



# **ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

## **EVALUACIÓN DEL RENDIMIENTO DE DISPOSITIVOS ACCESS POINT, MEDIANTE EL USO DE MECANISMOS DE CONECTIVIDAD EN REDES CON ALTA CONCURRENCIA DE USUARIOS**

**EDGAR MAURICIO ULLOA CÓNDOR**

**Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,  
presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH,  
como requisito parcial para la obtención del grado de:**

**MAGISTER EN INTERCONECTIVIDAD DE REDES**

**RIOBAMBA – ECUADOR**

**Septiembre, 2020**

**© 2020, Edgar Mauricio Ulloa Córdor.**

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.



## ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

### CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado *“EVALUACIÓN DEL RENDIMIENTO DE DISPOSITIVOS ACCESS POINT, MEDIANTE EL USO DE MECANISMOS DE CONECTIVIDAD EN REDES CON ALTA CONCURRENCIA DE USUARIOS”*, de responsabilidad del Ing. Edgar Mauricio Ulloa Córdor, ha sido prolijamente revisado y se autoriza su presentación.

#### Tribunal:

Ing. Oswaldo Geovanny Martínez Guashima; Mag. \_\_\_\_\_  
**PRESIDENTE** **FIRMA**

Ing. Germanía del Rocío Veloz Remache; Mag. \_\_\_\_\_  
**DIRECTOR** **FIRMA**

Ing. Gladys Lorena Aguirre Sailema; Mag \_\_\_\_\_  
**MIEMBRO** **FIRMA**

Ing. Paul Leónidas Tutillo Andrade; Mag \_\_\_\_\_  
**MIEMBRO** **FIRMA**

**Riobamba, septiembre 2020**

**DERECHOS INTELECTUALES**

Yo, Edgar Mauricio Ulloa Córdor, con cédula de identidad 0201886611, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

**EDGAR MAURICIO ULLOA CÓNDOR**

C.C.: 0201886611

## **DECLARACIÓN DE AUTENTICIDAD**

Yo, Edgar Mauricio Ulloa Córdor, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

**EDGAR MAURICIO ULLOA CÓNDOR**

C.C.: 0201886611

## **DEDICATORIA**

Dedico el presente trabajo de titulación a mi familia quienes han sido el pilar fundamental para alcanzar mi superación personal y profesional, a mi padre Edmundo Guillermo Ulloa Zavala y a mi madre Teresita de Jesús Cóndor Muñoz por brindarme su consejo y apoyo incondicional, por alentarme día a día a continuar con los estudios, a mis hermanos (as), tíos (as), a mis amigos y demás compañeros que me han apoyado para que todas mis metas se cumplan.

*Edgar Mauricio Ulloa Cóndor.*

## **AGRADECIMIENTO**

Deseo manifestar un sincero y profundo agradecimiento a la Escuela Superior Politécnica de Chimborazo por haberme permitido cursar el programa de maestría en interconectividad de redes con el fin de culminar un sueño más de mis aspiraciones en el área profesional.

A la coordinadora de la maestría en interconectividad de redes Ing. Blanca Faustina Hidalgo Ponce por su apoyo constante durante todo el periodo de realización de tesis.

A mi tutora Ing. Germania del Rocío Veloz Remache MSc. y miembros del tribunal Ing. Paúl Leónidas Tuttilo Andrade MSc. y la Ing. Lorena Aguirre MSc., por ser partícipes de este trabajo y haberme guiado durante el proceso de titulación, por compartir sus conocimientos en la elaboración de la investigación, por brindarme sus sabios consejos y la guía oportuna. A todas aquellas personas que han intervenido de forma directa o indirecta en el proceso de realización de esta investigación, siempre pensando y apoyando para que culminara con éxitos, les doy mi más profundo agradecimiento.

*Edgar Mauricio Ulloa Córdor.*

## **ÍNDICE DE CONTENIDO**

<b>RESUMEN</b> .....	xxiii
<b>ABSTRACT</b> .....	xxiv
<b>CAPÍTULO I</b> .....	1
<b>1. INTRODUCCIÓN</b> .....	1
1.1. Planteamiento del problema.....	1
1.2. Formulación del problema. ....	2
1.3. Sistematización del problema.....	2
1.4. Justificación de la investigación.....	3
1.5. Objetivos de la investigación. ....	4
1.5.1. <i>Objetivo General.</i> ....	4
1.5.2. <i>Objetivos Específicos.</i> ....	4
1.6. Hipótesis.....	5
1.7. Identificación de variables.....	5
1.7.1. <i>Variable Independiente.</i> ....	5
1.7.2. <i>Variable dependiente.</i> ....	5
1.8. Operacionalización de Variables. ....	5
1.9. Matriz de Consistencia. ....	6
<b>CAPÍTULO II</b> .....	7
<b>2. MARCO TEÓRICO</b> .....	7
2.1. Antecedentes del problema.....	7
2.2. Bases teóricas.....	13
2.2.1. <i>Redes de comunicaciones.</i> ....	13
2.2.2. <i>Redes WAN.</i> ....	13
2.2.3. <i>Redes LAN.</i> ....	14
2.2.4. <i>Redes inalámbricas.</i> ....	15
2.2.4.1. Topologías de redes inalámbricas.....	15
2.2.5. <i>Dispositivos Inalámbricos.</i> .....	17
2.2.6. <i>Access Point.</i> ....	18

<b>2.2.7.</b>	<b><i>Esquema de configuración de AP.</i></b> .....	19
<b>2.2.8.</b>	<b><i>Análisis Tecnología Wifi.</i></b> .....	19
<b>2.2.9.</b>	<b><i>Cobertura de radio.</i></b> .....	20
<b>2.2.10.</b>	<b><i>Equipamiento de cobertura.</i></b> .....	21
<b>2.2.11.</b>	<b><i>Estándares de telecomunicaciones.</i></b> .....	21
2.2.11.1.	Estándares IEEE 802.11.....	21
<b>2.2.12.</b>	<b><i>Bandas de Frecuencias Tecnología Wifi.</i></b> .....	25
2.2.12.1.	Banda de Frecuencia Wifi 2.4GHz y 5GHz.....	25
2.2.12.2.	Capacidad del canal wifi.....	26
<b>2.2.13.</b>	<b><i>Intensidad de la señal.</i></b> .....	26
<b>2.2.14.</b>	<b><i>Internet.</i></b> .....	27
2.2.14.1.	Datos.....	28
2.2.14.2.	Rendimiento.....	28
2.2.14.3.	Ancho de Banda.....	29
2.2.14.4.	Latencia.....	29
2.2.14.5.	Tráfico de red.....	30
2.2.14.6.	Throughput.....	30
2.2.14.7.	Jitter.....	30
2.2.14.8.	Pérdida de paquetes.....	31
2.2.14.9.	Pérdidas por obstáculos.....	31
<b>2.2.15.</b>	<b><i>Seguridad.</i></b> .....	32
2.2.15.1.	WEP.....	32
2.2.15.2.	WPA.....	32
2.2.15.3.	WPA2.....	33
2.2.15.4.	Seguridad 802.1x EAP.....	33
<b>2.2.16.</b>	<b><i>Pruebas de conectividad.</i></b> .....	34
<b>2.2.17.</b>	<b><i>FODA tecnología Wifi.</i></b> .....	34

2.2.17.1. Debilidades.....	34
2.2.17.2. Amenazas.....	35
2.2.17.3. Fortalezas.....	36
2.2.17.4. Oportunidades.....	36
2.2.17.5. Resumen FODA.....	37
<b>CAPÍTULO III.....</b>	<b>38</b>
<b>3. METODOLOGÍA DE LA INVESTIGACIÓN.....</b>	<b>38</b>
<b>3.1. Tipo y Diseño de Investigación.....</b>	<b>38</b>
3.1.1. <i>Tipo de Investigación.....</i>	38
3.1.2. <i>Diseño de Investigación.....</i>	38
<b>3.2. Métodos de Investigación.....</b>	<b>39</b>
<b>3.3. Enfoque de la Investigación.....</b>	<b>39</b>
<b>3.4. Alcance de la Investigación.....</b>	<b>39</b>
<b>3.5. Población de estudio.....</b>	<b>40</b>
<b>3.6. Unidad de Análisis.....</b>	<b>41</b>
<b>3.7. Selección de la Muestra.....</b>	<b>41</b>
<b>3.8. Tamaño de la Muestra.....</b>	<b>42</b>
<b>3.9. Técnica de recolección de datos primarios y secundarios.....</b>	<b>43</b>
<b>3.10. Análisis de mecanismos de conectividad.....</b>	<b>44</b>
<b>3.11. Análisis comparativo de los Estándares IEEE 802.11N y 802.11AC.....</b>	<b>46</b>
3.11.1. <i>Velocidad de transmisión.....</i>	48
3.11.2. <i>Capacidad del canal.....</i>	51
3.11.3. <i>Intensidad de señal.....</i>	52
3.11.4. <i>Tráfico de red.....</i>	53
3.11.5. <i>Retardo de Propagación.....</i>	53
3.11.6. <i>Jitter.....</i>	53
3.11.7. <i>Throughput (Rendimiento).....</i>	54
3.11.8. <i>Latencia.....</i>	54
3.11.9. <i>Seguridad.....</i>	55

3.11.10. <i>Resultado comparativo teórico.</i> .....	55
3.12. Escenarios de prueba de los estándares IEEE 802.11N y 802.11AC. ....	56
3.12.1. <i>Simulación en Cisco 8500 Series Wireless Controller.</i> .....	61
3.12.1.1. Estándar IEEE 802.11N en Cisco 8500 Series Wireless Controller. ....	62
3.12.1.2. Estándar IEEE 802.11AC en Cisco 8500 Series Wireless Controller. ....	65
3.12.1.3. Tabla comparativa del Estándar IEEE 802.11N y 802.11AC en Cisco 8500 Series Wireless Controller. ....	67
3.12.2. <i>Simulación en Cisco Prime Infrastructure.</i> .....	69
3.12.2.1. Estándar IEEE 802.11N en Cisco Prime Infrastructure. ....	69
3.12.2.2. Estándar IEEE 802.11AC en Cisco Prime Infrastructure. ....	73
3.12.2.3. Tabla comparativa del Estándar IEEE 802.11N y 802.11AC en Cisco Prime Infrastructure. ....	77
<b>CAPÍTULO IV</b> .....	81
<b>4. RESULTADOS Y DISCUSIÓN.</b> .....	81
<b>4.1. Selección de la prueba estadística.</b> .....	81
4.1.1. <i>Selección del valor alfa (<math>\alpha</math>).</i> .....	83
4.1.2. <i>Selección del Software estadístico.</i> .....	83
<b>4.2. Prueba T de Student para muestras independientes.</b> .....	84
4.2.1. <i>Prueba T de Student del indicador Intensidad de Señal.</i> .....	84
4.2.1.1. Normalidad en el indicador Intensidad de señal. ....	84
4.2.1.2. Igualdad de varianzas en el indicador Intensidad de señal. ....	85
4.2.1.3. Resultados prueba T de Student. ....	86
4.2.1.4. Decisión estadística. ....	88
4.2.2. <i>Prueba T de Student del indicador Calidad de Conexión.</i> .....	89
4.2.2.1. Normalidad en el indicador Calidad de conexión. ....	89
4.2.2.2. Igualdad de varianzas en el indicador Calidad de conexión. ....	90
4.2.2.3. Resultados prueba T de Student. ....	91
4.2.2.4. Decisión estadística. ....	93
4.2.3. <i>Prueba T de Student del indicador Throughput (Rendimiento).</i> .....	94

4.2.3.1.	Normalidad en el indicador Throughput.....	94
4.2.3.2.	Igualdad de varianzas en el indicador Throughput.....	95
4.2.3.3.	Resultados prueba T de Student. ....	96
4.2.3.4.	Decisión estadística. ....	98
<b>4.2.4.</b>	<b><i>Resumen de indicadores evaluados.</i></b> .....	<b>99</b>
<b>CAPÍTULO V</b> .....		<b>102</b>
<b>5.</b>	<b>PROPUESTA: GUÍA DE ESPECIFICACIONES TÉCNICAS DE LOS AP. ..</b>	<b>102</b>
<b>5.1.</b>	<b>INTRODUCCIÓN.....</b>	<b>106</b>
<b>5.2.</b>	<b>ALCANCE.....</b>	<b>106</b>
<b>5.3.</b>	<b>TIPOS DE USUARIOS.....</b>	<b>107</b>
<b>5.4.</b>	<b>GLOSARIO DE TÉRMINOS.....</b>	<b>107</b>
<b>5.5.</b>	<b>Identificar el lugar de instalación.....</b>	<b>107</b>
<b>5.5.1.</b>	<b><i>Usuario Administrador.</i></b> .....	<b>109</b>
<b>5.5.2.</b>	<b><i>Usuario Normal.</i></b> .....	<b>109</b>
<b>5.6.</b>	<b>Identificar a que usuarios está orientado el servicio.....</b>	<b>109</b>
<b>5.6.1.</b>	<b><i>Usuario Administrador.</i></b> .....	<b>110</b>
<b>5.6.2.</b>	<b><i>Usuario Normal.</i></b> .....	<b>111</b>
<b>5.7.</b>	<b>Requerimientos económicos de instalación.....</b>	<b>111</b>
<b>5.7.1.</b>	<b><i>Usuario Administrador.</i></b> .....	<b>112</b>
<b>5.7.2.</b>	<b><i>Usuario Normal.</i></b> .....	<b>114</b>
<b>5.8.</b>	<b>Requerimientos técnicos de los Access Point.....</b>	<b>116</b>
<b>5.8.1.</b>	<b><i>Usuario Administrador.</i></b> .....	<b>117</b>
<b>5.8.2.</b>	<b><i>Usuario Normal.</i></b> .....	<b>117</b>
<b>5.9.</b>	<b>Determinar ubicación física de los Access Point. ....</b>	<b>119</b>
<b>5.9.1.</b>	<b><i>Usuario Administrador.</i></b> .....	<b>119</b>
<b>5.9.2.</b>	<b><i>Usuario Normal.</i></b> .....	<b>120</b>
<b>5.10.</b>	<b>Determinar protocolos de seguridad de los Access Point. ....</b>	<b>121</b>
<b>5.10.1.</b>	<b><i>Usuario Administrador.</i></b> .....	<b>121</b>
<b>5.10.2.</b>	<b><i>Usuario Normal.</i></b> .....	<b>122</b>

<b>5.11.</b>	<b>Características de configuración por software.</b>	123
<b>5.11.1.</b>	<i>Usuario Administrador.</i>	123
<b>5.11.2.</b>	<i>Usuario Normal.</i>	125
<b>5.12.</b>	<b>Características de configuración por consola.</b>	126
<b>5.12.1.</b>	<i>Usuario Administrador.</i>	126
<b>5.12.2.</b>	<i>Usuario Normal.</i>	128
<b>CONCLUSIONES.</b>		129
<b>RECOMENDACIONES.</b>		131
<b>BIBLIOGRAFÍA.</b>		
<b>ANEXOS.</b>		

## ÍNDICE DE TABLAS

<b>Tabla 1-1:</b> Operacionalización de Variables.....	5
<b>Tabla 2-1:</b> Matriz de consistencia.....	6
<b>Tabla 1-2:</b> Equivalencias de intensidad de señal en dBm.....	9
<b>Tabla 2-2:</b> Características WLAN Access Point.....	16
<b>Tabla 3-2:</b> Estándares Tecnología Wifi.....	19
<b>Tabla 4-2:</b> Frecuencia Tecnología Wifi.....	22
<b>Tabla 5-2:</b> Diferencias de frecuencias 2.4 GHz y 5GHz.....	23
<b>Tabla 6-2:</b> Resumen FODA.....	31
<b>Tabla 1-3:</b> Velocidad de Transmisión comparativa entre estándar N y AC.....	39
<b>Tabla 2-3:</b> Velocidades de datos 802.11n en 2.4 GHz.....	41
<b>Tabla 3-3:</b> Velocidades de datos 802.11ac en 5 GHz.....	42
<b>Tabla 4-3:</b> Número máximo de canales no superpuestos.....	43
<b>Tabla 5-3:</b> Análisis comparativo de los estándares 802.11N y AC.....	46
<b>Tabla 6-3:</b> Access Point utilizados en red inalámbrica UCE.....	49
<b>Tabla 7-3:</b> Beneficios de AP Cisco series 1700.....	49
<b>Tabla 8-3:</b> Especificaciones Access Point Cisco series 1700.....	50
<b>Tabla 9-3:</b> Comparativa de los Estándares 802.11N y AC con Cisco 8500 Series.....	56

<b>Tabla 10-3:</b> Comparativa de los Estándares 802.11N y AC con Cisco Prime Infrastructure ....	65
<b>Tabla 1-4:</b> Selección de la prueba estadística .....	68
<b>Tabla 2-4:</b> Normalidad del indicador Intensidad de señal .....	70
<b>Tabla 3-4:</b> Igual de varianzas del indicador Intensidad de señal.....	71
<b>Tabla 4-4:</b> T de Student del indicador Intensidad de señal. ....	72
<b>Tabla 5-4:</b> Comparación de medias del indicador Intensidad de señal. ....	72
<b>Tabla 6-4:</b> Normalidad para el indicador Calidad de conexión. ....	74
<b>Tabla 7-4:</b> Igual de varianzas para el indicador Calidad de conexión. ....	75
<b>Tabla 8-4:</b> T de Student para el indicador Calidad de conexión. ....	76
<b>Tabla 9-4:</b> Comparación de medias para el indicador Calidad de conexión. ....	76
<b>Tabla 10-4:</b> Normalidad del indicador Throughput (Rendimiento).....	78
<b>Tabla 11-4:</b> Igual de varianzas del indicador Throughput (Rendimiento).....	79
<b>Tabla 12-4:</b> T de Student del indicador Throughput (Rendimiento).....	80
<b>Tabla 13-4:</b> Comparación de medias para el indicador Throughput (Rendimiento).....	81
<b>Tabla 14-4:</b> Indicadores de los Estándares 802.11N y AC con T de Student .....	82

## ÍNDICE DE FIGURAS

<b>Figura 1-2:</b> Modelos de APs Cisco existentes en la Red Inalámbrica UCE .....	8
<b>Figura 2-2:</b> Calidad de la Conexión – Intensidad de Señal.....	8
<b>Figura 3-2:</b> Calidad de la Señal versus Ruido.....	10
<b>Figura 4-2:</b> Tasa de Conexión.....	10
<b>Figura 5-2:</b> APs Cisco con antena Aironet 2700 y sin antena Aironet 1700 .....	11
<b>Figura 6-2:</b> Redes WAN .....	12
<b>Figura 7-2:</b> Redes LAN .....	13
<b>Figura 8-2:</b> Red Inalámbrica .....	13
<b>Figura 9-2:</b> Topología AD-HOC.....	14
<b>Figura 10-2:</b> Topología ESS .....	14
<b>Figura 11-2:</b> Topología BSS .....	15
<b>Figura 12-2:</b> Red Inalámbrica (Wifi) .....	17
<b>Figura 13-2:</b> Cobertura y alcance de radio.....	18
<b>Figura 14-2:</b> Comparación entre estándares .....	21
<b>Figura 15-2:</b> Intensidad de señal.....	24

<b>Figura 1-3:</b> Población de estudio .....	34
<b>Figura 2-3:</b> Estándares 802.11 más utilizados .....	38
<b>Figura 3-3:</b> Modelos de AP Cisco.....	39
<b>Figura 4-3:</b> Comparación de velocidades de transmisión .....	40
<b>Figura 5-3:</b> Canales adyacentes superpuestos.....	43
<b>Figura 6-3:</b> Cisco 8500 Series Wireless Controller (Dashboard) .....	47
<b>Figura 7-3:</b> Señalización Figura 7-3 .....	48
<b>Figura 8-3:</b> Ambiente de prueba teórico .....	48
<b>Figura 9-3:</b> Estructura física del ambiente de prueba 802.11N.....	51
<b>Figura 10-3:</b> Datos obtenidos en 802.11N en 2.4GHz.....	52
<b>Figura 11-3:</b> Calidad de señal en 802.11N en 2.4GHz .....	53
<b>Figura 12-3:</b> Estructura física del ambiente de prueba 802.11AC.....	54
<b>Figura 13-3:</b> Datos obtenidos en 802.11AC en 5GHz .....	55
<b>Figura 14-3:</b> Esquema de Red inalámbrica IEEE 802.11N en 2.4GHz .....	57
<b>Figura 15-3:</b> Datos obtenidos en IEEE 802.11N en 2.4GHz .....	58
<b>Figura 16-3:</b> Potencia de señal en IEEE 802.11N en 2.4GHz .....	60
<b>Figura 17-3:</b> Esquema de Red inalámbrica IEEE 802.11AC en 5GHz .....	61
<b>Figura 18-3:</b> Datos obtenidos en IEEE 802.11AC en 5GHz .....	61
<b>Figura 19-3:</b> Potencia de señal en IEEE 802.11N en 2.4GHz .....	63
<b>Figura 20-3:</b> Comparación de potencia de señal IEEE 802.11N y AC.....	64
<b>Figura 21-3:</b> Top de sistemas operativos activos en la red inalámbrica .....	65
<b>Figura 22-3:</b> Estándar Wifi móvil gama alta .....	66
<b>Figura 23-3:</b> Estándar Wifi móvil gama media.....	66

<b>Figura 1-5:</b> Top de sistemas operativos activos en la red inalámbrica .....	84
<b>Figura 2-5:</b> Estándar Wifi móvil gama alta .....	85
<b>Figura 3-5:</b> Estándar Wifi móvil gama media.....	85
<b>Figura 4-5:</b> Espacio abierto – Parque de la Ciudadela Universitaria UCE. ....	88
<b>Figura 5-5:</b> Espacio cerrado o cubierto – Edificio Facultad de Administración.....	89
<b>Figura 6-5:</b> Estándar Wifi móvil gama alta .....	90
<b>Figura 7-5:</b> Estándar Wifi móvil gama media.....	90
<b>Figura 8-5:</b> Access Point modelo antiguo con antenas en 2.4GHz.....	92
<b>Figura 9-5:</b> Slots de antenas con radios para 2.4GHz y 5GHz .....	93
<b>Figura 10-5:</b> Access Point con antenas externas e internas. ....	93
<b>Figura 11-5:</b> Routers Cisco a manera de Access Point para lugares pequeños.....	94
<b>Figura 12-5:</b> Routers TP-Link a manera de Access Point para lugares pequeños .....	95
<b>Figura 13-5:</b> Tipos de Access Point.....	95
<b>Figura 14-5:</b> Especificaciones de Router Cisco a manera de AP.....	96
<b>Figura 15-5:</b> Especificaciones de Router TP-LINK a manera de AP. ....	97
<b>Figura 16-5:</b> Protocolo 802.1x implementado en la UCE.....	100
<b>Figura 17-5:</b> Protocolo 802.1x implementado en la UCE.....	101
<b>Figura 18-5:</b> Interfaz de antenas habilitadas .....	102
<b>Figura 19-5:</b> Interfaz de radios habilitados .....	102
<b>Figura 20-5:</b> Configuración AP usuario normal .....	103
<b>Figura 21-5:</b> Consola de comandos para levantar/bajar Interfaz de Radios .....	104
<b>Figura 22-5:</b> Consola de comandos para levantar/bajar Interfaz de Radios .....	105

## ÍNDICE DE GRÁFICOS

<b>Gráfico 1-3:</b> Tráfico de clientes en IEEE 802.11N 2.4GHz .....	59
<b>Gráfico 2-3:</b> Porcentaje de clientes vs intensidad de señal en IEEE 802.11N en 2.4GHz.....	59
<b>Gráfico 3-3:</b> Tráfico de clientes en IEEE 802.11AC 5GHz.....	62
<b>Gráfico 4-3:</b> Porcentaje de clientes vs intensidad de señal en IEEE 802.11AC en 5GHz .....	63
<b>Gráfico 1-4:</b> Comparación de IEEE 802.11N y AC del indicador Intensidad de Señal.....	73
<b>Gráfico 2-4:</b> Comparación de IEEE 802.11N y AC del indicador Calidad de conexión.....	77
<b>Gráfico 3-4:</b> Comparación de IEEE 802.11N y AC del indicador Throughput.....	81
<b>Gráfico 4-4:</b> Resultados de IEEE 802.11N y AC del indicador Intensidad de Señal .....	82
<b>Gráfico 5-4:</b> Resultados de IEEE 802.11N y AC del indicador Calidad de Conexión .....	83
<b>Gráfico 6-4:</b> Resultados de IEEE 802.11N y AC del indicador Throughput.....	83

## **LISTADO DE ANEXOS**

**ANEXO A:** Cisco Aironet 1700 Series Access Point.

**ANEXO B:** Cisco 8500 Series Wireless Controller.

**ANEXO C:** Cisco Prime Infrastructure 3.x.

## ÍNDICE DE ABREVIATURAS

AP	ACCESS POINT
BSS	BUSINESS SUPPORT SYSTEMS
CPU	CENTRAL PROCESSOR UNIT
ESS	EXTENDED SERVICES SET
FCQ	FACULTAD DE CIENCIAS BIOLÓGICAS

FODA	FORTALEZAS, OPORTUNIDADES, DEBILIDADES Y AMENAZAS
IEEE	INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS
MAC	MEDIA ACCESS CONTROL
OSI	OPEN SYSTEM INTERCONNECTION
UCE	UNIVERSIDAD CENTRAL DEL ECUADOR
WIFI	WIRELESS FIDELITY
WLAN	WIRELESS LOCAL AREA NETWORK
WPAN	WIRELESS PERSONAL AREA NETWORK

## **RESUMEN**

La finalidad de esta investigación fue mejorar el rendimiento de dispositivos Access Point en redes con alta concurrencia de usuarios usando mecanismos de conectividad, los mismos que se

analizaron y posteriormente se seleccionaron por ser los más sobresalientes en la actualidad y más utilizados en la Universidad Central del Ecuador. De acuerdo al estudio los elegidos fueron los Estándares IEEE 802.11N y 802.11AC, que cuentan con parámetros de medición como ancho de banda, throughput, latencia, jitter, ruido, intensidad de señal, calidad de conexión, entre otros, con estos parámetros se pudo obtener resultados mediante la comparación estadística de sus datos. Luego se realizaron simulaciones en las herramientas: Cisco Prime Infrastructure y Cisco 8500 Series Wireless Controller, en estas se ejecutaron pruebas de los estándares en mención, midiendo parámetros como: tasa de velocidad configurada, tráfico, throughput, intensidad de señal, calidad de conexión o ruido, utilización del canal e interferencia, para obtener posibles criterios acerca del mejor mecanismo de conectividad, una vez evaluados arrojan resultados orientados hacia el estándar IEEE 802.11N. Para finalizar, mediante el análisis estadístico T de Student para muestras independientes se toma una muestra para cada estándar y se determina los resultados de los indicadores evaluados con los siguientes valores, intensidad de señal 60,88 dBm para 802.11N y -65,64 dBm para 802.11AC, calidad de conexión 29,19 dB para 802.11N y 26,24 dB para 802.11AC y throughput 4953,60 kbps para 802.11N y 3296,93 kbps para 802.11AC, datos que identifican y demuestran la superioridad del rendimiento de la red inalámbrica con el estándar 802.11N, así mismo y como punto final se emite ciertos criterios a manera de guía sobre características económicas, ubicación física, configuración por software y por comandos que deben tener los Access Point para trabajar de manera óptima y por ende permitan tener un rendimiento alto en la red inalámbrica.

**Palabras Clave:** <ACCESS POINT (AP)>, <CONECTIVIDAD>, <MECANISMOS>, <ESTÁNDAR>, <RUIDO>, <RENDIMIENTO>, <THROUGHPUT>, <WIRELESS FIDELITY (WIFI)>, <WIRELESS LOCAL AREA NETWORK (WLAN)>.

## **ABSTRACT**

The purpose of this research was to improve the performance of access point devices in networks with high concurrency of users using connectivity mechanisms. These were analyzed and later selected as the most outstanding and most used devices at the Central University of Ecuador. According to the study, the IEEE 802.11N and 802.11AC Standards were chosen, which have measurement parameters such as bandwidth, throughput, latency, jitter, noise, signal strength, and connection quality, among others. Then simulations were performed in the tools Cisco Prime Infrastructure and Cisco 8500 Series Wireless Controller. In these tests, standards in mention were executed, measuring parameters such as configured speed rate, traffic, throughput, signal strength, connection quality or noise, channel utilization and interference. Obtaining possible criteria about the best mechanism of connectivity, once evaluated, give results-oriented towards the standard IEEE 802.11N. Finally, through the Student T statistical analysis for independent samples, a sample is taken for each standard. The results of the evaluated indicators are determined with the following values, signal strength 60.88 dBm for 802.11N and -65.64 dBm for 802.11AC, connection quality 29.19 dB for 802.11N and 26.24 dB for 802.11AC and throughput 4953.60 kbps for 802.11N and 3296.93 kbps for 802.11AC, data that identify and demonstrate the superiority of the wireless network performance with the 802.11N standard. And as an endpoint, specific criteria are issued as a guide to economic characteristics, physical location, software, and command configuration that must have access points to work optimally and therefore allow high performance in the wireless network.

**Keywords:** <ACCESS POINT (AP)>, <CONNECTIVITY>, <MECHANISMS>, <STANDARD>, <NOISE>, <PERFORMANCE>, <THROUGHPUT>, <WIRELESS FIDELITY (WIFI)>, <WIRELESS LOCAL AREA NETWORK (WLAN)>.

# CAPÍTULO I

## 1. INTRODUCCIÓN

### 1.1. Planteamiento del problema.

Fruto de la tecnología se evidencia en la actualidad como el mundo ha logrado tener una comunicación global a través del internet, la misma que se ha convertido en la mayor fuente de comunicación en donde se conectan millones de dispositivos (*Ramírez, 2018*).

Al inicio la comunicación entre estos dispositivos se realizaba únicamente de manera cableada mediante el protocolo de internet (IP), por tal motivo en estos últimos años se ha notado el incremento de redes inalámbricas. Este crecimiento se debe a varios motivos, como el estilo de vida actual donde las personas prefieren una conexión sin cables, la necesidad de siempre estar conectados a redes locales o Internet, tener conexión constante sin estar atados a aspectos de movilidad, mayor flexibilidad, etc. (*Vásconez D 2014, p. 110*).

Las redes inalámbricas en sus inicios tenían desventajas significativas como las mencionadas anteriormente, no obstante, también ofrecían muchas ventajas. Entre las más destacadas podemos indicar la compatibilidad que se tiene con redes cableadas, la facilidad con la que se puede ejecutar la instalación de estos dispositivos, los bajos costos de su implementación, la simplicidad en la administración, la escalabilidad, la capacidad de brindar cobertura a pesar de tener barreras físicas, etc. Y para mantener el control y la estabilidad, se creó estándares de comunicación naciendo así el estándar IEEE, el cual generó un grupo de trabajo específico para redes inalámbricas, llamado 802.11 (*Vallejo A, 2017*).

Pero si bien, las redes inalámbricas han ido expandiéndose por sus extraordinarias ventajas, se debe mencionar que en sus inicios tuvieron algunos problemas, como el control de acceso a la MAC (*Histinfblogs.upv.es, 2017*), problemas de conectividad generados por la gran demanda de usuarios, entre otros. Usualmente los inconvenientes generales de conexiones inalámbricas se deben a errores de configuración, firmware incompatible, interferencias con otros dispositivos, etc. (*Sites.google.com, 2018*).

A nivel global, las redes de área local inalámbricas llamadas también WLAN han sido densamente desplegadas para proporcionar el acceso a Internet a los clientes móviles. A medida que la población de clientes inalámbricos sigue aumentando, este tipo de redes son saturadas y por lo

tanto algunos usuarios de una red inalámbrica pueden encontrarse con graves problemas de degradación del rendimiento, provocado por el masivo acceso al canal y la interferencia (Yao, Sheng, & Mi, 2016).

En Ecuador la mayoría de las fallas en la comunicación inalámbrica se han determinado por problemas en el rendimiento de la red, lo que significa que los dispositivos podrían tener vulnerabilidades en su seguridad y por ende, intrusos podrían tener un fácil acceso a la red (El Universo, 2017). También podría tratarse de un problema de infraestructura debido a que los usuarios con dispositivos móviles prefieren conectarse a puntos de acceso de redes inalámbricas, en lugar de usar los planes de datos móviles, y es por este motivo que las empresas e instituciones públicas y privadas que no poseen la capacidad y/o configuración adecuada para el masivo uso de sus redes, recurren a la adquisición de nuevos dispositivos Access Point que cubran las insuficiencias inalámbricas (Diario La Hora, 2017).

El problema de rendimiento también está ligado con la concurrencia de los usuarios conectados a una red, estos tienen inconvenientes de lentitud en el servicio (Internet e Intranet), desconexión constante de los Access Point y falta de conectividad a la red inalámbrica causada por el gran número de usuarios conectados en una red (De Luz S., 2011).

Una técnica emergente en esta investigación es el posicionamiento físico de los dispositivos basados en la intensidad de la señal en redes inalámbricas (Access Point), con el que se podrá determinar el número y ubicación de los usuarios con el fin de obtener datos que permitan identificar la afluencia de usuarios/dispositivos conectados a una red inalámbrica y a su vez determinar el estado de saturación de estos (Wang & Shao, 2017). Además, existen varios mecanismos de conectividad con los cuales se puede evaluar el rendimiento de una red, las medidas que a menudo son consideradas importantes son el Ancho de banda, el throughput, la latencia, Jitter, la tasa de error y la intensidad de señal.

## **1.2. Formulación del problema.**

¿El rendimiento de dispositivos Access Point en redes con alta concurrencia de usuarios mejorará con la aplicación de mecanismos de conectividad en la Universidad Central del Ecuador?

## **1.3. Sistematización del problema.**

¿Existen estudios acerca del estado actual de dispositivos inalámbricos Access Point que brinden soluciones de rendimiento y conectividad en redes con alta concurrencia de usuarios?

¿Con la mejora en el funcionamiento de dispositivos inalámbricos Access Point los usuarios finales tendrán una mejor fluidez en el servicio (Internet e Intranet), una conexión estable y navegación constante?

¿Existe una alineación correcta en los dispositivos Access Point, que permita cubrir las necesidades de conectividad inalámbrica de los usuarios de instituciones, empresas y establecimientos que cuentan con redes inalámbricas amplias?

¿Se ha establecido estándares de ubicaciones físicas de los Access Point con el fin de tener mejor rendimiento y cobertura inalámbrica?

¿Se reducirá la adquisición de nuevos equipos inalámbricos a partir del levantamiento de estudios que lleven al óptimo desempeño de dispositivos Access Point?

#### **1.4. Justificación de la investigación.**

Las redes inalámbricas han tomado gran importancia en la actualidad, su crecimiento en el ámbito tecnológico se debe al estilo de vida donde existe la necesidad de mantener una constante conectividad en redes locales o Internet, la facilidad a la movilidad, una mejor flexibilidad, entre otros. Esta investigación sirve y se proyecta en mejorar el rendimiento de dispositivos Access Point con el uso de mecanismos de conectividad tales como, una adecuada configuración del firmware, mejorar el posicionamiento físico, entre otros.

Mediante la evaluación del rendimiento de los dispositivos Access Point, se desea obtener mejoras en su funcionamiento, tanto en la parte de software que conllevaría a una óptima configuración y actualización de equipos inalámbricos y la de hardware que brindaría un buen posicionamiento físico y un excelente alcance que evite interferencias de señal entre ellos y con otros equipos inalámbricos.

Realizando dichas mejoras en el funcionamiento de los dispositivos inalámbricos Access Point se beneficiarán las instituciones, empresas y establecimientos que manejen redes con alta concurrencia de usuarios, porque permitirá tener una base de conocimiento acerca de la configuración de dispositivos inalámbricos Access Point. Por otro lado, se podrán conectar más usuarios con el mismo número de equipos, así como también, experimentarán fluidez en el servicio (Internet e Intranet), una conexión estable y navegación constante.

Además, esta investigación aportará en el ámbito de las telecomunicaciones, mediante la reducción de los costos de instalación en los equipos de configuración compleja, pero sobre todo en dispositivos inalámbricos Access Point, al mismo tiempo se busca tener un correcto posicionamiento físico que mejore el alcance del servicio, mejorar la disponibilidad al tener alta concurrencia de usuarios conectados al proveer un modelo de ajustes a nivel de firmware y como parte de la investigación aportar conocimientos e instrucciones a los administradores que manejan redes amplias, creando estándares de configuración y ubicación física que ayuden a tener un servicio de calidad (*Gordon W, 2015*).

Por lo antes mencionado esta investigación tiene como propósito, implantar mejoras en nuevos proyectos de telecomunicaciones inalámbricas. Centrándose en perfeccionar el rendimiento y conectividad de los establecimientos con redes amplias, como es el claro ejemplo de la Universidad Central del Ecuador que se beneficiará de esta investigación permitiendo que sus recursos tecnológicos sean optimizados mediante las acotaciones señaladas anteriormente.

## **1.5. Objetivos de la investigación.**

### **1.5.1. *Objetivo General.***

Evaluar el rendimiento de dispositivos Access Point en redes con alta concurrencia de usuarios, para mejorar el desempeño de estos mediante el uso de mecanismos de conectividad en la Universidad Central del Ecuador.

### **1.5.2. *Objetivos Específicos.***

- Analizar diversos mecanismos de conectividad y comparar los más eficientes para determinar cual ofrece mayor rendimiento en redes inalámbricas.
- Diseñar escenarios de pruebas en herramientas digitales, donde permita medir el rendimiento inalámbrico de los dos mejores mecanismos de conectividad.
- Implementar los dos mejores mecanismos de conectividad para que permita identificar cuál de ellos brindará un adecuado rendimiento de la red inalámbrica en la Universidad Central del Ecuador (UCE).

- Establecer una guía de implementación y características técnicas acerca del más sobresaliente mecanismo de conectividad el mismo que permita mejorar el rendimiento de los Access Point.

## 1.6. Hipótesis.

La aplicación de mecanismos de conectividad en dispositivos Access Point, mejora el rendimiento de redes inalámbricas con alta concurrencia de usuarios.

## 1.7. Identificación de variables.

### 1.7.1. Variable Independiente.

La aplicación de mecanismos de conectividad en dispositivos Access. Point.

### 1.7.2. Variable dependiente.

El rendimiento de las redes inalámbricas con alta concurrencia de usuarios.

## 1.8. Operacionalización de Variables.

**Tabla 1-1:** Operacionalización de Variables.

HIPÓTESIS	VARIABLES	CONCEPTO
La aplicación de	<p><b>Dependiente:</b> El rendimiento de las redes inalámbricas con alta concurrencia de usuarios.</p>	El rendimiento de una red se refiere a las medidas de calidad de servicio de un dispositivo de telecomunicaciones, cuando se conectan gran cantidad de personas a una red.

<p>mecanismos de conectividad en dispositivos Access Point, mejora el rendimiento de redes inalámbricas con alta concurrencia de usuarios.</p>	<p><b>Independiente:</b> La aplicación de mecanismos de conectividad en dispositivos Access Point.</p>	<p>Aplicación o ejecución de reglas o protocolos para la conectividad de red inalámbrica como: Último protocolo WIFI, lugar físico, canal de señal, interferencias, alcance de señal, ancho de banda.</p>
--	--	---

**Realizado por:** Edgar Ulloa.

### 1.9. Matriz de Consistencia.

**Tabla 2-1:** Matriz de consistencia.

Hipótesis General	Variables	Indicadores	Índices	Técnicas	Instrumentos
La aplicación de mecanismos de conectividad en dispositivos Access Point, mejora el rendimiento de redes inalámbricas con alta concurrencia de usuarios.	<p><b>Dependiente.</b></p> <p>El rendimiento de las redes inalámbricas con alta concurrencia de usuarios.</p>	<ul style="list-style-type: none"> <li>• Número de usuarios conectados.</li> <li>• Pruebas de velocidad de transmisión.</li> <li>• Pruebas uso del canal.</li> <li>• Pruebas uso de frecuencia.</li> <li>• Intensidad de Señal.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Porcentaje de ocurrencia de conexiones</b> = <math>\frac{\text{Total de conexiones detectadas}}{\text{Total de conexiones estimadas}}</math></li> <li>• <b>Porcentaje de utilización del medio</b> = <math>\frac{\text{Ancho de banda utilizado}}{\text{Ancho de banda existente}}</math></li> </ul>	<p>Pruebas.</p> <p>Toma de datos.</p> <p>Captura de tráfico.</p> <p>Observación.</p>	<p>Software:</p> <p>Cisco 8500 Series Wireless Controller.</p> <p>Cisco Prime Infrastructure.</p> <p>Speed Test.</p> <p>Wi-Fi analyzer.</p> <p>AP Cisco.</p> <p>SPSS.</p>
	<p><b>Independiente.</b></p> <p>La aplicación de mecanismos de conectividad en dispositivos Access Point.</p>	<ul style="list-style-type: none"> <li>• Análisis.</li> <li>• Precisión.</li> <li>• Ejecución.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Tasa de disponibilidad</b> = <math>\frac{\text{mecanismos de conectividad utilizados}}{\text{mecanismos de conectividad existentes}}</math></li> <li>• <b>Tasa de Precisión</b> = <math>\frac{\text{mecanismos eficaces}}{\text{mecanismos utilizados}}</math></li> <li>• <b>Tiempo de Respuesta</b> =</li> </ul>	<p>Pruebas.</p> <p>Medición.</p> <p>Observación</p> <p>Análisis.</p>	<p>Software:</p> <p>Cisco 8500 Series Wireless Controller.</p> <p>Cisco Prime Infrastructure.</p> <p>Speed Test.</p> <p>Wi-Fi analyzer.</p> <p>AP Cisco.</p> <p>SPSS.</p>

			$\frac{\text{Tiempo de respuesta desde la petición de usuario}}{\text{Tiempo de respuesta esperado}}$		
--	--	--	---	--	--

**Realizado por:** Edgar Ulloa.

## CAPÍTULO II

### 2. MARCO TEÓRICO

#### 2.1. Antecedentes del problema

En la actualidad se han encontrado los siguientes trabajos de investigaciones afines con el tema, para la propuesta de solución se puntualiza lo más notable de cada uno de ellos.

En el repositorio de Science Direct, reposa el siguiente Paper bajo el título “Predicción basada en el contexto de la demanda de puntos de acceso en redes WIFI” representada por los señores David Rodríguez Lozano, Juan A. Gómez Pulido, José M. Lanza Gutiérrez, Arturo Duran Domínguez, Ramón A. Fernández Díaz, en el año 2017.

“Las redes inalámbricas son infraestructuras insustituibles, ambientes donde estudiantes, profesores y empleados interactúan con la red para fines académicos y de investigación. Son tan importantes que las instituciones y empresas invierten constantemente para mejorar la cobertura, el ancho de banda, las latencias, la seguridad, la energía y los consumos, entre otros parámetros de calidad de servicio. Las infraestructuras inalámbricas son generalmente monitoreadas y controladas por software, estas son soluciones para gestionar los usuarios y los recursos, tales como los puntos de acceso inteligentes” (*Rodríguez-Lozano, Gómez-Pulido, Lanza-Gutiérrez, Duran-Domínguez, & Fernández-Díaz*).

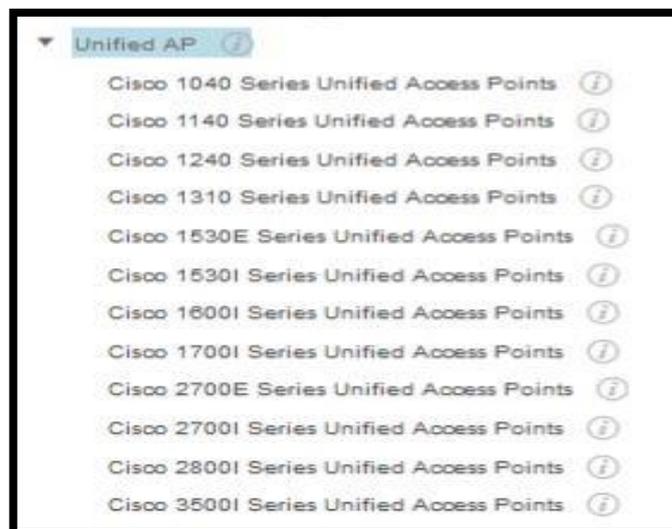
En el repositorio de Science Direct, reposa el siguiente Paper bajo el título “Analizando la solidez de una serie de puntos de acceso inalámbrico a interferentes de dispositivos móviles” representada por los señores David Schweitzer, Ruholla Jafari Marandi, Hugh Medal, en el año 2017.

“A través de otros experimentos se ha llegado a la conclusión de que la potencia total de la señal de una red inalámbrica sigue una curva en forma de S a medida que aumenta el número de emisores de interferencias y puntos de acceso. También se logró notar que el aumento de los puntos de acceso sólo mejora la robustez de la red por primera vez. Además, los casos de problemas en una red tienen una intensidad de señal entre el 39% y el 69%, lo que indica que el valor de los parámetros de interferencia y puntos de acceso (por ejemplo, número de emisores de interferencias, el número de períodos de tiempo) tienen un efecto sobre la intensidad de señal” (*Schweitzer, Jafari-Marandi, & Medal, 2017*).

De acuerdo a lo indagado en Ecuador, se cuenta con infraestructura establecida para el progreso de comunicación tecnológica inalámbrica y a diferencia de las redes cableadas, las redes inalámbricas tienden a ser altamente afectadas por las interferencias del medio, esto es provocado porque las señales transitan libremente, es decir al tener diversas señales compartiendo el mismo espacio existen colisiones de señal que afecta la calidad del servicio, esto ocasiona que cuando más lejos se encuentre de un punto de acceso a internet, más tiempo demora en descargar la información solicitada, por ende se requiere de una mejor y más robusta tecnología para mantener un buen servicio. Detrás de estos inconvenientes existen varias aplicaciones técnicas, además de otros problemas como la seguridad y la estabilidad (Arcotel 2017, p. 22).

Las complicaciones presentadas son debido al desconocimiento del uso correcto de dispositivos inalámbricos, las generalidades de estos inconvenientes se deben a fallas en la configuración de equipos como Enrutadores y Access Point. Entre estas dificultades se tiene la caída de la red, sea esta parcial o en su totalidad, el impedimento de conectar equipos a través de un adaptador inalámbrico, equipos conectados de manera inalámbrica los cuales no pueden acceder a sus recursos compartidos.

En la Universidad Central del Ecuador conforme a los datos obtenidos mediante la herramienta Cisco 8500 Series Wireless Controller se puede estipular que esta Institución posee una red inalámbrica de gran envergadura. La misma que cuenta con alrededor de 766 Access Point (AP) en diferentes modelos mostrados en la Figura 1-2.



**Figura 1-2:** Modelos de APs Cisco existentes en la Red Inalámbrica UCE.

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

Existen varios factores que indican escaso rendimiento en los Access Point como lo es la intensidad de la señal, que está en un rango de alrededor 7700 números de clientes en -65 RSSI (dBm) como intensidad de señal alta y alrededor de 1500 números de clientes en -75 RSSI (dBm) con intensidad de señal baja. Ver Figura 2-2.



**Figura 2-2:** Calidad de la Conexión – Intensidad de Señal.

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

Estos cálculos se establecen en base a la interpretación de valores del indicador de fuerza recibida RSSI donde:

“En una escala de 0 a -80 RSSI:

- 0: señal ideal, casi imposible de lograr.
- -40 a -60: señal eficiente con tasas de transmisión estables.
- -60: señal buena; ajustando la transmisión se logra una conexión al 80%.
- -70: señal media/baja; emite una señal regularmente buena.
- -80: señal mínima tolerable para una conexión. Suelen acontecer caídas que serían cortes de comunicación (pérdida de llamadas, datos y mensajes descompuestos).

El rango de valores presentados varía entre fabricantes y no están del todo estandarizados” (RSSI, 2019).

