliza CRC el cual es inseguro, ya que los intrusos pueden cambiar la información útil de la trama y recalculan el CRC y de esta manera los usuarios no se darían cuenta de la filtración de información que ocurrió. A diferencia de WEP, WPA utiliza el código de integridad de mensaje (MIC, *Message Integrity Code*), conocido también como Michael, éste código tiene protección contra ataques de repetición⁵, y también incluye un contador de tramas para mejorar la seguridad, a continuación se profundiza más en estos temas.

Código de Integridad de Mensaje (MIC, *Message Integrity Code*)

MIC se basa en crear un valor a partir de la combinación del paquete y enviar este valor junto con el paquete. La diferencia radica en que para calcular este valor se usa un algoritmo que es irreversible y que usa una llave, por lo cual un atacante no puede descifrarlo y volver a empaquetarlo de manera correcta.

Protocolo de integridad de llave temporal (TKIP, *Temporal Key Integrity Protocol*)

Este es un protocolo de seguridad desarrollado por varias empresas líderes del mercado el cual es usado en WPA. TKIP se usa para reemplazar WEP sin necesidad de reemplazar el *hardware* existente. TKIP se dio para asegurar las conexiones inalámbricas, mientras se daba el cambio hacia un 802.11i totalmente implementado por los dispositivos. TKIP también surge porque la seguridad de la capa de enlace estaba

⁵ Involucra la captura de información de forma pasiva, y luego su reenvío, por el medio de transmisión para lograr efectos no autorizados.

bastante comprometida por las falencias que tenía WEP, y no se podía esperar a las nuevas tecnologías que con los nuevos desarrollos ponían fin a estas falencias. Como se debía usar la misma tecnología física que usaba WEP, es decir el mismo *hardware*, TKIP también se basa en el algoritmo RC4 como lo hace WEP, pero a diferencia de WEP utiliza nuevos mecanismos para contrarrestar las falencias.

Dentro de las diferencias que se evidencian entre WEP y WPA se tiene, el número de bits del vector de inicialización el cual pasa de 24 a 48 bits, en lo concerniente al MIC o Michael, WEP tiene la debilidad de no ser capaz de detectar si alguien introduce datos en medio de una cadena de bits dentro de la trama, es decir, la integridad de los datos se ve comprometida, para ello WPA implementa MIC, el cual es un algoritmo fuerte de seguridad. MIC calcula un código de integridad de mensaje de 64 bits y lo cifra con TKIP. TKIP usa un conjunto de llaves temporales, las cuales se derivan a partir de una llave maestra y otros valores como la dirección física de las estaciones. La llave maestra es a su vez derivada del proceso 802.11x/EAP, o en el caso de llave pre compartida (PSK), se deriva de esta misma. También una diferencia fundamental es que WPA renueva automáticamente, con un tiempo configurable en el servidor RADIUS, el conjunto de llaves. Así mismo TKIP cambia la longitud de la llave a 128 bits, cambiando por sesión, por usuario y por paquete adicionalmente es temporal. A continuación se muestra una tabla con las diferencias entre WEP y WPA.

Característica	WEP	WPA
Autenticación	WEP – PSK	802.1X - EAP
Cifrado	RC4 40bits o 104 bits	TKIP RC4 128bits
Vector de Inicialización	24 bits	48 bits
Integridad de datos	CRC – 32	MIC
Gestión de llaves	No	801.1x EAP

Tabla 1–1 Comparación entre WEP y WPA

1.3.2. Acceso Protegido Wi-Fi versión 2 – WPA 2

Esta nueva versión de WPA, está basada en el estándar IEEE 802.11i, este estándar fue ratificado en julio de 2004 y busca una mayor seguridad en redes inalámbricas, lo que se conoce como seguridad de red robusta (RSN, *Robust Security Network*). WPA versión 2 implementa las características más importantes de 802.11i pero no todas. Desde marzo de 2006 es obligatoria para todos los dispositivos que estén certificados por la alianza Wi-Fi la opción de implementación de WPA 2, de esta manera se busca que los productos que salen al mercado tengan soporte para WPA 2. WPA 2 usa un algoritmo basado en el estándar de cifrado avanzado (AES, *Advanced Encryption Standard*), protocolo de código de autenticación de mensaje encadenado y cifrado por bloque (CCMP, *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), este tipo de cifrado es tan seguro que cumple con el estándar de procesamiento de información federal de los Estados Unidos de América 140-2 (FIPS, *Federal Information Processing Standards*), el cual deben cumplir todos los fabricantes privados que desean venderle al gobierno, el lado malo con AES es que en algunos casos se puede requerir el cambio de equipos *hardware* de las redes Wi-Fi para implementarlo, pero no es gran problema ya que desde el 2004 los productos tienen el soporte para WPA 2 [4][5].

1.3.2.1 Proceso de autenticación

Según [4], WPA 2 empresa trabaja con un servidor de autenticación, así que ahora se estudia la autenticación usada por WPA 2 empresa, la cual es 802.1x. El control de acceso de red basado en puerto (802.1x), provee medios de autenticar y autorizar los dispositivos que se encuentran en un puerto físico de una red LAN, para que hagan uso de estos recursos.

En la Figura 1-4 [6], se ilustra el proceso que se lleva a cabo cuando se usa 802.1x en el ambiente inalámbrico, y los pasos que se siguen son [5]:

1. El cliente inalámbrico o suplicante trata de conectarse.
2. El cliente se autentica con el servidor de autenticación.
3. Se generan las claves necesarias y se da la autorización por parte del servidor de Autenticación.
4. Se le autoriza el acceso a la red al suplicante.

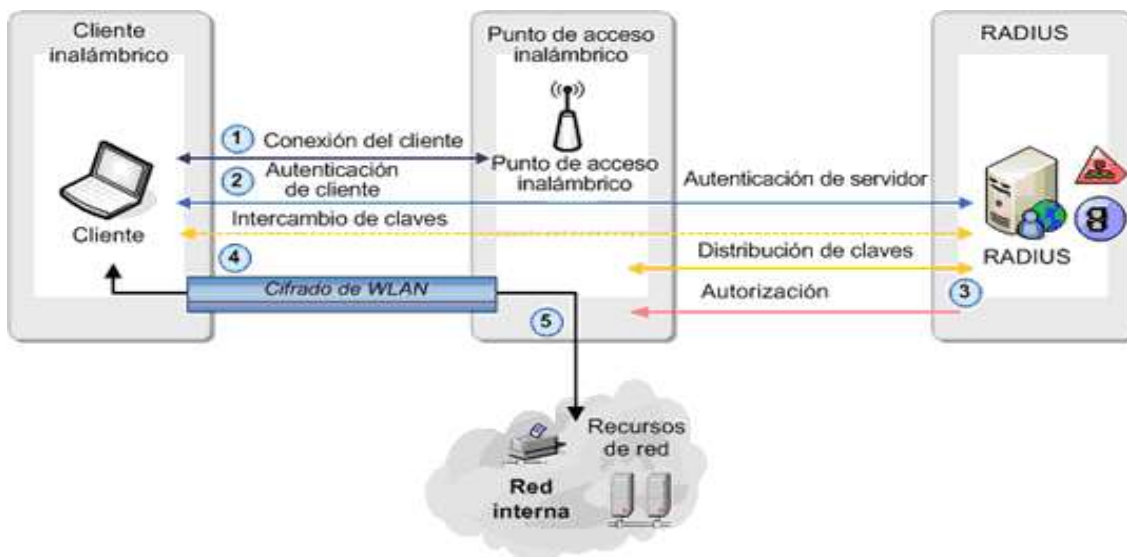


Figura 1-4 Funcionamiento de 802.1x.

Lo primero que se debe hacer es identificar 3 actores que hacen parte de este proceso, a) el suplicante o cliente inalámbrico el cual es el que se autentica, b) el autenticador, el cual está en el AP, y sirve de canal entre el suplicante y el servidor de autenticación, el cual es el tercer actor, c) el servidor de autenticación, éste es el encargado de autenticar el cliente inalámbrico y de garantizar o rechazar la conexión del mismo a la red cableada.

La primera acción que ocurre es cuando un cliente inalámbrico trata de acceder a una red, y busca un AP al cual asociarse. Cuando encuentra un AP en su rango de cobertura empieza el proceso de autenticación; lo primero que hace el AP es preguntar la identidad (autenticar) del cliente inalámbrico que se intenta conectar, mientras ocurre éste proceso de autenticación el único tráfico que se permite entre el cliente y la red cableada, es el tráfico del protocolo de autenticación extensible (EAP, *Extensible Authentication Protocol*) el cual se usa para la autenticación. EAP fue creado inicialmente para usarse con PPP

(protocolo punto a punto), pero se adaptó de manera que se encapsula en LAN⁶ para usarse con 802.1x, de esta manera se llama EAPOL (EAP sobre LAN). Antes de enviar cualquier mensaje, se crea un túnel de cifrado TLS (seguridad de capa de transporte), una vez se hace esto, el suplicante envía los datos al autenticador en formato EAPOL, y este los recibe y reencapsula en formato RADIUS y los reenvía hacia el servidor de autenticación. Durante el proceso de autenticación el AP simplemente reenvía los paquetes que vienen desde el cliente inalámbrico hacia el servidor de autenticación. Cuando el proceso termina exitosamente, el autenticador le permite al suplicante que se autenticó exitosamente el acceso a los recursos de la red.

1.3.2.2 Gestión de llaves de cifrado

Para asegurar una política de seguridad, se hace necesario y obligatorio el manejo de llaves, 802.11i implementa un régimen de derivación de llaves. En la Figura 1-5 [5], se observa el funcionamiento de la derivación de llaves en 802.11i.

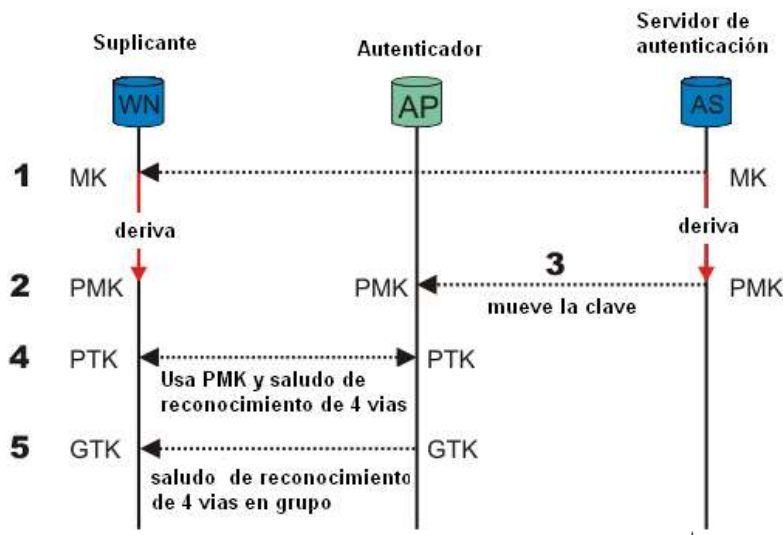


Figura 1-5 Gestión y derivación de llaves en 802.11i.

El proceso es el siguiente: primero, cuando el cliente inalámbrico se autentica con el servidor de autenticación, entre los últimos mensajes que se envían hacia el primero está la llave maestra (MK, *Master Key*), luego de esto, esta llave sólo la saben el cliente inalámbrico y el servidor de autenticación, esta llave se une a la sesión entre el cliente inalámbrico y el servidor de autenticación. Luego los dos, tanto el cliente inalámbrico como el sistema autónomo derivan una nueva llave, la llave maestra de pareja (PMK, *Pairwise Master Key*). Luego esta PMK se mueve hasta el autenticador (AP), únicamente el cliente inalámbrico o el servidor de autenticación pueden generar o derivar esta llave, esto es para que únicamente el servidor de autenticación tome decisiones de control de acceso. La PMK es una llave asociada a esa sesión entre el cliente inalámbrico y el sistema autónomo. Seguidamente se usa la PMK y un intercambio de mensajes o paquetes llamado saludo de 4 vías, éste se realiza entre el cliente inalámbrico y el AP con

⁶ Proceso de transformación de un mensaje EAP para ser transportado en 802.3.

el fin de generar, asociar y verificar una llave transitoria de pareja (PTK). A su vez la PTK es un conjunto de llaves usadas para diferentes propósitos y estas son [5]:

- KCK (Llave de confirmación de llave): se usa para verificar la posesión de PTK y para asociarla al AP.
- KEK (Llave de cifrado de llave): es usada para distribuir la GTK (Llave temporal de grupo).
- TK1 y TK2 (Llaves temporales 1 y 2): se usan para el cifrado y dependen de cómo se cifran los datos.
- GTK (Llave temporal de grupo): esta es una llave compartida por todos los suplicantes o usuarios móviles conectados al mismo autenticador, y se usa para asegurar el tráfico *multicast* y *broadcast*.

1.3.2.3 Llave precompartida (PSK)

En ambientes algo pequeños, como en oficinas o el hogar, se puede usar algo más sencillo, lo cual es una llave compartida previamente, cuando se hace esto, se salta todo el proceso de autenticación 802.1x, como se había dicho antes; cuando se usa este tipo de autenticación, se dice que es WPA personal. En este caso se usa la PSK como MK en la derivación de llaves.

1.4. MOVILIDAD EN Wi-Fi (*Roaming*)

Se debe resaltar que en este documento se hablará de *roaming*, el cual es referenciado como *handover* o *handoff*, e itinerancia en redes inalámbricas por distintos autores en diferentes libros e Internet, esta decisión se debe a la mayor incidencia del término *roaming* en las referencias ampliamente consultadas [7][8][9]. Aclarado lo anterior, *roaming* es el proceso que se presenta entre un AP y un suplicante cuando éste último pasa de la zona de cobertura de un AP hacia la zona de cobertura de otro AP, brindando así la posibilidad de que los usuarios se muevan libremente entre diferentes puntos de acceso, pero para esto se necesita que las coberturas se superpongan. Luego el suplicante haciendo uso de un algoritmo matemático de decisión escoge el punto de acceso al cual asociarse y hacer el cambio. Debido a que en el presente proyecto se trabajó con *streaming* de audio y video, el proceso de *roaming* es de interés particular para éste tipo de aplicaciones porque éstas son muy sensitivas al retardo y pérdida los paquetes [7].

1.4.1. Asociación con los APs

De acuerdo con [7][8][9], cada estación inalámbrica cuando se enciende busca los APs que hay en la zona. Cuando hay varios APs el suplicante atiende al que le envía la respuesta con una señal más fuerte en términos de potencia. De esta forma la estación inalámbrica se asocia con el AP que eligió, luego el AP identifica la estación por medio de la dirección MAC de la misma y la incluye en su lista de asociados. Los APs envían normalmente *beacons*⁷ entre 10 y 100 veces por segundo, para darse a conocer a las

⁷ Trama enviada desde los puntos de acceso para que los clientes sepan en donde están.

estaciones que se encuentran en la zona. Cuando una estación móvil entra en la zona de cobertura de otro AP mientras se mueve y detecta los *beacons* de este nuevo AP, con una mayor potencia, empieza el proceso de asociación con este nuevo AP. Para que el proceso de *roaming* sea lo más transparente posible al usuario o suplicante se requiere que haya solapamiento entre las zonas de cobertura de los APs que se involucran en la transición. Otro factor que juega un papel importante en este proceso es la velocidad con la que se mueve el suplicante en el momento de la transición de un AP a otro. El proceso de *roaming* se puede dividir en los 2 siguientes pasos:

A. Descubrimiento: debido a la movilidad del usuario móvil, la potencia de la señal o la relación señal/ruido llegan a valores muy bajos, frente a lo cual, la estación comienza a buscar un nuevo AP para asociarse; esto se logra mediante un proceso de búsqueda, por medio del cual encuentra los *beacons* de los APs cercanos que son enviados aproximadamente cada 100 ms y los pone en una lista de prioridad dependiendo de la potencia con que se reciban. Existen dos métodos de búsqueda: la activa y la pasiva. El pasivo es en el cual, la estación sólo escucha los *beacons*, es decir solo recibe los *beacons* que envían los APs y en los cuales se encuentra el SSID de la red y en el activo la estación además de escuchar *beacons* hace una difusión de tramas de petición de prueba llamadas *probe request*⁸ con un SSID previamente especificado, para ver si a algún AP cercano le corresponde éste SSID, esto es debido a que algunos APs pueden no difundir su SSID.

B. Reautenticación: La estación ahora trata de asociarse y reautenticarse al nuevo AP que esté de primero en la lista de prioridad, este proceso de reautenticación involucra una autenticación y reasociación al nuevo AP. También en esta fase se presenta un intercambio de credenciales y otra información del estado de la estación entre el AP anterior y el AP actual. Esto se logra por medio del protocolo Inter-puntos de acceso o con protocolos propietarios de los fabricantes de los APs. Los pasos anteriores introducen un retardo en el proceso de *roaming*. A continuación se explica cómo es el proceso con más detalle, en el que se asume que se hace una búsqueda activa.

Primero la estación móvil comienza haciendo una difusión de paquetes de prueba (sondas) y espera las respuestas de los APs cercanos, este proceso de paquetes de petición-respuesta enviados por la estación busca en todos los canales de radio. Luego de esto, sigue el proceso de autenticación entre la estación móvil y el nuevo AP, este proceso de autenticación depende del método que se esté usando, en el caso de este proyecto es aquí donde se involucra WPA y WPA 2, ya que estos son los métodos de autenticación elegidos por su alto nivel de seguridad. En especial, el caso de WPA/WPA 2 empresa, que sería el proceso más largo debido a que éste involucra todo el proceso visto en la autenticación 802.1x.

Una vez la estación móvil se ha autenticado sigue el proceso de reasociación, éste se lleva a cabo entre el anterior AP al cual estaba asociada la estación móvil y el nuevo AP al que se está asociando. Esta parte del proceso empieza con el envío de un paquete de petición de reasociación al nuevo AP, esto inicia otro proceso de intercambio de paquetes entre los dos APs con el protocolo propietario inter puntos de acceso, mediante el cual los dos APs intercambian información, además de los retardos introducidos por lo anteriormente mencionado existe un retardo adicional que es el que se produce por la actualización de las direcciones MAC en el sistema de distribución, aunque típicamente el

⁸ Trama que va desde el cliente inalámbrico para la búsqueda de nuevos puntos de acceso.

tiempo de retardo de un *roaming* se totaliza desde la primer trama *probe* hasta la recepción del paquete de respuesta de reasociación.

1.4.2. Tipos de *roaming*

Existen dos comportamientos de las estaciones móviles durante el *roaming*:

- *Roaming* transparente.
- *Roaming* nómada.

***Roaming* transparente:** éste comportamiento se puede ilustrar por ejemplo, como cuando una persona está realizando una llamada a través de un teléfono celular mientras conduce su carro por la autopista. Allí, las típicas tecnologías celulares como el sistema global para comunicaciones móviles (GSM, *Global System for mobile Communications*), o el acceso múltiple por división de tiempo (TDMA, *Time Division Multiple Access*) proporcionan unos pocos kilómetros de área de servicio, y gracias a las estaciones que hay en toda la autopista la persona se puede comunicar durante todo el trayecto sin que la comunicación se le corte en ningún momento. En este tipo de movilidad las aplicaciones requieren conexión de red constante durante el proceso de movilidad.

***Roaming* nómada:** se describe mejor como la utilización de un computador portátil con 802.11 habilitado en un entorno de oficina. A modo de ejemplo, un usuario móvil mantiene la conectividad de la red todo el tiempo con un único AP. Cuando el usuario decide moverse con su computador portátil a lo largo de un pasillo hacia una sala de conferencias y una vez en la sala de conferencias vuelve a su trabajo. Este tipo de Movilidad se considera nómada porque el usuario no está utilizando los servicios de red cuando se mueve, sólo lo hará cuando llegue a su destino.

Existen muchos detalles acerca del funcionamiento de *roaming* en 802.11 que deben ser desarrollados para entenderlo mucho mejor, dentro de éstos se resaltan: las sesiones entre el usuario y el punto de acceso durante la movilidad, el saber si ésta es una técnica orientada a conexión o no, saber si el *roaming* es también a nivel 3 o de red y algo muy importante la duración del *roaming*.

1.4.3 La naturaleza de *roaming* en 802.11

Roaming en 802.11 se conoce como "*break before make*", es decir: "romper antes de hacer", refiriéndose a la exigencia o requerimientos de una estación móvil asociada con un AP antes de la creación de una nueva asociación otro AP. Este proceso facilita un sencillo protocolo MAC pero introduce la posibilidad de pérdidas de datos durante el cambio de AP. Si 802.11 fuera "*make before break*" o "hacer antes de romper", una estación móvil se puede asociar a un nuevo AP sin antes estar desasociado con el AP anterior, esto lleva a necesitar una defensa en la sub capa MAC para asegurar una topología libre de bucles, pues, se tendría una estación conectada en la capa 2 y emitiendo simultáneamente desde su dominio a través de la conexión de red, este modelo generaría una tormenta de colisiones.

Para contrarrestar el inconveniente nombrado anteriormente, la arquitectura debe tener un algoritmo para evitarlo. Un ejemplo es el estándar 802.1d o protocolo de expansión de árbol (STP, *Spanning Tree Protocol*), especial para resolver posibles bucles, además de

esto la estación móvil asumiría la capacidad de escuchar y comunicarse en más de un canal a la vez y añadiría un mayor encabezado en el protocolo MAC aumentando la complejidad del *hardware* de radio y los costos de los dispositivos.

1.4.4 Funcionamiento del *roaming*

La forma como la aplicación opera está directamente relacionada a sus problemas durante el *roaming*. Técnicas orientadas a conexión al igual que las basadas en TCP son tolerantes a pérdidas de paquetes durante el *roaming*. TCP entonces ofrece una buena solución para transporte en 802.11, sin embargo, algunas aplicaciones usan UDP como protocolo de transporte, debido a que la característica de retransmisión de paquetes de TCP puede ser un inconveniente para aplicaciones en tiempo real o para voz sobre IP (VoIP, *Voice over IP*).

1.4.5 Dominio de *roaming*

Si varios AP se encuentran en el mismo dominio de *broadcast* y están configurados con el mismo identificador a esto se llama un ESS y están comunicados por el servicio de distribución o red cableada. 802.11 es un estándar que abarca la capa 1 OSI que corresponde a la interfaz física y la capa 2 que es la capa de enlace de datos, el estándar no se refiere a la capa 3 o capa de red. En la Figura 1-6 [10] se presenta el *roaming* en capa 2 dentro del mismo dominio. Este tipo de *roaming* es con el que se trabaja en este proyecto.

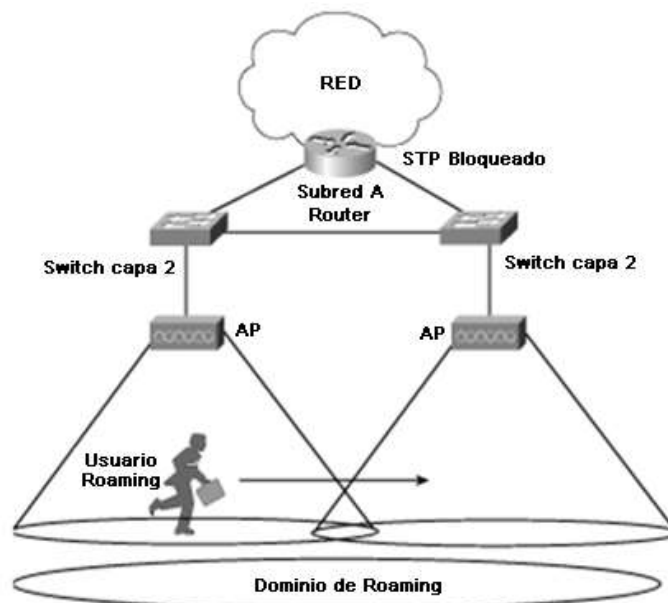


Figura 1-6 *Roaming* dentro de un dominio en la capa 2.

En la Figura 1-7 [10] se ilustra el *roaming* entre diferentes dominios en donde el usuario móvil se mueve a través de APs que se encuentran en una subred A y una subred B, en

este modelo se hace *roaming* de capa 3, el proceso es similar al anterior, la diferencia radica en que para mantener la conectividad se requiere de algún mecanismo mediante el cual se pueda continuar teniendo la misma dirección de red o subred que se tenía en la subred A y así al pasar a la nueva red B seguir recibiendo los paquetes sin ningún inconveniente. Actualmente el mecanismo encargado de hacer esto es el protocolo IP móvil, el cual fue desarrollado por el grupo de trabajo en ingeniería de internet (IETF, *Internet Engineering Task Force*) en el RFC 3344.

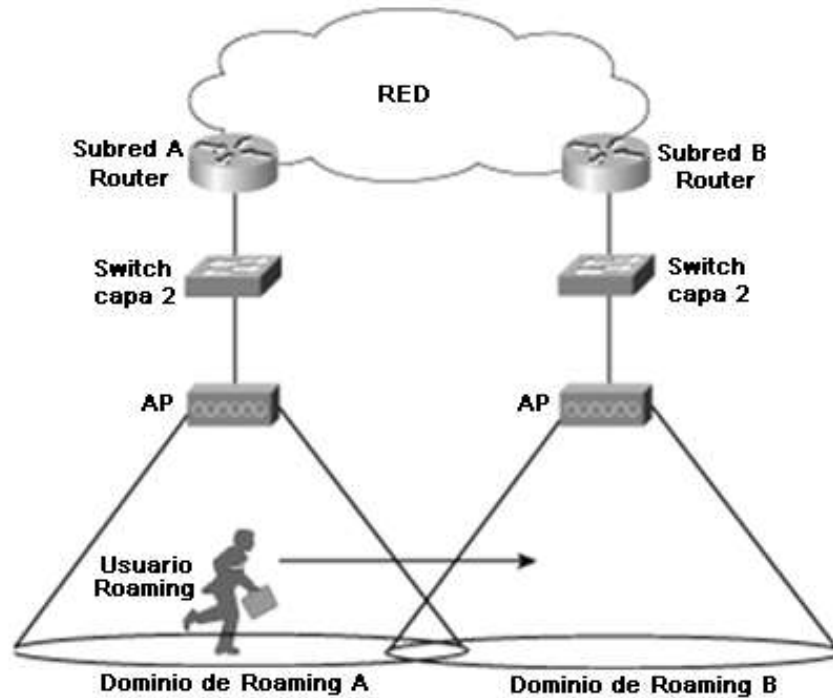


Figura 1-7 *Roaming* a través de los diferentes dominios.

1.4.6 Duración del *roaming*

Es el tiempo que tarda el *roaming* en completarse. Para que este proceso se lleve a cabo se deben cumplir los procesos de búsqueda de APs, de autenticación 802.11, de asociación 802.11 y el proceso de autenticación 802.1x. La duración total resultante de estos procesos equivale a la duración de *roaming*.

En algunas aplicaciones, tales como VoIP o *streaming*, los retardos son extremadamente sensibles y no se pueden tolerar cortes mientras se realizan estos procesos también es mucho más crítico cuando se hace el cambio a diferentes dominios. La siguiente es la secuencia de eventos en la capa 2 durante el *roaming* [10]:

- El cliente debe decidir hacer el *roaming*: esta tarea la realizan los algoritmos de *roaming* los cuales son específicos de cada fabricante y dependen de factores como potencia de la señal, tramas de reconocimiento, *beacons* perdidos, etc.
- El cliente decide a donde hacer el *roaming*: El cliente determina a que AP hacer el *roaming*, esto lo hace por medio de la búsqueda de nuevos APs ya sea antes de la

decisión de *roaming*, que es un proceso llamado “*preemptive AP discovery*” descubrimiento preventivo de AP o después de la decisión de *roaming*, que es un proceso llamado “*roam-time AP discovery*” descubrimiento de AP en el momento del *roaming*.

- El cliente inicia el *roaming*: El cliente utiliza las tramas de re asociación para asociarse con el nuevo AP.
- Una vez conectado con el nuevo AP el cliente puede reanudar las sesiones de aplicación.

1.4.7 Algoritmos de *roaming*

Son el mecanismo que determina cuando debe hacerse el *roaming*. Estos algoritmos no están definidos por 802.11; estos algoritmos se manejan por cada fabricante como un elemento confidencial, a pesar que esto puede causar una falta de interoperabilidad, por eso los fabricantes trabajan unidos para asegurar la interoperabilidad, el hecho de que los algoritmos sean hechos por los proveedores proporciona diferentes oportunidades para crear nuevos y mejores resultados derivados de la competencia. Es seguro asumir que cuestiones como la potencia de la señal, contadores de reintento y *beacons* perdidos se incluyen en los algoritmos. Por ejemplo: el algoritmo binario exponencial de *backoff para acceso al medio*, incrementa el contador de tramas reintentadas si las tramas no se pueden transmitir después de un número de intentos. Este proceso le indica al cliente que se encuentra fuera del alcance del AP.

Los algoritmos de *roaming* equilibran un *roaming* rápido y la estabilidad del cliente, por ejemplo, un algoritmo extremadamente sensible no puede tolerar la pérdida de *beacons* o la pérdida de un ACK⁹, el algoritmo tomaría estos datos como suficientes para iniciar el *roaming*.

1.4.8 Búsqueda de AP

Existen dos mecanismos para la búsqueda de un nuevo AP:

- Descubrimiento de AP preventivo.
- Descubrimiento de AP en el momento de *roaming*.

Cada mecanismo puede emplear uno o ambos de los siguientes métodos para buscar:

- **Búsqueda activa** - La estación móvil busca activamente un AP, este proceso generalmente implica el envío de solicitud del canal que está configurado para su uso, de esta forma se selecciona el AP ideal al cual se va a saltar.

La búsqueda activa trabaja de una forma minuciosa tratando de encontrar siempre APs libres al rastrear los canales, la duración de este proceso dura de 10 a 20 milisegundos (ms) dependiendo del fabricante.

- **Búsqueda pasiva** - La estación móvil no transmite sino que escucha los *beacons* en cada canal en intervalos de tiempo sin enviar solicitudes de conexión. La estación móvil

⁹ Trama de confirmación, de que otra trama llegó bien al destino.

busca repetidamente en todos los canales, este proceso es muy lento dado que se tiene que escuchar los *beacons* enviados por todos los AP, usualmente la velocidad de envío es de 10 *beacons* por segundo, de esta forma la estación móvil debe detenerse en cada uno de los canales por mucho más tiempo para asegurarse de que reciba la mayor parte de los *beacons* que fueron transmitidos. El cliente móvil lee la información de configuración como SSID, velocidades de transmisión soportadas y datos específicos de cada fabricante.

No existe una técnica ideal para el proceso de *roaming*. La búsqueda pasiva tiene los beneficios de que el cliente no necesita *transmitir probe requests*, pero puede no encontrar algún AP debido a que estaba escuchando en otro canal a otro AP. La búsqueda activa tiene la ventaja de buscar a los AP con los cuales se va a asociar, pero para esto requiere que la estación móvil este enviando *probe requests*. Dependiendo de la configuración que tenga la estación móvil en 802.11, puede ser más adecuada una búsqueda pasiva o una activa [10].

1.4.8.1 Descubrimiento de AP preventivo

El *roaming* preventivo es la función que proporciona a la estación móvil la capacidad de cambiar o hacer la transición a APs predeterminados, después de que se toma la decisión de hacer el *roaming*, permitiendo así un tiempo mínimo para realizar todo el proceso de *roaming*, sin embargo, para la estación móvil debe haber ya un AP seleccionado para realizar la nueva asociación, mientras se realiza la búsqueda de APs existen momentos en los que no se permite el *roaming*, pues se debe cambiar de canales para escuchar o para probar conectividad con otro AP, observar Figura 1-8 [10].

Este cambio crea dos problemas potenciales para la estación móvil que pueden afectar el proceso de *roaming*, siendo los siguientes:

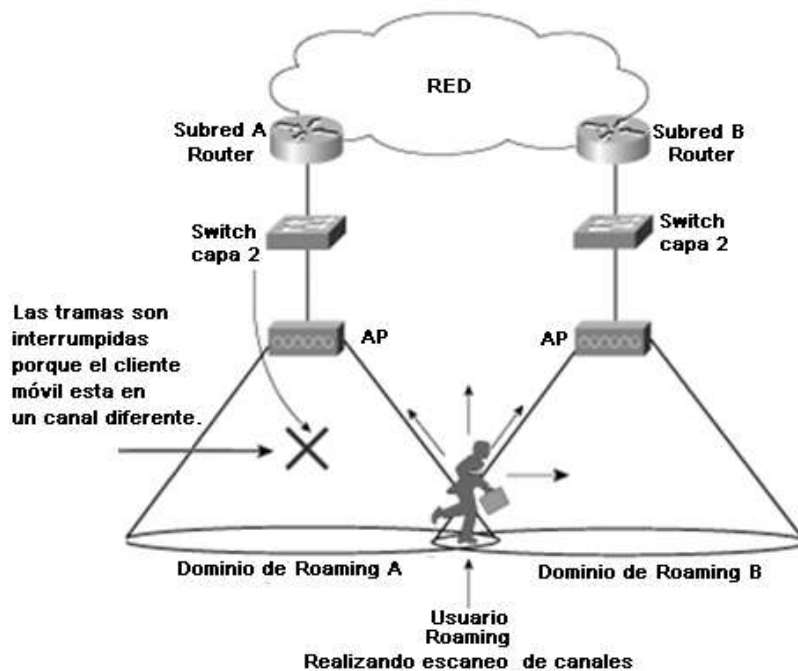


Figura 1-8 Descubrimiento de AP preventivo.

- El cliente no puede recibir los datos del AP en el que se encuentra asociado mientras que está escaneando los canales de forma activa o pasiva - Si el AP envía los datos a la estación móvil mientras que se realiza la búsqueda en los canales (lo que significa que la estación móvil está en diferentes canales dentro del AP), si se pierden los datos son retransmitidos por el AP.
- La estación móvil experimenta la degradación del servicio - La estación móvil no es capaz de transmitir datos al mismo tiempo que realiza la búsqueda activa o pasiva de los canales, por lo que cualquier aplicación que se ejecute en el cliente puede experimentar degradación del desempeño.

El descubrimiento de AP preventivo, puede ser interrumpido por el rápido movimiento de la estación móvil. Un cliente se puede mover tan rápido que el AP que estaba predeterminado para el *roaming* ya no es el mejor, por lo cual se deben hacer nuevamente decisiones de *roaming* y de esta manera se ve afectado el desempeño de las aplicaciones que están en el cliente móvil.

1.4.8.2 Descubrimiento de AP en el momento del *roaming*

La otra opción para el descubrimiento de AP es buscar un AP después de la decisión de desplazarse enviando a los nuevos AP tramas de reasociación, este tipo de descubrimiento no tiene el encabezado del *roaming* preventivo y debido a que la estación móvil no sabe a qué AP reasociarse puede durar mucho más tiempo el proceso de *roaming*, ver Figura 1-9 [10].

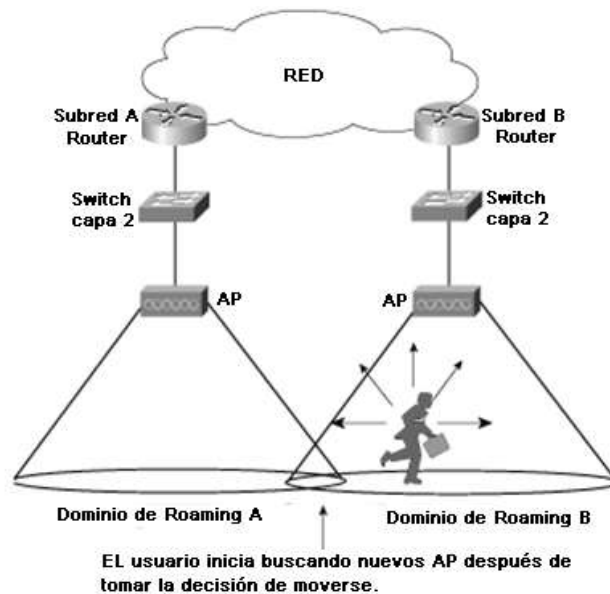


Figura 1-9 Descubrimiento de AP en el momento del *roaming*.

1.4.9 Proceso de *roaming* en la capa 2.

El proceso de *roaming* involucra muchos más procesos que sólo buscar y comunicarse con nuevos APs, la siguiente lista presenta algunas de las tareas a efectuarse durante el

roaming en la capa 2 [10]:

1. El AP actual debe determinar que la estación móvil se está moviendo fuera del área de servicio.
2. El AP debería destinar un *buffer* de datos para que la estación móvil pueda realizar el *roaming*.
3. El nuevo AP debería indicar al antiguo AP que la estación móvil puede realizar el *roaming* sin ningún problema, este paso suele activarse por medio de paquetes *unicast* o *multicast* del AP antiguo al AP nuevo transmitiéndole como dirección MAC fuente la MAC de la estación móvil.
4. El AP antiguo debe enviar el *buffer* de datos al nuevo AP
5. El AP antiguo debe determinar que la estación móvil se está alejando de su radio de cobertura.
6. El AP debe actualizar la tabla de direcciones MAC dentro del *switch*¹⁰ para prevenir las pérdidas de datos de la estación móvil.

Los pasos 2 y 3 no son obligatorios, ya que no están especificados en el estándar 802.11.

