ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE LAS MODALIDADES DE FRAUDE QUE UTILIZAN TECNOLOGÍAS VoIP

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

MARÍA JOSÉ MEZA AYALA

DIRECTOR: ING. PATRICIO ORTEGA

Quito, Diciembre 2007

DECLARACION

Yo, María José Meza Ayala, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

María José Meza Ayala

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por María José Meza Ayala, bajo mi supervisión.

_____

Ing. Patricio Ortega
DIRECTOR DE PROYECTO

ÍNDICE

CAPÍTULO II

CAPÍTULO III

DESARROLLO DE LOS SERVICIOS BASADOS EN LA TECNOLOGÍA DE VOZ SOBRE IP ……..……..……..... 136

CAPÍTULO IV

ASPECTOS REGULATORIOS…….……. 180

CAPÍTULO V

ANEXO F

ANEXO G

ANEXO H

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO III

CAPÍTULO III

RESUMEN

En el presente proyecto se realiza un estudio de las modalidades de fraude que utilizan tecnologías VoIP. Para ello el contenido del proyecto se ha dividido en cinco capítulos que se resumen de la siguiente manera:

Capítulo I "**Fundamentos de Voz Sobre IP (VoIP)".** Se realiza un estudio de la tecnología de Voz sobre IP, incluyendo un análisis de su plataforma, características, funcionalidad, protocolos utilizados, arquitectura, calidad de servicio, así como las ventajas y desventajas que ésta tecnología presenta.

Capítulo II **"Uso de Voz sobre IP (VoIP) como mecanismo de fraude".** En este capítulo se lleva a cabo un estudio de los diferentes tipos de fraude que afectan al usuario y a las operadoras de telecomunicaciones; esto como introducción, para luego realizar el estudio de como estos fraudes han evolucionado mediante las facilidades que ofrece la tecnología de Voz sobre IP. Se realiza además un análisis de las alternativas y recomendaciones a tomar en cuenta para la prevención y control de los mismos.

Capítulo III **"Desarrollo de los servicios basados en la tecnología de Voz Sobre IP".** Se realiza un estudio de los servicios que ofrece la tecnología de Voz sobre IP, así como un estudio del marco legal dentro del cual se desenvuelven en la actualidad en nuestro país.

Capítulo IV **"Aspectos Regulatorios".** En éste capítulo se realiza un análisis de la normativa para Voz sobre IP en nuestro país, así como un estudio de los posibles escenarios técnicos y regulatorios que podrían darse en el futuro, para la prestación de servicios y el control del fraude mediante la tecnología de Voz sobre IP.

Capítulo V **“Conclusiones y recomendaciones”.** Se presentan las conclusiones y recomendaciones que han surgido después de la realización del presente proyecto.

PRESENTACIÓN

La Voz sobre IP es un claro ejemplo del avance que ha tenido la tecnología, pero como es usual, esto permite que se creen más y nuevas metodologías de fraude, sobretodo con la Voz sobre IP, debido a la gran cantidad de ventajas tecnológicas y económicas que ofrece.

El presente proyecto plantea un análisis de todos los aspectos referentes a la tecnología de Voz sobre IP, así como del avance de los servicios que proporciona la misma, dando un mayor énfasis en los diferentes tipos de fraude que se cometen mediante el uso de la tecnología en estudio.

Además, se presenta un análisis del marco regulatorio dentro del cual se desenvuelve actualmente la prestación de servicios con la tecnología de Voz sobre IP, así como un estudio de los posibles escenarios técnicos y regulatorios que podría tener la tecnología en el futuro.

El proyecto “Estudio de las modalidades de Fraude que utilizan tecnologías VoIP”, ha sido puesto a consideración de la Dirección General de Investigación Especial en Telecomunicaciones de la Superintendencia de Telecomunicaciones, la cual ha manifestado que el documento en mención sería un aporte positivo para el desempeño de las funciones del organismo técnico de control, debido a la no existencia de textos de consulta referentes a este tema.

CAPITULO I

FUNDAMENTOS DE VOZ SOBRE IP (VoIP)

1.1 INTRODUCCIÓN

El crecimiento y fuerte implantación de las redes IP, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permiten la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP.

Si a todo lo anterior se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar consigo, la conclusión es clara: La VoIP (Voice Over Internet Protocol) es un tema estratégico al cual se le debe poner especial atención.

La telefonía sobre IP abre un espacio muy importante dentro del universo que es Internet, es la posibilidad de estar comunicados a costos más bajos y es la puerta de entrada de nuevos servicios apenas imaginados, entre muchas otras prestaciones.

Hubo un tiempo en que la voz sobre Internet era un "adorno" más de los tantos que permitía la Web, los estándares eran dudosos y el performance del sistema dejaba mucho que desear, aun así, muchos carriers en los Estados Unidos vieron amenazado su negocio y trataron de frenar por vías legales el avance de lo que meses después se planteaba como "Telefonía sobre Internet".

Hoy la telefonía sobre IP empieza a ver su hora más gloriosa y es el fruto más legítimo de la convergencia tecnológica.

El concepto original es relativamente simple: se trata de transformar la voz en "paquetes de información" manejables por una red IP (con protocolo Internet, materia que también incluye a las intranets y extranets).

Ciertamente, existen objeciones de importancia, que tienen que ver con la calidad del sistema en comparación con las de la telefonía tradicional. Sin embargo, la versatilidad y los costos del nuevo sistema hacen que las empresas de telecomunicaciones estén comenzando a considerar la posibilidad de dar servicios sobre IP (aunque todavía el marco regulatorio no lo permite en forma masiva).

En este capítulo se realizará un análisis sobre los conceptos necesarios para comprender el funcionamiento de la tecnología de Voz sobre IP.

1.2 FUNDAMENTOS BÁSICOS

1.2.1. REDES DE TELECOMUNICACIONES

Un Sistema de Telecomunicaciones consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones (Figura 1.1). Se denomina "red de telecomunicaciones" a la infraestructura encargada del transporte de la información. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal, a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte, y; por tanto, el usuario requiere distintos equipos terminales.

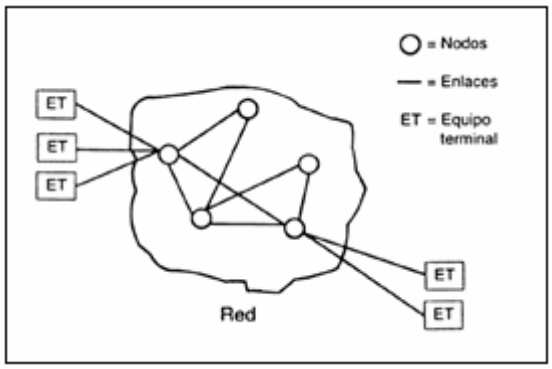


Figura 1.1: Red y equipo Terminal

La principal razón por la cual se han desarrollado las redes de telecomunicaciones es que el costo de establecer un enlace dedicado entre cualesquiera dos usuarios de una red resulta muy elevado, sobre todo considerando que no todo el tiempo todos los usuarios se comunican entre sí. Es mucho mejor contar con una conexión dedicada para que cada usuario tenga acceso a la red a través de su equipo terminal, pero, una vez dentro de la red, los mensajes utilizan enlaces que son compartidos con las comunicaciones de otros usuarios.

En general se puede afirmar que una red de telecomunicaciones está formada por los siguientes componentes:

- Un conjunto de nodos en los cuales se procesa la información, y

- Un conjunto de enlaces o canales que conectan los nodos entre sí y a través de los cuales se envía la información desde y hacia los nodos.

1.2.2 REDES CONMUTADAS

La red consiste en una sucesión alternante de nodos y canales de comunicación, es decir, después de ser transmitida la información a través de un canal, llega a un nodo, éste a su vez la procesa lo necesario para poder transmitirla por el siguiente canal para llegar al siguiente nodo, y así sucesivamente (Figura 1.2).

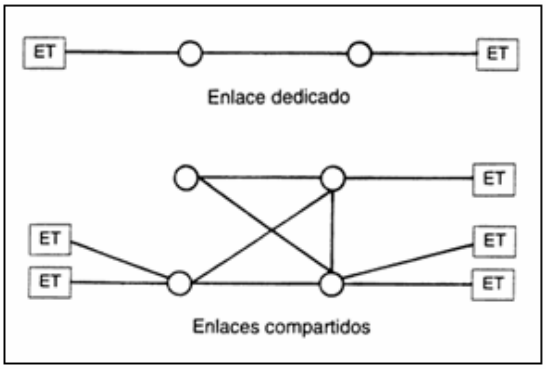


Figura 1.2: Red conmutada

Existen tres técnicas básicas de conmutación:

- Redes de Conmutación de Circuitos
- Redes de Conmutación de Mensajes
- Redes de Conmutación de Paquetes

1.2.2.1 Redes de Conmutación de Circuitos [5]

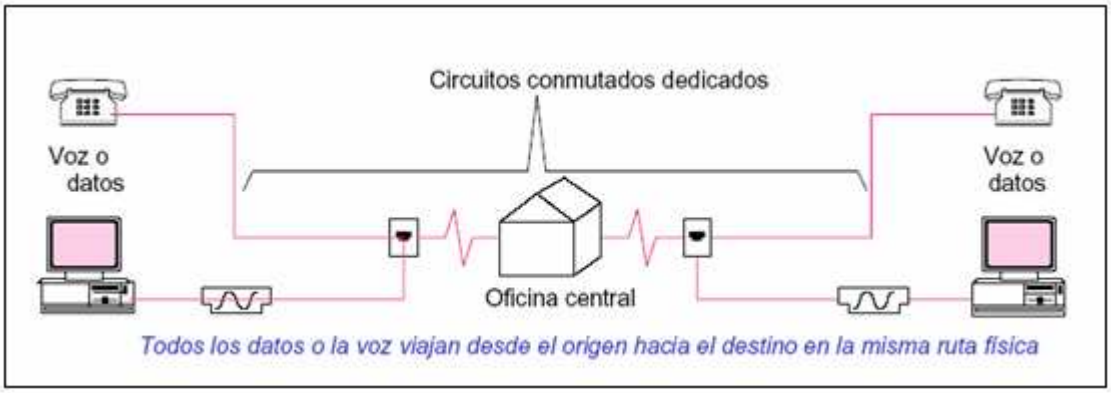


Figura 1.3: Conmutación de circuitos

En este caso a cada comunicación, es decir al tráfico generado entre cada par origen destino, se le asignan recursos de red de forma fija, de esta manera se reserva capacidad en los enlaces o medios de transmisión y en los nodos de conmutación, que se utilizarán única y exclusivamente para esta comunicación, así, cuando dos terminales necesitan comunicarse, deben, en primer lugar, establecer un camino o circuito reservado de extremo a extremo. Para compartir la capacidad de los medios se utilizan técnicas de multiplexación por división de frecuencia o, más usualmente, de multiplexación por división de tiempo, de este modo se reserva para cada comunicación, una región del espectro o un intervalo de tiempo determinado en las tramas de cada enlace, como indica la Figura 1.4, que representa un ejemplo de conmutación de circuitos.

Para realizar esta reserva de recursos de extremo a extremo se necesita señalización, es decir, es necesario intercambiar información entre los terminales y la red y entre nodos de la red. Así una conexión constará de tres fases:

Establecimiento de la conexión: En el momento en que comienza la comunicación, por ejemplo una conversación telefónica, se recorrerán todos los recursos (nodos y enlaces) que formen parte del trayecto entre el origen y el destino y se reservará la capacidad necesaria en los mismos, estableciéndose así

el circuito reservado entre origen y destino. En caso de que los recursos estén ocupados y no sea posible esta reserva, la conexión será rechazada.

Transferencia de información: En esta fase se realiza la transmisión de datos, voz, etc., a través del camino o circuito reservado en la fase anterior.

Liberación de la conexión: Una vez terminada la fase de transferencia se liberan todos los recursos reservados, de forma que puedan ser utilizados para cualquier otra conexión que se quiera establecer.

Con esta técnica de conmutación se logra tener una calidad de servicio garantizada en la fase de transferencia de información, ya que los recursos permanecen reservados (en exclusiva) para esa conexión. El retardo de la transmisión de extremo a extremo y la cantidad de información perdida serán mínimos. Sin embargo también presenta algunas desventajas como son:

- Uso ineficaz de los recursos durante los periodos de inactividad: Si en una conexión existen periodos de silencio los recursos siguen estando reservados pero no se utilizan, con lo que se está desperdiciando capacidad en el canal de comunicación. Un ejemplo claro es una conversación telefónica, en la que los periodos de silencio pueden ser bastante significativos.

- Si todos los circuitos están ocupados la comunicación es imposible: Como ya se ha dicho, la conexión puede ser rechazada en caso de que no exista capacidad suficiente en alguno de los recursos que se deben atravesar a lo largo de la red. Nunca se utiliza la capacidad máxima del canal para un solo circuito, aunque en realidad sea éste el que lo está utilizando de forma exclusiva. Un subcanal sólo utiliza la capacidad reservada para esa conexión.

- Se necesita señalización para establecer la conexión, lo que conlleva un

tiempo para cumplir con esta función, los datos no se empiezan a enviar hasta que la conexión no esté establecida.

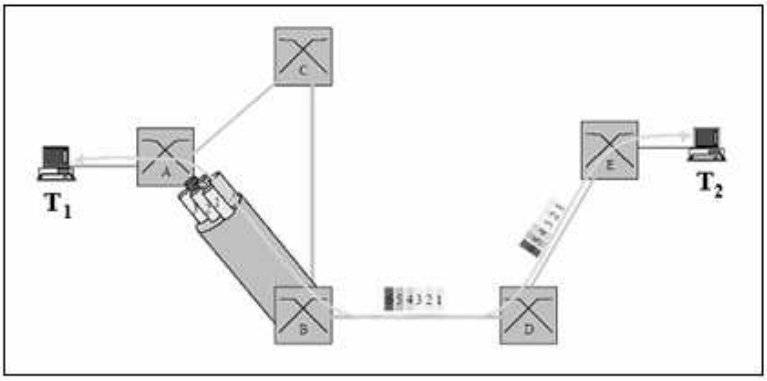


Figura 1.4: Ejemplo de Conmutación de Circuitos

1.2.2.2 Redes de Conmutación de Mensajes [5]

Esta es, en realidad, la técnica de conmutación más antigua que existe, ya que era la utilizada con el sistema telegráfico, en este caso se transmite a la red la información completa, formando lo que se conoce como mensaje. Al llegar a cada nodo el mensaje espera en una cola de entrada hasta que le llegue su turno para ser procesado y le sea asignado un enlace de salida para continuar su camino. Se realiza por tanto almacenamiento y reenvío del mensaje en cada nodo de red, como se representa en la Figura 1.5.

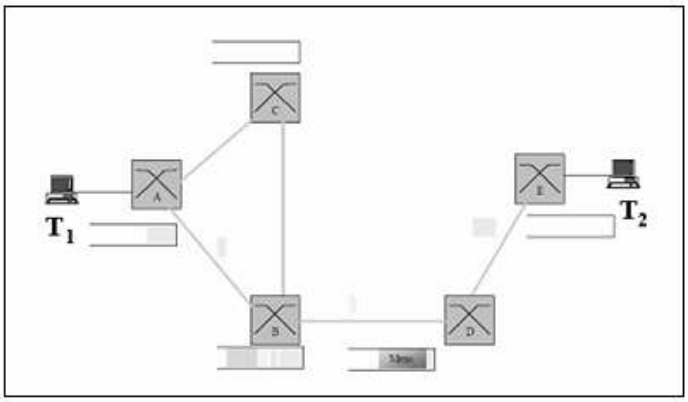


Figura 1.5: Ejemplo de Conmutación de Mensajes

De este modo, el retardo en cada nodo dependerá de la cantidad de mensajes que hayan llegado a él, del tamaño de los mismos y de su propio tamaño. Este retardo puede aumentar considerablemente, de tal forma que puede resultar imposible utilizar esta técnica para tráfico en el que los retardos deban mantenerse muy acotados, por ejemplo para tráfico que necesite respuesta en tiempo real, como sería el caso de las conversaciones telefónicas.
El que existan colas en los nodos implica que sea necesario almacenar los paquetes que llegan. Si en un nodo toda la memoria destinada a este fin está ocupada y llega un nuevo mensaje, este se perderá sin remisión.

Existe el inconveniente añadido de que si un terminal genera un mensaje de un tamaño pequeño y antes llega a la cola un mensaje muy grande, el primero se ve retrasado de forma innecesaria, cuando puede que incluso el emisor esté esperando una respuesta. Existen algunos mecanismos para aplacar este problema, dando prioridad a los mensajes más cortos de la cola, aunque es la conmutación de paquetes la que soluciona más eficientemente este inconveniente.

Por supuesto la conmutación de mensajes también tiene ventajas; al no reservar capacidad en enlaces y nodos y ser dinámica la asignación de la misma, se aprovecha la capacidad total del canal, no existiendo nunca periodos de silencio mientras alguna comunicación necesite el enlace. Por tanto, la multiplexación que se realiza aquí es estadística por división de tiempo. Cada mensaje utilizará toda la capacidad del enlace cuando le toque el turno de ser transmitido, instante que dependerá de las características de las demás comunicaciones que pretendan utilizar el enlace.

1.2.2.3 Redes de Conmutación de Paquetes [5]

Esta técnica está especialmente diseñada para cursar tráfico de datos. Se consigue utilizar los recursos de la red sólo cuando hay tráfico que transmitir, por lo que no se desperdicia capacidad en los periodos de inactividad. Es muy parecida a la técnica anterior.

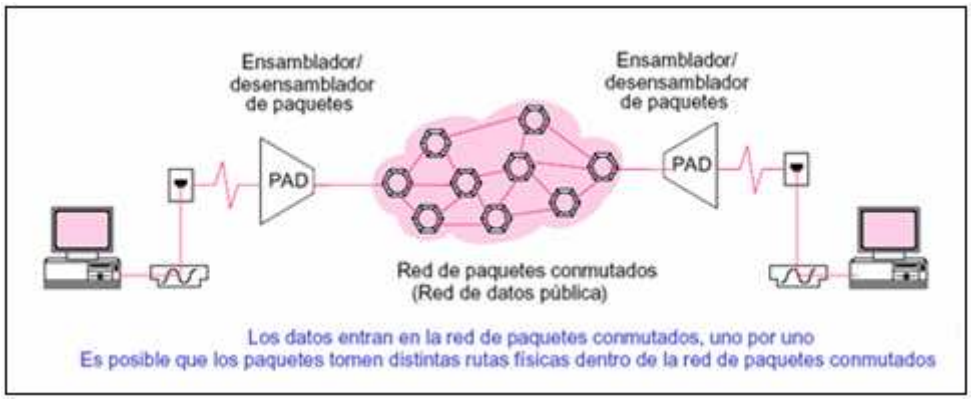


Figura 1.6: Conmutación de paquetes

Aquí los datos a transmitir entre origen y destino se dividirán en paquetes; el tamaño de estos paquetes puede ser variable y dependerá de diversos factores, pero se suele establecer una longitud máxima que nunca deberá superarse, de esta forma se asegura que ninguna comunicación se vea perjudicada frente a otra por el tamaño de los paquetes que utilicen.

También existen colas en los nodos, de forma que cada paquete espera hasta que pueda transmitirse en un enlace de salida.

Como en la conmutación de mensajes, los retardos vendrán dados por el tamaño de las colas y el tiempo de tratamiento de los paquetes que será función del tamaño de los mismos, ya que también se usa la técnica de almacenamiento y reenvío, estos retardos por lo tanto son variables y dependerán de la carga de tráfico en la red.

Como el tamaño de las colas es limitado, la memoria en los nodos de conmutación no es infinita, cuando se llenen habrá que descartar paquetes si llegan nuevos, de manera que se da también el problema de pérdidas de información, lo que degrada la QoS[1] ofrecida. En este caso, la multiplexación realizada es también estadística por división de tiempo, se utiliza la capacidad del enlace según se va necesitando y de forma exclusiva para cada paquete.

[1] QoS - Quality of Service

Cada paquete deberá llevar una cabecera en la que aparecerán datos como:

- La dirección del destino: para poder realizar el correcto encaminamiento de los paquetes.

- La longitud del paquete: en el caso de que los paquetes puedan tener distinta longitud, para poder saber dónde termina un paquete y empieza el siguiente, se utilizan secuencias de bits denominadas flags.

- El número de secuencia del paquete: se refiere a la posición que ocupa dentro del total de la información. Permitirá reensamblar en el destino los paquetes en el orden correcto para obtener la información transmitida, ya que existen casos en que los paquetes llegan desordenados.

- Información de control, por ejemplo para indicar el tipo de paquete, si es de datos o para mantenimiento y gestión de la red, etc.

Existen dos modalidades de conmutación de paquetes:

Orientada a conexión o de circuito virtual

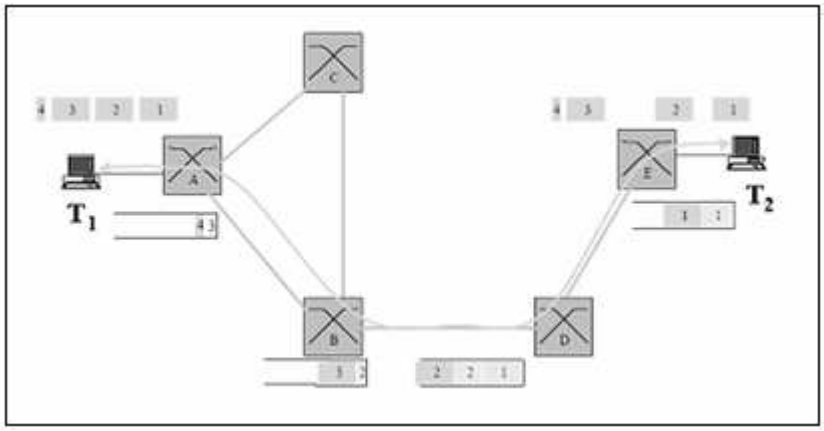


Figura 1.7: Conmutación de paquetes Orientada a conexión

Sólo el primer paquete de cada mensaje tiene que llevar la dirección de destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión.

No orientada a conexión o datagrama

En este caso cada paquete debe llevar la dirección de destino y cada uno de los nodos de la red deciden el camino que se debe seguir. La Figura 1.8 representa este tipo de conmutación.

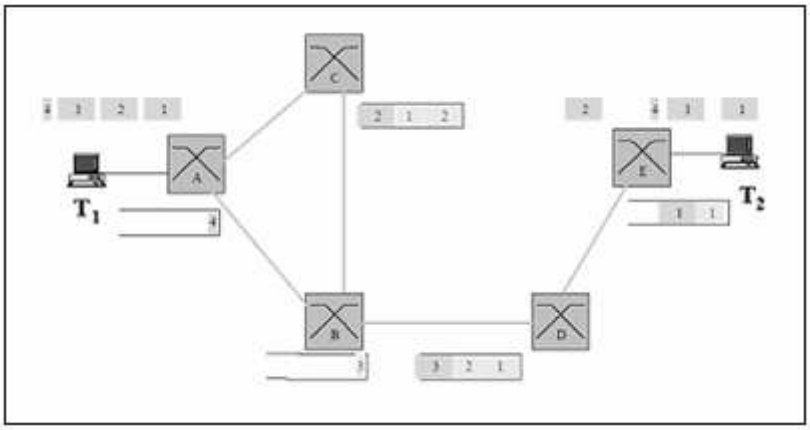


Figura 1.8: Conmutación de Paquetes No Orientada a Conexión

1.2.2.4 Comparación de las técnicas de conmutación

1.2.2.4.1 Retardos

Los enlaces utilizados sufren siempre dos retardos fijos, el de transmisión y el de propagación, el primero dependerá de la cantidad de información a transmitir y de la capacidad del enlace utilizado para ello. Evidentemente si se está utilizando conmutación de circuitos esta capacidad será la reservada para esa comunicación, aunque el resto no se esté utilizando. Si se está utilizando conmutación de mensajes o paquetes, la capacidad utilizada es la totalidad de la ofrecida por el enlace. De esta manera, ante una red poco cargada la conmutación de circuitos será menos eficiente en cuanto al retardo de transmisión

en cada enlace, ya que se está desaprovechando la capacidad del mismo. El retardo de propagación dependerá de la velocidad de propagación de la señal en el medio y de la longitud del enlace. Como estos parámetros no dependen de la técnica de conmutación utilizada no existen diferencias entre las distintas técnicas.

Si se utiliza conmutación de circuitos existe un retardo al establecer la conexión, consecuencia del intercambio de información de señalización que se lleva a cabo entre los terminales y la red y entre los nodos de conmutación para establecer el circuito. A partir del momento en que está establecido el circuito los únicos retardos sufridos son los inevitables de transmisión y propagación por los enlaces. En redes de conmutación de mensajes y paquetes no existe este retardo de establecimiento del circuito, ya que no hay que establecerlo.

Si se está utilizando conmutación de paquetes o de mensajes en cada nodo de red la información se almacena en una cola, donde ésta espera su turno para ser procesada y transmitida al enlace, esto provoca retardos en cada nodo que dependerán de la longitud de los mensajes o paquetes que están delante en la cola y de la longitud del propio mensaje o paquete; estos retardos tienen la característica de depender de la carga del sistema y por tanto son variables y difíciles de predecir y acotar. Si se utiliza conmutación de circuitos no existen colas en los nodos, por lo que no se da este problema.

Al utilizar conmutación de mensajes o paquetes se introduce información de control para el encaminamiento de los datos, esta información debe, por supuesto, transmitirse junto a los datos, por lo que consume capacidad en los enlaces aumentando el retardo en cada uno. Será necesario establecer la relación entre el tamaño de la información de control y el de los datos útiles, para que el rendimiento de la comunicación sea óptimo y los retardos provocados no sean excesivos.

La Figura 1.9 representa los retardos sufridos por la información cuando se utilizan redes con distintas técnicas de conmutación. T1 y T2 son los terminales, A

y B los nodos de conmutación que es necesario recorrer entre el origen y el destino.

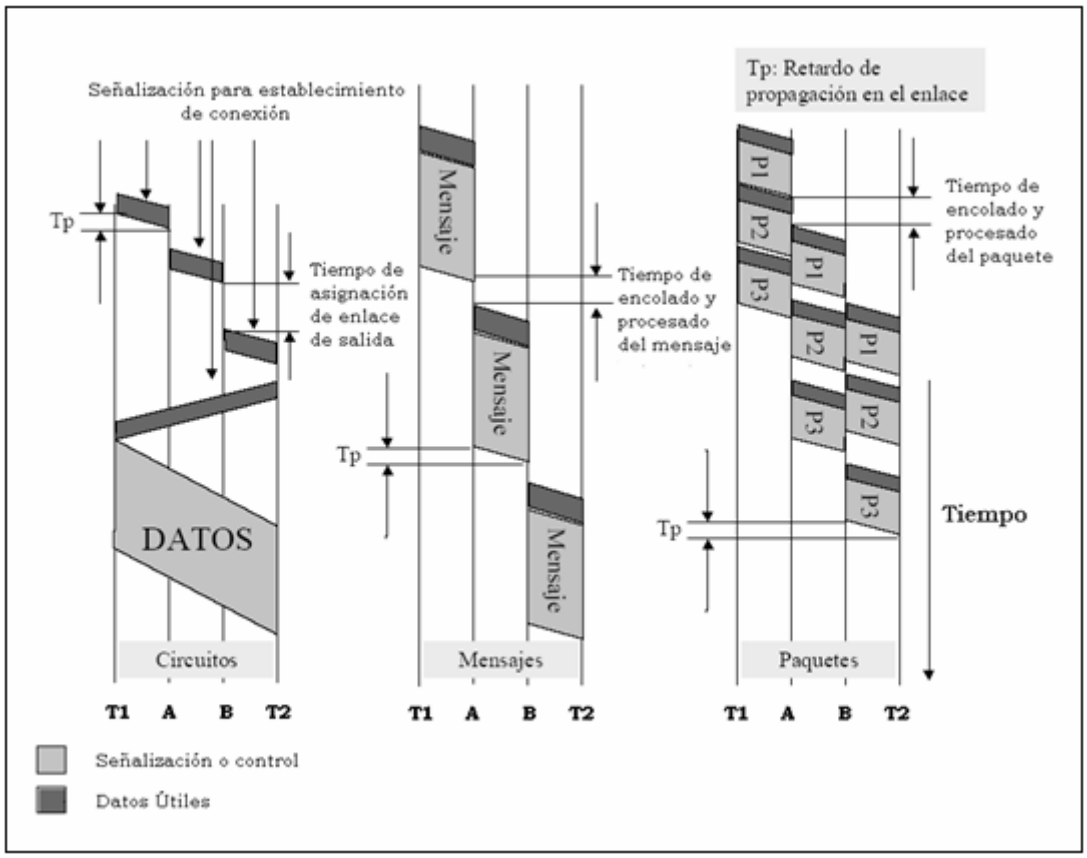


Figura 1.9: Retardos en la red según el tipo de conmutación

1.2.2.4.2 Tipos de tráfico

Ninguna técnica de conmutación es óptima para todo tipo de tráfico, por lo que se han venido desplegando redes especializadas para cada tipo. De esta manera cuando un usuario necesitaba transmitir voz utilizaba la red telefónica conmutada y si quería transmitir datos una red de conmutación de paquetes. Actualmente la filosofía es utilizar una única red para transmitir cualquier tipo de tráfico y presentar así un único interfaz al usuario.

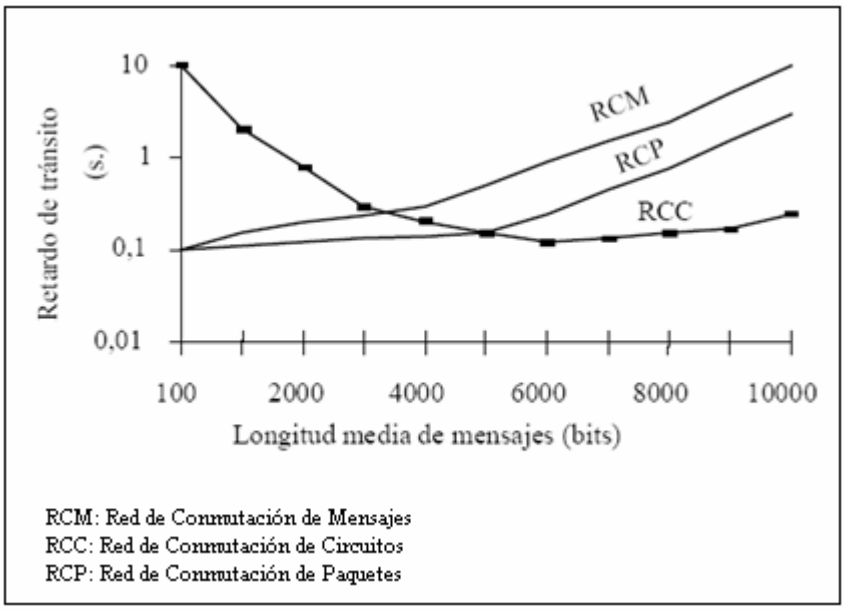


Figura 1.10: Resultados obtenidos de la comparación de las tres técnicas de conmutación

1.2.2.5 Conmutación de circuitos para voz y datos

Consistirá en integrar los distintos tráficos en una única infraestructura de conmutación de circuitos.

La conmutación de circuitos es apropiada para comunicaciones en tiempo real, como las transmisiones vocales, mientras que existen ciertas limitaciones a la hora de conmutar datos en modo circuito.

Para tráfico transaccional, como puede ser una consulta a bases de datos, es importante la relación entre el tiempo de establecimiento del circuito y la duración de la transacción.

Para transacciones cortas no sería eficiente conmutar en modo circuito, debido al tiempo de establecimiento. La velocidad efectiva de transmisión está relacionada no sólo con el tiempo de la transmisión, que dependerá de la capacidad del enlace utilizada, sino también con el tiempo de establecimiento del circuito.

Con tráfico interactivo, como puede ser un chat, existen pausas durante la transmisión originadas por el “tiempo de reacción” de los usuarios, durante las que no se utiliza el circuito, con la consecuente ineficiencia del uso del mismo.

1.2.2.6 Conmutación de paquetes para voz y datos

Consistirá en integrar los distintos tráficos en una única infraestructura de conmutación de paquetes. El problema en esta ocasión será ofrecer un retardo limitado para tráfico en tiempo real, para ello, por un lado se intentan adaptar estos flujos a la conmutación de paquetes, por ejemplo eliminando los periodos de silencio, cuya transmisión o conmutación resulta innecesaria; y utilizando técnicas de compresión que reducen el volumen de información a transmitir y que se basan en el hecho de la gran redundancia existente en señales de voz y vídeo. De esta forma se pueden convertir flujos de voz o vídeo en flujos discontinuos, susceptibles de ser transportados en forma de paquetes. Por otro lado, se adoptan medidas preventivas para minimizar el efecto del retardo variable, que impiden la reconstrucción periódica de las muestras con la pérdida de información consecuente.

1.2.3 DIGITALIZACIÓN Y CODIFICACIÓN DE LA VOZ

La digitalización consiste en la transcripción de señales analógicas en señales digitales, con el propósito de facilitar su procesamiento y hacer la señal resultante más inmune al ruido y otras interferencias a las que son más sensibles las señales analógicas.

1.2.3.1 Señal analógica versus señal digital

Una señal analógica es aquella que puede tomar una infinidad de valores (frecuencia y amplitud) dentro de un límite superior e inferior.

En la Figura 1.11 se muestra una representación gráfica de medio ciclo positivo (+), correspondiente a una señal eléctrica analógica de sonido con sus correspondientes armónicos. Como se podrá observar, los valores de variación de la tensión o voltaje en esta sinusoide pueden variar en una escala que va de “0” a “7” Voltios.

Figura 1.11. Señal Analógica

Una señal digital es aquella cuyos valores (frecuencia y amplitud) no son continuos sino discretos, lo que significa que la señal necesariamente ha de tomar valores fijos predeterminados. Estos valores fijos se toman del sistema binario, es decir que la señal va a quedar convertida en una combinación de unos y ceros.

1.2.3.2 Conversión analógica a digital

La digitalización o conversión analógica a digital consiste básicamente en realizar de forma periódica medidas de la amplitud de la señal y traducirlas a un lenguaje numérico.

En esta definición están presentes los cuatro procesos que intervienen en la conversión analógica a digital:

Muestreo

El muestreo (sampling) consiste en tomar muestras periódicas de la amplitud de onda. La velocidad con que se toman estas muestras, es decir, el número de muestras por segundo, es lo que se conoce como frecuencia de muestreo.

Figura 1.12: Muestreo (Sampling)

Teorema De Nyquist

"La frecuencia de muestreo mínima requerida para realizar una grabación digital de calidad, debe ser igual al doble de la frecuencia de audio de la señal analógica que se pretenda digitalizar y grabar".

Es decir, que la tasa de muestreo se debe realizar, al menos, al doble de la frecuencia de los sonidos más agudos que puede captar el oído humano que son 20 mil hertz por segundo (20 kHz). Por ese motivo se escogió la frecuencia de 44,1 kHz como tasa de muestreo para obtener "calidad de CD", pues al ser un poco más del doble de 20 kHz, incluye las frecuencias más altas que el sentido del oído puede captar.

Retención

Las muestras tomadas han de ser retenidas por un circuito de retención (Hold), el tiempo suficiente para permitir evaluar su nivel (cuantización).

Cuantización

En el proceso de cuantización se mide el nivel de voltaje de cada una de las muestras, consiste en asignar un margen de valor de una señal analizada a un único nivel de salida.

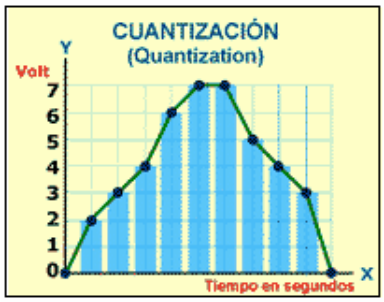


Figura 1.13: Cuantización (quantization)

Codificación

La codificación consiste en traducir los valores obtenidos durante la cuantización al código binario. Permite asignarle valores numéricos binarios equivalentes a los valores de tensiones o voltajes que conforman la señal eléctrica analógica original.

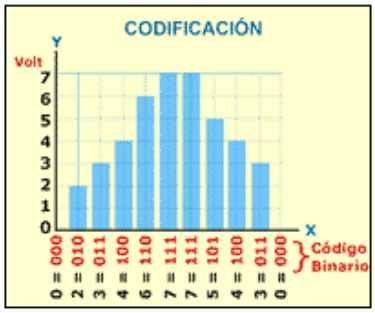


Figura 1.14: Codificación

Durante el muestreo y la retención la señal aún es analógica, puesto que aún puede tomar cualquier valor; no obstante, a partir de la cuantización, cuando toma valores finitos, la señal ya es digital.

1.2.3.3 CÓDEC

El códec es el código específico que se utiliza para la codificación/decodificación de los datos; precisamente, la palabra Códec es una abreviatura de Codificador-Decodificador.

1.2.3.3.1 Parámetros que definen el códec

Número de canales: Indica el tipo de sonido con que se va a tratar: monoaural, binaural o multicanal.

Frecuencia de muestreo: La frecuencia o tasa de muestreo se refiere a la cantidad de muestras de amplitud tomadas por unidad de tiempo en el proceso de muestreo. De acuerdo con el Teorema de muestreo de Nyquist-Shannon, la tasa de muestreo sólo determinará el ancho de banda base de la señal muestreada, es decir, limitará la frecuencia máxima de los componentes sinusoidales que forman una onda periódica.

Resolución: Se refiere al número de bits utilizados y determina la precisión con la que se reproduce la señal original. Se suelen utilizar 8, 10, 16 o 24 bits por muestra. Existe mayor precisión si se usa un mayor número de bits.

Bit rate: Es la velocidad o tasa de transferencia de datos. Su unidad es el bit por segundo (bps).

Pérdida: Algunos códecs al hacer la compresión eliminan cierta cantidad de información, por lo que la señal resultante no es igual a la original (compresión con pérdidas).

1.2.3.3.2 Codificación del sonido

Utiliza un tipo de CODEC específicamente diseñado para la compresión y descompresión de señales de audio.

Ejemplos de Códec de audio

- PAM (Modulación de amplitud de pulsos)
- PCM (Pulse Code Modulated)
- ADPCM (Adaptative Differential Pulse Code Modulated)

1.2.3.3.3 Compresión

La compresión consiste en la reducción de la cantidad de datos a transmitir, pues hay que tener en cuenta que la capacidad de almacenamiento de los enlaces es finita; al igual que los equipos de transmisión, los cuales pueden manejar sólo una determinada tasa de datos.

Existen dos tipos de compresión:

Compresión sin pérdidas: Se elimina la información repetida antes de la transmisión.

Compresión con pérdidas: Se desprecia cierta información considerada irrelevante. Este tipo de compresión puede producir pérdida de calidad en el resultado final.

1.2.4 TRANSMISIÓN DE VOZ DIGITALIZADA

La transmisión de voz digitalizada se realiza mediante ciertos protocolos, específicamente del protocolo TCP/IP.

1.2.4.1 El modelo de referencia OSI

A la hora de describir la estructura y función de los protocolos de comunicaciones se suele recurrir a un modelo de arquitectura desarrollado por la ISO[2]. Este modelo se denomina Modelo de Referencia OSI[3].

El modelo OSI esta constituido por 7 capas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.

[2] ISO - International Standards Organization
[3] OSI - Open Systems Interconnect

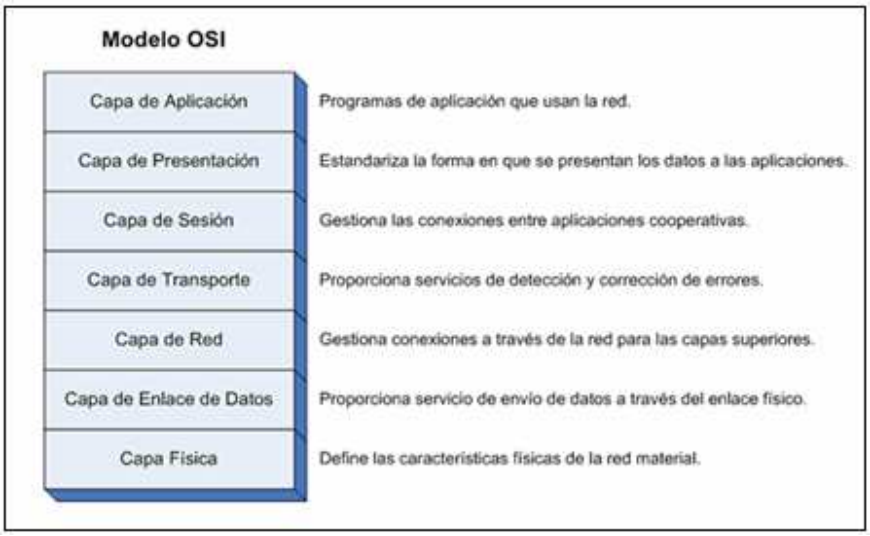


Figura 1.15: Capas del Modelo de Referencia OSI [6]

En una capa no se define un único protocolo sino una función de comunicación de datos que puede ser realizada por varios protocolos.

Cada protocolo se comunica con su igual en la capa equivalente de un sistema remoto y cada uno de ellos solo ha de ocuparse de la comunicación con su gemelo, sin preocuparse de las capas superior o inferior. Sin embargo, también debe haber acuerdo en como pasan los datos de capa en capa dentro de un mismo sistema, pues cada capa esta implicada en el envío de datos.

Las capas superiores delegan en las inferiores para la transmisión de los datos a través de la red subyacente. Los datos descienden por la pila, de capa en capa, hasta que son transmitidos a través de la red por los protocolos de la capa física; en el sistema remoto, irán ascendiendo por la pila hasta la aplicación correspondiente.

La ventaja de esta arquitectura es que, al aislar las funciones de comunicación de la red en capas, minimizamos el impacto de cambios tecnológicos en el juego de protocolos, es decir, podemos añadir nuevas aplicaciones sin cambios en la red física y también podemos añadir nuevo hardware a la red sin tener que reescribir el software de aplicación.

1.2.4.1.1 Capas Del Modelo OSI

Capa Física: Aquí se encuentran los medios materiales para la comunicación como los cables, conectores, etc., es decir los medios mecánicos y eléctricos.

Capa De Enlace: Se encarga de transformar la línea de transmisión común en una línea sin errores para la capa de red, además se encarga de solucionar los problemas de reenvío, o mensajes duplicados cuando hay destrucción de tramas.

Capa De Red: Se ocupa del control de la operación de la subred y de la interconexión de redes heterogéneas, solucionando problemas de protocolos diferentes.

Este nivel encamina los paquetes de la fuente al destino final a través de encaminadores (routers) intermedios. Debe existir conocimiento de la topología de la subred, evitar la congestión, y manejar saltos cuando la fuente y el destino están en redes distintas.

Capa de Transporte: El nivel de transporte permite que los usuarios puedan mejorar el servicio del nivel de red (que puede perder paquetes, puede tener routers que no funcionan, etc.).

Capa de Sesión: Permite a los usuarios sesionar entre sí, dejándolos acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.

Capa de Presentación: Se ocupa de los aspectos de sintaxis y semántica de la información que se transmite, por ejemplo la codificación de datos según un acuerdo. La realización de las funciones de la capa presentación se deben a que los formatos en que se representa la información que se transmite son distintos en cada máquina.

Capa de Aplicación: Contiene una variedad de protocolos que se necesitan frecuentemente, por ejemplo para la cantidad de terminales incompatibles que existen para trabajar con un mismo editor orientado a pantalla.
Otra función de esta capa es la de transferencia de archivos distintos entre dos o más máquinas, solucionando problemas de incompatibilidad. Además se encarga del sistema de correo electrónico, y otros servicios de propósitos generales.
El nivel de aplicación es siempre el más cercano al usuario.

1.2.4.1.2 Terminología en el Modelo OSI

Entidades: Elementos activos que se encuentran en cada una de las capas, estos pueden ser software o hardware. Cuando las entidades se encuentran en la misma capa son entidades pares.

Proveedor de servicio: Es cada entidad inferior a otra que le puede ofrecer servicios o funciones.

SAP: Es el punto de acceso a los servicios de una capa inferior, cada SAP tiene una dirección que lo identifica.

Interfaz: Es el conjunto de reglas que hace que las capas se puedan comunicar. Se usa una IDU[4] a través del SAP, la IDU consiste en una SDU[5], además de alguna información de control necesaria para que las capas inferiores realicen su trabajo, pero no forma parte de los datos.

1.2.4.2 Aproximación al modelo de arquitectura de los protocolos TCP/IP

El modelo de arquitectura de estos protocolos es más simple que el modelo OSI, como resultado de la agrupación de diversas capas en una sola o bien por no usar alguna de las capas propuestas en dicho modelo de referencia.

[4] IDU - Unidad de Datos de la Interfaz
[5] SDU - Unidad de Datos de Servicio

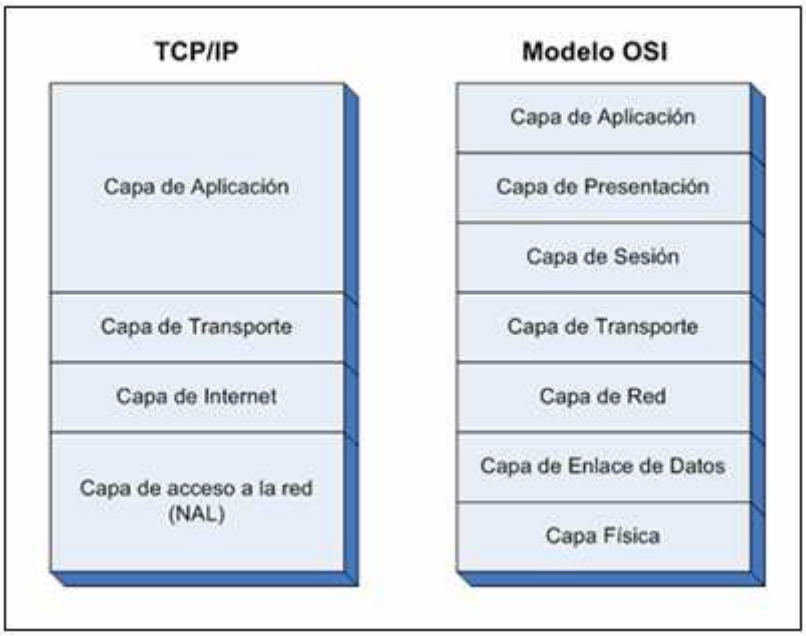


Figura 1.16: TCP/IP y Modelo OSI [6]

La capa de Presentación desaparece pues las funciones a definir en ellas se incluyen en las propias aplicaciones; lo mismo sucede con la capa de Sesión, cuyas funciones son incorporadas a la capa de Transporte en los protocolos TCP/IP. Finalmente la capa de enlace de datos no suele usarse en dicho paquete de protocolos.

De esta forma nos quedamos con un modelo en cuatro capas, tal y como se muestra en la Figura 1.16.

Al igual que en el modelo OSI, los datos descienden por la pila de protocolos en el sistema emisor y la escalan en el extremo receptor. Cada capa de la pila añade información de control a los datos a enviar a la capa inferior, para que el envío sea correcto, esta información de control se denomina cabecera, pues se coloca precediendo a los datos; a la adición de esta información en cada capa se le denomina encapsulamiento. Cuando los datos se reciben, tiene lugar el proceso inverso, es decir, según los datos ascienden por la pila, se van eliminando las cabeceras correspondientes.

