



EDGAR DE LA CRUZ ESPARZA

HERNÁN GEOVANNI TAIMAL

**ANEXO C
MANUALES DE INSTALACION Y USO DE MIDSEG**

**UNIVERSIDAD DEL CAUCA
FACULTADA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, MAYO DE 2009**

TABLA DE CONTENIDO

Anexo C.....	1
MANUALES DE INSTALACION Y USO DEL MidSEG	1
C.1 MANUAL DE INSTALACION	1
C.1.1. Manual de Instalación del SCSWI	1
C.1.2. Manual de Instalación del SSW	3
C.1.2.1. Configuración del SSW.....	3
C.1.2.2. Instalación de la Base de Datos en el SSW.....	4
C.1.2.3. Instalación del Driver de MySQL y del Api JAIN-SIP en el SSW.....	6
C.1.3. Manual de Instalación del SSP.....	6
C.1.3.1. Configuración del SSP	7
C.1.3.2. Instalación del Api JAIN-SIP en el SSP	8
C.2. MANUAL DE USUARIO	8
C.2.1. Manual de Uso del SCSWI y de la GUI de Referencia.....	8
C.2.2. Manual de Uso del SSW	13
C.2.3. Manual de Uso del SSP	15
Bibliografía.....	17

LISTA DE FIGURAS

<i>Figura 1. Ubicación de Archivos en el UE</i>	<i>2</i>
<i>Figura 2. Configuración de Java en el UE</i>	<i>3</i>
<i>Figura 3. Ubicación de Archivos en el SMSW</i>	<i>3</i>
<i>Figura 4. Archivo de Configuración del SSW.....</i>	<i>4</i>
<i>Figura 5. Creación de Base de Datos del SSW</i>	<i>4</i>
<i>Figura 6. Restauración de la ssw_db</i>	<i>5</i>
<i>Figura 7. Tabla Parámetros de la ssw_db</i>	<i>5</i>
<i>Figura 8. Tabla Conexiones_ipsec de la ssw_db</i>	<i>6</i>
<i>Figura 9. Configuración de JAVA en el SMSW</i>	<i>6</i>
<i>Figura 10. Ubicación de Archivos en el SMSP</i>	<i>7</i>
<i>Figura 11. Archivo de Configuración del SSP</i>	<i>8</i>
<i>Figura 12. Configuración de JAVA en el SMSP.....</i>	<i>8</i>
<i>Figura 13. Ejecución del SCSWI y la GUI de Referencia</i>	<i>9</i>
<i>Figura 14. Elección de Dominios a Registrar</i>	<i>10</i>
<i>Figura 15. Configuración de Valores para el Registro.....</i>	<i>11</i>
<i>Figura 16. Algoritmos de Autenticación para la Interfaz de Radio.</i>	<i>12</i>
<i>Figura 17. Algoritmos de Cifrado para la Interfaz de Radio</i>	<i>13</i>
<i>Figura 18. Iniciar el SSW en el SMSW</i>	<i>13</i>
<i>Figura 19. SSW Iniciado Correctamente.....</i>	<i>14</i>
<i>Figura 20. Parar y Salir del SSW</i>	<i>15</i>
<i>Figura 21. Iniciar el SSW en el SMSP.....</i>	<i>15</i>
<i>Figura 22. Iniciado Correctamente</i>	<i>16</i>
<i>Figura 23. Parar y Salir del SSP.....</i>	<i>16</i>

Anexo C

MANUALES DE INSTALACION Y USO DEL MidSEG

El presente documento está organizado en dos partes, la primera consiste en el manual de instalación de cada uno de los componentes del MidSEG y la segunda parte hace referencia al manual de uso de cada uno de ellos.

C.1 MANUAL DE INSTALACION

Para la instalación del MidSEG se asume la instalación y configuración de las herramientas descritas en el Anexo B necesarias para el funcionamiento de cada subsistema:

SCSWI

- JDK versión 1.6.
- IPsec-tools.

SSW

- JDK versión 1.6.
- IPsec-tools.
- MySQL.
- Iptables.
- Racoon

SSP

- JDK versión 1.6.
- IPsec-tools.
- Iptables.
- Racoon

Los recursos necesarios para la instalación de MidSEG son incluidos en el CD que acompaña la monografía.

C.1.1. Manual de Instalación del SCSWI

Para instalar el SCSWI copie el archivo scswi.jar del CD a una carpeta específica, en el ejemplo de la Figura 1 se copia el archivo a la ruta /home/cliente/Escritorio/jarSCWI.

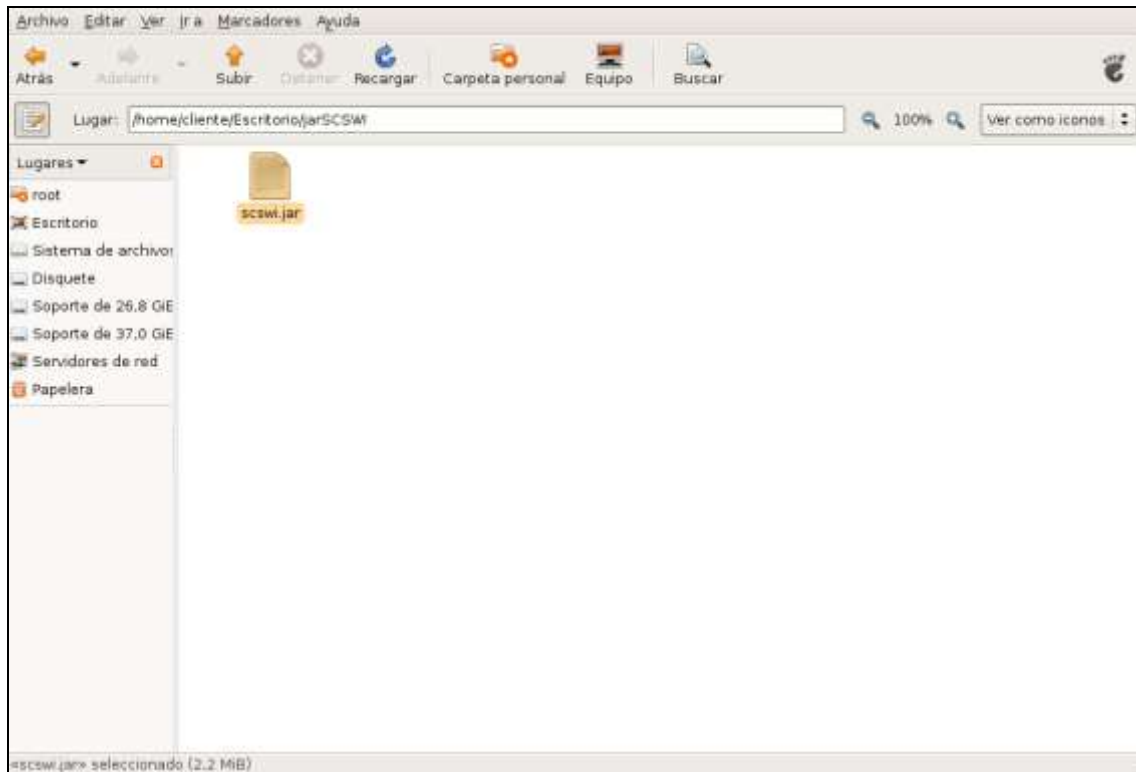


Figura 1. Ubicación de Archivos en el UE

Con el fin de permitir al SCSWI el uso del protocolo SIP agregue las siguientes librerías a su máquina virtual Java (JVM):

- JainSipApi1.2.jar: Interfaces y clases principales de SIP.
- JainSipRi1.2.jar: Implementación SIP de referencia.
- log4j-1.2.8.jar (Disponible dentro del archivo jain-sip-1.2.jar en la carpeta jain-sip/lib): Servicio de reportes para las aplicaciones.
- concurrent.jar (Disponible dentro del archivo jain-sip-1.2.jar en la carpeta jain-sip/lib): utilidades de concurrencia.

Para obtener las librerías del api Jain-Sip diríjase a la página <https://jain-sip.dev.java.net>. Copiar las librerías a la carpeta /jre/lib/ext de su JVM como se muestra en la Figura 2.