La Figura 1-10, Figura 1-11 y Figura 1-12 [10] ilustran una estación móvil entre dos APs en el mismo dominio de *roaming* conectándose a los diferentes conmutadores de Nivel 2.

En la Figura 1-10 [10], el servidor de aplicaciones envía los datos a la estación móvil con una dirección MAC A.B. El *switch* de capa 3 (L3) transmite las tramas con dirección de destino MAC A.B al SW1 a través de la interfaz 1 (Int 1). El SW1 comprueba su tabla de envío y transmite las tramas a AP1.

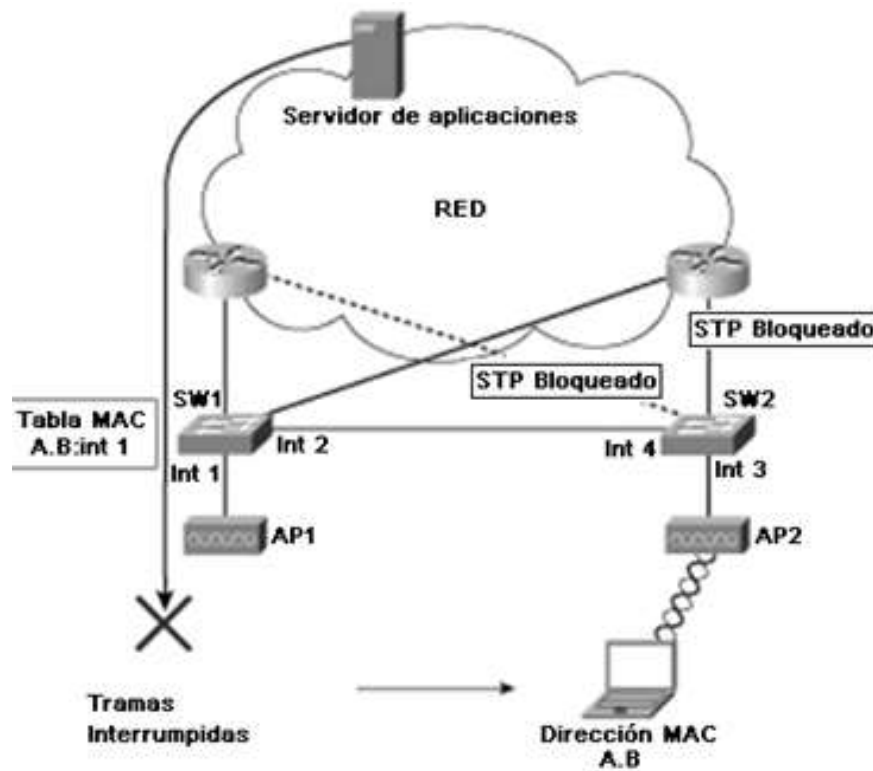


Figura 1-10 Solicitud de envío de datos a una estación móvil.

¹⁰ Dispositivo de conectividad de Capa 2

En la Figura 1-11 [10], la estación móvil se ha transferido al AP2 desde AP1, pero AP1 no sabe que el cliente se ha movido lejos de su cobertura. El servidor de aplicaciones sigue enviando las tramas a L3, y L3 a su vez envía las tramas a través de Int 1 al SW1 y AP1. AP1 intenta enviar las tramas a la estación móvil pero no pueden ser recibidos porque abandonó la conexión, a causa de esto no habrá respuesta. El AP2 resuelve esta situación mediante el envío de un paquete al AP1 en el cual el campo de dirección MAC fuente es la dirección MAC de la estación móvil, en este caso la dirección A.B.

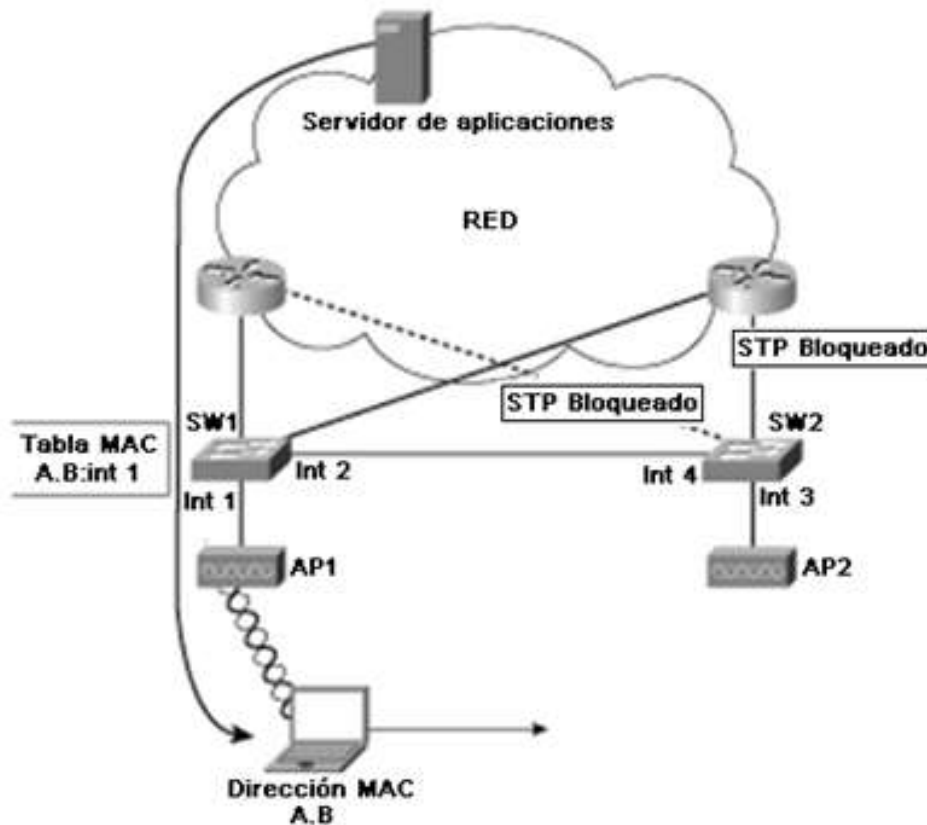


Figura 1-11 Pérdida de datos después de realizar el *roaming*.

En la Figura 1-12 [10], el AP2 envía una trama con dirección MAC fuente de la estación móvil a AP1, en este caso SW2 actualiza la tabla de direcciones ya que se ha recibido una nueva dirección MAC, la dirección de origen de las tramas (la dirección MAC A.B de la estación móvil) se asigna en la tabla de direcciones MAC y a la interfaz de entrada (Dirección MAC A.B asignada a Int 3). El switch de capa 3 (L3) actualiza su tabla para indicar el destino que se encuentra accesible en la interfaz 0 (Int 0). Las tramas se reenvían a SW1, y SW1 actualiza su tabla de la misma manera, SW1 está comprobando las direcciones MAC de las nuevas estaciones móviles para que los paquetes sean correctamente transmitidos a través de SW2 y AP2.

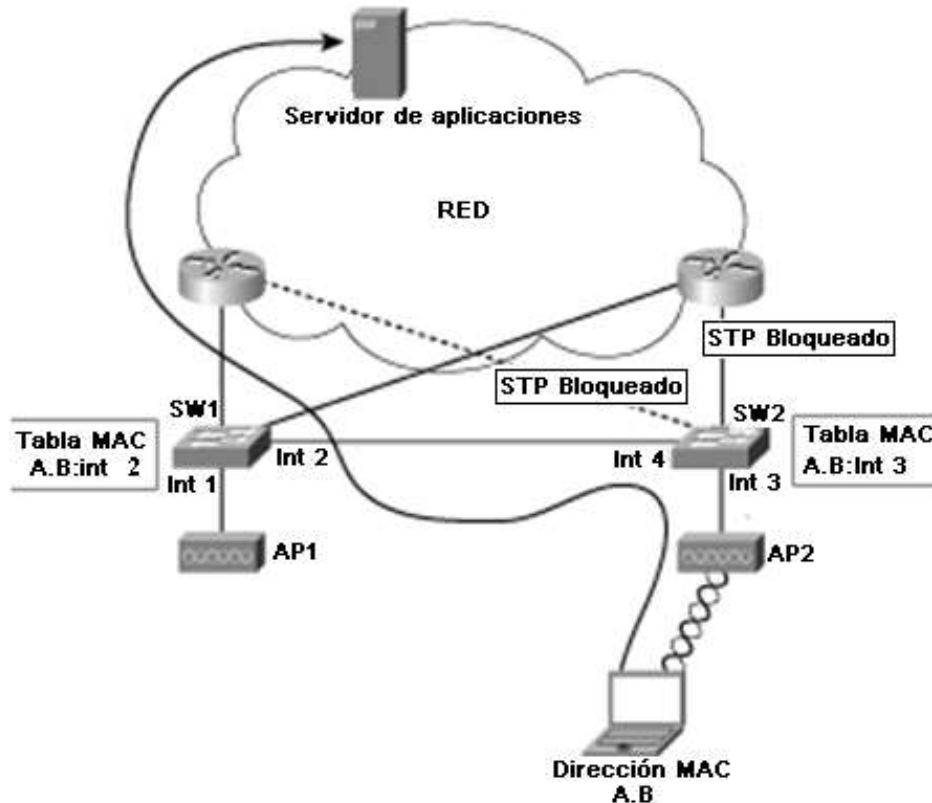


Figura 1-12 Actualización de las tablas de direcciones MAC.

Todo este proceso de *roaming* que se realiza cuando una estación móvil se mueve entre coberturas de diferentes APs y puede tomar un tiempo de entre 100 hasta 600 ms dependiendo de los fabricantes de los dispositivos usados[7]. Con esto se demuestra que el tiempo que normalmente toma el proceso de *roaming* es muy grande para aplicaciones como video y audio *streaming* ya que para estos un retardo mayor a 10 ms es detectable en forma de detrimento de la calidad de lo que se está escuchando, viendo o ambas, y es aquí donde radica la importancia del presente trabajo de grado ya que éste se enfoca directamente a este problema.

1.5. STREAMING

Esta tecnología permite usar la red para acceder a un contenido multimedia directamente emitido desde un portal en internet, un servidor dedicado multimedia o desde un dispositivo móvil, existen dos modalidades para la transmisión de este servicio las cuales pueden ser:

1.5.1 Streaming con precarga de *buffer*

Al acceder al servidor se inicia la transmisión de los paquetes a la estación cliente realizando una precarga del contenido cada vez que se ha descargado un nivel de paquetes óptimo que permita ser visualizado, en este caso depende de la aplicación de visualización u otros factores como la tasa de visualización. Éste contenido es precargado y visualizado dependiendo de la tasa de transmisión de paquetes del servidor a la estación cliente. El contenido es descargado totalmente en un *buffer* en la estación cliente para ser visualizado las veces que se requieran o que se desee. En este caso el

archivo multimedia origen no presenta cambios de ningún tipo. Por ejemplo, es una canción referenciada que puede oírse desde un portal web, la movilidad no afecta demasiado a este tipo de *streaming*, pues, el contenido es estable y solo hay que esperar a que los paquetes sean retransmitidos en caso de tener pérdidas.

1.5.2 *Streaming* en tiempo real

Al acceder al servidor existe un lapso de tiempo en el que son descargados los paquetes principales en la estación cliente, al iniciar la tasa de transmisión se crea un pequeño *buffer* en la estación cliente el cual tiene la particularidad de ser rescrito, esto quiere decir que mientras el contenido es descargado es puesto en cola y a la vez visualizado, de esta forma el *buffer* no ocupa grandes cantidades de información, debe existir un equilibrio entre la velocidad de visualización y la llegada de los paquetes a la cola del *buffer* en la estación cliente pues de lo contrario se eliminarán los paquetes porque el *buffer* ya está lleno o la visualización se cancelará por la falta de paquetes, la movilidad afecta enormemente, pues los paquetes perdidos no se pueden visualizar dejando al contenido entrecortado o requiriendo carga de *buffer* siendo esto un problema. Por ejemplo, un concurso el cual se transmite por *streaming* a un dispositivo móvil y en el momento antes de nombrar al ganador se empiezan a perder paquetes, esto no permitirá saber quien fue el ganador. En las capas superiores se tienen los protocolos multimedia, existen combinaciones entre los protocolos de las capas superiores para mejorar el acceso y facilitar la recepción del *streaming*, combinaciones como *streaming* de multimedia (MMS, *Multimedia Streaming*) sobre HTTP¹¹ o protocolo de mensajería en tiempo real (RTMP, *Real Time Messaging Protocol*) sobre HTTP son muy comunes en plataformas de internet¹². Todos los protocolos multimedia están diseñados para trabajar sobre TCP o UDP en la capa de transporte, algunos pueden trabajar sobre cualquiera de los dos como lo son RTSP, MMS. Etc.

- **Protocolo de transporte en tiempo real (RTP, *Real-time Transport Protocol*):** Implementa números de secuencia de paquetes IP para rearmar la información de voz y video, incluso cuando la red cambie de orden los paquetes de llegada brindando un medio uniforme de transmisión sobre IP sujeto a las limitaciones de audio y video. Antes del envío de los paquetes se identifica la información a transmitir agregándole marcadores temporales y números secuenciales controlando la llegada de los paquetes al destino.
- **Protocolo de control de transporte en tiempo real (RTCP, *Real-time control transport protocol*):** Se basa en transmisiones periódicas de paquetes de control que realizan todos los participantes de la sesión. Este es un protocolo de control para los flujos RTP permitiendo transmitir información sobre los participantes de la sesión y manejar calidad de servicio.
- **RTMP** - Combinación entre RTP y RTCP: el protocolo RTMP permite la administración de flujos multimedia (voz, video) sobre IP, debido a que RTP funciona sobre el protocolo UDP, el encabezado RTMP lleva información de sincronización y numeración.

¹¹ Protocolo usado ampliamente por internet, para la transmisión de información.

¹² Internet es la gran red de redes, por medio de la cual se comparte información de todo tipo.

Existen diversas técnicas para el uso eficiente de nuevos sistemas de multimedia como videoconferencia, *streaming* e IPTV. Se necesita un ajuste en la sincronización de los datos además de una forma especial de transmisión resguardada por los protocolos especializados y un grupo de capas multimedia divididas en señalización, calidad de servicio y transporte multimedia. La falta de información llevó a la construcción de la Figura 1-13 con el fin de tener un orden que involucrara la parte multimedia y Wi-Fi dentro de las capas de aplicación, presentación, sesión y transporte así como también las capas de red enlace de datos y física.

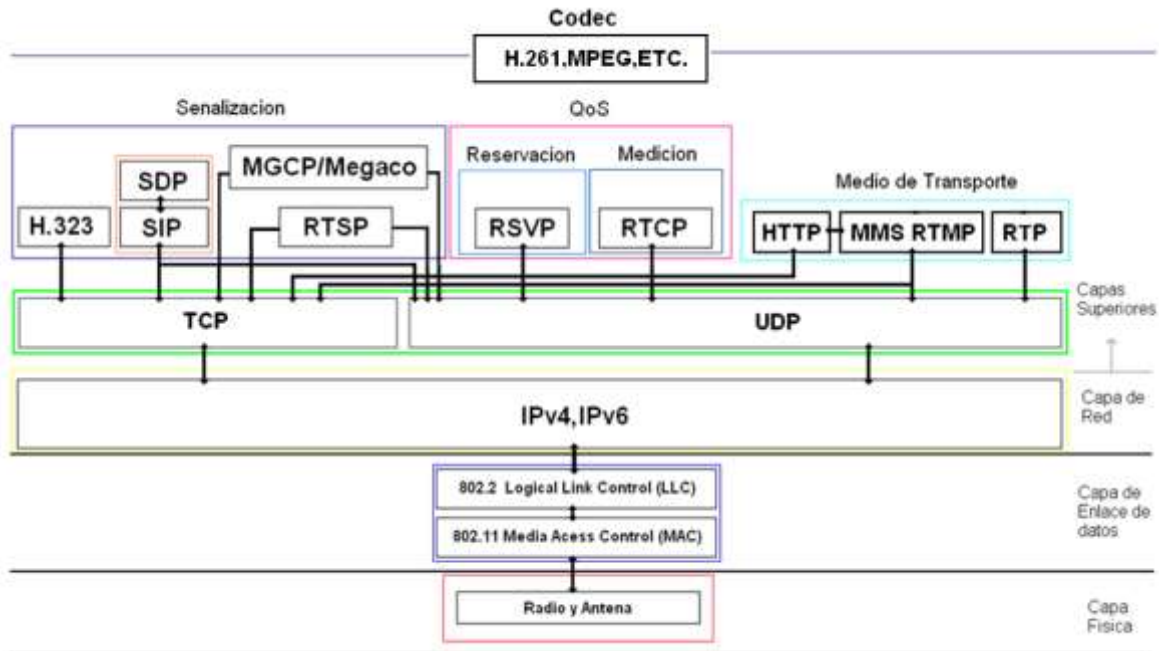


Figura 1-13 Capas de OSI para multimedia y 802.11.

1.5.3 Percepción humana

Lo importante en una comunicación es dar la percepción de tiempo real, esto significa una sincronización de todas las tramas transmitidas, pero la movilidad y otros factores afectan las tasas de envío y recepción de paquetes cambiando la alineación temporal de las tramas, pero aún una desalineación de audio y video es tolerable e imperceptible si es de menos de 20 milisegundos. La sensibilidad humana varía de acuerdo a la persona, siendo más imperceptible la desalineación y la falta de calidad para unos usuarios que para otros. La sensibilidad está determinada por la velocidad de las tramas (cuadros) y la resolución; el informe IS-191 emitido por el comité de sistemas de televisión avanzada (ATSC, *Advanced television Systems Comitte*) recomienda directrices respecto a la tolerancia máxima para los sistemas de emisión y lograr una calidad aceptable. Las directrices establecen que para cada flujo la incertidumbre no se debe exceder ± 15 milisegundos, existen 2 criterios para la tolerancia de sincronización tomando audio y video en codificaciones divididas.

- **Criterio de adelanto del audio** - En el peor escenario, el audio esta adelantado del video en la entrada del codificador 15 ms. El receptor suena el flujo de audio antes que el flujo de video con 15 ms de diferencia mientras que el flujo de video está 15 ms retrasado. Como resultado, la cantidad máxima de tiempo que el audio puede estar adelantado del

video en el dispositivo de presentación en el receptor es de = 45 ms [11].

- **Criterio de retraso de audio** - En el peor escenario, audio se atrasada del video en la entrada del codificador 45 ms. El receptor muestra que el flujo de audio con 15 ms de retraso mientras que el flujo de video esta 15 ms adelantado. Como resultado, la cantidad máxima de tiempo que el audio se puede atrasar del video en el dispositivo de presentación del receptor es de 75 ms [11].

1.5.4 Medición del desfase

El desfase del audio/video se mide en el dispositivo de salida justo en el tiempo de presentación. El dispositivo de salida se le llama también el dispositivo de presentación y el tiempo de presentación depende del dispositivo de salida:

- Para las pantallas de vídeo, el tiempo de presentación de una trama en una secuencia de video es el momento en que la imagen parpadea en la pantalla.
- Para los dispositivos de audio, el tiempo de presentación de trama en una secuencia de audio es el momento final de la muestra de audio.

El momento de la presentación de audio y de vídeo en los dispositivos de salida debe coincidir con el momento de la captura en los dispositivos de entrada. Estos dispositivos de entrada (cámara, micrófono) se denominan también dispositivos de captura. El método para determinar el tiempo de captura depende de los medios de comunicación:

- Para una cámara de vídeo, El tiempo de captura de un (trama) fotograma de vídeo es cuando el dispositivo de entrada se carga y acopla (CCD- *charge-coupled device*) a la cámara de video y se registra una imagen.
- Para un micrófono, El tiempo de captura de un (trama) buffer de audio es cuando el micrófono transductor graba el sonido en una muestra.

La Figura 1-14 [11] proporciona otra forma de ver la sincronización de los medios de comunicación. Este diagrama muestra el momento de ejecución de un gran número de flujos del dispositivo de presentación receptor sin sincronización.

Cada flujo podría ser un flujo de audio o vídeo. El marcador gris en cada secuencia corresponde al momento en que fueron enviadas las tramas, el reloj en el emisor es común para todos los paquetes y es la referencia para establecer la sincronización en la recepción, todos deben estar alineados sobre la línea gris, entonces, ahora el objetivo es añadir retardo a las tramas que llegan demasiado rápido, de modo que se sincronicen y sean ejecutadas al mismo tiempo.

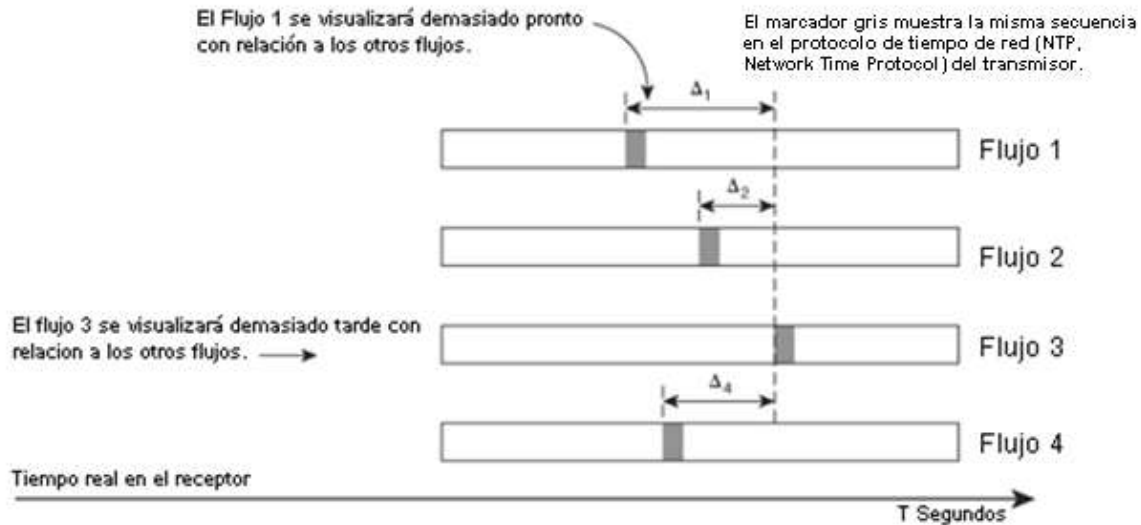


Figura 1-14 Recepción de los flujos sin sincronización.

1.5.5 Acumulación de retrasos

El desfase entre audio y video se puede acumular con el tiempo ya sea por la vía de vídeo o audio. Cada etapa de la videoconferencia, *streaming* o comunicación multimedia inyecta retardo, y estos retrasos están comprendidos en tres categorías principales: [11]

- **Las demoras en el transmisor** - La captura, codificación, y empaquetamiento crean demoras en los dispositivos de *hardware* final.
- **Retrasos en la red** - La red introduce retardos, incluyendo *gateways* y transcodificadores.
- **Las demoras en el receptor** - La demora por el *buffer*, el decodificador, y la demora en la reproducción de los dispositivos de *hardware* final.

Sin embargo, la mayoría de estos retrasos son desconocidos, difíciles de medir y cambian con el tiempo. La Figura 1-15 [11] presenta diferentes retrasos de audio y video de extremo a extremo, emitidos por caminos en los que se puede acumular retrasos con el tiempo, causando la asimetría entre el audio y el vídeo. El primer gráfico en la esquina superior izquierda muestra la relación original entre el vídeo y audio. También se muestra un escenario en el que la asimetría entre el audio y el vídeo aumenta en tres etapas de extremo a extremo de la ruta entre la fuente y el receptor. La red alberga elementos que introducen retrasos en los paquetes. En una red inalámbrica es mucho más considerable la opción de *buffers* ya que las tramas son enviadas y desalineadas llegando al cliente sin la sincronización adecuada para una perfecta reproducción.

La Figura 1-16 [11] enseña el video y el audio transmitidos desde una cámara y un micrófono respectivamente, lo primero que sucede es la captura de las señales analógicas en cada *hardware*, luego se pasa a una etapa en la cual son convertidas a señales digitales realizándole distintos procesos de compresión y codificación tanto al audio como al vídeo, a continuación, se empaquetan los datos codificados para el transporte a través de la red.

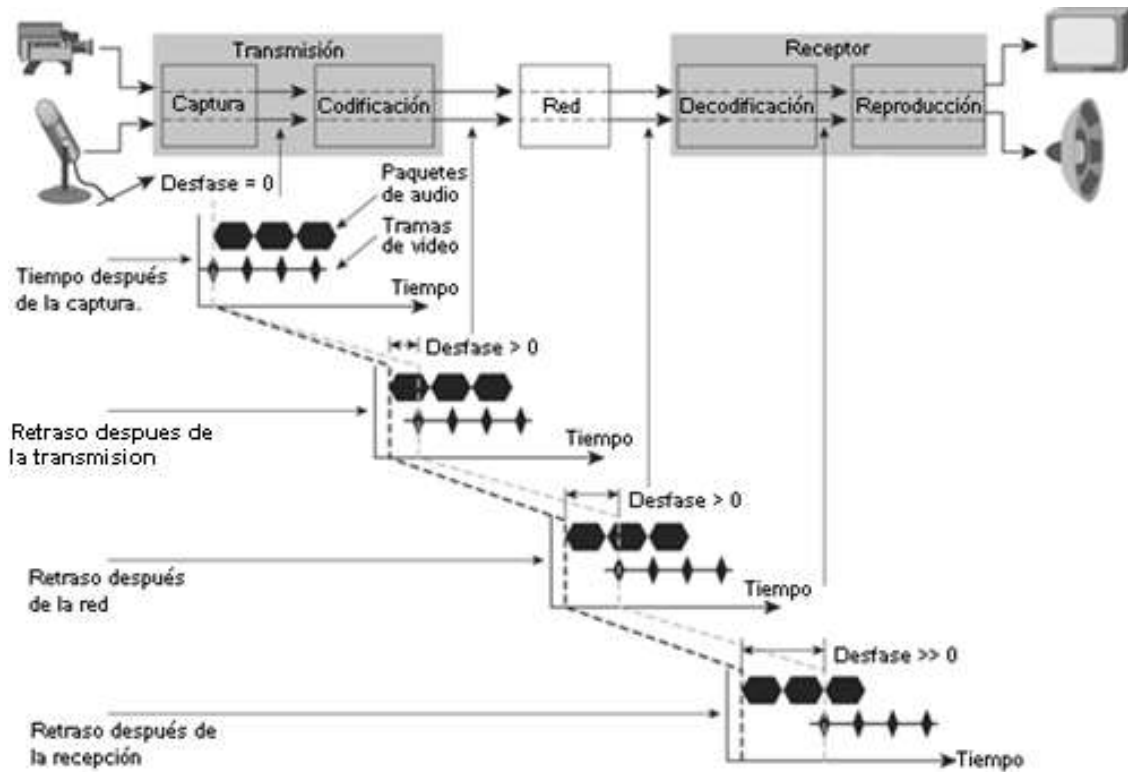


Figura 1-15 Acumulación del desfase de audio y vídeo.

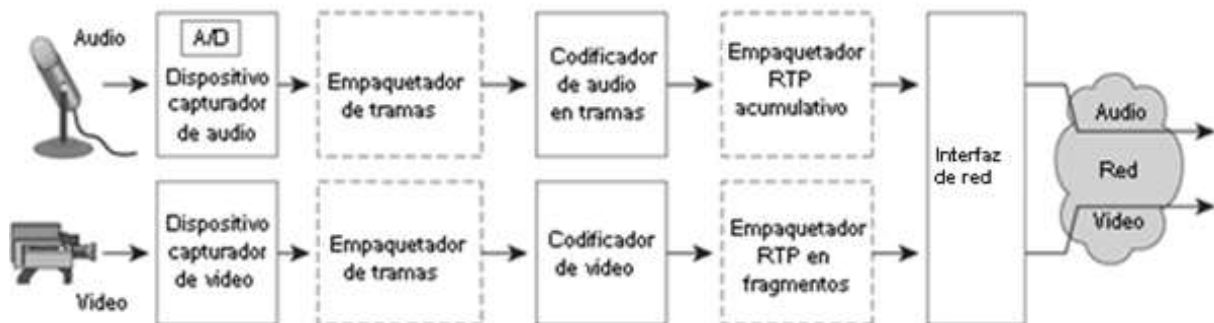


Figura 1-16 Procesamiento de fuente de audio y vídeo.

1.6 Transmisión de audio

Primero se usa un convertor análogo/digital para tomar muestras de audio analógico y convertirlas en muestras digitales. Para entender bien la sincronización es necesario entender cómo se procesan cada uno de los paquetes y analizar los puntos donde se presentan los retardos como los siguientes [11]:

- **Retardo en la captura y empaquetado del audio:** Normalmente, el *hardware* captura el audio y lo transforma en paquetes que contienen un número fijo de muestras. Los dispositivos o computadores tienen tamaños de paquetes configurables. Los tamaños de los paquetes vienen especificados en unidades de muestras. Por ejemplo si la frecuencia de muestra es de 44,1 kHz (44100 muestras / segundo), y si el paquete es de 64 muestras

le corresponde un retardo de:

$$\frac{64 \text{ muestras}}{44100 \text{ muestras x segundo}} = 1.5 \text{ ms}$$

El ejemplo anterior manda 689 paquetes por segundo. Si cada muestra es de tamaño de 16 bits, con canales izquierdo y derecho, cada paquete contiene:

$$64 \text{ muestras} \times 2 \text{ bytes/muestra} \times 2 \text{ canales} = 256 \text{ bytes}$$

- **Retardo del empaquetado de codificación:** Los codificadores/decodificadores de audio usan un algoritmo que toma partes de tamaño fijo de datos de entrada, conocidos como tramas de audio y produce salida de tramas de audio codificadas. Estas tramas no deben confundirse con las tramas de vídeo. Por ejemplo, el codificador/decodificador de audio G.723 especifica un tamaño de trama de entrada de 30 ms. Por 8-kHz de audio mono, 30 ms correspondientes a 240 bytes. Debido a que los codificadores/decodificadores deben tomar tramas de tamaño fijo de datos como entrada, es responsabilidad de la aplicación multimedia recoger los paquetes de la tarjeta de audio y empaquetarlos en tramas de la longitud adecuada para el codificador/decodificador. Debido a que se debe reunir múltiples paquetes de audio para montar una trama de audio, este tipo de empaquetado se considera como un proceso agregado [11].

La agregación siempre adiciona un retardo, porque el empaquetador debe esperar múltiples paquetes de entrada.

- **Retardo en el proceso de codificación:** Este retardo es causado por la codificación de audio de cada uno de las tramas hasta completar el proceso antes que la próxima trama de audio llegue. El codificador/decodificador G.711 utiliza un algoritmo simple que puede procesar tramas de audio casi sin demora. Por el contrario, el codificador/decodificador G.723 es más complejo y puede implicar un retardo. Sin embargo, para cualquier codificador/decodificador si se excede el retardo en un fragmento de tiempo puede presentar inconvenientes.

- **Retardo en el empaquetado RTP:** El empaquetado RTP reúne uno o más paquetes de audio codificados, y los vuelve un paquete RTP con cabecera RTP. El retardo de este tipo de empaquetado es desde el momento en que el empaquetador recibe los datos de audio suficientes para construir las tramas correspondientes a un paquete completo de RTP. Cuando está completo el paquete se envía a través de la interfaz de red.

Tanto el tamaño de los paquetes de audio codificados y el tamaño de los paquetes RTP implican retrasos significativos en el lado del que envía, por dos razones:

- **Procesamiento del paquete entero** - Los codificadores/decodificadores de audio avanzados, tales como G.728 necesitan tener acceso a todas las tramas de entrada de datos de audio antes de que se pueda comenzar el proceso de codificación. Este debe reunir múltiple tramas de audio para luego proceder a la codificación. Pero codificadores/decodificadores con baja complejidad, tales como G.711, no tienen que esperar que llegue la trama completa de datos. Debido a que el codificador/decodificador G.711 puede operar sobre muestras simples de audio a la vez, tiene un bajo retardo de tan sólo una muestra.

- Retardo en el empaquetado RTP - El empaquetado RTP especifica que las tramas de audio codificadas no deben ser fragmentadas a través de los paquetes RTP. Además, para una mayor eficiencia, un paquete de RTP contiene múltiples tramas de audio codificadas. El retardo de la interfaz de red es bajo en comparación con la etapa inicial y la etapa final. En la Figura 1-17 [11] se observan los procesos que sufre el audio desde su captura hasta el momento de la transmisión del paquete y los retardos en cada uno de estos eventos.

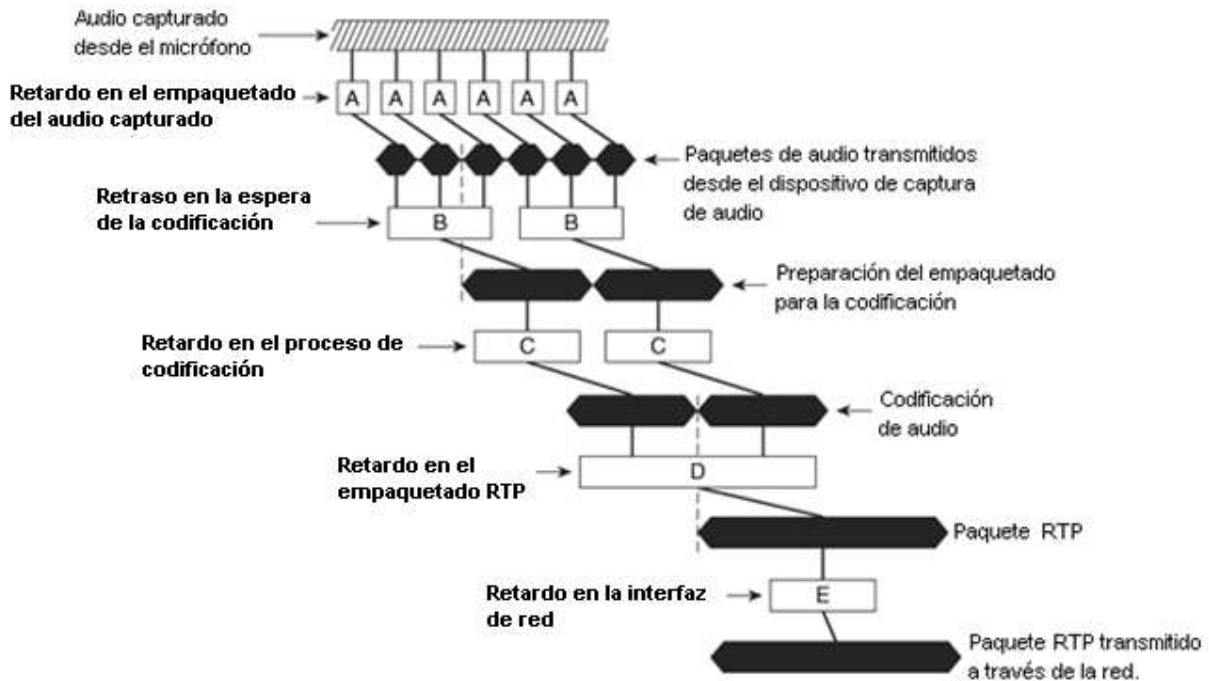


Figura 1-17 Retrasos de audio.

1.7 Formato fuente del vídeo

La mayoría de las terminales pueden aceptar señales de vídeo analógico de definición estándar de cámara de video. Existen tres formatos de vídeo [11]:

- Comité de sistemas nacionales de televisión (NTSC, *National Television System Committee*), utilizada principalmente en América del Norte y Japón.
- Línea alternada en fase (PAL, *Phase Alternating Line*), utilizado principalmente en Europa
- Color secuencial con memoria (SECAM, *Séquentiel Couleur à Mémoire*), utilizado principalmente en Francia

Para cada formato hay una resolución máxima y una tasa de envío de tramas correspondiente [11]:

- Formato NTSC resolución de 640x480 tasa de tramas de 29,97 tramas por segundo (FPS, *frames per Second*).
- Formato PAL, resolución de 720x576 tasa de tramas de 25 fps.
- Formato SECAM 720x576 tasa de tramas de 25 fps.

La resolución vertical de un fotograma (trama) de vídeo se mide en líneas de vídeo, y la resolución horizontal se mide en píxeles. A pesar de que la señal de vídeo NTSC tiene una velocidad de 29,97 fotogramas por segundo, la frecuencia de cuadro se la conoce como 30 FPS (fotogramas por segundo). Cada uno de estos formatos utiliza un proceso de búsqueda llamado entrelazado, lo que significa que cada trama es en realidad compuesta por dos campos entrelazados. La Figura 1-18 [11] muestra una secuencia de fotogramas (tramas) entrelazados de vídeo NTSC.

