- Telefonía IP y GNU/Linux: Asterisk la PBX open source -

Disertante: Fernando M. Villares

Temario a desarrollar

- Un poco de historia sobre la Telefonía…
- Generalidades sobre telefonía IP
- RTP y Protocolo SIP
- Telefonía IP y GNU/LINUX – Asterisk PBX
- IPSEC – VPN Conectividad Punto a Punto Remota
- Ejemplo de Interconexión segura mediante VPN
- Bibliografía

Un poco de Historia sobre la telefonía…

Un poco de historia sobre la telefonía…

La comunicaciones están al día de hoy en su 7ma. generación….

1era. Generación :
- *– Telégrafos*

2da. Generación :
- *– Telefonía analógica de switcheo manual*

3era. Generación :
- *– Telefonía analógica de switcheo mecánico*

4ta. Generación :
- *– Telefonía analógica de switcheo electrónico*

5ta. Generación :
- *– Telefonía PSTN DIGITAL – NGN*

6ta. Generación :
- *– Telefonía celular*

7ma. Generación :
- *– Telefonía Sobre Protocolo IP*

Generalidades Sobre Telefonía IP

Generalidades Sobre Telefonía IP – Un pantallazo Inicial

¿Qué es la Telefonía IP?

La telefonía IP o VoIP permite a los usuarios establecer llamadas de voz y fax sobre conexiones IP

En su origen, el Protocolo Internet se utilizó para el envío de datos, pero en la actualidad, y debido al importante desarrollo tecnológico que está experimentando este campo, disponemos de una tecnología que permite digitalizar la voz y comprimirla en paquetes de datos, que son enviados a través de cualquier moderno sistema de transmisión de datos para ser reconvertidos de nuevo en voz en el punto de destino.

Generalidades Sobre Telefonía IP – Un pantallazo Inicial

Redes de datos versus redes de voz

Redes de voz:

- concepto de conmutación de circuitos
- los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra

Redes de datos:

- concepto de conmutación de paquetes
- una misma comunicación sigue diferentes caminos entre origen y destino durante el tiempo que dura
- los recursos que intervienen en una conexión pueden ser utilizados por otras conexiones

El segundo tipo proporciona a los operadores mayor relación ingreso/recursos,

Generalidades Sobre Telefonía IP – Un pantallazo Inicial

Redes de datos versus redes de voz

Desventajas redes de datos:

- Transportan la información dividida en paquetes
- Estos paquetes pueden perderse
- No hay garantía sobre el tiempo que tardarán en llegar

Generalidades Sobre Telefonía IP – DIFERENCIAS

La telefonía hasta ahora :

Red de acceso que incluye:

- cableado
- red de transporte (ATM)
- La comunicación se lleva a cabo por conmutación de circuitos.

Los recursos destinados al desarrollo de una llamada telefónica no pueden ser utilizados por otra hasta que la primera no finaliza.

La telefonía IP

Red de transporte, que incluye:

- red basada en el protocolo IP, de conmutación de paquetes
- red de acceso, puede ser la misma que en el caso anterior, físicamente hablando (bucle de abonado).

Generalidades Sobre Telefonía IP – Equipamiento

Los elementos necesarios para que se puedan realizar llamadas de voz a través de una red IP:

Terminales IP o no IP:

- Entre los primeros está el teléfono IP, una pc, un fax IP.
- Entre los segundos está un teléfono convencional, un fax convencional a través de un ATA.

Si el terminal esta conectado a Internet de forma permanente, se les puede llamar en cualquier momento. Si es de forma no permanente vía módem, etc. no se les puede llamar si en ese momento no están conectados a Internet.

Generalidades Sobre Telefonía IP – Equipamiento

Gateway: Es el elemento encargado de hacer de puente entre la red telefónica convencional (PSTN) y la red IP.

Gatekeeper: Actúan en conjunto con varios Gateways, y se encarga de realizar tareas de autenticación de usuarios, control de ancho de banda, encaminamiento IP, etc. Es el núcleo de la red de telefonía IP.

Sip Proxy: Actúa como un switch y redirector ultrarrapido de llamadas con unas simples y pocas funciones en contraposición por ejemplo a Asterisk PBX donde se pueden switchear muchas menos llamadas por unidad de tiempo pero con cientos de funciones programables.

Generalidades Sobre Telefonía IP - Protocolos

- Existen múltiples protocolos de transporte de datos de VOIP cada uno con sus pros y sus contras:

1. **ITU H.323** – Muy usado pero antiguo y ampliamente superado en capacidades por nuevos protocolos
2. **IETF SIP** (session Initiation protocol) - Ampliamente utilizado y versátil permite gran cantidad de servicios extras.
3. **MCGP** - Praotocolo propietario de CISCO® utilizado ampliamente en sus sistemas de VOIP (requiere grandes costos por licenciamientos) Muy flexible y potente.
4. **IAX (inter-asterisk Protocol)** – Protocolo de muy bajo ancho de banda y alta calidad utilizado por sistemas de PBX IP asterisk que permite interconectar varias PBX en sites locales o remotos como si fuera una única central. Ideal para utilizar en enlaces de poco ancho de banda (xDSL, cable modem, etc)
5. **VOFR** - Protocolo de bajo nivel usado para transportar información de Voz Sobre enlaces Frame Relay

Generalidades Sobre Telefonía IP – VLANS y QoS

Existe un requisito indispensable para que la tecnología de VOIP funcione correctamente: ***QoS o calidad de servicio*** de punta a punta de la red

¿Que significa esto?

En una red de estándar la información de voz y video se transmite junto con el resto de los datos de una organización, si se llega a cierto volumen que logre saturar los enlaces, los paquetes de voz y video que son altamente sensibles al jitter y delay producirán una calidad de sonido e imagen inaceptables, esto se soluciona mediante el uso de equipamiento de red con soporte para QoS en capas 2 o 3 de OSI y/o separación de las redes mediante LANs virtuales en sus switchs / routers (VLAN's)

Generalidades Sobre Telefonía IP – Codecs

CODECS de VoIP y ancho de banda usado sin OVERHEAD IP

- **GSM** - 13 Kbps – Alta calidad (estándar red celular GSM)
- **iLBC** - 15Kbps: 13.3 Kbps – Alta calidad, alto uso de CPU
- **ITU G.711** - 64 Kbps, (*alaw/ulaw PCM*) Calidad estándar TECO
- **ITU G.722** - 48/56/64 Kbps – Alta calidad, casi igual que G711
- **ITU G.723.1** - 5.3/6.3 Kbps – Calidad Baja – Util para modems
- **ITU G.726** - 16/24/32/40 Kbps – Alta calidad
- **ITU G.728** - 16 Kbps – Media calidad / Alto uso de CPU
- **ITU G.729** - 8 Kbps, Media calidad – Muy usado
- **Speex** - 2.15 a 44.2 Kbps – Calidad Variable – Usa mucha CPU
- **LPC10** - 2.5 Kbps – Baja calidad – Poco Usado
- **DoD CELP** - 4.8 Kbps – Idem LPC10

Al uso de ancho de banda del codec debe sumarse aproximadamente 16kbps por cada canal de voz debido al overhead de encabezados RTP.

Generalidades Sobre Telefonía IP – Capacidades Teóricas

En una central analógica 1 llamada ocupa 1 canal, veamos como se comporta un sistema VoIP:

Usando como modelo 1 red FAST ETHERNET® de 100mbps FULL DUPLEX y teléfonos IP de calidad TECO a 64kbps con codec G711 y luego un codec de bajo ancho de banda a 8kbps como el G729

Capacidad total GATEWAY=200mbps/160kbps 1250 llamadas simult.

Capacidad total GATEWAY=200mbps/48kbps 4166 llamadas simult.

Como estadísticamente es poco probable que se usen todos los canales a la vez, (se usa el 30% aproximadamente si se estimó bien la red) esto significaría una capacidad de mas de 3750 internos en una red estándar sin compresión o mas de 12000 internos usando compresión G729.

Queda claro de esta forma la optimización y economía de uso de canales y recursos que trae aparejada esta tecnología.

RTP Y PROTOCOLO SIP

RTP Y PROTOCOLO SIP – RTP (real time protocol) -I-

- TCP no fue diseñado para transmitir este fin por lo que no cumple con las expectativas y necesidades de las nuevas aplicaciones.

- RTP es un protocolo que viene a llenar el vacío para la transmisión en tiempo real.

- RTP proporciona: transporte punto a punto p/redes uni o multicast

- RTP se creó específicamente para la transmisión de audio y vídeo, gracias a que incluye en su cabecera informaciones que sincronizan imagen y sonido, al tiempo que es capaz de determinar si se han perdido paquetes y si éstos han llegado en el orden correcto.

RTP Y PROTOCOLO SIP – RTP (real time protocol) -II-

` Las cabeceras del RTP también especifican el tipo de misión que realizamos, por lo que nos permiten diferentes tipos de compresión de datos.

RTP, define:

2 direcciones diferentes controladas desde dos puertos distintos, de forma que audio y vídeo viajan por separado controlados por el RTCP.

RSVP, tiene como objetivo añadir información feedback desde el cliente hacia el servidor para garantizar calidad de servicio.

No asegura entrega continua de información, ni de todos los paquetes, ni siquiera puede evitar la entrega desordenada

RTP Y PROTOCOLO SIP – RTP (Arquitectura)

Sesión: aplicaciones comunicandose con RTP identificadas por una dirección de red y dos puertos (RTP Y RTCP).

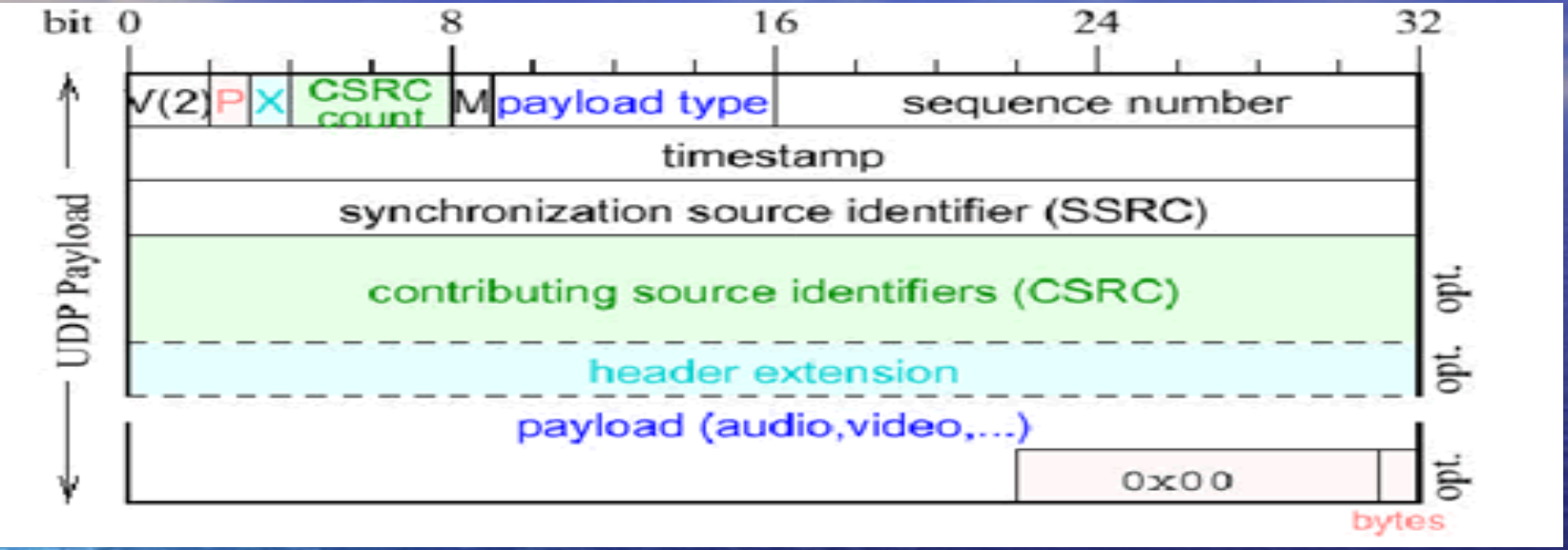
Transmisor: receptor y/o transmisor de datos, identificado con un valor de 32 bits único en la sesión (SSRC).

Stream: secuencia de paquetes originados por la misma fuente dentro de una sesión.

