

Manual de configuración de las comunicaciones en estaciones EHAS

EHAS. arnau@ehas.org (<http://www.ehas.org>)

Tabla de contenidos

1. Introducción	1
2. Instalación	2
3. Configuración.....	3
4. Protocolo de conexión radio y servicios.....	10
5. Servicios en estaciones ethernet.....	17
6. Certificación	17

Este documento es un manual de instalación y configuración -en un ordenador equipado con Linux/Debian- del software necesario para las estaciones EHAS que usan transceptores radio (VHF ó HF) o enlaces estándar ethernet para las comunicaciones de datos. Los servicios disponibles, entre otros, son: **transmisión de correo, navegación web, chat y gestión remota.**

1. Introducción

El proceso de instalación y configuración manual del software de comunicaciones (especialmente en los enlaces radio) y administración es largo y complejo. Por ello, se ha desarrollado un metapaquete (`ehas-station`), que reúne todas las aplicaciones y ficheros de configuración necesarios, además de servicios añadidos de envío de logs y sistema de gestión remota. En principio, estos paquetes están pensados para funcionar con la Metadistro-EHAS (<http://www.ehas.org/trabajo/bin/linux/ehas-metadistro/iso/>), pero puede instalarse en cualquier Linux/Debian sin ninguna limitación.

1.1. Comunicaciones radio

Las comunicaciones VHF se hacen con un modem FSK, que usa una velocidad cruda (de señalización) de 9600 bps. Las tasas de transmisión de usuario se situarán (en función de la calidad del canal), entre 3000 y 6000 bps. Todas las aplicaciones que usan el canal radio comprimen los datos enviados, por lo que en la mayoría de casos cabe esperar una mejora sustancial en la velocidad efectiva (normalmente se alcanzan factores 3 ó 4 de compresión).

Por su parte, las comunicaciones HF se hacen en este sistema con el módem Newqpsk (OFDM), que usa una velocidad cruda (de señalización) de 2500 bps. Las tasas de transmisión de usuario se situarán (en función de la calidad del canal), entre 500 y 1000 bps, consiguiéndose un factor de compresión efectivo en función del tipo de datos.

El sistema está basado en el uso de software libre (Postfix, BSMTP, UUCP, Soundmodem-Newqpsk, ALSA, etc) y el protocolo AX25 (mejorado con dos nuevas opciones: rechazo selectivo de paquetes -SREJ mejorado- y un sistema de asignación de turnos DAMA -denominado RRCONN, Round Robin Connections, en nuestra implementación-)

Las redes EHAS están formadas por agrupaciones de mini-redes. Cada una de estas mini-redes está formada por un servidor al que se conectan varios clientes. A su vez, el servidor central de esta micro-red puede ser el cliente de otra micro-red si no tiene acceso directo a Internet, y necesita enrutar el correo externo.

Figura 1. Red VHF

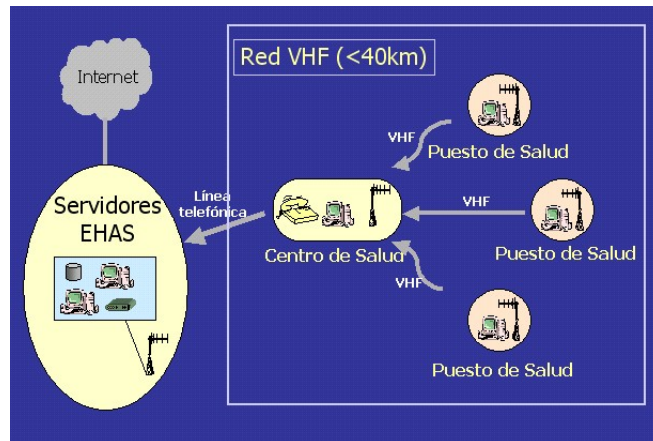
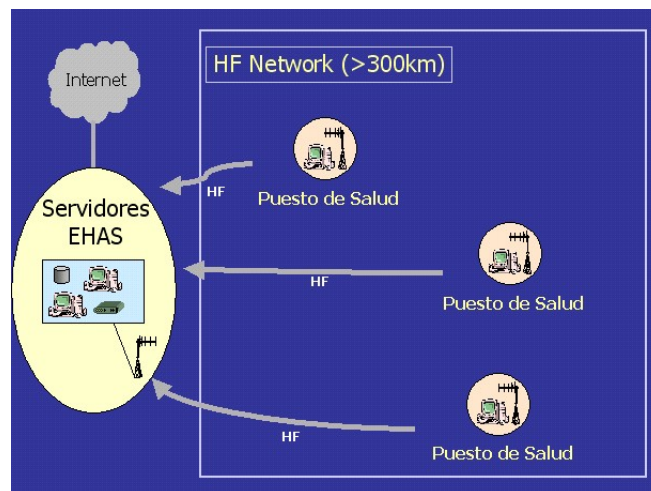


Figura 2. Red HF



1.2. Comunicaciones ethernet

La transferencia de información (correo y navegación) ethernet usa el protocolo TCP/IP, con la única particularidad que, por compatibilidad, el correo sigue el mismo esquema (UUCP/BSMTP) que el correo radio.

