PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN REDES DE COMUNICACIÓN

TEMA:

ESTUDIO DE QoS BASADO EN EL ESTÁNDAR IEEE 802.11e Y ALTERNATIVAS DE SEGURIDAD PARA LAS REDES LOCALES INALÁMBRICAS APLICADO EN LA WLAN DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

AUTOR: NARVÁEZ PUPIALES SANDRA KARINA

DIRECTOR: MSC. JUAN FRANCISCO CHAFLA

Quito, Noviembre 2015

PRESENTACIÓN

El presente estudio tiene como objetivo analizar la Calidad de Servicio en redes inalámbricas de área local a través del estándar IEEE 802.11e además de mecanismos de seguridad tomando como caso o referencia la infraestructura de la Universidad Politécnica Estatal del Carchi, en donde la definición de políticas y lineamientos se basan en los requerimientos propios y actuales de la institución.

En el primer capítulo se establecen los antecedentes, justificación, alcance y objetivos proporcionando una visión general y global de las ventajas de aplicar QoS a las WLANs para cubrir las demandas de los usuarios por servicios convergentes acorde al avance del entorno tecnológico pero haciendo hincapié en los riegos y vulnerabilidades presentes en este tipo de redes si no se considera la seguridad como uno de los parámetros principales para alcanzar la calidad.

El segundo capítulo referente al marco teórico en resumen se describe los principios, conceptos de las redes inalámbricas de área local, ventajas, desventajas, el estándar y arquitectura IEEE 802.11, Calidad de Servicio (IEEE 802.11e), herramientas de monitoreo de tráfico, recomendaciones para la formulación de políticas de QoS y finalmente un análisis de la seguridad WLAN tanto para mecanismos de capa 2 como capa 3.

El tercer capítulo corresponde en principio a analizar la situación actual de la red institucional, equipamiento utilizado, distribución y áreas de cobertura de los Puntos de Acceso, estadísticas de tráfico de la WLAN, planteamiento de los requerimientos y termina con la configuración e implementación de Calidad de Servicio y Seguridad además de las pruebas de funcionamiento pertinentes que avalan la mejora de las prestaciones del servicio inalámbrico.

Este estudio culmina en el capítulo cuatro en donde se exponen las conclusiones y recomendaciones obtenidas de la experiencia en función de la investigación y aplicación de los conceptos prácticos y teóricos e invita a los profesionales del área de TICs a considerar la implementación de estos parámetros para mejorar el performance de sus redes inalámbricas en ambientes institucionales sean públicos o privados con garantías de un servicio satisfactorio y exento de peligro gracias al diseño y aplicación de un modelo de seguridad válido para un entorno WLAN.

DEDICATORIA

A mis padres y hermanos por el apoyo incondicional y desmedido en todas las etapas de mi vida que con su ejemplo han forjado en mí los deseos de superación.

Sandra

AGRADECIMIENTO

A DIOS por ser pilar fundamental de mi vida.

A la Pontificia Universidad Católica del Ecuador y en especial a los docentes y compañeros de la maestría en Redes de Comunicación.

A la Universidad Politécnica Estatal del Carchi, por brindarme la apertura y el apoyo en la realización del presente trabajo.

Y de manera muy especial al Msc. Juan Francisco Chafla por su asesoría, orientación y dedicación en el desarrollo y culminación de este gran reto.

RESUMEN

El vertiginoso avance tecnológico en respuesta a los requerimientos incesantes de los usuarios ha promovido la popularización y utilización masiva de las redes inalámbricas de área local tanto en entornos de hogar como en las grandes empresas debido a las ventajas que éstas prestan resaltando entre ellas la movilidad, originando nuevas tendencias como BYOD en donde a través de un dispositivo inalámbrico (Tablets o smartphones) el usuario está en la capacidad de desarrollar sus actividades laborales con absoluta normalidad y disponer de todos los servicios institucionales con las medidas de seguridad pertinentes, siendo esto fruto de una combinación de productos y soluciones tecnológicas como plataformas inalámbricas unificadas, seguridad perimetral, control de acceso y aplicaciones.

Todo este anhelo se cristaliza inicialmente con el levantamiento de una infraestructura inalámbrica de grandes prestaciones en donde a más de contar con un diseño adecuado, planificado y equipamiento robusto se requiere de algo más para poder satisfacer la demanda actual de aplicaciones críticas y en tiempo real y esto es la Calidad de Servicio y Seguridad, que aunque podrían ser ámbitos diferentes éstos parámetros dependen entre sí, ya que sin seguridad no se podría garantizar la calidad.

Inicialmente el estándar que define las WLANs, es decir IEEE 802.11 no consideraba estos dos mecanismos pero a raíz de solventar las necesidades aparecen dos variantes 802.11e y 802.11i para dar fin a los inconvenientes presentados en este tipo de infraestructuras debido a la evolución y convergencia de los servicios. Es por eso que este estudio pretende dar a conocer los lineamientos y recomendaciones para implementar Calidad de Servicio y Seguridad en las redes Wireless tomando como referencia o caso la Universidad Politécnica Estatal del Carchi.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I. GENERALIDADES

1.1 ANTECEDENTES

La tendencia de comunicación cada vez es más exigente, la transmisión de voz, datos, video y nuevas aplicaciones multimedia basadas en IP requieren más recursos a través de las redes, en estos escenarios la movilidad juega un papel sumamente importante con el avance del entorno tecnológico por tal razón las comunicaciones inalámbricas cada vez son más importantes en la cotidianidad de los usuarios debiendo soportar el mismo tráfico que las tradicionales redes cableadas.

En los últimos años la tecnología inalámbrica ha acaparado interés sin precedentes por parte de la industria y principalmente de los beneficiarios por las ventajas que esta tecnología ofrece por ejemplo: los bajos costos de implementación, la interoperabilidad, un marco regulatorio que garantiza su libre uso y sobre todo la movilidad, características que se ven opacadas por la restricción de ancho de banda disponible cuando las aplicaciones transmitidas requieren más recursos, en este esquema es importante la Calidad de Servicio que se preste en la WLAN para garantizar los servicios al usuario final. Además una red inalámbrica presenta varios desafíos de seguridad en contraposición con las redes cableadas y varias de sus facilidades y ventajas se convierten en un verdadero problema cuya consecuencia afecta directamente a la privacidad de la información.

Muchas de las infraestructuras de comunicación en especial las redes inalámbricas locales (WLAN) se diseñan sin planificación ni proyección y peor aun teniendo en cuenta los criterios de Calidad de Servicio y Seguridad, en muchos de los casos implementaciones de este tipo funcionan inicialmente pero conforme se expande la red y se incrementa el número de usuarios se presentan inconvenientes como: pérdida de conectividad, saturación, zonas sin cobertura y sobre todo vulnerabilidades que son explotadas y aprovechadas por individuos malintencionados.

Particularmente la Universidad Politécnica Estatal del Carchi cuenta con una infraestructura tecnológica de última generación en cuanto a red inalámbrica se refiere y se evidencia claramente la necesidad de mejorar el servicio, puesto que el diseño lógico de la red y la configuración de los equipos tienen una planificación sencilla y sin proyección, por tal razón es primordial evaluar los parámetros de Calidad de Servicio basándose en el estándar IEEE 802.11e y las alternativas de seguridad para garantizar el acceso y disponibilidad de los recursos de la WLAN a los usuarios legítimos.

1.2 JUSTIFICACIÓN E IMPORTANCIA

Las aplicaciones y la concurrencia de los usuarios en la WLAN actualmente provocan que los recursos sean totalmente consumidos y la mayoría de veces sin garantías del servicio, haciéndose de esta forma indispensable la provisión de QoS en este tipo de redes.

Con la utilización del estándar IEEE 802.11e los Puntos de Acceso priorizan el tráfico, es decir que se da un tratamiento especial a cada tipo de información clasificándola básicamente en 4 tipos que son: Background, BestEffort, Video y Voice de esta manera se asegura la transmisión del tráfico con mayor relevancia a nivel de capa 2, en cuanto a capa 3 con la implementación de DiffServ se garantiza el servicio extremo a extremo.

La seguridad en una red inalámbrica es de vital importancia ya que a diferencia de las redes cableadas el acceso al medio de transmisión está disponible para todos solo habría de necesitar herramientas y tiempo para participar en una conexión como usuario legítimo. Existen algunos mecanismos de seguridad a nivel de capa 2 o nivel de enlace como las tecnologías de cifrado WEP, WPA/WPA2 y técnicas de filtrado MAC entre otras. Actualmente soluciones más viables y muy utilizadas como la autenticación permiten la validación de las transmisiones entre puntos de acceso y estaciones inalámbricas a nivel de capas superiores con la utilización de un portal cautivo que permite al usuario identificarse para acceder al recurso de la red inalámbrica.

A través de este estudio se evaluaran los parámetros de QoS de tal forma que permita eliminar las falencias existentes y se aproveche al máximo la infraestructura inalámbrica de la Universidad Politécnica Estatal del Carchi además del análisis de la mejor alternativa de seguridad que se adapte a las necesidades de la institución de esta forma fortaleciendo tecnológicamente al personal tanto administrativo, docente y estudiantil.

1.3 ALCANCE

El presente trabajo tiene como finalidad realizar un estudio del estado del arte de la Calidad de Servicio en base al estándar IEEE 802.11e ,estándar definido para cubrir la necesidad de QoS en redes inalámbricas además del análisis de las alternativas de seguridad que se ajusten a las necesidades y requerimientos actuales.

Específicamente este estudio se aplicará a la WLAN de la Universidad Politécnica Estatal del Carchi que requiere la mejora y garantía de los servicios ya que el incremento del tráfico y usuarios exige dar un tratamiento especial a las aplicaciones además este ambiente permitirá evaluar experimentalmente los parámetros de QoS (retardo, pérdida de paquetes, ancho de banda, latencia y jitter).

Se realizará una evaluación inicial de la red inalámbrica por medio de una auditoría a través de software informático de las aplicaciones que cursan por la WLAN, para de esta forma priorizar las clases de tráfico para la aplicación de QoS. Adicionalmente con esta información se determinará el ancho de banda que requerirá cada clase de tráfico y cada uno de los rangos aceptables de los parámetros de QoS.

Cabe señalar la definición de políticas tanto para Calidad de Servicio como de la Seguridad en la red como por ejemplo: qué tipos de tráfico tienen más prioridad que otros y las políticas de acceso a la red por parte de los usuarios inalámbricos y finalmente se realizará las pruebas de funcionamiento tras aplicar QoS y seguridad en la WLAN de la UPEC.

1.4 OBJETIVOS

1.4.1 *Objetivo General*

Evaluar la Calidad de Servicio en las redes inalámbricas partiendo del estándar IEEE 802.11e y alternativas de seguridad que permitan mejorar y garantizar el servicio en este tipo de infraestructuras.

1.4.2 *Objetivos Específicos*

- Analizar el estado del arte respecto al estándar IEEE 802.11e y técnicas de seguridad para las redes inalámbricas.

- Determinar los parámetros de QoS y requerimientos de seguridad indispensables en las redes WLAN.

- Aplicar QoS y seguridad en la WLAN de la UPEC acorde a los requerimientos de la institución tras el monitoreo de la red con la ayuda de software para verificar el tráfico y su comportamiento con la finalidad de definir las políticas a implementar.

- Realizar las pruebas de funcionamiento para verificar la disponibilidad y garantía del servicio de la red Inalámbrica con QoS y seguridad.

1.5 METODOLOGÍA

La Metodología para el desarrollo del presente proyecto es a través de procedimientos inductivos y experimentales que permiten estudiar a fondo el mecanismo y parámetros de QoS para redes inalámbricas teniendo en cuenta una característica fundamental que es la seguridad por tal razón se evaluarán alternativas para aplicar la más adecuada al caso de estudio que es la Universidad Politécnica Estatal del Carchi.

La tecnología que se va a evaluar para QoS a nivel de capa 2 está definida por el estándar IEEE 802.11e, la cual se considera de suma importancia porque permite la priorización de flujos de tráfico entre aplicaciones y terminales. Además el tráfico de voz y video se verá beneficiado por que puede ser tratado con mayor prioridad que otros tipos de tráfico. Para determinar el comportamiento actual de la red se utilizará el software NTOP que facilita una visión de las aplicaciones utilizadas por los clientes, así como verificar la cantidad de tráfico que genera cada una de estas. Finalmente con las observaciones y la información recolectada de la red se aplica QoS y seguridad.

CAPÍTULO II. MARCO TEÓRICO

2.1 REDES LOCALES INALÁMBRICAS (WLAN)

2.1.1 *Introducción a las WLAN*

En la actualidad uno de los mecanismos de comunicación más utilizados y en crecimiento son las redes inalámbricas de área local o WLAN, por tal razón existen diversidad de dispositivos a nivel de usuario en esta modalidad que facilitan la comunicación convirtiéndose así en un complemento importante de las redes LAN (Local Area Network) cuyos beneficios a más de cubrir lugares de difícil acceso permiten la movilidad a costos más asequibles.

Las WLAN tienen su origen hacia finales de los años 70 cuando ingenieros de IBM experimentaron transmisión con enlaces infrarrojos para la red local de una fábrica, posteriormente se utilizaron las microondas y en el año de 1985 la FCC (Federal Communications Comission) asigna un grupo de bandas de uso libre ISM (Industrial, Scientific and Medical) que propició el desarrollo comercial de las redes inalámbricas de área local. Hoy en día este esquema de comunicación tiene su protocolo estándar que es el IEEE[1] 802.11, a medida que el entorno tecnológico evoluciona y las necesidades de ancho de banda y cobertura crecen el estándar proporciona las variantes que se ajustan a estos requerimientos.

2.1.1.1 Definición de WLAN

Una WLAN es un sistema de comunicación que utiliza como medio físico de transmisión las ondas electromagnéticas en las bandas de frecuencia libres de 2,4 y 5Ghz permitiendo todas las funcionalidades y beneficios de las tradicionales LAN facilitando la movilidad de los usuarios y dispositivos sin la necesidad de conexiones cableadas.

[1] **IEEE** Institute of Electrical and Electronics Engineers

2.1.2 *Ventajas y Desventajas de las WLAN*

A continuación se describen las principales ventajas de las WLAN:

- Ofrecen movilidad permitiendo a los usuarios acceder a la información en cualquier lugar dentro de la organización.

- Escalabilidad ya que son fáciles de expandirse posteriormente a su instalación.

- Proveen conectividad en puntos o áreas donde difícilmente se puede cablear con tiempos de instalación más cortos y con la posibilidad de la reubicación de los terminales en caso de ser necesario.

- Existe un marco regulatorio que garantiza su uso libre.

- Son interoperables entre marcas que están reguladas por la Wi-fi Alliance.

En contrapartida a las ventajas se tienen las siguientes desventajas:

- Las velocidad de transmisión aún están por debajo a las brindadas por las redes cableadas pese a la existencia de un nuevo estándar IEEE 802.11 ac que propone una velocidad de transmisión real de 866 Mbps y teórica de 1,3 Gbps que no necesariamente se cumple en ambientes ideales.

- El espectro utilizado por las WLANs también es utilizado por otros dispositivos como los hornos microondas, teléfonos inalámbricos y dispositivos Bluetooth lo cual causa interferencia y saturación.

- Quizá una de los inconvenientes más grandes es la inseguridad ya que el acceso al medio de transmisión está totalmente disponible y bastaría con hacer uso de herramientas para

participar en una conexión legítima si no se ha tomado adecuadamente las medidas preventivas para el caso.

Pese a la existencia de estas desventajas las redes WLAN han tenido en los últimos años una gran aceptación por parte de los usuarios y fabricantes que han visto en esta tecnología una oportunidad comercial, con las nuevas mejoras al estándar IEEE 802.11 se espera que en los próximos años permitan velocidades de transmisión muy altas con la finalidad de cubrir las necesidades de comunicación más exigentes.

2.1.3 *Wi-Fi Alliance*

En 1991 compañías como Lucent, Nokia, 3Com, Cisco entre otras crearon una asociación conocida como WECA (Wireless Ethernet Compatibility) cuyo nombre fue sustituido por Wi-Fi Alliance posteriormente, su objetivo fundamental es establecer estándares para que los dispositivos WLAN sean compatibles bajo IEEE 802.11 con la marca registrada Wi-Fi. En la Figura 1 se muestra el logotipo que utilizan los fabricantes para certificar que sus productos son interoperables con otros.

Figura 1. Wi-Fi Alliance

Fuente: http://en.wikipedia.org/wiki/Wi-Fi_Alliance

Recientemente se creó la WiGig (Wireless Gigabit Alliance) en cooperación con la Wi-Fi Alliance para el crecimiento y expansión de las tecnologías inalámbricas a velocidades multi-gigabit bajo el estándar IEEE 802.11ad, de esta forma los usuarios podrán disfrutar de aplicaciones interactivas y multimedia en tiempo real utilizando el espectro de 60Ghz con lo

que se garantizaría la transmisión de grandes volúmenes de información. En la Figura 2 se presenta el logo de WiGig.

Figura 2. Wireless Gigabit Alliance (WiGig)

Fuente: http://en.wikipedia.org/wiki/Wireless_Gigabit_Alliance

2.1.4 *Arquitectura WLAN*

"La tecnología WLAN puede tomar el lugar de una red cableada tradicional o extender sus capacidades. De manera muy similar a sus contrapartes cableadas, el equipamiento WLAN consiste en adaptadores clientes y Access Points, que llevan a cabo funciones similares a las de los Hubs de networking cableado" (Cisco, 2006).

Según Cisco (2006), se puede disponer de una topología punto-punto también conocida como Ad- Hoc con la utilización solamente de los adaptadores de cliente para el caso de instalaciones provisionales y pequeñas, mientras que si se requiere de mayor funcionalidad y prestaciones se incorporan los Access Points de forma que trabajan en topología estrella y se la conoce con el nombre de red inalámbrica de infraestructura. En la Figura 3 se presenta un esquema de Red Ad-Hoc y una red inalámbrica con Access Point.

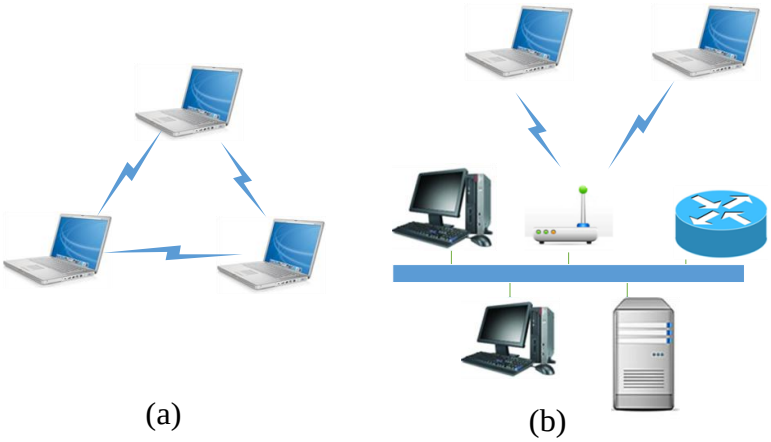


Figura 3. (a) Red Ad-Hoc. (b) Red inalámbrica con AP

Fuente: Propia

También existen otras configuraciones dentro de un ambiente WLAN como por ejemplo en ocasiones se requiere amplificar la señal para extender el área de cobertura, en este caso la configuración del Access Point requiere el modo de trabajo "Repetidor". Además es posible la interconexión entre segmentos de red remotos como la conectividad entre edificios distantes que pertenecen al mismo campus u organización, en este aspecto el modo de trabajo de los Puntos de Acceso constituye una configuración en modo Bridge ya sea punto a punto o punto a multipunto (véase la Figura 4).

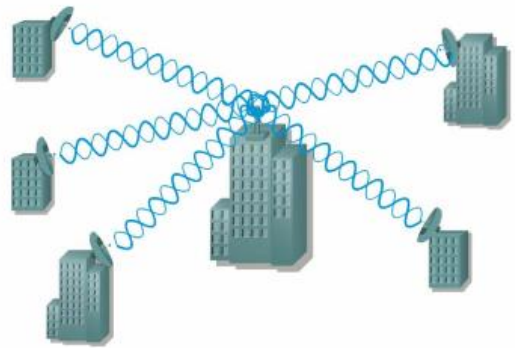


Figura 4. Access Points en modo de trabajo Bridge

Fuente: (Cisco, 2006)

Otra alternativa actualmente son las redes MESH (redes malladas) que combinan las topología Ad-Hoc e infraestructura en la que los Puntos de Acceso pueden cumplir dos funciones que son: establecer el backbone inalámbrico a 5Ghz (backhaul) y el rol de dar conectividad a los usuarios en las dos bandas (2,4 y 5Ghz) lo que no ocurre con las topología Bridge.

Cabe recalcar que en las arquitecturas Mesh los Puntos de Acceso cumplen con dos funciones y para lo cual están dotados del hardware y software necesario para trabajar en modo dual band (doble banda) que ha permitido no solamente la expansión de las WLAN en campus y organizaciones sino ampliar la cobertura a ambientes metropolitanos. En la Figura 5 se presenta un despliegue de arquitectura Mesh del fabricante Cisco.

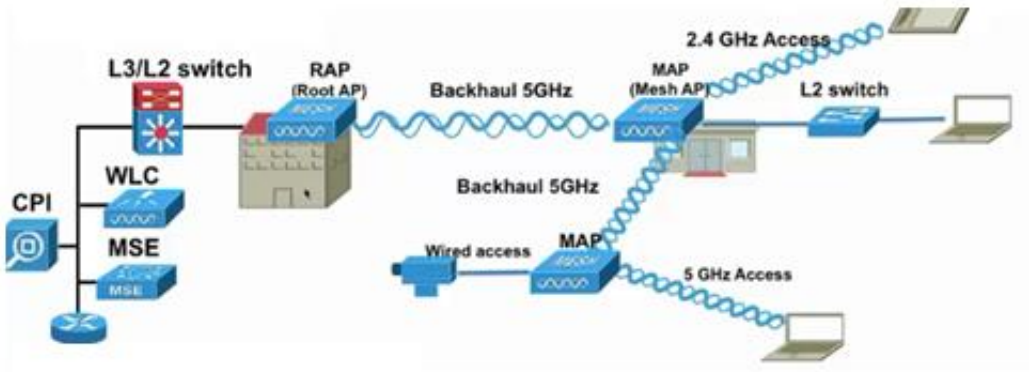


Figura 5. Despliegue de una red MESH

Fuente: (Cisco Live, 2014)

2.1.5 *Estándar IEEE 802.11 y sus variantes*

En Cisco (2006) se afirma que antes de existir los estándares para los sistemas inalámbricos los productos y soluciones eran incompatibles y ofrecían velocidades de datos muy bajas con costos muy elevados.

A raíz de la normalización de las redes inalámbricas de área local se obtuvo las siguientes ventajas: interoperabilidad con los diferentes productos de los diversos fabricantes, estabilidad, mayores velocidades y reducción de costos de esta tecnología.

El IEEE, es una asociación a nivel mundial sin ánimo de lucro creada en el año de 1884 con el afán de normalizar y estandarizar las nuevas tendencias tecnológicas con alrededor de 400 000 miembros en las diferentes áreas de la ingeniería como: Electricidad, Electrónica, Computación, Matemáticas, Biomedicina, Telecomunicación entre otras. En el ámbito del Networking ha desarrollado muchos estándares entre ellos el IEEE.802 tanto para redes de área local (LAN), redes de área amplia (WAN) y redes de área metropolitana (MAN), principalmente enfocado a las dos capas inferiores del modelo de referencia OSI (Open System Interconnection).

En cuanto a la estandarización de las redes inalámbricas de área local se maneja el IEEE 802.11 publicado en 1997 que define el uso de la capa Física y Enlace de Datos para el correcto funcionamiento de una WLAN.

A continuación se describe cada una de las variantes IEEE 802.11:

- **802.11 Legacy:** Es el estándar original que como ya se mencionó anteriormente fue publicado en el año de 1997 y ratifica velocidades de transmisión de 1 y 2 Mbps a frecuencias de 2,4Ghz (IR), incluyendo además la definición del protocolo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) con las técnicas de modulación FHSS (Frequency Hopping Spread Spectrum) y DSSS (Direct Sequence Spread Spectrum).

- **802.11a:** Esta revisión fue publicada en el año de 1999 operando en la banda de 5Ghz con velocidades de transmisión de 6 a 54Mbps usando como técnica de modulación OFDM (Orthogonal Frequency Division Multiplexing). Tiene como ventaja utilizar una banda no saturada pero a mayor frecuencia que implica menor alcance sumada la incompatibilidad con IEEE 802.11b.

- **802.11b:** Es una extensión del *IEEE 802.11 Legacy* que opera en la banda 2,4Ghz con velocidades de transmisión de 5,5 a 11Mbps, utiliza también el método CSMA/CA y modulación DSSS.

- **802.11c:** Esta revisión especifica los métodos necesarios para la interconexión de redes WLAN de diferentes tipos como por ejemplo las topologías tipo bridge, estos mecanismos ya han sido incluidos como parte del IEEE 802.11d.

- **802.11d:** Complemento a IEEE 802.11 en el que se establecen los procedimientos para permitir la operación internacional de las redes WLAN, de esta forma los dispositivos que cumplen con esta normativa pueden operar de acuerdo a las regulaciones del país incluyendo parámetros como el nombre del país y los canales disponibles.

- **802.11e:** Constituye una propuesta publicada en el 2005 que define los mecanismos necesarios para proporcionar QoS a las aplicaciones en tiempo real (voz y video) manteniendo compatibilidad con IEEE 802.11a y 802.11b con la definición de cuatro categorías de acceso al medio: Voice, Video, Background y Best Effort.

- **802.11f:** Esta especificación proporciona comunicación entre puntos de acceso inalámbricos de diferentes proveedores, es decir permite garantizar la interoperabilidad mediante el protocolo IAPP (Inter-Access Point Protocol) que faculta a los usuarios cambiarse de un punto de acceso a otro mientras está en movimiento sin la necesidad de mantener una misma marca de dispositivos, este mecanismos lleva el nombre de itinerancia o roaming.

- **802.11g:** Publicada en el año 2003, es una evolución del estándar IEEE 802.11b que utiliza la misma banda de frecuencia 2,4Ghz pero con la diferencia de operar con velocidades de transmisión mayores de 20 a 54 Mbps con técnicas de modulación DSSS y OFDM.

- **802.11h:** Constituye una modificación al estándar IEEE 802.11 que resuelve los inconvenientes de coexistencia con sistemas satelitales y de radar de las WLAN 802.11a que incorpora ciertas recomendaciones de la ITU (International Telecomunications Union) sugeridas por la oficina Europea de Radiocomunicaciones (ERO) dando como

resultado la capacidad de gestionar de forma dinámica la frecuencia (DFS) y potencia de transmisión (TPC) de los dispositivos inalámbricos.

- **802.11i:** Ratificado en el año 2004 abarca los mecanismos para combatir la vulnerabilidad de las redes inalámbricas de área local con los protocolos 802.1x[2], TKIP (Temporary Key Integrity Protocol), AES (Advanced Encryption Standard) en WPA2 (Wi-Fi Protected Access 2) robusteciendo de esta manera la autenticación de los usuarios así como el cifrado de la información.

- **802.11j:** Especificación japonesa equivalente a IEEE 802.11h que opera en las bandas de 4,9 a 5Ghz.

- **802.11k:** El objetivo de esta variante es gestionar eficientemente los recursos de radiofrecuencia en un entorno WLAN, para esto el Punto de Acceso tiene la funcionalidad de descubrimiento de los siguientes parámetros: Puntos de Acceso vecinos, distancia a la que se encuentran los usuarios que están conectados a los Puntos de Acceso vecinos y la carga de tráfico de los AP vecinos. Para ser implementados en los dispositivos solamente se requiere de una actualización de software.

- **802.11m:** Constituye el mantenimiento del estándar 802.11 y tiene las siguientes enmiendas: ma (publicada en el 2007), mb (publicada en el 2012) y mc (marzo 2015).

- **802.11n:** Ratificado en el año 2009, permite alcanzar velocidades superiores a las de 802.11g al hacer uso de varias antenas de transmisión y recepción para el envío de flujos de datos (data streams) simultáneamente, tecnología conocida como MIMO (Multiple-Input Multiple-Output) véase Figura 6. Dependiendo del número de flujos de datos transmitidos se puede alcanzar velocidades de 300, 450 o 600Mbps. Esta especificación es compatible con IEEE 802.11a/b/g por lo que opera en las bandas de 2,4 y 5Ghz con anchos de banda de canal de 20 y 40Mhz.

[2] **802.1x** Sistema de autenticación de usuario para el acceso a la red LAN o WLAN

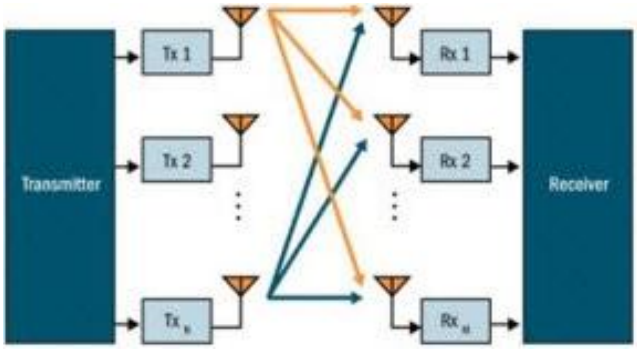


Figura 6. Tecnología MIMO

Fuente: (Moresco, 2012)

- **802.11p:** A través de modificaciones en la capa MAC se permite el desempeño en entornos vehiculares operando en el espectro de frecuencias de los 5Ghz, es conocida también con el nombre de WAVE (Wireless Access Vehicular Environment).

- **802.11r:** Conocida como Fast Transition Roaming proporciona los mecanismos necesarios para que la transición de un usuario a otro Punto de Acceso sea muy rápido al mismo tiempo evitando fallos de conexión y pérdidas de paquetes convirtiéndose así en una característica primordial para aplicaciones en tiempo real. Este tiempo de traspaso (hand-off) se da por el proceso de re-autenticación cada vez que un usuario nuevo intenta conectarse con un AP.

- **802.11s:** Esta especificación define el procedimiento que utilizan los dispositivos inalámbricos para conectarse y trabajar en un ambiente de red mallada o conocidas como redes Mesh.

- **802.11T:** Son las prácticas recomendadas para evaluar y medir el rendimiento en las redes inalámbrica de área local, también conocido como WPP (Wireless Performance Prediction).

- **802.11u:** Publicada en el año 2011 define los mecanismos para mejorar la interconexión con redes externas no 802.11 por medio de la detección y selección de redes además de la correspondencia de Calidad de Servicio DSCP (Differentiated Services Code Point) con las prioridades de capa 2 de las WLAN. Con estas capacidades por ejemplo es posible que un Access Point desempeñe la función de "relay" para el reenvío de una consulta de un usuario a un servidor de autenticación además de garantizar QoS de extremo a extremo.

- **802.11v:** Proporciona la configuración en red de los dispositivos clientes permitiendo la gestión centralizada utilizando mecanismos de capa 2, de esta forma es posible la supervisión, actualización, intercambio de información de la topología de red incluyendo información sobre el entorno RF.

- **802.11w**: Publicado en el año 2009 con la finalidad de brindar seguridad a las tramas de gestión, extendiendo la protección que aporta 802.11i (seguridad en las tramas de datos), de esta forma se concibe asegurar las principales operaciones de una red inalámbrica.

- **802.11y:** Esta variante define la operación y utilización de la banda de 3650 – 3700 Mhz, desarrollada especialmente para los Estados Unidos basándose en la 802.11a, la utilización de estas frecuencias requiere el pago de una mínima tarifa por una licencia a nivel nacional además de una tarifa nominal por el despliegue de cada estación base de alta potencia que son registradas en una base de datos de la FCC.

- **802.11z:** Enmienda publicada en el año 2010, constituye una mejora a DLS (Direct Link Setup) que define el mecanismo para transmitir datos directamente entre dos estaciones clientes que pertenecen a la misma WLAN al mismo tiempo que estos clientes siguen asociados con el Punto de Acceso con la finalidad de reducir la cantidad de tráfico que se transmite en la red evitando la congestión en los Puntos de Acceso. TDLS (Tunneled Direct Link Setup) permite el envío de contenido multimedia y otros datos de manera sencilla, segura y muy rápida facilitando la transferencia de contenido entre smartphones, tablets, televisores, cámaras o cualquier otro dispositivo de la red.

A continuación se presentan las variantes IEEE 802.11 más recientes y su ámbito de aplicación:

- **802.11aa:** Especifica mejoras en el control de acceso al medio (MAC) con la finalidad de dar soporte robusto a la transmisión de voz y audio, manteniendo al mismo tiempo la convivencia con otros tipos de tráfico.

- **802.11ac:** Publicada en diciembre de 2012 es una propuesta mejorada de 802.11n, con tasas de transmisión teóricas de 1,3 Gbps y radio de cobertura más amplio, utiliza la banda de 5Ghz ofreciendo más canales sin la molestosa interferencia. Además se amplía el ancho de banda hasta de 160Mhz y 8 flujos MIMO con modulación de alta densidad 256 QAM (Quadrature Amplitude Modulation).

- **802.11ad:** Conocida también con el nombre de WiGig fue publicada en el año 2012, constituye una serie de modificaciones en la capa física (PHY) y en la capa (MAC) para permitir la operación en la banda de los 60Ghz con velocidades de transmisión superiores a 1Gbps con el objeto de brindar a los usuarios aplicaciones multimedia y en tiempo real a través de comunicaciones directas, de corto alcance y gran rendimiento.

- **802.11ae:** Provee un mecanismo para la priorización de las tramas de gestión (QoS) con la finalidad de mejorar el rendimiento de una WLAN.

- **802.11af:** Conocida también con el nombre de White-Fi, permite la operación y utilización de las bandas VHF y UHF (54 y 790 Mhz) del espectro de TV no utilizadas con el uso de una base de datos de geolocalización autorizado que proporciona información sobre qué frecuencia, en qué momento y en qué condiciones se puede operar.

- **802.11ah:** Permite el servicio inalámbrico en bandas de frecuencia por debajo de 1Ghz (ISM), para posibilitar esta operación se requieren modificaciones tanto en la capa PHY como MAC con la finalidad de promover tecnologías como el Internet de las cosas (IoT), las comunicaciones M2M (Machine to Machine), redes de sensores a gran escala con un

importante ahorro energético, con mayor alcance y bajas tasas de transmisión específicamente para mensajes de datos pequeños y poco frecuentes.

- **802.11ai:** Esta variante de 802.11 proporciona el mecanismo Fast Initial Link Setup para lograr una configuración de enlace seguro entre una estación cliente STA y un Punto de Acceso en menos de 100ms para los servicios en tiempo real.

- **802.11aj:** Especifica las modificaciones en la capa PHY y MAC de 802.11ad para permitir la operación en la banda de 45Ghz, espectro disponible en algunas regiones del mundo como por ejemplo China.

- **802.11ak:** Enmienda conocida también con el nombre de General Links cuyo propósito es mejorar los enlaces 802.11 para el transporte en redes con topología bridge incluyendo 802.1Q garantizando QoS a través del mapeado de calidad de servicio en redes 802.11 y 802.3.

- **802.11aq:** Permitirá pre-asociación para el descubrimiento de servicios ofrecidos en la red por medio de mecanismos para anunciar la existencia de los mismos y entregar información que los describe con la finalidad conocer su disponibilidad antes de la asociación de las estaciones.

- **802.11ax:** Variante sucesora de 802.11ac cuyo objetivo es aumentar la eficiencia en las redes WLAN hasta de cuatro veces tomando en cuenta el ahorro energético además de mantener la compatibilidad y la convivencia con versiones anteriores.

- **802.11ay:** Extensión de 802.11ad con el propósito de ampliar el rendimiento, alcance y velocidad hasta de 100Gbps en el espectro de 60Ghz con un esquema de modulación muy alta y tecnología MIMO.

2.1.6 *Arquitectura 802.11*

La Arquitectura IEEE 802.11 define los mecanismos necesarios para la conectividad inalámbrica dentro de una red de área local en los niveles más bajos del modelo de referencia OSI (Capa Física y Capa de Enlace de Datos), precisamente a nivel de la capa Enlace de Datos se especifica la estructura y operación de la subcapa MAC usando además la subcapa LLC ya establecida en IEEE 802.2, véase la Figura 7.

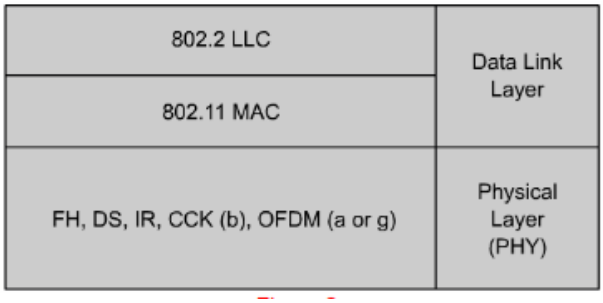


Figura 7. Capa Física y Enlace de Datos en IEEE 802.11

Fuente: (Cisco, 2006)

2.1.6.1 Descripción general de los componentes de la Arquitectura IEEE 802.11

"La arquitectura IEEE 802.11 consiste en varios componentes que interactúan para proporcionar conectividad inalámbrica. Estos componentes pueden soportar movilidad entre estaciones transparentes para las capas superiores" (Cisco, 2006, p. 43).

- ***BSS (Basic Service Set):*** Conjunto de estaciones que compiten por el acceso al medio inalámbrico incluyendo un componente llamado Punto de Acceso al que se conectan las estaciones, un BSS abarca un área RF o celda de cobertura además tiene un único ID de conjunto de servicios (SSID), en la Figura 8 a continuación se ilustran dos Basic Service Set.

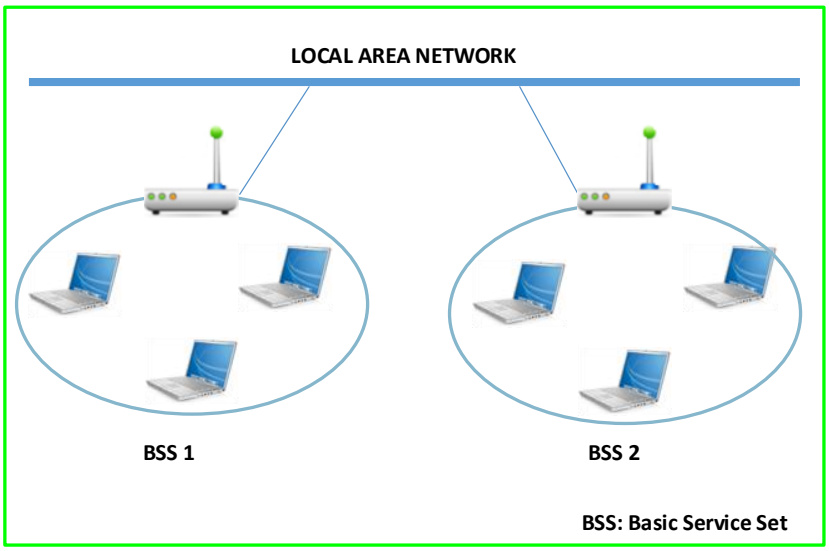


Figura 8. Basic Service Set

Fuente: Propia

- ***AP (Access Point):*** Es un dispositivo que contiene un transceptor de radio, funciona como un bridge o un punto de reenvío y puede actuar como un punto central de una red inalámbrica o como punto de conexión entre redes inalámbricas y redes cableadas. Un AP puede operar de las siguientes maneras:

    - *Modo Root:* el mecanismo más común en donde varios usuarios comparten el mismo punto de acceso.
    - *Modo Bridge:* el AP está configurado solamente para engancharse a otro punto de acceso con la finalidad de establecer un enlace punto a punto inalámbrico.
    - *Modo Repeater:* cuando se requiere extender las señal más allá de la cobertura actual.
    - *Modo Monitor:* en este modo el AP puede escuchar el tráfico de un canal pasivamente con el objeto de verificar problemas en la red inalámbrica, uso del canal o simplemente razones de mantenimiento y seguridad.

En la Figura 9 se presenta un AP Cisco Aironet 3702e, con soporte dual band (2,4 y 5Ghz) y funcionalidad IEEE 802.11ac.

Figura 9. Access Point Cisco Aironet 3702e

Fuente: http://www.cisco.com/c/en/us/products/wireless/index.html

- **DS (Distribution System):** es el medio que interconecta varios Conjuntos Básicos de Servicios (BSS), puede ser cableado o inalámbrico posibilitando enviar una trama MAC de una estación en un BSS1 a otra estación (remota) en otro BSS2, véase la Figura 10.

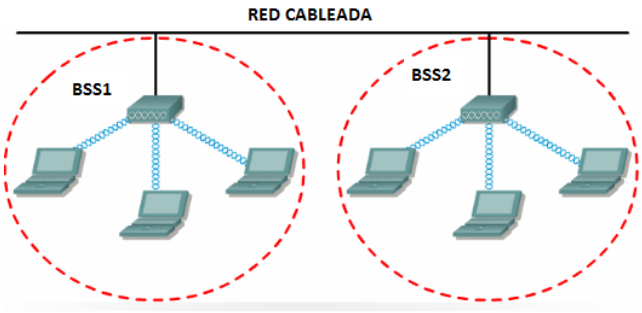


Figura 10. Distribution System

Fuente: (Cisco, 2006)

- **ESS (Extended Service Set):** Dos o más BSS conectados por un Distribution System, permite crear entornos inalámbricos amplios y complejos (Figura 11). Es posible que dos BSS se solapen pero sólo en términos de su área de cobertura pero con configuración de canal que no produzca interferencia.

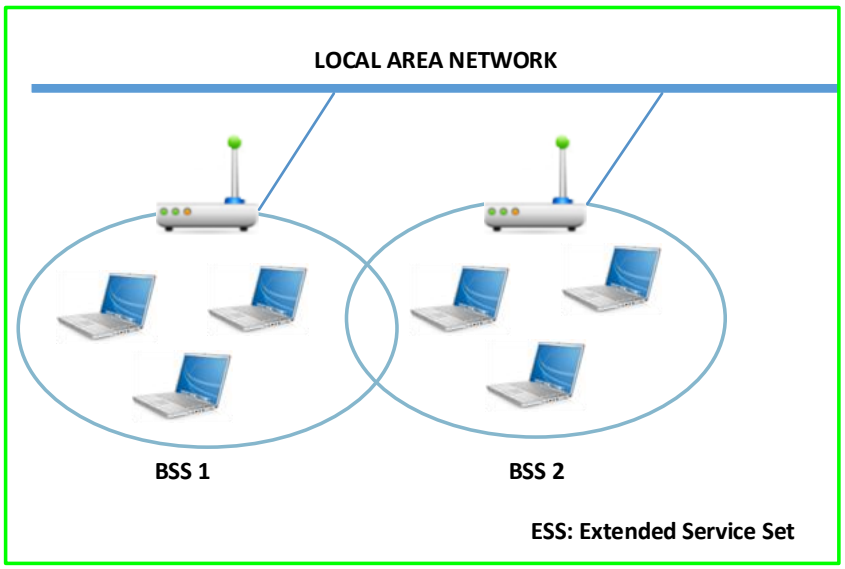


Figura 11. Extended Service Set

Fuente: Propia

- **IBSS (Independent Basis Service Set):** Es el modo de operación más básico en IEEE 802.11 y consiste en la comunicación directa de dos o más estaciones que usan el medio inalámbrico sin un Sistema de Distribución (DS), es decir una red Ad-Hoc.

- **STA (Station):** Una estación es un cliente wireless que se comunica con un Punto de Acceso u otra estación y poseen generalmente una sola tarjeta de red inalámbrica capaz de interpretar IEEE 802.11, estos dispositivos pueden ser laptos, smartphones, tablets e inclusive ordenadores de escritorios a los cuales se les puede incorporar una NIC (Network Interface Card) inalámbrica.

- **Roaming (Itinerancia):** Es una característica tanto de la red inalámbrica como de una estación para que pueda desplazarse por un ESS, es decir de una celda a otra o de un BSS a otro sin perder la conectividad a la red a través de un proceso de re-asociación que tiene lugar cuando una estación (STA) pierde intensidad de señal de un AP pero presencia intensidad de señal de otro más cercano tal como se muestra en la Figura 12.

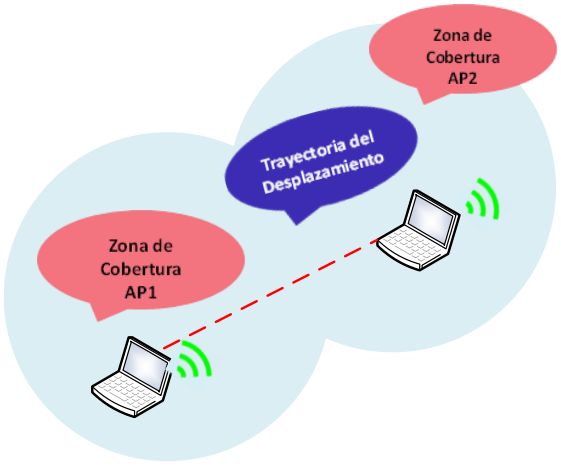


Figura 12. Itinerancia en Redes Inalámbricas de Área Local

Fuente: Propia

2.1.6.2 Servicios de la Arquitectura IEEE 802.11

El estándar IEEE 802.11 no limita la tecnología ni la utilización de un DS centralizado o distribuido, pero sí especifica los servicios. Existen dos tipos de servicios utilizados por la subcapa MAC: Servicio de Estación (SS) y Servicio del Sistema de Distribución (DSS).

Los Servicios de Estación (SS) son proporcionados por las estaciones (incluidos Puntos de Acceso y Puntos de Acceso con funcionalidad STA) y los servicios del Sistema de Distribución (DSS) pertenecen al Distribution System (DS), en la Figura 13 se resaltan estos dos tipos de servicios proporcionados por la arquitectura IEEE 802.11.

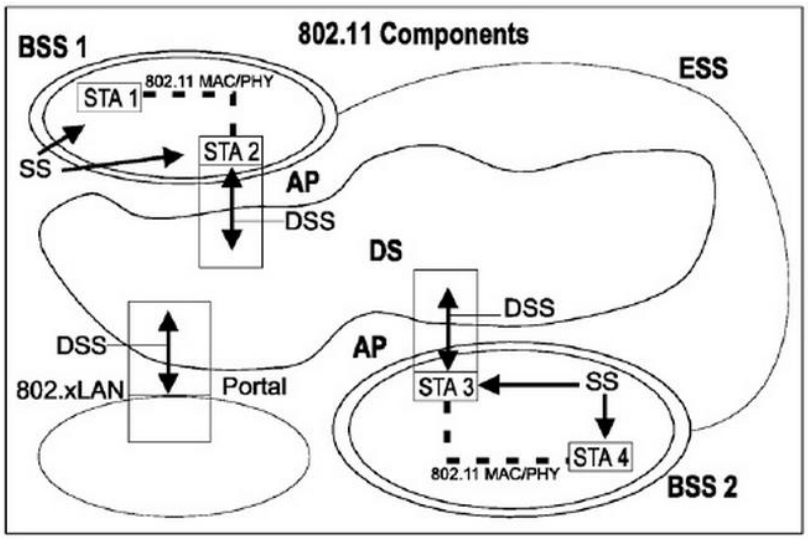


Figura 13. Servicios de la Arquitectura IEEE 802.11

Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012)

A continuación en la Tabla 1 se presentan los servicios en conjunto tanto para SS y DSS:

SS (Station Service)	DSS (Distribution System Service)
Authentication	Association
Deauthentication	Disassociation
Data Confidentiality	Distribution
MSDU Delivery	Integration
DFS	Reassociation
TPC	QoS Traffic Scheduling
Higher layer timer synchronization	Interworking with DS
QoS Traffic Scheduling	
Radio Measurement	

Tabla 1. Conjunto de Servicios de la Arquitectura IEEE 802.11

Fuente: Propia

2.1.6.3 Descripción de los Servicios de IEEE 802.11

Independientemente de su pertenencia a servicios de Estación o a servicios del Sistema de Distribución existen grupos con funcionalidades específicas: Seis de los servicios se utilizan para el soporte en la entrega de MSDU (MAC Service Data Unit) entre estaciones, tres de los servicios para controlar el acceso y confidencialidad de la WLAN, dos de los servicios para gestionar el espectro, uno para prestar apoyo a las aplicaciones LAN con los requisitos de Calidad de Servicio, otro de los servicios provee sincronización del temporizador de capas superiores y finalmente un servicio para la medición de la radio (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007). A continuación se describe brevemente cada uno de ellos:

2.1.6.3.1 Distribución de Mensajes dentro de un DS

- ***Distribución:*** Servicio DSS solicitado para entregar mensajes dentro de un DS de manera de que lleguen a su destinatario apropiado, el DS debe proporcionar suficiente información para poder determinar el punto de salida que corresponde al destinatario, esta información requiere de la asociación, reasociación y desasociación. Una vez el mensaje está dentro del DS sale del alcance de IEEE 802.11.

- ***Integración:*** Este servicio habilita la transferencia de datos entre una estación de la WLAN y una estación de la LAN. El término integración se refiere a una LAN alámbrica conectada al DS. El servicio de integración se encarga de cualquier traducción de direcciones y de la conversión de medios requeridos para el intercambio de datos (Bernal, 2008).

- ***Programación de tráfico QoS:*** Proporciona Calidad de Servicio en la transferencia de tramas intra-BSS bajo HCF[3] (Hybrid Coordination Function).

[3]**HCF** Función que además de permitirle a un AP coordinar la red le proporciona el medio para administrar el canal.

2.1.6.3.2 Servicios que soporta el DSS

Para que el servicio de Distribución dentro del DS funcione se requiere información de las estaciones en el ESS. Esta información es proporcionada por los servicios de asociación en donde el DS necesita saber la identidad del AP al cual se debe entregar el mensaje para que llegue a la estación destino (Bernal, 2008). Previamente a la definición de los conceptos relacionados con la asociación se describen los tipos de movilidad:

a) **Sin Transición:** Una STA es estacionaria o sólo se mueve dentro de un BSS.
b) **Transición BSS:** Una STA se mueve de un BSS a otro BSS dentro de un mismo ESS,
c) **Transición ESS:** Se refiere al movimiento de una estación de un BSS en un ESS a otro BSS en otro ESS.

Los servicios de asociación soportan los diferentes tipos de movilidad anteriormente descritos:

- ***Asociación:*** se establece una asociación inicial entre una estación y un Punto de Acceso, una estación antes de que transmita o reciba datos debe estar asociada a un AP, la información es acerca de la identidad y dirección de la estación. El AP puede comunicar esta información a otros AP en el ESS para facilitar la tarea de enrutamiento, entrega de tramas y movilidad entre ESSs (Bernal, 2008).

- ***Reasociación:*** Permite transferir una asociación existente desde un Punto de Acceso a otro de tal forma que una estación móvil puede moverse de un BSS a otro BSS dentro de un ESS.

- ***Disasociación:*** constituye una notificación antes que una solicitud y representa el término o fin de una asociación entre una STA y un AP.

2.1.6.3.3 Servicios de Control de Acceso y Confidencialidad de Datos

- ***Autenticación:*** Corresponde a un servicio (SS) que permite establecer identidades entre las estaciones STA que requieren comunicarse tanto en redes IBSS y ESS antes de la asociación, es decir la autenticación es un requisito previo a la asociación.

- ***Desautenticación***: Es un servicio (SS) y finaliza el proceso de autenticación establecidos por las STA.

- **Confidencialidad de Datos:** En una red LAN solamente aquellos dispositivos que están conectados físicamente son capaces de enviar y recibir tráfico dentro de la red, en el caso de una WLAN donde el medio es compartido cualquier tipo de dispositivo que esté cerca de la LAN está en la capacidad de transmitir y recibir datos inclusive interferir con el tráfico LAN de tal forma que un enlace inalámbrico sin confidencialidad degrada el nivel de seguridad de la LAN a la que pertenece una WLAN. Para solucionar este inconveniente IEEE Std 802.11 proporciona la capacidad de proteger el contenido de los mensajes proporcionando varios algoritmos de cifrado: WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol) y CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol).

2.1.6.3.4 Gestión de Espectro

Se requieren dos servicios para satisfacer las necesidades en algunos dominios reguladores para el funcionamiento en la banda de 5Ghz. Estos servicios se llaman Control de Potencia de Transmisión (TPC) y (DFS) Selección Dinámica de Frecuencias (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007).

- ***TPC:*** El servicio TPC tiene la finalidad de reducir la interferencia generada por los servicios de satélite y establece principalmente que la asociación de una STA con un AP en un BSS está basado en la capacidad de potencia de la estación entre otras.

- ***DFS:*** Para entornos WLAN que utilizan la banda de 5Ghz y se ven afectados por los sistemas de radar DFS proporciona la utilización uniforme de canales disponibles estableciendo básicamente lo siguiente:

    - La asociación de estaciones con un AP en un BSS se basa en los canales soportados por las estaciones.
    - Canales de prueba para verificar la presencia de radares.
    - Interrupción de las operaciones en caso de la detección de un sistema de radar en el mismo canal.
    - Selección y publicación de un nuevo canal en caso de existir interferencia con un sistema de radar.

2.1.6.3.5 Diferenciación de Tráfico y Soporte QoS

IEEE 802.11 utiliza un medio compartido y proporciona un control diferenciado de acceso al medio para manejar las transferencias de datos con requisitos de QoS. Las especificaciones relativas a la integración y operatividad de QoS en una WLAN con cualquier otro mecanismo de entrega de Calidad de Servicio extremo a extremo como Protocolo de Reserva de Recursos (RSVP) están más allá del alcance de esta norma (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007).

2.1.6.3.6 Temporizador de Sincronización en capas superiores

Algunas aplicaciones, por ejemplo, el transporte y la prestación de los flujos de audio o de video, requieren temporizadores compartidos entre diferentes STA sincronizados. Mayor precisión de sincronización puede ser un requisito adicional. En apoyo a este tipo de aplicaciones, esta norma define este servicio que permite a las capas por encima de la MAC sincronizar con precisión temporizadores dependientes de aplicaciones compartidas entre STA. Este servicio es utilizado por más de una aplicación a la vez (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007).

2.1.6.3.7 Medición de Radio

Este servicio proporciona lo siguiente:

- La capacidad de solicitar, reportar y realizar mediciones en los canales
- Una interfaz para recuperar las mediciones utilizando primitivas MLME (MAC Layer Management Entity) y acceso MIB (Management Information Base)
- Información sobre los AP vecinos

2.1.6.3.8 Funcionamiento con redes Externas

De manera general este servicio permite el inter-funcionamiento de un AP para acceder a servicios proporcionados por una red externa de acuerdo con la suscripción u otras características de esa red externa. Entre las funciones se tienen:

- Selección y descubrimiento de red
- Servicios de emergencia
- Distribución de la política QoS

2.1.6.4 Capa Física IEEE 802.11

En general con respecto al modelo de referencia OSI en la capa Física se define y especifica las características eléctricas, ópticas, de radio entre otras de las señales a transmitirse además de los mecanismos de conexión (mecánicas y físicas) aplicables al medio de transmisión. Entre las funciones que se realizan en esta capa están: la codificación/decodificación, señalización y transmisión/recepción de bits, en la Figura 13 se presentan algunas de las opciones de capa Física.

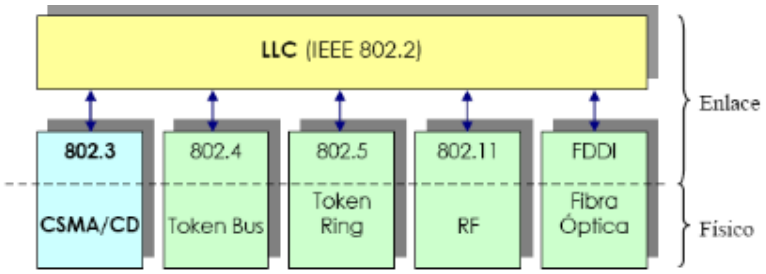


Figura 14. Capa Física

Fuente: (Villegas, 2008)

En la arquitectura IEEE 802.11, la capa Física (PHY) es la interfaz entre el medio inalámbrico y la subcapa MAC (Figura 14), cumple con las funciones de intercambiar tramas con la capa superior (MAC), hacer uso de la modulación con la finalidad de adaptar las señales al medio de transmisión y verificar la actividad del ambiente o del medio.

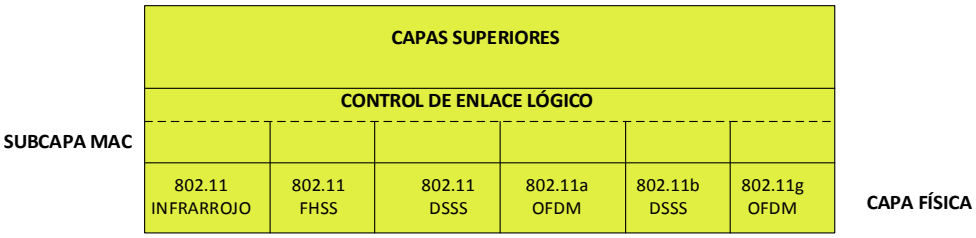


Figura 15. Capa Física (PHY) en IEEE 802.11

Fuente: Propia

Para interactuar la capa Física IEEE 802.11 con la subcapa MAC se definen dos entidades funcionales que son: ***PLCP*** (Physical Layer Convergence Procedure) y ***PMD*** (Physical Medium Dependent).

- ***PLCP (Physical Layer Convergence Procedure):*** Define un método para "transformar o asociar" los PDUs de la MAC (MPDUs) a un formato idóneo para la transmisión y recepción de datos entre estaciones que utilizan una capa PMD asociada (Bernal, 2008).

- ***PMD (Physical Medium Dependent):*** Especifica las características y mecanismos de transmisión y recepción de datos (modulación/demodulación) a través del medio inalámbrico entre dos o más estaciones que utilizan la misma PHY (Cisco, 2006).

Existen algunas técnicas para la transmisión por Radiofrecuencia que se han adoptado en cada una de las variantes IEEE 802.11 como por ejemplo Spread Spectrum (SS) o Espectro Ensanchado. Éste se basa en un ensanchamiento de la señal a transmitir a lo largo de una banda muy ancha de frecuencias con la finalidad de resistir a interferencias externas, capacidad de acceso múltiple y ofrecer un canal seguro para la comunicación. A su vez dentro de la técnica de Espectro Ensanchado existen dos mecanismos utilizados en IEEE 802.11 Legacy: FHSS (Espectro Ensanchado por Salto de Frecuencia) y DSSS (Espectro Ensanchado de Secuencia Directa) que no son interoperables entre sí.

Con FHSS el espectro de 2,4Ghz se divide en 75 subcanales de 1Mhz cada uno, tanto el transmisor como el receptor trabajan bajo un patrón de salto y la información es enviada sobre una secuencia de subcanales que solamente comprenden las partes involucradas. Cada transmisión 802.11 maneja un patrón de salto único con el objeto de minimizar la probabilidad de uso de los subcanales simultáneamente. La desventaja de este sistema es que está limitado a velocidades de transmisión de 2Mbps por tal razón no es utilizado ampliamente.

En cambio DSSS divide la banda de 2,4Ghz en 14 subcanales con una separación entre ellos de 5Mhz, el número de subcanales a utilizar lo adjudica cada dominio regulador por ejemplo en Estados Unidos son 11 canales disponibles (véase Tabla 2). Dentro de un canal, la mayor concentración de energía se expande en una banda de 22Mhz, por tal razón para evitar interferencia debe existir una separación de 25Mhz entre las frecuencias centrales de los canales, dando como resultado 3 canales sin solapamiento (1,6 y 11) que pueden coexistir en una misma zona.

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores				
		América (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japón (-J)
1	2412	×	×	—		×
2	2417	×	×	—	×	×
3	2422	×	×	×	×	×
4	2427	×	×	×	×	×
5	2432	×	×	×	×	×
6	2437	×	×	×	×	×
7	2442	×	×	×	×	×
8	2447	×	×	×	×	×
9	2452	×	×	×	×	×
10	2457	×	×	—	×	×
11	2462	×	×	—	×	×
12	2467	—	×	—	—	×
13	2472	—	×	—	—	×
14	2484	—	—	—	—	×

Tabla 2. Canales disponibles para algunos Dominios Reguladores

Fuente: http://es.wikipedia.org/wiki/IEEE_802.11

En la Figura 16, se muestran los canales en IEEE 802.11 que no se solapan (1,6 y 11).

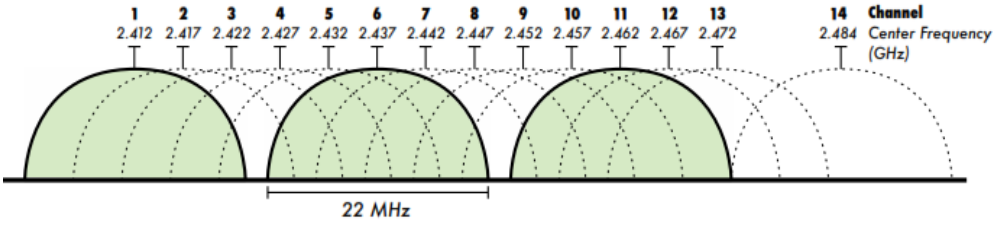


Figura 16. Canales sin solapamiento

Fuente: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf

Para la cobertura de áreas muy grandes es necesario seleccionar cuidadosamente los tres canales (1, 6 y 11) a utilizar de manera que no exista interferencia entre ellos hablando en términos de

frecuencia pero si solapamiento en términos de área de cobertura para posibilitar el roaming, en la Figura 17 se presenta un esquema ideal de la reutilización de los canales.

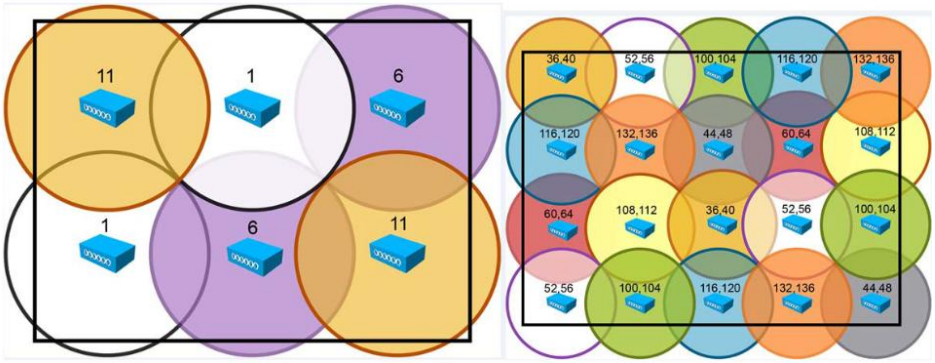


Figura 17. Reutilización de frecuencias

Fuente: (Cisco, 2013)

En DSSS para compensar el ruido que se introduce en el canal debido a su ancho de banda se usa la técnica denominada "chipping", en la que cada bit de datos se convierte en una serie de patrones de bits redundantes llamados "chips" (secuencia de Barke), específicamente 1 bit de datos está formado por 11 chips, dando como resultado un mecanismo sólido de detección y corrección de errores además de minimizar la necesidad de retransmisión en 802.11 Legacy, para el caso de 802.11b se usa otra técnica de codificación CCK (Complementary Code Keying) que permite superar las velocidades de transmisión de 1 y 2Mbps a 5,5 y 11Mbps.

Otra de las técnicas utilizadas en 802.11a/g/n/ac es OFDM (Orthogonal Frecuency Division Multiplexing) o Multiplexión por División en Frecuencias Ortogonales que consiste en la división de un canal en un número determinado de bandas de frecuencias equiespaciadas por las que se transmite una subportadora con una porción de la información del usuario. Las subportadoras son ortogonales entre sí es decir desfasadas 90° entre señales de la misma frecuencia, aumentando de esta forma el uso eficiente del espectro.

En la Tabla 3 se muestra de manera general los cambios y variaciones a la PHY IEEE 802.11:

IEEE 802.11	DESCRIPCIÓN PHY
802.11 Legacy	• 2,4Ghz ISM • Velocidades de transmisión de 1 y 2 Mbps • FHSS con modulaciones: FSK Gaussiana de dos niveles para 1Mbps y FSK Gaussiana de 4 niveles para 2Mbps. • DSSS con modulaciones: DBPSK (Differential Binary Phase Shift Keying) para 1Mbps y DQPSK (Differential Quadrature Phase Shift Keying) para 2Mbps. • Adicionalmente se especifica una PHY para IR (no utilizado) con longitudes de onda de 850 a 950nm con modulación 16 PPM (Pulse Position Modulation) para 1Mbps y 4 PPM para 2Mbps.
802.11a	• 5Ghz ISM (espectro relativamente no congestionado) • Velocidad de transmisión teórica de hasta 54Mbps (velocidad real 20Mbps) • Un total de 12 canales en el espectro asignado, cada uno de 20Mhz • OFDM (cada canal con 52 subportadoras donde: 48 para la transmisión de datos y las 4 restantes para monitoreo de desplazamientos de frecuencia y ICI (InterCarrier Interference). • Utiliza modulaciones: BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), 16QAM (Quadrature Amplitude Modulation), 64QAM.
802.11b	• Similar a 802.11Legacy • 2,4Ghz ISM • Velocidades de transmisión de 5,5 y 11Mbps (velocidad real 6Mbps) • HR-DSSS (High Rate Direct Sequence Spread Spectrum) con CCK para incrementar la velocidad de datos pico a 11Mbps a la vez que se utiliza DQPSK.
802.11g	• 2,4Ghz ISM y compatibilidad con versiones anteriores por medio de ERP (Extended Rate PHy) para proveer coexistencia. • Velocidad de transmisión teórica de hasta 54Mbps (velocidad real 22Mbps) • Utiliza los mismos esquemas de modulación para 1, 2, 5.5 y 11Mbps y para 54Mbps ERP-OFDM (802.11a pero a 2,4Ghz)
802.11n	• 2,4Ghz (compatibilidad 802.11b y 802.11g) y 5Ghz (compatibilidad 802.11a)

	• Ancho de Banda de canal de 20Mhz para la banda de 2,4Ghz y 40Mhz para la banda de 5Ghz. • Tasa de transmisión teórica de hasta 600Mbps (velocidad real 300Mbps) • Utiliza OFDM con modulación 16 QAM y 64 QAM. • Transmisión de hasta 4 flujos de información a la vez gracias a la tecnología MIMO (Múltiple Entrada, Múltiple Salida), es decir la utilización de hasta 4 antenas que trabajan de manera simultánea en la transmisión y recepción en un mismo Punto de Acceso para incrementar la velocidad.
802.11ac	• 5Ghz ISM • Ancho de Banda de canal de 20, 40, 80Mhz (mandatorios) y 160Mhz (opcional) • Velocidades de transmisión teóricas de hasta 1,3Gbps (velocidad real 867Mbps) • Utiliza OFDM con modulaciones 16/64/256 QAM • Transmisión de hasta 8 flujos de información por medio de una versión mejorada de la tecnología MIMO (MU-MIMO) o MIMO Multiusuario que utiliza el mecanismo SDMA (Acceso Múltiple por División Espacial) en la que múltiples transmisores envían señales separadas y múltiples receptores reciben señales separadas simultáneamente en la misma banda. • Utilización de la tecnología "Beamforming" que permite a los Puntos de Acceso determinar la ubicación de los dispositivos inalámbricos y dirigir una señal más fuerte hacia ellos.

