ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

INFORME DE PROYECTO DE GRADUACIÓN

"USO DE IPV6 PARA EL DESPLIEGUE DE UNA RED WISP"

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentado por:

JOSE ANTONIO FLORES BARZOLA

GUAYAQUIL – ECUADOR

2015

AGRADECIMIENTO

Agradezco a Dios primeramente por bendecirme para poder cumplir esta meta, a mi madre Irmita quien a lo largo de mi carrera ha velado por mí; siendo mi apoyo y a mis 2 hijos por ser mi fortaleza a cada instante. También quiero agradecer a mi familia por toda la ayuda y apoyo incondicional que me brindaron.

José Antonio Flores Barzola

DEDICATORIA

A Dios, por haberme guiado dándome las fuerzas para enfrentar los problemas que se me presentaron y para poder seguir adelante; a mi madre por darme su apoyo, y a los Ingenieros y tutores que con sus consejos, valores, hicieron posible que enfoque mi perseverancia para poder conseguir mis metas y darme los recursos didácticos necesarios para poder estudiar.

José Antonio Flores Barzola

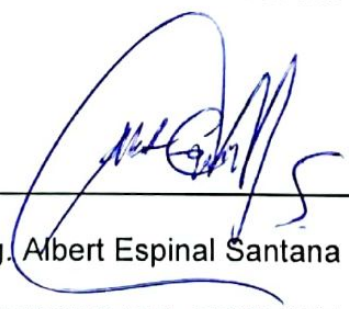
TRIBUNAL DE SUSTENTACIÓN

Dr. Sixto García Aguilar

SUBDECANO SUBROGANTE DE LA FIEC

Ing. José Patiño Sánchez

DIRECTOR DE PROYECTO DE GRADUACIÓN

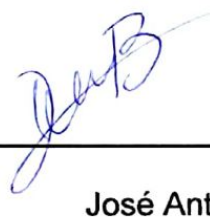


Ing. Albert Espinal Santana

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este proyecto de graduación, me corresponde exclusivamente; y el patrimonio intelectual del mismo a la Escuela Superior Politécnica del Litoral"



José Antonio Flores Barzola

RESUMEN

La presente documentación realiza un análisis e investigación sobre la nueva generación del Internet en base al protocolo IPV6, la cual nos ofrece una variedad de servicios entre uno de los cuales tenemos el despliegue WISP como lo analizaremos en este proyecto.

Cada día los proveedores de servicios de Internet se han visto obligados a realizar cambios para mejorar la transición del protocolo IPV4 a IPV6 en la red y ofrecer nuevos servicios tecnológicos con el fomento del nuevo protocolo.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Debido al aumento constante en los servicios y consumo de direcciones IP que brinda la entrada a Internet aparece un problema llamado “agotamiento de direcciones IP”, con gran demanda de conectividad de los usuarios y la masiva cantidad de dispositivos generados día a día; han obligado a los proveedores de Internet o ISP a realizar proyectos como el NAT o el proceso de subredes, pero llegando al límite surge la gran innovación tecnológica que nos abre las puertas a un universo de direcciones IP y de permisión al usuario para manejar más de una IP por dispositivo tanto así que el nuevo protocolo de IPV6 a diferencia de IPV4 nació con mejoras en su infraestructura y la calidad de sus servicios.

La implementación de las redes IPV6 no solo son del ámbito empresarial, lo cual es de gran importancia para las organizaciones o empresas que deseen migrar, también es para implementaciones de ámbito investigativo, educativo e incluso de carácter rural y recreativo puesto que el mantenimiento y administración de una infraestructura de red IPV6 puede llegar a ser autosustentable.

Desarrollé este proyecto conformado por cuatro capítulos, donde mostrare los requerimientos tecnológicos necesarios para implementar una infraestructura de red WISP IPV6 que brinda el servicio de internet conectado directamente con un ISP que brinde el servicio de IPV6 directamente funcional, al igual que se demuestra cuáles son las ventajas de este sistema y su funcionamiento.

CAPÍTULO 1

1.7 PRESENTACIÓN Y JUSTIFICACIÓN DEL PROYECTO.

1.1. ANTECEDENTES

Muchas instituciones educativas y empresas del sector público y privado desean implementar mecanismos de transición para sus migraciones de protocolo, buscan vías de comunicaciones rápida, bidireccionales y compatibles que se ajuste a sus necesidades , pero uno de los principales inconvenientes que se presentan en estas instituciones, es la correcta elección de los equipos y del software con los que se realizaría el levantamiento completo de la infraestructura de una red inalámbrica con protocolo IPV6, además de que tipo de

arquitectura usar ya que en los últimos años se ha venido usando para IPV4 pero con la aparición de IPV6 se abren un sin número de nuevas opciones y equipos que usarán medios inalámbricos para su conectividad.

Algunas parroquias y sectores urbanos han puesto de su parte para poder habilitar conexiones inalámbricas a costo de una pensión dividida para el número de usuarios que integren un comité o comitiva parroquial, pero los resultados no son satisfactorios.

En el ámbito empresarial se cuenta con márgenes de estudio, dedicación e inversión de estructuras nuevas como estas, obteniendo resultados convenientes.

Siendo un reto se busca la manera más segura y económica para crear un proyecto WISP con protocolo IPV6 y convergente con IPV4 para que beneficie una comunidad y pueda llevar la voz y levantar el proyecto en otras áreas aledañas.

1.2. DESCRIPCIÓN DEL PROBLEMA

Existen diferencias entre los protocolos IPV4 e IPv6, que sugieren mejoras en el desempeño de las redes de todo tipo de infraestructura para poder usar el nuevo protocolo. La descripción de una implementación del protocolo IPv6 en redes locales, rurales y de tipo móviles puede parecer algo complejo según el problema de conectividad en un parque con frondosos árboles, pero no imposible, comparándolo con la movilidad existencial que utiliza actualmente el protocolo IPV4 durante una transmisión de voz/datos y video en tiempo real, la cual es de mejor respuesta que hace unos 20 años atrás pero no hace rival ante el potenciado IPV6.

Ante el gran conocimiento o noticia del agotamiento de direcciones IPV4 se toma la decisión de incorporar a usuarios y clientes en la nueva era del IPV6 sacando así en buen uso de sus grandes habilidades como un protocolo joven y con espacio para la asignación de IP (s) a futuro tanto para usos investigativos, recreativos o educativos.

1.3. JUSTIFICACIÓN

Durante mucho tiempo y en la actualidad se ha usado IPV4, pero este protocolo tiene la limitante de agotamiento de direcciones. El aumento de uso de dispositivos móviles, obliga a buscar nuevas soluciones para la conectividad en la red, que sea escalable. Por lo tanto se ha considerado usar IPv6 en este proyecto y así dar a conocer los beneficios que se obtienen al implementar este protocolo.

1.4. DESCRIPCIÓN DEL PROYECTO

Considerado como uno de los sistema de direcciones más escalables y potentemente más amplio que el ya conocido en el mundo IPV4, utiliza un sistema de direcciones basado en 128 bits del estilo 2001:0db8:85a3:08d3:1319:8a2e:0370:CAFE, con lo que ya podemos tener infinidad de direcciones (2128 o 340 sex-trillones para ser exacto).

La principal ventaja de este nuevo sistema es, el aumento del número de direcciones disponibles, pero IPv6 tiene muchas ventajas adicionales que lo hacen aún más innovador. Con el nuevo sistema de empaquetamiento tenemos una mejora en el direccionamiento que nos posibilita crear redes mucho más

eficientes; también permite la autoconfiguración de direcciones gracias a mensajes entre los router e incluso podemos realizar muy eficientemente el multicast, que consiste en enviar un paquete a varios destinatarios. Bajo un entorno de áreas verdes lo que se considera a tratar en el proyecto como una zona explícita de un sector urbano recreativa donde los usuarios finales puedan conectarse vía WIFI o al puro estilo MESH, se plantea cambiar o en el mejor de los casos implementar una estructura innovadora de conectividad como lo es IPV6.

Al poder introducir en el ámbito urbano la tecnología del protocolo IPV6 se podrá realizar estudios de campo abierto sobre la reacción y aceptación del protocolo en los usuarios finales, considerando que se dará posibilidades investigativas para que los estudiantes que cursan semestres o cursos de desarrollo de aplicaciones tanto web como de actividades que involucren a IPV6, podrán tener un gran apoyo por el amplio direccionamiento que este da lugar y sin ningún costo más que lo correspondiente por el pago del ISP y de los equipos para cubrir el área a trabajar. Basados en proyectos paralelos de este enfoque para áreas verdes como parques o centros de distracción silvestre o zoológicos que trabajan bajo el control

poco sutil de IPV4 se plantea reestructurar ese enfoque a un plano más investigativo como lo es IPV6 e innovar para este proyecto concientizando a los usuarios aledaños y familiarizados con un comité urbano para que den luz verde a la culturización del nuevo protocolo y de sus posibilidades alcanzables y beneficiosas.

1.5. OBJETIVO GENERAL

Diseñar, implementar y gestionar una red IPV6 para la conectividad inalámbrica hacia internet en áreas verdes de un entorno urbano.

1.6. OBJETIVOS ESPECÍFICOS

- Diseñar y configurar el equipo a utilizar con protocolos de direcciones IPV6
- Analizar la Implementación de una red inalámbrica IPV6 que permite multiconectividad entre usuarios de un área urbana.
- Implementar un servidor que ayude con la petición de datos, páginas web y archivos, con control de carga.
- Realizar pruebas de la conectividad y su cobertura considerada con equipos de usuarios y sus diversos accesos.

- Análisis de las posible complicaciones que se presenten en la implementación de la red inalámbrica por punto de vista desde el rack hasta el área de cobertura mediante el uso de la herramienta Radio Mobile
- Medir la potencia de la señal conforme el cliente se mueve y encontrar las distancias donde se requiere un repetidor puente.

1.7. SOLUCION PROPUESTA

Según el problema, como solución se aplica en el proyecto la relación concreta que tiene el nuevo protocolo que se aplica en el campo establecido según este contexto experimental con fases de desarrollo y escalabilidades tecnológicas, hemos considerado como observación descriptiva a una solución propuesta nuestro plan de proyecto, que en su momento puede cambiar por las muestras captadas en el tiempo de desarrollar las pruebas en campo abierto; esto podría dar énfasis en los posibles problemas y soluciones de áreas o campos que podrían permitir mejorar el funcionamiento del mismo para el cliente /usuario final.

1.8. METODOLOGÍA

El estudio e implementación de la red inalámbrica en un medio urbano recreativo o áreas verdes comunitarias (parque) involucra el manejo de esquemas y factores que puedan favorecer o afectar el correcto funcionamiento de la red bajo el protocolo de IPV6.

Se ha considerado la elaboración de un esquema generalizado a factores que involucran el correcto funcionamiento de la red. Según este margen se realizará unas pruebas en campo abierto similar a lo investigado en el proyecto con particularidades que pueden en su mayor parte ser ampliadas, así la posibilidad de hacer útil el proyecto en un entorno verde dará un buen resultado investigativo.

1.9. RESULTADOS ESPERADOS

Se espera que en el transcurso de las pruebas en campo abierto según las metodologías escogidas y aplicadas el proyecto arroje resultados satisfactorios por las distintas pruebas con el uso del nuevo protocolo y las proximidades de los equipos a utilizarse, siendo así su aplicación real según lo

predeterminado como una tarea posible y exitosamente sustentable.

1.10. OBSERVACIONES

Según la metodología aplicada en el proyecto y la relación concreta que tiene en el nuevo protocolo aplicado en el campo establecido en este contexto experimental fases de desarrollo y escalabilidades tecnológicas. Si bien se considera como observación descriptiva nuestro plan de proyecto en su momento puede cambiar por las muestras captadas en el momento de desarrollar las pruebas en campo abierto; esto podría dar en su momento énfasis en los posibles problemas y soluciones de áreas o campos que podrían permitir mejorar el funcionamiento del mismo para el cliente o usuario final.

CAPÍTULO 2

2. MARCO TEÓRICO

2.1. REDES INALÁMBRICAS IPV6

Para entender lo que se plantea desarrollar con el proyecto en redes WISP con IPV6 entendamos primeramente que es una RED WISP y el Protocolo IPV6:

WIRELESS INTERNET SERVICE PROVIDER “WISP”, que en español se traduce a Proveedor de Servicio de Internet Inalámbrico. Pueden ser proveedores de servicios adicionales o de contenidos con infraestructuras WI-FI, WIMAX o HOTSPOTS.

Utilizando un modelo de despliegue en FENTOCELDAS [7] ha permitido crear una elevada densidad de cobertura sin necesidad de emplear instalaciones masivas de ADSL y puntos WIFI fijas para dar acceso a los usuarios de manera inalámbrica.

FEMTOCELDA, son puntos de acceso inalámbrico de baja potencia que combinan tecnologías móviles y de Internet dentro o fuera del hogar. Está considerada con la funcionalidad de una típica estación de base WIRELESS, pero en si amplía sus expectativas y da un despliegue de señal más sencillo y autónomo.

Una FEMTOCELDA es muy atractiva como una pequeña terminal que proporciona un gran poder de cobertura y estos al redirigir los servicios móviles a través de una red fija de banda ancha, da lugar a la vista de una próxima convergencia como alternativa de la tecnología fija móvil. Las FEMTOCELDAS no necesitan terminales duales a lo que es un punto a implementar no costoso según lo que se desee proyectar o dar su utilidad.

El proyecto WISP IPV6 está pensado para dar cobertura a muchas ideas como por ejemplo una de ellas podría ser su implementación usando FEMTOCELDAS y antenas de largo alcance. El proyecto

WISP IPV6 está pensado para dar cobertura a muchas ideas como por ejemplo una de ellas podría ser su implementación usando FEMTOCELDAS y antenas de largo alcance dicho ejemplo lo vemos en la Figura 2.1 a continuación [15].

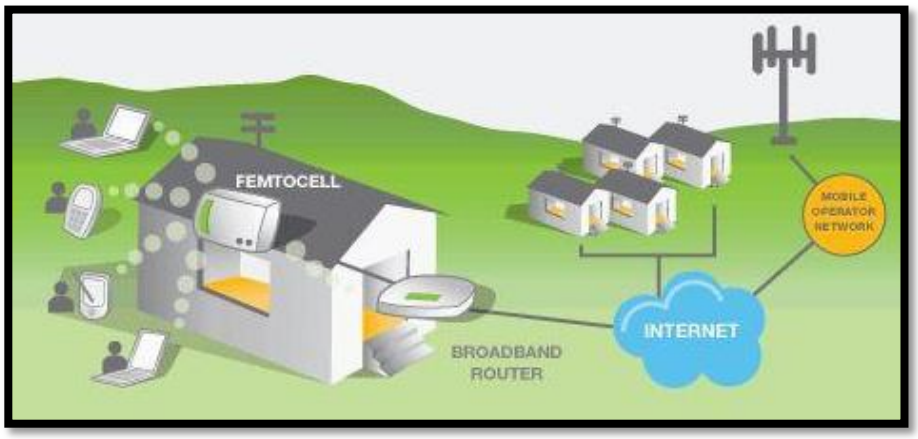


Figura 2.1 Análisis de la estructura de un diseño WISP con FEMTOCELDAS e IPV6 [15]

IPV6, ante el agotamiento de las ya conocidas IP`s de IPV4 y los múltiples cambios que se desarrollaron en su larga trayectoria por ser un protocolo no diseñado para el diario vivir y con mucho que desear en seguridad, se diseñó y pensó en muchas opciones alternativas para la creación del nuevo protocolo, a lo que se dio lugar al nacimiento de IPV6.

Con una gran variante en la estructura y funcionalidad de su cabecera y de su cuerpo en DATA IPV6 ha generado su nacimiento bajo las estrictas normas de calidad y seguridad (QoS para IPV6). Contando también con una escalabilidad ya mencionada en la descripción general y la eliminación de los paquetes broadcast y demás variantes contenedoras de IPV4, se ha dado una gran adaptabilidad en el campo WIRELESS protocolos auto configurables para su normal convergencia y migración.

Pero la denigración de muchos ataques de IPV4 al no ser posibles con IPV6 dará lugar sin duda a su profundo estudio e intentos de nuevas prácticas para evolucionar las amenazas antes ya conocidas en IPV4 para IPV6 aunque no es que se diga que no son posibles pero si tardarán en hacerlo dando lugar a una preparación de parte de los estudiantes e informáticos forenses; y como veremos en la figura 2.2 su trabajo es en conjunto con IPV4.

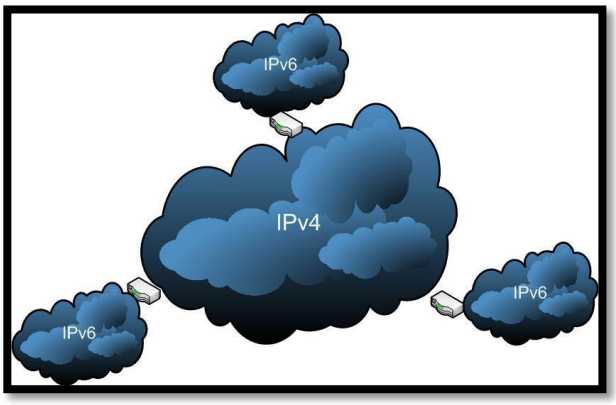


Figura 2.2 Entornos trabajando en conjunto IPV6 más IPV4

El nacimiento de IPV6 da lugar a una nueva era que es vital para su desarrollo.

2.1.1. Clasificación de las redes inalámbricas IPV6.

Las redes inalámbricas se caracterizan por su medio de transmisión usado para el intercambio de información entre dos o más estaciones de trabajo o centrales de transferencias de datos, intercambio dado por equipos como los nodos o las antenas y satélites mediante ondas electromagnéticas que viajan a través del aire. [2]

La figura 2.3 muestra la utilización necesaria de las redes inalámbricas con IPV6 para el avance tecnológico.

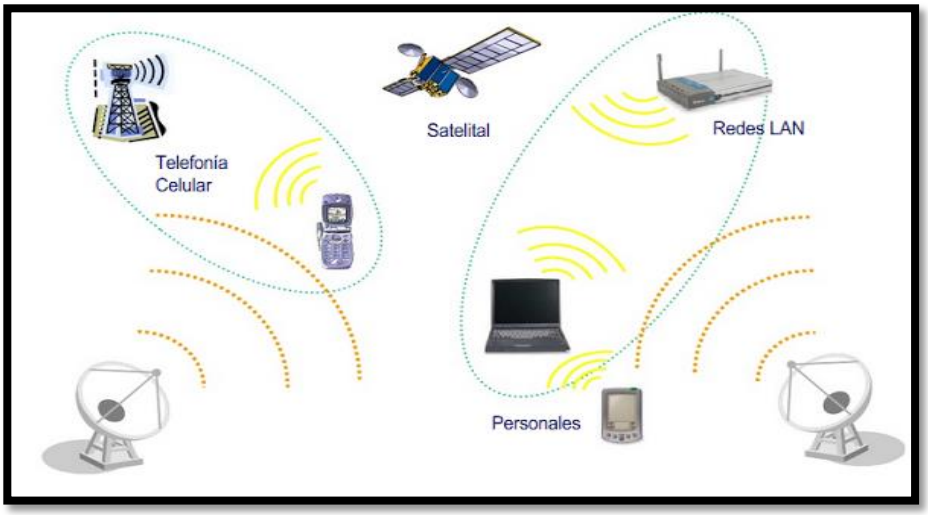


Figura 2.3 Uso de redes inalámbricas

Basándose en una clasificación de gran alcance tenemos las siguientes divisiones:

- Redes Inalámbricas Personales (PAN)
- Redes Inalámbricas Locales (WLAN)
- Redes Inalámbricas Metropolitanas (WMAN)
- Redes Inalámbricas Extendidas (WIDE AREA)
- Redes MESH.

Además de la clasificación de las redes inalámbricas [2] con aplicación en IPV6 tenemos algunos tipos de redes que

interactúan en los diferentes canales de transmisión a los cuales tenemos que considerar de manera nombrada para su conocimiento:

- Redes telefónicas:
    - 2ª generación: GSM.
    - 2.5 generación: GPRS, HSCSD.
    - 3ª, 4ª generación.
    - CDPD.
- Wireless Metropolitan Área Networks.
- IEEE 802.16.
- Satélites.
- Infrarrojos.
- Ultra Wideband (UWB).

a) Redes inalámbricas IPV6 (PAN)

Conexión netamente correspondiente a las Redes desarrolladas con dispositivos personales cuyo ámbito específico de aplicaciones es la conexión entre computadores, agendas, celulares, impresoras y demás artículos de ámbito personal.

Esta red originaria para IPV4 sufre un cambio en IPV6 por el modo de la autoconfiguración y la seguridad brindada a manera automática por el protocolo, también permitiendo la expansión de las IPs y dando lugar a la expansión y crecimiento del mismo sistema de red para acoplarse a nuevas estrategias comunicativas y dispositivos inalámbricos con sus correspondientes aplicaciones.

Soportada a una distancia no mayor de los 30 metros en entorno de oficinas, laboratorios y viviendas, se sujetan a estándares muy comprensibles ante su función:

- C (IrDA)
- Bluetooth
- IEEE 802.15 (unión con 802.11 en Bluetooth)
- Home RF (vivienda)

La red PAN (Personal Área Network) en conjunto al nuevo protocolo IPV6 se verá sometida a un marco gobernador para esta fijación en aplicaciones y servicios correspondientes al estándar IEEE 802.15 el

que maneja un cuerpo de estudios para su desarrollo y crecimiento evolutivo fijado para este tipo de conexiones.

Fijando metas en el mercado al estar familiarizados con uno de los estándares más comunes y útiles conocido como el poderoso Bluetooth [4] que fue originalmente diseñado por la empresa ERICSSON por el año de 1988 dio origen y permiso a la explotación de las redes PAN y ahora con IPV6 se desarrollara mucho mejor al manejar de una manera autónoma y creciente la globalización de diferentes utilidades en el intercambio de datos.

Equipos conectados por este medio usando radiofrecuencias que facilitan la comunicación entre equipos móviles y fijos con creaciones de redes inalámbricas sencillas entre ellas son usados para pequeños aplicativos y controles sensoriales de bajo alcance en hogares y oficinas. Los estudios demuestra que Bluetooth será capaz de dirigir por cuenta propia el tráfico IPV6 convirtiendo a futuro no tan distante y

palpable en una red compatible con internet a lo largo de las líneas de conexión WIFI (según SIG) ya que Bluetooth está destinado a conectar de manera autónoma muchos mecanismos de baja potencia dentro de la red PAN como los nodos de un sensor de red de equipos de cómputo o de monitoreo de clima y/o salud.

Característica perteneciente a la lógica de control de enlace Bluetooth y protocolo de adaptación (L2CAP) donde gracias a la flexibilidad de un intervalo de transferencias de datos de manera masiva se automatizara su reconexión de manera automática sin intervención del usuario cualquier tipo de conexión donde se haya detenido la negociación y retomada después, ayuda propuesta por parte de este estándar unido a IPV6.

Las redes de luz Infrarroja [5] están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso.

El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70´s, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de redes, se utiliza un "transreceptor" que envía un haz de luz infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente.

Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "transceptor infrarrojo". Los primeros transceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transceptor recibía la señal; Existen 3 Tipos: Punto a punto, Casi difuso y Difuso.

Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transceptor. Además la tecnología se ha mejorado utilizando un transceptor que difunde el haz en todo el cuarto a manera de Broadcast y es recogido mediante otros transceptores. La limitante de transferencia de datos está sujeta al alcance de los haces de luz dentro de una habitación a diferencia del Bluetooth pero le supera en potencia a lo que se estima un soporte de transferencia de datos muy robusto para un futuro.

El grupo de trabajo de red inalámbrica IEEE 802.11 está trabajando en una capa estándar MAC para redes infrarrojas compatibles y operables con IPV6 para la evolución y desarrollo de más tecnología.

b) Redes inalámbricas locales (WLAN)

Red LAN definida inalámbricamente en un área de alcance limitado como en un hogar, piso de edificio o estación de trabajo; sujeta al estándar IEEE 802.11 que establece una diversa serie de mecanismos y protocolos que da lugar a la diferenciación esquemática

de transmisión y modulación de señal para lograr mejores velocidades y rendimientos.

También conocida como la zona Wi-Fi en algunas entidades comerciales o laborales da un alcance en el mejor de sus casos de hasta 100-400 metros, siendo por vía aérea, conserva algunas similitudes de las redes LAN inalámbricas como la velocidad, alcance y soporte por número de nodos con la diferencia aplicada por su número en red (nodos), el roaming y el movimiento del punto de red.

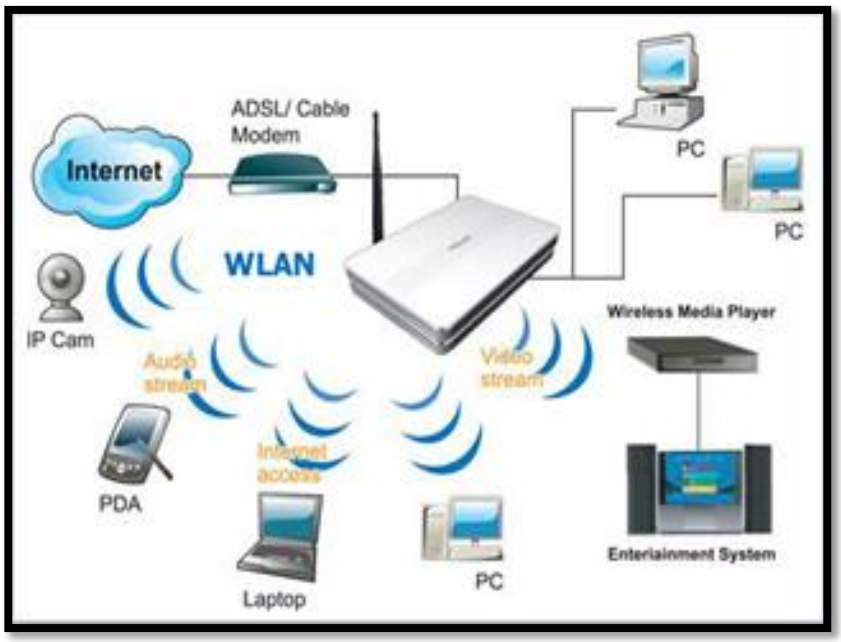


Figura 2.4 Convergencia de dispositivos móviles en la wlan según estándares IEEE y WECA

La figura 2.4 muestra un ejemplo de como las redes WLAN con IPV6 favorecen a los usuarios permitiendo disponer de muchas IP para su manejo. Gracias a los avances en la industria con la certificación y globalización de los mecanismos de operatividad inalámbrica según el estándar asignado por la IEEE 802.11 y la agrupación de la WECA (la Wireless Ethernet Compatibility Alliance) que da el "Wireless Fidelity" en sus abreviaturas WIFI.

Podemos dar como un punto a discutir la utilización de un esquema ideológico en la proyección de un proyecto WISP con asignaciones de protocolos IPV6 a mejorar y potencializar el esquema existencial de WLAN bajo el protocolo de IPV4 en un mejor esquema y con las utilizaciones alcanzables permitidas por el protocolo IPV6 por la rugosidad de sus esquemas automatizados y manuales designados.

c) Redes inalámbricas metropolitanas (WMAN)

Red WMAN como su nombre lo dice "red de área metropolitana" llega a ser la solución de acceso

inalámbrico de banda ancha (BWA- Broadband Wireless Access) con operatividad en ambientes tanto urbanos como rurales.

Considerando a mencionar 3 tipos de red WMAN a:

- IEEE 802.16 WIMAX
- ETSI HIPERMAN
- LDMS Local Multipoint Distribution Service

La aplicación de estas redes con la implementación del nuevo protocolo ya es un hecho en países de la vanguardia, donde gracias a la gran facilidad de direccionamiento y de la maniobrabilidad de la cabecera y del cuerpo IPV6 permite a manera metropolitana satisfacer muchas de las grandes demandas en el ámbito sensorial, educativo, comercial, aplicativo e investigativo.

La figura 2.5 muestra en ejemplo la red inalámbrica metropolitana y sus múltiples favores empresariales de la mano con IPV6 y fibra óptica [31].

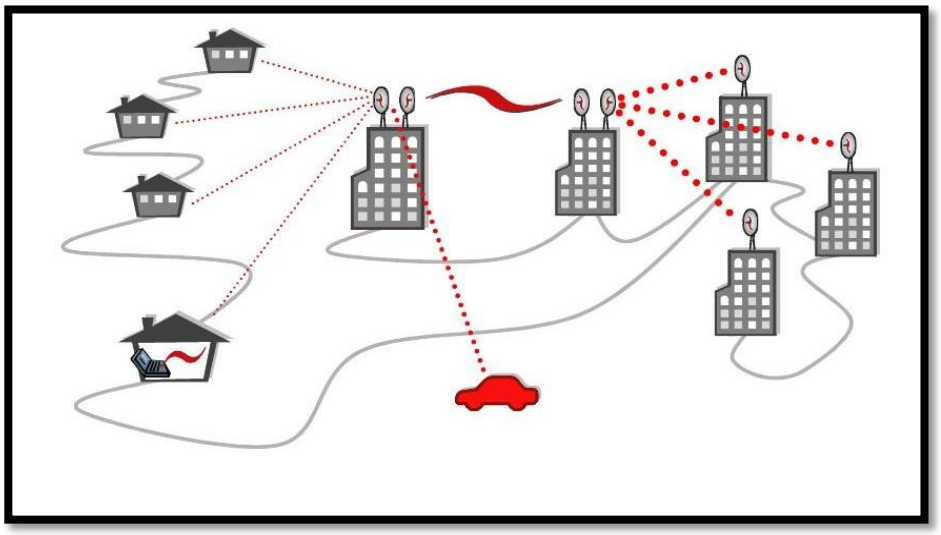


Figura 2.5 Red Metropolitana IPV6

d) Redes inalámbricas extendidas (WIDE AREA)

Conocida originalmente como las redes de la conectividad celular y/o satelital, que pueden abarcar cientos de kilómetros según donde se provee el servicio generalizado por la corporación celular, privada o pública contratada dan a conocerse con una gran propuesta evolutiva que en conjunto con el protocolo IPV6 ha generado muchos avances importantes y con la generación de una red de telecomunicaciones auto complementaria y evolutiva en tecnología.

Wide Área más conocida como las redes de celulares y satelitales permite según el surgimiento de muchos

estándares y servicios que las redes WISP sean un tipo de redes muy convergentes al punto de aprovechar sus múltiples beneficios para la interconexión entre usuarios finales.

Para esta tecnología tenemos los famosos: 1G no estandarizado, GSM (2g), TDMA, GPRS y UMTS (3g) y el 4G. En la figura 2.6 se muestra el ejemplo de la extensión de los diferentes tipos de redes inalámbricas existentes a lo que se aprecia de una mejor forma para quienes están pensadas esas redes una rápida evolución por el nuevo Ipv6.

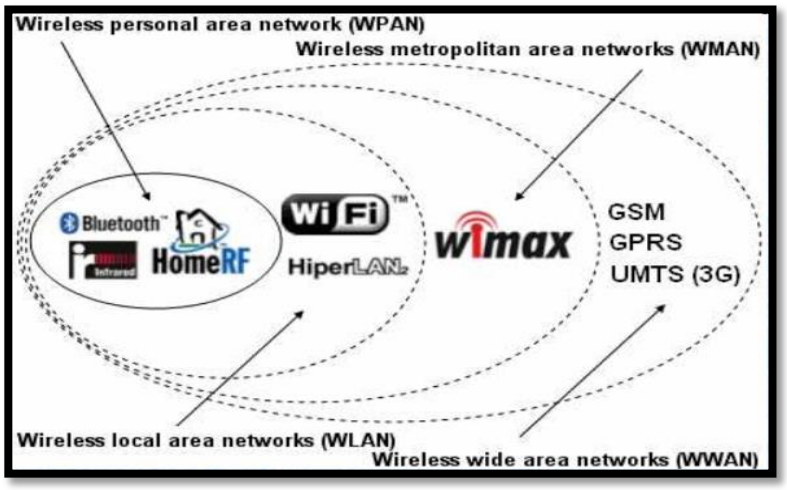


Figura 2.6 Divisiones de las redes inalámbricas

e) Redes MESH

Una red MESH [3] o Red Enmallada es una estructura formada por múltiples nodos y puntos de acceso a red "AP" que permite que dispositivos ajenos a la red puedan conectarse a la misma por medio de otros dispositivos que sí lo están.

Los usuarios pueden interconectarse entre sí, muy independiente de los AP presentes ya que un cliente nodo de la red MESH permite el paso de paquetes por medio de él hacia otros nodos; es decir la red MESH es autosustentable y creciente por si sola a disponibilidad de los usuarios.

Gracias al Protocolo IPV6 y a los diferentes proyectos tecnológicos las redes MESH han crecido mucho pero analizando este punto podemos ver cuáles son sus ventajas y desventajas:

Ventajas

- Transparencia entre protocolos (IPV4 - IPV6).
- Menor costo.

- Robustez.
- Facilidad de instalación.
- Alimentación.

Desventajas

- Latencia.
- Compartición del medio.
- Seguridad.
- Rendimiento.

Extendiendo su uso a muchos grupos abiertos como comunidades, comerciales y laboratorios. A continuación en la figura 2.7 se muestra un ejemplo del alcance y adaptabilidad de una red MESH a lo que se dan mejoras con la aplicación del protocolo IPV6.

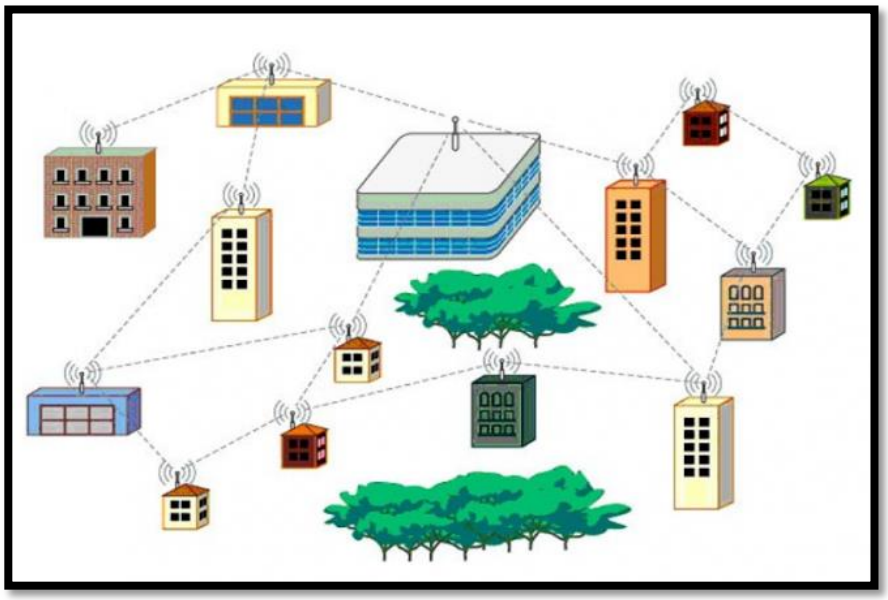


Figura 2.7 Red enmallada aplicada en una urbanización industrial y comercial.

2.1.2. Redes MESH y Protocolo IPV6

Una red MESH [6] apuntando al nuevo protocolo de direccionamiento IPV6 da una gran ventaja a diferencia de otras redes aplicadas, permiten que las tarjetas de red se comuniquen entre sí, independientemente del AP, dando lugar a que los dispositivos que actúan como puntos de red (tarjetas de red) pueden no mandar directamente sus paquetes al AP fijados sino que pueden pasarlos a otras tarjetas de red (usuarios móviles) para que lleguen a su destino.

Para cumplir esta meta es necesario contar con un protocolo de enrutamiento que permita transmitir la información hasta su

destino con el mínimo número de saltos posibles (Hops) o con un número que aun no siendo el mínimo sea suficientemente estable. La red Malla [8] es resistente a fallos, pues el colapso de varios o de un solo nodo no implica la caída de todo el sistema de la red.

Las redes MESH permiten cumplir con metas a los usuarios emprendedores gracias a los diferentes aplicativos que podrían escalar con IPV6 en su entorno empresarial, la figura 2.8 muestra un ejemplo gráfico de lo propuesto.

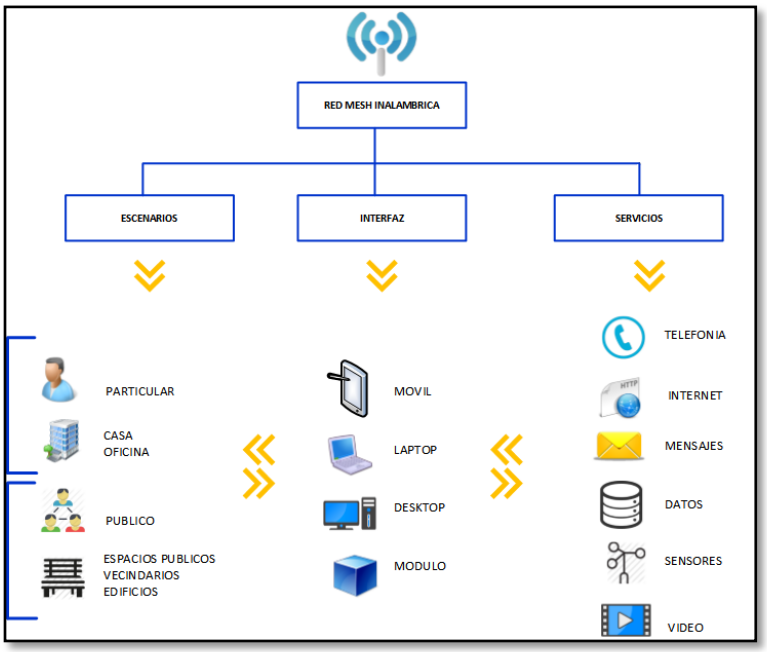


Figura 2.8 Estructura evolutiva MESH IPV6

El protocolo IPV6 mediante la proyección de un servidor DHCPv6 en una de las FEMTOCELDAS dará a lugar un juego muy importante en la aplicación de la malla con el nuevo protocolo, ya que la automatización del mismo protocolo con su servidor de direccionamiento automático hará posible que dispositivos dentro y fuera del área de la MESH que requieran participación obtendrán una dirección IPV6 con la que podrán evitarse las direcciones duplicadas y los conflictos de red.

Los usuarios no ajenos a la red dispondrán de una IP de 128 bits para sus dispositivos sean móviles o fijos dentro del desarrollo del proyecto WISP ya que con la disponibilidad de las FEMTOCELDAS en más de un área se podrá ejecutar una negociación muy agradable según donde se aplicará la idea.

2.1.3. Algoritmos de generación de seguridad IP

Aplicación de algoritmos y datagramas, el encabezado de autenticación nos brinda un mecanismo que le permite al destinatario de un datagrama asegurarse de la identidad de la fuente a lo cual el uso de cifrado de datos para el datagrama que vendría a ser su carga útil, refuerza su seguridad; sólo el verdadero destinatario puede leerlo; a menos de que sea

intervenido por un usuario de sombrero negro especializado en violar la seguridad autónoma de IPV6. Tenemos algunos algoritmos de generación de seguridad conocidos y aplicados para IPV4/IPV6, de los cuales se dará una ligera mención para no entrar a detalles de calculación criptográficas complejas:

- MD5.
- SHA-1.
- RIPEMD-160.