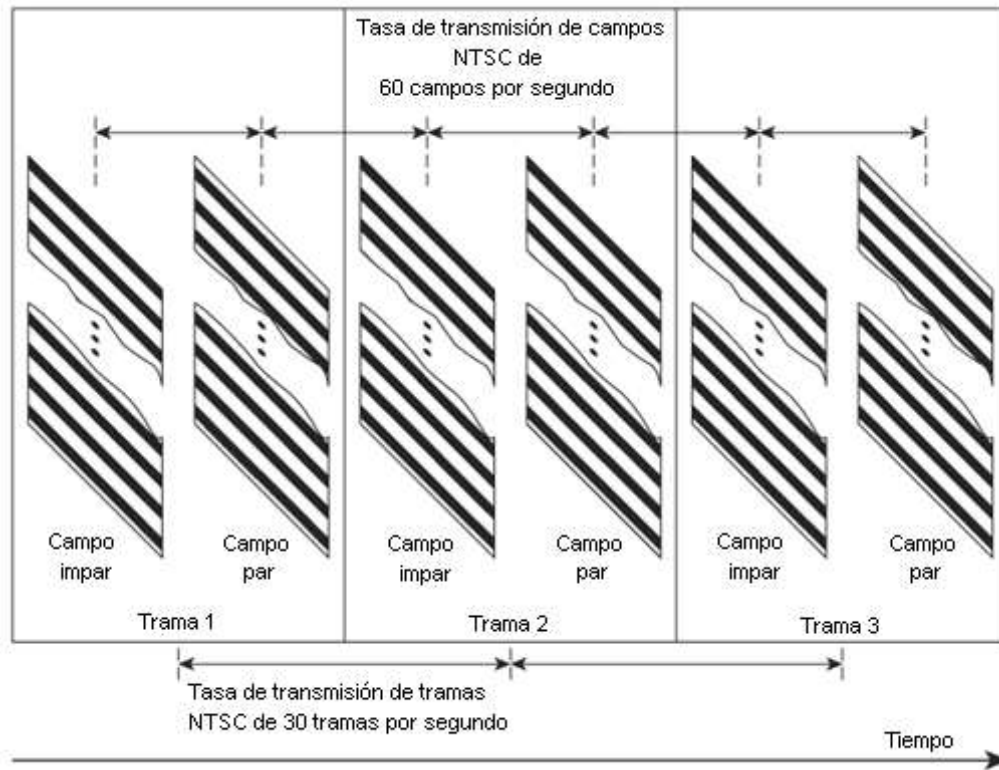


Figura 1-18 Secuencia vídeo entrelazado.

En la secuencia de la Figura 1-18, cada una de las tramas consta de dos campos: el campo impar es el primer campo y el campo par es el segundo campo. El campo impar capta cada línea de vídeo a partir de la primera línea. El campo par capta cada línea de vídeo a partir de la segunda línea. La tasa de campo es el doble de la frecuencia de trama, en este ejemplo, la tasa de campo es de 60 campos por segundo. El campo que se inicia con la línea superior de vídeo entrelazado en la trama se denomina el campo superior y el campo que termina con la línea inferior de vídeo entrelazado se denomina el campo inferior.

1.5.3 Transmisión de vídeo

El *hardware* de captura de vídeo digitaliza cada imagen de la cámara de vídeo y almacena la resultante de los campos de vídeo en una serie de *buffers* circulares en la memoria como se muestra en la Figura 1-19 [11].

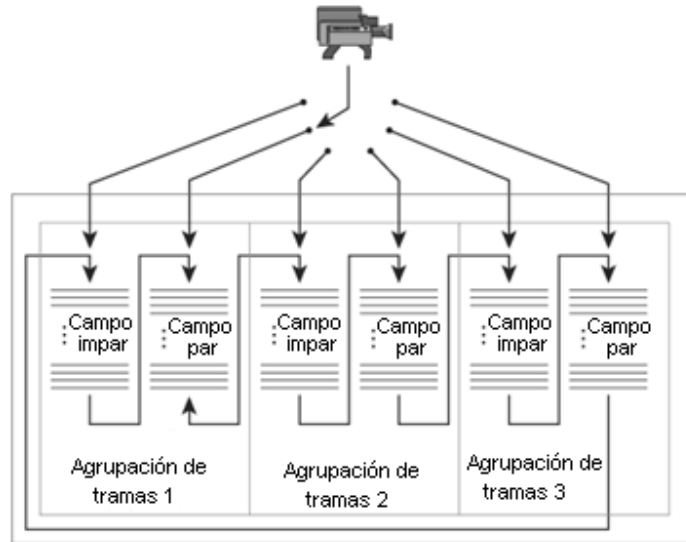


Figura 1-19 Buffer de captura de vídeo.

El *hardware* realiza la captura y se llena el *buffer* de tramas hasta la llegada de la última trama. Luego se inicia nuevamente el bucle empezando desde la trama 1 sobrescribiendo los datos en el *buffer*. Cada *buffer* de tramas contiene dos campos: el campo impar y el campo par de vídeo entrelazado. Para reducir el retardo de la captura y codificación, el codificador de vídeo inicia un nuevo campo de vídeo antes de la captura de *hardware* escribiendo todo en el campo de memoria con *buffers* en blanco. La Figura 1-20 [11] señala dos posibles escenarios de retardo en la captura de vídeo para el transmisor.

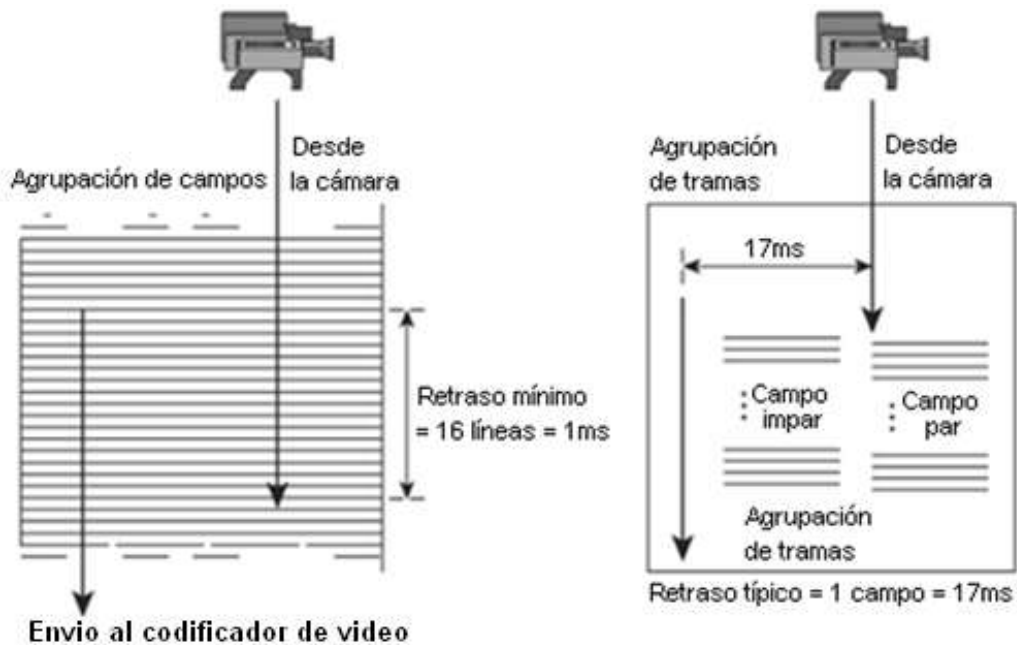


Figura 1-20 Retraso en la captura y codificación del vídeo.

La mayoría de los codificadores de vídeo funcionan con fragmentos de datos de vídeo que constan de 16 líneas a la vez. Por lo tanto, el codificador puede presentar bajo retardo en la captura para la procesando los datos después de que el dispositivo de captura a llenado o escrito las 16 líneas en el buffer lo cual corresponde a 1ms. Sin embargo, algunos codificadores de vídeo pueden esperar un campo entero de vídeo para llenar un *buffer* de tramas antes de comenzar el proceso de codificación para ese campo. En este caso, el retardo en la captura de vídeo es de 1 campo de video, que corresponde a 17 ms.

Un codificador puede codificar vídeo a una resolución mucho más baja, la Figura 1-21 [11] contiene un codificador que funciona a una resolución de 320x240, a una tasa nominal de envío de tramas de 30 de FPS, por la extracción de todos los campos impares y la escalabilidad de 640x240 a 320x240.

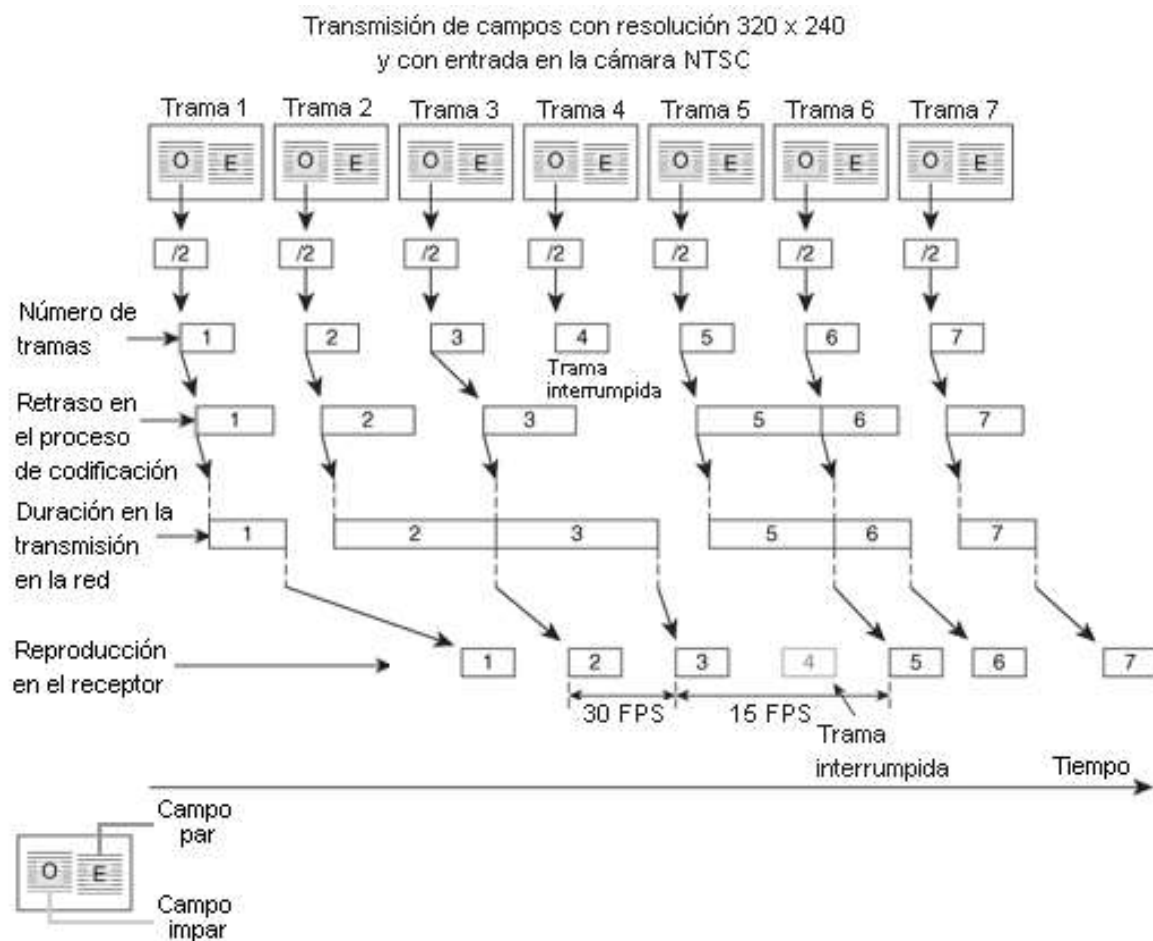


Figura 1-21 Proceso para codificar 30 FPS vídeo.

En este escenario, el codificador normalmente codifica todos los campos impares para alcanzar 30 FPS. Sin embargo, si el contenido del vídeo cambia en grandes proporciones como resultado del excesivo movimiento en el flujo de vídeo, el codificador puede fallar por dos razones:

- Los requisitos en procesamiento del codificador pueden aumentar, resultando un mayor retardo de codificación por trama, con lo cual el codificador reduce la velocidad de envío

de tramas.

- El movimiento extra en la entrada de vídeo podría hacer que el tamaño de los fotogramas (tramas) codificados se incrementen temporalmente. Luego de codificar las tramas más grandes, estas se envían con una tasa de transmisión que idealmente sería constante, y por lo tanto, el transmisor puede fallar al intentar transmitir en la red a tiempo real los fotogramas (tramas) codificados debido al tamaño y a la no continuidad de la tasa de transmisión. En respuesta, el codificador puede decidir saltarse las tramas para reducir la velocidad de envío de las mismas. Pausar temporalmente el proceso de codificación permite que la codificación de vídeo en flujo de bit no se envíe desmesuradamente por la interfaz de red.

La Figura 1-21 [11] presenta un ejemplo en el que tramas más grandes de vídeo codificado pueden causar que la transmisión ya no fuese en tiempo real. Típicamente los codificadores rastrean el retraso desde la captura hasta el tiempo de transmisión, si este retraso es superior al umbral, el codificador empieza a perder paquetes hasta que se sincroniza. En este ejemplo el codificador se atrasa y decide recobrar la sincronía dejando perder el cuarto paquete. Los codificadores realizan esta tarea rutinariamente para cambiar entre la velocidad de envío de las tramas, la calidad y la velocidad de bits. Existen dos tipos de retardos relacionados con el trayecto del vídeo en el lado de la captura [11]:

- Retardo en codificación de vídeo - Es el tiempo que se demora en codificar todas las tramas generadas. El vídeo que contiene grandes cantidades de movimiento toma más tiempo en ser codificado. En la Figura 1-21, el retardo del codificador cambia a través de la línea del tiempo. Sin embargo, a pesar de las variables de retardo introducidas por el codificador de vídeo a través del tiempo, el flujo de vídeo es reconstruido en el receptor con uniformidad de tiempo. En la parte de protocolo de transporte se tiene un retardo en la creación del empaquetado provisto por el protocolo.
- Retardo de empaquetamiento en RTP - La especificación de RTP determina la forma en que el flujo de bits de vídeo debe ser puesto en paquetes RTP. Típicamente, los *codificadores/decodificadores* de vídeo dividen la imagen de entrada en secciones llamadas *slices*, o grupos de bloques (GOB, *Group of Blocks*). En el proceso de empaquetamiento RTP se debe empalmar el flujo de bits codificado en estos puntos de corte o división del vídeo. Por lo tanto, el empaquetamiento RTP de vídeo debe esperar un cierto número de secciones enteras de flujo de bits de vídeo para llenar todo un paquete RTP. Este empaquetamiento causa un retardo necesario para componer un paquete RTP.

El proceso de recepción de audio y vídeo tiene varias fases, la Figura 1-22 [11] es un modelo de todos los eventos que se presentan en una transmisión de *streaming*, se inicia con la extracción del audio y vídeo, se continúa con el módulo de *buffer* de audio, seguido por el decodificador de audio y vídeo, luego las señales de audio y vídeo son transformadas en tramas, se transmiten y reciben, se transforman de señal digital a analógica con un conversor digital/análogo (D/A) y se pasa a los dispositivos de reproducción. La parte de vídeo consiste en un decodificador de vídeo, un *buffer* de tramas de vídeo y un dispositivo de reproducción de vídeo.

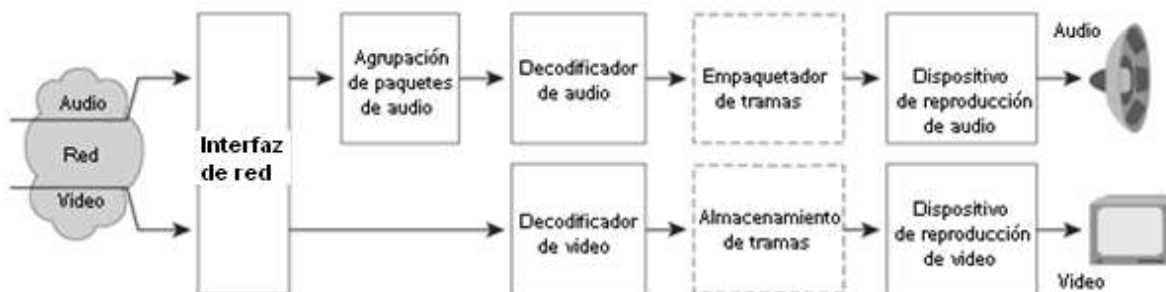


Figura 1-22 Procesamiento en el receptor.

1.5.4 Recepción de audio

El receptor utiliza un *buffer* de audio en la llegada de los paquetes, ya que no se maneja una sincronización en los tiempos de recepción y transmisión. Los paquetes se transmiten a través de la red y las fluctuaciones de velocidad modifican los intervalos de llegada de estos paquetes. El *buffer* manejado en la recepción debe ser grande para soportar los retardos temporales introducidos en el viaje del paquete, es indispensable tener un equilibrio entre tamaño del *buffer* y la reproducción para tener el menor porcentaje de retardo posible.

En el proceso de recepción de paquetes existe la posibilidad de pérdidas. La aplicación receptora de *streaming* sustituye estas pérdidas con fotogramas en blanco y silencio en el caso del audio hasta recobrar la sincronización con el servidor de *streaming*.

La Figura 1-23 [11] muestra una representación gráfica de los retrasos que suceden en la recepción de paquetes. Cada trama incluye varios fotogramas de video y *buffers* de audio, esto se debe a que en la recepción sólo ocurren 2 procesos, el desempaquetado y la reproducción y no se realiza un proceso de agregación a los paquetes recibidos.

El receptor presenta retardo en el vídeo:

- Retardo en el empaquetado - Este retardo puede ser necesario si el decodificador de vídeo necesita tener acceso a más de un grupo de bloques para iniciar el proceso de decodificación.
- Retardo en la decodificación - Este retardo es introducido en la reconstrucción de las trama de video.
- Retardo en la sincronización - Si es necesario, el receptor puede imponer un retardo en los fotogramas de vídeo para lograr la sincronización.
- Retardo en la reproducción - Luego de decodificar la última trama esta se pone en memoria, el retardo que se introduce aquí es el tiempo de espera hasta que se visualiza en la pantalla.

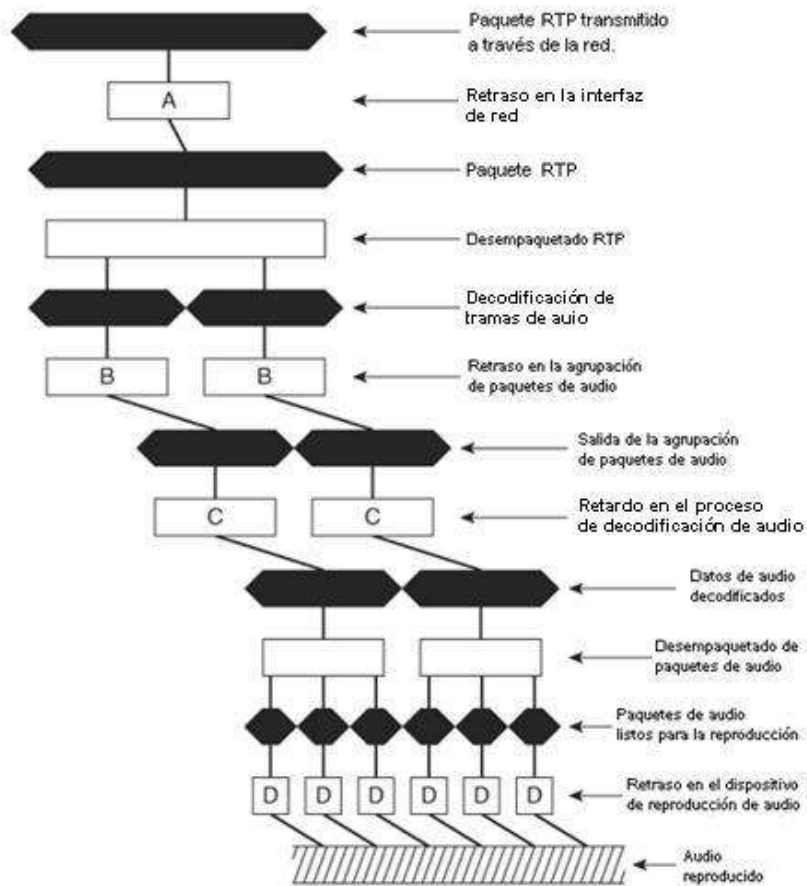


Figura 1-23 Acumulación de retardos en el proceso de recepción de audio.

1.6 FACTORES QUE INFLUYEN EN EL DESEMPEÑO DEL *STREAMING*

La investigación y recolección de información requerida en este proyecto, llevó a buscar analíticamente las variables que influyen en el *streaming* de audio y video en redes inalámbricas 802.11b/g, la búsqueda de dichos factores fue prioridad antes de iniciar cualquier actividad de experimentación, estos fueron la guía y foco para las actividades de investigación práctica que se desarrollaron posteriormente. Los resultados obtenidos en las actividades ratificaron los factores influyentes en el desempeño del *streaming* previamente estudiados.

Tomando como punto de partida el escenario de una red inalámbrica en topología ESS, cuando se implementa seguridad, se brinda el servicio de *streaming* y se hace *roaming*, se deduce que todos los factores convergen en el proceso del *roaming* ya que es allí donde se pone a prueba la capacidad de transición entre puntos de acceso o *roaming*. Si se estudia profundamente el efecto de *roaming* se encuentran factores que influyen directamente en el desempeño del mismo y son: el retardo de la búsqueda de APs, la reautenticación, la reasociación y la mala práctica de *roaming* debido a problemas de configuración de la topología ESS, ver sección 1.4.

1.6.1 Análisis de los factores influyentes

Concluida la búsqueda de las posibles variables que causan problemas en el *roaming* es preciso analizar los factores que en algún momento modifican el buen funcionamiento del *streaming* sobre las redes inalámbricas 802.11b/g en topología ESS. Si se tiene claro la

implicación de estos procesos se puede seguir la experimentación concebida en el capítulo 2 sin perder las razones primordiales de la investigación. A continuación se toma cada uno de los factores influyentes y se explica su importancia dentro del desempeño del *streaming*.

1.6.1.1 Ancho de banda

De las secciones 1.1 y 1.5 se resuelve que el ancho de banda afecta el *streaming* de audio y video, en éste caso se tiene a 802.11b el cual maneja anchos de banda de 11Mbps y 802.11g el cual maneja anchos de banda de hasta 54Mbps. Si el ancho de banda utilizado entre el equipo inalámbrico y el cliente móvil es el justo para la transmisión de *streaming* es posible que se tengan problemas en el momento de la renovación de llaves en una autenticación tipo personal o en el momento de la transferencia de información de autenticación tipo empresa para los métodos WPA y WPA 2 durante el *roaming* (ver sección 1.3 y 1.4.2). Si el ancho de banda no es el indicado, la movilidad dentro de las coberturas puede causar pérdidas de paquetes y retardos mientras se despeja el ancho de banda necesario para el tránsito de los paquetes entre el servidor de *streaming* y el cliente móvil.

1.6.1.2 Movilidad

En la sección 1.4 se deduce que la movilidad causa la pérdida de paquetes debido al cambio de velocidades durante la transición entre BSSs, a las bajas potencias de transmisión, a las interferencias en el momento del desplazamiento, así como el proceso de reautenticación y reasociación. La movilidad puede definir el momento preciso y transparente del proceso de *roaming*, debido a que el algoritmo de *roaming* estudia las potencias recibidas por el cliente móvil, de este modo si el cliente se mueve de forma rápida la lectura del indicador de fuerza de señal recibida (RSSI, *Received Signal Strength Indicator*) no será lo más clara creando bancos de no lectura de información y causando una mala decisión de *roaming* por parte de dispositivo inalámbrico del cliente móvil.

1.6.1.3 Roaming

Para la ejecución del *roaming* es crucial la detección previa de APs, esto se hace por medio de una búsqueda activa en el cliente móvil, observar sección 1.4.8, esta búsqueda se hace de una forma minuciosa tratando de encontrar siempre APs libres al buscar por los canales para disminuir el tiempo que requiere una reconexión, la duración de este proceso va de 10 a 20 milisegundos dependiendo del fabricante, el retardo causado por este evento se toma como crítico debido a que hay lapsos de tiempo en los que los paquetes se acumulan causando posteriormente una carga de *buffer* en la aplicación receptora.

1.6.1.4 Reautenticación

La autenticación en el momento de la transición entre puntos de acceso puede causar tiempos de espera diferentes dependiendo de la combinación de seguridad implementada, ver secciones 1.3 y 1.4.1, el tiempo de autenticación para PSK en la cual se introduce una contraseña en el cliente y en los puntos de acceso, puede ser menor que

el tiempo de autenticación tipo empresa en la cual hay autenticaciones y conversaciones entre el cliente, el punto de acceso y el servidor de autenticación RADIUS, el retardo causado por la autenticación es más crítico porque hay que mantener la seguridad y una buena transmisión de *streaming*. No se tiene un tiempo aproximado de autenticación para las configuraciones tipo personal y empresa pero se deduce que es mucho mejor utilizar en una red inalámbrica en topología ESS tipo *campus* la autenticación personal porque los procesos requeridos son menores que los necesarios para la autenticación tipo empresa.

1.6.1.5 Reasociación

Al examinar la sección 1.4.1 se encuentra que la asociación es el método por el cual los puntos de acceso conocen a los clientes que se están desplazando en la cobertura de la topología ESS, por medio de esta asociación se reorienta el tráfico de nuevo y se entrega el tráfico en *buffer* hacia el cliente móvil, se deduce que el retardo causado por el tiempo de reasociación es crítico debido a que si no se concluye a tiempo, los paquetes en *buffer* y los nuevos paquetes no podrán llegar hasta el solicitante en el momento requerido.

1.6.1.6 Mala configuración

La mala configuración o problemas espontáneos son críticos si no se ha verificado la topología ESS, si no se tiene bien configurada la seguridad en el AP al que se va a realizar la transición. Hay tiempos tal elevados de reintento de reautenticación a tal punto de enviar una respuesta de no reautenticación, no permitiendo el *roaming* y obligando al cliente a permanecer en el punto de acceso inicial pero con paquetes con un desempeño muy bajo. Si el punto de acceso no ha sido evaluado dentro de la red de distribución y no se alcanza el servidor de *streaming* se genera un corte inmediato, por eso son críticos los errores por mala configuración. La elección de éste factor como crítico se debe a la experiencia obtenida durante la formación profesional en donde siempre hay que considerar los inconvenientes de la mala configuración.

2 IMPACTO DEL ROAMING EN REDES 802.11b/g

Este capítulo es el punto medular de este trabajo de grado, reúne toda la investigación del funcionamiento de *roaming* para los estándares 802.11g y 802.11b. El desarrollo de las actividades propuestas arrojó resultados que fueron muy importantes para la creación de recomendaciones y la confrontación de la información con el estándar 802.11r el cual brinda una posible solución al problema planteado al inicio de este documento y analizado en los factores influyentes de la sección 1.6.

2.1 INTRODUCCIÓN A LAS PRUEBAS EXPERIMENTALES

Después de la recopilación y análisis del material teórico se procedió a realizar un grupo de actividades experimentales de forma incremental logrando la recolección de datos necesarios para comparación con el estándar 802.11r. La primera actividad dentro del cronograma fue la base de todo el proyecto porque se logra la ubicación de los equipos inalámbricos y se logran conclusiones muy importantes para las siguientes actividades.

2.1.1 Plan de trabajo para la actividad base

El siguiente es un listado procedimental para lograr el mejor ritmo organizacional de las prácticas y resultados.

- Inicio y requisitos para las pruebas.
- Estudio del ambiente propicio para el montaje.
- Montaje y verificación de la topología ESS.
- Configuración y verificación de coberturas con el funcionamiento de *roaming* en la topología ESS.
- Búsqueda de variables críticas en el desempeño del *roaming*.
- Análisis de resultados y generación de conclusiones.

2.2 INICIO DE LAS PRUEBAS EXPERIMENTALES

Luego de la recolección de la información necesaria plasmada en el capítulo 1 se dedujo muchas de las acciones a seguir en las siguientes actividades, esta primera experimentación sirvió para autoanalizar fallas en la metodología e información usada, esto con el fin de mejorar la experiencia y obtener los datos específicos que se usaron posteriormente.

2.2.1 Requisitos mínimos

Las actividades propuestas se realizaron con las herramientas citadas en el Apéndice A junto con los requisitos básicos *hardware* que se presentan en la Tabla 2-1 y los requisitos básicos *software* que se presentan en la Tabla 2-2.

Hardware:

Cantidad	Descripción	Interfaz Ethernet (MAC)	Interfaz Wi-Fi (MAC)	Función
1	Computador portátil DELL,R2G,DD160G,P 2.0GH,SO Windows XP	Broadcom NetLink ® Fast Ethernet 00:1C:23:F8:63:81	Intel® PROset/ Wireless 3945ABG 00:1C:BF:9E:9D:30	Cliente <i>Roaming</i> Verificador
1	Computador portátil HP,R2G,DD160G, P1.8GH,SO Windows XP	Nvidia Nforce 00:1E:68:A6:14:3D	Atheros AR5006ar 00:22:68:A2:22:49	Transmisor <i>Streaming</i> Verificador
1	Computador de escritorio Compaq,R256M,DD80G, P800MH SO Opensuse 10.2	00:10:B5:D6:68:12		Verificador Desempeño Autenticador
1	Access point D-Link DIR-300 (DD-WRT2)	00:1C:F0:3C:75:E1	00:1C:F0:3C:75:E1	Brindar red Inalámbrica (Punto <i>Roaming 1</i>)
1	Access point D-Link DIR-300 (DD-WRT1)	00:1C:F0:3C:6F:71	00:1C:F0:3C:6F:71	Brindar red Inalámbrica (Punto <i>Roaming 2</i>)
1	Switch D-Link	S/N:PL27283011113		Distribución y conexión de APs
1	Billion	00:04:ED:7E:0A:BA		Servidor DHCP
*Memoria RAM=R, disco duro=DD, procesador=P, sistema operativo=SO				

Tabla 2-1 Requisitos básicos *hardware*.

Software:

Nombre	Descripción
Herramientas de evaluación	<i>Software</i> de verificación (Detalle de su elección y uso en el Apéndice A)
VLC (Video Lan)	<i>Software</i> para transmisión <i>streaming</i> (Detalle de su elección y uso en el Apéndice F)
OpenSSL y Freeradius	<i>Software</i> para autenticación (Detalle de su elección y uso en el Apéndice D)
DD-WRT v24 RC4	<i>Software</i> para activación de 802.11i en puntos de acceso (Detalle de su elección y uso en el Apéndice H)
Distribución Windows y Linux	<i>Software</i> base

Tabla 2-2 Requisitos básicos *software*.

2.2.2 Estudio del ambiente propicio para el montaje

La instalación física adoptada para la evaluación de desempeño fue tipo campus con acceso a distribución de red (*switch* D-Link) y todo conectado a través de cable UTP categoría 5E. La topología ESS contiene varios BSS los que no necesariamente deben tener línea de vista dejando muchas posibilidades de ubicación. Para garantizar el servicio de conexión a los clientes móviles se debe mantener la calidad en la señal radiada durante la transición entre los BSSs, por estas razones se generó una lista

presentada en la Tabla 2-3 de los lugares en los que se podría montar las respectivas experimentaciones.

Edificación	Elección
Santo Domingo parque principal	Problemas con las paredes gruesas además de la dificultad de conexión con la distribución de red.
El Carmen parque principal	Problemas con las paredes gruesas además de la dificultad de conexión con la distribución de red.
Artes	Problemas con la distribución de red.
Educación	Problemas para la instalación de los APs.
Electrónica y Civil	Problemas para la instalación de los APs, además de la dificultad de conexión con la distribución de red.
Administración	Problemas con la distribución de red.

Tabla 2-3 Selección de edificación.

Debido a las dificultades expuestas en la Tabla 2-3 se tomó la decisión de ubicarlos en una casa grande tipo oficina con 80 metros de profundidad, 40 metros de frente y 2 pisos de alto, la adaptación de la cobertura a la edificación se realizó configurando las potencias de los equipos inalámbricos a 0 dbm = 1mW, antena de 2.5 dbi y línea de vista entre los puntos de acceso inalámbrico, esto se ajustó a la estructura escogida ya que se realizó un análisis de cobertura para el perfecto funcionamiento del *roaming* entre los BSSs. Las coberturas pueden ser continuas como la Figura 2-2 o discontinuas como la Figura 2-1 dejando dos escenarios posibles en los que un cliente móvil puede desarrollar el proceso de *roaming*.

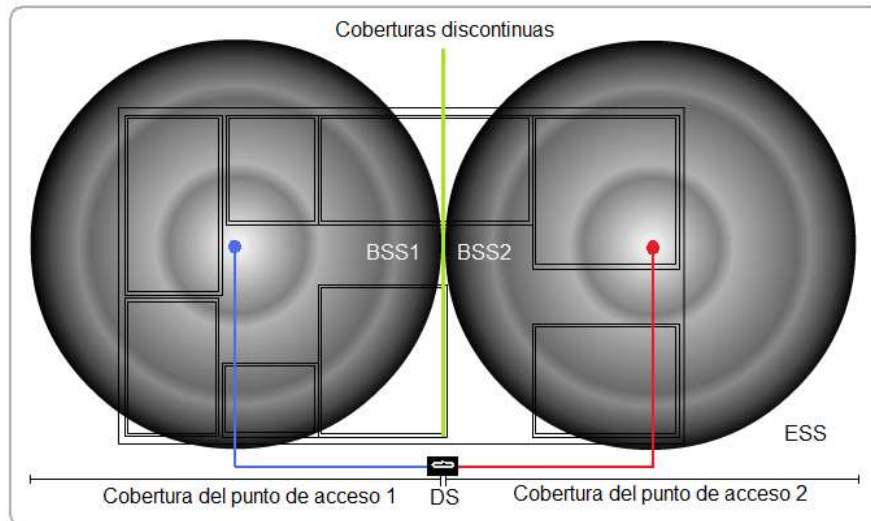


Figura 2-1 Escenario ESS.

La Figura 2-1 presenta un escenario ESS en que las coberturas no se traslapan y por esto no es objeto de la investigación debido a que esta configuración tiene el problema del corte violento de la comunicación en el momento de una transición. Como no existe traslape en las coberturas se forma un espacio en el que no hay cobertura de ningún AP, por lo tanto no es posible tener una la transmisión continua de paquetes, y necesitando un lapso muy grande para retomar la comunicación y las aplicaciones, con lo cual se causan muchos más paquetes perdidos en el cliente móvil debido a la búsqueda, autenticación y

asociación con el nuevo AP. La estructura deseable para un proceso de *roaming* debe contener un traslape para minimizar las pérdidas por transición como se observa en la Figura 2-2.

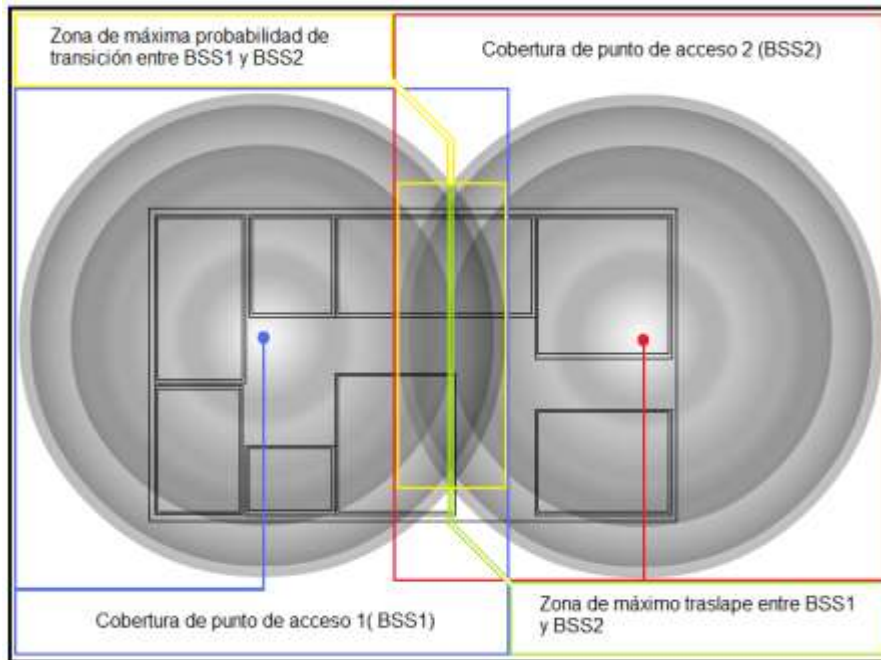


Figura 2-2 Estructura de traslape de los BSSs.

Fue importante crear una referencia para medir la cobertura continua ya que no existe la suficiente información para el diseño de redes inalámbricas en la topología ESS, por esta razón se estudió y estableció una técnica que relaciona el porcentaje de cobertura continua con la distancia de separación entre 2 puntos de acceso. En coberturas continuas donde existen más de 2 BSSs la técnica se aplica en parejas y se promedian los porcentajes obtenidos, es importante tener en cuenta que el porcentaje de cobertura continua que se presenta es un valor aproximado, debido a que los cálculos realizados son puramente experimentales.

El procedimiento de evaluación de cobertura continua inicia estableciendo una regla de porcentajes de 0% a 100%, en este caso el valor de porcentaje más bajo sería cuando no se presenta ningún traslape entre las coberturas de los 2 BSSs y el valor más alto sería cuando los dos puntos de acceso inalámbrico están en la misma ubicación espacial. No se recomienda valores de cobertura continua demasiados altos por las interferencias ni valores demasiado bajos por los cortes rápidos en la transferencia de paquetes. Es preciso realizar un análisis previo para el montaje de la topología ESS con las herramientas adecuadas (ver Apéndice A), dado que las coberturas deben contener el traslape necesario para que las aplicaciones ejecutadas no sufran mucho impacto. Debido a que se adecuó la potencia de los puntos de acceso a la edificación entonces el porcentaje de traslape tiene una correspondencia con la distancia de separación en cuanto a localización espacial, el ajuste de las potencias modificó la distancia de cobertura de unos 75 metros a 18 metros de radio, esto quiere decir que en la Figura 2-3 los equipos inalámbricos están ubicados a 36 metros el uno del otro lo cual corresponde al 0 % de cobertura continua.