La transmisión debe ser controlada para el mejor flujo de información, esto se debe a que si el envío de información es muy rápida se pierden paquetes y si el envío es muy lento se pierde calidad, por lo que se crea un protocolo para controlar el flujo de la información. Además se establecen, por ejemplo, que la información que contiene un paquete debe ser equivalente a 20 ms de audio.

RTP Y PROTOCOLO SIP – RTP (Arquitectura)

El paquete RTP tiene el siguiente formato:



- *Payload Type: tipo de información contenida*
- *SSRC: identificador de sincronización*
- *Sequence number: para detectar pérdida*
- *P: padding (para encriptar)*
- *M: market bit, indica comienzo de frame para delay*
- *CC: counter source count (para mezclas)*
- *CSRC: lista de identificadores en mezclas*
- *Payload: la información*

RTP Y PROTOCOLO SIP – RTCP (real time control protocol)

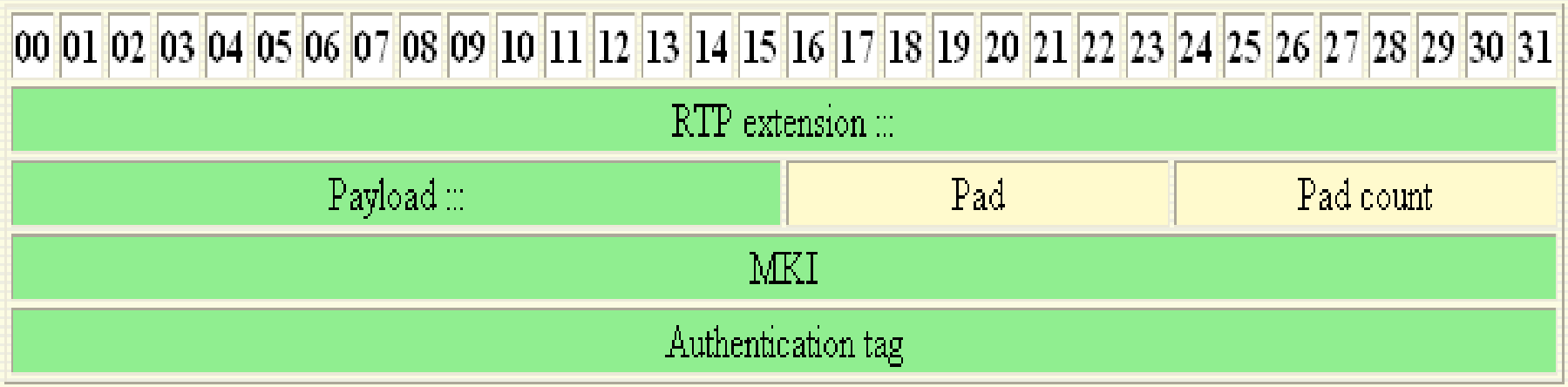
RTCP header:

RTCP permite mantener información de control sobre RTP, la idea es reservar y garantizar la calidad de servicio. Cuenta con varios tipos de paquetes:

- Sender Report: paquetes emitidos, datos para sincronización de varios streams.
- Receiver Report: paquetes perdidos, último recibido, timestamp para RTT
- Source Description: Canonical Name (CNAME), email, etc.
- Bye
- Específicos de la aplicación

RTP Y PROTOCOLO SIP – SRTP (secure real time protocol)

SRTP header:



MKI: usado para la adm. de claves.

AUTHENTICATION TAG: usado para llevar la información de autenticación

RTP Y PROTOCOLO SIP – SIP (session initiation protocol)

SIP (Protocolo de Inicio de Sesión): protocolo de señalización de Voz sobre IP adoptado en 1999 por la Fuerza de Trabajo de Ingeniería de Internet (IETF).

El protocolo es muy simple, muy similar a HTTP.

Características:

SIP es fácil de aprender y usar.

Diseñado para ambientes distribuidos.

Es un protocolo "liviano".

RTP Y PROTOCOLO SIP – SIP (session initiation protocol)

En el protocolo SIP al igual que en HTTP, los mensajes contienen encabezados y un cuerpo o contenido. Los contenidos de mensajes SIP para llamadas telefónicas son definidos por el protocolo SDP (sesion description protocol).

SIP es un protocolo basado en texto que usa codificacion UTF-8
SIP usa el puerto 5060 en UDP y TCP. Usa RTP como protocolo de transporte pero puede ser usado con cualquier transporte que se desee.

SIP ofrece todos los servicios típicos de la telefonia de nueva generación asi como la capacidad futura de ser expandido para ofrecer nuevos servicios a futuro.

TELEFONIA IP y GNU/LINUX: ASTERISK (*) THE OPEN SOURCE PBX

Telefónia IP y GNU/LINUX – Características de Asterisk PBX

Asterisk ofrece las funciones propias de las PBX clásicas y además características de avanzada, pudiendo trabajar tanto con sistemas de telefonía estándar tradicionales como con sistemas de Voz sobre IP puros así como con interconexión de centrales remotas, planes de numeración únicos y más.

Las centrales Asterisk tienen características que sólo ofrecen los grandes sistemas PBX propietarios como Correo de Voz, Conferencias, Colas de llamadas, Registros de llamada Detallados, Caller ID y decenas de funciones mas.

Telefonía IP y GNU/LINUX – Arquitectura de Asterisk PBX

Asterisk fue diseñado cuidadosamente para obtener la maxima flexibilidad posible. Esta conformado por API`s específicas definidas alrededor de un núcleo central de PBX Este núcleo maneja todas las interconexiones internas de la PBX abstrayendose totalmente de protocolos específicos, codecs, e interfases de hardware provenientes de las aplicaciones de telefonía. Todo esto permite a Asterisk usar todo tipo de hardware y tecnologías disponibles hoy o en el futuro para realizar sus funciones esenciales, conectar hardware y aplicaciones

Internamente el núcleo maneja estas tareas:

- **PBX Switching**
- **Lanzador de aplicaciones**
- **Traductor de Codecs**
- **Programación de tareas y Administración de I/O**

APIs de Carga de Módulos :

Existen 4 APIs definidas para carga de módulos, facilitando la abstracción de hardware y protocolos. Usando este sistema modular de carga el núcleo de asterisk no tiene que preocuparse de detalles tales como: que codecs están en uso, como se establece una llamada, etc.

- **API de CANALES**
- **API de aplicaciones**
- **API de traducción de Codecs**
- **API de manejo de Archivos**

*Telefonía IP y GNU/LINUX – AGI (* gateway interface)*

AGI (Interfaz de gateway asterisk): es una interfase para agregar funcionalidades a Asterisk por medio de diferentes lenguajes de programación como ser Perl, PHP, C, Pascal, Bourne Shell, Java, etc, todo depende de lo que uno decida

AGI puede controlar el plan de numeración (dialplan) ubicado en /etc/asterisk/extensions.conf

EAGI le da a la aplicación la posibilidad de acceder y controlar canales de sonido además de interaccionar con el plan de numeración

deadagi da acceso a un canal muerto, luego de colgar por ejemplo

Por motivos de debugging se puede tipear "agi debug" en el CLI.

Telefonía IP y GNU/LINUX – AGI (* gateway interface)

Si una aplicación AGI disca al exterior dicho script retoma la ejecución del plan de numeración y pierde contacto con el server *. Sigue procesandose en background por si mismo y es libre de ejecutar limpieza de canales y procesamiento post-discado

Se pueden además iniciar llamadas sin pasar por el plan de numeración:

Asterisk AUTO DIAL OUT: Mueve (no copia) un archivo dentro del directorio de spool de * y se realiza una llamada
Asterisk MANAGER API: Usa el comando *Originate*

Forma de uso: AGI(script.agi|arg1|arg2|..).

Telefonía IP y GNU/LINUX – PROTOCOLO IAX2

Después de que Mark Spencer creara Asterisk, la PBX open source, comenzó a ver cómo la falta de simplicidad de los protocolos de VoIP podría ser una gran barrera para el mercado, por lo que se le ocurrió crear un nuevo protocolo llamado IAX (Inter Asterisk eXchange)

Objetivos protocolo IAX:

- minimizar ancho de banda necesario para señalización y el medio,
- proporcionar soporte interno para trasparencia en la traducción de direcciones de red (NAT)
- permitir escalabilidad para futuras mejoras de funcionalidades.

Telefonía IP y GNU/LINUX – PROTOCOLO IAX2

- IAX2 no usa "Real-time Protocol" (RTP),
- IAX utiliza "User Datagram Protocol" (UDP) sobre un único puerto de Internet (4569) para transmitir y recibir la señalización y el medio,
- Usando codec g729 a través de protocolo IAX se pueden efectuar al menos 103 llamadas a través de 1Mbit de ancho de banda simétrico.
- A su vez en vez de "parsear" comandos de texto como el protocolo SIP, IAX utiliza solamente datos binarios para simplificar la comunicación entre sistemas.

Telefonía IP y GNU/LINUX – PROTOCOLO IAX2

- Las respuestas del protocolo IAX se envían de vuelta desde cualquier dirección IP (privadas o públicas) , si se cae de repente el enlace, el dispositivo IAX se percata en menos de 1 minuto.

- Toda la señalización tiene lugar dentro de la capa 2 de datos.

- El protocolo IAX transmite los paquetes de audio con tan sólo 4 bytes de cabecera y los comandos emplean un ancho de banda muy reducido.

Telefonía IP y GNU/LINUX – Capacidades del protocolo IAX

CONEXIONES INTER-CENTRALES A TRAVÉS DE IAX®:

Dependiendo del equipo a elegir y la cantidad de troncales e internos a compartir así como de la capacidad de los enlaces de interconexión disponibles, se pueden establecer interconexiones de centrales y unificación de Rutas de menor costo e internos en la cantidad especificada en la siguiente tabla:

Usando codecs calidad TECO G711 con IAX:

- **1er. Llamada – 80kbps**
- **2da. Llamada y de allí en más – 64kbps cada una**

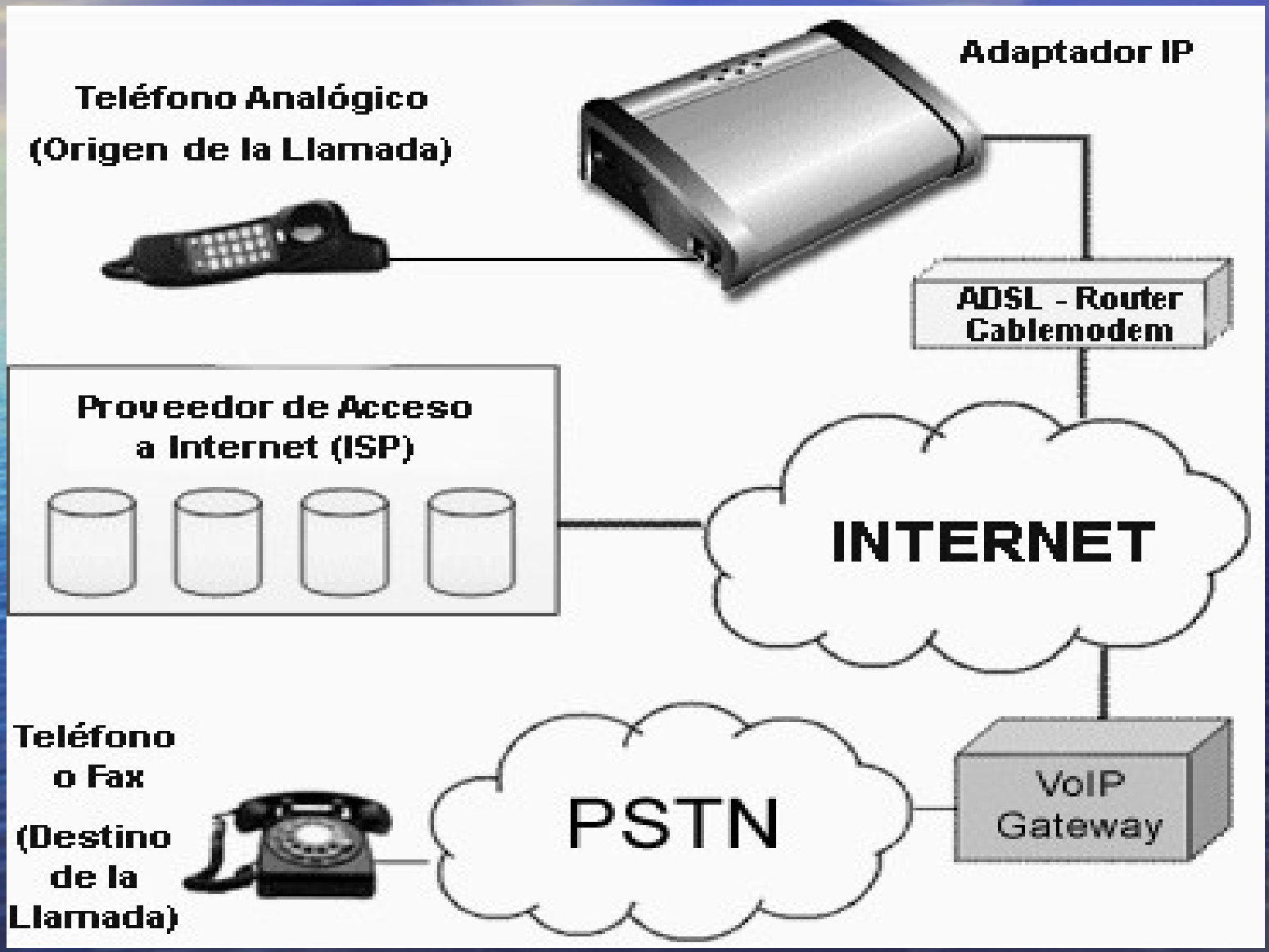
Cantidad de llamadas simultáneas por Megabit máximas: 15

