CAPITULO III

3. ANALISIS Y PRUEBAS DE LA CONECTIVIDAD Y SEGURIDAD DE LA RED INALÁMBRICA Y DE LAS COMUNICACIONES VOIP BAJO ESTANDARES 802.11g

3.1. Introducción

Hace 30 años Internet no existía, y las comunicaciones se realizaban por medio del teléfono a través de la red telefónica pública conmutada (PSTN), pero con el pasar de los años y el avance tecnológico han ido apareciendo nuevas tecnologías y aparatos bastante útiles que nos han permitido pensar en nuevas tecnologías de comunicación: PCS, teléfonos celulares y finalmente la popularización de la gran red Internet.

En nuestro país, en los últimos años las tecnologías han ido avanzando poco a poco y hoy podemos obtener grandes ventajas del Internet en lo que se refiere a las comunicaciones, Voz sobre IP llega a nuestro país para utilizar una comunicación en tiempo real por medio del PC a través del Internet, después de haber constatado que desde un PC con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, se podría pensar que la telefonía en IPv4 es algo más que un juguete, pues la calidad de voz que se obtiene a través de líneas convencionales es muy pobre.

No obstante, si en una empresa se dispone de una red de datos que tenga un ancho de banda bastante grande, también se podría pensar en la utilización de esta red para el tráfico de voz entre las distintas delegaciones de la empresa. Las ventajas que se obtendrían al utilizar la red para transmitir tanto la voz como los

datos son evidentes, ahorro de costos de comunicaciones, pues las llamadas entre las distintas sedes de la empresa saldrían gratis.

Este tipo de comunicación utilizado en muchas empresas y los beneficios que esta brinda hace que el grupo de investigación se plantee realizar un análisis a la voz sobre el Internet Protocol en una red inalámbrica ya que justificaría siempre y cuando los anchos de banda que aquí se manejan puedan satisfacer a los usuarios de este tipo de tecnología.

3.2. Justificación

Nuestro grupo en calidad de estudiantes de la carrera de Ingeniería en informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi hemos escogido este tema de investigación que se encuentra relacionado con nuestra especialidad y con los conocimientos que hemos adquirido en los años de estudio presencial.

Con la implementación de voz sobre IP se optimizara la comunicación entre distintos sitios de una empresa al mantener una comunicación directa y eficaz en el envió y recepción de datos de voz, a la vez se evitara la pérdida de tiempo al realizar llamadas de larga duración cuando se tenga que realizar una transacción vía telefónica

Actualmente las instituciones no cuentan con este tipo de comunicación ya que esta es una nueva tecnología que no se encuentra establecida en su totalidad en las diferentes empresas del país.

Los empleados de las distintas empresas en la que se va a realizar el presente trabajo de investigación utilizaran Voip como un medio de comunicación eficiente mejorando la coordinación.

Por lo expuesto anteriormente nuestra propuesta de investigación es factible de realizar ya que contamos con los medios necesarios para la ejecución de lo planificado.

3.3. Objetivos

- ✧ Recopilar la información bibliográfica necesaria para realizar el análisis de las herramientas de hardware y software mediante libros y sitios web.

- ✧ Analizar e interpretar los resultados obtenidos de la aplicación de los instrumentos de investigación para obtener información aplicando la estadística descriptiva.

- ✧ Efectuar un análisis de requerimientos para la configuración Voip para obtener la información específica para el desarrollo de esta aplicación definiendo su funcionalidad y objetivos utilizando las técnicas de investigación.

- ✧ Establecer parámetros de seguridad en el sistema operativo evitando el mal uso del mismo.

3.4. Análisis

Para poder realizar un análisis completo de la implementación de la red inalámbrica tenemos que tener en cuenta algunos conceptos que van a ser repetidos durante la fase de análisis y diseño, esto son:

3.4.1. Mecanismo de acceso

Hay de dos tipos:

Protocolos con arbitraje (FDMA - Frequency División Múltiple Access, TDMA - Time División Múltiple Access)

Protocolos de contienda (CDMA/CA - Carrier-Sense, Múltiple Access, Colusión Avoidance), COMA (Code División, Múltiple Access) y el CDMA/CD (detección de colisión).

3.4.1.1. Protocolos con arbitraje

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para

evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

3.4.1.2. Protocolos de acceso por contienda

Tienen similitudes al de Ethernet cableada de línea normal 802.3:

3.4.1.2.1. CSMA

(Code-division múltiple access = Acceso múltiple por división de tiempo).

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia. En este esquema se asigna una secuencia distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias pertenecientes a los demás nodos.

Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

3.4.1.2.2. CSMA/CD

(Carrier Sense, Múltiple Access, Colusión Detection)

En medios de transmisión tales como radio e infrarrojos, no es posible transmitir y recibir al mismo tiempo, la

detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseñó una variación denominada detección de colisiones (peine) para redes inalámbricas.

En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria pseudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama.

A continuación, el nodo realiza la detección de la portadora si el canal está ubre transmite la secuencia del peine. Por cada "1" del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada "O" del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

3.4.1.2.3. CSMA/CA

(Carrier-Sense, Múltiple Access, Colusión Avoidance)

Es el más utilizado, este protocolo evita colisiones en lugar de descubrirlas.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD

debido a que entre el final y el principio de una transmisión suelen provocarse colisiones.

En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI.

Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El Standard proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible.
Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802. 11.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido).

3.4.2. Seguridad

En el standard se dirigen suministros de seguridad como una característica optativa para aquellos afectados por la escucha secreta, es decir, por el "fisgoneo". Incluye dos aspectos básicos: autentificación y privacidad.

La seguridad de los datos se realiza por una compleja técnica de codificación, conocida como WEP (Wired Equivalent Privacy Algorithm).

WEP se basa en proteger los datos transmitidos en el medio RF, usando clave de 64 bits y el algoritmo de encriptación RC4 (desarrollado por RSA Security Inc.). La clave se configura en el punto de acceso y en sus estaciones (clientes wireless), de forma que sólo aquellos dispositivos con una clave válida puedan estar asociados a un determinado punto de acceso.

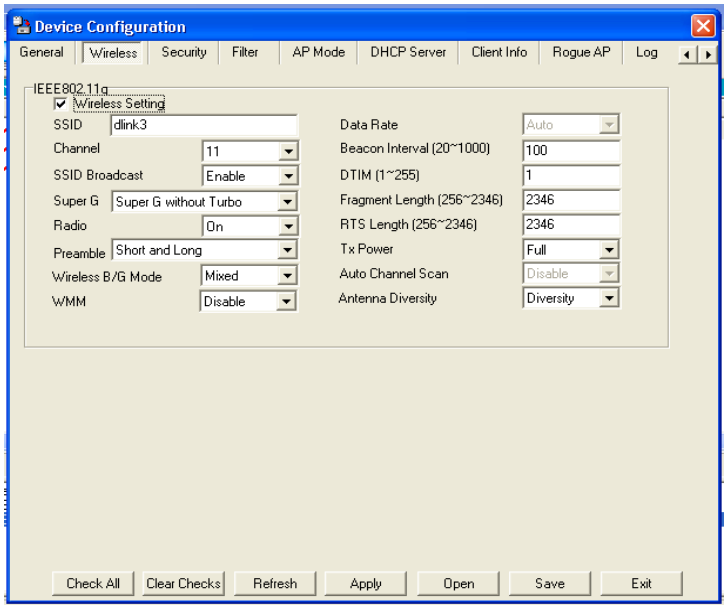
WEP, cuando se habilita, sólo protege la información del paquete de datos y no protege el encabezamiento de la capa física para que otras estaciones en la red puedan escuchar el control de datos necesario para manejar la red. Sin embargo, las otras estaciones no pueden distinguir las partes de datos del paquete.