Tabla 3. Variaciones PHY IEEE 802.11

Fuente: Propia

2.1.6.5 Capa MAC IEEE 802.11

Una WLAN IEEE 802.11 en el nivel Enlace de Datos se estructura de dos subcapas: LLC (Logical Link Control) y MAC (Media Access Control), véase la Figura 18. La subcapa LLC 802.2 es independiente de la topología, medio de transmisión y de las técnicas de control de acceso al medio de las capas MAC y PHY proporcionando una identificación de protocolo de capa superior (ULP), funciones de control de enlace de datos y servicios de conexión de tal

forma que las capas superiores como la capa de Red envían los datos de usuario al LLC esperando transmisiones sin errores a través de la red (Cisco, 2006).

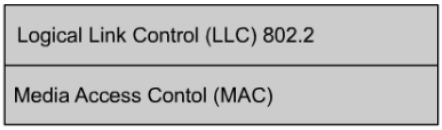


Figura 18. Data Link IEEE 802.11

Fuente: (Cisco, 2006)

La subcapa LLC proporciona tres clases de servicios de conexión:

- *Servicios sin conexión no confirmados:* servicio del mejor esfuerzo en el que se pueden intercambiar Unidades de Datos de Servicio de Enlace (LSDUs) sin el establecimiento de una conexión a nivel capa 2.

- *Servicios sin conexión confirmados:* permite el intercambio de LSDUs de manera confiable pero sin el establecimiento de una conexión en capa 2, como una transferencia de datos punto a punto.

- *Servicios orientados a conexión confirmados:* el intercambio de LSDUs es confiable ya que se lleva un control de flujo, secuencia y recuperación de errores en la capa de enlace de datos con transmisiones punto a punto.

Por otra parte la subcapa MAC IEEE 802.11 tiene como finalidad fundamental proveer los mecanismos de control y gestión de acceso al medio de transmisión, en este caso de naturaleza inalámbrica. Además de esta funcionalidad proporciona tres servicios que son:

- *Servicios de Datos Asíncronos:* capacidad de las entidades LLC para intercambiar (MSDUs) o Unidades de Datos de Servicio MAC, utiliza los servicios de nivel PHY subyacentes para el transporte de una MSDU a una entidad MAC luego la entrega a

LLC. Este transporte MSDU se realiza sobre la base del mayor esfuerzo y sin conexión de tal forma que no se garantiza su entrega exitosamente.

- *Servicios de Seguridad:* que contempla el servicio de autenticación y cifrado de la MSDU para cumplir con los objetivos de seguridad que son: integridad de los datos, confidencialidad y control de acceso a la WLAN.

- *Ordenamiento de MSDUs:* la subcapa MAC reordenará intencionalmente las MSDUs en el caso de ser necesario aumentar la probabilidad de una entrega exitosa pero cambiando el orden de la entrega de MSDUs broadcast y multicast otorgándoles a las MSDUs unicast prioridad.

2.1.6.6 Tipos de Tramas

IEEE 802.11 define tres tipos de tramas, cada tipo con su función específica:

- *Tramas de Datos:* transportan los datos o carga útil.

- *Tramas de Control:* para el control de acceso al medio y soporte de entrega de los otros tipos de tramas MAC.

    - RTS (Request to Send): Solicitud para enviar
    - CTS (Clear to Send): Despejado para enviar
    - ACK (Acknowledgment): Confirmación.

- *Tramas de Administración:* intercambian información de gestión pero sin enviarse a las capas superiores, generalmente cuando una STA inicia o suspende su participación en la WLAN. Estas son las tramas de gestión: beacon, solicitud de asociación, respuesta de asociación, solicitud de reasociación, respuesta de reasociación, autenticación, des-autenticación, disociación, solicitud de sondeo y respuesta de sondeo.

2.1.6.7 Arquitectura Funcional MAC IEEE 802.11

Antes de transmitir una trama una estación (STA) debe obtener acceso al medio ya sea por cualquiera de las dos funciones o mecanismos: DCF (Función de Coordinación Distribuida) o PCF (Función de Coordinación Puntual), véase Figura 19.

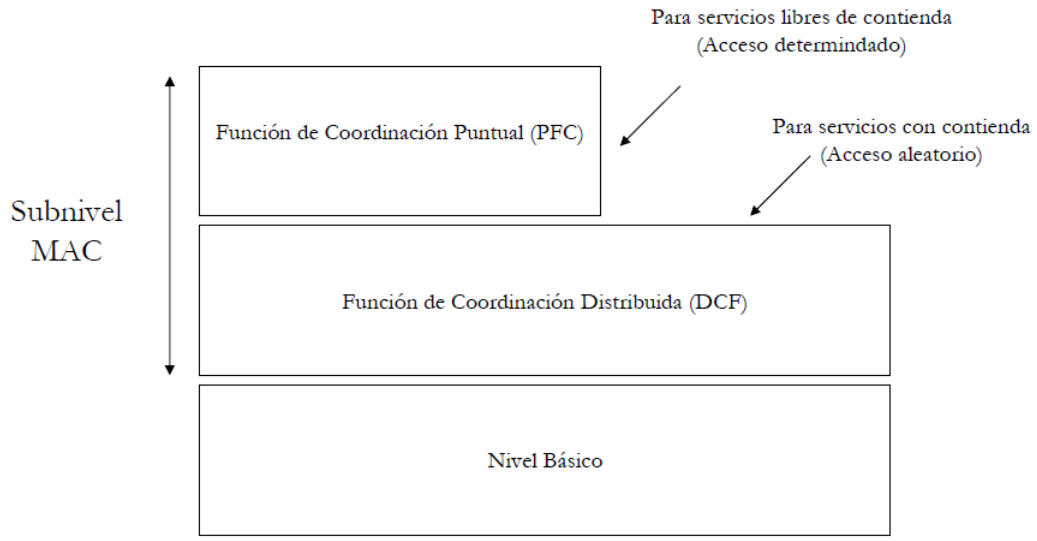


Figura 19. Arquitectura Funcional MAC

Fuente: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo1.pdf

DCF provee la funcionalidad para que las estaciones (STA) de un BSS escuchen el medio antes de transmitir datos de protocolo a nivel MAC por medio de técnicas de acceso aleatorias con servicios asíncronos y períodos de contención utilizando CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) y MACA (Multiple Access with Collision Avoidance). DCF se implementa en todas las STAs para su uso tanto en configuraciones de red Ad Hoc como de infraestructura (Cisco, 2006).

La Función de Coordinación Puntual es considerada como un mecanismo opcional que crea un acceso libre de contención y solo puede utilizarse en configuraciones de red tipo infraestructura, utiliza técnicas de acceso determinísticas proporcionando un servicio tipo síncrono que no tolera retardos aleatorios en el acceso al medio.

En PCF no se compite por el medio, un ente es el coordinador de acceso, generalmente un AP que controla la transmisión de las tramas. Este AP o Punto Coordinador obtiene el control del medio al inicio del período libre de contención utilizando un PIFS (PCF InterFrame Space) y si el medio está libre el coordinador envía una trama de *beacon* con la duración máxima del período libre de contención. Una vez que las estaciones reciben el *beacon* no pueden tomar control del acceso al medio hasta que termine el período libre de contención.

DCF y PCF pueden trabajar de manera conjunta dentro de un mismo BSS, siendo éste el caso los dos métodos se alternan con un período libre de contención seguido por un período de contención. Pero por defecto las estaciones que cumplen con IEEE 802.11 operan usando DCF ya que PCF es opcional y aplicable a transmisión de información crítica limitada por el tiempo como audio y video además de que impone mayor sobrecarga a la red debido a la transmisión de tramas para el polling o sondeo.

2.1.6.7.1 Protocolo de Acceso al Medio

El método de acceso al medio definido en el estándar IEEE 802.11 es muy diferente al de Ethernet debido a la naturaleza de los medios utilizados por ejemplo son comunicaciones Half-Dúplex[4] y no todos los nodos están al alcance unos de otros. En una LAN para coordinar el acceso al medio utiliza el protocolo CSMA/CD (Acceso Múltiple con Escucha de Portadora y Detección de Colisiones) de manera que los dispositivos de red escuchan el medio antes de transmitir, es decir si el canal y sus recursos están disponibles .

En los sistemas 802.11 se trata de evitar cualquier tipo de colisión a través de la funcionalidad DCF que a su vez proporciona el protocolo CSMA/CA al no poder transmitir y escuchar al mismo tiempo como lo que ocurre en una red LAN. Un dispositivo que desee enviar una trama empieza con un retroceso aleatorio con un número determinado de ranuras y espera hasta que el canal esté inactivo (Backoff), para lo cual debe detectar que no hay señal durante un periodo corto y empieza a realizar el conteo descendente haciendo pausa cuando se envían tramas.

[4]**Half-Duplex:** Transmisión de información bidireccional no simultáneo

Cuando el contador llega a 0 envía la trama y si ésta llega a su destino el dispositivo destino envía una confirmación. En caso de no existir esta confirmación se interpreta como un error o una colisión, de forma que el emisor duplica el período de retroceso e intenta de nuevo hasta que la trama se transmita con éxito o se llegue al número máximo de retransmisiones (Meden, 2013).

El hecho de que en las WLANs no todos los nodos están al alcance unos de otros genera dos inconvenientes:

1. ***Problema de los Nodos Escondidos*:** No todos los dispositivos están dentro del alcance de radio de todos los demás y las transmisiones que se realizan en una parte de la celda a lo mejor no se reciban en el resto de la misma celda y algún dispositivo en esta área puede concluir erróneamente que el canal está libre y empieza a transmitir provocando una colisión.

2. ***El Problema de los Nodos Expuestos:*** Un dispositivo desea transmitir y escucha el canal. Cuando oye una transmisión de otro dispositivo entonces concluye erróneamente que no puede enviar tramas aun cuando este último está transmitiendo a cualquier otro, de forma que esta decisión desperdicia una oportunidad de transmisión (Meden, 2013).

Para reducir estos inconvenientes y determinar qué STA es la que tiene que transmitir se define la detección del canal como un proceso que consiste tanto en una detección física (proporcionado por la PHY) como una detección virtual que incluye la transmisión de tramas de control (MACA) y retardos basados en prioridades (IFS).

El mecanismo de detección de portadora virtual denominado NAV o Vector de Asignación de Red (Network Allocation Vector), sirve como un registro lógico del momento en que una STA hace uso del canal. Cada trama tiene el campo NAV que representa el tiempo en que se completará la secuencia a la que pertenece esta trama, los dispositivos que escuchen esta trama conocen que el canal estará ocupado durante el tiempo indicado por el NAV, sin importar que puedan o no detectar señal física.

En cuanto a las tramas de control que deben intercambiarse entre el transmisor y el receptor para indicar a los nodos cercanos que se va a iniciar una transmisión son:

- ***RTS:*** El transmisor envía una trama RTS al receptor, la trama RTS incluye un campo que indica cuánto tiempo el transmisor controla el medio (o especifica la longitud de la trama que se va a transmitir). A este tiempo se le considera como *información de reservación*, las STA que escuchan esta trama almacenan localmente este valor en el NAV que actúa como un temporizador decreciente (Bernal, 2008).

- ***CTS:*** Con esta trama responde el receptor, también incluye el tiempo que tomará la transmisión de la trama de datos. Cuando un nodo escucha un CTS conoce que está cerca del receptor y que no puede transmitir el tiempo especificado.

- ***ACK:*** El receptor envía un ACK cuando haya recibido una trama satisfactoriamente, todos los nodos deben esperar el ACk antes de volver a transmitir. Si el transmisor no recibe ningún acuse de recibo durante un periodo de tiempo automáticamente se vuelve a retransmitir. En la Figura 19 se presentan las tramas de control: RTS, CTS y ACK.

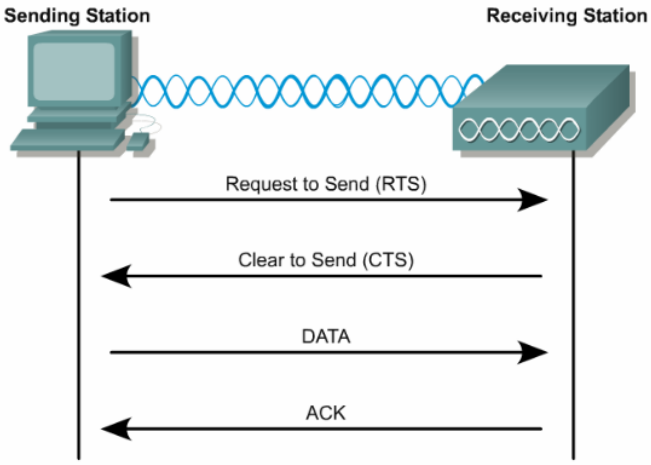


Figura 20. Tramas de Control: RTS, CTS y ACK

Fuente: (Cisco, 2006)

Para la transmisión de cada una de las tramas de control es necesario manejar tiempos "espacios interframe" o IFS, que se define como el tiempo desde el último bit del frame anterior al primer bit del preámbulo del frame subsiguiente (Cisco, 2006). Existen cuatro tipos de IFS que proporcionan prioridad para el acceso inalámbrico y se ordenan desde el más corto:

1. **SIFS:** espacio interframe más corto
2. **PIFS:** espacio interframe PCF (Función de Coordinación Puntual)
3. **DIFS:** espacio interframe DCF (Función de Coordinación Distribuida)
4. **EIFS:** espacio interframe extendido.

En la Figura 20 se muestran los espacios InterFrame necesarios para el envío de las tramas de control y datos en un mecanismo DCF.

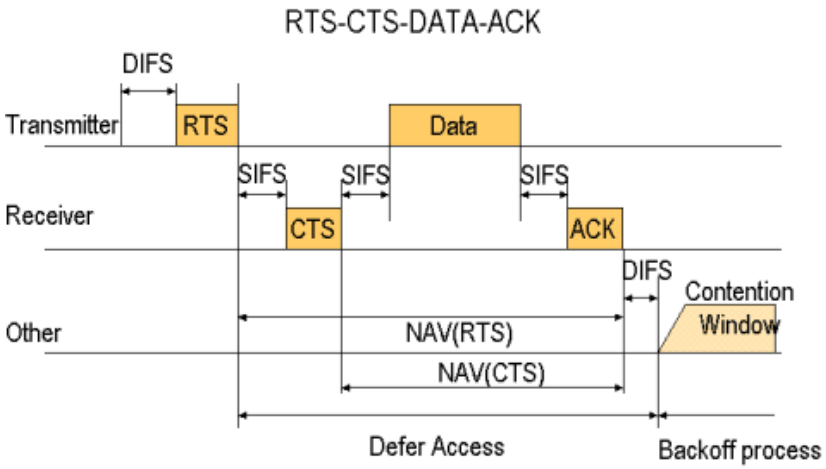


Figura 21. Tipos de InterFrame Space IFS

Fuente: http://www.soi.wide.ad.jp/class/99007/slides/09/index_23.html

2.1.6.8 Trama MAC IEEE 802.11

La trama MAC IEEE 802.11 está formada de los siguientes componentes:

- **Cabecera:** que comprende 9 campos: Control, Duración, Direccionamiento, Secuencia de Control y campos de control de QoS.

- **Cuerpo de la Trama:** Campo de longitud variable que contiene información sobre el tipo de trama, la longitud mínima de 0 bytes y la longitud máxima de 7955. En el caso de la trama MAC IEEE 802.11ac su longitud máxima es 11426.

- **Secuencia de Verificación de Trama:** (Frame Check Sequence) que incorpora un código de redundancia CRC de 32 bits.

En la Figura 22 se muestra el formato de una trama MAC completa.

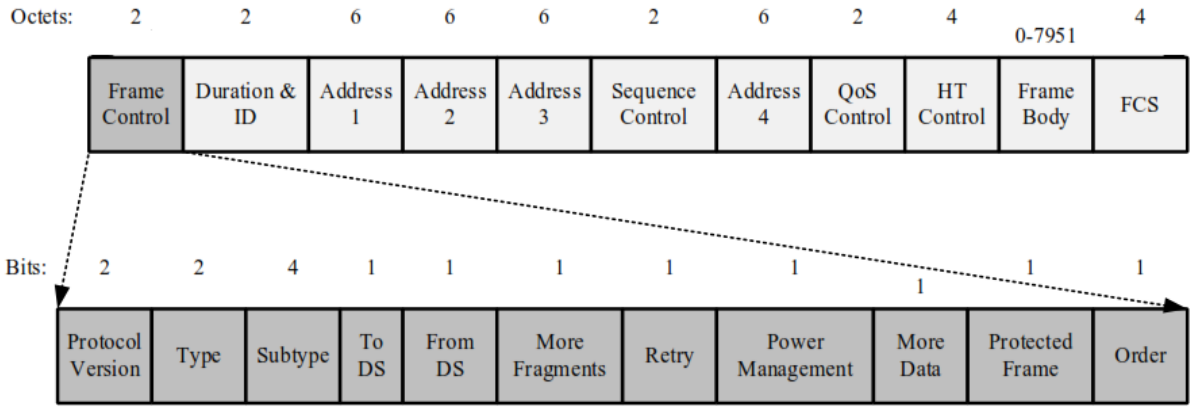


Figura 22. Trama MAC IEEE 802.11n

Fuente: (Soyinka, 2010)

A continuación en la Tabla 4 se resume la funcionalidad de los campos de la cabecera de la Trama MAC IEEE 802.11:

CAMPO	FUNCIÓN
Frame Control	Principalmente indica el tipo de trama, se compone de 16 bits y 11 subcampos que proveen información de control como por ejemplo versión del protocolo, administración de potencia entre otros.
Duration ID	El tiempo en microsegundos que el canal será utilizado para la transmisión de la trama.
Address 1, 2, 3 y 4	Son cuatro campos que contienen una dirección en el formato de la trama MAC (48 bits) y se utilizan para indicar el Basic Service Set Identifier (BSSID), el Destination Address (DA), el Source Address (SA), el Receiver Address (RA) y el Transmitter Address (TA). Estos cuatro campos se involucran con los subcampos To DS y From DS.
Sequence Control	Contiene el número de secuencia así como el número de fragmento de la trama que se está enviando ayudando a evitar las tramas duplicadas.
QoS Control	Campo de 16 bits referido al control de calidad del servicio que identifica el TC (Traffic Category).
HT Control	High Throughput tiene un tamaño de 4 octetos y permite proveer control de calidad de servicio sobre tramas de control, de datos y de gestión por ejemplo: RTS+HTC, BlockAckReq+HTC, PS-Poll+HTC.

Tabla 4. Campos de la Cabecera de la Trama MAC IEEE 802.11

Fuente: Propia

El campo Frame Control de la cabecera MAC IEEE 802.11 está formado por 11 subcampos que se explican a continuación en la Tabla 5:

SUBCAMPOS FC	DESCRIPCIÓN
Protocol Version	Subcampo con una longitud de 2 bits, su valor por defecto es 0 y los demás valores está reservados para futuras versiones del protocolo.
Type & Subtype	El subacampo Type tiene una longitud de 2 bits y Subtype una longitud de 4 bits, en conjunto identifican si la trama es de datos, control o gestión. Por ejemplo 00 (Management Frame), 01 (Control Frame), 10 (Data Frame) y 11 (Reservado).
To DS	Un bit que puede ser 1 si se desea que la trama se reenvíe usando un AP hacia el DS.
From DS	Un bit que puede ser 1 para las tramas provenientes de un DS caso contrario 0.
More Fragments	Indica que todavía existen fragmentos por transmitir.
Retry	Permite evitar el procesamiento de tramas duplicadas, el valor de 1 en una trama de datos o control indica significa que es una retransmisión de un frame anterior.
Power Management	Un bit que indica el estado de energía en la que se encontrará la estación después de haber completado la secuencia de intercambio de tramas. 1: STA en modo ahorro de energía 0: modo activo, siempre para las tramas transmitidas por los AP.
More Data	Un bit, en el que 1 significa que existen tramas almacenadas temporalmente en espera.
Protected Frame	Un valor de 1 representa que el cuerpo de la trama está cifrada con algún algoritmo de encriptación y solo es posible para algunos tipos de tramas de datos y de gestión.
Order	Un valor de 1 indica a la estación receptora que procese los datos según el orden de llegada.

Tabla 5. Subcampos de Frame Control

Fuente: http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F07+-+Capitulo+2.pdf

En base a la explicación de los subcampos Type y Subtype su funcionalidad radica en la identificación del tipo de trama (datos, control o administración). En la Tabla 6 se muestra los tipos de tramas tanto para DCF como para PCF de manera más específica,

Tipo de trama	Subcampo	Función de la trama
Gestión 0 0	0 0 0 0	Solicitud de asociación
	0 0 0 1	Respuesta de asociación
	0 0 1 0	Solicitud de reasociación
	0 0 1 1	Respuesta de reasociación
	0 1 0 0	Solicitud de sondeo
	0 1 0 1	Respuesta de sondeo
	0 1 1 0 – 0 1 1 1	Reservado
	1 0 0 0	Faro
	1 0 0 1	Trafico anunciado
	1 0 1 0	Disociación
	1 0 1 1	Autenticación
	1 1 0 0	Deautenticación
	1 1 0 1 – 1 1 1 1	Reservado
Control 0 1	0 0 0 0 – 1 0 0 1	Reservado
	1 0 1 0	Ahorro de energía
	1 0 1 1	RTS
	1 1 0 0	CTS
	1 1 0 1	ACK
	1 1 1 0	Fin CF
	1 1 1 1	Fin CF + CF ACK
Datos 1 0	0 0 0 0	Datos
	0 0 0 1	Datos + CF ACK
	0 0 1 0	Datos + trama CF
	0 0 1 1	Datos + CF ACK + Trama CF
	0 1 0 0	Null
	0 1 0 1	CF ACK
	0 1 1 0	Trama CF
	0 1 1 1	CF ACK + Trama CF
	1 0 0 0 – 1 1 1 1	Reservado
Reservado 1 1	0 0 0 0 – 1 1 1 1	

Tabla 6. Tipos de Tramas en base a la clasificación Type y Subtype

Fuente: http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%EDtulo+5.pdf

Con respecto a los subcampos To DS y From DS cada uno de un bit se tiene las siguientes posibles combinaciones:

- ***To DS=0 y From DS=0:*** Para el caso de redes Ad-Hoc ya que el DS no está involucrado en la comunicación.
    - **Address 1 (receiver):** DA
    - **Address 2 (transmitter):** SA
    - **Address 3:** BSSID
    - **Address 4:** no se utiliza

- ***To DS=0 y From DS=1:*** En redes de infraestructura para el caso de tramas de datos dirigidas desde un equipo en un DS a un STA.
    - **Address 1 (receiver):** DA es decir STA en este caso
    - **Address 2 (transmitter):** BSSID, el AP
    - **Address 3:** SA, es decir el equipo en el DS
    - **Address 4:** no se utiliza

- ***To DS=1 y From DS=0:*** En redes de infraestructura para el caso en que se transmite de una STA a un dispositivo en un DS.
    - **Address 1 (receiver):** BSSID, el AP
    - **Address 2 (transmitter):** SA, la STA
    - **Address 3:** DA, el equipo en el DS
    - **Address 4:** No se utiliza

- ***To DS=1 y From DS=1:*** Para el caso de un sistema de Distribución Inalámbrico (WDS) como en el ejemplo de la Figura 23 en el que se transmite desde un dispositivo en un DS a otro dispositivo en un DS cruzando por un WDS.
    - **Address 1 (receiver):** AP en el lado del servidor
    - **Address 2 (transmitter):** AP en el lado del cliente
    - **Address 3:** DA, el servidor
    - **Address 4:** SA, el cliente

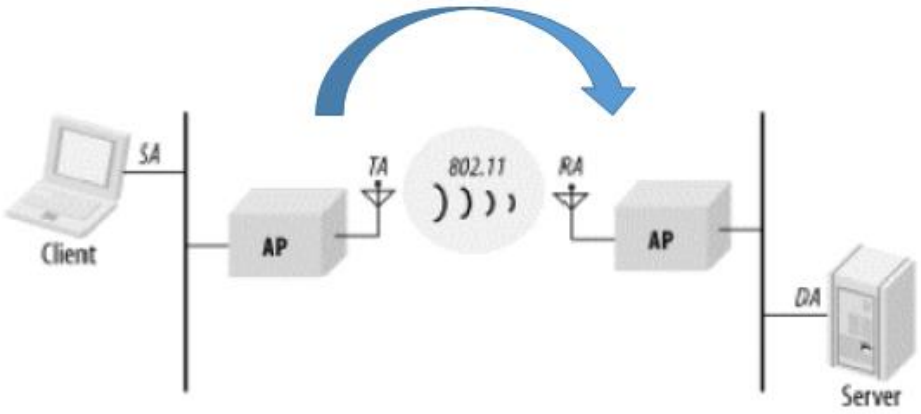


Figura 23. To DS y From DS en un Sistema de Distribución Inalámbrico

Fuente: (Bernal, 2008)

2.1.6.8.1 Formato de las Tramas de Gestión y Control

El propósito de las tramas de gestión es establecer inicialmente la comunicación entre las STA y los Puntos de Acceso mediante los servicios de autenticación y asociación, aunque también controla otros como la sincronización en un ambiente PCF. Las tramas de gestión tienen el mismo formato que las tramas de datos, además de un formato para la parte de los datos que varía con el subtipo y al igual que las de control en los subcampos To DS y From DS sus bits son cero (Meden, 2013).

En la Figura 24 se presenta la trama genérica de gestión en donde la Dirección Destino ocupa el campo Address 1, la Dirección de Origen ocupa el campo Address 2 y el BSSID el campo Address 3.

2 Octets	2 Octets	6 Octets	6 Octets	6 Octets	2 Octets	0-2312 Octets	4 Octets
Control Trama	Duración	DA	SA	BSSID	Sec. Control	Cuerpo Trama	FCS

Figura 24. Formato de la Trama de Gestión

Fuente: http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%EDtulo+5.pdf

Posterior al establecimiento de la autenticación y asociación entre una STA y un AP, las tramas de control son las encargadas de asistir en el envío de los datos. Son tres las tramas de control utilizadas en DCF (RTS, CTS y ACK), cuyo mecanismo de trabajo ya se ha explicado anteriormente.

Con respecto a las tramas RTS y CTS:

- En la Trama RTS el campo Duración (microsegundos) contiene el tiempo necesario para transmitirla además el tiempo necesario para un ACK y tres SIFS. El campo Address 1 se ocupa con la Dirección del Receiver (RA) y el campo Address 2 se ocupa con la dirección del Transmitter (TA).

- En la Trama CTS el campo Duración (microsegundos) contiene el tiempo de la anterior trama RTS menos el tiempo necesario para enviar el CTS y un SIFS. Esta trama contiene solo la Dirección de Receiver (RA).

En la Figura 25 se muestra el formato para las tramas RTS y CTS cuyo tamaño o longitud es más pequeño en comparación a las tramas de datos y gestión, en cuanto a la trama ACK ésta tiene el mismo formato que un frame CTS.

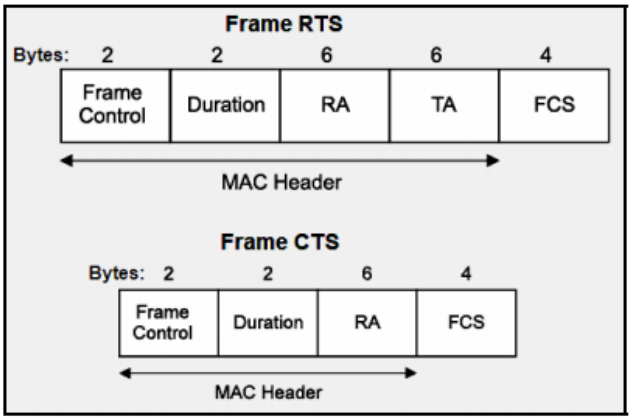


Figura 25. Tramas RTS y CTS

Fuente: http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F07+-+Capitulo+2.pdf

2.1.7 *Redes Inalámbricas Unificadas*

En esta sección se presentan las tendencias actuales de las redes inalámbricas específicamente se menciona sobre los aspectos de administración y gestión centralizadas para lo cual se describe algunas soluciones tecnológicas como Cisco Unified Wireless Network y componentes como: las Controladoras, Access Points, protocolos y software de gestión, además nuevas tendencias de gestión centralizada desde la nube para el caso de redes WLAN.

Actualmente hay un sin número de equipos Access Point o routers inalámbricos que permiten dar este servicio de movilidad a los usuarios, pero si se requiere un mayor número de Access Point para ciertas aéreas de cobertura dentro de una organización la administración de estos equipos se convierte en un dolor de cabeza porque cada dispositivo es independiente uno del otro de manera que no se tiene el control ni una gestión centralizada de la red inalámbrica y lo mismo percibe el usuario al tener que trasladarse de un lugar a otro y en cada lugar conectarse a diferentes redes inalámbricas estando aún en la misma organización.

Fabricantes como Cisco, HP, Ruckus, Motorola entre otros ofrecen soluciones de red inalámbrica unificada que permite tener una administración y control integrada para solventar las necesidades exigentes de comunicación actual por medio de recursos unificados cableados e inalámbricos. Estas soluciones se basan en un conjunto de herramientas de software, Puntos de Acceso, Bridges y Controladoras incluyendo servicios de seguridad.

El Fabricante Cisco por ejemplo ha creado el concepto de Cisco Unified Wireless Network (CUWN) que ayudan a solucionar los inconvenientes en despliegues a gran escala por medio de Wireless Lan Controller (WLC) que es el dispositivo que cumple el rol de CUWN. Además las funciones tradicionales de los Access Points como por ejemplo la asociación y la autenticación ahora la ejecuta el WLC, a estos AP se los conoce como Lightweight Access Points (LAPs) o Puntos de Acceso Ligeros en este entorno unificado (Cisco, 2008). A continuación en la Figura 26 se presentan equipos tanto Puntos de Acceso Indoor y Outdoor además de un Controlador Inalámbrico de la Familia Cisco que trabajan con el esquema CUWN.

Figura 26. Equipos Cisco con funcionalidad CUWN

Fuente: (Cisco, 2013)

Todas las configuraciones se realizan en el WLC de este modo un LAP descarga toda la configuración del controlador y actúa como una interfaz inalámbrica con el usuario. Las configuraciones más básicas que se realiza en el controlador son con respecto a las WLANs que se utilizarán, las interfaces virtuales que permiten configurar VLANs para cada WLAN y una vez que los LAP han sido reconocidos por la controladora y hayan descargado la configuración a éstos se los puede personalizar como por ejemplo: nombre, ubicación, dirección IP, administración vía telnet o SSH inclusive variar los canales en los que transmitirán los APs y los niveles de potencia, pese a que inicialmente la WLC configura dinámicamente estos parámetros.

Los WLC cuentan con interfaz gráfica amigable que permite una configuración y administración relativamente fácil, con esta interfaz se puede monitorear el estado de los Access Points, obtener estadísticas de usuarios por ejemplo cuántos están actualmente conectados a la red, mensajes de error que ayudan a controlar la disponibilidad de la red inalámbrica, configuración de los canales de operación, niveles de potencia entre otras. En la Figura 27 se muestra la interfaz gráfica de un WLC.

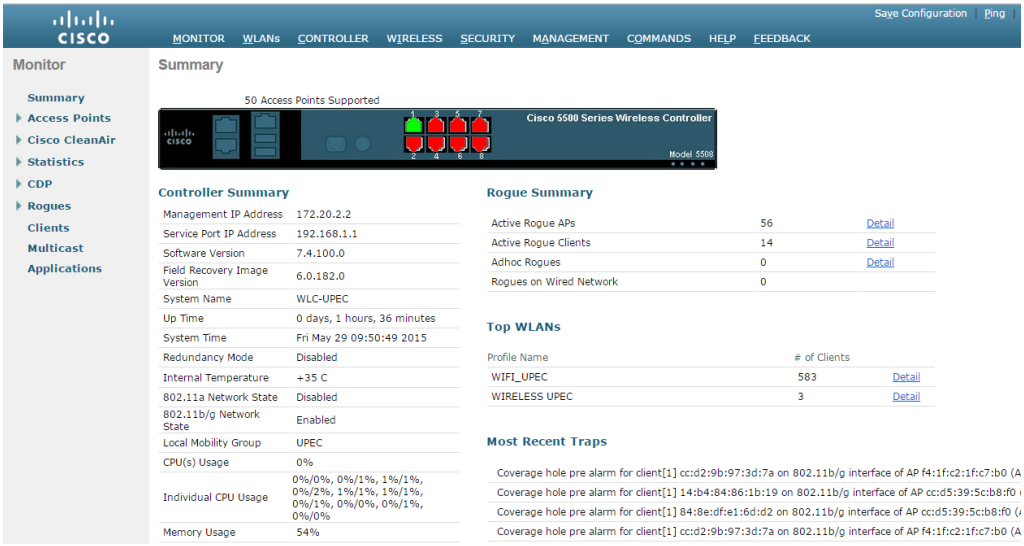


Figura 27. GUI Wireless Lan Controller Cisco

Fuente: (UPEC, 2015)

Para que un dispositivo tenga la capacidad de controlar un conjunto de Puntos de Acceso hacen uso de protocolos LWAPP (Lightweight Access Point Protocol) o CAPWAP (Control And Provisioning of Wireless Access Points), actualmente las soluciones de Cisco a partir de la versión de software 5.2 incorporan CAPWAP debido a que el tráfico de control es transmitido por un túnel DTLS[5] (Datagram Transport Layer Security) a diferencia de LWAPP que no utiliza este mecanismo, ofreciendo mayor seguridad al tráfico de control. LWAPP para capa 2 es obsoleto, pero LWAPP para capa 3 puede coexistir sin ningún problema con CAPWAP, de manera que los puntos de acceso con LWAPP pueden ser descubiertos y unirse a un controlador CAPWAP y actualizarse rápidamente.

Actualmente hay otras soluciones para administrar y gestionar de una manera centralizada una red inalámbrica desde la nube sin necesidad de contar con un hardware especializado para esta funcionalidad eliminando el gran costo económico de estos equipos, por ejemplo la solución Meraki puede gestionar Puntos de Acceso para interiores y exteriores solamente teniendo una conexión de Internet desde la cual se puede configurar, controlar usuarios inalámbricos y observar sus estadísticas de uso y conectividad véase la Figura 28.

[5]**DTLS:** Protocolo que proporciona privacidad en aplicaciones cliente-servidor

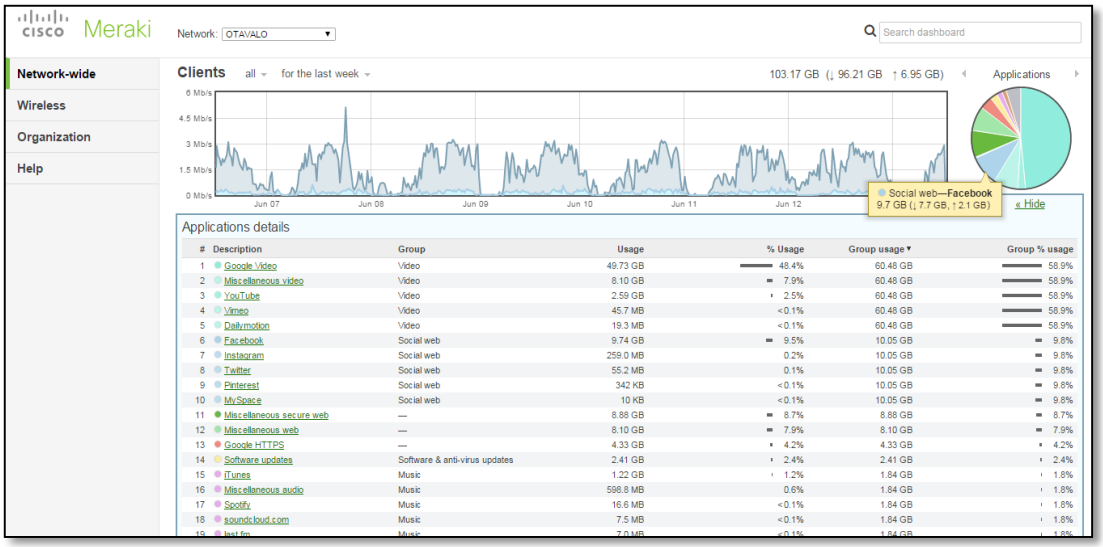


Figura 28. Meraki Browser para la gestión de Puntos de Acceso

Fuente: https://dashboard.meraki.com/

Finalmente, el crecimiento de estas tecnologías posibilita el establecimiento de nuevas tendencias como BYOD (Bring Your Own Device) o "trae tu propio dispositivo" en donde los usuarios de las organizaciones harán uso de sus tablets y smartphones para acceder a los recursos de la red utilizando la WLAN y por ende ésta debe garantizar alto rendimiento, gestión y seguridad con la finalidad de que el acceso de los usuarios sea totalmente transparente.

2.2 CALIDAD DE SERVICIO

La convergencia hoy en día es una de las características primordiales de las redes de comunicación, actualmente través de las infraestructuras de redes ya sea por medios como: fibra óptica, inalámbrico o cobre no solo se transmite datos sino que también tráfico de voz, video, multimedia, en general aplicaciones críticas y en tiempo real. Estos diferentes tipos de tráfico no tienen los mismos requerimientos en cuanto a: delay, jitter, descarte de paquetes y consumo de ancho de banda y por lo tanto la implementación de estos requiere de Calidad de Servicio, es decir mecanismos que garanticen su transmisión y recepción con parámetros aceptables y a satisfacción de los usuarios.

En este ámbito, las redes 802.11 ya no son una excepción debido a que sobre estas infraestructuras independientemente de su tamaño se usan para la transmisión y extensión de servicios convergentes o aplicaciones críticas y en tiempo real, razón por la cual es estrictamente necesario extender también las prestaciones de Calidad de Servicio a las WLANs.

2.2.1 *Introducción a la Calidad de Servicio*

La Calidad de Servicio o QoS (Quality of Service) según la UIT[6] se define como "el efecto global de la calidad del funcionamiento de un servicio que determina el grado de satisfacción de un usuario de dicho servicio".

Otras definiciones de QoS hacen referencia a la capacidad que tiene una red para proveer garantía y control en cuanto a la asignación de los recursos y diferenciación de servicios conforme a políticas de priorización de tráfico o aplicaciones, formuladas en base al entorno de cada organización.

Con los mecanismos de Calidad de Servicio implementados sobre una red es posible controlar los parámetros que influyen en la transmisión como son: latencia, jitter, pérdida de paquetes y consumo de ancho de banda de tal forma que se garantiza la disponibilidad y continuidad del servicio.

Gerometta (2009) señala que la implementación de Calidad de Servicio se basa en cuatro fases o etapas fundamentales que se explican a continuación:

- ***Identificación del Tráfico:*** consiste en reconocer los diferentes tipos de tráfico que circulan por la red por medio de auditorías con ayuda de herramientas ya sean basadas en software o hardware generalmente en horas pico o en las horas de mayor afluencia de tráfico.

[6]**UIT:** Unión Internacional de Telecomunicaciones.

- ***Clasificación de Tráfico:*** proceso fundamental de QoS responsable de categorizar el tráfico en clases identificado en el paso anterior, sin este mecanismo todo el tráfico es tratado de la misma forma, es decir sin prioridad (Modelo Best Effort).

- ***Marcado del Tráfico:*** mecanismo que permite identificar un paquete que pertenece a una clase mediante alguna marca para que sea distinguido al momento de aplicar la Política de QoS. La marcación de un paquete o trama se realiza utilizando algún campo destinado a este propósito básicamente en los encabezados de capa 2 y capa 3, siendo el marcaje en la capa de red el que permanece constante en una comunicación de extremo a extremo. En capa 3 se utiliza el campo ToS (Type of Service) del encabezado IP de 8 bits generando dos tipos de marcación: IP Precedence (utiliza 3 bits) y DSCP[7] (utiliza 6 bits); esta marcación utiliza el Modelo DiffServ[8]. En cuanto a la marcación en capa 2 en redes conmutadas se utiliza 3 bits del encabezado 802.1Q[9] denominados 802.1p para proporcionar hasta 8 clases, tanto DiffServ como 802.1p serán explicados ampliamente más adelante.

- ***Definición y aplicación de las Políticas:*** proceso que permite definir el nivel de servicio (SL) para cada clase de tráfico con la finalidad de dar un tratamiento especial y adecuado a cada uno de tal forma que se determina los requerimientos de ancho de banda, condiciones diferentes de delay, pérdida de paquetes, entre otros.

2.2.2 *Objetivos de la Calidad de Servicios*

Los objetivos que persigue la Calidad de Servicio dentro de la infraestructura de una red para dar respuesta a los diferentes requerimientos de las aplicaciones multimedia y en tiempo real son los siguientes:

- Controlar los recursos de la red mediante la asignación de ancho de banda estrictamente necesario dependiendo del consumo y exigencias de cada aplicación o servicio.

[7]**DSCP:** Differentiated Services Code Point o Punto de Código de Servicios Diferenciados
[8]**DiffServ:** Modelo de Servicios Diferenciados
[9]**802.1Q:** Estándar que especifica el etiquetado de tramas para la implementar VLANs

- Mejorar las prestaciones de las aplicaciones en tiempo real y sensitivas al retardo como la voz y video mediante la introducción de políticas de priorización a lo largo de la red y control de congestión.

- Maximizar el uso de la infraestructura de red mediante el uso eficiente de los recursos con el afán de garantizar la calidad de los servicios end-to-end de manera transparente a los usuarios.

- Facilitar a los administradores de red el manejo de los efectos de la congestión por medio de la generación de datos estadísticos y monitoreo de los recursos para verificar y evaluar el correcto funcionamiento de las políticas ya establecidas.

- Y finalmente proporcionar la convergencia de servicios en una red (voz, datos y video) de forma que se asegura y garantiza el nivel de satisfacción en función del número de usuarios y una alta disponibilidad para los diferentes tipos de tráfico.

2.2.3 *Parámetros de QoS*

Los parámetros que hay controlar y monitorear para garantizar la Calidad de Servicio y por ende posibilitar la convergencia de servicios son como se mencionó anteriormente la latencia, el jitter, la pérdida de paquetes y el ancho de banda; el éxito o fracaso de la implementación de QoS está en determinar los valores máximos y mínimos requeridos de cada parámetro en cada clase de servicio y su aplicación en la infraestructura de red. En breve se explica cada uno de los parámetros que influyen en QoS.

2.2.3.1 Retardo

El Retardo end-to-end se define como el tiempo que un paquete se toma desde el momento en que éste es enviado desde un punto de origen hasta su destino. Para determinar este parámetro se considera la suma de todos los retardos generados en todo el trayecto, así se tienen los

siguientes tipos de retardos que influyen directamente en la transmisión, que obviamente deben ser reducidos al mínimo para garantizar los servicios:

- ***Retardo por Procesamiento:*** tiempo en que tarda un dispositivo en tomar un paquete de la interfaz de entrada, examinarlo y colocarlo en la interfaz de salida.

- ***Retardo por encolamiento:*** Tiempo que se demora un paquete en la cola para ser despachado por la interfaz de salida.

- ***Retardo por Serialización:*** Tiempo que le toma a un dispositivo en colocar los bits de un paquete sobre el medio de transmisión.

- ***Retardo por Propagación:*** El tiempo necesario que le toma a un paquete en atravesar el medio de transmisión, éste varía dependiendo de las características del medio por ejemplo si el medio es Fibra óptica este retardo va a ser menor que un enlace inalámbrico o de radio.

2.2.3.2 Jitter

El Jitter es la variación en los tiempos de retardo de los diferentes paquetes que conformar un mismo flujo y se debe principalmente a que éstos paquetes son procesados, encolados y desencolados de manera independiente con lo cual al llegar a su destino cada uno llega con diferente retardo end-to-end afectando a la calidad de las aplicaciones en tiempo real, causado generalmente por la congestión del tráfico en un punto específico de la red. Para solventar este inconveniente la solución es utilizar un buffer que almacena todos los paquetes del mismo flujo antes de entregarlos a su destino de forma que se puede asegurar que todos lleguen en orden y a la misma velocidad aunque si se introduce un retardo adicional para el flujo.

2.2.3.3 Pérdida de Paquetes

La pérdida de paquetes mide en porcentaje la cantidad de paquetes que no han llegado a su destino debido principalmente a la falta de espacio en los buffers para la retención de paquetes entrantes en los momentos de congestión ocasionando su descarte que perjudica de manera sustancial a las aplicaciones en tiempo real. Para enfrentar este problema se puede aprovechar la retransmisión pero generando aún más congestión lo cual no es adecuado para las aplicaciones como la voz o el video IP en donde como consecuencia se puede obtener imágenes distorsionadas, audio desfasado, archivos dañados o una comunicación entrecortada. La manera adecuada de contrarrestar es a través de la utilización de mecanismos de encolamiento y técnicas de prevención de Congestión que deben ser definidas dentro de las políticas a aplicar en cada clase de tráfico.

2.2.3.4 Ancho de Banda

El Ancho de Banda es un término utilizado en redes de telecomunicación para referirse a la capacidad de un canal para transferir datos en un periodo determinado generalmente segundos (bits/s) a través de un sistema de comunicación digital de extremo a extremo. Esta capacidad es de gran importancia y se puede ver afectada o disminuida por razones como el retardo o la congestión que indudablemente podría repercutir en el performance de las aplicaciones.

Incrementar el Ancho de Banda implica también un incremento económico que puede contrarrestar momentáneamente algunas dificultades en la red pero conforme crece en número de usuarios y aplicaciones esta solución puede quedar limitada, siendo menester utilizar QoS mediante la clasificación, marcado y priorización del tráfico para utilizar adecuadamente este recurso indispensable.

2.2.4 *QoS en las WLAN IEEE 802.11e*

La expansión y crecimiento de las WLAN ha sido relativamente sorprendente ya que gracias a su aplicabilidad, bajo costo y movilidad se han convertido en un atractivo tanto para los sectores empresariales como redes de hogar y pequeña oficina. De la misma forma que se ha desarrollado la tecnología inalámbrica el estándar que la ampara ha tenido ciertas variantes con respecto a las posibilidades de transmisión, mejoras en la seguridad y calidad de servicio debido principalmente a las necesidades y requerimientos de los usuarios que contemplan hoy por hoy aplicaciones multimedia y en tiempo real, que para ser óptimas demandan el manejo adecuado especialmente de los parámetros de QoS.

En un principio el estándar IEEE 802.11 no estaba diseñado para el soporte de Calidad de Servicio, de manera que se centraba exclusivamente a controlar las colisiones a través de los mecanismos de acceso al medio DCF y PCF. En este entorno las posibilidades de DCF son servicios Best-Effort que se degradan aún más en situaciones de sobrecarga de la red y PCF no es lo suficientemente robusto como para garantizar los mínimos umbrales de los parámetros QoS de las exigencias actuales, lo que condujo a buscar la manera de aprovisionar QoS en las redes WLAN a través del grupo de trabajo 802.11e cuya enmienda fue publicada en el año 2005.

El estándar IEEE 802.11e es una propuesta que define los mecanismos para que una red inalámbrica WLAN proporcione QoS a las aplicaciones críticas y en tiempo real, contrarrestando las limitaciones típicas de este tipo de tecnologías (ancho de banda, pérdida de paquetes, delay y jitter elevados). En primera instancia haciendo el reconocimiento de nuevos elementos: QBSS (QoS Basic Service Set), QSTA (QoS Station) y QAP (QoS Access Point) e incorporando una tercera Función de Coordinación HCF (Hybrid Coordination Function) o Función de Coordinación Híbrida.

2.2.4.1 Función de Coordinación Híbrida

Con la aplicación de QoS a nivel de capa 2 por medio de 802.11e es posible que los Puntos de Acceso tengan la capacidad de tratar con prioridad a cierto tipo de tráfico de manera que los recursos compartidos de la WLAN se distribuyan entre diferentes aplicaciones lo que no ocurre normalmente con la operación de DCF y PCF ya que todos los dispositivos tienen igual oportunidad de transmitir resultando inadecuado para la VoIP, video streaming y otras aplicaciones sensibles. Para solventar esta dificultad se incorpora la Función de Coordinación Híbrida que implementa las siguientes mejoras:

- Proporciona dos métodos de acceso al canal: EDCA (Enhanced Distributed Channel Access) y HCCA (HCF Controlled Channel Access) que mejoran sustancialmente las funcionalidades de DCF y PCF correspondientemente, manteniendo la compatibilidad.

- Provee diferenciación de tráfico a través de la utilización del campo "QoS Control" de 16 bits en donde: del bit 0 a 7 están reservados para EDCA y del bit 8 a 15 para HCCA. Para el caso de EDCA, el método más común y extendido, se define cuatro categorías de acceso (AC) y ocho Prioridades de Usuario (UP) a nivel MAC, para esto se vale de los bits del subcampo TID (Identificador de Tráfico) cuyo etiquetado es idéntico a 802.1D[10] específicamente 802.1p para mapear a las categorías de acceso correspondientes.

- Incluye el concepto de TXOP (Oportunidad de Transmisión), que es un intervalo de tiempo durante el cual una QSTA tiene permiso para transmitir sus tramas, consta de un tiempo de inicio y una duración máxima y existen dos tipos dependiendo del método de acceso al canal en HCF de tal forma que puede ser EDCA-TXOP o HCCA-TXOP.

- Las tramas de confirmación ACK en 802.11e han pasado a ser opcionales, de esta manera si se decide no utilizarlas éstas no se enviarán por cada trama recibida correctamente mejorando el rendimiento de la capa MAC para aquel tráfico sensible al retardo pero a costa de disminuir la fiabilidad de la transmisión.

[10] **802.1D:** Estándar IEEE para bridges MAC, incluye el protocolo Spanning Tree y 802.1p

- Además se agrega dos nuevas funcionalidades: DLP (Direct Link Protocol) que permite la comunicación directa de estación a estación de un mismo BSS sin estar de por medio un Punto de Acceso como mecanismo para descongestionarlo y APSD (Automatic Power Save Delivery) para la gestión eficiente de energía totalmente útil en los teléfonos IP portables y cualquier otro dispositivo inalámbrico IP que funcione con baterías.

2.2.4.2 Campo QoS Control

La trama MAC 802.11 a efectos de proporcionar Calidad de Servicio en las redes inalámbricas de área local incrementa un nuevo campo denominado "QoS Control" de 2 bytes (veáse la Figura 29).

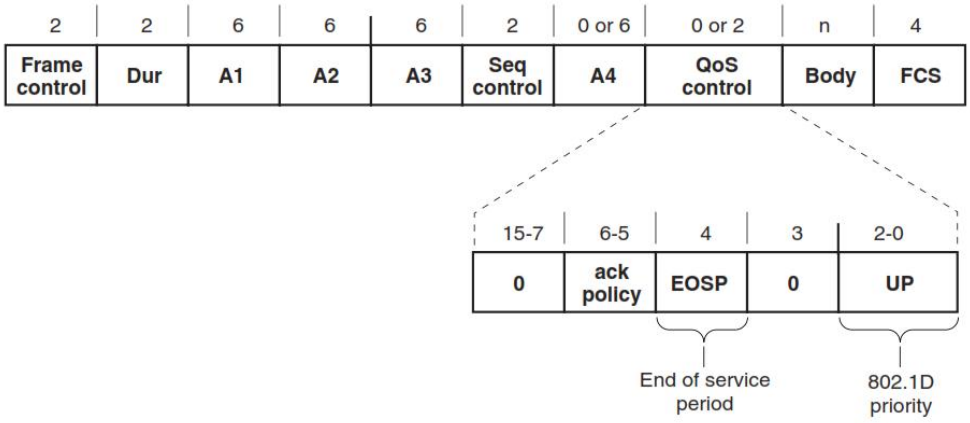


Figura 29. Campo QoS Control de la Trama MAC 802.11

Fuente: (Cisco, 2010)

Los 16 bits del campo QoS Control se distribuyen de la siguiente forma de acuerdo a una funcionalidad:

- **Bit 0 – 3:** Denominado TID (Traffic Indicator) de cuatro bits en donde los bits 0 a 2 se utilizan para identificar las ocho prioridades de usuarios de manera similar a 802.1D y el bit 3 se encuentra seteado en cero. El conjunto de MSDUs con la misma prioridad se refiere a una categoría de tráfico (TC).

- **Bit 4:** EOSP (End of Service Period), usado por el Punto de Acceso para indicar el final del período de servicio. Si este bit es 1 entonces el cliente puede volver a dormir.

- **Bit 5 – 6:** Conocido como ACK Policy y define la política ACK a utilizar después de la entrega de una trama QoS. Existen 4 políticas: ACK. No ACK, No Explicit ACK, Block ACK.

- **Bit 7:** Reservado para su uso futuro

- **Bit 8 – 15:** subcampo con una variedad de propósitos: TXOP limit, TXOP duration, AP PS buffer State, Queue Size.

    - *TXOP Limit:* Indica la oportunidad de transmisión otorgado por el AP.

    - *TXOP Duration Request:* El cliente usa este parámetro para indicar al AP cuánto tiempo requiere para su próximo TXOP.

    - *AP PS Buffer State:* Indica el estado del buffer de ahorro de energía para una STA particular.

    - *Queue Size:* O tamaño de la cola, un cliente utiliza este subcampo para informar al AP sobre el tráfico almacenado en el buffer y pendiente de enviar. El AP puede utilizar esta información para determinar la duración para el siguiente TXOP a ese cliente.

En la Tabla 7 se resume el mecanismo de utilización del campo QoS Control tanto para un Punto de Acceso como para una STA además se indica la funcionalidad de los bits 8 a 15 acorde al caso.

QoS Station	Bits 0-3	Bit 4	Bits 5-6	Bit 7	Bits 8-15
AP	TID/Access Class	EOSP	ACK Policy	Reserved	TXOP Limit
AP	TID/Access Class	EOSP	ACK Policy	Reserved	AP PS Buffer State
Client STA	TID/Access Class	0	ACK Policy	Reserved	TXOP Duration Requested
Client STA	TID/Access Class	1	ACK Policy	Reserved	Queue Size

Tabla 7. Campo QoS Control y propósitos de los bits 8-15

Fuente: (Nayanajith, 2014)

2.2.4.3 EDCA

EDCA (Enhanced Distributed Channel Access) es una nueva función de acceso al canal basado en contienda similar a DCF con algunas mejoras y diseñado para soportar la priorización de tráfico tal como lo hace DiffServ para grantizar QoS a lo largo de toda la infraestructura de red. Para esto se establecen cuatro categorías de acceso (AC) y ocho niveles de prioridad de usuario (UP) tal como se define en 802.1D. En la Tabla 8 se resume las prioridades y mapeo entre 802.1D y las categorías de acceso de 802.11e.

PRIORIDAD 802.1D	CATEGORÍA DE ACCESO (AC)	AC 802.11e	DESCRIPCIÓN 802.11e
1 & 2	AC0	AC_BK	Background
0 & 3	AC1	AC_BE	Best Effort
4 & 5	AC2	AC_VI	Video
6 & 7	AC3	AC_VO	Voice

Tabla 8. Mapeo de prioridades de usuario a las categorías de acceso

Fuente: (IEEE Std 802.11e™-2005, 2005)

Para dar trato preferencial a las aplicaciones o Categorías de Acceso EDCA introduce dos métodos:

- ***Primer método:*** Asignación de distintos IFS a cada categoría de Acceso a través de un nuevo tiempo de espera denominado AIFS (Arbitration InterFrame Space) utilizado para realizar la diferenciación entre distintos AC. Un AC de mayor prioridad tendrá un AIFS más corto que un AC de más baja prioridad, esto implica que las STA de alta prioridad esperarán menos tiempo para acceder al medio (veáse Figura 30). La expresión para determinar el AIFS según (Villalón, Cuenca & Orozco, 2006) es:

$$AIFS\,[AC] = AIFSN[AC] \times aSlotTime + SIFS$$

AIFSN (Arbitration InterFrame Space Number)

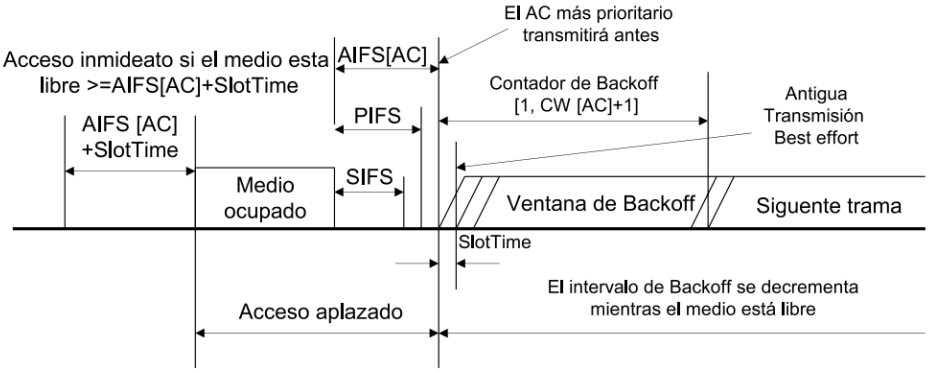


Figura 30. Espacio entre Tramas Arbitrario AIFS

Fuente: (Villalón et al., 2006)

- ***Segundo método:*** Asignación de distintos tamaños de ventana CW (Contention Window) mínimo y máximo para cada Categoría de Acceso, con la finalidad de conceder menores tiempos de espera a las estaciones con tráfico prioritario cuando se tenga que efectuar Backoff. (Erazo, Arana, Meza & Pérez, 2009) señalan que cada estación recibe los parámetros de contención en la trama beacon en el elemento "EDCA Parameter Set".

Otro factor diferencial con respecto a DCF es TXOP Limit u Oportunidad de Transmisión que limita el tiempo en el que una STA tiene los derechos para transmitir de manera que no se monopolice el medio inalámbrico y para que tampoco las otras estaciones disputen por el canal.

En resumen la priorización entre las diferentes categoría de acceso depende de la configuración de los parámetros antes indicados (AIFS, CWmin, CWmax y TXOP), en la Figura 31 se puede apreciar la categorización en clases y los métodos para asignar prioridad en EDCA.

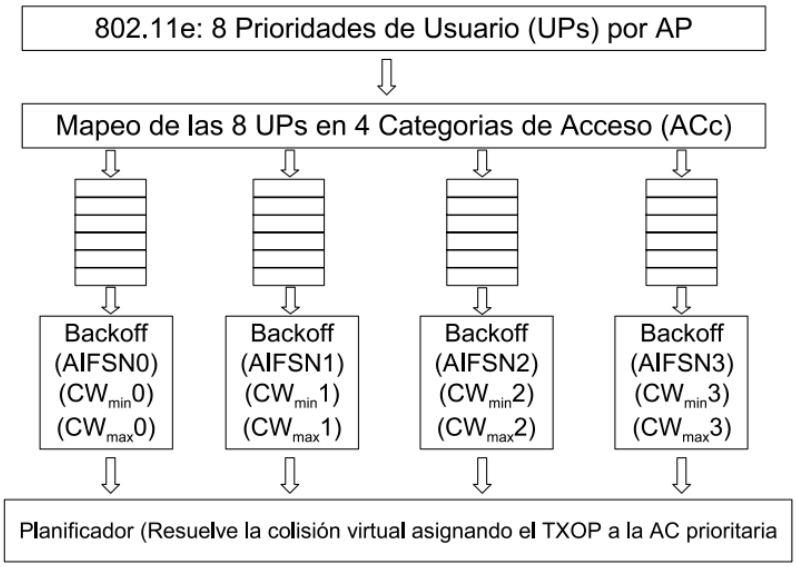


Figura 31. Categorización y priorización en EDCA

Fuente: (Villalón et al., 2006)

De acuerdo con (Erazo et al., 2009) una vez que los datos llegan al Punto de Acceso se cumple el siguiente proceso:

- La capa MAC 802.11e se encarga de clasificar y enviar las MSDU a las colas correspondientes, entonces estas MSDU de diferentes colas (AC) compiten internamente por el EDCA-TXOP que es controlado por el QAP y se transmite a las QSTA en las tramas beacon, en la Figura 32 se presenta el mecanismo de EDCA-TXOP.

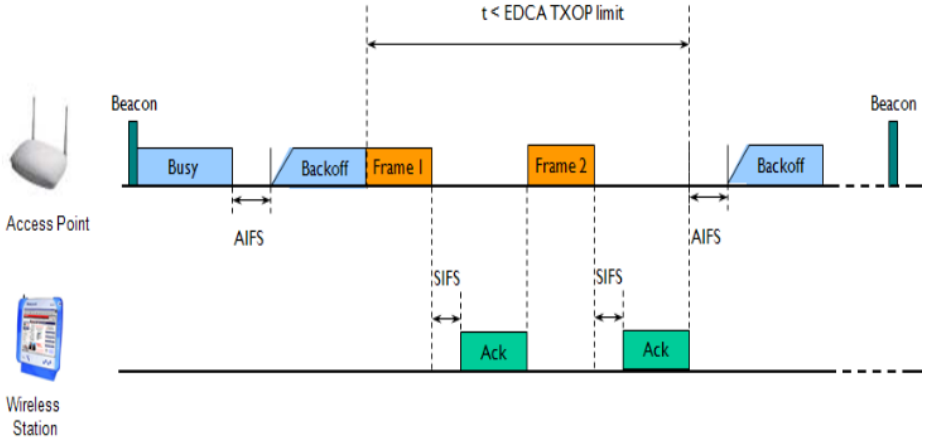


Figura 32. EDCA-TXOP

Fuente: (Darapuneni, 2009)

- El algoritmo de contienda interno calcula Backoff independientemente para cada cola (CA) según los parámetros especificados (AIFS, CWmin y CWmax) de manera que la cola con menor Backoff ganará la competición interna.

- La cola vencedora competirá externamente por el acceso al medio inalámbrico, cabe recalcar que el algoritmo de contienda externa no se ha modificado significativamente en comparación con DCF, a excepción de que en DCF el algoritmo de Backoff y tiempos de esperan son fijos mientras que en 802.11e son variables y configurados de acuerdo a la cola AC.

En el caso en que dos o más AC pertenecen a una misma QSTA y termina el mecanismo de Backoff en el mismo instante, ambos AC intentarán mandar los datos produciéndose una colisión, que en el estándar se ha denominado colisión interna. Siempre que esto se produzca, la capa MAC ofrecerá la oportunidad de transmisión al tráfico más prioritario, tratando el de menor prioridad igual que si se hubiera producido una colisión real.

2.2.4.4 HCCA

HCCA (HCF Controlled Channel Access) define otro mecanismo más avanzado y complejo para acceder al medio basado en períodos con contención (CP) y períodos libres de contención (CFP). Utiliza el sondeo controlado por el coordinador híbrido (HC) en este caso un QAP para ajustar la Calidad de Servicio con gran precisión con soporte para tráfico parametrizado y compatible con IntServ (Servicios Integrados), es opcional y menos extendido a comparación de EDCA de manera que es soportado por un número muy reducido de sistemas. A continuación las características más importantes de HCCA:

- Un HC tiene la capacidad de sondear tanto en CP como en CFP y otorga un TXOP a las QSTA que restringe la duración del acceso al medio. Bajo HCCA, las estaciones no compiten por el acceso al medio inalámbrico, pero confían en este Punto de Acceso para sondear con regularidad y así ganar acceso al canal, en este sentido, es similar PCF.

- HCCA maneja flujos de tráfico (TS), un TS es un conjunto específico de MSDUs viajando en una dirección sujeto a unas limitaciones de QoS específicas. Un TS en el enlace ascendente (hacia el AP) es identificado por su Identificador de Flujo de Tráfico (TSID) y la dirección mientras que en el enlace descendente (hacia la estación) es identificado por su TSID, dirección y la dirección de la estación. El AP puede soportar hasta ocho TS tanto en el enlace ascendente como en el descendente por cada estación asociada y utiliza para esta función los bits 8 a 15 del campo QoS Control. En la Tabla 9 se muestra una comparación entre el TSID (HCCA) y TID (EDCA).

HCF	Bits	Utilización
EDCA	0-7	TID, UP (Prioridades de Usuario)
HCCA	8-15	TSID, parametrización de QoS (TS)

Tabla 9. Campo QoS Control EDCA vs HCCA

Fuente: (IEEE Std 802.11e™-2005, 2005)

- La duración del período HCCA-TXOP se transmite a las estaciones QSTA directamente por el HC como parte de la trama QoS CF-Poll después de un PIFS y sin presencia de

Backoff. Pero también puede realizarse con la trama QoS (+)CF-Poll, cuando esto ocurre la QSTA tiene una duración límite especificada en el subcampo TXOP Limit (bits 8 a 15 del campo QoS Control), tal como se muestra en la Tabla 10.

Applicable frame subtypes	B0–B3	B4	B5–B6	B7	B8–B15
QoS (+)CF-Poll sent by AP	TID	EOSP	Ack Policy	A-MSDU Present	TXOP Limit
QoS Data, QoS Data+CF-Ack, QoS Null sent by AP		EOSP			AP PS Buffer State
QoS Data frames sent by non-AP station		0			TXOP Duration Requested
		1			Queue Size

Tabla 10. Bits del Campo QoS Control en HCCA

Fuente: (Perahia & Stacey, 2013)

- Finalmente, las QSTA están en la capacidad de requerir información acerca del estado de las colas de otras estaciones y también de mostrar dicha información que puede ser utilizada para dar prioridad a una estación sobre otras con el fin de especificar sus parámetros de transmisión (date rate, jitter, entre otros), mejorando la eficiencia de la WLAN. En la Figura 33 se presenta el esquema general del funcionamiento de HCCA.

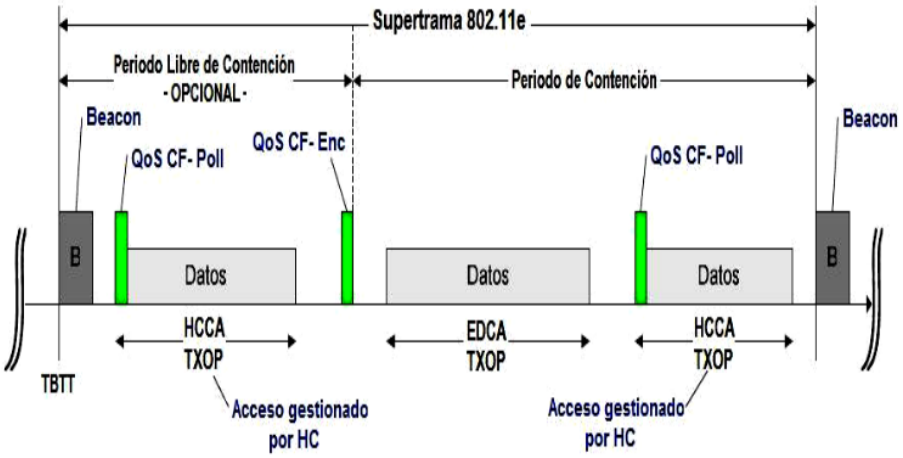


Figura 33. Esquema de Funcionamiento de HCCA

Fuente: (Erazo et al., 2009)

2.2.4.5 WMM

Para acelerar la adopción de tecnologías de Calidad de Servicio en las redes WLAN y mientras se realizaba la aprobación del estándar IEEE 802.11e la Alianza Wi-Fi desarrolló WMM o Wi-Fi Multimedia (versión certificada de EDCA) en el 2004, con la finalidad de facilitar la extensión e interoperabilidad de QoS en redes inalámbricas adoptando el mecanismo de clasificación de las redes cableadas. De esta forma el tráfico marcado que se recibe en el Punto de Acceso por la red cableada ya sea con 802.1p o DSCP será remarcado en 802.11 brindando prioridad a los diferentes tipos de tráfico que esta vez utilizan el medio inalámbrico (Gerometta, 2009).