Usando codecs de media calidad y bajo ancho de banda G729

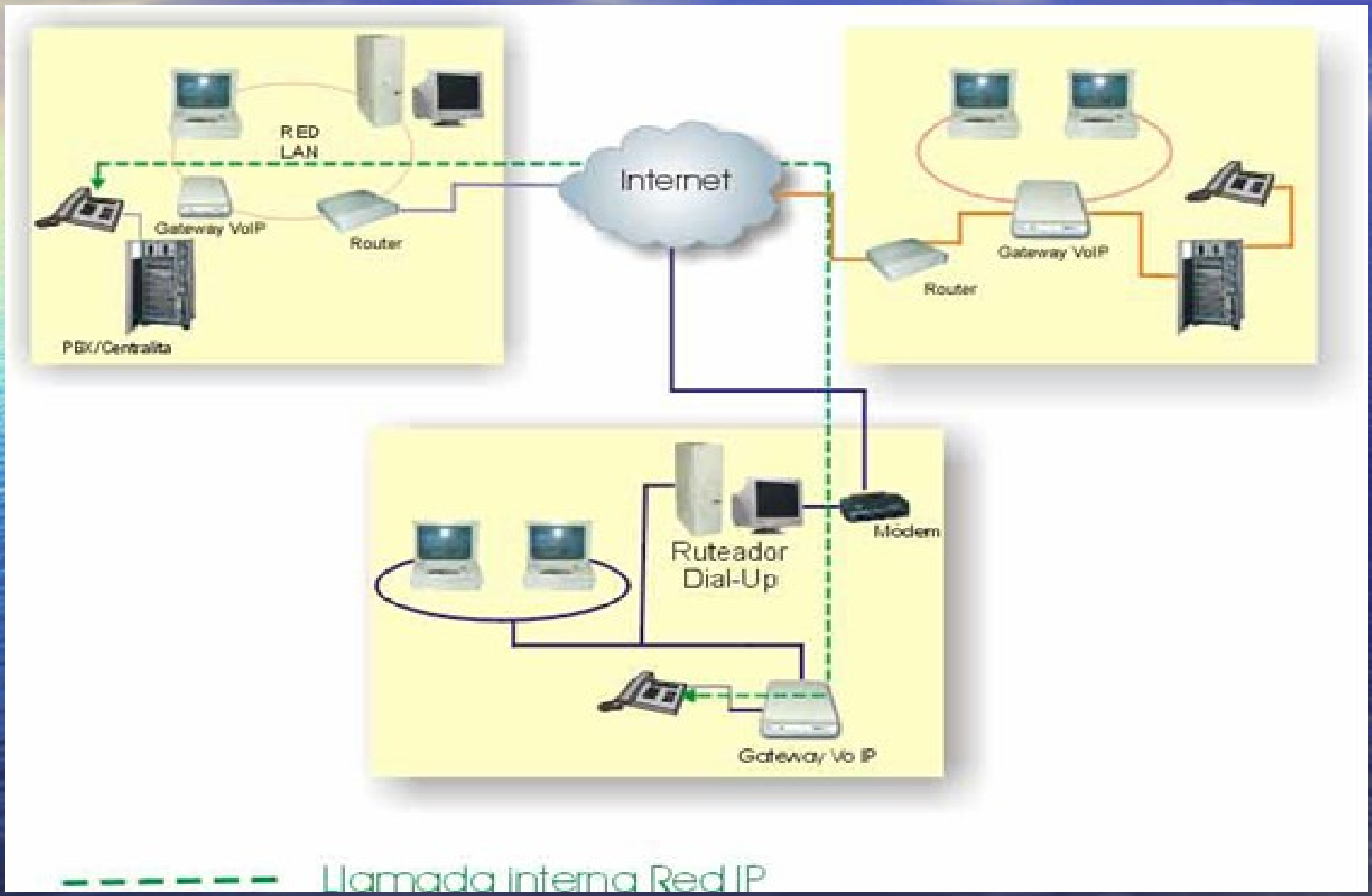
- **1er. Llamada – 24kbps**
- **2da. Llamada y de allí en más – 8kbps cada una**

Cantidad de llamadas simultáneas por Megabit máximas: 125

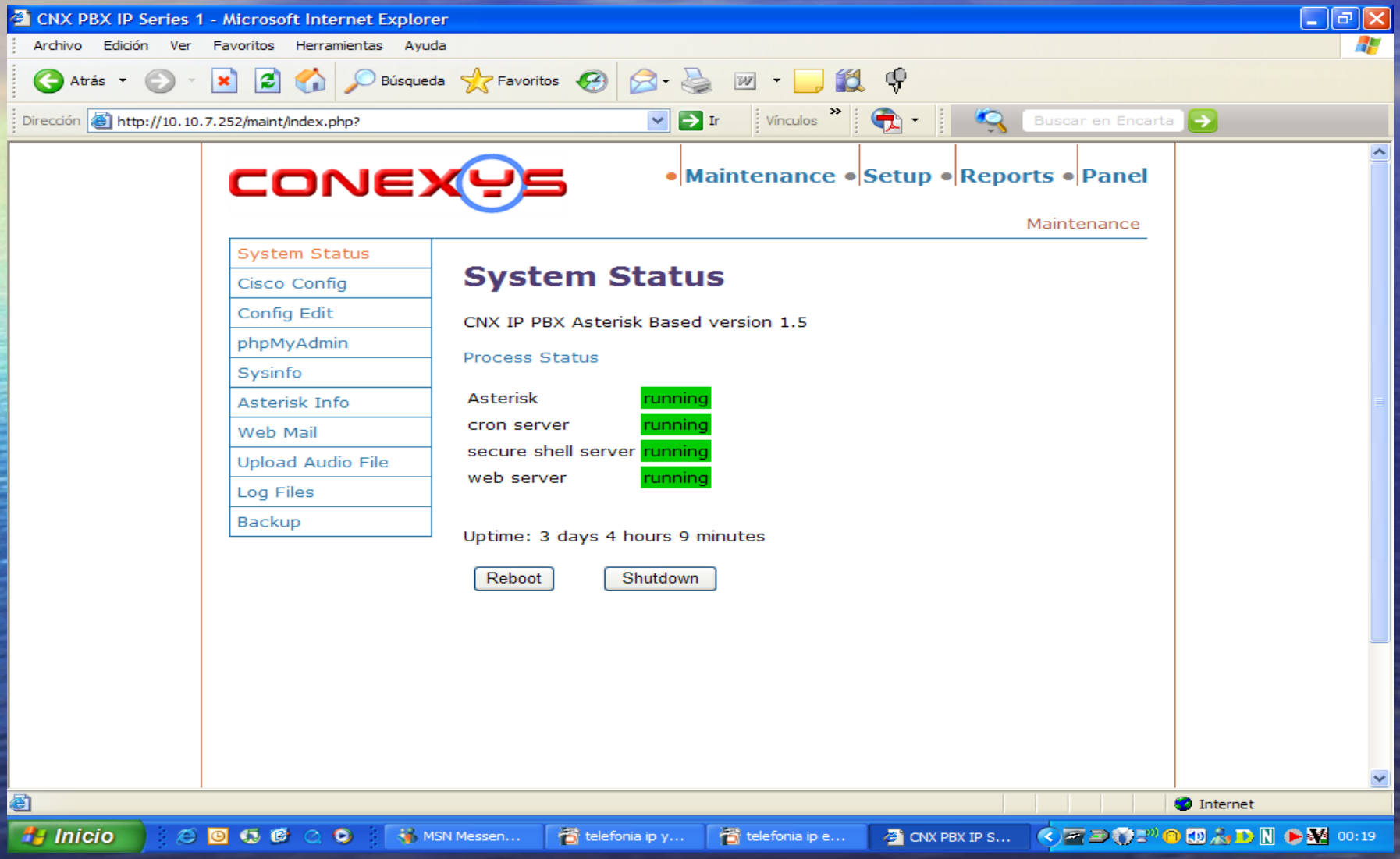
Esquema modelo Provider VoIP, Oficina Remota



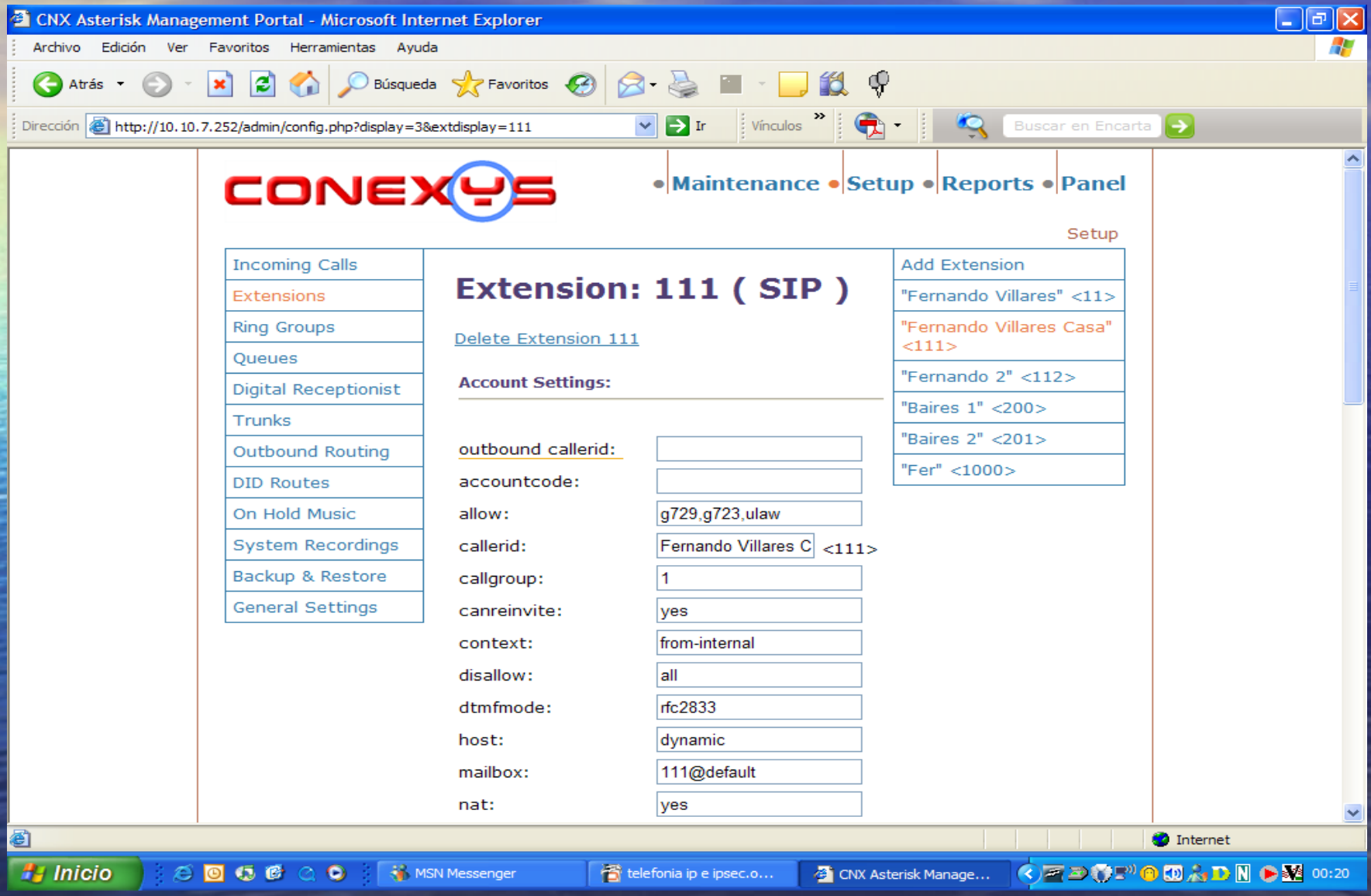
Esquema modelo interconexión de Centrales o sucursales



