UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

LLAMADA EN ESPERA DE INTERNET

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JUAN ALBERTO LEYVA HUAYÁN

PROMOCIÓN

1997 - I

LIMA - PERÚ

2006

LLAMADA EN ESPERA DE INTERNET

Dedicatoria:

Un eterno agradecimiento a

mis padres y hermanos

SUMARIO

En el presente informe brindaremos los principales elementos para la implementación del servicio de "Llamada en Espera de Internet" también conocido como ICW (Internet Call Waiting) que está orientado a las personas que hacen uso de Internet. Esta solución dará al usuario la facilidad del manejo de una llamada entrante a su línea telefónica mientras esté conectado a Internet, manejo que se interpreta como las acciones de: Rechazo de la llamada, atender la llamada a través de Internet haciendo uso de la funcionalidad multimedia de su computadora, desviar la llamada a su casilla de voz, enviar su mensaje por e-mail o desviar la llamada a otro teléfono que puede ser de línea fija o celular.

Se muestra la interacción de la red de circuitos conmutados PSTN con una red de datos usando protocolos estándares en complemento con desarrollos que personalizan el servicio según las necesidades del operador.

ÍNDICE

PRÓLOGO 1

CAPÍTULO I
GENERALIDADES 2

CAPÍTULO II
PROTOCOLOS Y STANDARES

2.1 Recomendación H.323 3
2.1.1 Interfuncionamiento con terminales de otros tipos 4
2.1.2 Versiones H.323 4
2.1.3 Componentes 5
2.1.4 Zona H.323 7
2.1.5 Protocolos especificados por H.323 7
2.2 Protocolo Ligero de Acceso al Directorio - LDAP 11
2.2.1 Modelo de protocolo 11
2.2.2 Indicaciones de implementación 12
2.3 Protocolo de Transferencia de Hipertexto - HTTP/1.1 12
2.4 Plan internacional de numeración de telecomunicaciones públicas E.164 12

CAPÍTULO III
ASPECTOS DE DISEÑO

3.1 Aspectos a considerar en el Diseño del Sistema 14
3.1.1 Plataforma base 14
3.1.2 Datos de Usuario 15
3.1.3 Datos de Configuración 15
3.1.4 Comunicaciones 15
3.1.5 Servicios Web 16
3.1.6 Privacidad 16
3.1.7 Seguridad 17
3.1.8 Escalabilidad 18
3.1.9 Flexibilidad y confiabilidad 18

CAPÍTULO IV

COMPONENTES SOFTWARE

4.1	Aspectos Generales	20
4.2	Componentes Principales	20
4.2.1	Servicio ICW	20
4.2.2	Servicio de Datos de Sesión	20
4.2.3	Protocolo Internet de Acceso al Directorio - LDAP	21
4.2.4	Servicio Gatekeeper ICW H.323	21
4.2.5	Librería Interfase de Red - NPS	23
4.2.6	Módulo Software de Telefonía - NPS	23
4.2.7	Módulo Software Mail - NPS	23
4.2.8	Cliente ICW	24
4.2.9	Servicios Web de Administración y Soporte	24
4.2.10	Servicio de Logeo de Trazas de Depuración	25
4.2.11	Servicio de Logeo y Traceo	25
4.2.12	Librería de Datos de Sesión	25
4.2.13	Librería de Logeo y Traceo	25
4.2.14	Librería de Pooling	26
4.2.15	Librería de Autentificación	26
4.2.16	Librería de Codificación y Decodificación	26
4.2.17	Interfase de acceso al Directorio LDAP	26
4.3	Componentes Auxiliares	26
4.4	Conectividad entre equipos	27
4.5	Interacción de los componentes	27
4.5.1	Registro del cliente	27
4.5.2	Cliente actualiza datos	29
4.5.3	Cliente cambia de clave	32
4.5.4	Cliente termina su sesión	32
4.5.5	Heartbeat del cliente	34
4.5.6	NPS Consulta estado del cliente	35
4.5.7	NPS Consulta a Usuario por Acción	36
4.5.8	Requerimiento de Localización del Gatekeeper	38

CAPÍTULO V

FUNCIONAMIENTO

5.1 Configuración en las centrales de conmutación 39

5.2 Tratamiento de las llamadas 41

5.3 Implementación 49

5.4 Requerimientos para Operación y Mantenimiento 49

CAPÍTULO VI

EQUIPAMIENTO

6.1 Hardware Básico 50

6.1.1 Servidor de Directorio 50

6.1.2 Servidor ICW Windows 2003 50

6.1.3 H.323 Gatekeeper 50

6.1.4 H.323 Gateway 51

6.1.5 Cliente ICW 51

6.1.6 Servidor de Correo 51

6.2 Alternativas de Fabricantes 51

CONCLUSIONES 53

ANEXO

Especificaciones Técnicas del Gateway y Gatekeeper 55

BIBLIOGRAFÍA 62

CAPÍTULO I
GENERALIDADES

"Llamada en Espera de Internet" es un servicio orientado a los usuarios que hacen uso de Internet y deseen estar pendientes de las llamadas a su número telefónico. Parte del diseño se basa en un Nodo Proveedor de Servicios (donde suelen implementarse servicios de valor añadido) en la Red Pública de Telefonía Conmutada (Public Switched Telephone Network - PSTN). Esta alternativa brinda la ventaja de combinar el servicio de mensajería de voz, identificación y transferencia de llamadas.

La propuesta provee la notificación inmediata al suscriptor de las llamadas recibidas mediante un pop-up en la pantalla de su PC cuando está conectado a Internet y le permite determinar el tratamiento que desea darle a la llamada. El suscriptor puede identificar las llamadas entrantes, aceptar las llamadas que considere importantes y transferir o rechazar otras emitiendo una locución.

El suscriptor tiene las siguientes opciones:

Responder la llamada en su PC vía VoIP
Enviar la llamada a la casilla de mensajes
Enviar mensaje recibido de la llamada a una dirección de correo electrónica
Rechazar la llamada asociando una locución
Transferir la llamada a un número de teléfono alternativo
Desconectar la sesión de Internet y responder la llamada en el número original si estaba conectado vía acceso conmutado.

La arquitectura de la solución permite integrarnos fácilmente a la red telefónica. Dado que hay una salida a Internet, debe brindarse la adecuada seguridad para prevenir el acceso no autorizado a los elementos de la red, particularmente aquellos que contienen información del suscriptor e información comercial. La arquitectura es distribuida facilitando la ubicación de firewalls para asegurar la óptima protección de cada sistema.

CAPÍTULO II
PROTOCOLOS Y ESTÁNDARES

A continuación se describen brevemente los protocolos y estándares que se emplean en el presente informe haciendo énfasis en los puntos que se mencionan o se utilizan más adelante en el desarrollo del servicio.

2.1 Recomendación H.323

El estándar H.323 es una importante tecnología para la transmisión de comunicaciones en tiempo real de audio, video y data sobre redes de paquetes. Especifica los componentes, protocolos y procedimientos que proveen servicios de comunicación multimedia: audio, video y data en tiempo real sobre redes de paquetes.

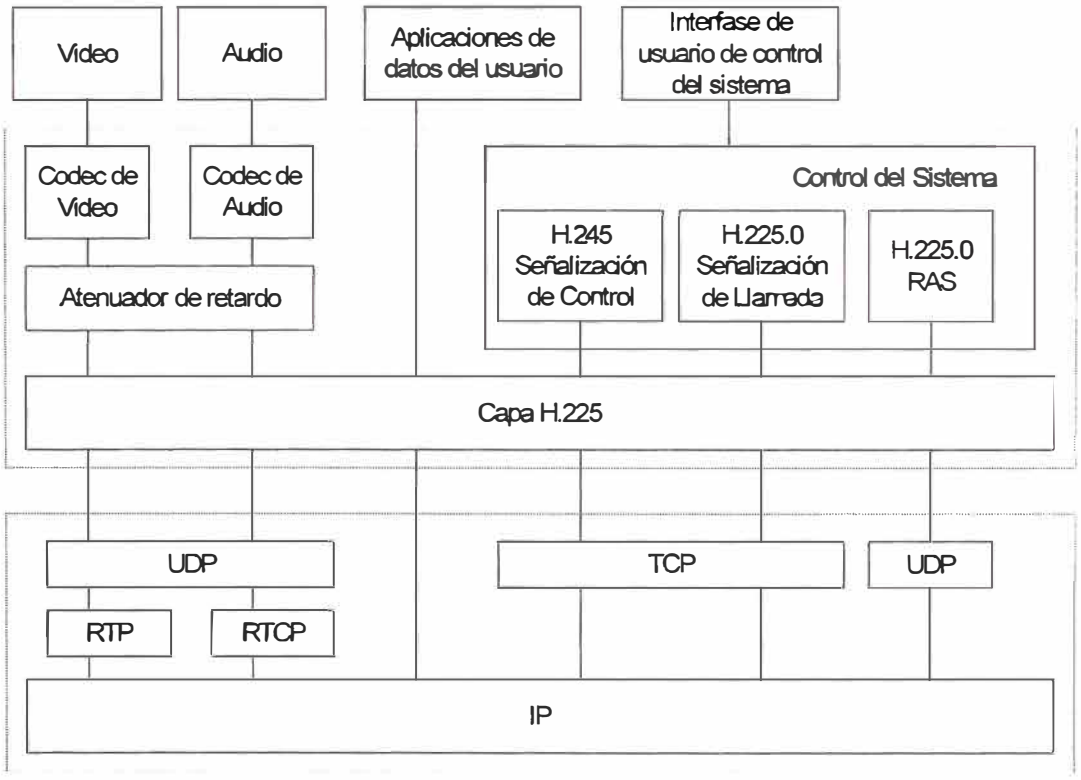


Fig. 2.1 PROTOCOLO H.323

En la fig. 2.1 se muestra la suit de protocolos H.323, que es parte de la familia de la recomendación ITU-T llamada H.32x que provee servicios de comunicación multimedia sobre una variedad de redes (1).

El término redes de paquetes incluye redes IP (incluyendo Internet) o Internet Packet Exchange (IPX), redes de área locales (LANs), redes empresariales, redes de área amplia (WANs). H.323 puede ser usada en una variedad de formas - solo audio (telefonía IP) que es la aplicada en el presente trabajo de "Llamada en Espera de Internet"; audio y video (videotelefonía); audio y datos; y audio video y datos. H.323 puede también ser usado en comunicaciones multimedia multipunto.

Por el gran número de servicios que brinda H.323, su aplicación se extiende a una variedad de áreas como las de consumo, negocios y entretenimiento.

2.1.1 Interfuncionamiento con terminales de otros tipos

El interfuncionamiento con otros terminales se llevará a cabo a través del gateway. Particularmente, el presente informe se enfoca en terminales vocales de la Red Pública de Telefonía Conmutada (PSTN). El gateway debe tener en cuenta las siguientes cuestiones:

Conversión de código de audio: de analógico a codificación G.711.

Conversión de trenes binarios: generación de la H.225.0.

Conversión de control (generación H.245).

Conversión de señalización de control de llamada.

Conversión de tono DTMF a/de mensaje *userInputIndication* H.245 y los tipos de cabida útil RTP.

2.1.2 Versiones H.323

El estándar H.323 está especificado por el grupo de estudio ITU-T. La versión 1 de la recomendación H.323 – sistemas de teléfono visual y equipamiento para LAN que no proveen una calidad de servicio garantizada (QoS) – fue aceptada en octubre de 1996. Fue, como su nombre sugiere, claramente orientada a comunicaciones multimedia en un entorno LAN.

La urgente necesidad de aplicaciones de voz sobre IP y telefonía IP sentó el camino para la revisión de la especificación H.323. La ausencia de un estándar para voz sobre IP resultó en productos que eran incompatibles. Con el desarrollo de voz sobre IP, surgieron nuevos requerimientos, tales como comunicaciones entre una PC-teléfono y un teléfono en una red tradicional de conmutación de circuitos, como la aplicación que se explicará más adelante. La versión 2 de H.323 – sistemas de comunicación multimedia

basada en paquetes – fue definida para adaptar estos requerimientos adicionales y fue aceptada en enero de 1998. Nuevas características han sido añadidas a este estándar dando como resultado las versiones 3 y 4, pero para el presente trabajo se recomienda usar la versión 2 dada su madurez alcanzada en el mercado.

2.1.3 Componentes

El estándar H.323 especifica 4 tipos de componentes, los cuales, cuando se interconectan, ofrecen servicios de comunicación multimedia punto-punto y punto-multipunto:

1. Terminales
2. Gateways
3. Gatekeepers
4. MCU (Unidades de Control Multipunto)

1. Terminales

Usados para comunicaciones multimedia bidireccionales en tiempo real, un terminal H.323 puede ser un computador personal o un dispositivo stand-alone, ejecutando el stack H.323 y aplicaciones multimedia. Soporta comunicaciones de audio y puede opcionalmente soportar comunicaciones de video y datos. Debido a que el servicio básico provisto por un terminal H.323 son comunicaciones de audio, un H.323 terminal tiene un papel clave en servicios de telefonía IP. El rol primario del H.323 es interactuar con otros terminales multimedia. Los terminales H.323 son compatibles con terminales H.324 en una red de circuitos conmutada y redes inalámbricas, con terminales H.310 en redes B-ISDN, con terminales H.320 en redes ISDN, con terminales H.321 en redes B-ISDN, y con terminales H.322 en LAN con QoS garantizadas. Los terminales H.323 pueden ser usados en conferencias multipunto.

2. Gateways

Un gateway conecta 2 redes disímiles. Un gateway H.323 provee conectividad entre una red H.323 y otra no-H.323. Por ejemplo, en la fig. 2.2, el gateway conecta y brinda comunicación entre un terminal H.323 y una red conmutada de circuitos (redes de circuitos conmutadas incluyen redes telefónicas conmutadas como la PSTN), que como se puede observar, es la funcionalidad que se utiliza en el servicio de "Llamada en Espera de Internet". La conectividad de redes disímiles se logra mediante la traducción de protocolos para *call setup* y *release*, convirtiendo formatos de media entre redes diferentes, y transfiriendo información entre las redes conectadas por el gateway. Sin embargo, no se requiere un gateway entre dos terminales sobre una red H.323.

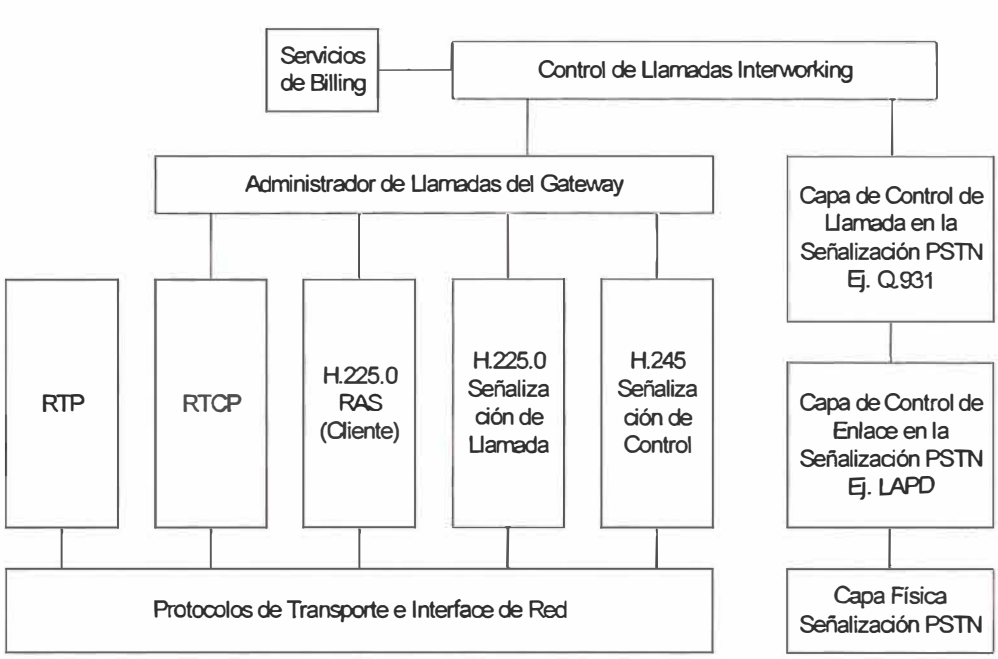


Fig. 2.2 STACK DE PROTOCOLOS DEL GATEWAY

3. Gatekeepers

Un Gatekeepers puede ser considerado el cerebro de una red H.323. Es el punto focal para llamadas entre una red H.323 (en la fig. 2.3 se muestran sus componentes).

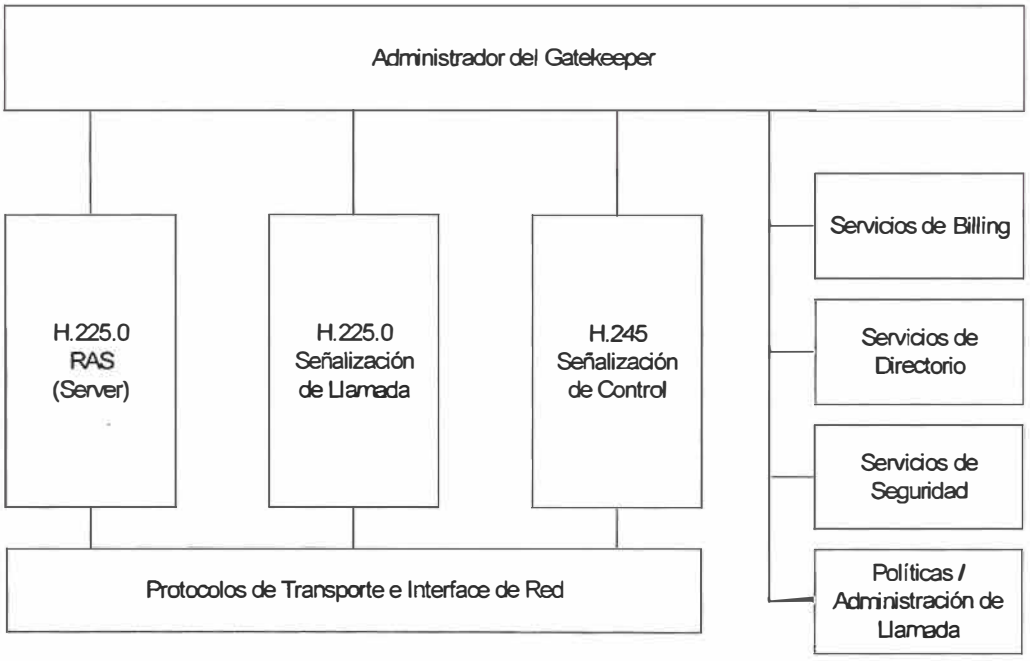


Fig. 2.3 COMPONENTES DEL GATEKEEPER

Aunque no siempre son requeridos, los gatekeepers ofrecen importantes servicios tales como direccionamiento, autorización y autentificación de terminales y gateways; manejo de ancho de banda; accounting; facturación y débito. Los gatekeepers pueden también brindar servicios de enrutamiento de llamada.