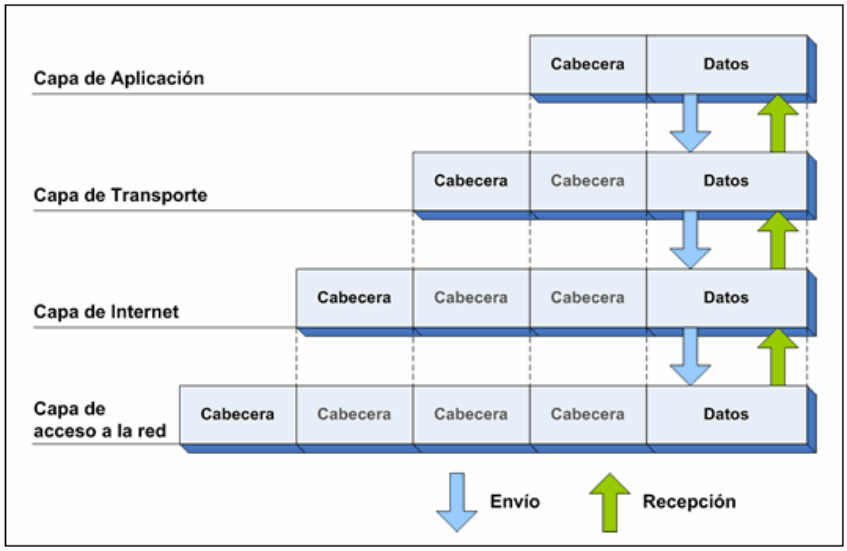


Figura 1.17: Estructura del Modelo TCP/IP [6]

Cada capa de la pila tiene su propia forma de entender los datos y, normalmente, una denominación especifica, sin embargo, todos son datos a transmitir, y los términos sólo nos indican la interpretación que cada capa hace de los mismos.

1.2.4.2.1 Capas de TCP/IP

Capa de acceso a la red: El software TCP/IP de nivel inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica.

Capa de Internet: La capa Internet maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina hacia la que se debe enviar el paquete. La capa Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo, para decidir si el mismo debe procesarse de manera local o debe ser transmitido. Por último, la capa Internet envía los mensajes ICMP[6] de error y control necesarios y maneja todos los mensajes ICMP entrantes.

[6] ICMP – Internet Control Message Protocol es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP).

Capa de transporte: La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Esta capa regula el flujo de información y puede también proporcionar un transporte confiable asegurando que los datos lleguen sin errores y en secuencia.

Capa de aplicación: Este es el nivel más alto, el cual interactúa con la capa de transporte para enviar o recibir datos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega.

1.2.4.3 Protocolo IP

El Protocolo de Internet IP es un protocolo no orientado a conexión, usado tanto por el origen como por el destino, para la comunicación de éstos a través de una red de paquetes conmutados.

Los datos en una red que se basa en IP son enviados en bloques conocidos como paquetes o datagramas. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo IP provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort)), no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad mediante checksums o sumas de comprobación de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir (datagramas) supera el tamaño máximo negociado (MTU) en el tramo de red por el que va a circular, podrá ser dividida en paquetes más pequeños y reensamblada luego cuando sea necesario. Estos fragmentos

podrán ir cada uno por un camino diferente dependiendo de como se encuentre la congestión de las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

1.2.4.3.1 Direccionamiento IP y enrutamiento

Quizás los aspectos más complejos de IP son el direccionamiento y el enrutamiento; el direccionamiento se refiere a la forma como se asigna una dirección IP y cómo se dividen y se agrupan subredes de equipos, el enrutamiento consiste en encontrar un camino que conecte una red con otra y aunque es llevado a cabo por todos los equipos, es realizado principalmente por enrutadores que no son más que computadores especializados en recibir y enviar paquetes por diferentes interfaces de red, así como proporcionar opciones de seguridad, redundancia de caminos y eficiencia en la utilización de los recursos.

1.2.4.3.2 Dirección IP

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP, que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se debe confundir con la dirección MAC[7] que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar.

Siempre que un usuario se conecta a Internet utiliza una dirección IP, esta dirección puede cambiar al reconectar; a esta forma de asignación de dirección IP se denomina una dirección IP dinámica.

[7] MAC – Media Access Control Address es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los primeros 24 bits) y por el fabricante (los ultimos 24 bits).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija o IP estática, es decir, no cambia con el tiempo. Los servidores de correo, DNS[8], FTP públicos o servidores WEB, necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se facilita su ubicación.

1.2.4.3.3 Enrutamiento

El enrutamiento es el mecanismo por el cual los paquetes de información se hacen llegar desde su origen a su destino final, siguiendo un camino o ruta a través de la red. En una red grande o en un conjunto de redes interconectadas, el camino a seguir hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.

Asociado al encaminamiento existe el concepto de métrica, que es una medida de lo "bueno" que es usar un camino determinado. La métrica puede estar asociada a distintas magnitudes: distancia, coste, retardo de transmisión, número de saltos, etc., o incluso a una combinación de varias magnitudes. Si la métrica es el retardo, es mejor un camino cuyo retardo total sea menor que el de otro; lo ideal en una red es conseguir el encaminamiento óptimo; tener caminos de distancia, costo o retardo mínimos. Típicamente el encaminamiento es una función implantada en la capa 3 (capa de red) del modelo de referencia OSI.

1.2.4.3.4 Versiones

En la actualidad, la mayoría de las máquinas conectadas a Internet operan sobre la versión 4 del protocolo IP: IPv4; sin embargo, es inevitable y necesaria la progresiva migración a la versión 6 de este protocolo: IPv6, también conocida como "IP Next Generation" (IPNG). La principal causa de esta migración es la escasez de direcciones IPv4 disponibles, que tendría solución empleando los 128 bits de direccionamiento IPv6.

[8] DNS – Domain Name System, es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Además de su escalabilidad, IPv6 presenta otra serie de ventajas frente a IPv4, como por ejemplo, mejoras en seguridad y calidad de servicio.
Hasta la migración definitiva a IPv6, parece probable que las dos versiones del protocolo convivirán durante un largo periodo.

Las versiones de la 0 a la 3 están reservadas o no fueron usadas, la versión 5 fue usada para un protocolo experimental; otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

1.2.4.4 Protocolo TCP

TCP[9] es el método usado por el protocolo IP para enviar datos a través de la red; mientras IP cuida del manejo del envío de los datos, TCP cuida el trato individual de cada uno de los paquetes, para el correcto enrutamiento de los mismos a través de Internet.

1.2.5 VOZ SOBRE IP

La Voz sobre IP (VoIP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos.

1.2.5.1 Telefonía IP

La Telefonía IP es una aplicación inmediata de la Voz sobre IP, de forma que permite la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. En general ofrece servicios de comunicación como voz, fax o aplicaciones de mensajes de voz, que son transportados vía redes IP, en lugar de ser transportados vía la red telefónica convencional.

La Voz sobre IP es una tecnología de telefonía que puede ser habilitada a través de una red de datos de conmutación de paquetes, vía el protocolo IP.

[9] TCP - Transmisión Control Protocol

La tecnología VoIP puede revolucionar las comunicaciones internas al ofrecer:

- Acceso a las redes corporativas desde pequeñas sedes a través de redes integradas de voz y datos conectadas a sucursales.

- Directorios corporativos basados en la intranet, con servicios de mensajes y números personales para quienes deben desplazarse.

- Redes privadas y gateways virtuales, gestionados para voz, que sustituyen a las VPN[10].

1.2.5.2 Elementos de la Voz sobre IP

El modelo de Voz sobre IP está formado por tres elementos principales:

El cliente: Este elemento establece y termina las llamadas de voz. Codifica, empaqueta y transmite la información de salida generada por el usuario; asimismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario. Cabe destacar que el elemento cliente se presenta en dos formas básicas: la primera es una suite de software corriendo en una PC, que el usuario controla mediante una interfaz gráfica (GUI); y la segunda puede ser un cliente "virtual" que reside en el gateway.

Servidores: El segundo elemento de la Voz sobre IP está basado en servidores, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real, como fuera de él. Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarifación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio, entre otros.

Gateways: El tercer elemento lo conforman los gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. La función

[10] VPN - Virtual Private Network

principal de un gateway es proveer la interfaz con la telefonía tradicional apropiada, funcionando como una plataforma para los clientes virtuales.
Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de la Calidad del Servicio y en el mejoramiento del mismo.

1.2.5.3 Características de Voz sobre IP

Por su estructura, la Voz sobre IP proporciona las siguientes características:

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.

- Proporciona el enlace a la red telefónica tradicional.

Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:

- Es independiente del tipo de red física que lo soporta y permite la integración con las grandes redes de IP actuales.

- Es independiente del hardware utilizado.

- Permite ser implementado tanto en software como en hardware.

1.2.5.4 Protocolos de Voz sobre IP

Hoy en día, existen varios protocolos para transmitir voz sobre redes IP, los cuales definen la manera en que los dispositivos deben establecer comunicación entre si, además de incluir especificaciones para Códecs de audio para convertir una señal auditiva a una digitalizada comprimida y viceversa.

1.2.5.4.1 H.323 [7]

H.323 es una recomendación del ITU-T, que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red. Es utilizado comúnmente para Voz sobre IP y para videoconferencia basada en IP.

H.323 se creó originalmente para proveer de un mecanismo para el transporte de aplicaciones multimedia en LANs[11], pero ha evolucionado rápidamente para dirigir las crecientes necesidades de las redes de VoIP.

Un punto fuerte de H.323 era la relativa y temprana disponibilidad de un grupo de estándares, no solo definiendo el modelo básico de llamada, sino que además definía servicios suplementarios, necesarios para dirigir las expectativas de comunicaciones comerciales. H.323 fue el primer estándar de VoIP en adoptar el estándar de IETF, el RTP[12] para transportar audio y vídeo sobre redes IP.

H.323 está adaptado para situaciones en las que se combina el trabajo entre IP y RDSI[13], y respectivamente entre IP y QSIG[14].

Al ser un modelo de llamada similar a RDSI, facilita la introducción de la Telefonía IP en las redes existentes de RDSI basadas en sistemas PBX. Por esto es posible el proyecto de una migración sin problemas hacia el IP basado en sistemas PBX.

Dentro del contexto de H.323, un IP basado en PBX es, en palabras sencillas, un Gatekeeper más algunos servicios suplementarios.

El estándar fue diseñado específicamente con los siguientes objetivos:

- Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931.

[11] LAN – Local Area Network
[12] RTP – Real Time Transport Protocol
[13] RDSI – Red Digital de Servicios Integrados
[14] QSIG – Protocolo de Señalización entre una centralita (PBX) en una Red Privada de Servicios Integrados.

- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.

- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

Los diseñadores de H.323 saben que los requisitos de la comunicación difieren de un lugar a otro, entre usuarios y entre compañías y obviamente con el tiempo los requisitos de la comunicación también cambian. Dados estos factores, los diseñadores de H.323 lo definieron de tal manera que las empresas que manufacturan los equipos pueden agregar sus propias especificaciones al protocolo y pueden definir otras estructuras de estándares que permiten a los dispositivos adquirir nuevas clases de características o capacidades.

H.323 establece los estándares para la compresión y descompresión de audio y vídeo, asegurando que los equipos de distintos fabricantes se intercomuniquen; así, los usuarios no se tienen que preocupar de cómo el equipo receptor actúa, siempre y cuando cumpla con este estándar.

Además la norma H.323 hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica. Por ejemplo, cuando se origina una llamada telefónica sobre Internet, los dos terminales deben negociar cual de los dos ejerce el control, de manera tal que sólo uno de ellos origine los mensajes especiales de control. Un punto importante es que se deben determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

A continuación se mencionan los protocolos más significativos para H.323:

RTP/RTCP (Real-Time Transport Protocol / Real-Time Transport Control Protocol):

Protocolos de transporte en tiempo real que proporcionan servicios de entrega de datos punto a punto.

RAS (Registration, Admission and Status):

Sirve para llevar a cabo procedimientos de registro, admisión, situación, cambio de ancho de banda entre puntos extremos (terminales, gateway, etc.) y el gatekeeper y estado de desconexión de los participantes.

Sólo se utiliza en zonas que tengan un gatekeeper. El canal de señalización RAS es independiente del canal de señalización de llamada, y del canal de control H.245. Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización RAS. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

H225.0:

Protocolo de control de llamada que permite establecer una conexión y una desconexión, el empaquetamiento de las tramas, la sincronización de tramas de medio y los formatos de los mensajes de control.

La función de señalización de la llamada H.225 utiliza un canal lógico de señalización para llevar mensajes de establecimiento y finalización de la llamada entre 2 puntos extremos H.323. El canal de señalización de llamada es independiente del canal de control H.245. Los procedimientos de apertura y cierre de canal lógico no se utilizan para establecer el canal de señalización. Se abre antes del establecimiento del canal de control H.245 y de cualquier otro canal lógico. Puede establecerse de terminal a terminal o de terminal a gatekeeper.

H.245:

Protocolo de control para comunicaciones multimedia, usado en el establecimiento y control de una llamada. Describe los mensajes y procedimientos

utilizados para abrir y cerrar canales lógicos para audio, video y datos, capacidad de intercambio, control e indicaciones.

Se utiliza el canal lógico de control H.245 para llevar mensajes de control extremo a extremo que rige el modo de funcionamiento de la entidad H.323. Se ocupa de negociar las capacidades (ancho de banda) intercambiadas, de la apertura y cierre de los canales lógicos y de los mensajes de control de flujo. En cada llamada, se puede transmitir cualquier número de canales lógicos de cada tipo de medio (audio, video o datos) pero solo existirá un canal lógico de control, el canal lógico 0.

H.450:
Describe los servicios suplementarios para transferencia, traspaso, retención, espera e identificación de llamadas.

H.235:
Describe la seguridad de H.323.

H.239:
Describe el uso de la doble trama en videoconferencia, normalmente una para video en tiempo real y la otra para presentación.

Q.931 (Digital Subscriber Signalling):
Este protocolo se define para la señalización de accesos RDSI básicos.

RSVP (Resource ReSerVation Protocol):
Protocolo de reserva de recursos en la red para cada flujo de información de usuario

T.120:
La recomendación T.120 define un conjunto de protocolos para conferencia de datos.

Entre los Códecs que recomienda usar la norma H.323 se encuentran principalmente:

G.711:
De los múltiples códecs de audio que pueden implementar los terminales H.323, este es el único obligatorio. Usa modulación por pulsos codificados (PCM) para conseguir tasas de bits de 56Kbps y 64Kbps.

H.261 y H.263:
Son los dos códecs de video que propone la recomendación H.323.

La función de señalización está basada en la recomendación H.225, que especifica el uso y soporte de mensajes de señalización Q.931/Q932. Las llamadas son enviadas sobre TCP iniciándose los mensajes de control de llamada Q.931 entre dos terminales para la conexión, mantenimiento y desconexión de llamadas.

Los mensajes más comunes de Q.931/Q.932 usados como mensajes de señalización H.323 son:

- Setup: Es enviado para iniciar una llamada H.323.
- Call Proceeding: Enviado por el Gatekeeper a un terminal advirtiendo del intento de establecer una llamada una vez analizado el número llamado.
- Alerting: Indica el inicio de la fase de generación de tono.
- Connect: Indica el comienzo de la conexión.
- Release Complete: Enviado por el terminal para iniciar la desconexión.

- Facility: Es un mensaje de la norma Q.932 usado como petición o reconocimiento de un servicio suplementario.

Función de control H.245

El canal de control H.245 es un conjunto de mensajes ASN.1 usados para el establecimiento y control de una llamada. Unas de las características que se intercambian son:

- Master Slave Determination (MSD): Este mensaje es usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación, decide quién actuará de Master y quién de Slave.

- Terminal Capability Set (TCS): Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

- Open Logical Channel (OLC): Mensaje para abrir el canal lógico de información y permite la recepción y codificación de los datos. Contiene la información del tipo de datos que serán transportados.

- Close Logical Channel (CLC): Mensaje para cerrar el canal lógico de información.

Figura 1.18: Pila de protocolos en VoIP (Voz sobre IP)

A continuación se analizará detalladamente una llamada H.323:

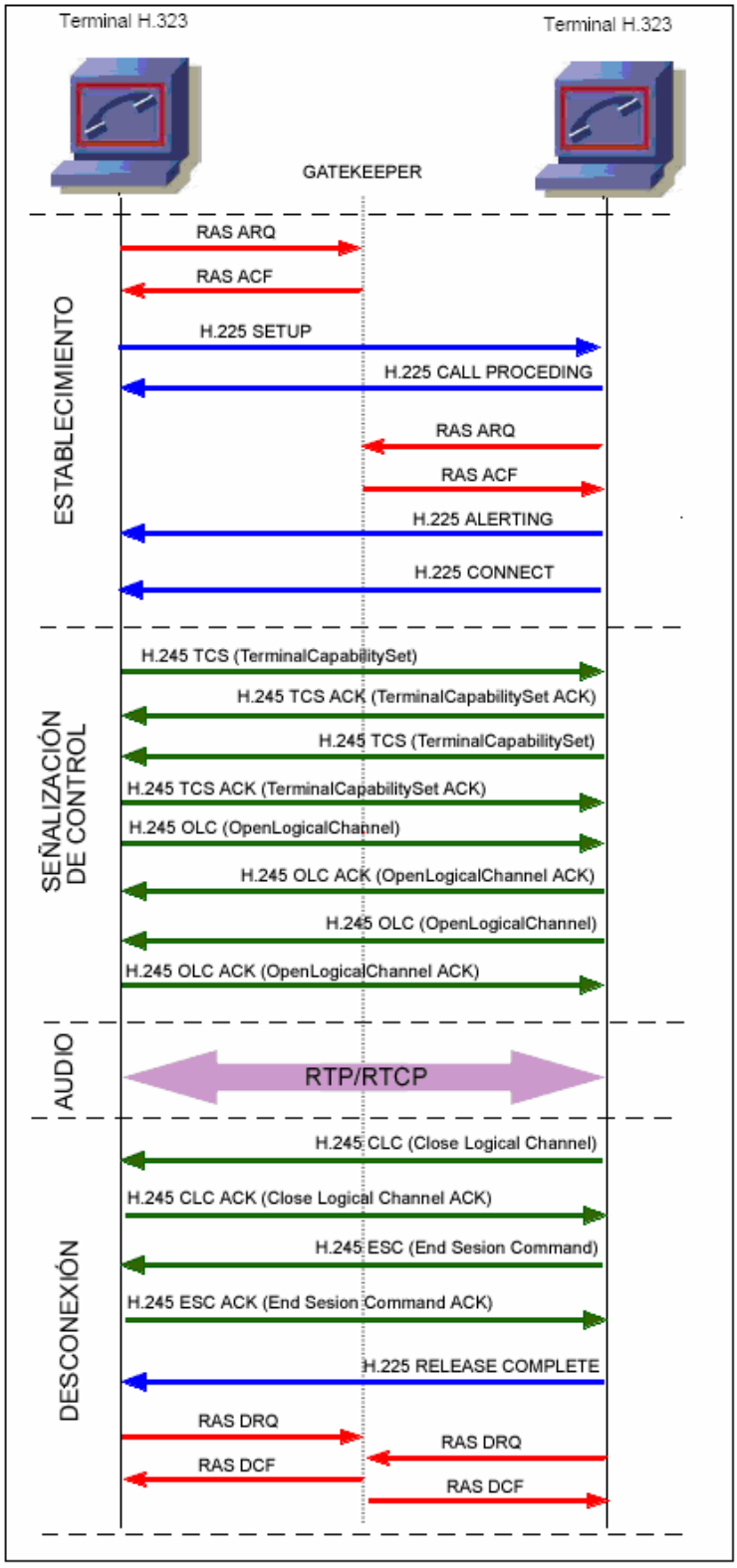


Figura 1.19: Llamada H.323

Una llamada H.323 se caracteriza por las siguientes fases:

1. ESTABLECIMIENTO

En esta fase lo primero que se observa es que uno de los terminales se registra en el gatekeeper utilizando el protocolo RAS[15] con los mensajes ARQ y ACF.

Posteriormente utilizando el protocolo H.225 (que se utiliza para establecimiento y liberación de la llamada) se manda un mensaje de SETUP para iniciar una llamada H.323.

El terminal llamado contesta con un CALL PROCEEDING advirtiendo del intento de establecer una llamada.

En este momento el segundo terminal tiene que registrarse con el gatekeeper utilizando el protocolo RAS de manera similar al primer terminal.

El mensaje ALERTING indica el inicio de la fase de generación de tono; y por último CONNECT indica el comienzo de la conexión.

2. SEÑALIZACIÓN DE CONTROL

En esta fase se abre una negociación mediante el protocolo H.245 (control de conferencia), sobre el intercambio de los mensajes (petición y respuesta), se establece cual de los terminales será Master y quién Slave y las capacidades de los participantes y Códecs de audio y video a utilizar. Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

3. AUDIO

Los terminales inician la comunicación y el intercambio de audio (o video) mediante el protocolo RTP/RTCP.

[15] RAS – Registro, Admisión y Estado

4. DESCONEXIÓN

En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes Close Logical Channel y End Session Comand de H.245.

Posteriormente utilizando H.225 se cierra la conexión con el mensaje RELEASE COMPLETE.

Por último se liberan los registros con el gatekeeper utilizando mensajes del protocolo RAS.

1.2.5.4.2 SIP

El protocolo SIP[16] fue desarrollado por el grupo MMUSIC[17] del IETF, definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero de 1996 en el RFC 2543, ahora obsoleto con la publicación de la nueva versión RFC 3261, en junio del 2002.

El propósito de SIP es la comunicación entre dispositivos multimedia, esto gracias a dos protocolos que son RTP/RTCP y SDP.

El protocolo RTP se usa para transportar los datos de voz en tiempo real, igual que para el protocolo H.323, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.

SIP fue diseñado de acuerdo al modelo de Internet, es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales (salvo el ruteo de los mensajes SIP).

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición

[16] SIP - Session Initiation Protocol
[17] MMUSIC - Multimedia Session Control

y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

Componentes

SIP soporta funcionalidades para el establecimiento y finalización de las sesiones multimedia: localización, disponibilidad, utilización de recursos, y características de negociación.

Para implementar estas funcionalidades, existen varios componentes distintos en SIP. Existen dos elementos fundamentales, los agentes de usuario (UA) y los servidores.

a. User Agent (UA): consiste de dos partes distintas, el User Agent Client (UAC) y el User Agent Server (UAS). Un UAC es una entidad lógica que genera peticiones SIP y recibe respuestas a las mismas; un UAS es una entidad lógica que genera respuestas a las peticiones SIP.

b. Los servidores SIP pueden ser de tres tipos:

Proxy Server: retransmiten solicitudes y deciden a qué otro servidor deben remitir, alterando los campos de la solicitud en caso necesario. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios. Este servidor tiene una funcionalidad semejante a la de un Proxy http, se encarga de encaminar las peticiones que recibe de otras entidades más próximas al destinatario. Existen dos tipos de Proxy Servers: Statefull Proxy y Stateless Proxy.

- Statefull Proxy: mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias, con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada.

- Stateless Proxy: no mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes.

Register Server: es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.

Redirect Server: es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor. La división de estos servidores es conceptual, cualquiera de ellos puede estar físicamente en una única máquina, la división de éstos puede ser por motivos de escalabilidad y rendimiento.

Mensajes

SIP es un protocolo textual que usa una semántica semejante a la del protocolo HTTP. Los UAC realizan las peticiones y los UAS retornan respuestas a las peticiones de los clientes. SIP define la comunicación a través de dos tipos de mensajes. Las solicitudes (métodos) y las respuestas (códigos de estado).

- Métodos SIP: Las peticiones SIP son caracterizadas por la línea inicial del mensaje, llamada Request-Line, que contiene el nombre del método, el identificador del destinatario de la petición (Request-URI) y la versión del protocolo SIP.

- Respuestas (Códigos de estado) SIP: Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor del mismo responde con un mensaje, este mensaje es similar al anterior, difiriendo en la línea inicial, llamada Status-Line, que contiene la versión de SIP, el código de la respuesta (Status–Code) y una pequeña descripción (Reason-Phrase). El código de la respuesta está compuesto por tres dígitos que permiten clasificar los diferentes tipos existentes.

Direccionamiento

Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres; normalmente, el agente de usuario no conoce la dirección IP del destinatario de la llamada, sino su email.

Las entidades SIP identifican a un usuario con las SIP URI[18]. Una SIP URI tiene un formato similar al del email, consta de un usuario y un dominio delimitado por una @, como muestran los siguientes casos:

- usuario@dominio, donde dominio es un nombre de dominio completo.
- usuario@equipo, donde equipo es el nombre de la máquina.
- usuario@dirección_ip, donde dirección_ip es la dirección IP del dispositivo.
- número_teléfono@gateway, donde el gateway permite acceder al número de teléfono a través de la red telefónica pública.

SDP

El protocolo SDP (Session Description Protocol) se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como SIP, SDP utiliza la codificación del texto; un mensaje SDP se compone de una serie de líneas, denominados campos, dónde los nombres son abreviados por una sola letra y están en un orden requerido para simplificar el análisis.

La Figura 1.20 muestra el proceso que lleva a cabo una llamada SIP:

[18] URI - Uniform Resource Identifiers

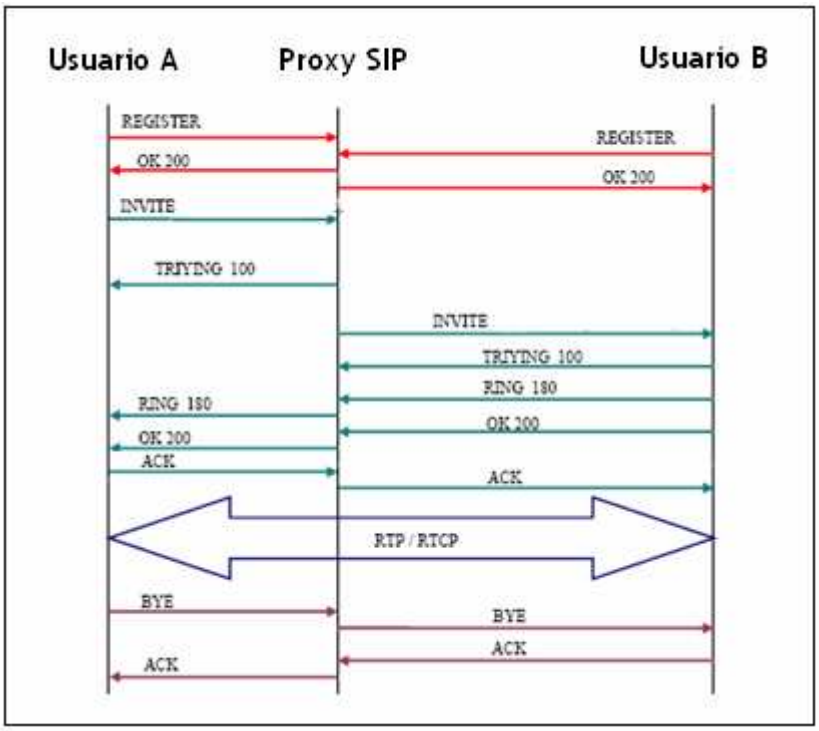


Figura 1.20: Llamada SIP

En la Tabla 1.1 se muestra una tabla de comparación entre los protocolos H.323 y SIP:

H.323	SIP
Protocolo Complejo	Protocolo mas Simple
Representación Binaria	Representación Textual
No demasiado modular	Muy Modular
No demasiado escalable	Muy Escalable
Muchos elementos	solo 37 cabeceras
Difícil detección de bucles	Fácil detección de bucles
Muy Extendido	Poco extendido

Tabla 1.1: Comparación entre H.323 y SIP

1.2.5.4.3 Megaco

Megaco o H.248 define el mecanismo necesario de llamada para permitir a un Media Gateway el control de puertas de enlace para soporte de llamadas de voz/fax entre redes RTC-IP o IP-IP.

Este protocolo está definido en el RFC 3525 y es el resultado del trabajo realizado por la IETF y la ITU.

Antes de la cooperación entre ITU e IETF, existían diversos protocolos que cumplían estas funciones; entre ellos se encontraban MDCP y MGCP.

H.248 es un complemento a los protocolos H.323 y SIP: se utilizará el H.248 para controlar las Media Gateways y el H.323 o SIP para comunicarse con otro controlador Media Gateway.

1.2.5.5 Arquitectura VoIP/H.323

H.323 define en su infraestructura los siguientes componentes más relevantes:

Terminal

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o MCU[19]. Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

Un terminal H.323 consta de las interfaces del equipo de usuario, el códec de video, el códec de audio, el equipo telemático, la capa H.225, las funciones de control del sistema y la interfaz con la red por paquetes.

a. Equipos de adquisición de información: Es un conjunto de cámaras, monitores, dispositivos de audio (micrófono y altavoces) y aplicaciones de datos, e interfaces de usuario asociados a cada uno de ellos.

[19] MCU - Unidad de Control Multipunto

b. Códec de audio: Todos los terminales deberán disponer de un códec de audio, para codificar y decodificar señales vocales (G.711), y ser capaces de transmitir y recibir ley A y ley μ. Un terminal puede, opcionalmente, ser capaz de codificar y decodificar señales vocales. El terminal H.323 puede, opcionalmente, enviar más de un canal de audio al mismo tiempo, por ejemplo, para hacer posible la difusión de 2 idiomas.

c. Códec de video: En los terminales H.323 es opcional.

d. Canal de datos: Uno o más canales de datos son opcionales. Pueden ser unidireccionales o bidireccionales.

e. Retardo en el trayecto de recepción: Incluye el retardo añadido a las tramas para mantener la sincronización y tener en cuenta la fluctuación de las llegadas de paquetes. No suele usarse en la transmisión sino en recepción, para añadir el retardo necesario en el trayecto de audio.

f. Unidad de control del sistema: Proporciona la señalización necesaria para el funcionamiento adecuado del terminal. Está formada por tres bloques principales: Función de control H.245, función de señalización de llamada H.225 y función de señalización RAS.

g. Capa H.225: Se encarga de dar formato a las tramas de video, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de red y de recuperarlos de los mensajes que han sido introducidos desde la interfaz de red. Además lleva a cabo también la alineación de trama, la numeración secuencial y la detección/corrección de errores.

h. Interfaz de red de paquetes: Es específica en cada implementación. Debe proveer los servicios descritos en la recomendación H.225. Esto significa que el servicio extremo a extremo fiable (por ejemplo, TCP) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada.

Gateway

Un gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

El Gateway dispone de uno o varios de las siguientes interfaces:

- FXO: Para conexión a extensiones de centralitas ó a la red telefónica básica.
- FXS: Para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M: Para conexión específica a centralitas.
- BRI: Acceso básico RDSI.
- PRI: Acceso primario RDSI.
- G703/G.704 (E&M digital): Conexión especifica a centralitas a 2 Mbps.

Gatekeeper

El gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El gatekeeper puede también ofrecer otros servicios tales como gestión del ancho de banda y localización de los gateways.

El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos, la primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN.

El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.

Además de las funciones anteriores, el Gatekeeper realiza los siguientes servicios de control:

- Control de admisiones: El gatekeeper puede rechazar aquellas llamadas procedentes de un terminal por ausencia de autorización a terminales o gateways particulares de acceso restringido o en determinadas franjas horarias.

- Control y gestión de ancho de banda: Para controlar el número de terminales H.323 a los que se permite el acceso simultáneo a la red, así como el rechazo de llamadas tanto entrantes como salientes para las que no se disponga de suficiente ancho de banda.

- Gestión de la zona: Lleva a cabo el registro y la admisión de los terminales y gateways de su zona.

MCU

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

Controlador Multipunto

Un controlador multipunto es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones. También puede controlar recursos de conferencia tales como multicasting de vídeo.

Procesador Multipunto

Un procesador multipunto es un componente de H.323 de hardware y software especializado, mezcla, conmuta y procesa audio, vídeo y / o flujo de datos para los participantes de una conferencia multipunto de tal forma que los procesadores del terminal no sean sobrecargados.

Proxy H.323

Un Proxy H.323 es un servidor que provee a los usuarios acceso a redes seguras de unas a otras confiando en la información que conforma la recomendación H.323. El Proxy H.323 se comporta como dos puntos remotos H.323 que envían mensajes call - set up, e información en tiempo real a un destino del lado seguro del firewall.

Además existen ciertos elementos, los cuales son también necesarios y permitirán construir las aplicaciones VoIP. Estos elementos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Servicios de Directorio.

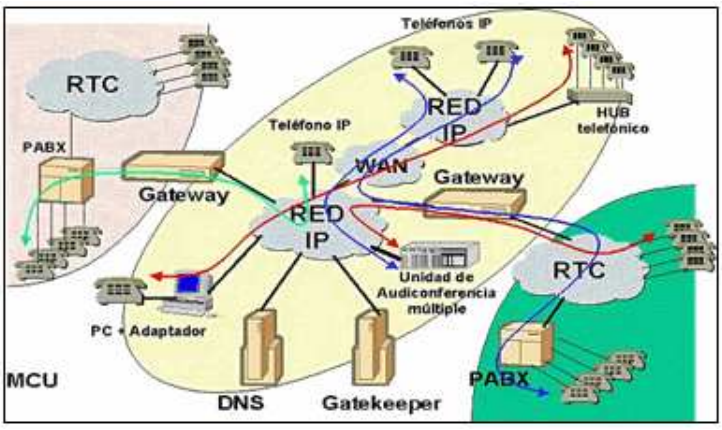


Figura 1.21: Arquitectura VoIP/H.323

1.2.5.6 Calidad del Servicio (QoS)

Este es el principal problema que presenta hoy en día la implantación tanto de VoIP como de todas las aplicaciones IP. Garantizar la calidad de servicio sobre una red IP, en base a retardos y ancho de banda, actualmente no es posible, es por eso que se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

La calidad de servicio se está logrando en base a los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda.

- Compresión de cabeceras aplicando los estándares RTP/RTCP.

- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:

  CQ (Custom Queuing): Asigna un porcentaje del ancho de banda disponible.

  PQ (Priority Queuing): Establece prioridad en las colas.

  WFQ (Weight Fair Queuing): Se asigna la prioridad al tráfico de menos carga.

  DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.

- La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

Anchos de Banda

En la tabla adjunta se muestra la relación existente entre los distintos algoritmos de compresión de voz utilizados y el ancho de banda requerido por los mismos:

VoCodecs	Ancho de Banda (BW)
G.711 PCM	64 kbps
G.726 ADPCM	16, 24, 32, 40 kbps
G.727 E-ADPCM	16, 24, 32, 40 kbps
G.729 CS-ACELP	8 kbps
G.728 LD-CELP	16 kbps
G.723.1 CELP	6.3 / 5.3 kbps

Tabla 1.2: Relación entre los Códecs de Voz y el Ancho de Banda que requiere cada uno

Retardo

Una vez establecidos los retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

1.2.5.7 Ventajas y Desventajas que presenta la solución de VoIP con respecto a la telefonía tradicional

1.2.5.7.1 Ventajas

- Un único número de teléfono: Casi como un celular. Permite tener un número de teléfono local que transfiera las llamadas a cualquier parte del mundo.

- Ahorro en llamadas de larga distancia: Las mayores ventajas que verá un usuario es la del ahorro en las llamadas de larga distancia, ya que las comunicaciones no dependerán del tiempo en el aire, es decir, no dependerá de la duración de la llamada, como estamos acostumbrados hasta ahora, sino más bien por el precio de mercado

del proveedor de Internet, ya que se estará pagando por un servicio más, dentro del paquete de datos que nos brinda la red.

- Reducción del abono telefónico: Además, para el usuario común, este sistema reduce los costos de las llamadas (hasta un 74%), cuyo precio depende del mercado pero no del tiempo de conexión, como sucede en la telefonía tradicional.

- Mensajería unificada y Correo de voz: Tiene la capacidad de proporcionar en el computador, un listado de mensajes de voz. Además permite realizar llamadas telefónicas y enviar faxes a través de una red de datos IP como si estuviese utilizando una red tradicional.

- Interoperabilidad de diversos proveedores.

- Uso de las redes de datos existentes.

- Independencia de tecnologías de transporte (capa 2), asegurando la inversión.

- Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay).

1.2.5.7.2 Desventajas

- Calidad de la comunicación: Algunas de sus desventajas son la calidad de la comunicación (ecos, interferencias, interrupciones, sonidos de fondo, distorsiones de sonido, etc.), que puede variar según la conexión a Internet y la velocidad de conexión del Proveedor de servicios de Internet. Garantizar la calidad de servicio sobre una red IP, actualmente no es posible por los retardos que se

presentan en el tránsito de los paquetes y los retardos de procesado de la conversación. Por otro lado el ancho de banda el cual no siempre está garantizado, hace desmejorar el servicio. Estos problemas de calidad en el servicio telefónico en el protocolo IP van disminuyendo a medida que las tecnologías involucradas van evolucionando, ya en los Estados Unidos hay servicios que garantizan una excelente calidad en la comunicación.

- Conexión a Internet: Sólo lo pueden usar aquellas personas que posean una conexión con Internet, tengan computadora con módem y una línea telefónica; algunos servicios no ofrecen la posibilidad de que el computador reciba una llamada, ni tampoco funcionan a través de un servidor proxy.

- Pérdida de información: Este tipo de redes transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de uno de ellos. Estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación, imaginemos una conversación de voz en la cual se pierde de vez en cuando información emitida y que sufre retrasos importantes, a veces durante conversaciones de Chat, recibimos dos o tres preguntas seguidas de nuestro interlocutor, debido a que lo que nosotros escribimos no ha llegado aún.

- Incompatibilidad de proveedores del servicio: No todos los sistemas utilizados por los Proveedores de Servicios de Telefonía por Internet son compatibles (Gateway, Gatekeeper, etc.) entre sí, este ha sido uno de los motivos que ha impedido que la telefonía IP se haya extendido con mayor rapidez. Actualmente esto se está corrigiendo, y casi todos los sistemas están basados en el protocolo H.323.

CAPITULO II

USO DE VOZ SOBRE IP (VoIP) COMO MECANISMO DE FRAUDE

2.1 INTRODUCCIÓN

Mientras que para ahorrar costos el mundo de los negocios abraza rápidamente la tecnología VoIP (Voz sobre IP), poca atención se está dando a los nuevos peligros que se introducen en las redes telefónicas.

Muchos negocios están actualmente sustituyendo o analizando sustituir su infraestructura de telefonía interna para recortar costos; incluso las compañías de telecomunicaciones, aunque a la expectativa de lo que hará VoIP al flujo de réditos, están transfiriendo con impaciencia mucho de su tráfico de red telefónica conmutada, espina dorsal de la red pública telefónica, a la tecnología VoIP.

Pero casi todos estos nuevos despliegues de VoIP están ocurriendo sin la debida atención al tema de la seguridad, lo que podría afectar seriamente a estas compañías y a los consumidores.

Los verdaderos costos de la VoIP y la exposición creciente a serios riesgos en la seguridad, pueden empequeñecer los ahorros ganados al reducir los cargos de las llamadas.

Internet y PSTN están convergiendo sin que se preste ninguna atención para asegurar las interconexiones, un hecho del cual los piratas informáticos están extremadamente concientes y ya están explotando activamente.

Ya existen herramientas disponibles en Internet, que proporcionan la capacidad

para estos ataques, y es solamente cuestión de tiempo antes de que se empaqueten para los atacantes menos expertos y así se conviertan en algo común.

Pero lo realmente alarmante no es justamente que los ataques sean posibles, sino que, si esos ataques están ocurriendo ya, nadie podría saberlo debido a la poca seguridad en la mayoría de los despliegues de VoIP.

En este capítulo se realizará un análisis de los diferentes tipos de fraude, dándole un mayor énfasis a aquellos realizados mediante la tecnología de Voz sobre IP, así como a las técnicas usadas para su detección, corrección y prevención.

2.2 FRAUDE – DEFINICIÓN [3]

Por fraude se entiende la acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete. Acto cumplido intencionalmente tendiente a eludir, herir o menoscabar disposiciones legales o derechos del Estado o de terceros. Engaño que se realiza eludiendo obligaciones legales o usurpando derechos con el fin de obtener un beneficio.

Las telecomunicaciones al ser una base tecnológica que recorre transversalmente cualquier actividad humana, no están exentas de que a través suyo se cometan diversos fraudes. Esto afecta a todos los prestadores de servicios de telecomunicaciones y, potencialmente, a todos los usuarios. Por ende, es importante que esta temática sea tratada de manera integral por los diferentes actores del sector.

Como prestadores de servicios, como reguladores y, en general, como actores activos y usuarios en el sector de las telecomunicaciones, tenemos la muy importante tarea de asumir el papel histórico de minimizar todos los focos que pongan en riesgo y/o en entredicho la capacidad sectorial de lucha en contra del fraude, que año tras año causa grandes pérdidas al sector y pone en riesgo el futuro de las empresas y de la obtención de los recursos necesarios para la realización de los planes de Universalidad del servicio por parte de los Estados, especialmente de los más pobres.

En general, el fraude afecta a todos los operadores de telecomunicaciones y prestadores de servicios e impacta directamente sobre los ingresos de las empresas. Las pérdidas generadas por las diferentes modalidades de fraude afectan directamente el costo operacional de los servicios. Puede afectar a los clientes, dificulta la eficiencia operacional y a la imagen corporativa de las compañías.

Diversas fuentes calculan que las compañías pierden cerca del 10% de sus ingresos por falta de herramientas tecnológicas y de procedimientos para el

control del fraude y aseguramiento de ingresos, que con los actuales márgenes de ganancia comprometen la supervivencia de las compañías.

En una encuesta realizada por la CFCA[20] a diversas compañías en 26 países, el 80% de las compañías contestaron que las pérdidas por fraude se habían incrementado y el 45% contestaron que había tendido a incrementar el fraude dentro de ellas.

Por otro lado, el continuo cambio de tecnología que está sufriendo el sector de las telecomunicaciones que va hacia la integración y convergencia de las redes que junto a tecnologías como IP hacen que exista gran cantidad de servicios sustitutos, exigen que sea necesario estudiar la migración hacia estas redes y los posibles impactos económico, social, de imagen y de seguridad en las compañías prestadoras de estos servicios.

Históricamente, el fraude en telecomunicaciones empezó desde el inicio de las redes; siempre ha estado alineado en dos vertientes: aquellos que buscan tener satisfacción por violar sistemas (hackers) y no buscan tomar partido de este ilícito y aquellos que quieren aprovechar las vulnerabilidades de las redes para obtener beneficios generalmente económicos derivados de su accionar.

1.2.1 RAZONES

1. Evolución de la industria

    - A partir de los años 90, el tráfico telefónico en el mundo sigue creciendo, pero a través de la telefonía móvil e Internet, tecnologías más vulnerables al fraude que la fija.

    - La apertura comercial, la privatización de los servicios y la falta de legislación.

[20] CFCA - Communications Fraud Control Association

- La evolución tecnológica, cuya razón de cambio es mucho mayor que la de la legislación.

2. La movilidad, la cual dificulta la identificación y ubicación del usuario

- A diferencia del cliente del servicio fijo (siempre es posible ubicarlo), el del móvil es más propenso a dejar cuentas sin pagar.

- La telefonía móvil estimula el fraude de suscripción (a través de documentos falsos), al facilitar el mentir respecto a la información personal.

3. La convergencia tecnológica

- La interconexión de prácticamente todas las redes del mundo, a través de la Internet, facilita y amplía las posibilidades de fraude.

- A futuro tendremos aun más integración de servicios (cuádruple play, por ejemplo), por lo que los riesgos crecen.

- La falta de legislación adecuada. A futuro en el Ecuador, incluso es necesario integrar en una sola legislación, la regulación de las “comunicaciones electrónicas”, como ya lo han hecho en Europa.

2.3 FRAUDES A LAS PLATAFORMAS E INFRAESTRUCTURA DE PRESTACIÓN DEL SERVICIO. (USO FRAUDULENTO DEL SERVICIO CON INTENCIÓN DE NO PAGO O QUE ESTE APAREZCA FACTURADO A UN TERCERO).

1.2.1 FRAUDE INTERNO

Los esfuerzos y recursos de los departamentos de fraude dentro de la industria de telecomunicaciones, están fuertemente concentrados en combatir los ataques desde fuentes externas, y el fraude interno raramente recibe la atención que se merece.

Debido a su conocimiento de expertos de los sistemas y procesos, los empleados de las empresas de telecomunicaciones están idealmente capacitados para llevar a cabo ataques a la red; dado que se trata de una especialización que requiere trabajar en muchas áreas del negocio, a menudo puede ser muy simple para el perpetrador esconder o encubrir sus actividades.

La metodología tradicional utilizada para la detección de fraude ha tendido a focalizarse en la actividad del usuario y en la información de la llamada, este enfoque permite la detección del fraude y normalmente entrega clasificaciones simples de los problemas de uso, pero a menudo no destaca la causa radical del problema, por consiguiente pasa por alto las implicaciones internas, permitiendo un mayor abuso.

El fraude interno es uno de los tipos de fraude más intangible, esto es porque puede ocurrir en cualquier parte dentro de los procesos de la organización, tales como: en el sistema de incorporación de clientes, en las plataformas de prepago, en la administración de servicios de facturación, en las base de datos de clientes y en las plataformas de administración de pagos.

Puede tomar la forma de: alteraciones en los detalles de facturación de un

individuo, creación de cuentas falsas, acceso a los detalles de una tarjeta de crédito, daños en elementos de la red, activación de virus o ataques Troyanos, etc.

A continuación se detallan las modalidades de fraude interno más comunes:

1.2.1.1 Acceso a las plataformas y programación de servicio a usuarios que no tienen suscripción o con suscripción inactiva

Corresponde a un tipo de fraude telefónico interno. Se da debido a que en las centrales telefónicas se encuentran líneas libres o sin asignar, ya sea por reserva técnica o porque no han sido asignadas a usuarios. La línea se activa temporalmente para realizar llamadas por parte del personal interno de la planta o para ser vendida de forma ilegal a terceras personas.

Cuando se implementa una red telefónica, se instala una capacidad estimada de líneas dependiendo de la demanda esperada en cada zona. La activación de una línea se realiza mediante comandos de software en la central y de manera lógica se le da tono; además, en el MDF[21] se hace la conexión hacia la red externa en la troncal correspondiente a la zona de residencia del usuario.

Las líneas que se encuentran libres, es decir, aquellas que no han sido asignadas a ningún usuario deben estar sin programación en la central y sin conexión en el distribuidor. Si esta línea se activa, el consumo que se realice no podrá ser cobrado a nadie ya que no está asignada a ningún usuario y el consumo se genera como inconsistencia en el sistema de facturación.

Detección y corrección

En el sistema de facturación se generan inconsistencias al aparecer líneas no asignadas con consumo. Se deben realizar visitas de campo por parte del personal técnico especializado, con el fin de identificar el sitio exacto del fraude.

[21] MDF - Main Distribution Facilities - Armario de distribución principal o punto de control central de la red

Prevención

Con el fin de minimizar el impacto, las empresas deben realizar periódicamente una comparación de usuarios y/o abonados inscritos en su sistema de facturación versus abonados activos en las centrales telefónicas, posteriormente a esa comparación se detectan las respectivas alarmas por inconsistencias.

1.2.1.2 Manipulación de información

Este es un tipo de fraude interno, que se realiza a través del acceso a las plataformas de facturación para borrar y/o alterar registros de uso del servicio.