En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado mediante 4 pasos [18].

SHA-(1-3), diseñado por la agencia de seguridad nacional estadounidense, ha entrado en competencias de HASH para lo cual la última versión conocida SHA-3 es la que más difiere y la que menos habilidades algorítmicas matemáticas contiene, pero los algoritmos de seguridad que robustecen los protocolos de IPV4 e IPV6 siempre son sometidos a ataques para encontrar debilidades continuas [20].

RIPEMD-160, diseñado por la comunidad académica, siendo este algoritmo el resumen de mensajes de 160 bits y función criptográfica de hash como una versión MEJORADA de RIPEMD basados sobre los principios de diseño de MD4 y similar en seguridad y funcionamiento al popularizado SHA-1.

La definición de Cálculos de Campos IPV6, hace mención a la diferenciación de los campos estructurales según sus funciones y longitudes (calculadas) de la evolución de IPV4 a IPV6 de lo cual se analizará la diferenciación entre los dos protocolos y el porqué de la importancia tanto para la seguridad del protocolo IPV6 como para su estabilidad y mejora en desempeño [21].

2.1.4. Diferencia de campos IPV4 Vs IPV6.

Considerando el HEADER del protocolo anterior IPV4 con su base de 32 bits se ha dado a conocer la gran ventaja que le lleva este nuevo protocolo ya implementado en algunas empresas mundiales, al igual que industrias transnacionales y compañías del sector público y privado con exitosas respuestas.

IPV6 da grandes respuestas ante esta serie de exigencias que antes IPV4 no podía satisfacer y con el gran aumento de números ID (Direcciones IP) de 128 bits tenemos grandes escalabilidades hacia las aplicaciones y equipos del futuro.

Consideremos las diferencias con la comparativa tomadas de las Gráficas y argumentos de la Página de LACNIC. A continuación en la figura 2.9 y 2.10 se muestran las diferencias entre la cabecera IPv4 e IPV6 [22].

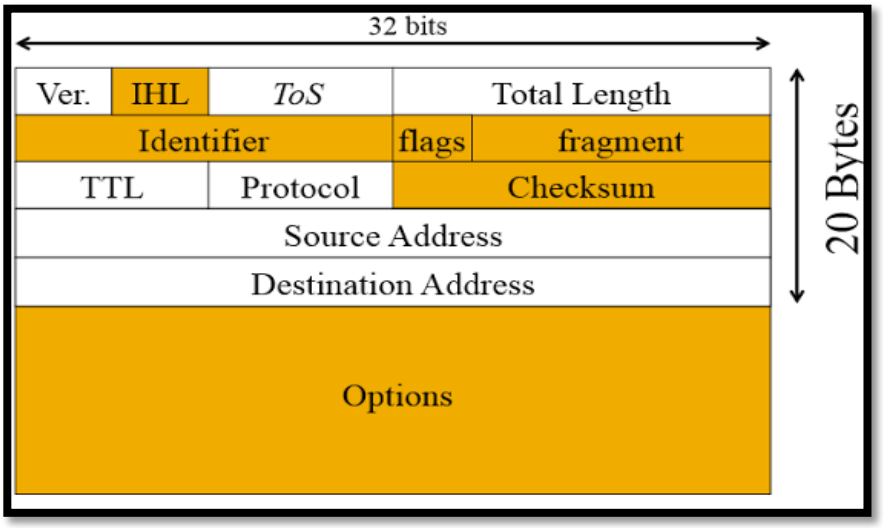


Figura 2.9 Cabecera IPv4

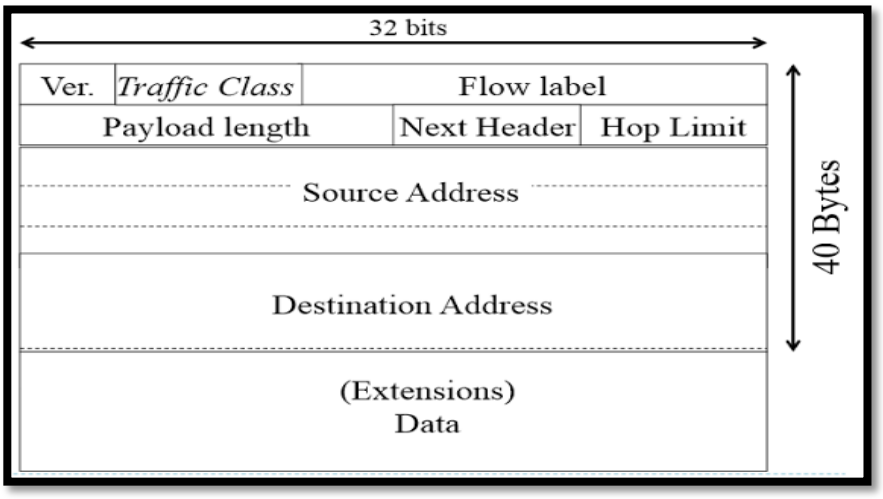


Figura 2.10 Cabecera IPV6

Considerando las gráficas a diferenciar entre los 2 Tipos de HEADER tanto del IPV4 como del IPV6 se trae a relucir 2 tipos de diferencias y un ADDRESSING considerados:

a) Extensiones Opcionales (1)

1.- Nuevo mecanismo que reemplaza IPv4 options.

2.- Una extensión IPV6:

- Cada extensión tiene su propio formato

- Es una n x 8 datagrama

- Empieza con campo de 1 byte 'Next Header' y que apunta a otra extensión a un protocolo de capa 4

3. - Hop-by-hop (jumbo Gram, Router alert)

-Siempre la primera extensión

- Analizado por cada Router

b) Extensiones Opcionales (2)

1.- Destination

2.- Routing (lose source routing)

3.- Fragmentation

4.- Security

- Authentication (AH)

- Encapsulating Security Payload (ESP): confidentiality

Para el direccionamiento notamos que IPV6 usa direcciones de 128 bits (recordando lo anteriormente dicho) y conserva similitudes con IPV4 en este punto como:

- Las direcciones pueden ser agregadas en un prefijo para simplificar el ruteo
- Se definirán diferentes tipos de direcciones como:
  a) UNICAST
  b) ANYCAST y
  c) MULTICAST.
- Las direcciones pueden manifestarse por alcances de tipo:
  a) Link-Local o

b) Globales

Por último se da por entendido que con el protocolo de IPV6 un host puede usar direcciones de diferentes tipos y alcances al mismo tiempo.

2.2. MECANISMO DE TRANSICIÓN CON IPV6

La transición de IPV4 a IPV6 es algo que se vio de antemano por equipos migratorios del protocolo a lo que se tomó la gradualidad de su desarrollo en planta por su estado de complejidad en el momento de ejecutarlo [10]. La coexistencia de IPV4 con IPV6 no será algo que terminará pronto, es más se fija una coexistencia mutua entre protocolos por un muy largo y prolongado tiempo por la dificultad de suspender servicios online en el momento de desarrollarlo.

Los mecanismos de transición propuestos por algunos de los operadores de internet (ISP), no será muy factibles sin antes una adquisición de equipos robustos que soportan el sistema de cálculos de 128 bits que exige el protocolo a diferencia del anterior que solo trabajaba con 32 bits y su sistema de cálculos era lo suficientemente soportable para tal sistema de procesamiento de paquetes [17].

En conjunto con los Servicios de Nombres (DNS) el trabajo de los equipos anteriores estará sujeto a muchas variantes puesto que no fueron diseñados para soportar tal cantidad de procesos, a lo que se considera una actualización paulatina de equipos de manera gradual para la interoperabilidad del protocolo hacia el cliente.

Para la habilitación de nodos de comunicación mutua tanto para IPV6 como para IPV4 según la funcionalidad transparente sea para transferencia de datos o transición se debe mejorar la comunicación aplicando mecanismos que empleen traducciones a nivel de la red cuando sea necesario (pero en el mejor de los casos es mejor evitar esto) o incluso mediante asignaciones definidas a corto tiempo de direcciones IPV4 que se involucraron dentro con las de IPV6 [24].

Considerando que IPV4 contiene configuraciones que netamente trabajan bajo la capa de red o incluso con información proveniente de la capa aplicativa como es el caso del FTP.

La propuesta de la comunicación entre nodos requiere el trabajo de ambas PILAS de los Protocolos de red conocidos como Dual Stack a lo que se considera lo siguiente:

- Evadir túneles, ya que los Routers no necesitan direcciones IPV4 sino DUAL STACK.
- Evadir traducciones, siempre que se considere el uso de aplicaciones con soporte IPV44 e IPV6.

Un estudio desarrollado por la Universidad Católica de Santiago de Guayaquil en febrero del 2013 sobre la transición a desarrollarse en Ecuador para el paso de IPV4 a IPV6 y su coexistencia en comunicación entre los 2 protocolos manifiesta que se debería considerar la elección de cualquiera de los mecanismos más comunes hasta la fecha conocidos.

Tipos de mecanismos para transición [1]

- Mecanismo DSTM.
- Mecanismo SIIT.
- Mecanismo BIS.
- Mecanismo TRT.
- Mecanismo Socks 64
- Mecanismo BIA.

a) Mecanismo DSTM.

Significa Dual Stack Transition Mechanism, cuya función es la de permitir a los nodos Dual Stack comunicarse con otras aplicaciones de solo uso IPV4; aunque la pila de IPV4 se encuentre habilitada se considera su configuración para la comunicación exitosa. Para ello un nodo IPV4 e IPV6 necesitarán direcciones IPV4 lo cual es solicitado al servidor DSTM manteniendo la comunicación entre el nodo y el servidor DSTM netamente por IPV6 [23].

A falta de encapsulamiento de IPV4 en las redes IPV6, el Equipo Dual Stack encapsula paquetes IPV4 dentro de paquetes IPV6 hasta el extremo del túnel, el mismo que será desencapsulado y enviado a la infraestructura IPV4 que mantenga la comunicación en vivo. El encapsulamiento se lo realiza virtualmente para lo cual se define una arquitectura en la DSTM donde:

a) Servidor DSTM se encargará de asignar direcciones IPV4 a los clientes que aún lo soliciten.

b) Router DSTM se encargara de realizar la encapsulación y el desencapsulamiento de los paquetes asegurando su envío.

c) Clientes DSTM capaces de configurar dinámicamente su pila IPV4 también podrán establecer túneles IPV4 sobre IPV6.

A continuación en la figura 2.11 se muestra un ejemplo del encapsulamiento realizado y definición de la arquitectura en la DSTM v4/v6 según servidores, routers y clientes.

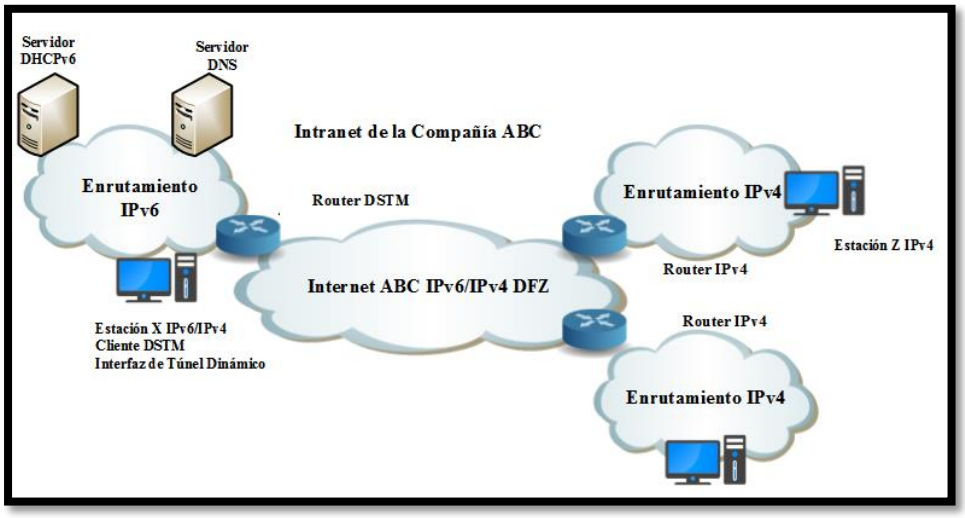


Figura 2.11 Encapsulamiento realizado y definición de Arquitectura en la DSTM v4/v6

En la figura 2.12 analizaremos como un equipo al entrar en contacto inmediato con él una dirección IPV4 temporal que trabaja en conjunto con su dirección IPV6 y se aplica el TEP (Tunnel End Point). El encapsulamiento se produce cuando un el paquete IPV4 se introduce dentro del paquete IPV6 y queda

configurada la interfaz del túnel cliente origen. Como se mostrará en la imagen a continuación

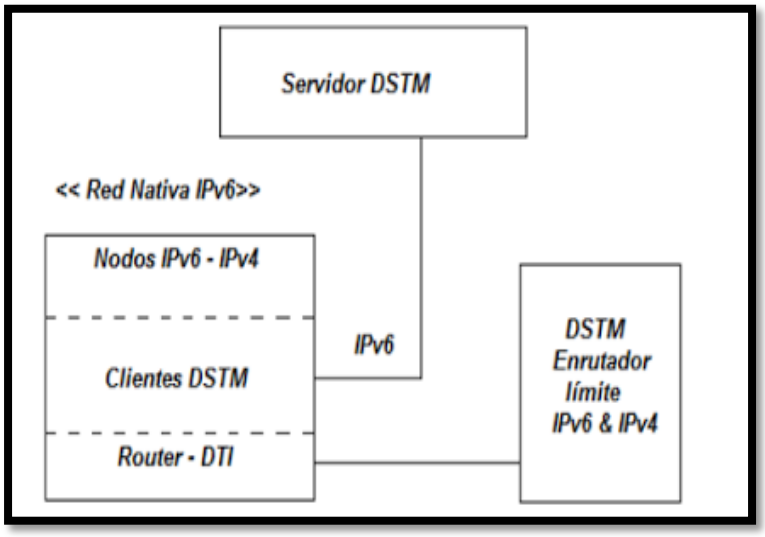


Figura 2.12 Encapsulamiento del paquete IPV4 introducido dentro del paquete IPV6

b) Mecanismo SIIT.

Stateless IP/ICMP Translation Algorithm (SIIT) encargado de traducir los paquetes a nivel de los nodos de red entre IPV4 e IPV6 donde se limitara a las cabeceras IP para cada paquete.

El Mecanismo SIIT emplea Direcciones IPV6 y direcciones IPV4 traducidas haciendo uso de dos tipos de traducciones.

a) Direcciones IPV4 mapeadas del tipo <<::ffff.a.b.c.d>> que identifican una máquina IPV4

b) Direcciones IPV4 traducidas del tipo <<: ffff: 0:a.b.c.d>> que identifican una máquina IPV6.

Por ello el nodo IPV6 obtendrá direcciones temporales de IPV4 que servirá como enrutamiento para los paquetes, a lo que se adjunta 3 tipos de direcciones:

- IPV4.
- IPV4-Traducidas
- IPV4-Mapeadas

Permitiendo la comunicaciones entre host IPV6 e IPV4. A continuación una muestra de cada caso

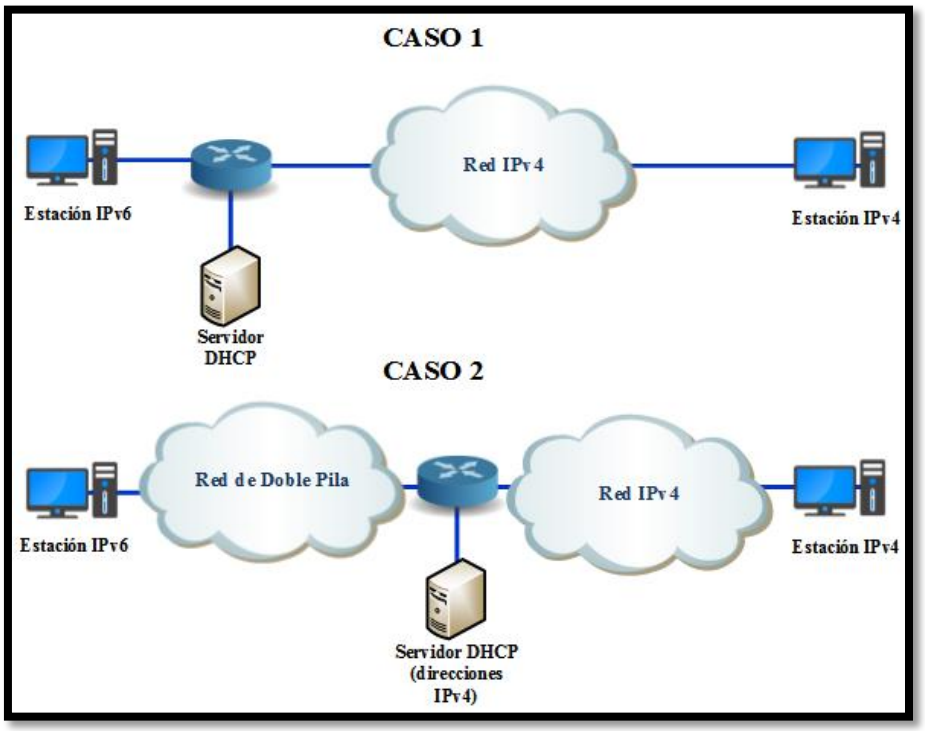


Figura 2.13 El Mecanismo SIIT emplea Direcciones IPV6 y direcciones IPV4 traducidas en 2 casos

En el caso 1 se demuestra la comunicación enrutada del SIIT tanto para redes IPV6 e IPV4 (RED PEQUEÑA). En el caso 2 se relata el método SIIT para sitios que tienen únicamente IPV6 en una red DUAL STACK.

La configuración destinada para los ordenadores que no usen la traducción SIIT debe de modificar aspectos para la implementación completa de IPV6 y con ello garantizaremos:

a) Transmisión y Recepción de paquetes IPV6 con direcciones Mapeadas IPV4.

b) Determinar si las Direcciones IPV4 traducidas deben ser Refrescadas o Asignadas.

c) la Utilización de comunicación entre paquetes IPV4 traducidas y mapeadas sea solo en conjunto [19].

c) Mecanismo BIS.

BIS (Bump In The Stack) permiten al host Dual Stack comunicarse con host IPV6 utilizando aplicaciones IPV4, ya que su utilidad se sujeta muy en lo particular a sistemas donde las aplicaciones aún no han migrado de IPV4 a IPV6 por carencia del código fuente.

Cuando las aplicaciones buscan comunicarse con mecanismos IPV6 siendo estas configuradas desde la fuente con el protocolo IPV4 y sus correspondientes estándares entran en acción el mecanismo BISS que realiza el mapeo entre una dirección IPV6 y una IPV4 para desarrollar su comunicación satisfactoria.

Con esto en mente sobre la traducción de aplicaciones de uso de IPV4 y redes en un alcance no superior a IPV6. El diseño de Stack consta de una pila Dual Stack en el cual se añadirá 3 módulos:

a) Un traductor.

b) un nombre de extensión de la resolución.

c) la dirección del mapeo.

El mecanismo BIS permite que ciertos HOST se conviertan en traductores autónomos para lo cual ya no será necesario un traductor externo.

BIS, ubicado en el área de seguridad del protocolo de IP y verificando datos que pasan por TCP/IPV4 e interface de RED realiza traducciones de IPV4 a IPV6 y viceversa. Negándose la comunicación de IPV6 a IPV4 por parte del mecanismo BIS o

de IPV4 a IPV4 a falta de traductor aplicativo en el medio, este dará error de conectividad en algún lugar de la ruta de comunicación.

Al igual que los mecanismos NAT-PT, SIIT y BPI este no puede funcionar con mecanismos Multicast, ni para aplicaciones que incorporen direcciones IP en sus cargas.

Se recomienda solo en estos casos una ALG (Application Layer Gateway). Analizando todo esto con un gráfico tenemos el siguiente ejemplo según figura 2.14.

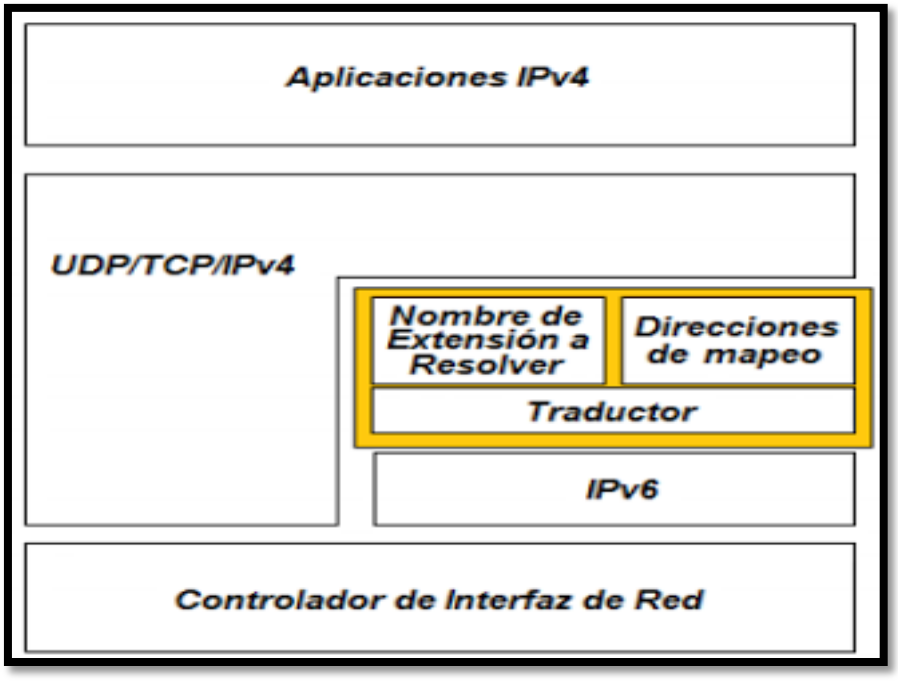


Figura 2.14 Pila Dual Stack con 3 módulos

d) Mecanismo TRT.

Transport Relay Translator (TRT) este mecanismo establece que los host IPV6 realizan un intercambio TCP/UDP con host IPV4 ósea da una comunicación directa entre aplicaciones IPV4 e IPV6 a diferencia de los mecanismos anteriores este actúa a nivel de la capa de transporte y a diferencia del BIS actúa como un canal alterno entre los 2 protocolos estableciendo una conexión tanto para IPV4 y otra para IPV6 permitiendo el reenvío de paquetes entre ambas direcciones.

Al ser innecesaria la modificación de parte de cualquiera de los host el mecanismo TRT es realmente sencillo de proponer y ejecutar en las redes con capacidades IPV6. Al ser traductor y ejecutarse en un nodo “DUAL STACK” puede desarrollarse una conexión con un host cliente o servidor.

Siempre que se desarrolle una red IPV6 es necesario mantener los parámetros de acceso a recursos de parte de las redes IPV4 externas y para ello se emplea el TRT o mecanismo de pasarela de traducción a nivel de transporte.

Las redes IPV6 e IPV4 son configuradas de una manera que sus nodos tanto para IPV4 e IPV6 se manejan que sus paquetes sean enviados a direcciones donde estarán sometidas a prefijos de red remota para el TRT, como mostraremos a continuación en la figura 2.15.

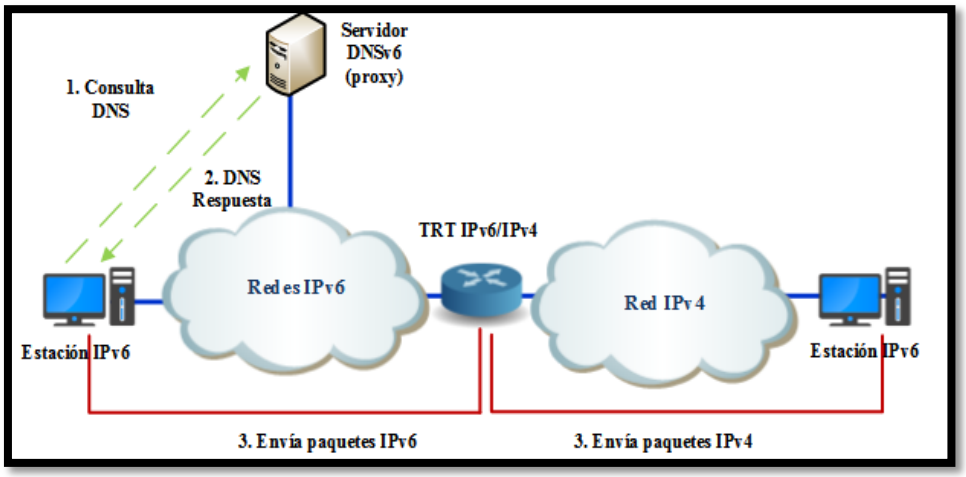


Figura 2.15 Mecanismo de pasarela de traducción a nivel de transporte

Una ventaja de TRT sobre otros mecanismo es que no tiene problemas de traducción de cabecera IPV4/IPV6 ni de fragmentación. Entre sus desventajas encontramos que soporta únicamente trafico bidireccional, requiere de un sistema de almacenamiento entre los nodos IPV4/IPV6 para la comunicación (parecido a NAT IPV4) y necesita de códigos especializados para las traducciones de protocolos

incompatibles con NAT y poder desarrollar el reenvío de los datos (NAT - UNFRIEND) así como mecanismo *Socks 64,* mecanismo cuya base es el PROXY SOCKS convencional, compuesto por una puerta de enlace implementado como un host de pila dual IPV4/IPV6 y un cliente de acogida cuyo software (Socks LIB) se desarrolla entre las capas de aplicación y de transporte .

Interceptando con esto las consultas de los DNS y respondiendo con falsas direcciones IPV4 a lo que el cliente proseguirá a hacer una llamada a la conexión API, donde LIB SOCKS sustituirá la dirección falsa original y envía el paquete al proxy para desarrollar la búsqueda del DNS propio. A continuación en la figura 2.16 veremos las conexiones interactuando

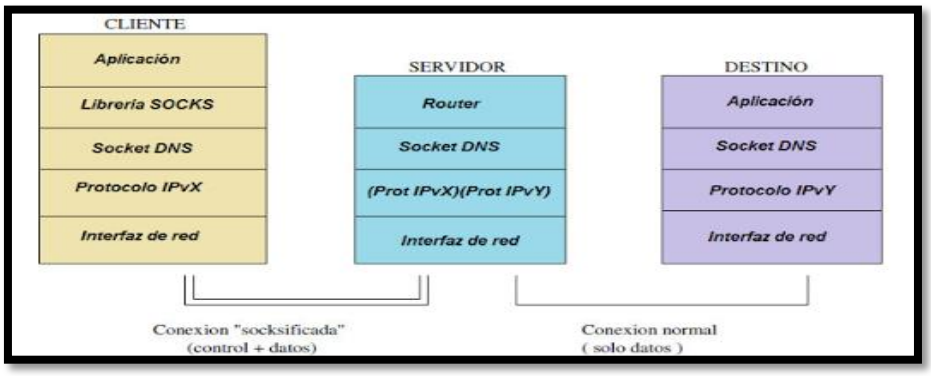


Figura 2.16 Interacción entre una consulta sofisticada y una normal

Si el Servidor DNS responde con un acuse de registro AAAA, el proxy abrirá un socket IPV6, no siendo así sólo abrirá un socket IPV4. Considerando esta solución como bidireccional lo que permite anfitriones host IPV4 e IPV6 para iniciar sesiones para lo que se necesita direcciones IPV4. Un ejemplo gráfico a continuación se muestra en la figura 2.17.

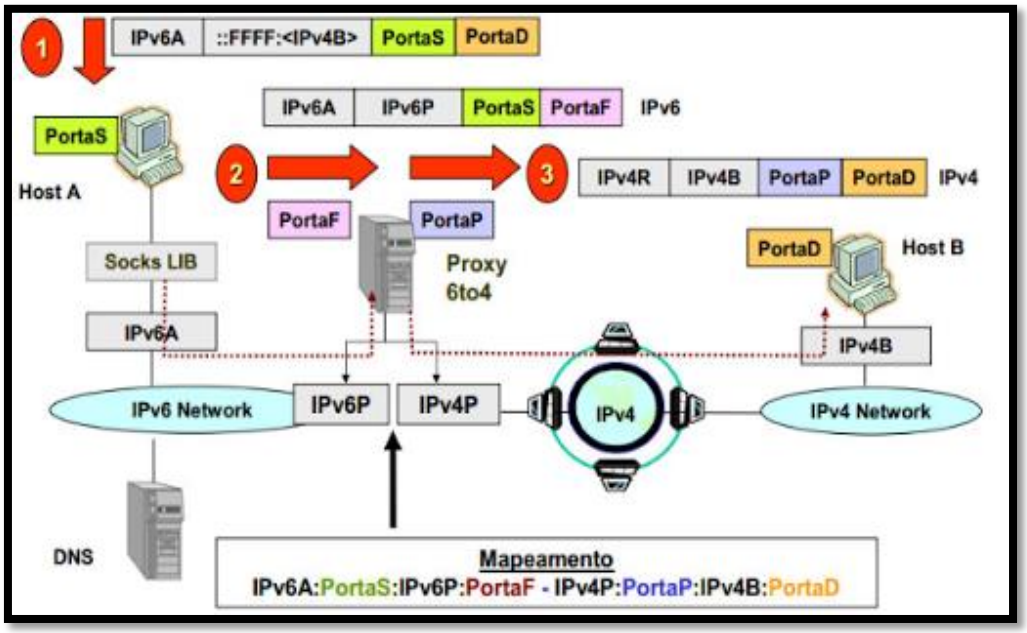


Figura 2.17 Solución Bidireccional que permite anfitriones host IPV4 e IPV6

Viéndose en la imagen la configuración del proxy, el mismo que se define como un mecanismo de reenvío de la capa de transporte permitiendo al host con una tabla de direcciones privadas y con acceso limitado a través del firewall le sea

concedido el acceso free a los recursos de internet. Teniendo a consecuencias de entender que por este método el proxy Socks para IPV4 se alojó comúnmente en una gran base DUAL un una dirección privada y otras públicas, recibiendo conexiones desde la interfaz IP a host internos privados y logrando así crear conexiones con servidores en internet por medio de una interfaz pública.

Esto se aplica de igual manera al desarrollarse el Proxy Socks 64 para IPV6 de manera dual con una IPV4 pública para redirigir el tráfico con las conexiones de interfaces IPV6 y viceversa.

e) Mecanismo BIA

Bump In The API (BIA) contiene similitudes al mecanismo BIS ya que este agrega una API de traducción entre el API de sockets y módulos de TCP/HOST IP con pila dual, permitiendo aplicaciones de comunicación con anfitriones IPV4 e IPV6, lo que refleja las funciones de la toma de socket IPV4 a IPV6 a IPV4. A continuación en la figura 2.18 se muestra un ejemplo.

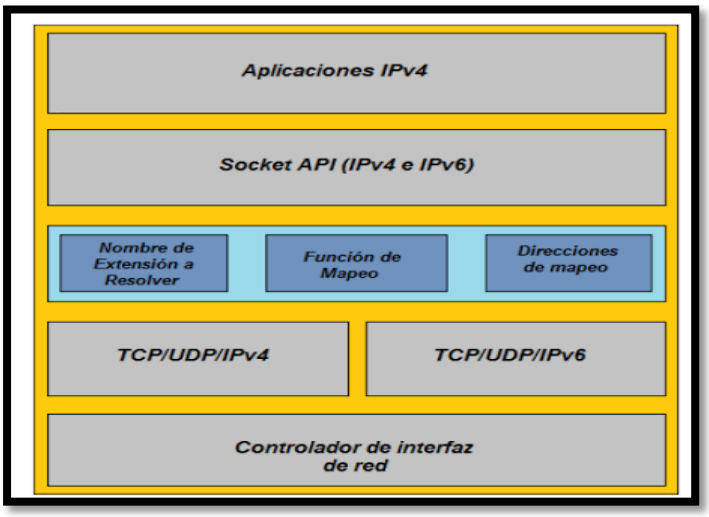


Figura 2.18 Detección de funciones del socket IPV4 e invoca las funciones correspondientes del socket IPV6 y Viceversa

Observando que las extensiones de resolución de nombres y las direcciones de mapeo funcionan de la misma manera que el BIS, estas detectarán las llamadas de las funciones del socket IPV4 e invoca las funciones correspondientes del socket IPV6 y viceversa.

BIA tiene ventajas en relación a BIS y es que no depende del controlador de interfaz de red y de no introducir una sobrecarga en la traducción de los encabezados de los paquetes. A pesar de esto sigue su incompatibilidad con la comunicación multicast.

Considerando todos estos mecanismos expuestos y en consideración que faltan como el 60% más de revisión de otros mecanismos declarados o en progreso de ser descubiertos se puede dar por sentado que el objetivo aplicativo de la transición de IPV4 a IPV6 es con el fin de migrar paulatinamente de IPV4 a IPV6, considerando que IPV4 está muy lejos de desaparecer la convivencia de los 2 protocolos se verá hasta el día que se note la superación de aplicaciones y equipos con bases de IPV6, a lo que IPV4 se verá ya opacado pero seguirá funcional.

CAPÍTULO 3

3. ANÁLISIS

3.1. ESTÁNDARES A CONSIDERAR EN IPV6

Existe una gran evolución de estándares IEEE 802.11 a nivel de plan que han ido desarrollándose en base al protocolo IPV4 y que ahora serán y están migrando a IPV6 [27].

Considerando por cultura general tenemos algunos de los estándares de redes inalámbricas:

- **IEEE 802.11** en RF e IR sobre ISM de 2.4GHz bajo el protocolo CSMA/CA.

- **IEEE 802.11a** Transmisión de 54 Mbps con velocidad de 20 Mbps en bandas de 5GHz.

- **IEEE 802.11b** puede variar de 1 a 5 y 11 Mbps en banda de 2.4 GHz y no es compatible con la IEEE 802.11a por su funcionamiento en distintas frecuencias.

- **IEEE 802.11e** estándar capaz de interactuar a nivel de la capa MAC con un elemento HCF con accesos EDCA y HCCA.

- **IEEE 802.11g** para conexiones Wireless con velocidad de 30 Mbps a frecuencia de 2.4GHz, compatible con 802.11b y con antenas parabólicas cubre distancias de 50 Km.

- **IEEE 802.11n** con una velocidad estimada de 600 Mbps superando a los estándares 802.11 (a, b y g) Y 802.11 AC; con una frecuencia real de 5GHz y permite usar la 2.4Ghz si está disponible el canal.

Para la consideración de un estándar apropiado para la implementación de IPV6 y de su antecesor IPV4 se considera el uso apropiado y bajo un estudio de pruebas por factor distancia

y velocidad con los equipos que permitan su implementación a 2 estándares como lo son:

- IEEE 802.11g
- IEEE 802.11m

A continuación en la figura 3.1 se observa un muestreo de rangos entre los estándares G y N [26].

Figura 3.1 Alcance de diferentes estándares [25]

Para la consideración de un estándar apropiado según la figura 3.1 para la implementación de IPV6 y de su antecesor IPV4 se considera el uso apropiado y bajo un estudio de pruebas por factor distancia y velocidad con los equipos que permitan su implementación a 2 estándares como lo son:

a) IEEE 802.11g

b) IEEE 802.11n.

3.1.1. Influencia por la doble pila en el uso de IPV6

En vista del uso del nuevo protocolo y la afectación ante el manejo de equipos antiguos, dando lugar a la asignación de nuevos equipos que soporten a IPV6 se considera los niveles de las capas OSI / TCP IP técnicamente como la doble pila, se ha manifestado un nivel de capa en particular que sufren una gran influencia en la manipulación directa por parte de ambos protocolos al momento de una transición y por parte de los nodos en el envío y recepción de paquetes. Ejemplos de la influencia de la doble pila en figuras 3.2 y 3.3 desde el punto de vista en modelos OSI IP v4/v6

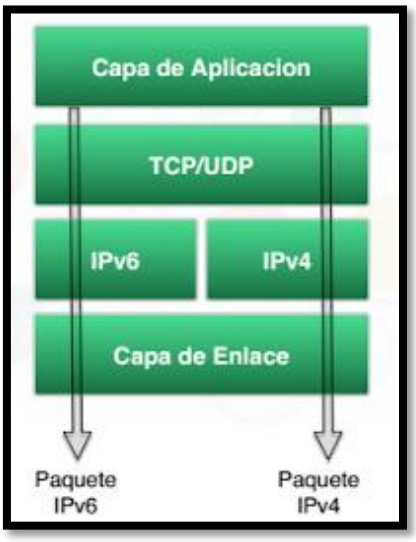


Figura 3.2 Estructura A análisis de doble pila según IPV4con nodos IPV6

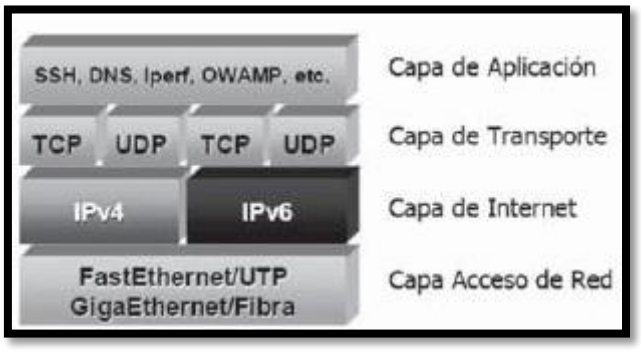


Figura 3.3 Estructura B análisis de doble pila según IPV6 con nodos IPv4

Doble Pila, conocida como una red de infraestructura capaz de encaminar ambos tipos de paquetes (IPV4 o IPV6).

Se consideran aspectos como:

- La configuración de los Servidores de DNS en IPV6.
- La Configuración de los Protocolos de Ruteo en IPV6.
- La Configuración de los Firewalls y su comportamiento y cambios sobre IPV6.
- Cambios en el Gerenciamiento de las REDES IPV6.

El Trabajo del Protocolo a nivel de capa 2, capa 3 y capa de aplicación estará influenciada por muchas operaciones de implementación donde aplicaciones y comunicaciones de transición se verán afectadas por factores que pueden dar soporte como tal a los trabajos de transición entre los dos protocolos y el modo de funcionamiento de IPV6.

De esta manera podremos analizar a detalle el trabajo de la doble pila a nivel de capa según los protocolos, un ejemplo se muestra en la figura 3.4.

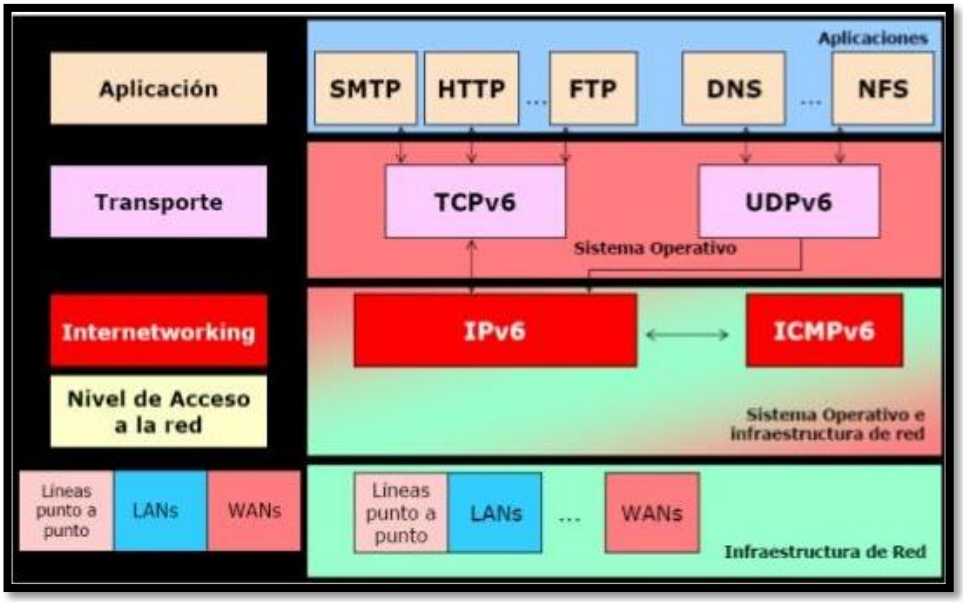


Figura 3.4 Trabajo de protocolos a niveles de capas

La influencia de IPV6 en las capas de los modelos de OSI y TCP IP se especializa en la calidad de servicios y la seguridad de los paquetes transportados y enviados en su mayoría.