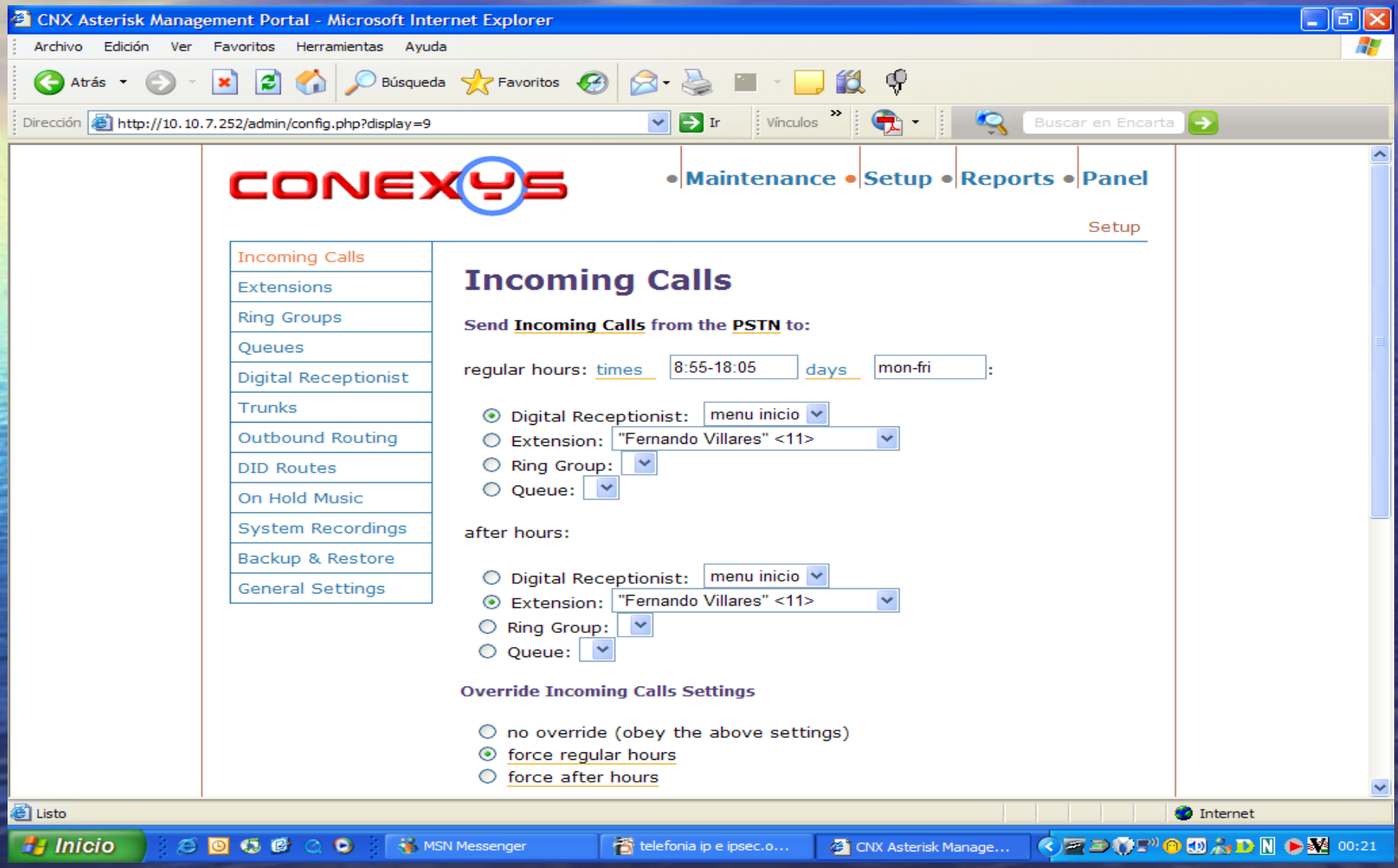
Pantallas de configuración de una CENTRAL ASTERISK



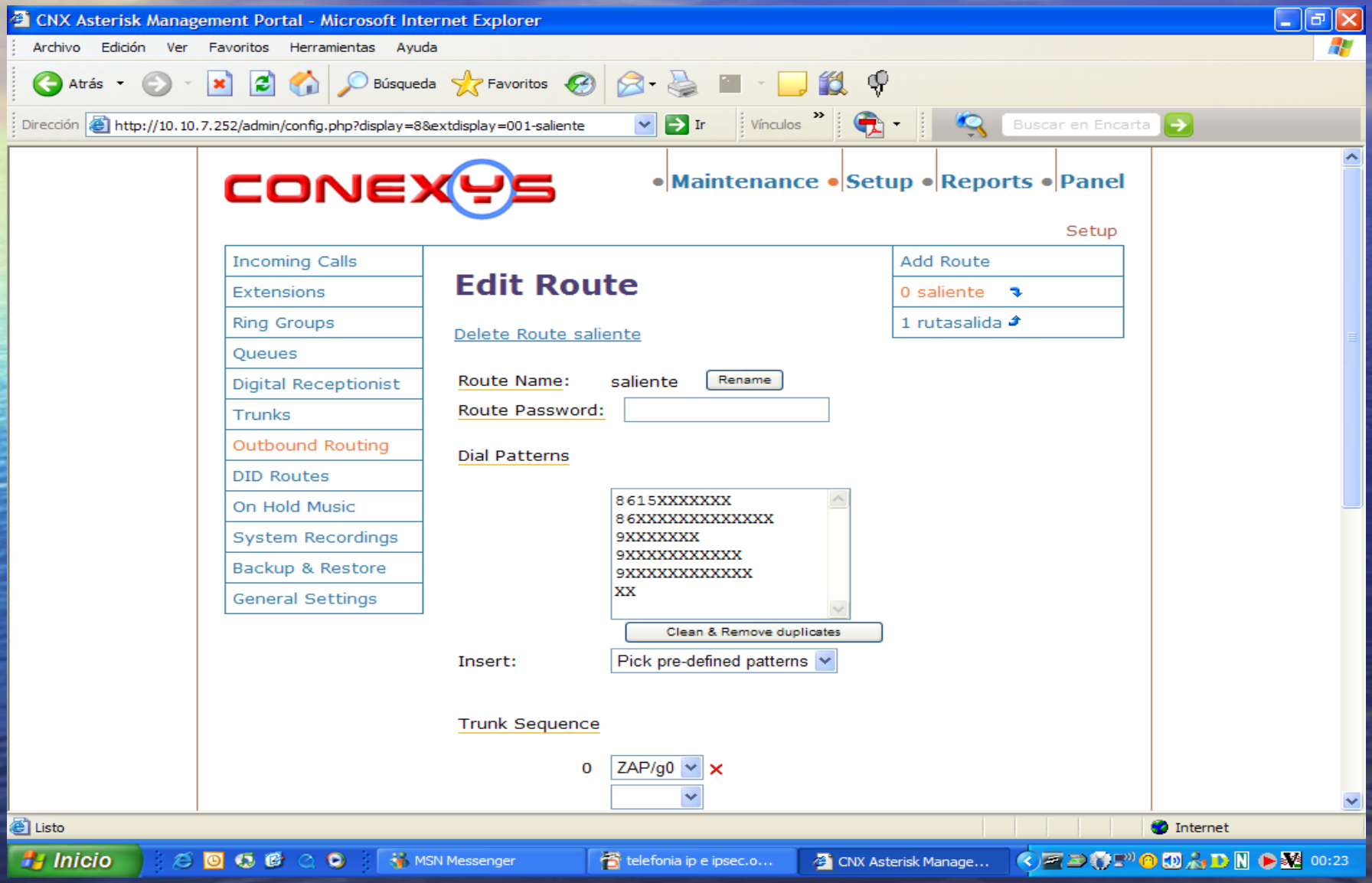
Pantallas de configuración de una CENTRAL ASTERISK



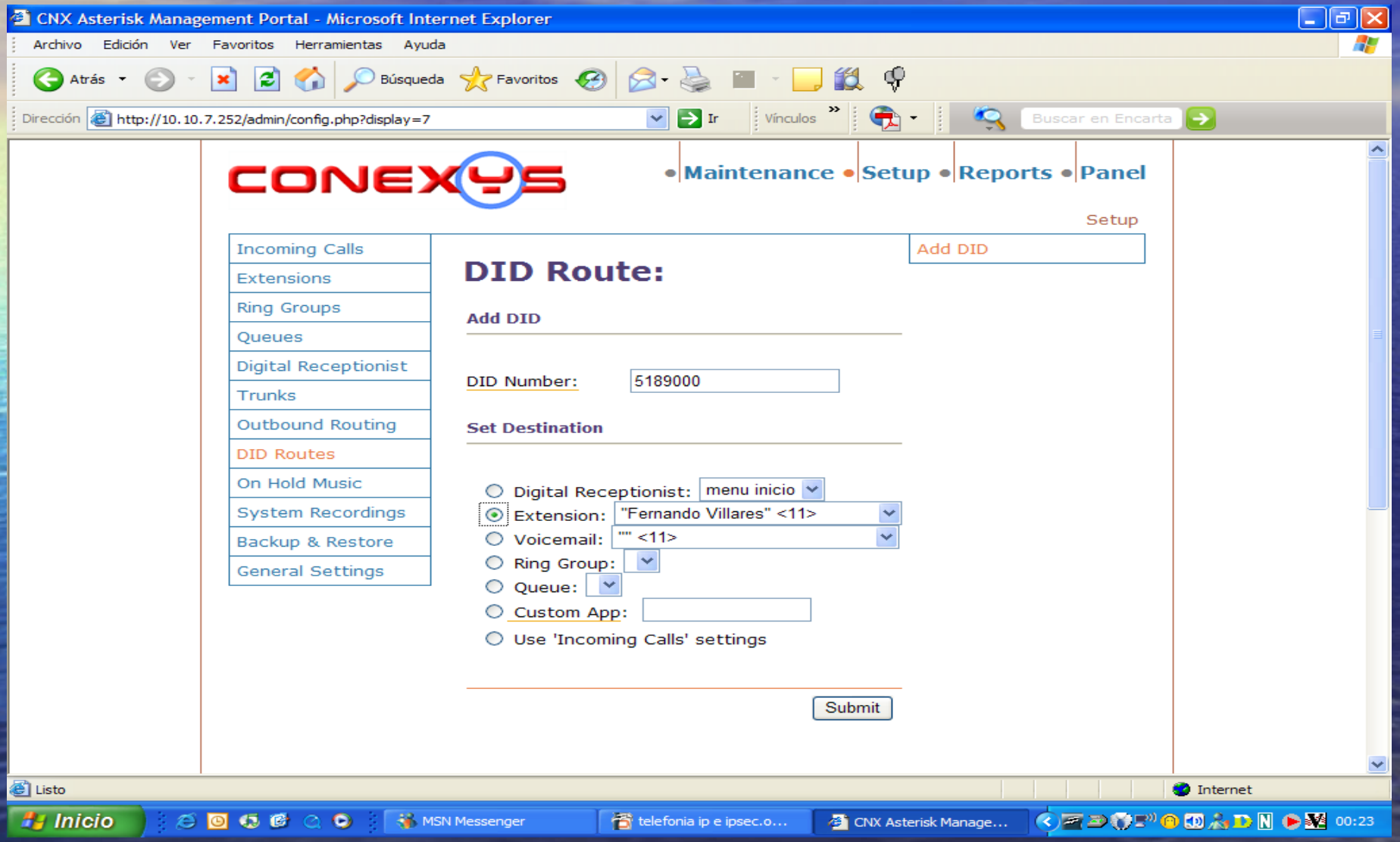
Pantallas de configuración de una CENTRAL ASTERISK