Se modifica la información de la base de datos de los clientes como nombres y direcciones, de tal manera que es imposible realizar el cobro de las facturas. También se pueden cambiar los datos de consumo en los sistemas de facturación, modificar la categoría de abonados en las centrales o el árbol de la ruta para evitar el cobro de las llamadas realizadas por un usuario o grupo de usuarios. También se puede vender información confidencial de la Compañía, mediante intromisión a los sistemas de información, rompiendo los niveles de seguridad de la red empresarial.

Detección y corrección

Debido a que los procesos de facturación se realizan de manera mensual en la mayoría de las empresas de telecomunicaciones, el seguimiento continuo es muy difícil de llevar a cabo. En una empresa con una gran cantidad de suscriptores es una tarea aún más compleja.

Uno de los primeros síntomas de que este fraude puede estar presentándose es en la comparación de la utilización de servicios reportados por las centrales y los servicios que se están facturando a los clientes que consumen dichos servicios. Las centrales reportan sus datos de utilización y estos son comparados con la

facturación creada para los clientes de dicha central, si los valores son inconsistentes, se pueden estar presentando problemas en las bases de datos que manejan esta información. Con base a los datos encontrados, se empieza a realizar la verificación de los clientes que pueden presentar dichas inconsistencias y una vez detectados, se verifica la configuración de la tasación del cliente para detectar si las inconsistencias fueron creadas o existen problemas con el modo en que se realiza la tasación.

Otra forma de detección se da cuando se encuentran cambios en los sistemas de tasación, facturación y recaudo de las centrales, por auditorías sobre los mismos.

Prevención

Para prevenir esta clase de inconvenientes, la empresa debe seleccionar muy bien el personal que tendrá a cargo dichas labores. A su vez, se pueden establecer auditorías externas, a cargo de la verificación de facturación y de los procesos de tarifación, para que de esta forma, se pueda estar atento a cualquier inconveniente que se pueda estar presentando.

Internamente se deben realizar verificaciones continuas sobre la integridad de la información que almacena la facturación de los clientes, así como el estado de los árboles de tasación en las centrales.

En algunas compañías, se tienen backups de las bases de datos que contienen dicha información, que permiten tener un respaldo en caso de daño o corrupción de las mismas. Estos backups deben tener un cuidado especial, que garantice que no sean manipulados mientras se encuentran almacenados.

1.2.1.3 Uso y venta de facilidades asignadas por las compañías para usufructo de terceros

Es un tipo de fraude telefónico interno, en el cual, se usan líneas de la Compañía

para la realización de llamadas de larga distancia. Las mencionadas líneas tienen la facilidad de llamada en conferencia para tramitar llamadas entre terceros. Estas llamadas son cargadas a las líneas de la Compañía.

Detección y corrección

En compañías grandes es difícil la detección de este tipo de fraudes y/o uso indebido de las facilidades de telecomunicaciones, debido al frecuente uso que se da a los servicios de telecomunicaciones por los usuarios. Un modo usado para la detección es verificar periódicamente el comportamiento de cada uno de los usuarios y generando la respectiva alarma cuando el comportamiento es atípico.

Prevención

Sistemas actuales de PBX, tienen la facilidad de bloquear diferentes destinos; para este caso, es conveniente asignar claves a los usuarios terminales de tal forma que se puedan asociar las llamadas a un código preestablecido.

1.2.2 FRAUDE EXTERNO

El fraude externo se asocia a todos aquellos hechos que personas ajenas a las compañías de telecomunicaciones realizan con el fin de obtener algún beneficio, ya sea personal o económico. Debido a la constante evolución tecnológica, las compañías de telecomunicaciones se han visto en la obligación de contar con departamentos especializados en analizar las actividades que puedan ser consideradas fraudulentas. Las tareas realizadas por estos departamentos en cada país y compañía varían dependiendo de las legislaciones existentes, en las cuales existe disparidad debido a que los entes estatales encargados de establecer estas legislaciones no van a la par con el desarrollo tecnológico, en algunos países, se han creado entes especializados con el fin de que sean estos organismos los que regulen las actividades en telecomunicaciones.

Ahora con los nuevos servicios de las redes de telecomunicaciones en un entorno completamente convergente, se predice la explosión de nuevas modalidades, dentro de las cuales se encuentran la piratería de software, suplantación de identidades de personas naturales y jurídicas (ejemplo: phishing o vishing (si se usa voz sobre IP)), terrorismo electrónico, dialers, virus informáticos, spyware, “By Pass”, Callback, Refilling, etc.

A continuación se detallan las modalidades de fraude externo más comunes:

1.2.2.1 Fraude de suscriptor

Se presenta cuando se utiliza documentación falsa o de terceros con la finalidad de que los cargos y la facturación se registren a nombre de otra persona. Por lo general, cuando se adquieren servicios de telefonía, el defraudador consume lo máximo posible y posteriormente se retira del local arrendado.

Afecta directamente a la (s) persona (s) suplantada(s) quienes son reportadas como usuario(s) moroso(s) a las centrales de riesgo y a bases de datos en el sector financiero. Por otro lado, la compañía de telecomunicaciones se ve afectada por pérdida de ingresos al no poder cobrar los consumos realizados, aumento en los reclamos, aumento de los costos, etc.

Detección y Corrección

La empresa debe contar con un departamento especializado en la recepción de documentos, el cual debe estar en la capacidad de detectar cuando un suscriptor esta tratando de contratar servicios con documentos falsos.

Prevención

La forma en que las empresas realizan la suscripción de sus clientes debe tener en cuenta los posibles fraudes que se puedan cometer. Aunque las modalidades en las que se comete el fraude cambian de acuerdo a los requerimientos que se

imponen, es importante establecer parámetros que permitan evitar al máximo ser víctimas de los defraudadores.

Se pueden establecer pautas para el control de este fraude, entre las cuales tenemos:

a) Contar con personal idóneo para la verificación de los documentos entregados por los clientes, capacitados en la detección e identificación de documentos falsos o adulterados.

b) Establecer requerimientos mínimos para la suscripción de clientes, dependiendo del tipo de servicio que se esté solicitando. Dichos requerimientos deben tener en cuenta el tipo de cliente que se va a manejar (corporativo, bancario, personal), el valor que facturará en promedio y el tipo de tráfico que va a manejar.

c) Realizar la verificación de los documentos entregados por los clientes. Dicha verificación se puede realizar ante autoridades civiles, centrales de riesgo y bases de datos propias de la compañía.

Para efectuar un análisis preventivo más detallado, tener en cuenta:

a) Verificar la consistencia de los datos:

- Nombres y Apellidos del solicitante y representante legal.
- Dirección de instalación, de cobro y revisión de puntos sucursales del negocio.
- Fecha de constitución de la empresa.
- Objeto social y uso del servicio.
- Tipo de letra sea el mismo en todo el documento.

b) Validar en el formato de la suscripción que todos los datos se diligencien de forma correcta (sin tachones y/o enmendaduras), teniendo en cuenta:

- Huella de la suscripción y cédula.
- Consistencia de los nombres y apellidos del solicitante con la cédula de ciudadanía.

c) En la Cédula de ciudadanía:

- Verificar la autenticidad del documento y veracidad de la identidad.
- Revisar con el documento original que la foto corresponda a la de la persona que solicita el servicio.
- Garantizar que la fotocopia que se entregue sea del documento original.

1.2.2.2 Uso de pines de tarjetas o claves de servicios especiales para realizar llamadas

Es un tipo de fraude telefónico externo, el cual se da cuando una persona se encuentra realizando una llamada desde un teléfono público haciendo uso de una tarjeta prepagada o de un servicio especial, el defraudador se acerca y observa los números digitados. De forma inmediata, los números son vendidos en el mercado negro para realizar llamadas con cargo a la tarjeta o servicio especial del cliente.

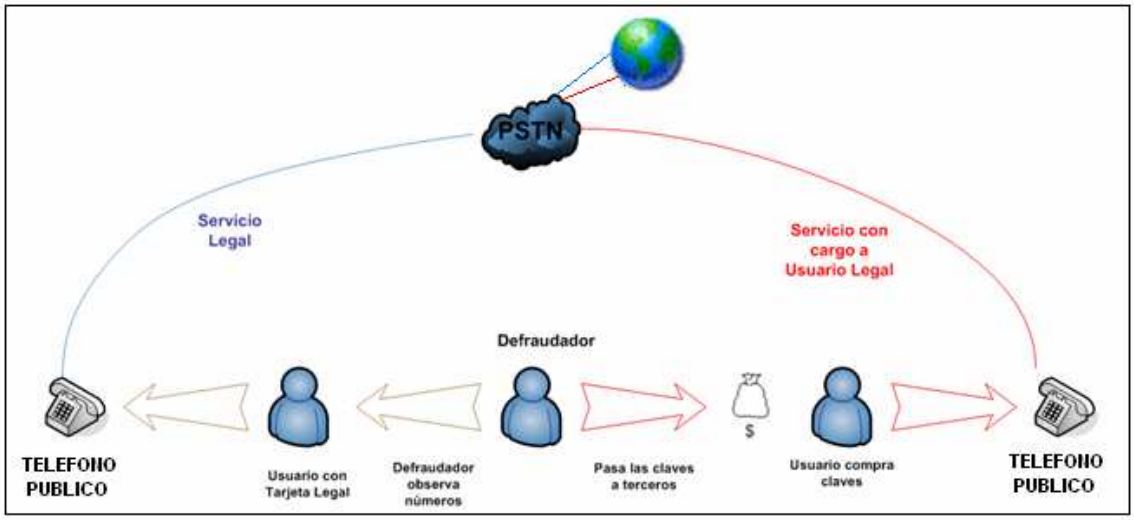


Figura 2.1: Uso de pines de tarjetas o claves de servicios especiales para realizar llamadas

Entre las formas de obtención están: la observación detallada del cliente cuando esta digitando o marcando las claves, a través de email induciendo a los clientes a enviar sus nombres de usuarios y passwords por este medio o en chats en línea donde los defraudadores engañan a las personas para la obtención de las claves.

Detección y corrección

Este tipo de fraude es, en la mayoría de los casos detectado por el reclamo de los clientes, quienes reportan llamadas no realizadas o servicios no utilizados con cargo a su cuenta, por terminación anticipada del cupo de su tarjeta prepagada, etc. Las compañías no pueden realizar un seguimiento exhaustivo de estos servicios ya que en la mayoría de las ocasiones, dichos servicios se realizan a través de conexiones remotas, desde distintos puntos geográficos, lo que imposibilita dicho seguimiento.

Una vez que las empresas son notificadas por parte de los usuarios, cambian las claves para evitar que se siga usando el servicio, pero ya se realizó un cargo al mismo, el cual la empresa no asume.

Prevención

Para prevenir este problema, se pueden tener en cuenta las siguientes recomendaciones, con el fin de minimizar los efectos de este fraude:

- Precaución al usar los servicios de la tarjeta en sitios públicos.
- Política de cambio de contraseñas.
- Acuerdo de confidencialidad.
- Asegurar el entendimiento por parte de los usuarios de las normas a aplicar.

1.2.2.3 Fraude en Audiotexto

Los servicios de audiotexto son aquellos que permiten al usuario tener acceso a bases de datos o a contenidos de diversa naturaleza por medio de servicios finales, que generalmente se prestan a través de las redes inteligentes de las operadoras de telefonía y se acceden mediante códigos 1-900.

Los servicios de Audiotexto, servicios de números de tarifas altas y servicios de ingresos compartidos, entregan en la actualidad la oportunidad para uno de los tipos de fraude de más rápido crecimiento en telecomunicaciones.

Los servicios de Audiotexto son, normalmente, muy simples de implementar por un individuo y pueden ser realizados sin interacción directa con la red, a través de alianzas de negocios, distribuidores o agentes especializados. Esto significa que se provee acceso a estos servicios sin ningún control real.

Se realizan llamadas para acceder al servicio, con el único objetivo de aumentar los ingresos para el dueño del mismo. Las líneas mediante las cuales se accede al servicio han sido previamente adquiridas mediante fraude de suscripción, con el fin de evitar el pago por el consumo de las mismas.

Estos servicios son particularmente atractivos para grupos delictivos organizados debido al potencial de generación de ingresos sustanciales con la mínima cantidad de tiempo y esfuerzo. A menudo el fraude en Audiotexto puede tener un doble impacto para la red: existe el ingreso no recaudado de las cuentas utilizadas para acceder el servicio, además de las cantidades que hay que pagar a los proveedores de las interconexiones.

Con el fin de entender como ocurre el fraude en servicios de Audiotexto, es necesario entender como funcionan en realidad los servicios de Audiotexto y el sistema de pagos involucrados.

Hay tres aspectos principales del fraude dentro de los servicios de Audiotexto:

- Abultamiento Artificial del Tráfico (AAT): cuando el nivel de llamadas a un servicio de Audiotexto es deliberadamente incrementado con el fin de aumentar el flujo de ingresos para el dueño del servicio

- Arbitraje: la manipulación o el evitar los pagos dentro del flujo de interconexiones entre los operadores

- Abuso con las llamadas: el intentar evitar los pagos por acceder números de servicios de Audiotexto

Es importante tener presente que el fraude en Audiotexto es una falta secundaria en la red, considerando que el defraudador tuvo que haber cometido un fraude primario, tal como un fraude de suscripción, para tener acceso a la red.

Detección y Prevención

Es importante el ser capaz de diferenciar y clasificar los servicios de Audiotexto, dentro del procesamiento de datos del sistema de administración de fraude. Esto entrega al operador la habilidad de detectar y prevenir rápida y exactamente este tipo de fraude. Sin embargo, es importante que el sistema realice esta tarea de una forma avanzada, no solamente basado en las tarifas de las llamadas o en el volumen de las mismas.

1.2.2.4 Fraude en Roaming

El Fraude en Roaming es el uso de un servicio móvil de un operador, mientras el usuario está fuera del país de "origen", sin la intención de pagar por las llamadas realizadas. El fraude en roaming es normalmente un fraude secundario, siendo el fraude de suscripción, el fraude primario, es decir, el defraudador tiene que obtener primero una suscripción a una red, utilizando identidades falsas o robadas.

El problema principal es el retardo en la transferencia de los registros de llamadas, entre las partes involucradas en el servicio roaming, este retardo puede significar hasta 72 horas antes que la red de origen reciba la información (en casos extremos, esto puede llegar a ser semanas). Este retardo en el monitoreo crea una ventana de oportunidad para el defraudador, y en ataques organizados, las pérdidas pueden ser extremadamente significativas.

Estimaciones de algunos sectores del mercado mundial indican que actualmente el Fraude de Roaming representa alrededor del 50% del fraude en GSM. Los operadores no solamente obtienen pérdidas por los ingresos no recaudados de las cuentas utilizadas para acceder el servicio, sino que también sufren pérdidas por el dinero que están obligados a pagar a sus socios de Roaming.

Las pérdidas continúan incrementándose a medida que se van creando nuevas empresas y no hay avances reales o que se logren acuerdos en términos de transferir registros de las llamadas en tiempo real.

El fraude se da cuando una vez en el extranjero, el usuario utiliza el servicio para llamar a otros destinos internacionales o a servicios de audiotexto ("premium rate services") con la intención de no pagar por ellos. Aunque en algunos casos involucran a individuos oportunistas, los casos más importantes son cometidos por organizaciones delictivas, quienes utilizan múltiples suscripciones fraudulentas para llevar acabo el ataque.

El servicio de roaming es muy atractivo para el defraudador: el servicio es relativamente simple de obtener (a menudo es un servicio estándar, incluido con la conexión); ofrece un potencial de altas ganancias (debido a los altos costos de las llamadas el acceso a la red puede ser revendido o utilizado en operaciones de audiotexto); y los retardos en la transferencia de la información entre los entes involucrados en el servicio de roaming, ayuda al defraudador a escapar de la detección.

Detección y Corrección

Cuando un suscriptor utiliza su teléfono en la red de otro operador, tiene lugar un proceso de autenticación, vía señalización SS7[22], entre la red visitada y la red de origen. De este requerimiento de autenticación, se puede extraer el país y la red que el suscriptor está visitando. Esta información es invaluable en la identificación del suscriptor que está haciendo roaming sin haber generado llamada alguna en la red de origen, lo cual es un fuerte indicador de fraude.

Se puede además realizar triangulaciones de autentificaciones y actualizaciones de ubicación, si un suscriptor continua realizando llamadas.

Prevención

La respuesta radica en enfrentar la causa que lo origina. La mayoría de los fraudes de roaming se originan como fraude de suscripción, por lo tanto, el impedir a los defraudadores obtener el servicio al inicio, es claramente el método más efectivo.

Para defraudadores que se las arreglan para deslizarse más allá de los mecanismos de control de llamada, se puede llevar a cabo el análisis de CDR's y la información de autenticación de roaming.

1.2.2.5 Robo de líneas telefónicas

Este tipo de fraude puede ser interno o externo, se da cuando líneas activas con asignación a usuarios son cambiadas de domicilio sin autorización del suscriptor o de la empresa local proveedora del servicio.

Es uno de los fraudes más comunes por la facilidad de cometerlo en cualquier punto de la red externa. Generalmente esto es realizado por personal de

[22] SS7 – Sistema de señalización por canal común N° 7

mantenimiento, instaladores de planta externa o por ex-funcionarios de la compañía que conocen la distribución de la red.

Las líneas telefónicas son utilizadas por terceros y el consumo es cobrado al suscriptor del servicio.

La acometida de la red externa al domicilio del suscriptor es más vulnerable cuando es aérea, puede ser robada desconectando el cable del domicilio y llevándolo a otro lugar, también puede realizarse en un armario al desconectar el par del abonado y empatarlo con otro que va hacia otro lugar, o entrar a una caja y romper la protección del cable troncal, derivar un cable y conectarlo a otro del mismo cable troncal que va hacia el domicilio del defraudador.

En sitios cerrados como edificios, se ingresan cables multipares que convergen en una caja ubicada en el sótano “strip telefónico”, desde este punto se reparten las líneas de abonado mediante multipares, el infractor conecta o deriva un par telefónico en cualquiera de los puntos y/o regletas instaladas en cada uno de los pisos del edificio y usualmente cambia constantemente el abonado que está derivando.

La compañía prestadora del servicio se ve afectada ya que se produce un daño en la infraestructura y existe un aumento de reclamos por parte de los clientes. De igual forma este tipo de fraude impacta directamente a la buena imagen de la compañía ante los clientes.

El usuario se ve afectado ya que cuando no se logra comprobar un fraude y/o uso indebido de la línea telefónica por parte de un tercero, debe pagar el monto total del consumo realizado por el defraudador.

Detección y corrección

El usuario realiza un reclamo por daño en la línea, y al verificarlo desde la central telefónica el abonado aparece activo; al realizar la revisión de la red externa se

encuentra la derivación o el traslado no autorizado. De igual forma, cuando un usuario que sea víctima de un robo reiterado y notorio (llamadas a larga distancia internacional, larga duración, alto coste, etc.), lo reporte al servicio de reclamos de la compañía.

Se debe realizar una demanda penal contra la persona que realizó la derivación. Si la derivación ocurrió en la acometida interna, deberá hacerlo el usuario ya que el debe responder por las llamadas realizadas a la Compañía, si es en cualquier otro punto de la red, el usuario no debe pagar los consumos realizados de manera fraudulenta y será la Compañía la que deberá actuar contra el defraudador.

Prevención

Controlar las llamadas que se han hecho una a una, primero buscar las de larga duración, luego las de larga distancia y por último las que se repiten varias veces. Es importante ver específicamente el tráfico de llamadas en un horario en el que no se está en casa, debido a que esta franja es la usada por el defraudador para apropiarse ilícitamente de la línea.

Para evitar un mayor impacto en las pérdidas económicas cuando se comete este tipo de fraude, se debe hacer uso del “código secreto” el cual es un mecanismo sencillo y muy seguro en donde se digita una clave para bloquear y desbloquear el tráfico internacional, nacional, a celular, a líneas premium etc.

Por parte de la empresa se puede optar por la adquisición de equipos de monitoreo y gestión que extraigan la señalización de los protocolos de voz tradicional para detectar comportamientos atípicos de un determinado abonado. De igual forma los anuncios en campañas publicitarias contribuyen para alertar a los usuarios y ayudan a evitar mayores impactos.

1.2.2.6 Derivaciones fraudulentas de teléfonos públicos

Es un tipo de fraude telefónico externo, el cual ocurre cuando se conecta otro

aparato telefónico en paralelo o directamente a la línea asociada al teléfono público, para originar trafico telefónico sin costo alguno.

Dado que los teléfonos públicos son un servicio abierto a la comunidad y que sus conexiones por ende también, estas se encuentran expuestas a vándalos y personas inescrupulosas que aprovechan este hecho para realizar conexiones fraudulentas.

Las empresas de telefonía se ven obligadas a prestar este tipo de servicio en el cual invierten capital en infraestructura. Al realizarse derivaciones fraudulentas, estas consumen recursos de conmutación, los cuales no son cubiertos por la recolección hecha por el teléfono, lo que conlleva a presentar pérdidas económicas.

Detección y corrección

La detección de este problema se puede realizar en varios frentes, el primero es la denuncia por parte de los habitantes de los sectores donde se encuentra dicho teléfono. Se puede informar a las personas sobre las formas en que se realizan estas conexiones (empalmes visibles o traslado del aparato telefónico), o al tratar de usar el teléfono notan que este se encuentra ocupado. Las empresas pueden publicar esta información en las propias cabinas telefónicas.

Las empresas a su vez, pueden realizan la verificación a través de comparaciones entre los valores facturados y los recaudados; si estos valores no concuerdan, se podría estar presentando la conexión ilegal. En base a estas verificaciones, se envía el personal al sitio para revisar el estado de las conexiones, a su vez, cuando se presenta la conexión fraudulenta, el teléfono se reporta como dañado, ya que puede no estar detectando las señales de las centrales de manera adecuada.

Prevención

Para evitar estos inconvenientes, muchas empresas a nivel mundial han optado por implementar el uso de tarjetas de telefonía pública, en este caso los teléfonos públicos realizan verificaciones de los saldos de las tarjetas y realizan los descargos a la misma, esto evita que, a pesar de que se realicen las conexiones fraudulentas, no se pueda hacer uso de los servicios, ya que las validaciones se hacen a través de la central.

1.2.2.7 Fraude de Tercer país

Es un tipo de fraude telefónico de suscriptor, en el cual, el defraudador arrienda una vivienda con una o varias líneas telefónicas, por las que realiza llamadas y no paga las facturas, permite que se suspenda y luego se retire la línea por falta de pago.

En este caso el defraudador consigue una o varias líneas telefónicas en su propio país y a través de la facilidad de llamada en conferencia o mediante un pequeño conmutador (muchas veces de fabricación casera), permite que usuarios de distintos países se comuniquen entre ellos, los cargos de ambas llamadas se facturan a las líneas adquiridas por el defraudador.

Un ejemplo de esta modalidad es la siguiente:

El defraudador en Ecuador llama al primer país, Kuwait, esta persona le dice el destino con el que desea comunicarse (Líbano) y la persona en Ecuador marca a través de una segunda línea (llamada en conferencia u otra línea) hacia el Líbano y los deja en conferencia; ambas llamadas son registradas en Ecuador.

Esto también se hace automáticamente a través de unos conmutadores que reciben la información digitada (graban los tonos multifrecuenciales) y luego lo remarca sobre otra línea.

Detección y corrección

Este tipo de fraude se detecta por la atipicidad del consumo hacia destinos no comunes por parte de empresas suscriptoras del servicio, incremento en el consumo de llamadas internacionales o llamadas a países con historia de este fraude (generalmente hacia países del medio oriente).

En el momento de ser detectada esta anomalía por parte del sistema de gestión, se debe verificar en el sistema de facturación el perfil del cliente, si es posible contactarlo y posteriormente realizar un corte del servicio de llamadas internacionales o nacionales salientes (esto depende de la regulación de cada uno de los países).

Prevención

La prevención en este tipo de fraudes está directamente ligada al estudio que se realiza del cliente antes de la puesta en marcha del servicio que se va a proveer, se debe realizar un estudio profundo del perfil y de la documentación entregada, en pocas palabras, tomar en cuenta las recomendaciones para prevención en el "fraude de suscriptor" y posteriormente realizar los respectivos monitoreos de tráfico de llamadas mediante herramientas destinadas para tal fin como lo son las sondas de monitoreo SS7, VoIP, NGN etc.

1.2.2.8 Llamadas realizadas por terceros sobre líneas empresariales con cargo a las mismas

Este tipo de fraude se realiza contra empresas que utilizan centrales PBX en sus instalaciones para conectarse a la red telefónica pública conmutada. Los defraudadores pueden acceder a través de los puertos DISA[23], la cual es una facilidad de las centrales de PBX que permite a un usuario externo realizar llamadas reoriginando desde ésta, quedando las llamadas cargadas al número del PBX. Esta opción se habilita para empleados que se encuentran fuera de la

[23] DISA - Direct Inward System Access - Discado Directo Entrante

sede de la empresa y requieran usar servicios que esta tiene contratados con su proveedor, pero, debido a que estos servicios pueden ser configurados para poder accederse desde distintos puntos, los defraudadores que conocen el funcionamiento de la planta, configuran los puertos para beneficiarse de los servicios de la compañía.

Generalmente, las personas que realizan este fraude conocen los passwords para el acceso a las plantas y con ellos pueden acceder a la configuración de la PBX.

Otra manera de realizar llamadas sobre los PBX, es utilizando un módem para conectarse al puerto de mantenimiento remoto. Una vez conectado, puede realizar llamadas o cambiar la configuración del PBX, generando reclamos por llamadas no realizadas y mal funcionamiento.

El defraudador conoce la clave de acceso para marcar sobre una extensión del PBX y realizar llamadas, ésta información se puede obtener a través de una persona de la Compañía o por robo de información confidencial; para acceder al módem debe conocer el número telefónico, o la extensión que corresponde y la clave para entrar al módulo de mantenimiento del PBX.

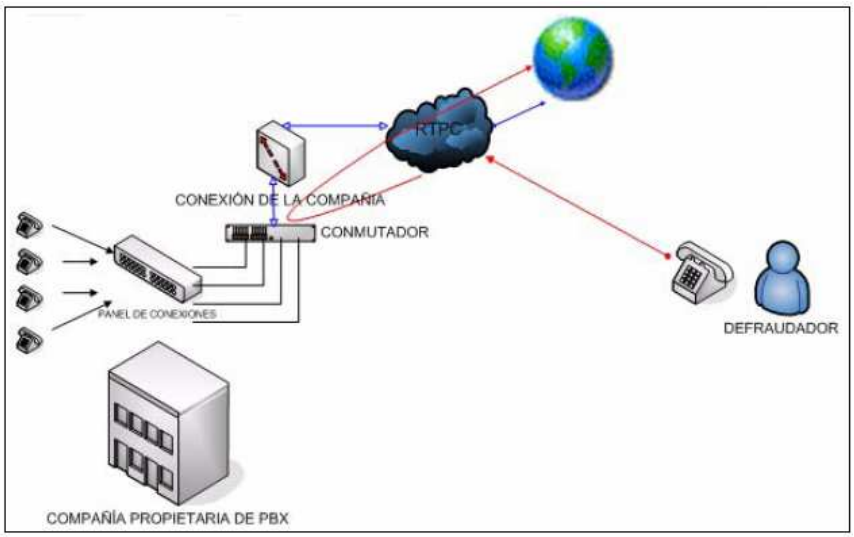


Figura 2.2: Llamadas realizadas por terceros sobre líneas empresariales con cargo a las mismas

Detección y corrección

La detección se debe hacer a través de pruebas de la planta en su entrada a producción. Aunque la empresa en la cual se instala el PBX puede no tener el conocimiento sobre la forma en que se puede realizar el fraude, es importante contar con empresas auditoras que certifiquen este tipo de labores para evitar inconvenientes. Se debe tener información detallada de los passwords de configuración de la planta y el personal que tiene el conocimiento de las mismas.

Se debe verificar los destinos de las llamadas de larga distancia, y si estos corresponden a destinos que la compañía requiere para su operación. Si los consumos a estos destinos son excesivos, puede presumirse la existencia de este tipo de fraude.

La forma en la cual se programan las plantas telefónicas y los accesos troncales en las empresas es la primera medida para evitar este problema. Si se dejan circuitos abiertos para realizar este tipo de conexiones, los costos de los servicios se van a ver afectados.

La mayoría de las empresas que tienen este tipo de tecnologías para sus servicios telefónicos, lo hacen a través de terceros, por lo tanto es necesario que se contraten empresas con respaldo y que garanticen que los servicios configurados no permitan este tipo de conexiones fraudulentas.

Prevención

Para prevenir este fraude, se puede optar por la adquisición de plantas que cuentan con software de gestión que permiten hacer seguimiento de los consumos de los circuitos contratados, con lo cual se conoce de primera mano la utilización de los circuitos, además se debe realizar el seguimiento de los servicios contratados a las empresas de telefonía. Se puede contratar servicios con plantas que permitan hacer seguimiento de los consumos de forma continua,

esto permite evitar que se realicen marcaciones a lugares no permitidos por la empresa.

Se debe contar con la lista de las personas que tienen acceso a los password de configuración, con el fin de establecer quien puede realizar cambios sin autorización.

FRAUDE AL USUARIO

1.2.3 SLAMMING (CAMBIOS DE OPERADOR)

Este es un tipo de fraude interno, pero en este caso quien resulta afectado es el cliente final.

Se define como la práctica ilegal de cambiar de operador a un usuario sin el consentimiento del mismo o usando métodos de engaño al cliente, quien está pensando que realiza una operación diferente, como, inscripción a una revista, llenado de cupones de actualización de datos, etc.

Este fraude es frecuente en países donde existen varios operadores prestando servicios por suscripción, como por ejemplo, de telefonía de larga distancia, Internet e incluso servicios de telefonía locales. Las compañías que realizan el Slamming tienen varias formas de efectuarlo: a través de llamadas a los clientes, en las cuales cualquier palabra que el usuario use la toman como aceptación del servicio, en campañas comerciales en las que se envían cartas, las cuales los clientes devuelven y sin saberlo, entre los documentos adjuntos está la aceptación del cambio de operador; otra metodología consiste en engañar al usuario haciéndole creer cosas, como que el operador que le está actualmente suministrando el servicio está en serías situaciones financieras y como beneficio a dichos usuarios ha decidido, para minimizar la afectación, ceder sus clientes; otra muy popular es crear ambientes de competencia desleal, como hacer percibir al usuario situaciones irreales como el cobro de servicios no contratados, la

posibilidad de cobros adicionales o mecanismos de desprestigio de los competidores, las cuales minan al usuario y hacen que cambie de operador por razones ficticias. Los operadores que optan por este fraude también realizan los enrutamientos de canales de interconexión de una forma que no es la más adecuada (ocasionando retardos innecesarios y bloqueos eventuales en la comunicación), lo cual hace que dichas conexiones no sean fiables, desembocando en bajas de calidad que el cliente percibe.

Detección y corrección

Este tipo de fraude se detecta cuando el operador recibe quejas por parte de sus usuarios, de que otra compañía esta cobrando por sus servicios de larga distancia o que se bloquean los servicios hacia otros operadores. Los usuarios perciben bajas en la calidad de sus servicios, ya que las conexiones hechas por el operador que realiza el slamming, generalmente se enrutan por circuitos que aumentan el retardo de las señales, lo cual afecta el servicio.

1.2.4 CRAMMING

Son servicios que son instalados a los clientes sin que estos los hayan solicitado, recibido, autorizado o utilizado.

El Cramming se presenta en dos categorías:

- A través de líneas síquicas, clubes personales, de viajes o de membresías.

- Programas o servicios de telecomunicaciones tales como correo de voz, llamadas por cobrar o tarjetas prepago.

El Cramming se realiza de diversas formas, entre las cuales podemos encontrar:

- Servicios 01 800: el usuario llama al número gratuito y dentro de la conversación engañan al usuario haciéndole decir su nombre y la frase “yo quiero” o algo similar, con lo cual comprometen al usuario a contratar servicios sin que este se entere.

- Formularios de inscripción: El usuario contesta a un formulario telefónicamente con la idea de ganar un premio y los promotores de forma inescrupulosa usan los datos para ingresarlo en programas de tarjetas telefónicas o servicios de terceros, los cuales se cargarán a la cuenta telefónica.

- Tarjetas de llamadas instantáneas: Algunas personas usan los teléfonos para hacer llamadas a líneas eróticas, en las cuales le ofrecen las “tarjetas de llamadas instantáneas”, ésta tarjeta contiene un código para acceder al servicio pero que es cargado al número telefónico desde el cual se realizó la petición.

- Llamadas internacionales: Algunos servicios de llamadas para adultos inician las sesiones solicitando a los clientes marcar ciertos códigos desconocidos, lo que están haciendo con estos códigos es enrutar las llamadas hacia destinos internacionales, mediante los cuales el servicio de llamadas gana más dinero mientras se permanezca más en línea.

Detección y corrección

La detección de este fraude se realiza a través de la denuncia de los clientes, cuando detectan en sus cuentas servicios que no han sido contratados por ellos o cargos por llamadas que el supone nunca realizó.

Prevención

Los clientes deben hacer un seguimiento de los servicios contratados a las empresas prestadoras de sus servicios, con el fin de establecer si están

pagando servicios adicionales no solicitados.

De la misma forma se debe informar a los clientes de compañías de telecomunicaciones sobre la forma en que se avalan las contrataciones de servicios, con el fin de prevenir de que sean víctimas de abusos por parte de las compañías.

Para prevenir este tipo de fraude es importante que los usuarios se enteren de manera clara del tipo de servicio que esta siendo ofrecido, para de esta forma saber si contratarlos o no.

1.2.5 CLONACIÓN DE TELÉFONOS CELULARES

Se realiza a través de la clonación del ESN[24] de los equipos celulares. Los defraudadores interceptan estos números a través de equipos de recepción de radio, teniendo dichos números, los reprograman en otros equipos, desde los cuales realizan llamadas a cargo del suscriptor con el ESN original.

En los teléfonos celulares de primera generación, la identificación de usuario se hace a través del ESN, éste dato viaja entre la señal que es transmitida cuando el usuario hace una llamada, así como cuando las recibe, los defraudadores capturan la señal de radio producida por el teléfono y toman el dato del ESN, a través de equipos especializados en descencriptar información, luego graban dicho número en un nuevo equipo, el cual se reconoce en la red con el ESN del usuario del que fue clonado. Las llamadas que realiza el defraudador se facturan al usuario original, quien recibe todo el cargo de las llamadas.

En otras ocasiones, cuando los teléfonos de los usuarios son robados o se extravían, los defraudadores toman el ESN directamente del equipo, el cual es válido hasta el momento del reporte por parte de la persona afectada a los operadores de servicio.

[24] ESN - Equipment Serial Number

Esta modalidad de fraude es muy usada por la delincuencia común y organizada con el fin de evitar el pago correspondiente a las llamadas realizadas y además evitar el seguimiento de las autoridades.

Detección y corrección

Cuando el usuario realiza el reporte de robo o pérdida de su aparato celular, la red identifica el ESN de dicho usuario e impide las llamadas del mismo, pero solo hasta ese momento es posible detectar el fraude.

Cuando la clonación se ha hecho a través de la captura del ESN, la detección se hace hasta el momento en que el usuario reporta que en su factura se le están cobrando llamadas que no realizó.

Se están desarrollando técnicas basadas en triangulación pasiva, utilizando la red existente para detectar la ubicación del teléfono que se clonó.

Cuando este fraude es detectado por las empresas de servicio celular, se procede al el bloqueo del ESN para evitar que continúe el consumo de llamadas.

Prevención

Con el robo o pérdida de celulares que usan la tecnología de ESN, se corre el riesgo de que estos sean clonados por personas expertas en estas tecnologías, es por eso que ante una eventualidad de estas, las victimas deben reportar la pérdida a sus proveedores de servicio para cancelar en la red los servicios asignados a su teléfono.

FRAUDES ONLINE

1.2.6 DIALERS

Los Dialers están dentro del grupo de “Fraude Online” más comunes. Son programas que, empleados de forma maliciosa, permiten el cambio de la conexión de una llamada local a Internet a través de un nodo local, a líneas de tarifa adicional, sin la autorización expresa del usuario.

Su objetivo es finalizar la conexión telefónica que el usuario de Internet esté utilizando en ese momento y establecer otra, marcando, bien sea un número de teléfono con tarifa especial o un número en otro país.

Descripción

Por tratarse de un programa informático, los Dialers, al igual que los virus, pueden estar ocultos en cualquier aplicación, esperando la situación propicia para llegar al computador. La forma más común de propagarse es a través de ciertas páginas de Internet que ofrecen, por lo general, acceso a contenido gratuito de entretenimiento (juegos, canciones, imágenes, videos, etc.), así como programas sin licencia y contenido para adultos. Estas páginas, que en la mayoría de casos carecen de criterios éticos, aprovechan la desinformación y confusión del usuario poco experto para lograr instalar este tipo de programas en su computador.

Muchos programas maliciosos, entre estos los Dialers, se descargan mediante un archivo ejecutable (extensión.exe), o mediante un control ActiveX[25].

Detección y corrección

Este tipo de fraude es detectado generalmente cuando el usuario hace reclamos a

[25] ActiveX – Es un estándar definido por Microsoft para ejecutar subprogramas que se encuentran en una página Web y solo funcionan con el navegador de Internet Explorer.

la empresa prestadora del servicio porque llegan a su factura llamadas de larga distancia a destinos desconocidos por él.

Otra forma de detectarlo es cuando se registran alarmas a nivel interno de la empresa por tráfico atípico a destinos internacionales.

Los pasos a seguir para corregir este tipo de fraude son:

- Interponer un reclamo, para tratar de identificar la página objeto de la denuncia, se puede acudir al Historial del navegador y después a la base de datos WHOIS[26] para relacionar un dominio con su propietario.

- Informar a la operadora y a la Superintendencia de Telecomunicaciones de los sitios web que no se ajusten a la legalidad, tomando nota de la dirección de la página que trata de modificar el acceso a la Red sin el consentimiento del usuario.

Prevención

La manera más eficaz de prevenir este tipo de ataque, es el bloqueo de LDI[27] y además evitar entrar a páginas o acceder a los links de los cuales se ha hablado anteriormente.

1.2.7 PHISHING

El Phishing es un fraude que tiene como objetivo el robo de datos bancarios por medio de suplantación de páginas web o envío de correos electrónicos, entre otras fórmulas.

[26] WHOIS – Es un protocolo TCP basado en preguntas / respuestas que es usado para consultar en una base de datos, para determinar el propietario de un nombre de dominio o una dirección IP en Internet.
[27] LDI - Larga Distancia Internacional

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito, dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico, suministrando sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial, estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, quien la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Detección y corrección

Generalmente es detectado por los usuarios después de que han entregado la información a los suplantadores o defraudadores y se han realizado transacciones bancarias que el usuario (afectado) afirma no haber realizado.

También se detecta porque algunas compañías ya han identificado las IP públicas que realizan este tipo de fraude y bloquean la salida de mensajes por medio de su propio firewall[28], cuando el usuario pregunta a su proveedor de correo y/o Internet el motivo de la falla, la empresa prestadora le informa que es por detección de fraude Phishing en ese destino.

Prevención

[28] Firewall – Es un elemento utilizado en redes de computadoras, que se encarga de aceptar o denegar de forma selectiva paquetes de red basándose en el origen o en el destino de estos paquetes. Normalmente, no entienden nada del protocolo subyacente y no inspeccionan su contenido.

Este fraude se puede prevenir a través de campañas en medios masivos o Internet sobre las formas en que estos se realizan, con el fin de que los usuarios sepan de primera mano la manera en que operan estos delincuentes (tipos de email enviados, URL que se usan, formas de verificar en los browser, etc.).
O una vez detectadas las direcciones de Internet públicas desde las cuales se comete este fraude, difundir dicha dirección por Internet para realizar el bloqueo de la misma en los firewall para denegar el acceso de la misma.

1.2.8 PHARMING

La palabra Pharming deriva del término Phishing, utilizado para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas web, intenta obtener información confidencial de los clientes.

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados. O bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix.

La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redireccionando el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

Corrección y Prevención

Algunos de los métodos tradicionales para combatir el pharming son: utilización de software especializado, protección DNS y addons para los exploradores web, como por ejemplo toolbars[29], etc.

[29] Toolbars – Son barras de herramientas que brindan servicios extra en Internet.

El Software especializado suele ser utilizado en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing, mientras que el uso de addons en los exploradores web permite a los usuarios domésticos protegerse de esta técnica.

La protección DNS permite evitar que los propios servidores DNS sean hackeados para realizar ataques Pharming. Los filtros Anti-Spam normalmente no protegen a los usuarios contra esta técnica.

1.2.9 SPYWARE

Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de Internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.

Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, como por ejemplo el programa Magic Lantern desarrollado por el FBI para combatir el terrorismo, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.
Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.

Algunos ejemplos de programas espía conocidos son Gator, Bonzi Buddy,o Kazaa.

Detección

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos y comerciales.
- Barras de búsquedas de sitios que no se pueden eliminar.
- Creación de carpetas tanto en el directorio raíz, como en "Archivos de programas", "Documents and Settings" y "WINDOWS".
- Modificación de valores de registro.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda más en iniciar el computador, debido a la carga de software Spyware que se inicia una vez alterado el registro a los fines de que el Spyware se active al iniciarse la computadora (con CCleaner se puede ayudar a eliminar alteraciones en el registro del sistema operativo hechas por Spyware; Spybot Search & Destroy detecta los posibles cambios e informa al usuario de los mismos).
- Al hacer click en un vínculo, el usuario retorna de nuevo a la misma página que el software espía hace aparecer.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.

- Aparición de un mensaje de infección no propio del sistema, así como un enlace web para descargar un supuesto antispyware.

- Al acceder a determinados sitios sobre el escritorio, se oculta o bloquea tanto el panel de control como los iconos de programas.

- Denegación de servicios de correo y mensajería instantánea.

Prevención

Los antivirus más recientes son capaces de eliminar programas espía; aunque también hay programas especializados en eliminarlos o bloquearlos. Se recomienda no usar un solo programa antiespía sino una combinación de varios, dado que en muchas ocasiones uno de ellos detecta algunas cosas que no encuentran los otros, y viceversa, por lo que el uso combinado, de varios de ellos, ofrece una protección mucho más completa. Algunos de ellos son: Spybot - Search & Destroy, Ad-Aware, AVG Antispyware, Spyware Doctor, Spy Sweeper, SUPERAntispyware, Zone Alarm, Windows Defender, Panda Antivirus, HijackThis, etc.

1.2.10 SPOOFING

Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad, generalmente para usos maliciosos o de investigación.
Se realiza mediante la creación de tramas TCP/IP utilizando una dirección IP falseada.

1.2.10.1 IP Spoofing

Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente

gracias a programas destinados a ello. Hay que tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas al host al que pertenece la IP legalmente. Para poder realizar IP Spoofing en sesiones TCP, se debe tener en cuenta el comportamiento de dicho protocolo con el envío de paquetes SYN y ACK con su ISN[30] específico y teniendo en cuenta que e propietario real de la IP podría (si no se le impide de alguna manera) cortar la conexión en cualquier momento al recibir paquetes sin haberlos solicitado. También hay que tener en cuenta que los routers actuales no admiten el envío de paquetes con IP origen no perteneciente a una de las redes que administra (los paquetes spoofeados no sobrepasan el router).

1.2.10.2 DNS Spoofing

Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación “Nombre de dominio – IP” ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio – IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).

1.2.10.3 ARP Spoofing

Suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Explicándolo de una manera más sencilla: El protocolo Ethernet trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando una máquina quiere comunicarse con una IP emite

[30] ISN - Initial Sequence Number Selection

una trama ARP-Request a la dirección de Broadcast pidiendo la MAC de la máquina poseedora de la IP con que desea comunicarse. La máquina con la IP solicitada responde con un ARP-reply indicando su MAC. Los switch y los host guardan una tabla local con la relación IP-MAC llamada “tabla ARP”. Dicha tabla ARP puede ser falseada por un host atacante que emita tramas ARP-reply indicando su MAC como destino válido para una IP específica, como por ejemplo la de un router, de esta manera la información dirigida al router pasaría por el host atacante quien podrá sniffar dicha información y redirigirla si así lo desea. El protocolo ARP trabaja a nivel de enlace de datos de OSI, por lo que esta técnica solo puede ser utilizada en redes LAN o en cualquier caso en la parte de la red que queda antes del primer router.

La idea es sencilla, y los efectos del ataque pueden ser muy negativos: desde negaciones de servicio hasta interceptación de datos, incluyendo algunos Man in the Middle contra ciertos protocolos cifrados.

1.2.10.4 Web Spoofing

Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL[31]. Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado (incluyendo las cargadas en nuevas ventanas del navegador) a través de su propia máquina, donde son modificadas para que cualquier evento generado por el cliente sea registrado (esto implica registrar cualquier dato introducido en un formulario, cualquier click en un enlace, etc.).

[31] SSL - Secure Socket Layer (Capa de Conexión Segura): Protocolo creado por Netscape con el fin de posibiltar la transmisión cifrada y segura de información a través de la red.

Prevención

Para evitar ataques de spoofing exitosos contra nuestros sistemas, podemos tomar diferentes medidas preventivas; en primer lugar, parece evidente que una gran ayuda es reforzar la predicción de números de secuencia TCP. Otra medida sencilla es eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas; el cifrado y el filtrado de las conexiones que pueden aceptar nuestras máquinas también son medidas de seguridad importantes para evitar el spoofing.

En el caso del ARP Spoofing, una manera de protegerse es mediante tablas ARP estáticas, esto siempre y cuando las direcciones IP a nivel de red sean fijas, lo cual puede ser difícil en redes grandes.

Para prevenir el Web Spoofing la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente se este sufriendo este tipo de ataque.

FRAUDE SOBRE PLATAFORMAS DE VOZ SOBRE IP

El hecho de que la Voz sobre IP, preste tal cantidad de ventajas y facilidades, tanto técnicas como económicas, ha provocado que ciertas personas se aprovechen de la situación para negociar con la tecnología de una infinidad de maneras, para de este modo obtener beneficios de manera ilegal. Incluso se han creado nuevas versiones de fraudes existentes usando la mencionada tecnología, a continuación se realiza un estudio de los fraudes más comunes.

1.2.11 FRAUDE HACIENDO USO DE LA INFRAESTRUCTURA VOIP DE EMPRESAS DE TELECOMUNICACIONES LEGALMENTE ESTABLECIDAS

Se constituye como un tipo de fraude interno, de terceros.

Actualmente algunas empresas de telecomunicaciones legalmente establecidas y con licencia para operar con llamadas nacionales e internacionales, cuentan con plataformas VoIP como infraestructura de red para recibir y generar llamadas. Dicha infraestructura puede ser vulnerable dependiendo la topología de conexión, a continuación se muestran algunos ejemplos:

1.2.11.1 Infraestructura con Softswitch

El softswitch es un dispositivo que utiliza estándares abiertos para crear redes integradas de última generación, en las que la inteligencia asociada a los servicios está desligada de la infraestructura de red; se considera la pieza central en las primeras implementaciones de las NGN[32]. Este dispositivo, combinación de hardware y software, provee control de llamada y servicios inteligentes para redes de conmutación de paquetes, y puede conmutar el tráfico de voz, datos y video de una manera eficiente.