2. Instalación

2.1. Repositorio

Para descargar los paquetes *debian* hay que editar el fichero `/etc/apt/sources.list` y añadir las líneas:

```
#!/etc/apt/sources.list
deb http://www.ahas.org/debian sarge contrib
deb-src http://www.ahas.org/debian sarge contrib
```

2.2. Instalación del metapaquete principal

El único paquete a instalar es **ahas-station**, quien a su vez instalará todos los paquetes necesarios.

```
apt-get update
apt-get install ahas-station
```

3. Configuración

El programa de configuración se inicia con el comando:

```
config-ahas
```

Donde veremos un menú de opciones como el siguiente:

```
+---Instalación de estación EHAS-----+
Selecciona una opción
+-----+
 1  Conectividad
 2  Automatización por hora
 3  Placa de interfaz
 4  Envío de logs
 5  Ejecucion remota segura
 6  Escritorio GNOME
 7  Configuración de red
 8  Establecer hora y fecha
 9  Salir
+-----+
+-----+
```

El sistema de configuración contempla dos tipos de conexión distintas:

- Radio: Conexiones en las que usemos transceptores HF ó VHF
- Ethernet: Cualquier otro tipo de conexión que permita el uso de TCP/IP directamente, y que normalmente tendrán velocidades de transmisión mayor (LAN, WiFi, módem telefónico, etc)

3.1. Conectividad radio (VHF/HF)

3.1.1. Limitación de correo

Dado que los canales radio son de muy baja velocidad, el sistema permite activar opciones para limitar el tamaño de los correos a enviar o recibir, para evitar una saturación en las colas de las estaciones.

3.1.2. Canal auxiliar PSK31 para HF

En las estaciones HF se ha habilitado un canal especial (que denominaremos **canal PSK31**) que utilizan los clientes para pedir conexión a los servidores. El canal PSK31 se sitúa en el espacio superior de la banda de transmisión (alrededor de 2500Hz), cerca del límite superior de la banda de transmisión de los transceptores, de forma que no interfiere con el módem usado en la transmisión de datos (**newqpsk**).

3.1.3. Camino dinámico

El sistema de transmisión de correo por UUCP permite conectar al servidor por cualquiera de las conexiones que se hayan creado (radio ó ethernet). El **camino dinámico** permite elegir una conexión en función de diversos parámetros, tamaño y antigüedad de la cola. Veamos un ejemplo:

camino dinámico: `conn1/conn2(queue<100K,old>1d)/conn3/conn2(old>1m)`

Primero intenta conectar usando la conexión *conn1*, si falla intentará *conn2* sólo si el tamaño de la cola es menor a 100 Kbytes y al menos de un día de antigüedad, después *conn3*, y finalmente *conn2* si la cola tiene más de un mes.

Las posibilidades de este sistema son múltiples, pero normalmente se usará para evitar el uso de conexiones de pago a no ser que sea imprescindible (colas muy grandes ó muy antiguas).

3.1.4. Proxy

El sistema de proxies permite que los clientes naveguen por internet o chateen usando el servidor como pasarela a Internet. Por tanto, esta opción sólo será posible si el servidor dispone de Internet.

3.1.5. Configuración de conexión cliente

Aquí configuramos los parámetros necesarios para las estaciones radio:

- *Crear nueva conexión.* Seleccionamos la clase de estación: **radio**.

Ahora ya podemos entrar a configurar la estación creada.

- Estado conexión: *ON* ó *OFF*
- Tipo de estación: *HF* ó *VHF*
- Modelo de radio: Descripción de la radio conectada, útil para el mantenimiento de la red. Debe ser lo más detallada posible.
- Configuración correo
 - *Intercambio de correo:* Estado del sistema de correo (*activado/desactivado*)
 - *Lista de estaciones:* Indicamos el nombre de host del servidor al que nos conectaremos.
 - *Contraseña local:* Contraseña UUCP de la estación local (por si recibe llamadas)
 - *Contraseñas remotas:* Indicamos la contraseña UUCP del servidor.
 - *Servidor a conectar:* Nombre de *host* del servidor al que nos conectaremos.
 - *Llamada PSK31 (sólo HF):* Las peticiones de acceso al servidor se pueden hacer en las estaciones HF de dos modos distintos (directamente en AX25 o por PSK31). Activamos esta opción si queremos usar el canal auxiliar PSK31.
 - *Servidor de llamadas PSK31 (sólo HF):* Desactivado en los clientes.

- *Automatización por hora:* Conexiones automáticas (por crontab) al servidor
 - *Horas de conexión (HC).* Si queremos que la conexión con el servidor se haga de forma automática por temporizador, debemos indicar las horas en las que el cliente intentará una conexión. El minuto se elige de forma pseudoaleatoria a partir del nombre de la estación (para evitar que todas las estaciones lo hagan a la vez).
 - *Llamar al servidor en HC.* Una vez configuradas las horas de conexión, indicamos si queremos que se hagan las llamadas o no.

- *Conexión dinámica:* Si existen caminos alternativos al servidor (una conexión ethernet, por ejemplo), se puede indicar las preferencias para la conexión.
- *Restricción de correo de la conexión*
 - *Restricción.* Indicamos si la estación tiene restricciones en la cola de correos de radio
 - *Tamaño máximo de mensaje.* Indicamos, en Kbytes, el tamaño máximo (una vez comprimido) de un mensaje a enviar.
 - *Tamaño máximo de la cola.* Indicamos, en Kbytes, el tamaño máximo (una vez comprimido) del conjunto de mensajes de enviar (cola de salida).

Si se supera el tamaño máximo permitido del mensaje, el sistema devuelve un correo de advertencia al usuario que envió el correo, indicando que éste ha sido borrado y por qué razón se ha hecho.
- *RelayHost TCP:* Si necesitamos usar otra estación de Relay (esto es, para que envíe los correos que la máquina tiene en la cola), indicamos aquí el host. Esta opción es especialmente útil para servidores en una Intranet que no tengan salida directa a Internet, y que deban usar un servidor principal para este fin.