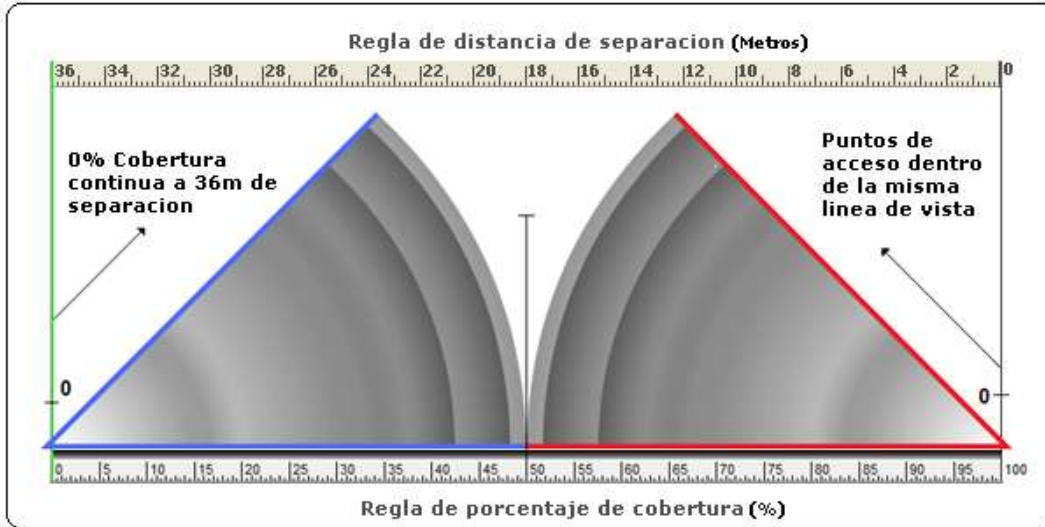


Figura 2-3 Estructura con 0% de cobertura continua.

La intención de un administrador de red es cubrir la mayor área de servicio para los clientes brindando siempre la mayor disponibilidad; el problema es encontrar la distancia de separación o ubicación de los puntos de acceso que mantenga excelentes resultados. El método propuesto consiste en seleccionar primero el porcentaje de cobertura continua deseado, se sugiere 25% para bandas de transmisión 802.11b/g. La siguiente tarea es la cobertura máxima de cada BSS y configurar todos los puntos de acceso con la misma distancia, con la información adquirida se crea la regla de distancia de separación y se sitúa en la parte superior como en la Figura 2-3.

El procedimiento a seguir es desplazar uno de los puntos de acceso de ubicación 0 metros manteniendo la línea de vista y desplazarlo para así encontrar los porcentajes de traslape deseados, es de resaltar que la ubicación vertical de los APs es la misma en las Figuras de traslape. La Figura 2-4 presenta un traslape de 5% de la señal entre los dos BSS correspondiente a una corrección en distancia adelantada de 34.2 metros en línea de vista.

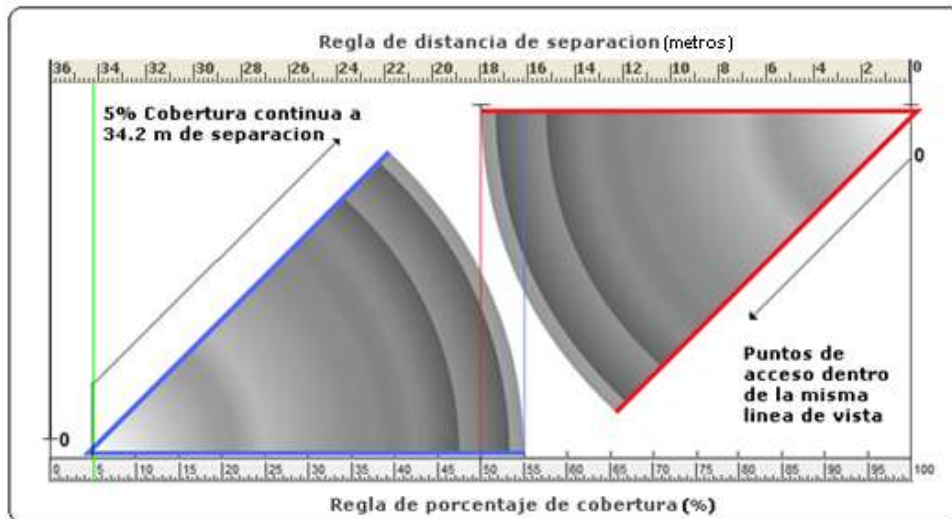


Figura 2-4 Estructura con 5% de cobertura continua.

En la Figura 2-5 se observa una configuración con un traslape del 50%, con este porcentaje se cubre gran parte del mismo espacio con los 2 BSS desperdiciando la posibilidad de tener mayor cobertura por cada AP. Utilizar en diseños de red inalámbrica porcentajes de cobertura continua mayores de 50% no es muy útil porque se desperdicia el área de cobertura, además de tener problemas de interferencia debido a la potencia y la proximidad entre los puntos de acceso.

Coberturas continuas con porcentajes altos no se utilizan para el diseño de redes inalámbricas en topologías ESS, pero para las experimentaciones es necesario verificar la topología ESS con funcionalidad en *roaming* a diferentes intervalos de cobertura iniciando en 0% y terminando en 80%, dado que de 80% a 100% no tiene sentido el estudio por la proximidad correspondiente a 7 metros introduciendo ruido de un punto de acceso a otro. En la Figura 2-6 se enseña otro ejemplo de uso de la técnica de relación de cobertura continua. Recordar que la distancia de separación es horizontal no vertical.

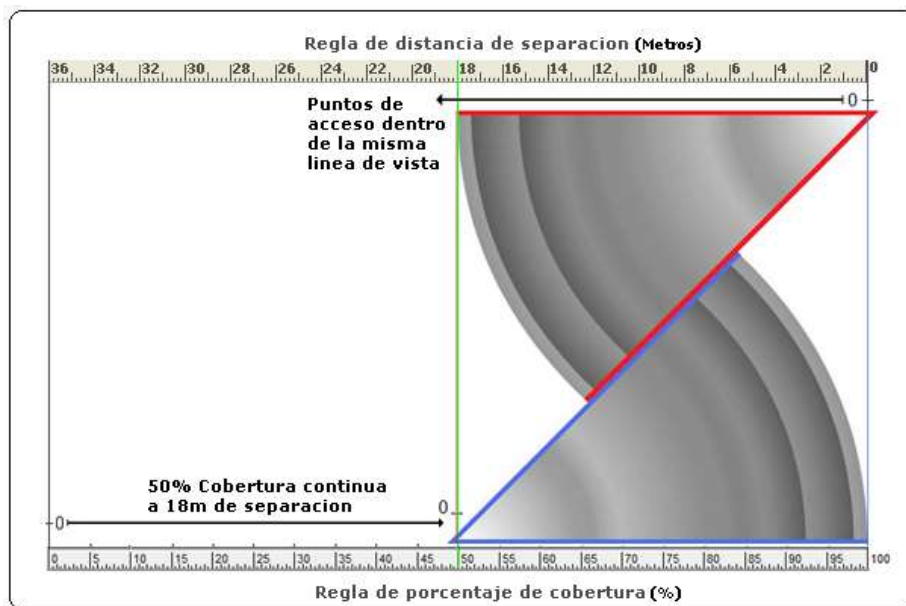


Figura 2-5 Estructura con 50% de cobertura continua.

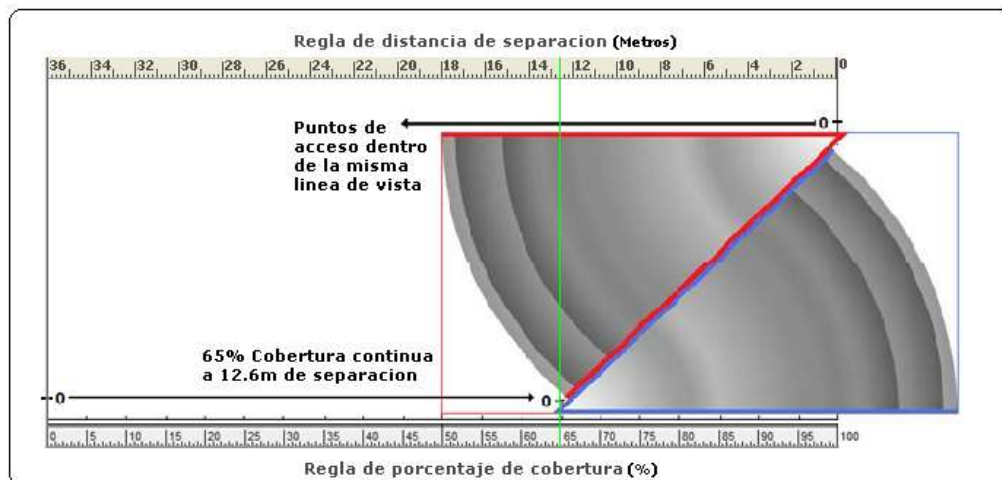


Figura 2-6 Estructura con 65% de cobertura continua.

El estudio de comprobación de coberturas se realizó con dos perspectivas, dirigido al perfecto funcionamiento del *roaming* verificando la pérdida de paquetes y segundo al perfecto funcionamiento del *roaming* verificando el retardo entre los puntos de acceso. El estándar 802.11g se ratificó en junio de 2003 siendo la evolución del estándar 802.11b, éste utiliza la banda de 2.4 GH (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbps. Actualmente se venden equipos con esta especificación y potencias de hasta 500 mw, lo que permite hacer comunicaciones de hasta 50 km con antenas apropiadas. En la práctica se logran la velocidades de transferencia en TCP/IP desde 3 Mbps hasta 6 Mbps (ver Apéndice C).

Luego de realizar un estudio de movilidad en la banda de transmisión 802.11g comparado con las muestras de un cliente estático en la banda de transmisión 802.11g como se enseña en la Figura 2-7 se deduce que la velocidad en la que mejor se aprovecha el ancho de banda y mayor estabilidad se percibe es cuando el cliente se mueve a una velocidad de 1m cada 8s¹³, el desplazamiento a 1m/8s es el de mejor valor de RSSI¹⁴ para 802.11g como se observa en la Figura 2-8. En el Apéndice B se presentan las tablas del estudio de movilidad para 802.11g usando las herramientas de evaluación descritas en el Apéndice A.

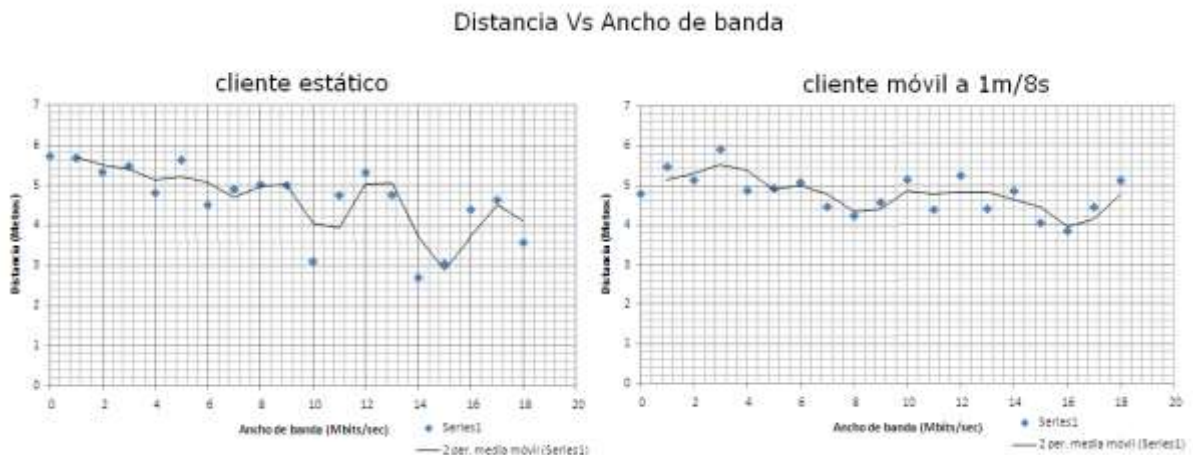


Figura 2-7 Comparación de ancho de banda en 802.11g.

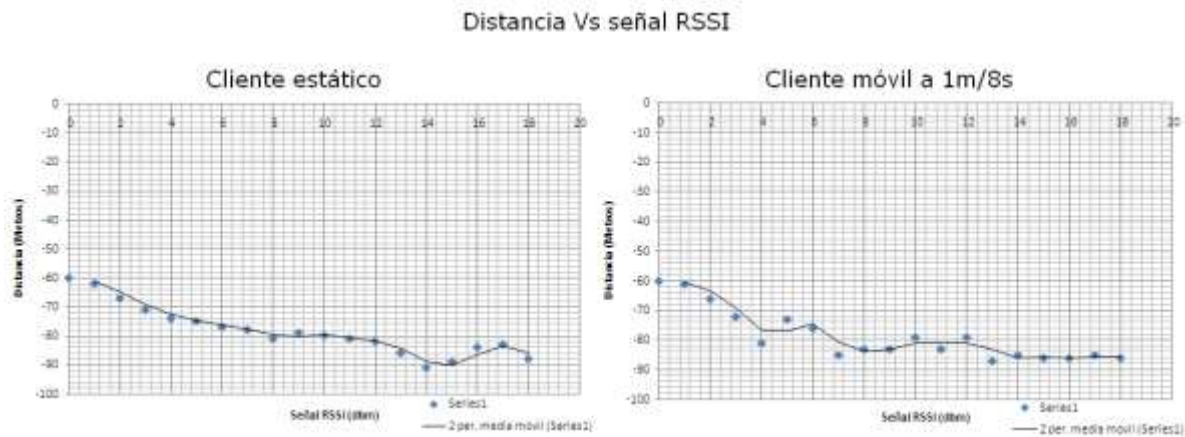


Figura 2-8 Comparación de señal RSSI en 802.11g.

¹³ La velocidad de 1m/8s es recorrer la distancia de 1 metro durante 8 segundos correspondiente a 12,5 cm/s.

¹⁴ Recordar de la sección 1.5 que éste es el valor de la intensidad de la señal recibida.

El estándar 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión sobre TCP/IP con este estándar es de aproximadamente 4 Mbps (ver Apéndice C).

Aunque también utiliza una técnica de espectro ensanchado basada en DSSS, en realidad la extensión 802.11b introduce la modulación de código complementario (CCK, *Complementary Code Keying*) para poder alcanzar la velocidad teórica de 11Mbps. El estándar también admite el uso de la codificación convolucional binaria de paquetes (PBCC, *Packet Binary Convolutional Coding*) como opcional.

Las Figuras 2-9 y 2-10 enseñan que una velocidad de 1m/8s presenta estabilidad en señal RSSI y ancho de banda para la banda de transmisión 802.11b, aunque a otras velocidades se dan valores altos de ancho de banda no son constantes, creando saltos que pueden causar problemas en aplicaciones que estén utilizando el canal de conexión inalámbrica. En el Apéndice B se presentan las tablas del estudio de movilidad para 802.11b usando las herramientas de evaluación del Apéndice A.

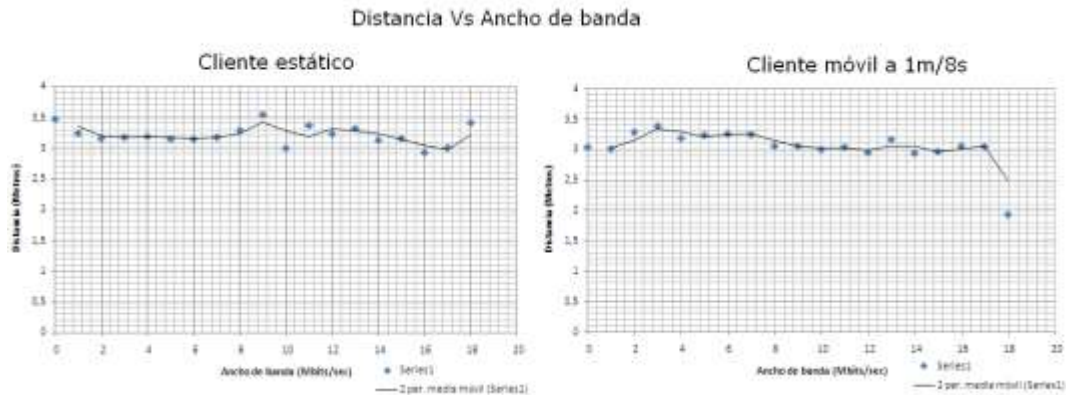


Figura 2-9 Comparación de ancho de banda en 802.11b.

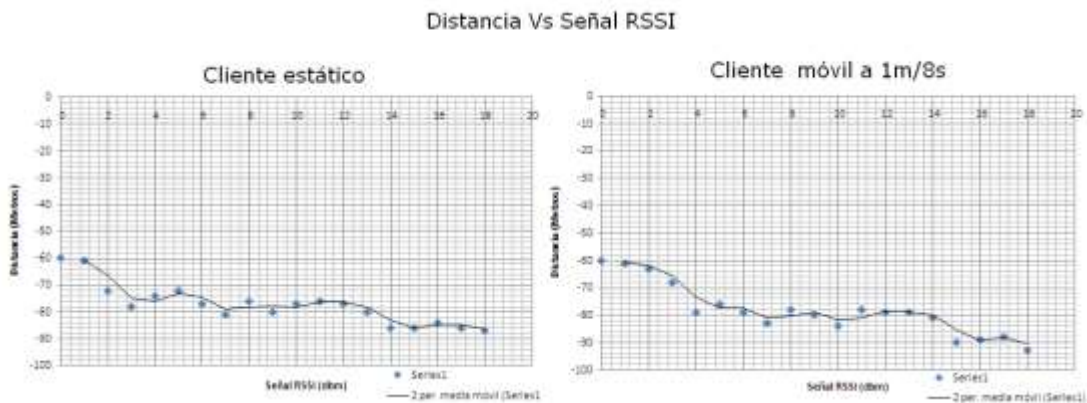


Figura 2-10 Comparación de señal RSSI en 802.11b.

Los datos del Apéndice C muestran los valores de calidad de movilidad y calidad de *roaming* que se obtuvieron utilizando las herramientas del Apéndice A trabajando en los estándares 802.11b y 802.11g. Dependiendo del promedio de traslape continuo de las coberturas, la distancia entre puntos de acceso y la intensidad de la movilidad se encuentra un valor que indica el nivel de calidad que se ha obtenido relacionado directamente con el ancho de banda, retardo, pérdida de paquetes en *roaming* y porcentaje de pérdida de paquetes en el caso de calidad de movilidad.

Debido a que no existe una fórmula que evalúe el desempeño del *roaming* ni de la movilidad en redes 802.11b y 802.11g, se tuvo en cuenta los factores críticos como el retardo de los paquetes en el momento de la transición, este se causa cuando un cliente se está alejando del AP y aumentando el tiempo de respuesta o retardo de los paquetes. Es preferible el aumento del retardo en los paquetes causado por las variaciones del ancho de banda que la pérdida de paquetes debido a que no se pudo mantener la comunicación. El ancho de banda y la potencia recibida también son factores críticos para definir el desempeño de la movilidad y el *roaming*, estos valores disminuyen cada vez que el cliente se aleja del AP ocasionando la ejecución del algoritmo de elección de un nuevo AP con mejor señal. La pérdida de paquetes constante señala la desconexión cuando se cambia de AP; la calidad de *roaming* y el porcentaje total de pérdida de paquetes ayuda a seleccionar si la transmisión es tolerante a la movilidad cuando se está ejecutando aplicaciones en el momento del *roaming*. Reuniendo estos factores influyentes se sugiere una fórmula empírica que contiene la información esencial y brinda una referencia para valorar la movilidad y el *roaming*, a continuación se muestra una fórmula que relaciona los elementos necesarios para evaluar el desempeño de la movilidad y *roaming*, el uso de esta referencia permitió seleccionar los valores más representativos para la investigación.

$QM = BW - PP - (1/R)$ y $QR = BW - PPR - (1/R)$, donde: QM= calidad de movilidad, QR= calidad de *roaming*, BW= ancho de banda, PP= porcentaje de pérdida de paquetes, PPR= pérdida de paquetes en *roaming* y R= retardo.

La intensidad de movilidad o agresividad de movilidad, la cual se configura en el cliente inalámbrico, es algo indispensable que permite realizar el proceso de *roaming* en el mejor momento posible para no experimentar demasiada pérdida de paquetes. Cuando su configuración esta en mínimo el cliente inalámbrico no realiza el *roaming* hasta que haya una degradación considerable en la potencia recibida del AP actual. En configuración media se experimenta un equilibrio entre la necesidad de hacer *roaming* y el desempeño inalámbrico, es decir es un punto medio para la toma de decisión de hacer *roaming*. Y en máximo el cliente inalámbrico observa continuamente la calidad del vínculo, si se presenta una degradación mínima se ejecuta el algoritmo de selección y se realiza la transición al nuevo AP.

En la Tabla 2-4 se consignan los resultados promedios de todo el estudio de *roaming* para 802.11b concentrado en el Apéndice C. En 802.11b se tienen valores cercanos en calidad de movilidad entre la configuración máxima y mínima, pero definitivamente es mejor la opción en máximo brindando más seguridad en el momento de moverse por las diferentes coberturas continuas. Si se observa la parte de distancia efectiva de *roaming* con la opción en mínimo se observa que se alcanza a mover dentro de la cobertura del segundo AP hasta 6,8 metros promedio, mientras que con la opción en máximo se recorre hasta 2,4 metros promedio, de esta manera provechando mejor la cobertura del segundo punto de acceso y permitiendo la renovación rápida de los paquetes sin problemas de degradación de la señal. La opción de intensidad de movilidad en un valor medio reduce la pérdida de paquetes durante el *roaming* resultando una calidad de *roaming* superior que con las opciones en mínimo y máximo, si se confrontan las dos calidades se puede ver que una intensidad de movilidad en mínimo resultaría en equilibrio entre movilidad y *roaming*.

Estándar 802.11b.			
Parámetro estudiado	Intensidad de la movilidad		
	Mínima	Media	Máxima
Promedio del porcentaje de paquetes perdidos (%)	0,823529	1	0,823529
Promedio de paquetes perdidos en <i>roaming</i>	0,411764	0,294117	0,470588
Promedio de retardo (ms)	45,23529	47	45,64705
Promedio de ancho de banda (Mbps)	2,678235	2,68	2,696470
Promedio de señal RSSI (dbm) WRT2	-88,1176	-83,9411	-80,0588
Promedio de señal RSSI (dbm) WRT1	-74,9411	-72,2941	-70,4117
Promedio distancia efectiva de <i>roaming</i> (metros)	6,879411	5,849411	2,427647
Promedio de calidad de movilidad	1,832239	1,657800	1,849991
Promedio de calidad de <i>roaming</i>	2,244004	2,363683	2,202928

Tabla 2-4 Promedios del estudio de *roaming* en 802.11b.

En la Tabla 2-5 se consignan los resultados promedios de todo el estudio de *roaming* para 802.11g concentrado en el Apéndice C. Para 802.11g se tiene una calidad de movilidad alta en la opción de intensidad de movilidad configurada en mínimo, en este estándar se tienen anchos de banda más altos por lo cual se envían muchos más paquetes y en caso de un corte en la conexión debido a la movilidad será mayor el porcentaje de paquetes perdidos. La mejor opción para este estándar es en mínimo pues se tiene mayor ancho de banda, menor retardo y los paquetes perdidos son bajos debido a que se mantiene la asociación hasta sentir una degradación de importancia en la potencia recibida.

Estándar de 802.11g.			
Parámetro estudiado	Intensidad de la movilidad		
	Mínima	Media	Máxima
Promedio del porcentaje de paquetes perdidos (%)	1,470588	1,647058	1,764705
Promedio de paquetes perdidos en <i>roaming</i>	0,529411	0,411764	0,882352
Promedio de retardo (ms)	65,411764	81,470588	93,882352
Promedio de ancho de banda (Mbps)	4,430588	4,285882	3,938823
Promedio de señal RSSI (dbm) WRT2	-89,705882	-90	-90,352941
Promedio de señal RSSI (dbm) WRT1	-79,882352	-77,058823	-76
Promedio distancia efectiva de <i>roaming</i> (metros)	7,441764	8,495882	9,954117
Promedio de calidad de movilidad	2,940066	2,623494	2,161459
Promedio de calidad de <i>roaming</i>	3,881242	3,858788	3,043812

Tabla 2-5 Promedios del estudio de *roaming* en 802.11g.

La Figura 2-11 muestra el nivel de la señal RSSI obtenida para cada cobertura con diferente intensidad de movilidad. Para el estándar 802.11g el primer AP con el nombre de DD-WRT2 inicia la movilidad con línea de vista directa hacia el otro AP con el nombre de DD-WRT1, la decisión de *roaming* se toma en una potencia de -85 dbm como AP disponible y -95 dbm como AP conectado.

El segundo AP con el nombre de DD-WRT1 termina el proceso de *roaming* presentando valores superiores a -90 dbm que corresponde a la nueva señal que toma el cliente móvil después de realizado el proceso de decisión de cambio de AP, además de observar que la intensidad de movilidad no funciona como debería ser, pues cuando las coberturas continuas son mayores a 50% los valores de DD-WRT2 se mantienen constantes, mientras que si se compara con la gráfica del estándar 802.11b se aprecia que al aumentar el traslape entre las coberturas también aumenta el valor de señal RSSI en el momento de *roaming*. El proceso de *roaming* es descrito perfectamente por la gráfica de 802.11b debido a que los movimientos generados por DD-WRT2 y DD-WRT1 son muy parecidos o muy cercanos al aumento del traslape de cobertura.

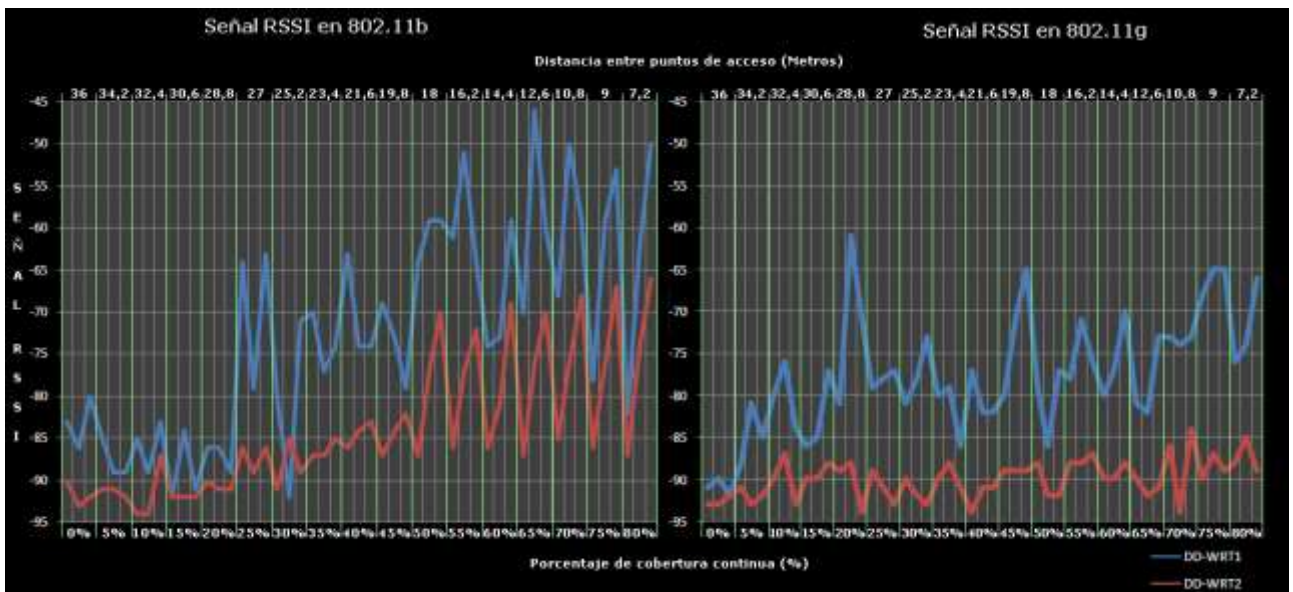


Figura 2-11 Comparación de Señal RSSI.

El estándar 802.11b presenta mayor estabilidad cuando hay movilidad debido a que tiene porcentajes de pérdida de paquetes más bajos que el estándar 802.11g. En la Figura 2-12 se observan las coberturas con menos pérdidas para 802.11b. Por ejemplo, el traslape de cobertura continua de 60% presenta 0% de pérdida de paquetes y para 802.11g se tiene que el mejor traslape de cobertura continua es la de 60% y 75% con un promedio de 1% de pérdidas. Se puede observar también que para los dos estándares, tanto 802.11b como 802.11g, hay 3 grupos de concentración de pérdidas divididos por 25% y 60% de traslape de cobertura continua.

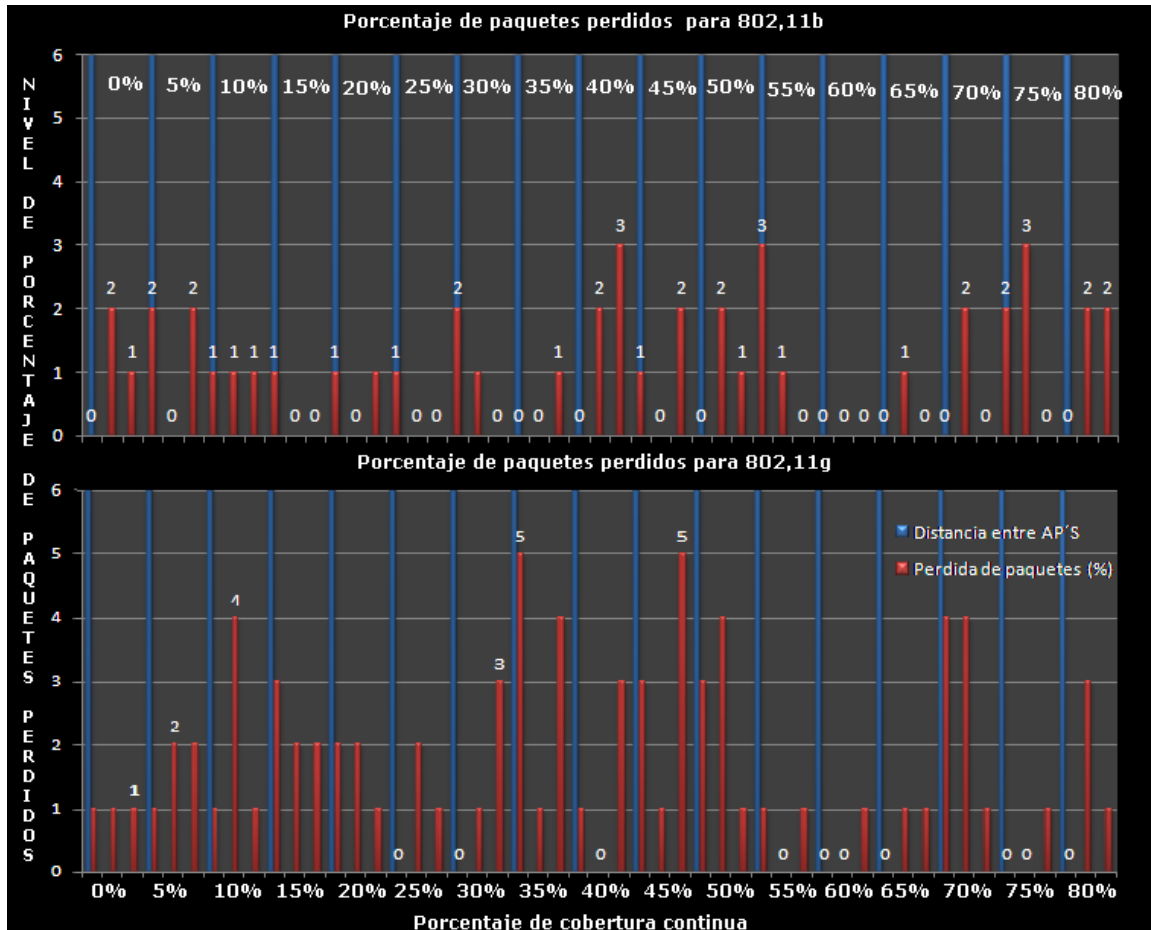


Figura 2-12 Comparación de porcentaje de paquetes perdidos.

El retardo es un factor importante para el proceso de *roaming*. Si se analiza la Figura 2-13 y los retardos producidos se logra percibir que en bajos porcentajes de cobertura continua el retardo es mayor, de esta forma para 802.11g empieza a lograr valores bajos de retardo después del 25% mientras que para 802.11b se perciben valores bajos desde el 15% brindando mejores resultados al aumentar el traslape de la cobertura. Cuando un cliente se aleja del AP en el cual está asociado el retardo aumenta gradualmente. Sin embargo, el retardo es más tolerable que la pérdida de paquetes durante el *roaming*.

El diseño de un ESS debe mantener el equilibrio entre el retardo, el porcentaje de pérdida de paquetes y la cobertura continua, la Figura 2-14 demuestra que cuando se supera el 50% de cobertura continua se comienza a percibir el aumento de la distancia entre los dos puntos de acceso en el momento del *roaming*. No es recomendable configuraciones en donde se sobrepasa el 50% de cobertura continua, debido a que si existen otros APs la tarjeta de red inalámbrica ejecutará el algoritmo de *roaming* resultando en inseguridad por encontrarse entre una señal baja RSSI transmitida por el segundo AP y una nueva señal RSSI transmitida por un tercer AP.

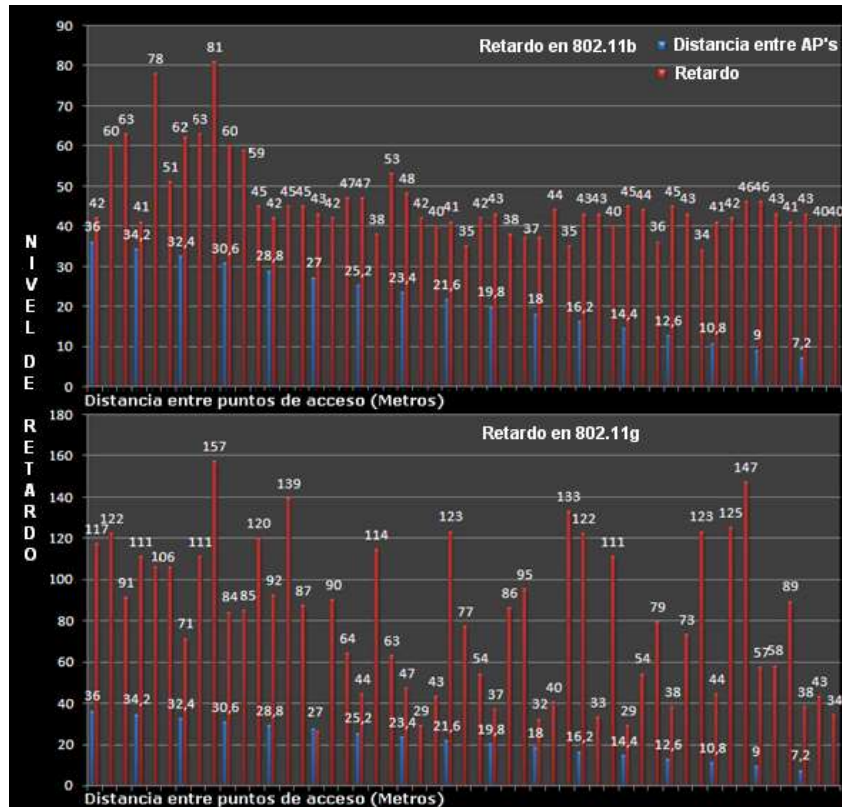


Figura 2-13 Comparación de retardo.