Tabla 1-2 de equivalencias aproximada para el nivel de cobertura en función de los dBm en aire:

**Tabla 1-2:** Equivalencias de intensidad de señal en dBm.

Intensidad de la señal - medido en dBm	Valoración

-30 dBm	Excelente
-67 dBm	Muy Bueno
-70 dBm	Bueno
-80 dBm	No es bueno
-90 dBm	Inutilizable

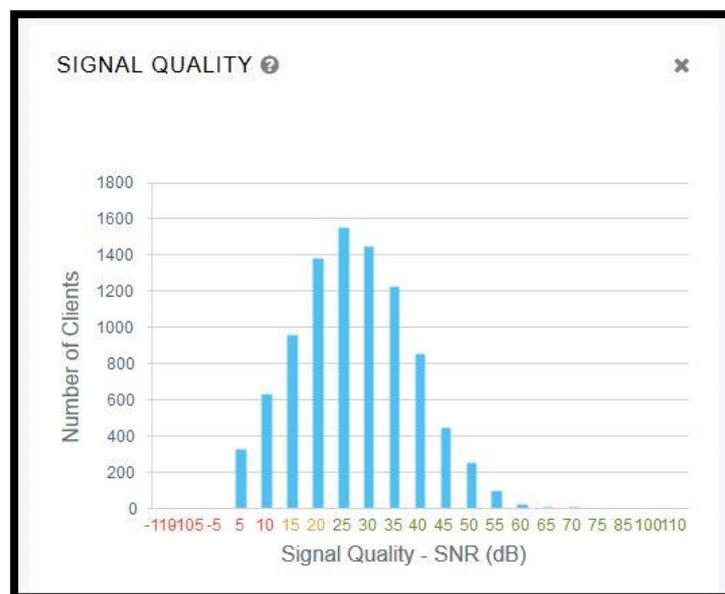
Fuente: RSSI, 2019.

Realizado por: RSSI, 2019.

Ligado a la intensidad de la señal se tiene en consideración la calidad de la conexión que es una medida de ingeniería electrónica que define la relación entre la potencia de una señal con la potencia del ruido que la corrompe (Garai, J, 2019). En general cuando el intervalo de la señal es más alto que el intervalo del ruido, la señal es más clara. Es decir, la Universidad Central del Ecuador también presenta un rango de calidad de señal medio como se puede ver en la figura 3-2, datos que son tomados de la herramienta Cisco 8500 Series Wireless Controller.

SNR o RUIDO:

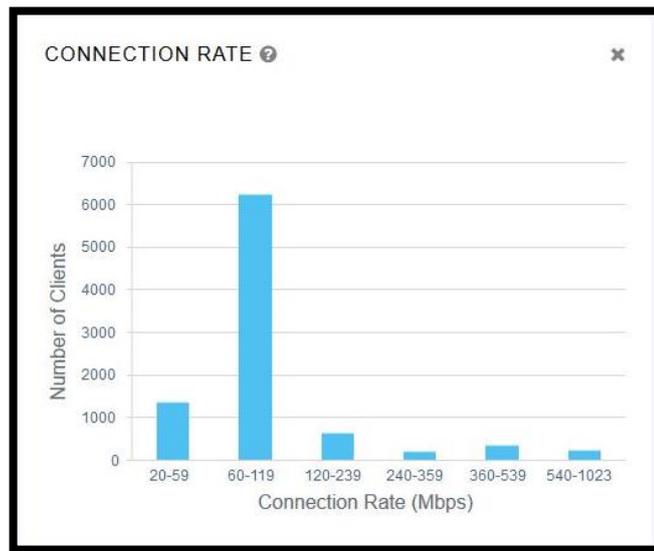
- 6dB o menos es terriblemente malo. Percibe problemas intermitentes de sincronismo.
- 7dB a 10dB señal aceptable.
- 11dB a 20dB señal buena, mínimos o sin problemas de sincronismo.
- 20dB a 28dB señal excelente.
- 29dB o más es asombroso.



**Figura 3-2:** Calidad de la Señal versus Ruido.

Fuente: Dirección de Tecnologías de la Información y Comunicación (UCE).

Otro factor importante e influyente en el rendimiento de los Access Point es la tasa de conexión existente en la Universidad Central del Ecuador que no es más que la velocidad a la que navega cada dispositivo dentro de la red inalámbrica y que de acuerdo a la toma de datos se encuentra en un rango de 6100 conexiones a una velocidad de 60 a 119 Mbps como se puede ver en la Figura 4-2.



**Figura 4-2:** Tasa de Conexión.

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

En la institución a investigar se puede ver varios modelos de Access Point, pero los datos obtenidos se toman centrándose en los dispositivos Access Point internos con antenas Cisco Aironet 2700 series y los Access Point sin antenas Cisco Aironet 1700 series los cuales se observan en la Figura 5-2.



**Figura 5-2:** APs Cisco con antena Aironet 2700 y sin antena Aironet 1700.

**Fuente:** Cisco datasheet AIR CAP 1702I.

Una vez expuestos los elementos antes mencionados se puede decir que en el presente proyecto de investigación se observan todos los datos que intervienen en el rendimiento de Access Point, dichos datos han sido obtenidos en la Universidad Central del Ecuador - Dirección de Tecnologías de la Información y Comunicación con el fin de conocer las formas y mecanismos de conexión que tiene esta Institución, siendo las de más realce las siguientes: protocolos de seguridad utilizados (WPA2 con PSK y WPA2 Enterprise con 802.1x), frecuencias (2.4GHz y 5GHz), estándares (802.11 A-B-G-N-AC), estas formas de conexión utilizadas en esta Institución permiten la selección más eficiente de los Mecanismos de Conectividad con el fin de solucionar las falencias del rendimiento de la red inalámbrica (AP), tomando como referencias el rendimiento versus concurrencia de usuarios o el rendimiento versus intensidad de señal.

Analizadas las referencias antes mencionadas se puede establecer mecanismos de conectividad que ayuden a la identificación y mejora del bajo rendimiento de dispositivos Access Point, además hay que considerar que el rendimiento de una red se refiere a las medidas de calidad de un servicio por lo tanto se debe elegir mecanismos de conectividad que ayuden a establecer resultados y posean internamente ciertos indicadores o parámetros medibles como por ejemplo Ancho de banda, el throughput, la latencia, Jitter, la tasa de error y la intensidad de señal, viendo desde un punto técnico los mecanismos de conectividad que se acoplan a estas medidas serían los estándares más actuales y utilizados por la institución, es decir, el estándar **IEEE 802.11n** en comparación con el estándar **IEEE 802.11ac**.

Cabe mencionar que en esta institución se manejan varios de los estándares existentes como: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac estas conexiones se establecen dependiendo de los dispositivos que se conectan a la red inalámbrica ya que no todos los dispositivos poseen en su tarjetería las 2 frecuencias (2.4GHz y 5GHz) ni los estándares más actuales.

## **2.2. Bases teóricas.**

### **2.2.1. Redes de comunicaciones.**

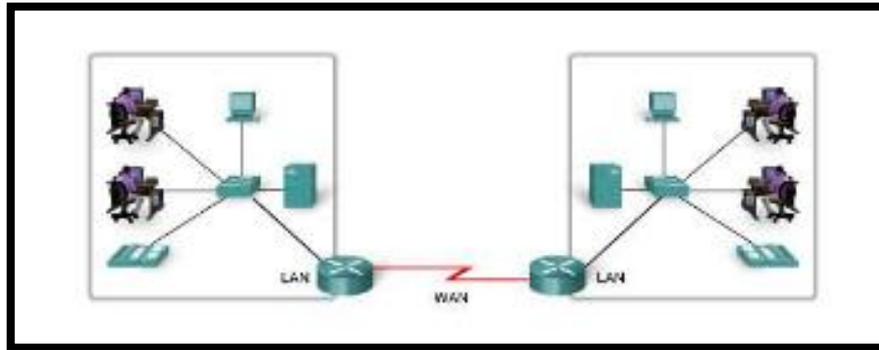
“Es un conjunto de elementos con características comunes interconectadas o conectadas a través de un medio físico común, con el objetivo de compartir y optimizar recursos a través de una disposición física en particular” (*Cidecam M, 2019*). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.).

“Los factores que aseguran el envío de los mensajes y la información en la red de datos son los medios de networking que conectan los dispositivos de red y los acuerdos y estándares que rigen su funcionamiento. A medida que crece la demanda para que más personas y dispositivos se comuniquen en un mundo móvil, las tecnologías de red de datos tendrán que adaptarse y desarrollarse” (*Cidecam M, 2019*).

### **2.2.2. Redes WAN.**

Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, la instalación y el mantenimiento de los mismos son aptitudes complementarias de la función de la red de una organización.

Las LAN y las WAN son muy útiles para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de correos electrónicos, capacitación corporativa y acceso a recursos (*Cidecam M, 2019*).



**Figura 6-2:** Redes WAN.

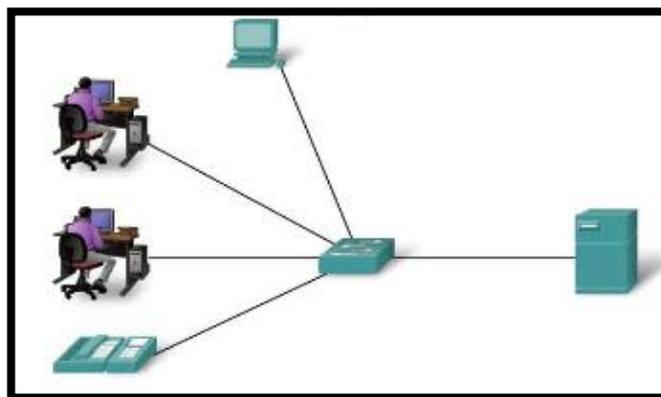
Fuente: Cidecam M, 2019.

### 2.2.3. Redes LAN.

Las infraestructuras de red pueden variar en gran medida en términos de:

- El tamaño del área cubierta.
- El número de usuarios conectados.
- El número y los tipos de servicios disponibles.

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina Red de área local (LAN). Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red (Cidecam M, 2019).

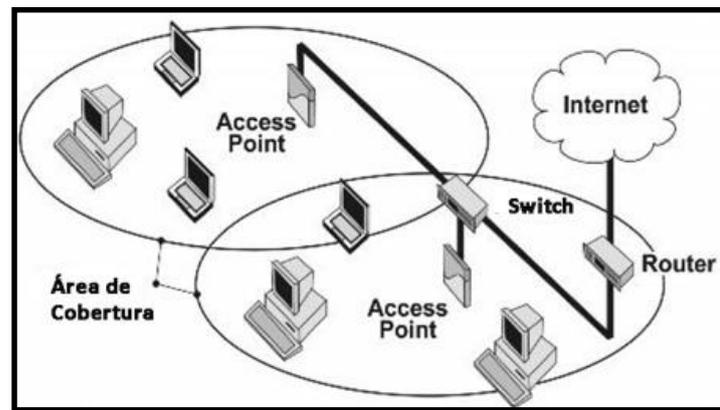


**Figura 7-2:** Redes LAN.

Fuente: Cidecam M, 2019.

#### 2.2.4. Redes inalámbricas.

“Se le llama red inalámbrica a la conexión de varios dispositivos inalámbricos o nodos que comparten información a través de ondas electromagnéticas, es decir, no dependen de una red cableada, el envío y recepción de datos se realiza a través de puertos” (Vallejo A, 2017). Las redes inalámbricas se han expandido gracias a que los costos son reducidos, porque evita la utilización de grandes cantidades de cableado ethernet y conexiones físicas entre nodos, entre sus desventajas se tiene la falta de seguridad, exigiendo que esta sea más robusta para evitar ataques o intrusos en la red.



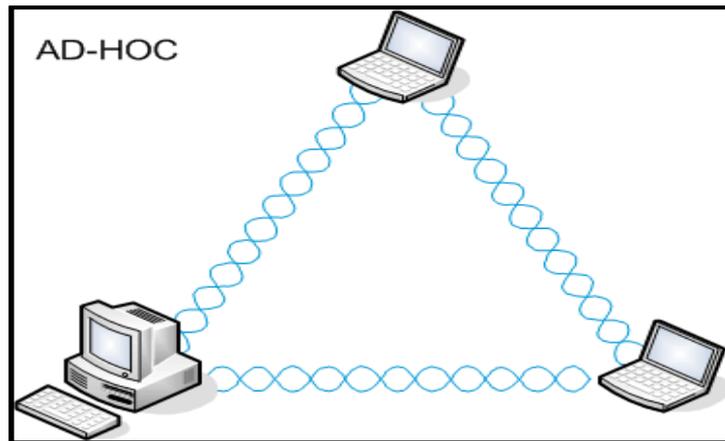
**Figura 8-2:** Red Inalámbrica.

Fuente: Vallejo A, 2017.

##### 2.2.4.1. Topologías de redes inalámbricas.

Referentes a las topologías de redes inalámbricas tenemos tres tipos relevantes:

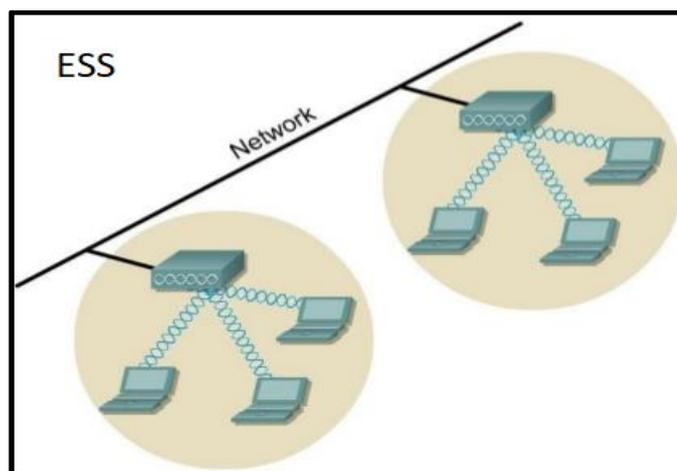
- La topología AD-HOC, es una conexión temporal que define a un conjunto de computadores que se conectan directamente sin requerir de un punto de acceso (AP) (Modo Ad – Hoc, 2019).



**Figura 9-2:** Topología AD-HOC.

Fuente: Modo Ad – Hoc, 2019.

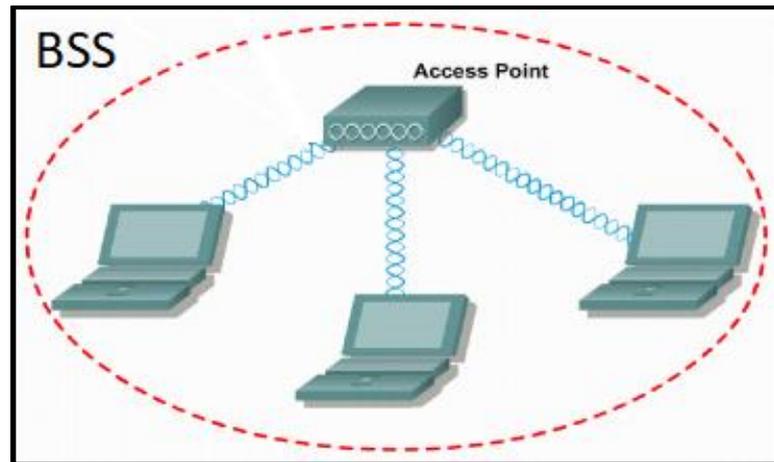
- La topología ESS, esta configuración permite unir varios puntos de acceso (AP) con el objetivo de crear una amplia cobertura de red inalámbrica (*Topologías inalámbricas, 2019*).



**Figura 10-2:** Topología ESS.

Fuente: Topologías inalámbricas, 2019 - Luis Ruiz Barcayola.

- La topología BSS, en la cual vamos a centrar esta investigación, trata acerca de la configuración donde se necesita disponer de un depósito central llamado Punto de Acceso (AP), el cual llevará la comunicación entre los distintos terminales de la red (*García, P. 2011*).



**Figura 11-2:** Topología BSS.

Fuente: Recalde, 2019.

Esta última topología es la de mayor uso o demanda dentro de instituciones y empresas que cuentan con una infraestructura de red de gran tamaño, porque con esta topología de red se puede realizar una cobertura más amplia, logrando cubrir la demanda de usuarios existentes y brindándoles servicio en todo el espacio físico de cobertura (Recalde, 2019).

### 2.2.5. Dispositivos Inalámbricos.

En la actualidad se ha dado una tendencia por eliminar los cables en los dispositivos tecnológicos, debido a esto nacieron las redes inalámbricas, con dispositivos que no necesitan cables y se manejan a distancias mediante señales electromagnéticas. Entre los dispositivos más usados tenemos los siguientes:

- Puntos de Acceso (AP) son dispositivos a través de los cuales las estaciones Wireless pueden conectarse de una manera rápida y fácil a una red inalámbrica, éstos son los que serán objeto de esta investigación.
- Bridge Inalámbrico son dispositivos que se usan para realizar la comunicación entre dos o más redes con el fin de conectar diferentes edificios. Este brinda velocidades elevadas de datos y llega a sitios difíciles de cablear.
- Enrutador Inalámbrico son dispositivos de comunicación inalámbrica en la que permite guiar los paquetes de datos a su destinatario correcto.

- Adaptadores son tarjetas que sirven para la comunicación inalámbrica, poseen una antena la cual permite la recepción y transmisión de datos.

### 2.2.6. Access Point.

Es un dispositivo de red inalámbrica y su función principal es interconectar en red varios equipos, tales como celulares, computadores portátiles, Tablet, etc., es decir, establecer una red local inalámbrica que conecta dispositivos móviles y equipos con tarjetas de red inalámbricas. Por lo general está conectado a una red cableada que le permite el acceso a internet y mediante esta distribuye el servicio de internet a los dispositivos inalámbricos (Pazmiño A, 2011, p. 53).

Es el dispositivo inalámbrico en el que se centrará la investigación, se trata de un dispositivo de capa dos por el cual las frecuencias Wireless pueden integrarse rápida y fácilmente a cualquier red cableada, este puede actuar de punto central de una red inalámbrica independiente, además que se usa como punto de conexión entre redes inalámbricas y cableadas.

**Tabla 2-2:** Características WLAN Access Point.

Característica	Descripción
Capa Física	Espectro ensanchado por secuencia directa (DSSS), Espectro ensanchado por salto de frecuencia (FHSS), Multiplexación por división de frecuencias ortogonales (OFDM), Infrarrojos (IR).
Seguridad de Datos y Red	Se basa en el algoritmo de cifrado RC4 para confidencialidad, autenticación e integridad. Se limita por la administración de claves.
Banda de Frecuencia	2.4 GHz y 5GHz
Tasa de Transferencia	1 Mbps, 2Mbps, 5.5 Mbps, 11 Mbps, 54 Mbps
Rango de Operación	100 metros
Aspectos Positivos	Se obtiene una velocidad de Ethernet sin usar cables, una variedad de productos y compañías, los costos están disminuyendo.
Aspectos Negativos	Poca seguridad, la tasa de transferencia disminuye con la distancia y carga.

**Fuente:** Suárez Gutiérrez, 2019, p. 10.

**Realizado por:** Manuel Suárez Gutiérrez

### **2.2.7. Esquema de configuración de AP.**

El esquema de configuración de dispositivos inalámbricos Access Point (AP) serán establecidos de acuerdo a las especificaciones técnicas de cada producto y a las estaciones que se tiene modeladas y montadas en el escenario digital, además se tomará como estación de pruebas reales a los ambientes que se tiene dentro de la institución a investigar.

Todo esto con el fin de realizar pruebas minuciosas del posicionamiento físico, ya que la adición de algunos AP podría cambiar drásticamente el rendimiento de los más lejanos, es decir, se requiere evidenciar que los mismos fenómenos aparecen mientras se cambia el número de estaciones por AP (*Ducourthial, Mottelet, & Busson*).

Además de buscar la correcta configuración de los dispositivos, orientándose siempre al fortalecimiento de los dispositivos inalámbricos en redes amplias con alta concentración y concurrencia de usuarios.

### **2.2.8. Análisis Tecnología Wifi.**

Esta tecnología basada en el estándar 802.11, permite su comunicación por ondas electromagnéticas en varios rangos de frecuencias, que se propagan en el aire, han contribuido decisivamente al desarrollo de tecnologías de comunicación. Ejemplos representativos de estas son: Wifi y la óptica de espacio libre, utilizando microondas y luz láser. Su importancia y utilización han ido en aumento por su versatilidad, movilidad y precios favorables.

La importancia y la utilización de Wifi han ido creciendo para complementar redes cableadas tradicionales. Wifi es considerado el más importante en el contexto de las organizaciones que poseen grandes redes. En este caso un punto de acceso, permite comunicaciones de dispositivos electrónicos Wifi con una red de área local cableada, a través de un enrutador. La red de área local inalámbrica (WLAN) surge basada en un Access Point. Wifi ha tomado un posicionamiento a nivel de redes personales, donde estas redes inalámbricas (WPAN) permite que los dispositivos personales se comuniquen punto a punto y las configuraciones punto a multipunto se utilicen tanto en interiores como en exteriores, con funciones direccionales y omnidireccionales específicas, las antenas Wifi utilizan microondas en las bandas de frecuencia de 2,4 y 5 GHz, además del estándar IEEE 802.11a, 802.11b, 802.11g, 802.11n, entre otros. (*Pacheco de Carvalho, Veiga, Ribeiro Pacheco, & Reis, 2013*).

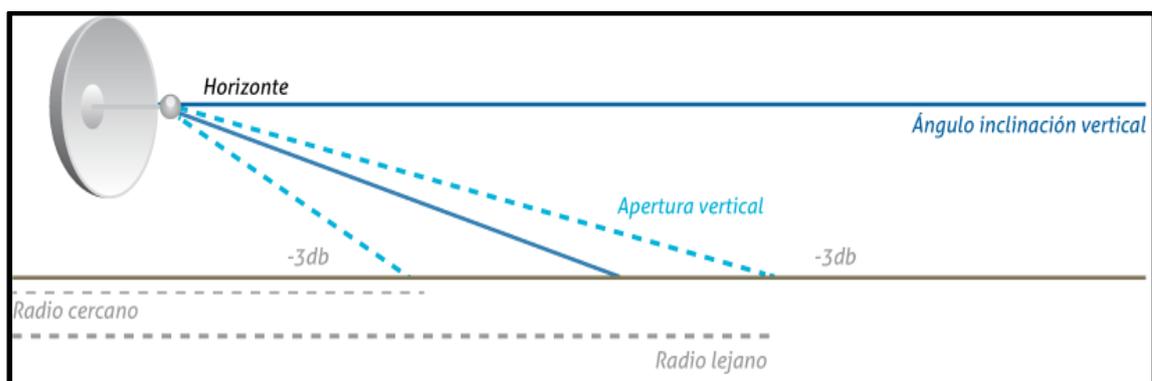


**Figura 12-2:** Red Inalámbrica (Wifi).

**Fuente:** Datacraft, 2019.

### 2.2.9. Cobertura de radio.

Es de mucha importancia conocer el alcance que tiene los dispositivos inalámbricos, ya que existe variación en las diferentes marcas y modelos. Por tal motivo se debe considerar que se requieren dispositivos inalámbricos diferentes para cada ambiente dentro de un establecimiento, siendo el objetivo principal de estos abastecer de cobertura a toda una organización (*Radio de cobertura Wifi, 2019*).



**Figura 13-2:** Cobertura y alcance de radio.

**Fuente:** Radio de cobertura Wifi, 2019.

### **2.2.10. Equipamiento de cobertura.**

Se determina a partir de la cobertura de radio con la que cuentan los diferentes equipos inalámbricos que son utilizados en una red de gran tamaño, para tener una referencia de los dispositivos existentes y los dispositivos que se usan en redes inalámbricas de gran tamaño, se indicarán algunos de estos dispositivos: Puntos de Acceso, Bridge Inalámbrico, enrutadores inalámbricos y adaptadores.

Cuando se trata de dar una excelente cobertura inalámbrica, los Access Point son los más adecuados para esta función ya que están específicamente creados para satisfacer coberturas grandes de señal inalámbrica.

### **2.2.11. Estándares de telecomunicaciones.**

“Un estándar de telecomunicaciones es un conjunto de normas, especificaciones y recomendaciones técnicas, así como el organismo de estandarización IEEE benefició en el ámbito de las redes inalámbricas con una variedad de especificaciones para este tipo de comunicación. El estándar IEEE 802.11 trabaja en la capa física y en la capa de enlace de datos del modelo OSI, implantando normas para el correcto desempeño y funcionalidad de las redes inalámbricas, en la actualidad existen varios protocolos, estos han ido evolucionando en nuevas adaptaciones para mejorar las funcionalidades de los dispositivos” (Betancourt S, 2016, p. 24).

#### **2.2.11.1. Estándares IEEE 802.11.**

“El estándar 802.11 en realidad es el primer estándar y permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda (también en los estándares 802.11a, b y g, llamados estándares físicos 802.11) o para especificar componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad” (Pillou J, 2019).

A continuación, en la Tabla 3-2 se muestra el estándar 802.11 con las variaciones respectivas a través de sus nuevas versiones:

**Tabla 3-2: Estándares Tecnología Wifi.**

Estándar	Nombre	Descripción
802.11a	wifi5	El estándar 802.11 (llamado wifi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps, aunque en la práctica es de 30 Mbps). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	wifi	El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Itinerancia	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.
802.11g		El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps, pero de 30 Mbps en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa

		que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h		El estándar 802.11h tiene por objeto unir el estándar 802.11 con el estándar europeo (Híper LAN 2, de ahí la h de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i		El estándar 802.11i está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.

Fuente: Pillou, 2019.

### **Estándar IEEE 802.11N**

Reconocido por la organización IEEE el 11 de septiembre del 2009 y también conocido como WIFI 4 creada para mejorar el rendimiento de la red con respecto a sus antecesores el estándar 802.11b y 802.11g, con una ampliación significativa en la velocidad máxima de transmisión de 54Mbps a un máximo de 600Mbps, trabaja en las bandas de frecuencias de 2.4GHz y 5GHz, también incorpora Múltiple-Input Múltiple-Output (MIMO) y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC.

MIMO en el estándar 802.11N es la tecnología que permite el uso de múltiples antenas transmisoras y receptoras de información, los beneficios de MIMO son optimizar el desempeño de la red facilitando manejar grandes cantidades de información a través de la diversidad de antenas y el multiplexado espacial. Además, usa diversas señales multi ruta para acrecentar la destreza del receptor de recobrar los mensajes de la señal.

Channel Bonding o unión de interfaces (40MHz) en el estándar 802.11N es la segunda tecnología añadida y mediante la cual utiliza dos canales separados o dos bandas adyacentes de 20MHz para transmitir datos simultáneamente, haciendo que se pueda duplicar la velocidad de la capa física disponible en un solo canal de 20MHz (Herrera Ramírez, Díaz Ramírez & Calafate, 2019).

### **Estándar IEEE 802.11AC**

El nuevo estándar inalámbrico 802.11ac tiene por objetivo garantizar una mayor velocidad a la red inalámbrica, con un aumento en la eficiencia del 10% y un consumo de energía menor, provee

un alcance mayor a velocidades Gigabit Ethernet. El estándar 802.11ac basa su éxito en el ya popular 802.11n, trayendo consigo mejoras en velocidad y escalabilidad, al combinar la tecnología inalámbrica con la capacidad Gigabit Ethernet (MX, 2019).

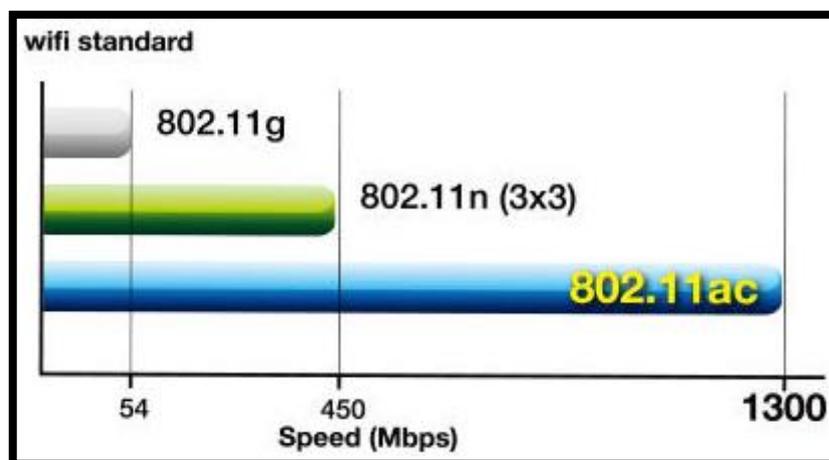
El aumento de velocidad en el estándar 802.11ac se logra gracias a las siguientes características:

**Aumento en los canales:** El ancho de canal para la transmisión en el estándar 802.11n tiene un máximo de 40MHz, y ahora el estándar 802.11ac lo incrementa hasta 80MHz o incluso hasta 160MHz, aumentando aún más la velocidad de datos por cada radio (MX, 2019).

**Incremento en la modulación:** El estándar 802.11ac ahora emplea 256QAM (Modulación de amplitud en cuadratura, por sus siglas en inglés, Quadrature Amplitude Modulation), lo que significa altas tasas de transferencia de datos (MX, 2019).

**Multi-user MIMO (MU-MIMO):** Soporte de transmisiones simultáneas a múltiples clientes, maximizando la utilización de la banda RF (MX, 2019).

El estándar 802.11ac opera únicamente en la banda de los 5GHz donde hay menos ruido e interferencia de tecnologías competidoras. Además, en esta banda hay mucho espacio disponible, lo que permite aumentar el número de canales de flujo en esta banda, a diferencia de los tres existentes en el 802.11n (MX, 2019).



**Figura 14-2:** Comparación entre estándares.

Fuente: MX, 2019.

### 2.2.12. Bandas de Frecuencias Tecnología Wifi.

Los estándares 802.11 A-B-G-N-AC también llamados estándares físicos, son modificaciones del estándar 802.11 y operan en frecuencias diferentes las cuales son 2.4GHz y 5GHZ, “lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos o distancias” (Pillou J, 2019). Cabe mencionar que en la actualidad existes nuevos estándares como el 802.11ac que funciona con conexiones de hasta 1300Mbps, opera en la banda de 5GHz.

**Tabla 4-2:** Frecuencia Tecnología Wifi.

Estándar	Banda de Frecuencia	Velocidad	Rango
802.11a	5 GHz	54 Mbps	10 m
802.11b	2,4 GHz	11 Mbps	100 m
802.11g	2,4 GHz	54 Mbps	100 m
802.11n	2.4GHz y 5GHz	600 Mbps	100 m
802.11ac	5 GHz	1300 Mbps	100 m

Fuente: Pillou, 2019.

#### 2.2.12.1. Banda de Frecuencia Wifi 2.4GHz y 5GHz.

Algunas características que identifican a “Ambos tipos de Wifi están en sus canales, el estándar, el rango de red, la velocidad y las interferencias. También es importante saber que es posible que algunos dispositivos antiguos sólo capten la señal de 2.4GHz, ya que es la que más tiempo lleva siendo utilizada, mientras que la 5GHz es relativamente nueva” (FM Y, 2019).

**Wifi 2.4 GHz**, al ser la más utilizada suele tener mayor número de interferencias, además tiene menor velocidad máxima de conexión, alcanzando por lo general velocidades de 50 o 60 Mbps como máximo. Es decir que las redes Wifi de 2.4 GHz son más lentas, pero alcanzan más distancias o poseen mejor rango de cobertura.

**Wifi 5 GHz**, “Que al ser menos utilizada tiene menos interferencias, por lo que la conexión debería ir mucho más ágil cuando se conecta a ella. También tiene más canales para que los dispositivos tengan más espacio en el que repartirse, alcanza velocidades cercanas a los 867 Mbps,

Sin embargo, las redes Wifi 5 GHz también tienen menor rango de cobertura, y tienen mayor problema para superar obstáculos como paredes” (FM Y, 2019).

**Tabla 5-2:** Diferencias de frecuencias 2.4 GHz y 5GHz.

<b>Diferencias</b>	<b>2.4GHz</b>	<b>5GHz</b>
<b>Canales</b>	14 canales no superpuestos	25 canales no superpuestos
<b>Interferencias</b>	Mayor Interferencias	Menor interferencias
<b>Velocidad Máxima</b>	Menor velocidad de conexión	Mayor velocidad de conexión
<b>Rango de Red</b>	Mayor rango	Menor rango
<b>Estándar</b>	IEEE 802.11b, 802.11g, 802.11n	IEEE 802.11a, 802.11n, 802.11ac

Fuente: FM Y, 2019.

#### 2.2.12.2. Capacidad del canal wifi.

Los canales wifi trabajan de forma diferente según la banda de frecuencia que se encuentren, dicho esto se tiene las bandas de frecuencia de 2.4GHz y 5GHz.

“La mayoría de Access Point transmiten en la banda de 2,4 GHz, que es la tradicional y con la que todos los móviles son compatibles. Esta va desde los 2.412 MHz hasta los 2.472 MHz y se divide en 13 canales. Estos 13 canales se reparten un espectro de 100 MHz, pero cada uno tiene 20 MHz, por lo que si se hace una evaluación numérica no salen las cuentas. A no ser que estos canales se solapan entre ellos. Pues si es exactamente lo que pasa. Los canales se solapan entre sí, de forma que cada canal ocupa una parte del espectro de los subyacentes” (Nieto, 2019).

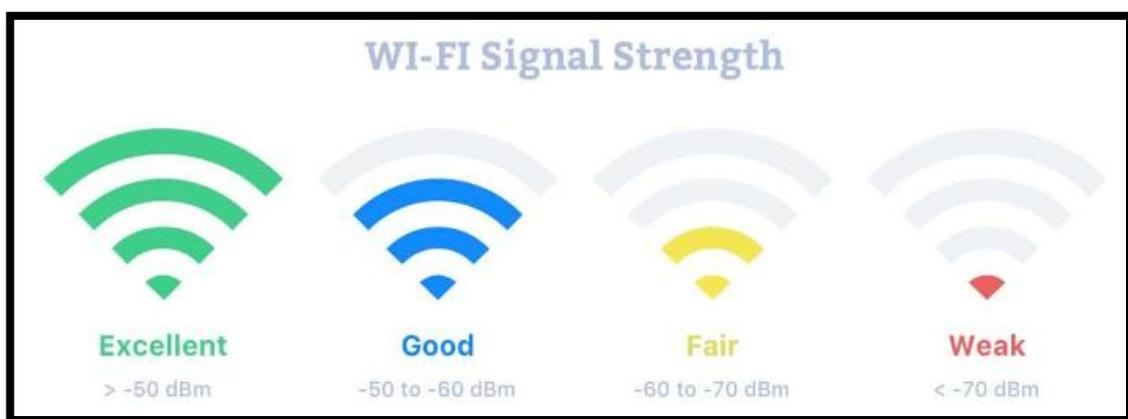
#### 2.2.13. Intensidad de la señal.

Son mediciones de RSSI y “Representan la calidad relativa de una señal recibida en un dispositivo, RSSI indica el nivel de potencia que se recibe después de cualquier posible pérdida en el nivel de antena y cable. Cuanto mayor sea el valor RSSI, más fuerte será la señal. Cuando

se mide en números negativos, el número que está más cerca de cero normalmente significa mejor señal# (Net Spot, 2019).

Como ejemplo se define que -50 dBm es una señal muy buena, -75 dBm es una señal razonable, y -100 dBm no emite ninguna señal. A pesar de que RSSI y dBm son unidades de medida diferentes, ambos muestran la intensidad de la señal. El dBm es una correlación de la potencia medida como referencias a un mW (miliwatt).

“Para la señal significativa de buena calidad de medición ha de sustraer el ruido de la línea de la potencia de la señal. Una mayor diferencia de señal a ruido significa una mejor intensidad de señal” (Net Spot, 2019).



**Figura 15-2:** Intensidad de señal.

Fuente: Net Spot, 2019.

Es de suma importancia analizar el esquema de infraestructura para ubicar los dispositivos inalámbricos e iniciar pruebas de potencia de señal para verificar que distancia alcanzan realmente pasando por alto las especificaciones técnicas del producto, si las interferencias por otros APs instalados fuera de la red UCE causan bajo rendimiento. Una vez establecidos estos datos y mediante software y hardware se analizará las ventajas y desventajas en las redes amplias con concurrencia de usuarios.

#### 2.2.14. Internet.

Con respecto a la evaluación del rendimiento en la Universidad Central del Ecuador, el internet es uno de los principales beneficios que se obtendría con las mejoras de este, siendo que el internet proviene del acrónimo **INTER**connected **NET**works y se le conoce como una red de redes, es decir que interconecta redes de computadoras entre sí mediante algún medio como cable coaxial, fibra,

óptica, radiofrecuencia, líneas telefónicas, entre otras. Además de ser un método de interconexión descentralizada, implementada en un conjunto de protocolos TCP/IP (Arranz, 2007).

#### 2.2.14.1. Datos.

“Para llegar a determinar el significado del término Dato, es importante dejar claro su origen etimológico. En concreto, podemos establecer la siguiente información al respecto: Datos, Esta palabra es fruto de la evolución de la palabra latina “datum”, que puede traducirse como dado” (Pérez Porto & Merino, 2019).

“Dato es una expresión que indica una información, un documento o un testimonio que permite alcanzar un conocimiento o deducir las consecuencias legítimas de un hecho. Por lo tanto, se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos” (Pérez Porto & Merino, 2019).

“Además, una red de datos se pone en funcionamiento con otros dos objetivos primordiales: compartir tanto el software como el hardware y otorgarle soporte y centralización a la administración pertinente” (Pérez Porto & Merino, 2019).

Al igual, al ponerla en marcha se logra optimizar notablemente la rapidez y fiabilidad de la compensación de información y minimizar costes en las empresas o entidades que opten por implementarlas.

#### 2.2.14.2. Rendimiento.

El rendimiento de una red tiene que ver con la calidad del servicio que este provee a los clientes asociados de dicha red. Para saber que una red está funcionando de manera óptima es medida o cuantificada mediante el cálculo de la velocidad de transmisión de datos, la cantidad de datos que llegan en forma íntegra desde un punto a otro, el tiempo de respuesta y evitando que los paquetes de datos transmitidos perciban interferencias de otros medios.

De acuerdo a ciertos factores de medición en los que intervienen la evaluación del rendimiento de Access Point usando como mecanismos de conectividad los estándares IEEE 802.11N y 802.11AC los mismos que son los más destacados en la Universidad Central del Ecuador y

mediante los cuales se pueden obtener datos relevantes del rendimiento. Las siguientes medidas son frecuentemente consideradas importantes.

#### 2.2.14.3. Ancho de Banda.

En conexiones a Internet el ancho de banda o bandwidth es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (bps), kilobytes por segundo (kbps), o megabytes por segundo (Mbps). En las redes de ordenadores, el ancho de banda a menudo se utiliza como sinónimo para la tasa de transferencia de datos, la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo).

El ancho de banda en redes inalámbricas funciona sobre las bandas de 2.4 GHz y “5GHz, dentro del espacio radioeléctrico. Este espectro está regulado para garantizar la interoperabilidad entre equipos, de tal modo que radio, telefonía móvil y otras conexiones inalámbricas puedan funcionar correctamente. Dentro del Wifi, hay varios canales de diferente amplitud” (González, 2018).

#### 2.2.14.4. Latencia.

“Tiempo que tarda en transmitirse un paquete dentro de la red, y es un factor clave en las conexiones a Internet. En función de la conexión que tengamos, esta latencia será mayor o menor. La latencia influye, por ejemplo, en el tiempo que tarda en cargar una web.

Para medir la latencia, se utiliza el ping, muy conocido sobre todo por aquellos que utilizan los videojuegos online. El ping, medido en milisegundos (o ms) mide el tiempo que tardan en comunicarse una conexión local con un equipo remoto en la red IP. Por ejemplo, en un videojuego de disparos, cuanto menor sea el ping, menos tiempo tardará en registrar el servidor que tú has disparado y que la bala ha alcanzado su objetivo” (Velocidad, 2019).

- “La tecnología de acceso a Internet: ADSL o Fibra.
- La distancia entre los dos puntos que quieran establecer la comunicación, y las redes o saltos intermedios por los que tengan que pasar los paquetes.
- Capacidad del dispositivo desde el que nos conectamos (ordenador, portátil, Tablet, móvil o consola) y la carga del servidor al que nos estamos conectando” (Velocidad, 2019).

#### 2.2.14.5. Tráfico de red.

En una comunicación el tráfico de red es el número de datos que se envían y se reciben o que a su vez viajan a través de un sistema. En un nivel de pequeños fragmentos, los paquetes se reciben y se transmiten mediante los anillos de recepción (Rx) y de transmisión (Tx) de una NIC. Desde estos anillos, los paquetes que se reciben son trasladados a la pila de red para realizar el debido procesamiento y los paquetes salientes son enviados a la red. Con esto se puede medir que tan alto es el porcentaje de utilización de una red.

#### 2.2.14.6. Throughput.

Es la tasa de transferencia efectiva (tamaño neto de trabajo o información que fluye en un sistema) y se refiere a la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación. Este dato puede ser entregado sobre un enlace físico o lógico, o a través de un cierto nodo de la red. Por regla general, el Throughput es medido en bits por segundo (bit/s o bps), y a veces en paquetes de datos por segundo o paquetes de datos por franja de tiempo. Será siempre inferior al ancho de banda disponible y estará controlado por la señal de radio (decibeles) y las limitaciones del hardware. Throughput, es considerado desde el primer bit de información que llega al receptor, para separar el concepto, con la latencia, ya que habitualmente son usados como sinónimos (*Gerometta, 2012*).

Time Window es la unidad en la cual Throughput es medida. La elección de una ventana de tiempo adecuado denominará generalmente los cálculos de Throughput; la latencia afecta en el cálculo de Throughput cuando es tomada en cuenta. Si esta no se incluye no afecta el Throughput.

#### 2.2.14.7. Jitter.

“Se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Las comunicaciones en tiempo real como VoIP son especialmente sensibles a este efecto. Frecuentemente, es un problema en enlaces lentos o congestionados. Se espera que el aumento de mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) puedan reducir los problemas del Jitter en el futuro” (*Voip, 2019*).

#### 2.2.14.8. Pérdida de paquetes.

En una comunicación existen paquetes que contienen la información necesaria para que cuando el destinatario los reciba, sea capaz de ordenar y usar la información.

Sabiendo esto, ya se puede entender que cuando se habla de la pérdida de paquetes se refiere a que uno o más fragmentos de información no han llegado de la forma esperada a su destino, lo que provoca:

- Información desfasada.
- Lentitud de carga.
- Interrupción en las cargas.
- Cierre de conexiones.
- Información incompleta.

Algunas causas habituales de la pérdida de paquetes son las que exponemos a continuación:

- Hardware dañado.
- Capacidad del hardware (cuellos de botella).
- Congestión en la red.
- Wifi.
- Bugs en el software de los dispositivos de red.

#### 2.2.14.9. Pérdidas por obstáculos.

“La madera, los materiales sintéticos y el cristal provocan una pérdida en la intensidad de señal, están catalogados como obstáculos con un potencial de interferencia de nivel bajo. Por encima de estos, el agua, el ladrillo o el mármol, provocan pérdida de 'nivel medio', mientras que en un nivel aún superior están la escayola, el hormigón o el cristal blindado. Además de estos anteriores, que tienen un potencial de interferencia alto, el mayor enemigo de la señal Wifi es el metal, que es el que causa las mayores interferencias y provoca mayores pérdidas de señal” (González C, 2019).

“Otro problema para la velocidad de la red inalámbrica y su señal son el resto de redes Wifi que estén funcionando en un radio próximo. Esto es, sencillamente, porque algunas pueden estar funcionando dentro del mismo canal en el espectro de radiofrecuencias. En ese caso, no sólo se pierde intensidad de señal y se reduce de forma considerable la velocidad de conexión, sino que

también se reduce de forma notable la estabilidad de la red y se puede comprometer su disponibilidad” (González C, 2019).

### **2.2.15. Seguridad.**

Si bien el uso avanzado y óptimo de dispositivos inalámbricos es importante también hay que centrarnos en una configuración que brinde un excelente servicio y que tenga robustez en su seguridad. Ya que por más que se tenga un servicio de calidad, este no serviría de nada si no se mantiene una seguridad alta que impida el ingreso de intrusos en la red.

“Los algoritmos de seguridad Wifi han pasado por muchos cambios y mejoras desde los años 90 para hacerse más seguros y eficaces. Se desarrollaron diferentes tipos de protocolos de seguridad inalámbricos para la protección de redes inalámbricas domésticas. Los protocolos de seguridad inalámbrica son WEP, WPA y WPA2, que cumplen el mismo propósito pero que son diferentes al mismo tiempo” (NetSpot, 2019).

#### **2.2.15.1. WEP.**

Privacidad equivalente al cableado (WEP) fue “Desarrollado para redes inalámbricas y aprobado como estándar de seguridad Wifi. WEP debía ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo, existen problemas de seguridad conocidos en WEP, que también es fácil de romper y difícil de configurar” (NetSpot, 2019).

Se hicieron sin número de procesos, pero “A pesar de todo el trabajo que se ha hecho para mejorar el sistema, WEP sigue siendo una solución altamente vulnerable. Los sistemas que dependen de este protocolo deben ser actualizados o reemplazados en caso de que la actualización de seguridad no sea posible. WEP fue oficialmente abandonada por la Alianza Wifi en 2004” (NetSpot, 2019).

#### **2.2.15.2. WPA.**

La seguridad WPA es creada para cubrir o solucionar los problemas de la seguridad WEP. Este mecanismo de seguridad ofrece algunas variantes de acuerdo al propósito que se vaya a disponer:

- “WPA-Personal: Utiliza un sistema de claves PSK o claves pre compartidas donde el administrador especifica su propia contraseña y todos los usuarios se conectan a la red con ella, de manera que sea más fácil recordarla.
- RADIUS: Enfocado a empresas, este sistema de seguridad se basa en un servidor en el que los usuarios deben autenticarse con un usuario y una contraseña diferente para cada uno en vez de conectarse todos con una contraseña global” (Sanz, Valero & Gómez Bolaños, 2016).

#### 2.2.15.3. WPA2.

“El cifrado WPA2 es la actualización del cifrado WPA y mejora tanto la seguridad como el rendimiento de este. Este sistema también cuenta con las variantes de claves personales PSK y sistemas RADIUS para la gestión de redes, aunque el cifrado es muy superior al de WPA. Además, el tipo de cifrado usado en WPA y WPA 2 es TKIP y AES” (Sanz, Valero & Gómez Bolaños, 2016).

Siendo AES el que brinda máxima seguridad en nuestra red y a la vez ofrece mejoras en el rendimiento, además de los progresos en la seguridad, AES tolera mayores velocidades que TKIP.

#### 2.2.15.4. Seguridad 802.1x EAP.

“Es un protocolo de acceso a puertos para proteger las redes mediante autenticación. Como resultado, este tipo de método de autenticación es extremadamente útil en el entorno Wifi debido a la naturaleza del medio. Si un usuario de Wifi se autentica a través de 802.1 X para el acceso a la red, se abre un puerto virtual en el punto de acceso que permite la comunicación. Si no se autoriza correctamente, el puerto virtual no se hace disponible y las comunicaciones se bloquean” (Intel, 2019).

Existe tres apartados básicos para la autenticación del 802.1 X:

- **Suplicante.** – Un usuario que está próximo a conectarse o solicitando acceso en la red wifi.
- **Autenticador.** - Un punto de acceso donde solicita credenciales.
- **Servidor de autenticación.** – Un equipo que contiene una base de datos para la autenticación, habitualmente es un servidor de RADIUS como Cisco ACS \*, Funk Steel-Belted RADIUS \*, o Microsoft IAS \*.

“El protocolo de autenticación extensible (EAP) se utiliza para pasar la información de autenticación entre el suplicante (la estación de trabajo Wifi) y el servidor de autenticación (Microsoft IAS u otro). El tipo EAP maneja y define realmente la autenticación. El punto de acceso que actúa como Autenticador es solamente un proxy para permitir que el suplicante y el servidor de autenticación se comuniquen” (Intel, 2019).