- *Configuración proxy*
 - *Estado del Proxy Cliente:* Activamos o desactivamos el uso del proxy en el cliente.
 - *Proxy remoto:* Indicamos el nombre de host del servidor radio que servirá de pasarela a Internet
 - *Navegador (puerto proxy):* Puerto que usará el navegador para la navegación
 - *Proxy remoto:* Puerto configurado en la máquina remota para el proxy (3128 para Squid)
 - *Estado del Proxy servidor:* Para los clientes mantenemos esta opción desactivada.

- *Soundmodem*
 - *Tarjeta de sonido*
 - *Dispositivo:* Tarjeta de sonido usada en esta conexión.
 - *Detectar tarjetas de sonido:* Analiza los dispositivos conectados para encontrar tarjetas de sonido a usar.
 - *Guardar valores actuales del mezclador:* Hay que ejecutar esta opción una vez finalizado el proceso de ajuste de volúmenes.
 - *Frecuencia de muestreo:* Indicar un valor de frecuencia de muestreo fija. Hay algunas tarjetas de sonido que sólo funcionan a la frecuencia fija de muestreo estándar (48000, normalmente). Si vemos problemas en la transmisión que no son atribuibles al nivel del señal, podemos probar a asignar este valor y ver si se produce alguna mejoría.

 - *Dispositivo PTT.* Nombre del dispositivo a usar para activar el PTT (*Push-to-Talk*) de la radio. /dev/ttySX son puertos series y /dev/parportX son los puertos paralelo. Se debe configurar

el serie cuando usamos una placa sencilla conectada al puerto RS-232 o paralelo, mientras que sera un puerto USB (*board0/board1...*) cuando usemos la placa de interfaz EHAS. Si estamos haciendo pruebas con conexión directa entre tarjetas de sonido, podemos dejarlo desactivado.

- *Parámetros de enlace AX.25*
 - *TxDelay*: Tiempo que AX.25 espera entre que activa el PTT hasta que realmente empieza a enviar datos. El valor depende del tipo de transceptor. Los valores típicos suelen estar entre 100 y 300 msecs (parámetro sólo usado en VHF)
 - *TxTail*. Tiempo que AX.25 espera entre que ha enviado el último bit de datos hasta que desactiva el PTT. Al igual que TxDelay, este valor también depende del tipo de transceptor. Típicamente entre 10 y 50 msecs (parámetro sólo usado en VHF)
 - *Slottime*. Tiempo de espera entre colisiones de paquete. Normalmente se pone el valor 10.
 - *Ppersist*. Valor de reintento de envío de paquete. Valor de 0 (poco agresivo) a 255 (muy agresivo).
 - *RRCNN*: Off para los clientes.

- *Autoarranca soundmodem*. Esta opción permite que cada cierto tiempo se compruebe que soundmodem (el *daemon* que controla las conexiones radio) está activo. Es útil en caso de que otro proceso este usando la tarjeta de sonido, así soundmodem puede recuperarlo. En las estaciones radio deberá estar normalmente a ON.

- *Placa de interfaz*
 - *Placa de Interfaz*: ON/OFF
 - *Dispositivo*: Indica la placa EHAS-USB que se usa (*board0/board1, ...*)
 - *Control de radio desde PC*. Activa o desactiva el control remoto de la radio por CAT (*Computer Aided Tuning*). Para poder usar esta opción debemos tener la placa de interfaz EHAS, y un transceptor soportado por ésta.
 - *Modelo de Radio (sólo HF)*: Están soportadas las radios Kenwood (pruebas hechas con el modelo TK-80) y ICOM (pruebas con el modelo IC-78)
 - *Canal de datos (sólo HF)*: Antes de empezar una conexión de datos de correo se cambiará a este canal.
 - *Canal proxy de datos (sólo HF)*: Antes de empezar una conexión de proxy se cambiará a este canal.
 - *Canal de Voz (sólo HF)*: Una vez finalizada la comunicación digital, se debe volver al canal de voz por defecto del transceptor. Aquí se indica el número de este canal.
 - *Potencia de transmisión (sólo HF)*: Establece la potencia de transmisión del transceptor para las comunicacion digitales (sólo disponible para Kenwood)
 - *Espera en cambio de Voz->Datos (sólo HF)*: Introduce el tiempo durante el que se comprueba el estado del PTT de usuario. Si pasado este tiempo, en segundos, el PTT no ha sido activado, el canal se considerará libre y podrá empezar una comunicación de datos. En caso contrario, se aborta la conexión.
 - *Daemon de temperatura*: Cada placa de interfaz tiene un sensor de temperatura y un ventilador para asegurar la disipación de calor. Se indica la temperatura de activación y desactivación del ventilador.
 - *Daemon de SWR*: SWR (*Standing-Wave-Ratio*, factor de onda reflejada). Se controla el valor de potencia que la antena devuelve y así se puede avisar al usuario si hay algún problema.

- *Control de botón de placa.* Si se activa esta opción, la pulsación del botón de placa parará la transmisión radio.

3.2. Conectividad ethernet (modem, WiFi)

Bajo este apartado se configura la salida de correo electrónico de la estación cuando queremos usar un canal UUCP sobre TCP/IP (y no sobre AX.25, como en el enlace radio). Esta opción será útil en los puestos o centros que dispongan de módem para acceso a la línea telefónica o de Internet de baja velocidad (por ejemplo, VSAT) e incluso para enlaces WiFi.

- *Crear nueva conexión.* Seleccionamos la clase de estación: **ethernet**.