Como se mencionó anteriormente WMM constituye la certificación de EDCA manteniendo el mismo esquema de trabajo, Categorías de Acceso y Niveles de Prioridad como en la versión original 802.11e. Cabe resaltar que algunos fabricantes que cuentan con esta certificación para sus soluciones WLAN renombran estas categorías de la siguiente manera: Platino (AC_VO), Oro (AC_VI), Plata (AC_BK) y Bronce (AC_BE), citando un ejemplo: el tráfico con más alta prioridad pertenecería a la clase Platino y será enviado antes que las clases Oro, Plata y Bronce (véase Tabla 11).

TIPO DE TRÁFICO	CATEGORÍA DE ACCESO WMM	NIVEL DE PRIORIDAD 802.11e (802.1p/802.1D)
VOZ	PLATINO (AC_VO)	6 o 7
VIDEO	ORO (AC_VI)	4 o 5
BACKGROUND	PLATA (AC_BK)	1 o 2
BEST EFFORT	BRONCE (AC_BE)	0 o 3

Tabla 11. Categorías de Acceso WMM

Fuente: (Gerometta, 2009)

En EDCA y por lo tanto en WMM se hace referencia o dos métodos para la priorización del tráfico una vez clasificado, estos métodos corresponden a la asignación de Tiempos de Espera Arbitrario (AIFS) y de la Ventana de Contención (CWmin y CWmax). Si los valores de AIFS y CW para una clase son los más pequeños se trata de tráfico de alta prioridad y si por lo contrario son los más altos se refiere a tráfico de muy baja prioridad. En la Figura 34 se puede apreciar los parámetros mencionados para cada una de las Categorías de Acceso.

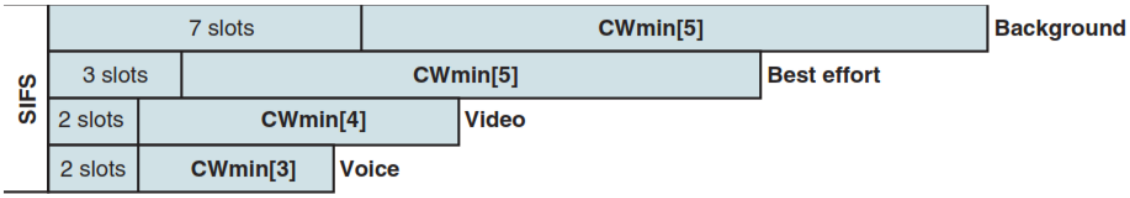


Figura 34. Métodos de Priorización para AC en WMM

Fuente: (Cisco, 2010)

Adicionalmente las AC de alta prioridad tienen más probabilidad de obtener una Oportunidad de Transmitir (TXOP) que las otras clases lo cual también favorece al envío de los paquetes con QoS. En la Tabla 12 se presentan los parámetros de priorización por Categoría de Acceso tanto para STA como para los AP, se presentan de manera separada ya que son ligeramente diferentes debido principalmente a que un Punto de Acceso puede tener varios clientes y debe enviar tramas más a menudo.

Access Category	CWmin	CWmax	AIFSN	TXOP Limit (802.11b	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	1	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	1	3.264 ms	1.504 ms

(a)

Access Category	CWmin	CWmax	AIFSN	TXOP Limit (802.11b	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264 ms	1.504 ms

(b)

Figura 35. (a) Parámetros WMM para un AP. (b) Parámetros WMM para un Cliente

Fuente: (Cisco, 2010)

Antes de la implementación de QoS (WMM) en una red inalámbrica es importante tomar en cuenta las siguientes observaciones:

- La mayoría de los dispositivos wireless disponibles en el mercado actualmente tienen soporte WMM y por lo tanto facilitan la extensión de QoS en una infraestructura de red.

- Para poder disfrutar de los beneficios de WMM en una WLAN se debe cumplir con las siguientes condiciones: el Punto de Acceso, el cliente o estación inalámbrica y la aplicación deben soportar y tener habilitado WMM (Erazo et al., 2009).

- Los dispositivos antiguos que no soportan WMM pueden funcionar en redes WLAN con WMM habilitado.

- En WMM el uso de HCCA es opcional inclusive se la denomina WMM-SA (Scheduled Access) pero esta certificación no llegó a concretarse a consecuencia de resultar compleja y menos extendida.

- Los paquetes que no se hayan asignado a una Categoría de Acceso son clasificados por defecto como una clase Best Effort (AC_BE).

En resumen WMM es una solución de QoS interoperable basada en la IEEE 802.11e con todo el apoyo de la industria, que cumple con los requisitos de todos los segmentos del mercado y de alcance mundial constituyéndose como una base sólida para el crecimiento y la extensión de la Calidad de Servicio a través de las redes WLAN mejorando enormemente la experiencia del usuario final, proporcionando el uso más amplio y eficiente de las redes inalámbricas de área local (Erazo et al., 2009).

2.2.4.6 TSpec Admission Control

Un flujo de tráfico es un conjunto de MSDUs que se entregan con la misma Especificación de Tráfico (TSpec). La Especificación de Tráfico es un elemento de información en las tramas Management con un nuevo subtipo (Action Management) que contiene las características de los flujos como: tamaño de los paquetes, velocidad mínima PHY, retardo permitido, entre otros. Es relativamente importante debido al limitado ancho de banda disponible en el medio inalámbrico, a través de este control es posible evitar problemas de congestión y por ende la degradación del performance de la WLAN. El estándar IEEE 802.11e especifica el uso de TPsec en los dos mecanismos de acceso al medio EDCA y HCCA.

El propósito de TSpec Admission Control es no negar el acceso a los clientes de la WLAN y proteger los recursos de alta prioridad de manera que limita la admisión a una categoría de acceso básicamente AC_VI y AC_VO, restringiendo la latencia de los flujos que trabajarán con QoS y además previniendo que muchos flujos sean encolados al mismo tiempo en una clase con el afán de garantizar el ancho de banda para las aplicaciones más prioritarias. Antes de generarse una solicitud TSpec el Punto de Acceso anuncia en una trama beacon si el control de Admisión es obligatorio para cualquier categoría de acceso en el subcampo AC Parameter bit ACM o Admission Control Mandatory (véase Figura 36).

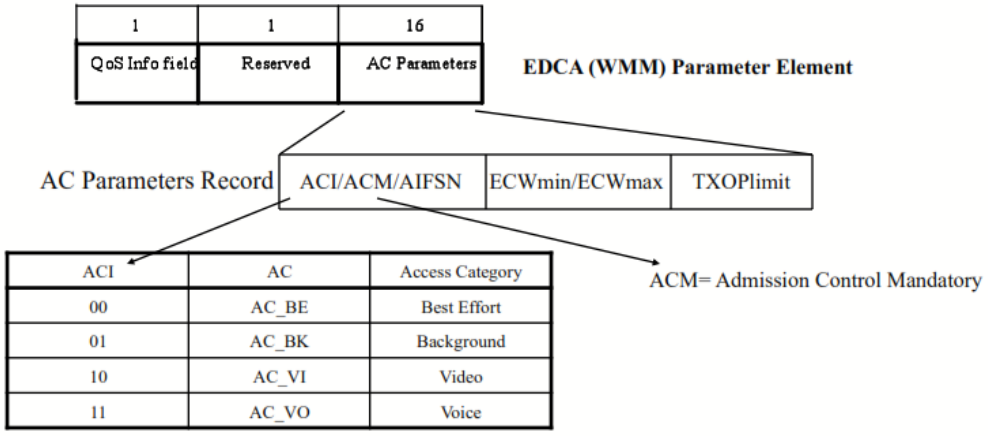


Figura 36. EDCA/WMM Parameter Element

Fuente: (Graham, 2008)

Posteriormente, la trama Action Management puede tener diferentes valores de acuerdo a una funcionalidad determinada como puede ser: trama ADDTS (Add Traffic Stream) Request o ADDTS Response y dentro de éstas especificarse el TSpec. Es importante mencionar que además los mensajes de asociación y re-asociación también pueden incluir el elemento TSpec cuando un cliente requiere asociarse con otro AP. En conclusión el objetivo de tener conocimiento sobre los parámetros (tasas de datos, tamaños de la trama, tasa de transmisión PHY, prioridad por usuario y delay permitido) es para permitirle calcular al AP si cuenta o no con los recursos para satisfacer la demanda con Calidad de Servicio. En la figura 37 se presenta los componentes del elemento TSpec de la trama ADDTS (Action Management).

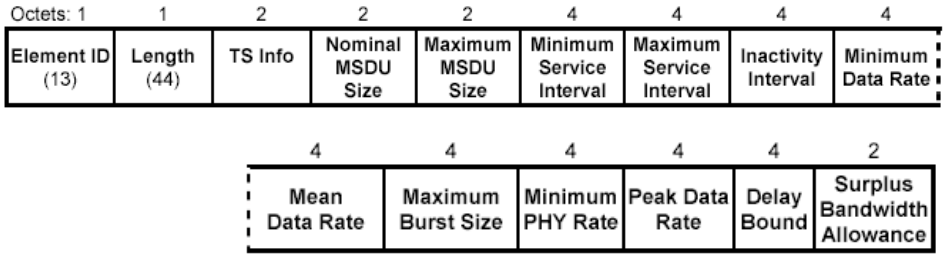


Figura 37. Elemento TSpec en una Trama de Solicitud ADDTS

Fuente: (IEEE Std 802.11e™-2005, 2005)

2.2.5 Otras Arquitecturas de QoS, Modelo DiffServ

A lo largo de este estudio se ha mencionado que es menester aplicar Calidad de Servicio para el soporte de aplicaciones críticas y en tiempo real en las WLAN, pero para posibilitar el QoS en una red de extremo a extremo es imprescindible aplicar otros mecanismos a nivel de capa 3. El IETF (Internet Engineering Task Force) atendiendo a este requerimiento propone dos formas diferentes para afrontar el soporte de Calidad de Servicio:

- ***IntServ (Integrated Services):*** Modelo de Servicios Integrados, utiliza el protocolo RSVP[11] (Resource Reservation Protocol) para la reserva de los recursos de cada flujo de tráfico en cada salto (router) con la finalidad de asegurar los requerimientos necesarios (encolamiento, capacidad de procesamiento, entre otros) en la comunicación end-to-end.

  Esta propuesta se desarrolló de manera emergente para mejorar la administración de los recursos de la red principalmente del ancho de banda con la aparición de nuevas aplicaciones como VoIP y video streaming. IntServ está basado en una arquitectura del mejor esfuerzo pensando en que la gestión de estos recursos constituye un punto clave para determinar la Calidad de Servicio. Sin embargo este mecanismo presenta desventajas con referencia al mantenimiento de la información de señalización generada por cada flujo de tráfico y como consecuencia provoca un overhead[12] por paquete afectando directamente al núcleo de la red siendo no opto para implementaciones a gran escala.

- ***DiffServ (Differentiated Services):*** Modelo de Servicios Diferenciados, proporciona Calidad de Servicio a nivel capa de red evitando los inconvenientes presentados en el Modelo IntServ por medio de la creación de agregados de tráfico identificados unos de otros por una marca en los paquetes, de modo que cada marca de paquetes corresponde

[11]**RSVP:** Protocolo de red y señalización en IntServ para la reserva de los recursos para cada flujo de tráfico.
[12]**Overhead:** Información de control o secuencia adicional a la carga útil de un paquete.

a una clase de tráfico a la cual se le debe asignar una política de priorización para ser reenviado por la red. Los puntos clave para la diferenciación del tráfico en DiffServ es la clasificación y marcaje.

2.2.5.1 Clasificación y Marcaje en DiffServ

La clasificación y marcaje del tráfico posterior al análisis exhaustivo de los paquetes para definir sus prioridades constituye el pilar fundamental de QoS, sin estos dos métodos todos los paquetes son tratados de la misma manera es decir como una clase Best Effort. Para realizar la categorización del tráfico se utilizan dos descriptores: IP Precedence y DSCP de la cabecera del paquete IP. Estos dos descriptores utilizan los bits del campo ToS (Type of Service) para proporcionar la diferenciación del tráfico (véase la Figura 38). Con respecto al datagrama IPv6 soporta el mismo campo ToS para la asignación de QoS pero con la denominación Traffic Class.

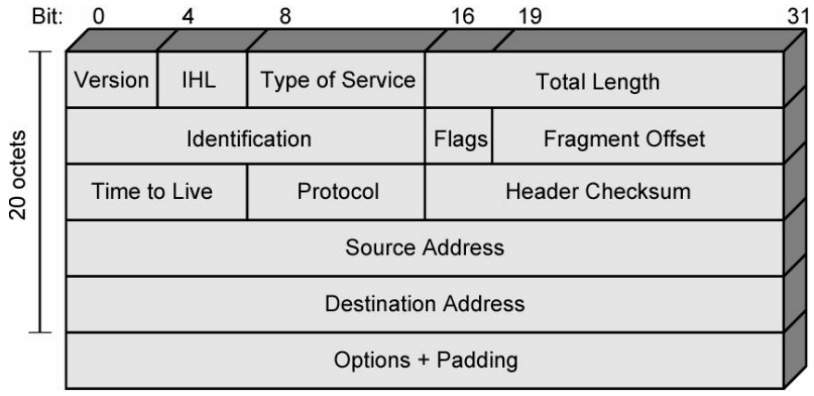


Figura 38. Campo ToS del datagrama IPv4

Fuente: http://ipv4to6.blogspot.com/p/protocolo-ip.html

Inicialmente se utilizaban los tres primeros bits más significativos "IP Precedence" para obtener hasta ocho niveles de servicio, los dos valores máximos están reservados para la utilización interna de la red, teniendo disponible seis clases. En la Figura 39 se puede apreciar la estructura del campo ToS.

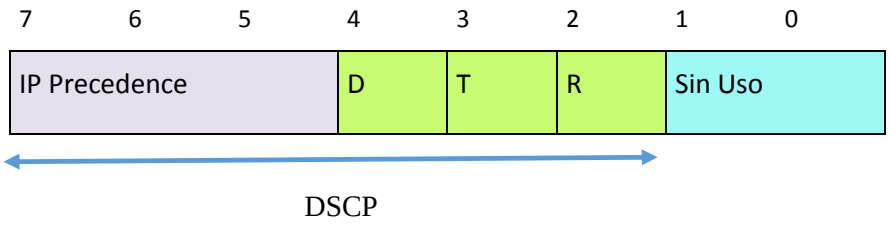


Figura 39. Estructura del campo ToS

Fuente: Propia

Los bits D (Delay), T (Throughput) y R (Reliability) fueron creados para especificar el retardo, flujo de salida, fiabilidad y requisitos de coste, actualmente en el modelo DiffServ determinan las características del servicio, ya que se utilizan los 6 bits para la definición de clases teniendo hasta 64 niveles de servicio. Los 6 bits en conjunto toman el nombre de DSCP (DiffServ Code Point) y cada valor DSCP recibe un tratamiento diferente en los nodos de red guardando compatibilidad con IP Precedence (véase Figura 39).

En DiffServ el grupo de paquetes con el mismo valor DSCP se denominan BA (Behavior Aggregate) y esperan el mismo tratamiento en los nodos de la red, a este tratamiento se le denomina PHB (Per Hop Behavior) y depende del SLA (Service Level Agreement) o política acordada. El PHB que puede recibir cada grupo de paquetes con la misma marca implica asignación en el tipo de encolamiento, reserva de ancho de banda, preferencias de dropping, priorización, entre otros. Por medio del valor DSCP se pueden definir 4 tipos de PHB en el modelo DiffServ:

- ***Default:*** Clase Best Effort, se caracteriza por tener los tres primeros bits DSCP en cero, los siguientes dos bits se utilizan para marcar alguna prioridad dentro de este mismo grupo y el ultimo bit en este PHB y en los restantes se encuentra en cero.

- ***EF (Expedited Forwarding):*** Tiene un valor DSCP igual a 101110, la más alta prioridad generalmente asignada a las aplicaciones sensibles como la VoIP, garantiza un retardo mínimo, bajas pérdidas de paquetes y un ancho de banda garantizado, es

decir provee el más alto nivel de QoS, en la Figura 40 se puede apreciar el valor DSCP para el PHB EF (46d), en donde los tres primeros bits corresponde al IP Precedence con un valor decimal 5 y los dos bits siguientes indican que no existe probabilidad de descarte para esta clase.

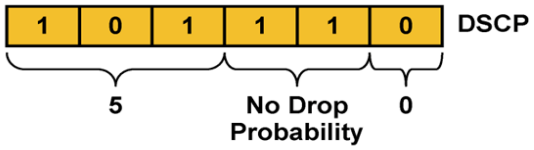


Figura 40. PHB Expedited Forwarding

Fuente: (Cisco, 2009)

- ***AF (Assure Forwarding):*** Constituye un PHB que ofrece un trato preferente, garantiza un ancho de banda y en caso de necesitar un extra lo permite si es que está disponible. Existen 4 subclases en este grupo (AF1, AF2, AF3 y AF4) a las cuales es posible asignarles una cantidad de recursos acorde a los SLA establecidos. Además define 3 categorías para la probabilidad de descarte (alta, media y baja) siendo como resultado 12 subclases. En la Figura 41 los tres primeros bits "a" representan el valor binario de la clase en decimales (1, 2, 3 y 4), los bits "d" indican la probabilidad de drop en donde 01 es la mínima probabilidad y 11 la máxima probabilidad.

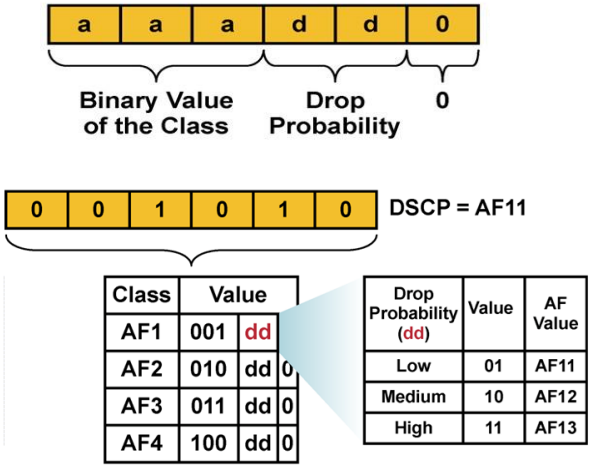


Figura 41. PHB Assure Forwarding

Fuente: (Cisco, 2009)

- ***Class-Selector:*** Se caracteriza por utilizar los tres primeros bits DSCP de manera que genera ocho tipos de comportamientos e igual que IP Precedence la clase 6 y 7 están reservadas, los tres últimos bits se encuentran en cero.

A continuación en la Figura 42 se presenta un resumen de los cuatro tipos de PHB en el modelo DiffServ y los valores o marcas para cada uno, adicionalmente cabe señalar que la clase AF es compatible con una única clase IP Precedence por ejemplo AF1 coincide con IP Precedence 1, AF2 con IP Precedence 2, etc.

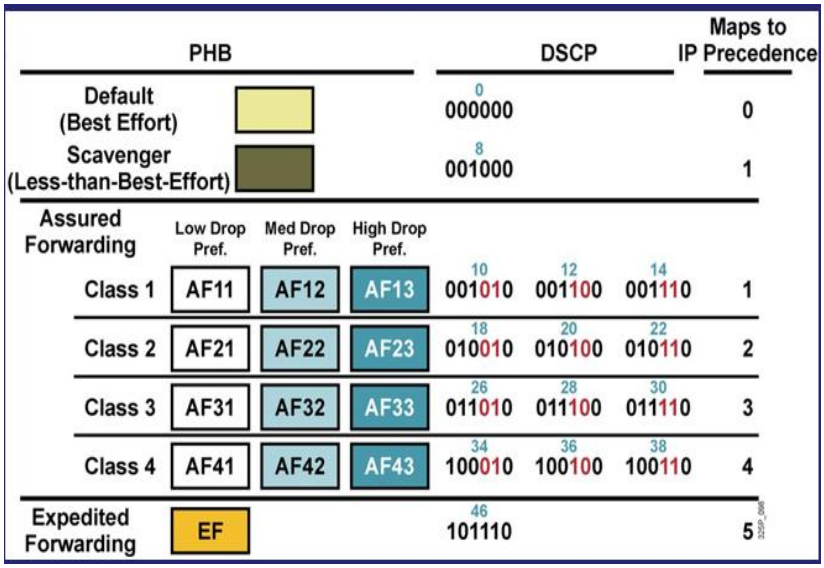


Figura 42. PHB y los valores DSCP correspondientes

Fuente: (Cisco, 2009)

2.2.5.2 Compatibilidad 802.1p

Los bits del campo ToS del datagrama IP pueden ser mapeados a los bits del campo PRI (Prioridad) de la etiqueta 802.1Q en la trama Ethernet para brindar CoS (Class of Service) a nivel de capa 2 en una red LAN. CoS corresponde a un esquema de clasificación de tráfico cuya diferencia con QoS radica en que no garantiza un ancho de banda o retardo mínimo como ocurre con los PHB de DiffServ, simplemente es un mecanismo de ayuda para los administradores al

momento de solicitar prioridad basándose en la importancia que tiene este tráfico dentro de la red o en base a las políticas ya establecidas.

Los 3 bits PRI (IEEE 802.1p) posibilitan el soporte de 8 CoS o Clases de Servicios a nivel de capa 2, en la Figura 43 se puede verificar la correspondencia de 801.p e IP Precedence para asegurar total consistencia de QoS end-to-end.

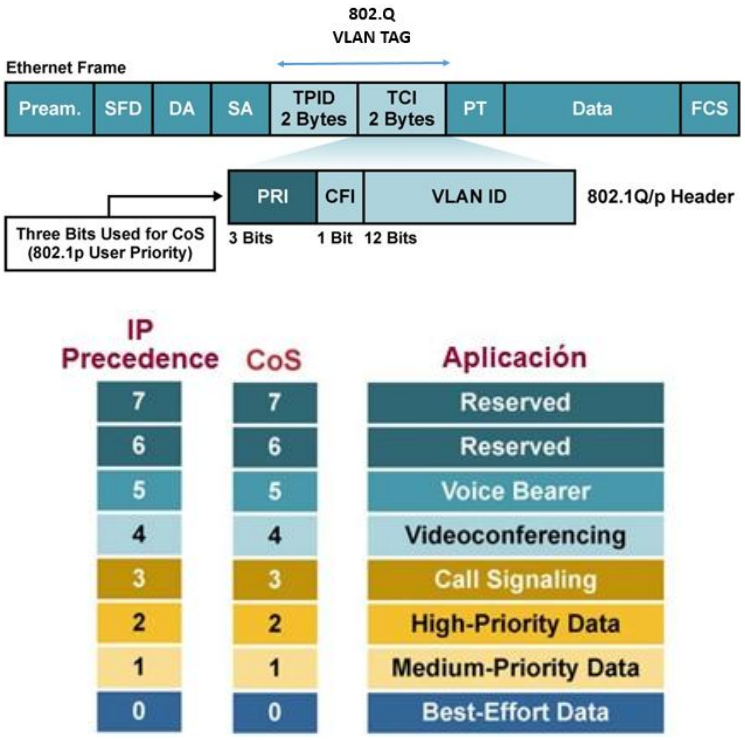


Figura 43. Correspondencia 802.1p e IP Precedence

Fuente: (Cisco, 2009)

Actualmente el valor IP Precedence es parte de DSCP de forma que estos dos valores no pueden ser configurados de manera simultánea en los equipos de red pero si esto ocurre el paquete quedará marcado con DSCP. Una de las ventajas más importantes de utilizar DSCP con relación a IP Precedence es la cantidad de clases o niveles de servicio que se pueden alcanzar por ejemplo con DSCP hasta 64 niveles y con IP Precedence hasta 8, éste último limita el crecimiento de aplicaciones multimedia y escalabilidad en la red.

2.2.5.3 Encolamiento o Control de Congestión

Una vez realizada la clasificación y marcaje del tráfico ya sea en DSCP o IP Precedence es necesario aplicar las políticas que garantizarán la prioridad de los paquetes, estás políticas tienen relación con la asignación de las técnicas de encolamiento o control de congestión aplicables a cada clase sobre todo en aquellas que requieren un tratamiento especial frente a otras. Es de suma importancia la utilización de estos mecanismos para contrarrestar los inconvenientes generados por la congestión y ésta ocurre generalmente debido a las siguientes situaciones:

- ***Desajuste de velocidad:*** Es decir la interfaz de entrada de los paquetes es de mayor velocidad que la interfaz de salida, causa más común de la congestión.

- ***Problema de Agregación:*** El tráfico de muchas interfaces convergen en una sola interfaz de salida o si el tráfico de múltiples flujos o aplicaciones confluyen en una sola interfaz (Problema de Confluencia).

(Cisco, 2009) define al Encolamiento como una técnica usada para controlar la congestión generada en una interfaz de salida en un dispositivo de red, creando colas (queues), reteniendo los paquetes y planificando su re-envío, caso contrario su desecho es indiscriminado a causa de los inconvenientes ya indicados anteriormente. En la Tabla 12 se presentan los algoritmos de encolamiento más comunes:

TÉCNICA DE ENCOLAMIENTO	**CARACTERÍSTICAS**
FIFO (First In First Out)	"El primer paquete en entrar es el primero en salir", es el algoritmo de encolamiento más simple y recomendado para interfaces de alta velocidad con poca probabilidad de congestión.
PQ (Priority Queue)	Dispone de 4 colas de prioridad: Alta, Media, Normal y Baja. Las colas se van despachando por orden pero vaciándose completamente las de más alta prioridad antes de seguir con las

	siguientes. Bajo este mecanismo las colas de baja prioridad pueden quedar desatendidas e incurrir en el trail drop.
RR (Round Robin)	Define varias colas pero atendidas por igual, es decir sin ningún tipo de priorización. Este mecanismo consiste en despachar un paquete de cada cola y luego repetir este proceso.
WRR (Weighted Round Robin)	Versión modificada de RR, asigna prioridad a cada cola basada en el "weight" o peso y puede ser medido en bytes. A mayor valor de weight mayor prioridad tendrá la cola, pero tiene un inconveniente ya que despacha un número determinado de bytes de cada cola (umbral de envío) y si éste es superado con frecuencia puede afectar al ancho de banda de la interfaz.
WFQ (Weighted Fair Queuing)	Divide el tráfico en flujos, provee una división justa del ancho de banda de la interfaz, asignando una atención más rápida a los flujos interactivos de bajo volumen (VoIP) y más ancho de banda a los de alta prioridad pero penalizando a aquellas de más alto volumen ya que no las asocia como aplicaciones en tiempo real. WFQ al ser un mecanismo que clasifica en flujos no posibilita la configuración manual de las clases y tampoco la asignación de BW fijos para cada una.
CBWFQ (Class Based Weighted Fair Queuing)	Resuelve las limitaciones de PQ, WRR y WFQ ya que permite la creación de colas para cada clase de tráfico, cada cola es asignada a un determinado ancho de banda a criterio del administrador. Con este mecanismo se pueden disponer de hasta 64 colas una por cada clase, cada cola es FIFO y provee un BW garantizado con un límite máximo de paquetes pero aun así no provee un servicio apropiado (bajo retardo) para las aplicaciones en tiempo real como la VoIP.
LLQ (Low Latency Queue)	Basado en CBWFQ incluye colas prioritarias para el tráfico sensible y en tiempo real con garantías de bajo retardo y una reserva de ancho de banda mínimo.

Tabla 12. Técnicas de Encolamiento y Control de Congestión

Fuente: Propia

2.2.5.4 Prevención de Congestión

A pesar de la utilización de las técnicas de encolamiento en especial aquellas que presentan inconvenientes puede suscitarse la congestión en las interfaces de un dispositivo de red y para evitar esto el mecanismo por default es el Trail Drop o descarte de paquetes tiendo de esta forma desventajas muy significativas ya que podrían causar la degradación de las aplicaciones en tiempo real al no existir diferenciación de tráfico para desechar paquetes. Los mecanismos que previenen este descarte sin diferenciación son los siguientes:

- ***RED (Random Early Detection):*** Descarta paquetes aleatoriamente antes de que ocurra la congestión incrementando la velocidad de descarte conforme el tamaño de la cola aumenta pero su desventaja radica en que no proporciona ninguna prioridad de desecho.

- ***WRED (Weighted Random Early Detection):*** A diferencia de RED realiza una distinción de tráfico según la prioridad de manera que es posible decidir que tráfico descartar. Con este mecanismo se puede manejar diferentes perfiles como: Mínimo Umbral, Máximo Umbral y Probabilidad de Drop con lo que WRED selecciona uno de estos acorde a las prioridades de los valores DSCP e IP Precedence.

- ***CBWRED (Class-Based Weighted Random Early Detection):*** Al utilizar la técnica de encolamiento CBWFQ la política de descarte de paquetes es Trail Drop por lo tanto si se utiliza WRED en este esquema automáticamente se está creando CBWRED o mejor dicho políticas de descarte de paquetes por cada clase, la única forma de asegurar el comportamiento de un PHB.

2.2.6 *Herramientas de Monitoreo de Tráfico*

En la actualidad existen una gran diversidad de herramientas de monitoreo y análisis de tráfico basadas en software ya sea a través de sistemas operativos Open Source o propietarios y también sistemas de monitoreo en software y hardware obviamente para funciones más específicas o sofisticadas. A continuación se describen brevemente las herramientas a utilizar en el presente

estudio con la finalidad de realizar la auditoría a la red inalámbrica de la UPEC e identificar los tipos de tráficos generados por los usuarios en dicha red.

2.2.6.1 PACKETSHAPER

Según (Blue Coat Systems, 2013) el PacketShaper es un dispositivo de gestión de tráfico y de administración de políticas QoS a nivel de aplicaciones, está integrado con WebPulse de Blue Coat para proporcionar detección y clasificación de tráfico en tiempo real, favoreciendo a los administradores de red al permitirles configurar límites y reserva de ancho de banda de manera que es posible garantizar una asignación equitativa entre todos los usuarios.

El mecanismo para proporcionar una elevada Calidad de Servicio a las aplicaciones críticas es a través de la supervisión, control y aceleración del tráfico permitiendo el alineamiento de los recursos de red de una organización con sus necesidades de negocio (Blue Coat Systems, 2013).

Con la finalidad de salvaguardar el rendimiento de las aplicaciones y descongestionar los nodos centrales PacketShaper trabaja básicamente sobre cuatro actividades:

- ***Clasificación:*** PacketShaper clasifica automáticamente el tráfico de la red por categorías ya predefinidas bajo criterios como: tipo de aplicación (clasificación en Nivel 7), tipo protocolo o subred.

- ***Análisis:*** Proporciona un diagnóstico en profundidad sobre el rendimiento de las aplicaciones, la utilización y rendimiento de la red con más de 60 métricas por cada tipo de tráfico.

- ***Control***: Facilita la aceleración de las aplicaciones críticas por medio de la asignación del ancho de banda, control de tráfico y aplicación de políticas. De esta forma es posible especificar mínimos y máximos de ancho de banda, restringir el tráfico no autorizado y contener a aplicaciones que desbordan los recursos sin ser urgentes ni necesarias.

- ***Informes:*** Utiliza el protocolo SNMP (Protocolo Simple de Gestión de Red) con finalidad de gestionar y administrar los recursos de la red y facilitar informes, gráficas y estadísticas sobre su uso posibilitando la verificación del cumplimiento de los objetivos.

En la Tabla 13 se resumen las características principales del PacketShaper:

OPERACIÓN	CARACTERÍSTICA	DESCRIPCIÓN
SUPERVISIÓN	Clasificación del Tráfico	Según la aplicación, protocolo, identificador de puerto, DiffServ, 802.1p, etiqueta MPLS, dirección IP o MAC, dirección del flujo, IP fuente o IP destino.
	Análisis y Gestión del tiempo de respuesta	Tiempos de respuesta (divididos en retardos del servidor y de la red), clientes y servidores que sufren los mayores retardos, porcentaje de ancho de banda malgastado y paquetes perdidos.
	Compromisos en el Nivel de Servicios (SLA)	Permite establecer compromisos en tiempos de respuesta con una precisión de milisegundos.
	Top 10	Determina las clases que generan la mayor parte del tráfico. Esta característica ayuda a localizar los problemas y solucionarlos con rapidez. Además se puede confirmar cuánto ancho de banda se emplea por aplicación.
	Mínimo y máximo por aplicación	Para realizar una reserva de ancho de banda y garantizar una aplicación o clase de tráfico.
	Mínimo y máximo por Sesión	Protege sesiones sensibles a la latencia, se establece un flujo mínimo y máximo para cada sesión individual de un tipo de tráfico.
	Mínimo y máximo dinámico por usuario	Controla dinámicamente el ancho de banda por usuario sin necesidad de configuraciones tediosas.
		Impone un flujo suave y constante que maximiza la capacidad. Reduce la latencia tanto en el

CONFORMACIÓN	Control de Flujo en sesiones TCP	tráfico de entrada como de salida, ajusta el tamaño de la ventana de acuerdo con las previsiones y mide el acuse de recibo para asegurar la entrega a tiempo.
	Control de Flujo en sesiones UDP	Restringe el tráfico de entrada y de salida a un ritmo determinado, garantiza un ancho de banda concreto y controla el jitter. Por ejemplo, la transferencia de VoIP requiere un ancho de banda mínimo y PacketShaper proporciona la cantidad precisa para eliminar el jitter y asegurar un comportamiento fiable.
ACELERACIÓN	Compresión a nivel de aplicación	El módulo de compresión identifica el tráfico comprimible y aplica la tecnología de compresión adecuada, lo cual aumenta la capacidad hasta de cuatro veces.
	Gestión de latencias	Utiliza técnicas avanzadas de gestión de tráfico para asegurar un rendimiento óptimo de las aplicaciones, incluso durante los momentos de tráfico intenso.

Tabla 13. Características principales del PacketShaper

Fuente: El Propia

2.2.6.2 NTOP

NTOP inicialmente concebido por Luca Deri y Stefano Suin de la Universidad de Pisa (Italia) es una herramienta de monitorización de tráfico en tiempo real que a través del control de usuarios y aplicaciones permite determinar el consumo de los recursos de la red en un instante determinado, facilitando la labor de diagnóstico para los administradores de TICs. A continuación se presentan las características más significativas de esta plataforma:

- Su interfaz es web (puerto TCP 3000) de modo que la visualización de las estadísticas es muy intuitiva.

- Viene con un recolector/emisor NetFlow/sFlow y RRD para almacenar persistentemente estadísticas de tráfico, es decir que en la práctica se puede analizar la información recolectada de un período anterior.

- Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, ARP/RARP, IPX, AppleTalk, Netbios y dentro de la monitorización TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, TELNET, SMTP/POP/IMAP, SNMP, entre otros.

- Detecta posibles paquetes perniciosos e inclusive a través de su sistema de alarmas se puede determinar las malas configuraciones de equipos.

- Es un software multiplataforma (Windows, Linux, Solaris y MacOSX) muy fácil y rápido de instalar que se ajusta a las necesidades de cada entorno de red.

Como se ha mencionado anteriormente el potencial de esta plataforma es la factibilidad de análisis de tráfico por medio de la monitorización con resultados con respecto a la utilización por ejemplo de los Protocolos (número de solicitudes, picos/tormentas) de modo que para cumplir con este requerimiento NTOP mide los siguientes tipos de tráfico:

- Datos enviados/recibidos: Volumen y paquetes, clasificados de acuerdo con el protocolo de red IP.

- Tráfico Multicast e historial de Sesiones TCP.

- Medición y Análisis de Ancho de Banda.

- Tráfico VoIP (SIP, Cisco SCCP), VLAN y BGP (Border Gateway Protocol).

- Detección de protocolos P2P (Peer-to-Peer).

2.2.6.3 WIRESHARK

Wireshark es un analizador de protocolos basado en Software Libre y disponible en la mayoría de sistemas operativos Unix incluyendo Linux y Windows utilizado para el análisis y solución de problemas de red similar a tcpdump pero con nuevas funcionalidades: interfaz gráfica, opciones de organización y filtrado de información, lo cual facilita visualizar todo el tráfico que pasa a través de una red pero previamente habilitando una configuración de puerto en modo promiscuo. Además de lo indicado constituye una poderosa herramienta para examinar los problemas de seguridad, depuración de implementaciones de protocolos y también como mecanismo didáctico para la comprensión del funcionamiento de los mismos. En breve se mencionan otras características y capacidades de Wireshark:

- Permite examinar y capturar datos de una red en tiempo real o de un archivo salvado con un completo lenguaje para filtrar lo que se necesita ver en base a muchos criterios.

- Muestra los paquetes con información de protocolo muy detallado y crea varias estadísticas.

- Necesita el paquete de librerías WinPcap para complementar su funcionamiento.

- Importa y exporta datos de paquetes desde y hacia muchos otros programas de captura.

- Tiene soporte para hasta 1100 protocolos en la actualidad y su visualización se basa en herramientas muy poderosas que identifica mediante el uso de colores los paquetes que cumplen con los filtros previamente previstos o configurados por los usuarios.

2.2.7 *Prioridad de Tráfico por Políticas*

Según (Erazo et al., 2009) la prioridad es la capacidad de proporcionar un tratado especial al tráfico a través de una jerarquización y asignación de requerimientos específicos para garantizarlo, estos requerimientos implican la concesión de un ancho de banda mínimo y máximo, disminución de retardos y reducción pérdida de paquetes en especial para el tráfico más sensible de manera que los paquetes con mayor prioridad deberán ser enviados siempre antes que los de menor nivel de servicio.

La priorización se define una vez determinados los tipos de tráficos circundantes por la red y acorde al cumplimiento de los objetivos de la organización, de no ser implementado este mecanismo y en general la Calidad de Servicio en una red el acceso a las aplicaciones multimedia y en tiempo real como la voz puede ser mermado o inhabilitado por otras no críticas o inclusive innecesarias por esta razón es importante antes de implementar QoS dimensionar y puntualizar adecuadamente las políticas a aplicar con la finalidad de otorgar prioridad al tráfico que lo requiere en virtud del entorno.

La definición de políticas de Calidad de Servicio con precisión incluye las siguientes tareas:

- Control del tráfico de Internet, recurso costoso y limitado que puede ser mal utilizado por los usuarios y aplicaciones como por ejemplo descarga de música, películas o juegos que puede restringir la descarga de correos institucionales, videoconferencias con sucursales, descarga de archivos, entre otros de carácter importante para la institución.

- Establecimiento de un límite mínimo y máximo de ancho de banda para cada clase de tráfico.

- Asignación de un nivel de prioridad para cada clase de tráfico, esto acorde a los objetivos organizacionales.

- Aplicación de mecanismos de control de congestión y prevención de congestión para cada clase.

Cabe recalcar algunas recomendaciones a la hora de formular las políticas y asignación de niveles de prioridad:

- Tener precaución de no crear excesivamente clases de tráfico, 4 o 5 clases es comúnmente aconsejable.

- No crear políticas muy complejas y sobredimensionadas.

- No asignar una gran cantidad de flujos a la clase de más alta prioridad.

- Disponer de las herramientas adecuadas en cuanto a hardware y software ya que si no se dispone de estas es complejo llevar a cabo el proceso de implementación de QoS ya que también se basa en otros requerimientos como: equipos de red robustos que soporten su configuración, cableado estructurado certificado, seguridad en la red, entre otros.

- Finalmente para garantizar la Calidad de Servicio además del cumplimiento a cabalidad de cada una de las fases de implementación es sumamente importante llevar la administración y control de las políticas aplicadas por el personal de TI, de forma sean escalables conforme crecen los usuarios y se expande la red.

2.2.8 *Beneficios de aplicar QoS*

Al implementar QoS en una WLAN y en general en una infraestructura de red se obtienen los siguientes beneficios:

- Posibilita la convergencia de la red y de los servicios ya que sobre la misma infraestructura es factible transmitir varias aplicaciones IP como voz, video y datos con garantías de extremo a extremo y escalabilidad en cuanto al crecimiento del número de usuarios y aplicaciones.

- La capacidad de priorizar el tráfico y mejorar las prestaciones de las aplicaciones en tiempo real, de esta forma el tráfico sensible al retardo o con otros requerimientos es enviado primero antes que otro u otros con menor prioridad.

- Permite hacer un uso eficiente de los recursos de la red como por ejemplo el ancho de banda y controlarlo por aplicación además del manejo adecuado de los mismos ante momentos de congestión.

- Contribuye sobre todo a mejorar las actividades productivas de las empresas y de las personas al disponer de servicios garantizados en todo momento y en cualquiera que sea el entorno como por ejemplo: la industria, banca, sector comercial, educación, salud entre otros.

2.3 SEGURIDAD EN REDES WLAN

2.3.1 *Introducción e importancia de la Seguridad en Redes Inalámbricas*

La seguridad en la red es el proceso por el cual se protegen los recursos de información digital de tal forma que los objetivos que persigue se concentran en mantener la integridad, la confidencialidad y asegurar la disponibilidad de los usuarios únicamente autorizados a acceder a dicha información, en este escenario las redes inalámbricas de área local no deben ser la excepción (Cisco, 2006).

En la actualidad la seguridad en una red inalámbrica es una de las principales preocupaciones de las empresas que están interesadas en implementarlas. Afortunadamente, tanto el conocimiento de los usuarios en materia de seguridad así como también las soluciones ofrecidas por los proveedores de tecnología están mejorando. Las redes inalámbricas actuales incorporan funciones complejas de seguridad y cuando estas redes cuentan con una protección adecuada, las compañías u organizaciones pueden aprovechar con confianza las ventajas que ofrecen (Cisco, 2015).

El conocimiento de los elementos de la seguridad de WLANs y el empleo de las mejores prácticas son de gran beneficio a la hora de explotar el potencial de las WLAN. El hablar de buenas prácticas de seguridad se refiere a asegurar que los usuarios solamente puedan realizar las tareas que tienen autorizado hacer, acceder solo a la información que tienen autorizado tener, garantizar que los usuarios no dañan los datos, aplicaciones o en sí el entorno operativo de la red o sistema y controlar los efectos de los errores con la finalidad de contrarrestar vulnerabilidades y prevenir ataques desde el medio inalámbrico.

2.3.1.1 Vulnerabilidades de las WLAN

Una vulnerabilidad se considera como una debilidad inherente en el diseño, configuración o implementación de una red o sistema que lo hace susceptible a las amenazas. Una amenaza corresponde a cualquier ente que se encuentra fuera o dentro de la misma red o sistema y atenta contra la seguridad de la información ya que puede interrumpir la operación, funcionamiento, disponibilidad o integridad haciendo uso de herramientas para consumar un ataque debido a la falta o deficiencia de políticas de seguridad.

Las WLAN son redes muy vulnerables ya que a diferencia de las redes cableadas el acceso al medio de transmisión es compartido y está disponible para todos aquellos dentro del área de cobertura solo habría de necesitar herramientas y tiempo para participar en una conexión como usuario legítimo. (Cisco, 2006) describe las principales vulnerabilidades en redes 802.11:

- ***Autenticación débil:*** únicamente de dispositivo, más no basada en usuario.

- ***Encriptación débil:*** principalmente del mecanismo de cifrado WEP (Wired Equivalent Privacy), actualmente obsoleto.

- ***No existencia de integridad de los mensajes:*** ICV[13] (Integrity Check Value) o Valor de Control de Integridad no es efectivo para asegurar la integridad de los mensajes.

[13]**ICV:** Conjunto de bits que se suman a la salida de datos tras aplicar una llave de cifrado que permite comprobar en el receptor si ha existido modificación de la información.

2.3.1.2 Amenazas de las WLAN

Según (Cisco, 2006) existen 4 tipos de amenazas para las redes 802.11:

- ***Estructuradas:*** provienen de hackers técnicamente competentes que conocen las vulnerabilidades de las redes inalámbricas y las explotan a cabalidad.

- ***No estructuradas:*** generadas por individuos inexpertos que hacen uso de herramientas de hacking y crackers de contraseñas.

- ***Internas:*** quizá las amenazas más peligrosas se deben a individuos que dentro de su red son usuarios autorizados pero por motivos mal intencionados hacen uso indebido de la información.

- ***Externas:*** pertenecen a los individuos u organizaciones que aun no teniendo acceso a la red se valen de mecanismos para ingresar desde el exterior ya sea desde edificios adyacentes, estacionamientos o áreas comunes.

2.3.1.3 Ataques a las WLAN

Un ataque es la acción mediante la cual un individuo toma control, daña o roba información de una red o sistema. Para consumarse un ataque se tienen las siguientes fases (Mieres, 2009):

- ***Reconocimiento:*** Esta fase involucra la obtención de información con respecto a la víctima en este caso persona u organización haciendo uso por ejemplo de la Ingeniería Social o el sniffing.

- ***Exploración:*** Utiliza la información obtenida en la primera fase para sondear al sistema víctima como por ejemplo: direcciones IP, nombres de host, datos de autenticación entre otros.

- ***Obtener Acceso:*** Materialización del ataque por medio de la explotación de las vulnerabilidades y defectos del sistema encontrados durante las dos primeras fases como la Denegación de Servicio (DoS), Denegación de Servicios Distribuidos (DDoS), Password Filtering entre otros.

- ***Mantener el Acceso:*** El atacante buscará implementar herramientas que le permitan acceder en otra ocasión a través de herramientas como: backdoors, rootkits y troyanos.

- ***Borrar Huellas:*** Tras la ejecución de las fases anteriores el atacante intentará borrar todas las huellas dejadas en su intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. Eliminará logs o archivos de registro y alarmas del sistema de detección de intrusos si lo hubiere.

2.3.1.3.1 Tipos de Ataques

A continuación se describen los tipos de ataques más comunes a las redes inalámbricas de área local:

- ***Wardriving:*** Es un método para detectar redes inalámbricas a través de cualquier dispositivo móvil y un software adecuado que ayuda a llevar a cabo una de las primeras fases de los ataques que es el reconocimiento ya que al detectar una red inalámbrica no segura realiza un análisis exhaustivo de las vulnerabilidades de dicha red.

- ***Denegación de Servicio (DoS):*** Consiste en negar algún tipo de recurso o servicio de la red a usuarios autorizados como por ejemplo la inundación de red con pedidos de disociación falsos como resultado desconectarán a los clientes 802.11 del Punto de Acceso. Además es importante resaltar que cualquier dispositivo que opere en la banda de 2,4 o 5Ghz puede ser usado como una herramienta potencial para un DoS.

- ***AP Furtivo:*** Generalmente los clientes se conectan al AP con la señal más fuerte y si este es un Punto de Acceso no autorizado los clientes se asocian sin ninguna dificultad y estará en la capacidad de acceder al tráfico de la red. Por esta razón un AP furtivo puede ser usado para realizar ataques generados por desconocidos como Man-in-the-Middle contra tráfico encriptado como SSL (Secure Sockets Layer) o SSH (Secure SHell). Adicional a esto un AP furtivo puede usar spoofing o suplantación de ARP e IP para engañar a los clientes para enviar sus contraseñas e información confidencial.

- ***Main-in-the-Middle:*** En este mecanismo el atacante se sitúa entre las dos partes que intentan comunicarse pasando totalmente desapercibido para poder interceptar los mensajes. Una de las opciones es utilizar el AP Furtivo y configurarlo con el mismo SSID del AP legítimo. Otra opción es utilizar una estación inalámbrica para suplantar la MAC ya sea del AP o de la estación logrando colocarse entre ambos dispositivos de manera transparente y ahora el tráfico de los usuarios se envía a la estación ilegítima que a su vez captura los datos y los reenvía al AP legítimo, el tráfico de retorno del AP legítimo de igual forma primero se envía a la estación no autorizado que captura y posteriormente se reenvía a la STA víctima. Por otra parte para iniciar este tipo de ataque es necesario valerse inicialmente de un sniffer para obtener datos como SSID, dirección MAC del AP y dirección MAC de la víctima y enviar al menos una trama de disasociación para que la víctima se desconecte de la fuente confiable y se conecte a la fuente del ataque. En la Figura 44 se esquematiza el ataque Man-in-the-Middle.

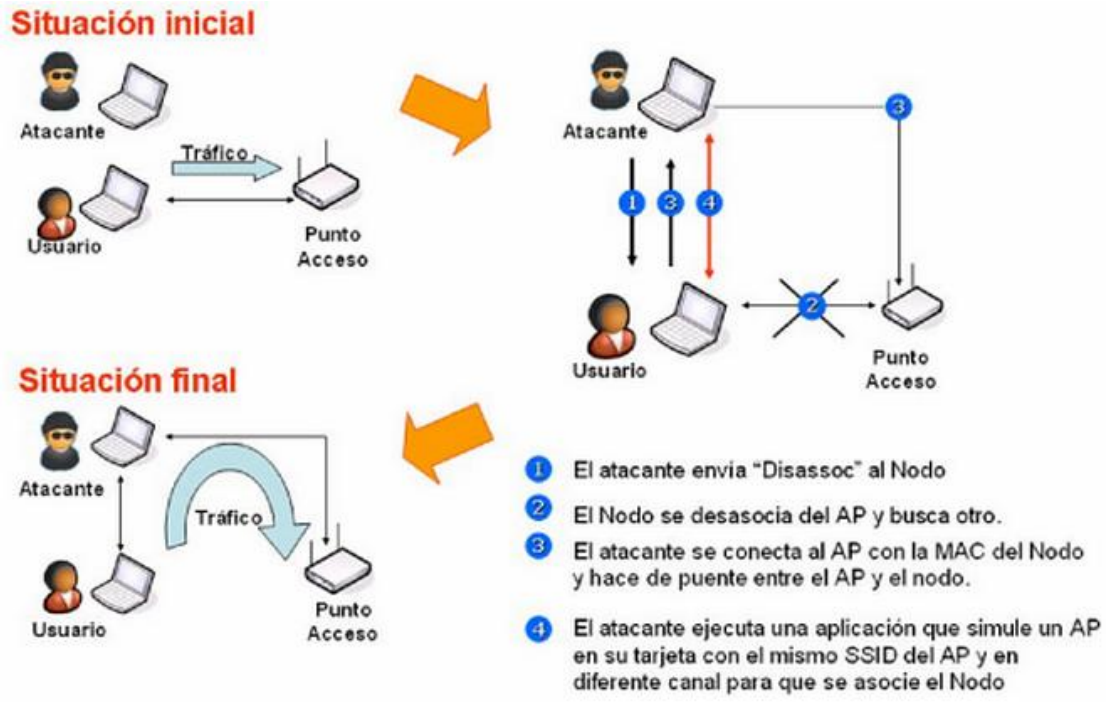


Figura 44. Ataque Man-in-the-Middle

Fuente: (Andreu, Pellejero & Lesta, 2006)

- ***ARP Poisoning:*** Al igual que el ataque Man-in-the-Middle consiste en acceder a la información entre dos terminales pero en este caso haciendo uso de dispositivos más sofisticados como un switch ya que recurre a la alteración de la tabla ARP que se mantiene de forma stateless (sin estados). Precisamente y basándose en la Figura 45 el hacker envía paquetes ARP REPLAY al PC3 comunicando que la dirección IP del PC1 tiene su MAC consiguiendo modificar el caché ARP del PC3, posteriormente realiza la misma acción para envenenar la caché ARP del PC1 con la MAC del hacker. Si el AP y el switch forman parte del mismo dominio de broadcast los paquetes ARP pasan de la red wireless a la red cableada (Panda Software International, 2005).

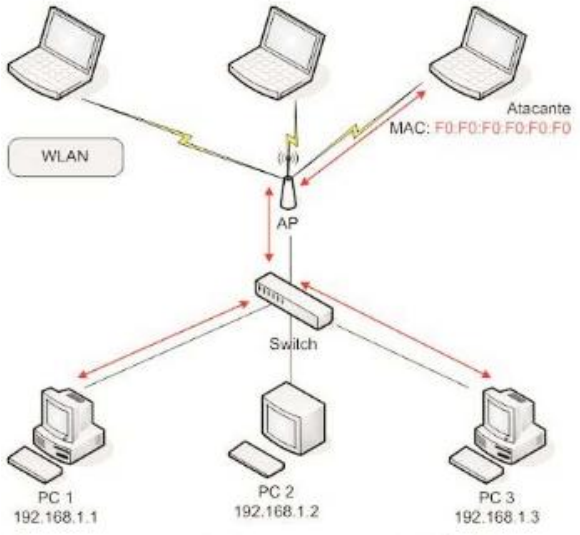


Figura 45. Ataque ARP Poisoning

Fuente: (Panda Software International, 2005)

- **Ingeniería Social:** Estrategia de ataque que se basa en el engaño y está netamente orientada a explotar las vulnerabilidades del factor humano ya que consiste en la obtención de información confidencial de un usuario cercano a un sistema u organización. La mejor defensa frente a este método no técnico es el entrenamiento y la concientización en la práctica de las políticas de seguridad.

El crecimiento y la gran aceptación de las redes inalámbricas de área local han conllevado a mejorar drásticamente los aspectos de seguridad y es así que existen algunos mecanismos que han evolucionado conforme al avance de las WLAN que se explicarán en la siguiente sección.

2.3.2 *Seguridad en redes 802.11*

Las malas prácticas de seguridad principalmente relacionadas con el uso y configuración de los Puntos de Accesos acarrean riesgos muy altos para los usuarios con la masificación de la tecnología WLAN. Estudios recientes demuestran que aún existen redes 802.11 que utilizan cifrado obsoleto o en su defecto son redes totalmente abiertas. Los mecanismos de seguridad

definidos para las redes 802.11 en el nivel Enlace de Datos se categorizan de la siguiente forma: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) y WPA2 (Wi-Fi Protected Access 2), existiendo mecanismos más apropiados y complejos en otros niveles que garantizan la protección de datos.

(Calderón, 2014) revela los resultados con respecto a la utilización de seguridad con una muestra de 11.295.560 de redes inalámbricas en México en un período comprendido de septiembre a diciembre de 2013 (véase la Tabla 14).

TIPO DE CIFRADO	REDES INALÁMBRICAS
Abiertas	681.447
WEP	4.727.606
WPA	1.043.437
WPA2	4.701.300
Otro	141.770

Tabla 14. Utilización de Seguridad en WLANs

Fuente: (Calderon, 2014)

De los resultados obtenidos en porcentaje (véase Figura 46) y no muy ajenos a la realidad de nuestro país se tiene que existe un gran número de usuarios que siguen utilizando WEP con una tasa de 41,85%, no muy lejos está WPA2 con 41,62% y con respecto a las redes abiertas en la actualidad ya son muy escasas, además parte de este estudio pone en conocimiento que una de las vulnerabilidades que pueden ser explotadas es la no modificación de la configuración de fábrica de los dispositivos de red inalámbrica (AP y Routers inalámbricos) poniendo en riesgo la seguridad de la información transmitida.

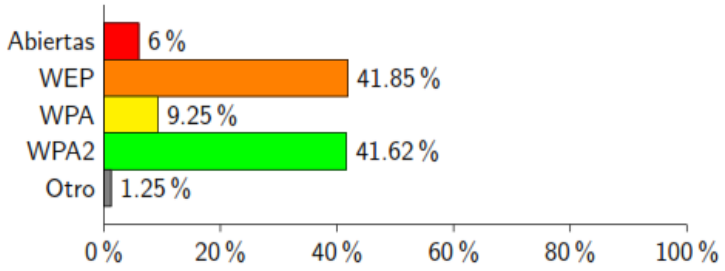


Figura 46. Porcentaje de utilización de Seguridad en WLANs

Fuente: (Calderón, 2014)

2.3.2.1 WEP

WEP o Privacidad Equivalente al Cable es el primer sistema de seguridad incluido en el estándar IEEE 802.11 que utiliza el algoritmo de encriptación simétrico por flujo RC4 (Rivest Cipher 4) para el cifrado de los datos a transmitir. A continuación se describe la metodología de WEP para cifrar y descifrar una trama de Datos:

1. La llave está formada de una clave conocida por las estaciones y el Punto de Acceso (40 o 104 bits) más 24 bits del (IV) o Vector de Inicialización dando como resultado 64 o 128 bits de entrada y como salida se tiene un vector de tamaño de 256 bits. Este proceso es parte de RC4 y se le conoce como KSA o algoritmo programador de claves.

2. Se calcula el CRC-32 de los datos a cifrar para la verificación de la integridad obteniendo un ICV (Valor de Comprobación de Integridad) que se concatena con el payload a transmitir en claro, es decir Datos+ICV.

3. Se aplica el segundo proceso de RC4 que es PRNG o módulo de generación de números pseudoaleatorios al resultado obtenido en el paso 1 que ahora toma el nombre de keystream de igual longitud que (Datos+ICV).

4. Se aplica la función XOR entre (keystream y Datos+ICV).

5. Al resultado de la función XOR se le añade el vector de inicialización en claro más la cabecera 802.11 y la trama cifrada está lista para transmitirse.

En el lado del receptor ocurre lo siguiente:

1. Se extrae el IV de la trama transmitida que está en texto claro y se la concatena con la clave ya conocida.

2. Se aplica RC4 (PRNG) con un keystream igual a lo de los datos cifrados y se realiza XOR entre el keystream y los datos cifrados.

3. Se obtiene como resultado el texto en claro más la comprobación CRC-32 que cabe recalcar no es la misma que se utiliza para FCS (Frame Check Sequence).

En la actualidad WEP es considerado como un mecanismo de cifrado inseguro y prácticamente obsoleto debido a la utilización de una sola clave compartida por las estaciones y el Punto de Acceso, también en la trama ya cifrada se incluye el IV en texto claro que con ayuda de herramientas en cuestión de minutos se podría averiguar la clave y por último es necesario resaltar que al transmitirse una trama cifrada la cabecera de la trama MAC 802.11 queda expuesta de manera que puede ser interpretada por una estación ilícita. Estas vulnerabilidades han dado paso a la realización de ciertos ataques como los que se mencionan a continuación:

- ***Fuerza Bruta:*** Supone probar reiteradamente el conjunto de palabras que forman el lenguaje manejado por el AP para implementar la definición de la clave (Giménez, 2008).

- ***Arbaugh:*** Consiste en una metodología para obtener el conjunto de palabras que forman el lenguaje de las cadenas de encriptación keystream para una clave precompartida dada ya que la cadena de cifrado depende de la clave y el IV utilizado (Giménez, 2008).

- ***FMS (Fluhrer- Mantin- Shamir):*** Permite obtener la clave de cifrado debido a una vulnerabilidad en el modo de operación de RC4 en sus módulos KSA y PNRG.

- ***De Inyección:*** Este tipo de ataque surge porque WEP no contempla ninguna medida de control a la llegada de paquetes IV del mismo valor de esta manera un atacante puede introducir un datagrama con un mismo valor IV las veces que necesite hasta que el proceso de descifrado sea correcto (Giménez, 2008).

2.3.2.2 WPA

WPA o Wi-Fi Protected Access es un sistema de seguridad a nivel MAC desarrollado por la Wi-Fi Alliance y el IEEE como resultado del borrador del estándar IEEE 802.11i que contrarresta las vulnerabilidades de WEP orientado tanto para entornos de pequeña oficinas, hogar y grandes empresas. Las mejoras introducidas son con respecto al mecanismo de autenticación y cifrado de datos:

- ***Autenticación:*** Es posible utilizar un ente centralizado para la distribución de claves (RADIUS) o en su defecto para los pequeños entornos una clave pre-compartida PSK (Pre-Shared Key) conocida por las estaciones y el AP, a través de la PSK se construye la PMK (Primary Master Key) cuyo resultado es 256 bits necesaria para iniciar el proceso de autenticación.

- ***Cifrado:*** Se utiliza TKIP (Temporal Key Integrity Protocol) que genera claves dinámicamente para cada trama a transmitir, a su vez emplea RC4 mejorado y bien implementado con la clave de 128 bits y un vector de inicialización de 48 bits. Adicional a esto se mejora la integridad de los mensajes con MIC (Message Integrity Code) también conocido como “Michael” ya que con el método anterior CRC fue posible alterar la información y actualizarlo sin la necesidad de la clave WEP.

A pesar de las mejoras mencionadas, WPA es susceptible a los siguientes ataques:

- ***Fuerza Bruta:*** El "talón de Aquiles" de WPA es sin duda el proceso de autenticación entre las estaciones de la red y el AP conocido como "4-way-handshake" o saludo de 4 vías que corresponde al intercambio de 4 paquetes y el problema se halla tanto en el segundo paquete como en el cuarto que van en dirección desde la estación al AP. El atacante puede capturar el MIC y un paquete sin cifrar EAPOL-key (necesario para el proceso) para inferir en la clave de cifrado mediante fuerza bruta.

- ***Denegación de Servicio:*** Debido a la propia implementación de 802.11i en cuanto al protocolo de cifrado TKIP y el estándar IEEE 802.1x (control de acceso basado en puertos) ya que por ejemplo con 802.1x el atacante puede inundar con tramas de inicio el AP objetivo, es decir con un envío masivo de "EAPOL Start" con diferentes direcciones MAC y así consumir los recursos del AP. En el caso de TKIP explotando sus vulnerabilidades en el manejo MIC (Giménez, 2008).

2.3.2.3 WPA2

WPA2 (Wi-Fi Protected Access 2) constituye la implementación comercial avalada por la Wi-Fi Alliance de la versión final de IEEE 802.11i cuya diferencia con respecto a WPA radica principalmente en la mejora del algoritmo de cifrado pasando de TKIP/RC4 a CCMP/AES. AES (Advanced Encryption Standard) es un algoritmo criptográfico para el cifrado de los datos mucho más robusto que RC4 y CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) es un protocolo que consta de un algoritmo de privacidad Counter Mode (CM) y de un algoritmo de integridad y autenticidad que es el Cipher Block Chaining Message Authentication Code (CBC-MAC) por esta razón existe la separación de la autenticación de usuario con la integridad y privacidad en WPA2.

Tanto en WPA como en WPA2 el mecanismo de autenticación es el mismo, se mantiene para entornos pequeños PSK o clave pre-compartida y para redes empresariales IEEE 802.1x/EAP (Extensible Authentication Protocol) que se explicará a mayor detalle en la siguiente sección. PSK en este entorno se le conoce como WPA2-Personal y la autenticación basada en

802.1x/EAP se la denomina WPA2-Enterprise, esta última utiliza un servidor RADIUS (Remote Authentication Dial-In User Service) para el manejo de las claves. En la Tabla 15 se muestra una comparativa entre WPA y WPA2 en los aspectos de autenticación y cifrado.

		WPA	WPA2
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP (RC4) / MIC	CCMP (AES) / CBC-MAC
Modo Empresarial	Autenticación	802.1x / EAP	802.1x / EAP
	Cifrado	TKIP (RC4) / MIC	CCMP (AES) / CBC-MAC

Tabla 15. Comparativa entre WPA y WPA2

Fuente: (Hernández, 2007)

La mejora con respecto al mecanismo de cifrado no imposibilita llevar a cabo un ataque de diccionario o fuerza bruta ya que la carencia de seguridad como se observó en WPA es el proceso inicial de autenticación "4-way-handshake" que no se ha corregido y que si puede ser evitado con el uso de una contraseña "fuerte" y su cambio periódico. En la Tabla 16 se muestra una comparativa entre los mecanismos de seguridad a nivel de capa 2:

	WEP	WPA	WPA2
Cifrado	RC4	TKIP/RC4	CCMP/AES
Longitud de Clave	40 o 104 bits	128 bits	128 bits
Vector de Inicialización	24 bits	48 bits	48 bits
Integridad	CRC-32	MIC	CCM
Integridad de la cabecera	Ninguna	MIC (MSDU)	CCM (MPDU)
Control de Claves	Ninguno	EAP	EAP
Autenticación	Sistema abierto o clave compartida	PSK RADIUS	PSK RADIUS

Tabla 16. Mecanismos de Seguridad capa 2

Fuente: Propia

2.3.3 *802.1x/EAP en redes WLAN*

Uno de los logros de 802.11i es la posibilidad de implementarlo ya sea en ambientes SOHO (Small Office Home Office) o en redes empresariales, para estas últimas se especifica el uso de IEEE 802.1x (Port Based Network Access Control) para la autenticación e intercambio de llaves y requiere de un servidor para esta funcionalidad a diferencia de las redes inalámbricas pequeñas en las cuales no se cuenta con un servidor y se utiliza la autenticación mediante una clave de uso compartido PSK como en el caso de WPA2 (Gómez, 2007).

El protocolo IEEE 802.1x fue desarrollado inicialmente para redes cableadas extendiéndose se aplicabilidad a las redes inalámbricas, además de poseer mecanismos de autenticación, autorización, distribución de claves incorpora control de acceso para los usuarios que se vayan a integrar en la red. La arquitectura de 802.1x se compone de las siguientes entidades funcionales:

- ***Suplicante:*** constituye la estación inalámbrica.

- ***Autenticador:*** desempeña un rol eminentemente pasivo ya que se limita a enviar todos los mensajes al servidor de autenticación.

- ***Servidor de Autenticación:*** un servidor AAA (Authentication, Authorization & Accounting) quién tomará las decisiones por ejemplo un servidor RADIUS.

En 802.1x el control de acceso se basa en habilitar y deshabilitar un puerto físico de la red LAN pero en el caso de las redes inalámbricas constituye un puerto virtual que a su vez se divide en dos puertos lógicos PAE (Port Access Entity), uno de autenticación que siempre está en modo abierto y el de servicio que se abre si es que existe una autenticación exitosa. Tanto el suplicante como el autenticador se consideran entidades de Autenticación por puerto (PAE) y el puerto virtual se considera a la asociación entre una estación inalámbrica y un Punto de Acceso, la tercera entidad es el servidor de autenticación y es quién toma la decisión de permitir o no el

acceso a los usuarios. En la Figura 47 se presenta las entidades funcionales de 802.1x para redes inalámbricas.