Se utiliza la misma clave de autentificación para encriptar y desencriptar los datos, de forma que solo las estaciones autorizadas puedan traducir correctamente los datos.

Para la investigación se consideran 2 aspectos de seguridad a más del antes ya mencionado como lo es WEP, además tenemos las configuraciones propias del Acive Directory de Windows 2003, y el filtro por direcciones MAC de las tarjetas de red inalámbricas instaladas en las computadoras.

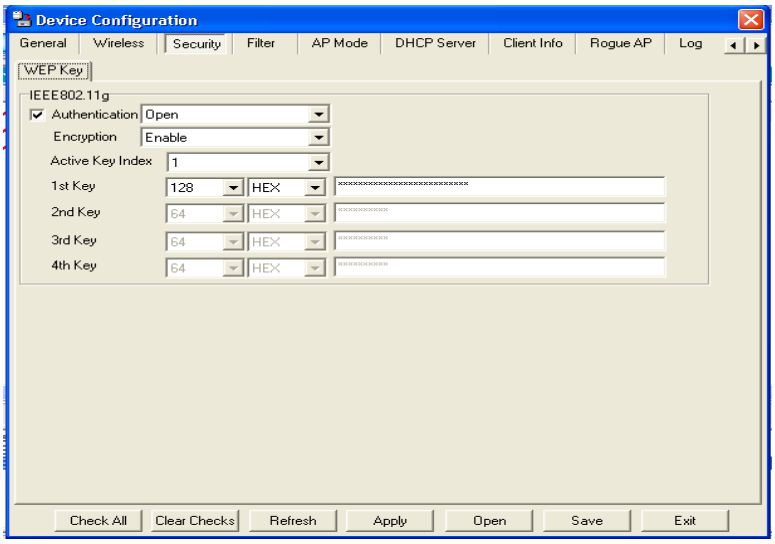
Todo esto se encuentra mejor explicado en la parte inferior de forma Gráfica.

Gráfico 3.1: Pantalla de configuración de Contraseñas en el AP
Fuente: Grupo Investigador



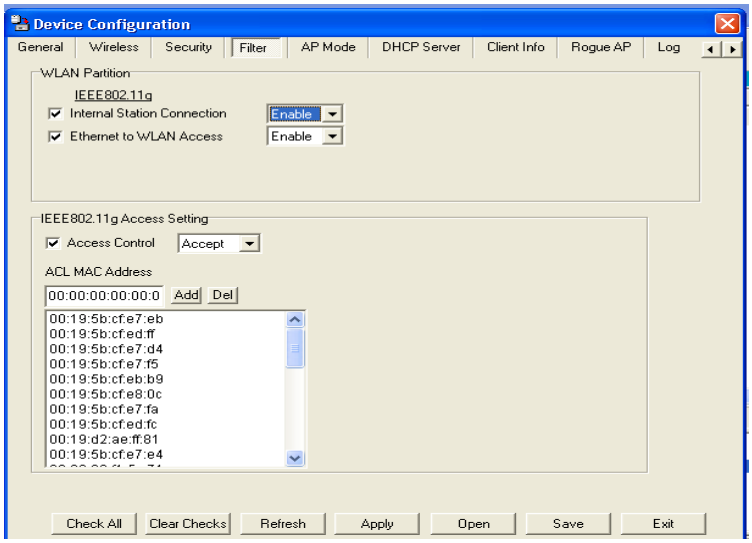
En la gráfica superior se muestra la pantalla de la configuración: SSID(**ESSID (Extended Service Set Identifier):** Nombre único de hasta 32 caracteres para identificar a la red wireless. Todos los componentes de la misma red WLAN deben usar el mismo), Channel(Canal: Una porción del espectro de radiofrecuencias que usan los dispositivos para comunicarse. El uso de diferentes canales ayuda a reducir interferencias canal de uso por defecto viene 6), SSID Broadcast (activar o desactivar el nombre la red), SuperG (Para transferencia de 108 mbps).

Gráfico 3.2: Pantalla de configuración de WEP
Fuente: Grupo investigador



En la pantalla superior la filtración de claves WEP para los usuarios de la red inalámbrica en Hexadecimal o ASCII, y como se puede observar el estándar utilizado en este proyecto es el 802.11g que es el estándar que mas seguridades proporciona en la actualidad.

Gráfico 3.3: Pantalla de configuración de Filtración MAC.
Fuente: El investigador



En la gráfica superior se puede observar la tercera alternativa de encriptación el filtrar las macs de los equipos de la red de cada uno de los usuarios.

3.4.3. Funcionalidad adicional

En las LAN inalámbricas la capa de MAC, además de efectuar la función de controlar el acceso al medio, desempeña otras funciones;

Fragmentación
Control de flujo
Manejo de múltiples tasas de transmisión
Gestión de potencia

En los diferentes tipos de LAN por cable es posible usar tramas grandes gracias a errores de bit bajos. En las LAN inalámbricas, el multicamino y las interferencias pueden elevar considerablemente los valores de errores de bit.
Para poder transmitir eficientemente por estos medios, hay que reducir el tamaño de las tramas. La capa MAC se encarga de fragmentar las tramas en otras más pequeñas antes de transmitirlas por el medio inalámbrico.

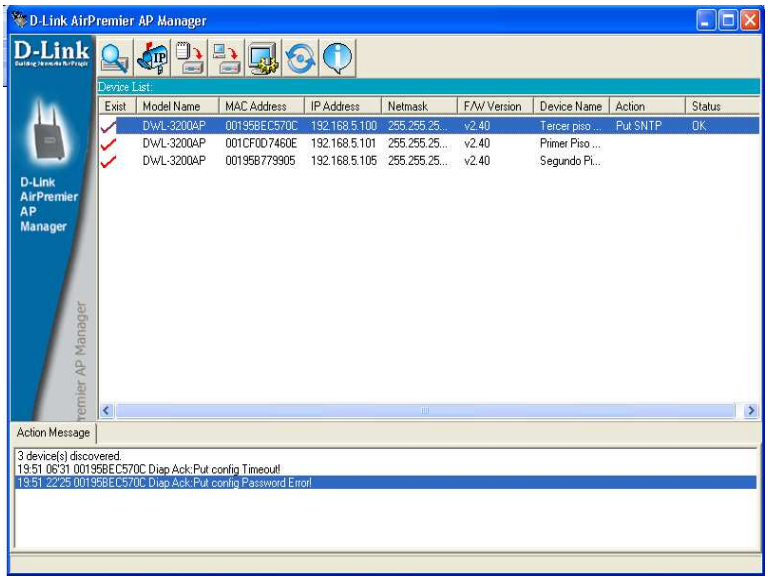
De la misma manera deberá ensamblar las tramas para obtener la trama original antes de entregarla a la capa superior.