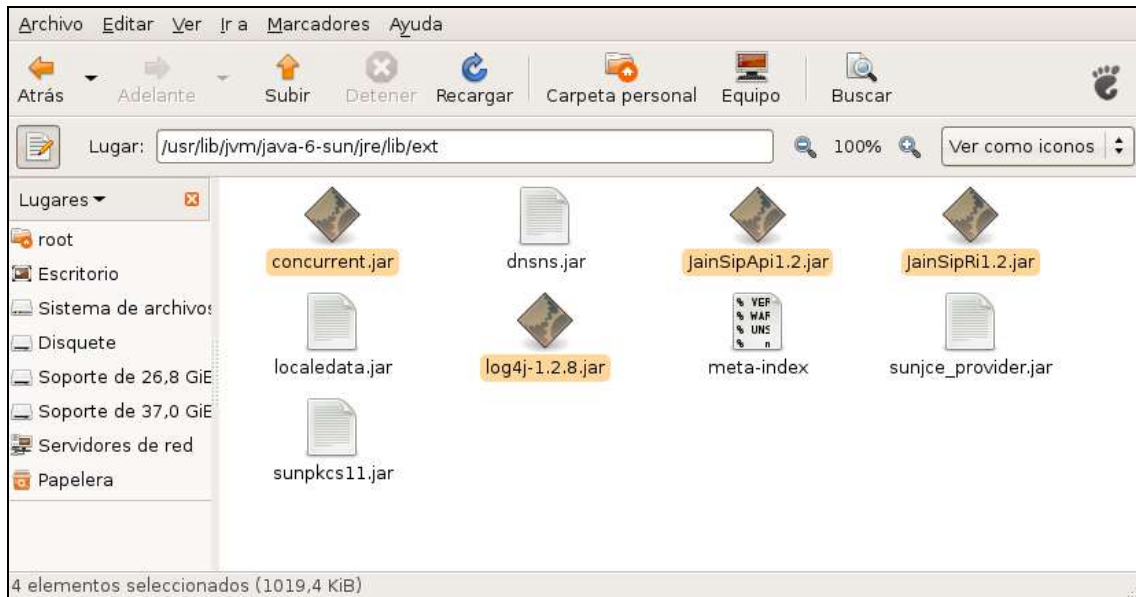


Figura 2. Configuración de Java en el UE

C.1.2. Manual de Instalación del SSW

Para la instalación del SSW copie el archivo ssw.jar y la carpeta config del CD a una carpeta específica. Dentro de la carpeta config se encuentra el archivo de configuración del SSW como se ve en la Figura 3.



Figura 3. Ubicación de Archivos en el SMSW

C.1.2.1. Configuración del SSW

El archivo de configuración consiste en un archivo con los siguientes campos:

Obligatorios

Stack_name: nombre que se le asigna al conjunto de propiedades SIP.

Stack_IP_address: dirección IP en la cual escucha el SSW.

Stack_domain: nombre del dominio que maneja el SSW.

Outbound_proxy: proxy de salida a la red IMS, en este caso la dirección IP y el puerto del SSP.

Ims_gateway: dirección IP del servidor por la cual alcanza el dominio IMS.

Wlan_gateway: dirección IP del servidor por la cual alcanza el dominio WLAN.

Listening point: corresponde a los puertos y protocolos de transporte habilitados en el servidor.

Network server_name: nombre del servidor SSW.

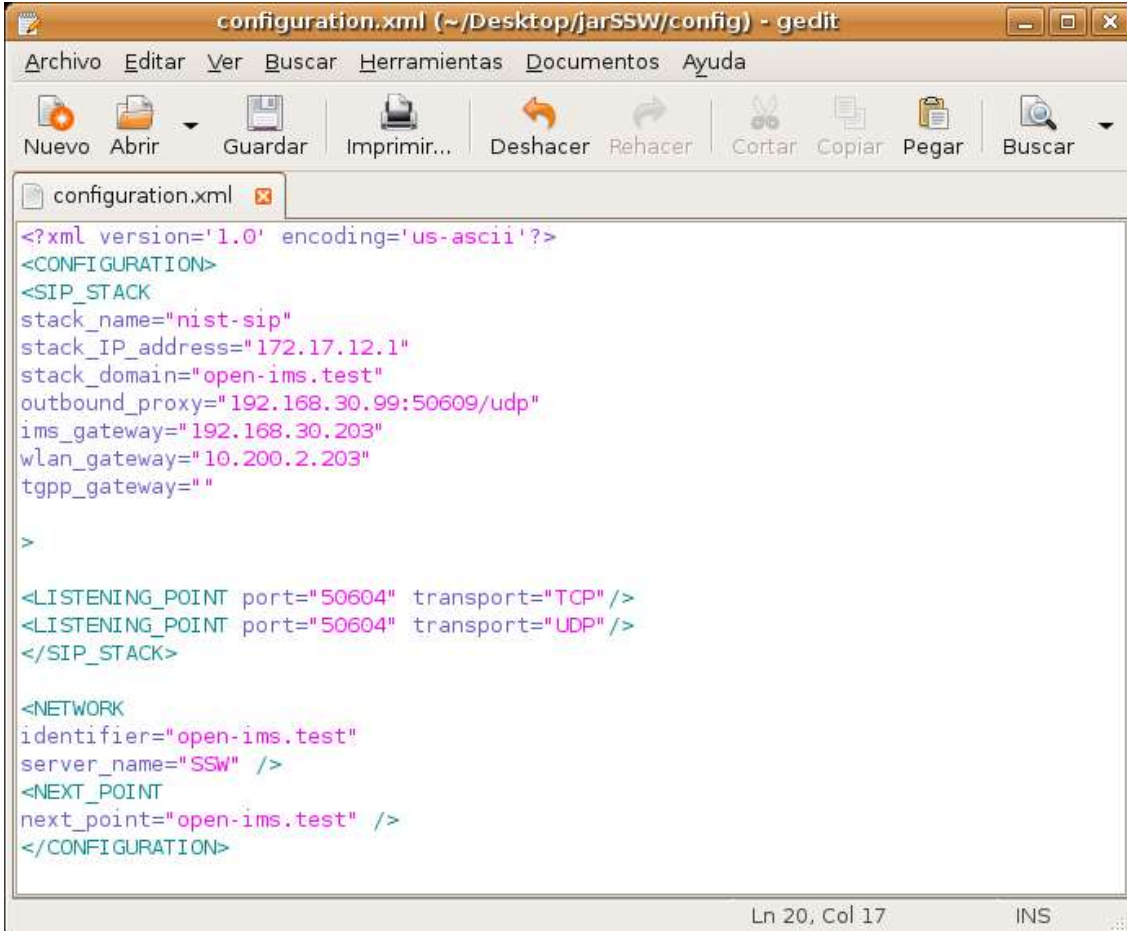
Opcionales

Next_point: corresponde al próximo salto de envío.

Network identifier: hace referencia al identificador de red.

Tgpp_gateway: dirección IP del servidor por la cual el SSW alcanza el dominio 3GPP.

En la Figura 4 se muestra la configuración con la cual se realizaron las pruebas del SSW en el MidSEG.

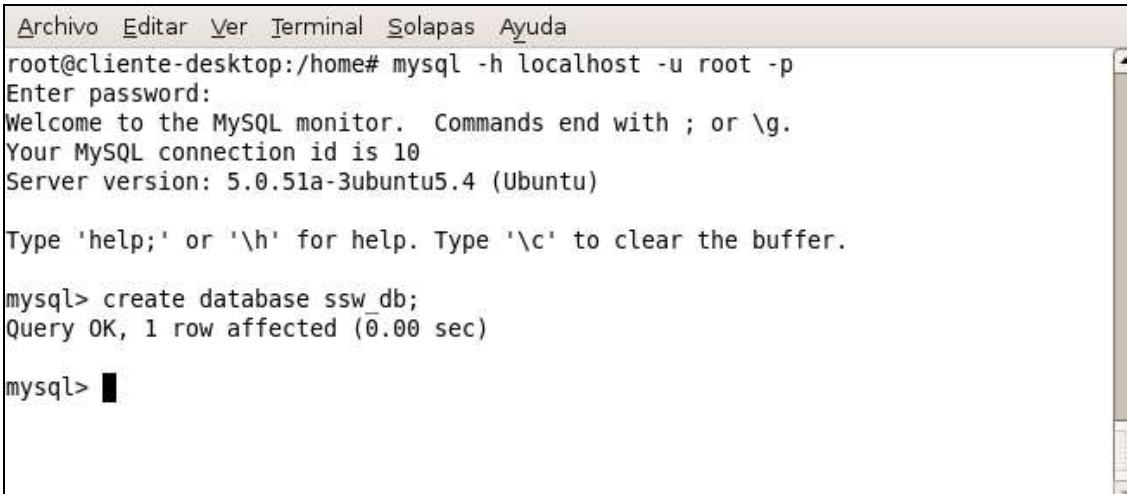


```
<?xml version='1.0' encoding='us-ascii'?>
<CONFIGURATION>
<SIP_STACK
stack_name="nist-sip"
stack_IP_address="172.17.12.1"
stack_domain="open-ims.test"
outbound_proxy="192.168.30.99:50609/udp"
ims_gateway="192.168.30.203"
wlan_gateway="10.200.2.203"
tgpp_gateway=""
>
<LISTENING_POINT port="50604" transport="TCP" />
<LISTENING_POINT port="50604" transport="UDP" />
</SIP_STACK>
<NETWORK
identifier="open-ims.test"
server_name="SSW" />
<NEXT_POINT
next_point="open-ims.test" />
</CONFIGURATION>
```

Figura 4. Archivo de Configuración del SSW

C.1.2.2. Instalación de la Base de Datos en el SSW.

