TRABAJO ESPECIAL DE GRADO

IMPLEMENTACION DE SOLUCION DE COMUNICACIONES UNIFICADAS PARA EL USO EN PERSONAL DE ANEW E-BUSINESS DISTRIBUTION C.A.

Presentado ante la Ilustre
Universidad Central de
Venezuela para optar al Título
de Ingeniero Electricista
Por el Br. Fernando Ariel, Fouillioux Serrano

Caracas, 2008

TRABAJO ESPECIAL DE GRADO

IMPLEMENTACION DE SOLUCION DE COMUNICACIONES UNIFICADAS PARA EL USO EN PERSONAL DE ANEW E-BUSINESS DISTRIBUTION C.A.

PROFESOR GUIA: María Eugenia, Alvarez
TUTOR INDUSTRIAL: Enrique Muñoz.

Presentado ante la Ilustre
Universidad Central de
Venezuela para optar al Título
de Ingeniero Electricista
Por el Br. Fernando Ariel, Fouillioux Serrano

Caracas, 2008

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

CONSTANCIA DE APROBACIÓN

Caracas, 09 de junio de 2008

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Fernando A. Fouillioux S. Fernández A., titulado:

"IMPLEMENTACIÓN DE SOLUCIÓN DE COMUNICACIÓNES UNIFICADAS PARA EL USO EN PERSONAL DE ANEW E-BUSINESS DISTRIBUTION C.A"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Carolina Regoli
Jurado

Prof. Franklin Martínez
Jurado

Prof. Maria E. Álvarez
Prof. Guía

Edificio Escuela de Ingeniería Eléctrica, piso 1, oficina 201, Ciudad Universitaria, Los Chaguaramos, Caracas 1051, D.F.
TELÉFONOS. (VOZ) +58 212 6053300 (FAX) +58 212 6053105
Mail: eie-com@elecrisc.ing.ucv.ve

DEDICATORIA

A DIOS y a mi familia.

AGRADECIMIENTOS

A mi Madre por ser quién es, por su belleza y dulzura, por sus sacrificios y su apoyo. Por correr conmigo al colegio y mostrarme lo bonito de la vida.

A mi Padre por su ejemplo, su cariño y su amor incondicional. A mi hermano por haber cuidado siempre de mí.

A José Ignacio Verde, que más que un amigo ha sido un hermano a lo largo de estos años.

A mis amigos, esos que compartieron conmigo los peores y mejores momentos de mi carrera como si fueran propios, Ricardo Ortiz, Cesar Ugaz, Servando Eugenio, Natalia Prato, Juan Carlos Mejías, Carmen Díaz.

A la Universidad Central de Venezuela, a la Escuela de Ingeniería Eléctrica y sus profesores, quienes me inculcaron lo necesario para ser un profesional completo, íntegro y digno.

A la Profesora María Eugenia, que me prestó su apoyo y me guió durante la elaboración de este trabajo. A María Auxiliadora, por su paciencia, dedicación y amabilidad.

Al personal de Anew e-B., que me ayudó y contribuyó con la elaboración de este trabajo, especialmente a José Gregorio Raspatella y Hellen Silva.

Fouillioux S., Fernando A.

IMPLEMENTACION DE SOLUCION DE COMUNICACIONES UNIFICADAS PARA EL USO EN PERSONAL DE ANEW E-BUSINESS DISTRIBUTION C.A.

Profesor Guía: María Eugenia Alvarez. Tutor Industrial: Ing. Enrique Muñoz. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Anew e-Business Distribution.

Palabras Claves: Comunicaciones unificadas, PBX (Private Branch Exchange), VoIP (Voice over IP), protocolo G.729, VPN (Virtual Private Network).

Resumen. Se implementa y se diseña un sistema de comunicaciones unificadas basado en la solución OmniTouch Unified Comunications de Alcatel, para satisfacer las necesidades de Anew e-Business Distribution. Se analizó la red de la compañía, y se efectuaron en ella las modificaciones necesarias para albergar la nueva solución de comunicaciones unificadas. Se configuró una VPN para permitir el acceso al sistema a usuarios remotos. Se dimensionó la solución para las necesidades específicas de la empresa. Se configuró la central telefónica para dar lugar a los nuevos servicios. Luego se hizo un estudio de diferentes protocolos de correo electrónico para así encontrar el más apropiado para la empresa. Se instalaron y configuraron los servidores necesarios para la solución. Se elaboraron manuales de acceso a la VPN y de uso del sistema para los usuarios. Se fijó un período de prueba para efectuar modificaciones a la configuración de la solución en base a recomendaciones de los usuarios y se configuraron políticas de enrutamiento según los perfiles de éstos últimos. Se realizó un análisis de las soluciones similares ofrecidas en el mercado para determinar el sistema más efectivo. Por último se hicieron inducciones de instalación y configuración del sistema al personal técnico de Anew e-Business.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

LISTA DE ACRONIMOS

ARS	Automatic Routing Selection
ACD	Automatic Call Distribution
ANI	Automatic Number Identification
ATM	Asynchronous Transfer Mode
CDR	Call Detail Recording
CPU	Control Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNIS	Dialed Number Identification Service
DNS	Domain Name Service
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
KSU	Key Service Unit
KTS	Key Telephone System
LAN	Local Area Network
LCR	Least Cost Routing
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control Address
MCU	Multipoint Control Unit
NAT	Network Address Translation
PBX	Private Branch Exchange
POP3	Post Office Protocol version 3
QoS	Quality of Service
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing

TELNET	TCP/IP Terminal Emulation Protocol
ToS	Type of service
TTS	Text to speech
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VxML	Voice Extensive Markup Language
WAN	Wide Area Network
XML	Extensive Markup Language

INTRODUCCIÓN

Para competir en el mundo de negocios de hoy, las empresas necesitan mejorar el flujo de comunicación interno y externo entre sus empleados, clientes y proveedores. El ambiente de trabajo dentro de una compañía se vuelve cada día más complejo, si bien hay más formas de comunicarse con un miembro de una organización, teléfono de oficina y celular, fax, e-mail, correo de voz, SMS, papel y memos, cuando este está fuera de la oficina, en una reunión, viajando o en trabajo de campo, y aunque posea un dispositivo con conexión a Internet puede dejar de recibir información importante, mensajes, noticias, etc.

En este proyecto se plantea la implementación de una solución de comunicaciones unificadas, usando el sistema Omnitouch Unified Communications (OTUC) desarrollado por Alcatel-Lucent. El concepto de comunicaciones unificadas implica mensajería instantánea, de voz, e-mails, voz, conferencias, accesibles desde cualquier lugar, y cualquier dispositivo. Esta implementación toma lugar en las oficinas de Anew e-Business Distribution, C.A., una compañía de telecomunicaciones cuyos empleados tienen un alto nivel de movilidad y deben contar con estos servicios de comunicaciones en donde se encuentren.

CAPÍTULO I

PROBLEMA

1.1.- Planteamiento del problema

Anew e-Business Distribution, C.A. es una empresa venezolana de capital privado formada por la totalidad del personal gerencial y operativo que hasta Junio 2001 fue responsable de la división Alcatel e-Business Group (Alcatel eBG) de Alcatel de Venezuela. Dicha división, ahora Anew eB C.A., se encarga del diseño e implementación de soluciones de telecomunicaciones empresariales y corporativas en el mercado venezolano. Esta empresa, en proceso de internacionalización cuenta con oficinas en España, Colombia y Panamá, y al ser su sede principal las oficinas de Caracas, los ejecutivos que ahí laboran necesitan movilidad y seguridad en el acceso a su red para poder trabajar en cualquier sitio como si estuviesen en su oficina. Es por ello que para aumentar la productividad, eficiencia y disminuir costos se implementa este sistema.

Anew e-B C.A. es un Premium Business Partner exclusivo de Alcatel, y como tal necesita una plataforma robusta de OTUC desplegada en sus oficinas para poder ofrecerlo a sus clientes, y así, agregarlo a su portafolio de soluciones. Esta instalación también serviría como laboratorio de pruebas donde simular las diferentes configuraciones que podrían aparecer en la instalación de un cliente.

1.2.- Descripción del proyecto

Las centrales telefónicas digitales modernas, ofrecen un sinnúmero de facilidades que las compañías recién empiezan a descubrir; facilidades que le permiten funcionar como Contact Center, ofrecer telefonía IP, buzón de voz, y muchas otras, las cuales mejoran la manera en que sus empleados se comunican y también la manera en que sus clientes perciben la atención que se les ofrece. La central PBX empresarial con que cuenta Anew en sus oficinas ofrece la oportunidad de integrarse con diferentes servidores y así ofrecer una solución de comunicaciones unificadas propietaria de Alcatel llamada OTUC.

El sistema OTUC se desplegará en al menos dos servidores, esto vendrá definido por el número de usuarios con que se cuente, las licencias que se hayan comprado y la capacidad en términos de hardware que la empresa facilite. Estos servidores, conectados a la red de la empresa, tendrán acceso a la central telefónica, el servidor de correo de la compañía y las estaciones de trabajo de los usuarios.

Para poder diseñar esta solución se debe hacer un análisis de la red de la empresa, su capacidad e impacto que una implantación de este tipo acarrea en términos de ancho de banda, características de seguridad y tipos de servidores, entre otros.

Cuando se disponga de toda la información se procederá a la instalación. Se configurarán los servidores, la central telefónica y se harán las modificaciones necesarias a la red para lograr la topología buscada. El próximo paso será el registro y configuración de los usuarios en los equipos, seguido de un período de prueba donde se solventará cualquier imprevisto y se afinarán las herramientas al gusto de cada uno.

1.3.- Objetivos

1.3.1.- Objetivo General

Diseñar e implementar la solución de comunicaciones unificadas para las oficinas en Caracas de la empresa Anew e-Business Distribution C.A. basado en el sistema OTUC.

1.3.2.- Objetivos Específicos

- Dimensionar adecuadamente la plataforma, número de puertos VxML utilizados, servidor de telefonía, de mensajería y asistente personal, servidor para herramientas de colaboración, en base al incremento previsto de usuarios y/o uso de la solución.
- Analizar los niveles de seguridad y acceso en Firewall y VPN de Anew e-B. C.A.
- Diseñar solución para asegurar el 100% de acceso de los usuarios móviles a los servicios de comunicaciones de Anew e-B. C.A.
- Determinar cual protocolo de e-mail: Imap, POP3 ó SMTP se adapta mejor a las necesidades específicas de Anew e-B. C.A.
- Definir política de enrutamiento según los perfiles de usuarios de Anew e-B C.A.
- Elaborar un manual del sistema para el uso interno de los empleados de Anew e-B. C.A.
- Análisis de rentabilidad, estudio técnico económico.

1.4.- Recursos y herramientas

El proyecto se desarrolló en las instalaciones principales de Anew e-B. C.A. (Caracas, Chuao, CCCT), donde se dispone de todos los recursos mencionados a

continuación y apoyo por parte de personal especializado. Los equipos, materiales y software necesario para el desarrollo de este proyecto, así como también los gastos que generó el mismo, fueron cubiertos por Anew.

- Especificaciones técnicas de los distintos equipos.
- Servidores dedicados para el sistema OTUC.
- Acceso total a central telefónica Alcatel OXE.
- Computadora Personal.
- Acceso a Internet.
- Impresora.
- Acceso a biblioteca técnica de Anew.

1.5.- Metodología

El desarrollo de este proyecto se dividió en las siguientes etapas:

Fase 1. Investigación y documentación, en la cual se recopiló información acerca de:

- El sistema OmniTouch Unified Communications, Linux Red Hat Enterprise, My Teamwork, sistema de manejo de licencias FlexLM, configuración y manejo de central telefónica OmniPCX Enterprise.
- Funcionamiento y configuración de equipos de Firewall Fortinet, switches y otros.
- Protocolos de E-mail y soluciones de servidores de correo.
- Otras herramientas necesarias para el desarrollo de la solución.
- Soluciones alternativas y costos y factibilidad de las mismas.

Fase 2. Desarrollo de la solución, donde se generaron los procedimientos y protocolos para la implementación, se hicieron estudios de red, se definieron las herramientas empleadas y se generaron las sugerencias necesarias para el logro de los objetivos planteados.

Fase 3. Implementación, se configuraron e instalaron los equipos necesarios, se dio lugar a las correcciones pertinentes en la red de Anew, todo esto sin interferir en las actividades de sus empleados. Además se supervisó el sistema durante un período de pruebas para comprobar la funcionalidad completa de la implementación y lograr la configuración optima.

Fase 4. Elaboración del Tomo

CAPÍTULO II

MARCO REFERENCIAL TEORICO

Para la mejor comprensión del tema tratado en este trabajo, se presentan a continuación una serie de conceptos de interés:

2.1.- Sistemas de conmutación corporativo [1]

En la actualidad los sistemas de conmutación que forman parte de una red corporativa pueden pertenecer a la propia entidad que hace uso de ellos o ser parte de una red pública que los cede para uso exclusivo de la misma. En ambos casos, las facilidades y servicios ofrecidos pueden ser similares, dependiendo de la implementación que se haga de esta. Serán las razones estratégicas y de negocios las que hagan decidirse por una u otra solución, siempre teniendo en consideración la oferta que hagan los operadores, el plan de tarifas ofrecidas y las condiciones del mercado.

Básicamente, los elementos principales de una red corporativa de voz son los sistemas de conmutación, a los que hay que añadir los elementos de transmisión, de supervisión y los propios equipos de usuario.

Como elementos de conmutación existen varios tipos de dispositivos que pueden efectuar esta función:

- Sistema multilínea o KTS
- Centrales o PBX
- Centrex

2.1.1.- Sistemas KTS (Key Telephone System) [1]

Los sistemas KTS son soluciones de voz corporativas destinadas a empresas pequeñas que necesitan más de una línea telefónica pero no generan el suficiente tráfico como para emplear una PBX. El principio en el que se basan este tipo de sistemas es que todos los teléfonos tienen acceso directo a cualquier línea y viceversa.

Están constituidos por una unidad de control denominada KSU (Key Service Unit) y un conjunto de terminales propietarios. La KSU contiene todos los elementos de conexión del sistema, la alimentación, las interfaces de líneas y troncales y se conecta entre las líneas externas y los terminales, de modo que todas las líneas y todos los terminales están unidos a la KSU.

Los terminales disponen de una serie de botones o teclas, cada uno de los cuales representan una de las líneas y pulsando un botón se obtiene el tono de invitación a marcar en la línea correspondiente. Es decir, el acceso a las líneas se lleva a cabo por selección directa

2.1.2.- Sistemas PBX (Private Branch Exchange) [1]

A medida que el tamaño de la empresa aumenta, encontramos que una única línea telefónica o sistema KTS no cubren las necesidades de la misma. Una mejor aproximación supondría mover una parte del conmutador central del operador a las oficinas de la empresa cliente. En este sentido una PBX ofrece mayor rendimiento tanto para el operador como la empresa usuaria. Así pues se trata de conmutación privada; de ahí muchas veces que se haga referencia a ellas como centrales.

Básicamente una PBX no es más que un dispositivo al que se conectan una serie de teléfonos fijos o inalámbricos (o dispositivos similares, tales como faxes, módems, tarjetas de voz, etc., capaces de recibir y realizar llamadas), que permite establecer una comunicación entre ellos. Habitualmente, las distintas conexiones internas a la PBX se conocen como extensiones y las externas (hacia la red pública) como líneas troncales o enlaces.

2.1.2.1.- Componentes de una PBX [1]

Las PBX modernas son ordenadores especializados que incluyen una matriz de conmutación cuya misión es conectar las llamadas de voz, aunque también son capaces de conmutar un conjunto limitado de datos. Dan servicios a un gran tipo de terminales de todo tipo, tanto cableados como inalámbricos.

Los componentes principales de una PBX se presentan en la figura 1:

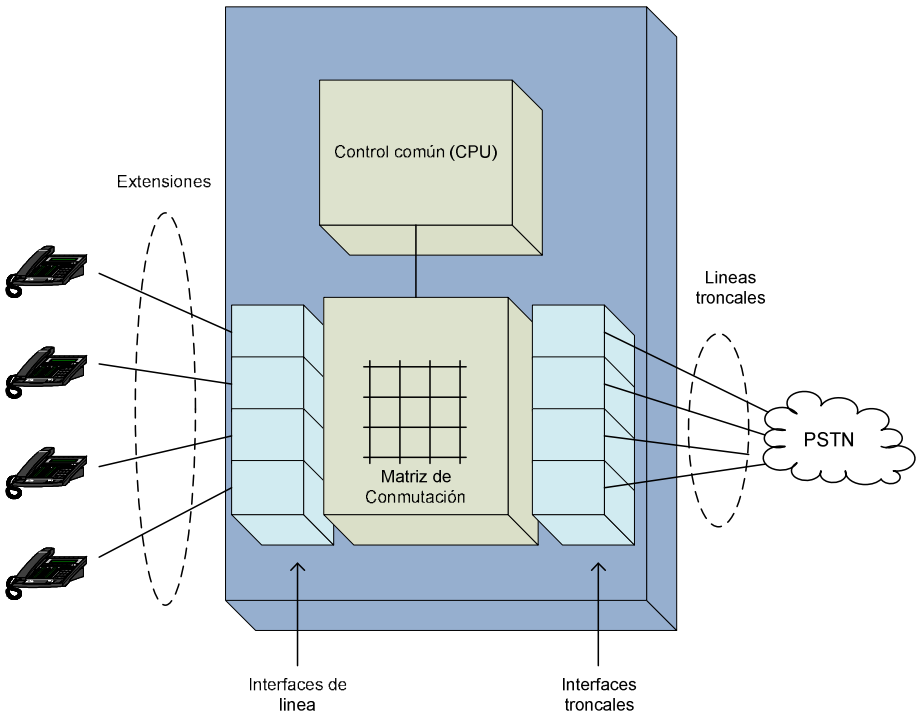


Figura 1 Componentes de una PBX

Control Común: consiste en un conjunto de programas lógicos almacenados que gobiernan el funcionamiento de todos y cada uno de los elementos del sistema.

El CPU (Central Processing Unit) controla el funcionamiento del conjunto:

- Establecimiento de llamadas
- Mantenimiento de llamadas
- Liberación de llamadas
- Monitorización de las prestaciones
- Realización de diagnósticos de estado del sistema
- Almacenamiento de datos para la realización de análisis e informes.

Es bastante común encontrarse con centrales que contengan redundancia de procesadores, puesto que estos sistemas son altamente escalables y fáciles de mejorar, y todas las funcionalidades que ofrece la central son programables.

Matriz de conmutación: Las PBX actuales emplean la multiplexación por división en tiempo, tanto en sistemas analógicos como digitales. En TDM (Time Division Multiplexing) las conversaciones muestreadas viajan secuencialmente a través de un único medio físico.

Interfaces troncales: se trata de tarjetas especiales que sirven de interfaz entre el conmutador de la PBX y las líneas troncales que conectan a la PBX con otros conmutadores. Estas troncales pueden ser unidireccionales salientes, unidireccionales entrantes o bidireccionales. Una PBX suele emplear las tres variantes para dar servicio a aplicaciones específicas, maximizar las prestaciones del sistema y asegurar un nivel mínimo de acceso entrante y saliente aceptable.

Las troncales pueden ser monocanal o multicanal, siendo estas últimas, capaces de soportar múltiples conversaciones simultáneamente. Las líneas troncales con las mismas características de direccionalidad se pueden agrupar. La PBX puede elegir entre las diferentes troncales del mismo grupo, basándose en secuencias de salto predefinidas por el usuario.

Interfaces de línea: Las interfaces de línea son placas de circuito impreso que pueden soportar varias estaciones del mismo tipo a través de múltiples puertos en una misma tarjeta. Existen dos modos de conexión:

Analógico: en el que la voz se transmite gracias a la variación de la corriente eléctrica. En este caso, la conexión se consigue a través de un set de cables a los cuales la PBX proporciona un cierto voltaje, formándose entre esta y el teléfono un circuito eléctrico. Mientras el teléfono este colgado el circuito no se cerrará. Es al descolgar el teléfono cuando se completa el circuito, permitiendo que fluya la corriente a través de él. Son precisamente las variaciones de esta corriente lo que permite la transmisión del sonido.

Digital: en la que la voz se representa mediante tramas de bits.

Equipo terminal: puesto que las PBX están diseñadas fundamentalmente para el tráfico de voz, por lo general, el terminal del usuario es un teléfono, aunque es posible encontrar un terminal de datos

2.1.2.2.- Configuración del sistema y capacidad [1]

La capacidad de la PBX debe analizarse con sumo detalle con el fin de asegurar que se adapte a las necesidades futuras y actuales de la empresa. En este sentido, es importante tener en cuenta los siguientes puntos:

Configuración centralizada o distribuida: las PBX se suelen configurar como un sistema centralizado, lo que facilita las labores de administración. Sin embargo en algunos entornos es necesario interconectar varias PBX entre si, por ejemplo, para formar una VPN (Virtual Private Network), dando lugar a una PBX distribuida de mayor capacidad.

Capacidad física: es una medida del número de líneas que se soportan.

Capacidad de conmutación: es una medida del número de conversaciones simultáneas que la PBX es capaz de cursar. Esta medida es crítica, sobre todo en aquellas PBX que pueden trabajar con voz y datos.

En este sentido se pueden distinguir dos tipos de centrales:

Con bloqueo: típicas de aplicaciones solo de voz, están diseñadas para soportar un nivel razonable de tráfico, siendo el resto de llamadas rechazadas durante los períodos de alta actividad. Puesto que las características del tráfico de voz son deterministas y la voz no consume mucho ancho de banda, es posible optimizar la capacidad del sistema para proporcionar altos niveles de disponibilidad, incluso durante los picos en las horas mas cargadas, a un coste razonable.

Sin Bloqueo: aseguran que la comunicación entre los terminales se establecerá. Existe una relación 1:1 entre las líneas y los intervalos de canal. Son bastante costosas, por lo que su aplicación queda circunscrita a aplicaciones muy específicas de voz y datos.

2.1.2.3.- Funcionalidades de las PBX [1]

Las PBX proporcionan un acceso compartido a la red telefónica así como una serie de funcionalidades entre las que destacan:

-Encaminamiento de menor coste LCR (Least Cost Routing): también se conoce por el nombre de selección automática de destino ARS (Automatic Routing Selection): permite al usuario elegir al proveedor más adecuado para que cada llamada alcance su destino en función de una serie de factores, entre los que se encuentran: naturaleza de la llamada, tipo de servicio, hora del día, día del año (festivo o laborable), etc.

-Grupos de captura: un usuario de un grupo puede contestar las llamadas de cualquiera de los usuarios de su grupo.

-Desvío de llamadas: el usuario puede predefinir (aunque también es posible hacerlo dinámicamente) una extensión a la que la llamada será transferida si el está ocupado o no contesta.

-Conferencia: se trata de conectar más de dos líneas entre si, de modo que el audio presente en una de ella se escuche en todas.

-Registro de información de las llamadas CDR (Call Detail Recording): proporciona información sobre todas las llamadas entrantes o salientes. Esta información puede ser empleada por el administrador del sistema para realizar informes sobre el uso de la red, e incluye, por lo general, el origen y el destino de la llamada, la troncal o grupo de troncales entrante y saliente, el tiempo de conexión, el código de acceso de marcado, el número de teléfono marcado y el código de autorización empleado.

Muchas de las PBX actuales incluyen software que permite la generación de una serie de informes que recogen, entre otros aspectos, los costes de uso por estación, códigos de cuenta de usuario, departamento o grupo de trabajo, etc. Sin

embargo, existe la posibilidad de que este software de gestión se ejecute en un ordenador dedicado que se conecta a la PBX por un puerto específico de la misma.

-Distribución automática de llamadas ACD (Automatic Call Distribution): Un software encamina las llamadas entrantes al agente más apropiado que se encuentre disponible en cada momento.

-Identificación del llamante CallerID: permite la identificación de la persona que realiza la llamada. Esta información se suele enviar al principio de la llamada generalmente entre el primer y el segundo tono. Si bien este servicio también es prestado por las centrales de conmutación de los operadores de telefonía, el objeto en el entorno de las PBX es diferente. El CallerID que proporciona la central del operador suele denominarse ANI (Automatic Number Identification) e identifica al abonado llamante mientras q la que se obtiene de una PBX es la identidad de la persona que tiene asignada la extensión desde la que se efectúa la llamada en cuestión.

-Identificación del número marcado DNIS (Dialed Number Identification Service): es el número marcado por el llamante para acceder el destino, lo que le permite a la PBX encaminar la llamada entrante a la extensión o grupo de extensiones apropiado en función del número llamado (generalmente, de sus cuatro últimos dígitos).

-Indicación de mensaje en espera: muchas PBX incluyen la capacidad de indicar al usuario que le acaban de dejar un mensaje en su buzón mediante el encendido de una luz en su terminal; una vez escuchado dicho mensaje el indicador se apaga.

-Supervisión de desconexión positiva: una de las principales funciones de la PBX es detectar cuando un llamante externo cuelga su teléfono. Esta capacidad

permite a la central colgar y completar la desconexión, de modo que la línea queda disponible para otras llamadas y la tasación termina.

-Transferencia directa: permite transferir llamadas directamente de un número a otro. La principal ventaja de la transferencia directa es la liberación de recursos, que quedan disponibles para nuevas llamadas.

2.1.3.- Centrex (Central Office Exchange Service) [1]

Las Centrex han sido desarrolladas como una alternativa a la utilización de una PBX en las ocasiones en las que no resulta rentable debido a que supone una inversión inicial muy alta con un período de amortización demasiado largo. Este es el caso de una organización que requiere de un número de extensiones o líneas reducido. El servicio Centrex consiste en el empleo de las extensiones de la central de un operador como si fueran una central propia. Tanto es así que desde un punto de vista físico las líneas de un grupo centrex no se diferencian en nada del resto de las líneas de abonados regulares de las centrales a las que pertenecen.

2.2.- OmniPCX Enterprise [2]

La OmniPCX Enterprise (versión de Linux) es un switch telefónico privado que se basa en una infraestructura de red de datos IP.

Los componentes principales de la OmniPCX Enterprise son:

- El Call Server, que es el centro de control del sistema
- Media Gateways, que dan soporte a equipos telefónicos estándares:
  - Cableado digital (Serie Reflexes y Alcatel 9) o sets análogos.
  - Líneas al público regular o a redes telefónicas privadas.
  - Estaciones telefónicas móviles.
  - Guías de Voz

- Compresores para garantizar el vínculo entre teléfonos estándares e IPs

- Terminales IP (Teléfonos IP: Reflexes y Alcatel Serie 8 - IP Touch -, PCs multimedia o terminales H.323)
- Sets móviles IP Touch: estos sets están vinculados a la OmniPCX Enterprise a través de una LAN inalámbrica.
- Aplicaciones externas tales como el correo de voz y la consola de administración OmniVista 4760.

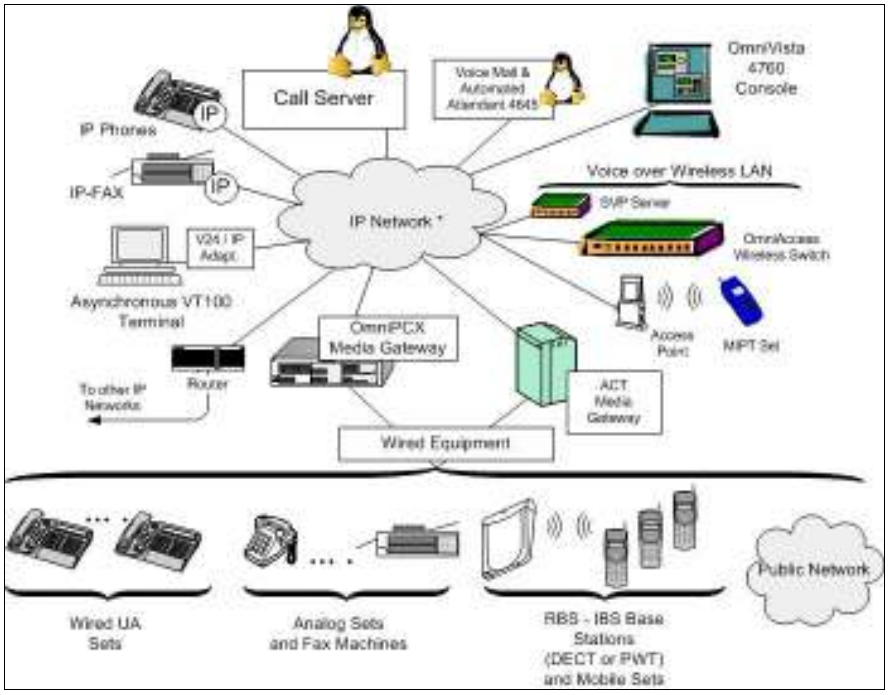


Figura 2 Configuración IP Típica OXE [2]

- Una OmniPCX Enterprise puede conectarse a las siguientes redes públicas:
  - Digital: ISDN T0/T1/T2
  - Digital: T1 CAS
  - Analógica: NDDI
  - Analógica: Loop start
  - Analog: Ground start.

2.3.1.- Principios de operación OmniPCX Enterprise

El Servidor de llamadas (Call Server) es un programa de software que corre bajo el sistema operativo Linux. Centraliza la configuración de cada elemento del sistema. También almacena el estatus actual de cada elemento en su memoria (teléfono, troncal, grupo troncal, etc.), por ejemplo, línea desocupada, repicando o en una conversación. Cuando un evento ocurre, por ejemplo, se levanta el auricular, este evento se notifica al servidor de llamadas (Call Server) a través del Media Gateway; el Call Server, de acuerdo a un set de configuraciones y estatutos, lleva a cabo las operaciones pertinentes para este evento. En el caso de que se levante el auricular de un set desocupado, puede enviar el tono de marcado. La orden se transmite al Media Gateway a través de la red IP. El Media Gateway interpreta la orden del Call Server y conecta el tono requerido al teléfono designado.

Protocolos Usados

- Tránsito de llamadas de voz sobre segmentos IP usa uno de los siguientes protocolos: G711, G723 o G729
- Tránsito de llamadas de datos sobre segmentos IP encapsulado en datagramas IP
- Las llamadas de FAX transitan los segmentos IP ya sea usando un protocolo propietario para equipos Alcatel o usando protocolo T38 (para equipos de otros fabricantes)

Aplicaciones Externas

Una aplicación externa es una aplicación que trabaja junto con el Call Server. No todas las aplicaciones externas están disponibles en todas las configuraciones.

Correo de Voz

Los sistemas de correo de voz de Alcatel, llamados 4635 y 4645 están disponibles para la OXE. Estos sistemas de correo de voz también ofrecen las características de contestadora automática y disponibilidad permanente. El sistema de correo de voz 4645 de Alcatel puede ser instalado en el mismo procesador que el servidor de llamadas o correr en una máquina dedicada. El sistema de correo de voz 4635 ofrece más características que el 4645 pero opera solo en ciertas tarjetas. Pueden ser usados correos de voz de otros fabricantes. Para estos casos la conexión con la OXE es a través de líneas analógicas y usando el protocolo VPS.