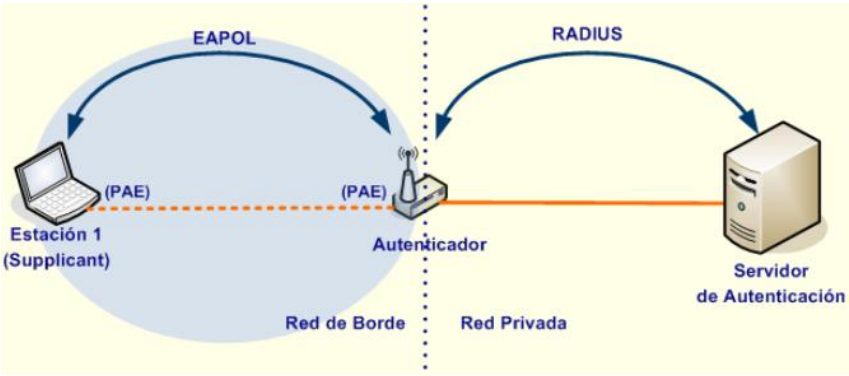


Figura 47. Entidades Funcionales de 802.1x

Fuente: (Gómez, 2007)

El suplicante y el autenticador se comunican mediante el protocolo EAP (Protocolo de Autenticación Extensible), constituye una estructura de protocolo que en lugar de especificar cómo autenticar a los usuarios permite incorporar métodos propios o subprotocolos que ejecutan las transacciones de autenticación y su utilización depende de las necesidades del caso que se explican más adelante (Gómez, 2007). EAP comprende cuatro tipos de mensajes para el transporte de los métodos de autenticación:

- ***Request Identity:*** mensaje de solicitud de identidad desde el AP al cliente.
- ***Identity Response:*** mensaje de respuesta desde el cliente al AP.
- ***Success:*** acceso permitido al cliente o suplicante.
- ***Fallo:*** mensaje para indicar al suplicante que se ha denegado la conexión

El protocolo utilizado en redes inalámbricas para transportar EAP específicamente se llama EAPOL (EAP Over LAN) y la diferencia radica en que los suplicantes en un entorno EAPOL pueden enviar un marco EAPOL-Start para el inicio del proceso de intercambio y un EAP-Logoff para desautorizar un puerto, esta comunicación únicamente válida entre suplicante y autenticador mientras que la comunicación entre el autenticador y el servidor de autenticación utilizan protocolos de capa más alta (véase la Figura 47).

2.3.3.1 Funcionamiento 802.1x

A continuación se especifica el procedimiento de autenticación en 802.1x con el protocolo EAPOL:

1. La estación inalámbrica o suplicante se asocia a la red 802.11.
2. Se inicia el intercambio 802.1x con el mensaje "EAPOL-Start" del Suplicante, suele ser opcional.
3. El Autenticador envía un mensaje "Request Identity" al Suplicante sin la necesidad de previamente haber recibido un "EAPOL-Start".
4. El Suplicante responde con un mensaje "Response Identity" al Autenticador que a su vez lo reenvía al Servidor RADIUS como una solicitud de acceso.
5. El RADIUS determina el tipo de autenticación que se requiere y envía un EAP-Request para el método requerido por ejemplo "EAP-Request PEAP", que está encapsulado dentro de un mensaje "RADIUS-Access-Challenge" que se envía primero al Autenticador y luego al Suplicante.
6. El suplicante proporciona las credenciales del usuario en un mensaje "EAP-Response" de acuerdo al método utilizado al Autenticador y éste lo envía al Servidor como un mensaje "RADIUS-Access-Request". Este procedimiento puede repetirse las veces que sean necesarias.
7. El Servidor de Autenticación concede el acceso a través de un mensaje "RADIUS-Access-Accept", que el Autenticador lo reenvía al Suplicante como un mensaje "Success", con esto se ha autorizado el puerto.

8. Una vez recibido el mensaje “RADIUS-Access-Accept” el Punto de Acceso distribuye las claves al Suplicante a través de un mensaje “EAPOL Key”.
9. Una vez con las claves instaladas el suplicante comienza a enviar datos a la red.
10. Si el suplicante desea finalizar su acceso a la red envía un mensaje “EAP Logoff” y el Autenticador cambia el estado del puerto es decir a “no autorizado”.

En la Figura 48 se presenta el proceso de autenticación realizado por las tres entidades funcionales de 802.1x.

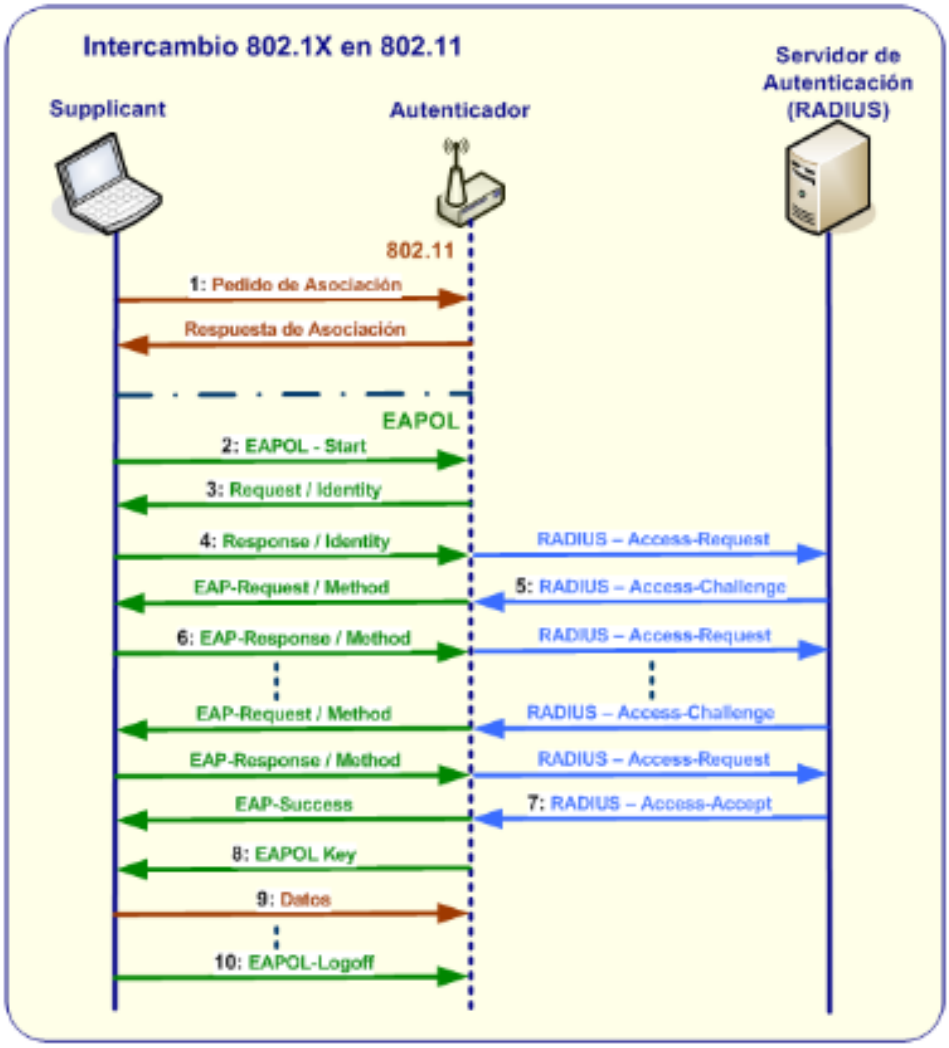


Figura 48. Proceso de Autenticación 802.1x en redes 802.11.

Fuente: (Gómez, 2007)

2.3.3.2 Tipos EAP en redes 802.11

EAP permite extender los métodos de autenticación para cumplir con las nuevas necesidades y requerimientos más allá de las redes LAN. Los métodos utilizados para redes inalámbricas son los siguientes:

- ***EAP-TLS:*** Es un método de autenticación muy seguro, utiliza el protocolo TLS (Transport Layer Security) para seguridad en la capa transporte que a su vez incorpora intercambio de Certificados Digitales tanto para los usuarios como para el servidor de autenticación además de criptografía asimétrica. La generación y distribución de certificados para todos los usuarios podría ser un inconveniente para las redes de las organizaciones pequeñas ya que se necesita de la implementación de una PKI (Infraestructura de Claves Públicas).

- ***EAP-TTLS:*** A diferencia de EAP-TLS usa certificados digitales solamente para autenticar la red hacia el cliente es decir para el servidor y mas no para autenticar a los clientes, pero en su lugar se utilizan métodos basados en contraseñas que obviamente reduce significativamente la cantidad de certificados en la red como. Al igual que EAP-TLS establece un túnel TLS entre el cliente y el servidor haciendo uso del certificado digital para autenticar al servidor (autenticación externa) y sobre este mismo túnel se realiza la autenticación del usuario mediante un nombre de usuario y contraseña (autenticación interna) con los métodos PAP, CHAP, MS-CHAP o MS-CHAP v2.

- ***EAP-PEAP:*** Tanto EAP-TTLS como EAP-PEAP son similares en su mecanismo de trabajo, la diferencia solamente se encuentra en la autenticación interna que es en dónde EAP-PEAP establece otra sesión EAP para autenticar a los usuarios.

- ***EAP-LEAP:*** Es un sistema EAP propietario de Cisco el cual requiere de un nombre de usuario y contraseña para establecer la autenticación con el servidor RADIUS

proporcionando distribución de clave de sesión segura y dinámica para cada cliente. Entre sus ventajas ofrece un roaming rápido y soporte para varios sistemas operativos.

- ***EAP-Fast:*** Autenticación flexible a través de túnel seguro desarrollado por Cisco y requiere de nombre de usuario y contraseña para la autenticación sin necesidad de requerir certificados digitales.

En la Tabla 17 se presenta una comparativa entre los diferentes métodos de autenticación EAP:

	EAP-TLS	EAP-TTLS	EAP-PEAP	EAP-LEAP	EAP-FAST
Solución de Seguridad	Estándar	Estándar	Estándar	Propietaria de Cisco	Estándar
Certificado Cliente	Si	No	No	No	No
Certificado Servidor	Si	Si	Si	No	No
Seguridad de las Credenciales	Buena	Buena	Buena	Débil	Buena
Generación de Claves Dinámicas	Si	Si	Si	Si	Si
Tunelización	Si	Si	Si	No	Si
Autenticación Base de Datos	Active Directory	Active Directory, LDAP, SQL	Active Directory, LDAP	Active Directory	Active Directory, LDAP

Tabla 17. Comparativa de los métodos de Autenticación EAP

Fuente: (Delgado, 2009)

2.3.4 *RADIUS*

Según (Delgado, 2009) RADIUS (Remote Authentication Dial-In User Service) es un protocolo ampliamente utilizado para proveer autenticación centralizada, autorización y auditoría de

cuentas (AAA) basado en el método de desafío/respuesta, en sus inicios para redes de acceso dial-up pero su uso se ha extendido hasta redes VPN (Redes Privadas Virtuales), LANs y WLANs.

La Autenticación corresponde al proceso de verificar la identidad que un cliente ha declarado por ejemplo uno de los métodos más comunes es a través de nombre de usuario y contraseña con la finalidad de establecer una relación de confianza entre el cliente y el servidor.

El proceso de Autorización se basa en un conjunto de reglas establecidas por el administrador de redes o sistemas en cuanto a lo que puede hacer un usuario autenticado en la red y la Auditoría corresponde al proceso que documenta el uso de los recursos por parte de los usuarios que acceden al sistema, estos datos pueden ayudar a controlar las autorizaciones y cobrar la utilización de los recursos en caso de ser necesario (Gómez, 2007).

Entre las principales características de RADIUS se tienen las siguientes:

- Se basa en el modelo Cliente-Servidor y en una clave de secreto compartido entre el Servidor y el NAS (Network Access Server) o Autenticador en referencia a 802.1x, esta clave no se transmite por la red.

- RADIUS es un protocolo stateless (sin estado) y utiliza UDP e IP para las conexiones, específicamente los puerto 1812 y 1813 UDP.

- Es flexible en cuanto al soporte de gran variedad de métodos de autenticación como: EAP, PAP, CHAP, entre otros.

Como ya se ha mencionado el protocolo de transporte del paquete RADIUS es UDP, por ende se inserta en el campo DATOS del paquete UDP, en la Figura 49 se presenta la estructura del paquete RADIUS.

Figura 49. Estructura del Paquete RADIUS

Fuente: (Gómez, 2007)

Los campos que componen la estructura del paquete RADIUS son los siguientes:

- ***Código:*** Este campo tiene una longitud de 1 byte y permite distinguir el tipo del mensaje: *Access-Request (1), Access-Accept (2), Access-Reject (3), Accounting-Request (4), Accounting-Response (5), Access-Challenge (11), Status-Server (12), Status-Client (13), Reservado (255).*

- ***Identificador:*** Con la finalidad de relacionar una respuesta con una solicitud evitando duplicidad de la información a procesar en el RADIUS, de manera que cuando un cliente solicita un servicio lo hace con un identificador diferente.

- ***Longitud:*** Tiene un tamaño de 2 bytes e indica el tamaño total del paquete, esto incluye los campos: *Código, Identificador, Longitud, Autenticador y Datos*. La longitud varía entre 20 y 4096 bytes, si el paquete es de mayor tamaño se elimina el excedente y si es muy pequeño se descarta.

- ***Autenticador:*** Permite verificar la integridad de los datos. Son dos tipos diferentes de valores (Solicitud y Respuesta). El primer valor se calcula de forma aleatoria, el segundo es calculado con MD5 (Message-Digest Algorithm 5) tomando en cuenta los siguiente parámetros: *Código, Identificador, Longitud, Autenticador de la Solicitud, Datos, Secreto.*

- ***Atributos y Valores:*** Es un campo de longitud variable y contiene los pares Atributo-Valor que intercambia el Servidor con el NAS. Es decir los atributos corresponden a variables que se les asigna una función, tipo de dato, longitud y un valor como por ejemplo: nombre de usuario, contraseña, número de puerto y método de autenticación.

Es decir que la información necesaria para el proceso AAA se encuentra en el campo "Atributos-Valores" cuyo formato se muestra en la Figura 50.

Figura 50. Formato del Campo Atributos
Fuente: (Gómez, 2007)

El subcampo *Tipo* corresponde al número o código del atributo, el rango de valores 192-223 está restringido solamente para uso experimental, el rango 224-240 pertenece a implementaciones específicas y el rango de 241-255 se encuentra reservado para su uso en el futuro. Lo que define cada código se especifica en las RFC 2865 y 2866 por ejemplo el valor 1 representa *"User-Name"*, el valor 2 *"User-Password"*, el valor 3 *"CHAP-Password"*, etc.

El subcampo *Longitud* indica la longitud del atributo transmitido que incluye el tamaño de todos los subcampos del campo Atributos. Finalmente el subcampo *Valor* puede tener o no los siguientes tipos de datos: texto, cadena, dirección IP, número entero y tiempo es decir información específica de cada atributo.

2.3.4.1 Proceso de Autenticación RADIUS

Los mensajes utilizados para los procesos de Autenticación y Autorización son: *Access-Request, Access-Accept, Access-Reject y Access-Challenge*. En primera instancia el cliente solicita el

acceso al Servidor a través de un *Access-Request*, dentro de este paquete existen atributos como un identificador del NAS, contraseña del usuario, nombre de usuario y el puerto de conexión, el servidor al recibir este paquete determina y comunica al cliente si su acceso está permitido *(Access-Accept)* o no permitido *(Access-Reject)*. En caso de ser un *Access-Accept*, éste debe contener la información necesaria con el fin de comenzar la utilización del servicio, pero antes de aceptar o negar el acceso el servidor puede enviar al cliente un desafío que requiera de una respuesta a través de un *Access-Challenge* y el cliente debe responder a este desafío con un paquete tipo *Access-Request* que incluya los atributos adecuados como por ejemplo información acerca del fabricante, Idle-Timeout, Session-Timeout o Proxy State.

Una vez satisfactoria la Autenticación se puede llevar a cabo el proceso de Accounting a través del puerto 1813 UDP. El cliente (NAS o Proxy Server) envía un paquete *Accounting-Request* al servidor RADIUS que transmite la información que se registrará como consecuencia de la utilización del servicio, tras recibir este paquete el servidor envía un Accounting-Response si es que puede almacenar la información caso contrario no existe ninguna respuesta por parte del servidor.

2.3.5 *Portales Cautivos*

Un Portal Cautivo constituye una solución alternativa de autenticación de capa 3 a diferencia de los métodos anteriormente revisados como WEP, WPA, WPA2 y 802.1x que son de capa 2, especialmente enfocados para áreas abiertas como aeropuertos, espacios públicos, cafeterías u hoteles conocidos generalmente con el nombre de HotSpot (punto caliente) aunque su uso no está restringido para cualquier otra red inalámbrica. Este sistema intercepta todo el tráfico HTTP/HTTPS y obliga a los usuarios de la red inalámbrica a primero autenticarse mediante el ingreso de sus credenciales a través de una página web (autenticación web) para su navegación por Internet de forma normal. Además el portal se podría encargar de controlar el tiempo de caducidad de las sesiones y del control del ancho de banda usado por cliente, todo esto con el afán de desalentar a quienes intenten usar los servicios de la WLAN de manera no autorizada.

En cuanto al proceso de autenticación, en el mismo Portal Cautivo se pueden registrar las credenciales de los usuarios de manera local y convivir con el servidor web o sino optar por un servidor externo RADIUS con certificados digitales para mejorar y garantizar la seguridad en la WLAN. Adicionalmente existen básicamente dos tipos de Portales Cautivos: basados en software y soluciones que incorporan un chasis, estas últimas no muy comunes. Dentro de las soluciones basadas en software y ampliamente utilizadas se tienen las siguientes: GRASE HotSpot, ChilliSpot, CoovaChilli, WiFiDog, PFSense, AirMarshal, entre otros.

Es menester mencionar que los portales cautivos tienen sus ventajas y desventajas, entre las ventajas está la simplicidad, autenticación centralizada y creación de políticas por usuario sin embargo como inconveniente está la ausencia de cifrado que se podría contrarrestar con la solicitud de re-autenticación periódica de forma automática.

2.3.5.1 Funcionamiento de un Portal Cautivo

El funcionamiento de un Portal Cautivo es muy sencillo, inicialmente el usuario se conecta a la red inalámbrica obteniendo una dirección IP y solicita desde su navegador cualquier página para su acceso por Internet, en seguida el portal cautivo le re-direcciona a otra página web en la que deberá ingresar las credenciales como nombre de usuario y contraseña para su verificación ya sea dentro de la base de datos local o en una externa a través de RADIUS (véase Figura 51). Una vez verificadas las credenciales por parte del Punto de Acceso como por el servidor AAA se autoriza satisfactoriamente al usuario para su navegación por Internet.

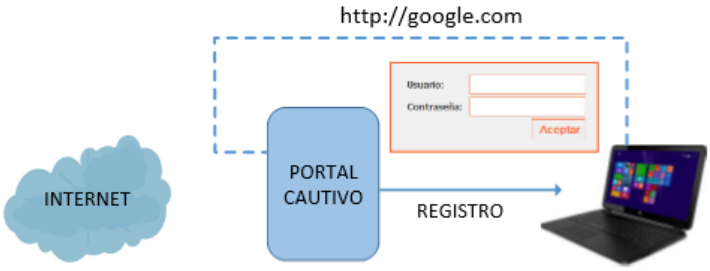


Figura 51. Funcionamiento de un Portal Cautivo

Fuente: Propia

2.3.6 Políticas y Recomendaciones de Seguridad para una WLAN

En la siguiente lista a continuación se presentan algunas medidas de seguridad que deben ser tomadas en cuenta para garantizar la confidencialidad, integridad y disponibilidad de las transmisiones a través de las redes inalámbricas:

- Cambiar las configuraciones de fábrica para la administración de los Puntos de Acceso como nombre de usuario, contraseña por otros más complejos y difíciles de adivinar además modificar la dirección IP y el SSID por defecto.

- Para entornos de redes inalámbricas pequeñas utilizar como mínimo requisito de seguridad autenticación basada en clave compartida PSK y cifrado de comunicaciones AES con contraseñas robustas y de más de 10 caracteres.

- WPA2/Enterprise es una opción muy recomendable para redes empresariales y corporaciones ya que utiliza para el cifrado de datos AES y para generar las contraseñas aleatorias y robustas utiliza el servidor RADIUS, junto a los protocolos 802.1X y EAP para la autenticación.

- Mantener actualizado el Firmware de los dispositivos inalámbricos especialmente Ruteadores Inalámbricos, Puntos de Acceso y Controladoras Inalámbricas.

- El Ocultar el SSID de la WLAN no dota de protección extra en cuanto seguridad caso contrario imposibilita la administración de la red al mismo tiempo que puede ser relativamente fácil encontrar el identificador con herramientas gratuitas que además son capaces de vulnerar la clave en especial de WEP.

- Las soluciones de Firewall, IDS (Intrusion Detection System), ACL (Access Control List) y segmentación a través de VLANs (Virtual Local Area Network) constituyen un complemento seguridad no solamente para los entornos de red cableada sino para las WLAN.

- En ambientes donde se dificulta el manejo de Certificados Digitales la utilización de autenticación web o portales cautivos constituye una opción alternativa.

- El acceso remoto a los dispositivos de la infraestructura inalámbrica debería ser a través de SSH (Secure SHell) que cifra la sesión de conexión haciendo imposible que se pueda obtener contraseñas no encriptadas.

Sugerencias para el usuario de una red inalámbrica:

- Es importante que los ordenadores en especial los portátiles tengan instalado y actualizado el software antivirus.

- Evitar conectarse a redes inalámbricas abiertas o redes inseguras detrás de las cuales puede existir un atacante realizando sniffing o cualquier otro tipo de ataque que afecte a la integridad de la información.

- No conectarse a redes inalámbricas ajenas además de ser un delito de igual forma no se conoce a ciencia cierta quién está detrás de ésta.

- Antes de ingresar a páginas o portales web es necesario comprobar a través de los Certificados que es realmente un sitio seguro ya que los hackers utilizan utilitarios exactamente iguales para suplantar páginas de instituciones financieras u otros para el robo de credenciales.

- En cuanto a las contraseñas de acceso a la red inalámbrica ya sea por clave pre-compartida o en un sistema basado en autenticación es importante que el usuario sea totalmente responsable para no divulgarlas.

CAPÍTULO III. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA WLAN DE LA UPEC

En este capítulo inicialmente se analiza la infraestructura de la red inalámbrica de la Universidad Politécnica Estatal del Carchi, luego se evalúa la distribución actual de los Puntos de Acceso con la finalidad de determinar si su ubicación proporciona cobertura a todas las áreas del campus universitario. Con la ayuda de herramientas de monitorización de tráfico se definen las políticas de clasificación y priorización para la implementación de Calidad de Servicio además de proceder a establecer y configurar los requerimientos de seguridad que finalmente son verificados a través de las pruebas de funcionamiento pertinentes en conjunto con QoS en la WLAN de la UPEC.

3.1 ANÁLISIS FÍSICO Y LÓGICO DE LA RED

Antes de analizar el estado situacional de la red inalámbrica de la UPEC es preciso señalar algunos datos básicos con referencia a su ubicación geográfica, misión y visón que contribuyen al desarrollo, alineamiento y levantamiento de los requerimientos de QoS y seguridad de la WLAN conforme a las políticas institucionales.

3.1.1 Antecedentes

La Universidad Politécnica Estatal del Carchi es una institución de educación superior del norte del país ubicada al suroeste de la ciudad de Tulcán con fecha de creación el 15 de marzo del 2006 y publicada en el registro oficial No. 244 del 5 de abril del 2006. Su misión está básicamente enfocada a la formación de profesionales humanistas, emprendedores y competentes, poseedores de conocimientos científicos y tecnológicos comprometidos con la investigación y solución de problemas del entorno; su visión: ser acreditada por su calidad y posicionamiento global (UPEC, 2015).

Uno de los objetivos estratégicos de la institución es "Garantizar los proceso de calidad en la educación superior a través de la gestión objetiva de los recursos universitarios y dotación de infraestructura y equipamiento que respondan a las exigencias del Sistema de Educación Superior y consoliden el proceso de institucionalidad" mediante la optimización de los espacios y dotación de equipamiento, tecnología de punta y el mejoramiento continuo en todos los ámbitos (UPEC, 2015).

En cuanto a infraestructura física, el campus principal de la Universidad Politécnica Estatal del Carchi tiene 5 hectáreas y cuenta con un Edificio Administrativo, cuatro edificios de Aulas (FCIIAEE[14] y FIACA[15]), un edificio de Laboratorios, un coliseo, un ágora, un auditorio, una cafetería, una plaza central, canchas deportivas y espacios de recreación; algunas de estas todavía en fase de construcción (véase Figura 52).

Figura 52. Maqueta del campus universitario UPEC

Fuente: (UPEC, 2015)

3.1.2 Infraestructura de la Red UPEC

En la actualidad la oferta académica de la Universidad Politécnica Estatal del Carchi se ha extendido con la creación de cuatro nuevas carreras: Ingeniería en Logística, Ingeniería en Informática, Ingeniería en Alimentos y Licenciatura en Administración Pública, lo cual además

[14]**FCIIAEE:** Facultad de Comercio Internacional, Integración, Administración y Economía Empresarial.
[15]**FIACA:** Facultad de Industrias Agropecuarias y Ciencias Ambientales.

de la exigencia de espacios físicos requiere el despliegue de infraestructura tecnológica con la incorporación al campus universitario de estudiantes, personal docente y administrativo. Este crecimiento y el despliegue de nuevas aplicaciones han contribuido a que la red de la UPEC presente ciertos inconvenientes con respecto a la gestión del ancho de banda y saturación para las aplicaciones con mayor criticidad que generalmente son más sensibles al ser transmitidas por el medio inalámbrico lo cual sugiere la necesidad inmediata del mejoramiento del servicio.

En esta sección se describe de manera general la LAN de la UPEC debido a que es muy importante conocer su situación ya que el performance de la WLAN también depende en gran parte del estado de la red de área local y del estado de los servicios ya sean internos y de los proveedores. En la Figura 53 se presenta el esquema general de la red, la Universidad tiene un enlace de Internet contratado con CEDIA[16] de 60Mbps el cual es distribuido mediante un router de borde Cisco de la serie 1900 y un pool de 30 direcciones IP públicas disponibles asignadas básicamente a los servidores. El router se encuentra conectado con el Firewall de la institución Cisco ASA 5520 con la finalidad de dar protección a la red principalmente de acciones mal intencionadas externas, éste cumple también con la funcionalidad de enrutar la red privada a la red pública y natear tanto el servicio de los usuarios así como las transacciones de los servidores.

A continuación del Cisco ASA se encuentra conectado el PacketShaper 7500, el cual tiene la función principal de segmentar el ancho de banda de acceso al Internet por subred o VLAN, además de ciertas restricciones en cuanto al acceso de aplicaciones como Youtube, redes sociales y descarga de música. Las VLANs están creadas en el switch Cisco Catalyst 4506, éste se encuentra conectado con el Segmentador de Ancho de Banda y hasta aquí llegan o se concentran los enlaces de Fibra Óptica de las diferentes dependencias a 1Gbps y a 10Gbps. Al switch Core también se encuentran enlazados los servidores de la red como el Sistema Integrado, Repositorio Digital, Aulas Virtuales, Telefonía IP entre otros (véase Figura 53).

[16]**CEDIA:** Fundación Consorcio Ecuatoriano para el desarrollo para el Internet Avanzado

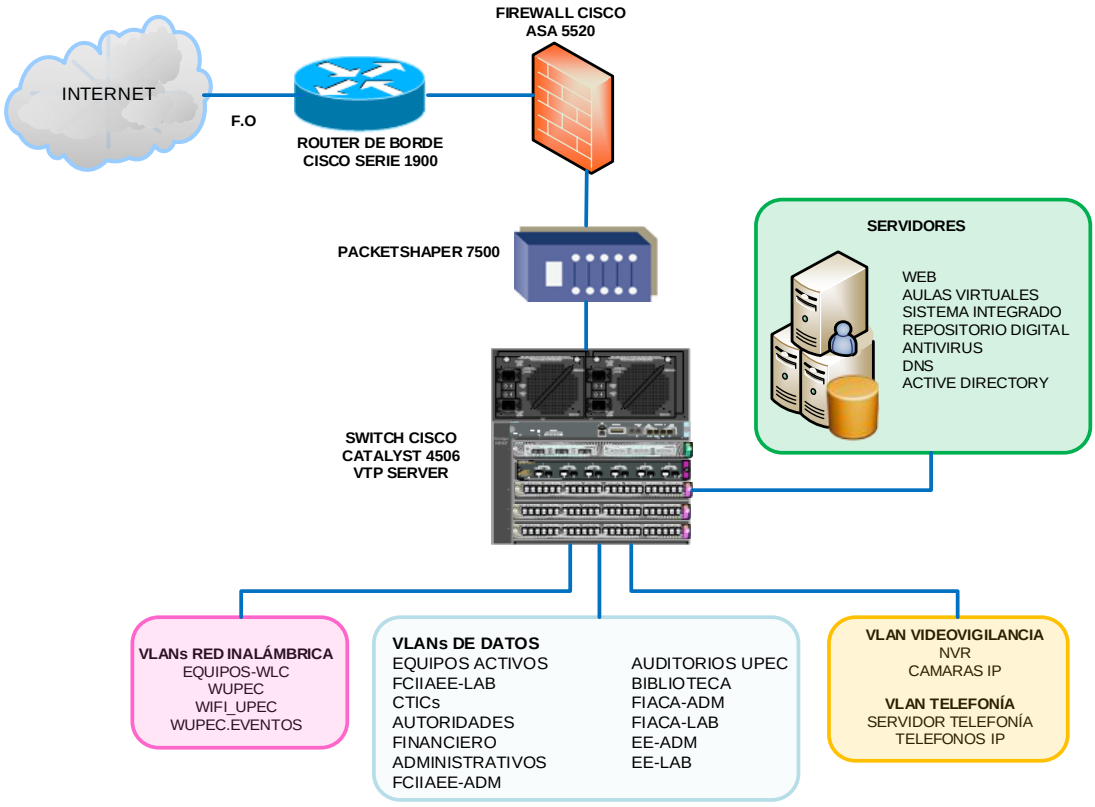


Figura 53. Esquema general de la red UPEC

Fuente: (UPEC, 2015)

Como se mencionó anteriormente el switch Cisco 4506 es el servidor de VLANs, a este conmutador modular capa 3 llegan los enlaces de Fibra Óptica de 1Gbps de todas las dependencias en total 10 a excepción de la interconexión con el edificio de Aulas 2, que es de 10Gbps (véase la Figura 54).

Los enlaces entre pisos o backbone vertical de las dependencias son de Fibra Óptica multimodo de 1Gbps, éstos interconectan en su mayoría a los switches de acceso Cisco Catalyst 2960 los cuales están configurados bajo la modalidad de VTP modo cliente y sus puertos de acceso asignados a las VLANs correspondientes. Para el caso de Aulas 1, 3 y 4 el recorrido de la F.O tanto para monomodo y multimodo es similar ya que el enlace principal llega desde el Edificio Administrativo a la Planta Alta 1 y desde ésta la conexión con multimodo a la Planta Alta 2 y Planta Baja, lo contrario sucede con Aulas 2, los enlaces de F.O se concentran en la Planta Baja

en el switch Cisco Catalyst 3560 y desde aquí se distribuyen los enlaces y comunicación a las plantas superiores como se ilustra en la Figura 54.

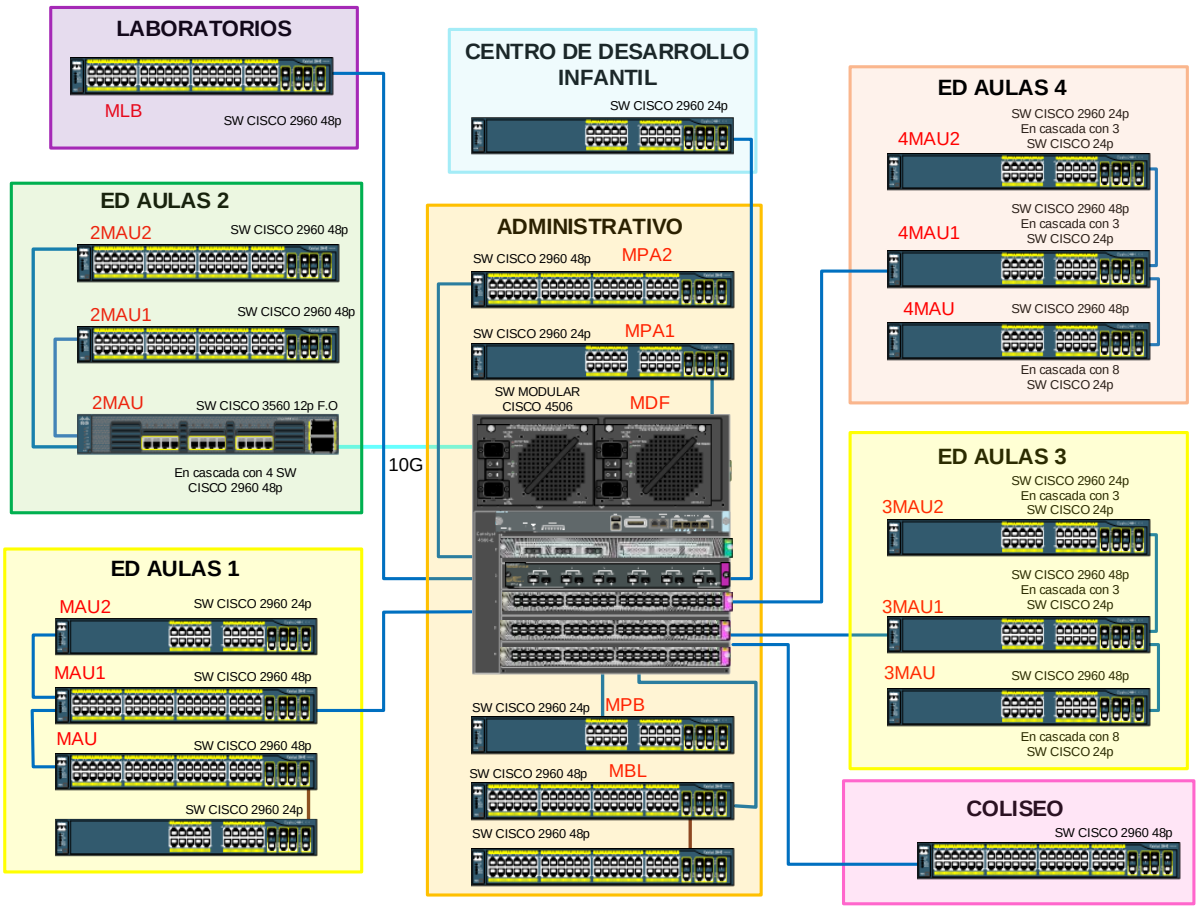


Figura 54. Enlaces de Fibra Óptica e interconexión de Equipos

Fuente: (UPEC, 2015)

3.1.3 Descripción de la WLAN

La Universidad Politécnica Estatal del Carchi cuenta con una red inalámbrica de área local a la vanguardia de la tecnología pero lamentablemente al no establecer las políticas de uso y asignación adecuada de los recursos el servicio conforme crece el número de usuarios y aplicaciones ha ido degradándose y por ende es sumamente importante determinar los lineamientos de asignación de recursos o Calidad de Servicio y de seguridad en la WLAN con el fin de alcanzar una red inalámbrica de mejores prestaciones y escalable.

La red inalámbrica básicamente está formada por dos componentes que son: los Puntos de Acceso y la Controladora inalámbrica Cisco WLC 5508 cuya capacidad permite la gestión y administración de hasta 500 AP y 7000 clientes inalámbricos. La WLC está atada al switch Cisco Catalyst 4506 por medio de un enlace en modo trunk (F.O multimodo a 1Gbps) por el cual sólo están permitidas las VLANs 2, 64, 68 y 72 funcionales para la WLAN del campus. La VLAN 2 está exclusivamente dedicada a la asignación de direccionamiento para los equipos inalámbricos mientras que las otras corresponden a los segmentos útiles para los usuarios los cuales obtienen direcciones IP dinámicamente mediante el servicio DHCP configurado en el siwtch core.

Las VLANs 64, 68 y 72 están ligadas a la WLC mediante interfaces dinámicas creadas y configuradas en la controladora, por ejemplo la VLAN 64 con nombre WUPEC en el switch core corresponde a la interfaz dinámica wupec perteneciente a la red inalámbrica WUPEC, exactamente lo mismo sucede con la VLAN 68, cuya interfaz dinámica es wifi_upec y WLAN WIFI_UPEC, para el caso de VLAN 72 pertenece a la WLAN WUPEC.EVENTOS e interfaz dinámica wupec.eventos, esta descripción se ilustra de mejor forma en la Figura 55.

Los Puntos de Acceso del campus corresponden a modelos del fabricante Cisco para ambientes indoor (1131, 1141 y 1262) y outdoor (1552). Estos AP pueden ser controlados y gestionados por la controladora a través del protocolo CAPWAP (sección 2.1.7).

Como se ha señalado anteriormente esta red actualmente maneja una configuración sencilla y sin proyección en base a que su nivel de seguridad se limita a una contraseña del tipo WPA2/Personal para el caso de WUPEC mientras que las otras WLAN no tienen restricción de acceso es decir no incorporan ningún mecanismo de seguridad sin contar con la ausencia en el manejo adecuado de los recursos que provoca saturación además de otro factor importante que es la pérdida de conectividad por existir zonas o áreas sin cobertura sobretodo en el interior de los edificios de Aulas.

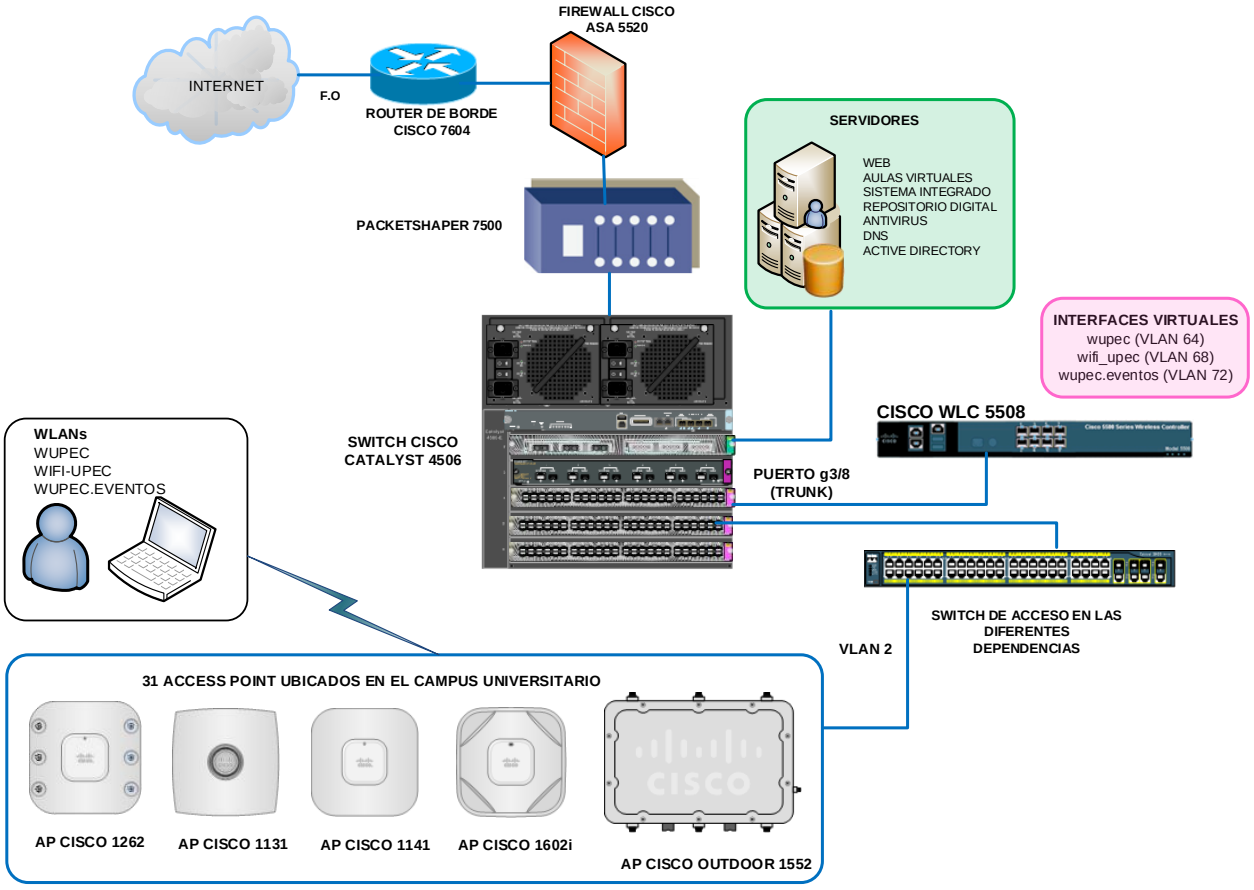


Figura 55. Esquema de la red inalámbrica de la UPEC

Fuente: (UPEC, 2015)

3.2 ÁREAS DE COBERTURA Y EVALUACIÓN DE LA UBICACIÓN DE LOS PUNTOS DE ACCESO

Los 31 Puntos de Acceso se encuentran distribuidos en el Edificio Administrativo, Edificio de Laboratorios, Aulas 1 y Aulas 2, además de cuatro AP para el área externa o espacios verdes. En el caso de Aulas 3, Aulas 4, Coliseo y demás áreas con influencia de usuarios se determinará en este estudio el número de Puntos de Acceso requerido a través de herramientas de simulación de áreas de cobertura. A continuación en la Tabla 18 se detallan los equipos actualmente instalados, su ubicación, modelo y dirección IP correspondientes.

Nro	PUNTOS DE ACCESO	UBICACIÓN	DIR IP	MODELO
1	AP1-PRUEBAS	REDES/DATA CENTER	172.x.2.61	1131
2	AP9-ADMIN-PA2-IZ	ED-ADMIN-PA2-IZ	172.x.2.29	1131
3	AP16-AULAS1-PA1-DR2	ED-AULAS1-PA1-DER2	172.x.2.32	1041
4	AP4-ADMIN-PB-LAB	ED-ADMIN-PB-LAB	172.x.2.35	1041
5	AP2-ADMIN-PB-CENTRAL	ED-ADMIN-PB-CENTRAL	172.x.2.36	1131
6	AP10-ADMIN-RECTORADO	RECTORADO	172.x.2130	1131
7	AP8-ADMIN-PA2-DR	ED-ADMIN-PA2	172.x.2.31	1131
8	AP17-AULAS1-PA1-IZ	ED-AULAS1-PA1-IZ	172.x.2.14	1262
9	AP19-AULAS1-PA2-IZ	ED-AULAS1-PA2-IZ	172.x.2.16	1262
10	AP13-AULAS1-PB-DR	ED-AULAS1-PB-DR	172.x.2.12	1262
11	AP6-ADMIN-BIBLIOTECA1-PA	BIBLIOTECA PA	172.x.2.37	1602i
12	AP3-ADMIN-PB-DR	ED-ADMIN-PB-DR	172.x.2.28	1141
13	AP19-BIBLIOTECA-HEMEROTECA	BIBLIOTECA	172.x.2.38	1602i
14	AP14-AULAS1-PB-IZ	ED-AULAS1-PB-IZ	172.x.2.11	1262
15	AP18-AULAS1-PA2-DR	ED-AULAS1-PA2-DR	172.x.2.15	1262
16	AP5-ADMIN-AUDI-BIBLIOTECA	AUDITORIO - BIBLIOTECA	172.x.2.33	1041
17	AP15-AULAS1-PA1-DR1	ED-AULAS1-PA1-DR	172.x.2.13	1262
18	AP11-ADMIN-EXTERNO-DC-1552	ED AMIN DATA-CENTER	172.x.2.9	1552
19	AP12-AULAS1-HOLD	ED-AULAS1-PB	172.x.2.24	1262
20	AP22-AULAS2-PB-DR	ED-AULAS2-PB-DR	172.x.2.18	1262
21	AP26-AULAS2-PA1-IZ	ED-AULAS2-PA1-IZ	172.x.2.19	1262
22	AP29-AULAS2-PA2-CENTRO	ED-AULAS2-PA2-CENTRO	172.x.2.34	1041
23	AP28-AULAS2-PA2-IZ	ED-AULAS2-PA2-IZ	172.x.2.21	1262
24	AP27-AULAS2-PA2-DR	ED-AULAS2-PA2-DR	172.x.2.22	1262
25	AP30-AULAS2-PB-EXTERIOR	EXTERIOR ED-AULAS2-PB	172.x.2.26	1262
26	AP23-AULAS2-PB-IZ	ED-AULAS2-PB-IZ	172.x.2.17	1262
27	AP25-AULAS2-PA1-DR	ED-AULAS2-PA1-DR	172.x.2.20	1262
28	APEXTERNO2-1552	ED AULAS 2	172.x.2.10	1552
29	AP24-AULAS2-PB-LAB-IZ	ED-AULAS2-PB-LAB INTERNO	172.x.2125	1262
30	AP21-EDIF-LAB-AUDITORIO	AUDITORIO-LABORATORIOS	172.x.2.23	1262
31	AP20-EDIF-LAB-EXTERIOR	EXTERIOR ED-LABORATORIOS-1ANT	172.x.2.27	1262

Tabla 18. Distribución de Puntos de Acceso WLAN UPEC

Fuente: (UPEC, 2015)

Con la utilización de la herramienta de Site Survey "Ekahaul" en conjunto con el recorrido físico por las instalaciones se plasma la infraestructura inalámbrica actual de la Universidad con el fin de determinar las áreas de cobertura de cada uno de los Puntos de Acceso instalados.

En la Figura 56 se ilustra el área de cobertura de los tres Puntos de Acceso instalados en la Planta Baja del Edificio Administrativo, en donde se puede apreciar que el RSSI (Indicador de fuerza de la señal recibida) para una señal óptima está en el rango de -40 a -60 dBm, mientras que para la parte izquierda de esta edificación no posee actualmente una señal óptima de cobertura.

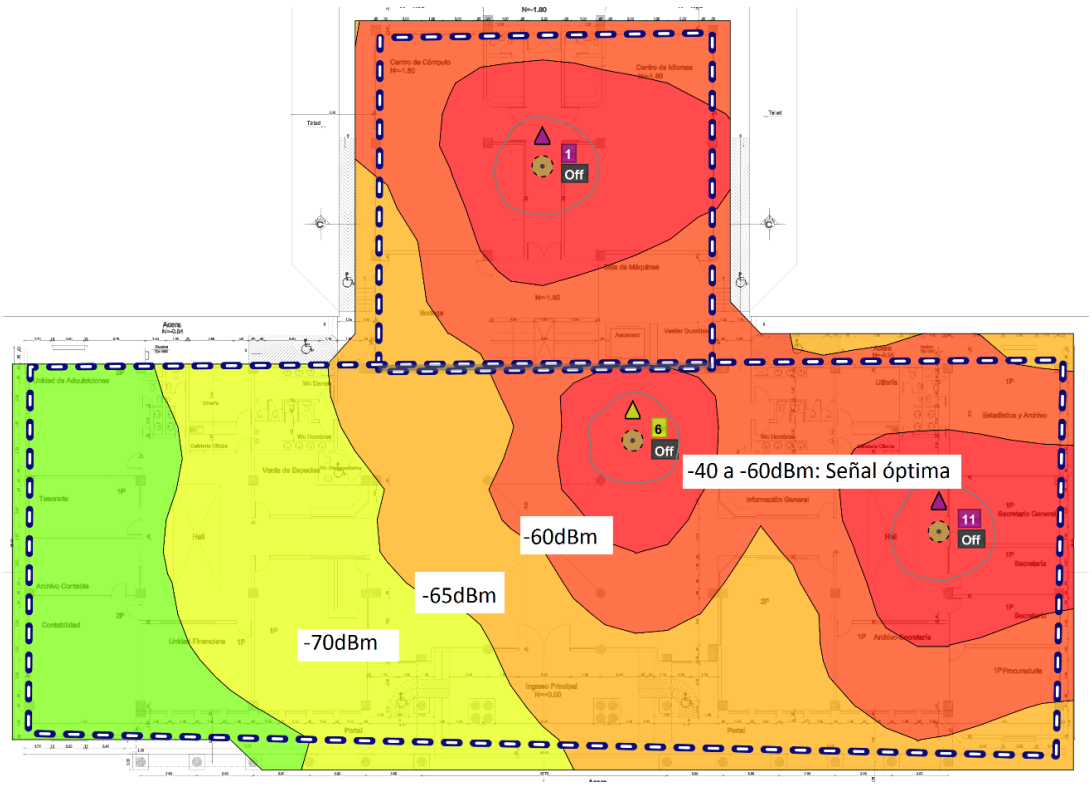


Figura 56. Área de cobertura Planta Baja Edificio Administrativo

Fuente: Propia

La Figura 57 representa el área de cobertura proporcionada por los dos Puntos de Acceso de la Planta Alta 1 del Edificio Administrativo, se puede verificar que la parte centro y principalmente el lado derecho no cuentan con una señal óptima.

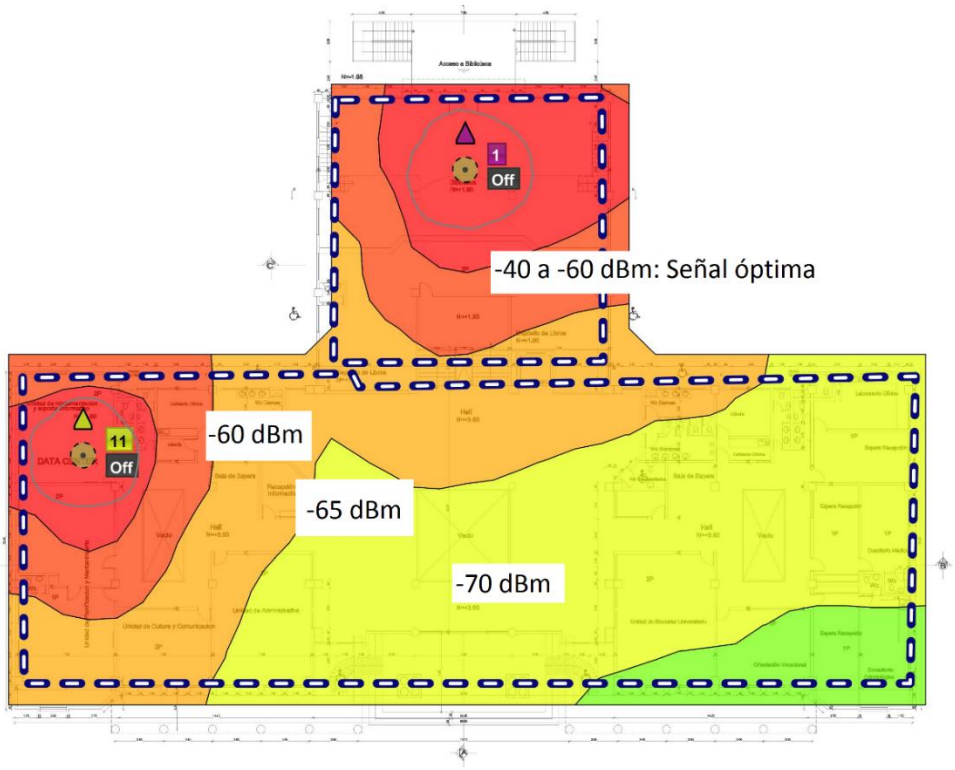


Figura 57. Área de Cobertura Edificio Administrativo Planta Alta 1

Fuente: El Propia

La Figura 58 ilustra el área de cobertura de los cuatro Access Points que actualmente proporcionan servicio tanto para la Planta Alta 2 como para la Biblioteca Planta Alta y se puede verificar que en esta zona la distribución y su ubicación son adecuadas. De igual forma la Figura 59 provee el esquema de cobertura para la Planta Alta 3 donde el AP está exclusivamente asignado para dar servicio a la sala de reuniones de Rectorado, en lo que respecta a las dependencias conjuntas al Rectorado por parte del Departamento de Tecnologías no se ha considerado pertinente.

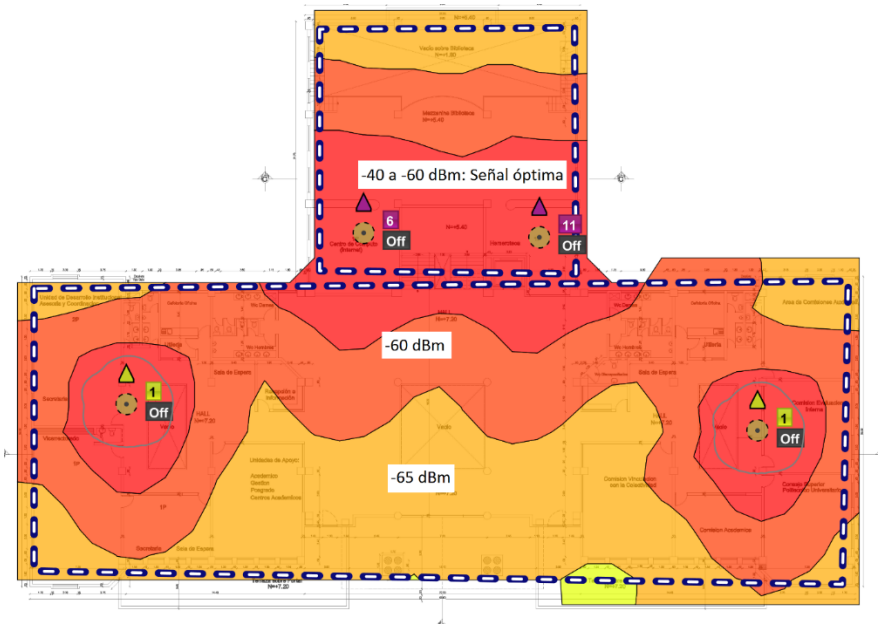


Figura 58. Área de cobertura Edificio Administrativo Planta Alta 2

Fuente: Propia

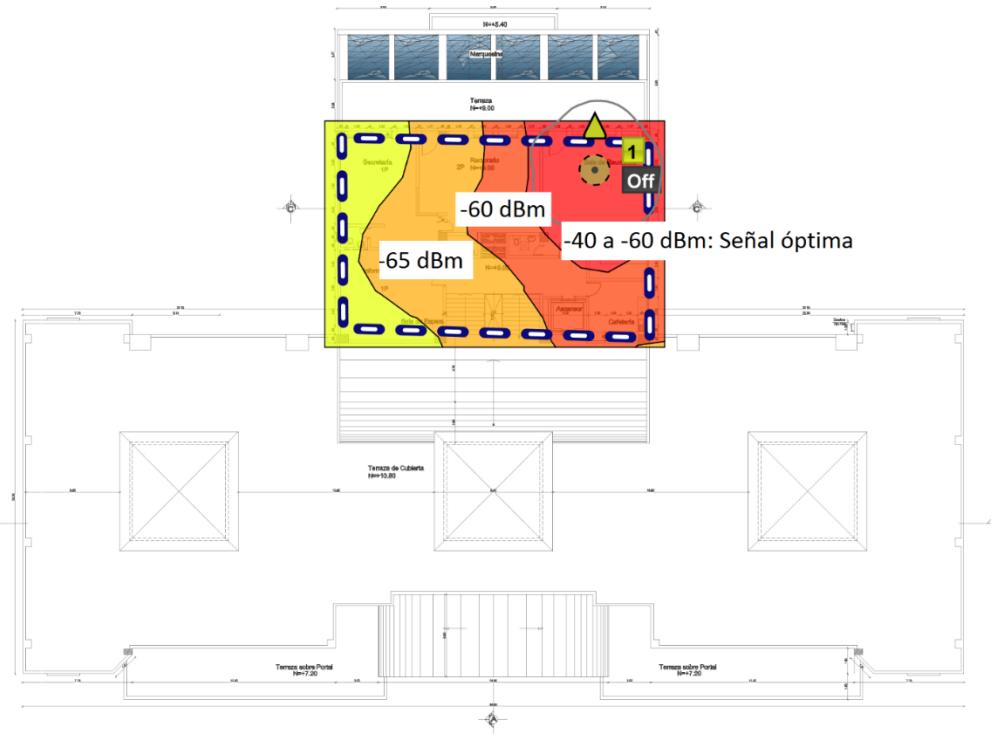


Figura 59. Área de Cobertura Edificio Administrativo Planta Alta 3

Fuente: Propia

La Planta Baja de Aulas 1 cuenta con tres Puntos de Acceso Cisco de modelo 1262 con tres antenas externas cada uno, colocados dos en los extremos y uno en la parte centro dando como resultado el área de cobertura que se puede apreciar en la Figura 60. Cabe señalar que la mayor parte de los estudiantes en sus horas libre se concentran en esta área por lo que se recomienda considerar la instalación de otro AP para mejorar las prestaciones del servicio inalámbrico.

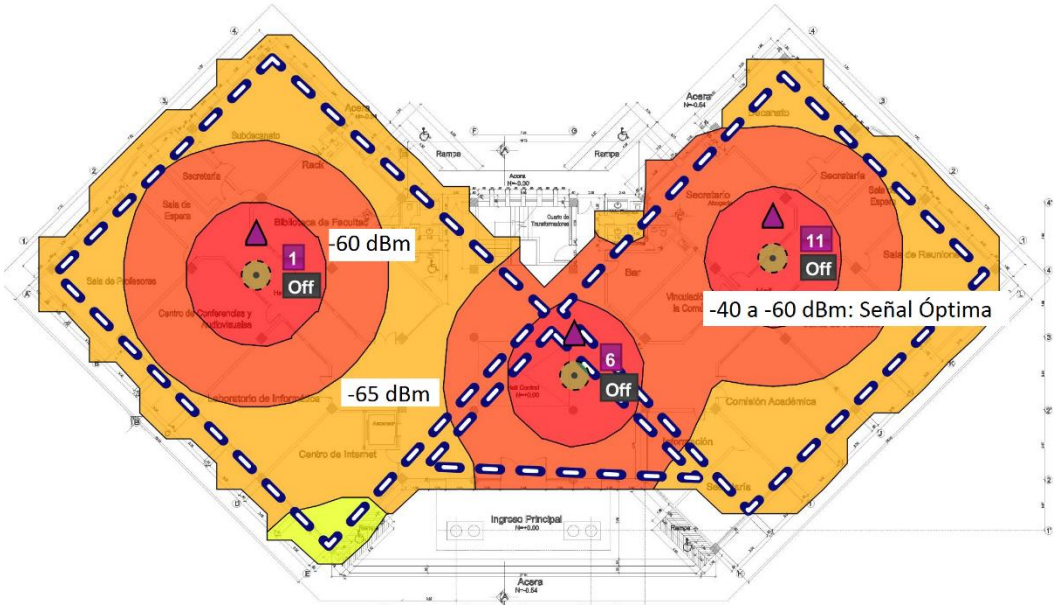


Figura 60. Área de Cobertura Edificio Aulas 1 Planta Baja

Fuente: Propia

En la Figura 61 se presenta el esquema de cobertura de señal inalámbrica para la Planta Alta 1, en éste se puede comprobar que la señal es un tanto baja para el área de secretaría y Dirección de Escuela, posteriormente en la Figura 62 se puede apreciar la Planta Alta 3 en dónde la parte centro de esta área no cuenta con una señal inalámbrica óptima, por lo que sería conveniente reubicar e incrementar el número de Puntos de Acceso en estas dos áreas.

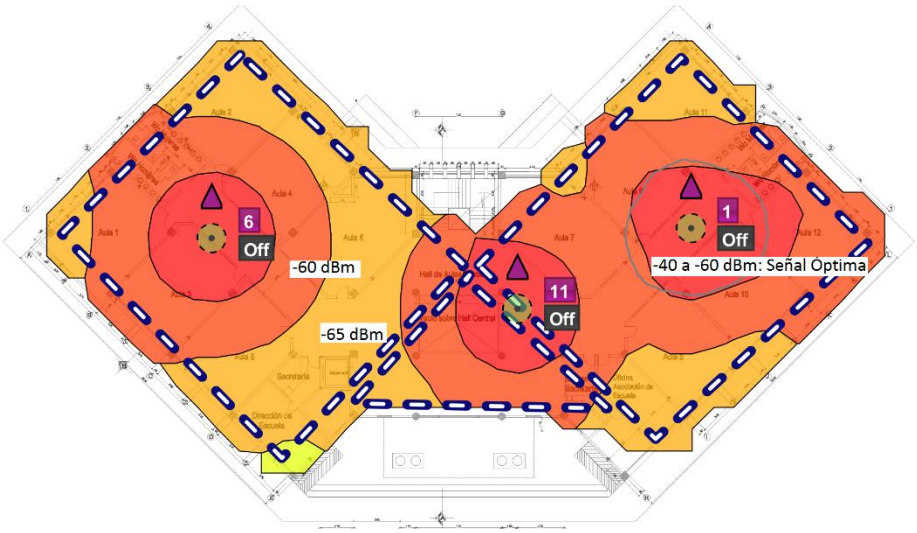


Figura 61. Área de Cobertura Edificio Aulas 1 Planta Alta 1

Fuente: Propia

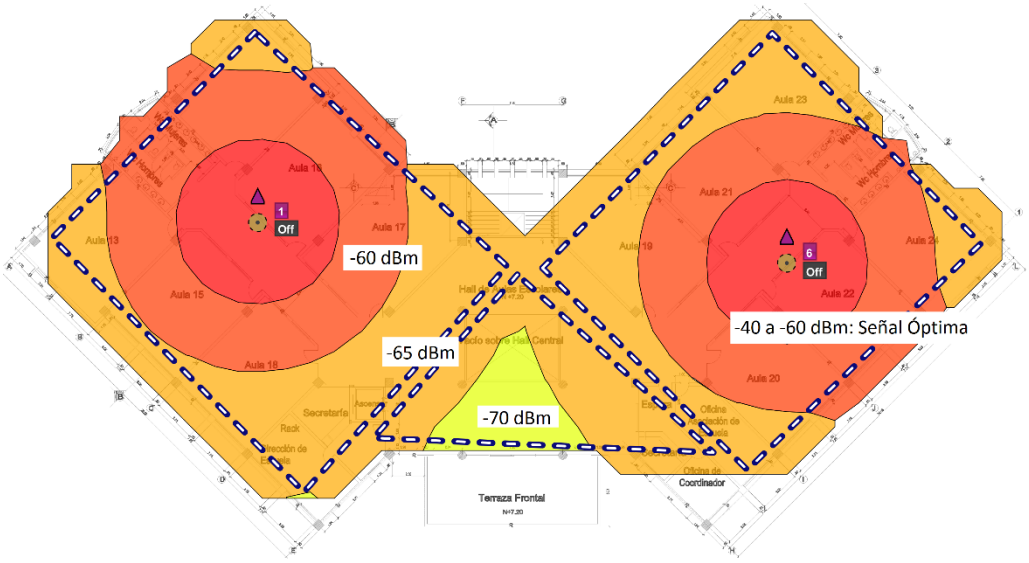


Figura 62. Área de Cobertura Edificio Aulas 1 Planta Alta 2

Fuente: Propia

En el caso del Edificio de Aulas 2 la distribución de Puntos de Acceso difiere a la distribución de Aulas 1 a pesar de tener el mismo diseño y arquitectura debido a los diferentes requerimientos de las dependencias en este edificio que se explican en breve.

En la Planta Baja existen tres Puntos de Acceso tanto en el lado izquierdo como en el derecho además de uno ubicado en el Laboratorio de la Facultad, con esta distribución se tiene una señal inalámbrica óptima a excepción del Hold del edificio (véase la Figura 63).

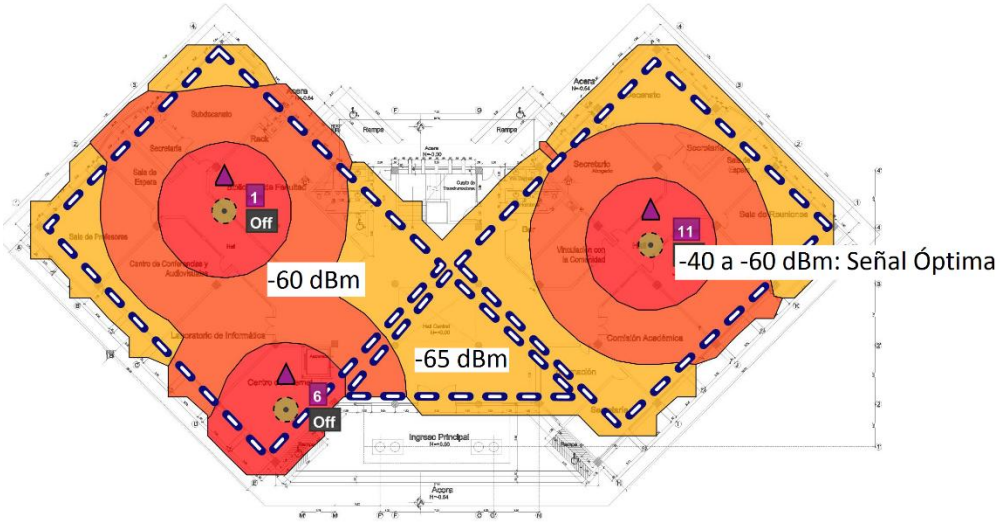


Figura 63. Área de Cobertura Edificio Aulas 2 Planta Baja

Fuente: Propia

De igual forma ocurre en la Planta Alta 1 en dónde existen dos AP, uno en cada ala del Edificio, verificándose de esta forma que no hay una señal óptima en su centro y que sería conveniente extender debido a que los estudiantes se concentran en esta área masivamente (véase Figura 64). Lo contrario sucede con la distribución de Planta Alta 3 en donde la señal es óptima y es brindada por tres puntos de acceso (véase Figura 65).

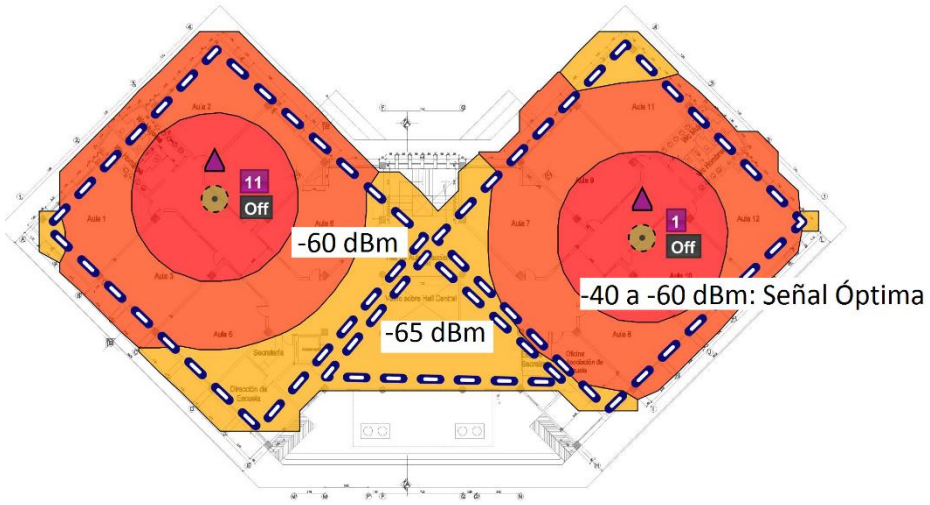


Figura 64. Área de Cobertura Edificio Aulas 2 Planta Alta 1

Fuente: Propia

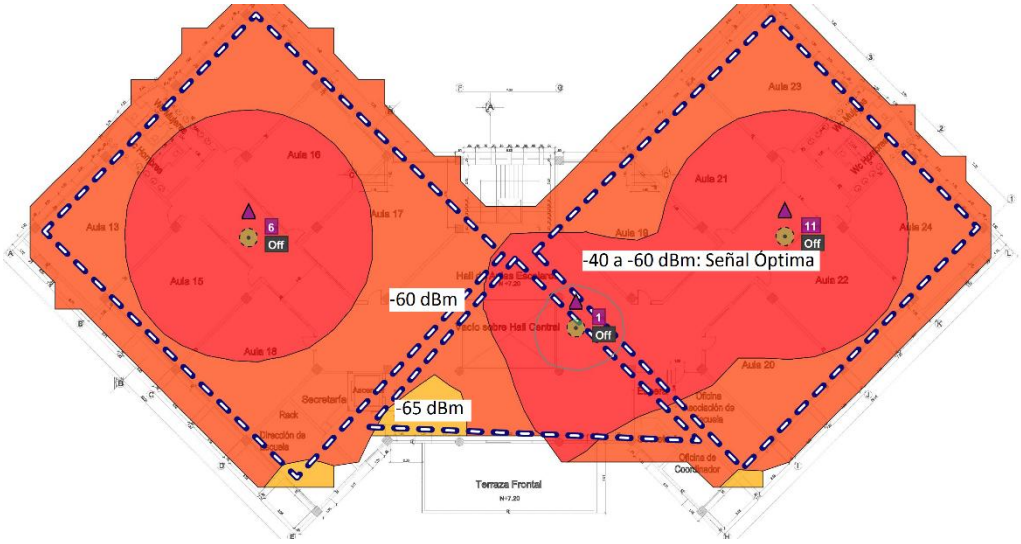


Figura 65. Área de Cobertura Edificio Aulas 2 Planta Alta 2

Fuente: Propia

En lo que corresponde a los Edificios de Aulas 3 y 4 actualmente no cuentan internamente con Puntos de Acceso por lo que más adelante en este estudio se recomienda una distribución y el modelo a utilizar.