3.1.2. Características presentes ante el protocolo IPV6

Considerando a IPV4 e IPV6 para el siguiente estudio de las características que se presentan delante del protocolo IPV6 y que en su mayoría algunas también son compatibles bajo ciertos criterios con el protocolo IPV4, se darán a mencionar dos puntos importantes respecto a las características presentes:

a) La autoconfiguración

Esto consiste en un conjunto de pasos donde un Host decide cómo configurar sus interfaces IPV6 (PLUG and PLAY). Con la creación de una dirección con un enlace local se analiza que no haya duplicados de direcciones o del enlace mismo y de determinar la información a utilizarse, ya que las direcciones al ser obtenidas mediante un DHCPv6 se generará según el protocolo,

múltiples direcciones de enlaces locales, direcciones globales y de SITIO.

Considerando esta opción tenemos 2 tipos de auto-configuraciones definidas por el protocolo:

- **Stateless,** esta configuración no depende de ninguna configuración manual de host ni de ninguna configuración mínima de router alguno, o de servidores adicionales; Esto permite a los host generar sus propias direcciones IPV6 localmente mediante información anunciada por los routers.

- **Stateful,** siendo esta una configuración predeterminada el host obtiene tanto direcciones como parámetros mediante un servidor que mantiene una base de datos con las direcciones asignadas de cada host en una tabla.

Ambos tipos de autoconfiguración se complementan mutuamente a diferencia de las configuraciones predeterminadas que nos

garantiza que cada host tiene una configuración IPV6 asignadas manualmente.

b) Direccionamiento IPV6.

Como se comentó anteriormente en el capítulo 1 de esta investigación, las direcciones IPV6 con 128 bits de longitud identifican interfaces de red, permitiendo que un nodo de lugar a la asignación de múltiples direcciones IPV6 y obteniendo la siguiente clasificación ya mencionada anteriormente pero a la que detallaremos un concepto breve a continuación:

- **Unicast,** identificador de una sola interfaz de red, cuyo paquete enviado sólo llegará a la interfaz destino identificada.

- **Anycast,** identificador de un conjunto de interfaces de red interactuando con un paquete a diversas de las interfaces identificadas con dicha dirección y es usado generalmente para tráfico redundante.

c) Protocolos de Enrutamiento IPV6

Al igual que en IPV4 el uso de los protocolos de direccionamiento se dará con un estudio de la necesidad empresarial según la arquitectura de red, sus políticas de seguridad y de conectividad para poder escoger el mejor y más adaptable protocolo de enrutamiento requerido pero estos con la finalidad de desplegarse en un entorno de IPV6 y traducciones en su mayor parte a IPV4 para la convergencia mutua de los 2 protocolos IP [25]. La figura 3.5 muestra un ejemplo de la autonomía de 2 sistemas que interactúan con Gateway a nivel interno y externo

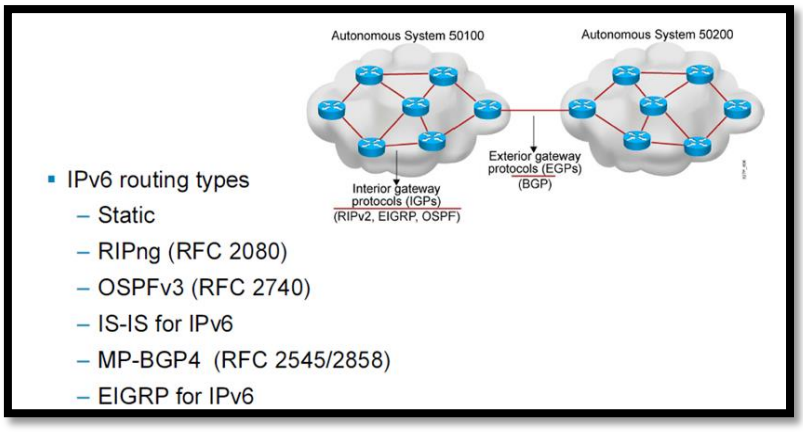


Figura 3.5 Tipos de ruteos del protocolo según autonomía de diseño

3.2. NODOS Y MOVILIDAD SEGÚN IPV6.

Unos de los nodos considerados para este Tema son los Siguientes:

- **Nodo IPV6/IPV4**, el cual es un host o enrutador que implementan los 2 protocolos IPV4 e IPV6

- N**odo IPV6 únicamente,** el cual puede ser un host o un enrutador que implementa IPV6 únicamente.

Nodo IPV6, el cual puede ser un Host o un enrutador que implementa IPV6. Los nodos IPV6/IPV4 y nodos IPV6 únicamente son nodos IPV6. La consideración de los diferentes tipos de nodos para el protocolo IPV6 se da por derecho de movilidad en IPV6.

Movilidad en IPV6, capacidad de mantener una misma dirección IP, a pesar de que este se desplace físicamente a otra área dentro de un rango manipulado por distintos nodos o AP para que sin importar su situación este sea accesible a internet manteniendo la misma dirección IP; capacidad que en ausencia no haría posible que los paquetes destinados a un nodo móvil no se mantuvieron posibilitados para llegar a

diferentes destinos mientras el nodo móvil se encuentre alejado de su vínculo principal o home link [28].

Encontraremos una definición por el protocolo de la movilidad basada en RFC-3775 como bien llamada: mobility support in IPV6. Un ejemplo de la movilidad se muestrea continuación en la figura 3.6

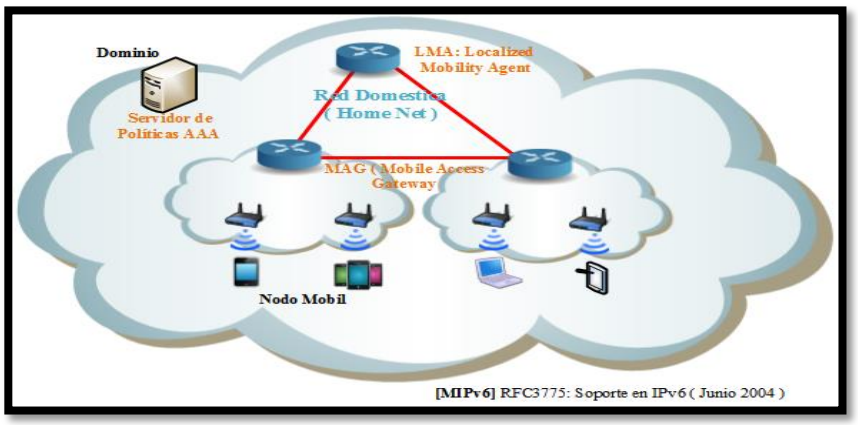


Figura 3.6 Movilidad IPV6 según red doméstica

Mediante los mecanismos de IPV6 un nodo puede obtener una dirección a usar un vínculo externo asociado a los nodos que pertenecen a la red vinculada, home address o que bien sean de otra red configurada para movilidad por IPV6 [13].

Tutorials Point nos indica:

- **Mobile Node**: dispositivo que necesita movilidad IPV6.

- **Home Link**: Este enlace se configura con el prefijo de subred a casa y aquí es donde el dispositivo móvil IPV6 recibe su domicilio.

- **Home Address**: Esta es la dirección que el nodo móvil adquiere desde el Home Link. Esta es la dirección permanente del nodo móvil. Si el nodo móvil se mantiene en el mismo Home Link, la comunicación entre las distintas entidades tiene lugar, como de costumbre.

- **Home Agent**: Este es un router que actúa como registrador para nodos móviles. Home Agent está conectado a Home Link y mantiene la información sobre todos los nodos móviles, su casa, direcciones y sus direcciones IP actuales.

- **Foreign Link**: Cualquier otro enlace que no es de nodo Móvil Home Link.

- **Care of Address**: Cuando un nodo móvil se apega a un enlace de relaciones exteriores, adquiere una nueva dirección

IP de la subred de link exterior, Home Agent mantiene la información de ambos, domicilio y atención de dirección, cuando las múltiples direcciones pueden ser asignadas a un nodo móvil, pero en cualquier caso, sólo una Care-of Address se ha vinculado con la dirección de la casa.

- **Correspondent Node**: Cualquier dispositivo habilitado para IPV6 que tiene la intención de tener una comunicación con Mobile Node.[TP]

3.3. METODOLOGÍAS CON MODELOS EJEMPLARES DE SISTEMAS QUE APLICAN IPV6

Para el análisis de este punto lo dividiremos en dos:

- Metodología aplicada,
- Modelos ejemplares de sistema aplicados con IPV6.

La metodología aplicada, para el enfoque de la implementación del proyecto integrador de redes WISP IPV6 sugiere un florecimiento global del protocolo por los Usuarios para futuros alcances y mejoras en la tecnologías.

La sustitución y convergencia de estos protocolos (IPV4 e IPV6) al permitir el énfasis en nuevas tecnologías y transición propuesta considerará un margen a seguir muy cauteloso y aplicable en redes de campo abierto.

La comprensión de una metodología en redes WISP hace referenciar al conjunto de procedimientos relacionados que se utilizarán para alcanzar diversos objetivos son:

- Escenarios de red,
- Infraestructura y equipamiento,
- Sistemas y servicios,
- Propuestas y limitaciones,
- Mecanismos de transición ,
- Direccionamientos y DNS, etc.

Entre otras opciones donde podremos analizar modelos estructurales y analíticos de proyectos ya implementados en IPV6 en diferentes regiones y empresas con exitosos resultados para lo cual nos hemos basado en argumentos entendidos de un esqueleto muy sólido a resistir exigencias que en algún momento podría verse tambalear.

Según lo mencionado en un principio: El estudio e implementación de la red WISP involucra el manejo de esquemas y factores que puedan favorecer o afectar el correcto funcionamiento de la red aérea bajo el protocolo de IPV6.

A lo cual mencionamos 3 Tipos de metodologías a escoger como la son:

Metodología

- Deductiva
- Inductiva y
- Analítica

Metodologías que recomiendan estudios en campo abierto similar a lo desarrollarse en el proyecto WISP v6 con particularidades que pueden en su mayor parte de utilidad para las pruebas en un entorno verde urbano de muchas variabilidades.

3.3.1. Modelos ejemplares de sistema aplicados con IPV6.

Considerándose *v*arios sistemas famosos aplicados en IPV6 como proyectos o tesis ejemplos [29] a mencionar exitosamente implementados en Ecuador y en otros

países da un reflejo de un 80 a 90 % de confiabilidad para el proyecto WISP en IPV6 a proponerse son:

1. Metodología de implementación de IPV6 en la red de la Universidad de Oriente, CORPUS-UONET. http://goo.gl/HD0eyC

2. Estudio de QOS sobre WLAN utilizando el estándar 802.11e aplicado a transmisiones de sistemas multimedia sobre IPV6. http://goo.gl/BlJlf1

3. Asignación de direccionamiento IPV6 en la red de la Universidad de Valencia. http://goo.gl/YFz9uz

4. Propuesta para la transición de IPV4 a IPV6 en el Ecuador a través de la Superintendencia de Telecomunicaciones (SUPERTEL), Universidad Católica de Guayaquil. http://goo.gl/79wEjg

5. La adopción de Google para IPV6 proyecto migratorio. http://goo.gl/sZOaQc

6. Plan de implementación para migración a IPV6 en la red de la Universidad Politécnica Salesiana de cuenca. http://goo.gl/48XtYj

7. Aplicación de IPV6 en la Universidad Nacional Autónoma de México UNAM. http://goo.gl/lmplTH

8. Revista Institucional de la SUPERTEL sobre la implementación de IPV6 en Ecuador (NAP.EC) artículos. http://goo.gl/AbznNu

CAPÍTULO 4

4. DISEÑO

4.1 DISEÑO DE LA RED WISP IPV6

Se ha considerado el diseño de la red WISP a manera generalizada para poder implementarse bajo un rango abierto en diversos escenarios no complejos en estructura geográfica pero que sean íntegros en áreas verdes.

El planteamiento del proyecto y su desarrollo según este diseño expuesto a implementarse en parques será para pertenencias de una comunidad barrial unidas a zonas pobladas sean estas dentro o fuera de un perímetro urbano para perseguir un beneficio tanto cultural como educacional. A continuación en la figura 4.1 analizaremos el diseño del proyecto con graficas de visión profesional, enfocándonos en nodos con configuración IPV6 y en como el usuario interactuará.

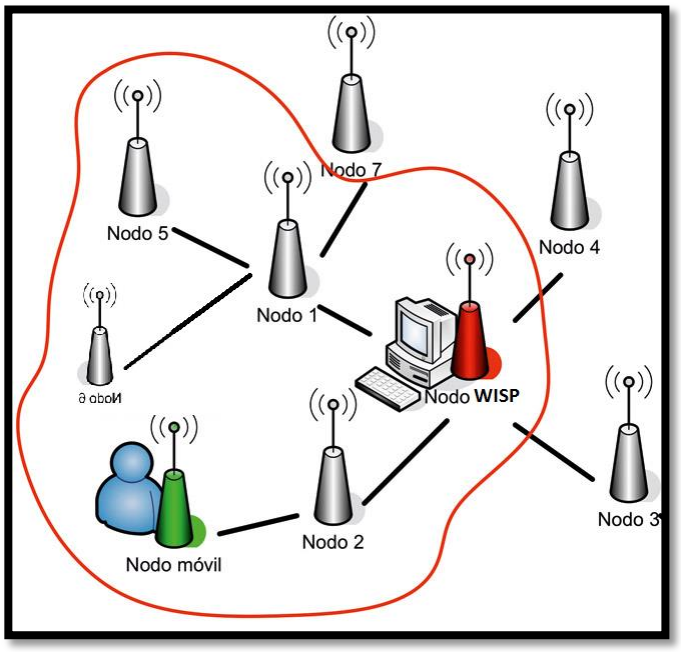


Figura 4. 1 Diseño del proyecto WISP

Para el diseño de la red WISP se va a implementar el modelo jerárquico de red, ya que se divide en 3 capas fundamentales las cuales van a proporcionar flexibilidad, escalabilidad y confiabilidad.

Existen muchos beneficios al utilizar un modelo jerárquico de la red ya que ayuda a hacer la red más predecible, lo cual puede definir funciones a cada capa permitiendo movilidad al momento de administrar la red o aplicar alguna configuración necesaria.

A continuación en la figura 4.2 se muestra un ejemplo de la interacción de las capas en dos nodos diferentes mediante un AP:

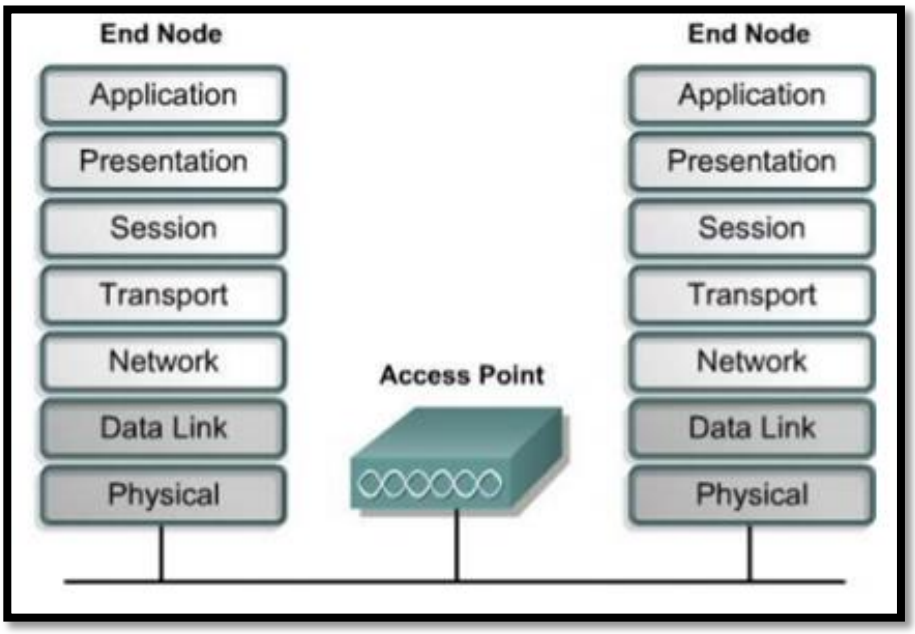


Figura 4. 2 Modelo de trabajo a nivel de capas en nodos finales

Las tres capas con las que se trabajaran para un modelo jerárquico de red son: núcleo, distribución y acceso.

- Capa Núcleo: También conocida como el BACKBONE, se encarga de llevar el tráfico de la red a gran velocidad y de forma confiable, la latencia y la velocidad es lo primordial en esta capa.

- Capa Distribución: Provee las bases de las políticas de conectividad y establece la delimitación entre la capa de acceso y la de núcleo, establece los límites de las capas para la manipulación de los paquetes.

- Capa Acceso: Provee el acceso a usuarios finales y grupos de trabajo a la red.

4.2 ELECCIÓN GEOGRÁFICA Y SELECTIVA DEL PROYECTO

Uno de los sectores estudiados para la implementación del proyecto, considerando el análisis y la predisposición de la ciudadanía referente a la información necesaria para la obtención de datos en vivo, se procedió a consultar por la posibilidad de la utilización del parque central ubicado en la ciudadela Entre Ríos, en el km 1.5 de la vía a Samborondón, con un dimensión aproximada de 145 metros de largo por 75 metros de ancho según un aproximado, con una población de áreas verdes de altura superior a los 3 metros, entre un 30% considerando el total del parque como un 100% a diferencia de los parques más frondosos de la región sierra y Amazonía cuyos parques contienen unidades de árboles que ocupan el 75% del sitio recreativo.

Según mapa trazado en la Figura 3.11 la ubicación geográfica es la mejor en sentido de planicie y líneas de vista tanto de las miras de los hogares como de los árboles y se analiza la frondosidad de las áreas verdes y de las ubicaciones de los puntos de luz para referencia en la figura 4.3 de los que se ubicaran como puntos WIFI

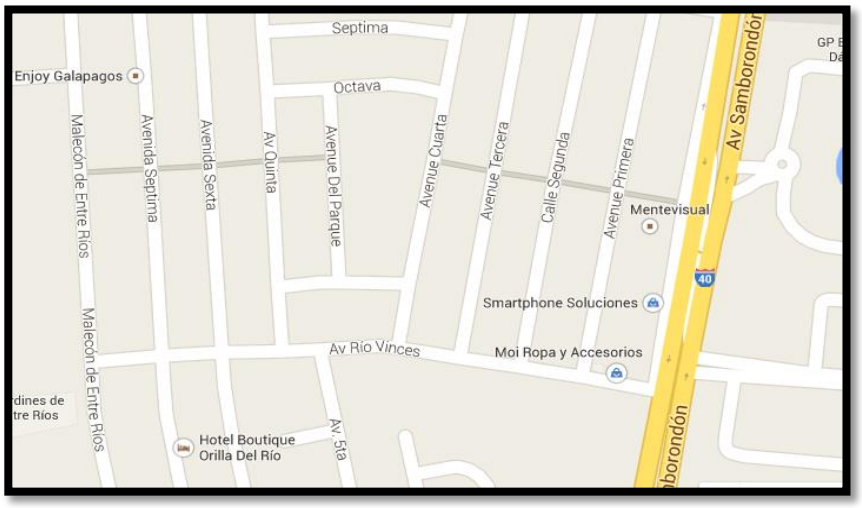


Figura 4. 3 Sector a probar el proyecto google Maps

La frondosidad de los árboles y áreas verdes del parque reflejan lo establecido según figuras 4.4 y figura 4.5 donde las líneas de vista entre dispositivos WIFI (AP) dan a revelar la cantidad de obstáculos que es de un aproximado del 40% en reflejo a otros parques lo que nos da una ventaja en la conectividad.

Figura 4. 4 Puntos de luz y frondosidad

Se considera el alcance de la señal según el dimensionamiento y las líneas de vista de corto alcance de los dispositivos a implementarse como lo son AP, routers y antenas de ser necesario.

Cada punto cuenta con un dimensionamiento casi exacto de “3 metros de alto por AP según el poste de su instalación en reflejo con las cámaras” cuyas probabilidades de crecimiento del proyecto en su migración a otras áreas más grandes y contando con una escalabilidad óptima con el 90% favorables el 10% restante que se lo dirige a márgenes de errores de instalación de equipos adicionales y etc. La ubicación según la Figura 4.5 con una vista aérea muestra todo lo que se considerara para la ubicación adecuada de cada punto de red.

Figura 4. 5 Parque vista aérea para proyecto WISPv6

Se plantea migrar la tecnología de IPV4 a IPV6 en uno de los parques de Ecuador con una de las mejores afluencia tecnológicas de cyber clientes o cibernautas tanto desde dispositivos móviles sean tabletas o portátiles como desde celulares o PALMS entre otros dispositivos tecnológicos de uso de IP.

4.3 COBERTURA APROXIMADA DE RED WISP IPV6

Se ha desarrollado una prueba en gráfico de la cobertura aproximada de la señal de los equipos y sus constantes interacciones y rango de potencias como lo es también su potencia en la frecuencia y distancias entre equipos; a sabiendas que estos puntos son variantes dependiendo de dónde se vaya a desarrollar el proyecto en base a la decisión de un cliente se recomienda desarrollar estos estudios de factores influyentes que podrían representar un importante papel a la hora de montar los equipos y su configuración.

Se ha considerado una vista en gráfico que dará tres (3) campos de colores referenciales a la potencia de la señal según la cantidad de obstáculos y la correspondiente línea de vista entre usuarios y antenas pero de una manera globalizada como se aprecia en la figura 4.6.

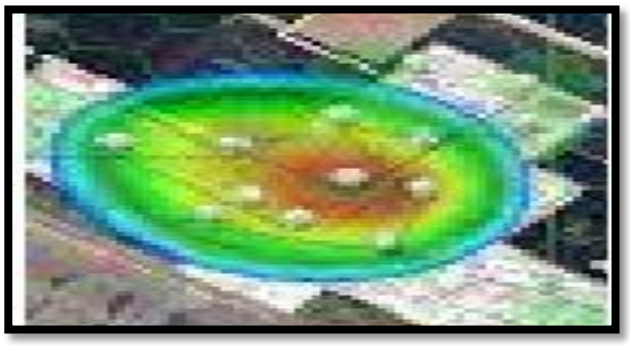


Figura 4. 6 Simulación con equipos paralelos del rango de cobertura de la red.

La distancia entre equipos tendrá un punto de mira entre puntos aproximado según lo estimado en 20 metros de distancia, donde no dificulte por línea de vista ya que para el caso se le propone un movimiento de puesto de antena a 12 o 15 metros por viscosidad de maleza.

La altura de equipos estará medida en postes de un aproximado de 3 metros y medios a lo que un estudio de maleza llevada con mi compañero nos reflejó que la línea de vista actual es buena.

4.4 DIMENSIONES Y COBERTURA DE LOS NODOS DE ACCESO

Existen premisas que se disponen al replanteo de WIFI en ámbitos abiertos y según el alcance de su radio:

- Cobertura total con puntos AP estratégicos.

- Los servicios de datos WIFI que soporta la red será de conveniencia para los clientes considerando un parámetro por encima de los 10 a 15 DB en relación al ruido.

Con estos marcos analíticos se pretende dar una velocidad de 54 Mbps, conectado a 802.11 b/g; lo que dará un uso funcional de la red incluso cuando se predisponga la compatibilidad con equipos de soporte 802.1n. En la siguiente figura 4.7 se muestra un análisis de la predisposición en un ambiente verde de la tecnología y su acople al usuario final.

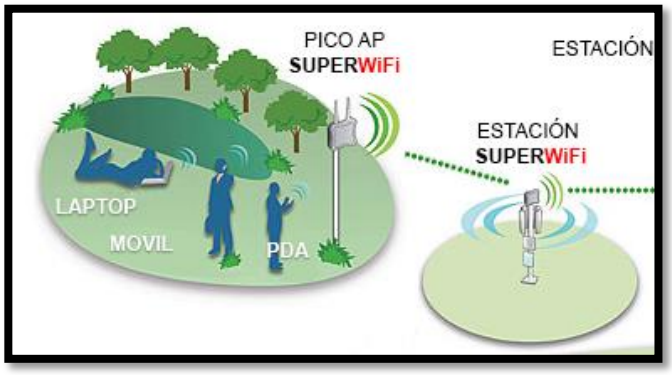


Figura 4. 7 Línea de vista y cobertura de Nodos

Se pretende con este estudio de cobertura de tamaño indiferenciado por la permisión de usar el proyecto para parques o sectores urbanos de dimensiones cambiantes, satisfacer una necesidad oportunista para el usuario que con uso responsable de tal servicio logre obtener un

beneficio al momento de acceder o incluso salir de un apuro para lo cual tenemos este estudio:

- Se puede analizar o identificar el nivel de potencia según la radio frecuencia necesaria por la “X” cantidad de obstáculos que encontremos.

- Inspeccionar las instalaciones vecinas para calcular el tipo de obstáculos potenciales a la señal de RF como armarios vecinos, antenas u otros equipos informáticos que puedan generar incluso caídas de la señal inesperadas.

- Sondear los sectores de constante utilización de la señal por parte del usuario para poder configurar un ancho de banda adecuado y dar un mejor equilibrio del tráfico de la red completa.

- Una determinación concreta en la ubicación de los puntos de red “AP” y el correcto sistema de protección de la alimentación cableada por tuberías.

Para poder dar cumplimiento a la mayoría de estos análisis tenemos la consideración a la potencia de la señal en DBM y su relación señal

a ruido. La figura 4.8 muestra las áreas de cobertura del parque a rendir la señalización WIFI o WIRELESS con el servidor WISP

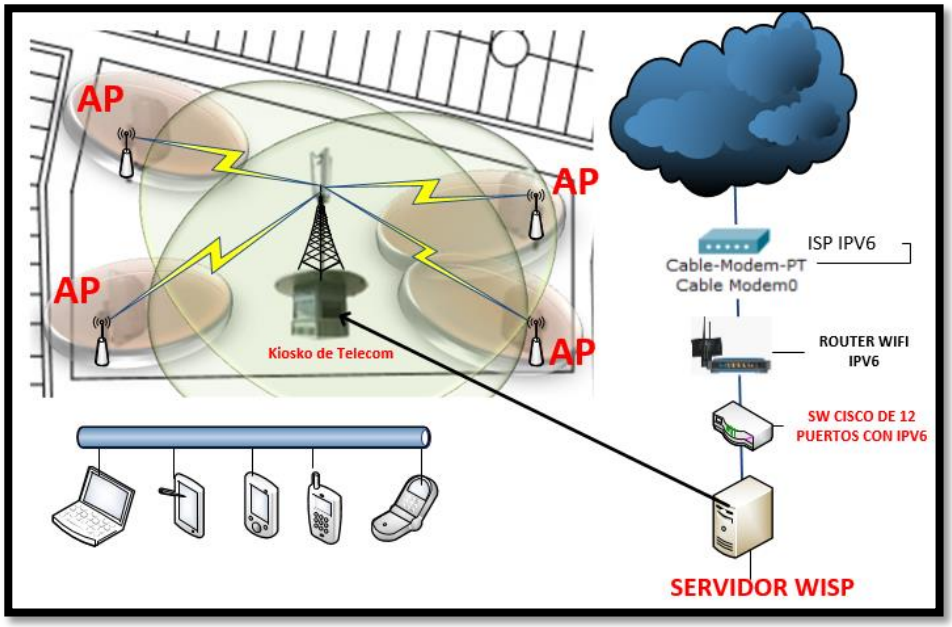


Figura 4. 8 Ejemplo de red WISP Trazado

En la gráfica se muestra las dimensiones a rendir con la cobertura de la señalización WIFI o WIRELESS con el servidor WISP.

Cobertura: Cobertura total en su 98% para datos en el medio

Muestreo: Para dar el servicio de datos más satisfactorio es necesario las muestras de la calidad de señal y el ancho de banda y las siguientes relaciones:

- Relación señal ruido, superior a los 10 -15 dBm
- Un Data Rate de 54 Mbps y el correcto estándar 802.11 b/g/n

Dentro de este análisis se procedió a consultar con un entorno de evaluación para comprobación de los sistemas en espacios libres y zonas urbanas como aplica en nuestro caso en relación con el parque seleccionado, a lo cual se muestra en la siguiente tabla 4.1 sobre el entorno de propagación de las señales de datos en espacios libres y con sistemas de celulares en urbanizaciones con y sin obstáculos así como en edificios, plantas y fábricas donde *n* significa la potencia de trabajo.

Tabla 4.1 Rangos de propagación con/sin Obstáculos

Entorno de Propagación	n
Espacio Libre	2
Sistema Celular en zona urbana	2.7 a 4
Sistema celular en zona urbana con obstáculos	3 a 5
Edificios con visión directa	1.6 a 1.8
Fabricas con visión directa	1.6 a 2
Plantas sin visión directa	2 a 4
Edificios con obstáculos	4 a 5
Fabricas con obstáculos	4 a 3

A continuación encontramos en la figura 4.9 una representación básica de la reacción de la distancia "**d**" que separa el punto de acceso y el receptor teniendo en cuenta un básico de altura de 3m y 1m de altura que representa al usuario en una posición fija en vertical.

La representación con distancias por **X0** representa un reflejo directo contra un obstáculo (muro o árbol) y la distancia plana del punto de acceso al equipo receptor en la figura.

Analizaremos puntos de vista desde los nodos (AP) hasta el cliente (usuario) con representación de distancias d0, x0, x y d

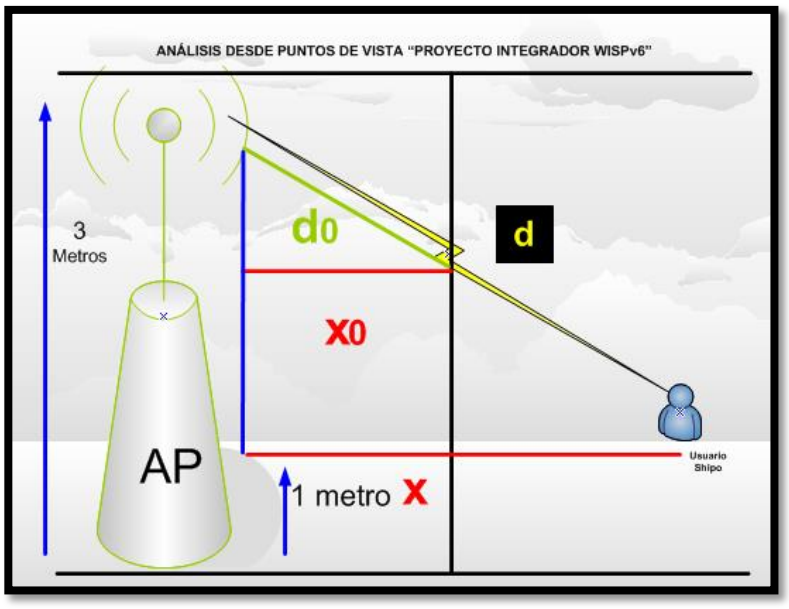


Figura 4. 9 Representación desde un AP a un Cliente

Muchos son los puntos donde los proveedores de internet (ISP) proponen proyectos de coberturas para sectores privados o urbanísticos a lo que se revela según la aplicación de google el siguiente mapa de puntos de coberturas WIFI con trabajo en IPV4 y que son potenciales a migrar con IPV6 según panorama presentado en la vía a Samborondón como lo muestra la figura 4.10.

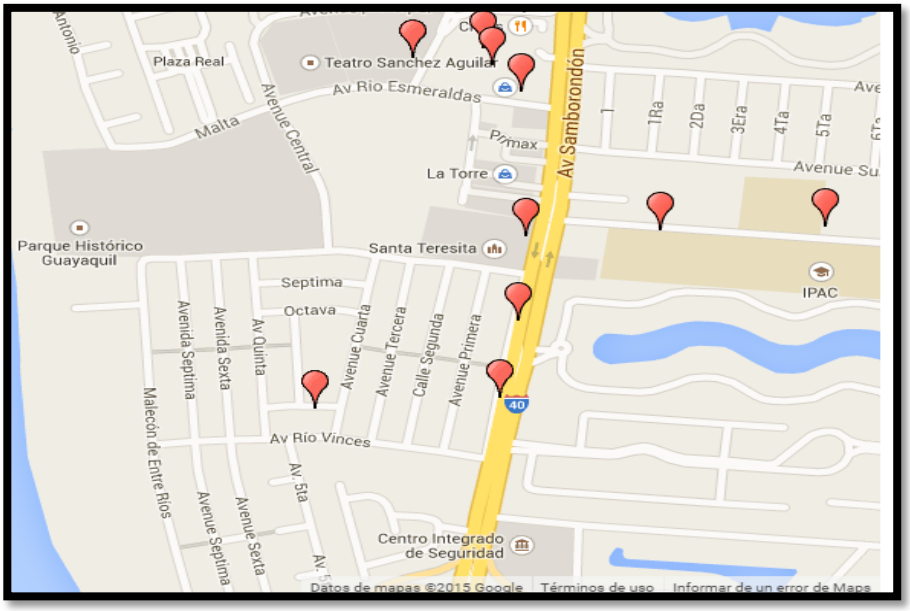


Figura 4. 10 Puntos con soporte por ISP para el Proyecto

4.5 APLICACIÓN DE SOFTWARE PARA EL PROYECTO.

Este punto está pensado y dirigido a la instalación de sistemas de configuración sean estas manuales y autónomas (scripts) del sistema operativo del servidor WIFI, DHCPv6 y demás sistemas a implementar

y configurar para el proyecto; dicha explicación y pasos explícitos se justificaran en el transcurso del documento, posteriormente solo se mencionará y señalará gráficamente lo más relevante en su aplicación y función.

Uno de los sistemas operativos a implementar será Windows Server 2008 R2, con alguno de los programas Virtual Box, Sistemas NMS, Ekahau, Cisco y aplicación de servidores DHCPv6, Wi-Fi y servidores apache, entre otros, cuyas configuraciones serán automatizadas en su mayoría de ser posible para una instalación autónoma, caso contrario se dará por instalaciones y configuraciones manuales.

NETKROM Network Management System (NMS) [33] es una aplicación con una interface gráfica de usuarios basada sobre java corriendo en cualquier sistema operativo. Su función principal es servir como una herramienta administrativa y de vigilancia para las unidades inalámbricas de la red.

WI - Fi Ekahau System (ESS)

Para los profesionales móviles, los gerentes de TI y administradores, Ekahau Site Survey TM es una herramienta de diseño fácil de usar por la verificación y solución de problemas.

ESS es visual, basado en una herramienta que se ejecuta en computadoras portátiles con Windows (también se ejecuta en una Mac usando Bootcamp). Ekahau Site Survey asegura un alto rendimiento y la capacidad (BYOD) para cualquier red Wi Fi (802.11 b/g/n/legado) útil para VoIP, video, ubicación geográfica, o transmisión de datos de alta velocidad. Si usted no tiene una red WIFI, ESS le sugerirá automáticamente la colocación de AP y configuraciones óptimas, pero si ya dispone de una red WIFI en su lugar, ESS permite estudios de campo rápidos y fáciles, el rendimiento y la capacidad de análisis permite la optimización y solución de problemas.[E]

La habilidad de manejar unidades inalámbricas sobre la red lo hace una aplicación bien útil. NMS deja el usuario configurar parámetros de hardware y software importantes de la unidad de acuerdo a los requerimientos del usuario. Además tiene la habilidad de enseñar información de transmisión de data.

4.6 PORTAL DE BIENVENIDA

Como bien se conoce en Linux, la aplicación de modificaciones de las páginas de internet según el explorador se las suele modificar o incluso configurarlas para la necesidad que se disponga con el primer log-on, tanto para la introducción de un usuario y una clave si

disponemos de un dominio o de una bienvenida para cuando el espacio es de libre acceso como en nuestro caso, a lo cual se usan por frecuencias configuraciones basadas en apache server pero en Windows se lo conoce como IIS server [38].

Según la página de Windows tenemos que: “El rol de servidor web (IIS) incluye Internet Información Services (IIS) 7, que es una plataforma web unificada que integra IIS, ASP.NET, Windows Communication Foundation y Windows SharePoint Services. IIS 7 permite compartir información con usuarios en Internet, en una intranet o en una extranet. Windows Server® 2008 ofrece IIS 7.0, que también se incluye con algunas ediciones de Windows Vista; Windows Server 2008 R2 ofrece IIS 7,5, que también se incluye en algunas ediciones de Windows 7.”[IS]

A continuación, en la figura 4.11 se muestra un ejemplar en práctica de cómo quedaría la página de bienvenida en coordinación con los ISP como creación y simulación de portal de bienvenida del proyecto con imagen.

Figura 4. 11 Portal de bienvenida con proveedor

La disponibilidad a la convergencia de este punto con diversos sistemas de las variadas plataformas que ofrece Windows según la aplicación del Internet Information Services (IIS) [37].

4.7 ELECCIÓN DEL ISP

Aunque bien es cierto que Ecuador carece por el momento de un ISP de IPV6 neto en su servicio y para el hogar o pymes, se ha considerado proveedores de internet en el país con la disponibilidad de su tecnología para brindar servicios de conectividad de a futuro de IPV6 y se consideró un estudio de implementación, gráfico de las transiciones y convivencia en ecuador con IPV6 e IPV4 que todos

usamos para pruebas tanto en Telconet como futuros ISP de IPV6 y a Movistar como un impulsor pleno de IPV6 dentro del país pero sin la disponibilidad de equipamiento para el correspondiente incentivo para inversiones grandes por temáticas da temor a pérdidas, ya que el riesgo de las empresas al cambio no está dotado del poder de convencimiento adecuado como para que elijan cambiar de IPV4 a IPV6 y así movistar pueda brindarles su tecnología.

Telconet como vemos en la figura 4.12 siendo un proveedor con una sede cercana a la urbanización maneja uno de los mejores planes pilotos a convencer y cambiar de protocolo [14].

Figura 4. 12 Telconet.S.A Proximidad a sector de proyecto.

Los siguientes gráficos muestran la evolución del protocolo por defecto y los tipos de direcciones IPV6, y ancho de banda promedio en Ecuador con el tiempo.

Ellos se generan utilizando los datos recogidos por el IPV6-test.com, prueba de conexión página, donde su actualización es mes a mes. A continuación, estadísticas con grafico muestran en parte celeste el uso de IPV4 en un 97.2% el soporte del protocolo en uso Vs IPV6 en un 14.7%, figura 4.13 como parte 1.