Herramientas de Administración de la OXE

La OXE puede ser administrada usando:

- Una herramienta genérica tal como **mgr**, basada en pantallas de caracteres que permiten que se ejecute una administración básica del sistema.
- La aplicación OmniVista 4760, ejecutándose en un PC dedicado, esta aplicación es particularmente útil cuando una red PCX debe ser administrada

Con ambos métodos, el acceso a la administración puede ser protegido contra intrusiones maliciosas. Varios mecanismos (tales como protocolos SSH y HTTPS) se usan para asegurar la protección

OmniTouch Unified Communication

OmniTouch Unified Communication es una aplicación de comunicaciones unificadas que agrupa, en su versión completa módulos de mensajería, asistente personal, telefonía y mensajería instantánea y colaboración.

2.3.- Comunicaciones Unificadas

Las comunicaciones unificadas hacen referencia a sistemas de comunicaciones y colaboración con funciones de presencia, telefonía y e-mail integrados, a través de una interfaz única para el usuario y disponible desde cualquier dispositivo, en cualquier lugar, en cualquier momento.

Las tecnologías envueltas en las comunicaciones unificadas implican la integración de sistemas de comunicación, sistemas de medios, dispositivos y aplicaciones. Esto se traduce, en integración de telefonía móvil y fija, e-mail, mensajería instantánea, aplicaciones de escritorio y también avanzadas aplicaciones de negocios, PBX, VoIP, presencia, correo de voz, fax, video y conferencias webs, mensajería unificada, correo de voz unificada y pizarras compartidas en un solo ambiente, ofreciendo al usuario una experiencia más simple y más efectiva. Todo esto con el propósito de optimizar las estructuras de negocios y mejorar las comunicaciones humanas al reducir el retardo y flujos administrativos, y eliminando la dependencia a medios o dispositivos.

2.4.- OmniTouch Unified Communication [3]

OmniTouch Unified Communication es un conjunto de aplicaciones de software que proporcionan mensajería unificada, conferencia de audio, datos y vídeo, enrutamiento personal, mensajería instantánea (IM), capacidades sofisticadas de Softphone, acceso al directorio universal e información de presencia. Esta herramienta integra todas o algunas de estas funciones en el entorno empresarial existente y permite acceder a ellas cuando se está fuera de la oficina con múltiples dispositivos.

Alcatel OmniTouch Unified Communication se compone por cuatro módulos:

- My Messaging

My Messaging proporciona la gestión de mensajes. La mensajería unificada ofrece un único buzón para todos los tipos de mensajes: e-mail, voz y fax, a través del programa de e-mail preferido del usuario, Microsoft Outlook o Lotus Notes de IBM. Permite también acceder a los mensajes con una interface Web o un teléfono de cualquier tipo (e-mails mediante la tecnología text to speech). Esto hace más fácil estar conectado mientras se está fuera de la oficina. My Messaging se integra con servidores de e-mail y buzón de voz (mensajería integrada con Alcatel 4635/4645).

- My Phone

My Phone gestiona las comunicaciones en tiempo real ya sea en la oficina o fuera de ella. My Phone ofrece un programa Softphone Web y un programa Softphone IP llamado 4980 Softphone Windows. Este último se integra con Microsoft Exchange/Outlook, Lotus Domino/Notes de IBM y directorios corporativos (LDAP). My Phone permite asociar cualquier teléfono (móvil, residencial, etc.) para audio o utilizar su PC multimedia con voz sobre IP (VoIP).

- My Assistant

My Assistant ofrece enrutamiento personal de las llamadas entrantes basado en reglas establecidas por el usuario. Tales capacidades de enrutamiento dan lugar a prestaciones “sígueme” y filtrado de llamadas según la identificación del que llama (ANI), hora del día y lugar. Las reglas de enrutamiento personal se pueden configurar desde la red interna o fuera de ella a través de una interface Web o mediante llamada por tonos desde cualquier terminal telefónico.

- My Teamwork

My Teamwork ofrece herramientas de colaboración para compartir conocimiento a través de voz, datos y vídeo conferencia. Mediante una interface web de usuario, los usuarios pueden iniciar conferencias, en directo o planificadas regularmente, de audio, datos, vídeo y para compartir aplicaciones. My Teamwork proporciona información de presencia y mensajería instantánea.

También se cuenta con un módulo web llamado Homepage Web, en el cual cada usuario cuenta con un panel de control para personalizar la configuración y acceso a los 4 módulos principales.

Servicios comunes

La integración de los cuatro módulos ofrece los siguientes servicios comunes:

- Acceso a Directorio Universal (LDAP, Directorio Activo, Contactos personales, directorio de OmniPCX, etc.).
- Integración con contactos (acceso a contactos de Microsoft Outlook y de Lotus Notes de IBM).
- Notificación de eventos (SMS, e-mail, voz).
- Presencia (telefonía, mensajería instantánea).
- Servicios Web (interfaces XML/SOAP que permiten la integración con otras aplicaciones empresariales).
- Acceso vocal VxML (las aplicaciones son accesibles por voz utilizando la interface VxML).
- Seguridad (autenticación y conectores para servidores de autenticación).

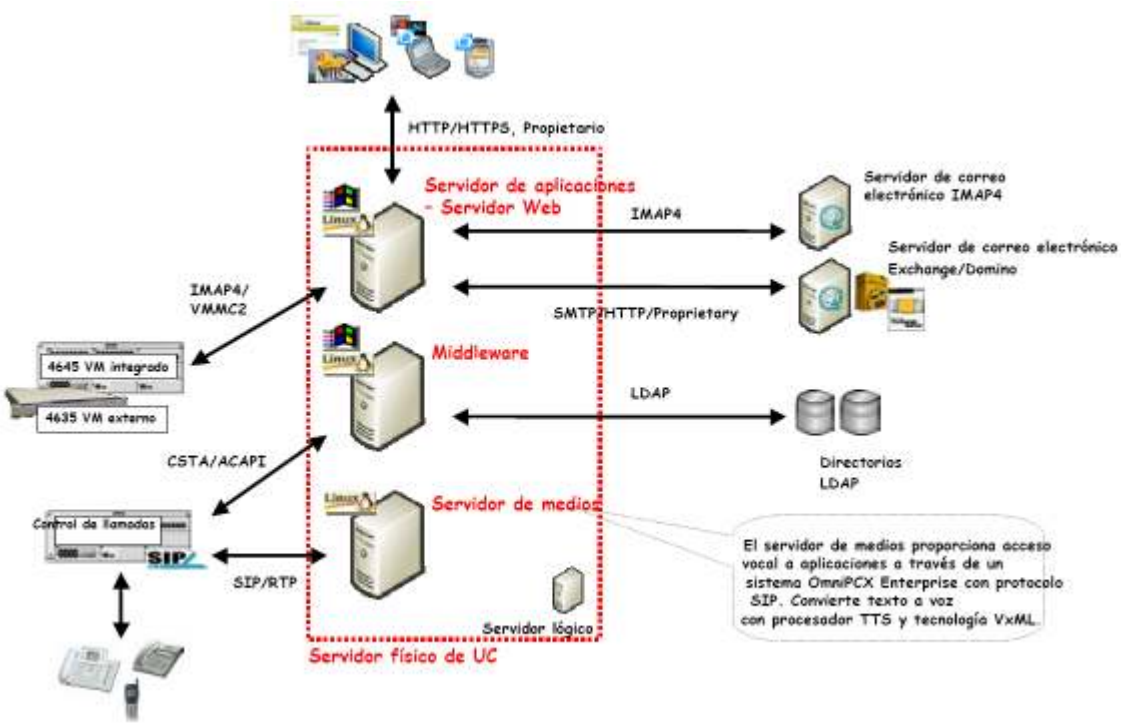


Figura 3 Servidores y protocolos de Otuc [4]

2.5.- Protocolos de correo electrónico.

SMTP (Simple Mail transfer protocol), POP3 (Post Office Protocol 3) e IMAP (Internet Message Access Protocol) son protocolos usados para la entrega de correos. Cada uno define un set de reglas específico para la comunicación entre clientes y servidores de correo, ofreciendo diferentes cualidades y características que les permiten adaptarse de a diferentes tipos de usuario.

SMTP

SMTP es un protocolo estándar de Internet de transporte de correo de host to host que tradicionalmente opera sobre TCP en el puerto 25. SMTP, esta definido por la IETF RFC 2821 y establece un formato de mensaje y un agente de transferencia de

mensajes, que almacena y reenvía el correo. SMTP usa un estilo de protocolo petición-respuesta asimétrica. Si la entrega de correos falla, el sistema pondrá en cola el mensaje e intentará reenviarlo luego. Sin embargo no existe ningún mecanismo de solicitar correos a los hosts, ni facilidades de buzones de correo o cualquier otra característica especial más allá de transporte de correo. Es por esto que se acostumbra tener un esquema en el cual las solicitudes de e-mail a los servidores se hagan bien a través del protocolo POP3 o IMAP4.

POP3

Post Office Protocol versión 3: Este es un protocolo estándar para recepción de e-mails. El protocolo POP3 controla la conexión entre un cliente de e-mail POP3 y el servidor donde se almacenan los e-mails. Esta diseñado pensando en dos parámetros, autenticación del usuario y manipulación de e-mails. El protocolo POP3 tiene 3 diferentes estados para manejar la conexión entre el servidor de correos y el cliente POP3, el estado de autenticación, el estado de transacción y el de actualización.

Durante el estado de autenticación, el cliente de correo POP3 que está conectado al servidor se debe autenticar antes de que el usuario recupere sus e-mails. Si el nombre de usuario y la contraseña que provee el cliente coinciden con las del servidor, se considera autenticado al usuario y comienza el estado de transacción. Si no coinciden, el usuario recibe un mensaje de error y no se le permite conectarse a recuperar los e-mails.

Para evitar pérdida de datos en el buzón de correos, luego de que el usuario ha sido autenticado, y el buzón ha sido bloqueado, no es posible descargar sino hasta que la conexión ha terminado. Además, solo un cliente se puede conectar a un buzón de correo a la vez, peticiones adicionales de conexión al correo son rechazadas.

Durante el estado de transacción, el cliente envía comandos POP3 al servidor, y este los recibe y responde de acuerdo al protocolo. Cualquier comando que no pertenezca al protocolo POP3 es ignorado, y un mensaje de error es enviado.

El estado de actualización cierra la conexión entre el cliente y el servidor. Es el último mensaje que el cliente transmite.

IMAP

IMAP es un protocolo para recuperar correos electrónicos almacenados en un servidor. En otras palabras le permite a un programa de cliente de correo (Outlook, Mozilla Thunderbird) acceder a mensajes remotos como si se tratasen de recursos locales. Por ejemplo, un correo almacenado en un servidor IMAP puede ser manipulado desde una computadora personal en casa, una estación de trabajo en la oficina o un notebook cuando se esta de viaje, sin la necesidad de transferir mensajes o archivos entre estos

La habilidad de acceder mensajes tanto nuevos como ya leídos desde más de una computadora se ha vuelto extremamente importante a medida que la confianza en los medios de mensajería electrónicos y el uso de múltiples computadores se incrementa; ahora bien, esta funcionalidad no siempre es una ventaja, el protocolo POP funciona mejor cuando se trabaja con una sola computadora, ya que fue diseñado para dar soporte al acceso de mensajes cuando no hay conexión, y en este esquema los mensajes descargados son eliminados del servidor. Este método de acceso no es compatible desde múltiples computadores, ya que los mensajes quedarían diseminados en estas. Así, a menos que todas máquinas compartan un sistema de archivos común, el modo de conexión para el cual fue creado IMAP liga un usuario a un sólo computador para manipulación y almacenamiento.

Las características resaltantes de IMAP son:

- Es totalmente compatible con estándares de mensajería de Internet, MIME.
- Permite el acceso y manejo de mensajes desde más de una computadora.
- Permite el acceso sin tener que apoyarse de protocolos menos eficientes.
- Da soporte a modos de acceso, con conexión, sin conexión
- El software del cliente no necesita saber el tipo de almacenamiento de archivos usado por el servidor.
- El protocolo incluye operaciones para crear, borrar y renombrar buzones de correo, revisar por nuevos mensajes, remover mensajes de manera permanente, establecer y quitar banderas, y búsqueda inteligente de mensajes por atributos, texto, o porciones de este último.

IMAP fue desarrollado originalmente en 1986 en la Universidad de Stanford. Sin embargo no captura la atención de los proveedores de servicios de mensajería electrónica sino hasta una década después, y aún así no es tan conocido como el protocolo POP, hecho que esta cambiando rápidamente gracias a más implementaciones de software que en sus últimas versiones lo recomiendan.

2.6.- Calidad de Servicio (QoS) [1]

La calidad de servicio hace referencia a la capacidad de la red para proporcionar ciertas preferencias a cada tipo de tráfico, asegurando cierto ancho de banda a cada servicio dependiendo de la aplicación. Este aspecto adquiere una importancia fundamental cuando se considera integrar de voz y datos en una misma infraestructura.

En una red de datos, la pérdida de paquetes es un fenómeno común. A diferencia de las redes en las que se establece un circuito físico entre los extremos de la comunicación, en las redes de datos los paquetes son enviados a medida que se generan sin conexión previa entre ambos extremos. En la secuencia de transmisión de

un paquete que procede de una o varias fuentes hacia el enlace del router, los mismos son puestos en cola hasta que pueden ser retransmitidos en el mismo orden que originalmente salieron. Así, las pérdidas ocurren cuando las colas se llenan y los routers son incapaces de aceptar más paquetes. Una solución sería cambiar el router por uno de mayor capacidad ó sustituir el enlace por uno de mayor ancho de banda, sin embargo muchas veces esta no es una solución viable, por lo que se apunta hacia la implementación de QoS.

2.6.1.- IEEE 802.1p [1]

- Es un protocolo encargado de definir como los switch deben discriminar la prioridad de las tramas que los atraviesan. Se trata de un proceso de capa 2 y por lo tanto es independiente del protocolo de la capa de red. El proceso se puede definir en tres estados:
    - Recepción de la trama: cuando un paquete recibe una trama por un determinado puerto, se asigna una prioridad de usuario.
    - Si a nivel de MAC (Media Access Control), es soportado el nivel de prioridad, como es el caso de Token Ring, la prioridad se extrae directamente de la trama capa 2.
    - En redes Ethernet, el switch generará la prioridad basándose en su propia configuración que, por lo general, consiste en un valor de prioridad por defecto que a su vez, es función del puerto por el que la trama ha sido recibida.
- Evaluación: en este proceso se decide si se descarta la trama o por el contrario se reenvía a uno o más puertos del switch. En el caso más común, un determinado puerto dispone de más de una cola de transmisión, en donde a cada una de ellas se le asigna un valor de prioridad comprendido entre 0 y n-1, donde n es el número de colas asociado al puerto de salida. De esta forma se logra que la prioridad del usuario obtenida en el proceso se mapea a un valor de trafico determinado previamente.

- Transmisión: el estándar define un algoritmo por defecto en el que las tramas solamente son seleccionadas para transmisión si todas las colas correspondientes a los valores de prioridad mas altos están vacías en el momento de la selección. Una vez que la trama a sido seleccionada, la importancia de usuario se mapea en la prioridad de acceso del puerto saliente.

2.6.2.-IEEE 802.1Q [1]

El estándar 802.1Q define una arquitectura de switches LAN virtuales en la que todos los tipos de tráfico tienen la capacidad de manejar señalización de la prioridad de usuario extremo a extremo independientemente de la información de usuario incluida en los protocolos MAC y de proporcionar servicios VLAN (Virtual Local Area Network). Esta etiqueta constituye una cabecera original que se inserta en la trama inmediatamente después de los campos de dirección origen y destino. Entonces, en función de etiquetado las tramas se pueden clasificar en tramas sin etiquetar, tramas etiquetadas y por último las que tienen prioridad.

Una vez dicho esto se pueden especificar las reglas en las que se basa 802.1q. Si la trama recibida incluye prioridad, se maneja este valor para el manejo de las colas y se le da una mayor importancia. Por el contrario, si estamos en presencia de una trama sin etiquetado no se le presta mayor atención; sin embargo, esta trama también es transmitida en su debido momento.

2.6.3.- IP ToS [1]

En IP versión 4 se establece un campo de 8 bits en la cabecera denominada ToS (Type of Service) y que utiliza para indicar el tipo de servicio. Este campo se divide en dos partes: Procedencia y MBZ (Must Be Zero). Los tres primeros bits de campo de procedencia indican la prioridad del paquete, estableciendo seis clases de servicio distintas. El resto se utiliza para solicitar a la red ciertas características del

servicio (mínimo retardo, máxima prioridad de cola, máxima fiabilidad y mínimo coste) excepto el último que siempre debe ser cero.

2.6.4.- Modelos de QoS [1]

Un modelo de servicio describe un conjunto de características de QoS extremo a extremo, entendido éste como la capacidad de la red para proporcionar el servicio requerido por un determinado tipo de tráfico desde un extremo de la red a otro. En general se distinguen tres modelos de QoS: Best Effort, IntServ y DiffServ.

- Best Effot (Mejor Esfuerzo): es un modelo de servicio único en el que una aplicación envía datos donde es necesario, sin límite de cantidad y sin ser necesario ningún permiso por parte de la red para proceder al envío de la aplicación. Por su parte, la red cursará el tráfico generado por la aplicación siempre que pueda, sin ninguna garantía en cuanto a fiabilidad o retardo. Este modelo resulta adecuado para una gran gama de aplicaciones de red.
- IntServ (Arquitectura de Servicios Integrados) es un modelo multiservicio capaz de acoplar, simultáneamente, diferentes requerimientos de QoS. En este modelo, la aplicación solicita a la red un tipo de servicio específico antes de enviar los datos. Esta petición se lleva a cabo a través de algún mecanismo de señalización que varía según el caso y mediante el cual la aplicación informa a la red de su perfil de tráfico y de sus requerimientos de ancho de banda y retardo. Una vez que la red confirma la petición de la aplicación esta comienza a enviar los datos de acuerdo al perfil que había especificado. En IntServ la red tiene una doble misión: por una parte, efectúa el control de admisión basándose en la información suministrada por la aplicación y en la disponibilidad de los recursos de la red, y por otra, se compromete a garantizar la calidad de servicio que se asegura, siempre y cuando la aplicación mantenga el perfil de tráfico que especificó. Para realizar estas acciones, se utilizan tareas de clasificación de tráfico, encolado inteligente,

adaptación del tráfico, entre otros. En general, se definen dos tipos de servicios:

- Garantizado: el retardo máximo ofrecido por la red es fijo. Apto para aplicaciones que descartan un paquete si este no ha llegado antes del instante de la utilización.
- Predictivo: el retardo máximo es aproximado. Es adecuado para aplicaciones que se adaptan a variaciones en el retardo a costa de la calidad.
- DiffServ (Servicios Diferenciados): Los servicios diferenciados proporcionan mecanismos de QoS para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio. Este servicio se basa en la clasificación de tráfico y asignación de prioridades. Utiliza diferente información de la cabecera de los paquetes para distinguir, clasificar los paquetes y conocer el tratamiento que debe recibir el tráfico en los nodos de la red DiffServ. Utiliza el campo tipo de servicio (TOS) en el datagrama de IPv4 o el campo de prioridad del datagrama IPv6.

2.7.- Señalización SIP (Session Initiation Protocol) [1]

El propósito de la señalización es el intercambio de información entre sistemas de cualquier tipo. La presencia de la señalización en una llamada telefónica implica que dos tipos de tráfico circulan por la red señalización, que controla el uso del canal de voz, y tráfico de voz.

La arquitectura de señalización debe soportar tanto los servicios tradicionales como los nuevos servicios ofrecidos por los puntos finales inteligentes, y conservar la privacidad e integridad del usuario. Por otra parte las expectativas de calidad del usuario exigen una red de señalización de altas prestaciones, su disponibilidad debe ser mayor al 99,9%. Así, la confiabilidad de la red no sólo debe

residir en sus elementos sino también en la arquitectura de señalización empleada. En este sentido, los requerimientos de calidad que se persiguen están enfocados a obtener bajo retardo y pérdida de paquetes.

Una de las arquitecturas de señalización propuesta por el IETF (Internet Enginering Task Force) recibe el nombre del protocolo más importante que emplea, SIP. Se trata de un protocolo de control de nivel de aplicación empleado para establecer, modificar o finalizar sesiones entre dos o más participantes. El protocolo SIP no define el tipo de sesión que se establece, sino que soporta desde sesiones de juegos hasta audio y videoconferencias.

SIP es un protocolo cliente/servidor, similar tanto en la sintaxis como en la semántica al HTTP. Al igual que ocurre en HTTP, en SIP las peticiones son generadas por una entidad (el cliente) y enviadas a otra entidad encargada de recibirlas (el servidor). Este procesa las peticiones y envía una respuesta al cliente. El par petición respuesta recibe el nombre de transacción. El propio protocolo dispone de mecanismos que garantizan la fiabilidad de las transacciones. Además, SIP depende del protocolo SDP (Session Initiation Protocol) para llevar a cabo la negociación del códec empleado.

Los servicios que soporta SIP son:

- Localización de usuarios: determinación del sistema final que participará en la comunicación.
- Establecimiento de llamada: timbre y acuerdo de los parámetros de la llamada entre el origen y el destino.
- Disponibilidad del usuario: determinación del deseo del llamado de participar en la comunicación.
- Características del usuario: determinación de los flujos y las características de los flujos que podrán ser empleados.

- Manejo de llamadas: transferencia y terminación de llamadas.

CAPÍTULO III

METODOLOGÍA

3.1.- Diseño de la Metodología

Para la realización de este proyecto se diseñó una metodología que permitió llevar un orden lógico para obtener resultados óptimos en cuanto al desarrollo de los objetivos planteados. El criterio empleado para este fin se desarrolla en diversas etapas, las cuales se definen a continuación:

3.1.1.- Investigación y documentación

Esta etapa se analizó la documentación necesaria para familiarizarse con las comunicaciones unificadas, sistemas CTI, así como los equipos a utilizar y los protocolos de señalización y datos que entren en juego. Se recopiló información referente a la central telefónica OXE R7, el sistema OTUC incluyendo todos sus módulos, VoIP, las recomendaciones de la UIT para Calidad de Servicio y transmisión en sistemas y redes digitales G.1000-G.1999. Se levantó la información pertinente a la arquitectura de la red de Anew. Para la elección del servidor de correos se hizo un estudio de las características y ventajas de los principales sistemas compatibles con el de comunicaciones unificadas y también se investigó de una solución que permitiese la coexistencia de este con el sistema de correos actual. Para el estudio de la capacidad de la red se estudió la aplicación para auditoria de redes para VoIP de Alcatel. Se analizaron las alternativas para acceder a los servidores de

comunicaciones unificadas desde Internet con los equipos con que se cuenta en Anew. Por último se realizó un estudio de los sistemas similares ofrecidos por los principales participantes en el área, sus ventajas e implicaciones económicas.

3.1.2.- Desarrollo

En esta etapa se realizaron las pruebas para determinar si la red interna podía soportar las nuevas aplicaciones. Estas pruebas se realizaron con la aplicación Alcatel VoIP Assessment Tool y sets telefónicos IP e-Reflexes. Se configuró una VPN y se realizaron pruebas de acceso desde Internet a diferentes servidores de la compañía. Se configuraron las rutas y puertos necesarios en los equipos. Se hizo el dimensionamiento de la solución en base a los resultados arrojados por el software ACTIS de Alcatel y el número de usuarios.

Se configuró la central telefónica para los nuevos servicios y usuarios. Se instalaron y configuraron los servidores de comunicaciones unificadas. Se revisó la configuración del servidor de dominios y se hicieron pruebas con un servidor de correos interno. Se plantearon diferentes alternativas para el servidor de correo.

3.1.3.- Supervisión del sistema.

En esta etapa se elaboraron las guías de usuario con la colaboración y experiencia de estos. Luego se dio un período de seguimiento al sistema, donde se tomaron en cuenta sugerencias para adaptarlas en la configuración final.

3.1.4.- Revisión de soluciones alternativas

Aquí se compararon en términos de funcionalidades y costes diferentes soluciones de comunicaciones unificadas equivalentes a la oferta de Alcatel.

3.1.5.- Elaboración del Tomo y entrenamiento de Personal de Anew.

En esta última etapa se elaboró el tomo del trabajo y también se adiestró al personal técnico de Anew e-Business en el proceso de instalación y configuración del sistema de comunicaciones unificadas.

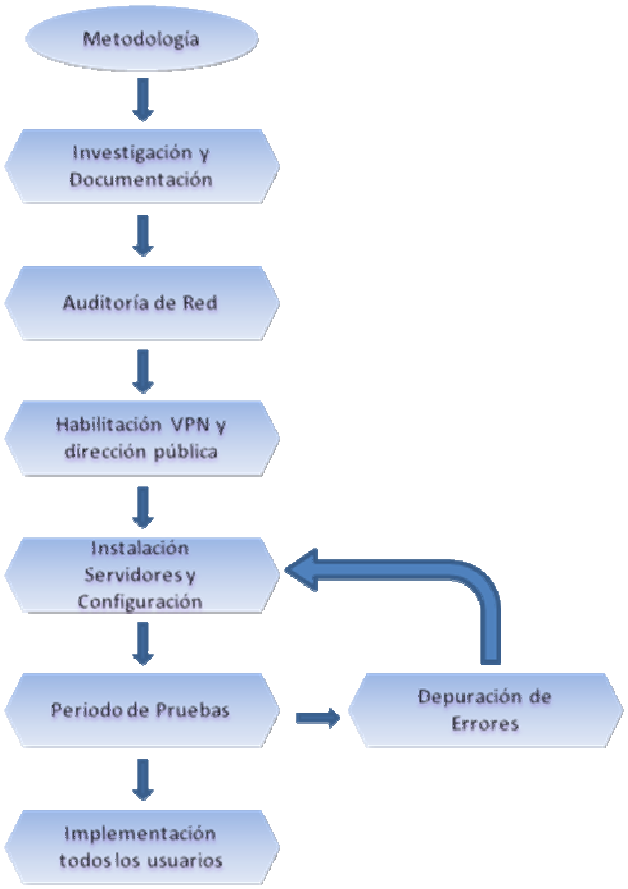


Figura 4 Metodología

3.2.- Aplicación de la Metodología

Una vez diseñada la metodología adecuada para el desarrollo del proyecto, se procedió a su aplicación. Se explican ahora con más detalle cada uno de los pasos realizados en la etapa de desarrollo.

3.2.1.- Análisis de la red de Anew.

La arquitectura de red de Anew es como se muestra en la siguiente figura:

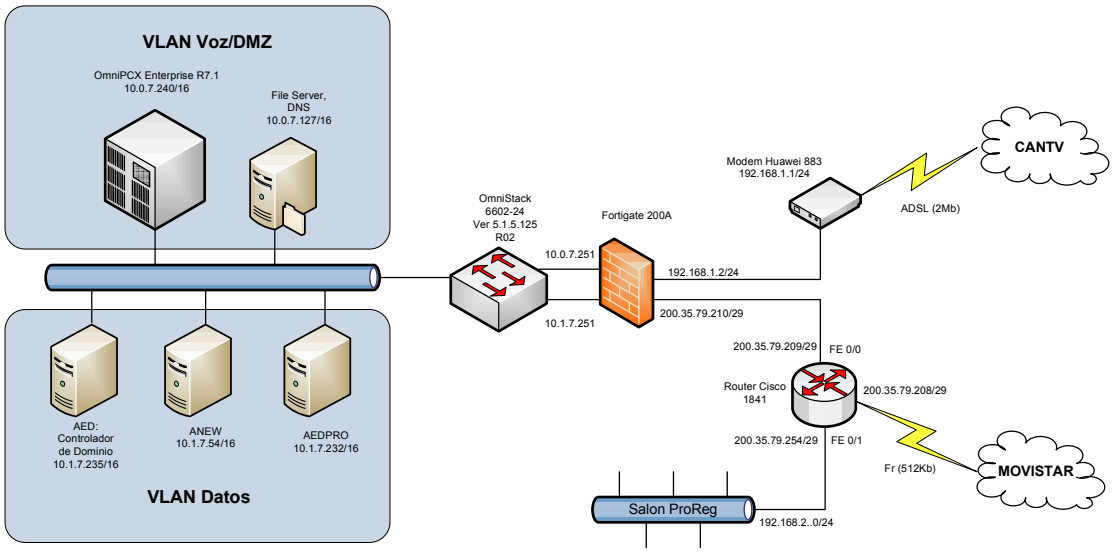


Figura 5 Diagrama de red de Anew

La conexión principal hacia Internet es a través de un enlace ADSL de 2 Mbps del proveedor de servicios CANTV. Hay un enlace Frame Relay secundario de respaldo a través de Movistar que proporciona un ancho de banda de 512 kbps. Ambas conexiones llegan a un Firewall Fortigate 200A que funge el papel de router dentro de la red. El manejo de las VLAN es llevado por un stack de switches Alcatel OmniStack 6602. En todos estos equipos se manejan y han sido configuradas políticas de calidad de servicio.

Se encontraron en esta red dos VLAN configuradas, una llamada VLAN Voz/DMZ y la VLAN Datos. En la primera se encontraban declarados todos los teléfonos de Anew, la central telefónica y el Servidor DNS, y en la segunda los servidores y PCs de los empleados de Anew.

3.2.2.- Despliegue de los Servidores.

La topología más común para instalar OTUC es aquella donde solo hay un Firewall sin DMZ configurado. El Firewall separa la Internet del área privada de la red. Aquí, el firewall revisa y detiene el flujo de información entrante de Internet y autoriza el tráfico saliente como acceso Web y transferencia de archivos, a través de FTP, por ejemplo.

Los clientes y servidores dentro del área privada típicamente son inaccesibles desde Internet. Esto implica que las conexiones TCP e intercambios UDP no pueden ser iniciados desde Internet hasta esta área privada. Si la red privada está configurada con direcciones privadas como es el caso de Anew, el firewall debe usar NAT para traducir las direcciones IP y permitir así a los usuarios finales conectarse a la Internet.