Para instalar la base de datos que utiliza el SSW se crea una con el nombre ssw_db tal como se muestra en la Figura 5.



```
root@cliente-desktop:/home# mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

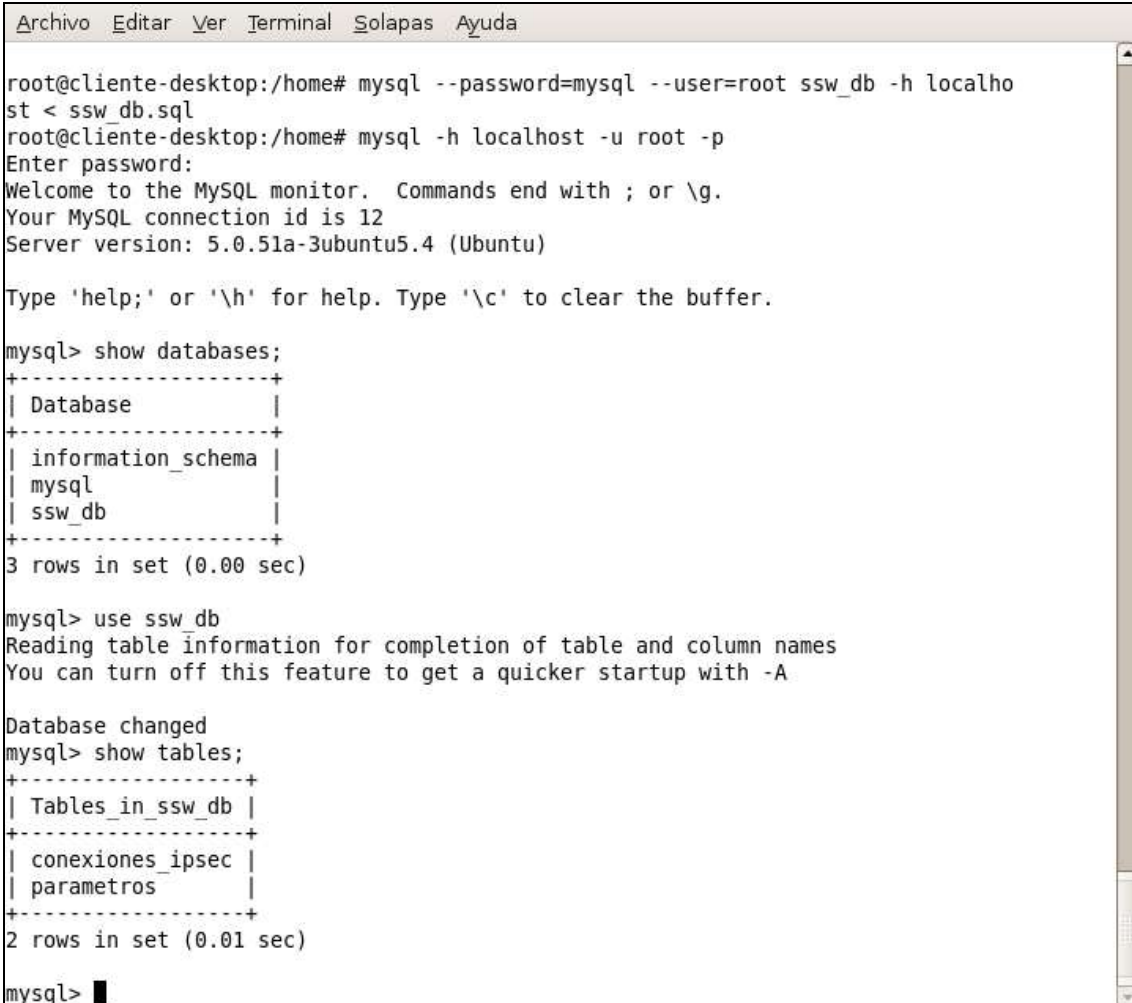
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> create database ssw_db;
Query OK, 1 row affected (0.00 sec)

mysql>
```

Figura 5. Creación de Base de Datos del SSW

Una vez creada la base de datos se procede a restaurarla utilizando el archivo ssw_db.sql suministrado Figura 6. Se puede confirmar el éxito de esta operación revisando las tablas creadas para la base de datos cuyos nombres son “conexiones_ipsec” y “parametros”.



```
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

root@cliente-desktop:/home# mysql --password=mysql --user=root ssw_db -h localho
st < ssw_db.sql
root@cliente-desktop:/home# mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| ssw_db |
+-----+
3 rows in set (0.00 sec)

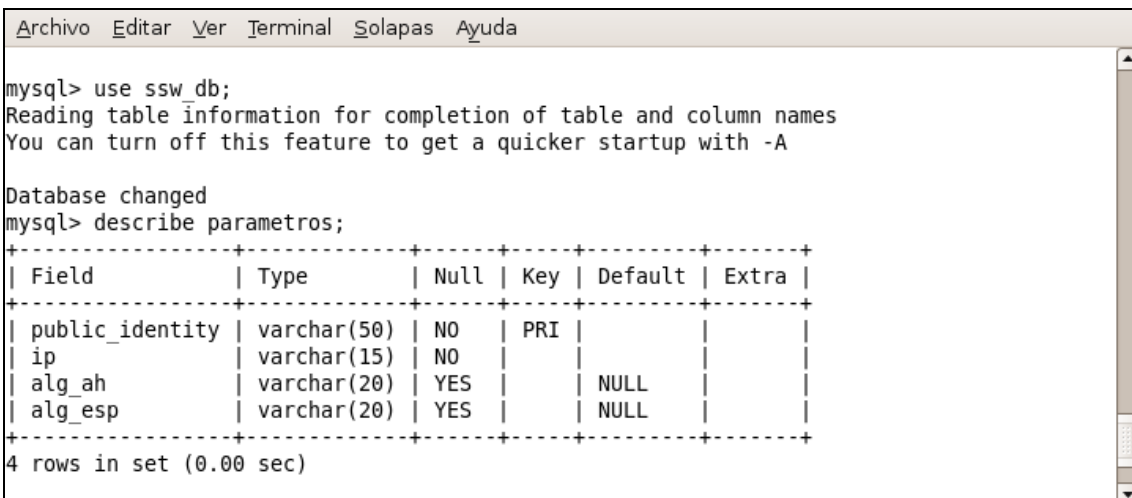
mysql> use ssw db
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_ssw_db |
+-----+
| conexiones_ipsec |
| parametros |
+-----+
2 rows in set (0.01 sec)

mysql> █
```

Figura 6. Restauración de la ssw_db

Las tablas “parametros” y “conexiones_ipsec” deben verse como en las figuras Figura 7 y Figura 8 respectivamente.



```
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

mysql> use ssw db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> describe parametros;
+-----+-----+-----+-----+-----+-----+
| Field          | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| public_identity | varchar(50)   | NO   | PRI |          |       |
| ip             | varchar(15)   | NO   |     |          |       |
| alg_ah         | varchar(20)   | YES  |     | NULL    |       |
| alg_esp        | varchar(20)   | YES  |     | NULL    |       |
+-----+-----+-----+-----+-----+-----+
4 rows in set (0.00 sec)
```

Figura 7. Tabla Parámetros de la ssw_db

```
Archivo Editar Ver Terminal Solapas Ayuda

mysql> describe conexiones_ipsec;
+-----+-----+-----+-----+-----+-----+
| Field          | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| public_identity | varchar(50)   | NO   | PRI |          |       |
| spi            | varchar(20)   | NO   |     |          |       |
| ip             | varchar(15)   | NO   |     |          |       |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>
```

Figura 8. Tabla Conexiones_ipsec de la ssw_db

C.1.1.2.3. Instalación del Driver de MySQL y del Api JAIN-SIP en el SSW

Al igual que en el equipo de usuario para que el SSW pueda hacer uso de la funcionalidad SIP se copian los archivos respectivos en la JVM y para acceder a la base de datos de MySQL se debe también copiar el driver mysql-connector-java-3.1.12-bin.jar ver Figura 9.