4. MCU (Unidades de Control Multipunto)

Los MCUs proveen soporte para conferencia de tres o más terminales H.323. Todos los terminales participantes en una conferencia establecen una conexión con el MCU. El MCU administra los recursos de conferencia, negocia entre terminales con el propósito de determinar el codificador/decodificador (CODEC) de audio y video a usar, y puede manipular el flujo de media. El servicio de "Llamada en Espera de Internet" por su arquitectura y definición no necesita de un MCU. Los gatekeepers, gateways, y MCUs son componentes lógicamente separados del estándar H.323 pero pueden ser implementados como un simple dispositivo físico. El servicio que se desarrolla en el presente informe no usará MCU.

2.1.4 Zona H.323

Una zona H.323 es un grupo de todos los terminales, gateways y MCUs administrados por un único gatekeeper. Una zona incluye al menos un terminal y puede incluir gateways y MCUs. Una zona puede ser independiente de una topología de red y puede ser compuesta de múltiples segmentos de red que son conectados usando routers u otros dispositivos.

2.1.5 Protocolos especificados por H.323

Los protocolos usados por H.323 se listan a continuación:

Real-time Transport Protocol (RTP)
Real-time Transport Control Protocol (RTCP)
H.225 Registro, admisión y status (RAS)
H.225 Señalización de llamada
H.245 Señalización de Control
CODECs de audio
CODECs de video

H.323 es independiente de la red de paquetes y los protocolos de transferencia sobre los que se ejecuta y no los especifica.

- **RTP (Real Time Transport Protocol)**

RTP esta diseñado para el soporte de tráfico en tiempo real, es decir, tráfico que necesita ser enviado y recibido en un período de tiempo muy pequeño. RTP es también un protocolo de encapsulación en el cual se transporta tráfico en tiempo real en el campo de datos del paquete RTP. El Real Time Transport Protocol es típicamente usado vía UDP.

- **RTCP (Real-Time Transport Control Protocol)**

RTCP es el complemento del RTP que proporciona servicios de control. La función primaria del RTCP es suministrar realimentación acerca de la calidad de los servicios que están entregando o recibiendo. Conceptualmente, un servidor puede ajustar la operación de su calidad de servicio sobre la base de la realimentación que recibe del cliente. Sin embargo la forma en la que se realizan estos ajustes no es definida por el RTCP.

- **H.225 Registro, Admisión y Status.**

La función de señalización RAS utiliza mensajes H.225.0 para llevar a cabo los procedimientos de registro, admisiones, cambios de ancho de banda, estado y desconexión entre puntos extremos y controladores de acceso. 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. En los entornos de red que no tienen un controlador de acceso, no se utiliza el canal de señalización RAS. En los entornos de red que sí tienen un controlador de acceso (una zona), el canal de señalización RAS se abre entre el punto extremo y el controlador de acceso. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

Localización de punto extremo

Un punto extremo o un controlador de acceso que tiene una dirección alias para un punto extremo y quisiera determinar su información de contacto puede emitir un mensaje de petición de localización (LRQ, *location request*). Este mensaje puede ser enviado al identificador TSAP de canal RAS del controlador de acceso específico o puede ser multidifundido como el mensaje GRQ a la dirección de multidifusión de descubrimiento conocida del controlador de acceso. El controlador de acceso con el que está registrado el punto extremo solicitado responderá con el mensaje de confirmación de localización (LCF, *location confirmation*) que contiene información de contacto del punto extremo o del controlador de acceso del punto extremo. La información de contacto incluirá las direcciones del canal de señalización de llamada y del canal RAS que han de utilizarse para alcanzar el punto extremo y opcionalmente información de destino adicional que

puede proporcionar información de marcación e información de extensión relativa al punto extremo solicitado.

Todos los controladores de acceso en los que no está registrado el punto extremo solicitado, devolverán un mensaje de rechazo de localización (LRJ, *location reject*) si han recibido el LRQ por el canal RAS. Los controladores de acceso en los que no está registrado el punto extremo no responderán a LRQ si reciben el LRQ en la dirección multidifusión de descubrimiento.

- H.225 Señalización de llamada

Se utiliza la señalización de llamada H.225.0 para establecer una conexión entre dos puntos extremos H.323. El canal de señalización de llamada es independiente del canal de RAS 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 de llamada. El canal de señalización de llamada se abre antes del establecimiento del canal H.245 y de cualquier otro canal lógico entre puntos extremos H.323. En los sistemas que no tienen un controlador de acceso, el canal de señalización de llamada se abre entre los dos puntos extremos que participan en la llamada. En los sistemas que sí tienen un controlador de acceso, el canal de señalización de llamada se abre entre el punto extremo y el controlador de acceso o entre los propios puntos extremos, según decida el controlador de acceso.

- Función de control H.245

La función de control H.245 se utiliza para llevar los mensajes de control de extremo a extremo que rigen el funcionamiento de la entidad H.323, incluyendo el intercambio de capacidades, apertura y cierre de canales lógicos, peticiones de modo preferido, mensajes de control de flujo e instrucciones e indicaciones generales.

La señalización H.245 se establece entre dos puntos extremos, un punto extremo y un MC o un punto extremo y un controlador de acceso. El punto extremo establecerá un canal de control H.245 en cada sentido para cada llamada en la que él participe. Este canal utilizará los mensajes y procedimientos de la Recomendación UIT-T H.245. Adviértase que un terminal, una MCU, un gateway o un controlador de acceso pueden soportar muchas llamadas y, por ello, muchos canales de control H.245. El canal de control H.245 se llevará por el canal lógico 0. Se considerará que el canal lógico 0 está permanentemente abierto desde el establecimiento del canal de control H.245 hasta la

terminación de este canal. Los procedimientos normales de apertura y cierre de canales lógicos no se aplicarán al canal de control H.245.

La Recomendación UIT-T H.245 especifica varias entidades de protocolo independientes que soportan señalización de punto extremo a punto extremo. Una entidad de protocolo se especifica por su sintaxis (mensajes), su semántica y un conjunto de procedimientos que establecen el intercambio de mensajes y la interacción con el usuario. Los puntos extremos H.323 soportarán la sintaxis, la semántica y los procedimientos de las siguientes entidades de protocolo:

Determinación principal/subordinado.
Intercambio de capacidades.
Señalización de canal lógico.
Señalización de canal lógico bidireccional
Señalización de cierre de canal lógico.
Petición de modo.
Determinación de retardo de ida y vuelta.
Señalización de bucle de mantenimiento.

Las instrucciones e indicaciones generales se elegirán del conjunto de mensajes contenido en la Rec. UIT-T H.245. Además, se pueden enviar otras instrucciones e indicaciones que hayan sido definidas específicamente para transferencia en banda dentro de trenes de vídeo, audio o datos.

Los mensajes H.245 se clasifican en cuatro categorías: de petición, respuesta, instrucción e indicación. Los mensajes de petición y respuesta son utilizados por las entidades de protocolo. Los mensajes de petición requieren una acción específica por parte del receptor, incluyendo una respuesta inmediata. Los mensajes de respuesta responden a una petición correspondiente. Los mensajes de instrucción requieren una acción específica, pero no una respuesta. Los mensajes de indicación son informativos solamente y no requieren ninguna acción o respuesta. Los terminales H.323 responderán a las instrucciones y peticiones H.245 y transmitirán indicaciones que reflejen el estado del terminal.

Los terminales H.323 deben ser capaces de descomponer analíticamente todos *mensajes de control de sistema multimedios (multimediaSystemControlMessage)* H.245. Luego, enviarán y recibirán todos los mensajes necesarios para implementar las funciones requeridas y aquellas funciones opcionales que soporte el terminal. Los terminales H.323 deben enviar el mensaje de *función no soportada*

(functionNotSupported) en respuesta a cualquier mensaje de petición, respuesta o instrucción no reconocida que reciban.

Se dispone de una indicación H.245, *indicación de entrada de usuario (userInputIndication)*, para el transporte de caracteres alfanuméricos de entrada del usuario desde un telemando o un teclado, equivalente a las señales multifrecuencia bitono (DTMF, *dual-tone multifrequency*) utilizadas en telefonía analógica o mensajes de números SBE (*Single Bit Extension*) de la Rec. UIT-T H.230. Esto se puede utilizar para operar manualmente equipos distantes tales como los sistemas de correo vocal o correo vídeo, los servicios de información por medio de un menú, etc. Los terminales H.323 soportarán la transmisión de los caracteres de entrada de usuario 0-9, "*" y "#". La transmisión de otros caracteres es opcional.

- CODECs de Audio

Codifican la señal de audio recibida del micrófono (terminal H.323 que transmite) y decodifica el código de audio recibido que es enviado al altavoz (terminal receptor). Dado que el audio es el mínimo servicio provisto por el estándar H.323, todos los terminales H.323 deben tener al menos un CODEC de audio como los siguientes:

Recomendación ITU-T G.711 (CODEC de audio a 64Kbps) mínimo requerido
Recomendación ITU-T G.722 (CODEC de audio a 64.56 y 48Kbps)
Recomendación ITU-T G.723.1 (CODEC de audio a 5.3 y 6.3Kbps)
Recomendación ITU-T G.728 (CODEC de audio a 16Kbps)
Recomendación ITU-T G.729 (CODEC de audio a 8Kbps)

2.2 Protocolo Ligero de Acceso al Directorio - LDAP

Es un protocolo estándar de red destinado a aplicaciones administrativas y de exploración que proveen acceso interactivo de lectura y escritura a directorios, en el segundo caso es necesaria autentificación segura. Los detalles se encuentran en la RFC 2251.

2.2.1 Modelo del Protocolo

El modelo general adoptado por este protocolo es uno de clientes ejecutando operaciones de protocolo contra un servidor. Es decir, un cliente transmite un protocolo petición describiendo la operación a ser ejecutada en el servidor, siendo éste último el responsable de la ejecución de las operaciones necesarias en el directorio. Completada las operaciones, el servidor retorna una respuesta conteniendo cualquier resultado o errores al cliente solicitante.

Manteniendo la meta inicial de reducir costos asociados con el uso del directorio, es un objetivo de este protocolo el minimizar la complejidad en el lado del cliente, facilitando de esta manera un amplio despliegue de aplicaciones capaces de usar el Directorio.

2.2.2 Indicaciones de Implementación

Algunas indicaciones importantes son:

Implementaciones Servidor

El servidor debe ser capaz de reconocer todos los nombres de tipo de atributo mandatorios e implementar la sintaxis especificada en la RFC 2251. Los servidores pueden reconocer nombres de tipo de atributo adicionales.

Implementaciones Cliente

Deben evitar lazos entre servidores, no deben contactar repetidamente un servidor por el mismo pedido con el mismo nombre de entrada destino, alcance y filtro. En la ausencia de previos acuerdos entre los servidores, los clientes no deben asumir que los servidores soportan algún esquema particular diferente a los referenciados en la RFC2251. Diferentes esquemas pueden tener diferentes tipos de atributos con los mismos nombres.

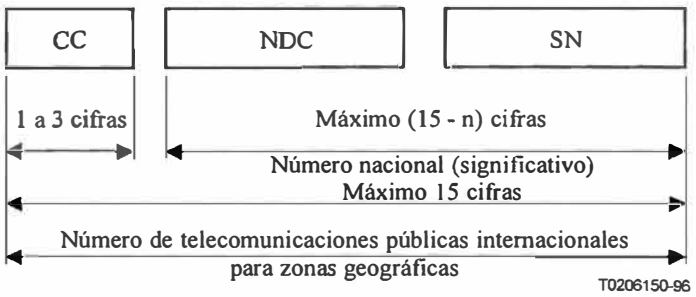
2.3 Protocolo de Transferencia de Hipertexto - HTTP/1.1

HTTP es un protocolo de nivel de aplicación para sistemas de información distribuido, cooperativo, hipermedia cuyo uso se inició desde 1990. Esta versión aparece como respuesta a ciertos cambios que se dan necesariamente con el avance y el desarrollo (2), ya que la versión previa no toma en suficiente consideración los efectos de proxies jerárquicos, caching, la necesidad de conexiones persistentes, o host virtuales. Además, la proliferación de aplicaciones implementadas de forma incompleta y auto denominadas “HTTP/1.0” han necesitado un cambio de la versión del protocolo dado que aplicaciones comunicándose deben conocer las verdaderas capacidades una de la otra. Los detalles se encuentran en la RFC 2616.

2.4 Plan internacional de numeración de telecomunicaciones públicas E.164

Un número E.164 indica unívocamente un punto de terminación en la red pública, ya que contiene la información necesaria para encaminar una llamada a este punto de terminación. A fin de lograr la comunicación entre una llamada realizada a través de la red pública de telefonía y un usuario conectado a Internet, será necesaria una traducción del número llamado E.164 a su par correspondiente registrado en la red de datos.

La Recomendación UIT-T E.164 define los números E.164 de la forma siguiente para las distintas zonas geográficas (fig. 2.4):



CC Indicativo de país para zonas geográficas
n Indicativo nacional de destino (opcional)
NDC Número de abonado
SN Número de cifras del indicativo de país

NOTA – Los prefijos nacional e internacional no forman parte del número de telecomunicaciones públicas internacionales para zonas geográficas.

Fig. 2.4 Recomendación UIT-T E.164

CAPÍTULO III
ASPECTOS DE DISEÑO

3.1 Aspectos a considerar en el diseño del sistema

Lo que se tratará a continuación son los aspectos que se deben tomar en cuenta para el diseño de este servicio. Estos conceptos e ideas permitirán ensamblar el conjunto tal como se presenta en el capítulo 4. Con respecto a la red PSTN, las características más resaltantes se indican en el siguiente capítulo.

3.1.1 Plataforma base

Considerando que el servicio va a ser ofrecido por un operador de telefonía, este debe contar con un buen nivel de confiabilidad. Para tal efecto sus componentes deben ser en lo posible de características superiores.

De las opciones disponibles en el mercado, una plataforma que permite esta implementación es la familia de sistemas operativos Windows Server 2003 (3). Se recomienda separar en servidores independientes ciertas funcionalidades especializadas como el almacenamiento de datos de usuario (Servidor de directorio LDAP visto mas adelante), el Servidor de Correo y los componentes propios del servicio.

La arquitectura será basada en componentes los cuales deberán ser implementados como servicios, aplicaciones o librerías nativas de Windows (Windows 2003 compatible dynamic-link libraries).

Los principales módulos deberán tener contadores de desempeño, para un monitoreo de rendimiento. Asimismo, deberán logear mensajes adecuadamente al Event Log del Windows 2003, tales como mensajes de error, preventivos, informativos, de inicio, etc.

Todo lo referente al logeo y traceo detallado para obtención de trazas, no será almacenada en el Event Log, esta información que normalmente sirve para análisis especializado, usará una librería interfase especial de logeo y traceo la cual interactuará con el servicio respectivo. Toda la información recibida deberá ser almacenada preferentemente en un archivo binario (mayor velocidad) el cual pueda decodificarse posteriormente con utilitarios desarrollados para este propósito. El logeo y traceo debe ser además, configurable por componente de tal manera que pueda habilitarse,

deshabilitarse o graduar el nivel de captura según los requerimientos del momento.

Los componentes requerirán también acceder al registro de Windows para almacenar cierta configuración específica para sus componentes, esta actividad se puede realizar utilizando el API de estándar Microsoft.

3.1.2 Datos de usuario

Es necesario contar con un almacenamiento seguro de la información de los datos de los clientes, así como un rápido acceso a los mismos, para ello se empleará un servidor de directorio LDAP.

LDAP (Lighweight Directory Access Protocol - Protocolo de Acceso Ligero a Directorio) es un protocolo de acceso unificado a un conjunto de información sobre una red, no es una base de datos en absoluto. Asimismo, el directorio de información LDAP es un tipo de base de datos optimizado para realizar consultas, pero no es una base de datos relacional.

Es en sí un servicio de directorio ordenado y distribuido que permite buscar información diversa en un entorno de red. Está ampliamente aceptado en el mercado y se encuentra disponible en una variedad de implementaciones. Considerando la plataforma base, el Directorio Activo de Windows se presenta como una buena alternativa (4).

Para el acceso al directorio se puede utilizar el API de Microsoft ADSI o implementar una interfase especial de acceso al Directorio Activo de Windows (LDAP).

3.1.3 Datos de Configuración

Los datos de configuración del sistema pueden ir centralizados en el directorio LDAP, otra alternativa es el registro del Servidor Windows 2003. Según las facilidades del desarrollo del sistema se optará por uno u otro.

La administración de dichos datos deberá realizarse vía Web, empleando un módulo de administración y los servicios Web disponibles.

3.1.4 Comunicaciones

Las comunicaciones entre todos los hosts que componen la estructura del servicio, independiente del protocolo, serán sobre TCP/IP.

El Servidor Windows 2003 ICW interactuará con los diferentes equipos y componentes software como se indica a continuación:

Gatekeeper Cisco: Usando el "Cisco Gatekeeper Transaction Protocol" (5), el cual esta basado en el protocolo H.225 RAS (Registration, Admisión and Status), el cual forma parte de la suite H.323 tal como se describe en un capítulo previo.

Cliente ICW en PC del usuario: Usando una secuencia de mensajes que se denominará de aquí en adelante Protocolo ICW.

Nodo proveedor de servicios (NPS, parte de datos): Usando el Protocolo ICW.

Directory Server: Usando el protocolo LDAP (Lightweight Directory Access Protocol).

PC del Administrador: Usando HTTP/HTTPS para una administración basada en Web.

3.1.5 Servicios Web

Entre las capacidades del Windows 2003 Server esta el IIS (Internet Information Service), el cual tiene importantes ventajas como capacidades de logeo y traceo, nivel de seguridad razonable y una característica de auditoría de la metabase, por lo que se usará en todos los servicios Web. También se usará otra de las destacadas características de IIS, las ASP (Windows Active Server Pages), un entorno de secuencias de comandos del lado del servidor que permite crear aplicaciones de Servidor Web dinámicas e interactivas, empleándose VBScript para toda escritura de scripts.

Las listas de control de acceso (Access Control Lists) son una buena alternativa de seguridad para restringir el acceso a la administración y soporte de páginas web.