En la Figura 66 se muestra el Punto de Acceso ubicado en el Auditorio de Planta Baja del Edificio de Laboratorios, los responsables del Departamento de Tecnología de la UPEC han creído conveniente ubicar solo este equipo puesto que en esta área específica concurren usuarios para ciertos eventos o conferencias, lo que no ocurre con las demás espacios del edificio ya que en la actualidad no se encuentran utilizados.

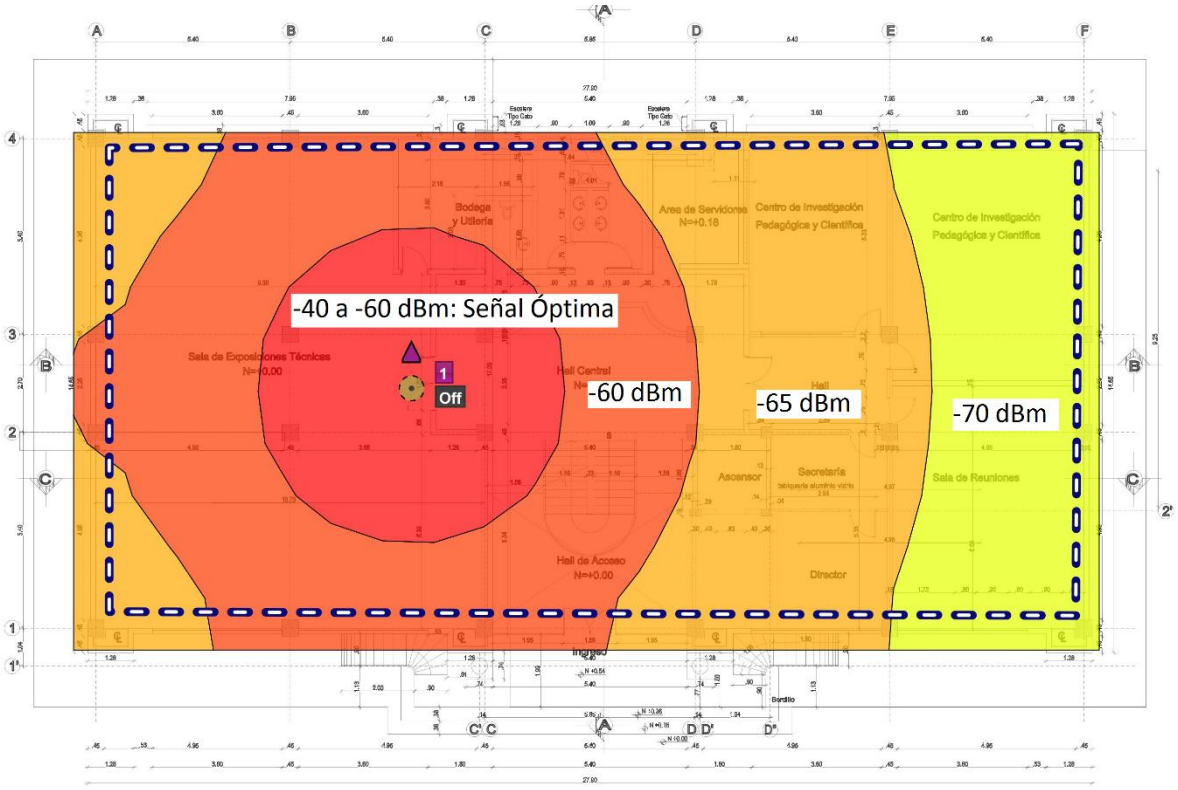


Figura 66. Área de Cobertura Edificio de Laboratorios Planta Baja

Fuente: Propia

Finalmente en la Figura 67 se presenta la distribución de los Puntos de Acceso para exteriores en el campus universitario, se puede identificar que la señal inalámbrica actual cubre un 60%

del área de manera óptima por lo que acorde a las políticas de Estado y de Educación Superior el requerimiento es el 100% para uso de todos los entes universitarios en especial de los estudiantes siendo importante extender la cobertura.

Figura 67. Área de Cobertura en los exteriores del Campus Universitario

Fuente: Propia

3.3 MONITOREO DEL TRÁFICO DE LA WLAN

Para el monitoreo de tráfico de las WLAN de la Universidad Politécnica Estatal del Carchi se utilizaron dos herramientas anteriormente descritas en la sección 2.2.6 (NTOP y PacketShaper) con la finalidad de determinar el comportamiento actual de la red inalámbrica además de la identificación de la información relacionada con el tipo, volumen y protocolos más utilizados por los usuarios con el objetivo de plantear las políticas de QoS adecuadamente en base el entorno de la UPEC.

Como se había indicado inicialmente en el análisis de la situación actual de la WLAN de la UPEC el ancho de banda de acceso a Internet contratado por la institución al proveedor de servicios actualmente es de 60 Mbps (véase Figura 68), los cuales están distribuidos acorde a los requerimientos y necesidades de cada una de las VLANs existentes en el campus.

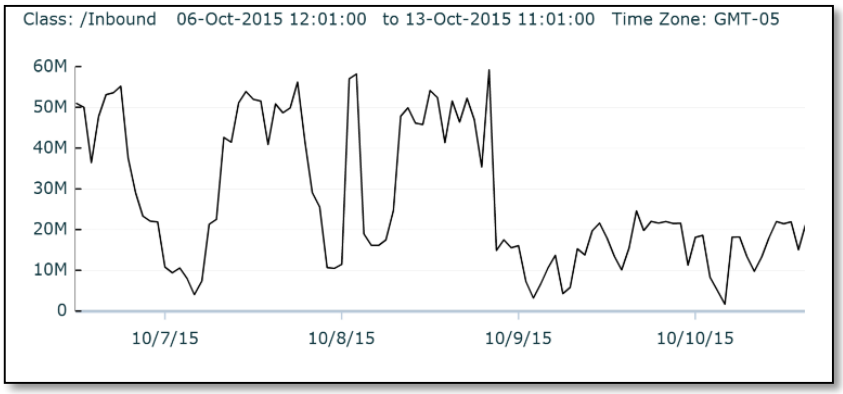


Figura 68. Ancho de Banda de acceso a Internet

Fuente: (PacketShaper, UPEC)

En la Figura 69 y 70 se puede apreciar con más exactitud la tasa promedio de la utilización del ancho de banda de acceso al Internet en dónde la mayor utilización es por parte de la WIFI_UPEC identificada en el PacketShaper como "WIFI-68" a través de aplicaciones SSL y HTTP.

Inbound

Inbound Link Utilization: 52% — **Total Bytes Received: 14.1G**

Average Rate	Average Rate (bps)	% of Total
WIFI-68/SSL	7.2M	23%
WIFI-68/SSL-No-Cert	5.4M	17%
WIFI-68/HTTP	3.7M	12%
ADMINISTRATIVO/SSL-No-Cert	3.2M	10%
WIFI-68/Default	1.6M	5%
WUPEC/HTTP	1.4M	4%
ADMINISTRATIVO/Default	1.2M	4%
BIBLIOTECA/HTTP	841k	3%
ADMINISTRATIVO/SSL	800k	3%
LAB-EADM-COMERCIO/Default	546k	2%
All other classes	5.4M	17%

Figura 69. Utilización de Ancho de Banda de acceso a Internet por VLAN

Fuente: (PacketShaper, UPEC)

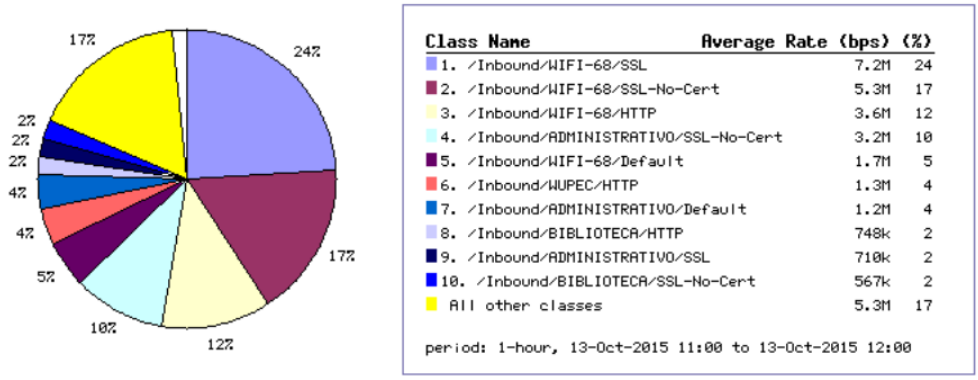


Figura 70. Estadística del uso de Ancho de Banda

Fuente: (PacketShaper, UPEC)

Con el uso del software de monitoreo NTOP y la configuración de un puerto SPAN en el switch de core Cisco Catalyst 4506 como espejo a la VLAN 64 (WUPEC) se obtuvo las siguientes estadísticas en cuanto al top de las aplicaciones más utilizadas. En la Figura 71 se puede evidenciar que las aplicaciones más habituales son en base a HTTP en un 65%, Quic (UDP Internet Connectios) en un 21,57%, SSL con un 4,27% y Youtube en un 1,38%.

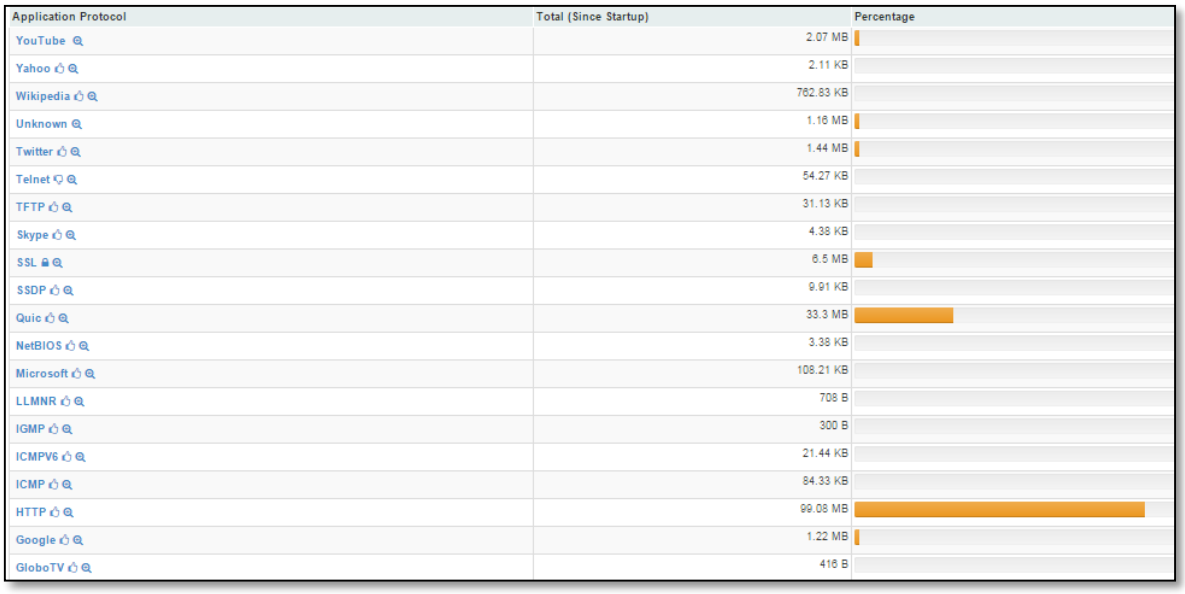


Figura 71. Top de aplicaciones en la WLAN WUPEC con NTOP

Fuente: Propia

La Figura 72 también refleja el top de las aplicaciones utilizadas por los usuarios de manera más esquemática para la WUPEC tomado en otra ocasión, de igual forma el tráfico HTTP representa un porcentaje alto en comparación a las otras teniendo un 33%, seguido de DNS, Dropbox y Youtube, este último con un 6,1%.

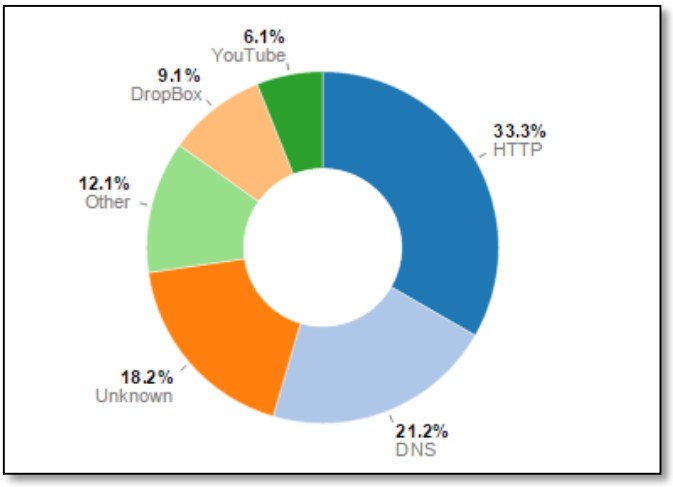


Figura 72. Estadística de la utilización de aplicaciones en la WUPEC con NTOP

Fuente: Propia

Además se puede evidenciar que no existe un control adecuado del manejo del recurso de ancho de banda en la red en especial en la VLAN 64 (WUPEC) en donde con el incremento de los usuarios y aplicaciones presenta picos al límite máximo acarreando en sí inconvenientes de saturación en ciertos momentos en esta WLAN siendo calificado por usuarios como inestable ya que los 5Mbps destinadas a éstos no están correctamente balanceados. La Figura 73 y 74 presenta las estadísticas concernientes al consumo de ancho de banda en la WLAN WUPEC.

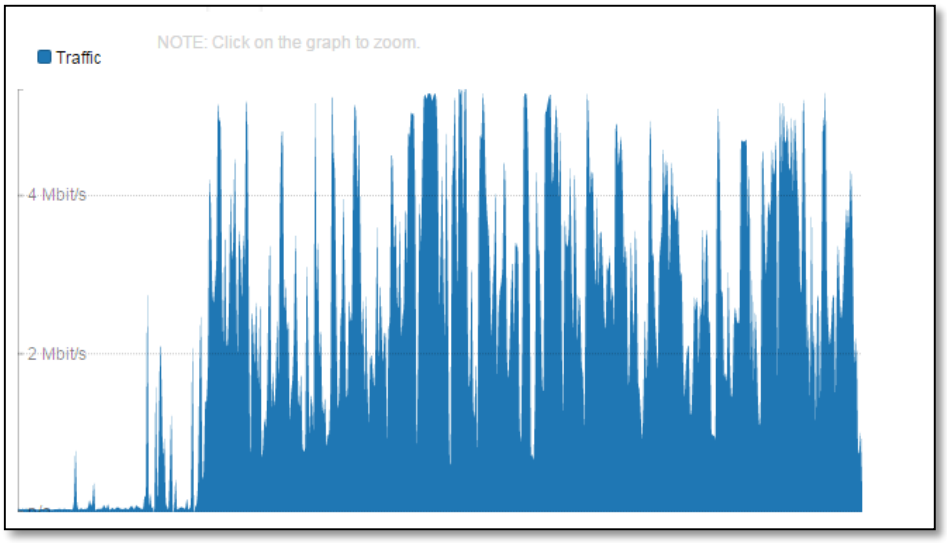


Figura 73. Tráfico generado en la WUPEC visualizado con la herramienta NTOP

Fuente: Propia

	Time	Value
Min	10/13/15 13:08:49	28.55 Kbit
Max	10/13/15 13:35:37	5.29 Mbit
Last	10/13/15 14:06:20	291.37 Kbit
Average	19.28 Mbit	
Total Traffic	1.35 GB	
Selection Time	Tue Oct 13 2015 14:02:13 GMT-0500 (Hora est. Pacífico, Sudamérica)	

Figura 74. Reporte de NTOP de la WLAN WUPEC

Fuente: Propia

Para el caso de la WLAN WIFI_UPEC la Figura 75, 76 y 77 presentan las estadísticas del top de puertos utilizados por los clientes, servidores y aplicaciones respectivamente en este entorno con la ayuda de NTOP. Es necesario recalcar que la utilización de tráfico HTTP supera a otros con un 61,6%, seguido de Youtube y Twitter de manera que este entorno es similar o parecido a lo que sucede en la WUPEC.

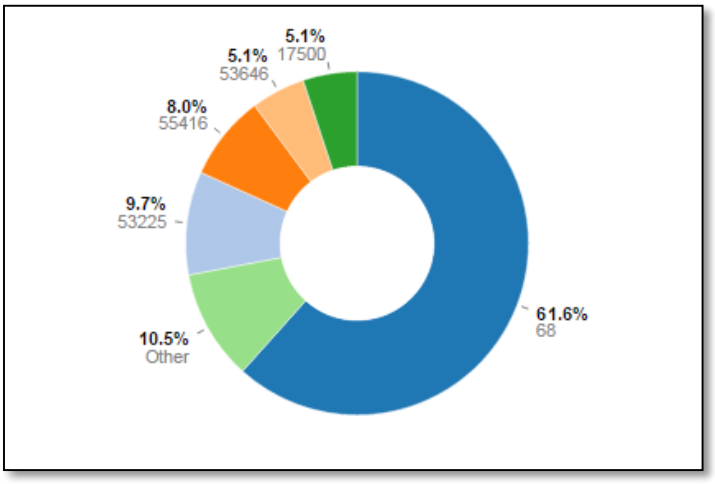


Figura 75. Puertos utilizados por los usuarios inalámbricos (WIFI_UPEC)

Fuente: Propia

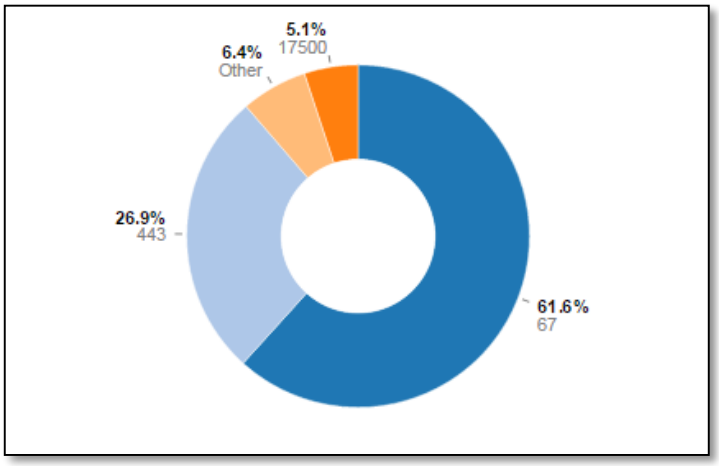


Figura 76. Puertos para comunicación a servidores en la WIFI_UPEC

Fuente: Propia

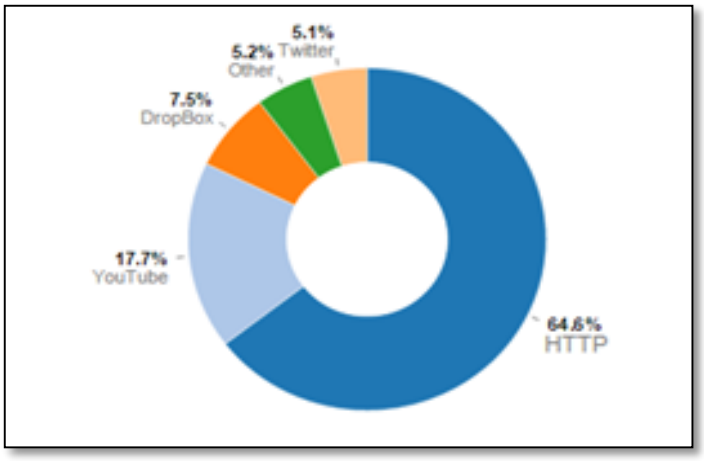


Figura 77. Aplicaciones mayormente utilizadas en la WIFI_UPEC

Fuente: Propia

3.4 ANÁLISIS DE REQUERIMIENTOS PARA QoS

En base al análisis de la situación actual de la WLAN de la Universidad Politécnica Estatal del Carchi a continuación se exponen los requerimientos necesarios para mejorar las prestaciones del servicio inalámbrico:

- Reubicación de algunos Puntos de Acceso e instalación de nuevos para dar mejor cobertura y por ende ampliar el servicio garantizando un buen nivel de señal.

- Disminuir la cantidad de usuarios permitidos por Punto de Acceso, si bien es cierto que la tecnología de Cisco permite hasta un total de 200, en un entorno real esto puede saturar el canal ofreciendo conectividad pero a un rendimiento sumamente bajo. Con este antecedente el fabricante recomienda no más de 30 usuarios asociados a cada AP para garantizar la transmisión de aplicaciones críticas y en tiempo real (Cisco, 2010).

- Se debe tomar en cuenta que una WLAN de alta capacidad puede requerir de muchos Puntos de Acceso pero hay que evitar la interferencia co-canal. La interferencia co-canal

puede disminuir el performance de la red en más de un 50% por ende es necesario planificar muy cuidadosamente la distribución de los canales para evitar este inconveniente.

- Considerar que en espacios donde existe mayor separación entre Puntos de Acceso se debe utilizar mayor potencia de transmisión para garantizar el roaming de los usuarios.

- Establecer mecanismos de redundancia en la red Wireless (Link Aggregation), actualmente el switch core y la controladora inalámbrica se enlazan a 1Gbps teniendo los equipos la capacidad de soportar hasta 8Gbps, lo cual incrementa la capacidad de transmisión y como resultado un acceso mucho más rápido a los servicios y aplicaciones de los usuarios inalámbricos.

- Además de estas variaciones a nivel físico de la WLAN es preciso trabajar a nivel del manejo del tráfico, por ende es imprescindible definir las políticas de asignación de los recursos de ancho de banda para las tres redes inalámbricas existentes en el campus universitario y la prioridad a las aplicaciones acorde a los objetivos institucionales.

- Implementar QoS en la WLAN de la UPEC y en la red de datos a través 802.1p y DiffServ para garantizar servicios de calidad de extremo a extremo.

3.5 ANÁLISIS DE REQUERIMIENTOS PARA LA SEGURIDAD EN LA WLAN

El desarrollo de políticas y procedimientos de seguridad es crucial para una WLAN de hecho una red inalámbrica sin seguridad no puede garantizar Calidad de Servicio de tal forma que el nivel de protección debe mantenerse y mejorarse durante toda la vida de las instalaciones. A continuación se definen los requerimientos recomendados para garantizar la confidencialidad, integridad y disponibilidad de las transmisiones a través de la red wireless de la UPEC con los recursos actuales:

- Utilizar un mecanismo de control de acceso para los usuarios de la red inalámbrica como por ejemplo la autenticación Web (Seguridad de Capa 3), uso de Active Directory y RADIUS para autorizar a los clientes con las credenciales correctas además de limitar el número de sesiones por usuario para evitar la congestión de la WLAN.

- Actualizar el IOS de la controladora inalámbrica que a su vez proporciona la actualización automática a los Puntos de Acceso y nuevas funcionalidades tanto en rendimiento como mecanismos de seguridad.

- Crear Listas de Control de Acceso para la restricción del acceso de los usuarios de la WLAN a las diferentes VLANs de datos de la institución, ya que el objetivo principal de la red inalámbrica es proporcionar la navegación por Internet.

- Reemplazar el uso de Telnet por SSH para el acceso remoto a los diferentes dispositivos de la WLAN como la controladora inalámbrica y los Puntos de Acceso.

- Concientizar a los usuarios para que sean totalmente responsables de salvaguardar sus credenciales de acceso a la red inalámbrica además de no abrir o descargar contenido no confiable por ende es importante que los ordenadores en especial los portátiles tengan instalado y actualizado el software antivirus.

CAPÍTULO IV. IMPLEMENTACIÓN DE QOS Y SEGURIDAD

Una vez establecidos los requerimientos en las secciones 3.4 y 3.5 relacionados con la Calidad de Servicio y Seguridad a efectuar en la WLAN de la UPEC a continuación se describen las configuraciones y recomendaciones que posibilitan mejorar las prestaciones del servicio de la red inalámbrica.

4.1 IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

Es preciso recordar que para contar con un servicio o conexión inalámbrica satisfactoria es primordial además de la clasificación y priorización del tráfico también corregir falencias con respecto a la ubicación de los Puntos de Acceso o mal diseño de las áreas de cobertura, distribución de canales y manejo de los niveles de potencia de la señal adecuados con la finalidad de proporcionar un servicio de excelente calidad totalmente transparente para los usuarios.

4.1.1 Propuesta de reubicación e instalación de Puntos de Acceso

Con la utilización del software de Site Survey Ekahaul en acompañamiento del recorrido físico por las instalaciones del campus universitario con un Punto de Acceso para pruebas de marca Cisco y modelo AIR-CAP3702I-A-K9 se corrobora la siguiente reubicación e instalación de los mismos en las diferentes dependencias de la UPEC.

Para el caso del Edifico Administrativo es recomendable ubicar tres nuevos Puntos de Acceso, uno en la Planta Baja lado izquierdo (véase Figura 78) y dos en la Planta Alta con ubicación en el centro y lado derecho además de la reubicación del AP Redes como lo indica la Figura 79.

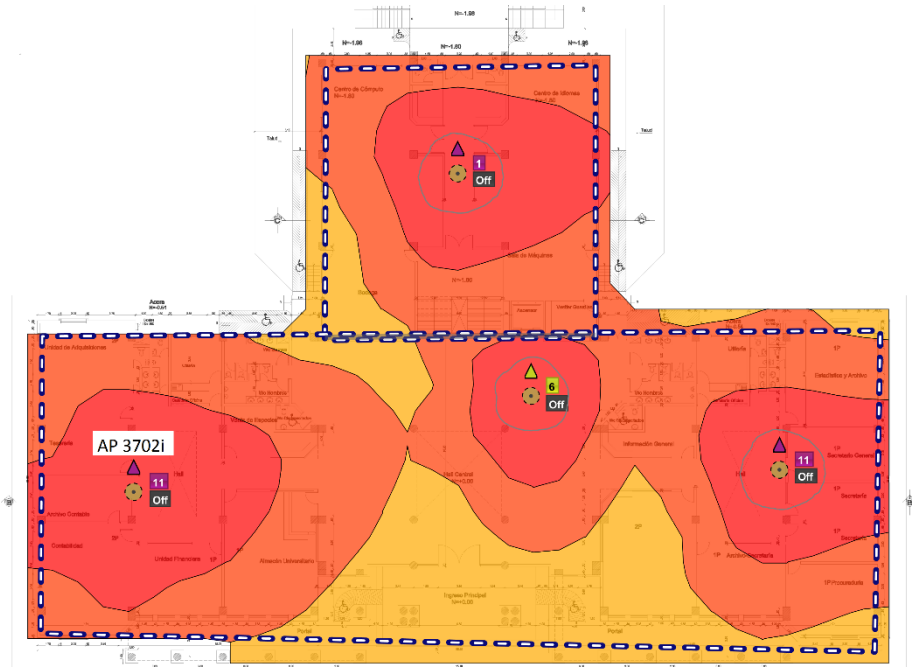


Figura 78. Cobertura AP 3702I en la Planta Baja Edificio Administrativo

Fuente: Propia

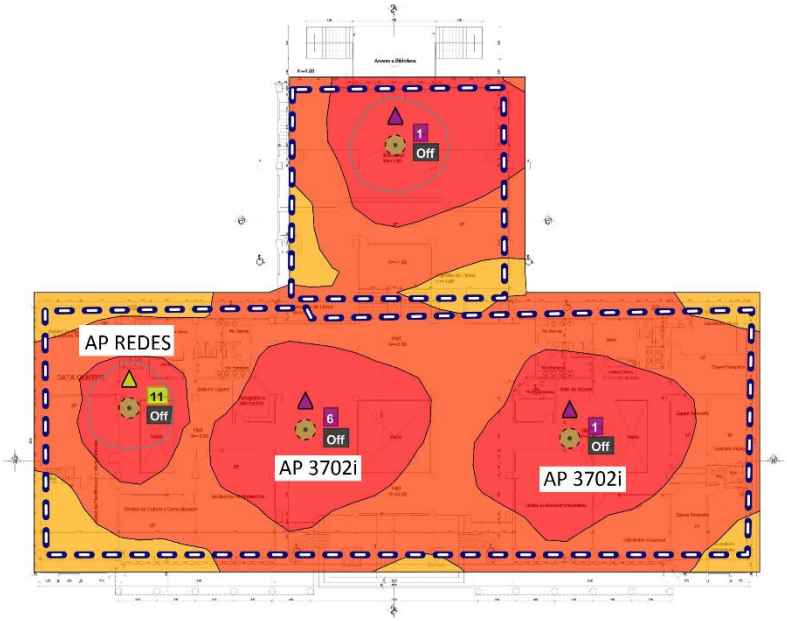


Figura 79. Cobertura y reubicación AP en la Planta Alta 1 Edificio Administrativo

Fuente: Propia

En el Edificio de Aulas 1 es pertinente realizar los siguientes cambios con el afán de mejorar las áreas de cobertura y nivel de señal:

- *Planta Baja:* Reubicación de los tres Puntos de Acceso además de la instalación de un AP 3702i para ampliar la cobertura en esta área (véase Figura 80).

- *Planta Alta 1:* Reubicación de los tres Puntos de Acceso e instalación de uno nuevo (AP 3702i) de manera que el AP 3702i y el AP 1040 cubren el ala izquierda de esta planta como se ilustra en la Figura 81.

- Planta Alta 2: Se requiere un nuevo AP para el hall además de la reubicación de los dos Puntos de Acceso de los extremos, es decir colocarlos en el centro de cada ala como se presenta en la Figura 82.

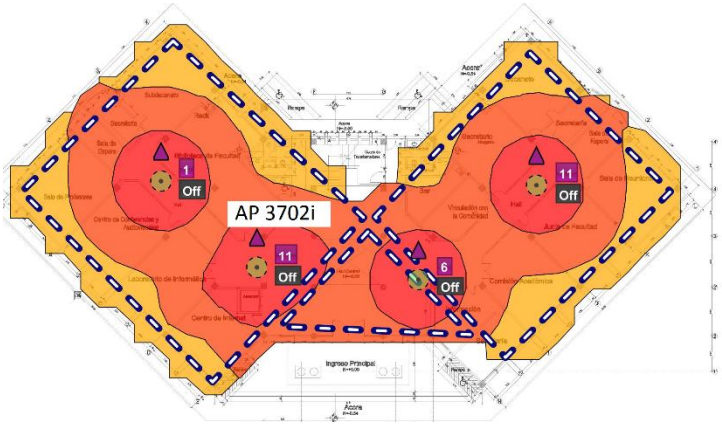


Figura 80. Cobertura y reubicación AP en la Planta Baja Edificio Aulas 1

Fuente: Propia

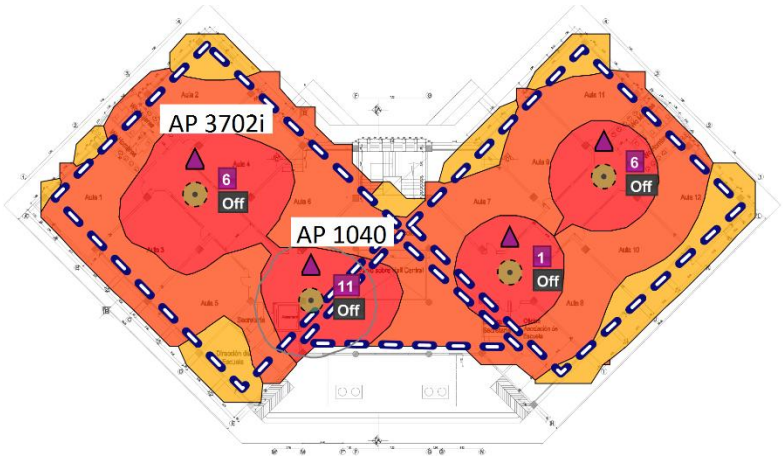


Figura 81. Cobertura y reubicación AP en la Planta Alta 1 Edificio Aulas 1

Fuente: Propia

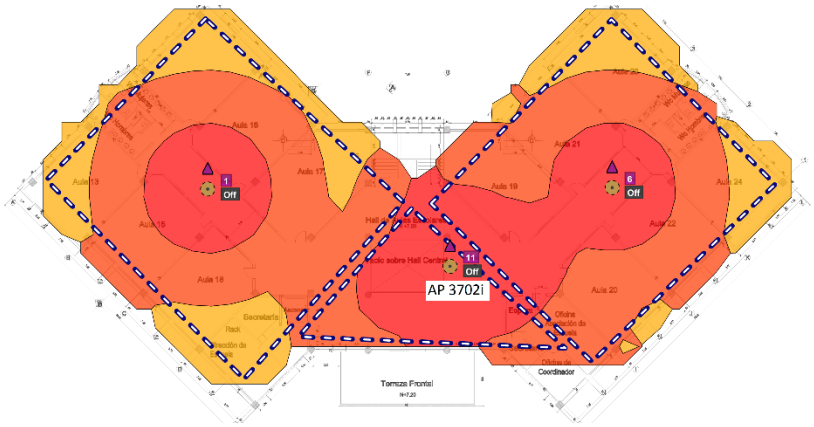


Figura 82. Cobertura y reubicación AP en la Planta Alta 2 Edificio Aulas 1

Fuente: Propia

Para el Edificio de Aulas 2 se realiza las siguientes sugerencias:

- *Planta Baja:* Ubicación de un nuevo AP 3702i para el área centro además de la reubicación de los tres Puntos de Acceso existentes como se indica en la Figura 83.

- *Planta Alta 1:* El hall actualmente presenta deficiencia de cobertura de tal forma que para compensar este inconveniente es necesario planear la ubicación de un nuevo AP, dando como resultado una señal óptima como se ilustra en la Figura 84.

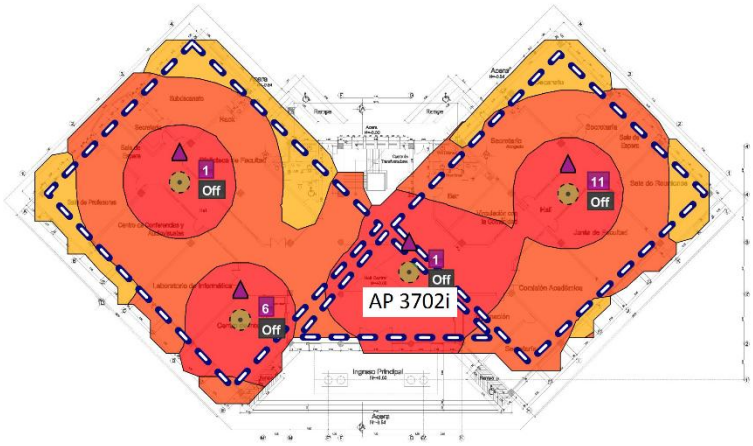


Figura 83. Cobertura y reubicación AP en la Planta Baja Edificio Aulas 2

Fuente: Propia

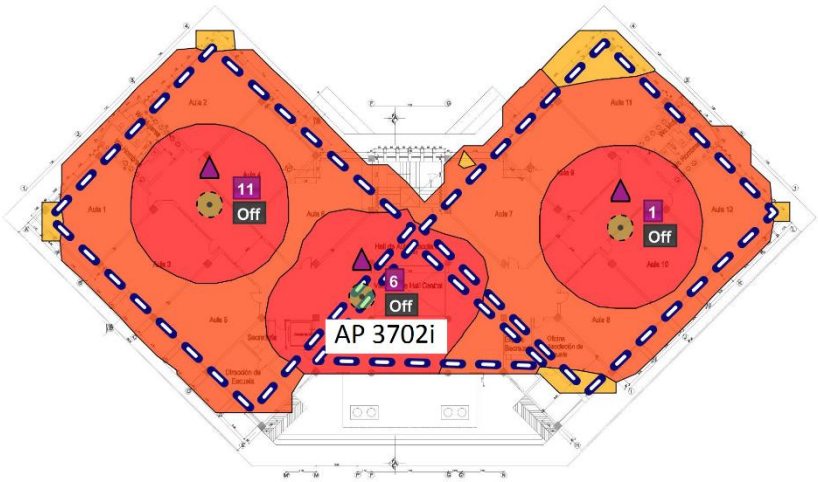


Figura 84. Cobertura AP 3702I en la Planta Alta 1 Edificio Aulas 2

Fuente: Propia

Aulas 3 y 4 actualmente no cuentan con un despliegue de red inalámbrica dentro de sus instalaciones respectivamente por ser construcciones relativamente nuevas y su implementación se prevé en los próximos meses, por ende se propone la distribución de Aulas 2 ya que el diseño y espacio físico es relativamente igual a éste. Siendo un total de 10 Puntos de Acceso

distribuidos en cada edificación sumando en total la cantidad de 20 cuyo presupuesto económico se adjunta en ANEXOS. A continuación se describe la distribución y ubicación, sirviendo este diseño para los dos edificios puesto que como se mencionó anteriormente tienen igual espacio arquitectónico:

- *Planta Baja:* Se propone la instalación de dos Puntos de Acceso para cada ala del edificio, uno para la cobertura en el hall y otro AP para el laboratorio de esta dependencia (véase Figura 85).

- *Planta Alta 1:* Dos Puntos de Acceso para cada uno de los extremos de los Edificios con la finalidad de dar servicio a las aulas y adicionalmente un AP para la cobertura en el hall como se presenta en la Figura 86.

- *Planta Alta 2:* Similar a la distribución de la Planta Alta 1, es decir tres Puntos de Acceso, dos para los extremos y uno para la parte centro como se puede apreciar en la Figura 87.

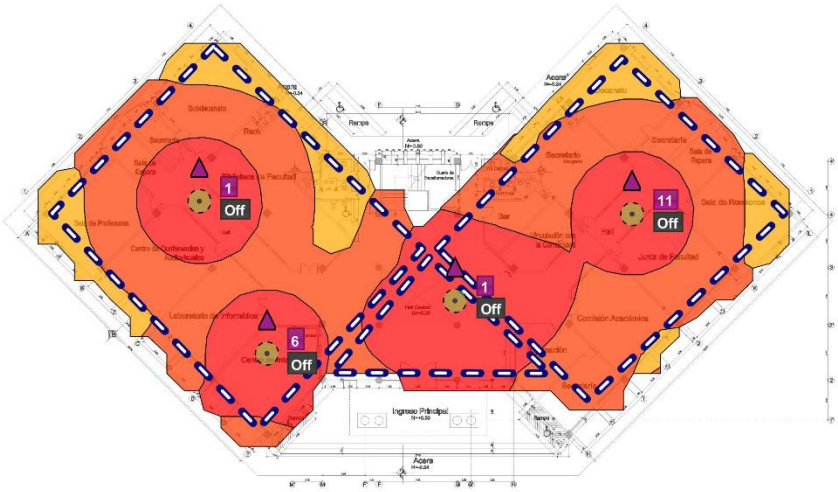


Figura 85. Planta Baja Edificio de Aulas 3

Fuente: Propia

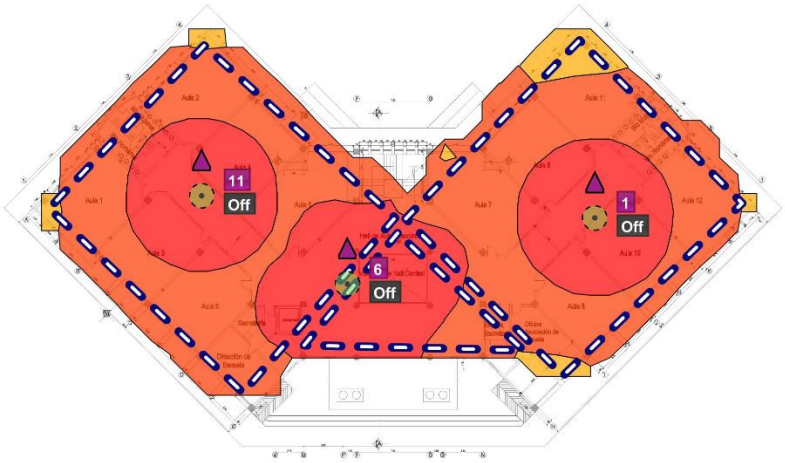


Figura 86. Planta Alta 1 Edificio Aulas 3

Fuente: Propia

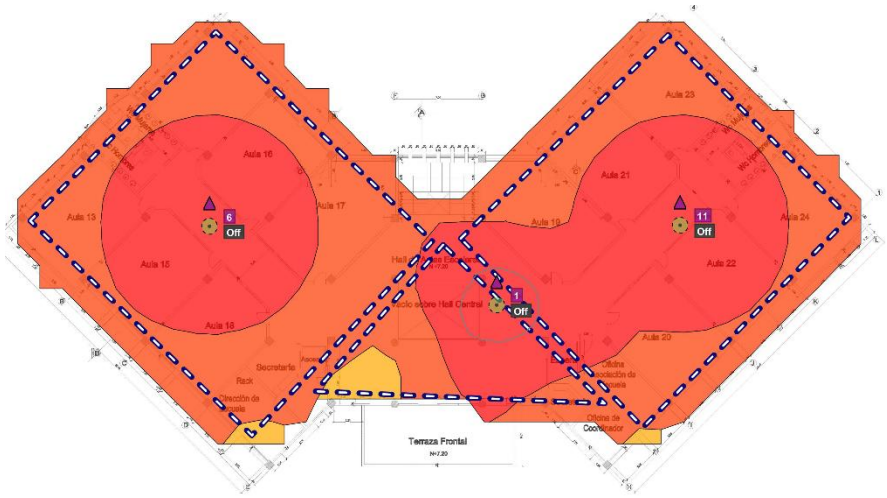


Figura 87. Planta Alta 2 Edificio Aulas 3

Fuente: Propia

Con relación a la cobertura de los espacios públicos y áreas verdes dentro del campus universitario también se considera su ampliación mediante la recomendación de la utilización de dos Puntos de Acceso Cisco modelo AIR-CAP1532E-A-K9, ubicados estratégicamente tal como se ilustra en la Figura 88.

Figura 88. Puntos de Acceso 1532E para ampliación de señal en el campus universitario

Fuente: Propia

4.1.2 Cantidad de usuarios por Punto de Acceso

Según lo recomendado por el fabricante y para el soporte adecuado de aplicaciones críticas y en tiempo real es preciso limitar la cantidad de usuarios a conectarse por Punto de Acceso y para esto dentro de la configuración vía web de la Controladora Inalámbrica, en la Opción WLANs, se selecciona la pestaña Advanced y modifica el parámetro "Maximum Allowed Clients per AP Radio" y se designa en el rango de 30 a 40 usuarios como máximo.

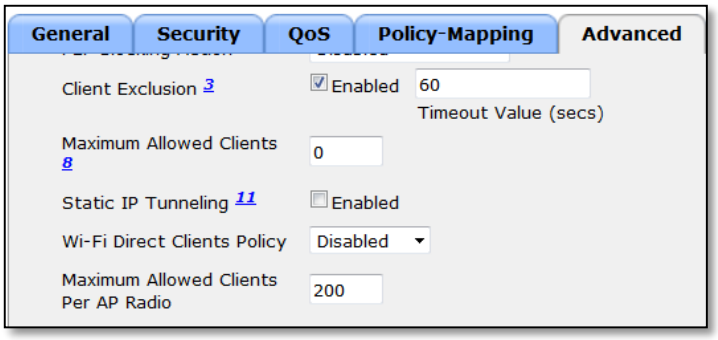


Figura 89. Cantidad de Usuarios por Punto de Acceso

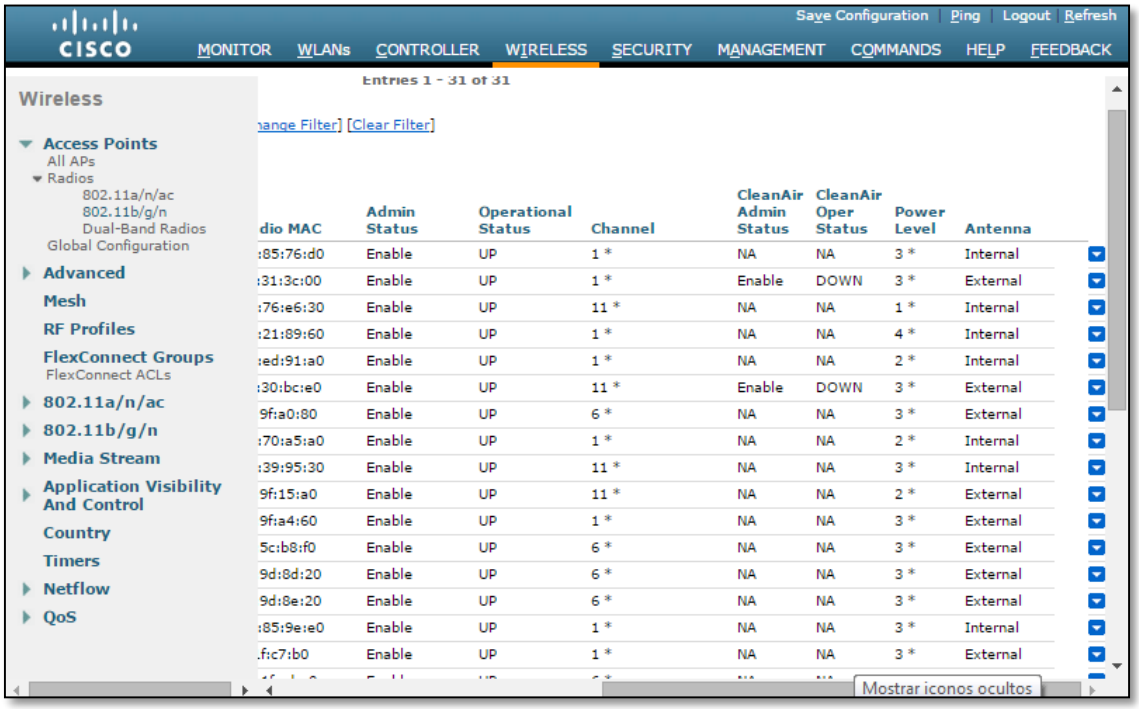
Fuente: Propia

4.1.3 Distribución de canales y niveles de potencia transmitida

Para la cobertura de grandes áreas se dispone de tres canales de radiofrecuencia en la banda de 2,4 Ghz sin solapamiento y estos son el 3,6 y 11. Si éstos no se hallan distribuidos correctamente se puede generar interferencia disminuyendo drásticamente el nivel de la señal y afectando el área de cobertura de cada Punto de Acceso. La solución de Red Inalámbrica Unificada de Cisco permite el manejo de la distribución de canales y el control de la potencia transmitida por cada AP tanto en forma manual como de manera automática, de hecho por default los Controladores Inalámbricos tienen estas características activadas denominada tecnología Clean Air, que permite tener una visibilidad total de lo que ocurre en el medio inalámbrico y esto se produce gracias a las nuevas funcionalidades basadas en software y hardware incorporado en las WLC, entre sus ventajas está la detección, clasificación, ubicación y mitigación de todo tipo de comunicaciones no deseadas posibilitando moldear el entorno mediante reajustes automáticos para optimizar los niveles de señal y superar los problemas de interferencia.

Inicialmente en las WLANs de la UPEC estos parámetros se hallaban configurados manualmente de tal forma que no existía una correcta distribución de canales y mucho menos la asignación adecuada del nivel de potencia, citando un ejemplo todos los AP de una misma planta del Edificio Administrativo se encontraban en el canal 1 y con nivel de potencia máximo es decir 1 correspondiente a 30mW lo que como resultado producía mucho ruido y una señal muy débil para los usuarios. A continuación en la Figura 90 se presenta la configuración de

canales así como el nivel de potencia asignada por el Controlador Inalámbrico haciendo uso de la tecnología Clean Air, el asterisco junto al valor representa la asignación automática.



dio MAC	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Power Level	Antenna
:85:76:d0	Enable	UP	1 *	NA	NA	3 *	Internal
:31:3c:00	Enable	UP	1 *	Enable	DOWN	3 *	External
:76:e6:30	Enable	UP	11 *	NA	NA	1 *	Internal
:21:89:60	Enable	UP	1 *	NA	NA	4 *	Internal
:ed:91:a0	Enable	UP	1 *	NA	NA	2 *	Internal
:30:bc:e0	Enable	UP	11 *	Enable	DOWN	3 *	External
9f:a0:80	Enable	UP	6 *	NA	NA	3 *	External
:70:a5:a0	Enable	UP	1 *	NA	NA	2 *	Internal
:39:95:30	Enable	UP	11 *	NA	NA	3 *	Internal
9f:15:a0	Enable	UP	11 *	NA	NA	2 *	External
9f:a4:60	Enable	UP	1 *	NA	NA	3 *	External
5c:b8:f0	Enable	UP	6 *	NA	NA	3 *	External
9d:8d:20	Enable	UP	6 *	NA	NA	3 *	External
9d:8e:20	Enable	UP	6 *	NA	NA	3 *	External
:85:9e:e0	Enable	UP	1 *	NA	NA	3 *	Internal
.f:c7:b0	Enable	UP	1 *	NA	NA	3 *	External

Figura 90. Asignación de canales y niveles de Potencia por Punto de Acceso

Fuente: Propia

4.1.4 Configuración del puerto de backup

Por el momento no se dispone de los componentes necesarios para habilitar enlaces agregados entre el switch core y el controlador inalámbrico, tanto las tarjetas SFP de 1Gbps y los patchcords de Fibra Óptica multimodo se presupuestan en la proforma de los ANEXOS para su posterior compra. Pero ante algún suceso como por ejemplo el daño del puerto del controlador actualmente utilizado se ha configurado el siguiente mecanismo:

- *Configuración de un puerto de backup:* En la pestaña Controller – Interfaces se selecciona una interfaz dinámica en este caso wupec y dentro de la configuración de la misma se tiene el Port Number que indica el puerto que está activo para el enlace con el

switch y en la opción Backup Port designamos el puerto que estaría activo en caso de falla del número 1 (véase Figura 91). Cabe recalcar que esto debe ser configurado para cada una de las interfaces dinámicas creadas inclusive para la interfaz management.

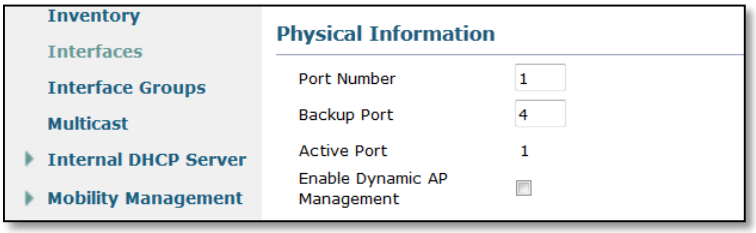


Figura 91. Backup Port

Fuente: Propia

4.1.5 Configuración de QoS

En esta sección se describe la Calidad de Servicio (QoS) desde el punto de vista de la implementación de una WLAN, en este caso basándose en la arquitectura y tecnología de la red inalámbrica de la Universidad Politécnica Estatal del Carchi que utiliza la solución Cisco Unified Wireless:

1. La solución de Red Inalámbrica de Cisco permite habilitar, configurar y editar algunas características de QoS a través del soporte de WMM, dentro de los principales están los perfiles de Calidad de Servicio en el WLC 5508. Cuatro perfiles pueden ser configurados o asignados a una WLAN: platino (AC_VO), oro (AC_VI), plata (AC_BK) y bronce (AC_BE). En la Figura 92 se muestra esta característica que se encuentra en la pestaña Wireless – QoS – Profiles.

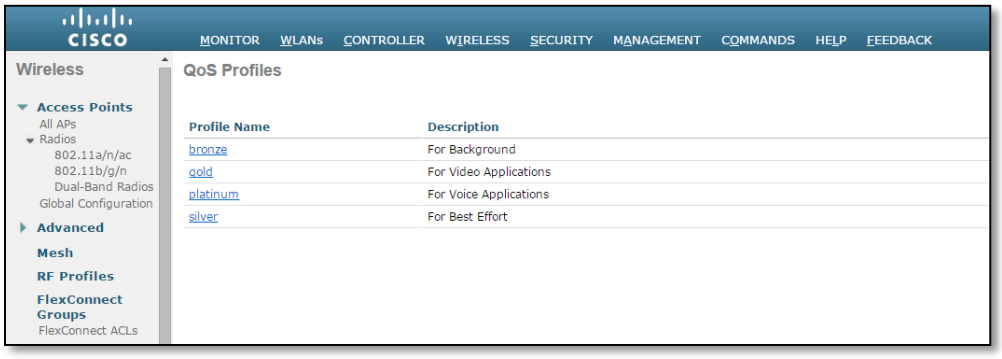


Figura 92. Perfiles QoS en la WLC 5508

Fuente: Propia

2. Cada uno de estos perfiles de QoS permiten la asignación de prioridad IEEE 802.1p (véase la Figura 93), además las opciones con respecto al uso de ancho de banda y RF en especial del tráfico de voz y video se encuentra en la misma pestaña Wireless pero en la sección 802.11b/g/n – RRM – Media como se presenta en la Figura 94. El fabricante recomienda utilizar los valores por defecto ya que están diseñados acorde a los lineamientos y parámetros de WMM para proveer servicios diferenciados.

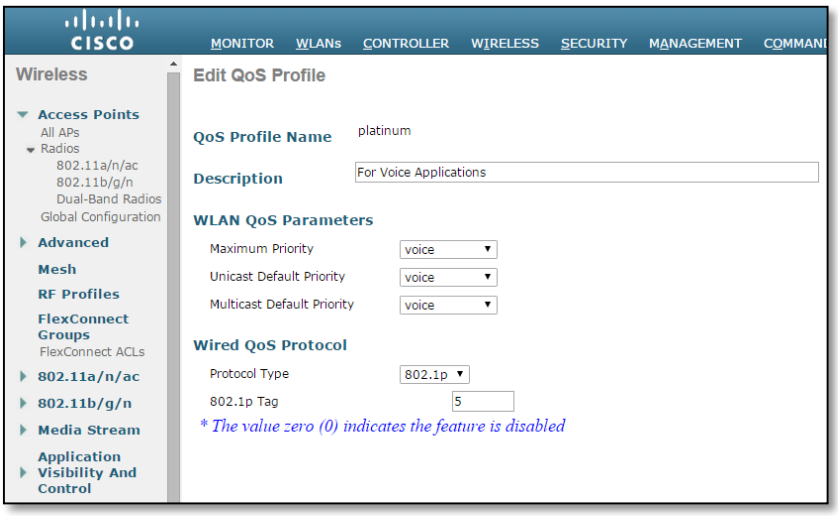


Figura 93. Opciones de Ancho de Banda RF en los perfiles QoS

Fuente: Propia

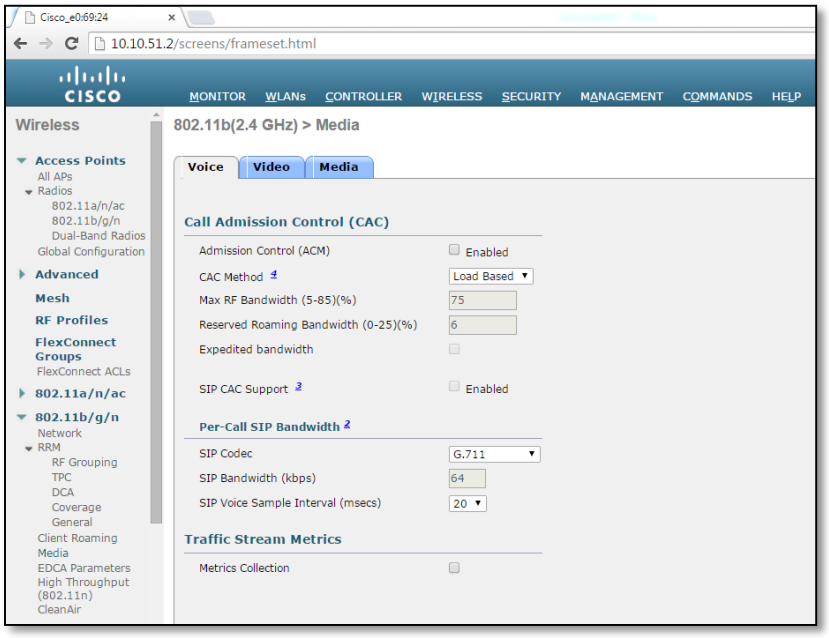


Figura 94. Asignación de Ancho de Banda RF para el tráfico de voz

Fuente: Propia

Es necesario señalar que en una WLAN al utilizar un perfil de QoS determinado la clasificación 802.1p controla dos aspectos importantes:

- Determina la Clase de Servicio (CoS) usada por los paquetes inicializados desde el controlador inalámbrico WLC. El valor CoS de un perfil es utilizado para marcar todas las tramas de una WLAN por ejemplo: una WLAN con un perfil QoS platino tiene una marca de 5 (CoS) de manera que los paquetes enviados desde la WLC usarán esta marca.

- Determina el valor máximo CoS que puede ser utilizado por los clientes conectados a la WLAN. El punto clave es que con una red inalámbrica unificada siempre hay que pensar en términos de 802.11e ya que ésta es la que asume la responsabilidad de la conversión a IEEE 802.1p.

3. Una WLAN puede ser configurada con los diferentes perfiles de QoS y esto va acorde a las políticas definidas por la institución, este parámetro de configuración se encuentra disponible en cada una de las WLANs en la pestaña QoS. En la Figura 95 se muestra el perfil asignado por defecto a WUPEC.

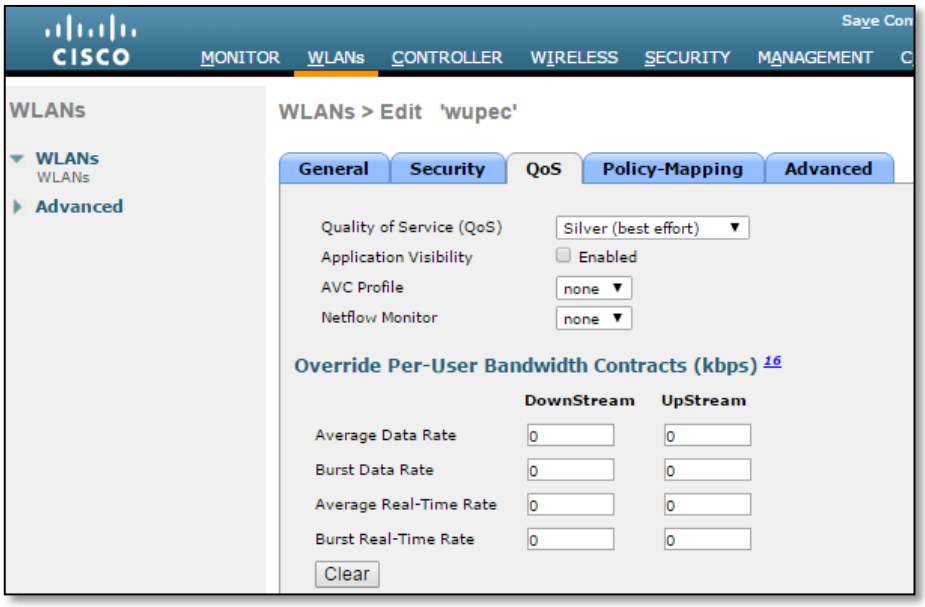


Figura 95. Configuración de Perfil QoS a una WLAN

Fuente: Propia

En cuanto a la asignación de perfiles de QoS a las WLANs existentes en el campus universitario se ha definido lo siguiente:

- WUPEC: Utiliza actualmente la VLAN 64 y está asignado su uso exclusivamente para el personal docente y administrativo de manera que su perfil es “Gold” cuya marca 802.1p es 4.

- WIFI_UPEC: Utiliza la VLAN 68 específicamente para el uso de los estudiantes de manera que el perfil asignado es “Silver” con marca 2.

- WUPEC.EVENTOS: Su finalidad es el acceso temporal de usuarios inalámbricos participantes de eventos, conferencias entre otros y para esto se ha definido también el perfil “Silver” en la VLAN 72.

Cabe resaltar que dentro de cada perfil se maneja la restricción de ancho de banda tanto para tráfico TCP (Average Data Rate & Burst Data Rate) y UDP (Average Real-Time Rate & Burst Real-Time Rate) en un rango de 0 a 60000 Kbps, por defecto la asignación de estos valores es 0 lo que representa que no hay restricción para el ancho de banda.

4. Además de los perfiles de QoS, la política WMM por WLAN puede ser controlada (Figura 96) con las siguientes opciones:

   - Deshabilitado: La WLAN no tiene capacidades WMM, es decir que no permite las negociaciones WMM por lo cual no admite la priorización del tráfico.

   - Permitido: Se pueden conectar a la WLAN los clientes con soporte WMM y clientes no-WMM.

   - Requerido: Sólo clientes WMM pueden ser asociados a esta WLAN.

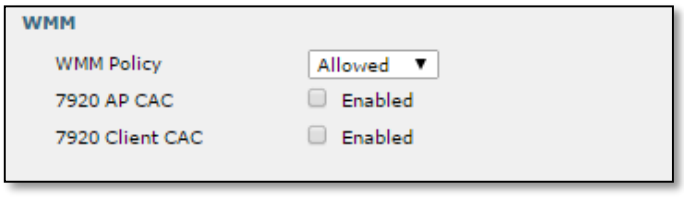


Figura 96. Control de la política WMM

Fuente: Propia

4.1.6 Mapeo 802.11e, 802.1p y DSCP

Una WLAN de datos en una red inalámbrica unificada es un túnel LWAPP (paquetes IP UDP), para mantener la clasificación QoS aplicada al tráfico de la WLAN se requiere de un proceso de mapeo desde DSCP a CoS (Figura 97). Por ejemplo cuando el tráfico clasificado es enviado a un cliente WLAN, ésta trama tiene una marca 802.1p y por ende el AP necesita trasladar a DSCP para el paquete LWAPP que lleva esta trama y tenga la prioridad apropiada en su camino.

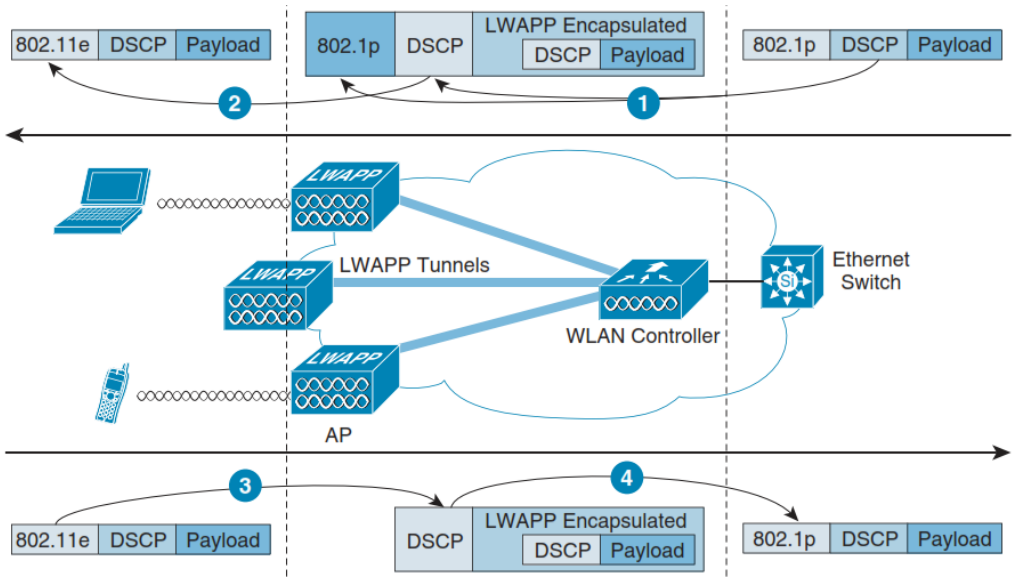


Figura 97. Mapeo 802.11e, 802.1p y DSCP en QoS-WLAN

Fuente: (Cisco, 2010)

A continuación se describe el proceso de mapeo de manera más específica en referencia a la Figura 97:

1. Una trama con una marca 802.1p y un paquete IP DSCP llegan a la interfaz ap manager del WLC (puerto conectado al switch core). El paquete IP DSCP es usado para determinar el DSCP del paquete LWAPP del WLC y 802.1p tiene un marca que corresponde a la tabla de traducción de QoS (véase Tabla 19).

Access Point QoS Traslation Values	IP DSCP	QoS Profile	802.1p	802.11e
Network Control	56 (CS7)	Platino	7	7
CAPWAP Control (802.11 Management)	48 (CS6)	Platino	6	7
Voice	46 (EF)	Platino	5	6
Interactive Video	34 (AF41)	Oro	4	5
Streaming Video	32 (CS4)	Oro	4	5
Mission Critical	26 (AF31)	Oro	3	4
Call Signaling	24 (CS3)	Oro	3	4
Transactional	18 (AF21)	Plata	2	3
Network Management	16 (CS2)	Plata	2	3
Bulk Data	10 (AF11)	Bronce	1	2

Tabla 19. Valores de conversión de un AP QoS

Fuente: (Cisco, 2010)

2. El paquete LWAPP con la marca DSCP llega al AP y se traduce a CoS 802.11e para su posterior envío al cliente WLAN.

3. En el tráfico de retorno la trama 802.11e es enviada al AP y se traduce en un valor DSCP LWAPP.

4. El DSCP del paquete entregado al WLC es igual al DSCP enviado por el cliente WLAN pero el valor CoS 802.1p depende de la correspondencia de la marca DSCP (véase la Tabla 19). Si la opción "Wired QoS Protocol" es ninguno entonces ningún valor 802.1p será establecido.

De manera resumida los múltiples mecanismos de clasificación y las capacidades del cliente requieren muchas estrategias en el ambiente QoS-WLAN:

- Las tablas de control LWAPP requieren el establecimiento de prioridades y están marcados con el DSCP CS6, es decir en 802.11e con la marca 6.