#### **2.2.16. Pruebas de conectividad.**

Mediante las herramientas de software Prime Infrastructure, Cisco 8500 Series Wireless Controller, Speed Test y Wifi Analyzer se puede ir obteniendo datos relevantes de protocolos de seguridad, estándares utilizados, intensidad de señal y canales wifi respecto al rendimiento tanto en escenarios digitales, así como también en un escenario físico real de la institución en la que se llevará a cabo la investigación. Mediante estas pruebas se podrá identificar mecanismos de o formas de conexión orientados al fortalecimiento de dispositivos inalámbricos Access Point.

#### **2.2.17. FODA tecnología Wifi.**

Es el análisis de las posibles soluciones propuestas en los objetos planteados de la investigación de acuerdo a este análisis FODA se espera tener una idea clara de las debilidades, amenazas, fortalezas y oportunidades que hay que tener en cuenta al momento de realizar la implementación y configuración de dispositivos inalámbricos en organizaciones que poseen redes de gran tamaño.

##### **2.2.17.1. Debilidades.**

“Las debilidades de la tecnología wifi en el protocolo más actual WPA2 indica que se ha podido obtener información sensible mediante este tipo de redes inalámbricas información como tarjetas de crédito, contraseñas, mensajes en chat email y fotos” (Santamaría L, 2019). Además, que no proporciona una conexión estable en velocidad de transmisión para distancias largas entre el dispositivo final y el punto de acceso (AP). Entre estas debilidades tenemos:

- La información está comprometida al conectarse a redes inalámbricas cuando se realiza transacciones bancarias o se provee datos personales.

- La información está comprometida al utilizar datos móviles (3g/4g) en caso de realizar una operación de compra online, abrir cuentas bancarias o gestionar temas laborales.
- Los usuarios no ejecutan actualizaciones automáticas el sistema operativo cuando el fabricante alerta de una actualización de seguridad.
- Los usuarios al no conocer de una configuración básica en los AP mantienen la opción o protocolo WPA2 desactivado.
- Al no navegar por páginas bajo el protocolo HTTPS la información tiende a ser insegura por no viajar cifrada en la red (*Santamaría L, 2019*).

#### 2.2.17.2. Amenazas.

“Las redes inalámbricas hoy en día son las más amenazadas y vulnerables dentro del mundo de las tecnologías. Por eso es necesario que todos los que utilizan las redes WIFI sepan los riesgos a los que se exponen cuando usan una red inalámbrica. Ya sea en una empresa, en casa o una cafetería cuando un usuario navega por internet y hace uso de las redes inalámbricas está abriendo la puerta a una serie de amenazas que pueden afectar a los usuarios” (*Seguridad T, 2019*). Por tal motivo es fundamental tener conocimiento de las amenazas potenciales que emiten riesgo en la seguridad de los usuarios conectados a una red inalámbrica.

- **“Redes inalámbricas con mayor tráfico.** Cuando una red wifi es utilizada por varios usuarios y ese número va creciendo también crece el riesgo de que alguien introduzca un virus que afecte al resto de usuarios.
- **Accesos no permitidos.** Las contraseñas de las redes inalámbricas puede que usen protocolos de seguridad antiguos y fáciles de craquear como los WEP.
- **Red sin seguridad.** Muchas veces se conectan a redes inalámbricas sin saber quién es el propietario o incluso redes que no tienen contraseña ni protección. En este caso pueden espiar nuestras comunicaciones privadas e utilizar la información con fines poco adecuados.
- **Inicios de sesión falsos.** Cuando se conectan a una red inalámbrica a veces hay una página de inicio o hotspot en la que se nos pide una serie de datos para acceder. Hay que tener cuidado porque pueden ser páginas falsas en las que solicitan datos para robar o para atacar a los dispositivos con malware.

- **Malware.** Se conectan a una red inalámbrica en cierto lugar y en casa, sin saberlo se pudo haber sufrido de un ataque de malware que se activará más tarde y transferirá los datos confidenciales al dispositivo.
- **Robo de datos mientras navega.** Cuando se conectan a una señal wifi se expone a perder documentos privados que se comparte mientras se navega. Por esto no es recomendable compartir información bancaria, porque se expone datos sensibles en la red.
- **Demandas judiciales.** Si en el uso de una red wifi se accede a contenidos ilegales o inapropiados, el emisor de dicha red puede sufrir demandas judiciales por dicho uso. Por eso, muchas empresas restringen determinados contenidos en la red para protegerse” (*Seguridad T, 2019*).

#### 2.2.17.3. Fortalezas.

Las fortalezas actuales de las redes inalámbricas están relacionadas al ámbito económico, es decir, una de las más destacadas es el bajo costo de instalación, debido a que se puede desplegar largas distancias sin necesidad de adquirir cable, también se puede indicar que tiene gran facilidad al momento de la implementación en las organizaciones ya que se adapta a la mayoría de tecnología vigentes hoy en día, entre estas fortalezas se tiene:

- Conectividad de fácil movilidad.
- Cero cables para las conexiones de red.
- La comodidad ofrecida es superior a redes cableadas porque con cualquiera con acceso puede conectarse desde distintos puntos dentro de un rango amplio de espacio.

#### 2.2.17.4. Oportunidades.

Se habla de sus mejoras a mediano y largo plazo, lo que asegura su éxito en el futuro, estos dispositivos están en constante desarrollo, además existen actualizaciones continuas del estándar y en la actualidad su uso sigue en crecimiento, algunas de estas oportunidades son:

- Mejora la velocidad al momento de navegar en internet.
- Red con mayor seguridad.
- Menor interferencias en la cobertura de señal.

2.2.17.5. Resumen FODA.

**Tabla 6-2:** Resumen FODA.

<b>F</b>		<b>O</b>	
• Conectividad de fácil movilidad		• Mejora la velocidad al navegar en internet	
• Cero cables para las conexiones de red		• Menor interferencias cobertura de señal	
• La comodidad superior de redes cableadas		• Red con mayor seguridad	
		<b>WIFI</b>	
<b>D</b>		<b>A</b>	
• La información está comprometida		• Redes inalámbricas muy transitadas	
• Los usuarios no ejecutan actualizaciones		• Accesos no permitidos	
• navegar por páginas sin el protocolo HTTPS		• Red sin seguridad	

Realizado por: Edgar Ulloa.. 2020

## CAPÍTULO III

### 3. METODOLOGÍA DE LA INVESTIGACIÓN.

#### 3.1. Tipo y Diseño de Investigación.

##### 3.1.1. Tipo de Investigación.

La presente investigación se clasifica como aplicativa, Experimental.

*Aplicativa:* debido a que busca aplicar soluciones a los problemas del sector investigado basándose en la comparativa de dos mecanismos de conectividad inalámbricos, investigaciones anteriores, hallazgos y desarrollos tecnológicos para perfeccionar la tecnología existente.

*Experimental:* ya que mediante el análisis realizado a los mecanismos de conectividad que se encuentran en auge en la actualidad y de mayor importancia en la Universidad Central del Ecuador se procedió a realizar pruebas experimentales en escenarios reales y sus respectivas simulaciones con las herramientas necesarias para tener un objetivo claro de la investigación, con estos datos se interpreta los indicadores y resultados, con el fin de optimizar el rendimiento de dispositivos inalámbricos Access Point.

##### 3.1.2. Diseño de Investigación.

Esta investigación posee un diseño cuantitativo, proponiendo evaluar y analizar estadísticamente el rendimiento de dispositivos inalámbricos Access Point de tal manera que permita comparar y aplicar los mecanismos de conectividad de más relevancia en la actualidad y de mayor uso en la Universidad Central del Ecuador, para lo cual previamente se analizó los componentes utilizados en la red Inalámbrica de la Universidad central del Ecuador, inclinándose por los siguientes mecanismos generales: Los Estándares o protocolos Wifi IEEE 802.11 de conexión inalámbrica, niveles de seguridad (WEP, WPA, WPA2, 802.1x) y bandas de frecuencia (2.4GHz y 5GHz).

### **3.2. Métodos de Investigación.**

*Método Científico:* Este método de investigación permite que el involucrado conozca el problema y objeto de investigación, realizando estudios del proceso natural sin ejecutar alteraciones con el fin de demostrar la hipótesis (*Cheerful, M., 2017*). Como bien lo dice el concepto esta investigación tiene un enfoque hacia el análisis de mecanismos de conectividad para luego mediante estos evaluar el rendimiento de Access Point sin tener que realizar variaciones sobre la marcha del presente proyecto.

*Método Deductivo:* Este método permite que el investigador realice varios pasos que lleven a la verificación de los enunciados, estos son la observación del fenómeno a estudiar, creación de una hipótesis para explicar el fenómeno y deducción de consecuencias o proposiciones. A lo largo de la investigación tal cual lo dice el concepto de este método, se realizan pasos que permiten ir confirmado cada uno de los objetivos propuestos mediante la selección de mecanismos de conectividad y la comparación de estos para definir una guía de implementación que ayude en posteriores investigaciones.

### **3.3. Enfoque de la Investigación.**

El presente trabajo investigativo tiene un enfoque Cuantitativo.

Cuantitativo debido a que el estudio y evaluación del rendimiento de dispositivos Access Point se orientan en medir estadísticamente el rendimiento de acuerdo a ciertos mecanismos de conectividad como son: Los Estándares IEEE 802.11 de conexión inalámbrica, Niveles de seguridad, Ancho de Banda, Canal de Señal, Intensidad de Señal y Frecuencias de Señal en 2.4Ghz y 5Ghz. Enfocándose en la comparación de los estándares de más uso y más actuales siendo estos el Estándar IEEE 802.11N y el Estándar IEEE 802.11AC.

### **3.4. Alcance de la Investigación.**

Esta investigación tiene un alcance explicativo ya que la información detallada respecto a los problemas de rendimiento en redes amplias con alta concurrencia de usuarios, así como también a los mecanismos de conectividad de mayor uso y de mayor importancia en la actualidad se van describiendo a lo largo de la investigación para obtener resultados que permitan emitir criterios respecto a los mecanismos de conectividad más relevantes y mediante los cuales se pueda

proveer una guía de implementación y características técnicas que deben tener estos dispositivos explicando las condiciones en que se manifiestan los indicadores para llevarnos a una posible solución del rendimiento en los Access Point.

### **3.5. Población de estudio.**

Para establecer la población de estudio se debe dar énfasis a instituciones que cuenten con una gran infraestructura tecnológica, así como también con gran demanda de usuarios y por ende gran número de conexiones activas dentro de una red, por tal motivo se seleccionó a la Universidad Central del Ecuador ya que cuenta con alrededor de 89.000 usuarios entre Estudiantes, Docentes y Administrativos los mismos que se conectan diariamente a la red inalámbrica. Además, cabe mencionar que en la parte tecnológica inalámbrica posee alrededor de 711 Access Point que brindan servicio inalámbrico, sin contar los demás equipos que forman parte de la red total de esta Institución.

Una vez analizados estos puntos, se puede evaluar el rendimiento basado en pruebas de carga y esfuerzo, es decir, esta investigación se establecerá de la siguiente manera:

- Número de conexiones inalámbricas activas en horas pico (Estudiantes, administrativos y docentes) de la Universidad Central del Ecuador - Periodo 2019-2019.

De acuerdo a los datos obtenidos diariamente de las conexiones inalámbricas activas de las horas pico comprendidas entre las 9:00 hasta las 12:00, se puede indicar que dichas conexiones tienden a estar siempre en rangos similares. En la Figura 1-3 se puede observar el número de conexiones en horas pico de toda la Universidad Central del Ecuador, siendo este valor el más alto y más cercano al promedio de conexiones diarias, por lo tanto, se tomará 12.564 conexiones inalámbricas activas como valor numérico de la población de estudio, estos datos fueron proporcionados por la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador en base a la herramienta Cisco Prime Infrastructure, consecuentemente este sería el número de conexiones que intervienen en la investigación, los cuales proporcionan los datos para la evaluación del rendimiento en la red inalámbrica de esta institución.



**Figura 1-3:** Población de Estudio.

**Fuente:** Cisco Prime Infrastructure.

### 3.6. Unidad de Análisis.

Por lo mencionado en la población de estudio, los objetos inmersos en esta investigación serían 12.564 conexiones a los Access Point en horas pico comprendidas entre las 9h00 hasta las 12h00 en la Universidad Central del Ecuador / Periodo Académico Marzo – Agosto del 2019, las mismas que fueron tomadas diariamente durante una semana y resultaron en promedio el número antes indicado. Cabe mencionar que las conexiones fueron a través de dispositivos inalámbricos como: Celular, Tablet, Laptop o Pc y estos cuentan con tarjetería inalámbrica específica para cada estándar, así se puede comparar dichos Estándares 802.11N y 802.11AC evaluando la tendencia de conexión a estos estándares y su a vez evaluar el rendimiento versus la intensidad de señal, calidad de conexión y throughput.

### 3.7. Selección de la Muestra.

“La muestra es la parte numérica y representa a un subconjunto de la población tomada” (Morillas A, 2015). En base a la población de estudio de 12.564 conexiones en horas pico de la Universidad Central del Ecuador, se selecciona la muestra de la población de estudio mediante la fórmula que

se observa a continuación en el punto 3.8. Tamaño de la muestra y se ejecuta pruebas de los mecanismos de conectividad de más uso en la UCE y de más relevancia en la actualidad, es decir, se usan dos muestras iguales, una para cada estándar, con el fin de comparar el Estándar 801.11N y el Estándar 801.11AC para obtener resultados del rendimiento versus la intensidad de señal, calidad de conexión y throughput.

### **3.8. Tamaño de la Muestra.**

Conforme a lo establecido en la unidad de análisis se define como población de estudio al número de conexiones realizadas a la red inalámbrica de toda la Universidad Central del Ecuador en las horas pico comprendidas entre las 9:00 hasta las 12:00, así mismo para la selección y tamaño de la muestra. Por lo tanto, se tomarán muestras de los indicadores en horarios pico del uso de la red inalámbrica.

#### **Fórmula:**

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1 - p)}{(N - 1) \cdot e^2 + Z^2 \cdot p \cdot (1 - p)}$$

Dónde:

n = pruebas que debemos seleccionar aleatoriamente.

Población de estudio: N = 12.564

Error máximo aceptable: e = 5% = 0,05

Nivel de confianza: Z = 95% = 1,96

Porcentaje estimado de la muestra: p = 50% = 0,5

$$n = \frac{12564 \cdot 1,96^2 \cdot 0,5 \cdot (1 - 0,5)}{(12564 - 1) \cdot 0,05^2 + 1,96^2 \cdot 0,5 \cdot (1 - 0,5)}$$

$$n = \frac{12564 \cdot 3,8416 \cdot 0,5 \cdot 0,5}{12563 \cdot 0,0025 + 3,8416 \cdot 0,5 \cdot 0,5}$$

$$n = \frac{12066,4656}{31,4075 + 0,9604}$$

$$n = \frac{12066,4656}{32,3679}$$

$$n = 372,791$$

Se obtiene que  $n = 373$ .

### 3.9. Técnica de recolección de datos primarios y secundarios.

Para la presente investigación se realiza las siguientes técnicas:

- *Búsqueda de información*, que permita obtener los datos necesarios acerca del objeto de estudio para su desarrollo, utilizando las fuentes primarias y secundarias útiles. En base a este conocimiento se realizó la indagación de la información con respecto a mecanismos de conectividad, conceptos relacionados a redes inalámbricas y selección de pruebas estadísticas que se acoplen al presente proyecto.
- *Pruebas* que permitan analizar y obtener datos acerca de los inconvenientes de rendimiento inalámbrico en redes con masiva concurrencia de usuarios como la realización de escenarios de pruebas con el fin de simular ambientes en los que se manejan los mecanismos de conectividad y posteriores pruebas reales para identificar cual estándar ofrece mejor rendimiento.
- *Observación* es una técnica cualitativa que permite ver los mecanismos de conectividad de mayor importancia en la actualidad y obtener resultados de las comparaciones de estos, es decir el análisis entre los estándares 802.11N y 802.11AC (*Cortés M & Iglesias León M,*

2004).

- *Análisis* que permita dar a conocer los resultados de la investigación mediante la comparación de los mecanismos de conectividad seleccionados como los de mayor relevancia y las posibles soluciones que se pueda dar al rendimiento de Access Point luego de obtener resultados de las pruebas estadísticas.

Las fuentes que se utilizaron para esta investigación son:

- **Primarias**
  - Libros.
  - Papers y Revistas Científicas.
  - Otras Investigaciones.
  - Internet.
- **Secundarias**
  - Observaciones.
  - Textos.

### **3.10. Análisis de mecanismos de conectividad.**

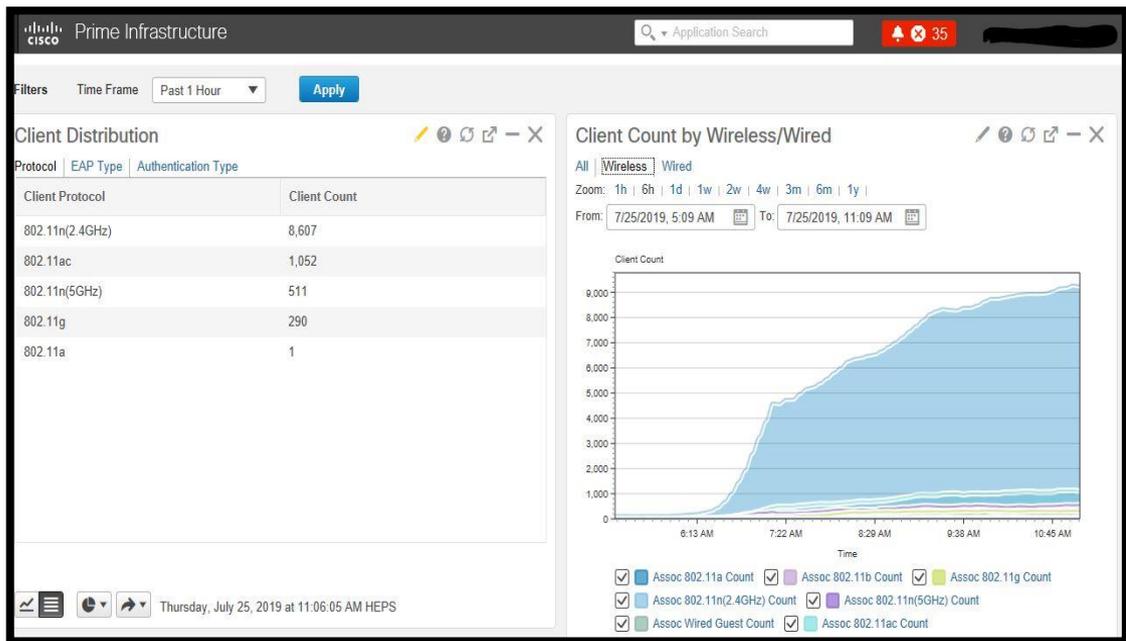
En primer lugar, se define a los mecanismos de conectividad inalámbricos como la forma o método en que un dispositivo inalámbrico se conecta a otro dispositivo proveedor de un servicio, es decir, por ejemplo, un mecanismo de conexión sería la forma en que un teléfono móvil se conecta a un Access Point a través de un protocolo de seguridad (mecanismo de conectividad), solicitando a dicho dispositivo credenciales para poder acceder a la red y por ende a sus servicios.

Entonces se puede decir que en los mecanismos de conectividad intervienen algunos parámetros e indicadores que otorgan un rendimiento diferenciado, por tal motivo se analizó los componentes utilizados en la red Inalámbrica de la Universidad Central del Ecuador, siendo los más destacados: Los Estándares o protocolos Wifi IEEE 802.11 de conexión inalámbrica, niveles de seguridad (WEP, WPA, WPA2, 802.1x) y bandas de frecuencia (2.4GHz y 5GHz). De acuerdo a estos parámetros se optó por seleccionar y comparar mecanismos de conectividad que conlleven al análisis profundo del rendimiento de Access Point.

Ahora bien, dentro de estas tres formas o mecanismos de conectar inalámbricamente a los dispositivos finales, se debe elegir y comparar aquellos mecanismos que posean indicadores medibles de rendimiento. Al analizar estos tres aspectos se tiene lo siguiente:

- **Estándares:** El estándar o protocolo wifi es un mecanismo de conectividad que poseen todos los Access Point, estos internamente manejan y están ligados a varios indicadores de rendimiento teóricos como: ancho de banda, throughput, latencia, intensidad de señal, calidad de conexión, Jitter, ancho de canal, entre otros.
- **Seguridades:** En lo que tiene que ver a seguridad (WEP, WPA, WPA2, 802.1x) es un mecanismo de conectividad que poseen los Access Point, pero no cuenta con indicadores medibles del rendimiento ya que solo intervienen o no credenciales de acceso y niveles de seguridad.
- **Frecuencias:** Con respecto a las bandas de frecuencia se podría tener un indicador de medición dependiendo de esta frecuencia, la cual indica que la Banda de frecuencia de 2.4GHz posee menor velocidad de transmisión con mayor alcance o cobertura, frente a la Banda de frecuencia de 5Ghz siendo todo lo contrario a la anterior ya que posee mayor velocidad de transmisión y menor alcance o cobertura.

Una vez analizados estos tres mecanismos de conectividad y conociendo que la Universidad Central del Ecuador con respecto a los estándares maneja lo siguiente: IEEE 802.11 a, b, g, n y ac, se identificó que dichos estándares son esenciales y que además intervienen directamente en el rendimiento de la red inalámbrica, por tal motivo se plantea la comparación de los estándares de mayor uso en la Universidad Central del Ecuador, siendo los más utilizados los Estándares 802.11N con 8607 clientes en banda de frecuencia de 2.4GHz y 802.11AC con 1052 clientes en banda de frecuencia de 5GHz, como se muestra en la Figura 2-3 según la herramienta de Cisco Prime Infrastructure manejada por el personal de la Dirección de Tecnologías de la Información y Comunicación (UCE).



**Figura 2-3:** Estándares 802.11 más utilizados.

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

Además, se tiene en cuenta el estado del arte actual donde indica que los Estándares han ido mejorando a lo largo del tiempo, es decir, cambiando de acuerdo a versiones optimizadas como la IEEE 802.11 a, b, g, n y ac. “La norma IEEE 802.11n es desarrollada y presentada mundialmente en un borrador en noviembre de 2007, para ser aprobada en septiembre de 2009. Y la norma IEEE 802.11ac que es una actualización de 802.11n fue aprobada mundialmente en enero del 2013” (IEEE, 2013).

### 3.11. Análisis comparativo de los Estándares IEEE 802.11N y 802.11AC.

Los Access Point manejados por la Dirección de Tecnologías de la Información y Comunicación y utilizados en la Universidad Central del Ecuador son de variados modelos de la marca Cisco como se observa en la Figura 3-3. La mayoría de estos Access Point Ciscos manejan los Estándares indicados anteriormente, es decir el 802.11 A, B, G, N y AC. Dentro de la Universidad Central del Ecuador los Access Point internos utilizados son los Cisco Aironet 1700i sin antena en los que se evalúa los Estándares 802.11N y AC, y con los que se tiene previsto comparar y obtener datos del rendimiento mediante algunos parámetros importantes como el ancho de banda, latencia, throughput, jitter, intensidad de señal, banda de frecuencia, canal de señal, entre otros.

Todo esto con el objetivo de tener claro que tecnología - Estándar es mejor respecto al otro y así poder aplicarla en redes con alta concurrencia de usuarios.



**Figura 3-3:** Modelos de AP Cisco.

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

Si bien es cierto en el marco teórico se citó a los dos Estándares, el 802.11N y 802.11AC indicando que cada uno de ellos tienen lineamientos diferentes, lo cuales se verán a continuación:

El estándar 802.11N trabaja en las bandas de frecuencia de 2.4GHz y 5GHz, es decir, maneja dos bandas de frecuencia con canales de 20 MHz de amplitud. “Amplitud es la que establece la tasa de transferencia de información para una mayor o menor velocidad máxima teórica. Este estándar ofrece la posibilidad de operar con una amplitud de canal, o ancho de banda de 40 MHz uniendo dos canales de 20 MHz para ello. Pero hay limitaciones, en tanto que se utilizan 13 canales de 20 MHz, y el espectro está ampliamente saturado por la cantidad de dispositivos que funcionan sobre la banda de 2,4 GHz, generando interferencias entre ellos y colapsos en el intercambio de datos” (González, 2018).

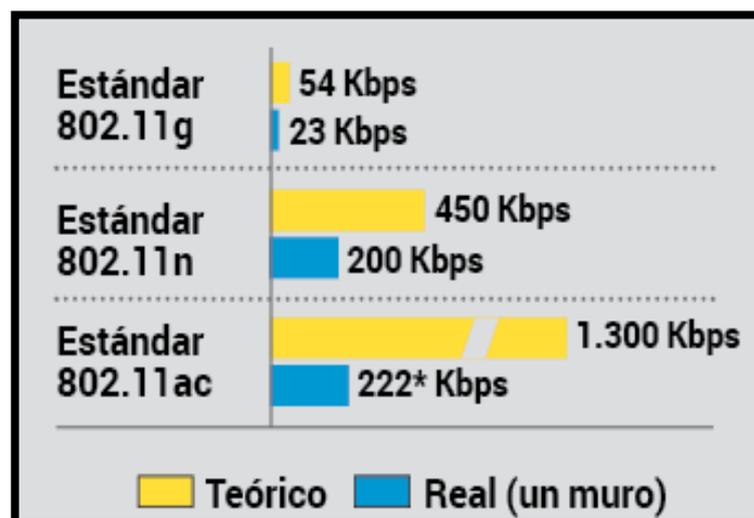
El estándar 802.11AC trabaja en la banda de frecuencia de 5GHz lo que quiere decir que posee mayor cantidad de canales y mayor ancho de banda. “En entornos de gran tamaño los dispositivos operan bajo los lineamientos ya citados, pero con cierta disminución en el alcance de la señal, lo ideal sería utilizar un mayor ancho de banda por canal para permitir un mayor flujo de transferencia y más velocidad entre el Router y los dispositivos conectados” (González, 2018).

Los elementos usados en este estándar consumen menos energía lo que significa que los dispositivos finales que funcionan con batería como laptops, teléfonos móviles, Tablet, entre otros puedan tener mejor rendimiento.

A manera general la banda de frecuencia de 2.4GHz en el Estándar 802.11N posee mayor alcance con menor velocidad transmisión y la banda de 5GHz en el Estándar 802.11AC posee menor alcance con mayor velocidad de transmisión, viendo aquí ciertas diferencias notables que podrán incurrir en el rendimiento de los Access Point. Además, por parte de los usuarios de la red inalámbrica también se denotan ciertos criterios como por ejemplo que los dispositivos que se conectan a la red cuentan con un solo Estándar en su tarjetería lo que limita el uso de frecuencias, estándares y demás punto claves de conexión. En breve se describe ciertos parámetros que son de mucha importancia para mejorar el rendimiento de Access Point, y queda a juicio tomar las ventajas indicadas en esta investigación.

### 3.11.1. Velocidad de transmisión.

Los estándares WLAN regulan las velocidades y el tipo de transmisión de los datos mediante las ondas de radio, en la Tabla 1-3 se observa una comparativa de la velocidad de transmisión según el estándar aplicado además en la Figura 4-3 se muestra una gráfica con el fin de entender de mejor manera las velocidades de transmisión teórico y real que maneja cada estándar.



**Figura 4-3:** Comparación de velocidades de transmisión.

Fuente: González, 2018.

**Tabla 1-3.** Velocidad de Transmisión comparativa entre estándar N y AC.

	<b>IEEE 802.11N</b>	<b>IEEE 802.11AC</b>
<b>Frecuencia de Operación</b>	2.4GHz y 5GHz	5GHz
<b>Canales</b>	20, 40MHz	20, 40, 80 y hasta 160 MHz
<b>Streams</b>	1 a 4	1 a 8
<b>MU-MIMO</b>	No	Si
<b>Máxima tasa de transferencia por radio (1x1)</b>	150 Mbps	450 Mbps
<b>Máxima tasa de transferencia por radio (3x3)</b>	450 Mbps	1.3 Gbps

Fuente: WNI México.

Realizado por: Edgar Ulloa.. 2020

Observando los datos anteriores de la Figura 4-3 se puede decir que el estándar 802.11N maneja una velocidad de transmisión teórica de entre 150 Kbps y 450 Kbps y una velocidad de transmisión real de 200 Kbps a diferencia del estándar 802.11AC que posee una velocidad de transmisión teórica de hasta 1300 Kbps y una velocidad de transmisión real de 222 Kbps, lo que indicaría que ambos estándares están bajo el mismo promedio con respecto a la velocidad de transmisión. También es importante indicar que las especificaciones de los Access Point Cisco Aironet 1700 Series usados para la investigación posee velocidades de datos en el estándar 802.11N en 2.4GHz tal cual se muestran en la Tabla 2-3.

**Tabla 2-3:** Velocidades de datos 802.11n en 2.4 GHz.

<b>Índice MCS</b>	<b>GI = 800ns</b>	<b>GI = 400ns</b>
	<b>Velocidad de 20-MHz (Mbps)</b>	<b>Velocidad de 20-MHz (Mbps)</b>
0	6.5	7.2
1	13	14.4
2	19.5	21.7
3	26	28.9
4	39	43.3

5	52	57.8
6	58.5	65
7	65	72.2
8	13	14.4
9	26	28.9
10	39	43.3
11	52	57.8
12	78	86.7
13	104	115.6
14	117	130
15	130	144.4

Fuente: Cisco Aironet 1700 Series Access Point Data Sheet.

El estándar 802.11AC está centrada en garantizar una mayor velocidad a la red inalámbrica, opera a una velocidad de transmisión teórica de hasta 1300 Mbps, pero en la realidad la velocidad es significativamente menor. A pesar de que posee menor alcance con la banda de 5GHz estos dispositivos en estándar 802.11AC pueden alcanzar distancias mayores gracias a la tecnología Beamforming que focaliza la señal de radio a cada dispositivo conectado.

En la Tabla 3-3 se puede observar las velocidades que maneja este estándar.

**Tabla 3-3:** Velocidades de datos 802.11ac (5 GHz).

Índice MCS	Corriente Espacial	GI = 800ns			GI = 400ns		
	Corriente Espacial	Velocidad 20MHz (Mbps)	Velocidad 40MHz (Mbps)	Velocidad 80MHz (Mbps)	Velocidad 20MHz (Mbps)	Velocidad 40MHz (Mbps)	Velocidad 80MHz ate(Mbps)
		0	1	6.5	13.5	29.3	7.2
1	1	13	27	58.5	14.4	30	65
2	1	19.5	40.5	87.8	21.7	45	97.5
3	1	26	54	117	28.9	60	130
4	1	39	81	175.5	43.3	90	195
5	1	52	108	234	57.8	120	260
6	1	58.5	121.5	263.3	65	135	292.5
7	1	65	135	292.5	72.2	150	325

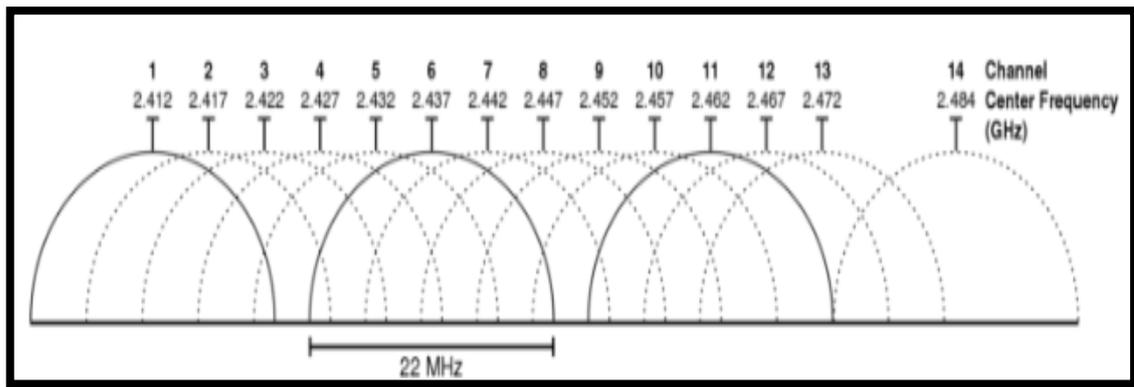
8	1	78	162	351	86.7	180	390
9	1	-	180	390	-	200	433.3
0	2	13	27	58.5	14.4	30	65
1	2	26	54	117	28.9	60	130
2	2	39	81	175.5	43.3	90	195
3	2	52	108	234	57.8	120	260
4	2	78	162	351	86.7	180	390
5	2	104	216	468	115.6	240	520
6	2	117	243	526.5	130	270	585
7	2	130	270	585	144.4	300	650
8	2	156	324	702	173.3	360	780
9	2	-	360	780	-	400	866.7

Fuente: Cisco Aironet 1700 Series Access Point Data Sheet.

### 3.11.2. Capacidad del canal.

La capacidad del canal respecto al rendimiento de una red tiene que ver con la velocidad máxima de transmisión de datos a través de un canal de comunicación, es medida en bits por segundos y depende del ancho de banda, ruido y tasa de errores permitida. Por lo tanto, el estándar 802.11N opera sobre un valor máximo de canal de 40MHz, mientras que el estándar 802.11AC opera sobre un valor máximo de canal de 160MHz, dándole al estándar 802.11AC una ventaja teórica significativa.

No obstante, cabe mencionar que existen 13 canales en la banda de 2.4GHZ que se encuentran superpuestos unos con otros, lo que también ocasionan interferencias y por ende un bajo rendimiento en la red. Lo ideal sería escoger canales que no se solapen entre ellos como se muestra en la Figura 5-3. Así como también se muestra el número máximo de canales superpuestos en la Tabla 4-3 de acuerdo a las especificaciones del Access Point Cisco 1700 Series.



**Figura 5-3:** Canales adyacentes superpuestos.

Fuente: González, 2018.

**Tabla 4-3:** Número máximo de canales no superpuestos.

	Estándar 802.11N en 2.4GHZ	Estándar 802.11AC en 5GHZ
Número máximo de canales no superpuestos	20 MHz = 3	20 MHz = 24 40 MHz = 11 80 MHz = 5

Fuente: Cisco Aironet 1700 Series Access Point Data Sheet.

Realizado por: Edgar Ulloa.. 2020

### 3.11.3. Intensidad de señal.

Como se mencionó en el marco teórico la intensidad de señal son mediciones de RSSI y “Representan la calidad relativa de una señal recibida en un dispositivo, RSSI indica el nivel de potencia que se recibe y cuanto mayor sea el valor RSSI, más fuerte será la señal” (Net Spot, 2019). Es decir, cuando una señal esta entre los rangos de 30dBm y -70dBm se considera una señal óptima, pero más depende de la ubicación física que se le dé a cada uno de los Access Point que intervienen en la emisión de señal y así mismo cada uno de los equipos clientes o dispositivos finales que se conecten al emisor (Access Point).

En razón de que la medición teórica depende de varios factores como ubicación física de equipos, características de dispositivos, interferencias físicas, entre otros. y no depende del estándar 802.11N ni del estándar 802.11AC no se define cuál de estos tiene mejor intensidad de señal o cual establece una ventaja notable para la investigación.

#### **3.11.4. Tráfico de red.**

Se refiere al tipo de información que viaja a través de una red, estas redes toleran diferentes tipos de tráfico (Voz, Vídeo, Datos, etc.) simultáneamente sobre una misma infraestructura. Cada tipo de tráfico tiene diferentes características y por tanto diferentes requerimientos, por ejemplo:

- VoIP es sensible al retardo y Jitter.
- TCP es tolerante a la pérdida de paquetes, pero no (Vídeo y Voz).

Entonces el tráfico de red sirve para ayudar a evaluar ciertos factores importantes del rendimiento de una red, y ahora con la ayuda de estándares con mecanismos de conexiones diferentes como el 802.11N y el 802.11AC, estas métricas de desempeño son analizadas para un determinado tráfico mediante:

- Retardo (ms).
- Jitter (ms).
- Rendimiento (Mbps).

Lo que indicaría que mediante los aspectos a ser medidos (Retardo, Jitter, Rendimiento) el estándar 802.11AC tiene ventajas teóricas sobre el estándar 802.11N.

#### **3.11.5. Retardo de Propagación.**

El retardo o retraso de propagación en una red es importante en cuanto tiene que ver a las implementaciones de redes ya que especifica y/o cuantifica el tiempo que demora un bit de datos para viajar a través de una red desde un nodo emisor a un nodo receptor. En tal razón el estándar 802.11N maneja una velocidad de transmisión teórica de hasta 600 Mbps por ende debería tener mayor retardo sobre el estándar 802.11AC que maneja una velocidad de transmisión teórica de hasta 1300 Kbps, haciendo que este último estándar tenga mejoras teóricas sobre su antecesor.

#### **3.11.6. Jitter.**

“Los paquetes en la red experimentan distintas cantidades de retardo. El retardo de un paquete varía a lo largo del camino entre el transmisor y el receptor. Esta variación en el retardo, se conoce como Jitter y afecta la calidad del flujo de audio y/o vídeo; las causas más comunes para su

aparición son: tiempos largos de espera de conexión, congestión del tráfico y la interferencia” (*Cuesta Palacios & Romero León, 2013*).

En relación al Jitter y comparando los estándares 802.11N y 802.11AC según la investigación que reposa en el dspace de la Universidad Salesiana “Análisis comparativo del desempeño del estándar IEEE 802.11ac respecto al IEEE 802.11n a través de simulación numérica apoyada por software” (*Ortiz, 2015*) realizada en Quito abril 2015, donde indica que los datos resultantes en el estándar 802.11AC son más estables por lo tanto el Jitter es menor que en el caso del estándar 802.11N.

En conclusión, se denota una superioridad respecto a Jitter en 802.11AC, lo que quiere decir que dicho estándar tiene menor variación de retardo (Jitter) en relación al estándar 802.11N.

### **3.11.7. Throughput (Rendimiento).**

Siendo el throughput la tasa de transferencia efectiva (tamaño neto de trabajo o información que fluye en un sistema) o la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación, teniendo en cuenta este concepto y verificando las ciertas características de cada estándar como:

- Banda de frecuencia.
- Capacidad de canal.
- Tasa máxima de transmisión.

Se deduce que el throughput para el estándar 802.11AC es mayor en comparación con su antecesor el estándar 802.11N, es decir tiene mayor tasa de transferencia de datos asumiendo también que las comparaciones anteriores de sus características se inclinan por el estándar 802.11AC.

### **3.11.8. Latencia.**

“Mide el tiempo que tarda en transmitirse un paquete dentro de la red, su medida es en milisegundos (ms), comúnmente para estas mediciones se utiliza el ping que se ejecuta dentro de una consola de comandos” (*Sanz, Valero & Gómez Bolaños, 2016*). Por tal motivo constituye un factor importante de las conexiones hacia el internet más no las conexiones que se realizan internamente dentro de una institución ya que el medio de transmisión, la distancia entre dos puntos que

requieran plasmar la comunicación y las redes o los saltos intermedios que tengan que atravesar los paquetes no son mediciones comparables para cada uno de los estándares investigados.

Tanto el estándar 802.11N como el estándar 802.11AC tienen saltos intermedios similares dentro de la red para conectarse a internet, esto depende más de la ubicación física que se le dé a cada uno de estos Access Point, consecuentemente cada estándar a pesar de tener diferencias en sus características no quiere decir que uno tenga mejores componentes que el otro y que tenga mayor o menor latencia, más bien se considera un punto imparcial entre estos dos estándares con respecto a la evaluación de la latencia.

### **3.11.9. Seguridad.**

De acuerdo a los conceptos mencionados en el capítulo I y capítulo II acerca de la seguridad que maneja la Universidad Central del Ecuador se identifica un nivel de seguridad alto manejado por WPA2 con PSK y WPA2 Enterprise con 802.1x EAP para los dos estándares.

Accediendo a estas tecnologías (WPA2 con PSK y WPA2 Enterprise con 802.1x EAP) mediante los 2 estándares se tiene las mismas opciones de seguridad lo que quiere decir que dicha seguridad no va a depender del mecanismo o estándar que se escoja, así que ninguno tiene ventaja sobre el otro con respecto a la seguridad.

### **3.11.10. Resultado comparativo teórico.**

Mediante este análisis comparativo del estándar 802.11N y el estándar 802.11AC se establece parámetros de medición los cuales permiten tener datos que demuestren cual estándar tiene mejor expectativa sobre el otro. Los parámetros medibles son Jitter, retardo, latencia, seguridad, throughput, tráfico de red, intensidad de señal, capacidad de canal y velocidad de transmisión. En total son 9 parámetros de los cuales se obtiene que el Estándar 802.11N posee 3 de estos equivalentes al 33.33% y el Estándar 802.11AC posee 9 parámetros equivalentes al 100%, es decir el Estándar 802.11AC posee mejores características sobre su antecesor y como punto final se obtiene una tabla de datos teóricos que representan las ventajas que tiene el un mecanismo sobre el otro, como se muestra en la Tabla 5-3:

**Tabla 5-3:** Análisis comparativo de los estándares 802.11N y AC.

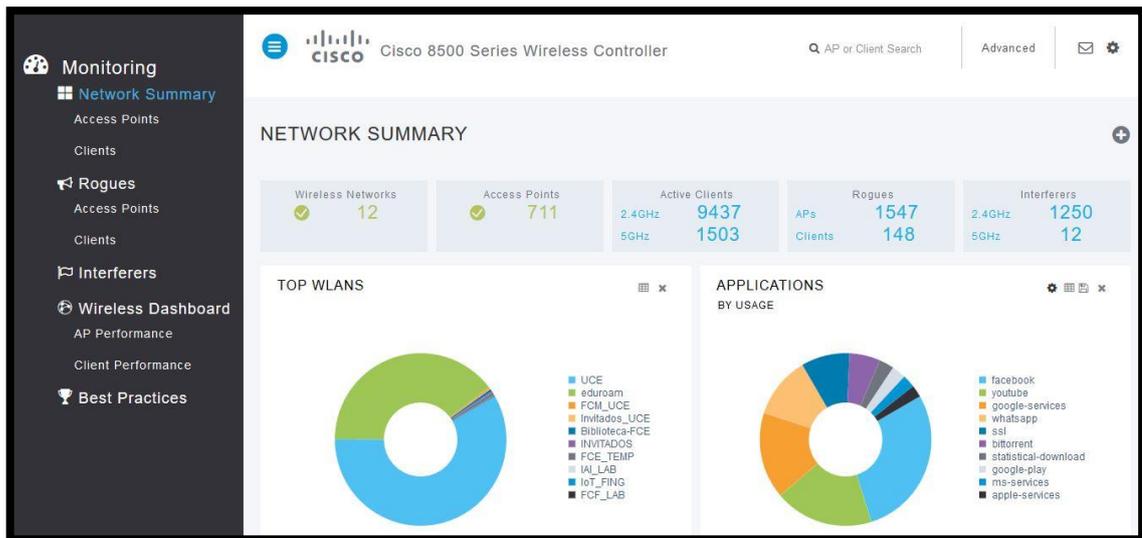
<b>TECNOLOGÍA</b>	<b>IEEE 802.11N</b>	<b>IEEE 802.11AC</b>
Jitter		✓
Retardo		✓
Latencia	✓	✓
Seguridad	✓	✓
Throughput		✓
Tráfico de Red		✓
Intensidad de Señal	✓	✓
Capacidad de Canal		✓
Velocidad de transmisión		✓
<b>TOTAL</b>	<b>3</b>	<b>9</b>
<b>PORCENTAJE %</b>	<b>33.33%</b>	<b>100%</b>

Realizado por: Edgar Ulloa.. 2020

### 3.12. Escenarios de prueba de los estándares IEEE 802.11N y 802.11AC.

Los escenarios de prueba de los mecanismos de conectividad IEEE 802.11N y 802.11AC se generan en base a la estructura física de la red inalámbrica, de la cual se va obtener datos que validen el rendimiento de sus Access Point, al igual se pretende tomar datos reales de las herramientas Cisco 8500 Series Wireless Controller y Cisco Prime Infrastructure instrumentos que intervienen en la infraestructura de la red en la Universidad Central del Ecuador.

Al momento la red inalámbrica de esta institución usa APs para ambientes internos y externos en diferentes modelos según se tiene registros en la herramienta Cisco 8500 Series Wireless Controller. Pero esta investigación se centra en los Access Point internos Cisco Aironet 1700 Series, en el **Anexo A:** Cisco Aironet 1700 Series, se puede encontrar una especificación más detallada de estos Access Point. En la Figura 6-3 se observa la interfaz de presentación de la herramienta Cisco 8500 Series Wireless Controller donde muestra un resumen de la red inalámbrica.



**Figura 6-3:** Cisco 8500 Series Wireless Controller (Dashboard).

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

Si bien se indicó en el apartado anterior en la Universidad Central del Ecuador se manejan Access Point para ambientes internos, externos, con antenas y sin antenas en diferentes modelos. Pero cabe recalcar que los de mayor impacto y utilización son los Cisco Aironet 1700i tal cual se muestra a continuación en la Tabla 6-3.

**Tabla 6-3:** Access Point utilizados en red inalámbrica UCE.

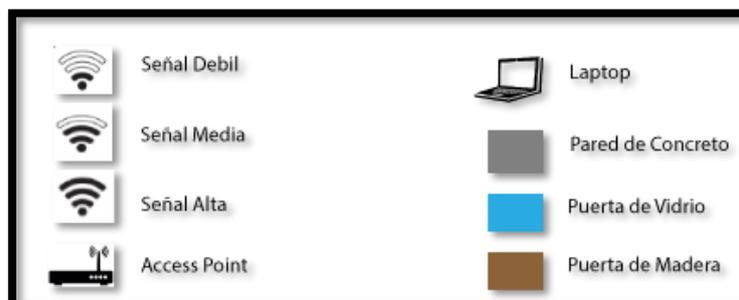
Modelo	Con Antenas	Sin Antenas	Número de APs	Ambiente
Cisco Aironet 1700i		✓	636	Interno
Cisco Aironet 2702e	✓		10	Interno
Cisco Aironet 1530i		✓	42	Externo
Cisco Aironet 1530e	✓		23	Externo

**Fuente:** Dirección de Tecnologías de la Información y Comunicación (UCE).

**Realizado por:** Edgar Ulloa.. 2020

Con el propósito de poder llevar a cabo la investigación se selecciona el diseño y estructura del escenario de pruebas de acuerdo a espacios reales de la institución para tener de manera clara el ambiente en el que se va a trabajar, es decir, ambientes internos donde permita comparar los mecanismos de conectividad más relevantes en esta institución los cuales son: Estándar 802.11N en banda de frecuencia de 2.4GHz y Estándar 802.11AC en banda de frecuencia de 5GHz.

En la Figura 7-3 se presenta la señalización que interviene en la Figura 8-3 con el fin de identificar y mantener claridad en los aspectos relacionados al rendimiento de la red inalámbrica en la Universidad Central del Ecuador.