Los componentes principales del softswitch son:

- Media Gateway
- Media Gateway Controller
- Signalling Gateway

Aunque muchas veces estos componentes se encuentran integrados, pueden estar separados, lo que requiere el uso de protocolos de comunicación entre los mismos.

[32] NGN – Next Generation Network

1.2.11.1.1 Características de la tecnología de softswitch

Una característica clave del softswitch es su capacidad de proveer a través de la red IP un sistema telefónico tradicional, confiable y de alta calidad. Sus interfaces de programación permiten a los fabricantes de software crear velozmente nuevos servicios basados en IP, que funcionen para ambas redes: la telefónica tradicional y la IP. De esta forma, se pueden ofrecer servicios de voz avanzados, así como nuevas aplicaciones multimedia.

Separar los servicios y el control de llamadas de la red de transporte subyacente es una característica esencial de las redes de telecomunicaciones basadas en softswitch. Soportan los servicios de voz, fax, vídeo, datos y posibilidades para los nuevos servicios que serán ofrecidos en el futuro.

La tecnología de softswitch permite una transición suave de la conmutación de circuitos a la conmutación de paquetes, con servicios diferenciados e interoperabilidad a través de redes heterogéneas. Un softswitch es generalmente entre un 40 y un 45 % menos costoso que un conmutador de circuitos, debido a que utiliza arquitectura de cómputo general, en donde el precio y desempeño han mejorado considerablemente.

Este tipo de infraestructura, presenta su mayor vulnerabilidad en la administración de la plataforma y está directamente relacionada con los usuarios que cuentan con perfiles administrativos y de cambios de configuraciones, ya que tienen la facilidad de configurar clientes “fantasmas” o falsos para realizar llamadas esporádicamente, manipular la facturación (modificar el reporte de facturación para que abonados y/o cuentas de usuarios prepago reflejen en sus cobros un consumo inferior al que realmente usaron), entregar a terceros claves privadas de clientes, etc.

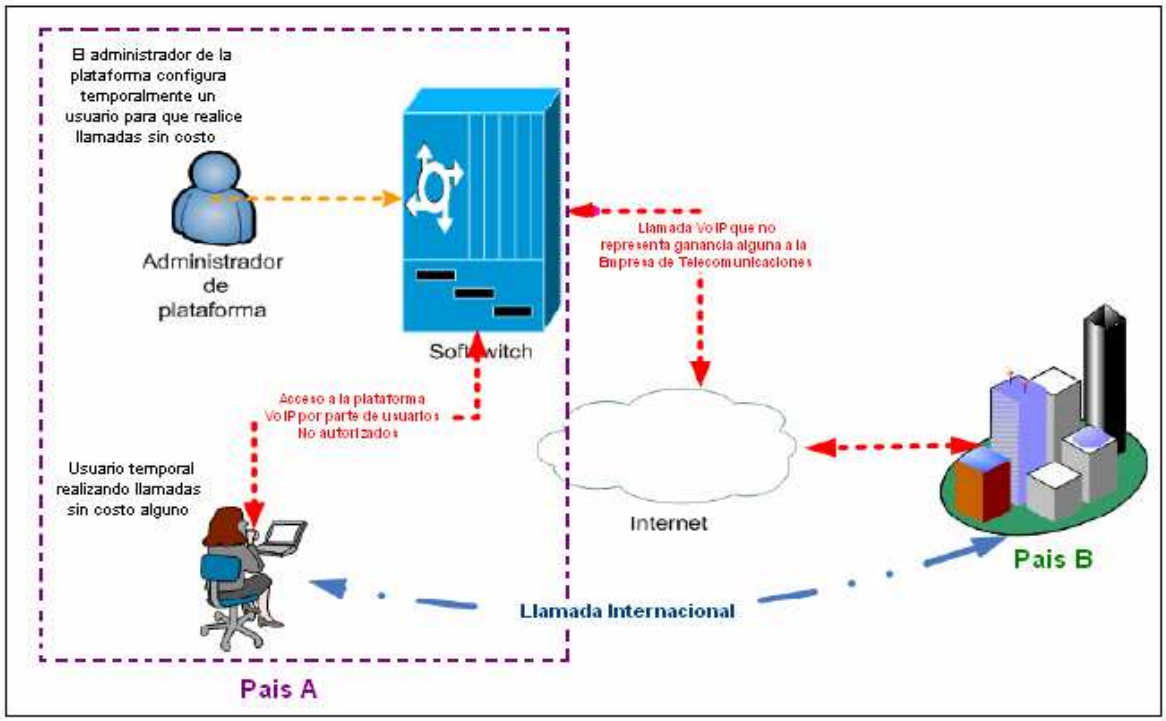


Figura 2.3: Infraestructura con Softswitch

Por otro lado se involucra también la “ingeniería social”, en donde un tercero copia la clave de acceso de la tarjeta prepago de un usuario y realiza llamadas a través de la plataforma VoIP hasta agotar su saldo.

1.2.11.2 Infraestructura con Gateways de voz

Existen plataformas de VoIP que cuentan con equipos que realizan individualmente tareas de enrutamiento de llamadas, administración, autenticación y facturación; entre ellos encontramos los gateways de voz.

El fraude es realizado por terceros (personas o empresas), quienes de una forma u otra consiguen las claves de autenticación de los usuarios y conocen las direcciones IP públicas de la plataforma VoIP.

Cuando obtienen esta información pueden realizar llamadas hacia diferentes países y estas son cargadas al suscriptor real.

Afecta a las empresas de telecomunicaciones autorizadas para prestar este tipo de servicio, ya que muchas veces se pierden disputas de tráfico con los clientes que detectan anomalías en la facturación (servicio post-pago). De igual forma, cuando el usuario final no tiene una plataforma que registre las llamadas para una posterior comparación con las cuentas de cobro, asume costos de usuarios fraudulentos. Cuando el servicio es prepago, el suscriptor pierde su saldo en minutos rápidamente.

La imagen de la empresa prestadora del servicio se ve afectada ya que el suscriptor pierde confianza en ella.

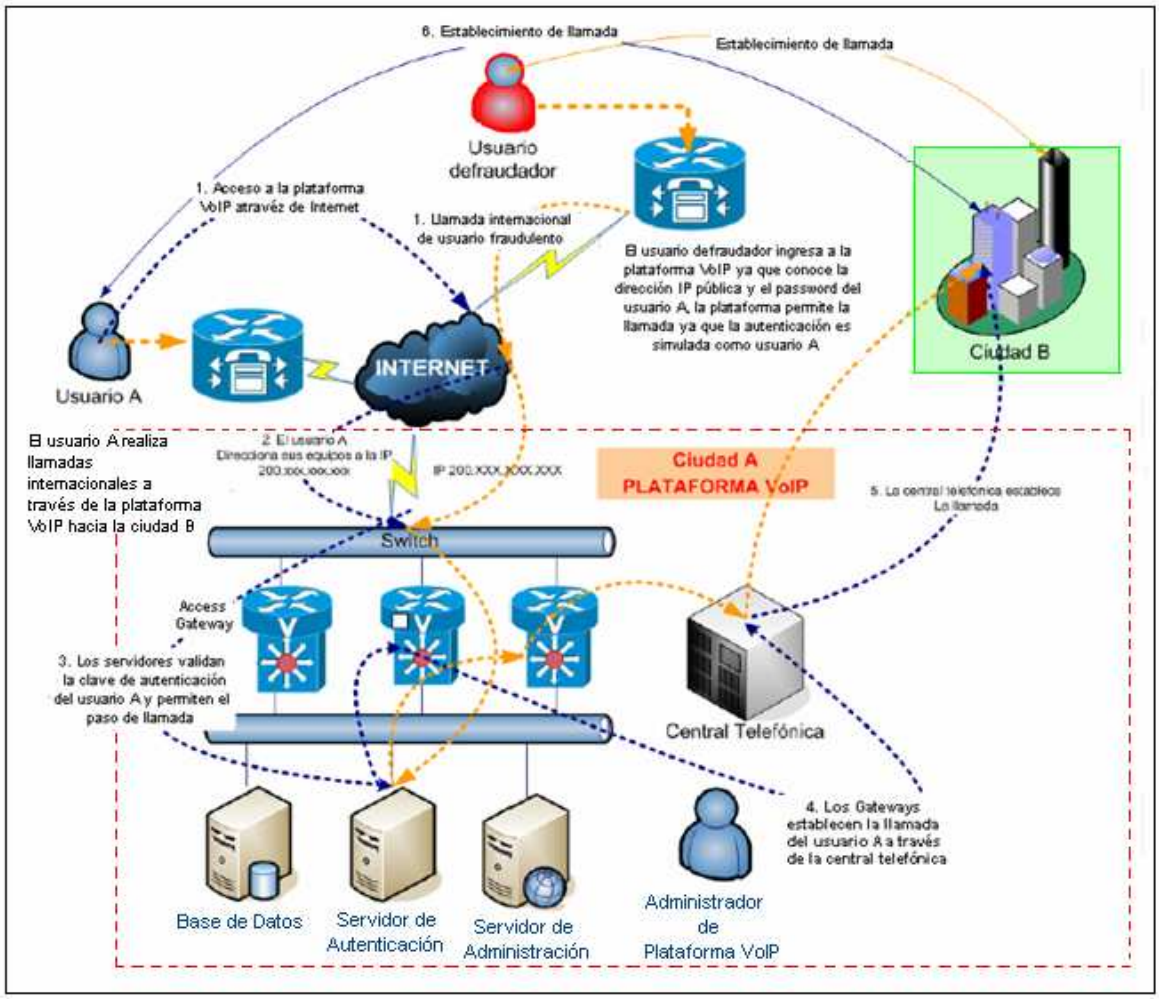


Figura 2.4: Infraestructura con Gateways de voz

Detección y Corrección

Generalmente este tipo de fraude es detectado posterior a las cuentas de cobro cuando se hacen comparaciones entre los minutos reflejados por la empresa prestadora del servicio y las plataformas del suscriptor. Cuando es detectado este tipo de fraude se verifican las direcciones IP de origen y se bloquean inmediatamente, de igual forma se cambian los password o claves de acceso.

Prevención

Se puede prevenir este tipo de fraude de las siguientes formas:

- Realizando auditorias periódicas de la administración y creación de usuarios.

- Comparando los clientes que realizaron llamadas versus los registrados en la plataforma de facturación.

- Autenticando y validando los suscriptores teniendo en cuenta la clave o password y la dirección IP de origen (no permitir el acceso de IP desconocidas o no suscritas inicialmente por los clientes).

- Instalando equipos de seguridad (firewall) que validen IP públicas que intentan acceder a la plataforma IP.

- Realizar estudios completos de equipos VoIP que cuenten integralmente con opciones de enrutamiento, seguridad, administración, facturación, etc.

- Existen en el mercado equipos especializados en el análisis de tráfico VoIP (sondas VoIP), que monitorean la red en tiempo real y que emiten alarmas de vulnerabilidad y anomalías de tráfico por sobrepaso en los umbrales típicos de las llamadas.

1.2.12 SISTEMAS “BY PASS”

De los tipos de fraude existentes, el que más perjuicio origina a las operadoras de telefonía y al estado ecuatoriano, lo constituye el “By Pass”, que en los últimos años ha causado pérdidas millonarias a nuestro país.

De forma resumida se puede decir que el “By Pass” encamina directamente el tráfico que viene del exterior hacia las centrales locales, sin pasar por la central de tráfico internacional (es decir, se evita la tarifación de la llamada internacional, y se la convierte en una llamada local).

El tráfico de llamadas entrantes es aproximadamente 8 veces mayor que el de las llamadas salientes y en este mismo sentido se comete el ilícito del “By Pass”. El “By Pass” se muestra como una ruta alternativa para los Carriers internacionales, el cual presenta un costo sumamente menor que el exigido por las compañías telefónicas locales; por este motivo deciden ingresar sus volúmenes de tráfico mediante esta vía alternativa; o, fomentar la implementación de sistemas de “By Pass” para ingresar su tráfico a un menor costo.

El tráfico telefónico internacional se enruta por Telepuertos privados (sean estos autorizados o no autorizados) y no por las estaciones terrenas internacionales de las empresas telefónicas. Del telepuerto privado, acceden a un local clandestino mediante enlaces de última milla: fibra óptica, Spread Spectrum, líneas dedicadas de cobre o microondas.

Previamente, se debió equipar el local clandestino con numerosas líneas telefónicas, dependiendo del tamaño del “By Pass”. Estas líneas son conseguidas a través de cómplices en la misma empresa telefónica o con documentación falsa, adulterada o robada (Fraude de suscripción).

Una vez que todo el volumen de tráfico ha ingresado al local clandestino, equipos de telecomunicaciones procesan la información como una mini central telefónica; las llamadas procesadas por la mini central telefónica generan llamadas locales

hacia los abonados finales en el Ecuador, completando así la llamada que se generó desde cualquier parte del mundo hacia nuestro país.

Las empresas telefónicas locales sólo perciben una llamada local, mientras la porción internacional la cobra la empresa que comete el fraude.

1.2.12.1 Tipos de sistemas “By Pass”

Entrante

Consiste en ingresar tráfico internacional recolectado en el extranjero, entre los operadores locales sin pasar por los operadores legales.

Saliente

Consiste en sacar tráfico internacional recolectado de tarjetas prepago ilegales, centros de reventa de minutos, comercialización empresarial ilegal, suscripción de usuarios.

1.2.12.2 Características de un sistema “By Pass”

- Utiliza grupos de líneas telefónicas. (Cuentas de telefonía)
- Necesitan un enlace internacional.
- Las líneas utilizadas generan considerables volúmenes de tráfico, mientras que casi no reciben llamadas.
- Registran mayor generación de tráfico los fines de semana y días festivos.
- El comportamiento del enlace internacional se presenta de manera simétrica, debido a que para comunicaciones de voz se requiere la misma capacidad, tanto para la transmisión como para la recepción, para garantizar calidad de servicio.

- Para líneas celulares la generación de tráfico se realiza desde una misma radiobase.

- Los operadores clandestinos involucrados en el "By Pass" ofrecen pagos por terminación de llamada a precios más bajos.

- Servicio para ciudades en que el tráfico internacional es alto.

- Costos de inversión, operación y mantenimiento muy bajos.

1.2.12.3 Ruta normal frente a ruta "By Pass"

El proceso llevado a cabo para que una llamada internacional (legalmente establecida) llegue a su destino se explica mediante la figura 2.5.

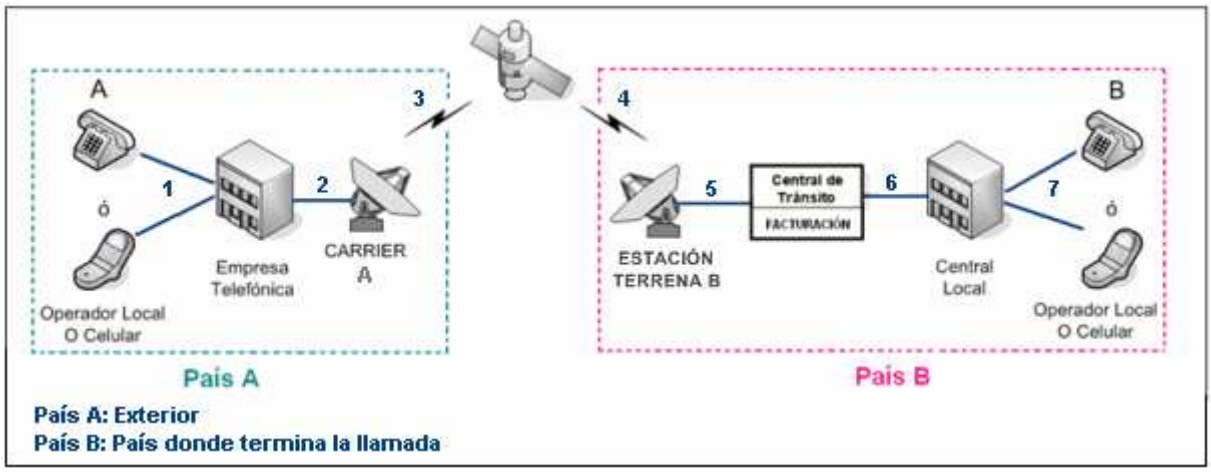


Figura 2.5: Ruta normal

Paso 1:

El usuario en el "País A", desea comunicarse con un usuario en el "País B", puede realizarlo mediante la Empresa Telefónica (la cual tiene contrato de concesión de telefonía internacional) o a su vez mediante el uso de tarjetas telefónicas

(legalmente establecidas). El usuario “A” marca el número de destino y la llamada ingresa a la empresa telefónica.

Pasos 2, 3 y 4:

La llamada es transferida por la Empresa Telefónica hacia un CARRIER “A”, con el cual tiene un acuerdo para enrutar las llamadas internacionales. Este CARRIER “A”, se encarga de entregar la llamada a la ESTACIÓN TERRENA “B”, con la cual tiene acuerdos la Central local del “País B” para terminar las llamadas internacionales.

Pasos 5 y 6:

La Central Local del “País B” recibe la llamada mediante la Central de Tránsito, la cual la factura como una Llamada Internacional.

Paso 7:

La Central Local del “País B” enruta la llamada para su recepción por el usuario en el “País B”.

El proceso llevado a cabo para que una llamada internacional establecida por ruta ilegal llegue a su destino se explica en la figura 2.6.

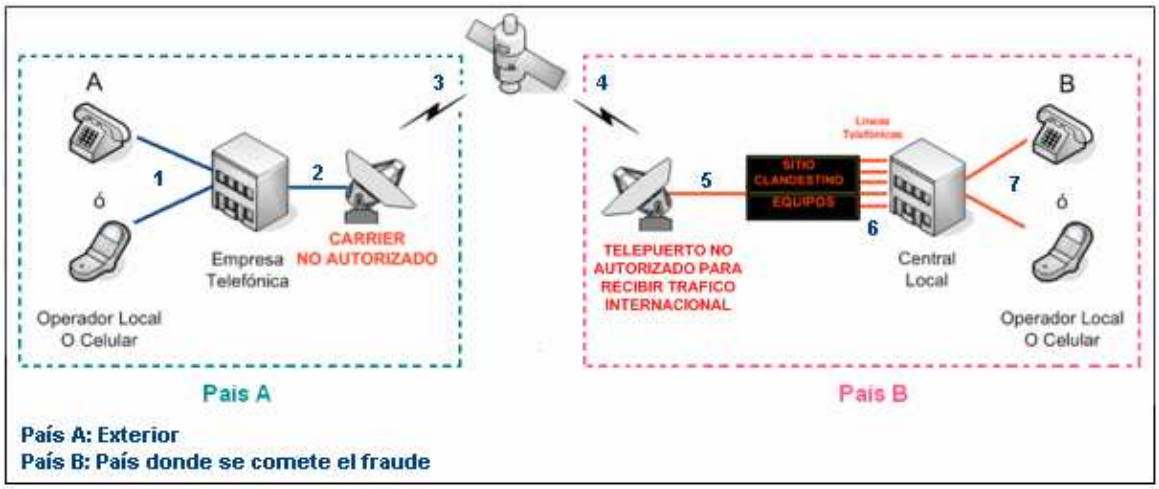


Figura 2.6: Ruta “By Pass”

Paso 1:

En este caso generalmente se usan tarjetas de telefonía internacional, el usuario prefiere adquirir estas tarjetas debido a que presentan un menor costo por minuto. El usuario en el “País A” sigue los pasos detallados en la parte posterior de la tarjeta (Ver Figura 2.10), y realiza la llamada deseada; la llamada ingresa a la Empresa Telefónica en el “País A”, en la cual se encapsula en paquetes IP.

Paso 2, 3 y 4:

El paquete IP que contiene la llamada se enruta hacia el CARRIER (el cual podría o no ser autorizado). El paquete es transferido por el CARRIER NO AUTORIZADO en el “País A” hacia el TELEPUERTO NO AUTORIZADO en el “País B”, el cual pertenece al Sitio Clandestino donde se procesa la llamada telefónica internacional no autorizada.

Paso 5:

Una vez que la información se recibe en el TELEPUERTO NO AUTORIZADO en el “País B”, el tráfico es ingresado al Sitio Clandestino, en el cual se desencapsula la información de los paquetes IP.

Paso 6:

Posteriormente se envía la información a su destino mediante las Líneas Telefónicas adquiridas por los defraudadores, la llamada es ingresada a la Central Local del “País B”, como si se tratara de una llamada local.

Paso 7:

La llamada es entregada al usuario del “País B”.

Como ya se dijo anteriormente, la forma de operar de los defraudadores empieza por la venta en el exterior de tarjetas de telefonía internacional, mediante las cuales las llamadas ingresan por ruta ilegal.

(a)

(b)

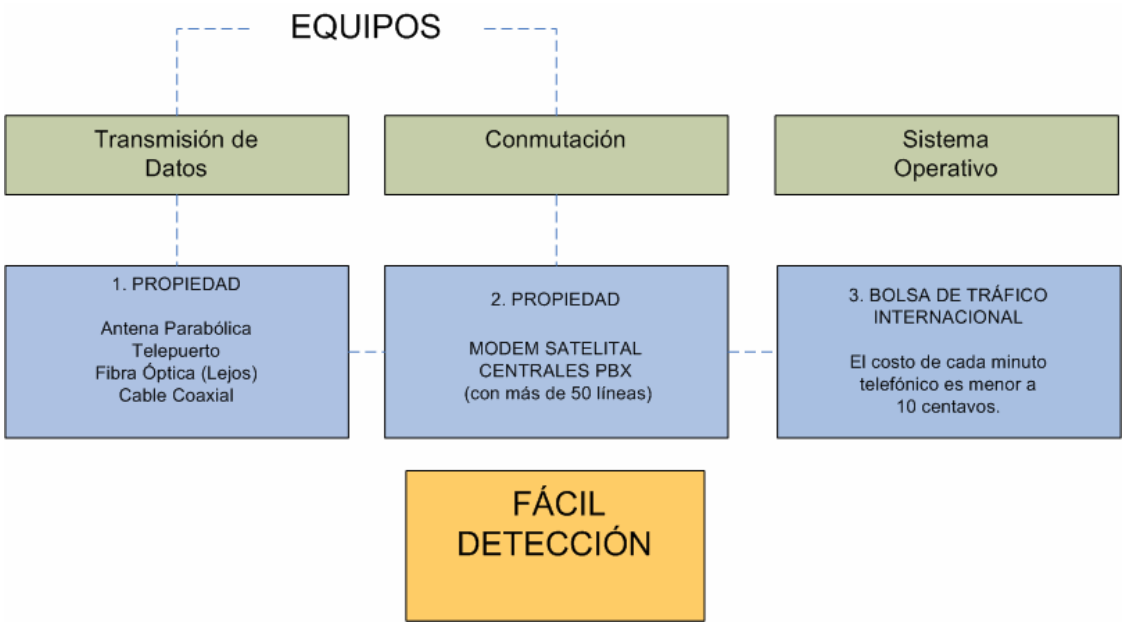
(c)

(d)

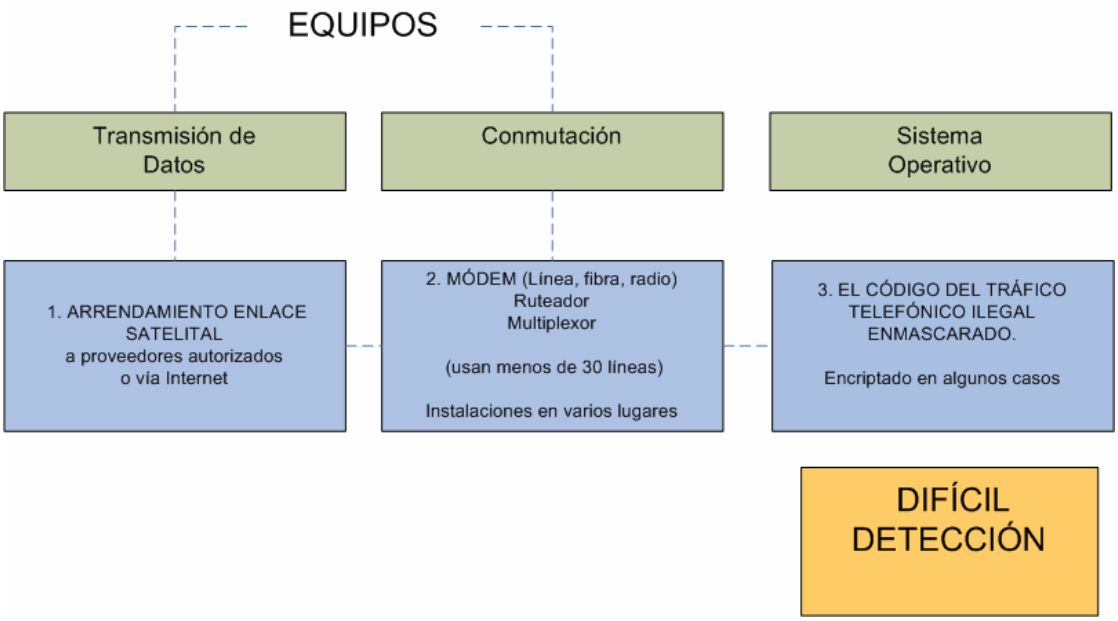
Figura 2.7: Tarjeta de Telefonía Internacional adquirida por INTERNET

1.2.12.4 Evolución tecnológica de los sistemas “By Pass”

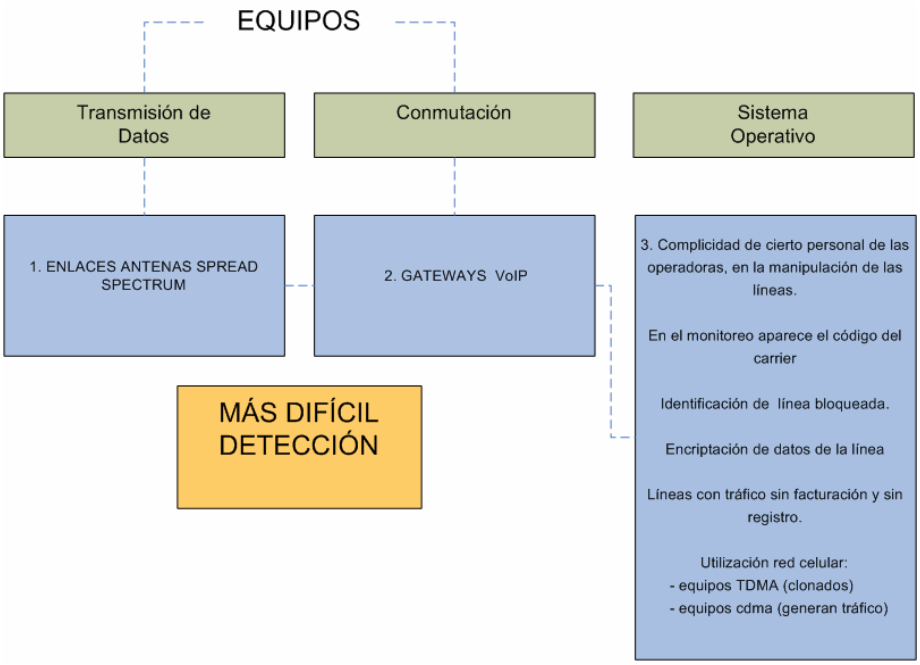
Primera etapa:



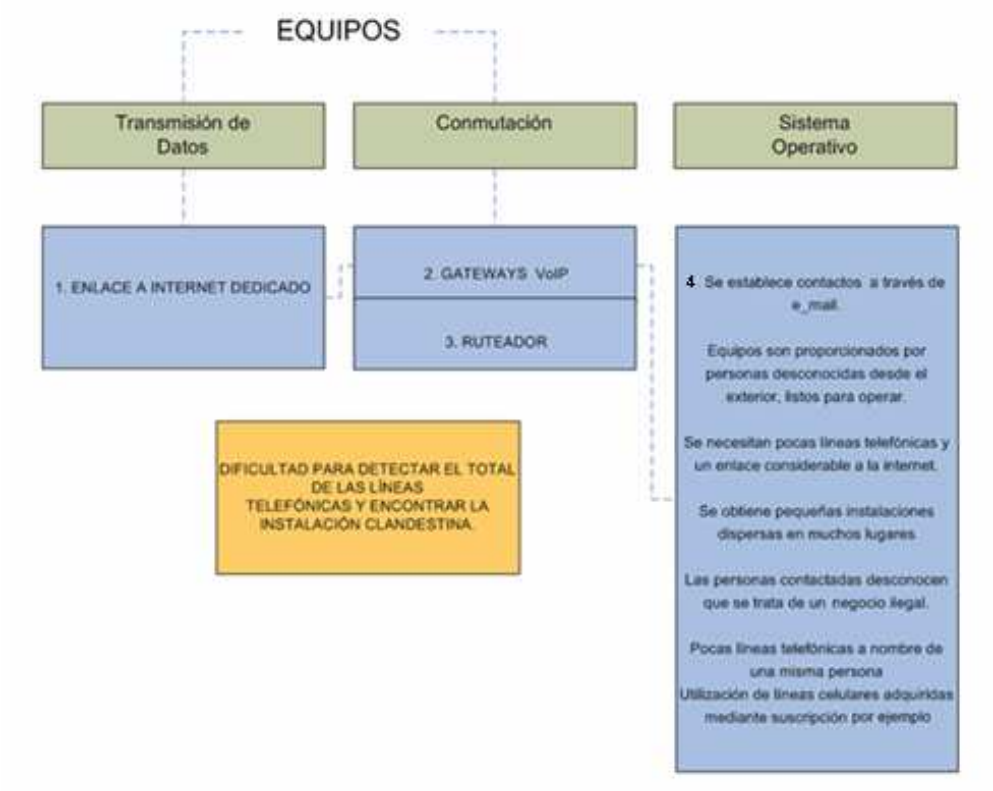
Segunda Etapa:



Tercera Etapa:



Cuarta Etapa:



1.2.12.5 Modalidades de sistemas “By Pass”

Con Líneas Convencionales (Fijas)

Se adquieren líneas convencionales en la empresa operadora y se hace uso de ellas como parte de la instalación “By Pass”.

Líneas correspondientes a una Cuenta

Generalmente mediante Fraude de Suscripción una persona obtiene una Cuenta con una cantidad significativa de números telefónicos, para posteriormente usarlos como terminales para una instalación “By Pass”.

Con Líneas Prepago

Al igual que en el caso anterior, existen usuarios que solicitan líneas prepago que ofrecen bajos costos por minuto, esto generalmente en sitios de venta autorizados y no exactamente en las matricez o sucursales propias de la operadora. La adquisición se realiza generalmente mediante fraude de suscripción, es decir entregando documentación falsa.

Con Líneas de Cabinas Públicas

Últimamente los defraudadores estan apropiándose de ciertos elementos de las cabinas públicas para usarlos en instalaciones “By Pass”, esto con el objetivo de utilizar la línea asignada a dicho teléfono.

Esto, además de provocar la pérdida económica para la operadora en cuanto al tráfico ilegal, se suma la pérdida que supone el daño de dichas cabinas, ya que hasta que los elementos de los cuales los defraudadores se apropiaron no sean repuestos, la cabina queda en desuso.

Con el uso de SIM BOX

Este es un tipo de fraude que afecta específicamente al Sistema Celular; se define como el uso de equipos especiales que permiten la utilización simultánea de una batería de tarjetas SIM[33] para exportar tráfico internacional.

Las tarjetas SIM son obtenidas mediante fraudes de suscripción, para importar o exportar tráfico internacional, típico fraude de "By Pass", a diferencia que están utilizando las redes celulares del propio operador.

Un equipo SIM BOX presenta las siguientes características:

- Permiten el manejo de alto volumen de tráfico.
- Operan como pasarelas o gateway GSM / IP y multiplexores de red.
- Soportan interfaces ANALÓGICAS, BRI[34], PRI[35], VoIP, ISDN[36], IP, etc.
- Su capacidad es modular con incrementos de hasta 60 tarjetas

Existen ciertas condiciones que permiten identificar o detectar el posible uso de una SIM BOX:

- Se registran tan solo llamadas salientes
- No se registra envío ni recepción de SMS
- No existe móvilidad. Actividad detectada en una sola celda.
- Tráfico alto.

[33] SIM – Subscriber Identify Module – Módulo de Identificación del Suscriptor: Es una tarjeta inteligente desmontable usada en teléfonos móviles, que almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un Terminal a otro simplemente cambiando la tarjeta.
[34] BRI - Basic Rate Interface
[35] PRI - Primary Rate Interface
[36] ISDN – Integrated Services Digital Network

1.2.12.6 Detección

La forma de detección de un sistema “By Pass” se explica a continuación:

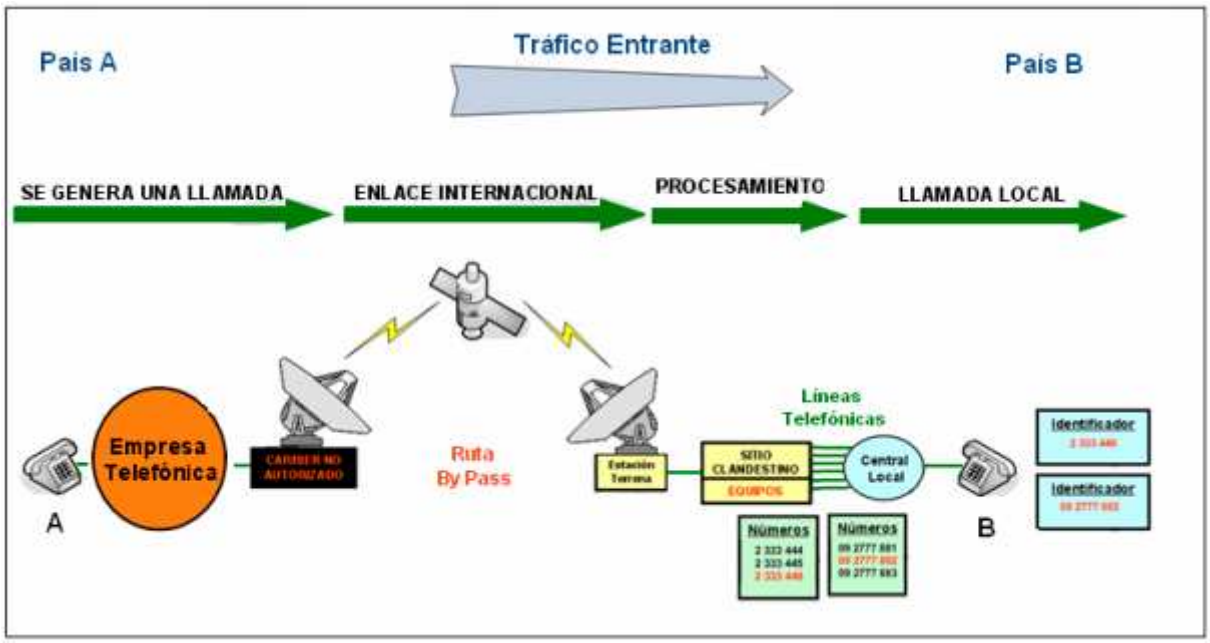


Figura 2.8: Detección de un Sistema “By Pass”

Al ingresar el tráfico al Sitio Clandestino, este es desencapsulado para poder ser enviado analógicamente mediante las Líneas Telefónicas adquiridas por el defraudador, en este momento la Llamada Internacional se convierte en Local, tomando así como identificación el número correspondiente a una de las líneas mencionadas, es por eso, que cuando el usuario del “País B” recibe la llamada, en su identificador visualiza un número local y no el correspondiente a un CARRIER INTERNACIONAL (Ej: 2 1000 14), que es lo que sucede usualmente.

Cada operadora telefónica debe contar con un departamento de Gerencia de Fraude, este departamento debe encargarse de la detección, control y gestión del fraude en telecomunicaciones.

Por parte del departamento se adquieren tarjetas de telefonía internacional en el exterior, considerando que el costo por minuto de llamada sea inferior al costo al cual se comercializan normalmente. Generalmente los costos están en un

promedio de 10 centavos el minuto en estas tarjetas, a pesar de que en la actualidad se están distribuyendo a un costo por minuto similar al de las tarjetas legales, es decir que las ganancias obtenidas por dicho fraude ahora son mucho mayores.

Una vez adquiridas las tarjetas se procede a realizar pruebas para detectar posibles Sistemas tipo “By Pass”, mediante un procedimiento llamado “Pruebas de Lazo o Loop”, el procedimiento se detalla a continuación:

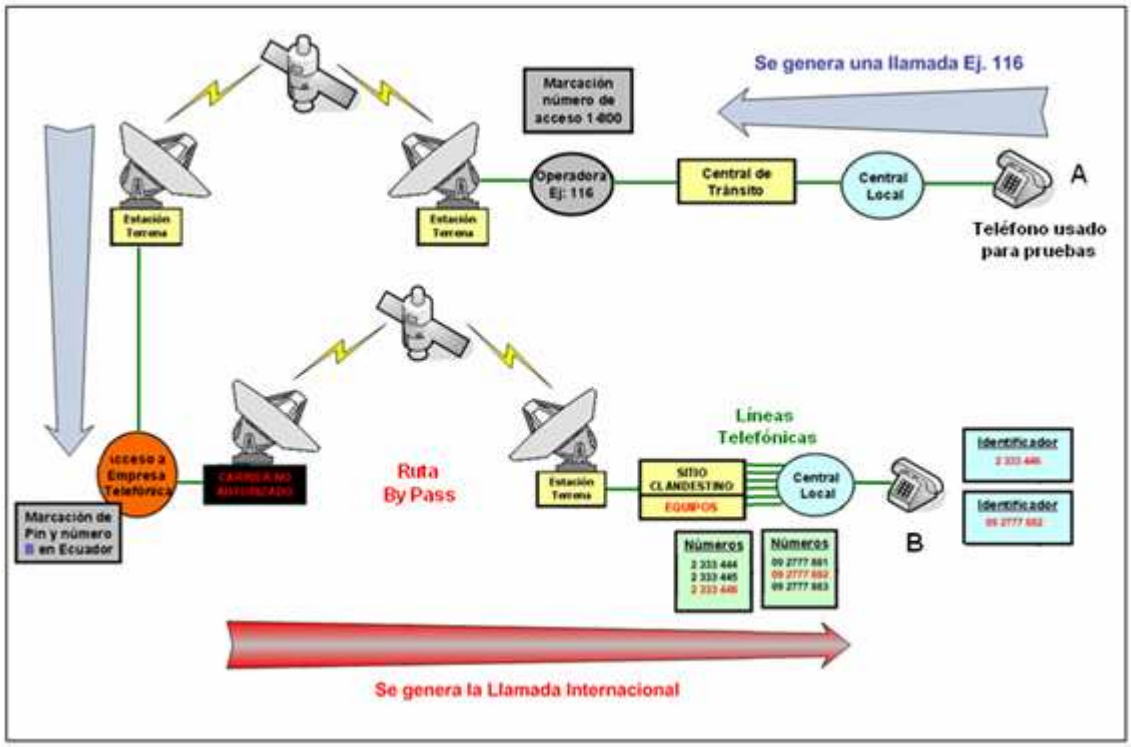


Figura 2.9: Detección de un sistema “By Pass” – “Loop” (Manual)

Se realiza una llamada mediante el uso de la tarjeta de telefonía internacional, adquirida en países donde existe un alto índice de migración ecuatoriana; y se realiza la llamada desde el mismo país donde se quiere identificar el posible fraude.

Se siguen las instrucciones que aparecen en la parte posterior de la tarjeta (Ver Figura 2.11) y de este modo la llamada ingresa a la empresa telefónica en el

“País B”, se proporcionan los datos correspondientes al número de destino (el número de destino es el de un terminal móvil o fijo, el cual está en posesión de quien realiza la prueba). Una vez que la llamada llevó a cabo su proceso (Ver Figura 2.5 y 2.6), el terminal fijo o móvil usado recibirá una llamada; en caso de que dicha llamada sea enrutada legalmente, el número que aparecerá en el identificador será el correspondiente a un CARRIER legalmente establecido, caso contrario (“By Pass”), el número que se visualizará, será un número local correspondiente a la operadora que está siendo afectada por el fraude.

Existe también la opción de realizar estas pruebas mediante un software; de esta manera se logra un control más eficaz ya que se obtendrá un número significativamente mayor de pruebas.

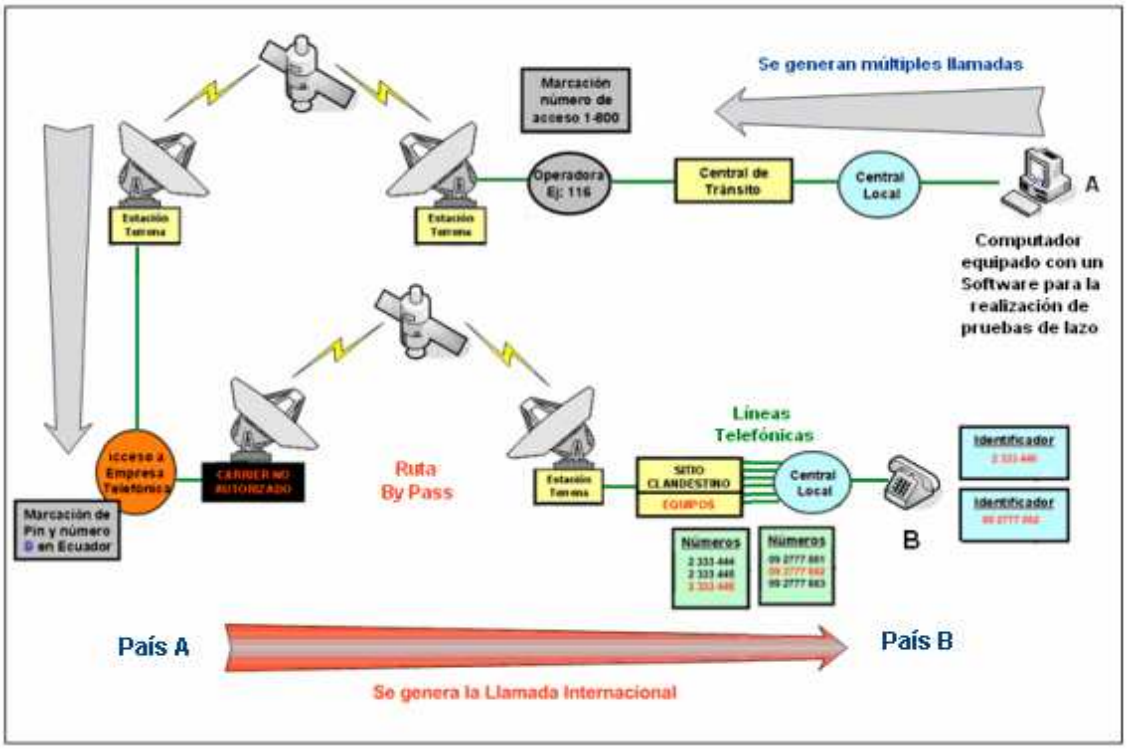


Figura 2.10: Detección de un sistema “By Pass” – “Loop” (Automático)

Figura 2.11: Tarjeta de Telefonía Internacional Prepagada

Una vez identificado el número o números que presuntamente pertenecerían a una instalación “By Pass” se procede a realizar la investigación respectiva para saber a quien pertenecen dichos números.

En el caso de que el número identificado corresponda a la serie de una Operadora de Telefonía Fija, la identificación del concesionario del número es relativamente fácil (en caso de que no exista Fraude de Suscripción en la adquisición de las líneas), ya que al ser “fijo”, se conoce exactamente la ubicación física de la línea.

Sucede lo contrario en el caso de que el número detectado corresponda a la serie de un Operador de Telefonía Móvil, ya que a pesar de que la empresa operadora tenga toda la información del usuario a quien pertenece el número, es muy difícil identificar el lugar en que se encuentra el terminal de dicho número.

Se han desarrollado algunos métodos para la posible ubicación de estos terminales, pero hasta el momento han resultado muy poco exactos. Debido a esto la ubicación de una instalación tipo “By Pass” con terminales móviles representa hoy en día uno de los mayores problemas para las operadoras de Telefonía Móvil.

1.2.12.7 Técnicas para la ubicación de un Sistema “By Pass”

En telefonía fija:

- Verificación en las Bases de Datos de la Empresa Operadora, para obtener la ubicación de la o las líneas según el o los números detectados.
- Verificación de los datos técnicos de instalación de las líneas.
- Seguimiento físico de los pares telefónicos.
- Identificación de la posición de los pares en el distribuidor telefónico.

En telefonía celular:

- Verificación de los datos personales de los clientes.
- Estudio de los parámetros técnicos de los aparatos celulares.
- Investigación sobre las características del enlace internacional.
- Estudio sobre el comportamiento de las líneas implicadas.

1.2.12.8 Prevención

Las empresas operadoras deben tomar en cuenta ciertos aspectos de seguridad en cuanto a la forma de distribuir o concesionar las líneas o chips a sus clientes (evitar fraude de suscripción); esto a fin de verificar a quien pertenecen las líneas, en caso de que se de un comportamiento poco usual en el tráfico que producen las mismas.

Se debe mantener e intensificar las pruebas técnicas de tráfico telefónico internacional realizadas por cada operadora, para lograr determinar los números telefónicos que se están utilizando para cursar tráfico telefónico ilegal.

Conviene solicitar a las empresas de telefonía móvil celular, el cambio de las series numéricas de las líneas telefónicas celulares detectadas; y, de aquellas series que no están protegidas contra la clonación.

Debe existir un estudio frecuente del tráfico generado y recibido por las líneas que pertenecen a cada operadora, en caso de detectar un comportamiento inusual, deberá procederse a la suspensión de dichas líneas, para evitar que se siga cursando tráfico ilegal.

La Superintendencia de Telecomunicaciones, solicita que las operadoras suscriban un acta de compromiso con sus usuarios, en la que garanticen el correcto uso del servicio, a fin de que en caso de mal uso de los mismos, este documento sirva como apoyo en los procesos legales que, en un caso de "By Pass", corresponden.

1.2.12.9 Control

Adquisición de equipos dotados de hardware y software que, con algoritmos característicos del fraude, están en la capacidad de identificar la operación de sistemas fraudulentos.

Realizar análisis de los CDRs[37] correspondientes a las llamadas realizadas y recibidas mediante las líneas de cada operadora, con el fin de determinar las características de las mismas y verificar su comportamiento.

Conformación de grupos de monitoreo permanentes, encargados de identificar el posible cometimiento de fraude telefónico.

Disposición de un grupo de élite, encargado de intervenir, desmontar y desarticular las bandas que clandestinamente prestan servicios ilegales de telecomunicaciones.

[37] CDRs - Call Detail Record

1.2.13 CALLBACK VOIP

Es el procedimiento mediante el cual se revierte el origen del tráfico internacional, haciendo una llamada disparo que no es contestada o tiene muy corta duración, para que un equipo en el otro extremo obtenga la información del llamante y devuelva la llamada con tono de ese otro país.