Dentro del menú de configuración tenemos:

- Configuración correo
 - *Intercambio de correo:* Estado del sistema de correo (activado/desactivado).
 - *Lista de estaciones:* Indicamos el nombre de host del servidor al que nos conectaremos.
 - *Contraseña local:* Contraseña UUCP de la estación local.
 - *Restricción de correo de la conexión*
 - *Restricción.* Indicamos si la estación tiene restricciones en la cola de correos de radio
 - *Tamaño máximo de mensaje.* Indicamos, en Kbytes, el tamaño máximo (una vez comprimido) de un mensaje a enviar.
 - *Tamaño máximo de la cola.* Indicamos, en Kbytes, el tamaño máximo (una vez comprimido) del conjunto de mensajes de enviar (cola de salida).
 - *Contraseñas remotas:* Indicamos la contraseña UUCP del servidor.
 - *Servidor:* Nombre de *host* del servidor al que nos conectaremos.
 - *Automatización por hora:* Conexiones automáticas (por crontab) al servidor
 - *Horas de conexión (HC).* Si queremos que la conexión con el servidor se haga de forma automática por temporizador, debemos indicar las horas en las que el cliente intentará una conexión. El minuto se elige de forma pseudoaleatoria a partir del nombre de la estación (para evitar que todas las estaciones lo prueben a la vez).
 - *Llamar al servidor en HC.* Una vez configuradas las horas de conexión, indicamos si queremos que se hagan las llamadas o no.
 - *Conexión dinámica:* Si existen caminos alternativos al servidor (una conexión radio, por ejemplo), se puede indicar las preferencias para la conexión.
- Usar modem: Si la conexión usa un módem telefónica hay que activar esta opción, para configurar los siguientes paquetes:
 - *Diald:* Llama automáticamente a nuestro proveedor de acceso, usando la conexión telefónica, cuando se detecta un intento de acceso a Internet. De igual forma, al detectar un tiempo de inactividad, el canal se cierra automáticamente.
 - *PPP:* Configuración del ISP (Proveedor de acceso a Internet)

3.3. Automatización por hora

- *Horas de arranque.* Esta entrada y la siguiente (parada) son útiles para servidores que deban funcionar durante parte del día y apagarse por las noches para ahorrar energía. Aquí indicamos la hora (formato *HH:MM*), en el que se enciende de forma diaria.

Este sistema de arranque automático usa el programa **nvr_{am}-wake_{up}**. Dicho programa, que sólo funciona en determinadas placas base, es capaz de modificar la hora de arranque de la BIOS. Si el configurador ve que la placa en uso no está soportada, usará entonces un programa propio llamado **faketimer**. Este programa es menos elegante pues cambia manualmente la hora en los procesos de arranque y parada. La hora de la BIOS, si finalmente se usa faketimer, debe estar configurada de esta forma:

- *RTC Alarm:* ON
- *Day (RTC Alarm):* 0
- *Hour (RTC Alarm):* 12:00

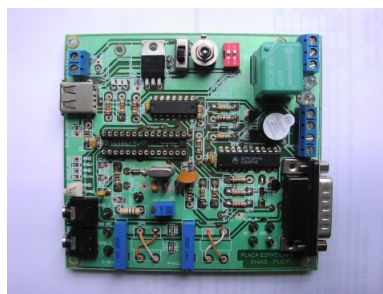
Si sólo se va a configurar una hora de arranque al día (caso común), no es recomendable hacer uso de esta opción, pues complica innecesariamente el arranque. Simplemente, se debe activar la opción correspondiente (RTC Alarm) de la que gran parte de las BIOS disponen.

- *Horas de parada.* Horas en que el PC se debe apagar. Se añade una entrada de **poweroff** en el crontab de EHAS (`/etc/cron.d/ehas`)

3.4. Placa de interfaz

La placa de interfaz permite controlar los transceptores radio y comunicarse con los sensores con los que se monitorea el óptimo funcionamiento de la estación (temperatura, voltaje batería, etc).

Figura 3. Placa de interfaz EHAS



- *Dispositivo.* Número de placa USB donde está conectado el intefaz (`board0/board1/...`).
- *Control del nivel de batería.* El ordenador testea de forma periódica el nivel de batería e informa, a través un applet para GNOME, si llega a niveles no adecuados.
- *Tensión de advertencia.* Cuando la batería baja de este valor, da un mensaje visual al usuario avisándole que debe apagar el ordenador lo antes posible.

- *Tensión de apagado.* Si la batería es inferior a este valor se asume que tiene un valor crítico, y se inicia el proceso de apagado de forma automática.
- *Control de botón de placa.* La placa de interfaz dispone de un botón con el que el usuario puede interrumpir cualquier comunicación radio, de tal forma que el canal queda libre para voz. Si queremos que el usuario tenga esta posibilidad, debemos activar esta opción; en caso contrario, la pulsación del botón se ignorará.
- *Control externo de voltaje.* Se fija los valores mínimos y máximos del ciclo de histéresis de carga de la batería. Impide el arranque del ordenador hasta que el nivel de carga sea el óptimo.

El script `/etc/init.d/edaemon` se encarga de la gestión de la placa de interfaz.

3.5. Envío de logs

Las estaciones cliente y servidor tienen la posibilidad de informar al servidor central sobre su estado y actividad. La información, si la opción está activada, se envía de forma diaria.

- *Dirección de correo.* Destino de los reportes de logs.
- *Enviar logs fijos:* El sistema centralizado de información de redes EHAS utiliza los logs que se envía de cada una de las estaciones para conocer su configuración. Siempre que se actualice un sistema por primera vez o se haga una modificación importante, se tiene que usar este comando para actualizar la información en el servidor central.
- *Modelo de ordenador.* Información sobre el modelo de ordenador y otras características destacables.
- *Postfix.* Indica si queremos enviar los logs relativos a Postfix (agente de correo).
- *Placa de Interfaz.* Logs de la placa de interfaz.
- *Radio.* Logs de las aplicaciones que usen los transceptores radio.
- *Modem.* Logs de las aplicaciones que usan el módem telefónico para conectarse.