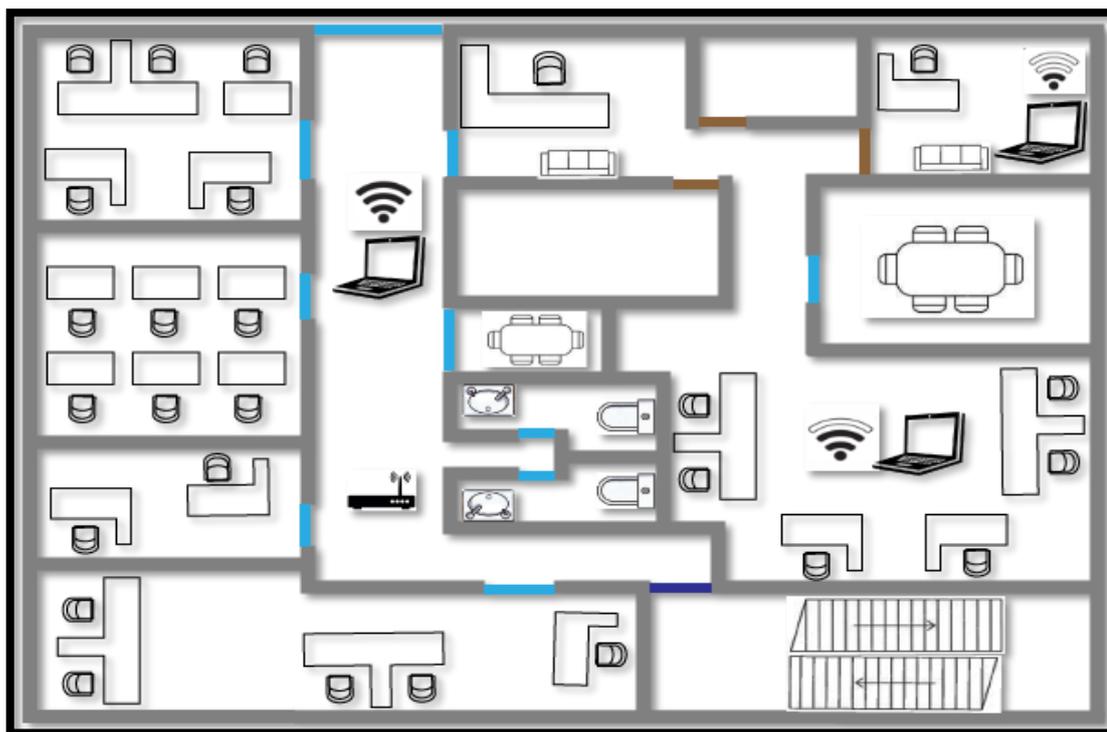


**Figura 7-3:** Señalización Figura 8-3.

**Realizado por:** Edgar Ulloa.. 2020

En la Figura 8-3, el escenario es una recreación similar a la infraestructura de la Universidad Central del Ecuador, de igual forma se ha tomado como referencia todos los dispositivos hallados en dicho espacio, si bien se puede notar que en esta área se tiene instalado Access Point en un pasillo el cual estaría ubicado en la parte céntrica de toda esta área, este AP fue ubicado de esta forma con el fin de unir los ambientes presentados en la Figura 8-3 y de tener un alcance total en toda el área.

En este escenario de prueba se toma en cuenta los dispositivos conectados en esta red inalámbrica con el fin de evaluar si la intensidad de señal disminuye o aumenta a causa de la concurrencia de usuarios y la posición del AP. Así como también se evaluará la velocidad de conexión en relación a la ubicación del dispositivo inalámbrico. Para esto se colocarán los dispositivos finales en puntos cercanos, medios y alejados al Access Point.



**Figura 8-3:** Ambiente de prueba teórico.

**Realizado por:** Edgar Ulloa.. 2020

El Access Point utilizado en espacios o áreas internas con antenas internas para esta investigación es Cisco Aironet 1702I, del cual se describe algunas especificaciones notables para su investigación:

Cisco Aironet 1700 Series Access Point posee doble banda, son puntos de acceso con estándar 802.11 a /g / n / ac, lo que incluye una tasa de conexión teórica de hasta 867 Mbps, permitiendo así más clientes inalámbricos asociados a la red, con lo cual se aprovecha las aplicaciones multimedia al contar con un buen ancho de banda, en la Tabla 7-3 se describe ciertos beneficios.

**Tabla 7-3:** Beneficios de AP Cisco series 1700.

Característica	Beneficio
802.11ac Wave con 3x3 de entrada y salida múltiple (MIMO) y dos flujos espaciales	Proporciona altas velocidades a través de un mayor rango de capacidad y fiabilidad que los puntos de acceso de la competencia. Proporciona hasta tres veces más ancho de banda que las redes 802.11n.

Cisco Aire limpio Espectro de Inteligencia	Los canales detectan la interferencia de RF y proporciona capacidades básicas de análisis de espectro mientras que la simplificación de las operaciones en curso son a través de 20-, 40-, y 80-MHz de ancho.
Punto de acceso móvil optimizado	Dirige dispositivos cliente para asociar con el punto de acceso en su rango de cobertura, ofrece la tasa de datos más rápida disponible.
Igualación MIMO	Aumenta el rendimiento de enlace ascendente y la fiabilidad, reduciendo el impacto de desvanecimiento de la señal

**Fuente:** Cisco Aironet 1700 Series Access Point Data Sheet.

**Realizado por:** Edgar Ulloa.. 2020

Por otra parte, en lo que tiene que ver a las especificaciones para los estándares 802.11N y 802.11AC se puede ver la Tabla 8-3 donde muestra las especificaciones de estos estándares y su funcionamiento dentro del Access Point 1702I.

**Tabla 8-3:** Especificaciones Access Point Cisco series 1700

	<b>Especificación</b>
Números de parte	Punto de acceso Cisco Aironet 1700i: entornos interiores, con antenas internas. <ul style="list-style-type: none"> <li>● AIR-CAP1702I- x -K9: banda dual, basada en controlador 802.11a/g/n/ac.</li> <li>● AIR-CAP1702I- x K910: Eco-pack (doble banda 802.11a/g/n/ac) 10 puntos de acceso por cantidad</li> </ul>
Controladores LAN inalámbricos compatibles	Cisco 2500 controladores inalámbricos Series, Módulo de mando inalámbrico Cisco para ISR G2, Cisco Wireless Módulo de servicios 2 (WiSM2) para Cisco Catalyst ® 6500 Series Switches, Cisco 5500 controladores inalámbricos Series, Cisco Flex ® 7500 controladores inalámbricos Series, Cisco 8500 controladores inalámbricos Series, Controlador inalámbrico virtual de Cisco; Controlador de LAN inalámbrica Cisco 5760,

	Switches Cisco Catalyst serie 3850, Switches Cisco Catalyst serie 3650
Capacidades 802.11n versión 2.0 y relacionadas	<ul style="list-style-type: none"> <li>● 3x3 MIMO con dos flujos espaciales.</li> <li>● Combinación de relación máxima (MRC).</li> <li>● Forma de haz 802.11n y 802.11a / g.</li> <li>● canales de 20 y 40 MHz.</li> <li>● Tasas de datos PHY de hasta 300 Mbps (40 MHz con 5 GHz).</li> <li>● Incorporación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx).</li> <li>● Selección de frecuencia dinámica 802.11 (DFS).</li> <li>● Soporte de diversidad de cambio cíclico (CSD)</li> </ul>
Capacidades 802.11ac Wave 1	<ul style="list-style-type: none"> <li>● 3x3 MIMO con dos flujos espaciales.</li> <li>● MRC.</li> <li>● Forma de haz explícito estándar 802.11ac.</li> <li>● Canales de 20, 40 y 80 MHz.</li> <li>● Velocidades de datos PHY de hasta 867 Mbps (80 MHz en 5 GHz).</li> <li>● Incorporación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx).</li> <li>● 802.11 DFS.</li> <li>● soporte CSD.</li> </ul>

**Fuente:** Cisco Aironet 1700 Series Access Point Data Sheet.

**Realizado por:** Edgar Ulloa.. 2020

### **3.12.1. Simulación en Cisco 8500 Series Wireless Controller.**

Para la toma de datos se utilizó la herramienta Cisco 8500 Series Wireless Controller que es un equipo de hardware y software que permite administrar datos de los Access Point conectados a su red inalámbrica. La información que se obtiene mediante esta herramienta son de suma importancia para validar el rendimiento de la red y poder realizar las respectivas correcciones.

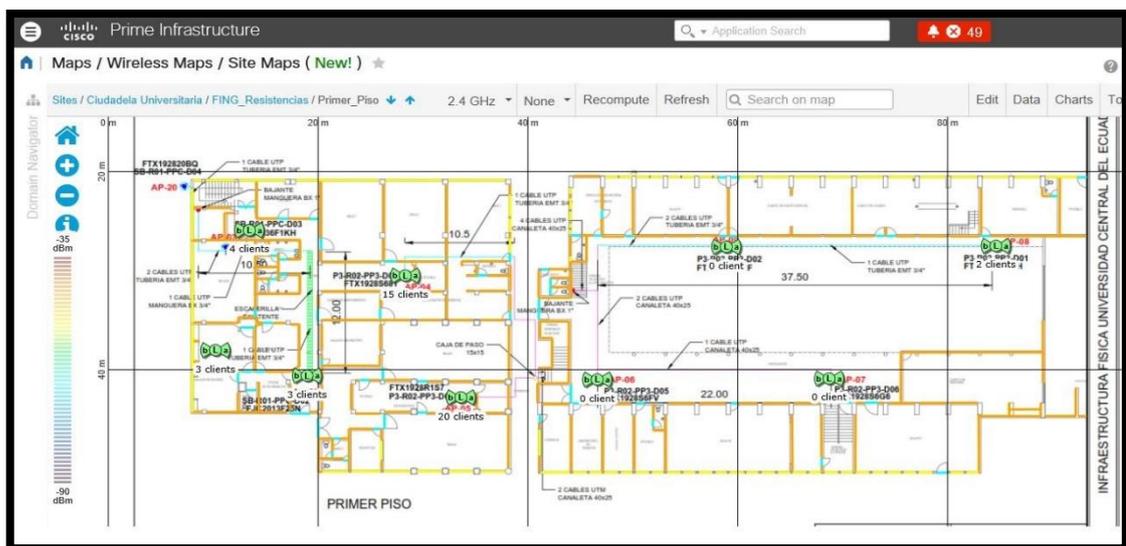
Mediante la herramienta se escoge los parámetros indicados para cada estándar 802.11N y 802.11AC a fin de obtener los datos necesarios que permitan la evaluación del rendimiento de

Access Point mediante estos dos mecanismos de conexión. Los parámetros ingresados en la herramienta Cisco 8500 Series Wireless Controller son:

- **Estándar:** Dependiendo de los datos que se quiere obtener se parametriza los estándares 802.11N o 802.11AC.
- **Frecuencia:** De acuerdo al estándar seleccionado anteriormente se escoge la frecuencia en la que se quiere obtener los datos, siendo estos la frecuencia 2.4GHz para el estándar 802.11N y 5GHz para el estándar 802.11AC.
- **Tipo de Antena:** Depende de los Access Point a los cuales se les evalúa el rendimiento.
- **Potencia del equipo:** Cada estándar posee diferente potencia, por lo tanto, depende de este, de la distancia y de las interferencias.
- **Posicionamiento Físico:** Una correcta ubicación física dependerá del análisis estructural del área o espacio donde se instale el Access Point.

### 3.12.1.1. Estándar IEEE 802.11N en Cisco 8500 Series Wireless Controller.

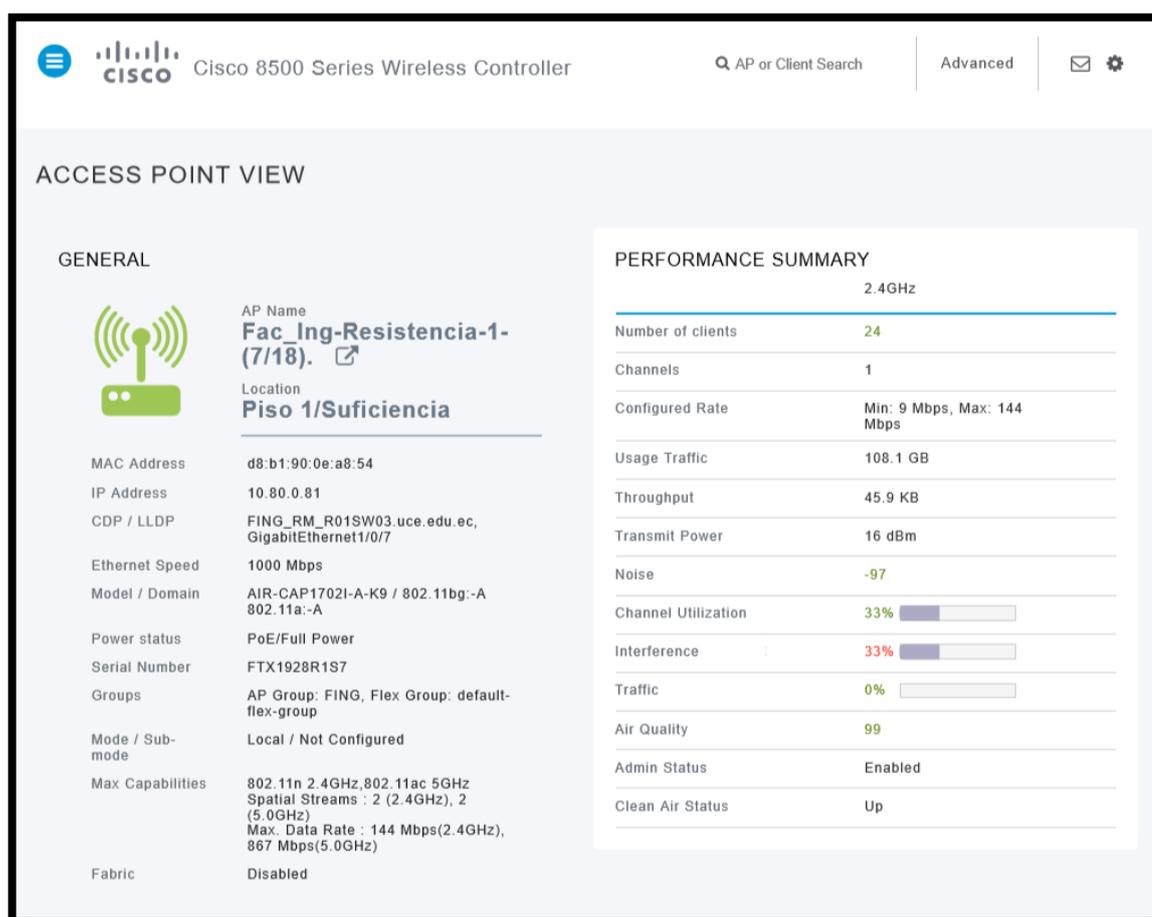
Mediante las herramientas Cisco se consigue perfilar el mapa de la infraestructura de la red inalámbrica, donde consta los parámetros ingresados en la controladora Cisco 8500 Series como estándar aplicado (IEEE 802.11N), banda de frecuencia (2.4GHz), número de clientes por Access Point, intensidad de señal, entre otros, tal cual se muestra en la Figura 9-3.



**Figura 9-3:** Estructura física del ambiente de prueba 802.11N.

Fuente: Herramienta Cisco Prime Infrastructure.

Una vez ubicado el área a ser evaluada se selecciona los parámetros necesarios que permitan obtener datos acerca del rendimiento de los Access Point mediante el mecanismo de conexión IEEE 802.11N. Con esto se espera tener información del número de canales utilizados, tasa de velocidad configurada, tráfico, throughput, poder de transmisión (intensidad de señal), ruido (calidad de conexión), utilización del canal e interferencia. A manera general la herramienta Cisco 8500 Series Wireless Controller presenta datos del estándar 802.11N en la banda de frecuencia 2.4GHz con los que se puede evaluar el rendimiento de este mecanismo de conexión, así como se muestra en la Figura 10-3.



**Figura 10-3:** Datos obtenidos en 802.11N en 2.4GHz.

**Fuente:** Herramienta Cisco 8500 Series Wireless Controller.

En la Figura 11-3 por medio de la Herramienta Cisco 8500 Series Wireless Controller y de una manera más detallada presenta un listado de los clientes conectados a la red inalámbrica en el cual se puede ver varios datos de importancia como:

- Nombre de usuario.

- Tiempo de actividad.
- Ancho de banda utilizado.
- Sistema operativo utilizado
- Estándar utilizado.
- Calidad de la señal.

FAC\_ING-RESISTENCIA-1-(7/18). DETAILS

CLIENTS RF TROUBLESHOOT CLEAN AIR TOOLS

Username	Uptime	Usage	OS	SSID	Capabilities	Signal Quality
dfpachacamas@...	1 hours	12 MB	Unclassified	UCE	802.11n	53dB
ajmartinezs	1 hours	108 MB	Android-Samsun...	eduroam	802.11n	18dB
jabarzalio	1 hours	41 MB	Android-Sony-Er...	eduroam	802.11n	42dB
amjuina	1 hours	91 MB	Unclassified	UCE	802.11n	38dB
ecoba	1 hours	5 MB	Unclassified	UCE	802.11n	41dB
kesanchezv1	1 hours	2 MB	Unclassified	UCE	802.11n	38dB
Mncaza	1 hours	4 MB	Android	UCE	802.11n	34dB
DJGUALOTOS	1 hours	8 MB	Unclassified	UCE	802.11n	30dB
jhmorecho	1 hours	575 KB	Unclassified	UCE	802.11n	49dB
snmedrano	1 hours	6 MB	Android-Samsun...	eduroam	802.11n	39dB
eccoeilo	58 minutes	7 MB	Unclassified	UCE	802.11n	39dB
cnvlliana	55 minutes	45 MB	Android	UCE	802.11n	33dB
ajchaal	52 minutes	1 MB	Unclassified	UCE	802.11n	43dB
ajchaal	49 minutes	456 KB	Unclassified	UCE	802.11n	43dB
wjllumigusin	46 minutes	9 MB	Unclassified	UCE	802.11n	31dB
edgonzalezb	39 minutes	2 MB	Unclassified	UCE	802.11n	38dB
gfgutierrez	14 minutes	623 KB	Unclassified	UCE	802.11n	29dB
sacajamarca	13 minutes	1 MB	Unclassified	UCE	802.11n	44dB
Jgvacat	13 minutes	1 MB	Android-Sony-Er...	eduroam	802.11n	31dB
Aigo	7 minutes	514 KB	Android-Samsun...	eduroam	802.11n	34dB
elpillajo	6 minutes	199 KB	Android	eduroam	802.11n	40dB
Unknown	4 minutes	16 KB	Unclassified	Invitados_UCE	802.11n	31dB
rmpilataxi	2 minutes	5 MB	Android	eduroam	802.11n	27dB
Unknown	1 minutes	286 KB	Android	Invitados_UCE	802.11n	53dB
cabayas	1 hours	3 MB	Unclassified	UCE	802.11ac	18dB
selena	1 hours	3 MB	Android	eduroam	802.11n	22dB
bscampos@uce....	1 hours	5 MB	Unclassified	UCE	802.11ac	28dB
nacedeno	1 hours	14 MB	Intel-Device	UCE	802.11ac	30dB
jallulluna	52 minutes	37 MB	Unclassified	UCE	802.11ac	23dB
lepalliaa	47 minutes	4 MB	Unclassified	UCE	802.11n	42dB
wanaguano	42 minutes	5 MB	Apple-iPhone	UCE	802.11n	21dB
cnviterim@uce....	32 minutes	7 MB	Unclassified	UCE	802.11ac	30dB

50 items per page 1 - 32 of 32 items

Figura 11-3: Datos obtenidos en 802.11N en 2.4GHz.

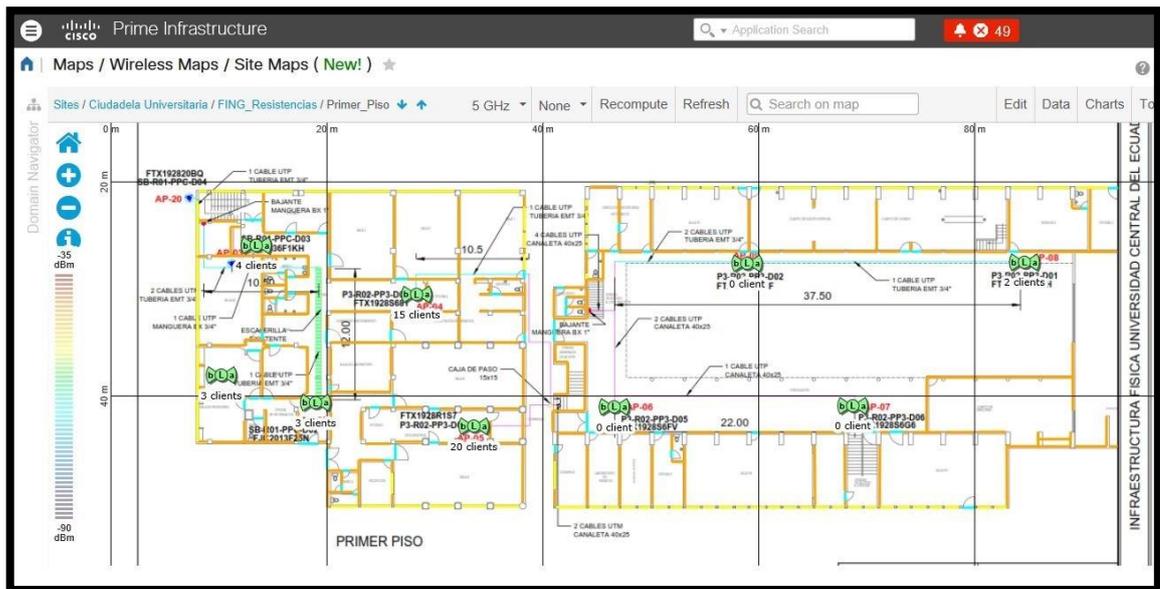
Fuente: Herramienta Cisco 8500 Series Wireless Controller.

Una vez que se obtiene los datos se procede al análisis de estos, y antes de sacar un resultado probable se toma en cuenta lo que se mencionó en el apartado “**10.3 Análisis de mecanismos de conectividad**” donde indica que uno de los estándares más utilizados en la Universidad Central del Ecuador es el IEEE 802.11N en banda de frecuencia 2.4GHz con 8607 clientes conectados según la Herramienta Prime Infrastructure, lo que quiere decir que este estándar posee alrededor del 80% de clientes conectados, es decir, los dispositivos finales tiene gran ventaja de clientes con respecto al estándar IEEE 802.11AC.

Sabiendo estos antecedentes se puede decir que los clientes poseen dispositivos (Pc, laptop, teléfonos móviles, tabletas) los cuales no cuentan en su tarjetería de red inalámbrica la compatibilidad necesaria para realizar la conexión a varios estándares o protocolo inalámbricos por lo que se deduce o aclara el motivo de que estos dispositivos opten en su mayoría por conectarse al estándar IEEE 802.11N en banda de frecuencia de 2.4GHz. Lo cual provoca que en este estándar tenga mayor utilización del canal (32%) y por ende mayor porcentaje de interferencias (32%), mayor uso del tráfico, un throughput de 45.9KB, posee una velocidad de transmisión y una intensidad de señal aceptable de acuerdo a la posición física del Access Point.

#### *3.12.1.2. Estándar IEEE 802.11AC en Cisco 8500 Series Wireless Controller.*

Al igual que en el estándar IEEE 802.11N mediante las herramientas Cisco se genera y se toma el mismo mapa de la infraestructura de la red inalámbrica con el fin de poder comparar los datos de los dos estándares, de la misma forma este consta de los parámetros ingresados en la controladora Cisco 8500 Series como estándar aplicado (IEEE 802.11AC), banda de frecuencia (5GHz), número de clientes por Access Point, intensidad de señal, entre otros, tal cual se muestra en la Figura 12-3.

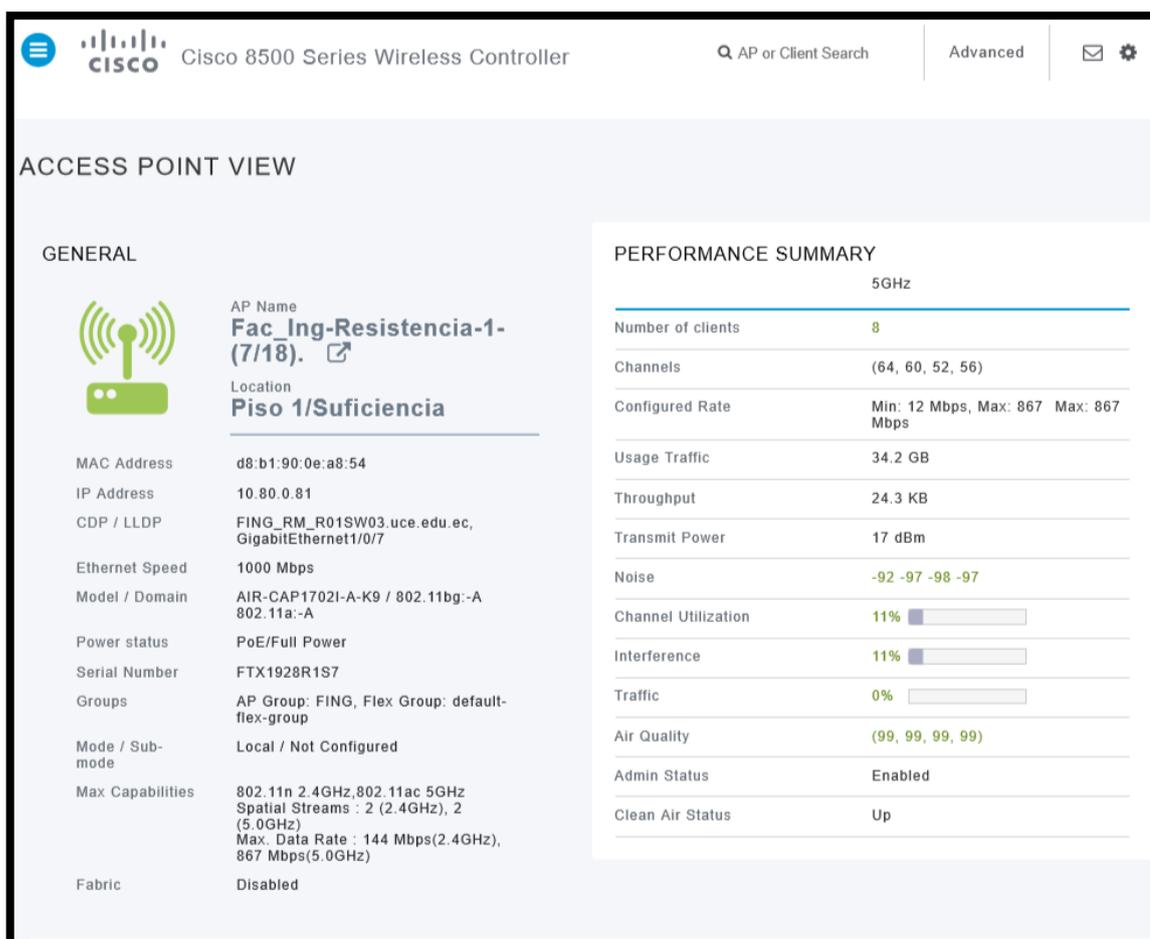


**Figura 12-3:** Estructura física del ambiente de prueba 802.11AC.

**Fuente:** Herramienta Cisco Prime Infrastructure.

De la misma forma se ubica el área a ser evaluada y se selecciona los parámetros necesarios que permitan obtener datos acerca del rendimiento de los Access Point mediante el mecanismo de conexión IEEE 802.11AC. Con esto se espera tener la misma información del estándar anterior para realizar la comparación, estos datos son: número de clientes conectados, canales utilizados, tasa de velocidad configurada, tráfico, throughput, poder de transmisión, ruido, utilización del canal e interferencia.

A manera general la herramienta Cisco 8500 Series Wireless Controller presenta datos del estándar 802.11AC en la banda de frecuencia 5GHz con los que se puede evaluar el rendimiento de este mecanismo de conexión, así como se muestra en la Figura 13-3.



**Figura 13-3:** Datos obtenidos en 802.11AC en 5GHz.

**Fuente:** Herramienta Cisco 8500 Series Wireless Controller.

Con los datos citados acerca del estándar que tiene mayor número de clientes y basándose en los resultados comparativos de los dos estándares se obtiene que los datos arrojados por el estándar 802.11AC son utilización del canal menor al estándar 802.11N (11%), menor porcentaje de interferencias con respecto al estándar 802.11N (11%), menor uso del tráfico en relación al estándar 802.11N, un throughput menor de 24.3.6KB, además posee una velocidad de transmisión y una intensidad de señal aceptable de acuerdo a la posición física del Access Point.

### 3.12.1.3. Tabla comparativa del Estándar IEEE 802.11N y 802.11AC en Cisco 8500 Series Wireless Controller.

En la Tabla 9-3 se presenta los resultados comparativos de los dos estándares donde indica los valores cuantificados por la herramienta Cisco 8500 Series Wireless Controller. Se compara las

tecnologías IEEE 802.11N y 802.11AC, donde indica que el estándar 802.11N posee una mejor calidad de señal, velocidad de transmisión más alta, throughput que tiene una mejor tasa de transferencia efectiva, así como también por la parte negativa mayor número de interferencias y una menor potencia de transmisión. Lo que lleva a pensar que este estándar tiene mejor rendimiento, siempre y cuando se dé a notar que dicho estándar también tiene mayor número de clientes lo que posiblemente causaría esta distinción, por otro lado, el mayor número de clientes no depende del estándar o modelo de Access Point sino más bien de la tarjetería de los dispositivos que se conectan a la red inalámbrica. Además, los datos obtenidos en la Tabla 9-3 muestran en color rojo los valores negativos y en amarillo los positivos, para emitir un porcentaje diferenciado entre los dos estándares, siendo el de mayores expectativas el estándar 802.11N con el 50% de valores positivos frente al 40% del estándar 802.11AC.

**Tabla 9-3:** Comparativa de los Estándares 802.11N y AC con Cisco 8500 Series.

INDICADOR	IEEE 802.11N	IEEE 802.11AC
Canales	1	60, 64, 52, 56
Ruido	97	92 - 97 - 98 - 97
Throughput	45.9KB	24.3KB
Interferencias	33%	11%
Trafico de red	108.1GB	34.2GB
Ancho de Canal (No considerado por ser valor fijo)	20MHz	80MHz
Calidad de la Señal	39dB	26dB
Utilización del Canal	33%	11%
Capacidad del Canal	144Mbps	867Mbps
Potencia de transmisión	16dBm	17dBm
Velocidad de transmisión	17Mbps	13Mbps
<b>TOTAL</b>	50%	40%

Realizado por: Edgar Ulloa.. 2020

### **3.12.2. Simulación en Cisco Prime Infrastructure.**

Cisco Prime Infrastructure es una herramienta de administración de red que proporciona una solución única para el aprovisionamiento, el monitoreo, la optimización y la resolución de problemas de dispositivos con cable e inalámbricos. Las interfaces gráficas robustas hacen que las implementaciones y operaciones de dispositivos sean simples y rentables.

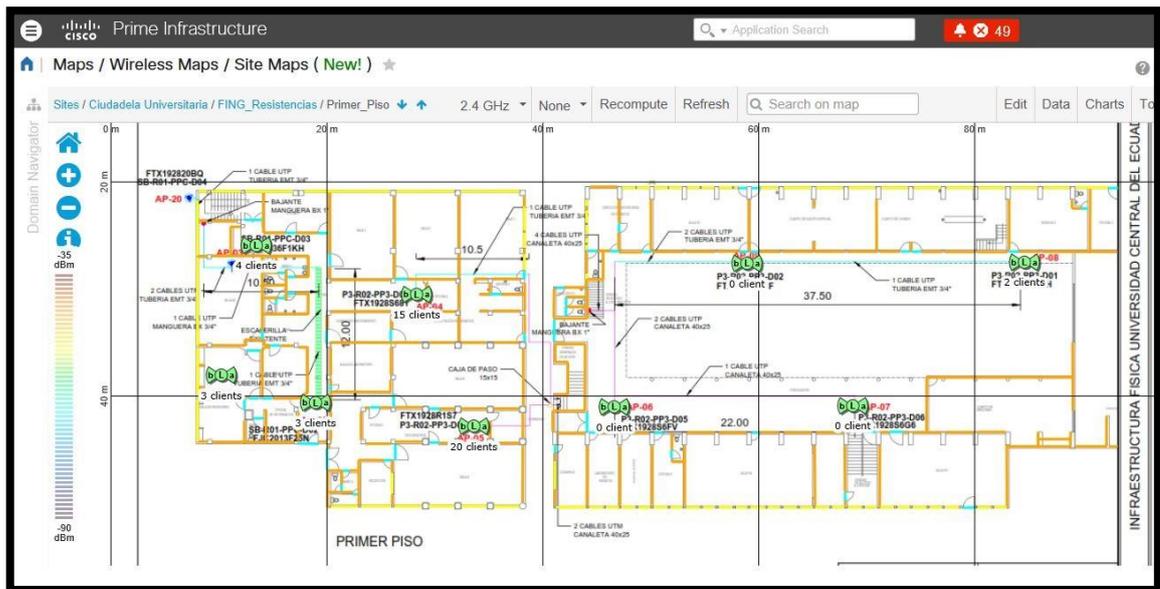
Posteriormente de realizar las simulaciones con la herramienta Cisco 8500 Series Wireless Controller se va a comparar ciertos datos en el Software señalado, es decir, Cisco Prime Infrastructure el cual es usado en las redes inalámbricas para obtención de datos optimización y monitoreo. Los datos utilizados son similares a los que se emplearon en la simulación con la herramienta Cisco 8500 Series Wireless Controller, siendo estos:

- Estándares IEEE 802.11N y estándar IEEE 802.11AC.
- Banda de frecuencia de 2.4GHz para el estándar IEEE 802.11N y banda de frecuencia de 5GHz para el estándar 802.11AC.
- Tipo de Antena: Depende de los Access Point a los cuales se les evalúa el rendimiento.
- Potencia del equipo: Cada estándar posee diferente potencia, por lo tanto, depende de este, de la distancia y de las interferencias.
- Posicionamiento Físico: Una correcta ubicación física dependerá del análisis estructural del área o espacio donde se instale el Access Point.

#### **3.12.2.1. Estándar IEEE 802.11N en Cisco Prime Infrastructure.**

Igual que la simulación anterior en la controladora, se plasma el mapa de la infraestructura de red inalámbrica con la herramienta Cisco Prime Infrastructure en esta se denotan varios elementos que intervienen en la toma de datos como extensión del área cubierta por los APs, número de Access Point, áreas físicas (paredes, puertas, ventanas), cables UTP, clientes conectados, banda de frecuencia en 2.4GHz, entre otros.

Esto con el fin de tener claro el ambiente en que se desarrollan los estándares en mención y ver cuál de ellos tiene un mejor rendimiento respecto al otro. A continuación, se presenta la Figura 14.3. donde se observa el mapa de simulación de la red inalámbrica en el estándar IEEE 802.11N en la banda de frecuencia de 2.4GHz.

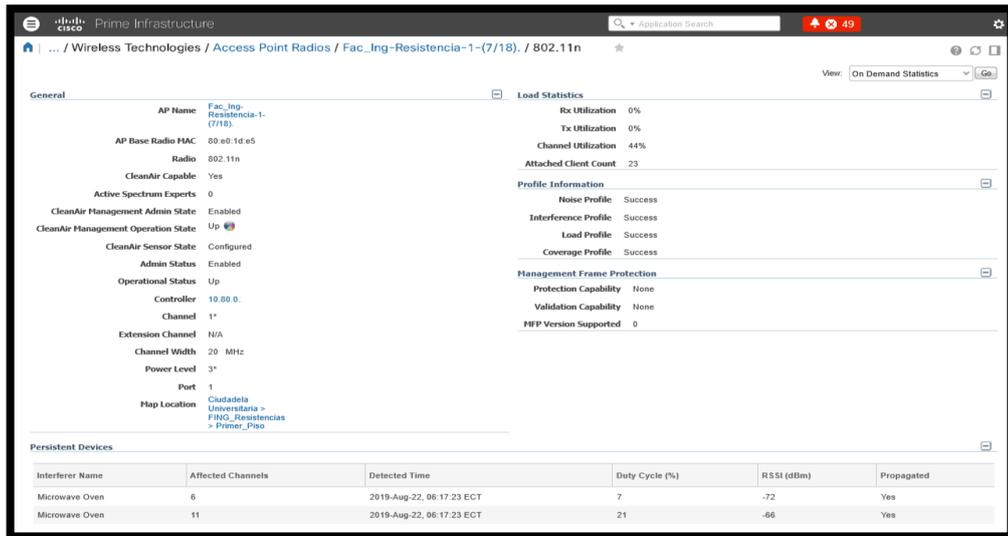


**Figura 14-3:** Esquema de Red inalámbrica IEEE 802.11N en 2.4GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

Seguidamente de la obtención del mapa de la infraestructura de red inalámbrica, mediante la Herramienta Cisco Prime Infrastructure se ingresan los parámetros necesarios para la obtención de datos. En la figura 15.3 a manera general se tiene el nombre del Access Point, Mac Address del dispositivo, IP del dispositivo, estándar Utilizado (IEEE 802.11N), canal utilizado (1), ancho de canal (20MHz), ubicación del mapa, utilización de Tx y Rx, clientes conectados, interferencias, intensidad de señal, calidad del aire, utilización del canal (44%), entre otros.

Cabe notar que gracias a esta herramienta también se puede visualizar el nombre de las interferencias y la medida de afectación con respecto a la señal emitida por el Access Point. Además, se muestran gráficos donde se valoran los datos principales que actúan en la comparativa de los dos estándares.



**Figura 15-3:** Datos obtenidos en IEEE 802.11N en 2.4GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

En el Gráfico 1-3 se observa el ancho de banda por tráfico de clientes, filtrado por el estándar IEEE 802.11N en la banda de frecuencia 2.4Ghz y que de acuerdo a la herramienta Cisco Prime Infrastructure oscila para sus valores máximos entre 290Mbps para bajada y 80Mbps para subida, es decir, debido a estos valores se llega a pensar que su utilización o demanda tiene una gran aceptación en los clientes. No obstante, nuevamente se hace énfasis en indicar que la mayor parte de clientes se conectan a este estándar debido a que sus dispositivos no cuentan con la capacidad necesaria para conectarse a varios estándares o al estándar más actual.

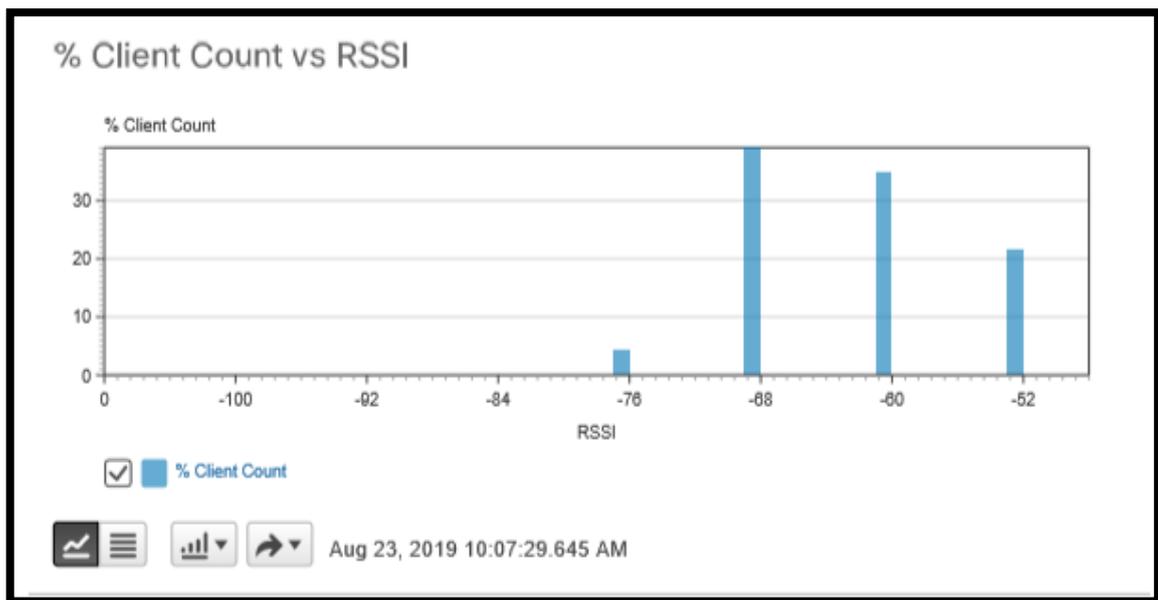


**Gráfico 1-3:** Tráfico de clientes en IEEE 802.11N 2.4GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

En lo que tiene que ver con la intensidad de señal en el Gráfico 2-3 se observa el porcentaje de clientes versus la potencia de señal, filtrado por el estándar IEEE 802.11N en la banda de frecuencia 2.4Ghz y de acuerdo a la herramienta Cisco Prime Infrastructure los valores oscilan entre -76dBm y -52dBm, debido a estos valores se llega a la conclusión que este estándar posee una calidad de señal en los rangos aceptables y traducida a como calidad de señal Muy buena según la Tabla 1-2. Equivalencias de intensidad de señal aceptables.

Así mismo se indica que la mayor parte de clientes se conectan a este estándar debido a que sus dispositivos no cuentan con la capacidad necesaria para conectarse a varios estándares o al estándar más actual.



**Gráfico 2-3:** Porcentaje de clientes vs intensidad de señal en IEEE 802.11N en 2.4GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

Al igual en lo que tiene que ver con la intensidad de señal en la Figura 16-3 se observa la potencia de señal emitida por el estándar IEEE 802.11N en la banda de frecuencia 2.4Ghz, así se tiene que la herramienta Cisco Prime Infrastructure presenta los datos a manera de mapa de calor, siendo los valores más altos representados por el color rojo oscuro (-35dBm) y los valores más bajos representados por el color verde oscuro (-90dBm), debido a estos valores se obtiene la conclusión que este estándar posee una calidad de señal aceptables ya que cubre la mayor parte del área física expuesta a la cobertura de la red inalámbrica.



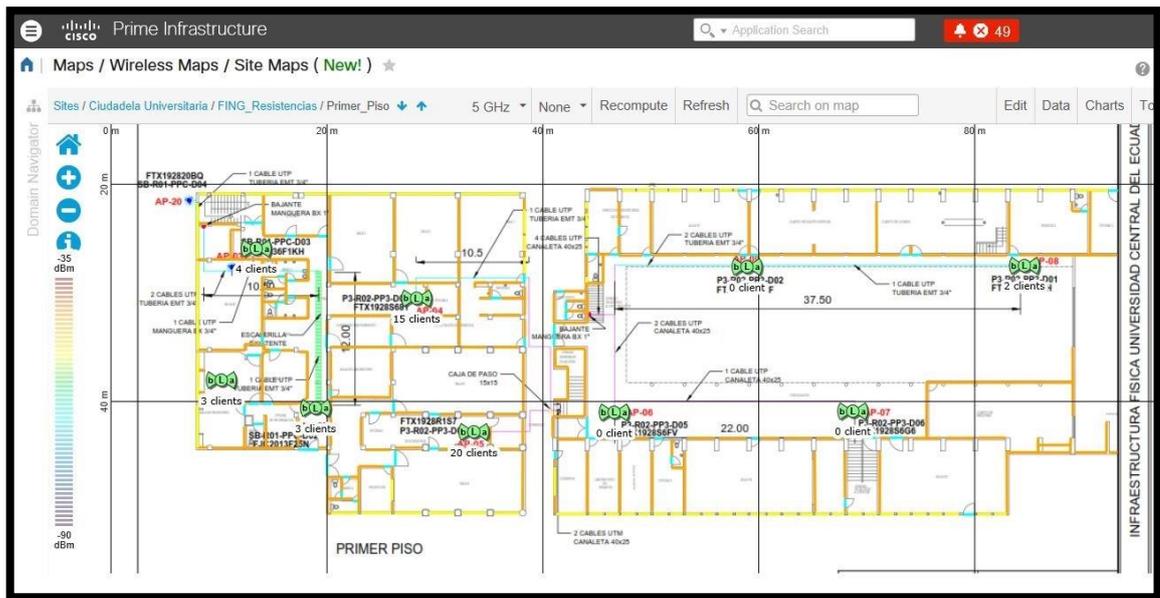
**Figura 16-3:** Potencia de señal en IEEE 802.11N en 2.4GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

### 3.12.2.2. Estándar IEEE 802.11AC en Cisco Prime Infrastructure.

Al igual que en el estándar anterior, primeramente, se obtiene el mapa en que se va a trabajar posteriormente se ingresa los parámetros relevantes para la obtención de datos como extensión del área cubierta por los APs, número de Access Point, áreas físicas (paredes, puertas, ventanas), cables UTP, clientes conectados, banda de frecuencia en 2.4GHz, entre otros.

A continuación, en la Figura 17-3 se presenta el mapa de la red inalámbrica en el estándar IEEE 802.11AC en banda de frecuencia de 5GHz.

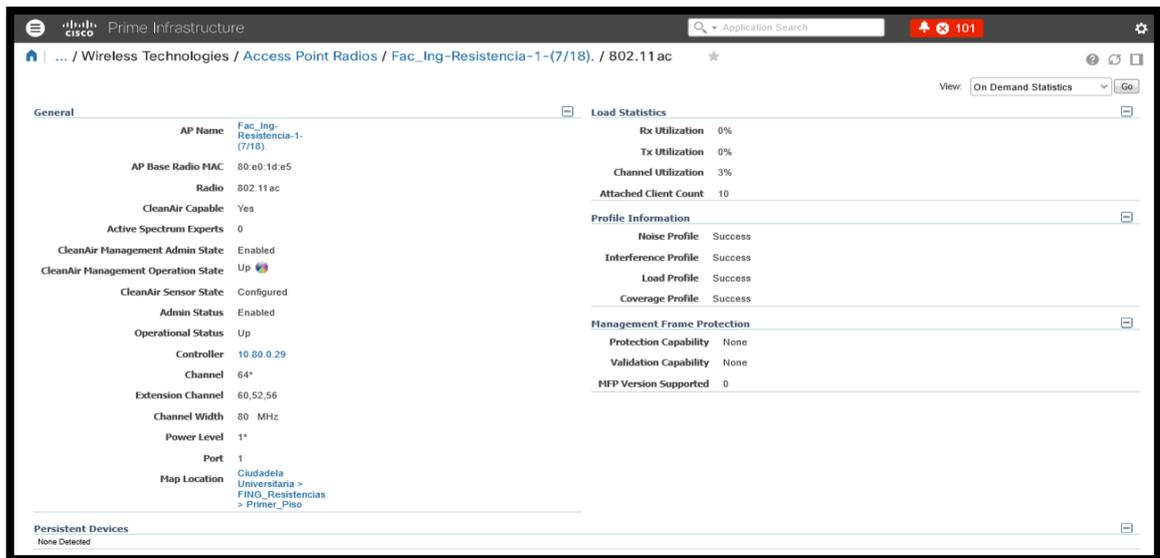


**Figura 17-3:** Esquema de Red inalámbrica IEEE 802.11AC en 5GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

En la Figura 18-3 se presenta de forma general datos del estándar IEEE 802.11AC en banda de frecuencia de 5GHz. Estos datos son evaluados según la herramienta Cisco Prime Infrastructure y arroja la siguiente información: nombre del Access Point, Mac Address del dispositivo, IP del dispositivo, estándar Utilizado (IEEE 802.11AC), canal utilizado (64), ancho de canal (80MHz), ubicación del mapa, utilización de Tx y Rx, clientes conectados, interferencias, intensidad de señal, calidad del aire, utilización del canal (3%), entre otros.

Cabe notar que gracias a esta herramienta también se puede visualizar el nombre de las interferencias y la medida de afectación con respecto a la señal emitida por el Access Point, en este caso no se encuentran dispositivos que afecten o interfieran la señal del este estándar.