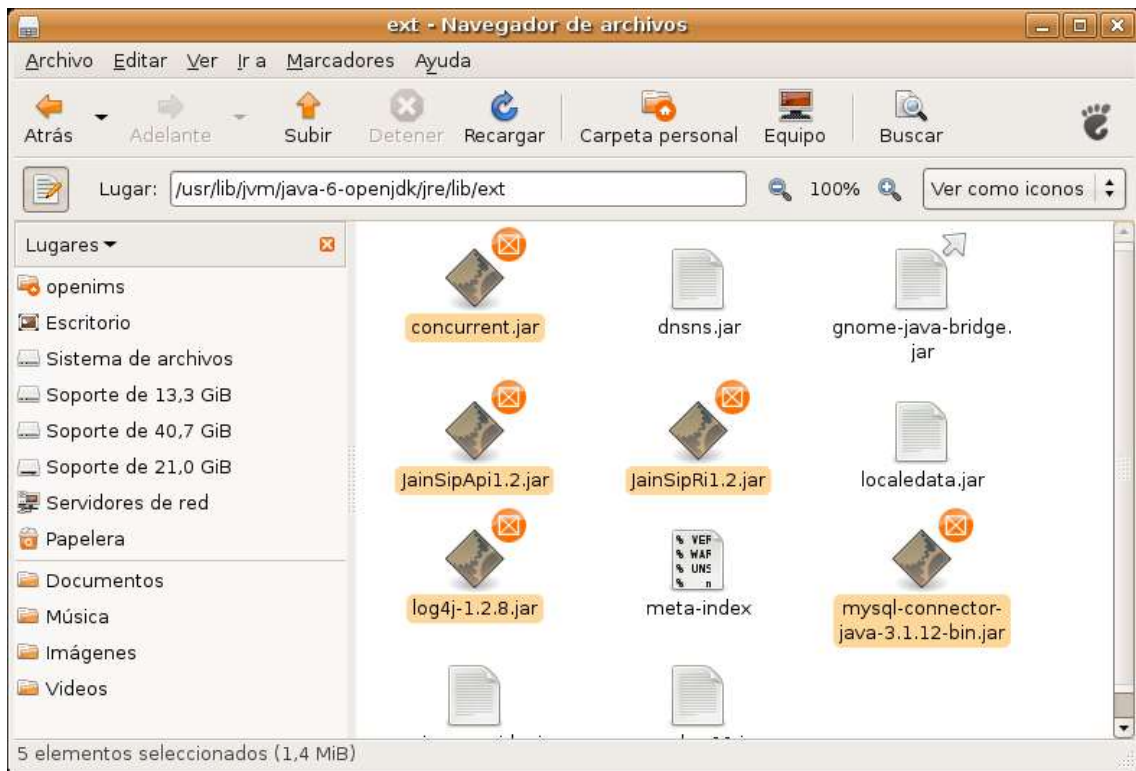


Figura 9. Configuración de JAVA en el SMSW

C.1.1.3. Manual de Instalación del SSP

Para la instalación del SSP copie el archivo ssp.jar y la carpeta config del CD a una carpeta específica. Dentro de la carpeta config se encuentra el archivo de configuración del SSP como se ve en la Figura 10.

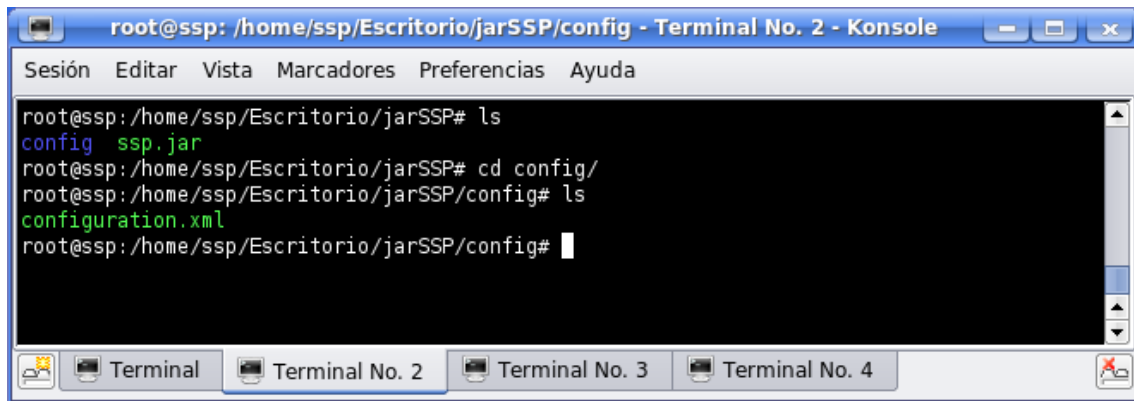


Figura 10. Ubicación de Archivos en el SMSMSP

C.1.3.1. Configuración del SSP

El archivo de configuración es un documento xml con los siguientes campos:

Obligatorios

Stack_name: nombre que se le asigna al conjunto de propiedades SIP.

Stack_IP_address: dirección IP sobre la cual va a estar escuchando el SSP.

Stack_domain: nombre del dominio que maneja el servidor SSP.

Outbound_proxy: proxy de salida a la red IMS, en este caso la dirección IP y el puerto del P-CSCF.

Listening point: corresponde a los puertos y protocolos de transporte habilitados en el servidor SSP.

Network server_name: nombre del servidor.

Opcionales

Next_point: corresponde al próximo salto de envío.

Network identifier: hace referencia al identificador de red.

En la Figura 11 se muestra la configuración con la cual se realizaron las pruebas del SSP en el MidSEG.

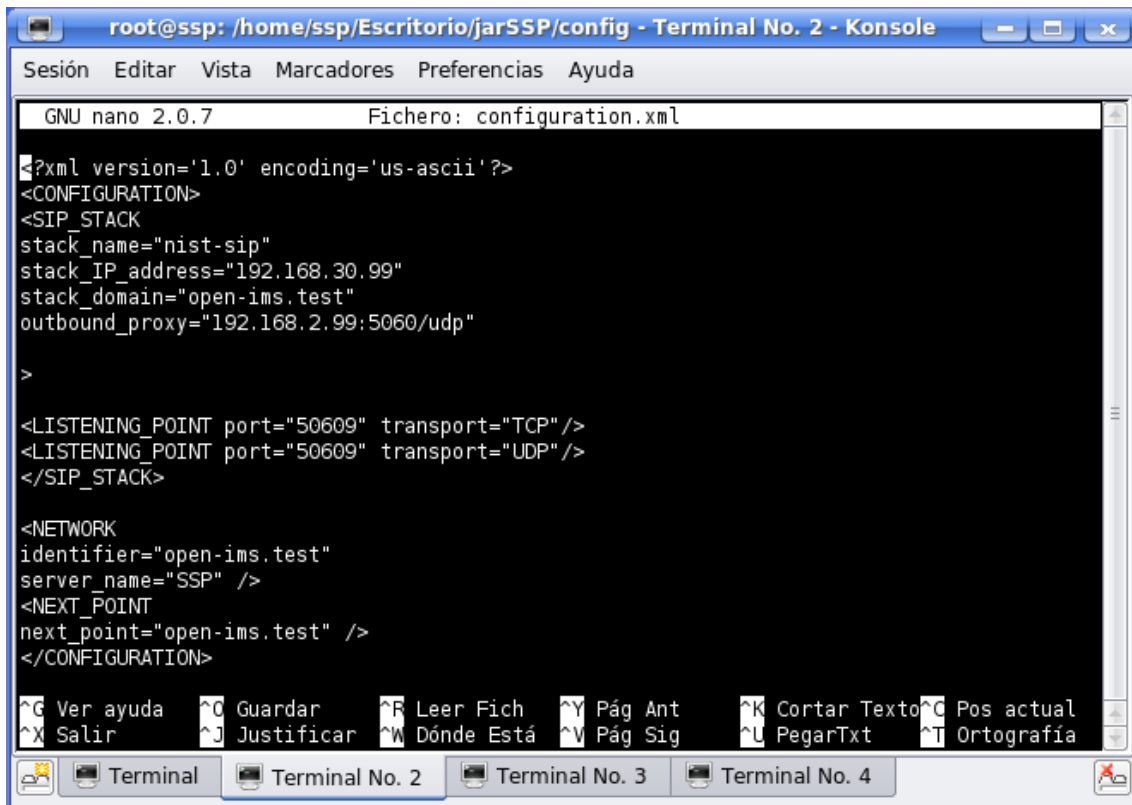


Figura 11. Archivo de Configuración del SSP

C.1.3.2. Instalación del Api JAIN-SIP en el SSP

Para que el SSP pueda hacer uso de la funcionalidad SIP se copian los archivos respectivos en la JVM del servidor ver Figura 12.