3.6. Establecer hora y fecha

El cambio de fecha y hora se hace en Linux con `date`. Este programa no tiene una sintaxis demasiado intuitiva, así que se ha añadido esta opción al configurador para poder modificar estos datos de forma sencilla. En este mismo menú se puede configurar el huso horario en el que se encuentra la estación.

- *Fecha.* Cambia fecha con format DD/MM/AAAA
- *Hora.* Cambia la hora, con formato: HH:MM
- *Zona horaria.* Cambia el huso horario local.

3.7. Ejecución remota segura

Dado que gran parte de las estaciones de las redes EHAS están aisladas físicamente y su acceso por SSH -además de tedioso- no es siempre posible, es muy útil tener algún método alternativo para enviar ficheros y comandos por correo electrónico a una o más estaciones. Entre otros usos, servirá para la actualización de paquetes, modificación de ficheros, tareas de mantenimiento, etc.

Un punto clave a la hora de implementar un sistema de estas características es la seguridad. Si bien el acceso al correo o a la navegación internet tiene un nivel de seguridad muy bajo, en este caso

debemos garantizar que ninguna persona no autorizada pueda ejecutar comandos en las estaciones, pues esto les permitiría ganar privilegios de administrador en las mismas.

El sistema está basado en GnuPG, una herramienta de claves públicas y privadas, que permite el envío seguro de correo electrónico. Las peticiones de ejecución remota sólo se deberían hacer desde los servidores centrales, para evitar que la clave privada GPG se distribuya en muchas máquinas. Todo el sistema está automatizado en las estaciones EHAS (en el paquete *ehas-station*). La ejecución, en el servidor, se hace con el comando:

```
gruntrun grunt@estacion.dominio 'comando'
```

La clave privada GPG se encuentra en el servidor central de EHAS.

3.8. Configuración de red

Llama al configurador externo de red **netconf** (incluido en el paquete **ehas-station**):

- *Configuración*. Se puede elegir entre una configuración **automática** (si tenemos acceso a un servidor DHCP) o **manual** (estática).
- *Daemons*. Estado de algunos servicios de red.
 - *Servidor DHCP*. La estación actúa de servidor DHCP (asigna direcciones IP automáticamente a otras estaciones).
 - *Servidor DNS*. La estación actúa de servidor DNS (sirve de servidor de resolución de nombres).
 - *Cliente NTP*. La estación tiene el cliente NTP activado (sincroniza la hora por red)
 - *Servidor NTP*. La estación actúa de servidor NTP (otras estaciones pueden usarla para sincronizar la hora)
- En caso de configuración estática, deberemos indicar:
 - *Hostname*
 - *IP*
 - *Máscara de red*
 - *Pasarela a Internet (gateway)*
 - *DNS primario y secundario*

4. Protocolo de conexión radio y servicios

El primer paso será instalar la metadistro EHAS en ambos ordenadores. Para ello, siga los pasos y consejos del documento *Instalación de EHAS-Metadistro*.

4.1. Conexionado

4.1.1. Conexión directa entre tarjetas de sonido

Las pruebas de transmisión es recomendable iniciarlas primero con conexión directa entre ordenadores (sin usar las radios), para simplificar el proceso. Así, conectamos las tarjetas de sonido (*speaker* y *micro*) de forma cruzada:

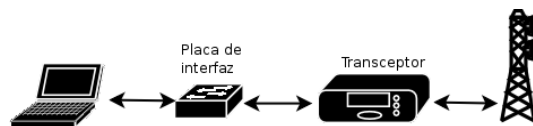
Figura 4. Conexión directa entre PCs (cruzado)



4.1.2. Conexión con radios

Las pruebas definitivas se hacen con el transceptor y la antena. En laboratorio se pueden sustituir las antenas por cargas.

Figura 5. Conexión con transceptor



4.2. Pruebas previas

4.2.1. Arranque/Parada

El sistema radio se activa con:

```
/etc/init.d/soundmodem-ehas restart
```

y se para con:

```
/etc/init.d/soundmodem-ehas stop
```

4.2.2. Mezclador

Llamamos *mezclador* al programa que permite modificar los valores de salida y grabación de una tarjeta de sonido. En la metadistro hay dos programas de este tipo instalados: **rexima** y **alsamixer**. Rexima es más sencillo de usar, pero en determinadas tarjetas de sonido no funciona bien; en estos casos es preferible usar alsamixer.

```

                                rexima

                                min . . . . . : . . . . . max
Vol          [ ===== | ----- ]      50% [ ]
Pcm          [ ===== | ----- ]      50%
Line        [ | ----- ]              0% [ ]
Mic          [ | ----- ]              0% [R]
CD           [ | ----- ]              0% [ ]
Pcm2        [ ===== | ----- ]      50%
IGain       [ ===== | ----- ]      50%
Line1       [ | ----- ]              0% [ ]
PhoneIn     [ | ----- ]              0% [ ]
PhoneOut    [ | ----- ]              0% [ ]
Video       [ ===== | ----- ]     100% [ ]
    
```

Los valores que afectan a la salida de la tarjeta de sonido son:

- **Vol.** Volumen general.
- **PCM.** Volumen de señales digitales
- **PCM2.** Volumen auxiliar de señales digitales

Los valores que afectan a la entrada:

- **Mic.** Debe estar seleccionado para grabación ([R] en rexima, seleccionado con la tecla espaciadora), pero normalmente el volumen puede estar a 0. Esto es así porque este control se refiere al volumen de loopback (reproducción de lo que llega), no del nivel de grabación.
- **InGain.** Volumen de entrada de grabación.