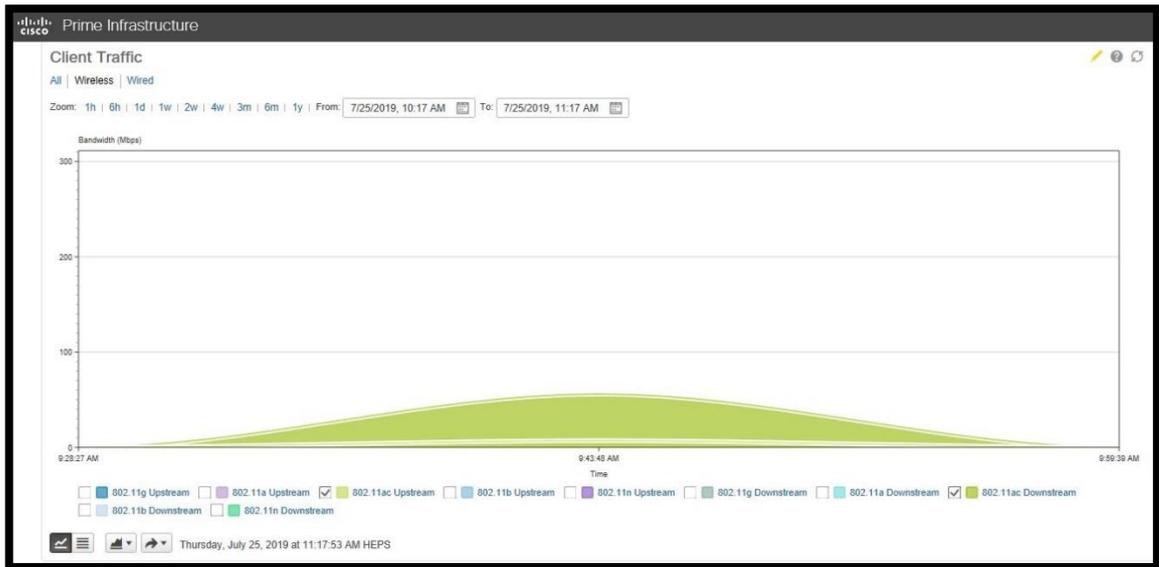
**Figura 18-3:** Datos obtenidos en IEEE 802.11AC en 5GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

Los valores obtenidos en la herramienta Cisco Prime Infrastructure muestran datos de importancia para poder evaluar y sacar conclusiones que permitan identificar el mejor mecanismo de conexión para redes con alta concurrencia de usuarios.

En el siguiente Gráfico 3-3 se muestra el ancho de banda que se maneja por el Tráfico de Clientes donde la velocidad máxima de descarga y subida de datos esta entre 100Mbps y 10Mbps respectivamente.

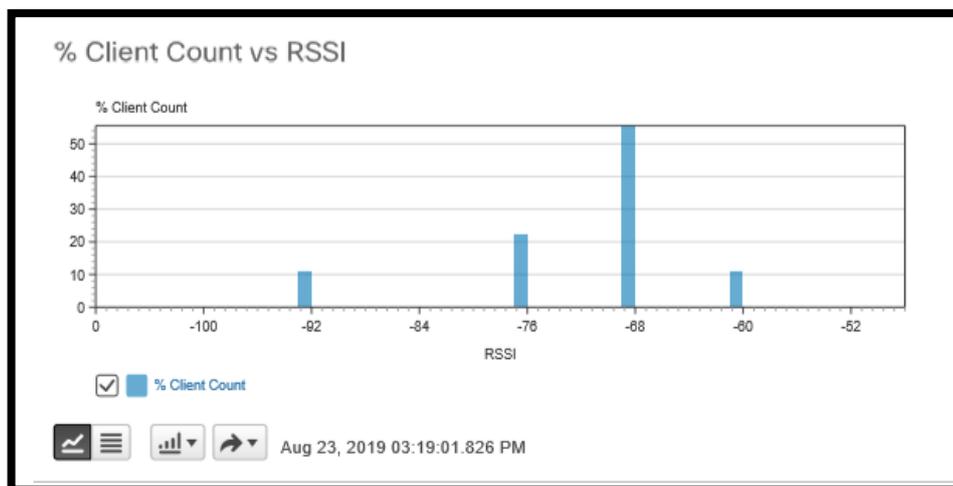
Analizando los datos de ambos estándares se llega a la conclusión que se alcanza mayores velocidades en el Estándar IEEE 802.11N y como ya antes se mencionó estos datos toman relevancia debido a que la mayoría de dispositivos optan por conectarse al estándar 802.11N, aclarando que toman esta opción por las capacidades individuales de cada dispositivo ya que no todos cuentan en su tarjeta de red inalámbrica la capacidad de conectarse a varios estándares o al estándar más actual.



**Gráfico 3-3:** Tráfico de clientes en IEEE 802.11AC 5GHz.

**Fuente:** Herramienta Cisco Prime Infrastructure.

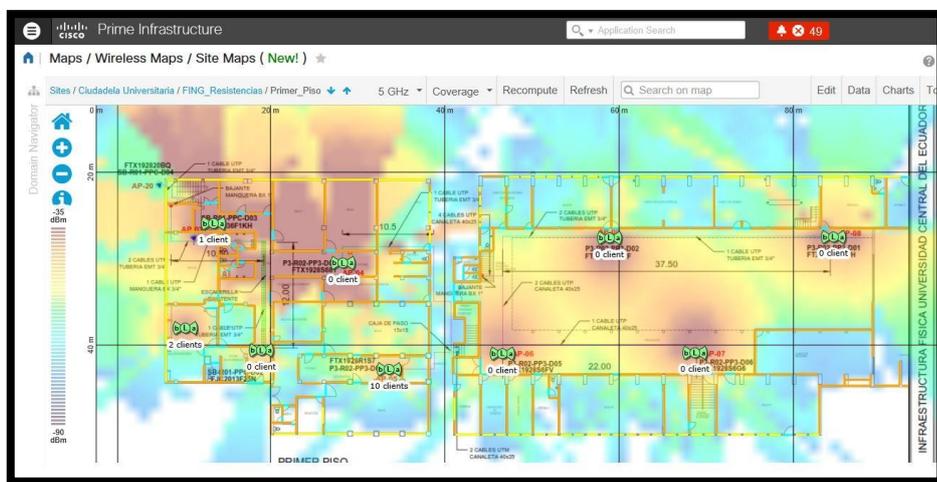
En el siguiente gráfico obtenido en la herramienta Cisco Prime Infrastructure muestra datos de importancia para poder evaluar y sacar conclusiones que permitan identificar el mejor mecanismo de conexión para redes con alta concurrencia de usuarios. En el Gráfico 4-3 se muestra el porcentaje de clientes versus la potencia de señal (dBm) donde se indica dicha potencia en un rango moderado el cual está entre -92dBm y -60dBm lo que significa que tiene una señal buena (cercana a una señal no tan buena) según la Tabla 1-2 Equivalencias de intensidad de señal aceptables. Lo que quiere decir que en este caso comparando los dos estándares el que obtiene mejor rendimiento es el 802.11N con respecto al 802.11AC.



**Gráfico 4-3:** Porcentaje de clientes vs intensidad de señal en IEEE 802.11AC en 5GHz.

Fuente: Herramienta Cisco Prime Infrastructure.

La Figura 19-3 al igual que en el estándar antepuesto muestra a manera de mapa de calor la potencia de señal en la que se desarrolla el estándar IEEE 802.11AC en la banda de frecuencia 5Ghz. Los valores más altos representados por el color rojo oscuro (-35dBm) y los valores más bajos representados por el color verde oscuro (-90dBm), en conclusión, a estos valores se obtiene que este estándar posee una potencia de señal aceptable ya que cubre gran parte del área física expuesta a la cobertura de la red inalámbrica. Pero en comparación con el estándar IEEE 802.11N se observa que tiene menor calidad de señal, por lo tanto, el que presenta mejor rendimiento es el Estándar 802.11N con respecto al Estándar 802.11AC.



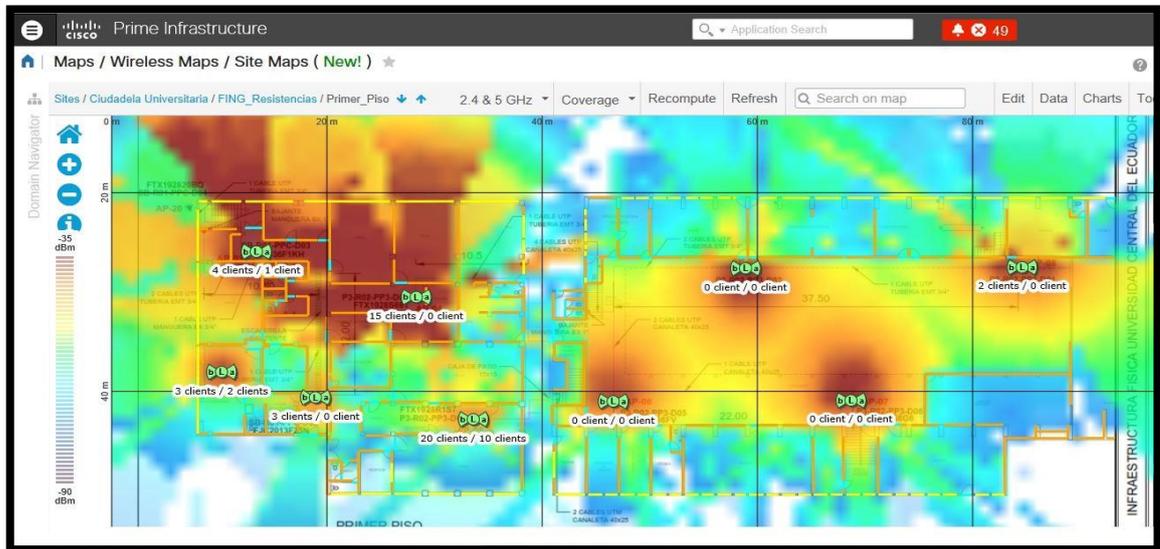
**Figura 19-3:** Potencia de señal en IEEE 802.11N en 2.4GHz.

Fuente: Herramienta Cisco Prime Infrastructure.

*3.12.2.3. Tabla comparativa del Estándar IEEE 802.11N y 802.11AC en Cisco Prime Infrastructure.*

Una vez que se obtuvo los datos del Estándar IEEE 802.11N y el Estándar IEEE 802.11AC mediante la herramienta Cisco Prime Infrastructure, se inicia la comparación de los datos equivalentes en esta simulación para lo cual primeramente se presenta la Figura 20-3 donde presenta la intensidad de señal en forma de mapa de calor, interviniendo los dos estándares 802.11N y 802.11AC en bandas de frecuencia 2.4GHz y 5Ghz respectivamente.

Claramente se observa en este mapa que la potencia de señal en los dos estándares es similar, pero guiándose en los resultados individuales anteriores se notó que el estándar 802.11N tiene un rendimiento mejorado con respecto al 802.11AC en lo que tiene que ver a la intensidad de señal.



**Figura 20-3:** Comparación de potencia de señal IEEE 802.11N y AC.

Fuente: Herramienta Cisco Prime Infrastructure.

A continuación, en la Tabla 10-3 se presenta los datos obtenidos de la Herramienta Cisco Prime Infrastructure. Las comparaciones de los dos estándares indican los valores cuantificados por los mecanismos de conexión IEEE 802.11N y 802.11AC, los mismos que al ser comparados recaen sobre el estándar 802.11N ya que posee una mejor calidad de señal, el tráfico de red muestra los datos que pasan por la red por lo tanto la velocidad de trasmisión es más alta según los datos obtenidos, así como también por la parte negativa este tiene mayor número de interferencias.

**Tabla 10-3:** Comparativa de los Estándares 802.11N y AC con Cisco Prime Infrastructure.

INDICADOR	IEEE 802.11N	IEEE 802.11AC
Frecuencia	2.4GHz	5GHz
Canales	1*	64*, 60, 52, 56
Interferencias por canal	1, 6, 11	44, 64, 149
Tráfico de red	290Mbps	100Mbps
Ancho de Canal (No considerado por valor fijo)	20MHz	80MHz

Intensidad de la Señal	-76dBm a -52dBm	-92dBm a -60dBm
Utilización del Canal	44%	03%
Capacidad del Canal	144Mbps	867Mbps
Velocidad de transmisión	Mayor según tráfico de red	Menor según tráfico de red
<b>TOTAL</b>	57,14%	28,57%

Realizado por: Edgar Ulloa.. 2020

Además, de los 7 indicadores evaluados en esta simulación de Cisco Prime Infrastructure se obtiene en color rojo los valores negativos y en amarillo los valores positivos dando como resultado 57,14% a favor del estándar 802.11N y 28,57% a favor del estándar 802.11AC.

En conclusión, las redes con alta concurrencia de usuarios tienden a conectarse al estándar 802.11N, es decir, tienen mayor número de clientes lo que posiblemente causaría que los datos se inclinen por este estándar, por otro lado, hay q recalcar que tener mayor número de conexiones no depende del estándar o modelo de Access Point sino más bien de la disponibilidad de la tarjetería de los dispositivos que se conectan a la red inalámbrica.

La mayoría de conexiones a los AP provienen de teléfonos móviles tal cual se muestra en la Figura 21-3 que señala que las conexiones se realizan mediante el sistema operativo Android los mismos que son parte fundamental en los teléfonos móviles.

	Name	Clients
1	Android	2844
2	Android-Samsung-Galaxy-Phone	969
3	Microsoft-Workstation	418
4	Samsung-Device	260
5	Apple-Device	233
6	Android-LG	99
7	Workstation	97
8	Intel-Device	74
9	Windows8-Workstation	67
10	Apple-iPhone	47

**Figura 21-3:** Top de sistemas operativos activos en la red inalámbrica.

**Fuente:** Herramienta Cisco 8500 Series Wireless Controller.

Así también se muestran en las Figuras 22-3 y 23-3 con respecto a los teléfonos móviles las especificaciones técnicas de conectividad, indicando que los móviles de gama alta poseen los

estándares 802.11 a/b/g/n/ac 2.4GHz+5GHz y los dispositivos de gama media/baja poseen los estándares 802.11 b/g/n 2.4GHz, y tratándose de una institución pública es entendible pensar que no todos los usuarios pueden tener un móvil de alta gama por su alto valor económico, lo cual justifica que las conexiones en redes con alta concurrencia de usuarios estén más orientadas hacia el estándar 802.11N.

Galaxy S7 edge		
VENTAJAS	ESPECIFICACIONES	RESEÑAS
<b>Conectividad</b>		
ANT+	Sí	Localización GPS, Glonass, Beidou
Auriculares	3.5mm Stereo	Wi-Fi 802.11 a/b/g/n/ac 2.4G+5GHz, VHT80 MU-MIMO
	Versión USB USB 2.0	MHL No

**Figura 22-3:** Estándar Wifi móvil gama alta.

Fuente: Samsung.com.

Galaxy J8 (Dual-SIM)		
BENEFICIOS	SPECS	RESEÑAS
<b>Conectividad</b>		
ANT+	Sí	Versión USB USB 2.0
Localización	GPS, Glonass, Beidou	MHL No
Wi-Fi	802.11 b/g/n 2.4GHz	Versión Bluetooth Bluetooth v4.2
	USB Interface Micro USB	Auriculares 3.5mm Stereo
	Wi-Fi Direct Sí	

**Figura 23-3:** Estándar Wifi móvil gama media.

Fuente: Samsung.com.

## CAPÍTULO IV

### 4. RESULTADOS Y DISCUSIÓN.

En el capítulo tres como primer punto se realizó el análisis de los mecanismos de conexión que están en auge en la actualidad y que a su vez tiene mayor impacto dentro de la Universidad Central del Ecuador. Estos mecanismos deben abarcar ciertos parámetros (Latencia, intensidad de señal, calidad de conexión, entre otros) medibles que permitan evaluar el rendimiento de los dispositivos Access Point en redes con alta concurrencia de usuarios, siendo los que recogen todas estas características los estándares IEEE 802.11N y AC.

En segundo punto se analizó y comparó dichos estándares para conocer ventajas y desventajas de su utilización, además se realizaron simulaciones en escenarios de pruebas y finalmente se realizaron pruebas en la red física inalámbrica para obtener resultados comparables de las dos tecnologías.

El presente capítulo se fundamenta en comparar los dos mecanismos de conectividad (estándares o protocolos) 802.11N y 802.11AC para ver los efectos que causa cada estándar dentro de la red inalámbrica de la Universidad Central del Ecuador, es decir evaluar el rendimiento versus los usuarios concurrentes que posee cada mecanismo de conexión. Los indicadores de mayor importancia que se evalúan dentro de cada estándar son: Intensidad de señal, la Calidad de conexión y el Throughput, de cada uno de estos indicadores se necesita saber y tener claro el número de datos a ser evaluados, por esto en el capítulo anterior se ejecutó los cálculos para la población de estudio y la muestra, mediante estos dos parámetros se obtendrán los datos finales.

#### 4.1. Selección de la prueba estadística.

Para la evaluación del rendimiento de dispositivos Access Point mediante mecanismos de conectividad en redes con alta concurrencia de usuarios se ha seleccionado los indicadores debido a la importancia y a la influencia directa que tienen en el rendimiento, siendo estos: la intensidad de señal, la calidad de conexión y el throughput, es decir indicadores que emitan datos numéricos medibles de los usuarios de la Universidad Central del Ecuador, mediante estos datos se realizará

comparación de los dos mecanismos de conectividad y finalmente se determinará el rendimiento de la red. Para esto se realizan cálculos estadísticos para cada indicador.

La selección del proceso estadístico identifica la manera correcta de procesar los datos, tal cual se muestra en la Tabla 1-4. Ahora bien, analizando dicha Tabla 1-4 y los datos que intervienen en esta investigación se tiene lo siguiente:

- Comparar dos grupos diferentes, es decir los dos mecanismos de conectividad en un mismo tiempo, siendo el estándar IEEE 802.11N el primer grupo y el estándar 802.11AC el segundo grupo, en estos dos estándares o grupos se seleccionan datos de los indicadores bajo las mismas consideraciones y parámetros (Intensidad de Señal, Calidad de Conexión y Throughput).
- De la misma forma se necesita cotejar grupos o muestras independientes (cuando los individuos de una muestra son distintos a los individuos de otra muestra) a través de la comparación de las medias de dos grupos de casos.

Entonces al evaluar la variable fija resulta que este caso es de Estudio Transversal ya que evalúa a dos grupos, el grupo 802.11N y al grupo 802.11AC en un mismo momento. Y la variable aleatoria sería la Numérica que en este caso serían los datos de cada indicador (Intensidad de Señal, Calidad de Conexión y Throughput). Por lo tanto, se selecciona la prueba T de Student para muestras independientes.

**Tabla 1-4:** Selección de la prueba estadística.

		PRUEBAS NO PARAMÉTRICAS			PRUEBAS PARAMÉTRICAS
Variable Aleatoria		NOMINAL DICOTÓMICA	NOMINAL POLITÓMICA	ORDINAL	NUMÉRICA
Variable Fija					
Estudio Transversal	Un grupo	X <sup>2</sup> Bondad de Ajuste Binomial	X <sup>2</sup> Bondad de Ajuste	X <sup>2</sup> Bondad de Ajuste	T de Student (una muestra)
	Dos grupos	X <sup>2</sup> Bondad de Ajuste Corrección de Yates Test exacto de Fisher	X <sup>2</sup> de Homogeneidad	U Mann-Withney	T de Student (muestras independientes)
	Muestras Independientes	Más de dos grupos	X <sup>2</sup> Bondad de Ajuste	H Kruskal-Wallis	ANOVA con un factor INTERsujetos
Estudio Longitudinal	Dos medidas	Mc Nemar	Q de Cochran	Wilcoxon	T de Student (muestras relacionadas)

Muestras Relacionadas	Más de dos medidas	Q de Cochran	Q de Cochran	Friedman	ANOVA para medidas repetidas INTERsujetos
-----------------------	--------------------	--------------	--------------	----------	---

Realizado por: Edgar Ulloa.. 2020

También se toma en consideración que el tamaño de la muestra para la prueba T de Student es determinada en la prueba de normalidad utilizando Kolmogorov-Smirnov cuando las muestras son grandes (mayor a 30 datos) y Shapiro-Wilk cuando las muestras son pequeñas (menor a 30 datos) tal cual se evidencia en el siguiente enunciado: “La T de Student, inicialmente se diseñó para examinar las diferencias entre dos muestras independientes y pequeñas que tengan distribución normal y homogeneidad en sus varianzas (en el artículo original, el autor no define qué es una muestra grande y/o pequeña). **William Sealy Gosset** hace hincapié en la normalidad de las dos muestras como crucial en el desarrollo de la prueba” (*Sánchez Turcios, 2015*).

#### 4.1.1. Selección del valor alfa ( $\alpha$ ).

De acuerdo a los cálculos en la prueba T de Student se necesita conocer el nivel o valor de alfa (nivel de significancia), el mismo que sería el porcentaje de error que se utilizará en las pruebas, por lo tanto, este valor será del 5% ya que debe ser igual al valor que se utilizó en el cálculo de la muestra.

$$\text{Alfa} = \alpha = 5\% = 0,05$$

#### 4.1.2. Selección del Software estadístico.

Para la obtención de resultados esta investigación se inclinó por seleccionar al Software SPSS (Statistical Package for the Social Sciences) que es un programa estadístico informático y que en la actualidad pertenece a IBM, este software se utiliza para realizar la recolección y análisis de datos dando como resultado tablas, gráficas y datos procesados. El SPSS se destaca por la capacidad de procesar un sin número de volúmenes de registros en poco tiempo.

## 4.2. Prueba T de Student para muestras independientes.

Como antecedente para obtener resultados de la prueba T de Student se debe redactar la hipótesis alterna y la hipótesis nula, posteriormente la prueba T de Student para muestras independientes se ejecuta en el software de IBM SPSS donde se ingresa los datos y se obtiene P-valor, pero para ello se debe pasar por los siguientes filtros: normalidad y la igualdad de varianza.

### 4.2.1. Prueba T de Student del indicador Intensidad de Señal.

Los parámetros de normalidad y la prueba de igualdad de varianzas son filtros que se deben pasar con el fin de obtener el cálculo del P-valor de la prueba T de Student para muestras independientes en la evaluación del indicador Intensidad de señal.

Lo primero que se hará es redactar la hipótesis estadística, es decir la hipótesis alterna y la hipótesis nula de la siguiente manera:

**H<sub>1</sub>** = Existe una diferencia significativa entre la media de Intensidad de señal con el estándar 802.11N y la media de Intensidad de señal con el estándar 802.11AC.

**H<sub>0</sub>** = No existe una diferencia significativa entre la media de Intensidad de señal con el estándar 802.11N y la media de Intensidad de señal con el estándar 802.11AC.

#### 4.2.1.1. Normalidad en el indicador Intensidad de señal.

En la prueba de normalidad se debe corroborar que la variable aleatoria en ambos casos 802.11N y 802.11AC se distribuye normalmente, para esto se usa la prueba de Kolmogorov-Smirnov ya que el tamaño de la muestra es mayor a 30 datos. El criterio para determinar si la variable aleatoria se distribuye normalmente es:

P-valor  $\Rightarrow$   $\alpha$  Aceptar **H<sub>0</sub>** = Los datos provienen de una distribución normal.

P-valor  $<$   $\alpha$  Aceptar **H<sub>1</sub>** = Los datos **No** provienen de una distribución normal.

Mediante el software estadístico de IBM SPSS se realizan los respectivos cálculos para la normalidad, una vez que se ingresó los datos, arroja los siguientes resultados como se puede ver en la Tabla 2-4:

**Tabla 2-4:** Normalidad del indicador Intensidad de señal.

Pruebas de normalidad							
Estándares		Kolmogorov-Smirnov			Shapiro-Wilk		
		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Intensidad De Señal	802.11n	0,052	373	,200*	0,990	373	0,705
	802.11ac	0,060	373	,200*	0,995	373	0,971

Realizado por: Edgar Ulloa.. 2020

En este indicador se observa el nivel de significancia evaluada por Kolmogorov-Smirnov para normalidad, ya que los datos ingresados son mayores a 30, estos datos son tomados de la Tabla 2-4 con el fin de ser comparados con el valor de alfa como se muestra a continuación:

$$P\text{-valor de } 802.11N = 0.200 > \alpha = 0.05$$

$$P\text{-valor de } 802.11AC = 0.200 > \alpha = 0.05$$

Entonces se observa que P-valor es mayor que el valor alfa en los dos casos, por lo tanto, se Acepta la  $H_0$ , lo que quiere decir que estos datos provienen de una distribución normal al demostrar que la Intensidad de señal en los dos mecanismos de conexión se comporta normalmente y puede dar paso al siguiente filtro para la prueba T de Student.

#### 4.2.1.2. Igualdad de varianzas en el indicador Intensidad de señal.

Al igual que en la normalidad la igualdad de varianzas es otro filtro que se debe pasar con el fin de obtener el cálculo del P-valor y así pasar a la prueba T de Student para muestras independientes en la evaluación de la variable Intensidad de señal. Entonces si las varianzas son iguales se cumple con este filtro y se procede al análisis de la hipótesis. Para la igualdad de varianzas se usa las siguientes consideraciones:

P-valor  $\Rightarrow \alpha$  Aceptar  $H_0$  = Las varianzas son iguales.

P-valor  $< \alpha$  Aceptar  $H_1$  = Existe diferencia significativa en las varianzas.

**Tabla 3-4:** Igual de varianzas del indicador Intensidad de señal.

<b>Prueba T de Student de muestras independientes</b>			
		Prueba de Levene de igualdad de varianzas	
		F	Sig.
Intensidad de Señal	Se asumen varianzas iguales	1,283	0,259
	No se asumen varianzas iguales		

Realizado por: Edgar Ulloa.. 2020

La igualdad de varianzas se valida mediante la prueba de Levene, en esta prueba se obtuvo los siguientes datos tal como muestra la Tabla 3-4.

$$P\text{-valor} = 0.259 > \alpha = 0.05$$

Entonces se observa que P-valor es mayor que alfa por lo que se acepta  $H_0$  y por lo tanto se asume que las varianzas son iguales. De esta forma se corrobora que se cumple los dos supuestos tanto el de normalidad como el de igualdad varianza para poder seguir con el P-valor de la prueba T de Student para muestras independientes.

#### 4.2.1.3. Resultados prueba T de Student.

Una vez que se corroboró la normalidad y la igualdad de varianzas, ya se puede obtener el P-valor para la prueba T de Student, mediante el siguiente criterio:

Si la probabilidad obtenida en **P-valor**  $\leq \alpha$ , **rechace  $H_0$**  (Se Acepta  **$H_1$** )

Si la probabilidad obtenida en **P-valor**  $> \alpha$ , **no rechace  $H_0$**  (Se Acepta  **$H_0$** )

Recordando el apartado 4.2.1. Prueba T de Student para la variable Intensidad de señal se obtiene lo siguiente:

**$H_1$**  = Existe una diferencia significativa entre la media de Intensidad de señal con el estándar 802.11N y la media de Intensidad de señal con el estándar 802.11AC.

$$H_1: \mu_a \neq \mu_b$$

$H_0$  = No existe una diferencia significativa entre la media de Intensidad de señal con el estándar 802.11N y la media de Intensidad de señal con el estándar 802.11AC.

$H_0: \mu_a = \mu_b$

En el software de IBM SPSS se obtienen los resultados de la variable intensidad de señal, en la Tabla 4-4 se observa el valor de significancia bilateral, el mismo que se toma en base al parámetro “Se asumen varianzas iguales”.

**Tabla 4-4:** T de Student para el indicador Intensidad de señal.

Prueba de muestras independientes						
Prueba T de Student para la igualdad de medias						
t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	95% de intervalo de confianza de la diferencia	
					Inferior	Superior
-3,141	188	0,002	-4,653	1,481	-7,575	-1,730
-3,141	183,606	0,002	-4,653	1,481	-7,576	-1,730

Realizado por: Edgar Ulloa.. 2020

En razón a la Tabla 4-4 se toma el valor obtenido, siendo este de 0.002 y que de acuerdo al criterio antes mencionado se puede decir que:

$$P\text{-valor} = 0.002 \leq \alpha = 0.05$$

Entonces se observa que P-valor es menor que alfa, por lo tanto, se rechaza  $H_0$  y se da paso a  $H_1$ : Existe una diferencia significativa entre la media de Intensidad de señal con el estándar 802.11N y la media de Intensidad de señal con el estándar 802.11AC.

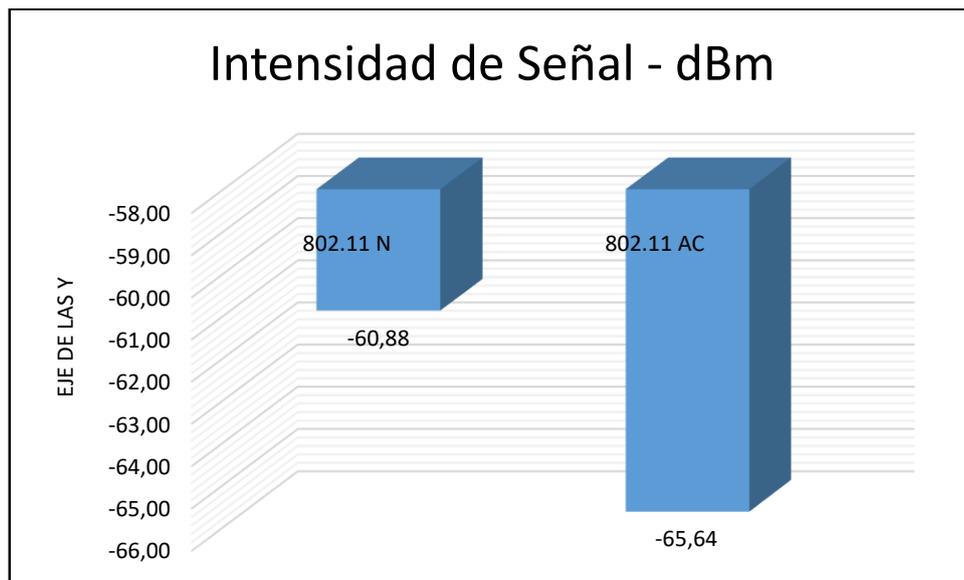
En la Tabla 5-4. se puede ver los resultados de las medias de intensidad de señal entre el estándar 802.11N y el estándar 802.11AC. Los cuales toman los siguientes valores: En el estándar IEEE 802.11N se tiene -60,88 dBm y en el estándar IEEE 802.11AC se tiene -65,54 dBm, sabiendo que la intensidad de señal se mide dBm y que mientras más cercano este al 0 (cero) indica que tiene mejor intensidad de señal, así se tiene que el estándar IEEE 802.11N tiene mejor rendimiento en comparación con el estándar IEEE 802.11AC en redes con alta concurrencia de usuarios con respecto al indicador intensidad de señal.

**Tabla 5-4:** Comparación de medias del indicador Intensidad de señal.

Estadísticas de grupo					
Estándares		N	Media	Desv. Desviación	Desv. Error promedio
Intensidad de Señal	802.11n	373	-60,88	9,387	0,963
	802.11ac	373	-65,54	10,972	1,126

Realizado por: Edgar Ulloa.. 2020

En el Gráfico 1-4. se observa los resultados de los dos estándares analizados, mostrando en su eje negativo los valores que se obtuvieron mediante la prueba T de Student en el indicador Intensidad de señal, cuyos valores son -60,88 dBm y -65,54 dBm para los estándares 802.11N y 802.11AC respectivamente, tomando como referencia que el valor es óptimo mientras más cercano este al cero, es decir el estándar 802.11N presenta mejor rendimiento sobre el estándar 802.11AC en redes con alta concurrencia de usuarios.



**Gráfico 1-4:** Comparación de IEEE 802.11N y AC del indicador Intensidad de Señal.

Realizado por: Edgar Ulloa.. 2020

#### 4.2.1.4. Decisión estadística.

Una vez concluidas las pruebas de T de Student para muestras independientes de la variable Intensidad de Señal se establece la siguiente conclusión: Existe una diferencia significativa entre

la media de Intensidad de señal con el estándar 802.11N y la media de Intensidad de señal con el estándar 802.11AC.

Es decir, el estándar IEEE 802.11N presenta -60,88 dBm y en el estándar IEEE 802.11AC presenta -65,54 dBm, sabiendo que la intensidad de señal se mide dBm y que mientras más cercano este al 0 (cero) indica que tiene mejor intensidad de señal, se establece que el estándar IEEE 802.11N tiene mejor rendimiento o tiene ventajas en comparación con el estándar IEEE 802.11AC con respecto a la intensidad de señal en redes con alta concurrencia de usuarios.

#### **4.2.2. Prueba T de Student del indicador Calidad de Conexión.**

Como se mencionó anteriormente la prueba de normalidad y la prueba de igualdad de varianzas son filtros que se deben pasar con el fin de obtener el cálculo del P-valor de la prueba T de Student para muestras independientes en la evaluación de la variable Calidad de conexión.

Lo primero que se hará es redactar la hipótesis estadística, es decir la hipótesis alterna y la hipótesis nula de la siguiente manera:

**H<sub>1</sub>** = Existe una diferencia significativa entre la media de Calidad de conexión en el estándar 802.11N y la media de Calidad de conexión en el estándar 802.11AC.

**H<sub>0</sub>** = No existe una diferencia significativa entre la media de Calidad de conexión en el estándar 802.11N y la media de Calidad de conexión en el estándar 802.11AC.

##### **4.2.2.1. Normalidad en el indicador Calidad de conexión.**

En la prueba de normalidad se debe ratificar que la variable aleatoria en ambos casos 802.11N y 802.11AC se distribuye normalmente, para esto se usa la prueba de Kolmogorov-Smirnov ya que el tamaño de la muestra es mayor a 30 datos. El criterio para determinar si la variable aleatoria se distribuye normalmente es:

P-valor  $\Rightarrow \alpha$  Aceptar **H<sub>0</sub>** = Los datos provienen de una distribución normal.

P-valor  $< \alpha$  Aceptar **H<sub>1</sub>** = Los datos No provienen de una distribución normal.

Mediante el software estadístico de IBM SPSS se realizan los respectivos cálculos para la normalidad, una vez que se ingresó los datos, arroja los siguientes resultados como se puede ver en la Tabla 6-4:

**Tabla 6-4:** Normalidad del indicador Calidad de conexión.

Pruebas de normalidad							
Estándares		Kolmogorov-Smirnov			Shapiro-Wilk		
		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Calidad de Conexión	802.11n	0,076	373	,200*	0,982	373	0,235
	802.11ac	0,072	373	,200*	0,976	373	0,072

Realizado por: Edgar Ulloa.. 2020

En este indicador se observa el nivel de significancia evaluada por Kolmogorov-Smirnov para normalidad, ya que los datos ingresados son mayores a 30, estos datos son tomados de la Tabla 6-4 con el fin de ser comparados con el valor de alfa como se muestra a continuación:

$$P\text{-valor de } 802.11N = 0.200 > \alpha = 0.05$$

$$P\text{-valor de } 802.11AC = 0.200 > \alpha = 0.05$$

Entonces se observa que P-valor es mayor que el valor alfa tanto en el estándar 802.11N y en el estándar 802.11AC, por lo tanto, se Acepta la  $H_0$ , lo que quiere decir que estos datos provienen de una distribución normal al demostrar que la Calidad de conexión en los dos mecanismos de conexión se comporta normalmente y puede dar paso al siguiente filtro para la prueba T de Student.

#### 4.2.2.2. Igualdad de varianzas en el indicador Calidad de conexión.

Al igual que en la normalidad la igualdad de varianzas es otro filtro que se debe pasar con el fin de obtener el cálculo del P-valor y así pasar a la prueba T de Student para muestras independientes en la evaluación de la variable Calidad de conexión. Entonces si las varianzas son iguales se cumple con este filtro y se procede al análisis de la hipótesis. Para la igualdad de varianzas se usa las siguientes consideraciones:

P-valor  $\Rightarrow \alpha$  Aceptar  $H_0$  = Las varianzas son iguales.

P-valor  $< \alpha$  Aceptar  $H_1$  = Existe diferencia significativa en las varianzas.

**Tabla 7-4:** Igual de varianzas del indicador Calidad de conexión.

Prueba T de Student de muestras independientes			
		Prueba de Levene de igualdad de varianzas	
		F	Sig.
Calidad de Conexión	Se asumen varianzas iguales	0,197	0,658
	No se asumen varianzas iguales		

Realizado por: Edgar Ulloa.. 2020

La igualdad de varianzas se valida mediante la prueba de Levene, en esta prueba se obtuvo los siguientes datos tal como muestra la Tabla 7-4.

$$P\text{-valor} = 0.658 > \alpha = 0.05$$

Entonces se observa que P-valor es mayor que el valor alfa, por lo que se acepta  $H_0$  y por lo tanto se asume que las varianzas son iguales. De esta forma se corrobora que se cumple los dos supuestos tanto el de normalidad como el de igualdad varianza para poder seguir con el cálculo del P-valor de la prueba T de Student para muestras independientes.

#### 4.2.2.3. Resultados prueba T de Student.

Luego que se corrobora la normalidad y la igualdad de varianzas, ya se puede obtener el P-valor para la prueba T de Student, mediante el siguiente criterio:

Si la probabilidad obtenida en **P-valor**  $\leq \alpha$ , **rechace  $H_0$**  (Se Acepta  **$H_1$** )

Si la probabilidad obtenida en **P-valor**  $> \alpha$ , **no rechace  $H_0$**  (Se Acepta  **$H_0$** )

Recordando el apartado 4.2.2. Prueba T de Student para la variable Calidad de Conexión se obtiene lo siguiente:

**$H_1$**  = Existe una diferencia significativa entre la media de Calidad de conexión en el estándar 802.11N y la media de Calidad de conexión en el estándar 802.11AC.

**$H_1$** :  $\mu_a \neq \mu_b$

**$H_0$**  = No existe una diferencia significativa entre la media de Calidad de conexión en el estándar 802.11N y la media de Calidad de conexión en el estándar 802.11AC.

$$H_0: \mu_a = \mu_b$$

En el software de IBM SPSS se obtienen los resultados de la variable Calidad de Conexión de la prueba de T de Student, la Tabla 8-4 muestra el valor de significancia bilateral, el mismo que se toma o se selecciona en base al parámetro “Se asumen varianzas iguales”.

**Tabla 8-4:** T de Student para el indicador Calidad de conexión.

Prueba de muestras independientes						
Prueba T de Student para la igualdad de medias						
t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	95% de intervalo de confianza de la diferencia	
					Inferior	Superior
-2,264	188	0,025	-2,947	1,302	-5,516	-0,379
-2,264	184,545	0,025	-2,947	1,302	-5,516	-0,379

Realizado por: Edgar Ulloa.. 2020

En razón a la tabla 8-4 se toma el valor obtenido, siendo este de 0.025 y que de acuerdo al criterio antes mencionado se puede decir que:

$$P\text{-valor} = 0.025 \leq \alpha = 0.05$$

Entonces se observa que P-valor es menor que alfa, por lo tanto, se rechaza  $H_0$  y se da paso a  $H_1$ : Existe una diferencia significativa entre la media de Calidad de conexión en el estándar 802.11N y la media de Calidad de conexión en el estándar 802.11AC.

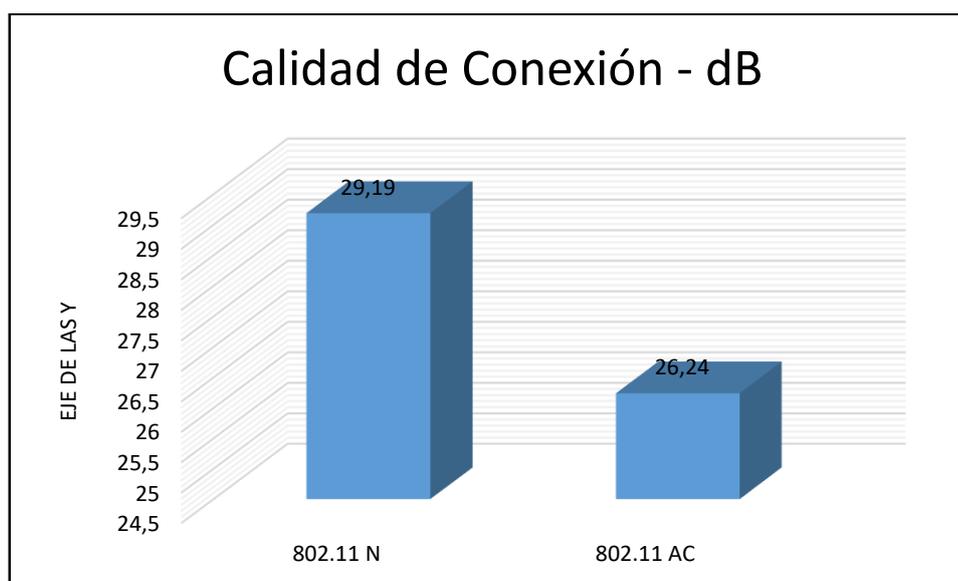
Seguidamente, en la Tabla 9-4. se puede ver los resultados de las medias de Calidad de conexión entre el estándar 802.11N y el estándar 802.11AC. Los cuales toman los siguientes valores: El estándar IEEE 802.11N presenta 29.19 dB y el estándar IEEE 802.11AC presenta 26.24 dB, sabiendo que la calidad de conexión depende del menor ruido propagado y que a su vez este se mide en dB, se establece que mientras el valor sea mayor a 6dB indica que tiene mejor Calidad de Conexión, así se tiene que el estándar IEEE 802.11N tiene mejor rendimiento en comparación con el estándar IEEE 802.11AC con respecto a la Calidad de Conexión en redes con alta concurrencia de usuarios.

**Tabla 9-4:** Comparación de medias del indicador Calidad de conexión.

Estadísticas de grupo					
Estándares		N	Media	Desv. Desviación	Desv. Error promedio
Calidad de Conexión	802.11n	373	29,19	9,568	0,982
	802.11ac	373	26,24	8,337	0,855

Realizado por: Edgar Ulloa.. 2020

En el Gráfico 2-4. se observa los resultados de los dos estándares analizados, mostrando en su eje positivo los valores que se obtuvieron mediante la prueba T de Student en el indicador Calidad de conexión cuyos valores son 29,19 dB y 26,24 dB para los estándares 802.11N y 802.11AC respectivamente, por lo tanto, el estándar 802.11N presenta mejor rendimiento sobre el estándar 802.11AC en redes con alta concurrencia de usuarios.



**Gráfico 2-4:** Comparación de IEEE 802.11N y AC del indicador Calidad de conexión.

Realizado por: Edgar Ulloa.. 2020

#### 4.2.2.4. Decisión estadística.

Una vez concluidas las pruebas de T de Student para muestras independientes de la variable Calidad de conexión se establece la siguiente conclusión: Existe una diferencia significativa entre la media de Calidad de conexión en el estándar 802.11N y la media de Calidad de conexión en el estándar 802.11AC.

Es decir, el estándar IEEE 802.11N presenta 29,19 dB y en el estándar IEEE 802.11AC presenta 26,24 dB, sabiendo que la calidad de conexión depende del menor ruido propagado y que a su vez este se mide en dB, se establece que mientras el valor sea mayor a 6dB indica que tiene mejor Calidad de Conexión, así se tiene que el estándar IEEE 802.11N tiene mejor rendimiento en comparación con el estándar IEEE 802.11AC con respecto a la Calidad de Conexión en redes con alta concurrencia de usuarios.

#### **4.2.3. Prueba T de Student del indicador Throughput (Rendimiento).**

Al igual que los dos casos anteriores, la prueba de normalidad y la prueba de igualdad de varianzas son filtros que se deben pasar con el fin de obtener el cálculo del P-valor de la prueba T de Student para muestras independientes en la evaluación de la variable Throughput.

Lo primero que se hará es redactar la hipótesis estadística, es decir la hipótesis alterna y la hipótesis nula de la siguiente manera:

**H<sub>1</sub>** = Existe una diferencia significativa entre la media de throughput en el estándar 802.11N y la media de throughput en el estándar 802.11AC.

**H<sub>0</sub>** = No existe una diferencia significativa entre la media de throughput en el estándar 802.11N y la media de throughput en el estándar 802.11AC.

##### *4.2.3.1. Normalidad en el indicador Throughput.*

En la prueba de normalidad se debe corroborar que la variable aleatoria en ambos casos 802.11N y 802.11AC se distribuye normalmente, para esto se usa la prueba de Kolmogorov-Smirnov ya que el tamaño de la muestra es mayor a 30 individuos. El criterio para determinar si la variable aleatoria se distribuye normalmente es:

P-valor  $\Rightarrow \alpha$  Aceptar **H<sub>0</sub>** = Los datos provienen de una distribución normal.

P-valor  $< \alpha$  Aceptar **H<sub>1</sub>** = Los datos No provienen de una distribución normal.

Mediante el software estadístico de IBM SPSS se realizan los respectivos cálculos para la normalidad, una vez que se ingresó los datos, arroja los siguientes resultados como se puede ver en la Tabla 10-4:

**Tabla 10-4:** Normalidad del indicador Throughput (Rendimiento).

Pruebas de normalidad							
Estándares		Kolmogorov-Smirnov			Shapiro-Wilk		
		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Throughput	802.11n	0,262	373	0,200	0,891	373	0,360
	802.11ac	0,157	373	0,200	0,875	373	0,246

Realizado por: Edgar Ulloa.. 2020

En este indicador se observa el nivel de significancia evaluada por Kolmogorov-Smirnov ya que los datos ingresados son mayores a 30, estos datos son tomados de la Tabla 10-4 con el fin de ser comparados con el valor de alfa como se muestra a continuación:

$$P\text{-valor de } 802.11N = 0.200 > \alpha = 0.05$$

$$P\text{-valor de } 802.11AC = 0.200 > \alpha = 0.05$$

Entonces se observa que P-valor es mayor que el valor alfa en los dos casos, por lo tanto, se Acepta la  $H_0$ , lo que quiere decir que estos datos provienen de una distribución normal al demostrar que el Throughput en los dos mecanismos de conexión se comporta normalmente y puede dar paso al siguiente filtro para la prueba T de Student.

#### 4.2.3.2. Igualdad de varianzas en el indicador Throughput.

Al igual que en la normalidad la igualdad de varianzas es otro filtro que se debe pasar con el fin de obtener el cálculo del P-valor y así pasar a la prueba T de Student para muestras independientes en la evaluación de la variable Throughput. Entonces si las varianzas son iguales cumple con este filtro y se procede al análisis de la hipótesis. Para la igualdad de varianzas se usa las siguientes consideraciones:

P-valor  $\Rightarrow \alpha$  Aceptar  $H_0$  = Las varianzas son iguales.

P-valor  $< \alpha$  Aceptar  $H_1$  = Existe diferencia significativa en las varianzas.

**Tabla 11-4:** Igual de varianzas del indicador Throughput (Rendimiento).

Prueba de muestras independientes	
Prueba de Levene de igualdad de varianzas	
F	Sig.

Throughput	Se asumen varianzas iguales	3,831	0,066
	No se asumen varianzas iguales		

Realizado por: Edgar Ulloa.. 2020

La igualdad de varianzas se valida mediante la prueba de Levene, en esta prueba se obtuvo los siguientes datos tal como muestra la Tabla 11-4.

$$P\text{-valor} = 0.066 > \alpha = 0.05$$

Entonces se observa que P-valor es mayor que alfa por lo que se acepta  $H_0$  y por lo tanto se asume que las varianzas son iguales. De esta forma se corrobora que se cumple los dos supuestos tanto el de normalidad como el de igualdad varianza para poder seguir con el P-valor de la prueba T de Student para muestras independientes.

#### 4.2.3.3. Resultados prueba T de Student.

Luego que se corrobora la normalidad y la igualdad de varianzas, ya se puede obtener el P-valor para la prueba T de Student, mediante la siguiente consideración:

Si la probabilidad obtenida en **P-valor**  $\leq \alpha$ , **rechace  $H_0$**  (Se Acepta  **$H_1$** )

Si la probabilidad obtenida en **P-valor**  $> \alpha$ , **no rechace  $H_0$**  (Se Acepta  **$H_0$** )

Recordando el apartado 4.2.3. Prueba T de Student para la variable Throughput (rendimiento) se obtiene lo siguiente:

**$H_1$**  = Existe una diferencia significativa entre la media de throughput en el estándar 802.11N y la media de throughput en el estándar 802.11AC.

$$H_1: \mu_a \neq \mu_b$$

**$H_0$**  = No existe una diferencia significativa entre la media de throughput en el estándar 802.11N y la media de throughput en el estándar 802.11AC.

$$H_0: \mu_a = \mu_b$$

En el software de IBM SPSS se obtienen los resultados de la variable Throughput (rendimiento) de la prueba de T de Student, la Tabla 12-4 muestra el valor de significancia bilateral, el mismo que se toma o se selecciona en base al parámetro “Se asumen varianzas iguales” según la Tabla 11-4 Prueba de Levene de igualdad de varianzas.