De esta manera, en la configuración idónea, tendríamos 2 áreas principales como se muestra en la siguiente figura:

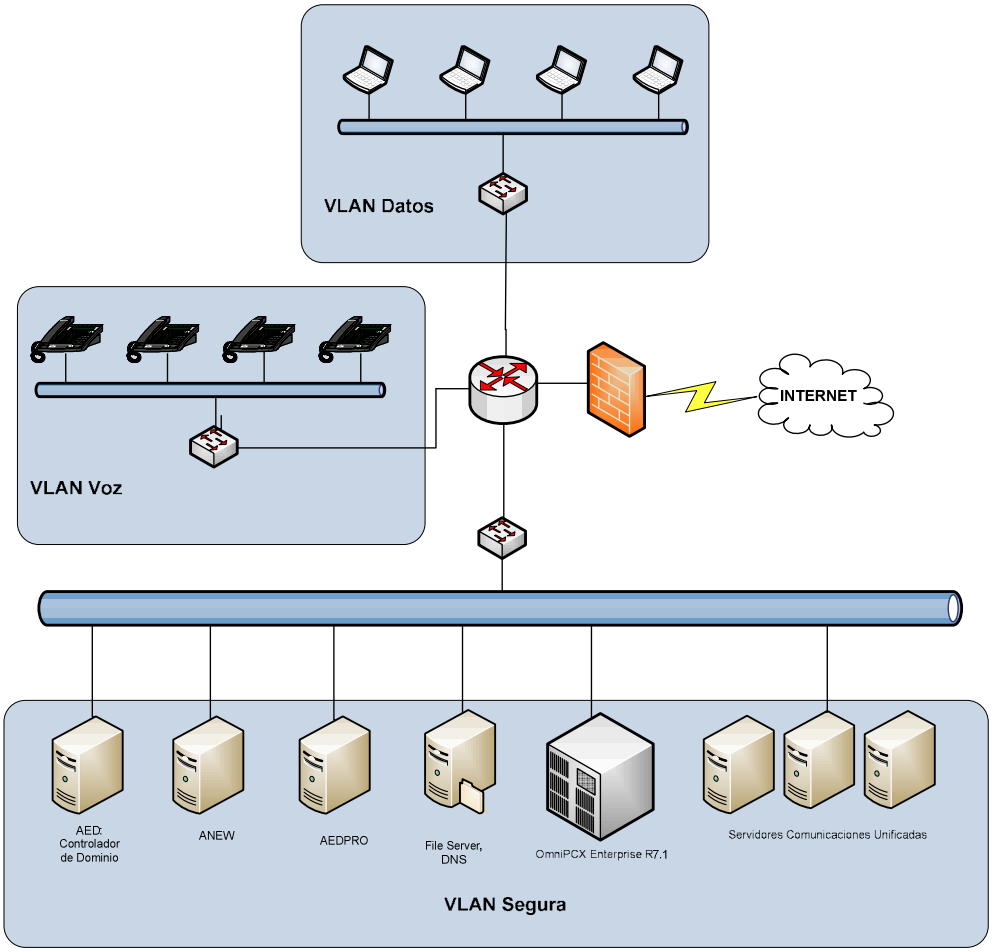


Figura 6 Topología idónea de red

En esta topología tenemos las siguientes áreas:

- El área de Internet que es un área de alto riesgo
- El área privada que debe ser un área segura. Para una arquitectura como la de Anew, en la cual hay tráfico telefónico y de datos, debería haber por lo menos 3 sub-áreas:
  - VLAN de Voz: Donde son desplegados los teléfonos.
  - VLAN de Datos: Donde solo deben ser desplegados PCs.
  - VLAN Segura: que debería contener solamente servidores (servidores webs, centrales telefónicas, servidores de correo, etc.)

Así, los servidores de Comunicaciones Unificadas estarían desplegados en un área de VLAN segura, separada de las otras VLANs (Voz y Datos).

Estas áreas pueden comunicarse entre ellas, pero sujetas a diferentes reglas de acceso. Estas reglas son determinadas por el router.

Los trabajadores remotos y usuarios finales pueden acceder a recursos internos de la compañía como servidores de correo, servidores de voz y servidores de webs. Para mantener segura la conexión a la LAN de la compañía, se deben usar enlaces encriptados a través de una VPN (IPSec ó SSL).

Otra topología avalada por Alcatel para el despliegue de los servidores de comunicaciones unificadas es ubicarlos en la zona conocida como DMZ. Los equipos albergados en el DMZ podrían ser accedidos por los usuarios de la red privada y los de Internet. Como Internet implica riesgos en la seguridad, se requiere un control estricto sobre lo que puede entrar de Internet a estos equipos, servidores normalmente, para evitar ataques externos. En la figura se muestra un ejemplo de esta topología:

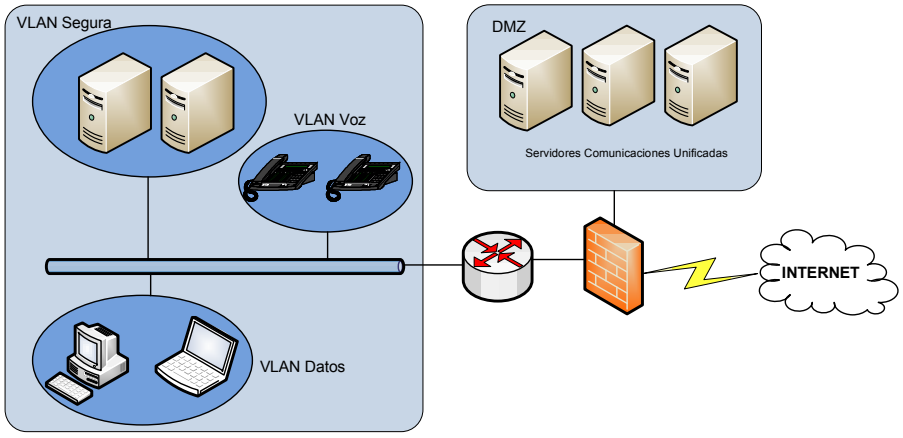


Figura 7 Topología de servidores en DMZ

De esta forma, los servidores ubicados en el DMZ serían accesibles desde Internet. Solo ciertas conexiones restringidas y permitidas podrían ser iniciadas. De contarse con direcciones públicas disponibles el router ejecuta un enrutamiento básico.

El enlace principal a través de CANTV que usa Anew no provee una dirección estática, sino una dinámica. Una dirección estática es necesaria para cualquiera de las dos configuraciones posibles, a través de VPN o desplegando los servidores en el DMZ. El enlace de Movistar ofrece un pool de direcciones públicas estáticas pero no ofrece un ancho de banda apropiado para múltiples aplicaciones multimedia; ante este inconveniente se solicitó a la compañía que adquiriese una dirección estática para el enlace CANTV, pero ésta decidió usar el enlace Frame Relay y ver su comportamiento antes de tomar esa acción.

De esta manera, con la limitante en términos de ancho de banda impuesta por el enlace Frame Relay, la opción de desplegar el servidor de comunicaciones unificadas en el DMZ pasó a ser la opción lógica a tomar. Esto se deduce del incremento considerable que experimentan los paquetes al circular por un enlace VPN, que podría afectar negativamente la calidad de la VoIP a ser transmitida. Ahora bien, como se comentó anteriormente, el firewall instalado en las oficinas de Anew se encarga de enrutar las conexiones, pero al no ser un router especializado carece de los recursos y medios necesarios para asignarle una de las direcciones públicas disponibles a los puertos DMZ. Así, la única opción disponible fue la que envuelve el uso de una VPN. Cabe destacar que el usar el router cisco conectado al enlace Movistar para asignarle una dirección pública a los servidores de comunicaciones unificadas no fue considerado como una opción válida, ya que hubiese dejado el sistema directamente en Internet, sin ningún tipo de protección. Finalmente se configuró la siguiente topología:

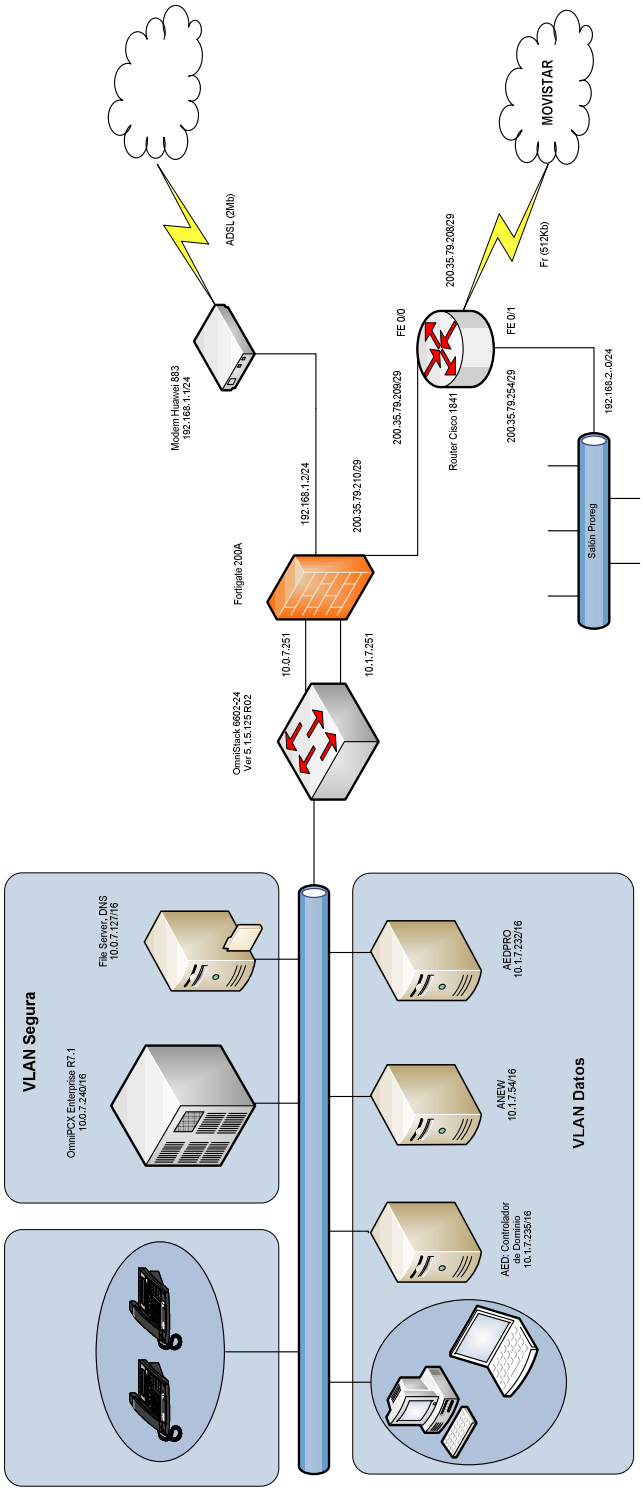


Figura 8 Topología de red definitiva de Anew

Se creó una VLAN exclusiva para la telefonía y así separar el tráfico de voz y data. Al estar los componentes de voz IP en una VLAN diferente a la de datos, se limitan los dominios de colisiones y de broadcast, que pueden impactar la calidad de voz. Esta nueva VLAN, llamada Voz, convive con las VLAN existentes, la llamada Segura donde se alojan la central telefónica y el DNS, y la VLAN Datos donde están todos los computadores de los trabajadores de Anew y otros servidores. Se dispuso que los servidores de comunicaciones unificadas se desplegaran en la VLAN Segura. Los dominios quedaron de la siguiente forma:

VLAN	Segura	Datos	Voz
Dominio	10.0.0.0/16	10.1.0.0/16	10.2.0.0/16

Tabla 1 VLAN Anew

Se seleccionó ese rango de direcciones para la VLAN Voz con el fin mantener la nomenclatura que se había usado previamente para las otras VLAN.

Para la crear la nueva VLAN se usó la herramienta Web de los switch Alcatel. En esta interfaz se creó la nueva entrada Voz, (ver figura 9), y luego, se asignaron todos los puertos correspondientes a los teléfonos IP de la oficina a esta nueva VLAN.

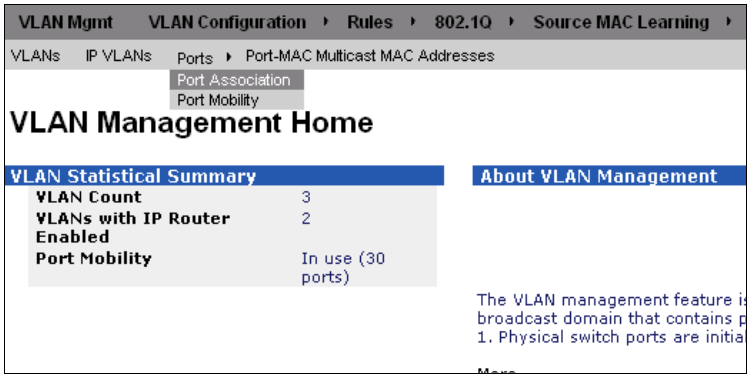


Figura 9 Interfaz web de los switches Alcatel

Los parámetros usados para la creación de la VLAN fueron los siguientes:

Figura 10 Ventana de nueva VLAN

El parámetro Admin Status habilita los parámetros administrativos de la VLAN. Cuando una VLAN esta administrativamente deshabilitada la asignación dinámica y estática de los puertos se mantiene, pero el tráfico en los puertos no se reenvía. Se fijó como habilitada.

Spanning Tree Protocol: Permite la participación del protocolo spanning tree para la VLAN. En los switches de Anew no hay rutas redundantes, por ello se deja desactivado.

VLAN Tag Mobile Port Status: Permite la clasificación de paquetes etiquetados 802.1q recibidos en puertos móviles. No hay puertos móviles configurados por lo tanto esa opción queda desactivada.

No fue necesaria configuración adicional en los teléfonos. En la PBX se definió un nuevo rango de direcciones a ser usadas para los sets, y estos tomaron las direcciones de manera automática.

3.2.3.- Creación de la VPN y puertos del Firewall

Anew solicitó un documento donde se especificaran todos los pasos que se efectuaron en la creación y configuración de la VPN. También se solicitó un manual para los usuarios remotos, donde estarían todas las instrucciones para acceder a la VPN. Ambos manuales se encuentran en los anexos. Los puertos fueron abiertos según lo indicado en la guía proporcionada por Alcatel llamada IP Services and Port numbers incluida en los anexos. En la creación de la VPN se usó la tecnología nativa del firewall para VPNs, IPsec.

3.2.4- Dimensionamiento de la aplicación

Anew e-Business distribution C.A. se organiza de la siguiente manera:

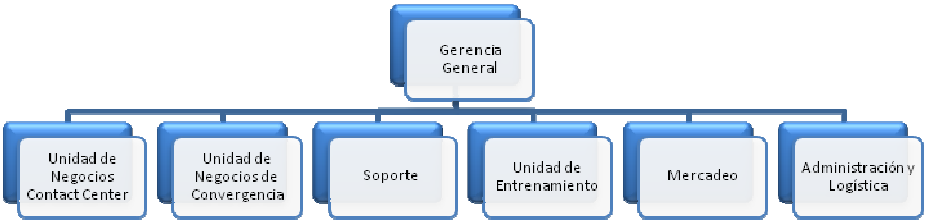


Figura 11 Estructura de Anew

En estos diferentes departamentos laboran un total de 56 personas. Si bien la aplicación esta diseñada para todo tipo de trabajadores independientemente de su rol dentro de la compañía, la aplicación se enfocó por los momentos a aquellos que forman parte del llamado equipo internacional. Este equipo internacional esta

conformado por 20 personas, que se encargan de vigilar y administrar la operación de la compañía en sus sedes en el extranjero. Esta vigilancia y administración implica traslados continuos entre las oficinas de Colombia, Panamá, Estados Unidos y España. A pesar de esta limitante, el diseño se hizo pensado en todos los empleados de Anew y en las proyecciones de crecimiento que la empresa tiene planeadas para el período de vida útil de la solución.

3.2.4.1.- Tiempo de vida útil y planes de crecimiento

Alcatel establece un tiempo de vida útil para sus productos de software de 3 años: Durante el último año de este período, denominado phase-out (ver figura 12), solo se ofrece asistencia técnica limitada, sin corrección de errores, y desaparece por completo a los 36 meses. La versión de Otuc instalada es la 4.1, ésta fue liberada en noviembre del año 2006, por ello se espera sea usada por lo menos hasta noviembre del 2009.

Name of period	Timeframe	Release-related activities
Active Commercial Delivery	From T0 to T0 + 18 months	Release N may be sold without restriction
Pre-phase-out period	From T0 +18 months to T0 + 24 months	No new orders can be placed for Release N, except to add nodes to an existing network or make add-ons to an existing system.
Phase-out period	From T0 + 24 months to T0 + 36 months	Only add-ons to existing systems are allowed. Support: no more bug fixing, but helpdesk is available
End of life	After T0 + 36 months	No more help desk support. Add-ons can be made to existing shelves, provided boards are still in the catalog.

Figura 12 Políticas de vida útil para productos Alcatel [5]

Anew e.-B. pretende incorporar a sus filas laborales durante el período de vida útil de OTUC (2008 y 2009) cerca de 40 nuevos trabajadores a través de

programas de recién graduados, el primero pautado para marzo del año 2008 y el siguiente para principios del 2009, terminando así con aproximadamente 100 personas.

El sistema de comunicaciones unificadas funciona bajo un modelo de licencias que permite instalar y configurar todos los servicios y usuarios que se quiera, pero solo se podrán habilitar aquellos que se han comprado. Así, se pudo configurar diseñar y configurar el sistema - en términos de hardware e infraestructura - pensando en los 100 empleados que habrá para el año 2009. Estos usuarios y servicios se irán habilitando a medida que la empresa lo crea pertinente.

3.2.4.2.- Número de Servidores y recursos necesarios.

Como se mencionó anteriormente, el sistema de comunicaciones unificadas de Alcatel OTUC, se maneja bajo un sistema de licencias que permite controlar el número de usuarios y servicios que se añaden al sistema. Estas licencias se clasificaron de dos maneras, aquellas que se instalan en los servidores de comunicaciones unificadas, y aquellas que se instalan en la central telefónica. Las primeras corresponden a la cantidad de usuarios y los permisos de cada uno, mientras que las segundas al número de puertos disponibles para el tráfico de diferentes aplicaciones y derechos a ciertos servicios.

Para la compra de todas estas licencias y verificar la coherencia en el pedido, se utiliza el software Actis de Alcatel. Actis sugiere valores típicos para ciertos parámetros, asociados a ocupación y tráfico del sistema, mas no realiza cálculos para determinar el uso óptimo de recursos. Para estos cálculos se usó una hoja de cálculo suministrada por Alcatel a través de su portal business partner.

Esta hoja de cálculo, Alcatel Sizing Tool, toma porcentajes de tráfico para los usuarios en diversas actividades y determina el número apropiado de puertos

VxML y Text to speech a ser utilizados por la central como el número de servidores requeridos para la instalación. Alcatel ofrece valores típicos de tráfico para el dimensionamiento basándose en el número de usuarios y área de la industria en la que la empresa se desarrolla. Dentro de esta clasificación, Anew e-Business se ubica como una empresa mediana - medium business - del sector telecomunicaciones. Estos valores están representados en la figura 13.

Customer Input to compute PC Deployment			Traffic Usage			Compute for
			Low	Medium	High	
Avg. number of calls per day per users	Total Outgoing & Incoming Calls		10	20	40	My Phone, My Messaging or
	Total Incoming Calls		5	10	20	My Assistant Server Number
Avg. number of emails per day per users	Total Received e-mails		10	20	40	My Messaging servers number
	Total Sent e-mails		5	10	20	
My Assistant	Number of users & % of users per profile (declared)	100	25%	50%	25%	My Assistant servers number
	Avg. Number of TUI calls per day per user		0,2	2	4	VxML ports number
	Avg. Seconds in system per TUI call		20	20	20	
	Busy hour percentage for TUI calls		8%	12%	16%	
My Phone	Number of users & % of users per profile (declared)	100	25%	50%	25%	My Phone servers number
	Avg. usage per day in muntes per user (Voice Messages)		0,2	2	4	VxML ports number
	Avg. seconds in system per TUI call		20	20	20	
	Busy hour percentage for TUI calls		8%	12%	16%	
My Messaging - Integrated (w/o webmail)	Number of users & % of users per profile (declared)	0	25%	50%	25%	My Messaging servers number
	Avg. usage per day in muntes per user (Voice Messages)		2	6	12	46x3 ports number
	Busy hour percentage		8%	12%	16%	
My Messaging - Integrated (w webmail)	Number of users & % of users per profile (declared)	0	25%	50%	25%	My Messaging servers number
	Avg. usage per day in minutes per user (email reading)		1	2	3	VxML ports number
	Avg. usage per day in minutes per user (Voice Messages)		2	6	12	46x3 ports number
	Busy hour percentage		8%	12%	16%	
My Messaging - Unified	Number of users & % of users per profile (declared)	100	25%	50%	25%	My Messaging servers number
	Avg. usage per day in minutes per user (Voice Messages email reading)		3	8	15	VxML ports number
	Busy hour percentage		8%	12%	16%	
	e-mail server type for My Messaging UM		Exchange			
My Teamwork	Number of conf. users & % of user per profile (declared)	100	25%	50%	25%	My Teamwork ports number
	Avg. usage per day in minutes per user		30	60	90	
	Busy hour percentage		2%	3%	4%	
Operating System Type	Linux or Windows		Linux			
PBXs Number			1			OTS Number

Figura 13 Alcatel Sizing Tool

Parte de los módulos My Assistant y My Messaging de Otuc no están disponibles para el sistema operativo Microsoft Windows, así, se escogió Linux Red Hat por ofrecer una versión más completa de la solución. Esta decisión afecta el número de servidores necesarios. A su vez, como la compañía aún no había decidido que sistema de correo implementar - de decidir adoptar alguno - se utilizó Microsoft

Exchange en el cálculo de manera provisional. Este parámetro determina la capacidad mínima en GB de los buzones de correo para los usuarios. Las otras opciones disponibles son servidores de correo IMAP4, POP3 e IBM Domino.

Los resultados que arrojó la herramienta se muestran en la siguiente tabla:

Server Results		
For All Aplications	Total Number of UC Servers	2
	Total ports required (VxML)	38
	Total TTS ports	19
My Messaging - Unified	Minimum daily mailboxes capacity for all users for voice messages (Gbytes)	1,16

Figura 14 Resultados Alcatel Sizing Tool

Ya con esta información se pudo finalmente llenar la orden de compra dentro del programa Actis para 20 usuarios con los siguientes valores:

OmniTouch Unified Communications	
Number of OTUC users	20
Number of additional users for collaboration	0
Options for telephony, messaging and one number services	
Voice ports (VxML)	38
Text to speech access	19
Additional languages for Text to speech	0
4980 Softphone users	20

Tabla 2 Orden de compra Actis

3.2.5.- Auditoria de Red Anew

Para preservar la calidad de voz Alcatel recomienda que cualquier interface Ethernet que lleve tráfico de voz, deba ser planificada de manera tal que no se utilice más del 30% de la capacidad nominal de la red (por ejemplo, 300Mb/s de un puerto de 1 Gb/sec). La capacidad mínima que hay en algún segmento de la red Ethernet de Anew – que es la que dictará la capacidad nominal – es de 100Mb/s. En esta red, dependiendo del códec usado, se pueden acomodar hasta 2000 streams de voz simultáneos asumiendo que no halla tráfico de datos en la red. Si bien esto suena muy conveniente en teoría, hay otros parámetros que también influirán en la calidad de voz, tales como el retraso (delay), el jitter y la pérdida de paquetes.

El sistema de comunicaciones unificadas OmniTouch UC trabaja con los códecs de audio G.711 y G.729. A la hora de decidir cual usar hay dos parámetros importantes que se deben tomar en cuenta, la calidad de audio que se espera tener y el ancho de banda con el que se dispone.

En la siguiente tabla se muestra el ancho de banda necesario para cada códec según el tipo de enlace en el que se este transmitiendo.

Códec	Bit rate (kbps)	Delay códec (ms)	Tamaño de paquete (bytes)	Encabezado IP/UDP/RTP (bytes)	Encabezado L2 (bytes)	Ancho de banda nominal (1 canal)
Ethernet						
G.711	64	1,5	160	40	14	85,6
G729	8	15	10	40	14	70,4
Frame Relay						
G.711	64	1,5	160	40	4	81,6
G.729	8	15	10	40	4	19,7
IPSEC [Tunel VPN]						
G.711	NA	NA	NA	NA	NA	91,73
G.729	NA	NA	NA	NA	NA	34,13

Tabla 3 Ocupación de ancho de banda de protocolos de audio

Dentro de la red de Anew, usando G.711, el códec más costoso en términos de ancho de banda, es posible permitir conversaciones simultáneas de los 100 posibles trabajadores de Anew y aún así contar cada uno con hasta 214,4 kbps para tráfico de datos cumpliendo la sugerencia del 30% de Alcatel.

$$AB_{usuario} = \frac{AB_{total} * 30\%}{\text{Número de usuarios}} - AB_{Stream} \quad [6]$$

Donde:

$AB_{usuario}$: El ancho de banda que dispondrá para cada aplicación.
AB_{total}: El ancho de banda de la red interna.
AB_{stream}: El Ancho de banda de cada canal de voz usando determinado códec.
Número de usuarios: el máximo de usuarios que puedan usar el sistema en un momento dado.

$$AB_{usuario} = \frac{100.000Kbps * 0,3}{100} - 85,6Kbps = 214,4\ Kbps$$

Este ancho de banda es suficiente para el tipo de aplicaciones que se usan normalmente en la oficina (correo electrónico, mensajería instantánea, herramientas de cotización y de diseño). Es importante resaltar que la red de Anew esta certificada para 100Mbps full dúplex. Ahora si bien el tráfico producido por las aplicaciones y portales de comunicaciones unificadas pueden ser despreciadas en estos cálculos según documentación de Alcatel, se debe tomar en cuenta el reducido ancho de banda con que cuentan los usuarios remotos a través de la VPN.

El ancho de banda varía, ya que no se siempre el canal está ocupado por completo. Las conversaciones normales incluyen grandes espacios de silencio, lo que implica muchas veces paquetes vacíos. Un códec, cuya norma indique un flujo de 64 kb se convierte en un flujo mayor de datos dentro de una red IP. La razón principal de

este aumento en el ancho de banda son los encabezados IP y UDP. Los protocolos de VoIP trabajan con paquetes pequeños, donde eventualmente, los encabezados son mucho más grandes que la data del paquete. El ancho de banda depende también de los protocolos de datalink, tamaño de la carga (payload), encabezados ATM, encabezados de compresión.

Como se mencionó anteriormente uno de los grupos de beneficiarios más importantes de la aplicación de comunicaciones unificadas son los usuarios remotos. Sin embargo, estos son los que más limitaciones tendrán debido al ancho de banda con que se cuenta para la VPN. Es por esta misma limitación que se decide usar el códec G.729, ya que usando una VPN en un enlace Frame Relay como el de la oficina, se puede economizar hasta un 62,7% en comparación al ancho de banda usado con el códec G.711. Tomando en cuenta la capacidad actual solo se podrá garantizar a través de la VPN un total de 7 conexiones simultáneas, esta cantidad podría aumentar en función de la supresión de silencios, pero no se puede decir nada con certeza más allá de este punto.

La recomendación UIT-T G.1010 define ciertas reglas para tener una calidad aceptable de voz, mensajería vocal, video, para aplicaciones multimedia extremo a extremo; estos parámetros se muestran en la siguiente tabla:

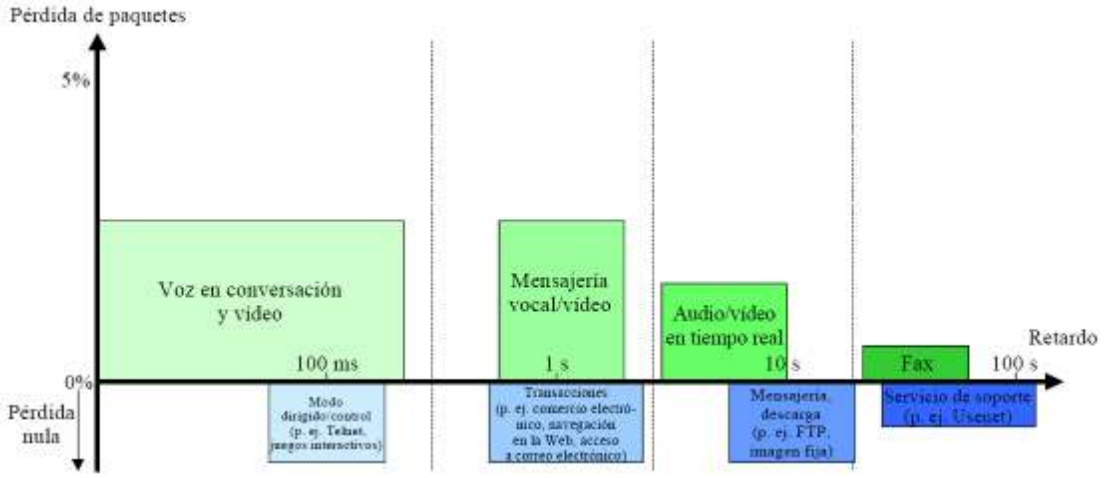


Figura 15 UIT G.1010 Correspondencia entre calidad y servicios [7]

Grado de simetría	Velocidades de datos típicas	Tiempo de transmisión en un sentido	Variación de retardos (jitter)	Pérdida de paquetes
Dos sentidos	4 - 64 kbps	< 150 ms	< 10 ms	< 3%

Tabla 4 Objetivos de calidad de funcionamiento para aplicaciones de audio y video [7]

Para comprobar si la red cumple con estos parámetros, se hicieron pruebas con la aplicación Alcatel VoIP Assessment Tool en conjunto con la aplicación Alcatel VoIP Simulation Tool para estresar la red de datos con flujos de VoIP. Así, se bombardeó la red con paquetes de VoIP con la segunda aplicación. Luego se configuró en dos teléfonos IP Alcatel la dirección del equipo donde se instaló la primera aplicación y ésta tomó control de ellos. La aplicación se encargó de realizar múltiples llamadas de un set al otro y analizar el intercambio de paquetes entre ambos. Estas pruebas fueron realizadas durante una semana en las horas de mayor actividad en la oficina según estadísticas del departamento de soporte, esto es, de 09:00 AM a 11:00 AM y de 3:00 PM a 4:00 PM.

Los parámetros usados en el software para realizar las llamadas se muestran a continuación:

```
SESSION PARAMETERS:
Prueba VoIP
Start immediately
Launch repeatedly
-----------------------------------------------
10.12.2007 08:57:32 CALL RESULTS...
IP PHONE 1: -------- QoS AvisoTicket --------
Local IP address : 10.2.255.10 (prueba), Ver.2.18.0
Remote IP address : 10.2.255.14 (prueba), Ver.2.18.0
Vlan Id : 65535
Duration : 28 sec
Codec : G729 8k
Every loop Immediately
Framing sent : 30 msec
Framing received : 30 msec
```

Los resultados de estas pruebas se muestran a continuación:

Semana del 15/10/2007 al 19/10/2007						
		Lunes	**Martes**	**Miércoles**	**Jueves**	**Viernes**
9:00 AM a 11:00 AM	Delay (ms)	35	30	33	39	38
	Jitter (ms)	7	6	4	4	7
	Pérdida de paquetes	<1%	<1%	<1%	<1%	<1%
	MOS	3,95	3,95	3,95	3,95	3,95
3:00 PM a 4:00 PM	Delay (ms)	28	29	37	28	30
	Jitter (ms)	2	3	2	2	2
	Pérdida de Paquetes.	<1%	<1%	<1%	<1%	<1%
	MOS	3,95	3,95	3,95	3,95	3,95

Tabla 5 Resultado de pruebas de calidad de VoIP

El valor MOS (Mean Opinion Score) fue calculado por la aplicación asumiendo un ruido ambiental de 35 dB según el modelo "E" de la recomendación G.107 de la UIT para cada llamada. Este valor que refleja es una aproximación por medio de algoritmos, ya que una prueba real de este tipo se realiza haciendo evaluaciones con una muestra significativa de personas. Si bien para datos el resultado es siempre el mismo, es consistente con lo que se espera de este códec, cuya máxima puntuación en MOS es de 4. En base a estos resultados se concluyó que la red está preparada para soportar y ofrecer un nivel de calidad aceptable para la implementación de VoIP a ser desplegada en la oficina.

3.2.6. –Elección del sistema de correos

El correo de Anew es manejado por una compañía llamada 1&1 Internet Inc. Ellos se encargan del manejo de dominios y también ofrecen un servicio de webmail compatible con los protocolo IMAP4 y POP3, lo que permite a todos los usuarios de la compañía manejar sus correos a través de utilidades como Outlook o Mozilla Thunderbird. Si bien 1&1 ofrece la opción de actualizar las cuentas a unas de tipo Microsoft Exchange, resulta muy costoso, y a fin de cuentas sería solo una solución temporal. Es por esto, que se decidió analizar cuál sería la mejor opción a la hora de implementar un servidor de correo.