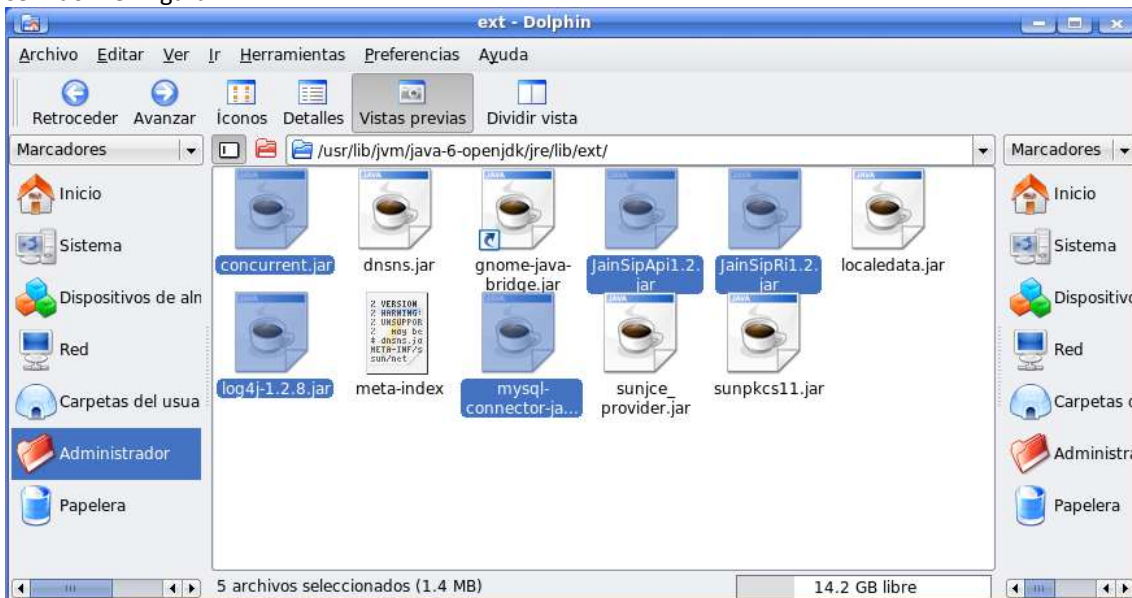


Figura 12. Configuración de JAVA en el SMSP

C.2. MANUAL DE USUARIO

C.2.1. Manual de Uso del SCSWI y de la GUI de Referencia

Para iniciar el cliente de prueba que contiene al SCSWI se ejecuta el archivo scswi.jar con la JVM en la cual se instaló el api JAIN-SIP, ver Figura 13.

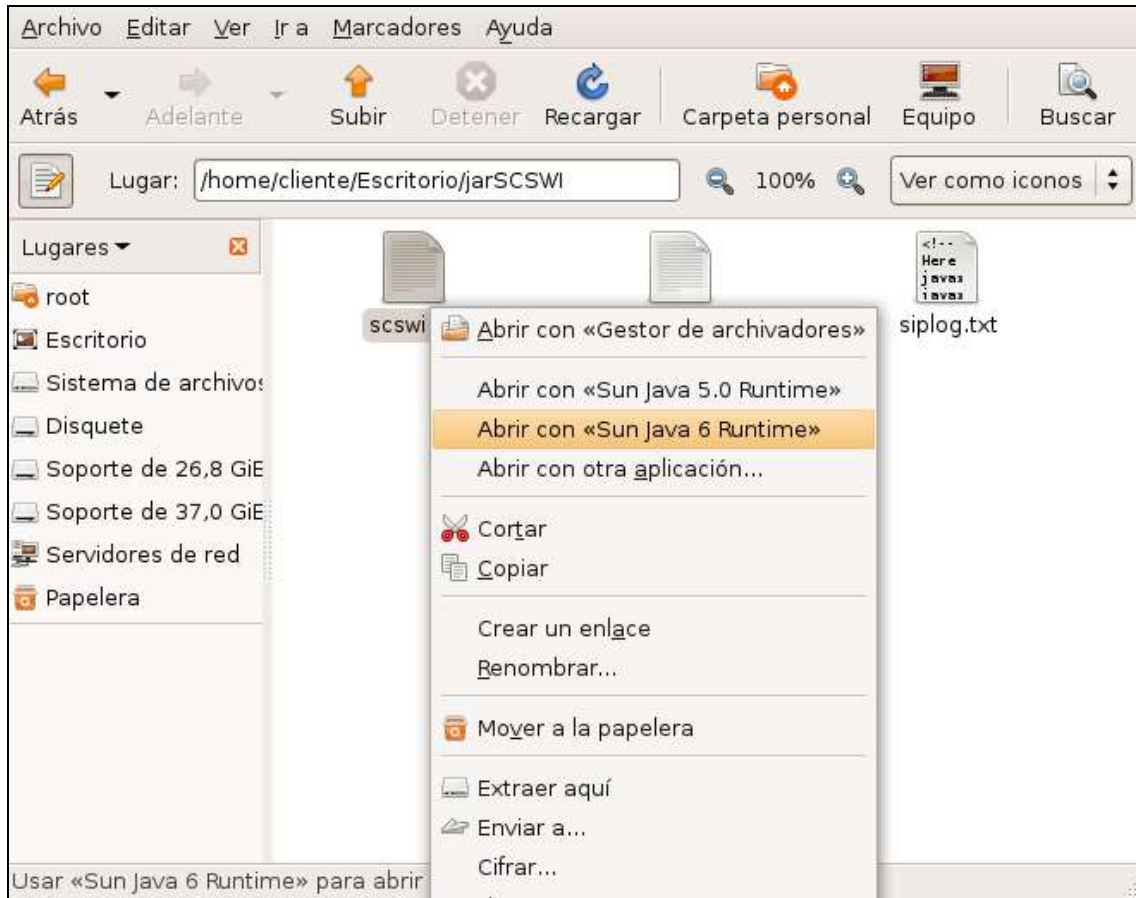


Figura 13. Ejecución del SCSWI y la GUI de Referencia

Al ejecutarse la aplicación se muestra la interfaz grafica de usuario, la cual está conformada por las pestañas Dominios, Configuración e Interfaz de Radio. En la pestaña Dominios se da la opción de elegir los dominios a registrar, WLAN, 3GPP e IMS, ver Figura 14.

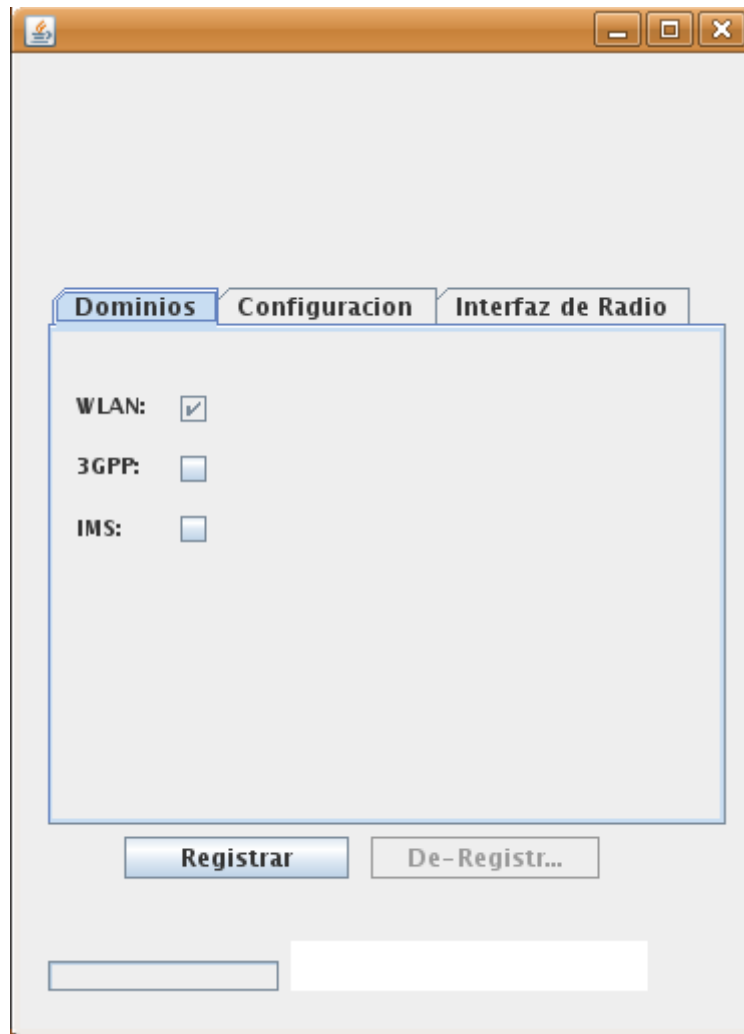


Figura 14. Elección de Dominios a Registrar

En la pestaña **Configuración** se muestran los campos necesarios para la comunicación por SIP:

Identidad Pública: corresponde a la identidad pública de usuario, escrita en forma de URI.