**Tabla 12-4:** T de Student del indicador Throughput (Rendimiento).

<b>Prueba de muestras independientes</b>						
Prueba T de Student para la igualdad de medias						
t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	95% de intervalo de confianza de la diferencia	
					Inferior	Superior
-1,395	18	0,023	-1656,667	1187,711	-4151,956	838,623
-1,053	4,890	0,017	-1656,667	1573,720	-5729,474	2416,140

Realizado por: Edgar Ulloa.. 2020

En razón a la Tabla 12-4 se toma el valor obtenido, siendo este de 0.023 y que de acuerdo a las consideraciones antes mencionadas se puede decir que:

$$P\text{-valor} = 0.023 \leq \alpha = 0.05$$

Entonces se observa que P-valor es menor que alfa, por lo tanto, se rechaza  $H_0$  y se da paso a  $H_1$ : Existe una diferencia significativa entre la media de throughput en el estándar 802.11N y la media de throughput en el estándar 802.11AC.

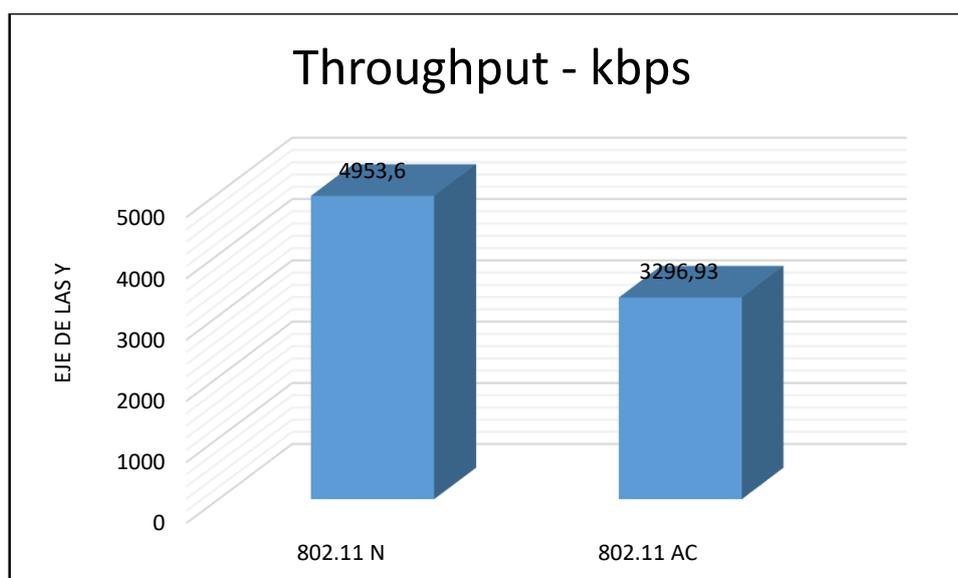
Luego, en la Tabla 13-4. se puede ver los resultados de las medias del indicador Throughput entre el estándar 802.11N y el estándar 802.11AC. Los cuales toman los siguientes valores: El estándar IEEE 802.11N presenta 4953,60 kbps y el estándar IEEE 802.11AC presenta 3296,93 kbps, sabiendo que el Throughput (Rendimiento) generalmente se mide en bps y es la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación, se establece que mientras más alto sea este valor, indica que tiene mejor tasa de transferencia, así se tiene que el estándar IEEE 802.11N tiene mejor rendimiento en comparación con el estándar IEEE 802.11AC con respecto al Throughput en redes con alta concurrencia de usuarios.

**Tabla 13-4:** Comparación de medias para el indicador Throughput (Rendimiento).

Estadísticas de grupo					
Estándares		N	Media	Desv. Desviación	Desv. Error promedio
Throughput	802.11n	373	3296,93	1899,187	490,368
	802.11ac	373	4953,60	3343,752	1495,371

Realizado por: Edgar Ulloa.. 2020

En el Gráfico 3-4. se observa los resultados de los dos estándares analizados, mostrando en su eje positivo los valores que se obtuvieron mediante la prueba T de Student en el indicador Throughput cuyos valores son 4953,60 kbps y 3296,93 kbps para los estándares 802.11N y 802.11AC respectivamente, por lo tanto, el estándar 802.11N presenta mejor velocidad, rendimiento y por ende mayor efectividad de paquetes entregados con éxito al receptor.



**Gráfico 3-4:** Comparación de IEEE 802.11N y AC del indicador Throughput.

Realizado por: Edgar Ulloa.. 2020

#### 4.2.3.4. Decisión estadística.

Concluidas las pruebas de T de Student para muestras independientes de la variable Throughput (rendimiento) se establece la siguiente conclusión: Existe una diferencia significativa entre la media de valores de throughput en el estándar 802.11N y la media de valores de throughput en el estándar 802.11AC.

Es decir, el estándar IEEE 802.11N presenta 3296,93 kbps y el estándar IEEE 802.11AC presenta 4953,60 kbps, sabiendo que el Throughput (Rendimiento) generalmente se mide en bps y es la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación, se establece que mientras más alto sea este valor, indica que tiene mejor tasa de transferencia, así se tiene que el estándar IEEE 802.11AC es mejor en comparación con el estándar IEEE 802.11N con respecto al Throughput.

Las variables analizadas intensidad de señal, calidad de conexión y throughput de acuerdo a los resultados obtenidos indica que las pruebas estadísticas de estos indicadores se inclinan a favor del Estándar IEEE 802.11AC obtenido ventajas sobre el otro estándar analizado.

#### **4.2.4. Resumen de indicadores evaluados.**

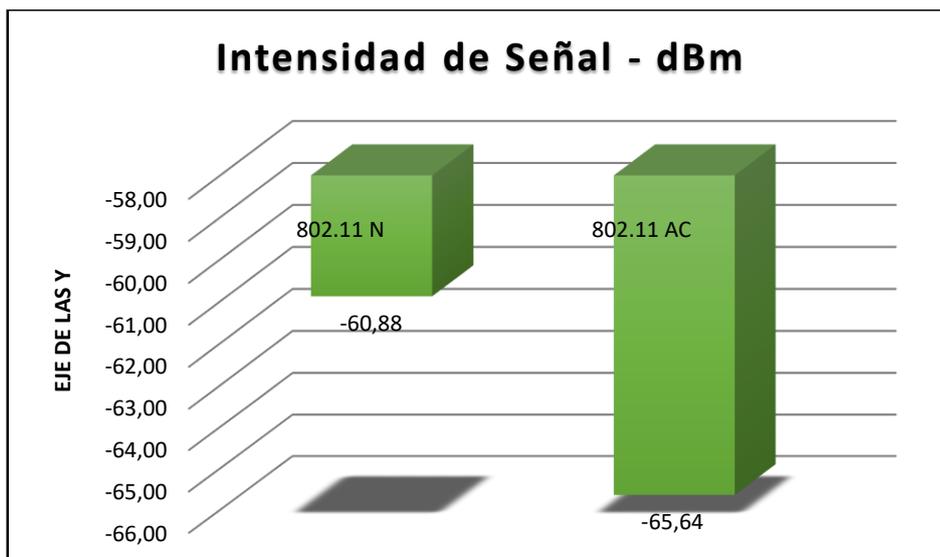
A continuación, en la Tabla 14-4 se presenta los resultados generales obtenidos de la Prueba T de Student para muestras independientes de los tres indicadores evaluados lo cual demuestra que el estándar 802.11 AC provee mejor rendimiento en la red inalámbrica.

**Tabla 14-4:** Indicadores de los Estándares 802.11N y AC con T de Student.

<b>INDICADOR</b>	<b>IEEE 802.11N</b>	<b>IEEE 802.11AC</b>
Intensidad de Señal	-60.88 dBm	-65.54 dBm
Calidad de Conexión	29.19 dB	26.24 dB
Throughput (Rendimiento)	4953.60 kbps	3296.93 kbps

**Realizado por:** Edgar Ulloa.. 2020

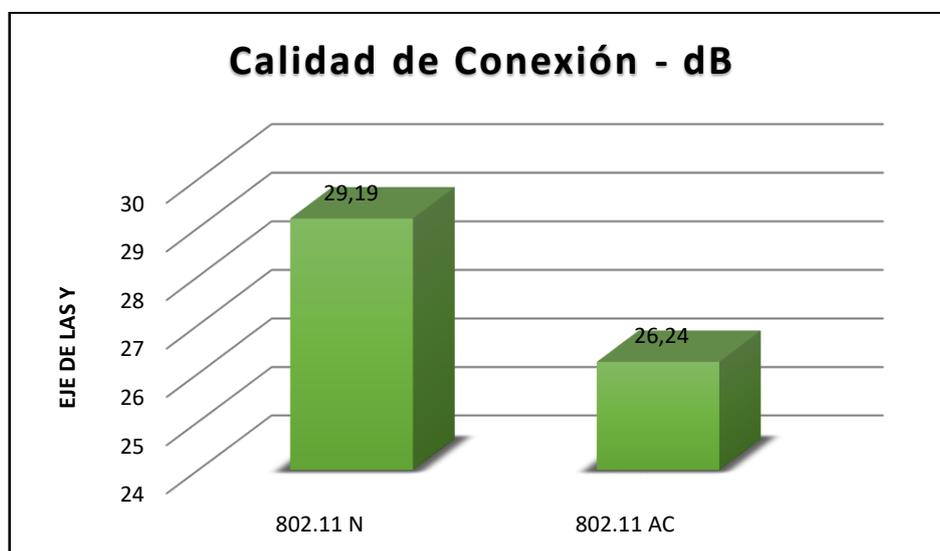
La Intensidad de señal se mide en dBm e indica que un valor mientras más cercano este al cero representa un mejor rendimiento, por la tanto en la prueba estadística se obtuvo una diferencia significativa de -60.88 dBm para el estándar 802.11N sobre -65.54 dBm para el estándar 802.11AC. Lo que indica que el mecanismo de conectividad 802.11N posee mejor rendimiento con respecto a la intensidad de señal que el estándar 802.11AC, tal cual se muestra en el siguiente Gráfico 4-4:



**Gráfico 4-4:** Resultados de IEEE 802.11N y AC del indicador Intensidad de Señal.

Realizado por: Edgar Ulloa.. 2020

La Calidad de Conexión de acuerdo a la medición basada en el ruido presenta que el estándar 802.11N posee 26.24 dB y el estándar 802.11AC posee 29.29 dB. Lo que indica que el mecanismo de conectividad 802.11AC presenta mejor rendimiento con respecto al indicador Calidad de conexión sobre el estándar 802.11N, tal cual se muestra en el Gráfico 5-4.

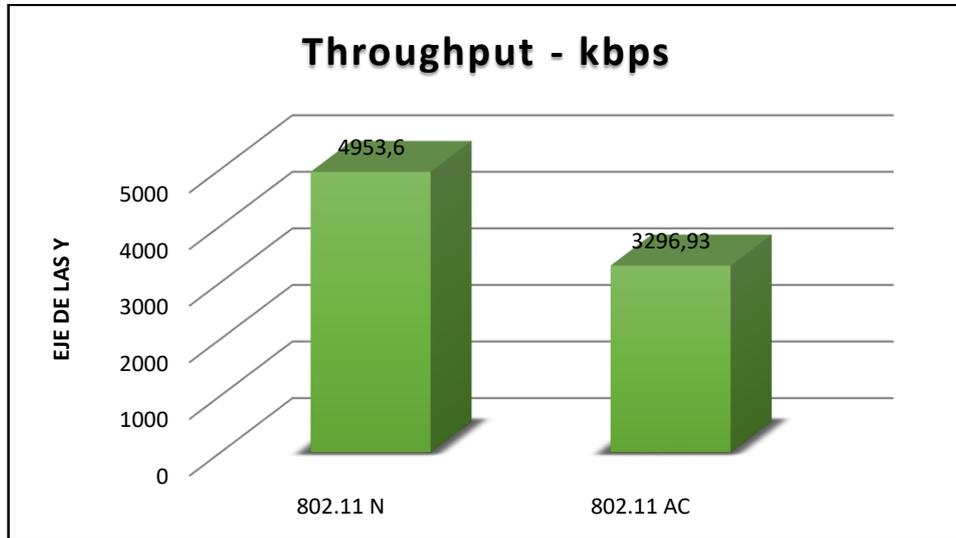


**Gráfico 5-4:** Resultados de IEEE 802.11N y AC del indicador Calidad de Conexión.

Realizado por: Edgar Ulloa.. 2020

El Throughput muestra el éxito de paquetes entregados y debe ser menor al ancho de banda. Así se obtuvo mediante la prueba estadística T de Student que posee 3296.93 kbps para el estándar 802.11N y 49.53.60 kbps para el estándar 802.11AC. Lo que indica que el mecanismo de

conectividad 802.11AC presenta mejor rendimiento con respecto al indicador Throughput que el estándar 802.11N, tal cual se muestra en el Gráfico 6-4.



**Gráfico 6-4:** Resultados de IEEE 802.11N y AC del indicador Throughput.

Realizado por: Edgar Ulloa.. 2020

## **CAPÍTULO V**

### **5. GUÍA DE ESPECIFICACIONES TÉCNICAS DE LOS AP.**

Como antecedente se puede indicar que los datos obtenidos en los escenarios de pruebas mediante las simulaciones con datos reales en Cisco 8500 Series Wireless Controller arrojan valores de 50% a favor del estándar 802.11N y 40% a favor del estándar 802.11AC. Lo cual se ratifica en las pruebas de simulaciones con datos reales mediante Cisco Prime Infrastructure que arrojan valores similares, siendo del 57.14% a favor del estándar 802.11N y 28.57% a favor del estándar 802.11AC. Recalcando que estos valores se inclinan por el estándar 802.11N debido a que los dispositivos finales al carecer de la disponibilidad de varios estándares (802.11 a, ac) en su tarjetería de red optan por conectarse con mayor afluencia a este estándar, por lo tanto, obtiene mejor rendimiento en los parámetros evaluados en estas simulaciones.

Además, la mayoría de conexiones a los AP provienen de teléfonos móviles tal cual se muestra en la Figura 1-5 que señala que las conexiones se realizan mediante el sistema operativo Android los mismos que son parte fundamental en los teléfonos móviles.

	Name	Clients
1	Android	2844
2	Android-Samsung-Galaxy-Phone	969
3	Microsoft-Workstation	418
4	Samsung-Device	260
5	Apple-Device	233
6	Android-LG	99
7	Workstation	97
8	Intel-Device	74
9	Windows8-Workstation	67
10	Apple-iPhone	47

**Figura 1-5:** Top de sistemas operativos activos en la red inalámbrica.

**Fuente:** Herramienta Cisco 8500 Series Wireless Controller.

Así también se muestran en las Figuras 2-5 y 3-5 con respecto a los teléfonos móviles las especificaciones técnicas de conectividad, indicando que los móviles de gama alta poseen los estándares 802.11 a/b/g/n/ac 2.4GHz+5GHz y los dispositivos de gama media/baja poseen los estándares 802.11 b/g/n 2.4GHz, y tratándose de una institución pública es entendible pensar que no todos los usuarios pueden tener acceso a un teléfono móvil de gama alta por su costoso valor económico que bordea los \$500, lo cual justifica que las conexiones en redes con alta concurrencia de usuarios estén más orientas hacia el estándar 802.11N.

Galaxy S7 edge		
VENTAJAS	ESPECIFICACIONES	RESEÑAS
<b>Conectividad</b>		
ANT+	Version USB	Localización
Sí	USB 2.0	GPS, Glonass, Beidou
Auriculares	MHL	Wi-Fi
3.5mm Stereo	No	802.11 a/b/g/n/ac 2.4G+5GHz, VHT80 MU-MIMO

**Figura 2-5:** Estándar Wifi móvil gama alta.

**Fuente:** Samsung.com.

Galaxy J8 (Dual-SIM)				
BENEFICIOS	SPECS	RESEÑAS	SOPORTE	COMPARAR
<b>Conectividad</b>				
<b>ANT+</b>	Si	<b>USB Interface</b>	Micro USB	<b>Versión USB</b> USB 2.0
<b>Localización</b>	GPS, Glonass, Beidou	<b>Auriculares</b>	3.5mm Stereo	<b>MHL</b> No
<b>Wi-Fi</b>	802.11 b/g/n 2.4GHz	<b>Wi-Fi Direct</b>	Si	<b>Versión Bluetooth</b> Bluetooth v4.2

**Figura 3-5:** Estándar Wifi móvil gama media.

**Fuente:** Samsung.com.

Ahora bien, en las pruebas estadísticas de los indicadores evaluados intensidad de señal, calidad de conexión y throughput obtienen una diferencia significativa a favor del estándar 802.11N que dan paso a proponer una guía de implementación de requerimientos técnicos acerca del mecanismo de conectividad de mayor rendimiento de acuerdo a la concurrencia de usuarios.

La propuesta trata en sí de realizar un análisis exhaustivo de los Access Point con los que se pueda plasmar mejoras en el rendimiento de estos dispositivos, utilizando el mecanismo de conexión de mayor realce, este a su vez está orientado a proponer características de adquisición que eviten altos consumos económicos, características de configuración con los que los administradores de red puedan guiarse para obtener mejor rendimiento, características de habilitación por software que son necesarias para poner en funcionamiento bandas duales de 2,4GHz + 5GHz, características de verificación por comandos que son necesarias para validar que ciertos parámetros estén habilitados, características de ubicación física de los Access Point para evitar interferencias con otros equipos que deterioren la señal y así mismo una distancia óptima de separación entre Access Point para evitar la degradación de la señal.

A continuación, se presenta la guía de especificaciones técnicas de los Access Point para mejorar el rendimiento de estos con la utilización del mecanismo de conectividad de mayor realce en las simulaciones y pruebas estadísticas:

ACCESS POINT

GUÍA DE

ESPECIFICACIONES

TÉCNICAS PARA

MEJORAR EL

RENDIMIENTO

## **GUÍA DE ESPECIFICACIONES TÉCNICAS DE LOS AP.**

### **5.1. INTRODUCCIÓN.**

Un Access Point cumple una tarea de suma importancia dentro de las redes inalámbricas ya que es el dispositivo encargado de interconectar terminales de comunicación inalámbrica, si bien es cierto en la actualidad se tiene gran variedad de Access Point de acuerdo a una gran variedad de modelos, marcas, características y precios.

De acuerdo a la investigación realizada de los mejores mecanismos de conectividad donde se obtiene mediante datos estadísticos que el estándar IEEE 802.11n brinda mejor rendimiento en redes con alta concurrencia de usuarios, se emite esta guía que proyecta suministrar especificaciones concretas que deben tener los Access Point al momento de ser instalados en una red inalámbrica, todo esto con el fin de tener un conocimiento avanzado del estándar en mención que proporcione un rendimiento óptimo dentro de una red inalámbrica.

### **5.2. ALCANCE.**

El presente documento abarca la guía necesaria para llegar al usuario Normal o Administrador de una red inalámbrica, el cual pueda tener el conocimiento necesario a la hora de instalar o implementar una red ya sea en casa o en una red de gran tamaño respectivamente. Es así que con esta guía se pretende encaminar al usuario, cuando este requiera implementar una red inalámbrica y le permita hacerlo de manera fácil tomando en cuenta los aspectos detallados en este manual.

### 5.3. TIPOS DE USUARIOS.

**Usuario Administrador:** Es el usuario que en la mayoría de casos poseen niveles académicos superiores, así como también conocimientos altos en telecomunicaciones y que están encargados de administrar y solventar problemas de redes con gran concurrencia de usuarios o que manejan redes de nivel corporativo.

**Usuario Normal:** Es el usuario que en la mayoría de casos no posee niveles académicos superiores y posee poco o nada de conocimiento de redes de telecomunicaciones, son usuarios que desean implementar o aumentar el tamaño de su red inalámbrica en casas o negocios pequeños.

### 5.4. GLOSARIO DE TÉRMINOS.

**Telecomunicaciones:** Sistema de comunicación a distancia que se realiza por medios eléctricos o electromagnéticos.

**Red Inalámbrica:** Permite el acceso a servicios y/o internet a usuarios con dispositivos móviles sin la necesidad de cables.

**Access Point:** Abreviado con las siglas AP, dispositivo de red que interconecta equipos de comunicación inalámbricos.

**Banda de Frecuencia:** Son intervalos de frecuencias del espectro electromagnético asignados a diferentes usos dentro de las radiocomunicaciones. En redes posee dos frecuencias 2.4GHz y 5GHz.

**Estándar 802.11:** Sirve y es considerado la base en la comunicación de las redes inalámbricas.

### 5.5. Identificar el lugar de instalación.

Como primer paso para mejorar el rendimiento de una red inalámbrica se debe conocer el espacio o lugar en donde se pretende realizar la instalación de la red, es decir:

- ✓ Espacios cerrados y/o cubiertos como casas, oficinas, departamentos, edificios.
- ✓ Espacios al aire libre como parques, canchas, estadios, entre otros.



**Figura 4-5:** Espacio abierto – Parque de la Ciudadela Universitaria UCE.

**Fuente:** Dirección de Comunicación y Cultura (UCE).



**Figura 5-5:** Espacio cerrado o cubierto – Edificio Facultad de Administración.

**Fuente:** Dirección de Comunicación y Cultura (UCE).

### **5.5.1. Usuario Administrador.**

Por lo general cuando se trata de un administrador de redes con gran concurrencia de usuarios se está hablando de redes inalámbricas de gran envergadura por lo tanto los espacios o lugares definidos para la instalación tienden a ser de gran tamaño, tanto en ambientes cubiertos como en ambientes al aire libre, estos lugares pueden ser edificios, aulas académicas, pisos administrativos y parques, canchas respectivamente.

Mediante este análisis se puede establecer que es necesario dispositivos Access Point de especificaciones y rendimiento alto para poder satisfacer las necesidades de los posibles clientes que se conectarán a la red inalámbrica ya que se sobreentiende que existiría gran concurrencia de usuarios al tratarse de un lugar amplio.

### **5.5.2. Usuario Normal.**

Cuando se habla de un usuario normal que desea una implementación de una red inalámbrica se puede pensar que se trata de una instalación mínima como en una casa, negocio pequeño como un cyber o un departamento de vivienda de espacio físico moderado.

El análisis que interviene en este caso permite establecer que se necesita dispositivos Access Point con especificaciones, costos y rendimiento medio para poder satisfacer las necesidades de los posibles clientes que se conectarán a la red inalámbrica ya que en este caso no sería numerosa la concurrencia de usuarios.

## **5.6. Identificar a que usuarios está orientado el servicio.**

Tomando como base la identificación del lugar de instalación de la red inalámbrica se puede deducir el número de clientes y por ende el número de conexiones que se enlazarán a la red. Además, en los dos casos de usuarios se puede obtener el número de usuarios posibles mediante los datos de las actividades de las empresas, es decir, cuando se trata de redes con gran concurrencia de usuarios y así mismo cuando se trata de redes pequeñas de casas o negocios, además se puede optar por el recurso de la observación de los posibles clientes y por ende las posibles conexiones.

Ligado a las conexiones están los usuarios y sus dispositivos, estos influyen directamente en el número de conexiones debido a los estándares que poseen. En las siguientes Figuras 6-5 y 7-5 se puede observar que los teléfonos móviles de gama alta poseen los estándares 802.11 a/b/g/n/ac 2.4GHz+5GHz y los dispositivos de gama media/baja poseen los estándares 802.11 b/g/n 2.4GHz.

Lo que indica que en redes con alta concurrencia de usuarios necesariamente se deben ubicar Access Point de especificaciones y rendimiento robusto porque las conexiones son altas a todos los estándares y en especial al 802.11n y 802.11ac que son los más actuales y más utilizados.

The screenshot shows the connectivity specifications for the Galaxy S7 edge. The page has a navigation bar with 'VENTAJAS', 'ESPECIFICACIONES', 'RESEÑAS', 'SOPORTE', and 'COMPARAR'. The 'RESEÑAS' tab is selected. The main heading is 'Conectividad'. The specifications are as follows:

ANT+	Versión USB	Localización
Si	USB 2.0	GPS, Glonass, Beidou
Auriculares	MHL	Wi-Fi
3.5mm Stereo	No	802.11 a/b/g/n/ac 2.4G+5GHz, VHT80 MU-MIMO

**Figura 6-5:** Estándares Wifi móvil gama alta.

Fuente: Samsung.com.

The screenshot shows the connectivity specifications for the Galaxy J8 (Dual-SIM). The page has a navigation bar with 'BENEFICIOS', 'SPECS', 'RESEÑAS', 'SOPORTE', and 'COMPARAR'. The 'COMPARAR' tab is selected. The main heading is 'Conectividad'. The specifications are as follows:

ANT+	USB Interface	Versión USB
Si	Micro USB	USB 2.0
Localización	Auriculares	MHL
GPS, Glonass, Beidou	3.5mm Stereo	No
Wi-Fi	Wi-Fi Direct	Versión Bluetooth
802.11 b/g/n 2.4GHz	Si	Bluetooth v4.2

**Figura 7-5:** Estándares Wifi móvil gama media.

Fuente: Samsung.com.

### 5.6.1. Usuario Administrador.

Los Administradores de redes con espacios amplios de cubrir inalámbricamente se sobreentiende que tendrán alta concurrencia de usuarios por lo tanto tienen que identificar los clientes quienes se conectarán a la red inalámbrica, por lo general en instituciones públicas que brindan servicios a clientes masivos poseen en su mayoría dispositivos finales de gama media/baja y en menor cantidad dispositivos de gama alta. Por lo que se tendrá que cubrir estos dos aspectos con Access Point que tengan una alta capacidad de estándares y rendimiento, es decir:

- ✓ De acuerdo a la gran cantidad de conexiones se recomienda la adquisición de AP con estándares 802.11 a/b/g/n/ac 2.4GHz+5GHz, todo esto pensado en la gran cantidad de usuarios/conexiones que optarán por conectarse a cualquiera de los estándares que provee el AP y en especial a los más actuales y de mayor uso.

#### **5.6.2. Usuario Normal.**

Los usuarios normales que desean implementar una red inalámbrica en sus casas o negocios pequeños podrán hacerlo con la identificación de sus clientes o personas cercanas que se conectarán a la red inalámbrica. Es decir:

- ✓ Los usuarios dependiendo de sus dispositivos intentarán conectarse a los estándares 802.11 a/b/g/n/ac 2.4GHz+5GHz, pero no es necesario la adquisición de un Access Point robusto ya que por lo general los dispositivos que se conectan son pocos y de gama media/baja, lo que significaría que con un AP con estándares 802.11 b/g/n 2.4GHz se cubriría la necesidad de dicha red.

#### **5.7. Requerimientos económicos de instalación.**

Cuando se habla del presupuesto de instalación de Access Point no solamente se trata de ver costos mínimos para las redes inalámbricas sino de ver dispositivos robustos en sus características de hardware y software y como segundo punto ver que no generen tantos gastos económicos en la implementación, administración y posteriormente en el soporte que se tenga que proveer a los mismos.

Luego de los análisis anteriores es necesario saber los costos que influyen en la instalación de la red inalámbrica, de esta forma se pueden abaratar costos ya que en lugares pequeños y

para pocas conexiones no es necesario adquirir Access Point de especificaciones, marcas y rendimiento robusto.

### 5.7.1. *Usuario Administrador.*

Al momento de la selección de un Access Point primeramente se debería escoger APs que cuenten en sus especificaciones técnicas con los todos estándares como IEEE 802.11 a/b/g/n/ac 2.4GHz+5GHz tal cual recomienda esta investigación gracias a los resultados estadísticos proporcionados en el capítulo tres.

En cuestión de costos, influye en gran magnitud poseer todos los estándares y por ende la utilidad de las antenas ya que de estas depende la transmisión de datos en bandas de frecuencia 2.4GHz y 5GHz. Para ellos se evalúa modelos de Access Point antiguos y actuales.



**Figura 8-5:** Access Point modelo antiguo con antenas en 2.4GHz.

**Realizado por:** Edgar Ulloa.

En el caso de Access Point antiguos como se muestra en la Figura 8-5 se puede notar el uso de antenas para el funcionamiento de las bandas de frecuencia de 2.4GHz y 5GHz. En las instituciones con gran concurrencia de usuarios existen AP con antenas que proporcionan la señal de forma omnidireccional y sectorial.

- ✓ Omnidireccional es un tipo de antena la cual emite su señal en forma de 360°, o radia su señal de potencia de forma uniforme en todas las direcciones.
- ✓ Sectorial es un tipo de antena la misma que emite su señal de forma directa, además posee mayor alcance horizontal, ciertos fabricantes cubren radios desde 30° a 120°.

Como ejemplo en la Figura 9-5 se observa un Access Point antiguo utilizado en la red inalámbrica de la Universidad Central del Ecuador, el mismo que solo conservaba antenas compatibles en los slots de banda de frecuencia de 2.4GHz dejando inutilizable la banda de frecuencia de 5GHz en la cual funciona el estándar IEEE 802.11AC, lo que quiere decir que este AP siempre estuvo trabajando bajo los estándares IEEE 802.11 b, g y n. No obstante, con esta observación se podría recuperar dicho AP simplemente con la adquisición de las antenas y obviamente viendo que soporte el estándar más actual 802.11AC.



**Figura 9-5:** Slots de antenas con radios para 2.4GHz y 5GHz.

Realizado por: Edgar Ulloa.

Para el caso de Access Point actuales los fabricantes han optado por hacer que los dispositivos vengan incluidos con antenas externas e internas y de la misma forma según este criterio serían evaluados los costos de estos dispositivos inalámbricos. Siendo los de mayor precio y robustez los Access Point con antenas externas.

A continuación, en la Figura 10-5 se presenta un gráfico de los Access Point con antenas internas y externas utilizados en la Universidad Central del Ecuador siendo su costo

aproximado de \$300 dólares para AP con antenas internas y de \$450 dólares para AP con antenas externas, costos evaluados en el año 2019.



**Figura 10-5:** Access Point con antenas externas e internas.

Realizado por: Edgar Ulloa.

En virtud de todo lo comentado con respecto a los costos es importante aclarar que la utilización de los Access Point se puede dar tanto en APs antiguos como nuevos siempre y cuando en sus características técnicas soporte varios estándares y de preferencia los más actuales y utilizados.

### **5.7.2. Usuario Normal.**

Al momento de la selección de un Access Point inicialmente se debería escoger un AP que cuenten en sus especificaciones técnicas con los estándares IEEE 802.11 a/b/g/n/ac 2.4GHz+5GHz, pero por tratarse de una instalación con poca concurrencia de usuarios y en un lugar pequeño, lo más recomendable sería adquirir un AP con especificaciones básicas de estándares como el IEEE 802.11 b/g/n/ ya que con este dispositivo se podrá cubrir las necesidades inalámbricas de los posibles usuarios.

En cuestión de costos se podría abaratar los mismos mediante la adquisición de Routers con funcionamiento a manera de AP. En el mercado existe un sin número de marcas y modelos de estos dispositivos, sus costos varían de la misma forma por su marca, modelo, estándares, alcance y velocidad de transmisión, es decir, los precios rondan ente los \$20 dólares a \$50 dólares, costos evaluados en el 2019.

En la siguiente Figura 11-5 se muestra routers Cisco utilizados en Ecuador por el proveedor de internet Netlife los mismos que funcionan a manera de AP y que poseen características básicas mencionadas en esta guía para la utilización de las redes inalámbricas en lugares pequeños y con poca concurrencia de usuarios. Se muestra esos dispositivos con el fin de indicar que estos routers a manera de AP funcionan correctamente para las necesidades de redes inalámbricas pequeñas y con pocos usuarios.



**Figura 11-5:** Routers Cisco a manera de Access Point para lugares pequeños.

**Fuente:** <https://www.linksys.com>

Así también se tiene en la Figura 12-5 Routers Tp-Link utilizados en Ecuador por el proveedor de internet Tv Cable los mismos que funcionan a manera de AP y que poseen características básicas mencionadas en esta guía para la utilización de las redes inalámbricas en lugares pequeños y con poca concurrencia de usuarios. Se muestra esos dispositivos con el fin de indicar que por cuestiones de costos y calidad estas grandes empresas usan estos routers a manera de AP ya que funcionan correctamente para las necesidades de redes inalámbricas pequeñas y con pocos usuarios.



**Figura 12-5:** Routers TP-Link a manera de Access Point para lugares pequeños.

Fuente: <https://www.tp-link.com/>

### 5.8. Requerimientos técnicos de los Access Point.

Un Access Point cumple una tarea de suma importancia dentro de las redes inalámbricas ya que es el dispositivo encargado de interconectar terminales de comunicación inalámbrica, si bien es cierto en la actualidad se tiene gran variedad de Access Point de acuerdo a modelos, marcas, características y precios. En la Figura 13-5 se observa ciertos modelos de Access Point con un punto importante a considerar, la utilización de las antenas ya que bajo este parámetro trabajan las bandas de frecuencia de 2.4Ghz y 5GHz y por ende de esta manera se define el estándar en el que funciona cada Access Point.



### **Figura 13-5:** Tipos de Access Point.

Realizado por: Edgar Ulloa.

#### **5.8.1. Usuario Administrador.**

Los administradores de redes de lugares grandes y con alta concurrencia de usuarios deben seleccionar Access Point robustos de acuerdo a los requerimientos de redes amplias como:

- ✓ Disponibilidad de Estándares IEEE 802.11 a/b/g/n/ac 2.4GHz+5GHz.
- ✓ Énfasis en los estándares más actuales y utilizados IEEE 802.11 n y ac 2.4GHz+5GHz respectivamente.
- ✓ Poseer protocolos altos de seguridad – 802.1x.
- ✓ Access Point con antenas internas y externas dependiendo del lugar de instalación.

#### **5.8.2. Usuario Normal.**

Los usuarios normales en sus redes inalámbricas para lugares pequeños y con poca concurrencia de usuarios deben seleccionar Access Point de gama media o baja ya que no es necesario costos ni características técnicas altas, más bien su adquisición es de acuerdo a los requerimientos del lugar de instalación y los posibles usuarios de la red.

En la mayoría de los casos y dependiendo del proveedor de internet se suele usar para redes de hogar o negocios pequeños Routers a manera de Puntos de Acceso, los mismos que dentro de sus especificaciones técnicas poseen idénticos parámetros de configuración que los AP. Las especificaciones básicas que deberían poseer estos dispositivos son:

- ✓ Disponibilidad básica de Estándares IEEE 802.11 b/g/n 2.4GHz.
- ✓ Énfasis en los estándares más actuales y utilizados dependiendo de la disponibilidad del AP adquirido IEEE 802.11n 2.4GHz.
- ✓ Se puede utilizar para redes pequeñas Routers a maneras de Access Point por optimizar costos.
- ✓ Poseer protocolos de seguridad medios como WPA o WPA2-PSK.

En las siguientes Figuras 14-5 y 15-5 se puede observar las especificaciones técnicas de estos routers a manera de AP para redes pequeñas en donde consta los estándares IEEE 802.11 b/g/n 2.4GHz.

Router inalámbrico N300 Linksys E900	
ESPECIFICACIONES TÉCNICAS	
<b>Nombre de modelo:</b> Linksys E900	<b>Temperatura de almacenaje:</b> De -20 a 70 °C
<b>Estándares de red:</b> <ul style="list-style-type: none"> <li>o IEEE 802.11b</li> <li>o IEEE 802.11a</li> <li>o IEEE 802.11g</li> <li>o IEEE 802.11n</li> <li>o IEEE 802.3</li> <li>o IEEE 802.3u</li> </ul>	<b>Humedad de funcionamiento:</b> 10 a 80 % sin condensación
<b>Bandas de radiofrecuencia:</b> 2,4 GHz	<b>Tasa de enlace máxima:</b> 300 Mbps
<b>Puertos:</b> 1 10/100 WAN, 4 10/100 LAN	<b>Compatibilidad con plataforma:</b> <ul style="list-style-type: none"> <li>o Windows XP</li> <li>o Windows Vista 32/64</li> <li>o Windows 7 32/64</li> <li>o Windows 8 32/64</li> <li>o Windows 8,1 32/64</li> <li>o Mac OS X 10.5.8 Leopard</li> <li>o Mac OS X 10.6.1 Snow Leopard</li> <li>o Mac OS X 10.7 Lion</li> <li>o Mac OS X 10.8 Mountain Lion</li> <li>o Mac OS X 10.9 Mavericks</li> </ul>
<b>Luces LED:</b> Electricidad, WLAN, Ethernet 1-4, Internet	
<b>Botones:</b> 1 botón de Reset (Reinicio)	
<b>Temperatura de funcionamiento:</b> Entre 0 y 40°C	

**Figura 14-5:** Especificaciones de Router Cisco a manera de AP.

Fuente: <https://www.linksys.com>

tp-link	
Routers Inalámbricos   TL-WR840N	
<a href="#">Visión General</a> <a href="#">Especificaciones</a> <a href="#">Soporte</a>	
<b>CARACTERÍSTICAS DE HARDWARE</b>	
Interface	4 10/100Mbps LAN PORTS 1 10/100Mbps WAN PORT
Botón	WPS/RESET Button
Fuente de Alimentación Externa	9VDC / 0.6A
Estándares Inalámbricos	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Dimensiones (W X D X H)	7.2 x 5.0 x 1.4in.(182 x 128 x 35 mm)
Antena	2 Antennas

**Figura 15-5:** Especificaciones de Router TP-LINK a manera de AP.

Fuente: <https://www.tp-link.com/>

## **5.9. Determinar ubicación física de los Access Point.**

La ubicación de un Access Point es vital para tener una buena cobertura y conectividad. Cualquiera que tenga una conexión de Internet ya sea en casa, negocio o sobre todo en áreas grandes de oficina, sabe que la ubicación del Access Point es de suma importancia para tener una buena señal en todos los ambientes.

Mucho influye la estructura de edificación al optar que no haya muchos muros que se interponga con la señal, como también el Access Point mismo que puede enfrentarse a interferencias entre sí por la utilización del mismo canal de señal y por supuesto la calidad del servicio que brinda el proveedor de Internet.

### **5.9.1. Usuario Administrador.**

En las de redes con alta concurrencia de usuarios los administradores pueden ayudarse de las herramientas de software que contienen mapas de calor y mapas de interferencias, todo esto viene incluidos en la adquisición de los Access Point y hacen que sea más fácil la ubicación física de estos dispositivos.

Como referencias también se puede mencionar lo siguiente:

- ✓ Ubica el Access Point en un lugar central en el ambiente a cubrir.
- ✓ Dependiendo el ambiente cubierto el Access Point se debe ubicar con una distancia mayor a 15 metros con respecto a otros dispositivos similares.
- ✓ Evita obstrucciones en el recorrido de la señal.
- ✓ Evita ubicar el Access Point cerca de los baños (Cerámica = agua, sílice, plomo, estaño y óxidos metálicos).
- ✓ Evitar ubicar el AP cerca de interferencias electromagnéticas como:
  - Otros Access Point.
  - Electrodomésticos Microondas.
  - Host spot.
  - Teléfonos fijos inalámbricos.
  - Antenas de Televisión Satelital.

Para reducir interferencias se recomienda evitar los siguientes obstáculos:

- ✓ Madera, materiales sintéticos y el cristal. (Pérdida de intensidad de señal baja).
- ✓ Agua, ladrillo y mármol. (Pérdida de intensidad de señal media).
- ✓ Escayola, hormigón y cristal blindado. (Pérdida de intensidad de señal alta).
- ✓ Metal. (Pérdida de intensidad de señal súper alta).

Adicionalmente, se recomienda evitar la utilización del mismo canal de señal, ya que en los Access Point de gama alta en su configuración pueden optar por configurar estos canales de manera automática haciendo que las señales no se solapen entre sí.

### **5.9.2. Usuario Normal.**

En las de redes pequeñas los usuarios pueden ayudarse con las indicaciones que se presentan a continuación.

- ✓ Ubica el Access Point o router en un lugar central en el ambiente a cubrir.
- ✓ Dependiendo el ambiente cubierto el Access Point se debe ubicar con una distancia mayor a 15 metros con respecto a otros dispositivos similares.
- ✓ Evita obstrucciones en el recorrido de la señal.
- ✓ Evita ubicar el Access Point en la cocina o en el baño. (Cerámica = agua, sílice, plomo, estaño y óxidos metálicos).
- ✓ Evitar ubicar el AP cerca de interferencias electromagnéticas como:
  - Otros Access Point.
  - Electrodomésticos Microondas.
  - Host spot.
  - Teléfonos fijos inalámbricos.
  - Antenas de Televisión Satelital.
- ✓ De ser posible sintoniza la antena.
- ✓ Si es necesario amplifica la señal.

Para reducir interferencias se recomienda evitar los siguientes obstáculos:

- ✓ Madera, materiales sintéticos y el cristal. (Pérdida de intensidad de señal baja).
- ✓ Agua, ladrillo y mármol. (Pérdida de intensidad de señal media).
- ✓ Escayola, hormigón y cristal blindado. (Pérdida de intensidad de señal alta).
- ✓ Metal. (Pérdida de intensidad de señal súper alta).

Adicionalmente, se recomienda evitar la utilización del mismo canal de señal, ya que en los Access Point de gama media/baja o routers a manera de AP en sus estándares 802.11 b/g/n de 2.4GHz poseen 12 canales de señal de transmisión por lo cual se sugiere trabajar en distintos canales a los ya utilizados en la red propia o vecina.

## **5.10. Determinar protocolos de seguridad de los Access Point.**

Para que la red inalámbrica tenga un rendimiento óptimo es necesario asegurar la conexión inalámbrica donde la demanda de usuarios sea alta o baja, es decir, debe tener robustez en este aspecto, por lo cual lo más recomendable es usar protocolos de seguridad, mediante los cuales se puede tener niveles altos que aseguren las redes inalámbricas.

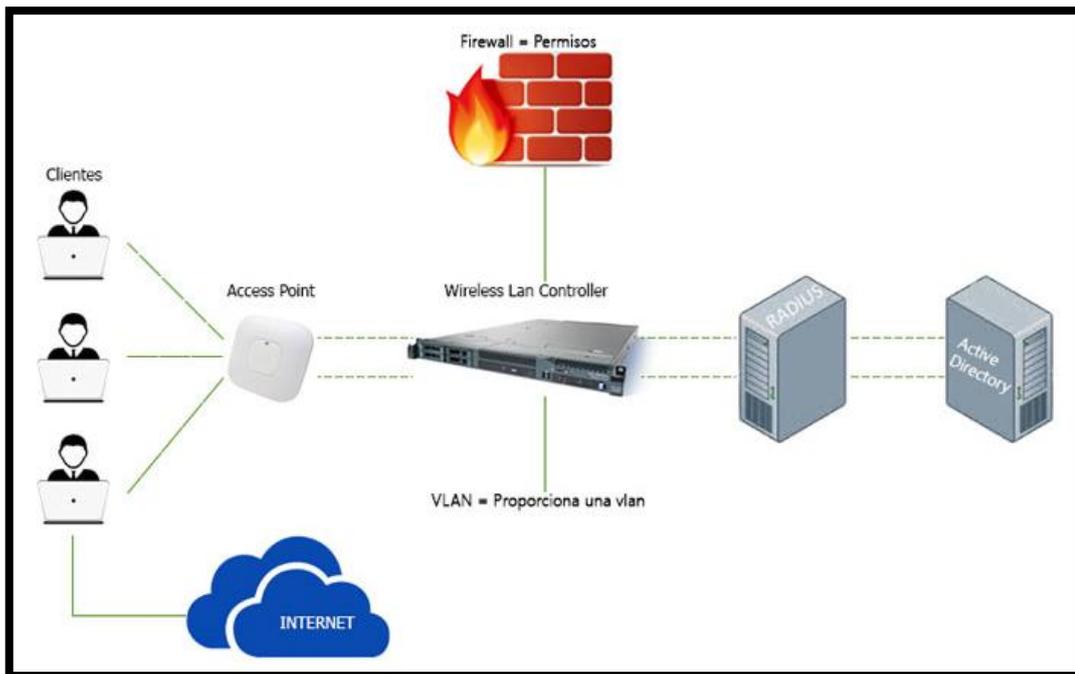
### **5.10.1. Usuario Administrador.**

En redes con lugares amplios y de gran concurrencia de usuarios es recomendable usar un protocolo de alta seguridad, así como el **802.1x** que se deriva de IEEE y que mediante el mismo se puede tener niveles altos de seguridad en las redes cableadas e inalámbricas.

La funcionalidad de este protocolo dentro de una institución con alta concurrencia de usuarios sería de la siguiente manera:

Los clientes solicitan autenticación a los Access Point, estos a través de la Wireless LAN Controller envían requerimiento al Servidor Radius y este a su vez solicita la Información de credenciales activas en el Servidor de Directorio Activo. Luego de realizar las peticiones, las repuestas son devueltas a través de los mismos medios hasta llegar a la controladora donde esta otorga acceso a una VLAN mediante la Capa de Distribución y así mismo otorga permisos mediante el firewall y finalmente brinda al cliente el servicio de internet.

Como ejemplo en la Figura 16-5 se puede observar el proceso y funcionalidad de un protocolo de seguridad alta implementado en la Universidad Central del Ecuador.



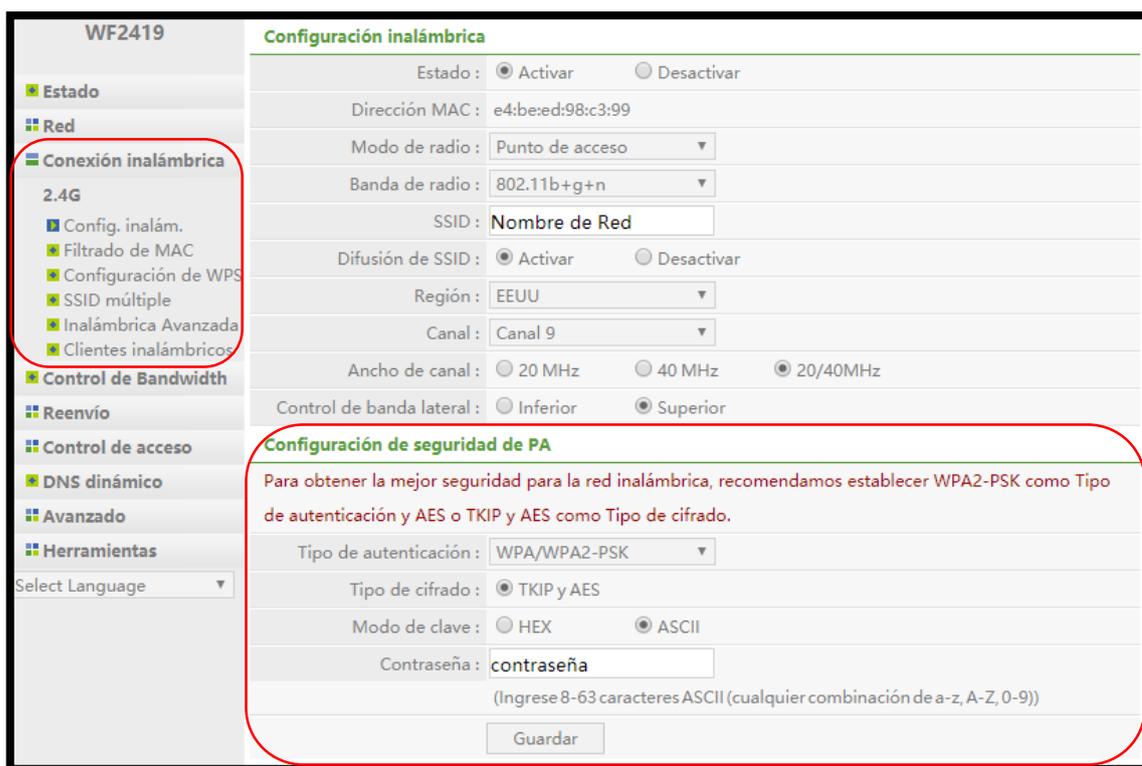
**Figura 16-5:** Protocolo 802.1x implementado en la UCE.

Realizado por: Edgar Ulloa.