- Los clientes WMM tienen la clasificación de sus tramas igual que los paquetes LWAPP al WLC, esto permite el mapeo CoS a DSCP.

- Los paquetes LWAPP procedentes del WLC tienen una clasificación DSCP que se determina por el DSCP que tiene configurada la interfaz de red LAN de la WLC.

- La clasificación 802.11e es usada cuando se envían tramas desde un AP a un cliente WMM y está determinada por la tabla de traducción DSCP a WMM.

- La interfaz Ethernet LWAPP del AP no utiliza CoS de Capa 2, al contrario tanto el controlador inalámbrico como el AP solamente se comunican utilizando LWAPP de capa 3 y por ende utilizan clasificación DSCP.

- Los Puntos de Acceso deben usar VLAN ID para soportar efectivamente QoS caso contrario no envína las etiquetas 802.1p.

- Los puntos de Acceso no re-clasifican tramas, éstos priorizan el tráfico en base al valor CoS del perfil de la WLAN.

4.1.7 Líneas de comando en el switch de acceso (Conexión AP-switch Cisco 2960)

La configuración de QoS del AP es relativamente trivial por que el switch debe confiar en el DSCP de los paquetes LWAPP que se envían desde el Punto de Acceso, no teniendo mucha relevancia el marcado CoS a continuación los comandos para ejecutar esta acción:

```
interface GigabitEthernet 1/0/3
 switchport access vlan 2
 switchport mode access
 mls qos trust dscp
 spanning-tree portfast
end
```

4.1.8 Líneas de comando WLC- switch Cisco 4506

La decisión de clasificación de Calidad de Servicio en el switch conectado al WLC es un poco más complicado que en el switch conectado al AP, ya que la elección puede ser en confiar en el DSCP o CoS del tráfico que viene del WLC. En esta decisión hay una serie de puntos a tener en cuenta:

- El tráfico entregado al WLC puede ser Upstream (subida) o Downstream (bajada). El tráfico descendente se encapsula en LWAPP y el de subida puede ser encapsulado o sin encapsular.

- Los valores DSCP de los paquetes LWAPP son controlados por las políticas de Calidad de Servicio en el WLC.

- Los valores CoS de las tramas salientes del WLC son fijados por las políticas QoS-WLAN independientemente de que si es tráfico upstream o downstream, encapsulado o sin encapsular.

La siguiente configuración muestra la elección de confiar en el CoS del WLC, esto permite centralizar la gestión de QoS-WLAN en lugar de tener que gestionar la configuración del WLC y una política adicional en la conexión del switch.

```
interface GigabitEthernet3/8
 description ENLACE-WLC
 switchport trunk native vlan 99
 switchport trunk allowed vlan 2,64,68,72
 switchport mode trunk
 mls qos trust cos
end
```

4.2 IMPLEMENTACIÓN DE SEGURIDAD

Dentro del desarrollo del presente estudio se ha revisado varios mecanismos de seguridad aplicados tanto a nivel de capa 2 como en capa 3, la opción que se adapta a la situación actual y en base a los recursos disponibles es la utilización del servicio RADIUS y Active Directory para la realización de la autenticación de los usuarios basado en el acceso web. En la actualidad la Universidad cuenta con un servidor Cisco UCS C220 M3 en el cual se encuentra funcionando el Directorio Activo en Windows Server 2012 por ende el objeto de esta sección es consolidar la interacción con RADIUS, DNS y el controlador inalámbrico además de un servidor web que proporciona una ventana en la que el usuario ingresa sus credenciales de autenticación. Las configuraciones de éstos servicios se describen en la sección de ANEXOS.

4.2.1 Sistema de Autenticación WEB

Para posibilitar la integración entre los diferentes servidores y la red inalámbrica unificada de la Universidad Politécnica Estatal del Carchi es necesario habilitar algunas configuraciones previas en el controlador inalámbrico WLC 5508 para su interacción con RADIUS y Active Directory, a continuación se explican con más detalle estas configuraciones:

1. Habilitar la comunicación con RADIUS en el controlador inalámbrico, para esto es necesario ir a la pestaña Security, en la opción AAA hacer clic en Authenticacion e indicar la dirección IP del servidor y puerto a utilizar 1812, la Figura 98 ilustra este procedimiento.

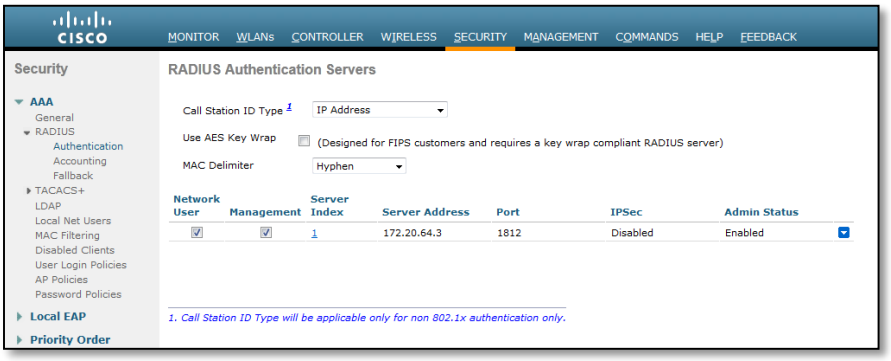


Figura 98. RADIUS Athentication Servers

Fuente: Propia

2. De igual forma se habilita el servicio de Accounting que se encuentra en la pestaña Security, opción AAA, se indica la IP del servidor y el puerto en este caso 1813 (véase la Figura 99).

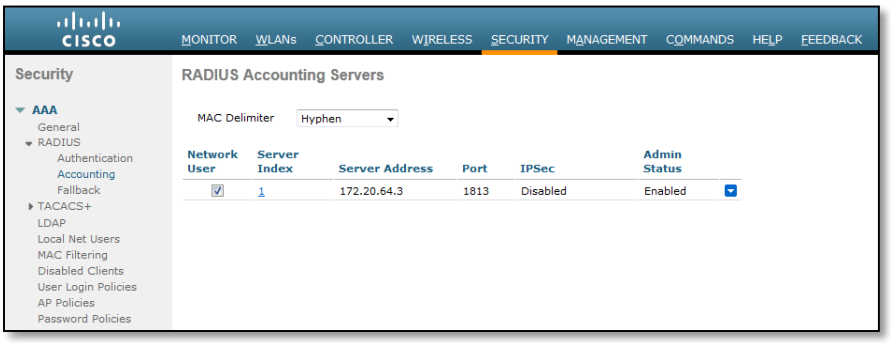


Figura 99. RADIUS Accounting Servers

Fuente: Propia

3. Es necesario crear una Lista de Control de Acceso para redireccionar todo el tráfico de la WLAN creada en el controlador inalámbrico hacia el servidor. La primera regla es con respecto al tráfico de salida cuyo origen es el servidor y destino la red de Internet (0.0.0.0/0) y la segunda regla referente al tráfico de entrada en donde el origen proviene de la red de Internet con destino al servidor.

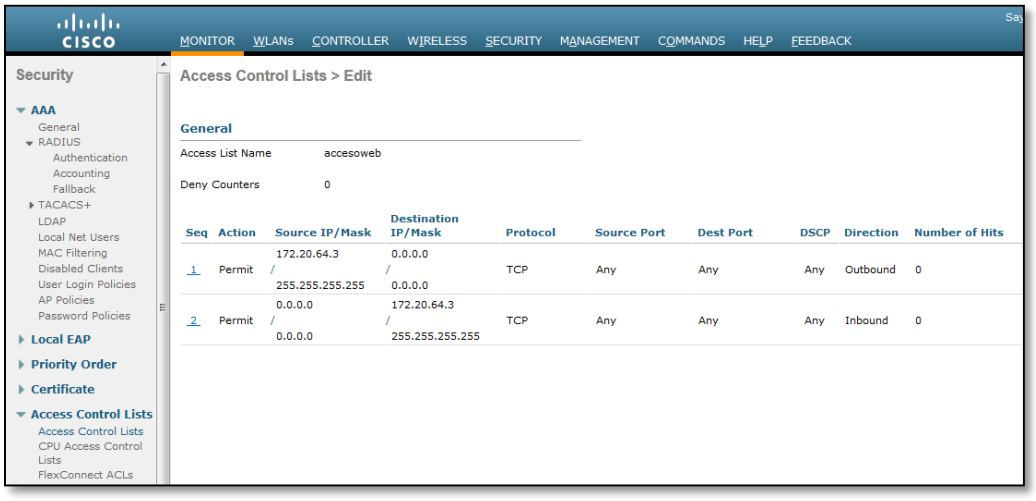


Figura 100. Lista de Acceso en WLC 5508

Fuente: Propia

4. Posteriormente se habilita la Autenticación en capa 3 sobre cada una de las WLANs creadas en este caso a la red inalámbrica "WUPEC". Esta opción se encuentra en la pestaña Security de la WLANs seleccionada con el siguiente procedimiento:

   - Escoger la opción Layer 3 y seleccionar Web Policy enseguida el método a utilizar es Authentication.
   - En Preauthentication ACL es necesario seleccionar la ACL anteriormente creada "accesoweb".
   - Habilitar Over-ride Global Config e indicar en Wen Auth type que la autenticación se redirigirá a un servidor externo "External (Re-direct to external server)" y finalmente la URL para alcanzar al servidor web en este caso http://autenticacion.wupec.edu.ec/login.html. La Figura 101 ilustra este procedimiento.

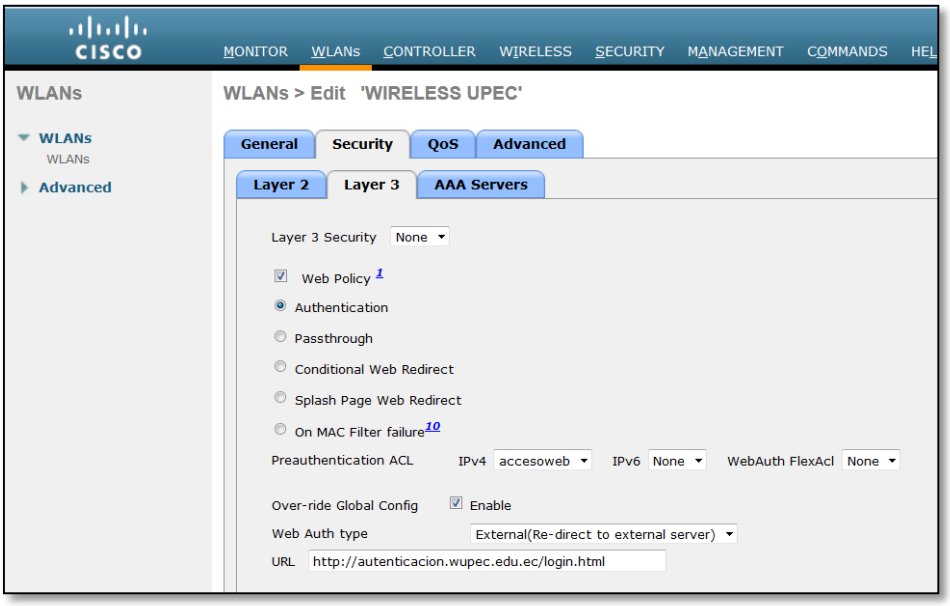


Figura 101. Activación de Autenticación de capa 3 en WLC Cisco 5508

Fuente: Propia

5. En la pestaña AAA Servers se activa la opción “Radius Server Overwrite interface” y check sobre Authenticaction Servers y Accounting Servers en donde se puede apreciar tanto la IP y puerto del servidor que ya se asignaron anteriormente (Figura 102).

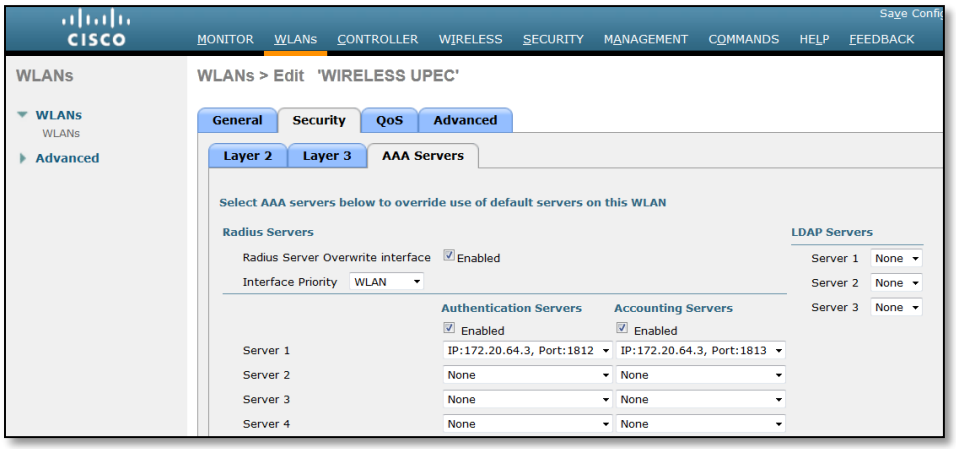


Figura 102. AAA Servers WLC Cisco 5508

Fuente: Propia

6. En la parte inferior de AAA Servers es necesario colocar el mecanismo de autenticación principal para este caso RADIUS (véase la Figura 103).

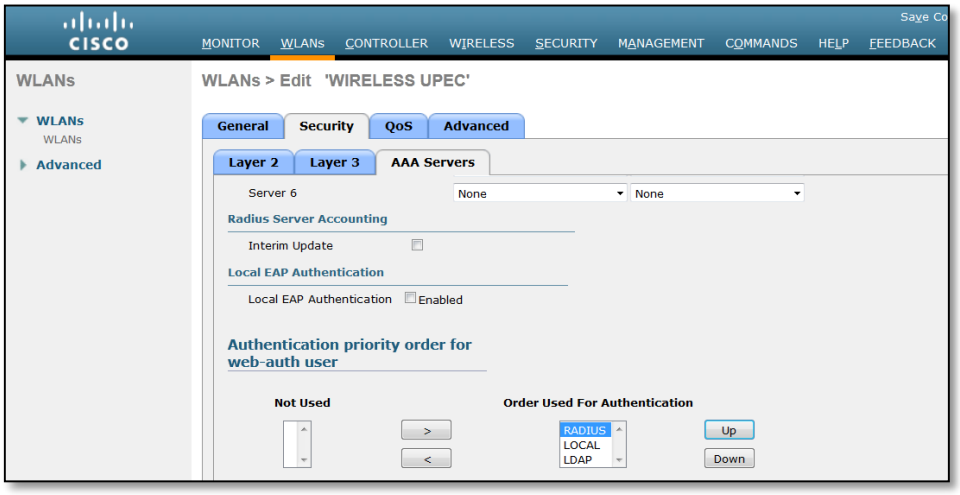


Figura 103. RADIUS principal mecanismo de Autenticación

Fuente: Propia

7. En la opción Security – Authentication se ingresa la Clave de Secreto Compartido que debe ser la misma que se creó al configurar el servidor RADIUS.

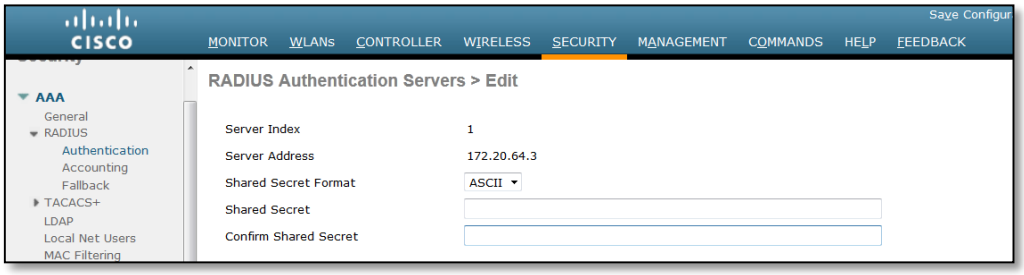


Figura 104. Clave de Secreto Compartido

Fuente: Propia

8. Al trabajar con el mecanismo de Autenticación en capa 3 el controlador inalámbrico cumple con la funcionalidad de un proxy web y por ende todas las conexiones generadas

por los usuarios se re-direccionan inicialmente al WLC, de manera lógica se apunta a la interfaz virtual 1.1.1.1 de manera que en la pestaña Controller se selecciona ésta y se ingresa en el DNS Host Name el nombre del servidor web al cual se va a dirigir la petición del cliente inalámbrico como se presenta en la Figura 105.

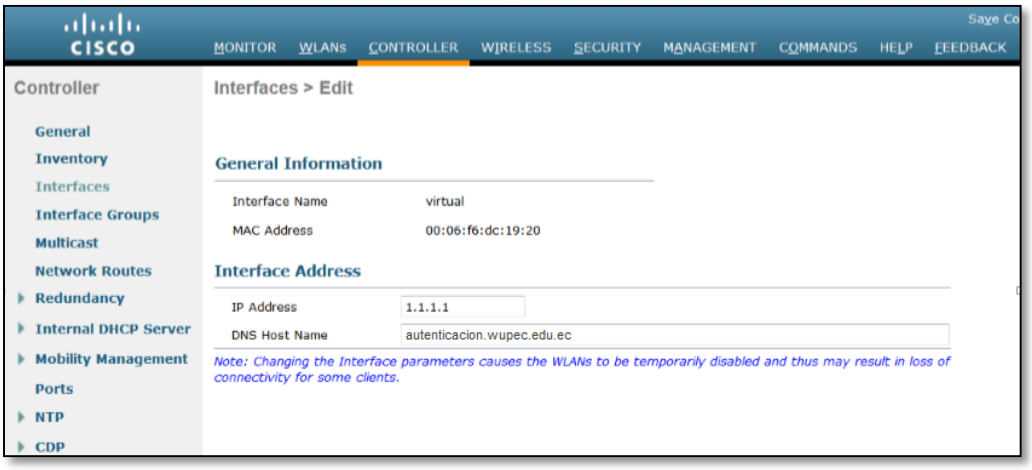


Figura 105. Interfaz Virtual 1.1.1.1

Fuente: Propia

9. Finalmente estas dos opciones ayudan a controlar el número de sesiones y tiempo por sesión de usuario:

   - **USER LOGIN POLICIES:** En la opción SECURITY - AAA - USER LOGIN POLICIES. Pueden ser 2 o 3 sesiones y luego clic en ADD. Controla el número máximo de conexiones simultáneas para un único nombre de usuario, por default 0 y hasta 8 (Figura 106).

   - **ENABLE SESSION TIMEOUT:** En la pestaña WLANs, elegir la WLAN (ej: WUPEC), en la opción ADVANCED, en Enable Session Timeout habilitar el tiempo de sesión en segundos, por default está configurado en 30 minutos. Tiempo máximo en segundos para una sesión antes de requerir autorización.

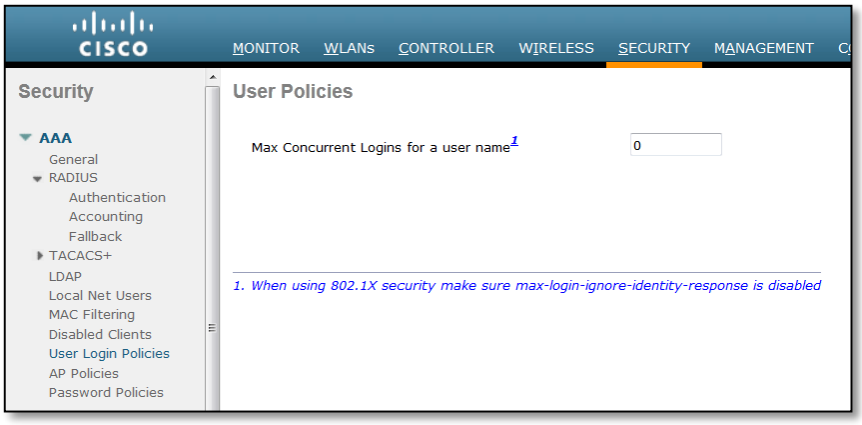


Figura 106. Restricción de sesiones por usuario

Fuente: Propia

4.2.2 Listas de Control de Acceso

A continuación se enlistan los comandos utilizados para restringir el acceso de los usuarios inalámbricos a las otras VLANs de datos:

- Creación de la Lista de Control de Acceso para la WLAN WIFI-UPEC

```
ip access-list standard RESTRICCION-WLAN-WIFI-UPEC
 deny   172.20.2.0 0.0.0.255
 deny   172.20.3.0 0.0.0.255
 deny   172.20.4.0 0.0.0.255
 deny   172.20.8.0 0.0.0.255
 deny   172.20.10.0 0.0.0.255
 deny   172.20.12.0 0.0.0.255
 deny   172.20.16.0 0.0.0.255
 deny   172.20.20.0 0.0.0.255
 deny   172.20.22.0 0.0.0.255
 deny   172.20.24.0 0.0.0.255
 deny   172.20.28.0 0.0.0.255
 deny   172.20.32.0 0.0.0.255
 deny   172.20.36.0 0.0.0.255
 deny   172.20.40.0 0.0.0.255
 deny   172.20.60.0 0.0.0.255
 deny   172.20.64.0 0.0.0.255
 deny   172.20.72.0 0.0.0.255
 permit any
```

- Aplicación de la Lista de Control de Acceso a la interfaz VLAN de la WLAN

```
interface Vlan68
 description WIFI_UPEC
 ip address 172.20.68.1 255.255.252.0
 ip access-group RESTRICCION-WLAN-WIFI-UPEC out
```

4.2.3 SSH para acceso remoto a la administración de los dispositivos

Se ha señalado que es muy importante proteger las conexiones remotas con los dispositivos de la red inalámbrica (WLC y Puntos de Acceso) por lo cual se ha procedido a habilitar SSH como mecanismo seguro tanto en el controlador inalámbrico como en los Puntos de Acceso para lo cual se realizó las siguientes configuraciones:

- **SSH en el WLC 5508:** En la pestaña Management seleccionar la opción Telnet-SSH y habilitar únicamente SSH. La Figura 107 ilustra esta acción.

Figura 107. SSH en el WLC 5508

Fuente: Propia

- **SSH en los Puntos de Acceso:** En la pestaña Wireless seleccionar el Punto de Acceso al cual se va a habilitar, dentro de las opciones disponibles del AP elegir Advanced y activar SSH como lo ilustra la Figura 108.

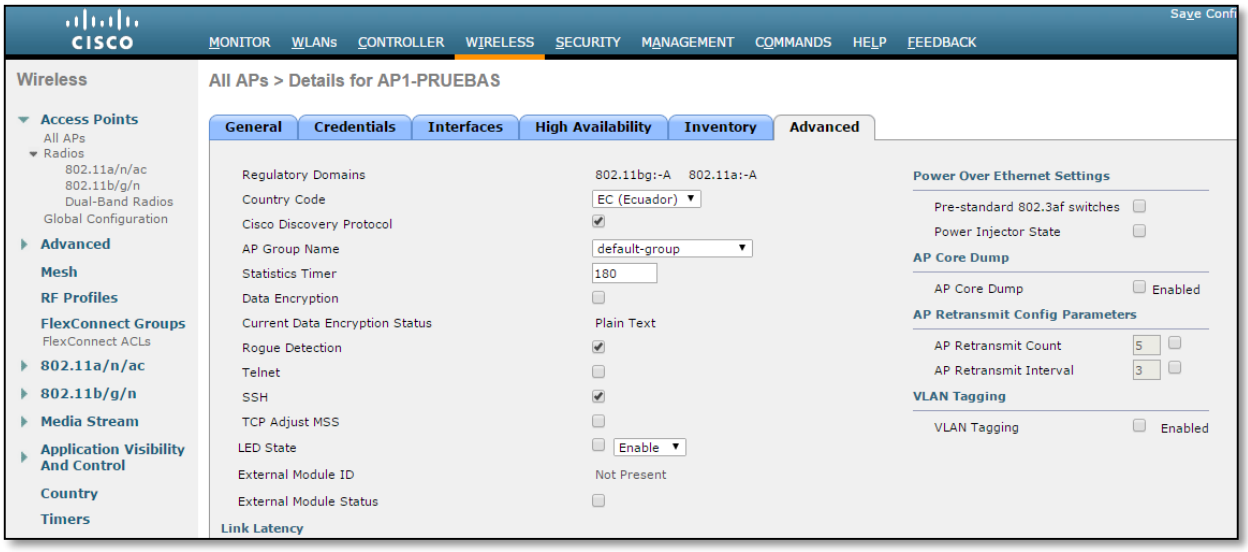


Figura 108. SSH en los Puntos de Acceso

Fuente: Propia

- Adicionalmente el usuario y contraseña establecidos ya sea para el acceso por Telnet o SSH en los Puntos de Acceso por default es “Cisco” por lo cual se procede a modificar en la opción Credentials y se asigna un usuario, una contraseña de acceso por consola y otra para el ingreso al modo privilegiado del AP (Figura 109).

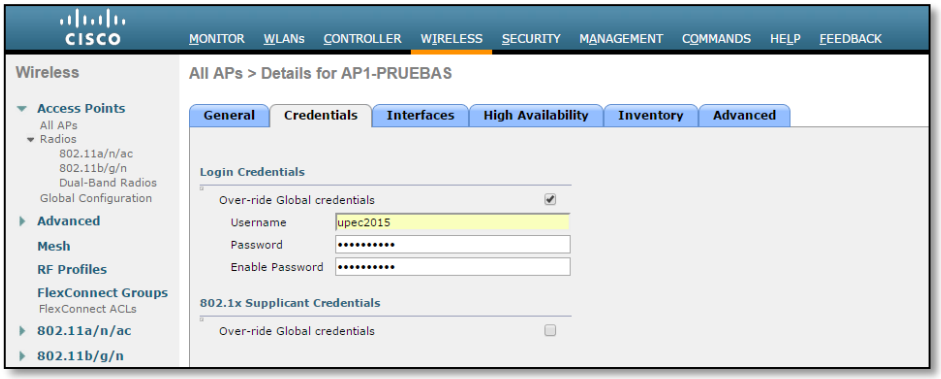


Figura 109. Credenciales de un Punto de Acceso

Fuente: Propia

4.3 PRUEBAS DE FUNCIONAMIENTO

En la presente sección se verifica el funcionamiento tanto de la implementación de QoS como seguridad en la WLAN de la UPEC, estos mecanismos proporcionan una mejora sustancial al rendimiento de la red inalámbrica ya que se ha tomado en cuenta aspectos no solamente de habilitación y configuración sino más bien con respecto a una mejor distribución de Puntos de Acceso, asignación adecuada de canales y potencia, Listas de control de Acceso, entre otras que también aportan en buena parte a percibir o tener un servicio más satisfactorio y seguro.

4.3.1 Calidad de Servicio

Para evaluar el rendimiento de la red inalámbrica con QoS se realizaron algunas pruebas haciendo uso de herramientas como el PacketShaper, Wireshark, descargas de archivos y conectividad que permite apreciar la mejora que se tiene al haber aplicado WMM en la WLAN de la UPEC, en los siguientes ítems se hace una explicación más detallada de cómo se obtuvo esta información.

4.3.1.1 Paquetes Transmitidos

En la Figura 110 se puede evidenciar a través de una gráfica obtenida desde el PacketShaper que ahora con el manejo de QoS en la WLAN WIFI_UPEC no existen pérdidas de paquetes de tal forma que tanto la transmisión de datos así como la conectividad de los usuarios inalámbricos está garantizada teniendo también una mínima tasa de retransmisión lo cual representa que el canal está siendo aprovechado para enviar información útil.

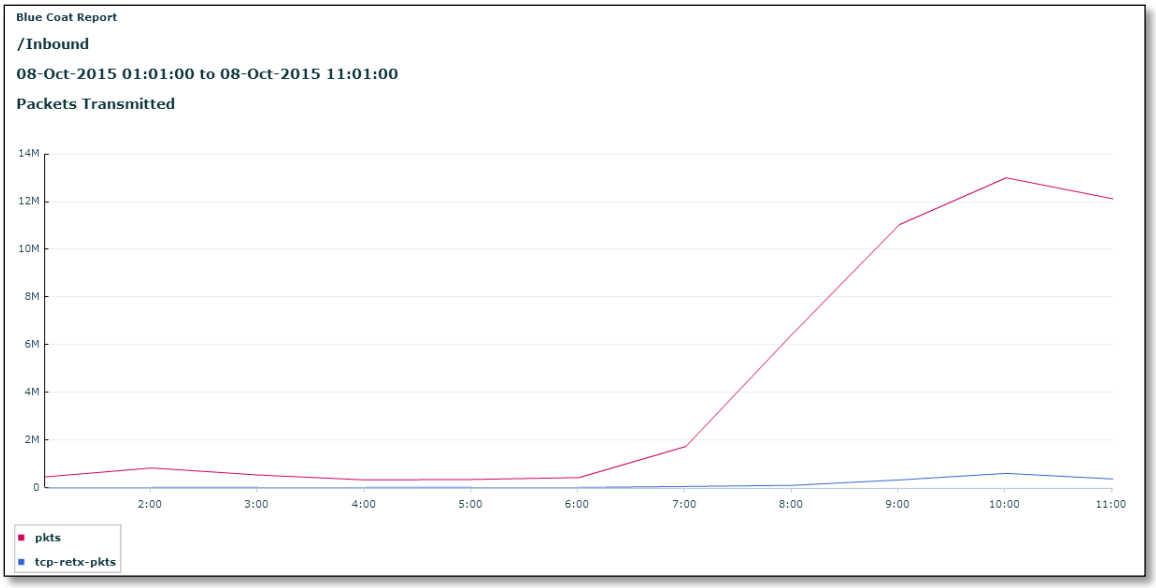
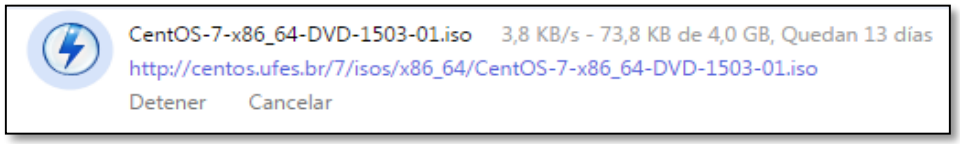


Figura 110. Paquetes Transmitidos en la WIFI_UPEC

Fuente: (PacketShaper, UPEC)

4.3.1.2 Descarga de Archivos

Con la finalidad de demostrar que la red inalámbrica tiene un mejor performance también se procedió a realizar la descarga de archivos antes y después de la configuración de QoS, la primera imagen relativa a la Figura 111 corresponde a la descarga antes de la Calidad de Servicio y se puede apreciar que la velocidad de transferencia es apenas de 3,8 Kbps con un tiempo de duración aproximado de 13 días mientras que la segunda imagen evidencia una tasa de transferencia más alta de 374 Kbps con un tiempo de duración de 3 horas en un entorno ya aplicado QoS.



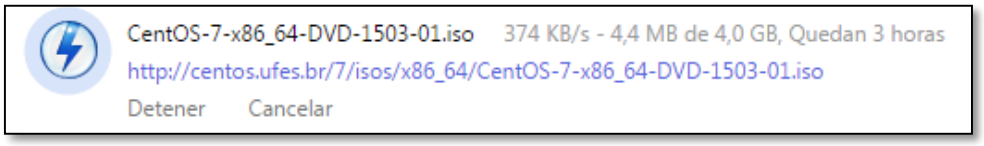


Figura 111. Pruebas de descarga de un archivo en la WIFI_UPEC

Fuente: Propia

4.3.1.3 Ping extendido (Tiempos de Respuesta)

La Figura 112 muestra la diferencia relativa a los tiempos de respuestas existentes antes y después de la configuración de Calidad de Servicio. La primera imagen corresponde a los retardos presentes en la WLAN WIFI_UPEC antes de aplicar QoS y se puede apreciar tiempos relativamente altos mientras que la segunda imagen prueba la reducción de estos tiempos y por ende se puede decir que la WLAN ha mejorado.

```
C:\Users\Sandrita>ping 172.20.8.243 -t

Haciendo ping a 172.20.8.243 con 32 bytes de datos:
Respuesta desde 172.20.8.243: bytes=32 tiempo=123ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=375ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=294ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=92ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=106ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=113ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=97ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=107ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=92ms TTL=127
```

```
C:\Users\Sandrita>ping 172.20.8.243 -t

Haciendo ping a 172.20.8.243 con 32 bytes de datos:
Respuesta desde 172.20.8.243: bytes=32 tiempo=22ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=9ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=2ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=18ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=4ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=7ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=3ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=2ms TTL=127
Respuesta desde 172.20.8.243: bytes=32 tiempo=11ms TTL=127
```

Figura 112. Prueba de conectividad en la WIFI_UPEC

Fuente: Propia

4.3.1.4 Incremento de Ancho de Banda

Uno de los inconvenientes anteriormente a la configuración de QoS consistía en la saturación del enlace en primera instancia por el mal manejo de los recursos seguido de distribución inadecuada del ancho de banda de tal forma que se decidió balancear como medida urgente por parte del personal administrador de la red y cuyo resultado se refleja en un incremento de 6 Mbps para la WIFI_UPEC y 2Mbps para los usuarios de la WUPEC como lo ilustra la Figura 113.

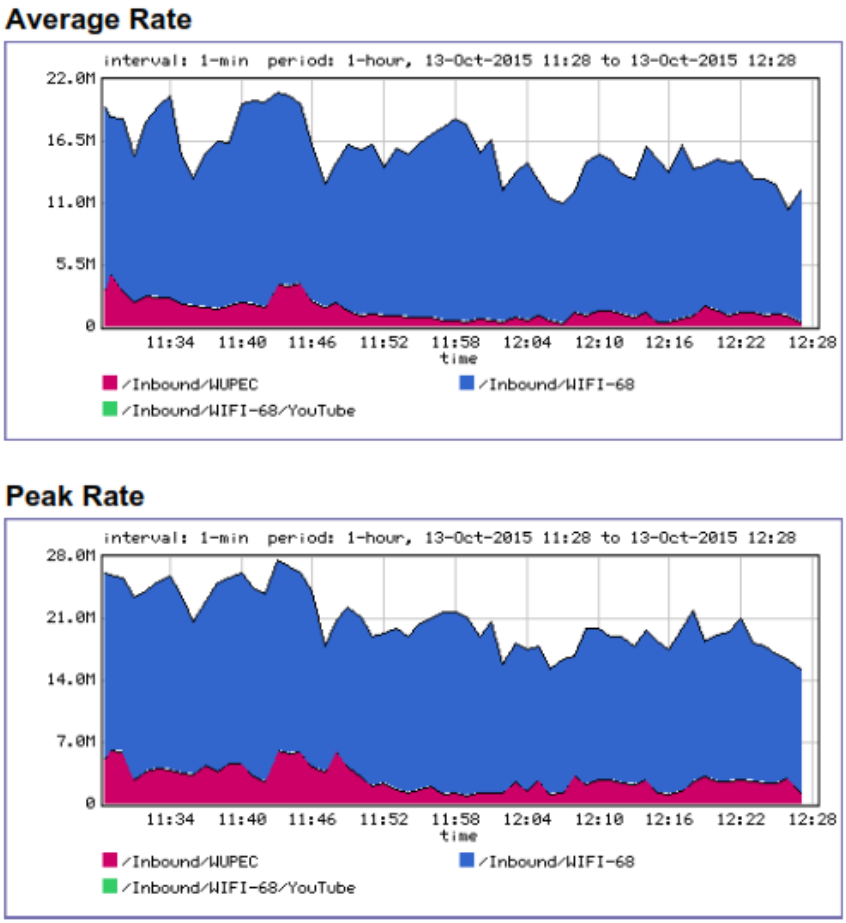


Figura 113. Incremento de Ancho de Banda para las WLANs de la UPEC

Fuente: (PacketShaper, UPEC)

4.3.1.5 Marcado 802.11e y DSCP

La etiqueta QoS de un paquete por la red inalámbrica cambia en los diferentes puntos de su recorrido, es decir que cuando los paquetes van en dirección al Punto de Acceso éste los encapsula en CAPWAP y le agrega el valor DSCP basado en el WMM de la trama 802.11 entrante como lo indica la Figura 114 que fue tomada de un host que envía tráfico hacia la WLAN. Cuando el paquete entra en el switch de acceso, éste confía en el valor DSCP y el valor se reescribe a CoS/802.1p antes de ser enviado por el puerto trunk a la WLC en puerto G3/8 (véase Figura 115), lo cual indica que este paquete ha sido tratado con prioridad en comparación a otros generado por la otra WLAN utilizando el marcado 802.11e y DSCP.

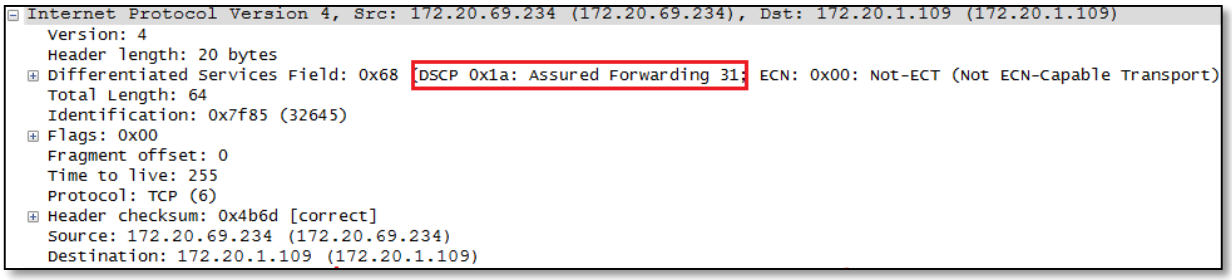


Figura 114. Marcado DSCP en un paquete con QoS

Fuente: Propia

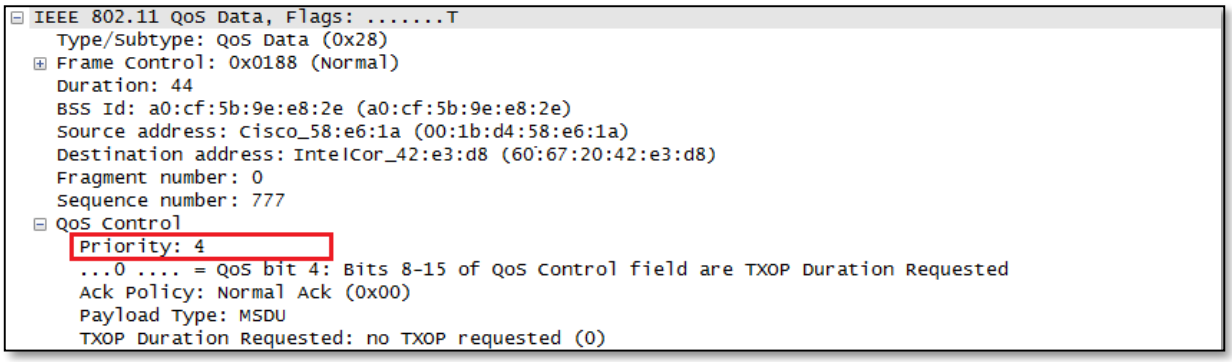


Figura 115. Marcado 802.11e en una trama con QoS

Fuente: Propia

4.3.2 Seguridad en la Red Inalámbrica

Tras la implementación de la autenticación web, Listas de Control de Acceso y configuración de SSH como mecanismos de seguridad para la red inalámbrica de la UPEC a continuación se verifica su funcionamiento.

4.3.2.1 Autenticación Web

El procedimiento para que un usuario legítimo de la red adquiera el servicio http o navegación por Internet es el siguiente:

- Inicialmente el cliente debe estar asociado a la WLAN y con una dirección IP válida.

- El usuario al abrir el navegador web y escribir una dirección URL por ejemplo, http://www.google.com envía una solicitud de DNS al servidor DNS para obtener la dirección IP de destino de www.google.com pero pasando primero por la WLC que recibe la solicitud DNS y la reenvía al server DNS, éste responde con un DNS Replay que contiene la dirección IP que inmediatamente es reenviada al cliente wireless.
- El cliente intenta abrir una conexión TCP con la IP de destino (www.google.com) así que envía un TCP SYN a ésta dirección IP.

- La WLC tiene reglas configuradas para el cliente y actúa como un proxy para www.google.com por ende envía un TCP SYN-ACK al cliente que realizó la solicitud DNS y el cliente envía un TCP ACK para completar la conexión TCP.

- El cliente envía un HTTP GET destinado a www.google.com, lo intercepta la WLC y es reenviado a http://<Virtual−Server−IP>/login.html. El Cliente cierra la conexión TCP con la dirección IP, por ejemplo www.google.com.

- Ahora el cliente va a http://autenticacion.wupec.edu.ec/login.html e intenta abrir una conexión TCP con la dirección IP virtual del WLC. Se envía un paquete TCP SYN de 1.1.1.1 a la WLC. El WLC responde con un TCP SYN-ACK y el cliente envía un TCP ACK al WLC para establecer la comunicación.

- El cliente envía un HTTP GET para /login.html destinado a 1.1.1.1 con el fin de solicitar la página de inicio de sesión. Esta petición es permitida hacia el servidor web externo y el servidor responde con la página de inicio de sesión predeterminado de tal forma que el cliente recibe la página de inicio de sesión en la ventana del navegador en el que el usuario puede ingresar sus credenciales que son validadas por el servidor RADIUS al existir en el Directorio Activo caso contrario el usuario no puede navegar por Internet.

En la Figura 116 se presenta la página de inicio de sesión para el ingreso de las credenciales del usuario legítimo de la red y en la Figura 117 se ilustra un acceso satisfactorio.

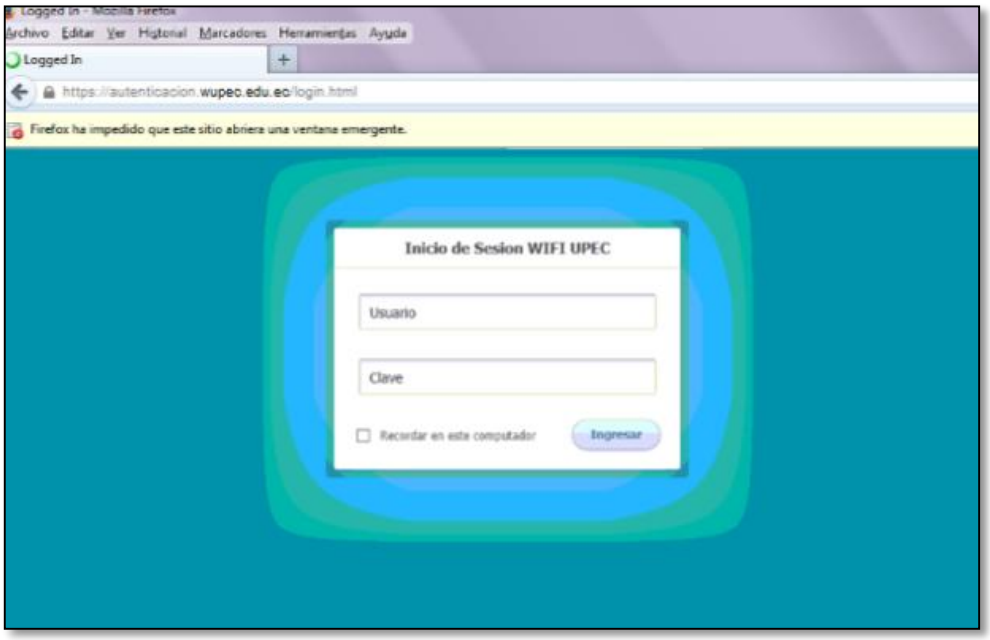


Figura 116. Página de inicio de sesión

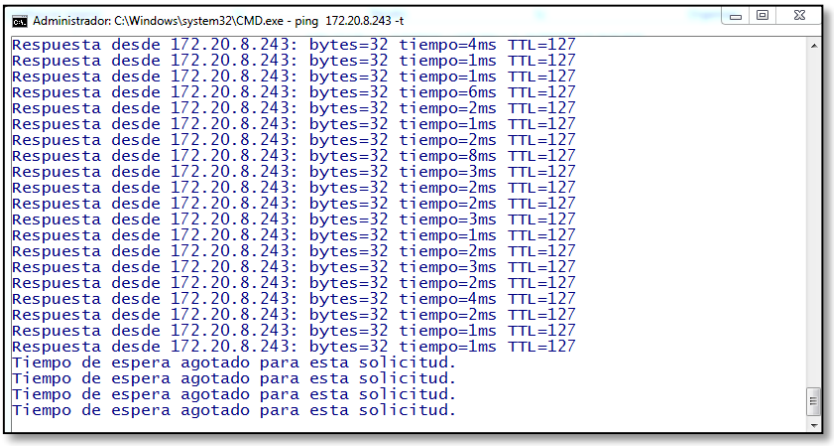
Fuente: Propia

Figura 117. Usuario correctamente validado

Fuente: Propia

4.3.2.2 Listas de Control de Acceso

Con el afán de dar protección a las VLANs de datos de accesos no autorizados por parte de los usuarios inalámbricos se configuró Listas de Control de Acceso en el switch core de la institución para evitar estos hechos. En la Figura 118 se puede verificar que una lapto con la dirección IP 172.20.70.101 perteneciente a la WLAN WIFI-UPEC tiene acceso restringido a la VLAN de CTICs específicamente en el ejemplo a la IP 172.20.8.243 correspondiente a un host justo en el momento en que se aplica la ACL en la interfaz de la VLAN 68 (WIFI-UPEC).



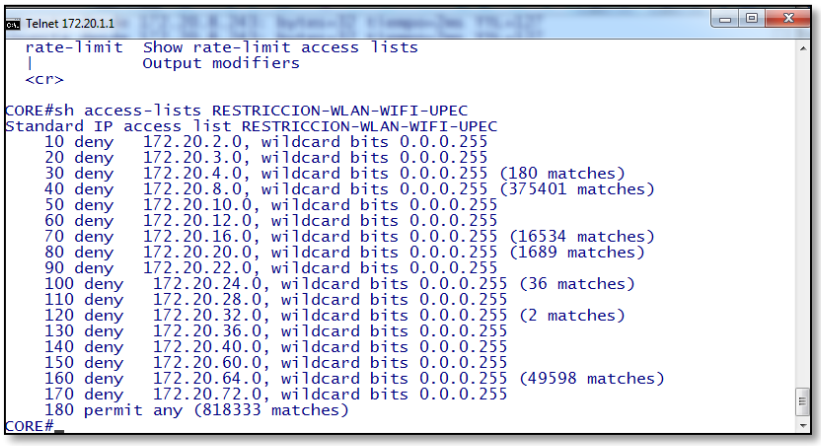


Figura 118. Acceso restringido a la VLAN de equipos inalámbricos

Fuente: Propia

4.3.2.3 Acceso remoto SSH

El acceso SSH tanto para la WLC 5508 y los Puntos de Acceso se puede verificar tanto en la Figura 119 (WLC) y Figura 120 para los APs, dando como resultado un mecanismo seguro para el acceso remoto a estos equipos de la red inalámbrica.

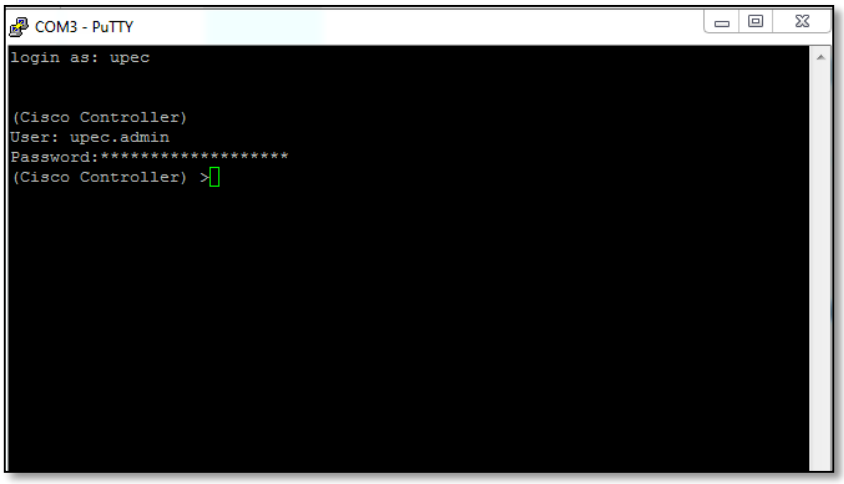


Figura 119. SSH en WLC 5508

Fuente: Propia

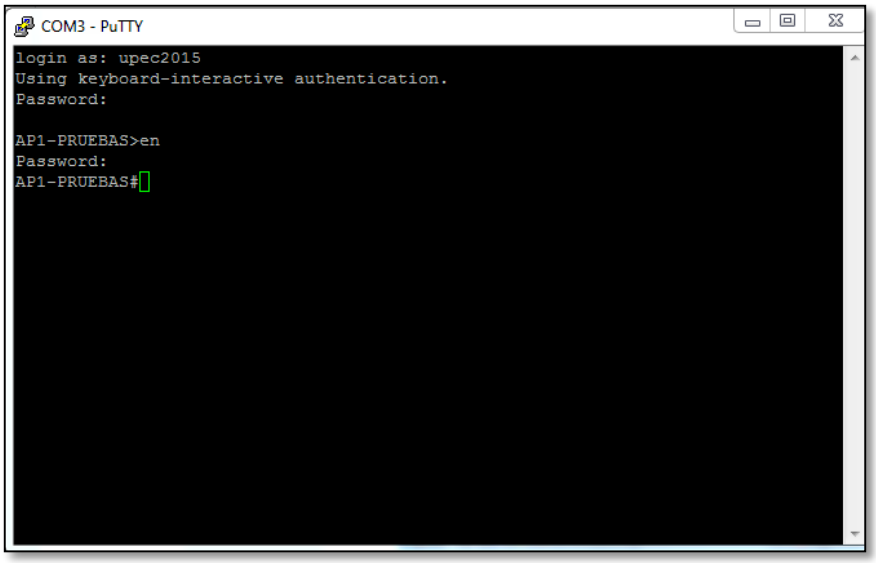


Figura 120. SSH en Puntos de Acceso

Fuente: Propia

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se exponen las conclusiones y recomendaciones obtenidas tras la realización del estudio de Calidad de Servicio y Seguridad en redes WLAN con aplicación a la red inalámbrica de la Universidad Politécnica Estatal del Carchi que además servirá de base y fundamento para la implementación en otros ambientes institucionales.

5.1 CONCLUSIONES

- En sus inicios las WLAN no estaban proyectadas ni tampoco especificadas para el soporte de servicios convergentes, de hecho su diseño principalmente fue motivado a ser o trabajar como una característica adicional de las redes cableadas, es decir una extensión de las mismas sobre las cuales se transmitiría solamente datos. A raíz de la expansión de las WLANs y aparición de nuevas aplicaciones como el caso de la VoIP, video streaming, multimedia entre otras las redes inalámbricas de área local se enfrentan a un gran reto debido a las altas prestaciones que éstas aplicaciones requieren y por ende los organismos de estandarización como la IEEE proponen una solución a este inconveniente, siendo en el año 2005 la publicación de la variante IEEE 802.11e que define la posibilidad de establecer diferentes tipos de tráfico en el medio inalámbrico con hasta 8 clases de servicios compatibles con 802.11p.

- La propuesta de la enmienda IEEE 802.11e contempla la definición de nuevos mecanismos para que una WLAN proporcione QoS a las aplicaciones críticas contrarrestando las limitaciones como el mal manejo del ancho de banda, pérdida de paquetes, delay y jitter. Estos mecanismos se relacionan principalmente con la implementación de una tercera función de Coordinación HCF, diferenciación de tráfico y la oportunidad de Transmisión TXOP manteniendo compatibilidad hacia atrás con DCF y PCF por medio de dos nuevos métodos de control de acceso EDCA y HCCA respectivamente.

- El método de acceso al medio inalámbrico EDCA es de carácter obligatorio y por ende el más común, la versión certificada por la Wi-Fi Alliance es WMM e incluye los elementos tradicionales de DCF como el protocolo CSMA/CA, backoff, los tiempos IFS y los complementa con otros para posibilitar QoS como son: TXOP-EDCA y los tiempos AIFS asociados para cada una de las categoría de acceso AC acorde al nivel de priorización.

- Antes de implementar QoS en redes WLAN también es necesario tener presente otros criterios que contribuyen de manera significativa a mejorar el performance en una red y son los siguientes: garantizar la Calidad de Servicio en la red Ethernet a través de 802.11p y DSCP, un ancho de banda de acceso a Internet adecuadamente dimensionado para la cantidad de usuarios, enlaces redundantes, manejo de seguridad perimetral y políticas de acceso interno, segmentación lógica de la red, equipamiento robusto y escalable, entre otros. Por lo tanto el éxito de Calidad de Servicio en una WLAN depende de la aplicación de estas técnicas sumada la administración correcta de los parámetros: jitter, delay y pérdida de paquetes por medio de la priorización y diferenciación del tráfico en el medio inalámbrico.

- Otro de los grandes retos con los que se enfrentan las WLANs es la seguridad, pues son entes vulnerables ya que a diferencia de las redes cableadas el acceso al medio de transmisión es compartido y está a entera disposición para todos aquellos que se encuentran dentro del área de cobertura si no se ha dispuesto de herramientas que controlen su acceso. Un usuario ilegítimo y con malas intenciones puede ser sumamente peligroso ya que además de provocar denegación de servicio puede sustraer información netamente sensible e importante tanto para el usuario afectado como para la organización. Es por eso que para superar este inconveniente se han incluido varios mecanismos a lo largo de estos años que además requieren de la estricta colaboración y constante monitoreo de parte de los administradores de red.

- Los mecanismos más recomendados para cerrar esta brecha de vulnerabilidad es WPA2 versión certificada de 802.11i totalmente flexible ya que permite su implementación tanto en ambientes SOHO como en sectores empresariales u organizacionales. Para el caso de redes SOHO es preciso hacer uso de la autenticación basada en clave pre compartida PSK y cifrado de comunicaciones AES con contraseñas robustas y cambio periódico de la misma. En los entornos organizacionales WPA2/Enterprise se ajusta a los requerimientos de seguridad mediante la utilización del cifrado AES en conjunto con la autenticación basada en RADIUS a través del protocolo 802.1x/EAP, cuya distribución y utilización de certificados digitales básicamente depende de los criterios de los administradores TI de cada entorno.

- No basta solamente con la implementación de WPA2/Enterprise como mecanismo de seguridad integral en una red inalámbrica a la par es imprescindible usar otras técnicas para garantizar la integridad de la información como por ejemplo: hacer uso de herramientas de Firewall, IDS, IPS, Listas de Control de Acceso, segmentación a través de VLANs, monitorización de AP maliciosos y socialización continua a los usuarios de las políticas e importancia del custodio de las claves de acceso.

5.2 RECOMENDACIONES

- Las redes inalámbricas de área local en muchas ocasiones se han convertido en el talón de Aquiles de los administradores de red, pero esto sucede básicamente por la falta de administración y monitoreo desde su implementación ya que se debería ir solventando los inconvenientes conforme van apareciendo, de tal forma que se sugiere la utilización de una herramienta ya sea basada en software libre o propietaria para controlar los recursos y componentes de la WLAN de la UPEC ya que actualmente resulta un poco incómoda la administración por la cantidad de Puntos de Acceso existentes que incrementarán más aún con el funcionamiento de los dos nuevos edificios.

- Es necesario establecer redundancia a través de Enlaces Agregados (Link Aggregation) entre el switch de core y el controlador inalámbrico de la UPEC para en primera instancia incrementar el canal de comunicaciones y mantener un mecanismo de respaldo en caso de falla de cualquiera de las interfaces, por lo tanto garantizar el servicio a los usuarios inalámbricos.

- Antes de la instalación y configuración de nuevos Puntos de Acceso y conforme se extiende la WLAN es conveniente como recomendación previa dimensionar los nuevos equipos a través de la realización de pruebas teóricas o en sitio del área de cobertura e interferencia de tal forma evitar problemas a futuro ya que si no se lo hizo correctamente prácticamente afectarán a la calidad de servicio de los usuarios de estas zonas y de la red en general.

- Monitorear y controlar constantemente el uso de los recursos, aplicaciones y políticas de Calidad de Servicio, ya que a diario aparecen nuevos mecanismos o herramientas que burlan a los firewalls de seguridad como el ultrasurf de manera que el usuario que lo instala utiliza aplicaciones ilegítimamente que consumen gran ancho de banda y afectar inmediatamente a la calidad de servicio de la WLAN.

- La implementación de Seguridad a la WLAN de la Universidad Politécnica Estatal del Carchi se realizó en base a la utilización de los componentes existentes actualmente sin embargo se aconseja que para manejar un nivel más alto de seguridad se incorpore los módulos de IPS e IDS al firewall actual ASA 5520 en conjunto con un servidor de registros o logs para almacenar las alertas que estos medios arrojan cuya utilidad es verdaderamente importante en caso de requerir detectar el origen de los ataques y también para llevar a cabo los controles de auditoría.

- De igual forma para la realización de este estudio se formuló políticas concernientes al uso y manejo de la WLAN pero se recomienda formular y trabajar en las políticas de seguridad integral de la universidad que incorpore a todos los entes institucionales: autoridades, personal administrativo y estudiantes y socializarlas continuamente. Es necesario que el usuario tenga conocimiento de la importancia de guardar celosamente sus claves y no sea presa fácil de los individuos mal intencionados que utilizan la Ingeniería Social para el robo de las mismas.

- Es conveniente además recomendar a los administradores de red realizar backups y mantenimientos periódicos de las configuraciones y funcionamiento no solamente de los equipos de la red inalámbrica sino de la red y equipos en general.

- En base al crecimiento de los usuarios y aplicaciones en la red de la UPEC es evidente también la necesidad de incrementar el ancho de banda de acceso al Internet además de una correcta distribución en base a los requerimientos de cada una de las VLANs ya que se ha evidenciado que existen VLANs cuyo número de usuarios es pequeño pero con un alto ancho de banda en comparación con la asignación a las redes inalámbricas.

BIBLIOGRAFÍA

Andreu, F., Pellejero, I. & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN*. Barcelona: Marcombo S.A.

Anónimo. (2011). *Diseño de una red Wi-Fi para la E.S.I.* Recuperado en abril de 2015 de: http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%EDtulo+5.pdf

Anónimo. (2013). *WLAN Red Inalámbrica de Área Local.* Recuperado en abril de 2015 de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo1.pdf

Anónimo. (2013). *Estándar IEEE 802.11*. Recuperado en abril de 2015 de: http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F07+-+Capitulo+2.pdf

Anónimo. (2015). *Desarrollo y Evolución de IPv6.* Recuperado en agosto de 2015 de: http://ipv4to6.blogspot.com/p/protocolo-ip.html

Ariganello, E. & Barrietos Sevilla, E. (2010). *Redes Cisco CCNP a Fondo*. Madrid: Alfaomega Ra-Ma.

Bernal, I. (2008). *Generalidades de WLAN.* Recuperado de: http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/Oct05Marzo06/Inalambricas/CLASES/802-11ParteIb.pdf

Blue Coat Systems Inc. (2013). *Visibilidad y Optimización para el Tráfico de Red.* Recuperado en agosto de 2015 de: https://www.bluecoat.com

Calderón, P. (2014). *Estadísticas de Redes Inalámbricas IEEE 802.11.* Recuperado en junio de 2015 de: http://www.websec.mx/Estadisticas_2013_de_Redes_802.11_en_MX.pdf

Cisco Press. (2006). *Fundamentals of Wireless LANs.* (1era Edición). Prentice Hall.

Cisco Press. (2009). *CCNP ONT Quality of Service.* California: Cisco Systems, Inc.

Cisco Validated Design Program. (2010). *Voice over Wireless LAN Design Guide.* California: Cisco Systems, Inc.

Cisco. (2013). *Cisco Aironet Series 1600/2600/3600 Access Point Deployment Guide.* Recuperado en mayo de 2015 de: http://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/Cisco_Aironet.html

Cisco. (2015). *Cisco Meraki.* Cisco Systems, Inc. Recuperado de: https://dashboard.meraki.com/

Cisco. (2015). *Protección de las Redes Inalámbricas*. Recuperado en octubre de 2014 de: http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

Darapuneni, S. (2009). *Analysis of IEEE 802.11e for QoS support in Wireless LANs.* Recuperado de: http://morse.colorado.edu/~tlen5520/Papers/Pres/Sri.pdf

Delgado, H. (2009). *Redes Inalámbricas*. Lima: Editora Macro E.I.R.L.

Erazo, C., Arana, J., Meza, I. & Pérez, S. (2009). *Implantación de Calidad de Servicio (QoS) en redes Inalámbricas Wi-Fi*. Escuela Superior de Ingeniería Mecánica y Eléctrica. México.

eslared.org. (2012). *Introducción a las Redes Wi-Fi.* Recuperado en marzo 2015 de: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf

Gerometta, O. (2009). *Calidad de servicio en redes WLAN.* Recuperado en octubre de 2014 de: http://librosnetworking.blogspot.com/2009/04/calidad-de-servicio-en-redes-wlan.html

Giménez, R. (2008). *Análisis de la Seguridad en Redes 802.11*. Proyecto de Fin de Carrera. Universidad de Valencia.

Gómez, P. (2007). *Arquitectura Unificada para el Control de Acceso en Redes Inalámbricas Seguras.* Tesis previa a la obtención del Título de Magister en Telinformática. Universidad de Mendoza. Argentina.

Graham, S. (2008). *802.11 QoS Tutorial*. Recuperado en agosto de 2015 de: http://www.ieee802.org/1/files/public/docs2008/avb-gs-802-11-qos-tutorial-1108.pdf

Hernández, A. (2007). *WPA vs WPA2*. Recuperado en junio de 2015 de: http://www.tlm.unavarra.es/research/seminars/slides/20071221-ana-WPA-presentacion.pdf

IEEE Std 802.11e™-2005. (2005). *Medium Access Control Enhancements for Quality of Service.* New York, USA: IEEE Standards Association.

IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007. (2012). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. New York, USA: IEEE Standards Association.

Jerome, H. (2014). *CCNA Wireless, master the 802.11 protocols*. Cisco Live. Cancun - México.

Lawrence, L. & Jun, M. (1999). *Wireless LAN IEEE 802.11*. Recuperado en abril de 2015 de: http://www.soi.wide.ad.jp/class/99007/slides/09/index_23.html

Meden, J. (2013). *IEEE 802.11ac.* Recuperado en marzo de 2015 de: http://jeuazarru.com/wp-content/uploads/2014/10/80211ac.pdf

Mieres, J. (2009). *Ataques Informáticos*. Recuperado en junio de 2015 de: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Moresco, A. (2012). *Evolución del Estándar IEEE 802.11 (Wi-Fi).* Recuperado en marzo de 2015 de: http://ticylamejorasocial.blogspot.com/2012/04/estandar-redes-locales-inalambricas.html

Nayanajith, R. (2014). *CWAP- MAC Header: QoS Control*. Recuperado en agosto de 2015 de: http://mrncciew.com/2014/10/03/cwap-mac-header-qos-control

Panda Software International. (2005). *Seguridad en Redes Inalámbricas.* Recuperado en octubre de 2014 de: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

Perahia, E. & Stacey, R. (2013). *Next Generation Wireless LANs*. (2da. Edición). New York: Cambridge University Press.

Stallings, W. (2002). *Comunicaciones y Redes de Computadoras*. (6ta. Edición). Recuperado en febrero 2015 de: https://richardfong.files.wordpress.com/2011/02/stallings-william-comunicaciones-y-redes-de-computadores.pdf.

Soyinka, W. (2010). *Wireless Network Administration a Beginners Guide*. USA: McGraw-Hill

Tanenbaum, A. (2005). *Redes de Computadoras*. México: Editorial Prentice Hall.

Tomasi, W. (2004). *Sistemas de Comunicaciones Electrónicas*. México: Editorial Pearson Educación.

UPEC. (2015). *Documentación archivos del Departamento de Tecnología.* Recopilados desde marzo a agosto 2015.

Villalón, J., Cuenca, P. & Orozco, L. (2006). *Estudio de QoS en WLANs IEEE 802.11e.* Recuperado de: https://investigacion.uclm.es/documentos/it_1135769841-Articulo_jose_villalon.pdf

Villegas, D. (2008). *Estándar IEEE 802.11 Wireless LAN*. Recuperado en abril de 2015 de: http://es.scribd.com/doc/13842125/ESTANDAR-IEEE-802-11#scribd

Watson, R. (2013). *Understanding the IEEE 802.11ac Wi-Fi Standard*. Recuperado en marzo 2015 de: http://www.merunetworks.com/collateral/white-papers/2012-wp-ieee-802-11ac-understanding-enterprise-wlan-challenges.pdf

wikipedia.org. (2013). *IEEE 802.11*. Recuperado en marzo de 2015 de: http://es.wikipedia.org/wiki/IEEE_802.11

GLOSARIO DE TÉRMINOS

ACL Lista de Control de Acceso, es un método utilizado dentro del ámbito de la red, específicamente en los routers o dispositivos capa 3 para establecer condiciones de acceso a destinos o equipos.

ASOCIACIÓN En redes WLAN, es el proceso que se ejecuta después de la autenticación, a través del cual un cliente wireless puede utilizar los servicios de un Access Point.

BACKHAUL Segmento de una red jerárquica comprendido entre el backbone y las redes que se conectan a través de él. Se suelen definir como canales de retorno.

BACKUP Es una copia de seguridad que contiene información verídica de cómo está trabajando un equipo en la actualidad y que se ejecuta con el fin de disponer de un respaldo en caso de pérdida.

CELDA Una celda es un espacio o superficie que cubre un transmisor en cierto lugar. Su extensión está limitada a la cantidad de potencia que suministre el transmisor mientras que sus restricciones están dadas por la topografía de la zona.

CIFRADO Es una técnica que logra transformar la información con el objetivo de ocultarla y protegerla de usuarios ajenos, con el fin de que solo el usuario legítimo pueda acceder a ella.

CSMA/CA Es un protocolo de Control de Acceso en redes WLAN que ayuda a prevenir las colisiones donde primero se escucha el canal para ver si está libre, luego se realiza el envío de los datos y se espera una respuesta por

parte del receptor para saber que los paquetes de información llegaron íntegros a su destino.

DFS (Dynamic Frequency Selection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

DSSS Tecnología de Espectro Ensanchado por Secuencia Directa. Esta técnica consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información. Este bit patrón es llamado un chip (o chipping code). La longitud del chip, tiene una probabilidad mayor de que los datos puedan ser recuperados. Si uno o más bits en el chip son "dañados" durante la transmisión, se pueden recuperar los datos originales a través de técnicas estadísticas aplicadas sobre las señales de radio, sin necesidad de retransmisiones.

FDMA Acceso Múltiple por División de Frecuencia, técnica de multiplexación que divide el espectro en canales con diferentes rangos de frecuencia con el fin de que al asignarles estos a los usuarios no existan interferencias.

FHSS Tecnología de Espectro Ensanchado por Salto en Frecuencia. Esta técnica utiliza una señal portadora que cambia de frecuencia en un patrón que es conocido por el transmisor y el receptor. Apropiadamente sincronizada, la red efectúa este cambio para mantener un único canal lógico de operación.

HANDSHAKE Su traducción es “apretón de manos”, constituye el saludo que hace un dispositivo de red a otro que intenta conectarse, por ejemplo, cuando un smartphone desea conectarse a una red, le envía una información al AP o

router diciendo: Soy un dispositivo que desea acceder a tu red y esta es la clave. La información en un handshake es cifrada.