3.1.6 Privacidad

a. Enfoque General

Algunas consideraciones importantes para la comunicación entre los componentes de hardware de sistema son:

De preferencia encriptar los datos trasmitidos a través de Internet con la finalidad de asegurar la privacidad de la información.

Los datos trasmitidos entre los siguientes componentes: Servidor ICW Windows 2003, Servidor LDAP, Nodo PS y el Gatekeeper H.323 utilizarán las medidas de seguridad provista por los sistemas operativos y APIs de esas plataformas. No será necesario considerar ninguna medida de seguridad adicional bajo el supuesto de que los sistemas protegidas por el firewall se consideran confiables

b. Privacidad entre equipos

Para la privacidad de los datos trasmitidos entre el cliente ICW y el servidor ICW Windows 2003 se recomienda emplear Secure Sockets Layer (SSL), por lo que su uso deberá ser una opción configurable.

La privacidad de los datos transmitidos entre una computadora del administrador y el servidor ICW Windows 2003 será implementado usando el soporte para HTTP sobre SSL provisto por IIS.

La privacidad de los datos transmitidos entre el servidor ICW Windows 2003 y el servidor LDAP no será asegurada considerando que esta en la red interna protegida por el firewall.

La privacidad de los datos transmitidos entre el servidor ICW Windows 2003 y el gatekeeper H.323 será dependiente del GKTMP (Cisco Gatekeeper Transaction Message Protocol)

c. Privacidad entre componentes

No se implementarán medidas específicas que aseguren privacidad entre componentes del Servidor ICW Windows 2003. La privacidad será asegurada por el firewall, previniendo de conexiones maliciosas a los puertos TCP implementados por los componentes del servidor ICW Windows 2003, y por el proceso del logeo al Server 2003 previniendo la instalación no autorizada de programas que puedan intentar usar las APIs como por ejemplo las interfases COM expuestas por los componentes de servidor ICW Windows 2003.

3.1.7 Seguridad

La seguridad es también una preocupación constante en toda red, normalmente debe lograrse a tres niveles: red, host y aplicación. Un atacante puede aprovechar un punto débil de cualquiera de estos niveles, la idea es reducir las posibilidades de que se produzca un ataque. En los párrafos siguientes se indicaran algunas consideraciones básicas.

La seguridad de las comunicaciones entre el servidor ICW Windows 2003 y sistemas externos deberá ser de la siguiente manera:

A las PC clientes ICW: usuario y contraseña alfanuméricos

Al Gatekeeper H.323: la provista por Cisco (Cisco Gatekeeper API)

Al servidor de Directorio LDAP: usuario y contraseña alfanuméricos.

Al servidor de Correo: usuario y contraseña alfanuméricos.

A otros elementos de dentro de la red de área local de los servidores Windows 2003: Aquella recomendada por el operador según sus políticas.

La seguridad de las comunicaciones entre el nodo Proveedor de Servicios (NPS) y

sistemas externos será de la siguiente manera:

Al servidor Windows 2003: ninguna medida de seguridad especial.

A otros elementos dentro de la red de área local del NPS: Aquella recomendada por el operador según sus políticas.

El acceso a la interfase de usuario de los servicios de Administración Web requerirá un usuario y contraseña válidos de Windows 2003. Para tal efecto, las ACL (Windows 2003 Access Control List) podrán ser usadas para restringir el acceso. Los que accederán podrían ser definidos como un grupo especialmente configurado para este propósito.

3.1.8 Escalabilidad

En general, se podría definir como la capacidad de un sistema de cambiar su tamaño o configuración para adaptarse a las circunstancias cambiantes, en el presente caso, a un número de usuarios cada vez mayor, sin perder calidad en los servicios brindados.

La arquitectura de este servicio es en principio simple, no más de un elemento de red a la vez. Para conseguir escalabilidad, los protocolos de comunicación se volverán más complejos para lograr una adecuada interacción, lo que a su vez se reflejara en mayores costos. Esta alternativa de desarrollo deberá ser evaluada en base a los requerimientos del operador, estimación de usuarios, montos de inversión, etc.

Los elementos de red que pueden variar para este fin son:

El NPS, dependiendo de la configuración de red provista por el operador.

El servidor Windows 2003, dependiendo principalmente de las proyecciones de usuarios.

El servidor LDAP, según las proyecciones de usuarios.

El Gatekeeper H.323

3.1.9 Flexibilidad y Confiabilidad

De la forma simple, la confiabilidad del sistema depende de la redundancia hardware más que software. Si se presentara alguna falla de software, algún bug, etc., que no sea el NPS, el sistema trabajaría parcialmente. De fallar el NPS, definitivamente no funcionaria este servicio.

Siendo el Servidor Windows 2003 y el Servidor de Directorio LDAP los dos elementos de la red más importantes para este servicio, es importante el que los desarrollos de software así como los protocolos de comunicación tengan la posibilidad de soportarlos, lo que contribuiría también a la escalabilidad del sistema.

Volviendo a la forma simple, si fallara:

El Servidor ICW Windows 2003: Solo estará disponible el desvío a la casilla de voz para no descartar la llamada.

El Servidor de Correo: No podrán enviarse vía e-mail los mensajes recibidos.

El Servicio ICW: Solo estará disponible el desvío a la casilla de voz para no descartar la llamada.

Servicio H.323 Gatekeeper ICW: El gateway no podrá conectar más ninguna llamada por VoIP.

Servicios de Directorio: Solo estará disponible el desvío a la casilla de voz para no descartar la llamada.

Nodo Proveedor de Servicios (NPS): La falla del Nodo Proveedor de Servicios implica que todos los abonados perderán el servicio de Llamada en Espera de Internet.

H.323 Gatekeeper: La falla del H.323 Gatekeeper se reflejará en el H.323 Gateway, este ya no conseguirá conectar a los clientes llamantes al módulo de VoIP porque no podrá obtener la dirección IP de la PC cliente ICW.

CAPÍTULO IV
COMPONENTES SOFTWARE

4.1 Aspectos Generales

De las consideraciones ya vistas en capítulos anteriores, ahora se verá como es que estas participan como un todo. Más adelante en la fig. 4.1 se muestra un diagrama que reúne todas estas partes. (6)(7)

4.2 Componentes Principales

4.2.1 Servicio ICW

Este importante componente debe ser desarrollado como un servicio Windows 2003-compliant (compatible) según lo indicado en el capítulo 3. Debe ofrecer las siguientes funciones:

a. Proveer un puerto TCP al que el software cliente ICW pueda conectarse, enviar y recibir mensajes del protocolo ICW. Asimismo, deberá soportar conexiones seguras SSL.
b. Ser punto de transferencia y control de estado de mensajes entre el cliente ICW y otros componentes del servicio tales como el LDAP y el Nodo Proveedor de Servicios.
c. Este componente interactuará con el Servicio de Datos de Sesión para el adecuado mantenimiento de la sesión de los clientes ICW que se encuentren activos.

4.2.2 Servicio de Datos de Sesión

Este servicio es el encargado de la administración de las sesiones establecidas en el Servidor ICW Windows 2003. Se usará para hacer un seguimiento a todos los usuarios que se encuentren en línea, almacenando para cada uno de ellos lo siguiente:

a. ID de sesión
b. Dirección IP
c. Puerto TCP
d. Número telefónico

Interactuará con la Librería Interfase de Datos Sesión para la administración de la sesión de los clientes ICW registrados, atendiendo por medio de ella, los requerimientos del Servicio Gatekeeper ICW H.323, Servicio ICW y servicios de Administración Web. Esta última con la finalidad atender consultas y generar de reportes estadísticos. Debe ejecutarse como un servicio Windows 2003-compliant.

4.2.3 Protocolo Internet de Acceso al Directorio - LDAP

Todos los datos del usuario serán almacenados en un directorio LDAP-compliant, como opción escogida esta el Active Directory de Microsoft. Esta elección se debe a que el Active Directory es un servicio de directorios escalable creado a partir de tecnologías de Internet estándar e integrados al sistema operativo Windows 2003. Entre las características más importantes es que proporciona acceso mediante LDAP y admite sistemas de autenticación flexibles y seguros.

Este componente interactuará con la Librería Interfase de autentificación y el Servicio ICW.

4.2.4 Servicio Gatekeeper ICW H.323

Debe ser desarrollado como un Windows 2003-compliant service según lo indicado en el capítulo 3. Debe ofrecer las siguientes funciones:

a. Ejecutar requerimientos de localización del Gatekeeper (dirección IP del cliente) utilizando el Gatekeeper Transaction Message Protocol - GKMTP.
b. Registrarse con el H.323 Gatekeeper al momento de arranque.

Este componente interactuará con el Servicio de Datos de Sesión para ejecutar la resolución de direcciones de E.164 a IP. Como se vio anteriormente, el Servicio de Datos de Sesión almacena esta información para todos los clientes que se encuentren en línea.

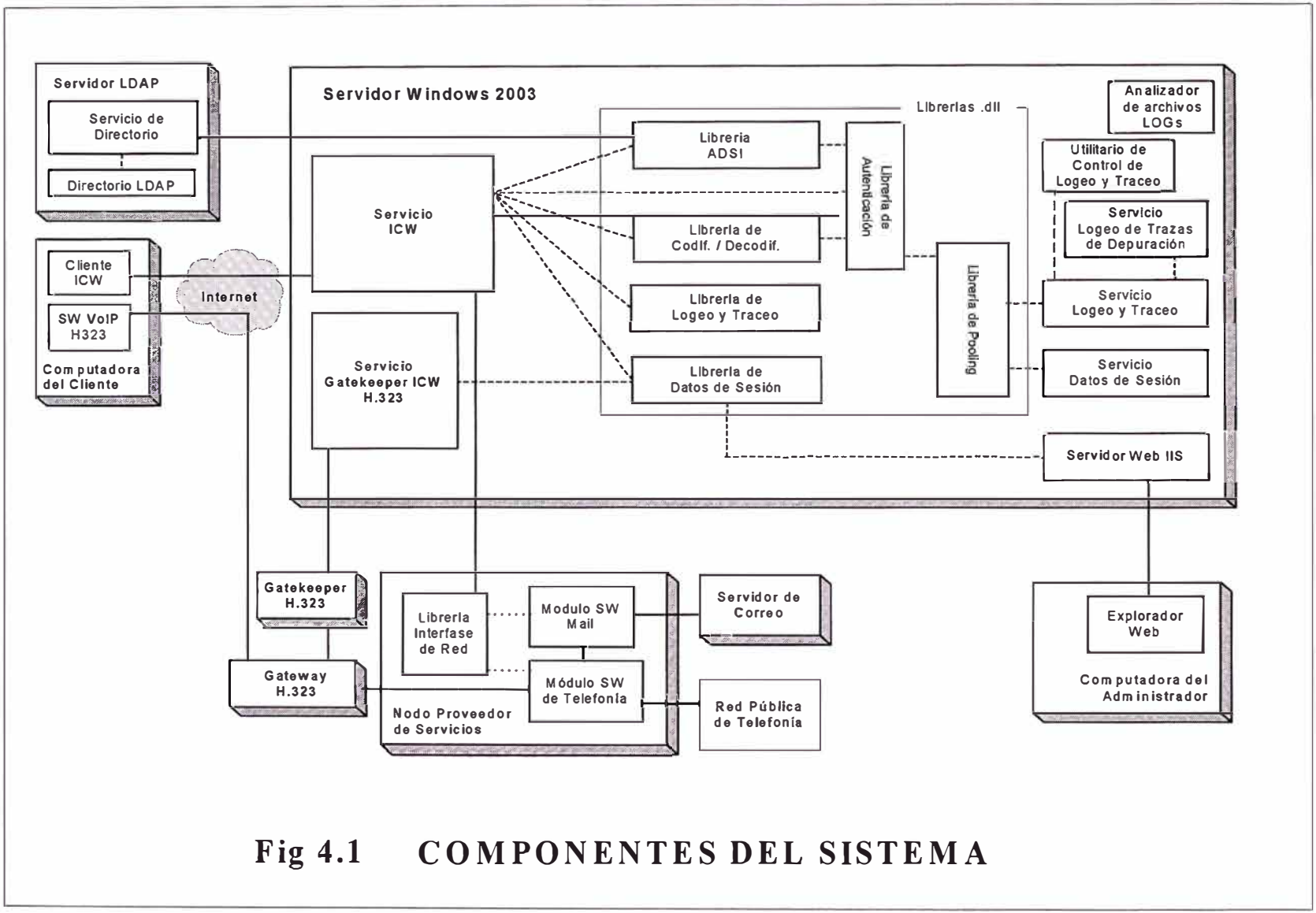


Fig 4.1 COMPONENTES DEL SISTEMA

4.2.5 Librería Interfase de Red - NPS

Este componente se encuentra en el Nodo Proveedor de Servicios y debe ser capaz de interactuar con el Servicio ICW. El propósito de este componente es:

a. Proporcionar un puerto TCP al cual el servicio ICW pueda conectarse.
b. Realizar las notificaciones de llamadas entrantes mientras el llamante se mantiene en espera.
c. Mantener el estado de notificación de llamadas entrantes iniciados por el Módulo Software de Telefonía.
d. Actualizar el estado de notificación de llamadas entrantes con información recibida por el Servicio ICW.
e. Reportar el estado de notificación de llamadas entrantes e información asociada de retorno al Módulo Software de Telefonía.

Este componente no recibirá ni procesará llamadas entrantes, tampoco se conectará directamente a la red telefónica.

4.2.6 Módulo Software de Telefonía - NPS

El propósito de este componente es:

a. Interactuar directamente con la PSTN, recibiendo la llamada desviada por la central local a la que pertenece el cliente ICW.
b. Dar una locución informativa al usuario sobre lo que esta ocurriendo con la llamada. Por ejemplo "El número que usted ha marcado se encuentra conectado a Internet, por favor espere un momento mientras conectamos su llamada".
c. De acuerdo a la información recibida por la Librería Interfase de Red, el Módulo Software de Telefonía procederá al adecuado tratamiento de la misma, como llamar al nuevo destino y cerrar el lazo. Éste nuevo destino puede ser el Gateway (VoIP) u otro número telefónico de la red de la red fija o móvil.
d. Si este NPS se encarga también de proporcionar el servicio de mensajería de voz, entonces solo habrá que hacer una transferencia interna al módulo software correspondiente. Si este no es el caso, se procederá como lo indica el ítem anterior, realizando la llamada a la Plataforma que administra las casillas de voz.

4.2.7 Módulo Software Mail - NPS

El propósito de este componente es:

a. Interactuar con el servidor de correo.
b. Dar una locución informativa al usuario sobre lo que esta ocurriendo con la llamada. Por ejemplo "Su mensaje será enviado al correo electrónico del

numero…." o simplemente dar una locución igual al de la casilla de voz. El operador definirá este punto.

c. Atender la llamada desviada por la central local a la que pertenece el cliente ICW, grabar el mensaje utilizando algún tipo de compresión estándar el cual será anexado al e-mail.
d. De acuerdo a la información recibida por la Librería Interfase de Red, generará el correo al destino especificado.

4.2.8 Cliente ICW

El cliente ICW reside en la PC del abonado. Cuando la PC del abonado está conectada a Internet, puede habilitar el cliente ICW lo que se traduce en el cliente conectándose y registrándose con el servicio ICW. El cliente ICW puede entonces ser utilizado para cambiar las preferencias del abonado (por ejemplo su correo electrónico o la especificación de desvío a casilla y/o correo electrónico, etc.).

Configurado adecuadamente el cliente ICW avisará al usuario acerca de llamadas entrantes (notificadas por el servicio ICW) presentándole una lista de posibles acciones como por ejemplo "Desconectar y tomar la llamada" (un pop-up y una señal audible serían los avisos mas convenientes). El cliente ICW notificará al servicio ICW de la acción del abonado, o después de un periodo de tiempo límite configurable, enviar un mensaje notificando que el abonado falló en responder a la notificación de llamada.

El cliente ICW deberá ser capaz de comunicarse con el Servicio ICW usando el protocolo ICW sobre SSL (Secure Sockets Layer). Esta facilidad debe estar disponible aunque dependerá del operador definir si se usa SSL o una conexión TCP convencional (estas opciones son mutuamente exclusivas). El sistema deberá proveer la opción de ser configurado para ejecutarse con o sin SSL.

4.2.9 Servicios Web de Administración y Soporte

El objetivo de este componente es permitir al operador las siguientes funciones:

a. Consultar, modificar, crear o eliminar usuarios.
b. Generar reporte detallando la actividad de los usuarios.
c. Generar un reporte que entregue detalles actuales de algún usuario.
d. Proveer un método para realizar cargas masivas de usuarios, para lo cual se deberán proporcionar por cada uno de ellos los siguientes datos:
    - Nombre de usuario
    - Número telefónico

- Acción por defecto (normalmente casilla de voz o e-mail en caso este disponible la cuenta de correo)
- E-mail, etc.

e. Consultar y realizar modificaciones a los parámetros de configuración del sistema.

Este componente deberá interactuar con el directorio LDAP con el fin de inscribir nuevos usuarios, realizar búsquedas o consultas de usuarios ya existentes, modificar o eliminar registros de usuarios. También deberá interactuar con la Librería Interfase de Datos de Sesión para obtener estadísticas de los usuarios que se encuentren usando el sistema con el propósito de generación de reportes. El acceso los servicios Web será usando el Internet Explorer debido a la autenticación propietaria empleada.

4.2.10 Servicio de Logeo de Trazas de Depuración

Tiene como finalidad registrar las trazas de depuración enviadas por el Servicio de Logeo y Traceo, normalmente un archivo intermedio binario para posterior proceso (optimiza el uso de recursos al escribir y almacenar los datos). Estos eventos son entregados por los diferentes módulos usando la Librería Interfase de Logeo y Traceo, y encoladas al Servicio de Logeo y Traceo. Debe desarrollarse como un servicio Windows 2003-compliant.

4.2.11 Servicio de Logeo y Traceo

Este servicio registra los eventos de auditoria, facturación y trazas de depuración encolados para registrarse. Se utiliza para monitorear las tres colas de eventos mencionados y enviarlos a sus respectivos subsistemas de registro mencionadas. Un aspecto importante a considerar es que la cola de facturación no debe tener la opción de deshabilitarse además de contar con prioridad sobre las demás. Debe desarrollarse como un servicio Windows 2003-compliant.

4.2.12 Librería de Datos de Sesión

Se utilizará para proveer acceso al Servicio de Datos de Sesión y Servicios de Administración Web. Deberá ser desarrollado como una librería de enlace dinámica (DLL) Windows 2003-compliant.