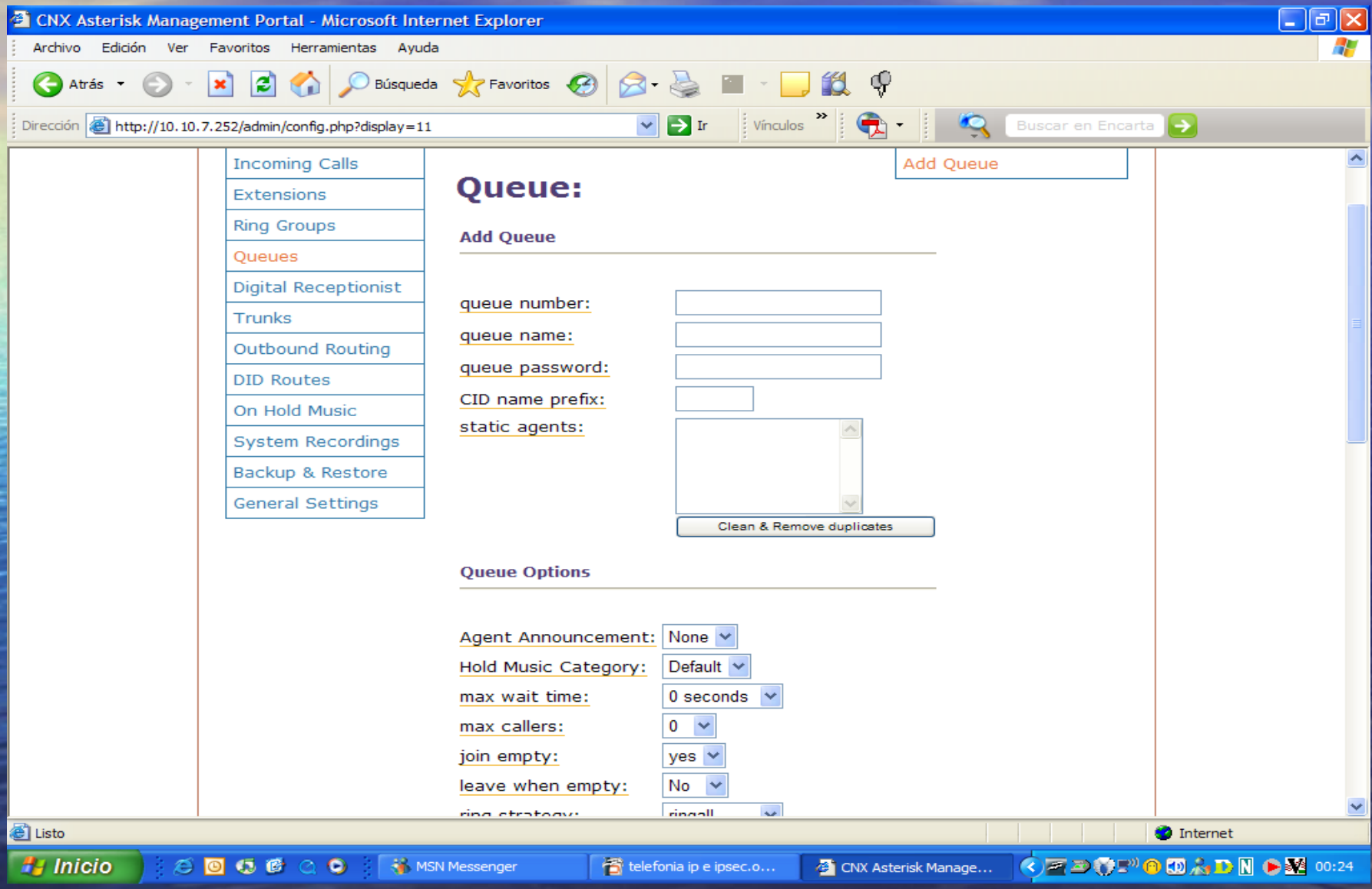
Pantallas de configuración de una CENTRAL ASTERISK



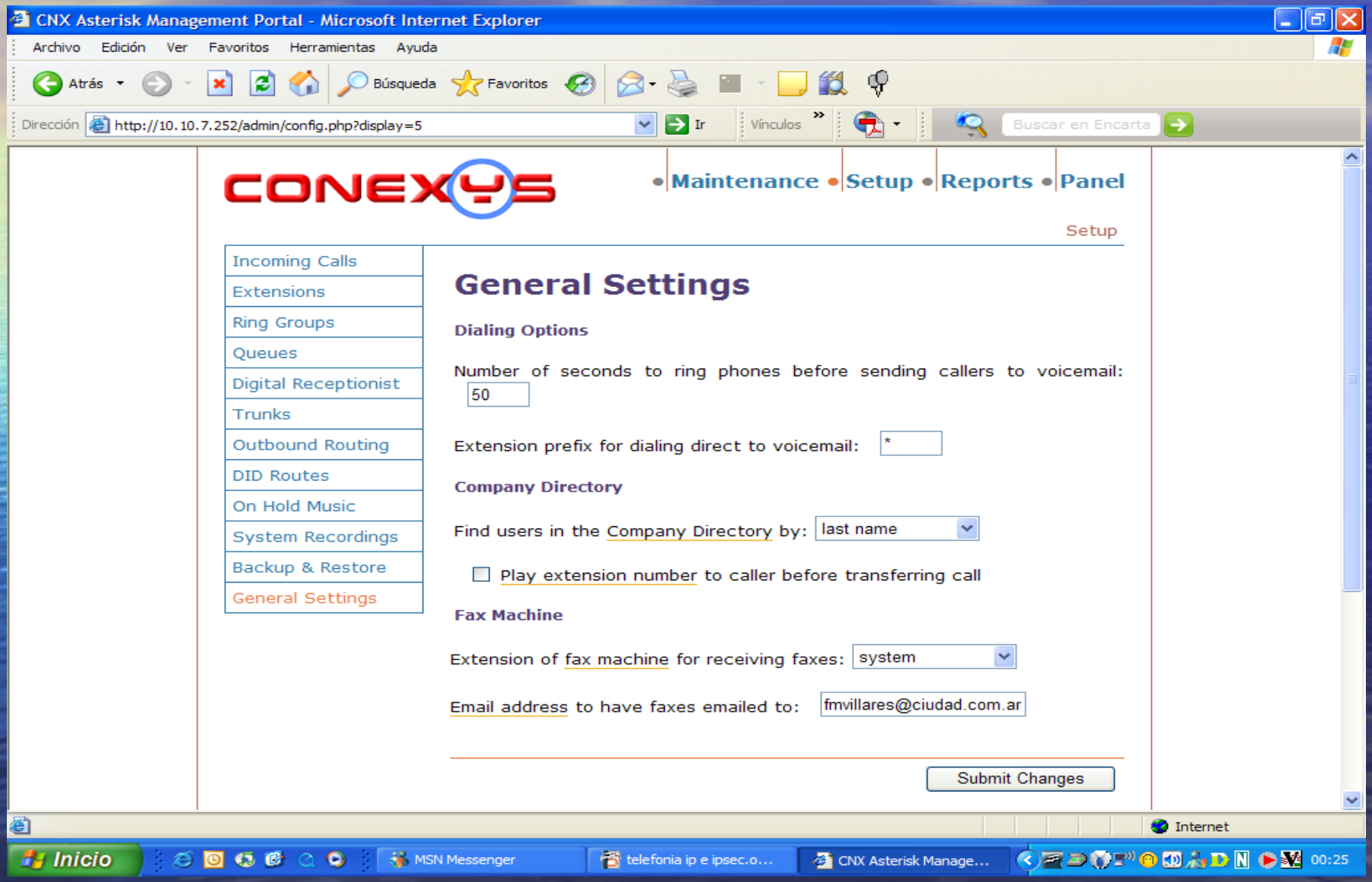
Pantallas de configuración de una CENTRAL ASTERISK



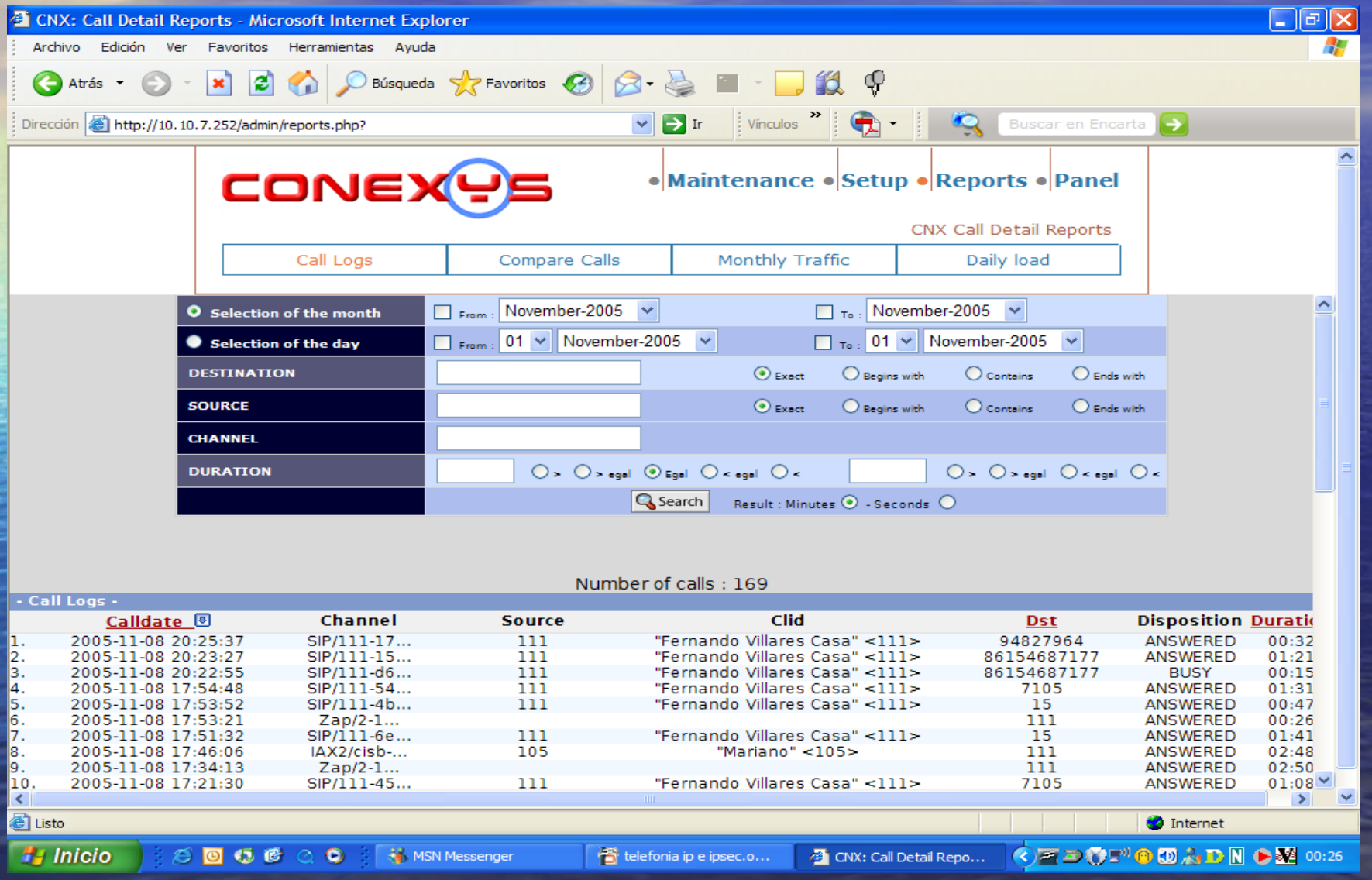
Pantallas de configuración de una CENTRAL ASTERISK