### 5.10.2. Usuario Normal.

Para los usuarios normales al momento de configurar la seguridad en sus Access Point o routers a manera de AP lo pueden hacer de manera sencilla ingresando a la configuración del dispositivo. Todo Access Point y en especial los routers a manera de AP vienen con un software de administración y es mediante este aspecto que se puede realizar configuraciones en este dispositivo, de la siguiente manera:

- ✓ Conectarse al AP de forma inalámbrica o alámbrica.
- ✓ Para acceder a las configuraciones, mediante un navegador digitar la siguiente IP de acuerdo a la marca del AP **192.168.1.1** o **192.168.0.1**.
- ✓ Buscar y presionar sobre el modulo o botón que diga “Conexión Inalámbrica”.
- ✓ Configurar los siguientes aspectos:
  - SSID = Nombre que se le dará a la red inalámbrica.
  - Modo Radio = Seleccionar modo Punto de Acceso (Access Point).
  - Tipo de Autenticación o Modo de seguridad = Seleccionar WPA/WPA2-PSK
  - Frase de paso o Contraseña = De acuerdo al tipo de seguridad (WPA/WPA2-PSK) se habilita el campo para colocar una contraseña no menor a 8 caracteres entre mayúsculas y minúsculas.



**Figura 17-5:** Protocolo 802.1x implementado en la UCE.

Realizado por: Edgar Ulloa.

## 5.11. Características de configuración por software.

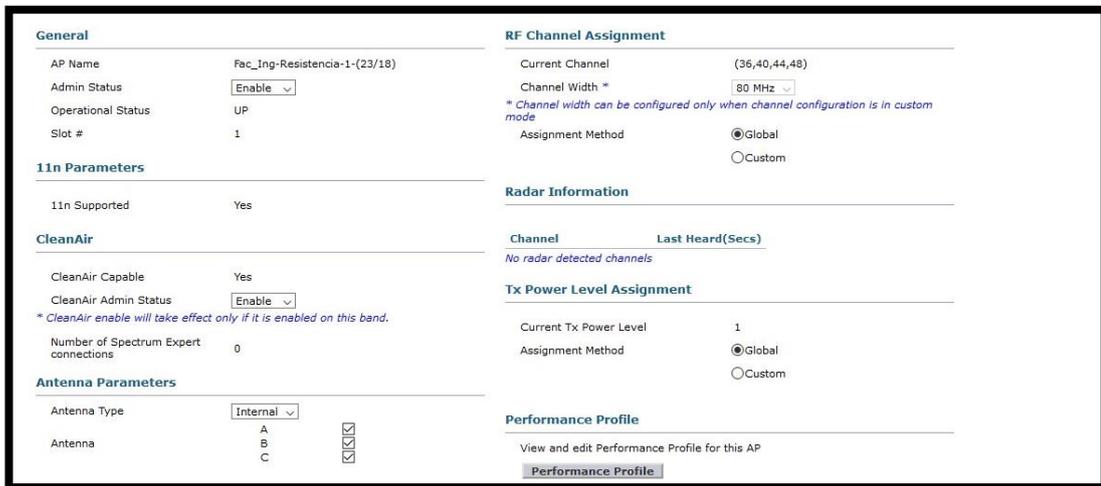
Una vez adquiridos y/o seleccionados los Access Point de trabajo que serán utilizados con el mecanismo de conectividad sugerido en esta investigación según los resultados estadísticos en redes con alta concurrencia de usuarios, se propone una revisión técnica de manera general con el fin de asegurar que estos dispositivos ejecuten sus tareas de forma normal y que se encuentren activos dentro de la red inalámbrica.

Mediante software se puede ingresar a ver el estado de los radios (banda de frecuencia de 2.4GHz y 5GHz) ver el tipo de antena instalado (interna o externa) y otros parámetros de importancia que validen el funcionamiento correcto del AP en los radios y estándares sugeridos.

### 5.11.1. Usuario Administrador.

Un usuario administrador gracias a las herramientas de software que viene incluidas en la adquisición de los Access Point puede determinar y validar por estos medios la utilización de los estándares y radios de frecuencias con el objetivo de tener optimizada su red inalámbrica.

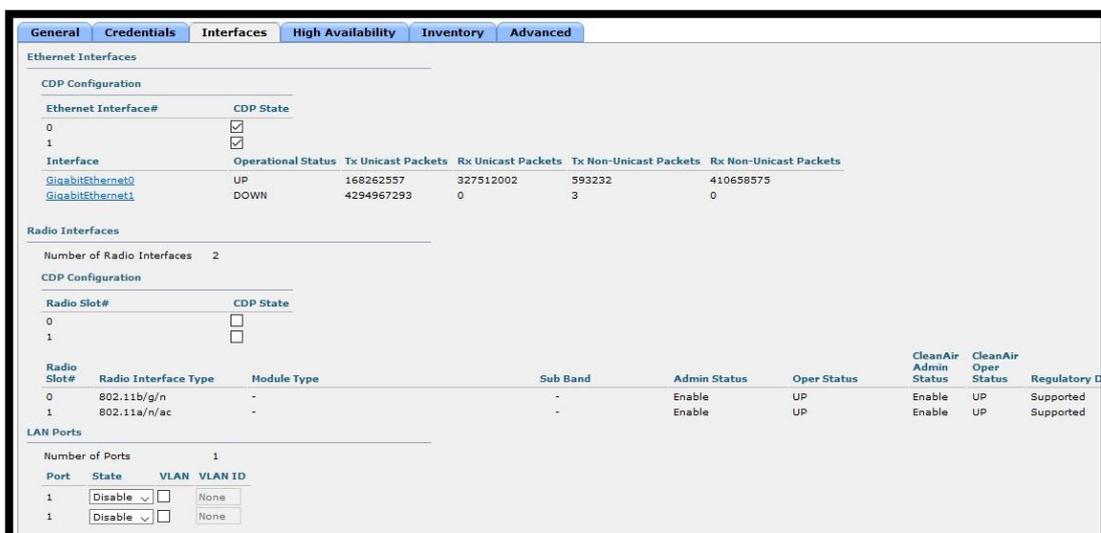
En la Figura 18-5 muestra en un primer plano la tenencia de slots de antenas para verificar cuantas se encuentran instaladas en la banda de frecuencia que se desea trabajar 5GHz.



**Figura 18-5:** Interfaz de antenas habilitadas.

Realizado por: Edgar Ulloa.

En la siguiente Figura 19-5 se presenta los slots disponibles (Radio 0 = 2.4GHz y Radio 1 = 5GHz) los mismos que pueden ser activados y desactivados mediante este software.

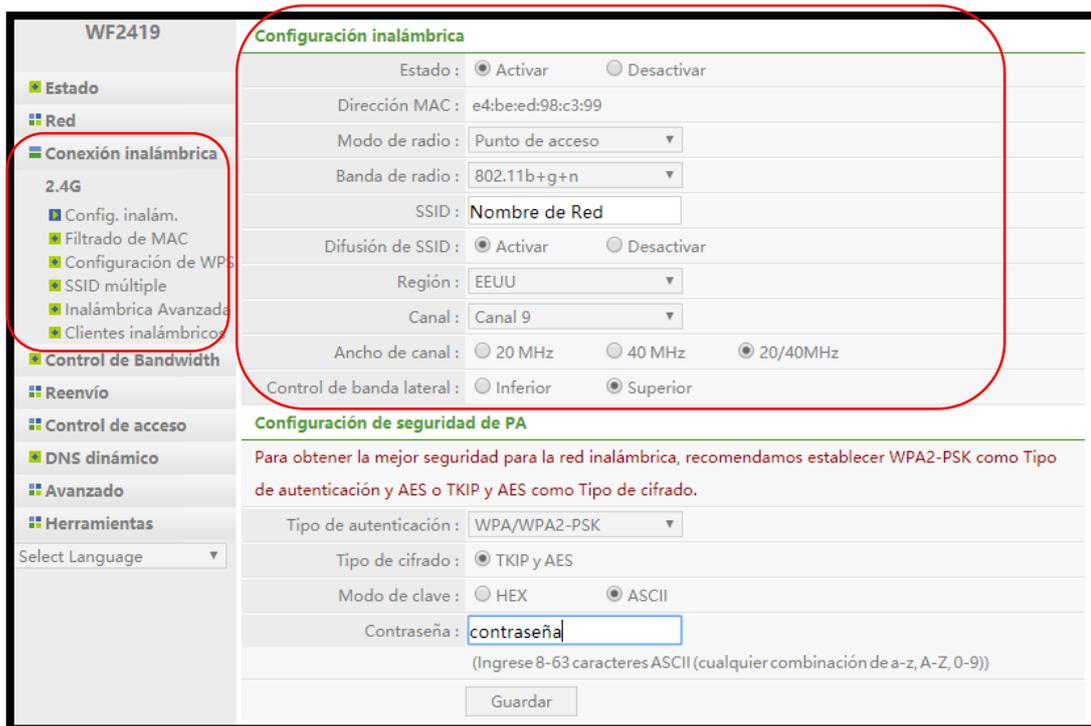


**Figura 19-5:** Interfaz de radios habilitados.

### 5.11.2. *Usuario Normal.*

Para los usuarios normales al momento de configurar sus Access Point o routers a manera de AP lo pueden hacer de manera sencilla ingresando a la configuración del dispositivo. Todo Access Point y en especial los routers a manera de AP vienen con un software de administración y es mediante este aspecto que se puede realizar configuraciones en este dispositivo, de la siguiente manera:

- ✓ Conectarse al AP de forma inalámbrica o alámbrica.
- ✓ Para acceder a las configuraciones, mediante un navegador digitar la siguiente IP de acuerdo a la marca del AP **192.168.1.1** o **192.168.0.1**.
- ✓ Buscar y presionar sobre el modulo o botón que diga “Conexión Inalámbrica”.
- ✓ Configurar los siguientes aspectos:
  - SSID = Nombre que se le dará a la red inalámbrica.
  - Modo Radio = Seleccionar modo Punto de Acceso (Access Point).
  - Banda de Radio = De preferencia seleccionar el estándar más actual y de mayor uso.
  - Difusión SSID = Activar para visualizar la red desde cualquier dispositivo cliente.
  - Ancho de canal = De preferencia mixto o automático de entre 20 ó 40 MHz.
  - Canal Inalámbrico = SI se tiene más de un AP cercano propio o vecino validar que no se encuentre en el mismo canal para evitar interferencias.



**Figura 20-5:** Configuración AP usuario normal.

Realizado por: Edgar Ulloa.

## 5.12. Características de configuración por consola.

Las configuraciones de software se pueden establecer como se mencionó anteriormente, no obstante, también existen configuración por consola, debido a que en ciertos casos se presentan problemas de la carga de interfaz gráfica ya sea por conexiones inestables o perdidas de acceso (claves) lo que causa demoras en la ejecución y validación de estos parámetros. Para esto se presenta la activación y desactivación de los radios (Radio 0 = 2.4GHz y Radio 1 = 5GHz) mediante consola.

### 5.12.1. Usuario Administrador.

El usuario administrador tiene la opción de ingresar mediante consola a la administración del Access Point, para configurar y validar que los radios en donde trabajan los estándares IEEE 802.11 a/b/g/n/ac en las bandas de frecuencia 2.4GHz y 5GHz estén activas y funcionando correctamente. Así como se ve a continuación en la Figura 21-5.

```

!
!
lldp run
bridge irb
!
!
interface Dot11Radio0
 no ip route-cache
 antenna gain 4
 ampdu transmit priority 1
 ampdu transmit priority 2
 ampdu transmit priority 3
 mbssid
 speed 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m1
4. m15.
 power local 12
 power client local
 packet retries 64 drop-packet
 station-role root
!
interface Dot11Radio1
 no ip route-cache
 antenna gain 7
 peakdetect
 ampdu transmit priority 1
 ampdu transmit priority 2
 ampdu transmit priority 3
 mbssid
 speed basic-12.0 18.0 basic-24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m14. m
15.
 power client local
 packet retries 64 drop-packet
 station-role root
!
interface GigabitEthernet0
 no ip route-cache
 duplex auto

```

**Figura 21-5:** Consola de comandos para levantar/bajar Interfaz de Radios.

**Realizado por:** Edgar Ulloa.

Consulta de radios disponibles:

router(config)# **show running-config**

Selección de radio:

router(config)# **interface radio <slot/puerto>**

Levantamiento de radio:

router(config)# **no shutdown**

Baja o apagado de radio:

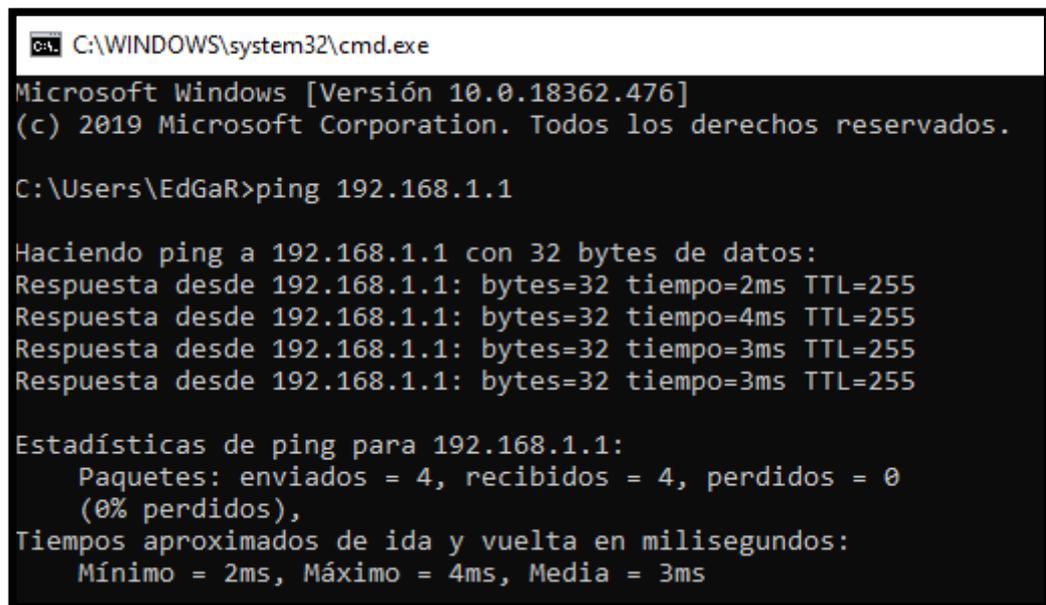
router(config)# **shutdown**

### 5.12.2. Usuario Normal.

El usuario normal tiene la opción de ingresar mediante consola de Windows para validar que el Access Point o router a manera de AP este configurado, activo y funcionando correctamente dentro de la red. Esto se ejecuta mediante un ping el cual indica que el dispositivo está activo, los pasos a seguir serían los siguientes:

- ✓ En el sistema operativo Windows presionar la tecla Windows + r.
- ✓ Se abre una ventana donde se debe ingresar el texto “cmd” y presionar aceptar.
- ✓ En la venta siguiente teclear “ping 192.168.1.1” este número de IP es de acuerdo al apartado **7.2 Usuario normal** de esta guía.
- ✓ Luego de eso se ejecutará en 4 líneas la respuesta de que el AP está activo o no en la red.

Así como se ve a continuación en la Figura 22-5.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.18362.476]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\EdGaR>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=255
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=255
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=255
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=255