También debe cumplir un control de flujo, cada vez que un segmento sea pasado a la capa física, deberá esperar que este sea transmitido antes de enviar el próximo segmento.

La gestión de la potencia se apoya en el nivel MAC para esas aplicaciones que requieren movilidad bajo el funcionamiento de la pila.

Se hacen provisiones en el protocolo para que las estaciones portátiles pasen a "modo dormido" durante un intervalo de tiempo definido por la estación base.

Gráfico 3.4: Pantalla de Detección de los AP.
Fuente: El investigador



En la parte superior observamos un gráfico de la configuración de los Access Point mediante las direcciones MAC(Funcionalidad), esto con el fin de ver las replicas que tiene.

3.4.4. Pasos básicos para asegurar una WLAN

El propósito de asegurar correctamente un punto de acceso(AP) es cortar el paso desde el exterior a nuestra red a personas que no tienen el permiso de entrar, es decir asegurar que la información fluya internamente.

Una red wireless es por definición más difícil de proteger que una red convencional o cableada entre otras cosas porque el medio es el aire y así como en una LAN tenemos unas tomas de red determinadas y

controladas, en principio, en una WLAN se puede acceder desde cualquier punto que permita la antena.

A pesar de esto siempre se pueden establecer una serie de medidas básicas pero efectivas no en el 100% de los casos pero se impide el acceso a la gran mayoría de los intrusos.

Para establecer este nivel básico de seguridad se debe realizar los siguientes pasos:

3.4.4.1. Colocación de la antena

El primer paso para cerrar el acceso no autorizado a un punto de acceso es colocar la antena de éste, de manera que limite el alcance de la antena al área de trabajo.

Nunca hay que colocar una antena cerca de una ventana ya que el cristal no bloquea la señal. Un esquema ideal sería colocar la antena en el centro del área dejando que solo una leve señal escape a través de los muros o ventanas de la oficina o lugar de trabajo. Si es imposible controlar este factor todavía se pueden tomar otras medidas de seguridad adicionales.

De acuerdo al número de usuarios en una oficina y como está se encuentre distribuida están ubicados los AP, cuando las oficinas no son muy grandes se procedió a colocar sobre las ventanas interiores del edificio para aprovechar el espacio de cobertura y que pueda abastecer las dos oficinas, como se muestra en la grafica siguiente:

Gráfico 3.5: Ubicación de los Access Point.
Fuente: El investigador

3.4.4.2. Usar seguridad

La seguridad es el problema más importante al que se enfrenta actualmente la tecnología WiFi, ya que si no se utilizan los medios adecuados acceder a una red WiFi protegida puede resultar relativamente sencillo.

Un gran número de redes inalámbricas son instaladas por administradores de redes y sistemas sin tener en cuenta políticas de seguridad. Lo que se traduce en una red abierta que no protege la información que circula por ella.

Al diseñar una red WiFi es necesario combinar dos tipos de seguridades:

- Físicas.
- Lógicas, que son las que ya se encuentran detalladas en un ítem anterior.

Las seguridades Físicas están dadas por las bondades que nos puede ofrecer la edificación, ya que al ser funcional como es nuestro caso el Departamento de Sistemas cuenta con un plan de

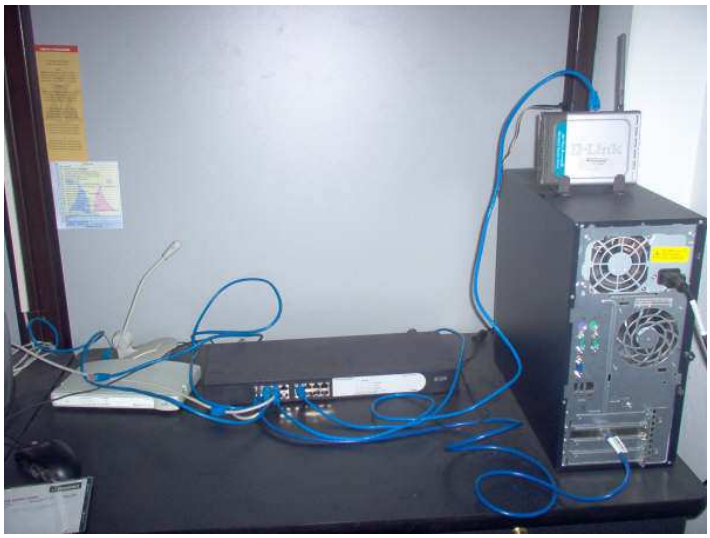
contingencia el mismo que va desde posibles desastres hasta invasión de un hacker.

Al hablar de hackers no debemos dejar de lado que el ataque puede ser interno por lo que se tomo la decisión de que solo un cable conecte al primer AP, este a su vez vía inalámbrica conecte al segundo piso y este replique su señal hacia un piso más abajo, de está manera estaríamos cubriendo toda la edificación como se puede observar en los planos del edificio en el anexo 3.

Gráfico 3.6: Ubicación de los Access Point.
Fuente: El investigador

En la grafica anterior se encuentra el Access Point que hace de base para las comunicaciones con los otros AP’s, es decir viene siendo una especie de Switch de Core y los que se encuentra en los otros pisos hacen de Switch de Enlace.

Gráfico 3.7: Ubicación de los Access Point.
Fuente: El investigador



Ventajas de la Implementación de una WLAN

- **Movilidad**: El usuario tiene acceso tanto a los recursos privados y públicos pertenecientes a la red desde cualquier lugar que pertenezca al área de cobertura de la red local WLAN, que es de gran beneficio para nosotros por los constantes cambios de edificios.

- **Flexibilidad**: Permite disponer de conectividad en aquellos lugares en los que realizar una conexión cableada es físicamente imposible o cuyo coste es prohibitivo. Además los usuarios pueden conectarse y desconectarse cuando sea necesario y de forma muy sencilla a distintas redes WLAN según se encuentren en un lugar o en otro, en distintos lugares de trabajo, aeropuertos, hoteles,…

- **Coste**: El coste y el tiempo de instalación disminuyen ya que no es necesario realizar la instalación de cableado. Es

una solución óptima cuando de trata de conexiones temporales y que cambian de lugar.

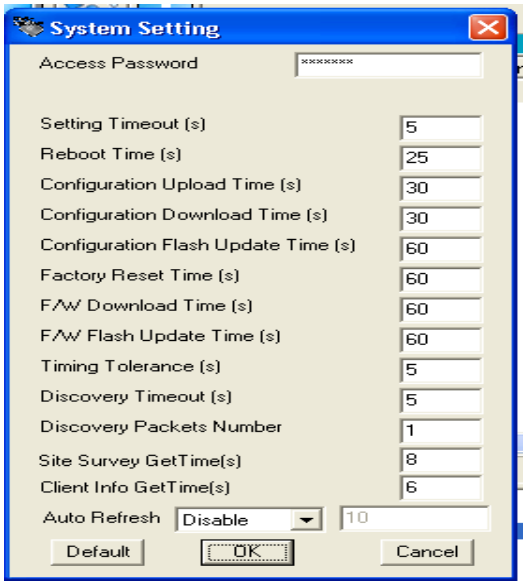
- **Escalabilidad**: La topología de la red se puede modificar muy fácilmente, se pueden añadir nuevos usuarios y dispositivos a la red sin modificar a los ya existentes. Lo que supone además una mayor libertad cuando se producen cambios organizativos dentro de la empresa.