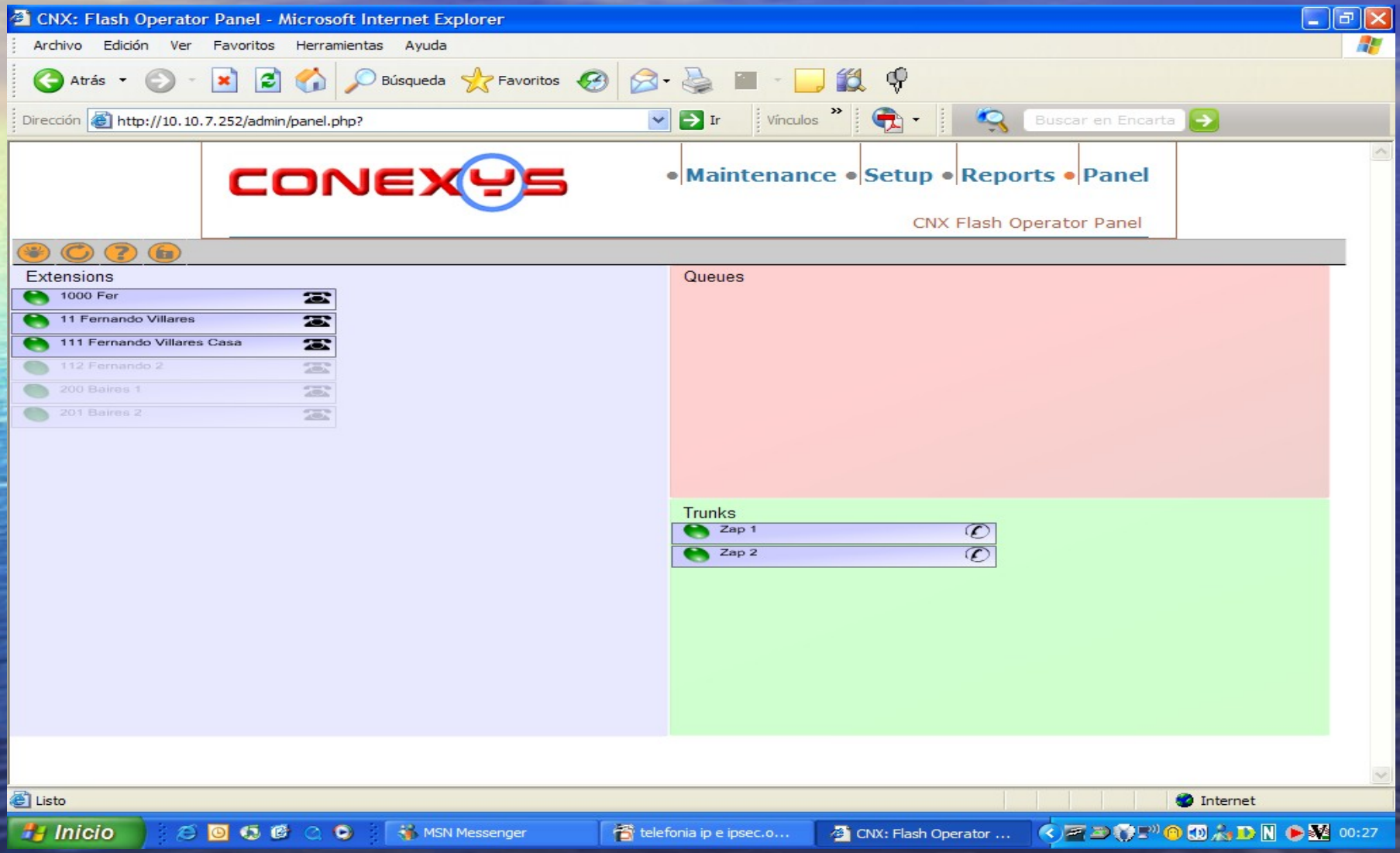
Pantallas de configuración de una CENTRAL ASTERISK



Pantallas de configuración de una CENTRAL ASTERISK



Pantallas de configuración de una CENTRAL ASTERISK



CONECTIVIDAD PUNTO A PUNTO REMOTA

VPN (mecanismos de cifrado y firma digital)

¿Que es una VPN? (virtual private network)

► ***Una VPN es una forma de conectar una o mas redes privadas preexistentes por medio de una red pública como Internet, de tal manera que la red parezca una sola desde el punto de vista de los usuarios.***

► ***Según las siglas la red es Virtual porque para los usuarios es como una única red y es Privada porque la comunicación a través de ella es segura y está protegida***

¿ Para qué se usa ?

► *Un escenario típico de uso de VPN es en una Empresa que tiene una serie de usuarios remotos a los que desea permitirle el acceso a sus servicios corporativos.*

► *Si esto fuera la única necesidad de la empresa, no hace falta VPN, la solución podría plantearse con tecnologías de Firewalls o Proxys. Por cualquier tipo de acceso (dial-up por ejemplo)*

► *¿ Ahora bien, que mas permite una VPN ?*

► *Una conexión Segura, y esto se logra cumpliendo estos cuatro requisitos:*

Requisitos de una VPN

- ***Confidencialidad***
- ***Autenticación***
- ***Integridad***
- ***No repudio***

Ventajas de las VPN

Utilizando VPN se Logra:

- *Ahorro en los costos de comunicaciones dedicadas*
- *Ahorro de costos operativos*
- *Entorno de trabajo independiente de trabajo de tiempo y lugar a un costo reducido*
- *Los servicios de la compañía están disponibles siempre*
- *Compartir Servicios con socios*

Otras ventajas de las VPN

- *Los servicios de la compañía están disponibles siempre, desde cualquier sitio del mundo los usuarios pueden utilizar los atributos de LAN de la Compañía (impresoras, archivos, etc.)*

- *Compartir Servicios con socios: una compañía puede ofrecer a sus socios bajo un ambiente controlado y seguro, información común a ambas entidades.*

¿ Que es la Criptografia ? (I)

► *La Criptografía se encarga de proteger los datos que son transportados o traficados a través de una red pública o red no confiable*

Red Pública: Ej. Internet

Red No confiable: Ej. Redes Wireless con encriptación WEP o WPA estándar

¿ Que es la Criptografia ? (II)

► *Criptografía: convierte datos o mensajes en algo ininteligible para terceros, por medio de una clave, permitiendo a receptores autorizados, con la misma recuperar el mensaje original.*

► *Encriptador o cifrador: es un sistema encargado de realizar la encriptación.*

¿ Qué es una Clave ?

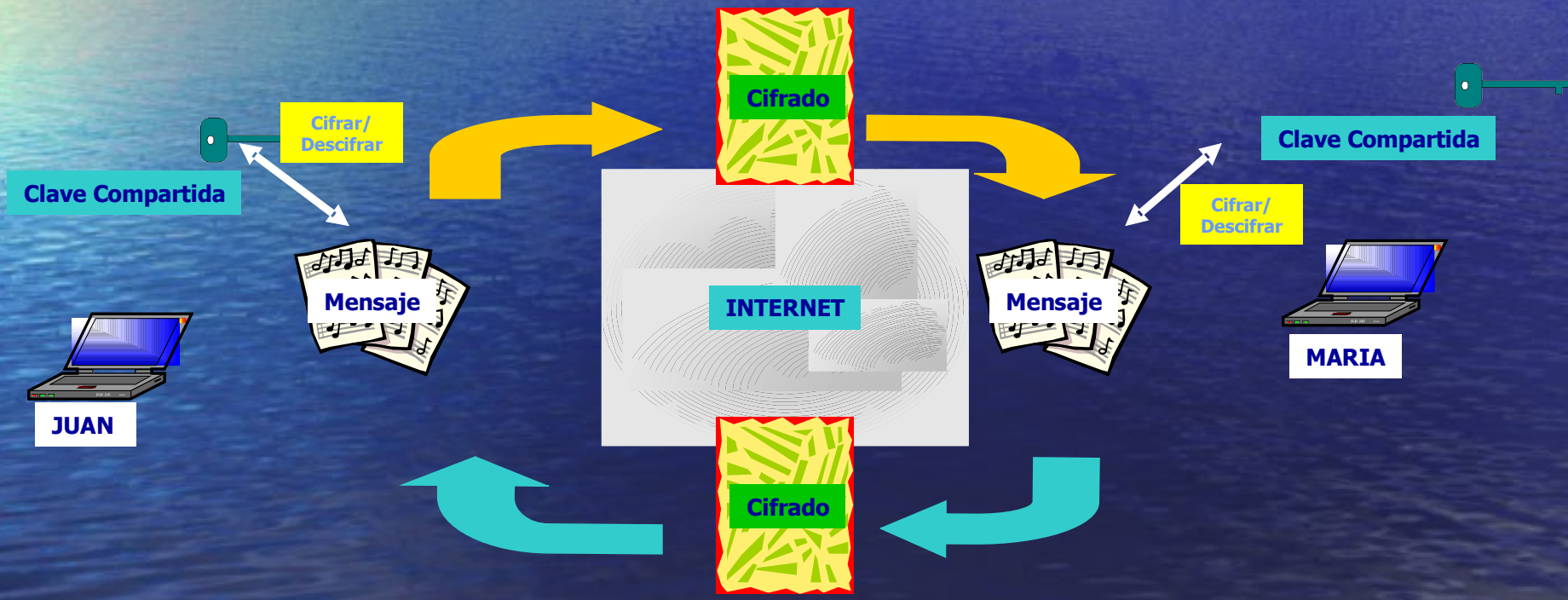
Es un dato de entrada a un algoritmo, que en conjunto
con el mensaje, produce una salida única.

Tipos de claves

- Claves de un solo uso.
- Claves Simétricas.
- Claves Asimétricas.

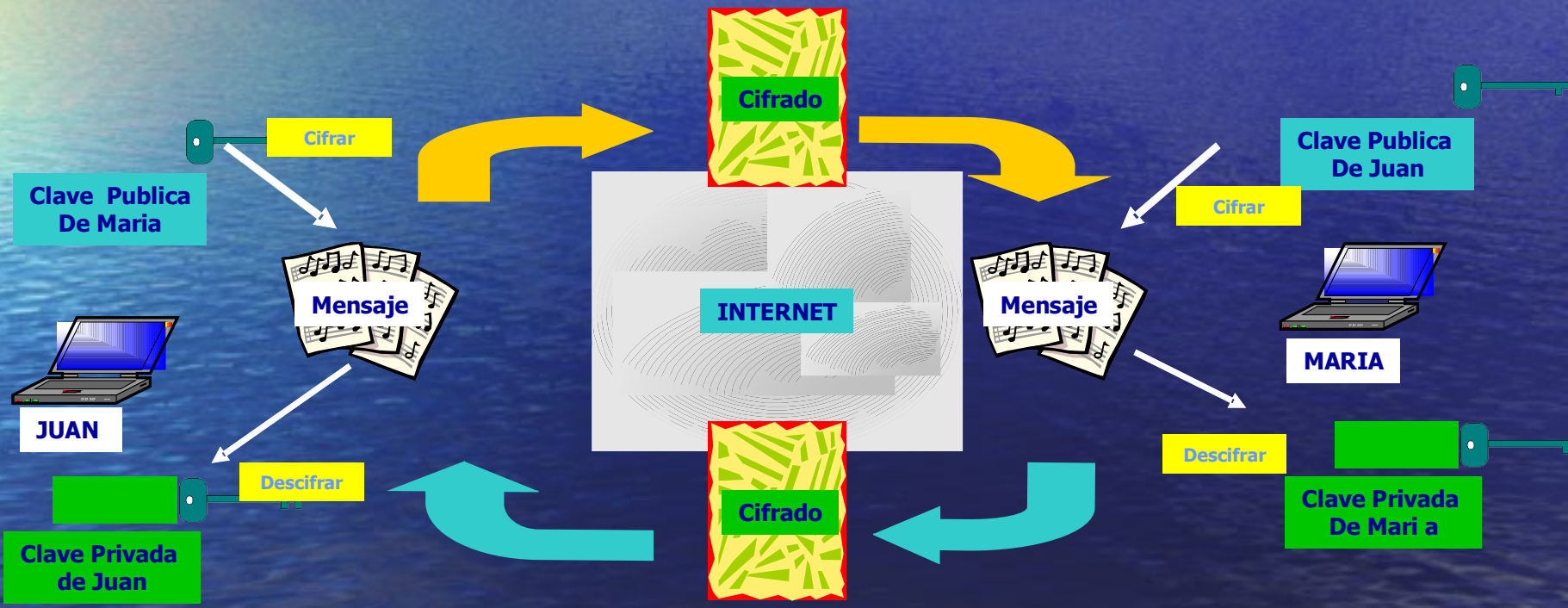
Tipos de claves

► Claves Simétricas: La misma clave es usada al iniciar el proceso de cifrado en origen y el de descifrado en destino.