Como se ha mencionado anteriormente, los usuarios de Anew poseen un alto nivel de movilidad, así, cuentan en muchas oportunidades con más de un PC, la estación de trabajo de la oficina, un PC en sus hogares y un laptop. Los empleados del departamento de Soporte y los del área Contact Center deben cumplir guardias nocturnas quincenales; en estas guardias ellos prestan primero asistencia telefónica y vía Internet al cliente para solucionar su problema. De no lograr la solución exitosa por estos medios se trasladan al sitio. Es así que este tipo de trabajador necesita acceso a sus correos electrónicos desde su hogar y desde la oficina.

Cuando un nuevo empleado llega a la oficina, se le configura una cuenta de correo con 1&1, y se le proporciona información de cómo configurar su cliente de correo para descargar los mensajes a través del protocolo POP3. Por este motivo, todos los trabajadores de Anew usan este protocolo, muchos desconocen las ventajas o diferencias de IMAP, o bien, no saben que pueden acceder a su cuenta a través de este último.

Para hacer una justa comparación entre ambos protocolos se realizó una tabla donde se muestran las características comunes de ambos y aquellas que los diferencian.

Características comunes	**IMAP4**	**POP3**
Soporta acceso sin conexión.	•	•
Los correos nuevos pueden ser recuperados de cualquier lugar en la red.	•	•
El protocolo es abierto, definido por la RFC.	•	•
Implementaciones y códigos fuente gratis disponibles.	•	•
Clientes disponibles.	•	•
Implementaciones comerciales disponibles.	•	•
Orientado a Internet (no se necesitan Gateways SMTP).	•	•
Solo maneja acceso, se apoya en SMTP para envío.	•	•
Soporta identificación de mensajes persistente.	•	•
Ventajas de POP3		
Protocolo Simple, fácil de implementar.		•
Más software de clientes disponibles.		•
Ventajas de IMAP4		
Puede manipular banderas de estatus de mensajes persistentes.	•	
Puede almacenar mensajes y vistas previas.	•	
Puede acceder y manejar múltiples buzones de correo.	•	
Soporta actualizaciones simultáneas y permite buzones de correo	•	

compartidos.		
Se adapta al uso de datos diferentes a los de correos electrónicos, NetNews, documentos.	•	
Se adapta a esquemas sin conexión, con mínimo tiempo de conexión y de espacio en disco.	•	
Permite el uso óptimo del desempeño, especialmente sobre enlaces de baja velocidad.	•	

Tabla 6 Comparación entre IMAP4 y POP3

Por razones de movilidad y facilidad de acceso desde múltiples equipos se recomienda el uso de un servidor de correos IMAP4. El proveedor de servicios que se utiliza actualmente puede proporcionar este servicio, pero aún no había sido configurado por los usuarios. De tomarse la decisión de instalar un servidor de correos propio albergado dentro de la compañía, existen numerosas distribuciones para todos los sistemas operativos. Le fueron enviados al departamento de soporte las instrucciones para habilitar IMAP a los usuarios de Anew, como se indica en la pagina de ayuda de 1&1.

Las ventajas de tener un servidor de correos propio son muchas, y es por ellos que se recomienda instalar uno. Entre estas destacan:

- Ahorro de costes en contratación de servicios externos.
- Gestión de cuentas y listas de correo.
- La información interna no sale al exterior de la empresa, lo que aumenta la seguridad.
- Posibilidad de instalar software antivirus, antispam, y portal webmail.
- Control total sobre su administración

3.2.7. -Configuración de la central telefónica

A través de la aplicación Telnet, se puede acceder al sistema operativo de la central telefónica. Una vez aquí, con el comando mgr (manager) se tiene una interfaz gráfica para la configuración de sus prestaciones, facilidades y servicios. Estas configuraciones fueron hechas siguiendo las indicaciones de los manuales de instalación de Otuc y bajo la tutela del departamento técnico de la empresa.

Figura 16 Utilidad de configuración mgr

3.2.7.1.- Usuarios configurados

Esta es la lista de usuarios a los que se configuró la solución:

Nombre	Correo electrónico	Extensión Regular[†]	Extensión MPC2[‡]
Angel Aguilera	aaguilera@anew.com.ve	812	19812

[†] Se refiere al número de la extensión correspondiente al set telefónico físico de cada usuario.

[‡] Este es el número de extensión virtual Multimedia PC2 creado para cada usuario de otuc.

Sioly Coronado	scoronado@anew.com.ve	883	19883
José Escalona	jescalona@anew.com.ve	816	19816
Edgar Escobar	eescobar@anew.com.ve	817	19817
Alberto Flores	aflores@anew.com.ve	819	19819
Fernando Fouillioux	ffouillioux@anew.com.ve	850	19850
Francisco Fraino	ffraino@anew.com.ve	865	19865
Daniel García	dgarcia@anew.com.ve	841	19841
Darío García	dagarcia@anew.com.ve	842	19842
José Granados	jgranados@anew.com.ve	814	19814
Néstor López	nlopez@anew.com.ve	835	19835
Mayauri Méndez	mmendez@anew.com.ve	825	19825
Enrique Muñoz	emuñoz@anew.com.ve	826	19826
Antonio Parra	aparra@anew.com.ve	895	19895
Carlos Pérez	cperez@anew.com.ve	864	19864
José Raspatella	jraspatella@anew.com.ve	824	19824
José Romero	jromero@anew.com.ve	809	19809
Hellen Silva	hsilva@anew.com.ve	832	19832
Edgar Suarez	esuarez@anew.com.ve	858	19858
María Trovato	mtrovato@anew.com.ve	800	19800
Franco Uccelletti	fuccelletti@anew.com.ve	863	19863

Tabla 7 Usuarios de Otuc

3.2.7.2.- Creación de extensiones Multimedia PC2

Para todos los usuarios existentes se creó otra extensión con un tipo de teléfono Multimedia PC2, que será utilizado por la aplicación My Web Softphone. Las extensiones se reflejan en la tabla de arriba

Directory number	:	Número de directorio vacío	|19850
Directory name	:	Nombre de directorio	|ffouillioux
Directory first name	:	Nombre del usuario	|fernando
Set Type	:	Tipo de teléfono configurado	|+4035

3.2.7.3.- Creación facilidad nomádica y grupo troncal IP

La creación de facilidad nomádica para usuarios remotos se hizo a través del menú users/create.

Directory number	:	Número de directorio vacío	|19700
Directory name	:	Nombre de directorio	|ghostz
Directory first name	:	Nombre del usuario	|nomadic
Set Type	:	Tipo de teléfono configurado	|+analog
Ghost Z	:	+True	|+True
Ghost Z Features	:	+nomadic	|+nomadic

Luego a través del menú /Trunk Groups/create se creó el grupo troncal usado por los usuarios remotos

Trunk Group Id	:	Número de grupo troncal vacío	|120
Trunk Group Type	:	+T2	|T2
Trunk Group Name	:	Nombre que se quiere	|IP
Remote Network	:	Número de red	|15
Node Number	:	Número de nodo	|1
Q931 Signal Variant	:	+ISDN all countries	|+ISDN all |countries
T2 Specificity	:	+IP	|+IP

Y luego se hicieron modificaciones adicionales a través de /Trunk Groups/Trunk Group/Review-Modify

Trunk Group Id	:	Número de grupo troncal	|120
No of digits unused	:	Número de dígitos a suprimir	|0

Se configuró la dirección física del gabinete para la tarjeta de acceso VoIP en la central, /Trunk Groups/Trunk Group/T2 T1 T0 Access/Create

Trunk Group Id	:	Número de grupo troncal	|120
Physical Address	:	Acceso a la tarjeta de VoIP	|0-4-0
Tipo de acceso	:	+T2	|+T2
Trunk Group Type	:	+T2	|T2

Y por último se agrego la facilidad “Park Call/Retreive” a los usuarios remotos (para permitir el cambio de modo VoIP a modo normal) /Classes of Service/Phone Features COS/Review-Modify

Phone Feature COS	:	Número de clase de servicio	|0
Park Call/Retrieve	:	0 para prohibir 1 para permitir	|1

3.2.7.4.- Configuración My Phone Touch User Interface

Para la comunicación entre la central telefónica y cada una de las aplicaciones de OTUC se deben configurar aplicaciones de correos de voz externos.

/Applications/external voice mail/creation

Voice Mail dir number	:	Número de directorio vacío	|19701

Directory name	:	Nombre de directorio	|TUIMyPhone
Connection COS Id	:	Clase de servicio usada	|0
Public Network COS	:	Categoría de red pública	|2
URL User Name	:	Número MyPhoneTUI usado por SIP	|19701
Remote SIP Domain	:	False proxy integrado, True no	|+False
URL Domain	:	URL del dominio SIP	|10.0.7.240
Public Network COS	:	Categoría de red pública	|2
SIP Authentication	:	Solo en caso de autenticación	|19701
SIP Passwd	:	Solo en caso de autenticación	|19701

3.2.7.5.- Configuración para My Assistant

Para la utilidad Web My Assistant se configura un enlace hibrido local /Inter-Node Links/Logical links (ABC-F)/create

Link Name	:	Nombre del enlace	|Loop
Link Type	:	+Hybrid	|+Hybrid
Adjacent Node	:	Número de nodo	|1
Adjacent Network	:	Número de Network Id libre	|12
Multi Access hybrid link	:	+True	|+True

Luego, /Inter-Node Links/Logical links (ABC-F)/Hybrid Link Access/create

Link Name	:	Nombre del enlace	|Loop
Access Number	:	1	|1
Signaling Type	:	+ B Channel	|+ B Channel

E igual para el número de acceso 2, /Inter-Node Links/Logical links (ABC-F)/Hybrid Link Access/create

Link Name	:	Nombre del enlace	|Loop
Access Number	:	2	|2
Signaling Type	:	+ B Channel	|+ B Channel

Creación del número RSI (Routing Service Interface), /Application/ CCD/RSI/create.

RSI Directory Number	:	Número de directorio vacío	|19710
Directory Name	:	Nombre del directorio	|RSI
Node Number	:	Número de nodo	|1
Entity	:	Asociación a la central N.1	|1
Ringing Overflow Timer	:	150	|150
Local Call Authorization	:	+True	|+True
RSI Supervised Transfer	:	+True	|+True
Application Type	:	+ecc	|+ecc

Configuración adicional para reglas de filtrado en los eventos CSTA /Application/CSTA/Review-Modify

Set Callback on calling device	:	+Yes	|+Yes

3.2.7.6.- Configuración My Assistant Touch User Interface

Se creó una aplicacion de correo externo para permitir la comunicación entre la aplicación y la central.

/Applications/external voice mail/creation

Voice Mail dir number	:	Número de directorio vacío	|19702
Directory name	:	Nombre de directorio	|My Assistant
Connection COS Id	:	Clase de servicio usada	|0

Public Network COS	:	Categoría de red pública	|2
URL User Name	:	Número MyPhoneTUI usado por SIP	|19702
Remote SIP Domain	:	False proxy integrado, True no	|+False
URL Domain	:	URL del dominio SIP	|10.0.7.240
Public Network COS	:	Categoría de red pública	|2
SIP Authentication	:	Solo en caso de autenticación	|19702
SIP Passwd	:	Solo en caso de autenticación	|19702

3.2.7.7.- Configuración My Messaging

Se creó una aplicacion de correo externo para permitir la comunicación entre la aplicación My Messaging Web/TUI y la central.

/Applications/external voice mail/creation

Voice Mail dir number	:	Número de directorio vacío	|19703
Directory name	:	Nombre de directorio	|Messaging
Connection COS Id	:	Clase de servicio usada |0	
Public Network COS	:	Categoría de red pública	|2
URL User Name	:	Número MyPhoneTUI usado por SIP	|19703
Remote SIP Domain	:	False proxy integrado, True no	|+False
URL Domain	:	URL del dominio SIP	|10.0.7.240
Public Network COS	:	Categoría de red pública	|2
SIP Authentication	:	Solo en caso de autenticación	|19703
SIP Passwd	:	Solo en caso de autenticación	|19703

3.2.7.8.- Parámetros de administración común

Se configuró el prefijo de acceso al buzón de voz y las características telefónicas COS /Translator/Prefix Plan

Number	:	Número disponible en el plan	|898
Prefix Meaning	:	+Local Features	|+Local Feat.
Local Features	:	+Voice Mail Access	|+Voice Mail | access

Se asignó el derecho en Clases de Servicio:
/Classes of Service/Phone Features Classes of Service/Review-modify/PCX Services

Voice Mail access	:	0 para prohibir 1 autorizar	|1
Conversation Recording	:	0 para prohibir 1 autorizar	|1

Para asegurar el funcionamiento correcto de los reenvíos, el parámetro de sistema GF diversión on joining debe ser fijado en No.

/System/Other System Param./External Signaling Parameters

GF diversión on joining	:	+NO	|NO

Creación de optimización de prefijos: /Translator/Prefix Plan/creation.

Number	:	Número disponible en el directorio	|19899
Prefix Meaning	:	+Local Features	|+Local Feat.
Local Meaning	:	+PCX Address in DPNSS	|+PCX |Address in |DPNSS

Se habilitaron las tablas de enrutamiento de red, /Translator/Network routing table/Review-modify

Network No	:	Número disponible en el directorio	|2
Rank of first digits to to be send	:	+Valor por defecto	|1
Protocol Type	:	Valor por defecto	|+ABC-F

Creación de un grupo troncal SIP, /Trunk group/creation.

Trunk Group Id	:	Número de grupo troncal	|119
Trunk Group Type	:	+T2	|T2
Trunk Group Name	:	Nombre	|SIP
Remote network	:	Número de red remota	|2
Node Number	:	Número de nodo	|1
Q931 Signal Variant	:	+ABC-F	|+ABC-F
T2 Specificity	:	+SIP	|+SIP

Configuración adicional grupo SIP /Trunk group/Trunk group/Review-modify

Trunk Group Id	:	Número de grupo troncal	|119
Trunk Group Type	:	+T2	|+T2
Supervised by routing	:	Valor por defecto	|+false
IP Compression Type	:	Tipo de compresió a usar	|+G729
Dialing end to end	:		|YES
DMTF end to end signal t	:		|YES

Para la configuración del Gateway SIP se siguieron los siguientes cambios:

/SIP/SIP Gateway/Review-modify

SIP Subnetwork	:	Número de red	|2

SIP Trunk Group	:	Número de grupo trocal SIP	|119
IPAddress	:	Dirección de la PBX	|10.0.7.240
Machine Name-Host	:	Nombre de la PBX	|ANEW
SIP Port Number	:	Valor por defecto	|6060
SIP Proxy Port Number	:	Valor por defecto	|5060
SIP Suscribe min duration	:	Default Value	|1800
SIP Suscribe max duration:		Default Value	|86400
DNS Local Domain Name:		Nombre de dominio	|anew.com.ve

La configuración de SIP Proxy, /SIP/SIP Proxy/Review-modify:

Min Authentication mode	:	SIP none o Digest	|+SIP none

Se agregaron las direcciones de los servidores de comunicaciones unificadas a las direcciones confiables para SIP, /SIP/Trusted IP Addresses/Create:

Trusted IP Address	:	Dirección IP Servidor Media	|10.0.7.126
			|10.0.7.236

Y por ultimo parametros varios:
/IP/IP Parameters/Review-modify

System Option	:	+ Direct RTP	|+ Direct RTP
Direct RTP	:	Auténtico	|+True

Instant Voice Mail, /Applications/external voice mail/creation:

Voice Mail dir number	:	Número de directorio vacío	|19704
Directory name	:	Nombre de directorio	|VoiceIt
Connection COS Id	:	Clase de servicio usada |0	
Public Network COS	:	Categoría de red pública	|2

URL User Name	:	Número MyPhoneTUI usado por SIP	|19704
Remote SIP Domain	:	False proxy integrado, True no	|+False
URL Domain	:	URL del dominio SIP	|10.0.7.240
Public Network COS	:	Categoría de red pública	|2
SIP Authentication	:	Solo en caso de autenticación	|19704
SIP Passwd	:	Solo en caso de autenticación	|19704

Automated Attendant, /Applications/external voice mail/creation:

Voice Mail dir number	:	Número de directorio vacío	|19705
Directory name	:	Nombre de directorio	|AA
Connection COS Id	:	Clase de servicio usada |0	
Public Network COS	:	Categoría de red pública	|2
URL User Name	:	Número MyPhoneTUI usado por SIP	|19705
Remote SIP Domain	:	False proxy integrado, True no	|+False
URL Domain	:	URL del dominio SIP	|10.0.7.240
Public Network COS	:	Categoría de red pública	|2
SIP Authentication	:	Solo en caso de autenticación	|19705
SIP Passwd	:	Solo en caso de autenticación	|19705

Voice Home Page , /Applications/external voice mail/creation:

Voice Mail dir number	:	Número de directorio vacío	|19706
Directory name	:	Nombre de directorio	|VHP
Connection COS Id	:	Clase de servicio usada |0	
Public Network COS	:	Categoría de red pública	|2
URL User Name	:	Número MyPhoneTUI usado por SIP	|19705
Remote SIP Domain	:	False proxy integrado, True no	|+False
URL Domain	:	URL del dominio SIP	|10.0.7.240
Public Network COS	:	Categoría de red pública	|2

SIP Authentication	:	Solo en caso de autenticación	|19705
SIP Passwd	:	Solo en caso de autenticación	|19705

Broadcast para todos los elementos creados:

System/Broadcast
Operational: +Yes

3.2.7.9.- Configuración correo de voz 4635

El acceso a la configuración del correo de voz 4635 se logra conectando directamente un PC a la tarjeta VPU5 (encargada del correo de voz en la PBX) por medio de un cable 10/100 Base T. Una vez el enlace establecido se hizo telnet a su dirección IP: 10.0.7.242.

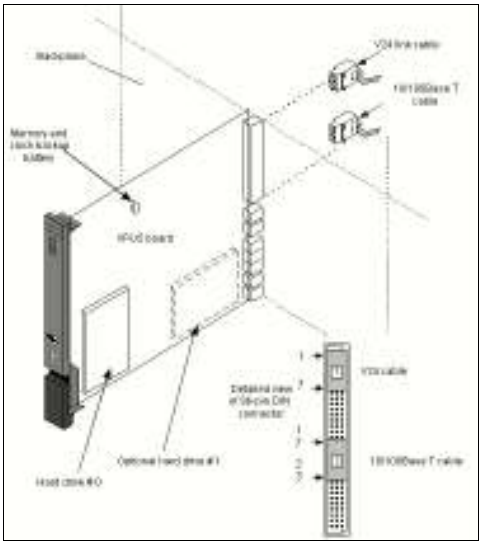


Figura 17 Esquema de conexiones de la tarjeta VPU5 [8]

Del menú general, se seleccionó el menú 17 – External Applications
Se seleccionó el menú 2 - Application Administration
Luego menú 1- Add Application

Siguiendo la documentación se añadieron las aplicaciones 240, 241 y 253, correspondientes a IVR LAN, ASA LAN e InterMail VPMOD TO HOST respectivamente. Se habilitó la opción My Messaging en el menú de clases de servicio y se habilitó el servidor IMAP interno, a través del menú 17 – External Application Management.

3.2.8.- Instalación de los servidores de comunicaciones unificadas.

Para la instalación de los servidores se utilizaron dos equipos Dell PowerEdge 850 homologados por Alcatel para la solución de comunicaciones unificadas. Uno se reservó para el servidor de media, aplicaciones y middleware (Servidor Otuc), y el segundo exclusivamente para My Teamwork.

3.2.8.1.- Instalación del servidor Otuc.

Los servidores fueron entregados con arreglos Raid 1 de 72 GB. El primer paso fue instalar una versión de Red Hat Enterprise 4 de Alcatel. Los parámetros para configurar los dispositivos de red fueron los siguientes:

Login: root
Password: xxxxxxx
IP Address: 10.0.7.126
FQDN (Fully Qualified Domain Name): otuc.anew.com.ve
Subnet Mask: 255.255.0.0
DNS Server IP Address: 10.0.7.127
Default Gateway address: 10.0.7.251

La dirección IP del servidor de comunicaciones unificadas fue tomada de manera aleatoria de un pool de direcciones disponibles en la VLAN correspondiente a los servidores. Esta dirección, al igual que la elegida para el servidor correspondiente

a My Teamwork fue registrada en el DNS interno de la compañía. Este sistema de DNS se basa en Linux, específicamente en el sistema BIND.

Por motivos de seguridad en la instalación por defecto los servicios de servidor FTP y Telnet están deshabilitados. Fueron activados con los siguientes comandos:

./chkconfig --level 345 telnet on
./chkconfig --level 345 vsftpd on
./service vsftd start

Vsftpd hace referencia al servicio Very Safe FTP Daemon que es quién da acceso vía FTP al servidor de Linux. A diferencia de Telnet este debe ser activado también con el comando service start. Ambos servicios fueron configurados para ser ejecutados en los niveles o runlevels 3, 4 y 5 de usuario. El nivel 3 se asocia al estado multiusuario a nivel de consola, el nivel 4 se deja para ser definido por el usuario y el 5 se refiere a un estado multiusuario con interfaz gráfica.

Para el correcto funcionamiento de la señalización por medio del protocolo SIP la sincronía de los eventos es fundamental, por ello se sincroniza el servidor contra la central telefónica por medio del comando ntpdate.

./ntpdate 10.0.7.240

Ya para dar por concluida la instalación del sistema operativo se hicieron pruebas a la configuración de red usando el comando ping contra otros servidores, en la misma VLAN que el servidor y contra estaciones de trabajo ubicados en otra VLAN. También se uso el comando host para comprobar el registro correcto en el servidor DNS.

Una vez instalado el sistema operativo se procedió a la instalación de la aplicación como tal, con la excepción de My Teamwork. Este proceso se realizó de manera remota gracias a la utilidad de escritorio remoto VNC embebida en Red Hat.

Usando el modo tutorial, la aplicación ofrece una Interfaz gráfica amigable donde solo se seleccionan la ruta de instalación y módulos e idiomas de ayuda. Los módulos instalados fueron los siguientes:

- My Unified Messaging
- My Integrated Messaging
- My Assistant
- My Phone
- My Phone Coupling Servers
- My Messaging Coupling Server
- My Assistant Coupling Server
- My Noe Applications.
- Application Server
- Media Server
- Tomcat Server
- Apache Server
- API Framework
- Sybase Database Server
- Sybase Databases
- FLEXlm license server
- Supervision Application
- Web Administration,
- OmniPCX Open Telephony Server
- ACAPI Server and its own LDAP Server
- LDAP server for the DataAccess
- LDAP Schema
- DataAccess
- Presentation Server,
- CRS, IMS, UDAS, ECS
- PCX Management
- Unified Login Server
- A4980 Update
- Extensions Update
- WebAdmin Help On Line
- Application Help On Line
- PhoneSetProgramming
- WSP Tapi
- Authentication Applications
- Backup Application
- Alcatel Logs Rotate
- Supervision Agent, Supervision Client

Una vez finalizado, se reinició el servidor y se dio inicio a la configuración inicial. Como primer paso con el comando passwd se definió la contraseña de un nuevo usuario usado por la aplicación llamado htuser. Este usuario será usado para todas las sesiones remotas ftp y telnet al servidor.

Luego, se copió en la ruta ./opt/Alcatel/FlexLM las licencias suministradas por Alcatel. FlexLM es el servicio que se encarga del licenciamiento y permisos de la aplicación para cada usuario final. Al archivo de licencias, alcoutc.lic, se le asignan las siguientes propiedades de lectura y escritura:

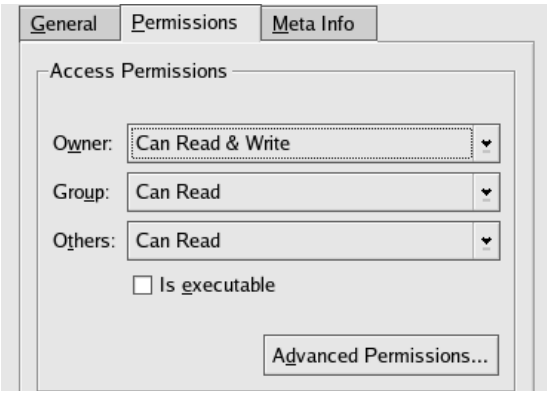


Figura 18 Permisos archivos de licencias

El motor del módulo de Text to speech es instalado en este momento, una vez que ya se ha configurado el licenciamiento. También se instalan los idiomas que se van a utilizar con él. Para Anew e-B se instaló solamente el idioma Español-Mexicano. Para esto se utilizo el administrador de paquetes rpm de Linux.

rpm -ivh ./media/cdrom/rs-api-4.0.8-i386.rpm --nodeps | Motor del módulo

rpm –ivh ./media/cdrom/rs-Spanish-MX-Isabel-4.0-1.i386.rpm --force | Lenguaje

La solución de comunicaciones unificadas incluye una herramienta script llamada postInstall.sh. Esta chequea la coherencia de archivos, y actualiza ciertos módulos. Luego de la instalación de TTS fue ejecutada de manera exitosa.

./media/cdrom/Servers/Complements/Scripts/Linux/postInstall.sh

Luego de reiniciar el servidor se chequeó el estatus de los daemons. Los daemons son programas que corren de fondo, son iniciados como procesos y no están bajo directo control del usuario. Para hacer esto se utiliza el comando service Nombre_Daemon status. El estatus que se busca tener en todos es Started o Running, o sea, iniciado o funcionando.

Application Server:	app_servd	[Started]
OpenLDAP Server:	ldapd	[Started]
Sybase Server:	sybased	[Started]
PostgreSQL:	postgresql	[Started]
Open Telephony Server:	tsad	[Started]
ACAPI Server:	acapi	[Started]
Data Access Server:	dtad	[Started]
Tomcat Server:	tomcatd	[Started]
Integrated Messaging Service:	imsd	[Started]
Call Routing Service:	crsd	[Started]
Universal Directory Access Service:	udasd	[Started]
FLEXlm License server:	flexlmd	[Started]
Presentation server:	pserverd	[Started]
Supervision Agent:	supervision_agentd	[Started]
Supervision Client:	supervision_clientd	[Started]
Media Server:	ecc-ms	[Failed]
	sip-server	[Failed]
	rms-launcher	[Failed]
	rs-launcher	[Failed]
Enhanced_Communication_Service:	ecsd	[Started]
Apache 2 Server:	apache2d	[Started]

Logs Rotate: alc_logs_rotated [Started]

Los servicios correspondientes al Media Server no aparecen funcionando porque aún no se había configurado ninguna central telefónica en la interface de administración. Muchos de estos servicios dependen en otros así que el orden en que se cargan es importante. De caerse o perderse un servicio deben detenerse todos y luego levantarse todos para mantener la continuidad y garantizar el correcto funcionamiento. Esto se logra a través de dos comandos, service otucd stop y service otucd start.

Con los servicios funcionando correctamente se hacen dos últimas pruebas, la primera es acceder a la página de administración y a la página principal del portal de comunicaciones unificadas a través de un PC, y la otra ejecutar un script de revisión del sistema incluido en los medios de instalación de Otuc. Ambas pruebas fueron exitosas.

Y desde una estación de trabajo dentro de la oficina, se abrieron las siguientes direcciones, http://otuc.anew.com.ve/WebAdmin, correspondiente al módulo de administración, y http://otuc.anew.com.ve/, el portal de acceso para los usuarios de manera exitosa por medio de un navegador de Internet.

3.2.8.2.- Instalación del servidor My Teamwork.

Al igual que Otuc, My Teamwork funciona sobre el sistema operativo Red Hat Enterprise 4. Ahora bien, aunque ambos servidores, el servidor Otuc y el servidor My Teamwork, compartan plataformas, hay una gran diferencia, la aplicación My Teamwork es completamente cerrada, el único contacto que un administrador puede tener con la aplicaciones a través de una consola de configuración. En ningún momento, ni siquiera durante la instalación da acceso directo al usuario o administrador al sistema operativo. Esta decisión por parte del fabricante de no

ofrecer acceso directo, es para garantizar la seguridad e integridad del sistema ante vulnerabilidades del sistema operativo.

Luego de iniciar el servidor con la media de instalación, se presenta una serie de pantallas, donde sin necesidad de supervisión se ve el estado de la instalación. El sistema formatea el disco duro, transfiere las imágenes e instala los paquetes necesarios. Luego muestra una ejecuta una post-instalación y se muestra la siguiente consola de configuración:

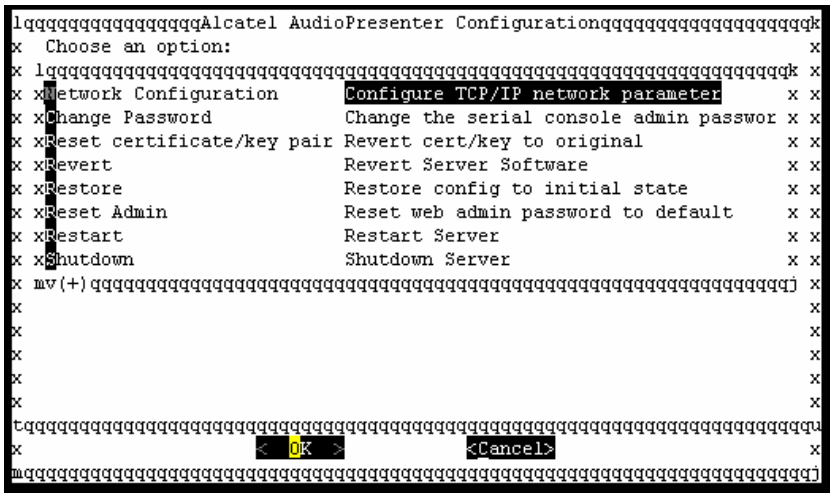


Figura 19 Consola de administración My Teamwork

Aquí se configuran los parámetros de red del sistema y se establece una contraseña para el usuario administrador. Este usuario será usado por el administrador para configurar ciertos parámetros del sistema a través de la interfaz web que ofrece My Teamwork:

Login: admin
Password: xxxxxxx
IP Address: 10.0.7.236
FQDN (Fully Qualified Domain Name): myteamwork.anew.com.ve
Subnet Mask: 255.255.0.0

DNS Server IP Address: 10.0.7.127
Default Gateway address: 10.0.7.251

Desde una computadora con acceso al servidor se accede a la configuración web, por medio de la siguiente dirección, https://myteamwork.anew.com.ve/admin. Se usa el usuario y contraseña definido anteriormente. Al ingresar por primera vez se cargan las licencias en el sistema.

El sistema que utiliza My Teamwork para permitir a sus usuarios compartir archivos, documentos, presentaciones u otras aplicaciones se apoya en el uso de maquinas virtuales. Estas máquinas virtuales se ejecutan de fondo en el servidor, y si bien son invisibles para el usuario final el administrador debe asegurarse del correcto funcionamiento de esta. Para configurar la máquina virtual se necesita lo siguiente:

- Una licencia válida de VMware instalada en el servidor.
- Una copia de Microsoft Windows XP Professional y el serial asociado a esta.
- Una copia de Microsoft Office 2003 y el serial asociado.
- Acceso a la administración web a través de un navegador web en una estación de trabajo.
- TightVNC instalado en la estación de trabajo.

El procedimiento que se siguió fue el siguiente:

A través de un navegador web se llegó a la interfaz de administración, y una ves ahí se fue al menú Advanced Settings / Construct Document Conversion VM.