Identidad Privada: corresponde a la identidad privada de usuario.

Clave Secreta: corresponde a la clave secreta compartida con el HSS de la red IMS.

Dirección IP: dirección IP del equipo cliente.

Puerto: puerto por el cual el scswi escucha para la comunicación SIP.

Nombre de Dominio: nombre de dominio de la red IMS a la que pertenece el usuario.

Servidor Proxy: dirección IP y puerto del SSW, corresponde al proxy que gestiona el registro del usuario.

Expires: tiempo de expiración para las solicitudes de registro.

En la Figura 15 se muestra la configuración que se utilizó en la prueba del MidSEG.

Configuración	Valor
Identidad Publica:	sip:bob@open-ims.test
Identidad Privada:	bob@open-ims.test
Clave Secreta:	bob
Direccion Ip:	172.17.12.12
Puerto:	50601
Nombre de Domin...:	open-ims.test
Servidor Proxy:	172.17.12.1:50604/UDP
Expires:	3600

Figura 15. Configuración de Valores para el Registro

En la pestaña **Interfaz de Radio** se muestra las opciones de seguridad que brinda el MidSEG para proteger la interfaz inalámbrica que comunica al UE con SMSW:

El algoritmo de Autenticación es obligatorio, en su configuración por defecto se encuentra hmac-md5 con una clave de 128 bits, como opciones está hmac-sha1 y hmac-sha2-256 con longitud de claves de 160 y 254 respectivamente (ver Figura 16). Se recomienda la utilización de los algoritmos hmac-sha1 y hmac-sha2-256 porque: el utilizar el algoritmo HMAC permite autenticar la fuente del mensaje y verificar su integridad, y al hacer uso de las funciones Hash se vale de la imposibilidad de los algoritmos para de encontrar dos mensajes con el mismo resultado [1][2].

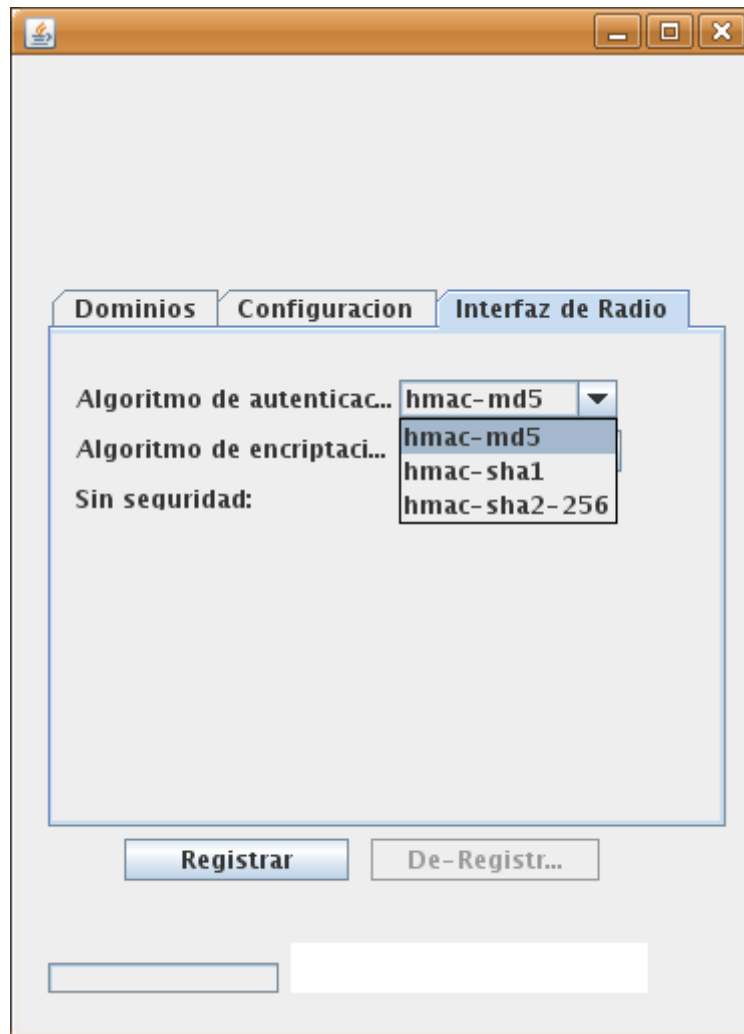


Figura 16. Algoritmos de Autenticación para la Interfaz de Radio.

El algoritmo de cifrado no se estableció como obligatorio y su valor por defecto es Ninguno. Como posibles opciones de configuración para establecer cifrado en la interfaz aérea se encuentran, des-cbc con longitud de clave de 64 bits, 3des-cbc con longitud de clave 192 bits y rijndael-cbc con longitud de clave 256 bits (ver Figura 17). Por seguridad se recomienda la utilización del algoritmo rijndael-cbc principalmente porque: utiliza una clave de mayor longitud que la de los otros dos algoritmos lo cual garantiza mayor protección contra ataques de fuerza bruta, no ha sido vulnerado y porque fue elegido como el Estándar Avanzado de Encriptación (AES) por el Instituto Nacional de Estándares y Tecnología (NIST) de los EEUU [3].

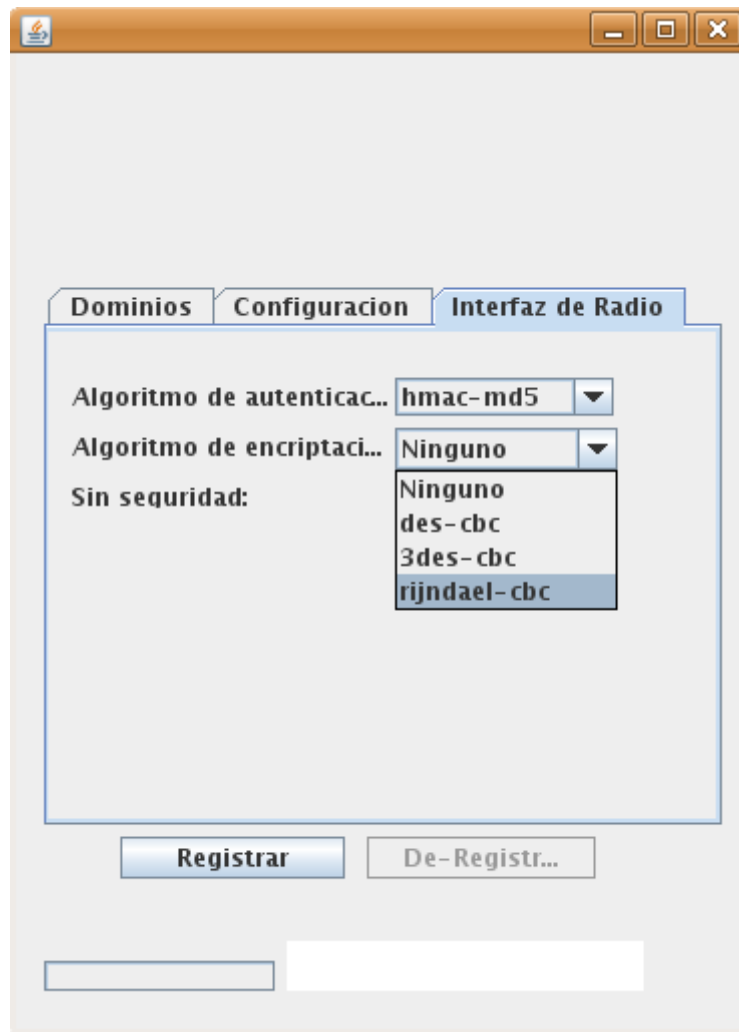


Figura 17. Algoritmos de Cifrado para la Interfaz de Radio

Configurados estos valores el inicio del registro se realiza con el botón Registrar, en el área blanca se muestra el estado del proceso y para des-registrarse se hace uso del botón De-Registrar.

C.2.2. Manual de Uso del SSW

Para arrancar la aplicación SSW se ubica en la carpeta donde se copió el archivo ssw.jar y se lo ejecuta haciendo uso del comando `java -jar` como se ve en la Figura 18. Para iniciar el servicio se usa el comando `start`.