Tipos de claves

► Claves Asimétricas: Claves diferentes son usadas para Cifrar y descifrar mensajes



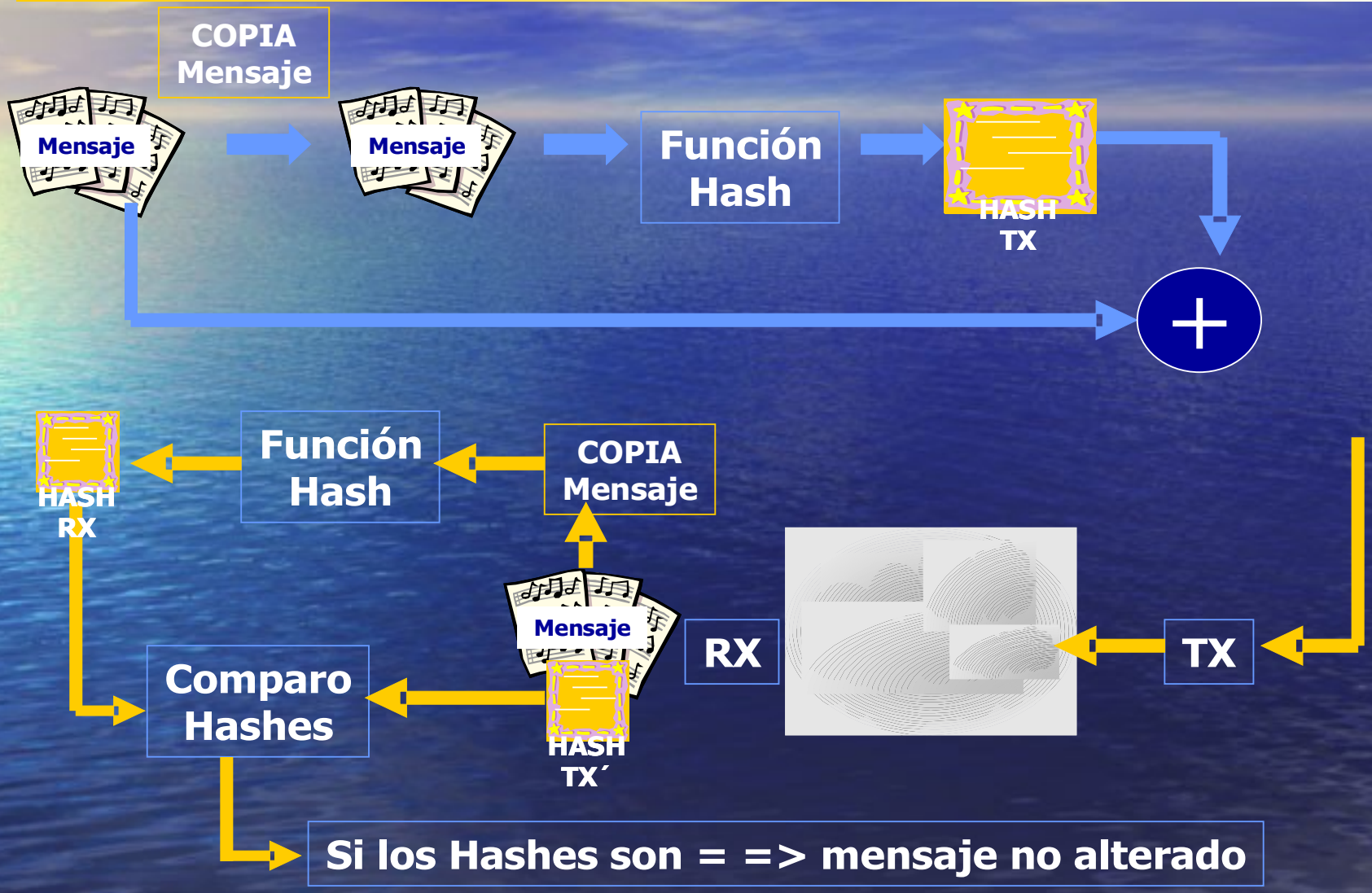
Funciones Hash

Que es un Hash?

Es una función o algoritmo matemático que se le aplica a un argumento (mensaje), y arroja como resultado un valor ÚNICO, Denominado Hash, si bien puede ser conocido el algoritmo con el que se creo un Hash, la función inversa de un Hash no devuelve nunca el MENSAJE ORIGINAL.

Ej. Grafico: Fruta → Licuado → Jugo de fruta

Que función Cumple el Hash



Algoritmos de Cifrado mas conocidos

Dentro de los algoritmos usados con IPSec:
DES: algoritmo de cifrado con claves 56 bits
3DES: algoritmo de cifrado con claves 168 bits (3 veces DES)
Otros: AES, RSA,Lucifer, RC2, RC4, RC5, GOST, IDEA, FEAL, REDOC, 3Way, TwoFISH, BlowFish, etc

Vulnerabilidades DES-3DES

Con ataque por fuerza bruta: en 3hs con Pentium IV se puede quebrar una DES

Con segmentación de claves con 1 millón de Pentium IV se puede quebrar una 3DES en 10.000 de años.

Algoritmos de Hash

- MD5 (Message Digest V5) El mas antiguo.

- SHA (Secure Hash Algorithm) Mas nuevo y mas seguro.

- HMAC (Hash- based Message Authentication Code) Adiciona una clave junto al mensaje en el proceso de Hashing.

IPsec, utiliza HMAC-MD5 y HMAC-SHA en todo el proceso de Hashing.

Orígenes de IPSEC

- *1994, RFC 1636 del IAB (Internet Arquitectura Board), en Paper "La Seguridad en la Arquitectura de Internet"*

Aquí se identificaron:

- *Intrusión no autorizada*
- *Control de Tráfico*
- *Encriptación o Cifrado*
- *Autenticación*

IPSEC

- *IPsec es un acrónimo de IP Security*
- *Objetivo: brindar seguridad y autenticación para las comunicaciones IP.*
- *IPSec brinda seguridad en niveles de capa 3 y 4 del modelo OSI*
- *Existen dos modalidades de Ipsec: Transporte y Tunneling*

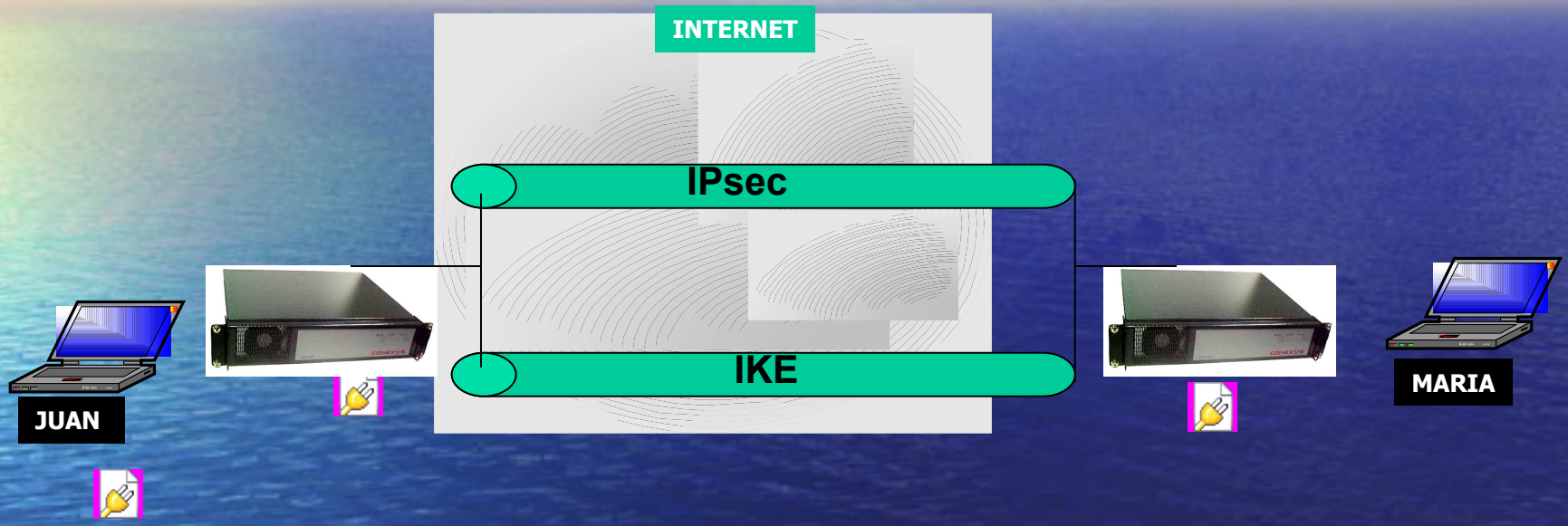
Servicios de IPsec

- *AH, Authentication Header, garantiza la autenticación de la cabecera*
- *ESP, Encapsulating Security Payload, autenticación y cifrado.*
- *IKE: Garantiza el Intercambio seguro de claves*

Integrantes del IPsec

- *Cifrado: DES, 3DES, AES, BlowFish (data encription standard- advanced encription standard)*
- *Integridad/veracidad: IKE (internet key exchange), X.509v3 (certificados digitales), SHA-MD5, RSA/DSS*
- *Transporte: AH/ESP (authentication header, encapsulating security payload), Tunneling, Transport.*

IKE: Internet Key Exchange



IKE es el mecanismo de intercambio de claves VPN. Aborda los temas de seguridad usando los métodos mencionados en los RFC 2407, 2408 y 2409. gestiona el intercambio de claves criptográficas que normalmente se deberían gestionar a mano. Para ello hace uso de un proceso en dos fases para establecer parámetros de IPSec entre dos nodos.

IKE: Internet Key Exchange

Fase 1 - Los dos extremos de conexiones establecen un canal seguro, autenticado, sobre el cual se comunican (Asociación de Seguridad SA) Utiliza claves asimétricas de sesión utilizando el algoritmo de Diffie - Hellman

Métodos usados

Modo Principal: envía la información de autenticación en una cierta secuencia, al tiempo que provee protección para la identidad.
Modo Agresivo. toda la información sobre autenticación se envía al mismo tiempo. Sólo debería usarse cuando no tengamos ancho de banda.

Fase 2 - Las Asociaciones de Seguridad se negocian en nombre de IPSec. La fase 2 establece túneles entre hosts IPSec. El Modo Rápido se usa en la fase 2 porque no es necesario repetir una autenticación total ya que la fase 1 ya ha establecido las SA.