En la caja etiquetada como Step 1: Enter Product Keys se ingresaron los seriales de las copias de Windows Xp y Office.

Se inició una sesión con TightVNC entre el servidor y la estación de trabajo. TightVNC es un software de escritorio remoto de código libre disponible para múltiples plataformas. Para iniciarla se abrió de cliente VNC en la estación de

trabajo. Luego en la caja titulada Step 2: Open VM Window, se ingreso la dirección IP de la estación de trabajo y se presionó el botón Open. Apareció una ventana de la máquina virtual.

Se insertó el CD de Windows en el servidor, y en la caja etiquetada Step 3:Construct Document Conversion VM se seleccionaron las casillas Initialize e Install Windows and Office. Se seleccionó Start. Se pudo ver la actividad de instalación en la ventana de la maquina virtual TightVNC en el PC del cliente. Apareció un mensaje en el servidor pidiendo fuese insertado el CD de Office 2003. Se debe resaltar que ambas versiones deben ser las versiones americanas en ingles. Ya lista la instalación de la máquina virtual se cambió la configuración del disco duro de ésta para no permitir más cambios a la imagen, con la opción Non-Persistant. Se seleccionó el botón Complete en la caja Step 4: Complete or Cancel Document Conversion VM

Figura 20 Instalación máquina virtual

3.2.9.- Configuración y Administración.

La administración y configuración se hace a través del portal web de Otuc, http://otuc.anew.com.ve/WebAdmin.

La primera vez que se hace contacto con la herramienta de administración web aparece un cuadro de dialogo solicitando la dirección de la central telefónica. En el caso de Anew e-B, se introdujo la dirección IP 10.0.7.240.

Una vez llenado este campo tenemos acceso a la pantalla principal de administración, donde contamos con los siguientes menús:

- Provisioning: Inclusión de usuarios, administradores e importación.
- Configuration: Configuración de servicios y aplicaciones.
- System: Configuración general del sistema, correo de voz y central telefónica.
- Reporting: Estatus de las licencias, alarmas, autenticaciones y monitoreo.

Figura 21 Página principal de administración Otuc

La configuración se realizó en el siguiente orden, de acuerdo a lo especificado en la documentación de la aplicación de comunicaciones unificadas.

Configuración UDAS Universal Directory

Se configuró la información necesaria para el acceso al servidor de Directorio Activo, que se usará para sincronizar a los usuarios.

Server Display Name	:	Nombre que aparecerá en la conf.	|Active Directory
Server Host	:	Dirección IP del servidor	|10.1.7.135
Server Port	:	Puerto a usar	|389
Root	:	Raíz de búsqueda en el directorio	|cn=users, |dc=anew, |dc=com, |dc=ve

Configuración servicio IMS.

smtp IP Address	:	Dirección IP servidor smtp	|smtp.cantv.net
			|Directory
Http Host	:	Dirección IP del servidor web	|10.0.7.126

Configuración del servicio Media Server

En la menú de configuración del servicio se seleccionó Add Primary

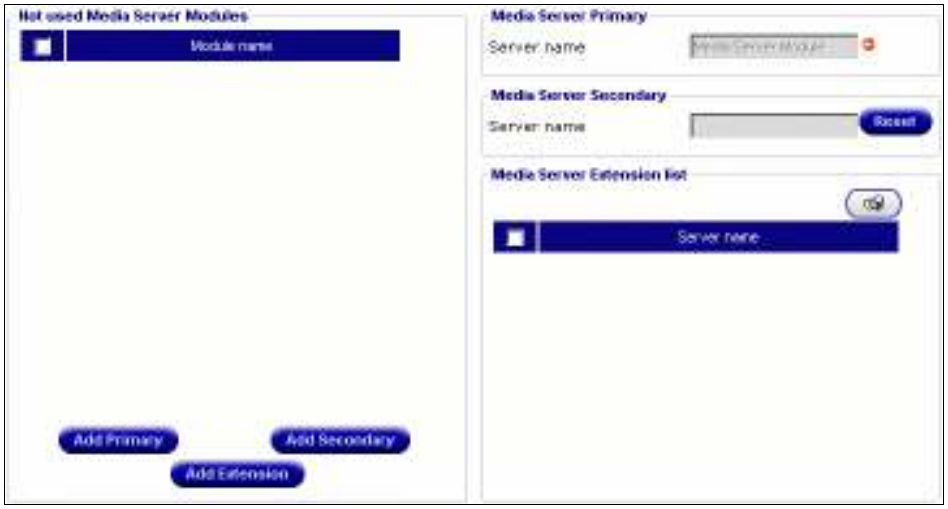


Figura 22 Media Server Service

Una vez ahí se seleccionó el idioma de TTS instalado, duración máxima de grabación y PBX:

TTS Lenguage	:	Lenguaje Instalado	|+Spanish
Recording Duration	:	Máximo tiempo de grabación en segs.	|14000
PBX	:	PBX	|Call Server

Se registraron las aplicaciones con la numeración que fue configurada en la central telefónica:

- TUIMyPhone: 19701
- MyAssistant: 19702
- Messaging: 19703
- RSI: 19710
- VoiceIT: 19704
- AA: 19705
- VHP: 19706

Se configuraron los parámetros RTP:

Default Law	:	Default Law	|+A Law
Quality of Service	:	Parámetros de QOS	|DiffServ
IP TOS	:	Parámetros TOS	|Minimize
			|Delay

Configuración Servicio ECS (Enhanced Communication Service) My Teamwork

Server Host Name	:	Nombre o dirección servidor ACS	|10.0.7.236
Server Sip Port Number	:	Puerto usado para SIP por el Serv.	|8080
Server IP ICS HTTP P. N.	:	Puerto usado para IP ICS HTTP	|80
IM/Presence .	:	Método usado para M.I y presencia	|ICS/HTTP

Configuración Aplicación My Messaging

En el menú aplicaciones se seleccionó My Messaging y se creó una nueva instancia con los siguientes valores:

Servidor IMAP

Name .	:	Nombre del servidor	|imap.1and1.com
Custom Name	:	Nombre que se quiere	|Imap4
Protocol	:	Protocolo usado	|IMAP4
Port	:	Puerto usado	|143
Domain Name	:	Nombre del dominio	|anew.com.ve

Servidor de Transferencia

Name .	:	Nombre del servidor	|mail.cantv.net
Custom Name	:	Nombre que se quiere	|SMTP
Protocol	:	Protocolo usado	|SMTP
Port	:	Puerto usado	|25

Mensajería Integrada 46x5 (Buzón de Voz)

Display Name .	:	Nombre	|Mensajería Integrada
Type	:	4635 ó 4645	|+4635
Http Host	:	Dirección IP	|10.0.7.242
Http Port	:	Puerto usado	|80
Http Path	:	Ruta Http	|/
Voince Mail Number.	:	Número de Buzón en PBX	|892
Custom Name	:	Nombre que se quiere	|Imap4
Protocol	:	Protocolo usado	|IMAP4
Port	:	Puerto usado	|143
Domain Name	:	Nombre del dominio	|anew.com.ve

Creación de Usuarios.

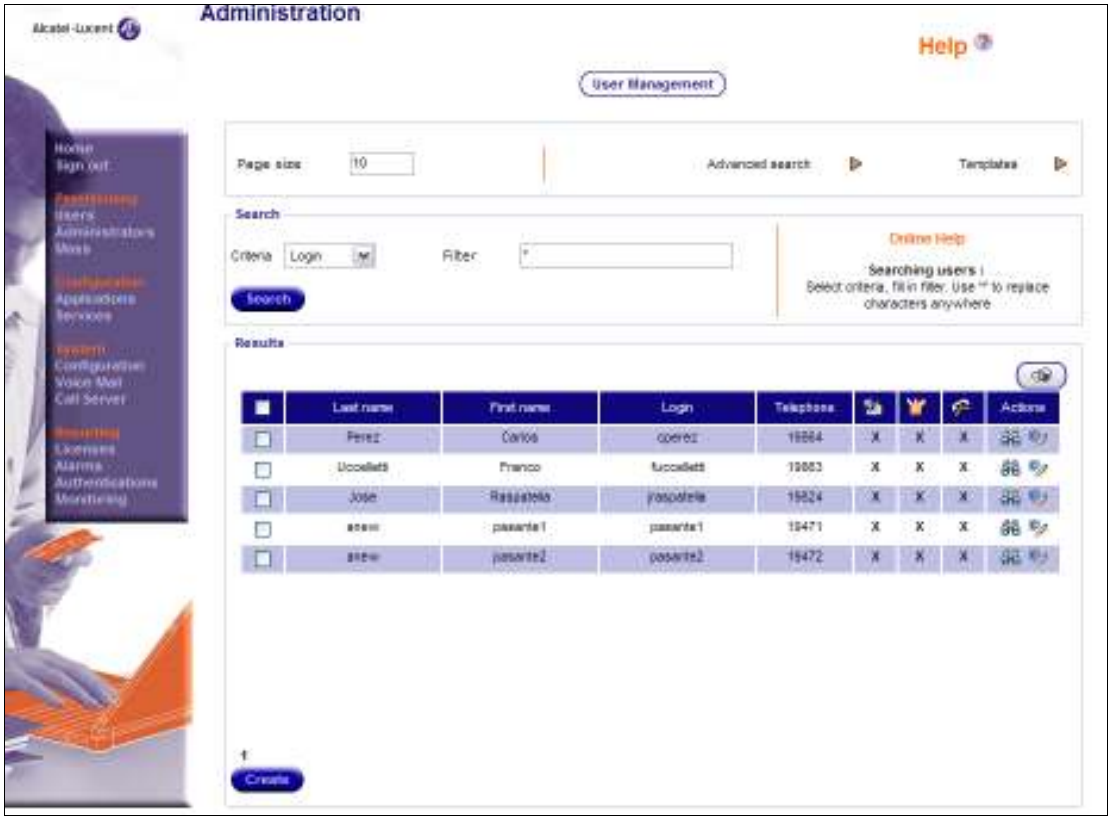


Figura 23 Creación de usuarios

El menú Provisioning / Users es donde se registran lo usuarios. Para cada uno de ellos ingresó la siguiente información:

Saludo /Nombre /Apellido / Login Externo / Lenguaje / Departamento / Reglas de Marcado / Id de Presencia / Password / Telefono de Oficina / Fax / Teléfono Móvil / Pager / E-mail / Servicios Disponibles

Los datos fueron exportados desde el Directorio Activo y completados con información suministrada por los usuarios.

3.2.10.- Políticas de enrutamiento según los diferentes perfiles.

Dentro de Anew e-B se pueden definir 3 perfiles básicos de usuario:

- Vendedores y ejecutivos con alta movilidad: Este grupo de usuarios pasa la mayor parte del día fuera de la oficina. Durante sus actividades diarias asisten a reuniones con clientes donde se discuten oportunidades de negocios. Supervisan la operación de la compañía en el exterior. No realizan ningún tipo de guardias.
- Arquitectos de soluciones y personal de soporte: Son la fuerza laboral técnica de la compañía. Instalan y dan servicio a las diferentes soluciones del portafolio de Anew. Realizan guardias de dos semanas de duración con rotación de dos semanas, durante las están a completa disposición del cliente, las 24 horas del día.
- Personal regular: Este grupo esta conformado por el resto del personal, staff administrativo, secretarias, welcome center. Normalmente no salen de las premisas de la oficina, y tienen un horario fijo de 8:30 AM a 5:00 PM.

Con el módulo My Assistant se pueden configurar las políticas de enrutamiento para las llamadas recibidas por cada usuario. Así las llamadas pueden ser desviadas a distintos números de teléfono predefinidos (de oficina, del domicilio particular, un celular, el buzón de voz o cualquier otro). Los criterios para definir estos eventos se basan en número del llamante, tipo de llamada entrante, día de la semana y hora del día.

De esta forma, se definen ciertas reglas para cada tipo de usuario, que pueden ser activadas o desactivadas en cualquier momento. Para cada usuario se definieron 6 grupos de números telefónicos, Números Personales, Clientes regulares, Clientes VIP, Emergencias, Oficina, Oficina Guardia.

Vendedores y ejecutivos con alta movilidad	
Nombre de la regla	Descripción

Reunión[§]	Todas las llamadas, con la excepción de emergencias, son desviadas al buzón de voz.
Personales	Si se reciben llamadas pertenecientes al grupo de números personales en el teléfono de oficina y no son atendidas, se envían al teléfono móvil del usuario durante el horario de oficina.
Clientes VIP	Si se reciben llamadas pertenecientes al grupo de clientes VIP en el teléfono de oficina y no son atendidas, se envían al teléfono móvil del usuario en cualquier horario de lunes a viernes.
Cliente Regulares	Si se reciben llamadas pertenecientes al grupo de clientes regulares en el teléfono de oficina y no son atendidas, se envían al teléfono móvil del usuario en horario de oficina.

Arquitectos de soluciones y personal de soporte	
Nombre de la regla	Descripción
Reunión	Todas las llamadas, con la excepción de emergencias, son desviadas al buzón de voz.
Personales	Si se reciben llamadas pertenecientes al grupo de números personales en el teléfono de oficina y no son atendidas, se envían al teléfono móvil del usuario durante el horario de oficina.
En cliente	Si se reciben llamadas pertenecientes a los grupos de oficina, clientes regulares, clientes VIP, emergencias y oficina y no son atendidas se envían al teléfono móvil durante el horario de oficina
Guardia	Si durante el período de guardia se reciben llamadas al

[§] Reunión esta desactivada por defecto, sólo se debe activar ante actividades programadas

	teléfono de oficina del grupo oficina u oficina guardia y no son atendidas son enviadas al teléfono móvil de guardias, en cualquier horario, cualquier día de este período.

Personal Regular	
Nombre de la regla	Descripción
Reunión	Todas las llamadas, con la excepción de emergencias, son desviadas al buzón de voz.
Regla general	Cualquier llamada no atendida ira al buzón de voz del usuario

Tabla 8 Enrutamiento Personal Anew

3.2.11.- Período de pruebas y elaboración de manuales.

Previo al inicio del período de pruebas se dictó una inducción del sistema en las oficinas. Se mostró paso a paso la configuración de un nuevo usuario, y se explicó como ingresar al sistema por primera vez. También se suministró material impreso con instrucciones de uso; este material se fue refinando durante las siguientes semanas basándose en las sugerencias del personal de Anew. Algunos fragmentos muy técnicos del documento fueron removidos ya que ocasionaban cierta confusión en algunos usuarios. Estos documentos describen brevemente como instalar el cliente para establecer una VPN hacia la compañía y como acceder al sistema de comunicaciones unificadas.

Finalmente al cabo de dos semanas de pruebas, se entregó la administración del sistema al departamento de Soporte de la compañía junto con un cd que contiene tanto la documentación definitiva para los usuarios como las utilidades necesarias para establecer una VPN y acceder remotamente al sistema. Esta documentación se encuentra en los anexos. Cabe destacar que por solicitud del departamento técnico se formó un laboratorio donde en un servidor de pruebas se instaló la aplicación desde

cero, para familiarizarse con este proceso. Este laboratorio no contaba con el licenciamiento necesario para operar pero cumplía su propósito, ya que en los planes de la compañía se encuentra el ofrecer este producto a nuevos clientes. No se redactó documentación adicional para esta etapa.

3.2.12.- Análisis técnico económico, comparación con otras soluciones.

Según reportes de Gartner, una firma de investigación y consultoría americana, el liderazgo durante el año 2007 en soluciones de comunicaciones unificadas es llevado por las siguientes empresas [9]:

- Microsoft, con Microsoft Communications Server 2007.
- Cisco, con Cisco Unified Communications Release 6.0.
- Nortel, con Nortel Unified Communications Services.
- IBM, con IBM UC^2.
- Alcatel , Omnitouch Unified Communications.
- Avaya, Avaya Unified Communications.

Las comunicaciones unificadas aún están en sus inicios. Se conocen los conceptos que conlleva, pero cada fabricante y desarrollador ofrece su interpretación de estos, esperando que su visión cale en el mercado. Es por esto que en diferentes soluciones, módulos de nombres similares o que anuncien las mismas características difieren enormemente. Cada una de estas aproximaciones a las comunicaciones unficadas tiene sus fortalezas y desventajas. Soluciones como las de Microsoft formadas por un amplio grupo de aplicaciones bien conocidas y con la capacidad de integrarse con cualquier tipo de PBX, hacen que su uso sea fácil e intuitivo para usuarios y administradores de productos Microsoft; soluciones como la de Cisco tienen un rendimiento ya probado en ciertas áreas como las conferencias Web con su solución Webex.

A pesar de esto, no hay un mejor modelo, sino uno más conveniente, ninguna solución ofrece todo lo que una empresa podría necesitar para comunicarse. Las compañías deben tomar decisiones evaluando las opciones emergentes y basándose en sus necesidades actuales y a largo plazo.

Para el análisis se escogieron las dos soluciones de comunicaciones unificadas más populares, la de Microsoft llamada Office Communications Server 2007, y la de Cisco, Unified Communications Release 6. Las ventajas, características y desventajas de ambas serán comparadas contra la solución de Alcatel, Omnitouch Unified Communications. Para evaluarlas se tomó en cuenta información disponible en Internet donde se muestran sus características y también se logró usar y experimentar algunos de sus módulos

Microsoft Office Communications Server 2007

Microsoft OCS 2007 es una suite de paquetes conocidos de Microsoft con nuevas funcionalidades. Ms OCS ofrece unir los servicios clásicos de una compañía, sistemas telefónicos de escritorio, Internet, faxes, sistemas IP-PBX y PBX convencionales, correo de voz, mensajería instantánea, dispositivos móviles (Windows Mobile). La solución completa de Ms OCS 2007 se comprende de los siguientes módulos y aplicaciones:

- Microsoft Office Server 2007.
- Microsoft Exchange Hosted Services.
- Microsoft Office Outlook 2007.
- Microsoft Office Comunicator 2007.
- Microsoft Exchange Server 2007.
- Microsoft Office Live Meeting service 2007.

La suite de Microsoft ofrece compatibilidad con soluciones de los siguientes fabricantes:

- Alcatel OmniPCX R.9
- Avaya Communication Manager 4.x
- Cisco Unified Communications
- Ericsson MX-1
- Mitel 3300 v8
- NEC Univerge SV7000
- Nortel CS1000 v5
- Siemens HiPath 8000 v8.1

Microsoft ofrece un plan de evaluación de 3 meses de su solución disponible a través de su sitio de Internet. Si bien se tomó parte en este proceso, no fue del todo exitoso ya que se carecía de muchos de los servidores necesarios para su instalación, y se realizó todo en un mismo equipo a través del uso de máquinas virtuales. Los módulos que se pudieron ejecutar de manera adecuada mostraron lo que se esperaba, una integración uniforme y eficiente que hace muy natural la experiencia al usuario.

Cisco Unified Communications Release 6.0.

La oferta de Cisco ofrece la integración de soluciones tales como: mensajería, conferencias de voz, de video y web, y de clientes de comunicaciones unificadas. Ofrece integración con directorios activos, presencia, información preferencial (determina quien tiene acceso a que información personal) y se integra con herramientas de negocios comunes. Esta compuesta de los siguientes módulos:

- Cisco Unified Personal Communicator: ofrece voz, video, mensajería instantánea, conferencias, información de presencia a través de una sola aplicación compatible con PCs y Macs.

- Cisco Unified CallConnector: herramienta para falicilitar y simplificar la colaboración en Microsoft Office.
- Cisco IP Communicator: Le da a un PC las funciones de un teléfono IP, ofreciendo llamadas de alta calidad en el camino, o desde cualquier punto que los usuarios puedan acceder a la red corporativa.
- Cisco Unified MeetingPlace: solución de conferencias de voz de video y web para organizaciones grandes y medianas.
- Cisco Unity Connection: provee opciones para voz o mensajería integrada.
- Cisco Unified Video Advantage: permite a los usuarios de teléfonos IP Cisco, hacer y recibir video llamadas con los componentes de video mostrados en un PC.

Cisco tiene una política mucho más restrictiva con respecto a las demostraciones, y son también muy celosos con el tema de costos. En las numerosas sesiones que se mantuvieron con servicio técnico de Alcatel-Lucent muchas veces se usaron herramientas del módulo Cisco Unified Meeting Place, y resulto ser una herramienta muy completa y bastante confiable.

Basandose en las características de cada solución se puede construir la siguiente tabla:

	Alcatel	**Microsoft**	**Cisco**
VoIP	Completa	Completa	Completa
Mensajería unificada	No incluye Fax	Completa	Completa
Asistente Personal	Si	No	No
Integración con PBX	Solo con Alcatel OXE	Varios fabricantes	Opciones limitadas

Presencia	Si	Si	Si
Conferencias	Web/Audio	Video/Web/Audio	Video/Web/Audio
Integración con herramientas de negocios	Si	Si	Si
Opciones para diferentes tipos de empresas	Muy limitadas	Diversos paquetes	Diversos paquetes
Costo aproximado (100 usuarios) US$	9.000-12.000	3.800 – 17.900	6.300 – 28.000

Tabla 9 Características de diferentes soluciones de UC

Cada solución tiene atributos que la hacen destacar en un campo. Cisco es quien más opciones de videoconferencias ofrece y da soporte a plataformas tanto de Windows como de Apple. Su servicio de conferencias Webex es usado hasta por el personal de soporte de Alcatel. Microsoft se destaca en integrar todos los servicios y productos de manejo de redes que ellos mismos ofrecen, directorio activo, correo Exchange, Microsoft Office y también proporciona múltiples opciones de licencias. Ambas compañías, Microsoft y Cisco, se caracterizan por ofrecer actualizaciones constantes a sus productos que aumentan la seguridad y el desempeño de las aplicaciones. Alcatel se destaca con su servicio de asistente personal embebido en el módulo My Assistant que permite enrutar llamadas de múltiples maneras y ofrece una integración a nivel de software tan buena como la de Microsoft.

En definitiva, Microsoft y Cisco respectivamente llevan la delantera en esta primera generación de soluciones de comunicaciones unificadas. Ofrecen productos más económicos y con más características. Vale mencionar que la próxima versión de comunicaciones unificadas de Alcatel, promete solventar muchos de estos problemas, y con la experiencia ganada en el campo puede ofrecer una opción realmente

competitiva.

CAPÍTULO IV

CONCLUSIONES

La solución de comunicaciones unificadas de Alcatel no es una solución del todo completa. Una de sus mayores desventajas es que sólo se integra con PBX Alcatel empresariales, lo que disminuye considerablemente el grupo de empresas dispuestas a adoptar esta solución. El costo de una central telefónica OXE sencilla para febrero de 2008 oscilaba entre los 330.000 BsF., y para una empresa que ya cuenta con una PBX de otro fabricante una inversión de este tipo no tiene sentido. Es así que al buscar una implementación de este tipo recurren a aquellas compatibles con la plataforma en la que han invertido. Otro punto débil son las video conferencias y la mensajería unificada de faxes, que solo pueden establecerse con soluciones de terceros no incluidas en la solución.

Si bien este modelo no es favorable para todas las compañías, aquellas que ya cuentan con una central OXE encontrarán una amplia gama de nuevas funciones y facilidades para sus empleados por un costo relativamente bajo. El sistema muestra una interfaz gráfica amigable e intuitiva, con todas las opciones fácilmente accesibles. Todas las herramientas tienen una forma web, accesible a través de cualquier navegador de Internet, y otra forma más robusta, a través de las aplicaciones incluidas. El mantenimiento para el administrador es mínimo, mostró una excelente estabilidad dentro de Anew, y según pruebas realizadas por la empresa Miercom, una consultora especializada en telecomunicaciones, el sistema puede soportar y mantener

un excelente tiempo de respuesta en configuraciones con hasta 10.000 llamadas de voz, e-mails y faxes.

El retardo humano es un factor crítico en los negocios. La posibilidad de oír e-mails por teléfono en cualquier dispositivo móvil desde un aeropuerto, o bien recibir a través de correo electrónico mensajes de voz dejados en la contestadora del teléfono de oficina le da un nuevo sentido a la movilidad y reduce esa latencia considerablemente. Solo queda de parte de las empresas buscar la solución que mejor se adapte a sus necesidades y enseñar a sus empleados a sacar el máximo provecho de estas herramientas.

En líneas generales, las herramientas que ofrecen las comunicaciones unificadas probarán ser muy valiosas en los modelos laborales que impliquen alta movilidad. La solución que ofrece Alcatel es una excelente muestra de lo que estas pueden hacer y de cómo la integración de diferentes servicios conocidos, ya sea telefonía, mensajería, correo, les da una nueva dimensión en el ámbito laboral; pero solo será una inversión sensata para empresas que cuenten con centrales telefónicas Alcatel empresariales o esté en sus planes adoptar una.

RECOMENDACIONES

- Solicitar una dirección pública estática para el enlace de CANTV. Las direcciones estáticas con que se cuenta son las del enlace Frame Relay, pero resultó ser muy inestable y no se recomienda usarlo. En las pruebas de acceso efectuadas mostró problemas de manera regular. A su vez, de usar sólo el enlace CANTV, se recomienda adquirir más ancho de banda según vayan aumentando los usuarios.

- Instalar un router especializado para el manejo de la red de la oficina. Actualmente es el firewall quien se encarga de esta función, y no ofrece todas las funciones que un router proporcionaría. Además la carga de recursos que conlleva usarlos de esta manera entorpece la red.

- Activar en el firewall la protección antivirus, actualmente sin licencias y por lo tanto desactivada, y establecer una política más severa en lo que atañe a servicios permitidos. Cuando se realizó la auditoría de red se hicieron pruebas de los paquetes que circulaban por ésta, y cerca de 12 PCs mostraban tráfico Peer to Peer constante, con hasta 20 diferentes conexiones cada una. Este tipo de servicios, usan todos los recursos de red que consiguen disponible, y en una empresa de telecomunicaciones el ancho de banda es un recurso vital que no puede ser desperdiciado.

- Instalar un servidor de correos propio. Además de las ventajas ya mencionadas en el trabajo, el sistema de correos de 1 and 1 usado actualmente es muy lento, hasta 4 veces mas lento que servicios ofrecidos de manera gratuita por proveedores como Google (Gmail) o Microsoft (Hotmail) según observaciones hechas dentro de las oficinas de Anew.

- Ubicar los servidores de que aún se encuentran en la VLAN Datos en la VLAN segura. El servidor de Directorio Activo y dos servidores de archivos aún no han sido cambiados de VLAN debido a los cambios que implicaría en la configuración de ciertas aplicaciones, pero no se sugiere tener a estos en el mismo segmento que las estaciones de trabajo de Anew.

- Agregar a los planes de entrenamiento para nuevos empleados de la empresa un módulo donde se expongan las herramientas que ofrece el sistema de comunicaciones unificadas y cómo sacar el mejor provecho de ellas.

- Realizar pruebas de Mean Opinion Score con un número significativo de personas dentro de la oficina para determinar los valores reales de calidad de voz que ofrece el sistema.

REFERENCIAS BIBLIOGRÁFICAS

[1] Huidoro, Jose. Rolán, David. Integración de voz y datos, Primera Edición. España 2003.

[2] Alcatel. Alcatel OmniPCX Enterprise Overview description. Alcatel, Francia, 2006.

[3] Alcatel. Alcatel OmniTouch Unified Communication Overview description. Alcatel, Francia, 2006.

[4] Alcatel-Lucent. Alcatel-Lucent OmniTouch Unified Communications Application Suite IP Services and Port Numbers. Alcatel-Lucent, Estados Unidos de Norte América, 2007.

[5] Portal de Business Partner Alcatel-Lucent. (www.alcatelbusinesspartner.com)

[6] Alcatel. Alcatel OmniTouch Unified Communication Participant's Guide Install Expert. Alcatel University, Francia, 2006

[7] UIT – T G.1010 (11/2001). Sistemas y medios de transmisión, sistemas y redes digitales. – Sector Normalización

[8] Alcatel. Alcatel OmniPCX Enterprise Installation Manuals. Alcatel, Francia, 2006

[9] Gartner. Magic Quadrant for Unified Communications. Gartner, Estados Unidos de Norte América, 2007.

BIBLIOGRAFÍA

- Huidrobo, José M. Integración de voz y datos, primera edición. España: McGraw-Hill, 2001.

- Forouzan, Behrouz A. Transmisión de datos y redes de comunicaciones, segunda edición. España: McGraw-Hill, 2001.

- Tomasi, Wayne. Advanced Electronic Communications Systems, tercera edición. Estados Unidos de Norte América: Prentice Hall, 1994.

- Khalid, Mohamed. Wainner, Scott. IPSec VPN Design. Estados Unidos de Norte América, Editoral: Cisco Press, 2005.

- Noonan, Wes. Dubrawsky, Ido. Firewall Fundamentals. Estados Unidos de Norte América, Editoral: Cisco Press, 2006.

- Kotelly, Blade. The Art and Business of Speech Recognition: Creating the Noble Voice. Estados Unidos de Norte América, Editorial: Addison Wesley, 2003.

- SIP Demystified. <www.digitalengineeringlibrary.com>

- Alcatel. Alcatel OmniTouch Unified Communication Overview description. Alcatel, Francia, 2006.

- Alcatel. Alcatel OmniPCX Enterprise Overview description. Alcatel, Francia, 2006.

- Alcatel. Alcatel OmniTouch Unified Communication Participant's Guide Install Expert. Alcatel University, Francia, 2006.

- Alcatel-Lucent. Alcatel-Lucent OmniTouch Unified Communications Application Suite IP Services and Port Numbers. Alcatel-Lucent, Estados Unidos de Norte América, 2007.

- Nortel Position Paper. Business Optimized Communications: Nortel's unified communications strategy for enterprise transformation. Nortel, Estados Unidos de Norte América, 2007.

- Miercom. TeckDrive Brief Alcatel-Lucent My Instant Communicator. Miercom, Estados Unidos de Norte América, 2008.

- Miercom. Lab Testing Summary Report: Cisco Unified Communications system Release 6.0. Miercom, Estados Unidos de Norte América, 2007.

- Gartner. Magic Quadrant for Unified Communications. Gartner, Estados Unidos de Norte América, 2007.

- UIT – T G.1010 (11/2001). Sistemas y medios de transmisión, sistemas y redes digitales. – Sector Normalización.

- Enciclopedia virtual de consulta. (http://www.wikipedia.com)

- Productos de comunicaciones unificadas:
  http://office.microsoft.com/en-us/communicationsserver/FX102406241033.aspx
  http://www-306.ibm.com/software/lotus/unified-communications/
  www.microsoft.com/uc/default.mspx

www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns152/networking_solutions_package.html

GLOSARIO

Ancho de banda La cantidad de datos o tráfico que pueden ser transmitidos en una determinada cantidad de tiempo. Para sistemas digitales el ancho de banda generalmente es expresado de bits por segundo (bps).

Backbone Conexión de alta velocidad dentro de una red que conecta a otros circuitos.

Cabecera Porción de un paquete, precediendo los datos, que contiene las direcciones fuente y destino y campos de detección de errores.

DNS Abreviatura Domain Name Service. Asocia un nombre con una dirección IP específica. Esto resulta ser muy útil en el Internet ya que facilita la navegación gracias al uso renombres en las direcciones.