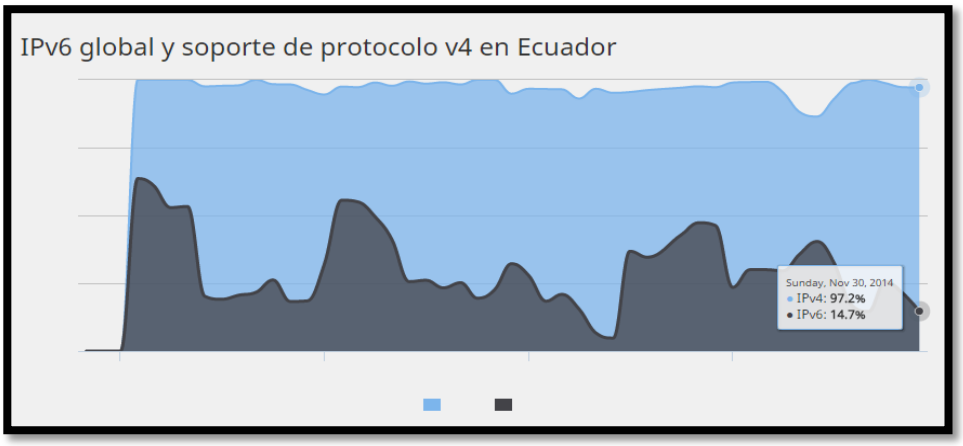


Figura 4. 13 IPV6 estadística ecuador soporte de protocolos IPV4 y v6

Las cifras son porcentajes, mostrados para IPV4 en celeste y para IPV6 en plomo por lo que pueden esperar de casi el 100% de los ejércitos de apoyo IPV4 con un crecimiento lento para IPV6. A continuación uno de los proveedores de IP en Ecuador lanzando una prueba de cuenta CEDIA obtiene mejor resultados según los 25 ISP participantes en 2014 figura 4.14

Top 25 proveedores de servicios de Internet para IPv6 en Ecuador (diciembre 2014)

	Proveedor de servicios Internet	IPv6 pruebas de cuenta
1.	Cedia	6

Figura 4. 14 Proveedor paréntesis de movistar según pruebas realizadas

La figura 4.15 muestra el porcentaje de los navegadores que incumplen a IPV6 vs. IPV4 cuando se visita la prueba de conexión IPV6-test.

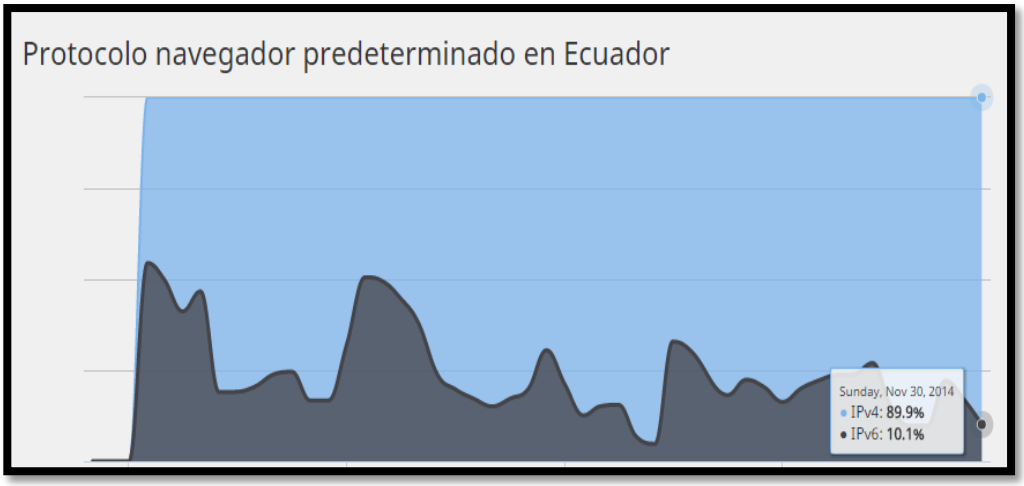


Figura 4. 15 Navegadores predeterminados en Ecuador IP v4/v6

En algunos casos con conexiones de túnel el protocolo de IPV4 se mantiene con un valor predeterminado, a lo que en este gráfico número 4.16 se muestra el porcentaje de los navegadores que son por

defecto para IPV6 vs. IPV4 para los usuarios que tienen conectividad tanto IPV4 e IPV6.

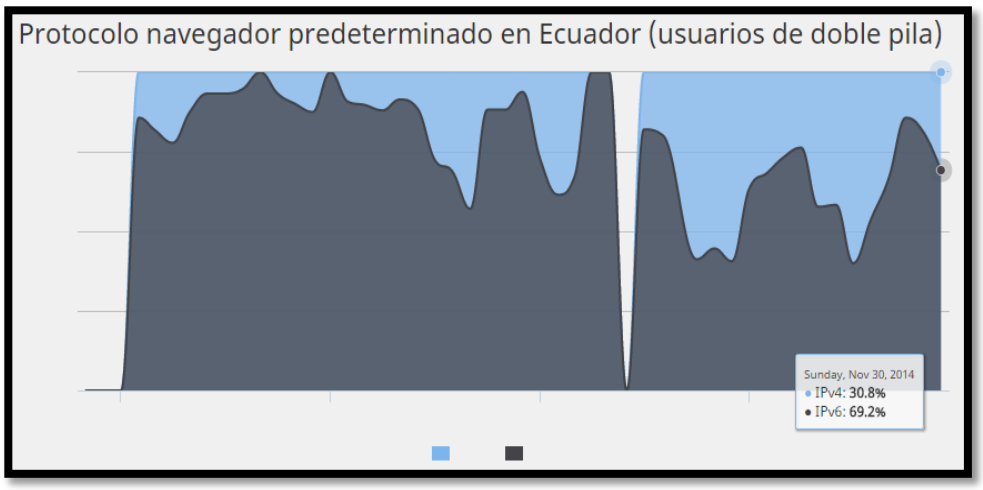


Figura 4. 16 Avances de pruebas de IPV6 con usuarios de doble pila

Figura 4.17 CEDIA [30] en las pruebas de servicios entre IP v4/v6 obtiene un tanto del %50 de éxito en uso aplicativo tanto para v4 y v6.

	Proveedor de servicios Internet	Recuento de comprobación	IPv4	IPv4%	IPv6	IPv6%
1.	Cedia	6	3	50,0%	3	50,0%

Figura 4. 17 Conectividades según IPV4 e IPV6 en pruebas de recuento

En la imagen 4.18 se puede ver la evolución de los tipos de direcciones con el tiempo, y medir el uso de 6to4 y Teredo túnel conectividad.

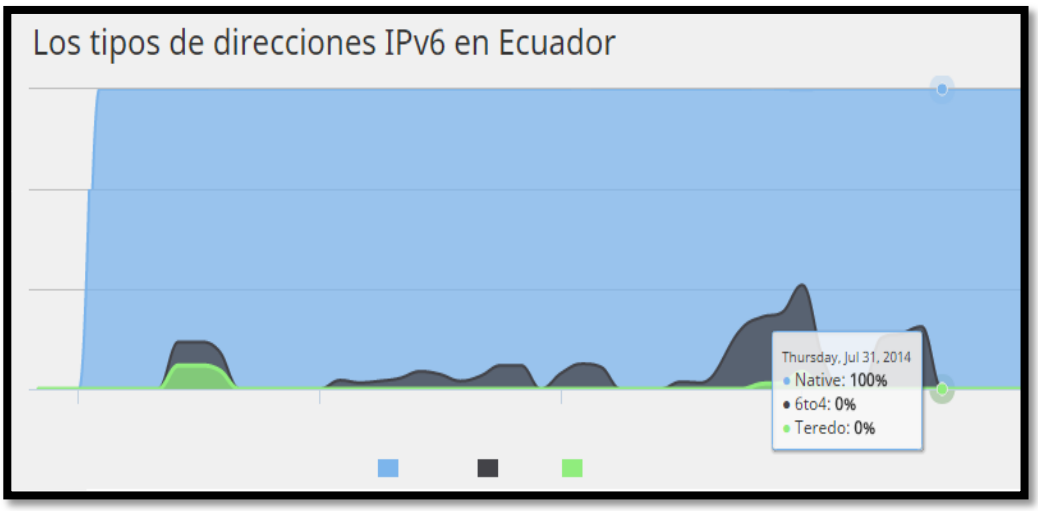


Figura 4. 18 Tres tipos de direcciones IPV6 Nativa, Teredo y 6to4

Cabe señalar que debido a que 6rd trabaja con direcciones nativas, no puede ser detectada aquí como tunelizado. Este es también el caso de túneles VPN basados en v4 y v6 donde en la figura 4.19 mostramos en un cuadro el ancho de banda según un radio (Ratio) de Downstream realizado en Ecuador en el 2014.

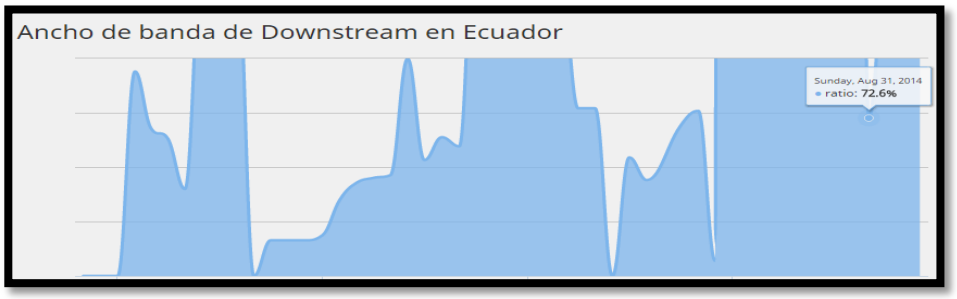


Figura 4. 19 Downstream ecuador y consumo de su ancho de banda

El anterior gráfico ilustra la brecha de velocidad de conexión entre IPV4 e IPV6, números representan la velocidad v6 como porcentaje de la velocidad IPV4, puesto que las velocidades más bajas IPV6 son a menudo causados por la sobrecarga de túneles o conectividad IPV6 insuficiente o capacidad mirando a los ISP" [C]. En conclusión según el análisis, Movistar presenta como buen ISP en el incentivo de la introducción de IPV6 al Ecuador con velocidades aún no anunciadas al público.

4.8 ANÁLISIS DE EQUIPOS Y TECNOLOGÍA

La consideración de equipos se ha previsto en 2 categorías dependiendo la necesidad y pre disponibilidad económica del cliente y del espesor de las áreas verdes y su altura. Para ello se ha creado según un estudio de compatibilidad de tecnologías una variedad electiva de recursos a implementar con la misma convergencia y

compatibilidad IPV6 para el proyecto WISP. A continuación tenemos un listado de equipos.

A. Estaciones cliente Fijas (suscribir station)

Se utilizará la solución modelo: Netkrom ISPAIR 54Mb 3.4 to 3.7GHz CPE. Los sistemas WIRELESS ISPAIR 54Mb son usados para proveer a los usuarios finales acceso a la Internet usando una arquitectura punto-multipunto a 70 Mbps en las bandas desde 2.4 GHz hasta 5 GHz.

Uno de los equipos inalámbricos con los que podremos obtener un gran ancho de banda a distancias bastante largas y a un precio bastante razonable. Estos equipos ofrecen distintas características tales como Routing, Firewall, NAT, DHCP, control de ancho de banda y mucho más.

El cliente CPE el cual tiene la antena integrada es la más comprensible solución inalámbrica, el cual incluye un router inalámbrico potente con característica de Power Over Ethernet (PoE), todo integrado con una antena de alta ganancia.

La antena Flat Panel ofrece una amplia cobertura territorial sin ninguna pérdida de señal y además el inyector Power over Ethernet le provee la posibilidad de entregar la necesaria potencia y datos a su Router (el cual está adjunto a las antenas) a través de un simple cable Ethernet.

A continuación en la figura 4.20 mostramos imágenes del modelo: Netkrom ISPAIR 54Mb 3.4 to 3.7GHz CPE

Figura 4. 20 Antenas para exterior Netkrom ISPAIR 54Mb CPE (ISP-CPE350)

.

Características del AP:

a) Solución rentable.

b) Completa solución impermeable para exteriores.

c) Todo en un dispositivo inalámbrico – CPE.

d) Power over Ethernet integrado.

e) Gestión vía web y función SNMP.

f) Conexión inalámbrica de alta velocidad (hasta 70 Mbps).

g) Distancia de conexión hasta 24km.

h) Firewall, NAT, IP Routing, DHCP.

i) Seguridad de alto nivel con full 64/128Bit WEP y encriptación WPA-WPA2.

j) Chipset Atheros XR – Características avanzadas para larga distancia.

k) WDS – (WIRELESS DISTRIBUTION SYSTEM).

l) Control de ancho de banda.

m) SPI Firewall y filtrado de paquetes y URL´s.

n) Alineador de Antenas y escaneado de sitios inalámbricos.

o) Instalación rápida y simple para estaciones bases y clientes.

B. Sistema operativo del WISP

Para la implantación se instalará el sistema operativo Windows Server el cual debido a sus características es la opción viable como sistema operativo compatible con la tecnología de Netkrom, Cisco y Ekahau donde darán lugar a la tecnología inalámbrica que habremos de adoptar, solo utilizaremos el

sistema operativo ya que la misma trae consigo las aplicaciones de gestión y administración del sistema y la correcta implementación de un DHCPv6 y un Apache Server de ser necesario en virtual [11].

C. Antenas de panel sector de 5.8 GHz

Después de analizar la información se ha decidido utilizar las antenas de panel de la compañía Netkrom: modelo W58-17SP para frecuencia de 5.8GHz, ganancia 16dBi, 120º de sector de polarización y 30º de inclinación del panel, para lo cual si es necesario se ocupará tres paneles para tener la cobertura total de 360º grados.

I. Descripción

Los sistemas de antena de Sector Horizontalmente Polarizados ofrecidos por Netkrom son construidos de plástico UV estable ABS radomes y anaqueles robustos galvanizados para una larga vida de servicio, en condiciones ambientales extremas.

Las antenas de panel Netkrom con sectores convenientes hasta 5.8Ghz como se muestra en la figura 4.21 desde diferentes puntos de vista son una de las mejores opciones en el momento

de plantear convergencia con otros dispositivos WIFI y además da mayor cobertura.

Figura 4. 21 W24-17SP90 Antena de Panel y Sectores VPOL con polarización vertical y horizontal.

Su polarización horizontal tiene el potencial de interferencia reducida, en los sistemas que son instalados en áreas con niveles altos de ruido de RF verticalmente polarizado o donde el sistema central debe evitar potenciales problemas futuros con la interferencia. Los componentes de la base son fáciles para instalar y adaptarse hasta 30 grados de inclinación.

II. Características

- Horizontalmente polarizado.
- Modelos de: 90o 17dBi y 120o 16dBi.

- Conector integrado tipo N Hembra.
- Sumamente resistente para una larga vida de servicio en ambientes extremos.
- Completamente impermeable.

III. Aplicaciones

a) 5.8GHz y aplicaciones de banda U-NII

b) Antenas para estación base

c) Para sistemas inalámbricos

d) Sistemas punto multi-punto

e) Sistemas inalámbricos de banda ancha

D. Analizador de Espectro Cisco y Tecnología Ekahau.

Para las pruebas recomendadas se escoge el analizador de espectro y un acompañante complementario como veremos en la Figura 4.22

Figura 4. 22 Analizador de Espectros e Interfaces

Actualmente conocemos un equipo Cisco capaz de analizar un espectro y dar la información correcta en tiempo real sobre interferencias, coberturas, niveles de saturación y los distintos canales ocupados en el medio en donde se pretende establecer una implementación de ámbitos WIFI o WIMAX como lo es el analizador de espectro Cisco.

Una de las tecnologías a nivel de software consideradas a pretender en caso de ser exitoso como ahorrador monetario es nuestro buen amigo EKAHAU [E] ya que es uno de los ÚNICOS softwares existentes en el mercado basado en tiempo real para sistemas de calibración, localización de puntos de red y demás como se verá en la siguiente figura 4.23.

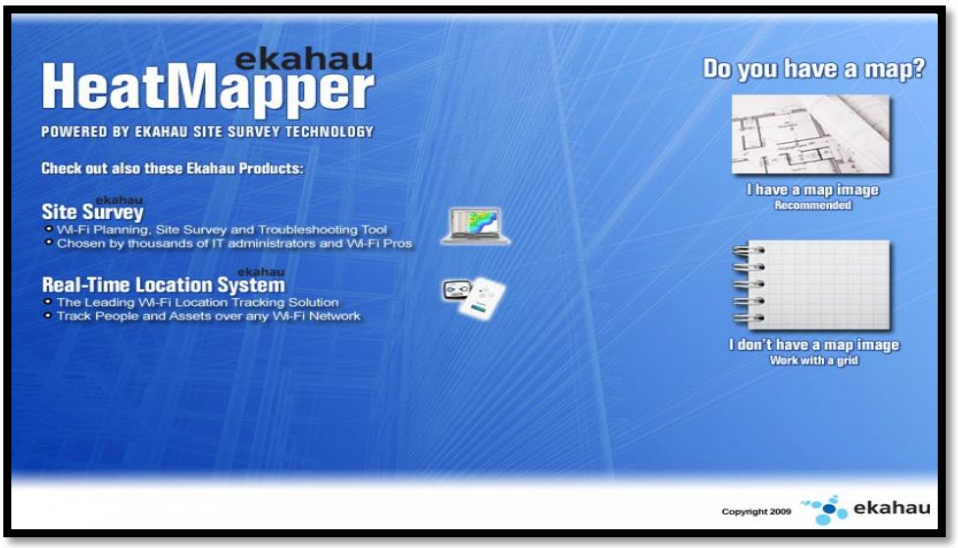


Figura 4. 23 Sistema Ekahau, monitor en tiempo real

Comparte una compatibilidad con equipos pasivos y activos de uso WIRELESS goza de la precisión de hasta 1 metro en el mejor de los sistemas de implementación de red y de las consideraciones cognitivas de los AP, lo que permite localizar muchos dispositivos a la vez y sobre el mismo mapa de situación tanto en coordenadas x, y, de edificaciones y pisos correspondientes dado el caso, habitaciones y zonas sobre cualquier estándar 802.11. Para la correcta modalidad de control a utilizar el sistema EKAHAU tenemos la:

- EPE (Ekahau Positioning Engine) software utilizado como centro de control y es el que se encarga de crear la

plataforma de ubicación de todos los equipos compatibles con EKAHAU.

- Los Access Points en el área de localización permiten enviar la información de la red incluyendo a esta la red cableada cumpliendo la condición de pertenencia de nuestra red de un mínimo de 3 APs

- Ekahau Client: software que se debe instalar en dispositivos clientes como PDA, TAGs y portátiles que en su medida deberá de estar dotado de una tarjeta de red que cuente con un transceptor de radio y una antena para su localización [33].

4.9 ESCALABILIDAD DE LOS EQUIPOS

Para este punto se considera la ubicación dentro del kiosko donde se va a alojar el "rack" considerando una zona céntrica dentro del parque o lateral entrante situado a un costado del comité lo que daría una implementación de antenas del tipo de 270º.

La escalabilidad se sujeta al equipo elegido y analizado dentro de un margen en vista a las posibilidades de poder usar el proyecto no solo

en una implementación sino en más de un sector de similar o mayor tamaño donde la evolución de dispositivos clientes se someta al equipo de una manera futura y escalable.

A continuación se muestra en la figura 4.24 la arquitectura del kiosko que aloja el rack a conocimientos que dicho diseño escogido según similares en google contiene lo más exacto de lo que se intenta armar para alojar los equipos del servidor WISP además que puede sufrir cambios dependiendo el sector a elegir su implementación pero con la garantía del 95.9% de escalabilidad programada, dando libertad a un 4.1 % de errores varios.

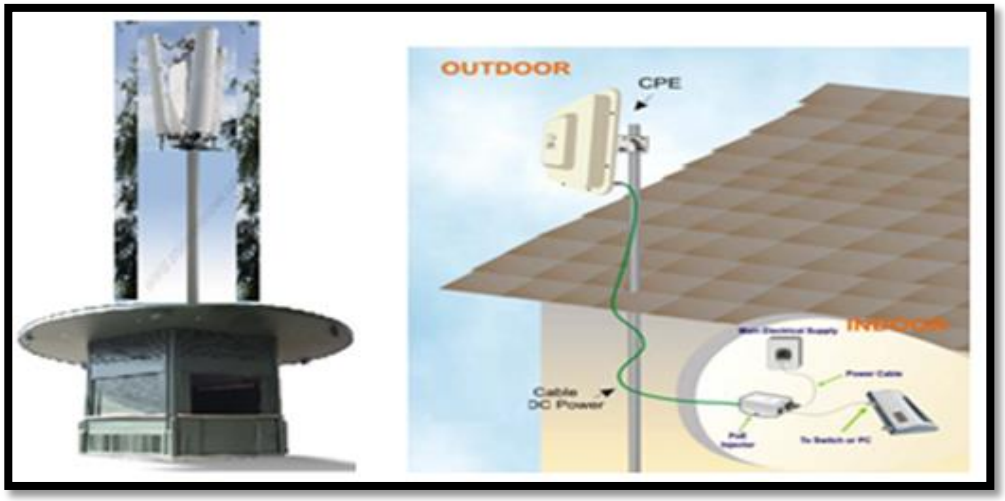


Figura 4. 24 Quiosco e instalación in door de una antena

Modelo de kiosco WIFI y muestra de su instalación indoor/outdoor

4.10 CONFIGURACIÓN DE EQUIPOS Y HERRAMIENTAS

Para el siguiente punto mostraremos a manera de capturas de pantalla la configuración planteada en los escenarios de prueba para la conectividad:

a) Hardware

- **Configuración de equipos Netkrom**:

Como vemos en la figura 3.27 el correcto acoplamiento de los componentes para la instalación de las antenas Netkrom o de cualquier otra marca seleccionada por el cliente a los cuales se eligió (en este caso) por su gran cobertura y escalabilidad y cómodo presupuesto en costos.

Observaremos en la figura 4.25 cómo se desarrolla el punto de habilitación eléctrico y de red según un POE inyector dejado a libre mercado y un SWITCH (SW) también dejado a libre mercado, considerando siempre que la base (tubo) sujetador este bien seguro [32].

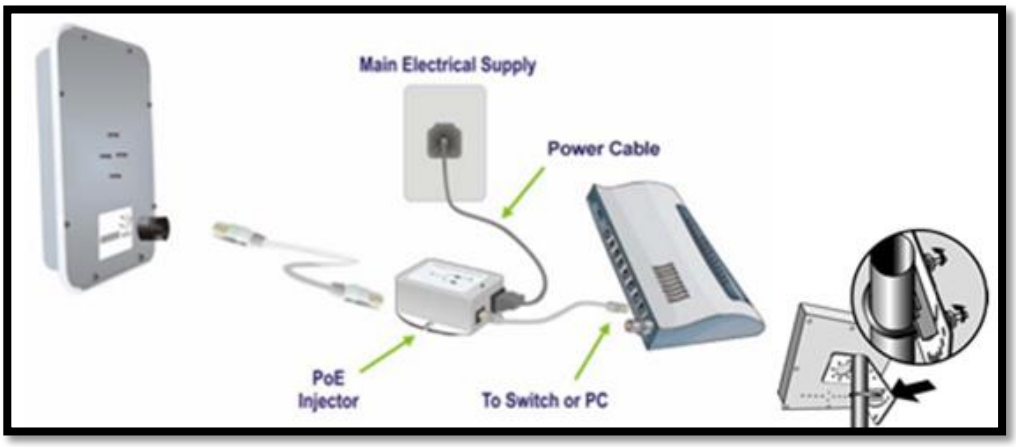


Figura 4. 25 Acoplamiento e instalación de antena Netkrom ISP-CPE350

UPS: la instalación de los UPS [35] para dar soporte a los muchos sistemas y equipos que estarán alojados en el kiosco será de objeto necesario para mantener un sistema levantado de comunicación WIFI por IPV6 constante hacia el cliente a lo que se midió una demanda de equipo de almacenamiento de energía o UPS con las siguientes características:

Los Sistemas UPS SmartOnline ofrecen el mayor nivel de protección de energía disponible para equipos destinados a misiones críticas. La tecnología de doble conversión asegura salida de onda sinusoidal pura, con cero tiempos de transferencia a respaldo por batería durante un apagón. La operación constante en línea aísla

completamente al equipo delicado de cualquier problema de energía en la línea de CA.

Los modelos SmartOnline aceptan el rango más amplio de variaciones de voltaje y frecuencia de entrada, entregando la energía de CA más pura y altamente regulada en forma consistente para sus delicados servidores y equipo de red [UP]

- **Computador**

El computador asignado para este proceso de instalación e implementación física de un servidor WISP con un servidor DHCPV6 y demás programas que impliquen el correcto estudio implementativo, debe de cumplir con un robusto sistema de soporte de softwares para poder ejercer lo planteado a lo que se escoge el siguiente sistema de computador para lo previsto.

Procesador INTEL CORE i7-4790 3.6GHZ LGA 1150

Procesador Intel Core i7-4790, 3.60 GHz Turbo @4GHz, 8MB Total Intel Smart Cache, LGA 1150 de cuarta

generación, 22nm. Soporta: Intel VT-x, VT-d, Turbo Boost Technology.

- **Placa madre**

Gigabyte o ASUS Chipset Intel H81 Socket LGA 1150 DDR3 SN/VD/NW Micro-ATX que incorpora: USB Power 3x, Dual BIOS, SATA 6Gb/s, soporta hasta 16GB de RAM DDR3.

- **I/O Panel**

1 x Puerto de VGA/D-Sub, 1 x Puerto de VGA/DVI-D, 1 x Puerto de HDMI, 1 x Puerto de Óptica SPDIF Out Port, 8 x puertos listos para uso del USB 2.0/1.1, 1 x RJ-45 LED de puertos de LAN.

- **Memoria RAM y disco duro**

4GB DDR3 1333MHz PC3 10600; WD: 500GB 7200 rpm. Serial ATA 6Gbs.

- **Case atx y monitor**

Case USB Frontal: incluye Tobera y fuente de 500 watt; Monitor LG 20M35A-B o más actual, LED 19.5",

Resolución: 1600x900, contraste: 30000:1, conector VGA, auto voltaje.

2 unidades de tarjetas de red bidireccional red conectividad CHIPSET REALTEK® 8111E con velocidad 10/100/1000 MB/S. Gigabit LAN.

- **Pararrayos**

Protección integral de cargas críticas y retención contra descargas atmosféricas siendo un pararrayos para las torres: tipo Franklin, emisión temprana de Iones (ESE), plan seis puntos de Erico y sistemas con arreglos de disipación podemos considerar ya que nuestro sistema se basa en una antena central con una elevación aproximada de 7 metros por encima del kiosko para poder cubrir con línea de vista la mayor cantidad de antenas del sector con las que se instalarán y se procederá a trabajar y dará protección en caso de caídas de rayos a las mismas por su sistemas [PR].

En la figura 4.26 encontramos un ejemplar de pararrayos ionizantes, puntas franklin, electrodos activos de cobre

electrolítico con cobertura desde 35 m hasta 100 m de radio. Cumple normas: nfc 17-102 francesa y la une 21.186 española [36].

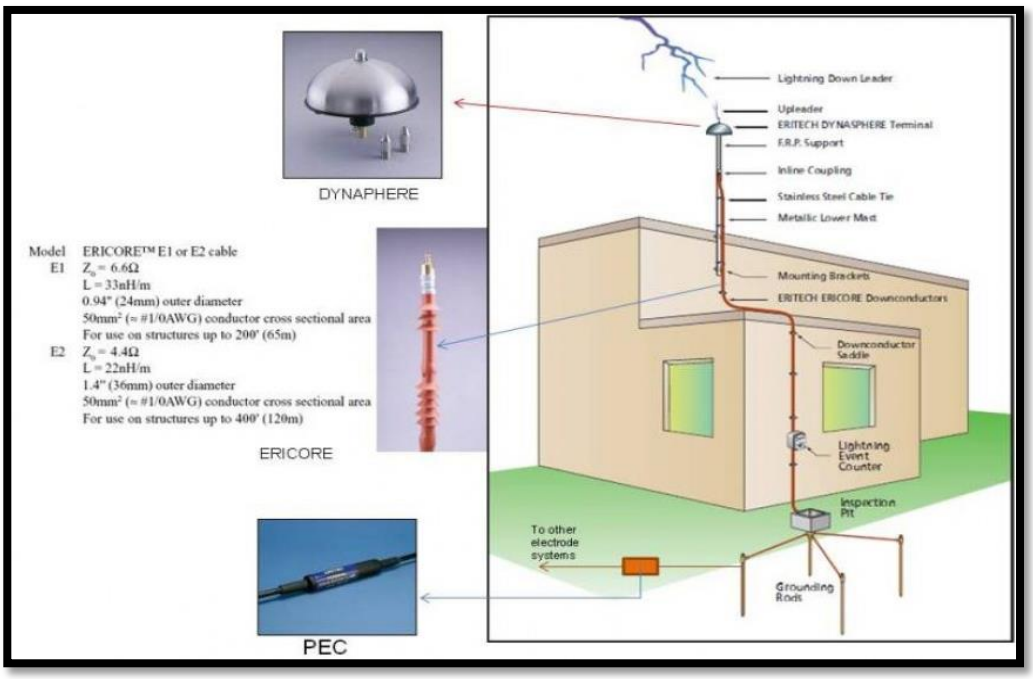


Figura 4. 26 Solución de pararrayos en hogar y punto tierra

b) Software:

Las siguientes instalaciones reposan dentro de los anexos:

1. Instalación de sistemas Netkrom
2. Instalación de software InSiDER
3. Instalación de DHCPv6 en Windows 2008 Server [16].

4.11 SISTEMA DE CONTROL ELÉCTRICO DE EQUIPOS

Analizando cautelosamente surge una pregunta sobre el mecanismo de alimentación eléctrica del proyecto pero esta pregunta tiene su respuesta lógica auto pensante; al igual que el cableado eléctrico de los dispositivos AP y del mismo kiosko de los equipos administrativos del proyecto será visto de una manera especial tendremos su alimentación eléctrica disponible en los postes de adaptación de los equipos AP y sistema de alumbrados.

Entiéndase por control de encendido y apagado a la manera de administrar el tiempo de utilización de los servicios expuesto y de la búsqueda de ahorrar lo mayor posible energía eléctrica.

Se observara como el sistema de alimentación eléctrica del sistema de alumbrado dará alimentación a los equipos según uniones realizadas por personal calificado de la misma empresa eléctrica hacia los postes WIFI de los AP.

Como se observa en la imagen 3.9 donde uno de los puntos de red de cámaras que dan control en el parque por vía IPV4 del tipo cableado RJ45 cat 5 dentro de canaletas y tubos que aíslan

a los cables del exterior y viajan dentro de uno de los postes eléctricos instalados, dan la idea de la aplicación del proyecto, con la instalación de los AP en cada uno de los puntos del espectro especulado para la señalización podríamos obtener muchas facilidades en lugares que ya tienen implementaciones similares.

Se pretende dar un método de Backup a los dispositivos AP mediante cableado de cat 6 que viaje paralelo a los de cat 5 de las cámaras instaladas según lo mostrado a continuación en la figura 4.27.

Figura 4. 27 Postes WIFI y postes de alumbrado eléctrico más cámaras

Se considera aplicar un sistema de UPS como implementación de redundancia eléctrica activable para los AP y demás equipos en momentos de suspensión eléctrica por apagones. Este sistema será adaptable y auto convergente con el sistema eléctrico del sector a implementar el proyecto.

La descripción de los equipos UPS se dará en los anexos correspondientes al igual que otros elementos adicionales de mucha importancia. La forma de los postes de alumbrado será distinta a los de WIFI y darán apoyo a la implementación

4.12 ENCUESTA DE ACEPTACIÓN PROYECTO WISP IPV6

Análisis urbano fijado frente a la necesidad de la utilización de los medios de la nube para los usuarios finales a lo que se espera con este proyecto se tome la consideración de centralizar el uso y necesidad de la web a lo que estas encuestas revelaron las principales actividades de los internautas a los que se plantea en la tabla 4.1 un margen de actividad por categorías:

Tabla 4.2 Tabla comparativa de uso de internet para diferencias de necesidades

Categoría	Actividad	Porcentaje
Social	Enviar/recibir e-mails	75%
Búsqueda	Realizar investigaciones personales	68%
Entretenimiento	Descargar músicas	51%
Negocios	Buscar trabajo	13%

La nube en cuestión de tiempo ha evolucionado según las necesidades y actividades recurrentes de los usuarios y los programas que estos utilizan al día, por lo que se procura incentivar a los usuarios mediante un portal de bienvenida cuando ingresen a la web compartida de IPV6 WISP con la utilización de medios, que se encuentran hoy disponibles en la nube sin necesidad de instalación en equipos, como lo podremos ver en la figura 4.28:

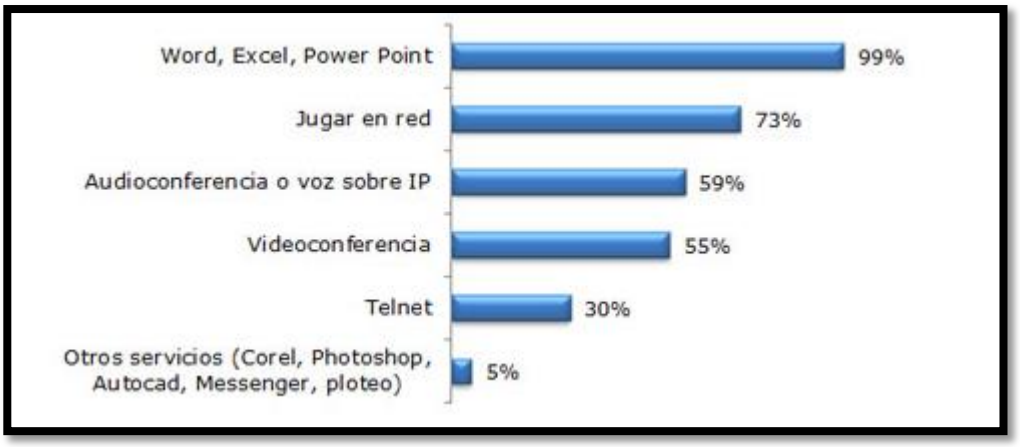


Figura 4. 28 Grafica de porcentaje de uso de datos y servicios

IPV6 revela que la mayoría de los servicios mostrados en la nube y compatibles con IPV4 son de mejor respuesta con IPv6, a lo que en una encuesta a los usuarios sobre el agrado de poder dar permisibilidad para la implementación del proyecto en

parques de su sector a lo que, según se pudo apuntar en la figura 4.29, mostramos sus respuestas y opiniones:

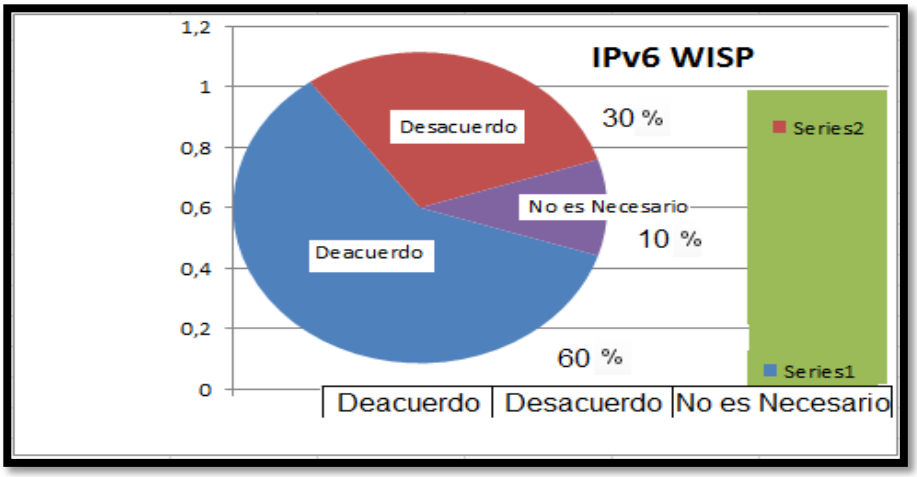


Figura 4. 29 Resultados estadísticos a la comunidad de entre ríos

CAPÍTULO 5

5. IMPLEMENTACIÓN

5.1. ESTRUCTURA DEL DISEÑO PROPUESTO WISP IPV6

La figura 5.1 muestra el diseño propuesto WISP para el acceso a internet en un parque.

- Servidor DHCPv6: el cual tiene como tarea asignar las direcciones IP [34].

- Router inalámbrico interno: se encontrara dentro de la estación de trabajo, servirá como medio de conexión para el administrador de red, para poder verificar cualquier incidencia.

- Una antena sectorial: el cual servirá de medio de interconexión para los puntos de accesos distribuidos en toda el área donde se vaya a implementar la solución.

- Puntos de acceso: equipos encargados de brindar conexión a los usuarios finales.

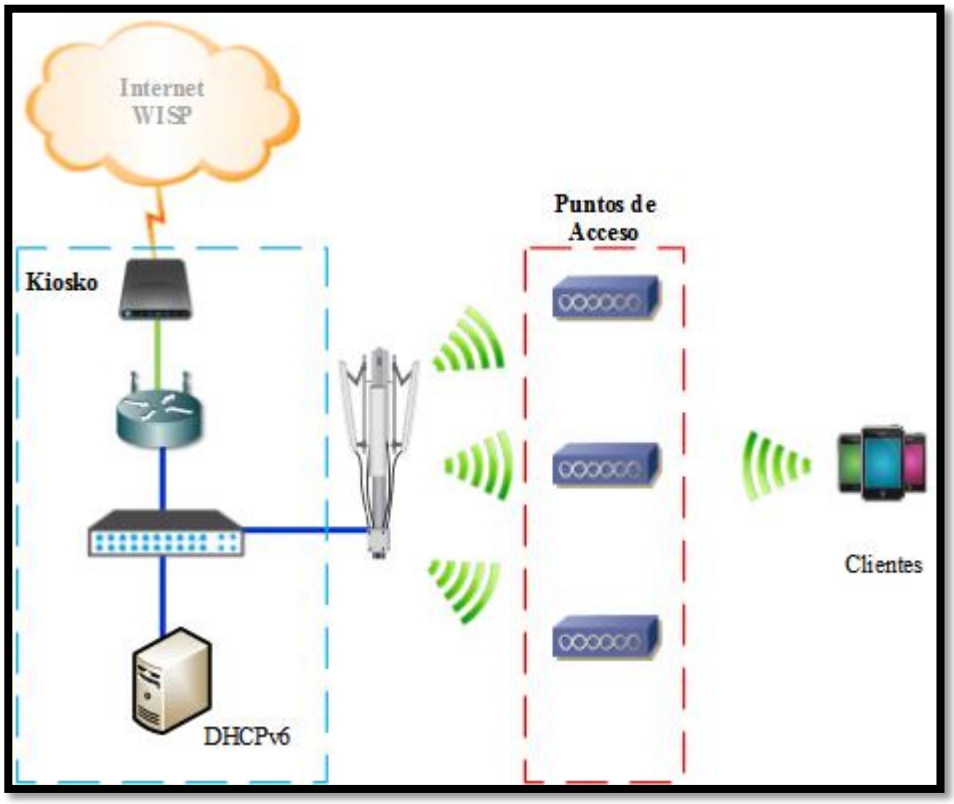


Figura 5 1 Diseño lógico red de la infraestructura WISP

5.2. PRUEBAS A REALIZAR

Las pruebas realizadas en el sitio contaron con la interconexión de un cliente hacia la red WISP, para comprobar el funcionamiento de la implementación y sus posibles fallos. En la tabla 5.1 se muestra el direccionamiento IPv6 y su prefijo de red el cual se tomó para realizar las respectivas pruebas.