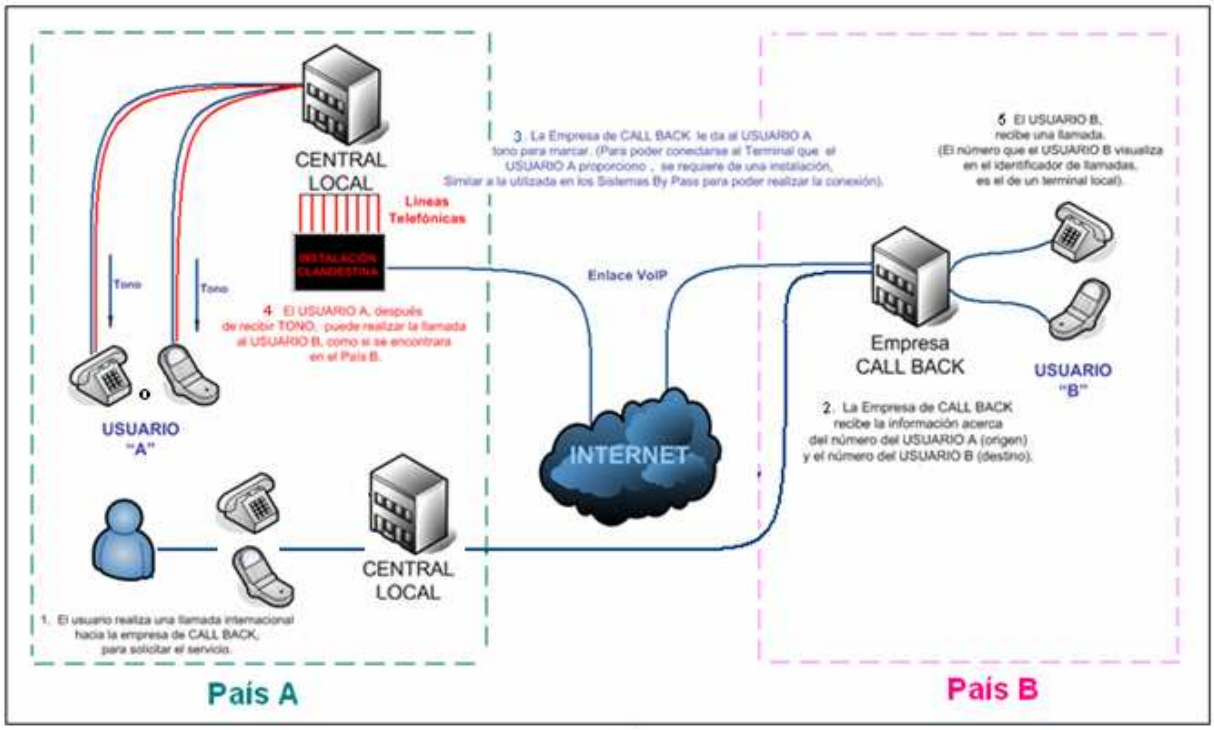


Figura 2.12: Sistema Callback VoIP

La existencia de este tipo de Fraude se presenta debido a que las tarifas para llamadas internacionales en ciertos países son sumamente elevadas.

Dicho servicio está a disposición del público, en páginas de Internet generalmente. Es realmente muy fácil encontrar en la red este tipo de servicio ya que existen una gran cantidad de empresas que lo ofrecen.

A continuación se muestran unos ejemplos:

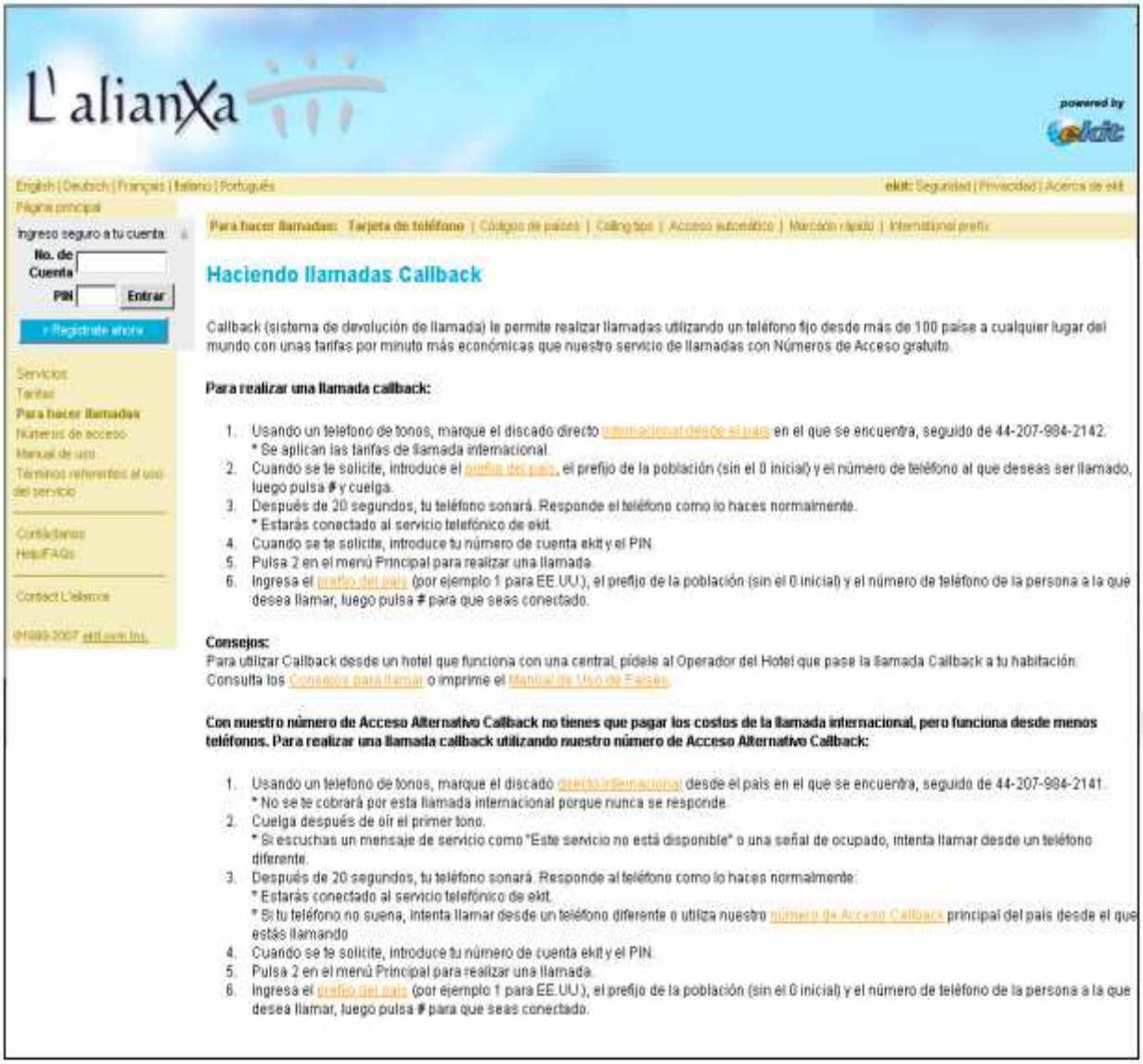


Figura 2.13: Página WEB que ofrece el servicio de Callback [21]

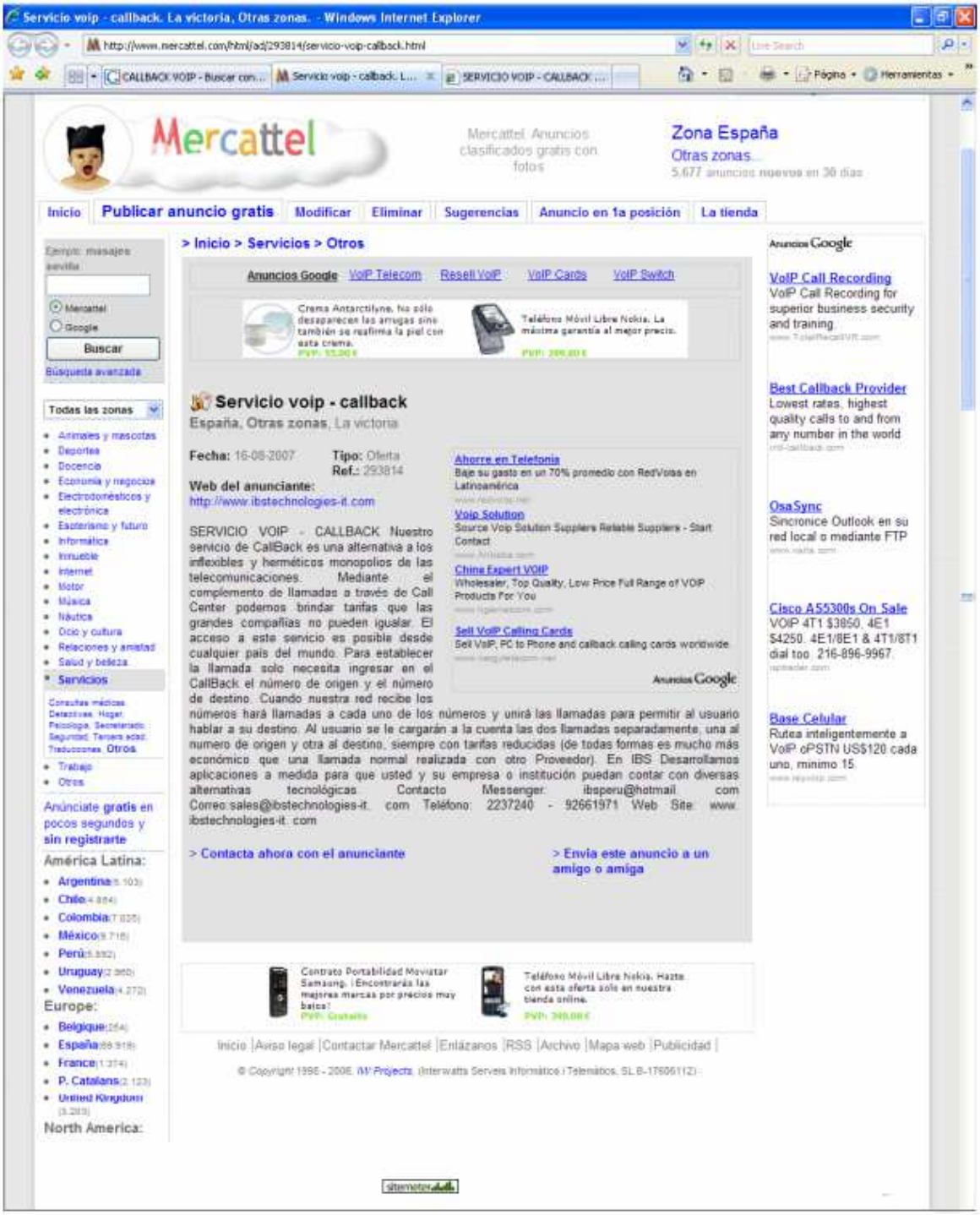


Figura 2.14: Página WEB que ofrece el servicio de VoIP – Callback [22]

Es interesante mencionar que, a partir del 2005 se presentó una técnica variante en cuanto a la ejecución del Callback, en dicha técnica, la llamada telefónica internacional de disparo hacia la empresa que presta ese servicio desde el exterior, se realiza mediante una llamada VoIP, generada incluso desde una

página Web donde se publicita el servicio. De esta manera, la llamada internacional de retorno dirigida desde la empresa extranjera hacia un número telefónico en nuestro país, se registrará por la operadora afectada simplemente como una llamada local, ya que los defraudadores disponen de una Instalación Clandestina la cual permitirá la conexión, desconociendo que constituye en realidad la llamada internacional que permitirá brindar el servicio Callback, pues, dicha llamada al ser recibida por el cliente, brindará tono para marcar tal y como si se encontrara en el exterior, de esta manera la empresa afectada no cuenta con los parámetros técnicos necesarios para evidenciar el servicio fraudulento del cual está siendo víctima.

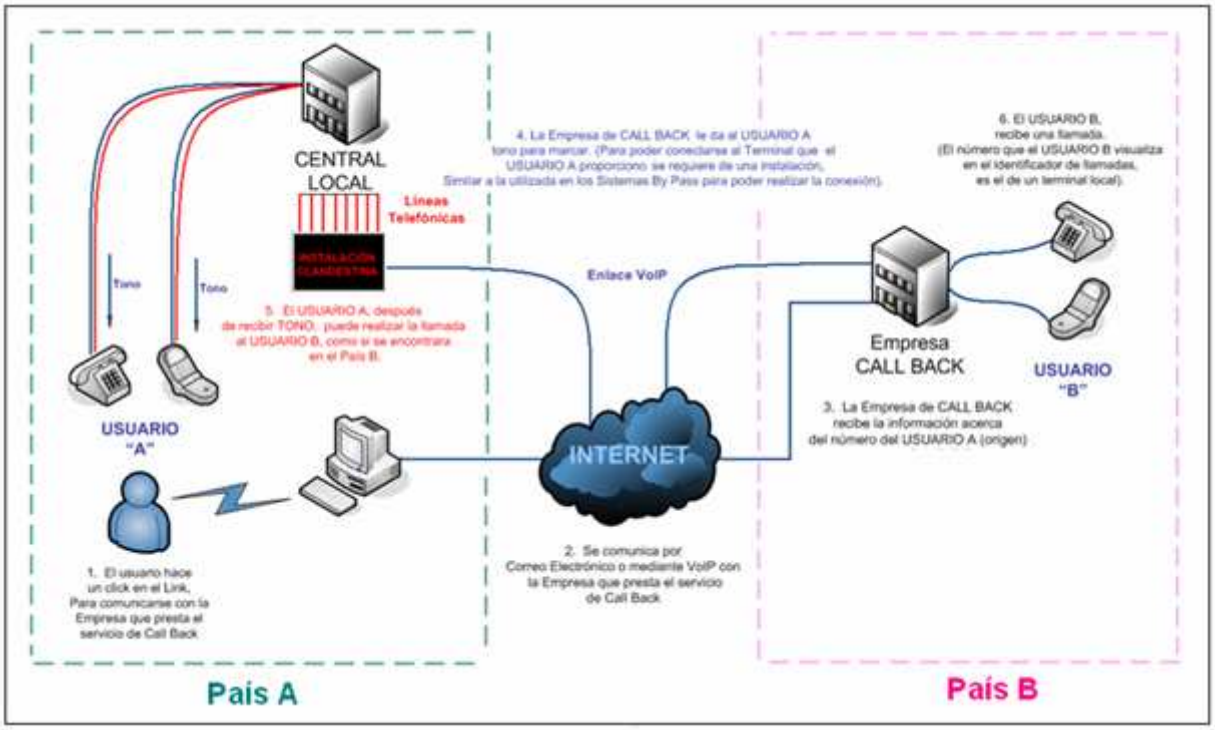


Figura 2.15: Sistema Callback formado íntegramente con VoIP

1.2.13.1 Detección y Corrección

En este caso, no existe un método específico para la detección de este tipo de fraude, pero pueden considerarse ciertos aspectos que podrían ayudar en la detección:

La operadora telefónica puede realizar un análisis del comportamiento de las líneas que pertenecen a su red. Una manera de asumir que se esta dando este tipo de fraude se da cuando se detectan grandes cantidades de llamadas hacia un solo destino en el extranjero, con duración mínima.

El servicio Callback puede incluso escapar a las técnicas de detección, al ser implementado íntegramente con tecnología VoIP, en cuyo caso tanto la llamada internacional de disparo como la de retorno, se cursarán independientes al control de la operadora afectada, quien bajo esas circunstancias técnicas, percibirá a la llamada internacional de retorno como si se tratara solamente de una llamada local.

Con estas consideraciones, la detección de este tipo de fraude combinado, se hace posible realizar en dos etapas; la primera, con la identificación de los portales Web donde se ofrece el servicio Callback hacia nuestro país, mismo que deberá ser solicitado; la segunda, dotando de un identificador de llamadas, al terminal telefónico que recibirá la llamada internacional de retorno.

Entonces al hacer uso del servicio, será posible identificar los números de las líneas telefónicas utilizadas para terminar las llamadas internacionales de retorno en nuestro país.

Con los números telefónicos identificados, será posible efectuar las acciones técnicas necesarias para localizar el sitio donde se encuentra la infraestructura de telecomunicaciones utilizada para prestar este servicio ilegal.

1.2.14 REFILLING

Procedimiento mediante el cual el país que origina el tráfico lo enruta a un tercer país, que no es el destino final; ese tercer país, reenruta este tráfico hasta su último destino.

Debido a las diferencias tarifarias entre los países en el proceso, el país que origina el tráfico paga una tarifa más baja al tercero, el cual genera nuevos ingresos al obtener el tráfico adicional. Todo lo anterior a costa de menores ingresos para el país destino.

En el caso de un Refilling interno, la Empresa Operadora legalmente establecida en el País A llega a un acuerdo con la empresa operadora legalmente establecida en el País C, para que el tráfico telefónico internacional originado en el País A y destinado al País B, pase primero por dicha operadora; esto debido a que los cargos tarifarios entre el País A y el País B son sumamente altos, entonces, de la manera explicada, al reenrutar las llamadas, los costos de interconexión y terminación de llamada a pagar por el País A son menores. Cabe mencionar que si el Sistema Refilling se efectúa de la manera señalada, no es necesario el uso de la Voz sobre IP.

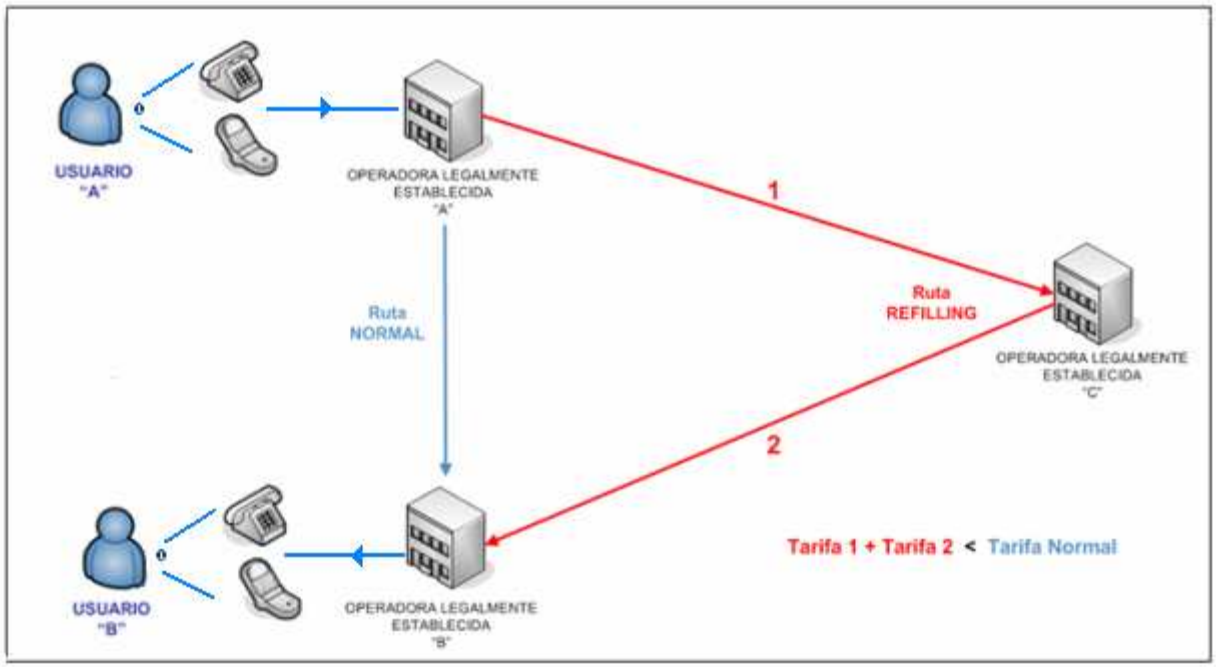


Figura 2.16: Sistema Refilling Interno

Existe también la posibilidad de que este tipo de fraude se realice mediante VoIP, en este caso no se llega a ningún acuerdo con la Empresa Operadora del País C,

por el contrario, se hace uso de una instalación clandestina en el mencionado País

Los sistemas refilling, que son constituidos utilizando tecnología VoIP, están estructurados de esa manera dentro del transporte y procesamiento de la información telefónica al igual que los denominados sistemas “By Pass”, con la única diferencia que los sistemas refilling no terminan las llamadas telefónicas internacionales en el país donde se encuentran instalados, es decir, un sistema refilling, desde las líneas telefónicas que lo conforman realiza la marcación hacia destinos internacionales y no hacia locales como lo hace un sistema “By Pass”.

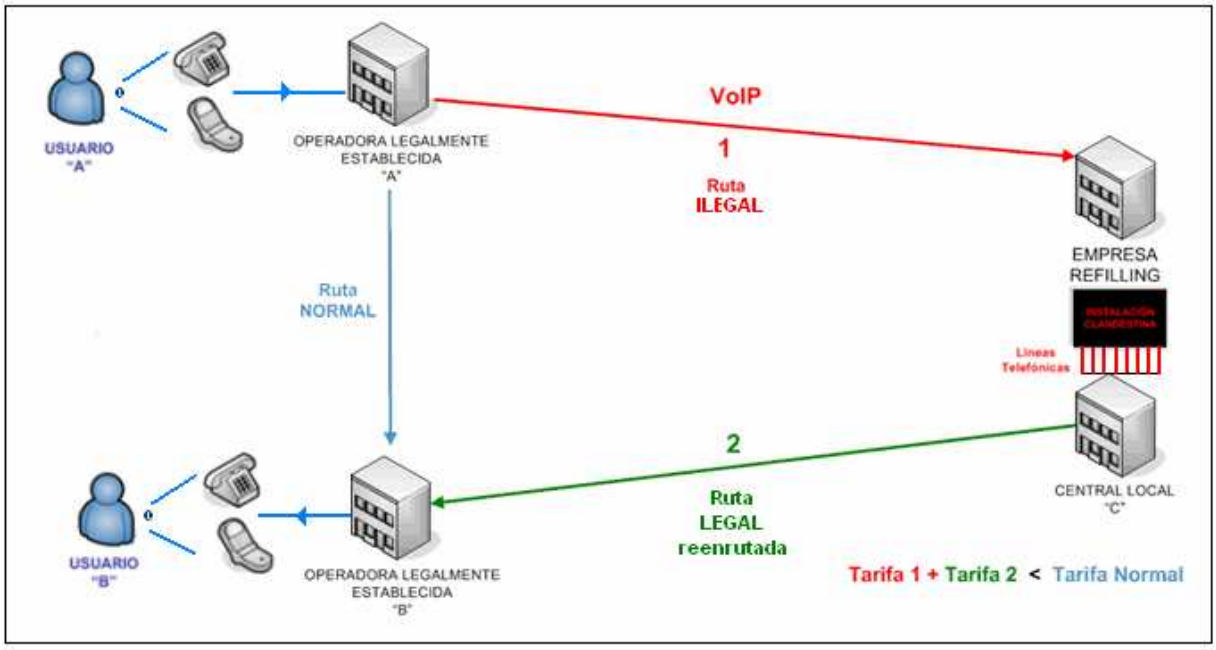


Figura 2.17: Sistema Refilling VoIP

En el caso de un Sistema Refilling con Voz sobre IP, el fraude es generalmente realizado por terceros, es decir por personas ajenas a las Empresas Operadoras. En este tipo de fraude, no solo son afectados los intereses de la Operadora de Destino, al no adoptar los réditos por recibir una llamada internacional proveniente del País A; si no también la operadora C, ya que además de enrutar las llamadas

internacionales con destino B que pertenecen a su propio país, deberá enrutar hacia el mismo destino las llamadas provenientes del País A.

1.2.14.1 Detección y Corrección

Es bastante común en la actualidad, que al detectar técnicamente números utilizados en sistemas “By Pass”, esos números también estén siendo empleados en sistemas refilling; sin embargo, a fin de efectuar un control más específico y que resulta oportuno, las operadoras telefónicas internacionales para combatir los sistemas refilling implementan procedimientos que cuantifican estadísticamente los volúmenes de tráfico telefónico internacional cursado hacia diversos países, de tal manera que, al detectarse un incremento sustancial a cualquiera de esos destinos, se obtenga una alerta que indique un incremento no justificado.

Posteriormente, se identifica a aquellos números que generaron altos volúmenes de tráfico internacional hacia un mismo destino, para así, basándose en la información tanto administrativa como técnica de esos números, efectuar una investigación que permita ubicar la infraestructura de telecomunicaciones que conforma el sistema refilling detectado, tal como si se tratara de un sistema “By Pass”.

Cabe señalar, que los sistemas refilling tienen su razón de ser, básicamente en las circunstancias de carácter comercial y político entre ciertos países, las cuales inciden directamente en las tasas de terminación de llamadas establecidas de un país a otro. Ese es el caso entre USA y CUBA. El costo de interconexión y terminación de una llamada proveniente de los Estados Unidos hacia Cuba, es sumamente alto (1 USD por minuto, en promedio).

El hecho por el cual son tan “famosos” los sistemas refilling hacia CUBA, radica en que no sería muy buena idea instalar un Sistema “By Pass” en el mencionado país; esto debido a que las sanciones aplicadas a un defraudador en este país serían sumamente severas, no solo por cometer este tipo de fraude en si, sino por

el hecho de haber realizado negocios con un país con el que no se tienen las mejores relaciones.

1.2.15 VISHING

Una de las herramientas más populares entre los cracker desde los comienzos de la comunicación informática es el war - dialling, el cracker utiliza un programa para que su equipo realice llamadas (mediante un módem) a secuencias de números de teléfono semialeatorias dentro de una zona. Si responde un módem, entonces se puede asumir con seguridad que su interlocutor es un ordenador. A continuación, la lista de respuestas de módem (ordenadores) puede convertirse en el objetivo de la intrusión informática para, de ese modo, obtener lo que busca.

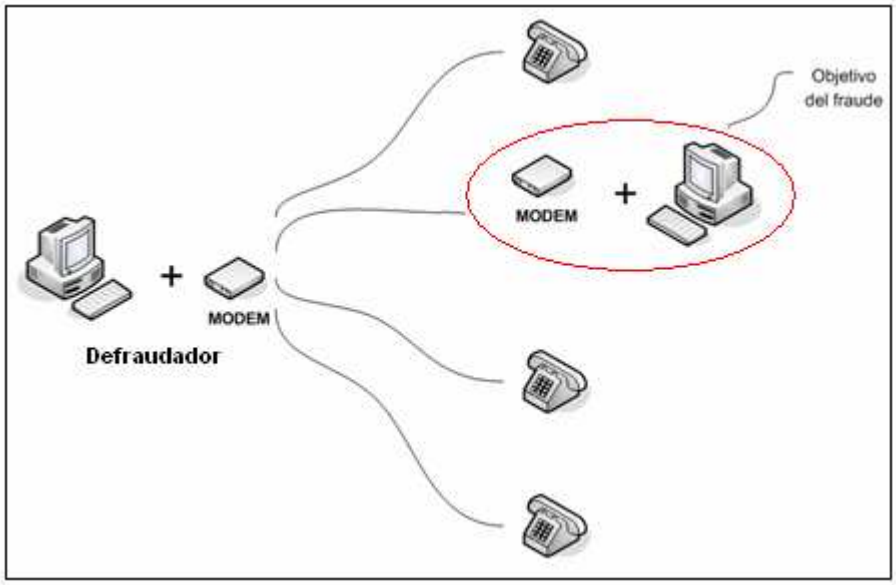


Figura 2.18: War - dialling

Puesto que los módem ya no son muy utilizados, han ocupado su lugar los ataques del tipo port scan (buscadores de puertos) que pueden llevar a cabo funciones muy parecidas. Desde un ordenador, el intruso explora un intervalo de direcciones IP en busca de equipos con puertos especiales abiertos. Los que dan una respuesta positiva son más susceptibles de ser el objetivo de una

exploración más minuciosa que se materializa en un intento de intrusión para acabar en un control absoluto del ordenador. A continuación, el intruso puede utilizar el ordenador para cualquier fin que desee (spamming, botnets, etc.).

En términos generales podríamos definir el phishing como:

Un ataque de ingeniería social que intenta engañarle para que revele información personal, como contraseñas y números de tarjeta de crédito, con la intención de cometer un fraude.

Vishing es el resultado de combinar las dos técnicas mencionadas anteriormente, el uso de la Voz sobre IP (VoIP) y el phishing.

La telefonía IP permite en muchos países tener un número local, que en muchos de los casos no corresponde al lugar en que el Terminal se encuentra físicamente, es decir, que en realidad puede estar operando en otra parte del mundo. Este nuevo fraude consiste en el envío de un correo electrónico que especifica un teléfono gratuito al que llamar, donde voces automáticas con un aspecto muy profesional, convencen a la víctima para que facilite su información personal, como su número de cuenta, tarjeta, número PIN, etc.

Para llegar a gente que ni siquiera tiene Internet, incluso se dedican a llamar a toda una zona, dejando mensajes en el contestador automático del estilo "Llame inmediatamente al número xxxxxxx, pues hay importantes problemas con su cuenta bancaria". El hecho del bajo precio o incluso la gratuidad de las llamadas por Voz sobre IP incrementa estas prácticas delictivas.

1.2.15.1 Modo de Operación

1. Se utiliza un ordenador para realizar llamadas a secuencias de números (la parte "V")

El primer paso consiste en configurar un equipo que utilice voz sobre IP (VoIP)

para llamar a muchos números de teléfono pertenecientes a una zona. A diferencia de la técnica del war-dialling, aquí la distancia no es un problema ya que el coste telefónico deja de tener importancia. No obstante, tal y como veremos en el segundo punto, el idioma empleado en la región a la que se llama puede ser crucial para el éxito del vishing.

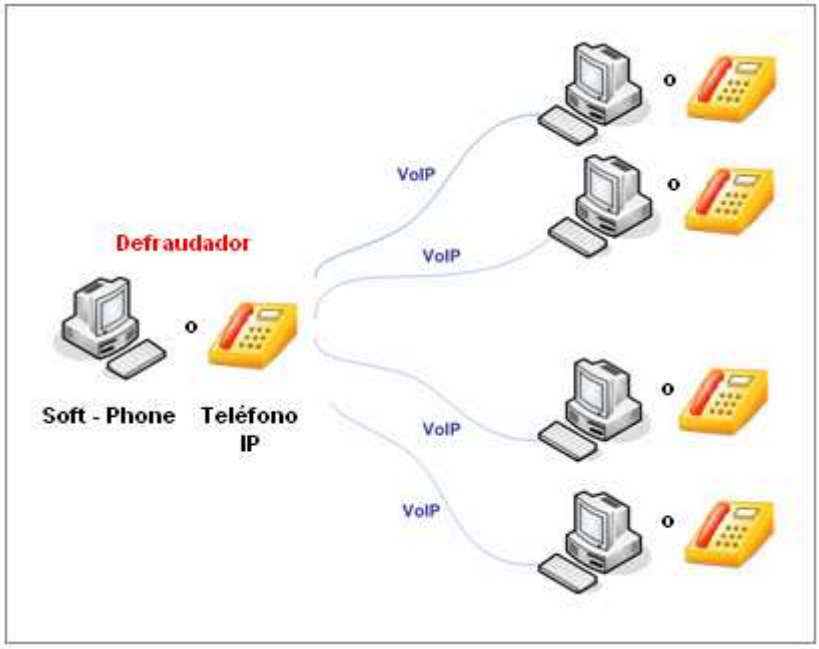


Figura 2.19: Vishing (Parte "V")

2. Se reproduce un mensaje pregrabado (la parte "ishing")

Probablemente algunos números a los que se llame responderán. La persona que haya puesto en marcha todo el plan tendrá en ese momento un mensaje pregrabado que desempeña la función del phishing. Por ejemplo, puede recibir un mensaje que parece proceder del departamento de fraudes de tarjetas de crédito del banco y en él se le proporcionan instrucciones para llamar a otro número de teléfono y así poder arreglar el problema.

Este mensaje pregrabado debe realizarse en el mismo idioma que el utilizado en la región en la que se realiza el Vishing. Un mensaje automático, por ejemplo, enviado en alemán a personas de Francia que afirme proceder de su banco no

resulta muy creíble y sólo conseguirá engañar a los más crédulos (quienes por supuesto podrían ser el objetivo).

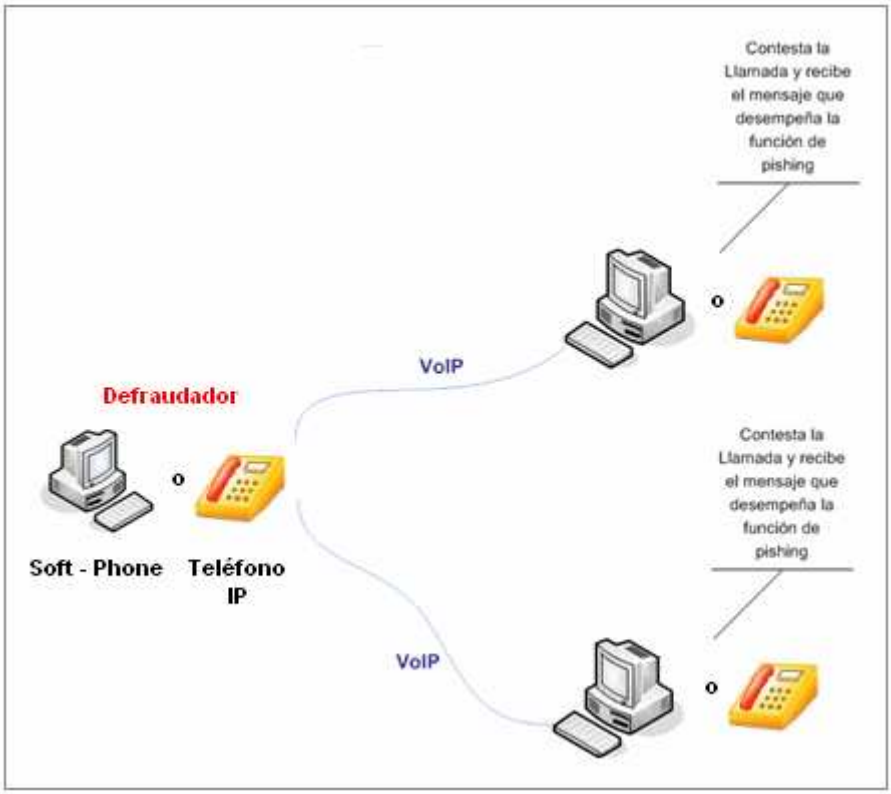


Figura 2.20: Vishing (Parte "ishing")

3. Se obtiene la información

Si el engaño del punto 2 resulta convincente, algunos de los que contestaron a la llamada automática y escucharon el mensaje llamarán al número sugerido.

En este paso, el intruso dispone de varias opciones:

- Puede utilizar sus habilidades de ingeniería social personales y responder al teléfono en persona para intentar engañar a la persona y que ésta le facilite información personal, como el número de tarjeta de crédito, su código PIN, fecha de nacimiento, dirección, etc. En este paso, la opción con un mayor índice de éxitos es el contacto telefónico personal. No

obstante, la desventaja es que el intruso sólo puede hablar con una persona al mismo tiempo.

- Puede grabar con anterioridad otro mensaje en el que se cuente alguna historia creíble para intentar engañar a la persona y que de ese modo desvele información personal.

Por ejemplo, una historia creíble podría ser que el departamento de tarjetas de crédito del banco ha sufrido una avería en sus bases de datos al mismo tiempo que se han robado algunos números de tarjetas de crédito. Puesto que la información de base de datos y de clientes no está disponible, se le pregunta a la persona en cuestión si no le importaría introducir su número de tarjeta de crédito y el número de teléfono, y el banco le devolverá la llamada en el caso de que la tarjeta de crédito se encuentre entre las extraviadas.

Las técnicas de persuasión que se pueden utilizar en esta situación sólo se ven limitadas por la imaginación del estafador. La desventaja es que la invención tiene que ser lo bastante general como para que se aplique y convenza al mayor número de personas posible.

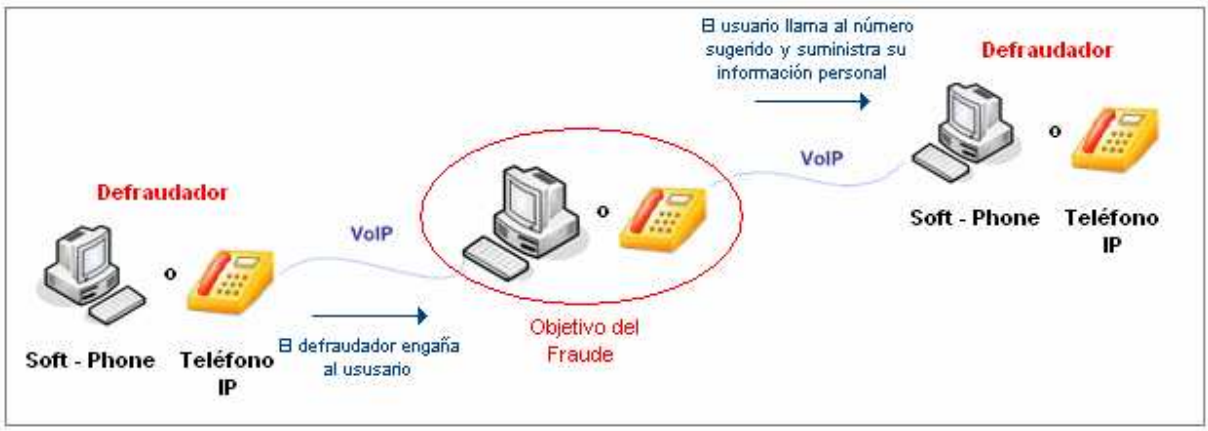


Figura 2.21: Obtención de la información

4. Se comete el fraude y/o se obtiene más información

A continuación, si la recopilación de información obtenida mediante los tres pasos anteriores ha tenido éxito, el estafador puede utilizar esa información para cometer el fraude en sí. En el ejemplo mencionado anteriormente, se trataba de un fraude de tarjetas de crédito, pero podría tratarse de cualquier cosa.

En este punto, el estafador también puede utilizar la información recopilada para obtener incluso más información, en lo que sería la conspiración definitiva (aunque poco común), que le permitiría adoptar la identidad de la otra persona.

1.2.15.2 Control y Prevención

Se están utilizando nuevas aplicaciones (en ese caso la mensajería instantánea) para propagar el software malintencionado. Esto ocurría principalmente porque la mensajería instantánea era un medio nuevo y los usuarios no estaban alerta de la misma forma que lo estaban con respecto a, por ejemplo, el uso de mensajes de correo electrónico para distribuir el software malintencionado.

La atención que las organizaciones de seguridad, las financieras y los medios han dedicado al Phishing ha sido bastante exhaustiva desde hace algún tiempo. El enfoque se ha centrado principalmente en los intentos de Phishing a través del correo electrónico; sin embargo, una nueva manera (Voz sobre IP), utilizado como canal de comunicaciones para el Phishing, proporcionará durante algún tiempo un índice de éxito mayor que el que obtenía el Phishing con canales más tradicionales.

Esto siempre es así cuando se empiezan a utilizar nuevos canales; el consejo general que se puede aplicar, independientemente de los medios y técnicas empleadas por los estafadores, es el siguiente:

“Utilizar el escepticismo inteligente en cualquier relación en la que se le pida que divulgue datos personales”

La AUI[38] recomienda que siempre que se tenga que hablar con el banco se lo haga a través de los números de teléfono oficiales que aparecen en la tarjeta de crédito, y no suministrar datos financieros a través de un correo electrónico ni de un teléfono que se facilitaría para realizar llamadas mediante VoIP.

Cabe mencionar que existe otro tipo de fraude similar llamado **Smishing,** este consiste prácticamente en lo mismo, pero usando los mensajes SMS de los teléfonos móviles como captación de la víctima. Al llamar se encuentra con los mismos tipos de conversaciones grabadas, que sutilmente hacen que el estafado proporcione los datos de su cuenta.

1.2.16 VBOMBING

Existe un problema de seguridad recientemente descubierto, nos referimos al llamado Vbombing, en el cual no sólo se compromete el contenido de una conversación, sino también la información sobre la propia llamada. Estos datos podrían ser interceptados y registrados por terceros para conocer las llamadas entrantes y salientes de un Terminal y luego configurar y dirigir llamadas sin consentimiento del propietario hacia un único Terminal VoIP o grabar los datos de todos sus contactos para “bombardear” sus buzones de voz IP con spot (Spam over Internet Telephony). Otro riesgo es que los paquetes de datos sean interceptados para alterar los parámetros de una llamada, escuchar una conversación o retransmitirla íntegramente.

Prevención

Una de las formas de proteger las comunicaciones basadas en voz sobre IP es la “encriptación”, tanto de la señal de la llamada (para que las direcciones de teléfono no aparezcan con claridad) como de los paquetes de datos (lo que prácticamente impide insertar palabras en una conversación). Esto implica perder

[38] AUI –Asociación de Usuarios de Internet

ancho de banda, algo que se solucionaría, según los expertos, cambiando a la última versión del Protocolo de Internet (IPv6).

Además, es importante proteger periódicamente de hackers y spammers los elementos que componen la red VoIP (terminales, gatekeepers, gateways, enrutadores, conmutadores, etc.) con las actualizaciones y parches oportunos.

Estructurar la red separando voz y datos para llevar una gestión paralela puede ser de ayuda también a la hora de garantizar una mayor seguridad y calidad del servicio.

FRAUDES MÁS COMUNES EN EL ECUADOR

Se puede manifestar que, actualmente en el Ecuador los principales fraudes en los cuales se utiliza tecnología VoIP, son los siguientes: los denominados sistemas telefónicos “By Pass” o llamadas derivadas; el “Refilling” o reoriginación de llamadas y el “call back” o llamadas revertidas; así también, se han presentado ataques a la infraestructura de VoIP de diversas empresas, sea que presten servicios de telecomunicaciones o que solo utilicen dichos servicios, esto a nivel de accesos fraudulentos a “gateways” o “softswitch” con los que cuentan dichas empresas, la técnica de fraude implementada en esos casos permite al defraudador obtener diversas opciones de utilización de la infraestructura vulnerada, y así obtener los servicios que se prestan sobre esa plataforma tecnológica, causando perjuicios económicos a la empresa propietaria de la infraestructura mencionada.

El Vishing y el Vbombing, en nuestro país no están aún muy difundidos, sobre todo por que el uso el servicio de Internet es bastante deficiente. Todo lo contrario sucede en países desarrollados, en los cuales, sobre todo el Vishing es uno de los fraudes más comunes.

SEGURIDAD EN SISTEMAS VoIP

Los riesgos que conlleva usar sistemas VoIP no son muy diferentes de los que se pueden encontrar en las redes habituales de IP.

Lo primero que se debería tener en mente a la hora de usar Voz sobre IP es la encriptación, aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz, encriptar es la única forma de prevenir un ataque.

Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN, el protocolo IPsec (IP segura) y otros protocolos como SRTP (Secure RTP). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente y emplear un procesador dedicado de encriptación.

Lo próximo, como debería esperarse, podría ser el proceso de asegurar todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Se necesita configurar cada uno de esos dispositivos para asegurar que estén en línea con lo que se demanda en términos de seguridad.

Los servidores pueden tener pequeñas funciones trabajando y sólo abriendo los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberían estar actualizados en términos de parches.

Por último, se puede emplear un firewall y un IDS[39] para ayudar a proteger la red de voz. Los firewalls de VoIP son complicados de manejar y tienen múltiples requerimientos; los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones, lo cual haría que el manejo del firewall sea más dificultoso.

[39] IDS - Intrusion Detection System

Un IDS puede monitorizar la red para detectar cualquier anomalía en el servicio o un abuso potencial, las advertencias son una clave para prevenir los ataques posteriores. Y sin duda no hay mejor defensa que estar prevenido para el ataque.

1.2.17 REDES PRIVADAS VIRTUALES – VPN

Es una red privada que se extiende mediante un proceso de encapsulación y en su caso de encriptación de los paquetes de datos a distintos puntos remotos, mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública

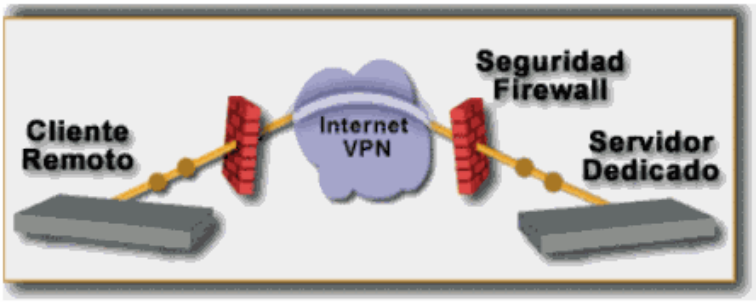


Figura 2.22: Como funciona una VPN

En la figura anterior se muestra como viajan los datos a través de una VPN, desde el servidor dedicado parten los datos, llegando a el firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de internet donde se genera un túnel dedicado únicamente para nuestros datos, para que estos con una velocidad y ancho de banda garantizado, lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como IP, IPsec, Frame Relay, ATM, etc.

1.2.18 IPSec

La meta de este protocolo es proporcionar varios servicios de seguridad para el tráfico de la capa IP, tanto a través de IPv4 e IPv6. Los componentes fundamentales de la arquitectura de seguridad IPSec son los siguientes:

- Protocolos de Seguridad: Cabecera de autenticación (AH) y los Datos Seguros Encapsulados (ESP).
- Asociaciones de Seguridad.
- Manejo de Clave: manual y automática (Internet Key Exchange, IKE).
- Algoritmos para la autenticación y encriptación.

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue adecuado a IPv4. La arquitectura IPsec se describe en el RFC2401.

IPsec emplea dos protocolos diferentes (AH (Authentication Header, protocolo IP 51) y ESP (Encapsulated Security Payload, protocolo IP 50)), para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores; estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en extractos HMAC[40]. Para el cálculo de estos HMAC se emplean algoritmos de como MD5 y SHA para calcular

[40] HMAC - Hash Message Authentication Codes

un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar si este tiene acceso a la clave secreta.

Para proteger la confidencialidad de los datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad SA[41]. Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad SAD[42].

1.2.19 FIREWALLS

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuales de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información de Internet deberá pasar a través del mismo, donde los datos podrán

[41] SA - Security Associations
[42] SAD - Security Asocciation Databases

ser inspeccionados. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñado para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

CAPITULO III

DESARROLLO DE LOS SERVICIOS BASADOS EN LA TECNOLOGÍA DE VOZ SOBRE IP

INTRODUCCIÓN

La transmisión de tráfico de voz sobre redes de paquetes ha experimentado grandes avances en los últimos años, tanto por el desarrollo de estándares como por la aparición de productos basados en tecnología IP. A mediano plazo esta tecnología se vislumbra prometedora motivada por su utilización en redes móviles de tecnología UMTS y el salto de tecnología de transmisión de voz tradicional hacia tecnologías de transmisión de Voz sobre IP (VoIP) basadas en el despliegue de una única red de paquetes integradora de todos los servicios.

Durante los primeros pasos de esta tecnología se fijó como aspecto diferenciador, respecto a la tecnología clásica de transmisión basada en circuitos, los aspectos relacionados con el costo, especialmente en entornos corporativos donde existe una red de datos, típicamente propiedad de la propia organización y una red telefónica, normalmente contratada a uno o varios operadores con facilidades de grupo cerrado de usuarios, numeración reducida, etc. Sin embargo la reducción de los precios del mercado motivada por la aparición de la competencia en el mismo, junto con la falta de soluciones que garanticen de un modo eficiente calidad para la transmisión sobre redes de datos, han provocado que esta tecnología no haya tenido el éxito esperado por las primeras previsiones. Hasta ahora existen distintos ejemplos tanto de operadores que han apostado por esta tecnología para ofrecer el servicio de voz, como de organizaciones privadas. Sin embargo, en ambos casos, estas entidades han debido realizar un sobredimensionado de la red para garantizar aspectos de QoS.