Ethernet Esquema de red de 10 ó 100 Mbps. desarrollado originalmente por Xerox Corporation. Está muy extendida en redes de área local, ya que está disponible para muchos tipos de ordenadores, no precisa de licencias y existen componentes para soportarla de diversos fabricantes

Firewall En construcciones un firewall es una pared contruída de materiales resistentes al calor o al fuego como el concreto, cuyo propósito es el de detener o entorpecer la propagación del fuego en un edificio. De la misma manera, un firewall dentro de una red cumple el propósito de evitar que el tráfico no autorizado vaya de una red a otra. La aplicación más común de un firewall es vigilar entre una red confiable y una no confiable, típicamente el Internet.

Frame Relay Es una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

FTP Abreviatura File Transfer Protocol. Es un servicio confiable

	orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten FTP. El propósito principal de FTP es transferir archivos desde un computador hacia otro copiando y moviendo archivos desde los servidores hacia los clientes
Full-Dúplex	Ambas estaciones pueden enviar y recibir información al mismo tiempo.
Gateway	Puerta de Interconexión. Permite la conexión de redes con diferentes interfaces y protocolos.
IP	Abreviatura Protocolo de Internet. Es el mecanismo de transmisión utilizado por los protocolos TCP7IP, esta basado en datagramas sin conexión y no fiable, ofrece un servicio de mejor entrega posible.
LAN	Abreviatura Local Area Network. Es una red de área local, generalmente opera dentro de un área muy reducida, suele conectar enlaces de una única oficina, edificio o campus. Dependiendo de las necesidades de la organización.
Presencia	Es un sistema usado para determinar la disponibilidad de una persona a ser contactada. No se relaciona con la ubicación de este usuario. En la telefonía tradicional la presencia puede ser determinada hasta cierto grado basándose en el estatus del auricular remoto. Si no se atiende el teléfono luego de ciertos repiques probablemente el destinatario no se encuentra. Un tono ocupado indica que el destinatario esta presente pero no disponible. Dentro de una empresa la presencia también puede envolver el cargo de la persona dentro de la misma, su localización física y organizacional y una amplia gama de información personal.
Router	Conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.
Semidúplex	Cada estación puede tanto enviar como recibir, pero no al mismo tiempo.
Símplex	Es un modo de transmisión donde la comunicación es unidireccional, solamente una de las dos estaciones puede transmitir y la otra solo recibe.

Switch	Es un dispositivo electrónico de interconexión de que opera en la capa 2.Un conmutador interconecta dos o más segmentos de red, permitiendo el tráfico de datos de un segmento a otro, de acuerdo a la dirección MAC de los equipos.
SSL	SSL es la tecnología de seguridad estándar para establecer vínculos encriptados entre un servidor web y un navegador. Este vinculo garantiza que toda la data que circula entre el servidor web y el navegador se mantiene privada y sin alterar. El estándar SSL es usado por millones de websites para proteger las transacciones en línea de sus clientes
TTS, Síntesis de la voz	La síntesis de la voz consiste en la generación automática de una secuencia de habla idéntica a la que pronunciaría una persona al leer el texto correspondiente a dicha secuencia. En este sentido, cabe destacar que debe tratarse de un proceso totalmente automático, cuyo objetivo sea la emulación lo más ajustada posible del modo de leer del ser humano, aceptando como entrada un texto arbitrario.
TCP	Abreviatura Transmission Control Protocol. Es un protocolo de Capa 4 orientado a conexión que suministra una transmisión de datos full-duplex confiable. Forma parte del TCP/IP.
TELNET	Abreviatura Terminal Network. Es un programa de aplicación cliente-servidor que permite el establecimiento de una conexión con un sistema remoto de forma que el Terminal local aparece como un Terminal del sistema remoto.
UDP	Abreviatura User Datagram Protocol. Es un protocolo de transporte no orientado a conexión de la pila de protocolo TCP/IP. El UDP es un protocolo simple que intercambia datagramas sin acuse de recibo ni garantía de entrega.
UTP	Cable de par trenzado, es el tipo más frecuente de medio de comunicación que se usa en redes, su frecuencia de operación es desde 100Hhz hasta 5MHz. Están conformados por pares trenzados generalmente de cobre y de acuerdo al número de pares de establecen categorías.
VoIP:	Abreviatura Voice over Internet Protocol. Es un protocolo que hace posible que la señal de voz viaje a través de Internet

y redes IP.

VxML VoiceXML es el formato XML estándar para definir diálogos de voz interactivos entre un humano y una computadora. Esta diseñado para crear diálogos de audio que ofrecen habla sintetizada, audio digitalizado, reconocimiento de voz y de marcación por tonos, grabación de la conversación y telefonía. Su objetivo principal es llevar las ventajas del desarrollo web y entrega de contenido a aplicaciones de respuesta de voz interactivo

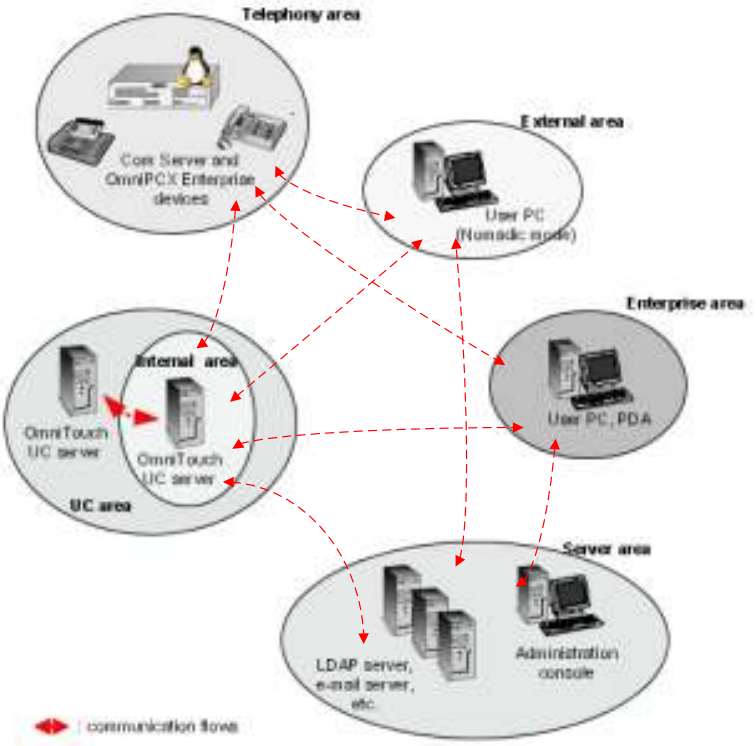
WAN Abreviatura Wide Area Network. Conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias a través de la interconexión de LAN´s.

ANEXOS

SERVICIOS PUERTOS Y PROTOCOLOS USADOS POR EL SISTEMA ALCATEL OTUC

Los servicios ejecutándose en el servidor de UC dependerán de los módulos que se estén comunicando. Para los propósitos de describir el flujo entre los componentes definiremos seis áreas de comunicaciones.

- Area Interna: Se refiere a los puertos usados para los enlaces entre los procesadores del mismo servidor OmniTouch UC (topología de un solo servidor)
- Area UC: Se refiere a los puertos usados para los enlaces entre los procesos localizados en servidores OmniTouch UC separados.
- Area de Telefonía: Ser refiere a los puertos usados para los enlaces entre los servidores OmniTouch UC y la central Alcatel-Lucent OmniPCX Enterprise (Com Server, teléfonos IP, SIP Gateway, H.323 Gateway, correos de voz, etc.).
- Area de Servidor: Se refiere a los puertos usados para los enlaces entre los servidores OmniTouch UC y el servidor LDAP, servidor de correos, web server, etc.
- Area Enterprise: Se refiere a los puertos usados para los enlaces entre los servidores OmniTouch UC y los componentes dentro de la LAN , p. ej. clientes OmniTouch UC
- Area Externa: Se refiere a los puertos usados para los enlaces entre los servidores OmniTouch UC y los componentes fuera de la LAN de la compañía. Esta área esta específicamente diseñada para los clientes de OmniTouch UC en modo nomádico. Es posible ofrecer acceso externo para aplicaciones web a esta area. En este caso, el cliente usa una VPN para acceder a la LAN de la compañía.


Telephony area
Core Server and
OmniPCX Enterprise
devices
External area
User PC
(Nomadic mode)
Enterprise area
User PC, PDA
Internal area
OmniTouch
UC server
OmniTouch
UC server
UC area
Server area
LDAP server,
e-mail server,
etc.
Administration
console
communication flows

Lista de servicios Usados y Abiertos en el área External:

Servicios abiertos:

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
OTS	3595/TCP	ATAPI [1]	CTI connection for thick clients (Nomadic case)
	All	Authent	3595 for 1st instance, 3596 for 2d, etc. (configuration on WBM)
Flexlm	27000/TCP	Proprietary	Licenses
	All		Configure on WBM with config file
Flexlm	Dyn_Lnx/tcp	Proprietary	Licenses (nomadic) – daemon
	All		Dynamic negotiation on 27000 cnx or fixed on alcotuc.lic/VENDOR line

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
EVS	8016/TCP	HTTPS	Events notification (for My Instant Communicator)
	All	Authent + SSL	Configure on WBM
Apache	443/TCP	HTTPS	Accessing UC applications and Nomadic for UC clients located in External area
	All	Authent + SSL	On Application Server primary
ACS	443/TCP	HTTPS	Accessing Teamwork services (for My Instant Communicator)
	Teamwork services	Authent + SSL	

Lista de servicios Usados y Abiertos en el área Enterprise:

Servicios Abiertos:

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
OTS	3595/TCP	ATAPI [1]	CTI connection for thick clients
	All	Authent	3595 for 1st instance, 3596 for 2d, etc. (configuration on WBM)
Flexlm	27000/TCP	Proprietary	Licenses
	All		Configure via WBM and config file
Flexlm	Dyn_Lnx/tcp	Proprietary	Licenses (nomadic) – daemon
	All		Dynamic negotiation on 27000 cnx or fixed on alcotuc.lic/VENDOR line
EVS	8016/TCP	HTTPS	Events notification (for My Instant Communicator)
	All	Authent + SSL	Configure via WBM

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Apache	443/TCP	HTTPS	Accessing UC applications
	All	Authent + SSL	On Application Server primary
ACS	443/TCP	HTTPS	Accessing Teamwork services (for My Instant Communicator)
	Teamwork services	Authent + SSL	
Apache	8082/TCP	HTTP	Notification for MWI (Message Waiting Indicator) by Add-In on OmniTouch UC server
	Messaging services		

Lista de servicios Usados y Abiertos en el área Server

Servicios Abiertos**:**

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Apache	443/TCP	HTTPS	XML openness
	XML openness	Authent + SSL	On Application Server (AS) Primary
Apache	8082/TCP	HTTP	Notification by agent on mail server
	Messaging services		
Sshd	22/TCP and UDP	SSH	Maintenance, backup/restore and installation
	All	Authent + SSL	

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
CRS	3128/TCP	HTTP	Maintenance
	One Number services		Administrator connection
MS (SIP server)	8015/TCP	HTTP	Maintenance
	TUI		Administrator connection
OTS	3595/TCP	ATAPI (1)	OTS administration
	All	Authent	3595 for 1st instance, 3596 for 2d, etc. (configuration on WBM) Administrator connection
OTS	3695/TCP	HTTP	OTS maintenance
	All		3595 for 1st instance, 3596 for 2d, etc. (configuration on WBM) Administrator connection
PRS	2009/TCP	Proprietary	PRS monitoring
	IP Touch		Administrator connection

Servicios usados:

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Mail Server (plug-in)	8000/TCP	Proprietary	Mail boxes access
	Messaging services		
Mail Server (plug-in)	8001/TCP	Proprietary	Notification filter configuration
	Messaging services		
Mail Server (plug-in)	8002/TCP	Proprietary	Mail boxes access
	Messaging services		
Mail Server	25/TCP	SMTP	Mail sending
	Messaging services		
Mail Server	143/TCP	IMAP4	Mail management
	Messaging services		
3rd party application	80/TCP	HTTP/SOAP	XML notification
	XML openness		

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
LDAP server	636/TCP	LDAPS	LDAP directory access and authentication
	All	Authent + SSL	
RADIUS server	1812/UDP	RADIUS	RADIUS authentication
	Authentication	Authent + RADIUS	To configure with Config file
RADIUS server	1813/UDP	RADIUS	RADIUS authentication (not used)
	Authentication	Authent + RADIUS	To configure with Config file (not used)
Domain Controller Server	NTLM dependent	NTLM	NTLM authentication
	Authentication	Authent + NTLM	To configure with Config file

Lista de servicios Usados y Abiertos en el área Telephony:

Servicios abiertos:

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
PRS	2000/UDP	Proprietary (PRS link)	Applicative link from Alcatel-Lucent OmniPCX Enterprise CS
	IP Touch		
Apache	80/TCP	HTTP	Applicative direct link from Alcatel-Lucent OmniPCX Enterprise CS
	IP Touch		On each Application Server
MS (SIP server)	5060/TCP and UDP	SIP	Signaling for TUI access
	TUI	Authent	Configure via WBM

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
MS (RS)	12000/UDP	RTP/RTCP	Voice for TUI access
	TUI		12000 RTP - 12001 RTCP, next com: 12002 RTP - 12003 RTCP, etc.

Servicios usados:

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Alcatel-Lucent OmniPCX Enterprise CS (SIP gateway)	5060/TCP and UDP	SIP	Signaling for TUI access
	TUI + Teamwork services	Authent	Configure via WBM
Alcatel-Lucent OmniPCX Enterprise CS (eqt)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	RTP/RTCP	Voice for TUI access
	TUI + Teamwork services		
Alcatel-Lucent OmniPCX Enterprise CS (CSTA server)	2570/UDP	Proprietary (PRS link)	IP Touch application access
	IP Touch		Configure via WBM
Alcatel-Lucent OmniPCX Enterprise CS (mngt)	2555/UDP	CSTA	CTI link
	All	Authent	
Alcatel-Lucent OmniPCX Enterprise CS	2535/TCP	CMISE/CMIP	Alcatel-Lucent OmniPCX Enterprise CS management link
	All	Authent	
4635 voice mail	80/TCP	HTTP/VMMC2	Voice mail control
	Messaging services		
4635 voice mail	143/TCP	IMAP4	Voice mail management
	Messaging services	Authent	
4645 voice mail	443/TCP	HTTPS/VMMC2	Voice mail control
	Messaging services	Authent + SSL	
4645 voice mail	143/TCP	IMAP4	Voice mail management
	Messaging services	Authent	

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Alcatel-Lucent OmniPCX Enterprise CS (MTA)	25/TCP	SMTP	Mail sending
	Messaging services		

Lista de servicios Usados y Abiertos en el área UC:

Servicios Abiertos

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Apache	80/TCP	HTTP	Applicative link
	All		On each Application Server

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Apache	443/TCP	HTTPS	Applicative link from PRS
	IP Touch	Authent + SSL	Application Server Primary
Apache	8085/TCP	HTTP	Internal link for UM legacy infrastructure
	Messaging Services		On each Application Server
Apache (smartPRS)	2570/UDP	Proprietary (PRS link)	Applicative link for PDA clients
	IP Touch		Where the smartPRS is installed
PRS	2010/TCP	HTTP	Configuration notification
	IP Touch		
PRS	2011/TCP	HTTP/SOAP	Application notification
	IP Touch		
MS (SIP server)	8015/TCP	HTTP	Applicative link
	TUI		
MS (SIP server)	7999/TCP	Proprietary (US - SMCP)	Application link
	TUI		
FlexLM	27000/tcp	Proprietary	Licenses
	All		
FlexLM	Dyn_Lnx/tcp	Proprietary	Licenses (nomadic) – daemon
	All		Dynamic negotiation on 27000 cnx or fixed on alcotuc.lic/VENDOR line
FWK	9754/TCP	RMI	Application link and configuration notification
	All		Configure via WBM
IMS	9755/TCP	RMI	IMS API and configuration notification
	Messaging services		
CRS	9756/TCP	RMI	CRS API and configuration notification
	One Number services		Configure via WBM
PMS	9757/TCP	RMI	PMS API and configuration notification
	All		Configure via WBM

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
UDAS	9758/TCP	RMI	UDAS API and configuration notification
	All		Configure via WBM
MS (msaccess)	9759/TCP	RMI	Configuration notification and supervision
	TUI		Configure via WBM
EVS	9760/TCP	RMI	Configuration notification (and RMI interface for events)
	All		Configure via WBM
Tomcat (UC legacy applications)	9761/TCP	RMI	Configuration notification
	All		Configure via WBM
ECS	9762/TCP	RMI	API ECS and configuration notification
	All		Configure via WBM
Sybase	2638/TCP	Sybase	Accessing Data Base
	All		Configure via WBM
LDAP server (openLDAP)	389/TCP	LDAP	Accessing Data Base
	All		
PostgreSQL	5432/TCP	PostgreSQL	Accessing Data Base
	Messaging services		
OTS	3695/TCP	HTTP/SOAP	OTS API and configuration
	All		3595 for 1st instance, 3596 for 2d, etc. (configuration on WBM)
CRS	3999/TCP	XML	Routing
	One Number services		
ACAPI	8389/TCP	CORBA	Accessing Alcatel-Lucent OmniPCX Enterprise CS management
	All		
EVS	8014/TCP	HTTP	Dialog with Apache in proxy mode for WSP/extension connection
	Telephony Services		
Tomcat (UM legacy applications)	8007/TCP	AJPv13	Apache connection for applicative requests treatment
	All		

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Tomcat (UC applications)	10009/TCP	AJPv13	Apache connection for applicative requests treatment
	All		
DTA	5009/TCP	RMI	Accessing configuration (dialog between DTA components)
	All		
DTA	4446/TCP	XML	Alarms – XML API (for ACS and OTS components)
	All		
ACS	80/TCP	HTTP/ICS	Teamwork API
	Teamwork services		
ACS	5060/TCP	SIP	Teamwork via SIP
	Teamwork services		
EVS	16200/TCP	JMS	Events (dialog between EVS components)
	All		Configure via WBM
EVS	16100/TCP	XML	Events XML API
	All		Configure via WBM
JSA	10110/TCP	JMX	Supervision (Link for JSC)
	All		
Tomcat Admin	8009/tcp	APJv13	Apache connection for mail notification and portlet population (UM legacy)
	All		
Tomcat homepage	8005/tcp	APJv12	Apache connection in AJPv12 on Tomcat HP (UM legacy - not used anymore)

Lista de servicios Usados y Abiertos en el área Internal:

Todos los puertos listados en la lista de servicios abiertos en el área UC pueden ser abiertos en esta configuración, excepto los usados por ACS. Todos los puertos mostrados a continuación están abiertos y usados en el área Internal:

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
MS (RS)	8554/UDP	RTSP	Voice stream control
	TUI		The client is MS (rms) hosted on the same server (configuration on WBM)
Tomcat	10111/TCP	JMX	Supervision (by JSA)
	All		The client is the JSA hosted on the same server
JSC	10109/TCP	RMI	Supervision (by WBS)
	All		WBS et JSC is hosted on the same server

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
DTA	4445/UDP	RMI	Alarms – RMI API
	All		By configuration (ecc.properties), UC components send alarms on local DTA

Lista de servicios Usados y Abiertos en el área External (contra otras áreas):

Servicios Abiertos

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
4980 Softphone/ GAELIC (1)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	RTP/RTCP	Voice (Nomadic VoIP mode)
	Telephony services		To configure on Alcatel-Lucent OmniPCX Enterprise CS

Servicios Usados

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Flexlm	Dyn_Lnx/tcp	Proprietary	Licenses (nomadic) – daemon
	All		Dynamic negotiation on 27000 cnx or fixed on alcotuc.lic/VENDOR line
EVS	8016/TCP	HTTPS	Events notification (for My Instant Communicator)
	All	Authent + SSL	Configure via WBM
Apache	443/TCP	HTTPS	Accessing UC applications and Nomadic for WSP
	All	Authent + SSL	On Application Server primary
ACS	443/TCP	HTTPS	Accessing Teamwork services (for My Instant Communicator)
	Teamwork services	Authent + SSL	

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Alcatel-Lucent OmniPCX Enterprise CS (H323 gateway)	1720/TCP	H323/H225	Signaling (Specific to Nomadic VoIP mode)
	Telephony services		To configure via Alcatel-Lucent OmniPCX Enterprise CS
Alcatel-Lucent OmniPCX Enterprise CS (H323 gateway)	31000-31059/TCP	H323/H245	Signaling (Specific to Nomadic VoIP mode)
	Telephony services		To configure via Alcatel-Lucent OmniPCX Enterprise CS
Alcatel-Lucent OmniPCX Enterprise CS (eqpt)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	RTP/RTCP	Voice
	Telephony services		To configure via Alcatel-Lucent OmniPCX Enterprise CS
LDAP server	636/TCP	LDAPS	LDAP access from Alcatel-Lucent 4980 Softphone (in Nomadic VoIP mode)
	Telephony services	Authent + SSL	To configure via LDAP server and Alcatel-Lucent 4980 Softphone
OTS	3595/TCP	ATAPI (1)	CTI connection for thick clients (Nomadic VoIP mode)
	All	Authent	3595 for 1st instance, 3596 for 2d, 3597… (configuration on WBM)
Flexlm	27000/TCP	Proprietary	Licenses (Nomadic)
	All		Configure via WBM and config file

Lista de servicios Usados y Abiertos en el área Enterprise:

Servicios Abiertos

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
4980 Softphone/ GAELIC (1)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	UA	Signaling
	Telephony services		To configure on Alcatel-Lucent OmniPCX Enterprise CS
4980 Softphone/ GAELIC (1)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	RTP/RTCP	Signaling
	Telephony services		To configure on Alcatel-Lucent OmniPCX Enterprise CS

Servicios Usados

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Flexlm	Dyn_Lnx/tcp	Proprietary	Licenses (nomadic) – daemon
	All		Dynamic negotiation on 27000 cnx or fixed on alcotuc.lic/VENDOR line
EVS	8016/TCP	HTTPS	Events notification (for My Instant Communicator)
	All	Authent + SSL	Configure via WBM
Apache	443/TCP	HTTPS	Accessing UC applications
	All	Authent + SSL	On Application Server primary
ACS	443/TCP	HTTPS	Accessing Teamwork services (for My Instant Communicator)
	Teamwork services	Authent + SSL	

Service	Port	Protocol	Purpose
	Context	Authent./Encrypt.	Note
Alcatel-Lucent OmniPCX Enterprise CS (Call Handling)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	UA	Signaling
	Telephone Services		To configure via Alcatel-Lucent OmniPCX Enterprise CS
Alcatel-Lucent OmniPCX Enterprise CS (TFTP server)	69/UDP	TFTP	Alcatel-Lucent OmniPCX Enterprise CS IP parameters
	Telephone Services		To configure via Alcatel-Lucent OmniPCX Enterprise CS
Alcatel-Lucent OmniPCX Enterprise CS (eqpt)	Alcatel-Lucent OmniPCX Enterprise CS dependant/UDP	RTP/RTCP	Voice
	Telephone Services		To configure via Alcatel-Lucent OmniPCX Enterprise CS
MS (RS)	12000/UDP	RTP/RTCP (1)	Voice for TUI access
	TUI		Direct RTP - 12000 RTP - 12001 RTCP, next com: 12002 RTP - 12003 RTCP, etc.
Apache	8082/TCP	HTTP	Notification for MWI (Message Waiting Indicator) by Add-In on OmniTouch UC server
	Messaging services		
LDAP server	636/TCP	LDAPS	LDAP access from Alcatel-Lucent 4980 Softphone (directory search)
	Telephone Services	Authent + SSL	To configure via LDAP server and Alcatel-Lucent 4980 Softphone
OTS	3595/TCP	ATAPI (1)	CTI connection for thick clients
	All	Authent	3595 for 1st instance, 3596 for 2d, 3597… (configuration on WBM)
Flexlm	27000/TCP	Proprietary	Licenses
	All		Configure via WBM and config file

PROYECTO DE IMPLEMENTACIÓN DE VPN EN ANEW

1. Objetivo general de la configuración de VPN´s en Anew.

Establecimiento de VPN´s que permitan el acceso a los servidores de datos de la red interna de Anew a través de la red pública.

2. Puntos a mejorar.

- Accesibilidad: Establecer métodos mas efectivos para el acceso a unidades de almacenamiento, eliminar la necesidad de conocer rutas de red para obtener la información.
- Acceso Remoto: En los momentos no se dispone de métodos de acceso remoto a los servidores internos de la empresa y a la información contenida en estos. Permitir el acceso remoto a esta información va a permitir a los usuarios realizar algunas funciones desde sus hogares por ejemplo revisando y actualizando ofertas sin necesidad de hacer presencia en las instalaciones de la empresa. También es una oferta atractiva en caso de una emergencia en la que no seria posible el traslado físico.

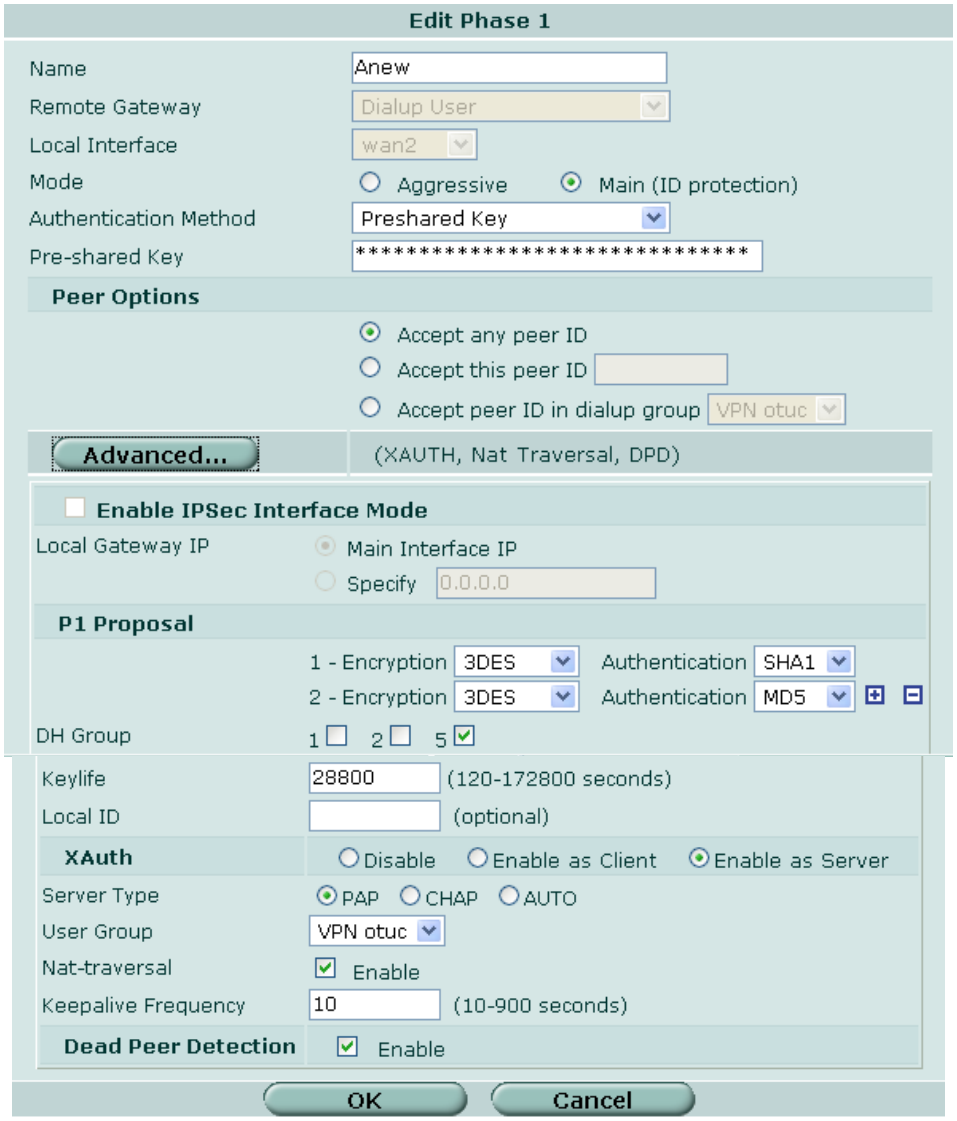
3. Configuración de la VPN.

Bueno, lo primero de todo, para configurar el firewall que establezca VPN's, nos logeamos en él, vamos en el menú de la izquierda a "VPN" > "IPSEC" y tenemos que crear la primera fase desde "Create Phase 1".

Tenemos que configurar todas las siguientes opciones:
"Name": le "Anew".
"Remote Gateway": El tipo de conexión que tendremos de entrada, en mi caso para conectarnos desde cualquier PC con el FortiClient es "Dialup User".
"Local interface": A que interfaz le entrarán las conexiones, lo normal WAN1 o WAN2, en mi caso "WAN1".
"Mode": "Main"
"Authentication Method": La opción que se eligió fué ponerle una contraseña común para que se conecten por VPN, con "Preshared Key"
"Preshared Key": Introducimos el password que interese, en este caso es "**merlin**".
"Peer options": Indicamos que acepte todos > "Accept any peer ID".
- Pinchamos en el botón "Advanced..." para ver más opciones de la conexión.
Tenemos dos opciones de conexión segura, elegimos las más seguras, ahora sólo queda que los clientes sean compatibles, la primera será "Encryption": "3DES" y **"Authentication":** "SHA1" y si esta conexión no fuera posible, la siguiente será:
"Encryption": "3DES" y "Authentication": "MD5".
"DH Group": Marcamos únicamente "5".
"Keylife": Por defecto 28800.
"XAuth": La habilitaremos pero como servidor, "Enable as server".
"Server type": PAP.
"User Group": Seleccionamos el grupo de usuarios que pueden conectarse a

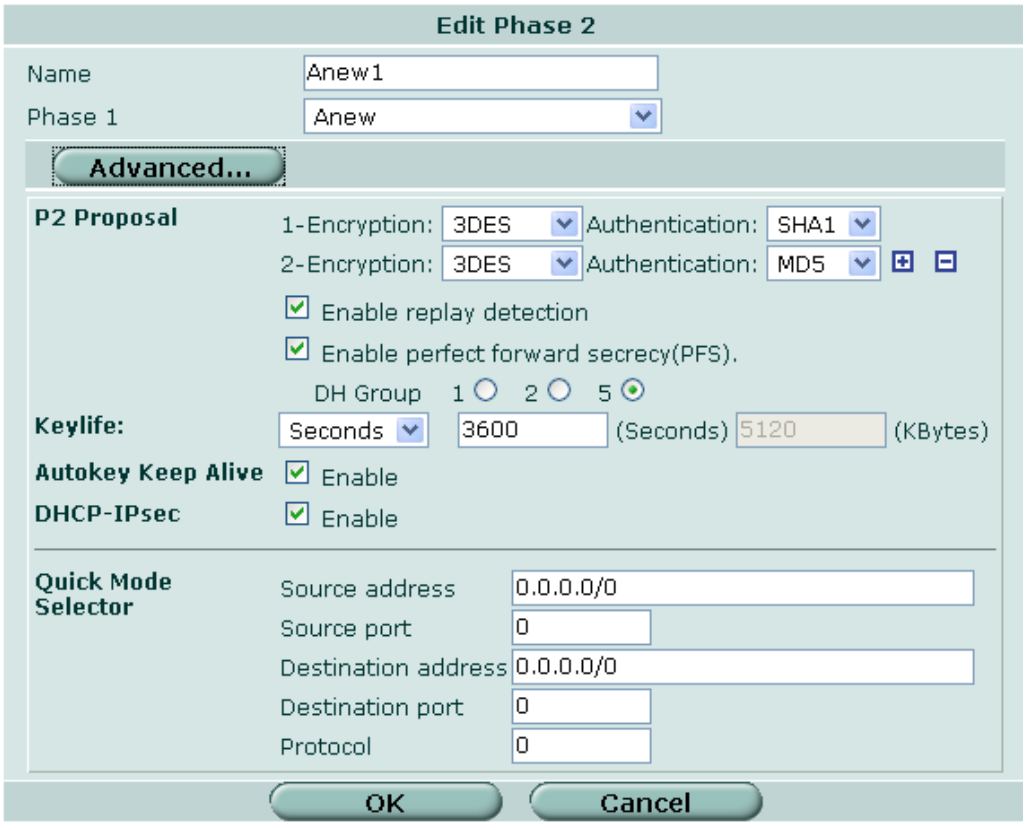
esta VPN, así que todos los usuarios que nos interesen que se conecten los debemos de meter en este grupo (y si no existe, lo creamos y metemos a unos usuarios de prueba).
"Nat Trasversal": La habilitamos "Enable".
"Keepalive Frecuency": 10 que es el valor que viene predeterminado.
"Dead Peer Detection": También habilitado, "Enable".