Tabla 5.1 Direccionamiento IPV6 y Gateway en servidores y Routers

Nombre	IPV6	Gateway
Prefijo IPV6	fdad:569a:a785:1::/64	
Servidor DHCP	fdad:569a:a785:1::1	fdad:569a:a785:1:c2a0:bbff:fef5:b1518
Router	fdad:569a:a785:1:c2a0:bbff:fef5:b158	

En este caso como parte de las pruebas se utilizó un router inalámbrico el cual servirá de medio de comunicación entre los clientes y el servidor DHCP.

El servidor fue configurado con una IPV6 estática, ya que este cumplirá el rol de DHCP, y asignara las direcciones a los múltiples usuarios en la red, la figura 5.2 muestra la configuración respectiva en la tarjeta de red.

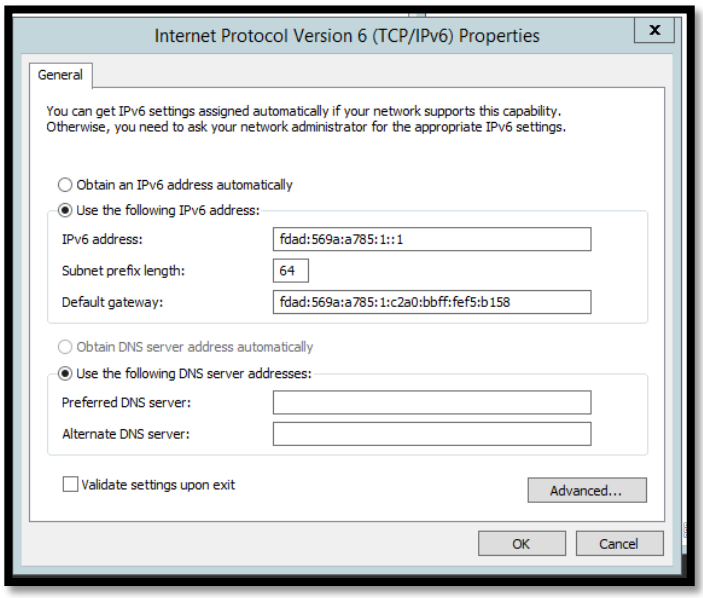


Figura 5 2 Configuración IPV6 en el Servidor DHCP

Una vez asignada la dirección IP en el servidor, se configura el rol DHCPv6, similar a IPV4, con la diferencia de que con IPV6 se tendrá un rango mucho mayor de direcciones IP´s. En la imagen 5.3, se muestra el servidor en funcionamiento, el cual le ha asignado una dirección IP a un cliente.

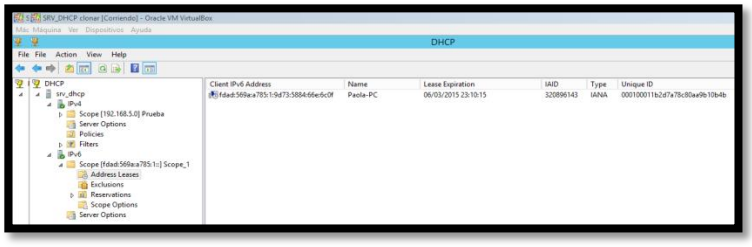


Figura 5 3 Funcionamiento del Servidor DHCPv6

En la figura 5.4, se puede observar la dirección IP de una estación de trabajo, asignada por el servidor.

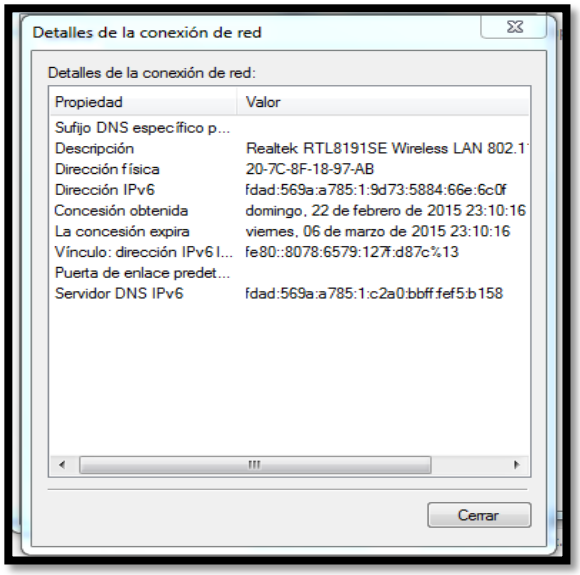


Figura 5 4 Funcionamiento del Servidor DHCPv6

Así como en IPV4, en IPV6 se puede utilizar programas para el monitoreo constante de la red, la potencia de la señal de red, el canal en el que trabaja el punto de acceso, el tipo de seguridad, su SSID y demás parámetros que son de mucha utilidad para el administrador de red.

En la figura 5.5 se muestra el software InSSIDer usado para comprobar la potencia y el estado de la red inalámbrica a la cual los clientes se van a conectar.

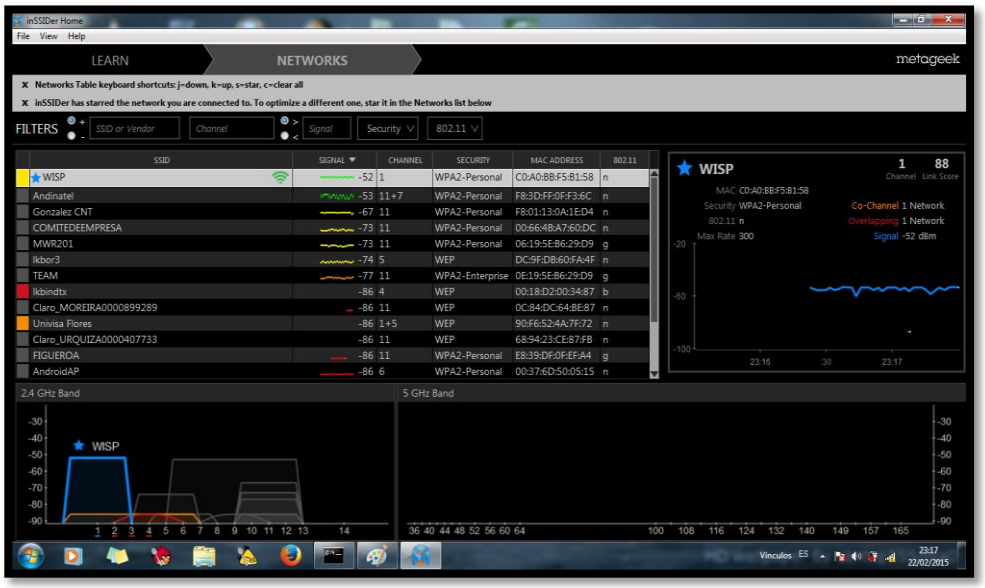


Figura 5 5 Software InSSIDer usado para comprobar la potencia y el estado de la red inalámbrica

5.3. GESTIÓN DE RED, ACCESOS Y RECURSOS IPV6

La gestión de red está compuesta por varios parámetros los cuales permiten tener un conocimiento más específico de lo que está pasando en la red y así poder dar una oportuna solución a cualquier incidencia que suceda. Para la solución propuesta de la red WISP se obtendrá información de los siguientes parámetros de gestión analizados en capítulos anteriores:

- Monitoreo:
- Configuración.
- Topología.
- Gestión de incidencias.
- Seguridad de red.

Se toma en consideración la importancia de la seguridad con respecto al acceso de los recursos compartidos, esto quiere decir que ningún usuario conectado en la red pueda ver o acceder a la información de otro usuario por lo que se plantea el uso de políticas de acceso a la red.

5.4. REDUNDANCIAS Y PLAN DE CONTINGENCIA IPV6

En toda infraestructura de red se debe implementar un plan de contingencia para asegurar la disponibilidad de red en el caso de algún incidente a nivel físico o lógico. La figura 5.6 muestra los elementos usados para un plan de contingencia en la infraestructura de red en caso de existir algún fallo en los equipos de red.

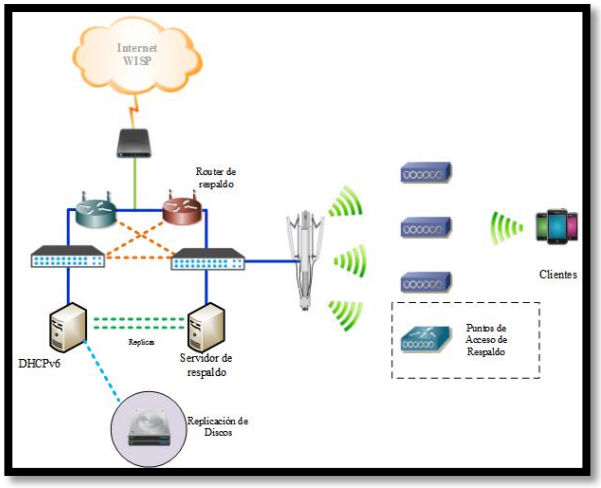


Figura 5 6 Diseño de red: Plan de contingencia.

5.5. FILTROS TCP/UDP

Según lo aprendido en clases de CCNA sobre la utilidad de los filtros TCP UDP e IP, que también van de la mano con la parte de accesos y recursos, se analiza la importancia del por qué no dejar a un lado el uso de los filtros tanto en IPV4 como en IPV6 como veremos en la figura 5.7 al mostrarnos la trayectoria del paquete [12].

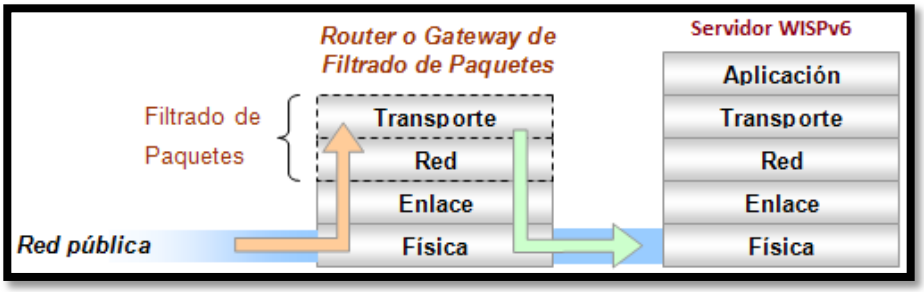


Figura 5 7 Separación de tráfico de paquetes TCP/UDP/IP

5.6. SISTEMA DE SEGURIDAD DE IPV6 VÍA WIFI

Los Equipos a implementar para el despliegue de la red WISP contarán con sistemas de seguridad configurables de manera automática o manual y con una conectividad en paralelo con una DMZ que contendrá la lista de usuarios unidos a la red y de un sistema de control de antivirus básico puesto que el proyecto se desplegará en un área libre al público.

La seguridad a proteger según IPV6 se da a manera de claves generadas por negociantes donde los equipos y dispositivos trabajan en conjunto para generar las claves y sus respectivas encriptaciones según las normas del protocolo IPV6. Se consideró un artículo en cuestión donde a fiel texto menciona lo siguiente respecto al proceso de tramitación de la clave de seguridad:

Para enviar un mensaje autenticado, el equipo fuente, primero construye un datagrama que contiene todos los encabezados IP y la carga útil; después, reemplaza los campos que pueden cambiarse por 0 (por ejemplo, el campo Hop limit [Límite de saltos]).

El datagrama se completa con 0 para convertirse en un múltiplo de 16 bytes. De manera similar, la clave secreta utilizada también se completa con 0 para que se convierta en un múltiplo de 16 bytes. Entonces, se calcula una suma de comprobación del cifrado después de la concatenación de la clave de seguridad completa, del datagrama completo y, nuevamente, de la clave de seguridad completa.

El encabezado de autenticación consta de 3 partes. La primera tiene 4 bytes que especifican el número del encabezado siguiente, la

longitud del encabezado de autenticación y 16 bits cero. La segunda define el número clave de 32 bits. La tercera contiene la suma de comprobación del cifrado (con MD5 o cualquier otro algoritmo). El destinatario utiliza el número clave para encontrar la clave secreta. El valor completo de la clave secreta se agrega antes y después de que se complete la carga útil, los campos de encabezados variables eliminan sus ceros, y después se calcula la suma de comprobación del cifrado.

Si el resultado del cálculo es equivalente a la suma de comprobación del cifrado contenida en el encabezado de autenticación, el destinatario puede estar seguro de que el datagrama realmente proviene de la fuente con la que comparte la clave secreta. También se asegura de que el datagrama no se haya falsificado sin su conocimiento.

Para los datagramas que deben enviarse de manera secreta, se debe utilizar el encabezado de extensión carga útil cifrada. Este encabezado comienza con un número clave de 32 bits seguido por la carga útil cifrada.”[K]

5.7. MARCO DE EVALUACIONES.

Durante la práctica se analizaron varios posibles y constantes errores de conectividad que se resolvieron para poder dar con la implementación según un campo de laboratorio provisional montado, las prácticas que votaron error en las configuraciones que se hicieron en el DHCP y los equipos routers o AP, son errores que nos permitieron en las pruebas desarrolladas analizar y evaluar parámetros como:

Conectividad de equipos, conectividad de dispositivos, conectividad de servidor y seguridad de control de acceso y firewall. Errores comunes que se les podría presentar a los usuarios al conectarse a las redes WIFI, tal como no ver la red hasta que por “a” o “b” motivo figuren como conectados pero sin poder entrar a internet, nada que sea complejo o difícil de investigar y resolver a lo que al final se les dio una atención y se le resolvieron.

a) **Evaluación de tráfico en dispositivos móviles.**

   Según el ancho de banda configurado por los parámetros adquiridos con el ISP que nos brinda conectividad directa a IPV6 siendo disponible a futuro en Ecuador, tendremos que analizar 2 factores entre un análisis de resultados con

dispositivos móviles, donde una comparativa nos dará luz verde a trabajar y el control de error(es) para la conexión exitosa a la red [9].

En dispositivos móviles que soportan IPV6 (celulares, laptops, tabletas) en los cuales la red es más rápida o más lenta, notamos una diferencia de fluidez de paquetes, permitiendo el análisis del tráfico, es decir, si en un dispositivo portátil la red es rápida o aceptable al usuario, sus paquetes de video, voz y datos están dentro del considerado tráfico normal y controlado, pero a diferencia de celulares y tabletas que no se someten a muchos campos de seguridad, es más rápido porque no implica tanto permisos ni aplicativos, en otras palabras se pone en descubierto solamente tráfico de datos que no dialoga con parámetros y permisos, razón por la que se evidencio que en celulares el tráfico de datos es más ligero y rápido que en las portátiles.

b) Muestreo estadístico y observaciones.

El desempeño de las múltiples muestras en 4 APs que se pudieron efectuar en el laboratorio con la conectividad WISP

IPv6 en un área donde la comunicación era libre para la población como se determinó en su momento, se obtiene entre las fechas finales del mes de abril del año 2015 los siguientes resultados dados en la tabla 5.6:

Tabla 5. 6 Análisis con Tráfico de Datos

Noción Estadística de los Valores Totales

	kB	MB	GB
Media	277.6	**133.6**	**1.8**
Mediana	118.5	70.3	1.7
Moda	0	142.9	1.3
Mínimo	1.4	1.5	1.0
Máximo	809.5	996.5	3.8
Desviación Estándar	311.95	194.50	0.61
Varianza	97311.31	37829.5	0.4

En la siguiente tabla 5.7 tendremos el resultado de los diferentes tipos de datos con los cuales se trabajará en las muestras y en las observaciones para obtener un punto de criterio y una confiabilidad cercana.

Tabla 5. 7 Agrupación de Datos Para Muestras

Muestras Agrupadas y Ordenadas de Datos de los 4 APs							
B / 8		**kB / 1024**		**MB / 1024**		**GB**	
400.0	B	1.4	kB	1.5	MB	1.0	GB
548.0	B	14.2	kB	1.7	MB	1.1	GB
		25.5	kB	2.0	MB	1.2	GB
		59.3	kB	2.4	MB	1.2	GB
		325.8	kB	3.1	MB	1.3	GB
		435.3	kB	22.1	MB	1.3	GB
		709.1	kB	27.7	MB	1.3	GB
		809.5	kB	27.8	MB	1.4	GB
		118.5	**kB**	31.2	MB	1.4	GB
				46.8	MB	1.5	GB
				58.6	MB	1.6	GB
				62.0	MB	1.6	GB
				68.3	MB	1.6	GB
				70.3	MB	1.7	GB
				80.8	MB	1.7	GB
				97.3	MB	1.8	GB
				141.0	MB	1.8	GB
				142.9	MB	1.8	GB
				142.9	MB	1.9	GB
				145.7	MB	2.1	GB
				159.9	MB	2.1	GB
				185.6	MB	2.2	GB
				210.5	MB	2.3	GB
				223.6	MB	2.4	GB
				228.1	MB	2.9	GB
				248.5	MB	3.8	**GB**
				442.0	MB		
				996.5	MB		
				2.4	**MB**		

Para esta muestra en la siguiente figura 5.8 se detalla el constante uso de los datos, sean estos en B, kB, MB, y GB con la que los dispositivos móviles de usuarios finales tienden a conectarse o a negociar dentro de las muestras recogidas de los diferentes AP.

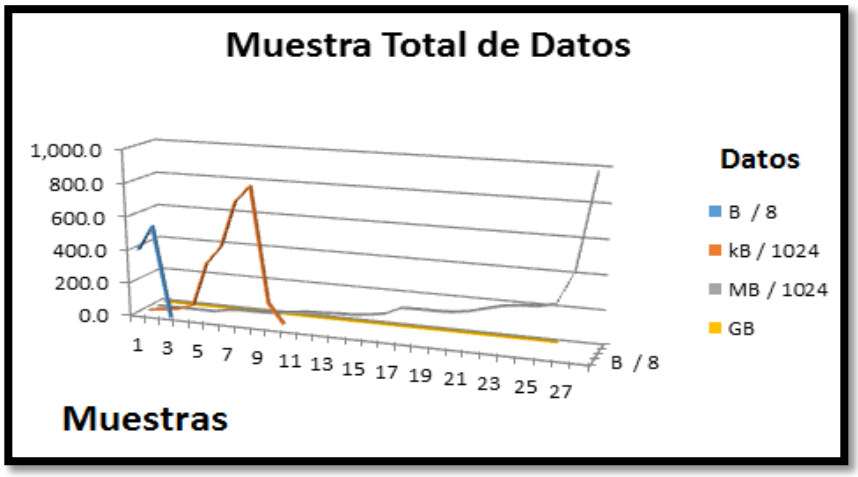


Figura 5 8 Muestras de consumos de Datos en dispositivos móviles

Veremos que el consumo en GB por separado nos da un resultado mostrado en la tabla 5.8 al que se le sometió a cálculos de media, mediana, moda, max, min, varianza y desviación estándar para poder calcular la confianza:

Tabla 5. 8 Muestra Total Calculada de los Datos en GB

Noción estadística de los valores Totales en GB	
Cálculos	GB
Media	1.8
Mediana	1.7
Moda	1.3
Mínimo	1
Máximo	3.8
Desviación Estándar	0.61
Varianza	0.4

La constancia de la noción estadística de los valores totales en GB según analizamos en la tabla anterior refleja una línea optima ante la graficación de su media, mediana y moda como veremos en la figura 5.9:

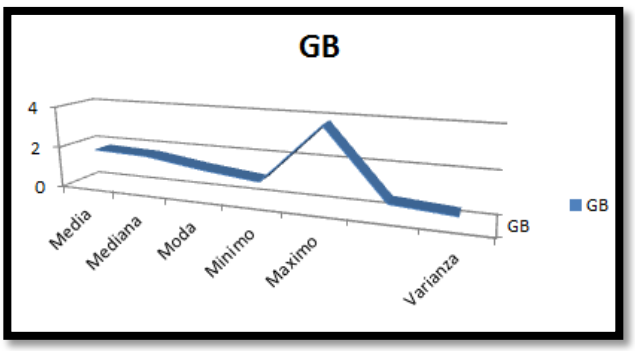


Figura 5 9 Estadísticas Aplicadas a Datos en GB

Para el cálculo del número de observaciones de los AP el cual es muy importante a considerar para el cálculo final de la

confiabilidad, se aplica la fórmula de la figura 5.10, donde tenemos que:

n = Tamaño de la muestra que deseamos calcular.

n' = Número de observaciones del estudio preliminar.

Σ = Suma de los valores

x = Valor de las observaciones.

40 = Constante para un nivel de confianza de 94,45%

$$n = \left(\frac{40\sqrt{n'\sum x^2 - \sum(x)^2}}{\sum x}\right)^2$$

Figura 5 10 Formula del cálculo de la Observación

Para esto, la resolución con los datos obtenidos la tenemos en la figura 5.11:

$$n = \left(\frac{40\sqrt{4(1111) - (63)^2}}{63}\right)^2$$

$$n = \left(\frac{40\sqrt{475}}{63}\right)^2 = \left(\frac{40(21.79)}{63}\right)^2$$

$$n = \left(\frac{871.77}{63}\right)^2 = (13.83)^2 = 191.26 \cong 192$$

Figura 5 11 Remplazando valores para la formula

A continuación, en la tabla 5.9 tenemos los resultados para la obtención de las observaciones que nos servirán para el cálculo de la confiabilidad de las muestras recolectadas y así revelar que tan confiable es el proyecto.

Tabla 5. 9 Numero de Observaciones para el cálculo de Confianza

Observaciones			n
AP 1	14	196	**192**
AP 2	25	625	
AP 3	11	121	
AP 4	13	169	
Total Σx	**63**		
Total Σx²		**1111**	
Muestras n'	**4**		

Para estos resultados veremos el reflejo de las líneas en la figura 5.12 de los campos de “x” y de “x²” según su trabajo en los diferentes AP de los que se obtuvieron las muestras:

Figura 5 12 Reflejo de las Observaciones como muestras

Para ver el nivel de confianza tenemos que estimar las características confiables del fenómeno investigado; donde deberemos considerar la probabilidad de que ocurra el evento (p) y la de que no se realice (q); siempre tomando en consideración que la suma de ambos valores p + q será invariablemente igual a 1, cuando no contemos con suficiente información, le asignaremos p = 0.50 q = 0.50. Para ello tenemos en la figura 5.13 a consultar los valores de "Z" y de "e" según el nivel de confianza con el que se calculen las muestras u observaciones [39]:

TABLA DE APOYO AL CALCULO DEL TAMAÑO DE UNA MUESTRA POR NIVELES DE CONFIANZA

Certeza	95%	94%	93%	92%	91%	90%	80%	62.27%	50%
Z	**1.96**	1.88	1.81	1.75	1.69	1.65	1.28	1	0.6745
Z^2	3.84	3.53	3.28	3.06	2.86	2.72	1.64	1.00	0.45
e	0.05	0.06	0.07	0.08	0.09	0.10	0.20	0.37	0.50
e^2	0.0025	0.0036	0.0049	0.0064	0.0081	0.01	0.04	0.1369	0.25

Figura 5 13 Tabla de porcentajes de Confianza y de error [39]

Las siguientes formulas de la figura 5.14 nos revelaran el modo más preciso de ver la confiabilidad de nuestro proyecto WISPIPv6.

Población infinita	Población Finita
$n = \frac{p \bullet q}{e^2}$	$n = \frac{Z^2 p \bullet q \bullet N}{Ne^2 + Z^2 p \bullet q}$
Cuando no se sabe el número exacto de unidades del que está compuesta la población.	Cuando se conoce cuántos elementos tiene la población
En donde: **Z** = nivel de confianza. **p** = Probabilidad a favor. **q** = Probabilidad en contra.	**N** = Universo **e** = error de estimación. **n** = tamaño de la muestra

Figura 5 14 Formulas de confianza aplicada

A lo cual tenemos como resultados los datos que se obtienen en la siguiente tabla 5.10 del nivel de confianza:

Tabla 5. 10 Aplicación de Niveles de Confianza

Nivel de confianza		
%	**Z**	**e**
90	45.18	5
95	122	6.4

El nivel de confianza mostrado a continuación en la figura 5.15 donde notaremos la evaluación con los 2 valores diferentes de confianza en “Z” y los de errores en “e” para ver el más cercano a la realidad a lo cual se ha considerado los siguientes resultados:

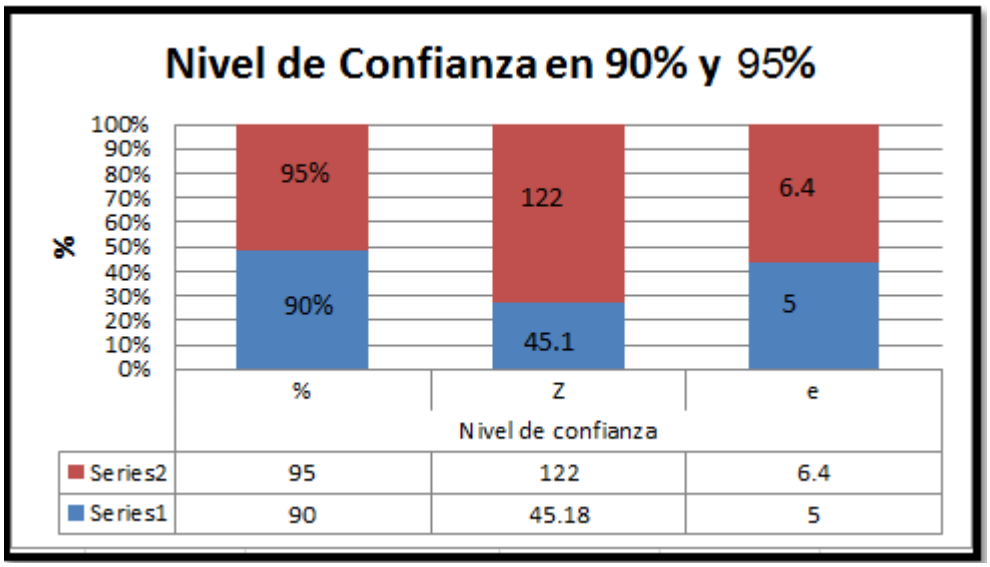


Figura 5 15 Resultados Gráficos del Nivel de Confianza Obtenido

Por lo tanto tenemos estos datos con la obtención de confiabilidad usando muestras aleatorias según cálculos de observaciones con las 2 evaluaciones tanto para el 90% de confianza y un 10% de error, o con un 95% de confianza y un 5% de error, para el cual es más factible el cálculo con el 95% de confianza.

CONCLUSIONES

1. En base al estudio realizado para este proyecto, podemos dar a conocer uno de tantos beneficios que nos ofrece internet por vía IPV6, como es el uso de un ya establecido protocolo seguro que favorece de gran manera a las empresas u organizaciones al optimizar sus recursos informáticos, generándoles reducción de costos en la mayor parte implementada del cuarto del rack.

2. Podemos concluir que el nuevo protocolo se ha convertido en un recurso de gran utilidad para las todas las organizaciones y personas naturales, por el motivo que este mismo nos ayuda a que las empresas y demás entidades fijen una meta por la era de la comunicación, a lo que optarían por el protocolo investigado, y a su vez no tengan que preocuparse por una demanda gigante de procesos administrativos de la red, tal como lo era en IPV4 y en su mayor noticia se cuenta con la

disponibilidad de un número muy grande de nuevas IPs para su utilización en la nube, sea estas independientemente por usuario o por dispositivo.

3. IPV6 tiene las mismas funcionalidades e incluso mejoras con sus funciones automatizadas y siendo un protocolo pensado primeramente en la seguridad según su diseño y estructura, a diferencia de IPV4 que fue diseñado solo como comunicación. Adicionalmente se puede realizar video llamadas, mensajería y transferencia de datos sean de manera investigativa o por implementación.

4. Como beneficio para los usuarios aleatorios pertenecientes a la comunidad, tendrían acceso en parques a internet con sus dispositivos que soportan IPV6 para que la concientización del uso del protocolo comience desde un lugar cercano a casa teniendo de ejemplo lo implementado como proyecto WISPv6 en el mismo parque de su comunidad.

5. La implementación del proyecto WISPv6 en esta área de recreación urbana o parque solo es la primera fase de un proyecto de convergencia más ambicioso y de grandes dimensiones.

6. La responsabilidad de IT debe garantizar que sus redes funcionen de manera fiable, predecible y consistente. El aumento de los equipos que demandan una IP y se manejan bajo tráfico sumamente pesado en ciertas ocasiones, pide casi obligadamente la predisposición de un técnico de IT para el correspondiente monitoreo y control de la red WISPv6 y de sus nodos.

RECOMENDACIONES

1. Como la tecnología avanza diariamente se estima que en este proyecto haya mejoras constantes; por recomendaciones a futuro para el total provecho de las personas que requieran por su agrado desarrollar el proyecto en base a modificaciones adaptables a las tecnologías que se puedan brindar con el pasar de los años y el perfeccionamiento de en las transmisiones de tipo seguro y en la minimización de errores.

2. Debemos conocer cuáles son las limitaciones de la red que implementemos y cuáles son sus próximas evoluciones o mejoras según el avance de la tecnología, lo que comprenderá la capacidad y calidad de tráfico e infraestructuras de switching con el soporte a IPV6 ante la futura implementación de nuevos equipos.

3. Es importante que nuestro ISP cuente con conexiones directas al protocolo IPV6 o al menos un modo adaptado al 6to4, aplicando esto sería necesario no pasar por alto la revisión de las políticas generalizadas del proyecto y establecer los procedimientos adecuados para los usuarios móviles que posee la urbanización como un solo sistema fiable, dado el caso que se decida plantearlo en un escenario más administrativo.

4. Es importante sujetarse a un estándar de convergencia para futuras actualizaciones, donde el personal de IT que se encuentre trabajando con este servicio directa o indirectamente, vea la migración de alguna implementación paralela con el anterior protocolo con facilidad por la familiarización con el proyecto WISPv6.

5. Como una última recomendación se plantea que para el uso de este servicio en su máxima plenitud se debe contar con una conexión de internet estable a IPV6 así como un profundo análisis de los pros y los contras de la red donde se implementaría el servicio, o en ausencia del mismo analizar el margen estructural de las redes WAN de IPV6 según los rangos de la frecuencia de la red.

BIBLIOGRAFÍA

[1] Manuel, Securing and Enhancing Routing Protocols for Mobil Networks, 09/05/2007 Virtual, http://goo.gl/epYvu7

[2] Published by: Hugo Arriagada Albarran on Jun 17, 2010 https://es.scribd.com/doc/33193823/7/Clasificacion-de-las-Redes-Inalambricas

[3] Camilo Astudillo, Página web, Redes MESH, 2011-2012 vi: Juan Carlos Jeldes http://wiki.ead.pucv.cl/index.php/Red_MESH

[4] Published by Tony Smith, 5 Dec 2013, BLUETOOTH Smart to tap IPV6-powered Internet of Things, http://www.theregister.co.uk/2013/12/05/BLUETOOTH_upgraded_for_IPV6powered_internet_of_things/

[5] Published by: Tulio Briceno on Oct 17, 2011 Copyright https://es.scribd.com/doc/69195852/Red-Por-INFRARROJOS

[6] Published by: Grace González: Universidad de Panamá y Universitaria Octavio Méndez Pereira Revista http://goo.gl/8lgWRO

[7] Stephen Shankland. «Why AT&T should buy you a femtocell». 2010-03-29. CNET News. Archivado desde el original el 2013-03-08. http://es.wikipedia.org/wiki/FEMTOCELDA

[8] Fundación Wikimedia, Página web, REDES MESH, 2011-2015 vi: Contribuyentes http://es.wikipedia.org/wiki/WISP

[9] LACNIC. (2012). El Tráfico IPV6. Septiembre 2014, de NIC México Sitio web: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

[10] J Coellar Solórzano. (2013). PROPUESTA PARA LA TRANSICIÓN DE IPV4 A IPV6. Noviembre 2014, de Imaginar.org Sitio web: http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

[11] Skysat & MikroTik RouterOS. (2012). Un WISP 100% Automatizado. 2015, de ryohnosuke Sitio web: http://goo.gl/91LFhx

[12] Textos científicos IT. (2006). CONTROL DE ACCESO Y FILTROS. 2015, de Textos cientificos.com Sitio web: http://goo.gl/jQZRNu [Filtros TCP/UDP]

[13] Elizabeth, a Review of Current Routing Protocols for Mobile WIRELESS Networks, 30/04/2007.

[14]. Mohapatra, Prasant, Ad Hoc Networks Technologies and Protocols, Springer Science, Boston 2005.

[15] Published by: Explicacion de la serie CEM on Oct 10, 2010 Copyright http://www.emfexplained.info/spa/?ID=25184 [Imagen 2.1]

[16] Droms, R.; Bound, J.; Volz, B.; Lemon, T.; Perkins, C.; Carney, M. (2003) "Dynamic Host Configuration Protocol for IPV6 (DHCPv6)", IETF, Instalación de Software http://goo.gl/aO3wEH [Punto 4.10]

[17] Published by: LACNIC by: Sofia Silva: transición http://www.labs.lacnic.net/site/sites/default/files/IPV6_1hour_ES.pdf [Imagen 2.9 y 2.10]

[18] Published by: wikipedia. (2012). MD5. 15-12-2014, de Wikimedia Sitio web: http://es.wikipedia.org/wiki/MD5 [Punto 2.1.3]

[19] Nico Van Haute. (2012). Autenticado de Paquetes IPV6. Septiembre 2014, de ccmbenchmark.com Sitio web: http://es.kioskea.net/contents/268-protocolo-ipv6 [k]

[20] Fundación Wikimedia.(2011). Secure Hash Algorithm. 25 sep. 2014, de wikipedia.org Sitio web: http://es.wikipedia.org/wiki/Secure_Hash_Algorithm [2.1.3] [SHA-1]

[21] Fundación Wikimedia. (2012). RIPEMD-160. 18 abril del 2013, de wikipedia.org Sitio web: http://es.wikipedia.org/wiki/RIPEMD-160 RIPEMD-160 [2.1.3] [RIPEMD]

[22] Jordi Pallet Martínez y Alberto Cabellos. (Enero del 2014). Campos IPV6. 2015, de 6sos.org Sitio web: http://goo.gl/RXtTh [2.1.4]

[23] Jim Bound, Laurent Toutain, Octavio Medina, Francis Dupont, Hossam Affi, Alain Durand. Mecanismo DSTM. Diciembre 2014, de www.IPV6.rennes.enst-bretagne Sitio web: http://www.ietf.org/proceedings/54/slides/ngtrans-7.pdf [Mecanismo DSTM]

[24] Carlos A. Castillo Medina, Felipe Forero Rodríguez. (Junio 2013). Mecanismos de transición de IPV4 a IPV6. Diciembre del 2014, de

www.scielo.org.co Sitio web: http://www.scielo.org.co/scielo.php?pid=S0123-921X2013000200010&script=sci_arttext [Movilidad IPV6]

[25] Marco Antonio Arenas Porcel. (Noviembre de 2011). Características y Protocolos de enrutamiento IPv6. Enero 2015, de Academia Cisco - Slideshare.net Sitio web: http://es.slideshare.net/MarcoAntonioArenasPorcel/i-pv6-conferenceintro [Imagen 3.4 y 3.5]

[26] Leo Prieto, Michael Diamond. (2007). WIFI 802.11g/n más rápido y más lejos que nunca. 2015, de fayerwayer.com y Wi-Fi Alliance, Sitio web: https://www.fayerwayer.com/2007/05/80211n-wi-fi-mas-rapido-y-mas-lejos-que-nunca/ [Imagen 3.1]

[27] Sonnettech, Aria extremen pci. (2008). Estándares a Considerar en IP/WIFI. 2015, de Aria Extreme.com Sitio web: http://www.sonnettech.com/product/ariaextremenpci.html [Punto 3.1]

[28] Mr. Gordon Moore, Dr. Jahangir Alam. (2002). Movilidad de IPV6. 2015, de tutorial point.com Sitio web: http://goo.gl/4bX6MT [TP] [Punto 3.2] [Imagen 3.6]

[29] Portalipv6. (2000). Países Latinoamericanos que implementan IPV6. 2015, de Lacnic Sitio web: http://portalipv6.lacnic.net/quienes-implementan/

[30] Ing. Fabián Carrasco Castro... (2008). Internet Comercial IPV6. 2014, de CEDIA Sitio web: https://www.cedia.org.ec/internet-comercial [C] [Punto 4.7] [Imagen 4.13 hasta 4.19]

[31] Érica Ordoñez Bravo. (2008). Diseño de una red inalámbrica con tecnología WIMAX. 2014, de Espol - Dspace Sitio web: http://www.dspace.espol.edu.ec/bitstream/123456789/16136/1/D-39968.pdf [D] [Anexo]

[32] Netkrom, Wavekrom y Airnet. (2002). Configuration e Instalación de Equipos Netkrom. 2015, de Netkrom Sitio web: http://www.netkrom.com/legado/support/manual/ISPAIR_54Mb_CPE_500_900_Quick_Configuration_Guide.pdf [figuras 4.24 y 4.25] [Equipos Netkrom]

[33] Ekahau IT (WIFI). (2008) Ekahau Site Survey Software. 2015, de Ekahau Sitio web: http://goo.gl/f2p80I [Punto 4.8 literal D] [E]

[34] Tknika, Google Site. (2008). DHCPv6 Windows 2008 Server. 2015, de Bideoak & Google Site Sitio web: https://sites.google.com/site/tknikaipv6/1-3-1-DHCPv6-server-windows-2008 [Anexos Windows Server] [S]

[35] UPS SmartOnline & Tripp.Lite. (2010). UPS SmartOnline. 2015, de Tripp.Lite Sitio web: http://www.tripplite.com/products/series/sid/934 [Punto 4.10 literal A] [up]

[36] Icelcom. (2007). Pararrayos para las torres. 2015, de Icelcom Sitio web: http://www.incelcom.com/servicios.html [Punto 4.10 literal A figura 4.26] [PR]

[37] Polo 21 & Windows. (Septiembre de 2009). Servidor web (IIS). Enero del 2015, de Microsoft Sitio web: https://goo.gl/CDk4S3 [Punto 4.6 IIS] [IS]

[38] Polo 21 & Windows. (Septiembre de 2009). Servidor web (IIS). Enero del 2015, de Microsoft Sitio web: http://support.microsoft.com/kb/323972/es [Configuración IIS] [CF]

[39] Mario Suarez. (2012). Cálculo del tamaño de la muestra. abril del 2015, de Monografias.com S.A. Sitio web: http://goo.gl/dnIhc [Muestras Estadísticas]

[40] Wikipedia España & Wikimedia. (2000). Anexos Proyecto WISPv6. 2015, de IT - Europa y Latinoamérica Sitio web: http://es.wikipedia.org [Glosario]

[41] Departamento de CVA. ITESM. (2000). Como Hacer una Bibliografía web. 2015, de CVA. ITESM Sitio web: http://goo.gl/UHnueE [Bibliografía]

ANEXOS

- **COSTOS DE EQUIPOS**

Netkrom ISPAIR 54Mb 3.4 to 3.7GHz CPE (ISP-CPE350)	**http://www.vsatplus.net/ispair-54mb-3-4-to-3-7ghz-cpe-long-range-subscriber-15-miles-24km.html**	
W24-17SP90 Sector Panel Antena VPOL	http://www.vsatplus.net/2-3-2-7-ghz-17dbi-90-sector-panel-antenna-vpol-n-female-connector.html	
UPS de Doble Conversión En Línea SmartOnline de 3kVA, 2U en Rack/Torre, tomacorrientes NEMA	http://articulo.mercadolibre.com.ec/MEC-406721421-ups-de-doble-conversion-en-linea-smartonline-de-1000va-800w-_JM http://www.tripplite.com/ups-doble-conversi%C3%B3n-en-l%C3%ADnea-3kva-2u-rack-torre-tomacorrientes-nema-100v-110v-115v-120v-127v~SU3000RTXL2U/	
Computador Intel Core i7-4770 - Cuarta generación - Monitor LED 18.5" HD	http://www.tecnosmart.com.ec/v2/productos/computadora/pcs-de-escritorio/computador-intel-core-i7-basico-intel-puro-6.html	
Funda De Conectores Rj45 Nexxt Categoría 6 Cat6 100 Unidades	http://articulo.mercadolibre.com.ec/MEC-406614504-funda-de-conectores-rj45-nexxt-categoria-6-cat6-100-unidades-_JM	
Bobina De Cable Ftp Blindado Cat 6a Marca Panduit	http://articulo.mercadolibre.com.ec/MEC-406888312-bobina-de-cable-ftp-blindado-cat-6a-marca-panduit-_JM	
Pararrayos, Ionizantes, O De Cebado	http://articulo.mercadolibre.com.ec/MEC-406817437-pararrayos-ionizantes-o-de-cebado-quito-ecuador-_JM http://www.paginasamarillas.info.ec/busqueda/pararrayos	
Router WIRELESS D-link Dir-657 HD Media 1000 Red Wifi IPV6	http://articulo.mercadolibre.com.ec/MEC-406827203-router-wireless-d-link-dir-657-hd-media-1000-red-wifi-ipv6-_JM	
Cisco Sg200-18 Switch Gigabit 16 Puertos + 2 Spf Capa 2	http://articulo.mercadolibre.com.ec/MEC-406790558-cisco-sg200-18-switch-gigabit-16-puertos-2-spf-capa-2-_JM	

EQUIPO	DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
Netkrom ISPAIR 54Mb 3.4 to 3.7GHz CPE	Todo en un dispositivo WIRELESS CPE, Integrated Power sobre Ethernet,Gestión Web y soporte SNMP, Enlaces de datos inalámbrico de alta velocidad (hasta 54 Mbps), Distancia de conexión hasta 15 millas (24km) Firewall , NAT, enrutamiento IP , DHCP, Alto nivel de seguridad con plena cifrado 64 / WEP 128 Atheros XR Chipset	4	500	2000
W24-17SP90 Sector Panel Antena VPOL	Rendimiento banda ancha con polarización vertical, 60 , 90, 120 y 180 °; Tipo N Hembra Conector Integrado y Extremadamente resistente para una larga vida útil en ambientes extremos resistente a la intemperie	3	251	753
Bobina De Cable Ftp Blindado Cat 6a Marca Panduit	BOBINA DE CABLE FTP BLINDADO CAT 6A MARCA PANDUIT	3	350	1050
UPS de Doble Conversión En Línea SmartOnline	UPS de doble conversión, en línea de 1000VA / 1kVA / 800 watts, Salida de 100/110/120V +/-2% a 50/60Hz, alta eficiencia con la opción de modo económico con Tiempo de autonomía ampliable, módulos de batería Hot-Swap, profundidad instalada de solamente 34,3 cm / 13,5	1	350	350
Pararrayos, Ionizantes, O De Cebado	PARARRAYOS IONIZANTES CON COBERTURA DESDE 35 M HASTA 100 M DE RADIO. PUNTAS FRANKLIN DESDE 100 USD. ELECTRODOS ACTIVOS DE COBRE ELECTROLITOCO.	1	450	450
Router WIRELESS D-link Dir-657 HD Media 1000 Red WIFI IPV6	Puertos LAN/WAN 1000Mbps GE con estándar IEEE 802.11b/g/N para 2.4GHz y Soporta DHCP server, DHCP cliente además de Soportar IPV6 y PPPoE en el puerto WAN y Administración por Web Browser.	1	140	140
Cisco Sg200-18 Switch Gigabit 16 Puertos + 2 Spf Capa 2	Inteligencia de QoS integrada para dar prioridad al tráfico sensible a demoras; Seguridad de red integrada como la seguridad de puertos IEEE 802.1X para controlar el acceso a su red; Compatibilidad nativa de IPV6 además de la IPV4 tradicional. http://goo.gl/MiomN4	1	450	450
Computador Intel Core i7-4770 - Cuarta generación - Monitor LED 18.5" HD	MAINBOARD INTEL DB85FL / Gigabyte B85M / ASUS B85 Socket LGA-1150, PROCESADOR INTEL Core i7-4770 3.4GHZ 8MB LGA-1150 Haswell, DISCO DURO 500 GB SATA III 6Gbps Seagate / Samsung / Western Digital, MEMORIA RAM 4GB DDR3 1333mhz Kingston (Con Garantía de por vida), MONITOR LED 18.5" LG - HD 720p	1	800	800
Funda De Conectores Rj45 Nexxt Categoría 6 Cat6 100 Unidades	Fabricados con material termoplástico de alto impacto pueden ser utilizados para aplicaciones de redes, de redes categoría 6. Se pueden utilizar con cables sólidos o multifilar. Cuenta con 8 contactos de bronce fosforoso, bañados con oro y níquel.	1	25	25
			Total	6018

- **GLOSARIO**

IP: Protocolo de Internet, es quien se encarga de la comunicación entre el origen y el destino.