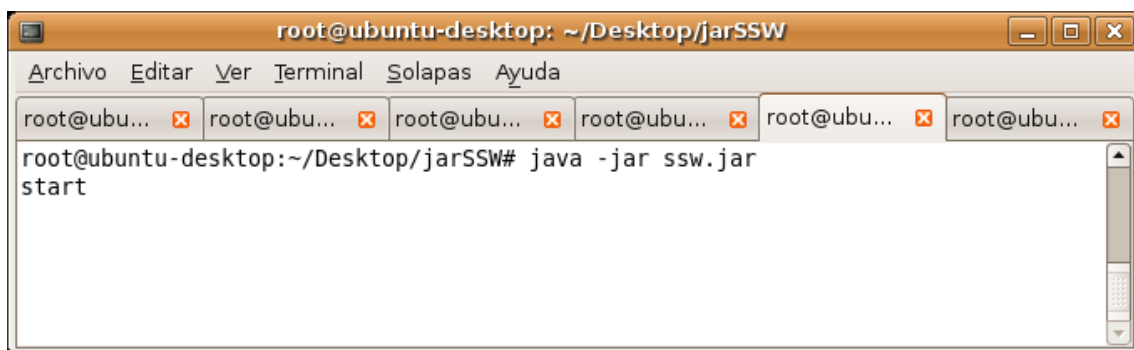
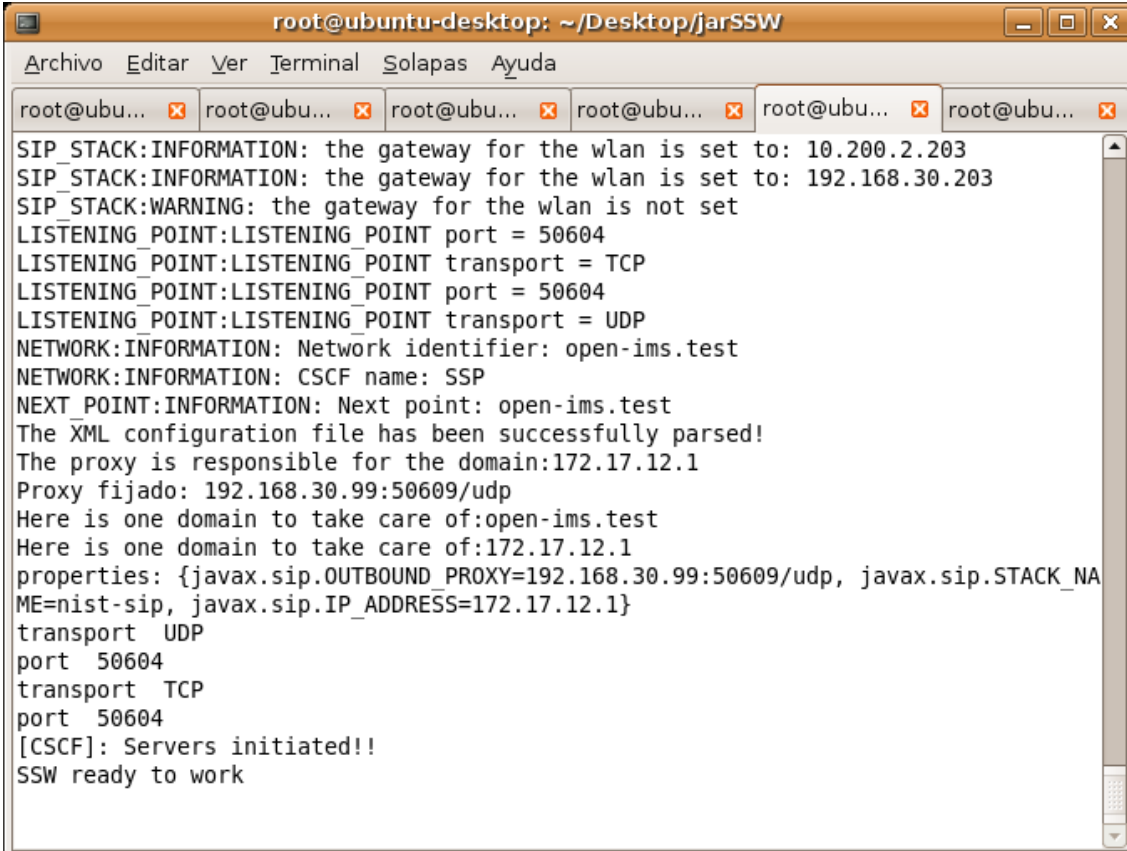


Figura 18. Iniciar el SSW en el SMSW

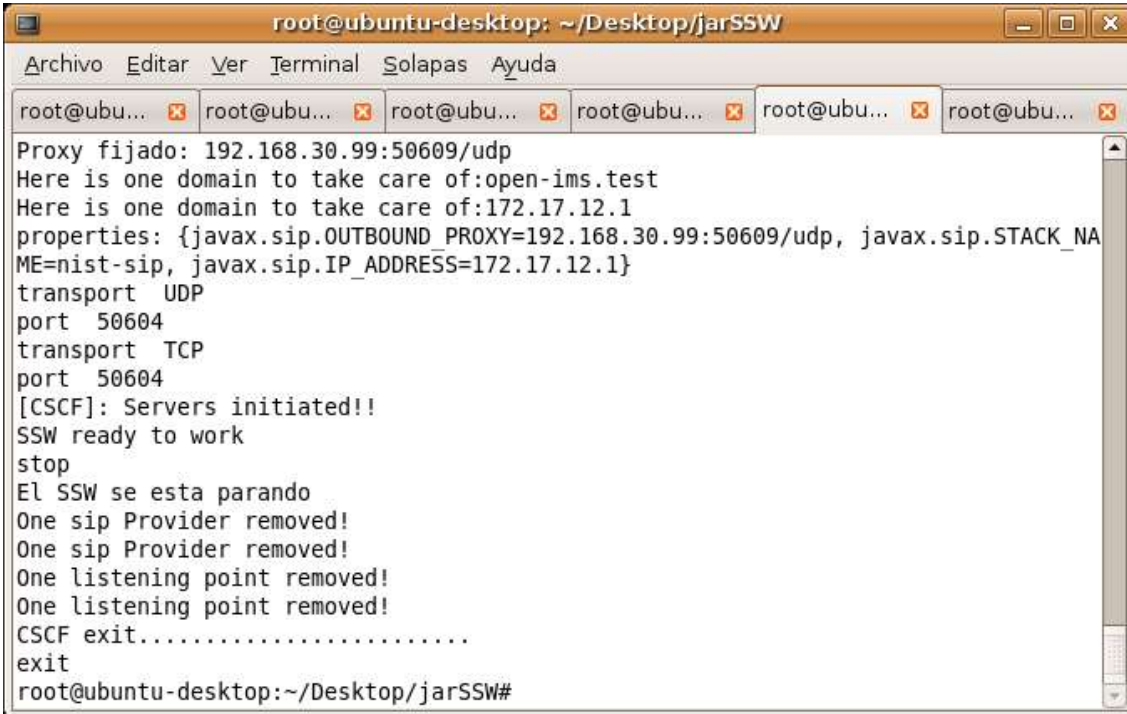
Si el servicio fue correctamente configurado e iniciado se debe visualizar algo semejante a lo mostrado en la Figura 19.



```
root@ubuntu-desktop: ~/Desktop/jarSSW
Archivo Editar Ver Terminal Solapas Ayuda
root@ubu... x root@ubu... x root@ubu... x root@ubu... x root@ubu... x root@ubu... x
SIP_STACK:INFORMATION: the gateway for the wlan is set to: 10.200.2.203
SIP_STACK:INFORMATION: the gateway for the wlan is set to: 192.168.30.203
SIP_STACK:WARNING: the gateway for the wlan is not set
LISTENING_POINT:LISTENING_POINT port = 50604
LISTENING_POINT:LISTENING_POINT transport = TCP
LISTENING_POINT:LISTENING_POINT port = 50604
LISTENING_POINT:LISTENING_POINT transport = UDP
NETWORK:INFORMATION: Network identifier: open-ims.test
NETWORK:INFORMATION: CSCF name: SSP
NEXT_POINT:INFORMATION: Next point: open-ims.test
The XML configuration file has been successfully parsed!
The proxy is responsible for the domain:172.17.12.1
Proxy fijado: 192.168.30.99:50609/udp
Here is one domain to take care of:open-ims.test
Here is one domain to take care of:172.17.12.1
properties: {javax.sip.OUTBOUND_PROXY=192.168.30.99:50609/udp, javax.sip.STACK_NAME=nist-sip, javax.sip.IP_ADDRESS=172.17.12.1}
transport UDP
port 50604
transport TCP
port 50604
[CSCF]: Servers initiated!!
SSW ready to work
```

Figura 19. SSW Iniciado Correctamente

Para parar el servicio y salir de la aplicación se usan los comandos stop y exit respectivamente (ver Figura 20).