Una vez que tenemos así los valores aceptamos, damos a "OK".



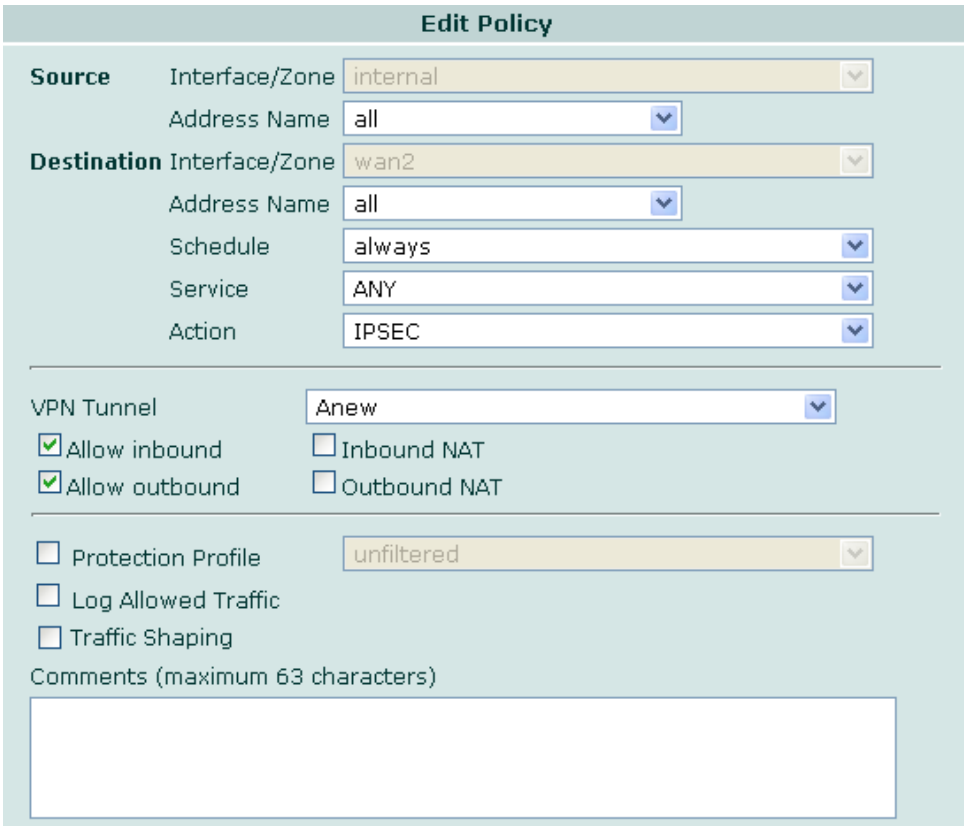
Ahora falta crear la otra fase, pulsamos sobre "Create Phase 2".

Rellenamos la misma información que hemos metido para la primera fase:
"Name": El nombre que querramos, en este caso para ser como el anterior, le pongo "Anew1".
"Phase 1": Selecciono la que he creado antes, "Anew".
- Pulsamos sobre "Advanced..."
Ponemos la misma encriptación que en la primera fase.
Y habilitamos PFS "Enable perfect forward secrecy" y el de "Enable replay detection".
"DH Group" lo dejamos sólo con "5"
En "Keylife" le dejamos el tiempo que viene predeterminado.
"Autokey Keep Alive" lo habilitamos.
"DHCP-IPsec" también para usar un servidor DHCP de la red.
Damos a "OK".

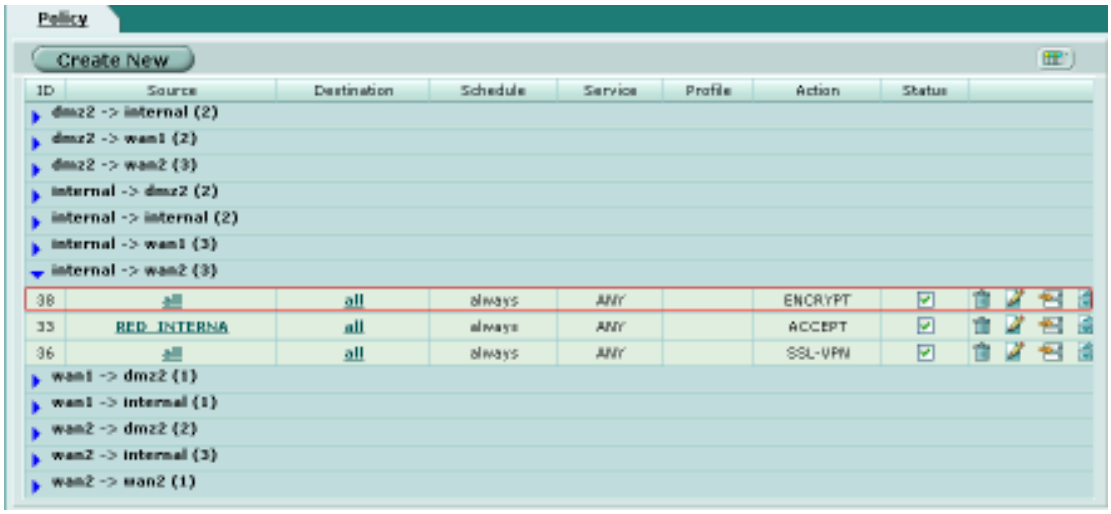


Ahora debemos crear una regla para permitir estas conexiones VPN de Internet a nuestra LAN. Para ello, vamos a "Firewall" > "Policy" > Y pulsamos sobre "Create New".

En **"Source"** tenemos que poner a donde queremos que vaya la encriptación de la VPN, o sea **el destino** en este caso sería "internal".
"**Address Name**: all"
En **"Destination"** desde donde vendrá la conexión, en este caso viene por la "wan2" debido a que en esta interfaz se cuenta con una dirección IP estática..
"**Address Name**: all"
Siempre queremos que esté operativo: "Schedule: always".
Que funcionen todos los protocolos, que pase todo el tráfico por la VPN, así que en "**Service**" indicamos "ANY".
Y la diferencia es que en "**Action**" tenemos que poner "IPSEC" para que se cree un tunel seguro.
En "**VPN Tunnel**" indicamos cual es nuestra primera fase, en mi caso era "Anew" y marcamos los dos checks de "Allow inbound" y "Allow outbound" para que haya trafico tanto entrante como saliente por la VPN, osea, que el que se conecte pueda acceder a recursos de la red y se pueda acceder a él.
Damos a "OK".

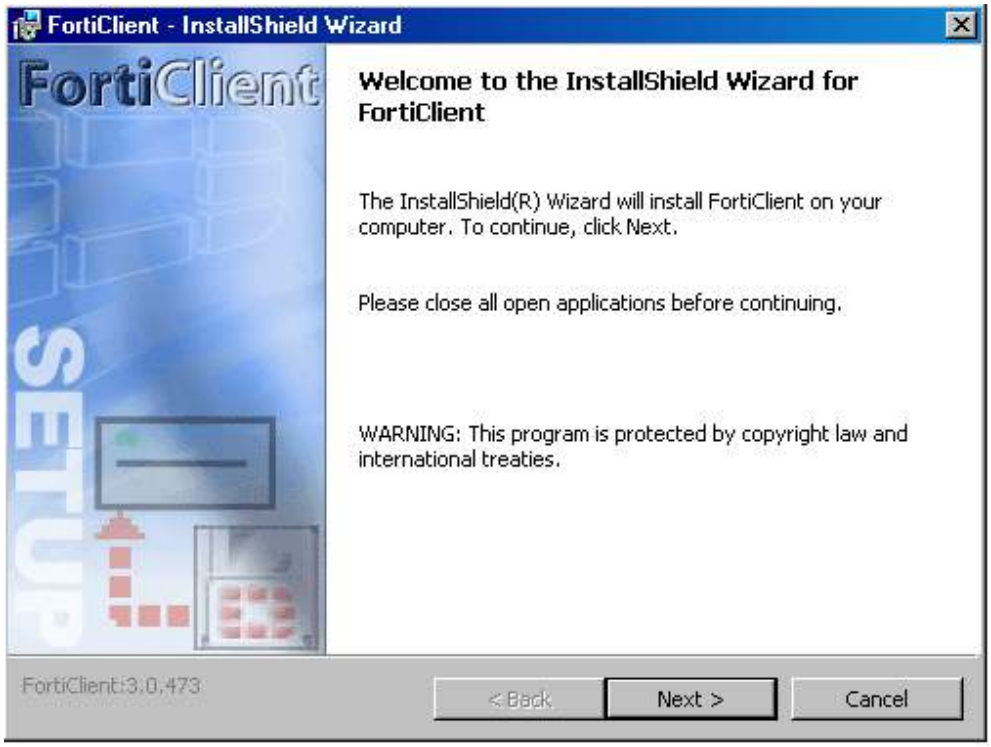


Comprobamos que está en las reglas de "internal -> wan1" y en "Action" pone "ENCRYPT".

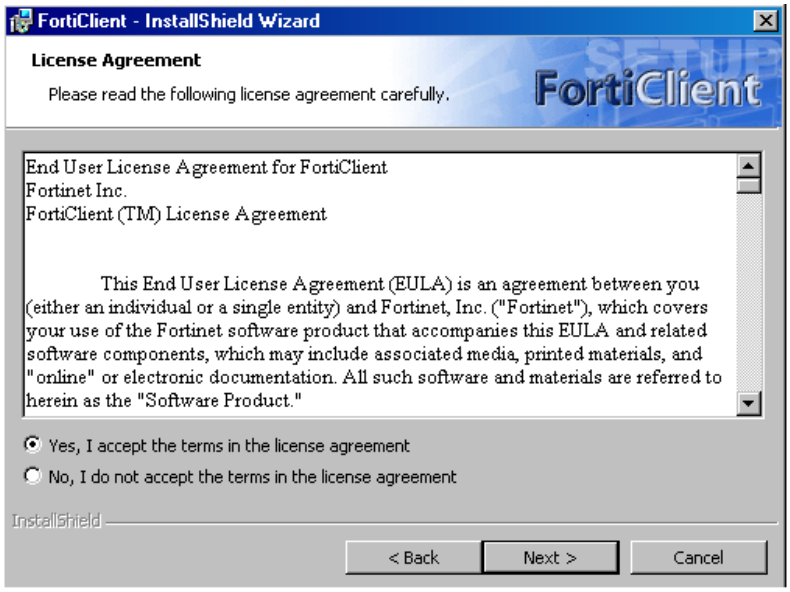


No se configuró un servidor DCHP para éste túnel.

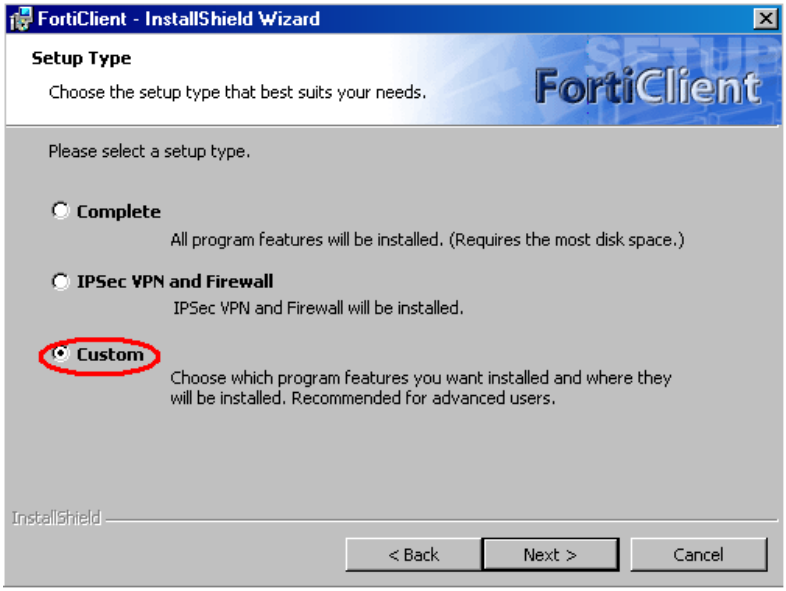
4. Instalación del Cliente VPN "FortiClient".



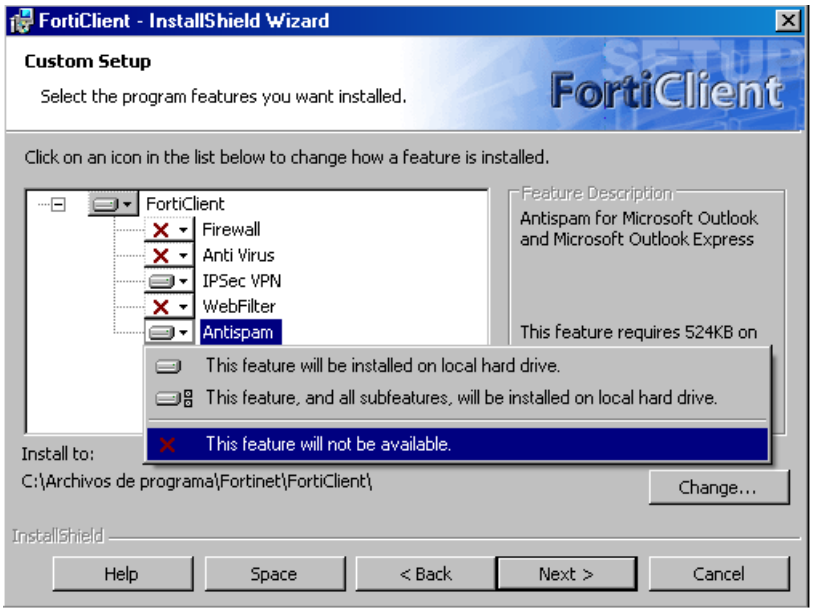
Ahora aceptamos las condiciones del acuerdo de licencias.



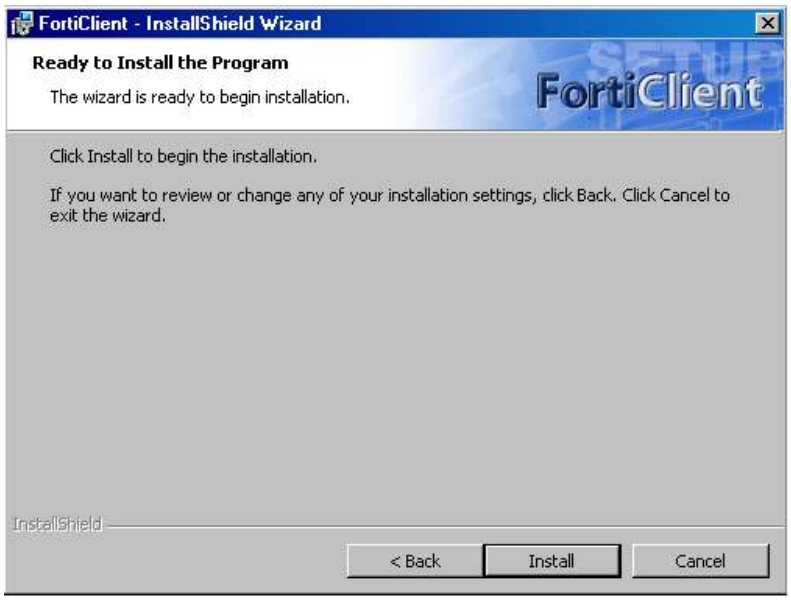
En el modo de instalación seleccionamos la opción **Custom** y hacemos click en **Next** para continuar con la instalación.



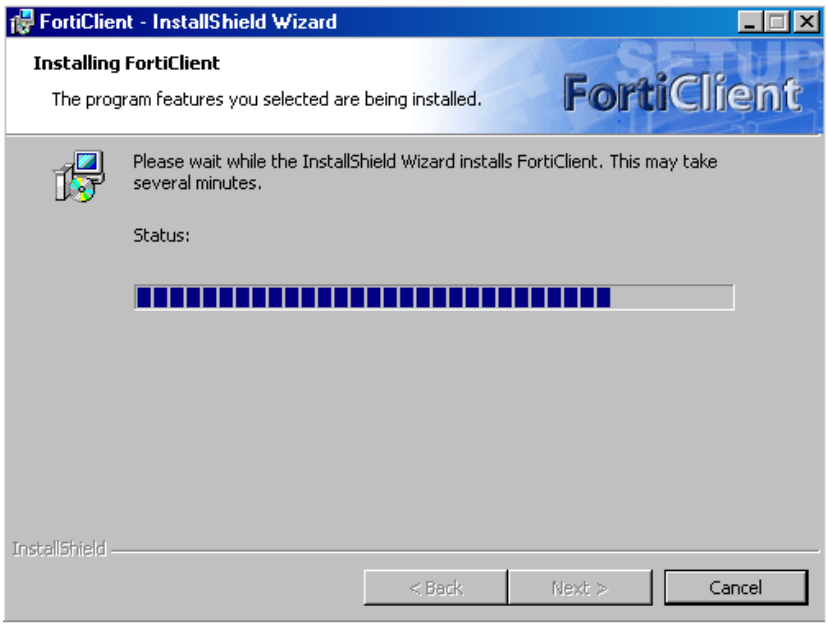
En esta pantalla debemos instalar solamente el cliente VPN, si se instalan los otros servicios y ya existe un antivirus en el PC se empezaran a generar errores, por lo que solo utilizaremos la aplicación para establecer la conexión VPN. Debemos cancelar todos los servicios a excepción de **IPSecVPN**. Después hacemos click en **Next**.



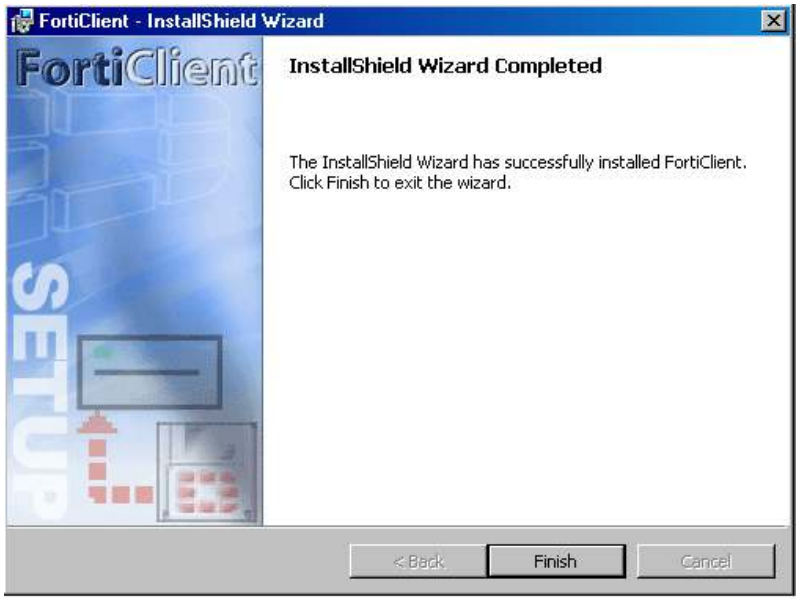
Finalmente hacemos clic en **Install** para empezar la instalación del cliente VPN.



Esperamos que se realice la instalación. Este proceso dura varios minutos, el tiempo va a depender del equipo donde se este instalando el cliente.



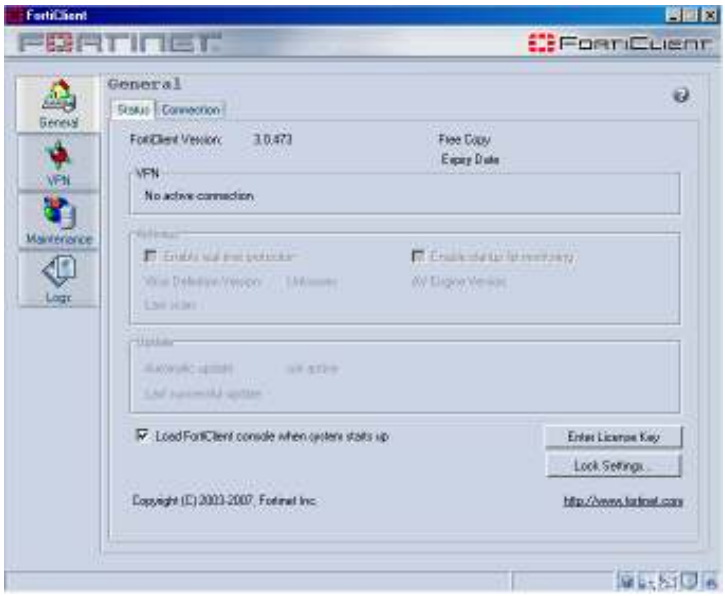
Hacemos click en **Finish** para terminar la instalación y automáticamente se abrirá el cliente. No es necesario reiniciar el sistema.



5. Configuración del cliente VPN.

NOTA: Esta configuración de Forticlient fue hecha para un cliente real por lo que los datos en esta demostración deben cambiarse dependiendo del usuario que se vaya a conectar.

Una vez que se ha instalado el cliente VPN se abrirá la consola principal de FortiClient en el que podemos observar la versión y otros datos generales del cliente.



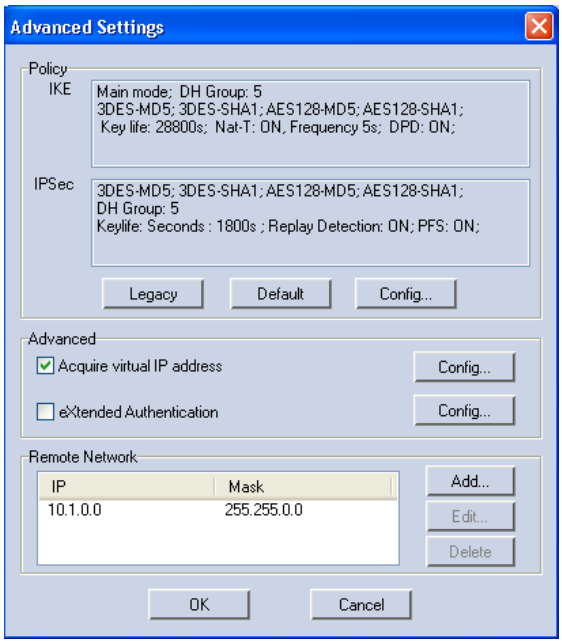
Hacemos clic en la pestaña **VPN** para acceder a la configuración de las conexiones VPN del cliente. Una vez allí seleccionamos **Advanced** y luego en **Add** para crear una nueva conexión VPN.

En la ventana que aparece rellenamos los campos con los siguientes valores:

Connection Name: **VPN a anew**.
Configuration: Seleccionamos **Manual**.
Remote Gateway: **200.35.79.210**
Remote Network: **10.1.0.0 / 255.255.0.0**
Authentication Method: **Preshared Key**
Preshared Key: **XXXXXX**

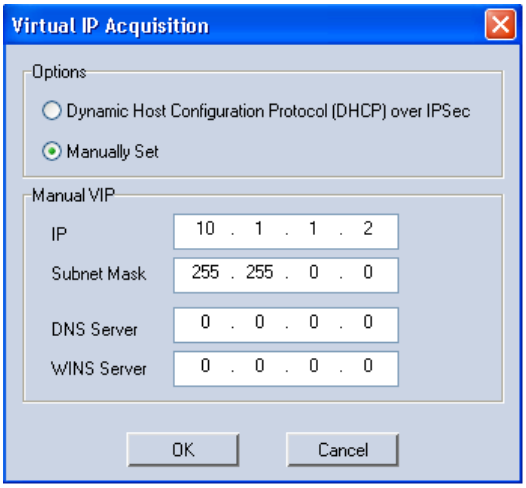
Luego de establecer estos valores hacemos click en **Advanced**.

Ahora marcamos la opción **Acquire virtual IP address** y hacemos click en el botón **Config** que se encuentra al lado.

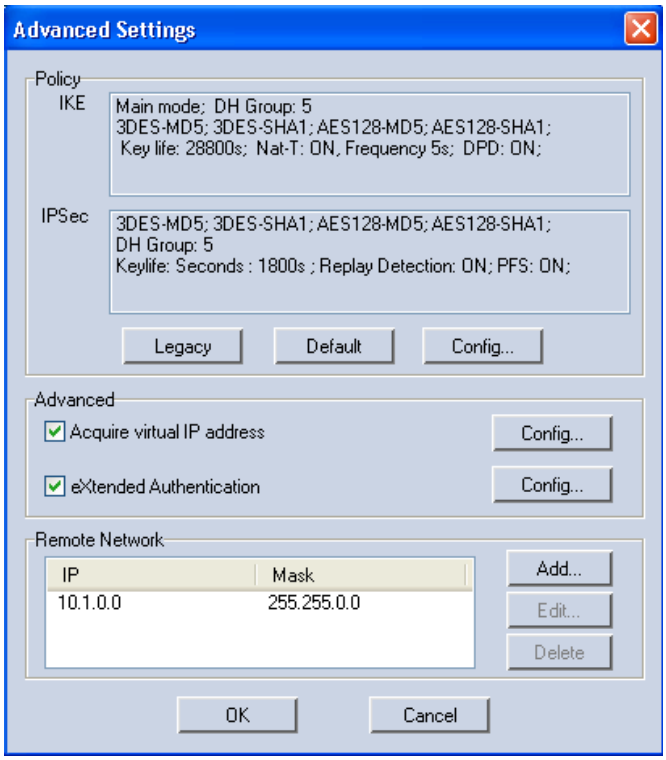


Seleccionamos la opción **Manually Set** y los campos siguientes los rellenamos con los siguientes valores:

IP: **10.1.1.2**
Subset Mask: **255.255.0.0**
DNS Server: **0.0.0.0**
WINS Server: **0.0.0.0**
Una vez rellenados los campos hacemos click en **OK.**



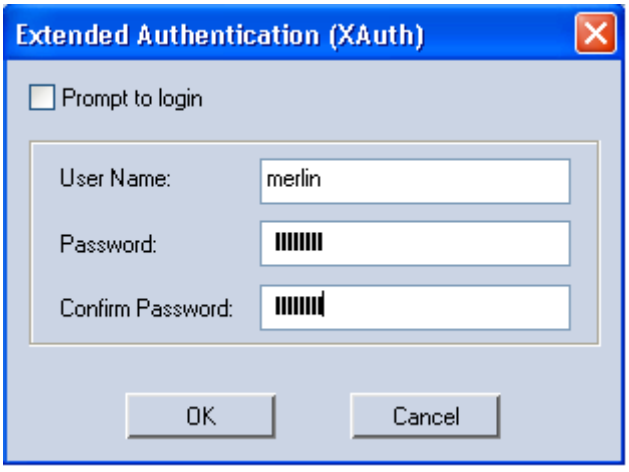
Ahora seleccionamos la opción **eXtended Authentication** y hacemos click en el botón **Config** que se encuentra al lado.



Deseleccionamos la opción **Prompt to login** y llenamos los campos siguientes con los siguientes valores:

User Name: **merlin**
Password: **xxxxxx**
Confirm Password: **xxxxxxx**

Finalmente hacemos click en **OK**.



Hacemos click en **OK**, luego nuevamente en **OK** y el cliente ya estará configurado para conectarse con Anew.


FortiClient
FORTINET
FortiClient
VPN
General
VPN
Maintenance
Logs
Connections
Monitor
My Certificates
CA Certificates
CRL
Name
Gateway / Policy Server
Authentication
Status
VPN a anew
200.35.79.210
Preshared Key
Down
Connect
Advanced >>>
Options
Start VPN before logging on to Windows
Keep IPSec service running forever unless manually stopped
Beep when connection error occurs
Continuously
Stop after
60
seconds
Apply

INSTRUCCIONES PARA ACCEDER A OMNITOUCH UNIFIED COMUNICATIONS.

Para acceder a la página principal de OTUC o ejecutar el Softphone 4980 dentro de la oficina se deben seguir los pasos reseñados a continuación; para acceder a estos servicios desde fuera de la compañía se deben primero seguir los procedimientos explicados en el documento **Conexión VPN Cliente Merlin** para establecer una VPN.

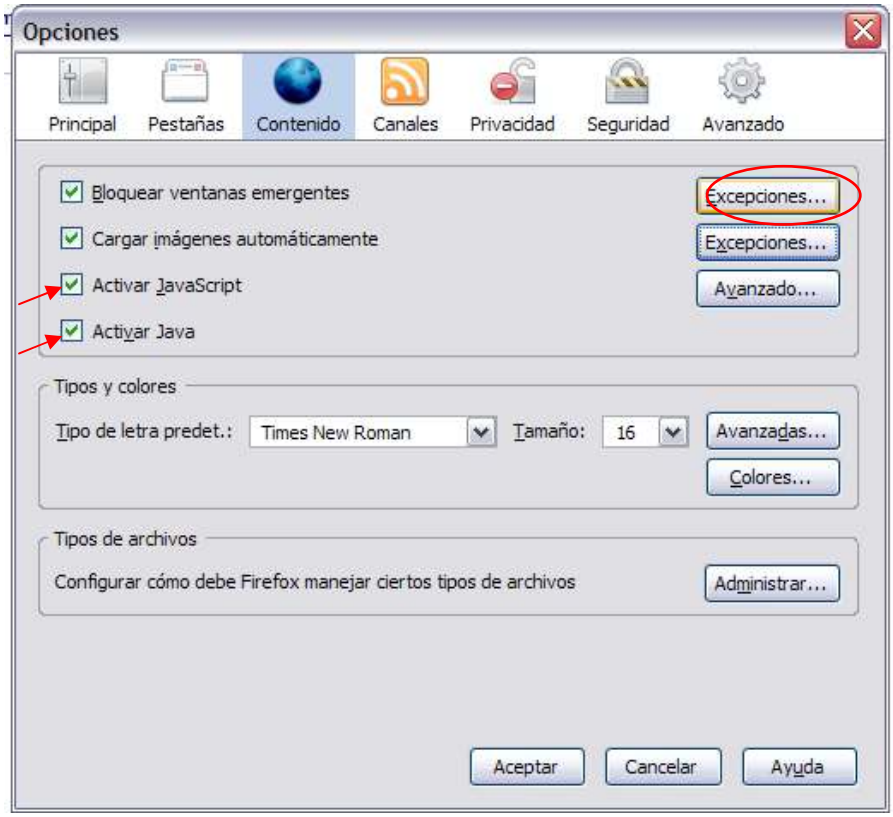
1. Preparar Windows y el navegador web de su preferencia.