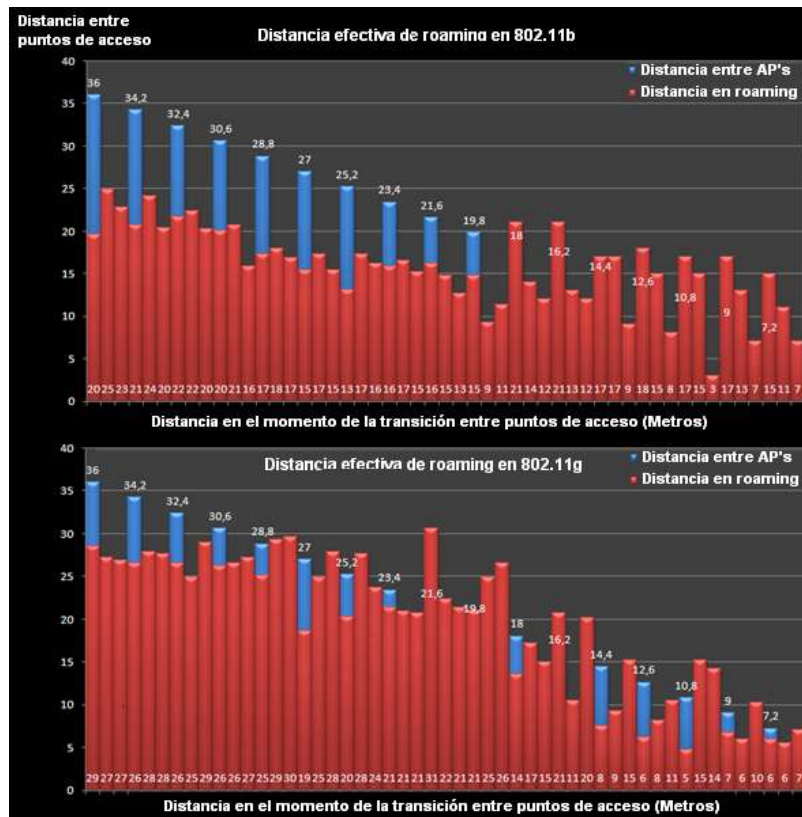


Figura 2-14 Distancia efectiva de roaming en 802.11b/g.

El porcentaje de cobertura continua con mayor desempeño depende de los valores de calidad de movilidad y calidad de *roaming* más altos registrados en la Figura 2-15 y concentrados en el Apéndice C. Cuando las variables críticas son mínimas o nulas el valor de calidad de movilidad es el mismo que la calidad de *roaming* siendo necesario evaluar solo la calidad de movilidad. El estudio muestra que para 802.11g el valor registrado de 5,84 de calidad de movilidad con distancia entre puntos de acceso de 16,2 metros que corresponde a 55% de traslape de cobertura continua con intensidad de movilidad media, aunque también se tiene un segundo valor de calidad de *roaming* de 5,15 con distancia entre puntos de acceso de 27 metros que corresponde a 25% de traslape de cobertura continua con intensidad de movilidad mínima.

En la banda de transmisión de 802.11b se logra el valor más alto de calidad de movilidad a una distancia de 27 metros correspondiente a 25% de traslape de cobertura continua con intensidad de movilidad media. Los valores más altos de calidad de *roaming* se han encontrado con la configuración de intensidad de movilidad en medio. Para un diseño en topología ESS con el funcionamiento de *roaming* se tienen valores claves encontrados con anterioridad pero para el desarrollo de las siguientes actividades o experimentaciones se trabajó con 25% de cobertura continua para los dos estándares b y g, y se ubicarán los dos APs a una distancia de 27 metros de separación de forma permanente para mantener un equilibrio en los datos.

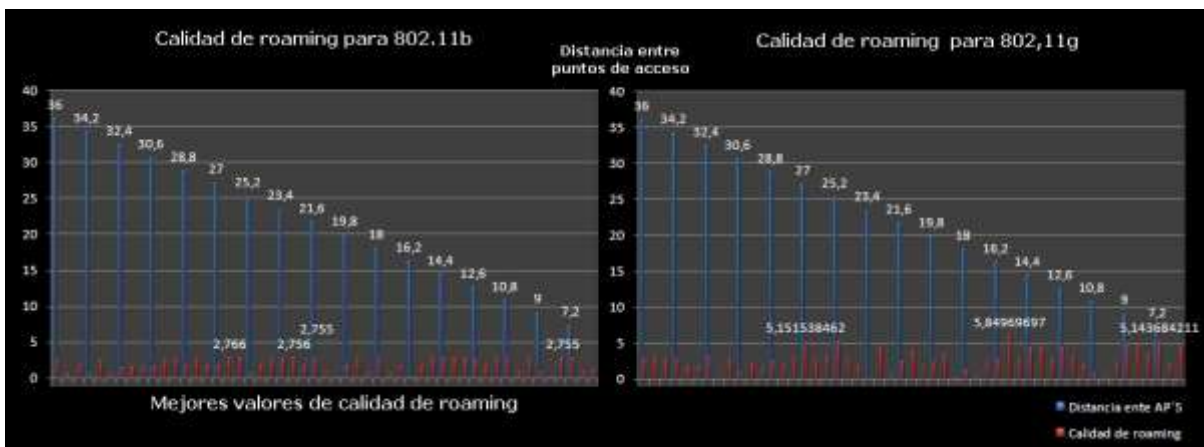


Figura 2-15 Comparación de calidad de movilidad.

Si se analizan las bandas de transmisión de 802.11b/g se encuentra que entre más ancho de banda se tenga menor retardo se producirá y por consiguiente menos pérdida de paquetes. El retardo está ligado a la pérdida de paquetes, pues, en el proceso de *roaming* el ancho de banda y el retardo son los valores determinantes para que el porcentaje de pérdida de paquetes aumente o se mantenga por debajo del mínimo.

2.3 MONTAJE Y COMPROBACIÓN DEL ROAMING PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS SIN SEGURIDAD NI STREAMING

2.3.1 Montaje y verificación de la topología ESS

Básicamente un ESS está compuesto por un sistema de distribución y varios BSSs. Al tener estos dos componentes unidos se está hablando de un nuevo tipo de red o topología la cual es un conjunto de servicio extendido. Al unir varios BSSs lo que se logra fundamentalmente es aumentar la cobertura de una red IEEE 802.11 como se observa en la Figura 2-16.

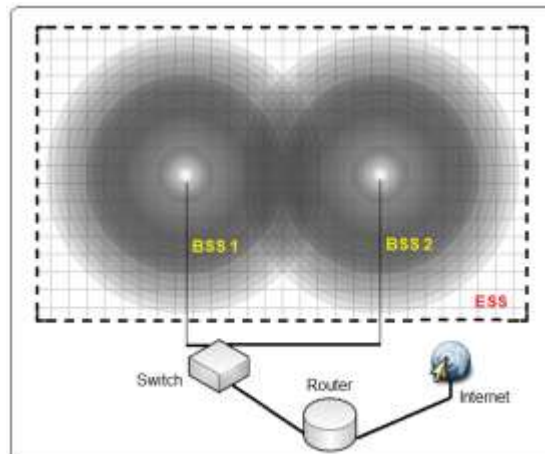


Figura 2-16 Estructura de servicio Extendido ESS.

La estructura ESS se construye con un grupo de BSSs ubicados según el análisis de coberturas y potencias el cual demostró que debe haber un traslape de 25% de la coberturas continuas para tener los mejores resultados, la ubicación espacial de estos APs se hizo pensando en el mejor desempeño que se pudo alcanzar con los estudios previos, para esto se logró un equilibrio entre potencias y posición espacial teniendo siempre una línea de vista entre los equipos. Para el correcto funcionamiento de la topología fue necesaria una actualización de firmware en los APs (ver Apéndice H).

2.3.1.1 Estructura física BSS

Los puntos de acceso D-Link están situados según los resultados obtenidos en el Apéndice C, la conexión entre los equipos inalámbricos se hizo con UTP categoría 5E cruzado conectado al sistema de distribución entre puertos LAN que en este caso es un *switch* D-Link de 8 puertos. En las prácticas no se debe tener en cuenta el puerto WAN del AP. Esta estructura se utilizará durante toda las experimentaciones.

2.3.1.2 Estructura lógica: Direccionamiento

La estructura de servicio inalámbrico ESS estará lista después de configurar el direccionamiento de los equipos de red, la Tabla 2-6 fue usada como guía para evitar problemas de direcciones IP duplicadas o conflictos de enrutamiento.

Nombre	Descripción	Cobertura	Interfaz Wi-Fi o Ethernet (Mac)	Dirección IP
DD-WRT1 (AP1)	Access point D-Link DIR-300	BSS1	00:1C:F0:3C:6F:71	192.168.1.1
DD-WRT2 (AP2)	Access point D-Link DIR-300	BSS2	00:1C:F0:3C:75:E1	192.168.1.2
Streaming VLC	Servidor de <i>streaming</i>		00:1E:68:A6:14:3D	192.168.1.3
RADIUS	Servidor RADIUS		00:10:B5:D6:68:12	192.168.1.4
Switch D-Link (DS)	<i>Switch</i> D-Link	----	S/N:PL27283011113	
Billion (DHCP)	<i>Router</i> Billion	----	00:04:ED:7E:0A:BA	192.168.1.254

Tabla 2-6 Configuración del direccionamiento.

La verificación se hizo con las herramientas del Apéndice A. La primera parte consiste en

asociarse a cada AP y esperar que el servidor DHCP brinde direcciones válidas. La segunda parte es constatar la conectividad de toda la red, para esto se utilizó la herramienta ping con cada cliente y AP enviando tramas y verificando que se obtuviera una respuesta positiva de recepción en el lado contrario.

2.3.1.3 Montaje BSS

Los APs deben tener un 25% de cobertura continua ubicándose con 27 metros de separación horizontal. Lo primero que se hizo fue ubicar el AP1 que corresponde a BSS1 o DD-WRT1 y contar 27 metros con línea de vista directa y ubicar el segundo AP o BSS2 exactamente a los 27 metros a una altura de 1,5 metros medida desde el piso para los dos puntos de acceso. Los equipos se conectaron físicamente con un cable UTP categoría 5E hasta un *switch* D-Link de 8 puertos que está en la mitad de los 27 metros, a este *switch* está conectado un equipo de escritorio el cual hará funciones de servidor de autenticación y verificación de conectividad.

2.3.2 Configuración y verificación de cobertura con el funcionamiento de roaming en la topología ESS

Para comprobar el perfecto funcionamiento de *roaming* se utilizaron las herramientas del Apéndice A, si un cliente móvil se desplaza de un AP a otro en el momento del *roaming* se detecta un evento de transición con las herramientas llamadas: Intel PROSet/Wireless (estadísticas avanzadas), Intel PROSet/Wireless (visor de sucesos). De esta forma se comprueba que hubo un cambio de AP realizado por un algoritmo de *roaming* simple, pero en esta ocasión se comprobó el funcionamiento de *roaming* evaluando el procedimiento en las estructuras básicas del ESS. Para estas pruebas se usó la misma estructura de la sección 2.3.1.

2.3.2.1 Estructura física cliente móvil

Hace referencia a la perfecta instalación, configuración y verificación de la tarjeta de red inalámbrica; para comprobar este correcto funcionamiento se debe ingresar al administrador de dispositivos y buscar si se encuentra el dispositivo con su respectivo sistema controlador y sin ningún tipo de problema.

2.3.2.2 Estructura lógica del usuario móvil:

Se parte del escenario de ubicación del primer AP porque este es el primer nodo de cubrimiento móvil de los siguientes BSSs, en este momento la red se encuentra sin seguridad para realizar la prueba de *roaming* satisfactoria y encontrar rápidamente algún problema. El proceso lógico de conexión inalámbrica normalmente se lleva a cabo de la siguiente manera:

- 1) Se activa el dispositivo inalámbrico del cliente móvil.
- 2) El dispositivo detecta el SSID radiado por el AP1 llamado "ServerA", en este caso con una longitud de 7 letras entre mayúsculas y minúsculas.
- 3) Se agrega la red inalámbrica dentro del perfil del usuario inalámbrico.
- 4) El AP1 asigna la información necesaria para ser cliente permanente.

Las propiedades avanzadas de los dispositivos inalámbricos cambian según el fabricante. Aunque la mayoría contienen valores especiales que se deben estudiar, como la opción de intensidad de movilidad o agresividad de la itinerancia que varía su nombre de acuerdo a la tarjeta o adaptador inalámbrico, Observar ejemplo en la Figura 2-17. La conclusión del estudio de *roaming* hallado en el Apéndice C sugiere una agresividad de itinerancia en medio para 802.11b y una agresividad de itinerancia en mínimo para 802.11g.

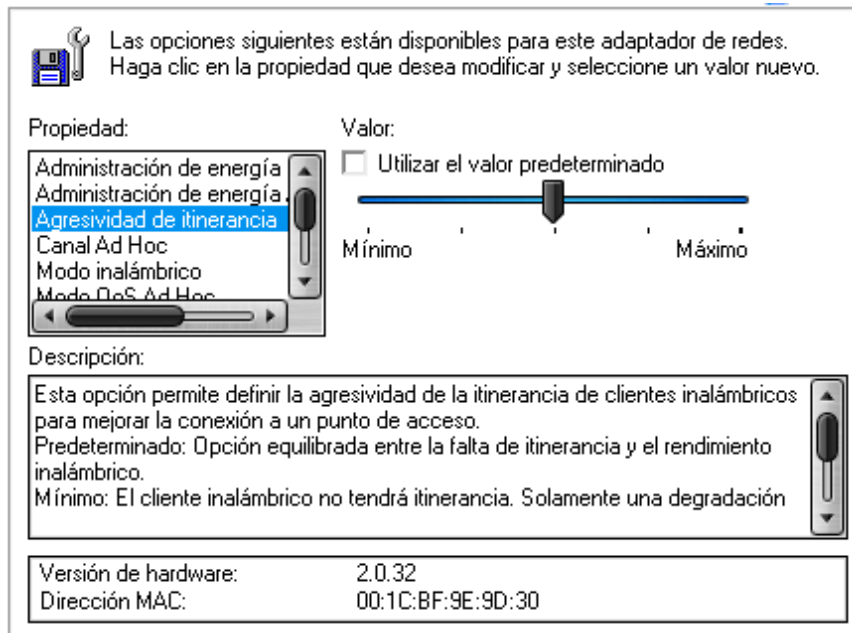


Figura 2-17 Configuración de la intensidad de movilidad.

2.3.2.3 Estructura lógica de la topología ESS

La topología ESS de experimentación contiene tan solo 2 BSS pero podrían ser varios ampliando la cobertura; hay valores que se deben configurar por igual en todos los AP cómo: SSID, seguridad, canales de transmisión, dirección del servidor DHCP, potencia de transmisión, la opción de emisión de SSID habilitada y ocultar red desactivada; pero hay datos que deben ser diferentes para que no existan conflictos como dirección IP y nombre del AP.

2.3.2.4 SSID

Esta valor debe ser igual para reducir el tiempo de asociación en el momento del cambio de AP, por eso se ha escogido un valor de siete letras el cual es "ServerA".

2.3.2.5 Configuración del Servidor DHCP

Esta característica tiene dos opciones, DHCP *server* y DHCP *forward*. El inconveniente aparece cuando hay varios AP con la opción de DHCP *server* con varios clientes móviles, pues se presentan conflictos en repetidas ocasiones debido a la duplicación de direcciones IP en el momento del *roaming* entre los puntos de acceso. Si se piensa utilizar esta elección lo mejor es establecer los rangos de direcciones IP de cada DHCP diferentes para que así exista una diferencia en el momento de cambio. La asignación de una nueva dirección IP introducirá más retardo para completar el *roaming*. La mejor

opción es utilizar un DHCP *forward* para de esta manera evitar los conflictos con direcciones IP duplicadas además de quitar carga de procesamiento a los APs, dejando esto a un servidor DHCP centralizado.

2.3.2.6 Potencia de transmisión

Para que exista un equilibrio en las coberturas de los BSS es mejor que todos tengan el mismo valor de potencia, en este caso los dos BSS están ajustados a 0dbm = 1mW generando una cobertura de 18 metros de radio.

2.3.2.7 Ganancia de la antena

Lo mejor es que los equipos tengan las características más parecidas en cuanto a potencia y ganancia de las antenas. En la experimentación se utilizó una antena de tipo omnidireccional y con una ganancia de antena de 2.5 dbi,

2.3.2.8 Configuración de seguridad

Para mantener la transparencia del *roaming*, reducir el tiempo e interrupciones durante el *roaming*, la configuración de seguridad es la misma para todos los puntos de acceso.

2.3.2.9 Modo de la red inalámbrica

Es importante que el modo sea igual en los APs para mantener el ancho de banda, la velocidad de transmisión y la continuidad de la información enviada a través del canal inalámbrico.

2.3.2.10 Dirección IP del AP

Este valor tiene que ser diferente en cada AP de la topología ESS ya que puede crear conflictos de direccionamiento, es indispensable dejar un bloque de direcciones libres para asignar si se tiene pensado aumentar el número de APs dentro de la topología ESS.

2.3.2.11 Nombre del AP

Debe ser diferente en cada AP para no crear conflictos con el enrutamiento.

La verificación de la topología ESS con funcionalidad de *roaming* se realizó para los dos estándares 802.11g y 802.11b utilizando las herramientas de verificación del Apéndice A. La Figura 2-18 y la Figura 2-19 demuestran el momento exacto en que se efectúa el *roaming* y se registra en el visor de sucesos el evento de itinerancia, además de los valores RSSI en el instante en que se realizó el cambio de AP otros datos importantes se pueden visualizar los cuales ayudan a encontrar resultados y generar conclusiones .

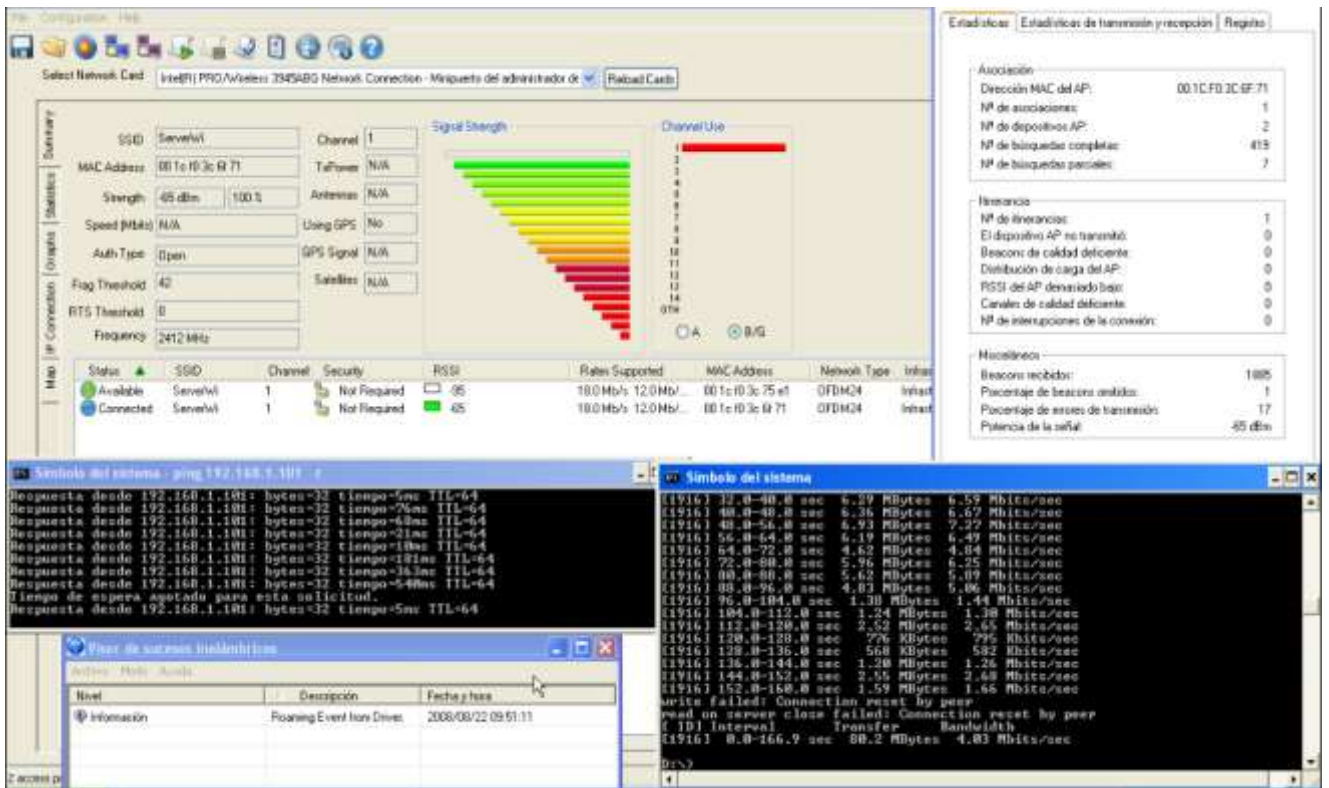


Figura 2-18 Verificación de *roaming* en 802.11g.

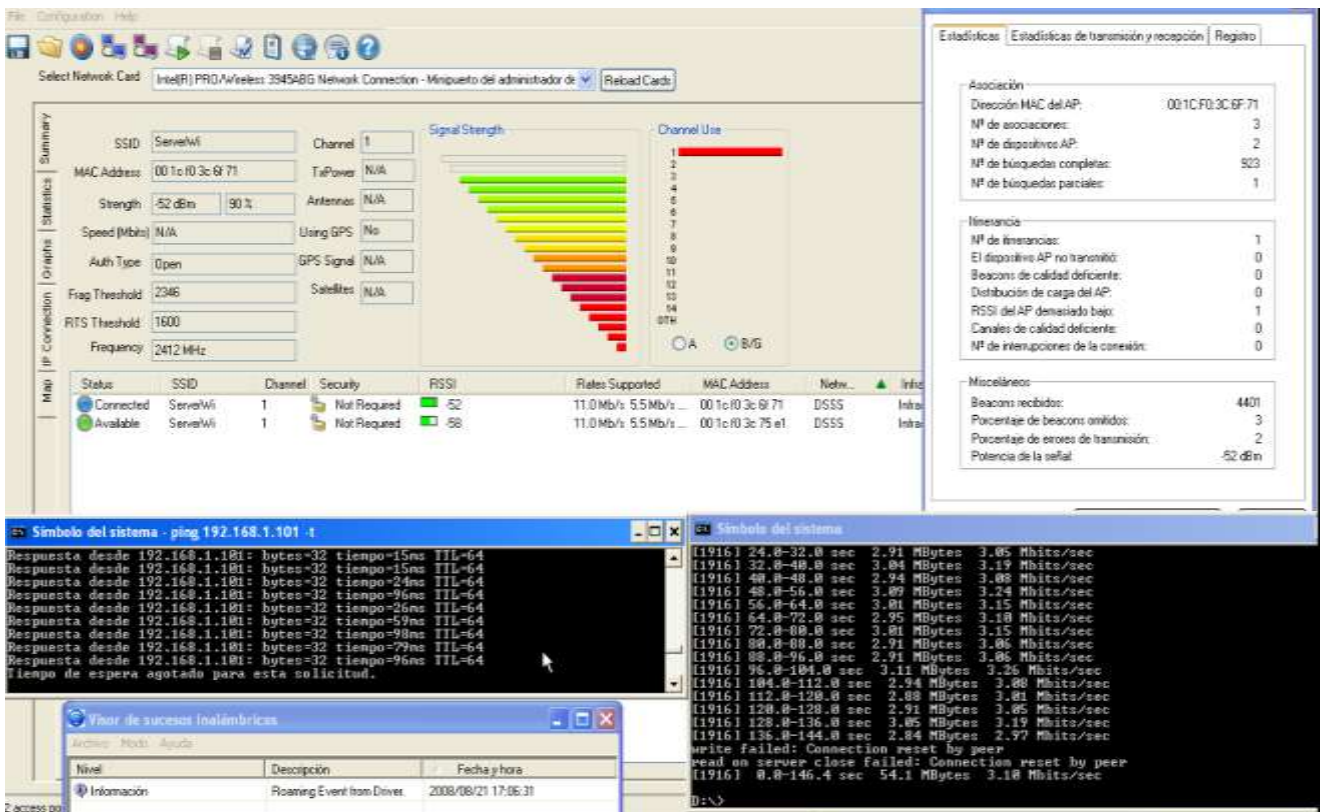


Figura 2-19 Verificación de *roaming* en 802.11b.

2.3.3 Búsqueda de variables críticas en el desempeño del *roaming*

Analizadas las gráficas de retardo, ancho de banda y porcentaje de pérdida de paquetes, se puede apreciar que las variables más influyentes en el *roaming* sin tener en cuenta la seguridad ni el *streaming* son, el porcentaje de traslape de cobertura continua, la movilidad en el instante de *roaming* y la intensidad de movilidad. Estas variables son determinantes para generar un proceso de *roaming* transparente. La correcta elección del porcentaje de cobertura continua combinado con la opción de intensidad de movilidad puede arrojar 0% de pérdida de paquetes.

El retardo es generado por el movimiento del cliente móvil entre los APs y las variaciones del ancho de banda. Estas variables se controlan si se toma el mejor porcentaje de traslape de cobertura continua y se configura la opción de intensidad de movilidad que correspondió al mayor valor de calidad de *roaming* (ver Apéndice C)

2.3.4 Análisis de resultados y generación de conclusiones

La información agrupada en los Apéndices B y C, permiten el análisis de los valores de calidad de movilidad y calidad de *roaming* junto con la intensidad de movilidad y porcentaje de cobertura. Los resultados de su estudio se muestran en las Tablas 2-7 y 2-8. En 802.11b los mejores valores de *roaming* son entre el 25% y 40% con más incidencia de la opción de intensidad de movilidad en medio, 40% con la opción en mínimo y 75% con la opción en máximo. En 802.11g los mejores valores de *roaming* se encuentran dispersos en valores de porcentaje de cobertura altos: 55%, 25%, 80% y 30% con una gran incidencia de intensidad de movilidad en mínimo.

Mejores valores de calidad de movilidad y <i>roaming</i> para 802.11b.		
Porcentaje de cobertura continua	Intensidad de movilidad	Calidad de <i>roaming</i>
25%	Medio	2,766190476
35%	Medio	2,756190476
40%	Mínimo	2,755609756
75%	Máximo	2,755609756

Tabla 2-7 Calidad de movilidad y *roaming* en 802.11b.

Mejores valores de calidad de movilidad y <i>roaming</i> para 802.11g.		
Porcentaje de cobertura continua	Intensidad de movilidad	Calidad de <i>roaming</i>
55%	Medio	5,84969697
25%	Mínimo	5,151538462
80%	Mínimo	5,143684211
30%	Mínimo	5,117272727

Tabla 2-8 Calidad de movilidad y *roaming* en 802.11g.

Si se evalúa la incidencia de la cobertura en las dos bandas de transmisión se puede ver que 25% es la mejor cobertura para la topología ESS. Los resultados señalan que en mínimo se obtienen mejores resultados y en medio siempre hay menos pérdida de paquetes durante el *roaming*, pero en mínimo se tiene mejor ancho de banda; por esta razón todas estas actividades y las siguientes se hicieron a una velocidad de 1m/8s con la

configuración de intensidad de movilidad en mínimo. En este momento el único proceso que introducirá retardo o cortes en la conexión será la renovación de la dirección IP que consta de la desconexión del AP antiguo y conexión con el nuevo AP; esto debido a que no se ha configurado ningún tipo de seguridad.

2.4 CONFIGURACIÓN Y VERIFICACIÓN DEL *ROAMING* PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS CON SEGURIDAD Y SIN *STREAMING*

2.4.1 Montaje de la topología ESS con seguridad y sin *streaming*

El montaje permanece de forma constante al igual que el citado en la sección 2.3.1, simplemente que en este caso se tendrá un equipo de autenticación y verificación conectado directamente al sistema de distribución como se observa en la Figura 2-20.

La autenticación personal se hace ante un AP ingresando una clave o llave de validación y la autenticación empresa se hace usando un servidor de autenticación que en este caso fue RADIUS. Se dividieron físicamente los servicios de autenticación y de DHCP, para evitar conflictos en asignación de direcciones IP, mantener la misma dirección IP en las transiciones entre APs, aumentar la velocidad de autenticación y mejorar la posibilidad de *roaming*.

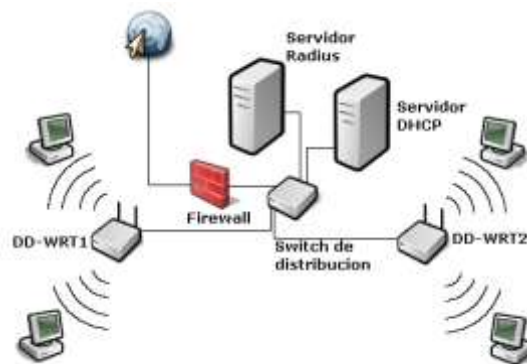


Figura 2-20 Topología ESS con seguridad y sin *streaming*.

El sistema operativo utilizado para la autenticación fue Opensuse 10.2. Esto se logró tras un trabajo largo y desgastante y muchas pruebas con fallas y errores al intentar con otras distribuciones sin ningún resultado óptimo. Esta distribución de Linux fue la que permitió realizar la autenticación sin inconvenientes así mismo su instalación y configuración (ver Apéndice D). Freeradius ofrece las opciones más comunes para un cliente inalámbrico como son TLS con certificados personalizados para cada cliente, TTLS con PAP, CHAP, MS-CHAP, PEAP con GTC, MS-CHAPV2. Las pruebas para WPA y WPA 2 en empresa fueron validadas para cada tipo de autenticación RADIUS para confrontar los distintos tiempos del proceso de validación. Los resultados del estudio completo de seguridad sin *roaming* se encuentran en el Apéndice E. El estudio resumido del Apéndice E es vital ya que brinda conclusiones importantes referidas a la validación de un cliente en una ubicación estática con diferentes tipos de autenticación, el tiempo promedio en que un cliente se asocia a un AP es de 1 a 2 segundos y para su mejor entendimiento es dividido en 5 paquetes.

La Figura 2-21 es una muestra de la asignación de dirección IP a un cliente móvil tomada con la herramienta Wireshark (ver Apéndice A), el paquete número 1 es del protocolo de árbol de extensión (STP, *Spanning Tree protocol*) el cual le permite a los dispositivos de

interconexión activar automáticamente los enlaces de conexión y evitar bucles indeseados. Luego los 4 paquetes que se pueden ver desde el segundo hasta el quinto muestran el proceso de asignación de dirección IP. Primero hay una búsqueda del servidor con la orden DHCP *Discover*, luego el servidor envía un DHCP *offer* el cual brinda la dirección a la estación móvil solicitante. Después se finaliza el intercambio de paquetes con un DHCP *Request* y un DHCP *ACK* los cuales son el punto final a la conexión y dan por entendido que la estación móvil acepta la dirección IP.

No.	Source	Destination	Protocol	Info
1	D-Link_3c:6f:71	Spanning-tree-(for-br	STP	Conf. Root =
2	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
3	192.168.1.1	192.168.1.100	DHCP	DHCP offer
4	0.0.0.0	255.255.255.255	DHCP	DHCP Request
5	192.168.1.1	192.168.1.100	DHCP	DHCP ACK

Figura 2-21 Paquetes básicos de conexión.

La variación del tiempo de asignación de dirección IP es producida por la respuesta del servidor DHCP y por la congestión de los canales utilizados para su alcance, esto quiere decir que si se aumenta el número de conexiones con clientes móviles, el tiempo para obtener una dirección IP aumentará gradualmente debido a la capacidad y uso continuo del canal, así como también del servidor DHCP. Su estudio se puede ver en la Tabla B12 en la parte final del Apéndice B.

El Apéndice E demuestra que el tipo de autenticación de red personal no maneja mucha diferencia al utilizar WPA o WPA 2 pero se obtiene mejores resultados utilizando TKIP que AES y en este caso por mínima que sea la diferencia, la banda de transmisión de 802.11g es mejor que 802.11b por milisegundos, además se nota que se obtienen mejores resultados con un tamaño de clave de cifrado superior a 20 valores ASCII, pues se obtuvieron valores por debajo de 2 segundos entre rangos de autenticación de 0,095377 hasta 5,098085 (segundos). En la banda de transmisión 802.11b se ve una disminución del tiempo de autenticación con TTLS y cifrado de datos AES y 802.11g disminuye su tiempo de autenticación con TLS, además en las dos opciones la certificación reduce el tiempo de autenticación pero sin validar la información de servidor, lo cual puede mejorar el establecimiento de la conexión entre rangos de 0,217683 hasta 6.414367 segundos.

Si se analiza el Apéndice E y se toman los valores de tiempo de autenticación para el tipo empresa y personal se puede ver que el periodo de duración se mantiene por debajo de los 2 segundos. La diferencia de tiempo entre los 2 tipos de autenticación es del orden de milisegundos más bajo para personal, pero si se evalúa la eficiencia, la seguridad de la conexión y la información, resulta mejor utilizar el tipo de autenticación de red empresa con servidor RADIUS.

La elección de la herramienta de gestión de red inalámbrica¹⁵ influye en el momento de la autenticación y en el manejo de los paquetes. El Apéndice E muestra que el uso de Windows como herramienta de gestión inalámbrica reduce el tiempo de asignación de dirección IP, pero la herramienta propietaria Intel PROset/ Wireless administra la autenticación mejor al reducir el tiempo de autenticación.

¹⁵ La herramienta de gestión de red inalámbrica permite al cliente móvil el manejo de todas las opciones necesarias para la conexión con el punto de acceso.

2.4.2 Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con la funcionalidad de *roaming*

El estudio de seguridad concentrado en el Apéndice E indica los valores de bloque de seguridad que tuvieron los mejores resultados para el tipo de seguridad empresa y personal siendo gestionado por la herramienta Intel PROset/ Wireless wifi (Ver Apéndice A). La experimentación que evalúa la seguridad con *roaming*, se hizo tomando las combinaciones de seguridad óptimas y deficientes¹⁶ encontradas en el estudio de seguridad sin *roaming* y se compuso una serie de nuevas pruebas de WPA con *roaming* expresadas en la Tabla 2-9 manejando una cobertura continua de 25 % y una intensidad de movilidad configurada en mínimo. Es indispensable ver el estudio completo en el Apéndice E.

Composición de las pruebas de WPA con <i>roaming</i> .									
Tipo de autenticación		Empresa				Personal			
Banda de transmisión		802.11g		802.11b		802.11g		802.11b	
Resultado		Opt.	Def.	Opt.	Def.	Opt.	Def.	Opt.	Def.
Combinación de seguridad		TLS	PEAP	TTLS	PEAP	40	20	20	30
			MSCHAPV2	PAP	GTC	ASCII	ASCII	ASCII	ASCII
Codificación de los datos		TKIP	AES	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP
Combinación de seguridad	Certificación	Con	Con	Con	Con	Ninguno			
	Validación	Sin	Sin	Sin	Sin				
Identidad de movilidad		**LO\AA		**LO\AA					
**LO\AA = LOWENBRAUN\Andres Arce = Dominio\Usuario: La identidad de movilidad es la Información brindada por el usuario que es necesaria para la autenticación y que es confrontada por el RADIUS en el archivo users. Opt = Óptimo, Def = Deficiente.									

Tabla 2-9 Composición de las pruebas de WPA con *roaming*.

Los resultados de la composición de WPA con *roaming* señalan que la autenticación de red WPA empresa tiene problemas al utilizar autenticación con tarjeta de testigo genérico (GTC, *Generic Token Card*), debido a que una nueva conexión con un AP requiere la entrada manual de la contraseña de autenticación por parte del usuario móvil, generando pérdida de paquetes por cada segundo que no se complete la actualización de la información. Debido a lo anterior el porcentaje de pérdida de paquetes es mucho mayor que los otros métodos. Si se compara a TLS y PEAP-MSCHAPV2 en la banda de transmisión 802.11g se observa que TLS es más rápido con la autenticación en *roaming* pero no realiza el proceso de forma transparente al tener paquetes perdidos en el instante exacto de transición al otro AP. Se puede decir que el túnel de autenticación PEAP hace un mejor trabajo que TLS (Ver Apéndice E).

En el estándar 802.11b se evidencia que un túnel de autenticación TTLS es óptimo ya que el proceso de *roaming* se ejecuta muy bien aunque con pérdida de paquetes, pero es la combinación óptima presente porque se nota su estabilidad ante la transmisión de los datos (ver Tabla E11 Apéndice E).

El tipo de autenticación de red WPA personal demuestra mejores resultados, esto es predecible debido a que se restan algunos pasos en la autenticación al ser solo el AP y el cliente los que validan la información de certificación. Se puede ver que un tamaño de

¹⁶ La combinación de seguridad óptima es la que obtuvo mejores resultados respecto a retardo y pérdida de paquetes y la combinación de seguridad deficiente es la que obtuvo los más bajos resultados respecto a retardo y pérdida de paquetes.

llave de codificación pequeña no siempre es relacionado con menor tiempo de autenticación, pero lo que sí se puede deducir es que al disminuir el tiempo de autenticación se redujo también el número de paquetes que se pierden en el proceso de *roaming* (ver Apéndice E).

El retardo encontrado en el tipo de autenticación empresa es más alto que el de tipo personal con unos promedios de retardo medio-alto y medio respectivamente, según la Tabla B11 del Apéndice B.

2.4.3 Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con la funcionalidad de *roaming*

El estudio de autenticación concentrado en el Apéndice E indica los valores de bloque de autenticación que registraron los mejores resultados para el tipo de autenticación empresa y personal, y la autenticación siendo gestionada por la herramienta Intel PROset/ wireless Wi-Fi, ver Apéndice A. La experimentación que evalúa la seguridad con *roaming*, se hizo tomando las combinaciones de seguridad óptimas y deficientes encontradas en el estudio de seguridad sin *roaming* y se realizaron una serie de nuevas pruebas de WPA 2 con *roaming* expresadas en la Tabla 2-10 manejando una cobertura continua de 25 % y intensidad de movilidad en mínimo, el estudio completo se encuentra en el Apéndice E.