WISP: Acrónimo para WIRELESS INTERNET SERVICE PROVIDER o Proveedor de Servicio de Internet Inalámbrico.

WIMAX: Siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 50 km

WIFI: Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

HOTSPOTS: Es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios en una zona de alta demanda de tráfico de Internet.

QoS: Es el rendimiento promedio de una red de sistemas y telefonías, particularmente el rendimiento visto por los usuarios de la red y se encarga de medir la calidad de servicio de la red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter,etc.

NODOS: En una red de ordenadores cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también es un nodo.

HSCSD: High-Speed Circuit-Switched Data (HSCSD), es una mejora al mecanismo de transmisión de datos de GSM o circuit-switched data (CSD).

CDPD: Celular Digital Packet Data, es una tecnología de transmisión de datos en terminales TDMA, El sistema está basado en la tecnología IBM CelluPlan II, pero desarrollada por Ericsson y descontinuada a finales de los 90, que pretendía mejorar las prestaciones de la existente tecnología celular analógica.

TDMA: La Multiplicación por división de tiempo (Time División Múltiple Access o TDM) es una técnica que permite la transmisión de señales digítales.

IRDA: Infra red Data Association (IrDA), "Asociación de Datos Infra-rojos", define un estándar físico en la forma de transmisión y recepción de datos por rayos INFRARROJOS.

L2CAP: Logical Link Control and Adaptation Protocol (Protocolo de control y adaptación del enlace lógico) es utilizado dentro de la pila de protocolos de BLUETOOTH y se utiliza para pasar paquetes con y sin orientación a la conexión a sus capas superiores incluyendo tanto al Host Controller Interface (HCI) como directamente al gestor del enlace.

HIPERMAN: Estándar creado por el Instituto Europeo de Normas de Telecomunicaciones (ETSI) dirigido principalmente para proveer DSL inalámbrica de banda ancha, cubriendo un área geográfica grande. Se considera una alternativa europea y coreana WIMAX.

DSL: La línea de abonado digital o línea de suscripción digital, “Digital Subscriber Line” (DSL), es una familia de tecnologías que proporcionan el acceso a Internet mediante la transmisión de datos a través de los cables de una red telefónica local.

LDSM: Permite la comunicación de los administradores de red para verificar el estado de funcionamiento del hardware del servidor, reducir al mínimo la probabilidad de inactividad del servidor, restaurar los servidores con mayor rapidez cuando se producen problemas, aumenta la fiabilidad y la disponibilidad y administra servidores de forma remota para un rendimiento óptimo.

DATAGRAMA: Es un paquete de datos que constituye el mínimo bloque de información en una red de conmutación por datagramas, la cual es uno de los dos tipos de protocolo de comunicación por conmutación de paquetes usados para encaminar rutas diversas de dichas unidades de información, entre nodos de una red, por lo que se dice que no está orientado a conexión

IEEE: Institute of Electrical and Electronics Engineers (IEEE) es una asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.

AP: WIRELESS Access Point, conocido por las siglas (WAP o AP), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas.

DBM: Unidad de medida de potencia expresada en decibelios (dB) relativa a un milivatio (mW).

- **INSTALACIÓN DE SISTEMAS**

A. **Configurar un sitio web predeterminado**

Cuando “se instala IIS, está reconfigurado para servir como un sitio de web predeterminado; sin embargo, es aconsejable cambiar algunas de las opciones. Para cambiar la configuración básica del sitio web y para emular los pasos necesarios para configurar Apache por primera vez mediante el archivo de configuración:

a) Inicie sesión en el equipo servidor web como administrador.
b) Haga clic en inicio, seleccione configuración y, a continuación, haga clic en panel de control.
c) Haga doble clic en herramientas administrativas y, a continuación, haga doble clic en administrador de servicios internet.
d) Haga clic con el botón secundario en el sitio web que desea configurar en el panel izquierdo y, a continuación, haga clic en propiedades.
e) Haga clic en la ficha sitio web.
f) En el cuadro descripción, escriba una descripción para el sitio web.
g) Escriba la dirección de protocolo internet (IP) para utilizar para el sitio web o deje el valor predeterminado de todos (sin asignar).
h) Modificar el puerto de protocolo de control de transmisión (TCP) según corresponda.
i) Haga clic en la ficha directorio principal.

j) Para utilizar una carpeta en el equipo local, haga clic en un directorio en este equipo y, a continuación, haga clic en examinar para localizar la carpeta que desea utilizar.

k) Para utilizar una carpeta que se ha compartido desde otro equipo de la red, haga clic en un recurso compartido de otro equipo y, a continuación, escriba la ruta de acceso de red o haga clic en examinar para seleccionar la carpeta compartida.

l) Haga clic en lectura para conceder acceso de lectura a la carpeta (obligatorio).

m) Haga clic en aceptar para aceptar las propiedades del sitio web.

B. **Pasos para configurarlo el portal web.**

Para lo siguiente se necesita seguir una línea de pasos para terminar con la configuración básica pero para nuestro caso será suficiente y podremos escoger lo que mejor nos venga en la parte de la página configurada con su bienvenida:

Inicie sesión en el equipo servidor web como administrador.

Haga clic en inicio, seleccione configuración y, a continuación, haga clic en panel de control.

Haga doble clic en herramientas administrativas y, a continuación, haga doble clic en administrador de servicios internet.

Haga clic en acción, seleccione nuevo y, a continuación, haga clic en sitio web.

Cuando se inicie el asistente para creación de sitios web, haga clic en siguiente.

Escriba una descripción para el sitio web.

Esta descripción se utiliza internamente para identificar el sitio web sólo en el administrador de servicios internet.

Seleccione la dirección IP para el sitio.

Si selecciona todo (sin asignar), el sitio web es accesible en todas las interfaces y todas las direcciones IP configuran.

Escriba el número de puerto TCP para publicar el sitio.

Escriba el nombre de encabezado de Host (el nombre real que se utiliza para tener acceso a este sitio).

Haga clic en siguiente.

Escriba la ruta de acceso a la carpeta que contiene los documentos del sitio web o haga clic en examinar para seleccionar la carpeta y, a continuación, haga clic en siguiente.

Seleccione los permisos de acceso para el sitio web y, a continuación, haga clic en siguiente.

Haga clic en finalizar [38].

- **Comparativas de términos entre Apache y IIS**

Crear un nuevo sitio Web

Para crear un nuevo sitio Web en Apache, debe configurar un host virtual y configurar las opciones individuales para el host.

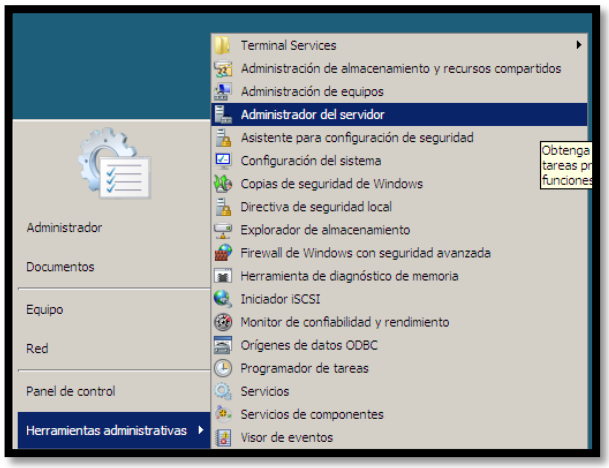
Término de Apache	Término IIS
DocumentRoot	Directorio principal del sitio Web IIS
NombreDeServidor	Encabezado de Host IIS
Escuchar	Dirección IP de IIS y el puerto TCP

En el gráfico anterior se aprecia la igualdad de términos entre Apache y IIS". [CF]

C. Instalación del servidor DHCPv6 para el proyecto WISP v6

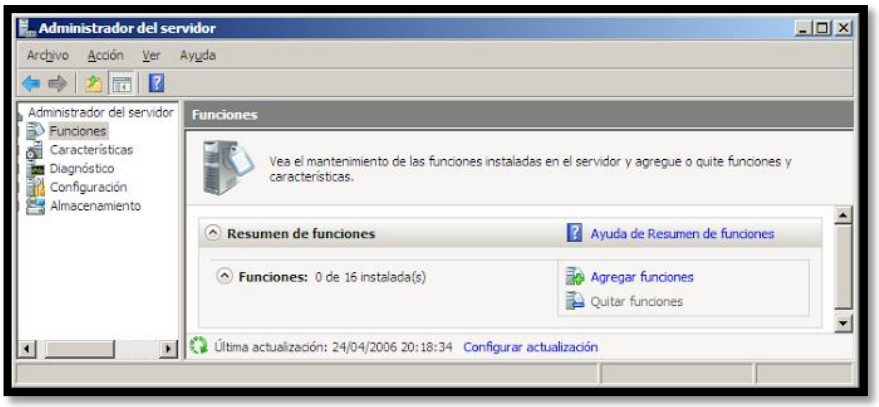
A continuación y para comenzar con la instalación de DHCP deberemos dar los siguientes pasos:

Inicio --> Herramientas administrativas --> Administrador del servidor

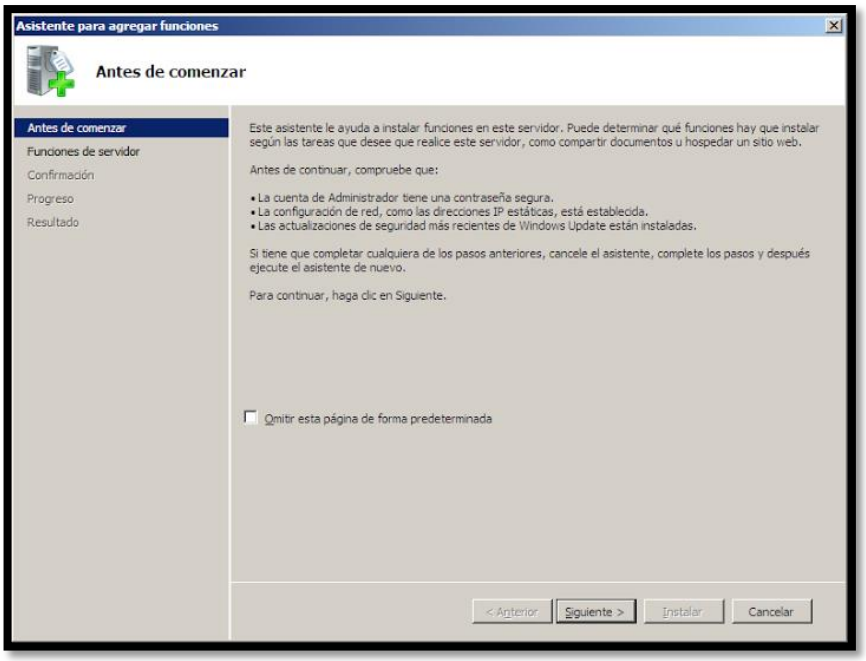


[http://es.wikipedia.org/wiki/DHCPv6]

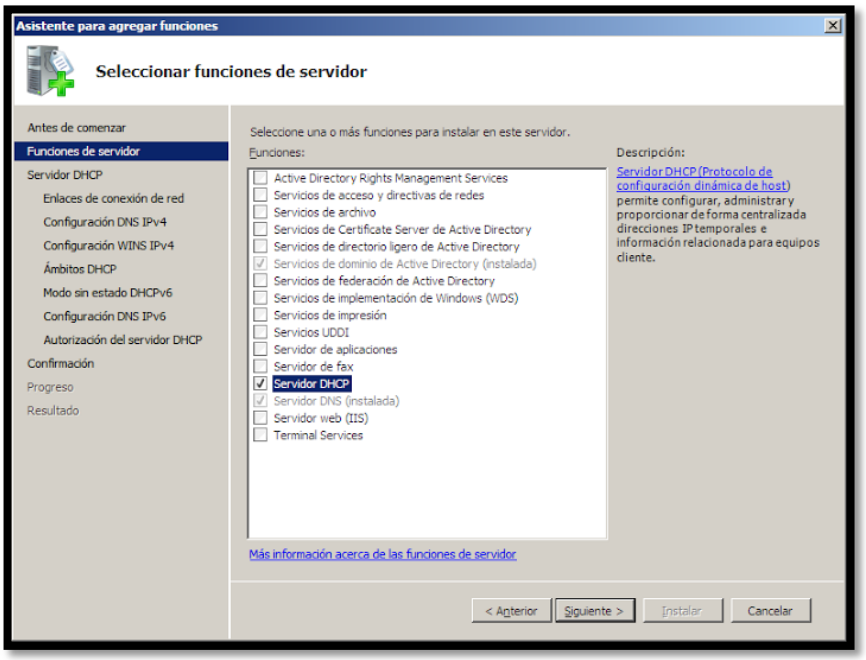
A continuación agregaremos una función:



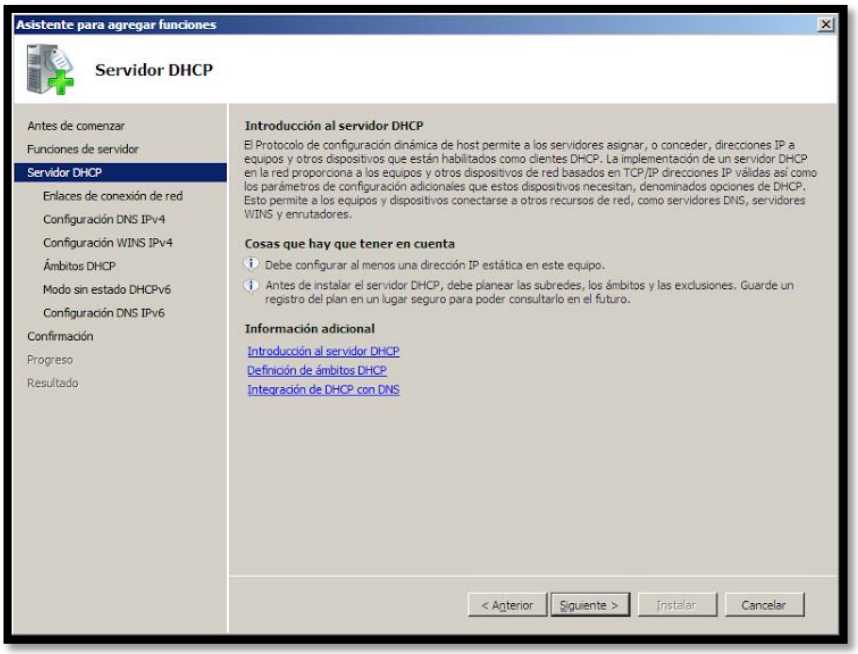
Leemos las advertencias, nosotros hemos instalado en el servidor una IPV4 estática: 192.168.0.80



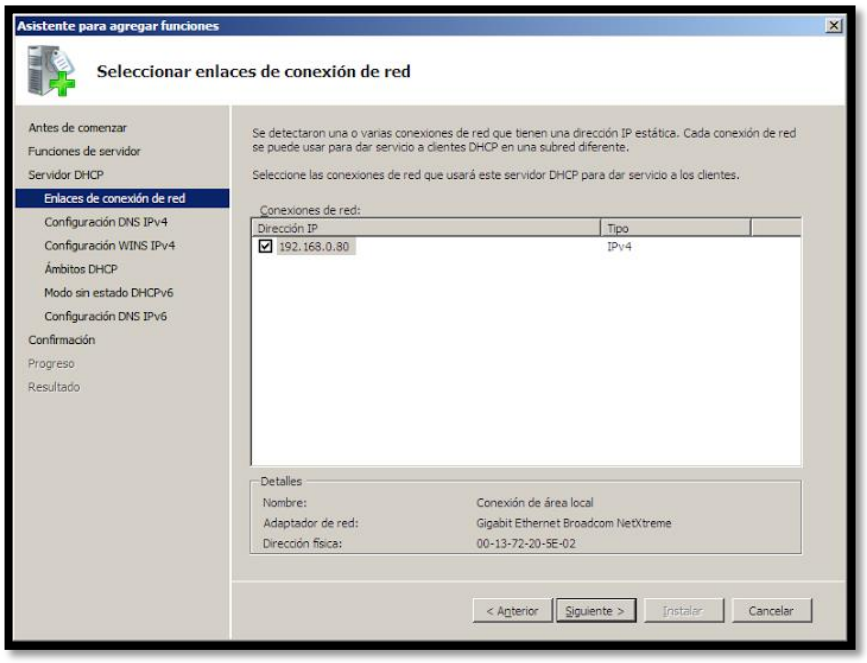
Agregamos el servidor DHCP:



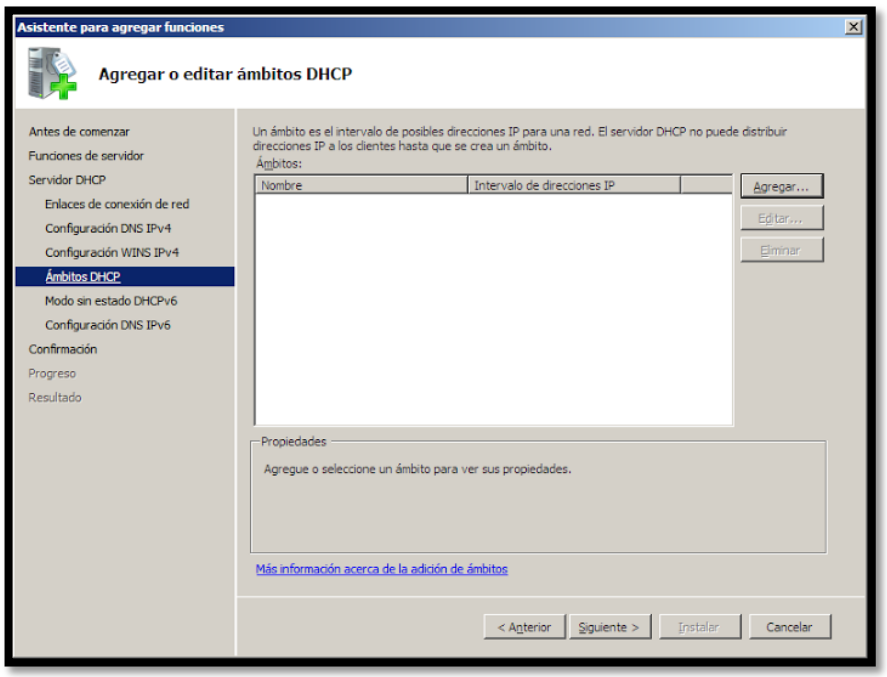
Podemos leer la ayuda para profundizar:



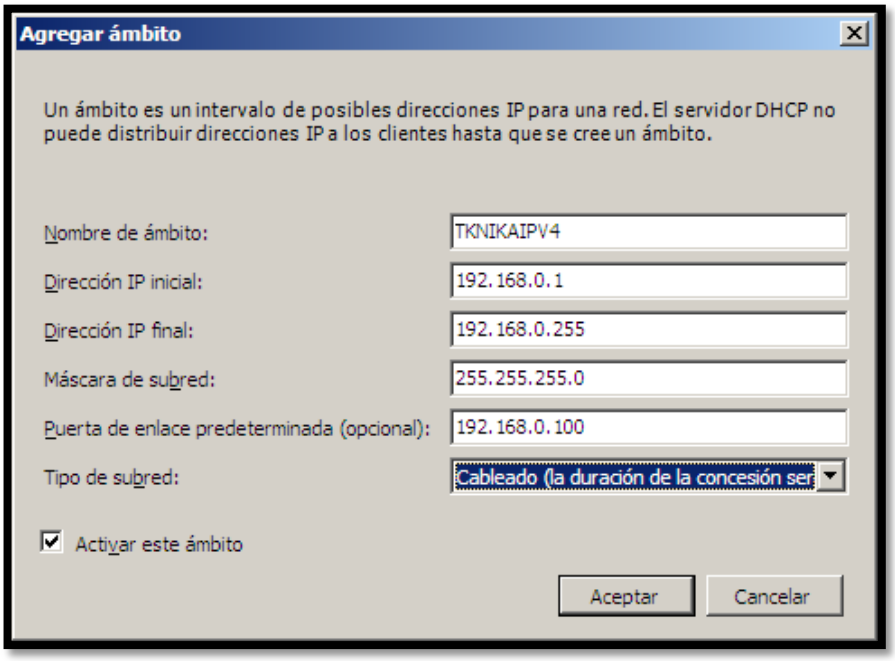
Obtenemos la configuración IPV4 que hemos establecido anteriormente en el servidor:



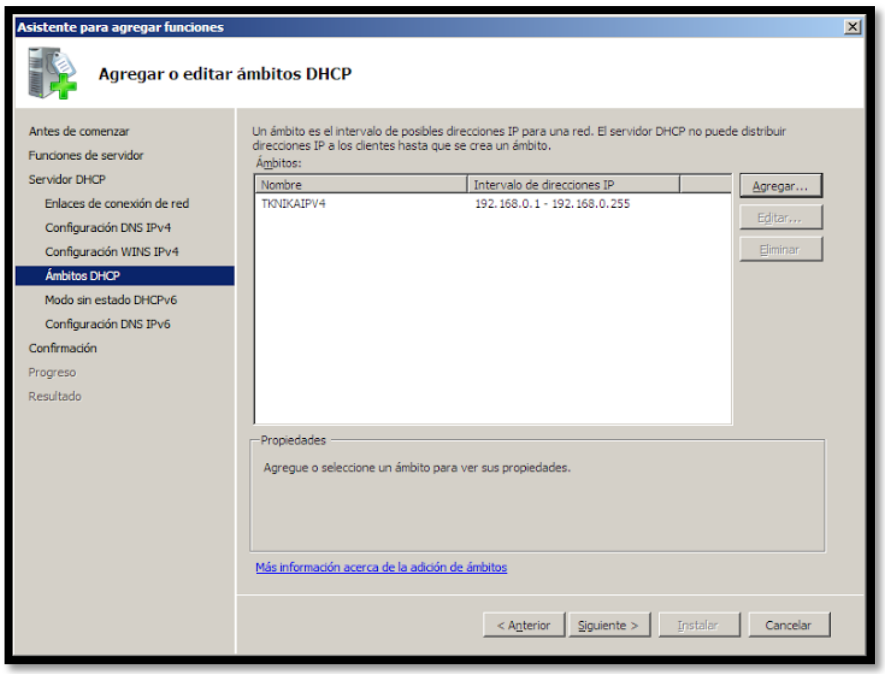
Vamos a definir un ámbito IPV4: **Red:** 192.168.0.x **Mascara:** 255.255.255.0



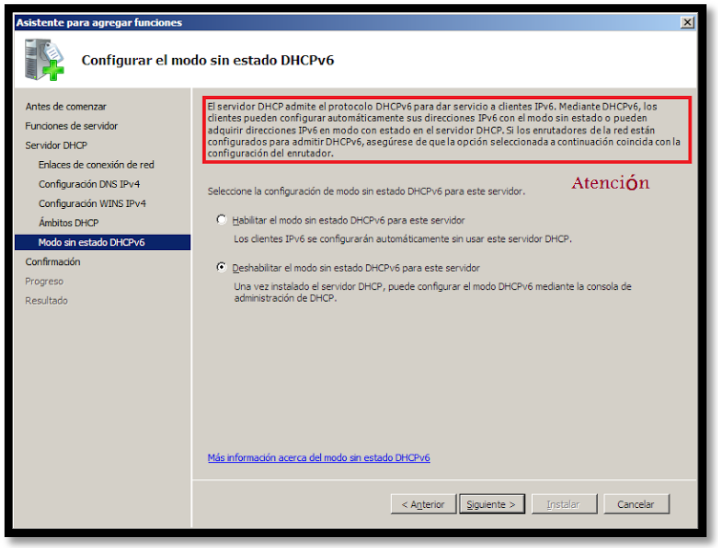
La puerta de enlace es opcional, en nuestro caso representa un Router que podremos añadir posteriormente.



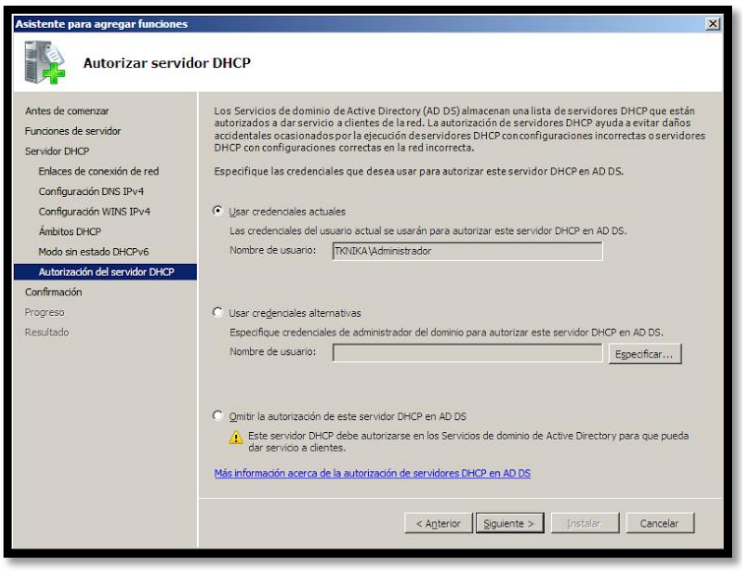
Observamos que el ámbito IPV4 es correcto.



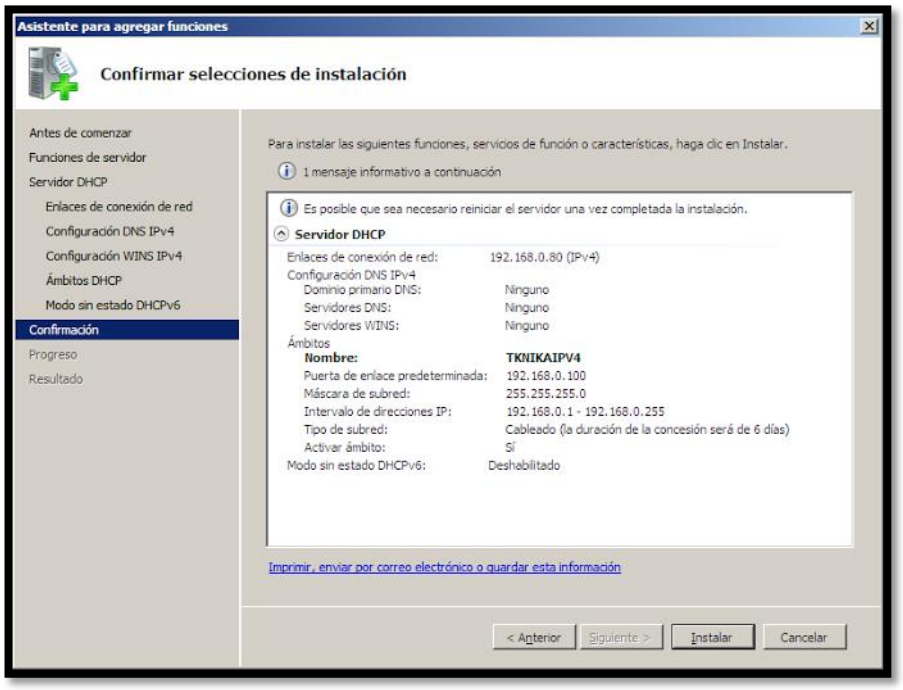
Comenzamos a configurar el ámbito IPV6. Observar con atención la siguiente ventana. En nuestro caso debemos deshabilitar el modo sin estado para este servidor.



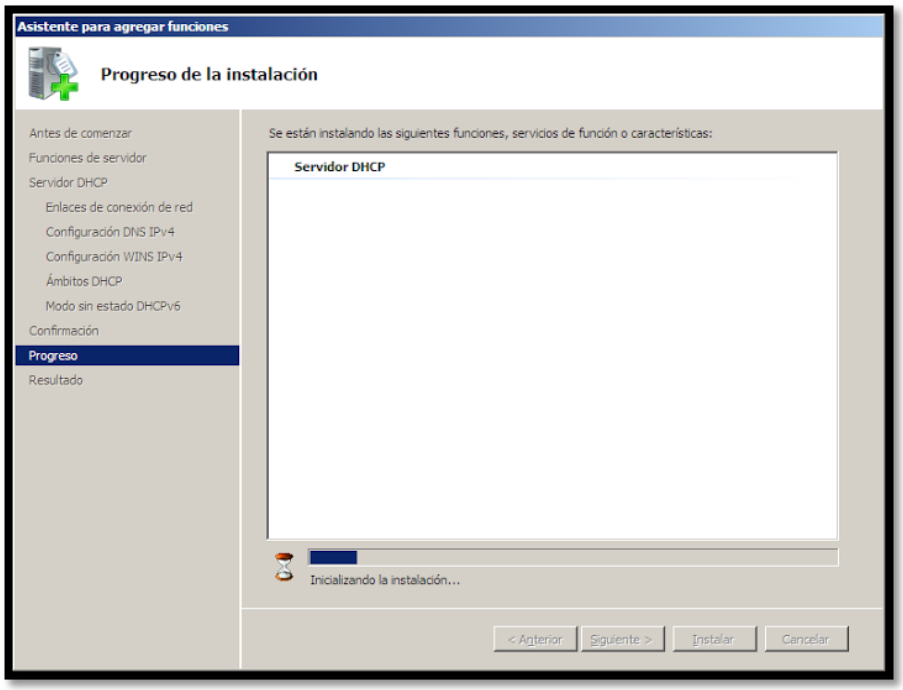
Usamos las credenciales actuales del usuario administrador:



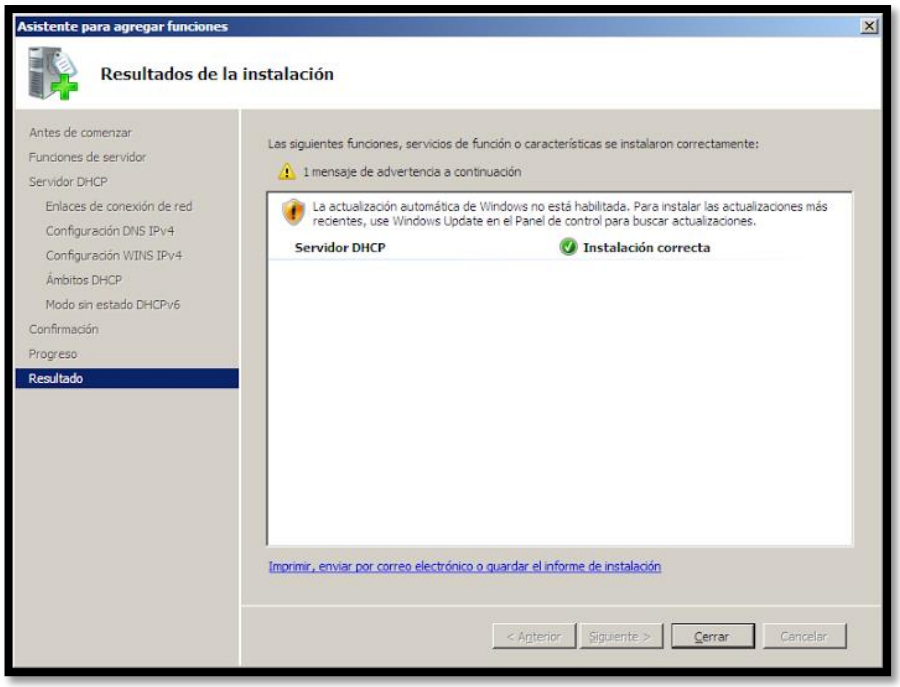
Confirmamos si todo es correcto:



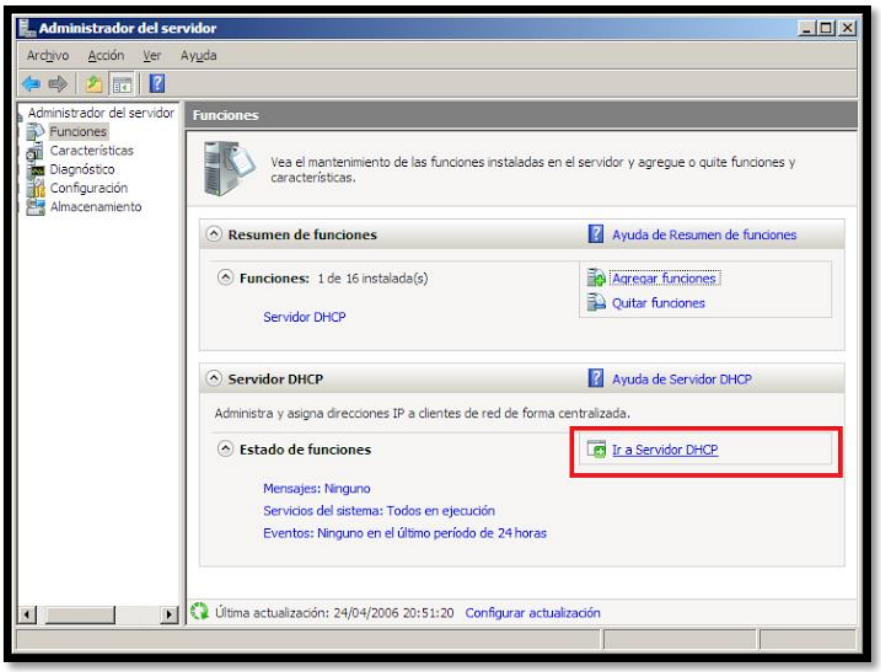
El servidor DHCPv4 se instalará:



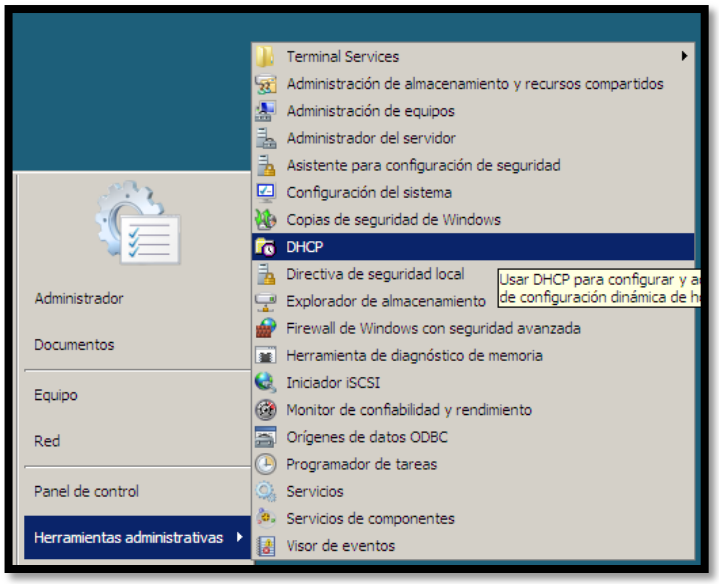
La instalación ha sido satisfactoria:



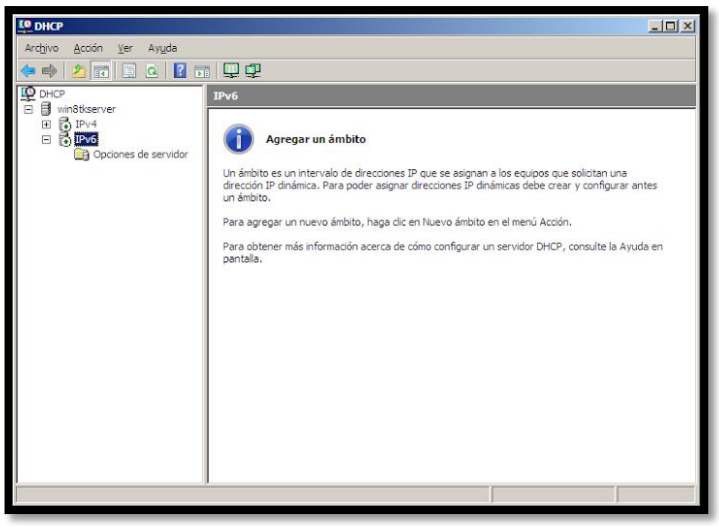
En el Administrador del servidor vamos al servidor DHCP:



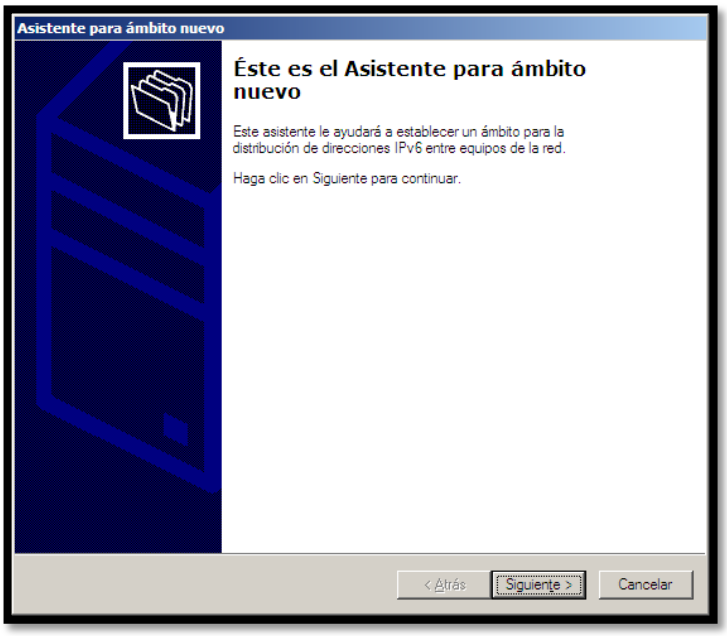
O podemos hacerlo: Inicio-->Herramientas administrativas-->DHCP



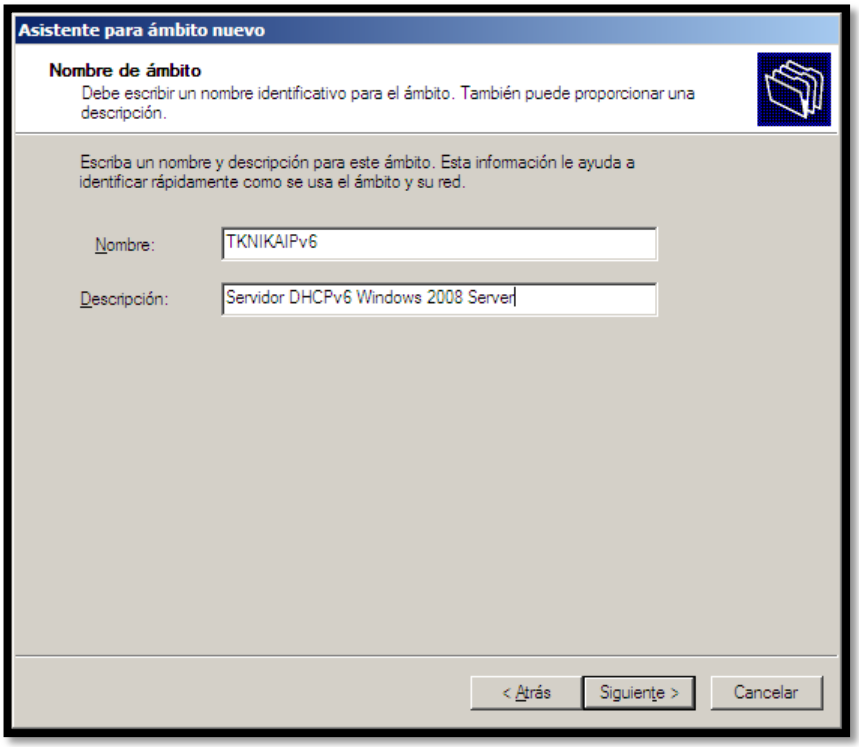
Una vez IPV4 está activo y con su ámbito definido, nos situamos en IP6, botón derecho agregamos ámbito:



Se ejecuta el asistente de ámbito nuevo:

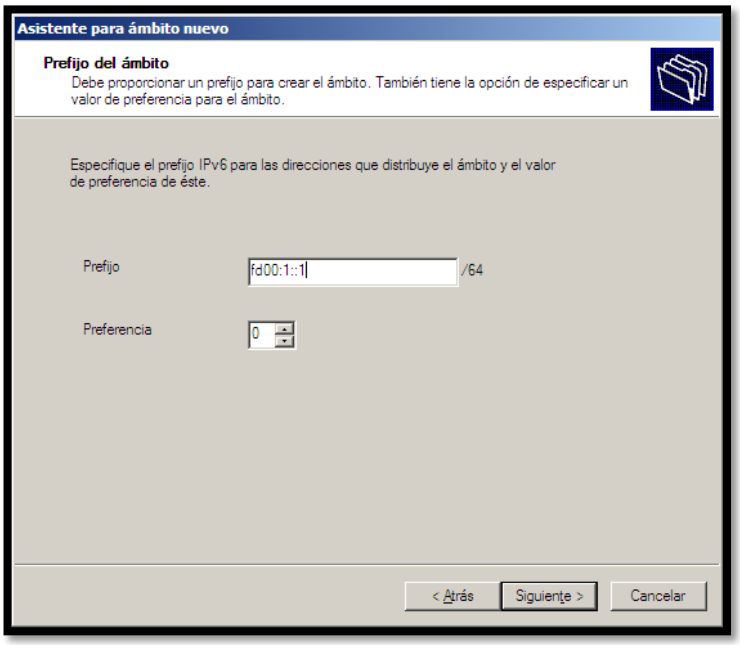


Damos un nombre y descripción al ámbito:

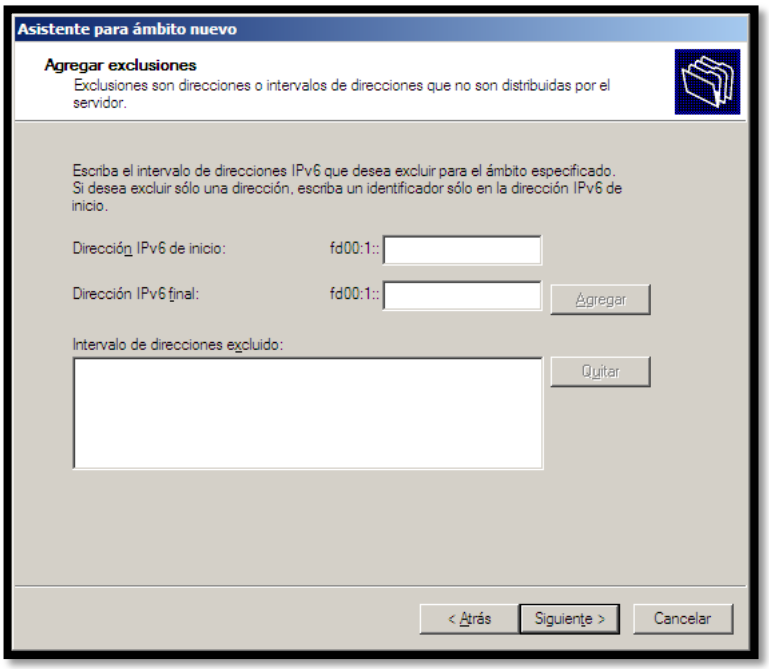


Debemos elegir el prefijo de las direcciones IPV6 que vamos a repartir. Por ejemplo, elegimos un prefijo de direcciones locales únicas para nuestra organización fd00:1::1, en este caso elegimos el prefijo fd00:1::1/64 En cada caso el administrador del sistema elegirá el ámbito que más le interese.

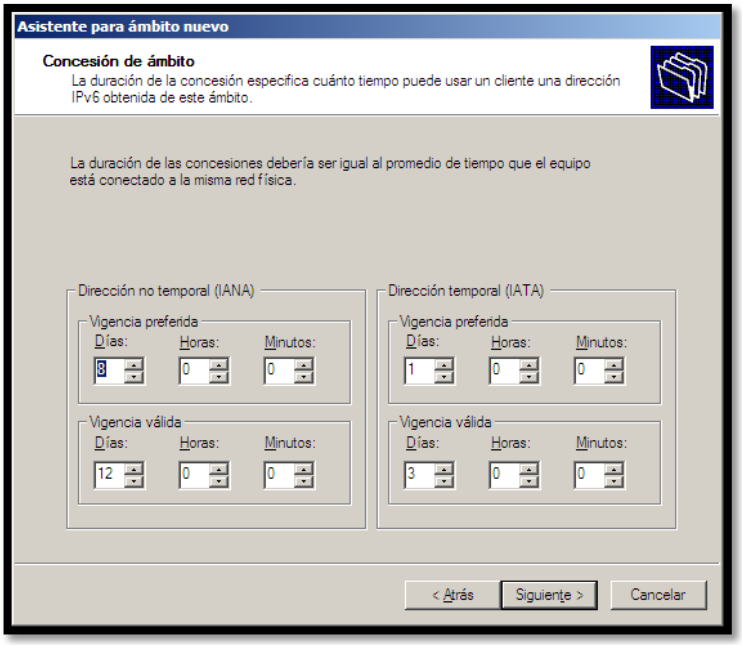
La preferencia determina el grado de prioridad que tiene el servidor DHCPv6. Dentro de una red puede existir más de un servidor DHCPv6, en ese caso, se establece la prioridad de cada uno, siendo el número 0 el que tiene mayor prioridad a la hora de asignar las direcciones IPV6.



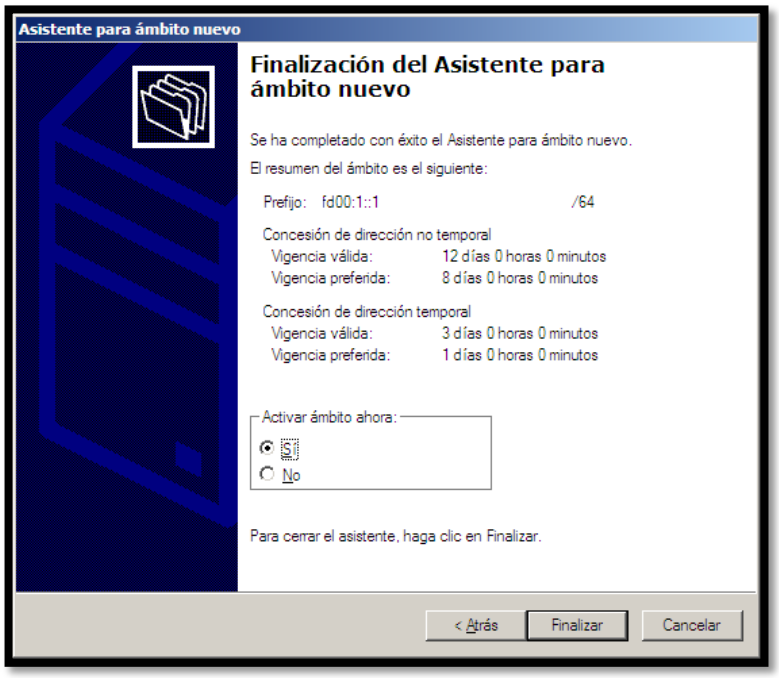
Si queremos agregar exclusiones (direcciones que no nos interesa que distribuya el servidor), este es el momento. Nosotros de momento no agregaremos exclusiones.



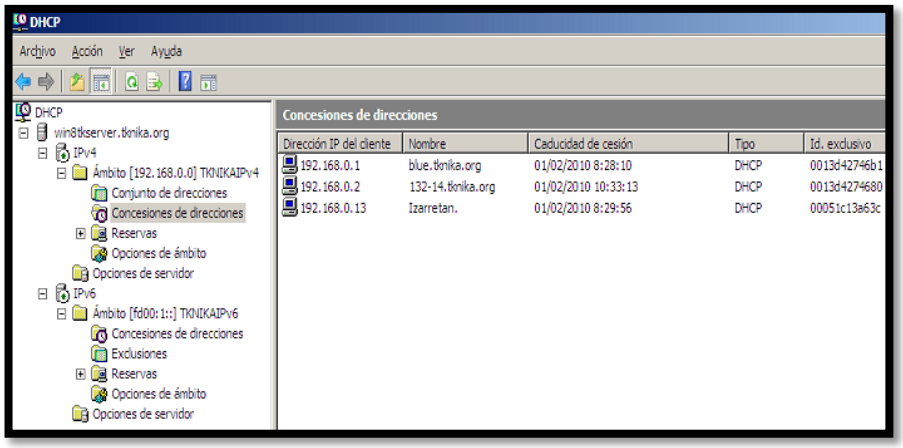
Por último, debemos indicar la vigencia de las concesiones:



El asistente muestra un resumen de la configuración y nos permite finalizar.

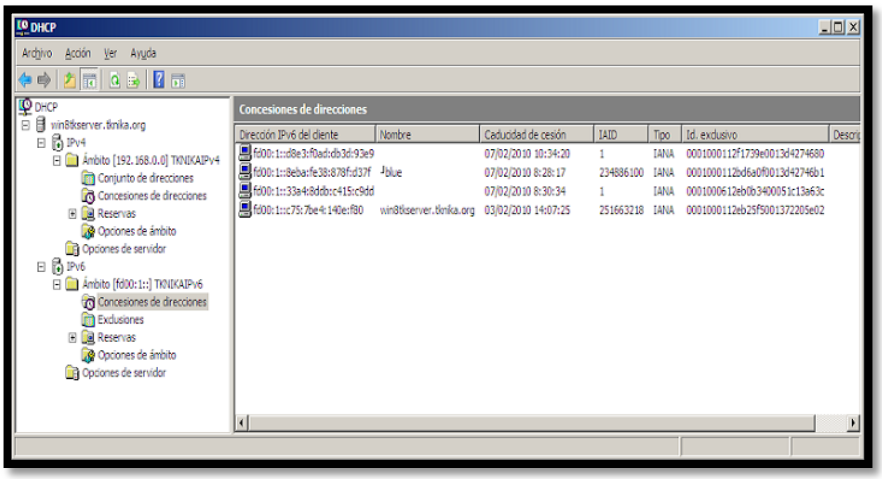


En el caso de IPV4 siempre que los sistemas operativos de los ordenadores cliente indique en la configuración TCP/IP del adaptador de red que la dirección se obtenga de forma automática para observar las concesiones basta ir a la opción concesiones de direcciones en el servidor DHCP IPV4. En nuestro caso, observamos los tres ordenadores de la red.

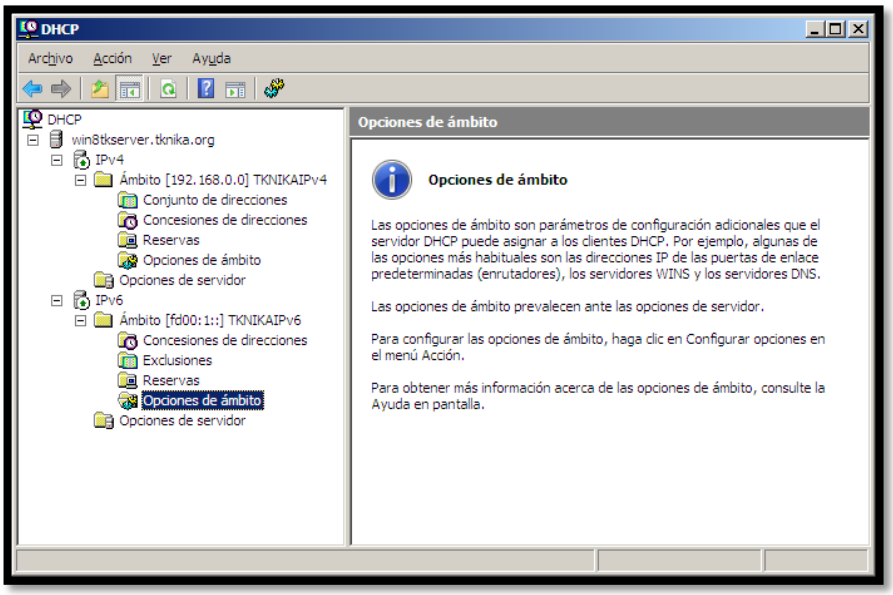


En el caso de IPV6 para los clientes Windows XP y Ubuntu-Linux (de momento) es necesario instalar un cliente DHCPv6 como veremos en los siguientes apartados. En el caso de Windows 7 el cliente viene instalado en el propio sistema operativo. Lo único que debemos tener en cuenta en Windows 7 es la configuración del Firewall que incorpora el sistema que en algunos casos impide la asignación de una dirección por parte del servidor.

Una vez instalados los clientes (como veremos más adelante), bastaría con ir a la opción concesiones de direcciones en el apartado IPV6 y obtendremos la información de cada cliente. En nuestro caso:



Para terminar, normalmente, además de repartir las direcciones IP el servidor se encarga de asignar puertas de enlace predeterminadas o servidores DNS. Dichas opciones pueden seleccionarse en opciones de ámbito.



La configuración del servidor DHCPv6 para Windows Server 2008 se ha realizado satisfactoriamente.

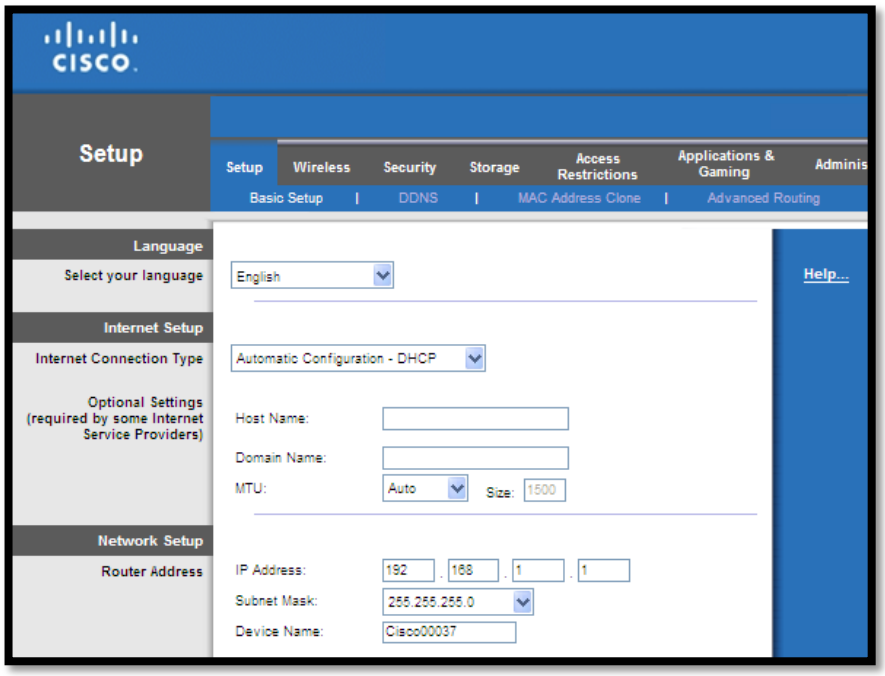
D. Configuración del Router WIFI con acceso a IPV6

A continuación se dará a detalle cómo se configura un router WIFI con IPV6 el cual estará sujeto a un DHCPv6 para la generación de las IPV6 que se darán a los usuarios y a los equipos.

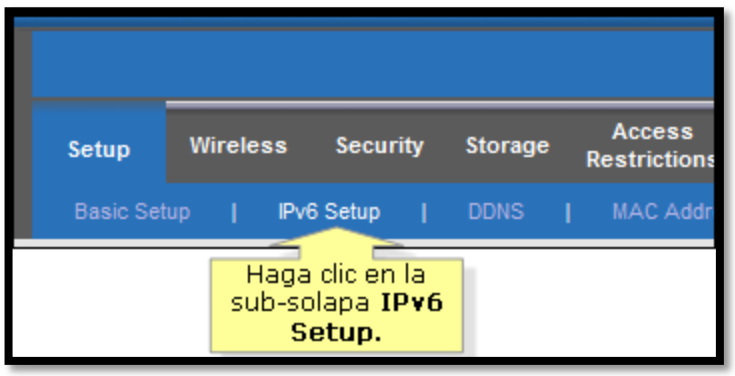
IPv6 enabled (E1200V2 and E1500)

Supports the latest Internet protocol technology to future-proof your network.

1. Primero entramos a la interface del equipo:



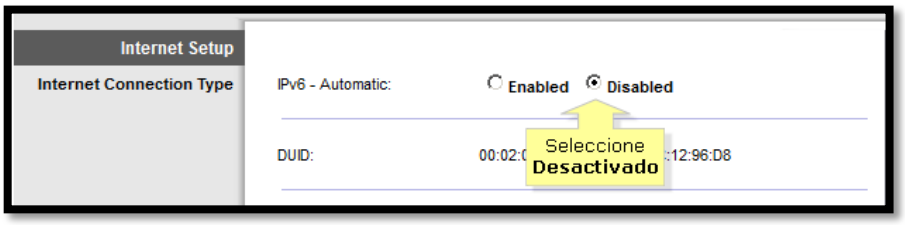
2. A continuación en la pestaña o casilla de configuración [SETUP] damos clic en IPV6setup



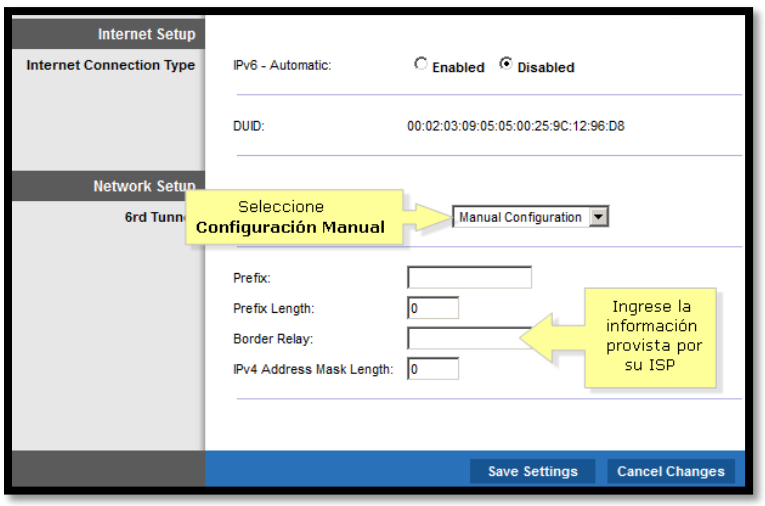
En caso que no aparezca la casilla de IPV6setup se considera actualizar el firmware [Pasos en el Link]

http://kb.linksys.com/Linksys/ukp.aspx?pid=88&g=94&vw=1&articleid=22280

3. En la sección de tipo de conexión de internet seleccione desactivado en IPV6 – automático.

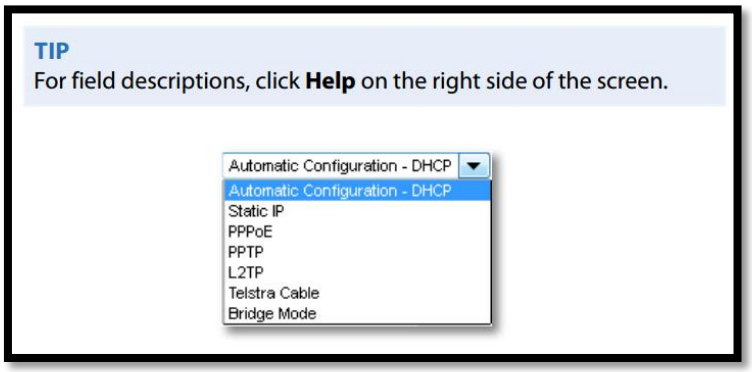


A continuación seleccione configuración manual y luego ingrese la información provista por su ISP para los campos de prefijo, longitud del prefijo, relevo de frontera y longitud de la máscara de la dirección IPV4.



4. Guardamos Configuración

Para la configuración del DHCP en el router WIFI se solicita desactivar la configuración automática e ingresar la configuración mostrada en la instalación del DHPV6.



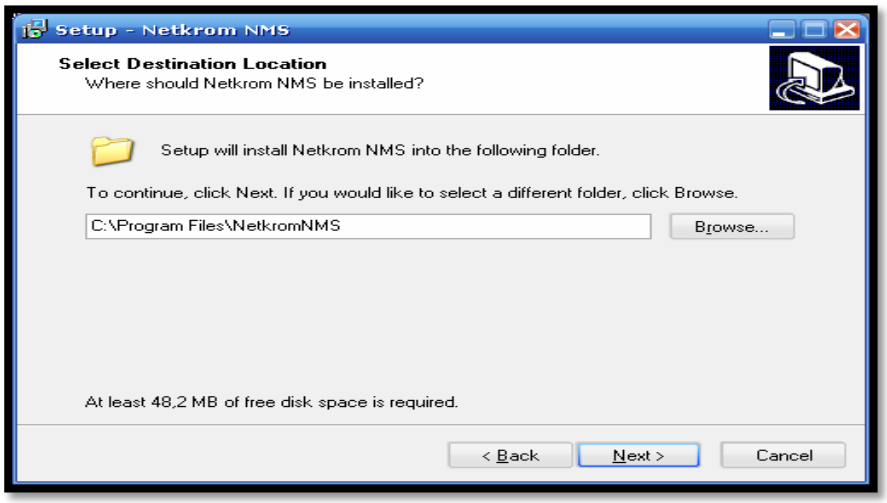
Además de recordar la configuración a implementar para temas de DNS y de Firewall, con lo que se configurara los demás equipos.

E. **Instalación de sistemas Netkrom:**

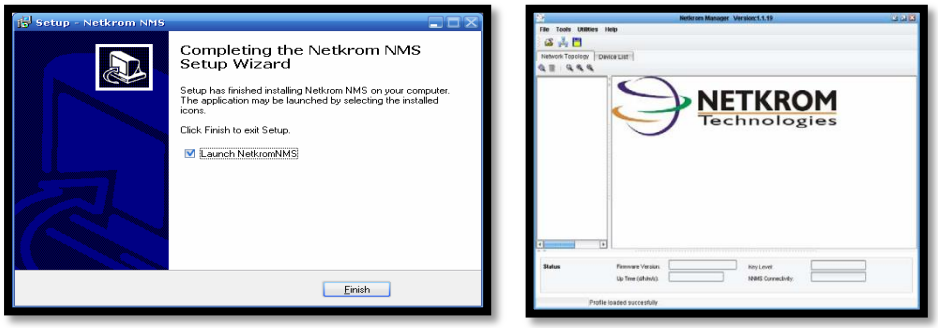
NMS: Visitando http://www.netkrom.com/es se dará clic en la opción de soporte y descargar drivers; baje la versión más nueva del Netkrom Network Manager.

Después que la descarga esté completada, ejecute el instalador del NNMS. Siga las instrucciones de la instalación del wizard.

Seleccione el folder donde el NNMS va a ser instalado y presione el botón “Next”.



Finalmente, el proceso de instalación ha terminado.



Ahora puede ejecutar el NNMS en su sistema.

- **PAÍSES Y ENTIDADES SUDAMERICANAS CON IMPLEMENTACIÓN DE IPV6** [D]

Organización	País / Región	Estado de implementación			Detalles
		Ya implementado	Actualmente implementando	Con planes de implementación	
Airsat (Grape S.A.)	Argentina		X		Desplegar
ALFANUMERIC S.A	Nicaragua		X		Desplegar
Americana Digital	Brasil	X			Desplegar
BT Latinoamérica	Argentina	X			Desplegar
Cablemas Telecomunicaciones SA de CV	México		X		Desplegar
CENIT	Venezuela	X			Desplegar
Cooperativa Telefónica de Villa Gobernador Gálvez Limitada (TelVGG)	Argentina	X			Desplegar
Comunicaciones IBW Nic	Nicaragua	X			Desplegar
Empresa de Recursos Tecnológicos E.R.T E.S.P	Colombia	X			Desplegar
ETB S.A. ESP	Colombia		X		Desplegar
Global Crossing	América Latina y Caribe	X			Desplegar
Google	Global	X			Desplegar
GTD	Chile	X			Desplegar
ICE – Instituto Costarricense de Electricidad y Telecomunicaciones	Costa Rica	X			Desplegar
Infotec	México	X			Desplegar
INTERNEXA	Colombia	X			Desplegar
IPLAN	Argentina		X		Desplegar
Media Commerce Telecomunicaciones S.A.S	Colombia	X			Desplegar

Ministerio de Tecnologías de la Información y las Comunicaciones	Colombia			X	Desplegar
NAP.EC	Ecuador	X			Desplegar
NET	Brasil	X			Desplegar
NipCable do Brasil Telecom LTDA	Brasil	X			Desplegar
NIC Chile	Chile	X			Desplegar
NIC MX	México	X			Desplegar
Nodosud SA	Argentina		X		Desplegar
Operbes, S.A. de C.V.	México	X			Desplegar
RENATA	Colombia	X			Desplegar
RIU – Red Interconexión Universitaria	Argentina		X		Desplegar
SMITCOMS	Antillas Neerlandesas			X	Desplegar
Telecentro S.A.	Argentina		X		Desplegar
Telecom Argentina S.A.	Argentina		X		Desplegar
Telefonía Celular de Nicaragua (Telefónica Nicaragua)	Nicaragua	X			Desplegar
Tigo Guatemala	GT	X			Desplegar
Telmex Colombia (Claro Fijo)	Colombia	X			Desplegar
TRICOM	República Dominicana	X			Desplegar
UNE EPM Telecomunicaciones S.A.	Colombia	X			Desplegar
Universidad APEC	República Dominicana		X		Desplegar
Universidad del Atlántico (UA)	Colombia	X			Desplegar
Universidad Centro Occidental Lisandro Alvarado (UCLA)	Venezuela		X		Desplegar

Universidad Nacional Abierta (UNA)	Venezuela		X		Desplegar
Universidad Nacional Autónoma de México (UNAM)	México	X			Desplegar
Universidad Nacional de Loja	Ecuador	X			Desplegar
Universidad de Oriente	Venezuela		X		Desplegar
Universidad Pontificia Bolivariana Seccional Medellín	Colombia	X			Desplegar
Universidad Pontificia Bolivariana, Seccional Bucaramanga	Colombia	X			Desplegar
Universidad Técnica Federico Santa María (UTFSM)	Chile	X			Desplegar
Universidad Técnica Particular de Loja	Ecuador	X			Desplegar
Universidad tecnológica centroamericana (UNITEC)	Honduras		X		Desplegar
VTR Banda Ancha S.A.	Chile		X		Desplegar
YouTube	Global vía Google Network	X			Desplegar

- **DETALLE ESTADÍSTICO**

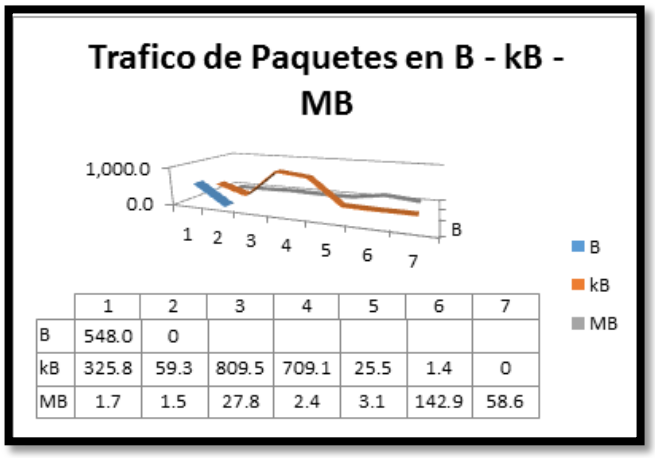
Para AP1:

En la siguiente Tabla donde se muestra el cálculo de los datos sometidos a media, mediana, moda, máximo, mínimo, desviación estándar y varianza que nos revela el comportamiento de los usuarios según muestras establecidas.

Noción Estadística de los Valores Totales

	hh:mm	B	kB	MB
Media	0:27:53	548.0	321.8	34.0
Mediana	0:03:50	548.0	192.6	3.1
Moda	0:03:16	0	0	1
Mínimo	0:01:30	0	0	0.7
Máximo	2:25:07	0	0	142.9
Desviación Estándar	0.0313	0	0	50.04
Varianza	0.00098	0	0	2503.78

A continuación tenemos la siguiente figura, el grafico de los datos evaluados en AP1 para ver el tipo de datos consumidos con mayor frecuencia en los dispositivos móviles.



	1	2	3	4	5	6	7
B	548.0	0					
kB	325.8	59.3	809.5	709.1	25.5	1.4	0
MB	1.7	1.5	27.8	2.4	3.1	142.9	58.6

Para estos calculos se recolecto de cada AP muestras del trafico de entrada y salida y las horas de conectividad y según esto se calcula el tipo de dispositivos usados en la conectividad.

Muestra AP1

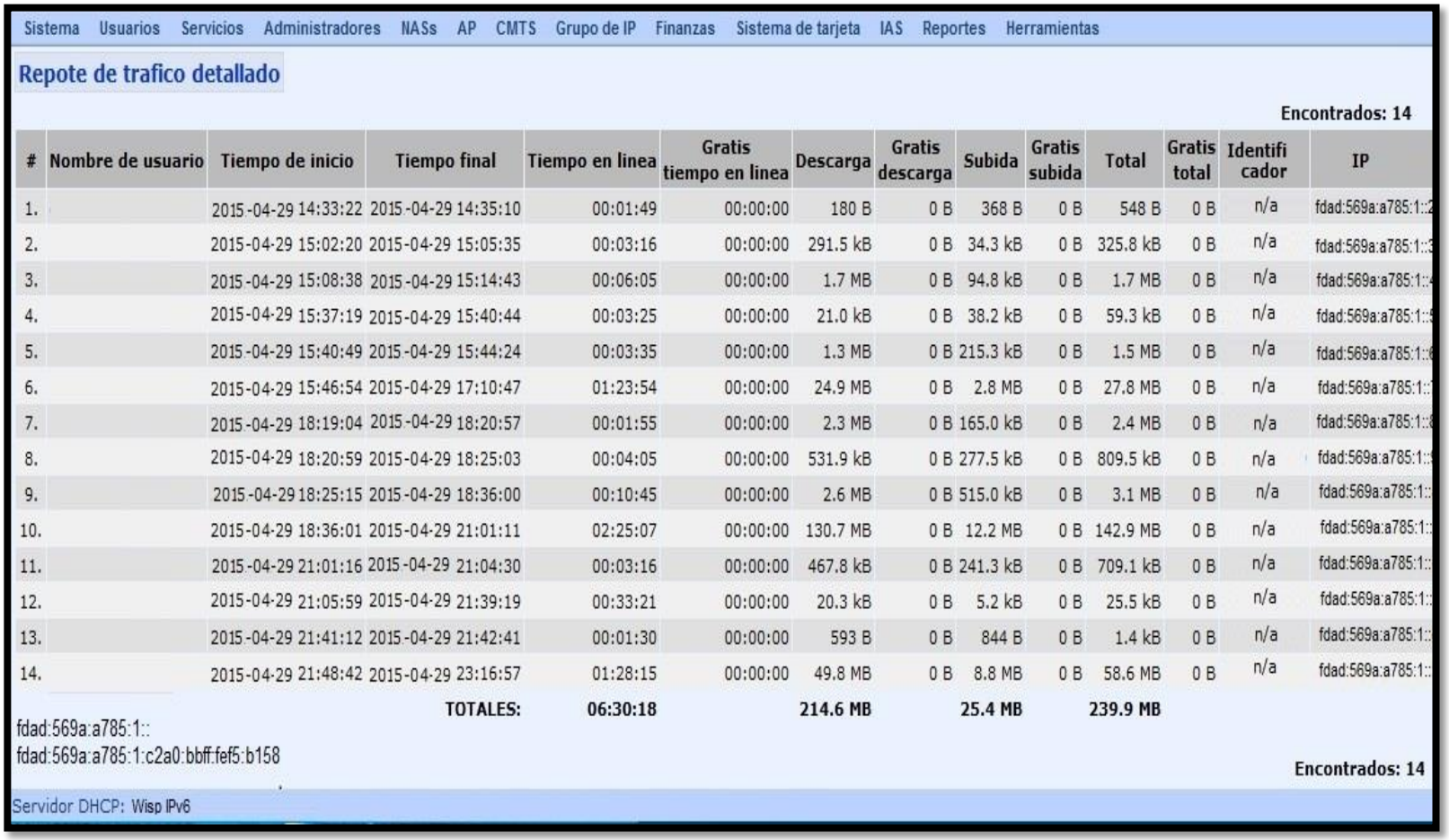
Usuarios	Tiempo en línea	Datos: Voz/Ip/Video					
	hh:mm:ss	Descargas	Tipo	Subidas	Tipo	Total Up &Down	Peso
1	0:01:49	180.0	**B**	368.0	**B**	**548.0**	**B**
2	0:03:16	291.5	**kB**	34.0	**kB**	**325.8**	**kB**
3	0:06:05	1.7	**MB**	94.8	**kB**	**1.7**	**MB**
4	0:03:25	21.0	**kB**	34.0	**kB**	**59.3**	**kB**
5	0:03:35	1.7	**MB**	215.3	**kB**	**1.5**	**MB**
6	1:23:54	24.9	**MB**	2.8	**MB**	**27.8**	**MB**
7	0:01:55	2.3	**MB**	165.0	**kB**	**2.4**	**MB**
8	0:04:05	531.9	**kB**	277.5	**kB**	**809.5**	**kB**

9	0:10:45	2.6	**MB**	515.0	**kB**	**3.1**	**MB**
10	2:25:07	130.7	**MB**	12.2	**MB**	**142.9**	**MB**
11	0:03:16	467.8	**kB**	241.3	**kB**	**709.1**	**kB**
12	0:33:21	20.3	**kB**	5.2	**kB**	**25.5**	**kB**
13	0:01:30	593.0	**B**	844.0	**B**	**1.4**	**kB**
14	1:28:15	49.8	**MB**	8.8	**MB**	**58.6**	**MB**
Total	**6:30:18**	**2.3**	**GB**	**26.6**	**MB**	**239.9**	**MB**

Separando los consumos de subida y bajada tenemos una pequeña tabla explicativa donde se incluye ya transformados en 0.7MB los datos de B.