4.2.13 Librería de Logeo y Traceo

El propósito de esta librería es proporcionar a los componentes una interfase tanto al Servicio de Logeo y Traceo como al Servicio de Logeo de Trazas de Depuración.

Deberá ser desarrollado como una librería de enlace dinámica (DLL) Windows 2003-compliant.

4.2.14 Librería de Pooling

Este componente tiene como propósito proporcionar un mecanismo de pooling a las conexiones TCP. Considerando que una de las tareas más demandantes de recursos es la creación de la conexión inicial, proporcionará mejor capacidad de respuesta al sistema. Deberá ser desarrollado como una librería de enlace dinámica (DLL) Windows 2003-compliant.

4.2.15 Librería de Autentificación

La función de este componente es proveer un mecanismo para autenticar los intentos de registro de los clientes ICW contra los datos que se tienen en el Directorio LDAP. Deberá ser desarrollado como una librería de enlace dinámica (DLL) Windows 2003-compliant.

4.2.16 Librería de Codificación y Decodificación

Este componente tiene como finalidad proveer seguridad en el uso de las contraseñas de los clientes mediante su cifrado y descifrado, guardándose encriptada en el directorio LDAP. Deberá ser desarrollado como una librería de enlace dinámica (DLL) Windows 2003-compliant.

4.2.17 Interfase para el acceso al Directorio LDAP

Este componente tiene como objetivo proveer acceso a los datos de los usuarios almacenados en directorio LDAP. Se empleará el API de Microsoft ADSI.

4.3 Componentes Auxiliares

a. Utilitario de Control de Logeo y Traceo

Proporcionará al administrador el control del logeo y traceo de los componentes del sistema, permitiendo modificar las opciones de captura de información según los requerimientos. Deberá ser desarrollado como una aplicación ejecutable Windows 2003-compliant.

b. Analizador de archivos LOG

El propósito de este componente es permitir al administrador extraer y revisar los archivos LOGs producidos por el Servicio de Logeo de Trazas de Depuración,

interpretando los datos almacenados en los archivos binarios centralizados. Deberá ser desarrollado como una aplicación ejecutable Windows 2003-compliant.

4.4 Conectividad entre equipos

A continuación se indicará en que componente del sistema deberá estar la responsabilidad por la iniciación de la conexión entre equipos físicamente separados y mas adelante se verá gráficamente con más detalle cada caso.

a. Cliente ICW - Servicio ICW

El Cliente ICW iniciará de una conexión TCP con el Servicio ICW con propósitos de enviar los mensajes de actualización y registro de las preferencias de usuario. El Servicio ICW iniciará de una conexión TCP con el Cliente ICW para notificar a los usuarios sobre las llamadas en espera.

b. Servicio ICW - Librería Interfase de Red (NPS)

Al arranque, el Servicio ICW iniciará la creación de conexiones TCP con Librería Interfase de Red. La Librería Interfase de Red iniciará la conexión TCP cuando requiera consultar el estado de un cliente conectado o la acción a ejecutar con la llamada que mantiene en espera.

c. Servicio H.323 Gatekeeper - H.323 Gatekeeper

Al arranque, el Servicio H.323 Gatekeeper iniciará conexión con el H.323 Gatekeeper con propósitos de registro.

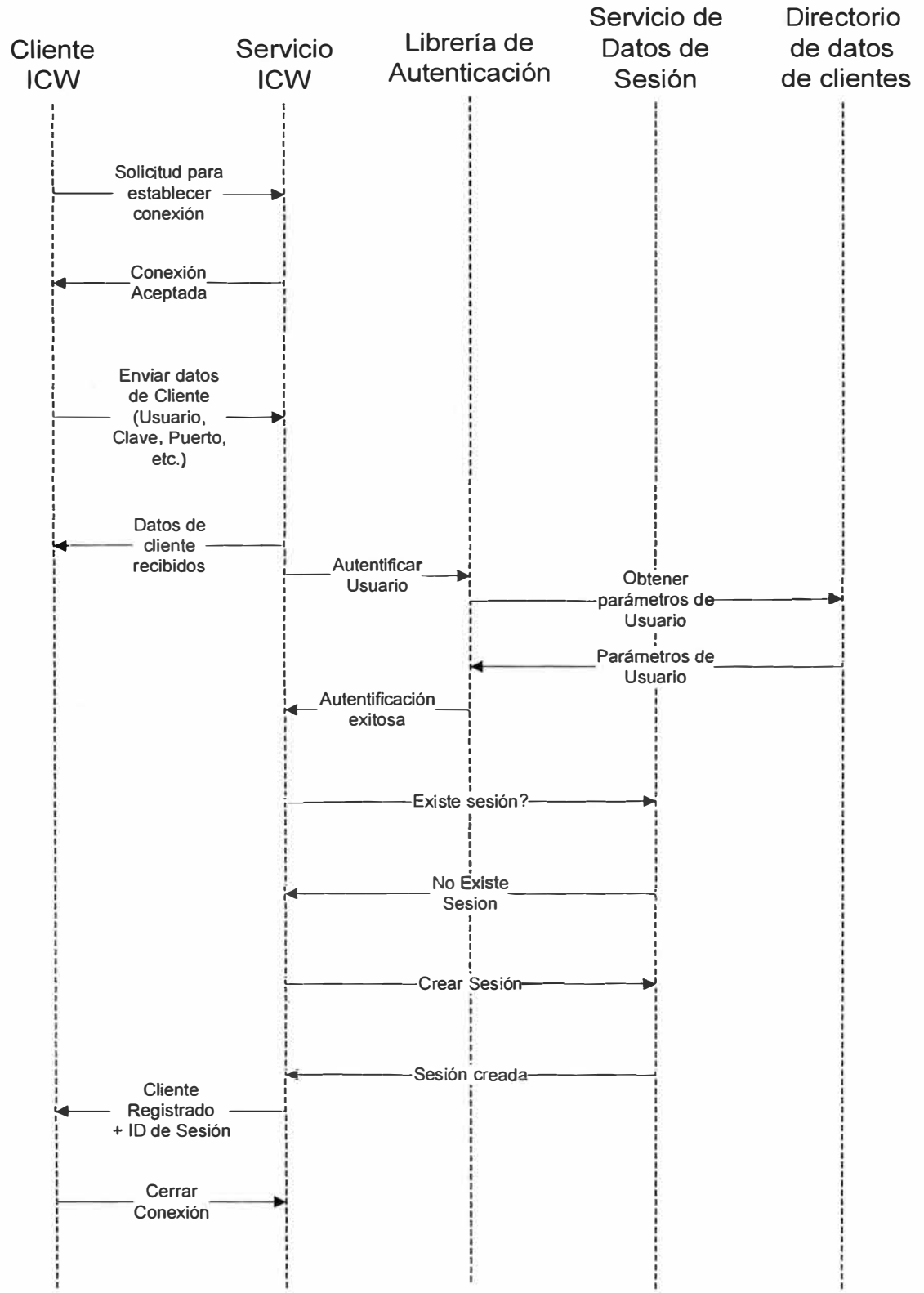
4.5 Interacción de los componentes

A continuación se presentarán las diferentes posibles situaciones de interacción entre los componentes del sistema: Cliente ICW, Servicio ICW, Directorio LDAP, Servicio de Datos de Sesión, Librería de Autentificación, Servicio Gatekeeper ICW H.323, Gatekeeper, Librería Interfase de Red (NPS). Además, se revisarán situaciones diversas fuera de los casos normales, que pueden ocurrir y se requieren controlar para que el flujo de la llamada continúe. (8)(9)

4.5.1 Registro del cliente

El registro del cliente seguirá la secuencia indicada en la fig. 4.2. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados hasta completar el registro del cliente. Pero pueden presentarse además situaciones que logren alterar el flujo, como las que se indican a continuación:

Fig. 4.2 Registro del Cliente



Sesión ya existe

Ante esta situación, el Servicio ICW debería realizar una actualización dicha sesión con el Servicio de Datos de Sesión, estableciendo los nuevos datos. Este caso puede ocurrir cuando el ID de alguna sesión anterior no se eliminó por algún posible error y coincide con el nuevo ID que se intenta registrar o también puede ocurrir que el usuario intente registrarse desde otra PC, con lo cual estaría cancelando su sesión anterior. Luego de la actualización, se sigue el proceso de registro normal.

Validación fallida del cliente

Cuando la librería de autentificación verifica los datos de usuario en el Servidor de Directorio LDAP y encuentra alguna inconsistencia, devuelve al Servicio ICW el resultado de una autentificación no exitosa que termina con una validación fallida del usuario, es decir, no podrá registrarse.

Máximo número de sesiones

El sistema tiene un límite máximo de sesiones capaz de administrar. Puede darse el caso en el cual se alcance dicho limite, ante lo cual, el Servicio de Datos de Sesión deberá rechazar cualquier intento adicional de registrar una nueva sesión que supere este máximo. Aquí también se termina con una validación fallida del usuario, es decir, no podrá registrarse. Con el correcto dimensionado de la capacidad del sistema no debería presentarse esta situación.

4.5.2 Cliente actualiza datos

La actualización de datos del cliente seguirá la secuencia indicada en la fig. 4.3. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados hasta que el cliente actualice sus datos tales como su correo electrónico, desvío a casilla y/o correo electrónico. También podría definirse una acción predeterminada diferente a la casilla y/o correo electrónico, dependerá del operador. Pero pueden presentarse además situaciones que logren alterar el flujo, como las que se indican a continuación:

Dirección IP no válida

Cuando el Servicio ICW verifique la dirección IP del cliente con los parámetros de sesión registrados en el Servicio de Datos de Sesión, puede ocurrir que no sea la misma. Ante esto, el Servicio ICW deberá rechazar inmediatamente la solicitud de actualización.

ID de Sesión no válido

Cuando el Servicio ICW reciba como respuesta del Servicio de Datos de Sesión que el ID de sesión no existe, deberá rechazar inmediatamente la solicitud de actualización.

Fig. 4.3 Cliente actualiza datos

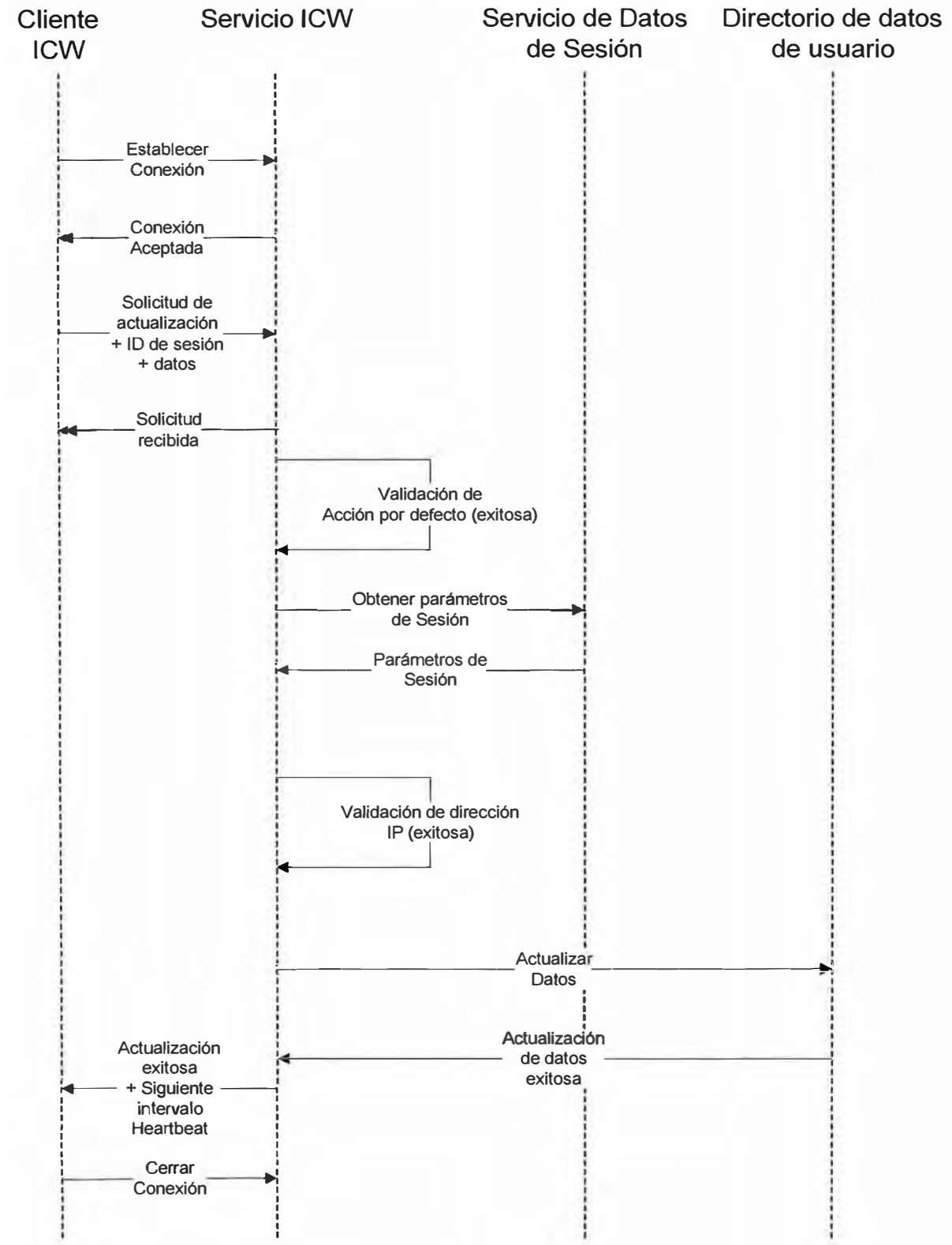
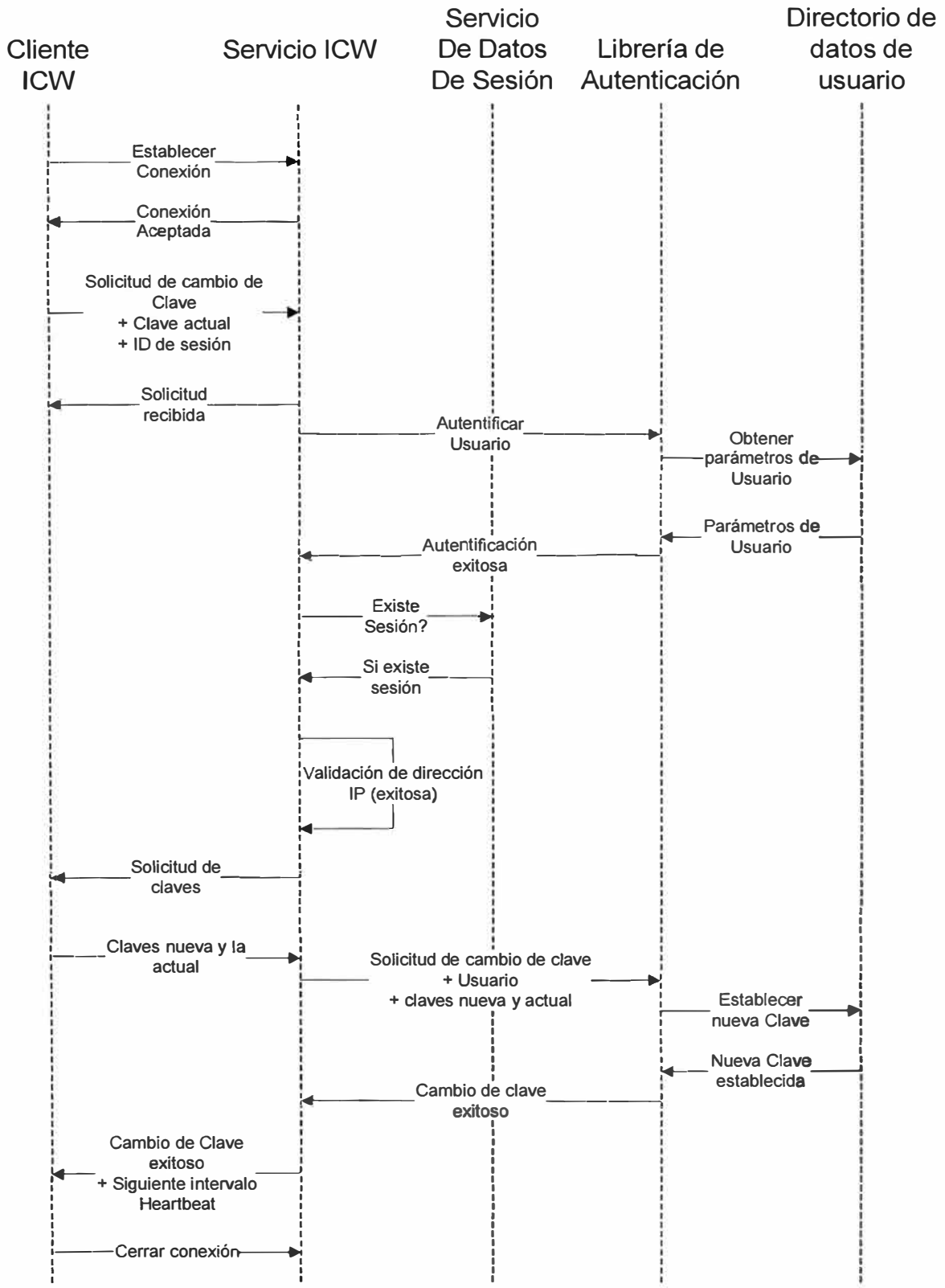


Fig 4.4 Cliente cambia de clave



- **Acción no es válida**

Cuando el Servicio ICW encuentre alguna inconsistencia en el cambio de acción solicitada por el cliente, el flujo deberá continuar para verificar el ID de la sesión así como el IP asegurándose de la validez de la conexión. Con la verificación exitosa, deberá rechazar la actualización solicitada pero enviando el siguiente intervalo de heartbeat pues se trata de un cliente válido que esta activo.

4.5.3 Cliente cambia de clave

El cambio de clave del cliente seguirá la secuencia indicada en la fig. 4.4. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados hasta que el cliente haya establecido su nueva clave. Pero pueden presentarse además situaciones que logren alterar el flujo, como las que se indican a continuación:

No se establece nueva clave

Si luego de todas las validaciones (autenticación exitosa, ID de sesión y dirección IP) no se puede realizar el cambio de la clave en el Directorio de Datos de Usuario, el Servicio ICW deberá responder que el cambio de clave no fue exitoso y enviará el siguiente intervalo de heartbeat pues se trata de un cliente válido que esta activo (al usuario debería notificársele para que reintente luego).