El presente capítulo introduce las más difundidas tecnologías de transmisión de VoIP actualmente estandarizadas, así como el análisis del Marco Regulatorio en nuestro país para la prestación de sus servicios.

APLICACIONES DE VOZ SOBRE IP

La Voz sobre IP es la tecnología que permite la conexión de conversaciones de voz sobre Internet o red de ordenadores. Se pueden realizar llamadas telefónicas a cualquier lugar del mundo, tanto a números VoIP como a personas con números telefónicos fijos o móviles.

Las nuevas tecnologías VoIP son las alternativas más demandadas en los últimos años debido a los avanzados servicios que pueden ofrecer. Características tales como recepción de mensajes de voz en una cuenta de correo (voicemail), identificar llamadas entrantes y transferirlas a los usuarios apropiados, etc. son servicios básicos. Puesto que estas características son módulos de software que funcionan sobre un servidor estándar, básicamente no hay limitaciones a desarrollar nuevas funciones y características. La telefonía tradicional puede ofrecer tales posibilidades pero a precios elevados, mientras que los proveedores de VoIP lo ofrecen como un servicio básico.

Con VoIP no sólo se tiene la oportunidad de obtener tarifas muy diversas y económicas, sino que también se pueden reducir a cero los gastos de las llamadas que se realicen, ya que si a quien se quiere llamar también usa VoIP, todas las llamadas internas serán completamente gratuitas.

Durante los últimos años, sucedieron cosas interesantes:

Aparición de redes virtuales en IP

El esquema de conectividad de todos contra todos permite segmentar en módulos a los servicios sobre IP convirtiendo a la voz en una aplicación más de datos.

Paquetización de la voz

El desarrollo de VoIP, ya como un módulo o aplicación más de la red, fue explotado por distintas aplicaciones para su aprovechamiento.

Mejoramiento de esquemas de QoS

Permite que una conversación sea entendible sin importar la distancia de las personas involucradas o el volumen de tráfico de la red.

Desarrollo del concepto de Open Source

Las aplicaciones desarrolladas bajo este concepto integran las funcionalidades tradicionales de un PBX.

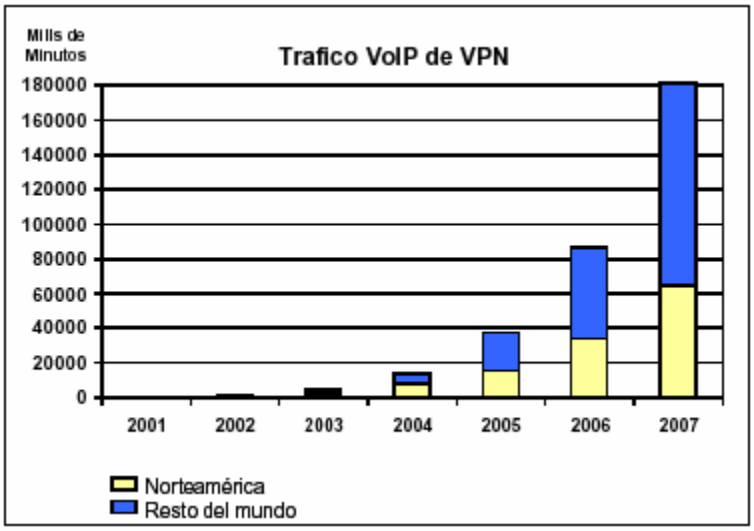


Figura 3.1: Tráfico VoIP de VPN[43]

La demanda por PBX tradicionales de voz ha disminuido durante los últimos años mediante:

- Sustitución de PBX obsoletos
- Habilitación de equipos tradicionales para manejar IP en ellos
- PBX 100% IP

[43] Fuente: Probe Research Inc.: Researching the Big Guys + Global Enterprise Forecast.

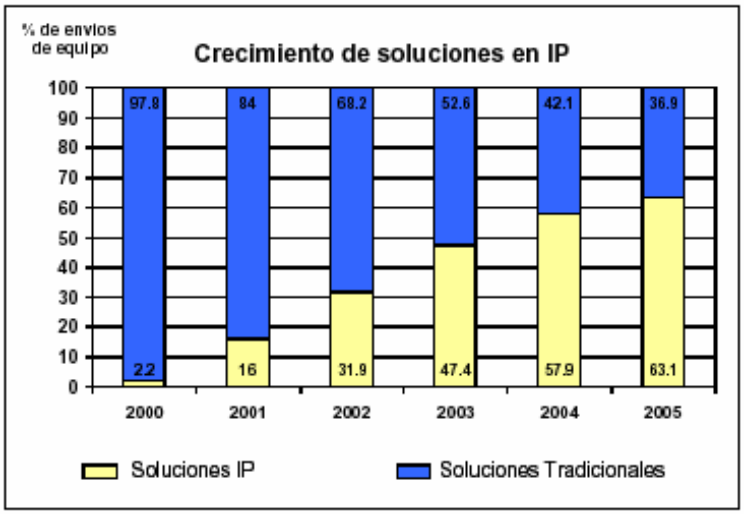


Figura 3.2: Crecimiento de soluciones en IP[44]

Los sucesos descritos durante estos últimos años causaron una disrupción en varios ámbitos de los servicios de telecomunicaciones, por que son innovaciones radicales sobre productos existentes. VoIP sigue siendo voz, pero en paquetes y no sobre circuitos dedicados, sino compartiendo con otras aplicaciones de datos.

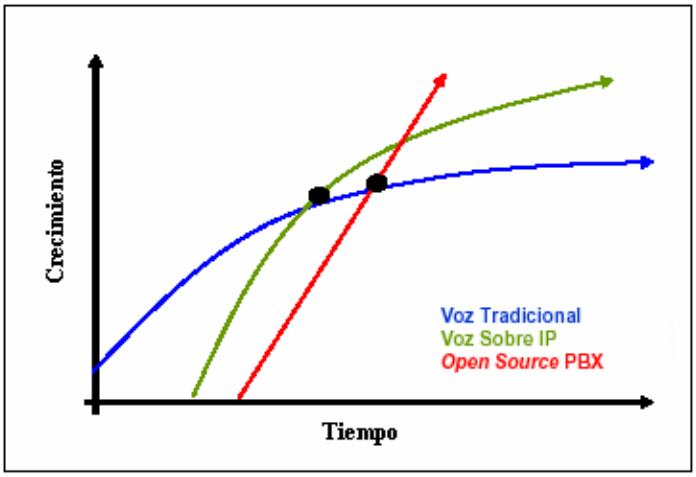


Figura 3.3: Curvas de comparación

Los puntos de disrupción mostrados en la Figura 3.3, dan una idea de la velocidad de la innovación que se dio en este ámbito.

[44] Fuente: The Yankee Group; Frost & Sullivan; Forrester Research: Team Analysts

Cualquier red de IP empresarial (privada) sirve de transporte, así como el Internet.

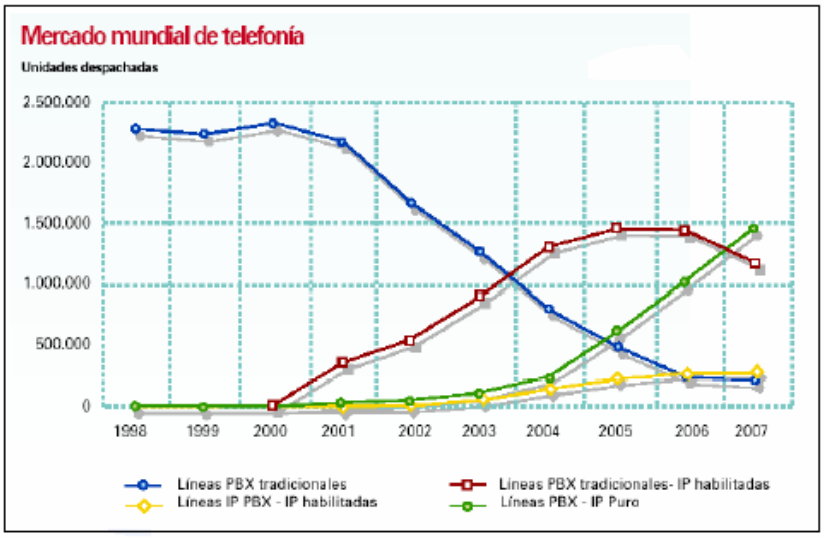


Figura 3.4: Mercado Mundial de Telefonía[45]

En el 2005 hay un punto de inflexión en que las órdenes de IPBX superan a los PBX tradicionales.

VoIP hace más eficiente el manejo de la voz sobre la red, ya que en lugar de manejar un circuito dedicado de 64Kbps por canal de voz (dependiendo de la configuración y del CODEC que se utilice), puede llegar a ocupar 8Kbps por canal:

Las velocidades actuales tanto de LAN como de WAN, hacen que el ancho de banda no sea un impedimento técnico para la implementación de estos servicios. Permite que mediante acceso remoto, el usuario pueda acceder a la red de voz y datos de su oficina.

Facilita la integración de redes, cableado y aplicaciones.

VoIP conlleva algunos retos para su implementación:

[45] Fuente: Gartner Group 2007

- Calidad de los enlaces: Se requiere tener un esquema de QoS que garantice la secuencia para asegurar la entrega de los paquetes en orden ya que en IP no hay garantía de esto.

- Retraso en la red: Debido a la ocupación de la red y la misma característica del tráfico de las aplicaciones del cliente, se pueden originar retrasos en la entrega de paquetes de voz.

- Firewalls y equipo de seguridad: Los esquemas de seguridad usados bloquearán
  el tráfico de voz debido a la naturaleza de esta aplicación, la cual se considera insegura.

- Monitoreo de red: El manejo y administración de la red cambia al introducir voz.

- Seguridad: Una aplicación más sobre la red implica nuevos riesgos.

- Costumbre en el uso de la red telefónica tradicional.

1.2.20 CARACTERÍSTICAS [27]

1.2.20.1 Movilidad

Los números fijos de la red telefónica tradicional están siempre ligados a un sitio geográfico específico. Con VoIP esta limitación desaparece. Ahora se puede desviar las llamadas sin gastos adicionales. Por ejemplo, las llamadas que se reciban desde un número fijo de Madrid pueden ser desviadas a un teléfono VoIP en Japón o cualquier otro lugar del mundo. Los usuarios finales podrán acogerse a las ventajas de servicios VoIP en cualquier lugar siempre que estos tengan acceso a:

- Conexión a Internet propia: Puesto que un teléfono VoIP no siempre tiene que estar instalado en un lugar geográfico específico, a diferencia de una

conexión clásica de teléfono. Las llamadas se reciben en el lugar en que se encuentre el teléfono VoIP.

- Otros accesos de conexión a Internet WIFI[46]/ GPRS[47] / 3G[48] / UMTS[49].

- Configuración del software telefónico para que apunte a la dirección IP pública del servidor.

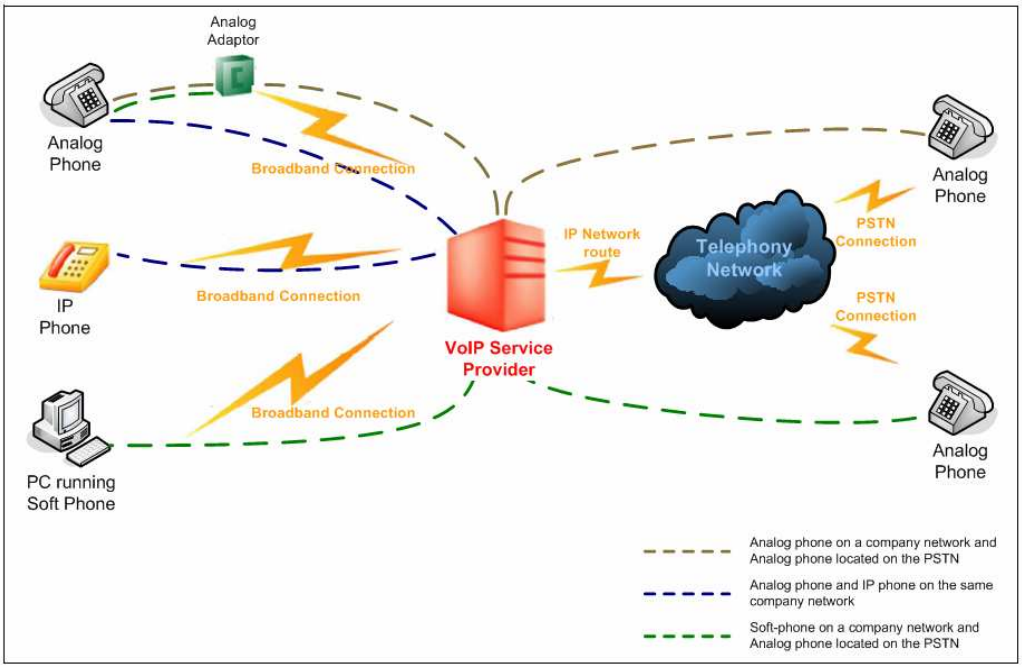


Figura 3.5: Red de Voz sobre IP

[46] WIFI: Es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Creado para ser utilizado en redes locales inalámbricas, es frecuente que en la actualidad también se utilice para acceder a Internet.

[47] GPRS – General Packet Radio Service. Es una tecnología digital de telefonía móvil.

[48] 3G: Es una abreviatura para tercera-generación de telefonía móvil. Los servicios asociados con la tercera generación proporcionan la posibilidad para transferir tanto voz y datos (una llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de correo-e, y mensajería instantánea).

[49] UMTS – Universal Mobile Telecommunications System, es una de las tecnologías usadas por los móviles de tercera generación (3G). Sucesor de GSM, también llamado W-CDMA.

1.2.20.2 Portabilidad

VoIP permite a los usuarios finales la portabilidad; en caso de que:

- Se cambien desde un teléfono tradicional al sistema VoIP.
- Se cambien entre diferentes cuentas VoIP (carriers).
- Se cambien a un uso profesional, para acceder a desvíos y transferencias avanzadas de llamadas VoIP.

VoIP está construido sobre una serie de programas de código fuente libre. Esto significa que a la hora de comprar un producto VoIP no se tendrá problemas de compatibilidad con cualquier fabricante de sistema VoIP. Cuando dos usuarios hablan el uno al otro con VoIP, no importa la marca de fábrica del equipo que utilicen o el tipo de dispositivo. Por ejemplo, un llamador podría utilizar un teléfono IP y el otro un teléfono tradicional con un adaptador de VoIP.

1.2.20.3 Calidad de la Voz

La calidad de las transmisiones de voz a través de redes IP depende de varios factores controlables:

- El CODEC de salida (es el algoritmo que convierte la señal de voz análoga en datos digitales para la transmisión de una llamada, interpretado luego por el aparato receptor).
- End-to-end: Retraso sufrido por la transmisión entre usuarios, y las variaciones de la latencia.
- Control de la calidad del servicio (QoS): Un requisito básico para los sistemas de VoIP.

- Para resolver la demanda de la comunicación por voz en tiempo real, las redes IP deben ofrecer la prioridad al tráfico VoIP, para así asegurar las transmisiones, ya que podrían darse cortes de llamadas, déficit de señal u otros inconvenientes.

1.2.20.4 Disponibilidad y confianza

La red de VoIP dispone de sistemas de energía de reserva para seguir siendo operacional durante un fallo de suministro. A diferencia de la telefonía tradicional, los sistemas de VoIP ofrecen soluciones más flexibles de reserva y redundancia. Tales soluciones son opcionales, pero excluyentes, son las siguientes:

- Configuración de servidores en espera, que almacenarán la copia actual del sistema de telefonía para cuando el servidor principal falle, el sistema puede recuperarse en una cuestión de segundos cambiando a los servidores que mantiene en stand-by.

- Remisión automática de las llamadas entrantes con localización de reserva, en el supuesto, por ejemplo, de un desastre natural.

Desde el punto de vista del empresario, los riesgos de un sistema de VoIP son similares a los de una empresa que ofrezca alojamiento web o cuentas de correos.

Una caída del servidor VoIP puede tener los mismos efectos que la caída de una página web y sus servicios.

1.2.20.5 Seguridad

VoIP no es invulnerable a las amenazas de seguridad en la red. Las amenazas existen y son reales. Sin embargo, los riesgos implicados sobre una infraestructura de VoIP en funcionamiento no superan los de una conexión a Internet. VoIP trata comunicaciones de voz como comunicaciones de datos, por lo tanto, las configuraciones de seguridad básicas que afectan VoIP son las mismas que las que afectan a comunicaciones de datos sobre las redes IP. El primer paso para asegurar las comunicaciones de VoIP es usar los mecanismos de defensa tales como cortafuegos, cifrados, etc.

El potencial ahorro de recursos, al poder reutilizar infraestructura existente para datos (Internet en sí) y transmitir voz sobre ella, ha producido una serie de aplicaciones y productos diseñados para tomar ventaja de esta tecnología, en forma de equipos especializados para actuar como PBX o conmutadores, software para instalarse en servidores de datos, o en aplicaciones tipo "Messenger" para uso personal en PC, etc.

APLICACIONES

Dentro de Voz sobre IP, actualmente existen innumerables aplicaciones, por este motivo a continuación se describen las que tienen mayor relevancia para el objetivo de estudio.

1.2.21 CENTRALITAS PBX [28]

Una central telefónica privada (PBX) es un dispositivo que permite a las empresas conectar sus terminales telefónicos de forma independiente al proveedor de telefonía. De esta forma se consigue que todas las llamadas internas de una misma empresa sean conmutadas directamente sin necesidad de salir al exterior por la red pública de telefonía (PSTN o RDSI), disminuyendo notablemente la factura mensual.

Las primeras PBX, requerían de la contribución de una persona encargada de conectar distintos cables para establecer la comunicación entre distintas terminales de una empresa. Estas centrales eran conocidas como PBMX (Manual PBX). El avance tecnológico rápidamente permitió prescindir de estos operadores para dar paso a un nuevo sistema electromecánico de conmutación totalmente automático llamado PABX (Automatic PBX).

A todos los dispositivos conectados a la PBX se les conoce como extensiones y pueden ser tanto teléfonos, como faxes o módems, aunque estos últimos pueden degradar la calidad de la línea. Además, también es posible conectar a la centralita un determinado número de líneas troncales para poder realizar y recibir llamadas del exterior e incluso conectar varias PBX entre si para realizar llamadas entre las distintas sedes de una compañía. Normalmente para establecer la comunicación con el exterior, la PBX requiere que se marque el número 9 ó 0 seguido del número de destino. De esta forma la centralita es capaz de identificar que se trata de una llamada hacia el exterior y así poder seleccionar la utilización de una de las líneas troncales disponibles.

1.2.21.1 Funcionalidades

Tal y como se ha definido anteriormente, el objetivo principal de una central PBX es establecer y mantener la comunicación entre dos puntos finales durante todo el tiempo requerido por los usuarios.

A continuación se enumeran algunos de los servicios más extendidos en las centralitas telefónicas:

- Operadora Automática / Virtual: permite al llamante transferir la llamada a la extensión deseada mediante menús interactivos sin la intervención física de una operadora. Es un sistema basado en el reconocimiento de voz y/o de tonos DTMF[50], generados al marcar el teclado del teléfono. De esta forma se consigue sustituir la labor efectuada por una persona que solo

[50] DTMF - Dual Tone MultiFrecuency

podrá atender una llamada al tiempo, por un servicio de atención automatizado capaz de atender múltiples llamadas simultáneamente.

- Marcación Rápida a números de servicio público como servicios de emergencia, policía o bomberos.

- Buzón de Voz: servicio de almacenamiento de mensajes de voz (contestador automático). El mensaje de bienvenida puede personalizarse.

- Transferencia de llamada a otra extensión para que sea atendida, por ejemplo, por otro departamento.

- Desvío de llamada a otra terminal en caso de que la extensión no conteste o esté ocupada.

- Follow – me: listado de números a los que redireccionar la llamada en caso de que la extensión no conteste. Los empleados pueden configurar esta lista, por ejemplo, para desviar la llamada a su móvil en caso de no encontrarse en su puesto de trabajo.

- Llamada en espera, parking de llamadas (call park): posibilidad de mantener conversaciones en espera para atender una llamada entrante.

- Música en espera (MOH - Music on Hold): servicio de reproducción de música para rellenar el silencio producido al mantener al llamante en espera.

- Tarifación de llamadas: sistema de cálculo del coste de una llamada.

- CallerID o identificación de llamada.

- DDI (Direct Dialling-In): enrutamiento de llamadas mediante la marcación directa a una extensión desde el exterior.

- Salas de conferencia: conversación entre más de dos terminales.
- Listas Negras: restricción del acceso a determinados números.
- Registro y listado de llamadas entrantes y salientes.
- Envío y recepción automática de faxes.
- Monitorización de llamadas en curso.
- Grabación y escucha de llamadas.
- Integración con bases de datos: posibilidad de almacenar y recuperar información.
- Mensajería SMS: servicio de envío de mensajes cortos.

1.2.21.2 IPBX

La tendencia actual de los fabricantes de PBX es incorporar a sus centralitas la posibilidad de transmitir la voz sobre redes de datos. No es solo la reducción de costes, sino que la integración simplifica y amplia las posibilidades de generar nuevos servicios de valor añadido.

El término IPBX (Intranet PBX) hace referencia a aquellas centralitas capaces de transmitir la voz sobre redes IP basándose en el protocolo VoIP. Para la conexión a la red de Area Local (LAN), hace uso de tarjetas ethernet y al igual que el resto de PBXs, también posee algunas de las interfaces anteriormente definidas para la conexión con otras redes de voz, esto implica la necesidad de complejos mecanismos software que adapten la señal de voz durante la comunicación a cada uno de los diferentes estándares.

1.2.21.2.1 Software IPBX

El uso del software pone en funcionamiento las herramientas básicas de un hardware tradicional PBX así como los servicios digitales de última generación. Básicamente, actúa como una centralita telefónica automática que conecta a usuarios. Además, ofrece nuevos servicios más avanzados que un usuario tradicional de telefonía analógica desearía tener. El sistema IPBX puede ser controlado desde la red usando el panel de control del software. Desde una IP o URL podrá gestionar las características de ejecución, las conexiones y claves de acceso para múltiples usuarios.

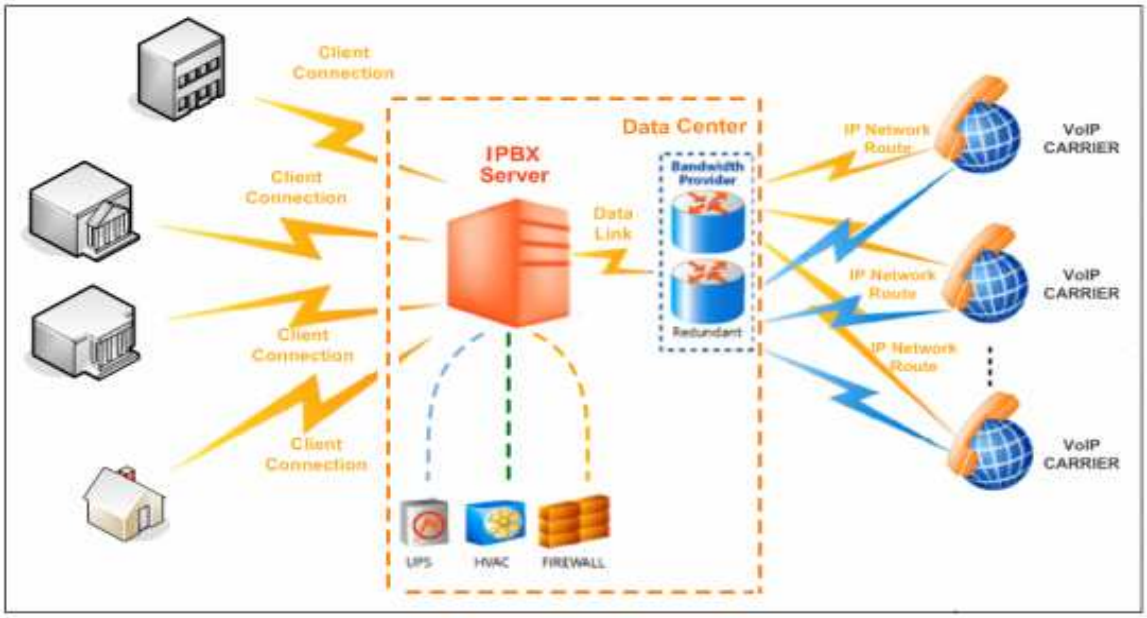


Figura 3.6: IPBX Server

1.2.21.2.2 Componentes y equipamiento

Un sistema de infraestructura básico necesario requiere un servidor con conexión a Internet banda ancha y el alojamiento del software IPBX exclusivamente para la inclusión de uno o más operadores de VoIP (VoIP Carriers), ideal para ofrecer servicios de la telefonía a varias oficinas y empresas múltiples.

- Servidor: Una máquina exclusiva para ejecutar el software IPBX.

- Red IP: Conecta los teléfonos al IPBX y el IPBX a los proveedores VoIP.

- Teléfono tradicional analógico con adaptadores VoIP.

- Teléfono IP.

- Software Telefónico: Aplicaciones de Software para PCs y PDAs.

- Proveedores VoIP. La función de los proveedores de VoIP es la de ofrecer una infraestructura que pueda desviar y conectar las llamadas que origina el sistema con los números de teléfono de otras infraestructuras (IP o PSTN).

1.2.21.3 Aplicaciones para la simulación de una IPBX

1.2.21.3.1 Asterisk [29]

Asterisk, es una aplicación de centralita telefónica PBX bajo licencia GPL (Código Abierto).

Asterisk pese a ser una aplicación software ofrece las mismas características y servicios que los caros sistemas propietarios PBX, Asterisk entre otras cosas ofrece buzón de voz, salas de conferencia o música en espera, entre otros.

Figura 3.7: Sitio Oficial Asterisk [30]

Ventajas

- Reducción de costes, no solo por el hecho de integrar voz y datos bajo una misma infraestructura, sino por el hecho de que Asterisk sea una aplicación de código abierto evitando tener que pagar grandes cantidades por licencias.

- Facilita la integración y desarrollo de nuevos servicios de valor añadido.

- Compatibilidad con un gran número de protocolos VoIP y códecs.

- Es posible conectar Asterisk con otras centralitas, lo que le convierte en una solución flexible para futuros redimensionamientos.

Asterisk está formado por un núcleo principal encargado de gestionar todo el sistema PBX. Sus funciones principales son:

- Interconectar de forma automática cada llamada entre los usuarios participantes, teniendo en cuenta el tipo de protocolo utilizado por cada terminal.

- Lanzar los servicios de valor añadido cuando sean requeridos.

- Traducir y adaptar los códecs a cada terminal involucrado en la comunicación.

- Gestionar el sistema para que funcione de la forma más óptima en cualquier condición de carga.

Asterisk unifica internamente:

PBX Switching: La esencia de Asterisk por supuesto es su sistema de intercambio y switcheo privado, conectando usuarios y realizando tareas automáticas.

Lanzador de Aplicaciones: Ejecuta aplicaciones con servicios específicos para usuarios, como casilla de voz, ejecución de archivos de audio y listado de contactos.

Traductor de CODECS: Usa módulos de Códec, para codificar y decodificar varios formatos de audio comprimidos en la industria de la telefonía. Un cierto

número de Códecs están disponibles para diferentes necesidades, incluida la calidad y el ancho de banda disponible.

Indexador y Gestor de entrada/salida: Ejecuta tareas de bajo nivel y gerenciamiento de sistema para performances óptimas bajo condiciones de carga.

Estado actual

La versión estable de Asterisk está compuesta por los módulos siguientes:

- Asterisk: Ficheros base del proyecto.
- Zaptel: Soporte para hardware. Drivers de tarjetas.
- Addons: Complementos y añadidos del paquete Asterisk. Opcional.
- Libpri: Soporte para conexiones digitales. Opcional.
- Sounds: Aporta sonidos y frases en diferentes idiomas.

Cada módulo cuenta con una versión estable y una versión de desarrollo. La forma de identificar las versiones se realiza mediante la utilización de tres números separados por un punto. Teniendo desde el inicio como primer número el uno, el segundo número indica la versión, mientras que el tercero muestra la revisión liberada. En las revisiones se llevan a cabo correcciones, pero no se incluyen nuevas funcionalidades.

Versiones

Las versiones tanto estables como de desarrollo de cada módulo a fecha de diciembre de 2006 son las siguientes:

Version 1.2 - Estable

- Asterisk Version 1.2.14
- Zaptel Version 1.2.12
- Libpri Version 1.2.4

- Addons Version 1.2.5
- Sounds Version 1.2.1

Version 1.4 – Desarrollo

- Asterisk Version 1.4.0
- Zaptel Version 1.4.0
- Libpri Version 1.4.0
- Addons Version 1.4.0

Nota: Ahora ambas versiones son consideradas estables en producción.

Protocolos

MGCP [31]

MGCP es un protocolo de control de dispositivos, donde un gateway esclavo MG (Media Gateway) es controlado por un maestro MGC (Media Gateway Controller, también llamado Call Agent.).

MGCP, Media Gateway Control Protocol, es un protocolo interno de VoIP cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente - servidor. MGCP está definido informalmente en la RFC 3435.

Está compuesto por:

- Un MGC (Media Gateway Controller).
- Uno o más MG (Media Gateway).
- Uno o más SG (Signaling Gateway).

Un gateway tradicional, cumple con la función de ofrecer conectividad y traducción entre dos redes diferentes e incompatibles como lo son las de Conmutación de Paquetes y las de Conmutación de Circuitos. En esta función, el

gateway realiza la conversión del flujo de datos, y además realiza también la conversión de la señalización, bidireccionalmente. MGCP separa conceptualmente estas funciones en los tres elementos previamente señalados. Así, la conversión del contenido multimedia es realizada por el MG, el control de la señalización del lado IP es realizada por el MGC, y el control de la señalización del lado de la red de Conmutación de Circuitos es realizada por el SG.

MGCP introduce esta división en los roles con la intención de aliviar a la entidad encargada de transformar el audio para ambos lados, de las tareas de señalización, concentrando en el MGC el procesamiento de la señalización.
El control de calidad de servicio QoS se integra en el gateway GW o en el controlador de llamadas MGC. Este protocolo tiene su origen en el SGCP (de Cisco y Bellcore) e IPDC. Bellcore y Level3 plantearon el MGCP a varios organismos.

IAX2 [32]

IAX (Inter-Asterisk eXchange protocol) es uno de los protocolos utilizado por Asterisk, es un servidor PBX (centralita telefónica) de código abierto patrocinado por Digium. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX.

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de códecs y un gran número de streams, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

El diseño de IAX se basó en muchos estándares de transmisión de datos, incluidos SIP (el cual es el más común actualmente), MGCP y RTCP.

El principal objetivo de IAX ha sido minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red IP, con particular atención al control y a las llamadas de voz y proveyendo un soporte nativo para ser transparente a NAT. La estructura básica de IAX se fundamenta en la multiplexación de la señalización y del flujo de datos sobre un simple puerto UDP entre dos sistemas.

IAX es un protocolo binario y está diseñado y organizado de manera que reduce la carga en flujos de datos de voz. El ancho de banda para algunas aplicaciones se sacrifica en favor del ancho de banda para VoIP.

1.2.21.3.2 3CX [33]

El conmutador telefónico 3CX libera a las empresas de los costos de compra y administración asociados con un conmutador PBX propietario.

El conmutador telefónico 3CX está basado en un estándar SIP abierto y como resultado funciona con cualquier pasarela o teléfono basado en SIP. Esto elimina la necesidad de costosas centrales telefónicas propietarias, su instalación especializada y experimentada administración.

Figura 3.8: Teléfono Virtual de 3CX

El conmutador telefónico 3CX para Windows edición gratuita es único, ya que hasta ahora el software gratis de conmutador IP sólo se encontraba disponible para Linux.

3CX para Windows es un conmutador IP que reemplaza completamente un conmutador PBX propietario, soporta teléfonos SIP físicos y virtuales, servicios VoIP y líneas telefónicas tradicionales PSTN, es mucho menos costoso que un conmutador PBX y puede reducir sustancialmente los costos al utilizar un proveedor de servicios VoIP, además elimina la red de cableado telefónico y permite a los usuarios el cambiar de lugar simplemente llevando consigo su teléfono.

Figura 3.9: Página WEB Oficial 3CX [34]

Características

- Sistema telefónico completo: Provee conmutación de llamadas, enrutamiento y colas.
- Escalable: Extensiones y líneas telefónicas ilimitadas. No se requiere módulos de expansión propietarios.
- Configuración basada en Web e indicación de estado: fácil administración del conmutador telefónico.
- Reduce costos de llamadas de larga distancia y entre oficinas.
- Utiliza teléfonos SIP estándar.
- Elimina el cableado telefónico y hace el cambio de oficinas más fácil.

1.2.21.3.3 SIPX

Figura 3.10: Configuración SIPX

SIPX es una aplicación de Código Abierto, del protocolo SIP, basado en el sistema de comunicaciones IPBX. Similar a un PBX tradicional, permite conectar varios teléfonos para hacer llamadas entre si, incluso permite la conexión a otros servicios del teléfono, incluso a la PSTN y los servicios SIP Trunking.

SIPX ECS (Enterprise Communications Server), es usado por empresas que tienen entre 200 y 10000 usuarios. SIPX reemplaza las tradicionales PBX con un software basado en aplicaciones que corren en el hardware de un servidor con Sistema Operativo standard.

Figura 3.11: Pagina WEB Oficial SIPX [35]

SIPX esta disponible en varias distribuciones del Sistema Operativo Linux, incluyendo, Red Hat, Fedora Core, entre otros.

Como la mayoría de IP PBXs (con software libre, o no), SIPX proporciona las características de los PBX tradicionales.

1.2.21.3.4 YATE

YATE (Yet Another Telephony Engine), es la nueva generación en telefonía; voz, videos, datos y mensajes instantáneos pueden ser unificados, aumenta la eficacia de comunicaciones y minimiza el coste de la infraestructura para negocios.

YATE puede ser usado por un servidor de Voz sobre IP a un IVR.

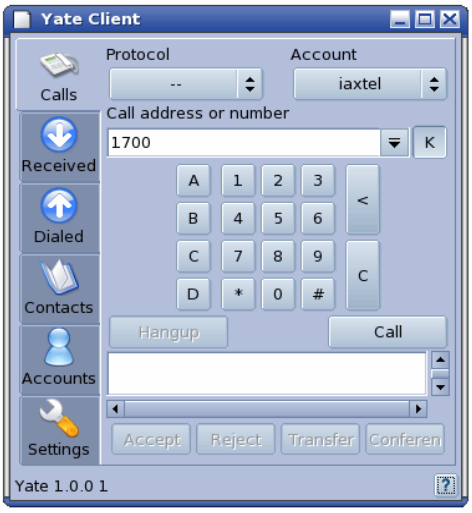


Figura 3.12: Software YATE para LINUX

Figura 3.13: Software YATE para WINDOWS

Está escrito en C++ y está apoyado sobre varios lenguajes de programación e incluso cualquier Sistema Operativo Unix.

La mayor aplicación de YATE es la de conversión SIP-H323, debido a que es el único conversor de Código Abierto estable.

YATE puede usarse como: Servidor VoIP, Cliente VoIP, VoIP – PSTN Gateway, PC2Phone y Phone2PC Gateway, Gatekeeper H.323, H.323 - SIP Proxy, SIP router, Servidor y/o cliente IAX (Inter-Asterisk eXchange protocol), Servidor y/o cliente de Telefonía IP, Servidor Call center, IVR (Interactive Voice Response) y Sistema de tarjetas prepago y postpago.

Comparación entre SIPX, Asterisk y YATE

	SIPX	Asterisk	YATE
Protocolos	SIP	SIP, H323, SCCP, MGCP, IAX	SIP, H323, IAX
Requerimientos de Hardware	P4 a 2.4 GH, 512MB RAM, 80GB DD	PII a 300 MHz 128 MB RAM 4GB DD	PII a 300 MHz 128 MB RAM
Correo de Voz y Operadora Automática	Si	Si	Si
Funcionalidad	Selección de rutas, Desvío, Conferencia, IVR, Tarificador	Selección de rutas, Desvío, Captura, Conferencia, IVR, Texto a voz, Tarificador	Selección de rutas, Desvío, Captura, Conferencia, IVR, Texto a voz, Tarificador
Interfaces PSTN	E1, T1, BRI, FXO	E1, T1, BRI, FXO	E1, T1, BRI, FXO
Escalabilidad	Hasta 4,000 puertos con un P4	Hasta 2,000 puertos con un P4	Hasta 2,000 puertos con un P4

Tabla 3.1: Comparación entre SIPX, Asterisk y YATE

1.2.21.3.5 OpenPBX

OpenPBX es un software de Código Abierto, desarrollado en PERL, contiene todas y más de las características encontradas comúnmente en soluciones comerciales high-end a un precio que esta a un módico alcance.
Las características incluyen la administración remota, la integración con centrales telefónicas, interconexión entre diferentes OpenPBX y un costo más bajo que una solución propietaria.

Beneficios

Correo de Voz por mail, auto-discado, auto-atención de llamadas, voicemail tradicional, música en espera, conferencia, grupos, identificación de llamadas, líneas telefónicas seguras, receptor de alarmas, indexado de mensajes, autenticación, contestador automático, listas negras, reenvío de llamadas si la línea está ocupada o no responde, monitoreo, parking, Caller ID, bloqueo Caller ID, tarjetas de llamada, almacenamiento de base de datos, Direct Inward System Access (DISA), Distributed Universal Number Discovery (DUNDi™), IVR, Macros, Open Settlement Protocol (OSP), Conversión de protocolos, Roaming, Mensajes de Texto (SMS), acceso por streaming, Text-to-Speech y Trunking (Radio).

Como valor agregado, OpenPBX tiene la posibilidad de grabación sobre sus líneas telefónicas y sistema de Mail to Fax / Fax to Mail (Recepción y envío de mails como fax).

OpenPBX es simple, pero diferente de otros productos de telefonía, esencialmente actúa como un middleware, conectando tecnologías de telefonía a bajo nivel y las aplicaciones en la cima, creando un ambiente consistente de gestión de telefonía

Los protocolos incluidos de VoIP son: SIP, H.323, IAX, MGCP (tanto gateways como teléfonos).
Las tecnologías tradicionales incluidas son: TDM, ISDN PRI, POTS analógicos, Servicios PSNT, ISDN BRI (básico).

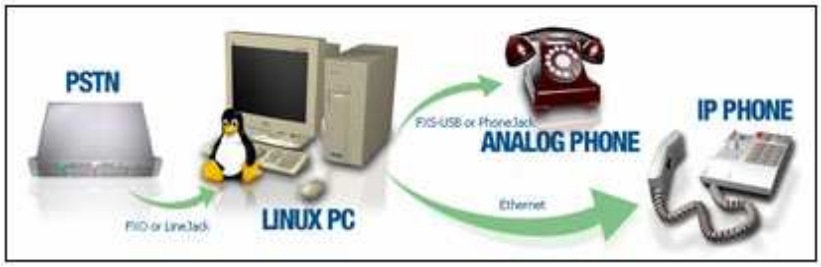


Figura 3.14: Open PBX

Una PBX configurada con Openpbx, bien puede ser de un solo puerto PSNT o de un solo teléfono IP, si bien esto no es muy práctico esto muestra la escalabilidad de la aplicación.

1.2.21.3.6 FreeSWITCH

FreeSWITCH es una plataforma de telefonía de Código Abierto, diseñada para facilitar la transmisión de voz y chat (soft-phone - soft-switch). Puede ser usado como un simple switch, un media gateway o un media server to host, para ser utilizado por aplicaciones IVR mediante XML para el control de la llamada.

Soporta varios protocolos de comunicación como SIP, H.323 e IAX2, lo cual facilita la unión con otros software PBX de Código Abierto como SIPX, OpenPBX, YATE o Asterisk.
Soporta CODECS de banda ancha y angosta, por lo cual representa una solución ideal. Los canales de voz y conferencia pueden operar a 8, 16 o 32 KHz. FreeSWITCH corre en varios sistemas operativos, entre ellos Windows, Max OS X, Linux, BSD y Solaris.

El código de FreeSWITCH a contribuido en la elaboración de sistemas como SipX, Asterisk y OpenPBX.

1.2.22 OTRAS APLICACIONES DE VOZ SOBRE IP

1.2.22.1 Skype [36]

Skype es una red de telefonía entre pares por Internet, fundada en 2003 por los creadores de Kazaa. El código y protocolo de Skype permanecen cerrados y propietarios, pero los usuarios interesados pueden descargar gratuitamente la aplicación del sitio oficial. Los usuarios de Skype pueden hablar entre ellos gratuitamente.

Dentro de los servicios más importantes que Skype ofrece, está SkypeOut que permite a los usuarios llamar a teléfonos convencionales, cobrándoseles diversas tarifas según el país de destino: $ 0,017 por minuto en muchos de ellos, incluyendo en algunos los teléfonos móviles, subiendo en otros hasta $ 0,55. Las tarifas para llamar a Ecuador están entre $ 0.15 y $ 0.24. (Ver Figura 3.15).

Figura 3.15: Servicio SkypeOut [37]

Otra opción que brinda Skype es SkypeIn, gracias al cual se otorga un número de teléfono para que desde un aparato telefónico en cualquier parte del mundo la gente pueda ser contactada. El costo para acceder al servicio es de $ 18 por tres meses, y $ 60 por 12 meses. (Ver Figura 3.16).

Figura 3.16: Servicio Skypeln [38]

Skype provee además un servicio de buzón de voz gratuito. La interfaz de Skype es muy parecida a otros software de mensajería instantánea tales como MSN Messenger o Yahoo! Messenger, y de igual forma que en éstos es posible entablar una conversación de mensajes instantáneos con los usuarios del mismo software.

1.2.22.1.1 Protocolo

Skype utiliza un protocolo propietario. Su éxito reside en la gran compresión de éste sin afectar prácticamente a la calidad de la transmisión de voz. Uno de los problemas que tienen los protocolos de VoIP como SIP y H.323, es que suelen usar conexiones peer-to-peer mediante UDP[51], lo cual da muchos problemas a la hora de realizar NAT[52]. Aunque hoy en día existe una solución llamada STUN[53], varios clientes de VoIP como Jabber Google Talk y SIP OpenWengo funcionan

[51] UDP - User Datagram Protocol
[52] NAT - Network Address Translation
[53] STUN - Simple Traversal of UDP (User Datagram Protocol) through NATs

bien con los NAT. El programa ha sido desarrollado en Pascal, usando Delphi y más tarde ha sido adecuado para Linux.

Su funcionamiento básicamente consiste en establecer una conexión con un clúster de servidores (servidores redundantes) de Skype para iniciar sesión, una vez iniciada la sesión se devuelve la lista de contactos y cuando se inicia una llamada se establece una conexión directa con el usuario, de esta manera se elimina el consumo de ancho de banda utilizado por la voz en los servidores de Skype y así se incrementa la seguridad al ser una conexión directa.

1.2.22.1.2 Seguridad

Skype utiliza el algoritmo AES a 256-bit para cifrar la voz, la transferencia de archivos o un mensaje instantáneo. Para la versión pagada se utiliza el algoritmo RSA a 2048-bit para el acceso a voicemail y 1536-bit para la negociación a la hora de establecer la conexión.

Ya que el código de Skype es propietario, además de ser un código cerrado, la seguridad del programa no puede ser firmemente establecida por expertos independientes; es por eso que sus usuarios, expertos e inexpertos por igual deben basar el uso del producto confiando meramente en el fabricante o en el comportamiento del programa descargándolo de fuentes autorizadas por el fabricante.

1.2.22.2 Ekiga

Ekiga (GnomeMeeting) es una aplicación de software libre y código abierto (Licencia GPL), usado específicamente para video conferencia y telefonía por IP para GNOME y WINDOWS. Soporta protocolos SIP y H.323 y es interoperable con Microsoft NetMeeting. Esta soportado por muchos CODECS de audio y video.

Permite todas las características modernas de una videoconferencia como soporte de proveedor inteligente o llamadas de telefonía desde el ordenador a un teléfono.

Figura 3.17: Ekiga

1.2.22.3 WengoPhone

WengoPhone es también un software libre y de código abierto (Licencia GPL), mediante el cual, gran cantidad de usuarios tienen la posibilidad de comunicarse con otros usuarios de VoIP sin costo. Entre sus funciones están, envío de SMS y video llamadas.

1.2.23 SOFTPHONES MÁS UTILIZADOS

Para realizar la conexión con los Software VoIP detallados anteriormente y poner en contacto a todos los usuarios que se conectan a el, existe una gran cantidad de softphones, teléfonos reales que se conectan a la red de datos en lugar de la red de telefonía.

A continuación se describen los más importantes:

1.2.23.1 X –Lite

X – Lite (Windows / Linux / MAC / PocketPC), es un software creado inicialmente bajo Windows, es el más utilizado en todo el mundo gracias a su precio, su vistosidad y al gran número de plataformas soportadas además de su soporte de Video Conferencia; es el softphone más competitivo.

Figura 3.18: X - Lite

1.2.23.2 SJPhone

SJPhone (Windows / Linux / Mac / PocketPC) es un softphone de Código Abierto, que permite hablar con cualquier otro softphone instalado en un PC o PDA, cualquier teléfono IP, o con teléfonos tradicionales o móviles; soporta SIP y H.323 y es completamente compatible con la mayoría de proveedores de Voz sobre IP, su diseño es menos atractivo que X-Lite pero igual de robusto y funcional.

Figura 3.19: SJPhone

1.2.23.3 Ekiga

Ekiga (comunmente conocido como GnomeMeeting), es una aplicación de Código Abierto de Voz sobre IP y video conferencia para GNOME. Ekiga utiliza tanto protocolo H.323 como SIP. Soporta una gran variedad de CODECS de audio y video, y es capáz de interoperar con otros software compatibles con SIP, como Asterisk y Microsoft NetMeeting.

Figura 3.20: Ekiga

1.2.23.4 PPCIAX (PocketPC)

El único softphone para PocketPC que soporta el protocolo IAX (Inter-Asterisk eXchange Protocol), tiene muy buena presentación en cuanto a diseño y funciona bastante bien.

Figura 3.21: PPCIAX (PocketPC)

1.2.24 EQUIPOS UTILIZADOS PARA EL TRANSPORTE DE VOZ

1.2.24.1 Teléfono IP

Equipos que permiten comunicarse por medio de un computador a través de Internet. Se conecta directamente a la red de datos. Estos teléfonos tienen un mini-concentrador integrado para que puedan compartir la conexión de red con el ordenador.

Figura 3.22: Teléfono IP

Figura 3.23: Teléfonos VoIP con USB

Figura 3.24: Teléfonos VoIP con tecnología DECT

1.2.24.2 Adaptador IP

Si se desea usar un teléfono convencional con el sistema telefónico VoIP, se puede hacer uso de un adaptador IP. Un adaptador IP permite enchufar el puerto de red Ethernet en el adaptador y luego enchufar el teléfono en el adaptador.

De esa forma, un teléfono antiguo aparecerá en el software del sistema telefónico VoIP como un teléfono SIP normal.

Figura 3.25: Adaptador ATA

Figura 3.26: Teléfono con tecnología de fijo, VoIP y DECT combinado

1.2.24.3 Hubs Telefónicos

Concentradores de redes telefónicas.