- **Compatibilidad**: Las redes WLAN son completamente compatibles con todos los servicios de las redes LAN cableadas, como por ejemplo la transmisión de voz (**VoIP**) y video por la red. Se pueden realizar llamadas a través de Internet utilizando teléfonos WiFi, siempre que se cuente con la arquitectura de red adecuada.

3.4.4.2.1. Configuraciones

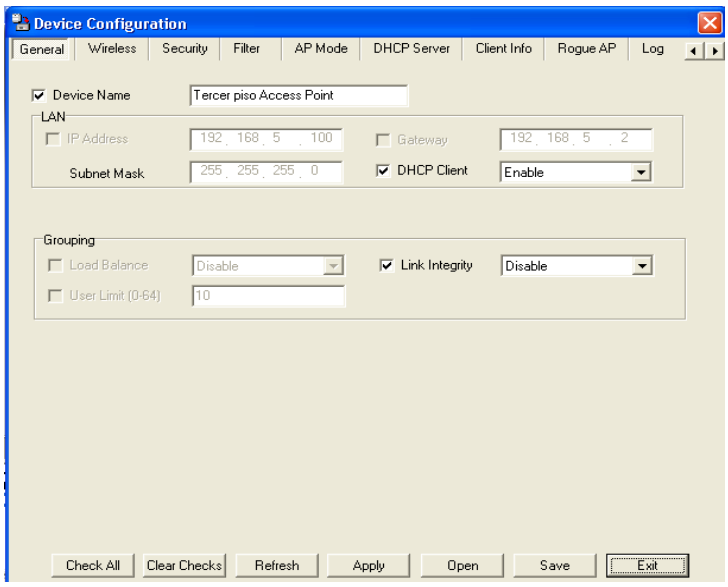
Las configuraciones para el presente trabajo de investigación en las oficinas de la Diocesis se lo realizo de acuerdo a los estándares que rigen la IEEE(Instituto de Ingenieros Eléctricos y Electrónicos), de igual manera se tomo como referencia las recomendaciones que vienen los manuales de los Access Point.

Gráfico 3.8: Configuración de los Access Point.
Fuente: El investigador



En la pantalla que se encuentra en la parte superior está la pantalla de configuración de passwords para el acceso o no al Access Point.

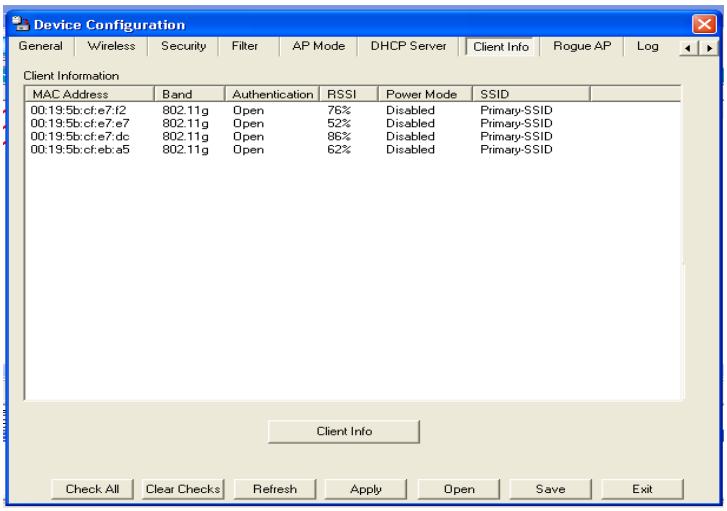
Gráfico 3.9: Configuración de los Access Point.
Fuente: El investigador



Este Gráfico nos muestra la pantalla principal de configuración de los AP, que para nuestro caso el principal está con la IP 192.168.5.100, tenemos habilitada la opción

de DHCP para la asignación de IP a todos los equipos que se conecten a la red inalámbrica.

Gráfico 3.10: Configuración de los Access Point.
Fuente: Grupo investigador

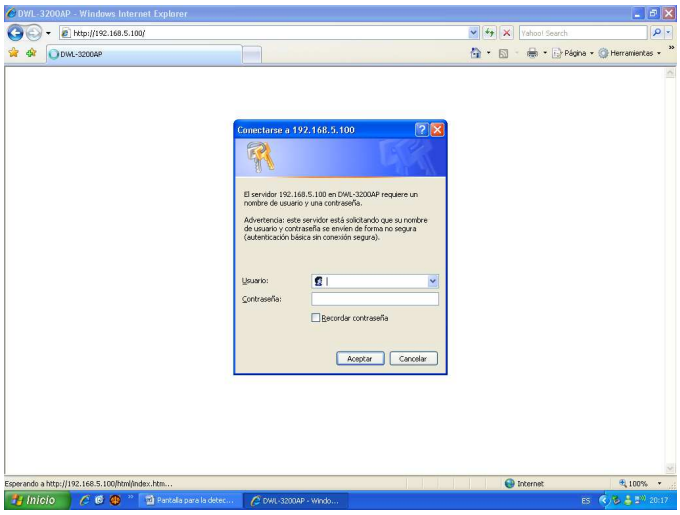


Una vez configurado el AP, debemos tener bajo administración todos los equipos que acceden al concentrador, esto se lo puede hacer mediante las direcciones IP o con las direcciones MAC de las tarjetas de red.

3.4.4.2.2. Configuración WEB

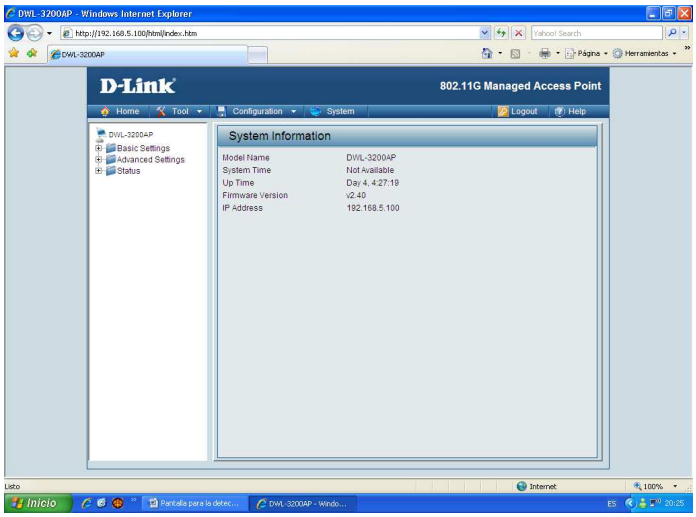
En la actualidad la gran mayoría de configuraciones de equipos se los hace remotamente, es así que la marca DLINK ofrece está opción de realizar configuraciones vía WEB.