Si la entrada de micrófono no funciona adecuadamente, se puede probar con la entrada de *LineIn* de la tarjeta de sonido (seleccionarla entonces como entrada en el mezclador)

Estas indicaciones son generales, pues los mezcladores de las tarjetas de sonido difieren mucho según el modelo.

Los ajustes de volumen del mezclador para la correcta comunicación es un proceso complejo y que requiere algo de experiencia. En conexión directa la dificultad no es excesiva, simplemente hay que ajustar las volúmenes de salida y entrada para tener un nivel bueno (75-80% del máximo, definido éste como la anchura de la pantalla) en dsplevel, sin llegar nunca a saturar (evitar el mensaje de "clipping").

En la conexión con transceptores hay que hacer un doble ajuste, el de salida que va a la radio (que no debe saturar el transceptor) y el de entrada. La saturación en el transceptor depende del modelo; hay algunos que en el display indican la potencia efectiva que se está transmitiendo, y otros en el que veremos consultar las especificaciones del equipo. En cualquier caso, siempre se puede ajustar probando la mejora o degradación de la señal en recepción (estas pruebas hay que hacerlas en laboratorio, pues en campo resultará muy complejo un ajuste adecuado).

Una vez encontrados los valores adecuados para un modelo concreto de transceptor y tarjeta de sonido, se pueden guardar los valores para futuras instalaciones.

4.2.3. Ficheros de log

- **Soundmodem**

Soundmodem y los programas de comunicación dejan logs en `daemon.log`. Para ver en tiempo real los cambios en este fichero, es muy útil tener siempre una ventana abierta, usando el comando `tail` con la opción `-f`:

```
tail -f /var/log/daemon.log
```

- **UUCP**

Los logs de UUCP se encuentra en `uucp/Log`:

```
tail -f /var/log/uucp/Log
```

- **Correo**

Los logs de correo se encuentra en `mail.log`:

```
tail -f /var/log/mail.log
```

- **Módem**

Las conexiones telefónicas dejan logs en:

- `PPP:` `/var/log/daemon.log`
- `diald:` `/var/log/diald.log`

4.2.4. Test de enlace

Lo primero que hay que hacer es comprobar que el enlace AX25 es bueno. Para ello, se puede enviar un paquete de una estación a otra, y ver que se recibe correctamente (de la estación A a la estación B):

```
(A) call nombre_conexion TEST
```

```
(B) listen -ta
```

```
vhf: EAX25: fm URUBAH to TEST ctl SABME+ 05:34:58
```

Si el paquete se recibe, aparecerá una línea como la de arriba. Aún así, se debe comprobar los errores que ha habido en la comunicación. En pruebas de laboratorio no debería haber errores, pues las condiciones son las mejores posibles. En el fichero de logs HF deberemos ver algo así:

```
soundmodem[5046]: Sync: 10 (inter-symbol)
soundmodem[5046]: Preamble at: +0.20Hz
soundmodem[5046]: RX: Control block: l: 58, FECL: 4, FEC = 31, reqFEC = 20
soundmodem[5046]: newqpskrx[CHUPH]: BCH. Errors = 0/1728
soundmodem[5046]: Packet done at: +0.20Hz, final path metric: 0
soundmodem[5046]: S/N ratio: 22 31 21 25 25 23 24 15 23 31 21 25 24 25 17 dB
soundmodem[5046]: newqpskrx[CHUPH]: S/N ratio = 21.6
```

Vemos que tenemos 0 bits erróneos, lo cual es normal en pruebas de laboratorio (en campo ya tendremos una tasa diferente).

Para VHF el log tiene una forma como ésta:

```
localhost soundmodem[5129]: newfsk: (64/64)-(120/120) rate = 6, req = 1, l: 75. OK (ts:
localhost soundmodem[5129]: Frame 01. DATA_OK. Errors = 0/600
localhost soundmodem[5129]: newfsk: Window OK: RX-Frames: 1/1. Errors = 0/600 (0.00%)
```

Si el paquete no se recibe o llega con muchos errores, debemos comprobar que la configuración sea la misma en ambos ordenadores, que las conexiones son correctas, que los valores del mezclador de las tarjetas de sonido son los adecuados, etc.

Para comprobar que el nivel de audio es el correcto, podemos usar el programa **dsplevel** (antes debemos liberar la tarjeta de sonido con **/etc/init.d/soundmodem-ehas stop**). Este programa muestra el nivel de entrada de audio y tienen una anchura máxima de 80 caracteres (a partir de ahí indicará que se está saturando).

Para el ajuste fino de los volúmenes en transmisión y recepción se puede usar la aplicación de prueba de enlace:

```
etestax25 -c connection
```

Una vez ajustado los niveles de audio, es importante guardar los valores del mezclador o se perderán al reiniciar soundmodem. Para ello, podemos ir a la opción que hemos visto antes en config-ehas, pero manualmente podemos hacer lo mismo con:

```
alsactl store
```

4.2.5. Test de enlace PSK31 (sólo HF)

En el apartado anterior hemos comprobado que la comunicación con el módem newqpsk es correcta, pero si en la configuración de la conexión hemos marcado el uso de PSK31 como canal de conexión, debemos hacer pruebas para comprobar que funciona correctamente.