Dirección IP no válida

Como en casos anteriores, cuando el Servicio ICW verifique la dirección IP del cliente ICW con los parámetros de sesión registrados en el Servicio de Datos de Sesión y esta resulte incorrecta, deberá rechazar inmediatamente la solicitud de cambio de clave.

ID de Sesión no válido

Cuando el Servicio ICW reciba como respuesta del Servicio de Datos de Sesión que el ID de sesión no existe, deberá rechazar inmediatamente la solicitud de cambio de clave.

4.5.4 Cliente termina su sesión

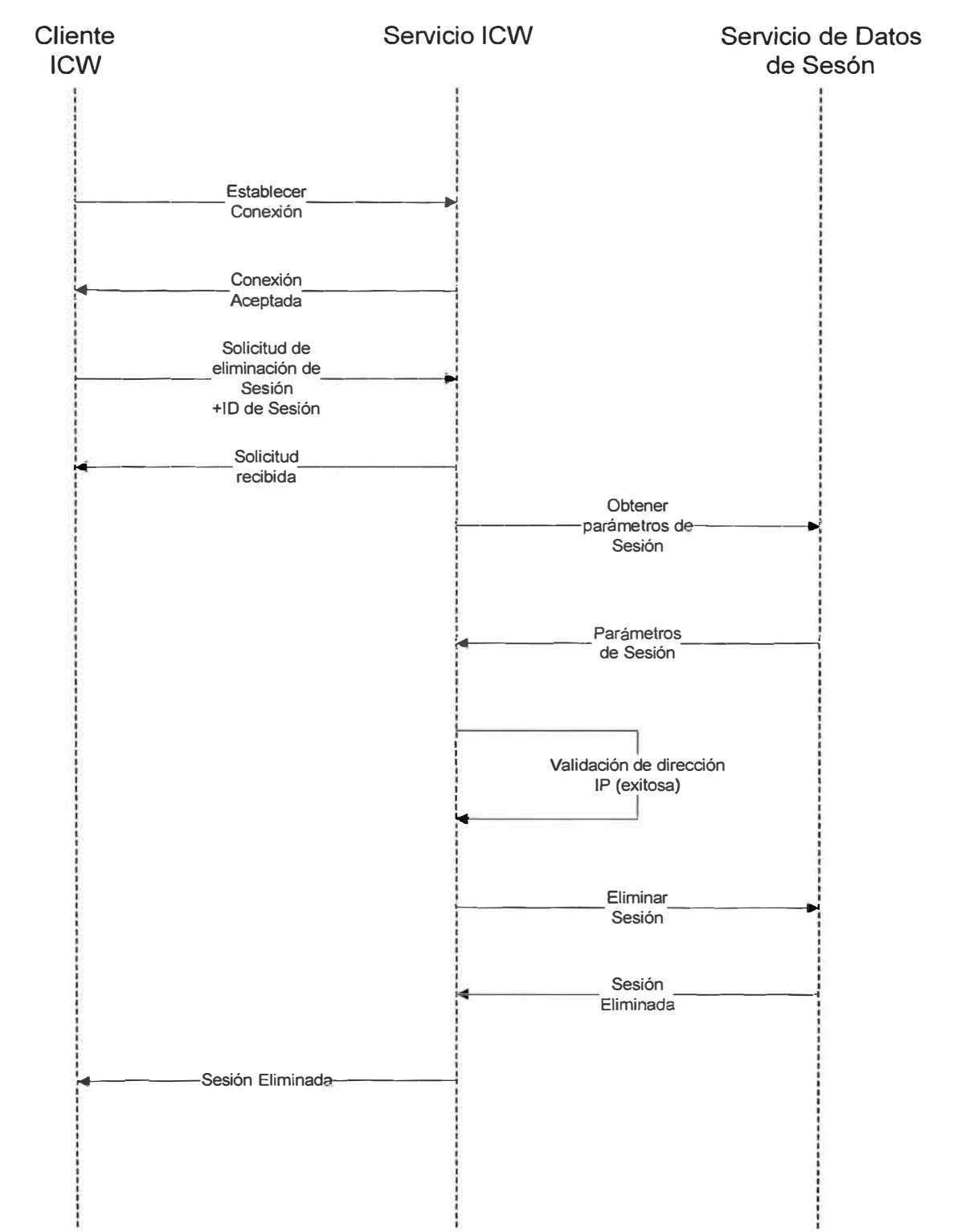
El cierre de sesión del cliente seguirá la secuencia indicada en la fig. 4.5. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados hasta la eliminación de la sesión. Pero pueden presentarse además situaciones que logren alterar el flujo, como las que se indican a continuación:

Dirección IP no válida

Cuando que el Servicio ICW verifique la dirección IP del cliente con los parámetros de sesión registrados en el Servicio de Datos de Sesión y esta resulte incorrecta, deberá

responder inmediatamente al Cliente ICW que la solicitud de eliminación de sesión no fue exitosa.

Fig. 4.5 Cliente termina su sesión



ID de Sesión no válido

Cuando el Servicio ICW reciba como respuesta del Servicio de Datos de Sesión que el ID de sesión no existe, deberá responder inmediatamente al Cliente ICW que la solicitud de eliminación de sesión no fue exitosa debido a que no existe.

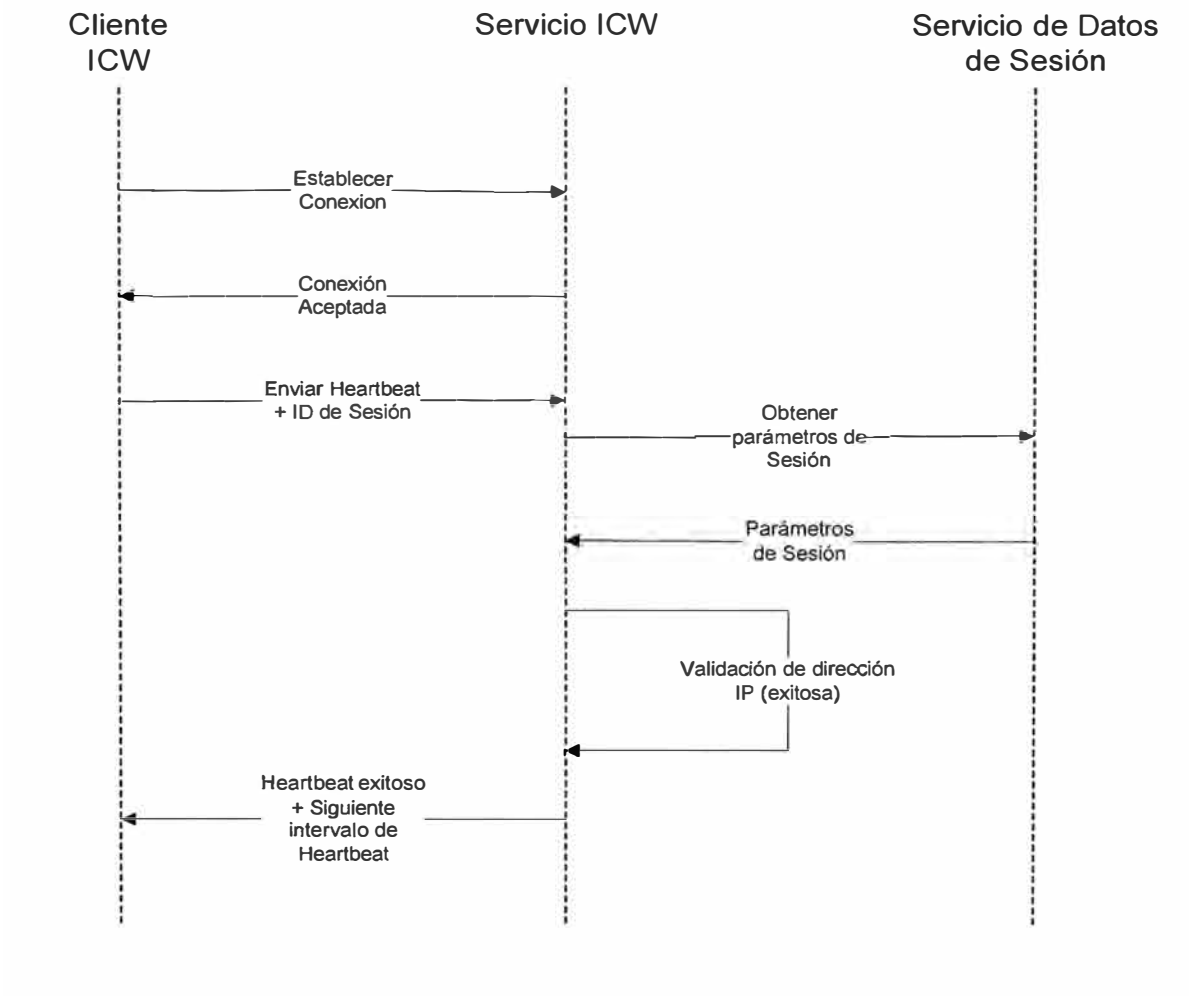
Ocurre un error

Si el Servicio de Datos de Sesión responde al Servicio ICW que no puede eliminar la sesión, este último responderá inmediatamente al Cliente ICW que su solicitud no se pudo ejecutar.

4.5.5 Heartbeat del cliente

Para el mantenimiento de la sesión, se requiere enviar periódicamente este mensaje de heartbeat, el cual seguirá la secuencia indicada en la fig. 4.6. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados hasta que se envía el siguiente intervalo de heartbeat. Pero pueden presentarse además situaciones que logren alterar el flujo, como las que se indican a continuación:

Fig. 4.6 Heartbeat del cliente



Dirección IP no válida

Cuando el Servicio ICW verifique la dirección IP del cliente con los parámetros de sesión registrados en el Servicio de Datos de Sesión y esta sea incorrecta, deberá responder inmediatamente al Cliente ICW con un mensaje de rechazo de heartbeat. Esto implica que dicho cliente deberá registrarse nuevamente.

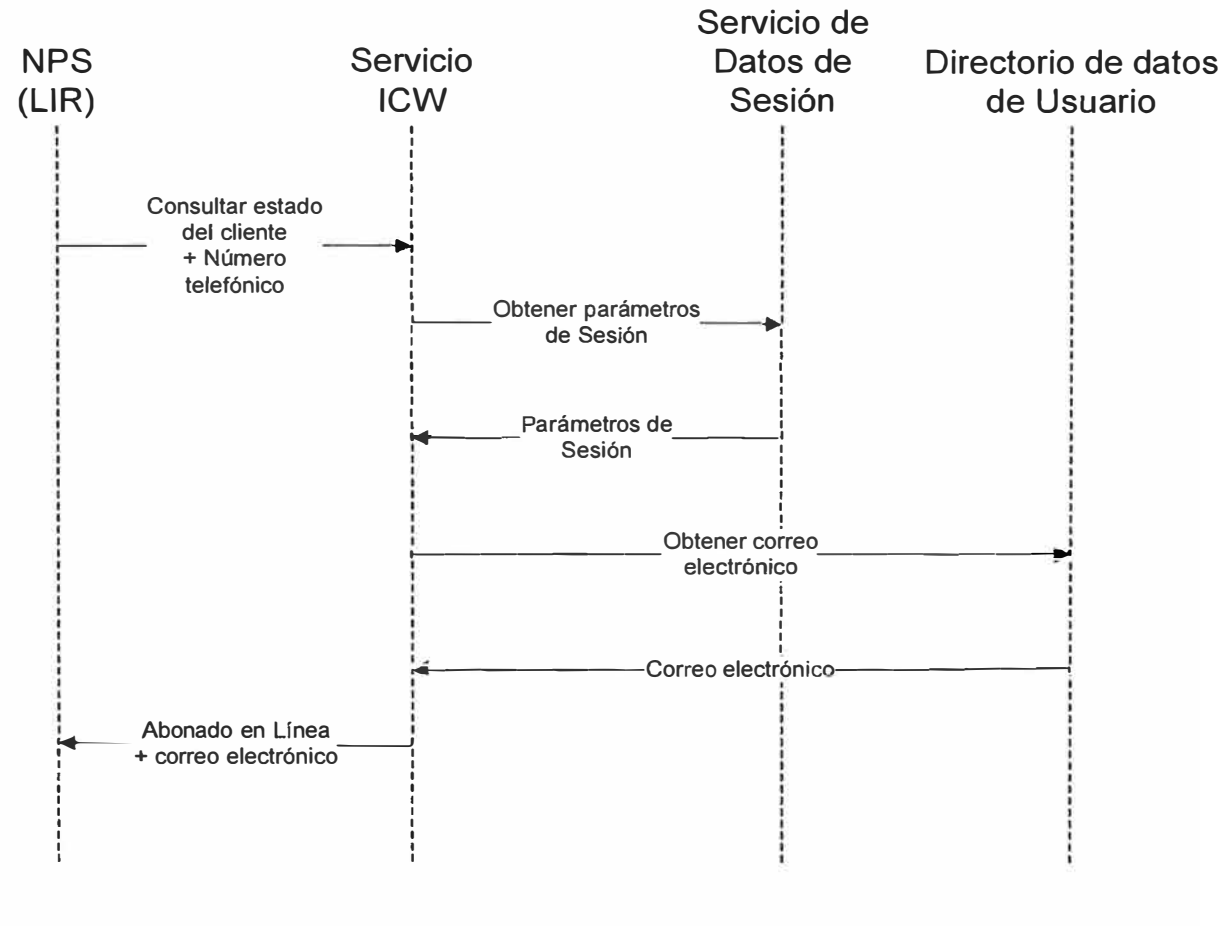
ID de Sesión no válida

Cuando el Servicio ICW reciba como respuesta del Servicio de Datos de Sesión que el ID de sesión no existe, deberá responder inmediatamente al Cliente ICW con un mensaje de rechazo de heartbeat. Esto implica que dicho cliente deberá registrarse nuevamente.

4.5.6 NPS Consulta estado del cliente

En el momento que el NPS reciba una llamada, deberá consultar al Servicio de Datos de Sesión el estado del cliente según la secuencia indicada en la fig. 4.7. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados hasta contar con el correo electrónico que se almacenó. Pero puede presentarse la siguiente situación:

Fig. 4.7 NPS Consulta estado del cliente



NPS Consulta estado del cliente – Cliente no esta en línea/error

Cuando el Servicio ICW verifique que la sesión no existe o se le devuelve algún error, consultará el correo electrónico del usuario y contestará al NPS que no está en línea. El NPS realizará entonces el desvío a la casilla de voz y/o a su cuenta de correo electrónico. Ya no será posible que consulte la acción a tomar al usuario.

4.5.7 NPS Consulta a Usuario por Acción

Si se ha determinado que el cliente esta en línea, se continuará con la consulta al usuario sobre la acción a realizar con la llamada que se encuentra retenida por el NPS. La consulta se realizará según la secuencia indicada en la fig. 4.8. Aquí se esta libre de errores y se ejecutan cada unos de los pasos indicados, enviando al NPS la respuesta del usuario para que tome acción con la llamada que se encuentra en espera. Pero pueden presentarse además situaciones que logren alterar el flujo, como las que se indican a continuación:

Cliente no responde a notificación

Luego de que el Servicio ICW envíe la notificación de llamada en espera al Cliente ICW, y este no responda, deberá indicarle al NPS que no hubo respuesta del usuario. Entonces el NPS procederá a desviar la llamada a la casilla de voz y/o a su cuenta de correo electrónico.

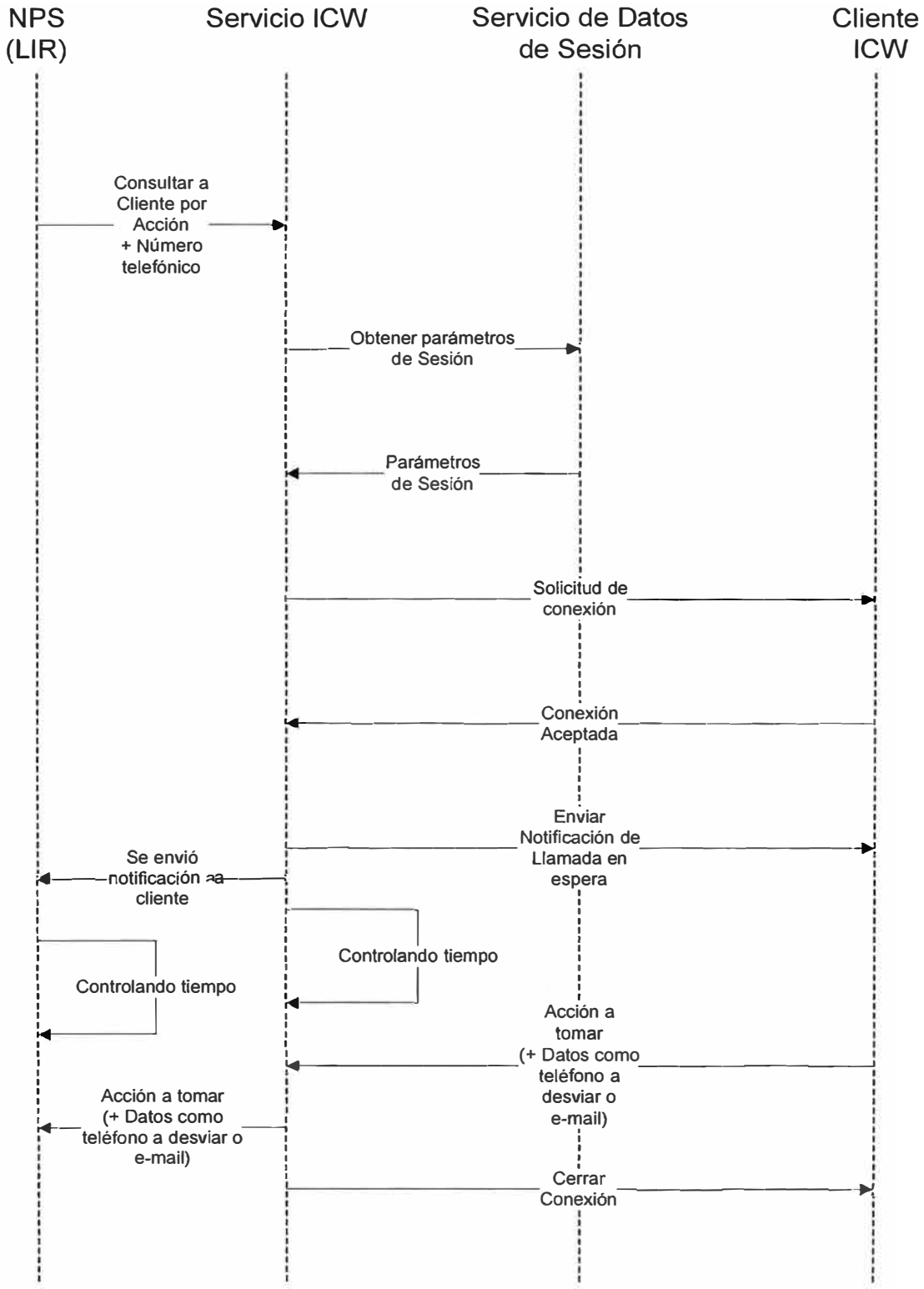
Falla notificación conexión con cliente

Si no recibe respuesta a la solicitud de conexión con el cliente, puede asumirse una falla o problema con la comunicación, lo que será notificado al NPS para que desvíe la llamada a la casilla de voz y/o a su cuenta de correo electrónico.