1.1. Ejecute el archivo **Cambio al Host.bat** que se encuentra en la carpeta de programas. Este archivo agrega al archivo host de Windows la dirección de otuc.

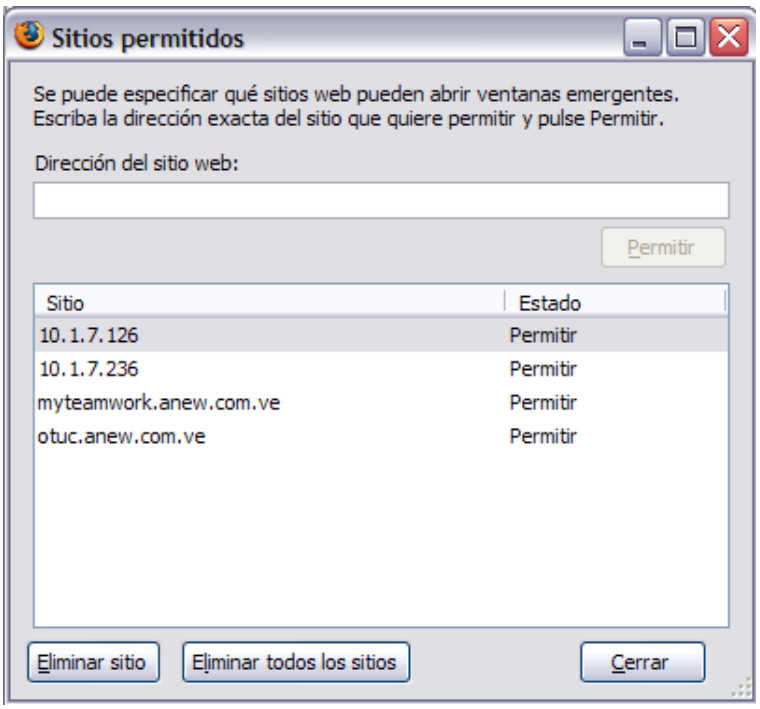
Presione cualquier tecla cuando diga **Listo!** .

1.2. Si se usa Mozilla Firefox.

En el menú **herramientas, opciones** ir a la pestaña de contenido
Asegurarse de que las casillas Activar JavaScript y Activar Java estén habilitadas
En opciones, habilitar activar Java y habilitar Java Scripts,



Hacer click en Excepciones de Ventanas Emergentes. Ahí agregar las siguientes direcciones:

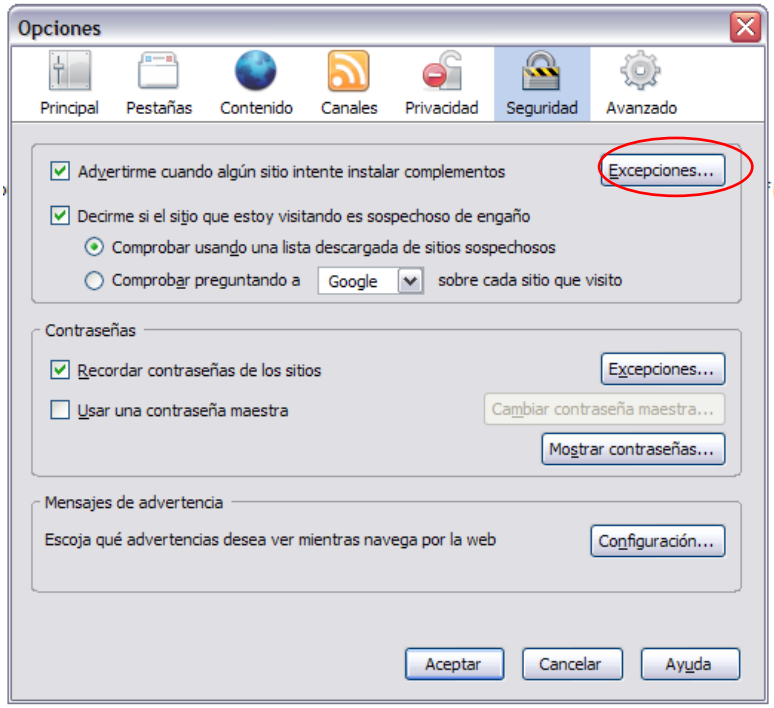


- 10.0.7.126
- 10.0.7.236
- otuc.anew.com.ve
- myteamwork.anew.com.ve

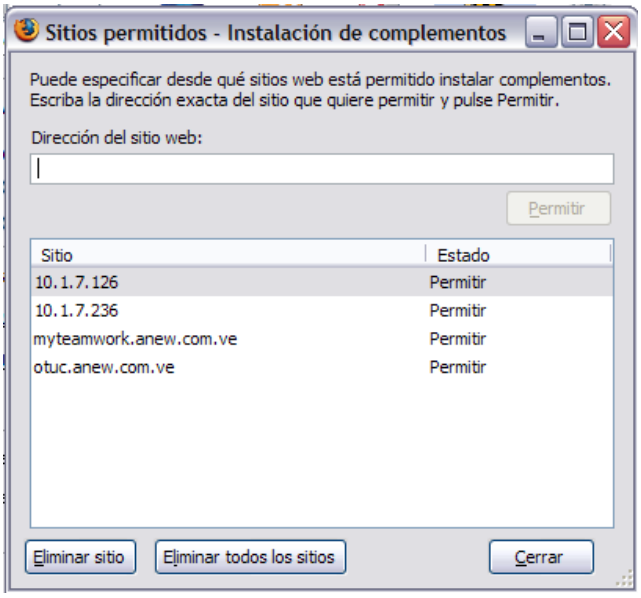
Para agregarlas basta con escribir la dirección bajo **Dirección del sitio web** y luego hacer click en **Permitir**.

Hacer Click en **Cerrar**.

En la pestaña de Seguridad se debe hacer click en **Excepciones** de **Advertirme cuando un sitio intente instalar componentes**:

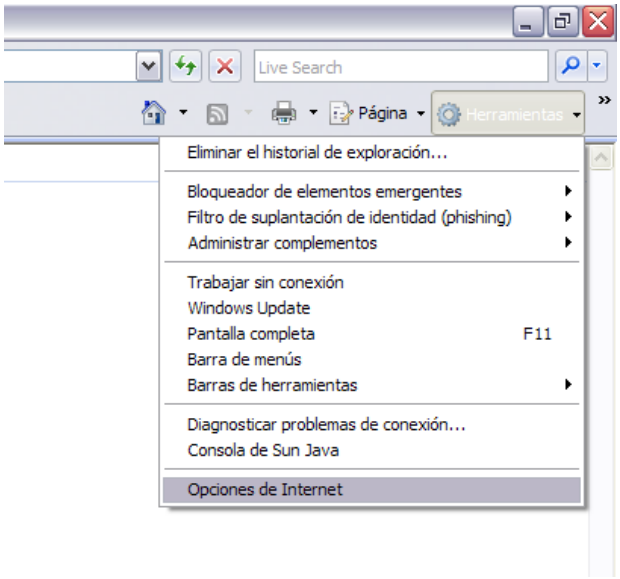


Y ahí agregar las mismas direcciones anteriores:



1.3. Si se usa Internet Explorer .

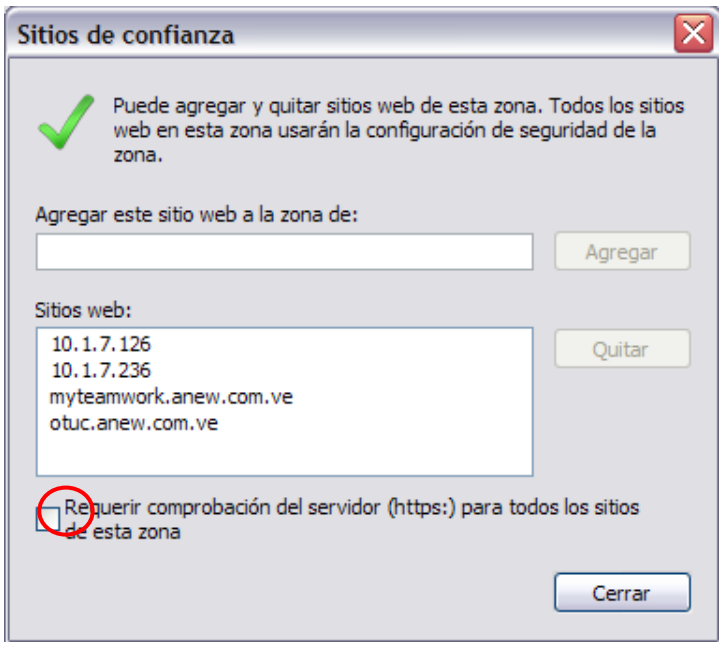
En el menú **Herramientas** hacer click en **Opciones de Internet**.



En la pestaña de seguridad hacer click en **Sitios de confianza** y luego en **Sitios**.

Una vez ahí agregar las siguientes direcciones IP a la lista (verificar que la casilla de comprobación del servidor https: este desactivada):

- 10.0.7.126
- 10.0.7.236
- otuc.anew.com.ve
- myteamwork.anew.com.ve

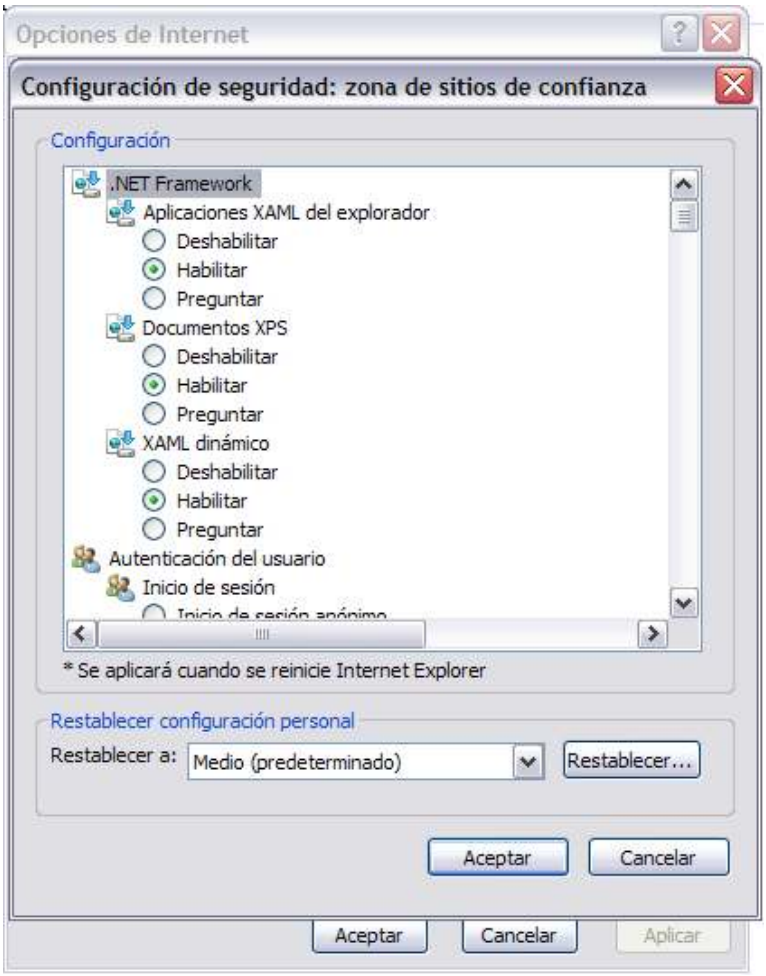


Luego de agregar las direcciones, se puede cerrar esa ventana.

Ahora, se procede a personalizar el nivel de seguridad de los sitios seguros, haciendo click en **Nivel Personalizado**


Opciones de Internet
Conexiones
Programas
Opciones avanzadas
General
Seguridad
Privacidad
Contenido
Seleccione una zona para ver o cambiar la configuración de seguridad.
Internet
Intranet local
Sitios de confianza
Sitios restringidos
Sitios de confianza
Esta zona contiene sitios web que sabe que no van a perjudicar a su equipo o a sus archivos.
Sitios
Esta zona tiene por lo menos un sitio web.
Nivel de seguridad para esta zona
Personalizado
Configuración personalizada.
-Haga clic en Nivel personalizado para cambiar la configuración
-Haga clic en Nivel predeterminado para usar la configuración recomendada.
Nivel personalizado...
Nivel predeterminado
Restablecer todas las zonas al nivel predeterminado
Aceptar
Cancelar
Aplicar

Aquí se cambiaran las siguientes políticas de seguridad:



Inicializar y generar scripts de los controles de ActiveX no marcados como seguros para scripts

- Habilitar

Permitir Scriptlets

- Habilitar

Ejecutar aplicaciones y archivos no seguros

- Preguntar

Tener acceso a origen de datos entre dominios

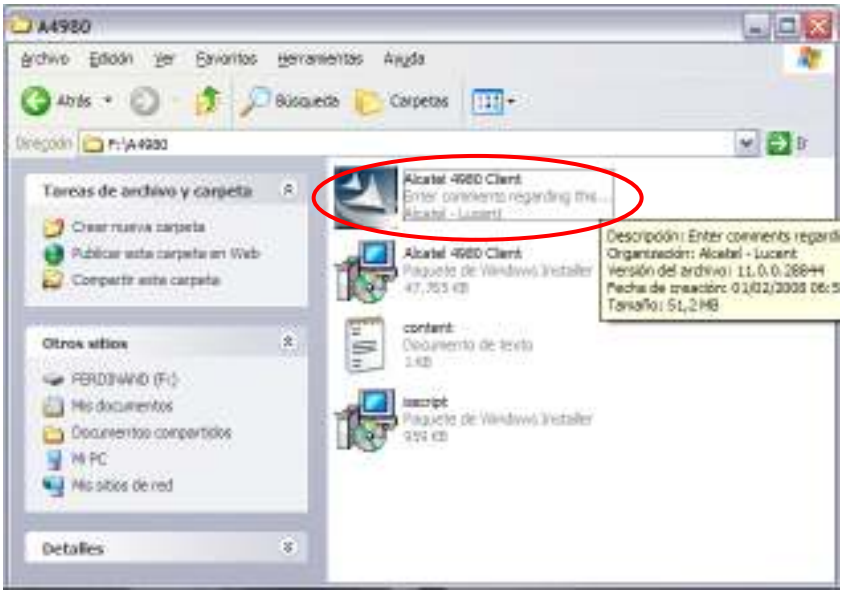
- Habilitar

Usar el bloqueador de elementos emergentes

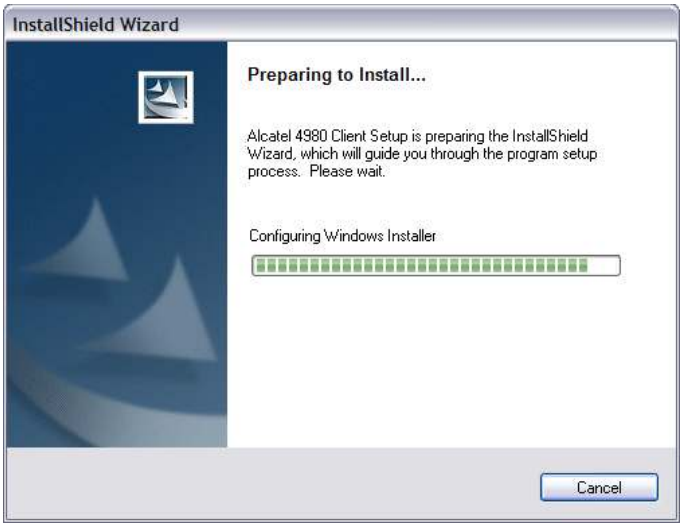
- Deshabilitar

1.4. Instalación.

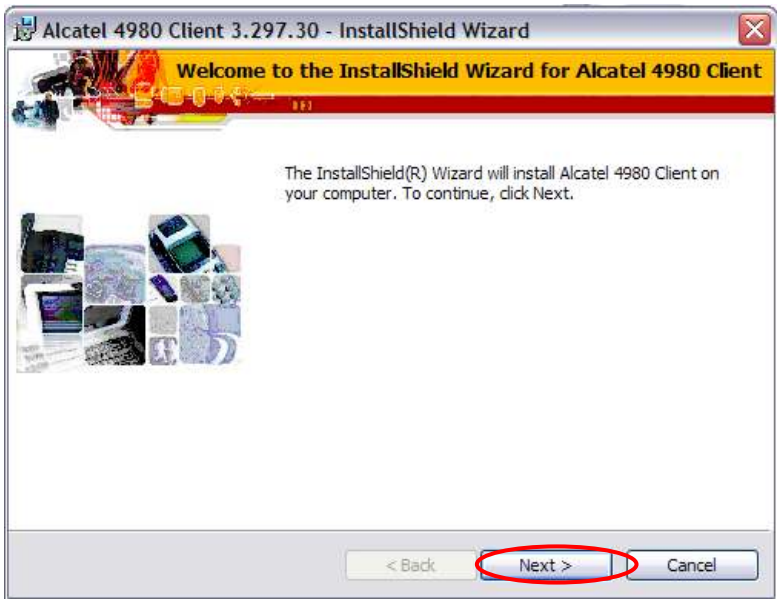
Se le proporcionará una Carpeta llamada A4980, dentro de la carpeta de programas, de ella ejecutará el Archivo **Alcatel 4980 Client.exe** que se muestra a continuación:



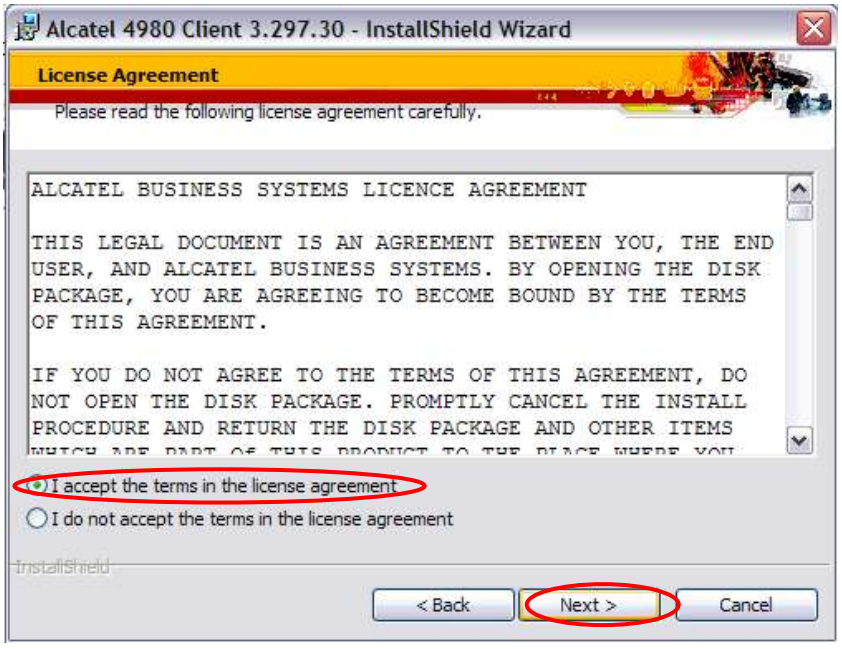
A continuación aparecerá el Asistente de Instalación



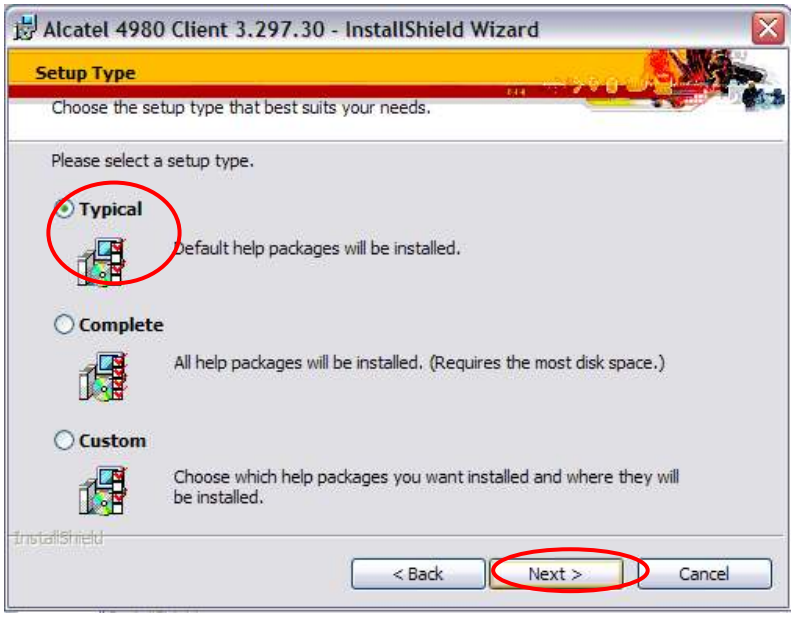
Haga click en **Next**:



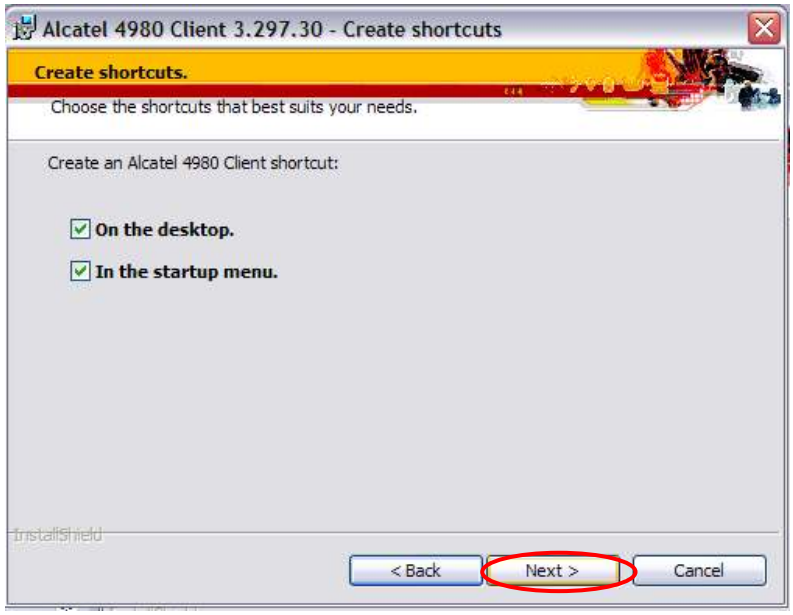
Marque la casilla de **I accept the terms in the license agreement** y presione **Next** para continuar con la instalación



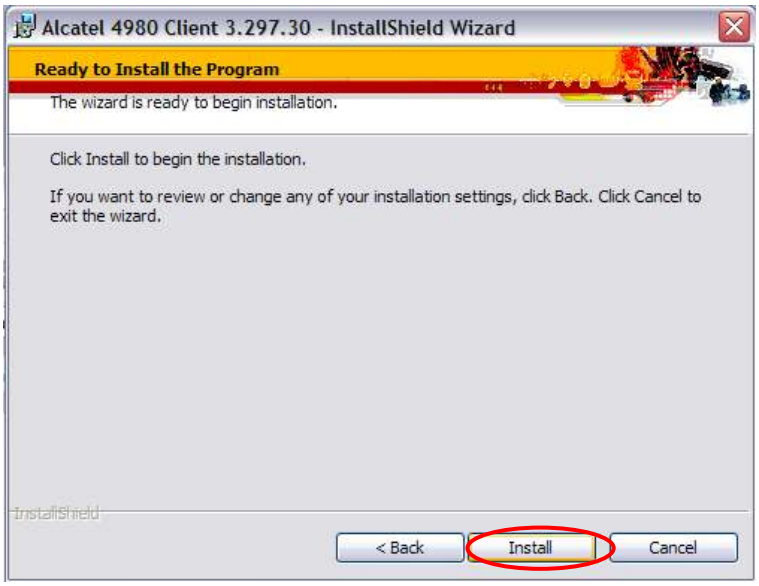
Cuando se le pregunte seleccione el tipo de Instalación **Typical** y haga click en **Next**:



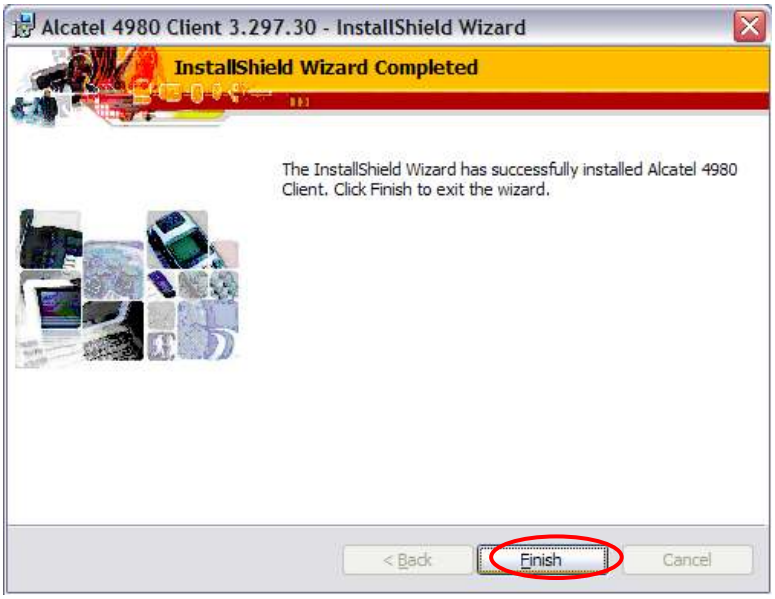
Haga click en **Next** nuevamente:



Haga click en **Install**:



Para terminar con la Instalación haga click en **Finish**:



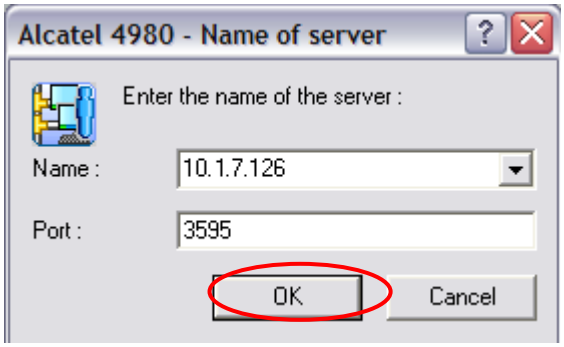
1.5. Ejecución y Configuración.

En su escritorio y en **Inicio/Todos los Programas/Alcatel/A4980** aparecerá un ícono como el siguiente, ejecútelo:

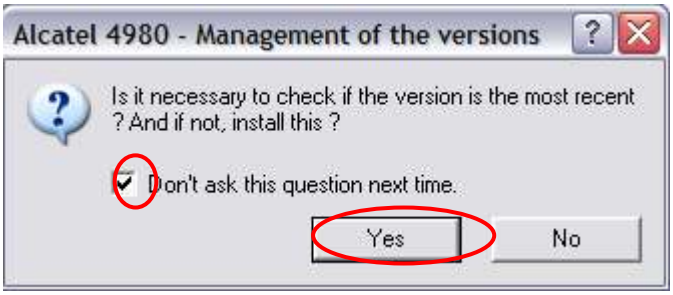
Aparecerá la siguiente ventana, donde pondrá la dirección y puerto que se muestra a continuación:

- Name: 10.0.7.126
- Port: 3595

Presione OK



El cliente debe revisar que la versión que se esta usando sea la mas reciente, marque la casilla **Don't ask this question next time** para que no vuelva a aparecer esta ventana y haga click en **Yes**.



Su nombre de usuario y contraseña para ingresar al sistema serán por defecto la inicial de su nombre y su apellido de la siguiente forma:

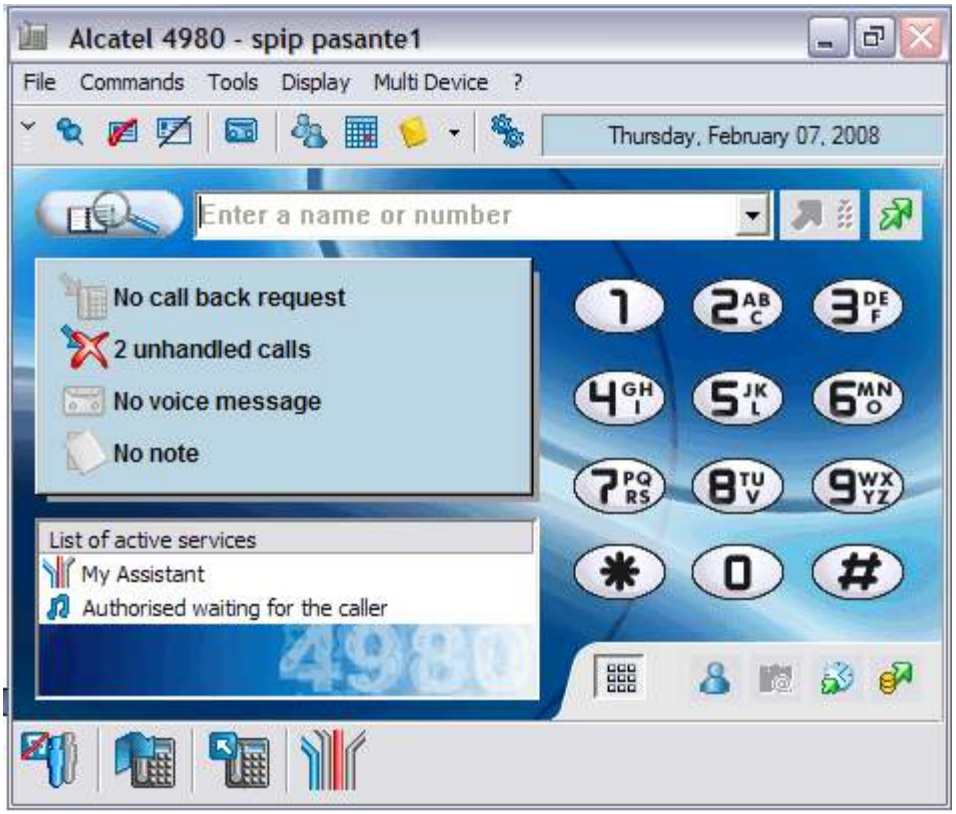
Nombre de Usuario: napellido Contraseña: napellido

Para cambiar su contraseña vaya a la siguiente dirección en su navegador de Internet:

https://10.0.7.126/WebAdmin/passwords

Para lograr la mejor calidad de audio dentro del Softphone 4980 se recomienda el uso de un headset.

Finalmente luego de introducir su contraseña y nombre de usuario llegará a la ventana principal del programa.



2. Página principal de Otuc y My Teamwork

Aquellos usuarios que deseen usar MyTeamwork deben saber que el nombre de usuario y la contraseña con que se trabaja no es la misma con respecto a los otros módulos de Otuc; el nombre se escribe en forma de e-mail, napellido@anew.com.ve, por ejemplo:

Nombre de usuario: napellido@anew.com.ve Contraseña: napellido

La primera vez que entren al sistema se les pedirá una nueva contraseña

La dirección para acceder a **My Teamwork** es la siguiente, simplemente escríbala en la barra de direcciones de su navegador de Internet:

10.0.7.236

La dirección para acceder a **My web Softphone** y **My Assistant** es la siguiente:

10.0.7.126

En los archivos Pdf incluidos encontrará documentación detallada de los módulos disponibles.