HOTSPOT Lugar que ofrece servicio de Internet ya sea pagado o gratuito, comúnmente se localizan en zonas de abundante tráfico como aeropuertos, cafeterías, parques u otros puntos de concentración.

IV El Vector de Inicialización es un bloque de bits requerido para permitir un cifrado en flujo o por bloques y su tamaño depende del algoritmo utilizado, se genera automáticamente y es diferente para cada trama.

MESH Es una red mallada muy útil puesto que si un nodo se daña, la información no se pierde porque puede seguirse enviando por los demás nodos cercanos con lo que se ha podido incrementar la cobertura en ambientes grandes como campus, sus nodos cumplen con dos funciones que son establecer el backbone inalámbrico y dar conectividad a los usuarios.

MIMO (Multiple Input Multiple Output) técnica de transmisión en redes inalámbricas que posibilita la utilización de varias antenas a la vez en un mismo Punto de Acceso tanto para la transmisión como para la recepción simultánea, con esta tecnología se dividen los datos a transmitir en segmentos de forma que pueden ser enviados utilizando las múltiples antenas para luego en el destino reestablecerse a su forma inicial.

MSDU MAC Service Data Unit (SDU a nivel MAC), es el conjunto de datos que proviene de la capa superior aún no encapsulada. La capa N recibe la SDU desde la capa de arriba, N+1. Posiblemente los datos recibidos no entren en una PDU mínima de la capa N y para ello deberá realizar una fragmentación. Luego procede a agregarle el encabezado y posiblemente un terminador a cada fragmento. Cada uno de los segmentos que se

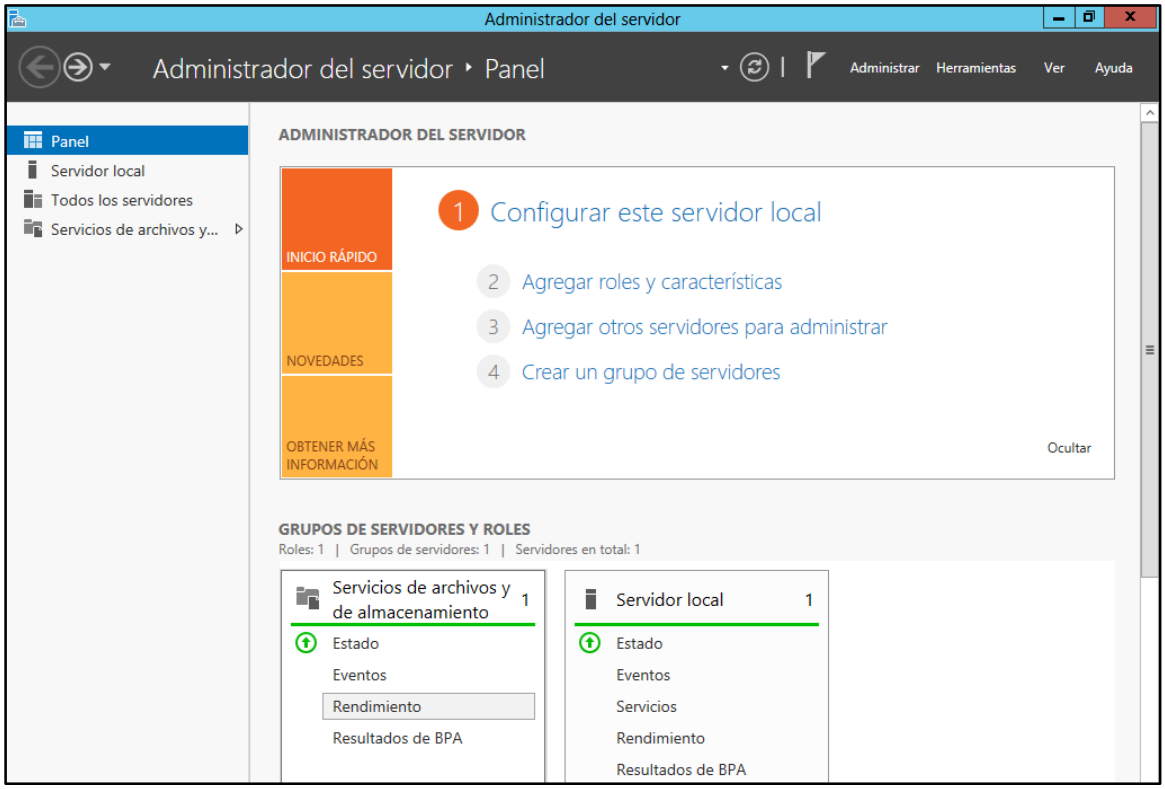
	obtienen es una PDU de la capa N, que prontamente será una SDU de la capa N-1.
MPDU	MAC Protocol Data Unit (PDU a nivel MAC), especifica el conjunto de datos a enviar al protocolo par ubicado en el receptor.
PSK	Pre Shared Key, es una clave secreta que se comparte previamente a la utilización de un canal entre dos dispositivos, cuyos parámetros se fijan por el tipo de sistema. Se utiliza en cifrado WiFi.
RC4	Es un algoritmo de cifrado de flujo diseñado por Ron Rivest para RSA Data Security. Se basa en el uso de una permutación aleatoria y tiene un periodo estimado de más de 10100. Además, es un algoritmo de ejecución rápida en software.
ROAMING	Es un término utilizado en las comunicaciones inalámbricas, aplicado cuando un dispositivo al moverse de una zona de cobertura a otra, no pierde conectividad.
SITE SURVEY	Es un estudio a profundidad en el sitio donde se va a realizar un determinado proyecto, en donde se centra en ver las necesidades de los clientes, verificar si el servicio hacia el cliente va a beneficiarlo, teniendo en cuenta la infraestructura del lugar para saber por dónde puede ir los elementos que se conectan en un sistema de red.
THROUGHPUT	Es el rendimiento de la red es decir la tasa de bits que se entregaron exitosamente en una transmisión.
TLS	Transport Layer Security es un protocolo capaz de garantizar la privacidad e integridad de los paquetes entre aplicaciones servidor-cliente que se comunican en la red.

TPC	Transmitter Power Control, es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.
VoIP	Voz sobre protocolo de Internet, describe un conjunto de tecnologías, las cuáles se implementa para utilizar como enrutamiento de comunicaciones para transmitir voz sobre IP.
WLC	Wireless LAN Controller, dispositivo utilizado para gestionar políticas de seguridad y servicios que se proveen a través de puntos de acceso inalámbricos.

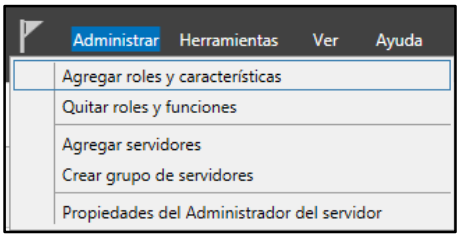
ANEXOS

INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR WEB

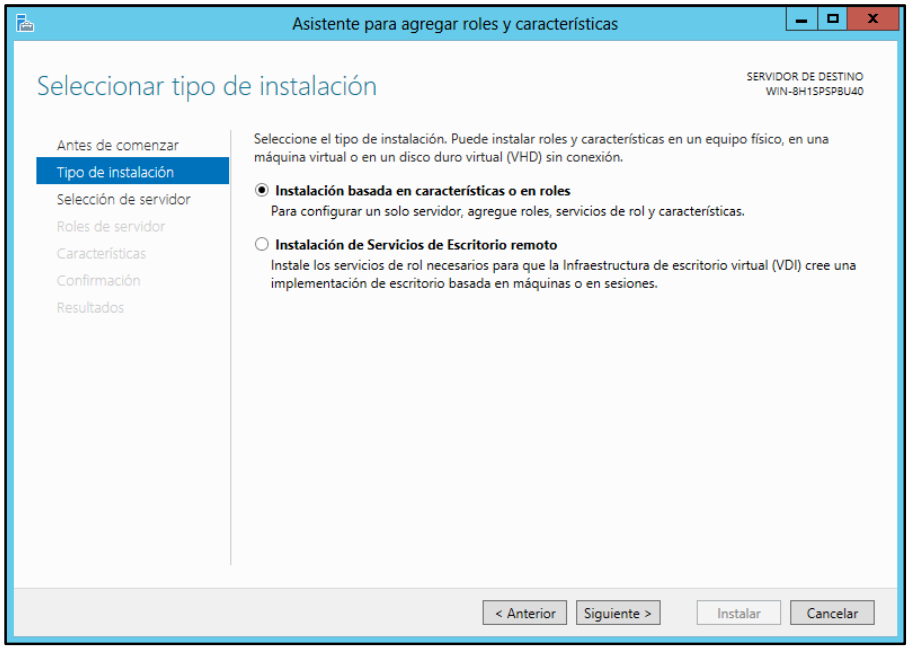
- Clic en el icono del Administrador del Servidor en donde aparece la siguiente pantalla:



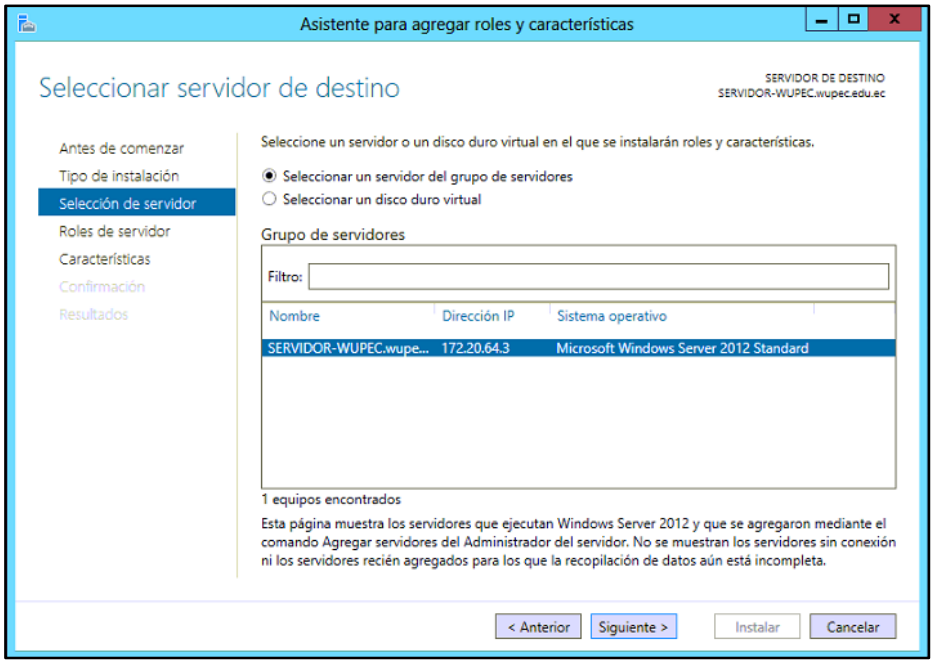
- En la pantalla principal del Administrador del Servidor ir a la opción de Administrar / Agregar Roles y Características



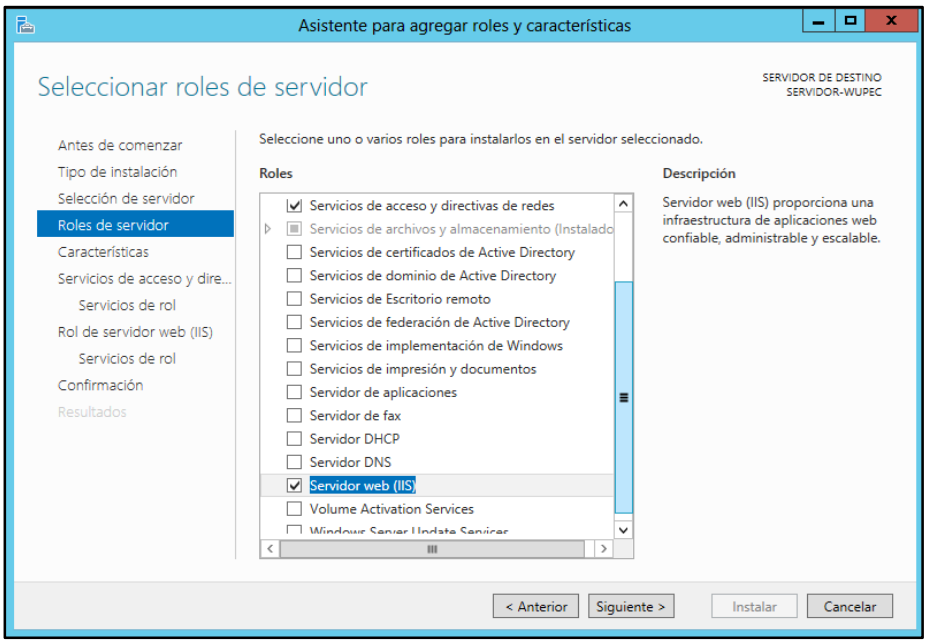
- Aparece un asistente para agregar los servicios que se requiera en el servidor, en este caso se va a instalar el servidor web y clic en la opción de Instalación basada en características o en roles.



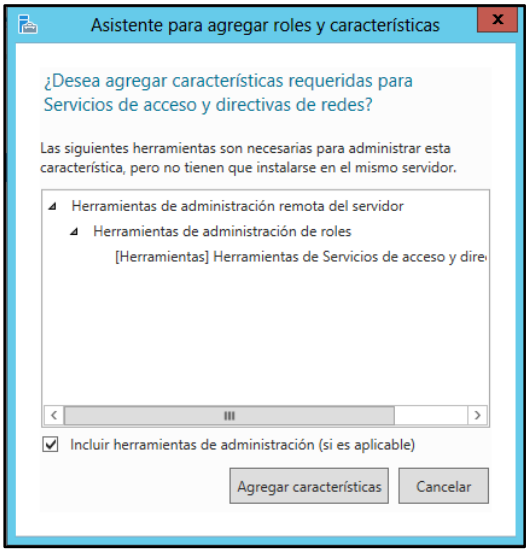
- Seleccionar un servidor del Grupo de servidores, en este caso SERVIDOR-WUPEC



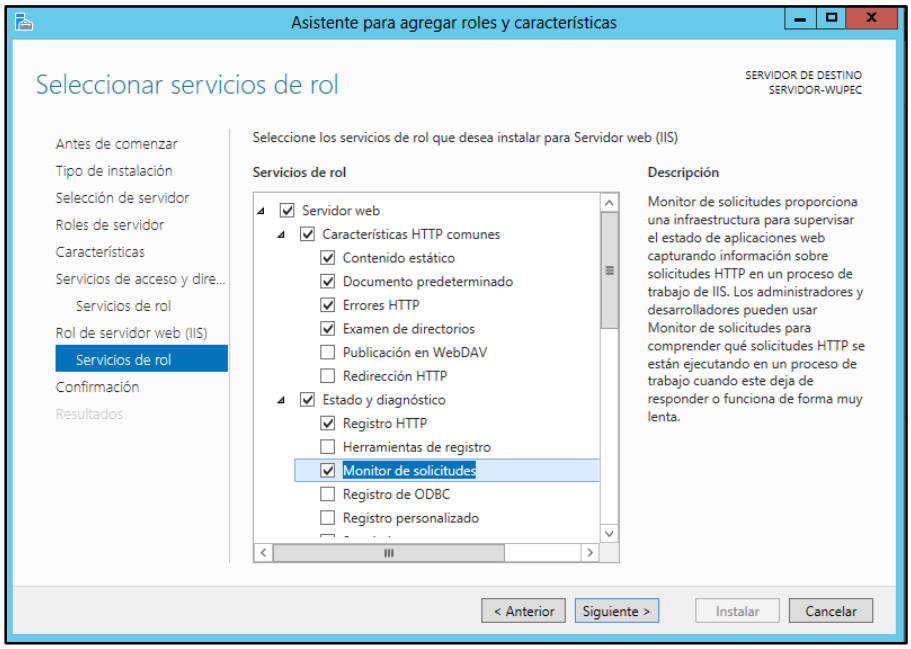
- Seleccionar Servidor Web (IIS).



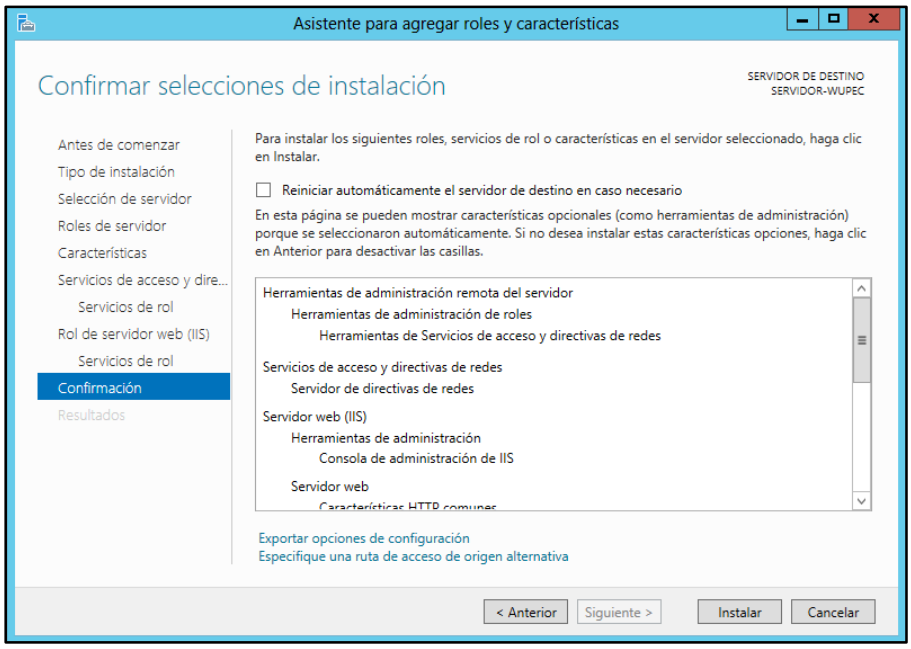
- Clic en el botón Agregar características.



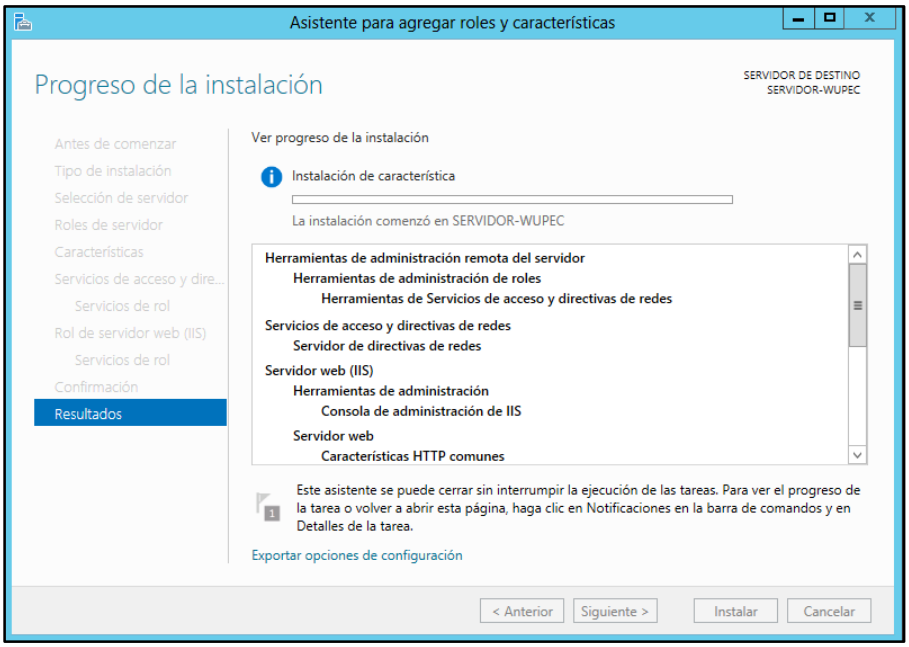
- Seleccionar servicios de rol del Servidor Web, la opción Monitor de solicitudes.



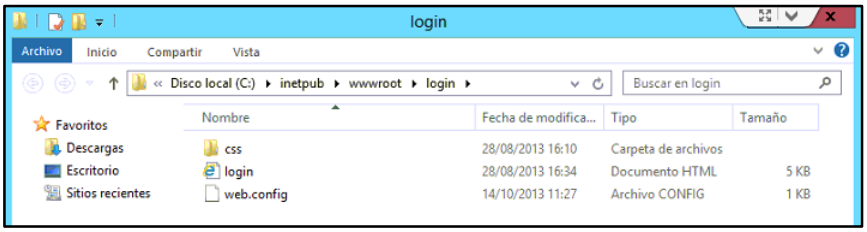
- Seleccionar reiniciar automáticamente el servidor de destino en caso necesario y clic en Instalar.



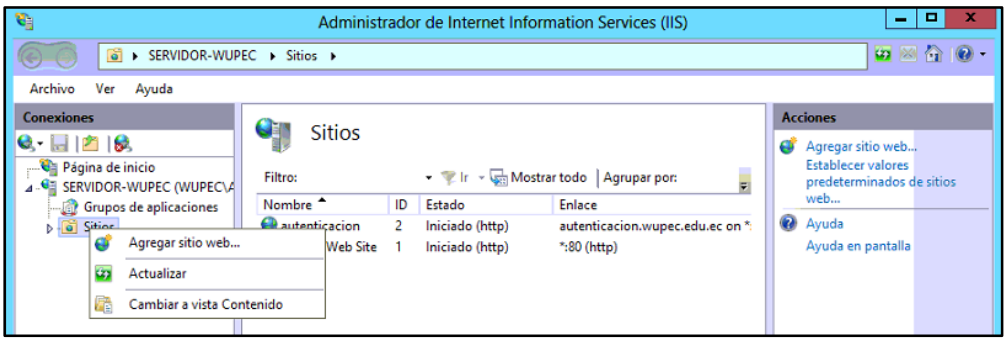
- Verificar el progreso de instalación del servidor Web.



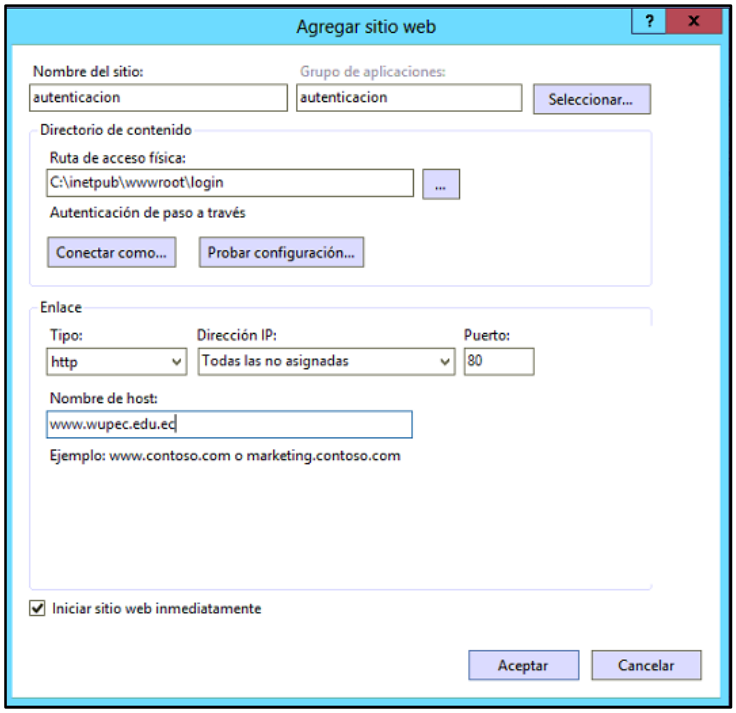
- Una vez instalado es necesario reiniciar este servicio y copiar el archivo html en el directorio C:/inetpub/wwwroot/login



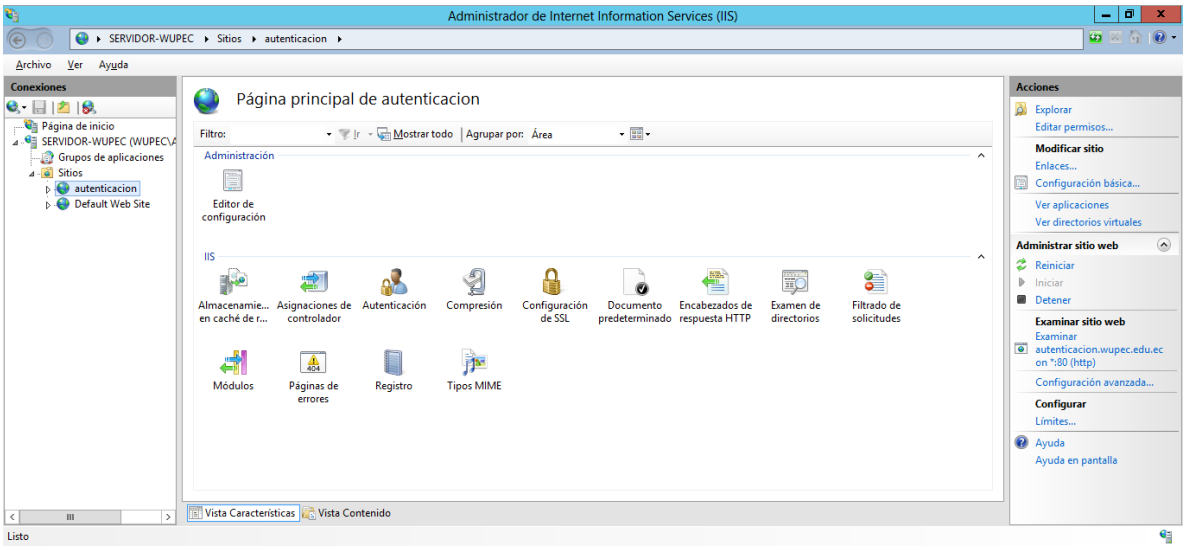
- Ir a Herramientas / Servidor Web (IIS) y clic en SERVIDOR-WUPEC / Sitios/ Agregar sitio web



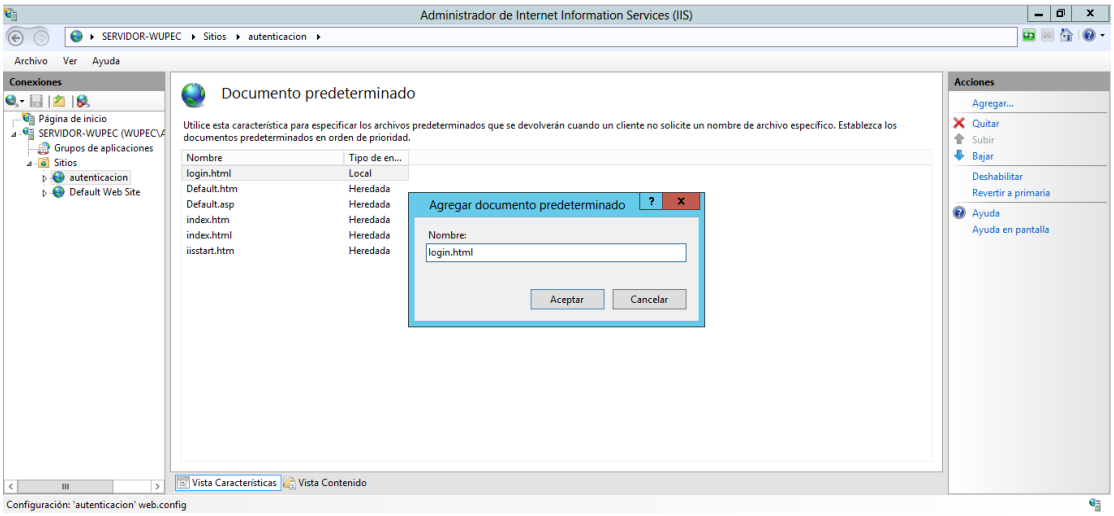
- Es necesario especificar los datos necesarios del sitio web:
    - Nombre del sitio: autenticación
    - Grupo de aplicación: autenticación
    - Ruta de acceso física: C:\inetpub\wwwroot\login
    - Enlace Tipo: http
    - Dirección IP: 172.20.64.3
    - Puerto: 80
    - Nombre del host: www.wupec.edu.ec



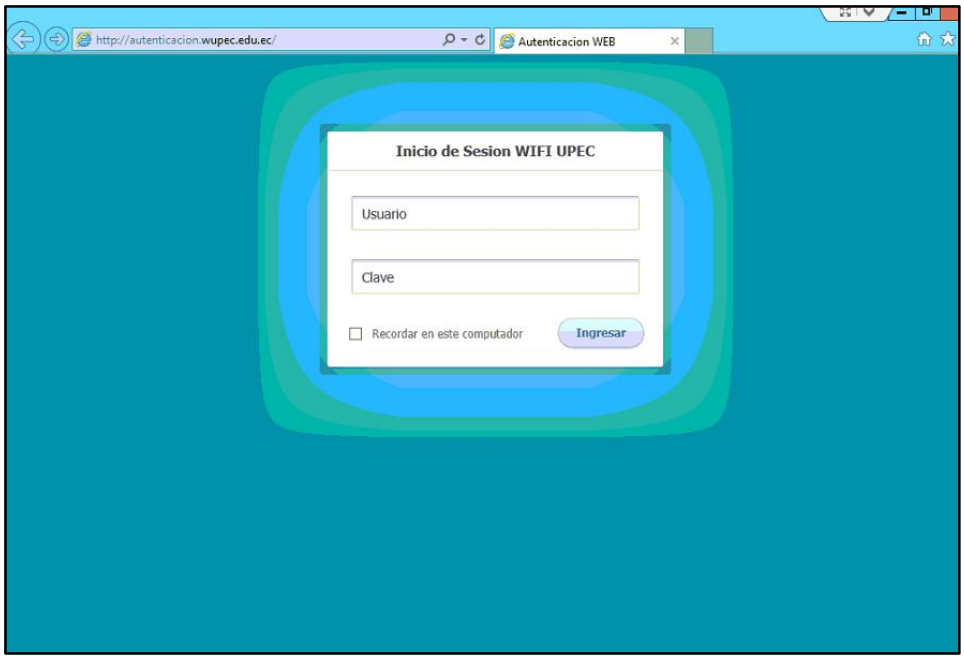
- Posteriormente ir a Sitios/ autenticacion / Documento predeterminado



- Ingresar documento predeterminado: login.html

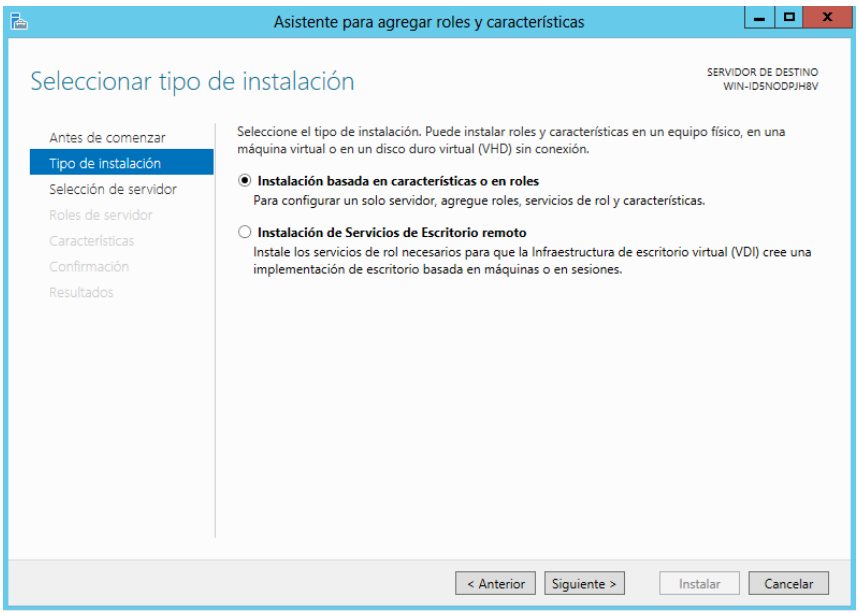


- Verificar si el servidor está corriendo para esto ir al panel de Acciones / Examinar sitio Web y debe aparecer la página de autenticación de usuarios.

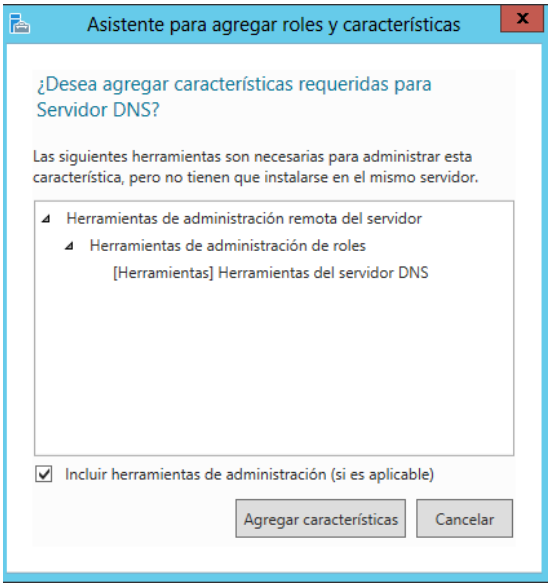


INSTALACIÓN DEL SERVIDOR DNS

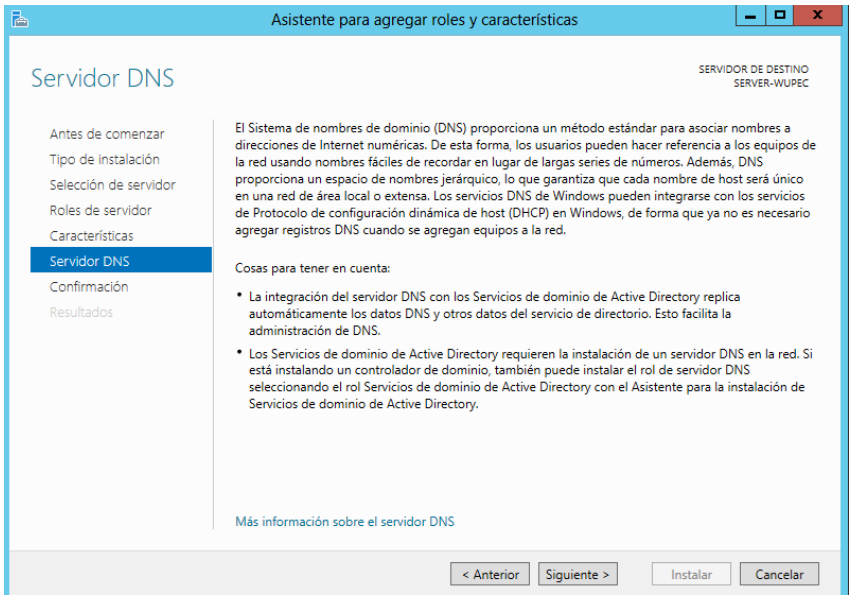
- En el lado derecho superior hacer clic en la pestaña Administrar- Agregar roles y características. Luego seleccionar Tipo de Instalación: Instalación basada en características o en roles y clic en Siguiente.



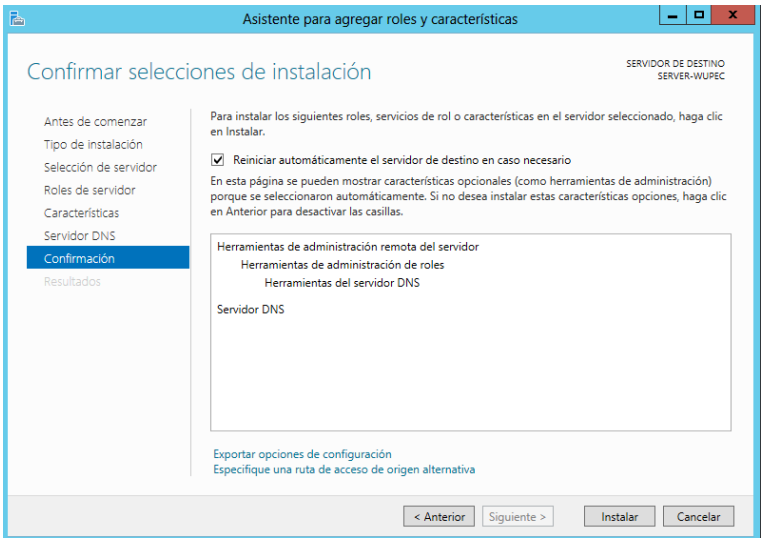
- En Roles del Servidor seleccionar Servidor DNS y clic en Agregar Características y clic en siguiente.



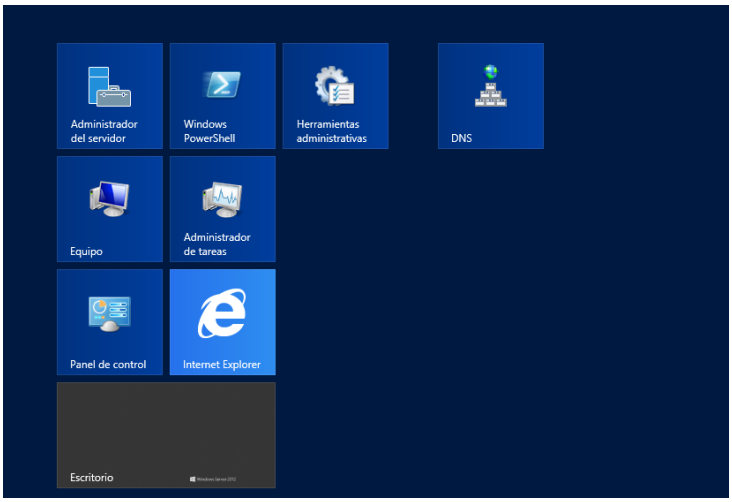
- Clic en Siguiente, aquí se explican algunas de las características de un Servidor DNS.



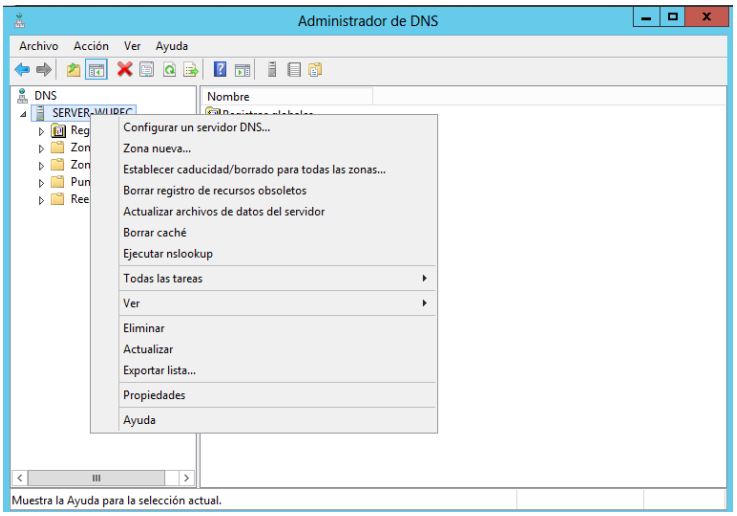
- Seleccionar la opción de reinicio automático del Servidor, clic en Sí y finalmente clic en INSTALAR.



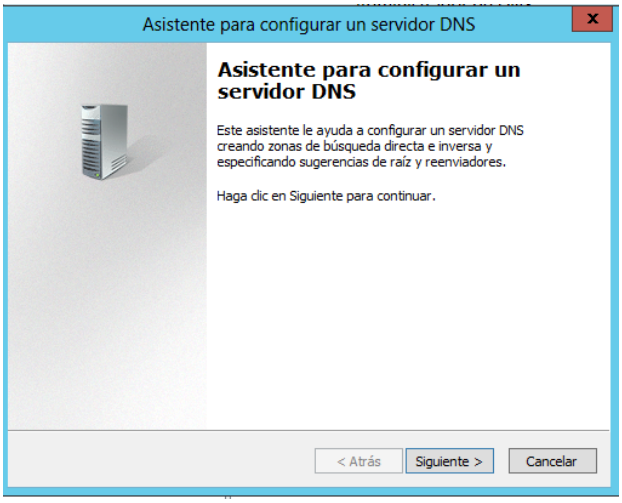
- Una vez instalado el Server DNS, hacer clic en INICIO y clic en DNS.



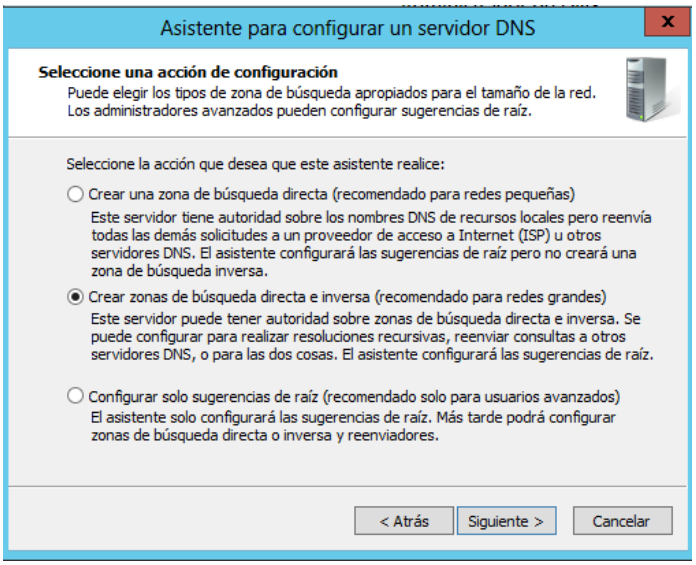
- Hacer clic derecho sobre SERVER-WUPEC y seleccionar Configurar un servidor DNS.



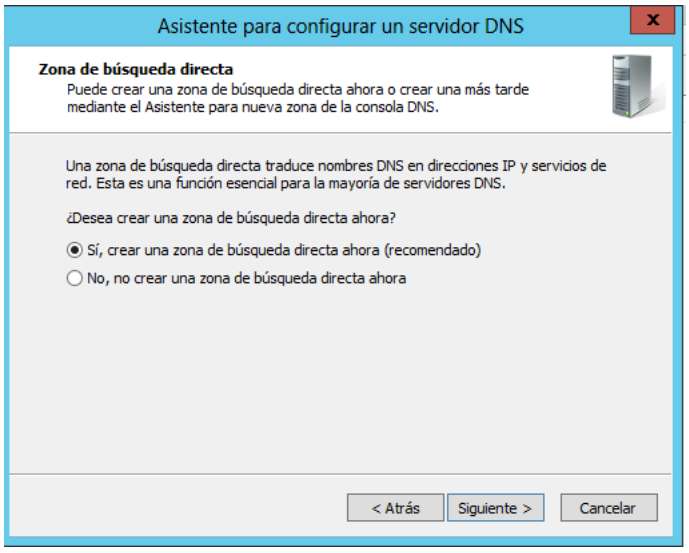
- Aparece un Asistente para la configuración del servidor y clic en Siguiente



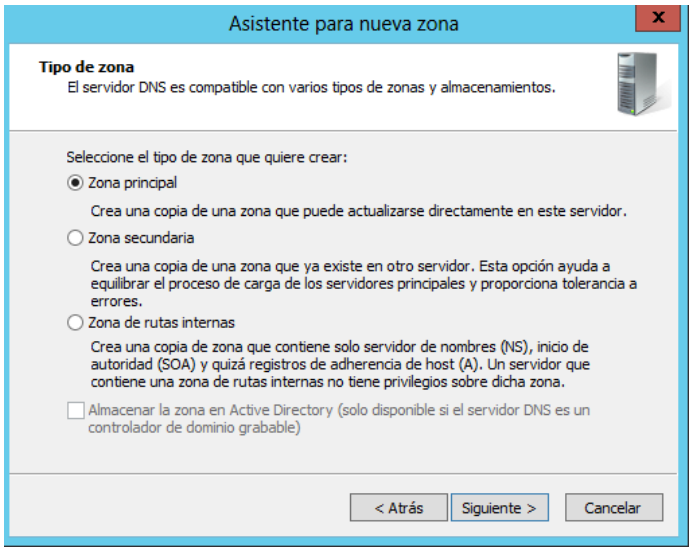
- Seleccionar la opción: Crear zonas de Búsqueda Directa e Inversa y clic en Siguiente.



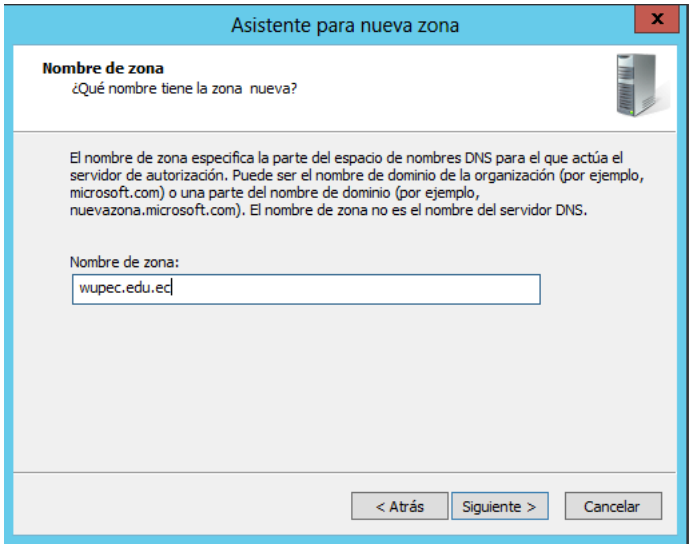
- Seleccionar la opción: Crear una zona de búsqueda ahora y clic en siguiente.



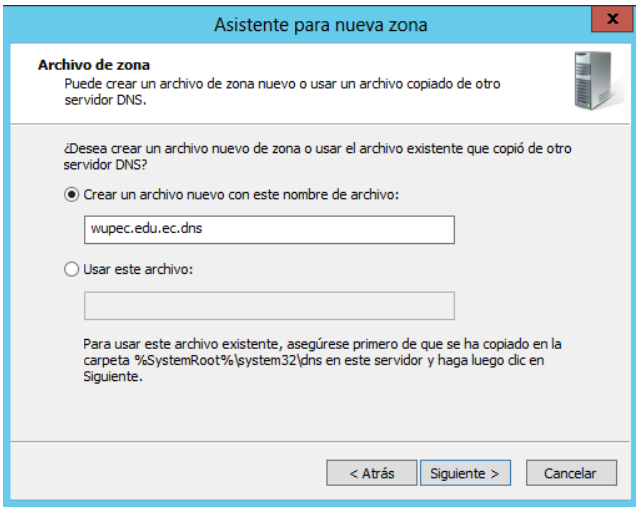
- Tipo de Zona: Zona Principal y clic en Siguiente.



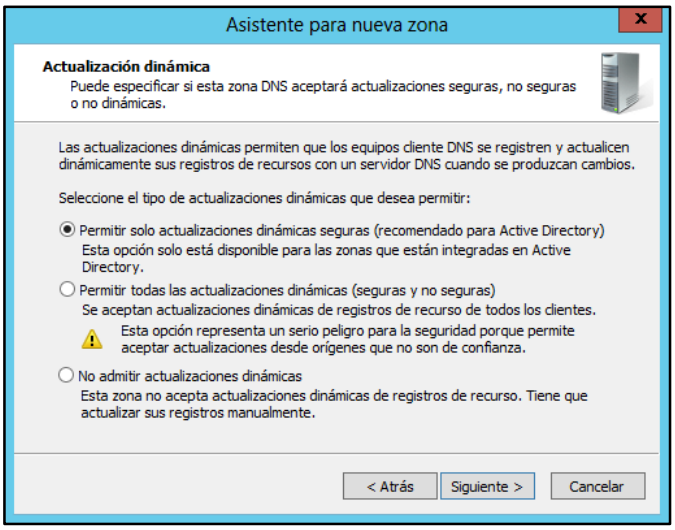
- Crear el Nombre de Zona



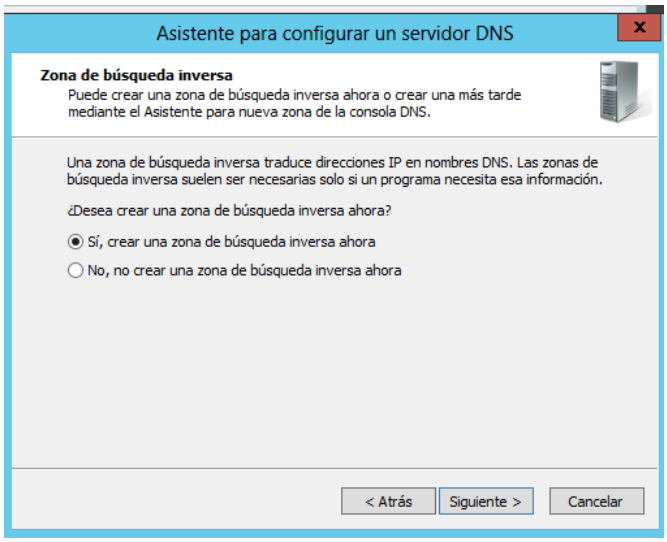
- Archivo de Zona: Seleccionar Crear un archivo nuevo y clic en Siguiente



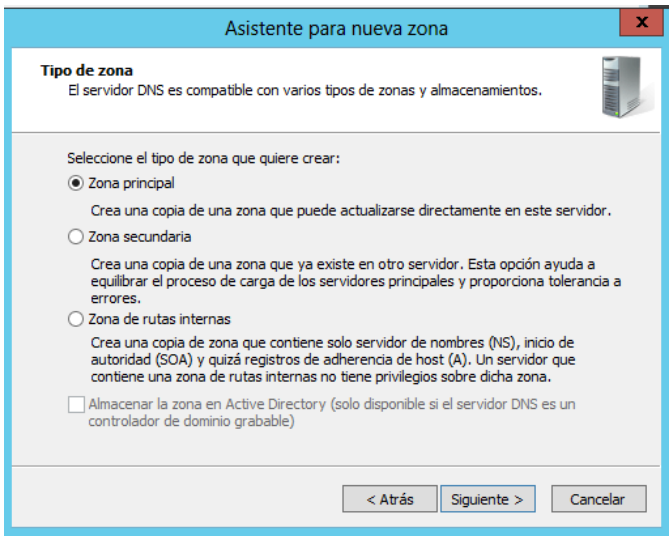
- Actualización Dinámica: Como ya está instalado el Active Directory seleccionar "Permitir solo actualizaciones dinámicas seguras", la primera opción.



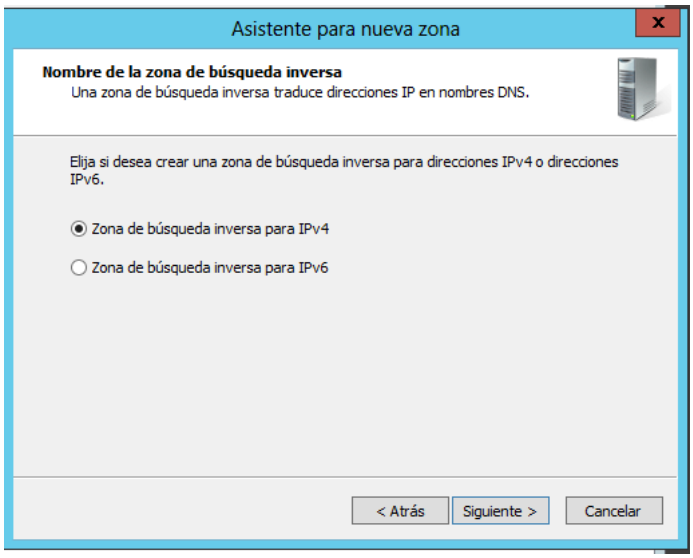
- Zona de Búsqueda Inversa: Seleccionar "Sí crear una zona de búsqueda inversa ahora" y clic en Siguiente.



- Tipo de Zona: Zona Principal y clic en Siguiente



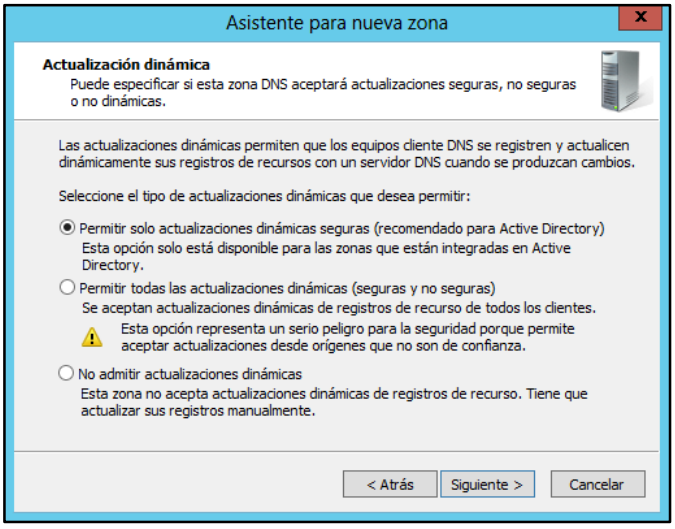
- Nombre de la Zona de Búsqueda Inversa: Elegir la opción Zona de búsqueda inversa para IPv4 y clic en Siguiente



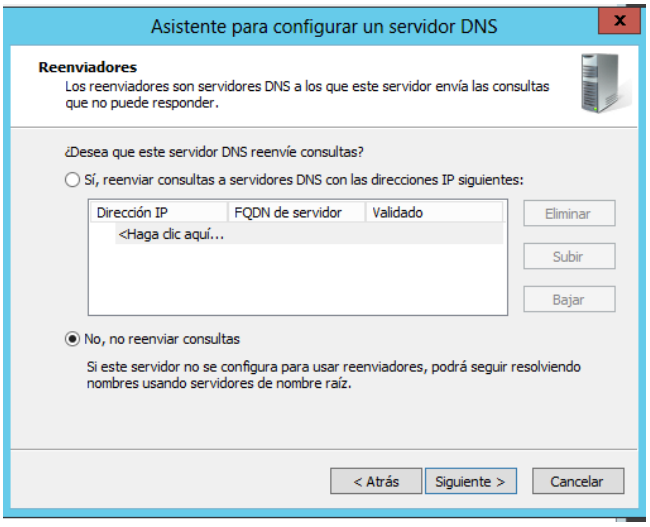
- Nombre de la zona de Búsqueda Inversa. Id. De red: 172.20.64

- En Archivo de Zona seleccionar crear un archivo nuevo con este nombre de archivo: 64.20.172.in-addr.arpa.dns

- Actualización Dinámica: Para Active Directory activar Permitir solo actualizaciones dinámicas seguras”

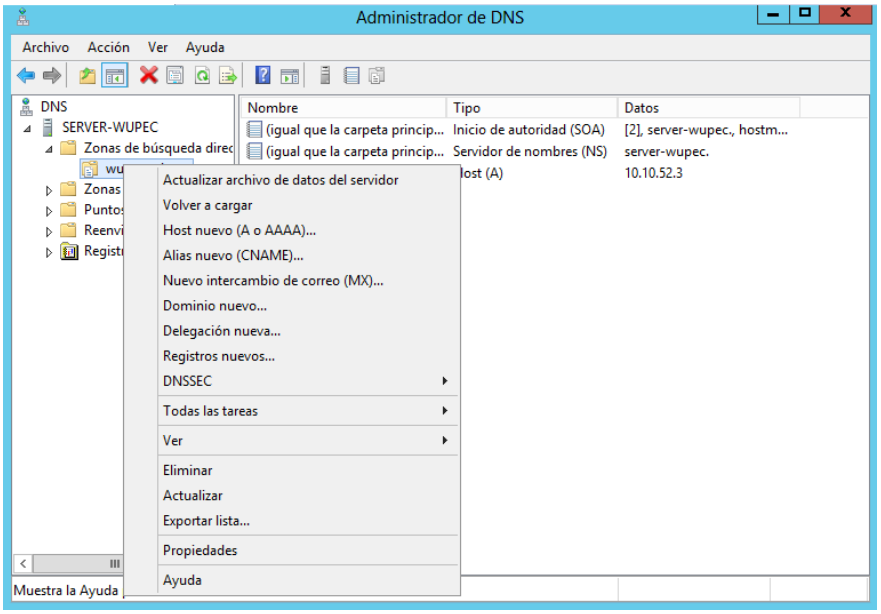


- REENVIADORES: En el caso de que este servidor DNS no pueda resolver consultas se enviará a otros servidores para que lo hagan.

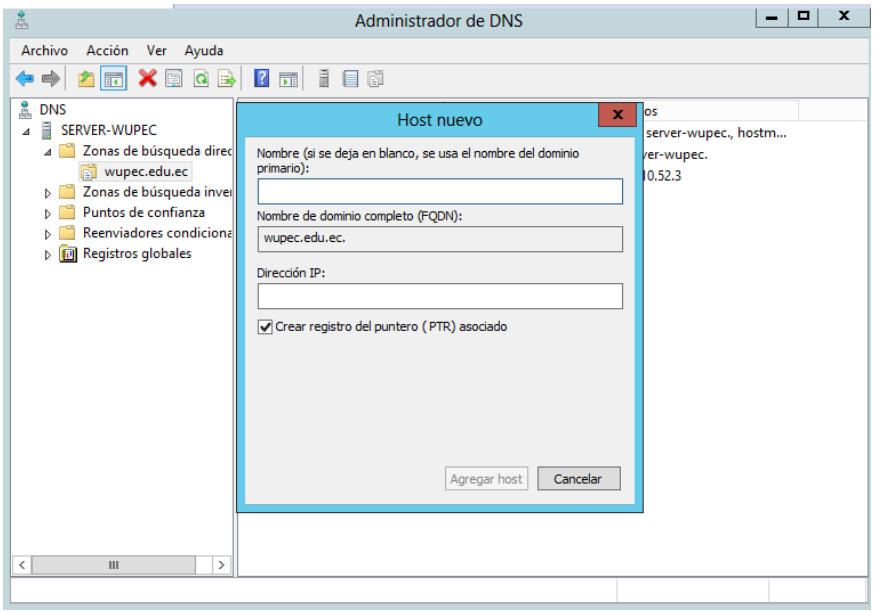


- Clic en Finalizar

- En la configuración de DNS, hacer clic sobre el dominio en este caso (wupec.edu.ec) y agregar Nuevo Host A o AAA.



- Aparece la siguiente ventana

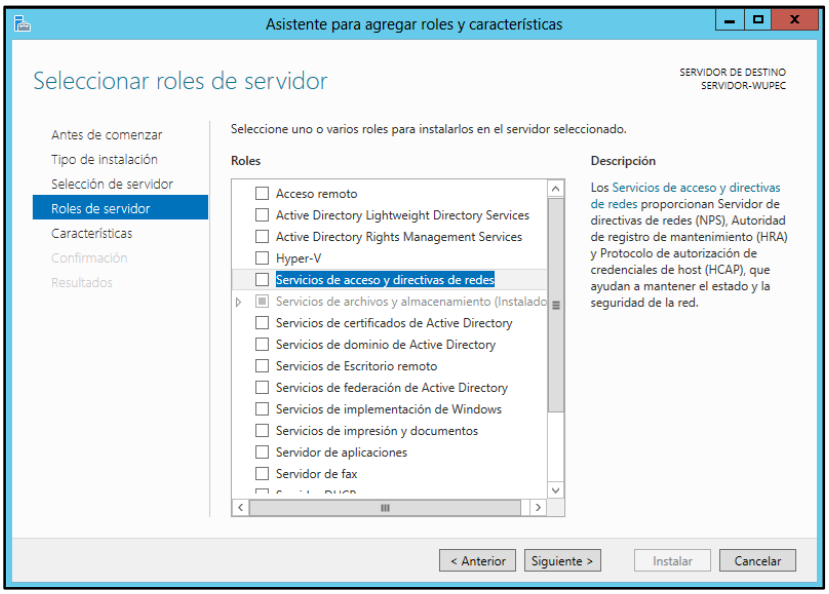


- En nombre: autenticación y se autocompleta el nombre de dominio completo: autenticación.wupec.edu.ec.
    - En Dirección IP: 1.1.1.1 (dirección virtual de WLC Cisco) y seleccionar la opción Crear registro de puntero y clic en agregar host.

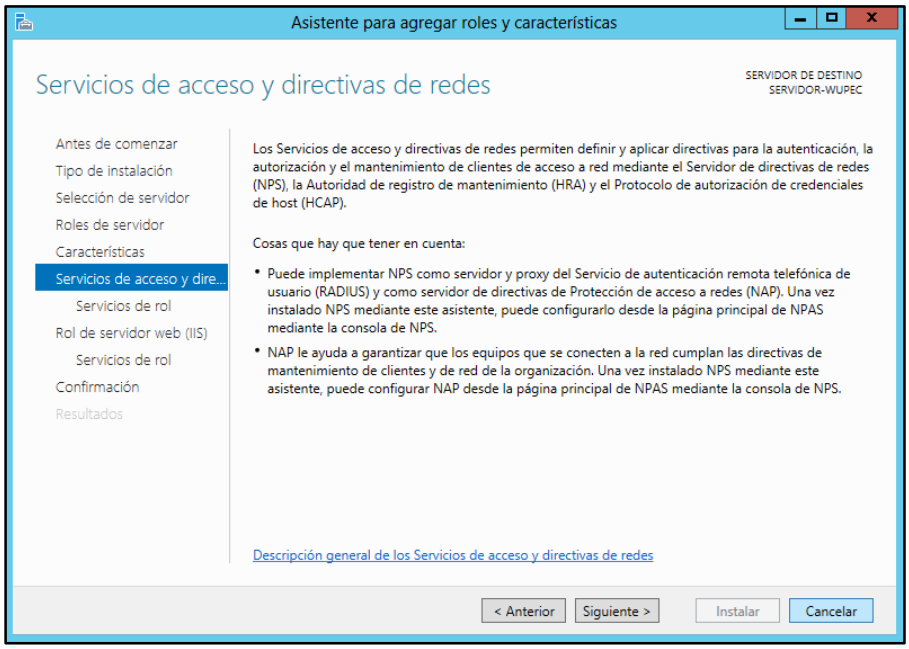
- Finalmente reiniciar el Servidor y verificar desde un cliente con el comando ***nslookup wifi.wupec.edu.ec.*** En **REENVIADORES** poner la IP del DNS del proveedor, e igual forma en la tarjeta de red de este servidor DNS poner el DNS del proveedor, además si es necesario reiniciar el servidor, no basta con actualizarlo.

INSTALACIÓN DEL SERVIDOR DE DIRECTIVAS DE REDES (RADIUS)

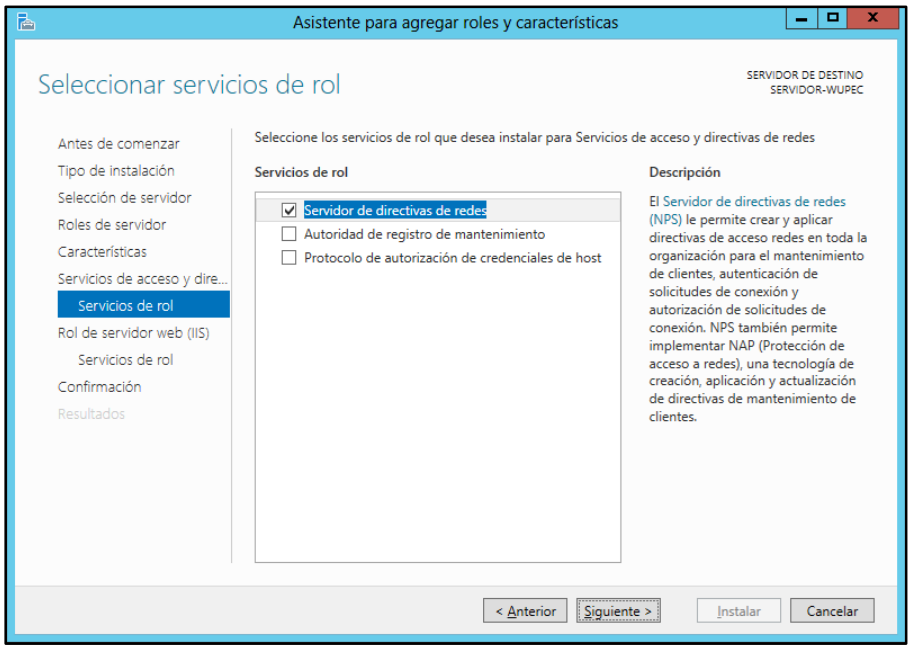
- Seleccionar roles de servidor: Servicios de acceso y directivas de redes.



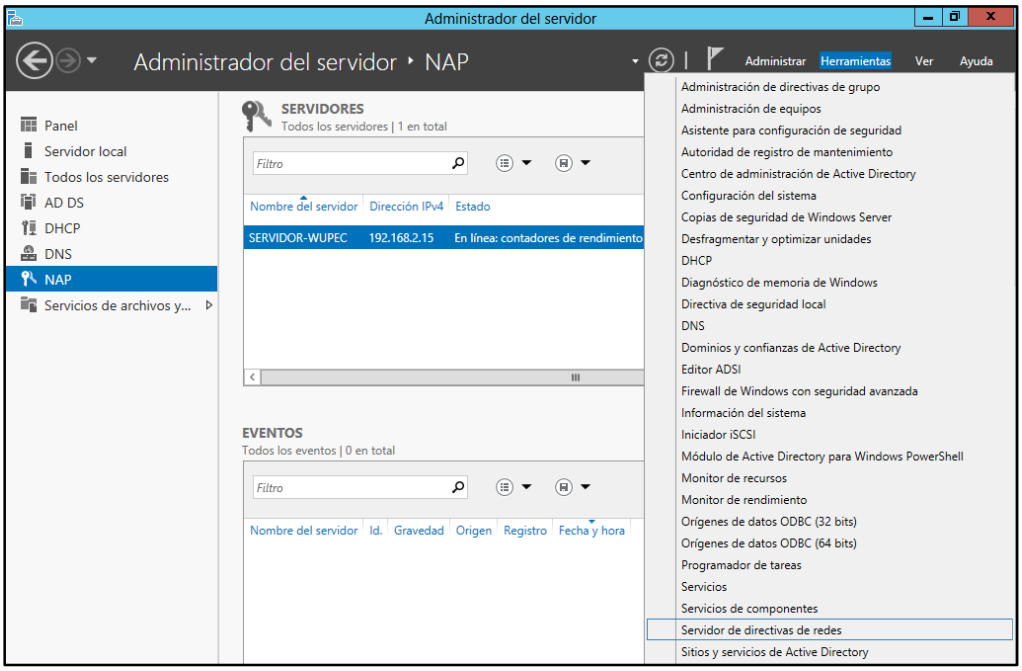
- Siguiente para continuar con la instalación.