Composición de las pruebas de WPA 2 con <i>roaming</i> .									
Tipo de autenticación		Empresa				Personal			
Banda de transmisión		802.11g		802.11b		802.11g		802.11b	
Resultado		Opt.	Def.	Opt.	Def.	Opt.	Def.	Opt.	Def.
Combinación de seguridad		TLS	PEAP	TTLS	PEAP	30	50	63	10 ASCII
			GTC	CHAP	GTC	ASCII	ASCII	ASCII	
Codificación de los datos		TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP
Combinación de seguridad	Certificación	Con	Con	Con	Con	Ninguno			
	Validación	Sin	Sin	Sin	Sin				
Identidad de movilidad		**LO\AA		**LO\AA					

**LO\AA = LOWENBRAUN\Andres Arce = Dominio\Usuario: La identidad de movilidad es la Información brindada por el usuario que es necesaria para la autenticación y que es confrontada por el RADIUS en el archivo *users*.
Opt = Óptimo, Def = Deficiente.

Tabla 2-10 Composición de las pruebas de WPA 2 con *roaming*.

Los resultados de las pruebas de WPA 2 con *roaming* señalan que la autenticación de red WPA 2 empresa para las dos bandas de transmisión con la combinación de seguridad PEAP-GTC no es apta para ninguna de las dos debido a la información solicitada en el evento de *roaming*. Los túneles TLS o TTLS son indicados para su implementación para el proceso de reautenticación, sin embargo, hay paquetes perdidos en la transición entre APs. La desconexión se ve reflejada en el corte de aplicaciones TCP que son orientadas a conexión en las que una desconexión corresponde a la pérdida total de toda la sincronización. Ninguna configuración que utilice un servidor RADIUS brinda el ambiente idóneo para una aplicación en tiempo real que pueda soportar *roaming* siendo orientada a conexión, es inminente la desconexión y no se puede controlar la incertidumbre del envío de paquetes por la red de distribución.

Los resultados de WPA 2 personal siempre presentan un número reducido de paquetes que se pierden durante el *roaming*, la llave de codificación seleccionada puede ser crucial en el momento de tener un efecto de *roaming* totalmente transparente, observar Tabla E14 y complementar con el Apéndice E.

El retardo encontrado en el tipo de autenticación empresa es más alto que el tipo de autenticación personal con unos promedios de retardo medio-alto y medio respectivamente según la Tabla B11 del Apéndice B.

2.4.4 Búsqueda de variables críticas que influyen en el desempeño cuando hay *roaming* y seguridad

La elección de seguridad es importante y se puede ver en los resultados del estudio en el Apéndice E. En todo proceso de *roaming* hay un problema y es la desconexión y reconexión porque siempre que un cliente se encuentre en función de *roaming* hay varios pasos los cuales se traducen en tiempo y discontinuidad en la transmisión. El tiempo de reconexión está ligado directamente al túnel de autenticación que se utilice y al protocolo de autenticación. El tiempo de reautenticación con el nuevo AP depende directamente del proceso que se lleve a cabo para la validación y asignación de dirección IP. La conversación que se mantiene entre el cliente móvil, el AP y el servidor RADIUS genera un grupo de eventos en los que se transmite la información de autenticación y las llaves de cifrado. Con el tipo de autenticación empresa el servidor entrega la información de autenticación o propone el método de túnel de autenticación que está configurado como predeterminado en el servidor RADIUS, esto se le presenta al cliente facilitando la autenticación durante el *roaming*, aquí es donde se dividen los procesos dependiendo del método y protocolo de autenticación. Luego de la comunicación y establecimiento de los túneles de cifrado se pasa al bloque de derivación de llaves de cifrado que consta de la PTK que es la llave temporal de pareja y GTK que es la llave temporal de grupo, en este bloque se realiza un intercambio de mensajes entre el AP y el cliente móvil para luego terminar con la asignación de dirección IP al cliente.

Luego de estudiar el proceso de *roaming* detalladamente se descubrió que las variables críticas entre seguridad y *roaming* se encuentran implícitas en el número de eventos realizados y el tiempo límite para cumplir satisfactoriamente el proceso de transición entre puntos de acceso. La Figura 2-22 presenta el número de eventos necesarios para cumplir con una autenticación, entre mayor sea el número de eventos o si se sobrecarga la conexión con mucha más seguridad ya sea certificaciones o validaciones, mayor será el tiempo de autenticación y mayor será el retardo presentado por el número de paquetes transmitidos entre el autenticador y el cliente móvil.

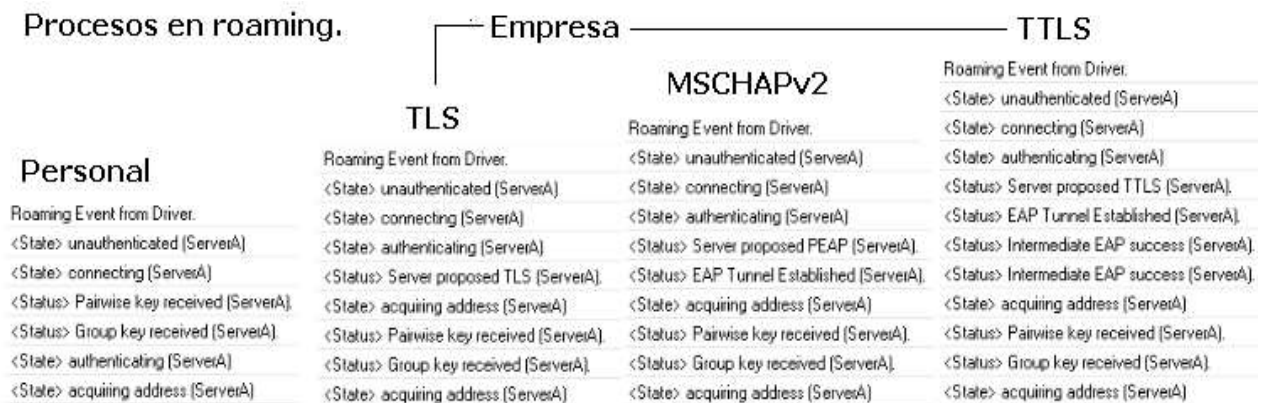


Figura 2-22 Procesos de autenticación en redes inalámbricas.

El proceso de una autenticación inicial es diferente al proceso de autenticación en *roaming* con un AP desconocido y al proceso de autenticación en *roaming* con un AP conocido, la diferencia puede notarse en la Figura 2-23 y esto se expresa en más eventos y tiempo de autenticación.

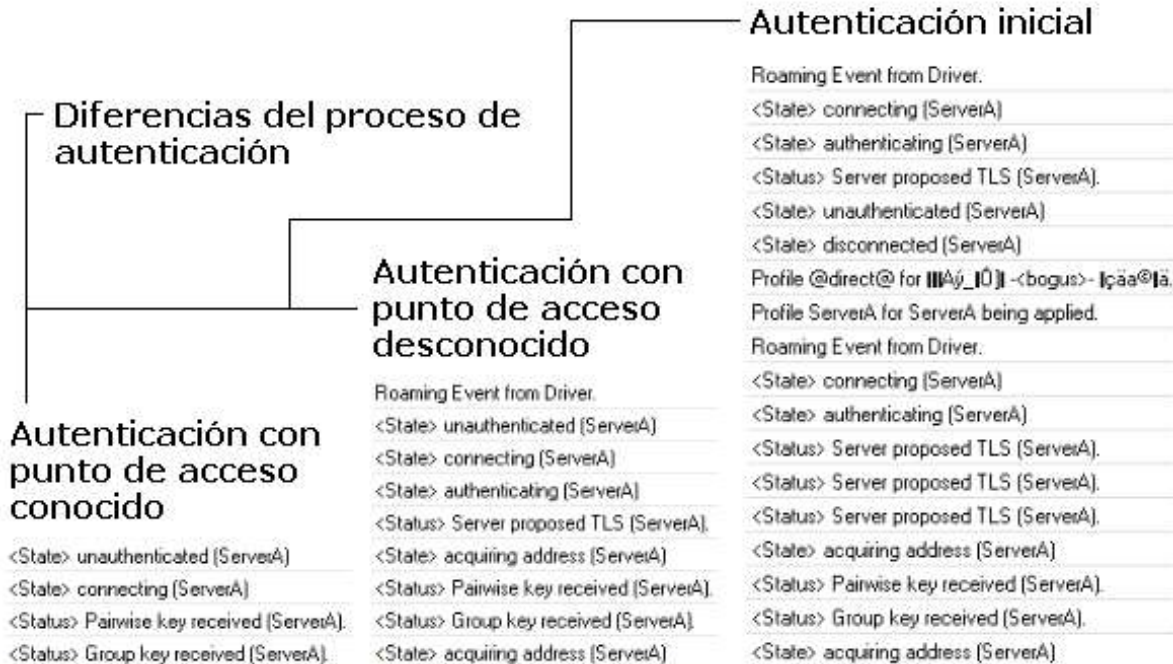


Figura 2-23 Diferencias del proceso de autenticación.

2.4.5 Análisis de resultados y generación de conclusiones

Los datos adquiridos dejan ver claramente que utilizar una autenticación tipo empresa es más robusto que una autenticación tipo personal. Si se equilibra el funcionamiento de *roaming* con una buena asignación de seguridad se va a tener buenos resultados. Dependiendo del estándar hay opciones importantes, para 802.11g utilizar WPA 2 empresa con tipo de autenticación TLS+TKIP más certificación pero sin validación de servidor de autenticación y para 802.11b utilizar WPA 2 personal con un tamaño de codificación de datos 10 ASCII y codificación de datos TKIP, se concluye que en los dos casos los resultados serán los mejores. Entre mayor sea el equilibrio que se desea menos problemas y más transparente será el servicio de *roaming* para el cliente.

Los paquetes perdidos son causa del número de eventos requeridos que forman la comunicación entre el AP y el servidor RADIUS. Cuando un cliente ya se ha autenticado con un AP y ejecuta el proceso de *roaming*, los eventos se reducen a una conversación entre el cliente móvil y el AP e incluyen la desconexión, la conexión y la derivación de llaves de cifrado.

Las Figuras 2-24 a 2-28 contienen a la derecha los eventos (capturados con la herramienta Intel PROset Wireless - visor de sucesos) correspondientes a los paquetes capturados y mostrados a la izquierda (capturados con la herramienta *wireshark*) que se ven en el instante del *roaming*.

La autenticación apoyada por un servidor RADIUS es bastante segura y aunque la autenticación PSK es más rápida por el número de eventos que presenta, la autenticación con RADIUS es comparable con la PSK en el momento del *roaming*, debido a que su

diferencia es de 1 segundo como máximo en el momento de la transición con APs desconocidos y 0 segundos de diferencia en el momento de la transición con APs conocidos (ver Apéndice E y herramientas de evaluación del Apéndice A).

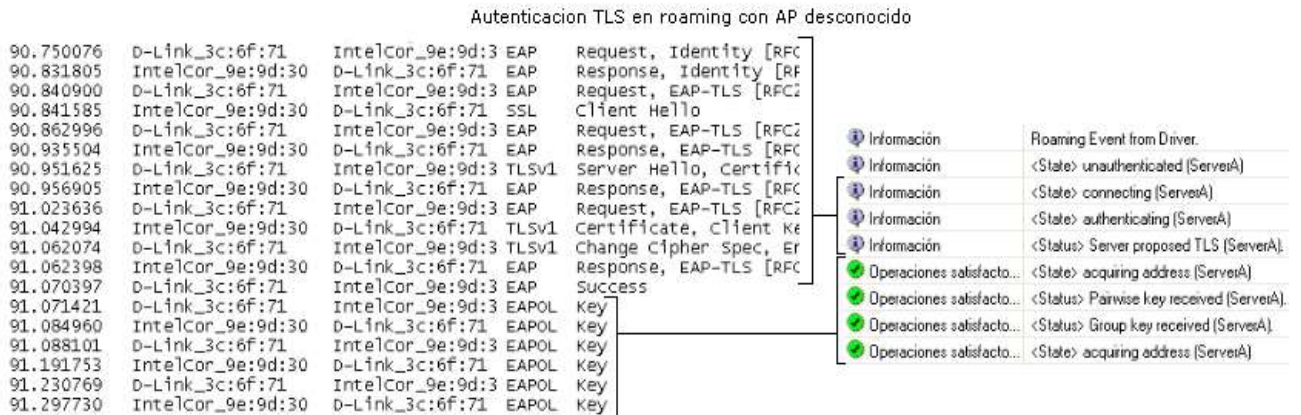


Figura 2-24 Autenticación TLS en *roaming* con AP desconocido.

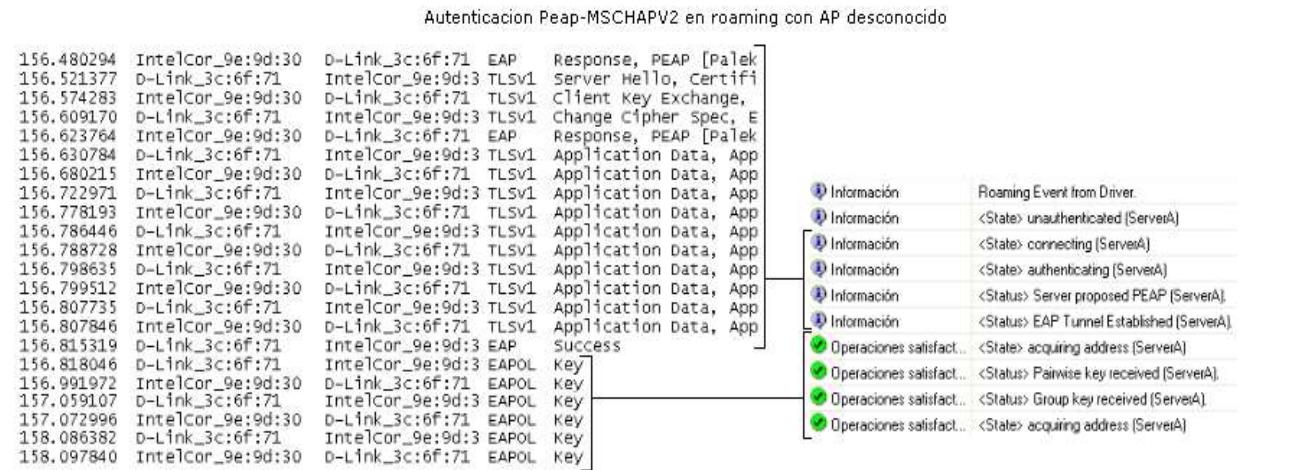


Figura 2-25 Autenticación PEAP-MSCHAPV2 en *roaming* con AP desconocido.

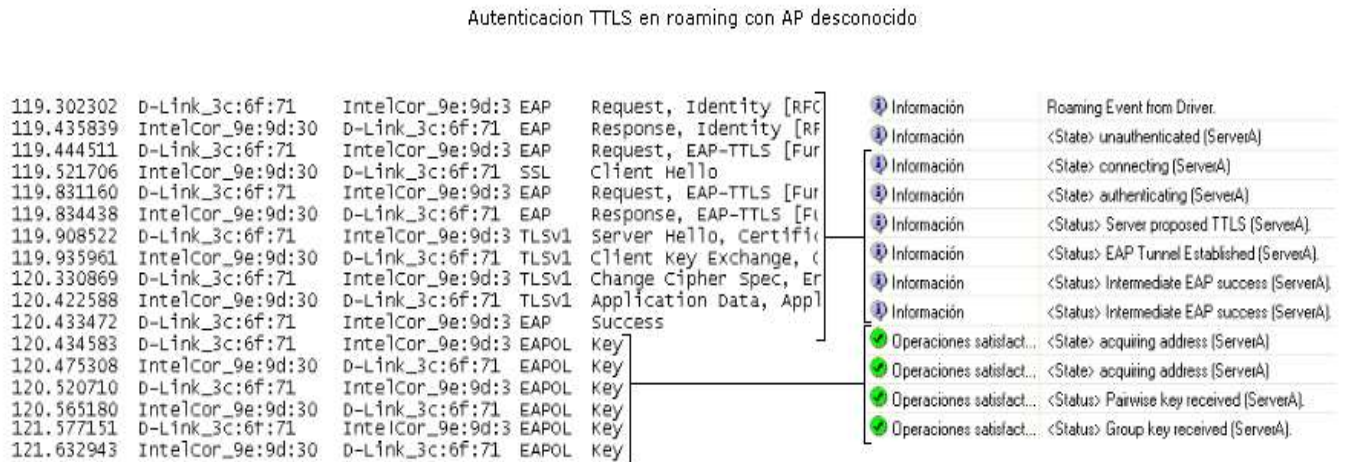


Figura 2-26 Autenticación TTLS en *roaming* con AP desconocido.

Autenticación PSK en roaming con AP desconocido

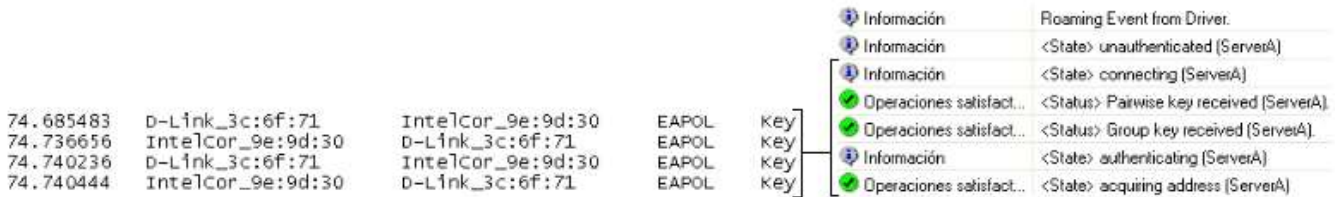


Figura 2-27 Autenticación PSK en *roaming* con AP desconocido.

Autenticación Peap-GTC en roaming con AP desconocido

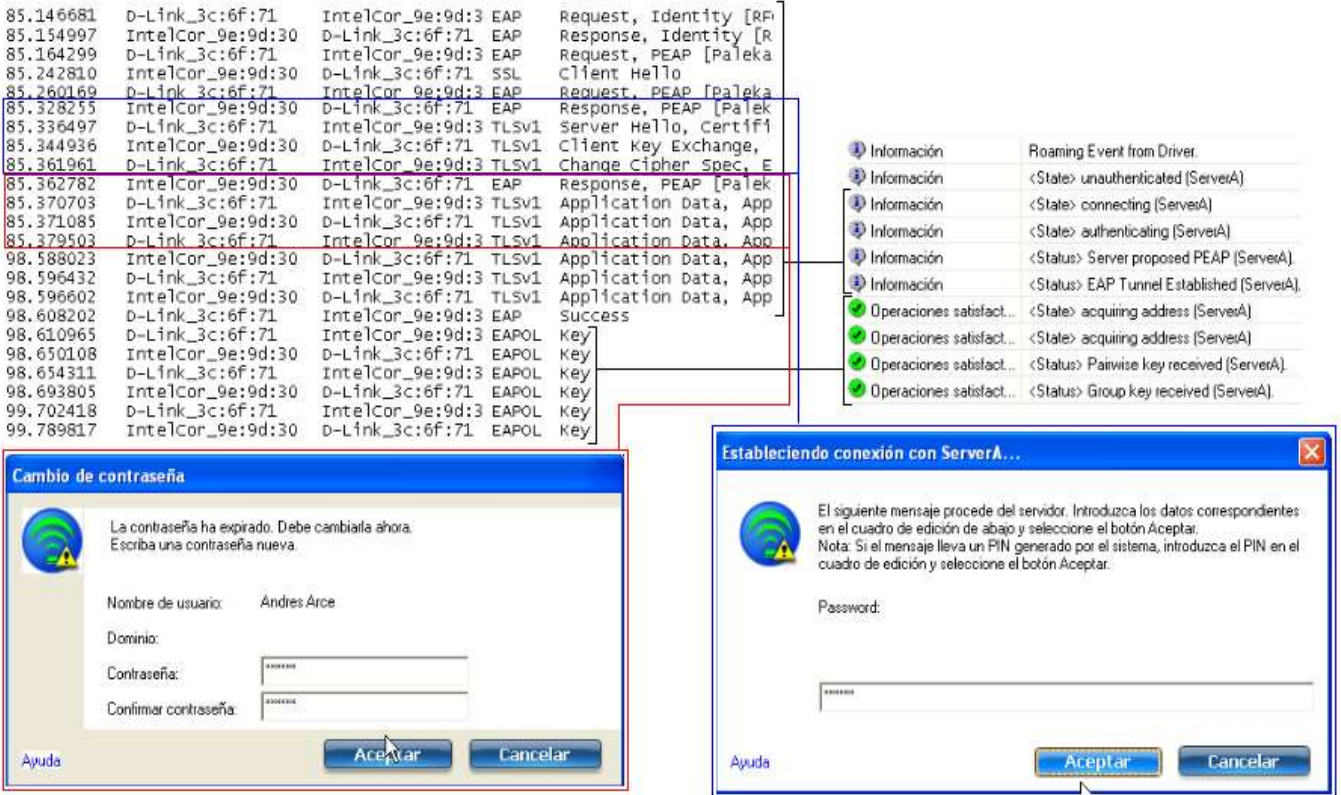


Figura 2-28 Autenticación PEAP-GTC en *roaming* con AP desconocido.

El *roaming* entre puntos de acceso conocidos reduce los paquetes perdidos a cero pero aumenta el tiempo de transmisión y recepción de paquetes en WPA al no presentar la mejora de 802.11i de preautenticación y caché de llaves. En WPA 2 se reducen las pérdidas y el tiempo de transmisión al cumplir con 802.11i aunque sigue ocurriendo la desconexión y conexión pero la finalidad es la transparencia o reducción al máximo de la caída abrupta causada por el movimiento del cliente entre puntos de acceso.

Es totalmente importante que el servidor DHCP esté centralizado y no configurado en un AP, debe estar configurado ya sea como servicio en el mismo servidor RADIUS o un equipo de red con la opción de configuración DHCP. Esta topología ayudará en el momento de adquisición de dirección IP y no causará conflictos ya que si no está en el lugar indicado o hay más de un servidor, se presentarían problemas de direcciones IP duplicadas y de trayectos diferentes para acceder al servicio, influyendo también en los tiempos de *roaming*.

2.5 CONFIGURACIÓN Y VERIFICACIÓN DEL *ROAMING* PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS SIN SEGURIDAD Y CON *STREAMING*

2.5.1 Montaje de la topología ESS sin seguridad y con servidor de *streaming*

El montaje permanece de forma constante al igual que el montaje citado en la sección 2.3.1 con la diferencia que se aumentó un equipo de transmisión y verificación de *streaming* conectado directamente al sistema de distribución, la instalación del servidor de *streaming* VLC se realiza en un sistema operativo Linux Opensuse 10.2 preinstalado en el computador que se encuentra fijo. La instalación y configuración del servidor de *streaming* se puede ver en el Apéndice F. El cliente móvil que recibe la transmisión de *streaming* debe conectarse exactamente unos segundos después de que el servidor de *streaming* inicia la transmisión debido a que al tratar de llevar la transmisión del servidor se perderán paquetes, por defecto siempre se pierden paquetes al conectarse los cuales son remplazados por paquetes en blanco, para nivelar la tasa de transmisión y empezar la decodificación y reproducción de los paquetes.

El proceso de encapsulamiento, codificación y transporte puede ser crucial para el éxito de una transmisión, el uso individual de encapsulamiento en el transmisor consume mucho más recursos en tasa de bit de lectura y tasa de envío, ya que la información es tomada inmediatamente de los medios, empaquetada y enviada, esto genera paquetes más grandes en tamaño con lo cual se crean problemas en la necesidad de más ancho de banda para transmitir y problemas en la reproducción debido a que la velocidad de reproducción es mayor a la velocidad en que se reciben y decodifican los paquetes. La codificación minimiza el tamaño de los paquetes a enviar y minimiza la velocidad necesaria para transmitir los paquetes, con lo cual se pueden usar en comunicaciones con bajos anchos de banda. La reducción de video consiste en estudiar la información tomada de varios fotogramas y clasificar el cambio generado por el movimiento, de esta forma solo se codificara o enviara el espacio que representa un cambio en la imagen, y por ende siendo menor el tamaño en comparación con toda la información total de los fotogramas.

Para la reducción del tamaño de los paquetes audio se estudia el sonido y su ausencia, de esta forma cuando no se está generando audio no hay necesidad de enviar *buffer* de silencio simplemente no se envía la información minimizando el tamaño del paquete final. El único problema de la codificación es que se introduce un pequeño tiempo adicional mientras las muestras tomadas de los medios multimedia son tratadas y codificadas por separado para luego tomar fotogramas codificados y un *buffer* de audio para empaquetarlo en un solo paquete el cual será enviado, de esta forma se duplica el tiempo de codificación ya que el receptor debe decodificar para reproducirlo. Este tiempo de procesamiento de las señales de audio y video se ve reflejado en los paquetes que por defecto se pierden para estabilizar la velocidad de recepción y decodificación. Para mantener la comunicación visual con el cliente se reproducen fotogramas en blanco y el audio se encuentra en silencio hasta que del proceso de recepción y decodificación dan como resultado señales por separado de audio y video las cuales posteriormente se reproducen.

2.5.2 Estudio de desempeño del servicio de *streaming* en tiempo real en redes 802.11b/g

El estudio de desempeño del servidor de *streaming* se hizo en una ubicación en la cual existe una degradación de la señal RSSI en topología BSS con el fin de poder observar la pérdida de paquetes. En el momento de *roaming* estos lugares en el extremo de las coberturas serán los que se experimenten durante el movimiento. El estudio de ancho de banda del Apéndice B muestra que el estándar 802.11b presenta un promedio superior a 2 Mbps y el estándar 802.11g presenta un promedio superior a 4 Mbps. La prueba se realizó bajo el estándar 802.11b estudiando el encapsulamiento y la transcodificación en video con tasa de bit de 2 Mbps y transcodificación de audio con tasa de bit de 256 Kbps y para 802.11g y encapsulamiento y la transcodificación en video con tasa de bit de 3 Mbps y transcodificación de audio con tasa de bit de 512 Kbps para 802.11g, el estudio evaluó en el video el número de fotogramas perdidos, fotogramas en blanco y en audio los *buffers* perdidos en un cliente VLC. La calidad de audio manejada es calidad CD con una velocidad de muestreo de 44,1 KH con 16 bit por muestra manejando 2 canales de audio o estéreo.

⊕ Estudio y configuración de los métodos de encapsulamiento y codificador/decodificador de audio para un servicio de *streaming* de audio en tiempo real en 802.11b/g

Los 9 métodos de encapsulamiento se pusieron a prueba durante un minuto y se observó como respondían frente a la captura de audio, evaluando los *buffers* perdidos en su totalidad y el cumplimiento del tiempo de muestra (ver características de encapsulamiento en el Apéndice F).

El Apéndice F concentra el estudio completo de *streaming* con el cual los diferentes de encapsulación fueron evaluados, sacando como mejor candidato a Mpeg-Ps. Éste brinda la estabilidad de transmisión tolerable al movimiento, pero no lo suficiente debido al ancho de banda libre necesario que debe tolerar 802.11b. Esto se puede probar debido a que un mayor ancho de banda proporcionado por 802.11g logró soportar más carga de paquetes sobre la red teniendo valores de cero en la pérdida de *buffers* para casi la mayoría de métodos de encapsulamiento. Por esta razón se estudió los codificadores/decodificadores que funcionan con cada método de encapsulamiento para encontrar la combinación con mejor funcionamiento.

La pérdida de *buffers* de audio es un problema grave porque la comunicación se pierde y el cliente no estará satisfecho con la recepción debido a que no puede entender lo que dice el audio. Se puede ver que el promedio de *buffers* reproducidos durante un minuto es superior a 2000. La transmisión de audio no es tolerable a la pérdida de esta información debido a que la reproducción de pocos paquetes no brinda un entendimiento lógico comparado con la señal original transmitida.

La codificación mejoró la forma de transmisión en tal grado que el ancho de banda necesario para la transmisión de la misma información disminuyó. Los *buffers* perdidos también bajaron de cantidad y amplió la estabilidad a las fluctuaciones generadas por la recepción de los paquetes. Los últimos 6 codificadores/decodificadores de audio no pueden ser utilizados ya que no proporcionan un nivel de calidad bueno. Se puede decir que la combinación óptima para transmitir audio por *streaming* en 802.11b y 802.11g sería encapsulamiento MP4 con codificación Mp4a y la combinación deficiente sería Mov con codificación S16l. (ver Apéndice F)

⊕ **Estudio y configuración de los métodos de encapsulamiento y codificador/decodificador de video para un servicio de *streaming* de video en 802.11b/g**

Los 9 métodos de encapsulamiento se pusieron a prueba durante un minuto y se observó como respondían frente a la captura de video, evaluando los fotogramas perdidos, fotogramas en blanco y el cumplimiento del tiempo de muestra (ver Apéndice F). El tamaño de los paquetes de video emitidos por el encapsulamiento son demasiado grandes perdiendo la sincronía entre recepción y reproducción, a causa de la avalancha de paquetes en recepción se pierde la continuidad en la reproducción tomando la decisión de descartar paquetes y reproducir fotogramas en blanco mientras se alcanza el nivel de estabilidad necesario. El método de encapsulamiento óptimo sería el que mayor tiempo de reproducción tenga demostrando estabilidad, es decir, el que tenga menos fotogramas en blanco lo cual indica un nivel mayor de fotogramas reales, pues cuando hay pérdida de fotogramas reales de video se reproducen fotogramas en blanco para no perder la atención del cliente. También el mejor método de encapsulamiento es el que presenta menor número de fotogramas perdidos los cuales son fotogramas que no pueden ser vistos a causa de errores. El Apéndice F demuestra que el método de encapsulamiento que mejor se comporta con respecto a pérdida de paquetes y reproducción de paquetes en blanco es mp4 al utilizarlo sin ningún tipo de codificación.

En la banda de transmisión de 802.11b los métodos de encapsulamiento no superan el minuto de prueba mientras que en 802.11g todos superan la prueba de tiempo de reproducción. La utilización de la codificación de video aumenta sin dudas el tiempo de sostenimiento del *streaming* y reduce el número de pérdida de paquetes. Para esta sección la combinación óptima para transmitir video por *streaming* sería mp4 con codificación Div3 y la combinación deficiente sería Mpeg-TS con codificación Mp2v (ver Apéndice F).

⊕ **Estudio y configuración de los métodos de encapsulamiento, codificador/decodificador de audio y codificador/decodificador de video para un servicio de *streaming* de audio y *streaming* de video en 802.11b/g**

Los 9 métodos de encapsulamiento se pusieron a prueba durante un minuto y se observó como respondían frente a la captura de audio y captura de video, evaluando los *buffers* perdidos, fotogramas perdidos, fotogramas en blanco y el cumplimiento del tiempo de muestra (ver Apéndice F). El encapsulamiento de audio y video en un solo paquete introducirá considerablemente más carga a la transmisión perturbando la estabilidad en la reproducción, el Apéndice F denota que el codificador/decodificador ASF es el que mayor tiempo de reproducción mantiene con promedio de pérdidas normales para los estándares 802.11b y 802.11g sin utilizar ninguna codificación y Mpeg-TS presenta pérdida de paquetes superiores y tiempo de reproducción por debajo del tiempo de muestra o tiempo de prueba estipulado de 60 segundos.

El *streaming* funciona empaquetando el video o el audio por separado para luego generar el contenedor que es enviado por la red, por esta razón si se quiere mejorar la combinación de ASF o Mpeg-TS sería complementar la configuración del servicio con las codificaciones óptimas y deficientes en audio y en video de la siguiente forma, ASF con codificación de audio Mp4a y codificación de video Div3, esta es la óptima. Y Mpeg-TS con codificación de audio S16l y codificación de video Mp2v, esta es la deficiente.

2.5.3 Estudio del desempeño del servicio de *streaming* en tiempo real durante el *roaming* en 802.11b/g

Este estudio evaluó el proceso de *roaming* con las combinaciones óptimas y deficientes de encapsulamiento y codificadores/decodificadores de *streaming* de audio, *streaming* de video, y *streaming* de audio y video encontrados en la sección anterior. Esta sección se enfocó en evaluar el *roaming* en una topología ESS con traslape de cobertura continua de 25% sin seguridad con el servicio de *streaming* en tiempo real.

El comportamiento del *streaming* se ve afectado por la transición rápida entre puntos de acceso, cuando un cliente se conecta con el servidor de *streaming* hay paquetes que son descartados mientras se crea una sincronización de recepción y transmisión de los paquetes discontinuos, el tiempo de estabilización se ve reflejado en un retraso de la señal original con la señal recibida, esto quiere decir que aunque exista un corte en la conexión hay paquetes atrasados que seguirán reproduciéndose, si esto ocurre, la aplicación cliente reproducirá paquetes en blanco hasta que restablezca la recepción de paquetes. Es necesario un sistema cliente que al perder sincronización o paquetes repare la conexión hacia el servidor y reciba nuevos paquetes para crear un nuevo flujo de datos. La transmisión de audio y video en un mismo paquete presenta mucha más carga en tamaño y procesamiento. La utilización de codificadores/decodificadores mejoró sin duda la fluidez y redujo las pérdidas y uso de la red (ver Apéndice F).

2.5.4 Análisis de resultados y generación de conclusiones

Para un cliente móvil es mejor tener una aplicación receptora de paquetes que tenga la opción de reconexión inmediata al perder sincronización o desconexión con el servidor de *streaming*. Cuando se definieron los métodos de encapsulamiento y los codificadores/decodificadores que se evaluarían durante el *roaming* se tenían información de su funcionamiento, en la prueba realizada se confirmó la tolerancia a la movilidad cuando se utilizan las combinaciones estudiadas en las secciones anteriores de audio y video en especial.

Es importante describir que el efecto de transición a puntos de acceso desconocidos es diferente que transiciones a puntos de acceso conocidos. La transición a puntos de acceso desconocidos genera en la aplicación receptora un problema de espera de paquetes debido a que no se detecta una desconexión física del AP obligando a la aplicación a esperar por la recepción de paquetes del servidor de *streaming* con lo cual se causa la reproducción de paquetes en blanco. La transición a puntos de acceso conocidos es mucho mejor por el tiempo de reconexión y porque el cambio se hace mucho más limpio detectando la desconexión física dándole a la aplicación la orden de reconectarse con el servidor inmediatamente, de esta manera son pocos los segundos que se pierden de entendimiento lógico (ver Apéndice F).

2.6 CONFIGURACIÓN Y VERIFICACIÓN DEL ROAMING PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS CON SEGURIDAD WPA Y CON STREAMING

2.6.1 Montaje de la topología ESS con seguridad WPA y servidor de *streaming*

En esta sección se utilizó el montaje citado en la sección 2.4.1 complementando con un

servidor de *streaming*. Para las experimentaciones se utilizaron las combinaciones óptimas de transmisión de *streaming* en las que se obtuvieron menos pérdidas y tolerancia a la movilidad así como también las que no se deberían utilizar en transmisiones con poco ancho de banda.

La experimentación está enfocada a la detección del suceso del *roaming* para estudiar el impacto causado por la seguridad en una transición entre puntos de acceso en los que se ha preconfigurado WPA empresa y WPA personal. Se tiene ya información del funcionamiento de la seguridad WPA y WPA 2 en el momento de *roaming* y el *streaming* en el momento del *roaming*, ahora se evalúa en conjunto el impacto generado en las transmisiones de *streaming* obtenido los tiempos y observando el tiempo de reconexión necesario para recuperar la transmisión ya capturada (ver estudio completo en el Apéndice G).

Por cada AP que sea agregado a la red de distribución es necesario integrarlo en el servidor de RADIUS, adicionando una porción de código en el archivo `clients.conf` ubicado en la carpeta `raddb` del servidor RADIUS.

```
client 192.168.1.2 {
    secret      = perseo2      *Dirección IP del AP
    shortname   = DD-WRT2     *Llave secreta compartida con RADIUS
    nastype    = other        *Nombre del AP
}
                                *Nombre de fabricante
```

Es importante que la configuración de dirección IP de cada AP sea diferente al igual que la contraseña secreta compartida entre el AP y el servidor RADIUS. La configuración del servidor de *streaming* se hace teniendo en cuenta el estándar que en este caso son 802.11b utilizando valores de velocidad de 2Mbps en video y 256 Kbps en audio y 802.11g utilizando valores de velocidad de 3Mbps en video y 512 Kbps en audio.

2.6.2 Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con el servicio de *streaming* de audio con mayor y menor desempeño

La autenticación WPA personal contiene menos eventos por lo tanto el tiempo de autenticación es menor generando buenos resultados en el momento de la transición entre puntos de acceso y la movilidad. Se puede ver perfectamente que aunque existen paquetes perdidos en el momento del *roaming*, el *streaming* de audio es lo suficientemente bajo en consumo de ancho de banda como para soportar los cambios de señal RSSI y cobertura. Se tiene la combinación de mp4 y mp4a que es la opción de mejor desempeño y se tiene mov y s16l que es la opción de desempeño deficiente. Las dos elecciones se soportan muy bien debido al suficiente ancho de banda del canal inalámbrico. Ver Tabla G1 o el estudio completo en el Apéndice G.