En el cliente debemos enviar una señal de prueba (beacon: *-b*) y comprobar que se recibe correctamente en el servidor (usando la frecuencia de 2500Hz: *-f2500*):

```
send-psk31 -f2500 beacon
```

En recepción (en el servidor), debemos inspeccionar el log daemon.log y comprobar que el paquete de prueba ha sido recibido. En tal caso, la salida será algo parecido a esto:

```
localhost psk31-module: Rx: (16/16). rate = 5, inlv = 1, length: 56. OK
localhost psk31-module: CRC_DATA_OK. Error= 0 /448
localhost recv-psk31: received: BBBBBBBBBBBBBBBBBB
localhost psk31-module: Packet received at: 2499.76 Hz
```

4.3. Correo

- **Llamada manual**

La llamada manual al servidor de correo se hace con la orden:

```
call-ehas -c connection user-uucp
```

La transmisión de correo se hace con UUCP. Inspeccionamos la traza del *listen*, y si la comunicación ha sido correcta, la última parte será algo parecido a:

```
EAX25: fm CENTRH to URUBAH ctl I55^ pid=F0(Text) len 36 07:22:24
```

```
0000 ....î.HY.....î.HY..0000000..0000000.
hf: EAX25: fm URUBAH to CENTRH ctl I65^ pid=F0(Text) len 25 07:22:31
0000 ....î.HY..000000..000000.
hf: EAX25: fm URUBAH to CENTRH ctl DISC+ 07:22:31
hf: EAX25: fm CENTRH to URUBAH ctl UA- 07:22:31
```

Si por el contrario la comunicación acaba antes, seguramente haya un problema con la configuración UUCP. Para ello, hay que mirar el log de UUCP (`/var/log/uucp/Log`) de ambos ordenadores.

- **Llamada automática**

La llamada automática (la que se hace a través del **cron**), ejecuta:

```
call-ehas -c connection uucp
```

Debemos comprobar que esta llamada funciona correctamente, así que lo ejecutamos manualmente y comprobamos que el servidor recibe la llamada y contesta.

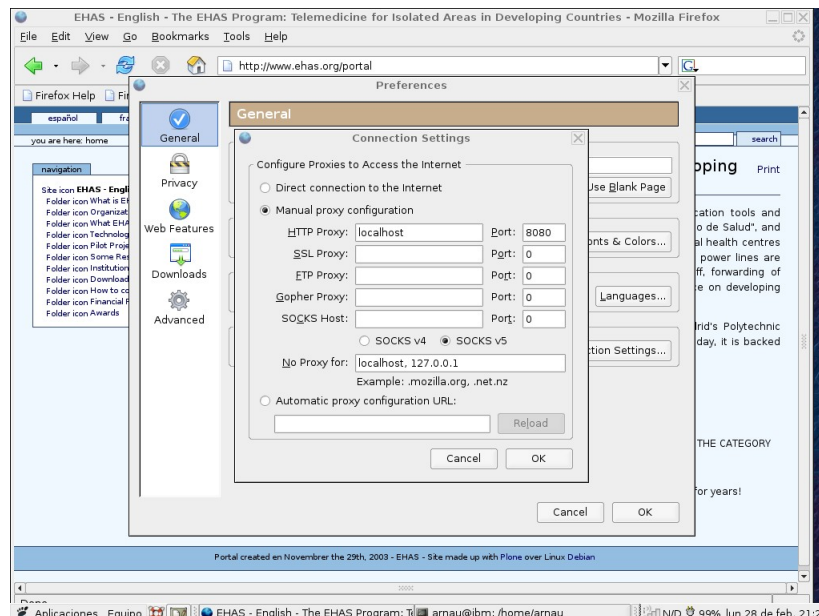
4.4. Proxy web

Para navegar por Internet, tanto cliente como servidor deben habilitar la opción correspondiente en la configuración. Se recomienda activar esta opción sólo cuando sea necesaria, pues previsiblemente aumentará el tráfico de la subred de forma considerable.

El sistema de navegación es transparente y funciona siempre que la configuración del navegador sea la siguiente:

- *HTTP: localhost*
- *puerto: 8080*

Figura 6. Configuración del proxy en navegador web



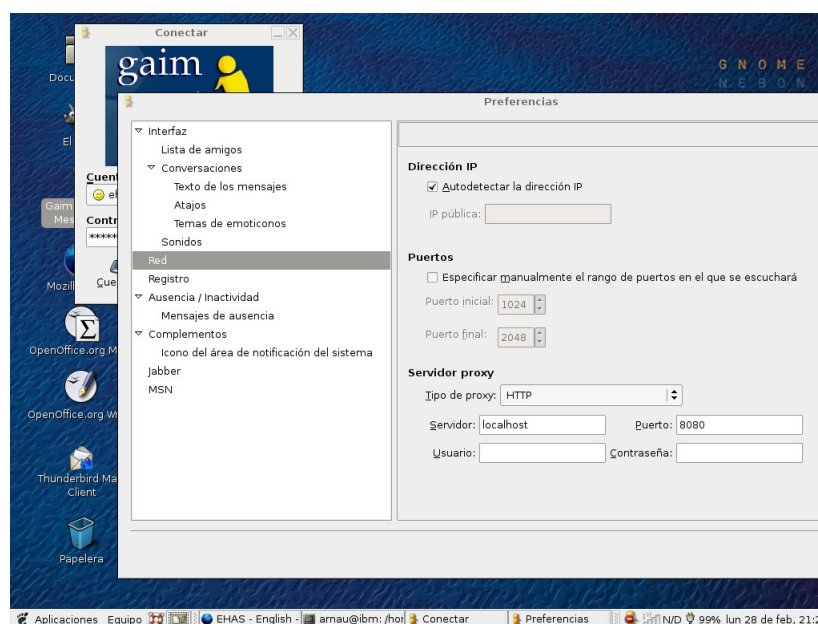
En el servidor se puede limitar el tiempo de navegación para las estaciones. El tiempo de navegación es por estación (no por usuario) y se renueva cada día. Una vez agotado el tiempo de navegación de una estación, no podrá volver a conectar hasta el día siguiente.