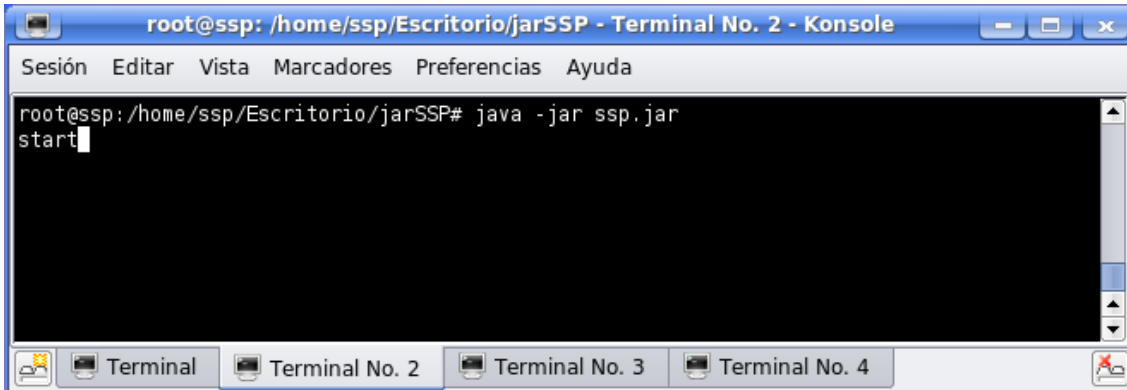


```
root@ubuntu-desktop: ~/Desktop/jarSSW
Archivo Editar Ver Terminal Solapas Ayuda
root@ubu... x root@ubu... x root@ubu... x root@ubu... x root@ubu... x root@ubu... x
Proxy fijado: 192.168.30.99:50609/udp
Here is one domain to take care of:open-ims.test
Here is one domain to take care of:172.17.12.1
properties: {javax.sip.OUTBOUND_PROXY=192.168.30.99:50609/udp, javax.sip.STACK_NAME=nist-sip, javax.sip.IP_ADDRESS=172.17.12.1}
transport UDP
port 50604
transport TCP
port 50604
[CSCF]: Servers initiated!!
SSW ready to work
stop
El SSW se esta parando
One sip Provider removed!
One sip Provider removed!
One listening point removed!
One listening point removed!
CSCF exit.....
exit
root@ubuntu-desktop:~/Desktop/jarSSW#
```

Figura 20. Parar y Salir del SSW

C.2.3. Manual de Uso del SSP

Para arrancar la aplicación SSP se ubica en la carpeta donde se copió el archivo ssp.jar y se lo ejecuta haciendo uso del comando `java -jar` como se ve en la Figura 21. Para iniciar el servicio se usa el comando `start`.



```
root@ssp: /home/ssp/Escritorio/jarSSP - Terminal No. 2 - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
root@ssp:/home/ssp/Escritorio/jarSSP# java -jar ssp.jar
start
```

Figura 21. Iniciar el SSW en el SMSP

Si el servicio fue correctamente configurado e iniciado se debe visualizar algo semejante a lo mostrado en la Figura 22.

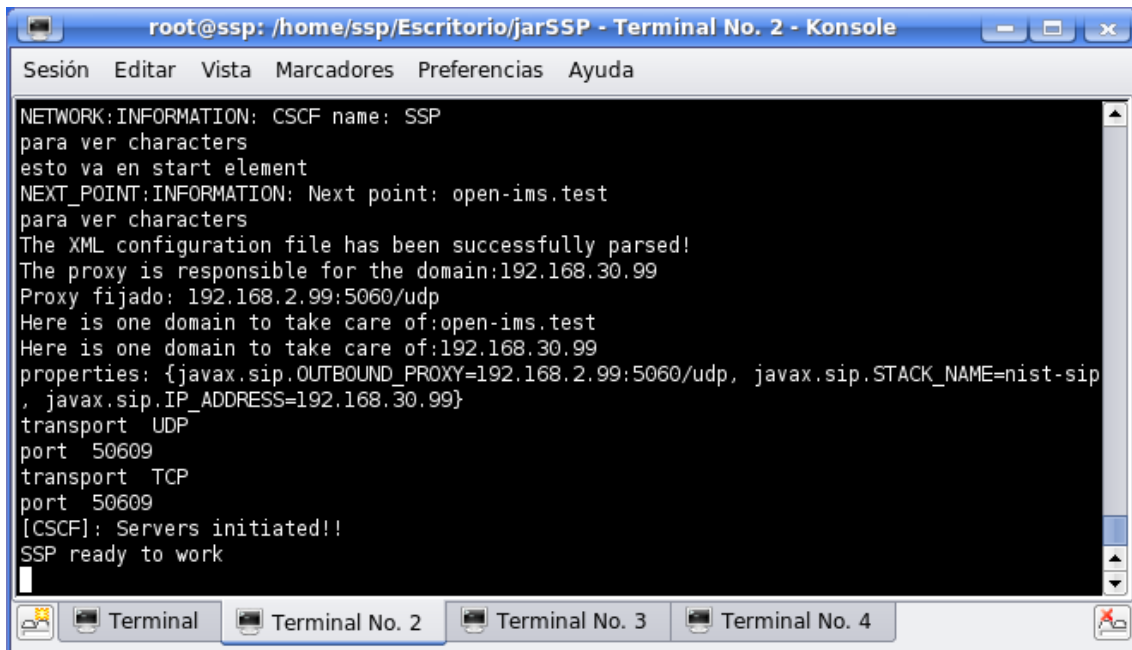


Figura 22. Iniciado Correctamente

Para parar el servicio y salir de la aplicación se usan los comandos `stop` y `exit` respectivamente (ver Figura 23).

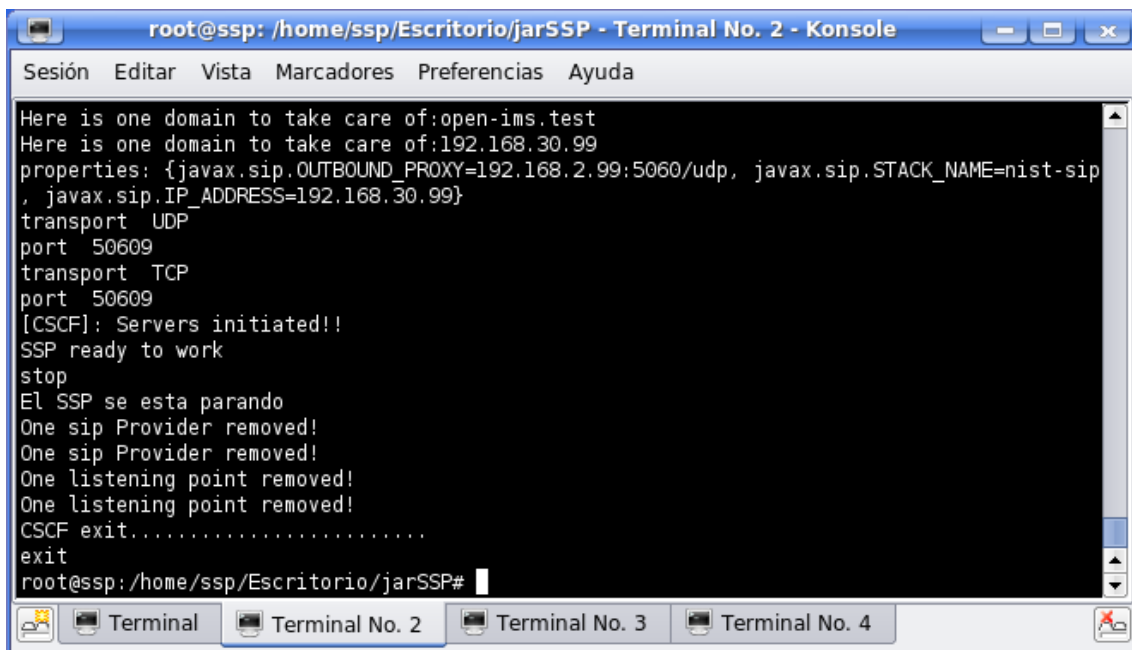


Figura 23. Parar y Salir del SSP

Bibliografía

- [1] National Institute of Standards and Technology, "The Keyed-Hash Message Authentication Code (HMAC)", Julio de 2008.
- [2] National Institute of Standards and Technology," Federal Information Processing Standards Publication 180-2", Agosto 1 de 2002.
- [3] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 197", Noviembre 26 de 2001.