La autenticación empresa tiene un número de eventos mayor que la autenticación personal, el tiempo de autenticación en *roaming* está ligado al número de paquetes que estén circulando en la red en ese momento. Los eventos de certificación son un conjunto de conversaciones entre el cliente móvil, el AP y el servidor RADIUS. Al perder la sincronía de esta conversación la autenticación puede que no se concluya o puede aumentar el tiempo de autenticación. Se ve que una combinación de seguridad

PEAP+GTC+TKIP no sería óptimo utilizarla debido a que el tiempo que toma la autenticación es demasiado alta. Una buena opción de seguridad podría ser TLS+TKIP, claramente se puede notar que la elección de un buen método de encapsulamiento y codificador/decodificador de audio puede reducir el tiempo de autenticación y generar mayor desempeño en la movilidad y en el *roaming*, sin embargo, una combinación de seguridad mal seleccionada puede aumentar el tiempo de recepción de paquetes de *streaming* de audio. Ver Tabla G2 o el estudio completo en el Apéndice G.

2.6.3 Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con el servicio de *streaming* de video con mayor y menor desempeño

El ancho de banda necesario para la transmisión de video es mucho mayor que la transmisión de audio, la elección de Mp4+Mp4a se hizo porque en conjunto su consumo de recursos de red son bajos al contrario que Mov+Mp2v, por esta razón se tiene un mayor número de fotogramas perdidos y fotogramas en blanco cuando no se establece bien la sincronía de tamaño del paquete y transmisión de la información. El tipo de seguridad personal no afecta demasiado al *streaming* de video por sus tiempos de autenticación bajos los cuales no generan problemas críticos en la movilidad ni en el *roaming* (Ver Tabla G3 o el estudio completo en el Apéndice G).

Un caso contrario es el uso de WPA empresa con *streaming* de video, en éste se encuentran valores superiores de autenticación aumentando considerablemente el tiempo necesario para la reconexión con el servidor de *streaming*, además de tener fotogramas perdidos y en blanco mayormente producidos por Mov+Mp2v. También se presenta un mayor número de paquetes perdidos a causa de autenticaciones demasiado extensas en eventos y tiempo (Ver Tabla G4 o el estudio completo en el Apéndice G).

Un caso contrario es el uso de WPA empresa con *streaming* de video, en éste se encuentran valores superiores de autenticación aumentando considerablemente el tiempo necesario para la reconexión con el servidor de *streaming*, además de tener fotogramas perdidos y en blanco en mayor número producidos por Mov+Mp2v, también presenta un mayor número de paquetes perdidos causados por autenticaciones demasiado extensas en eventos y tiempo hasta su conclusión.

2.6.4 Estudio y configuración de WPA (personal y empresa usando servidor RADIUS) con el servicio de *streaming* de audio y video con mayor y menor desempeño

El uso de *streaming* de audio y video en un mismo canal inalámbrico necesitará muchos más recursos de red, el tiempo de autenticación es un poco mayor que utilizar *streaming* de audio o *streaming* de video. Es más difícil realizar las peticiones y las conversaciones necesarias entre el AP y el cliente móvil cuando existe un gran número de paquetes inundando la red, sin embargo, lo que más se ve afectado es el video, pues el audio es reproducido con normalidad a diferencia del video que presenta fotogramas perdidos y fotogramas en blanco. Ver Tabla G5 o el estudio completo en el Apéndice G.

En este caso es visible que la seguridad afecta al *streaming* y el *streaming* a su vez afecta la seguridad, es preciso aclarar que un proceso de autenticación extenso causa muchos paquetes perdidos causados por la desconexión previa a la autenticación con el nuevo AP, esto es reflejado en el tiempo de reconexión con el servidor de *streaming*, además de los paquetes perdidos por la movilidad y paquetes perdidos en el momento que se ejecuta el algoritmo de cambio de AP. Ver Tabla G6 o el estudio completo en el Apéndice G.

2.6.5 Análisis de resultados y generación de conclusiones

Se sabe que las combinaciones de *streaming* que se utilizaron funcionaron de la forma adecuada, lo que se necesita es conocer el grado de impacto en el *streaming* debido a la seguridad, la movilidad y el *roaming*. El tiempo de reconexión en un momento de transición entre puntos de acceso sin seguridad es de 9 segundos promedio, de los cuales 6 segundos son de conexión y sincronización y 3 segundos son de llenado del *buffer* de paquetes, luego de esto empieza la reproducción de la información ver la columna de tiempo para reproducción de las Tablas F14 y F15.

Si se analiza la Tabla 2-11, la configuración de seguridad con una transmisión de *streaming* experimenta menos tiempo de desconexión cuando la transición se hace entre puntos de acceso conocidos, debido a que el proceso de cambio de AP es mucho más rápido debido al número menor de eventos requeridos, además de esto se puede ver algo inesperado y es que el tiempo de reconexión con puntos de acceso desconocidos es menor o igual cuando se utiliza una autenticación con certificación WPA empresa, además de que la banda de transmisión de 802.11b es más estable en este sentido dando valores bajos con respecto a la banda 802.11g (ver estudio completo en el Apéndice G).

Tiempo de reconexión de <i>streaming</i> .								
Banda de transmisión	802.11b				802.11g			
Tipo de autenticación	WPA Personal		WPA Empresa		WPA Personal		WPA Empresa	
Tamaño de llave de codificación	20 ASCII	30 ASCII			20 ASCII	40 ASCII		
Combinación de seguridad			TTLS+ PAP+ TKIP	PEAP+ GTC+ TKIP			TLS+ TKIP	PEAP+ MSCHAPV2+ TKIP
Tiempo de reconexión con AP desconocido (s)	40	40	39	37	41	41	40	39
Tiempo de reconexión con AP conocido (s)	15	17	25	50	42	35	55	30

Tabla 2-11 Tiempo de reconexión de *streaming* para WPA.

2.7 CONFIGURACIÓN Y VERIFICACIÓN DEL ROAMING PARA IEEE 802.11B/G EN LA TOPOLOGÍA ESS CON SEGURIDAD WPA 2 Y CON STREAMING

2.7.1 Montaje de la topología ESS con seguridad WPA 2 y servidor de *streaming*

El montaje utilizado en esta sección es el citado en la sección 2.7.1 con la diferencia de que se configuró en los puntos de acceso el tipo de seguridad WPA 2 personal y WPA 2 empresa correspondientemente con las opciones de *streaming* con mayor y menor desempeño (ver estudio completo en el Apéndice G).

Las dos opciones de seguridad WPA 2 tienen campos de configuración diferentes como se observa en la Figura 2-29, la elección de seguridad personal requiere una clave o llave la cual será pedida en el momento de conectarse al AP. En el tipo de seguridad empresa se tiene los campos de configuración del servidor RADIUS, el puerto donde se envía la información y la llave secreta compartida con el servidor RADIUS. Estos datos deben coincidir con la información asignada en el servidor de autenticación RADIUS para establecer la comunicación y para que se transmita la información entre AP, servidor RADIUS y el cliente móvil.

Configuración de seguridad WPA 2 en el punto de acceso

Physical Interface ath0 SSID [ServerA] HWAddr [00:1C:F0:3C:75:E1]	
Security Mode	WPA2 Personal
WPA Algorithms	TKIP
WPA Shared Key	••••••••••••••••
Key Renewal Interval (in seconds)	3600 <input type="checkbox"/> Unmask

Physical Interface ath0 SSID [ServerA] HWAddr [00:1C:F0:3C:75:E1]	
Security Mode	WPA2 Enterprise
WPA Algorithms	TKIP
RADIUS Server Address	192, 168, 1, 100
RADIUS Server Port (Default: 1812)	1812
RADIUS Shared Secret	perseo2
Key Renewal Interval (in seconds)	3600

Figura 2-29 Configuración de seguridad WPA 2 en AP

2.7.2 Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con el servicio de *streaming* de audio con mayor y menor desempeño

El tipo de seguridad WPA 2 personal maneja la transición entre puntos de acceso de una forma más estable que WPA personal debido a que se disminuyó el número de paquetes perdidos durante el *roaming*. El envío de paquetes de *streaming* de audio se soporta muy bien con el ancho de banda brindado por el canal inalámbrico. Sin embargo, se puede ver que un tamaño de paquete grande como por ejemplo el uso de Mov+S16l aumenta el tiempo de respuesta casi en el doble del tiempo de respuesta de Mp4+Mp4a, además se puede ver que una transmisión de *streaming* de audio no es tan sensible a la movilidad debido a la capacidad de las bandas de transmisión. Ver Tabla G7 o el estudio completo en el Apéndice G.

Es evidente que al utilizar opciones como TTLS+PAP+TKIP y TLS+TKIP pues se experimenta menos pérdida de paquetes en el momento del *roaming* y los tiempos de autenticación son menores de 1 segundo. El número de eventos necesarios para concluir la transición entre puntos de acceso es crucial en el momento de requerir una estabilidad y sostenimiento de la señal ya que se introduce un valor de tiempo por cada proceso que sea ejecutado luego de iniciar el trascurso de cambio entre puntos de acceso. Ver Tabla G8 o el estudio completo en el Apéndice G.

2.7.3 Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con el servicio de *streaming* de video con mayor y menor desempeño

Al comparar el nivel de fotogramas perdidos obtenidos al usar WPA personal y WPA 2 personal se puede ver que WPA 2 reduce el nivel de pérdidas dándole un buen funcionamiento a la transmisión de video, esta debería ser una razón para elegirla en una

red tipo campus o metropolitana; pero el problema es la tendencia a violar este tipo de seguridad con la abundancia de programas que encuentran la contraseña de conexión en algún tiempo de ejecución. El tiempo de respuesta de los paquetes de ida y vuelta está relacionado con el tamaño y uso del canal inalámbrico de tal manera que una autenticación rápida implica menos pérdidas en el momento de transición de AP. Ver Tabla G9 o el estudio completo en el Apéndice G.

La combinación de seguridad TTLS+PAP+TKIP y TLS+TKIP para el tipo de seguridad WPA 2 muestra que es posible tener un equilibrio entre seguridad y eficiencia, las pérdidas se ven reducidas al igual que el tiempo de autenticación y los fotogramas perdidos, los tiempos de autenticación para los métodos PEAP aumentan bastante y superan los 10 segundos siendo un inconveniente porque incrementa los fotogramas que se están perdiendo a causa de la desconexión. La autenticación causa directamente un incremento en los fotogramas perdidos y en blanco. A pesar que se tiene una configuración de *streaming* de video con buen desempeño, se pierden fotogramas cuando hay movilidad. Ver Tabla G10 o el estudio completo en el Apéndice G.

2.7.4 Estudio y configuración de WPA 2 (personal y empresa usando servidor RADIUS) con el servicio de *streaming* de audio y video con mayor y menor desempeño

La configuración tipo personal no altera demasiado la naturaleza de la transmisión y recepción de *streaming* de audio y *streaming* de video. Puede verse que las pérdidas de fotogramas y *buffers* se presentan en las combinaciones de *streaming* con desempeño deficiente, esta opción de seguridad se ve bastante estable comparada con WPA personal además de mantener valores de retardo o tiempo de respuesta referentes al uso y tránsito en la toda red. Ver Tabla G11 o el estudio completo en el Apéndice G. El uso del método de autenticación TTLS+PAP+TKIP usada con WPA 2 empresa es una buena alternativa en un ambiente de movilidad, la seguridad brindada por una configuración de estas es mejor que utilizar una llave como se hace en WPA 2 personal. Es más robusto en seguridad tener un control de cada cliente móvil, además de la administración necesaria para concluir esta posibilidad. Ver Tabla G12 o el estudio completo en el Apéndice G.

2.7.5 Análisis de resultados y generación de conclusiones

La Tabla 2-12 demuestra que si la transición se hace entre puntos de acceso desconocidos se experimenta un efecto en común visto en cualquiera de las configuraciones de WPA y WPA 2 con un promedio de 40 segundos de intención de reconexión desde el momento en que se ejecutó el algoritmo de *roaming*. Cuando se realiza el cambio entre puntos de acceso desconocidos no es suficiente que se mantenga la misma dirección IP después del cambio, porque se pierde la continuidad de los paquetes y se crea un proceso de espera de los paquetes dejando a la aplicación reproduciendo paquetes en blanco mientras espera la llegada de los paquetes con información. Esto se debe a que la desconexión no se hace de la forma adecuada debido a que la transmisión de datos está sujeta al AP inicial y se presenta una incertidumbre de la trayectoria que seguirá el cliente móvil, no se sabe si se alejara del AP manteniendo su cobertura y cambiara a otro AP. Los 40 segundos de reconexión son la ventana de espera ya establecida en el reproductor de Windows media cuando este valor cambia se debe a una detección de conexión o desconexión (ver estudio completo en el Apéndice F y G).

Tiempo de reconexión de <i>streaming</i> .								
Banda de transmisión	802.11b				802.11g			
Tipo de autenticación	WPA 2 Personal		WPA 2 Empresa		WPA 2 Personal		WPA 2 Empresa	
Tamaño de llave de codificación	10 ASCII	63 ASCII			30 ASCII	50 ASCII		
Combinación de seguridad			TTLS+ CHAP+ TKIP	PEAP+ GTC+ TKIP			TLS+ TKIP	PEAP+ GTC+ TKIP
Tiempo de reconexión con AP desconocido (s)	43	39	40	40	41	41	39	40
Tiempo de reconexión con AP conocido (s)	40	40	40	45	36	29	28	12

Tabla 2-12 Tiempo de reconexión de *streaming* para WPA 2.

Se reduce al máximo el retardo y las pérdidas si se utiliza en 802.11b el tipo de seguridad WPA personal con un tamaño de llave de codificación de 20 ASCII y en 802.11g el tipo de seguridad WPA 2 empresa en la configuración TLS+TKIP.

3 ANÁLISIS DEL ESTÁNDAR IEEE 802.11r

Este es uno de los últimos estándares aprobados por la IEEE, el 15 de julio de 2008, también conocido como transición rápida de BSS (FT, *Fast BSS Transition*) está enfocado en permitir la conexión continua, rápida y segura a estaciones inalámbricas en movimiento. Si un cliente inalámbrico se aleja mucho de su AP y entra en la cobertura de otro AP, el proceso de reconexión puede ser automático, pero toma hasta 500ms dependiendo de la seguridad implementada, debido a esto no es posible un buen desempeño de aplicaciones sensibles al retardo y pérdida de paquetes debido a los cortes tan largos de la comunicación.

El proceso de reconexión puede tardar unos 100 milisegundos, con los actuales métodos y procedimientos, esto sin contar el proceso de autenticación el cual es un punto muy sensible a tratar en las redes actuales y con los nuevos estándares y procedimientos que están diseñados para este fin, como lo es por ejemplo el estándar IEEE 802.11i, si se usa conexiones protegidas el tiempo de reconexión se puede alargar hasta 500ms y mucho más.[21]

Con la implementación de 802.11r lo que se busca es una transición entre distintos puntos de acceso de forma automática, rápida y segura, con un tiempo de reconexión menor de 50 ms incluso menos de 30ms. Esto se logra cuando los clientes establecen con anterioridad la seguridad y la calidad de servicio que quieren usar en el nuevo AP. Lo que hace este nuevo estándar es hacer una sola autenticación inicial cuando por primera vez la estación inalámbrica se une a la red o dominio de movilidad (MD, *Mobility Domain*), una vez se realiza todo el proceso de asociación inicial y si la estación realiza una transición de BSS dentro del mismo MD se utilizan llaves derivadas de la primera asociación y por lo tanto no es necesario repetir el proceso completo.

Para lograr esto de una manera eficiente, 802.11r introduce una nueva jerarquía de llaves, esta se basa en un sistema multinivel donde el dispositivo de mayor rango se encarga de manejar el material de cifrado o llaves principales. Este deriva y pasa llaves a los dispositivos de más bajo rango.

Otro punto a tener en cuenta es que para la calidad de la voz, audio y video en redes inalámbricas se estableció el estándar IEEE 802.11e, con este se logra diferenciar los servicios y de esta manera reservar recursos para los servicios más sensibles, pero cuando se trata de *roaming* los recursos no se reservan antes de la transición. El estándar 802.11r tiene la opción de permitir a los clientes que implementan calidad de servicio (QoS, *Quality of Service*) hacer una petición de recursos al AP destino antes de iniciar la transición.

Como siempre, con este tipo de protocolos, desde que se aprueba hasta que empiezan a aparecer los primeros dispositivos que los usan aún pasará un tiempo, aunque muchos fabricantes de dispositivos inalámbricos como CISCO y ARUBA ya han comenzado el trabajo, más aún, cuando ellos hicieron parte de los equipos que desarrollaron el estándar. Pero para que aplicaciones como la VoIP y videoconferencia, puedan llegar a ser realmente universales se necesitarán, además de estos protocolos que mejoran sustancialmente el desempeño de las redes, que la conectividad Wi-Fi esté presente en todos lados, algo para lo que aún falta camino por recorrer y mucho más en países como Colombia.

Este nuevo estándar introduce dos nuevos protocolos que forman parte del servicio de reasociación y única y exclusivamente se aplican a transiciones entre APs que se encuentran en el mismo dominio de movilidad, es decir, dentro del mismo ESS. Los protocolos FT necesitan intercambiar información durante la asociación inicial, o durante la reasociación, entre la estación y el AP, este primer proceso se llama asociación inicial FT de dominio de movilidad, una vez ya se ha hecho esta asociación, las reasociaciones siguientes dentro del mismo ESS o dominio de movilidad pueden hacer uso de los protocolos FT [12].

Los dos protocolos que se definen son:

- **Protocolo FT:** Este protocolo es usado cuando una estación hace una transición a un AP destino y no requiere o no tiene una petición previa de recursos antes de realizar dicha transición.
- **Protocolo de petición de recursos FT:** Este protocolo a diferencia del anterior realiza peticiones de recursos antes de realizar la transición hacia el AP destino.

Para que una estación pueda usar los protocolos definidos en éste estándar, se debe manejar uno de los dos métodos diseñados para el intercambio de los mensajes, estos tipos son:

- **Sobre el aire (OTA, *Over-the-air*):**
Con este método la estación que va a realizar la transición se comunica directamente con el AP destino usando autenticación 802.11 con el algoritmo de autenticación FT.
- **Sobre el sistema de distribución (OTDS, *Over-the-DS*)**
Mediante este método la estación se comunica con el AP destino, a través del actual AP en el cual está asociado. La comunicación entre la estación móvil (STA, *Station*) y el AP actual es transportada mediante tramas de acción FT. Luego la comunicación entre el AP actual y el AP destino se realiza con un método de encapsulación descrito en el anexo A. El AP actual convierte entre las 2 encapsulaciones.

3.1 COMPARACIÓN DE LOS PROCESOS DE ROAMING CON Y SIN 802.11r

Para ver de una manera más práctica los aportes del estándar 802.11r al proceso de *roaming* en 802.11, a continuación se hace la comparación de los procesos que se llevan a cabo durante el *roaming* en el caso que se implementa seguridad WPA 2, ya que este es el caso al que se refiere el estándar 802.11r. En la mayoría de estudios revisados [7][13][14] el tiempo de *roaming* va desde el momento en que se empieza la búsqueda de nuevos APs a través del envío de tramas *probe request* para luego seguir con la autenticación y asociación en el nuevo AP. Sin embargo, en el presente estudio el *roaming* se mide como el tiempo que va desde el momento que el algoritmo de *roaming* decide desconectarse del AP actual y conectarse a un nuevo AP, es decir desde la petición de autenticación, pasando por la reasociación y luego por la autenticación 802.11x terminando con el intercambio o instalación de las llaves de cifrado tanto en el AP como en la STA. La manera exacta como el algoritmo toma la decisión de hacer la transición a otro AP es totalmente un secreto que guarda cada fabricante [15] [16] [17], motivo que puede causar problemas de interoperación, pero que a la vez genera una competencia que puede ayudar a generar mejores algoritmos de decisión de *roaming*. También para la presente comparación se debe tener en cuenta que se hace cuando se realiza el *roaming* por primera vez hacia un AP, es decir que no se puede implementar los mecanismos de

preautenticación y cacheo¹⁷ de llaves.

En la Figura 3-1 se aprecia el proceso de *roaming* normal en el cual se está implementando WPA 2 de forma general. A partir de la figura 3-1 se procede a dividir el proceso de *roaming* en 3 partes. La primera fase es de la autenticación sencilla 802.11, es decir, la de que se hace con sistema abierto, en esta fase también se incluye la asociación al AP, la cual incluye los paquetes de petición de asociación por parte de la STA y la respuesta de asociación desde el AP. La fase dos tiene que ver con el sistema de autenticación 802.1x, esta es la parte más sensible del proceso y es de las que más contribuye con el retardo del *roaming*, aquí el retardo depende del tipo de EAP[18] usado y también en parte de la red que se tiene en el sistema de distribución, ya que es por aquí por donde se intercambian los mensajes con el servidor de autenticación. Y por último la fase que se identifica es la del saludo de cuatro vías en el que se intercambian e instalan las llaves de cifrado tanto en el AP como en la STA.

Como se ve en la Figura 3-1 el proceso de *roaming* conlleva varios procesos cuando se está implementando 802.11i, y de esta forma se generan retardos muy grandes en tiempo, con lo cual se ven afectadas las aplicaciones sensibles a la pérdida de paquetes. Seguidamente se analizan los pasos o procedimientos del nuevo estándar IEEE 802.11r para de esta manera ver el aporte real del estándar a los retardos involucrados en el proceso de *roaming*. En el caso del estándar 802.11r, se analiza el tipo ODS, con el cual se hace el intercambio de paquetes con el AP destino a través del AP actual y utilizando el DS.

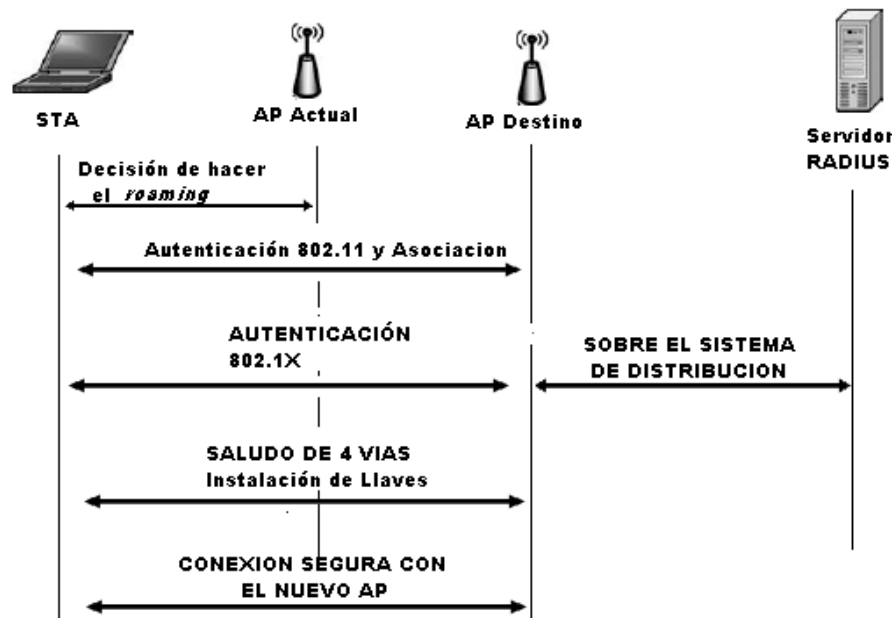


Figura 3-1 Proceso de *roaming* en 802.11i (WPA 2).

La Figura 3-2 muestra el proceso mediante el cual se hace *roaming* implementando el nuevo estándar 802.11r (ver Anexo 1).

¹⁷ Cacheo se refiere a una técnica en la cual se almacenan las llaves de cifrado para ser usadas posteriormente.

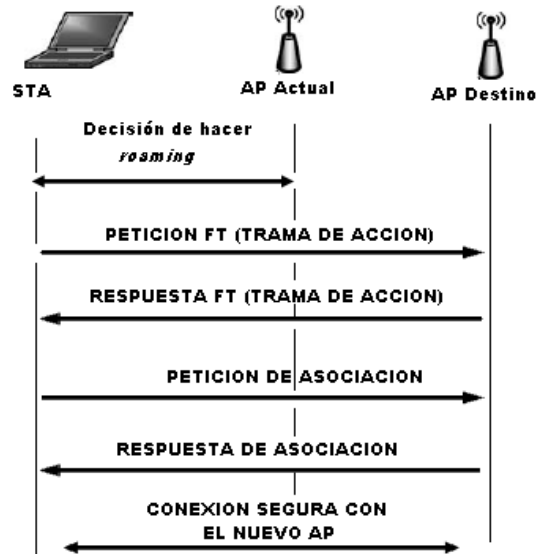


Figura 3-2 Proceso de *roaming* con 802.11r.

Como se aprecia en las Figuras 3-1 y 3-2, se puede ver la diferencia en el número de mensajes intercambiados en el momento de *roaming*. Aquí ya hay una diferencia con la cual se reduce el retardo. También otro factor con el que se reducen los retardos durante el *roaming* es que no hay la necesidad de intercambiar mensajes con el servidor de autenticación. El estándar IEEE 802.11r reduce todo el proceso de *roaming* a cuatro mensajes que se intercambian con el AP destino a través del AP actual, con estos 4 mensajes se realiza la autenticación y asociación 802.11 así como la gestión de llaves para el cifrado WPA2. Para mayor información acerca del funcionamiento del estándar 802.11r ver Anexo A.

A continuación se presenta una comparación teórica entre la solución propuesta en el estándar IEEE 802.11r y la experiencia obtenida en las pruebas del segundo capítulo, esto se hace a través de la revisión de los puntos que se tomaron como factores críticos en el concepto del *roaming* y se confrontan con lo que el nuevo estándar IEEE 802.11r propone.

- **Ancho de banda**

Cuando hay *roaming* se pierden paquetes esto se debe a que el ancho de banda disponible es mucho menor debido a la utilización que hace de él los servicios de *streaming* se pierden muchos paquetes más de los normales. Es aquí donde 802.11r desempeña un papel fundamental al disminuir el número de paquetes a intercambiar para la autenticación y el intercambio de llaves durante el proceso de *roaming* ya que se supondría que las posibilidades de que estos paquetes lleguen de forma exitosa son mucho mayores lo cual llevaría a una mejoría en este aspecto del ancho de banda.

- **Búsqueda**

En lo concerniente a la búsqueda realizada por la estación antes de realizar una transición, no hay cambios ya que la estación realiza los mismos procedimientos para buscar un AP destino y para tomar la decisión de hacer la transición. El estándar 802.11r se centra en el proceso que viene luego de que ya se ha elegido un AP hacia el cual realizar la transición.

- Seguridad

La información contenida en las tablas 3-1, 3-2, 3-3 y 3-4 compara los tiempos encontrados en la experimentación (ver Apéndice E), con el tiempo ofrecido por el estándar 802.11r [21].

Característica	802.11g WPA Empresa	802.11g WPA Personal	802.11g WPA 2 Empresa	802.11g WPA 2 Personal
Combinación de seguridad	TLS+TKIP	20 ASCII + TKIP	TLS + TKIP	50 ASCII + TKIP
Autenticación 802.1X (Completa ms)	630	15,5	488,5	6,5
IEEE 802.11r (ms)	50[21]			

Tabla 3-1 Tiempos de *roaming* sin *streaming* en 802.11g.

Característica	802.11g WPA Empresa	802.11g WPA Personal	802.11g WPA 2 Empresa	802.11g WPA 2 Personal
Combinación de seguridad	TLS + TKIP	20 ASCII + TKIP	TLS +TKIP	50 ASCII + TKIP
Autenticación 802.1X (Completa - ms)	691,5	65,5	291	159,5
Autenticación 802.1x AP conocido (ms)	174,4	167,3	278	23,8
Diferencia de los tiempos (ms)	517,1	101,8	13	135,7
IEEE 802.11r (ms)	50 [21]			

Tabla 3-2 Tiempos de *roaming* con *streaming* en 802.11g.

Característica	802.11b WPA Empresa	802.11b WPA Personal	802.11b WPA 2 Empresa	802.11b WPA 2 Personal
Combinación de seguridad	TTLS+ PAP +TKIP	30 ASCII + TKIP	TTLS + CHAP + TKIP	63 ASCII + TKIP
Autenticación 802.1X (Completa ms)	635	11	839	53
IEEE 802.11r (ms)	50 [21]			

Tabla 3-3 Tiempos de *roaming* sin *streaming* en 802.11b.

Característica	802.11b WPA Empresa	802.11b WPA Personal	802.11b WPA 2 Empresa	802.11b WPA 2 Personal
Combinación de seguridad	TTLS + PAP + TKIP	30 ASCII + TKIP	TTLS + CHAP + TKIP	63 ASCII + TKIP
Autenticación 802.1X (Completa - ms)	1146,5	35	364	173,5
Autenticación 802.1x AP conocido (ms)	717	598	4,3	33,8
Diferencia de los tiempos(ms)	429,5	563	359,7	139,7
IEEE 802.11r(ms)	50[21]			

Tabla 3-4 Tiempos de *roaming* con *streaming* en 802.11b.

Característica	Empresa		Personal		IEEE 802.11r
	WPA	WPA 2	WPA	WPA 2	
Tiempo de búsqueda	Igual	Igual	Igual	Igual	Igual
Seguridad	Alta	Alta	Baja	Media	Alta (Existe una vulnerabilidad en el intercambio de llaves entre APs a través del DS durante el proceso de <i>roaming</i>)
Desasociación y desautenticación	Se hace antes de comenzar el proceso de autenticación.				Se hace después de terminar el proceso de autenticación, es el último paso de la autenticación.
Reasociación	Se hace luego de aprobada la reautenticación.				Igual
Transporte de datos durante el <i>roaming</i>	Hay pérdidas por la desconexión temporal que sucede en el proceso de reconexión al nuevo AP.				Pérdidas mucho menores debido a la reducción del tiempo de desconexión-conexión.
Movilidad	Algoritmo de ejecución del <i>roaming</i> presente en todo momento.				Igual
Ancho de Banda	Igual (Cuando hay más ancho de banda habrá más probabilidad de autenticación exitosa)				Un poco más debido al número menor de eventos en el <i>roaming</i> .
Número de eventos en <i>roaming</i> (AP Desconocido)	Dependiendo de la certificación de 8 a 12		4 Eventos		2 eventos
Número de eventos en <i>roaming</i> (AP Conocido)	4 eventos		4 eventos		2 eventos
Tiempo de autenticación. (AP desconocido ms)	883	742	56	35	50[21]
Tiempo de autentic. (AP conocido ms)	35	288	250	5	

Tabla 3-5 Comparación de diferentes aspectos de 802.11 con 802.11r.

4 RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE UNA RED SEGURA Y DE CALIDAD PARA EL *STREAMING*

Las recomendaciones para encontrar un equilibrio entre seguridad, *streaming* y *roaming* se obtuvieron por medio de un conjunto sólido de pruebas experimentales realizadas para evaluar el impacto presentado en una transmisión de *streaming* en cuanto a retardo y pérdida de paquetes al implementar soluciones WPA y WPA 2 en la topología inalámbrica ESS para 802.11b/g.

4.1 RECOMENDACIONES DE DISEÑO PARA LA TOPOLOGÍAS ESS EN REDES 802.11b/g

Todo diseño de arquitectura de red inicia con un análisis previo el cual estudia el número de clientes soportados, estructura lógica y física tanto del cliente como del proveedor de servicios, en este caso se han definido el tipo de topología que se utilizará y el ambiente en el que los clientes interactuarán. Ver sección 2.3.

4.1.1 Análisis previo

El análisis se centra en el establecimiento de una red inalámbrica ESS, la topología es simple, varios puntos de acceso unidos por una red de distribución con características de movilidad y *roaming*. Los estudios realizados muestran que un cliente pierde menos paquetes cuando se desplaza por las coberturas inalámbricas con una velocidad baja, por ejemplo 1 metro cada 8 segundos la cual es la velocidad que dio mejores resultados entre entendimiento lógico de la información consultada por el cliente móvil y la pérdida de paquetes. Lo principal para el montaje a realizar es la ubicación de los puntos de acceso.

⊕ Alcance

Como alcance se refiere a la ubicación y cobertura de los puntos de acceso. Es importante tener en cuenta que el 25% de cobertura continua es la mejor cobertura y la que más equilibrio presenta para las bandas de transmisión de 802.11b y 802.11g. Normalmente la intención de un administrador de red es cubrir la mayor área de servicio posible, por consiguiente, se debe encontrar la distancia de separación entre puntos de acceso correspondiente al porcentaje de cobertura continua del 25%. Para lograr esta cobertura se pueden seguir los siguientes pasos:

- 1) Se configura la potencia de transmisión en los puntos de acceso.
- 2) Se mide la distancia de la cobertura que se alcanza con la potencia anterior.
- 3) Utilizando como modelo la figura 2-3 de la sección 2.2.2, se ubica en la regla superior el doble de la distancia obtenida y se procede a seleccionar en la parte inferior el porcentaje de cobertura continua deseado moviendo el AP de la izquierda a 25%, con lo cual obtenemos su correspondiente en distancia en la parte superior donde se puso el valor de la distancia.

La Figura 4-1 demuestra cómo se relacionan la distancia y el porcentaje de cobertura continua. El caso de estudio mostrado en la figura hace referencia al 5% de cobertura continua que señala 34,2 metros de separación entre los puntos de acceso, el uso de las reglas como método de relación entre distancia y cobertura continua fue creado y utilizado

por el grupo de desarrollo del presente proyecto para la búsqueda de la mejor ubicación de los APs para obtener el mejor desempeño.

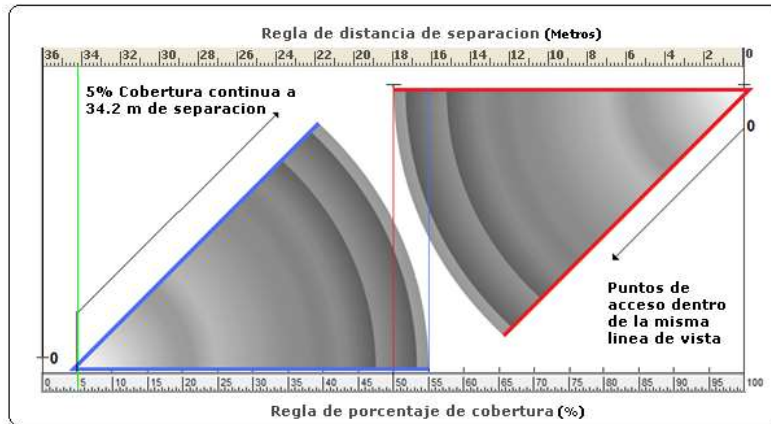


Figura 4-1 Referencia entre distancia y cobertura continua.

⊕ Construcción

Luego de obtener la distancia entre puntos de acceso correspondiente al 25% de cobertura continua sugerida o el porcentaje deseado por el administrador, se procede a la ubicación física utilizando cable UTP categoría 5E cruzado entre puntos de acceso y el *switch* de distribución. El cable UTP categoría 5E directo es usado para la conexión de servidores o equipos adicionales con el *switch* de distribución. Teniendo en cuenta la distancia entre puntos de acceso y la ubicación física se puede dar soporte a un trayecto concurrencido o un área amplia. El diseño puede necesitar más de 2 puntos de acceso, para tener menos problemas de interferencias se intercalan los canales de transmisión [22] como presenta la Figura 4-2.

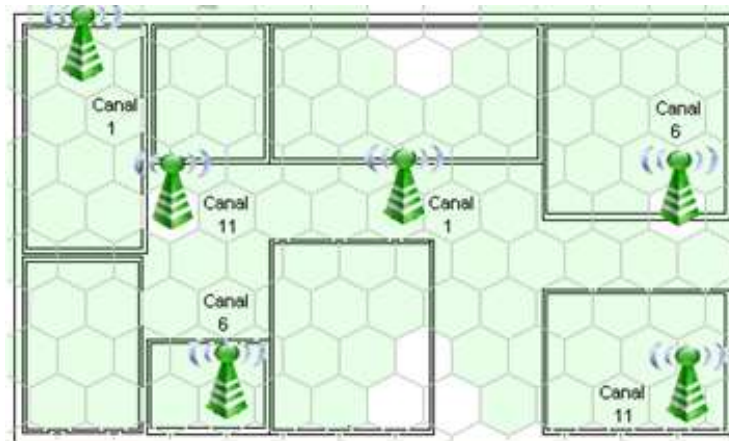


Figura 4-2 Estructura de canales para el diseño.

Hay que tener en cuenta de no exceder la distancia de 100 metros entre el *switch* y el AP. En caso de sobrepasar la distancia es mejor redistribuir los APS y el *switch* para mantener siempre el mejor ancho de banda debido a que se presentan degradaciones de la señal al sobrepasar esta longitud de 100m.

⊕ **Software y protocolos**

Es recomendable el uso de una aplicación controladora propietaria para la tarjeta de red inalámbrica del cliente móvil. La posibilidad de certificación y autenticación son mayores que al utilizar Windows como herramienta de gestión inalámbrica. El *software* controlador de los APs puede ser modificado a versiones mucho mejores con opciones especiales de administración y calidad de servicio. Hay muchos equipos que se puede actualizar con el firmware DD-WRT v24 RC-4 (10/10/07) el cual fue probado y utilizado con excelentes resultados. El servidor RADIUS y el servidor DHCP pueden estar en una distribución Linux como Opensuse 10.2, con los paquetes Freeradius y Dhcpd. La red inalámbrica es el medio de comunicación por esta razón los protocolos son los referentes a una red de este tipo.