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 4ms, Media = 3ms
```

**Figura 22-5:** Consola de comandos para levantar/bajar Interfaz de Radios.

Realizado por: Edgar Ulloa.

## CONCLUSIONES.

- Las simulaciones realizadas a los dos mejores mecanismos de conectividad 802.11N y 802.11AC en las herramientas de software Cisco Prime Infrastructure y Cisco 8500 Series Wireless Controller ayudaron a establecer información relevante, obtener resultados acerca del rendimiento de Access Point y a analizar el comportamiento cuando existe gran concurrencia de usuarios, mediante la comparación de sus datos.
- En la Universidad Central del Ecuador se encuentran implementados los estándares de conexión IEEE 802.11 a, b, g, n y ac. De los cuales se eligieron los de mayor relevancia en la actualidad y de mayor demanda en esta Institución Educativa de acuerdo a los datos obtenidos en Cisco Prime Infrastructure. Los elegidos son los estándares 802.11N y 802.11AC, los que mediante su comparación estadística dieron como resultado la inclinación por el estándar 802.11N, indicando mejoras significativas en las variables evaluadas frente al otro estándar analizado.
- Luego de analizar y comparar los mecanismos de conectividad mediante el método estadístico T de Student con Kolmogorov-Smirnov en el software SPSS, se establece que el estándar IEEE 802.11N es la opción idónea a ser aplicada en redes con alta concurrencia de usuarios, debido a los resultados obtenidos como son la intensidad de señal con -60.88 dBm, calidad de conexión con 29.19 dB y throughput con 4953.60 kbps que son mejores sobre el estándar IEEE 802.11AC.
- Se evidencia también que en las simulaciones la tendencia de conexión a estos estándares se inclina por el IEEE 802.11N debido a que los dispositivos finales no cuentan en su tarjetería con la disponibilidad de todos los estándares IEEE 802.11 a, b, g, n y ac, haciendo que el rendimiento tome tendencia sobre este estándar.
- Los resultados estadísticos de la comparación de los dos mecanismos de conectividad permiten o dan paso a establecer como propuesta una guía de especificaciones,

implementaciones y características técnicas de los Access Point con relación al análisis de estos dispositivos para mejorar el rendimiento en base a ciertos aspectos.

## RECOMENDACIONES.

- Es recomendable usar datos cercanos a la realidad para saber el funcionamiento en vivo de los Access Point mediante esta forma se puede ir analizando de manera más óptima los indicadores en los cuales se basa la investigación y con los que se pueda obtener mejores resultados.
- Los equipos Access Point deben ser considerados y analizados previamente con respecto a la ubicación y características físicas, características técnicas y costos, con el fin de obtener una proyección general de estos, y proponer su utilización tanto de los Access Point antiguos como actuales siempre y cuando dispongan de bandas duales para la utilización de varios estándares.
- Se debe conocer a profundidad los parámetros evaluados en la investigación, porque cada parámetro se concatena con un valor medible con el fin de obtener resultados, así se tiene el ejemplo para la medición de la calidad de conexión donde interviene el valor medible del ruido el mismo que se mide dB e indica que tan buena es una señal de conexión evaluando el poco o mucho valor que emita el ruido.
- Previo a la evaluación del rendimiento de los Access Point se debe analizar la ubicación física de los Access Point de tal manera que estos se ubiquen en una parte céntrica al área de cobertura, todo esto con el fin de emitir mejores resultados con respecto a la variable de intensidad de señal.
- Se recomienda realizar una verificación periódica de los Access Point, validando si las interfaces de Radio están trabajando con normalidad ya que bajo estos criterios se pone en funcionamiento las bandas de frecuencia de 2,4GHz + 5GHz en la que trabajan todos los estándares.

- Se recomienda tomar en cuenta que los dispositivos finales tienen a conectarse en mayor cantidad al estándar IEEE 802.11N debido a las características de la tarjetería inalámbrica que poseen estos dispositivos, además recalcar que por este motivo esto influye en el rendimiento de los Access Point.

## BIBLIOGRAFÍA.

- Anónimo, (2017). Significado de Itinerancia. Recuperado de: <https://www.significados.com/itinerancia/>.
- Anónimo, (2017). Métodos de la Investigación. Metodologia02.blogspot.com. Recuperado de: <http://metodologia02.blogspot.com/p/metodos-de-la-investigacion.html>.
- Arcotel, (2017). Boletín Estadístico del sector de Telecomunicaciones. Recuperado de: <http://www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf>.
- Betancourt S, (2016). Análisis y Diseño de una Solución de Red Isp Wimax Basada en IEEE 802.16 m-2011. Recuperado de: <http://www.dspace.uce.edu.ec/bitstream/25000/6868/1/T-UCE-0011-274.pdf>
- Cheerful, M. (2017). Métodos (página 2) - Monografias.com. Recuperado de: <http://www.monografias.com/trabajos11/metods/metods2.shtml>.
- Cortés Cortés, M., & Iglesias León, M. (2004). Retrieved 30 July 2019, from [http://www.unacar.mx/contenido/gaceta/ediciones/metodologia\\_investigacion.pdf](http://www.unacar.mx/contenido/gaceta/ediciones/metodologia_investigacion.pdf)
- Cidecam, M. (2019). 1.3.5 Definición de Red de Comunicaciones y su Importancia. Recuperado de: [http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/135\\_definicion\\_de\\_red\\_de\\_comunicaciones\\_y\\_su\\_importancia.html](http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/135_definicion_de_red_de_comunicaciones_y_su_importancia.html)
- Diario La Hora, (2017). Ecuatorianos se conectan a celulares por Wifi. Recuperado de: [http://lahora.com.ec/index.php/noticias/show/1101928645/-1/Ecuatorianos\\_se\\_conectan\\_a\\_celulares\\_por\\_WiFi.html#.WPUiOj4X3IU](http://lahora.com.ec/index.php/noticias/show/1101928645/-1/Ecuatorianos_se_conectan_a_celulares_por_WiFi.html#.WPUiOj4X3IU).
- De Luz S. (2011). Máximas conexiones simultáneas que soporta un router neutro: Manual para averiguarlo. Recuperado de: <https://www.redeszone.net/2011/05/06/maximas-conexiones-simultaneas-que-soporta-un-router-neutro-manual-para-averiguarlo/>

- Ducourthial, B., Mottelet, S., & Busson, A. Improving fairness between close Wi-Fi access points. *Journal of Network and Computer Applications*. de: <http://dx.doi.org/10.1016/j.jnca.2017.03.001>
- El Universo, (2017). ¿Te están robando wifi? Pasos para confirmar, encontrar al ladrón y proteger la red. Recuperado de: <http://www.eluniverso.com/vida-estilo/2015/05/11/nota/4864186/te-estan-robando-wifi-pasos-confirmar-encontrar-ladron-proteger>.
- FM, Y. (2019). WiFi 2.4GHz y 5GHz: cuáles son las diferencias y cuál elegir. Retrieved from <https://www.xataka.com/basics/wifi-2-4g-y-5g-cuales-son-las-diferencias-y-cual-elegir>
- Gordon W., (2015). Como mejorar Wifi. Recurado de: <https://es.gizmodo.com/las-10-mejores-maneras-de-mejorar-la-velocidad-y-el-alc-1727913687>.
- García, P. (2011). Topologías de las redes inalámbricas. Recuperado de: <http://plgarcia.blogspot.com/2011/06/definicion.html>.
- González, C. (2018). ¿20, 40 u 80 MHz? Configura el ancho de banda de tu Router Wifi correctamente. Recuperado 7 agosto 2019, de <https://www.adslzone.net/2018/05/18/ancho-banda-canal-wifi-20-40-80-mhz/>
- Gerometta, O. (2012). Medición de performance de enlaces. Retrieved 7 August 2019, from <http://librosnetworking.blogspot.com/2012/02/medicion-de-performance-de-enlaces.html>
- Garai, J. (2019). Entendiendo la relación señal ruido y la atenuación. Retrieved from <http://www.nireleku.com/2013/01/entendiendo-la-relacion-senal-ruido-y-la-atenuacion/>
- González, C. (2019). Cómo evitar que tu WiFi pierda velocidad y señal. Retrieved from

Histinf.blogs.upv.es. (2017). Historia de las Redes Inalámbricas – Historia de la Informática. Recuperado de: <http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/>.

Hora, D. (2017). Ecuatorianos se conectan a celulares por Wifi - La Hora. La Hora Noticias de Ecuador, sus provincias y el mundo. Recuperado de: <https://lahora.com.ec/noticia/1101928645/ecuatorianos-se-conectan-a-celulares-por-wifi>.

Herrera Ramírez, E., Díaz Ramírez, A., & Calafate, C. (2019). Desarrollando el estándar IEEE 802.11n, un paso adelante en WLAN. Retrieved 31 July 2019, from [http://www.grc.upv.es/calafate/download/Cicomp07\\_Estandar80211n.pdf](http://www.grc.upv.es/calafate/download/Cicomp07_Estandar80211n.pdf)

Internet: ¿cómo resolver problemas de IP con su red Wifi? | Datacraft. (2019). Retrieved from <http://www.datacraft.com.ar/internet-problemas-ip/>

Intel. (2019). Descripción del 802.11 X y tipos EAP. Retrieved from <https://www.intel.la/content/www/xl/es/support/articles/000006999/network-and-ii-wireless-networking.html>

MX, W. (2019). El nuevo estándar inalámbrico 802.11ac. Recuperado 31 Julio 2019, de [https://www.wni.mx/index.php?option=com\\_content&view=article&id=75:80211ac&catid=31:general&Itemid=79](https://www.wni.mx/index.php?option=com_content&view=article&id=75:80211ac&catid=31:general&Itemid=79)

Modo Ad – Hoc. (2019). Recuperado de: <https://sobretodoredes.wordpress.com/redes-inalambricas/modos-de-operacion/modo-ad-hoc/>

Nieto, J. (2019). Cómo cambiar el canal de tu Wifi para ganar potencia y cobertura. Retrieved 12 September 2019, from <https://www.xatakandroid.com/tutoriales/como-cambiar-canal-tu-wifi-para-ganar-potencia-cobertura>

NetSpot. (2019). Cómo comprobar el valor RSSI. Retrieved from <https://www.netspotapp.com/es/what-is-rssi-level.html>

- NetSpot (2019). WEP, WPA, WPA2 y WPA3 y sus diferencias. Retrieved from <https://www.netspotapp.com/es/wifi-encryption-and-security.html>
- Ortiz, D. (2015). Análisis comparativo del desempeño del estándar IEEE 802.11ac respecto al IEEE 802.11 a través de simulación numérica apoyada por software. Retrieved 22 August 2019, from <https://dspace.ups.edu.ec/bitstream/123456789/10181/1/UPS%20-%20ST001829.pdf>
- Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Pacheco, C. F., & Reis, A. D. (2013). Performance Evaluation of Laboratory Wi-Fi IEEE 802.11a Wpa Point-to-multipoint Links. *Procedia Technology*, 9, 146-151. doi: <http://dx.doi.org/10.1016/j.protcy.2013.12.016>
- Pazmiño A, (2011). Aplicación de Hacking Ético para la Determinación de Vulnerabilidades de Acceso a Redes Inalámbricas Wifi. Recuperado de: <http://dspace.esPOCH.edu.ec/bitstream/123456789/1726/1/98T00005.pdf>
- Pérez Porto, J., & Merino, M. (2019). Definición de red de datos. Recuperado 7 August 2019, de <https://definicion.de/red-de-datos/>
- Pillou, J. (2019). Introducción a wifi (802.11 o Wifi). Retrieved from <https://es.ccm.net/contents/789-introduccion-a-wifi-802-11-o-wifi>
- Recalde, A. (2019). Recuperado de: [https://www.tlm.unavarra.es/~daniel/docencia/rba/rba06\\_07/trabajos/resumenes/gr01-RedesInalambricas.pdf](https://www.tlm.unavarra.es/~daniel/docencia/rba/rba06_07/trabajos/resumenes/gr01-RedesInalambricas.pdf)
- Ramírez, P. (2018). Comunicación y redes sociales. [online] EL PAÍS. Recuperado de: [https://elpais.com/elpais/2014/12/19/eps/1419013223\\_225275.html](https://elpais.com/elpais/2014/12/19/eps/1419013223_225275.html).
- Radio de cobertura Wifi. (2019). Recuperado de: <https://www.wifisafe.com/blog/radio-de-cobertura/>

- Rodríguez-Lozano, David, Gómez-Pulido, Juan A., Lanza-Gutiérrez, José M., Duran-Domínguez, Arturo, & Fernández-Díaz, Ramón A. Context-aware prediction of Access points demand in Wifi networks. *Computer Networks*. doi: <http://dx.doi.org/10.1016/j.comnet.2017.01.002>
- Sites.google.com. (2018). Problemas de las Redes Inalámbricas - Redes Inalámbricas. Recuperado de: <https://sites.google.com/site/ticredin/problemas-de-las-redes-inalambricas>.
- Schweitzer, David, Jafari-Marandi, Ruholla, & Medal, Hugh. (2017). Analyzing the robustness of an array of wireless access points to mobile jammers. *Computers & Industrial Engineering*, 107, 25-38. de: <http://dx.doi.org/10.1016/j.cie.2017.02.022>
- Santamaría, L. (2019). La debilidad de las redes WIFI. Recuperado de: <http://www.evolucion.es/2017/10/debilidad-redes-wifi>
- Seguridad, T. (2019). Redes inalámbricas amenazadas - Blog Seguridad. Recuperado de: <https://blogseguridad.tyco.es/consejos/consejos-de-seguridad-hogar/redes-inalambricas-amenazadas-riesgos/>
- [https://cincodias.elpais.com/cincodias/2016/01/19/lifestyle/1453215028\\_259438.html](https://cincodias.elpais.com/cincodias/2016/01/19/lifestyle/1453215028_259438.html)
- Sanz, J., Valero, C., & Gómez Bolaños, D. (2016). Tipos de contraseña y cifrado para red WiFi: WEP, WPA, WPA2, TKIP, AES. (2019). Retrieved from <https://www.testdevelocidad.es/wifi/wi-fi-diferentes-tipos-clave-debemos-elegir/>
- Suárez Gutiérrez, M. (2019). MECANISMOS DE SEGURIDAD EN REDES INALÁMBRICAS (1st ed., p. 10).

Sánchez Turcios, R. (2015). t-Student: Usos y abusos. Recuperado 7 noviembre 2019, de [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0188-21982015000100009](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-21982015000100009)

Topologías inalámbricas. (2019). Recuperado de: <https://es.slideshare.net/LarryRuiz/topologas-inalmbricas-gran-tarea-23961833>

Vallejo A, (2017). HISTORIA Y EVOLUCIÓN DE REDES INALÁMBRICAS. Recuperado de: <https://prezi.com/a9aghvc4mfb9/historia-y-evolucion-de-redes-inalambricas/>

Velocidad, T. (2019). Qué es la latencia, y cómo podemos mejorarla. Retrieved from <https://www.testdevelocidad.es/2016/08/18/la-latencia-podemos-mejorarla/>

Vásconez D. 2014, p. 110. Diseño de una red inalámbrica tipo malla (wnm) estándar 802.11 de transmisión y la optimización de cobertura en la unidad educativa mayor Ambato  
Recuperado de: [http://repo.uta.edu.ec/bitstream/123456789/6989/1/Tesis\\_t873mrt.pdf](http://repo.uta.edu.ec/bitstream/123456789/6989/1/Tesis_t873mrt.pdf).

Voip, f. (2019). VoIP Foro - QoS - jitter - Causas, soluciones y valores recomendados. Retrieved 7 August 2019, from [http://www.voipforo.com/QoS/QoS\\_Jitter.php](http://www.voipforo.com/QoS/QoS_Jitter.php)

Vallejo A, (2017). Historia y Evolución de Redes Inalámbricas. Recuperado de: <https://prezi.com/a9aghvc4mfb9/historia-y-evolucion-de-redes-inalambricas>.

Velázquez D, 2017. Concurrencia de Procesos. Recuperado de: <https://www.webprogramacion.com/43/sistemas-operativos/concurrencia-de-procesos.aspx>

Wang, Y., & Shao, L. (2017). Understanding occupancy pattern and improving building energy efficiency through Wifi based indoor positioning. Building and Environment, 114, 106-117. doi: <http://dx.doi.org/10.1016/j.buildenv.2016.12.015>

Yao, Yi, Sheng, Bo, & Mi, Ningfang. (2016). A new packet scheduling algorithm for access points in crowded WLANs. *Ad Hoc Networks*, 36, Part 1, 100-110. doi: <http://dx.doi.org/10.1016/j.adhoc.2015.06.001>

## **ANEXOS.**

**ANEXO A:** Cisco Aironet 1700 Series Access Point. Especificaciones del Access Point utilizado para las pruebas y cálculos estadísticos.

## Cisco Aironet 1700 Series Access Points

**Doble Banda puntos de acceso con la onda 802.11ac 1 Soporte en el Integrated 5-GHz Radio**

**Ideal para entornos de oficina**

- Diseño elegante con antena interna
- acción correctiva automática
- UL 2043 para plenum para la instalación-techo por encima o suspensión de falsos techos
- implementaciones basadas en controlador y autónomas

**Los foros de solución de problemas**

- Información de interferencia histórica para el análisis de back-intime y resolución de problemas más rápida
- monitorización 24x7
- índice de calidad del aire proporciona una instantánea del rendimiento de la red y el impacto de interferencia

**Seguridad robusta y de aplicación de políticas**

- Detecta puntos de acceso y los ataques de denegación ofservice
- protección del marco de gestión detecta usuarios maliciosos y alerta a los administradores de red
- Políticas prohíben los dispositivos que interfieren con o ponen en peligro la seguridad de la red



### Descripción del producto

**Si usted opera una red pequeña o mediana empresa, desplegar el Cisco Aironet Serie 1700**

Punto de Acceso para la última 802.11ac tecnología Wi-Fi a un precio atractivo. La serie 1700 cumple con las crecientes necesidades de las redes inalámbricas mediante la mejor rendimiento que 802.11n y la disponibilidad de las características clave de gestión de RF para mejorar las experiencias inalámbricas.

La serie 1700 es compatible con 802.11ac Wave 1 capacidades estándar. Eso incluye una tasa de conexión teórica de hasta 867 Mbps. El rendimiento añadido le permite mantenerse a la vanguardia de la creciente requisitos de ancho de banda como:

- Más clientes inalámbricos asociarse a la red
- Los usuarios aprovechar las aplicaciones multimedia mucho ancho de banda
- Los trabajadores móviles utilizan cada vez más múltiples dispositivos Wi-Fi

### Características y Beneficios

Sobre la base del patrimonio Cisco Aironet de la excelencia de RF, los 1700 puntos de acceso de la serie se ejecutan en un chipset innovador especialmente diseñado con una arquitectura RF mejor en su clase. La Serie 1700 es un componente de la insignia de Cisco, 802.11ac a habilitar puntos de acceso Aironet que proporcionan experiencias de movilidad robustos.

**Tabla 1.** Capacidades primarias y Sus ventajas

Característica	Beneficio
<b>802.11ac Wave 1 de soporte con 3x3 de entrada múltiple y salida múltiple (MIMO) y dos flujos espaciales</b>	Proporciona altas velocidades a través de un mayor rango de mayor capacidad y fiabilidad que los puntos de acceso de la competencia. Proporciona hasta tres veces más ancho de banda que las redes 802.11n.
<b>Cisco Aire limpo. Exprimir espectro de Inteligencia</b>	canales Detecta la Interferencia de RF y proporciona capacidades básicas de análisis de espectro mientras que la simplificación de las operaciones en curso a través de 20-, 40-, y 80-MHz de ancho
<b>punto de acceso móvil optimizado</b>	Dirige dispositivos cliente para asociar con el punto de acceso en su rango de cobertura, que ofrece la tasa de datos más rápida disponible
<b>igualación MIMO</b>	Aumenta el rendimiento de enlace ascendente y la fiabilidad, reduciendo el impacto de desvanecimiento de la señal

Especificaciones del producto

Ítem	Especificación
Los números de pieza	<p><b>Cisco Aironet 1700i Punto de Acceso:</b> entornos de interior, con antenas internas</p> <ul style="list-style-type: none"> <li>• AIR-CAP1702I-X-K9: de doble banda, basado en un controlador 802.11a / g / n / ac</li> <li>• AIR-CAP1702I-X-K910: Eco-pack (802.11a de doble banda / g / n / ac) puntos de acceso 10 de cantidad</li> </ul> <p><b>SMARTnet® Servicio para el 1700i punto de acceso Cisco Aironet con antenas internas</b></p> <ul style="list-style-type: none"> <li>• CON-SNT-C172IX: SMARTnet 8x5xNBD de punto de acceso 1700i (banda dual 802.11a / g / n / ac)</li> <li>• CON-SNT-C172IX10: SMARTnet 8x5xNBD para 10-cantidad del punto de eco-pack acceso 1700i (banda dual 802.11a / g / n / ac)</li> </ul> <p>dominios reguladores: (x = dominio regulador)</p> <p>Los clientes son responsables de verificar la aprobación para su uso en sus respectivos países. Para verificar la aprobación e identificar el dominio regulador que corresponde a un determinado país, visita <a href="http://www.cisco.com/go/aironet/compliance">http://www.cisco.com/go/aironet/compliance</a>. No todos los dominios reguladores han sido aprobados. Y cuando sean aprobados, los números de referencia estarán disponibles en la lista global de precio.</p> <p>Servicios de Cisco Wireless LAN</p> <ul style="list-style-type: none"> <li>• AS-WLAN-Cnsit: <a href="#">Cisco Wireless LAN Red de Planificación y Diseño del Servicio</a></li> <li>• AS-WLAN-Cnsit: <a href="#">Cisco Wireless LAN Servicio de migración 802.11n</a></li> <li>• AS-WLAN-Cnsit: <a href="#">Cisco Wireless LAN Rendimiento y Servicio de Evaluación de Seguridad</a></li> </ul>
<b>Software</b>	<p>Cisco Unified Wireless Network Software versión 8.0 o posterior AP Autónoma de</p> <p>Cisco IOS Software versión 15.3.3 o posterior-JAB</p>
Los controladores de LAN inalámbrica compatibles	<p>Cisco 2500 controladores inalámbricos Series, módulo controlador de Cisco inalámbrica para ISR G2, servicios inalámbricos de Cisco Módulo 2 (WISM2) para Cisco <b>Catalyst® 6500 switches de la serie Cisco 5500, mandos inalámbricos de la serie Cisco Flex® 7500 Mandos inalámbricos de la serie Cisco 8500, mandos inalámbricos de la serie, mando inalámbrico Cisco Virtual</b>; Cisco 5760 Controlador de LAN inalámbrica, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 3650 Series Switches</p>
<b>versión 802.11n 2.0 (y afines) capacidades</b>	<ul style="list-style-type: none"> <li>• MIMO 3x3 con dos flujos espaciales</li> <li>• combinación de relación máxima (MRC)</li> <li>• 802.11n y 802.11a / g de formación de haces</li> <li>• canales 20 y 40 MHz</li> <li>• velocidades de datos PHY de hasta 300 Mbps (40 MHz con 6 GHz)</li> <li>• agregación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx)</li> <li>• 802.11 Selección de Frecuencia Dinámica (DFS)</li> <li>• la diversidad desplazamiento cíclico de soporte (CSD)</li> </ul>
<b>802.11ac Wave 1 capacidades</b>	<ul style="list-style-type: none"> <li>• MIMO 3x3 con dos flujos espaciales</li> <li>• MRC</li> <li>• 802.11ac estándar de formación de haz explícita</li> <li>• 20-, canales de 40-, y 80-MHz</li> <li>• velocidades de datos PHY de hasta 867 Mbps (80 MHz en 5 GHz)</li> <li>• agregación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx)</li> <li>• 802.11 DFS</li> <li>• apoyo CSD</li> </ul>

Ítem	Especificación						
velocidades de datos soportadas	802.11a: 6, 9, 12, 18, 24, 36, 48, y 54 Mbps						
	802.11g: 1, 2, 5,5, 6, 9, 11, 12, 18, 24, 36, 48, y 54 Mbps						
	velocidades de datos 802.11n en 2,4 GHz:						
	Índice de MCS:	estándar americano - 800 ns		GI = 400 ns			
		20-MHz Rate (Mbps)		20-MHz Rate (Mbps)			
	0	6.5		7.2			
	1	13		14.4			
	2	19.5		21.7			
	3	26		28.9			
	4	39		43.3			
	5	52		57.8			
	6	58.5		sesenta y cinco			
	7	sesenta y cinco		72.2			
	8	13		14.4			
	9	26		28.9			
	10	39		43.3			
	11	52		57.8			
	12	78		86.7			
	13	104		115,6			
	14	117		130			
	15	130		144,4			
	velocidades de datos 802.11ac (5 GHz):						
	Índice de MCS:	flujos espaciales	estándar americano - 800ns			GI = 400ns	
20-MHz Rate (Mbps)			40-MHz Rate (Mbps)	80-MHz Rate (Mbps)	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	80-MHz Rate (Mbps)
0	1	6.5	13.5	29.3	7.2	15	32.5
1	1	13	27	58.5	14.4	30	sesenta y cinco
2	1	19.5	40.5	87.8	21.7	45	97.5
3	1	26	54	117	28.9	60	130
4	1	39	81	175,5	43.3	90	195
5	1	52	108	234	57.8	120	260
6	1	58.5	121,5	263.3	sesenta y cinco	135	292,5
7	1	sesenta y cinco	135	292,5	72.2	150	325
8	1	78	162	351	86.7	180	390
9	1	-	180	390	-	200	433,3
0	2	13	27	58.5	14.4	30	sesenta y cinco

Índice de MCS: La modulación y codificación índice del esquema (MCS) determina el número de flujos espaciales, la modulación, la velocidad de codificación, y los valores de velocidad de datos.

GI: Un intervalo de protección (GI) entre los símbolos ayuda a los receptores a superar los efectos de los retardos multitrayecto.

Índice de MCS: La modulación y codificación índice del esquema (MCS) determina el número de flujos espaciales, la modulación, la velocidad de codificación, y los valores de velocidad de datos.

GI: Un intervalo de protección (GI) entre los símbolos ayuda a los receptores a superar los efectos de los retardos multitrayecto.

Ít	Especificación							
	1	2	26	54	117	28.9	60	130
	2	2	39	81	175,5	43.3	90	195
	3	2	52	108	234	57.8	120	260
	4	2	78	162	351	86.7	180	390
	5	2	104	216	468	115,6	240	520
	6	2	117	243	526,5	130	270	585
	7	2	130	270	585	144,4	300	650
	8	2	156	324	702	173,3	360	780
	9	2	-	360	780	-	400	866,7
<b>banda de frecuencia y 20 MHz canales de operación</b>	<b>A (un dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,462 GHz; 11 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,500-5,700 GHz; 8 canales (excluye 5,600 a 5,640 GHz)</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>C (C dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>D (D dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,462 GHz; 11 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>E (E dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,500-5,700 GHz; 8 canales (excluye 5,600 a 5,640 GHz)</li> </ul> <b>F (F dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,745-5,805 GHz; 4 canales</li> </ul> <b>H (H dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,350 GHz; 8 canales</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>I (I dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,320 GHz; 8 canales</li> </ul> <b>K (K dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,500-5,620 GHz; 7 canales</li> <li>5,745-5,805 GHz; 4 canales</li> </ul>				<b>N (N dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,462 GHz; 11 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>Q (Q dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,500-5,700 GHz; 11 canales</li> </ul> <b>R (dominio regulador R):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,660-5,805 GHz; 7 canales</li> </ul> <b>S (S dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,472 GHz; 13 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,500-5,700 GHz; 11 canales</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>T (T dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,462 GHz; 11 canales</li> <li>5,280-5,320 GHz; 3 canales</li> <li>5,500-5,700 GHz; 8 canales (excluye 5,600 a 5,640 GHz)</li> <li>5,745-5,825 GHz; 5 canales</li> </ul> <b>Z (Z dominio regulador):</b> <ul style="list-style-type: none"> <li>2,412-2,462 GHz; 11 canales</li> <li>5,180-5,320 GHz; 8 canales</li> <li>5,500-5,700 GHz; 8 canales (excluye 5,600 a 5,640 GHz)</li> <li>5,745-5,825 GHz; 5 canales</li> </ul>			
<b>Nota:</b> Los clientes son responsables de verificar la aprobación para su uso en sus respectivos países. Para verificar la aprobación e identificar el dominio regulador que corresponde a un determinado país, visita <a href="http://www.cisco.com/go/aironet/compliance">http://www.cisco.com/go/aironet/compliance</a> .								
<b>número máximo de canales que no se superponen</b>	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>802.11b / g: <ul style="list-style-type: none"> <li>20 MHz: 3</li> </ul> </li> <li>802.11n: <ul style="list-style-type: none"> <li>20 MHz: 3</li> </ul> </li> </ul>				<b>5 GHz</b> <ul style="list-style-type: none"> <li>802.11a: <ul style="list-style-type: none"> <li>20 MHz: 24</li> </ul> </li> <li>802.11n: <ul style="list-style-type: none"> <li>20 MHz: 24</li> <li>40 MHz: 11</li> </ul> </li> <li>802.11ac: <ul style="list-style-type: none"> <li>20 MHz: 24</li> <li>40 MHz: 11</li> <li>80 MHz: 5</li> </ul> </li> </ul>			
<b>Nota:</b> Esto varía según el dominio regulador. Consulte la documentación del producto para obtener detalles específicos para cada dominio regulador.								

Ítem	Especificación								
sensibilidad de recepción	<ul style="list-style-type: none"> <li>802.11b (CCK) <ul style="list-style-type: none"> <li>-101 dBm @ 1 Mbps</li> <li>-99 dBm @ 2 Mbps</li> <li>-93 dBm @ 5,5 Mbps</li> <li>-90 dBm @ 11 Mbps</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>802.11g (no HT20) <ul style="list-style-type: none"> <li>-93 dBm @ 6 Mbps</li> <li>-92 dBm @ 9 Mbps</li> <li>-92 dBm @ 12 Mbps</li> <li>-91 dBm @ 18 Mbps</li> <li>-88 dBm @ 24 Mbps</li> <li>-85 dBm @ 36 Mbps</li> <li>-80 dBm @ 48 Mbps</li> <li>-79 dBm @ 54 Mbps</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>802.11a (no HT20) <ul style="list-style-type: none"> <li>-93 dBm @ 6 Mbps</li> <li>-92 dBm @ 9 Mbps</li> <li>-92 dBm @ 12 Mbps</li> <li>-91 dBm @ 18 Mbps</li> <li>-88 dBm @ 24 Mbps</li> <li>-85 dBm @ 36 Mbps</li> <li>-80 dBm @ 48 Mbps</li> <li>-79 dBm @ 54 Mbps</li> </ul> </li> </ul>						
	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>802.11n (HT20) <ul style="list-style-type: none"> <li>-93 dBm @ MCS0</li> <li>-92 dBm @ MCS1</li> <li>-90 dBm @ MCS2</li> <li>-87 dBm @ MCS3</li> <li>-84 dBm @ MCS4</li> <li>-79 dBm @ MCS5</li> <li>-78 dBm @ MCS6</li> <li>-77 dBm @ MCS7</li> <li>-92 dBm @ MCS8</li> <li>-90 dBm @ MCS9</li> <li>-88 dBm @ MCS10</li> <li>-85 dBm @ MCS11</li> <li>-82 dBm @ MCS12</li> <li>-78 dBm @ MCS13</li> <li>-76 dBm @ MCS14</li> <li>-75 dBm @ MCS15</li> </ul> </li> </ul>		<b>5 GHz</b> <ul style="list-style-type: none"> <li>802.11n (HT20) <ul style="list-style-type: none"> <li>-93 dBm @ MCS0</li> <li>-92 dBm @ MCS1</li> <li>-90 dBm @ MCS2</li> <li>-87 dBm @ MCS3</li> <li>-84 dBm @ MCS4</li> <li>-80 dBm @ MCS5</li> <li>-78 dBm @ MCS6</li> <li>-77 dBm @ MCS7</li> <li>-92 dBm @ MCS8</li> <li>-90 dBm @ MCS9</li> <li>-88 dBm @ MCS10</li> <li>-85 dBm @ MCS11</li> <li>-82 dBm @ MCS12</li> <li>-77 dBm @ MCS13</li> <li>-76 dBm @ MCS14</li> <li>-74 dBm @ MCS15</li> </ul> </li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>802.11n (HT40) <ul style="list-style-type: none"> <li>-90 dBm @ MCS0</li> <li>-88 dBm @ MCS1</li> <li>-87 dBm @ MCS2</li> <li>-84 dBm @ MCS3</li> <li>-81 dBm @ MCS4</li> <li>-76 dBm @ MCS5</li> <li>-75 dBm @ MCS6</li> <li>-74 dBm @ MCS7</li> <li>-89 dBm @ MCS8</li> <li>-87 dBm @ MCS9</li> <li>-85 dBm @ MCS10</li> <li>-82 dBm @ MCS11</li> <li>-78 dBm @ MCS12</li> <li>-74 dBm @ MCS13</li> <li>-73 dBm @ MCS14</li> <li>-71 dBm @ MCS15</li> </ul> </li> </ul>					
	<b>802.11ac Sensibilidad de Recepción</b>								
	<b>802.11ac (no HT80)</b> <ul style="list-style-type: none"> <li>-86 dBm @ 6 Mbps</li> <li>-74 dBm @ 54 Mbps</li> </ul>								
	índice de MCS	flujos espaciales	VHT20	VHT40	VHT80	VHT20-STBC	VHT40-STBC	VHT80-STBC	
	0	1	-92 dBm	-89 dBm	-85 dBm	-92 dBm	-89 dBm	-85 dBm	
	8	1	-73 dBm			-73 dBm			
	9	1		-68 dBm	-65 dBm		-68 dBm	-65 dBm	
	0	2	-91 dBm	-87 dBm	-84 dBm				
	8	2	-71 dBm						
	9	2		-66 dBm	-62 dBm				
potencia de transmisión máxima	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>802.11b <ul style="list-style-type: none"> <li>22 dBm, 3 antenas</li> </ul> </li> <li>802.11g <ul style="list-style-type: none"> <li>22 dBm, 3 antenas</li> </ul> </li> <li>802.11n (HT20) <ul style="list-style-type: none"> <li>22 dBm, 3 antenas</li> </ul> </li> </ul>		<b>5 GHz</b> <ul style="list-style-type: none"> <li>802.11a <ul style="list-style-type: none"> <li>22 dBm, 3 antenas</li> </ul> </li> <li>802.11n (HT20) <ul style="list-style-type: none"> <li>22 dBm, 3 antenas</li> </ul> </li> <li>802.11n (HT40) <ul style="list-style-type: none"> <li>22 dBm, 3 antenas</li> </ul> </li> <li>802.11ac <ul style="list-style-type: none"> <li>no HT80: 22 dBm, 3 antenas</li> </ul> </li> </ul>						

Índice de MCS: La modulación y codificación índice del esquema (MCS) determina el número de flujos espaciales, la modulación, la velocidad de codificación, y los valores de velocidad de datos.

Ítem	Especificación		
	<ul style="list-style-type: none"> <li>• VHT20 22 dBm, 3 antenas</li> <li>• VHT40: 22 dBm, 3 antenas</li> <li>• VHT80: 22 dBm, 3 antenas</li> <li>• VHT20-STBC: 22 dBm, 3 antenas</li> <li>• VHT40-STBC: 22 dBm, 3 antenas</li> <li>• VHT80-STBC: 22 dBm, 3 antenas</li> </ul>		
<p><b>Nota:</b> El ajuste de la potencia máxima variará por canal y de acuerdo a las regulaciones de cada país. Consulte la documentación del producto para obtener detalles específicos.</p>			
ajustes de potencia de transmisión disponibles	<table border="0"> <tr> <td style="vertical-align: top;"> <b>2.4 GHz</b> <ul style="list-style-type: none"> <li>• 22 dBm (160 mW)</li> <li>• 19 dBm (80 mW)</li> <li>• 16 dBm (40 mW)</li> <li>• 13 dBm (20 mW)</li> <li>• 10 dBm (10 mW)</li> <li>• 7 dBm (5 mW)</li> <li>• 4 dBm (2,5 mW)</li> <li>• 2 dBm (1,25 mW)</li> </ul> </td> <td style="vertical-align: top;"> <b>5 GHz</b> <ul style="list-style-type: none"> <li>• 22 dBm (160 mW)</li> <li>• 19 dBm (80 mW)</li> <li>• 16 dBm (40 mW)</li> <li>• 13 dBm (20 mW)</li> <li>• 10 dBm (10 mW)</li> <li>• 7 dBm (5 mW)</li> <li>• 4 dBm (2,5 mW)</li> <li>• 1 dBm (1,25 mW)</li> </ul> </td> </tr> </table>	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>• 22 dBm (160 mW)</li> <li>• 19 dBm (80 mW)</li> <li>• 16 dBm (40 mW)</li> <li>• 13 dBm (20 mW)</li> <li>• 10 dBm (10 mW)</li> <li>• 7 dBm (5 mW)</li> <li>• 4 dBm (2,5 mW)</li> <li>• 2 dBm (1,25 mW)</li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>• 22 dBm (160 mW)</li> <li>• 19 dBm (80 mW)</li> <li>• 16 dBm (40 mW)</li> <li>• 13 dBm (20 mW)</li> <li>• 10 dBm (10 mW)</li> <li>• 7 dBm (5 mW)</li> <li>• 4 dBm (2,5 mW)</li> <li>• 1 dBm (1,25 mW)</li> </ul>
<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>• 22 dBm (160 mW)</li> <li>• 19 dBm (80 mW)</li> <li>• 16 dBm (40 mW)</li> <li>• 13 dBm (20 mW)</li> <li>• 10 dBm (10 mW)</li> <li>• 7 dBm (5 mW)</li> <li>• 4 dBm (2,5 mW)</li> <li>• 2 dBm (1,25 mW)</li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>• 22 dBm (160 mW)</li> <li>• 19 dBm (80 mW)</li> <li>• 16 dBm (40 mW)</li> <li>• 13 dBm (20 mW)</li> <li>• 10 dBm (10 mW)</li> <li>• 7 dBm (5 mW)</li> <li>• 4 dBm (2,5 mW)</li> <li>• 1 dBm (1,25 mW)</li> </ul>		
<p><b>Nota:</b> El ajuste de la potencia máxima variará por canal y de acuerdo a las regulaciones de cada país. Consulte la documentación del producto para obtener detalles específicos.</p>			
antena integrada	<ul style="list-style-type: none"> <li>• 2.4 GHz, ganar 4 dBi, internas Omni, anchura de haz horizontal 360 °</li> <li>• 5 GHz, ganar 4 dBi, omni, anchura de haz horizontal interna de 360 °</li> </ul>		
Interfaces	<ul style="list-style-type: none"> <li>• 2x10 / 100 / 1000BASE-T de detección automática (RJ-45)</li> <li>• puerto de la consola de gestión (RJ-45)</li> </ul>		
indicadores	<ul style="list-style-type: none"> <li>• LED de estado indica el estado del gestor de arranque, el estado de asociación, el estado de funcionamiento, las advertencias del cargador de arranque, los errores del gestor de arranque</li> </ul>		
Dimensiones (W x L x H)	<ul style="list-style-type: none"> <li>• Punto de acceso (sin soporte de montaje): 8,69 x 8,69 x 1,99 in (22,1 x 22,1 x 5,1 cm).</li> </ul>		
Peso	<ul style="list-style-type: none"> <li>• 2,2 lb (1,0 kg)</li> </ul>		
Ambiental	<p><b>Cisco Aironet 1702i</b></p> <ul style="list-style-type: none"> <li>• De no funcionamiento (almacenamiento) Temperatura: -22 ° a 168 ° F (-30 ° a 70 ° C)</li> <li>• Sin funcionamiento (almacenamiento) Prueba de altitud: 28 ° C, 16.000 pies.</li> <li>• Temperatura de funcionamiento: 32 ° a 104 ° F (0 ° a 40 ° C)</li> <li>• Humedad de funcionamiento: 10% a 90% por ciento (sin condensación)</li> <li>• prueba de Altitud de funcionamiento: 40 ° C, 9843 pies.</li> </ul>		
Memoria del sistema	<ul style="list-style-type: none"> <li>• 512 MB de DRAM</li> <li>• 64 MB de flash</li> </ul>		
los requisitos de potencia de entrada	<ul style="list-style-type: none"> <li>• AP1700: 44-57 VDC</li> <li>• Fuente de alimentación y el inyector de potencia: 100 a 240 VCA; 50 a 60 Hz</li> </ul>		
Poder de dibujo	<ul style="list-style-type: none"> <li>• AP1700: 15W</li> </ul>		
las opciones de alimentación	<ul style="list-style-type: none"> <li>• 802.3at PoE +</li> <li>• PoE mejorada</li> <li>• inyectores de potencia Cisco AP1700 (AIR-PWRINJ5 =)</li> <li>• Cisco AP1700 fuente de alimentación local (AIR-PWR-B =)</li> </ul>		
Garantía	<p>garantía de hardware limitada de por vida</p>		
normas de cumplimiento	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CAN / CSA-C22.2 No. 60950-1</li> <li>• UL 2043</li> <li>• IEC 60950-1</li> <li>• EN 60950-1</li> <li>• 50155</li> <li>• Autorizaciones de radio: <ul style="list-style-type: none"> <li>• FCC Parte 15.247, 15.407</li> <li>• RS-210 (Canadá)</li> </ul> </li> </ul>		

Ít	Especificación
	<ul style="list-style-type: none"> <li>▸ ES 300.328, 301.893 ES (Europa)</li> <li>▸ ARIB-STD 66 (Japón)</li> <li>▸ ARIB STD-T71 (Japón)</li> <li>▸ EMI y la susceptibilidad (clase B)</li> <li>▸ FCC Parte 15.107 y 15.109</li> <li>▸ ICES-003 (Canadá)</li> <li>▸ VCCI (Japón)</li> <li>▸ ES 301,489 a 1 y 17 (Europa)</li> <li>▸ EN 60601-1-2 requisitos de compatibilidad electromagnética para la Directiva 93/42 / CEE del Consejo</li> <li>● Los estándares IEEE: <ul style="list-style-type: none"> <li>▸ IEEE 802.11a / b / g, 802.11n, 802.11h, 802.11d</li> <li>▸ Proyecto de IEEE 802.11ac 6</li> </ul> </li> <li>● Seguridad: <ul style="list-style-type: none"> <li>▸ 802.11i, acceso Wi-Fi Protected Access 2 (WPA2), WPA</li> <li>▸ 802.1X</li> <li>▸ Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP)</li> </ul> </li> <li>● Protocolo de autenticación extensible (EAP) tipos: <ul style="list-style-type: none"> <li>▸ EAP-Transport Layer Security (TLS)</li> <li>▸ EAP-TLS de túnel (TTLS) o desafío mutuo de Microsoft versión 2 del protocolo de autenticación (MSCHAPv2)</li> <li>▸ EAP protegido (PEAP) v0 o EAP-MSCHAPv2</li> <li>▸ EAP-flexible de autenticación a través de túnel Seguro (FAST)</li> <li>▸ v1 PEAP o EAP-Generic Token Card (GTC)</li> <li>▸ Módulo de identidad EAP-suscriptor (SIM)</li> </ul> </li> <li>● Multimedia: <ul style="list-style-type: none"> <li>▸ Wi-Fi Multimedia (WMM)</li> </ul> </li> <li>● Otros: <ul style="list-style-type: none"> <li>▸ FCC Boletín OET-65C</li> <li>▸ RSS-102 Wi-Fi CERTIFIED ~ a, b, g, n, ac</li> </ul> </li> </ul>

#### Información sobre pedidos

Para hacer un pedido, visite el [Cisco página principal de pedidos](#) . Para descargar el software, visite el [Centro de Software de Cisco](#) .

**Tabla 2.** Información sobre pedidos

Nombre / Descripción	Número de pieza
Cisco Aironet punto de acceso 1702i; De doble banda, basado en un controlador 802.11a / g / n / ac (individuales)	AIR-CAP1702I-x-K9
Cisco Aironet punto de acceso 1702i; De doble banda, basado en un controlador 802.11a / g / n / ac eco-pack (10 cantidad)	AIR-CAP1702I-xK910

#### Garantía de hardware limitada de por vida

Los Cisco Aironet 1700 Series Access Points vienen con una garantía limitada de por vida que proporciona cobertura de garantía completa del hardware durante el tiempo que el usuario final original continúa siendo el propietario o usar el producto. La garantía incluye el reemplazo de material por adelantado de 10 días y se asegura de que los medios de comunicación de software son por 90 días sin defectos. Para más detalles, visita <http://www.cisco.com/go/warranty> .

---

### Servicios de Cisco Wireless LAN

Darse cuenta del valor de negocios total de sus inversiones en tecnología, más rápido con servicios inteligentes personalizadas de Cisco y de nuestros socios. Con el respaldo de experiencia en redes de profundidad y un amplio ecosistema de socios, Servicios de Cisco Wireless LAN le permiten desplegar un sonido, red de movilidad escalable que fomenta la colaboración multimedia. Al mismo tiempo, se puede mejorar la eficiencia operativa obtenida de una infraestructura de red cableada e inalámbrica convergente basado en la Red inalámbrica unificada de Cisco. Junto con sus socios, ofrecemos plan de expertos, construimos, y los servicios se ejecutan para acelerar su transición a los servicios avanzados de movilidad. A continuación, le ayudamos a optimizar continuamente el rendimiento, la fiabilidad y la seguridad de que la arquitectura después de la implementación. Para más detalles, visita

<http://www.cisco.com/go/wirelesslanservices>.

### Cisco capital

#### Financiación para ayudarle a alcanzar sus objetivos

Cisco capital® puede ayudarle a adquirir la tecnología que necesita para alcanzar sus objetivos y seguir siendo competitivos. Podemos ayudarle a reducir los gastos de capital. Acelerar su crecimiento. Optimizar sus dólares de inversión y retomo de la inversión. Financiación del capital de Cisco le da flexibilidad en la adquisición de hardware, software, servicios y equipos de terceros complementaria. Y hay un solo pago predecible. Cisco Capital está disponible en más de 100 países. Aprende más.

### Para más información

Para obtener más información sobre el Cisco Aironet 1700 Series, visita <http://www.cisco.com/go/wireless> o póngase en contacto con su representante de cuenta local.



---

Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

**ANEXO B:** Cisco 8500 Series Wireless Controller. Especificaciones de la herramienta utilizada para pruebas y simulaciones.



# Cisco 8500 Series Wireless Controllers

The Cisco® 8500 Series Wireless Controllers are a highly scalable and flexible platform that enables mission-critical wireless networking for enterprise and service provider deployments.

<p><b>Lower CapEx and OpEx</b></p> <ul style="list-style-type: none"> <li>Consolidate multiple controllers into one controller with support for up to 6000 access points, and save on rack space with a 1RU platform.</li> <li>Deploy fewer controllers in a data center by consolidating many controllers into one controller that supports centralized deployments and Cisco FlexConnect™ and mesh access point deployments.</li> <li>Gain significant savings in operations by configuring, managing, and troubleshooting up to 6000 access points and 64,000 clients with a single point of touch.</li> </ul>
<p><b>Multilayer High Availability (HA)</b></p> <ul style="list-style-type: none"> <li>Service Set Identifier (SSID) HA with sub-second access point and client failover.</li> <li>Dual-redundant power supplies installed.</li> <li>Dual-redundant 10 Gigabit Ethernet connectivity.</li> </ul>
<p><b>Service Provider Wi-Fi</b></p> <ul style="list-style-type: none"> <li>Wi-Fi Certified Passpoint (Hotspot 2.0) for mobile data offload.</li> <li>Network-based mobility management with Proxy Mobile IPv6 Mobility Access Gateway (MAG) support for integration with cellular data networks.</li> </ul>
<p><b>Licensing Flexibility and Investment Protection</b></p> <ul style="list-style-type: none"> <li>Additional access point capacity licenses can be added over time.</li> <li>Right-to-use licensing (with EULA acceptance) for faster and easier license enablement.</li> </ul>
<p><b>FlexConnect, Centralized, and Mesh Deployment Flexibility in a Single Controller</b></p> <ul style="list-style-type: none"> <li>Intelligent RF control plane, centralized software update, control and management, and troubleshooting.</li> <li>Mesh access point support for deployments where full Ethernet cabling is not available.</li> <li>Deploy Cisco FlexConnect in sites with up to 100 access points in up to 2000 groups.</li> </ul>
<p><b>Comprehensive Wired and Wireless Security</b></p> <ul style="list-style-type: none"> <li>Full access point-to-controller encryption via the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.</li> <li>Supports rogue access point detection and detection of denial-of-service attacks.</li> <li>Management frame protection detects malicious users and alerts network administrators.</li> </ul>
<p><b>Secured Guest Access</b></p> <ul style="list-style-type: none"> <li>Deploy simple and secure guest access services across 6000 sites.</li> </ul>

Designed for 802.11ac and [802.11n](#) performance and maximum scalability, the 8500 Series offers enhanced uptime for high-scale deployments with support for:

- 6000 access points and 64,000 clients in a 1RU form factor
- 4096 VLANs for large-scale deployments
- Sub-second access point and client failover for Service Set Identifier (SSID) high availability
- Dual-redundant power supplies installed (AC or DC)
- Dual-redundant 10 Gigabit Ethernet connectivity

Figure 1. Cisco 8500 Series Wireless Controller



## Features

The Cisco 8500 Series Wireless Controllers (Figure 1) provide centralized control, management, and troubleshooting for enterprise and service provider deployments. The 8500 Series offers flexibility to support multiple deployment modes in the same controller: for example, centralized mode for campus, Cisco FlexConnect™ mode for lean branches managed over the WAN, and mesh (bridge) mode for deployments where full Ethernet cabling is unavailable.

The Cisco 8500 Series Wireless Controllers support Cisco Application Visibility and Control (AVC). Cisco AVC includes the Network-Based Application Recognition 2 (NBAR-2) engine, Cisco's deep packet inspection (DPI) capability, which classifies applications, applies quality of service (QoS) settings to either drop or mark the traffic, and prioritizes business-critical applications in the network. Cisco AVC uses NetFlow Version 9 to export the flows to [Cisco Prime™ Infrastructure](#) or a third-party NetFlow collector.

The Cisco 8500 Series also supports Bonjour Services Directory to enable Bonjour Services to be advertised and utilized in a separate Layer 3 network. A wireless policy engine on the Cisco 8500 Series enables profiling of wireless devices and enforcement of policies such as VLAN assignment, QoS, access control lists (ACLs), and time-of-day- based access.

Cisco 8500 Series Wireless Controllers automate wireless configuration and management functions and allow network managers to have the visibility and control needed to cost-effectively manage, secure, and optimize the performance of their branch networks. As a component of the Cisco Unified [Wireless Network](#), this controller provides real-time communications between [Cisco Aironet® access points](#), [Cisco Prime Infrastructure](#), and the [Cisco Mobility Services Engine](#), and is interoperable with other Cisco controllers.

The Cisco 8500 Series has integrated Cisco CleanAir® technology, providing the industry's only self-healing and self-optimizing wireless network for branches.

### Software Licensing Flexibility

Cisco 8500 Series Wireless Controllers provide right-to-use license enablement (with EULA agreement) for faster time to deployment, with the flexibility to add additional access points (up to 6000 access points) as business needs grow. Table 1 lists the features and benefits of the Cisco 8500 Series Wireless Controllers.

**Table 1.** Features and Benefits

Feature	Benefits
<b>Scalability</b>	<ul style="list-style-type: none"> <li>• Supports 100,300, 500, 1000, 3000, or 6000 access points</li> <li>• Supports 64,000 clients</li> <li>• Supports up to 6000 branch locations (up to 2000 Cisco FlexConnect groups) with 100 access points per Flex-group and multiple Flex-groups per remote location</li> <li>• Supports up to 4096 VLANs</li> </ul>
<b>RF management</b>	<ul style="list-style-type: none"> <li>• Provides both real-time and historical information about RF interference affecting network performance across controllers, through systemwide integration of <a href="#">Cisco CleanAir technology</a></li> </ul>
<b>Cisco FlexConnect, centralized switching, and mesh access point support</b>	<ul style="list-style-type: none"> <li>• Centralized control, management, and client troubleshooting</li> <li>• Seamless client access in the event of a WAN link failure (local data switching)</li> <li>• Highly secure guest access</li> <li>• Indoor and outdoor mesh access point support</li> <li>• Efficient access point upgrade that optimizes the WAN link utilization for downloading access point images</li> <li>• Cisco OfficeExtend technology that supports corporate wireless service for mobile and remote workers with secure wired tunnels to Cisco Aironet Access Points</li> <li>• Rogue detection for Payment Card Industry (PCI) compliance</li> </ul>
<b>Service provider Wi-Fi</b>	<ul style="list-style-type: none"> <li>• Wi-Fi Certified Passpoint (Hotspot 2.0), facilitating hotspot operation for mobile data offloads</li> <li>• Network-based mobility management with Proxy Mobile IPv6 Mobility Access Gateway (MAG) support for integration with cellular data networks</li> </ul>
<b>Comprehensive end-to-end security</b>	<ul style="list-style-type: none"> <li>• Offers CAPWAP-compliant Datagram Transport Layer Security (DTLS) encryption on the control plane between access points and controllers across remote WAN links</li> </ul>
<b>End-to-end voice</b>	<ul style="list-style-type: none"> <li>• Supports <a href="#">Cisco Unified Communications</a> for improved collaboration through messaging, presence, and conferencing</li> <li>• Supports all <a href="#">Cisco Unified IP Phones</a> for cost-effective, real-time voice services</li> </ul>
<b>Fault tolerance and high availability</b>	<ul style="list-style-type: none"> <li>• Access points continue to provide seamless services when a controller fails; provides failover to another backup controller for centralized control and management</li> <li>• SSID high availability with sub-second access point and client failover from the primary to standby controller</li> <li>• Redundant power supply helps ensure maximum availability</li> <li>• 10 Gigabit Ethernet connectivity: Two 10 Gigabit Ethernet ports for redundancy</li> </ul>
<b>Enterprise Wireless Mesh</b>	<ul style="list-style-type: none"> <li>• Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network</li> <li>• Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing</li> </ul>

Feature	Benefits
<b>High-performance video</b>	<ul style="list-style-type: none"> <li>Integrates Cisco VideoStream technology as part of the medianet framework to optimize the delivery of video applications across the WLAN</li> </ul>
<b>Mobility, security, and management for IPv6 and dual-stack clients</b>	<ul style="list-style-type: none"> <li>Highly secure, reliable wireless connectivity and consistent end-user experience</li> <li>Increased network availability through proactive blocking of known threats</li> <li>Equips administrators for IPv6 planning, troubleshooting, and client traceability from Cisco Prime Infrastructure</li> </ul>
<b>Environmentally responsible</b>	<ul style="list-style-type: none"> <li>Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours</li> </ul>

Table 2 lists the product specifications for the Cisco 8500 Series Wireless Controllers.

**Table 2.** Product Specifications

Item	Specifications
<b>Wireless</b>	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, <a href="#">802.11n</a> , 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac
<b>Wired/switching/routing</b>	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
<b>Data RFCs</b>	<ul style="list-style-type: none"> <li>RFC 768 UDP</li> <li>RFC 791 IP</li> <li>RFC 2460 IPv6 (pass-through Bridging mode only)</li> <li>RFC 792 ICMP</li> <li>RFC 793 TCP</li> <li>RFC 826 ARP</li> <li>RFC 1122 Requirements for Internet Hosts</li> <li>RFC 1519 CIDR</li> <li>RFC 1542 BOOTP</li> <li>RFC 2131 DHCP</li> <li>RFC 5415 CAPWAP Protocol Specification</li> <li>RFC 4346 TLS Protocol Version 1.1</li> </ul>
<b>Security standards</b>	<ul style="list-style-type: none"> <li>Wi-Fi Protected Access (WPA)</li> <li>IEEE 802.11i (WPA2, RSN)</li> <li>RFC 1321 MD5 Message-Digest Algorithm</li> <li>RFC 1851 ESP Triple DES Transform</li> <li>RFC 2104 HMAC: Keyed Hashing for Message Authentication</li> <li>RFC 2246 TLS Protocol Version 1.0</li> <li>RFC 2401 Security Architecture for the Internet Protocol</li> <li>RFC 2403 HMAC-MD5-96 within ESP and AH</li> <li>RFC 2404 HMAC-SHA-1-96 within ESP and AH</li> <li>RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV</li> <li>RFC 2407 Interpretation for ISAKMP</li> <li>RFC 2408 ISAKMP</li> <li>RFC 2409 IKE</li> <li>RFC 2451 ESP CBC-Mode Cipher Algorithms</li> <li>RFC 3280 Internet X.509 PKI Certificate and CRL Profile</li> <li>RFC 4347 Datagram Transport Layer Security</li> <li>RFC 4346 TLS Protocol Version 1.1</li> </ul>
<b>Encryption</b>	<ul style="list-style-type: none"> <li>Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys)</li> <li>Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP)</li> <li>Data Encryption Standard (DES): DES-CBC, 3DES</li> <li>Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit</li> <li>Datagram Transport Layer Security (DTLS): AES-CBC</li> <li>IPsec: DES-CBC, 3DES, AES-CBC</li> </ul>

Item	Specifications
<b>Authentication, authorization, and accounting (AAA)</b>	<ul style="list-style-type: none"> <li>• IEEE 802.1X</li> <li>• RFC 2548 Microsoft Vendor-Specific RADIUS Attributes</li> <li>• RFC 2716 PPP EAP-TLS</li> <li>• RFC 2865 RADIUS Authentication</li> <li>• RFC 2866 RADIUS Accounting</li> <li>• RFC 2867 RADIUS Tunnel Accounting</li> <li>• RFC 2869 RADIUS Extensions</li> <li>• RFC 3576 Dynamic Authorization Extensions to RADIUS</li> <li>• RFC 5176 Dynamic Authorization Extensions to RADIUS</li> <li>• RFC 3579 RADIUS Support for EAP</li> <li>• RFC 3580 IEEE 802.1X RADIUS Guidelines</li> <li>• RFC 3748 Extensible Authentication Protocol</li> <li>• Web-based authentication</li> <li>• TACACS support for management users</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>• Simple Network Management Protocol (SNMP) v1, v2c, v3</li> <li>• RFC 854 Telnet</li> <li>• RFC 1155 Management Information for TCP/IP-Based Internets</li> <li>• RFC 1156 MIB</li> <li>• RFC 1157 SNMP</li> <li>• RFC 1213 SNMP MIB II</li> <li>• RFC 1350 TFTP</li> <li>• RFC 1643 Ethernet MIB</li> <li>• RFC 2030 Sntp</li> <li>• RFC 2616 HTTP</li> <li>• RFC 2665 Ethernet-Like Interface types MIB</li> <li>• RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions</li> <li>• RFC 2819 RMON MIB</li> <li>• RFC 2863 Interfaces Group MIB</li> <li>• RFC 3164 Syslog</li> <li>• RFC 3414 User-Based Security Model (USM) for SNMPv3</li> <li>• RFC 3418 MIB for SNMP</li> <li>• RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs</li> <li>• Cisco private MIBs</li> </ul>
<b>Management interfaces</b>	<ul style="list-style-type: none"> <li>• Web-based: HTTP/HTTPS</li> <li>• Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port</li> <li>• Cisco Prime Infrastructure</li> </ul>
<b>Interfaces and Indicators</b>	<ul style="list-style-type: none"> <li>• 2 10 Gigabit Ethernet interfaces</li> <li>• Small Form-Factor Pluggable (SFP) options (only Cisco SFPs supported): SFP-10G-SR, SFP-10G-LR</li> <li>• LED indicators: Network Link, Diagnostics</li> <li>• 1 service port: 10/100/1000 Mbps Ethernet (RJ-45)</li> </ul>
<b>Physical dimensions</b>	<ul style="list-style-type: none"> <li>• Dimensions (WxDxH): 17.30 x 28.00 x 1.69 in. (440.0 x 711.4 x 43.0 mm)</li> <li>• Weight: 35.1 lb (15.9 kg) with 2 power supplies</li> </ul>

Item	Specifications
<b>Environmental conditions</b>	<p>Air temperature:</p> <ul style="list-style-type: none"> <li>Appliance on: 10° to 35°C (50° to 95°F); altitude: 0 to 914.4 m (3000 ft), decrease system temperature by 1.8°F (1.0°C) for every 1000-foot (305-m) increase in altitude</li> <li>Appliance off: 5° to 45°C (41° to 113°F); maximum altitude: 3048 m (10,000 ft)</li> <li>Storage: -40° to 60°C (-40° to 140°F); maximum altitude: 3048 m (10,000 ft)</li> </ul> <p>Humidity:</p> <ul style="list-style-type: none"> <li>Appliance on: 20% to 80%; maximum dew point: 70°F (21°C); maximum rate of change: 9°F (5°C)/hr</li> <li>Appliance off: 8% to 80%; maximum dew point: 80°F (27°C)</li> </ul> <p>Electrical input:</p> <ul style="list-style-type: none"> <li>Sine-wave input (47 - 63 Hz) required</li> <li>Input voltage range (DC): <ul style="list-style-type: none"> <li>Minimum: -40 VDC</li> <li>Maximum: -75 VDC</li> </ul> </li> <li>Input voltage low range: <ul style="list-style-type: none"> <li>Minimum: 100 VAC</li> <li>Maximum: 127 VAC</li> </ul> </li> <li>Input voltage high range: <ul style="list-style-type: none"> <li>Minimum: 200 VAC</li> <li>Maximum: 240 VAC</li> </ul> </li> <li>Input kilovolt-amperes (kVA), approximately: <ul style="list-style-type: none"> <li>Minimum: 0.090 kVA</li> <li>Maximum: 0.700 kVA</li> </ul> </li> <li>Heat output (maximum) 2302 Btu per hour (675 watts)</li> <li>Acoustical noise emissions: <ul style="list-style-type: none"> <li>Sound power, idling: 6.1 bels maximum</li> <li>Sound power, operating: 6.1 bels maximum</li> </ul> </li> </ul>
<b>Regulatory compliance</b>	<p>CE Mark</p> <p>Safety:</p> <ul style="list-style-type: none"> <li>UL 60950-1:2003</li> <li>EN 60950:2000</li> <li>EMI and susceptibility (Class A)</li> <li>U.S.: FCC Part 15.107 and 15.109</li> <li>Canada: ICES-003</li> <li>Japan: VCCI</li> <li>Europe: EN 55022, EN 55024</li> </ul>

Table 3 lists ordering and accessories information for the Cisco 8500 Series Wireless Controllers.

To place an order, visit the Cisco ordering website: <http://www.cisco.com/en/US/ordering/index.shtml>.

**Table 3.** Ordering Information

Part Number	Product Name	Cisco SMARTnet® Service 8x5xNBD
<b>AIR-CT8510-100-K9</b>	8500 Series Controller for up to 100 Cisco access points	CON-SNT-AIRC8510
<b>AIR-CT8510-300-K9</b>	8500 Series Controller for up to 300 Cisco access points	CON-SNT-AIRCT853
<b>AIR-CT8510-500-K9</b>	8500 Series Controller for up to 500 Cisco access points	CON-SNT-AIRCT855
<b>AIR-CT8510-1K-K9</b>	8500 Series Controller for up to 1000 Cisco access points	CON-SNT-AIRCT85Z
<b>AIR-CT8510-3K-K9</b>	8500 Series Controller for up to 3000 Cisco access points	CON-SNT-AIRCT85K
<b>AIR-CT8510-6K-K9</b>	8500 Series Controller for up to 6000 Cisco access points	CON-SNT-AIRCT856
<b>AIR-CT8510-HA-K9</b>	8500 Series Controller for High Availability	CON-SNT-AIRCT85
<b>AIR-CT8510-SP-K9</b>	8500 Series Wireless Controller with 0 APs included, Dual AC PSU	CON-SNT-AIRCT85B
<b>AIR-CT85DC-SP-K9</b>	8500 Series Wireless Controller with 0 APs included, Dual DC PSU	CON-SNT-AIRCT85A

## Additive Capacity Upgrade Licenses

Tables 4 and 5 show the additive capacity upgrade licenses that are available for the Cisco 8500 Series Wireless Controller.

**Table 4.** Ordering Information for Additive Capacity Licenses (e-Delivery PAKs)

	Part Number	Product Description	SWSS 8x5xNBD
<b>e-License</b>	L-LIC-CT8500-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key	CON-ECMU-LICCT85
	L-LIC-CT8500-1A	1 Access Point Adder License for the 8510 Controller (e-Delivery)	CON-ECMU-LICCT85A
	L-LIC-CT8500-100A	100 Access Point Adder License for the 8510 Controller (e-Delivery)	CON-ECMU-LICCT851
	L-LIC-CT8500-500A	500 Access Point Adder License for the 8510 Controller (e-Delivery)	CON-ECMU-LICCT855
	L-LIC-CT8500-1000A	1000 Access Point Adder License for the 8510 Controller (e-Delivery)	CON-ECMU-CT851KA

**Table 5.** Ordering Information for Additive Capacity Licenses (Paper PAKs)

	Part Number	Product Description	SWSS 8x5xNBD
<b>Paper License</b>	LIC-CT8500-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many controllers under one product authorization key	CON-ECMU-CT8500UP
	LIC-CT8500-1A	1A Access Point Adder License for the 8510 Controller	CON-ECMU-LICCT85A
	LIC-CT8500-100A	100 Access Point Adder License for the 8510 Controller	CON-ECMU-LICCT851
	LIC-CT8500-500A	500 Access Point Adder License for the 8510 Controller	CON-ECMU-LICCT855
	LIC-CT8500-1000A	1000 Access Point Adder License for the 8510 Controller	CON-ECMU-CT851KA

Table 6 shows the optional DTLs license for the Cisco 8500 Series Wireless Controllers.

Datagram Transport Layer Security (DTLS) is required for all Cisco OfficeExtend deployments to encrypt the data plane traffic. To enable this functionality, you must obtain a \$0 DTLS license. Customers planning to install this device physically in Russia must obtain a paper PAK in order to enable a DTLS license and should not download the license from Cisco.com. Please consult your local government regulations to ensure that data DTLS encryption is permitted.

The DTLS paper PAK license is designated for customers who purchase a controller with DTLS disabled due to import restrictions but get permission to add DTLS support after initial purchase. This optional DTLS license is required for Cisco OfficeExtend deployment.

**Table 6.** Optional Licensing (PAKs) and Accessories

Part Number	Description
<b>LIC-CT8500-UPG</b>	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key
<b>LIC-CT8510-DTLS-K9</b>	Cisco 8500 Series Controller DTLS License (paper Certificate - U.S. Mail)
<b>L-LIC-CT8500-UPG</b>	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key
<b>L-LIC-CT85-DTLS-K9</b>	Cisco 8500 Series Controller DTLS License (electronic certificate - must not be ordered by Russian customers)
<b>AIR-SRVR-PWR=</b>	Field replaceable AC power supply for wireless appliances
<b>AIR-SVR-PWR-DC=</b>	Field replaceable DC Power Supply for 8510DC (AIR-CT85DC-K9)
<b>AIR-SRVR-300GB-HD=</b>	Field replaceable 300GB HD for wireless/management servers

---

## Service and Support

Realize the full business value of your wireless network and mobility services investments faster with intelligent, customized services from Cisco and our partners. Backed by deep networking expertise and a broad ecosystem of partners, Cisco professional and technical services enable you to successfully plan, build, and run your network as a powerful business platform. Our services can help you successfully deploy the Cisco 8500 Series Wireless Controller and integrate mobility solutions effectively to lower the total cost of ownership and secure your wireless network.

To learn more about Cisco Wireless LAN service offers, visit: <http://www.cisco.com/go/wirelesslanservices>.

## Summary

The Cisco 8500 Series Wireless Controllers are designed to support large-scale service provider and large-campus deployments. They simplify deployment and operation of wireless networks, helping to ensure smooth performance, enhance security, and maximize network availability. The Cisco 8500 Series manages all the Cisco access points within campus, service provider, and branch locations, eliminating complexity and providing network administrators with visibility and control of their wireless LANs.

## Cisco Capital

### Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more](#).

## For More Information

For more information about Cisco wireless controllers, contact your local account representative or visit: [http://www.cisco.com/en/US/products/ps6302/Products\\_Sub\\_Category\\_Home.html](http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html).

For more information about the Cisco Unified Wireless Network framework, visit: <http://www.cisco.com/go/unifiedwireless>.



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

**ANEXO C:** Cisco 8500 Prime Infrastructure. Especificaciones de la herramienta utilizada para pruebas y simulaciones.





Data sheet  
Cisco public

# Cisco Prime Infrastructure 3.x

---

# Contents

Overview	3
Cisco Prime Infrastructure highlights	4
Ordering and licensing information	6
Product specifications	6
Technical services	6
Cisco Capital	7

---

## One Management and One Assurance of Enterprise Networks from Campus/Branch to the Data Center

### Overview

Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from a single graphical interface. Cisco Prime Infrastructure provides network administrators a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

To overcome these challenges, IT professionals need a comprehensive solution to manage, visualize, and monitor the network from a single graphical interface. Cisco Prime™ Infrastructure provides lifecycle management, assurance visibility, and troubleshooting capabilities network-wide - from the wireless user in the branch office, across the WAN, and to the data center. In essence, it is One Management and One Assurance, for One Network (Figure 1).

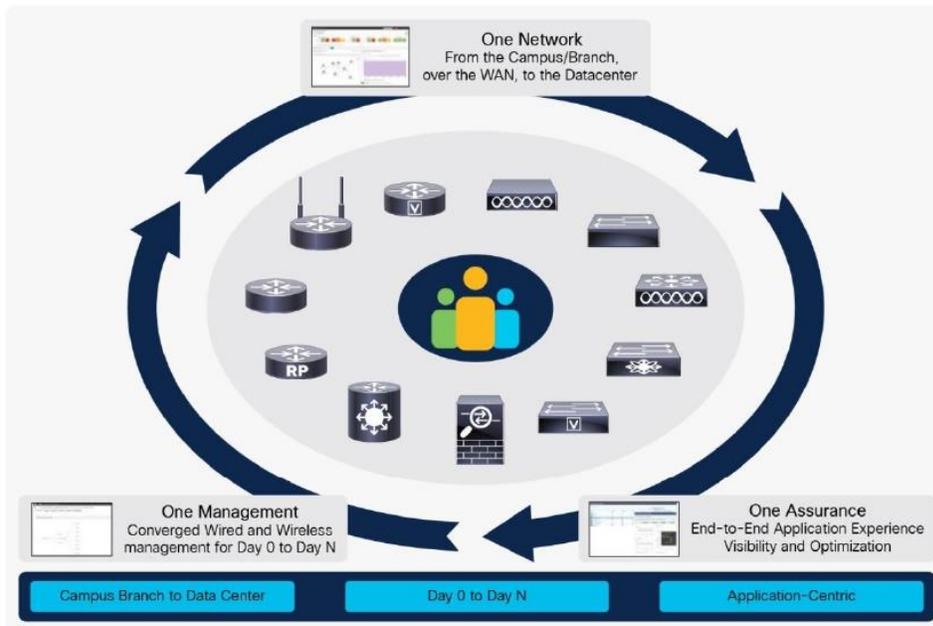


Figure 1.  
Cisco Prime Infrastructure

---

## Cisco Prime Infrastructure highlights

Cisco Prime Infrastructure allows/helps you to manage your network more efficiently and effectively, thereby enabling you to achieve the highest levels of wireless and wired network performance, service assurance, and application-centric end-user experience.

- **Single-pane-of-glass management:** Cisco Prime Infrastructure delivers a single, unified platform for network service provisioning, monitoring and assurance, and change and compliance management. It accelerates the device and services deployment and helps you rapidly resolve problems that can affect the end-user experience. It minimizes the amount of time you spend managing the existing network so you can maximize the time you spend in supporting business growth.
- **Simplified deployment of Cisco® capabilities:** Cisco Prime Infrastructure makes the design and fulfillment of Cisco differentiated features and services fast and efficient. With out-of-the-box support for technologies such as Intelligent WAN (IWAN), Distributed Wireless with Converged Access, Application Visibility and Control (AVC), Zone-Based Firewall, and Cisco TrustSec® 6.4 Identity-Based Networking Services, it helps you get the most from the intelligence built in to your Cisco devices as quickly as possible.
- **Deep Application Visibility:** Cisco Prime Infrastructure configures and uses embedded Cisco instrumentation and industry-leading technologies for application visibility and network policy optimization. These technologies include NetFlow, Network-Based Application Recognition 2 (NBAR2), Simple Network Management Protocol (SNMP), and more. Cisco Prime Infrastructure also triggers the capture, processing, and drill-down into application performance and packet diagnostics data from distributed Cisco Network Analysis Module (NAM) deployments.
- **Comprehensive coverage of enterprise mobility:** Cisco Prime Infrastructure delivers pinpoint visibility into the who, what, when, where, and how of wireless access through its own data collection and key integrations. It includes 802.11ac support; correlated wired-wireless client visibility; unified access infrastructure monitoring; spatial mapping; integrated security and policy application and troubleshooting with [Cisco Identity Services Engine \(ISE\)](#) integration; integrated location-based tracking of interferers, rogues, and Wi-Fi client reporting with [Cisco Mobility Services Engine \(MSE\)](#) and Cisco CleanAir® integration; RF prediction tools; and more.
- **Unified assurance across network and compute:** Cisco Prime Infrastructure delivers scalable management and service assurance across the breadth of enterprise infrastructure in your branch office, campus, and data center networks including network equipment, UCS servers, and virtual machines. The ability to track a user in the branch connecting via a mobile or wired device, all the way to a compute resource in the data center, is essential for fast onboarding, remediation, and troubleshooting.
- **Centralized visibility of distributed networks:** Large or global organizations often distribute network management by domain, region, or country. Cisco Prime Infrastructure Operations Center helps you visualize up to 10 Cisco Prime Infrastructure instances, scaling your network-management capability while maintaining centralized visibility and control.
- **What is new in Prime Infrastructure 3.x?**
  - Cisco Prime Infrastructure 3.x offers new capabilities and a few are highlighted below.

- 
- **Platform Enhancements:**
    - **New User Interface:** Modern user interface with HTML 5.0 (and removal of flash) provides operators with a quick and easy view to isolate issues in the network and identify root cause remediation. The new interface also allows customers to have a superior experience independent of/irrespective of whether they are using a tablet or a traditional PC.
    - **Alarm Customization:** Network operators have the ability to customize alarms based on the operational needs of the enterprise. Customizable syslog-based alarms provide the ability to custom create new alarms and prioritize operator response.
    - **Correlated Performance Graphs:** Correlated charts enable administrators to carry out comparative troubleshooting of network KPIs. The overlay of alarms and configuration change events in the correlated graphs helps connect network change events to performance degradation/improvements.
    - **Configuration Compliance:** With the addition of a compliance engine, the product provides operators the ability to specify the golden network configuration and perform an audit of the network devices against the configuration archive or the device configuration. The audit report identifies devices that are out of compliance. Operators can remediate the devices that are out of compliance with the desired configuration. This engine also helps ingenerating reports for EoL/EoS/PCI for network device and Hardware modules. The CVE, CVSS, and Caveats fields are listed in the PSIRT report/page.
    - **Japanese Localization Support:** Provides alternative UI support in Kanji.
  - **Wireless Management:** Simplified client troubleshooting enables network operators to easily identify the root cause of client issues in a graphical format, speeding up problem identification and resolution. Rogue management and troubleshooting is simplified with enhancements to Switch Port Tracing (SPT) to identify rogue devices on the wire in the network.
  - **Routing - Intelligent WAN (IWAN) management:** Guided workflows based on Cisco Validated Designs and best practices radically simplify deployment and management of Cisco IWAN devices and services. The workflow speeds up provisioning of services such as Dynamic Multipoint VPN (DMVPN) and Performance Routing (PFR) and simplifies Quality-of-Service (QoS) configuration and monitoring. The new PFR monitoring dashboard provides visibility on how application path optimization is working on alternative transport routes and aids troubleshooting of route change events driven by IWAN.
  - **Web Content Accessibility Guidelines (WCAG 2.0):** Runs all the PI 3.x WCAG tests according to the Web Content Accessibility Guidelines 2.0 (<https://www.w3.org/TR/WCAG20/>) checklist.
  - **Cisco DNA Center (Cisco DNAC) Co-Existence:** Objective of the Co-Existence is to enable Prime Infrastructure customers to jump-start with Cisco DNA Center using minimal efforts. To help Migrate Devices, Location Groups, Maps, and CMX Servers from Prime Infrastructure to Cisco DNA Center seamlessly using the workflow. Allow Incremental updates to the migrated dataset and start using Cisco DNA Center Assurance for the migrated sites from Day 1. Refer [Cisco DNA Center and Prime Co-Existence](#) for more details.
  - **Device Support in Wired and Wireless devices:** In Prime Infrastructure it covers almost all categories of network devices on Routing, Switching, IoT device, Wireless device with access points, and Mobility Express Mode. Refer [Cisco Prime Infrastructure 3.6 Supported Devices](#) and [Cisco Wireless Solutions Software Compatibility Matrix](#).

## Ordering and licensing information

For details, refer to the [Cisco Prime Infrastructure 3.x Ordering and Licensing Guide](#). This guide also provides information about obtaining an evaluation copy of Prime Infrastructure 3.x.

## Product specifications

Table 1 provides product specifications for the various virtual and physical appliance deployment options supported by Cisco Prime Infrastructure.

Prime Infrastructure is available on the Prime Infrastructure Physical Appliance and Cisco Digital Network Architecture Center (Cisco DNA Center) Appliance. Prime Infrastructure 3.6 is not supported on the PRIME-NCS-APL-K9 (also known as "Gen 1"). Prime Infrastructure 3.6 is supported on PI-UCS-APL-K9 (also known as the Gen 2 appliance), PI-UCSM5-APL-K9 (also known as Gen 3 appliance – 44 core only for Cisco DNA Center) and DN1-HW-APL (also known as Cisco DNA Center Appliance). You can upgrade a Prime Infrastructure Physical Appliance running Prime Infrastructure 3.4.x or 3.5.x to Prime Infrastructure 3.6. You can upgrade the older versions to 3.4.x or 3.5.x to upgrade to the Prime Infrastructure 3.6.

**Table 1.** Product specifications for Cisco Prime Infrastructure 3.x

VMware	VMware ESXi Version 6.0, 6.5, or 6.7				
<b>Virtual appliance resource requirements</b>	Recommended Virtual Appliance	vCPU (Virtual CPUs)	Memory (DRAM)	Minimum Hard Disk Drive Size **	Disk Input/output Bandwidth
	Express	4	12 GB	300 GB	200 MBps
	Express Plus	8	16 GB	600 GB	200 MBps
	Standard	16	16 GB	900 GB	200 MBps
	Pro	16	24 GB	1200 GB	320 MBps **
<b>Physical appliance specifications</b>	Physical Appliance *	CPU	Memory (DRAM)	Hard Disk Drive Size	Disk Input/output Bandwidth
	(Gen 2) Cisco Prime Appliance *	10 Core Physical CPUs - 20 Threads	64 GB	4 x 900GB RAID10	320 MBps **
	(Gen 3) Cisco Prime Appliance	20 Core Physical CPUs – 40 Threads	64 GB	4x1.2 TB RAID 10	320 MBps **
	Gen 1 Cisco DNA Center Appliance	44 Core Physical CPUs – 88 Threads	256 GB	6 X 1.9 TB; 4 X 2 480 GB	320 MBps **

\* Hard Disk Drive sizes mentioned above are the VM sizes for thick allocation. It is recommended to leave an additional 50% of space free in the data-store of the VM, to allow taking snapshots of the VM when required, as snapshots will take additional space.

\*\* Customers upgrading from PI 2.2 to PI 3.x are recommended to configure Disk I/O Bandwidth to 320 Mbps to minimize performance degradation.

\* Gen-3 Appliance are supported starting Prime Infrastructure 3.5. [End-of-Sale and End-of-Life Announcement for the Cisco Prime Infrastructure HW Gen2 Appliance and 3.1 and 3.2 Software](#).

## Technical services

Cisco Prime Infrastructure 3.x is available with the new Cisco Software Support Service (SWSS), which provides reactive maintenance support in the form of technical support, access to Cisco.com, software support, and access to major and minor

---

upgrades from the Cisco.com software download site during the service contract term. For more information, please refer to the [Cisco Software Support Service](#) description.

The Cisco Prime Appliance option comes with a Cisco go-day hardware warranty. Adding a contract for a technical service offering to your device coverage, such as Cisco SMARTnet<sup>®</sup> Service, provides access to the Cisco TAC and can provide a variety of hardware replacement options to meet critical business needs, updates for licensed operating system software, and registered access to the extensive Cisco.com knowledge base and support tools.

## Cisco Capital

### Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. [Learn more.](#)

For more information about Cisco warranties, visit: <https://www.cisco.com/go/warranty>.

For information about Cisco Technical Services, visit: <https://www.cisco.com/go/ts>.

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

”