Gráfico 3.11: Configuración Web de los Access Point.
Fuente: Grupo investigador



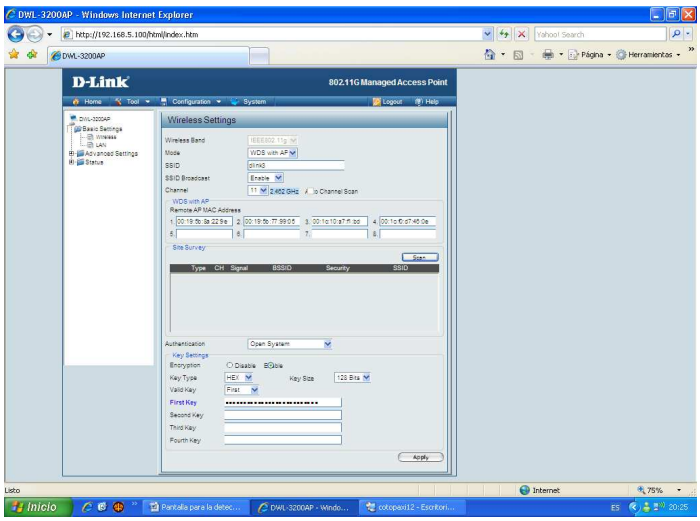
Pantalla de ingreso mediante contraseñas a la página de configuración vía Web del AP principal.

Gráfico 3.12: Configuración Web de los Access Point.
Fuente: Grupo investigador



Pantalla principal de las configuraciones de los AP´s mediante páginas web, en esta se encuentra todas las opciones configurables de la red inalámbrica.

Gráfico 3.13: Configuración Web de los Access Point.
Fuente: Grupo investigador



Pantalla para filtrado MAC, una vez ingresado aquí las direcciones de las tarjetas de red, la red inalámbrica le permitirá conectarse caso contrario no se lo podría hacer, ya que es una de las tres distintas formas de seguridades que se gestiona.

3.4.4.2.3. Funcionamiento

Para poder poner en práctica el funcionamiento debemos tener instalado en todos los computadores tarjetas de red inalámbricas, ya que es el elemento principal que se necesita para poder entrar dentro de la cobertura de las redes inalámbricas.

Gráfico 3.14: Instalación tarjeta de Red Inalámbrica.
Fuente: Grupo investigador

En la grafica anterior se puede observar la instalación de la tarjeta de red de inalámbrica en el CPU, en la parte posterior se puede observar la antena de la tarjeta.

Gráfico 3.15: Configuración tarjeta de Red Inalámbrica.
Fuente: El investigador

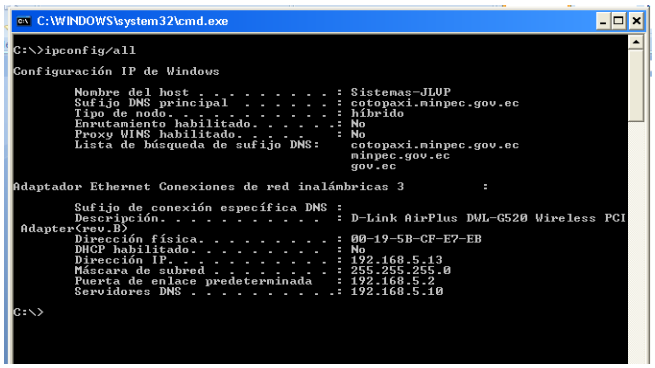
En la gráfica anterior podemos observar como la tarjeta inalámbrica detecta la cobertura que tiene, que en nuestro caso dispone de 100Mbps para lo que es la red LAN.

Gráfico 3.16: Configuración tarjeta de Red Inalámbrica.
Fuente: Grupo investigador

Nos brinda la opción de los AP's dependiendo el radio de cobertura de cada uno de los dispositivos se puede acceder a la red inalámbrica como se puede observar en la gráfica anterior.

De igual manera podemos darnos cuenta que nuestros equipos disponen de un muy buen radio de cobertura el mismo que no está limitado para ningún número de usuarios.

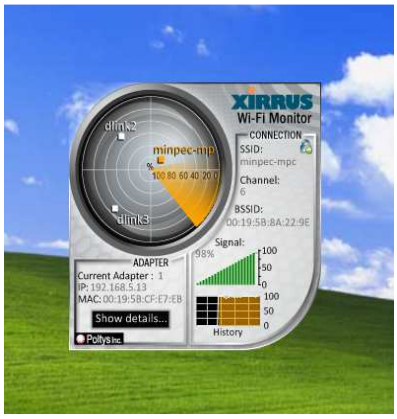
Gráfico 3.17: Configuración Dirección IP de la Red Inalámbrica.
Fuente: Grupo investigador



Podemos observar como el DHCP asigna la dirección IP dinámica a la computadora que solicita este servicio.

Otra de las maneras es mediante el rastreo en forma de radar:

Gráfico 318: rastreo en forma de radar
Fuente: Grupo investigador

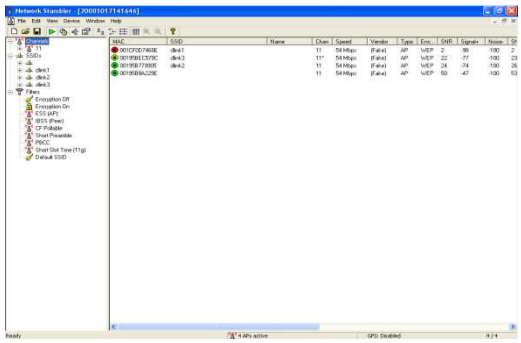


3.4.4.3. Análisis de las seguridades implementadas

Network Stumbler es un scanner Wireless para plataforma Windows, y es el programa que utilizaremos para localizar las redes fig. 3.21 wireless con nuestra tarjeta de red. Es un programa basado en consola de monitoreo con muchas opciones que nos da información como la dirección MAC, el nombre de la red, la velocidad de la red, en algunos casos nos da la información o nombre del fabricante del Acces Point, el tipo de encriptación, entre otros datos.

El Netstumbler sólo detecta las redes que hacen Broadcast de SSID, no detecta redes Hidden o Cloacked. Para entender mejor este trabajo vamos a explicar de forma muy general algunos parámetros utilizados en el programa Network Stumbler (Netstumbler).

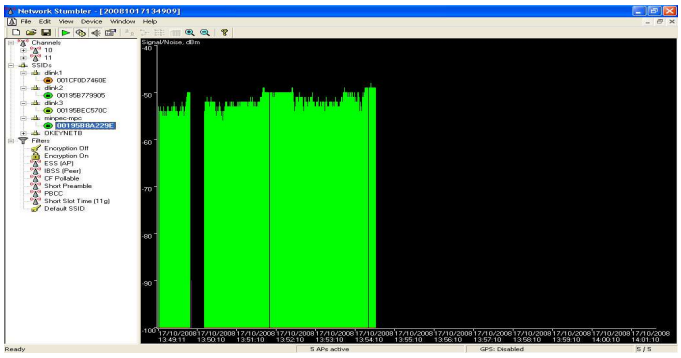
Gráfico 3.19: rastreo en forma de radar
Fuente: Grupo investigador



En el siguiente grafico nos muestra el porcentaje o la intensidad de la señal de conectividad de la tarjeta inalámbrica con el Access Point el mismo que esta deshabilitado el SSID BROADCATS.