ID de Sesión no válido

Cuando el Servicio ICW reciba como respuesta del Servicio de Datos de Sesión que el ID de sesión no existe, deberá notificarlo al NPS para que desvíe la llamada a la casilla de voz y/o a su cuenta de correo electrónico.

Fig. 4.8 NPS Consulta a cliente por acción



4.5.8 Requerimiento de Localización del Gatekeeper

Cuando el Gatekeeper necesite obtener la dirección IP del cliente con el que se desea establecer una sesión de VoIP, realizará la consulta al Servicio de Datos de Sesión a través de Servicio Gatekeeper ICW H.323, siguiendo la secuencia de la fig. 4.9. Pero puede presentarse la siguiente situación:

ID de Sesión no válido

Cuando el Servicio Gatekeeper ICW H.323 verifique que la sesión no existe o se le devuelva algún error, responderá con un mensaje Response LRQ vacío (NULL).

GKTMP RAS Messages

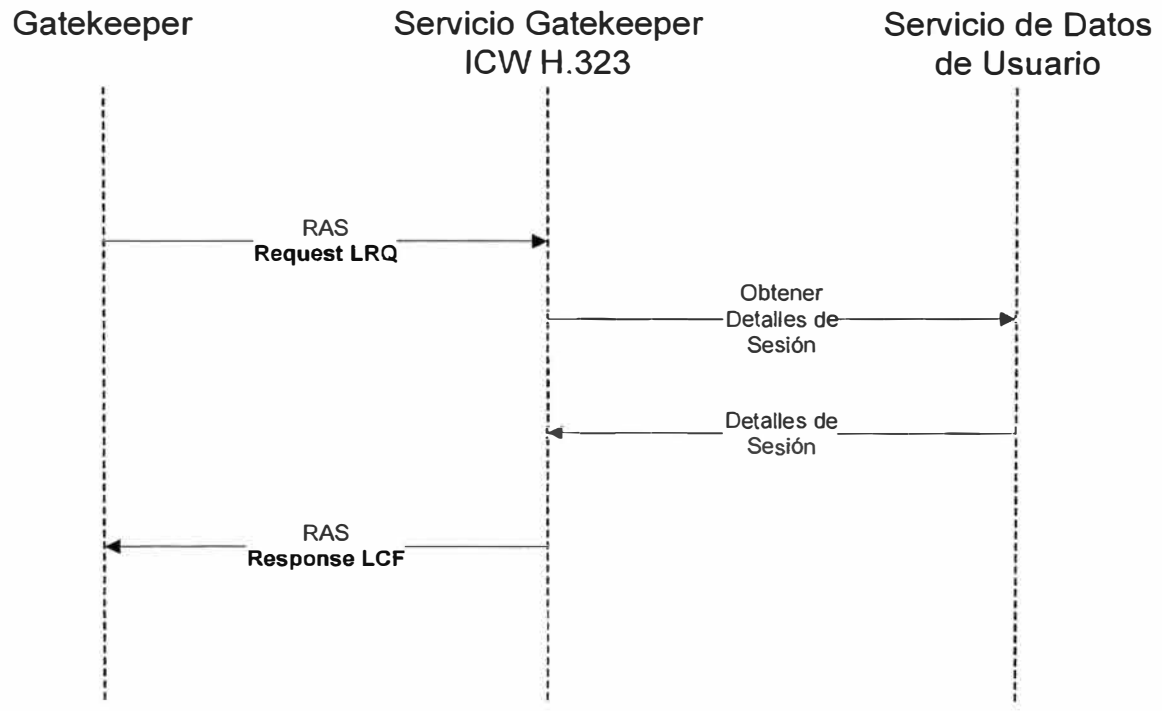
Usado para intercambiar mensajes RAS entre el Cisco IOS Gatekeeper y aplicaciones externas:

Request LRQ (Location Request): Un mensaje de consulta entre 2 gatekeepers H.323 para encontrar la dirección de un elemento final H.323.

Response LRQ: Mensaje de respuesta al Request LRQ, vacío (null) para que continúe el proceso normalmente.

Response LCF (Location Confirmation): En este caso para es para completar el proceso del requerimiento.

Fig. 4.9 Requerimiento de Localización del Gatekeeper



CAPÍTULO V
FUNCIONAMIENTO

5.1 Configuración en las centrales de conmutación

En las centrales de conmutación debe configurarse al abonado la facilidad de desvío por "ocupado" y "no contesta", con la finalidad de que cada vez que no conteste las llamadas en dicho número o la línea este ocupada con otra llamada o este conectado a Internet mediante acceso conmutado, cualquier llamada entrante sea desviada al NPS a través de un código previamente establecido como se observa en la fig. 5.1.

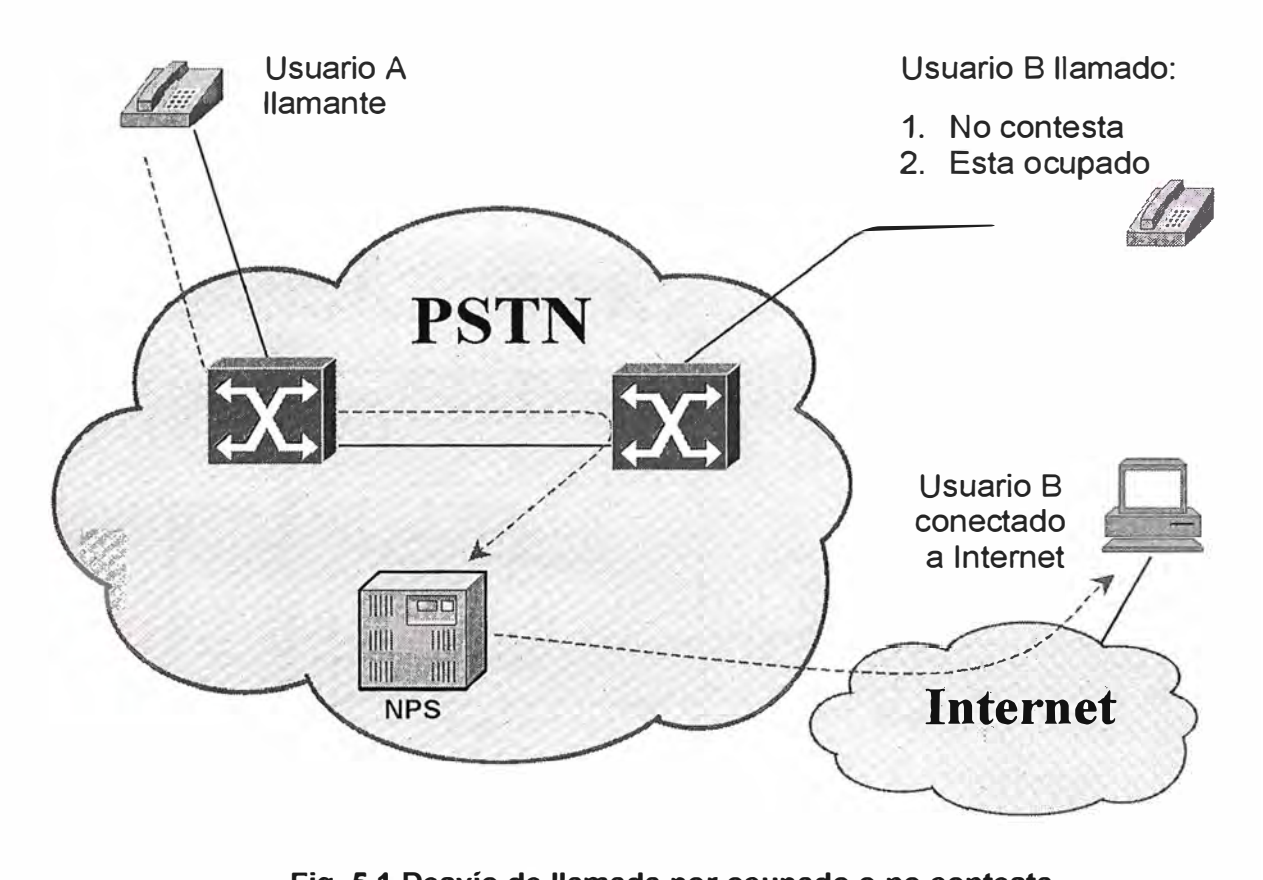


Fig. 5.1 Desvío de llamada por ocupado o no contesta

Debe tenerse en cuenta la compatibilidad de este servicio con otros servicios suplementarios o de valor añadido.

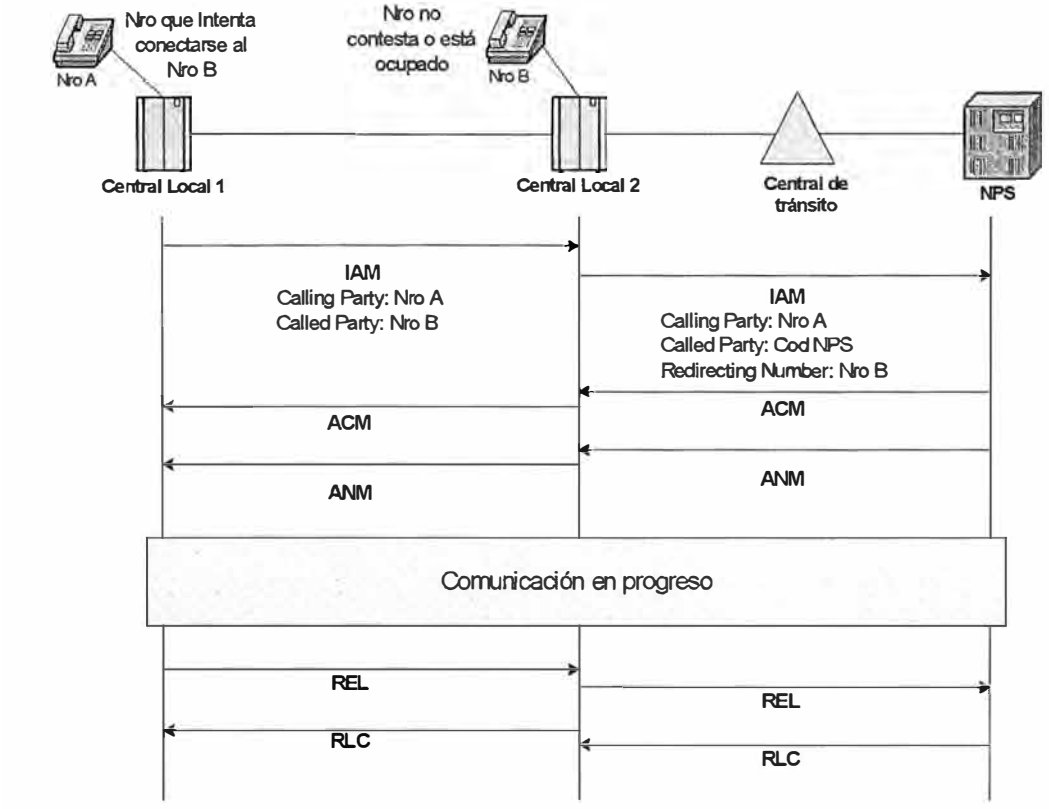
Por ejemplo, el caso del servicio de llamada en espera o el de mensajería de voz (que puede incluir al anterior) es bastante ilustrativo al respecto.

Está diseñado de tal manera que cuando estuviese ocupada la línea telefónica con una llamada, ya sea que ésta se haya realizado desde el número del cliente o se haya recibido -cual sea el caso-, se recibirá un tono intermitente que indicará la presencia de una llamada por atender (llamada en espera), lo que representa un problema pues el tono dentro de banda cortará la conexión a Internet si estuviese conectado vía acceso conmutado.

Según se puede observar, no hay compatibilidad entre ambos servicios. Si se desease contar con el servicio de "Llamada en espera de Internet" debería desactivarse la mensajería de voz ya que estaría incluido en este servicio o también, la llamada en espera si se conecta vía acceso conmutado.

A continuación, en la fig. 5.2, se muestra como podrían transferirse los números involucrados al Nodo Proveedor de Servicios por medio de señalización N7 (10), desde que se inicia la llamada hasta que es terminada, en este caso por el Nro A.

Fig. 5.2 Transferencia de los números al NPS



Otro aspecto importante a considerar en la interconexión de la red PSTN es el hecho de que todas las centrales no van a conectarse directamente con el NPS donde se brinde el servicio de "Llamada en espera de Internet". Es decir, deberá existir un punto intermedio, una central de tránsito con la cual se realizará todo este proceso.

Con respecto a los códigos de acceso, se necesitan básicamente dos para la interconexión de la PSTN y el NPS, uno de ellos es para acceder desde la PSTN al NPS, de forma que esta pueda identificar el servicio (ver figura anterior) y el otro de salida desde el NPS a la red PSTN (central de tránsito) con destino al Gateway. El objetivo final de estos códigos es dar un adecuado tratamiento a las llamadas.

5.2 Tratamiento de las llamadas

Como se ha descrito anteriormente, este servicio provee al usuario varias opciones con respecto al tratamiento una llamada entrante mientras esta conectado a Internet (implica que su línea telefónica está ocupada)

A continuación se mostrarán algunos diagramas de interconexión del servicio de Llamada en Espera de Internet, describiendo gráficamente como es tratada una llamada que es desviada a este servicio para sus diferentes alternativas disponibles:

Fig. 5.3 Interconexión de los equipos
Fig. 5.4 Registro del Cliente ICW
Fig. 5.5 Cliente registrado es llamado
Fig. 5.6 Llamada atendida mediante VoIP
Fig. 5.7 Llamada desviada (A celular, a otro número o al propio o casilla de voz en otra plataforma)
Fig. 5.8 Llamada desviada a la Casilla (en NPS)
Fig. 5.9 Mensaje enviado a correo electrónico