⊕ **Equipos**

Los equipos de la marca D-Link son muy gestionables. En este caso se pueden utilizar los equipos de red inalámbrica D-Link dir-300 y el *Switch* D-Link de 8 puertos Ethernet. Para manejar las direcciones IP dinámicamente es necesario usar un servidor DHCP dedicado a esa labor, en este caso se puede utilizar un *Router* Billion el cual es fácil de configurar. Los equipos para la autenticación RADIUS pueden ser computadores básicos que soporten la instalación y ejecución de la distribución Linux, es aconsejable que todos los APs a utilizar sean del mismo fabricante para mayor compatibilidad.

⊕ **Configuración**

El objetivo de configurar una red inalámbrica en topología ESS es brindar movilidad y transparencia, por esta razón hay algunos lineamientos que se deben seguir:

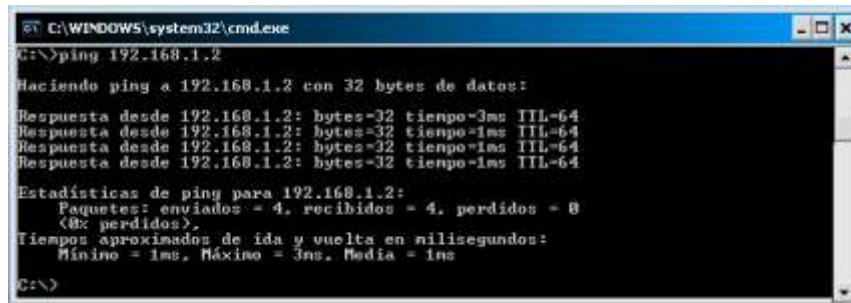
- 1) La elección del SSID radiado por los puntos de acceso.
- 2) La elección del mecanismo de seguridad (consultar de la Tabla 4-1).
- 3) Configurar la potencia y el estándar según el diseño e implementación deseados (consultar de las Tablas 4-2 y 4-4).

Se recomienda que el servidor DHCP sea independiente y centralizado con respecto a la red de distribución ya sea un equipo físico como un *router* o un paquete configurado en una distribución Linux, esto es para liberar a los puntos de acceso de procesos y que su carga sea netamente de sostenimiento de los clientes móviles. Los equipos inalámbricos, servidor DHCP y servidor RADIUS son configurados de forma estática con una dirección IP clase C 192.168.1.x, la elección de la dirección IP depende del número de usuarios y equipos que vaya a soportar la topología diseñada; el servidor DHCP puede entregar direcciones IP desde la 192.168.1.100 en adelante para tener direcciones disponibles en caso de agregar un nuevo AP.

La configuración de seguridad debe ser la misma en todos los puntos de acceso para que prime el sentido de transparencia, si se utiliza la opción de empresa hay que tener la información del servidor RADIUS y si se utiliza la opción de personal se recomienda tener la misma contraseña configurada en todos los puntos de acceso.

4.1.2 Pruebas y verificación

La verificación se hace por medio de una prueba de ping entre clientes móviles o de un cliente móvil a un AP. Con una respuesta satisfactoria se verifica la correcta instalación y configuración de toda la red ESS.



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:

Respuesta desde 192.168.1.2: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 3ms, Media = 1ms

C:\>
```

Figura 4-3 Verificación de conectividad.

4.2 RECOMENDACIONES PARA EQUILIBRAR LA IMPLEMENTACIÓN ENTRE SEGURIDAD Y *STREAMING* EN UNA TOPOLOGÍA ESS PARA REDES 802.11b/g

Aquí se describe la implementación de seguridad con diferentes combinaciones de autenticación alcanzadas por el servidor RADIUS y la implementación de diferentes combinaciones de *streaming* de audio y video como servicio de comunicación multimedia; es obligatorio que la topología ESS esté previamente ajustada y probada para percibir el desempeño de la autenticación y el servicio de *streaming* de audio y video. Cada implementación se sugiere por equilibrio y por sus mejores resultados en la experimentación realizada, ver capítulo 2.

4.2.1 Implementación de seguridad

En esta etapa se implementan métodos que evitan los intrusos y prácticas dañinas sobre la red inalámbrica teniendo en cuenta la continuidad de las aplicaciones ejecutadas en el momento del *roaming*. Después de ser instalado y configurado el servidor RADIUS se ingresa la dirección IP estática en el campo de direccionamiento en la parte de red en la distribución Linux; este dato es importante ya que se necesita saberlo para la configuración de la sección de seguridad empresa de los APs y también se necesita en el archivo `clients.conf` el cual está presente en la carpeta del servidor RADIUS. Se debe incluir la información de cada AP con su dirección, nombre y llave compartida secreta (ver información completa en el capítulo 2 y Apéndice D).

El procedimiento para la elección de seguridad sería el siguiente: el administrador de la red inalámbrica estudia los recursos que posee para configurar la seguridad dentro de su perímetro, lo primero en buscar es un servidor de autenticación RADIUS ejecutado sobre una distribución Linux, de esta forma se dividen las posibilidades en las opciones personal y empresa, luego el administrador estudia la posibilidad de que los clientes y los equipos inalámbricos tengan la opción de WPA 2 multiplicando las posibilidades a 4, WPA (personal y empresa) y WPA 2 (personal y empresa). Ahora el administrador debe tomar la decisión de la tecnología de transmisión a utilizar, seleccionando 802.11b o 802.11g, dando como resultado final 8 opciones de seguridad.

La Tabla 4-1 simplifica lo encontrado en las experimentaciones y muestra las combinaciones óptimas de seguridad que un administrador dependiendo de sus recursos puede escoger para obtener los mejores resultados en pérdida de paquetes, retardo y prevención contra usuarios malintencionados dando potencialidad a las aplicaciones en tiempo real. Estos resultados traen implícitas las mejoras del procesamiento al *streaming* durante la movilidad y el *roaming*.

Combinaciones óptimas de seguridad para <i>streaming</i> .				
Banda de transmisión	Tipo de autenticación de red			
	Personal		Empresa	
	WPA	WPA 2	WPA	WPA 2
802.11g	20 ASCII + TKIP	50 ASCII + TKIP	TLS+TKIP*	TLS+TKIP*
802.11b	30 ASCII + TKIP	63 ASCII + TKIP	TTLS + PAP + TKIP*	TTLS + CHAP + TKIP*

***Identidad de movilidad = Dominio/Usuario, con certificación, sin validación.**

Tabla 4-1 Combinaciones óptimas de seguridad.

De los estudios del Apéndice C resultan las Tablas 2-4, 2-5, 4-1 y 4-2, de éstas se dedujo que 802.11b es más tolerante al retardo y pérdida de paquetes, esto se debe al ancho de banda de cada una de las tecnologías mencionadas. Se recomienda escoger el *streaming* que se desea usar antes de escoger la tecnología a usar. En una transmisión de *streaming* la velocidad de bits se conoce como la cantidad de bits extraída de los medios y que es enviado cada segundo por la red. Si la velocidad es demasiado grande no habrá buena sincronización entre recepción y reproducción causando la desconexión o reintento de conexión (Ver Tablas F8 y F9 del Apéndice F), por esta razón se elije primero la calidad del *streaming* que se usará para luego configurar la banda de transmisión. En la tabla 4-2 se puede ver la tolerancia al retardo y pérdida de paquetes y el ancho de banda de las dos tecnologías evaluadas en este estudio.

Tolerancia a retardo y pérdida de paquetes.		
Banda de transmisión	Tolerancia.	Velocidad
802.11g	Media	54 Mbps
802.11b	Alto	11Mbps

Tabla 4-2 Tolerancia a retardo y perdida de paquetes para 802.11b/g.

Los resultados de la Tabla 4-3 son el tiempo promedio que se obtuvo al medir el proceso de los eventos de autenticación para todas las combinaciones de certificación cuando se configura el tipo empresa y una serie de tamaños de llave de codificación cuando se configura personal, ver configuraciones utilizadas en la Tabla 4-1. Se puede observar en la Tabla 4-3 la diferencia de 0,093 segundos entre WPA o WPA 2, realmente se podría deducir que la elección de cualquiera de las dos sería muy similar, pero eso no es del todo cierto, aunque los valores generales WPA y WPA 2 son muy cercanos entre sí, individualmente el tiempo de autenticación se reduce dependiendo del método utilizado para la autenticación ya sea personal o empresa, además de evidenciar que el tipo autenticación personal muestra en su gran mayoría tiempos más bajos que el tipo de autenticación empresa del orden de milisegundos. 802.11g logra valores de tiempo de autenticación menores que 802.11b debido al ancho de banda utilizado, esta guía es importante para autenticaciones estáticas en donde el cliente no se desplaza.

Tiempo promedio de autenticación sin <i>roaming</i>				
Banda de transmisión	Tipo de autenticación de red			
	WPA (s)		WPA 2(s)	
	Personal	Empresa	Personal	Empresa
802.11g	2,4208	2,9814	2,5402	2,9331
802.11b	2,8555	2,7893	2,8411	3,1046
Tiempo promedio (s)	2,76175		2,85475	

Tabla 4-3 Tiempo promedio de autenticación sin *roaming* para 802.11b/g.

Para encontrar los tiempos promedio de autenticación en *roaming* de la Tabla 4-4 fue necesario encontrar las mejores opciones de certificación, tamaño de llave de codificación las cuales se pusieron a prueba en el *roaming*. Todo este estudio se puede apreciar en las Tablas E6 y E7 del Apéndice E. La Tabla 4-4 señala una diferencia de 0,025 segundos entre WPA y WPA 2, de igual forma se ve que la autenticación en el momento del *roaming* se reduce si se utiliza el tipo de autenticación personal y se reduce más usando 802.11g.

Tiempo promedio de autenticación en <i>roaming</i>				
Banda de transmisión	Tipo de autenticación de red			
	WPA (s)		WPA 2 (s)	
	Personal	Empresa	Personal	Empresa
802.11g	0,0163	0,6305	0,0069	0,4892
802.11b	0,0116	0,6306	0,0535	0,8392
Tiempo promedio	0,3222		0,3472	

Tabla 4-4 Tiempo promedio de autenticación con *roaming* para 802.11b/g.

Cuando lo que se quiere es mantener un nivel de seguridad máximo junto con el mayor desempeño de la red conservando la accesibilidad y flexibilidad para el cliente. En el Apéndice E se encuentra un estudio muy importante, éste prueba el uso de TKIP y AES en cuanto a velocidad de autenticación con diferentes métodos de autenticación. La gran presencia de reducción en tiempo utilizando la codificación de datos TKIP concluye que es mejor su implementación al pensar en velocidad de conexión en un momento de *roaming*. La combinación de seguridad óptima sería WPA 2 en 802.11g con una autenticación TLS+TKIP, más la certificación de cliente frente a un servidor RADIUS sin validación¹⁸; el uso de la validación en una configuración de red inalámbrica agrega un más seguridad con lo cual a su vez se aumenta el tiempo de autenticación. La razón de la elección de TLS+TKIP se debe a una serie de pruebas concentradas en el Apéndice E donde se encontró que presentaba tiempos reducidos de autenticación, bajo promedio de pérdida de paquetes y latencia para el *streaming* de audio y video. Si lo que se desea es mantener un nivel de seguridad medio pero con máxima eficiencia por parte de las aplicaciones multimedia se debe tomar como combinación de seguridad WPA personal en 802.11b con un tamaño de llave de codificación de 20 ASCII + TKIP. La razón de la elección es porque se obtuvo una máxima tolerancia a la movilidad y al *roaming*. La Figura 4-4 presenta los campos de elección de información más importantes.

3.1.1 Implementación de *streaming* de audio y video soportada por VLC

La implementación de un servidor de *streaming* dentro de una red inalámbrica en la topología ESS está ligada a factores externos y de configuración de la aplicación tanto en el servidor como en el cliente. Los aspectos a tomar en cuenta son la seguridad, movilidad, problemas de conexión y mala configuración o elección errónea de la forma como se maneja la información multimedia. Las recomendaciones se concentran en la designación de la combinación óptima de métodos de encapsulamiento y codificadores/decodificadores para *streaming* de audio y video. La aplicación que se seleccionó para las experimentaciones de *streaming* fue VLC. Ver información completa en el capítulo 2 y el Apéndice D.

¹⁸ La validación es una autenticación adicional que consiste en la verificación del nombre de red del servidor escrito por el cliente en la configuración inalámbrica.

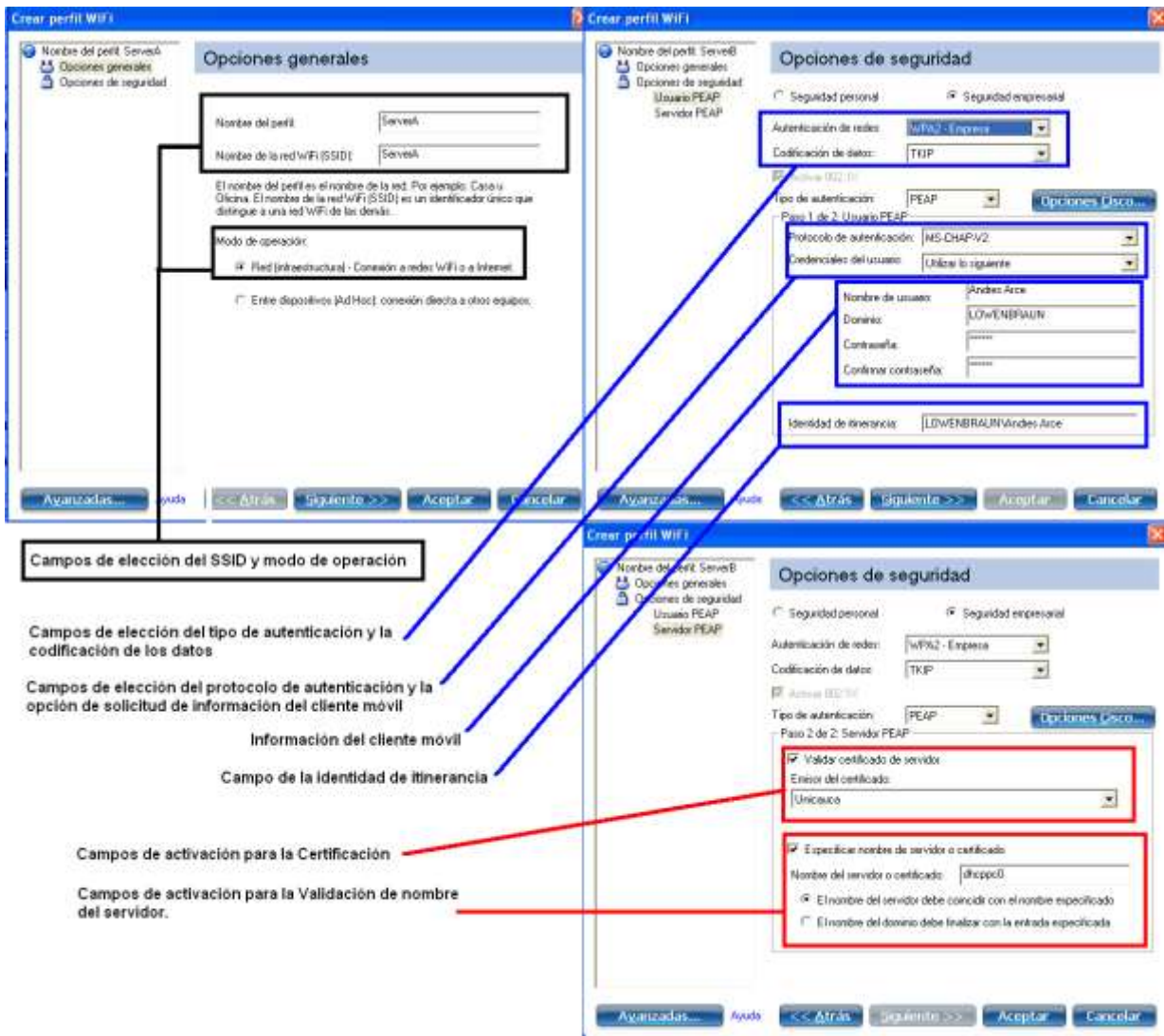


Figura 4-4 Campos de información para configuración de 802.11b/g.

Es importante complementar la información de transmisión de *streaming* con el Apéndice F el cual presenta la pérdida de paquetes y el retardo al implementar configuraciones de seguridad demasiado robustas en cuanto a limitación de recursos y rechazo de intrusos. El servidor de *streaming* VLC tiene opciones configurables en cuanto a codificador/decodificador de audio, codificador/decodificador de video, métodos de encapsulamiento y medios de transporte, estos medios de transporte pueden ser orientados a conexión a través de TCP/IP como HTTP y MMSH, también medios de transmisión no orientados a conexión a través de UDP/IP como RTP y UDP. En este caso las transmisiones de *streaming* son orientadas a conexión utilizando MMSH, debido a que primero se establece la conexión entre el cliente y el servidor por medio de una sincronización para luego enviar los paquetes y de esta manera haciendo más confiable la transmisión.

Para la sugerencia de los métodos de encapsulamiento y la codificación se tomaron todas las opciones encontradas en el servidor de *streaming* VLC y se pusieron a prueba para luego elegir las de desempeño óptimo y desempeño deficiente como comparación frente a cambios ocurridos a causa de la autenticación, la movilidad o el *roaming*.

Las pérdidas de *buffer* de audio, fotogramas de video y fotogramas en blanco se pueden reducir si se utilizan codificadores/decodificadores para la preparación y reducción del tamaño de los paquetes enviados, el uso de la banda de transmisión también afecta al *streaming*.

Pérdidas en <i>streaming</i> durante el <i>roaming</i> .						
Banda de transmisión	Característica	Audio	Video	Audio y video		
	Método de encapsulamiento	Mp4	Mp4	Asf	Asf	Mp4
	Codificación	Mpa4	Div3	---	Mp4a+Div3	Mp4a+Div3
802.11g (Tasa de bit de audio de 512Kbps y video de 3Mbps)		0	*(0+32 74)	*(47+1117)+ 284	*(0+254)+0	*(0+238)+0
802.11b (Tasa de bit de audio de 256Kbps y video de 2Mbps)		0	*(0+10 56)	*(90+2251)+ 555	*(0+238)+0	*(0+235)+0
* (Fotogramas perdidos + fotogramas en blanco) + buffers perdidos.						

Tabla 4-5 Pérdidas en *streaming* durante el *roaming* para 802.11b/g.

La Tabla 4-5 presenta el trabajo realizado con las combinaciones óptimas de *streaming* de audio y video puestas a prueba durante el *roaming*, las cuales obtuvieron los valores más bajos en pérdidas, alta tolerancia a la movilidad y al *roaming*, el tamaño de los *buffers* de audio son pequeños y pueden ser emitidos por los anchos de banda de 802.11b/g sin desarrollar pérdidas durante su funcionamiento, sin embargo, se sugiere la utilización de Mp4 + Mp4a para la transmisión de audio sobre una red inalámbrica en topología ESS con el servicio de *roaming* y no se sugiere el uso de Mov + S16l ni la codificación A52 pues su desempeño sobre la red inalámbrica es deficiente.

El *streaming* de video contiene los fotogramas en blanco que son los reproducidos cuando no se tiene bloques de video recibidos o mientras se sincroniza la recepción de paquetes, los fotogramas perdidos por la falta de sincronización de los paquetes recibidos y los fotogramas perdidos en el transporte desde el servidor al usuario final. El tiempo de sincronización dura un promedio de 7 segundos y la suma de fotogramas perdidos y en blanco es mínima cuando se utiliza la combinación de Mp4 + Div3 y no se sugiere el uso de Mov + Mp2v debido a su mal desempeño sobre la red inalámbrica,

El uso de codificación es vital cuando se tiene un ancho de banda limitado, se puede ver claramente que el nivel de pérdidas en audio y video se reduce cuando se integra la opción de codificación a tal punto de no tener pérdidas durante la movilidad y *roaming*, por eso aunque se tenga un método de encapsulamiento es mejor combinarlo con su correspondiente codificación en audio y video, se sugiere Mp4+Mp4a+Div3 por su estabilidad y por su rápida sincronización de paquetes entre cliente, servidor y no se recomienda el uso de Mov + S16l + Mp2v ni Mpeg-Ts + S16l +Mp2v. La velocidad de transmisión de *streaming* tiene variables influyentes como la autenticación y el *roaming* que pueden en su momento causar retardos y pérdida de paquetes en la transmisión y la recepción del *streaming*. El ancho de banda utilizado por el *streaming* será disminuido si se utiliza la combinación adecuada de codificador/decodificador y encapsulamiento, de esta manera permitiendo la carga rápida de *buffers* y fotogramas manteniendo la continuidad en la reproducción.

3.1.2 Implementación de *roaming*

La implementación de *roaming* en la red inalámbrica en topología ESS no es compleja, la emisión de los SSID es mejor que sea igual dentro de toda la red para que el cliente se sienta cubierto por un único AP y no existan confusiones, además, el establecimiento de nombres de SSID por cada punto de acceso causa la preconfiguración de cada perfil de conexión, si el cliente no ha configurado todos los SSID entonces en el momento del *roaming* tendrá problemas de accesibilidad si se tiene implementado la característica de seguridad. El servidor DHCP es mejor que sea independiente de los puntos de acceso para conservar un solo direccionamiento en toda la red, así no se tendrán problemas con direcciones IP duplicadas en el proceso de *roaming* y será más fácil encontrar errores si se presentan. Si la red diseñada es extensa es preciso mantener el *roaming* en la capa 2 o en un mismo dominio, pues el uso de equipos de enrutamiento de capa 3 introduce retardos adicionales en el momento del *roaming*, los cuales pueden ser reducidos configurando políticas de calidad de servicio.

La Figura 4-5 describe el proceso de *roaming* dentro de una red inalámbrica en topología ESS. Cuando el usuario móvil se transfiere a un nuevo AP el tráfico es detenido y se ejecuta el evento de *roaming*, se desautentica y desasocia del AP inicial y empieza una nueva autenticación, si es aceptada se procede a la asociación y recepción de tráfico, si la autenticación no es válida por algún motivo el AP limita al cliente de recursos y sigue intentando la autenticación.

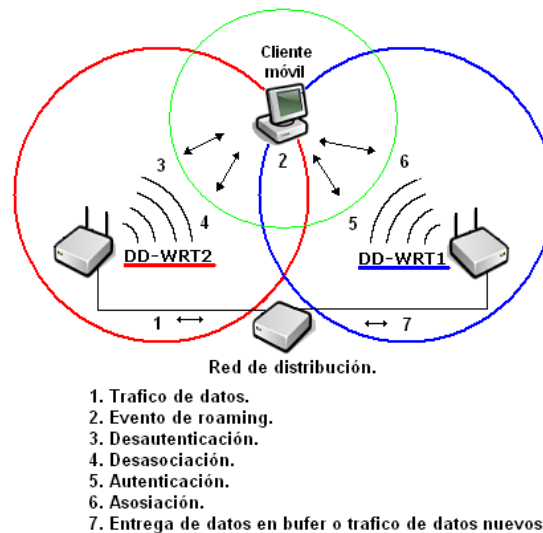


Figura 4-5 Proceso de *roaming* en la experimentación.

Dentro de la configuración avanzada del dispositivo inalámbrico del cliente móvil se localiza la opción de agresividad de la itinerancia o intensidad de movilidad la cual determina la ejecución de cambio de AP. Esta característica siempre se encuentra en predeterminado o medio, pero configurándola en mínimo se obtienen mejores resultados disminuyendo el promedio de paquetes perdidos, en la experimentación se encontraron las curvas de decisión de *roaming* para las bandas de transmisión de 802.11b y 802.11g.

CONCLUSIONES Y RECOMENDACIONES

- Desarrollada la lista de actividades satisfactoriamente y sobrellevadas las innumerables dificultades para ejecutar toda la experimentación, se encontraron resultados que permitieron ser la guía hacia la generación de recomendaciones para la implementación de una topología ESS con funcionamiento de *roaming*. El uso de *streaming* dentro de redes inalámbricas es un servicio que se impone debido al surgimiento y la necesidad de comunicación y diversión; realmente seguir las recomendaciones propuestas en este documento es basarse en un estudio estricto y completo el cual permitirá el diseño y configuración del servicio de *streaming* en topologías ESS para 802.11b/g. Las recomendaciones propuestas pueden ser la base para la creación o formulación de nuevos proyectos debido al esfuerzo reflejado en su proceso de sustentación.
- Se encontraron combinaciones óptimas sugeridas en la sección 4.2.1 y 4.2.2 para la configuración de *streaming* y mecanismos de seguridad para mantener el equilibrio entre eficiencia, retardo, pérdida de paquetes y seguridad.

Las siguientes afirmaciones se apoyan en los Apéndices B al Apéndice G.

- En WPA personal el tiempo de *roaming* es mayor cuando se hace hacia un AP desconocido que cuando se hace hacia un AP conocido, con esto se corrobora que como WPA no maneja la técnica de preautenticación y precacheo de llaves entonces no influye en el tiempo de transición si el AP es conocido o desconocido.
- Con WPA 2 personal el tiempo es menor cuando se hace la transición a un AP conocido con lo cual se comprueba la utilidad de la preautenticación y el cacheo de llaves.
- WPA 2 personal ofrece el mejor tiempo siempre cuando la transición se realiza hacia un AP conocido.
- WPA y WPA 2 personal siempre ofrece el menor tiempo de *roaming* que el tipo empresarial.
- En WPA personal tanto en 802.11b como en 802.11g, el tiempo es menor cuando el AP es desconocido, algo que al parecer no es normal, pero después del análisis teórico se puede concluir que es lo esperado ya que WPA no cuenta con las técnicas de preautenticación y cacheo de llaves con lo cual los tiempos pueden o no ser mayores o menores dependiendo de los factores mencionados con anterioridad y que fueron base de este estudio.
- Siempre que se usa WPA y WPA 2 personal el promedio de tiempo que disminuye es siempre proporcional. A diferencia cuando se usa WPA y WPA 2 tipo empresa el tiempo que disminuye es variable, esto se debe a que el número de eventos cuando

se usa el tipo personal es muy similar tanto en 802.11b como en 802.11g, pero en el tipo empresa estos eventos son variables ya que dependen del tipo de autenticación que se utilice, de allí la que la proporción en que disminuyen los tiempos sea diferente.

- Se puede concluir a partir del análisis de todos los tiempos que se obtuvieron como resultado de las pruebas experimentales, que la tecnología 802.11g ofrece un mejor comportamiento para el *streaming* con seguridad, con respecto a 802.11b.
- Fue obligatorio desarrollar estudios que sirvieron de apoyo a las actividades propuestas debido a la metodología empleada (Modelo de investigación experimental complementado con un modelo cíclico de verificación de hipótesis), ya que, permitió la granularidad del trabajo de grado. La característica de *roaming* es muy usada en el entorno inalámbrico en el que la popularización y la comodidad son símbolos de evolución, competitividad y tecnología.
- Los factores críticos establecidos analíticamente en el capítulo 1 fueron de vital importancia en el momento de realizar las experimentaciones porque crearon los lineamientos para la rutina de actividades y entrega exitosa de resultados; se corroboró con mediciones los retardos y pérdidas presentadas en *roaming* cuando se transmite *streaming* y se implementa la característica de seguridad, de las observaciones encontradas algunas de las conclusiones son, los retardos causados por la búsqueda de canales no se pueden clasificar como críticos debido a la naturaleza del *streaming*, estos paquetes contienen varios fotogramas y *buffers* los cuales son reproducidos mientras se recibe un nuevo paquete o se transmite otra información por el mismo canal de red. El ancho de banda, el tipo de autenticación, y la reasociación son factores que contribuyen de forma real y directa al retardo y las pérdidas.
- De la misma manera, se puede concluir que a pesar de las técnicas de cacheo de PMK y la preautenticación, que son dos métodos que ofrece el estándar IEEE 802.11i para minimizar el tiempo de *roaming*, no se logran los tiempos deseados para una transición transparente entre APs como se detallan en la secciones 2.6.5, 2.7.5, 4.2.2 y 4.2.1, adicionalmente, tienen el problema que para su correcto funcionamiento la STA debe haber realizado el proceso completo de autenticación por lo menos una vez con el AP con el que desea realizar la nueva transición. También es un problema que estas técnicas no son obligatorias en el estándar IEEE 802.11i, así que no está garantizada la interoperabilidad.
- A través del desarrollo experimental se verificó lo que se esperaba después del análisis teórico de WPA y WPA 2, concerniente con los métodos de operación Personal y Empresa. De los estudios se deduce que el modo personal es mucho más rápido que el modo empresarial usando servidor RADIUS; esto se debe a que en todas las pruebas realizadas se reflejaron todos los tiempos de los intercambios de mensajes que se dieron con los dos tipos de implementaciones dando como resultado tiempos menores para el modo personal.
- Un aspecto fundamental que se logra concluir después del análisis del estándar IEEE 802.11r, es que este nuevo mecanismo de seguridad reduce el tiempo manteniendo

un nivel robusto en el cifrado de los datos. Se puede ver que mediante un cambio en el manejo y gestión de las llaves se logra convertir un proceso largo de reautenticación y derivación de llaves en un proceso mucho más corto eliminando el proceso de reautenticación 802.1x\EAP y añadiendo el proceso de derivación de llaves en un proceso corto de intercambio de 4 mensajes o 6 mensajes en el caso de el protocolo con petición de recursos. A pesar de esto, se encontró analíticamente que éste nuevo estándar no va encaminado a mejorar aplicaciones como streaming ya que este tipo de aplicaciones son mucho más sensibles a los retardos por su naturaleza orientada a conexión. Cuando se hace una transición a otro AP se corta completamente la recepción de paquetes y es obligatoria la reconexión de la aplicación con el servidor de streaming.

- Adicionalmente se puede concluir a partir del análisis del estándar 802.11r que a pesar de que se mejora el tiempo de *roaming* notablemente, se desmejora un poco la seguridad, esto se debe a que para evitar la reautenticación 802.1x cuando se realiza el *roaming*, el estándar se basa en su nueva jerarquía de llaves mediante la cual se distribuye la llave PMK hacia los nuevos APs a través del DS, y el estándar no establece ninguna norma o característica especial para este proceso, es aquí donde puede haber alguna vulnerabilidad en la seguridad en el momento de distribuir la llave por el DS.
- Después de analizar todas las características del *roaming* durante las pruebas de laboratorio, se comprobó el *problema* que implica para aplicaciones como el *streaming*, realizar un cambio de AP cuando se está usando WPA y WPA 2. Cabe resaltar que las pruebas fueron realizadas en un *ambiente ideal* respecto a tráfico, es decir, el único tráfico que fluía en la red durante las pruebas fue el de los servidores de *streaming*; es de esperarse que en una red con tráfico adicional al de *streaming* en un ambiente empresarial, pública o universitaria, que los resultados sean peores debido al aumento de los recursos y la disminución del ancho de banda.
- Es recomendable que la actualización de *Firmware* para los D-LINK sea una versión estable y con una correcta funcionalidad, es importante que la implementación de *streaming* sea soportada por los clientes en sus dispositivos móviles en cuanto a codificadores/decodificadores y recursos de audio y video. En el proceso de *roaming* es inevitable la desconexión causada por el cambio de AP, por esta razón se recomienda el uso de aplicaciones no orientadas a conexión para servicios multimedia, además, para el diseño e implementación de redes ESS se sugiere remitirse al capítulo 4.
- Como trabajo futuro se podría pensar en la implementación de *streaming* con calidad de servicio para redes inalámbricas como 802.16 o redes celulares de tercera generación. Los estudios generados en las experimentaciones son contribución a posteriores investigaciones que brinden mejores resultados y contribuyan al desarrollo de nuevos estándares; el Apéndice I consta de una serie de propuestas basadas en el conocimiento obtenido durante la experimentación, sería un excelente trabajo futuro el corroborar los modelos sugeridos y verificar si existe una optimización significativa.
- También se recomienda para trabajos futuros analizar experimentalmente el estándar 802.11r ya que en el momento no se tienen dispositivos que lo soporten y por ende no hay resultados reales de los tiempos que se logran implementando este estándar.

- Luego de trabajar con *roaming*, y ver que es un tema muy interesante, se recomienda para trabajos futuros analizar el roaming vertical, es decir, roaming entre diferentes tecnologías físicas, por ejemplo, roaming entre 802.11 y 3G, o entre 802.11 y 802.16, ya que este tipo de servicio está siendo requerido e investigado en la actualidad.

REFERENCIAS BIBLIOGRÁFICAS

- [1] ANSI/IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications", Piscataway USA,1999. 528 p.
- [2] GAST, Matthew S. "802.11 Wireless Networks, The Definitive Guide", O'Reilly, Junio 2002. 464 p.
- [3] Eva Herrera-Ramírez, Arnoldo Díaz-Ramírez, Carlos T. Calafate, "Desarrollando el estándar IEEE 802.11n, un paso adelante en WLAN", [en línea] septiembre 2007, Disponible en: <<http://cachanilla.itmexicali.edu.mx/~adiaz/Publicaciones/Estandar80211.pdf>> [consulta: marzo 2008]
- [4] EDNEY, Jon y ARBAUGH, William A. "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison Wesley, Julio 2003. 480 p.
- [5] Lars Strand, "802.1x Port-Based Authentication HOWTO", [en línea] julio 2004, Disponible en: <http://tldp.org/HOWTO/html_single/8021X-HOWTO>. [consulta: agosto 2007]
- [6] MICROSOFT, "Planeamiento de la implementación de seguridad en LAN inalámbricas". [en línea] Disponible en: <http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_2.msp>. [consulta: agosto 2007]
- [7] ARUNESH Mishra, MINHO Shin y ARBAUG William , University of Maryland. "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", [en línea]. Abril 2003. Disponible en: <<http://www.cs.umd.edu/~waa/pubs/handoff-lat-acm.pdf>>, [consulta: mayo 2006].
- [8] Peter Thornycroft, "Handover Mechanics for Wi-Fi Phones: Handover Defined". Mayo 2007 [en línea]. Disponible en: <<https://edge.arubanetworks.com/article/handover-mechanics-Wi-Fi-phones-handover-defined>> [consulta: agosto 2007]
- [9] Peter Thornycroft, "Handover Mechanics for Wi-Fi Phones: Putting it All Together", [en línea]. Mayo 2007. Disponible en: <<https://edge.arubanetworks.com/article/handover-mechanics-Wi-Fi-phones-putting-it-all-together>>. [consulta: agosto 2007]
- [10] Pejman Roshan, Jonathan Leary, "802.11 Wireless LAN Fundamentals", Cisco Press, diciembre 2003. 312 p.
- [11] Michael Adams , "LIP Synchronization in Video Conferencing" [en línea] agosto 2001, Disponible en: <www.ciscopress.com/content/images/9781587052682/samplechapter/1587052687_CH07.pdf>. [consulta julio 2008]
- [12] IEEE, "802.11r-2008", [en línea] julio 2008, Disponible en: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=4573291&number=4573292>[consulta septiembre 2008]
- [13] Jon-Olov Vatn "An experimental study of IEEE 802.11b handover performance and its effect on voice traffic" [en línea] julio 2003, Disponible en: <www.it.kth.se/~vatn/research/handover-perf.pdf> [consulta noviembre 2008]
- [14] Ivan Martinovic, Frank A. Zdarsky, Adam Bachorek, and Jens B. Schmitt, "Measurement and Analysis of Handover Latencies", noviembre 2007, [en línea] Disponible en: <www.ew2007.org/papers/1569014924.pdf> [consulta noviembre 2008]
- [15] Virusprot.com, "Roaming en redes Wi-fi", diciembre 2006 [en línea], Disponible en: <<http://www.virusprot.com/cursos/Redes-Inal%C3%A1mbricas-Curso-gratis5.htm>>, [consulta noviembre 2008]
- [16] Virusprot.com "Los mejores malos consejos", abril 2008 [en línea], Disponible en: <<http://www.acis.org.co/fileadmin/Conferencias/ConfEduarTabacAbril24.pdf>>, [consulta noviembre 2008]
- [17] www.codealias.info, "The 802.11 handoff process", [en línea], Disponible en: <http://www.codealias.info/technotes/performance_evaluation_of_wireless_security_system_s_part_2_-_the_802.11_handoff_process> [consulta diciembre 2008]
- [18] Paul Goransson, Raymond Greenlaw, "Secure Roaming In 802.11 Networks", Newnes, 2007, 343 pag.
- [19] Alfonso Fernández Durán, Mariano Molina García, José I. Alonso, "Efecto del tamaño de la ventana de promediado y la histeresis variable en algoritmos de handover horizontal en redes convergentes" mayo 2007 [en línea], Disponible en: <http://telecomid.webs.upv.es/ftp/CD/Programa%20Oficial%20Telecom%20I+D%202007_07_14_archivos/pdf/69.pdf> [consulta diciembre 2008]

- [20] Juha-Pekka Mäkelä, "Effects of handoff algorithms on the performance of multimedia wireless networks" junio 2008 [en línea], Disponible en: <<http://herkules.oulu.fi/isbn9789514288241/isbn9789514288241.pdf>> [consulta diciembre 2008]
- [21] Ahmed, H. Hassanein H., "A performance study of roaming in wireless local area networks based on IEEE 802.11r", junio de 2008 [en línea], Disponible en: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4563250> [consulta octubre 2008]
- [22] Rogelio Montañana, "Redes Inalámbricas", 2008 [en línea], Disponible en: <www.uv.es/montanan/ampliacion> [consulta diciembre 2008]