4.5. Chat

El sistema de chat usa un cliente de conversación (Gaim) que permite el uso de un proxy web, así que su configuración es exactamente la misma que la necesaria para la navegación:

- *HTTP: localhost*
- *puerto: 8080*

Figura 7. Configuración del proxy en Gaim



4.6. Administración remota

4.6.1. Shell no segura

Podemos entrar en cualquier estación radio con la orden:

```
call-ehas -c connection shell [ESTACION]
```

Este método no es seguro, pues la comunicación va sobre AX25 sin ningún tipo de encriptación. El password del administrador podría ser interceptado por cualquier intruso que viera trazas de la comunicación.

4.6.2. Shell segura (SSH)

Este método permite entrar en una estación de forma segura, creando un túnel SSH entre las dos estaciones. La orden es:

```
call-ehas -c connection ssh [ESTACION]
```

4.7. Chat de administración

Este chat está pensado sólo para los instaladores y montadores de la red:

```
call-ehas -c connection admin-chat ESTACION
```

5. Servicios en estaciones ethernet

5.1. Correo

- **Llamada manual**

La llamada manual al servidor de correo se hace con la orden:

```
call-ehas -c connection user-uucp
```

Debemos inspeccionar los logs de UUCP (`/var/log/uucp/Log`) de ambos ordenadores y comprobar que la conexión se ha realizado correctamente.

- **Llamada automática**

La llamada automática (la que se hace a través del **cron**), ejecuta:

```
call-ehas -c connection uucp
```

Debemos comprobar que esta llamada funciona correctamente, así que lo ejecutamos manualmente y comprobamos que el servidor recibe la llamada y contesta.

5.2. Proxy web/chat/shell

Las estaciones ethernet pueden usar el protocolo TCP/IP directamente, así que la configuración de todos estos servicios se hace de igual forma que en una red interna.

6. Certificación

A continuación se indican una serie de pruebas que hay que realizar en la estación para certificar que cumple las especificaciones de nuestro sistema.

Atención

Estas pruebas deben hacerse en laboratorio. Realizarlas en campo, donde no disponemos del material ni los recursos adecuados para solucionarlos, es totalmente desaconsejable.

6.1. Radio/Ethernet

6.1.1. Correo

Las conexiones manuales de correo se hacen con el icono correspondiente en el escritorio. Las pruebas a hacer son:

- *Correo saliente (cliente->servidor)*
Enviar un correo del cliente al servidor y comprobar recepción
- *Correo saliente (cliente->internet)*
Enviar un correo del cliente a una dirección externa en Internet.
- *Correo entrante (servidor->cliente)*
Enviar un correo del servidor al cliente.
- *Correo entrante (internet->cliente)*
Enviar un correo externa de Internet al cliente.
- *Transmisión automática de correo.*
Si se ha indicado una hora de conexión en la configuración, comprobar que ésta se produce en la hora y minuto seleccionado.

6.1.2. Proxy Web

Conectar con el servidor con el icono correspondiente y comprobar que el navegador puede acceder a Internet.

6.1.3. Chat

Confirmamos que el programa de chat funciona correctamente.

6.2. Miscelánea

- *Hora de arranque y parada.*
Comprobar que el sistema funciona según los parámetros de configuración. Asegurar que al rearrancar la estación la hora del sistema es la correcta.
- *Applet para GNOME*

Figura 8. Applet con radio HF



El sistema gráfico de la Metadistro usa GNOME, así que para este entorno se ha diseñado un applet que informa sobre ciertos parámetros de importancia para la estación. A medida que se vayan aumentando los sensores, el applet se irá adaptando. En la actualidad, muestra los siguientes datos:

1. *Radio*. Muestra el estado, la temperatura de radio e información sobre la cola de salida
2. *Ethernet*. Muestra la cola de salida de las conexiones ethernet.
3. *Batería*. Nivel de batería gráfico. Da dos avisos (de batería baja, y de apagado inmediato por nivel crítico)

El applet se actualiza cada 10 segundos.

- *Placa de Interfaz*
 - *Voltaje de la batería*. El valor se actualiza cada 10 segundos, y queda en el fichero: `/var/run/eboard/bat level`. Si se dispone de una fuente de alimentación, se puede simular la caída de tensión y así confirmar que el usuario recibe los avisos de voltaje bajo y muy bajo (en este caso la estación se apagará). El applet se actualiza cada 30 segundos, así que puede haber algo de retraso en los mensajes de advertencia.
 - *Ventilador*. Comprobar la activación del ventilador con un aumento de temperatura.

Se ha creado un script para realizar de forma rápida y sencilla una comprobación del correcto funcionamiento:

- Pruebas la placa asociada a una conexión (LED, buzzer, ventilador, PTT, canal VHF, ignición, estado de radio, botón, temperatura, SWR y CAT)

```
etestboard -c conexion
```

- Prueba los parámetros globales (batería, LED, buzzer y botón)

```
etestboard
```

- *Reporte de logs*

Los logs se envían de forma diaria. Para simular un envío se puede hacer:

```
/etc/cron.daily/zzehaslogs -f
```

- *Ejecución remota*

Los envíos de ejecución remota sólo se deberían hacer desde los servidores centrales, para evitar que la clave privada GPG esté en muchas máquinas. La orden (en el servidor) es la siguiente:

```
gruntrun grunt@estacion.dominio comando
```

El proceso de ejecución es automático en las estaciones clientes, y lo lleva a cabo el paquete **grunt-ehas**.