Cabeceras IP Modo transporte y Modo Túnel

- ***TRANSPORTE***

- ***TUNEL***

Conectividad InterAsterisk - VPN y QoS con software Libre

En particular por cuestiones de seguridad, realmente creo necesario establecer, para conectar 2 PBX asterisk una VPN entre los 2 sites, una vez realizado este paso, la interconexión de los 2 planes de numeración es realmente muy simple como veremos en este ejemplo:

En el (serverA)
Archivo /etc/asterisk/iax.conf

[general]
register => <user>:<password>@<serverB IP>
[serverB]
type=friend
user=<user>
secret=<password>
host=<serverB IP>

Archivo /etc/asterisk/*extensions.conf*
exten => _7XXX,1,Dial(IAX2/serverB/${EXTEN:1},30,r)
exten => _7XXX,2,Congestion

Conectividad InterAsterisk - VPN y QoS con software Libre

En el (serverB)

Archivo /etc/asterisk/*iax.conf*

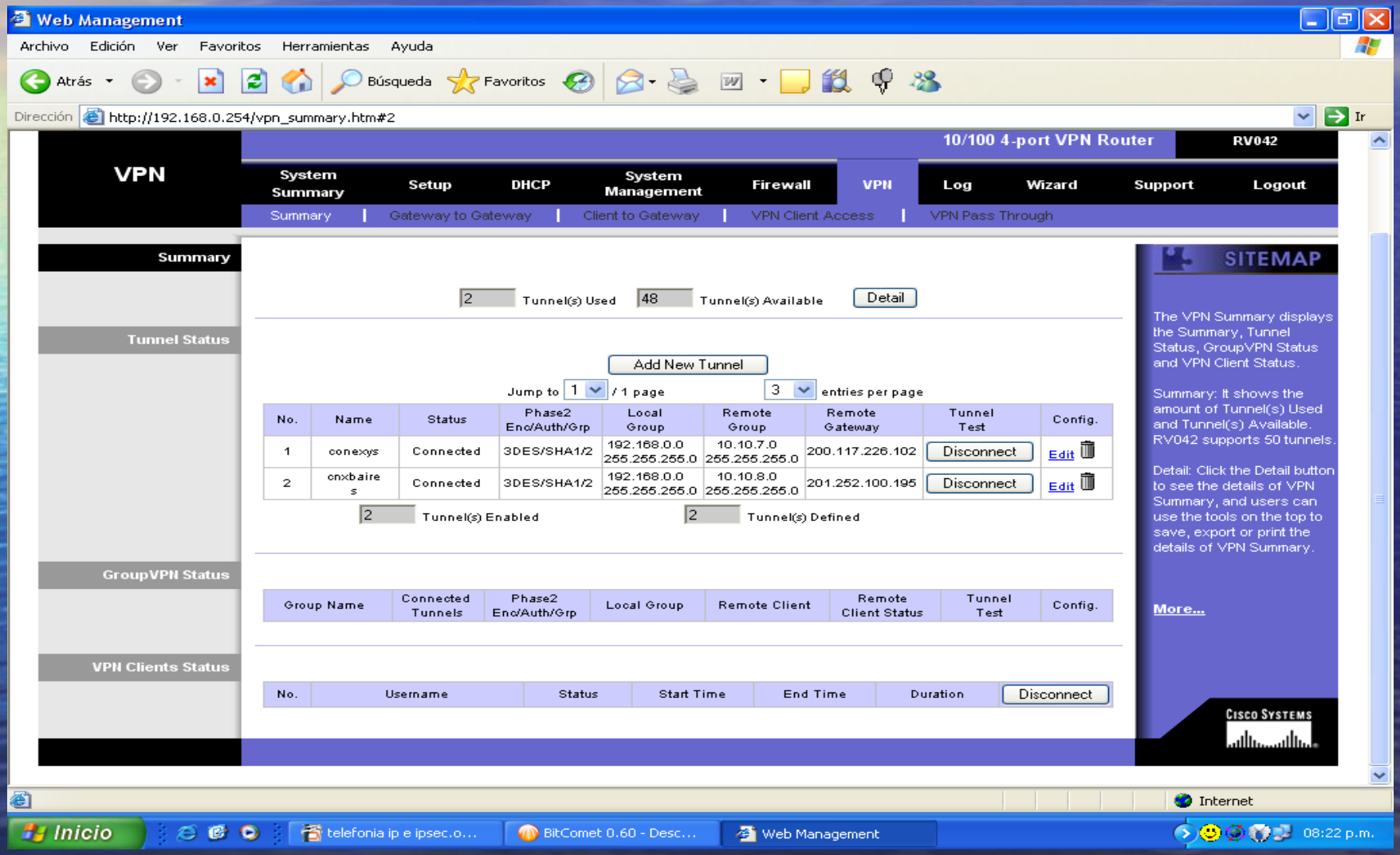
```
[serverA]
type=friend
user=<user>
secret=<password>
host=<dynamic> | <serverA IP>
```

Archivo /etc/asterisk/*extensions.conf*

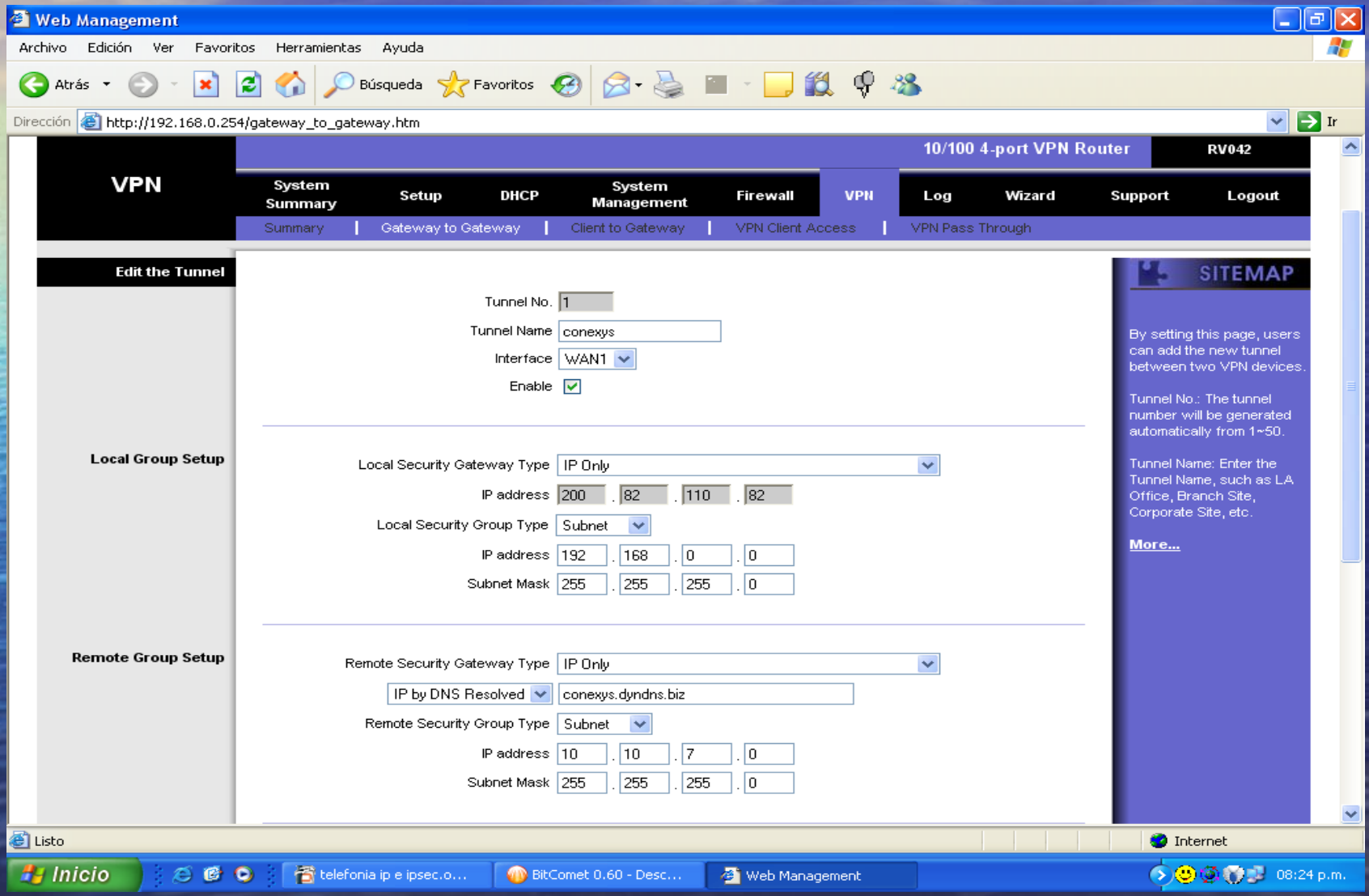
```
exten => _8XXX,1,Dial(IAX2/serverA/${EXTEN:1},30,r)
exten => _8XXX,2,Congestion
```

De esta forma con las 2 centrales ya conectadas, solo nos queda ver como manejamos el tema de la calidad de servicio (QoS) en la red WAN de interconexión de centrales para asegurar una comunicación estable y de alta calidad. Como solución propuesta, usaremos firewalls y servers VPN en servidores distintos a los usados por la central IP, basados en el proyecto libre m0n0wall

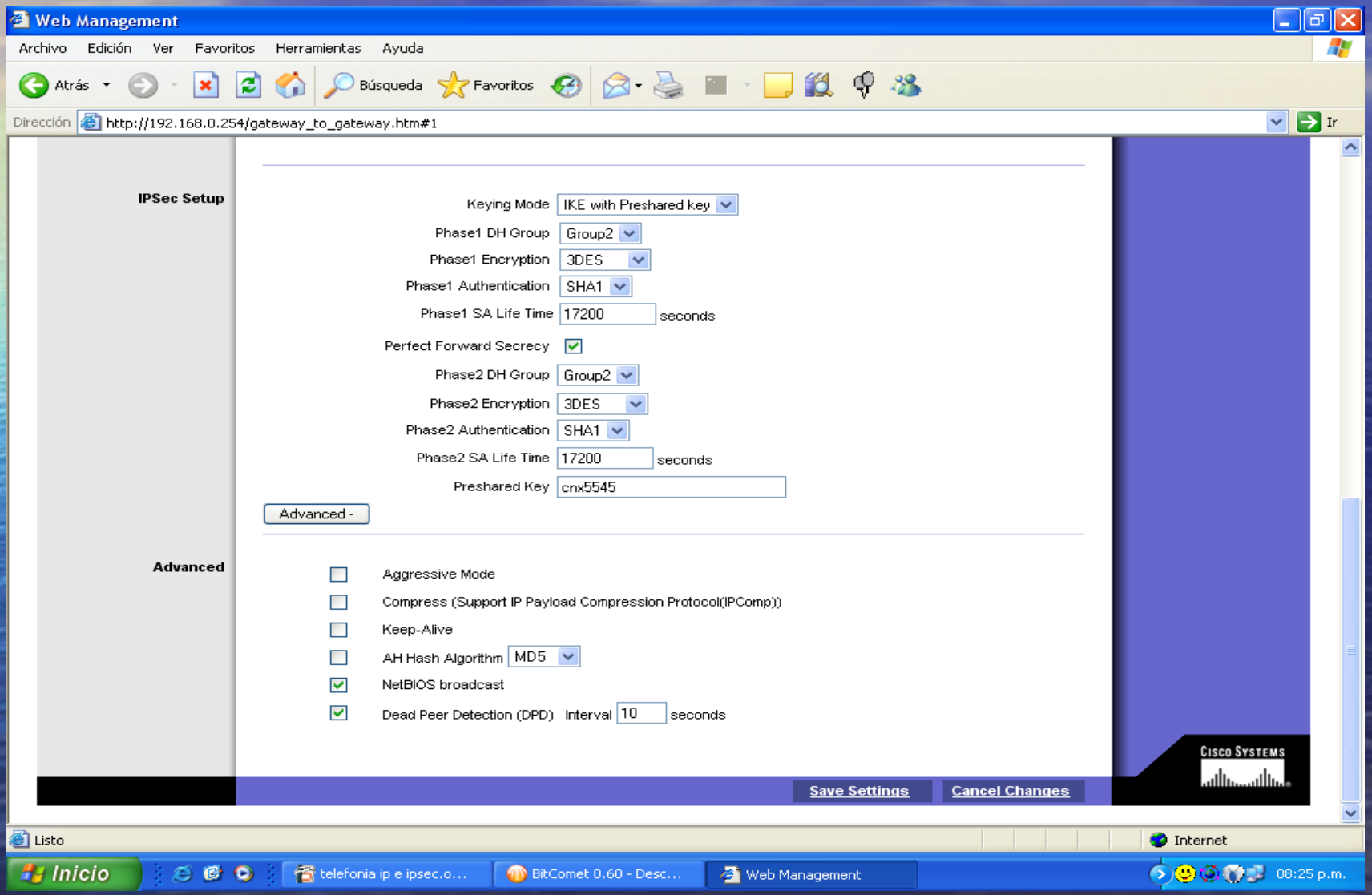
EJEMPLO DE CONFIGURACION TUNEL VPN IPSEC



EJEMPLO DE CONFIGURACION TUNEL VPN IPSEC



EJEMPLO DE CONFIGURACION TUNEL VPN IPSEC



Bibliografía

- *Internet Engineering Task Force (www.ietf.org) RFC 2401-2764-2709-2411-2521-2685*
- *Recursos VoIP – Web Page – (www.recursosvoip.com)*
- *Cisco (www.cisco.com) IPsec (white paper)*
- *Voip-Info Web Page – www.voip-info.org*
- *Asterisk PBX Home Page – www.asterisk.org*
- *m0n0wall Firewall Project –m0n0.ch/wall*
- *Intel Voip Solutions – www.intel.com*
- *Groupware PHPProjekt - www.phprojekt.com*
- *Digium Hardware Webpages - www.digium.com*
- *Sugar CRM & Asterisk@Home - asteriskathome.sourceforge.net*

Muchas Gracias !!!!!