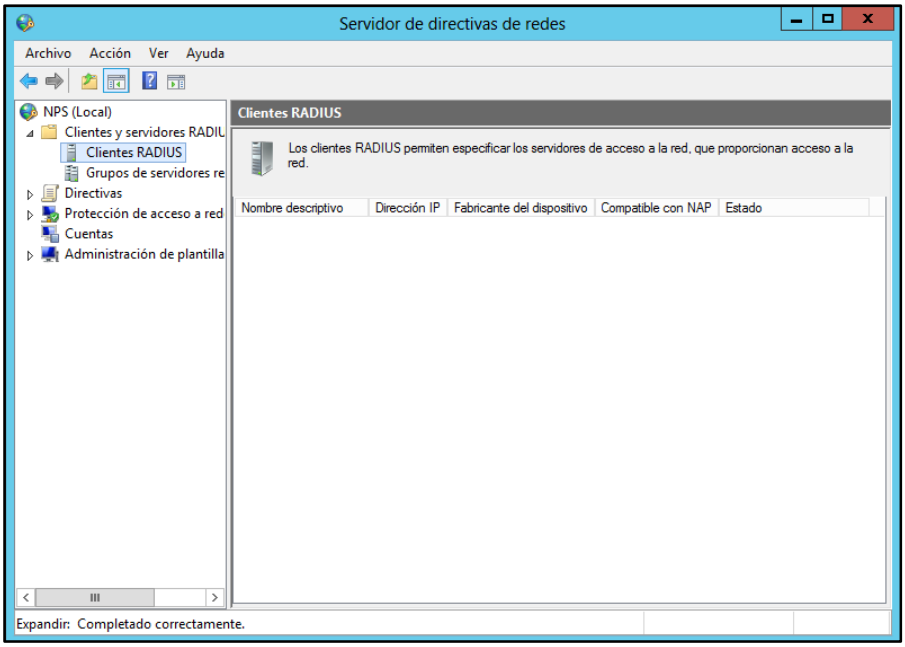
- Seleccionar Servidor de directivas de redes en servicios de rol.



- Una vez instalado ir a Herramientas / Servidor de Directivas de Redes (NAP)

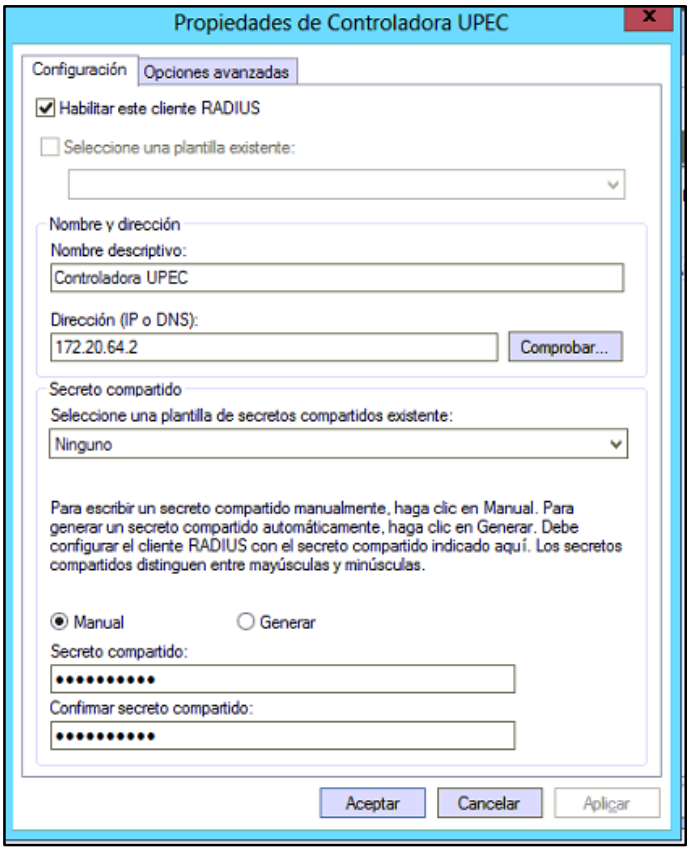


- Ir a Clientes y servidores RADIUS / Clientes RADIUS

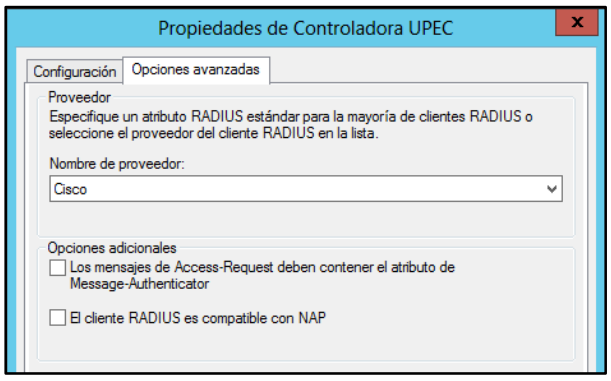


- Clic derecho nuevo cliente RADIUS
  - Habilitar este cliente RADIUS

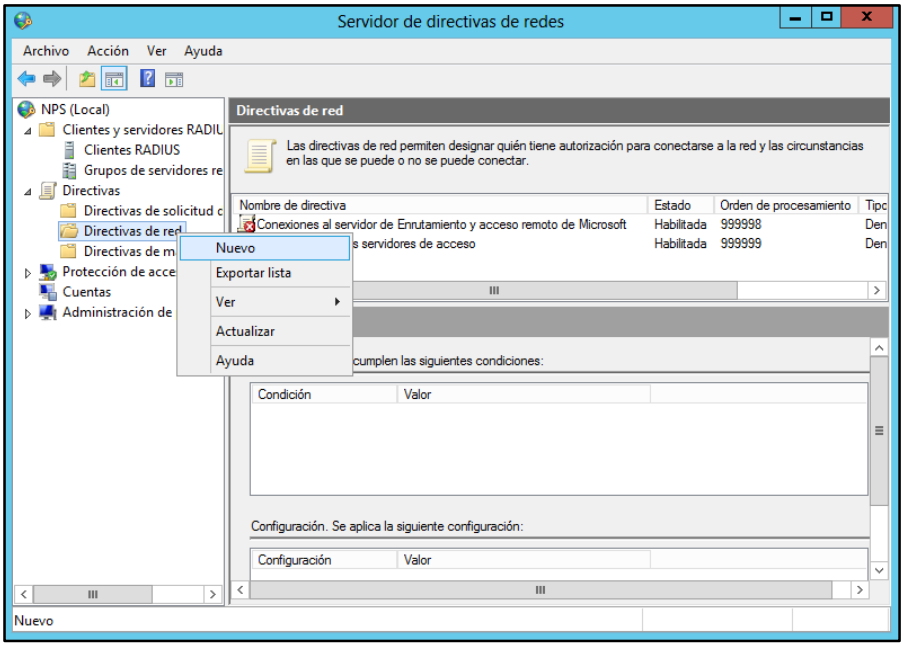
- Nombre descriptivo: Controladora UPEC
- Dirección (IP o DNS): 172.20.64.2 (IP de la controladora Cisco)
- Y habilitar una Clave de Secreto compartido que deberá ser configurada también en la WLC 5508.



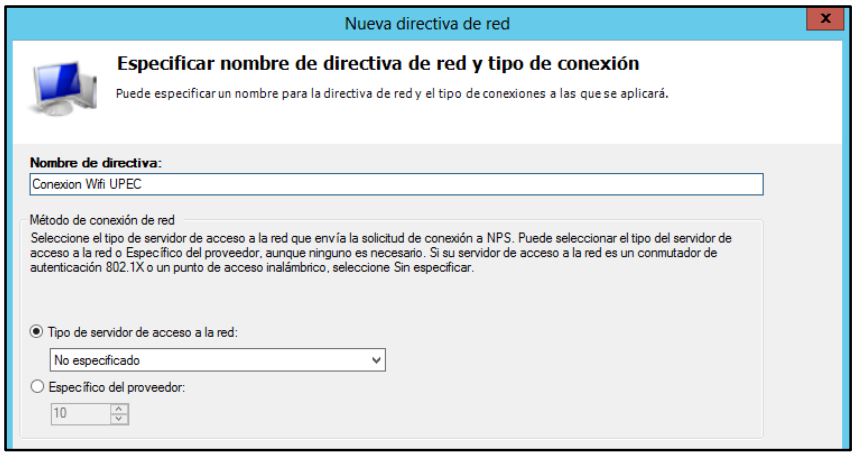
- En la pestaña Opciones avanzadas colocar el nombre del proveedor: Cisco



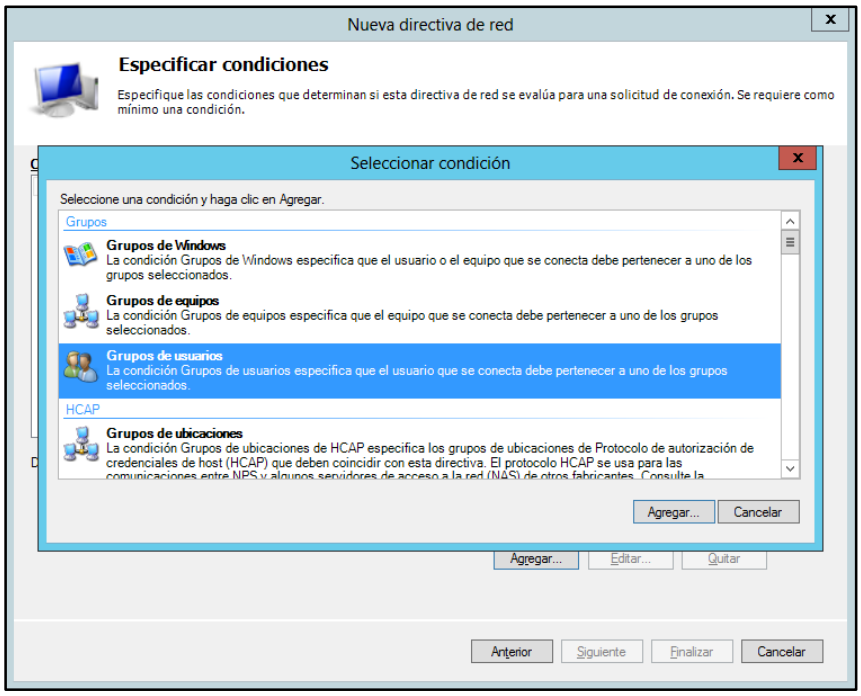
- Crear una directiva de red para esto clic derecho en Directivas de red / Nuevo



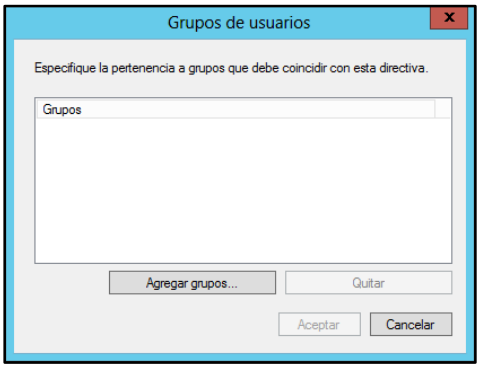
- Especificar nombre de directiva de red y tipo de conexión
  - Nombre de directiva: Conexión Wifi UPEC
  - Tipo de Servidor de acceso a la red: No especificado



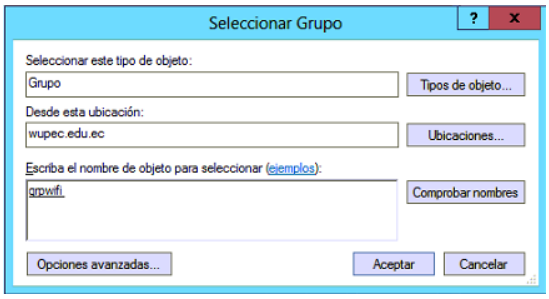
- Agregar / Grupos de usuarios



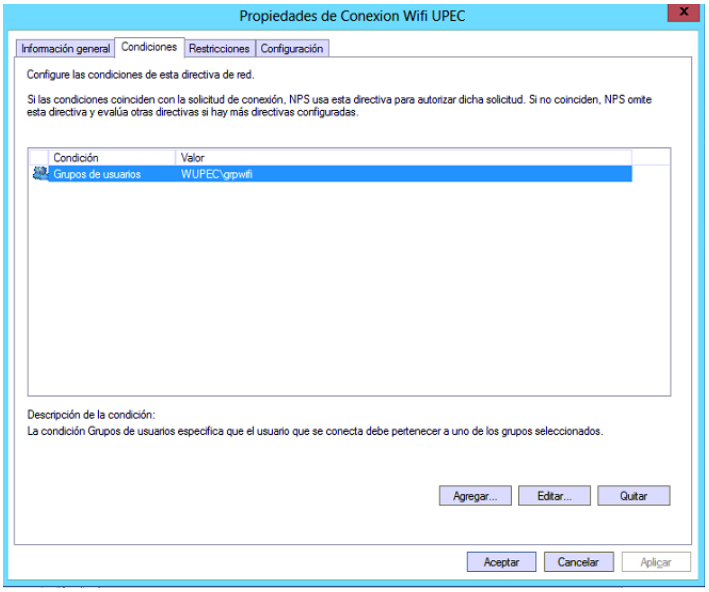
- Agregar el grupo al cual los usuarios deben pertenecer para tener acceso al servicio de Internet.



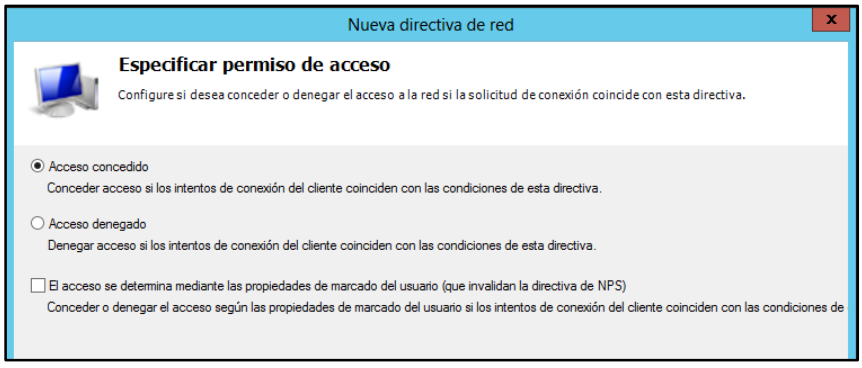
- Escribir el nombre de objeto para seleccionar y comprobar nombres para verificar que si existe el grupo dentro del Active Directory (grpwifi).



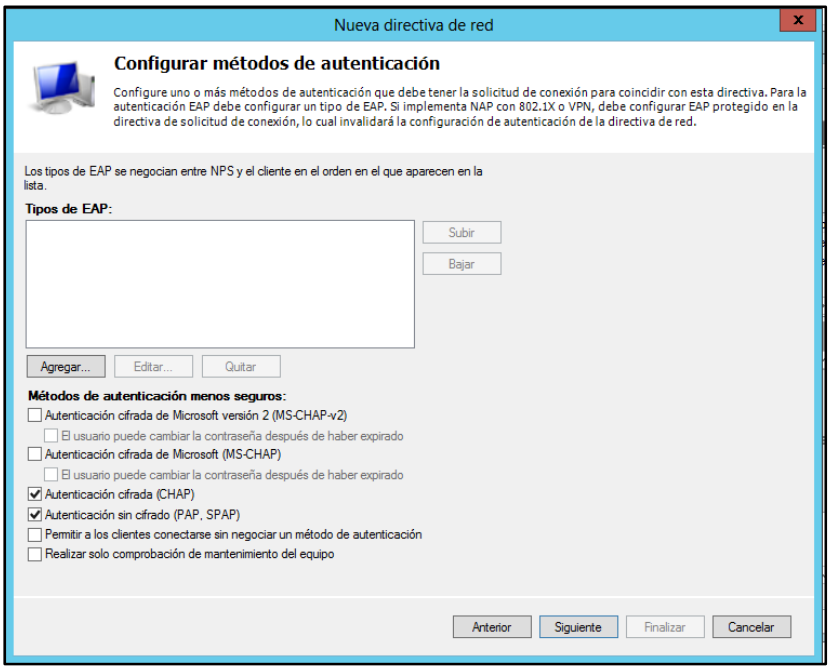
- Una vez agregado todos los grupos de usuarios continuar con la configuración del Servidor.



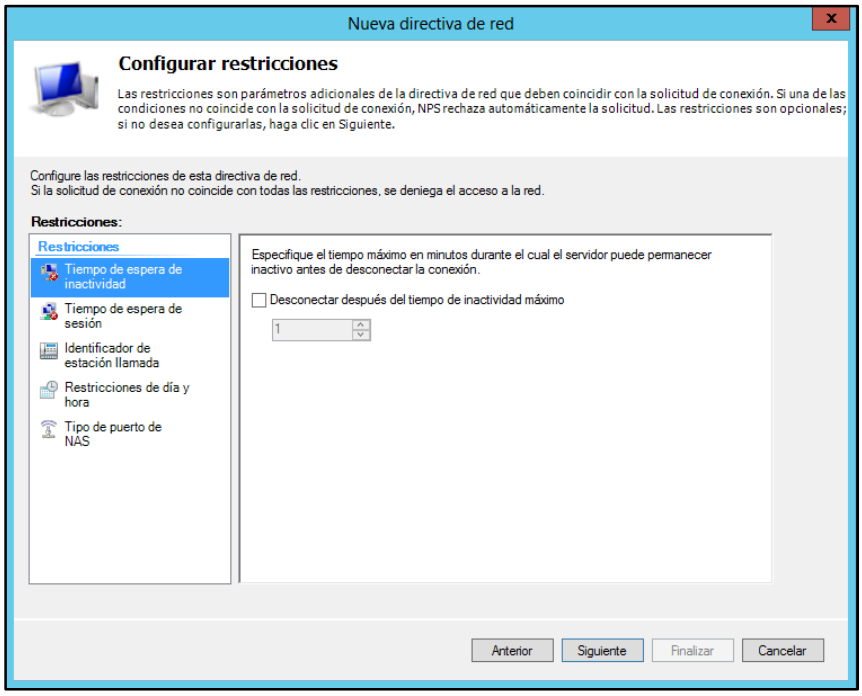
- Especificar permiso de acceso: Acceso concedido



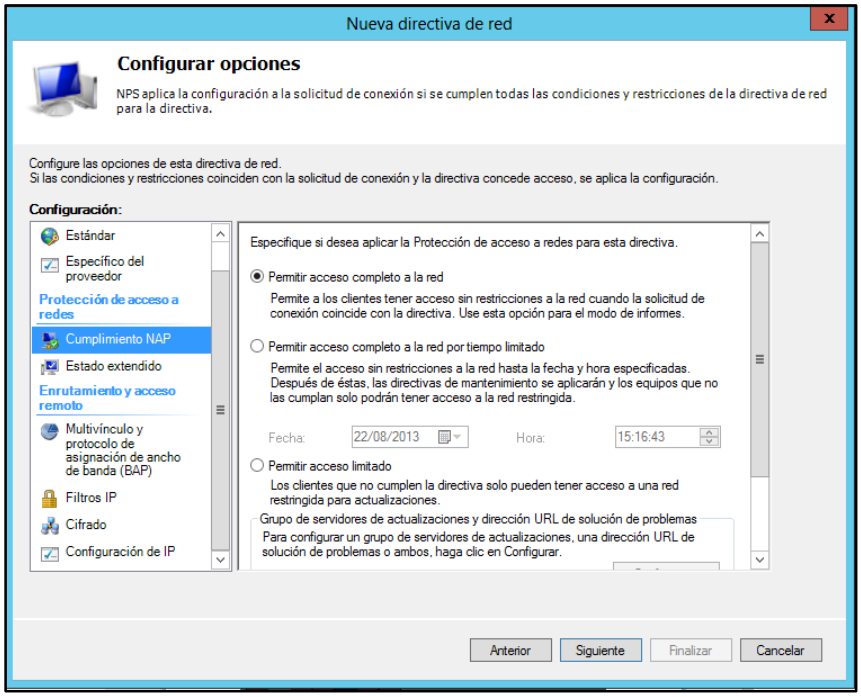
- Configurar métodos de autenticación (Dejar los métodos de autenticación por defecto)



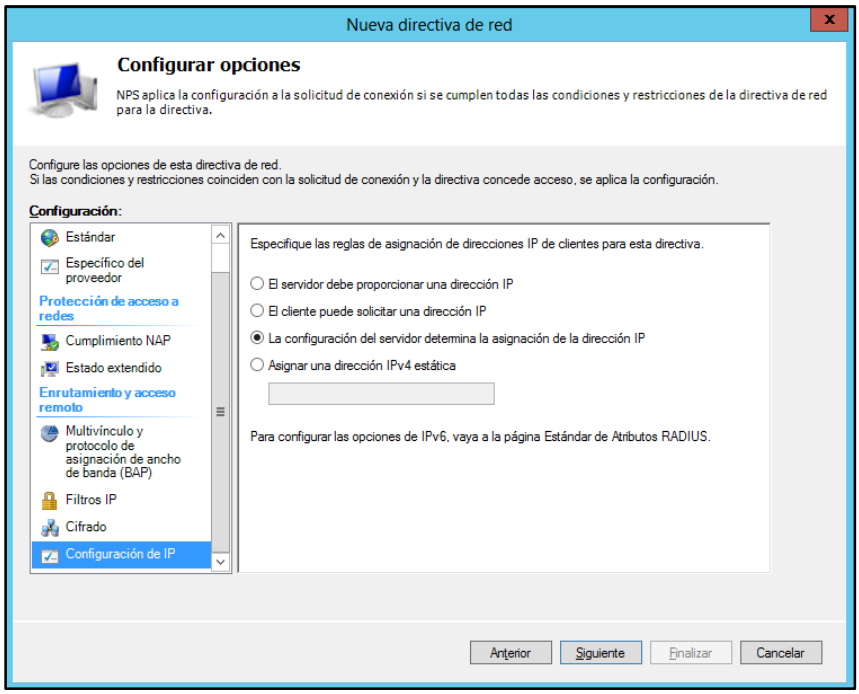
- Configurar las restricciones: Tiempo de espera de inactividad, Tiempo de espera de sesión, Identificador de estación llamada y Restricciones de día y hora.



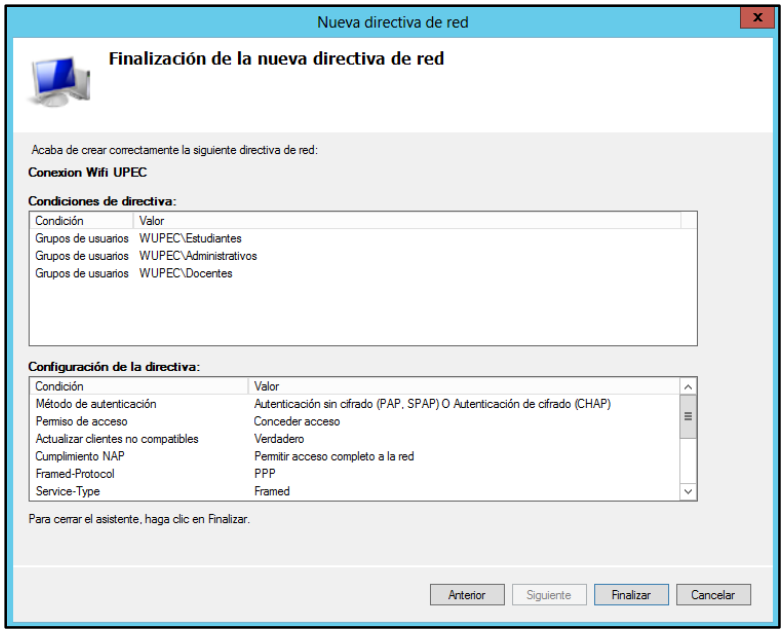
- Cumplimiento de NAP: Permitir acceso completo a la red



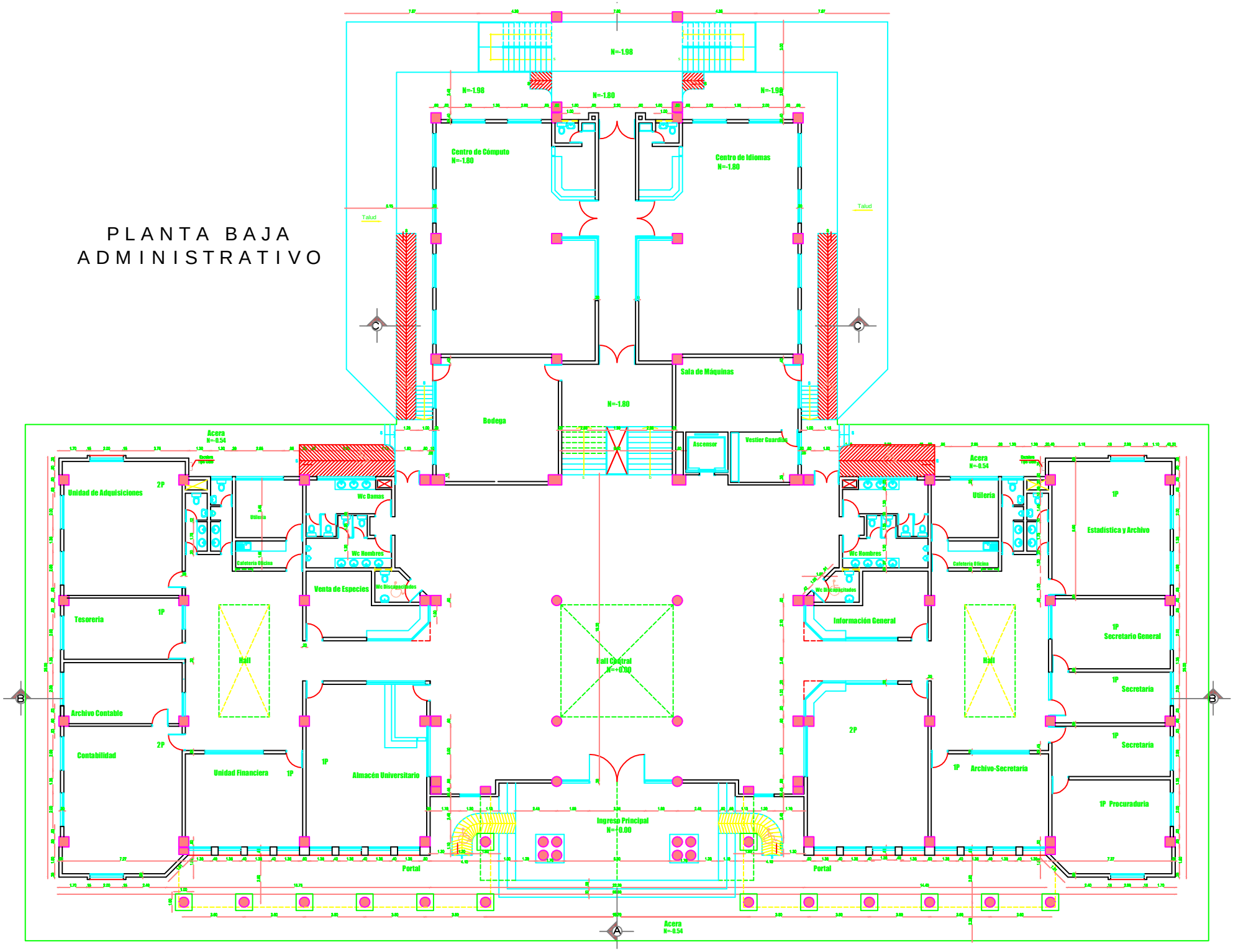
- Configuración de la dirección IP: La configuración del servidor determina la asignación de la dirección IP



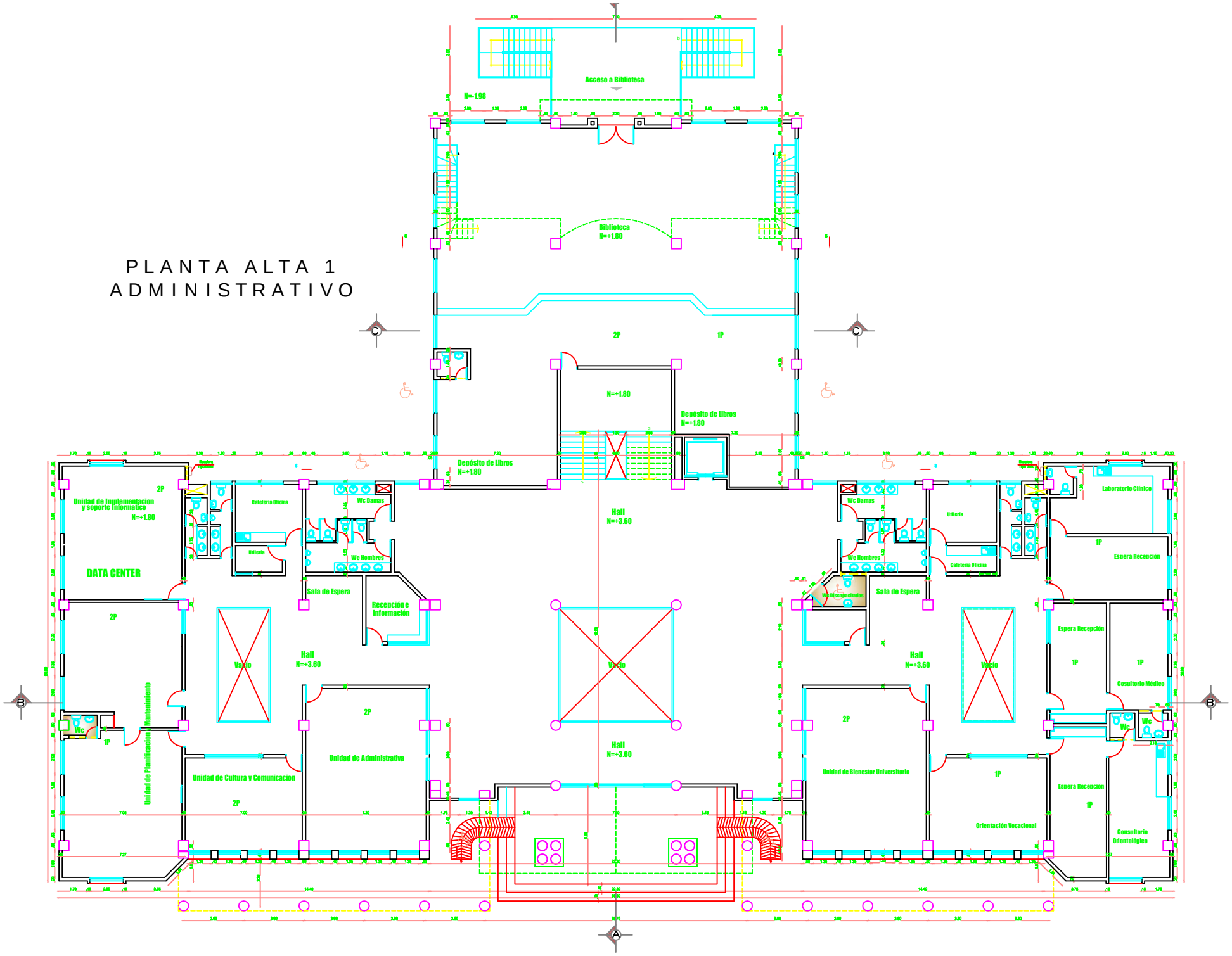
- Finalización de la nueva directiva



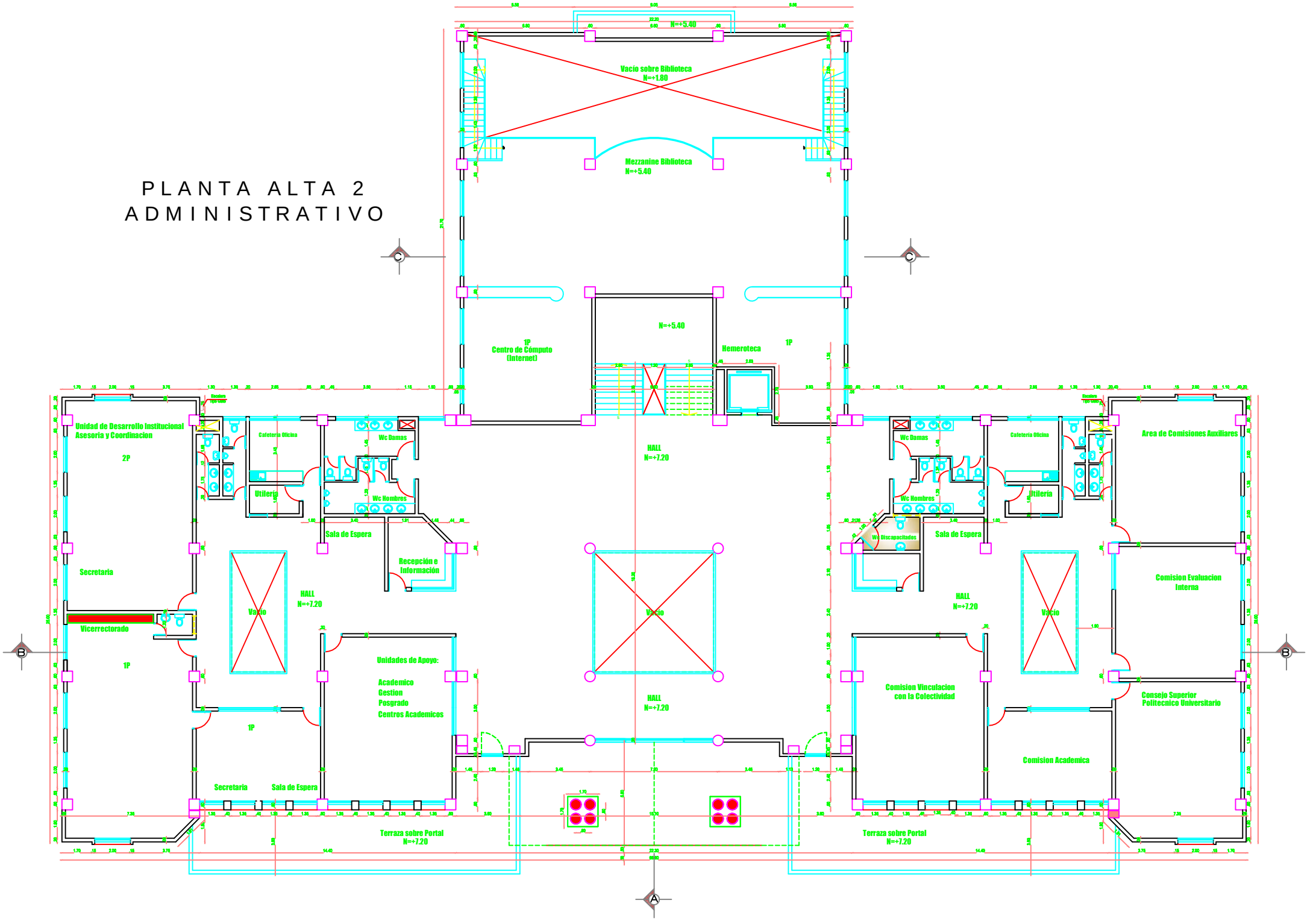
PLANTA BAJA
ADMINISTRATIVO



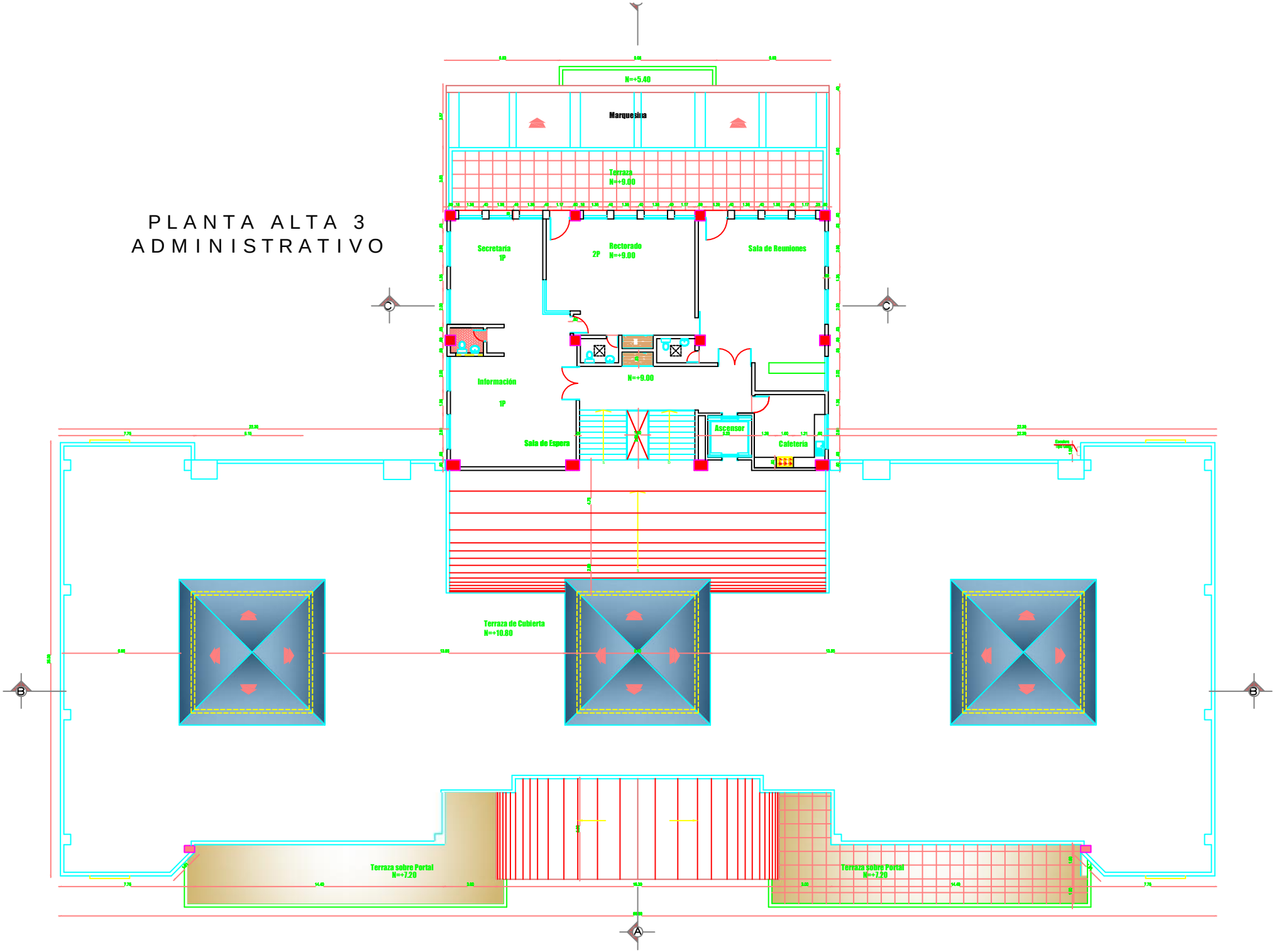
PLANTA ALTA 1
ADMINISTRATIVO



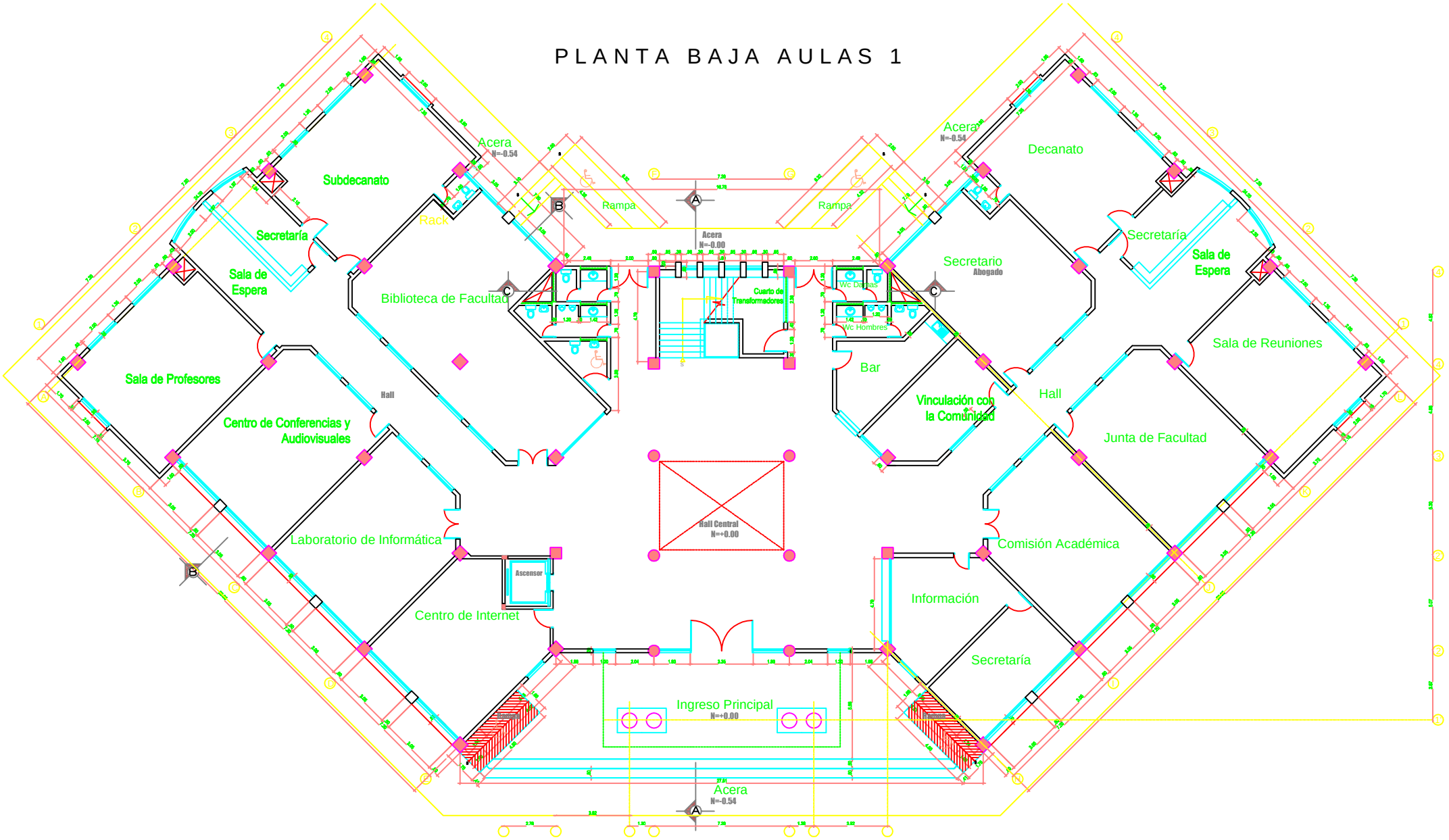
PLANTA ALTA 2
ADMINISTRATIVO



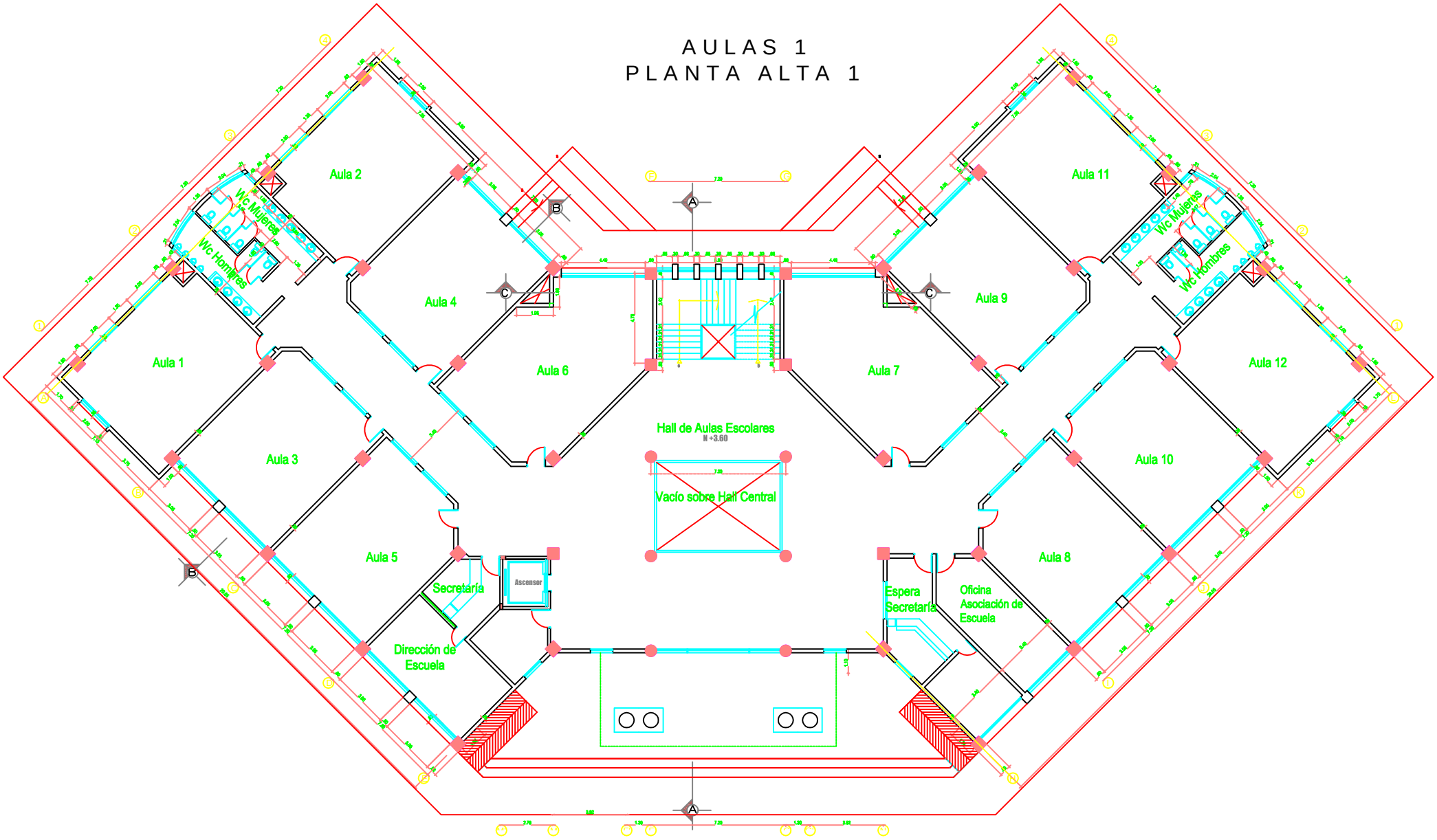
PLANTA ALTA 3
ADMINISTRATIVO



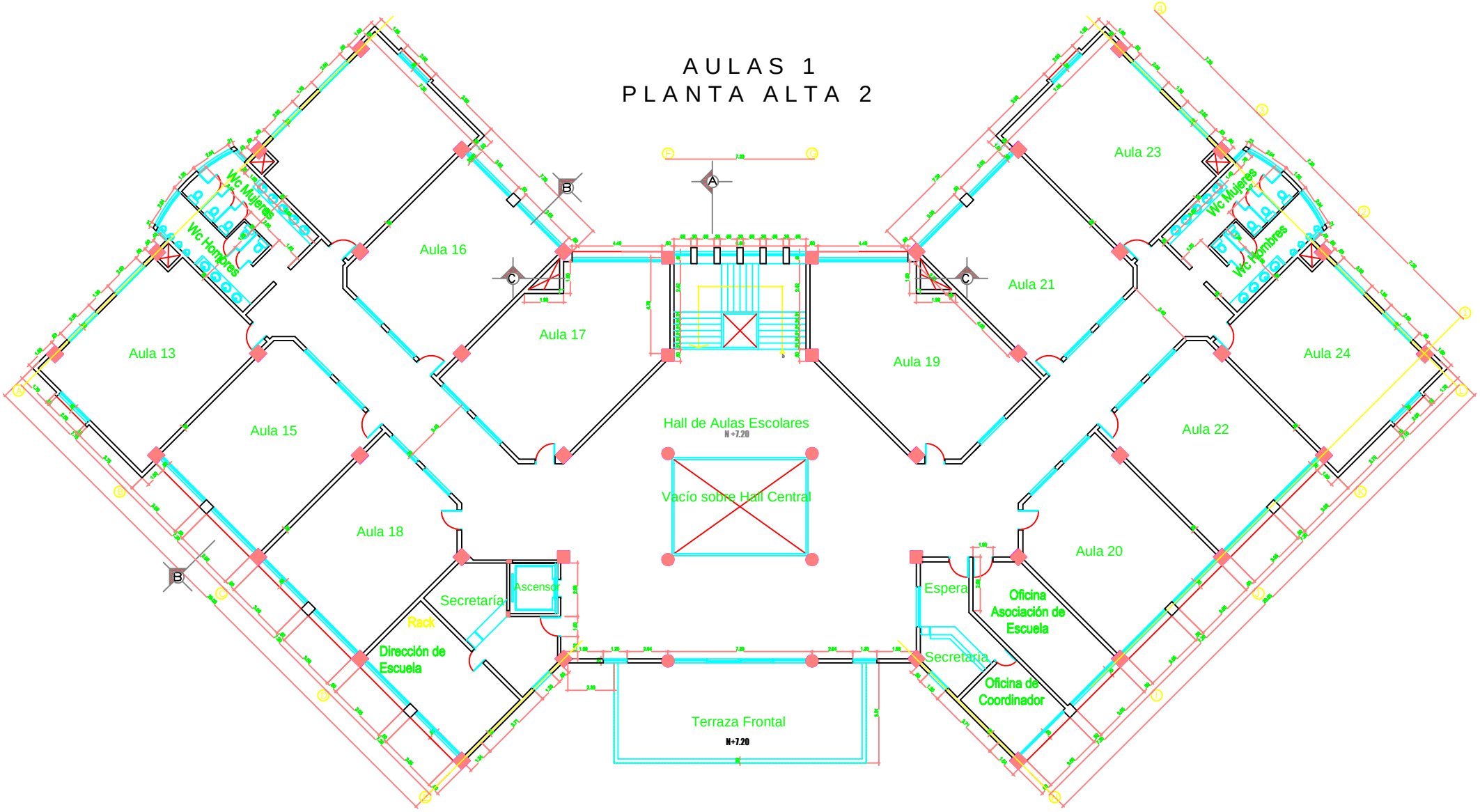
PLANTA BAJA AULAS 1



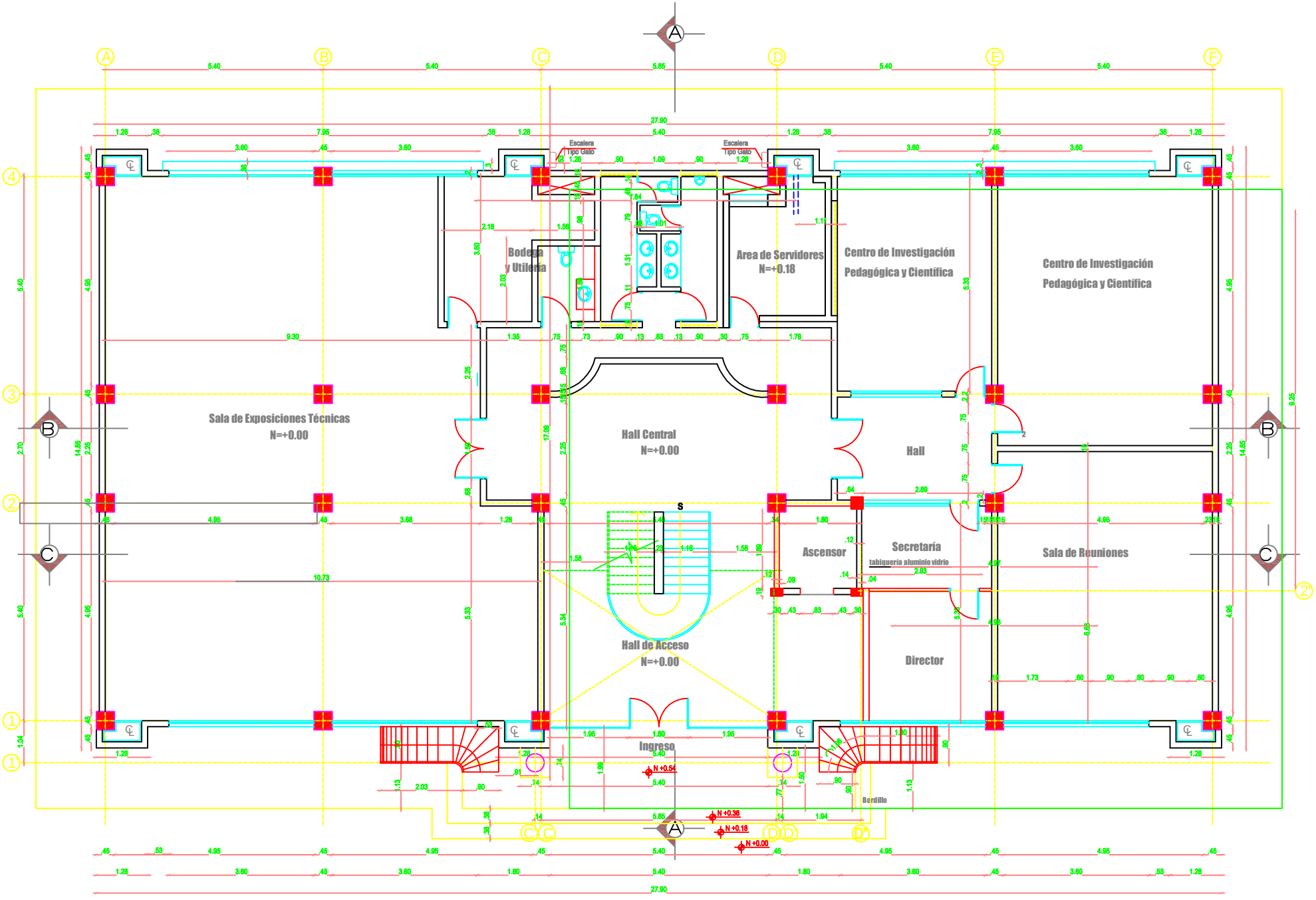
AULAS 1
PLANTA ALTA 1



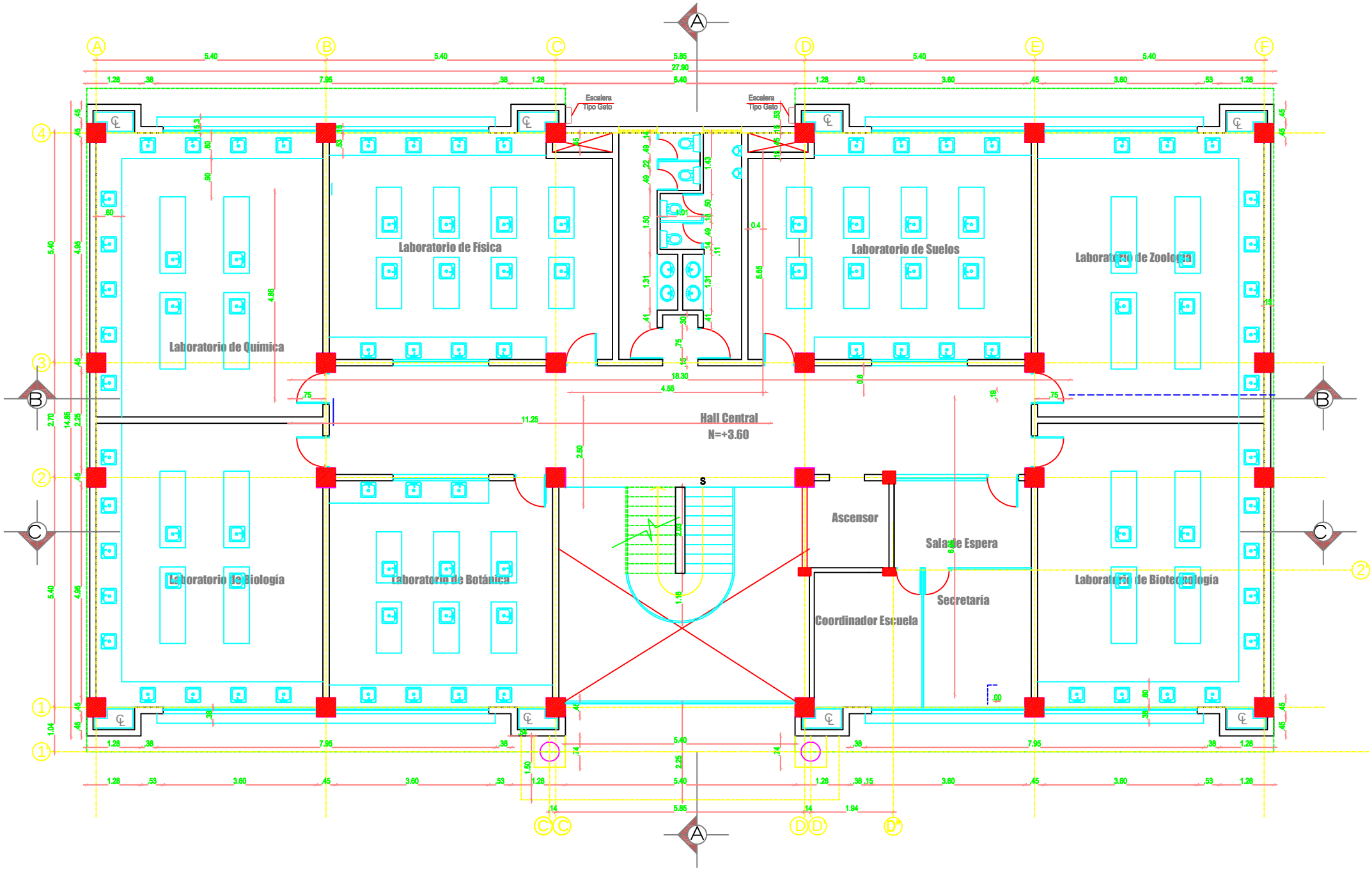
AULAS 1
PLANTA ALTA 2



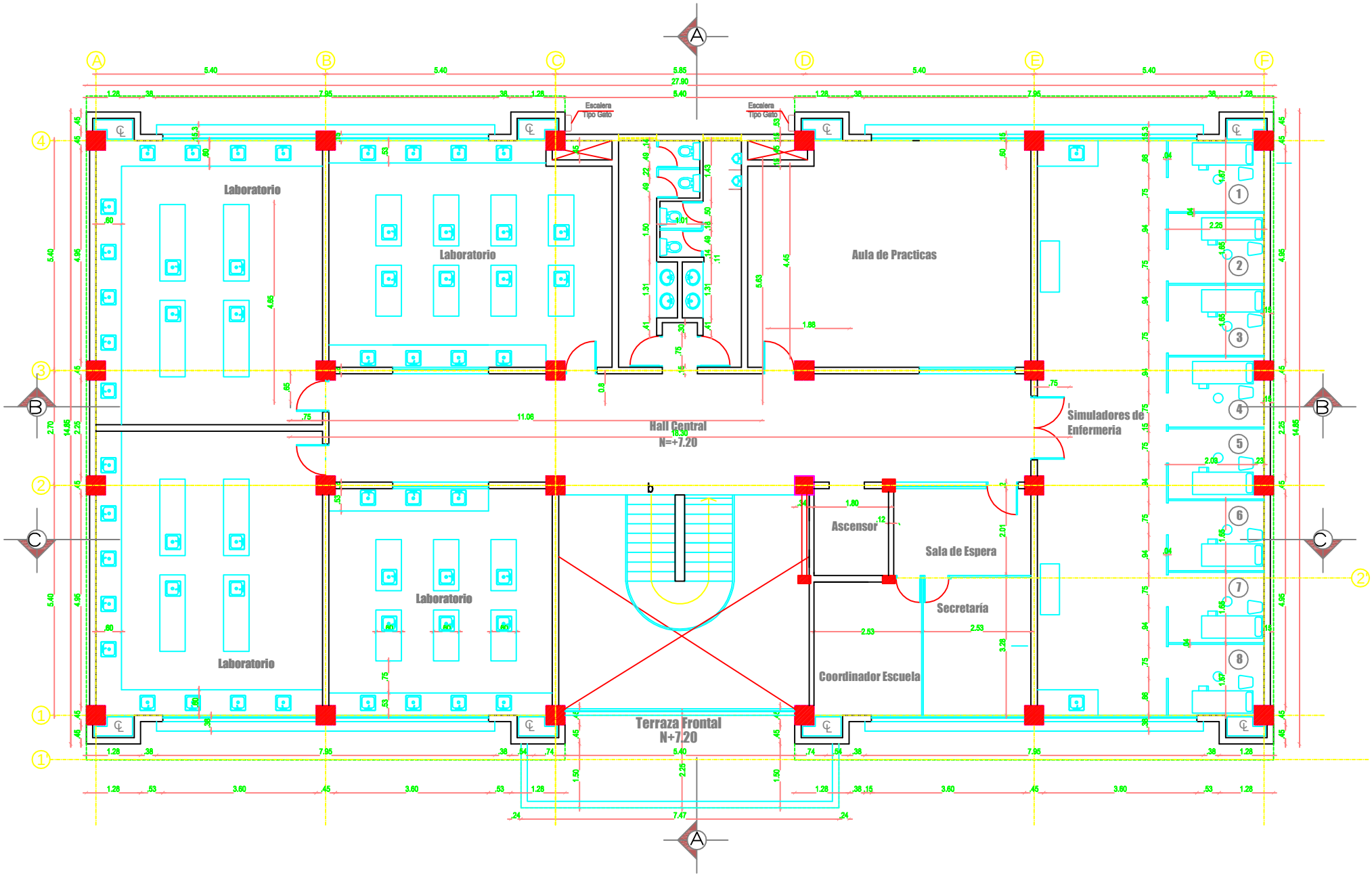
LABORATORIOS
PLANTA BAJA



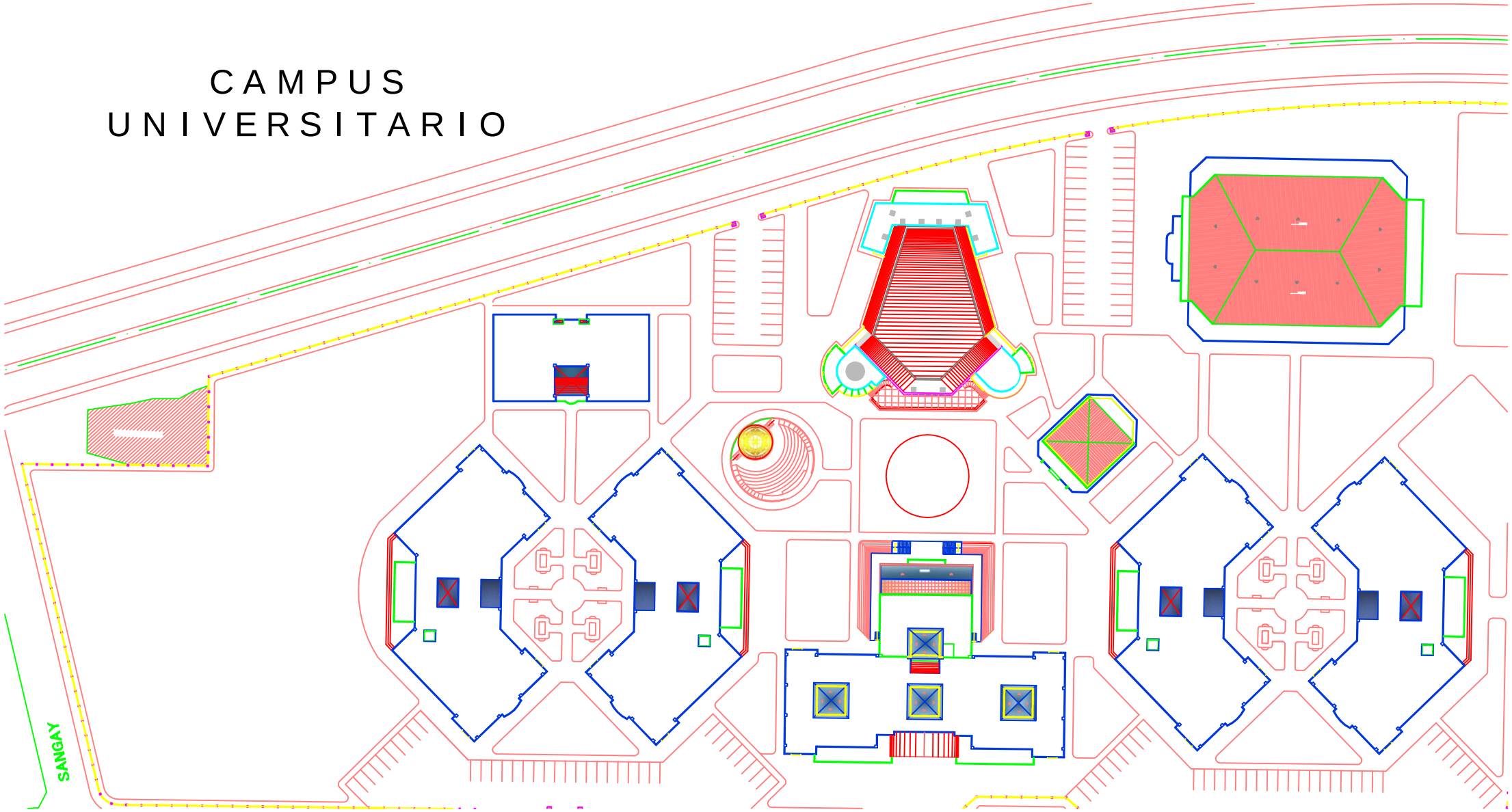
LABORATORIOS
PLANTA ALTA 1



LABORATORIOS
PLANTA ALTA 2



CAMPUS UNIVERSITARIO



PROFORMA

AMPLIACION DE LA RED INALAMBRICA PARA EL CAMPUS Y NUEVOS EDIFICIOS UPEC

CANT	DESCRIPCION	P. UNIT	P. TOTAL
	ADICIONALES PARA CONTROLADORA		-
4	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	780,00	3.120,00
4	Patch cord de Fibra optica tipo LC- LC OM3	34,50	138,00
1	25 AP Adder License for the 5508 Controller (eDelivery)	11997,00	11.997,00
	ACCESS POINT PARA EXTERIORES		-
2	802.11N Outdoor Access Point,Ext. Ant.,Uniband,A Reg. Dom.	1495,00	2.990,00
4	2.4 GHz 4dBi/5 GHz 7dBi Dual Band Omni Ant., Gray, N conn.	349,00	1.396,00
2	Power Injector - 30W non-rugged-SPARE	149,00	298,00
2	SMARTNET 8X5XNBD 802.11n Low-Profile	412,50	825,00
2	1532 Series Pole-Mount Kit	372,00	744,00
2	Polo metalico de con base para montaje de AP externo	295,00	590,00
	ACCESS POINT PARA INTERIORES		-
28	802.11ac Ctrlr AP 4x4:3SS w/CleanAir; Int Ant; A Reg Domain	1495,00	41.860,00
28	Power Injector - AP-3600 Series w/ Modules-SPARE	149,00	4.172,00
28	SMARTNET 8X5XNBD 802.11ac Ctrlr AP 4x	247,50	6.930,00
			-
	INFRAESTRUCTURA DE CABLEADO PARA ACCESS POINT		-
30	Puntos de cableado estructurado cat-6A certificación (incluye material)	231,00	6.930,00
1	Servicio de Implementación y la solución Inalámbrica	2985,00	2.985,00
	Montaje de equipos, configuración de equipos, memoria técnica		-
	Pruebas de Funcionamiento, capacitación al personal.		-
		Subtotal	84.975,00
		IVA 12 %	10.197,00
		TOTAL	**95.172,00**

Garantia: 3 año contra defectos de fábrica mediante contratos SmarNet
Forma de Pago : 50% Anticipo y 50% contra entrega de los trabajos
Tiempo de Entrega: 60 Dias

Atentamente,

Esteban Vallejos
Gerente General