Figura 3.27: Hub Telefónico

1.2.24.4 Pasarela VOIP

Una pasarela VoIP es un dispositivo que convierte el tráfico de telefonía en paquetes IP, para luego ser transmitido por una red de datos. Se usan de 2 formas:

- Para convertir líneas telefónicas PSTN entrantes en VoIP. De esta forma, la pasarela VoIP permite recibir y realizar llamadas en la red telefónica tradicional.

- Para conectar una centralita tradicional con la red IP.

La pasarela VoIP permite realizar llamadas a través de redes de datos, luego, las llamadas se podrán realizar a través de un proveedor de servicios VoIP y en el caso de una empresa con oficinas múltiples, se puede reducir el costo de las llamadas entre oficinas mediante el enrutamiento de las llamadas a través de Internet. Las pasarelas VoIP se encuentran disponibles como unidades externas o como tarjetas PCI; la gran mayoría de los dispositivos son unidades externas. Una pasarela VoIP tendrá un conector para la red IP y uno o más puertos para conectar las líneas telefónicas a ella.

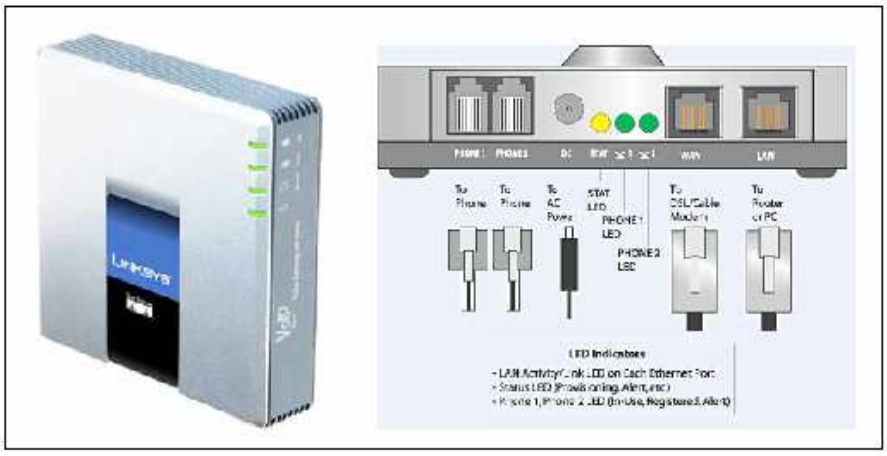


Figura 3.28: Pasarela VoIP Analógica

MARCO LEGAL APLICABLE

El marco legal que rige la prestación de servicios usando la tecnología de Voz sobre IP en el Ecuador, está dado por los reglamentos mencionados a continuación:

- Según el Articulo 3, literales a) y d) y el Articulo 4, 5 y 6 de la RESOLUCIÓN 073-02-CONATEL-2005[54], dada en Quito, 25 de Enero del 2005.

*"**ARTICULO 3.** La Voz sobre Internet podrá ser ofrecida por los Centros de Información y Acceso a la Red de Internet o "Ciber Cafés" de acuerdo a las siguientes condiciones:*

a) La Voz sobre Internet podrá ofrecerse exclusivamente para tráfico internacional saliente, prohibiéndose su utilización para la realización de llamadas locales, regionales, llamadas de larga distancia nacional, llamadas a servicios celulares o llamadas al servicio móvil avanzado.

[54] Ver ANEXO F

d) Los "Centros de Información y acceso a la red de Internet" o "Ciber Cafés" que ofrezcan Voz sobre Internet, de conformidad con lo señalado en el literal a) del presente artículo requerirán únicamente de un certificado de registro, de conformidad con el artículo 7 de la presente resolución. "

"***ARTICULO 4.*** *Se prohíbe a los "Centros de información y acceso a la red de Internet" o "Ciber Cafés" el uso de dispositivos de conmutación, tales como Gateways o similares que permitan conectar las llamadas sobre Internet a la red telefónica pública conmutada, a las redes de telefonía móvil celular o del servicio móvil avanzado y de esta manera permitan la terminación de llamadas en dichas redes. "*

"***ARTICULO 5.*** *Quedan excluidos de la presente regulación los establecimientos que deseen ofrecer Voz sobre Internet y que no cumplan con las condiciones establecidas en los Artículos 3 y 4 de la presente Resolución, independientemente de la facilidad tecnológica que utilicen; dichos establecimientos deberán sujetarse a lo que se establece en el "Reglamento del servicio de telefonía pública."*

"***ARTICULO 6.*** *Quedan excluidos de la presente regulación los locutorios, cabinas y otros establecimientos que ofrezcan el servicio de transmisión de voz, ya sea por medio de conmutación de paquetes o utilizando conmutación de circuitos. Estos establecimientos deberán sujetarse a lo que se establece en el "Reglamento del servicio de telefonía pública, o a la reventa de servicios."*

- Según el Artículo 1, 2, 3, 4, 5 y 6 de la RESOLUCIÓN 491-21-CONATEL-2006[55], dada en Quito, 8 de Septiembre de 2006:

"***ARTICULO 1.*** *La Voz sobre Internet, cursada a través de la red Internet, permite a sus usuarios comunicarse entre si o entre un usuario conectado a la red Internet con un usuario conectado a una Red Pública de Telecomunicaciones. La Voz*

[55] Ver ANEXO G

sobre Internet es reconocida como una aplicación tecnológica disponible en Internet. El video, los datos y multimedios cursados a través de la red Internet, son igualmente reconocidos como aplicaciones tecnológicas disponibles en Internet."

*"**ARTICULO 2.** Cuando un operador de telecomunicaciones preste el servicio de telefonía utilizando Protocolo IP, el operador está sujeto al marco legal, las normas de regulación y control aplicables."*

*"**ARTICULO 3.** Los proveedores de Servicio de Valor Agregado de Internet no restringirán a sus usuarios el acceso a las aplicaciones detalladas en el Articulo 1 de la presente Resolución, incluido su uso, sin perjuicio de origen, marca o proveedor de tales aplicaciones."*

*"**ARTICULO 4.** Cualquier persona natural o jurídica, incluyendo a los proveedores de Servicio de Valor Agregado de Internet dentro de los servicios que prestan a sus usuarios, podrán comercializar dispositivos y planes para el uso de las aplicaciones detalladas en el Artículo 1 de la presente Resolución."*

*"**ARTICULO 5.** Ninguna persona natural o jurídica, incluyendo a los Proveedores de Servicio de Valor Agregado de Internet, podrán usar, dentro del territorio nacional, dispositivos de conmutación, tales como interfaces o compuertas (gateways) o similares, que permitan conectar las comunicaciones de Voz sobre Internet o las llamadas sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador.*

Se exceptúan de ésta limitación a los operadores de telecomunicaciones debidamente autorizados."

*"**ARTICULO 6.** El CONATEL, a través de la SENATEL, no concederá recurso de numeración telefónica, de conformidad al Plan Técnico Fundamental de Numeración, para las aplicaciones detalladas en el Artículo 1 de la presente Resolución."*

Estudio:

El objetivo de realizar un estudio de la reglamentación para Voz sobre IP en el Ecuador, es el verificar si las aplicaciones mencionadas en el presente capítulo pueden prestarse legalmente en nuestro país.

Según lo descrito en los artículos señalados, en el Ecuador se prohíbe la conexión o terminación de las llamadas sobre Internet en la red telefónica pública conmutada o en las redes de telefonía móvil, además se manifiesta que podrá ser utilizada exclusivamente para tráfico internacional saliente, impidiéndose su utilización para la realización de llamadas con terminación dentro del territorio nacional, así como el no uso de dispositivos de conmutación (gateways) o similares, que permitan conectar las comunicaciones de Voz sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador, exceptuándose de lo mencionado los operadores que cuenten con la debida autorización.

Para el caso en estudio, vamos a tomar como ejemplo al servicio Skype Out (generado en el exterior hacia un teléfono IP con numeración en nuestro país).

Esta aplicación en el Ecuador no es posible, debido a que no está dentro de la regulación un plan de numeración para Voz sobre IP, el cual se establecería dentro de un marco regulatorio que haría posible la conexión legal entre las llamadas VoIP y la red telefónica pública conmutada o las redes de telefonía móvil en nuestro país (Ver Figura 3.29).

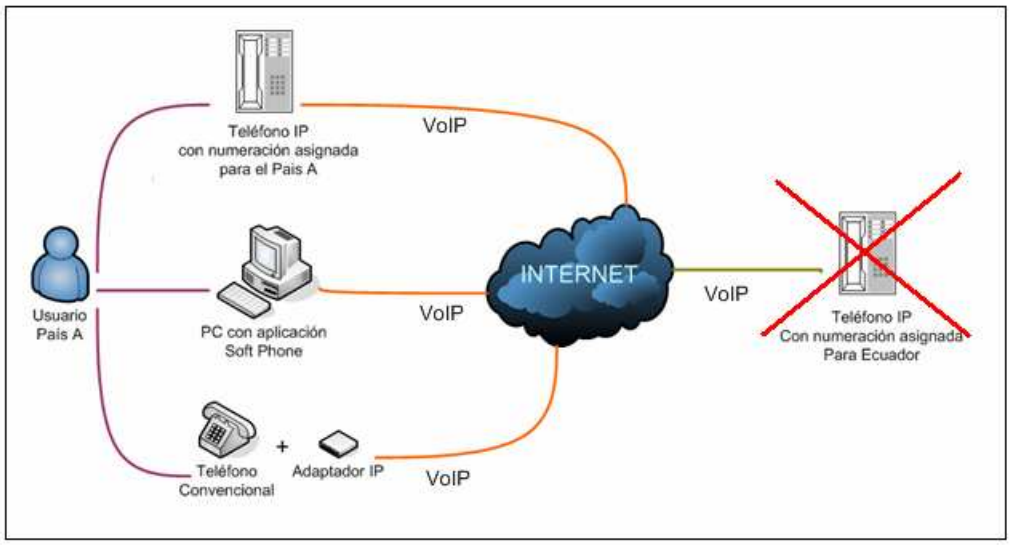


Figura 3.29: Proceso de llamada Skype a un teléfono IP (con numeración) en Ecuador.

Cabe mencionar que podría llevarse a cabo el servicio mencionado, en caso de que la llamada fuera generada hacia un teléfono perteneciente a las operadoras autorizadas, en el cual, el tráfico no sería IP durante toda la comunicación, ya que al llegar a la operadora que serviría como Central de Tránsito para enrutar la llamada hacia su destino final, la información podría que ser desempaquetada, en caso de que la operadora trabaje con conmutación de circuitos.

Si la comunicación fuera realizada de este modo, la tarifa cobrada por Skype sería más alta, ya que se deben cubrir los costos de terminación de la misma, a la operadora legalmente establecida, como es el caso de nuestro país. (Ver Figura 3.30).

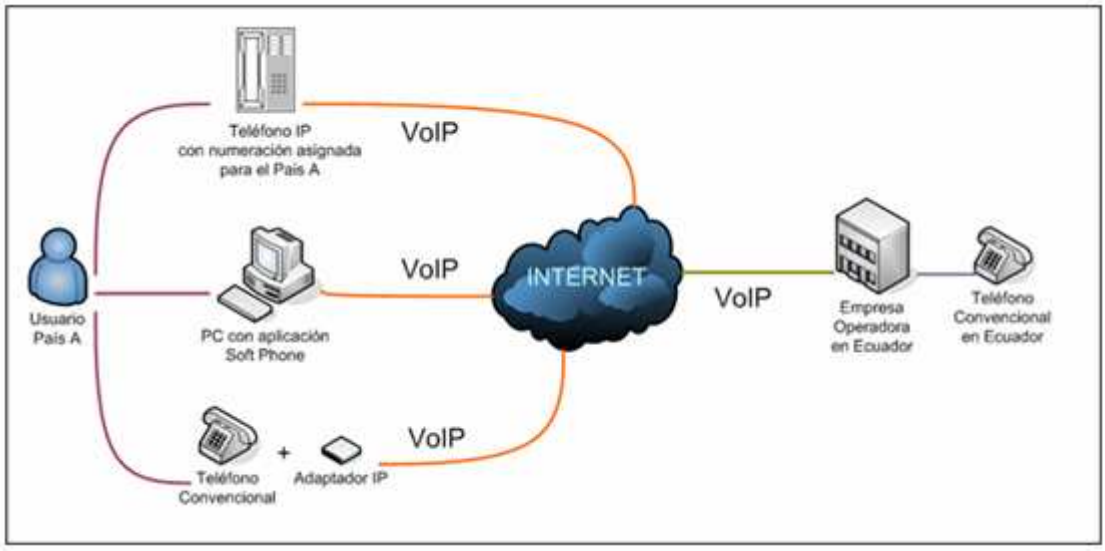


Figura 3.30: Proceso de llamada Skype a un teléfono convencional usando la infraestructura de una Operadora Legalmente establecida en Ecuador para terminar la llamada.

En caso de que la comunicación sea en sentido contrario, es decir, usar Skype Out generando una llamada desde el Ecuador, mediante un Soft Phone por ejemplo, hacia un terminal IP en el exterior, es posible, debido a que algunos países cuentan con un plan de numeración para Voz sobre IP, en caso de no ser así se llevaría a cabo mediante el proceso mencionado en el párrafo anterior.

Existe otro servicio ofrecido por Skype, llamado SkypeIn, gracias al cual se otorga numeración (de Skype), al Terminal IP utilizado. Existen muchas discrepancias con respecto a este tema, pero, no existe ninguna regulación que lo impida directamemte por tratarse de un Servicio de Valor Agregado (Ver Figura 3.31).

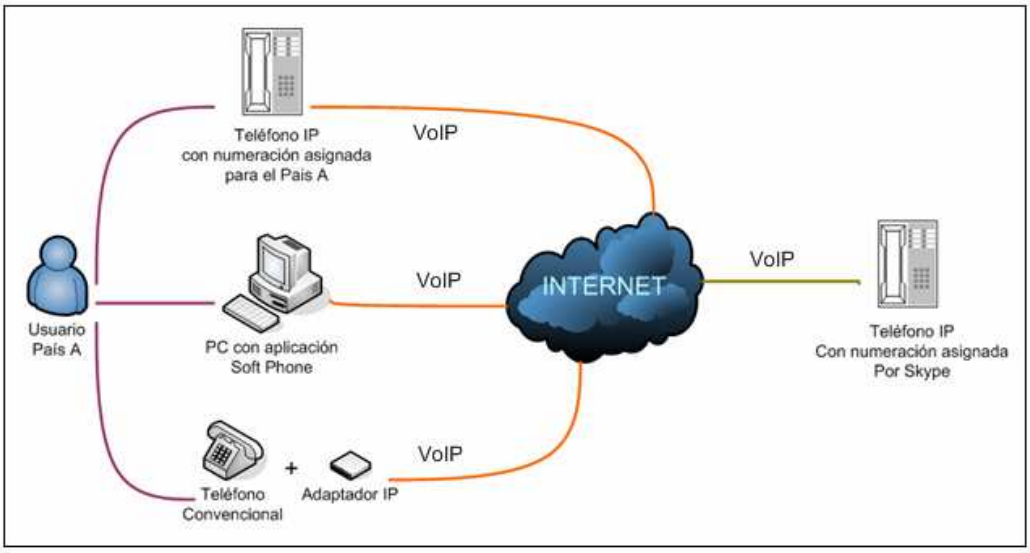


Figura 3.31 Proceso de llamada Skype a un teléfono IP (con numeración proporcionada por Skype), en Ecuador.

Según las resoluciones mencionadas, los proveedores de Servicio de Valor Agregado de Internet, podrán ofrecer y comercializar a sus usuarios aplicaciones de Voz sobre IP, siempre y cuando se siga tratando como un “Servicio de Valor Agregado”, dentro de este aspecto entra el uso de Soft Phones o las centralitas IP o IPBX, las cuales pueden ser empleadas libremente por los usuarios o compañías que así lo requieran, haciendo uso de la misma sin sobrepasar lo estipulado en el marco regulatorio.

CAPITULO IV

ASPECTOS REGULATORIOS

INTRODUCCIÓN

Es indudable que el proceso de convergencia entre las telecomunicaciones y la informática, ha dejado de ser una visión futurista para instalarse como una realidad que impone desafíos a todo nivel en el ordenamiento sectorial.

A nivel internacional, el debate respecto de la Voz sobre IP está puesto en primera línea. La ecuación a resolver es, cómo hacer posible la introducción de esta tecnología en el ambiente público, resguardando los incentivos al desarrollo de redes, generando beneficios a los consumidores y sin causar inestabilidades en el ambiente regulatorio que produzcan distorsiones.

La regulación de la llamada Telefonía IP es un tema de discusión en el mundo entero; en los últimos tiempos las autoridades reguladoras de diversos países han presentado consultas públicas para proponer distintas formas de enfrentar la regulación de la Telefonía IP, con el objetivo de definir un instrumento normativo que permita la introducción de esta tecnología sin causar inestabilidades regulatorias, de manera que los usuarios finales puedan disponer de más y mejores servicios.

El protocolo IP se está aplicando en la actualidad en redes de transporte, redes de datos, redes inalámbricas, entre otras. En el futuro se perfila como el protocolo base en el núcleo de las redes celulares (3G) y en las redes inalámbricas de acceso (WLAN y WMAN); además de lo anterior, se espera también que la cuarta generación móvil (4G) sea aquella que integre las redes móviles celulares

con las redes locales inalámbricas, donde el protocolo IP será fundamental para su desarrollo.

Este contexto exige un marco regulatorio que permita satisfacer las necesidades que se generarán en los usuarios, con las mínimas barreras posibles.

Por lo anterior, el tipo de regulación que se defina para proveer servicios IP, entre otros aspectos deberá considerar los derechos y obligaciones que las concesionarias tendrán, tanto desde el punto de vista de los tipos de servicios que proveerán, como de la calidad de los mismos, o de las relaciones entre concesionarias o permisionarias, entre otros aspectos.

En éste capítulo se llevará a cabo un estudio de la normativa en nuestro país para la prestación de servicios y control del fraude con la tecnología de Voz sobre IP, así como de las posibles alternativas o escenarios regulatorios que en el futuro con una nueva normativa podrían presentarse.

REGULACIÓN PARA VOZ SOBRE IP EN EL ECUADOR

Una persona natural o jurídica, para prestar el servicio de acceso a la red de Internet, debe contar con el respectivo título habilitante, que para este caso, corresponde a un "Permiso de explotación de Servicios de Valor Agregado", el cual es otorgado por la SENATEL[56], permiso en el cual consta que no se autoriza cursar voz.

La ley en nuestro país regula servicios no tecnología, razón por la cual, para cursar voz, es necesario contar con el respectivo título habilitante que para ese caso, constituye una "Concesión para prestar servicios de telefonía", ya sea local, regional, nacional, o internacional. El Concesionario legalmente autorizado, para prestar sus servicios puede utilizar la tecnología que más le convenga, entre ellas la denominada Voz sobre IP (VoIP), lógicamente todas esas condiciones tecnológicas constan en el correspondiente contrato de concesión suscrito con la SENATEL.

Para un mejor entendimiento de la regulación para Voz sobre IP en nuestro país, se llevará a cabo un estudio de los reglamentos que rigen la legal prestación de los servicios usando la tecnología mencionada.

Los principales elementos que definen la regulación para la prestación de servicios y, el control de fraude con Voz sobre IP en nuestro país, son los siguientes:

- Resolución 073-02-CONATEL-2005 – Regulación de los Centros de Acceso a Internet y Ciber Cafés;

- Resolución 491-21-CONATEL-2006 – Regulación para Voz sobre IP;

- Reglamento del Servicio Telefónico de Larga Distancia Internacional; y,

[56] SENATEL – Secretaría Nacional de Telecomunicaciones

- Artículo 422 del Código Penal

Para efectos de estudio, se extraerán los literales más relevantes de cada resolución:

1.2.25 RESOLUCIÓN 073-02-CONATEL-2005 – REGULACIÓN DE LOS CENTROS DE ACCESO A INTERNET Y CIBER CAFÉS[57]

Según:

" ARTÍCULO 3. *La Voz sobre Internet podrá ser ofrecida por los Centros de Información y Acceso a la Red de Internet o "Ciber Cafés" de acuerdo a las siguientes condiciones:*

a) *La Voz sobre Internet podrá ofrecerse exclusivamente para tráfico internacional saliente, prohibiéndose su utilización para la realización de llamadas locales, regionales, llamadas de larga distancia nacional, llamadas a servicios celulares o llamadas a servicio móvil avanzado.* [Lo subrayado me pertenece].

b) *(Derogado por la Resolución 491-21-CONATEL-2006 – Regulación para Voz sobre IP)*

c) *(Derogado por la Resolución 491-21-CONATEL-2006 – Regulación para Voz sobre IP)*

d) *Los "Centros de información y acceso a la red de Internet" o "Ciber Cafés" que ofrezcan Voz sobre Internet, de conformidad con lo señalado en el literal a) del presente artículo requerirán únicamente de un certificado de registro, de conformidad con el artículo 7 de la presente Resolución.*

[57] Ver ANEXO F

e) *Los "Centros de información y acceso a la red de Internet" o "Ciber Cafés" deberán presentar semestralmente a la Secretaría Nacional de Telecomunicaciones reportes relacionados con las aplicaciones prestadas por los Ciber Cafés en los formatos a publicarse en la página web del CONATEL.*

f) *Los "Centros de información y acceso a la red de Internet" o "Ciber Cafés" deberán presentar semestralmente a la Secretaría Nacional de Telecomunicaciones y a la Superintendencia de Telecomunicaciones, reportes relativos al tráfico de voz que cursan por Internet en los formatos a publicarse en la página web del CONATEL.*

ARTÍCULO 4. *Se prohíbe a los "Centros de información y acceso a la red de Internet" o "Ciber Cafés" el uso de dispositivos de conmutación, tales como Gateways o similares que permitan conectar las llamadas sobre Internet a la red telefónica pública conmutada, a las redes de telefonía móvil celular o del servicio móvil avanzado y de esta manera permitan la terminación de llamadas en dichas redes. "* [Lo subrayado me pertenece].

1.2.26 RESOLUCIÓN 491-21-CONATEL-2006 – REGULACIÓN PARA VOZ SOBRE IP[58]

Según:

" ARTÍCULO UNO. *La Voz sobre Internet, cursada a través de la red Internet, permite a sus usuarios comunicarse entre sí o entre un usuario conectado a la red Internet con un usuario conectado a una Red Pública de Telecomunicaciones. La Voz sobre Internet es reconocida como una aplicación tecnológica disponible en Internet. El video, los datos y multimedios cursados a través de la red Internet,*

[58] Ver ANEXO G

son igualmente reconocidos como aplicaciones tecnológicas disponibles en Internet.

ARTÍCULO DOS. *Cuando un operador de telecomunicaciones preste el servicio de telefonía utilizando Protocolo IP, el operador está sujeto al marco legal, las normas de regulación y control aplicables.*

ARTÍCULO TRES. *Los proveedores de Servicio de Valor Agregado de Internet no restringirán a sus usuarios el acceso a las aplicaciones detalladas en el Artículo 1 de la presente Resolución, incluido su uso, sin perjuicio de origen, marca o proveedor de tales aplicaciones.* [Lo subrayado me pertenece].

ARTICULO CUATRO. *Cualquier persona natural o jurídica, incluyendo a los proveedores de Servicio de Valor Agregado de Internet dentro de los servicios que prestan a sus usuarios, podrán comercializar dispositivos y planes para el uso de las aplicaciones detalladas en el Artículo 1 de la presente Resolución.* [Lo subrayado me pertenece].

ARTICULO CINCO. *Ninguna persona natural o jurídica, incluyendo a los Proveedores de Servicio de Valor Agregado de Internet, podrán usar, dentro del territorio nacional, dispositivos de conmutación, tales como interfaces o compuertas (gateways) o similares, que permitan conectar las comunicaciones de Voz sobre Internet o las llamadas sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador.* [Lo subrayado me pertenece].
Se exceptúan de esta limitación a los operadores de telecomunicaciones debidamente autorizados.

ARTICULO SEIS. *El CONATEL, a través de la SENATEL, no concederá recurso de numeración telefónica, de conformidad al Plan Técnico Fundamental de Numeración, para las aplicaciones detalladas en el Artículo 1 de la presente Resolución. "* [Lo subrayado me pertenece].

1.2.27 REGLAMENTO DEL SERVICIO TELEFÓNICO DE LARGA DISTANCIA INTERNACIONAL[59]

Según:

" LIBRO I

TITULO IV

DE LA INSTALACIÓN Y OPERACIÓN DE LOS CENTROS INTERNACIONALES

ARTÍCULO 6. *El CSFTF[60] o CSM[61] que explote el Servicio de Larga Distancia Internacional (STLDI) está obligado a registrar su infraestructura de conmutación y transmisión que utilizará para este servicio. La información para el registro será como mínimo la siguiente:*

A) Dirección y coordenadas geográficas para la ubicación del nodo o nodos a cursar tráfico internacional;

B) Detalle de la infraestructura para la transmisión y recepción de tráfico internacional;

C) Nombre del nodo o nodos de conmutación que va a operar como nodo Internacional;

D) Marca, modelo, modo de operación (TDM, VoIP, entre otros) del nodo o nodos de conmutación;

E) Diagrama esquemático y topología de la red que incluyan los enlaces hacia otras redes nacionales o internacionales; y,

---

[59] Ver ANEXO E
[60] CSFTF - Concesionario del Servicio Final de Telefonía Fija
[61] CSM - Concesionario del Servicio Móvil

F) La central de conmutación que opere como centro internacional deberá contar con sistemas necesarios para llevar en forma diaria el registro de por lo menos la siguiente información sobre tráfico telefónico internacional:

1. *Número de comunicaciones entrantes recibidas a otros CSFTF o CSM desglosadas por cada uno de estos.*

2. *Número de comunicaciones entrantes completadas.*

3. *Número de comunicaciones salientes cursadas;*

4. *Duración de cada comunicación completada tanto entrante como saliente;*

5. *Fecha, hora, minuto, segundo de inicio y fin de cada comunicación completada de tráfico internacional, tanto entrante como saliente;*

6. *País y número de destino de cada comunicación;*

7. *Operadores nacionales e internacionales involucrados en cada comunicación;*

8. *Identificación de tipo de tráfico telefónico internacional de cada llamada.*

9. *El volumen de tráfico internacional entrante y saliente expresado en minutos y segundos.*

El registro de la infraestructura deberá ser realizado por la Secretaría Nacional de Telecomunicaciones, con (30) días de anticipación a la puesta en operación.

TÍTULO VI
DE LOS DERECHOS Y OBLIGACIONES

CAPÍTULO I
OBLIGACIONES DE LOS CONCESIONARIOS

"ARTÍCULO 13. *Se prohíbe expresamente el reoriginamiento o enmascaramiento del tráfico internacional entrante o saliente con los operadores extranjeros o entre operadores nacionales con los cuales se mantengan relaciones de interconexión.* [Lo subrayado me pertenece].

ARTÍCULO 15. *Para efectos de control, el CSFTF o CSM que explote el servicio telefónico de larga distancia internacional adoptará las previsiones de registro necesarias, que permita a la Superintendencia de Telecomunicaciones supervisar el cumplimiento de sus obligaciones. Dichos registros corresponderán a la tasación y facturación de las comunicaciones, el tráfico, los reclamos de los usuarios, el bloqueo y desbloqueo del acceso al STLDI, la suspensión y reconexión del servicio telefónico, entre otros.*

Para efectos de supervisión y control por parte de la Superintendencia, el CSFTF o CSM que explote el servicio telefónico de larga distancia internacional garantizará, por un período de (12) meses a partir de su generación, la custodia de los registros fuente de la información relacionado con la prestación del servicio. " [Lo subrayado me pertenece].

1.2.28 ARTÍCULO 422 DEL CÓDIGO PENAL[62]

"Quienes ofrezcan, presten o comercialicen servicios de telecomunicaciones, sin estar legalmente facultados, mediante concesión, autorización, licencia, permiso, convenios o cualquier otra forma de contratación administrativa, salvo la

[62] Ver ANEXO H

utilización de servicios de internet, serán reprimidos con prisión de dos a cinco años.

Estarán comprendidos en esta disposición, quienes se encuentren en posesión clandestina de instalaciones que, por su configuración y demás datos técnicos, hagan presumir que entre sus finalidades está la de destinarlos a ofrecer los servicios señalados en el inciso anterior, aún cuando no estén siendo utilizados.

Las sanciones indicadas en este artículo, se aplicarán sin perjuicio de las responsabilidades administrativas y civiles previstas en la Ley Especial de Telecomunicaciones y sus reglamentos."

1.2.29 ESTUDIO

Según los artículos de los reglamentos anteriormente mencionados, la Voz sobre IP podrá ofrecerse solamente para tráfico internacional saliente, prohibiéndose su utilización para la realización de llamadas locales, regionales, llamadas de larga distancia nacional, llamadas a servicios celulares o llamadas a servicio móvil avanzado, mediante el uso de dispositivos de conmutación, tales como Gateways o similares.

Se manifiesta que los proveedores de Servicio de Valor Agregado de Internet no podrán limitar a sus usuarios el acceso a las aplicaciones que ofrece la tecnología de Voz sobre IP, como son: comunicarse entre usuarios o entre un usuario conectado a la red Internet con un usuario conectado a una Red Pública de Telecomunicaciones del exterior, además que cualquier persona natural o jurídica, incluyendo a los proveedores de Servicio de Valor Agregado de Internet dentro de los servicios que prestan a sus usuarios, podrán comercializar dispositivos y planes para el uso de las aplicaciones mencionadas. Todo esto siempre y cuando no se usen dentro del territorio nacional dispositivos de conmutación, tales como, interfaces o compuertas (gateways) o similares, que permitan conectar las

comunicaciones de Voz sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador (exceptuando a los operadores autorizados).

Además expresa que, el CONATEL, no concederá numeración telefónica para este tipo de aplicaciones, lo cual garantiza que desde la infraestructura VoIP proporcionada por los prestadores de los servicios implementados con esa tecnología, no sea posible realizar llamadas telefónicas hacia abonados de redes nacionales que si cuentan con un plan fundamental de numeración.

Menciona la necesidad de que las empresas que tengan concesión para prestar el servicio telefónico de larga distancia internacional, presenten y registren la totalidad de su infraestructura de conmutación y transmisión utilizada, esto permite al ente controlador ejecutar un accionar más efectivo dentro de sus funciones.

Por otro lado, se prohíbe el reoriginamiento o enmascaramiento del tráfico internacional entrante o saliente con los operadores extranjeros o entre operadores nacionales con los cuales se mantengan relaciones de interconexión. Se ha rescatado este aspecto, debido a que muchas veces es parte de un fraude telefónico el enmascaramiento del tráfico internacional, de manera que el mencionado fraude pase desapercibido para los organismos de control o por las unidades que controlan el fraude en las operadoras autorizadas, las cuales serían las principales perjudicadas.

Además, para efectos de control, los concesionarios que exploten el servicio telefónico de larga distancia internacional deben garantizar, por un período de 12 meses a partir de su generación, la custodia de los registros fuente de la información relacionada con la prestación del servicio (CDR´s). Esta información es sumamente necesaria, debido a que puede ser tomada como evidencia en caso de existir fraude por parte de alguna empresa prestadora del servicio telefónico.

Con respecto a las acciones penales que podrían tomarse, en los casos de fraude, tenemos lo siguiente:

Un sistema telefónico clandestino (By pass, Call Back, Refilling, entre otros), incurre en lo contemplado en el artículo 422 del Código Penal, ya que permite prestar el servicio telefónico internacional sin contar con autorización.

En lo que a Ecuador se refiere, conforme a lo contemplado en el Art. 422, no se puede considerar dentro de la utilización de servicios de Internet, a un sistema clandestino de telecomunicaciones, como lo es el “By pass”, “Call Back”, “Refilling”, etc., técnicamente dichos sistemas pueden ser implementados utilizando las ventajas y facilidades del protocolo IP, primordialmente para establecer su enlace internacional, hecho que de ninguna manera constituye un servicio de internet; evidenciado esto, en que la operadora telefónica afectada recibe las llamadas internacionales como llamadas locales normales, sin incidencia alguna del protocolo IP (“By Pass” o “Call Back”) en lo que a la prestación del servicio ilegal se refiere, o con un aparente origen que no corresponde a aquel donde en realidad se generan las llamadas telefónicas internacionales (“Refilling”), eventos en los cuales tampoco incide de manera alguna el protocolo IP dentro de la prestación del servicio. Se debe mencionar que, la incidencia de la tecnología VoIP en esta clase de sistemas ilegales se hace presente en la implementación de los mismos, para lo cual se aprovecha las ventajas que dicha tecnología presenta, lo cual se refleja en la rápida proliferación que esos sistemas tuvieron en la etapa en la que apareció la tecnología VoIP.

Al estar en posesión de equipos que por sus características, permitan ofrecer servicios fraudulentos como los anteriormente mencionados, se admite proceder judicialmente aún cuando los equipos hayan sido desconectados.

Por otro lado, el comportamiento de las líneas telefónicas involucradas, constituye una evidencia técnica, que demuestra la generación inusual de tráfico telefónico, e incluso, permiten cuantificar las pérdidas ocasionadas a la operadora afectada.

EXPERIENCIAS EN OTROS PAÍSES

1.2.30 ESTADOS UNIDOS

En los Estados Unidos se ha creado (diciembre de 2003) un Foro [46], por iniciativa política de ese país y de la FCC ante el debate interno sobre si la VoIP ha de estar regulada como otros servicios o al contrario sujeta a una regulación mínima, y así analizar las implicaciones regulatorias de la VoIP a la vista de la potencialidad del servicio y de sus menores costes.

El 12 de febrero de 2004 la FCC[63] decidió que los servicios de VoIP totalmente basados en la Internet pública (extremo a extremo) son "servicios de información", los cuales no están regulados en los Estados Unidos. El mismo día la FCC aprobó una consulta pública para establecer reglas sobre el estatus regulatorio de los servicios IP, la cual ha sido publicada el 10 de marzo de 2004 [47]. Se pretende identificar las características de los servicios soportados sobre tecnología IP para aplicarles la regulación más apropiada, así como abordar las cuestiones relativas a la protección de los consumidores y las compensaciones a los operadores de acceso y el servicio universal conforme la VoIP vaya generalizándose.

1.2.31 JAPÓN

La experiencia de países como Japón demuestra que es posible captar el interés de una buena porción del tráfico de voz, donde la VoIP es utilizada por más del 10% de los hogares. Los operadores que ofrecen el servicio de VoIP tienen en su lista de clientes a importantes empresas y contabilizan alrededor de 4 millones de abonados ADSL que pueden disponer de su servicio.

En este país, se ha abierto una numeración específica para telefonía IP que se caracteriza por comenzar con el código "050" seguido de ocho cifras: 050-XXXX-

[63] FCC – Federal Communications Commission

XXXX. Dado que en el Japón las llamadas nacionales tienen un código de área seguido de ocho cifras (06- XXXX-XXXX), el código 050 tiene una función similar, creando un dominio nacional de telefonía IP distinto, lo que facilita el encaminamiento de las llamadas a través de redes IP.

1.2.32 EUROPA

En Europa se prestan servicios de VoIP prácticamente en la mayoría de los países, siendo de especial interés los ejemplos de Finlandia y el Reino Unido por los servicios de sus ex incumbentes.

En Finlandia el regulador Ficora[64] ha requerido a TeliaSonera que su servicio de VoIP sobre ADSL cumpla con todos los requisitos de un servicio telefónico regulado disponible al público. Para este servicio, TeliaSonera emplea la misma numeración que para otros servicios telefónicos disponibles al público.

Por otro lado, en el Reino Unido, BT lanzó un servicio de VoIP conocido como “Broadband Voice”, el cual es una oferta complementaria a su servicio telefónico tradicional con precios más baratos que éste. Broadband Voice requiere una conexión de banda ancha, ya sea de la propia BT o de otro operador de ADSL o cable módem. El servicio tiene un alcance restringido, pues, entre otras limitaciones, no permite llamar a números de emergencia ni a números de tarifación adicional.

En España, ante una petición de numeración geográfica del operador BT España, para ofrecer un servicio del tipo VoIP, la CMT[65], estableció el normal uso de la numeración geográfica para un servicio telefónico disponible al público, sin posibilidad de reubicación geográfica, está numeración está compartida con el servicio telefónico fijo (rango 8). Está establecida también en este país una numeración específica (rango 51), la cual puede ser utilizada para prestar

[64] Decisión de FICORA 629/543/2003 de 29 octubre 2003.
[65] CMT - Comisión del Mercado de las Telecomunicaciones

servicios nómadas en todo el territorio nacional, aunque se requiere que el abonado resida en España.

Para ambos tipos de numeración, específica y geográfica, se exige a los operadores el encaminamiento gratuito de las llamadas al centro de atención de emergencias 112.

En Europa se están planteando escenarios parecidos con atribuciones específicas de numeración para la VoIP como las atribuciones del "85" en Noruega, las realizadas

tras consultas públicas como el rango "056" en el Reino Unido y del "0780" en Austria, así como la del "032" en Alemania.

CONSIDERACIONES PREVIAS A UNA REGULACIÓN EFECTIVA Y REAL PARA LA PRESTACIÓN DE SERVICIOS CON LA TECNOLOGIA DE VOZ SOBRE IP

1.2.33 EVOLUCIÓN DE LA VOZ SOBRE IP Y EL CAMBIO DE PARADIGMAS

El desarrollo de nuevos estándares y especificaciones ha permitido una evolución progresiva y acelerada de la Voz sobre IP. El estándar H.323 define elementos y componentes de la Voz sobre IP y sugiere la manera de establecer, enrutar y terminar llamadas telefónicas a través de la red de Internet; entonces, frente a este constante cambio y evolución de las telecomunicaciones, la Voz sobre IP ha resultado ser una tecnología bastante prometedora, crea un mercado global para servicios de voz cada vez más competitivo. Es por esto que la voz sobre IP ha captado el interés de los proveedores de servicios de voz en todo el mundo porque brinda la capacidad de ofrecer una variedad de nuevos servicios y al mismo tiempo ofrece la posibilidad de reducir significativamente los costos de infraestructura. La Voz sobre IP, por tanto, está cambiando el paradigma de

acceso a la información, fusionando los servicios de voz, datos, vídeos y otros relacionados, sobre una sola estructura de acceso convergente, haciendo posible una transición pacífica entre las redes públicas telefónicas conmutadas y las redes de siguiente generación.

El protocolo IP y esta nueva tecnología se perfilan como el punto central de las demás redes, es por ello que una regulación que se defina para proveer servicios IP debería considerar los derechos y obligaciones que las concesionarias de estos servicios tendrían, tanto desde el punto de vista de los servicios que proveen, como de la calidad de los mismos, o las relaciones entre las concesionarias y las permisionarias; y, deberán estar orientadas a promover la libre competencia, la protección y garantía de los derechos de los usuarios, la calidad y seguridad del servicio, las sanciones aplicadas en el caso de conductas ilegales, etc.
Los aspectos regulatorios a ser revisados serían los títulos habilitantes, el hecho de saber si se requieren licencias, clasificación de los servicios, interconexión, servicio universal, calidad y seguridad del servicio, etc. Todos estos aspectos deberán ser evaluados al momento de tomar en consideración una regulación de los servicios de Voz sobre IP.

1.2.34 OBJETIVOS DE POLÍTICA Y PRINCIPIOS REGULATORIOS

En el ámbito del perfeccionamiento del marco regulatorio del sector de telecomunicaciones, es necesario tener presente aquellos objetivos que se basan principalmente en el interés del Estado por favorecer el desarrollo de nuevas tecnologías que permitan a los consumidores disponer de más y mejores servicios de telecomunicaciones.

Por otro lado y no menos importante, resulta el desarrollo de las redes y la infraestructura necesaria para el fortalecimiento de los servicios de telecomunicaciones. La misma red Internet, como es obvio, no existiría si no

fuese por el despliegue de redes físicas e inalámbricas, lo cual también es válido para cualquier servicio sustentado técnicamente sobre dichas redes.

Las regulaciones que se establezcan deben estar orientadas a minimizar las distorsiones que puedan existir en el mercado, sin perjuicio de los mayores grados de eficiencia que se puedan obtener con el mayor volumen de competencia que podría introducirse con la llegada de nuevas tecnologías.

La regulación de la Telefonía IP deberá responder a ciertos principios fundamentales para el logro de los objetivos de esta política.
Estos son:

1. Regulación de servicios: La política regulatoria se orienta a maximizar el bienestar de la sociedad en términos de la calidad, precio y cobertura de los servicios que se ofrecen.

2. Neutralidad tecnológica: La tecnología debe ser transparente para la regulación. El marco regulatorio no debe favorecer un tipo de tecnología por sobre otro.

3. No discriminación: La regulación no debe establecer diferencias en lo que se refiere a la prestación de servicios equivalentes. Tratamientos asimétricos solamente se justifican por razones de competencia.

4. Beneficio y protección del consumidor: La regulación debe establecer un conjunto de garantías mínimas que den resguardo a los consumidores respecto de las empresas en presencia de relaciones asimétricas.

5. Apertura a la innovación y la inversión: La regulación debe establecer las condiciones adecuadas para permitir el cambio tecnológico, la innovación y en ese contexto, favorecer la inversión. Un ambiente estable y con regulaciones claras, disminuye la incertidumbre e impulsa la inversión y el desarrollo.

6. Mínimo necesario: La regulación debe orientarse a corregir problemas o asimetrías presentes en el mercado, procurando generar las mínimas distorsiones. En consideración a ello, la regulación debe dimensionarse en función de las necesidades específicas y revisarse continuamente, con el objeto de ajustarse dinámicamente a dichos requerimientos.

7. Apertura a la inversión: la regulación debe facilitar el desarrollo de proyectos que generen riqueza para el país y, que fortalezcan la infraestructura nacional de telecomunicaciones para el desarrollo de actividades económicas y la consolidación de la posición del país como plataforma de negocios.

1.2.35 NATURALEZA DEL SERVICIO

Con el objeto de evaluar las distintas regulaciones que se pueden implementar para este tipo de servicios, se definen a continuación los elementos que los caracterizan genéricamente.

Ubicación

Se refiere a la cualidad de asociar el servicio con una ubicación geográfica determinada. La naturaleza geográfica está definida por la integración entre las redes de acceso y el servicio, o por el contrario, si se accede al servicio a través de Internet. Las tecnologías desarrolladas para la prestación del servicio de VoIP permiten la ubicuidad automática, es decir, los usuarios mantienen su identificación dentro de la red independientemente de su posición geográfica en el mundo.

Medio de acceso

El medio de acceso es la red, por medio de la cual el usuario puede hacer uso del servicio. Los medios de acceso pueden ser diversos e incluyen conexiones físicas

e inalámbricas, con diversos grados de calidad en dependencia de las cualidades de cada uno.

Interconexión

Se refiere a si se interconecta con la red pública telefónica y/o con otros servicios VoIP. Esta cualidad constituye un elemento central en la definición del servicio, por cuanto establece su naturaleza de servicio público o restringido.

Numeración

Asociado a lo anterior, tendría que definirse si usa numeración del servicio público telefónico, o si se establece numeración especial para identificar el servicio como distinto del telefónico tradicional (calidad, tarifa). La numeración a asignar dependerá de si el operador se interconecta o no con la red pública telefónica.

Calidad

La calidad está determinada por el medio de acceso y la integración entre el servicio y dicho medio.

1.2.36 DIFICULTADES NORMATIVAS DE LA VOIP [48]

Muchas de las empresas de telecomunicaciones del mundo están instalando redes, basadas en el protocolo Internet (IP), que transmiten voz y datos; de este modo, los operadores pueden invertir en una sola red que se puede utilizar más eficazmente para distintas modalidades de tráfico.

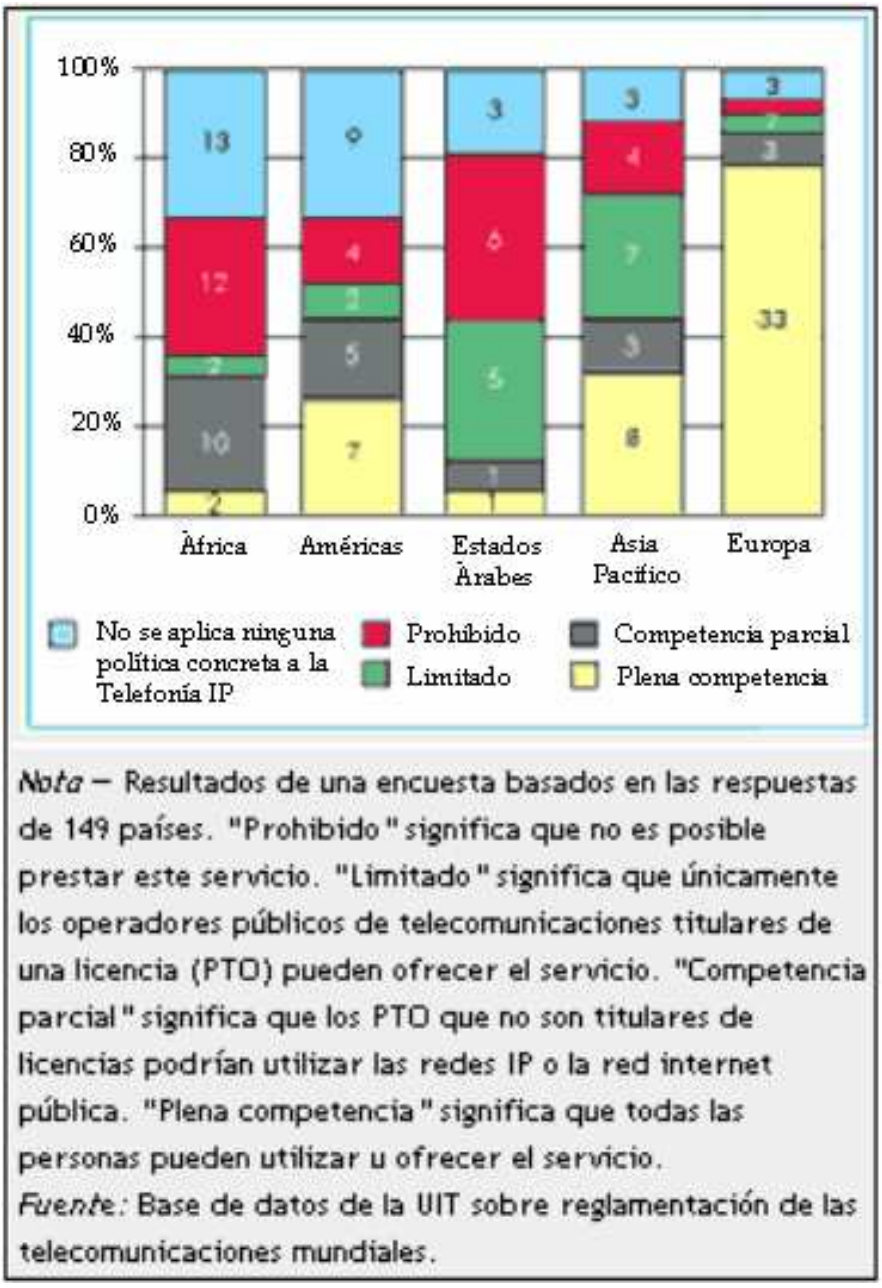
El tráfico internacional cursado por medio de la tecnología de Voz sobre IP (VoIP) está en aumento. Entre 20 y 25% de los operadores titulares de África, por ejemplo, utilizaban la VoIP para transmitir parte de su tráfico internacional en 2004.