Fig. 5.3 Interconexión de los equipos

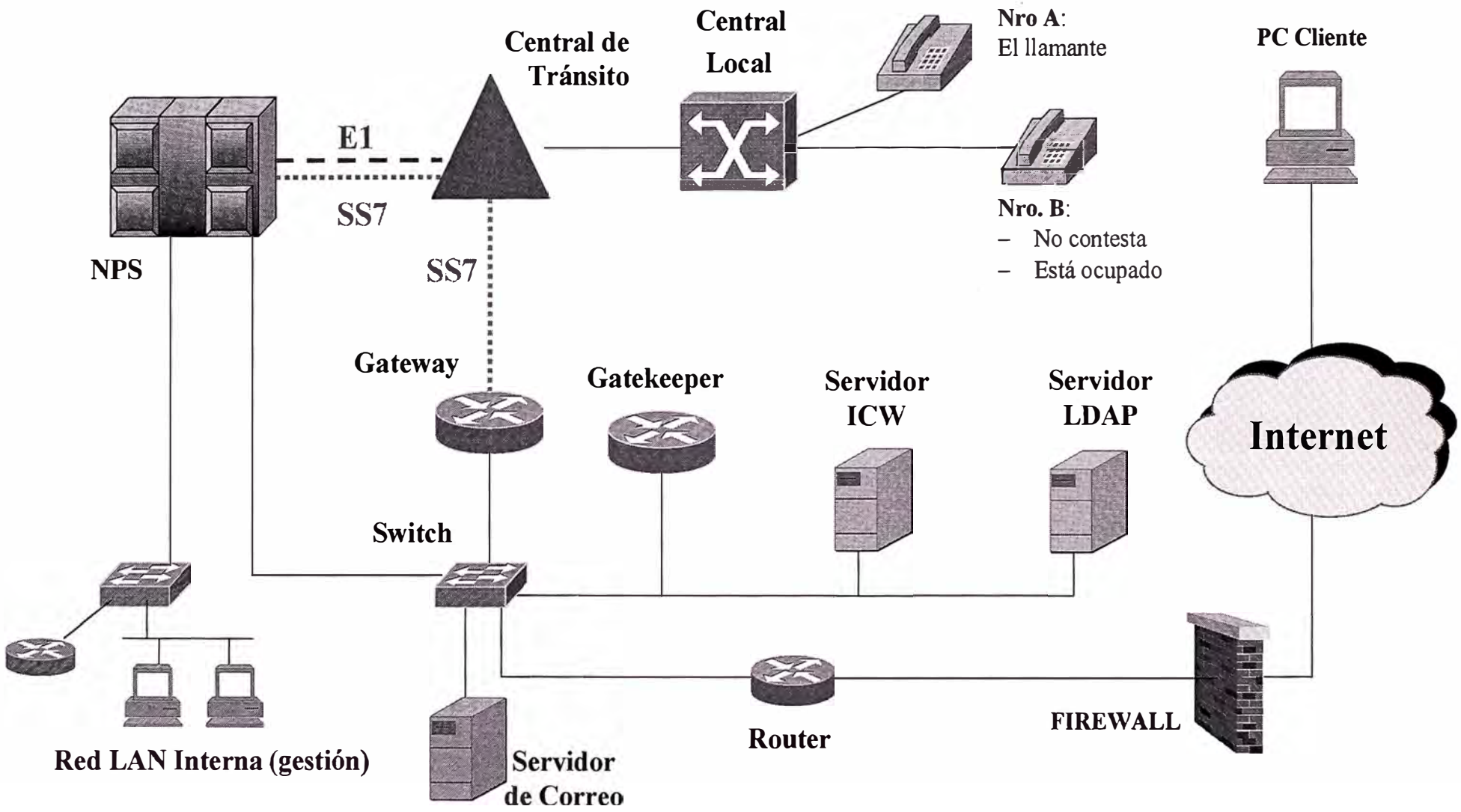


Fig. 5.4 Registro del Cliente ICW

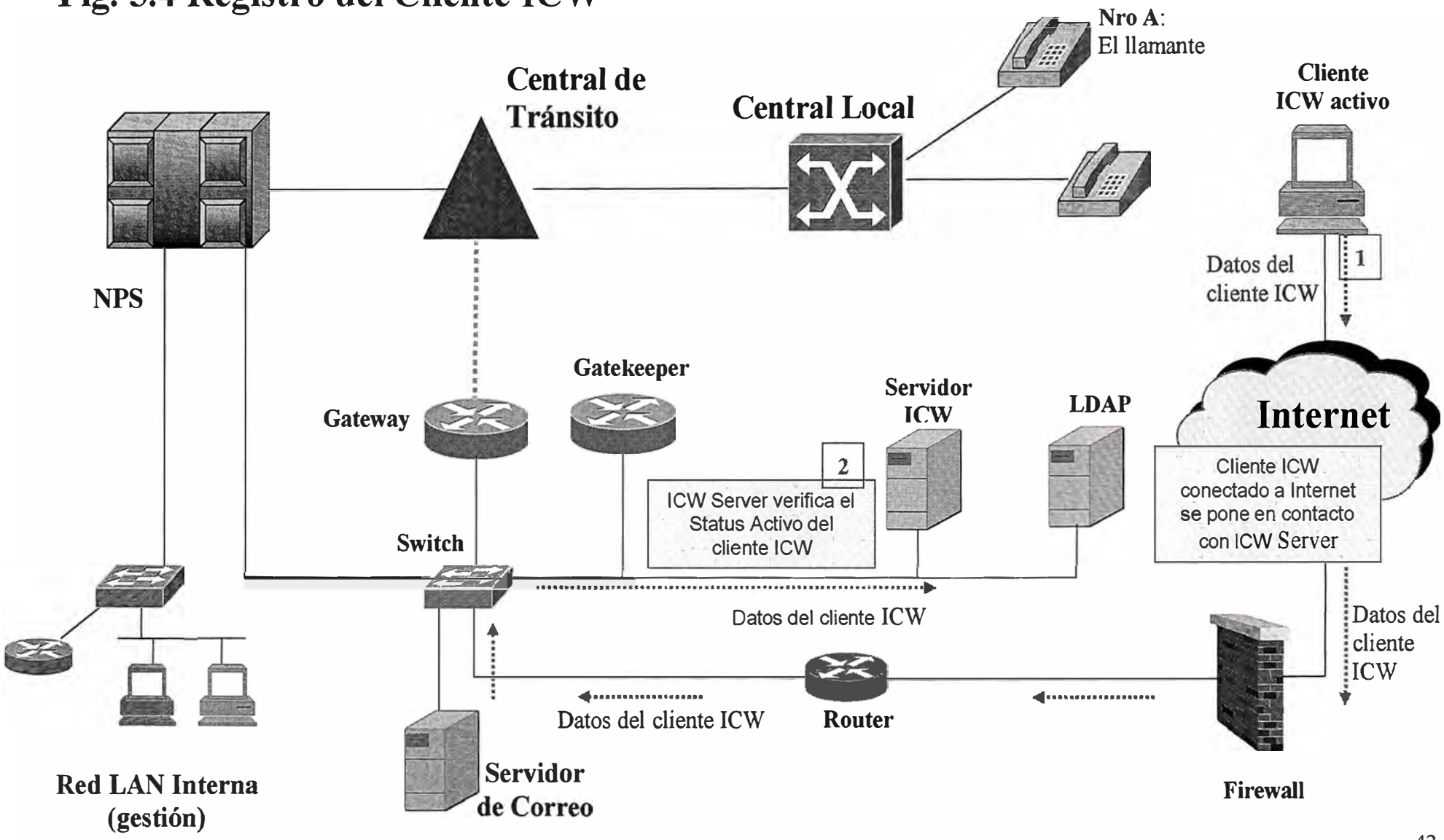


Fig. 5.5 Cliente registrado es llamado

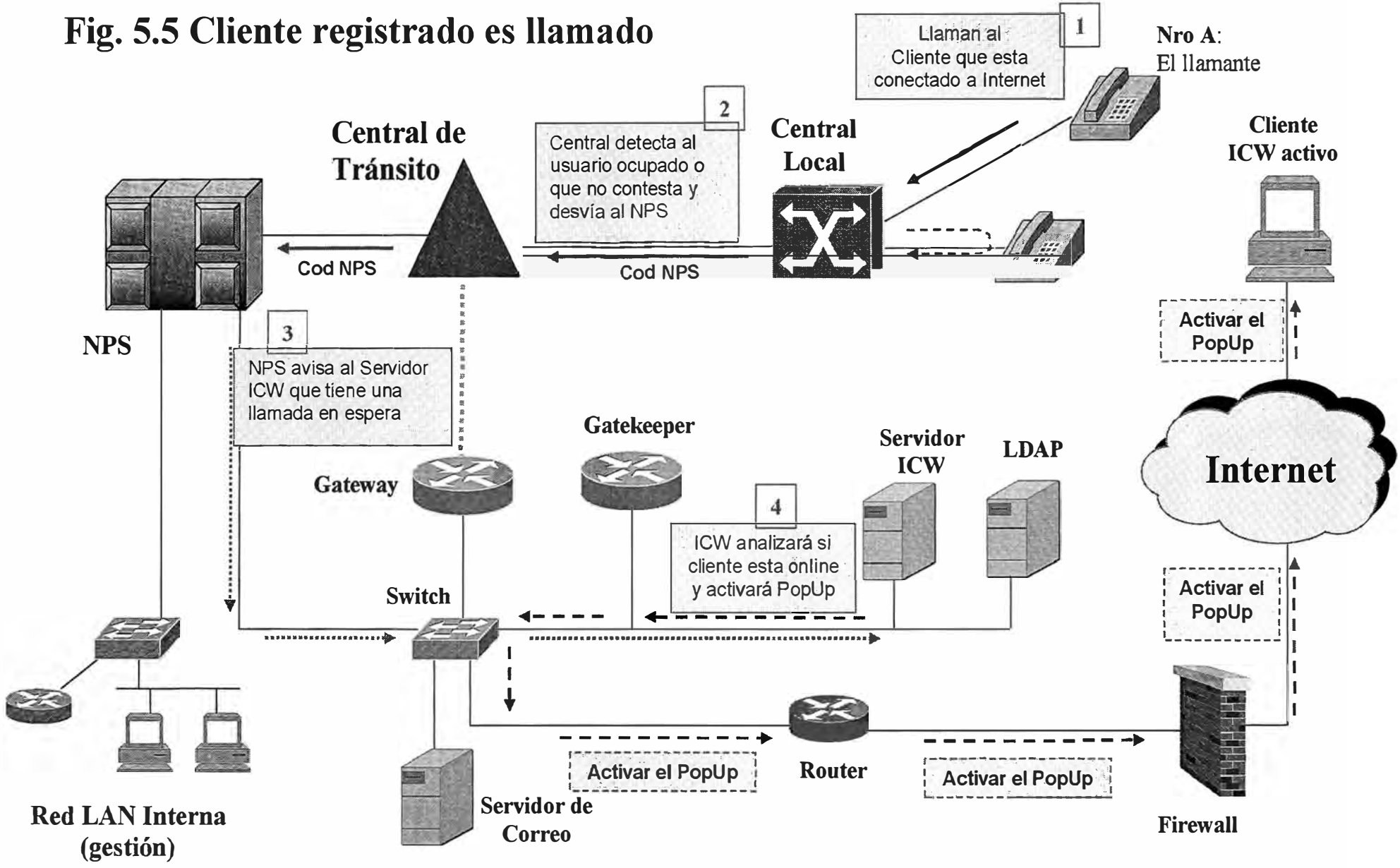


Fig. 5.6 Llamada atendida mediante VoIP

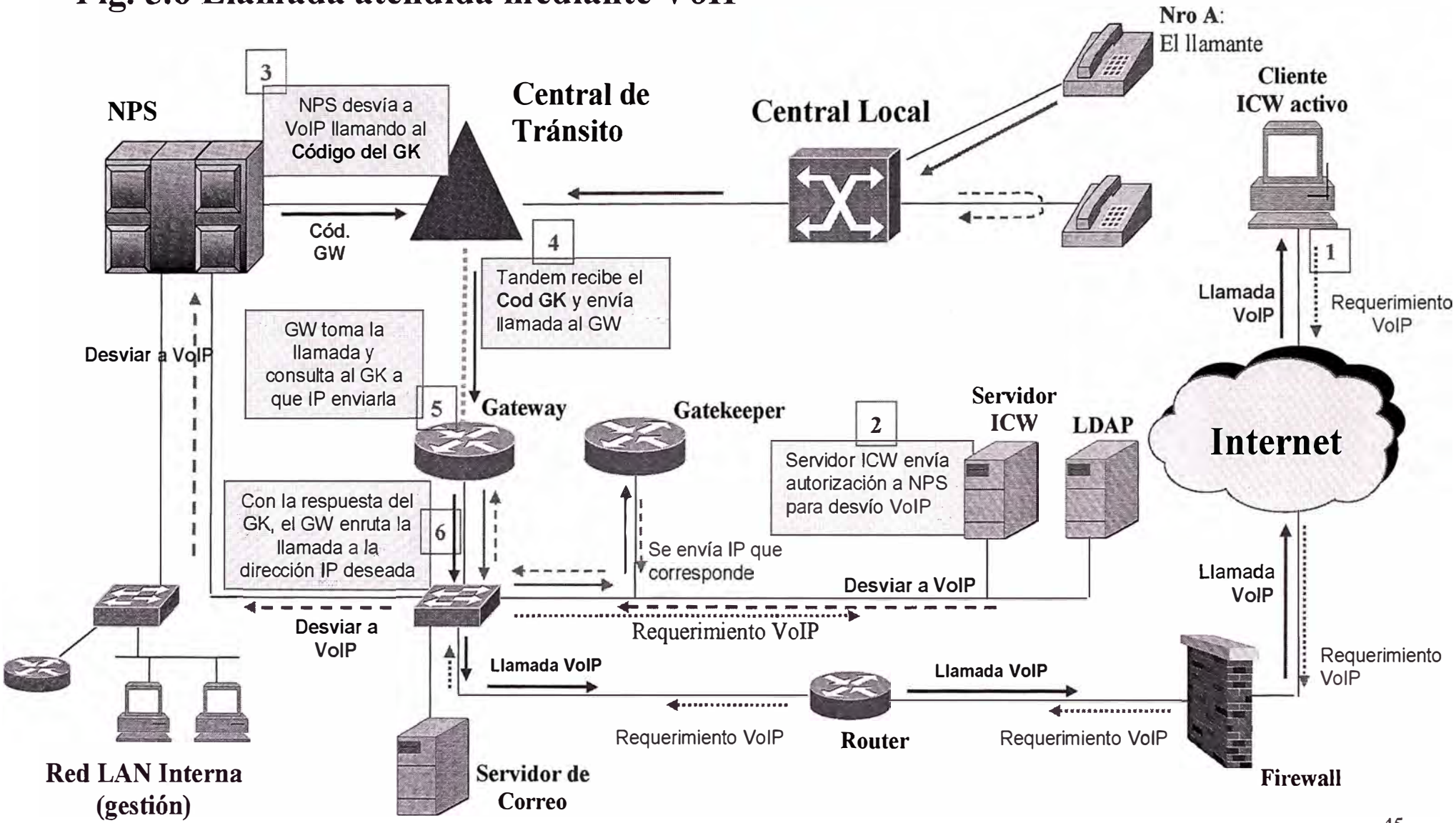
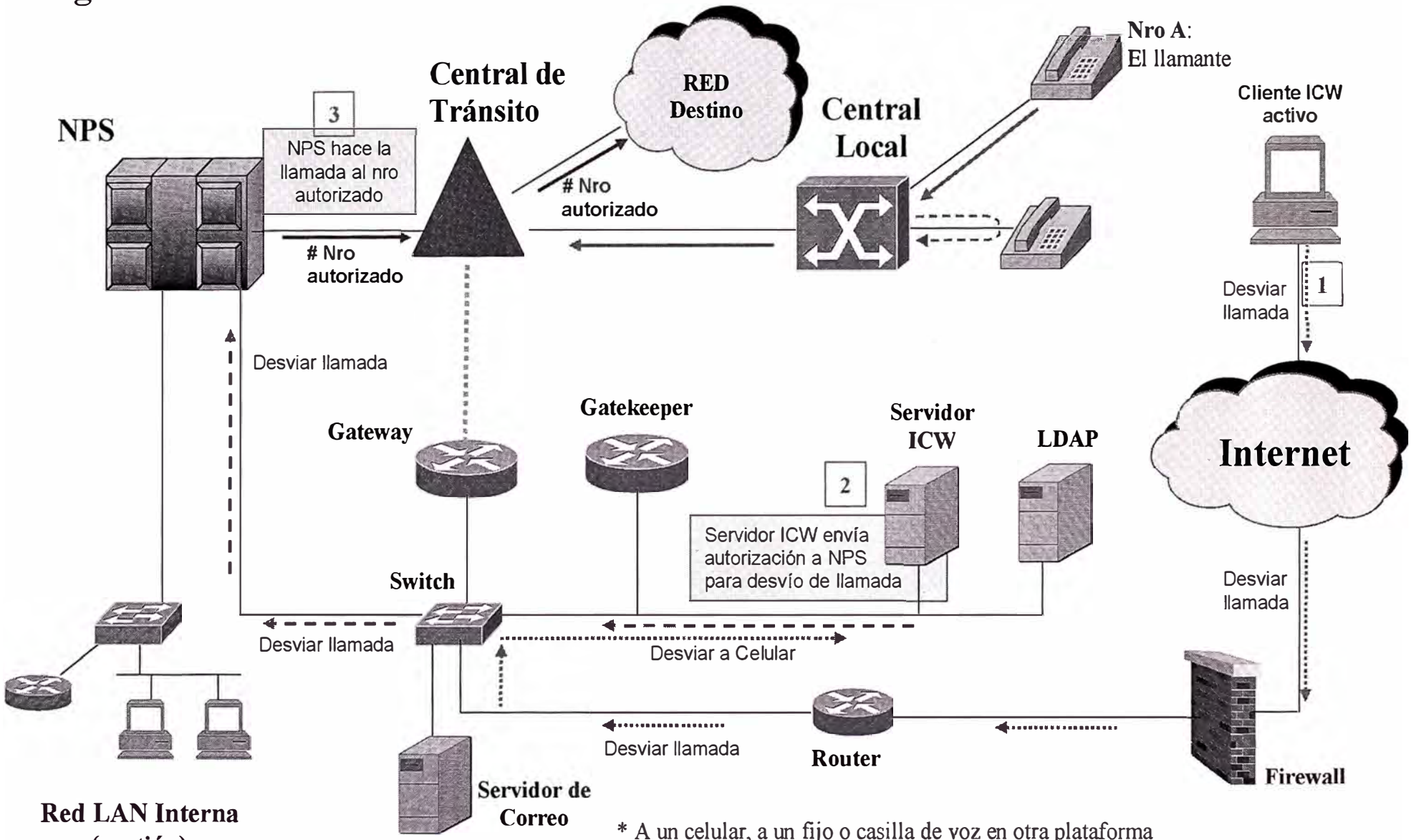


Fig. 5.7 Llamada desviada *



* A un celular, a un fijo o casilla de voz en otra plataforma

Fig. 5.8 Llamada desviada a la Casilla (en NPS)