Total Up &Down	
0.7	MB
1.5	MB
1.7	MB
2.4	MB
3.1	MB
27.8	MB
58.6	MB
142.9	MB

Imágenes de las pantallas de la administracion de los AP muestreados con la conectividad Wisp



Sistema Usuarios Servicios Administradores NASs AP CMTS Grupo de IP Finanzas Sistema de tarjeta IAS Reportes Herramientas

Repote de trafico detallado

Encontrados: 14

#	Nombre de usuario	Tiempo de inicio	Tiempo final	Tiempo en linea	Gratis tiempo en linea	Descarga	Gratis descarga	Subida	Gratis subida	Total	Gratis total	Identificador	IP
1.		2015-04-29 14:33:22	2015-04-29 14:35:10	00:01:49	00:00:00	180 B	0 B	368 B	0 B	548 B	0 B	n/a	fdad:569a:a785:1::2
2.		2015-04-29 15:02:20	2015-04-29 15:05:35	00:03:16	00:00:00	291.5 kB	0 B	34.3 kB	0 B	325.8 kB	0 B	n/a	fdad:569a:a785:1::3
3.		2015-04-29 15:08:38	2015-04-29 15:14:43	00:06:05	00:00:00	1.7 MB	0 B	94.8 kB	0 B	1.7 MB	0 B	n/a	fdad:569a:a785:1::4
4.		2015-04-29 15:37:19	2015-04-29 15:40:44	00:03:25	00:00:00	21.0 kB	0 B	38.2 kB	0 B	59.3 kB	0 B	n/a	fdad:569a:a785:1::5
5.		2015-04-29 15:40:49	2015-04-29 15:44:24	00:03:35	00:00:00	1.3 MB	0 B	215.3 kB	0 B	1.5 MB	0 B	n/a	fdad:569a:a785:1::6
6.		2015-04-29 15:46:54	2015-04-29 17:10:47	01:23:54	00:00:00	24.9 MB	0 B	2.8 MB	0 B	27.8 MB	0 B	n/a	fdad:569a:a785:1::7
7.		2015-04-29 18:19:04	2015-04-29 18:20:57	00:01:55	00:00:00	2.3 MB	0 B	165.0 kB	0 B	2.4 MB	0 B	n/a	fdad:569a:a785:1::8
8.		2015-04-29 18:20:59	2015-04-29 18:25:03	00:04:05	00:00:00	531.9 kB	0 B	277.5 kB	0 B	809.5 kB	0 B	n/a	fdad:569a:a785:1::9
9.		2015-04-29 18:25:15	2015-04-29 18:36:00	00:10:45	00:00:00	2.6 MB	0 B	515.0 kB	0 B	3.1 MB	0 B	n/a	fdad:569a:a785:1::a
10.		2015-04-29 18:36:01	2015-04-29 21:01:11	02:25:07	00:00:00	130.7 MB	0 B	12.2 MB	0 B	142.9 MB	0 B	n/a	fdad:569a:a785:1::b
11.		2015-04-29 21:01:16	2015-04-29 21:04:30	00:03:16	00:00:00	467.8 kB	0 B	241.3 kB	0 B	709.1 kB	0 B	n/a	fdad:569a:a785:1::c
12.		2015-04-29 21:05:59	2015-04-29 21:39:19	00:33:21	00:00:00	20.3 kB	0 B	5.2 kB	0 B	25.5 kB	0 B	n/a	fdad:569a:a785:1::d
13.		2015-04-29 21:41:12	2015-04-29 21:42:41	00:01:30	00:00:00	593 B	0 B	844 B	0 B	1.4 kB	0 B	n/a	fdad:569a:a785:1::e
14.		2015-04-29 21:48:42	2015-04-29 23:16:57	01:28:15	00:00:00	49.8 MB	0 B	8.8 MB	0 B	58.6 MB	0 B	n/a	fdad:569a:a785:1::f
			TOTALES:	**06:30:18**		**214.6 MB**		**25.4 MB**		**239.9 MB**			

fdad:569a:a785:1::
fdad:569a:a785:1:c2a0:bbff:fef5:b158

Encontrados: 14

Servidor DHCP: Wisp IPv6

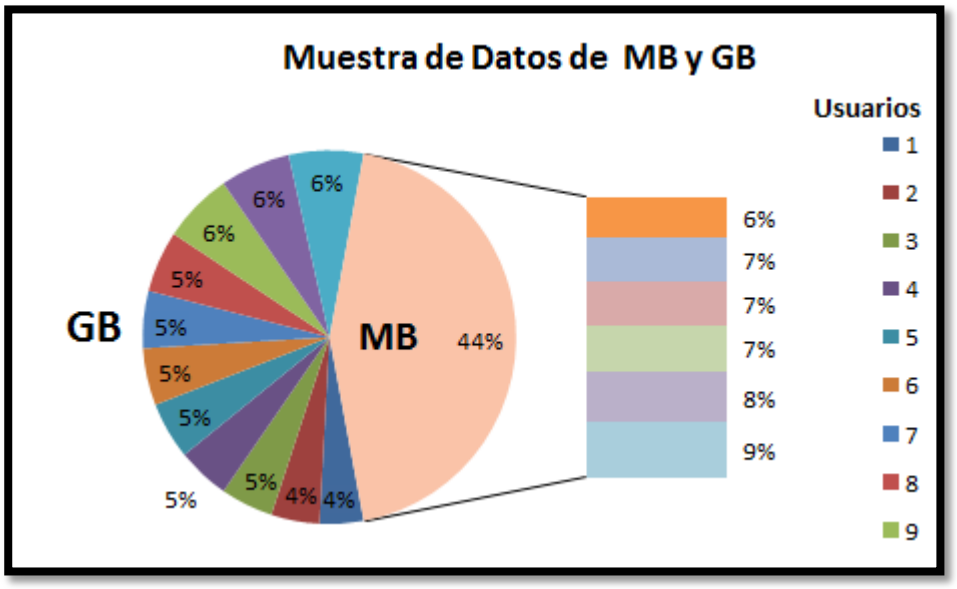
Para AP2:

En la siguiente tabla mostraremos el cálculo de los datos sometidos en ap2 a media, mediana, moda, máximo, mínimo, desviación estándar y varianza que nos revela el comportamiento de los usuarios según muestras establecidas.

Noción estadística de los valores Totales AP2

	hh:mm	B	kB	MB	GB
Media	11:44:59	1.6	1.6	429.5	2.0
Mediana	12:37:25	0.0	0.0	223.6	1.6
Moda	0:00:00	0.0	0.0	0.0	1.3
Mínimo	1:20:03	0.0	0.0	68.3	1.0
Máximo	14:10:46	0.0	0.0	996.5	2.3
Desviación Estándar	0.1210	0.0	0.0	497.17	0.36
Varianza	0.0147	0.0	0.0	247174.62	0.13

Con estas muestras tendremos la siguiente gráfica correspondiente a los consumos de MB y GB con sus porcentajes en uso.



Para los calculos que se muestran en la sig tabla, se recolecto de AP2 muestras del trafico de entrada y salida y las horas de conectividad y según esto se calcula el tipo de dispositivos usados en la conectividad al igual que AP1.

MuestraAP2

Usuarios	Tiempo en línea	Datos: Voz/Ip/Video					
	hh:mm:ss	Descargas	Tipo	Subidas	Tipo	Total Up&Down	Peso
1	12:27:14	1.9	**GB**	211.3	**MB**	**2.1**	**GB**
2	13:52:45	1.6	**GB**	183.6	**MB**	**1.8**	**GB**
3	14:10:46	1.1	**GB**	156.3	**MB**	**1.2**	**GB**
4	13:54:39	1.2	**GB**	208.6	**MB**	**1.4**	**GB**

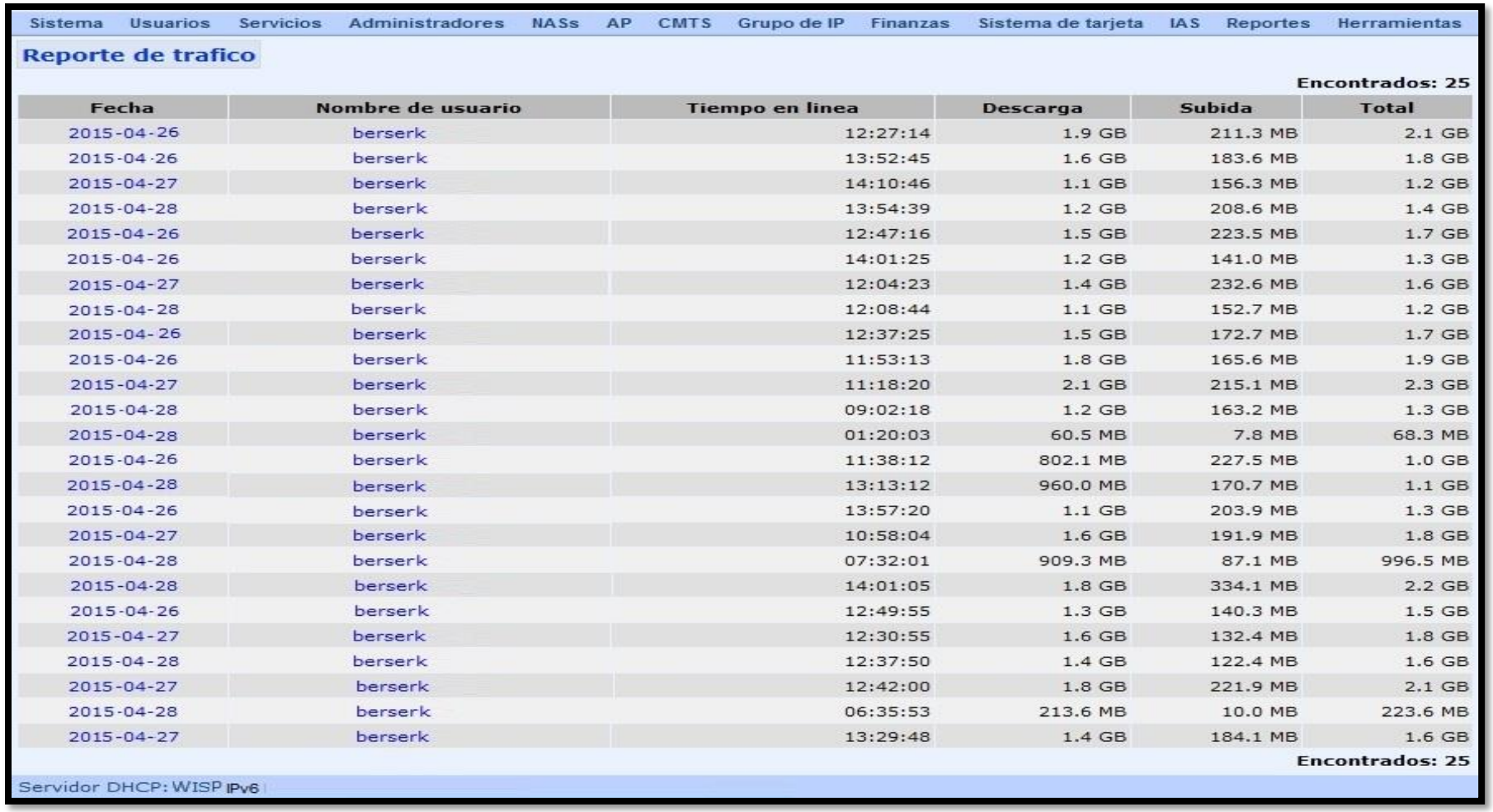
5	12:47:16	1.5	**GB**	223.5	**MB**	**1.7**	**GB**
6	14:01:25	1.2	**GB**	141.0	**MB**	**1.3**	**GB**
7	12:04:23	1.4	**GB**	232.6	**MB**	**1.6**	**GB**
8	12:08:44	1.1	**GB**	152.7	**MB**	**1.2**	**GB**
9	12:37:25	1.5	**GB**	172.7	**MB**	**1.7**	**GB**
10	11:53:13	1.8	**GB**	165.6	**MB**	**1.9**	**GB**
11	11:18:20	2.1	**GB**	215.1	**MB**	**2.3**	**GB**
12	9:02:18	1.2	**GB**	163.2	**MB**	**1.3**	**GB**
13	1:20:03	60.5	**MB**	7.8	**MB**	**68.3**	**MB**
14	11:38:12	802.1	**MB**	227.5	**MB**	**1.0**	**GB**
15	13:13:12	960.0	**MB**	170.7	**MB**	**1.1**	**GB**
16	13:57:20	1.1	**GB**	203.9	**MB**	**1.3**	**GB**
17	10:58:04	1.6	**GB**	191.9	**MB**	**1.8**	**GB**
18	7:32:01	909.3	**MB**	87.1	**MB**	**996.5**	**MB**
19	14:01:05	1.8	**GB**	334.1	**MB**	**2.2**	**GB**
20	12:49:55	1.3	**GB**	140.3	**MB**	**1.5**	**GB**
21	12:30:55	1.6	**GB**	132.4	**MB**	**1.8**	**GB**
22	12:37:50	1.4	**GB**	122.4	**MB**	**1.6**	**GB**
23	12:42:00	1.8	**GB**	221.9	**MB**	**2.1**	**GB**
24	6:35:53	213.6	**MB**	10.0	**MB**	**223.6**	**MB**
25	13:29:48	1.4	**GB**	184.1	**MB**	**1.6**	**GB**
Total	**293:44:46**	**32.5**	**GB**	**4.2**	**GB**	**36.8**	**GB**

Separando los consumos de subida y bajada tenemos 2 pequeñas tablas explicativa donde se incluye ya transformados en 1.3GB los datos de MB ubicados en la primera tabla

MB	GB
68.3	**1.0**
223.6	**1.1**
996.5	**1.2**
	1.2
	1.3
	1.3
	1.3
	1.4
	1.6
	1.6
	1.7
	1.7
	1.8
	1.8
	1.9
	2.1
	2.3

Total Up &Down	
1.0	**GB**
1.1	**GB**
1.2	**GB**
1.2	**GB**
1.3	**GB**
1.3	**GB**
1.3	**GB**
1.3	**GB**
1.4	**GB**
1.5	**GB**
1.6	**GB**
1.6	**GB**
1.6	**GB**
1.7	**GB**
1.7	**GB**
1.8	**GB**
1.8	**GB**
1.8	**GB**
1.9	**GB**
2.1	**GB**
2.1	**GB**
2.2	**GB**
2.3	**GB**

Imágenes de las pantallas del AP2 teniendo un total de 25 objetos (usuarios)con la conectividad Wisp



Sistema Usuarios Servicios Administradores NASs AP CMTS Grupo de IP Finanzas Sistema de tarjeta IAS Reportes Herramientas

Reporte de trafico

Encontrados: 25

Fecha	Nombre de usuario	Tiempo en linea	Descarga	Subida	Total
2015-04-26	berserk	12:27:14	1.9 GB	211.3 MB	2.1 GB
2015-04-26	berserk	13:52:45	1.6 GB	183.6 MB	1.8 GB
2015-04-27	berserk	14:10:46	1.1 GB	156.3 MB	1.2 GB
2015-04-28	berserk	13:54:39	1.2 GB	208.6 MB	1.4 GB
2015-04-26	berserk	12:47:16	1.5 GB	223.5 MB	1.7 GB
2015-04-26	berserk	14:01:25	1.2 GB	141.0 MB	1.3 GB
2015-04-27	berserk	12:04:23	1.4 GB	232.6 MB	1.6 GB
2015-04-28	berserk	12:08:44	1.1 GB	152.7 MB	1.2 GB
2015-04-26	berserk	12:37:25	1.5 GB	172.7 MB	1.7 GB
2015-04-26	berserk	11:53:13	1.8 GB	165.6 MB	1.9 GB
2015-04-27	berserk	11:18:20	2.1 GB	215.1 MB	2.3 GB
2015-04-28	berserk	09:02:18	1.2 GB	163.2 MB	1.3 GB
2015-04-28	berserk	01:20:03	60.5 MB	7.8 MB	68.3 MB
2015-04-26	berserk	11:38:12	802.1 MB	227.5 MB	1.0 GB
2015-04-28	berserk	13:13:12	960.0 MB	170.7 MB	1.1 GB
2015-04-26	berserk	13:57:20	1.1 GB	203.9 MB	1.3 GB
2015-04-27	berserk	10:58:04	1.6 GB	191.9 MB	1.8 GB
2015-04-28	berserk	07:32:01	909.3 MB	87.1 MB	996.5 MB
2015-04-28	berserk	14:01:05	1.8 GB	334.1 MB	2.2 GB
2015-04-26	berserk	12:49:55	1.3 GB	140.3 MB	1.5 GB
2015-04-27	berserk	12:30:55	1.6 GB	132.4 MB	1.8 GB
2015-04-28	berserk	12:37:50	1.4 GB	122.4 MB	1.6 GB
2015-04-27	berserk	12:42:00	1.8 GB	221.9 MB	2.1 GB
2015-04-28	berserk	06:35:53	213.6 MB	10.0 MB	223.6 MB
2015-04-27	berserk	13:29:48	1.4 GB	184.1 MB	1.6 GB

Encontrados: 25

Servidor DHCP: WISP IPv6

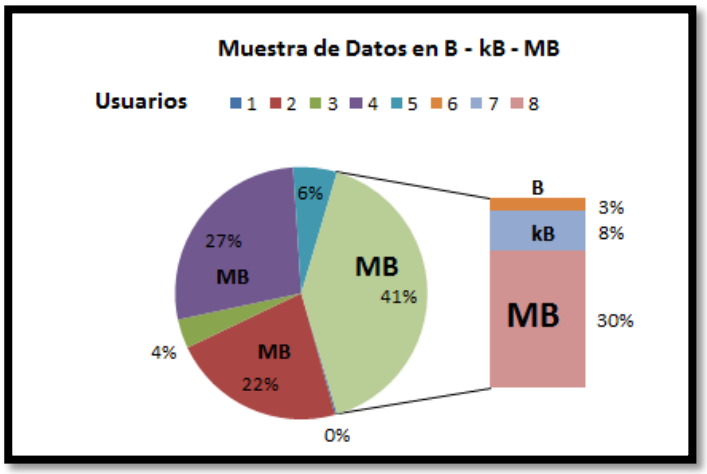
Para AP3:

En la siguiente tabla mostraremos que nos revela el comportamiento de los usuarios según observaciones establecidas.

Muestra AP3

Usuarios	**Tiempo en línea**	**Datos: Voz/Ip/Video**					
	hh:mm:ss	**Descargas**	**Tipo**	**Subidas**	**Tipo**	**Total Up &Down**	**Peso**
1	0:15:06	1.7	MB	312.1	kB	**2.0**	MB
2	5:00:51	172.3	MB	13.4	MB	**185.6**	MB
3	00:37:28	29.8	MB	1.4	MB	**31.2**	MB
4	3:36:08	218.0	MB	10.0	MB	**228.1**	MB
5	0:18:45	180.0	B	220.0	B	**400.0**	B
6	0:53:43	301.6	kB	133.7	kB	**435.3**	kB
7	0:15:06	1.7	kB	12.6	kB	**14.2**	kB
8	2:34:07	38.5	MB	8.3	MB	**46.8**	MB
9	3:07:14	17.6	MB	4.5	MB	**22.1**	MB
10	3:25:27	63.4	MB	6.9	MB	**70.3**	MB
11	6:06:41	232.2	MB	16.3	MB	**248.5**	MB
Total	**25:33:08**	**773.8**	MB	**61.3**	MB	**835.1**	MB

A lo que nos quedaría de la siguiente manera los cálculos respectivos a este AP3 en las nociones estadísticas para determinar la confiabilidad más adelante:



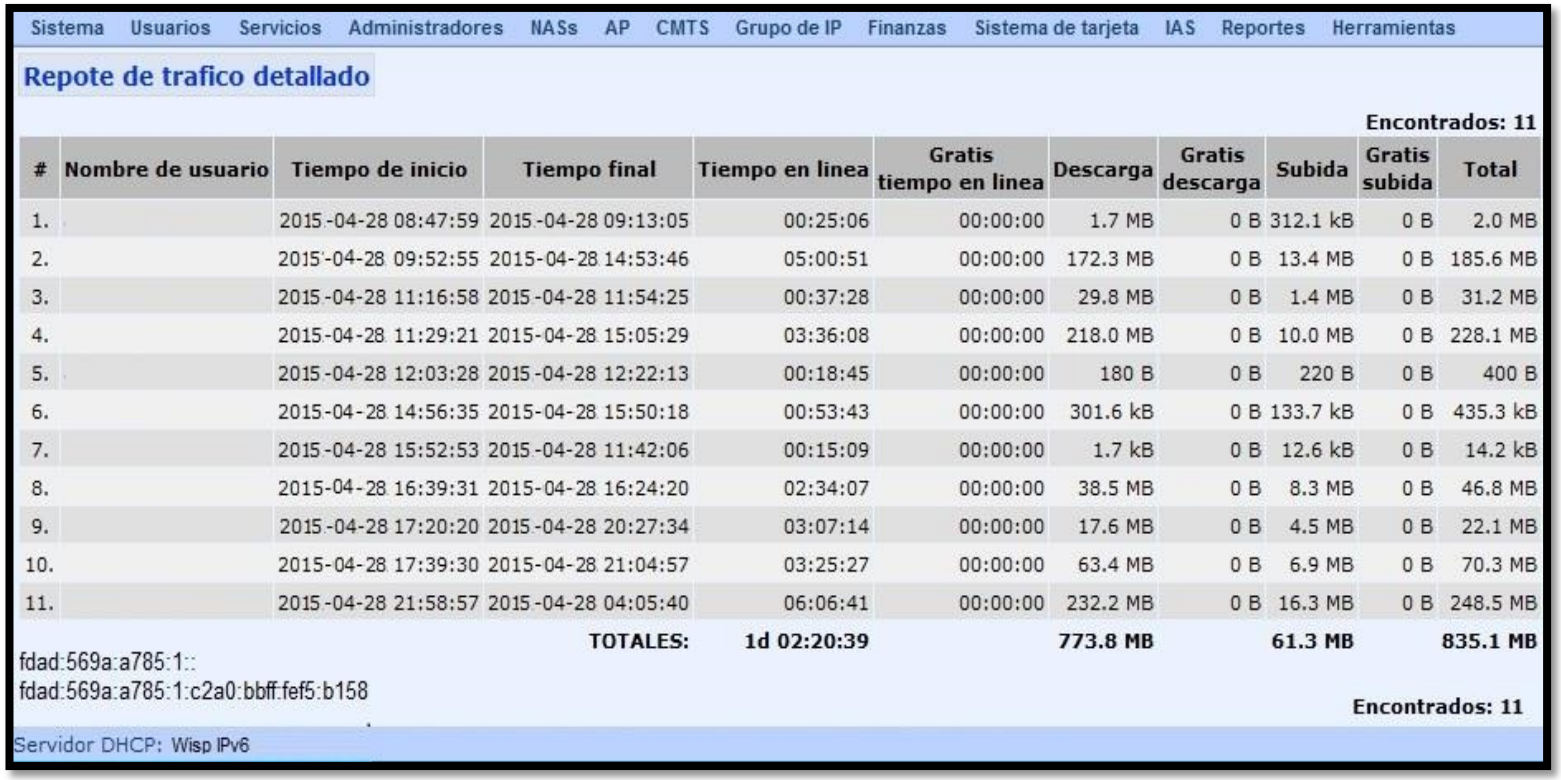
Agrupación de los valores encontrados y puestos de la siguiente manera:

B	kB	MB
400.0	**435.3**	**2.0**
	14.2	**185.6**
		31.2
		228.1
		46.8
		22.1
		70.3
		248.5

Con los datos recolectados en AP3 realizamos la tabla donde mostraremos el cálculo de media, mediana, moda, máximo, mínimo, desviación estándar y varianza que nos revela el comportamiento de los usuarios según mostro grafico anterior.

Noción estadística de los valores Totales de AP3				
	hh:mm	**B**	**kB**	**MB**
Media	**2:33:19**	**400.0**	**224.75**	**92.78**
Mediana	2:50:41	0	0	46.80
Moda	0:15:06	0	0	0
Mínimo	0:15:06	0	0	0.44
Máximo	6:06:41	0	0	248.50
Desviación Estándar	0.088581941	0	0	93.90
Varianza	0.00784676	0	0	9918.84

Imágenes de las pantallas del AP3 teniendo un total de 11 objetos (usuarios) con la conectividad.



Sistema Usuarios Servicios Administradores NASs AP CMTS Grupo de IP Finanzas Sistema de tarjeta IAS Reportes Herramientas

Repote de trafico detallado

Encontrados: 11

#	Nombre de usuario	Tiempo de inicio	Tiempo final	Tiempo en linea	Gratis tiempo en linea	Descarga	Gratis descarga	Subida	Gratis subida	Total
1.		2015-04-28 08:47:59	2015-04-28 09:13:05	00:25:06	00:00:00	1.7 MB	0 B	312.1 kB	0 B	2.0 MB
2.		2015-04-28 09:52:55	2015-04-28 14:53:46	05:00:51	00:00:00	172.3 MB	0 B	13.4 MB	0 B	185.6 MB
3.		2015-04-28 11:16:58	2015-04-28 11:54:25	00:37:28	00:00:00	29.8 MB	0 B	1.4 MB	0 B	31.2 MB
4.		2015-04-28 11:29:21	2015-04-28 15:05:29	03:36:08	00:00:00	218.0 MB	0 B	10.0 MB	0 B	228.1 MB
5.		2015-04-28 12:03:28	2015-04-28 12:22:13	00:18:45	00:00:00	180 B	0 B	220 B	0 B	400 B
6.		2015-04-28 14:56:35	2015-04-28 15:50:18	00:53:43	00:00:00	301.6 kB	0 B	133.7 kB	0 B	435.3 kB
7.		2015-04-28 15:52:53	2015-04-28 11:42:06	00:15:09	00:00:00	1.7 kB	0 B	12.6 kB	0 B	14.2 kB
8.		2015-04-28 16:39:31	2015-04-28 16:24:20	02:34:07	00:00:00	38.5 MB	0 B	8.3 MB	0 B	46.8 MB
9.		2015-04-28 17:20:20	2015-04-28 20:27:34	03:07:14	00:00:00	17.6 MB	0 B	4.5 MB	0 B	22.1 MB
10.		2015-04-28 17:39:30	2015-04-28 21:04:57	03:25:27	00:00:00	63.4 MB	0 B	6.9 MB	0 B	70.3 MB
11.		2015-04-28 21:58:57	2015-04-28 04:05:40	06:06:41	00:00:00	232.2 MB	0 B	16.3 MB	0 B	248.5 MB
			TOTALES:	**1d 02:20:39**		**773.8 MB**		**61.3 MB**		**835.1 MB**

fdad:569a:a785:1::
fdad:569a:a785:1:c2a0:bbff:fef5:b158

Encontrados: 11

Servidor DHCP: Wisp IPv6

Para AP4:

En la siguiente tabla se destaca el comportamiento de los usuarios según con el consumo de datos en GB.

Muestra AP 4

Usuarios	**Tiempo en línea**	**Datos: Voz/Ip/Video**					
	hh:mm:ss	**Descargas**	**Tipo**	**Subidas**	**Tipo**	**Total Up&Down**	**Peso**
1	1:25:49	73.7	MB	72.0	MB	**145.7**	MB
2	9:54:16	55.3	MB	25.5	MB	**80.8**	MB
3	2:58:05	209.1	MB	1.4	MB	**210.5**	MB
4	0:53:00	96.0	MB	45.0	MB	**141.0**	MB
5	7:00:35	1.3	GB	78.0	MB	**1.4**	GB
6	0:53:00	24.9	MB	2.8	MB	**27.7**	MB
7	3:43:55	2.3	MB	95.0	MB	**97.3**	MB
8	0:45:05	9.9	MB	150.0	MB	**159.9**	MB
9	1:45:00	2.6	GB	240.0	MB	**2.9**	GB
10	9:43:07	130.7	MB	12.2	MB	**142.9**	MB
11	0:03:16	411.0	MB	31.0	MB	**442.0**	MB
12	1:33:21	2.0	GB	321.0	MB	**2.4**	GB
13	0:01:30	12.0	MB	50.0	MB	**62.0**	MB
Total	**40:39:59**	**6.9**	**GB**	**1.1**	**GB**	**8.0**	**GB**

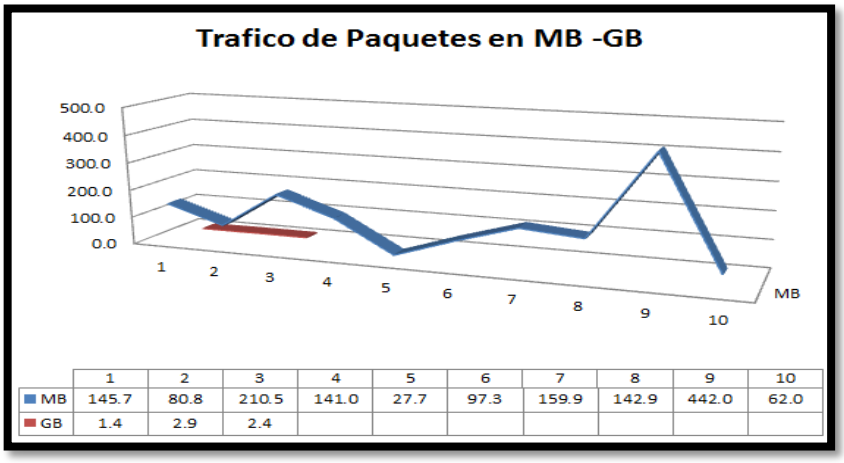
Con los datos recolectados en AP4 realizamos la tabla donde mostraremos el cálculo de media, mediana, moda, máximo, mínimo, desviación estándar y varianza como hemos venido haciendo desde el AP1, AP2 y AP3.

Noción estadística de los valores Totales AP4		
	hh:mm	**MB**
Media	**3:07:41**	**761.0**
Mediana	1:33:21	142.9
Moda	**0:53:00**	0
Mínimo	0:01:30	27.7
Máximo	9:54:16	6,860.8
Desviación Estándar	0.14577	2026.04
Varianza	0.02125	4104823.4

Agrupando los valores tenemos como resultado una tabla y un gráfico expresivo donde se nos revela el comportamiento del consumo la red la internet WISP.

Tabla Agrupada y Grafica AP4

MB	GB
145.7	1.4
80.8	2.9
210.5	2.4
141.0	
27.7	
97.3	
159.9	
142.9	
442.0	
62.0	



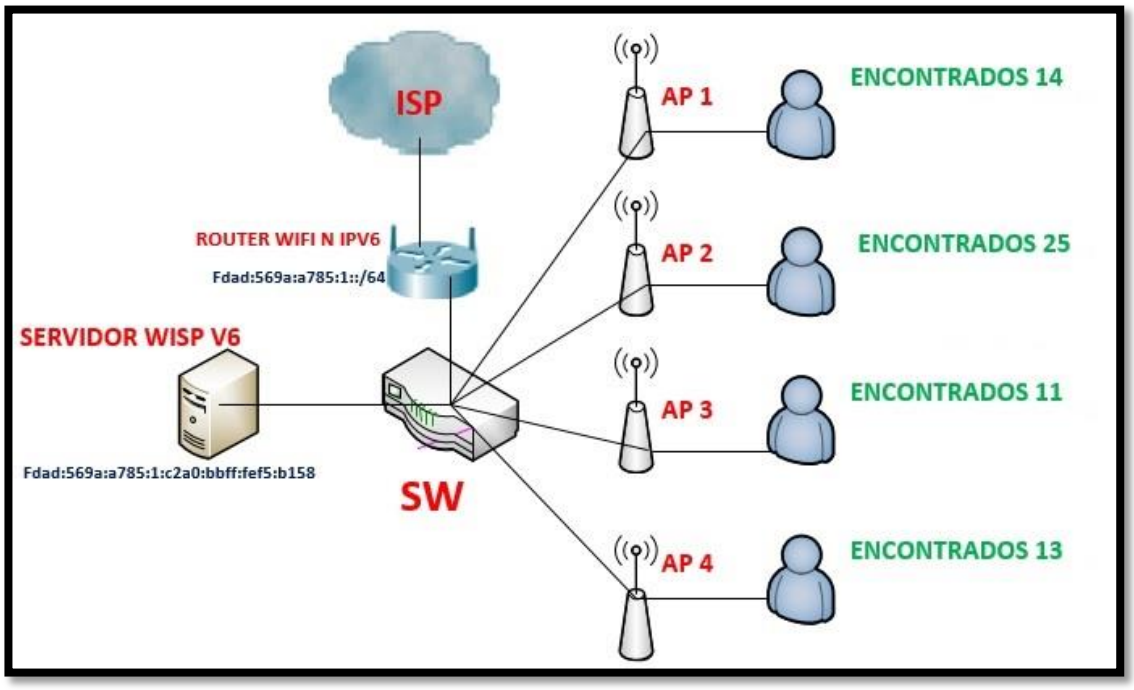
Y para concluir las muestras generales de los datos agrupados de los 4 APs con los que se tomaron las muestras de una manera más global, datos que nos servirán para calcular muestras y confiabilidad del proyecto.

- **Muestras Globales de los APs y Consumo de Datos de los Usuarios con sus diferentes equipos móviles:**

Datos Totales Recolectados de AP en Down & Up							
AP 1		**AP 2**		**AP 3**		**AP 4**	
548.0	B	2.1	GB	2.0	MB	27.7	MB
325.8	kB	1.8	GB	185.6	MB	62.0	MB
1.7	MB	1.2	GB	31.2	MB	80.8	MB
59.3	kB	1.4	GB	228.1	MB	97.3	MB
1.5	MB	1.7	GB	400.0	B	141.0	MB
27.8	MB	1.3	GB	435.3	kB	142.9	MB
2.4	MB	1.6	GB	14.2	kB	145.7	MB
809.5	kB	1.2	GB	46.8	MB	159.9	MB
3.1	MB	1.7	GB	22.1	MB	210.5	MB

142.9	MB	1.9	GB	70.3	MB	442.0	MB
709.1	kB	2.3	GB	248.5	MB	1.4	GB
25.5	kB	1.3	GB			2.9	GB
1.4	kB	68.3	MB			2.4	GB
58.6	MB	1.0	GB				
		1.1	GB				
		1.3	GB				
		1.8	GB				
		996.5	MB				
		2.2	GB				
		1.5	GB				
		1.8	GB				
		1.6	GB				
		2.1	GB				
		223.6	MB				
		1.6	GB				

Usuarios Encontrados en las muestras de los AP



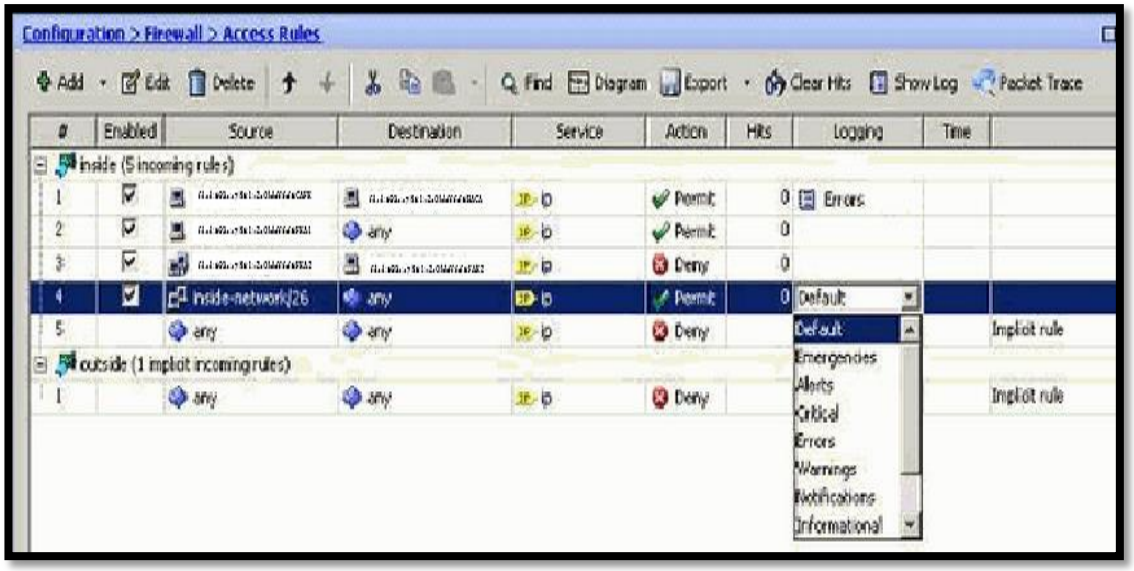
- **CONTROL DE DESCARGAS Y ACCESO EN CASO DE SER NECESARIO.**

Si se preguntan cómo controlar o evitar que el ancho de banda se consuma más por descargas de usuarios en específicos, tenemos el siguiente PLAN a accionar de ser necesario.

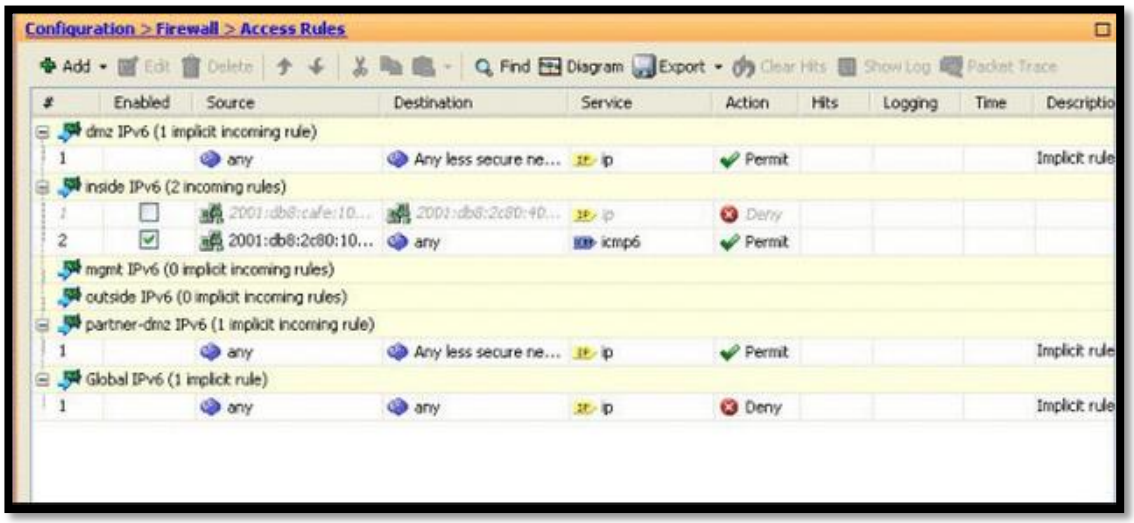
Consistes en la activación de un Firewall que en conjunto con la configuración del Switch se podrá manejar y controlar tráfico entrante y saliente con las descargas e incluso el ingreso a diferentes paginas o segmentos de la red si es necesario con la implementación de ACLs y Vlans.

- **Configuración ejemplo con Firewall**

Interface de firewall para control de permisos.



- **Control de Tráfico y Seguridad**



- **Como quedaría el Diseño con Firewall?**