Gráfico 3.20: Porcentaje de la Intensidad de la Señal

Fuente: Grupo investigador



Wirelessmon

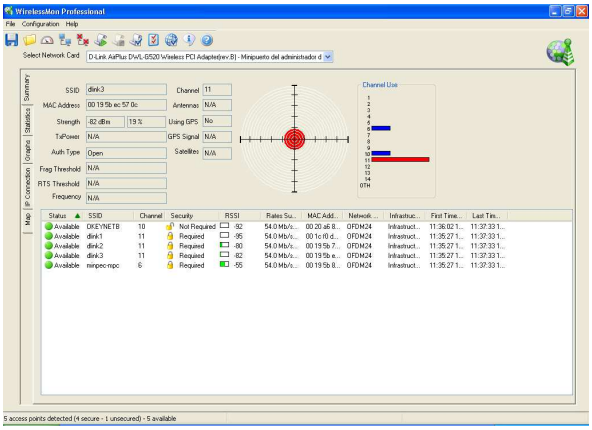
Con este software podemos ver las redes inalámbricas que están dentro del alcance de nuestra antena de la tarjeta de red inalámbrica.

En este grafico se muetra la señal de intensida de cada uno los acces point que nuestra tarjeta de red inalambrica puede capatr o

estan al alance en el mismo que esta habilitadoi el SSID (minpec-mpc) para que todas las personas puedan ver el nombre de nuestro Access Point.

Gráfico 3.21: Habilitación del SSID

Fuente: Grupo investigador



3.5 Análisis y Pruebas de VoIP (Voice over Internet Protocol, Voz sobre Protocolo de Internet)

Para el diseño de voz sobre la red, por medio del protocolo IP debemos considerar los siguientes puntos:

- Grado o porcentaje del tráfico de voz total que utilizara IP, VoIP

- El códec utilizado, es necesario tomar una solución de compromiso entre calidad y ancho de banda

- El protocolo de señalización a utilizar, tanto para conexiones internas como para comunicaciones con otros usuarios/operadores

- El análisis de la calidad de voz, con las nuevas infraestructuras y equipos, aparecen nuevos factores de degradación a la calidad y es necesario realizar nuevas medidas de los Gestores de Infraestructura que demandan servicios orientados a las necesidades de negocios de sus organizaciones.

- La gestión de presupuestos restrictivos y la necesidad de atención en tiempo real de las incidencias, solicitudes de servicio, cambios y problemas que se presentan continuamente implican que sea necesaria la aplicación de metodologías y herramientas para el éxito en la gestión de los Sistemas de Información y la atención a los usuarios.

3.5.1 Grado de integración

La Telefonía sobre IP ha venido creciendo y adaptándose a las necesidades de los usuarios, por lo que podemos decir que el mercado detecta una nueva necesidad en el usuario y crea las herramientas necesarias para cubrirla. En la actualidad la telefonía IP cubre tres escenarios:

- El primer escenario, lo realizamos por medio de una IP PBX, la cual nos permite interconectarnos entre los puntos de una red privada, en donde podemos colocar equipos IP o softphones para este propósito, realizando llamadas sin costo.

- El segundo escenario, los usuarios se conectan a través de Internet a otros usuarios que tengan direcciones IP públicas, la llamada entre equipos IP son gratuitas.

- El tercer escenario, tiene dos partes que se completan; las llamadas por medio de proveedores ITSP (Internet Telephony Service Provider) a través de la red de Internet dirigida a la telefonía PSTN, teniendo el costo de interconexión con su destino, y la fusión de la telefonía PSTN y VoIP en una sola central IP PBX.

Las aplicaciones de VoIP están aún abiertas y se presentan como el conjunto de posibilidades y servicios interminables y aun sin definir para las distintas aplicaciones internas. La oficina en casa, el desvío de mensajes de voz o videoconferencia son servicios que están emergiendo ahora y que crean nuevas necesidades que el usuario va a demandar a corto plazo. Ya queda lejos la época en la que los clientes pensaban solo en “ahorro” al pensar en VoIP, comienza la época de la calidad.

3.5.2 Protocolos de datos (códec)

El plano de datos (Voz) es el proveedor necesario para llevar el tráfico de un usuario a otro. La elección del códec es el primer factor que interviene en la calidad de la llamada VoIP. Generalmente, cuanto mayor es la tasa de bits que

utiliza el códec, mayores son la calidad y el ancho de banda, con lo que se permiten un número menor de llamadas simultáneamente.

Para los objetivos planteados para el presente trabajo debemos tomar en cuenta el ancho de banda que nos ofrece el sistema de Internet ISP que es de 128 Kbps simétrico.

3.5.3 Protocolos del plano de control

Los protocolos de señalización permiten a los usuarios interconectar sus teléfonos de Voz sobre IP. Hay muchos tipos de protocolos de señalizaron diferentes, para nuestro diseño se ha quedado por el H.323V4.

El H.323 es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPBX sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol).

Este estándar define un amplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define mucho más que los terminales. El estándar define los siguientes componentes más relevantes:

- Terminal
- Gateway
- Gatekeeper
- Unidad de Control Multipunto (MCU)

3.5.4 Medidas de calidad de voz

En una red, aparecen numerosos elementos o factores que afectan a la calidad general. El elemento que más afecta a la calidad de las llamadas de VoIP es el diseño, implementación y uso de la red en la que tiene lugar estas llamadas.

Una llamada típicamente se originara en un CPE (Equipo de Premisas de Cliente), circulara primero a través de la LAN del cliente, circulara posteriormente a través de un enlace WAN, la red del proveedor de servicios y vuelve a otra red LAN y por último el CPE del extremo remoto. Equipo CPE y los enlaces WAN son los más vulnerables a factores degradantes.

Hay varios puntos en los que puede afectar a una llamada de VoIP, como son jitter de paquete, la perdida de paquete y retardo.

Jitter de Paquete- está causado por la diferencia de tiempo de llegadas de los distintos paquetes IP. Estos paquetes deberían llegar sin espacios para tener la misma calidad que una conversión real.

Perdida de paquete – es la pérdida de uno o más paquetes. A menudo esta causado por la configuración en la red o por la poca calidad del enlace.

Retardo- es el tiempo que necesita la voz para viajar desde el micrófono de un teléfono al auricular del teléfono remoto, es la suma del retardo que introduce el CÓDEC seleccionado, el buffer del jitter en el teléfono y el trayecto utilizado para transportar los paquetes a través de la red.

3.5.5 MEDICIÓN DE LA QoS.

Hay muchos métodos para medir la calidad de una llamada de VoIP, pero en general existen dos grandes grupos, de forma intrusita o con tráfico real.

Intrusita: no es en tiempo real, equipos en dos extremos.

Con tráfico real: en tiempo real de la comunicación.

Estos métodos utilizan el envío de una señal conocida a través de la red, la captan en el otro extremo, y la comparan con la señal enviada. Se estudia la degradación de la señal recibida con la original, debido a la dificultad de analiza las señales, los equipos que utilizan este método tienen una complejidad elevada y no pueden realizar el análisis en tiempo real de la red en todo momento. Los algoritmos más utilizados para esta comparación son:

- PSQM.- Percentual Speech Quality Measurement, está diseñado para evitar la naturaleza subjetiva del Mean Opinion Score (MOS) y el proceso que resulta necesario para MOS, esfuerzo y recursos para

conseguir reunir un gran número de personas en una habitación y que escuchen innumerables llamadas VoIP. Las medidas PSQM se realizan transmitiendo una señal conocida, analizándola después del códec, en el otro extremo, se degrada se compra con la original y de este modo se obtiene un valor PSQM. Sin embargo estas medidas fueron diseñadas para analizar solo los efectos de la compresión/descompresión de las funciones del códec. Es decir, PSQM, no tiene capacidad de analizar los efectos por el trayecto a través de la red, como pueden ser la pérdida o el jitter de paquetes.