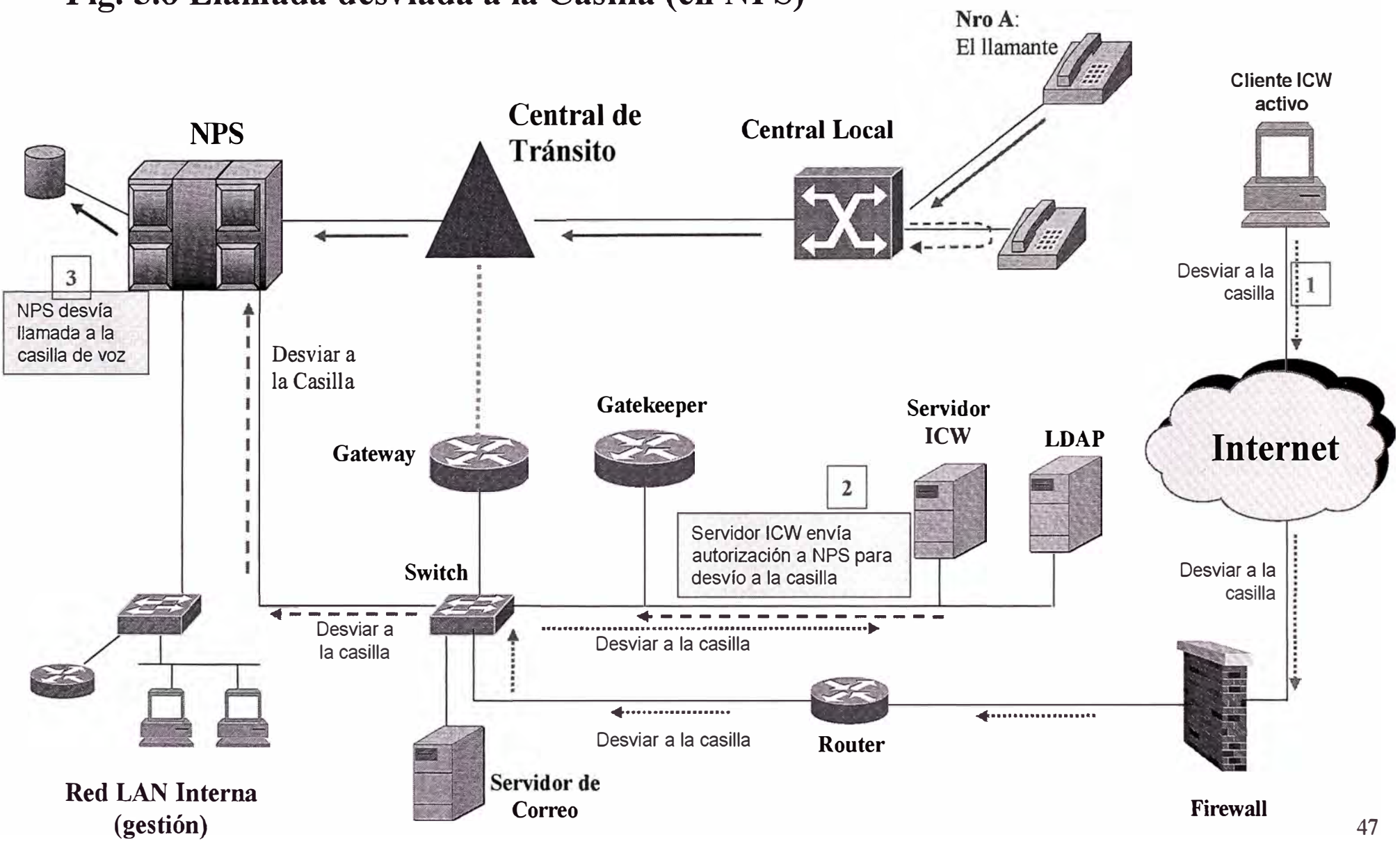
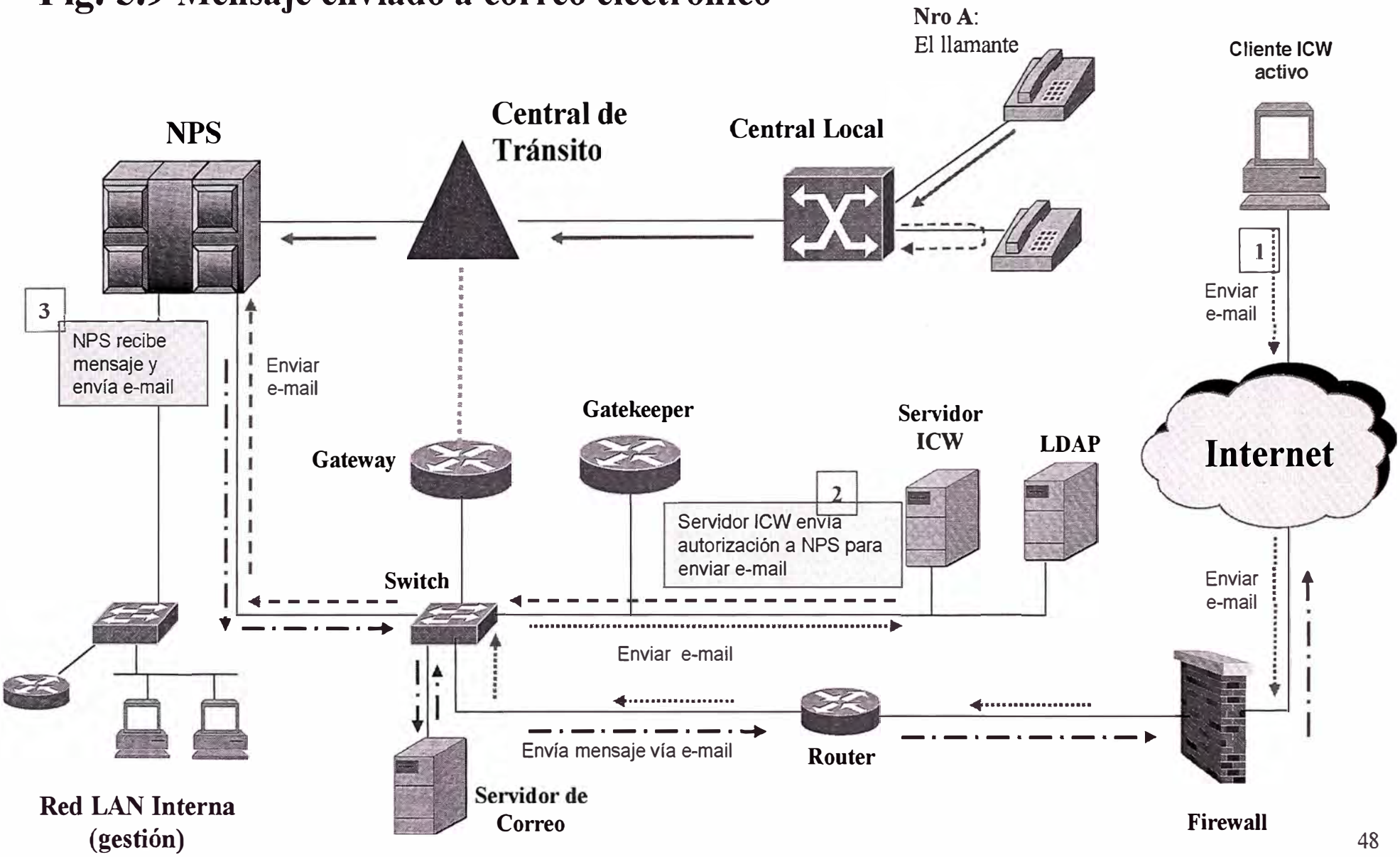


Fig. 5.9 Mensaje enviado a correo electrónico



5.3 Implementación

Se consideran los equipos que se describirán en el capítulo VI - Equipamiento del presente informe, preferentemente deberán encontrarse físicamente en un mismo local.

Los enlaces (E1s) entre la central de tránsito y el Nodo Proveedor de Servicios: Por lo menos 02 E1s que aseguren conectividad y la señalización de no haber una previa conexión.

Enlaces (E1s) entre la central de tránsito y el Gateway H.323. Por lo menos 02 E1s que aseguren conectividad y la señalización: Hay 2 opciones disponibles con respecto a la señalización: N7 o R2.

Considerar los números restringidos para efectos de tasación, son los números que se compararán con los de una tabla, de ser iguales la llamada no progresará (se comparan las series o números).

5.4 Requerimientos para Operación y Mantenimiento

Algunas consideraciones importantes:

Capacitación necesaria del personal involucrado en la operación y mantenimiento de los servicios en el Sistema Operativo Windows 2003 Server así como en manejo de los equipos Cisco y software relacionado.

Se sugiere que todos los equipos necesarios para el funcionamiento del servicio se encuentren ubicados en un mismo lugar para fines de interconexión, operación y mantenimiento.

Se debe contar con los medios necesarios para el respaldo periódico de la información.

Se debe proveer un acceso de consulta al servicio con la finalidad de que el personal que atiende a los clientes pueda observar el estado de las cuentas y contar así con un medio que le permita absolver consultas o reclamos en el menor tiempo posible.

CAPÍTULO VI
EQUIPAMIENTO

6.1 Hardware Básico

6.1.1 Servidor de Directorio

El servidor de directorio es usado para albergar un directorio LDAP-compliant en el cual se almacenará todos los datos de usuario. El Active Directory de Microsoft es una opción destacable que además se integraría mejor a la red con el servidor ICW Windows 2003. Debe observarse que de contar con mapeo de atributos de esquema, se podría utilizar cualquier otro proveedor de servidores de directorio.

6.1.2 Servidor ICW Windows 2003

Aquí se encuentra una considerable parte de la arquitectura, por lo que debería permitir escalabilidad, con el respectivo soporte software. Las funciones que se ejecutan en este servidor son:

Escuchar y autentificar los intentos de registro provenientes de los clientes ICW contra los datos de abonados registrados en Directorio LDAP.

Mantener una lista de los abonados que se encuentren actualmente registrados (clientes ICW en línea)

Actualizar apropiadamente los registros de abonados en el directorio LDAP.

Mediante mensajes heartbeat actualizar la lista de clientes en línea

Escuchar y procesar los requerimientos del Gatekeeper H.323 para la resolución de direcciones E.164 a IP permitiendo realizar la llamada VoIP.

Escuchar los requerimientos del Nodo Proveedor de Servicios tales como notificaciones de llamada en espera, parámetros del sistema, etc.

6.1.3 H.323 Gatekeeper

Pasa los requerimientos para la resolución de direcciones de E.164 a IP desde el H.323 Gateway al servidor ICW Windows 2003 que es el que provee el servicio de resolución de direcciones.

6.1.4 H.323 Gateway

Recibe las llamadas de la red PSTN (específicamente, desde la central Tandem) provenientes del Nodo Proveedor de Servicios para que pueda ser enviada a través de Internet (VoIP) al usuario que así desee contestarla.

6.1.5 Cliente ICW

Es una computadora personal que debe cumplir al menos con los mínimos requerimientos que exija el componente de software cliente ICW.

Para poder recibir las llamadas a través de Internet (VoIP), necesitará software H.323-compliant.

6.1.6 Servidor de Correo

Permitirá en envío de correo saliente a Internet utilizando el SMTP, protocolo estándar de Internet para transportar y entregar mensajes electrónicos.

Recibirá del NPS mensajes de correo a destinatarios de un dominio remoto, mediante el DNS buscará la dirección IP del dominio de destino y después intenta entregar el mensaje.

6.2 Alternativas de Fabricantes

La solución ICW puede contar con equipos de diversos fabricantes. Su selección y dimensionamiento se definen según los requerimientos software de los diferentes componentes para una cantidad determinada de usuarios. Se debe asegurar un adecuado soporte técnico que permita la continuidad del servicio en caso de problemas o averías. Con respecto al Gatekeeper y Gateway, Cisco ofrece alternativas variadas, algunas se muestran en el apéndice A, en los otros casos, HP es una buena opción.

Servidor Windows 2003

Fabricante	Diverso

Servidor LDAP

Fabricante	Diverso

Servidor de Correo

Fabricante	Diverso

Firewall

Fabricante	Cisco

Gateway H.323

Fabricante	Cisco

Gatekeeper H.323

Fabricante	Cisco

Switch

Fabricante	Cisco

CONCLUSIONES

1 Lo que se presenta en este informe es una alternativa flexible para la notificación de llamadas mientras se esta conectado a Internet, lo que representa un beneficio mutuo tanto para las personas con crecientes necesidades de comunicación como para el operador, que mejora su tasa de llamadas completadas así como la posibilidad de generación de nuevas llamadas. Durante la implementación del software principalmente se verá si es necesario realizar alguna variante que mejore el rendimiento y desempeño del sistema teniendo en cuenta la arquitectura de la red telefónica del operador.

2 Este servicio puede brindarse a cualquier abonado de la red pero deben considerarse ciertas restricciones. No todos los clientes tienen libre disponibilidad de realizar llamadas, por tal motivo, deben manejarse controles que permitan restringir desvíos a ciertos números como pueden ser larga distancia, celulares, etc. Esta función es comúnmente implementada en los Nodos Proveedores de Servicios pues es usado por otros servicios que también originan llamadas. Aunque esto reduce la cantidad de llamadas y el potencial ingreso económico, es una medida necesaria para prevenir la ejecución de llamadas que luego no van a poder ser cobradas.

3 En caso de utilizarse señalización N7 entre el Gateway y la central de tránsito, habría que asignarle un punto de señalización al Gateway, además, dicho Gateway debe soportar N7 lo cual eleva su costo. Tiene la ventaja de hacer más sencilla la instalación, las pruebas y la detección de errores si aparecieran problemas antes o durante el funcionamiento. Si se utiliza señalización R2, el Gateway resulta más económico pero perdemos las facilidades anteriormente mencionadas.

4 La calidad de la voz será relativamente limitada a través de Internet en comparación con la red conmutada, ya que se ve afectada por los retardos y

el ancho de banda disponible, los cuales varían y pueden degradar mas la voz si se cuenta con una conexión vía módem.

Para brindar protección a la red en la que se da el servicio, los Firewalls pueden ser de uso compartido o independientes, dependerá de la disponibilidad de equipo y las facilidades de configuración que ofrezcan para mantener las condiciones mínimas de seguridad.

ANEXO A

Especificaciones técnicas del Gateway y Gatekeeper

Supported Cisco Gateways and Gatekeepers

Cisco Gateways	Cisco Gatekeepers
1750 Access Router	3640 Multiservice Platform
Catalyst 2600 Series Switches	3660 Multiservice Platform
3600 Series Routers	7200 Series Routers
AS5300 Series Universal Access Server	—
AS5350 Universal Gateway	—
AS5400 Series Universal Gateways	—
AS5800 Series Universal Access Servers	—
AS5850 Universal Gateway	—
7200 Series Routers	—

Cisco Platform and Software Specifications

Cisco Platforms	Cisco IOS Releases
Cisco IOS Gatekeeper Release—Cisco 3640, 3660, and 7200 platforms	12.2(2)XA, 12.2(2)T, 12.2(11)T, 12.2(2)XU (Cisco 3660 and

	7200 only)
Cisco IOS Gateway Release—Cisco 1750 and 2600 platforms	12.2.7
Cisco IOS Gateway Release—Cisco 3640, 3660, and 7200 platforms	12.2.7, 12.2(2)XA, 12.2(11)T
Cisco IOS Gateway Release—Cisco 5300, 5350, 5400, 5800, and 5850 platforms	12.2.7 (no 5350 or 5850), 12.2(2)XB, 12.2(11)T 12.2(2)XU (no 5800)

Data Sheet - Cisco AS5300/Voice Gateway

Cisco AS5300/Voice Gateway Technical Specifications

Standard Specifications	
Processor Type	150-MHz R4700
Memory	64 MB DRAM
Flash Memory	16 MB system Flash, single or dual bank, up to 16 MB boot Flash
Chassis Slots	Three
Ethernet (RJ-45)	Two (one 10 MB, one 10/100 MB)
Voice/Fax Ports	Up to 96 (T1) or 120(E1)
56K Modems	Up to 48 (T1) or 60 (E1) modems when 48 (T1) or 60 (E1) voice ports are installed

ISDN PRI, T1, or E1	Supports PRI Q.931 and channel-associated signaling
Other Standard Components	Power supply and cord, console cable, two RJ-48C cables, carrier card tool
Dimensions (H x W x D)	3.4 x 17.5 x 18.25 in. (xx cm [need to provide])
Weight	32 lb (19 kg)
Environmental Conditions and Power Requirements	
Operating Temperature	32 to 104° F (0 to 40° C)
Nonoperating Temperature	-40 to 185° F (-40 to 85° C)
Operating Humidity	5 to 95%, noncondensing
Noise Level	34 dB @ 3 ft (0.914 m)
Input Voltage, AC Power Supply	100 to 240 VAC2
Current	2 to 5A
Frequency	50/60 Hz
Input AC Power	200 to 400W (maximum)
Input Voltage, DC Power Supply	-48 to -60 VDC
Maximum Input Current	9.0A

Typical Input Current	3.0 to 4.0A
Input DC Power	200 to 400W (maximum)
Protection	Current limit, overpower, over temperature
Typical Output Power	350W
WAN Interface Options	Quad T1/PRI (RJ-45); Quad E1/PRI (RJ-45)
Auxillary Interfaces	- Console and Auxiliary Ports - Asynchronous serial (RJ-45)

Typical Input Current	3.0 to 4.0A
Input DC Power	200 to 400W (maximum)
Protection	Current limit, overpower, over temperature
Typical Output Power	350W
WAN Interface Options	Quad T1/PRI (RJ-45); Quad E1/PRI (RJ-45)
Auxillary Interfaces	- Console and Auxiliary Ports - Asynchronous serial (RJ-45)

Data Sheet - *Cisco* 3600 Series Multifunction Platform - Gatekeeper

H.323 Version 2 Support

H.323 Version 2 Support upgrades Cisco IOS software to comply with the mandatory requirements in the Version 2 specification. This upgrade enhances the existing Voice Over IP GateWay, the Multimedia Conference Manager (GateKeeper and Proxy), and the DTMF digital relay by using H.245.

DTMF is the tone generated on a touch-tone phone when you press keypad digits. The tones are compressed into a single stream at one end of a call and decompressed at the other end by using H.245 messages. However, doing this can lead to distortion, depending upon the CODEC used. Thus, the DTMF-relay is used to configure a method to transport DTMF tones generated after the call is established out-of-band. The three methods are:

- The standard H.323 out-of-band method uses H.245 to send digits as audible DTMF tones with voice; (the "h245-signal" option).
- The H.245 "alphanumeric" method (the "h245-alphaneumeric" option) also uses User Input Indication as part of a control channel, and is another standard H.245 transmission method.
- The "cisco-rtp" method sends the voice stream but with an identifier indicating that the DTMF tones are added.

H.323 Version 2 defines a lightweight registration procedure that requires full registration for initial registration, but uses an abbreviated renewal procedure to update the gatekeeper and minimize overhead. Lightweight registration requires each endpoint to specify a TimeToLive (TTL) value in its Registration Request (RRQ) message.

The H.323 Version 2 gateway supports the registration of fully-qualified E.164 numbers with the gatekeeper for phones connected directly to the gateway. Tunneling through H.225 User-to-User Information Element (UUIE) facilitates transparent handling of supplementary services between two endpoints through a

VoIP network. This eliminates the need to interpret various supplementary signaling messages in the VoIP gateways.

The H.323 Version 2 gatekeeper selects a destination gateway by choosing a gateway from among all gateways registered in a zone by allowing you to assign selection priorities to these gateways based on the dialed prefix. Gateway resource reporting allows the gateway to notify the gatekeeper when H.323 resources are getting low. The gatekeeper uses this information to determine which gateway it will use to complete a call and maintains a separate gateway list ordered by priority for each of its zone-prefixes.

Cisco 3600 Series Technical Specifications

Cisco 3600 Series Feature	Cisco 3640/3640A	Cisco 3620
Processor Type	100-MHz IDT R4700 RISC	80-MHz IDT R4700 RISC
Flash Memory	16 MB, upgradable to 32 MB	16 MB, upgradable to 32 MB
System Memory	32 MB DRAM, upgradable to 128 MB DRAM	32 MB DRAM, upgradable to 64 MB DRAM
Network Module Slots	Four slots	Two slots
Power	AC, DC, Redundant Power Option	AC, DC, Redundant Power Option
Dimensions (WxHxD)	17.5-in. x 3.44-in. x 15.75-in.	17.5-in. x 1.69-in. x 14.25-in.
Performance	50-70 kpps	20-40 kpps
Console and Auxiliary Ports (up to 115.2 kbps)	Yes	Yes
Rack and Wall Mounting	Yes	Yes
Dual Type II PC Card Slots	Yes	Yes

BIBLIOGRAFÍA

1. Comisión de Estudio 16 del UIT-T ,*UIT-T Rec. H.323 Sistemas de comunicación multimedios basados en paquetes*, 2000

2. The Internet Engineering Task Force - Network Working Group, *RFC 2616 - Hypertext Transfer Protocol - HTTP/1.1*, 1999

3. http://www.microsoft.com/spain/servidores/windowsserver2003/default.mspx (Windows Server 2003)

4. http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx (Windows Server 2003 Active Directory)

5. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/gktmpv31/howgktmp.htm#xtocid22 (Implementing an External Interface to the Cisco IOS Gatekeeper - Internet Call-Waiting

6. http://public.support.unisys.com/napcare/docs/icw/11_2/pdf/41789462-001.PDF (Internet Call Waiting)

7. http://www.cs.columbia.edu/sip/articles/Espi9912_Implementation.pdf (Internet Call Waiting con SIP / H.323)

8. http://www.eurescom.de/~pub-deliverables/P900-series/P909/D2/Annex2/InternetCallWaiting.doc (IN)

9. http://ftp.eurescom.de/~public-web-deliverables/P900-series/P909/services/icwdt/icwdt-components/dt-pir4.5.doc (IN)

10. ITU -T, *White Book - ISUP ITU R4*, 1993