Nuevos actores del mercado también ofrecen VoIP, tales como los Proveedores de Servicios de Internet (ISP) en Ciber Cafés. La VoIP también afecta a los sistemas de telecomunicaciones más antiguos y entraña la pérdida de tráfico saliente internacional al por menor, así como reducciones del tráfico internacional entrante sujeto a tasas de liquidación (porque el tráfico generado por los clientes VoIP en el extranjero elude el sistema internacional de tarifación).

Si bien la VoIP plantea cada vez más problemas a los operadores de infraestructuras existentes, también permite ofrecer servicios más asequibles a los clientes. El auge de la VoIP ha puesto de manifiesto el frágil equilibrio que deben lograr muchos reguladores entre el fomentar un acceso poco oneroso a los servicios y, por otro, el deseo de proteger a los operadores establecidos.

No es sorprendente, por lo tanto, que este auge haya dado lugar a numerosas reacciones normativas, de la simple prohibición a la legalización total (Figura 4.1).

La autorización o prohibición de la VoIP no es, sin embargo, más que una de las numerosas dificultades que se han de afrontar, además de la elaboración de marcos normativos para la interconexión de redes con conmutación de circuitos con otras basadas en IP, así como diversas cuestiones planteadas por el hecho de que los clientes de la VoIP pueden utilizar el servicio en todas partes y, no dependen de una línea fija ni de un terminal móvil, lo cual plantea, por ejemplo, dificultades para los servicios tradicionales de numeración y de emergencia.



Nota – Resultados de una encuesta basados en las respuestas de 149 países. "Prohibido" significa que no es posible prestar este servicio. "Limitado" significa que únicamente los operadores públicos de telecomunicaciones titulares de una licencia (PTO) pueden ofrecer el servicio. "Competencia parcial" significa que los PTO que no son titulares de licencias podrían utilizar las redes IP o la red internet pública. "Plena competencia" significa que todas las personas pueden utilizar u ofrecer el servicio.
Fuente: Base de datos de la UIT sobre reglamentación de las telecomunicaciones mundiales.

Figura 4.1: Situación reglamentaria de las transmisiones vocales por el protocolo Internet (VoIP) por Región, 2005

POSIBLES ESCENARIOS Y ALTERNATIVAS DE REGULACIÓN [4]

1.2.37 VOZ SOBRE LA INTERNET PÚBLICA

La Internet pública, como red de redes, sigue su imparable crecimiento permitiendo un acceso cada vez más universal a todo tipo de información y fomentando el camino hacia una verdadera sociedad de la información. Pionera de esta tecnología, la *web* está "tejida" sobre el mismo protocolo Internet. Sin embargo, aunque sobre un sustrato tecnológico común, las tecnologías IP más avanzadas han permitido desarrollar aplicaciones de mayor nivel para el soporte de servicios interactivos como la VoIP (por ejemplo: sobre MPLS) asegurando niveles adecuados de calidad de servicio en redes de operadores establecidos.

Desde hace ya algún tiempo, se viene observando un fenómeno de innegable interés. Favorecidos por la creciente penetración de los accesos de banda ancha, tanto en el sector de empresas como en el residencial, la cual ha estado promovida por los operadores tradicionales y entrantes establecidos, otros tipos de entidades están ofreciendo servicios de VoIP utilizando conjuntamente las redes del operador que provee el acceso físico (por ejemplo: el par de cobre), un acceso de banda ancha a la Internet pública (por ejemplo: un ADSL básico ó un cable MODEM) y la propia Internet pública (que se forma en gran medida con las redes IP propias y redes *backbone* de los distintos operadores).

Así, con una infraestructura utilizada sin ningún tipo de remuneración a terceros por este tipo de proveedores de servicios Internet, y aunque sin garantías de calidad de servicio, se están ofreciendo servicios de VoIP transparentes al control inmediato por los operadores establecidos y con creciente aceptación por determinados tipos de usuarios atraídos por tarifas gratuitas o muy ventajosas. Entre estos sistemas se encuentran los conocidos como *peer-to-peer* y los *instant messaging*. A la provisión de estos servicios de voz sobre IP se le suele conocer como "**telefonía Internet**" o **VoIP**$_{\textbf{web}}$ queriendo significar que aunque es VoIP su soporte básico está en la Internet pública o *web*.

Una de las características más relevantes del concepto de VoIP$_{web}$ sería que no ofrece la interoperabilidad con los otros servicios telefónicos (no pueden dirigirse llamadas a numeraciones telefónicas sino únicamente a los nombres de usuario del servicio) y a los efectos de las redes empleadas para su provisión, estos tráficos de voz no se diferenciarían del tráfico habitual de acceso a Internet (con calidad no garantizada ó "*best effort*") y, por consiguiente, las condiciones aplicables, incluidas las regulatorias, si hubiera alguna, serían las mismas que para cualquier otro servicio de acceso a Internet, es decir, prácticamente ningún tipo de regulación, ni de compromiso de calidad, como tampoco ningún tipo de contribución a los costes incurridos por las redes de acceso ni las redes de conmutación de paquetes IP que permiten encaminar estos tráficos hasta la Internet pública, más allá de lo que un usuario abonaría por el coste del acceso a Internet (normalmente una tarifa plana).

Es decir, no sería hoy posible (al menos de forma sencilla), ni identificar estos tráficos como de voz ni aplicarles por tanto ningún tipo de obligaciones asociados al actual concepto de servicio telefónico ya que las comunicaciones se establecen entre los extremos mediante terminales asociados en el momento de la comunicación a nombres (por ejemplo: direcciones *e-mail*), que representan direcciones IP de red y no números de un plan de numeración telefónico.

Una penetración significativa de prestación de servicios de voz de esta manera, impulsado por un uso creciente de PCs multimedia y servicios de acceso de banda ancha, llevaría inevitablemente a una disminución del tráfico "regulado" de voz en los operadores con título habilitante para la prestación del servicio telefónico regulado. El efecto sobre los operadores establecidos podría ser sentido como "fuga de tráfico", aunque ésta se realice a través de sus propios accesos y redes.

Una de las cuestiones en la regulación, debe considerar el saber cuales serían las implicaciones de la VoIP$_{web}$, pero su relevancia comienza a no ser despreciable cuando ya se observa en análisis económicos de consideración que la pérdida por operadores tradicionales en favor de otras entidades de tráfico de voz vía VoIP, es una amenaza de importancia a la hora de valorar las expectativas sobre los

potenciales ingresos y beneficios de esos operadores. No parece evidente que la VoIP$_{web}$ pueda ser un sustitutivo de la telefonía regulada.

El actual Servicio telefónico convencional, disponible desde cualquier acceso que se ofrezca, ha de permitir al menos:

- Acceso a servicios de emergencia y de directorio.
- Interoperabilidad y acceso a otros servicios y por tanto interconexión.
- Derechos de desconexión de determinados servicios.
- Interceptación de llamadas.
- La portabilidad numérica entre operadores (en el caso de la VoIP$_{web}$ no hay asociación directa entre número telefónico e identificación del punto de terminación de la red).
- Garantías de seguridad e integridad de la red.
- Protección a los consumidores en contratos, calidad de servicio, facturación o reclamos.

Además de otras obligaciones y derechos de los usuarios que la telefonía regulada ha de cumplir, y que los proveedores de VoIP$_{web}$ no podrían hoy técnicamente satisfacer, ni tienen incentivos para hacerlo.

Es decir, podríamos contemplar en el corto y medio plazo un escenario posible en el que un porcentaje de abonados del servicio telefónico regulado dispongan también de un acceso de banda ancha y una gran parte de las comunicaciones de voz de mayor costo fuese realizada mediante VoIP$_{web}$. Si el impacto de la disminución de tráfico regulado y “controlado” fuese importante, sería posible pensar en consecuencias derivadas sobre los costos del servicio universal

(posiblemente mayores), las cuotas de abono y acceso a la banda ancha, o una potencial redefinición de los mercados de telefonía con el consecuente replanteamiento de las obligaciones asociadas, entre otros efectos derivados.

1.2.38 VOZ SOBRE LA INTERNET PÚBLICA CON ESCENARIOS MIXTOS (VOIP$_{WEB}$ Y RED TRADICIONAL)

Es técnicamente posible desde luego ofrecer un servicio de VoIP$_{web}$ exclusivamente sobre la Internet pública utilizando, en uno o más extremos de la comunicación, numeraciones telefónicas E.164[66] que, en tal caso, deberían haber sido previamente asignadas por el regulador a dicho operador de VoIP$_{web}$ haciendo más "visible" el servicio.

Existen escenarios mixtos cuando las comunicaciones se efectúan entre terminales conectados a servicios/redes de VoIP$_{web}$ y terminales telefónicos conectados a redes tradicionales de circuitos (Ej: usuario de VoIP$_{web}$ llama a un número telefónico geográfico ó móvil). Estas comunicaciones podrían producirse en ambos sentidos si el cliente de los servicios de la red VoIP$_{web}$ dispusiera también de una numeración telefónica asociada al servicio.
En cualquier caso, entre la red del proveedor de servicios VoIP$_{web}$ y la del operador con red de circuitos deberá existir en algún momento (aunque sea vía tránsito) un punto de interconexión o de acceso a la red telefónica. Para ello el operador de VoIP$_{web}$ deberá disponer de una pasarela para la señalización SS7 o la correspondiente de acceso con la red de conmutación de circuitos del operador tradicional, además de adaptar el formato de la señal vocal a las características de la red en la que vaya a terminar la llamada.

En un escenario mixto (web - red telefónica de circuitos), cuando las llamadas terminan en un número telefónico de una red convencional, las posibles tarifas aplicables por el operador de VoIP$_{web}$ podrían probablemente ser menores que las

[66] E.164: Es una recomendación de la UIT que asigna a cada país un código numérico (código de país), usado para las llamadas internacionales.

convencionales por los ahorros producidos en la parte de red IP, aunque dependerán en gran medida de los precios de terminación en la otra red. En el otro sentido, para terminar las llamadas sobre el cliente de $VoIP_{web}$, este operador debería disponer de algún tipo de numeración telefónica, y aquí se plantea una de las principales preguntas, sobre si es pertinente favorecer este tipo de comunicaciones y asignar numeración telefónica (y ello sujeto a qué condiciones) a los operadores de $VoIP_{web}$.

Nos encontraríamos entonces ya con un servicio de VoIP prestado por un agente que ha notificado la prestación de un servicio que requiere asignación de numeración (como en particular el servicio telefónico), supuesto que se analiza igualmente en el siguiente apartado. En todo caso, de ser posible, la tarifa aplicable por el operador tradicional dependería del tipo de numeración telefónica del destino, ya sea geográfica, móvil, o una numeración específicamente atribuida para este tipo de servicios de VoIP.

1.2.39 VOZ SOBRE REDES IP DE OPERADORES QUE HAN NOTIFICADO EL SERVICIO TELEFÓNICO

En un ámbito distinto estarían los servicios de voz o telefonía sobre protocolo Internet ofrecidos por entidades establecidas y registradas (con autorización) para prestar servicios de telefonía utilizando el protocolo Internet (VoIP) y, transporte por su propia red de operador, en toda o en parte de la comunicación extremo a extremo. En estos servicios habría que diferenciar las redes privadas de centralitas IP de los servicios de VoIP soportados sobre redes públicas, incluidas las redes privadas virtuales sobre IP (VPNoIP).

Se podrían considerar tres escenarios básicos:

a. Las redes de acceso utilizan tecnología de circuitos (línea analógica o acceso digital RDSI o móvil) pero las redes de tránsito (una de ellas al menos) son de tecnología VoIP;

b. Una de las redes de acceso es de VoIP (la de origen o la de terminación);

c. Todo el encaminamiento de la comunicación se realiza mediante VoIP.

En el caso (a) el usuario no debería percibir diferencias. En el caso (b) el llamante o el llamado utilizan un acceso IP para el soporte telefónico vocal, pero una parte de la comunicación se soportará en circuitos. En el caso (c) toda la comunicación se soportaría en protocolo IP.

Se asume en todos los escenarios que, al margen de que la verdadera identificación de los accesos IP en las redes sea un URL[67] o una dirección IP, la comunicación telefónica se realiza entre números telefónicos de un plan nacional de numeración (E.164).

El usuario no debería apreciar diferencias importantes con la calidad acostumbrada en la comunicación mediante conmutación de circuitos, aunque la percepción subjetiva de la calidad podría ser menor a la habitual en ciertos casos. Se supone no obstante que un nivel suficiente de calidad de la comunicación estará garantizada por códecs apropiados y técnicas IP como MPLS que hoy en día podrían hacer casi indistinta la percepción de la calidad de los servicios de VoIP y de voz sobre circuitos.

En todos los escenarios la comunicación se efectuará entre numeraciones telefónicas, pero con algunas salvedades. En el caso (a) la numeración está asociada a un punto de terminación de red fijo, o mediante una numeración móvil a un acceso radio.

En el caso (b) sin embargo, aunque el acceso IP esté identificado por una dirección IP (o URL), tendrá también asociada una dirección E.164, aunque la dirección IP permitirá reubicación de acceso (en sentido de movilidad geográfica) en el caso de la red fija cuando se acceda desde otro punto de terminación de red

[67] URL – Universal Resource Locator: permite identificar un recurso en una red IP sin necesidad de conocer la dirección IP en la que se encuentra. Así por ejemplo, en el caso del protocolo de Voz sobre IP, SIP, la identidad del usuario podría venir dado por un URL del tipo “sip: usuario@dominio.ec”.

distinto del asociado. En (c) la reubicación o movilidad en el caso de redes fijas será posible en ambos extremos de la comunicación.

Lo esencial en el escenario (a) es que para los usuarios (llamante y llamado) el hecho de cursar parte del encaminamiento de la llamada con soporte de VoIP podría ser totalmente transparente puesto que sus terminales y su forma de comunicarse no difieren de la telefonía convencional. Así la red de tránsito de VoIP podría ser perfectamente una red seleccionada o preseleccionada siendo quien factura al cliente llamante, por lo que este escenario (a) no sería diferenciable del Servicio telefónico Convencional.

En adelante hablaremos de los servicios de telefonía o voz sobre IP prestados sobre su propia red IP por operadores establecidos y registrados con autorización como "**telefonía IP**" y los abreviaremos como **VoIP$_{red}$**. Los servicios de VoIP$_{red}$ soportados en la red IP de un operador deberán poder interoperar (en interconexión) con los Servicios telefónicos Convencionales o telefonía regulada soportados por dichas redes, evitando crear dominios incomunicados.

Incluso una aplicación perfecta de la neutralidad tecnológica podría llevar a la necesidad de que la VoIP$_{red}$ fuese a efectos regulatorios totalmente comparable al Servicio telefónico Convencional. Sin embargo, las actuales prestaciones de la VoIP podrían en algunos aspectos ser más limitadas que las soportadas por la telefonía regulada, a la vez que ofrecer por otro lado otras prestaciones no disponibles en el Servicio telefónico Convencional. Por ejemplo, la posibilidad de reubicación o movilidad de acceso en redes fijas (por identificación real mediante dirección IP y ficticia mediante dirección ó numeración telefónica) hace más versátil al servicio de VoIP eliminando la unicidad de la relación PTR/ubicación-fija/número-telefónico y vacía de cierto sentido la información sobre tarifas aplicables al usuario en la llamada.

Si bien un operador de VoIP$_{red}$ podría ofrecer un servicio de telefonía con unas características equivalentes al Servicio telefónico Convencional en el escenario (a), cumpliendo con todas las obligaciones derivadas del servicio público, los menores costos intrínsecos de IP, y sus mayores potencialidades y versatilidad

podrían verse, en cierta medida limitados en los escenarios (b) y (c) por la rígida concepción de una definición de servicio muy ligada a la conmutación de circuitos. Un ejemplo de servicio en línea con los escenarios (b) y (c) podría ser el lanzado en los EEUU por el operador AT&T con el nombre comercial de CallVantage [49].

En el siguiente cuadro se recogen los servicios considerados:

Escenario	***Observaciones***
Telefonía Internet (VoIPweb) sin interoperabilidad con el Servicio Telefónico Convencional.	sin asignación de numeración telefónica.
Telefonía Internet (VoIPweb) en interoperabilidad con el Servicio Telefónico Convencional.	con asignación de numeración telefónica
Telefonía IP (VoIP red) de operadores con red IP propia e interoperabilidad con el Servicio Telefónico Convencional.	acceso directo IP y asignación de numeración telefónica
Telefonía con acceso telefónico convencional prestada usando tecnologías IP	regulado como STDP convencional

Tabla 4.1: Servicios considerados - Resumen

MARCO REGULATORIO Y NEUTRALIDAD TECNOLÓGICA

La VoIP no parece encajar bien en el nuevo marco por varias razones. Desde un punto de vista de neutralidad, debería ser irrelevante que un servicio “telefónico” se soporte en conmutación de circuitos o de paquetes. La definición de servicio telefónico disponible al público liga necesariamente este servicio a números de planes de numeración telefónica, sin embargo bastaría identificar dos terminales distantes por medio de direcciones IP o identificadores URL para establecer una comunicación vocal entre ellos empleando VoIP. Quizá la definición referida

pudiera pretender justamente dejar ‘fuera de la regulación’ a los servicios de VoIP sin numeración telefónica, pero si éstos pudieran desde una perspectiva de usuario ser totalmente sustitutivos de los servicios tradicionales, parecería que la definición referida no es tecnológicamente neutral.

Desde luego, como ya se ha comentado, es posible asociar a una dirección IP una numeración telefónica. Un operador podría plantearse hoy ofrecer un servicio telefónico fijo sustitutivo del clásico mediante $VoIP_{red}$. Sin embargo se encontrará con varios inconvenientes derivados del actual marco regulatorio. Por un lado tendrá que asignar un número telefónico a cada abonado, con lo que habrá de optar por un número geográfico. No obstante, los costos de provisión de la $VoIP_{red}$ permitirían ofrecer tarifas menores y así competir mejor en el ámbito de los Servicios Telefónicos Convencionales. Ninguna de las numeraciones telefónicas actuales parece ser apropiada, por lo que una atribución específica aliviaría este problema.

Mediante el empleo de la numeración geográfica sus abonados quedarían ‘atados’ al punto de terminación de red que identifica dicha numeración, con lo que se impediría una facilidad de reubicación de acceso o movilidad de ubicación fija, ya que las llamadas a los abonados del servicio $VoIP_{red}$ pueden ser encaminadas a una determinada dirección IP con independencia del punto de terminación de red en que el abonado está en cada momento. Así, con el nuevo marco, un operador de $VoIP_{red}$ podría ofrecer un servicio telefónico “regulatoriamente correcto” pero claramente limitado si se emplea numeración geográfica.

La antes mencionada reubicación de acceso o movilidad de ubicación permitida por la VoIP presentaría distorsiones cuando un abonado con numeración fija de la provincia “A” y de una ciudad “a_i” estuviese, por ejemplo, realmente conectado a un punto de terminación de red de la ciudad “b_j” de una provincia “B”. Se perdería el sentido de las tarifas (al llamante se le aplicarían siempre tarifas de acuerdo a su supuesta ubicación en la ciudad a_i). Con las tecnologías IP la distancia se vuelve mucho menos relevante (los costos son mayores según la distancia pero mucho menos importantes que en conmutación de circuitos) por lo que los

conceptos de “local” o “larga distancia” perderían en buena medida su significado convencional.

El actual marco no impide la prestación de los servicios de VoIP, pero en la práctica condiciona sus mayores potencialidades ante lo que puede ser necesaria la introducción de niveles de regulación más apropiados para nuevos servicios que, como la VoIP, podrían considerarse innovadores y diferenciados de la telefonía clásica fuertemente regulada. En particular, además de otros conceptos en las Directivas, la neutralidad tecnológica se vuelve paradójicamente impracticable cuando una tecnología como la de IP puede ofrecer un servicio de VoIP percibido por los usuarios como muy similar a la telefonía convencional, aunque presenta importantes diferencias con ella tanto en sentido positivo (por ejemplo: menores precios, reubicación, flexibilidad y conjunción con servicios convergentes) como en sentido negativo (actualmente es posible que técnicamente no pudiese cumplir alguna de las obligaciones regulatorias del servicio telefónico disponible al público).

LA VoIP COMO UN SERVICIO DIFERENCIADO

Cuando los servicios de VoIP se ofrecen involucrando el acceso (escenarios previos (b) y (c)), y no solamente por operadores *carriers* seleccionados o preseleccionados para cursar llamadas entre accesos de otras redes (escenario (a)), parecen evidenciarse como servicios diferenciados del Servicio Telefónico Convencional o telefonía regulada convencional.

El servicio de VoIP (desde el acceso) implicará normalmente la contratación y el soporte del servicio sobre un acceso de banda ancha, en absoluto necesario en el Servicio Telefónico Convencional para el que basta el contrato estándar de acceso telefónico. Algunas facilidades y garantías de calidad, disponibles con el servicio universal o con el Servicio Telefónico Convencional, pueden no disfrutarse actualmente con los servicios de VoIP. Asimismo, el servicio de VoIP permite la reubicación del acceso fijo y el ofrecimiento de un servicio con tarifas

significativamente diferenciables de las asociadas a la telefonía convencional. Por ello, además de otras consideraciones que los hacen muy distintos por su soporte tecnológico, desde la perspectiva de la demanda el Servicio Telefónico Convencional y los servicios de VoIP no parecerían ser hoy servicios sustituibles, a excepción, como ya se ha comentado, de cuando se considera como Servicio Telefónico Convencional ofrecido al nivel de tránsito por un operador seleccionado o cuando deliberadamente un operador pueda y quiera equipararlo, lo que sería totalmente transparente para el usuario (neutralidad tecnológica).

En este punto parece necesario plantear la pregunta sobre la consideración de los servicios de VoIP que involucren una forma de acceso distinta a la convencional como servicios diferenciados.

Hay que resaltar que la VoIP se caracteriza también por un gran potencial de crecimiento y las muy distintas formas en que podrá llegar a ofrecerse, por lo que cabría preguntarse igualmente si sería razonable considerarlo como servicio emergente.

ESCENARIOS REGULATORIOS POSIBLES PARA LA VoIP EN EL CORTO PLAZO

En Ecuador, así como en gran parte de países en el mundo, se viene debatiendo sobre cuál es la mejor caracterización de la VoIP, en el contexto del actual marco regulatorio y de las leyes sobre competencia y protección al consumidor, con el objetivo de alcanzar un tratamiento de la Voz sobre IP lo más armonizado posible, proporcionando certidumbre legal y salvaguardando los intereses de los consumidores, a la vez que se ofrecen suficientes incentivos de desarrollo de los servicios de Voz sobre IP.

A continuación se mencionan algunos de los posibles escenarios que regirían el desenvolvimiento de los servicios basados en Voz sobre IP, así como sus alternativas de regulación:

1.2.40 ESCENARIO DE TELEFONÍA INTERNET ($VoIP_{web}$)

En esta alternativa, la $VoIP_{web}$ o "telefonía Internet" se daría siempre y cuando las llamadas extremo a extremo entre iguales (peer-to-peer) no fuesen diferenciables de los accesos a la Internet pública desde los extremos de la comunicación.

En principio, no sería necesario ningún tipo de numeración telefónica para la prestación de este servicio. Este escenario ha surgido en el entorno no regulado de Internet.

1.2.41 $VoIP_{web}$ (CON NUMERACIÓN TELEFÓNICA) EN INTEROPERABILIDAD CON EL SERVICIO TELEFÓNICO CONVENCIONAL[68]

Cuando existan escenarios mixtos, es decir, con una de las terminaciones perteneciendo a una red convencional (PSTN ó SMC (Servicio Móvil Celular) ó SMA (Servicio Móvil Avanzado), este extremo estará identificado por una numeración telefónica. Cuando la llamada se origina mediante $VoIP_{web}$ y termina en un número tradicional, podría no garantizarse la recepción en destino de la identificación de la línea llamante (asociada al acceso de banda ancha).

En el otro sentido de la comunicación, el prestador del servicio de $VoIP_{web}$ debería normalmente disponer de una numeración telefónica para que ambos servicios pudieran interoperar, asumiendo que sería una numeración específica de VoIP. Ello llevaría también a plantear la necesidad de portabilidad numérica en el dominio de la numeración de VoIP (ver siguiente escenario).

En cuanto a la regulación asociada a estos escenarios, una regulación mínima podría exigir la interconexión e interoperabilidad del servicio de telefonía y una clara información al abonado conectado a la red tradicional sobre las tarifas

[68] Con Servicio Telefónico Convencional, nos referimos al servicio telefónico tradicional, al cual actualmente tiene acceso el público, sea telefonía fija o móvil.

aplicadas, las limitaciones del servicio y la posible falta de garantía de calidad en las llamadas a usuarios de $VoIP_{web}$.

1.2.42 $VoIP_{red}$ DE OPERADORES CON RED IP PROPIA E INTEROPERABILIDAD CON EL SERVICIO TELEFÓNICO CONVENCIONAL

La interoperabilidad con el Servicio Telefónico Convencional, así como el fomento del desarrollo de los servicios de VoIP llevarían a la necesidad de que estos operadores para sus redes/servicios de telefonía IP hubieran de disponer de numeración telefónica. Actualmente en la mayoría de los casos, estos operadores disponen también de redes de conmutación de circuitos.

La numeración telefónica podría ser geográfica, numeración personal, móvil o de algún otro tipo de las numeraciones atribuidas. Sin embargo, los menores costos inherentes a la provisión de servicios de VoIP y las facilidades adicionales como la reubicación de acceso, junto con posibles limitaciones en la actualidad a emular todas las características impuestas al Servicio Telefónico Convencional, parecen hacer muy idónea la atribución de numeración específica para la VoIP para un mejor desarrollo del servicio, evitando lastrar los incentivos a la innovación, la competencia en el mercado de la telefonía y el acceso a la banda ancha.
Garantizado el servicio universal en cualquier ubicación fija (mediante el servicio de banda estrecha), se debería permitir que los operadores pudiesen competir en el mercado de la VoIP en igualdad de condiciones. Una numeración telefónica específica caracterizaría claramente a la familia de servicios de VoIP, los cuales tendrían en cualquier caso como referencias al Servicio Telefónico Convencional por un lado y al servicio universal por otro como servicios competidores a emular y superar en prestaciones.
Si bien la atribución de numeración telefónica es una competencia del CONATEL, puede ser de gran interés analizar cuál sería la mejor de las opciones de tal numeración de VoIP.

En cualquier caso la numeración específica de VoIP debería claramente identificar a un usuario de un servicio de VoIP, teniendo en cuenta las posibilidades técnicas de movilidad del servicio, y facilitar el encaminamiento en las redes y en interconexión.

Asumiendo la posibilidad de atribución de una numeración específica, cabría plantearse qué obligaciones regulatorias serían apropiadas para la $VoIP_{red}$, atendiendo al criterio general de regulación mínima, y en contraste con el Servicio Telefónico Convencional. De hecho, la mayoría de los abonados a estos servicios de VoIP normalmente dispondrán de un acceso telefónico convencional con servicio universal, o de un Servicio Telefónico Convencional (Ej: de un operador de cable), asociado a un bucle físico sobre el que también dispondrán de un acceso de banda ancha (pe. ADSL o cable -módem) que les permitirá acceder a servicios del tipo de VoIP.
Por ello podría considerarse suficiente (en principio) exigir interconexión e interoperabilidad de servicios entre la $VoIP_{red}$ y el Servicio Telefónico Convencional, así como una clara información a los abonados conectados tanto a la red del Servicio Telefónico Convencional como a los conectados a través de la $VoIP_{red}$ sobre las tarifas aplicadas, las limitaciones del servicio y, en su caso, sobre la posible falta de garantía de calidad cuando se utilice el servicio.

El acceso a los servicios de emergencia será, sin duda, una situación controvertida y que afectaría principalmente a aquéllos abonados que no dispusieran de un Servicio Telefónico alternativo (bien fijo sobre el mismo acceso físico o bien un servicio móvil), al poder quedar aislados respecto de la posibilidad de acceder adecuadamente a los servicios de emergencia si su proveedor de $VoIP_{red}$ no se lo garantizara. Lo mismo puede decirse del acceso a los servicios de directorio y a las guías, así como de las obligaciones sobre seguridad e integridad de la red.

Respecto de la portabilidad numérica, no parecería oportuno exigir portabilidad cruzada entre los dominios de numeración de VoIP y los de Servicio Telefónico Convencional, por la conveniencia de que permanezcan de momento separados.

Sin embargo, la portabilidad por cambio de operador dentro del propio dominio de numeración específica para VoIP, sería sin duda de claro interés para los usuarios y para el fomento de una mayor competencia, no debiendo plantear mayores inconvenientes para los operadores de VoIP.

En cuanto a la protección del consumidor, estas obligaciones parecen esenciales cubriendo los aspectos contractuales, la calidad de servicio garantizada y una necesidad de ofrecer información muy clara y precisa sobre las facilidades y limitaciones del servicio contratado.
En este punto y retomando el problema del acceso a los servicios de emergencia, cabe preguntarse si sería exigible una “regulación social” fuerte, al objeto de garantizar el máximo confort a los usuarios de los servicios de VoIP.

Es esperable que el fomento de los servicios de VoIP y el rápido desarrollo tecnológico de las tecnologías IP haga desaparecer, en un tiempo razonable, las limitaciones en cuanto a facilidades soportadas hoy por los actuales Servicios Telefónicos Convencionales. Aunque el proceso no será desde luego inmediato, es claro que la mayoría de las facilidades de los Servicios Telefónicos Convencionales serán absorbidas por la VoIP y que sus menores costes y mayores prestaciones potenciales facilitarán la progresiva migración de todos los servicios telefónicos hacia las tecnologías convergentes hoy representadas por IP. Es desde la convicción de este escenario futuro donde se podría plantear una regulación mínima para los servicios emergentes de VoIP.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1.2.43 CONCLUSIONES SOBRE ASPECTOS TECNOLÓGICOS

- La Voz sobre IP es una tecnología que permite la transmisión de la voz a través de redes IP, en forma de paquetes de datos. La aplicación más notoria de esta tecnología, es la realización de llamadas telefónicas ordinarias a través de la red.

- Los principales objetivos que busca la Voz sobre IP son:

    - Acoplamiento operativo con la red telefónica pública conmutada;
    - Proporcionar servicios de uso común;
    - Asegurar Calidad de Servicio (QoS), y;
    - Proporcionar seguridad de beneficios.

- A corto plazo la VoIP traerá importantes transformaciones en el negocio de las telecomunicaciones y, a medio plazo, podría sustituir las llamadas desde líneas fijas.

- Debido a que el servicio que ofrece la tecnología de Voz sobre IP, es independiente del lugar en que se encuentre el usuario y no depende de una línea fija ni de un terminal móvil, existe dificultad para acceder a los servicios tradicionales de directorio y de emergencia, que ofrece cada país.

- Existe controversia a nivel mundial al momento de elegir una numeración (específica o geográfica), para telefonía IP.

  En el caso de que la elección sea una numeración geográfica, el usuario quedaría atado al punto de terminación de red que identifica dicha numeración.

  En el caso de que la numeración escogida fuera específica, se aprovecharía la movilidad o reubicación de acceso que ofrece la tecnología. Pero a su vez, existe la posibilidad de que esto facilite el que se cometan ciertos tipos de fraude, como lo es el Vishing.

  Por lo tanto, se concluye que una numeración geográfica es la más apropiada, no solo por lo mencionado anteriormente, sino además por que al aplicar una numeración específica se podrían presentar distorsiones en cuanto a las tarifas aplicables, ya que el usuario pagará la misma tarifa asociada a dicha numeración y a su supuesta ubicación, sin importar el lugar geográfico en el cual se encuentre.

- El uso de las aplicaciones que ofrece la tecnología de Voz sobre IP, representa para el usuario una gran cantidad de ventajas y facilidades tecnológicas y económicas.

- Para las compañías, la migración de las PBX tradicionales a las IPBX, no solo representa una reducción significativa en los costos, sino que además permite el incluir una gran cantidad de nuevos servicios de valor añadido, los cuales representarían una optimización en el trabajo que desempeña el conmutador telefónico de la empresa.

- La VoIP es una solución viable, ya operativa a través de algunas redes privadas y se convertirá en un serio competidor de la telefonía tradicional. Sin embargo, sólo será competitiva cuando se hagan efectivos una mayor

calidad y un menor precio, y cuando los servicios y aplicaciones asociados sean mayores o iguales a los ofrecidos por la telefonía tradicional.

- Existe una falta de seguridad en el diseño y el desarrollo de VoIP, y los compradores no toman el tema de la seguridad en consideración. Las empresas se han enfocado casi exclusivamente en el precio, las características y el desempeño, a menudo liberando nuevos sistemas que están abiertos a insospechadas amenazas.

- Es una realidad el que los mismos tipos de ataques que afectan las redes de datos puedan afectar las redes VoIP, como consecuencia, el contenido de las comunicaciones VoIP es vulnerable a los ataques, el hackeo, las modificaciones, las intercepciones y los reenrutamientos. Además, el hecho de que las comunicaciones de voz y de datos se ejecuten en la misma infraestructura, un ataque al sistema VoIP podría hacer peligrar toda la disponibilidad de la red IP, lo que pondría en peligro la capacidad de la empresa para comunicarse por medio de voz y de datos.

- Se ha comprobado que con la aparición de la tecnología de Voz sobre IP se dio una proliferación del fraude (especialmente del “By pass”), ya que los defraudadores aprovecharon su uso debido a la reducción de costos que significaría el aplicarlo en el establecimiento del enlace internacional.

- Es un hecho que los sistemas fraudulentos, serán implementados siempre que permitan obtener beneficios económicos considerables, en tal virtud, mientras dicha condición se mantenga, esos sistemas ilegales serán estructurados con lo último en tecnología, procurando escapar a todo tipo de control y aprovechando cualquier brecha tecnológica o regulatoria permitida.

- Debido al gran crecimiento de las redes de telefonía móvil celular, en nuestro país su número de usuarios a superado notablemente al de las operadoras de telefonía fija, lo cual permite prever que el principal mercado

para la instalación de sistemas “By pass”, “Callback” o “Refilling”, es el de la telefonía celular.

- La ubicación de los sistemas de telecomunicaciones utilizados para cometer fraude usando líneas telefónicas celulares, es técnicamente compleja, cuanto más si se instalan en sitios urbanos donde existe gran cantidad de edificios, por esta razón, es necesario enfocar la estrategia de combate con otros recursos técnicos, que permitan evidenciar y sustentar ante las autoridades que con el uso de las líneas telefónicas celulares detectadas se está cometiendo un delito.

- El método para el control de fraude telefónico más comúnmente usado por las operadoras en el mundo, es el corte o suspensión de las líneas en las cuales se ha identificado un comportamiento inusual.

1.2.44 CONCLUSIONES SOBRE LA REGULACIÓN

- La tecnología IP desafía el modelo regulatorio que se ha desarrollado por más de un siglo, es inevitable el crecimiento y desarrollo de los servicios IP en razón de las ventajas que éstos proporcionan, la facilidad de convergencia que ofrecen, la integración de servicios de voz, datos, vídeo y funciones multimedia bajo una sola tecnología universal representa un reto para todos los actores del sector de las telecomunicaciones, es necesario tener una definición clara sobre la naturaleza de los servicios de voz sobre IP y sobre su clasificación antes de hacer cualquier ejercicio de regularización, toda norma que regula cierta actividad comercial debe tender a imitar las condiciones que ese mismo mercado va definiendo para su propia existencia, cualquier regulación podría crear distorsiones. Dado el incipiente mercado de voz sobre IP se concluye que la regulación debe esperar a que el mismo madure lo suficiente para que vaya definiendo sus propias limitaciones y alcances, y que en caso de ser regulado cualquier norma debe ser flexible y permisible para garantizar su desarrollo y

evolución, salvaguardando la libre competencia, los principios de no - discriminación, la protección de los derechos y garantías de los usuarios, así como la protección a las prestadoras actuales de telefonía convencional que han hecho una importante inversión en infraestructura.

- La regulación para Voz sobre IP en nuestro país, enuncia que la mencionada tecnología podrá ofrecerse exclusivamente para tráfico internacional saliente, más no para la realización de llamadas hacia destinos dentro del territorio nacional, así como se prohíbe la utilización de dispositivos de conmutación como gateways o similares que permitan conectar las comunicaciones de Voz sobre IP a las Redes Públicas de Telecomunicaciones del Ecuador, a no ser que se cuente con el permiso para su utilización. Cabe mencionar que a pesar de lo mencionado, la ley en el Ecuador da la libertad a las operadoras para que puedan prestar y usar los servicios que esta tecnología ofrece, esto siempre y cuando se cuente con el permiso respectivo y se lo siga tratando como un servicio de valor agregado y más no como un servicio de telefonía.

- En el Ecuador está condenado penalmente el prestar servicios de telecomunicaciones sin contar con una concesión, autorización, licencia o permiso.

- Se debe recordar que mediante el uso de herramientas tecnológicas adecuadas, se pueden encontrar fisuras regulatorias, que son aprovechadas por personas inescrupulosas para cometer todo tipo de fraudes.

1.2.45 CONCLUSIONES SOBRE ASPECTOS ECONÓMICOS

- La VoIP puede ser el punto de partida de grandes cambios en el mercado mundial de las telecomunicaciones, si finalmente se opta por considerar este servicio como de telefonía, las compañías de telefonía local y los

vendedores tradicionales de equipos de comunicación pueden ser los más perjudicados. Por el contrario, la nueva generación de vendedores de equipos, las compañías de TV por cable, los ISP y las compañías de telefonía de larga distancia podrían ser los más beneficiados.

- Un significativo y creciente problema actual para las organizaciones, es la pérdida de ingreso a través de deuda incobrable (es decir, el no pago por bienes y servicios recibidos). El uso de tecnologías avanzadas puede proporcionar un soporte invaluable a las políticas existentes de revisión dentro de la organización y en los chequeos de las entidades de crédito.

- El fraude es un problema de muchos millones de dólares que afecta a todas las organizaciones en mayor o menor grado. El mercado de las telecomunicaciones y los sectores financieros en particular brindan ricas cosechas, y son un blanco predilecto para los defraudadores.

- Debido a las grandes pérdidas anuales de ingreso, por incumplimiento de clientes en sus compromisos de pago y sobre todo por el fraude, las empresas están buscando soluciones que puedan ayudar a recuperar ingresos en forma eficaz y eficiente.

RECOMENDACIONES

- Se espera que el uso de VoIP aumente rápidamente en los próximos años, pero se observa que un gran porcentaje de las empresas no tienen planes específicos para garantizar la seguridad de la implementación de esta tecnología. Sin embargo, no es aconsejable ignorar el tema de la seguridad, ya que es muy probable que en el futuro los atacantes busquen cada vez más maneras de explotarla. Si una empresa decide adoptar el sistema VoIP, debe estar preparada para hacer frente a la falta de seguridad que actualmente trae aparejada la implementación de estos

sistemas. Si la empresa conoce y asume el compromiso de garantizar seguridad, puede disfrutar del ahorro de costos que ofrece la Voz sobre IP.

- Una regulación para telefonía IP deberá responder a ciertos principios, tales como:

    - Maximizar el bienestar de la sociedad;

    - No debe favorecer un tipo de tecnología sobre otro, es decir que la tecnología debe ser transparente para la regulación;

    - Beneficiar y proteger al consumidor;

    - Debe ofrecer apertura a la innovación y a la inversión; y,

    - Debe dimensionarse en función de las necesidades específicas y revisarse continuamente para ajustarse a dichos requerimientos.

- El combate del fraude, debe ser realizado de manera conjunta tanto por la operadora de telefonía, como por Organismo Técnico de Control; y, debe estar sustentado en una permanente coordinación dentro de los ámbitos técnico y judicial.

- Es indispensable que toda operadora de telefonía debidamente autorizada cuente con un sistema formal de control de tráfico internacional.

- Las operadoras de telefonía legalmente autorizadas deben efectuar constantemente pruebas de control de tráfico telefónico internacional, a fin de detectar si su red está siendo afectada por sistemas telefónicos fraudulentos.

- Por parte de las operadoras de telefonía fija y móvil, es necesario que se realice un monitoreo continuo de la facturación de sus usuarios , esto con

el fin de crear un patrón de comportamiento y de esta manera identificar comportamientos no usuales y evitar la pérdida de recursos para la empresa.

- Es recomendable intercambiar experiencias entre operadoras de telefonía, así como con el Organismo Técnico de Control, a fin de efectuar un combate eficaz a los sistemas ilegales de telecomunicaciones.

- Las líneas telefónicas celulares que se han utilizado para cursar tráfico telefónico ilegal, en su mayoría han sido adquiridas de manera legal, y el pago por el servicio prestado ha sido siempre oportuno ante las empresas operadoras, por esta razón, es recomendable que se implementen filtros dentro del proceso de asignación de cuentas conformadas por grupos de líneas telefónicas celulares.

- Las operadoras deben estar en proceso de continua investigación acerca de los nuevos tipos de fraude, para que de este modo la detección y el control sean más efectivos.

- Es recomendable que las operadoras de telefonía consideren iniciar una campaña publicitaria, advirtiendo a sus usuarios sobre estas prácticas no autorizadas y sus consecuencias.

- En cuanto a fraudes como el Vishing, es recomendable utilizar el escepticismo inteligente en cualquier relación en la que se pida al usuario que divulgue datos personales, por otro lado, siempre que se tenga que hablar con el banco se lo debe hacer a través de los números de teléfono oficiales, y no facilitar datos financieros a través de un correo electrónico ni de un teléfono que se facilitaría para realizar llamadas mediante VoIP.

REFERENCIAS BIBLIOGRÁFICAS Y DE INTERNET

Textos:

[1] FML SECURING BUSINESS, *Detección, Control y Gestión del Fraude en Telecomunicaciones*, 2005

[2] REVENUE ASSURANCE & FRAUD MANAGEMENT – Latin America, *Avalie e Implemente Estratégias para Combater as Fraudes em Redes Atuais e de Próxima Geraçao*, Septiembre 2007

[3] Universidad Distrital Francisco José De Caldas, *Técnicas de Detección, Prevención y Control del Fraude en Telecomunicaciones.*

[4] COMISIÓN DEL MERCADO DE LAS TELECOMUNICACIONES, *Consulta Pública sobre la provisión de servicios de Voz mediante tecnologías basadas en el Protocolo Internet (VoIP).*

Páginas WEB:

[5] Redes y Servicios, *Panorámica de las Telecomunicaciones - Conmutación,* http://trajano.us.es/~isabel/publicaciones/tema5.pdf

[6] Textos Científicos.com, *TCP/IP y el modelo OSI,* http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

[7] VoIP Foro.com, *Protocolos VoIP – H.323*, http://www.voipforo.com/H323/H323objetivo.php

[8] Wikipedia, *Voz sobre IP*, http://es.wikipedia.org/wiki/Voz_sobre_IP

[9] La Voz sobre IP , *Lo que se cuece en el mundo de la Telefonía por Internet*, http://itsp.typepad.com/voip/2007/01/porque_85_empre.html

[10] Monografías.com, *VoIP Voz sobre IP*, http://www.monografias.com/trabajos3/voip/voip.shtml

[11] VoIP Foro.com, *Diccionario*, http://www.voipforo.com/diccionario/A.php

[12] Wikipedia, *Modelo OSI*, http://es.wikipedia.org/wiki/Modelo_OSI

[13] Consejo Nacional de Telecomunicaciones, http://www.conatel.gov.ec

[14] Wikipedia, *Redes de Comunicaciones*, http://es.wikipedia.org/wiki/redesdecomunicaciones

[15] Así funciona, *Así funciona la Conversión Analógico Digital*, http://www.asifunciona.com/electronica/af_conv_ad/conv_ad_4.htm

[16] Monografías.com, *Descripción detallada sobre Voz sobre IP (VoIP)*, http://www.monografias.com/trabajos11/descripip/descripip.shtml

[17] RFC3261 - http://rfc.net/rfc3261.html

[18] RFC3508 - http://rfc.net/rfc3508.html

[19] RFC3362 - http://rfc.net/rfc3362.html

[20] RFC4566 - http://rfc.net/rfc4566.html

[21] L' alianza, *Haciendo llamadas Callback*, http://www.lalianxa.ekit.com/ekit/About/ Making PhonecardCalls

[22] Mercattel, *Servicio VoIP Callback*, http://www.mercattel.com/html/ad/293814/servicio-voip-callback.html

[23] INTECO, *1era Campaña contra el Robo de Identidad y el Fraude on-line*, http://www.nomasfraude.com/spain/sabias_que/amenazas/

[24] Alerta en línea, *Su red de seguridad – VoIP - Voz sobre protocolo de Internet* http://alertaenlinea.gov/telefonia_voip.html

[25] NORMAN, *"VISHING": la nueva tecnología reaviva las antiguas actividades delictivas*, http://www.norman.com/Virus/Security_Information/2006/41573/es

[26] Federal Communications Comission (FCC), http://www.fcc.gov

[27] Aplicaciones Web, *Servicio VoIP*, http://www.aplicacionesweb.net/servicio_voip.htm

[28] Universidad Politécnica de Catalunya – *Implementación de Servicios VoIP sobre Asterisk* - https://upcommons.upc.edu/pfc/bitstream/2099.1/3812/1/54629-1.pdf

[29] Wikipedia, *Asterisk,* http://es.wikipedia.org/wiki/Asterisk

[30] Asterisk, http://www.asterisk.org/

[31] Wikipedia, *MGCP*, http://es.wikipedia.org/wiki/MGCP

[32] Wikipedia, *IAX2*, http://es.wikipedia.org/wiki/IAX2

[33] Mundo Contact, *Soluciones en la Industria*, http://www.mundo-contact.com/ soluciones _ detalle. php?recordID=1284

[34] 3CX Software based PBX for Windows, - *Descubra las ventajas de una centralita telefónica VoIP*, http://www.3cx.es/

[35] SipXtreme, www.sipx.com

[36] Wikipedia, *Skype*, http://es.wikipedia.org/wiki/Skype

[37] Skype, *Skypeout,* www.skype.com/intl/es/products/skypeout/

[38] Skype, *Skypeln*, www.skype.com/intl/es/products/skypeln/

[39] ITSP, *Por que 85 empresas prefieren VoIP*, http://itsp.typepad.com/voip/2007/01/ porque _85 _empre.html

[40] AplicacionesVoIP,*Aplicaciones*,http://www.impra.com.mx/Aplicaciones/VoIP/VoIP.htm

[41] Aplicaciones Web, *Servicio VoIP*, http://www.aplicacionesweb.net/servicio_voip.htm

[42] Aplicaciones Web, http://www.aplicacionesweb.net/

[43] VoIP Now, *Open Source*, http://www.voipnow.org/2007/04/74_open_source_.html

[44] Jitel, http://enjambre.it.uc3m.es/~piscis/papers/jitel02.pdf

[45] VoIP Now, *Demo*, https://voipnowdemo.4psa.com/index.php

[46] Federal Communications Comission (FCC), *VoIP*, http://www.fcc.gov/voip/

[47] NPR in the matter of IP, *Enabled Services*, http://hraunfoss.fcc.gov/edocs_public/ attachmatch /FCC-04-28A1.pdf

[48] ITU, *ITU News*, http://www.itu.int/itunews/manager/display.asp?lang=es&year=2006 &issue = 05&ipage=development1&ext=html

[49] CallVantage, http://www.usa.att.com/callvantage/action/smp

[50] COFETEL, *Noticias*, http://www.cft.gob.mx/cofetel/html/secc_nva/PDF_noticias/cp_ VoIP. pdf