- PESQ y PAMS, fueron diseñados para aumentar el rango que cubría las medidas PSQM, incluir distorsión, filtrado y otras desigualdades del canal. Pero tampoco analizan todos los factores.

3.6 Medio de comunicación (teléfono)

3.6.1 Teléfono Generic IP-AU100 y el USB Phone K60606

Los teléfonos Generic IP-AU100 con soporte para voz sobre IP y el USB Phone K60606, cumplen con los criterios planteados en el diseño por ser uno de los teléfonos pioneros en el mercado de la telefonía sobre IP, el precio los vuelven cómodos y atractivos.

Para trabajar con VoIP y para explotar las virtudes que presentan los equipos se los debe configurar junto con una PBX.

3.6.1.1 Funciones del Generic IP-AU100

- Compatible con Usb 2.0
- Control de volumen
- Llamadas de PC a PC
- Llamadas de PC a teléfono
- No requiere cable de poder
- Práctico tamaño
- Compatible con sistemas operativos Windows 2000, XP, Vista

3.6.1.2 Funciones del USB Phone K60606

- Identificador de llamadas
- Llamadas de PC a PC
- Llamadas de PC a teléfono
- Compatible con Usb1.1 y 2.0
- Compatible con sistemas operativos Windows 2000, XP, Vista
- Procesador de 400 Mhz o más
- No requiere tarjeta de sonido
- Reducción de ruido

3.7 Implementación de un sistema de Voz sobre IP VOIP

Para la implementación de un sistema VoIP necesitamos instalar en primer lugar una IP-PBX, que para nuestro proyecto es la central 3CX, su distribución no es gratuita, lo cual nos facilitará que se pueda conectar un número indeterminado de teléfonos para hacer llamadas entre sí e incluso conectarnos por un VoIP.

Una vez instalado el software de 3CX, procedemos a configurar las extensiones necesarias, desde la central IP-PBX.

3.7.1 Central IP-PBX con 3CX

La Centralita telefónica 3CX para Windows es una Centralita telefónica que reemplaza completamente a los sistemas telefónicos propietarios tradicionales; soporta teléfonos SIP virtuales/físicos de SIP-H.323 estándar, servicios VOIP y líneas telefónicas tradicionales, ofreciendo numerosos beneficios:

- No hay necesidad de cableado telefónico, los teléfonos utilizan la red de computadores.
- Es más fácil de instalar y manejar, a través de la interfaz de configuración basada en web.

- Los empleados pueden moverse de oficinas sin necesidad de cambios en el cableado o configuración de la IP PBX.
- Escoge entre los diferentes teléfonos SIP basados en hardware en vez de quedar atado con un solo proveedor.
- Ahorra en los costos de las llamadas utilizando cualquier servicio VOIP SIP o WAN.

La versión del software es la 5.0, el último release oficial, todos los paquetes adicionales que pueda usar ya sea sonidos o drivers son la misma versión. Los protocolos que se utiliza para tener comunicaciones es SIP (Session Initiation Protocolo) y H.323V4, el cliente es 3CX Client, en su versión para Windows y Linux.

Tradicionalmente, los productos telefónicos son diseñados para ejecutar una tarea específica en una red. Sin embargo, gran cantidad de aplicaciones de telefonía comparten gran cantidad de tecnología.

El Sistema Telefónico de 3CX es mucho más barato que la Centralita tradicional y puede reducir sustancialmente el costo de las llamadas mediante el uso de un proveedor de servicios VOIP. Su administración basada en la Web hace que el manejo del sistema telefónico sea fácil.

La Planta Telefónica VOIP de 3CX elimina la red de cableado telefónico y permite que los usuarios se comuniquen con el centro de información simplemente levantado su teléfono. Aquí sus principales características:

- Un completo sistema telefónico: Brinda conmutación, enrutamiento y cola de llamadas.
- El costo de compra es infinitamente inferior al precio de una Centralita tradicional basada en hardware.
- Ampliables extensiones y líneas telefónicas ilimitadas. No se necesitan módulos propietarios de expansión.
- Configuración basada en la Web e indicación de estado. Un sistema telefónico de fácil manejo.
- Contestador automático (p. ej. 1 para ventas, 2 para soporte, etc.).
- Reduce el costo de las llamadas de larga distancia y entre oficinas.
- No más sistemas telefónicos propietarios caros: Utiliza los teléfonos SIP estándares.
- Elimina el cableado telefónico y hace que el traslado entre oficinas sea más fácil.

Para poder hacer todo esto, 3CX funciona mediante canales. Estos canales son drives para distintos tipos de conexiones para protocolos de VoIP como SIP y H.323., teléfonos y Softphones se conectan a un canal, algunos de ellos se registran (en el proyecto todos se registran) para dar a conocer que están en línea.

En el proyecto se va utilizar como protocolo el SIP junto con el H.323V4. Es un protocolo basado en texto que usa la codificación UTF-8 y en el puerto 5060 para conexiones TCP y UDP, y ofrece todas las gamas de posibilidades de la telefonía moderna. Dado que es un protocolo muy flexible es posible agregar funciones y aumentar la operabilidad.

Entender la configuración de 3CX es muy fácil, ya que nos permite configurarla paso a paso, para que la central sepa que hacer. Ahora en el siguiente paso vamos a dar a conocer los archivos de configuración y cuáles fueron los que utilizamos para la PBX.

Esto hace que sea el entorno ideal para empresas de todo tipo, que quieran una solución óptima para las telecomunicaciones, ya que puede trabajar desde un simple servidor de Voz sobre IP hasta una compleja PBX.

3.7.2 Instalación de 3CX

Requerimientos del Sistema

La central telefónica 3CX para Windows requiere lo siguiente:

- Windows XP, Vista, 2000 (server & professional) o 2003 server

- Puertos 5060 (SIP), 5481 (Apache) deben estar libres y abiertos y 5480 (Postgres), 5482 (Servidor de Medios) deben estar libres.
- Teléfonos SIP basados en hardware o software
- Opcional una pasarela VOIP (si se necesita conectar líneas telefónicas PSTN)
- Opcional cuenta de proveedor de servicio VOIP (si se quiere hacer llamadas a través de Internet).

3CX es un software desarrollado por la empresa Microsoft Gold Certified Partner y posee 4 versiones Free Edition, Enterprise Edition, Pro Edition y Small Business Edition.

Se ejecuta el archivo de instalación haciendo doble clic sobre el archivo 3CXPHONE SYSTEM5.EXE. Luego haga clic en 'Next' para iniciar la instalación.

Se le preguntará que revise y luego apruebe el acuerdo de licencia, así como también el escoger una ruta para la instalación.

Central telefónica 3CX necesitará aproximadamente un mínimo de 50 Mb de espacio libre en disco duro. Se necesitará reservar espacio adicional para almacenar correos de archivo de voz y archivos de avisos de sistema.

La instalación preguntará cuantos dígitos se desea para los números de extensión.

Preguntará por el nombre de usuario y contraseña preferido, el cual será necesario para iniciar sesión en la consola de administración y administrar la central telefónica.

La instalación preguntará por el FQDN de la central telefónica 3CX. Los teléfonos IP contactan el servidor de la central telefónica utilizando una dirección IP o un FQDN.

Si se utiliza un FQDN, entonces se tiene que especificar el FQDN del servidor. Este valor no es relevante si se especifica la dirección IP del servidor en la configuración del teléfono.

Hacemos clic en “Install” para iniciar la instalación de central telefónica 3CX. La instalación ahora copiará los archivos e instalará los servicios Windows necesarios.

Hacemos clic en ‘Finish’ cuando este todo listo.

Una vez la instalación se ha completado, se puede conectar a la consola de administración de central telefónica 3CX al hacer clic en la opción de consola

de administración (management console) del grupo de programas central telefónica 3CX.

Para conectar a la consola de administración desde una máquina remota, abra un navegador web e ingrese el nombre de la máquina en la cual central telefónica 3CX está instalada, seguido por el puerto 5481. (Por ejemplo: http:// central-telefonica:5481).

3.7.3 Activando la central telefónica 3CX

Si se ha comprado una versión Small Business, Pro o Empresarial (Enterprise), entonces se puede activar la licencia dirigiéndose a la página General > Activar Licencia, en la consola de administración 3CX.

Gráfico 3.21: Habilitación del SSID
Fuente: Grupo investigador

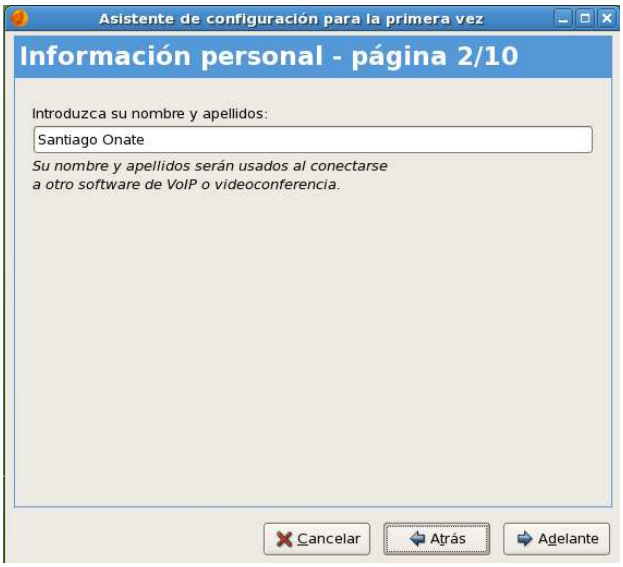
Ingrese su clave de licencia, empresa, nombre de contacto, email, teléfono y país y luego hacemos clic en “Activate”, para activar su licencia. Esta

información será enviada a nuestro servidor de claves de licencia y su clave de licencia e instalación serán activados. Se necesitará hacer esto cada vez que se re-instale central telefónica 3CX o se instale una actualización.

Para la activación de los clientes configurados en el servidor se siguió la siguiente secuencia de pasos:

Grafico 3.22: Configuración de los usuarios en el Servidor

Fuente: Grupo Investigador



En el grafico que se desplego para iniciar la configuración de los usuarios de voz sobre IP o para video conferencia cuando configuramos el servidor de Linux, estos servirán para poder tenerlos en cuenta en las direcciones IP que se encuentran en el servidor de las comunicaciones, es necesario notar que nuestro servidor cuenta con un servidor de DHCP que es el que facilita todas las configuraciones de los servicios para las comunicaciones sean estas de voz o video, con esto hacemos de que la primera dirección IP que para nuestro caso es la 100 sea la extensión a la que se está llamando.

Grafico 3.23: Asignación de contraseñas de los usuarios en el Servidor

Fuente: Grupo Investigador

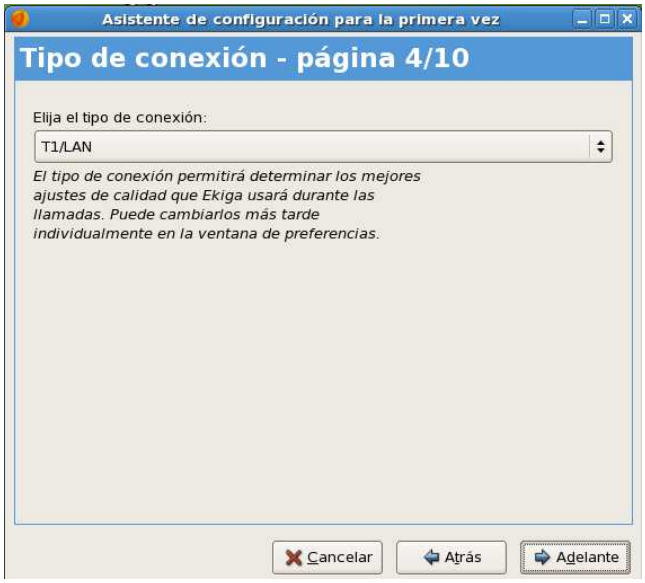
Para las comunicaciones que se realicen hacia el exterior de la red de WLAN se lo debe realizar mediante una autorización que se lo realiza desde el servidor de VoIP el mismo que cuenta como se puede observar en el servicio SIP que es el que permite una adecuada administración de cuentas de usuarios del servidor y por supuesto de los clientes.

Las autorizaciones se las debe realizar al momento de dar el alta a los usuarios de las cuentas en el servidor de ekiga que es el modo grafico de 3cx de Windows pero en el servidor de Linux, esto con el fin de ahorrar costos de licencias.

Los servicios de este servidor están dados para las comunicaciones mediante VoIP y Video conferencias las mismas que vienen previamente configuradas y se suben las direcciones IP del servidor de cuentas dinámicas DHCP.

Grafico 3.24: Configuración de los usuarios en el red LAN

Fuente: Grupo Investigador



Una vez configuradas las cuentas se designa el ambito de accion de los usuarios que por defecto vienen marcadas como redes LAN y que en nuestro caso serian las WLAN.

Grafico 3.25: Resumen de la configuración de los usuarios en el Servidor

Fuente: Grupo Investigador

Una vez configuradas todas las cuentas y loa ámbitos de actuación lo que queda es poner en marcha las comunicaciones como se demostró en la parte

superior del presente capitulo en el cual se realizaba una comunicación entre usuarios dentro de la diócesis de la ciudad de Latacunga.

La comunicaron mediante redes inalámbricas par lo que es VoIP tienen muchas ventajas pero existen muchos retardos en los tiempos de retardo de voz ya que en ocasiones sobre pasa el segundo, lo que es preocupante ya que una comunicación se la debe realizar en tiempo real es decir con intervalos no mayores a 5mseg.

Como investigación justifica pero llegando al campo practico no es suficiente con tener comunicaciones sino se las puede explotar de una manera adecuada por lo que siempre lo que es mediante cableado estructurado en velocidades que sobre pasen los 100Mbps va a ser lo ideal.